

DYLAN MACH

# COMPUTER PROGRAMMING FOR BEGINNERS

```
def operation == "MIRROR_Z":  
    mirror_mod.use_x = False  
    mirror_mod.use_y = True  
    mirror_mod.use_z = False  
elif operation == "MIRROR_Z":  
    mirror_mod.use_x = False  
    mirror_mod.use_y = False  
    mirror_mod.use_z = True  
  
#selection at the end -add back the deselect  
mirror_ob.select= 1  
modifier_ob.select=1  
bpy.context.scene.objects.active = modifier_ob  
print("Selected" + str(modifier_ob)) # modifier  
mirror_ob.select = 0  
bpy.context.selected_objects[0]  
bpy.data.objects[mirror_ob.name].select = 1
```

4 BOOKS IN 1:  
LINUX COMMAND-LINE + PYTHON PROGRAMMING  
NETWORKING + HACKING WITH KALI LINUX.

LINUX COMMAND-LINE

DYLAN MACH

1

PYTHON PROGRAMMING

DYLAN MACH

2

NETWORKING

DYLAN MACH

3

HACKING WITH KALI LINUX

DYLAN MACH

4

# COMPUTER PROGRAMMING for Beginners

---

*4 Books in 1:*

*LINUX Command-Line for Beginners,  
Python Programming for Beginners  
Networking for Beginners,  
Hacking with Kali Linux*

*Cybersecurity, Wireless, LTE, Networks, and Penetration Testing*

---

by Dylan Mach

**© Copyright 2020 by Dylan Mach - All rights reserved.**

The content contained within this book may not be reproduced, duplicated or transmitted without direct written permission from the author or the publisher.

Under no circumstances will any blame or legal responsibility be held against the publisher, or author, for any damages, reparation, or monetary loss due to the information contained within this book. Either directly or indirectly.

**Legal Notice:**

This book is copyright protected. This book is only for personal use. You cannot amend, distribute, sell, use, quote or paraphrase any part, or the content within this book, without the consent of the author or publisher.

**Disclaimer Notice:**

Please note the information contained within this document is for educational and entertainment purposes only. All effort has been executed to present accurate, up to date, and reliable, complete information. No warranties of any kind are declared or implied. Readers acknowledge that the author is not engaging in the rendering of legal, financial, medical or professional advice. The content within this book has been derived from various sources. Please consult a licensed professional before attempting any techniques outlined in this book.

By reading this document, the reader agrees that under no circumstances is the author responsible for any losses, direct or indirect, which are incurred as a result of the use of the information contained within this document, including, but not limited to, — errors, omissions, or inaccuracies.

# **LINUX Command-Line for Beginners**

---

---

*A Comprehensive Step-by-Step Starting  
Guide to Learn Linux from Scratch to  
Bash Scripting and Shell Programming*

---

---

By Dylan Mach



**© Copyright 2019 by Dylan Mach - All rights reserved.**

The content contained within this book may not be reproduced, duplicated or transmitted without direct written permission from the author or the publisher.

Under no circumstances will any blame or legal responsibility be held against the publisher, or author, for any damages, reparation, or monetary loss due to the information contained within this book. Either directly or indirectly.

**Legal Notice:**

This book is copyright protected. This book is only for personal use. You cannot amend, distribute, sell, use, quote or paraphrase any part, or the content within this book, without the consent of the author or publisher.

**Disclaimer Notice:**

Please note the information contained within this document is for educational and entertainment purposes only. All effort has been executed to present accurate, up to date, and reliable, complete information. No warranties of any kind are declared or implied. Readers acknowledge that the author is not engaging in the rendering of legal, financial, medical or professional advice. The content within this book has been derived from various sources. Please consult a licensed professional before attempting any techniques outlined in this book.

By reading this document, the reader agrees that under no circumstances is the author responsible for any losses, direct or indirect, which are incurred as a result of the use of the information contained within this document, including, but not limited to, — errors, omissions, or inaccuracies.

# Table of Contents

[Introduction](#)

## **[Chapter 1: What is Linux and Why Using It?](#)**

[What is Linux OS?](#)

[Why Using Linux?](#)

[A host of different distributions](#)

[Linux is the same as freedom](#)

[Linux is excellent in reliability](#)

[Linux saves you money](#)

[You can easily try Linux](#)

[Linux can run on outdated systems](#)

[More sophisticated than before](#)

## **[Chapter 2: Linux Distributions and Types of Installations](#)**

[Linux distribution for multi-purpose](#)

[Advanced users best Linux distributions](#)

[Older computers' best Linux distributions](#)

[Best distributions of Linux server](#)

[Beginners' best Linux distributions](#)

[Server Roles and Types of Installations](#)

## **[Chapter 3: Introduction to Linux Kernel and Operating System](#)**

[The System Preparation](#)

## **[Chapter 4: Installing Linux on Virtual Machine](#)**

[VMware Workstation Player Installation](#)

[The Importance of Virtual Machine](#)

## **[Chapter 5: Linux User Management and System Administration](#)**

[How to Manage Users and Groups as a Linux Administrator](#)

[Linux Group](#)

[The File System of Linux](#)

## **[Chapter 6: Linux Directory Structures](#)**

[Basic functions of the filesystem](#)

[Directory Structure of Linux](#)

## **[Chapter 7: Working with Disk, Media, and Data Files \(gzip – tar\)](#)**

[Analyze Disk Space and Hard Disk Partition on Linux with These Commands](#)

[Linux Data Manipulation](#)

[Creating from the Command-line a File for Tar GZip](#)

**[Chapter 8: File, Directory Manager, Permissions, Networking, and SSH](#)**

[SSH Command](#)

**[Chapter 9: Linux Terminals, Editors, and Shell](#)**

**[Chapter 10: Basic Linux Shell Commands](#)**

[Shell Commands](#)

[Other languages](#)

**[Chapter 11: Shell Scripting](#)**

[Features of Shell Scripting](#)

**[Chapter 12: Building Script](#)**

[Errors](#)

**[Chapter 13: Basic Bash Shell Commands](#)**

**[Chapter 14: Advanced Bash Shell Commands](#)**

**[Conclusion](#)**

# Introduction

Congratulations on purchasing your copy of *LINUX Command-Line for Beginners: A Comprehensive Step-By-Step Starting Guide to Learn Linux from Scratch to Bash Scripting and Shell Programming* and thank you for doing so.

Linux is in virtually everything we use today. If you are a beginner or you are just starting to learn everything about Linux operating system, you will soon realize that downloading this eBook is a smart way into having a clear understanding of the world of Linux as well as several of its distributions. Usually, navigating through the Linux command-line can be quite tricky. In this book, you will see multiple approaches that you can model to have a smooth operation with Linux. Also, certain Linux distributions you can use not only as a beginner but also those that can function if you attempt to use it on your old system. Ultimately, this book takes a step further to analyze basic Linux shell commands as well as shell scripting.

To this end, some of the chapters in this book will discuss Linux user management and administration, where it examines some of the duties of Linux system administrator, including handling directories, users extensively, and files, basic bash commands, root, or superuser management, and so much more. Also, this book will discuss Linux file functions as well as defining the three types of Linux file ownership, permissions, and SSH commands. You will learn about other SSH commands, Linux terminals, editors, and shell.

With a clear perception of directories, file managers, and editors out of the way, this book will discuss how you can create a file for tar gzip from the command-line, how you can mount and unmounts media, and also Linux data manipulation.

On the shelves, there are several books on Linux Command-line, and for making this book your choice, we will like to appreciate the gesture. From our end, we are striving to see that this book provides you with all the practical and necessary information you will need to succeed. Once again, thank you!



# Chapter 1: What is Linux and Why Using It?

Strengthening almost everything from mobile phones, servers, and PCs, Linux is a standard operating system that people commonly use. Indeed, all over the world, several individuals use Linux in all fields and applications you can imagine. Linux has been around since the 90s. From your TV stick to the fridge and everything, Linux runs everything. And much of the internet has support from Linux. Since the computer operating system has powered several innovations, many scientific breakthroughs have Linux to thank. Even though for decades, Linux has been supplying secure, reliable OS duties, the word “Linux” has no familiarity with the general public.

But Linux operating system is everywhere, from enterprise servers to home desktops, home appliances, supercomputers, cars, and smartphones. Everywhere, you will find Linux, and it is on your television, Roku devices, refrigerators, and thermostats. For being one of the stress-free, most secure and reliable operating system available, Linux prides itself as a preferred platform running embedded systems, servers, and desktops all over the world.

## What is Linux OS?

In the first place, what do you understand by an OS or operating system? In a physical computer, the management of the hardware is the duty of the computer code known as the operating system. Between the hardware and software, the operating system exists as a layer. Also, in assembler, communicating with a graphics card or addressing a CPU is not what most people want to know. And what acts as a middleman is an operating system like Windows or Linux.

Therefore, Linux, like Mac OS, iOS, and Windows, is an operating system. Essentially, Linux operating system powers Android, which is the most popular platform in the world. The software is likely not to function without the operating system since, as an operating system, Linux manages the communication between the hardware and software.

There are so many different pieces that Linux operating system comprises and they are:

- **Applications** – not all the complete array of apps that the desktop environments provide. As such, you can quickly find and install several thousands of software that are high-quality through Linux, typical of macOS and Windows. There are simplicity and centralization in the application installation by most modern Linux distributions. For example, typical of GNOME Software, there is Ubuntu Software Center by Ubuntu Linux that, from one centralized platform, speeds up the discovery and installation of apps among thousands of them for users.
- **Desktop environment** – users can interact with this piece. You can choose from several desktop environments like Xfce, KDE, Enlightenment, Pantheon, Mate, Cinnamon, GNOME, and so on. There are built-in applications for each desktop environment, including games, web browsers, configuration tools, and file managers.
- **Graphical server** – on your monitor, you will get a graphic display with this subsystem. It is known as X or X-server by many people.
- **Daemons** – after logging into the desktop or startup during boot, these are background services such as scheduling, sound, printing, and so on.
- **Init system** – user space is bootstrapped by this subsystem, and the control of daemons is in its charge. As such, systemd, as the most controversial, is an init system most widely used. When the bootloader, like Unified Bootloader or GRUB, handles the initial booting, the init system manages the boot process.
- **OS Kernel** – kernel can be referred to as a complete piece known as Linux for the management of the peripheral devices, memory, CPU, and the core of the system is the kernel.
- **Bootloader** – this software manages the process of the computer boot. It is a splash screen that pops up in the operating system

and soon goes away to boot for most users.

- **OS Shell** – the shell is what we use to tell our operating system the things we want it to do. As the command line by many, you use text to instruct the OS. However, the code of command-lines is known by quite a few people. As such, this caused people to stay away from using Linux. The modern distribution of Linux changed this since, just like Windows, Linux will use a desktop.

## Why Using Linux?

Most people ask this question almost all the time. When the OS that ships virtually all servers, laptops, and desktops function correctly, why would anyone bother to learn a wholly different computing environment? The answer to that question will pose another question rather than a response; are you okay with the working of your current operating system? Or are you struggling with license fees, costly repairs, crashes, slowdowns, malware, and viruses? For you, Linux may be the perfect platform if you find yourself struggling with the above. On the planet, right now, the most reliable computer ecosystem is Linux. For a desktop platform, you will have a perfect solution when you combine such the entry's zero cost with reliability. As there isn't any payment for server licensing or the software, you can have as many computers as you like to install Linux. Also, you won't have any requirement to make any payment to access Linux.

Besides that, what about having as long as you want, a stress-free, stable operating system if you are not bothered about the zero cost implications? There hasn't been an issue of viruses, malware, or ransomware by so many people using Linux, both on server platform and desktop, for more than two decades. The thing is, such attacks have no power over Linux. If only the kernel is updated, they are necessary for server reboots. And it may not be entirely out of the ordinary for a Linux server to go for years without being rebooted. You will surely enjoy dependability and stability when recommended updates are strictly followed.

Also, our computers have most of the desktop operating systems we use, and changing the operating system is something we rarely probe. What's more? Learning a new operating system is not what most people are inclined to do. However, here are some of the reasons you need to try out Linux:

## A host of different distributions

There is variance in the Linux different distributions or editions. Some are for server software, while others are designed for desktop use. And while some are designed with beginners in mind, others have their focus on the advanced users. Most Linux editions otherwise referred to as distributions, use USB drive for installation, an optical disk, or can be downloaded for free. The Linux distributions are quite endless. Though some popular choices are openSUSE and Debian, the default preferences for desktop users are mostly Linux Mint, Arch, and Fedora. Courtesy of Ubuntu Unity, Ubuntu becomes one of the most modern Linux distributions. Through the inclusion of openSUSE, you can get a more traditional Linux look with KDE. Also, it is quite a long list if you are looking for the list of server Linux OS. CentOS, SUSE Enterprise, Ubuntu Server, and Red Hat are some of the most well-known distributions. However, you may need to invest in some money with the use of some Linux server distributions as licensing may be required to use Red Hat. But, quite essential for your business is the support, which you get for your license fee in return.

## Linux is the same as freedom

There is a need to have the definition of an open source as equivalent to Linux. There are a set of principles that any software follows, such as:

- For any of your modified software, copies will have no restrictions
- The software distribution will have no limit
- There will be permission to make any changes needed by you, examine it, as well as study and disassemble the software
- Irrespective of your goals or motive for running it, the full freedom to run the software

Primarily, open-source software does not correlate to a community, and you need to understand that. Linux is built by this community, and Linux enjoys robust maintenance from that community. As such, people made Linux as software for the rest of the world, if you are wondering what Linux is and

what has brought about the popularity of Linux. It is all about this philosophy of open source.

## Linux is excellent in reliability

Since it is quite reliable, for system administrators, life is comfortable with the use of Linux. As such, not every day that you will need to monitor your server, and there are no worries with running it. Also, without impacting the whole Linux OS, you can often restart the separate services because of the way they built Linux. You must rely on a tool called an operating system, going by convention. You can have the game-changing effect of reliability that Linux brings with it if the cost isn't the most significant factor for you. And what is the biggest benefit of the Linux operating system? The biggest reason to adopt Linux is that Linux has overall immunity to random issues of an operating system as well as malicious software and viruses and also its inherent reliability.

## Linux saves you money

For you to try out Linux, you won't have to pay anything since Linux has a collaborative and open-source nature. Without licensing payment, it doesn't matter if you have multiple computers; you can go ahead and have the operating system installed freely on them. For many Linux distributions, whether desktop or server editions, this is simply the situation. For example, just for the software installation on one server, concerning the version of 2012, you will have to part with \$1,200 to use the Windows Server of Microsoft. You will have additional client access license charges if you are the type that wants several clients to have access to it. And what about the required licenses for you to run web, Windows-based services, etc.? Contrary to that, there is an inclusion of open-source server software in Linux distributions that comes without any cost. Also, without any payment for licensing, you can make use of several web pages. And with just a few clicks, you can have up and running, an entirely efficient Linux web server.

## You can easily try Linux

Linux is quite simple to try when you are prepared to experiment with it. If you are feeling hesitant, there's no need for you to have your Windows discarded. You may want to give the preferred operating system a whirl with

a live DVD or drive before installing on the hard drive of your PC on a Linux distribution. You will have to install a flash drive or DVD on a Linux distribution, a bootable system. Then, instead of your drive, have your system configured to boot from that. The fuss and muss are quite minimal as you quickly test-drive some operating systems of Linux, and the primary storage drive you have is safe since it doesn't touch it.

## Linux can run on outdated systems

A while ago, they have Windows XP tossed to the wolves, and the Windows Vista is swiftly on the brink to the end. However, some outdated PCs and many people rely on them. If you select a lightweight distribution designed for aging PCs, it can breathe a new life into your computer as well as splashes updated OS on your system. For old PCs, you can choose Ubuntu or Puppy Linux. You will also notice that there is nothing stressful concerning the transition. Since they designed it for Windows XP refugees, there is abundance when it comes to accessing Linux alternatives. For the mimic of feel and look of the operating system of Microsoft, which is highly revered, these distributions provide dedicated "Windows XP Modes."

## More sophisticated than before

The desktop's fundamental values are what most main Linux distributors follow. So, the established interface of the PC gets the spit-polish from distributions such as Linux Mint and Fedora, while with the Windows 8 disaster, Microsoft enraged the world. People can wrap their head around some Linux distributions if Windows 7 and Windows XP is their preference. It is typical for them to switch to Linux because of the learning curve that they will need to use Windows 8 or Windows 10. There is also a similarity with the Start menu of the long-established Windows with the Start menu of Linux Mint. Most fundamentally, using it with PC hardware, there is an eradication of the widespread incompatibility of Linux, particularly audio components and networking. Even though with Intel's Secure Boot enabled to have additional steps performed for the installation of Linux on your system, there is a wide range of PC hardware and modern PCs that work with most Linux operating systems. Better yet, to know whether it will work or not before you go ahead with any installation, you can have Linux distributions tested on your system to remember your preference.

There are several compelling reasons you might want to consider to try out Linux on your computer, or at least, give it a hassle-free trial run. And if you are set to go ahead with it, let's discuss the Linux distributions and how you can push forward and make the proper installation of Linux in the next chapter.

# Chapter 2: Linux Distributions and Types of Installations

You may have no clear answer if you are asking for the best Linux distributions since, in one way or the other, there are several numbers of Linux distributions, and coming up with an exact amount also can be quite tricky. As some of them appear to be unique, others are simply a clone of one another. Well, that is the beauty of Linux, even if it's a mess. However, you don't have to worry because, below, you will find the list of the best Linux distributions even when there are thousands of them around. Since there is always something for everyone, we must categorize these distributions.

## Linux distribution for multi-purpose

For both servers and desktops, as an advanced/beginner-friendly OS, you can utilize some Linux distributions. Thus, you will read below about a separate segment of these distributions, and they are:

### **Debian:**

As an excellent distribution itself, Debian has its base on Ubuntu. Debian tends to be working correctly for not only the desktop but also the servers. Though by scanning through the official documentation, you can quickly get started, it may not be the ideal operating system for beginners. There are some necessary enhancements and several changes introduced by the recent release of Debian 10 Buster. So, test-drive it for you to see!

### **Manjaro:**

The Arch Linux provides the source for Manjaro. For newbies, Manjaro makes it quite easy to use Arch Linux even though it is tailored for advanced users. So have no worries. This Linux distribution is indeed beginner-friendly and straightforward. There are a bunch of useful built-in GUI applications, as well as a fantastic user interface. While downloading Manjaro, there's an option of selecting a desktop environment. For Manjaro, most people have a preference for the KDE desktop.

### **Fedora:**

The two editions that Fedora provides are separate. It offers for servers and also for laptops/desktops. Those are Fedora Server and Fedora Workstation.



Well, Fedora may be your option if you wish to opt for a user-friendly with a possibility of a learning curve for a snappy desktop OS. Anyways, your server can get a fresh breath of a new life when you choose Fedora if you are looking for an operating system for Linux.

## Advanced users best Linux distributions

First, before you begin your exploration into Linux distributions that are designed for advanced users only, you need to get comfortable troubleshooting your way to resolve issues with the different package commands and managers. Indeed, there will be a need for you to collect specific requirements if you are a professional. However, it will worth your while to check out these distributions if, as a standard user, you have been using Linux for some time.

### **Slackware:**

Though still delighting in the preference of many people, one of the oldest Linux distributions is Slackware. You may want to consider using Slackware for setting up an ideal environment for yourself if you intend to develop or compile software. Slackware tends to be a fantastic choice for advanced users, even with a significant decrease in the number of developers and users utilizing it. Also, it is believed that Slackware will continue to carry its flagship as one of the best Linux distributions out there with the current news of it getting a Patreon page.

### **Gentoo:**

Gentoo Linux is quite compulsory for anyone who knows how to compile the source code. Though there is a required necessary technical knowledge to make it work, Gentoo is a lightweight distribution. If you need to know some information about it, you can obtain it through the official handbook. However, to make the most of it might take you a lot of time to figure if you are not sure of what you are doing.

### **Arch Linux:**

This distribution comes with a huge learning curve even though it is a powerful yet simple distribution. Everything you need may not be installed at a time, much unlike others. You will have to add packages required as you configure the system. Also, without GUI, there are a set of commands you will need to follow when you are installing Arch Linux. Also, it may be quite

essential to have a clear understanding of some critical things to do after you install Arch Linux if you wish to go ahead with the installation. It's indeed useful to say that there is an active community behind Arch Linux in addition to all the simplicity and versatility. As such, you won't have any need to worry if you run into a problem.

## Older computers' best Linux distributions

You can make use of some of the best Linux distributions available if you don't wish to upgrade your system or have an old one lying around. Here are some of the best distributions you can use for your old computers.

### **Sparky Linux:**

For low-end systems, based on Debian, Sparky Linux tends to be a perfect Linux distribution. Different users can enjoy several special editions or varieties provided by Sparky Linux, as well as a fast streaming experience. For example, it rolls releases specific to a group of users while offering a stable version with varieties. For gamers, one familiar type for them is the Sparky Linux GameOver since a bunch of pre-installed games is included in it.

### **antiX:**

As a lightweight Linux distribution and partially responsible for MX Linux, both new and old computers can use antiX. Though working quite correctly, the UI of antiX is not that impressive. Without the need to install it, antiX can be utilized as live CD distribution, and it is based on Debian. For you not to lose settings with every reboot, you can save the settings as opposed to some other distributions. Not only that, using its feature of "Live persistence," your root directory can also have some changes saved by you. As such, antiX can be your choice if you intend to offer a snappy user experience on old hardware with the use of a live-USB distribution.

### **Bodhi:**

Though it runs well on older configurations, unlike Ubuntu, it is well on top of Ubuntu that they designed and built Bodhi Linux. As a continuation of the Enlightenment 17 desktop, Bodhi Linux's Moksha Desktop is its main highlight. The fast and intuitive streaming is the typical experience users will get for using it. On your older systems, you can as well give it a try even though people's opinion of it is not for personal use.

**Solus Budgie:**

It is an impressive lightweight desktop OS with Solus 4 Fortitude as a recent major release. Desktop environments such as MATE or GNOME are natural for this when you want to opt into them. However, while being light on system resources, as a beginners' full-fledged Linux distribution, Solus Budgie happens to be one of the favorites of so many people.

**Puppy Linux:**

One of the smallest distributions you can see out there is Puppy Linux. If you want your outdated system to have a quick system execution, you can give it a try. With the addition of several new useful features, the user experience has improved over the years.

As for some of the lightweight Linux distributions, other options you can try out in this category are Peppermint, Lubuntu, and Linux Lite.

## Best distributions of Linux server

Enterprise support, performance, and stability are all that are essential when it comes to a Linux distributions' choice for servers. However, you need to pay attention to some of these recommendations, whether the purpose is for something crucial or a web server when installing it.

**CentOS:**

For RHEL, you will need to subscribe. Nevertheless, since the sources of Red Hat Linux have been derived from it, RHEL's community edition is quite similar to CentOS. Also, it is a free and open-source as well. For sometimes now, it tends to be an excellent preference. It is considerably less parallel to the number of hosting providers using it. However, people's opinion of CentOS is that of a reliable Linux distribution since its software packages are the latest. On several cloud platforms, CentOS images can be found. You can as well decide on the CentOS image that is self-hosted, which it offers if you don't.

**SUSE Linux enterprise server:**

There's a need to separate this distribution from OpenSUSE, and as such, there's no need to worry. Maintained by the community, OpenSUSE is an open-source distribution even when everything comes under a standard brand "SUSE." For cloud-based servers, one of the most popular solutions is the SUSE Linux enterprise server. And to manage your open-source solution and

to get priority support, you may need to go for a subscription.

### **Linux Red Hat:**

For organizations and businesses, the top-notch platform is the Linux Red Hat. For servers, the highly prevalent range may not be Red hat if we go by the numbers. However, Lenovo, for instance, is among those that have their reliance on RHEL as the primary selection of enterprise users. Technically, there is a correlation between Red Hat and Fedora. And for RHEL to have it on it, anything that Red Hats supports gets tested on Fedora. For you to be sure it will suit your needs, the official documentation of the distribution is worth checking.

### **Ubuntu servers:**

Your server can get unique options depending on where you want it. Ubuntu Cloud may be the perfect ideal for an optimized solution to run Google Cloud Platform, Azure, AWS, and some others. In either case, you can have it installed on your server if you want to opt for Ubuntu Server packages. However, judging by the number, when it comes to deployment on the cloud, the highly popular Linux distribution is Ubuntu. And unless you have particular requirements, the recommendation will be the LTS editions.

As options for a few of the distributions mentioned above, Debian and Fedora are some of the distributions to explore.

## **Beginners' best Linux distributions**

This segment deals with a list of distributions that are quite easy to use. Without the requirement of knowing any tips or commands, you can begin using it right away, and there's no need to dig deeper.

### **Pop!\_OS:**

Computer science professionals or developers will experience an excellent pick by Sytem76 from Pop!\_OS. If you are beginning to use Linux, it is also quite a great choice as it is not limited to coders. Though the UI feels smooth and a lot more intuitive, it is based on Ubuntu. Also, it enforces full-disk encryption out of the box in addition to the UI.

### **Zorin OS:**

One of the most intuitive and good-looking OS for desktop is another Ubuntu-based distribution, which is Zorin OS. Notably, the recommendation for users without any Linux background will be this distribution after Zorin OS 15 release. It also comes baked in as well as a lot of GUI-based applications. Though ensure to choose the “Lite” edition because you can also install it on older PCs. There are also “Ultimate,” “Education,” and “Core” editions. However, consider getting the Ultimate version if you intend to help improve Zorin and also support the developers. Otherwise, select the Core edition for free.

### **MX Linux:**

It has been a while now that MX Linux has been in the game. On Distrowatch.com, at present, MX Linux is a highly preferred Linux distribution. You will be amazed as to how you will get familiar with it if you haven’t used it before. With Xfce being its desktop environment and also based on Debian, an increasingly popular Linux distribution is MX Linux, unlike Ubuntu. Also, any Mac/Windows user can easily use it as it is packed with several GUI tools in addition to its excellent stability. Also, for installation with one-click facilitation, the package manager is ideally tailored for this. And as one of the sources that are already in the package manager, you will see Flathub there, and in no time, you can install it after searching for Flatpak packages.

### **elementary OS:**

An elegant Linux distribution out there is the elementary OS. It is easy to get comfortable with it if you have already used a Mac-powered system because the UI has a similar resemblance to MacOS. While keeping the performance in mind and also looking as pretty as possible, delivering a user-friendly Linux environment is the focus of this distribution that is based on Ubuntu.

### **Linux Mint:**

Among beginners, another popular Linux is Linux Mint Cinnamon. When Windows XP was discontinued, as a result, many users opted for it since there’s a resemblance between Windows XP and the default Cinnamon desktop. It has the applications available for Ubuntu since it is on Ubuntu that Linux Mint is grounded. It becomes a prominent choice for new users of Linux because of the ease of use and simplicity.

### **Ubuntu:**

One of the most undoubtedly popular Linux distributions is Ubuntu, and on several laptops available, you can even find it pre-installed. You will get comfortable with its user interface. As per your requirements, you can easily customize the look of it if you play around. Mainly, theme installation is also another option for you. When you want to get started with Ubuntu, you will need to learn more about it. Also, Ubuntu users have a massive community that you can find in addition to what it provides. So, go to a subreddit or the forum if you face any issue. You need to check out some coverage online on Ubuntu in case they require direct solutions in no time.

Ultimately, you can give some of these distributions recommended above a try. And quite honestly, the choices will be subjective depending on personal preferences to each of them even when there are quite several Linux distributions that deserve mention.

## Server Roles and Types of Installations

Since more operating systems have a great connection with it, this attribute is a unique feature of Linux. Thus, you can have other OS running alongside Linux. With more operating systems in place and for the installation of Linux, the general process of installation is to install Linux again. When you do that, the computer will have 100 percent resources dedication to run Linux. However, as part of an OS sequence which is obtainable on a computer, it is not quite hard to have Linux installed. Also, as an approach you can use to run or install on a computer any distribution of Linux, you can make use of some of these approaches below;

### **Linux fresh installation**

One popular method of installation available is this method. From a DVD/CD, you will install Linux after formatting the hard drive of your computer when you jump into this technique. Then, it is only on the operating system of your computer that Linux will then run. Available methods of installation are:

- PXE
- Kickstart
- Network installation through HTTP, FTP, or NFS

- Hard drive
- CD-ROM

### **Linux as a VM inside another operating system**

Inside another operating system, you may want to consider running Linux as a VM if you prefer to run your favorite open-source software or want an easy way to access a Linux desktop even when you like your current, non-Linux desktop OS. You will need to download and install a Virtual Server application as a simple step, although there are several ways to go by it. Then, under the host software, install your Linux distribution. Thus, you may perform on Linux everything you can do with your other operating system. Even when your other operating systems don't offer some things, there are a lot of things that Linux can provide you.

### **Live DVD/CD booting Linux**

You may choose to try Linux from a Live DVD/CD when you want to retain your primary operating system and to see if you like it, you want to give Linux a try. As a Live CD, several Linux installations offer this running or downloading. As such, from the DVD/CD, Linux will run as an entire operating system that is quite bootable. And instead of running it on a hard drive, you can load your files into the memory of your computer. That means, from a DVD/CD, Linux can be run and then exclusive of any variance, return to its old OS of your system as you remove the DVD/CD when you reboot your computer. Until you discover your preferred choice, you can easily sample some Linux distributions.

### **Dual-booting**

You will have a dual booting system when you want to install Linux and also keep an existing operating system as well. You will then need to decide which one you would like to boot into during the boot process since you will have a PC that can use two different operating systems.

By now, you must be having a bit of understanding of Linux, as well as some distributions that you can use them. Now, it is time to take things further and introduce to you Linux Kernel as well as the operating systems.

# Chapter 3: Introduction to Linux Kernel and Operating System

By what means does a computer manage the most complex tasks with such accuracy and efficiency? Well, the short and simple answer is that a computer does everything with the help of the operating system. The operating system makes life easier and performs different tasks through the efficient use of hardware resources. At a high level, there are two parts we can divide the OS. The first part will be the utility programs, while the other is the kernel. The kernel services some of the system resources requests like network connectivity, memory, storage, CPU, and so on, as asked by the various user space processes. And in Linux/GNU, there will be an exploration of the loadable kernel modules by this column. Since the whole operating system solely run in supervisor mode, this makes Linux kernel monolithic. With each subsystem responsible for performing specific tasks, it consists of several subsystems, even though the kernel is a single process. Broadly, these following tasks are performed by any kernel.

## **Dynamically loadable kernel modules**

To ensure that our system is up-to-date, most times, we install security patches and kernel updates. A reboot is often necessary in the case of MS Windows. However, this is far from being suitable. For example, when it is in a production server, the machine cannot be rebooted. Then, without a system reboot, wouldn't it be ideal for removing or adding functionality from or to the kernel on-the-fly? For the kernel modules, the Linux kernels work on the dynamic unloading and loading. And at runtime, any code piece is a kernel module that you can add to the kernel. Without any interruption, when the system is up and running, you can unload and load the modules. You can use the `insmod` command to dynamically link a kernel module to the running kernel and also unlink it by using the `rmmod` command, as an object code.

## **Networking**

One of the vital parts of the operating system is the networking because it works with data transfer between hosts and also allows communication. As routing functionality gets enabled by it, it is also through it that network packets get transmitted, identified, and collected.



## **Device control**

There are several devices required for any computer system. However, for the layer to offer functionality, there is a need for a device driver to make the devices usable. Video/audio drivers, Bluetooth drivers, graphics drivers, and so on are some of the types of drivers present.

## **File system**

The file system heavily influences the Linux/GNU system. Nearly everything is a file in Linux/GNU. Also, conventional for the organization of data hierarchically, journaling and compression of data, deletion, and creation of files, and so on are the storage relation requirements controlled by this subsystem. All primary file systems have the support of the Linux kernel, such as MS Windows NTFS.

## **Memory management**

This subsystem handles every related request. The pages are chunks of fixed size as divided from available memory, and on any demand, can be de-allocated or allocated from or to the process. As it creates the illusions of contiguous ample address space to a physical address space, it also maps the process virtual address with the help of the memory management unit, MMU.

## **Process management**

The life-cycle gets this subsystem to handle the process. Through inter-process communication, it allows data sharing and connection between processes as it also destroys and creates processes. Also, it enables resource sharing and schedules processes with the help of the process scheduler.

## **Some Useful Utilities**

For the provision of useful information about the kernel modules, Linux/GNU offers several user-space utilities. Now, let's dive into them.

*dmesg*: though it is a different methodology that the kernel uses, it is on the standard output stream that any user-space program displays its output, i.e., */dev/stdout*. For us to manage the contents of the ring buffer, with the use of the *dmesg* command, the kernel appends its output to the ring buffer.

*modinfo*: as a command-line argument, the module that passes such process displays the information by this command. For modules, it searches the */lib/modules/<version>* directory if the argument is not on a filename. Also,

it is on the `field:value` format that `modinfo` shows each attribute of the module.

It is essential to note that the kernel version is `<version>`, and it is through the execution of the `uname -r` command that we can obtain it.

*rmmod*: when you want to unload modules from the kernel, you can make use of this command. It is only when the current module is not in use that you can unload. Also used to unload modules forcibly, the `-force` or `-f` has the support of *rmmod*. However, the danger in using this option is extreme, and to remove modules, you can still make use of a safer way. As it waits until the module is no longer used, *rmmod* will isolate the module with the option of `--wait` or `-w`.

## The System Preparation

Now, it's action time. An environment for development is all we need to create now. We will have a Debian-based Linux/GNU distribution like Ubuntu and CentOS or a RPM-based Linux/GNU distribution installed as the required packages.

### CentOS installation

As a root user and by implementing the command below, the first step is to have the compiler for *GCC* installed:

```
[root]# yum -y install GCC
```

Now, the packages to develop the kernel are the next in the installation level:

```
[root]# yum -y install kernel-devel
```

In conclusion, the utility of the *make* comes next for the installation:

```
[root]# yum -y install make
```

### Ubuntu installation

The compiler for *GCC* is the first in the installation line:

```
[mickey] Sudo apt-get install GCC
```

Then, the packages for kernel development come next:

```
[mickey] Sudo apt-get install kernel-package
```

Then, the utility of the make installation:

```
[mickey] Sudo apt-get install make
```

And we have the kernel module

Now, we have prepared our system. Then, we will need to have the initial module of a kernel written. Using the following contents, use *hello.c* to have the file saved when you open your favorite text editor:

```
#include <linux/kernel.h>
#include <linux/module.h>

Int init_module (void)
{
    printk(KERN_INFO "Hello, World !!!\n");

    return 0;
}

void cleanup_module(void)
{
    printk(KERN_INFO "Exiting ...\n");
}

MODULE_LICENSE("GPL");
MODULE_AUTHOR("Narendra Kangralkar.");
MODULE_DESCRIPTION("Hello world module.");
```

At least, there are two functions for any module. The function of cleanup is the first and second initialization. As such, a cleanup utility is

*cleanup\_module()* while the initialization function is *init\_module()*. And once you load the module and before the module is unloaded, there will be a call for the initialization function, and then the call for the function of cleanup. Other macros, as well as *MODULE\_LICENSE*, are quite easy to follow. Relatively the same as *printf()*, the user-space is the syntax, which is a *printk()*. However, at a regular productivity stream, it doesn't print messages, unlike *printf()*. Instead, it is the kernel's ring buffer that receives messages that it appends. There is a priority from each declaration of *printk()*. In the example, *KERN\_INFO* priority is used. And between the string of format and *KERN\_INFO*, you won't see any comma (,) there. Without the presence of unconditional priority, you can make use of *DEFAULT\_MESSAGE\_LOGLEVEL* priority. As an indication of success, there is the return 0 in *init\_module()* final declaration.

*cleanup\_module()* and *init\_modules()* are the name of the cleanup and initialization functions. However, we can make use of whichever name in place of cleanup and initialization function with ( $\geq 2.3.13$ ), which is the new kernel. For rearward similarity, there is support for these dated names. In place of the register of the cleanup and initialization functions, the macros provided by the kernel are *module\_exit* and *module\_init*. Now, with the names of the preference we have for cleanup and initialization functions, let's rewrite the same module:

```
#include <linux/kernel.h>
#include <linux/module.h>

Static int _init hello_init(void)
{
    printk(KERN_INFO "Hello, World !!!\n");

    return 0;
}

static void _exit hello_exit(void)
{
    printk(KERN_INFO "Exiting ...\n");

    return 0;
}
```

```

}

static void _exit hello_exit(void)
{
    printk(KERN_INFO "Exiting ... \n");
}

module_init(hello_init);
module_exit(hello_exit);
MODULE_LICENSE("GPL");
MODULE_AUTHOR("Narendra Kangralkar.");
MODULE_DESCRIPTION("Hello world module.");
MODULE_VERSION("1.0");

```

What we have in this place is that the cleanup and initialization functions imply the `_exit` and `_init` keywords.

## Module loading and compilation

Right now, the procedure for module compilation needs to be understood. We will make use of the build system of the kernel for the compilation of the kernel module. Before you have it saved as *Makefile*, you may want to have the process of the collection written down as you, once again, open your favorite text editor. Here, you need to pay attention because you must have a similar directory for the modules of kernel *Makefile* and *hello.c*.

There is a requirement for the kernel headers for us to have the modules built. From the kernel's source, the kernel build system is incited by the above *makefile*, and finally, to complete the module, the *makefile* of the kernel may have our *Makefile* invoked. You can complete the process as name *hello.ko* for the kernel module you develop since, to have the module built, all the requirements are now in our possession.

The first compilation of the first module of the kernel is now successful. Now, it is time to examine the way to, inside a kernel, unload and also load this module. You must take note that to unload or load kernel modules; we need to acquire the root user privileges. You will need to have the command *insmod* executed when you change to the mode of a super-user to load a

module as you will see the following:

```
[root]# insmod hello.ko
```

And the success job has been done by *insmod*. However, the output is necessary for us to find. It is the ring buffer of the kernel that the output is appended. Well, through the execution of *dmesg* command, we can as well find out:

```
[root]# dmesg
```

```
Hello, World !!!
```

Also, we can verify if or not the module is stocked by using the command *lsmod* :

```
[root]# lsmod | grep hello
```

```
hello 859 0
```

All that is required of you is to check the output of the *dmesg* command as you have the command *rmmod* executed. As you see below, to unload the module from the kernel. Now, through the function of cleanup, you will see the message from *dmesg*. Some macros within the module give us the module's information. And in such an attractively configured style below, displaying the information is the command *modinfo*.

### **How to identify the process' PID**

For us to identify a Process ID, which is the existing process's PID, we may need to compose one more module of the kernel. In the header, defined as the *<linux/sched.h>*, it is in the structure of the *task\_struct* that the related information of the kernel stocks all progression. As an indicator of the existing process, it offers an *existing* variable. You are only required to have the *current->pid* variable value printed to have the current process PID identified. The (*pid.c*), a complete code of working, will then be given.

In the object file's name, with a slight modification, similar to an original *makefile* is the *Makefile*. With the use of the *dmesg* command, have the output squared after inserting the module and then make the compilation.

## **Bridging several files with a module**

From a single file, the module compilation has been explored. However, dividing the module into multiple files can be quite convenient, and for a single module, we have multiple source files in a large project. For the building of a module that extends over two files, we must understand the process. From the file *hello.c*, we can divide the cleanup and initialization functions to become two individual files such as *cleanup.c* and *startup.c*. The change will be like this for *cleanup.c*. Then, we will have the exciting part concerning the two modules, the *Makefile*. Self-explanatory enough is the *Makefile*. Now, in our proposition: with the use of *cleanup.o* and *startup.o*, develop the final kernel object. It is time for the compilation and testing of the module. When we utilize the command *modinfo*, we may display module information. From each module, author-related information, license, description, and versions are now shown through the command *modinfo*. It is now the time for output verification by unloading and loading the module for *final.ko*.

The best place to learn more about modules is the kernel source code. When you go online, you can download the latest source code. Right now, we will have to go ahead and discuss in detail how you can install Linux on Virtual Machines. Let's go!

# Chapter 4: Installing Linux on Virtual Machine

You might not be sure about dual booting even after installing Linux when you try it from a live CD/DVD. It can be quite useful to use a virtual machine, VM, to install your preferred Linux operating system. What this translates into is that the conditions of a hardware environment are the replication of a software environment. With the limit only coming from the components inside it, the base of your physical PC's hardware is the environment. For example, with two cores, it may be impossible to have on a processor, a virtual four-core CPU. However, on a CPU equipped computer, the outcomes can be far superior, while virtualization can be achieved on many systems. As there are several of them in Windows, for the installation of the Linux operating system to be easy, several virtualization tools are quite available. The one among them to produces the significantly accomplished virtual machine applications is VMware. Now, with the use of VMware Workstation Player, it is time to discover the process of Linux installation in Windows.

## VMware Workstation Player Installation

In the initial phase, you will need to have the latest version of the VMware Workstation Player tool downloaded by going to the VMware website. With the 64-bit version, it is about 80 MB for the release of 12.5. For home, personal, and non-commercial use as an evaluation version, you can find VMware Workstation Player for free. For non-profit organizations and students, getting value from the free version is all that makes VMware delighted. As for the functionality factor, the standard virtual machine tasks hosts everything included in the VMware Workstation Player. However, for the business of all levels are the extensive selections of virtualization solutions offered by VMware.

Then, it's time for installation after you must have downloaded VMware Workstation Player. An Enhanced Keyboard Driver installation option will be available for you as you get your guide from a standard installation wizard. Also, you will be able to handle the international keyboards provided



by this feature. Just in case, you will see that it's worth installing even as you mightn't need it in the first place. When prompted, restart Windows as you proceed via the installation wizard.

### **Desired Linux operating system selection**

For the kind of Linux that you want to give a try, you likely know it. In a VM, while you will find some Linux distributions not especially suitable, others will be. Conventionally, in VMware, for ARM architecture like the Raspberry Pi, running Linux distributions may not be possible. As such, with the x64 and x86, you may not be able to virtualize the ARM. However, it is time to examine QEMU.

### **Virtual machine configuration**

You can as well proceed with the setting of your VM with the download of your Linux operating system. When prompted, input your email address as you begin to launch VMware Workstation Player. Getting the software for free is what this aspect is all about, and the email list of the VMware gets you on board. The primary application of VMware Workstation Player will load when you have completed that level. And to proceed, your virtual machine will require the creation of an account. The ISO, installer disc image file is the default that you will choose. Note that there is an option of installing the OS later by merely having a blank disk to create a virtual system. Then, you will click "Next" after the installation of your preferred operating system. Your chosen guest OS will install automatically as a message about the installation of VMware Easy Install.

### **Account creation**

Your password, username, and the preferred name are all the information you will enter in the next screen and then hit the "next" button when you name your VM. For the operating system that you are installing, what most times follow its name is the default, and also for your VM, you may go ahead and choose a location. Hit the "next" button again, and you will select the disk capacity for your VM. As a series of files or a file for the physical disk of your computer, this is a saved virtual hard disk. Either option is there for you to select. Meanwhile, you can either alter or accept a recommended size used for your virtual HDD. It could be more than striking because increasing tends to be a safer option. Hit the "next" button again, whatever your choice to come to a screen with "ready to create the virtual machine." Hit on the "finish" button, and the VM will start. So far, after creation, run your virtual

machine. Soon, you get the suggestion for the tools of VMware for Linux package, which will arrive through an alert. As an approach to the Easy Installation process, this may not be that necessary. But it's fine when you accept this.

### **Virtual hardware customization**

The customize hardware is another option on the screen for “ready to create...” Now, in another way beyond the HDD, you may want to tweak the hardware of the virtual machine. There are so many options you can choose from, including network adaptor configuration, processors, and memory. You may want to check out the screen of Processors. You will come across a reference to a Virtualization engine in the right-hand pane. This process is already in Automatic by default. As such, indeed, for Linux, you may not have to worry about anything. However, you can set this to Intel VT-x or other alternatives if you run into any problems. Then, in the Memory screen, you can deal with specific issues of performance. Here, also, as a recommended maximum and minimum for your virtual machine, you can see the diagram of the suggested size of RAM. Stick to these recommendations as it tends to be ideal. You may likely slow everything from running the VM software to standard system tasks with the impact on your PC performance when you set the Ram too high, and you will still have issues at hand by going too small.

Ultimately, your settings for display will require a bit of your time. Here, you can decide to set up multiple monitors in your virtual machine or utilize the host computer's monitor settings since you will have the ability to toggle 3D acceleration. There will be a display of a recommended amount as with system memory for the guest operating system, and you can also adjust the graphics memory.

### **Using Linux in VMware Workstation Player after installation**

On a physical desktop machine, it is typical of the operating system installed in the virtual machine to boot the ISO. You can go ahead and automate the entire process through the method of Easy Install, and to apply for setting in the guest, the virtual OS, you can use your Windows host OS configuration. It is useful to pay attention here because you can have the overall control over the operating system installation if you chose the option to install the OS later. Then, you can begin to use the guest OS since you will have access to log into the virtual machine when the installation is complete with the use of

Easy Install. As simple as that! Subsequently, with the menu where your virtual machine can be opened, you can also launch the VM.

## The Importance of Virtual Machine

For Linux, hardware happened to be a significant encounter in 2005. People were having different issues with USB devices, graphics, Bluetooth, and even wireless. And to make things work, you might have to find wrappers and drivers all the time a new invention came people's way. Since the virtual machine appeared not to be the option, and for any user of Linux to identify the solution, they must interact with the 'real' hardware. However, there have been so many changes. On Linux, a handful of hardware works unplanned. There has been a shift in the focus on the distributions' unique features with less essence on the support for hardware. You can write about them on a similar machine if you can easily play with multiple distributions, and you are a virtual machines' heavy user.

Now, for new users of Linux and the ways they can take advantage of them, let's discuss some benefits of virtual machines even though in the enterprise segment, virtual machines are used extensively.

### **Who needs to use a virtual machine?**

Since there is no availability of specific proprietary services and software, some users of Linux have to boot in twofold. And there is only support for Windows concerning tax filling software as well as some related works by the government in many countries. For you to run Windows software, you can easily use a virtual machine instead of working through the pain and complexity of dual booting. Then, it is only on gaming that the virtual machines may not function. Mainly when you are playing resource-hungry games such as Crysis, to have the desired gaming experience, you may need to talk to real RAM, GPU, and CPU. Since between the hardware and the application, you may not like a virtual layer, video, and audio editing may not work either. Virtual machines work great outside of these and even a few other capacities.

Also, by switching to Linux or formatting the operating system they were used to or playing with Linux, for the individuals that attempt to make a change as non-Linux users, a virtual machine may also be useful. When they are ready, they will have the self-assurance to make the shift since virtual

machines get these individuals comfortable with Linux. As such, inside your Windows 10 or Mac OS, you can be running Linux. Above all, to switch between distributions without having to reboot on the same hardware, you can run multiple Linux distributions on virtual machines. Instead of entirely dependent on anyone or being vendor-locked, you will need to be versed with several major distributions as a Linux user. And without having to log out to change the environment, on the same system, you may similarly run various desktop backgrounds with the use of virtual machines. You may not know the type of operating system your client or employer would be using. Thus, in any Linux, you will need some knowledge because you certainly don't want to know only one distribution if you're aspiring to become a developer or system admin. And for testing your applications, you will require several distributions if you are a developer.

As you can see now, working with virtual machines has several advantages. Also, operating virtualization has some significant benefits, which is efficiency, apart from multi-booting. Switching between different distributions and having hard drives formatted can be a waste of your time. So, it is as simple as starting the latest application, and without affecting your work, you can begin a new virtual machine for distribution with virtual machines. A virtual machine can be bliss if you are an enthusiast or distribution-hopper. Keep your attention on several other distributions such as Linux Mint, Fedora, Ubuntu, Kubuntu, OpenSUSE, and so many others even if you are an Arch Linux user. As it takes up space and misuse of financial means, having several physical systems can be virtually impossible. It pays to make a good investment in some multicore processor and more RAM, which can run additional virtual systems than buying six physical machines. Now, you won't experience any form of downtime if, on the same machines, you handle nearly a dozen distributions.

### **The types of virtual machines to use**

You have some alternatives, including VirtualBox, Xen, KVM, Qemu, VMware, and so much more. Others have their advantages and also their disadvantages. Though, solutions such as KVM tend to be quite efficient and more powerful even if you have a preference for VirtualBox. As a new user of Linux, you will find the ease of use of the VirtualBox. And without technical know-how that can be quite hard-core, you can access its tons of functionalities and features. Since VirtualBox can be installed on Mac,

Windows, and Linux, and the support for cross-platform is its most significant advantage.

# Chapter 5: Linux User Management and System Administration

In computing technology, the major strength is Linux. Linux powers several of the cloud-servers, supercomputers, personal computers, mobile phones, and web servers. In addition to using command-line interface tools and Linux tools to take backups, creating, enhancing, and maintaining user reports or accounts, managing the operations of a computer system is the job of a Linux systems administrator. Linux powers most of the computing devices because of its open-source environment, high security, and high stability. It is essential to know and understand the specific qualities of an administrator of a Linux system:

- Handling users, directories, and file
- Basic bash command
- Managing superuser or root
- Files system hierarchy
- Linux file systems

## **A Linux administrator's duties**

For an institute or organization that needs an excellent IT foundation, a reliable criterion is the system administrator. Hence, all-time requirements will be the need for efficient Linux administrators. As there may be additional duties and responsibilities to the role, from each organization, the job profile might change. Here are a few responsibilities of a Linux administrator:

- During an issue with the server, it is the job of the administrator to troubleshoot.
- Essential security tools and system installation. To make necessary recommendations after analyzing hardware requirements, the administrator works with the data network engineer and other departments or personnel.

- Ranging from login issues to disaster recovery, Linux administrator detects and solves the service problems.
- For the Linux environments and its users, creating, maintaining, and enhancing the required tools.
- One of the characters of a Linux administrator is to communicate at all times in a professional, cultivated manner with customers, vendors, and staff.
- Apart from offering excellent customer support for ISP, web hosting, and LAN customers about troubleshooting all increased support troubles, Linux administrator also fixes and analyzes all error logs.
- Part of the duties is listing backup, creating new stored procedures, and taking regular backup of data.
- Internet request maintenance, such as PHP, MySQL, Apache, RADIUS, and DNS.

### **Linux system admin career process**

- Learn how to install and use Linux environment
- Have Linux administration certification
- Become an expert in documentation
- Look for help and support by joining community or group of a local Linux users

Necessarily, taking backup and managing the operations, such as examining hardware and software systems, are a few roles of the Linux systems administrator. Also, the admin must be able to describe technical knowledge understanding quite profoundly.

## **How to Manage Users and Groups as a Linux Administrator**

All at the same time, more than one user can make use of Linux since it is a

multi-user operating system. And to manage users in a system, Linux offers a beautiful mechanism. Therefore, getting along with the groups and users in a system is the most significant function of a system administrator. And we will use the CentOS Linux distribution to talk about all the commands used below.

## **Linux user**

The unique identification number, UID, is a binary number that uniquely identifies an account of a user of a system. Normal users and super or root user are the two types of users. There will be limited access to files for the regular users while there will be full access to all the data for super or root user. A user account can be modified, deleted, or added by a superuser. It is in the `/etc/passwd/` file that the full account information is stored and also on the `/etc/shadow/` file that a hash password is stored.

## **Using a default setting to create a user**

At the command prompt, by running the `useradd` command, a user can be added. Use `passwd` utility to set a password after creating the user like this:

```
[root@localhost handy32]# useradd enirban
```

```
[root@localhost handy32]# passwd anirban
```

*Changing password for user anirban.*

*New password:*

*Retype new password:*

*passwd: all authentication tokens updated successfully.*

There will be an automatic setting of the default shell to `/bin/bash`, creation of the home directory (`/home/<username>`), and the assigning of a UID by the system. Anytime the system has added to it a new user and also uses the user name for the group, a user private group is created by the `useradd` command. When a user is created, specify the full name of the user. For the specification of the full name of the user, use `useradd` with the option `-c` as a system administrator:

```
[root@localhost handy32]# useradd -c "Anirban Choudhury" handy32
```



## Using UID to create a user

Using the `-u` option and a custom UID, a user can be created like this:

```
[root@localhost handy32]# useradd -u 1036 handy32
```

## Using the home directory with a non-default to create a user

By doing the below, you can set a home directory with a non-default:

```
[root@localhost handy32]# useradd -d /home/test handy32
```

## Having user added to a supplementary group and primary group

Through the specification of the `-G` and `-g` option, it is possible to specify a complementary group and the primary one as an administrator.

```
[root@localhost handy32]# useradd -g "head" -G "faculty" handy32
```

## User lock and unlock

A user account can be locked or unlocked by a superuser. Using the option `-` / , you only have to invoke `passwd` to lock an account.

```
[root@localhost handy32]# passwd -/ handy32
```

*For user handy32, Locking password*

*passwd: Success*

To unlock an account, you can use `passwd` and the `-u` option:

```
[root@localhost handy32]# passwd -u handy32
```

*For user handy32 to unlock password*

*passwd: Success*

## Changing username

For username login change, use `usermod` command with the `-/` option:

```
[root@localhost handy32]# usermod -/ "nishant" handy32
```

## User removal

Using the home directory and a user with the combination of the `-r` option and `userdel` :

```
[root@localhost handy32]# userdel -r handy32
```

## Linux Group

A mechanism used for the collection and organization of users is the Linux group. The group ID, GID, is a uniquely associated ID for each group, like the user ID. We have the supplementary and primary groups as the two types of groups. The primary group belongs to each user and of zero or more than zero complementary groups. It is in `/etc/group/` that the information of the group is stored and also in the `/etc/gshadow` file that the respective passwords are stored.

### Using the default setting to create a group

As a root user, run the `groupadd` command with the default settings to add a new group:

```
[root@localhost handy32]# groupadd employee
```

Using the group name, type `gpasswd` if you want to add a password:

```
[root@localhost handy32]# gpasswd employee
```

For group employee, changing the password

New Password:

Re-enter new password:

### Using a specified GID to create a group

With the use of the `-g` option, execute the `groupadd` command to specify the group's GID explicitly:

```
[root@localhost handy32]# groupadd -g 1200 manager
```

### Group password removal

Using the proper group name, run `gpasswd -r` to remove a group password:

```
[root@localhost handy32]# gpasswd -r employee
```

### **Changing the name of the group**

As a superuser, use the `-n` option as you run the `groupmod` command to change the name of the group:

```
[root@localhost handy32]# groupmod -n hrsupervisor employee
```

### **Changing the GID of the group**

Along with `-g`, run the `groupmod` command to change the group's GID:

```
[root@localhost handy32]# groupmod -g 1050 manager
```

### **Deleting a group**

You will first need to delete the users of that primary group before you can delete a primary group. With the group name, run the `groupdel` command to delete a group:

```
[root@localhost handy32]# groupdel employee
```

## **The File System of Linux**

The technique of storing files on a hard disk is a file system. And Linux supports several types of file systems including:

- Special-purpose file systems: debugfs, tmpfs, sysfs, procfs, etc.
- Flash storage file systems: YAFFS, JFFS2, ubifs, etc.
- Conventional disk file systems: NTFS, JFS, Btrfs, XFS, ext4, ext3, ext2, etc.

### **The hierarchy standard of the file system**

The file system hierarchy is a standard layout used to store files for the Linux system. Here are some directory structures for the most common Linux:

### **The online manual page for Linux**

There is a help or support for every single command for Linux, and this is

one of the key features of Linux. You will have to type the following command for the manual page of the Linux to be accessed:

```
[handy32@localhost~]$man /s
```

The command page of the manual will be provided when you do this.

### **Root or superuser**

For anyone to do any alteration to a service or program of Linux with access to all kinds of permission, this account is a special kind of user account. To become root or superuser, you will use the `su` command and to become one, all you have to do is to enter the root password by typing the following command:

```
[handy32@localhost~]$su
```

### **Directories and files handling**

Everything is a file inside Linux. As such, through file operation related commands, there's an interaction with them during the time of dealing with device files or standard text files. Below are a few operations on the files:

#### **File creation:**

For the creation of a file, two commands are quite necessary, and they are `cat` and `touch`. To create an empty file, you can make use of the `touch` by following the example below:

```
[handy32@localhost~]$touch file1
```

To view or create a file, you will use the `cat` which you do by following this step:

```
[handy32@localhost~]$cat>file1
```

Also, you can use the command below to view a file type:

```
[handy32@localhost~]$cat file1
```

### **Copying a file:**

For you to copy a file from one location to another, you can use the `cp` command like this:

```
[handy32@localhost~]$cp file1 /home/sandra/Documents/
```

The current working directory will be copied by this command to `/home/bhargab/Documents/`.

### **Removing a file:**

You can type the command below to remove a file:

```
[handy32@localhost~]$rm file1
```

### **Moving or renaming a file:**

To rename or move a file; the command you can use is the `mv`. Use below command to move a file from one place to another:

```
[handy32@localhost~]$mv file1 /home/sandra/Document
```

Under `/home/sandra/`, the Document directory will get the file1 with the use of the above command. Then, from file1 to file2, you can perform the below command to rename a file.

```
[handy32@localhost~]$mv file1 file2
```

### **Directories and files listing:**

The contents are the `ls` lists, which are directories and files of the specified directory or current directory. For the contents of the current directory to be displayed, use the below command:

```
[handy32@localhost~]$ls
```

The directory name, as well as the file name, will be listed by this command. You can use the command below to list all files in the hidden files and also your home directory:

```
[handy32@localhost~]$ls □a
```

With the `/l` option, type `ls` to view files in a long-listing format:

```
[handy32@localhost~]$ls □l
```

Below, you will see a portion of the output:

Total of 48

```
drwxr-xr-x. 2 handy32 handy32 4096 Jan 25 21:32 Desktop
drwxr-xr-x. 2 handy32 handy32 4096 Apr 24 16:33 Documents
drwxr-xr-x. 6 handy32 handy32 4096 Jan 20 23:55 Downloads
-rw-rw-r--. 1 handy32 handy32 1024 Apr 28 22:18 file1
-rw-rw-r--. 1 handy32 handy32 1024 Apr 28 22:01 file2
-rw-rw-r--. 1 handy32 handy32 1024 Apr 28 22:01 file3
drwxr-xr-x. 2 handy32 handy32 4096 Dec 20 08:48 Music
drwxr-xr-x. 2 handy32 handy32 4096 Dec 20 08:48 Pictures
drwxr-xr-x. 2 handy32 handy32 4096 Dec 20 08:48 Public
drwxr-xr-x. 2 handy32 handy32 4096 Dec 20 08:48 Videos
```

48 is the total number of disk blocks, as indicated by the total 48. In each of the lines, there are nine columns, and the following permission was represented by each column, including file name, time and date, bytes sizes, group name, and numbers of links. There are 10 subfields in the permission field, and the type of file is what the first field represents. The (u) permission denotes the next three fields, while the representations of the group (g) permissions are the seventh, sixth, and fifth fields. The (o) permissions have its representation in the last three fields with read permission from (r), execute permission from (x), and write permission from (w).

### **The soft and hard links**

In the hard disk, a connection between the actual data and a file name is a link, and these are soft and hard links. When you follow the command below, you can create a hard link:

```
[handy32@localhost~]$ln file1 file2
```

And by following the command below, create a soft link:

```
[handy32@localhost~]$ln □S file1 file3
```

## **Changing Mod:**

For every file in Linux, there are three types of connected permission, and they are (x) for execute, (w) for write, and (r) for read. Through the superuser or the owner of the file, it is easy to change the existing file permission. To embed a *write* permission to the group, use the command below:

```
[handy32@localhost~]$chmod g+w filel
```

Also, use the following command for other users to have an execute permission:

```
[handy32@localhost~]$chmod o+x filel
```

You may use the following the command below when you want to take away execute permission from a group:

```
[handy32@localhost~]$chmod g-x filel
```

## **Current working directory**

Below, you will see the display of the current working directory through the *pwd* command:

```
[sandrahandy32@localhost~]$pwd  
/home/sandra
```

As such, the */home/sandra/* is the current working directory.

## **Directory creation:**

For the creation of a directory, you can use the *mkdir* command like this:

```
[sandrahandy32@localhost~]$mkdir myDir
```

Under */home/sandra/*, a directory will be created.

## **Directory removal:**

For an empty directory to be removed, you will use the *rmdir* command like

this:

```
[sandrahandy32@localhost~]$rmdir MyDir
```

You will also remove the parent directories and not only the specified directory with the *p* option using *rmdir* .

```
[handy32@localhost~]$rmdir -p myDir.
```

So far, we have covered extensively so many angles on the system administration and also Linux user management. You may want to go back and read through them for some time to get abreast of some of the things discussed in this segment. When you do, you can get over to the next section, where we will go in-depth on Linux directory structures.



# Chapter 6: Linux Directory Structures

There are needs for data storage on an HDD, hard disk of several types, or a few similarities, including a USB for every general-purpose computer. These needs come with a couple of reasons. In the first place, anytime you switch off your computer, the contents of the RAM can be lost. And as for the use of solid-state drives and USB memory sticks, after the removal of power, the maintenance of the stored data in them tends to be the function of non-volatile RAM types. Quite expensive is the flash RAM than other related categories like the volatile, standard RAM such as DDR3. The disk space is not as expensive as the standard RAM because the data storage by hard drives tends to be the second reason. Regarding per byte cost, RAM is still more useful. There's been a rapid drop in the value of both disk and RAM. As per unit, the hard drive is about 71 times less expensive the RAM, based on a 2TB hard drive costs against 16GB of RAM as a quick calculation of the cost per byte.

In a few confusing and different ways, there are a lot of discussions from several quarters about filesystems. With regards to the perspective of a document or analysis, you will need to distinguish the exact meaning since the word itself can have multiple meanings. For using it in distinctive conditions and based on people's observations, let's attempt to define several meanings of the term 'filesystem.' The intention is to make this definition grounded on its several handlings as we strive to adapt to the conventional official meanings.

1. With a specific kind of filesystem, a formatted logical or partition volume that, on a Linux filesystem, can be mounted on a specified point.
2. A particular formatted data storage like XFS, BTRFS, EXT4, EXT#, EXT2, etc. 100 filesystems types have support on Linux, including the newest in addition to the oldest. And to define accessing and storing the data, these filesystem varieties function by its metadata structures.

3. The start of the entire Linux directory structure is at the top (/) root directory.

## Basic functions of the filesystem

There are specific inescapable and exciting details that the disk storage encompasses with it as a necessity. Essentially, the provision of non-volatile data storage is one of the ultimate functions and purposes of a filesystem. However, from that requirement, there are some other essential functions. The provision of a namespace is what the whole filesystems have to execute; a methodology of organizational and naming. And out of the entire set of characters available, this process defines the manner with which you can brand a file, particularly the subset of characters and the length of a filename that you can use in place of filenames. Also, atop a disk, the data's logical structure is what it defines, including limping files in a vast, single conglomeration as well as for organizing files with the directories usage. For the provision of that namespace's rational base, quite necessary is the structure of metadata when the namespace has been defined. As such, for the support of a classified directory structure, there is an obligatory addition of data structures. These structures make the determination of the used space blocks upon the disk as well as those available. As for the maintenance of the directories' names and files, the structures that allow that and also the statistics about the data position or locations which, on the disk, belong to the folder, last accessed or modified, as well as times and sizes they were created. For the storing of the sophisticated material of the disk's subdivisions, they make use of other metadata, including logical partitions and volumes. It represents the structures and more complex metadata, which, separated and independent of the filesystem metadata, confine the data expressing the filesystem accumulated on the partition or drive.

Also, for the provision of access to the function of the system calls that control filesystem objects such as directories and files, API, Application Programming Interface is also required for filesystems. The tasks of deleting, moving, and creating files are provided by the APIs. Including the location on a filesystem that you place a file, part of the things APIs offer is algorithms that determine things. For minimizing and speeding the disk fragmentation, objectives may be the purpose of such algorithms. As a pattern for rights of entry definition to directories and files, there is also a

security model in the place provided by modern filesystems. As a user, you can have a way into other people's files or the OS as a result of the Linux filesystem security model. For the implementation of these purposes, the required software is the ultimate building block. And as a technique to enhance programmer efficiency and both system, the application of two-part software is what Linux uses. The virtual filesystem of Linux is this implementation's first part of the two. For the access to the filesystems of all types and also the provision of a single command set for the developers and the kernel is done by this virtual filesystem. And the driver of the specific required device to interface gets a call from the virtual filesystem software to the several kinds of filesystems. The second section of the execution is the drivers of the filesystem-exclusive appliance. On the logical or partition volume and to those explicit to the types of the filesystem, the filesystem commands' standard set is interpreted by the device driver.

## Directory Structure of Linux

The file system structure of Linux can appear particularly alien if you are the type that is coming from Windows. Now mostly with three-letter names, the cryptic-sounding directories and `a/` option have replaced the forgotten drive letters as well as the `C:\` drive. What defines some other Unix-related OS and the structure of file systems on Linux is the FHS, Filesystem Hierarchy Standard. However, also contained in the Linux filesystems are some directories that are not yet defined by the standard.

### **/var – Variable Data Files**

As it must be read-only in the usual operation, the writable counterpart to the `/usr` directory is the `/var` directory. During normal operation, we can write to the `/var` directory the log files as well as all things else that would normally be written to `/usr`. For example, in `/var/log`, the log file can be found there.

### **/usr – Read-Only Data & User Binaries**

Contrary to files and applications that the system uses, users use files and applications that contain the directory `/usr`. For example, rather than the directory `/sbin`, the location of the non-elemental binaries of the system administration, the location of non-essential applications is within the directory `/usr/bin`. There are other directories contained in the `/usr` directory, including architecture-free folder such as `graphics` which share location in `/usr/`. This process prevents them from mucking up the rest of the system,

where the local directory `usr/` is, by default, found installed in the locally assembled applications.

### **/tmp – Temporary Files**

Whenever your system is restarted, since it is in the `/tmp` directory where application stored temporary files, the utilities like `tmpwatch` will have these files deleted at any time.

### **/srv – Service data**

The ‘data for services provided by the system’ is contained by the `/srv` directory. You would probably store the files of your website in a directory inside the `/srv` directory if you were using the Apache HTTP server to serve a website.

### **/selinux SELinux Virtual File System**

With SELinux, the directory `/selinux` contains special files if, for security purposes, Red Hat and Fedora use SELinux by your Linux distribution. It is the same as the `/proc`. On Ubuntu, this folder’s presence appears to be a bug since Ubuntu doesn’t use SELinux.

### **/sbin – System Administration Binaries**

The directory `/bin` is parallel to the directory `/sbin`. And for system administration, it is generally intended to be run by the root user as it contains essential binaries.

### **/run – State Files Application**

For the requirement, such as process IDs and sockets, to store transient place, the directory `/run` gives a standard place application as it is fairly new. Since files in `/tmp` may be deleted, `/tmp` can’t store these files.

### **/root – Home Directory for Root**

The home directory for the root operator is the directory `/root`. As the system root directory, its location is at `/root` instead of `/home/root` for the location.

### **/proc – Kernel & Process Files**

Since it doesn’t contain standard files, the directory `/dev` is the same as the `/proc` directory. Special files to process and represent information are all that it contains.

### **/opt – Optional Packages**

For optional software packages, these directories are contained in the directory /opt. Since the standard filesystem hierarchy doesn't have its respect, the proprietary software commonly uses it. For instance, as you install it, it might dump the files of proprietary programs in /opt/application.

### **/mnt – Transitory Mount Points**

While using them, where the temporary filesystems are mounted by the system administrator is the directory /mnt. For example, for the execution of a few operations of file recovery, you may well want to mount a partition on windows /mnt/ for Windows if you are mounting it. However, to mount other system files, you may choose any space on the system.

### **/media – Removable Media**

Where the devices inserted into the computer are mounted is where subdirectories contain the /media directory. For instance, a directory will automatically be created inside the /media directory as you insert a CD into your Linux system. And inside this directory, you can access the contents of the CD.

### **/lost+found – Recovered Files**

There is a `lost+found` directory in each filesystem of Linux. As such, a filesystem check will be performed at the next boot if the filesystem crashes. And for the extensive recovery of data, it is in the `lost+found` directory will any corrupted files found be placed.

### **/lib – Essential Shared Libraries**

In the /sbin and /bin directories, required essential binaries are contained libraries in the /lib directory. Binaries needed by libraries within a /usr/bin folder are located within /usr/lib.

### **/home – Home Files**

For each user, the directory /home contains a file for home. For example, /home/greg will be the location for the home folder if your username is Greg. User-explicit formation file and user's data files are contained in this home folder. On the system, for you to have other files modified as the superuser, each user needs to obtain elevated permission even when they only have the write access to their home folder.

### **/etc. – Configuration Files**

Though easily edited by hand in a text editor, the maintenance of the

configuration files is contained by the /etc. directory. Be aware that the system-wide configuration files are contained by the /etc/ directory, and it is in each home directory of the user that user-specific configuration files are located.

### **/dev – Devices Files**

As files, devices are exposed by Linux. As such, devices that have the representation of some special files are the directory /dev. Though they seem like files, much known to us, we can't call them original files. For instance, in the system, the major SATA drive is represented by the /dev/sda. For you to inform it to edit /dev/sda, you could begin a compartment editor if you want to partition it as virtual devices without any hardware correlation. Also, pseudo-devices are contained in this directory. For example, there are only random numbers that the /dev/random produces. As it creates no output, an exceptional device is /dev/null that instinctively have all inputs discarded when, toward /dev/ null, a command's output is piped.

### **/cdrom – CD-ROMs Historical Mount Point**

A directory that doesn't belong to the standard of FHS is the directory /cdrom. However, when you go to Ubuntu and other OS, you will find it. For CD-ROMs inserted in the system, it is a temporary location. However, it is inside the /media directory for the standard location of temporary media.

### **/boot – Static Boot Files**

The files needed to boot the system is contained by the /boot directory. For example, stored here are your Linux kernels and the GRUB boot loader's files. Though their location with other files is in the /etc directory, the configuration files of the boot loader are not located here.

### **/bin – Essential User Binaries**

When the system is mounted in a single-user mode, the essential user binaries, otherwise known as programs that must be present, are contained within the /bin directory. It is in /usr/bin that applications like Firefox is stored, while the location for vital utilities and system programs like bash shell are in /bin directory. You can also store in another partition the /usr directory. Though, even if no other filesystems are mounted, you will be sure to have these essential utilities when you place these files in the /bin directory. As it contains crucial binaries for system administration, similar to

it is the /sbin directory.

### **/ - the Root Directory**

Known as the root directory, it is under the / directory that you can locate everything on the Linux system. On Windows, the C:\ directory is quite similar to / directory. However, since Linux doesn't have drive letters, this is not strictly true. On Windows, while D:\ is the location for another partition, on Linux, it is in another folder under / directory that other partition would appear.

## Chapter 7: Working with Disk, Media, and Data Files (gzip – tar)

Before you can use them, you must structure storage devices like USB drives and hard drives since the regular practice in Linux is deleting and creating partitions. *Partitions* often host separate sections of devices with considerable storage after they have been divided. Also, you can divide into isolated parts of the hard drive using the partitions where, as a discrete hard drive, each section behaves as such. If you administer several OS, partitioning can be particularly useful. In Linux, otherwise known as disk partition manipulation, you can remove or create this with the use of several powerful tools. As such, devices with large disk can benefit as well as several disk partitions, and we will go in-depth on how to use the `parted` command. Here are some common commands like `cfdisk` and `fdisk`, as well as the difference between `parted`.

- **Reliability:** in a DOS partition, only one copy of the partition table is stored. At the end and the beginning of the disk, two copies of the partition table are kept by the GPT. Also, done with DOS partitions to check the partition table integrity, the GPT uses a CRC checksum.
- **More partitions:** it is only 16 partitions that the tables of DOS partition permit with the use of extended and primary partitions. Having many more is what you can choose and by default, can get up to 128 partitions with GPT.
- **Larger disks:** in some cases, up to 16TB is possible even though a partition of the DOS table tends to format up to 2TB of disk space. However, up to 8ZiB of space can be addressed by a GPT partition table.
- **GPT format:** while, to DOS partition tables, `cfdisk` and `fdisk` are limited, a Globally Unique Identifiers Partition Table, GPT can be created by the `parted` command.

It is recommended to use `parted` to function with disk partitions because working with them will require more flexibility in today's larger disks. Most often, part of the operating system installation process is the creation of the



disk partition. When an existing system is getting an addition of a storage device, direct use of the `parted` command is most useful.

## Analyze Disk Space and Hard Disk Partition on Linux with These Commands

For you to check the partitions on your systems, there are some commands you can use. Part of what the commands might do is checking what partitions exist on every floppy disk and some additional details such as filesystem, consumed space, total size, so many others. Though they can also modify them, there are some tools for partitioning where the partition material can be displayed, including `cfdisk`, `sfdisk`, and `fdisk`.

### **hwinfo**

You can make use of `hwinfo` to print out the partition and disk list, as a general-purpose hardware information tool. However, like the other commands, the output doesn't print details about each partition.

### **blkid**

Though it doesn't report the space on the partitions, `blkid` prints the block devices, storage and partitions media, attributes such as `uuid` and file system type.

### **lsblk**

Optical drives and disk partitions, as well as all the storage blocks, are listed out by `lsblk`. If any, it lists out the mount point and, most notably, the total size of the block/partition. On the partitions, free/used space is not reported. It indicates that the filesystem is not yet mounted if there is no MOUNTPOINT. Also, it means that there is no disk for DVD/CD. With a device such as the model and label, `lsblk` is capable of displaying more information.

### **pydf**

Written in Python is the improved version of `pydf`, and in an easy to read manner, it prints out all the hard disk partitions. Also, it is only the mounted file systems that `pydf` is limited to show.

### **df**

This command prints out details about only mounted filesystems even though

it is not a partitioning utility. Even filesystems that are not real disk partitions are some of the list generated by `df`. When you use it, you will discover that the actual partitions or devices are only the file systems that start with a `/dev`, and to filter out the real hard disk partitions or filesystems, you can use `grep`. Then, use `df` to display only actual disk partitions with the type of partition.

### **parted**

If needed, this modifies the list as it also lists out the partitions being another command-line utility.

### **cfdisk**

Based on `ncurses` with an interactive user interface, the partition editor of Linux is `cfdisk`. Use it to modify or create current partitions in addition to listing out those partitions. One partition can only run at a time with `cfdisk`, and as such, pass the device name to `cfdisk` if the details of a specific disk are required.

### **sfdisk**

In addition to a goal similar to `fdisk`, however, with additional features, another utility is `sfdisk`. Each partition's size can be displayed in MB.

### **fdisk**

For the checking of the partition on a disk, the most commonly used command is the `fdisk`. Like filesystem type, you can get the display of the partitions and details with the use of the `fdisk` command. However, each partition size report may not be available with `fdisk`.

## Linux Data Manipulation

It can be confusing with the Linux world if you are the type that is quite used to Windows. What with no image, link, or anything to click, few hints, no wizards, and so on. And also, before anything can be done, you need to know what it is you want. Let's assume that, somehow contrary to your interest, you have no choice but to use the shell prompt of Linux and learning the agonizing, cryptic program where the `xkcd` forms its basis does not tally with your burning desire. However, for the processing of your data, the use of the command-line might have in it some good reasons. Attempting to make use of Excel to deal with this data may not be suitable even with the new

technologies offering digital data terabytes and more instruments providing a digital output. You may not also get anywhere near luck with the use of CSV files. However, with the use of free, reasonably simple utilities on Linux, these can be easily managed. Also, another reason for taking this path is that the powerful mainstream tools for Linux come with no cost.

Though we may want to leave out most of these, however, SAS, Mathematica, MATLAB, and so on have been ported to Linux and are a few excellent branded tools. As it works better on Linux and as second nature on Linux, we may not imply that using native applications and utilities may not do well on Windows. Also, there is a constant assurance that on Linux, it will work always. Since there's a payment option for Apple and Microsoft in money and time by releasing yet another pointless upgrade to bump their profit, you don't need to learn a new interface every 6 months.

### **Identifying the file type**

It is possible you are not aware of the kind of data it is even though the data might have been generated in the lab. The file is a device that can proffer some help even though it is not foolproof. The response it tends to give comes from the question: "what file type is it?" If there are any diagnostic characteristics, file peeks inside the file to see them, unlike the endings of the file name mapping approach of Windows, which has filename.typ to a specific type. And it can be quite helpful suppose there's been name-mangled or renamed in translation to the file.

### **Hypotheses**

With the installation of Linux standard famous utilities, including *R*, the hypothesis is that on a Linux, you have access to a bash shell. For this exercise, a directory can be created. For DataDir, it is quite on *\$DDIR* that you can give it your reference, though you can give it any name you like. And to the DDIR variable of the shell, you may as well have actual term assigned to it:

```
Export DDIR=/stephen/leo/
```

bash> is the prefix of the shell commands and to test your shell, including comments with embed (with # as a prefix; you may as well ignore them) can

mouse into it. Also, you may want to ignore the prefix `bash>` . Also, at the UC Irvine and on the cluster nodes of the interactive BDUC, accessible here are all the defined utilities. And for any Linux distribution, you can get them without any costs, except they state otherwise.

### **The size of the file**

`red+blue all.txt.gz` , a tab-bordered data file of 25MB is what we are going to use. By pressing upon the link with a right-clicking, you can download it in Firefox and hit 'save.' For this exercise, use the directory `$DDIR` to save it. Then, use `gunzip blue+red_all.txt.gz` to decompress it. After that, with `ls` , the result of the entire bytes will be achieved.

### **Using Linux to Mount and Unmount Media**

With the use of the operating system of a Linux, you can have media mounted and unmounted with this process. You must be aware that the default Red Hat installation is what this process uses, and thus, with the use of other Linux operating system types, the commands, structures, and file names might not be the same. Now, let's get down to the business!

If you are mounting a CD, follow the steps below:

1. Ensure that, on your server, there is a presence of the `/mnt/cdrom` directory. You can type `mkdir/mnt/cdrom` if there's no existence of this directory. Then, hit the 'enter' button.
2. Then, have `mount/dev/scd0 -t iso9660 -o ro /mnt/cdrom` typed for you to mount the CD. Again, hit the 'enter' button.

If the disk is the instrument you want to mount, you can follow the below command:

1. Be certain that on the server, you have `/mnt/floppy` directory. You may want to type the below command if there's no existence of this directory:

`mkdir/mnt/disk`

Again, hit the 'enter' button.

2. You can type the following command to have the disk mounted:

*mount/dev/sda -o auto/mnt/disk*

Then, hit the 'enter' button.

For you to unmount the media, you can follow the command below:

1. Input CD and hit enter.
2. Follow the commands below:
  - You can type the command below if it is your CD that you want to unmount:

*unmounts /mnt/cdrom*

Then, hit the 'enter' button.

- You can type the command below if it is a disk that you want to unmounts:

*unmounts mnt/floppy*

Again, hit the 'enter' button.

## Creating from the Command-line a File for Tar GZip

If you are managing your backups away from Time Machine or you want to have file groups transferred, having the zip files made could have been something you are probably doing. The command line can be an excellent option for you to make a gzip and tar archive if you prefer better compression and also additional advanced options using the user-friendly and accessible tools of GUI zip. And typical of Linux elements, even in Mac OS X, the syntax will be similar.

### **Bundle creation the archive of tar gzip**

You can make use of the syntax from the (terminal/applications/) command-line. For example, you could have jpg files directories compressed by typing some specific commands.

Here, a wildcard is the \*, which means that you can have .jpe compressed from any file that has the extension .jpg, and that is all. Though offering compression on its own, tar packages become a bundle of a single file from a

set of files as two distinctive products are the resulting `.tar.gz.` file. Therefore, gzip compression is quite valuable to supplement for you to have the tar compressed. And if you want it, you can have them as different commands while running them. However, as you can automatically have the tar file gzipped since the flag `-z` is what tar command offers, there is no much need for it.

# Chapter 8: File, Directory Manager, Permissions, Networking, and SSH

As a layer generally, the operating system that handles your data positioning on the storage is any filesystem on Linux. And even if you discover any unsupported filesystem type, you will not know which file starts where and what files end where without it. For software that can deal with it, you may even download it. As such, what are the Linux filesystem types? You will notice that Linux provides several filesystems such as the ones below when you attempt to install it: swap, btrfs, jfs, ext4, ext3, ext2, ext

Therefore, what are these filesystems that Linux provides?

## **Btrfs**

Oracle made this one, and in some distributions, it is not entirely stable as Ext. However, if you have to, you may think that it is a replacement for it, and it has excellent performance.

## **XFS**

Using it with small files, it works slowly being an old filesystem

## **JFS**

IBM made this old filesystem and, whether, with big or small files, it works quite well. However, after a long time, as indicated by reports, it failed, and files get corrupted.

## **Ext4**

With a significant speed, this gives room for large files. If you are looking for an option for SSD disk, you may want to go for this, and it is the suggested default filesystem you will see when you want to install Linux.

## **Ext3**

With backward compatibility and upgrades, it comes with Ext2. And since this filesystem doesn't give any support for disk snapshots or file recovery, servers no longer use this type of filesystem.

## **Ext2**

This gives room for 2 terabytes of data allowed as the Linux first filesystem.

## **Ext**

Because of limitations, people are no longer using this old one.

## **High-Level Explanation**

Now is the time to know from the high-level, what is inside those filesystems since you are familiar with the Linux filesystem. If you are someone coming from Windows, it will be possible to install partitions such as D:\ and C:\, usually C:\, because Windows has partitions like them. Though we have discussed it in some previous chapter, what is the filesystem structure of Linux? You will see the Linux filesystem hierarchy when you navigate to the root partition, which is /.

## **Linux Directory Management Commands**

For us to translate between IP addresses and domain names, the domain name system, DNS, is what we utilize. For example, on a Linux system, for DNS hookup, you may use the `host` command or `dig` command. Similarly, it is not by inode number but by file names that people refer to Linux files. As such, what is the directory's actual function? It is according to your usage that you tend to group the files. For example, you can do that under `/etc/` directory that all configuration files are stored. Thus, making a connection between the file names and their connected inode number is the purpose of a directory. And you will discover two sub-directories inside every directory named:

1. `..` (double period) – the pointer to the previous directory, i.e., the directory above the one you are in at present. Except for the root directory, it is in every directory that the “`..`” appears. And to the same inode as “`.`” that the “`..`” always points.
2. `.` (single period) – which means the current directory

For us to list directories and files, we can use the `ls` command, including on Linux `..` and `.` directories.

```
ls -la
```

## **Directory**

A sub-directory is contained inside another directory. A tree structure forms at the end of the directories and to see directory tree structure, use the `tree` command:



```
$ tree /etc | less
```

Typical of a file, a directory has an inode. As it connects each name with an inode number, it is a specially formatted file containing records. Under ext2/3 filesystem, it is quite vital to take note of the following limitation of directories:

- There is a chance for an unlimited number of subdirectories in Ext4 and other modern Linux filesystems
- In a single directory, there is a soft upper limit of about 10-15k files
- In a single directory, there is an upper limit of 32768 subdirectories

However, without any issues, using a hashed directory index, which is under-development, allows 100k-1M+ files in a single directory, according to the official documentation of ext2/3 filesystems. And related to directory, below are some bash shell alias commands:

```
alias ..='cd..'
```

```
alias d='ls -l | grep -E "^d"'
```

## Linux directory management commands

For you to work with files and directories, here is a list of standard Linux commands:

Command	Description	Example(s)
diff command	Compares the content of any two files	<i>diff old.c new.c</i>
egrep command	Though, extended regular expression supported, it is the same as grep	<i>egrep -I 'err cri warn ' /var/log/messages</i>
grep command	In the specific files, it finds a specific search string	<i>grep "nameserver" /etc/resolv.conf</i>
more command	At a time, through text one screenful, it serves as a filter for paging.	<i>more /etc/hosts</i>

less command	The content of the specified file is seen by it.	<i>less resume.txt</i>
cat command	Displays the contents of a file	<i>cat data.txt</i>
file command	This detects the contents of the specified files.	<i>file /etc/resolv.conf</i>
find command	In a given directory, this searches for a file	<i>find \$HOME -name "hello.c"</i>
locate command	Finding in which directory of a specified file is located	<i>locate file!</i>
chmod command	Changes the access permissions	<i>chmod 0444 dir1</i>
chgrp command	With the specified group name, this command transfers the group ownership of a given file to the group.	<i>chgrp dir1</i>
chown command	With the specified username, it transfers ownership of a file.	<i>chown username file</i>
ln command	From source to target, it creates an internal link	<i>ln -s /etc/hosts/tmp/link</i>
rm command	From the filesystem, this command removes the specified files, and unless the option <i>-r</i> is used, <i>rm</i> doesn't remove directories	<i>rm files!</i> <i>rm -r dir1</i>
cp command	Copies source to the target	<i>cp -r dir1 /path/to/dir2</i>
mv command	Deleting the source after copying to the target	<i>mv dir1 dir2</i>
cd command	cd changes to the home directory of the user without any parameters	<i>cd</i>
pwd command	This command displays the name of the working or current directory.	<i>pwd</i>
cd .. command	Go back to the previous directory.	<i>cd ..</i>
cd command	Change the current directory	<i>cd /etc/</i>
rmdir command	If it is already empty, this deletes the specified directory.	<i>rmdir dir1</i>
mkdir command	A new directory is created through this command.	<i>mkdir dir1</i>

## Managing Directories

Since, from Nautilus, you can copy, move, delete, or create them, you must learn to treat your directories like files and related to files directories with the use of commands from a shell prompt.

### Creating directories

For you to have a fresh sub-directory conceived, you must learn to write permission. It is at the /temp/ directory and the home directory, as well as the subdirectories that most users have these permissions. You will have to navigate to your new directory for you to use Nautilus in creating an original directory. In the window's blank portion, right-click and then choose to create a folder. Then, using the untitled folder with the highlighted text, a new folder icon will appear. Before you hit the 'enter' button, remember to give this new folder a name. When you attempt to use a shell prompt to have an original directory conceived, the `mkdir` command is all you need to use. You can replace the `<directory-name>` by simply type in: `mkdir <directory-name>` with the new directory's intended title.

### Deleting directories

It is on the Desktop that you click and then **Trash** the icon or move it to the Trash after right-clicking on it to delete a directory from Nautilus. You will need to enter the `rmdir` command to delete a directory that is empty from the prompt of the shell. It is the `rm -rf <directory>` command that you will need for you to delete an unlikely empty directory and also all the things within such directory.

### Dot directories

Dotfiles are also part of the applications created by "dot" directories. Also, other files required by the application, a hidden directory of configuration, is a directory for dot, and these files are a single hidden configuration file. Generally, these directories are user-specific non-configuration files, and their accessibility is to the user that has them installed.

## Linux File Permissions

Since several users can have access simultaneously, and as a multi-user operating system, Linux is a clone of UNIX. Also, without any modifications, anyone can use Linux in servers and mainframes. However, because vital

data can be removed, changed, or corrupted by malign or unsolicited individuals, this situation raises security concerns. As such, there are two levels of authorizations divided by Linux for adequate security, and they are:

1. Permission
2. Ownership

In Linux, a critical concept is ownership and permissions. We will begin the discussion with the Ownership as both of them will be examined.

### **Linux file ownership**

There are 3 types of owners assigned for every directory and file on your Linux system.

#### **Group:**

There are multiple users contained in a user-group. Also, similar access permissions to the files will be given to all users belonging to a group. Several individuals will require access to a file if you have a project. You can go ahead and add all users to a group instead of manually assigning permissions to each user. Then, no one else can modify or read the files when you assign group permission to file.

#### **User:**

The owner of the file is a user, and you will be the owner if, by default, you are the one who creates a file. Thus, as an owner, you can also be called a user.

#### **Other:**

This case points to having access to a file by any other users. This type of user does not belong to a user group that owns the file or created the file. Mostly, this can be anyone else. Therefore, it is also referred to as setting permissions for the world when you set permission for others.

Ultimately, the question of distinction arises. How can you go about separating these three user types without exposing vital information from one group to another group? It is typical of hiding your image from your computer from your colleague who works on your Linux computer. Now, this is the case of permissions, and it is through user behavior that you can define it. For you to have a full grasp of the permission system on Linux, we may

have to discuss more on it.

## Permissions

For all the 3 owners discussed above, the 3 permissions below define every directory and file in your Linux system.

- **Execute:** as you can effectively run it, you have an extension “.exe” as an executable program in Windows. However, you won’t be able to run an application unless the execute permission is set in Linux. And provided you set permission for write and read, though you can’t run it, you might still be able to modify or see the program code.
- **Write:** you will have the influence of editing the contents of a file through the write permission. Also, in the directory, you can rename, remove, and add files as part of the authority you get from the write permission. You can assume where the file is stored, having no permission on the directory, and you have to write permission on file. The file contents can be modified by you. However, removing, moving, or renaming the file from the directory will not be possible for you.
- **Read:** you can read and open a file through the authority given to you by this permission. Also, you can list the content of a directory since you have the read permission.

## SSH Command

Mainly, `ssh` command is included in every Linux system. The SSH client gets started through this command and on a remote machine, enables a secure connection to the SSH server. From a remote machine to logging, the `ssh` command is used for executing commands on the remote device and transferring files between the two computers.

### SSH command in Linux

Over an insecure network and between two hosts, the provision of a secure encrypted connection is made by the `ssh` command. Also, for tunneling other applications, it can be used for file transfer and terminal access. From a remote location, you can securely run Graphical X11 applications over SSH.

## **Other SSH commands**

With each of them having its page, besides the client `ssh`, there are other SSH commands.

- `sshd` – OpenSSH server
- `sftp` – file transfer with FTP-related command interface
- `scp` – file transfer with RCP-related command interface
- `ssh-add` – a tool to add a key to the agent
- `ssh-agent` – agent to hold private key for single sign-on
- `ssh-copy-id` – configures a public key as authorized on a server
- `ssh-keygen` – creates a key pair for public-key authentication

# Chapter 9: Linux Terminals, Editors, and Shell

You can find help to get started with the terminal, whether it's been a while you have been using Linux or you are a new user of Linux. Without doubts, a terminal is a powerful tool with lots of values, and it is not something that can scare you. It is not really by reading a single book or article that you will be able to learn everything you need to know about the terminal. Firsthand, to play with the terminal takes experience.

## **Basic usage of terminal**

You will see the bash shell on the application menu of your desktop when you launch a terminal. And by default, bash is what most Linux distributions use even though there are other shells. At the prompt, by typing its name, you can launch a program. Then, it is all a program from command-line utilities to graphical applications such as Firefox concerning everything you launch here. Though those functions are typical of programs, for essential file management, bash has a few built-in commands. And to launch it, you may not need to have the entire path typed to a program, unlike on Windows. For example, you will have to type the whole path to Firefox's .exe file when, on Windows, you attempt to open Firefox. You can type the command below on Linux:

*firefox*

To run it, after typing a command, go ahead and hit 'enter.' On Linux, programs don't have file extensions, and there's no need to add a .exe or anything else. Also, accepting arguments is part of terminal commands. You can utilize specific types of arguments concerning the program. For example, as arguments, web addresses are accepted by Firefox.

## **Installing software**

Installing software from the terminal is one of the most efficient things to do. The fancy frontend of some terminal commands that they use in the background, such as the Ubuntu Software Center, is the software management applications. Then, you can install them with a terminal background instead of doing it one after the other by selecting and clicking around applications. Also, you can have several apps installed with a distinct

command. Since you can see the package management systems by other distributions, you can follow the following command when you intend to install a new software package on Ubuntu:

*sudo apt-get install packagegename*

Though it works similar to the Firefox command above, it may appear a bit complicated. With root (administrator) privileges, before launching `apt-get`, `sudo`, you can have the above line launched. Installing a package named `packagegename` is what `packagegename` will install by reading the argument `apt-get` program. However, it is as arguments that you can also specify multiple packages. For example, you could execute the command below to install Pidgin instant messenger and the Chromium web browser:

*sudo apt-get install chromium-browser pidgin*

Also, you could do it with a single command like the above if you want to install all your favorite software after installing Ubuntu. Since you can guess them reasonably quickly, the package names of your preferred programs are all you would need to know. Also, with the help of the tab completion trick, your guesses can be refined.

## **Text Editors for Linux Desktop**

It makes it quite useful for some text editors to also double up as an IDE. Also, they are the default editors. In the Linux environment and for the Linux desktop environment in developing an application, these are quite helpful. The focus will be on a few text editors even though out there, there are a lot of text editors. As such, let's jump right into them:

### **GNU Emacs**

For the Linux environment, one of the oldest text editors is GNU Emacs that has been here for quite some time. GNU's project founder, Richard Stallman, was the one who developed it. All around the world, for thousands of Linux programmers boast of it as their preferred and favorite text editors by using it. With the use of C and LISP, they were able to develop it. To install emacs on Linux Mint or Ubuntu, you can use the commands below:

```
linuxtechi@linuxtechi:~/Downloads$ sudo apt-get update
```



```
linuxtechi@linuxtechi:~/Downloads$ sudo apt-get install emacs
```

There are some included unique features of GNU Emacs, which are:

- Extensive support and documentation
- Debugger interface extension
- News and mail options

For Linux Desktop, Atom and *notepadqq* can also be IDE and Text Editors, apart from these text editors.

### **Nano**

In the UNIX operating system, another popular text editor used is Nano. In 2000, it was released, and it is the same as the Pico text editor. Also, to make it as an advanced and powerful text editor, it comes packed with some additional functionality. And it is in the interface only that it can run in a command-line. Here are a few unique features of Nano:

- Autoconf support
- Tab completion
- Auto Indentation
- Case sensitive search

### **Kwrite**

It was in 2000 that Kwrite was first released to the public, and KDE developed this text editor. From KDE, along with the KParts technology, it is entirely based on the text editor for Kate. Making it a more powerful development environment, to a large extent, you can extend the Kwrite's functionality with the help of additional plugin installation. Also, along with encoding your file, it can be used to edit a remote file. On Linux Mint or Ubuntu, to install kwrite, use the command below:

```
linuxtechi@linuxtechi:~/Downloads$ sudo apt-get install kwrite
```

A few unique features of Kwrite are:

- vi input mode
- Syntax highlighting
- Auto indentation
- Word completion

## **Eclipse**

Eclipse editor can be a suitable option as an advanced and robust editor of code/text for frontend designers and developers. Since it contains several features that support developing and writing Java applications easily, it is entirely in JAVA that it was developed. Also, it is popular among Java developers. For anyone to accomplish extra language support, there may be a requirement for additional plugins if they need it. As the editor can have several advanced functionalities when you insert them with the help of additional plugins, the Eclipse IDE becomes even more powerful. And for the development of programs for COBOL, Ruby on Rails, C++, C, Python, and PHP, you can as well use it. For you to have eclipse installed on Linux Mint or Ubuntu, use the command below:

```
linuxtechi@linuxtechi:~$ sudo apt update
```

```
linuxtechi@linuxtechi:~$ sudo apt install eclipse
```

A few of Eclipse's unique features are:

- Plugin support
- For Java developer, tools for Java Development are included
- Open-source and free text editor

## **Kate**

Loaded with the Kubuntu environment, as a default editor, you may have to know about the text editor of Kate if you are familiar with the Kubuntu

desktop environment. Given that you can exploit it as a powerful IDE, you also have the opportunity of working with multiple files simultaneously since it is easy to use text editor, it is also a lightweight. Use the command below to install Kate on Linux Mint or Ubuntu:

```
linuxtechi@linuxtechi:~$ sudo apt-get install kate
```

Kate has some exceptional features, and they are:

- Sets indentation for documents automatically
- Auto-detects languages
- Supports several languages
- A powerful IDE

## **Gedit**

Gedit comes loaded by default as a text editor in a GNOME desktop environment. Gedit follows similar objectives as it comes with a simple and clean user interface, and it is lightweight, just as the objective of GNOME to always offer functionalities that are straightforward and clean. With the GNOME desktop environment, getting access to it by the public didn't happen until 2000. It supports entirely for internationalized text as it is completely developed using C language. Gedit possess a few unique features, and they are:

- Supports several programming languages
- Supports internationalized text
- Syntax highlighting

## **Brackets**

For the Linux environment, in 2014, the Brackets was launched by Adobe as a text editor. It has exciting packed features that make working with this editor a lot of fun as an open-sourced text editor. With a clean interface, it is also simple and easy to use. For programmers and web designers to get much-needed help, it is designed as a code editor and also as a text editor.

They used JavaScript, CSS, and HTML to develop it completely. With its sophisticated qualities, a few quality text editors may not qualify for all the features it has even as it is on the lightweight side. For the installation on Linux Mint or Ubuntu, you can use the command below:

```
linuxtechi@linuxtechi:~$ sudo add-apt-repository ppa:webupd8team/brackets
```

```
linuxtechi@linuxtechi:~$ sudo apt-get update
```

```
linuxtechi@linuxtechi:~$ sudo apt-get install brackets
```

Brackets text editor has a few unique features, which are:

- Focused visual tools Pre-processor support
- Inline editing
- Live preview

### **Sublime text editor**

For the Linux environment, a text editor with so much esteem is a sublime text editor. You can use it as a development environment as well as a text editor; it is packed with several features. Along with various markup languages, it supports a lot of programming. Also, by extending its functionality to a great extent, the many available plugins have made the text editor more sophisticated. You can navigate to any file in your system or easily navigate to the code section through the help of the “Goto Anything” feature, and this is one of the distinctive highlights of this text editor. On Linux Mint or Ubuntu, to install the stable version of the sublime text editor, all you have to do is to refer to some specific commands. A few of the sublime text editor’s exclusive elements are:

- Project-specific preferences
- Parallel editing of code
- Python-based plugin API
- Excellent command palette

## **Geany**

For the Linux environment, one relatively recognized text editor that has the integration of the GTK+ toolkit is Geany. For developers and programmers, Geany can also work as an exceptional environment for development. Geany may be a suitable choice for you if you want a development environment and also a text editor. Other packages are not necessary to be installed with it for it to work quite well as it supports nearly all major programming languages and it is lightweight. For the installation of Geany on Linux Mint or Ubuntu, you only need to refer to a particular command. Geany has a few unique features, and they are:

- Interface that is easily pluggable
- Line numbering for easy tracking of code
- Lots of customized options
- Syntax highlighting for easy development
- Clean and easy to use interface

## **VIM**

Vim will be your best choice if you prefer a lot of options and powerful performance to edit your text in an advanced text editor since the default “vi” editor in Linux may appear to bore you. As it is the default Linux text editor’s advanced version, the meaning of vim is “vi improved,” as suggested by the name. They have the specific need of the developers in mind when they are designing it. Also, for its highly configurable options, it is called a programmer editor. You can use it as a standalone GUI application or as a command-line utility, which is the same as the Vi editor. Here are a few unique features of VIM:

- Automatic commands
- Digraph input
- Split screen
- Session screen
- Tab expansion

- Tag system
- Syntax coloring

### **Introduction to Linux Shell**

You are indirectly interacting with a shell if you are using any major operating system. And every time you use a terminal, you are interacting with a shell if you are running Linux Mint, Ubuntu, or any other Linux distribution. There are a few terminologies that are quite essential before we proceed, and we will discuss them in-depth in the following chapter.

# Chapter 10: Basic Linux Shell Commands

On Linux, the command used for analysis is the shell. In a window of terminal emulation, the program users interact with is the shell. On Linux, the workstation's `mate-terminal` GUI is the emulation window. Also, it is an application like `PuTTY` or secure shell client; `SSH` secure on a system with Windows that, around the network, you can register into Linux. In some business or organizational settings, they make use of the Bourne Again Shell, `bash`. If you prefer, you can choose from some of the available shells like the TC-Shell, C-Shell, as well as the Bourne Shell. As specific features are appropriate to each of them, they all boast of the same characteristics. The features below belong to `bash`:

- As it remembers the last few commands, the history mechanism of the shell is indeed functional. In addition to a reference number, to list the previous few commands, you can make use of the `history` command.

For you to rerun a command, you can cut and paste from the history in a terminal emulation window of a workstation. Also, to rerun any command from history, the symbol “`!`” can be used.

- There is also “job control” for the shell, and in the background, you can run any programs that don't require any terminal interaction.

Available straightaway for other commands is the shell and the program `sort` in the background. In this case, the job control number “1” is printed by the shell as well as “3470,” which is the process identity number. As it is running in the foreground, you can also use the special character `Ctrl + z` to suspend a program. You can then use `fg` to continue it in the foreground and even the `bg` command to put the program in the background. You can refer to them by their job number if there is more than one running program in the background or suspended. As such, use the `jobs` command to list the status of all stopped or background jobs to see your jobs and their job numbers.

- You can write the scripts of shell commands, and similar to the compiled programs, you can invoke them as such by merely naming them. For example, we can first create a file in `~/bin` containing the specific command to create a script that counts the number of C program files in this recent directory.

Before running it like normal, we can use the `chmod` command to make the file executable.

- With *if-then-else* statements, *for* loops, and *while* loops, bash is an interpretive programming language. When you type the command below, you will get more details about the Linux on-line documentation:
- The shell possesses numeric and string-valued variables.

The directory for home is `$HOME` as pre-set for some variables, and to see a list of assigned variables, type the `set` command.

- You can find it cumbersome to enter, or for the frequent execution of specific commands or groups of commands; you may want to assign *aliases*. For example, in a recent directory, to have the number of files of C program counted, we can assign an alias “countc” for the number counting of lines output using `wc` and have the files listed using `ls`.
- To *pipe* one program’s output to another program’s input, the shell boasts of such a facility. “|” is the symbol of the pipe. For example, in the `wc` program, we may have the output piped after we might have `cat` the file for us to count the number of words in file A.
- The *standard output* and *standard input* are the concept that most Linux programs and commands observe. An onslaught of output written by the program is the average output, and a flood of data read by the programs is the standard input. Most times, accompanying the terminal is most of these so that your screen can get this output while it is from your keyboard that you get the input. You can have the standard *redirected* to output and input through the shell.



- In your recent directory, to match filenames, the shell will expand the wildcards. For example, you can use a specific command to give a directory listing of the file with names “*anything.c*”
- Filenames are represented by the *argument* strings that the commands have. For example, in your home directory, the command can change the current directory to “*bin* , ” and the meaning of *tilde* is that the shell is your home directory.
- For it to identify it, the process entails verifying to discover the built-in element is connected to the command and may then explore for a collection of directories by typing in a command name. The *search path* is what this means and included in the current directory is the search path, its subdirectory “*bin*,” and your home directory. And through typing their names, you may invoke them after you must have written your programs. No matter what your current directory is, if in the directory, you deposit such a program, it will be found and then run.
- By naming them, you can invoke commands. Most Linux commands are just programs that the shell executes. For example, the command *ls* can list the names of its files and read the recent directory as you get a specific result when you run it.
- There is an associated current directory that, similar to other programs, the shell has. When locating files, as the starting point, programs running on Linux use the current directory. In the filesystem of Linux, getting a different location by changing the recent directory is possible by using the *cd* command of the shell.
- The user can configure this command prompt. A dollar symbol preceded by “*bash*,” as well as the version number of the bash program, is the default prompt.

With the use of the up-arrow keyboard, you can use previous commands of edit and recall with the help of an additional mechanism of bash. On top of the terminal, the final command will re-appear once you push the up-arrow, and to get the earlier commands, press the up-arrow once more. Hit on

“RETURN” to have the command replayed. You can insert characters within the command or to delete by repositioning the cursor with the use of the key for back-arrow or from the end, remove characters by using the delete key to amend the command before rerunning it.

## Shell Commands

Below, you will find a summary of the commands available. For each command, the reference on the manual page can give you more details. The command `man` can be used after your preferred name to see these online.

### Database management

Available are Oracle and MySQL

Command	Description
MySQL-workbench	GUI interface for MySQL
Sqldeveloper	Oracle SQL Developer GUI interface
Mysql	Run the MySQL SQL interface
Sqlplus	Run the Oracle SQL interpreter

### Word processing

LibreOffice is available and compatible with Microsoft Office.

Command	Description
LibreOffice	start applications for LibreOffice

Load at Antichi Colli EURU1269036 For developing high-quality printed documents using Linux or other operating systems, an extensively used language of typesetting is `TeX`. When you intend to format manual pages, the standard typical Linux text formatting people generally use is another program collection built on `Troff`.

## TeX

Command	Description
Dvips	Convert a DVI file to POST SCRIPT
Xdvi	DVI previewer
Pdflatex	latex formatter with PDF output
latex	latex formatter
tex	text formatting and typesetting

## Troff

Command	Description
Pic	troff preprocessor for drawing pictures
groff	GNU troff interface for laserprinting
nroff	text formatting language
troff	text formatting and typesetting language
Grap	pic preprocessor for drawing graphs
tbl	prepare tables for nroff or troff
eqn	mathematical preprocessor for troff

## General commands

Command	Description
aspell	interactive spelling checker
spell	check text for spelling error
acroread	PDF viewer
evince	GNOME PostScript previewer
fmt	simple text formatter

## Programming

Available are these languages and programming tools.

## FORTRAN

Command	Description

f95	GNU Fortran 95 compiler
-----	-------------------------

## JAVA

Command	Description
eclipse	Java integrated development environment on Linux
javac	JAVA compiler
appletviewer	JAVA applet viewer

## C++

Command	Description
g++	GNU C++ Compiler

## C

Command	Description
cxref	generate C program cross reference
indent	indent and format C program source
ctrace	C program debugger
gcc	GNU ANSI C Compiler
cb	C program beautifier

## General

Command	Description
strip	remove symbol table and relocate bits
nm	print program's name list
Size	print program's size
make	maintain groups of programs

## Other languages (not on all systems are these available)

Command	Description
asp	web page embedded language

mathematica	symbolic maths package
php	web page embedded language
squeak	Smalltalk
python	object-oriented programming language
perl	general purpose language
gcl	GNU Common Lisp
mattab	maths package
bc	interactive arithmetic language processor

## Networking

Command	Description
google-chrome	web browser
firefox	web browser
curl	transfer data from a url
rsh	remote shell
rlogin	gaining access remotely to a Linux host
ssh	secure shell terminal or command connection
telnet	getting to another host by connecting through the terminal
wget	non-interactive network downloader
scp	copy of remote file for secure shell
rcp	remote file copy
sftp	program for transferring file in secure shell
tftp	trivial file transfer program
ftp	file transfer program

## Messages between users

There is support for on-screen messages to other users and world-wide electronic mail in the Linux systems.

Command	Description
thunderbird	GUI mail handling tool on Linux
Mail	mail program for easy read or send
pine	vdu-based mail utility
wall	send a message to all local users

## Printing

Expect the printer name to be given following a *-p* argument as most commands which can be used to print files. And as simple text files, files may be sent to the printers or for the laser printers; they may be processed in various ways.

Command	Description
<i>a2ps-Pprinter</i>	format text file in PostScript and print on laser printer
<i>dvips-Pprinter</i>	postprocess TeX file into PostScript and print on a laser printer
<i>LPR-Pprinter</i>	send a file to a printer

Direct from some applications or with the use of the GUI print manager; you can use the shell to print files. It is by name that you need to specify a printer, and some of them are:

Printer Name	Location
tl4_lw	Teaching Lab 4 (C/2.10) laser printer
tl2_lw	Teaching Lab 2 (C/2.05) laser printer
tl3_lw	Teaching Lab 3 (C/2.08) laser print
tl1_lw	Teaching Lab 1 (C/2.04) laser printer

## Status

These commands alter or list information about the system.

Command	Description
printenv	display value of a shell variable
who	list logged in users
w	show what logged in users are doing
netstat	show network status
vmstat	report virtual memory statistics
lun	list user names or login ID
users	print names of logged-in users
last	show last logins of users

uptime	display system status
kill	send a signal to a process
Tty	print current terminal name
iostat	report I/O statistics
homequota	show quota and file usage
time	time a command
groups	show group memberships
stty	Set terminal options
script	keep script of terminal session
du	print amount of disk usage
reset	reset terminal mode
quota -v	display disk usage and limits
date	print the date
ps	print process status statistic

## Information

Here are some shell commands that give information.

Command	Description
yelp	GNOME help viewer
info	displays command information pages online
man	displays manual pages online
apropos	locate commands by keyword lookup

## Compressed files

To save space, you may need to compress files. You can use the following to examine and create compressed files.

Command	Description
zcmp, zdiff	compare compressed files
gunzip	uncompress gzipped files
zcat	cat a compressed file
uncompress	uncompress files
zmore	file perusal filter for crt viewing of compressed text

gzip	compress files
------	----------------

## Manipulating data

You can use the command below to alter or compare the contents of files.

Command	Description
wc	count characters, lines, and words
look	find lines in sorted data
join	join files on some common field
uniq	report repeated lines in a file
gawk	pattern processing and scanning language
tr	translate characters
expand, unexpand	expand tabs to spaces and vice versa
split	split file into smaller files
diff	differential file comparator
sort	sort file data
cut	cut out selected fields of each line of a file
sed	stream text editor
comm	compare sorted data
paste	merge file data
cmp	compare the contents of two files
perl	data manipulation language
awk	Pattern processing and scanning language

## File editors

You can amend and create files by using editors.

Command	Description
vi, vim	standard text editor
gedit	GNOME text editor
pluma	Mate GUI text editor
pico	easy text editor for vdu\$
ex, edit	line editor
xemacs	emacs with mouse action
emacs	GNU project Emacs



## Files directory

You can handle files and create file directory through these commands.

Command	Description
lpq	spool queue examination program
touch	update modification and access times of a file
just	text justification program
tail	print last lines from file
head	give first few lines
rm, rmdir	remove (unlink) directories or files
grep	search file for regular expression
pwd	print working directory
find	Find files
mv	rename or move file type
file	determine file type
more, page	display file data at your terminal
cp	copy file data
mkdir	make a new directory
chmod	change file mode
ls	list and generate statistics for files
chgrp	change file group
lprm, cancel	Remove jobs from line printer queue
cd	change current directory
lpr	spool file for line printing

## Logging out

Command	Description
logout	log out of a Linux terminal

You must take note that you must exit the Desktop Environment instead of a Linux workstation.

# Chapter 11: Shell Scripting

For a Linux-based OS, a text file that has commands sequence is a shell script. The commands sequence of the shell script would have to be typed into a single script at a time into the keyboard. As an interpreter for commands set that you use to communicate with the system, the shell is the CLI, command-line interface's operating system. For them to save time, a user must repeatedly use the command sequence of a shell script. There are subcommands, comments, and parameters that the shell needs to follow, just like other programs. And it is by entering the file name on a command-line in the shell that users can initiate the sequence of commands. A shell script is known as a batch file in the DOS operating system as it also referred to as an EXEC in the mainframe VM operating system of IBM.

You can enter the command for the system execution since it is within the operating system of Linux that you will find the shell program. On a Linux computer, the shell program will start, providing the chance to have your commands entered through an interface when a terminal window is opened. The command-line interface is what this interface is referred to by people. On the screen, you can see the display of the output, and the shell executes it when a command is entered. Also, stored in a file, some commands can also be executed by the shell in addition to being able to execute and accept commands interactively. Shell scripting is recognized as the mode of this execution.

## **How shell script works**

Giving the shell executive permission, making the script accessible to the shell, and writing the script are some of the fundamental steps involved with shell scripting. You can use a graphical user interface, GUI, word processor, or text editor to write shell script since it contains ASCII. The shell can interpret the language of a series of commands in the content of the script. Shortcuts, arrays, *if/then/else* statements, variables, and loops are some of the functions that shell scripts support. In a location that the shell can access, you can use the .sh or .txt extension to save the file once complete.

## **Background to the shell**

In the 1970s, Ken Thomson developed V6 Shell, a shell program to start with Unix. Its scripting proficiency was quite lacking even as it was a shell with

interactive features. In 1977, Bourne Shell came on board and for the root account; as the default shell, it remains in use today. And through the years, it has been quite useful through the scripting abilities. By the 80s, Korn Shell and C-Shell gave the public something to talk about as the highly popular shell variants. There was a drastic difference from the original shell as specific syntax has been brought by every one of these shells. As such, Bash is an extremely prominent shell today. As the unique Bourne Shell's massively enhanced variant, it stands for Bourne-Again- Shell.

### **Shell script applications examples**

By typing one line at a time, you can save quite a lot of time from doing some repetitive task when you use a shell script. Below are some of the examples of applications that you can use a shell script for:

- Monitoring a system
- Executing routine backups
- Linking existing programs together
- Manipulating files
- Completing batch
- Creating a program or running a programming environment
- Automating the code compiling process

### **Shell script execution**

As the shell's argument, all you have to do is to pass the script path if you want to execute a shell script. You need to pay attention to the fact that LF characters, Line-Feed, are required for terminating the lines by the shell. It is easy to run into errors if, on a Linux system, you attempt to execute shell script promptly or write it on Windows. For line termination, Carriage-return-Line-Feed, the combination of CR-LF is what Windows uses, and you will need to have it in LF-only conversion. For means to go about achieving this, you can check your Windows editor.

As a command, the shell script can be executed directly using another way. As your shell script's first line, you can insert the *hashbang* declaration below:

**#!/bin/bash**

Then, you can do some command to make your script file executable. Right now, without having to reference the shell explicitly, you can have the script file executed directly.

### **Benefits of shell scripts**

Things are meant to be efficient and simple when you use shell script. It removes any interpretation issues since it is a similar syntax that it uses on the shell command-line that it uses in the script. Also, more than other programming languages, it requires less of learning curves and also faster when it comes to writing code for a shell script. However, if left unnoticed, this tends to prove extremely costly if there is an error in a shell script. Also, there may not be compatibility with different platforms connected with shell scripting, and more than individual commands; shell scripts can also be slower to execute. All the same, here are more advantages of shell scripts.

### **Portable:**

When the shell itself is present, you can transfer a shell script to another Unix and Unix-related OS. Also, shell scripts are much more portable than C/C++ programs when you are in the process of transferring a shell script from different architectures like Sparc, MIPS, x86, and so on. You will have to attempt to run a C/C++, build the program, and copy the source code for you to transfer and use a C/C++ program. Then, if it uses the architecture-specific code, it may not work as expected.

### **Transparency:**

Since it is a text file, you can check out the kind of actions the shell script is performing by viewing it quite easily. By contrast, it is if you have access to the source code or the source code wants to inform you that you can know the type of program in a language like C/C++. For example, it is possible to find out if any files are getting deleted by a shell script and then have those files copied to another place if you need those files. Also, because you may gain access to view the source code, shell scripts can be quite simple to diagnose than the regular programs. Though to avoid such errors, creating and checking programs are some of the responsibilities of a compliant shell script. You can as well create the directory as you look in the script code.

**Easier to develop:**

Inside a regular program written in C/C++, you can efficiently perform similar actions as the shell script. However, the shell script can be debugged and written far easier than a program like C/C++. By redirecting output, removing directories and files, and also execution of external commands, the shell is great for all these specific system administration tasks and more. For a much lower level operation, including manipulating data structures, invoking system calls, and so on, C/C++ programs tend to be much suitable for them.

**Multiple commands combination:**

One of the benefits of shell scripting is you can have multiple distinct sequences of commands as well as automating frequent tasks. For you to remember the direction in which you can execute multiple commands can be quite challenging than a single command. The Linux OS system sequence of boot-up is a perfect example here. For it to get the system into a proper state, the operating system executes a series of commands as one aspect of the boot-up process. The shell scripts that exist in the directory */etc* are these commands. You may end up performing the process by hand in the absence of shell scripts, and a system booting process complexity will come to your realization if you take a look at these shell scripts types. The */etc/profile* is an example of a shell script, and with the access of a user into the system, it can thus be executed.

**Task automation:**

Your executed tasks can be frequently automated when you use shell scripts, and this is the first benefit of it. Let's assume that daily, you need to perform a set of tasks. You can run these commands on the script after storing them in a file when you have to execute multiple commands on your Linux daily. For example:

- For too low or too high prices, when specific conditions are met, trigger an SMS or email as you parse the fetched data or fetch stock prices.
- As some log files appear to be growing every day, you can compress them.

- You can upload and archive a folder or file to a cloud storage facility every day like S3.

## Features of Shell Scripting

### **Shell scripting is powerful**

For every Linux-based operating system, you can get help almost for every one of them without any complaint, and it is convenient. You will have an excellent basis when you merge it with the standard accessible tool such as `sed`, `grep`, and `awk`.

### **Readability**

It is much lower to develop anything that is unreadable with a shell script. You can certainly make use of some unique features of the shell that others do not know of them.

### **Regularly accessible**

On all the programs you come across, you can always use shell scripting. By automating repetitive steps, it makes your life quite easier. All you need do is to insert your preferred commands in a file and run it happily after making it executable. As it is quick to master, so it is quite simple to learn.

### **Repeating**

In your shell script, you don't need recurring similar statements every day. Create a compelling set of functions and consist of that in your existing and new shell scripts. While you can call your function "Display," resist it when you are about to use "echo."

### **Conclusion**

To write workflow for epsilon, ETL, and several other tools to save time, quite useful for many organizations, is the scope of the shell scripts. And with the use of any of the shell scripts, professionals and users of Linux who want to automate tasks on Linux are the target audience of learning shell scripting technologies. For conditional programs that contain limited functions, loops, and statements, shell scripts can help to create these complex programs. Also, you can store data with shell scripts.

# Chapter 12: Building Script

Using the language of programming for the shell are short programs, while the interpretation can be achieved through the shell scripts and a process of the shell. On Linux and other operating systems, they are quite ideal for task automation. For Unix-related OS, a program that provides the text-only, traditional interface is a shell program. You can read commands that you type into a terminal window as an all-text mode window, as well as console, which is an all-text display mode, and then run its primary function. The very common versatile and highly used *bash* is the default shell on Linux as groups of commands that you can translate, which is compiled or interpreted into a machine language form, and that can be wholly understood by the system's CPU, the central processing unit. You write computer programs with artificial, precise language, which is a programming language.

To create shell scripts, shell scripting language or shell programming language are the *bash* feature, and other Unix-related OS use shells with each of them containing the programming language with built-in features. You can easily have shell scripts created, and when you go online and in several books are available for a comprehensive selection of undertakings with or without notification. These factors are some of the advantages of using shell scripts. Also, in the Unix-related OS default installation, shell scripts are used extensively.

## The first script

Here, you will see a useful introduction to shell scripts handling and creation with the following example. All previous lines of the screen of your monitor are cleared by the script, and on it, the text, *Good morning, world*, is written by it. You may not need a word processor but only need to have a text editor like *vi* or *gedit* opened when you want to create this script.

Also, with the functions of copy and paste used in the standard keyboard, you can copy the above code, open the text editor, and paste it into it. Then, the script is complete and quite close to running it after you have given a name to the file and have this plain text saved. By having the file name after a forward slash and a dot typed without any spaces between them and then hit on the 'enter' button, you will be ready to run scripts. For example, you can use the command below in the attempt to run it if you have the above script saved as *morning*:

```
./morning
```

Nevertheless, since you must first set the file to be *executable*, on the screen,

you can see the message of error. In that situation, the script will not run. For the new files, *write* and *read* are the only permissions they have by default. With its option of 755, you can make use of the `chmod` command to easily solve the problem. Using this, however in the same directory as the one below, you will have the ability not only to write and read the file, but you can also execute it:

```
chmod 755 morning
```

Then, while in the same directory and by typing the command below, you can prepare to run the script. To continue, hit the ‘enter’ button:

```
./morning
```

### **The operation process**

The type of shell to use for the interpretation of the script and for locating the shell is the first three lines will tell the operating systems. As the directory */bin* is its location, the shell is *bash*, and as such, the */bin/bash* is what the line contains. For the operating system to receive its signal that it is offering the shell’s location and name and other scripting languages, an exclamation mark, and a pound sign always precedes this instruction.

For you to dispense the command *clear*, it is the second line that the shell informs. With this easy command, you can remove all previous output and commands from the terminal or console window that there is a release of the command. On the screen, the *Good morning, world* phrase is what the shell gets from the third line. For whatever follows it to be repeated from the shell instruction, it uses the *echo* command. In a more advanced script, the quotation marks can make a big difference to use them as a useful programming drill even though they may not be necessary. An input data, an *argument* that the command `echo` receives is the *Good morning, world*, which is in slightly more technical terms. Also, scripts that people use freely are `echo` and `clear`, as is the case with other commands. For example, you will get the prompt to enter the next command, and you will have the entire previous output and commands removed when you type *clear* on the screen and hit the ‘enter’ button.

### **It isn’t working!**

There can be some reasons for the phrase *Good morning, world* not to appear at the top of the screen and some of them are:



1. For the *owner* of the file, they forget to change the permissions to *execute*.
2. In the same directory, the command was not issued where the file is located.
3. Instead of a text editor, a word processor was used to create it, and as such, the file is not a plain text file.
4. After the slash or period, space was inserted.
5. In the command, you omit or reverse the forward-slash or the period.
6. There is a difference in the name of the file and the one used in the command. For example, there can be a difference between capitalization, spelling, or even an extra or minor space.
7. You omit the word `echo`, and as a result, you made an error as you attempt to copy the code.

As the administrative user or the root, it is vital not to practice executing and writing scripts. You can damage the operating system with an improperly written script. Also, it could lead to necessarily reinstalling the operating system as a whole and result in the loss of valuable data in the worst-case scenario. You can easily use a command like `adduser` to quickly create one if an ordinary user account does not yet exist on the computer because of this reason.

## **Experiments**

Before you make a move to more complicated examples, if you are a curious user, you can do a variety of instructive, simple experiments. With the suggestions below, they make up of code revision, using a different file name or a similar name of a file to save the changes, and then with the above explanation, executing them.

1. Attempt to have a few of the wording altered. For instance, have the line changed to “*Good morning, people!*” `echo` .
2. For the line that you will write on the screen, you can have a

line, or more additional lines added as one horizontal space follow them at in any case, with each beginning having the word `echo` .

3. Concerning both lines of `echo` , you can also leave an empty line. Though by having `echo` typed on it, you can create a blank line, and that is all. It will be seen that this will not affect the result.
4. Then, have blank horizontal spaces inserted. Based on if you enter the primary reference marks before or after, there will be a different result.
5. To have a different location directory for the execution of the file. As such, when it is issued, you will have to add to the command name beginning, the executable script path. For example, if you have moved the file to `test` , a term of a subdirectory, you will have `./test/morning` .
6. You will want to add to the script file, some other command as another experiment like `df` that reveals the disk space usage, `uname` , which gives information about the hardware and software of a system, `pwd` that informs the present directory, and `ps` that explains the processes currently on the system. It is vital to understand that with any appropriate arguments or options, you can use these as well as other commands within the script.

## **Hello, World!**

For you to have the shell script created:

1. `vi` is the text editor suitable for you to use for this, and within the file, have in its logic and commands of Linux that you required.
2. You will need to escape from `vi`, and before doing so, close after saving the file.
3. The executable form of the script is quite essential
4. Then, you can move on to the environment of production once the output satisfies you after testing the script.

5. A line in Bash, which is a straightforward program, informs a command of the computer. So, use your preferred text editor like vi to start it.

### **Necessary Commands of vi:**

- To vacate vi:

Type :q after pressing ESC

- To search for a string:

type /wordToSearch after pressing ESC

- To jump to a line:

type :the line number after pressing ESC

- To quit after saving a file:

type :x after pressing ESC

OR

type :wq after pressing ESC

- To store a file:

type :w filename after pressing ESC

- To go into command mode:

```
press ESC
```

- To go into edit mode:

```
type I after pressing ESC
```

- To open a file:

```
vi filename
```

### The script running after saving it

On the screen, a message of error is what the `./hello.sh` command displayed. Since for the `hello.sh` script, you have not set executed permission, it may end up not running the script.

### Chmod command

To change the access permission of a file, you can make use of the `chmod` command. As follows, below is the syntax:

```
chmod ugo+rx filename
```

Where:

- x: execute permission
- w: write permission
- r: read permission
- =: overwrite current permissions

- -: removes the permission
- +: adds the permission
- o: others
- g: groups
- u: users

Below is how you can express permission through a numerical way:

- 0: no permissions at all
- 7: read, write, and execute permissions
- 1: execute permission
- 2: write permission
- 4: read permission

## Errors

The *robustness* of the program is often the measure used to differentiate a good and inadequate program. As such, when things go wrong, this is the ability of the program to handle these circumstances.

### Exit status

When it finishes, returning to the exit condition is what every program that is well-written does. Zero will be the exit status when a program completes quite successfully. Then, in some way, the program failed if there is nothing more than zero for the exit status. For the program exit status in the scripts that you call, it is entirely vital to check them. Also, when they finish, there must be a meaningful return on the exit status of your scripts. Specific lines of code like `$some_directory` can be written for the creation system by the system administrator of a Unix.

If everything goes quite well enough, this way might not have been the wrong way of going about doing this. To the name that the `$some_directory` contained, the working directory was changed by the two lines and also in such a directory, delete the file. That is quite the projected action. And if the

named directory in that `$some_directory` doesn't exist, what will then happen? Then, on the directory that is currently operational, the script will have the command `rm` executed and the command `cd` will fail. Indeed, not the planned action!

### **The exit category check**

For you to respond and get the program's exit status, you can use several ways. First, the environment alternative of the `$?` and its contents require adequate observation and for the execution of the last command is an exit status that the `$?` will contain.

Except to revert zero's exit status and also one respectively, the `false` and `true` commands are programs that remain dormant. And for the previous program, the exit position is what is contained in the `$?` environment option. Hence, it is quite essential to have the exit category checked.

The `cd` command's exit level is examined in this variety, and on standard error, we can have the error message printed if it's not zero and with 1 as the exit status, have the script terminated. However, we can save ourselves a few typing efforts by using some smarter techniques even when this happens to be an effective way-out to the crisis. Since it is the given commands of the exit status that it evaluates, we can make use of the statement *if* precisely as the next approach to attempt.

If there's a success with the command `cd`, we can check it here. And for the indication that an error has happened, a code of 1 is the program exit. As for the output is the error message, you can then execute `rm`.

# Chapter 13: Basic Bash Shell Commands

In a circumstance that a directory tends to be a *root directory* by possessing no parent directory or within a single other directories, it is a *subdirectory* that is known as “parent.” Thus, modern filesystems have folder or directory trees. And you can always get to the root directory by going from child directory to parent directory, which is typical of traversing backward through the file tree. Though Unix and Unix-like system only have `\`, a single root directory, such as Windows’ drives: `A:\`, `C:\`, etc., some filesystems have multiple root directories.

`pwd / ls / cd`

As we refer to the *working directory* or the current directory, it is always within some directories that the user is always using when working within a filesystem. With `pwd`, print the working directory of the user. Using `ls`, make a list of files and child directories, etc., that is, the content of this directory. Here, you need to pay attention to some of these points:

- Instead of `ls -l -a`, you can sometimes chain flag like `ls -la`
- Have a combination of several flags such as `ls -l -a`
- Reveal file details with `ls -l`
- Using `ls -a` to reveal hidden (“dot”) files

Using `cd` (change directory) to change to a different directory and the parent directory, the shorthand for `cd` is `cd`. To home directory normally `/home/username` or similar directory, the shorthand for `cd ~` or simply `cd` is `cd`. For this directory, `cd.` may not make any much impact since `.` is shorthand. Use `cd -` to go back to the most recent directory. And by using `cd ../,,etc.`, you can jump multiple directories levels. To home directory user, `cd ~user` means `cd`.

`;/ && / &`

Commands are the things that you type into the command-line and stored somewhere on your computer; they always execute some machine code. Sometimes, a built-in Linux command is this machine code, and sometimes

also, it is some code that you wrote yourself and perhaps an app. Occasionally, right after another, we will want to run one command, and we can as well use the “;” (semicolon) to do that:

The meaning of the semicolon is *l* first (*ls*) lists the contents of the working directory, and then *l* (*pwd*) prints its location. Then, *&&* can be used to chain commands, which is another useful tool. If the command to the left fails, the command to the right will not run. On the same line, you can use both *&&* and *;* multiple times.

Even if the first one fails, the second will run with *;*. There is a completely different function fulfilled by *&* even when it looks similar to *&&*. Usually, before it gives you access to enter another one, the command-line will wait for that command to finish when you execute a long-running command. You will be able to perform a new command while an older one is still going and also prevents this from happening when you put *&* after a command.

It is essential to know that we assume that the process or job is “backgrounded” when, to hide it, we make use of *&* after a command. Then, use the *job* command to see what background jobs are currently running.

## Getting Help

*man*

For you to bring manual for that command (with *q*, quit *man*), type *man* before nearly any command.

*-h*

And for you to bring up a help menu for that command, type *--help* or *-h*.

## Viewing and editing files

*nano / nedit*

For people or beginners that want to learn a million shortcuts, as a command-line text editor with minimalistic characteristics, *nano* is a great editor. For the first few years of coding career, it will be sufficient for any developer or programmer. As it allows for syntax highlighting, drag-and-drop, point-and-click editing, *nedit* opens up an X Window as a small graphical editor. When you plan to make some changes to a script and then rerun it over, you may want to use *nedit* for that. Atom, Notepad++, *gedit*, *vim*, *vi*, *emacs*, and some others are other common editors like graphical user interface, GUI or



command-line interface, CLI. Others are VS Code, Light Table, and Micro. The syntax highlighting, search and replace, and some other things are the basic convenience that all modern editors provide. Though `nano` and `nedit` don't have as many more features as `emacs` and `vi(m)`, their learning curves tend to be much steeper. You will discover the one that works for you after trying out a few different editors.

### *head / tail / cat / less*

File's few first lines are the `head` outputs. Though the default is 10, the number of lines to show is specified by the `-n` flag. File's last few lines are the `tail` outputs. Beginning from the  $N$ -th line with `tail -n +N`, you can get the end of the file or, like above, you can get the last  $n$  lines. Usually, the terminal, but what sends files to the standard output stream and concatenates a list of files is `cat`. You can use it to view files quickly, and with multiple files or just a single file, you can make use of the `cat`. But, here, pay close attention; you may be accused of a UUOC, Useless Use of Cat if you use `cat` in this way. You may not worry yourself too much about that because it's not a big deal.

For you to quickly view a file, another tool is `less` as it opens vim-like, read-only window. `more` is another command. However, `less` has a higher recommendation than `more` since it provides a superset of the functionality of `more`. At their `man` pages, you can learn about `more` and `less`.

## Creating and deleting directories and files

### *mkdir / rm / rmdir*

For you to create new, empty directories, you can use `mkdir`. As this is non-recoverable, you need to be cautious as using `rm` can remove any file. Then, with the `-i` flag, an “are you sure?” prompt can be removed. With the use of `rmdir`, you can remove an empty directory. Then, you could see a reference to its parent directory (`..`) as well as a reference to the directory itself (`.`) when you `ls -a` in an empty directory. It is only empty directories that `rmdir` removes.

However, using `rm -rf` (`-r` = recursive, `-f` =force) cannot remove a directory and all of its content.

### *touch*

It is to modify file timestamps that `touch` was created. However, you can also

create an empty file using it and such as `nano`, by opening it with a text editor, you can create a new file. You can also edit the file. Also, `touch` can be used as well. Note: `^z` (Ctrl+z) is the background a process. Then, hit `^z` with editing file. Shown by the jobs command where `N` is the job index, use `kill %N` to kill a background process. While it is running, press `^c` (Ctrl+c) to kill the current (foreground) from processing.

## History of command, links making, and copying and making files

*mv / cp / ln*

To rename or move a file, use `mv`. You can `mv` a file to a new file, to rename it, or keep the same file or `mv` a file to a new directory. Then, copy a file using `cp`. And for you to create a hard link to a file, use `ln`. Also, you can get a soft link created to a file with `ln -s`. In memory that contains a file, the same actual bytes are referenced in hard links, and while it points to those bytes, the soft links refer to the original file name.

## Command history

For you to be able to rerun and complete commands, there are two main features that you can get from `bash`. *Tab completion* is the first feature. For guessing the precise action you are attempting to take, you only need to press the key <tab> after you have the first section of the command typed. Then, you will complete the command after you must have typed `ls t` and press the TAB key. Note that if an ambiguity case arises, it may be required of you to press the <tab> several times. And as for your previously typed commands, you can get the short history of them since `bash` keeps them, and by typing `^r`(Ctrl+r), you will have the chance to have a search through for those commands. If you want to see the command history search, hit `^r`(Ctrl+r).

## Processes, disk usage, and directory trees

*ps / du / df*

For the hard drives of your system or the disks, if you want to know the amount of space your files have taken up, `df` will be there to show you. If you go through this command, you will notice that the meaning of `-h` is “human-readable” and not “help.” And rather than writing out integer, huge

bytes number, to display disk or file sizes, it is `G` for gigabytes and `K` for kilobytes that some commands use. For the subdirectories of a specific directory, the file space usage is what the `du` shows. You may use `df` for you to discover the free space of a particular hard drive. Also, using `du` will allow you to know the quantity of a directory's space. From the specified directory, the flag `--max-depth=N` are directories `N` levels fewer or down, which `du` takes. For current processes running by the users, it is shown by the `ps`.

*tree/ mkdir -p*

It is only a single directory, by default, that `mkdir` makes. As such, using `mkdir` only, it may be hard for you to make `d/e/f` since `d/e` directory has no existence. And also, if there is no such existence for them, all directories in the path can be made when we pass to `mkdir` from the `-p`. Also, when we have a nicely-formatted directory printed, we can visualize the structure of a directory better through the help of the `tree`. With a specified directory, in the beginning, the whole structure of the `tree` is printed by it. However, using the flag `-L`, you will have the power of restricting it to a particular number of levels. Then, using `-prune`, in the output of the `tree`, the empty directory can be hidden. You must know that the directory that is not that empty or the “recursive empty” will also be removed by this command, but which has in them other recursively empty directories or other empty directories.

## Miscellaneous

*exit / logout / passwd*

You can use `passwd` to have the password of your account changed. To verify it, you may have to provide the current password you are using. Then, to forestall any typo situation, it will want you to enter your new password two times. In a situation where it is only a user account that you have, the shell you have logged in will exit with the use of `logout`. And to have any shell exited, then use the `exit`.

*clear / \**

For you to have your new terminal line moved on to the screen top, then run `clear`. Below the line of your current prompt, you will have blank lines added to them by this command. Thus, you can clear your workspace with this. And in the situation of looking for specific files, wildcard, also known as Kleene

Star, \*, is perfect for it. And since it is equivalent to more characters or zero, in a command, you can make use of the glob several times.

## Processor usage, memory, and disk

*htop / top*

The processes that are running recently as well as their memory usage, owners, and many can be displayed through the `top`. The variant of the `top`, which is interactive and enhanced, is an `htop`. You need to know that the display processes can be restricted by using a `username` only to those owners while passing the flag `-u username`.

*ncdu*

Typical of an enhanced `du`, it is the file space usage overview, which is navigable that the `ncdu` offers. Also, it is a `vim`-related window with a read-only feature that it can open. When you want to quite, press `q`.

## REPLs

Though they utilize it for specific programming languages, typical of the command-line is Real-Evaluate-Print Loop, which is REPL. While you can use the function `quit()` for you to quit, the command `python` is what you can use to open the Python REPL. Also, using the command `R`, you can have the R REPL opened as well as using the function `q()` for you to quit. With the command `scala`, you can also have the Scala REPL opened and the command `:quit` when you want to quit. With Java REPL, you can use command `jshell` to have it opened and `/exit` command for you to quit. Optionally, with the use of `^d`(Ctrl+d), you can exit any of the REPLs. As `^d` signifies the input's end on Unix, it is also the marker for the end of the file, EOF.

*-v / --version / -version*

For most programs and commands to have the software version, they possess the flag `--version` or `-version`. This information tends to be available easily for most applications, even though there is a less intuitive factor for most. You need to take notice of the use of `-v` by some programs for the version flag, and this means 'verbose' for using `-v` by others, which, while debugging information or printing several diagnostics, can run the application.

## Environment variables

Within your `bash` shell, the tenacious variables that you can use and create are the environment variable, and “env vars” is their short-term. You can use it with the sign of a dollar ( `$` ), and for their definition, they make use of the equal sign ( `=` ). When you use `printenv`, the entire recently-defined env vars can be seen. Using the sign `=`, you can have a new environment variable set. You must be careful to note that your `=` has no space after or before. Using `echo` with a preceding sign of `$`, you can have a particular env var printed to the terminal. Attempt to surround other whitespace or all spaces around the environment variables with the quotes ( `“...”` ). Also, be cautious because you won’t get any warning and will probably overwrite an env var by having a value reassigned to it. Apart from those above, you can also use the command `export` to define the env vars. Also, they can be available to sub-processes, which are commands you called from this shell when you provide the meaning this way. When you use the command `unset` or leave the right-hand side of the `=` blank, you can have the environment variables unset.

# Chapter 14: Advanced Bash Shell Commands

As a fairly powerful programming language and not only appropriating seam connecting the user and the kernel of the operating system, the shell is a command interpreter. And by *gluing* together compiled binaries, utilities, tools, and system calls, you can build applications through a straightforward device called a script inside a shell program. By a shell script, available for invocation are indeed the whole catalog of Unix tools, utilities, and commands. Also, there can be additional flexibility and power to scripts through external shell commands like loop and testing constructs, if that were not enough. Without requiring a complete compactly designed programming language with plenty of the bells and whistles, it is to administrative systems tasks as well as other routines, repetitive jobs that shell scripts exceptionally lend themselves.

## Introduction to Regular Expression

A sequence of characters is an expression. Metacharacters are those characters that have an interpretation beyond and above the factual connotation that they have. For example, a speech by someone may be denoted by a quote symbol and ditto the subsequent symbols for a meta-meaning. Metacharacters or characters that specify or match patterns are regular expressions. Here are some of the components that a regular expression contains:

- **Modifiers.** By modifying, for the range of text that the regular expression is to match, these narrow or expand it. The backlash, brackets, and asterisk are some of the modifiers.
- **An anchor.** For the match between the text line and the regular expression, it is the anchor that designates this position. For example, anchors are \$ and ^.
- **A character set.** These characters retain their literal meaning. And with no metacharacters, a character set is the simplest type of regular expression.

String manipulation and text search are the significant applications aimed at regular expression, and it is a part of a sequence or a string that matches a set of characters or a single character for a regular expression.

- Escaped “angle brackets” -- `\<...\>` -- mark word boundaries.

Since otherwise, they possess only their literal character and meaning, the angle brackets need to be escaped.

The word “the” matches “`\<the\>`” and not the words “*others*,” “*there*,” “*them*,” etc. The only way to be sure that a particular regular expression works is to test it .

- The backlash -- `\` -- their character gets interpreted as it escapes a unique character.

Instead of its regular expression meaning of end-of-line, a “`\$`” reverts to its literal meaning of “\$.” Also, the literal meaning of “`\`” is a “`\\`.”

- Brackets – [...] – for a single regular expression to have a match, enclose a set of characters.

There is a match for common word patterns with the combination of sequences of bracketed characters. “there is a match between *yes*, *Yes*, *YES*, *yEs*, etc., and “`[Yy][Ee][Ss]`.” Another matches for any Social Security number are “`[0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]`.”

Except for those in the range *b* to *d*, all characters match “`^[^b-d]`.” Inverting or negating `^` is a typical instance for the meaning of the following regular expression (in a different context, taking on a role similar to !).

Any digit or lowercase letter that matches “`[a-z0-9]`”.

In the ranges of *k* to *y* and *b* to *P*, any of the characters that match “`[B-Pk=y]`.”

In the range of *c* to *n*, any of the characters that match “`[c-n]`.”

The characters *x*, *y*, or *z* match “`[xyz]`.”

- The end of a regular expression matches the end of a line, which is the dollar sign -- `$` --.

Matching blank lines is “`^$`.”

At the end of the line, XXX matches “XXX\$.”

- The beginning of a line matches the caret `--^--` and which negates the meaning of a set of characters in a regular expression depending on context sometimes.
- Except for a newline, any one character matches the dot `--.`

Though, not 13 additional character missing, “13” matches *13 + at least one of any character, including space: 1133, 11333*.

- As well as *zero* instances, any number that has the repetition of the regular expression or character string matches the asterisk `--*`.

“1133\*” matches *11 + one or more 3’s: 113, 1133, 1133333, and so on*.

- Extended regular expressions. Additional characters that the basic set have also. It is in *Perl*, *awk*, and *egrep* that they use it.
- One or more of a preceding regular expression matches the plus `--+--`. Though it does not match zero occurrences, it is the same role as in the `*` that it serves.
- Zero or one of the previous regular expression matches the question mark `--?--`. It is for matching single characters generally.
- Escaped “curly brackets” `--\{\}` – the previous regular expression to match is the indication of the number of the occurrences.

Because it is the literal character meaning that they only have otherwise, it is quite vital to escape the curly brackets. Technically, the fundamental regular expression arrangement does not correlate with this usage.

For the character in the 0 to 9 range, “[0-9]\{5}” matches precisely five digits.

Note: as the non-POSIX compliant, classic *awk* version with a regular expression, curly brackets are not available. However, without being escaped, they have permission from the option *-re-interval* which *gawk* has. The versions that have no obligation from escaping the curly brackets are some



## **egrep** and **perl**.

- Parentheses – () – has in its enclosure a set of regular expressions. Using `expr` in substring extraction, with the following operator “|” they tend to be quite useful.
- The regular expression or the `--|--` the alternate character set matches it.

As do the GNU utilities, there is support for some version of *ex*, *ed*, and *sed* the lengthy regular expressions escaped version in the above description.

- Character Classes of POSIX. `[ : class : ]`

For the match of identifying characters range, this is an alternate method.

- `[ : xdigit : ]` matches hexadecimal digits. This is the same as 0-9A-Fa-f.
- `[ : upper : ]` matches uppercase characters of alphabets. As such, A-Z tends to be the same.
- `[ : space : ]` matches whitespace characters (horizontal and space tab).
- `[ : print : ]` (printable characters) in the scope of ASCII 32 – 126, it matches characters. Though adding the space character, this tends to be similar to the `[ : graph : ]` below.
- `[ : lower : ]` characters of the alphabet with a lowercase that matches. The a-z is quite the same as this.
- `[ : graph : ]` (graphic printable characters). Though excluding the space character, in the scale of ASCII 33 – 126, it matches characters. This is similar to `[ : print : ]` above.
- `[ : digit : ]` matches (decimal) digits. This is equivalent to 0-9.
- `[ : cntrl : ]` matches control characters.
- `[ : blank : ]` matches a tab or space.
- `[ : alpha : ]` matches alphabetic characters. This is equivalent to A-Za-z.
- `[ : alnum : ]` matches numeric or alphabetic characters. This is

equivalent to A-Za-z0-9 .

## Conclusion

Thank you for making it through to the end of *LINUX Command-Line for Beginners: A Comprehensive Step-By-Step Starting Guide to Learn Linux from Scratch to Bash Scripting and Shell Programming*, let's hope it was informative and able to provide you with all of the tools you need to achieve your goals whatever they may be.

Chances are if you've made it to this point, it is because you want to know how you can navigate through the Linux operating system as well as having a clear grasp of the several command-lines and also the best ways of using them. You have made it to this point because you want to know all about many different pieces than Linux operating system comprises and also how you can install different distributions of Linux.

You will see that you can deal with types of installations for servers and also their roles. Reading through this book, you have learned how you can use Linux as a virtual machine inside another operating system, what dual booting is all about, and how you can boot Linux with the use of live CD/DVD.

In this book, you have read about Linux kernel and the operating systems, Linux directory structures, some of the fundamental Linux shell commands, how you can work with the disk, media, and data, and so much more. For you to get an understanding of how you can ideally use Linux and some of the associating programs, this book has shed enough light on essential terminals, editors, and shell.

# **Python Programming for Beginners**

---

*The Ultimate Crash Course to Learn  
Python Computer Language Faster  
and Easier*

*Introduction to Machine Learning and  
Artificial Intelligence*

---

By Dylan Mach

**© Copyright 2019 by Dylan Mach - All rights reserved.**

The content contained within this book may not be reproduced, duplicated or transmitted without direct written permission from the author or the publisher.

Under no circumstances will any blame or legal responsibility be held against the publisher, or author, for any damages, reparation, or monetary loss due to the information contained within this book. Either directly or indirectly.

**Legal Notice:**

This book is copyright protected. This book is only for personal use. You cannot amend, distribute, sell, use, quote or paraphrase any part, or the content within this book, without the consent of the author or publisher.

**Disclaimer Notice:**

Please note the information contained within this document is for educational and entertainment purposes only. All effort has been executed to present accurate, up to date, and reliable, complete information. No warranties of any kind are declared or implied. Readers acknowledge that the author is not engaging in the rendering of legal, financial, medical or professional advice. The content within this book has been derived from various sources. Please consult a licensed professional before attempting any techniques outlined in this book.

By reading this document, the reader agrees that under no circumstances is the author responsible for any losses, direct or indirect, which are incurred as a result of the use of the information contained within this document, including, but not limited to, — errors, omissions, or inaccuracies.



## Table of content

[Conclusion](#)

[Introduction](#)

[Chapter 1: Introduction to Python](#)

[Chapter 2: Variables](#)

[Chapter 3: Operators](#)

[Chapter 4: Loops](#)

[Chapter 5: Functions](#)

[Chapter 6: Object-Oriented Programming-OOP](#)

[Chapter 7: Modules](#)

[Chapter 8: File handling](#)

[Conclusion](#)

# Introduction

Congratulations on purchasing *Python programming for beginners: The ultimate crash course to learn python computer language faster and easier* and thank you for doing so.

In this book, you will find a lot of really important and essential theories that will help you to get started into the Python programming language. Besides, you will find a lot of examples that will help you to understand in a more visual way the things that we have explained here.

In the following chapters you will find a short introduction to how programming languages started, who invented Python, who uses python nowadays, and all the information that is needed to learn Python from scratch such as variables, operators, data types, functions, loops, statements, exceptions, how to create classes, modules, a whole chapter about Object-Oriented Programming, also known as OOP, file handling of .txt, .PDF, .xlsx, and a lot of information that will make you a Python programmer.

We strongly recommend reading the codes here written, analyze them, understand them, and then try to do an example using each one of them in order to remember them easily. Because as you will see, there are tons of commands and statements that won't be easy to learn and remember if they are not used

There are plenty of books on this subject on the market, thanks again for choosing this one! Every effort was made to ensure it is full of as much useful information as possible, please enjoy!

# Chapter 1: Introduction to Python

We can define programming as the process of designing, coding, debugging and maintaining the source code of a computer program, which means, that we say the steps to follow for the creation of the source code of computer programs.

The programming language, are all those rules or regulations, symbols and particular words used for the creation of a program, and with it, offer a solution to a particular problem. The best-known programming languages are: Basic (1964), C++ (1983), Python (1991), Java (1995), C# (2000), among others.

Programming is one of the stages for software development; programming specifies the structure and behavior of a program, verifying if it is working properly or not. Programming includes the specification of the algorithm defined as the sequence of steps and operations that the program must perform to solve a problem, for the algorithm to work, the program must be implemented in a compatible and correct language.

We could consider programming even easier than learning a new language because the programming language will be governed by a set of rules, which are, generally, always similar so you could say that it might be considered as a natural language.

In order to better understand the subject of programming, we could start with the beginnings of programming and how all this universe of languages and programs we know today began. We could start saying that programming began when the first computer was created in the fifteenth century, when a machine capable of doing basic operations and square roots appeared (Gottfried Wilhelm von Leibniz), although the one that actually

served as a great influence for the creation of the first computer was the differential machine for calculating polynomials with the support of Lady Ada Countess (1815-1852), known as the first person who entered programming, and from whom comes the name of the programming language ADA, created by the DoD (Department of the United States), in the 1970s.

Initially, it was programmed in binary codes (bi=2), in other words, it consists of strings of 0s and 1s, which is the language directly understood by the computer, or what is known as machine language, a language considered fundamental for the computer to be thus capable of interpreting the information supplied. Later the languages of high level appeared, using words in English, to give orders to follow, using intermediate processes between the language and the computer, this process can be a compiler or an interpreter.

The syntax of these programming languages is much simpler than our languages and they use a much smaller vocabulary and set of rules. In summary, we could say that programming is a set of sentences written in a programming language that tells the computer what tasks to perform and in what order, through a series of instructions that fully detail the process.

In the world of programming languages, we find interpreted languages, such as javascript, where a program called interpreter executes the sentences while reading the text file where they are written, which is why these programs are often also called scripts.

On the other hand, we have compiled languages such as Java, in this case, we must previously convert the text file to a "translation" through a program called compiler and the resulting file is the one that will finally run on the computer.



In this book we will speak specifically of the Python programming language, being this an interpreted language whose main and most important characteristic is the application of a syntax that favors the application of readable code. We could say that the interpreter is a type of program that executes a code directly, that is to say, it does not need to be compiled, and that is the case of our target language.

## **What is Python?**

Python is one of the most important programming languages nowadays, being a general-purpose language, in this book you will have the language bases so that you can start with it. With this language, you can create a huge and varied amount of applications, because it allows you to create different kinds of applications since it doesn't have a defined purpose.

## **History of Python**

This language was created by Guido Van Rossum in the early 1990s, at the Centre for Mathematics and Informatics (CWI, Netherlands), specifically in 1989, as Van Rossum himself explained in one of his interviews:

"In December 1989, I was looking for a hobby programming project to keep me busy during the Christmas weeks. My office would be closed and I would have nothing but my computer at home. I decided to write an interpreter for the new scripting language I had been coming up with recently: an ABC descendant that Unix/c hackers would like. I chose Python's name for the project, finding myself in a slightly irreverent state of mind (and being a big fan of Monty Python's Flying Circus)."

It began to be implemented in December 1989, and in February 1990 was released the first public version, version 0.9.0. Version 1.0 was released

in January 1994, version 2.0 was released in October 2000 and version 3.0 was released on December 2008.

This programming language has as fundamental philosophy to have a syntax that favors a readable code, it is a high-level language that can be extended with C or C++, it has several programming environments that allow to edit programs, interact with the interpreter, develop projects, debug, among others and at the moment it is supported by a large community that facilitates its learning and that is producing a new progress in its already known new versions.

Python is a high-level programming language, interpreted and multipurpose, being currently one of the most used programming languages for software development. In recent years it has become a very valuable tool in the area of programming, this language is under a license of free software, under a license of Open Source or open-source approved by OSI (Open System Interconnect), so it is a program that can be used and distributed freely, either for personal or commercial use. The purpose of Python Software Foundation, "is to promote, protect and advance the Python programming language and to support and facilitate the growth of a diverse and international community of Python programmers".

The main advantage of an open and free technology is that it can be used without having to cover licensing costs. Free software is one of the most popular technological movements in the 21st century.

This language can be executed from any environment and distributed at the discretion of the user, modify if necessary, thus having a quick and easy basic tool for building programs.

To understand why we must learn python, it is necessary to

understand the main characteristics of this language, that is why we will start talking about its main characteristics:

- It is a multiparadigm programming language, which means that we do not have to focus on a single way of programming, but we can do object-oriented programming, iterative programming, and functional programming, so we are not forced to focus on a single paradigm, hence its name of multiparadigm.
- It is a multiplatform language, which indicates that we can program in different environments or operating systems, such as Windows, Linux, etc..
- It is a very easy language to learn because it is simple and minimalist, and this is one of the main reasons why most people decide to have Python as their first programming language, because it has the simplest syntax to learn, it is an interpreted language, by this we mean that when executing a program, it will have the ability to execute itself taking instruction by instruction.
- It uses a dynamic typed, that can be explained in the following way, when we create a variable, and we store an initial type of data to it, the dynamic typed means that throughout the program this variable could change and store another value of another type of data, that later we will see this in detail.
- At the moment, we can also point out that this language

occupies the position number four of the TIOBE index, which is an index that catalogs the languages according to their current popularity, being Java in first place, then in second place is the C language, in the third place is the C++ language and in the fourth Python, which indicates that it is a very popular and widely used language nowadays.

Now, knowing the characteristics of the program it is important to differentiate why we should learn Python and how it will serve us, what we can program with it, so well, being a general-purpose language, almost everything can be programmed with it: such as desktop applications with graphical interfaces and databases, web applications, games, custom applications, as a point of sale system for your business, for example, artificial intelligence, among others.

We will now talk about the development environment of this language, we can say that a development environment is a text editor in which we will be able to copy all the Python code, run our programs, do our tests, and so on. We will mention some of these editors, such as PyCharm, PyDev, Sublime Text 3, ATOM, VIM, as well as many others, in this book we will work with Visual Studio Code.

## **What can I do with Python?**

As it is an easy to learn language, meaning it has a quite high learning curve, like many modern languages, as well as a very clean and simple syntax, as explained above, it is a very versatile language, because with it and the standard library we can write desktop applications and web applications. Python has excellent support for object-oriented programming (OOP), the only limitation for this language is your imagination. This programming language is built in such a way that there will always be a more optimal way

to do things. This language is also used to work with artificial intelligence or robotics, where it is currently most used is for Big Data as it is a language that can handle a lot of data and complex operations.

## **In the area of video games:**

The area of video games has its advantages and disadvantages, being Python an interpreted language, it is twice (or more) slower than a compiled language like Java, C++ or C#; you can do wonders of games in Python using libraries such as Pygame, SDL2 (Binding), OpenGL (binding), only that your game will not run as an executable made with C++ for example, instead it will run with the Python interpreter. But you will have an excellent language with a lot of support and documentation, and very few lines of code.

Finally, we can mention the scientific area, this is where Python shines. The syntax of Python and the bunch of libraries it gives you by default makes it perfect for scientific programming, plus in the Python community, there are huge libraries for mathematics and all that this entails.

## **Why should we use Python as a programming language?**

Mainly we could say that we should use it because it is a very versatile language and general-purpose, this means that if your scope is not defined, you can create a huge number of applications using this language, suppose that your main goal is to create a web application, with Python you can do it, but probably tomorrow your interest will focus on scientific applications, because with Python you can also do it. In fact, the main development area of this language is the scientific area, if on the opposite you want to develop a low-level application, or you would like to use it in hardware because it is also possible to do it with this programming language, it is absolutely possible. That is why we talk about it being a versatile

language since it does not have a rigorously defined scope.

## **Who uses Python today?**

At the present time, this programming language is very commonly used, in addition, it has a wide range of uses, from the compilation and processing of data to the learning of a computer, which is why many of the important companies are currently working with this versatile programming language. We will mention some of these companies:

1. Google; it is a company that has handled this language from practically its beginning, in fact, its founders explained in one of their interviews that, "Python where we can, C++ where we must". This leads us to think that C++ is used for Google when memory control is imperative. So it is currently one of the company's official languages along with C++, Java and Go, which are the other three languages used. It is worth mentioning that Guido van Rossum himself worked in Google from 2005 to 2012, which indicates how important Python is for Google.

2. Facebook; in this company, Python is also part of this important social network, being in third place of language most used just behind C++, for example; in this company are handled more than five thousand confirmations of service and utilities such as infrastructure management, binary distribution, hardware images, and operational automation. As we have mentioned before, the ease of use of Python's libraries helps engineers to avoid having to maintain so many codes, making it easier to focus on brand optimization.

3. Spotify; one of the most important music companies today, is a large Python operator, due to how fast it is to write and encode on it. To provide suggestions and recommendations for all its users, Spotify relies heavily on a large volume of analysis and has Luigi, which is a Python

module that synchronizes with Hadoop.

4. Netflix; this company uses python in a similar way to Spotify as it relies on this language to enhance its server-side analysis. Most of the engineers who work for this company are free to choose the language to work with, and most of them choose this language to encode.

5. Dropbox; this cloud-based storage system uses this language in its client's desktop. In 2012 Rossum joined this company on the condition that they would allow him to be just an engineer, not a leader or a manager, during his time at the company he helped to generate the ability to share data warehouses with other users within the Dropbox community.

6. Industrial Light and Magic (ILM) is a special effects center, founded by George Lucas himself in 1975, to create special effects for the well-known movies Star Wars. ILM selected Python 1.4, because it is much faster to integrate into their existing infrastructure, also, the easy Interoperability of Python with C+ and C++ made easy for ILM to import Python into their patented lighting software.

In this way we can see how Python is in more and more places, using this language to wrap software components, expand graphic applications, among other skills, it has a wide range of code libraries and is more sensitive in development areas

## **How do I know which Python version should I use?**

In Python, there are currently two versions that are incompatible between themselves, which causes a lot of confusion to any user who is starting to program or even any user who is starting in the same language. These versions are called Python 2.x which was released in 2000 and was updated until 2010, however, in 2008 was released version 3.x which is

currently in full development of new versions and improvements in their commands.

## **But, do these versions contain the same tools?**

Well, there is a big difference between each version of Python among which highlights that in Python 3.x the print sentence is taken into account as a function, so it is necessary to call it and enclose in parentheses what you want to print. Unlike in the version 2.x which does not need parentheses to print.

When you are going to iterate a dictionary in Python version 2.x, the key-value elements are used through the items() and iteritems() methods. In the current version of Python 3.x, this operation is done only through the items(), keys() and values() methods and when using the iteritems() method we will obtain an exception of the AttributeError type.

There is also a change in the input function, which in the Python 2.x version takes the data without converting the variable type. In this version, if we enter an integer variable, its entry will be of the "int" type and if we want it to be treated as a string we would have to call the function "raw\_input" since this will be in charge of converting "int" data to string.

In the Python 3.x version, this takes a big step forward since the "raw\_input" function is suppressed and any conversion would be easily done through the input() function.

## **Now that I know which version to use, how can I install Python according to my operating system?**

The Python programming language is included by default in the Mac OS and Linux operating systems, the only thing to do is to update according



to the version you have, however, for Windows users, the program must be installed since it is not included in the system.

### Install Python on Windows

Go to <https://www.python.org/downloads/>

Choose the version of your preference to install: 2.x and 3.x. It is always recommended for new users to use the latest version of Python (3.x), this facilitates understanding thanks to its simplified tools. However, if you are using a recycled code, it is recommended to use the version in which it was written.

Once the download is finished, run the program.

If you are a new user, it is recommended to install Python with its default settings. If you are a language experienced user, you can do the custom installation.

Verify that the program and its interpreter work correctly.

### Install or upgrade Python for Mac OS

Python comes by default in OS X with version 2.7. If you need to upgrade your version to 3.x just follow these steps:

Enter [python.org/downloads](https://python.org/downloads) on your computer, the link will automatically detect the operating system you have and it will show you the files compatible with the computer to start the download.

Click on the PKG file to start its installation and if you are a new user.

Start the Python program by typing "Python3" in order to start the interface of this new version.

### Installing or Upgrading Python For Linux

In almost all Linux distributions Python is previously installed by default, so it is not necessarily needed to install but rather update, the only detail is that for a policy issue of installation the vast majority comes with Python 2.x and not with Python 3.x, as should be, especially if we consider that most modern applications require or recommend version 3.x to compile.

To upgrade Python, just follow these steps:

Check the Python version you have, since the Linux Operating System is included with the program, however, its version may vary.

On the Linux terminal type "sudo apt-get install Python".

Then in the same terminal type "sudo yum install Python".

Enter as a root user by typing "pacman-S python".

Finally, start the program and check that it works correctly so you can start programming.

## Learning to use Python

Once Python is downloaded, you will need a code editor that allows you to interpret and write code for programs. There is a great variety of editors, this depends and goes according to the preference and level of experience of the user with the programming since it will be your ally while programming.

Among the best-known editors are:

**Visual Studio Code:** It is a multi-platform source code editor with a dark interface; it has an optimized user interface. This editor has multiple tools and even allows real-time updates of our code while compiling. You do

not need a complete IDE and it is possible to change the appearance of your interface through the themes it brings.

Visual Studio Code supports a wide variety of languages, including Python, Php, Java, C++, Ruby, Go, C, SQL, JavaScript, Batch, and Objective-C.

**Sublime text:** This is a multiplatform editor with a dark interface, which allows to execute a great variety of documents in multiple tabs and offers a full-screen mode, thus facilitating the user's visual space in the computer. This has a panel that allows you to move through the code quickly and easily. Sublime text is capable of interpreting a wide variety of programming languages such as Python, CSS, C++, HTML, Matlab, R, SQL, C, Php) and has autosave, another fact and advantage of this editor is that it allows running files in Python with just a shortcut on the keyboard; Ctrl+B.

**Geany:** This is a multiplatform code editor of the Linux operating system, which is ideal for application development and even software development for this operating system and also that it is possible to operate on operating systems such as Windows, Mac OS or any other system with GTK library support. In addition, this editor is distinguished for being fast and lightweight, is completely independent and supports languages such as HTML, C++, JAVA, PHP, PYTHON, and C.

**Wing:** This is another paid integrated development environment for Python, it is owned by the company Wingware. It was created mainly for professional developers. It offers a great set of tools and features necessary for Python programming, it is compatible with Windows, OS X, and Linux and works with Python 3.x versions. Wing has a free basic version, a personal edition and a professional edition which can be considered very powerful when creating a program.

**Komodo Edit:** This is an open-source editor oriented to dynamic languages including Python, JavaScript, HTML, CSS, Perl, NodeJS. Komodo is considered one of the most popular code editors for applications today and also has a premium package that includes a number of useful tools, such as allowing writing codes and collaborating in the development of other codes in real-time, exploring databases, removing bugs. It is mostly focused on small project developers.

**Ninja IDE:** This is a text editor for development, which will only allow us to create projects in Python and at the same time run them in order to correct any errors that may occur at any moment.

## **Python's Keywords:**

It is well known that in every programming language there is a series of words and commands which are found in a reserved way and can not be used for anything other than to fulfill its function. In Python there is also has a set of words, these are called: reserved words or keywords, and are nothing more than a set of words in which each element contains a special meaning and is an indispensable part of the syntax of its language for the correct development of the code.

These words must be written exactly as shown in the following table, which will contain some of the reserved words of the language. If this is not done, the program will not be able to recognize them and can generate a type of exception called: `NameError`, this is because Python does not distinguish between upper and lower case or as it is formally known: case sensitive.

If we write `false`, the Python interpreter will not be able to understand that we are referring to the `False` operator and will throw us an error because this is not defined.

The following table will show the set of keywords for the Python 3.x version (version with which we are going to work in the next programs), which have defined approximately 33 reserved words; these same ones form the nucleus of the syntax of this programming language.

“and”	“def”	“finally”	“in”	“or”	“while”
“as”	“del”	“for”	“is”	“pass”	“with”
“assert”	“elif”	“from”	“lambda”	“raise”	“yield”
“break”	“else”	“global”	“None”	“return”	
“class”	“except”	“if”	“nonlocal”	“True”	
“continue”	“False”	“import”	“not”	“try”	

Of this group, there are a certain number of words which are considered "essential", these could be the ones we are going to use the most and we will explain them in-depth in the next chapters.

True & False: These expressions are those whose values are thrown to us by the program as a result of evaluating logical expressions.

and & or: These expressions are those that we use as connectors for the logical expressions (True & False), in order to be able to create much more complex expressions.

if, elif & else: These expressions are those which are used to build blocks of conditions, in order to make certain decisions within the same programs.

For & while: These expressions are used to build loops or formally: repetitive blocks.

Def & return: These expressions are those that represent instructions, which will be used to define our own functions. In other words: these expressions represent a series of instructions that will be in charge of carrying

out a certain task as indicated.

Import & from: These expressions are those used to add additional functionalities.

If you are using a code that has been written in Python 2.x version or you simply want to start in this version, we can see that unlike Python 3.x version, this version has only 31 reserved words or keywords.

“and”	“def”	“finally”	“in”	“print”	“yield”
“as”	“del”	“for”	“is”	“raise”	
“assert”	“elif”	“from”	“lambda”	“return”	
“break”	“else”	“global”	“not”	“try”	
“class”	“except”	“if”	“or”	“while”	
“continue”	“exec”	“import”	“pass”	“with”	

What are the differences in keywords between Python 2.x and Python 3.x?

Below, we will mention those important differences that cannot be noticed at first sight:

- Python 3.x incorporates the words "True", "False" and "None".
- In Python 2.x the words "exec" and "print" that were part of the keywords, become integrated functions in Python 3.x with the syntax `exec()` and `print()`.

## How can I find these words?

In Python, there is a module whose name is known as keyword module of the standard library, this is responsible for exporting a list called: `kwlist`. which contains all the keywords that are reserved in our programming language, Python.

Another easier way to consult these keywords is through the `help()` command, this is just a function that comes integrated and facilitates us to consult information, documentation and get a clearer help on the components of our program.

If in any given situation you need to quickly consult the operation or meaning of a particular keyword (only of the Python programming language), you can do it through the command `help()`, once introduced this, you must write the keyword to consult and immediately will show us on screen all the information of the word requested.

## **Python syntax and its importance**

Now we will talk about the most important thing and it will be what will allow us to advance in our code and in programming in general: The syntax; we know very well that Python is an interpreted programming language, but what does this really mean?

Our Python programming language works through tabulations, this is informally known as indentation or spaces. This means that, at the moment of executing a program, it is going to follow an order of interpretation, which works through the tab key on our keyboard which is just the key containing arrows located above Caps Lock, these tabs work in each loop or conditional sentence.

When we have a correct indentation we can avoid the use of keys and brackets and we can even avoid some reserved words to start and end a program that marks a block of code. This allows the program to have better use and operation.

Having a good indentation also helps us to make our code look uniform in order to facilitate reading and provide comfort to any third party

who reads it, and even to ourselves, because we can locate an error effectively and quickly.

It is important to emphasize that the first line of the code should never be indented, the indentation will always go after this and with 4 boxes of space.

Physical and logical lines: A program in Python is composed of a set of logical lines, they are formed by a certain amount of physical lines.

But... What are physical lines?

Physical lines are those lines that are used to enumerate our code editor, or formally can be described as a sequence of characters which end when entering the end-of-line character `"\n"`.

And what are logical lines?

Logical lines are those that go with Python syntax logic components and their end is determined by the NEWLINE token which determines the end of each line and starts another.

These physical lines have the ability to be united through an action called "implicit union of lines" to form a single logical line, using characters such as parentheses `()`, square brackets `[]` and keys `{}`.

If we start a logical line with the start characters such as `"(", "[", "{"` it will extend through all the necessary logical lines until it ends with its closing symbol `)", "]", "{"`.

There are two types of statements in Python:

Simple statements: These types of statements are those that must be completed in a single logical line. For example:



Print objects in the program: `print()`

Generate exceptions: `raise EndSearch (location)`

Access Attributes: `from sys import stdin`

Access modules: `import sys`

Execute functions through expressions: `log.write()`

Compound statements: These types of statements are those that must begin with the compound statement clause, followed by the contained statement on the next line. This must be correctly indented since it will be part of the body of our code. It will always start with a keyword and end with a colon ":".

An example of compound sentences is sequence and iteration for, else, else, if, elif, loops while, and else.

Make comments in the code: A comment in Python refers to a set of characters which are not executable, these are made in a text line of our program. The comment is represented with the numeral character ( # ). At the moment of programming, the comments can be very useful to be able to explain in detail each action carried out in a program code to people outside the code, or even for ourselves.

## **Our first program: Hello world**

Once we have installed the code editor of our preference and already knowing a little about the Python programming language syntax, we can proceed to write our first program: Hello world.

If you already have experience in programming is common to ask yourself, "Why is "Hello World" always the first program to enter any

programming language? Well, the simple phrase Hello World is characterized by being an extremely simple code, especially at the time of running and can serve as a test to ensure that we have installed our program well and its interpreter. In this way, when working with heavy programs we are going to be sure that everything will work correctly.

From now on all the examples will be based on version 3.x for better understanding.

The syntax that we are going to use for this code will be: `print("Hello World");`

## **Running a program on Linux**

1. Create a directory called projects on your primary user's desktop
2. Create a plain text file with the name: Helloworld.py
3. Type the syntax of your code
4. Run the following command: `Home/projects/Helloworld.py`.
5. Once this is done, your code should be displayed as indicated.

## **To run in windows:**

1. Create a directory called projects in unit C: \

2. Within this directory, we'll need to create a plain text file
3. Write the code syntax
4. Save the file as Helloworld.py (the name may vary according to your preference)
5. Run from the MS-DOS console: C:\Python27\Python C:\Projects\Helloworld.py, or also from the same program Visual Studio, you can do F5.
6. Once this is done, your code should be shown on screen as indicated.

## **Running a program on Mac OsX**

1. Click on File in a new browser window.
2. Create a folder with the name of your preference, in which you will save future projects.
3. Within this folder, we will need to create a new folder called Projects (all programs will be stored here).
4. Click on Applications and then on TextEdit.
5. Select Plain Text.
6. Type the syntax of the program.

7. Click on "save as" from the menu file in TextEdit.
8. Save the file as: Helloworld.py (or the name of your preference) and select the folder already mentioned.
9. Select Applications, then utilities and terminal.
10. Select the folder in which you saved your program.
11. Run cd of the folder.
12. Execute ls and it should show on screen the file Helloworld.py
13. Type the following command: Helloworld.py

Once this is done, your code should be displayed as indicated

# Chapter 2: Variables

## Flow control

What are flow diagrams?


They are tools that are used for any type of programming language, which are used to represent or create the structure of the program or algorithm.



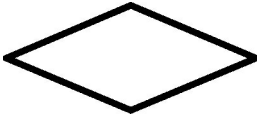

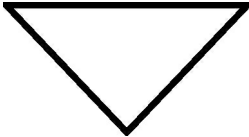

The flow diagrams or also called flowchart, are a way to graphically represent an algorithm (the steps that are executed in the program), facilitating its interpretation to a person.

The creation of the structure of the algorithm or program can be considered the first part of the development of the algorithm and the preparation for the most important step that is coding.

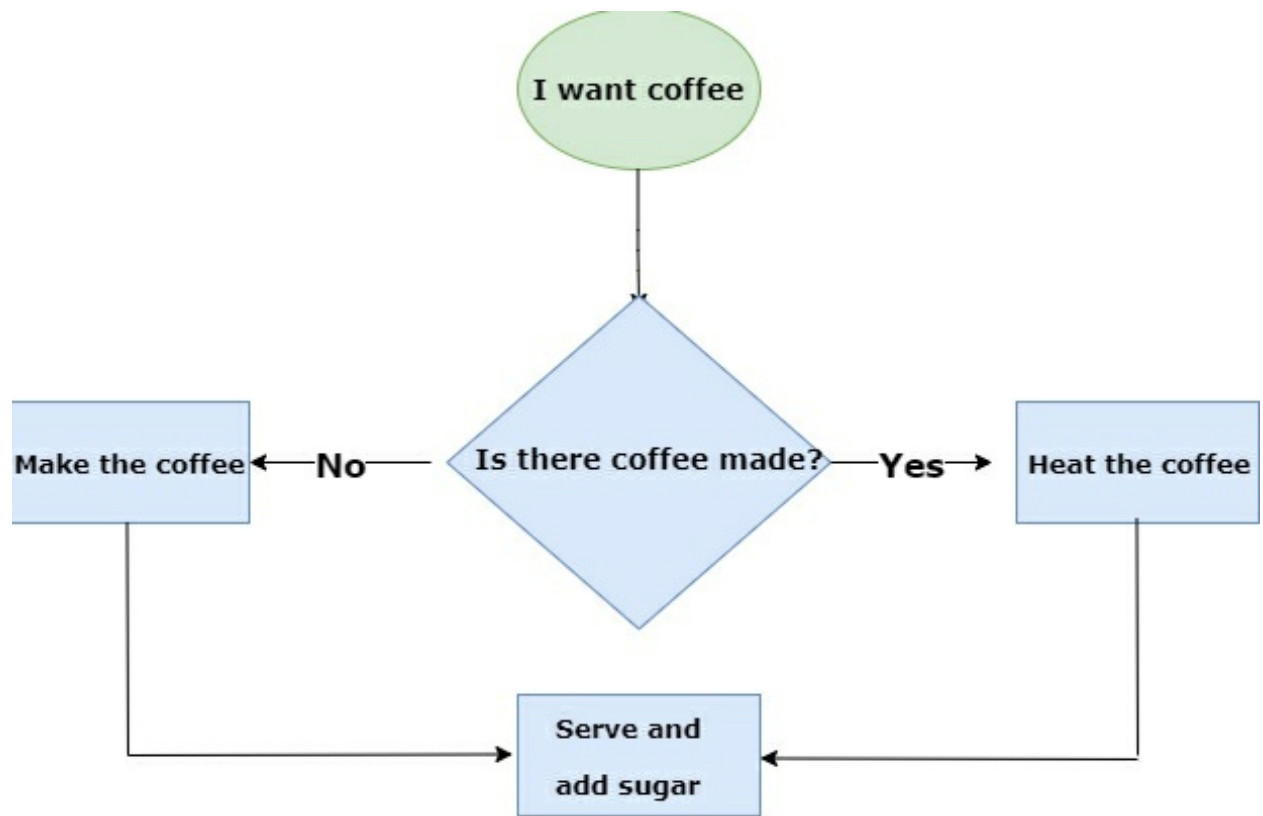
At the time of elaborating a program, it is advisable to make a flowchart so that any person can understand in a simple way the function of the algorithm. Currently, there are a variety of software and online tools that facilitate the elaboration of these diagrams.

Main figures and meaning:

	Start / end: Indicates the starting or ending of the diagram
	Input / Output of data: These are data which are assigned to the input and output variables at the

	beginning and ending of our code.
	Process: This is what executes the order of the operation
	Decision: Indicates a position in the flowchart, this is used for logical expressions. In this case, the sequence is going to split in two cases, a positive and a negative one. This is also used to apply conditionals
	Document: This is used generally to make a document
	Inspection: This is used for some cases where an inspection is required.
	Flowline: This is used to indicate the direction of the diagram

For example:



# Variables

What are the variables in Python?

It is quite sure that we have always heard the concept of variable in mathematics since these are defined as an unknown symbol represented by letters (x, y, z, i, n) which (mostly) store a numerical value.

In this case, when we talk about variables in programming, these represent a space reserved in the memory of our program or computer that can be modified and used multiple times. These variables have a very similar representation and meaning; since they represent a box capable of storing values. Unlike mathematical variables, these can store complex words such as cities, names, passes, simple letters, and ages.

In Python, a variable can be interpreted as a "label" to the data information stored box, and these data can be understood as objects. Python is also able to distinguish between upper and lower case letters (as we previously mentioned this is known as case sensitive), which means that it will not be the same to call a variable Song to a variable called song.

We cannot forget that being Python a programming language that is object-oriented, the data structure of our programs will be based on these same, therefore, the label we put to the variables cannot match the names of the commands or otherwise it will throw us an error.

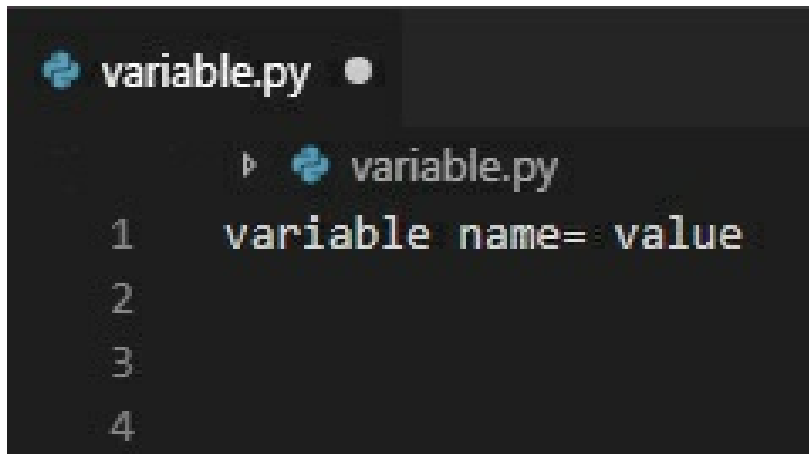
## Declare variables in Python

Python has the advantage of being a dynamic programming language; this means that it is not necessary to specify the type of data with which we will work since its interpreter is able to infer the type of data to use. Unlike C++ that, to declare a variable, it is necessary and obligatory to specify the type of data with which the variable will be stored in the memory so that its compiler



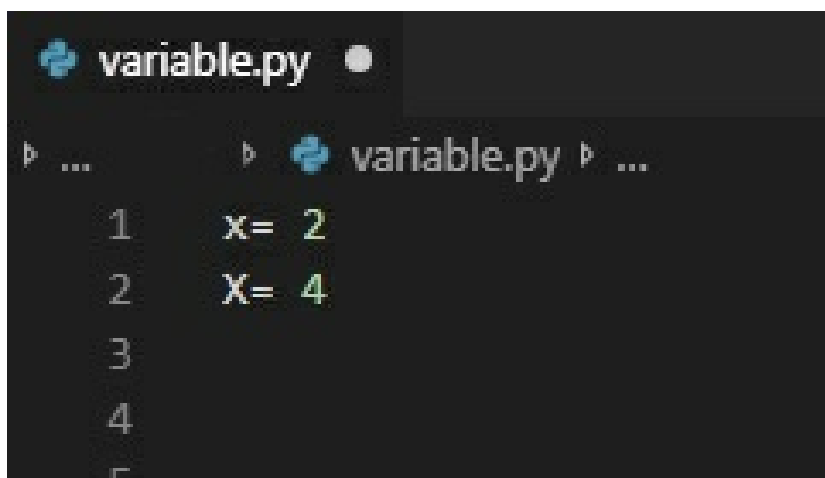
can be able to interpret it.

For example:



```
variable.py
1 variable name= value
2
3
4
```

As we can see, Python uses the symbol "=" to assign the values to the variable, once this is done the variable starts with this value, since there is no possible way to declare a variable without any initial value.



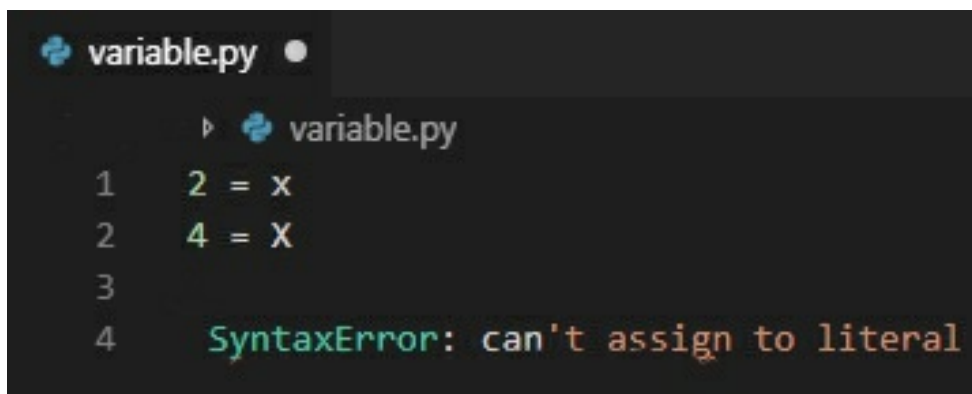
```
variable.py
1 x= 2
2 X= 4
3
4
5
```

We can observe in this example the declaration of two variables of name x with different values, this is totally valid since as we can observe, a variable is written in small letters and another variable is written in capital letters.

It is important to keep in mind that in Python there are operations that, when defined, are not allowed between types (classes) that are not compatible, so

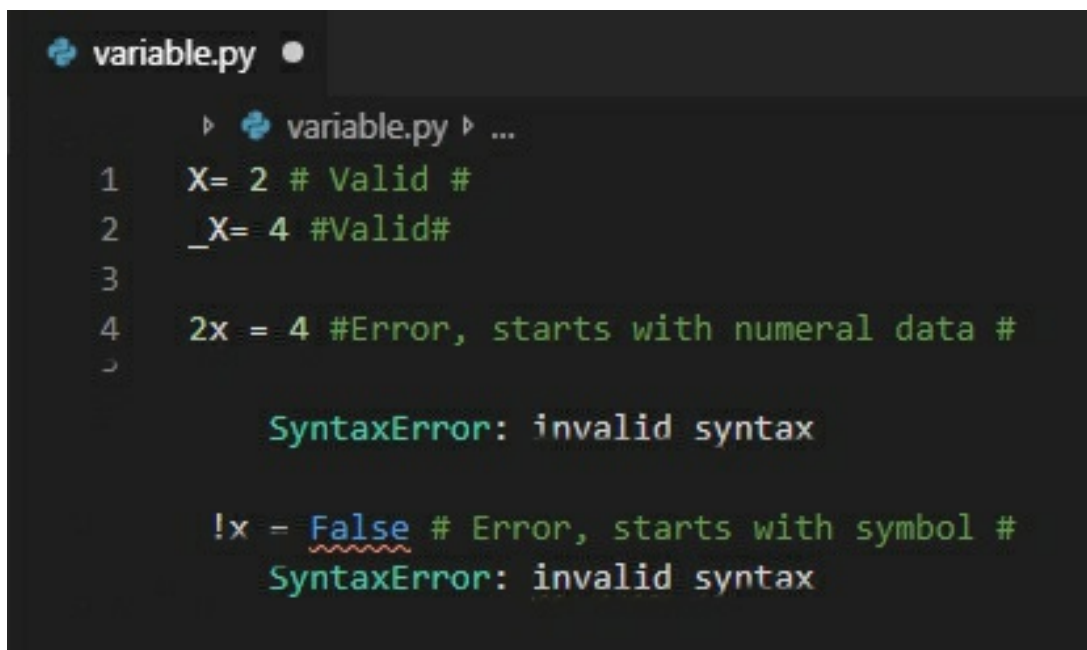
that when each data is identified it becomes an inherited object to the type of data to which it belongs.

To be able to declare a variable it is necessary for it to go from left to right, otherwise, it will result in a syntax error.



```
variable.py
1 2 = x
2 4 = X
3
4 SyntaxError: can't assign to literal
```

It is essential that variable names begin with a letter or underscore (the rest of the name can contain letters, numbers, and underscores).



```
variable.py
1 X= 2 # Valid #
2 _X= 4 #Valid#
3
4 2x = 4 #Error, starts with numeral data #
5
6 SyntaxError: invalid syntax
7
8 !x = False # Error, starts with symbol #
9
10 SyntaxError: invalid syntax
```

It is also possible to assign multiple values to multiple variables on the same line, as long as there are the same number of arguments on both the left and right.

```

1  a, b, c = 2, 4, 6
2

```

## Data Types

- Integers: Integer data in Python can identify integers of either decimal, binary, hexadecimal, or octal type.

There are two ways to declare a variable as integer: An int is placed prior to the variable name as follows:

```

variable.py x
+
1  int Number = 4
2

```

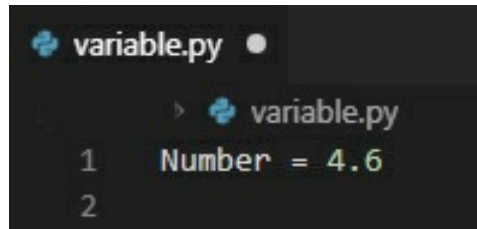
The other way is the most common, in which we only write the name of the variable to be declared.

```

variable.py ●
1  Number = 4
2

```

- Float: The data of the type float are in charge of covering all the set of real numbers ex: 3.14, 21, -85.6. When we perform an operation with float type data, it will not always give us a result with an exact number, many times it can be an approximation and its declaration is very similar to the declaration of variables of the integer type.



```
variable.py
> variable.py
1 Number = 4.6
2
```

- Complex: The data of the complex type refer to the set of operations with complex numbers, these are expressed as data of the type float separated by the operand symbol, the first number is going to present to the real number and its imaginary component is going to be identified being accompanied by a letter j. At the moment of declaring a variable of the complex type it must be declared in the following way:



```
variable.py
> variable.py ▶ ...
1 vari = complex(4+14j)
2 print(vari)
3
```

- String: Data of the string type refers to a sequence or string of characters that are enclosed in apostrophes or quotation marks.

String types:

\": double quotation mark.

\': single quotation mark.

\n: Line break.

\t: Tab horizontally.

Example:



```
variable.py •
variable.py ▸ ...
1  string= "Hello world"
2  string2= "This is my String example"
3  print(string)
4  print(string2)
```

- Bool: Boolean data consists of only two (2) digits, which evaluate logical expressions. This is very important for future chapters because it will allow us to understand conditionals or cycles.

If a logical expression is true, its numerical value will be 1.

If a logical expression is false, its numerical value will be 0.

- Lists: List type data allows the program to store within it, certain items of any different data type, as well as being able to have repeated items. These same are written with curly brackets.

```
variable.py •
variable.py ▸ ...
1  a = 2
2  b = 4
3  string = "Hello people"
4  bool= True
5
6  list=[a, b, string, bool, 3, False, "good luck"]
7
8  print(list)
```

- Tuples: Tuples type data are able to store several items within it, this type of data can be similar to lists but differs in the following things: Their declaration is made with a parenthesis (), unlike the lists that are declared with square brackets []; when we declare Tuples, these same are immutable, unlike the lists that when we declare them, can be changed, and finally because they are immutable, their search for data is much more effective than in a list.

His statement is as follows:

```
variable.py •
variable.py ▸ ...
1  a = 2
2  b = 4
3  string = "Tuple"
4  bool= True
5
6  Tup=(a, b, string, bool)
7
8  print(Tup)
```

- Set: This type of data in Python is based on a data structure, which can consist of multiple elements whose order in the set is not defined. Sets are able to add, remove and iterate elements of a set, as well as perform common operations such as differentiate, verify if an element belongs to the set, differentiate and intersect.

To define a set we only need to name the function set (). If it has a list, a tuple or a string, it will return a compound of the elements. Example:



```
variable.py x
  ▶ variable.py ▶ ...
1  A = {5, 3, 2}
2  A = set('PYTHON')
3  print(A)
```

- Dictionaries: This type of data is defined as a structure that has certain special characteristics that allow us to store any integer value, list, string, and even functions. Dictionaries allow us to identify each element by a key.

It is important to keep in mind that when working with dictionaries the 'keys' cannot be repeated data, likewise, it is not possible to access the keys through their associated value. It is also important to know that these do not meet a specific order, but that this type of data is guided by the keys.

In order to define a dictionary, we enclose with curly brackets {} the list of values to be entered. Each key pair is separated with commas and the key together with the value is separated by a colon. For example:

```

variable.py •
> variable.py ▶ ...
1 user = {'name' : 'John', 'Age' : 20, 'Knowledge': ['Python programming','C++ programming','JavaScript']}
2
3 print (user['name'])
4 print (user['Age'])
5 print (user['Knowledge'])

```

That will print:

```

John
20
['Python programming', 'C++ programming', 'JavaScript']

```

Here we can see that we have created the dictionary and also the program shows us that we have accessed each key separately.

## Dictionary methods:

**get():** This method receives a key as a parameter and returns its value. If it doesn't find a value, it returns an object of type none.

For example:

```

variable.py •
> variable.py ▶ ...
1 user={'name' : 'John', 'age' : 20, 'knowledge': ['Python programming','C++ programming','JavaScript'] }
2 print(user.get('name'))
3

```

In this case, it will return the value name, which in this case will be John.

**Item():** This type of method is in charge of returning a list of tuples, in which each one is composed of two elements in which the first element will be the key and the second element will be its value. For example:



```
variable.py x
variable.py ▸ ...
1 user={'name' : 'John', 'age' : 20, 'knowledge': ['Python programming','C++ programming','JavaScript'] }
2 print(user.items())
```

**Keys():** This type of method only returns the keys of our dictionary. Example:

```
variable.py x
variable.py ▸ ...
1 user={'name' : 'John', 'age' : 20, 'knowledge': ['Python programming','C++ programming','JavaScript'] }
2 print(user.keys())
```

**Values():** This type of method only returns the values of their respective keys from our dictionary.

```
variable.py x
variable.py ▸ ...
1 user={'name' : 'John', 'age' : 20, 'knowledge': ['Python programming','C++ programming','JavaScript'] }
2 print(user.values())
```

**Clear():** This method eliminates all the items and leaves our dictionary empty. For example:

```
variable.py x
variable.py ▸ ...
1 user={'name' : 'John', 'age' : 20, 'knowledge': ['Python programming','C++ programming','JavaScript'] }
2 print(user.clear())
```

**Copy():** This method returns a copy of the original dictionary. For example:

```
variable.py x
variable.py ▸ ...
1 user={'name' : 'John', 'age' : 20, 'knowledge': ['Python programming','C++ programming','JavaScript'] }
2 print(user.copy())
```

## Redeclaring variables in Python:

A great advantage that Python has is its ability to allow redeclaring variables in a simple way, from changing their value to changing the type of variable without complications. For example:

```
variable.py •  
  ▶ variable.py ▶ ...  
1  a=4  
2  print(a)  
3  a=8  
4  print(a)  
5  a=True  
6  print(a)  
7  a= "Julia"  
8  print(a)  
9
```

In the last example, we can observe that the first declaration of the variable "a" is assigned the value 4, which is an integer, then the variable is redeclared with the value 8, therefore, at that time the variable is integer, then we have redeclared the variable again and we have converted it to a Boolean value, since we have assigned it the value True. Finally, we have assigned to the variable a string which we can see as a name "Julia" so at that time the variable is of string type.

## Concatenate strings

To concatenate character strings we will only need to use the addition operand (+). It is important to note that you must specifically and explicitly mark the place where we want to leave the space blank.

```
variable.py ●  
▶ variable.py ▶ ...  
1 a= "Hello world"  
2 b=" this is an example"  
3 c= a + b  
4 print(c)  
5
```

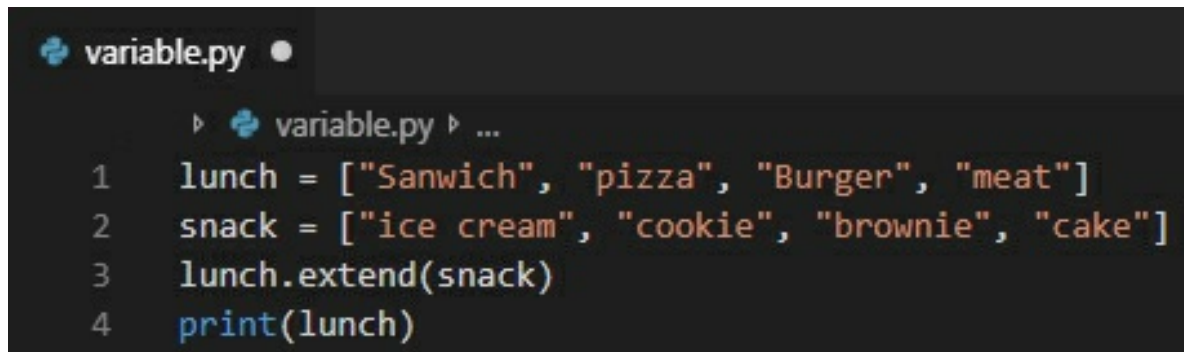
As we can see in the last example, the variable "a" was created, which contained the value "Hello world", then the variable "b" was created, which contained the value "this is an example" and later the final variable "c" was created, this last one was in charge of carrying out the concatenation of "a" and "b".

The concatenation of variables can also be done with integer and boolean values, but to do this you must convert these variables into strings beforehand. How do you do this? Well, it's very simple, we do it calling the function `str()`. For example:

```
variable.py ✕  
▶ variable.py ▶ ...  
1 string= "class of "  
2 date= 2019  
3 date=str(date)  
4 final=string + date  
5 print(final)  
6
```

As we could see in the example, we have created a string variable that contains the value "class of ", and then the integer type date variable is created and contains the value "2019". Then we redeclare our variable date to string type with the function str().

Another very common example is concatenating lists, this we do through the function extend(), for example:



```
variable.py
▶ variable.py ▶ ...
1 lunch = ["Sanwich", "pizza", "Burger", "meat"]
2 snack = ["ice cream", "cookie", "brownie", "cake"]
3 lunch.extend(snack)
4 print(lunch)
```

We can see in the previous example that a list has been created with some lunch options; then another list has been created with some snack options and finally, the command lunch.extend(snack) is created concatenating list number 1 with list number 2.

## Global Variables

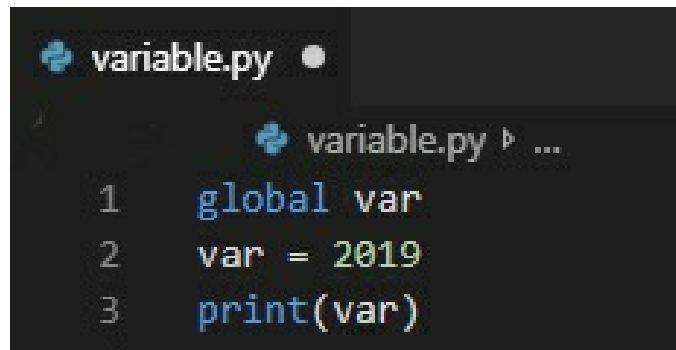
Global variables are those used throughout the program; once declared, they may be used as a main function or any other type of function.

This type of variable can be modified in any part of the program, this could seem an advantage, but it could also cause confusion both for the programmer or another external person who is going to read the program. Another point that could be considered negative with global variables is that they can take up more space than common ones because they cannot be destroyed at the end of running the function, on the other hand, this one does not allow the code to be reusable; this makes Python programming language

one of the most attractive.

In general terms, it is considered a bad practice to work with global variables, but it is never too much to have complete knowledge. Next, we will see how to declare a global variable.

For this it is necessary to use the global command:



```
variable.py
1  global var
2  var = 2019
3  print(var)
```

As we could see in the last example, calling or declaring a global variable is not very complicated. We could say that it is similar to what we have seen to declare variables; the only difference is that from now on the variable "var" is going to have a global character so that any function is going to be able to access it in a simple way.

## Local variables

Local variables are those that are only used in one function and are deleted from memory when their execution is completed. Unlike global variables, local variables allow us to save quantities of lines of codes, making modular programming much more agile and easy, thus allowing the reuse of the code, which makes Python one of the most striking programming languages.

The main advantage of using local variables in a Python program is

that it facilitates the reading of the code, making it simple to understand; global variables allow any error to be fixed more effectively and easily. Having reduced lines of code, it is very unlikely that confusion will be generated at the time of interpreting it.

It is considered a good practice to use local variables at the moment of programming since nowadays it is intended to obtain much simpler codes to interpret by users who do not have so much experience in programming.

To better understand this, we will make an example that explains in a clear way the use of these variables at the moment of programming.

Example: We are going to create a problem in which it must be responsible for taking the following data from a person:

1. Name and Lastname
2. Age
3. Country of origin



```
variable.py x
> variable.py ▸ ...
1 full_name = input("Full name: ")
2 age = input("Age: ")
3 country_origin = input("country of origin: ")
4 print("Full name"+full_name + "\n" + "Age"+ age + "\n"+"Country of origin" + country_origin)
5
```

We can observe that the syntax focuses more than everything on the input() command, what does this mean? This is only the function that allows a user-program interaction to be possible. In this way, the variables "full\_name", "age" and "country\_origin" will have the value that the user introduces at the moment to the console.

```
Full name: Python programmer  
Age: 100  
country of origin: Worldwide
```

# Chapter 3: Operators

Operators are mathematical symbols that carry out a specific operation between operands, operators can receive variable operands. Operands are those arguments that operators receive in order to perform their functions. So we can conclude that operators are those special symbols that are capable of performing logical and arithmetic operations.

Types of operators:

- Logic operators.
  - Arithmetic operators.
  - Comparison operators.
  - Assignment operators.
  - Special operators.
- Logical or conditional operators: This type of operators are those that are commonly used to group, deny and exclude some expressions of our code.

1. Operator not: This type of operator is the one in charge of negating or returning a value opposite to the Boolean value.

not True=False.

not False=True.

2. Operator Or: This type of operator is the one that evaluates the



values on the right side and the values on the left side in order to finally return a true value if at least one condition is met.

False or True = True

True or false = True

True or True = True

False or False = False

3. Operator And: This type of operator is responsible for assessing whether the conditions between the value on the left side and the value on the right side are met correctly:

True and False = False

True and True = True

False and True = False

False and False = False

- Comparison operators: These types of operators are those that we use to compare (as its name says) some values stored in the program so that later this at the time of compiling we can return a value of the True / False type as a result of fulfilling a condition.

1. Operator !=: This type of operator is in charge of evaluating if these stored values are different and depending on the result of the analysis, this will give us a True/False. E.g.

$20 \neq 20$  The result is going to be False

$14 \neq 15$  The result will be True

2. Operator  $==$ : This type of operator is in charge of evaluating if these values are the same for different types of data and depending on the result obtained in its analysis, its result will give us a True/False. E.g.

$19 == 19$  The result will be True

$10 == 5$  The result will be False

3. Operator  $>$ : This type of operator is in charge of evaluating whether the value entered on the left side has a position greater than that of the value positioned on the right side. E.g.

$30 > 25$  The result will be True

$9 > 28$  The result will be False

4. Operator  $<$ : This type of operator is the one that will evaluate if the value entered on the left side has a lower position than the value positioned on the right side. E.g.

$26 < 9$  Result will be False

$14 < 22$  The result will be True

5. Operator  $>=$ : This type of operator is in charge of evaluating whether the value entered on the left side has a position greater

than or equal to that of the value positioned on the right side.  
E.g.

20 > 14 The result will be True

10 > 26 The result will be False

10 >= 10 The Result will be True

6. Operator <=: This type of operator is the one that will evaluate if the value entered on the left side has a position less than or equal to the value positioned on the right side. E.g.

20 < 11 The result will be False

16 < 25 The result will be True

15 <= 15 The result will be True

- Assignment operators: These types of operators are those that are used in the program to assign (as its name says) a value to a variable, in this case, these operators will be followed by a symbol of equality ( = )

1. Operator Equality ( = ): This type of operator is considered the main one and will always be positioned on the left side of the variable. E.g.

> A = 10 → The value of A will be 10

2. Operator Sum - equality ( += ) This type of operator is responsible for adding to the variable on the left side, with the value located on the right side.  
E.g.

> A = 10; A += 8 → A = 18

It would be equivalent to expressing:  $A=10; A + 8 \rightarrow A=18$

3. Operator subtracts - equality ( -= ) This type of operator is the one that subtracts from the variable on the left side, with the value located on the right side. E.g.

>  $A=10; A -= 8 \rightarrow A=2$

It would be equivalent to expressing:  $A=10; A - 8 \rightarrow A=2$

4. Operator Rest - equality ( %= ) This type of operator is responsible for returning the rest of the division on the left side, to the value located on the right side.

>  $A=10; A \%= 8 \rightarrow A=2$

It would be equivalent to expressing  $A=10; A \% 8 \rightarrow A=2$

5. Integer Operator - equality ( //= ) This type of operator is responsible for calculating the integer division of the variable on the left side, with the value located on the right side.

>  $A=10; A //= 8 \rightarrow A=1$

It would be equivalent to expressing  $A=10; A // 8 \rightarrow A=1$

6. Operator Product - equality ( \*= ) This type of operator is responsible for multiplying the variable on the left side, with the value located on the right side. E.g.

>  $A=10; A *= 8 \rightarrow A=80$

It would be equivalent to expressing:  $A=10; A * 8 \rightarrow A=80$

7. Operator Division - equality ( /= ) This type of operator is in charge of dividing the variable on the left side, with the value located on the right side.

E.g.

>A= 10; A /= 8 → A= 1,25

It would be equivalent to expressing A= 10; A \* 8 → A= 1,25

8. Exponent Operator - equality ( \*\*= ) This type of operator is responsible for calculating the exponent of the variable on the left side, with the value located on the right side. E.g.

>A= 10; A \*\*= 8 → A = 100000000

It would be equivalent to expressing A= 10; A \*\* 8 → A= 100000000

- Special Operators: These types of operators are commonly used in program loops, to check for repeated variables and even to know if an element is stored within others.

1. Operator In: This operator will return a 'True' if an element is stored inside another. E.g.

A= [80, 40] 80 in A

The result that is going to return will be of the true type because the value 80 is positioned in A

2. Operator Is: This type of operator will return a True if its values stored in the variables are the same. E.g.

X= 80; Y= 80. → X is Y

The result to be returned will be of the True type because both variables contain the same stored value.

3. Operator Not in: This type of operator will return a True if an element is

not stored inside another element. E.g.

A = [80, 40] 40 not in A.

The result that is going to return will be of the False type because the value 40 is positioned in A.

4. Operator Not is: This type of operator will return a True if the values stored in the variables are not equal. E.g.

X = 80; Y = 40. → X not is Y

The result that is going to return will be of the True type because both variables contain stored different values, therefore, they are different.

- Arithmetic Operators: These types of operators are those used to perform simple mathematical operations.

1. Sum Operator ( + ): This type of operator will add values of the numerical type. E.g.

$$40 + 40 = 80$$

2. Operator subtracts ( - ): This type of operator will subtract values from the numerical type. E.g.

$$40 - 40 = 0$$

3. Operator multiplication ( \* ): This type of operator will multiply numerical values. E.g.

$$40 * 40 = 1600$$

4. Operator division ( / ): This type of operator will be responsible

for dividing numerical type values. E.g.

$$10 / 2 = 5$$

5. Exponent operator ( \*\* ): This type of operator will calculate the exponent of a stored value between values with numerical data type. E.g.

$$4^{**} 2 = 16$$

6. Integer Division Operator ( // ): This type of operator is responsible for calculating the integer division of a stored value with numeric data type in which only the integer part will return. E.g.

$$5 // 2 = 2$$

Note: It is important to note that, when working with two operands of the integer type, the program will assume that you want the variable to yield a result of the integer type. E.g.

If we operate  $A = 7 // 2$  = Our result will be 3.

If you want to get the decimals as in the first example, just add at least one decimal value to either of the two operands. E.g.

$$G = 7.0 / 2 = 3.5$$

7. Operator Module: This type of operator is responsible for returning the rest of the division between the two operands. Ex,=.

$$7 \% 2 = 1. \text{ The division module is } 1$$

The order of precedence or priority of arithmetic operators is as follows:

1. Exponent ( \*\* )
2. Multiplication ( \* ), Division ( / ), Whole Division ( // ), Module ( % )

In line 2 we can see that the rest of the operators are grouped together, this means that they all have the same order of priority, but at the time of operating they will be resolved by that order of precedence.

Example:

When operating:  $8*10/2$

This means that the operation is to be carried out as follows:

$8*10 = 80 / 2 = 40$ . The result of our operation is 40.

On the other hand, this order of precedence can be manipulated by using parentheses ().

Example:

When operating  $80*(10/2)$

This means that the operation is to be carried out as follows:

$10/2 = 5 * 4 = 20$ .

Let's make two small examples to work with operators, let's calculate the area of a rectangle and the other is to see if the key is correct.

First example, area of the rectangle:

```
operators.py x
1  b=int(input("Please enter the base: "))
2  h=int(input("Please enter the height: "))
3  print("The area is "+str(b*h))
4
```



In this example, the first thing we do is to declare the variables, the first is variable `b`, which is related to the base, which goes through several stages, but we put it in a single line to save space.

To explain it better, the first thing we can observe is that there is an input in the declaration of both `b` and `h`, which is an input type, so that it is going to be saved as a string, for this reason, we can also observe the `int` function, which will turn that string into an integer, to be able to do operations on them. Do you know why is that?

Because it is impossible to add two strings, since it is very different to add  $1 + 1$  than `"1" + "1"`, because the first is a sum of integers, and its result will be equal to 2, but the second we do not know, because it is a sum of ASCII characters. And well, as you can see, the same thing is done with the variable `h`, therefore, `b` and `h` are two integers entered by the user.

The next action is to print in screen the following string `"The area is"` concatenated with the string related to the multiplication of the base and the height, because it is not possible to concatenate a string with an integer, for this reason, the function `str()` is used.

As you can see, this is a very basic example, and here comes a question, what happens if you enter a negative value? If, for example, you enter -5 and 2, the value returned will be -10, and this is a big mistake since there are no negative areas, therefore, it is an error that our program has. The errors can be solved by using conditionals, or also with the handling of exceptions since they will take into account these cases.

Second example, key verification:

 operators.py

```
1 password="12345"  
2 passuser=input("Please enter the password here: ")  
3 print("User "+str(password==passuser))  
4
```

The first thing is that we define the password variable as a string "12345", then, the passuser variable is declared, which is related to the input function, it will show on the screen "Please enter the password here: ", the same will make in passuser is a string.

Finally, it will be printed in screen if the key is correct or not, for it, will be printed in screen "User" and this one will concatenate with the result of comparing if password is strictly equal to passuser, but in order for this to be concatenated, it will be necessary to convert this comparison into a string, because it is necessary to delimit that when some comparison is made, the return is a boolean, and it cannot be concatenated with a string, unless it is converted, due to that, we made use of the function str().

## Conditionals

With the help of logical operators, and well, of logic in general, we will base ourselves in order to be able to use the instructions, because they will allow us to make more complex programs, since they allow us to set conditions, like what? Well, for example:

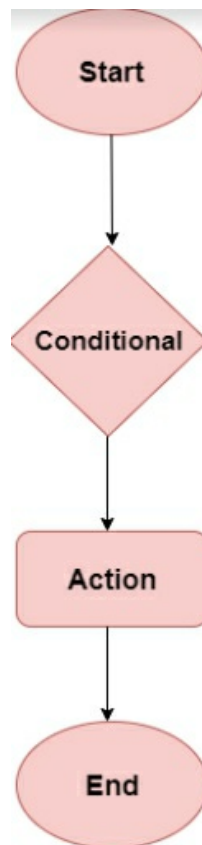
If it rains today, I take my sweater; if it doesn't rain, I don't take it.

In the same way, conditionals work, since an action is going to be carried out if a certain circumstance is fulfilled, but if the expected does not happen, something else will happen.

Among the conditionals, we will find the if, the else, and the elif; there are also the cases in which we use exceptions, which are used to prevent the program from collapsing.

- if statement: This is a simple conditional, if a certain circumstance happens, an action will be taken, otherwise nothing will happen and the usual or expected flow will continue. This can be used for simple programs such as access by age, How? Well, in case the client is not old enough, it will not let him get in.

The flowchart of the if conditional is as follows:



---

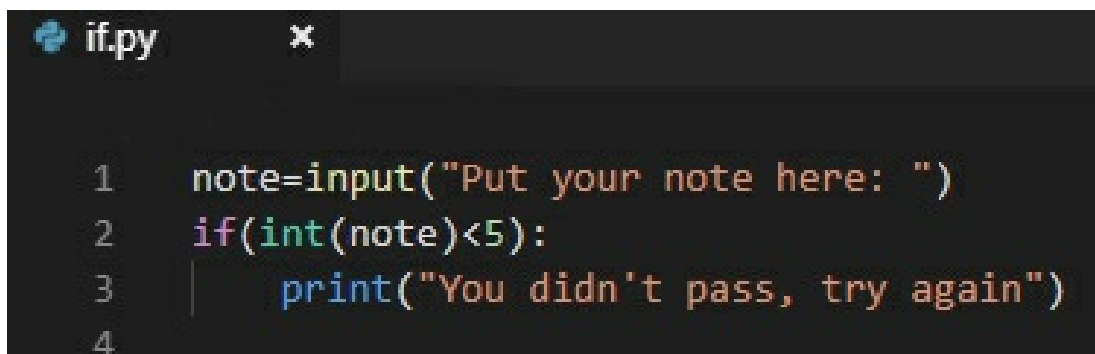
Now, the syntax of If in Python is as follows:

- If + condition: Then inside this block, with the required indentation, the following commands will be executed, obviously, if the condition is met.

Now some important things that have to be remembered when making the if blocks, in terms of syntax:

- The first line is always the if + condition, followed by a colon ( : ), since this way it is clear that a block is being started.
- The following lines indicate the instructions that will be fulfilled, but of course, obviously, they will occur in case the condition is true.
- Finally, it is the indentation that the block of instructions must have since in case these same are not placed correctly, the program will not understand what you specifically want and it will happen that it is not going to do what you requested or simply close the program.

A clearer example of the syntax is this, which will show whether a student passed an exam or not:



```
1  note=input("Put your note here: ")
2  if(int(note)<5):
3      print("You didn't pass, try again")
4
```

As we can see here, a note variable was created, which is related to the input function, awaiting the note that the user obtained, this variable is of the string type.

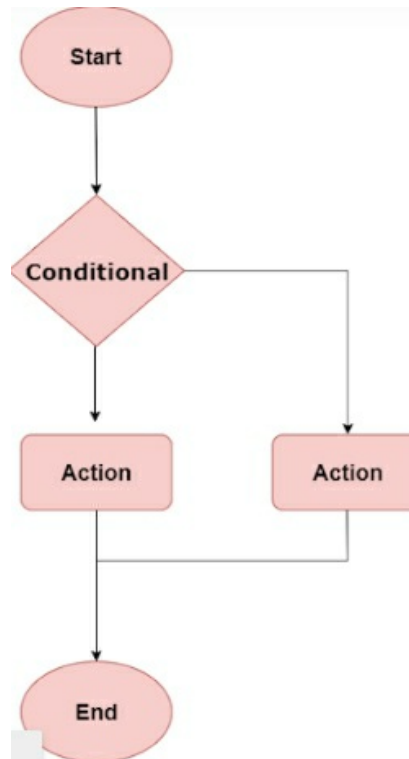
Subsequently, we enter the conditional part, specifically the if, and the condition to compare is that, if the note that the user obtained is lower than

five, then a screen will print that the user did not pass, and needs to try again. As you can see, at the part of the if condition, the `int()` function was used, which is needed because the `note` variable is a string, and a comparison of a number with a string cannot be made, therefore it is necessary to change the type of string variable to integer, in order to make the corresponding comparison.

But what if the condition is false? Can you do another action? Well, you do, since there is another statement, and it is the `else`, which is used when the condition of the `if` is false and you need to do another action, then go to the usual flow, if you want to see this statement better explained, read the following paragraphs, which are responsible for explaining the statement.

- `else + condition`: The `else` condition is used when the `if` condition is false, what does this mean? This is nothing more than if the clause of the condition is not fulfilled, the program will close automatically; so that this does not happen we make use of the `else` instruction which will tell the program to perform another action.

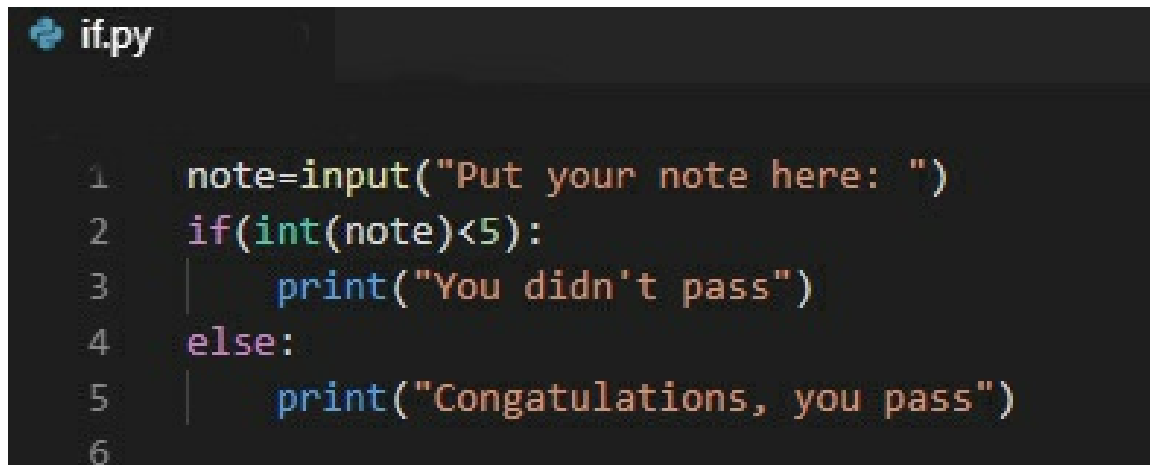
The flowchart of the `else` conditional is the following:



We can observe that the syntax of the conditional else is very similar to the syntax of the conditional if, only that, in this case, the conditional does not have to be placed, but it is of fundamental importance to maintain a correct indentation.

To observe in detail the programming of the else conditional, we will make a test program, in this way we will be able to see clearly the difference between conditionals.

It will be a modification to the past program, with the objective of showing how powerful the use of conditionals can be.

A screenshot of a code editor window titled 'if.py'. The code is written in Python and uses syntax highlighting. It consists of six lines: line 1 is 'note=input("Put your note here: ")', line 2 is 'if(int(note)<5):', line 3 is ' print("You didn't pass")', line 4 is 'else:', line 5 is ' print("Congatulations, you pass")', and line 6 is empty. The background is dark, and the text is in various colors (blue, green, yellow, red) to highlight different parts of the code.

```
1  note=input("Put your note here: ")
2  if(int(note)<5):
3      print("You didn't pass")
4  else:
5      print("Congatulations, you pass")
6
```

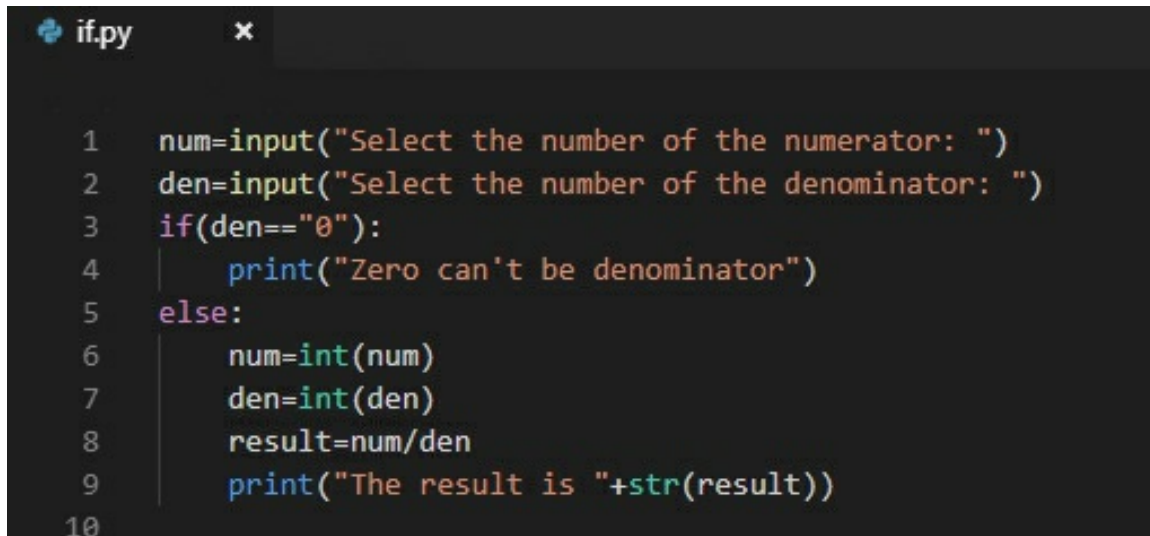
In this example, we can see that the note variable was created, which is an entry that the user will choose, well, in this case, he will put his note, so that then the program will say if his note was enough to pass or not, so, to make clear to the user that he has to enter his note, the following string "Put your note here" will be printed on the screen, so the user knows that he has to put his note in the program.

After this, the conditional block was placed, in which the condition means that if the transformation to integer of the note entered by the user is less than five, "You didn't pass" will be printed on the screen, and then the program will end, since the block of the else will not be entered, because the condition is true. But if the condition is not true, it will be passed to else, which will print on the screen the next string "Congratulations, you passed", in order to show users that with their note they passed or not the exam.

As you could have observed, the use of if and else, is very useful, we would say that fundamental, because, thanks to it, you can make the program able to have different results and not have a single simple flow, because as you can guess, that type of programs that do not have logical bifurcations, are not widely used.

Another example that we can see is the division, with the same, we

can see another very important utility of conditionals because the denominator cannot be equal to zero, because the division between zero is not defined and would be a mathematical error.



```
1 num=input("Select the number of the numerator: ")
2 den=input("Select the number of the denominator: ")
3 if(den=="0"):
4     print("Zero can't be denominator")
5 else:
6     num=int(num)
7     den=int(den)
8     result=num/den
9     print("The result is "+str(result))
10
```

Here we can see the example of the division since we have the problem previously explained.

The first thing is to create the variable num, it will be related to the numerator of the division, it will be declared next to an input function, so that the user enters the value he wants. Then the same will be done with the den variable, which is related to the denominator of the division.

Then we will enter the block of conditionals, the condition we will look for is that the variable den is equal to string "0", to know if, at the time of making the division, it can be or not. If the condition is true, the following string "Zero can't be denominator" will be printed on the screen, in order to show the user that the number he put as denominator does not meet the mathematical requirements. But, in the case that the condition is different from zero, the division can be done, therefore, we enter inside the else block; the first thing we do is to convert into integers the variable num and the



variable den, but what is the objective of doing this in this part of the code? Well, to be able to do mathematical operations, both with num and den will have to be integers, but it is done in the part of the else, as a part of code optimization, because in the case that the denominator had been zero, time would have been spent on unnecessary instructions, because no operation was going to be performed, since the division between zero is not allowed, as you already know. At this moment, you will say that there is no difference between doing it here or not, but there is, imagine that you have to do that a million times, that would generate a big computational expense in something that is not going to be used, that is why it is always important to make this type of reasoning, in such a way that it is trying to make the program as optimal as possible.

The next action is to make the division between the numerator and the denominator, and this value will be stored in the result variable, to finally print the obtained result on screen.

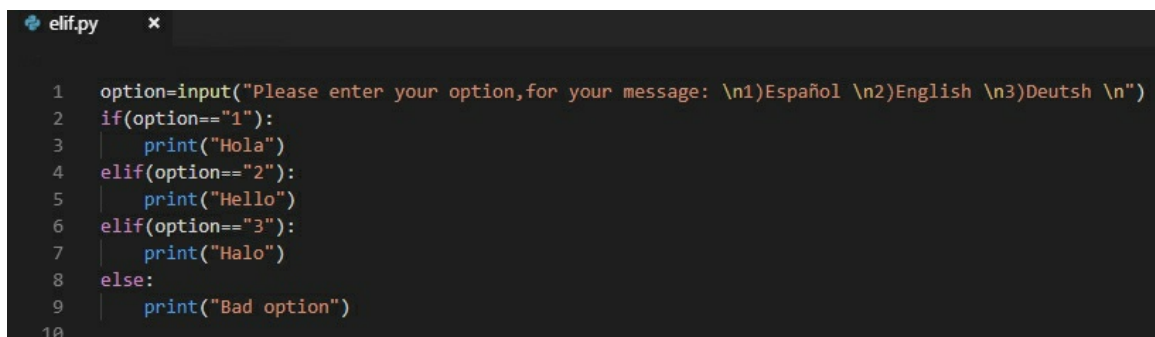
If you are a little bit of a programmer, or already know how to program in C or Arduino, to say some languages, you will be waiting, in these explanations of the conditional sentences, the explanation of how the switch is used here, because in Python these are not found, in Python it is used the elif is used and its explanation can be seen below.

- elif + condition: We use the elif conditional as a faster and more effective way to join an else with elif for when there is more than one condition. For example: in other programming languages, it is very common to use the switch() conditional for multiple conditions. In the case of Python, this is replaced by elif(), this is nothing more than

placing an additional conditional on the else to obtain multiple cases.

This is commonly used when you have multiple conditions, which have many different ways to perform.

Now, we will see an example to be able to understand in a very clear way how this works, and in this way, we will enter the conditionals.



```
1 option=input("Please enter your option,for your message: \n1)Español \n2)English \n3)Deutsh \n")
2 if(option=="1"):
3     print("Hola")
4 elif(option=="2"):
5     print("Hello")
6 elif(option=="3"):
7     print("Halo")
8 else:
9     print("Bad option")
10
```

In the elif example, we can see that the option variable has been created, which is related to the option that the user wants to enter into his program, as can be seen in the code, the options are 1 for the answer to be in Spanish, 2 for the answer to be in English, and finally 3 for the answer of the program to be in German.

When entering the conditional block, the first thing we see is the if, which will have the condition that the variable option is the same strict as the string "1", if it is true, the string "Hello" will be shown on the screen; then, if this option is not fulfilled, it will go to the first elif, which will have a different condition, in this case is the one that says that the variable option is the same strict as the string "2", if this option is true, then it will show the message on screen, which says "Hello"; the last elif has the condition which indicates that the variable option has to be the same strict as the string "3", if it is true, it will proceed to send a message in German that says the following:

"Halo". But if no case is fulfilled it will go to the else block, and this indicates that it will print in the console, a message that says "Bad option".

Therefore, we could see that the program has three options, and each one is a message that will be shown to the user saying hello in different languages, such as Spanish, German and English.

As we could see the examples of conditionals, we could see the great usefulness that they have in the programming, since they allow us to place an accumulation of options to our programs, and that they respond in a different way, depending on the situation.

But these conditionals are not the only ones that we can use for special conditions, another very useful tool, which is used a lot in programming, are the exceptions, as these catch any error, for the program to run in a correct way, moreover, in the example of division by zero you can use this tool, but not only for division by zero, but many more times, the only thing you need is the tools that you will see below.

## **Exception handling:**

When we program, it is very frequent that we find errors during the execution of our programs. Two very common types of errors we might encounter on our way are syntax errors and exceptions. As we have already seen, syntax errors are those that occur when we enter code incorrectly.

In the case of exceptions, the syntax errors presented are different. How is this? Well, they happen while during the execution of a program something unexpected happens. For example, let's suppose a program in which we ask a user to enter a number to fill in a requirement. Now imagine that when the user is going to enter the data, he writes a string instead of a number, the program will automatically show a `TypeError` error.

When we don't handle exceptions properly, our program will close immediately because the interpreter won't know what to do in a special case like that.

Returning to the example shown above, we know that as long as we enter an integer value as an input value, our program will work correctly. However, if we enter a string the other type of error will be an exception to the `ValueError` type.

Some of the most common exceptions are:

`NameError`: The type of exception `NameError`, is the one that occurs when a program is not able to locate a global or local name. When the program is going to show us that it has not been possible to locate, it will include the wrong name in the message.

`TypeError`: The type of exception `TypeError`, is the one that occurs when an inappropriate object passes through the function as its argument. When the program is going to show us the type of error that has been presented, it will include in detail the correct ways to work with the arguments.

`ValueError`: The type of exception `ValueError`, is the one that occurs when an argument of the function contains its correct defined types, but its value is not adequate.

`NotImplementedError`: The type of exception `NotImplementedError`, is the one that occurs when an object that supports an operation has not been implemented. These types of errors are considered not to be used when a function supports an input argument, the most appropriate would be to use an exception of the `TypeError` type.

`ZeroDivisionError`: The `ZeroDivisionError` type of exception is one

that occurs when a zero type of data is provided to the argument (such as a denominator) in a division operation or module operation.

**FileNotFoundError:** The `FileNotFoundError` exception type, is the one that occurs when a dictionary or file that has been requested is not existing in the program.

**Handling exceptions:** It is known that in each programming language there are certain quantities of reversed words, which make it easier for us to handle any exception that may arise when programming. In this way, we can take quick action to prevent the program from being interrupted.

In Python, when we handle exceptions we perform operations called "blocks", these blocks will be mostly used with the `try`, `except` & `finally` sentences.

So how does this work?

Raising the exception is going to happen in the following way: in the `try` block, you will find all the code, which could be raised with an exception. (It is known the term `raise` for programmers as the action of generating an exception.)

Once this is done, the exception block will be located, this is the one that will be in charge of enclosing the exception to obtain an opportunity to process it by sending a specific sample message.

Lastly, we have the `finally` block, which we are going to use to perform an action. This will be done no matter if the exception has been made or not, this way the block will be executed regardless of the previous conditions.

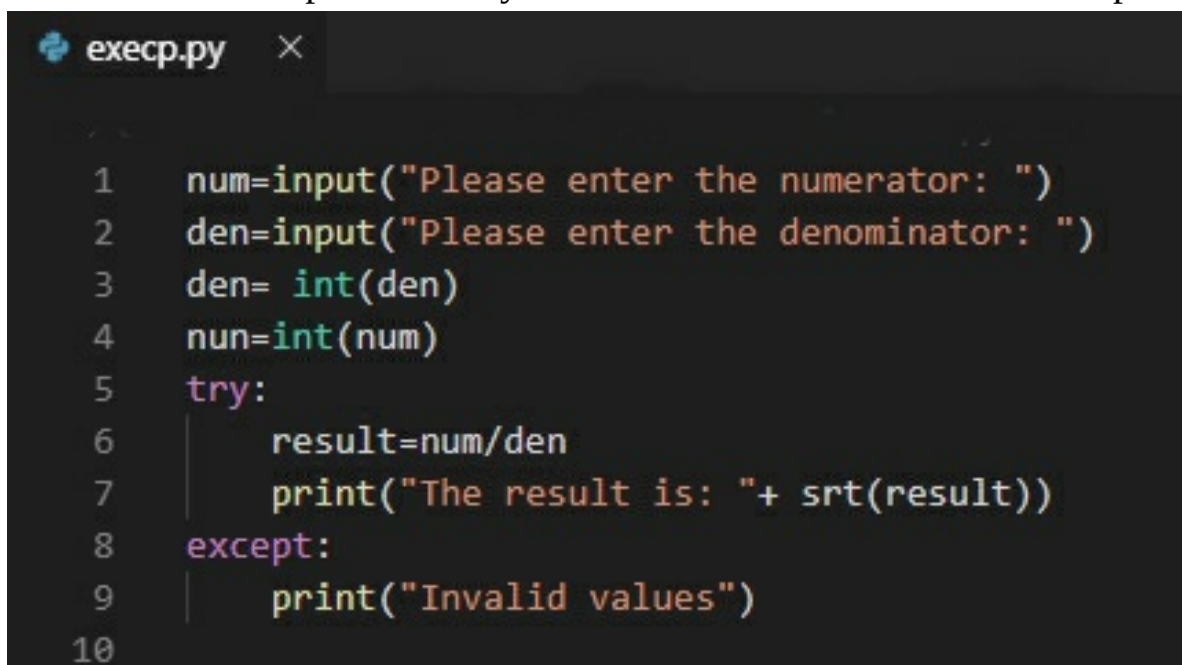
When we program exceptions the sentence `finally` is always considered very useful but many times there is not much emphasis on its

importance.

Which is the finally block? What is it used for? What is it based on?

Let's suppose that we have written a code in the try block, it will take care of a certain task and will use a large amount of resources which have to be released once they cease to be used. These resources will be eliminated or released through the finally clause and the code will be executed without taking into consideration if the try block has been able to raise the exception it had.

As we know, it is not possible to make a division by zero, so we will use a similar example to show you how useful it is to work with exceptions.



```
1  num=input("Please enter the numerator: ")
2  den=input("Please enter the denominator: ")
3  den= int(den)
4  nun=int(num)
5  try:
6      result=num/den
7      print("The result is: "+ str(result))
8  except:
9      print("Invalid values")
10
```

The first thing is to declare the variable num, which is related to the input function, it will be waiting for the data to be entered by the user, in such a way that a decimal value will be expected to be stored in num; in an analogous way, the same is done with the variable den, which is designed to be the denominator of the division.

The following action to all this, is to change the type of format of each variable, for it is used the function `int()`, to convert the variable `num` and `den` to integers, since as they are related to an input, the same ones will be stored as a string and it will be impossible to make arithmetic operations with them, for this reason, they are transformed to variables of type `int`.

Now we will enter the exceptions, since we first enter the `try` block, which is in charge, as its name indicates, of trying to do certain actions, if no exception occurs; what we mean by this is that, in this case, if `den` is not equal to zero, no exception should occur, therefore, the value of the division between `num` and `den` should be stored in the variable `result`, then the value of it will be printed on screen.

But in the case that some error occurs, specifically some exception, it will enter in the exceptions and will proceed to print in screen that the entered values are not valid.

Another example that we must show, is one which takes the block finally, so we can see its functionality, for this, we will continue with the examples of divisions, but now we are going to put two exceptions, one that will appear in the case that the values that are entered are not decimal, therefore, it will be impossible to convert these data into integers, for this reason, the first exception will be triggered. Then it will be verified if the denominator is equal to zero, and if it is true, another exception will have to be thrown.

```
execp.py x
1  num=input("Please enter the numerator: ")
2  den=input("Please enter the denominator: ")
3  try:
4      den= int(den)
5      num=int(num)
6  except:
7      print("Error, you put a ASCII data, please try again")
8      num=int(input("Please enter the numerator: "))
9      den=int(input("Please enter the denominator: "))
10 try:
11     result=num/den
12     print("The result is: "+str(result))
13 except:
14     print("Error, the den has a value equal to zero")
15 finally:
16     print("Thanks for use this program")
17
```

Here we can see better the example, the first thing we see, and that we should expect, is that both the variable num, and the variable den, are using the input() function, which will be in charge of receiving the value that the user wants, in this case, the value of the numerator and the denominator respectively.

Then we enter the first block of instructions, What are we trying to do in this section? The first thing is to convert the strings that are both num and den, to integer variables in order to continue with the relevant mathematical operations, for this reason, it is important to make the type transformation, because as you know, it is not possible to divide a letter between another letter, because mathematically it does not make sense. The first thing is the try block, which as its name indicates, will try to do something, if there is not anything that generates some error, then it will do it without any problem, but in the case that it is not possible to do that, then it will enter inside the block



except, which will be in charge of processing the exception. That block, in case, that an error has been found, will enter in action since it will try to fix the error found, the first thing it will do is to show in screen the error, it will transmit to you that erroneous ASCII data was placed, that please try again. Then the num variable will be Redeclared, which will be input type since it will be waiting for the values entered by the user, and then it will be transformed to an integer type variable, the same will be done with the den variable.

Later, the other block of exceptions will be entered, the first instruction we find in it is to declare the result variable, which will be the division between the num and den; to then place on the screen the result of the division. And well, as you should know, this block will try to do that, but there is the possibility of an error, but what could it be? Well, the main one is the division by zero, more than a programming error, it is a mathematical error, therefore, this block cannot be executed and the part of the exception will be entered. The same one will try to communicate to the user that an error exists, this message will say to him that the denominator has a value equal to zero, for this reason, it is not going to be possible to execute the division.

At last, we will enter the finally block, which will make an instruction no matter what happens, no matter if the try or the excepts are executed, this block will always be executed. It, in this case, will print a message, in which it will be thankful to have used this program.

But if you verify the previous example and this one, the block finally does not do anything very special, but it does, the difference is that this is always done, now, if you want to get an example, in which is used more and is more important the finally, you will see it when you use the databases,

because always, whatever happens, it is essential to close the connection to a database, because if this is not done, it may cause some errors that any programmers want to have.

# Chapter 4: Loops

## What is a Loop?

A loop (or cycle), is a control structure that is in charge of repeating a block of instructions, while a certain condition is fulfilled, within the loops we also have the so-called infinite loops in which their condition is never fulfilled. As in most programming languages, Python has a while and for.

1. Loop For: Python's for statement iterates on the items of any sequence (either a list, a string of characters or dictionary), in the order they appear in the sequence. Where the code is called "loop body" and its repetitions "iterations".

Where iteration is defined by performing a number of actions repeated times. The for loop is in charge of going through these actions in order to look for elements that fulfill certain conditions and that at the same time can carry out the specified instructions. So all these elements must be iterable.

The syntax of a for loop is as follows:

```
for variable + an iterable element (list, string, range, etc.) :  
    loop body.
```

It is necessary to specify the variable in which the items of the element are going to be saved, then we write our sentence for with a variable that will store the items and finally we write in which will be our element to iterate.

The loop is executed as long as it fulfills a condition, so once the iteration is finished, this will make the loop stop.

Example:

```
1  x=0
2  for x in range(4):
3      print(x)
4  print("End")
5
```

The first thing we can see is that we define the variable x, which starts at zero, this is because it is going to iterate, and must start with zero.

Then we fully enter the for cycle, and as you can see, it is specified that the variable x, is going to iterate within the range of 4, What does this mean? Well, x is going to iterate four times and take the value of zero, one, two and three.

The next part is the block inside the for, which is a simple print, and this is going to show us the value that has x in each part of the for, until it gets to be valued four, when it has that value, it will automatically quit the cycle.

Finally, End will be written to show that the program is finished and the cycle was quit.

## Types of for loops:

1. Loop "for" with lists: you can make for cycles with lists, in this case, it will iterate within each value of the list.

In order to better understand what we are talking about, we will make some examples of each one of these ways of using the for.

- a. Loop "for" with list and the function "range"; in this loop are presented list data types and with the help of the function len()

and range(), it is possible to make a for, these are very useful to print data.

-range() is a function that, as mentioned above, returns a list of integers, accepting as arguments the beginning of the list, the end and the increment between one element and the next. We can also omit one or two of them, as explained below;

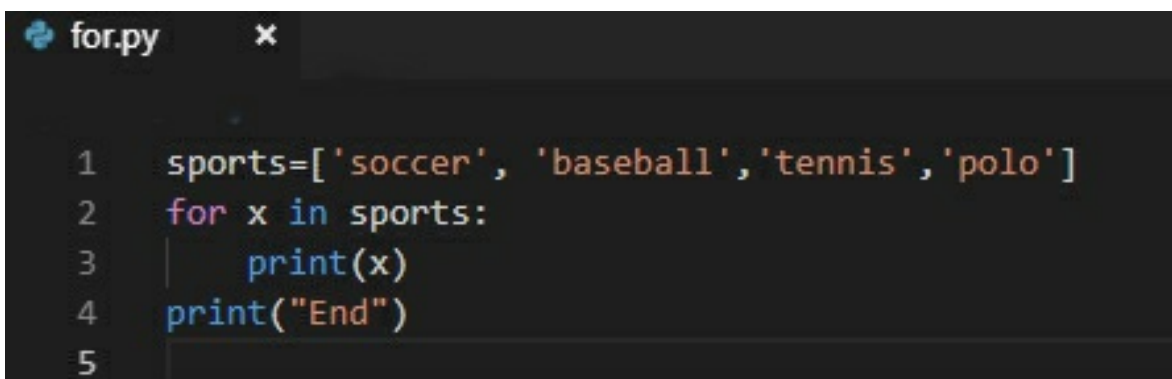
- range ( n ); this type of function takes care of returning a list of integers beginning with 0 and ending in n-1.

- range ( beginning, end); this type of function is in charge of returning the list of integers located between the beginning and the end, without including the latter.

- range (beginning, end, step); this type of function takes charge of returning the list of integers, as in the previous case, only that between the beginning and the next element will exist a difference of step, and so on.

Let's do two examples, one without the range function, and another with it.

1) Use of for and lists, without the use of range:



```
1  sports=['soccer', 'baseball', 'tennis', 'polo']
2  for x in sports:
3      print(x)
4  print("End")
5
```

As you can see in the example, first, a list was created, which has the name sports, it has as items, different sports, such as soccer, baseball, tennis, and polo.

Subsequently, the for cycle was defined, and, What does the x variable do this time? What it does is iterate within the sports list, so x will take the values of each item it has within the list.

The next thing is to define the for block, it is important to remember the indentation because if this is not done, no action will be done because Python takes this very seriously. Since we already placed the indentation, we define the block, which is a simple print, and what this does is print the values of x, and well, as we have already explained, x will take the value of the items from the list in question.

And well, to finish, will be printed on-screen "End", to show that the program has finished and quit the cycle correctly.

2) Use of for and lists, with the use of range:



```
1 sports=['soccer', 'baseball', 'tennis', 'polo']
2 for x in range(len(sports)):
3     print("The sport "+str(x+1)+" is "+sports[x])
4 print("End")
5
```

In the example, we can see a change; the first one is that in this case we use the range, but we are going to go step by step to explain the code and make it very simple.

The first thing, as we have already seen, is to make a list, in this case, the same list of the previous example, with the consequences that this entails, this means that the items of the previous example, will be the same as the current ones.

Then, we define the for, in this case, we place the range, with which we mean that x iterate from zero to the range of numbers that the len function

returns to us, but, what does this mean? Well, `x` is going to iterate within a list of the length that the `len` function tells us, therefore, if `len` returns a value of four, then the variable `x` will iterate from zero to three, taking the values zero, one, two, three, and as you can see, it will iterate four times, as the `len` function said, of course, if it gives us a value of four.

Afterward, we programmed the `for` block, which is a `print`, but in this case, "The sport" was printed, then it was concatenated with the string that returned the function `str(x+1)`, but, why `x+1`? Because as `x` varies from zero to the number that gives us the function range, the first position of the sport will be zero, for that reason, we added one, and so it will appear on the screen, that the first sport, is in position one. After this, it is concatenated with " is " and it is also concatenated with `sport[x]`, in this case, as if it is a list, it is concatenated with the item of the position `x` of the list, and these positions go from zero to the value `n-1` of range.

And finally, "End" was printed on the screen, to say that the program has finished, and the `for` cycle was finished correctly.

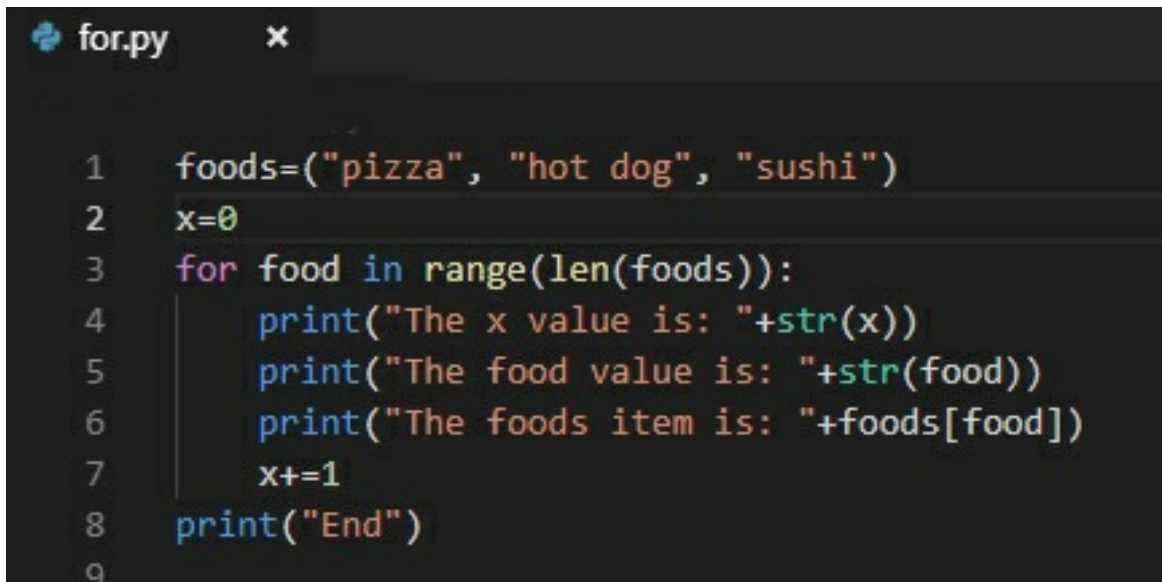
It is important to remember, that for the variable `x` to vary, this has to iterate within a list, and as it has been said before, the function range returns a list of `m` numbers, therefore if we say that `a = range(10)`, we can obtain that `a` will be equal to `[0, 1, 2, 3, 4, 5, 6, 7, 8, 9]`, therefore, the variable `x` will vary from zero to nine.

- b. Loop "for" with Tuples; tuples are sequence objects, specifically, it is an immutable list data type, so it cannot be modified after its creation. This type of program is not very difficult to design, since, to program in tuples and cycles, it is done in a similar way that with lists, the only detail is to keep in

mind the difference that exists between list and tuple.

Two examples will be shown in the same way, the first one will be with range and the other one will obviate this function.

#### 1) Loop for with Tuples and range:



```
1  foods=("pizza", "hot dog", "sushi")
2  x=0
3  for food in range(len(foods)):
4      print("The x value is: "+str(x))
5      print("The food value is: "+str(food))
6      print("The foods item is: "+foods[food])
7      x+=1
8  print("End")
9
```

Here the first thing we see is that we create the tuple foods, which has some items within it, among which are the strings "pizza", "hot dog" and "sushi", and as you should know, after creating a tuple, it cannot be modified, or changed, or anything like that.

Then a variable x was declared, which has the assigned value of zero.

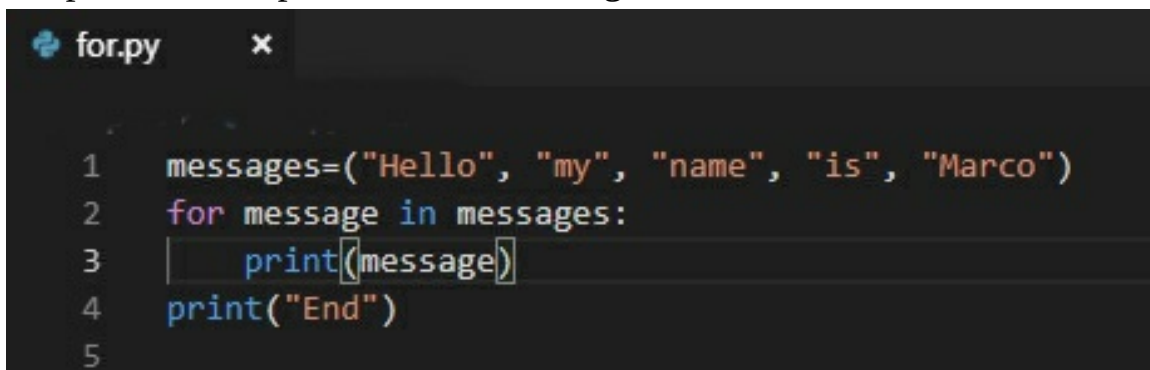
Next step is to declare the for, and as you can see, in this case, it is not going to iterate the variable x, but a food variable, which is going to iterate within the list that is going to return the range function, which should give a list of three elements, and, Why three elements? Well, as you already know, the len function returns the value of the length of a list or a tuple, and as in this case, the tuple foods has three elements, then the range function should create a tuple that goes from zero to two.



Then, to see more clearly how the variable food iterates, the following instructions were programmed, first the value that has the variable x was printed in that instant, then, the value of food was printed in that instant, with the objective of verifying if they have the same value, and as you already know, to concatenate an integer with a string, the function str was used. Next act is to print the item of the corresponding food, for that reason "The food item is: " is concatenated with foods[food], since we can select a specific value of the tuple foods, and well, in this case, it will be the one that is in the food position. Last but not least, it is said that x will be updated to the next value.

To finalize the code, the string "End" will be printed in the console, to make it clear that the program has finished and that it ended in a correct way.

## 2) Loop for with Tuples and without range:

A screenshot of a code editor window titled 'for.py'. The code is as follows:

```
1 messages=("Hello", "my", "name", "is", "Marco")
2 for message in messages:
3     print(message)
4 print("End")
5
```

In this example, we can see that it is very nice since we send a message with the tuple, but how does this work? Well...

First, we create the tuple messages, which has the following items, "Hello", "my", "name", "is", "Marco", as we can see, is a tuple of five items, therefore it has a length of five.

Next step is to create the for, in this case, the variable message, it will iterate inside the tuple messages; Then the variable message will be printed,

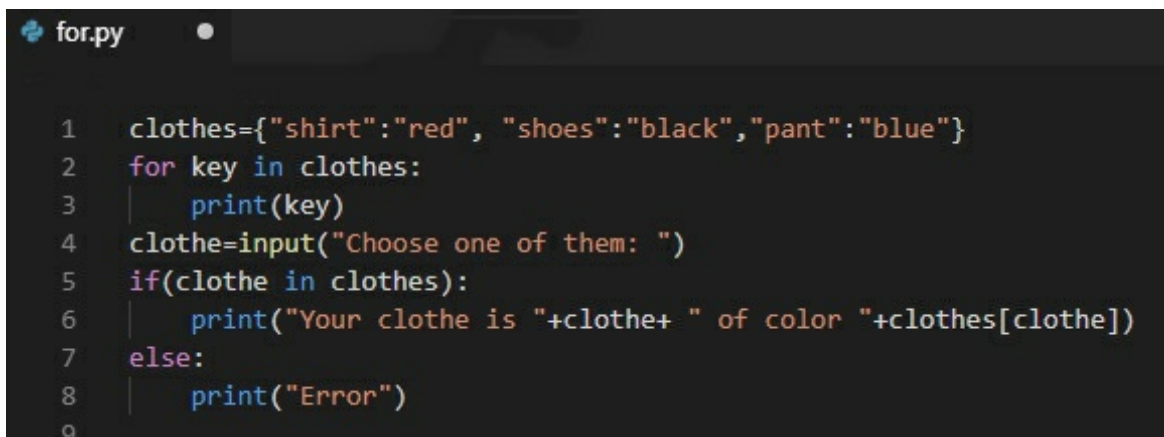
in the position that it is, with which, you will be able to infer that each message will be printed with a line break.

And finally, as it has been done in the previous examples, it will be printed in console "End" to show that it has left the cycle and the program is finished.

- c. Loop "for" with dictionary; the dictionary defines a one-to-one relationship between keys and values, the dictionary type objects allow a series of operators integrated in the Python interpreter for its management.

Analogous to the loops explained above, this "for" loop with dictionary is worked in a very similar way, since all these types of data are similar. But it is worth mentioning that they are different types and are treated in a different way, therefore, even if they are handled similarly, it should never be forgotten that they are different types of data.

Example:



```
1  clothes={"shirt":"red", "shoes":"black","pant":"blue"}
2  for key in clothes:
3      print(key)
4  clothe=input("Choose one of them: ")
5  if(clothe in clothes):
6      print("Your clothe is "+clothe+ " of color "+clothes[clothe])
7  else:
8      print("Error")
9
```

In this example we can see how to work with dictionaries; with the variable we created called clothes, which, as you know, is a dictionary. This has the items "shirt", which has a value associated with "red", there is also

“shoes”, which is related to “black”, and finally “pant”, which relates to “blue”.

After that, we created the for cycle, which tells us that the key variable will iterate in all the values of the clothes dictionary. And if you run this code, in your favorite text editor, you will note that the key variable, will only have associated the values of "shirt", "shoes" and "pant", this can be observed, because the cycle inside the for, what it does is to print the key-value inside the dictionary.

Then, we create the clothe variable, which is a variable that will receive an input, which will depend on the user. When receiving the user's value, an if will be made, and in the case that the variable clothe is inside clothes, as you can see in the condition of the if, it will be entered there, and it will be printed that "Your clothe is" + the option chosen by the user + "of color " + clothes[clothe]; but what are clothes[clothe]? It is the value associated with the clothe selected by the user, better said, if the user chooses "pant", then clothes[clothe] will throw the value of "blue".

Finally, the else condition means that if no clothe is found inside clothes, then "Error" will be printed, and this is very useful since if no value is found inside a database, it will be thrown that the requested value is found or not.

2. Loop "While"; it allows us to execute cycles or periodic sequences that allow us to do things multiple times in a row. This cycle will allow us to execute a block continuously, as long as the while condition is true, and by this, we mean "True". This loop will be in charge of evaluating the condition and if it is correct, the loop is executed and the condition is checked again at the end and if it is still true "True", the program will be

executed again, if this condition is not correct "False", it will be omitted and the common execution of the program will be carried out.

There are several types of "while" loops; like the "while" loop controlled by counting, the infinite while and others; all very useful in specific conditions.

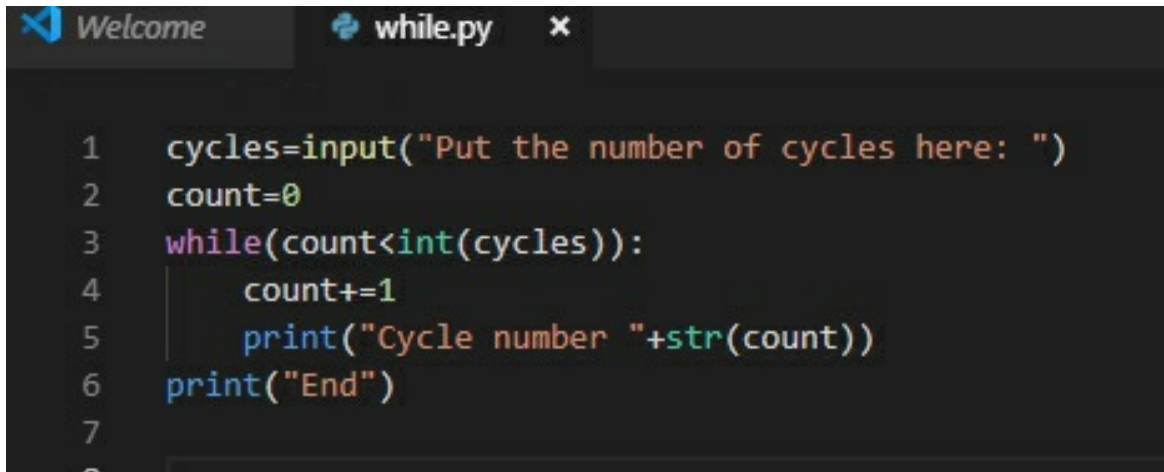
Its syntax is very simple, and is as follows:

While (condition):

Block of instructions within the cycle

Now let's make a simple example, which will consist of the cycle printing a number, as many times as the user wants.

Example:

A screenshot of a code editor window with two tabs: 'Welcome' and 'while.py'. The 'while.py' tab is active, showing a Python script. The script consists of seven lines of code: line 1: `cycles=input("Put the number of cycles here: ")`; line 2: `count=0`; line 3: `while(count<int(cycles)):`; line 4: `count+=1`; line 5: `print("Cycle number "+str(count))`; line 6: `print("End")`; line 7: an empty line. The code is color-coded: strings are in orange, integers in green, and keywords in blue.

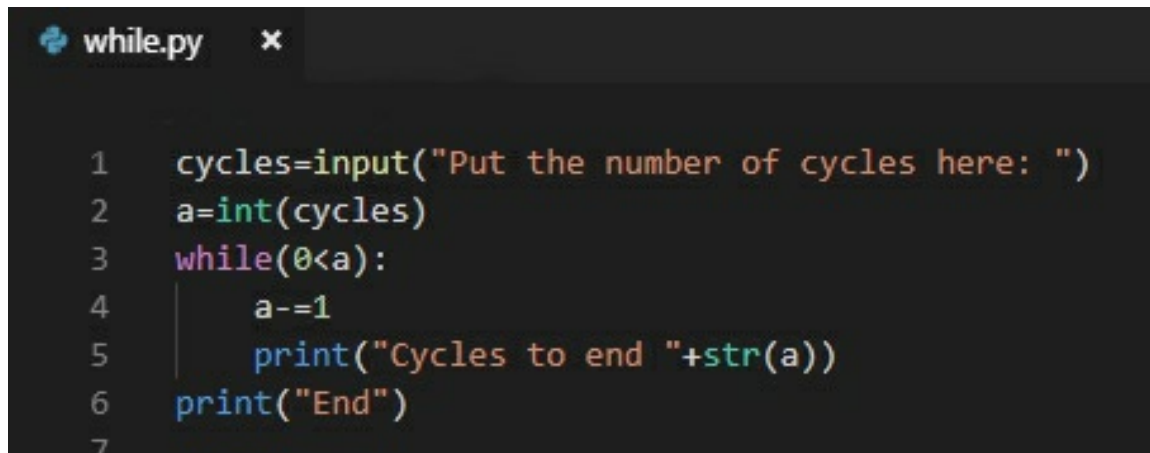
In this example, we can observe several things, the first is that we create a variable `cycles`, which is an entry, which will allow us, as users to enter the number of cycles we want to do in this program, of course, you must never forget that this type of entry is a string, therefore, to do mathematical operations, it is necessary to transform this type of input.

Then another variable will be created, called `count`, which has a fundamental function, and it is to be the cycle counter of our program, with which we define that the same one will begin in zero, for then, to start the count.

The next action is, to begin with the while cycle, as we can see in the syntax previously explained, first it is declared that we are going to make a while, then, between the parentheses we have the condition.

- a. Loop "while" controlled by counting; in this cycle, there is a counter, and this counter will increase as the cycles are carried out, this process will be repeated as many times as necessary until the expected number is reached. We will understand this loop better with the example that we will see next.

Although we have already seen an example of the while controlled by counting, that was the last one, it is never too much to take another example, the same through the counting method, in this case, we are going to make the counter go from higher to lower, as we will see below.



```
while.py x
1  cycles=input("Put the number of cycles here: ")
2  a=int(cycles)
3  while(0<a):
4      a-=1
5      print("Cycles to end "+str(a))
6  print("End")
7
```

In this example, we make a turn of one hundred and eighty degrees, because the counter does not have to reach the maximum value, but starts in it and is going to decrease.

The first thing is that a variable called cycles is created, which is related to an input that the user will write, in which he will enter the number of cycles he wants to do. Next act is to create a variable a, which needs the function int(), since it turns the variable cycles into an integer, because as you should know, the variable cycles is a string, since the entries are saved that way, and with the strings it is not possible to perform arithmetic operations.

In the following line, we declare the while loop, and as it can be observed, the condition is that zero has to be lower strictly than a, therefore, in the moment that a is equal to zero, the cycle will be exited and the other instruction will be passed.

Then, inside the block of instructions that are inside the cycle, the variable a has to be decreased, this is done through the instruction a-=1,

which is equivalent to saying that  $a = a - 1$ , and it can be observed easily as the variable  $a$  is decreased by a unit.

The next instruction is to print on screen the following message "Cycles to end" concatenated with the number of missing cycles to exit the cycle.

Finally, the "End" string is placed on the screen to say that the program has finished and that the while was exited correctly.

This type of cycles by counts are very useful, we are going to use them first with the utility of those cycles in which it is necessary that the counter grows, the first utility that comes to our head is to make a programmed chronometer, in such a way that when arriving at the maximum value, it is going to leave the cycle and show in screen that the required time has been fulfilled, now, there are also other utilities as it can be to check a list with a known length, therefore we will be moving item by item; although this last utility easily can be replaced by a loop for. Now, while cycles per count, but in this case, that the counter goes decreasing, could be used to make a countdown to sound an alarm or something like that.

- b. Infinite "while" loop: This type of while is very useful, in the case that an accumulation of instructions is done a number of times not determined, with this we mean that we do not know how many times it is going to be done, therefore the programmer, will make the condition a while( True), and of course, as you can see, the True boolean, allows the while to work constantly.

Let's code two examples, one that we use an infinite while, the strict way, and another not so much, although the programmer does not know the

number of cycles that will be done, does not use the True condition to force the block to be repeated indefinitely.

Examples:

1) While with the True condition:



```
while.py x
1  import time
2  x=1
3  while(True):
4      print(x)
5      x+=1
6      time.sleep(1)
7
```

The first thing we observe that is different is the import of the time module, but those are issues that we will see later, at this time is not something very important.

Now what really interests us is the declaration of the variable x as one since this will work as a kind of counter, so it will increase little by little.

The next step is to create or, better said, declare the while, and as you can see, the condition inside the while is True, therefore, it will always be fulfilled, which indicates that the cycle will be repeated at all times, unless some sentences are declared, which we will see later.

Inside the while block, the variable x will be printed on the screen, and this is where it makes sense to use x as a counter since it will allow us to see in the console the specific second that has happened since the program started. Then it increases the value of x, because as we have already said, it

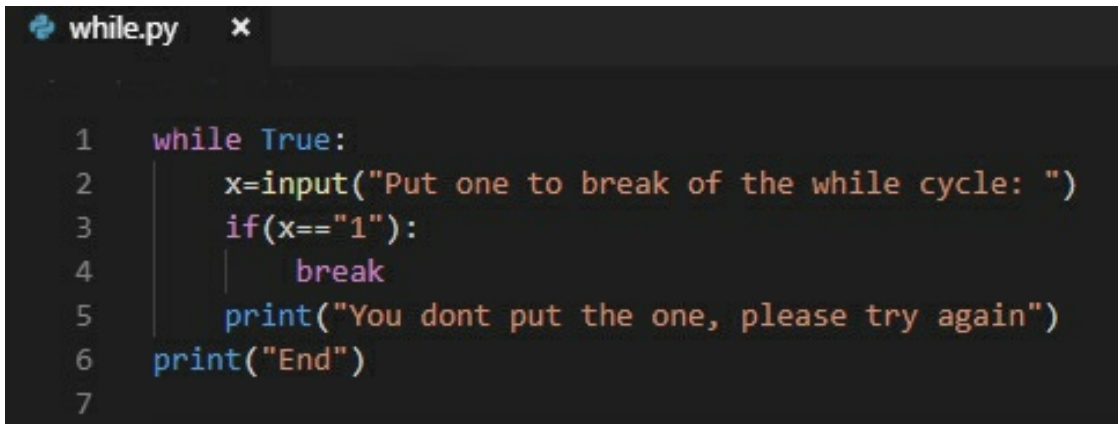


has a counter function, and it will increase one by one.

Finally, we use the library time, so that will make a delay of a second, that's why our program works as a chronometer, which will show us on screen the second in which we are after running the code, and the same will be updated every second.

## Sentences used in the while loop:

1. Break Sentence: the word break is used to interrupt the cycles or abandon the cycles even when they have not finished, meaning that the evaluated expression of while remains in the true position. To be able to evaluate and understand this sentence, let's see the following example.



```
while.py x
1  while True:
2      x=input("Put one to break of the while cycle: ")
3      if(x=="1"):
4          break
5      print("You dont put the one, please try again")
6  print("End")
7
```

In this example, we see how to implement infinite while cycles, because as you can see in the first line, the condition inside the while is always going to be true, therefore we are in front of an infinite cycle.

Later, we declare the variable x, which is related to the input function, which will be waiting for the user to enter any value, specifically, it is necessary to enter a one so that it exits the cycle, in case that what user enters is not the indicated value, then the cycle will be repeated.

As you can see in line three, you have a statement of an if, which asks if x is equal to the string "1", Why is it compared with a string? Because, as we already know, x is a string because it is related to the input function, at the moment in which this variable is declared. If the condition is true, the "break" sentence will be used, which specifies us to exit the infinite cycle.

If the condition is not true, then the following string "You don't put the one, please try again" will be printed on the screen.

Finally, at the moment of exiting the cycle, the usual "End" will be printed, to show that the cycle was executed correctly, and the program was finished.

What we can learn from our example with the break? or what benefit we can get from it? Well, the first thing is that the sentence break is extremely useful to get out of the cycles, it does not have to be strictly an infinite cycle, because it can be used in a cycle that is operated by counting or another method, therefore, it is important to remember that. Another fundamental thing is that this type of sentence, not only works for a while but can also be used in for cycles, therefore, are an essential tool when programming.

But in what cases should this type of statement be used? Well, the first case that comes to mind is the handling of some exception that may occur within the cycles, in the event that something unwanted occurs, it gets out of it and notifies the error or does what you desire to program. Another case may be an access system since a specific key was requested, and in the case that the correct key is not entered, the user will not be allowed to enter another part of the program.

2. Sentence Continue: This sentence ends up being very useful

when programming, when applying it we will be omitting what follows the sentence within the cycle. That is to say, if we fulfill some previous conditions, as, for example, if after several "if" or else, or other steps, we manage to reach a continue sentence, we will proceed to omit the rest of the instructions of the cycle, and then do another iteration. We could summarize that the instruction continues inside a loop forces the interpreter to return to the beginning of the loop ignoring all the instructions and interactions that are inside it.

The next example will show a while cycle, which will omit the values that are multiples of five, if these values are multiples, then it will not be printed on screen and the next iteration will be done automatically.

```
while.py

1  cycles=input("Please put the numer of cycles: ")
2  count=1
3  while(count-1<int(cycles)):
4      a=count
5      count+=1
6      if(a%5 == 0):
7          print("Error, continue")
8          continue
9      else:
10         print("Not is multiple of 5")
11         print(a)
12     print("End")
13
```

To start, the variable cycles is created, which is an input, which asks the user to enter the number of cycles he wants to do, and, as is well known, you have that cycles is a string.

Next, it creates the variable count, which is integer type, this will have the function of counter, to know the cycle in which we are, to reach the maximum level that the user wants.

Now we will create the while loop, which specifies that count-1 has to be lower than cycles, and, Why count -1? Well, in order to fulfill what the user wants; since if the condition was, a lower or equal to cycles, the code will be less optimal, for this reason, only a strict lower is placed, and as the counter starts in one, it is necessary to subtract a unit and that the number of corresponding cycles is met.

In the following line, the variable a is declared, which has the same count value, because to know the current value of the cycle, and well, as it is obvious, the counter is increased by one unit, through the instruction in line five, which says count += 1.

Subsequently, one enters the block of conditionals, in this case, the condition is  $a \% 5 == 0$ , but what does this mean? Well, the rest that gives the division between a and five, has to be strictly equal to zero, in order to enter the if. In the case that the condition is true, the orders found in the if block will be performed, these instructions are the following; the first thing is to print on screen that there was an error, then the continue sentence will be used. If this condition is false, the instruction containing the else block will be passed, which is based on notifying that the cycle is a multiple of five.

At the end of the conditionals, the cycle number is printed on the screen to know when we are in the program.

And finally, a screen print is placed to show that the program has been completed and the cycle was exited correctly.

Now, what can we learn from this program? The first thing is the use of

the continue, because its function, specifically is to go directly to the next while cycle, omitting the other lines of the block, well, in this case, it is the same, since when arriving at the continue we pass to the other cycle, but in the case that this sentence is not found, the value of a would be printed, as you can see that it is the next instruction after the conditional block, but this type of sentences, interrupt the natural flow of the program, being very useful for the handling of some exception that happens within the cycles.

3. Pass Sentence: It is a null expression, in other words, this sentence does nothing, but it allows us to create a loop without placing code in its body to be able to add it later and use it in this way as a temporary filler, with this we mean to add some type of delay to the program; or as well in the case that you manage the programming with assembler or with processors, it is a way to make a nop. It is a sentence that will not affect in anything the behavior of the code, and it should be noted that not only can be used in cycles, it can also be used anywhere in the code without any problem, with these words, we mean that the sentence can also be used in a common function without any trouble, but this is not worth to mention yet, because we have not seen functions, but it is not excessive to know that the pass can be implemented with the functions. We could say to establish a difference that continues will take care of ending the current interaction, but will continue with the next iteration of that loop, going back to the beginning, while pass is not going to do anything, just continue with the following instructions without going back to the beginning. Next, let's see an example of what it is.

```
while.py x
1  cycles=input("Please put the numer of cycles: ")
2  count=1
3  while(count-1<int(cycles)):
4      a=count
5      count+=1
6      if(a%5 == 0):
7          print("Error, continue")
8          pass
9      else:
10         print("Not is multiple of 5")
11         print(a)
12     print("End")
13
```

By looking at the previous example, we can see how we declare the variable `cycles`, which is going to wait for the user to specify how many cycles to use, the input will be of the string type.

Then the count counter will be created, which will start from one for convenience, but has the function of knowing what is the current position of the cycle.

The following order, is the creation of the while cycle, with the condition that `count-1`, has to be strictly lower than `int(cycles)`, it is worth noting that the use of the `int()` function, since the `cycles` variable is of string type and making comparisons with strings and integers is not possible since they are different types of data. The reason of the `count- 1` is explained in the previous example, so we don't have to repeat it, but remember that we are making comparisons starting from zero and that is the reason why the comparison is strictly lower and is not lower or equal since we would make one more cycle.

The following instructions are to declare the variable `a`, which will be assigned the value of `count`, this is to be able to make operations on this value and not lose it; then the value of `count` will be increased by one unit, since if this variable is not increased, we will be doing the same thing infinitely.

The next part is the conditional phase, which is in charge of verifying if it is a multiple of five, and we do this by using the `"%"` operator since it will return the rest of the division we place, so that if we place, for example `10% 3`, it will return the value of 1, which is the rest; in an analogous way it is done here, since when putting the following instruction `a% 5`, we are asking for the rest between these values, and to know if a number is a multiple of another, because the rest between both should be zero, for this reason, the strict equality is made to zero, in the case that the condition is fulfilled, because we will be in front of a number that is divisible by five, or multiples of five, being those the numbers that we want to find.

Now in such a case that the if condition is met, we will proceed to make a cumulus of instructions, the same will be, to print in screen that an error has been produced and that it is going to continue, then, the following instruction is the sentence `pass`, which will not do anything, is like causing a small delay in the program, depending on the frequency of the clock of the processor of our machine, but those are subjects that do not interest us very much. But, if the condition is false, then it will enter inside the block of the `else`, and this only will print that this number of the cycle is not multiple of the five.

Now, at the moment that the conditional block was finished, therefore, it does not matter if the condition is true or false, the number of the cycle in which we are will be printed on screen, by the command `print( a)`, because `a` is the current position.

Finally, when exiting the while cycle, the "End" string will be printed on the screen, which indicates that the while loop has been correctly exited and the program has been completed.

Now, when trying to find a utility to the pass sentence, you don't really find many at this moment that you haven't seen the functions, since now it's just a delay, but it's not a delay appreciable by the user, since the computer clock frequency is in GHz, therefore it's so fast that it's not appreciable, but when you see the functions, there will be times when a complex program is being developed, and there are parts that have not been created, but for the program to work it already had to have created the functions, but the body of the functions has not yet been developed, which is why the use of these sentences is important, so that our software does not break, for saying so.



# Chapter 5: Functions

A function is basically a portion or block of reusable code that performs a given task. It is a code block with an associated name, which receives arguments as input, in addition, follows a sequence of sentences, which executes a desired operation and then returns a value and perform a task, this block can be called when we need, and this can be considered a great advantage. Python is a language that gives us a lot of flexibility when creating these functions.

The use of these functions is a very important component within the paradigm of programming called structured and therefore has several advantages:

- \* It allows reusing the same function in different programs, therefore, when it does the functions, it is not necessary to repeat the code a lot of times.
- \* It allows segmenting a complex program in modules that are simpler, and in this way, we will have an easier programming, as well as a more facilitated debugging, it is as the saying goes, "Divide and conquer", therefore, it is a very used technique.

The Python programming language has what we call functions integrated into the language, which allows us to create functions defined by the user himself to be used later in his own program. These functions are presented below:

Function	Use	Example	Result
Print ()	This function allows the program to	Print ("Hello")	"Hello"

	print in screen the desired argument		
Len ()	This function allows you to determine the length of the characters that a string contains	Len ("Hello world")	11
Join()	This function allows you to convert a string to another by using "-"	List=['Python', 'is'] Join (List)	'Python-is'
Split()	This function will let you convert a string into a list	A=("This will be a list") List2= a.split()	A=[ 'This', 'will', 'be', 'a', 'list']
Replace()	This function, as it names indicates, will let you replace a string for another	Text= "The house is green" Print (Text) Text= Text.replace("green", "yellow") Print(Text)	"The house is green" "The house is yellow"
Upper() and lower()	This function allows us to	Text= "The house is green"	"THE HOUSE IS"

	convert into upper or lower case all the letters in a string	Text.upper() Print (Text) Text.lower() Print(Text)	GREEN” “the house is green”
Ord()	This function will let you use ASCII data type	Print (ord('A'))	65
Tuple()	This function will convert a string into a tuple	Words= tuple (“I am old”) Print(Words)	('I', 'a', 'm', 'o', 'l', 'd')
Type()	This function will return the type of data of an element	X=5 Print(type(X))	<class 'int'>
List ()	This function will let you create lists from an element	Word= list('Hello') Print (Word)	['H', 'e', 'l', 'l', 'o']
Round ()	This function will round the decimal part of a number to its nearest integer	Print (round(15,746))	16
Str()	This function will convert a	X=5 A=str(X)	“5”

	numerical value into a string	Print (A)	
Range()	This function will create a list of n elements. It is mainly used in the for cycle	X=range(3) Print(X)	[0, 1, 2]
Float ()	This function will allow us to convert any value to a decimal type of value	A=float("5.55") Print(A)	5.55
Max() & Min()	These functions will determinate the higher and the lower values in a set of numbers	X= [2, 6, 3, 8, 0] Print (max(X)) Print(min(X))	8 0
Sum()	This function will add the numbers of a set of numbers	X=[3, 1, 6] Print(sum(X))	10
Int()	This function will convert any value into an	A=("35") Print (int(A))	35

	integer		
--	---------	--	--

## **What rules do I have to follow to be able to define a function?**

- The input parameters must be defined within the parenthesis of the function.
- When we develop the code, we must identify the indentation very well and correctly (4 characters of space).
- The code of the function will always start after we place the colon. “: “

It should be noted that a function will not be executed until it is invoked, and to be able to invoke a function it must be called by its name. For example:

function.py

```
1  a=[1, 2, 3, 4, 5]
2  b=[1, 0, 1, 0, 1]
3  num="5 6 7 8 9"
4  c=num.split()
5  print(c)
6  e=[]
7  for x in c:
8      d=int(x)
9      e.append(d)
10 c=e
11 d=[]
12 for x in range(len(a)):
13     e=a[x]+b[x]+c[x]
14     d.append(e)
15 e=min(d)
16 f=max(d)
17 g=sum(d)
18 print(a)
19 print(b)
20 print(c)
21 print(d)
22 print(e)
23 print(f)
24 print(g)
25
```

As we can see in this example, which is quite complete, at first we created variables a and b, they are lists, which have within them integer values, specifically five items, a is a list of numbers ranging from one to five, while b is an iteration of values of ones and zeros.

The second, is the creation of the variable `num`, it is a string, in which is written "5 6 7 8 9", and as we saw previously, the function `split()`, creates an arrangement of strings, each item will be a word, separated by white space, in the code, specifically in line four, we make use of this function, in which we convert the variable `c`, in a list of strings, which should have the form `["5", "6", "7", "8", "9"]`, but it is not possible to do mathematical operations with this type of data, as they are, to be more specific, as strings, therefore we are going to proceed to convert all these items into integers, so that you verify that it is true what we say here, we use the print of the list `c`, so that you can see the list of strings.

To achieve our goal, first we declare the variable `e` as an empty list, then we use a for cycle, in which the variable `x`, will iterate within the array `c`, which has its items as strings, therefore, within a variable `d`, the integer that results after applying the function `int()` to the element of the list `c` at that time. Then the value of `d` is added, within the list `e`, until the number of iterations is finished. The next action is to store in `c`, the list that was stored in `e`, in order to have a better order of the variables.

Subsequently, the variable `d` was assigned the value of an empty list, in order to store data within it. Then, with the help of a for, which is going to iterate as many times as the number of items in the list `a`, as we are going to have to move through all its items, since what we want is to create another list, which contains the sum of `a`, `b` and `c`, so inside the same bubble, it is said that `e` will be equal to the sum of the item that is in position `x`, of lists `a`, `b` and `c`. After adding the three items, the append function will be used to add the value obtained to the `d` list.

## **How to create your own function?**

To be able to create a function of our own, we must follow the "def" sentence and proceed to name it, except that this time it will not be the name of a predefined function, but this time it will have a name created by us.

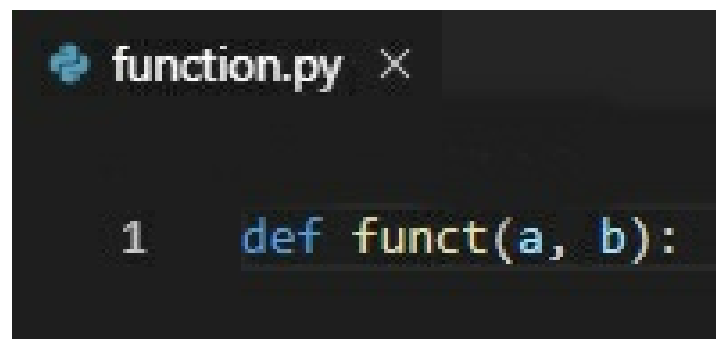
## How can I call a function?

To be able to call a function, we only have to declare it when we start in our code. This is fundamental because it is not possible to invoke a function that has not been created in advance. Example:

## Parameters

We define parameters as a type of value that is entered into the function when the function is invoked, a function may be able to receive one or more parameters. These parameters must be separated by a comma "," in order to be invoked.

Example:

A screenshot of a code editor window titled "function.py". The editor shows a single line of Python code: `1 def funct(a, b):`. The text is color-coded: "def" is blue, "funct" is green, and "a, b" are blue. The line number "1" is on the left.

As you can see in this small example, because it is very simple, really, it was just to show how the first part of a function should be defined.

The sentence that can never be missing when defining a function is the `def`, which is the one that specifies that a function is going to be created or, better said, indicates that a function is being defined.

Then we can see that follows a word, in this case, `funct`, that word



was to put a name to our function, and then you can see a parenthesis, which has two letters, a and b, meaning that these are going to be the parameters that our function will receive to work.

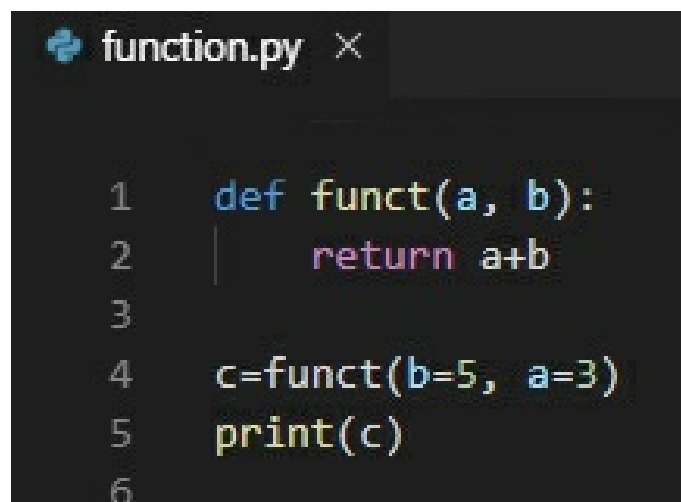
## How can we define arguments and parameters?

As we already know, we call parameters to the values that the function receives when it is defined. When the function is invoked, these values are called arguments and divided according to their type.

These arguments are divided into several types:

### Arguments by name:

When we are going to invoke a function, we must indicate in the arguments the value that each parameter will contain starting from its name.



```
function.py x
1  def funct(a, b):
2      return a+b
3
4  c=funct(b=5, a=3)
5  print(c)
6
```

As we can see, we continue with the funct function, in this case, we still have the same parameters a and b, we also see how the definition is exactly the same, the only difference is at line two, as it indicates that the sum of a with b is going to return. The return sentence will be explained later, but it is not something too complicated, the same name tells us what it does, to return a value.

Then in the following lines, the variable c is created, which will be equal to the value returned by the function we have created, and as we said previously, it will be equal to the sum of its parameters a and b. As you can

see, when you call the function in line four, first write the name of the function, in this case `funct`, and the arguments that are going to be passed, are previously specified with the name, as you can see, the argument that has a value of five, is specified that it will be parameter `b` of the `funct` function, analogously is done with parameter `a`.

Finally, the value of `c` is printed on the screen, so that you can visualize that the result is correct.

## Argument by position:

When we send an argument to a function, they receive the defined parameters in order.



```
function.py ×  
  
1  def hello(name, color):  
2      print("Hello "+name+ " your favorite color is "+color)  
3  
4  a=input("What is your name? ")  
5  b=input("What is your favorite color? ")  
6  hello(a,b)  
7
```

In this example, another function will be created, which is called `hello`, and has as parameters both `name` and `color`, this function was created to make a message on screen, in which the user will be greeted with his name and will also be told what is his favorite color.

To call this function first it is necessary to declare two variables, the first one is the variable `a`, who is in charge of storing the value of the string related to the user's name, while `b`, is in charge of storing the string related to the user's favorite color, these variables are related to the `input` function, which means that they will be waiting for the user to enter the value he wants.

Finally, the hello function is called, making use of its name, but in this case, the arguments were passed by order and not by name, so you have to be very aware for the correct order, since, if there is an error in this, the program can easily collapse or fail to do what is required.

As you could see, the ways to pass the arguments are different, you can use the one you prefer, it depends on your preferences; in the case that you find it easier or faster by position do it that way, but take into account that you have to be aware that the argument is in the correct parameter position, but if you like it more by name, do it that way, of course, you also have to be aware that you are writing the parameter names correctly.

## Call without arguments

When we call a function that has some defined parameters, if these are not passed correctly an error will be generated.

A screenshot of a code editor window titled 'function.py'. The code is as follows:

```
1 def hello():  
2     print("Hello")  
3  
4 hello()  
5
```

In this example, the hello function is created, which is not going to have parameters, and this will only make a screen print, with the message "Hello".

Then, to call it, only the name of the function will be written with parentheses, in the following way name().

## Return statement

As we have seen before, most Python functions will contain a return value which can be explicit or implicit.

We know that return is a reserved word whose purposes are to finish the execution of some function and then return the value obtained as a result. If you want to visualize an example of this, you can see the one that is in arguments by position, since it can be observed that the function has the return sentence, which will return the value of the sum of a plus b; and also, as you can observe in this example, that value is stored in the variable c, to then print it.

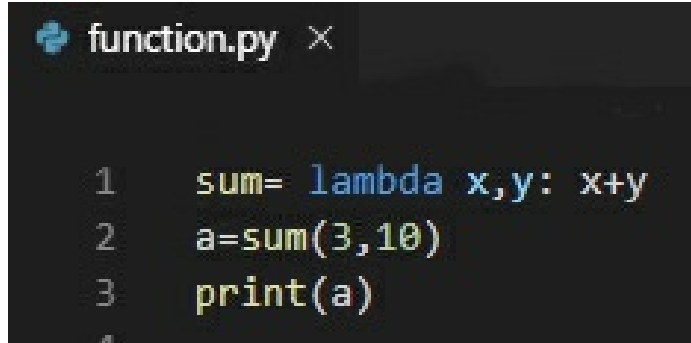
## **Lambda function**

We define lambda functions as a special type of function which is part of the predefined functions in Python. What do we mean by this? This type of function is mainly noted for being "exclusive" because it allows us to create "anonymous" functions quickly because it has a somewhat exclusive syntax.

The lambda functions are able to execute an expression and return the result of it, it can contain optional parameters in its structure, but nevertheless, this function has its own restrictions.

## **Syntax of the lambda function**

The syntax of the lambda function in Python is very simple since it is based only on writing the reserved word lambda, followed by the arguments that come with the action and finally separating with their respective double point ":".



```
function.py ×  
  
1  sum= lambda x,y: x+y  
2  a=sum(3,10)  
3  print(a)
```

In this example, we see the use of the function lambda, in this case to the variable sum, we make use of the sentence lambda, in order to create a function that has as purpose to make the sum of two numbers, both x and y. For that reason, it is observed that the parameters that we have is the one of x and y; for then inside the block of the function, return the sum of both.

Finally, to call the function, to the variable that we declared as a, we assigned the value that returns sum, for then, to make sure that the result is certain, we proceeded to print in screen the value that stores the variable a, and if you get to run this program, you will be able to observe that it will give 13.

The lambda function is commonly used when you need to invoke a function for a short time (this function does not require a name) and is mostly used together with the integrated functions filter(), map().

## Filter() function

The filter() function is the one (as its name indicates) that is in charge of filtering. What does this mean? This function takes a sequence as arguments, either a list or an iterator, then it will return an iterable with the elements already filtered (this will return a true if the condition is met).

```
function.py

1  def pair(n):
2      if(n>0 and n%2==0):
3          return True
4      else:
5          return False
6
7  numbers=[]
8  for x in range(25):
9      numbers.append(x)
10
11  pairs=filter(pair, numbers)
12
13  for x in pairs:
14      print("The number "+str(x)+" is pair")
15
```

For this example, the first thing we need is a conditional function, to know what we are going to filter, in our case, we will create the pair function, which will have as parameter, the integer n, then we enter a conditional block, in the part of the if, the condition would be that n has to be higher than zero, since the zero is a number that is not even, the other condition that must be fulfilled at the same time, is that the rest of the division between n and two has to be strictly equal to zero, because as you should know, this is the definition of a pair number.

The next step is to fill our arrangement of numbers that we are going to filter, for it we create the variable numbers, which will be an empty list. To then enter a for loop, in which a variable x will vary from zero to 24, as you can see in line 8, this is thanks to the range function, which gives us the limits

of the for. The next thing to do is to fill in our list, this is done using the append function, in the numbers variable, which, if you remember is an empty list, after it is filled in, it already becomes a list with integer values as items.

We are already able to filter the list, and we do it creating a list called pairs, which will use the filter function, and the same one will return the values of the arrangement that the function returns to us as True, as for example 2, since this one is higher than zero and the module of the division of the same one, between two is equal to zero, therefore, it fulfills the requirements.

The last step is to print in screen all the obtained pairs, and we do it with the help of another cycle for, in which a variable x, will iterate through all the list and will print us that those numbers are even.

## **Function map()**

The map() function is the one that is in charge of executing each element on a list or tuple to be able to return a sequence of elements which will be the result of the operation.



```
function.py ×  
  
1  def sum(a, b):  
2      return a + b  
3  
4  list1=[1, 0, 1, 0, 1]  
5  list2=[0, 2, 0, 2, 0]  
6  c=map(sum, list1, list2)  
7  print(list(c))  
8  
9  string1=["Hello, ", "are "]  
10 string2=["how ", "you"]  
11 c=map(sum, string1, string2)  
12 print(list(c))  
13
```

In this example, we can see in the first lines, the definition of a function called sum, which has as parameters, variables a and b do not have to be exclusively integers, they can be strings or any other type of data. It will return a+b, whether it is a concatenation or a sum.

Later, we created two lists, the "List1" and the "List2", the same, are lists that have within them, an iteration of numbers between one and zero, this is for List1, now for the case two it is analogous, but in this case, are iterations between the numbers two and zero.

Then, we declare a variable c, it will make use of the map function, and will receive as arguments, the function sum, list1, and list2, what this will do is to create a list that will be in a specific memory address, which will

have as items, the sum of list1 and list2. To print what is in c, it is important to use the list() sentence, since if you want to show the desired data, we have to tell the program that we want to see the list that is in that memory address.

Later, two variables were defined, the first is string1 and the second is string2, which will have a message. After the declarations, the map variable is used, and it receives the parameters sum, string1 and string2, what we are doing in this case, is concatenating the strings that there are as item of each list. Finally, we will print in screen the value of the list that is in the address c.

## **What are the differences between the lambda functions and the functions defined with "def" sentence?**

We know that functions created with the lambda function can also be created with the "def" statement. What does this mean? This means nothing more than creating a function with either of these two statements is considered a correct action. This is because by both methods you can get the same result, with simpler options.

We can see this as a path, both reach the same destination, the difference is that one is longer and heavier and another is much simpler, as that is the lambda function used for, to make it easier to use functions in our code.

When we create a lambda type function, it will only focus on using a single line of code, thus minimizing the number of lines that can be used in a code, unlike the def statement, which usually occupies many times more than one line of code.

When using the lambda keyword, we create an object or function which is not going to have the need to be defined with a name, unlike the def statement which must be defined at the beginning of the program so that it can interpret it.

Although using the lambda function is much simpler for the code, many times the def statement is more understandable for those users who are starting as programmers and even for those users who have programming knowledge but not so much experience.

It is of fundamental need that at the moment of operating with the lambda function, this one is assigned a variable since if this is not done, the same one is going to operate only in the line in which it is going to be defined.

# Chapter 6: Object-Oriented Programming-OOP

At this level, we are already able to design the program based on functions, so that we are able to use statements that manipulate the data. In this programming language, we can find procedure-oriented programming and object-oriented programming, which uses types defined by the programmer to organize both codes and data.

## What is OOP and what are its advantages?

It is a form of programming used by modern languages, which consists of transferring the behavior that objects have in real life to the programming code. It is a way of organizing your program combining data and functionality by wrapping it in something called an object. Some of the programming languages that use this object-oriented paradigm are Python, C++, Java, Visual, etc.

As advantages we can mention the following:

- We can divide the programs into pieces, parts, modules or classes to this concept in programming are called modularization.
- It is a code that can be reusable, unlike what happens with procedure-oriented programming, so, if we get to create an application with this object-oriented program and later want to make another similar application we can reuse this code. Now in order to be able to reuse the code of one application in another, we have to know and understand the concept of "inheritance".
- If there is a fault in any line of code, the program continues to work, it is likely that the line of code that generated the error will not perform the

intended task, but the rest of the program will.

- Encapsulation.

Object-oriented programming is responsible for applying programming techniques such as:

- a. Abstraction: Abstraction refers to the process of design and interpretation, which focuses on recognizing the important characteristics of an object; thus filtering out and ignoring the particularities that will not be considered important.

Abstraction focuses on defining the characteristics of an object, which distinguish it from other types. It focuses on what it is, not what it does, and then specifies what it should be implemented in.

For example: We are going to apply abstraction to flowers.

Object: Flowers

Characteristics

- Colors
- Leaves
- Nectar
- Roots

Functionalities:

- Production of seeds and fruits
- Pollination
- Reproduction

- b. Inheritance: some objects share the same properties and methods as other objects, and also add new properties and methods. We

call this inheritance, a class that inherits from another, as happens in real life when in a family group one of the children inherits the skin color of one of the parents, he would be inheriting or having their own characteristics or properties, but also one in common with one of their parents, the same happens in programming.

What does this mean? In a simpler way we can say that when we create a new class, we can implement the same data of the base class. This new class will have more specific data than the original class, which contains a more general view.

In Python, when a class does not inherit another, it must be inherited from an object, which is the main Python class that defines an object.

Once an object has been created, or once the class instance has been made, it is possible to access its method and properties and for that Python uses a very simple syntax which is, the name of the object, followed by the point and the property or the method to which you want to access.

Python also supports a limited form of multiple inheritances.

## **Types of inheritance:**

- Basic Inheritance: This occurs when a class inherits only one base class.
- Multiple inheritance: This occurs when a class inherits two or more base classes.
- Polymorphism: Refers to those different behaviors, which are associated with objects that are different, but may share the same name. When you call an object by its name (which has several objects), its behavior will be based on the object you are currently using.

## **Types of polymorphism:**

- Parametric polymorphism: Parametric polymorphism is the one that allows functions and classes to be written in a generic way, in this way the data of the same can be manipulated without taking into account its type.
- Polymorphism of subtypes: The polymorphism of subtypes is the one in which the subtypes of a type (class) allow to substitute the behavior of the functions of the original type with an own implementation.
- Ad Hoc Polymorphism: Ad Hoc polymorphism refers to those functions, which vary their behavior according to the type of arguments they receive.

What is the terminology or vocabulary that we are going to use in OOP?

We will mention the most commonly used vocabulary to better understand this code:

- Class: Classes are models on which objects are built, that is, models where the common characteristics of a group of objects are written. To better understand this term we will do it by means of analogies, for example, if we have a car, the class would be the chassis and the wheels, since it is a common characteristic among the group of objects that are the cars. If we want to create a Python application that builds cars, the first thing we have to do is to create a class that defines what are the common characteristics of the cars we want to make and this class must have defined within it the construction of a chassis and the construction of four wheels.

In this case, to see another abstraction, let's show an example of classes, but in this case, the class will be a house.

A screenshot of a code editor window titled 'class.py'. The code defines a class named 'house' with attributes 'color', 'doors', 'kitchen', 'bathroom', and 'levels'. It also creates an instance 'house1' and prints a message.

```
1 class house():
2     color="red"
3     doors=6
4     kitchen=True
5     bathroom=3
6     levels=2
7
8 house1=house()
9 print("We create a house")
```

As we can see in the example, the first thing to do is to declare that house is a class, using the reserved word class. Within it, it has some attributes, such as that the color is red, it has six doors, that it does have a kitchen, it has three bathrooms and two floors.



Now the next step is to create a variable and convert it as a class, for it, any name is placed and then the same is entered the name of the class and parentheses. As you can see in the example, house1 is an object, which has a house class and has all the attributes previously explained.

Finally, to know if the class has been created well, a print is made in the console to verify the proper functioning of the program.

- Exemplar of class, which is the same as to speak of the instance of class, and of object belonging to a class, which means that, exemplar, instance and object of class are synonyms; an instance would be an object or exemplar belonging to a class. For example, following with the automobile, we have already talked about that the class defines the characteristics that are common to it, and that define the objects that we are going to use, and we have seen that the class is formed in our example by the chassis and the wheels, but the objects that belong to that class could be different models of automobiles, that share a common characteristic that is to have the same chassis (it should be noted that there are cars that despite belonging to other brands are assembled with identical chassis) and four wheels, so we can have two cars with their own characteristics that are defined within the object itself (the car), such as color, model, weight, seats, steering wheel, then we could say that a specific car is an object belonging to the class, an exemplar of class or that is an instance of class; and another car of another brand would be another different object belonging to the same class, a different instance of the same class, or a different exemplar of the same class.

- Modularization; When we create a complex application applied to objects such as Python, for example, the most normal is that this application is composed of several classes, not a single class, which can also occur, but the normal is that if the application is complex it will be composed of several

classes, the concept of modularization derives from an application can be composed of several classes, for example, applying it to real objects, if we imagine an old sound system, they were made up of several modules, the corresponding to the cassette, equalizer, radio, and disk, which means that the object was made up of several modules. These modules have the advantage to work in an independent way, that is to say, when the radio was damaged, we could use the module of cassette, in programming this leads to an advantage, if you have a program written in Python divided in modules and one of the classes for any reason fails the most probable thing is that the program continues working, just that the class in which you have problems will not be able to carry out its task as with the analogy of the sound equipment.

- Encapsulation; the functioning of a complete class of our object-oriented program is encapsulated, that means that the other classes do not handle any information about each other; going back to the analogy of the previous sound equipment, if we take the equalizer module of the sound equipment, the internal functioning of the equalizer corresponds only to the equalizer, meaning the functioning of the cassette module, nothing knows or understands the equalizer module, and that is what is known as encapsulation. Somehow all the classes are connected so that they function as equipment, but at the same time, each of the classes is encapsulated so that the internal functioning of that class is not accessible from outside. The different parts of a program are connected so that they form part of a team with something called access methods. Creating access methods we get to connect one class with another so that they work as a unit or a team, but these access methods will only have access to certain characteristics of each of the classes. You can access from one class

to another so that they are connected to each other, but there are certain characteristics of each of the classes that are encapsulated so that they are not accessible

How do we build classes, objects, and how do we access the properties and characteristics of an object in Python?

To access the properties and characteristics of an object we use what is known as nomenclature of the point, commonly used in object-oriented programming, to explain what it is, we will do it based on an example.

Suppose that we have given our object a name, we call it myCar, all objects, instances or exemplars must have a name, in order to access the properties of the car in our program we use the nomenclature of the point:

E.g. Syntax: Name of the object. Property = New Value

```
myCar.color="red"
```

This is the syntax in the case of Python that we have to follow if we want to access the property of the object, we use the nomenclature of the point. To access the behavior of the object from the code, we also use the nomenclature of the point.

E.g. Syntax: Object name.behavior

```
myCar.starts()
```

```
myCar.stops()
```

In the following example, you will learn how to access the attributes of a class, through the nomenclature of the point, so you can understand better.

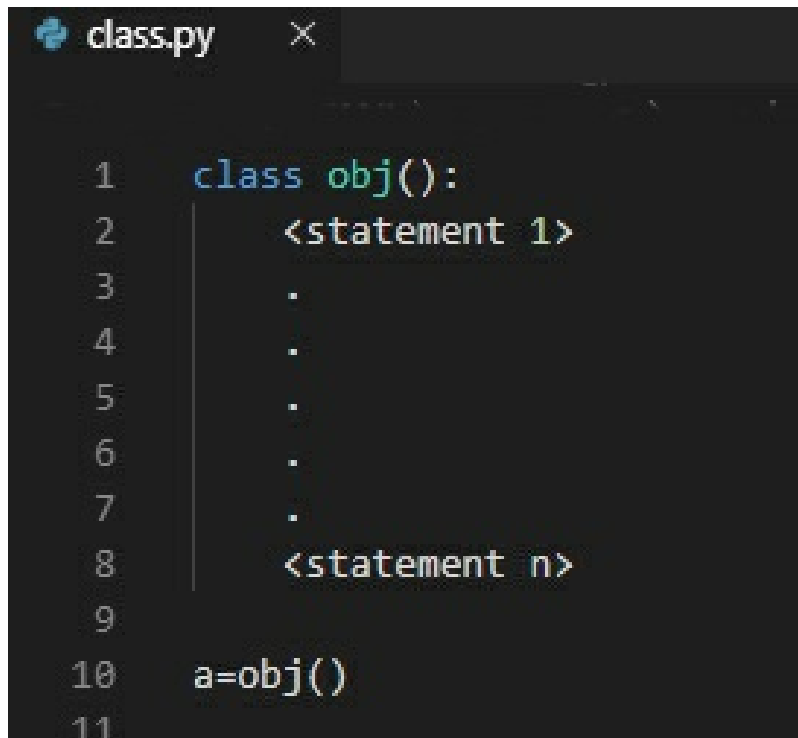
A screenshot of a code editor window titled 'class.py'. The code defines a class 'house' with attributes 'color', 'doors', 'kitchen', 'bathroom', and 'levels'. It then creates an instance 'house1' and prints its attributes using string formatting.

```
1 class house():
2     color="red"
3     doors=6
4     kitchen=True
5     bathroom=3
6     levels=2
7
8 house1=house()
9 print("The house color is "+house1.color+", have "+str(house1.doors)+" doors")
10 print("The house have "+str(house1.levels)+" levels, and "+str(house1.bathroom)+" bathrooms")
```

The first thing we see in this example is the creation of the house class, which has its attributes, like the color, which in this case is red, the doors that have six, or the floors that have two.

Then, we can see how we create our house1 instance, which is of the house type. But we do not only want to stay with the creation of the class, but we also want to access the data that these have, therefore we will make a screen print of the attributes that the house has, as you can see, what we proceed to do, is to concatenate the string that we have written, and concatenate it with the attribute we want, now, to access to it, we have to name the instance, and through the nomenclature of the point, the attribute we want to access.

Now we are going to talk about how to build a code of what a class is; being the class the base to later be able to create objects, examplers or instances that belong to that class.

A screenshot of a code editor window titled 'class.py'. The code is written in Python and shows the syntax for defining a class. It starts with a line number 1 followed by 'class obj():'. Line 2 has an indented '<statement 1>'. Lines 3 through 7 have indented dots representing multiple statements. Line 8 has an indented '<statement n>'. Line 9 is empty. Line 10 has 'a=obj()' and line 11 is empty. The code is color-coded: 'class' is blue, 'obj()' is green, and the statements are in a light green color.

```
1 class obj():
2     <statement 1>
3     .
4     .
5     .
6     .
7     .
8     <statement n>
9
10 a=obj()
11
```

This, more than an example, is an explanation of the syntax to the declaration of a class, because, although we sound repetitive, the declaration of them, is something fundamental in the programming oriented to objects, because as already you must suppose, it is the basis. Therefore, the first thing is to make the statement of the class `nameobject():`, with this, we are creating a class, which is named `nameobject`. Then, inside it, there is a cumulus of statements, which are responsible for giving value to the attributes of the instances and to work with the methods, which will be explained later.

There are cases in which you will ask yourself, but all the houses are red or all the plants have three leaves? And well, obviously the answer is no, for that we are going to work with the builders, they will allow us to give uniqueness to the instances. These are methods, but it is not too much to say since now that these are the ones that allow us to give different values to each instance, at the moment of initializing them, we will see them later.

Although you should already know what an attribute is, since we have

worked with them previously in this chapter, we will now proceed to explain them formally.

#### Attribute:

We define attributes as those values that variables possess within each object. What do we mean by this? Let's imagine the case of a classroom in a school; an attribute that each classroom may possess is the grade the students are in or the age of them.

The word attribute can be used for anything after a point, for example, if we have the expression, `z.real`, `real` is an attribute of the object `z`, what we had previously called as the nomenclature of the point.

The attributes can be read-only, or write-only. In this last case, the assignment to attributes is possible. The attributes of a module can be written: `module.the_answer = 42`, these attributes can also be deleted when desired with the instruction `del`. As, for example: `del module.the_answer`, will eliminate the attribute `the_answer` of the object with module name.

```
class.py  X
1  class house():
2      color="red"
3      dors=6
4      kitchen=True
5      bathroom=3
6      levels=2
7
8  house1=house()
9  house1.color="green"
10 print(house1.color)
11
```

The first thing we do in this example is the definition of the class `house()`, and within it, we define each attribute of the same, like `color`, `bathroom`, `kitchen`, among others.

The next step is the creation of the `house1` instance, which is of the `house` type, as you may have expected, but if you want to paint the house, we will proceed to access the attribute, by means of the instruction `house1.color = "green"` in this way, the color has been changed from `house1` to `"green"`.

To make sure that the color has been changed correctly, a screen print of the `color` attribute of the `house1` instance is made using the nomenclature of the dot.

#### Methods:

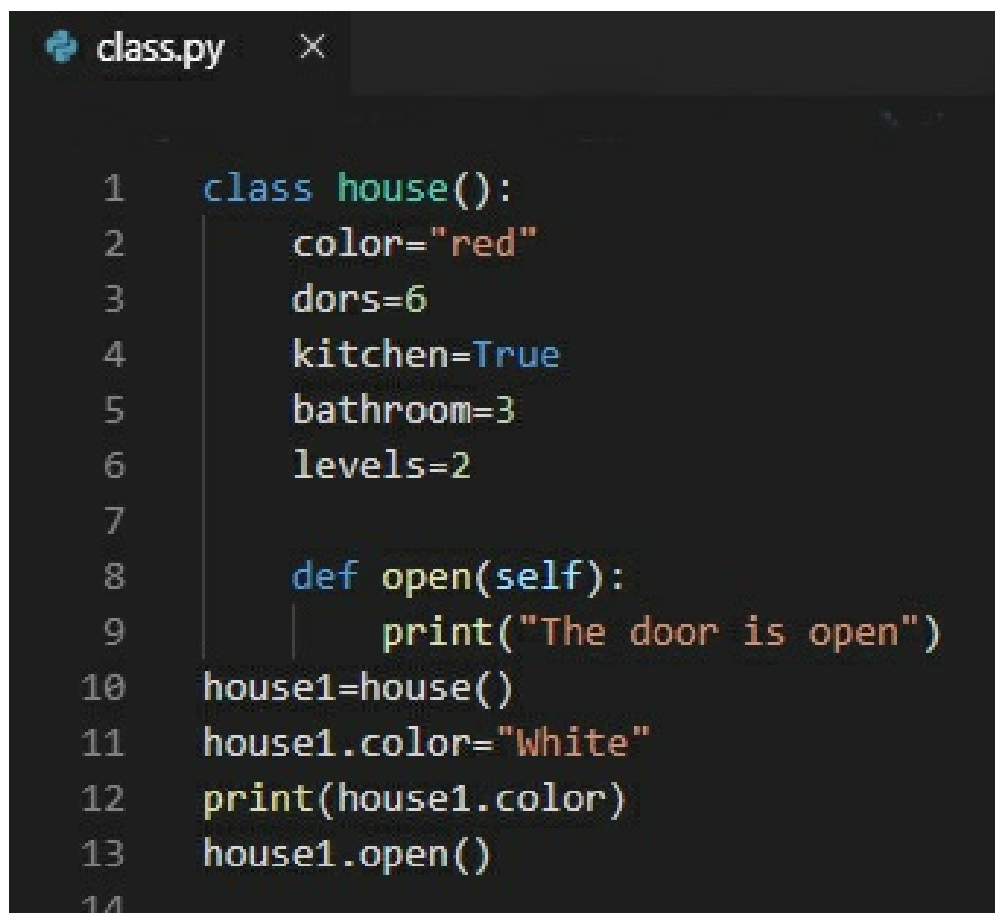
Since we have seen that each object has certain attributes that have certain specific behaviors; now we will call methods to each function created within each class. How is this? So let's go back to the last example of the classroom, it has two methods or actions which are to study and attend classes.

To create a method we use the word `def`, that we already know, but when we write it, there is a keyword that we cannot forget, which is a parameter of the method, this word is `self`, and this one is used to be able to access to the attributes of the class. We can observe that there is a difference between method and function and is that a method is a special function that belongs to the class being created, while a function does not belong to any class.

The characteristics of a method are the reserved word called `def`, name of the function, a default parameter called `self`.

Often, the first argument of the method is called self. this is nothing more than a convention; the name self means nothing to Python, in the sense that it is indifferent to put this as first or last parameter (because the position does not matter, but yes or yes it has to be the word self), but if you do not follow this convention your code could be less readable to other Python programmers.

If the concept of what attributes are, has been well understood, we will be able to observe that working with the methods is very simple, only that when working with them, we have to take into account that means to add behavior to objects, so that you can change attributes when accessing a method or return some value.

A screenshot of a code editor window titled 'class.py'. The code defines a class named 'house' with attributes 'color', 'doors', 'kitchen', 'bathroom', and 'levels'. It also defines a method 'open' that prints 'The door is open'. Below the class definition, an instance 'house1' is created, its 'color' attribute is changed to 'White', and the 'open' method is called.

```
1  class house():
2      color="red"
3      doors=6
4      kitchen=True
5      bathroom=3
6      levels=2
7
8      def open(self):
9          print("The door is open")
10 house1=house()
11 house1.color="White"
12 print(house1.color)
13 house1.open()
14
```

In this example, we see again, how to create the class house, but it



differs from the others because it has created a different method, called open, as you can see, it makes use of the sentence def, then we will put the name of the method, then, within some parentheses, place the parameters, always, but always we must place the self as parameters, you can also add others, but the self can not miss. After this, it is treated as a normal function, as you can see, the method is responsible for sending a message, which communicates that the door is open.

Later you can see how to create the instance house1, which is class house, one of the actions that are done on house1, is to change the color of it, the new color is white, another important action is access to the methods, and as you can see, it is also done through the nomenclature of the dot.

## **Constructors:**

Now that you have basic knowledge of classes, you should ask yourself if all the instances of one class are the same as the others, because if this were true, everything would be very monotonous, and the OOP would not be very powerful, as it really is, for this reason, the constructors have been created, which initialize the classes with values that the programmer wants.

A constructor, is the one that creates or assigns values to the initial attributes of an instance, and to do this, it is necessary to use a method, moreover, a constructor is a method of a class, to use it, we make use of the reserved word `__init__(self, a, b, c, ...)`, being a, b, c, the parameters that we want to initialize, since they are values that we can introduce as users and thus be able to assign the values to the attributes, in order to achieve diversity in our objects.

```
class.py  X
1  class house():
2      def __init__(self, color, dors, kitchen, bathroom, levels):
3          self.color=color
4          self.dors=dors
5          self.kitchen=kitchen
6          self.bathroom=bathroom
7          self.levels=levels
8
9      def open(self):
10         print("The door is open")
11
12     def paint(self, c):
13         self.color=c
14 house1=house("blue", 5, True, 2, 1)
15 print(house1.color)
16 house1.paint("black")
17 print(house1.color)
18 house1.open()
19
```

In this example, we can already see how things change and become more fun, the first thing is that a constructor was used, the same has as parameters the self, color, doors, kitchen, among others. After the constructor's statement we use the word self and place the corresponding value, as you can see between lines three and seven, for example, in the instruction of line 3, what is said is that the variable color of that specific instance, is going to have the value, what the argument has valued when the instance was initialized.

Then you can see how the open method was created, that method, only shows on screen that the door has been opened; the other method that has been created, in this case, is one called paint, which is responsible for changing the color of that instance, this was done using the sentence self.color, to specify that the instance is going to change.

Subsequently, the house1 instance is created, and it is given as

argument "blue", 5, True, 2, 1 to the constructor so that he initializes his attributes in those specific values and thus to be able to remove the monotony that we had before.

After having created the instance, the color of the house is printed in screen, or well, better said, of the house1 instance, at this moment, it should print the string "blue", then, it makes use of the paint method, to change the color of the instance, to the black color, to verify that the color has been changed correctly, the color of the house1 instance is printed in screen, and for this case, the string "black" should appear in console.

Finally, the open method is used, so that it appears on the screen that the doors are open.

Since we know how to make use of the builders, we can apply the concept of inheritance previously applied, so that a class related to it, inherits, behaviors and attributes of its parent class.

```

class.py x
1  class house():
2      def __init__(self, color, dors, kitchen, bathroom, levels):
3          self.color=color
4          self.dors=dors
5          self.kitchen=kitchen
6          self.bathroom=bathroom
7          self.levels=levels
8
9      def open(self):
10         print("The door is open")
11
12     def paint(self, c):
13         self.color=c
14 class apartment(house):
15     def __init__(self, color, dors, kitchen, bathroom, levels, stairs, elevator):
16         house.__init__(self, color, dors, kitchen, bathroom, levels)
17         self.stairs=stairs
18         self.elevator=elevator
19     def elevatoron(self):
20         if(self.elevator==True):
21             print("The elevator is in PB")
22         else:
23             print("You dont have elevator")
24 house1=house("blue", 5, True, 2, 1)
25 print(house1.color)
26 house1.paint("black")
27 print(house1.color)
28 house1.open()
29 apartment1=apartment("orange", 2, True, 2, 1, True, True)
30 apartment1.elevatoron()
31 apartment1.open()
32

```

In this example, we can see how inheritance works, since we have already seen the first lines of the code, it is not necessary to explain them in-depth, since what we do is create the house class, initialize the house constructor and create some methods such as paint and open.

Then, we define the second class, which is apartment. Why do we say that it is a daughter of house class? Well, we already know that an apartment is a house, but a house doesn't have to be an apartment, it can be a mansion or a townhouse, therefore it doesn't have to be an apartment, whereas in the opposite case, that is always true.

As we can see, at the moment of defining the apartment class, we

enter as parameter, the parent class, in this case, house. Then we start the constructor, which should have the word reserved `__init__`, and put the parameters self and all that those that are missing, with this we mean both the parameters of entry of the class house, plus the additional ones of the class apartment, as it can be stairs, and elevator, since the apartments can have stairs or not, in an analogical way it is done with the elevators. They must be initialized as well. Later, as we can see, we will call the function of constructors of the parent class, so that the same ones are initialized, using the nomenclature of the dot, then, it is when the other attributes that are not in house, like stairs or elevator were initialized. A method that was created within the apartment class, was the `elevatoron()` which, depending on whether the instance created has an apartment or not, when calling this method, will appear on screen that the elevator is on the ground floor.

Already after having created all the classes, we proceed to create the instances, to verify that the classes were created correctly, in a similar way to how the object house1 was created, this one is created, with the same values of the previous example, the color of the object is printed, then the function `paint()` is used, and the color is changed to black, and finally the door is opened. Then, the other object that creates the apartment1, which has as arguments the orange color, two doors, True on kitchen, two baths, one floor, stairs and also has elevator. In the program is called the function `elevatoron()` to call the elevator and reach the ground floor, and show the user that this in PB, then proceeds to open the doors of the apartment with the help of the `open` method.

As we can see, object-oriented programming is extremely useful, since it allows us to see the problems of programming as problems of real-life and make solutions as if they were objects with which we run into in

everyday life, for that reason, we strongly recommend programming this way, as it reduces the number of lines to use, and makes the code reusable, in addition to being more understandable.

# Chapter 7: Modules

The modules are files with extension `.py` (that we have been using until now), additionally a module instead of having extension `py`, it also has the extension `.pyc`; (what would be a compiled Python file), a module can also be a file written totally in C for those that are using CPython.

Modules have their own namespace, and in addition, they can contain variables, functions, classes and even contain other modules, a module within another or a submodule.

## How useful are the modules?

The modules are mainly used to organize and reuse the code, this leads us to two terms that are fundamental in OOP as are modularization and reuse.

When we want to make a complex application and we need a code to reuse it since it was previously programmed in another application, this is one of the advantages that modules have, they allow us to reuse our code in different applications.

The modularization, in this case, we divide the module in codes, in small parts, when we realize a complex application, we can do it in a single file of thousands of lines of code, or we can divide it in small parts, in small files with a smaller number of lines of codes since it is always going to be easier for us to handle.

## How can we create a module in Python?

We can easily create a module through the file extension `.py`, once created the file we can save it where we want, this is what we know as import.

Python provides us with a large number of modules in its standard library, in the official Python manual we can find this library through the following link: <http://docs.python.org/modindex.html>.

Inside a module, its name is available in the value of the global variable `_name_`.

## **Import Sentence**

A module can contain executable statements and function definitions; with these statements, we are able to initialize the module. They are executed only the first time the module is in an import statement.

Modules can import other modules. It is actually usual to place all import declarations at the beginning of the module (or script, for that matter). The names of the imported modules will be placed in the global namespace of the importing module.

The import sentence has the following syntax

Once the interpreter finds the import statement, it will import the module if it is present in the search path, where a search path is nothing more than a list of directories that the interpreter searches for before importing a module.



# Chapter 8: File handling

The Python programming language allows us to work on two different levels when we refer to file systems and directories. One of them is through the module `os`, which facilitates us to work with the whole system of files and directories, at the level of the operating system itself.

The second level is the one that allows us to work with files, this is done by manipulating their reading and writing at the application level, and treating each file as an object.

In python as well as in any other language, the files are manipulated in three steps, first they are opened, then they are operated on or edited and finally they are closed.

## What is a file?

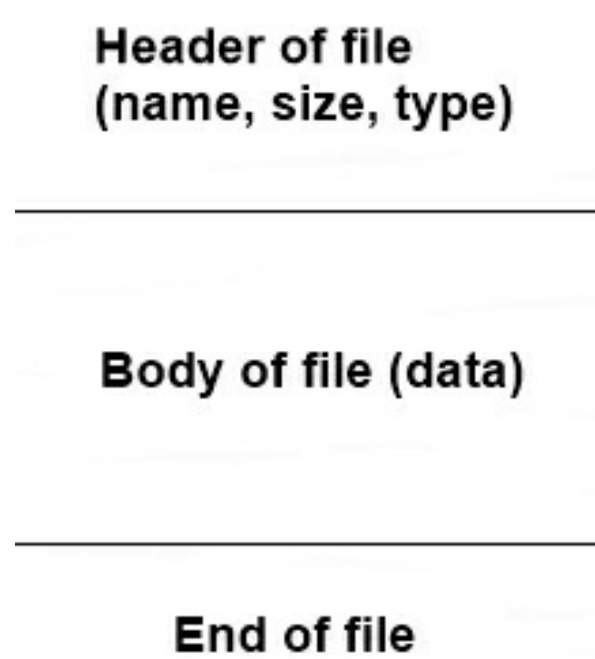
A python file is a set of bytes, which are composed of a structure, and within this we find in the header, where all the data of the file is handled such as, for example, the name, size and type of file we are working with; the data is part of the body of the file, where the written content is handled by the editor and finally the end of the file, where we notify the code through this sentence that we reach the end of the file. In this way, we can describe the structure of a file.

The structure of the files is composed in the following way:

- File header: These are the data that the file will contain (name, size, type)
- File Data: This will be the body of the file and will have some content written by the programmer.

- End of file: This sentence is the one that will indicate that the file has reached its end.

Our file will look like this:



## How can I access a file?

There are two very basic ways to access a file, one is to use it as a text file, where you proceed line by line, the other is to treat it as a binary file, where you proceed byte by byte.

Now, to assign a variable a file type value, we will need to use the function `open ()`, which will allow us to open a file.

## Open() function

To open a file in Python, we have to use the `open()` function, since this will receive the name of the file and the way in which the file will be opened as parameters. If the file opening mode is not entered, it will open in the default way in a read-only file.

We must keep in mind that the operations to open the files are limited because it is not possible to read a file that was opened only for writing, you cannot write to a file which has been opened only for reading.

The open () function consists of two parameters:

- It is the path to the file we want to open.
- It is the mode in which we can open it.

Its syntax is as follows:

```
)  
1  function = open("file.txt", "w")  
2  function.write()  
3  function.close()
```

Of which the parameters:

**File:** This is an argument that provides the name of the file we want to access with the open() function, this is what will be the path of our file.

The argument file is considered a fundamental argument, since it is the main one (allowing us to open the file), unlike the rest of the arguments which can be optional and have values that are already predetermined.

**Mode:** The access modes are those that are in charge of defining the way in which the file is going to be opened (it could be for reading, writing, editing).

There are a variety of access modes, these are:

r	This is the default open mode. Opens the file for reading only
r+	This mode opens the file for its reading and writing

rb	This mode opens the file for reading only in a binary format
w	This mode opens the file for writing only. In case the file does not exist, this mode creates it
w+	This is similar to the w mode, but this allows the file to be read
wb	This mode is similar to the w mode, but this opens the file in a binary format
wb+	This mode is similar to the wb mode, but this allows the file to be read
a	This mode opens a file to be added. The file starts writing from the end
ab	This is similar to mode a, but opens the file in a binary format
a+	This mode is pretty much like the mode a, but allows us to read the file.

In summary, we have three letters, or three main modes: r,w and a. And two submodes, + and b.

In Python, there are two types of files: Text files and plain files. It is very important to specify in which format the file will be opened to avoid any error in our code.

## Read a file:

There are three ways to read a file:

1. `read([n])`
2. `readlines()`
3. `readline([n])`

Surely at this point, we have the question of what is meant by the letter `n` enclosed in parentheses and square brackets? It's very simple, the letter `n` is going to notify the bytes that the file is going to read and interpret.

## Read method ([ ])

```
1 myfile = open("D:\\pythonfile\\mypythonfile.txt","r")
2 myfile.read(9)
```

There we could see that inside the `read()` there is a number 9, which will tell Python that he has to read only the first nine letters of the file

## Readline(n) Method

The `readline` method is the one that reads a line from the file, so that the read bytes can be returned in the form of a string. The `readline` method is not able to read more than one line of code, even if the byte `n` exceeds the line quantity.

Its syntax is very similar to the syntax of the `read()` method.

```
1 myfile = open("D:\\pythonfile\\mypythonfile.txt","r")
2 myfile.readline()
```

## Readlines(n) Method

The `readlines` method is the one that reads all the lines of the file, so that the read bytes can be taken up again in the form of a string. Unlike the `readline` method, this one is able to read all the lines.

Like the `read()` method and `readline()` its syntax are very similar:

```
1 myfile = open("D:\\pythonfile\\mypythonfile.txt","r")
2 myfile.readlines()
```

Once we have opened a file, there are many types of information (attributes) we could get to know more about our files. These attributes are:

`File.name`: This is an attribute that will return the name of the file.

`File.mode`: This is an attribute that will return the accesses with which we have opened a file.

`file.closed`: This is an attribute that will return a "True" if the file we were working with is closed and if the file we were working with is still open, it will return a "False".

## Close() function

The `close` function is the method by which any type of information that has been written in the memory of our program is eliminated, in order to proceed to close the file. But that is not the only way to close a file; we can also do it when we reassign an object from one file to another file.

The syntax of the `close` function is as follows:



```
1 mvfile.close()  
2
```

## What's a buffer?

We can define the buffer as a file which is given a temporary use in the ram memory; this will contain a fragment of data that composes the sequence of files in our operating system. We use buffers very often when we work with a file which we do not know the storage size.

It is important to keep in mind that, if the size of the file were to exceed the ram memory that our equipment has, its processing unit will not be able to execute the program and work correctly.

What is the size of a buffer for? The size of a buffer is the one that will indicate the available storage space while we use the file. Through the function: `io.DEFAULT_BUFFER_SIZE` the program will show us the size of our file in the platform in a predetermined way.

We can observe this in a clearer way:

```
1  import io
2      print("Default buffer size:"io.DEFAULT_BUFFER_SIZE)
3      file= open("Myfile.txt", mode= "r", buffering=6)
4      print(file.line_buffering)
5  file_contents=file.buffer
6  for line in file_contents
7      print(line)
```

## Errors

In our files, we are going to find a string (of the optional type) which is going to specify the way in which we could handle the coding errors in our program.

Errors can only be used in txt mode files.

These are the following:



Ignore_errors()	This will avoid the comments with a wrong or unknown format
Strict_errors()	This is going to generate a subclass or UnicodeError in case that any mistake or fail comes out in our code file

## Encoding

The string encoding is frequently used when we work with data storage and this is nothing more than the representation of the encoding of characters, whose system is based on bits and bytes as a representation of the same character.

This is expressed as follows:

```
1 string.encode(encoding="UTF-8", errors="strict")
2
```

## Newline

The Newline mode is the one that is going to control the functionalities of the new lines, which can be '\r', " ", none, '\n', and '\r\n'.

The newlines are universal and can be seen as a way of interpreting the text sequences of our code.

1. The end-of-line sentence in Windows: "\r\n".
2. The end-of-line sentence in Max Os: "\r".
3. The end-of-line sentence in UNIX: "\n"

On input: If the newline is of the None type, the universal newline

mode is automatically activated.

Input lines can end in `"\r"`, `"\n"` or `"\r\n"` and are automatically translated to `"\n"` before being returned by our program. If their respective legal parameters when coding are met, the entry of the lines will end only by the same given string and their final line will not be translated at the time of return.

On output: If the newline is of the `None` type, any type of character `"\n"` that has been written, will be translated to a line separator which we call `"os.linesep"`.

If the newline is of the type `" "` no type of translator is going to be made, and in case the newline meets any value of which are considered the legal for the code, they will be automatically translated to the string.

Example of newline reading for `" "`.

```
1 string.encode(mode="r", newline= " ")
2
```

Example of newline reading for `none`:

```
1 string.encode(mode="w", newline= "none")
2
```

## Manage files through the `"os"` module

The `"os"` module allows us to perform certain operations, these will depend on an operating system (actions such as starting a process, listing files in a folder, end process and others).

There are a variety of methods with the "os" module which allow us to manage files, these are:

os.makedirs()	This method of the “os” module will create a new file
os.path.getsize()	This method of the “os” module will show the size of a file in bytes.
os.remove(file_name)	This method of the “os” module will delete a file or the program
os.getcwd ()	This method of the “os” module will show us the actual directory from where we will be working
os.listdir()	This method of the “os” module will list all the content of any folder of our file
os.rename (current_new)	This method of the “os” module will rename a file
os.path.isdir()	This method of the “os” module will transfer the parameters of the program to a folder
os.chdir()	This method of the “os” module will change or update the direction of any folder or directory
os.path.isfile()	This method of the “os” module will transform a parameter into a file.

**Xlsx files:** xlsx files are those files in which you work with spreadsheets, how is this? Well, this is nothing more than working with

programs like Excel. For example, if we have the windows operating system on our computer, we have the advantage that when working with this type of files, the weight of it will be much lighter than other types of files.

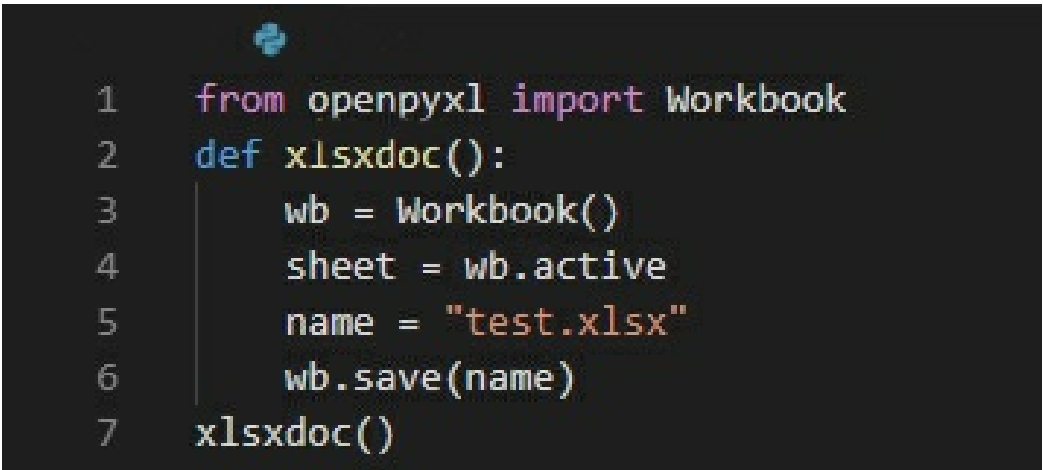
The xlsx type files are very useful when working with databases, statistics, calculations, numerical type data, graphics and even certain types of basic automation.

In this chapter we are going to learn to work the basic functionalities of this type of files, this includes creating files, opening files and modifying files.

To start this, first we will have to install the necessary library; we do this by executing the command "pip3 install openpyxl" in our Python terminal.

Once executed this command it is going to download and install the openpyxl module in our Python files, we can also look for documentation to get the necessary information about this module.

Create an xlsx file: To create a file with this module, let's use the openpyxl() Workbook() function.

A code editor window with a dark background and light blue, green, and orange syntax highlighting. The code is as follows:

```
1  from openpyxl import Workbook
2  def xlsxdoc():
3      wb = Workbook()
4      sheet = wb.active
5      name = "test.xlsx"
6      wb.save(name)
7  xlsxdoc()
```

This is the first step that we will do to manage the files of the type `xlsx`, we can see that first we have created the file importing the function `Workbook` of the module `openpyxl`; followed by this to the variable `wb` we have assigned the function `Workbook()` with this we declare that this will be the document with which we are going to work (we create the object in the form of a worksheet in this format). Once this is done, we activate the object whose name is `wb` in order to assign it a name and finally save the file.

## Add information to the file with this module:

In order to add information to our file, we will need to use another type of functions that come included with the object, one of them is the `append` function.



```
1  from openpyxl import Workbook
2  def xlsdoc():
3      wb = Workbook()
4      sheet = wb.active
5      sheet["B4"] = "Goodnight"
6      name = "test.xlsx"
7      wb.save(name)
8  xlsdoc()
```

We can observe that this is similar to the last example that we needed to create a document, for it we did the usual steps: we created in the function `xlsdoc()` the object `wb`, we activated the object and there we added the information. In this new space we will need to know the specific position in which we are going to write, in this case, we will write in the fourth box of the second row "B4" and these will be matched with a string that says "goodnight". The final steps are exactly the same as the last example, therefore, we will place the name and save it with the `save` command.

There is a simpler way to write and enter data, we can do this through the function `append()`

```
1  from openpyxl import Workbook
2  def xlsdoc():
3      wb = Workbook()
4      sheet = wb.active
5      messages = ("Hello" , "good morning", "goodnight" )
6      sheet.append = (messages)
7      name = "test.xlsx"
8      wb.save(name)
9  xlsdoc()
```

We can observe that we have created the document "test.xlsx" with the steps that we explained previously, we can observe that we have created a tuple called messages, this tuple has three items that are:

"Hello", "goodmorning", "goodnight".

Once the tuple is created, we use the `append` function, which will allow us to attach all the information contained in the tuple messages and finally save the document with the `save` function.

The `append()` function only admits iterable data, what does this mean? This refers to the data of type arrangements, tuples since, if they are not entered in this way, our program will return an error.

## Read documents in xlsx

```
1  from openpyxl import Workbook
2  name = "test.xlsx"
3  def xlsxdoc():
4      wb = load_Workbook(name)
5      sheet = wb.active
6      file1 = sheet["C1"].value
7      file2 = sheet["C2"].value
8      file3 = sheet["C3"].value
9      print(file1)
10     print(file2)
11     print(file3)
12  xlsxdoc()
```

Let's go back to our first example to get information from xlsx files, we could see that, for this, we imported the `load_workbook` class. The first thing we need to know is the name of the file we want to open and for this, we created the variable with the name.

It is important that the files are located in the same folder in which the program is stored, because otherwise the program will throw us an error. Inside the function `xlsdoc()` we will create the object `wb` that will be with which we are going to work, followed by this the object "sheet" is created which is going to represent the sheet that we are going to use.

Once all this is done, we are going to request the information of the specific boxes "C1", "C2", "C3" next to the function value, to validate that the information that we acquire is real, we print all the information requested.

# Handling PDF files

It is known that the initials of this type of file are: "Portable Document Format", which have grown significantly over the years, are mostly used in business and education. This is due to the fact that they provide a great amount of benefits in which its security is highlighted, allowing to add access keys to control who can edit the document and even add a watermark to it to avoid plagiarism of information.

Other outstanding data is that these documents can be seen from any device since it is not necessary to have a specific program; in addition, the weight of the files is much lower since these texts are compressed, unlike Word documents.

A disadvantage of PDF files could be that they are not easy to edit once they have been created.

In this chapter, we will only learn how to create PDF files.

To create a PDF file the first thing we will have to do is to download the library through the command "Pip3 install fpdf", followed by this we can proceed to create our document:

```
1  from fpdf import FPDF
2
3  pdfdoc = FPDF()
4  pdfdoc.set_font('Times New Roman', 'B', 12)
5  pdfdoc.add_page()
6  pdfdoc.cell(12, 10, "First PDF program", 5, 6, "C")
7  pdfdoc.output("first PDF", 'F')
```

This is a simple level example, but at the same time, it is much more difficult than other types of files. To start a document you need a lot of



commands, for it we will import the FPDF class from the fpdf library, followed by this we create the pdfdoc object and this will be the pdf document. Once created this document, we will have to customize the formats, size, and style of the letters we are going to use. To do this we use the command `set_font`.

In this case, the type of Font that we are going to use is going to be Times New Roman, with bold style and a size of 12.

Followed by this we will add a page through the command `add_page()`, since we will need a page on which to write and the function `fpdf` does not create a blank page by default. Then, we're going to insert information with the `cell()` function which contains a set of very important arguments.

The cell function will contain the width and height that the cell will occupy, it must include the message that will be written in string format, in case it is required that the edges to come with some detail included we must add 1 since the 0 is by default and does not allow anything to be inserted.

If you want to add a cell below or located to the right, you place a 0 and otherwise is placed 1, if you want the text to be centered to the right, left, up or down a string will be placed and if you want in it to be centered you write C

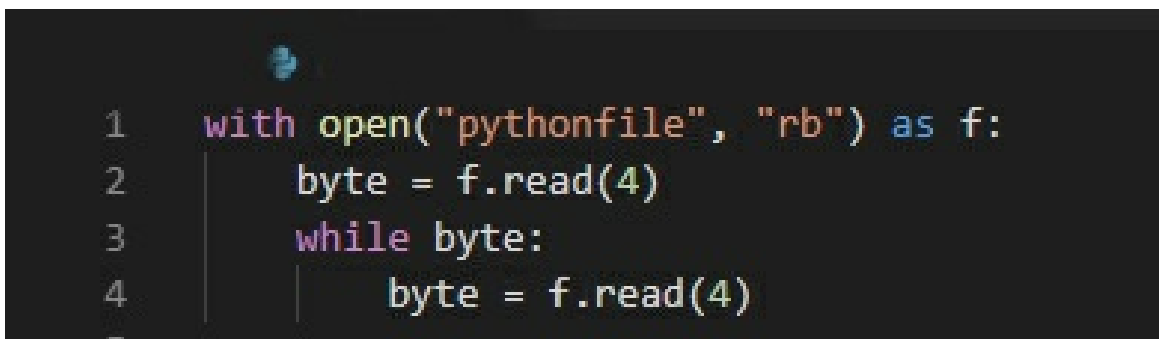
Finally, we will have to save the document through the command `output()`, and the arguments that will go with them will be the name of the file (with the ".pdf" included since we want a file in pdf) and then a string "F".

## **Managing BIN files**

As we saw earlier, not all files are necessarily text files. These same ones can be processed by lines and even there exist certain files that when being processed, each byte contains a particular meaning for the program; for that reason, they need to be manipulated in their specific format.

A clear example of this are the files in Binary, to work with this type of files is no more than adding a b in the space of the parameter mode.

For example:

A screenshot of a code editor with a dark background. It shows a Python script with four lines of code. Line 1: `with open("pythonfile", "rb") as f:`. Line 2:  `byte = f.read(4)`. Line 3:  `while byte:`. Line 4:  `byte = f.read(4)`. The code is color-coded: `with` is purple, `open` is green, `"pythonfile"` is orange, `"rb"` is orange, `as` is blue, `f` is green, `byte` is green, `=` is white, `f.read(4)` is green, `while` is purple, and `:` is white. There is a small blue cursor icon at the end of line 1.

```
1  with open("pythonfile", "rb") as f:
2      byte = f.read(4)
3      while byte:
4          byte = f.read(4)
```

When we handle a binary file, it is very important to know the current position of the data we need in order to modify it. If you don't know the current position, the `file.tell()` function will indicate the number of bytes that have elapsed since we started the file.

In case you want to modify the current position in the file, we use the function `file.seek(star, from)` which will allow us to move a certain amount of bytes from start to finish.

# Conclusion

Thank you for making it through to the end of *Python programming for beginners: The ultimate crash course to learn python computer language faster and easier*, we really hope that you found it informative and that you were able to approach all of the tools here provided that you needed to achieve your goals of learning Python programming language

Now that you have finished this book, you should be able to do a lot of programs for different situations. The next step is to keep practicing a lot, in order to become a master of Python. While programming, sometimes you might think that some things are impossible to code, or that you are not good enough to do them. But that is not right; you just have to think a lot in order to make it happen. Also while programming you may find that your code or program is not working, do not worry, even the smartest people write codes that do not work at the beginning. You just have to keep trying.

As you know, nowadays technology is everywhere and so programming is, our recommendation is that you try to code and solve problems of your daily activities in order to broaden your vision of the world since all electronics have hundreds and hundreds of lines of codes on it.

Good luck with programming!!

```
if: (you_have_doubts)
    print("Read_The_Book_Again")
else:
    print("GOODBYE")
```

# **Networking for Beginners**

---

*Easy Guide to Learn Basic/Advanced  
Computer Network, Hardware,  
Wireless, and Cabling. LTE, Internet,  
and Cyber Security*

---

By Dylan Mach



© Copyright 2019 by Dylan Mach - All rights reserved.

The content contained within this book may not be reproduced, duplicated or transmitted without direct written permission from the author or the publisher.

Under no circumstances will any blame or legal responsibility be held against the publisher, or author, for any damages, reparation, or monetary loss due to the information contained within this book. Either directly or indirectly.

**Legal Notice:**

This book is copyright protected. This book is only for personal use. You cannot amend, distribute, sell, use, quote or paraphrase any part, or the content within this book, without the consent of the author or publisher.

**Disclaimer Notice:**

Please note the information contained within this document is for educational and entertainment purposes only. All effort has been executed to present accurate, up to date, and reliable, complete information. No warranties of any kind are declared or implied. Readers acknowledge that the author is not engaging in the rendering of legal, financial, medical or professional advice. The content within this book has been derived from various sources. Please consult a licensed professional before attempting any techniques outlined in this book.

By reading this document, the reader agrees that under no circumstances is the author responsible for any losses, direct or indirect, which are incurred as a result of the use of the information contained within this document, including, but not limited to, — errors, omissions, or inaccuracies.

# Table of Contents

[Introduction](#)

## [\*\*Chapter 1: Introduction to Machine Learning and Computer Networking\*\*](#)

[Computer Networking](#)

[History of Computer Networks](#)

[Components of Computer Networking](#)

[Routers](#)

[Network Interface Card](#)

[Protocols](#)

[Types of Computer Networks](#)

[Local Area Network \(LAN\)](#)

[Personal Area Network \(PAN\)](#)

[Metropolitan Area Network \(MAN\)](#)

[Wide Area Network \(WAN\)](#)

[Machine Learning](#)

## [Machine Learning Vs. Computer Programming](#)

[General Steps in Machine Learning](#)

[Collection and Preparation of Data](#)

[Selection of Instructing Models](#)

[Evaluation of Models](#)

[Types of Machine Learning Algorithms](#)

[Supervised Algorithms](#)

[Unsupervised Algorithms](#)

[Reinforcement Algorithms](#)

[Applications of Machine Learning](#)

## [\*\*Chapter 2: Properties of a Computer Network\*\*](#)

### [\*\*Properties of Computer Network\*\*](#)

[Uses of Computer Networks](#)

### [Use in Business Applications](#)

[Computer Networks: Mobile Users](#)

[More Information on Types of Computer Networks](#)

[Basic Elements of Computer Networks](#)

[Choosing a Suitable Computer Network](#)

## [\*\*Chapter 3: Easy Guide to Learn Basic Computer Network\*\*](#)

[The Important Components of a Computer Network](#)

[The Classification of Computer Network](#)  
[Basing on Geographical Location](#)  
[Based on the Access Type](#)  
[Basing on Relationships between End Devices](#)  
[The Internetwork](#)

## **[Chapter 4: What Are the Basic Cybersecurity Fundamentals?](#)**

[What Is Cybersecurity?](#)  
[Botnets Attacks](#)  
[Crypto-currency Hijacking](#)  
[Ransomware](#)  
[Phishing](#)  
[Social Engineering Attacks](#)  
[The History of Cybersecurity](#)  
[The Importance of Cybersecurity](#)  
[What Are Cybersecurity Fundamentals?](#)

## **[Chapter 5: What Are the Concepts of Networking?](#)**

[Components of Network](#)  
[Classification Based on Access Type](#)  
[Classification Based on Relationships between Relevant Devices](#)  
[Networking Plan](#)  
[Networking Types and Structures](#)  
[Networking Layout and Topologies](#)  
[Networking Topology – Logical Vs. Physical](#)  
[Classification of Computer Networks](#)  
[Classification Based on Geographical locations](#)  
[Networking Layers and Protocols](#)  
[Transmission Control Protocol](#)

## **[Chapter 6: Information Tech Guide](#)**

[Understanding Information Technology](#)  
[Hardware](#)  
[1. CPU](#)  
[2. Peripherals](#)  
[Wireless and LTE](#)  
[LTE \(Long Term Evolution\)](#)  
[An Overview of LTE](#)  
[LTE Requirements](#)  
[Standard Definitions on Wireless and LTE](#)

[Cabling](#)

[Types of Cable Network](#)

[Choosing a Cable Network](#)

[Advantages of Cabling Network](#)

[Cybersecurity](#)

[Significance of Cybersecurity](#)

[How to Managing Cyber Security](#)

[Network Address](#)

[Functions of the IP protocol](#)

[Private and Public IP Addresses](#)

[Assigning of IP Addresses](#)

[Data Transmission](#)

[Importance of Networks](#)

[Other Similarities](#)

## **[Chapter 7: What Are the Best Network Monitoring Tools?](#)**

[Basic Fundamentals of Computer Networking](#)

[The Internet Protocol](#)

[Understanding Cyber Security](#)

## **[Chapter 8: Types of Firewall](#)**

[How Do Firewalls Work?](#)

[The Types of Firewalls](#)

[The Application of This Kind of Firewalls](#)

[The Stateful Multilayer Firewall](#)

[The Proxy Firewalls](#)

[The Software Firewalls](#)

[Hardware Firewall](#)

[The Application Firewall](#)

[The Next Generation Firewalls](#)

[The Stateful Inspection Firewall](#)

[Telephony-Related Firewalls](#)

## **[Chapter 9: Understanding Cybersecurity](#)**

[Importance of Cybersecurity](#)

[Data Security Measures and Its Importance](#)

[What Does Data Security Mean?](#)

[Data Security Technologies](#)

[Types of Data Security](#)

[Securing Data](#)



[Importance of Data Security](#)

## [\*\*Chapter 10: Types of Cyber-Attacks and How to Prevent Them\*\*](#)

[Types of Cyber Attacks](#)

[Malware Attacks](#)

[Eavesdropping Attacks](#)

[Cross-Site Scripting Attacks](#)

[Password Attacks](#)

[Drive-By Attack](#)

[Phishing Attacks](#)

[Man-In-The-Middle Attacks](#)

[SQL Injection Attack](#)

[How to Prevent Cyber Attacks](#)

# Introduction

Congratulations on downloading Networking for Beginners, and thank you for doing so. The world is becoming digital, and everyone has to keep up with the constant emerging technologies. However, you can't involve in any type of technology without understanding the basics at first. That is, you have to initially learn the principles of different computer components before sinking deeper into complex activities such as computer programming and more.

The following chapters will discuss all you need to know about networking in the computing world essential for those who are venturing into the industry. Some may have limited knowledge about networking, but you are likely to become a pro soon when using this guide. Therefore, you will learn about different protocols used in networking as well as interconnection and the internet, among others. There are fundamental concepts in networking and may also include other forms of operations related to computer networks.

That said, you will learn about computer networking and understand how the modern telecommunication network facilitates the sharing of resources among machines. Networking is a fundamental field of computer study which allows for computers to become interconnected globally. Also, you will learn about machine learning as a form of algorithms and statistical methods of how machines acquire an ability to perform a given task. Machine learning is a broad topic but essential for beginners, especially when they want to learn about how computers are capable of making decisions on situations like humans.

There are plenty of books on this subject on the market, thanks again for choosing this one! Every effort was made to ensure it is full of as much useful information as possible. Please enjoy!

# **Chapter 1: Introduction to Machine Learning and Computer Networking**

Machine learning and computer networking is both an essential field of study in computing but accompany different concepts. That is, they are topics that represent a similar study area on the contrary cover various sections of computer systems. In this case, machine learning entails computer algorithms and statistical models which facilitate the process of machine learning on data fed, the identity of suitable patterns, and the selection of the most favorable outcome. On the other hand, computer networking deals with the connections and interconnection of different computers globally, therefore, enabling data sharing, resource management, and user applications.

## **Computer Networking**

Computer networking is the computing knowledge of studying and analyzing the communications techniques of computing devices or systems connected or interconnected together to exchange information or resources. A computer network is therefore defined as a group of computers allied together to communicate and share data and resources. Networking in computers solely depends on theoretical and practical applications of computer engineering, sciences, and telecommunication and information technologies. As to build computer networking between machines, an individual is required to have a router, network card, and specific protocols.

## **History of Computer Networks**

Computer networking began during the rise of computers in the 1950s but utilized closed network systems used by the military. Unlike the modern networking systems, the late 1950s saw the use of military radars, which transitioned into MOS transistors consisting of transceivers, routers telecommunication circuits, and base station modules. Different developers proposed various forms of computer networking, including the introduction of a telephone switch in 1965 by the Western Electric. The first critical progress of computer networks began in the 1970s, which saw multiple modifications of devices used today to promote networking.

One of them includes the Xerox PARC, which refers to the use of Ethernet,

the X.25 used expanding IP network coverage and the creation of a host. From the supply of 50kb/s circuit in 1969 to the current 10mb/s to 100mb/s, the networking industry has undergone significant changes. However, the improvement is predicted to increase in the future, seeing the fastest modes of networks emerge, therefore building the computer networking sector. Besides, the higher speeds of the system have already been experienced with 2018. And this is because of the introduction of rates of up to 400 GB/s through the use of Ethernet fiber cables.

## Components of Computer Networking

### Routers

A router is the most common network device which forwards data packets in computer networks with a primary function of directing traffic on the internet. The packets such as web pages are transmitted from one router to another comprising of an internetwork while waiting to reach a desirable node destination. Routers are commonly used in homes and small networks and perform using network cables rather than installed drivers and connected to the computers by use of USBs or specific wires.

Routers may either be wireless or consist of cables linked by ports to allow for devices to connect to the internet. They usually linked to the modem, for instance, fiber and DSL, or WAN ports via network cables to facilitate the connection. Based on your desirable network link, your network speed will vary, with some regulating the rate you receive per individual router. Besides, routers may follow specific IP addresses depending on the internet connection, with the private addresses being the primary gateway default one for different devices in the network. Multiple links to one router, including both wireless and wired devices, enable each one to communicate freely, such as the sharing of a printer.

### Network Interface Card

A network card is an electronic device that connects one computer to a network, usually to a Local Area Network (LAN). Most modern computers have an embedded network interface card in the motherboard instead of having an external chip to connect a network. These cards are critical when the computer exchanges data with the computer network using a given

protocol such as CSMA/CD. Previous versions of network cards used included protocols such as ARCNET incorporated in 1977, but today most computers use Ethernet. The use of Ethernet network cards has been the most common with the revolution of computer networking being witnessed each year.

Internet speeds often vary on network interface cards based on the protocol standards supported. The previous Ethernet cards supported up to 10mb/s with the current adapters supporting from 100mb/s up to 1000mb/s. Network cards do not necessarily support wireless connections, but routers also contain these cards, which determines the speeds for a given computer network. The same has been projected to increase in the near future with the use of Ethernet network cards. In this case, speeds are to grow in the coming years, with rates tripling the current figure. This is attributed to the expansion of usage of computer networking across different platforms, both in small enterprises to commercial use over the years.

## Protocols

Computer networking also comprises connection protocols that consist of rules for two or more systems to exchange data. Other than regulations, protocols also include syntaxes, communications synchronization, and semantics, as well as error recovery techniques, use in both hardware and software of computer connection. In other words, protocols are a set of rules which connect the server to the routers regardless of the variations in infrastructure, designs, and standards. As to exchange information, both parties must adhere to accept the protocols built in the hardware, software, or both.

Networking protocols usually accompany similar languages for the devices to facilitate the interaction between the two computers in the exchange of information. Network protocols typically utilize the Open Systems Interconnection (OSI) model used to break down the complicated process to readily defined functions and operations. There are multiple protocols used in computer networking, Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Protocol (IP), Hypertext Transfer Protocol (HTTP), and File Transfer Protocol (FTP), among others.

## Types of Computer Networks

## Local Area Network (LAN)

Local Area Network, commonly referred by its abbreviation, LAN, is a group of computer systems using and sharing a particular internet connection within a given small area such as the office or residential building. The LAN connection is usually through a communication medium, for instance, coaxial cables used by two or more personal computers. This type of computer network is often cheaper than other types and accessed by those within the area and uses hardware such as adapters and Ethernet cables. Transfer of data is commonly extremely fast with considerably higher security. The connection only supports those within the area, and anyone outside tends to lack the transmission of information.

## Personal Area Network (PAN)

This is a type of private network arranged within an area of 10 meters and often for personal use with devices within a given range. Personal Area Network was first researched and introduced by Thomas Zimmerman, who established that an individual could create a connection with communities with devices within 30 feet. Both wired and wireless PAN can be used in this type to connect to devices around the source. The source more so may generate from media players, laptops, and mobile phones. Wireless is usually connected using hotspots, Bluetooth, and Wi-Fi connected to devices within a given range. Wired PAN is connected by USB cables to facilitate the connection of a given network. Personal Area Network always moves with the person and can include offline systems and uses to connect devices using a VPN in small home networks.

## Metropolitan Area Network (MAN)

Metropolitan Area Network is computer network which covers a wide range of a geographical area by interconnecting several LAN connections. This type of computer network is often used by government agencies to connect to different federal facilities as well as their citizens and private organizations. Some of the protocols in MAN include ISDN, Frame Relay, and OC-3, among others, which connect to different LANs through an exchange line. This form of a computer network is used in larger areas than that of LAN and such as airline reservations, military communication, colleges, and between

banks.

## Wide Area Network (WAN)

Wide Area Network is extended computer network coverage over a large geographical area such as between states or countries. It is quite extensive than LAN and WAN and not limited to one domain but covers an entirely larger area by use of satellite connections or fiber optic cables. WAN is the largest of all computer networks in the world and used in businesses, government operations, and educational purposes. Some of the advantages of WAN include centralized data, fast message transfer, coverage of a full geographical area, higher bandwidth, and supports global businesses. On the other hand, WAN can become disadvantageous in the case of a security breach; it demands a firewall and rigid antiviruses, expensive setup costs, and difficulty fixing problems due to its more comprehensive coverage.

## Machine Learning

As mentioned, machine learning is the method of data analysis by computers where algorithms and statistical models play a role for machines to learn from data and patterns and then make decisions without human interactions. Since its incorporation in the late 1950s, machine learning has gained popularity and become a vast topic in computing. It is a branch of artificial intelligence enabling computers to provide analytical information about the future with limited human interaction. Machine learning can, therefore, be learned in different ways depending on the part an individual chooses to follow.

The idea of machine learning takes the form of the human brain, including the neurons and how they facilitate the assimilation of information, thinking, and making decisions. When the concept was first introduced to computers in 1943, it focused on neural networks where machines became capable of learning on their own, depending on the information fed. That is, machines were able to observe, learn, understand, analyze, and make decisions based on the event without depending on individual instructions. However, the slow development of computers at the time increased the challenges of machine learning when compared to the current days.

As humans have the ability to develop and expand their knowledge about an event or something they first or learn, the same technique, therefore, facilitate machine learning. Besides, humans depend on networks of neurons in the

brain, and computers utilize a similar pattern. As such, machine work with the same technique, therefore, can manage to make decisions and conclusions without any human interaction. However, the decisions made by computers are widely based on mathematical and algorithms that have expanded to make them predict the outcome of things that haven't happened yet. Currently, different methods have been used, therefore enabling computers to learn specific information; therefore, be able to provide predictions, conclusions, and decisions based on specific datasets.

## **Machine Learning Vs. Computer Programming**

Machine learning has been widely confused with computer language programming, which in this case, has significant dissimilarities. As defined, machine learning is all about the machine receiving specific data sets, selecting the most reliable algorithm, learn and determine the outcome without any human interaction. It, therefore, has limited interaction, especially when analysis the information, learning, and making positive outcomes. On the contrary, computer programming requires human interaction who first selects datasets to use and writing them in the machine. The codes are then executed to create a specific program, which is, therefore, the outcome. In programming, machines rarely learn but generated results based on the instructions provided by humans.

### **General Steps in Machine Learning**

#### **Collection and Preparation of Data**

Humans can never learn and have knowledge about something without having an interaction or understanding the basics. Similarly, machines face a similar challenge, as they also have to gain access to relevant information about something before learning in detail about it. As such, the first step in machine learning is to collect the necessary data and prepare it in a way that fits a given criterion. The collection comprises of gaining access to specific details about a given element and begin having an understanding about it. The computer then prepares the system to internalize the information before providing the needed knowledge.



## Selection of Instructing Models

Humans also undergo trial and error in order to come up with an effective solution to a problem at hand. Machine learning also creates multiple models based on the instructions fed to provide the most suitable model, which can solve a given problem. In this case, the computer uses algorithms which have been modified differently since their incorporation. Over the years, more models have been developed with the objective of making machines more specific in some regions of specialization. In this step, computers, therefore, select the most desirable model that best suits a given dataset and train itself through learning more about the information at hand. This ensures that the information fed and the outcomes are more likely to become beneficial and provide the intended solution.

## Evaluation of Models

The last step is now to put the model selected into practice by trying to figure out if the model which enables the machine to learn and make decisions without human interaction. Machines readily learn from the information fed and create patterns and work like how we behave on newfound knowledge in our minds. That is, when supplied with well-tested details, the machine will offer excellent results with inadequate tests leading to vague and harmful outcomes. In this step, you need to feed the computer with the relevant models and data which provide an algorithm where the machine will follow and deliver effective results. Therefore, test the data and model, which provides certainty of delivering exceptional results.

## Types of Machine Learning Algorithms

### Supervised Algorithms

As mentioned, machine learning comprises of multiple types depending on how the data fed is to yield the outcome. One of the models is the supervised algorithm, where the datasets undergo a given set of parameters, which in turn determine the outcome. The machine initially specifies the data into labels as well as the training data included. In this case, the data is initially tested to ascertain its outcome, therefore, controlling the outcome. This type

of algorithm usually has a manageable as a result is generally intended. Supervised algorithms are further subdivided into classification and regression algorithms.

The classification algorithm uses the K-Nearest Neighbor classification algorithm, which is responsible for sorting data into individual labels. The data is classified depending on the similarities between variables or the information inputted in the machine. On the other hand, regression algorithms focus on mathematical relationships and the dependency of variables. That is, it provides an immediate analysis of numerical datasets with similarities essential for predicting the future. The regression algorithm includes two forms depending on the information fed, linear, and logistic regression models.

## Unsupervised Algorithms

This is the opposite of supervised algorithms and consists of unlabeled datasets, which in most cases, the results are undetermined. The unsupervised algorithm is classified into K-means clustering, recurrent, and artificial neural network. The artificial neural networks resemble the brain neurons, which are connected and interconnected to enhance learning, thinking, and making decisions without any interventions. K-means clustering entails the grouping of similar data into clusters to promote learning in machines. While recurrent neural networks use the memory in the nodes of computer neurons to analyze sequential information for the benefit of encouraging decision making in devices.

## Reinforcement Algorithms

Reinforcement algorithms are where the machines determine specific information is the datasets within particular contexts. As one of the types of machine learning algorithms, reinforcement models are the most beneficial as learning of specific datasets leads to the maximization of the outcome. However, if the wrong dataset is fed into the machine, it may result in extensive punishments or other related dangers. But when using the right parameters, the device will make the needed corrections and yield positive results. Besides, this type of machine learning algorithm enables you to quickly make corrections, modifications, or change the outcome if you feel it may become undesirable in the future.

# Applications of Machine Learning

Since the introduction of machine learning in the computing industry, different sectors have benefited significantly in their operations. More so, it has popularity between developers as well as other users, making it applicable in different areas. In this case, the applications of machine learning range from small scale technological businesses to commercial use. One of the common areas includes social media such as Facebook and Twitter used for sentimental analysis, spam filtering, facial recognition, among others. It is also applied in the e-commerce sector to display items that are mostly searched by specific clients. Machine learning is also used in areas such as transport, health, trading, visual assistance, and financial services.

# Chapter 2: Properties of a Computer Network

A computer network is defined as a digital telecommunications network that allows resources to be shared between nodes. A telecommunication network is a number of terminal nodes having connected links that would enable telecommunication between some terminals. Transmission links in the network act as a connection between nodes. Telecommunications network allows for interactions and transfer of information over long distances.

Computer network involves a connection between computer systems and computer hardware devices via communication channels. The communication channels enable communication and sharing of resources amongst many users. The connections between nodes are referred to as data links. The establishment of the data links is usually from cable media, including optic cables or wires, and wireless media, including Wi-Fi.

Network nodes are the network computer devices originating, routing, and terminating the data. Typically, the nodes are identified through network addresses, and generally include elements such as phones, personal computers, networking hardware, and servers. The devices are easily networked together as long as one of the tools has the ability to exchange information with the other devices. The devices can either have or not have a direct connection with each other.

A wide range of services and applications are supported by computer networks. Some of them include accessing the digital audio, digital video, World Wide Web, the common use of storage servers, and applications, fax machines, and printers. It may also include the use of instant messaging and e-mail applications. Computer networks differ from other telecommunication networks because of the transmitting mediums they use in carrying their signals, protocols used in organizing network traffic, size of the networks, the mechanism in controlling traffic, organizational intent, and topology. One of the most common computer networks is the Internet.

Computer networks have been in existence since the late 1950s. During this time, computer networks involved the Semi-Automatic Ground Environment. The SAGE was a radar system used by the U.S military. A reorganization

was later planned in 1959. It was based on the network of the OGAS, which were computing center networks. The MOS transistor was also invented in 1959 at Bell Labs by Dawon Kahng, and Mohamed Atalla. The conductor was one of the significant steps towards computer network communication infrastructure. It included base station modules, routers, memory chips, telecommunication circuits, microprocessors, transceivers, and RF power amplifiers.

SABRE a system in the commercial airline reservation, managed to go online with two mainframes that were connected together in 1960. The intergalactic computer network was later invented in 1963. It allowed for general communications amongst many computer users. In 1964, some researchers came up with an operation where a computer was used in routing and managing connections between telephones.

The concept of packet switching was developed all through the 1960s. It allowed for information to be transferred among computers through a network. A telephone was also used in implementing the precise control of computers. A paper was later published on Wide Area Network that allowed computers to share time.

French CYCLADES hosts were developed by 1973. The hosts had the responsibility to deliver data instead of centralizing services on the network reliably. A formal memo was written in the same year with a description of Ethernet. Ethernet is one of the most common networking systems used in the world today. Robert Metcalfe worked from 1979 in a bid to make Ethernet open standard. Ethernet continued being upgraded to a 10Mbit/s protocol in the 1980s.

By 1995, Ethernet was supporting gigabit speeds. It has the capability of having a transmission speed of up to 400Gbit/s as recorded in 2018. The continued use of Ethernet results from its capacity to adapt and to scale easily.

## **Properties of Computer Network**

Computer networking is considered a subdivision of electronics engineering, computer engineering, computer science, electrical engineering, information technology, or telecommunications. This is because the practical and theoretical computer networking relies on have close relations to the fields.

Computer networks allow for efficient interpersonal communication between

users. They can effectively communicate through video telephone calls, telephone, online chats, instant messaging, video conferencing, and e-mails. It also allows for network and computing resources sharing among users. Accessing and using resources is made easier through the devices on the network. Users can, for instance, share printers and storage devices together. Data, files, and other forms of information can also be shared effectively using computer networks.

## Uses of Computer Networks

If it were not beneficial, people would not have considered creating a connection between computers through a network. There are numerous users of computer networks in the world today. They are used to benefit both individuals and companies in the long run.

## Use in Business Applications

- **Resource Sharing**

The main goal of computer networks is ensuring the anything about a business is available to all those who take part. Computer networks allow for this access by making all equipment, data, and programs available to any person using the network. Any user can access the use of the computer network regardless of their physical location.

- **Server-Client Model**

In such a model, the information about a business is stored on servers, which are powerful computers. The servers are housed centrally, and a system administrator is used to maintain them. The business employees usually have clients, which are simple machines on their office desks. The server-client model allows for easier access to remote data and information by these employees.

- **Communication-Medium**

Employees in a business setting need to communicate on various issues affecting business operations regularly. Computer networks, therefore, offer a powerful medium for communication among the employees. Almost all companies have several computers with logged-in e-mails. Employees use these computers when on great deals of communicating on a daily basis. An employer can send a message, and everyone engaging in the business operations can easily receive it.

- **eCommerce**

One of the most significant targets of every business is the ability to do business with potential customers through the Internet. In the modern world, most customers prefer doing their shopping from home. Numerous ventures such as music vendors, books, and food stores have considered using computer networks to meet the needs of their customers.

- **High Reliability because of Alternative Sources of Data**

Computer networks provide higher reliability by providing numerous sources of data. This means that general files can be copied on many machines. When one of the machines is not available, another one can be used to access the same information. The concept of Reliability is significant in banking, military, nuclear reactor safety, and military. This is because such sectors require consistent operations, even when there are hardware and software failures.

- **Money-Saving**

Computer networking is a significant concept of the financial aspect for many companies and businesses. This is because it saves a considerable amount of money. Computer networks provide an option for using personal computers rather than mainframe computers that are quite expensive. Companies can effectively use the peer to peer model by networking all personal computers together. Everyone in the organization can access the network for many

purposes, such as communication. The domain model offered by computer networks can help to provide security to the operations of an organization. Clients involved in the organization can access data and communicate with the organization through the server.

- **Computer Networks:**

## **Home Applications**

Home users also consider using computer networks for various reasons. Some of these include:

Accessing remote information- People connect their devices for easier access to useful information.

Person-to- person communication- This communication includes sending e-mails or other forms of communication. Remote users are able to communicate with other people easily. They are able to see and hear from other people who are away from them without delays. Video-conferencing is one of the most popular person-to-person communication, is used in remote schools, or receiving medical opinions from medical practitioners who are distant. People also consider using computer networks to access information posted by worldwide newsgroups easily. Through these networks, people easily give their feedbacks regardless of their physical location.

Interactive Entertainment- Computer networks allow for easier access to videos on demand, multi-person simulation games, and participation of people in live television programs such as discussions, and quizzes. It is through these networks that people can feel the entertainment from the comfort of their homes. People also use computer networks as home applications for electronic commerce.

## **Computer Networks: Mobile Users**

Mobile computers include personal digital assistants and notebooks. They are one of the segments in the computer industry growing at a very rapid rate. Owners of mobile computers usually possess desktop computers in their offices and prefer connecting them to their portable computers based at home. Computer networks allow for wireless connection to these devices, even when in an airplane or a car. One main reason why people connect to these



mobile computers is to allow them to receive telephone calls and messages, send faxes, e-mails, access remote files, and surf through the web. People are able to do all this from any location away from their office.

## More Information on Types of Computer Networks

Computer networks are basically used for numerous tasks in the world today. Some of the tasks include downloading attachments and printing documents. This is done by referring to several devices within a room and spreading them across the entire world. This can be defined based on their purpose or their size. Below are some of the common types of computer networks.

- **Personal Area Network (PAN)**

A personal area network is the most basic and smallest type of computer network. It is comprised of a computer(s), phones, tablets, printers, and a wireless modem. PAN revolves around a single person within a building. The networks are commonly used in residences and small offices. Their management is controlled by one organization or person from one device.

- **Local Area Network (LAN)**

Local area networks are popularly discussed by people in the world today. They are one of the most original, simplest, and common types of computer networks. They are used in connecting together several computers and devices of low voltage. The devices are usually within short distances, such as different rooms within a building or several buildings close to each other. They help in sharing resources and information among the connected devices. LAN computer networks are commonly used by enterprises. They are easily manageable and maintainable.

- **Wireless Local Area Network (WLAN)**

WLAN networks function in a similar way as the LAN networks. The networks use wireless network technology. Some of them include Wi-Fi. WLAN networks do not require devices to have physical cables when

connecting to it.

- **Campus Area Network**

Campus area networks are quite larger than Local area networks but smaller than the metropolitan area networks. CANs are commonly used in small businesses, universities, colleges, and large school districts. Campus area networks are spread across a number of buildings that are closer to each other. They allow any user in the different buildings to connect and share resources.

- 

- **Metropolitan Area Networks**

Metropolitan networks are larger than the local area networks but smaller than the wide-area networks. They include the elements of both types of computer networks. MANS computer networks can spread on a whole geographical area such as a city or a town. The ownership and management of the computer network is usually under one company, such as a local council or by a single person such as the owner of a particular company.

- **Wide Area Network**

Wide area network is quite complex as compared to the local area network. WANs computer networks easily create connections with computers in wide distant locations. Low voltage devices, as well as computers, create a remote connection with each other. They do this through a single large network allowing communication even longer distances. WAN computer networks have different categories, with the Internet being the most basic type. The Internet allows for the connection of computers all over the globe. Numerous public and administration entities typically own WAN computer networks. This is possible due to its wider reach.

- **Storage-Area Network (SAN)**

SAN computer networks are of high-speed and significantly dedicated. They create connections between shared sources of storage devices and various servers. SAN networks do not rely on WAN and LAN. The computer networks typically removed the storage devices from the computer networks and put them on their high-performance networks. The computer networks are accessible similarly to drives attached to servers. Some of the types of Storage Area Networks include, unified SANs, and converged virtual SANs.

- **System-Area Network**

This type of computer network is quite new and is also abbreviated as SANs. The computer networks are basically used in defining relative local networks. The networks are designed high-speed connections in applications involving servers, processors, as well as storage area networks. Computers are connected to this type of network operating as single systems and offer very rapid speeds.

- **Passive Optical Local Area Network (POLAN)**

POLAN computer networks are used as a substitute for traditional switch-based Ethernet LANs. The technology used in POLAN computer networks is added to structured cabling. The reason behind the integration is overcoming concerns on the support of traditional network applications, and Ethernet protocols. Optical splitters are used in POLAN to enhance the splitting of optical signals from a single strand. Single-mode-mode optical fibers are transformed into numerous signals that serve devices and users.

- **Enterprise Private Network (EPN)**

Enterprise private Networks are owned by businesses that typically build them. Businesses prefer this type of computer networks as a way of securing

the connection between various locations that share the network.

- **Virtual Private Network (VPN)**

The extension of a private network all over the Internet is made possible by the use of Virtual Private Network. Sending and receiving information and data between connected devices is also made possible by the VPNs computer networks. The process is also possible when users are using devices that are not directly connected. Access to remote private networks is also made possible through a connection referred to as point-to-point.

## **Basic Elements of Computer Networks**

Computer Networks comprise of systems through which a connection is created between numerous nodes. The links help them to share resources and information. Computer network elements are the fundamental objects used in computer networks. Basically, there are four significant elements of computer networking. These include computers, transmission medium, protocols, and network software. For a computer network to successfully function, all the elements have to work in coordination.

- **Computers**

Computers are digital devices that can accept input in the form of data, process it through the use of data structures, and predefined algorithms, performing tasks in the form of output. The process can be defined as transforming raw data into useful information. The output provided includes performing several physical tasks as well as storing data, transforming it as well as retrieving it when in need. The network is created by computers to allow for leveraging of distributed models of programming and interchanging data to allow for equivalent processing.

- **Transmission Medium**

The transmission medium is the path through which users send data from one place to a new place. When representing data, computers and

telecommunication devices make use of signals. The transmission of the signals from one device to the other is generally through electromagnetic energy. They are transmitted through air, vacuums, and different modes from the sender to the receiver. There are two types of transmission mediums. The Guided or Wired transmission mediums include optical fiber cables, twisted pair cable, and coaxial cables. The Unguided or Wireless transmission mediums include infrared, radio waves, and microwaves.

- **Protocols**

Protocols are the defined conventions and rules guiding communication between computer network devices. Computer network protocols consist of device mechanisms used in identifying and making connections between each other. Formality rules are used in specifying the method of packaging data in the form of received and sent messages. There are three types of protocols. The internet protocols, wireless network protocols, and network routing protocols.

Internet protocols are the rules set to govern the format of sending data through the Internet or over another network. They are the standards used to address and route data on the Internet. The internet protocols deliver packets from the host to a destination host entirely depending on the addresses on the headers of the packages. Wireless network protocols involve a collection of wireless devices and laptops engaging in communication through radio waves. Computer network routing protocols, on the other hand, are used in specifying methods through which routers are communicating with each other. They do this through the distribution of information, enabling them to choose routes among nodes within computer networks. Routing algorithms are used when determining particular routes of choice. Computer network routing protocols are capable of adjusting dynamically to evolving conditions, including disabled computers, and data lines.

- **Network Software**

Computer networks use network software as foundation elements for all networks. Network software assists administrators in deploying, managing, and monitoring any network. Numerous traditional networks consist of

special hardware, including switches and routers that integrate networking software in the combination. Networking software consists of a wide range of software applied in designing, implementing, operating, and monitoring computer networks. Most traditional computer networks were based on hardware but embedded in the software. Defined Networking, that was software like emerged and led to the separation of software from hardware. This separation made network software much adaptable to the evolving nature of computer networks.

## Choosing a Suitable Computer Network

There are factors that one should consider when selecting a computer network type for an organization. These factors include:

**The Organization-** One should consider finding out the sector of the economy that the organization operates, what the organization is providing, the number of people employed in the organization, as well as the jobs they are working on.

**Existing Systems-** It is essential to check on the existing computer network components, the network operating system, network architecture, transmission medium, and topology.

**Number of Users-** Prior to choosing a computer network for an organization, it is crucial to check on the number of users. This is because organizations tend to have users working on separate as well as shared workstations.

**Functionality-** Consider checking on tasks undertaken by the network users as well as software applications being used in carrying out the tasks.

**Budget-** Consider choosing a computer network operator that is within your budget. This helps to guarantee successful implementation and maintenance of the network.

# **Chapter 3: Easy Guide to Learn Basic Computer Network**

This article discusses the basic components of computer networking and the easy ways you can learn them. It also extensively discusses the advanced features of computer networking as well as how you can learn and apply them. Read on to find out!

Computer Networking has been in existence for quite some time now, and with time, technology has become quicker and more affordable. These networks are a build-up of various devices and components, including computers, routers, and switches, which are linked together by wireless signals or cables. Learning how these networks and connections are assembled is very essential in creating a network that can be used for many purposes.

In the quest of breaking this giant of a topic down, let us start by discussing the essential components of any computer network.

## **The Important Components of a Computer Network**

This is the first thing you need to look at when learning computer networks. Any computer network is made up of four very important components: Media, Networking Devices, Protocols, and End Devices. Let us discuss each of these essential components.

- **The End Devices**

This is a kind of device that either sends or receives a set of data or information within a particular network. End devices can be laptops, smartphones, PC, or any kind of machine with the capabilities of receiving or sending the set of data within the connected network. For your information, you will need a minimum of two devices to build a network.

There are two types of end devices: client end devices and the server end devices. The server end device is responsible for providing service or data. On the other hand, the client end device is one which is responsible for

receiving the data offered from the former (the server end device).

- **The Media**

This is a very important component of the computer network that provides connectivity and linkage for the end devices. End devices are not able to exchange services or data unless they are connected through any kind of media. As of today, there exist mainly two categories or types of media: the wired media and the wireless media.

Radio signals are mainly applied in transferring data and information between the end devices when using Wireless Media. In wired media, however, cables are used instead.

The above-mentioned types of media are further subdivided into various subtypes depending on factors like the data transfer speed, length, frequency band, among others. The subtypes are commonly referred to as media standards. The media standards that are popular and widely applied are the IEEE802.11 (also known as Wi-Fi standards) and the Ethernet.

The two media standards play different essential roles. The Ethernet is responsible for defining standards for wired media while the IEEE802.11 plays a role in defining standards for wireless media.

- **The Protocols**

Just like the previous two, this is a very important component of a computer network. Protocols are responsible for the communication between the involved end devices; they could be two or more. A protocol is defined as a group of rules that highlights and specifies the standards for a specific or all the stages of communication.

Below are some known roles played by protocols.

- Starting and ending the communication process.
- Doing Encryption and compressions before transferring any data.
- Packaging data in such a format that it is able to travel within a network.



- Establishing and providing logical addresses
- Carrying out error correction processes
- Performing media authentication

Two popular models of networking describe the functionalities of most common protocols: TCP/IP model and the OSI reference model. These models categorize the entire process of communication into logical layers. They further explain how each protocol works in every layer, which enables the process of communication.

## • The Networking Device

This is an essential component of computer networking that works in between the end devices. It is responsible for controlling the smooth flow of data. Depending on its functionality, networking devices are categorized into three different types; the forwarding device, the connecting device, and lastly, the securing device. Below, we discuss the functionality of each of the mentioned devices.

- **Connecting Device:** It is responsible for connecting two or more types of protocols and media. In situations where two end devices are situated in different geographical networks or connected via a distinct type of media, they will require a connecting hatchet to carry out data exchange. This functionality can be provided through Multilayer and Router switch.
- **Securing Device:** This device is responsible for securing data from any unauthorized access. The securing device does security checks basing on the predefined rules whenever it receives a data packet. It then forwards it or rejects it based on the decision made. Some of the commonly known devices that perform these functions are NAT and Firewall.
- **Forwarding Device:** This is a device responsible for forwarding data. It has multiple sections and ports mainly used in connecting more two or more end devices in just one network. The two commonly known devices for these

functions are Hub, Ethernet, and Bridge switches.

Having learned about the four essential components of a computer network, we next discuss other features that are much significance in computer networking.

Routers, switches, and wireless access points play a very significant role in computer networks. Below, discuss how this is done.

- **Switches**

These are the basic requirement for the majority of business networks. A switch, as most of us know, acts as controller linking printers, computers and servers within a computer network.

They enable the devices within a network to establish communication within themselves as wells as building a network commonly shared resources. Switches save a lot of money through resource allocation and sharing. They also increase the rate of productivity. There exist two commonly known types of switches in computer networking; managed switches and unmanaged switches.

An unmanaged type of switch is that which is able to work outside the box and can not be configured. The network equipment established at home specifically offers unmanaged switches. On the other hand, a managed switch is that which can be configured. It gives you the capability to adjust and monitor the progress of network traffic. It, therefore, gives you more control over the entire networking process.

- **Routers**

These are essential components that are responsible for connecting multiple sets of networks. They are also tasked with connecting the computers within a given network to a functioning Internet. They make it possible for all the networked devices or computers to share one Internet connection, which in the long run, saves you money.

Routers act as dispatchers. They analyze the data sent across a given network, find the quickest route data can travel and sends it that way.

They are able to link your business to the outside world, protect the vital

information from threats, and even make decisions on the computers that are eligible to receive more attention over others.

Apart from the known networking roles they play, routers are equipped with a set of more features that make the networking process even easier and safer. Basing on the needs you have, for instance, you can buy a router with a virtual private network commonly known as VPN, a firewall, or the Internet Protocol, which is commonly known as IP.

- **The Access Points**

This is another essential aspect of a computer network that enables the devices to link to the network (a wireless network) without using cables. Wireless networks make it easier to invite fresh devices on online networks and give a flexible form of assistance to remote workers.

They act as amplifiers for your computer network. While routers provide bandwidth, the access point broadens the provided bandwidth in ways that networks are able to provide support to a good number of devices. These devices can then access the Internet from locations far away from where the router is located.

What you should know, however, is that the access points don't just extend the Wi-Fi reach. It also provides essential information about devices connected to the network; it also gives proactive safety measures and plays other critical functions.

Additionally, the access points can support various IEEE standards. Every standard, as we have discussed earlier, is an assortment that has been ratified over a period of time. Such standards run on a set of different frequencies, produce a different set of bandwidth and provide the help needed from a host of deferent channels.

- **Wireless Networks**

When creating a wireless network, you have the option to choose between four different types of deployment. Every form of deployment has characteristics that work better in various solution searching missions.

- **Cisco Mobility Express:** Cisco mobility is a simple, best

performing wireless solution that is aimed at helping medium or small-sized companies. It is equipped with complete features of Cisco that usually preconfigured the best practices of Cisco advance. The defaults created will enable the fast and effortless deployment of Wi-Fi that can operate in a few minutes. This is the most recommended module, especially for small computer networking businesses.

- **The Centralized Deployment:** The commonly known type of computer networking system is centralized deployment. They are basically used in learning institutions where structures are located closer together. This kind of deployment involves a wireless network that eases upgrades and ensures the advanced functionality of wireless networks. The controllers of these devices are installed based on-premises and set up in mostly in a central location.
- **The Converged Deployment:** This kind of deployment is mostly done in small proximity establishments like small campuses or branch offices. That provides a set of consistency in both wired and wireless connections. The convergent deployment redirects the wired and wireless connections on a single network and then carries out the double role of the switch and as the wireless controller.
- **The Cloud-Based Deployment:** This deployment method puts into use the cloud to run the devices dispatched on-site at different locations. This kind of solution needs a Cisco Meraki cloud-managed gadget that gives a full view of a computer network through visible dashboards.

# The Classification of Computer Network

Having learned about the essential details of a computer network, it is time we discussed the classification of computer networks. This is a very important topic for anyone in quest of learning computer networking.

Computer networks are categorized based on various factors, namely: the geographical location, the relationship between devices, and the access types. Let us look at each criterion and find out the credentials in detail.

## Basing on Geographical Location

When using the geographical coverage criteria, the network device is subdivided into three different types: MAN, WAN, and LAN. The network spread in small, medium, and much wider geographical areas are referred to as the WAN, LAN, and MAN work networks in that order.

## Based on the Access Type

When basing on allowing different users to have access to the network resources, the network can be grouped into three different types: Intranet, Extranet, and lastly, the Internet.

Intranet refers to any private network. In this kind of network, users from outside do not have access to provided network resources.

An extranet is almost similar to an intranet as it is a private network. In this network, however, external users are allowed access to a small portion of internet resources after proper scrutiny and authorization.

The Internet, on the other hand, is a public network. Any individual or user can have access to it provided they have devices that can access it.

## Basing on Relationships between End Devices

In this criteria, the Internet is broken down into two sets: the clients/server network and the peer to peer network. In the peer to peer network, the available end devices all have fair, equal rights. In the client/server network, however, the decision on which client will receive what rights lie in the hands of the server.

Next, we look at the various types of computer networks. This is also a very important area where, as a person learning computer networking, you need to know.

Computer networks are categorized by their size. There are mainly four types of computer networks, namely; WAN (Wide Area Network), MAN(Metropolitan Area Network), PAN (Personal Area Network) and LAN (Local Area Network). Let us discuss each of these networks extensively and find out what they entail.

- **Local Area Network (LAN)**

LAN refers to a number of computers linked and connected to one another within a small space like a house or office. The Local Area Network is mainly used in the connection of two or more computers via a communication channel such as the coaxial cable and the twisted pair. LAN is cheaper because it is constructed with affordable hardware, including Ethernet cables, network adapters as well as hubs. Data is transferred quicker in LAN than any other network. The Local Area Network gives more secure network options.

- **The Personal Area Network (PAN)**

This is a type of network that is arranged around an individual, to be more specific, within ten meters. PAN is mainly used in connecting computer devices that mainly for personal use. Thomas Zimmerman, a research scientist, first brought the idea of Personal Area Network. This kind of network can cover an area of up to 30 feet. You can use personal computers to develop this kind of network. Such kinds of computers are mobile phones, laptops, desktops, play stations, and media players.

As of today, there exist two categories of Personal Area Network: Wired Personal Area Network and the Wireless Personal Area Network. The wireless one is developed by the use of wireless innovations like Bluetooth and Wi-Fi. This is usually a low range network.

The wired network, on the other hand, is built by the use of USB cables.

- **Examples of PAN**

**The Body Area Network:** this is a kind of network that is moved along with a person. For instance, mobile networks are

moved with an individual. Now suppose that the individual in possession of the mobile network establishes a connection and invites other devices to share the information and connection.

**Offline Networks:** This kind of network can be built when just at home. It is specially designed to connect and link different devices, namely computers, printers, and radio sets. You, however, need to note that the devices are not connected to the Internet.

**The Small Home Office:** This kind of network is mainly used to link and connect a number of elements to the internet connection and a cooperate link through a VPN.

- **The Metropolitan Area Network (MAN)**

MAN is a kind of network that can cover a large geographical area by joining a different kind of local area network to create a larger network. The metropolitan area network is mainly used in government organizations as well as private companies to connect citizens. In this kind of network, there are several local area networks connected via a telephone line. Some of the commonly used protocols in metropolitan area networks are ATM, Frame Relay ADSL, among others. MAN has a wide coverage and range compared to the local land network.

- **Uses of MAN**

It is used in establishing communication between financial institutions like banks within a city.

MAN can be applied in the reservation of airlines.

Additionally, a metropolitan area network is used in learning institutions that are located within a city. It is also used in the creation of communication modules in the military.

- **The Wide Area Network (WAN)**

WAN is a kind of network that covers very large geographical locations and

regions like countries or States. WAN is very big compared to the local area network. It is not pinned down to a single location but rather can be distributed over large areas through fiber optic cables or satellite links. For your information, the Internet is one of the best forms of WAN. The Wide Area Network is largely used in fields of education, business, and government.

- **Examples of WAN**

**The mobile broadband:** in this kind of network, the 4G network is popularly used across a country.

**Last Mile Internet:** This is the situation where a telecommunication company provides internet services to users in different locations by connecting their residences with fiber optic internet.

**The Private Network:** Banks provide a set of private networks that can connect up to forty-four offices. The private network is build using telephone lines usually provided by telecom companies in charge.

- **Advantages of WAN**

Highlighted below are some of the advantages of WAN.

**The geographical coverage:** WAN covers a larger geographical location than any other network. For instance, if a branch of a certain office is located in a different town or city, you can be connected to it through the Wide Area Network. The Internet gives a leeway through which you can be able to connect with a branch located in a different location.

**It offers Centralized Data:** Data is centralized in Wide area networks. You, therefore, don't require to have emails or other back up systems.

Wide Area Network has provided an updated file. Various software organizations have work done on live servers. This means that programmers are able to access updated files within a matter of seconds.



WAN networks provide for the exchange of Messages where they are transferred in a fast way. You can see how this is applied in real life through web apps like Facebook and Skype, which allow you to communicate with loved ones.

WAN enables the sharing of resources and software: You are allowed to share software and a host of other resources like RAM when using the wide-area network.

Additionally, WAN enables you to do business in large, global regions.

Lastly, the wide-area network has higher bandwidth. It occurs If you decide to use lines that have been leased for your company when WAN gives you the highest bandwidth. Higher bandwidth is capable of increasing the rate of data transfer, which in return improves the productivity of your organization.

## The Internetwork

This can be defined as a number of computer networks, WAN, or LANs that are linked using devices and configured by the basic addressing machine. The process of doing all this is referred to as interconnection. Having interconnections between commercial, public, and private computer networks can also be referred to as internetworking. Mostly, internetworking uses internet protocol. Open System Interconnection (OSI) is the model of reference used in internetworking.

# **Chapter 4: What Are the Basic Cybersecurity Fundamentals?**

Cybersecurity is a popular name in the internet and other technological advancement areas. It has got many concerns recently due to the increased cyber threats and attacks. Simply because; more systems are being targeted using more sophisticated strategies in assaults. It is a menace that has an impact on small-scale and large-scale businesses, individuals, organizations, schools, workplaces, and so on. It is with great importance that we all have to understand cybersecurity and what measures we can invent to solve any threats and attacks.

Recently, there has been growth in the use of mobile banking, social networking, and online shopping by individuals, businesses, organizations, or enterprises. As much as it is a convenient way of getting services, it can come with a lot of danger. Simply because all these services can be acquired online, and that is an excellent harbor of cybercriminals who are waiting to lay a trap on your system. To be on a safe side, you may need to have the basic knowledge of cybersecurity fundamentals.

## **What Is Cybersecurity?**

It is the process of protecting programs, computer systems, networks, sensitive information, and software applications. It involves using several techniques, practices, and procedures against cyber-attacks, damage, or unauthorized access.

Cybersecurity is a vital aspect in any organization as it guarantees them the safety of their data. However, in some cases, it is tricky solving the cyber-attack menace due to inadequate systems, advanced threats, and attackers. Though, it does not mean it is entirely impossible to get the system going and protect your information at any cost. Let's have a look at some of these attacks and threats affecting information:

## **Botnets Attacks**

Initially, botnets referred to as a network or group of devices connected on

the same network to work together. However, this worked in the wrong way. Hackers and other cybercriminals have taken the objective of turning its primary function to create chaos. They do this by injecting malware or other malicious codes to disrupt its normal functioning. It happens due to stealing sensitive and confidential data or emails and also spreading spam emails. In most cases, these attacks are prone to large scale organizations that have a large volume of data at their disposal. These hackers take advantage and manipulate the system to their advantage and creating chaos within the organization.

## Crypto-currency Hijacking

In recent times, there has been the use of digital currency and mining. It is so prevalent in the business world, and so is with cybercriminals. They are inventing new ways of using the crypto-currency mining for their convenience on a disruptive and harmful way. They use crypto hacking, a program that injected into the mining systems. It then silently accesses the CPU, GPU, and power resources of the affected system to mine for the crypto-currency inform of Monero coins. It is an advanced threat that gets the hacker using your resources such as the internet and electricity. The process in itself is complex and wears off your system comfortably and later affects its functionality. In most cases, the cryptocurrency traders and their investors are at significant risk.

## Ransomware

It is a type of software encryption program file that uses a unique, robust encryption algorithm to encrypt data on a target system. This threat makes it hard to view any files on any application. The authors of this threat have a unique decryption key for the affected systems, which clears them using a remote server. In this case, the hackers involved in its creation will demand a ransom from the affected person to decrypt their data and save their systems. However, this does not guarantee you will have all your data back after paying the ransom.

## Phishing

Here a typical kind of attack that involves sending spam emails to people or organizations by imitating legitimate sources. Most of the emails sent through

this fraudulent way tend to have secure attachments to confuse you into thinking they came from a real person. For instance, they have active job offers, invoices, offers, and promotions from reputable companies or organizations or can be an email from a higher official of the organization and a government official.

However, the main objective of these emails is to steal sensitive and valuable data such as bank account details, credit card numbers, login credentials, company financial audits, and much more. To rule them out, you need knowledge in phishing email campaigns and their solutions. You can also consider using email filtering options to block the attacks.

## Social Engineering Attacks

It is a new attack used by cyber attackers to gather all the sensitive information about an individual or an organization. It comes in the form of displays of attractive prizes, huge offers, and promotions, advertisements. You will fall prey immediately. You provide your bank account details. All the details you provide are will be cloned and used for fraudulent financial transactions, identity frauds, crimes, and so on.

Since 2007, the ZEUS virus acted as a social engineering attack used for stealing bank account details and other banking related details from unsuspecting people across the world. They not only come with financial issues but can also lead to downloads of highly destructive threats to your system, which may affect its functioning and capabilities.

# The History of Cybersecurity

Cybersecurity is not that old in the technology sector as it dated back to 40 years ago when words like worms, spyware, malware, or viruses meant a different thing. Not only in the information technology sector but for any common man in the business sector, organization, and so on. Since its beginning, it brought mixed reactions as it came as a result of a research project. It is a fantastic fact from the 1970s. Robert Thomas was a researcher for BBN technologies in Cambridge, Massachusetts, at the time he created the computer worm referred to as 'the creeper.' During that time, the creeper infected several computers by attacking one machine after the other with the message; "I'm THE CREEPER: CATCH ME IF YOU CAN."

It was an aggressive threat. Afterward, Ray Tomlinson, the inventor, and creator of email created a similar program referred to as 'the Reaper.' It was to be an antivirus that would delete and clear the creeper.

In the late 1980s, there was another creation of a man called Robert Morris, whose idea was to test the size of the internet. He then wrote a program that would invade the networks, UNIX terminals, and copied itself. The plan referred to was the Morris worm. It was such an aggressive worm that it was disabled and slowed down the functionality of the computer, leaving them unusable. He was the first person to be convicted under the computer fraud and abuse act.

Since then, there has been the creation of invasive, aggressive, and deadliest computer viruses that are prone to cure and are hard to control and detect. That is the main reason that brought about the idea of cybersecurity to help protect data against these deadly attacks.

## The Importance of Cybersecurity

Cybersecurity is so critical in an organization or the workplace as the results that felt with its absence are unfriendly. Recently, the increase in threats that led to a lot of damage to individuals and organizations. Handling this cyber menace is hard and needs a lot of effort to ensure all your data is safe and protected from unauthorized persons. There is a need to ensure you have the right strategies to protect your data from threats and minimizing the damages in the event of attacks. However, to be safer, you need a good grip on the knowledge of cybersecurity fundamentals.

Here are the reasons as to why cybersecurity needs implementation at large:

- There is an aggressive rise in threats and cyber-attacks. For this reason, most organizations are finding it necessary to upgrade their cybersecurity not to fall prey to these attacks. It is a common issue and is taking a toll on individual, organization, banking, business information, which later leads to losses and destruction. It has been witnessed in several countries and giving it the attention it requires will save you a lot. There have been cases where cybercrimes and attacks have cost people up to billions in shillings every year, and that is very alarming.
- There is an increase in techniques and strategies used by the cyber attackers on reaching their targeted persons. They are using more advanced ways to attack, and that has been proven more destructive. They have learned about modern technology and how well to create their malicious threats to affect data to gain profit. That is why you need to learn about cybersecurity and its implementation to keep up with the advancements. It is not that easy mastering all the protective measures, but learning how well to protect your data from the attackers could keep you safe for longer.
- There are new regulations on data protection from GDR, who are expecting every organization to protect the data at their disposal. It is essential due to the increased threats to see to it that your sensitive data is protected and taken care of. In recent times, due to many cases of threats, there are new developments in the courts regarding data theft. To be on the safe side, protecting your information is more important than a long time wasted in the courts.
- Cyber-attacks are very demanding. Once you are affected by threats or attacks, it will take a toll on your resources and organization. There are cases you need to pay ransoms to clear the risks but without surety of getting your information intact. Depending on who took your data, you may end up in reputation breaches and a total financial problem on your business and so on. You can prevent all these scenarios by getting the right preventive measure and ensure your data is protected.

# What Are Cybersecurity Fundamentals?

For cybersecurity to be thoroughly analyzed, it follows three basic concepts referred to as 'the CIA Triad,' including confidentiality, integrity, and availability. This model was designed to offer guidance to organizations, institutions, or companies to form an effective security policy. They are essential as their working together will ensure you get the best results in resolving your Cybersecurity issues about information security. These include:

- **Confidentiality**

This concept is beneficial in limiting the access of any information. It works by restricting sensitive and vulnerable information from being accessed by third parties such as hackers and cyber attackers. In any organization, for example, there is a need to protect one's information for easy access as that may cause problems if breached. For this reason, organizations and institutions avoid sharing information and educate their workers or colleagues on the effects and how well to protect the data they hold using secure and robust passwords.

You can easily protect your data by handling it differently. You do not have to make the task too complicated. Making the people in an organization have the idea of how dangerous it is to have your information out there for people to access can significantly help. However, at some point, it may prove a daunting task at first but may greatly be improved by sharing experiences with the affected persons.

To ensure there is confidentiality, you can use data classification, data encryption, biometric verification, and two-factor authentication as well as security tokens.

- **Integrity**

Integrity gives you the guarantee of accurate, trustworthy, correct, and consistent data that is unchanged over some time. To protect your data in the transit from third users, ensure it is original, meaning; the data is not changed, altered, deleted, or allowed illegal access. The safety of data starts

with you. Letting other people into your information is very risky.

Putting up proper data protection and security measures in your workplace, institution, or organization will guarantee your data of safety. For this to work, there needs to be user access rules and control as well as file permissions to avoid data breaches and sharing. Ensure a trusted system or person handle the data files. Not everybody can process your information the same way; some may have a hidden agenda.

It is a need to monitor your data against theft, threats, and breaches. All this requires an advanced tool and equipment. These tools ensure your information is intact at all times, and if any risk is detected, the organization will know about it and create ways of amending the issue. In most cases, organizations prefer the use of tools such as cryptographic checksum and checksum to verify their data and information integrity.

Moreover, some attacks or threats can lead to data loss or destruction. For this, there is a need for an effective and reliable backup plan. In most cases, cloud backups are the number one trusted solutions as per now.

- **Availability**

In this case, you need to have your systems in the right condition. Which includes the software, hardware, devices, networks, and security equipment. To give the best results, they should be up to date and well maintained. It will ensure you have proper functionality and easy access to all the data you need without any hindrances. It will also guarantee healthy communication within the system, having a reliable bandwidth.

You will also need to look for types of equipment that are effective for disaster management. In cases of disaster, system attacks, or threats, there needs to be tools and utilities that will help you solve your issues. In this case, disaster recovery plans, firewalls, effective backup plans, and proxy servers are among the best services you can consider as attack solutions.

For these utilities to work accordingly, they should undergo multiple layers of security to determine the safety of constituents of cybersecurity. In most cases, this feature involves networks, computers, hardware systems, or software programs involving the data shared through them.

For an organization to reap results of safe and reliable data storage and protection, there ought to support from both ends. For instance, in an



organization, a practical cyber approach, there is a need to involve the people, computers, networks, processes as well as the technology in large or small scale or individually. Realizing a future with fewer cyber-attacks and threats requires a better organization and support systems that work together. You may also be amazed by how many solutions you can come up with to detect the threats and solve them.

# Chapter 5: What Are the Concepts of Networking?

Networking is a series of interconnection of computers worldwide to form an overall structure or system. The base or core for networking includes: types of computer networks, types of network equipment/the hardware, Ethernet, wireless local area network, internet service provider, TCP/IP, and other internet protocols and Net routing, switching and bridging.

There are three critical types of computer networks that are geographically based. These include the Local Area Network (LAN), the Wider Area Network (WAN), and the Metropolitan Area Network (MAN). LAN involves the interconnection of computers within a specific locality covering a small geographical area. It is majorly within buildings. There are further three types of LAN technology, which include Ethernet, Token Ring, and Fiber Distributed Data Interconnect (FDDI). The three categories of LAN are based on a specific arrangement of elements in the computer network. Ethernet LANs is based on a bus topology and broadcast communication. The Token Ring LANs are based on a ring topology. The (FDDI) uses optical fibers and an improved Token Ring mechanism based on two rings flowing in opposite directions. The WANs is an interconnection of computers covering a larger geographical area than the LANs, probably between cities and countries. Here, data is transmitted using such media as fiber optic cable and satellite in most cases. It is based on packet switching technology in which information is transmitted over a digital network is grouped into packets. Examples of WAN technology include Asynchronous Transfer Mode (ATM) and Integrated Services Digital Network (ISDN). Metropolitan Area Network is the interconnection of computers covering a much larger geographical area than WANs. The interconnection here is majorly between continents. The equipment sending data in this case to any significant distance is probably sending it to a minicomputer or a mainframe computer. Data is transmitted using terminal emulation software on the personal computer. This is because more extensive networks are designed to be accessed by terminals. A personal computer emulates or imitates a terminal.

Without networks, we wouldn't accomplish much. Just as human networks

make us more efficient, so do computer networks. In business, networks are extremely important. All business operations depend on various forms of networking. Networking helps organizations to save time and money. It also helps organizations and individuals to create new streams of income.

Some concepts shape networking. At first glance, these concepts may seem complex. But if you familiarize yourself with the principles of computer networking, it gets easier.

The reality is that networks are everywhere, and we all work within them. You are used to them to such an extent that you don't even realize it. In this article, we will focus on the concepts of networking. Our main objective is to help you have a better grasp of networking.

A network is a group of several entities that are connected in one way or another. This could be objects or people. It allows the flow of information among the entities involved. However, this has to happen under a set of clear guidelines.

In this piece, we'll be focusing on computer networking. An individual computer can help you accomplish a particular basic task. It undoubtedly boosts your productivity. But when you are using numerous computers that are connected, your productivity becomes greater.

Computers use data networks to process and share important information. Ten staff members can access important information at the same time without sharing a computer. Networking makes it possible for them to do so on different computers. This is made possible by a bunch of interconnected computers. It certainly enhances and promotes coordination within a team working for a common goal.

Imagine what would happen without a network. A team would solely have to rely on one computer to get work done. This could greatly undermine the team's productivity. The team would need a lot of time to complete simple tasks.

Therefore, a computer network can best be described as a group of computers that are linked together. The linking may be done through physical lines. The ultimate goal is to enable efficient exchanging of information in terms of speed and convenience.

When one computer is connected to another, the output is increased. And when several networks are linked together, they form one powerful network. This helps employees to have access to a larger pool of information. With such resources at their disposal, you can rest assured that they can accomplish

a lot more.

## Components of Network

There are four essential components of a computer network. These are networking devices, end devices, protocols, and the media.

- **End Devices**

Networking takes place between devices. End devices play the role of data transmission. They either send or receive various types of data. These are laptops, PCs, phones, or tablets. A network needs at least two devices to function. There are server devices that are tasked with providing data and client devices that depend on the data provided.

- **Media**

Devices have to be connected through a special medium. This medium is known as the media. There are two forms of media. That's the wired and wireless media.

Wireless media uses signals while wired media uses cables.

- **Protocols**

Protocols are important rules in networking. They aid communication between the devices and also set the standards of communication. Normally, protocols can initiate as well as terminate any form of communication between devices. Also, they encrypt the data before it is sent. The data is packaged in a form that can be transmitted within the relevant channels.

- **Networking Devices**

In between devices, there is a networking device. A networking device's main role is to control the flow of data between the end devices. It also forwards the data. This device is categorized into three categories. That's the connecting device, securing device, and forwarding device.

## Classification Based on Access Type

The classification based on access types includes Intranet, Extranet, and the Internet.

- **Intranet**

An intranet is a private network. External users can't access this network whatsoever. Not unless they use some unscrupulous methods to do so.

- **Extranet**

An extranet is also a private network. The resources within this network are not available to the public. External are only granted access through a strict authorization process. Full access is not granted to external users. Whatever access they may be given is partial.

- **Internet**

The internet is an open network that anyone with a computer can access. It has a vast resource that the public can utilize.

## Classification Based on Relationships between Relevant Devices

This classification is based on the relationship between the end devices. The network is classified into two. That's the peer to peer network and client-server network that will be covered in great detail later.

## Networking Plan

When creating a network of computers, you ought to have a network plan. This is because numerous computers are used, hence the need to manage them. Also, you want to ensure that information is kept within particular confines.

The connections should be planned to control the flow of information. Employees should have access to the information that's relevant to their duties. A computer network doesn't mean that everybody in the organization

is allowed to access all the information available.

The plan should give clear guidelines on where various types of information should be stored. A plan also defines what information will be accessed by the employees at a given time.

## Networking Types and Structures

Networking types are structured differently. They can either be wired or wireless. Also, they could be a combination of both. About a decade ago, most networks were wired. The computer network landscape has since changed. Modern networks mix both wired and wireless connections. Wired networks use Ethernet technology.

### **Advantages of Wired Networks**

- Wired networks are not only reliable but also fast and secure.
- Ethernet ports can also be found in most computing devices, including laptops and desktops.

### **Disadvantages of Wired Networks**

- Wired networks must use cables. And it is costly to run cables.
- Using a wired network within buildings is challenging. This is due to the sophisticated infrastructure. Multiple cables would be required to run between the buildings.
- A wired network doesn't support devices such as smartphones and tablets.

### **Wireless Networks**

Wireless networks don't rely on cables. These networks used the Wi-Fi protocol to transmit data.

### **Advantages of Wireless Networks**

- They are easy to set up. Moreover, you don't require multiple cables running from one point to the other.
- A wireless network offers great flexibility and convenience. They can be used in public places, offices, and homes. Mobile devices use a wireless network. Therefore, you can use all your internet supported devices at your convenience.

## Disadvantages of Wireless Networks

- A wireless network is certainly not as secure as a wired network.
- A wireless network is also commonly limited by range. Once you get out of the stipulated range, you can't use it.
- Wireless networks are much slower. The connectivity isn't as fast as it is with a wired network.

## Networking Layout and Topologies

To expand a network, the nodes have to be connected. You might not need this in your small office, but as you expand, you'll certainly need it. Though there are many ways to connect these nodes, some of the most common methods include Bluetooth, Wi-Fi, and so on.

These methods of connection are built on various topologies. The common ones are:

- Ring
- Bus
- Mesh
- Hybrid
- Star

Each topology has its strengths and weak points. Wi-Fi and modern Ethernet use a hybrid topology. The hybrid topology is a combination of bus and star. Bluetooth and Wi-Fi can also run on a mesh topology.

## Networking Topology – Logical Vs. Physical

The physical connection of network nodes doesn't necessarily dictate how they communicate. Typically, small offices and home networks use the physical bus topology.

- **Peer to Peer Networking**

In peer to peer networking, all the involved nodes are considered to be equal. All nodes can communicate free with each other.

There are no superior nodes with special responsibilities in this kind of networking.

- **Advantages of Peer to Peer Networking**

- ☐ The peer to peer network doesn't depend on a single node. It is, therefore, unlikely that the failure of a single node will undermine the entire network.
- ☐ Additionally, peer to peer network isn't sophisticated. This makes it easy to set up.
- ☐ A peer to peer network is quite reliable and resilient. It doesn't breakdown without a good reason.
- ☐ This network comes with an excellent distribution of data traffic. And that makes it tremendously effective.
- ☐ The hardware used in peer to peer networking is inexpensive. So, the initial cost of running this network is affordable.
- ☐ Most networks require a strong central administrator. However, the peer to peer network doesn't rely on a central administrator.

- **Disadvantages**

- ☐ It is challenging to secure a peer to peer network. This makes it susceptible to threats.
- ☐ Every network requires a backup. Nonetheless, peer to peer the network is difficult to back up.
- ☐ Locating information on a peer to peer network isn't easy.

- **Client-Server**

A client-server network is based on a superior server. The server is tasked with a special role. For example, it could be a control or a web server.

The client has to connect to the server to use certain services. An example of this type of networking is the internet web.



- **Advantages**

- ☐ The client-server network is administered with the utmost ease.
- ☐ It has a specially dedicated node that makes locating of information extremely easy.
- ☐ A client-server has exceptional safety levels.
- ☐ This network is easy to manage.

- **Disadvantages**

- ☐ Servers can fail. When they fail, the network is jeopardized. These are single points of failure that greatly undermine the entire network.
- ☐ The client-server hardware doesn't come cheap. It requires a significant investment, which can be out of reach for both homes and small office owners.
- ☐ This network can get concentrated at some point. This may cause some downtime within a network.
- ☐ The best modern examples of a client-server network include Twitter, Facebook, and Google Search.

## Classification of Computer Networks

Computer networks are classified into various categories. The classifications are based on geographical locations, the relationship between the devices used, and access types.

### Classification Based on Geographical locations

**LAN-Local Area Network:** It links devices within one office or several offices. Ethernet and Token Ring fall within this category.

**MAN-Metropolitan Area Network:** It is a slightly larger network with the capacity to connect devices across buildings.

**WAN-Wide Area Network:** This is a massive network that links devices to multiple devices across countries. A good example of the WAN network includes the Asynchronous Transfer Mode and the Integrated Services Digital

Network.

**PAN-Personal Area Network:** This network is used within a personal area to link devices. It is the kind of network that you use to link your laptop to a printer.

## Networking Layers and Protocols

A protocol is a predetermined set of guidelines that dictates how computers should communicate with each other. HTTP is one of the popular protocols, which you may have across in your interactions with computers. This protocol supports communication between a particular web browser and its server.

Good examples of data link protocols include are Wi-Fi and Ethernet. These protocols shape the data as it appears on the media. Both of them use a physical address that's referred to as the MAC address. It has a capacity of 48 bits.

Other popular MAC addresses include the EUI 64 that has 64 bits.

Networking can be divided into numerous layers or levels.

There is the OSI network that utilizes a seven-layer model. Also, there is a common TCP/IP network, which uses a four-layer model. Here are the four levels of the TCP/IP network, and their respective examples:

- Data link-level- Ethernet or Wi-Fi.
- Transport level- UDP or TCP.
- Networking-IP
- Application level-HTTP

As the sending process is progress, these layers add a distinct header to the data. The headers are then systematically eliminated as the data moves towards its destination.

## Transmission Control Protocol

TCP provides a safe mode of transmitting data. The transmission takes place through IP packets. The packets have accurate error detection capability. All the data that's transmitted in packets reach as their destination as sent. Data can't be accidentally altered in any way. You can rest assured that the data

reaches its destination in its original order.

Before the process of transmitting data is initiated, there has to be a safe connection between the computers involved.

- It is the role of TCP to convert the data into packets.
- Other Applications Protocol in Networking
- FTP (File Transfer Protocol)
- File transfer protocol aids the transfer of various files of data between two computers. The computers need to have an active internet connection.
- Telnet (Terminal Protocol)
- Sometimes, the user needs to connect to a terminal mode. The terminal protocol enables the user to do so.
- SMTP (Simple Mail Transfer Protocol)
- SMTP is a protocol that simply the electronic mail service.

## **Chapter 6: Information Tech Guide**

Computer technology is used to assist and link people in the contemporary world in many ways. The laptops, desktops, and mobile phones they all network together to perform multiple operations at the same time. The government, individual, and organization depend on these devices for essential things like in the entertainment, food production, communication, education, care, and transportation.

### **Understanding Information Technology**

Information technology – It is the use of a computer, network, storage, and other devices into to secure process, create, store electronic data or information, and exchange all manner of electronic data. Computer technology is the study of computer networks and developing several software programs. It comprises of computer database design, programming, and networking. All these programs correlate to ensure that a computer works

properly.

A computer machine is a programmable device that is designed to operate arithmetic and logical operation given by the user and provides a desirable processed output. The computer has two major categories, which are hardware and software. The hardware consists of all layers of physical and tangible components of a computer, such as CPU (central processing unit), keyboard, monitor mouse, and motherboard. While Software is the instructions stored in a computer to run the hardware, these instructions command the computer to perform a specific task, and such Software is operating systems and applications.

Computer technology is any machine that takes commands and calculates the instructions accordingly; the operation can be record-keeping, bailing, planning, and transactions. All these operations take place in a commercially available machine that has been customized according to their functionality. Such machines that are common to our daily process are gas station pumps, ATM, barcode scanners, and GPS units. However, each of those machines they all rely on circuit boards and digital data to meet the demand and needs of the customer.

Most customers gain improvement in access to services through the internet by ordering products, send emails, scan the barcode through a smartphone, and read reviews before purchasing anything on the website. Most of the programs in television use audio, visual, and animation and special effects in the production of their programs. Audiovisual games employ graphics created by a computer and plugged in a laptop or home-based entertainment where the player can play by themselves or with others using the internet.

The use of applications on the mobile phone can be beneficial in the following ways:

make order in a restaurant, preservation in a hotel, book an appointment with a doctor, purchase movie tickets usually save time that could have been used to wait in a queue.

# Hardware

Computer hardware are physical, tangible components of a computer they include. Examples are:

Monitor, control unit (CU), keyboard, mouse, motherboard, central processing unit (CPU), hard driver, random access memory (RAM), and power supply.

## 1. CPU

It is considered to be the mind of the computer machine that performs all kinds of operations like data processing, storage of data, and instructions. CPU controls all the activities that make up a computer. There are three components of a CPU:

- **ALU (Arithmetic Logic Unit)**

It is the logical part of the CPU in a computer. When you need to carry out mathematical or logical decisions in a computer, the information is carried out by ALU. The ALU contemplates the information in bits. Bits are binary logic 0's and 1's. They are made up of memories built in the CPU know as registers, which are used to hold data, and data at this point is classified as binary information. They are processed accordingly to instructions.

- **CU (Control Unit)**

It is a component of a CPU in a computer that guides the operation of the processor. It communicates to the computer memory, output, and input devices and ALU on how to respond to the database instruction and does not process any data.

- **Memory**

Memory is a part of a computer that stores data and information that is necessary for functioning. There are two types of memories:

- **Ram** – Random Access Memory is the internal memory of the CPU that is responsible for storing data, programs, and

the result of an application. The mind is read and writes hence volatile meaning stores data when the computer is working. When the machine is switched off, data is lost or erased. Examples of RAM are Dynamic Random Access Memory (DRAM) - it is a physical memory used in personal computers. This type of memory must be continuously refreshed, or it loses its contents, and it is economical. Static Random Access Memory (SRAM) – this memory is faster and less volatile than DRAM; hence requires more power and very expensive and does not require to be refreshed. Synchronous Dynamic Random Access Memory this memory has a higher processing speed.

- **Read-Only Memory (ROM)** – this type of memory where you can only read, but you cannot write. This kind of memory is non-volatile. The information stored in this memory is permanent, the memory stores instructions that are required to start a computer machine or bootstrap. There are many types of ROM. Examples are MROM (Masked ROM), Programmable Read-only Memory, Erasable and Programmable Read-Only Memory and EPROM

## 2. Peripherals

These are devices connected to the computer externally when these devices are disconnected to the computer will still function, but the functions performed by the peripheral will not be available. Examples of peripheral are;

- **Monitor**

A monitor is a visual display unit and is the primary output device of a computer. They display images as small dots called pixels that are arranged in a computer in a rectangular form that sharpens the images. The size of an image will depend on the number of pixels used.

- **Keyboard**

It is an input device that helps to input data into a computer. It consists of keys that are responsible for inputting alphabets, numbers, and special characters into a computer. They can also navigate using the keyboard to perform a particular shortcut in a computer machine.

- **Mouse**

It is a pointing device that uses cursor. A control device that has a small box with a corpulent ball at its base, which intellects the movement of the mouse and sends the signals to the CPU to process data.

- **Printer**

It is an output device that is used to print processes data into a paper. Examples of printers are: Impact printers- They write the data by striking the ribbon, which is usually pressed on the document to print. Non-impact printers – this kind of printers print the characters without using the ribbon. They print the whole page of a paper at a time. They are a laser printer, page printer, or inkjet printers.

- **Joy Stick**

This kind of peripherals moves the cursor into a position in a monitor and used in a Computer-Aided Design (CAD).

- **Scanner**

This device allows the user to scan printed papers and converts them into a file that is used in a computer device.

## Wireless and LTE

These are devices that change electrical signals into waves; they connect a wired network using Wi-Fi. They are three main types of wireless devices which are WAN, PAN, and LAN. Wireless Wide Area Network made

through the use of mobile phone signals. They are created and maintained by a mobile phone service provider. Wireless local area network uses radio waves, but the backbone of these networks are sustained using cables with a wireless access point connecting the network. This kind of wireless can be used in a room to being used in an entire university or a hospital. Wireless Personal Area Network (WPAN) they are a form of network that is short in range. They use Bluetooth technology and commonly interconnect compatible devices near the central location. The range of WPAN has a variety of thirty feet.

The devices that are used by networks vary from computers, tablets, phones, and laptops and refer to as clients. When accessing the network through hotspot or use of a router in office or home, the device is referred to as the client. Some router can operate as a client; this can happen when a card is in a computer and connect to other access points or connect to more detached Apps. The Apps can be a standalone device that bridges between a wireless and an Ethernet or a router. The Apps can cover a wide range of areas using wireless networks depending on the power of the computer and type of antenna used by the device.

Some phones, laptops, or wireless router, can support a mode known as Ad-Hoc that allows the device to connect directly together without an access point between that controls the connections. Not all the computers have the Ad-Hoc, and some are hidden. The devices that Ad-Hoc enabled to create a mesh of network, and when they are enabled is called Mesh Nodes.

The wireless network that connects distance areas like two building they need a more focused antenna such as dish antenna. Dish antenna sent thin beams of the network into a specific direction. This long-distance coverage is called point to point connection; this means that two points are connected. The process requires two devices, one configured to the Access point and the other one as a client.

## LTE (Long Term Evolution)

It is a term mostly used as 4G LTE and is the standard wireless data. The transmissions that allow one to watch their favorite documentary online or download and watch it later very fast. 4g wireless communication was developed by the 3rd generation partnership project that provides ten times the speed of the 3G network on a mobile phone.



The 4G technologies are designed to provide an IP address based on data, voice, and multimedia streaming.

## An Overview of LTE

This is a name given to 3GPP evolved, standard requirement to deal with the increasing data throughout the provision of market. The group that started to work with 3GPP RAN standardized for LTE in late 2004, and by 2007, all the LTE features that were related to its functionality were finished. And in early 2008, most performance specification and protocol were finished and released.

## LTE Requirements

Requirements are written, and defined concept from scratch, absolute fashion, and others meant relation to UTRA nomenclature. The following are LTE design parameters:

- Mobility of up to 350km/h
- Spectrum flexibility, seamless coexistence with other previous technologies hence reduced flexibility and cost
- All systems should support data rates of 100 Mbps in a downlink and 50Mbps in the uplink, within a 20MHz bandwidth or a spectral efficiency value of 5bps/Hz and 2.4bps/Hz respectively.
- Downlink and uplink use throughput per MHz at five %point of CDF

The 4G is ten times faster than 3G, can download something at a speed of 22 and 5 Mbps, while 4G is a significant improvement over 3G. Most cellular phones carry and advertise their network as 4G LTE, as it sounds the same as 4G, and some of the cell phones display a 4G LTE. 4G and 4G LTE differences;

The consumer can tell the difference between a 4G and LTE by the speed of downloading something. The mobile phone companies are always updating their cellular LTE network and are closing a gap between a 4G and LTE. The

LTE-A is the currently fastest option available right now.

## Standard Definitions on Wireless and LTE

**Antenna** – Converts the electrical signals into radio waves and generally connected to a radio device that transmits the messages into a radio receiver and the interface between the electrical signals in radio and the movement of indicators through the inflight.

**Ad-Hoc Network** – this is a Device network that is available in a laptop or computer machine connections and is shown as a computer to computer networks. The Ad-hoc can be unplanned or decentralizes network connections.

**AP (Access Point)** – these are devices that allow other wireless devices to connect into a wired network using Wi-Fi.

**Ethernet** – This is a type of networking protocol that defines some cable and connections that are used for wiring devices together. In most cases, the Ethernet cabling is categorized into five or six e.g., a cell phone, computer, or tablet.

**Node** – this is an individual device in a mesh net of the network.

**Power over the internet** – these describe as the system which passes electrical control along with figures on Ethernet cabling.

## Cabling

A cable network is a service delivery that supplies the devices like computer, television or a laptop programs that a user has subscribed to. The availability of such depends on the local franchise area. The number of available channels and networks will depend on some factors. The average cable viewer has the option of viewing more than 150 networks through a cable subscription. The cable system manager decides on the channels and networks to be carried on a specific place. The channel and network are selections are based on the viewer analysis and franchise agreement with the viewer.

## Types of Cable Network

They are three different types of a cable network:

Basic, pay and pay per view. The basic network is available per at the lowest and is very popular for people whose budget is limited. There are at least 60

cable channels that can be defined as a first cable network.

The pay cable network is those that charge a flat monthly subscription. The flat-rate payment is required as the network does not run any television advertisement. Hence they need some monthly subscription in order to profit the company. A movie TV station is a good example of such a network.

Pay per view cable network is TV channels that charge a fee for every individual program watched. The pay-per-view program is a network that shows movies that can be rented and viewed. Other programs allow the customer to go and watch the program elsewhere, like the movie theatre.

## Choosing a Cable Network

You can only choose one cable network; each cable provider tends to offer cable packages that deliver different level of programs. An example, a basic cable network may provide 60 channels, and premium offers over 100 applications. It's only you who can choose the best package that fits your budget.

## Advantages of Cabling Network

It is essential to evaluate the cable network before installation. A net that will make use of physical cabling will be more robust and secure compared to wireless network technology.

**Security** – This is the most important advantage as the cabling network offers a higher level of security than the wireless networks. However, the measure of protection will include the protected WI-FI network and passwords that help to improve the safety of a wireless network. Hence they can never be securing than the cable network.

**Speed** – not all the cable networks will provide speedy connections, but the newer types of twisted data cabling can operate up to 10 gigabits. An example is a fiber optic cabling transmits light rather than standard data information, making it optimal for high speed and ranges.

**Reduced interference** – with a proper installation cabling network will help reduce the interference caused by electrical hitch, known as electrical, mechanical obstruction, and radiofrequency. On the other hand, the wireless network is more susceptible to radio frequency interference.

**Consistence connections** – Compared to the wireless connection, the cabling is more consistence in connection. When the data is transferred in wireless

connections, there is a lapse in network connections caused by electrical interferences.

**Expandability** – Each router or a hub will provide support of up to 255 devices.

# Cybersecurity

Cybersecurity is a process or practice that is designed to protect network programs, devices, and data from being attacked, unauthorized access or damaged.

## Significance of Cybersecurity

Most of the co-operations and organization collect and stored in a large amount of data in storage devices, a large amount of the data can contain a large amount of sensitive information. Organization and governmental bodies transmit a large amount of raw data across some network and other devices while doing their business. Cybersecurity is dedicated to protecting the information, the programmers, and the system used to store data. The spying on these data are national insecurity and can lead to terrorism.

For an organization to function and coordinate effectively, they need effective cybersecurity. There are a few elements of excellent cybersecurity. They are:

- Great data security
- Application security
- Network security cloud security
- Endpoint security
- Mobile security
- Disaster recovery continuity plan
- And end-user education on security

The organization is advised to promote proactive measures and adapt more approaches to cybersecurity. The NIST (National Institute of Standards and Technology) issued necessary guidelines on the risk and a framework that recommends a shift on continuous monitoring and data focus approach to cabbing cybersecurity.

## How to Managing Cyber Security

The NCSA (National Cyber Security Alliance) gives a recommendation on a

top-down approach to cybersecurity, which organization management leads and prioritizing the management of cybersecurity. The NCSA advises all the organizations to be ready and prepared for any eventuality. Cyber risk assessment should be put in place in case of any behavior that impacts the functioning of the organization. The organization should have an outline of the damages that an organization would incur in the case of cyber-attack. The cyber risk assessment should consider any regulation that impacts the way the organization collects, stores, and secures data.

Having the best cybersecurity or combining cybersecurity measures and educating the employees on cyber-attacks is the best effort an organization can do to cab the cyber-attack. It may appear like a difficult task but it always to start small and focus on securing the most sensitive information hence going forward to protecting all the data

In conclusion, information technology helps organizations, individual businesses, and governments to increase their efficiency and improvements in effectively processing information. It helps the consumer to buy and sell new relevant technology devices, thus creating a world of business-minded people. Also, technology creates a safe environment by purchasing and installing CCTV cameras. Regardless, there is a continuity of demand for innovative technology solutions leaving room for advancement.

## Network Address

Networks come with an IP address. All devices attached to a network have an IP address. You can locate the device using its IP address.

An IP address (Internet Protocol Address) is assigned to every device in a numerical representation. This is for every device that participates in a computing activity. The device has to be, however, dependent on an internet protocol.

The IPv6 and the IPv4 are the two common versions of the Internet Protocol. IPv4 has been used since the birth of the internet. It is used both in corporate networks as well as the internet. Networking experts predict that it will be replaced by IPv6 in the future. This is attributed to the fact that the IPv6 has a larger capacity. While the IPv4 is just 32 bits, IPv6 is 128 bits. This means that it can effortlessly accommodate a larger number of devices.

## Functions of the IP protocol

During the sending of data, the initial data is decomposed into datagrams. Each datagram has a header. The header consists of the port number of the destination and the IP address.

Datagrams are sent to specific gateways. The process is successive as the gateways are sent from one gateway to the other. This process goes on until the datagrams reach the intended gateways.

## Private and Public IP Addresses

You might have heard of private IP addresses. Such addresses are not routable. They can be used in both business and home networks.

On the other hand, public IP addresses are routable. They travel on the internet.

## Assigning of IP Addresses

In case you are wondering how IP addresses are assigned, we will tell you how.

For modern networks, IP addresses are assigned automatically. This happens under the DHCP. It doesn't mean that they can't be assigned manually. It is possible, but only on rare occasions.

### Domain Names and IP Addresses

People prefer to use names as a form of address. Names are easy to remember. But computers use numbers. If you type a domain name into a web browser, the system translates into an IP address. A DNS server that's found on the internet is tasked with the translation process.

## Data Transmission

There is a lot of data transmission that takes place within a network. How does it take place? Data transmission is done through packet switching. The messages are first segmented into segments that are known as packets. The packets are then transmitted from one computer to the next. Upon delivery, data is then extracted from each of these packets. The original message is then reconstructed.

The packets are well-coiffed. They have a data area and a header. Headers consist of two addresses. That's the source and the destination address. Additionally, the header carries sequencing information that helps to reconstruct the original message.

# Importance of Networks

A computer machine has been designed for the sole purpose of manipulating data. When computers are linked together, great things are accomplished. The networks are instrumental in the sharing of information and other resources among people. These resources include the internet, file sharing, and applications.

Networks make it easy for colleagues to communicate either through email or other platforms available on the internet. The same applies to industrial computers because the information has to be shared constantly.

Networking enables businesses to save money. For example, instead of buying a printer for all your employees, you can use networking to link one printer to many computers. This allows all your employees to share a single printer effectively.

## Similarities between Different Types of Networks

Although there are various types of networks, there is a similarity between them. For example, networks share servers. These are computers that are endowed with sharable resources within a particular network.

## Other Similarities

The server serves clients. Clients are computers that access depends on the information held on the server. They all access the pool of information offered by a network server.

A Connection medium that enhances the connection of several computers within a network

Another similarity is computer peripherals. Printers and files are also used within different networks.

As you can see, computer networking is a well-structured process that makes work easy. Government agencies and business organizations use to rely on networking to streamline their functions. Networking saves such organizations millions of dollars every year.

Besides that, networking helps organizations to work more efficiently. Teams can tackle various projects with much ease when they network.

Networking aids the sharing of important information between the involved parties. Organizations store massive information. It is difficult to store, manage, and process the data manually. Moreover, organizations are large. And all the data that's gathered and used can be overwhelming.



Apart from the complex duties that simplified by networking, there are other minor but equally important functions. For example, networking aids the configuration of various computers in an office. This enables the employs to share the fax machine, or a printer through a network.

It is not only a large organization that benefits from networking. In this digital area, all types of businesses depend on networks. Therefore, it is important to be familiar with the concepts of networking.

# Chapter 7: What Are the Best Network Monitoring Tools?

Networking is also referred to as computer networking. It is a term used to refer to transportation and exchange of data between nodes through a universal medium in the information system. Networking involves using a network, designing construction, managing, maintaining, and operating the network software, infrastructure, and policies.

Networking allows for the connection of devices and endpoints together on a local area network or a bigger network. This is one of the most effective services that business owners all over the world can take advantage of. Computer networking provides valid and reliable ways of resources and information sharing within an organization or a business. It helps people to benefit from their information technology equipment and systems.

The significant benefits of networking include:

**File sharing** – Data can be easily shared among different users. Data can as well be accessed remotely when it is kept on other connected devices.

**Resource sharing** – Computer networking helps in sharing resources between different peripheral devices connected to the network. They include copiers, scanners, and printers. Resource sharing helps to save money because the software can as well be shared among different users.

**Sharing one Internet connection** – Having a single internet connection is cost-efficient and enhances the protection of systems when the network is adequately secured.

**Increasing the storage capacity** – Networking allows for the access of multimedia, and vital files when they are stored remotely in other networks-connected storage devices and machines.

Computer networking also improves communication in that customers, staff, and suppliers easily share information and keep in touch. It allows for everyone interested in business access common databases, thus avoiding duplication of data, preventing errors, and saving time. Networking also makes it easier for organizational staff to work on queries, thus delivering better standards of service. The improvements are possible because of customer's data sharing through the networks.

Computer networking also has incredible benefits on costs. Information is stored in one standard and centralized database, thus increasing the efficiency of the drive and reducing costs. Staffs are able to deal with many customers in little time because they are all accessing product and customer databases. Minimum IT support is also required because network administration can be efficiently centralized. Sharing of internet access, and peripherals sharing can also help in cutting costs.

Improving consistency and reducing errors are other significant benefits of computer networking. This is because all staff in a business or organization are accessing similar information and from a single source. It allows for the easier making of standard version manuals and directories accessible to each staff. Backing up of data from individual points on a scheduled basis provides for consistency.

The skills required when operating computer networking entirely depends on the network's complexity. Large enterprises, for instance, may have more security requirements due to multiple nodes. Such companies, therefore, require experienced network administrators who can successfully manage and maintain the network. This may be different from smaller organizations whereby there are few nodes involved, thus requiring less security.

## Basic Fundamentals of Computer Networking

Computer networking has been in existence for quite a long time, and as years go by, advancements continue to be made. Networking involves multiple devices such as routers, computers, and switches being connected to each other through wireless signals or cables. Building a wireless network needs one to understand all the basics of joining networks.

Many people have an aim of becoming expert IT technicians, and understanding only the hardware may not be so helpful to them. Many people get stuck at the networking point due to misunderstandings. The paragraphs below will explain some of the basic fundamentals of networking. They will give an understanding of how computers communicate through networks. Understanding the interaction and communication between computers is essential to anyone who wants to become a networking administrator.

Networking protocols are essential for developers dealing with applications relating to servers that use JAVA or programming based on Socket, such as bash or python, as well as System Admin. Computer networking is done

through diverse sets of IP protocol suites. The most popularly used protocols include IP and TCP. IP is an abbreviation for Internet Protocols. Each of the protocols has unique architecture, as well as diverse functionalities.

## The Internet Protocol

The internet protocol gives the definition of the networking communication protocols principals. It is helpful in relaying many datagrams through network boundaries. The internet protocol's primary purpose is providing routing functions that help in the establishment of inter-networking connection, enabling the internet. The primary function is delivering packets from one host to the other host while depending on present IP addresses. The IP addresses are available on the packets' headers.

The internet protocols have four layers, with each layer having a set of instructions it carries out. The four layers include the application layer, the data link layer, the network layer, and the transport layer.

### 1. The Basic Fundamental of Networking Layer – The Application Layer

The application layer appears at the topmost of IP and TCP protocols in networking. The primary purpose of the layer is transferring data through computers from a particular end to the other. The application layer works in conjunction with processes and applications using transport layer protocols. The processes and applications transport explicit instructions that help in the execution of tasks and enhances communication with the second layer. Application layer protocols have the following elements.

**Hypertext transfer** protocol that is commonly applied in modern webs. It provided a base for the founding of the World Wide Web. The protocol acts in the form of requesting and responding. It engages in multiple activities for the client.

**File transfer protocol** engages in the transfer of data to several networks. Its main tasks involve transferring and controlling data between computers using client and server architecture models. In many cases, the protocol can either use a password for authentication or can anonymously and automatically connect.

**A simple mail transfer** protocol is used when transmitting emails. The protocol is based on texts. It consists of three elements the MAIL that determines the returning address, RCTP allowing for connection with the

recipient, and DATA acting as the message's body.

**The simple network management** protocol is based on IP addresses. Its principal function is consistently collecting information on IP addresses from different machines. There are many devices that support the use of a simple network management protocol. There are also many diverse versions of the particular protocol.

## **2. The Basic Fundamental of Networking – The Presentation Layer**

The presentation layer works on the translation or converting data, for instance, encoding character, and compressing data between software applications, and networking devices. It is considered to be efficient when dealing with secure transactions such as money transfer and banking. It is useful because it allows for encryption and decryption of such reliable data. The presentation layer also helps in the conversion of formats.

## **3. The Networking Session Layer**

As a basic fundamental in networking, the networking session layer has the responsibility of opening, closing, and managing end-user application's sessions. The sessions can include many requests and responses taking place inside the software. The layer also facilitates the combinations of packets as well as sorting them in an appropriate order.

## **4. The Transport Layer**

The task of the transport layer is communicating with the application layer about transferring data to the necessary hosts. In performing its role, the transport layer uses the transmission control protocol in most cases due to its reliability. The control protocol helps in the transmission of data from the application layer into smaller sizes of data and later transferring them one by one to the network. It is commonly used when people want to download and upload large files. It ensures there is no loss of packets that could lead to the corruption of downloaded and uploaded data.

## **5. The Networking Network Layer**

The networking network layer is also referred to as the internet layer. Its main purpose is to route data above networks. The Internet protocol is used when differentiating addresses. The internet control message protocol is commonly used in commanding the ping to check on whether the host is active. It also sends error messages through the network, describing if a host is not

responding or is down.

## **6. The Networking Data Link Layer**

It is also referred to as the Network Interface Layer. Its main function is providing drivers for diverse devices found in the Operating System. The drivers communicate and transfer data to networks. The network interface card facilitates communication between devices. The transfer of data is done either through cables or wirelessly through routers and Wi-Fi. The significant protocols used in transferring data are the address resolution protocols and point to point protocols.

## **7. The Networking Physical Layer**

The physical networking layer is a vital layer found in the OSI computer networking model. It comprises of networking hardware. It is considered to be the most complex layer in networking due to the diversity of networking devices that are available. Its primary function is transferring raw bits over physical hardware through nodes used for the connection. It comprises of the hardware, including the wireless hardware consisting of Wi-Fi, connectors, cables, and network interface cards.

# **Understanding Cyber Security**

Cybersecurity is also referred to as computer security or information technology security. It is the act of protecting computer systems from damage or theft to their software, hardware, and electronic data. It also means preventing the misdirection and disruption of computer systems from the services they are responsible for providing.

The increase in dependence on computer systems, wireless networks, and the internet has led to the popularity in the field of cybersecurity. It is one of the most concerned matters in the contemporary world due to overgrowing cases of cyber-attacks and threats. Due to its complexity, cybersecurity has also become one of the challenges facing the technology field today.

Cyber attackers are making use of more refined techniques to target and attack computer systems. Small and large organizations, as well as individuals, are being impacted by these cyber threats and attacks. They have considered cybersecurity as a priority in their everyday operations. The focus is on coming up with the best measures to control and eliminate cyber threats and attacks. Employees in organizations are being trained on the best measures to deal with cyber-attacks. Almost everything we do today is linked

to the internet, thus increasing chances for vulnerabilities, flaws, and breaches.

Cybersecurity is defined as a process and techniques that are involved in the protection of sensitive data, networks, computer systems, and software applications from potential cyber-attacks. Cyber-attack is a terminology used in covering multiple topics. Most of the common issues covered by cyber-attacks include exploitation of resources, disruption of the normal functioning of businesses and processes involved, tampering systems, and the data stored in them, unauthorized access to sensitive information and targeted systems, and use of ransomware attacks in encryption of data and extortion of money from victims.

Cyber-attacks have been quite innovative, and attackers can disrupt security and hack computer systems. Businesses, therefore, have to come up with strategies through which they can effectively fight back the dangerous attacks. Understanding the importance of cybersecurity needs one to recognize some common forms of attacks and threats.

**Ransomware** – This is a software program involved in file encryption. It uses exceptional algorithms in robust encryption in encrypting files within the targeted system. Ransomware threat authors, applies a rare key for each target, saving each on a remote server. Users are, therefore, unable to access these files through any application. The attackers take advantage of the situation by extorting money from the victims for decryption of data or providing the decryption code.

**Botnets Attacks** – The main reason for designing botnets was for them to perform particular tasks in a group. Cyber attackers are, however, using them for all the wrong purposes. They use it by accessing and injecting malware or malicious code that disrupts the functionality of the network. Common botnets include spreading spam emails, stealing of personal data, and distributed denial of service. Large-scale organizations and businesses are primary victims of botnets attacks because of colossal data access.

**Social engineering attacks** – Cybercriminals are using social engineering attacks strategy to gain computer user's sensitive details. The tactic involves tricking users through attractive prizes, advertisements, huge offers, and requesting the user to feed their confidential and bank account information. The information that users feed is cloned and used in identity and financial fraud.

**Cryptocurrency Hijacking** – Cryptocurrency hijacking is a new addition in

the modern cyber world. Advancement in digital mining and currency has led to an increase of cyber-crimes. Cybercriminals are coming up with ways through which they can benefit from cryptocurrency. Traders and investors who focus on cryptocurrency are becoming primary soft targets for this form of attack. The hijacking process involves designing and injecting mining codes silently to the computer systems. The crypto jacker uses power resources, GPU, and CPU of the target system in mining for cryptocurrency. Monero coins are particularly mined utilizing this kind of technique. The target victim usually incurs the vast internet and electricity bills. The lifespan of the victim devices is also reduced.

**Phishing** – This is a common cyber-attack whereby the attacker sends a spam email and attempts to imitate any legitimate source. Emails sent through phishing usually have strong messages and are followed by attachments such as big job offers, and an invoice. The aim of the attacker is to steal confidential and sensitive data. They are able to gather information such as credit card numbers, login credentials, and information on bank accounts. Email filtering techniques can help one in avoiding such attacks.

Experiencing cyber-attacks has become so prevalent in most organizations and businesses today. It is vital to research techniques being applied and the measures to avoid these attacks. Educating oneself on the basics of cybersecurity and its use can as well reduce the risks of being attacked.

Cybersecurity is a broad term based on three major concepts. The concepts are named "The CIA Triad." This means that it is comprised of confidentiality, integrity, and availability. The model was designed to act as a guide to businesses and organizations on crucial policies involved in cybersecurity in information technology.

## **1. Confidentiality**

These are the rules that provide some limitations to accessing information. Confidentiality consists in taking appropriate measures to eliminate the risks of confidential and sensitive information being accessed by cyber hackers and attackers. In most organizations and large-scale businesses, people are either denied or allowed access to information depending on how it is categorized. The right person in each department is authorized to access the information. Proper training is also given to these people about using strong passwords to secure their accounts and sharing information. Data protection is enhanced by changing how data is handled.



## **2. Integrity**

Integrity guarantees accuracy, trustworthiness, and consistency of data over a period. It ensures that the data in transit is not altered, deleted, changed, or illegally accessed. Appropriate measures are taken to ensure the safety of the data. A data breach is controlled through user access and file permission control measures. Change or breach in particular data can be detected by the use of appropriate technologies and tools. Regular backups help in coping with potential data loss, unintended deletion, or cyber-attacks.

## **3. Availability**

Availability means that all essential components, such as devices, networks, software, hardware, and security tools, should be adequately maintained and consistently upgraded. This helps in ensuring the proper functioning and data access without disruption. It also means providing consistent communication between multiple components by giving adequate bandwidth. Availability also means providing diverse equipment for security in case of any cyber-attacks. Disaster recovery plans, reasonable backup solutions, firewalls, and proxy servers are efficient utilities in coping with cyber-attacks.

# Chapter 8: Types of Firewall

A firewall is a kind of cybersecurity tool that protects a computer network from being tempered or compromised: preventing attacks from hackers who try breaking into the system from outside. Firewalls can be in various forms; it can be in the form of a software or hardware on a computer. For a firewall to work efficiently, it has to be connected to at least two network interfaces with one protected and the other that is exposed to attacks or threats. Therefore, you can consider a firewall to a form of gateway installed between two sets of a network.

## How Do Firewalls Work?

Having known what firewalls are and what they do, it is time you learned how they work! Firewalls work by examining all the available data packets that pass through them to assess whether they meet the guidelines and regulations posed by the Access Control List (ACL) and created by the person administrating the network. If the data packets meet the rules set by ACL, they will be allowed to maneuver inside the connection.

Additionally, firewalls play a critical role in keeping a log of essential procedures and activities occurring within a network. Again, the necessary actions are only identified by the administrator. He then configures the related firewall to keep the logs basing on the level of importance.

The process of filtering logs can be done basing on several things, including the packet attributes, address, state, and protocols. Firewalls, however, only display the packet headers on screens.

Having known how firewalls work, we next discuss the types of firewalls. Read on to find out!

## The Types of Firewalls

Firewalls are categorized into different types. This is done depending on the level of security they provide and the advancement they have. Below, we discuss extensively on the types of firewalls in existence today.

- **The Packet Filtering Firewall**

This is a type of firewall that is usually installed on routers that connect or link the network in the inside to the internet. The package filtering firewall is only implemented on the OSI model of a network layer. It works based on the rules defined by the Access Control Lists. Packet filtering firewalls work by checking the whole set of packets provided and verify them against the set of instructions provided by the administrator through the ACL. In situations where a package doesn't meet the set of rules defined by the administrator, that packet gets dropped immediately, and logs are informed and update accordingly. When using packet filtering firewalls, administrators have the power to build their ACL basing on the protocol, address, and packet attributes.

- **Advantages of Packet Filtering Firewalls**

- ☐ One of the significant benefits of packet filtering firewalls is that they are very affordable.
- ☐ Packet filtering firewalls also need lower resource usage to make them cost-efficient.
- ☐ Additionally, they are the best suited for those of us with smaller networks.

- **Disadvantages of Packet Filtering Firewalls**

- ☐ As we mentioned earlier, the packet filtering firewalls only work network layers, and they cannot work on complex instruction based type of models.
- ☐ Additionally, packet filtering firewalls are also very vulnerable, especially to spoofing on most occasions.

- **The Circuit Level Gateway Firewalls**

This is a type of firewall that is installed at session layers of any OSI model. They are used to monitor events and sessions such as the TCP multiple way handshakes to determine whether the connection requested is legit or not. In circuit-level gateway firewalls, the significant and vital screening takes place before the link is launched. The information channeled to a computer device on the other side of the network via circuit-level gateway looks to have come from a portal. This feature plays a vital role in establishing cover stealth for

private networks from strangers.

- **Advantages of Circuit Level Gateway Firewalls**

- ☐ Just like the Packet Filtering Firewalls, the circuit-level gateway firewalls are also very affordable and cost-friendly.
- ☐ Circuit Level Gateway Firewalls also give the private network anonymity, making it very secure from threats and hackers.

- **Disadvantages of Circuit Level Gateway Firewalls**

- ☐ One of the significant drawbacks of the circuit-level gateway firewalls is they are not able to filter the individual packets. This makes them very vulnerable because once a connection is established, hackers can take advantage of it.

## The Application of This Kind of Firewalls

The gateway firewall circuit levels are applied in many dimensions of technology in today's world. The application-level gateways, for instance, are used in the layer one in the application of an OSI tool and can give security and protecting the specific Application Layer of the Protocol in question. One good example of the level application Gateway Firewalls is the proxy server. This kind of firewall, however, can only work with protocols that are highlighted. A good example is, if you installed a web application basing on a firewall, it only will be able to enable the HTTP Protocols Data. The Circuit level gateway firewalls are meant to understand app-specific commands like the HTTP: POST and HTTP: GET as installed on application layers for Special Protocols.

Additionally, the application level firewalls can also be used as the caching servers that play an essential role in improving network performance, making it easier to log the level of traffic.

## The Stateful Multilayer Firewall

This firewall is made of a combination of all the firewalls we have discussed so far. They are very advanced firewalls and complex in equal measure. Stateful Multilayer Inspection Firewalls can be used to filter the packets in network layers through the use of ACLs.

Additionally, the Stateful Multilayer Inspection firewall also checks for the single sessions provided on the session layers as well as evaluating packets on the ALG. This type of firewall is compatible with transparent mode enabling direct linkage and connections between the server and the client, something that wasn't possible a few years ago. The Stateful multilayer inspection firewall implements the algorithms and critical security models that are specified by protocols; hence, in the long run, making data transfer and connections easier and secure.

## The Proxy Firewalls

These kinds of firewalls operate in application layers with the primary purpose of filtering the incoming traffic between the current network and the source of traffic; this explains the name 'proxy firewall.' Proxy firewalls are transported through a cloud-based tool or a different proxy element. Instead of allowing traffic link up and connect directly, it first identifies a relationship or connection to the origin of traffic and verifies the data packets that come in.

This kind of inspection can be compared to that of a Stateful multilayer inspection firewall because it focuses on both the TCP multiple way handshake protocols and the data packets. Proxy firewalls, however, can also carry out deep-layer packet checks and inspections, verifying the real contents of the information-carrying package to ascertain it has no malware.

Upon completion of the check and the data, the packet is given the green light to proceed to the destination; the proxy firewall transfers it off. This procedure builds another layer of gap or separation between the individual devices on operating on your network and the client. This enables them to make another layer of anonymity hence securing your network.

The major advantage of Proxy Firewalls is that they are more secure thanks to the extra layer of anonymity created. They are also pocket-friendly and affordable.

If there is any setback when using proxy firewalls, is that they can slow down the entire internet because they require more steps during the data packet transfer process.

# The Software Firewalls

This refers to any firewalls installed on a local device instead of a separate piece of hardware. One of the significant advantages of software firewalls is that they are critical when defensive measures by separating the individual network point end from each other.

One of the significant setbacks of software firewalls, however, is that maintaining them on different sets of devices can be time-consuming and extremely difficult. Additionally, some tools on the network connection may not be compatible with any of the software firewalls. In such occurrences, you will, therefore, have to use various software firewalls for every asset.

## Hardware Firewall

This is one of the most popular types of firewalls in the world. The hardware firewall is applied majorly in the modern-day networks as either a LAN network or a border device (used to protect internally placed LAN networks acquired from the internet or any other unwarranted networks) or protecting the internal systems in more significant enterprises. The hardware firewalls mostly have a lot of physical network attributes that can be applied in creating various security zones that are different from Layer 3 elements. Every physical tool can be categorized further into sub-interfaces that, when well propagated, can help expand the secure zones.

When the hardware firewall is operating on its separate hardware application, it can handle vast volumes of data packets as well as millions of network connections. Hardware firewalls work best in generally high performing machines. The feature that makes the hardware firewall one of the best firewalls to work with is the ability to keep hackers and threats at bay. They are well advanced to alert the administrator of any potential risks and how they can deal with them. Hardware firewalls are, however, more expensive compared to the other firewalls.

Some of the most popular brands that use the hardware firewall are FortiGate, Checkpoint, Sonic Wall, and Palo Alto.

## The Application Firewall

Just as its name goes, the application firewall is a type of firewall that operates at layer seven of the operating system model. Its primary functions

are controlling and inspecting the data packets at every application level. This firewall has information about what a typical application should have and that a malicious use contains. It is, therefore, well equipped to filter out any unwarranted access.

For instance, the app firewall that secures a website server has knowledge of the web associated HTTP attacks such as cross-site crippling, and it guarantees the application from such threats by checking into HTTP app traffic. Some of the popular elements that use the application firewall are the Web app firewall. The website app firewall protects the traffic from internet users that come in towards the computer network. Application firewalls are fast gaining popularity thanks to its affordable pricing. It is also one of the most efficient firewalls that help keep threats and hackers at bay.

## The Next Generation Firewalls

The next-generation firewall is a term mostly used by manufacturers to refer to a brand of firewalls that are advanced and use high technology standards. What this means is that the next generation firewall combines almost all the firewalls we have discussed above. It is a state of the art kind of firewall that gives application-level inspection and protection.

The next-generation firewall provides comprehensive analysis and inspection and can locate corrupted traffic in all the layers of the OSI model and any layer associated with it. It contains a host of advanced features, including antivirus features, intrusion detection, and prevention, among others.

These features are, however, licensed separately, forcing any interested buyer to spend a little more money to activate all the protections. A good number of next-generation firewalls establish communication using the cloud service security that belongs to the manufacturer to obtain the threat level information from the secure cloud.

What makes next-generation firewalls very efficient is that they have a combination of other features that are well advanced and able to deal with potential threats and incoming hacker detection. The feature that makes the next-generation firewalls one of the best firewalls to work with is the ability to detect security threats even with the slightest detection of malicious activity. They are well advanced to alert the administrator of any system dysfunctions and how they can deal with them. The next-generation firewalls are, however, more expensive compared to the other firewalls. The reason behind this, however, is that they are more advanced and sophisticated

compared to any other firewall.

## The Stateful Inspection Firewall

A majority of the modern-day firewalls put into use the feature of stateful inspection. This might be difficult to understand, and the example highlighted below will help you comprehend it.

In a communication medium between a server and a client (for instance, a person with a website browser engaging in a conversation with a web server), the indicated client browser will initiate an HTTP communication with the server serving the website at port 80. Now assuming that this firewall (the state inspection firewall) allows the HTTP traffic being transferred to pass through it, the data packets will, therefore, be able to reach the servers, which will initiate an instant reply as it is the case with every TCP communication model.

The stateful inspection firewall will store the initiating link that exists between the client, and the server is what is called a state table. The table will have information about details such as the destination IP, the source IP, TCP flags, and the destination ports. This means that any reply coming in from the external web servers that are similar to the connection installed before will have to go through the firewall first then reach the designated servers without the need for extra configuration. The above-mentioned process makes setup easier since the user doesn't have to apply any set of rules on the firewall to reply to the incoming data packets. The data packets mentioned above will instead be allowed automatically only if they are associated with the already installed network connection from the client to the server.

The feature that makes the stateful inspection firewalls one of the best firewalls to work with is the ability to detect security threats even with the slightest detection of malicious activity. They are well advanced to alert the administrator of any system dysfunctions and how they can deal with them. The stateful inspection firewalls are, however, more expensive compared to the other firewalls. The reason behind, however, is that they are more advanced and sophisticated compared to most of the firewalls.

## Telephony-Related Firewalls

Just as its name goes, the telephony related firewalls are a type of firewall that operates at layer seven of the operating system model. The primary



functions of telephony related firewalls are controlling and inspecting the data packets at every application level. This firewall has information about what a regular application should have and that a malicious use contains. It is, therefore, well equipped to filter out any unwarranted access.

For instance, the app firewall that secures a website server has knowledge of the web associated HTTP attacks such as cross-site crippling, and it ensures the application from such threats by checking into HTTP app traffic. Some of the popular elements that use the application firewall are the Web app firewall.

The website app firewall protects the traffic from internet users that come in towards the computer network. Application firewalls are fast gaining popularity thanks to its affordable pricing. It is also one of the most efficient firewalls that help keep threats and hackers at bay.

# Chapter 9: Understanding Cybersecurity

Cybersecurity is the protection of computers' mobile devices, servers, networks, data, and electronic systems from cyber-attacks and malicious viruses. Cybersecurity can also refer to as information technology security. Cyber securities are designed to protect and maintain the confidentiality of the data stored in the internet-connected systems. The organization should have a secure and effective response to cyber-attacks. The purpose of installing such security measures is to prevent data breaches and identity theft. Cybersecurity is classified into the following categories:

- **Information security**

The protection of data from unauthorized personnel. Goals of securing data protect the confidentiality of the data and preserve the integrity of information either in storage or in transit.

- **Application security**

The procedure of developing, adding, and testing safety features in an application to prevent security attacks against opportunistic malware. A conceded application could make available access to information designed to protect the device. Adequate security always begins at the designing of the app even before the application is installed.

- **Network security**

They are policies and practices implemented to break and monitor accessibility, modification, and misuse of computer or mobile network from unauthorized. The security of the network mostly involves authorizing access of information to authorized persons and usually controlled by the administrator. Network users are assigned by passwords and authority

information to access data and programs that are within their security clearance.

- **Operational security**

Operational security includes the processes that recognize and identifies critical information, also determine whether the information, if accessed by malicious individuals, could be useful to them. Operational security also executes and selects a measure that removes any exploitation of helpful information.

- **Disaster recovery and continuity of business**

It is a planning strategy that is capable of restoring data and critical information in inventing that the system was hacked or destroyed during the disaster. When protecting your data, it is good to understand and plan. The plan arises when the application and usage of information after disaster tricks. Continuity of business includes a strategy and action that guarantees that the business will continues after the disaster.

- **End-user education**

The cybersecurity starts with your employees. The end-user is the specific person who uses the hardware device or software program after installation in the machine. Make sure that you educate your employees or yourself on the matter concerning software program or device. The end-user education plays a vital role in keeping the information of the organization safe. The end users are the first line of protection against cyber-attacks.

## Importance of Cybersecurity

Cybersecurity considers as most important to an organization, government, institution, and individual. It is essential to protect the family and loved ones from cyber fraud and identity theft. Most of the cyber-attacks happen because of lack of awareness. Cybersecurity has always evolved since the discovery of computers. The modern-day the cyber attackers have improved their tactics in breaking down the systems also installed the internet has improved,

making it easier to attack the businesses.

The attackers have developed tools that are designed to exploit the weaknesses of the computer or mobile device. Most hackers do not attack the network, but the website or the server of the organization or individual. Hackers find it difficult to hack the network, as the most network of the organization has a firewall installed hence problematic for them to access. The following are the requirement for cybersecurity:

- Firewall
- Web filtering software
- Endpoint protection
- Intrusion prevention systems
- Radius server
- Logging software
- Encryption

Organizations and businesses can suffer a large amount of money when they fail to safeguard and handle confidential data effectively. There are numerous methods to use to make sure that your data is safe.

An example is hardening, which means that confidential data stored in the corner of a structure, meaning that the information stored inside of a hard shell that cannot be cracked. Placing logging software, any hacker who attempts to access the information in the hardened network will be logged and traced. Installing and using VPNs and encrypted links makes it harder for hackers to access your data. Most hackers will not invest too much to hack into a new security system. It takes time to hack the system, thus increasing the chances of getting caught.

Honeypot is another method of cybersecurity. Placing the right software in the system, any connection that goes in and out of the network can be traced fast. This area of the network is set deliberately and makes the network seem vulnerable. When the hacker attacks the systems, they go straight to the vulnerable area of the net. When they reach there, they steal files and later find out that the data are empty and leave a trace that they were attacking the system.

When cyber network security is secure, the attackers will use a method of

social engineering. Social engineering is the method of sending emails telling them to click here. Social engineering has evolved from being told to click here to taking place in internet browsing. Hackers apply the following tactics, phishing, vishing, smishing, and whaling. It is difficult to access the information that was lost since it appears that the data was gladly given. In social engineering, even the smallest mistake of giving out a password to a user account is enough to provide access to hackers to hack data and confidential information about the organization.

Salami cyber-attack hackers steal little money from several banks that lead to a large amount. These attacks can go undetected since the nature of the type of cybercrime.

An electrical protocol should be put in place to detect malware in real-time. The use of heuristic analysis is to observe the behavior of an application or a program to protect it against viruses that change their shape. The organization should train and educate and make them understand their part in keeping the data of the organization protected and report any malicious activity. The organization should put plans in place to deal with any attacks effectively and respond keenly to reduce the impact of the attack on the business.

## Data Security Measures and Its Importance

We live in a world where most people use electronic devices & systems in almost every deal and transaction. Technology has resulted in many computer networks and electronic systems, and indeed, they all deal with data. What you might not know is that data one element considered to be very valuable, and internet users are very keen to find out how their information and personal data are handled. Data is, therefore, a precious asset and can have a massive impact on people. It needs severe protective measures to ensure information is secure and brings us to what we shall be discussing in this article: data security and its importance.

## What Does Data Security Mean?

Data security refers to the technical process of safeguarding data and keeping it from corrupted and unauthorized access. It isn't all types of data that are essential and sensitive, but others are precious and essential. Having unauthorized people get access to that kind of information can cause a lot of problems because they can use them to do things they are not allowed to do.

Data security, therefore, is a defensive measure established to help keep data safe and out of reach for any unauthorized access. There exist a lot of ways you can protect data, as we have discussed below.

The basic concepts of any data security system are confidentiality, integrity, and, lastly, availability. The three concepts are commonly abbreviated as CIA. It is the underlying security model guiding organizations and companies to protect their valuable data from unauthorized people and hackers. Now let's break down each of the concepts and find out what they mean.

- Confidentiality is a concept that makes sure data is available to individuals with authorized access and does not fall in the wrong hands.
- Integrity makes sure that data is accurate and well reliable.
- Availability, on the other hand, is a virtue that makes sure data is readily accessible to serve the needs of clients.

So, what should you consider when setting up data security? Discussed below are some of the essential things you ought to consider when coming up with a security model.

Where is the valuable data placed or located? You can't say you are protecting something if you have no idea where that thing is put.

The other thing you should consider is who can access your sensitive data? If you have no records of people allowed to access sensitive data, leaves you at high risk if getting accessed by an unauthorized individual. Know who has access to your data because it will give you an idea of the kind of person you are dealing with, and it makes it easier for you to pinpoint any unauthorized access.

Have you actualized the consistent checking and instant alerting on the data? Activating real-time alerts and establishing a continuous monitoring process will ensure the security covers all high alert areas. The real-time alerts play a role in detecting any malicious activity, unwarranted access, and alerts the user before it gets too late.

Below we look at the types of data security, let us discuss some of the technologies used in data security.

## Data Security Technologies

Discussed below are some of the technologies applied in data security today. They are used to reduce the risk involved as well as preventing the security breaches.

- **Data Auditing**

Auditing data when a security breach occurs plays a critical role in preventing it from happening again. Data auditing helps discover essential details of what might have caused the violation. It revealed the people that had access to data during the time of the security breach, how it happened, and the path followed when accessing the file. This kind of technology, therefore, plays a vital role in the process of investigation.

Apart from that, when advanced data auditing solutions are implemented, the information technology administrators can have access to critical visibilities needed to keep unauthorized access at bay.

- **The Real-Time Data Alerts**

In typical situations in today's world, it will take several months for a company to notice they have been breached. One sad fact is that the majority of the companies realize there has been a security breach from their customers or other sources, instead of getting the information their information technology departments.

The real-time data alert technology and constant monitoring of data activity make it easier for you to be able to detect security breaches, accidental destruction, as well as unwarranted access to critical personal data.

- **The Data Risk Assessment Technology**

In light of what we have discussed earlier, the data risk assessment technology plays a crucial role in helping organizations know their most vulnerable kind of data and give information about how it can be fixed. The process of doing so starts by identifying the data that is very important and vulnerable, and it can be easily accessible. The risk assessment technology gives a summary of all the found details giving complex feedback on the level of vulnerability and alerts you where you need to work on first.

- **Minimize Data**

During the last ten years of information technology, there has been a significant shift in how people perceive data. In the past, people preferred having more data than less. The more data you had, the more ahead you were. In today's world, however, data is more of a liability. The potential loss of billions of shillings, securing breach that can destroy the reputation of an entire company as well as the hefty fines associated with collecting more data than what is recommended makes data a very risky asset.

In that connection, it is advised to have only the data you require. Don't ask for people's telephone numbers and home addresses when you only need their identification numbers.

Having learned the data protection technologies, we move on to the types of data protection. Read on to find out!

## Types of Data Security

As we have learned earlier, data security protects sensible and vulnerable data from unauthorized access. Almost everything in today's world revolves around computers and the Internet. Music and entertainment transport and infrastructure, healthcare, shopping, and other social aspects have all gone digital. Banks also run their transactions on online platforms.

This high dependency on the Internet should make us question the vulnerability of the information and data we have shared. How easily can critical data be accessed without an authorization? Such a question will automatically lead to putting security measures into place.

Discussed below are some of the data security types that can help protect your sensitive data.

- **Critical Security Infrastructure**

This type of data pertains to the advanced cybersecurity systems we rely on in modern society. Let us break it further down and mention a few examples of critical infrastructure: traffic lights, shopping centers as well as the electricity grid. Having any of these vital infrastructures makes it an easy target for unauthorized access and cyber-attacks. For instance, an electricity



grid can easily be a target of cyber-attacks.

Therefore, companies and organizations whose data involves the critical infrastructure should put measures in place to protect it from getting in the wrong hands. They need to understand the sensitivity of the information they are handling because it is a critical factor in society's well-being.

Additionally, those companies that do not directly deal with critical infrastructure should come with defensive measures to protect it because an attack on could have a significant impact on everyone, including them.

- **The Application Security**

This is one of the must-have data security measures you should consider. It works using the hardware and software techniques to handle impending security threats that can arise towards any sensible data.

Having practical information kept in applications is high risk because they are easily accessible over the Internet, and hackers will access it. Only do so when there are adequate security measures to keep data secured from unauthorized access.

Antivirus programs are some of the application security types. Such protective measures help ensure there is no unauthorized access to data. Additionally, these measures also provide companies that can detect any suspicious activities and puts in place defensive counter attacks.

- **The Network Security**

Having known that data security is more concerned with the threats coming from outside, the network security protects your data from any unauthorized access from people that could have malicious intentions. The network security system keeps data safe by regulating who has access to it and setting security measures; it also detects who has unauthorized access.

With the current technological advances, security measures are getting more sophisticated with the introduction of machine learning to regulate any abnormal traffic as well as detecting threats earlier enough. This type of data protection keeps on implementing procedures and policies that help in preventing unwarranted access and exploitation of data.

Examples of network security implementations include monitored internet

access, strong passwords, and software encryption firewalls.

- **The Cloud Security**

The cloud is a result of competent security measures. This is a kind of data security type that is software-based. It monitors and protects data in the cloud resources. Cloud security companies are consistently implementing and developing new cloud security tools that are playing a pivotal role in securing data.

There is a particular myth associated with cloud computing that it is insecure compared to other data security measures. People think that storing your data manually is more secure because you can control it. Research has, however, revealed that storing data in the cloud is safer than storing it physically in a hard disc. It is also easier to control data stored in the cloud.

In 2018, a research carried out by Alert revealed that data stored on-premise receives an average of 62 attacks while data kept in the cloud experiences an average of 25 attacks.

Storing data in the cloud is more secure, saves you the stress of regularly checking on it, and very affordable. It highly recommended using the cloud as your data storage platform. The future is even bright for cloud security thanks to ongoing technological advancements.

- **The IoT (Internet of Things) Security**

Internet of things refers to various critical cyber-physical elements, including printers, Wi-Fi routers, and CCTV cameras. IoT is a type of data security that focuses more on the networks, consumer devices, and other places where data is stored. There exist a lot of IoT devices that are vulnerable to security breaches. This, therefore, needs severe protective measures from all concerned users.

According to research, security is the biggest reason why enterprises hesitate about buying the Internet of things devices. They fear involving it in their business because sensible data might be accessed by unwarranted personnel. It, therefore, needs everyone's efforts to come up with measures of how data and information can be secured through the Internet of things. Failure to this, we shall be losing critical information and data to unauthorized people who will ruin it.

If your business is run on online platforms, for instance, someone can hack into your system and get your products for free. They can also take your funds and leave you in a financial crisis. This paints the picture of the importance of data security.

Next, we discuss some of the steps you should take when securing data. Read on to find out!

## Securing Data

Data security is vital not only for business establishments but for a regular computer user as well. We have discussed the various ways data is essential to us and why we need to secure it. Losing valuable information like bank account details, payment information, as well as client information, can be very difficult to replace. You can imagine the level of damage that can happen if such information falls into the wrong hands.

Losing data to natural disasters like fires or floods is crushing and mostly uncontrollable, but losing such sensitive data to malware infections or hackers can result in such dire consequences. The good news, however, is that you can control and prevent cybersecurity attacks. Discussed below are the measures you need to take towards safeguarding your data.

- **Assess the Risks**

Any data security measure begins with assessing the levels of risk available. This goes a long way in helping you identify the possible risks and what can be the case if you lost sensitive data through system crash or malware infections.

Below are other threats you are likely to identify during a risk assessment

- during natural disasters, such as floods, fires, and malicious damage.
- People authorized to have access to data.
- Identify individuals that regularly use the Internet and e-mail systems in which people are allowed to access sensitive data and those who aren't.
- The use of passwords and how you will maintain them.
- Which kind of firewall and malware solutions are you going to use?

- Educate and sensitize people working with you about what they should do when faced with a security breach.

After carefully analyzing the high potential security threats, go ahead and identify more severe risks and prioritize them. It is also advisable to outline a business continuity plan that your team will use in case of a system breakdown. You likewise frequently check security implementations to ensure they meet the standards of your growing business.

- **Secure Your Data**

After carefully assessing the security threats your data is facing, the next thing should be coming up with defensive measures to prevent that from happening. Given the seriousness of the threats sensitive information faces in the modern world, the best step you can take to keep off intruders should involve a combination of advanced technology, physical preventive tools as well as educated staff. Ensure you are operating on well-defined policies and make your staff is aware of them. Highlighted below are some of the steps you can take towards securing data.

Data security is vital not only for business establishments but for a regular computer user as well. We have discussed the various ways data is essential to us and why we need to secure it. Losing valuable information like bank account details, payment information, as well as client information, can be very difficult to replace. You can imagine the level of damage that can happen if such information falls into the wrong hands

- Install alarms and monitoring cameras in your data center or office.
- Don't allow public access to computers that contain manage sensitive data.
- Come up with active security measures that will restrict internet access.
- Always update the anti-malware system. An outdated system is as good as useless.
- Additionally, ensure the operating system is equipped with the latest features.
- Prevent hacking attacks by installing intrusion detecting

software.

- Ensure your system has a reliable supply of power.

- **Ensure Mobile Data is Secured**

In today's world, handheld devices have become a popular way of storing data and communication. It is, however, alarming how data is lost through such devices. Handheld devices are very vulnerable to data theft by getting damaged or being stolen. You, therefore, need to put different measures in place to ensure data is secured and safeguarded. Below are some of the things you can do.

- Always back up your data on removable devices and stored on multiple copies.
- Whenever the device is left somewhere, always activate the password protection.
- When you are in a public place, always ensure you don't leave the device in a home, it can be stolen
- Mobile devices are very fragile; always ensure you protect them from impending physical damage.

It takes a lot of effort to protect data from attacks and cyber threats. It might be costly in some cases, but it is worth every penny. Losing sensitive data to hackers can be something you will never recover from. To protect your data when you can!

## Importance of Data Security

From the beginning of the article up to this point, you are now aware of the significant data carries and why we should protect it. I believe that it has been well tackled. Next, we discuss the importance of data and why it should be kept from falling in the wrong hands. Below are some of the many essential uses of data.

- **Data is liable**

Those of us in the business industry will understand how data is important to

us and what it means by calling it an asset. The information regarding the type of products and services provided is essential. In business, for example, you cannot share your strategic plans with and financial objectives with a competitor, they will use it against you, and you will be on the losing end. Other forms of essential data, like client information, are also something precious. It will cost you a lot when such kind of information is breached and finds its way into the hackers. Not only will the clients sue you, but it will also affect the company's image seriously. You are therefore advised to keep information and data secure using the methods we discussed earlier in this article or risk losing it all. Consequently, it needs everyone's efforts to come up with measures of how data and information can be secured through the Internet of things. Failure to this, we shall be losing critical information and data to unauthorized people who will ruin it.

- **It Maintains the Business Reputation**

Almost all kinds of businesses provide products and services to their customers or rather clients. When a customer walks into your business establishments and buys a product or service using the credit card, they trust you with sensitive information. It is, therefore, up to you to keep such sensitive data secure and prevent it from reaching unauthorized personnel. Any kind of security breach, no matter how small that could lead to leaking of information, can have severe damage to the reputation of your business. The client whose data has been leaked might take legal action against your business and trust me; you won't like the consequences. All firms and companies are, therefore, advised to take data security seriously. It will not only impact your business negatively by tainting its reputation but by making you incur extra costs dealing with court proceedings and other legal actions taken against your business.

# **Chapter 10: Types of Cyber-Attacks and How to Prevent Them**

In computing, there are situations where sensitive information may face a threat of access by unwanted people. Computers and computer networks are the critical points where these data can be exploited and used for various reasons. People who gain access to this information usually attempt to steal, benefit, destroy, expose, modify, disable, or control. The access is often unauthorized and targets computer infrastructures, networks, information systems, and private data. This way, cyber-attacks can, therefore, be termed as cyber terrorism or cyber warfare undertaken by individuals, groups, organizations, or society.

A cyber-attack is, therefore, deliberate access to unauthorized information of computer networks, systems, and other technological devices by the use of malicious datasets or codes. The outcome is usually a disruption as well as the compromise of the information resulting in loss of essential data and identity theft, among others. Also referred to as computer network attack, cyber-attacks began in the 1980s and rose over the years. However, measures have been implemented, especially in government and institutional data, to ascertain the security of such information. An attacker, in this case, is an individual, group, or the process of data access to restricted information.

The prevalence of cyber-attacks has become rampant in different regions globally with 2017, seeing the rise of up to two billion stolen data accompanied by a ransomware payment reaching two billion US dollars. Some cyberattacks target private devices, therefore, resulting in identity theft, especially for banks and credit cards. Others focus on user sensitive details to access central databases. On the other hand, the world has also experienced global cyber-attacks where viruses have been planted in computers. Individuals behind such attacks often highlight their demands and provide an antivirus after their conditions are met. As such, there have been multiple types of cyberattacks depending on the attacker and specific data under threat.

## **Types of Cyber Attacks**

Denial of service attacks also includes distributed denial of service, is where the attacker targets the resource system of the computer and makes it unresponsive to service requests. However, the distributed denial of service attack originates from different host machines damaged by malicious software from an attacker. This type of cyber-attack does not necessarily provide direct benefits to the attacker. It only stops the whole process, which may become quite beneficial if the system is of a business competitor. Besides, denial of service attacks may come in handy when an attacker wants to launch an attack hence stops the resource system, including securities and firewalls, and commence an attack.

Denial of service attacks may also come in different forms, TCP SYN flood attack, botnets, ping-of-death, smurf, and teardrop. The TCP SYN flood attack is where the attacker targets Transmission Control Protocols when the system is awaiting connections requests in a queue and becomes unresponsive during the initialization of the connection. Teardrop aims the sequential IP packets by making them overlap, therefore confusing the system and causing it to crash. Smurf attacks use IP spoofing while ping of death focuses on IP packets as well. Botnets, on the other hand, are quite different as they involve millions of computers affected by malware, and the hacker can choose which to attack as he or she has control over all the systems.

## Malware Attacks

This is another type of cyber-attack consisting of unwanted software being installed into a computer system without the knowledge of the owner. In most cases, the software is established when an individual is online or has a connection where a hacker can gain access to their computers. More so, malware attacks come in different forms based on where it intends to damage. Most of them attach to original codes and propagate to simulate the application or the internet. Common types of malware attacks include macro viruses, file and system infectors, stealth and polymorphic viruses, logic bombs, Trojans, ransomware, worms, and droppers.

Viruses are the most common malware attack depending on how they are meant to infect a given system. Macro viruses are specifically intended to affect computer applications, for example, Microsoft Word and Excel, when initialized. Polymorphic viruses focus on encryptions and decryption,



especially when using a decryption program, while stealth viruses are responsible for compromising malware detection applications and conceal the scope of an infected file. File and system infectors comprise cyber-attacks that use a virus to infect specific areas within the computer, such as executable codes of files and records in the hard disk.

Trojans are programs that hide within essential system applications but accompany a malicious function. In this case, Trojans allows a hacker to open and gain access to the necessary files without interacting with securities installed. Worms are also a type of malware attack that is commonly transferred by email attachments and activated once the mail is opened. Droppers are another form of malware but used to spread and hide viruses making scanning processes difficult to identify malware. Ransomware is the most dangerous type of malware as it blocks the user from accessing information; therefore, it may be used as a threat to specific demands to be met.

## Eavesdropping Attacks

These are cyber-attacks which occur when an attacker intercepts network traffic and gain access to crucial data such as passwords and other confidential information transferred through the connection. Researchers have categorized eavesdropping into two, active, and passive eavesdropping. Passive eavesdropping entails an attacker monitoring and listening to the message being transferred and learning about it. Active eavesdropping involves a hacker physical disguising as a beneficial party to the user by requesting the message to the transmitter in a process refers to as probing or scanning. Passive eavesdropping is the most dangerous form as they often go unnoticed when compared to active eavesdropping. The best technique to use to avoid eavesdropping attacks is through data encryption.

## Cross-Site Scripting Attacks

In some cases, an attacker may use cross-site scripting to gain access to sensitive data through thirty party web resources. That is, the attacker first establishes the targeted information or system and introduces contents consisting of malicious JavaScript in the website database. This malicious program will remain in the database until when the victim opts to requests the webpage. The website will accompany the content with the page embedded

within the HTML body to the browser of the victim. When the page completes loading, the malicious script will execute, allowing the attacker to gain access to the computer.

In some instances, the hacker may choose to accompany other vulnerabilities that provide more loopholes to access different areas of your computer. The hacker will then be able to collect all the information needed, including controlling the machine. Cross-site scripting may take various forms, but JavaScript is the most supported and standard used on the web today. Cross-site scripting can, however, affect not only one victim, but also affect others who load similar websites. As to avoid this type of cyber-attack, ensure all the web information is first filtered and validated as well as preventing sending specific information to the resource. Besides, you can disable client-side scripting, making the user have control of the information shared through the web resources.

## Password Attacks

Passwords are the most common attacks experienced by victims as they are the sole mechanisms to authenticate the access of user data in specific areas. Acquiring someone's password is most preferably when peeking on their devices or ATMs or other peeks. However, this is not cyber-attacks, as hackers usually gain access to the computer and collect these passwords to open private accounts through computer connections. Like most cyberattacks, password attacks come in different forms and include decryption of passwords, gaining access to the database, outright guessing, and through social engineering.

One of the most common is brute-force password access, which is the guessing of different possible potential words or numbers used as passwords with the intention of one being correct. Another form is through a dictionary attack where a hacker tries to gain access to the connection and computer, and copy the encrypted file and compare it to the dictionary with a similar and possible password format. Some may go ahead and decrypt the password and gain access. One of the primary countermeasures to avoid password attacks is by introducing an account lockout policy that automatically locks after specific password attempts.

## Drive-By Attack

These are another common type of cyber-attack where an attacker can readily spread malware through insecure websites. That is, they quickly install malicious script in HTTP or PHP codes in one or more webpages targeting victims who visit these sites. Drive-by scripts may either install the malware into the victim's computer directly or redirect them to the websites of the hacker. In this case, the malware can download immediately the web is loaded or visiting a given website or pop-up pages. This type of cyber-attack does not rely on the user clicking anything or accepting any downloads. This will then enable an attacker to infect your computer without your consent.

When installed into your system, drive-by attacks may infect a program, the operating system as a whole, or browser with security issues. The primary solution for this type of cyber-attack is to keep your computer browser, operating system, and applications updated. You can as well stay away from websites that look suspicious or possess malicious codes essential for causing infections. However, understand that any website can be hacked and compromise the security of your computer. More so, remove any unnecessary or excess applications and programs as they make your device more vulnerable to threats. In other words, the more plugins you have, the more susceptible you are to drive-by cyber-attacks.

## Phishing Attacks

Phishing and spear-phishing is the process of sending emails to victims with the aim of gaining access to their personal information or persuade them to do something. The emails are often fake but seem genuine and accompany malware, which quickly loads into your system when you open the attachment. Some useful links to certain websites that lure you into following the instructions given and ending up submitting private data to attackers. The trickery used generally combines social engineering and related techniques to ensure the victim is well influenced to accept to the terms highlighted. Attackers usually have a deeper understanding of their victims, therefore, creating content which suits their personality and relevance.

Identifying these forms of cyberattacks is ordinarily tricky to victims, henceforth finding it hard to defend or resist from handing over crucial data, primarily when a hacker uses email spoofing. Others use website cloning, which commonly fools victims to believe that the emails are legitimate and from trusted sources. There are several ways to reduce and protect yourself from phishing attacks, and one of them is through the use of critical thinking

by taking the time to read through and understanding about the sender. Another form is by hovering on the link by deciphering the URL and understands it but never click at first. You can also analyze the headers by learning about the domain and by sandboxing to try and figure out the legitimacy of the mail.

## Man-In-The-Middle Attacks

Man-in-the-middle cyber-attacks occur when an attacker gets access between the connection of the victim and server. This type also comes in different forms, which are session hijacking, IP spoofing, and replays. IP spoofing is where the attacker convinces your computer that it is communicating with a genuine entity, therefore, allowing for the access. Similarly, the attacker sends packets with IP source resembling the host instead of the original IP source address making its accept it and act on it. A replay attack is when the attacker impersonates the victim by saving old messages and sending them sooner after the interception. Replays are, however, not valid to hackers as victims can readily prevent them through nonce and timestamps.

Session hijacking is where the attacker intervenes in a session of trusted clients and servers while the primary IP address is substituted, and the server continues with the session. The client first connects to the server, and when the hijacking happens, the attacker gains control by disconnecting the server the client. It then replaces the IP address and continues the sessions with the server as well as the client. With limited countermeasures to man-in-the-middles cyber-attacks, data encryption, and the use of digital certificates may play a significant role in preventing these threats. You should know it is always challenging to understand when an attacker is within a given service; therefore, crucial to forever remain protected against man-in-the-middle cyber-attacks.

## SQL Injection Attack

This is a driven-database website attack that occurs when an attacker runs a SQL query within a specific database through the data inputs of a client. The commands are injected in data-planes to execute predefined SQL instructions. When injected successfully, SQL queries access confidential and other sensitive information from the database enabling the attacker to perform the intended purpose. In this case, the data becomes open to the attacker who

then can read, change, execute operations, copy, recover and issue commands within the operating system.

For example, a website form may require a user's account name or password, which can be readily be pulled from the database. When such individuals use SQL injections successfully, it allows the information to be drawn from the database and delivered to the attacker at an instant as it already has the details from the victim. The vulnerabilities typically arise due to SQL lacking the ability to differentiate between controls and data planes, thus essential for dynamic SQL, PHP, and ASP. As to protect yourself from this type of cyber-attack, use the least privilege model, which facilitates permissions in your database. This model allows for stable codes that only validate input data of applications through stored procedures and prepared statements.

# How to Prevent Cyber Attacks

- **Limit Individuals Accessing Your System**

As already mentioned, among the primary causes of cyberattacks is public use of computer networks and the sharing of communication devices. This has been found to contribute to cyber threats and attacks commonly happening today. As to curb this, you can begin by limiting the number of people accessing your system, especially strangers and uninvited people. You can achieve this by securing your computers by updating software and the use of antiviruses as well as updating the operating system. You can again use company-approved programs and applications rather than purchasing from third parties. This method of prevention is quite useful, especially when you have doubts about people and sources, which tend to cause a threat to your files.

- **Learn About Cyber Attacks**

You can never begin protecting yourself from something you have no idea about how it works; therefore, the need to learn the basics. One of the best ways to do this is through learning about cyber-attacks and become aware of how they operate and harm computers. Having a general knowledge enables you to figure out ways of handling threats and the accompanying attacks when they happen as well as the mitigation measures. This will hence provide exceptional results, especially when you receive emails that you have no idea what they are and go ahead understanding instead of clicking every link you see. Search about facts and continually gain more knowledge with time as attackers also change their tactics over time.

- **Regulate System Infiltration**

Malware is common, and sometimes avoiding them may become a challenge; therefore, continually infect more computers globally. However, you can prevent this type of cyber-attack by readily regulating infiltrations by malware. As to achieve this, ensure any device inserted in your computer is free from any malware such as viruses. You can check it while offline to

avoid spreading it through your network. Also, ensure that no third party accesses your computer and enters unknown data as some may plant-specific instructions that allow them to control your system remotely.

- **Enhance Physical Protection**

Other than focusing on online, computer programs, and application security, you should also put in mind the protection of the physical computer itself. Begin by having a lengthy and robust password of not less than eight characters with a mixture of lower and upper letters as well as numbers and symbols. Use identity card authentications where the need is to ascertain your data, especially when providing security to confidential information. Keep all these securities protected at all times without having vulnerabilities that may compromise your cyber-attack security measures.

- **Ghettoize Networks**

Another primary source of computer cyber-attack is through the network, which connects different devices to the server. The host typically has limited threats to your system, but third parties, which are hackers, in this case, may use your connection as an entry point to access your data. Then you have to conceal these loopholes as they contribute to threats of cyber-attacks. One of the practices to do is to prevent other people's devices from accessing private networks by securing stations that facilitate file sharing. Another form is through becoming very cautious, especially on what you share online, as some information you share may be used against you. Besides, ensure that you avoid using public networks with devices that consist of critical and sensitive data as most hackers may take advantage and benefit from your mistake.

- **Constantly Update Your Securities**

Most often, the best way to prevent cyber-attacks is to ensure that your system is full of all applications, software, and programs that facilitate the needed protection. What many fail to understand is that cyber-attacks, especially for malware change over time, and if you fail to make an update,

your securities may fail to protect the system. In this case, the best way to handle these attracts is by ensuring that antiviruses, antispyware, firewalls, and software in the operating system are updated. Make these updates regularly to ensure you have the more recent version of your securities. You should be aware that hackers also understand this, and any delays in making updates may cost you. As such, ensure that you quickly make the updates as soon as they are available.



# Hacking with Kali Linux

---

*A Comprehensive Guide for Beginners  
to Learn Basic Hacking,  
Cybersecurity, Wireless Networks, and  
Penetration Testing*

---

By Dylan Mach



© Copyright 2019 by Dylan Mach - All rights reserved.

The content contained within this book may not be reproduced, duplicated or transmitted without direct written permission from the author or the publisher.

Under no circumstances will any blame or legal responsibility be held against the publisher, or author, for any damages, reparation, or monetary loss due to the information contained within this book. Either directly or indirectly.

**Legal Notice:**

This book is copyright protected. This book is only for personal use. You cannot amend, distribute, sell, use, quote or paraphrase any part, or the content within this book, without the consent of the author or publisher.

**Disclaimer Notice:**

Please note the information contained within this document is for educational and entertainment purposes only. All effort has been executed to present accurate, up to date, and reliable, complete information. No warranties of any kind are declared or implied. Readers acknowledge that the author is not engaging in the rendering of legal, financial, medical or professional advice. The content within this book has been derived from various sources. Please consult a licensed professional before attempting any techniques outlined in this book.

By reading this document, the reader agrees that under no circumstances is the author responsible for any losses, direct or indirect, which are incurred as a result of the use of the information contained within this document, including, but not limited to, — errors, omissions, or inaccuracies.

# Table of Contents

## **Introduction**

## **Chapter 1: Definition of Hacking and Types of Hackers**

Purpose of Hacking

Types of Hackers

Hackivist

Grey hat

Ethical Hacker

Cracker

Types of Hacking

DNS Spoofing

Cookie Theft

UI Redress

Virus

Phishing

How Do Hackers Get Access into Computer Systems

Guarding Against Hacking

## **Chapter 2: Cybersecurity**

Cyber Threat Scale

Advancement of Cybersecurity

Protecting the End-User

## **Chapter 3: Types of Cyber Attacks**

Birthday Attack

Eavesdropping Attack

XSS, Cross-Site Scripting Attack

SQL Injection Attack

Password Attack

Drive-By Attack

Phishing and Spear Phishing Attacks

MitM, Man-in-the-Middle Attack

Replay

IP Spoofing

Session Hijacking

DoS, Denial-of Service, and DDoS Distributed Denial-of-Service Attacks

Botnets

[Ping of Death Attack](#)

[Smurf Attack](#)

[Teardrop Attack](#)

[TCP SYN Flood Attack](#)

## **Chapter 4: Types of Malware**

[Spyware](#)

[Adware](#)

[Ransomware](#)

[Droppers](#)

[Worms](#)

[Logic Bombs](#)

[Trojans](#)

[Stealth Viruses](#)

[Polymorphic Viruses](#)

[System or Boot-Record Infections](#)

[File Infectors](#)

[Macro Viruses](#)

## **Chapter 5: How the Hacking Process Works**

[Preparation Phase](#)

## **Chapter 6: Why Hackers Use Linux**

[Why Hackers Prefer Linux Operating System](#)

[Easy to Use](#)

[Less RAM Consumption](#)

[Linux is the Future](#)

[No Requirement for Drivers](#)

[Serious Take on Privacy](#)

[Hacking Tools are Often Written for Linux](#)

[Several Programming Languages Have the Support of Linux](#)

[Less Vulnerable](#)

[Low Cost](#)

[Flexibility](#)

[Maintenance](#)

[Portable and Light](#)

[Command-Line Interface](#)

[Multitasking](#)

[Network Friendly](#)

[Stability](#)

## **Chapter 7: Kali Linux Installation and Updates**

[Kali Linux Installation](#)

[Requirements for Installation](#)

[The Installation Process](#)

[Updating Kali Linux](#)

## **Chapter 8: Installing Kali Linux on Virtual Machine**

## **Chapter 9: How to Organize Kali Linux**

[Overview of the Desktop](#)

[Apache Webserver](#)

[Screencasting](#)

[Places Menu](#)

[Workspaces](#)

[Auto-Minimizing Windows](#)

[Command-Line Tools](#)

[Application Menu](#)

[Favorites Bar](#)

## **Chapter 10: Scanning (nmap, massscan, hping3) and Managing Networks (Wireshark)**

[Effective Use of nmap](#)

[Enumerating a Huge Quantity of Hosts with Massscan](#)

[Massscan Features](#)

[Uses of Masscan](#)

[Hping3 as a Packet Generator and Network Scanning Tool](#)

[Some of the Usages of hping Network Scanning Tool](#)

[Securing and Monitoring Your Network with Wireshark](#)

[Wireshark Installation](#)

## **Chapter 11: Firewalls**

[Functions of Firewalls](#)

[The Definition of Personal Firewall](#)

[The Need for Personal Firewall](#)

[Using a Personal Firewall for Defense](#)

[Firewalls Types](#)

[SMLI, Stateful Multilayer Inspection Firewalls](#)

[NAT, Network Address Translation Firewalls](#)

[Proxy Firewalls](#)

[NGFW, Next-Generation Firewalls](#)

## **Chapter 12: Obtaining User Information: Maltego, Scraping,**

## **Shodan/Censys.io**

[Architecture of Maltego](#)

[Launching Maltego](#)

[Web Scraping with Python](#)

[Shodan and Censys](#)

## **Chapter 13: Kali Linux on Portable Devices Like Raspberry Pi**

[Step 1: Installation of Kali on the Raspberry Pi](#)

[Installation of Kali to Windows SD Card](#)

[Kali installation in OS X SD Card](#)

[Step 2: the Display Hook-Up](#)

[Step 3: Have Everything Plugged in and Launch](#)

[Step 4: Enable Wi-Fi as you Log in](#)

## **Chapter 14: MalDuino**

[Elite](#)

[Lite](#)

[The Hardware](#)

[The Setup](#)

[The Software](#)

[Protecting Yourself From MalDuino](#)

[Admin Rights Lockdown](#)

[Duckhunt](#)

[Physical Protection](#)

## **Chapter 15: Kismet**

[Watching the Activities of Wi-Fi User Using Kismet](#)

[What We Can Get From Wi-Fi](#)

[Essential Tools](#)

## **Chapter 16: Bypassing a Hidden SSH**

## **Chapter 17: Bypassing a Mac Address Authentication and Open Authentication**

## **Chapter 18: Hacking WPA and WPA2**

## **Chapter 19: Secure and Anonymous Using Tor, Proxy Chains, and VPN**

[What is Tor](#)

[Using Proxy Chains](#)

[VPNs](#)

## **Chapter 20: IP Spoofing**

## **Chapter 21: Penetration Testing with Metasploit**

## **Conclusion**

# Introduction

Congratulations on purchasing *Hacking with Kali Linux*, and thank you for doing so.

The following chapters will discuss all of the different parts that we need to know more about when it is time to work with the idea of hacking and working with Kali Linux in order to get this all done. There are a lot of different tools that we are able to utilize when it comes to hacking, but one of the very best operating systems that we are able to use to make this into a reality is the Kali Linux system. This guidebook is going to take some time to go through all of that and learn more about how we can make it all work.

The start of this guidebook is going to take a look at some of the basics of hacking, the reasons that we would want to spend some time looking at hacking and using it for our own networks, and a good look at the difference between ethical hackers, unethical hackers, and everyone in between.

From there, we are going to take a look at a bit about cybersecurity and cyber attacks. With our modern world and the fact that so many people are online and trying to share and look at information all of the time, it is no wonder that hackers are trying to find methods that will allow them to get onto the computers and networks out there to steal personal and financial information any time that they would like. That is why we are going to take some time to look at how we can keep our networks safe and secure with cybersecurity while also knowing which types of cyber attacks are the most likely.

Now it is time to take this a bit further and look more at how hacking is going to work. We are going to take a look at the hacking process in more details, while also looking at malware, and how that, and a few other types of attacks are going to be able to come into play to help us really see results.

Then it is time to move on to some of the things that we are able to do with the Kali Linux system. This is often considered one of the best coding operating systems to work with, and we are going to take the time to look at what it is about and how we are able to use it for our needs. In this part, we are going to look at the reasons that people like to work with Linux, how to set up Kali Linux, how to work with Kali in a Virtual Machine if this is the



best option for us, and even how to organize Kali Linux, so it is ready for some of the attacks that we want to do.

This is just the beginning of what we are able to do when it comes to hacking. Now that we have set the stage and we are all ready to go with some of this, it is time to take it a bit further and look at some of the neat things that we can use Kali Linux to help us out with. We are going to look at how to scan and manage our networks, the importance of firewalls, how to obtain user information when we want, the use of Kali Linux on some of the portable devices we want to use, and even how to work with MalDuino and Kismet.

This is not all, though. We are going to take a look at a few more of the steps that we are able to work with when it is time to hack a network of our choice and gather up the information that we would like. To finish out this guidebook, we are also going to spend some time looking at how we are able to bypass a hidden SSHS, how to hack onto the WPA and WPA2 wireless systems, how to use some of the different tools out there to make sure that you stay hidden and no one will be able to trace the attacks back to you, and how we are able to use Metasploit to help us complete our own penetration testing.

As we can see with this guidebook, there are a ton of different parts that need to come into play so that we can really complete the attack that we would like to work with. All of these are different methods that hackers, those who are brand new and those who have been in the game for some time, are able to do. When you are looking to protect your own network or the network for someone else, or you would like to hack onto another network, you will be happy that you have all of these tools ready to help you get this work done.

There are a lot of cool things that we are able to do when it is time to work with the process of hacking, and having this all prepared and ready to go can be one of the best methods you can choose to protect your own network. When you are ready to learn more about hacking and all of the tools and techniques that we are able to use when hacking along with the Kali Linux system, make sure to check out this guidebook to get started.

There are plenty of books on this subject on the market, thanks again for choosing this one! Every effort was made to ensure it is full of as much useful information as possible; please enjoy!

# Chapter 1: Definition of Hacking and Types of Hackers

The process of hacking involves getting unauthorized access into a computer system, or a group of computer systems. Hackers get access to systems by cracking codes or passwords. The technique hackers use to obtain code or password is cracking and a hacker is someone that undertakes the process of hacking. Hackers can hack an email account, a social media site, a website, an entire LAN network, or a group of systems. Ultimately, it is through password algorithms programs that the hackers obtain access to a password. For each of their daily needs, people and also businesses make use of laptops or computers. For a seamless flow of business applications and information, several organizations have WAN, wide area network, website or domain, or a computer network. As a result, there is a high-risk exposure of these networks to hackers as well as the outside world of hacking.

## Purpose of Hacking

Mostly, the objective of some hackers is to cause certain reputational or financial harm to an entity, group, or person through their malicious or criminal intent. They achieve this by spreading malicious or incorrect rumors that can cause the disruption of the business after they embezzle their funds or steal their confidential data. Companies can find themselves in some socially detrimental situations with this misleading information. Also, as punishable by law, hacking is a form of internet or cybercrime. However, government law agencies and specific accredited institutions engage in another side of hacking on a professional level. With this case, their intention is to prevent individuals from causing any harm or counter the wrong intentions of the hackers. Also, this type of hacking is done to protect and save the citizens and society at large.

## Types of Hackers

It is quite essential for us to differentiate between the objectives and roles of hackers by knowing their types to get the detail on the above-broached objectives.

## Hacktivist

Leaving contentious information on a website that they hack is the focus of these types of hackers. They do this to spread religious, social, and political messages. Also, other nations can be targeted by these hackers.

## Grey hat

These types of hackers have no intention of fraudulent when they access a system without any authorization. They are between the black and white hat hackers. The objective of these hackers is to show the stakeholders of the system parts of its weaknesses and vulnerabilities.

## Ethical Hacker

The objective of these types of hackers is to eliminate and identify suspected weaknesses. They assess systems by getting access as officially and recognized stamped hackers and they are known also as white hat. A few things they also do is to retrieve critical information needed for security purposes, crack codes of anti-social or illegal setups, and vulnerability assessment. They are paid, certified, and trained experts.

The ethical hackers are the only individuals who are allowed to do this kind of hacking legally. They know the same kinds of rules to follow as a black hat hacker and will use some of the same ideas along the way. But they have usually gained permission to go through and do some of these options, rather than trying to do it to gain their own personal advantage.

For the ethical hacker, the goal is to keep the system as safe and secure as possible along the way. They want to either protect their own network, or the network of someone else who knows what they are here. This will make it easier for them to get onto the network without doing so in an illegal manner.

These hackers are going to use a lot of the same methods for their attacks, as we see with some of the other types of hackers. This means that they are going to rely on penetration testing, mapping out attacks, and more. But they are going to do it as a way to help them figure out where the vulnerabilities in the system are rather than looking at ways that you can exploit them.

## Cracker

These are black hat. They secure entry into websites or computer networks

through an unauthorized manner and also with a mala fide intention. There is also an attachment of personal gain in their intention through privacy rights violations to benefit criminal organizations, stealing of funds from online bank accounts, stealing confidential organizational information, and so on. These days, these hackers engage in their activities in a shady manner and they belong to this category.

## Types of Hacking

The threats that websites have to deal with are some of the most frequent threats of hacking. Hackers engage in the process of making the contents of a website public or changed with the use of unauthorized access. The individuals or groups that are opposed to social or political organizations most times target their websites. Also, they hack national or governmental information website, and this is entirely common. Here are some of common the hacking methods they use on the websites:

### DNS Spoofing

Sometimes, users might forget about the cache data of a domain or website, and this method of hacking uses this cache data. Then, it points the data to another malicious website.

### Cookie Theft

Cookies contain login passwords, confidential information, and so on, and with the use of malicious codes, hackers will have access to the website to steal cookies. When a legitimate company uses these, it is going to help them provide you with a better service overall. But it does store a lot of extra information on you and your system, and if the hacker is able to steal these cookies, they will be able to use them in any manner that they would like. This could be dangerous and is a big reason that it is often best to turn off and disable the use of cookies in the first place.

### UI Redress

Hackers use this method by creating a fake user interface. Thus, users will be directed to another website altogether when they click with the intention of going to a specific site.

# Virus

When hackers get access to a specific website, they release a virus into the files of the website. Their objectives are to corrupt the resources or information on such a website. There are a lot of different types of viruses that we are able to meet up with, and they can be spread through email attachments, websites that have been compromised, and more.

These viruses can take over the computer, shutting down files, stealing information, and even spreading to some of the contacts that you have on your system to get the information that the hackers would like to have. This is why it is so important to go through and be careful about the kinds of websites that you open, and to make sure that you are not going to websites that could harm your computer.

# Phishing

They use this method to replicate the original website, and as such, the hackers will easily seize and misuse the unsuspecting user's information like credit card details, account password, and so many more.

Many times these are going to be sent through email. The email is going to appear as it comes from the legitimate source, such as your bank or another site that you spend some time on, asking for you to check out a message or change your username and password.

Because the hacker does a great job of hiding things and making it look official, it does not take that long for people to fall for it. Even the website is going to look legitimate so it is easy to click on the different items and enter the information. If someone does fall for this, the hacker is able to take all of that information and use it to actually get into the account of yours that they would like.

# How Do Hackers Get Access into Computer Systems

We can get information by working and communicating with others through the help of some good guys in the computer world that create networks. And then, for a variety of reasons, we have some not-so-good individuals that cause troubles by using their computers to worm their way into those networks. These set of individuals are hackers and part of the things they engage in include:

- Shut down a website by creating heavy traffic to it
- Obtain credit card information
- Get passwords
- Steal secrets

Whether by disrupting business as usual or stealing information for their gain, hackers are always at work. Every now and then, there will always be news about them, and at a point, you may likely be wondering about just exactly what hackers are doing. They are always getting in the system by stealing passwords. For them to crack the security of a network, the first step for them is to find out a password. As a result, to make your password hard to figure out by anyone, it is quite useful to change them regularly. For you to know what hackers do when people discuss them, here are some key terms that you may probably hear about them:

- **Trojan horse:** this technique appears to be a helpful program and users are tricked into clicking and opening it. But the computers of such users can get unexpected attacks which can be behind the scenes or unnoticed. Because these are going to sneak onto the computer through methods that are secret, such as being on a program that seems legitimate, it is hard to detect them. But when the Trojan horse gets into the system, it can open up back doors and other things to help the hacker get the information that they want.
- **Session hijacking:** this technique involves hackers inserting malicious data packets into an actual data transmission over the internet connection.
- **Script kiddie:** this is unsophisticated or young hackers who act like a real hacker while using hackers' tools. These individuals are not going to care that much about learning how to hack. They want to complete an attack, but they don't really care about the basics that go with it or the codes that they need to use. Instead, they are going to just take on some of the tools and programs that are already out there and will use these to help them out. They just want to complete the hack and get the information out of it, without having to worry about learning

any of the techniques along the way.

- **Root kit:** an intruder can disguise and expand his control over your system by using this set of tools.
- **Root access:** for any hacker to get complete control over a system, root access is the highest level of access. Root access is the most desired by serious hackers to a computer system.
- **Email worm:** hackers use a natural-looking email message to send a mini-program or virus-laden script to an unsuspecting victim.
- **Denial-of-service attack:** hackers use this method to flood a website with false traffic, thereby preventing the system of the victim or crippling it from handling its normal traffic. This one is going to turn down the server for a particular company and can make it hard for legitimate users to get onto the system at all. This allows the hacker to have a chance to leave a Trojan or a back door or something else on that network.
  - **Distributed Denial of Service:** This one is going to be a bit different because it is going to utilize more than one computer to do the attack. In the DoS, the hacker is just using one computer, and the firewall can usually see that IP address and will stop allowing the service from that address. With the DDoS, the hacker is using a lot of different computers to do the process which makes it harder for the firewall to stop the attack.
- **Buffer overflow:** hackers use this method by overrunning an application buffer to deliver malicious commands to a system.
- **Back door:** hackers get access to a computer system using this secret pathway. Trojan horses, viruses, and other types of malware are able to come in and utilize this option to help them get onto the system and come back and forth as many times as they would like. If you are trying to protect your own computer or another system, make sure that when you are all done, you fix it all up so there are no potential back doors for a hacker to get through.

# Guarding Against Hacking

A persistent threat that is continuously affecting the security of a nation and its citizens is hacking. At the level of the individual, when hackers wipe away the entire hard-earned financial savings of someone, it can result in untold financial losses. Also, it can lead to long-term repercussions and major financial losses through the theft of data at the organizational level. It is essential to block this vicious menace and safeguard it.

There are a lot of things that you are able to do to make sure that you can keep your own network safe against another hacker. Setting this up well, and being careful about how your own network is going to behave is going to be so important to keep the hackers out. Some of the different steps that you are able to take in order to guard against any hackers that would like to get on your network will include:

1. Be careful about the emails that you use. Many of the attacks that we are going to explore in this guidebook are going to be activated with the help of email. This isn't true all of the time. But if you are careful with some of the emails that you open, especially the attachments, then you can avoid a lot of these attacks from a hacker.
2. Pick out some strong passwords that are harder to guess or get through with a brute force attack. Pick out passwords that are long, use a combination of letters, numbers and symbols, and ones that are not going to be related back to you or easy to guess at all. Many hackers are going to start by trying to attack your passwords because this is a weak point in your security. You can fix this with the help of a strong password.
3. Do a penetration test to look for some of the vulnerabilities that are on the system. We will take a look at how to work with penetration testing later on, but this is a great way to figure out which places the hacker may try to use in order to get onto your network. Doing one for yourself will help to keep it protected.
4. Change passwords on a regular basis. When you change the password on a regular basis, it is a lot harder for the hacker to guess what it is or use some of the other methods of password



cracking to get through with the help of the password.

5. Do not share information about the network with anyone else. Any important and sensitive information about your network needs to be kept secret and hidden. The more people who know about your network, the more likely it is that the information will get out, and a hacker will be able to utilize this.
6. Consider encrypting the information that you send to others in your communications. This makes it hard for anyone who does not have the right key to read any of the information that you are sending, even if it does get intercepted.
7. Pick out a strong security protocol to protect your network. Make sure that you are not working with the WEP option because this one is often easier for a hacker to get through. While the WPA and WPA2 are still options that are vulnerable to an attack, they are a lot stronger and can keep you safer along the way.
8. Use anti-malware and anti-virus software. These will make it harder for any of the attacks that the hacker is trying to send your way to get through.
9. Make sure that you are updating your software and operating system as often as it is needed. These updates are going to help cut out some of the vulnerabilities that are found in the operating system you use, and other software, so doing the update will make it harder for a hacker to get onto your system.

As you can see, there are going to be a lot of options that you are able to work with when it is time to protect your computer compared to some of the hacks that are coming your way. Make sure to work with some of these options, and you will find that it is a lot harder for a hacker to get on your system and use it for their own advantage along the way.

# Chapter 2: Cybersecurity

The practice of defending data, networks, electronic systems, mobile devices, servers, and computers from malicious attacks is cybersecurity. Also, they refer to it as electronic information security or information technology security. Common categories can also fit into the terms as well as a variety of contexts, from mobile to business computing.

- The most unpredictable cybersecurity factor is end-user education. When people fail to follow healthy security practices, they can accidentally introduce a virus to an otherwise secure system. Thus, it is quite vital for the security of any organization to educate its employees not to plug in unidentified USB drives and to delete suspicious email attachments.
- For any causes of loss of data or operations, the manner with which an organization responds to a cybersecurity incident is the business continuity and disaster recovery. And for the organization to return to the same operating capacity as before the event, the processes that dictate how the organization restores its information and operation are the disaster recovery policies. While the organization is attempting to operate without specific resources, the organization has a plan that it falls back on, which is the business continuity.
- The decisions and procedures of protecting and handling data assets are operational security. This process encompasses the activities that determine where and how data may be shared or stored and the users' permissions while accessing a network.
- When data is in transit or in storage, the privacy and integrity of data are protected by the information security.
- For devices and software to be free of threats is the focus of the application security. Even though it is designed to protect data, a compromised application could provide access to the data. Before the deployment of a device or program, the design phase is the beginning of the successful security.
- Irrespective of if an attack may come from opportunistic

malware or targeted attackers, the practice of securing a computer network from intruders is the network security.

## Cyber Threat Scale

Every year, about \$19 billion is spent by the U.S. government on cybersecurity. However, the pace at which the cyber-attacks are evolving is quite fast. According to NIST, the National Institute of Standards and Technology, real-time monitoring of all electronic resources is recommended to aid in early detection and combat the proliferation of malicious code. Cybersecurity counter three-fold threats and they are:

1. To cause fear or panic, the intention of cyberterror is to undermine electronic systems
2. Most times, politically motivated information gathering is involved in cyber-attacks
3. For financial gain or to cause disruption, groups or single actors can target systems through cybercrime.

Ransomware, Trojans, spyware, worms, and viruses are some of the common techniques attackers utilize to control networks or computers. For surreptitious data collection, they make use of Trojans and spyware and to damage or self-replicate systems or files. They use worms or viruses. All the information of the user is encrypted by ransomware, who waits for an opportunity to do so, and for the user to get access to their encrypted information, there will be demands for payment. A legitimate-looking download can contain a malware payload and they use it and also unsolicited email attachment to spread malicious code.

Irrespective of size, all industries have their fair share of the cybersecurity. In recent years, government, finance, manufacturing, and healthcare are some of the industries that reported the most cyberattacks. Since these industries collect medical and financial data, several of these sectors are more appealing to cybercriminals. However, they can also target all businesses that use networks for customer attacks, corporate espionage, and customer data.

More than before, the world relies on technology. As such, there is a surge in digital data creation. Today, computers are used to store a great deal of that data by governments and businesses, and they transmit it across networks to

other computers. There is vulnerability in devices and their underlying systems that undermine the objectives and health of an organization when exploited. For any business, there can be a range of devastating consequences with a data breach. Through the loss of partner and consumer trust, a data breach can unravel the reputation of a company. A company can lose its competitive advantage through the loss of vital data such as intellectual property or source files. Also, because of non-compliance with data protection regulations, corporate revenue can be impacted through a data breach. About \$3.6 million is the average cost that a data breach can cost an affected organization. It is quite critical for organizations to implement and adopt a strong cybersecurity approach with high-profile data breaches making media headlines.

## Advancement of Cybersecurity

The focus of traditional cybersecurity is on the implementation of defensive measures around a defined perimeter. BYOD, Bring Your Own Device and remote workers are the recent enablement initiatives that have expended the attack surface, reduced the visibility into cyber activity, and dissolved the perimeter. Today, despite the record levels of security spending, there is a rapid increment in breaches. The focus is on human-centric cybersecurity for a global organization. It is a new approach that, instead of an exponential number of growing threats, places focus on changes in user behavior. Where data resides, human-centric cybersecurity extends security controls into all the systems and also offers insight into the manner with which an end-user interacts with data even when the organization is not in control exclusively. Ultimately, to reduce threat detection and investigation times as well as prioritize and surface the most serious threats, this approach is designed to identify behavioral anomalies.

## Protecting the End-User

So, what are the security measures provided by cybersecurity for systems and users? First, to encrypt files, emails, and other vital data, cybersecurity relies on cryptographic protocols. Not only does this technique guard against theft or loss, but it also protects information in transit. Also, the computer is scanned by the end-user security software for pieces of malicious code,

quarantines this code, and then deletes it from the system. For malicious code hidden in MBR, Master Boot Record with a specific design to wipe or encrypt data from the hard drive of computers, security programs can also remove them after it has detected them. There is also a focus on real-time malware detection by electronic security protocols. For some to monitor the behavior of a program and its code to defend against Trojans and viruses that change their shape with each execution, both metamorphic and polymorphic malware, they make use of behavioral analysis and heuristic. From the network of a user, security programs can confine potentially malicious programs to a virtual bubble to learn how to better detect new infections and analyze their behavior. And as experts of cybersecurity identify new ways to combat new threats, security programs continue to evolve new defenses.

# Chapter 3: Types of Cyber Attacks

With the use of several techniques to destroy, alter, or steal information or data systems, any targeted offensive action that focuses on personal, computer devices, infrastructures, or computer information systems is a cyberattack. Without further ado, here are some of the common cyberattacks today:

## Birthday Attack

The creation of the birthday attacks is developed against hash algorithms which people use to confirm the integrity of a digital signature, software, or a message. A fixed length MD, message digest, which is independent of the input message length, is produced by a processed hash function message. The message has the characteristics of this MD uniquely. The probability of finding two random messages is the reference for the birthday attack, which, when processed by a hash function, generates the same MD. The attacker can safely replace the message of the user with his if the attacker calculates a similar MD for the message as the user has. And even if they compare MDs, the receiver will not be able to detect the replacement.

## Eavesdropping Attack

Attackers intercept the network traffic for the eavesdropping attack to happen. For some confidential information that a user might be sending over the network such as credit card numbers and passwords, an attacker can obtain those data by eavesdropping. There are two types of eavesdropping attackers, and they are active and passive:

- Active eavesdropping: by sending queries to transmitters, the attackers will disguise themselves as friendly units as they actively grab the information. They call this process as tampering, scanning, or probing.
- Passive eavesdropping: when attackers listen to the message transmission in the network, they will detect the information.

Also, since by conducting passive eavesdropping before active attacks

require the attacker to gain knowledge of the friendly units, quite essential than spotting active ones is detecting passive eavesdropping attacks. To guard against eavesdropping, the best countermeasure is data encryption.

## XSS, Cross-Site Scripting Attack

For running scriptable applications or scripts in the web browser of the victim, it is the third-party web resources that the XSS attacks use. Essentially, the attacker will use malicious JavaScript by injecting a payload into the database of a website. Using the payload of the attacker as part of the HTML body, the website will transmit the page to the browser of the victim to execute the malicious script when the victim requests a page from the website. For example, the attacker can use the cookie from the server of the attacker after extracting it for session hijacking when it sends this cookie of the victim. When they use XSS to exploit more vulnerability, there can be the most dangerous consequences. Attackers can control and access the machine of the victim remotely, collect as they discover network information, capture screenshots, or log keystrokes in addition to stealing cookies through these vulnerabilities. Since there is a wide support for JavaScript on the web, it is the most widely abused while, within Flash, ActiveX, and VBScript, they can take advantage of XSS.

Data input can be sanitized by the developers when users in an HTTP request before reflecting it back to defend against XSS attacks. And before echoing back anything to the user, it is essential to see that all data is escaped, filtered, and validated, including the values of query parameters during searchers. Special characters like >, <, /, &, ?, spaces can be converted to their respective URL encoded equivalent of HTML. Users can have the option of disabling client-side scripts.

## SQL Injection Attack

For websites that are database-driven, one common issue is the SQL injection. The process happens when, from client to server, a malefactor executes a SQL query to the database through the input data. In order to run predefined SQL commands, it is possible to insert SQL commands into data-plane input, for example, instead of the password or login. From the database, sensitive data can be exploited by a successful SQL injection. Also, it can

issue commands to the operating system, recover the content of a given file, execute administration operations like shutdown on the database, and also modify (delete, update, or insert) database data. For example, the account of a user can be requested by a web form on a website and then to pull up the connected account information using dynamic SQL, send it to the database. The process can leave a hole for attackers even when this works for users who are properly entering their account number.

There is no specific distinction between the data and control planes with the vulnerability to this type of cybersecurity attack. Thus, if a site utilizes dynamic SQL, SQL injections can work mostly. Also, because of the prevalence of older functional interfaces, SQL injection is quite common with ASP and PHP applications. And due to the availability of the programmatic interface nature, the less likely easily exploited SQL injections are ASP.NET and J2EE. In your database, apply the least privilege model of permission to protect yourself from a SQL injection attacks. It is vital not to include any dynamic SQL as you adhere to the process and parameterized queries for the prepared statements. And to prevent injection attacks, you will require a strong database for the executed code. Also, at the application level, it is vital to validate input data against a white list.

## Password Attack

Obtaining passwords tend to be the effective and common attack approaches since to authenticate users to an information system, passwords are the most commonly used mechanism. Through outright guessing, gaining access to a password database, using social engineering, acquiring unencrypted passwords by sniffing the connection to the network, or looking around the desk of a person, attackers can get access to the password of a person. Then, they can use a systematic or random manner to execute the last approach.

- Using the **dictionary attack**, attack attempts to gain access to the network or computer of a user by using a dictionary of common passwords. Attackers may compare the results after applying similar encryption to a commonly used password dictionary as they copy an encrypted file that contains the passwords.
- Attackers may hope that one password will work after using a



random approach to guess different passwords. This process is called **Brute-force**. The process tends to be logical for attackers when they use hobbies, title, job, name, and similar terms of the person to guess passwords related to the person.

An account lockout policy that will lock your account after some invalid password attempts is all that is needed to protect yourself from brute-force and dictionary attacks.

## Drive-By Attack

The prevalent technique to spread malware is the drive-by download attacks. On one of the pages, attackers will have a malicious script planted into PHP or HTTP code. With this planted, the script could redirect the victim to a site controlled by the hackers or might install malware directly onto the visitor's computer. When viewing or visiting a pop-up window or an email message or when you are visiting a website, drive-by downloads can take place. You can be infected with a drive-by attack even if you don't open a malicious email attachment or click on a download button. For you to enable the attack, you may not necessarily have to do anything, which makes drive-by attack different from other kinds of cybersecurity attacks. Due to a lack of updates or unsuccessful updates, a drive-by download can take advantage of a web browser, operating system, or an app that contained security flaws.

You may be required to avoid websites that could contain malicious code and keep your operating systems or browsers up to date to guard yourself against drive-by attacks. Even though those websites are liable to hacking, try to stick to the sites you use normally. And always delete unnecessary apps or programs from your device. Drive-by attacks can exploit more vulnerability on your system when you have more plug-ins.

## Phishing and Spear Phishing Attacks

The purpose of a phishing attack is to influence users to do something or gain personal information by sending an email that seems to originate from trusted sources. This type of attack utilizes technical trickery and social engineering. Malware can be loaded into your computer through an attachment of an email. Also, you can be tricked into handing over your personal information

or downloading the malware through a link to an illegitimate website. A phishing activity that is quite targeted is spear phishing. A bit of research goes into the targets by the attacker, after which relevant and personal messages are created. Spear phishing appears to be quite hard to be identified and guarding against it can also be harder. Email spoofing is one of the simplest approaches hackers use to conduct a spear-phishing attack. They make the email seem like it is coming from a known person like your partner or management since they have falsified the information in the section “From” of the email. Also, website cloning is another method that scammers use to infuse credibility to their story. They will fool you to enter login credentials or personally identifiable information, PII.

Here are some methods you can engage in cutting down on the risk of phishing:

- **Sandboxing:** you can make use of a sandbox environment to test the content of the email, clicking the links inside the email, or logging activity from opening the attachment
- **Email header analysis:** how an email got to your address is the purpose of email headers. As is stated in the email, there must be similarity in the domain of the “Return-Path” and the “Reply-to” parameters.
- **Hovering over the links:** don’t attempt to click it when you move your mouse over the link. You will know where it will actually take you when you hover your mouse over the link, and to decipher the URL, you will need to apply critical thinking.
- **Critical thinking:** just because you have 200 other unread messages in your inbox or you are stressed or busy, you will take it that an email is the real deal. You will want to take a minute to analyze the email.
- 

## MitM, Man-in-the-Middle Attack

In the situation where a hacker plants itself between a server and the communications, a MitM attack is happening. Some of the man-in-the-middle attack types include:

## Replay

Attackers can impersonate one of the participants by intercepting and saving old messages and attempt to send them later; thereby, a replay attack is taking place. You can use a string that changes later or a random number to counter which nonce or session timestamps to easily counter it.

## IP Spoofing

IP spoofing happens when a system provides the attacker with access to it, thinking that it is communicating with a trusted, known entity. A target host gets a trusted, known host from the attacker who, instead of its own IP source address, sends a packet with such an IP source. It is possible for the target host to act upon it after accepting the packet.

## Session Hijacking

Between the network server and a trusted client, attackers can hijack a session in this type of MitM attack. While the belief of the server is that of a communication with the client as it continues the session, there will be a substitution of the IP address of the attacking computer for the trusted client. For example, the process of the attack can go thus:

1. There is a connection by the client to a server.
2. The client's control is gained by the computer of the attacker.
3. The computer of the attacker disconnects the client from the server.
4. The attacker uses their IP address to replace that of the IP address of the client, thereby, spoofing the sequence numbers of the client.
5. There is a continuous dialog by the computer of the attacker with the server, and the belief of the server is that the communication still continues with the client.

For the prevention of all MitM attacks at present, there is no configuration or single technology to do the magic. Overall, effective safeguards against MitM attacks are digital certification and encryption, with both assuring integrity and confidentiality of communications. However, that encryption

might not help with the way attackers will inject a man-in-the-middle attack. For example, the public key of a man named Greg may be intercepted by an attacker and as such, makes the substitution of that key as his key. Then, anyone could unknowingly use the substituted public key by the attacker, thinking they are sending an encrypted message to Greg. Therefore, the intended message for Greg can be read by the attacker and then uses the genuine Greg's encrypted key to send the message to Greg, and Greg will never notice that the message has been compromised. Also, before sending the message to Greg, the attacker can modify the message. Ultimately, because of the MitM attack, Greg will believe that his information is protected since he is using encryption.

Now, how do you distinguish between the ownership of the public key between the two of them? Solving such a problem like this instigates the development of hash functions and certificate authorities. The following technique can be utilized when someone wants to be sure that an attacker will not see a message they want to send to Greg and that the message will indeed come from that message without any modification from an attacker:

1. A symmetric key will be encrypted by the person after they have created it with their own public key.
2. Then, the person will forward the encrypted symmetric key to Greg.
3. After that, the person will digitally sign a hash function of the message that they have computed.
4. Then, with the use of the symmetric key, the person will encrypt the signed hash message and their message and then sends forward the whole thing to Greg.
5. Since only Greg has the private key to decrypt the encryption, Greg will be able to receive the symmetric key from the person.
6. Since he has the symmetric key, the only person that can decrypt the symmetric signed hash and encrypted message is Greg.
7. And because Greg can compare the received message's hash with digitally signed one and can compute the hash of the received message, Greg can confirm that the message has not been altered.
8. Since only the person can sign the hash for it to verify with the

person's public key, Greg can also prove to himself that the person was the sender.

## DoS, Denial-of Service, and DDoS Distributed Denial-of-Service Attacks

When the resources of a system cannot respond to service requests, it means a denial-of-service attack has overwhelmed such a system. Though, the attacker controls the malicious software that they have infected in a large number of other host machines, the attack of a DDoS is also on the resources of a system. Attackers don't gain direct benefit from denial-of-service, unlike attacks that they developed to increase or gain access. DoS attacks satisfy some of the attackers. However, there may be real enough benefits for attackers if the attacked resources belong to a business competitor. Also, for attackers to launch a new type of attack, they tend to result in DoS attacks to take a system offline. Here are some of the various kinds of DDoS and DoS attacks:

### Botnets

For hackers to implement DDoS attacks, they can infect millions of systems with malware using botnets. And to carry out the attacks against the target systems, they use these bots or zombie systems. Most times, these will overwhelm the processing capacity and bandwidth of the target system. And since the locations of the botnets are quite differing, it can be difficult to trace these DDoS attacks. The mitigation of botnets can arise through:

- Using black hole filtering. Before it enters a protected network, it drops undesirable traffic. The host of the Border Gateway Protocol is required to forward routing updates to ISP routers in the event of detecting a DDoS attack. At the next hop, null0 interface will receive all traffic heading to victim servers.
- To deny traffic from spoofed addresses, using RFC3704 filtering, which its correct source network can be traced for that traffic. For example, from bogon list addresses, packets will be dropped by RFC3704 filtering.

## Ping of Death Attack

Ping of death attacks makes use of an IP size over the maximum of 65,535 bytes to ping a target system using IP packets. The IP packet is fragmented by the attackers since IP packets of this size are not allowed. Then, other crashes can ensue as well as buffer overflow when the target system reassembles the packet. When you use a firewall, you can block the attack of the ping of death as the IP packets that have been fragmented will be checked for maximum size.

## Smurf Attack

Attackers saturate a target network with traffic with the ICMP as well as using IP spoofing with this attack. Attackers target the broadcast IP addresses with the use of ICMP echo requests. As such, the origin of these ICMP requests is from the address of a spoofed victim. For example, for the attackers to broadcast address 10.255.255.255, the attacker would spoof an ICMP echo request from 10.0.0.10 if the intended victim address is 10.0.0.10. All IPs in the range will get this request, and it would overwhelm the network since all the responses are going back to 10.0.0.10. Not only can this method generate a vast amount of network congestion, but it can also be automated as it can be repeatable. You may want to disable IP-directed broadcasts at the routers for you to protect your devices from this attack. Then, you will be able to protect the ICMP echo broadcast request at the network devices. Also, to keep them from responding to ICMP packets from broadcast addresses, another option is to configure the end systems.

## Teardrop Attack

Attackers use this method to offset fields in sequential Internet Protocol packets by causing the fragmentation and length to overlap one another on the attacked host. Though it will fail, during the process, there will be an attempt by the attacked system to reconstruct packets. Then, the system will crash eventually due to confusion. You may want to block ports 445 and 139 as you disable SMBv2 for you to protect against this DoS attack if you don't have patches.

## TCP SYN Flood Attack

It is during a TCP session initialization handshake when attackers exploit the use of the buffer space that they use this attack. The small in-process queue of the target system will be flooded with connection requests from the device of the attackers. However, when the target system replies to those requests, it doesn't respond. And while waiting for the response from the device of the attacker, the process will cause the target system to time out. Ultimately, when the connection queue fills up, it makes the system to become unusable or crash. For you to countermeasure a TCPSYN flood attacks, here are some preventions:

- On open connections, decrease the timeout, and increase the size of the connection queue
- For you to stop inbound SYN packets, place servers behind a firewall configured

# Chapter 4: Types of Malware

The unwanted software that someone installs in your system without your consent is the precise definition of malicious software. There can be a legitimate attachment of this software to propagate and code, meaning that, across the Internet, it can replicate itself or lurk useful applications. A few common malware types include:

## Spyware

They use spyware to collect user's browsing habits, their computer, as well as their information. And without your knowledge, spyware tracks everything you do, and a remote user gets those data. Also, spyware can have malicious programs from the Internet installed or downloaded. When you install another freeware application, spyware is usually a separate program that is installed unknowingly and its working is quite similar to adware.

## Adware

Companies use adware, a software application for marketing purposes. When any program is running, there will be a display of the advertising banners. While you browse any website, you can download adware automatically to your computer. On the screen of your computer, through a bar or pop-up, you can view it.

## Ransomware

This type of malware threatens to delete or publish the data of the victim after blocking them unless there will be payment of a ransom by the victim. The more advanced malware utilizes the cryptoviral extortion technique. Doing this will encrypt the files of the victim and without the decryption key, makes it almost impossible to recover. It can be quite hard for a knowledgeable individual to reverse the lock on the system with the use of some simple computer ransomware.

## Droppers

For the installation of viruses on computers, they make use of a program called a dropper. Virus-scanning software cannot detect a dropper since it is



not affected by malicious code in several instances. Also, for virus software that is resident on a compromised system, a dropper can connect to the internet and download updates.

## Worms

Worms propagate across computers and networks as self-contained programs, and since they have no attachment to a host file, they differ from viruses. They use email attachment to spread worms and it gets activated when you open the program. Apart from conducting malicious activities, the worm can also send a copy of itself to all contact of the email address of an infected computer. Then, there can be an event of denial-of-service attacks against nodes on the network when a worm spreads across the internet and overload email servers.

## Logic Bombs

Appended to an application is a type of malicious software, which is a logic bomb. A specific occurrence triggers it such as a specific time and date or a logical condition.

## Trojans

Usually, Trojans has a malicious function and are hidden in a useful program. Since Trojans do not replicate, this major trait separates it from viruses. Also, attackers can exploit a backdoor established by a Trojan to launch attacks on a system. For example, so hackers can perform an attack after using it to listen, they can program a Trojan to open a high-numbered port.

## Stealth Viruses

For stealth viruses to conceal themselves, they take over the functions of a system. The report of the software is that of uninfected since they have compromised the malware detection. They change the time and date of the last modification of the file and conceal any increase in the size of an infected file.

## Polymorphic Viruses

When the viruses vary cycles of decryption and encryption, they use this

process to conceal themselves. So, initially decrypted by a decryption program is a connected mutation engine and the encrypted virus. A code area will be thus be infected by the encrypted virus. Then, there will be a development of a new decryption routine by the mutation engine. Using an algorithm corresponding to the new decryption routine, a copy of the virus and the mutation engine will then be encrypted by the virus. The new code will then have an attachment of the encrypted package of virus and mutation engine. Thus, the process continues to repeat itself. It is quite tricky to detect such viruses. However, due to the several modifications of their source code, they have a high level of entropy. For quick detection, you can use Process Hacker.

## System or Boot-Record Infections

The hard disks will give a record of a boot-record by the virus attached to the master boot. So it can propagate to other computers and disks, it will look at the boot sector and load the virus into memory when you start the system.

## File Infectors

These types of viruses associate themselves with executable code like .exe files. As the code loads, the virus will be installed. And with the creation of a virus file with a similar name, which is an .exe extension, another version of a file infector will connect itself with a file. Thus, the virus code will execute when the file is opened.

## Macro Viruses

Those that get infected by these viruses are applications like Excel or Microsoft Word. Macro viruses attach to the initialization sequence of an application. Before it transfers control to the application, the virus executes instructions when the application is opened. In the computer system, there will be a replication of the virus before it attaches to other codes.

# Chapter 5: How the Hacking Process Works

System information leakage is the primary use of hacking before. There is now dark connotation connected to hack in the recent years, courtesy of some villain players. On the other hand, for them to be assured of their systems' weaknesses and strengths, hackers are employed by various corporations to do this. They earn a fat salary through a positive trust they build, and also, they are aware of the point that they need to stop. So, without further ado, let's make a deep dive into the art of hacking.

## Preparation Phase

A programming language is highly required here. Though you will see some essential guidelines, you must not restrict yourself to a specific language. Tolerance is quite needed in this stage because it might take time to learn programming language.

- It is compulsory to know assembly language. Though there are several variables of it, your processor understands only this language. Also, when you don't know assembly, exploiting a program may not be possible.
- You will also need to know bash scripting. The manipulation of Linux/Unix systems will be done with ease, including getting most of the job done for you through writing scripts.
- Since PHP is what most web applications use, you must try to learn PHP, and also, in this field, a reasonable choice for you is perl.
- You can also automate several tasks with powerful, high-level scripting languages like Ruby and Python.
- The languages they used in building Windows and Linux are C++ and C. most especially; it teaches how memory works and also assemble language.

Then, your target needs to be in the picture. This process is referred to as

enumeration, which is how you will gather vital information about your target. You will have fewer surprises when you know more about your target in advance.

Now, the process of hacking can begin. For your commands, put a \*nix terminal into use. For users of Windows, a \*nix will help in emulation through Cygwin. Nmap doesn't need Cygwin as it runs on Windows and uses WinPCap. However, because of the lack of raw sockets, Nmap doesn't work well on Windows systems. Also, because of their flexibility, BSD and Linux must be in your list of considerations. And there are several pre-installed tools with several Linux distributions. Alternatively, in the Windows Store, you can find a \*nix terminal on Windows 10 fall Creators Updates or later and courtesy of Windows Linux Subsystem, the Linux command-line can be emulated by Windows.

Now, the first step is to secure your system. For you to give enough protection to yourself, you need to quite understand all common techniques. You need an authorization from your target for you to attack as you begin with the fundamentals. You can do this by using virtual machines to set up your laboratory, ask for written permission from your target, or even attack your network. You will get in trouble if you attempt to attack a network because it is illegal, no matter its content.

The process of testing your target is the next stage. Will you be able to get to the remote system? Though it is what most operating systems use, the result of using the ping utility to be sure your target is alive may not be quite concrete. Paranoid administrators of systems can easily shut it off since it relies on the ICMP protocol. Then, you will need to define the OS. When you intend to run a port scan, try nmap or pOf. So you can make your plan of action; running a scan of the ports will tell you the kind of router or firewall your target is using and you will see the ports that are open on the OS and the machine. Then, you can use the -O switch to activate OS detection in nmap.

By now, you would have discovered an open port or a path in the system. Most times, there is a strong protection for certain ports like HTTP (80) and FTP (20).

- The evidence of a secure shell, SSH, service running on the target is an open port 22, and this can be brute force sometimes.
- It is possible your target could have forgotten other UDP and TCP ports, including several UDP ports left open for LAN

gaming and also Telnet.

The next process is the authentication after you must have cracked the password. Brute force is among several techniques you can use to crack a password. You can try every potential password that a predefined dictionary of brute force software contains.

- Most times, finding your way into a system tends to be much easier even without cracking the password
- For you to upload it to the secure site, you can go for a TCP scan installation or acquire a rooted tablet. Then, you will cause the password to appear on your proxy when the IP address opens
- It may not be a good idea to attempt a login to a remote machine using every possible password. While it may take some time to complete, it could pollute the system logs, and intrusion detection systems can detect it easily
- For you to crack password quickly, you may result in using Rainbow Tables. You need to understand that it is only if the hash of the password is in your possession can the password cracking be a good method
- As it is thousands of times faster, another processor is the newer techniques that use the graphics card
- You can get a massive speed boost by cutting the MD5 algorithms and also exploiting the weaknesses of most hashing algorithms can significantly improve the speed of the cracking since they are generally weak
- Brute force can take a lot of time since users are using strong passwords. However, brute force techniques have improved with several major improvements

The privilege of a super-user is what you need to get now. If it is a Windows system you are trying to crack, you will need administrator privileges, and if your target is a \*nix machine, the root privileges are all you need.

- You may not be able to access all the features of a connection that you gain access into. However, you can do everything if

you have the root, administrator, or super-user account

- Except it has been altered, the admin account comes by default for routers, and it is administrator account for Windows
- You may require a specific level of authentication for you to get the most information because they have all been protected. You will require super-user privileges to see all the files on a computer. In BSD and Linux OS, root users get similar privileges as a user account

Now, you may want to engage in some different tricks. Most times, you may want to bump up your authorization level by causing the memory to dump so you can inject code or perform a task at a higher level by creating a buffer overflow to gain super-user status.

- You can do this by finding or writing an insecure program that you can execute on their machine
- If the bugged software has setuid bit set, this will happen in Unix-like systems, and as such, it is as a super-user that the program will be executed

You may want to have a backdoor developed at this stage. It tends to be ideal that you can come back again when you have gained complete access to a system. You can backdoor certain essential system services like the SSH server. Though, during the next upgrade of the system, your backdoor may be removed. Then, the solution is to backdoor also the compiler itself so you have a possible way of coming back through every compiled software. And your tracks must be covered. It is quite critical that the system administrator knows nothing about the compromise of the system. Never have more than necessary files created or make a change to the website. Also, you don't need to create more users. Make fast actions. Ensure that your secret password is hard-coded anytime you patch a server like SSHD. Though without containing any crucial information, the server must let them in if anyone attempts to login with this password.

# Chapter 6: Why Hackers Use Linux

There are several special features on the Linux operating system that make it more dominating than any other OS. With Unix as its old version, the operating system of Linux is an open source. Day by day, there is a rapid development in the use of Linux. And rather than using any other operating systems such as Mac or Windows, hackers like to use Linux because of the additional benefits Linux operating system has over others. The operating system of Linux has remarkable special features that make it more dominating than other systems even though their operating systems are more user-friendly.

## Why Hackers Prefer Linux Operating System

For the challenge of it, and because they want to make money from their natural hacking capacities, hackers break into the networks of computers or standalone personal computer systems. And to test their skills, hackers will need the operating system, which offers maximum security. Thus, Linux appears to be the best choice for hackers since it makes it more secure for them in all of their activities. For libraries and Linux applications, they have written millions of lines of code today. This process has allowed it to be integrated into broadly diverse projects as it is done in an extremely modular manner. For example, you can have a part of a library used as a network hijacking code, even with it allowing you to sniff the network for proactive performance monitoring. Also, network security can be hacked with ease.

As it is flexible, hackers have the opportunity of playing their entire fashionable activities using the playground of Linux. Also, it is quite simple for hackers to understand, learn, and use Linux since they can use their penetrating testing methods to know if there is insecurity. Linux is quite secure since when problems arise, hackers can patch it because they have the ability to look at each and every line of Linux code. It can also be used at any time by any user working on it and not only some programmers working in some corporate organizations. Here are some of the benefits of Linux over others:

### Easy to Use

The general belief is that Linux is only for hackers and programmers, and that tends to be the widespread myth. However, this analog is far from being the truth. You will easily have a basic understanding of Linux if you have been using it for some time. It is not the same as the operating system of Windows. As such, it could be quite tricky when we make the switch to a different operating system. You will find Linux to be user-friendly and more convenient than Windows.

## Less RAM Consumption

Linux consumes lesser processing utility and RAM as well as requires lesser space for disk since it is quite light. Thus, you can have other operating systems such as Windows and OS X installed with it.

## Linux is the Future

First, Android is based on Linux and also, the choice for web servers is the Linux operating system for its robustness, flexibility, and stability.

## No Requirement for Drivers

You don't need separate drivers before you can use Linux. Within the Linux kernel, you will find all the necessary drivers you will need when you install Linux. As a result, to install drivers for hardware, you won't need CDs anymore.

## Serious Take on Privacy

All over the Internet, many people are talking about Windows 10 and the issue of privacy. Usually, your data is collected by Windows 10. However, there is no case of anyone collecting information and data about you for monetary gain when you use Linux operating system.

## Hacking Tools are Often Written for Linux

Nmap and Metasploit, some of the popular hacking tools are ported for Windows. However, Linux has some better tools and in a much better way, manages memory, and not all capabilities are transferred from Linux.

## Several Programming Languages Have the Support of



# Linux

Most programming languages have abundant support from Linux. On Linux, working perfectly are Perl, Python, Ruby, PHP, Java, and C++/C. It is effective and simple when you want to use Linux for any of the scripting languages.

## Less Vulnerable

There is so much vulnerability in virtually all the operating systems available except Linux. Linux has fewer vulnerabilities, and it prides itself as the most secure operating system.

## Low Cost

It is widely known that Linux is an open-source operating system and so, you can get it online for free as well as freely install and use all the applications without any payment.

## Flexibility

You can use Linux for high-performance desktop and server applications, as well as embedded systems.

## Maintenance

It is quite easy to maintain the operating system of Linux. You can install all the software with ease. It is even easier to search for their software since every variant of Linux has its central software repository.

## Portable and Light

From nearly any Linux distribution that they want, the customized live boot drives and disks are there for hackers to develop. Since the resources it consumes are quite fewer, it is quick to install. The fact that it consumes fewer resources makes Linux light-weight.

## Command-Line Interface

Windows and Mac don't have the specially designed, highly-integrated, and

strong command-line interface which Linux boasts of having. Other Linux users and hackers will have control over their system with greater access.

## Multitasking

All at the same time, you can make use of Linux, as that is how it is designed. For example, your other works will not experience any form of slowdown with a large printing job in the background. Also, your primary processes will not be disturbed even with several works done at the same time.

## Network Friendly

Linux is effective in managing network over it since it offers several commands and libraries that hackers use to test network penetrations. Hence, as an open-source operating system, the team that contributes to it does so over the internet network. Also, more than any other operating system, Linux makes network backup faster as a reliable operating system.

## Stability

When you want to maintain performance levels, the only OS that doesn't require any periodic rebooting is Linux. Also, the cause of memory leaks cannot slow it down or make it freeze up too. For many years, you can continue to use this operating system.

Since hackers can increase their hacking capabilities and also test their skills on this operating system, it makes Linux as their best choice. The setup programs and installation is user-friendly, and several Linux distributions have tools that make installation of more software quite user-friendly.

# Chapter 7: Kali Linux Installation and Updates

A security-focused operating system is one of the most essential things to have when you are looking for a career in information security. You can efficiently perform tedious and time-consuming tasks with the help of a suitable operating system. At present, the operating systems of Linux are indeed countless. However, one of the best choices is Kali Linux. cybersecurity professionals use it for assessing network security, ethical hacking, and penetration testing.

Kali Linux will be one of the first names to be mentioned when it comes to offensive Linux distributions, hacking, and penetration testing. There are several information security tasks as various command-line hacking tools that Linux comes pre-packaged like application security, computer forensics, network security, and penetration testing. Fundamentally, when you attempt to engage in ethical hacking, the operating system of Linux is an ultimate solution.

## Kali Linux Installation

The process of installing Kali Linux can be quite simple, and the options of installation are numerous. The techniques most people prefer are:

1. Using the operating system to dual boot Kali Linux
2. With virtualization software like VirtualBox or VMware
3. Installation of hard disk for Kali Linux
4. Making a Kali Linux bootable USB drive while installing Kali Linux

The focus will be on using virtualization software to install Kali Linux even while there are several options available. For you to perform a comprehensive penetration test using all the tools you need, you can set up your machine by following these steps.

## Requirements for Installation

- USB support / DVD-CD drive
- While working with VirtualBox or VMware, the recommendation is around 4 GB
- The recommendation for your hard drive is a minimum free space of 20 GB

## The Installation Process

### **Step 1: VMware installation:**

First, a kind of virtualization software is essential to run Kali Linux. For many people, there is a preference for VMware even when they can use VirtualBox by Oracle as part of several options that they can choose from. From your applications folder, launch VMware when you have finished with the installation.

### **Step 2: Kali Linux download and image integrity checking:**

You can choose the one that best suits your needs when you go to the official download page to download Kali Linux. Also, there are some hexadecimal numbers on the download page. There is nothing so important about them. Also, for the tasks that are related to security is the intention of Kali Linux. As such, the integrity checking of your downloaded image is highly required. The file's SHA-256 fingerprint needs to be checked and make a comparison with the one you see on the site you make the download.

### **Step 3: a new virtual machine launch:**

You will hit the 'create a new virtual machine' button when you get to the homepage of the VMware Workstation Pro. Before you configure the details of virtual machine, you must have chosen the guest operating system after selecting the iso file of Kali Linux. Choose the Kali Linux VM to start the virtual machine, and you will click on the green button with 'power on' inscription. You will see the machine starting up!

### **The process of installation**

In the GRUB menu, you will get the prompt to choose your preferred mode of installation when the machine is powered up. Before you continue, choose the graphical installation. You will be taken to another page where you will be prompted to choose your layout for the keyboard, the location of your country, and the language you prefer. Then, the loader will have the related

settings of your network configured after installing extra components when you are through with the local information. Then, for this installation, a domain and hostname will be prompted by the installer. Before you continue with the installation, you will have to provide the appropriate information for the environment. You will press continue when you have set a password for the Kali Linux machine. An important note here: make sure you keep your password carefully! Then, set your time zone will be prompted by the installer after you must have set your password. At the partitioning of the disk, it will pause. From the disk partition, four choices will be provided to you by the installer. The ‘guided – use entire disk’ option is the easiest of them all. For additional granular configuration options, the method of ‘manual’ partitioning can only be used by experienced users. If you are a new user, the recommendation is to choose all files when you are choosing the partitioning disk and you can click on ‘continue.’ Then, on the host machine, the entire changes you want to make can then be confirmed. You must be careful here since you can have the data on the disk erased if you continue. So, the process of file installation will be run through by the installer when you confirm the changes in the partition. As this process can take some minutes, the installation will be done automatically. If you prefer to obtain future pieces of updates and software, the setup for a network mirror will be inquired by the system when the necessary files are installed. If you want to use the repositories of Kali, make sure you have this functionality enabled. Then, the related files of the package manager will be configured. Next, the boot loader of GRUB is the next thing you will be asked to install. Choose ‘yes,’ and since it will be required to boot Kali, you will choose the device to write the important information for boot loader to the hard drive. To finish the installation, hit the ‘continue’ button when the installation of GRUB to the disk has finished. Then, specific files for the final stage will be installed. By now, brace up yourself because your journey of exploring Kali Linux has just begun since you have successfully installed Kali.

## Updating Kali Linux

The packages index list is the first step of an update for your Kali Linux system. You will enter the following command when you open the terminal;

```
$ sudo apt update
```

As an option, for all scheduled packages for update, you can display them.

You have the opportunity of upgrading all packages at once with the use of `apt install PACKAGE-NAME` as well as individual package upgrade at this stage. Now, you have completely upgraded your Kali Linux.

# Chapter 8: Installing Kali Linux on Virtual Machine

In similar hardware that you currently have, you can run different operating systems in a number of ways. And some of the options available for you are hard disks, USBs, and DVDs. In this chapter, the assumption is that for you to run your Kali Linux, you have no dedicated computer and as such, we are going to use a virtual PC or a virtualized environment to run it. You must have had virtual box installed on your computer for us to begin the process. And in case you don't have it on your system, it is free to download when you go to the official website of VirtualBox. For the hardware that we will be using to install Kali Linux, this software will be emulating this hardware.

It is widely known that unless you have access to software, it can be quite tricky to download such software. Thus, you will download Kali Linux ISO image from its official page. And in case you want to follow along as you mirror that, the flavor of the Kali Linux KDE 64-bit is what we will be using. The size of its download is around 3.2 GB, and for you to download, it might take a while. You will then have the .ISO image mounted into the virtual machine when you have dealt with that one. If you have the intention of using it in another machine, you can have it burned into a USB or bootable DVD. However, you may need to take into account certain considerations. Then, you may open VirtualBox when the image is downloaded.

Now, you will hit on the 'new' button for you to create a new virtual machine, which is the first thing you will do. Then, in the natural operational system, you will have to specify the existence of this machine's files of the service files. You can select Linux for type because it is on top Linux that Kali is built. And for version, Ubuntu 64-bit will be your choice. Though to get Kali up and running on VirtualBox, it is an ideal default setting for us. There is no guarantee it will work perfectly by specifying version and type. Then, the prompt for the amount of memory we want will be the next. You can go for 2GB as even 1GB will still work. Alternatively, you can go ahead and give it as much as you want if you have enough memory.

The hard drive setup is the next step here, which the VirtualBox will ask you. You may choose to use an existing one or create one. So as not to go back and forth between several emulators, you can select VirtualBox Disk Image after selecting the hard drive file type. If you are using VMware, for instance,

a more suitable option will be VHD. After that, your storage allocation on the physical hard drive is the next option to choose. Then, you can select dynamic allocation. Next, the amount of allocation for this machine is what you will now choose. You must consider checking how much memory you have available before you go ahead with this action. The place you want to keep your virtual disks can be specified inside VirtualBox. You may then go ahead and hit the 'create' button. But, that is not the end of the process. For us to be sure we can understand them, we may want to play around the main settings. For future reference, you will have the freedom of tackling the virtual environment and this is quite essential. You may want to read more on the topic of virtual machine settings because it is an extensive topic.

You can as well move on to the system settings since, during the creation process, you have covered some items. If you don't have a floppy drive, you can remove floppy under the system. You can prompt VirtualBox to check for any media in the DVD player first in the boot order. It is useful to know that in the initial install, that is the base for our Kali image. If it is necessary, you may want to check that later also, but you can have 2MB for the base memory. As per the above image, ensure that you mirror the extended features. Then, you can boost the memory of the image up to around 128 MB when you move on to 'Display.' Also, in case you want to get naughty with specific graphics, you can have the 3D acceleration enabled. You may run the risk of burning some circuitry and do not give it excessive video memory of you are running on old hardware. After that, you can do one of the most vital settings, which is to check the storage. Ensure that the image file you have downloaded from the official page of Kali Linux is pointing to the empty CD-ROM drive. Also, for you to be given the options to choose your .ISO file, you can achieve that by clicking on the disc icon under attributes.

Now, it is believed that you have mounted the CD-ROM image since the drive represents the .ISO image. You can leave the live DVD/CD checkbox as default and not tick it. You will have to pay attention to the main configuration by checking the settings for the network. Some of them are:

- Generic networking
- Host-only networking
- Internal networking
- Bridged networking
- NAT networking



- Network Address Translation, NAT
- Not attached

You can go to the official page of VirtualBox for you to know more about each mode. And provided your internet connection is wired, this default mode could be enough if all you want to do is to view email inside the guest, download files, and browse the web. As it is for the beginners, you can, for now, use NAT. When you launch the machine, everything should be working well if you are connected via an Ethernet cable. Without an interface card, it may not be possible for you to reach the web in case you don't have a wired connection. Then, you only have to hit on the 'start' to launch the operating system if you intend running Kali in a virtual environment.

# Chapter 9: How to Organize Kali Linux

Kali 2.0 was launched by Offensive Security after ten years of evolution. And of all the Kali/Backtrack releases, the easiest to use by far is Kali 2.0. There are some new features with the new Kali if you are used to the original Kali. However, there's nothing better than this! They have streamlined and reorganized the menus completely with a helpful icon representing many of the tools. Here are some new things about Kali 2.0:

- Built-in screencasting
- Desktop notifications
- For faster Metasploit loading, there is a native Ruby 2.0
- New categories and menus
- New user interface

They have streamlined the Kali 2.0 quite well, and compared to earlier versions of Backtrack/Kali; the layout flows quite well. As it is laid out in a concise and clear manner, the feel is that of having everything at your fingertips. To organize your Kali, you can follow the following ways as we examine some of its components.

## Overview of the Desktop

Again, everything you will need is at your fingertips on the desktop, which feels and looks quite good.

## Apache Webserver

At present, it seems they have removed the Apache web server for restart, start, and stop service icons from Kali 2.0. Well, you may want to use the command below if you want to start them from a terminal prompt:

- To restart – you can use “`/etc/init.d/apache2 restart`” or “`service apache2 restart`”

- To stop – you can use “ /etc/init.d/apache2 stop ” or “service apache2 stop”
- To start – you can use “ /etc/init.d/apache2 start ” or “service apache2 start”

You will notice the change from Kali 1 concerning the default webpage as you can now surf the webserver of Kali. Now, located in a folder called HTTP, there is one level deeper for the root website as well. As such, instead of the old directory “/var/www/,” you can now drop the folders or pages of your website into the directory “/var/www/html/” when you use the Apache server.

## Screencasting

You can now use screencasting because there is a built-in screencasting feature in Kali 2.0. You have the ability to record in real-time the adventures of your security testing.

## Places Menu

Within your Kali, you have links to various locations contained in the Places menu.

## Workspaces

There are also workspaces in the earlier versions of Backtrack/Linux. Workspace is the additional desktop screens that you can use in case you don't know the workspace. For all the windows that you have opened, you can get an overview of them using the 'super key.' Also, you can open the workspace menu if you have a touch-screen monitor. Between the workspaces, you will have the ability of dragging and dropping specific running programs.

## Auto-Minimizing Windows

At times, some windows disappear or auto-minimize, which is another thing

in the new Kali 2.0. On the favorite bar, to the left of the associated icon, you will see a white circle when a window is minimized. The first terminal window will appear if you click on the terminal icon once, and both minimized terminal windows will reappear when you click it twice. Also, to see minimized windows, you can press “Alt-tab.” Then, to see additional windows, you can arrow around when you have the “alt-tab” pressed.

## Command-Line Tools

It is in the directory “/usr/share” that they have the majority of tools installed. When you type the names of these tools in a terminal, you can run these tools and also other tools in the menu. For you to familiarize yourself with both the share directory and the menu system, you may want to take a few moments on that.

## Application Menu

Under the Application menu, you will see the location of a list of common program favorites. And by type, there is a logical layout of the tools. For example, if you want to see the most common web app testing tools, all you have to do is click on the Web Application Analysis menu item. You will see a list of all of the tools for a specific category. It is due to the fact the top tools are shown by the menu system, and in Kali, not all of the tools are available. Essentially, available in the menu system of Kali are only a fraction of the installed tools and it is only from the command-line that most of the tools can be available.

## Favorites Bar

On the desktop’s left side, you will see a customizable “Favorite bar” in the new Kali. With this, you can get into the action quickly since you can get the applications you use most time with this menu list. Through the required dependencies, you can start the represented tool automatically with just a click. For example, before you launch Metasploit, if you want to be sure you have created the default database, you can prestart the database software by clicking on the button for Metasploit. Then, you can see various applications on the bottom of the favorites bar by clicking on the “show applications.” In

folders, you can arrange the programs by type. You can also use the search bar by typing what you want if you don't see the app you are looking for.

# Chapter 10: Scanning (nmap, massscan, hping3) and Managing Networks (Wireshark)

During the course of penetration testing, a very essential host detector and network scanning tool are network mapped, nmap. Mainly, they use nmap as a security scanner and vulnerability detector which makes it a powerful utility as well as using it to enumerate and gather information. Since it can run on several different operating systems such as Mac, BSD, Linux, and Windows, this makes nmap a multipurpose tool. They use nmap for several powerful purposes including:

- Securing holes and detecting the vulnerability, such as nmap scripts
- Operating system detection, software version, and hardware address
- It works for service discovery, that is, detecting the version and software to the respective port
- Port enumeration and discovery; detecting ports that are open on the host
- Host discovery; detecting the live host on the network

As a common tool, nmap is available for both the graphical user interface and command-line interface. And to perform scanning, nmap utilizes several methods, some of which are FTP bounce scanning, TCP reverse ident scanning, TCP connect() scanning, and many more.

## Effective Use of nmap

Since we have a difference between an advance scanning and basic, simple scanning, the target machine has a huge dependence on the usage of nmap. For us to get the right outcome by bypassing the intrusion preventive/detection software and firewall, there is a need to make use of advanced techniques. You will see some examples below of a few basic

commands their usage:

On the target system, if you intend to scan a specific port, such as scanning only on the target computer Telnet, FTP, and HTTP, then you will need relevant parameter to use the nmap command. Also, you may as well call the file in the exclude parameter if the lists of IP addresses that you intend to exclude are contained in a file that you have. Another scenario is that since it tends to be dangerous for you, you may want to exclude specific IP addresses if you want to scan the entire subnet. As such, use the excluding parameter when you use the nmap command. You will need to add an `-sL` parameter to the command if you intend to see the entire list of the hosts that you are scanning.

## Enumerating a Huge Quantity of Hosts with Massscan

For a while now, massscan has been around, and all around the world, pentesters are making use of it. In a second, masscan can transmit up to 10 million packets as a reconnaissance tool. Massscan utilizes a custom IP/TCP stack and asynchronous transmission with different reception and transmission of packets using different threads.

You can quickly enumerate a vast amount of hosts using massscan. Essentially, massscan can scan the whole internet as quickly as 6 minutes, according to the author of the tool. And because of the high rate of its transmission, they also use massscan for stress testing. For anyone to accomplish those high rates, they will need special drivers like NICs and PF\_RING. Since it interacts with the use of similar style of nmap, this part makes it a convenient tool.

## Massscan Features

- Custom IP/TCP stack
- Basic vulnerability scanning such as heartbleed
- Banner grabbing
- Nmap style target option and specification
- Nmap style output
- Ultrafast port scanning: up to 10M packets per second in transmission (requiring PF\_RING drivers and capable – NIC)

## Uses of Masscan

- Random scanning for knowledge or fun
- Internet enumeration
- Enumeration of several subnets within an organization
- Enumeration of a large number of hosts
- For the mapping of the network, massscan can be used as the first recon tool

## Hping3 as a Packet Generator and Network Scanning Tool

As a free analyzer and packet generator for the IP/TCP protocol for the Antirez distribution, hping is a network scanning tool. For network security, hping3 is one kind of a tester, and for security testing and auditing of networks and firewalls, it is one of the de facto tools. They also use it for the exploitation of the idle scan scanning method, which now has its implementation in the nmap security scanner. As an analyzer/assembler for IP/TCP packet, a command-line oriented is the network scanning tool hping. Even when hping can do more than sending ICMP echo requests, the ping(8) Unix command inspired the interface. Its features include the ability to send files between a covered channel, possession of a traceroute mode, and support for RAW-IP, ICMP, UDP, and TCP protocols. In the past, they only used hping as a network scanning tool. However, some people use it in several manners to test hosts and networks.

## Some of the Usages of hping Network Scanning Tool

- Network scanning tool
- Using Tk interface, it is simple to use networking utilities
- Prototype IDS systems
- Security and networking research in the event of emulating complicated IP/TCP behaviour
- Concept exploits proof
- Automated firewalling tests
- Write real applications related to IP/TCP security and testing



- Learn IP/TCP
- Networking research
- Exploitation of identified vulnerabilities of IP/TCP stacks
- Test IDSes
- Test firewalling rules
- Perform the idle scan (with an easy user interface for implementation in nmap)
- Using the standard utilities network scanning tool to probe/ping/traceroute hosts behind a firewall that blocks attempts
- Students learning IP/TCP can also get adequate knowledge through hping
- Auditing IP/TCP stacks
- Remote uptime guessing
- Remote OS fingerprinting
- Advanced traceroute, under all the supported protocols
- Manual path MTU discovery
- Using fragmentation, TOS, and different protocols for network testing
- Advanced port scanning
- Firewall testing

## Securing and Monitoring Your Network with Wireshark

The toolkit for a network security analyst is one of the most powerful tools known as wireshark that people also referred to before as Ethereal. Through a variety of levels, from bits comprising a single packet to information on connection, wireshark can examine the details of traffic as it peers inside the network as a network packet analyzer. Wireshark can troubleshoot security issues in the network of a device and also analyze security events through its depth and flexibility inspection. Since it is free, the price of wireshark is also great!

### Wireshark Installation

It is as simple as ABC to install Wireshark. For Mac OS X or Windows, you can download the binary versions. Also, for most flavors of Unix/Linux, there's availability of Wireshark through the standard software distribution systems. And on other operating systems, the source code is available for installation. For the Windows version, the team that developed Wireshark built it on top of the WinPcap packet capture library. And if you don't have WinPcap already in your installation and you are using Windows, you may have to have it installed to run it. Here is a caveat: before you run Wireshark installer, you can use the manual process to remove an outdated version of WinPcap through the "Add/Remove Programs" in the control panel. The process of installation is the same with the wizard-based sequence that uses two main prompts: at startup, it will ask if you intend to start the WinPcap Netgroup Packet Filter, NPF service and if you want to have WinPcap installed. For you to capture packets, you can choose the former option that will allow you even if you don't have administrator privileges. It is only administrators that will be able to run Wireshark if you have this service enabled.

# Chapter 11: Firewalls

Based on a set of security rules, when you intend to block or permit data packets as well as monitor outgoing and incoming network traffic, a network security device that you can use is a firewall. For a firewall to block malicious traffic such as hackers and viruses, you will need to establish a barrier between your incoming traffic and internal network from external sources. You can improve the connection of computer security like the internet or LAN when you use tools like firewalls. An integral part of your network's comprehensive security framework is the firewall. With the use of a code wall that inspects each individual data packet as it arrives, the firewall's either side, both outbound and inbound from the system, to determine whether it can give it access to be blocked or pass, a firewall completely isolates your computer from the Internet.

When it enables granular control over the kinds of system processes and functions that have access to the resources of networking, you can further enhance the security through the capability of firewalls. For it to deny or allow traffic, there are several host conditions and signatures that these firewalls use. You can operate, setup, and install firewalls relatively easily even when they sound complex. The belief of some people is that when they have a firewall installed, the traffic that passes through the network segment will be controlled. However, a firewall that is host-based can be suitable for you. On your computer, you can have them executed, including using it with Internet Connection Firewall, ICF. Fundamentally, there is a similarity to the function of the two firewalls; to stop intrusion and offer a strong technique of access control policy. To put it simply, as access control policy enforcement points, a firewall is a system that safeguards your computer.

## Functions of Firewalls

In essence, here are some of the basic functions of firewalls:

- Act as an intermediary
- Report and record events
- Control and manage network traffic
- Validate access

- Defend resources

## The Definition of Personal Firewall

In the world of secure computing, it's quite essential for you to understand your need for a firewall. And since it aids our understanding of how a firewall may address those needs, we need to understand the goals of information security.

## The Need for Personal Firewall

Electronically, you will connect your computer to a broad network in the times of high-speed Internet access. You will have limited protection or control unless you have installed a personal firewall. There are some drawbacks to any high-speed connection, typical of anything else. Ironically, the same feature that makes a connection with a high-speed vulnerable is the same reason that makes it attractive. In some ways, you may be leaving your front door of your house unlocked and open with your connection to the high-speed internet. Some of the features of high-speed internet connections include:

- Constant active connection – this is the fact that when your computer is connected to the internet every time, it is vulnerable
- Access of high-speed – this means that it can be quite faster for intruders to break into your computer
- A regular IP – it will be easier for an intruder to find your computer again and again after they have discovered you

## Using a Personal Firewall for Defense

Compared to an ordinary 56Kbps connection, now it is clear to you how, when you are online on a high-speed internet connection, you are vulnerable. Now, the threat posed by this type of connection is now known to you, and how you can defend yourself against it is what you need to know. Here are some of the vital reasons for a personal firewall:

- You can easily develop policies for security to suit your

individual needs since most personal firewalls are highly configurable

- When your computer's program tries to connect to the internet, you wish to be kept informed
- The home network that you run requires you to keep it isolated from the internet
- You use a public WiFi network when you connect to the internet in an airport, café, or park
- With an 'always on' broadband connection, you surf the internet at home

## Firewalls Types

Though the two are suitable, you can have firewalls as hardware or software. With port applications and numbers, you can regulate traffic through the installation of a software firewall program on your computer while you can install the hardware firewall type between the gateway and your network. The most common firewall type is the packet-filtering firewalls, and in case they don't match an established security rule set, they prevent packets from passing through after they have examined them. The purpose of these firewall types is to analyze the destination and source of the packets for IP addresses. It will thus be trusted to enter the network if the packets match those of an 'allowed' rule on the firewall.

Stateless and stateful are the two categories of the packet-filtering firewalls. The ones that are easy targets for hackers are the stateless firewalls since they lack context by examining packets independently of one another. On the other hand, stateful firewalls tend to be much more secure because they remember information about previously passed packets. Though packet-filtering firewalls ultimately offer quite basic protection and tend to be quite inadequate, they can be indeed effective. For example, for them to determine the adverse effect of the application that the content of the requests is reaching can be quite hard for them. Thus, there will be no way for the firewall to know when there could be a deletion of a database from a misconceived trusted source if it allows a malicious request. Those that are equipped to detect such threats are the proxy and next-generation firewalls.

## SMLI, Stateful Multilayer Inspection Firewalls

While these firewalls compare them against trusted packets, they filter packets at the application, transport, and network layers. Also, if they pass the layer individually, SMLI only allows them to pass after they examined the entire packet, which is typical of NGFW firewalls. They ensure the potential of all initiated communications happening only with trusted sources as they determine the state of the communication and also by examining the packets.

## NAT, Network Address Translation Firewalls

These firewalls keep individual IP address hidden when they use a single IP address to connect to the internet by allowing several devices with independent network addresses. As such, they offer greater security against attacks because attackers can't capture specific details when they are scanning a network for IP addresses. These firewalls are rooted between outside traffic and a group of computers with proxy firewalls having similarities with NAT firewalls.

## Proxy Firewalls

At the level of application, these firewalls have the network filtered. They are planted between two end systems, which are not like the basic firewalls. The firewall must receive a request from the client and using a set of security for the evaluation, and after that, keep it blocked or give permission. Essentially, layer 7 protocols like FTP and HTTP are monitored by proxy firewalls and for them to detect malicious traffic, they utilize both deep packet and stateful inspections.

## NGFW, Next-Generation Firewalls

These firewalls blend additional functionality with the technology of traditional firewall like anti-virus, intrusion prevention systems, encrypted traffic inspection, and many more. Essentially, it has the inclusion of DPI, deep packet inspection. It is within the packet itself that deep packet inspection examines the data while looking at packet headers is what basic firewalls only look. With this process, users can stop, categorize, and identify packets effectively with malicious data.

# **Chapter 12: Obtaining User Information: Maltego, Scraping, Shodan/Censys.io**

Maltego reveals how information is connected to each other as a forensic and open-source application. The relationship between several information types can aid in identifying the unknown relationship as well as giving a better picture of their links. When you use maltego, you will have the ability to find relationships and also the people's link, such as mutual friends, social profiles, websites, and companies with the gathered information relationships. You may want to gather the connection between net blocks, DNS names, and domains if you intend to gather information regarding any infrastructure.

## **Architecture of Maltego**

Seed servers receive the request from the maltego client over HTTPS in XML format. Then, it is the TAS servers that will take the request from the seed server before the service provider then get the request. The maltego client will then get the results of the request. For more privacy, you may want to consider having your TAS servers. At present, the basic and professional modules are the two types of maltego, and the availability of the modules are the two major differences between both servers. CTAS is what the basic server has while in the professional server, you will see the PTTAS, SQLTAS, and CTAS.

From within maltego, you can perform several pentesting related tasks with PTTAS, including banner grabbing, port scan, and so on. Also, accessing SQL database is possible for TAS through SQLTAS. You can also get results after performing numerous SQL queries using this module. Postgress, Oracle, DB2, MSSQL, and MySQL are some of the supported types. Then, available in public sever are the transforms that are contained in the commercial TAS.

## **Launching Maltego**

For anyone to start maltego, you will go to the applications and look for backtrack. From there, you will get the information gathering and then to the network analysis where you will then see DNS analysis. From there, you will get into maltego. You will be prompted to register your product if you are accessing it for the first time. You will only need to input your email address and password if you have registered an account already. It will update the transforms when you have validated your login.

Hit on the tab 'investigate' after the updates of the transforms, and from the palette; you can choose your desired option. In the palette, you will see two major categories, which are personal and infrastructure. Also, other entities can be imported into the palette, for example, the Shodan entity. With the aid of their banner, you can find specific switches, routers, servers, and so on through a search engine like Shodan.

## Web Scraping with Python

Let's assume you want to quickly pull a huge quantity of data from websites as fast as possible, how can you accomplish this feat without getting your data by going to each website at a time? Well, the short answer is web scraping. For what you intend to do to be faster and easier, you may want to result to web scraping. If you want to collect data from websites and when the volume is huge, you can use web scraping. However, what can instigate someone to want to collect massive data from sites? It is essential to discuss the web scraping application for us to understand the reason:

- **Job listings:** some details from websites regarding interviews, job openings, and so on, which users can easily access since it is listed in one place.
- **Development and research:** they collect temperature, general information, statistics, and so on from websites, which are a large set of information by using web scraping, and they use the result for R&D or to carry out surveys after analyzing it.
- **Social media scraping:** finding out what is trending by collecting data from social media websites like Twitter through web scraping.
- **Gathering email address:** web scraping is used by several



organizations that use email marketing to send bulk emails after collecting them.

- **Price comparison:** for the comparison of the prices of products, web scraping is used by services like ParseHub to obtain information from online shopping sites.

The extraction of a massive quantity of information from websites is a technique of web scraping. The website's data are not structured, and to have it in a structured form, these unstructured data are collected by web scraping to do the job. Writing code, APIs, and online services are some of the different ways to scrape websites. Web scraping is allowed by some websites, while others don't allow it if we want to shift to the legal side of it. You may want to look at the "robots.txt" file of the website for you to know if such a website allows web scraping or not.

## Shodan and Censys

It is in the Internet of Things that we are now living. Starting from the street security cameras and traffic light management systems to home WiFi routers, things that are connected to the Internet are always in our encounter. And it is both on the web and the real world that we can find all of them because they have a connection. With Google helping to discover your sought-after data on the web, you can also find these connected devices with some special search engines.

Let's welcome Shodan and Censys!

Since it has been in existence for about 7 years now, for the Internet of Things, the foremost, as well as the first search engine, is shodan. The inspiration behind the name came from a highly villainous artificial intelligence named Shodan, who was the System Shock, the computer game series' main antagonist. Though it has the capability of wrecking harm, shodan in the real-world is not as relentless. However, you will want to know how the search engine works before we go on to the bad news.

Shodan is typically similar to someone that knocks on every door that they see as they wander throughout the neighborhood. However, there is the whole world instead of some city or knocking on every IPv4 address. This person would have some information and will give it to you if you ask them about a specific part of the neighborhood or a specific type of doors. The person would tell you the number of the doors, the individuals who answer these

doors, and their utterances. And about those Internet of Things, you can get their information from shodan, which includes whether there is a web interface you can use, their type, and how they are called. Through, relatively cheap, you will need to subscribe to you to use shodan because it is not completely free.

Except there are no locks on some doors, you may find nothing so weird about knocking on some doors. And for the bad guys to break in, it may not be possible for anyone. Some systems that use default passwords and logins, including IP cameras and unprotected routers, are the representations of these doors in the world of Internet of things. You will see yourself gaining complete access to the password and login when you have managed to figure out them after entering their web-interface. And because you can easily find these default information about passwords and logins on the manufacturers' website, everything is no longer rocket science. And if it has the support of an IP camera, you can control and even see everything if it is an IP camera. Also, you may alter the settings if it is a router. You can even use a scary voice to talk to the poor baby if it is a baby monitor. Everything is up to the standards of your morals.

# Chapter 13: Kali Linux on Portable Devices Like Raspberry Pi

Though, it can be fun enough to test networks, spoof accounts, or crack WiFi passwords. However, you may need an easily portable rig if you intend to take the show on the road. And so, here come the Raspberry Pi and Kali Linux. They designed Kali Linux for network penetration testing as an operating system. For you to test for Bluetooth vulnerabilities, spoof networks, WiFi passwords cracking, and plenty of other things, you have the chance of running it on your laptop. You need to know that you can be charged with a felony and get yourself arrested for violating the Computer Security Act if you break into protected networks using this knowledge. You can only use this knowledge to play with networks you control, for your learning, or simply use it for good. Now, since we have talked extensively about Kali Linux, and for the sake of not repeating all that you have read before, our focus will be on how we will build our Raspberry Pi and the version we will use. So, let's get it done!

For you to use Raspberry Pi, they don't require a lot of power for you to use them as a credit sized, small computer. You will have a super-portable system testing device that you can easily take with you anywhere you go with the combination of Kali Linux and Raspberry Pi.

## The Essentials

- For you to perform initial installation, you will need a desktop computer
- Get a portable, small wireless keyboard with touchpad that one side of a small bag can contain
- It tends to be quite useful if you are carrying the Raspberry Pi with you around. So, a case is fine but optional
- New version of point-to-this-screen is essential though with Raspberry Pi 2 or newer versions; it doesn't fit flush
- An 8 GB SD card
- A Wi-Fi card
- You will be fine with a few external 5V batteries that use a USB part built for smartphones. So, you need a pack of battery

- Model 2 or B/B+ of Raspberry Pi. Though to install Raspberry Pi 2, you will need some additional steps; you may want to use the Model B+ if you don't wish to go through those steps.

- 

## Step 1: Installation of Kali on the Raspberry Pi

For the Raspberry Pi, downloading and installing the touch screen build for Kali Linux will be the first thing you will need to do. The installation process is quite typical of installing any other operating system for Raspberry Pi. Here is a quick way to go about it:

### Installation of Kali to Windows SD Card

1. For your hardware, you will need to download the Kali Linux Raspberry Pi. You can grab the Pi 2 version for Raspberry Pi 2 and the TFT version for model B/B++. Inside it, you will unzip the img file. You will need to take note here because, for Raspberry Pi, you will have to download the standard version of Kali Linux if you're not using the touch screen display.
2. You will need to have the application (.exec file) unzipped within after downloading Win32DiskImager.
3. With the use of a card reader, you will then have your SD card inserted into the Windows computer.
4. Then, you will double-click on the application, Win32DiskImager.exe that you have just downloaded.
5. At the top right of the device, you will click on the drop-down menu to select from the list if the application doesn't automatically detect your SD card.
6. The Raspbian .img file that you have just downloaded can be found when you click on the folder icon of the file from the application's image section.
7. Win32DiskImager will work its magic as you wait for it after you have clicked the 'write' button. You can insert your card into your Raspberry Pi after you have safely ejected your SD

card when it finishes.

## Kali installation in OS X SD Card

1. For you to work with it on your hardware, you will firstly need to have Kali Linux Raspberry Pi image downloaded. You will take Pi 2 version for Raspberry Pi 2 and TFT version for model B/B++. The standard version of Kali Linux for the Raspberry Pi is essential to be downloaded if it is the screen display that you are using.
2. For your installed version of OS X, have the appropriate version selected as you unzip the application after you have downloaded RPi-sd card builder.
3. With the use of a card reader, have your SD card inserted into your Mac.
4. Then, you can have your RPi-sd card builder opened. There will be an instant prompt for you to select an image of Raspbian. The file that you have had downloaded earlier is all you will have to select.
5. Then, another prompt will inquire about the connection of your SD card. All that is required of you is to click on 'continue' since it is connected when you inserted it earlier. Then, the options for SD card will be presented to you. It will be checked, and you won't see anything else on the list if you have only had one inserted. Click ok on the card you want to use if not.
6. Then, you will enter the password for administration and press enter.
7. If there is any ejection of the SD card, you will see yet another prompt. Since for the application to perform a direct copy, it needs to unmount; there's nothing weird about it. In the Finder, for your SD card not to be available any longer, you will need to double-click it. A word of caution here: NEVER remove it from your USB port. You can click continue when you are sure.
8. Your SD card prepping will finish by the RPi-sd card builder. Then, you can insert it into your Raspberry Pi unit after you

have safely ejected it.

## Step 2: the Display Hook-Up

The touch screen works perfectly with the general-purpose input/output, which the Raspberry Pi has. You will see how this works ideally because, in the corner, it is the set of pins on your Raspberry Pi. Click into the display of the Raspberry Pi.

## Step 3: Have Everything Plugged in and Launch

At this stage, you will need to plug in everything through the attacked display. Have your Wi-Fi adapter plugged into the USB ports. After that, plug the Pi into your pack of batteries. Here, you can experience a clunky and slow process for the startup. If it takes some time, don't panic. First, before the startup process of the boot, for a bit while, you will see a white screen. Finally, a login screen will greet you. For you to get your screen working, you may have to work through some form of setup if you are using a Raspberry Pi 2. You may simply have to go to the next step if it is the B+ that you are using. Mainly, to get the screen running, there may be some needed steps for the current Raspberry Pi 2. A white, sad screen will welcome you when you boot it up initially. However, getting the screen working is not too hard. Unfortunately, Pi attachment may not require an HDMI monitor or through this part, you may need access into SSH. Then, to boot up your Pi, simply connect either of those.

## Step 4: Enable Wi-Fi as you Log in

For you to make use of the tools within Kali Linux, you will want to enable the Wi-Fi card as you log in. your Wi-Fi card will be recognized automatically by the Raspberry Pi. However, it is essential to get into your network. The user interface of Kali Linux then needs to be powered up in the first place. Finally, you must change your device's password before you engage in anything else. If you don't, your device can be controlled by another person with the hacking skills.

# Chapter 14: MalDuino

MalDuino has the capabilities of keyboard injection as an arduino-powered USB device. At superhuman speed, MalDuino will act as a typing, keyboard commands when you power it. Anything is possible with MalDuino since you can alter the desktop wallpaper or gain a reverse shell. Also, MalDuino can work well for pranksters, hobbyists, and penetration testers. The best BadUSB experience is all that MalDuino aims to provide. And using open-source libraries, it is through the arduino IDE that they have MalDuino programmed when it comes to software. You can convert the script written in DuckyScript into the code MalDuino will understand. For them to program it simply like, they would an Arduino; this makes it possible for expert arduino tinkerers to program it as well as making it newbie-friendly. The two versions of MalDuino are Lite and Elite.

## Elite

You can select the script you intend running from the card since this version has four DIP switches and a Micro-SD card reader, and it is quite bigger. Also, you can program the keystroke injection scripts that the Micro-SD card stored apart from burning the firmware only once. This process is in contrary to the Lite version, which, when you want to run a different script, it will need to be flashed. You can drop, repurpose, or reprogram all these features altogether because it is straight from the Arduino that they programmed the two MalDuinos. Although you may have a few pins to play around with, you can purchase one and simply prefer to use it as a usual Arduino. You will be prompted to participate in the crowd-funding campaign particularly with the freedom that it offers.

## Lite

The Lite version contains a switch apart from the USB connector, and this version is quite small. You can choose between programming and running mode with the function of the switch and the indication that the script has finished running through a LED. With more than enough space for most scripts, on its 32KB of onboard memory, the Lite stores a script. You can use the script converter to convert the scripts to malduino-friendly code since you can use a text editor to write scripts. Then, with the Arduino IDE, you can as

well upload a script. Using the switch at the back, you can toggle the Lite into ready mode after you have unplugged the MalDuino Lite. Then, you can start using it!

## The Hardware

The board of the Elite version measures around 4.6 cm x 1.1 cm, roughly 1.8 in x 0.43 in, which you can use an old case for it. For the Micro-SD card and DIP switches, you may need to cut some holes for them. It may come to your realization that the firmware it ships with is likely some kind of QC test for the dips after you exercise some RTFM and play around with the switches. Depending on which switches are on, these features make the output of MalDuino the numbers 1 to 4.

## The Setup

Your Arduino IDE must not only be installed but also up to date when you want to set up the MalDuino. Because they programmed the Elite as a ‘Sparkfun Pro Micro’ that runs at 8 MHz and 3.3 V, it will be required of you to install the Sparkfun boards and open up the board manager. Then, the online portal of the Malduino Script Converter is your next point to go since there so many purposes that it servers like:

- For you to import to the IDE, it auto-generates the Arduino project
- You will have the freedom of selecting the language of your keyboard layout
- Between the Elite and Lite version, you can convert scripts through it

You only need to have the MalDuino flashed once and then store new scripts using the Micro-SD card when it is in normal operation as you empty script to download the project or create a simple script for the Elite version.

## The Software

For you to run a command, a quick shortcut will be the combination of the ALT-F2 since you are running Linux. As such, you can save a file to 1111.txt after scripting that into a file. Then, for a file that corresponds to the recent



dip switch state, the search will be on the Elite for the Micro-SD card if you power the dip switch 4 and 2. As such, there will be an attempt by the software on parsing the content and finding the file with the name 0101.txt, i.e., not the binary representation of the number 4 and 2 but in dip switch order 1,2,3, and 4. Then, there will be a quick flashing of the red LED when it finishes. It is possible that only command functioning accurately is the ALT-F2 combo, and nearly all commands worked. Thus, you won't get any run command window without ALT-F2.

## Protecting Yourself From MalDuino

As keystroke injection tools, a wider family of USB devices, referred to as BadUSBs is MalDuino. They have the capability of doing several types of devilish things by taking advantage of keyboard input as a trusted method of interfacing with a computer. However, what are the measures you can take to guard yourself against MalDuino? You can mitigate or protect yourself from the dangers of BadUSB attacks with the following 3 ways:

### Admin Rights Lockdown

It doesn't matter if you are concerned about BadUSB attack or you are not; doing this can be quite useful. If you want to make changes to the admin-level, you only have to provide the prompt of yes or no to make changes that require admin rights on Windows 10. Even if the person is the admin, you will see that it is wrong and silly to provide someone that level of control. Before handling the keys to the castle, you can change this with a registry level edit to make the operating system require your admin password.

### Duckhunt

This technique is applicable on Windows. There is a small application on github that can run as a backdoor process. The rate at which your keys are typed is what it continually monitors. When it detects unusual typing speeds, it will block all HID. However, some of the first few characters of an attach can likely get through and that is the only downside of it.

### Physical Protection

It is simply a catch-all solution, and it is quite vital not to allow unauthorized

devices from being plugged into your system. You can invest in some port blocker devices to block all access to USB ports physically. You may have to look deeper in the case of critical infrastructure. All the same, you can prevent any attack by using it when you are out in public.

# Chapter 15: Kismet

As a wireless intrusion detection framework, kismet is a wardriving tool, sniffer, device detector, and wireless network. While kismet functions in compliance with hardware such as RTLSDR as well as some specialized capture hardware, it also works with certain software-defined radio, Bluetooth interfaces, and Wi-Fi interfaces. To some extent and under the WSL framework, kismet also functions with Windows but works well with OS X and Linux. Kismet works with Bluetooth and Wi-Fi interfaces, as well as other hardware devices on Linux. The built-in Wi-Fi interfaces enable it to function on OS X and works with remote captures on Windows 10.

## Watching the Activities of Wi-Fi User Using Kismet

With a sight's direct line and directional Wi-Fi antenna, it is possible to detect the signals of Wi-fi passing through the walls of your home, even with its walls of privacy. People can learn a huge amount of data from this information, such as nearby devices' manufacturers, the movements of the residents, and also the network they use at a given time. For fixed targets, using kismet in a fixed situation can result in more nuanced information. Thus, it is ideal at displaying relationships between devices over time instead of just looking for the access point out there. The draw is from signal intelligence methods when we spy on users using kismet, whereby it is through the signals it conveys that we hope to learn about what we can't see. Here, Wi-Fi is the things we are dealing with and the devices that someone owns, human activity, connected devices, and routers are the things we are trying to see. Doing this goes a long way to your imagination.

You will be more inclined to put off your Wi-Fi on unused devices and make a switch to a wired network if you are able to figure out that someone could see whether you were using your laptop or on your PlayStation and whether you were in your house. Using a wireless network, they use kismet to scan every available Wi-Fi channels silently by putting it in monitor mode for wireless packets for it to work its magic. You can see automated beacon frames as these packets that can be broadcasted by the wireless APs several times in a second. Also, not yet connected probe frames and data packets exchanged from connected devices. Kismet has the ability to visualize the activity of devices associated with specific networks as well as the networks

themselves.

## What We Can Get From Wi-Fi

So, how do we manage this situation? You can get on to explore nuanced details about a network you want to watch when you have identified it. You may want to look for details such as the network connection of the hardware and electronics of someone or an organization. You will be able to know the kind of configuration for some devices and also the recognition of various setups types for fingerprint. Not only will laptops and smartphones be plain to you, but you will also have the ability to see connected hydroponics or 3D printers with a setup such as this.

Now, the kind of person you are has a lot of dependence on the usefulness of this information. It would be useful to a thief who wants to discover expensive electronics by snooping around all homes in wireless range. Using a jamming attack, you can potentially target one or avoid one completely because wireless security cameras can be detected by kismet. And when no one is in the house, we can easily infer since it's quite possible for us to see when the devices of clients use data, disappear, and appear. Also, with the use of the Wi-Fi signal data, hackers can combine data of the GPS by wardriving around a neighborhood. Doing this, each address of the wireless network will be possible for hackers when they build a map. Essentially, as there are already mapped networks by Google and Wigle Wifi, there could be an existence of this data. In the neighborhoods, for the detection of suspicious wireless activity, people can also use it as a neighborhood watch.

## Essential Tools

There are some things needs to adhere to this guide. You will need kismet for you to run a Linux system, and for the scanning, you will also need a wireless network adapter that is compatible with Kali. Here, the older version which is stable is what we will discuss even though different wireless cards like macOS can run on the recent type of kismet. If your desire is to have it run on the Raspberry Pi, kismet will function perfectly on a Kali-Pi installation as well as a virtual machine.

### **Step 1: kismet installation:**

The git repository will have to undergo a cloning process before the installation of kismet on Kali Linux. You may not need to worry about any

dependencies based on the type of operating system that you are using. However, the slightly longer list of dependencies for kismet may be needed to be installed for smooth running of kismet. Since you will have to sort, login, decode, and detect a huge number of wireless data, they are quite needed. Also, you will need to install lots of libraries because you will be controlling a wireless card. Then, you will need to have the installation configured by navigating to the kismet directory. For your specific operating system distribution, this process will have the installation configured. Then, you can create the installation after the completion of that process. You will use the *suidinstall* option to complete the installation by running the resulting file with it. Then, you will install kismet. After the installation, you will need to capture packets as a non-root user by adding yourself to the kismet group. Ensure that your actual username is replaced in the space for “YourUsername.”

### **Step 2: monitor-mode your wireless card:**

With the USB settings, you will attach your wireless network card to the virtual machine or to your computer. The commands *ifconfig* or *ip a* can be used to find your card. You can use a “wlan0” or “wlan1” to name your card. You can then put your card in a monitor mode after naming it. At the end of the card’s name, you will see a “mon” as it is renamed with this process. And to launch kismet, you will use this name.

### **Step 3: launch kismet:**

It is simple to begin using kismet. For your card that you have put in wireless monitor mode, ensure to put the term after the *-c* since to specify the source it captures, kismet makes use of the *-c*. Then, kismet will start capturing packets after starting up. Then, you can return to the menu and make some customizations.

Several Wi-Fi devices that you can detect nearby will appear before you as you start kismet. Based on whether you are using 5 GHz, 2.4 GHz, or the two of them, you will have variance in the number of devices that you can detect.

# Chapter 16: Bypassing a Hidden SSH

Now we need to take some time to look at going through and bypassing one of the SSH logins. We are going to do this by adding our own key to a remote server and then getting the access that we want. So if we want to go through and setup the SSH keys so that we can quickly and efficiently log in without a password, we are able to do this with a single command. This is going to be a simple process to go through.

The SSH is going to be known as the Secure Shell, and it is going to be a cryptographic network protocol that is going to be useful for helping us to operate the network services securely over a network that is unsecured. The typical applications that we are going to see with this one are going to include options like logging in with the command line and remote command execution, but it is possible that any network that you want to use is going to be secured with the SSH protocol.

The first step in this process is to make sure that we have been able to run the keygen command in order to generate the keys. If you have already generated some of these keys, then we are able to skip these steps. The code that we are able to use for this one is below

```
ssh-keygen -t rsa
```

Then we are able to go through and use this particular command in order to push the key so that it becomes connected to the remote server. This is going to be something that we are able to modify in order to match the user name of the server and the host name of your server as well. We will be able to go through and use the code below to make this happen.

```
cat ~/.ssh/id_rsa.pub | ssh user@hostname 'cat >> .ssh/authorized_keys'
```

The first time that we copy over these keys, we are going to need to enter the password to help the program get set up and ready to go. After that first time, though, we should be able to login without needing a password, or even use the rsync or scp without entering the password at all. You are able to test this with the following command:

*ssh user@hostname*

It is definitely going to be a lot easier to go through compared to typing in a password all of the time.

And, that is all that we need to do. It is going to spend some time helping us to get onto the SSH and will make it easier for us to get onto this without needing to use a password each time that we do the work. Getting this done can be hard, and you do need to know the password the first time around, but if you are able to get ahold of this, and you will be able to get onto the network any time that you would like.

# **Chapter 17: Bypassing a Mac Address Authentication and Open Authentication**

Another thing that we are able to do when it comes to hacking is to bypass the Mac Address Authentication in order to get onto the network that we want to use. This is going to be a feature that we are going to find with Mac addresses that will allow us to get onto the system and use it in the manner that we would like. This will ensure that we are able to either get onto our network when it is not working well or on another option that we would like to use, such as hacking into another computer. Let's take a look at how this is going to work.

The Media Access Control address, or the MAC address, is going to be interesting because it is able to uniquely identify each node that is going to show up in a network. It is going to take the form of six pairs of hexadecimal digits, which can include 0 to 9, and all of the letters A to F, that are going to be separated out by either dashes or colons.

This MAC address is usually going to be associated with the network adaptor or a device that has some networking capabilities. Because of this reason, it is going to be known in many cases as the physical address. The first three pairs of these digits in the address are going to be called the Organizational Unique Identifier, and we need to take some time to look at them because they help us to identify the company that either sold or manufactured the device. Then the last three pairs of digits that are going to show up are going to be the specific numbers that just go to that device, and can be like the serial number of the whole process.

With this in mind, we are going to spend some time going through and looking at some of the steps that we need to use in order to bypass the MAC address filtering on some of our wireless networks. The first step that we need to work with is considering that we are going to working with a router that has the MAC Filtering Configured in the first place. We can say that our MAC address is going to be AA-BB-OO-11-22. This is one that is allowed to show up when we are using the MAC filtering on our own wireless network.



Then it is time to move on. We can log into the machine that we are using for Kali Linux and then put that Wi-Fi adapter into the mode that allows it to monitor what is going on around it. This is going to be done with the airmon-ng and can be done with the simple command into our terminal below:

*Airmon-ng start wlan()*

Now it is possible that some of the processes with Kali Linux when you do this will show us some errors. If you do end up with some issues or an error message here, then you need to kill the process in this program that seems to be having the issue. You are able to do this with the command below:

*Kill [pid]*

Now it is time to go through and launch another part of this process, which is the Airodump-ng. This will help us to locate the wireless network that we want to work with, and will even help us to see which clients are connected in this whole process. The command that we are able to use to make this one happen is below:

*airodump-ng -c [channel] -bssid [target router MAC Address] -i wlan0mon*

This should then show us a whole list of the clients who are connected to this device at the bottom of our terminal. Then the second column is going to list the MAC addresses of all the connected clients we will be able to spoof at this time in order to get that wireless networked authenticated so we can do what we would like on it.

The one thing to note at this time is that you are only going to get a list with this step if there is actually someone who is connected to the wireless network that we are looking at. If you do not have someone currently connected to the device, then you will not get a list at this point.

Now it is time for us to go on to the next step. After having been able to go through and find the MAC address that you want to use, it is time to go through the process of using the MacChange in order to spoof the MAC address that we want to work with. We are going to spend our time spoofing the MAC address of your wireless adapter, but the first thing that we need to

do here before we get started, we need to take down the interface for monitoring known as wlan0mon and wlan0. This is going to allow us to make some of the changes that we want to the MAC address. We are able to do this with the following command to make things a little easier:

```
Airmon-ng stop wlan0mon
```

When that process is done, we are able to take down the wireless interface who's MAC address we want to spoof in the following command:

```
Ifconfig wlan0 down
```

Then this is going to bring us the MacChanger. We are able to use this tool in order to change up the MAC address. The code that we are able to do with this one will be below:

```
Macchanger -m [New MAC Address] wlan0
```

And then we want to go through and bring all of that back up. Remember, a few steps above, we went through and closed down the system so that we could change ours and get ourselves on this option. But now we want to go through and bring it all back up again. The code that we are able to work with here will include:

```
Ifconfig wlan0 up
```

Now that we have been able to change up the MAC address that is on our wireless adapter to a white listed MAC address that the other network will allow, we are able to try out authenticating with the network and see whether this worked and if we are able to connect to the process as well.

And that is all there is to get this done. Keep in mind that this process can take a bit of time if you are not going to find someone who is on the network right in the beginning. You may need to have some patience with this one to make sure that it is going to work the way that you would like and to ensure that you can actually find the right MAC address that is going to work with that router.

But once you have been able to go through and change up your MAC address so that it works well with one of the other options that belong to that wireless network so that you are able to get on as well. This is a simple process is going to be able to help us learn more about the process and how we are able to work with getting onto the network that we would like along the way.

# Chapter 18: Hacking WPA and WPA2

The world of wireless networks is going to be great for a lot of consumers. It adds on a lot of protection to the networks of the past, and it is going to be important to helping us to work with our wireless network while on the move and without having to be connected to your cable all of the time. The WPA and WPA2 options are going to be some of the best when it comes to keeping your information safe, but it is possible for hackers to get onto them if they are patient, and they are ready to go through and take on the hard work. That is why we are going to spend some time in this chapter taking a look at the steps that are necessary to hack onto these two wireless networks.

The first thing that we need to take a look at is preparing our attack. We need to first have a better understanding of when we are able to legally hack into a Wi-Fi network. In most regions, the only time that you are able to legally hack onto some of these networks is when the network belongs to you, or if it belongs to someone who has given us written permission to hack into the network so that you can check it and make sure that it is safe from a hacker. Hacking networks that don't meet the criteria that are above, then the hacking process is illegal and it could be known as a federal crime if you are caught in the act.

Now that this is out of the way, it is time for us to go through and download the disk image of Kali Linux. This is going to be one of the preferred tools to work with when it is time to hack these networks. You can download the installation image, also known as the ISO, by using the following steps:

1. The first step that we will work with is to go to the <https://www.kali.org/downloads/> on the web browser of your needs.
2. Click HTTP next to any of the versions of this that you would like to use.
3. Wait for the file to finish with the downloading process.

From here, we want to be able to attach a flash drive over to the computer that we are working with. The flash drive that we are using is required to come with 4 gigabytes of space or higher in order to complete this process.

Then we can make the flash drive bootable. Finish up the rest of the steps that you need to do to get the Kali Linux system set up and ready to go on your own computer.

When the Kali Linux system is set up and ready, it is time to begin the actual hack that we want to accomplish. We can do this by opening up the terminal for Kali Linux on your computer. You can find and click on this Terminal app icon, which is going to look like a black box that has a white “>\_” on it. You can also just click on Alt, Ctrl, T to open this terminal up.

This is the time where you will want to install Aircrack to help with the attack. You are able to type in the command that is below to help you get this one started:

```
sudo apt-get install aircrack-ng
```

When the prompt comes up for this one, you will want to enter in the password. You can type in the password you use to log into that computer in the first place. Then press on the Enter button. This is going to make sure that the root access is going to be enabled for any of the other commands that you would like to be able to execute in the Terminal. If you decide at this time to open up another window for a Terminal, which is possible, remember that you may have to go through and run a command with the sudo prefix or choose to enter the password into the system again to get the best results.

This is where we are going to be able to install the Aircrack-ng program that we were talking about before. When it prompts you to, you should press on Y, then wait until the program has time to finish installing overall. When this installation is done, it is time to turn on the airmon-ng. type in the command to do this and then press on Enter to continue.

Then it is time for us to go through and find the name of the monitor that we want to use. You are going to find this located somewhere in the Interface column. If you are working to do this attack on your own network, then it is going to be named as wlan0. If you do not see the name of the monitor at all, then be aware that your specific card for Wi-Fi is not going to support this kind of monitoring at all.

Now it is time for us to go through and start the process of monitoring our network. You are able to do this with the following command below, and

then press enter when you are done

*Airmon-ng start wlan0.*

Make sure that you press the right name of the network that you would like to monitor. If you are doing your own, then you would add in the wlan0. But if you are trying to monitor the wireless of another computer, then you will need to make some changes in order to handle this and make sure that you are actually managing the different network that you would like.

Then we need to go through and enable a monitor mode interface with this. When we find that, we are able to enter the following command to help us get this set up:

*Iwconfig*

Now, there could be a few different processes that show up, and it is possible that some of them are going to return errors to us. If this happens, then we will want to kill any of the processes that are going to return errors to us. This is often going to happen when the Wi-Fi card is going to conflict with some of the running services on your computer. You are able to kill these processes when you go through and use the command below:

*Airmon-ng check kill*

While we are here, we want to review the name of the monitor interface. In most cases, the name is going to be something that is pretty simple, like mon0 or wlan0mon. We also want to make sure to tell the computer that it is time to listen to some of the nearby routers. To get a list of the routers that happen to be in the same range as you, you are able to enter the command below:

*Airodump-ng mon0*

Make that you replace the mon0 with the right part. We want to have it filled in as the name of the monitor interface that we used in the previous step, or

this is not going to work the way that we would like.

As you are searching around, we need to make sure that we are doing some searching here. We need to be able to find the router that we would most like to hack. At the end of each string of text that comes your way, you are going to see a name. You want to look through this to find the one that belongs to the network that you would most like to hack into in the process.

During this process, we need to make sure that we are working with the right router, and that we are choosing one that comes with WPA or WPA2 security that is attached back to it. If you see one of these on the left of the name of the network, then it is time to proceed. Otherwise, this is not going to be a network that you are able to hack along the way.

This is where we are going to be able to note the MAC address and the channel number of the router that we want to work with. These are going to be the pieces of information that we should notice on the left of the name of the network. The MAC address is going to be the line of numbers that we are going to find on the far-left side of the line for the router. On the other hand, the channel is going to be a number of some sort that is found to the left of the tag that you have for the WPA or WPA2.

In this part, we are going to be able to monitor the selected network until we see a handshake. This is going to occur when an item connects to a network, or when the computer is able to connect to a router. Enter in the code below in order to make sure that we are replacing the components that are necessary of the command with the information on the network:

```
Airodum-ng -c channel – bssid MAC -w /root/Desktop/ mon0
```

In this one, there are going to be a few things that are going to happen. First, we are able to replace the channel with the channel number that we were able to find in the other step.

Then we want to replace MAC with the MAC address that we plan to use or spy on here.

Remember that we also need to go through and replace the mon0 with whatever the name of the interface is that you want to work with.

When this is all in place, we just wait around for some time to see that handshake appears. Once you see a line that has the tag of WPA handshake,

and it is followed with a MAC address that shows up at the top of your screen on the right, then it is time to proceed. It is also possible for us to move this along and not wait around all of the time, it is possible for us to force a handshake using the deauth attack before we continue on with this part.

When it is time to go through and get that handshake, then you will be able to get onto the network and look at what is going on, as long as the other person does not have the proper security on their network at that time. You will then be able to get through some of the security protocols that are there, and this allows you to look around, read through and change some of the packets that are shown, and so much more. You need to work with a few tools to make this happen, but it can be a successful method to finish the hack that you would like to accomplish.



# Chapter 19: Secure and Anonymous Using Tor, Proxy Chains, and VPN

There are going to be some situations where you would like to get onto a network and do some of the work that you want, without other people being able to track where you are going. Being secure and anonymous online is something that a lot of people aim for in their work, and it is sometimes hard to make sure that you can get to this point, and maintain that secrecy. That is why we are going to spend some time looking at the different methods that we are able to use to keep ourselves hidden and safe when we are online.

## What is Tor

Tor is going to be a protocol for internet networking that has been designed in order to anonymize the data that is relayed across it. Using this software is going to make it, at a minimum, hard, if not impossible, for snoops to come onto the network and see your social media posts search history, webmail and other online activity that you try to do. They will also find that it is hard to figure out what country you are from, just by analyzing your IP address. This can be useful for a lot of people who want to be online.

When you run this service, some of the bigger data collectors, like Google Ads and other options will not be able to go through and perform some of the traffic analysis that they want, and they will not be able to go through and gather up some data on the habits that you are doing online. This also makes it harder for hackers to gather that information as well.

The Tor network is interesting in that it is going to run through the servers of thousands of volunteers who are found through the world. The data that you use is going to be bundled up in packets that are encrypted when they enter into this network. Then, unlike how we see with our traditional internet connections, Tor is going to be able to strip away part of the header of the packet, which is going to be part of the addressing information that can be used to help us learn some things about the sender, such as the operating system where this message was originally sent from.

Finally, Tor is going to be able to encrypt the rest of the information that we

use for addressing, called the packet wrapper. This is something that the regular connections that we use with the internet are not going to use this. Then our data packets, which are encrypted and modified, will be routed through many of these volunteer servers, known as relays, while it makes its way to the final destination. The roundabout way that these packets are going to travel on this network is going to make it harder to track.

Each of the relay parts is going to decrypt just enough of that wrapper to know which relay the data came from in the first place, and which relay it needs to send that packet to the net. The relay is then able to rewrap this in a new wrapper before sending it along again.

While this method is not 100 percent accurate all of the time, it is going to be able to keep your information a lot safer than we will see with regular connections to the internet. The fact that we are encrypting the data that we use, and that we are able to work with this in a manner that relies on relays rather than sending it just one place at a time, can make it a lot easier and more secure to work with.

## Using Proxy Chains

Another option that we are able to work with here to ensure that our information is going to stay safe and secure along the way is to work with these proxy chains. These are going to make it a lot harder for the hacker to find us and what we are doing. It will utilize an intermediary machine whose IP address is going to be the one left on the other system, rather than our own. And the Proxy system is set up to make this all work.

The proxy chain is going to be used to help us to accept our own traffic, and then we will forward it on to the target that should receive it. The proxy is going to spend time logging all of the traffic that we would like to send in either direction, but the good news is that if someone would like to look through this log, they would need to get a search warrant or a subpoena to do it, and this makes it harder for us to get onto the other network without anyone finding us.

If we are able to take some of our coding skills and string more than one of these proxies into a chain, it is going to become even more difficult for the other computer to detect the original IP address that we want to work with. On the other hand, if one of the proxies is found to be out of the jurisdiction

of the victim, then it is going to be really unlikely that any traffic is going to actually come back to our own IP address.

The good news is that, if you would like to stay hidden with the help of proxies, both BackTrack and Kali with Linux are going to have some good tools that are going to help with doing this process, and this is going to be known as a proxy chain. It is up to you to determine if this is the right option to keep your network secret and hidden.

## VPNs

Another tool that we are able to work with when it is time to keep our network safe is the VPN. This is going to stand for a Virtual Private Network, and it is going to allow you a way to create a secure connection to another network through the internet. These can be a great option to use in some cases when we would like to access websites that are restricted based on your region, to help your browsing activity from others seeing it, and more.

These VPNs are really popular though they are not going to be used in many cases for the original purpose for what they were designed for. They were originally made to help connect a business network together over the internet or allow you a way to access a business network when we are at home.

To keep this as simple as possible, the VPN is going to be able to connect your computer, tablet, or smartphone to another computer or another server somewhere on the internet, and you are able to browse the internet with that connection to keep things safe. So, if you see that this server is found in another country, it is going to seem as if you are actually in that company and allows us to pull up information and services that we would normally never be able to gain access to at all.

There are a lot of great ways that we are able to benefit when it comes to working on the VPN. These are going to include:

1. Will help us to bypass some of the restrictions on location when it comes to websites or streaming some of the video and audio that we would like to get ahold of.
2. It can make it easier to stream some of the content that we

would like on Hulu and Netflix.

3. Will make it easier to protect yourself from things like snooping or issues with hotspots of Wi-Fi so that it is harder for a hacker to gain the access that they want.
4. Will help us to gain at least a little bit of anonymity when we are online and can really hide our true location from others.
5. Makes it easier to protecting yourself from being logged when you are torrenting.

It is common for people to work with VPN and other services when they would like to bypass some of the geographic restrictions to watch the shows and movies that they would like in different countries or even to help with torrenting. This can be especially useful when you would like to hack, though, because it makes it harder for others to find you and figure out where all of the attacks are coming from in the first place.

# Chapter 20: IP Spoofing

The next topic that we need to spend a bit of time on here is the idea of IP spoofing. This is going to be a process where we are able to create packets for the Internet Protocol that are going to have modified source addresses in them, to either help us hide the identity of the person who is sending the information, to help us to impersonate another system of computers, and sometimes for both. This is often going to be the technique that a hacker is going to use when they would like to perform a DDoS attack against their target device or against the surrounding infrastructure.

Sending and receiving these packets is going to be one of the main methods that these networked computers and devices are going to communicate, and it is going to be kind of the basis of how the modern internet is going to work. All of these IP packets are going to come with a header, which is then going to be followed by the body of the packet, and will contain some of the important information on routing like the source address. In a normal packet, one that the hacker has not messed around with, the source IP address is simply going to be the address of who sent the packet. But if the hacker has been able to spoof the packet, then the address is going to be forged instead.

IP spoofing is going to be analogous to an attacker sending out a package to someone with the wrong address to return listed out. If the person who received the package wants to stop the sender from sending out this package, blocking all of the packages that come from that address is not going to do much good because the return address can be changed as well.

Along the same idea here, if the receiver would like to be able to respond to the return address that they see on the packet, their response package is going to not head to the real sender. Instead, it is going to head to whichever IP address that the hacker stole to use. The ability to spoof the addresses of packets is going to be one of the biggest vulnerabilities that we are going to see with these DDoS attacks.

For example, the DDoS attack is going to be reliant on spoofing with the goal of overwhelming a target with traffic while masking the identity of the source that comes with it. This is going to make it harder to work with any mitigating efforts if the IP address of the source is false, and it is randomized

on a continuous basis, blocking the requests that are malicious are going to be a lot harder to do. IP spoofing, as a result, is going to make it really hard for cyber security teams and law enforcement to track down who is causing the attack.

Along the same lines, we are going to find that spoofing is also going to be used to help us masquerade as another device when we would like. So that the responses that come with this are going to be sent over to the device that we are targeting instead of over to us. Some attacks, including the volumetric attacks like DNS amplification, are going to rely on this kind of vulnerability. The ability that we have in order to modify the source IP is going to be a big part of the design that we are going to see with the TCP/IP protocol, which means that we are always going to have to be worried about what is happening here.

Tangential to the DDoS attacks that we talked about before, spoofing is going to be done with the whole aim of hiding and pretending to be another device. This is going to allow the hacker to come in and sidestep the authentication and to gain access to or hijack the session of another user. The hacker is then able to go through the process of doing whatever they would like with this network, which is going to allow them to cause some damage and attack the network, without anyone being able to attach it back to them.

# Chapter 21: Penetration Testing with Metasploit

The final thing that we are going to take a look at here is how to work on a penetration test, and how we are able to use the Metasploit system to help us get all of this done. Penetration testing, or a pen test, is going to be a process that involves attacking some of the information systems in a similar way as an attacker would to your system. This helps us to find some of the vulnerabilities in the system and close them up before the hacker can get to them.

The distinguishing characteristic that we are going to find with pen testing is that there will not be any harm done to the system, and the owner of that system will provide the necessary consent before you get started. The vulnerability that we will see will be defined as a weakness in the security that is going to exist in a part of our system that will provide an entry point for the hacker to use to start their attack. There are a number of places where these vulnerabilities are going to show up, such as errors in the design, bugs, and more.

Some of the most common entry points for these attacks and places where we need to check out before a hacker can get to them includes the browsers, SQL injection, flash, ActiveX, and social engineering.

Due to the different scenarios that can cause an attack, different penetration testing types are going to be needed. The three types of testing that we are able to look through can include white box, black box, and gray box testing. When we start out with some of the black box testing, then none of the information about that system is going to be provided back to the person who is doing the testing. It is going to be the responsibility of our tester in order to gather up the right information about the system that they are supposed to attack.

Then we are able to move on to the white box testing. This helps because it is going to provide complete information about the target system from the beginning. This is going to be useful because it helps us to understand some of the impacts that can happen with an internal attack on the network.

And then we finally have the grey box attack. This is going to be where the tester is going to get some of the information about this system, but not all of it. These tests are going to be the most useful to help us better understand what can happen, and the main impact, of one of these external attacks.

So, we need to work through the four stages that are going to happen when we work with penetration testing and the Metasploit process. The first stage that we are going to focus on is the planning out the test that we want to use. The objective of this is to help us to identify the scope and even the strategy that we want to use in order to carry out this test. The scope of this test is going to be informed by currently practiced policies and standards.

The second stage that we are able to work with is going to be known as discovery. There are going to be three things that we are able to do here. The first one is to gather up some of the information on the system and some of the data that it holds. This is going to be known as fingerprinting. Then we reach the second activity and that is known as scanning and even probing system ports. And finally, the third activity is going to help us to identify any vulnerabilities that the system is going to have.

The third stage of this testing is going to be all about the attack. This stage is going to be able to help us identify the exploits for the vulnerabilities. An exploit is going to be a computer program that has the objective of utilizing a vulnerability in order to get the necessary access to that system overall. After the hacker is able to gain this access, the payload is going to be the software that will help them to gain the necessary control over that compromised system. The exploit is going to be done in order to help deliver the payload that we are working with here.

And then we end up with the fourth stage. This is one that can often be forgotten, but if you are doing this process for someone else, then you will want to pay attention to it to help them out. This stage is going to be known as reporting. The objective that we are going to see with this stage is that it helps us to create a detailed report of some of the identified vulnerabilities of the system, the impact that they have on our business, and some of the necessary solutions.

Although there are going to be a ton of different tools that are able to help out with this process, Metasploit is going to be one of the tools that is used the



most. That is why we are going to spend some time looking at how to do this kind of process, the process of working with a penetration testing, and how it can be done with Metasploit.

First, we have to realize that Metasploit is going to be a framework that has been organized into modules. The first type is going to be to do the exploit. These types of modules are designed in a manner so that they are able to take advantage of any weaknesses that are found in a system. These are going to be things like code injection, application exploits, and buffer overflow.

Then there are going to be some of the auxiliary modules. These are going to be the ones that will perform some actions, but these actions are not set up to take direct advantage of some of the weaknesses on the system. For example, these can be things like service denial and scanning.

The third type of module that is found on this system is going to be the post-exploitation modules. These are important as well because their main focus is going to be helping us gather information on some of the target systems.

And finally, we are going to find the payload modules. These are going to be the modules that can run after a weakness has been exploited in a successful manner. The payload is going to provide the means to help us control the system that we were able to exploit along the way. With this payload, it is easier to open up the meterpreter to help write out the DLL files.

So now, we need to take a moment to download this system to get it up and running. We are going to go through and do it with the Windows installation here, but you are able to go through and make changes and do some of the work that you would like to prevent other issues along the way as well, and it will work in a similar manner on other systems. You just need to go to the Metasploit website and then click that you want to do the Windows installation.

From here, you will want to download the installer, and then there will be some prompts that show up that will help you to get this installation completed. To help confirm that the installation was a success, you need to start the command prompt, making sure that you are the administrator, and then use the command of “`commandsfvenom.bat -helpd`.” If you get an output, then this will show you that it worked, and it should list out all of the

different options that are available for you to use from this part.

There are a few options that we are able to work with here. For example, if we would like to be able to list out all of the payloads that are available, we would be able to work with the command of “msfvenom.bat -list payloads.” This could be a long list, but it still shows us what is available here.

If you would like to go through and start up the console that is available with Metasploit, you will need to use the command of msfconsole.bat. You will then be able to access the msf console, which is going to be the tool that we can use for the command line that is going to work with this program.

The next thing on the list that we are able to focus on, we need to list out all of the exploits that we have available with the help of the command help search. If we want to go through and search around for a specific exploit, you will need to use the CVE number, platform, or name. Let’s say that we want to be able to list out all of the exploits that happened in the year of 2018. To do this, we would need to bring out the command of “search cve:2018” and this should list out all of the parts that we need.

To go through this process and then gather up some of the information about the exploit that happened, we need to pass the url of that exploit and make sure that it is in the info command. The code that we are able to work with to make this happen includes:

*Exploit/multi/browser/java\_jre17\_exec.*

After we are able to look through the list and then we can find an interesting exploit that we want to use, it is time to use the command that we used above. After we issue the command that we want to work with that specific exploit, it is possible for us to set some of the options that we want to use with the set command. This could be something like setting the local port and local host. The commands that we are able to use to make this one is going to happen will include the following:

```
set SRVHOST 0.0.0.0  
set SRVHOST 8080
```

If you would like to be able to go through and check the variables that we are

able to set, we would want to work with the command, show options to get it done. When the exploit that we are working with has more than one target, we are able to set a specific target by specifying an ID to the set target command. Some of the available targets that we will want to work with are going to be listed with the help of the command of show targets.

Working with the Metasploit program is going to make it a lot easier for us to go through and complete one of our own penetration tests. This is going to make it easier for us to go through and learn a bit more about our system, and figure out where some of the most common vulnerabilities are going to show up and how we are able to close them up and keep the hackers out.

# Conclusion

Thank you for making it through to the end of *Hacking with Kali Linux*, let's hope it was informative and able to provide you with all of the tools you need to achieve your goals whatever they may be.

The next step is to get to be where we are able to spend a bit of time learning more about the world of hacking and how we are able to utilize it for some of our own needs. Whether you are looking to protect your own network and make sure that a hacker is not able to get onto the system, or you are more interested in hacking onto another network and taking the information (which, as we discussed, is illegal), you can utilize a lot of the techniques and other methods that are found in this guidebook.

There are a lot of different parts that come together when we are trying to work with hacking, and Kali Linux is going to be a great resource to help us get through some of these hacking, and will ensure that we are able to get this all done. We spent some time taking a look at how to set up the Kali Linux system so that it is ready to go and help us with all of the hacking that we want to do along the way.

In addition to being able to work with the Kali Linux system in order to get some of our hacking done, we also need to spend some time taking a look at some of the other hacking techniques that we are able to use. We are going to spend some time looking at how to do a penetration test, some of the man in the middle attacks, denial of service attacks, how to get onto some of the wireless networks, and the importance of a penetration test.

Then we took some time to look at the different parts that are able to help us to keep our networks safe. For example, with the help of a good firewall and the use of penetration testing, and even VPN's and other options like this to keep your anonymity when you are online, you will be able to make it a bit harder for the hacker to find you, and this makes it so much easier for you to keep all of that information as safe as possible.

There are many parts that come to the world of hacking, and it is important that we learn some of the methods and techniques that come with this in order to keep things organized and to keep the hackers out. When you are

ready to learn a bit more about hacking and how it can work for some of our needs, make sure to check out this guidebook to help you to get started.