INDEX

Sr.no	Aim	Date	Page No	Sign
1	A.Use the following tools to perform footprinting and reconnaissance			
	i. Recon-ng (Using Kali Linux) ii. FOCA Tool iii. Windows Command Line Utilities			
	• Ping			
	• Tracert using Ping			
	• Tracert			
	• NSLookup			
	iv. Website Copier Tool – HTTrack v. Metasploit (for information gathering) vi. Whois Lookup Tools for Mobile – DNS Tools, Whois, Ultra Tools Mobile vii. Smart Whois viii. eMailTracker Pro ix. Tools for Mobile – Network Scanner, Fing – Network Tool, Network Discovery Tool, Port Droid Tool			
	B. Scan the network using the following tools:			
	i. Hping2 / Hping3 ii. Advanced IP Scanner i ii. Angry IP Scanner iv. Masscan v. NEET vi. CurrPorts vii. Colasoft Packet Builder viii. The Dude			
2	A. Use Proxy Workbench to see the data passing through it and save the data to file.			

	B. Perform Network Discovery using the following tools:			
	i. Solar Wind Network Topology Mapper ii. OpManager iii. Network View iv. LANState Pro			
	C. Use the following censorship circumvention tools:			
	i. Alkasir ii. Tails OS iii. 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			
	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

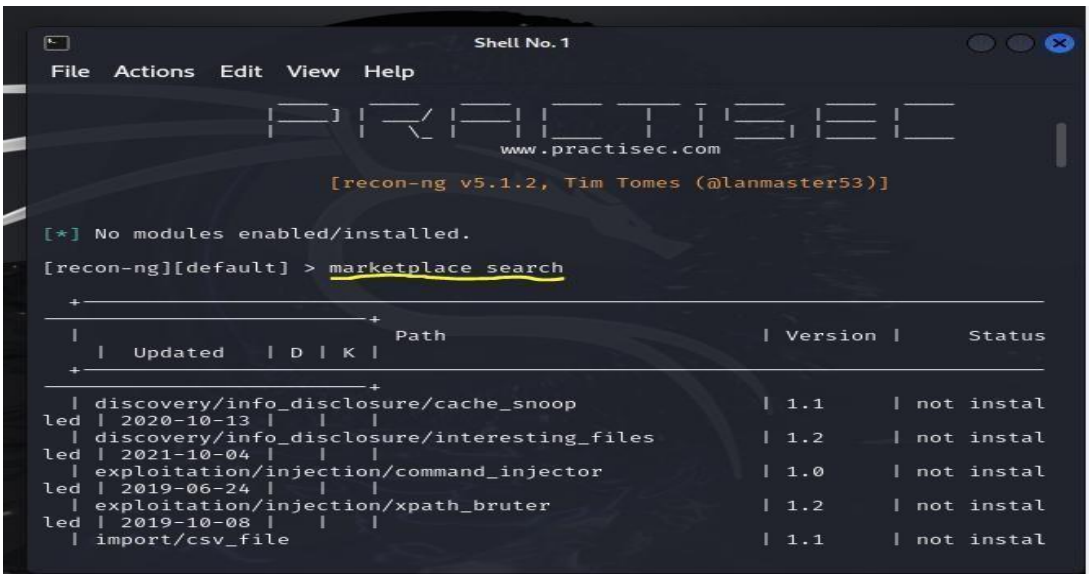
Aim: Use the following tools to perform **footprinting** and **reconnaissance.**

Aim: Recon -ng

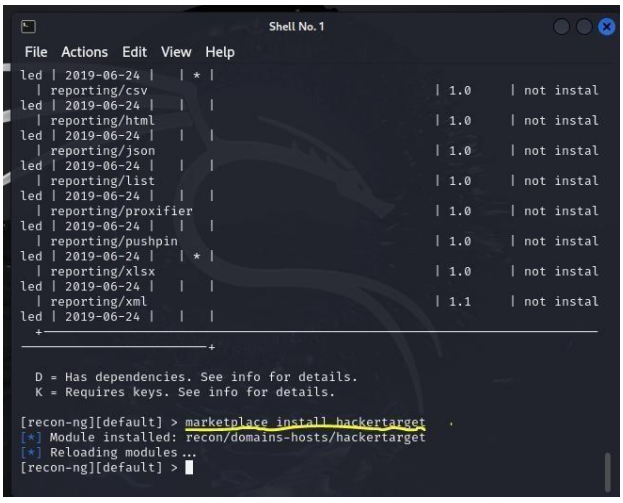
Commands:

1. marketplace search
2. --marketplace search ssl
3. --marketplace info ssltools
4. marketplace install hackertarget
5. modules load hackertarget
6. show options
7. options set SOURCE tesla.com
8. run

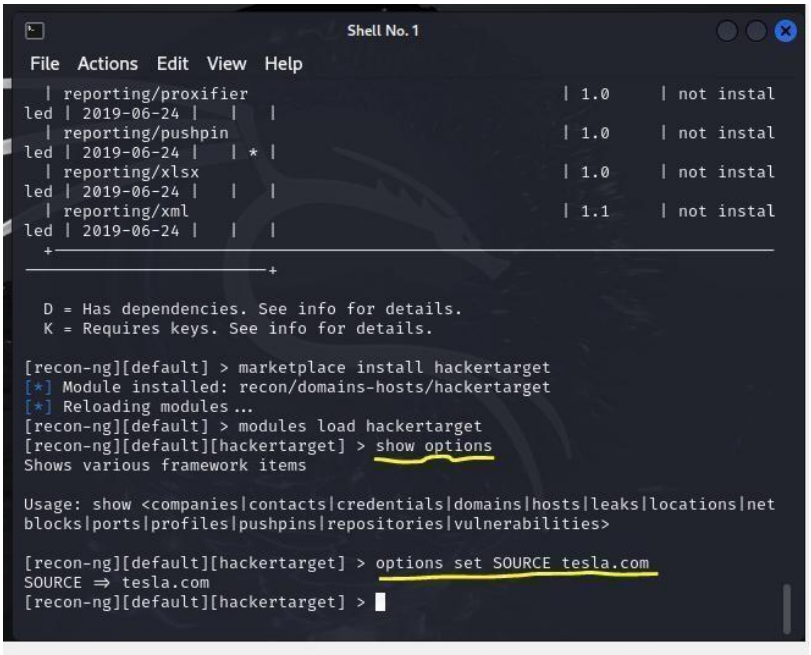
Step 1: Open Recon-ng in the Kali linux, enter below command to search the library. Command "marketplace search"



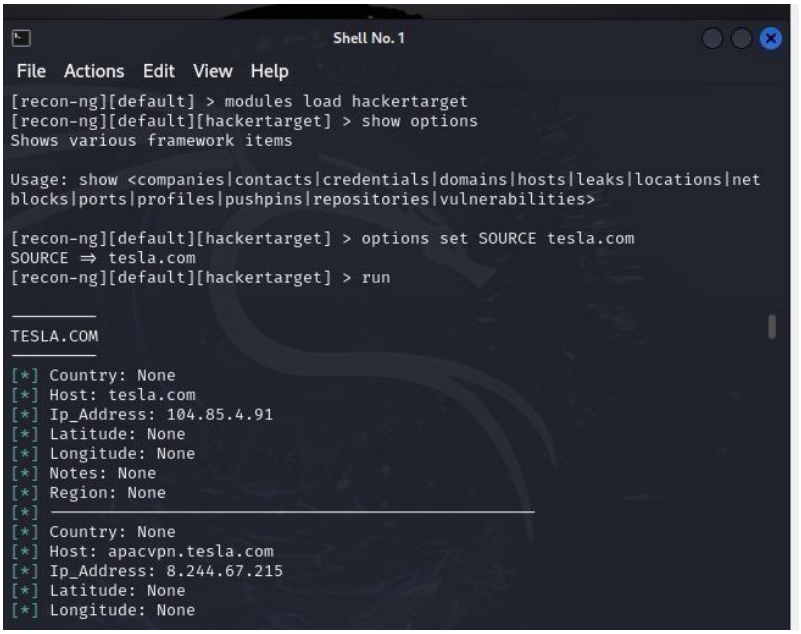
Step2: Use the command to install the package "marketplace install hackertarget"



Step 3 : Now load the package using command "modules load hackertarget" and run next command "options set SOURCE tesla.com" to set the address we desire scan.



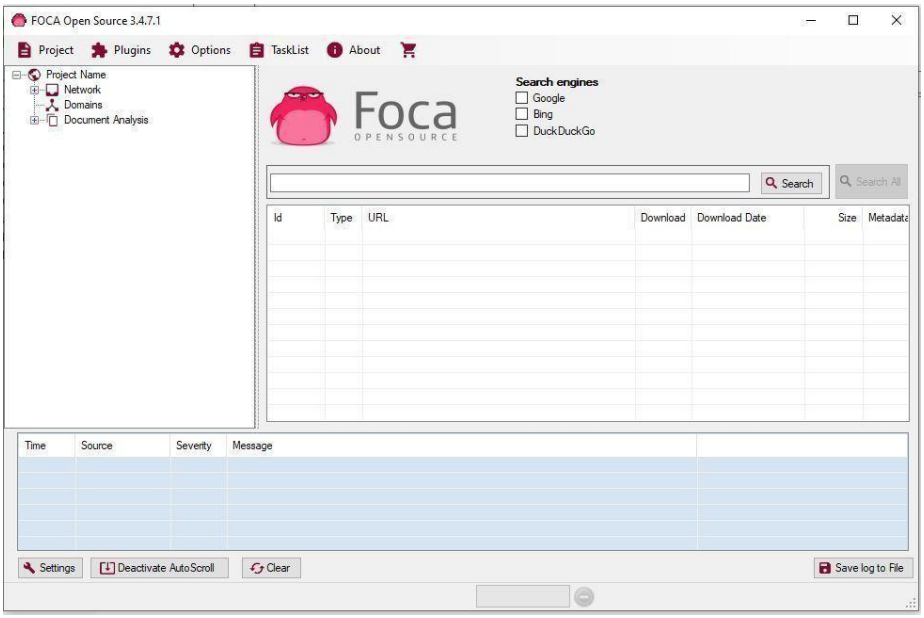
Step 6: Use command run to execute the scan.



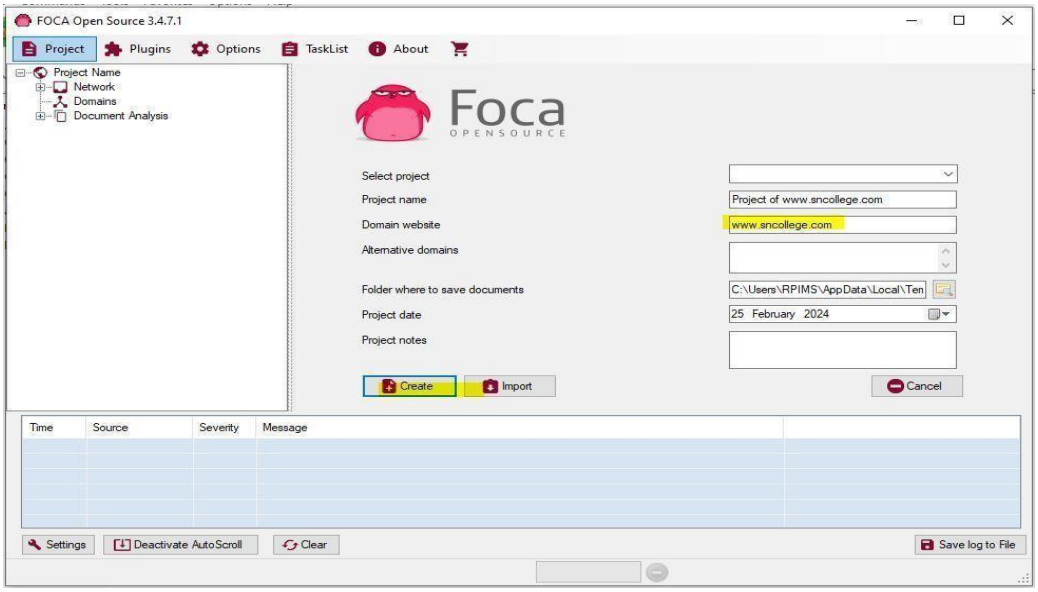
Practical no 2

Aim:- Use of **FOCA Tools**.

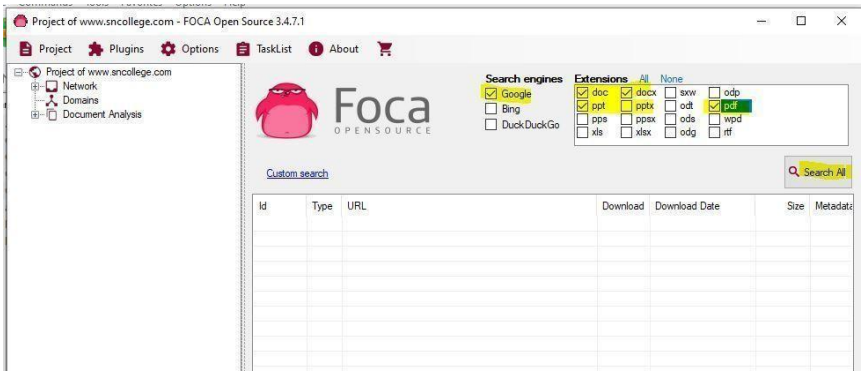
Step 1: Open FOCA Tool, goto project -> select new project.



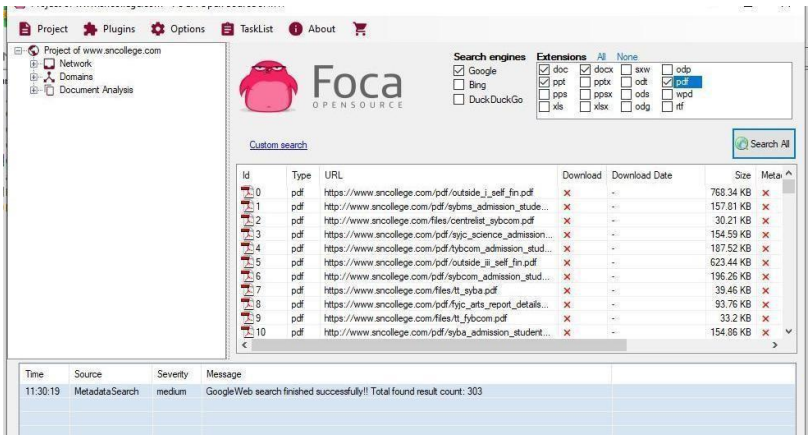
Step 2: Enter the URL then click the "Create" button.



Step 3: Select the search engine and add the extension. Click on the "Search all" button.



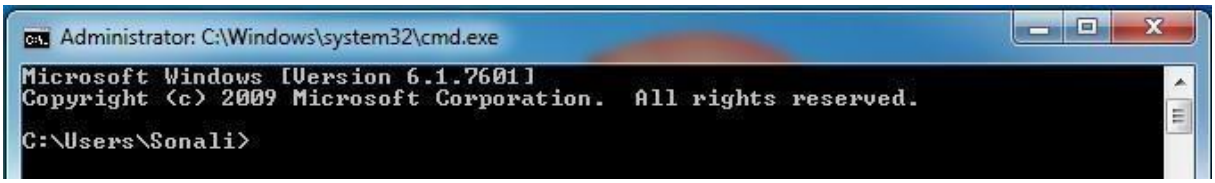
Step 4: You will find the document getting the download.



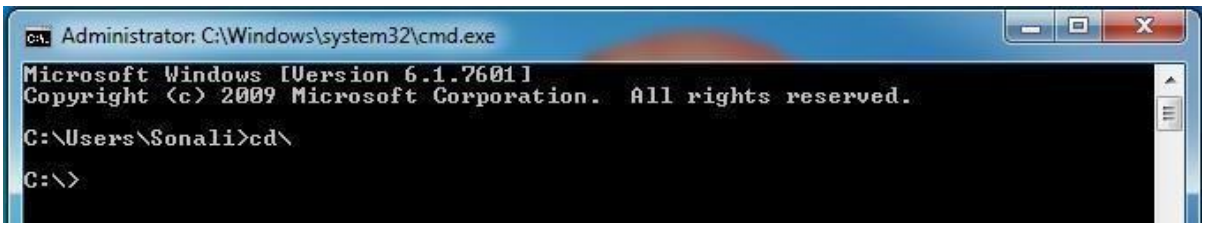
Practical no 3

Aim : USING TRACE ROUTE

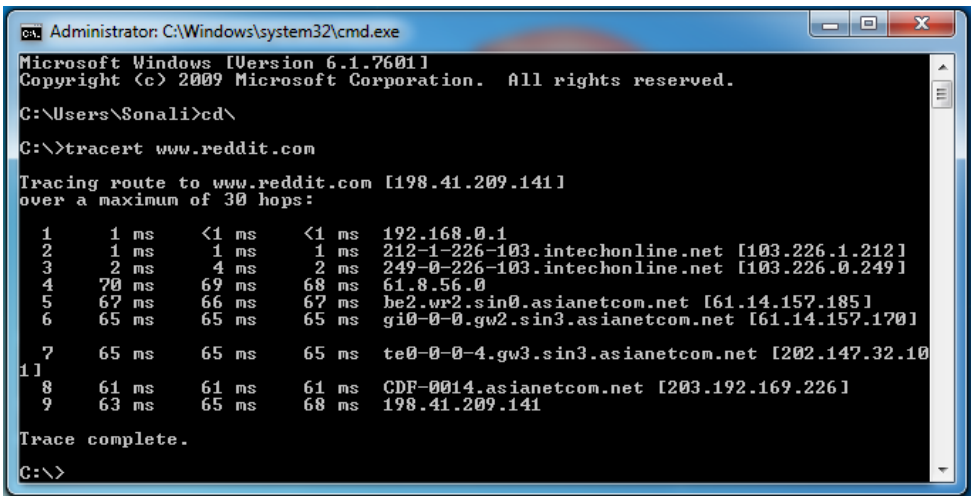
Step 1: Open cmd prompt.



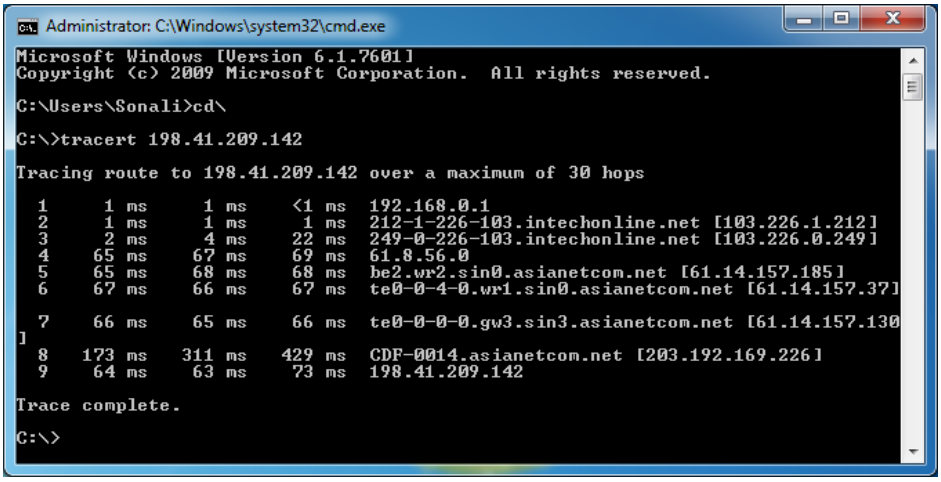
Step 2: Type cd\ and enter it will redirect to "C/directory".



Step 3: Type tracert command and type www.reddit.com and press "Enter".



Step 4: Type tracert command and type ipaddress of reddit.com and press "Enter".



Step 5:
This practical is used to find out the MTU of the destination machine.

- We ping a computer using the 'p
- To specify the data length in bytes we use –lswitch
- To specify that the packet should not be fragmented we use –f
- We now have to adjust the –lvalue till we get a reply. The border where the reply is received is said to be its MTU

```
D:\>ping 192.168.2.1 -l 1478 -f

Pinging 192.168.2.1 with 1478 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

D:\>ping 192.168.2.1 -l 1474 -f

Pinging 192.168.2.1 with 1474 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- Response is received at –l1472, hence the MTU size is 1472 Bytes

```
Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

D:\>ping 192.168.2.1 -l 1472 -f

Pinging 192.168.2.1 with 1472 bytes of data:
Reply from 192.168.2.1: bytes=1472 time<1ms TTL=64
Reply from 192.168.2.1: bytes=1472 time<1ms TTL=64
Reply from 192.168.2.1: bytes=1472 time<1ms TTL=64
Reply from 192.168.2.1: bytes=1472 time<1ms TTL=64

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

TraceRoute using Ping

- We can perform traceroute by using the –n and –Iswitches.
- -n means number of replies to show and –Imeans obtain reply from the machine in the next hop
- Open command prompt
- Ping certifiedhacker.com –n 1 –I1

```
D:\>ping 192.168.2.1 -l 1500 -n 1

Pinging 192.168.2.1 with 1500 bytes of data:
Reply from 192.168.2.1: bytes=1500 time<1ms TTL=64

Ping statistics for 192.168.2.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\>ping 192.168.2.1 -l 1500 -n 1 -f

Pinging 192.168.2.1 with 1500 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 192.168.2.1:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
```

```
D:\>ping certifiedhacker.com -n 1 -i 1

Pinging certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Reply from 192.168.0.1: TTL expired in transit.

Ping statistics for 202.75.54.101:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

- Above, the local router replies back.
- Keep on increasing the I value until the certiedhacker.com site directly replies to the ping.
- At each I value, the device in the route will reply back

```
D:\>ping certifiedhacker.com -n 1 -i 2

Pinging certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Request timed out.

Ping statistics for 202.75.54.101:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

D:\>ping certifiedhacker.com -n 1 -i 3

Pinging certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Request timed out.

Ping statistics for 202.75.54.101:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

D:\>ping certifiedhacker.com -n 1 -i 4

Pinging certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Reply from 121.241.80.6: TTL expired in transit.

Ping statistics for 202.75.54.101:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

- At i=4, reply comes back from 121.241.80.6
- At i=14, the reply comes from the server hosting the certifiedhacker site

```
D:\>ping certifiedhacker.com -n 1 -i 14

Pinging certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Reply from 202.75.54.101: bytes=32 time=155ms TTL=114

Ping statistics for 202.75.54.101:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 155ms, Maximum = 155ms, Average = 155ms
```

Node	IP
1	192.168.0.1
2	219.91.185.1
3	203.187.223.1
4	121.241.80.6
5	172.17.169.202
6	Timed Out
7	180.87.12.53
8	180.87.12.2
9	180.87.112.1
10	116.0.67.174
11	10.55.208.148
12	1.9.244.26
13	Timed Out
14	202.75.54.101 (Destination)

NSLookup

- NSLookup is used to perform DNS Foorprinting by using the windows command **nslookup**
- When we type nslookup, it shows us our current DNS Server

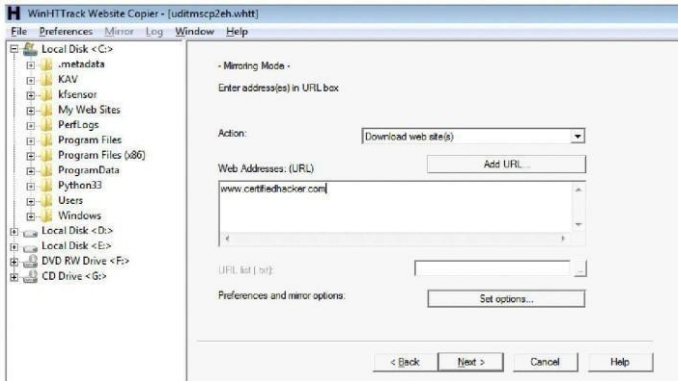
- To specify the DNS query type we want, we use the command
  set type = <recordname> followed by the website name on the next line
  Set type = mx Certifiedhacker.com

- We can set the **query type** as A, ANY, CNAME, MX, NS, PTR, SOA, SRV
  A Record

Aim: HTTrack Website Copier

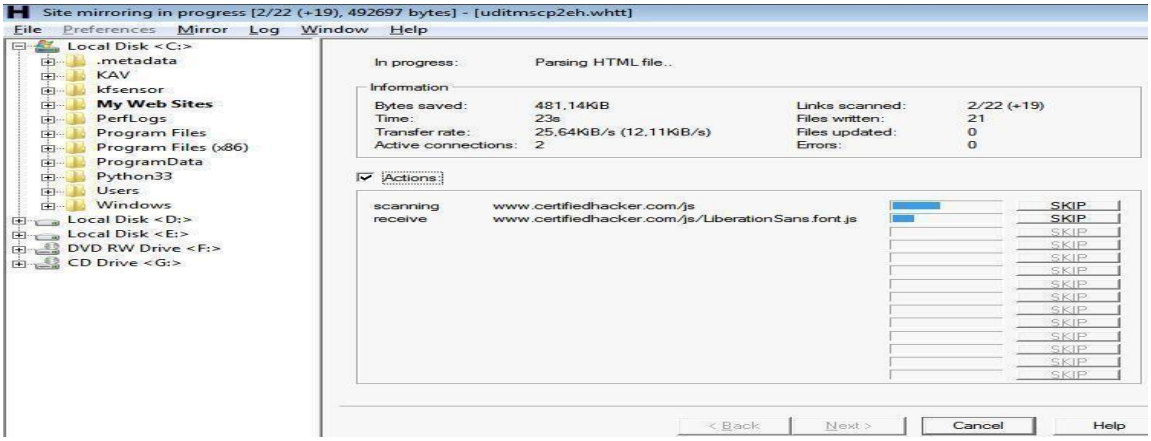
Start > Programs >

- HTTrack Website Copier
- Click on 'Next' to create Project
- Give a name to project Click on 'Next'

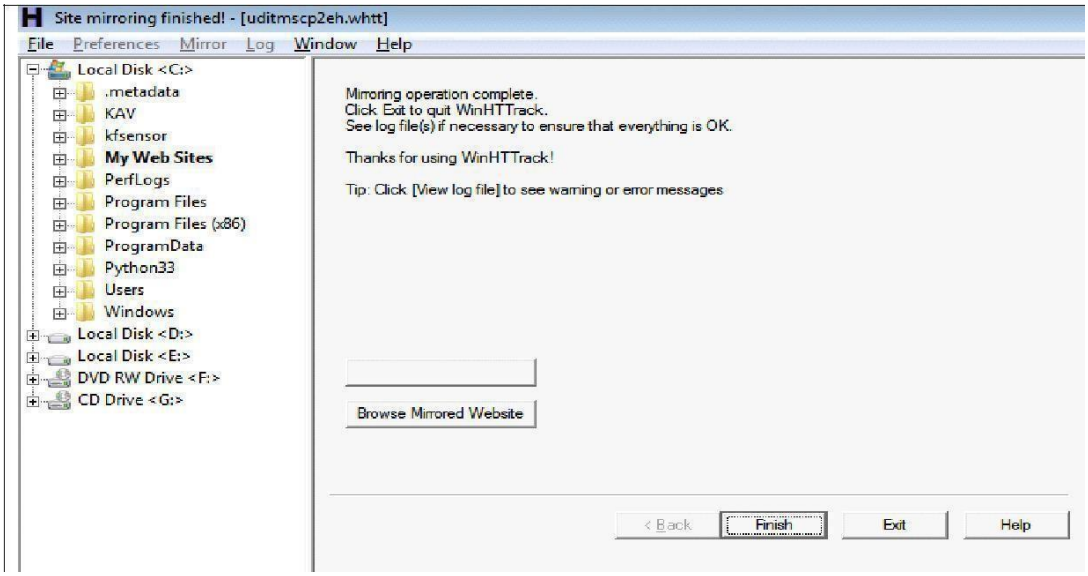


- Click on ‘Add URL’ and give the UR
- Any additional options that need t
- Then click 'Next'
- By default, the radio button will be selected for Please adjust connection parameters if necessary, then press FINISH to launch the mirroring operation.

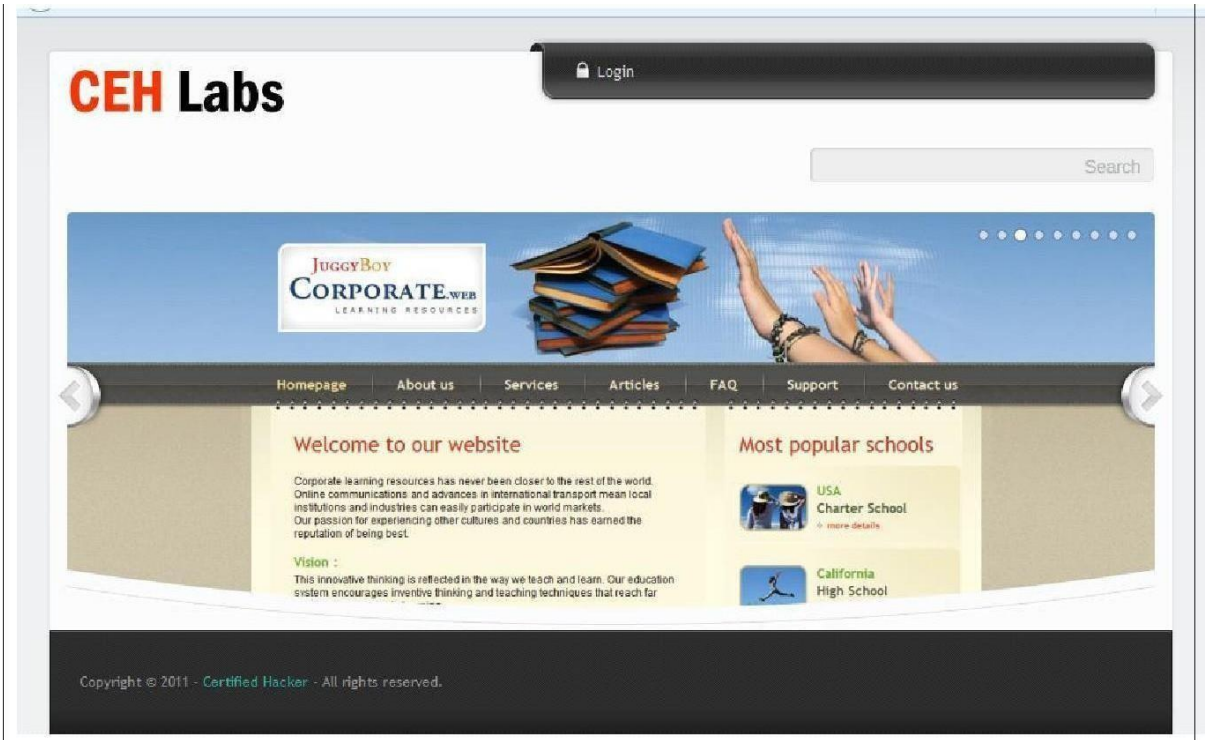
The mirroring of the site now begins. The site will be downloaded and be saved in the C:\My Web Sites\<Project Name>



Process of mirroring the website.

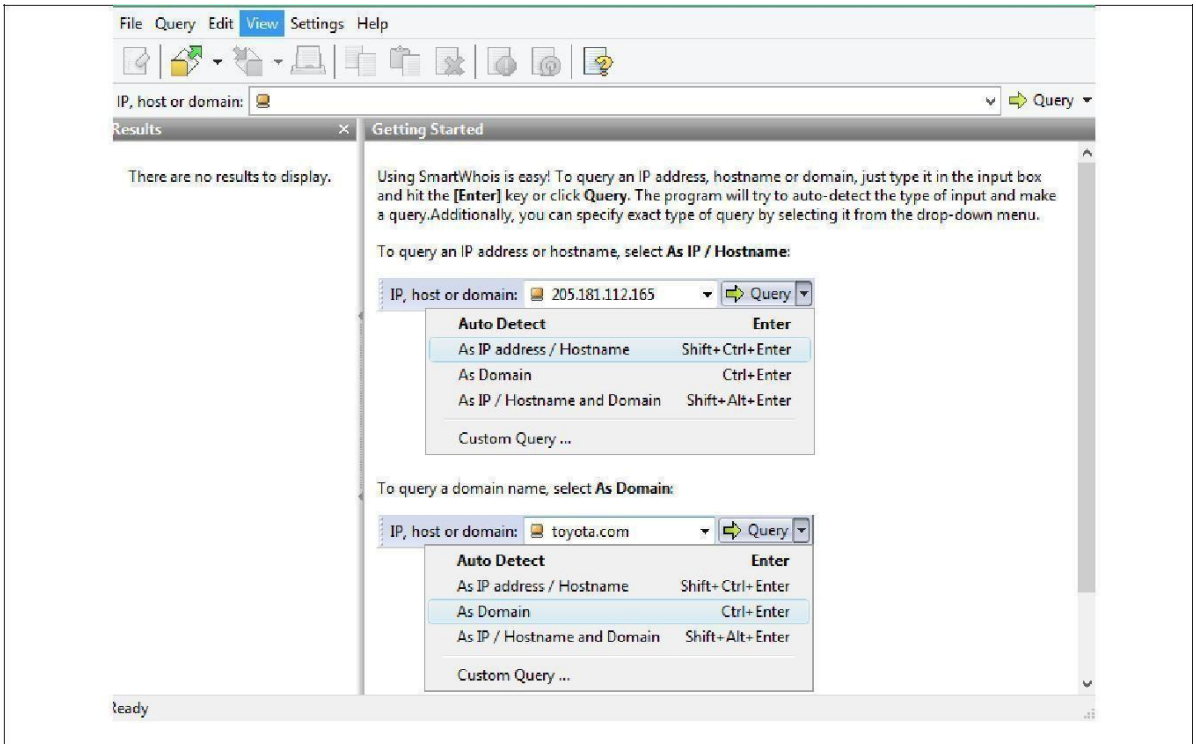


Once the Website Mirroring has been completed, you can click on the Browse Mirrored Website button and then browse the offline copy of the website.

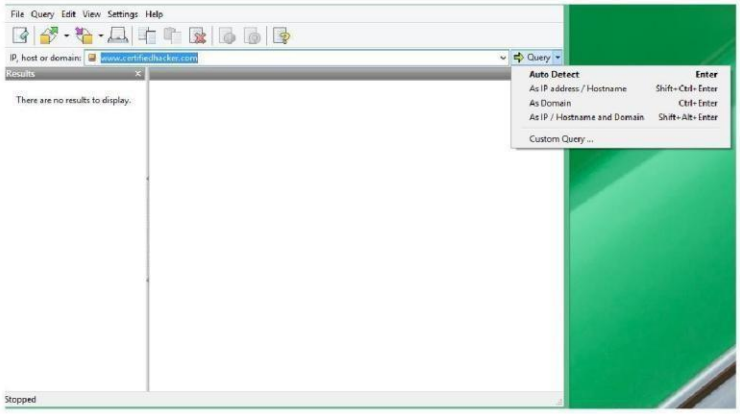


SmartWHOis

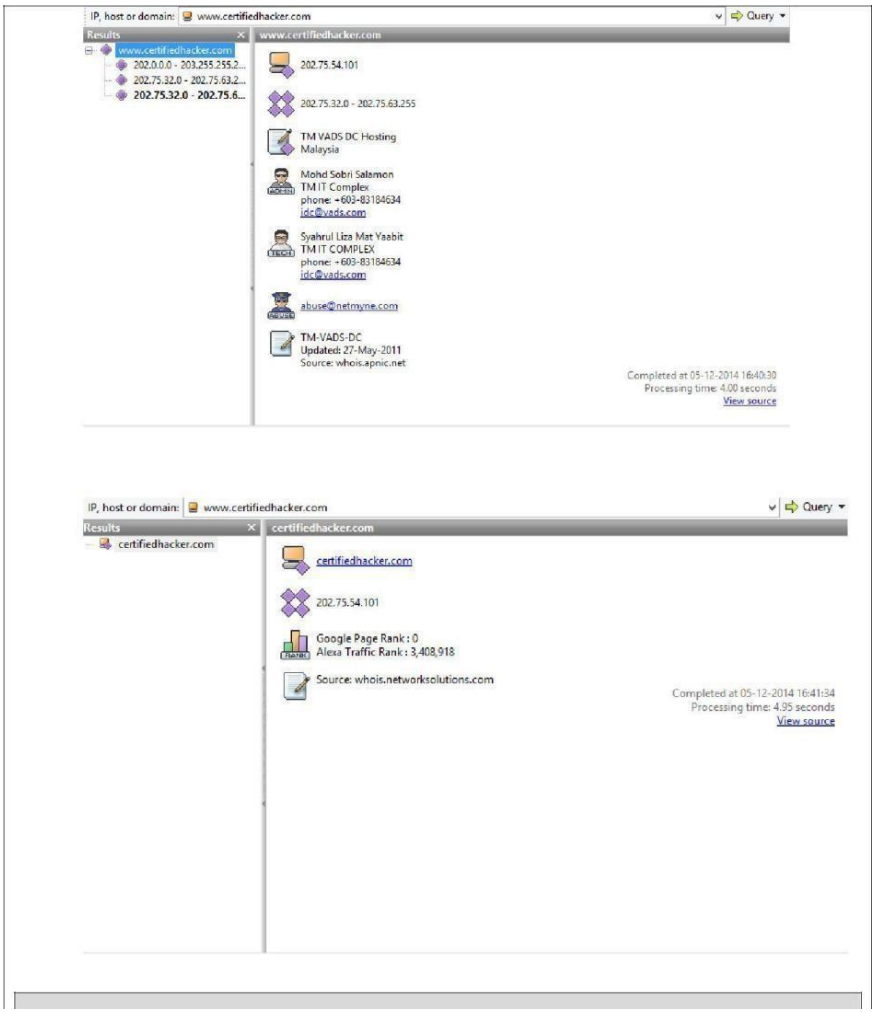
- SmartWHOis is used to perform WHOIS Footprinting against an entered IP Address or a Domain Name
- Run it from, Start > Programs > SmartWhois



Type an IP address, hostname, or domain name in the address bar

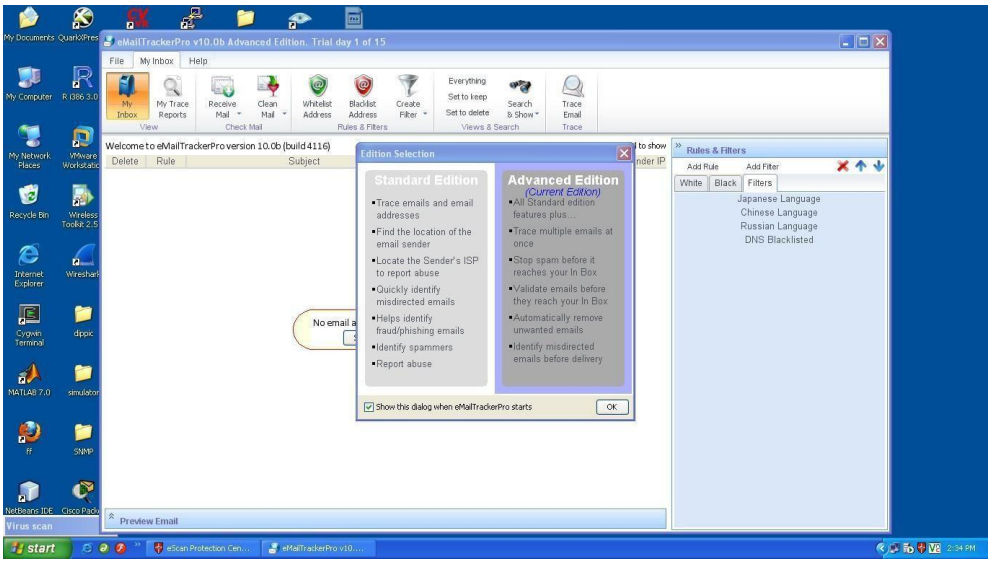


- Different queries will return different results.
- IP Address / Hostname Query results

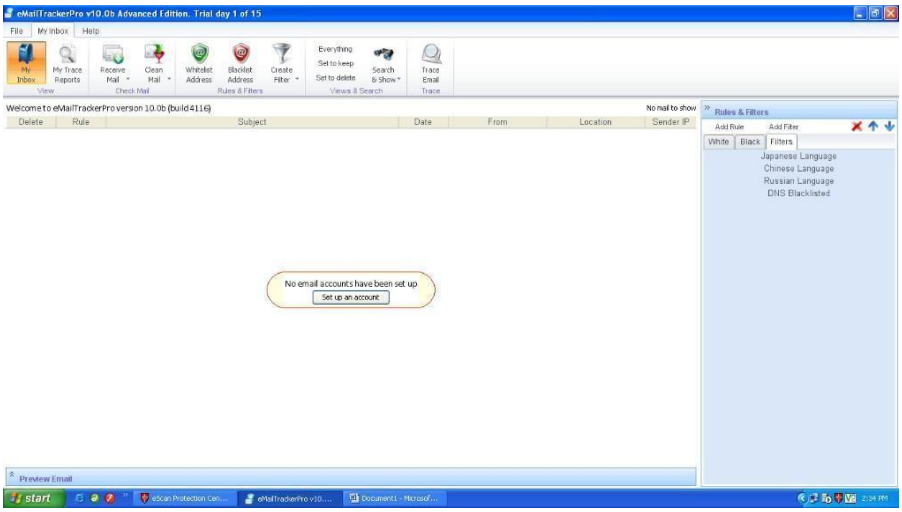


USING EMAIL TRACKER

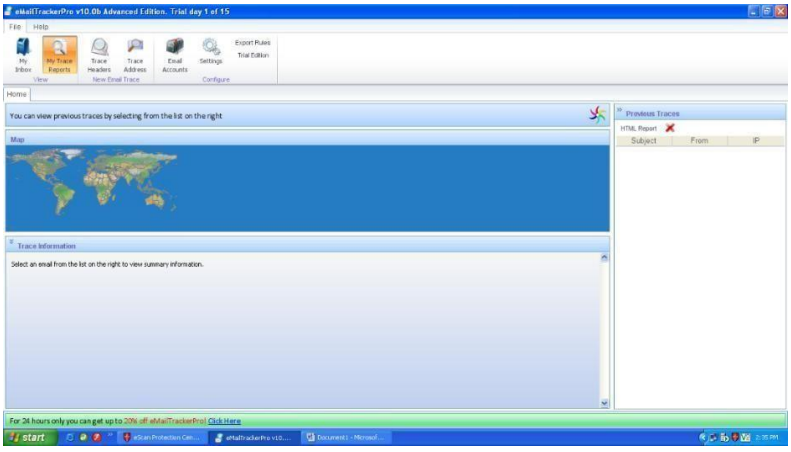
Step 1: Open emailTracker.



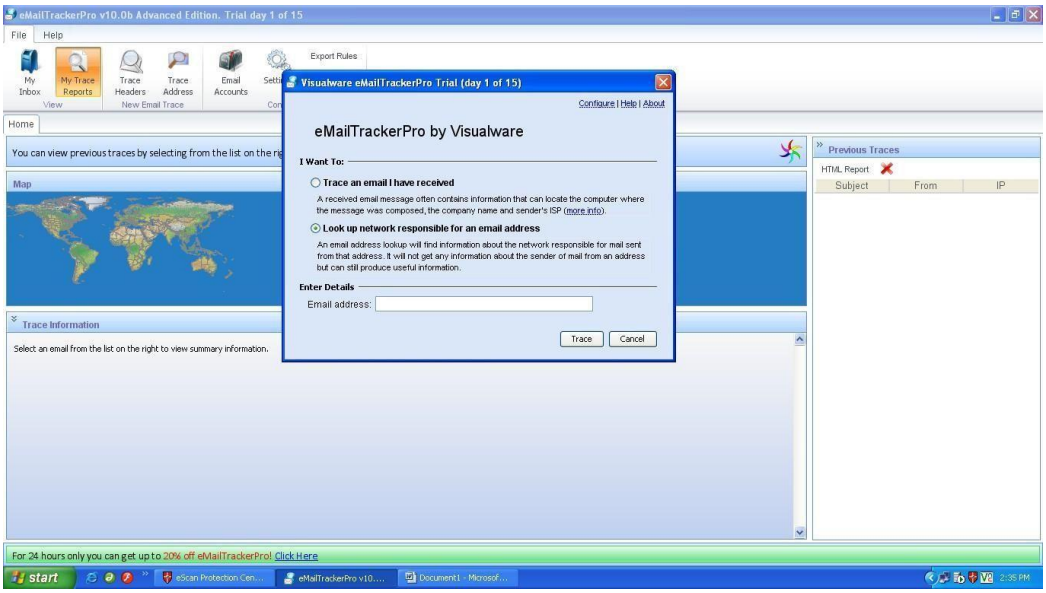
Step 2: Check if there are any reports generated previously.



Step 3: Check for My trace Reports.



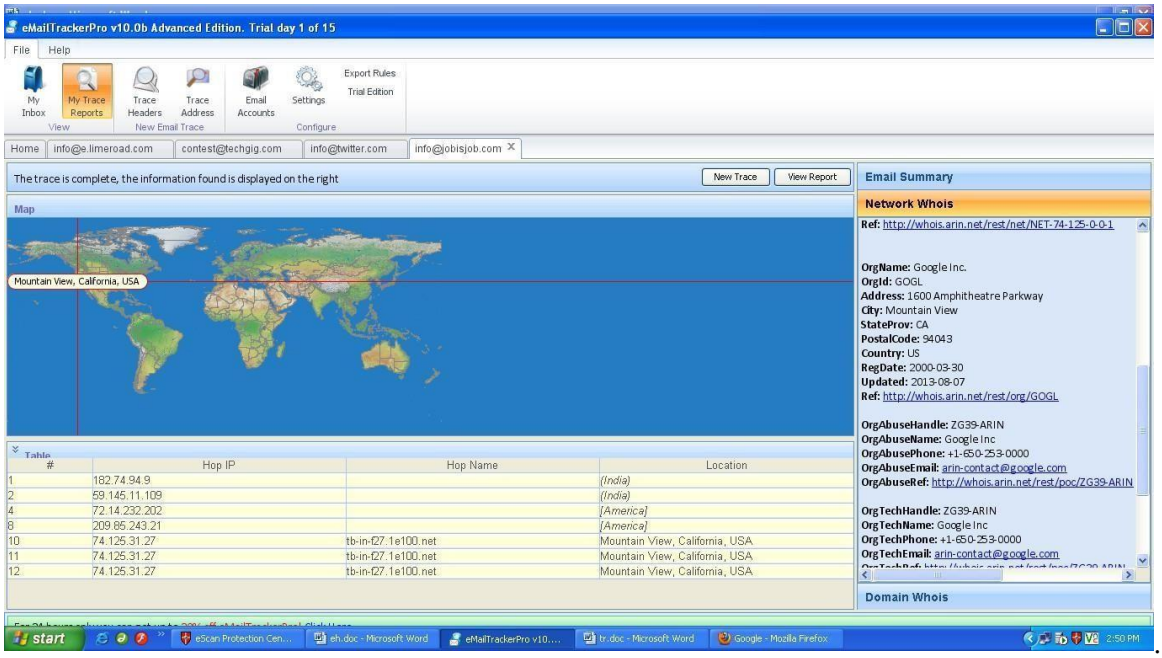
Step 4: Click on Trace address, a new window will open.



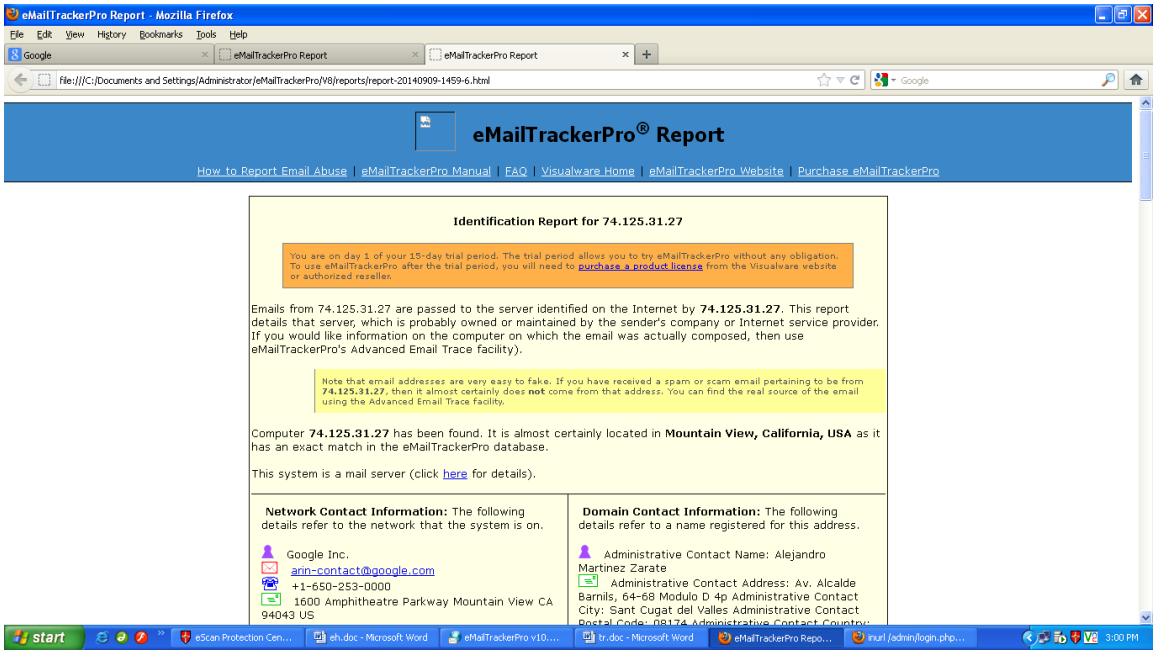
Step 5: Click on second option and enter email address you want to trace and click on trace button.

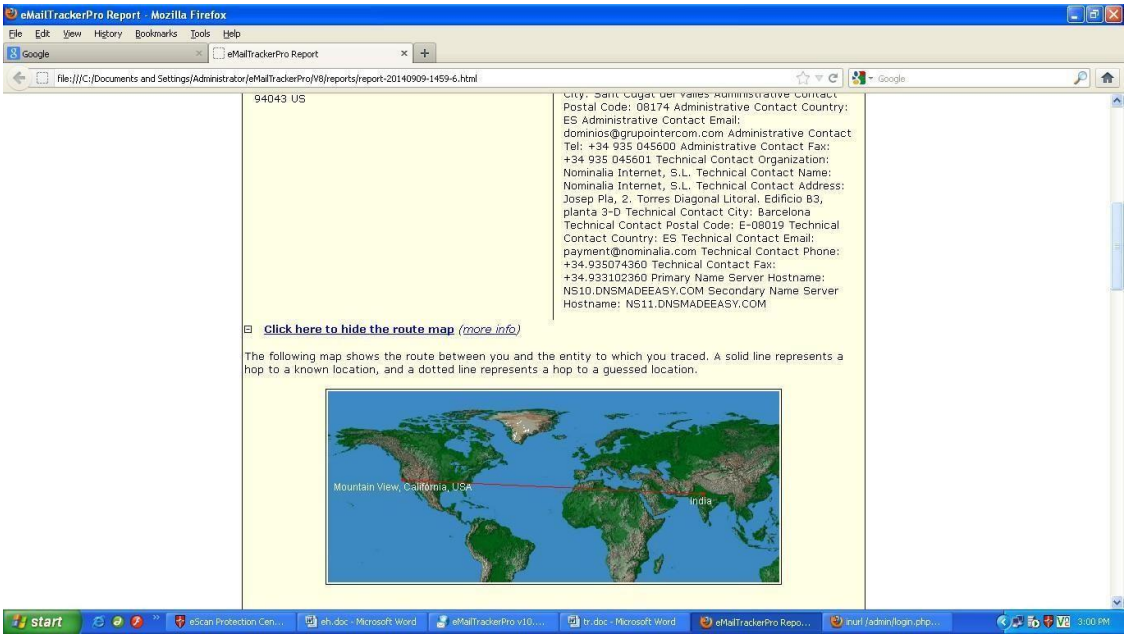
Step 6: The eMailTracker will search for the location and information about the email address entered.

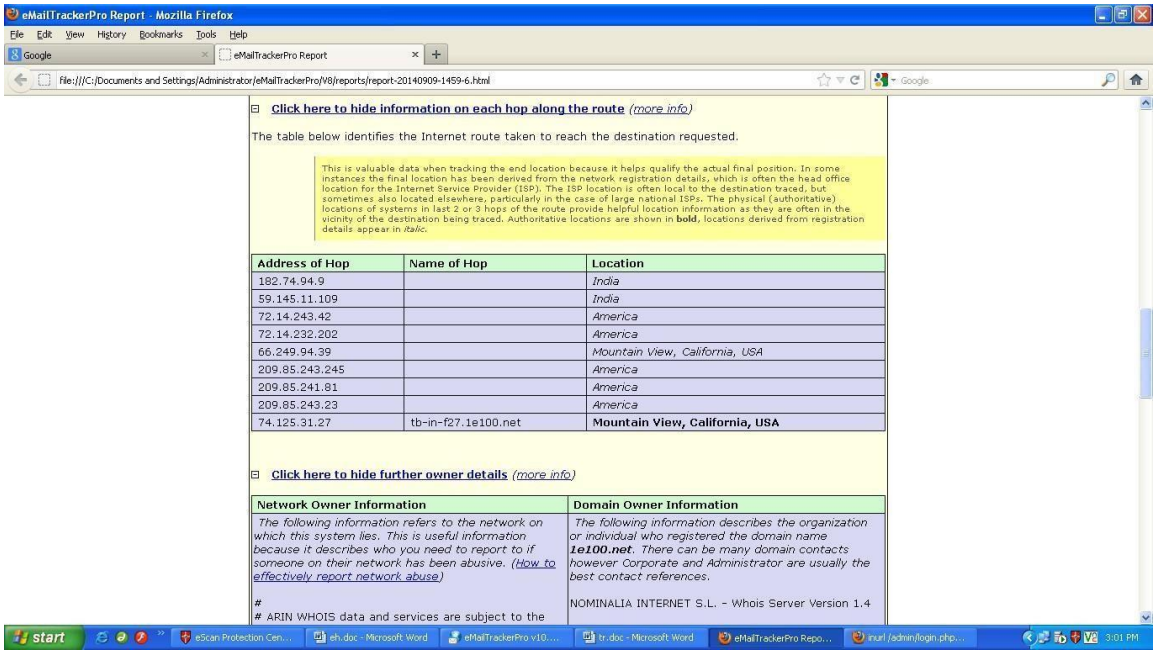
Figure: Location details and email summary.

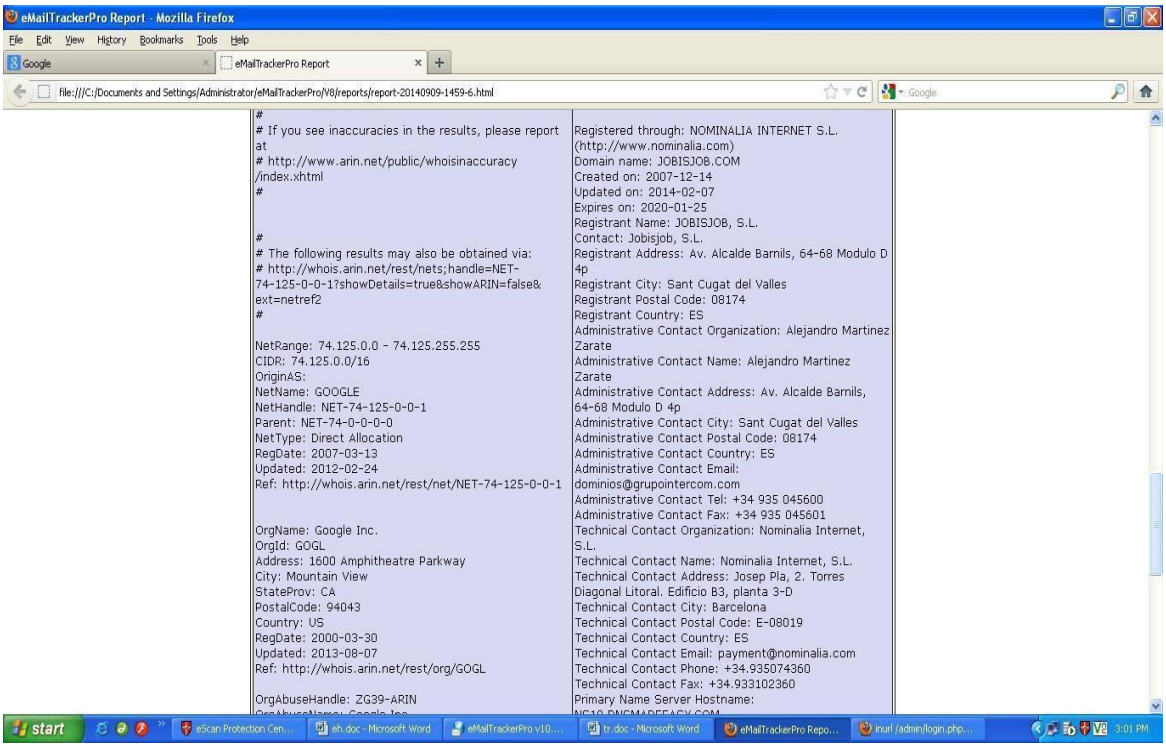


Step 7: Now click on View report and the following report will be generated in browser.


eMailTrackerPro Report - Mozilla Firefox
eMailTrackerPro® Report
How to Report Email Abuse | eMailTrackerPro Manual | FAQ | Visualware Home | eMailTrackerPro Website | Purchase eMailTrackerPro
Identification Report for 74.125.31.27
You are on day 1 of your 15-day trial period. The trial period allows you to try eMailTrackerPro without any obligation. To use eMailTrackerPro after the trial period, you will need to purchase a product license from the Visualware website or authorized reseller.
Emails from 74.125.31.27 are passed to the server identified on the Internet by 74.125.31.27. This report details that server, which is probably owned or maintained by the sender's company or Internet service provider. If you would like information on the computer on which the email was actually composed, then use eMailTrackerPro's Advanced Email Trace facility).
Note that email addresses are very easy to fake. If you have received a spam or scam email pertaining to be from 74.125.31.27, then it almost certainly does not come from that address. You can find the real source of the email using the Advanced Email Trace facility.
Computer 74.125.31.27 has been found. It is almost certainly located in Mountain View, California, USA as it has an exact match in the eMailTrackerPro database.
This system is a mail server (click here for details).
Network Contact Information: The following details refer to the network that the system is on.
Google Inc.
arin-contact@google.com
+1-650-253-0000
1600 Amphitheatre Parkway Mountain View CA 94043 US
Domain Contact Information: The following details refer to a name registered for this address.
Administrative Contact Name: Alejandro Martinez Zarate
Administrative Contact Address: Av. Alcalde Barnils, 64-68 Modulo D 4p Administrative Contact City: Sant Cugat del Valles Administrative Contact
start


eMailTrackerPro Report - Mozilla Firefox
94043 US
Postal Code: 08174 Administrative Contact Country: ES Administrative Contact Email: dominios@grupointercom.com Administrative Contact Tel: +34 935 045600 Administrative Contact Fax: +34 935 045601 Technical Contact Organization: Nominalia Internet, S.L. Technical Contact Name: Nominalia Internet, S.L. Technical Contact Address: Josep Pla, 2. Torres Diagonal Litoral. Edificio B3, planta 3-D Technical Contact City: Barcelona Technical Contact Postal Code: E-08019 Technical Contact Country: ES Technical Contact Email: payment@nominalia.com Technical Contact Phone: +34.935074360 Technical Contact Fax: +34.933102360 Primary Name Server Hostname: NS10.DNSMADEEASY.COM Secondary Name Server Hostname: NS11.DNSMADEEASY.COM
Click here to hide the route map (more info)
The following map shows the route between you and the entity to which you traced. A solid line represents a hop to a known location, and a dotted line represents a hop to a guessed location.
Mountain View, California, USA
India
start





Scan the network using the following tools:

i. Hping2 / Hping3

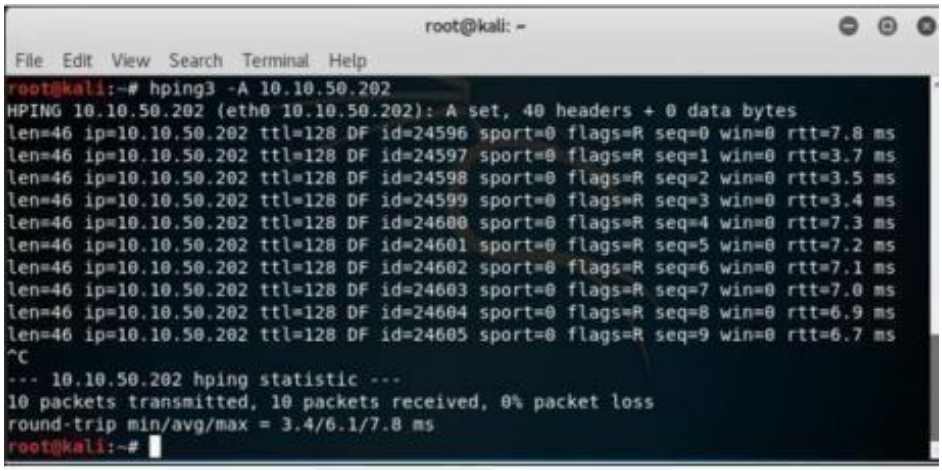
Hping is a command-line TCP/IP packet assembler and analyzer tool that is used to send customized TCP/IP packets and display the target reply as ping command display the ICMP Echo Reply packet from targeted host. Hping can also handle fragmentation, arbitrary packetsbody, and size and file transfer.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

- Test firewall rules.

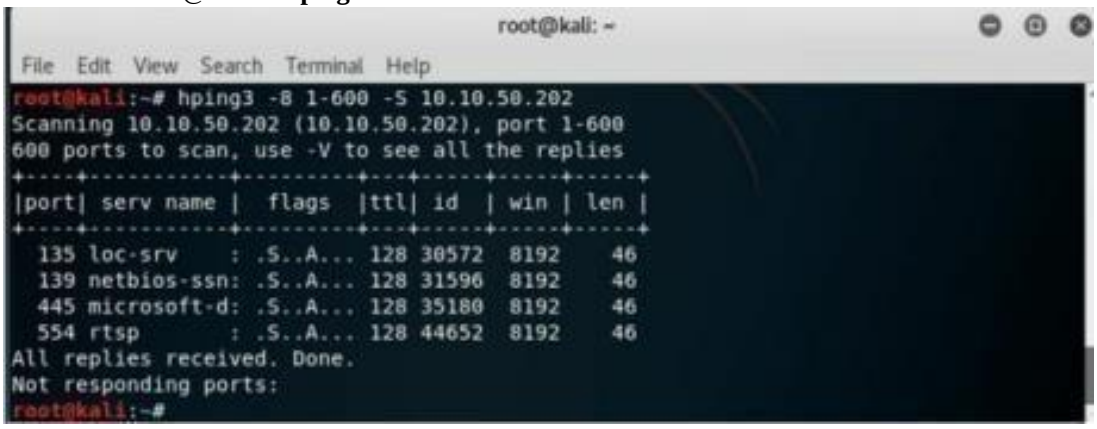
- Advanced port scanning.
- Testing net performance.
- Path MTU discovery.
- Transferring files between even fascist firewall rules.
- Traceroute-like under different protocols.
- Remote OS fingerprinting & others

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

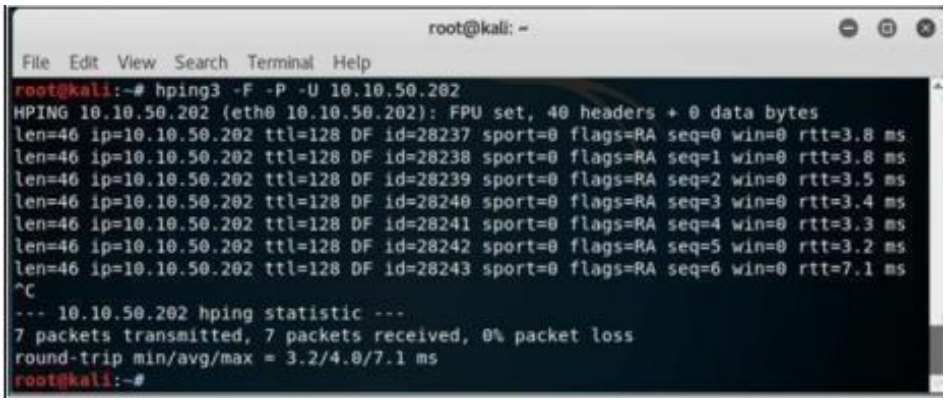
- To create an ACK packet: root@kali:~#
  hping3 –A 192.168.0.1



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

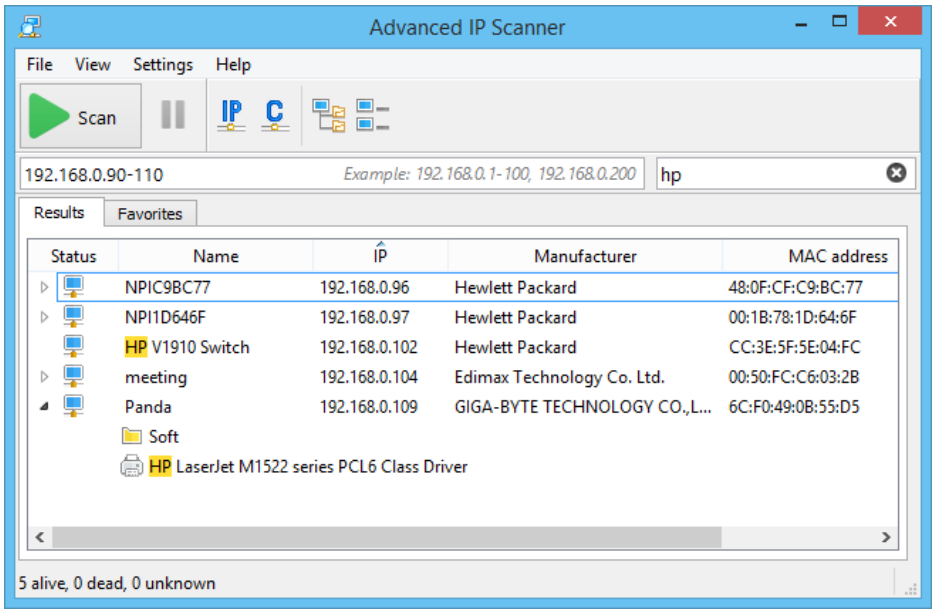


To create a packet with FIN, URG, and PSH flags setsroot@kali:~# **hping3 –F –P -U 10.10.50.202**



ii. Advanced IP Scanner

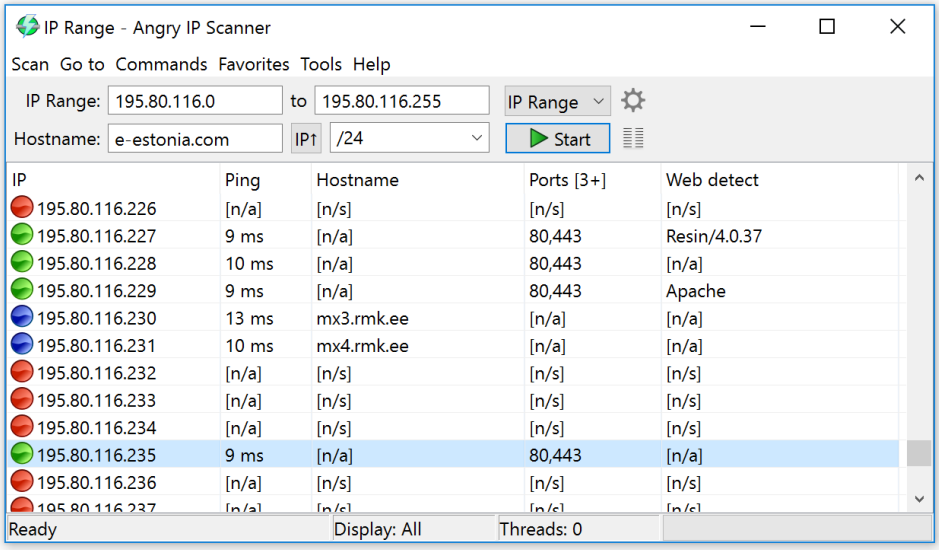
Advanced IP Scanner is **a fast and powerful network scanner with a user-friendly interface**.In seconds, Advanced IP Scanner can locate all computers on your wired or wireless local network and scan their ports. The program provides easy access to various network resources such as HTTP, HTTPS, FTP,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



i. 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 otherfeatures.

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



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

III. Masscan

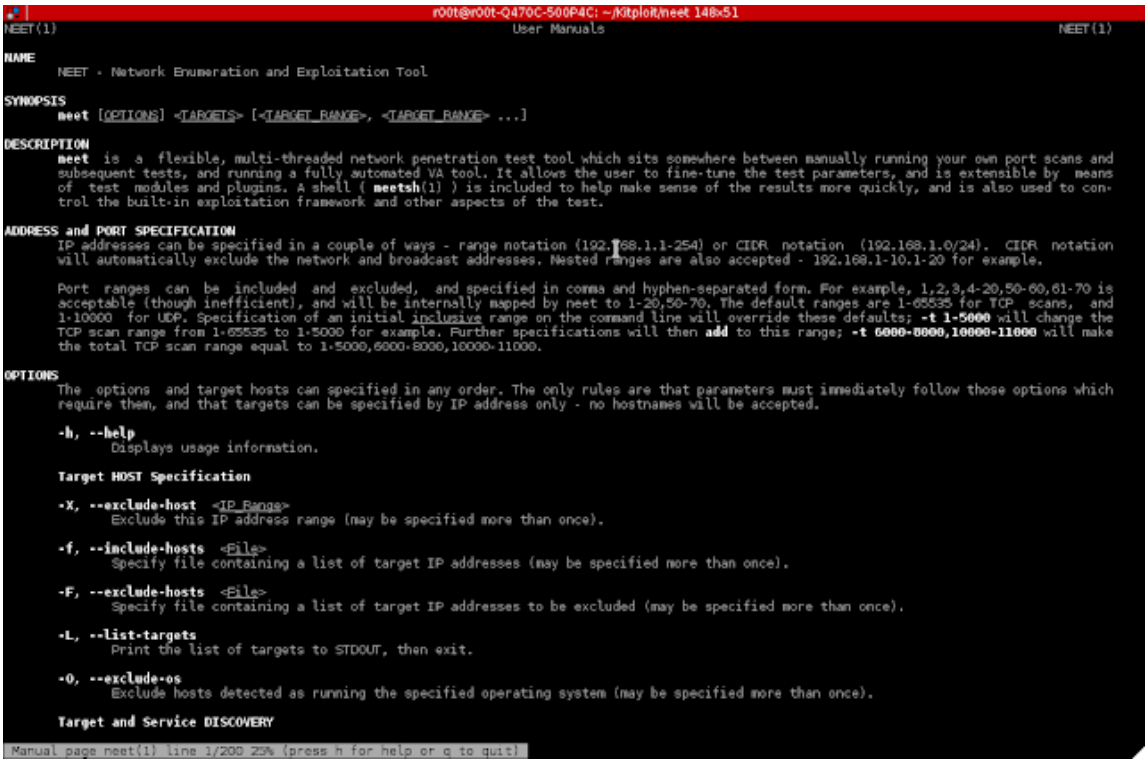
MASSCAN is **TCP port scanner which transmits SYN packets asynchronously and produces results similar to nmap, the most famous port scanner**. Internally, it operates morelike scanrand, unicornscan, and ZMap, using asynchronous transmission. It's a flexible utility that allows arbitrary address and port 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-ethInitiating 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 192.168.1.220Discovered open port 80/tcp on
192.168.1.230

i.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 muchnetwork information as possible in clear, easy-to-use formats. The core scanning engine finds andidentifies 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 allowthe user to tune the test parameters for network scanning in the most efficient and practical way.



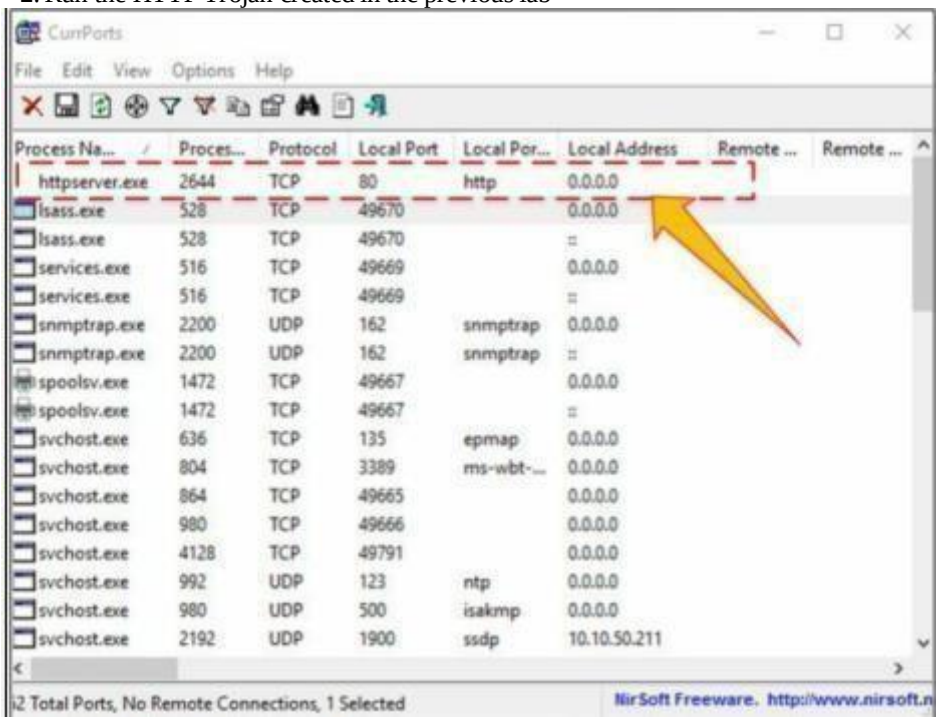
CurrPorts

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 detectand kill the connection.

Topology:

Configuration:

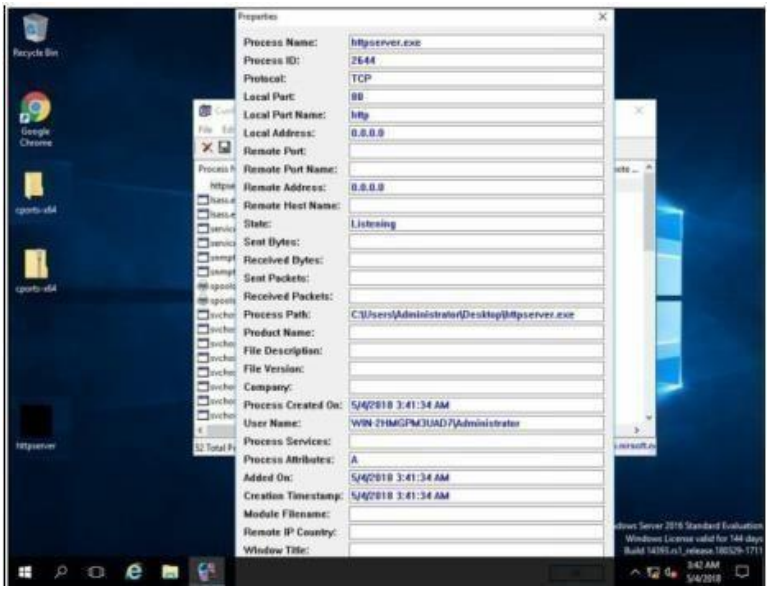
1. Run the application **Currports** on Windows Server 2016 and observe theprocesses.
2. Run the HTTP Trojan created in the previous lab



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

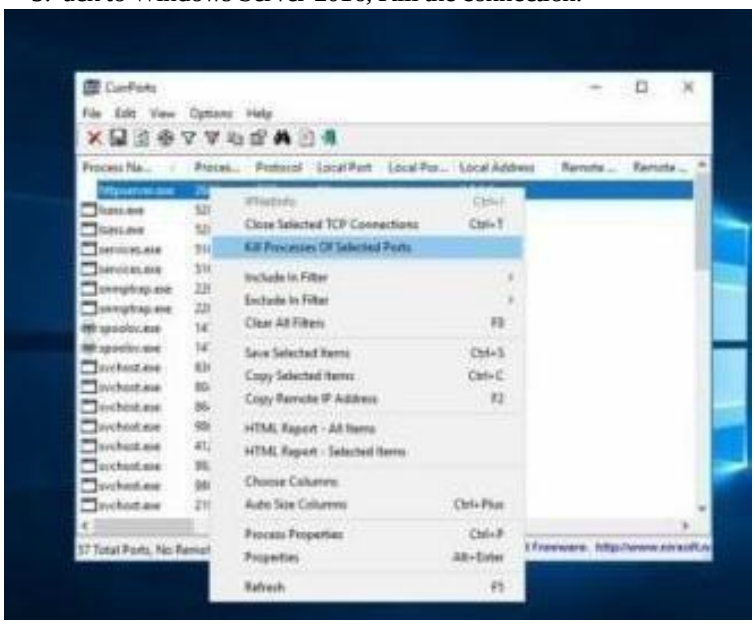


Properties are showing more details about tcp connection.

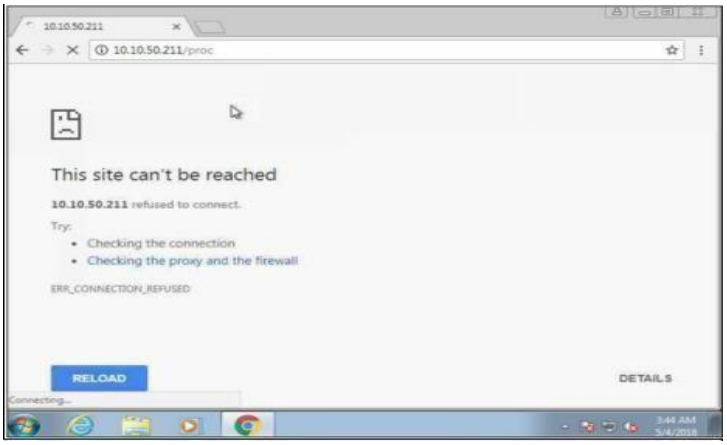
4. Go to Windows 7 machine and initiate the connection as mentioned in the previous lab using aweb browser.

Connection successfully established.

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



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



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

Available options are: -

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

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

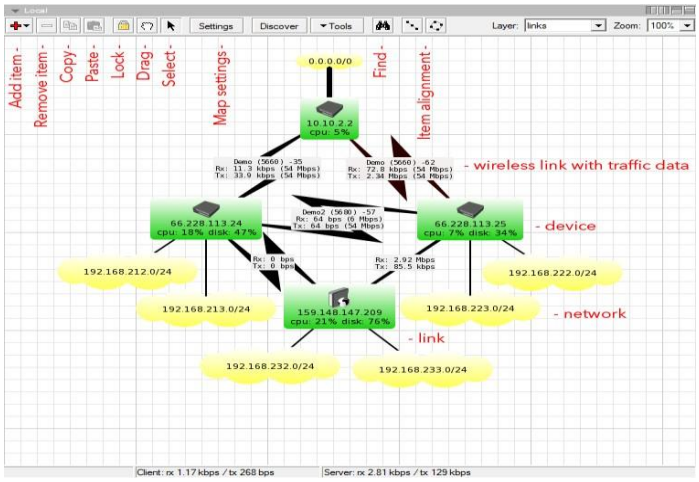
ii. The Dude

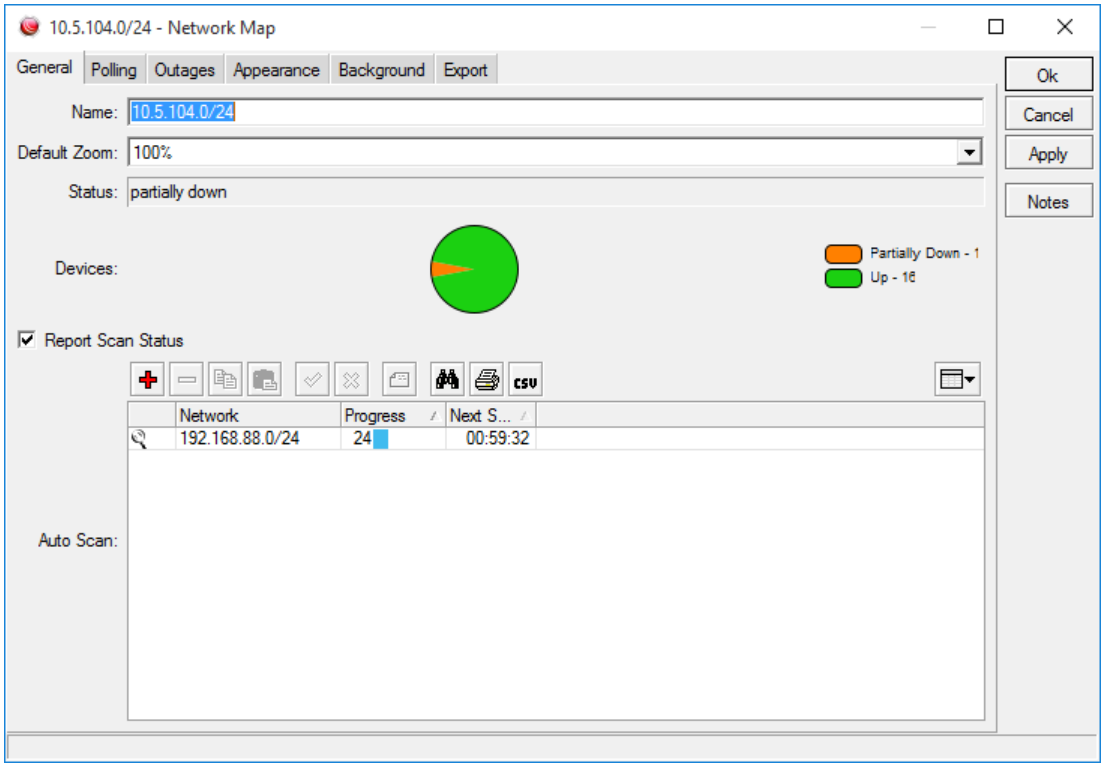
The Dude network monitor is a new application by MikroTik which can dramatically improve the way you manage your network environment. It will automatically scan all devices within specified subnets, draw and layout a map of your networks, monitor services of your devices andalert you in case some service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

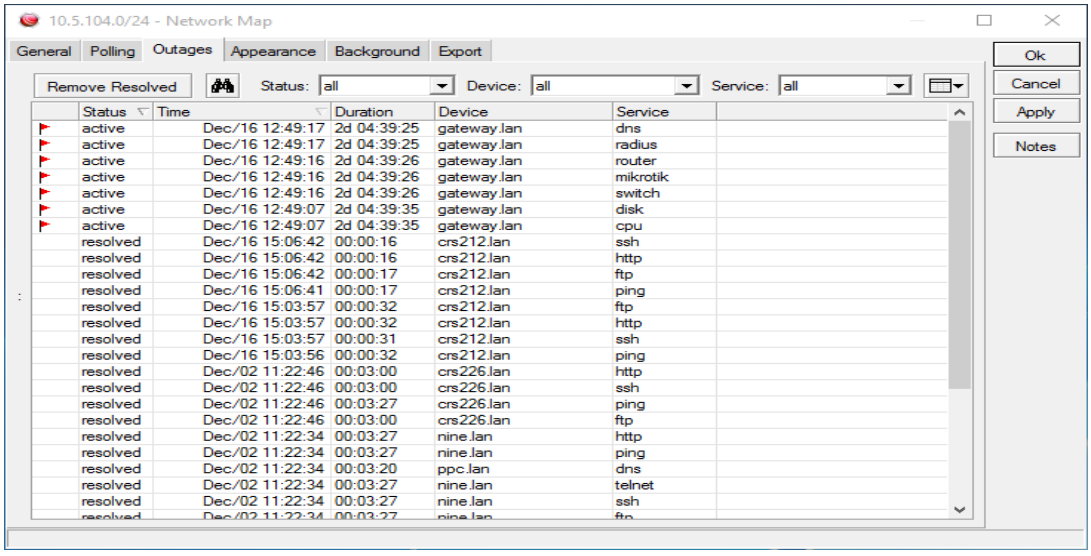
Main Features:

- 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





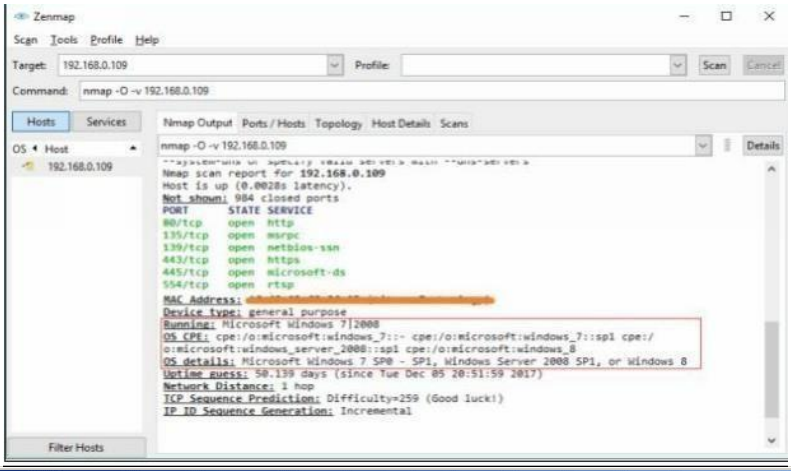


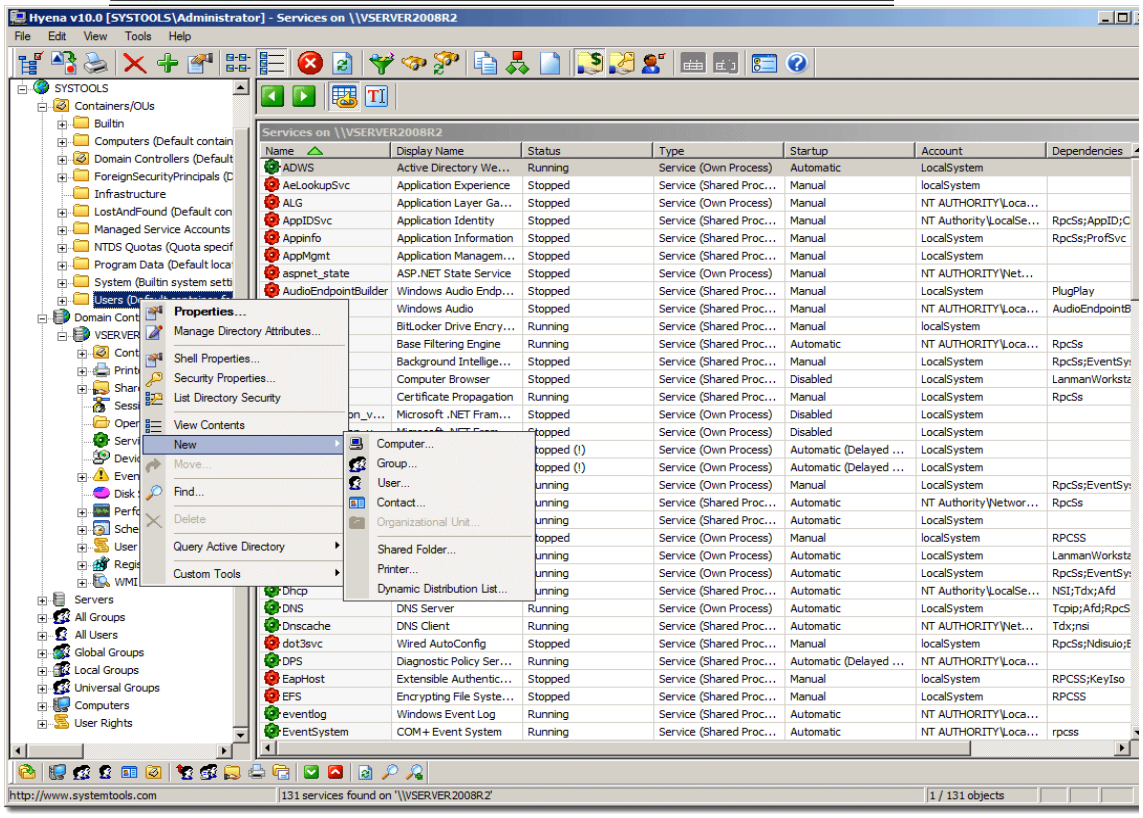
Perform Enumeration using the following tools:

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 someclues regarding nature of an operating system disclosing the type an OS. To perform OS detection with nmap perform the following: nmap -O<ip address>

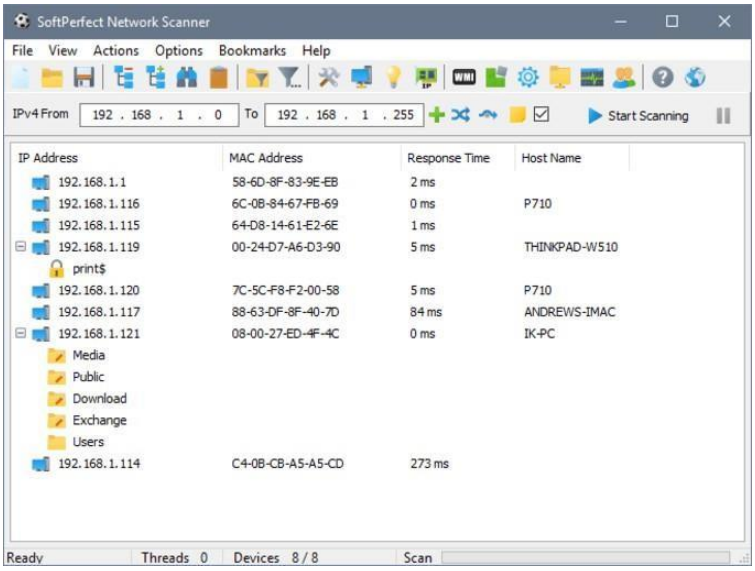
```
┌──(ritik㉿ritik)-[~]
└─$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 ritik:45204             del12s05-in-f4.1e:https ESTABLISHED
tcp        0      0 ritik:49222             server-13-224-20-:https 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
```





i. 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, S

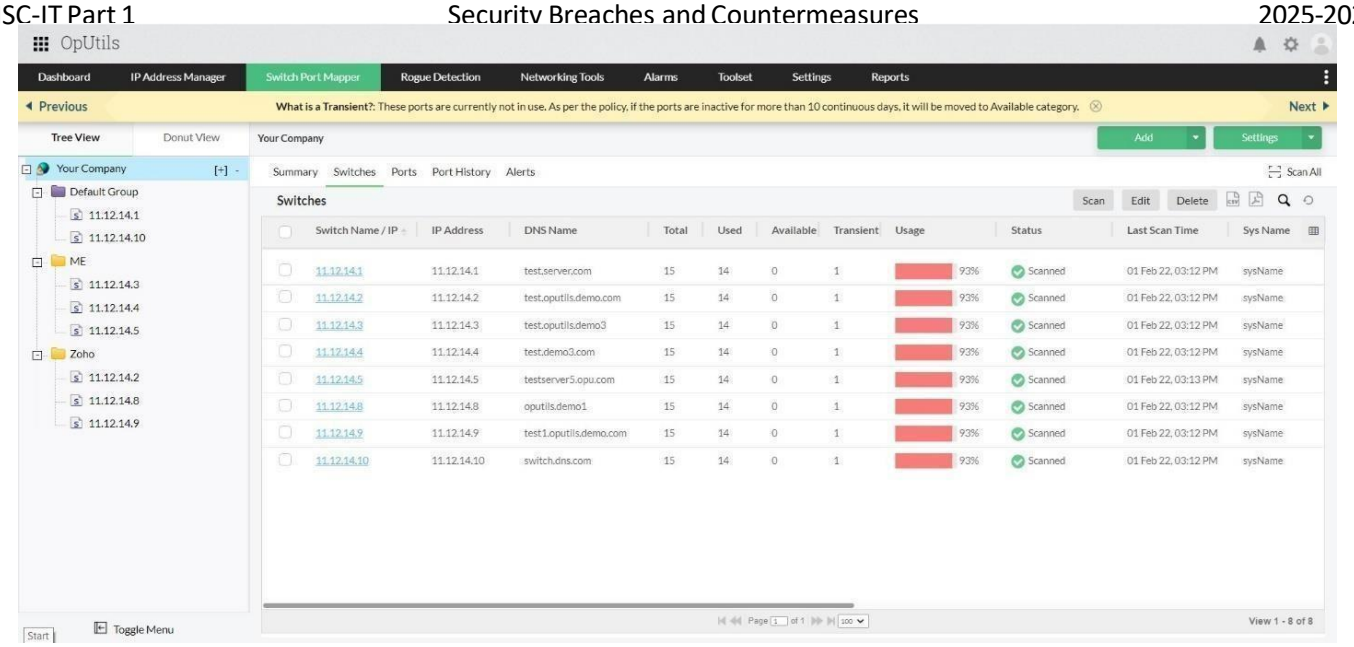


MP, HTTP, SSH andPowerShell.

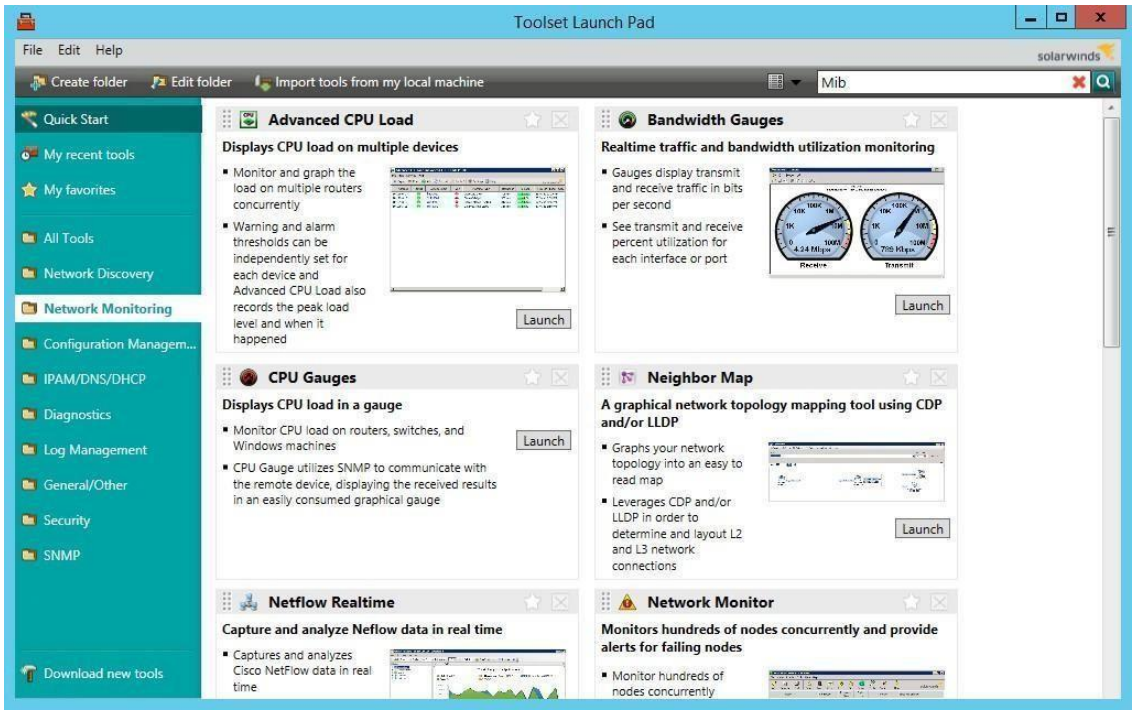
ii. OpUtils

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

i. 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 bandwidthmeasurements.



ii. 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 namedEthereal, the project was renamed Wireshark in May 2006 due to trademark issues

SECTION 2

Perform the vulnerability analysis using the following tools:

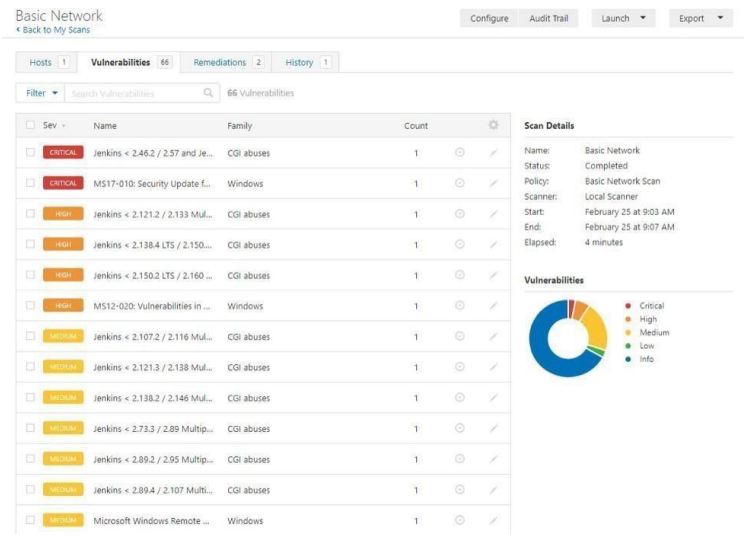
i. Nessus

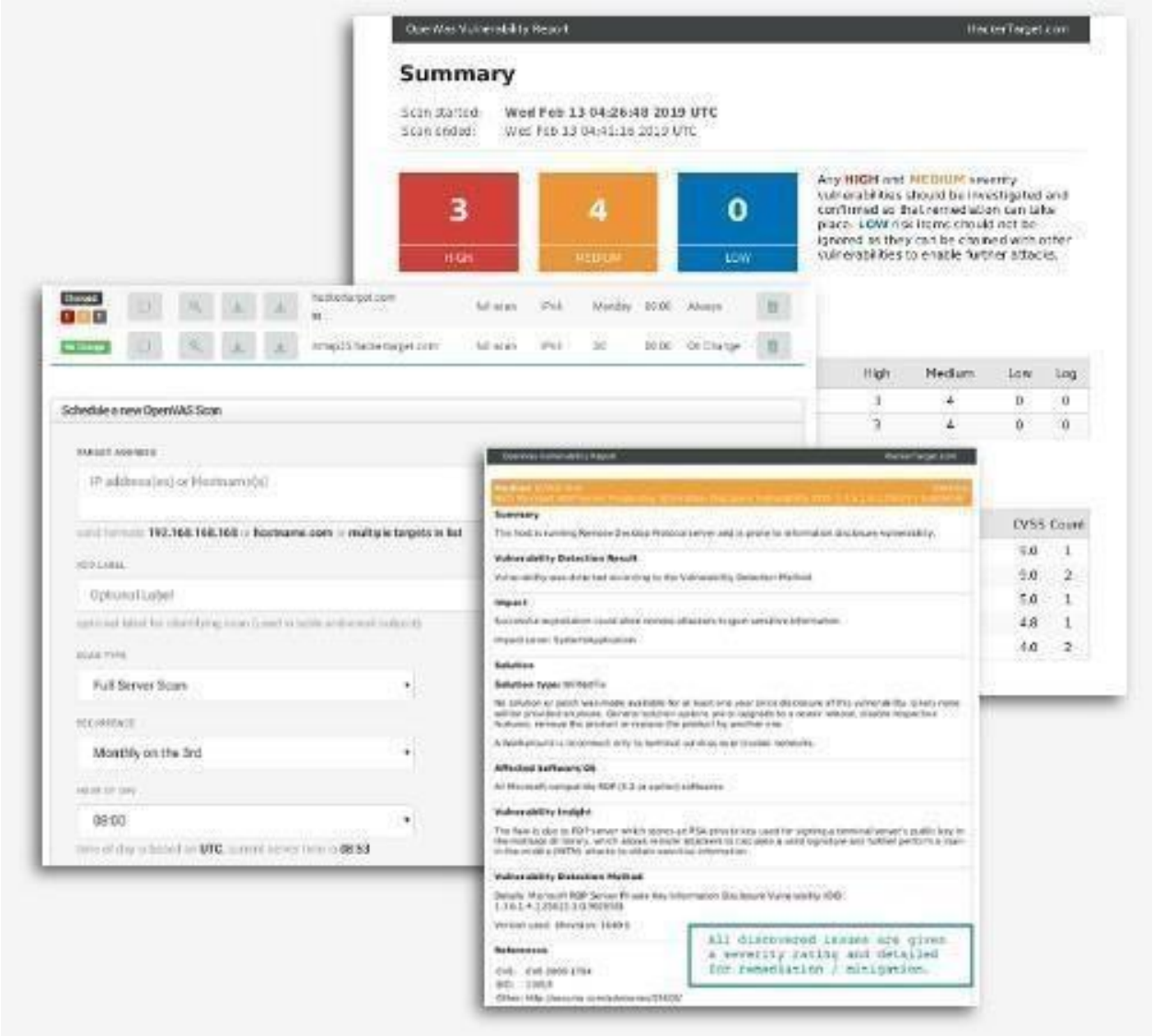
Nessus is a proprietary vulnerability scanner developed by Tenable, Inc. Tenable.io is a subscription-based service. Tenable also contains what was previously known as Nessus Cloud,which used to be Tenable's Software-as-a-Service solution. Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easycross-linking between compliant security tools. In fact, Nessus is one of the many vulnerabilityscanners 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.

OpenVas

OpenVAS is a full-featured vulnerability scanner. Its capabilities include unauthenticated andauthenticated 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 anddaily 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 EnterpriseAppliance, 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
4
0
High
Medium
Low
Any HIGH and MEDIUM severity vulnerabilities should be investigated and confirmed so that remediation can take place. LOW risk items should not be ignored as they can be chained with other vulnerabilities to enable further attacks.
Schedule a new OpenVAS Scan
IP address(es) or Hostname(s)
Optional Label
Full Server Scan
Monthly on the 3rd
09:00
All discovered issues are given a severity rating and detailed for remediation / mitigation.

Practical No. 4

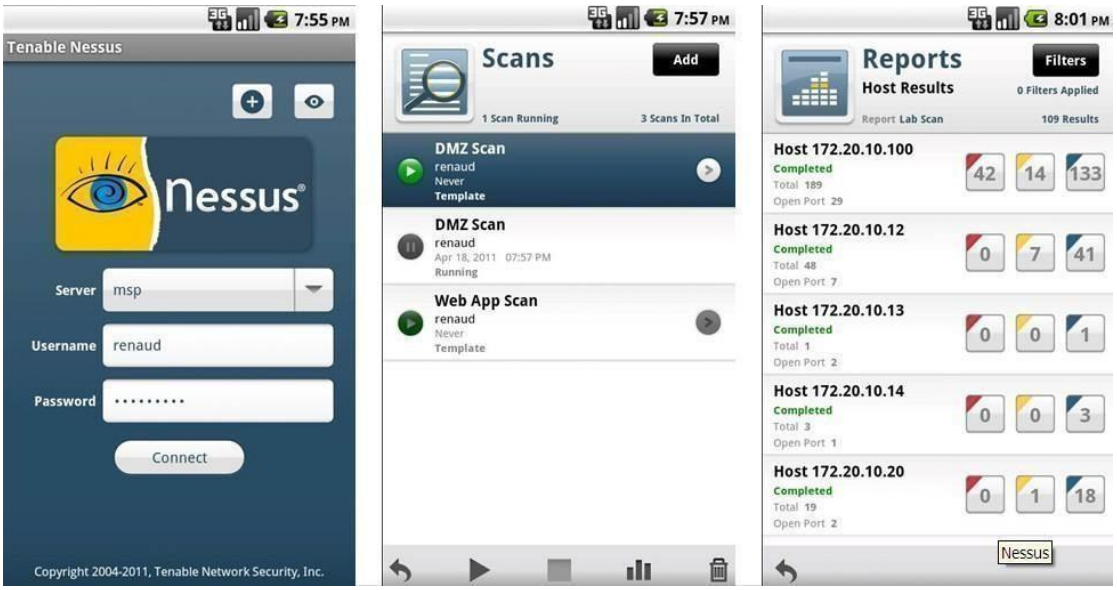
a. Perform mobile network scanning using NESSUS

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 ActiveDirectory servers that contain information from Microsoft Exchange Servers.

- To query for information, the Nessus scanner must be able to reach the Mobile DeviceMan-agement servers. Ensure no screening devices block traffic to these systems fromthe 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 tothe management servers, you do not need to configure a scan policy to scan specific hosts.

- tothe 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 retrievesinformation 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 accordingto our need, and to do so Click on "**Add Table**". After this, a new box will appear named "**Rainbow Table Properties**"

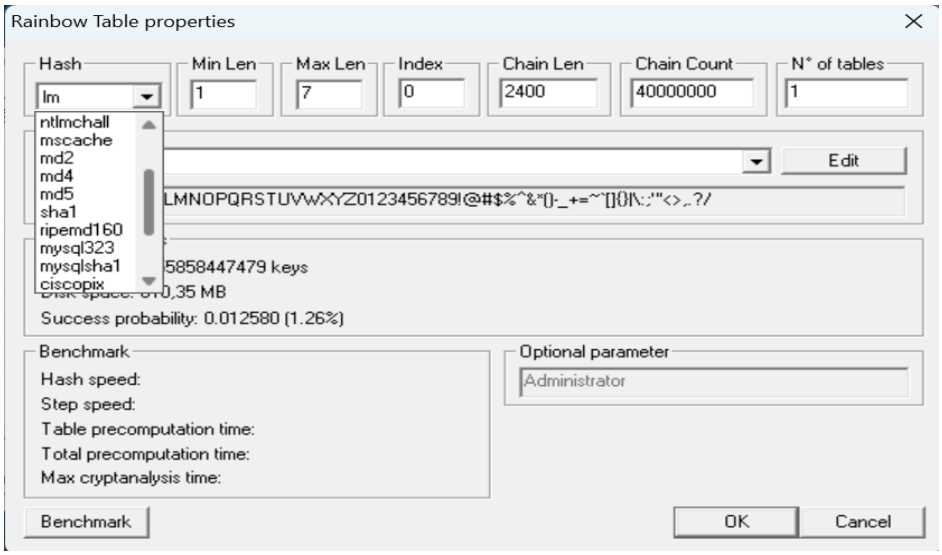
c. Perform the System Hacking using the following tools:

ii. Winrtgen

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

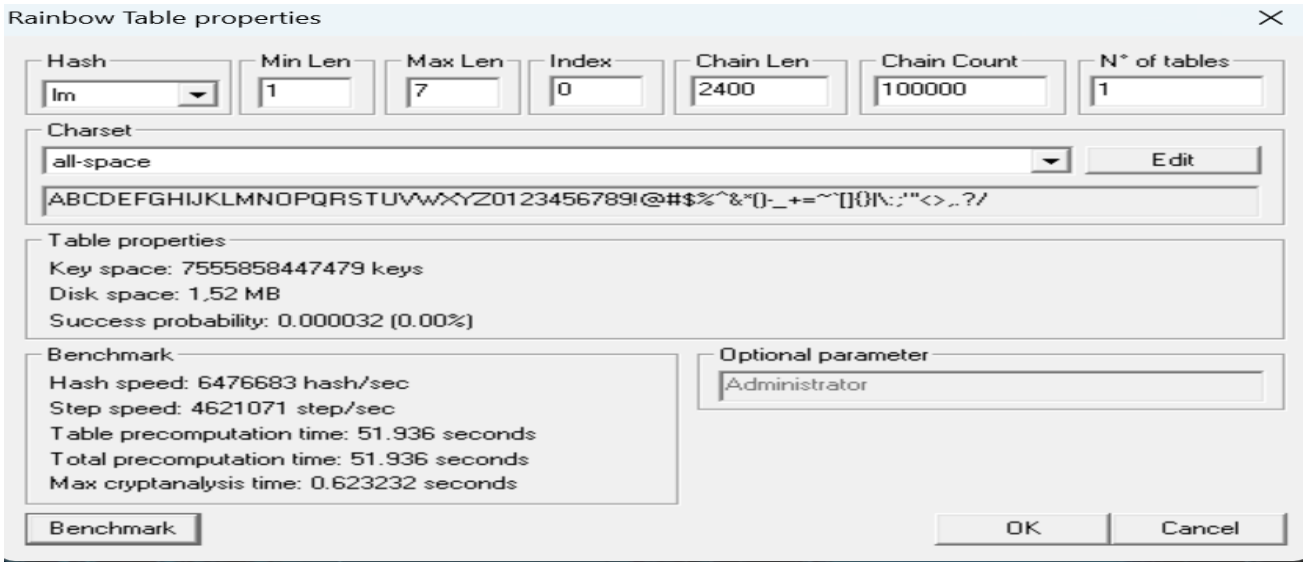
To generate rainbow tables first we will have to modify the properties of WinRTGen accordingto our need, and to do so Click on "**Add Table**". After this, a new box will appear named "**Rainbow Table Properties**"

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

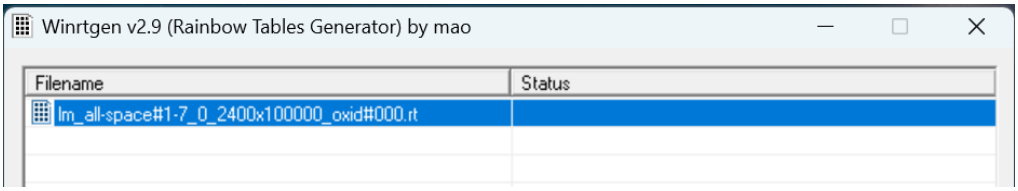


Hash: The type of encryption we want the rainbow table to be generated. For exampleMD5, MD4, SHA1, etc

After assigning the values to the properties according to our needs click on "Benchmarks". Thiswill 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

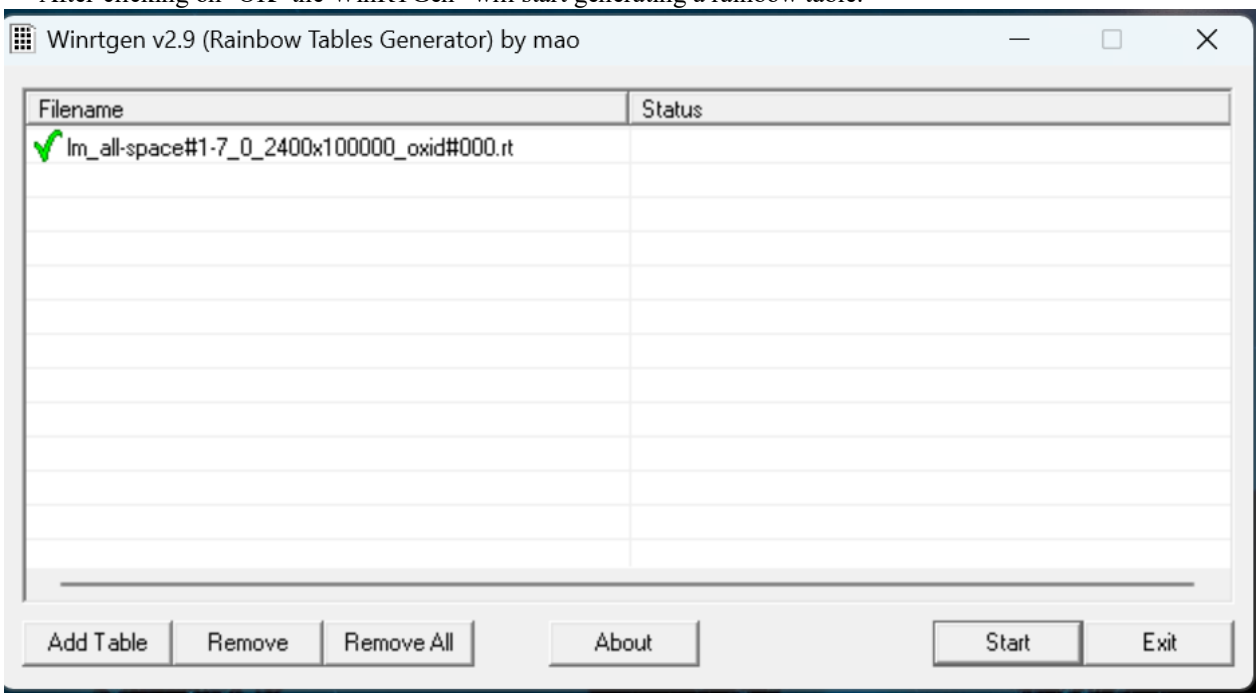


After “Benchmark” click on “Ok”. This will add the Rainbow Table to the queue in the mainwindow



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.



This table will be saved to your WinRTGen Directory.

iii. 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 inSAM 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 afterextracting it.

This utility was created by Tarasco. This utility dumps the system’s SAM file’s credentials afterextracting 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 commandsbelow to save the registry values for the SAM file and system file in a system file:

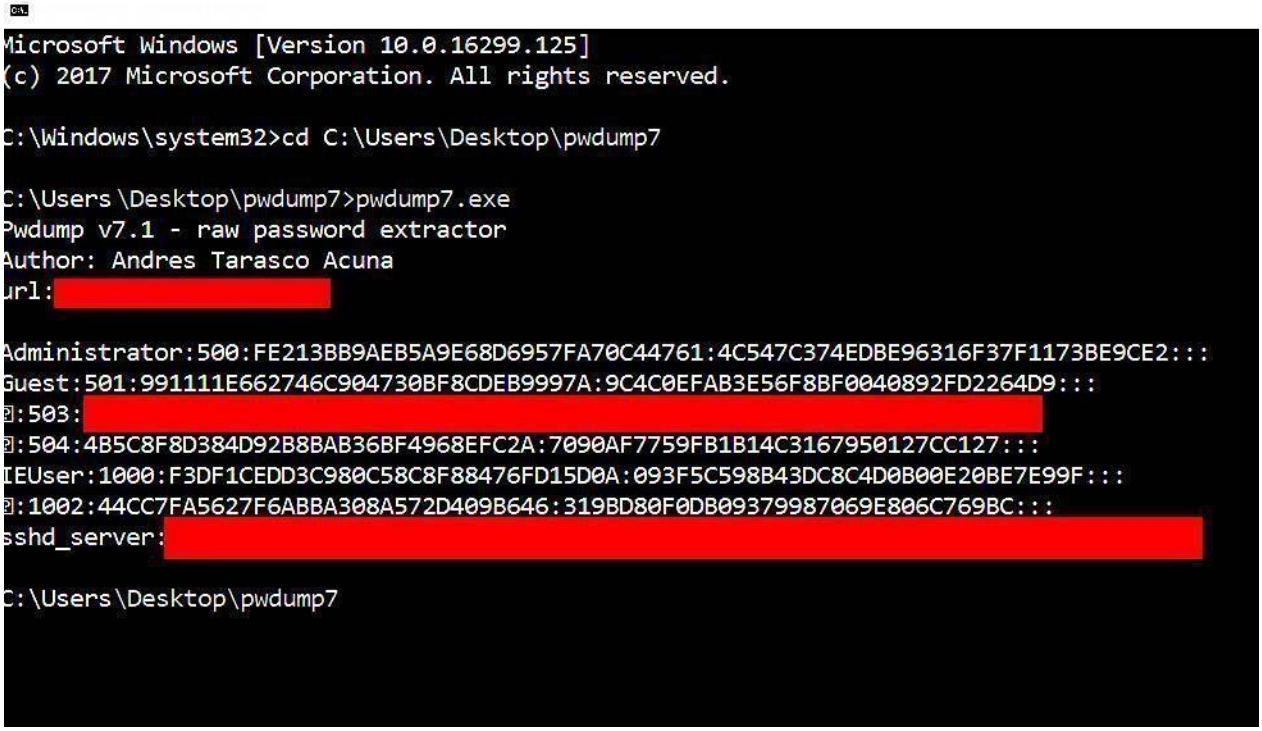
reg save hklm\sam c:\sam

PwDump7.exe

As a result, it will spill all the hashes kept in the SAM file. The next step is to use the commandsbelow 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



iv. Ophcrack

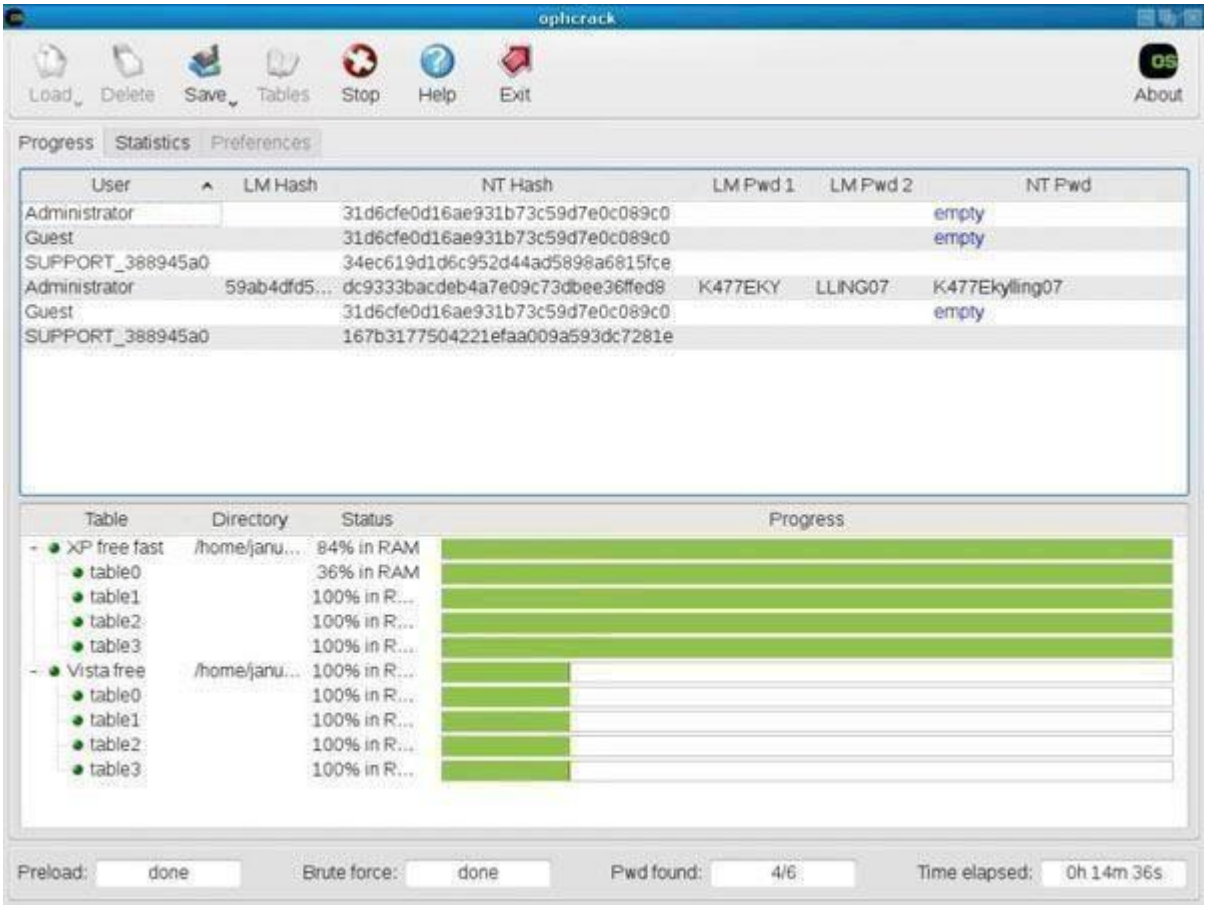
When it comes to free Windows password crackers, users usually opt for Ophcrack as it is freeand easily available.

Step 1: Since we are assuming that your Windows PC is locked and you do not know thepassword, the first step needs to be carried out on a different PC with internet access andadministrator privileges.
Step 2 : Download the correct version of Ophcrack Live CD from the official website to thesecond PC.
Step 3 : Burn the ISO file to a USB or CD. To do this, you will need an ISO burningapplication.
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 Windowsinstallation. This is made possible by the fact that Ophcrack itself contains a small operatingsystem that can run independently of your Windows OS. In a few moments, you will see theOphcrack 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 diskpartition 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 accountsand their passwords displayed in column format. Against the previously locked username, lookfor an entry in the NT Pwd column.

Step 7: This will be your recovered password, so note it down. You can now remove the LiveCD 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.

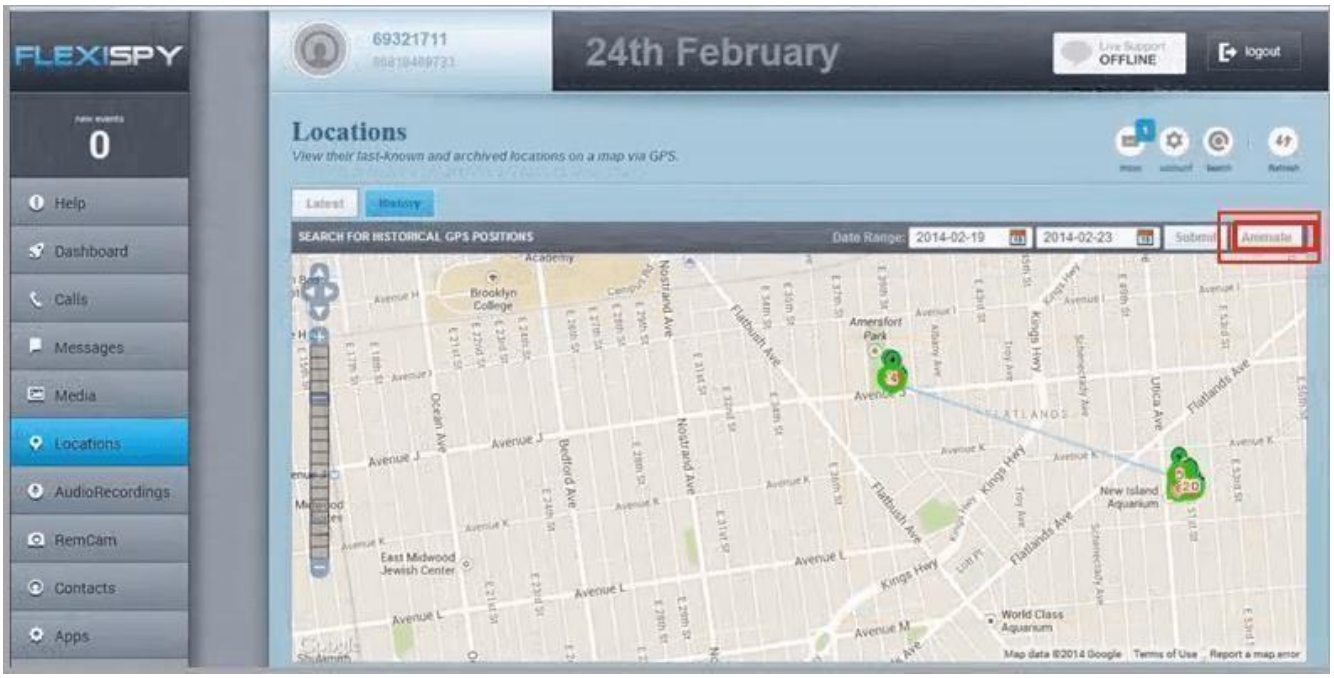


V. Flexispy

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 monitoringsystem 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 itsrecorder and record conversations without the owner noticing.



vi. 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. Anotherform 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 witha file but not in the file itself on an NTFS system. NTFS ADS is a Windows hidden stream thatstores 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 fromthe system administrator.

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

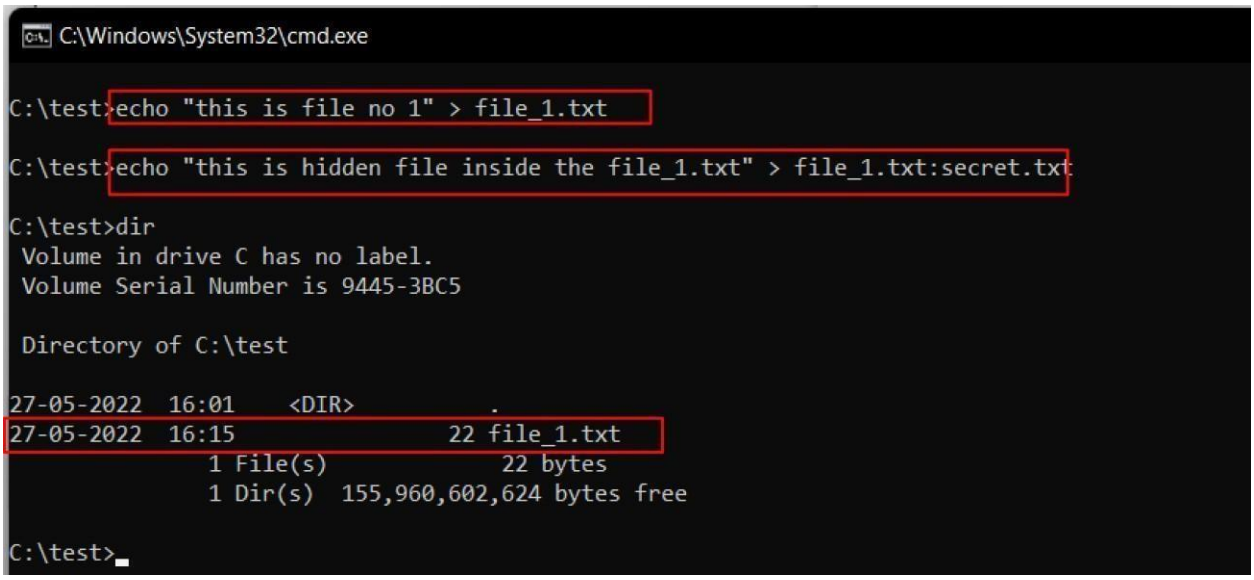
Creation of NTFS streams:

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

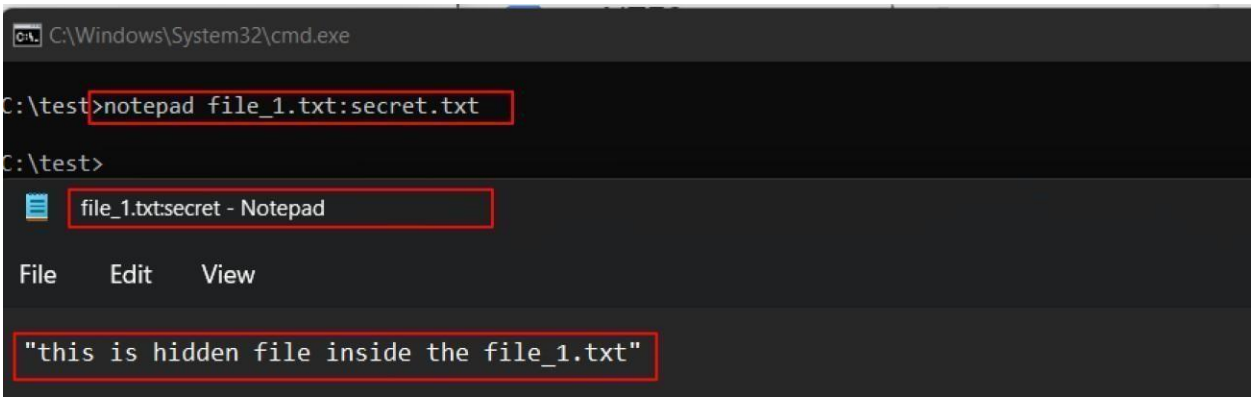
filename.extension:alternativeNmae

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 ahidden 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.txtyou will only find the data present in file_1.txt. And also stream willnot be shown in the directory as well.
The following command can be used to view or modify the stream hidden in file_1.txt notepadfile_1.txt:secret.txt



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

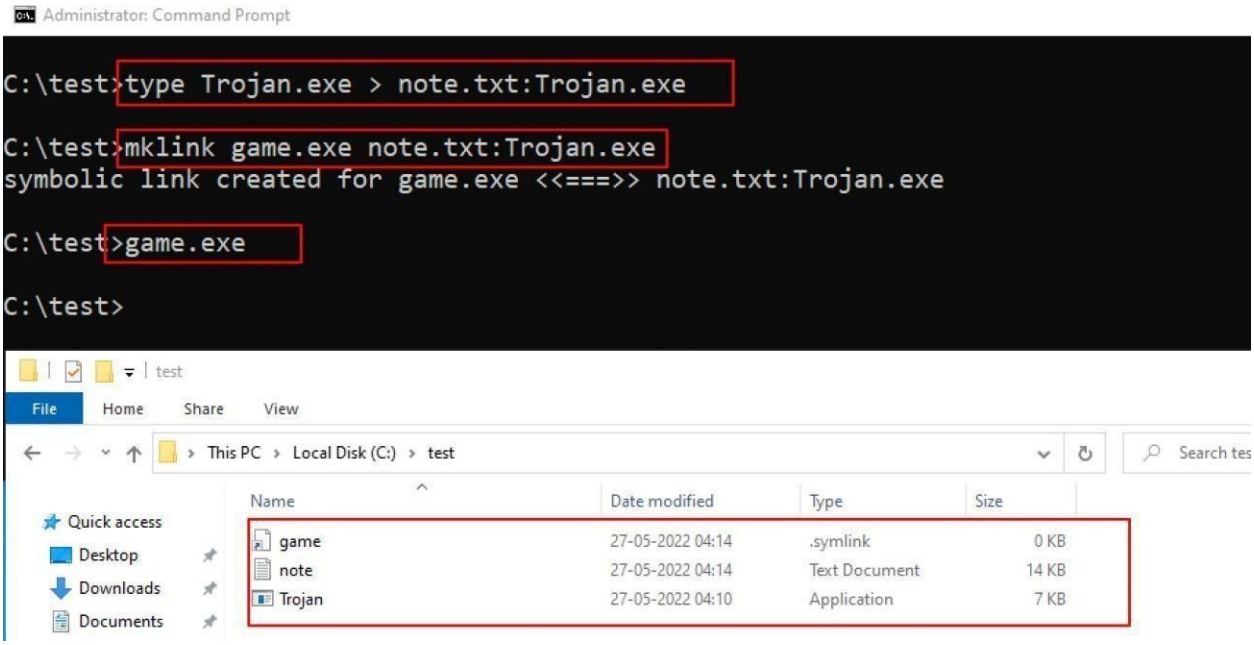
C:\test>type Trojan.exe > note.txt:Trojan.exe

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 fromthe 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.exeis theshortcut created to launch trojan.exe.

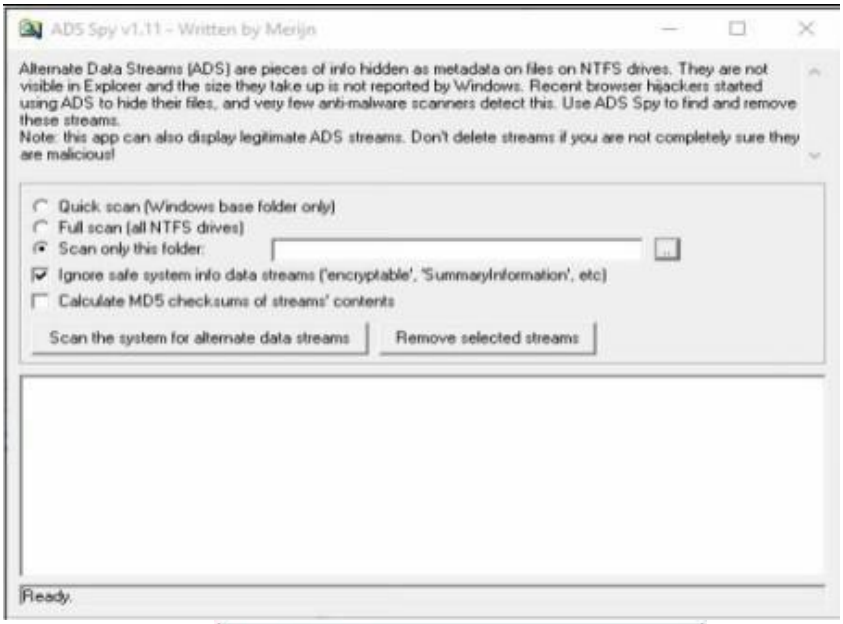


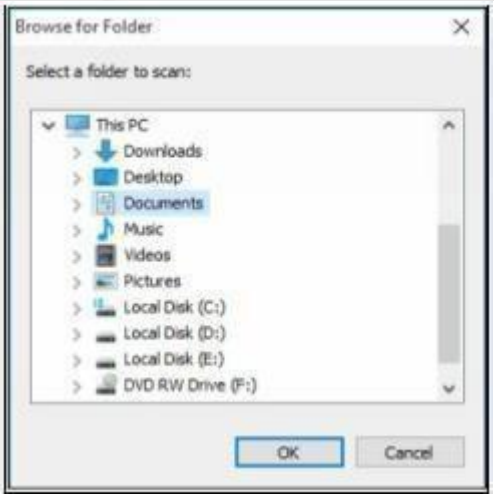
vi.ADS Spy

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 folderonly.



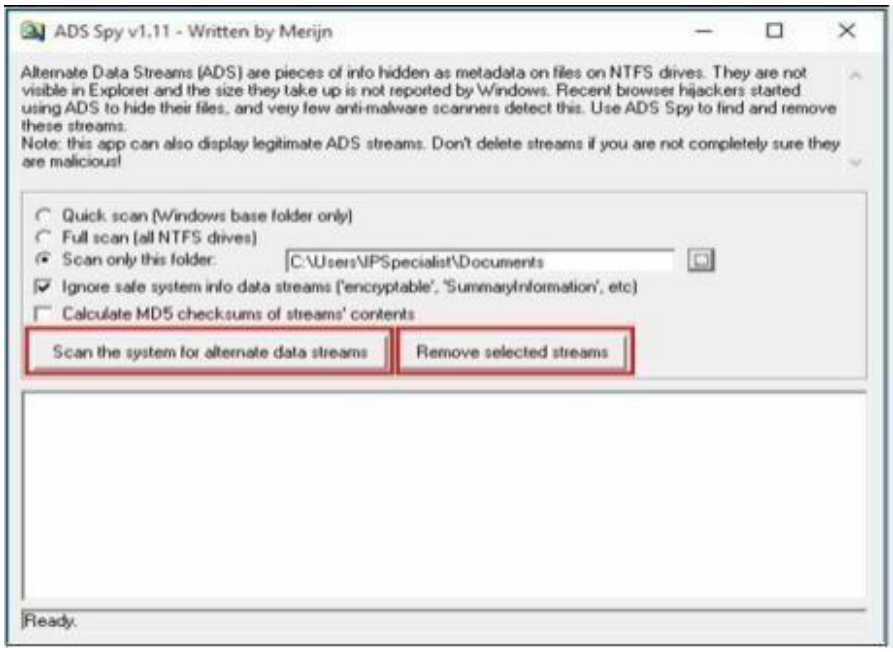


Select an Option, if you want to scan for ADS, click "**Scan the system for ADS**"/ or click

removes button to remove the file

vii. Snow

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



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

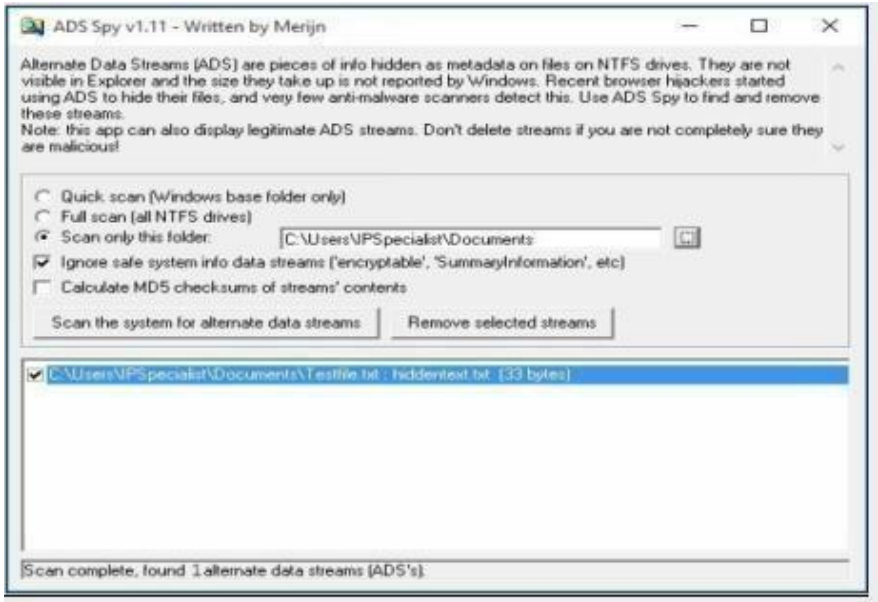
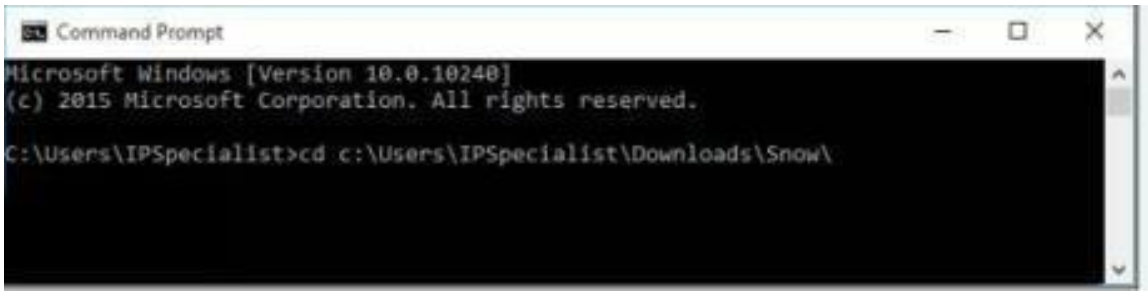


Figure 6-50 ADS Detection

Go to Command Prompt

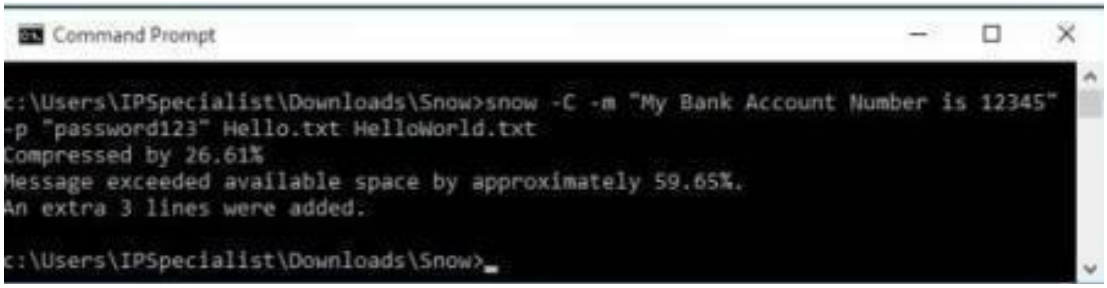
Change the directory to run Snow tool



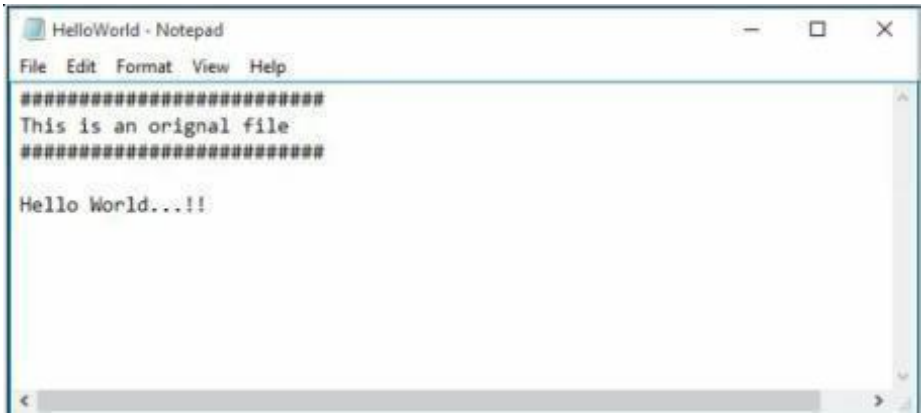
Type the command

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 ofsource file containing hidden information.



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

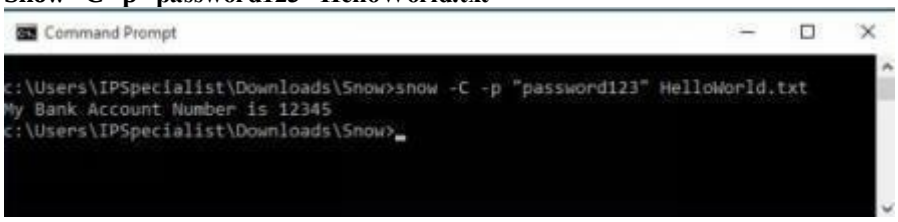


New File has the same text as an original file without any hidden information. This file can besent to the target.

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 theprevious section.

viii. Quickstego

Image Steganography using QuickStego

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

2. Enter the Text or Upload Text File
3. Click Hide Text Button
4. Enter the Text or Upload Text File
5. Click Hide Text Button

1. Save Image

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

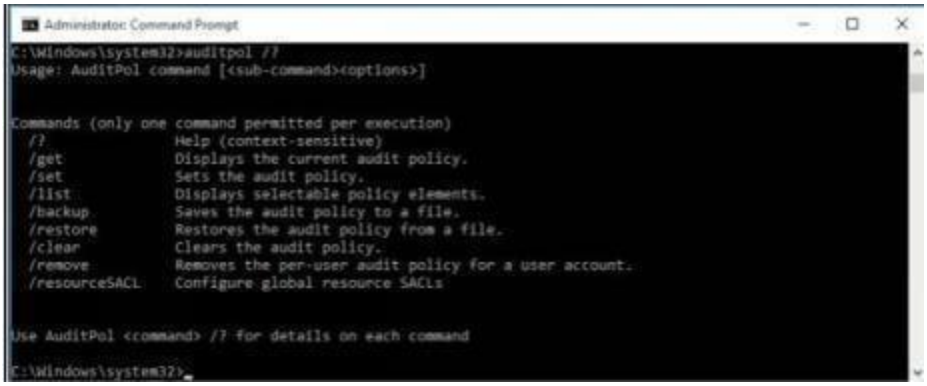
Recovering Data from Image Steganography using QuickStego

1. Open QuickStego
2. Click Get Text

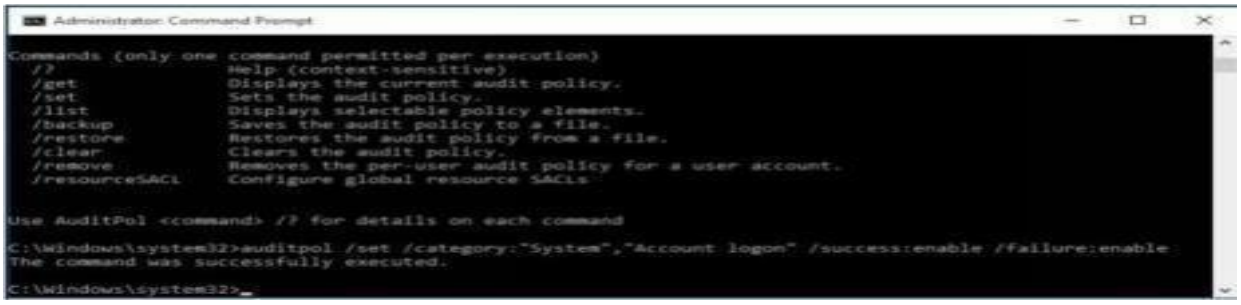
3. Open and Compare Both Images
Left Image is without Hidden Text; Right Image is with hidden text

ix. Clearing Audit Policies

Enabling and Clearing Audit Policies
To check command's available option Enter
C:\Windows\system32> **auditpol /?**



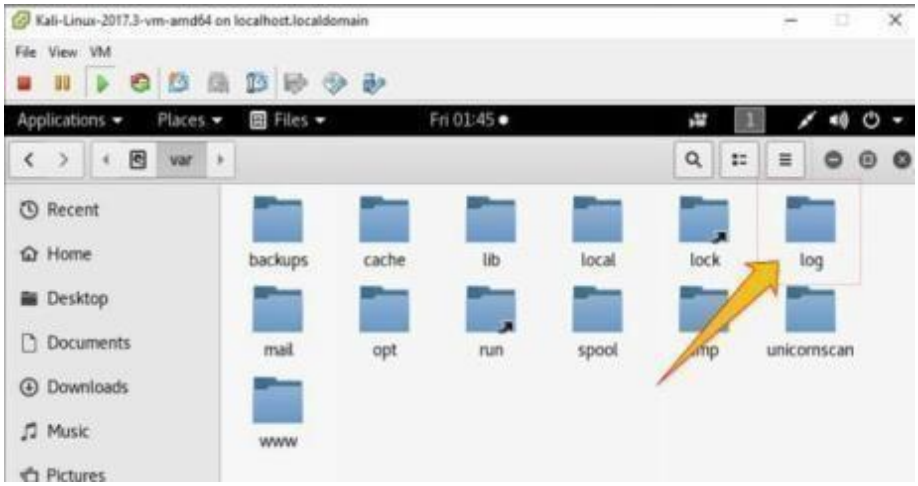
Enter the following command to enable auditing for System and Account logon: -
C:\Windows\system32>**auditpol /set /category:"System","Accountlogon" /success:enable /failure:enable**



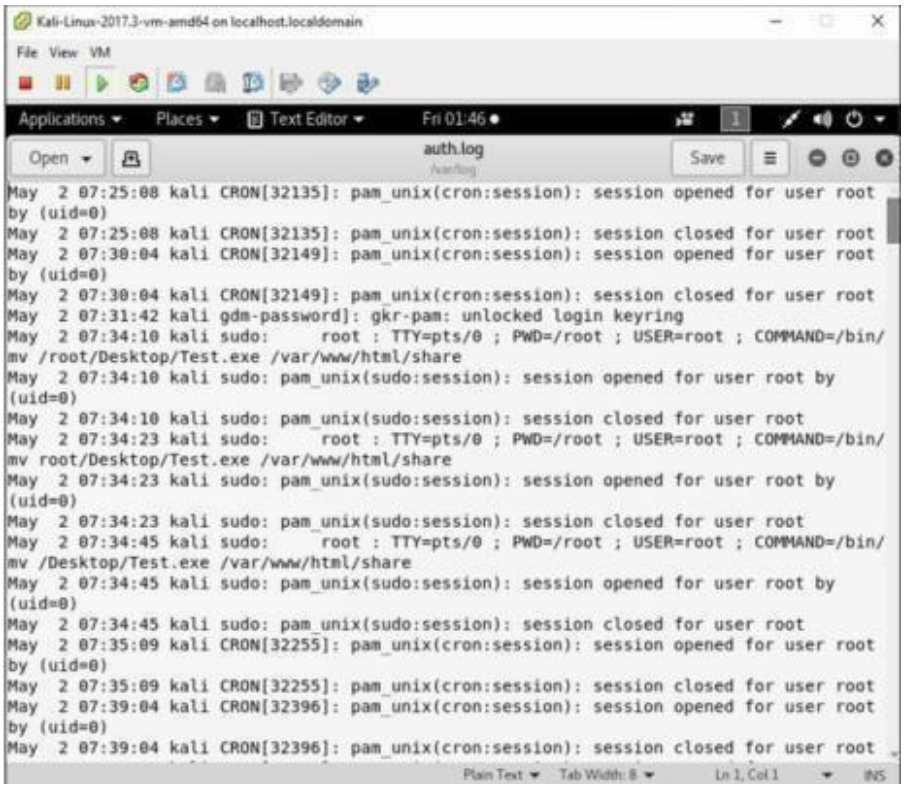
To check Auditing is enabled, enter the command C:\Windows\system32>**auditpol logon","System"/get /category:"Account**

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**

1. Go to **Logs** folder:



1. Select any log file:
2. Open any log file; you can delete

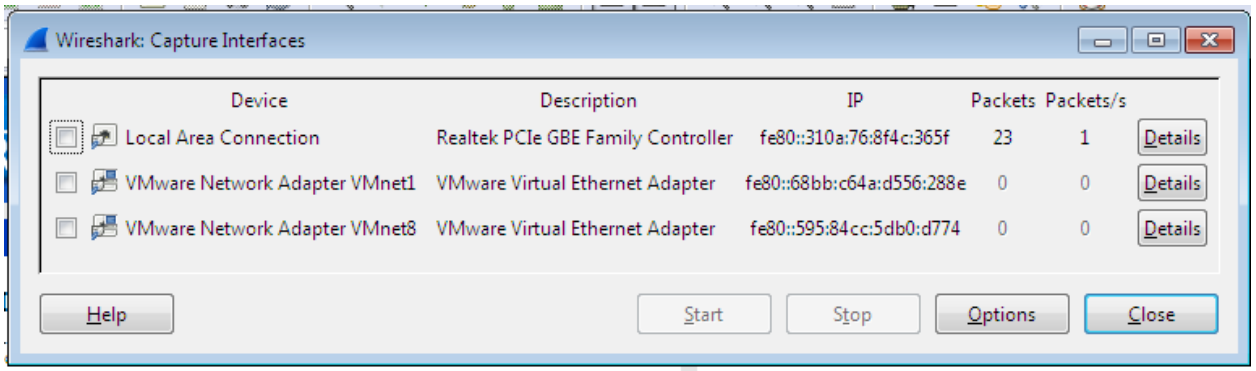


Practical No. 5

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 theentire network stack in Wireshark, which technically makes what we have captured frames ratherthan packets.

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



Select the network adapter (wired or wireless) that you are currently using to connect tothe 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 thenetwork 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:

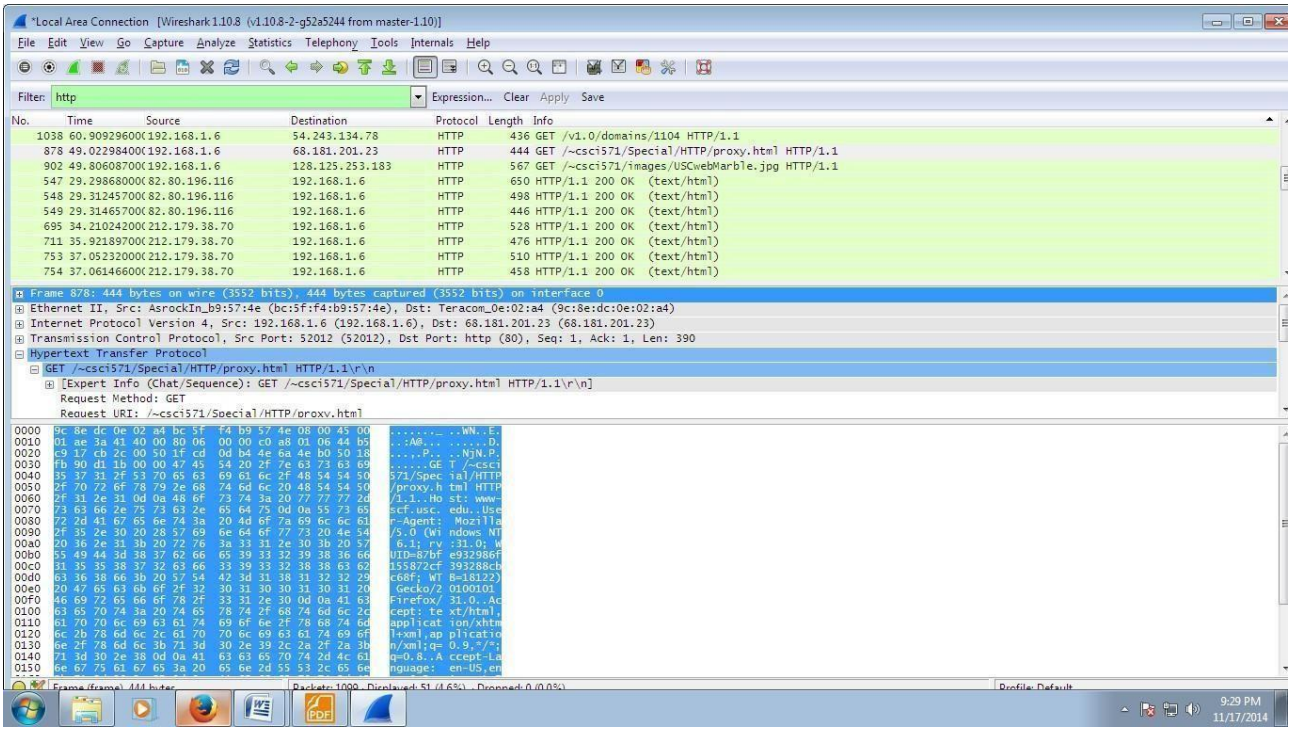
Examining HTTP Traffic

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. Selectthis packet.
- In the middle frame of the Wireshark window, expand the "Hypertext TransferProtocol" 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 therequested web page.

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 appreciatethe ability to hand enter a new MAC address.

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

Figure A

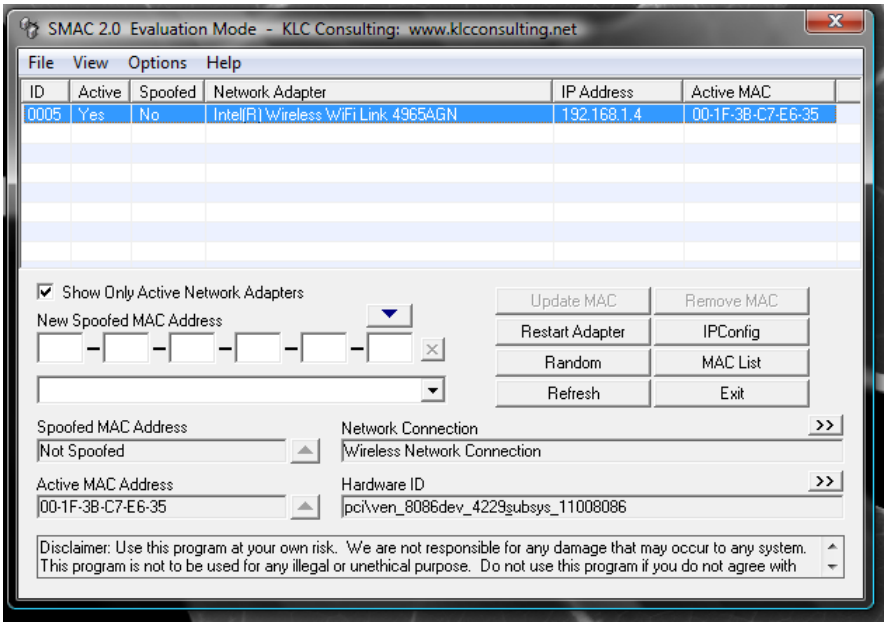
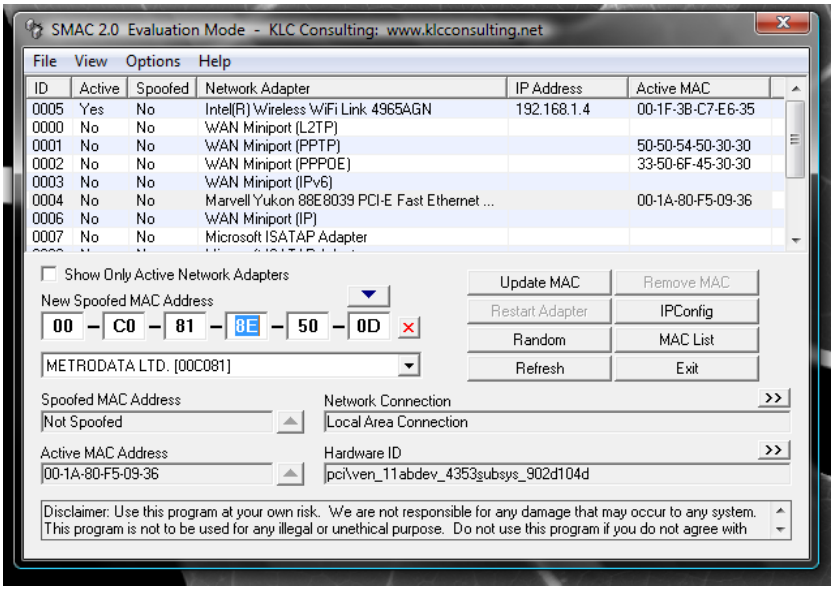


Figure C



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 (oryou can just take the first random address you get). Once you have your address, select the Options menu and make sure Automatically RestartAdapter is checked. Once that is checked, hit the Update MAC Address button and the newMAC address will be applied.

C.Use Caspa Network Analyser.

When we correctly deployed Capsa, we cannot wait to start our first capture right away. Capsa7'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 panelfirst.

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.

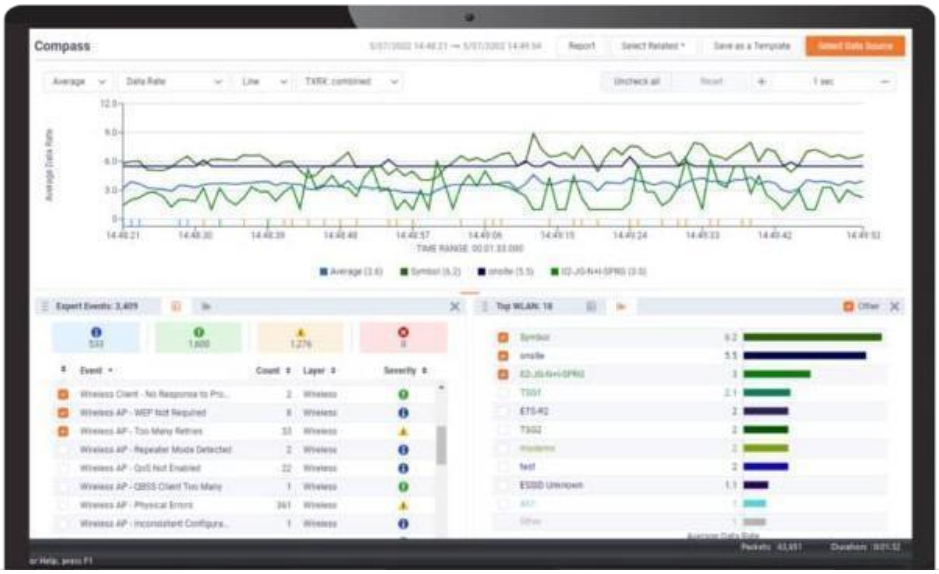
Click the big Run button to start a capture right away

Use Omnipeek Network Analyzer.

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

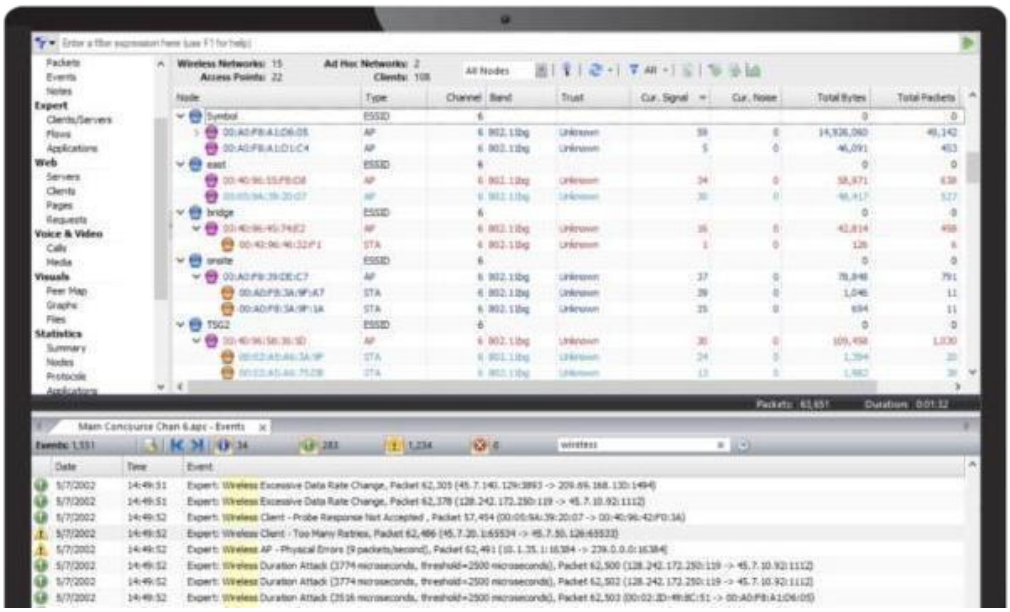
Real-Time Network Protocol Analyzer

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.



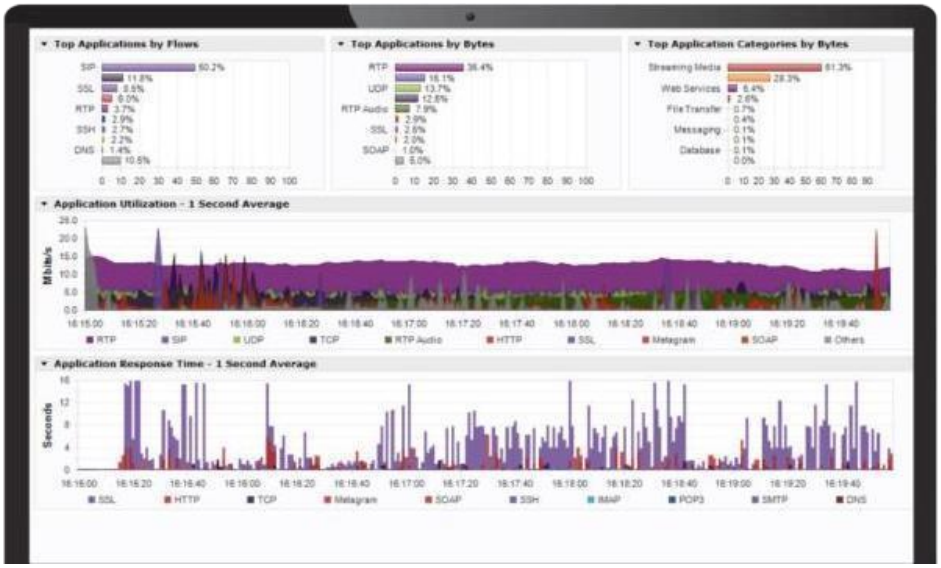
Intuitive Graphic Displays and Visualization

Omnipeek delivers intuitive visualization and effective forensics for faster resolution of networkand application



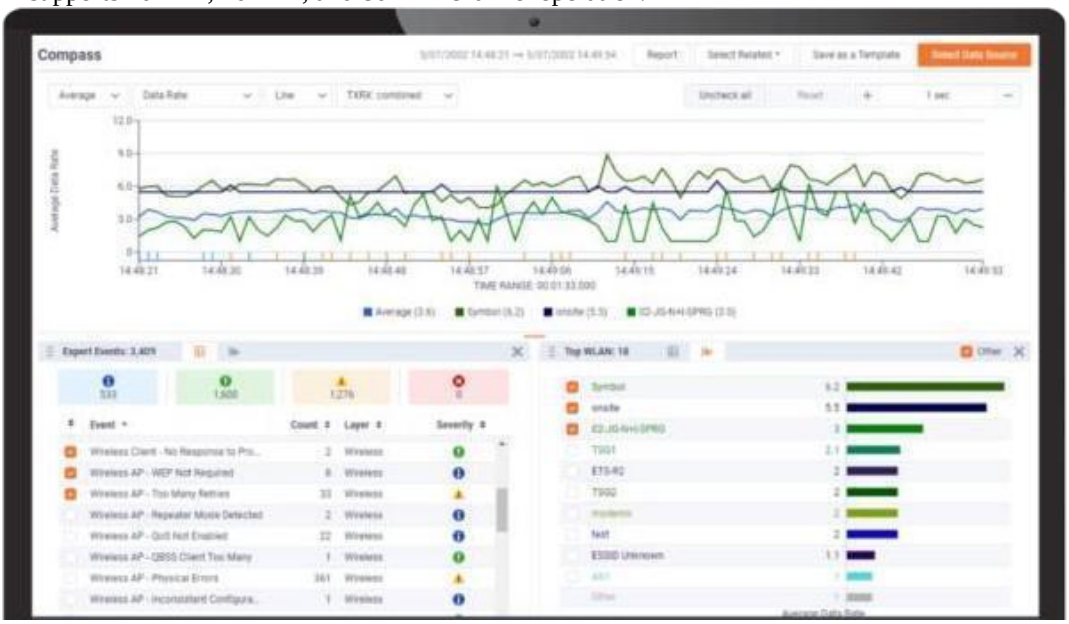
Best-In-Class Network Analysis Workflow

Widely recognized as the best network analysis workflow in the industry, we make it easy todrill 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 packetcapture. 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

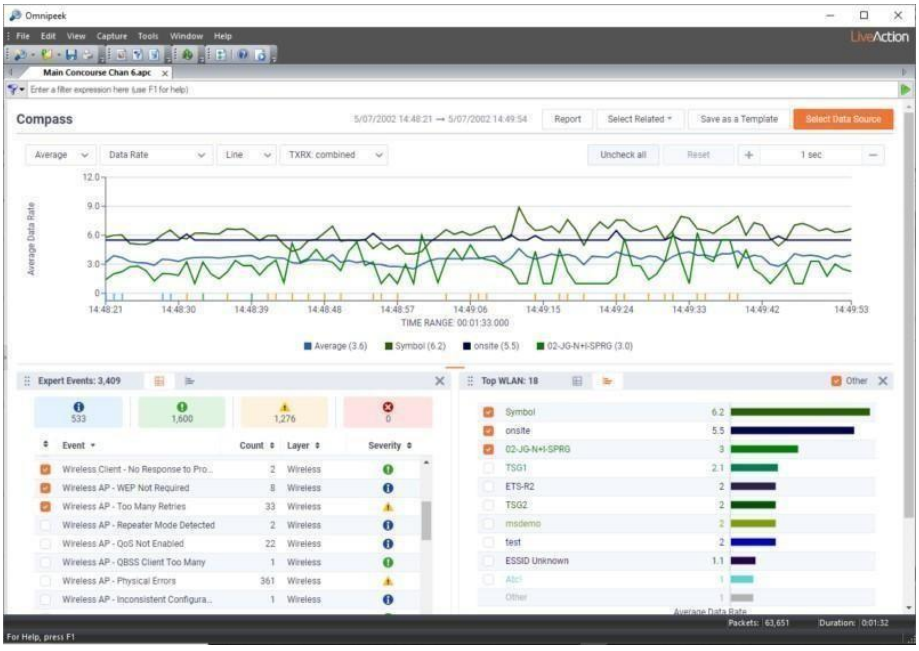
Integrating with LiveCapture, Omnipeek extends network monitoring and visibility for troubleshooting application-level issues at remote sites and branches, WAN links, and datacenters.

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 theneed to travel to a

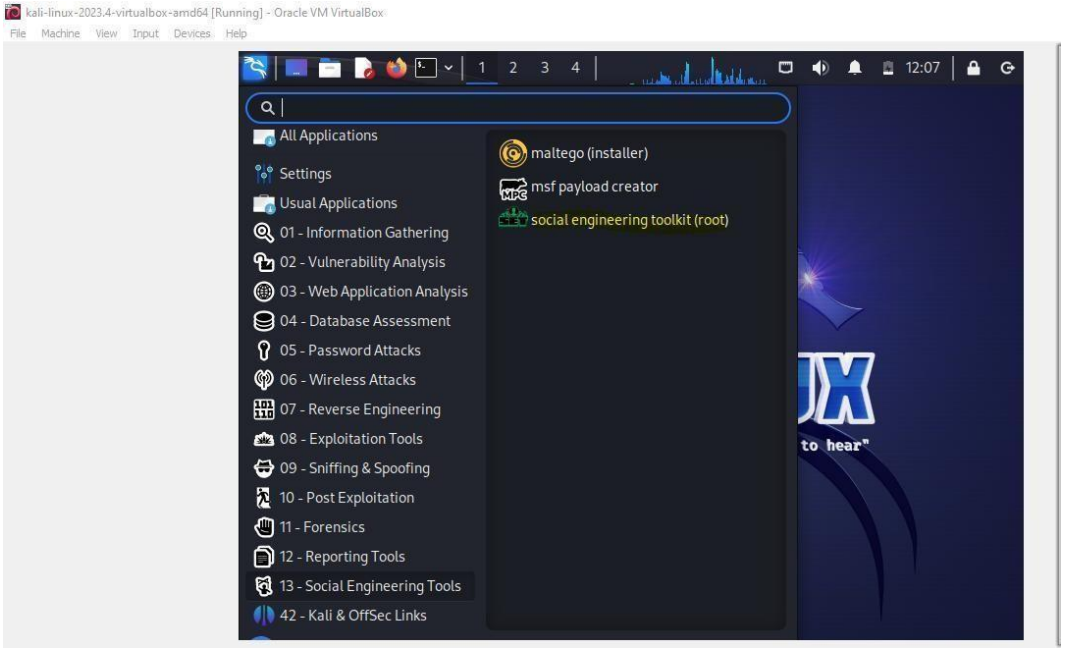


user's location

Section III A.

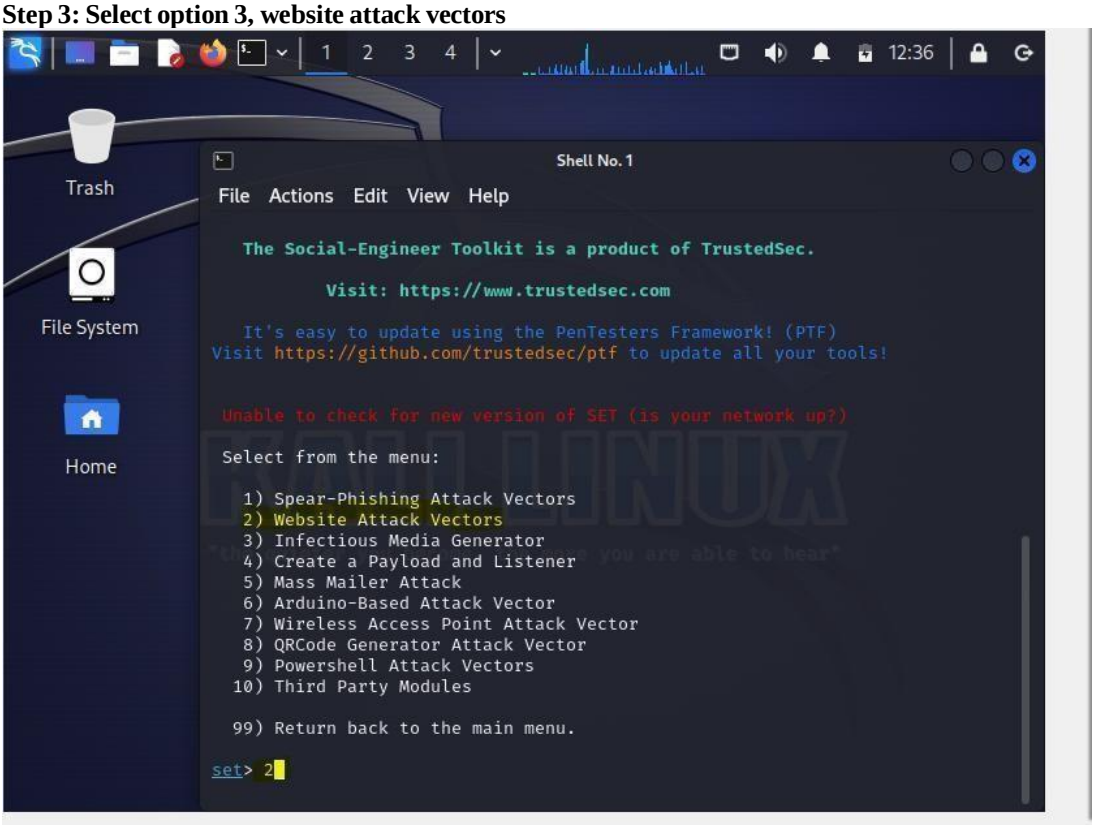
Aim: Use Social Engineering Toolkit on Kali Linux**.**

Step 1: Select social engineering toolkit in the Kali Linux.

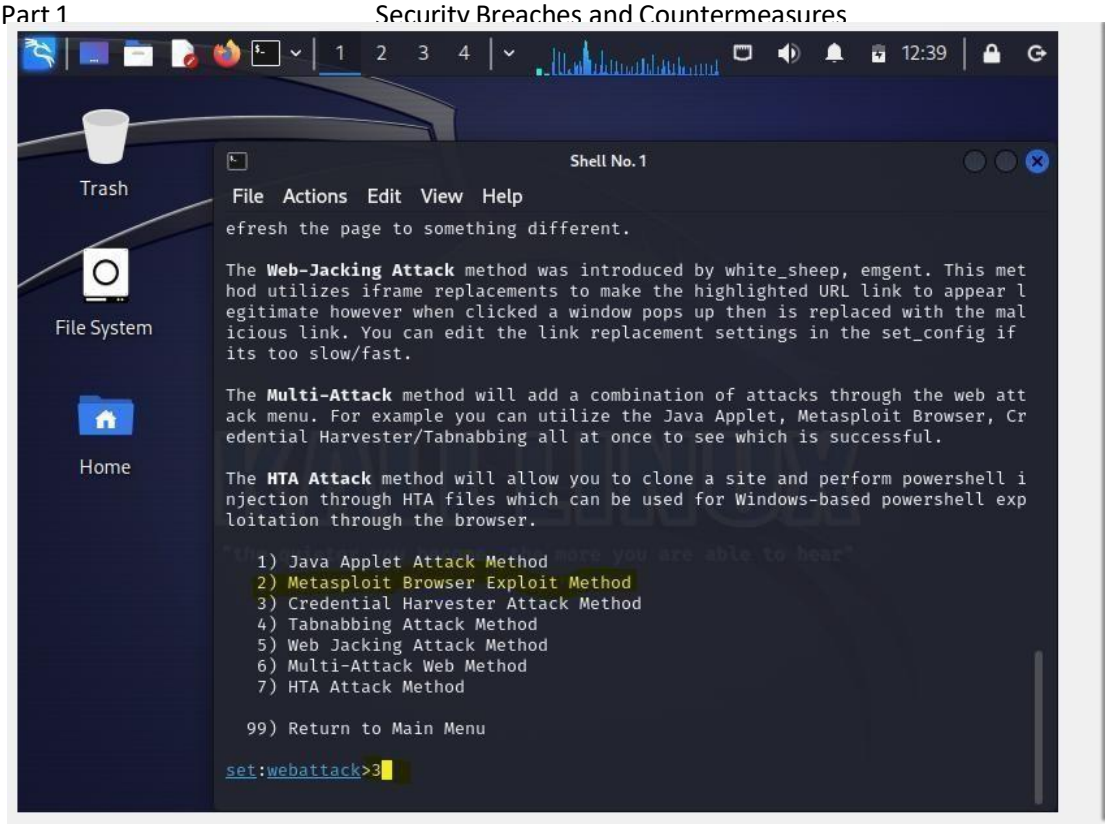


Step 2: Select option 1. Social engineering attack

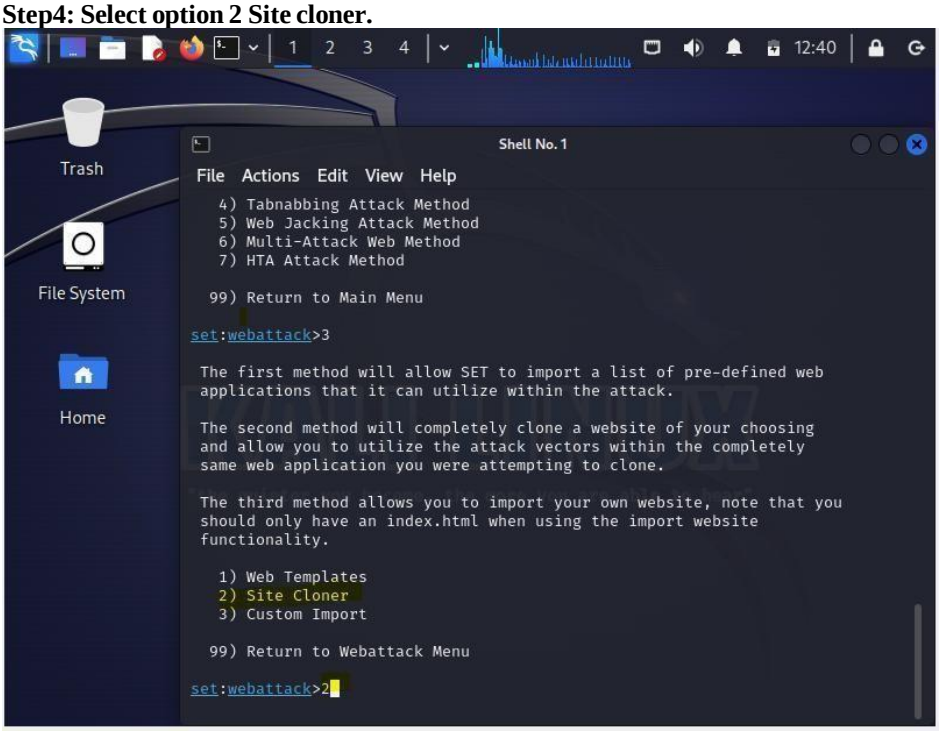
Step 3: Select option 3, website attack vectors



Step 4: Select Credential Harvester attack method



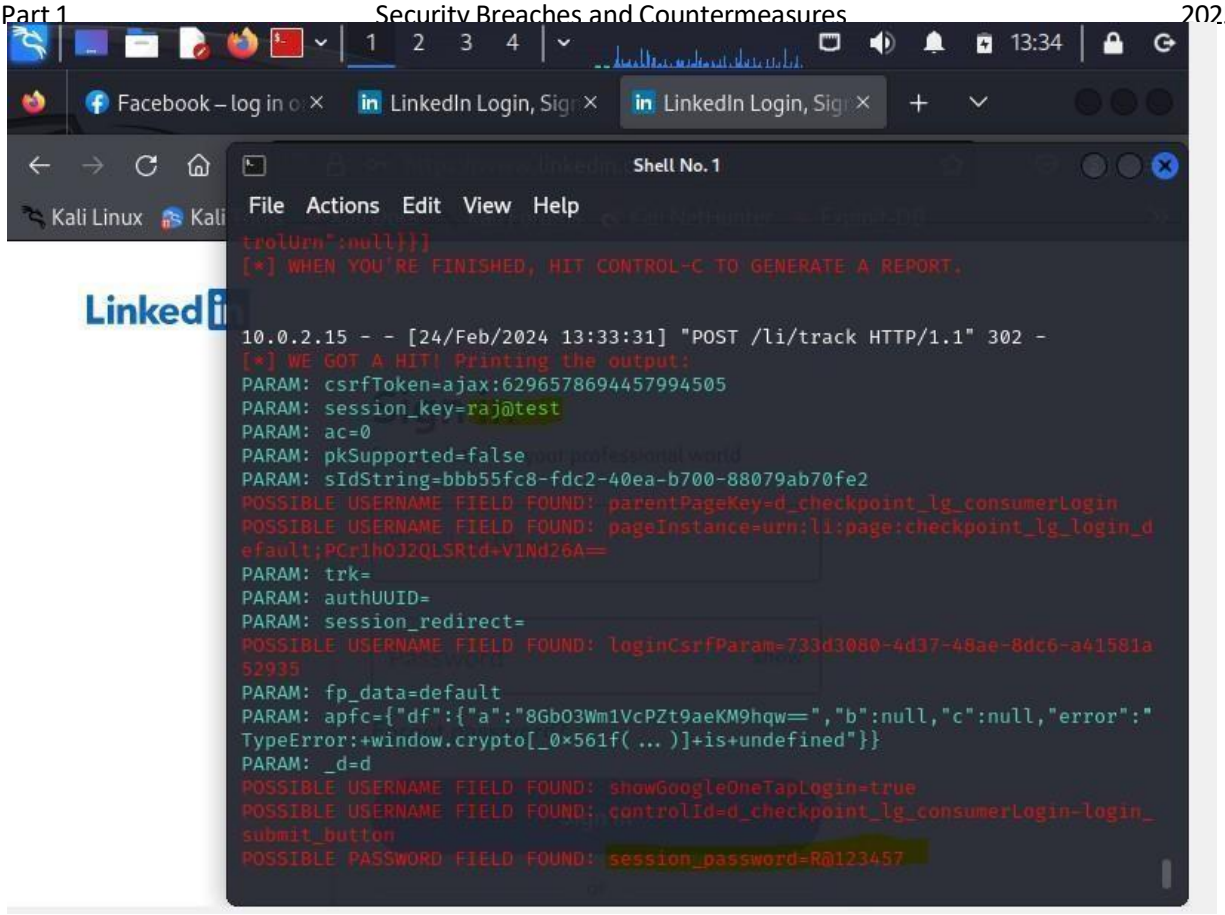
Step4: Select option 2 Site cloner.



Step 5: Enter IP of the local server and URL of the attacking site

Step 6: now enter the ip in the browser, you will find clone website:

Step 7: You can see in the terminal the user id and password is being displayed.



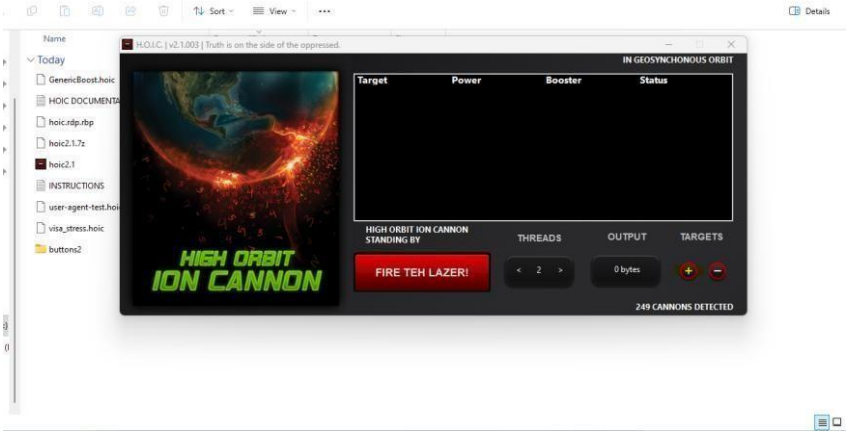
Step 8: Post the attack user is redirected to the original site:

Section III A.

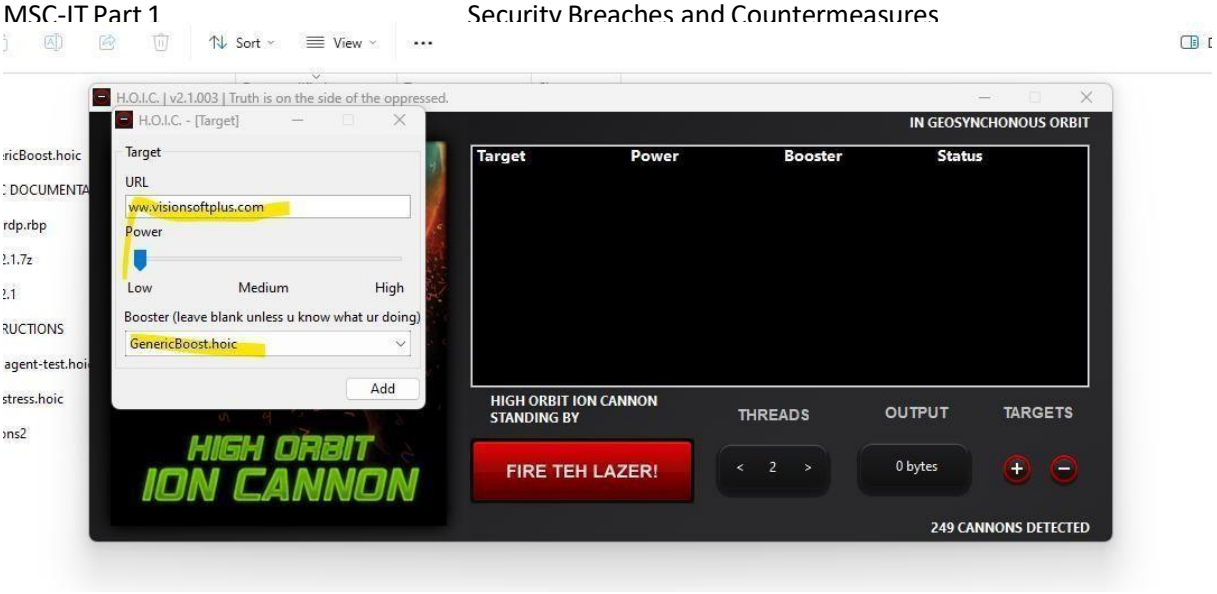
a. Aim: Perform the DDOS attack using the following tools

I. HOIC

Step 1. Open hoic2.1.exe, once it open click on the "+" button

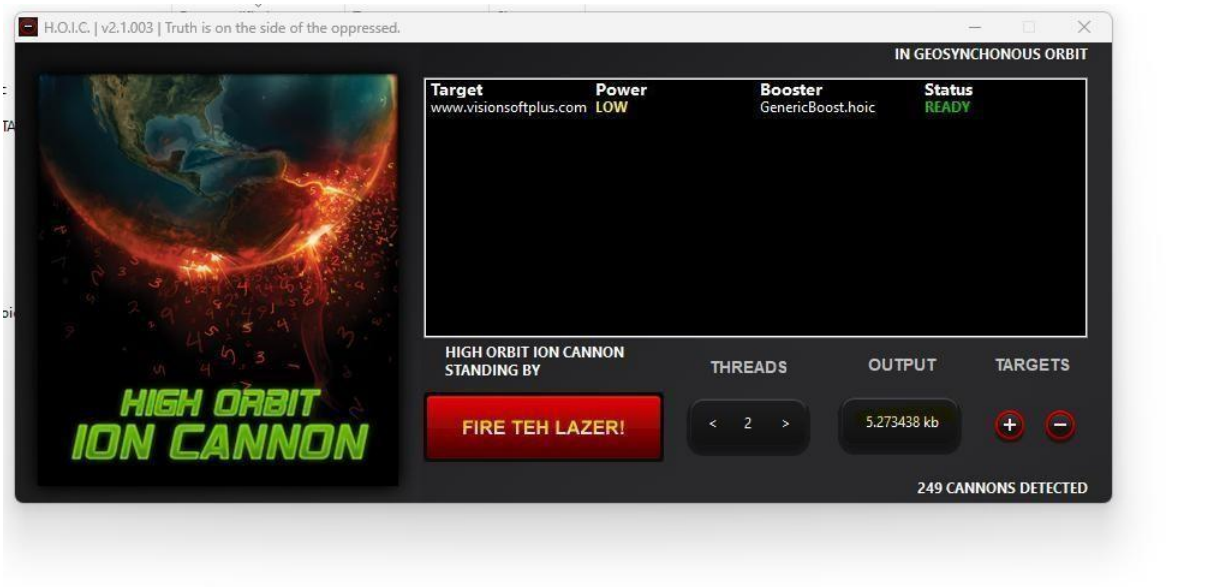


Step2: enter the url you want to attack, then click on add button.



Step 3: Click on fire button to attack

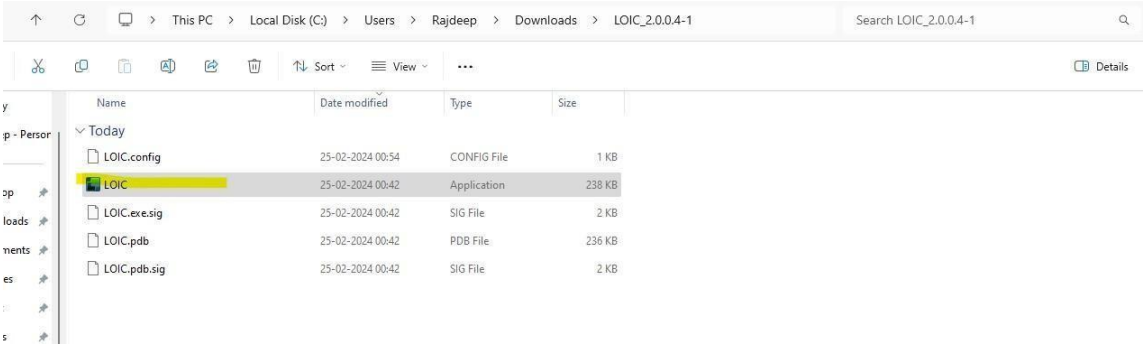
Step 4: you can see the attack is carried on and check the same on wire shark also



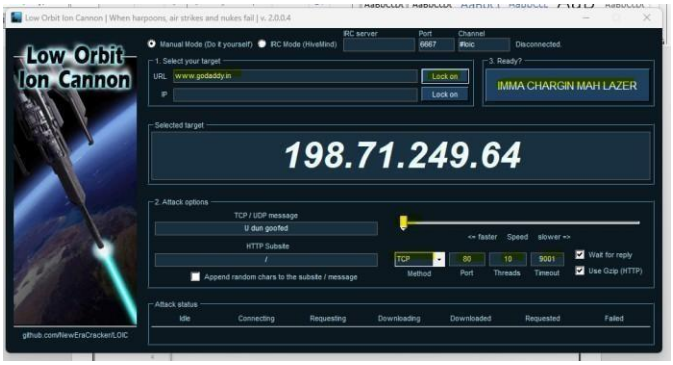
Step 5: To stop the attack again click on the Fire button.

II. LOIC

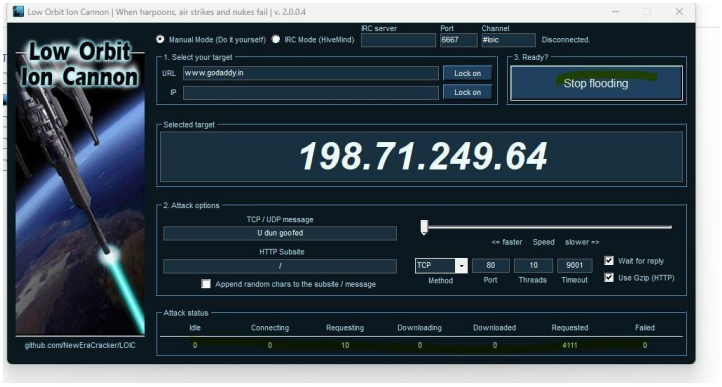
Step 1. Click on the loic.exe:



Step 2. Enter the URL click on Lock On button, change the parameter Like speed, method, number of thread, timeout. And the click on IMMA Chargin button.



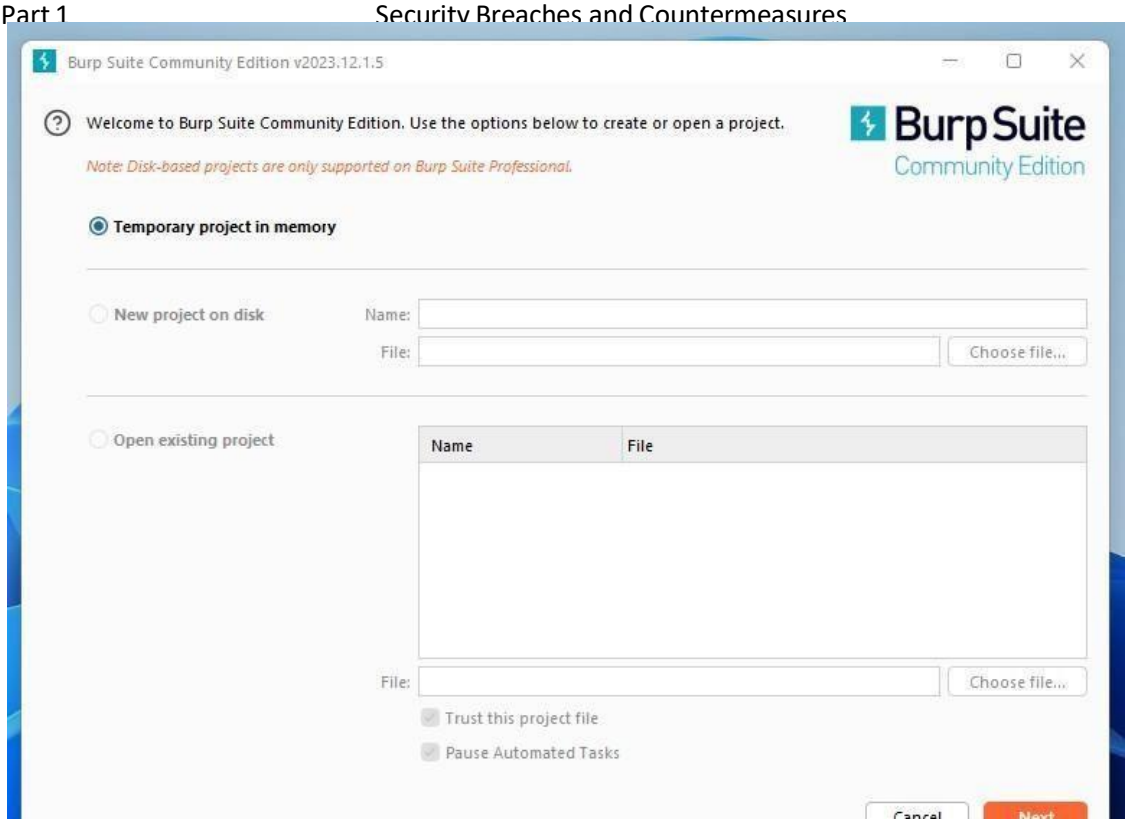
Step 3: You can see the number of requests getting hit. Click on Stop button to stop the DDOS attack.



C. Aim: Using Burp Suite to inspect and modify traffic between the browser and target application

Application name : Burp tool

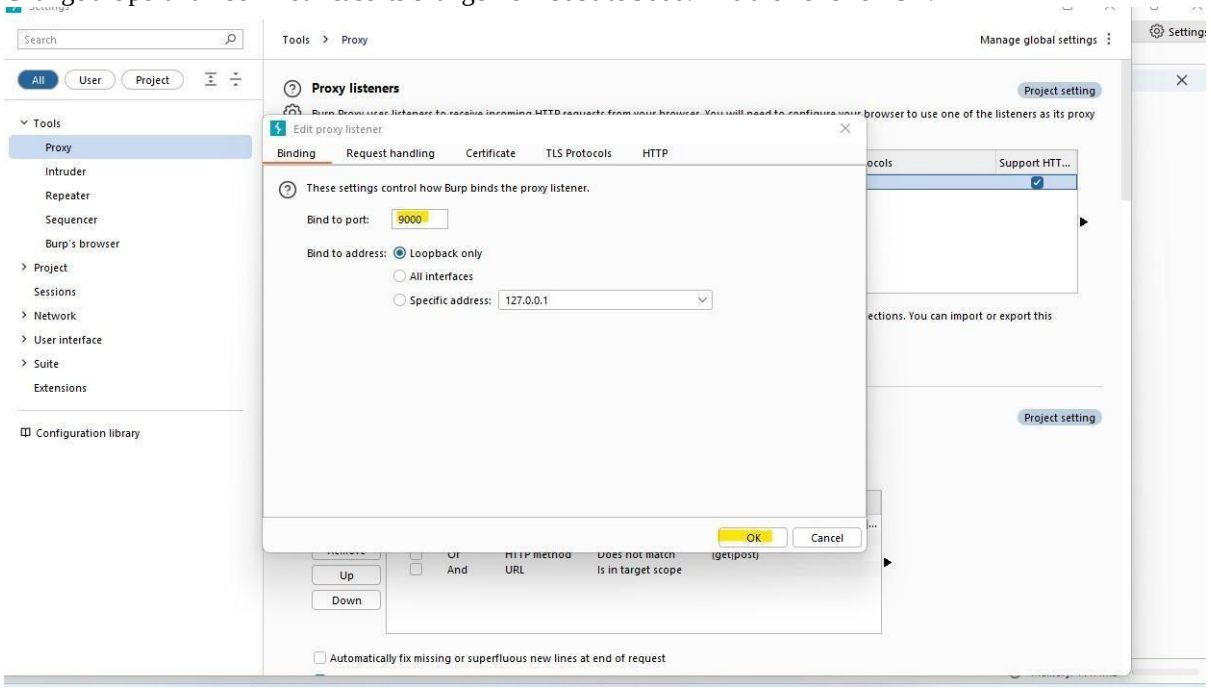
1. Open Burp Tool: Click on next



2. Click on start Burp

3. Select Proxy in the tab:
4. Go to proxy setting:

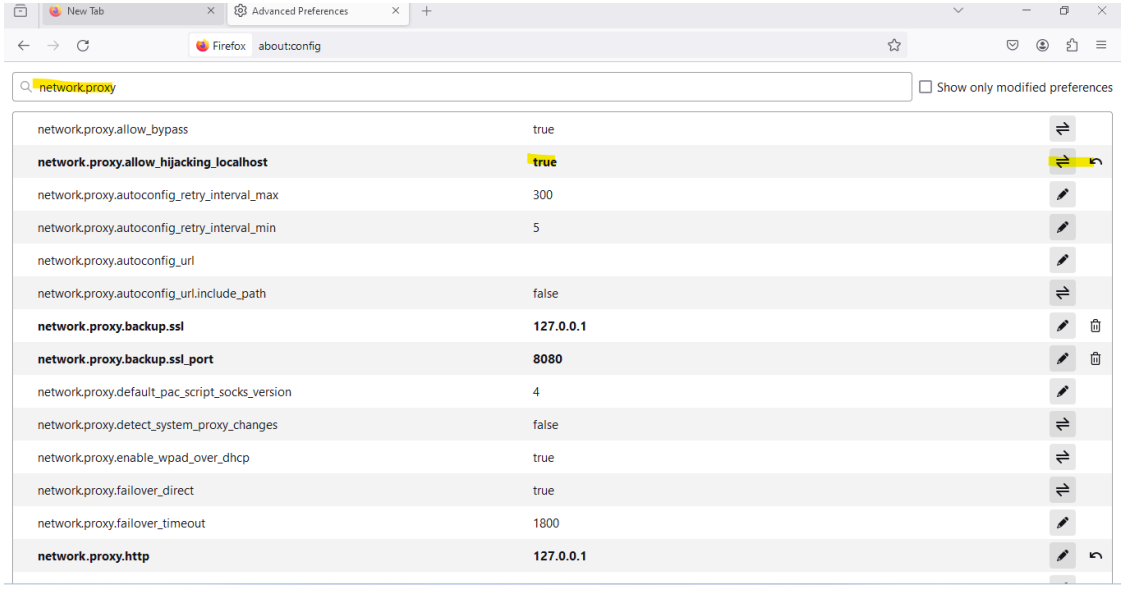
5. Click on Edit:
6. Change the port number in our case its change from 8080 to 9000. And then click on OK.



9. Now go to the firefox browser: goto settings or preference depending on the version:

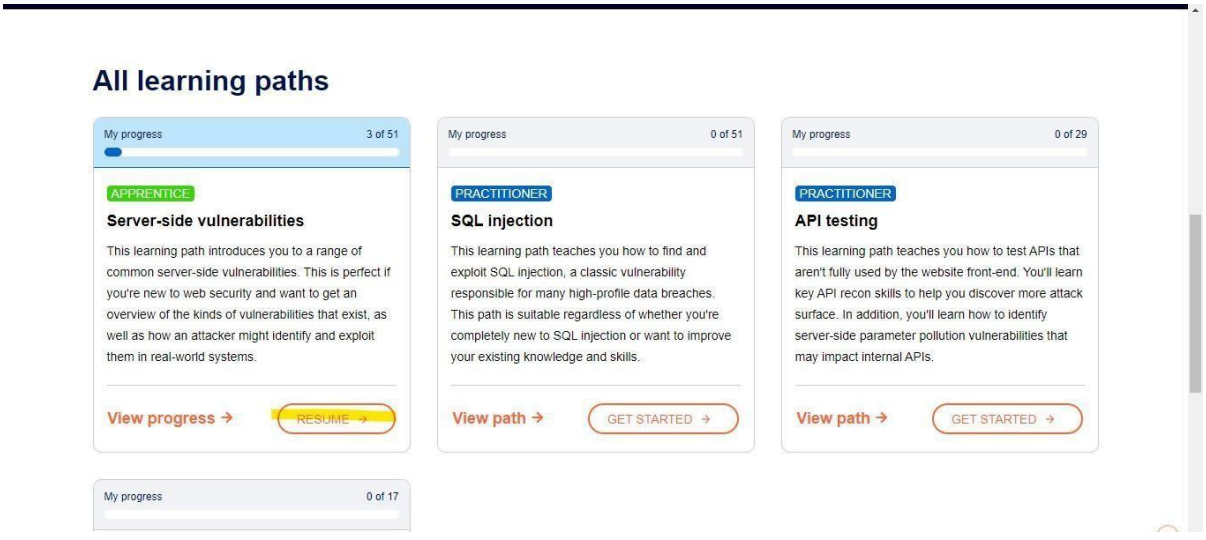
10. Search for proxy in the search bar and then click on setting:

11. Now do the following steps:
a. select manual
b. Enter ip as 127.0.0.1 and port as 9000.
c. select option also use this proxy for HTTPS
d. click on ok
12. Now go to firefox search bar and type “about:config”. In the screen click on “Accept the Risk and Continue”.
13. Enter: “network.proxy” and select the option as per the image below, click on the right side button to make the value true:



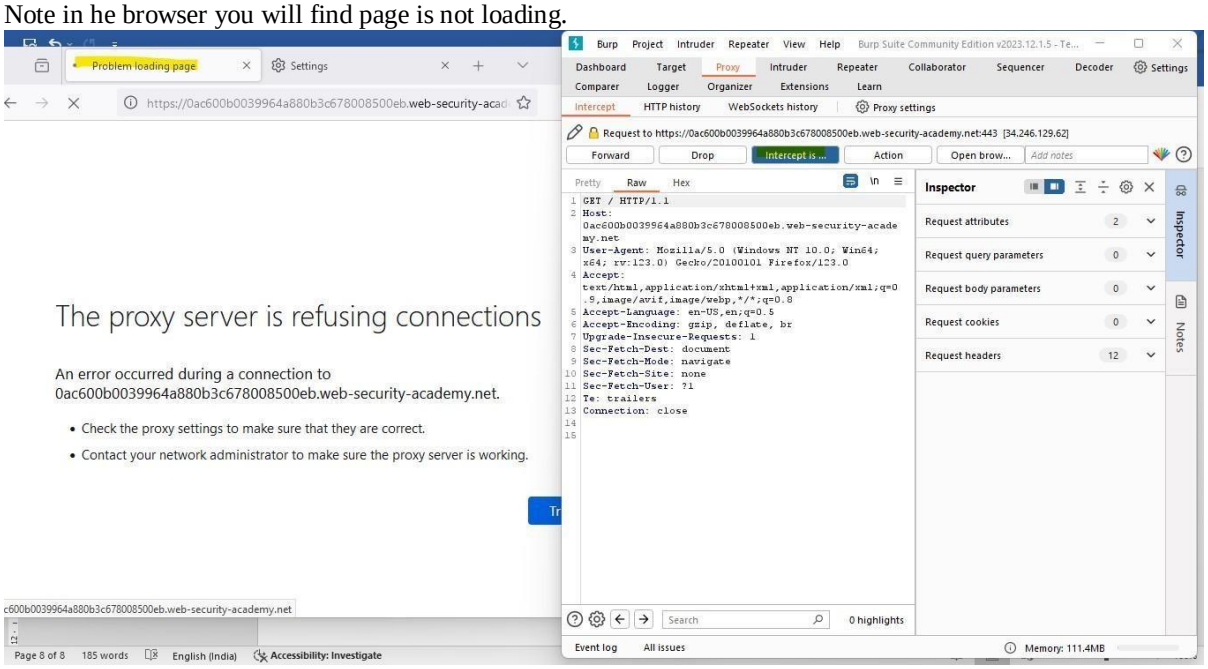
14. go to web security academy, login and select academy go to:
15. scroll dow click on all path button:

15. click on button “resume” on server side validation section:

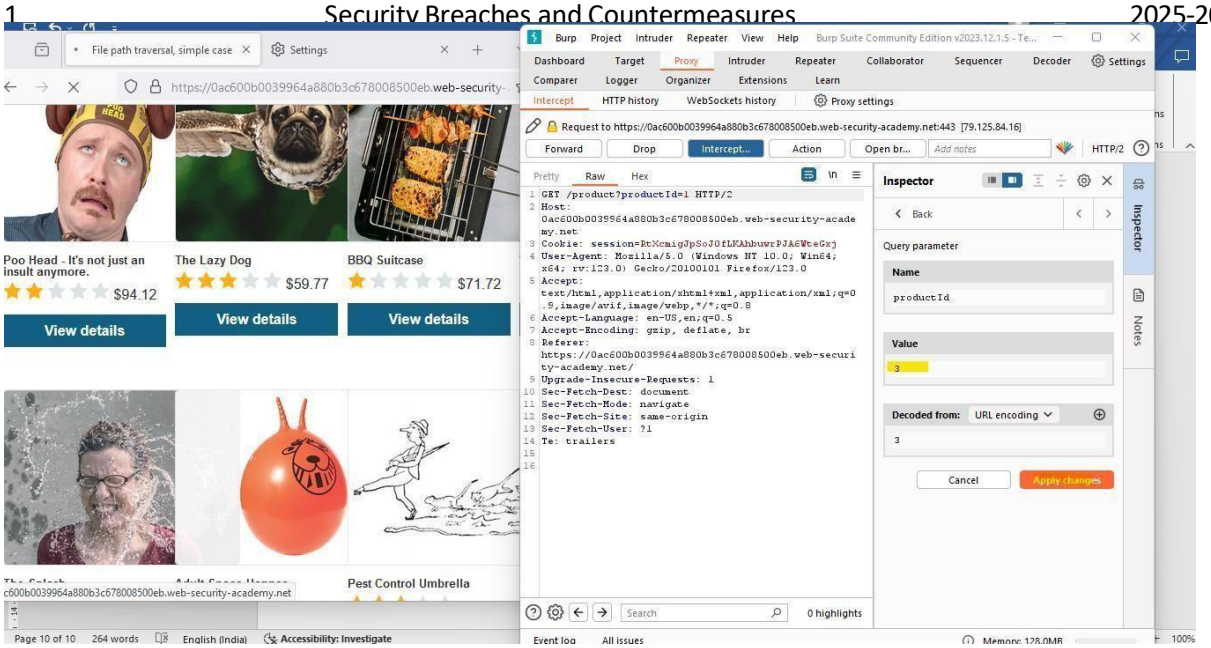


16. click on access Lab:

17. Once the lab is open click on start the interception on in the burp tool.
Note in he browser you will find page is not loading.



18. To load the field click on forward button.
Note you will have to click multiple time to load the entire page.
19. click on the first grid view details button:
20. Click forward on the burb application, go to request query parameter:
21. change the value of the productid to 3. Click on apply changes:

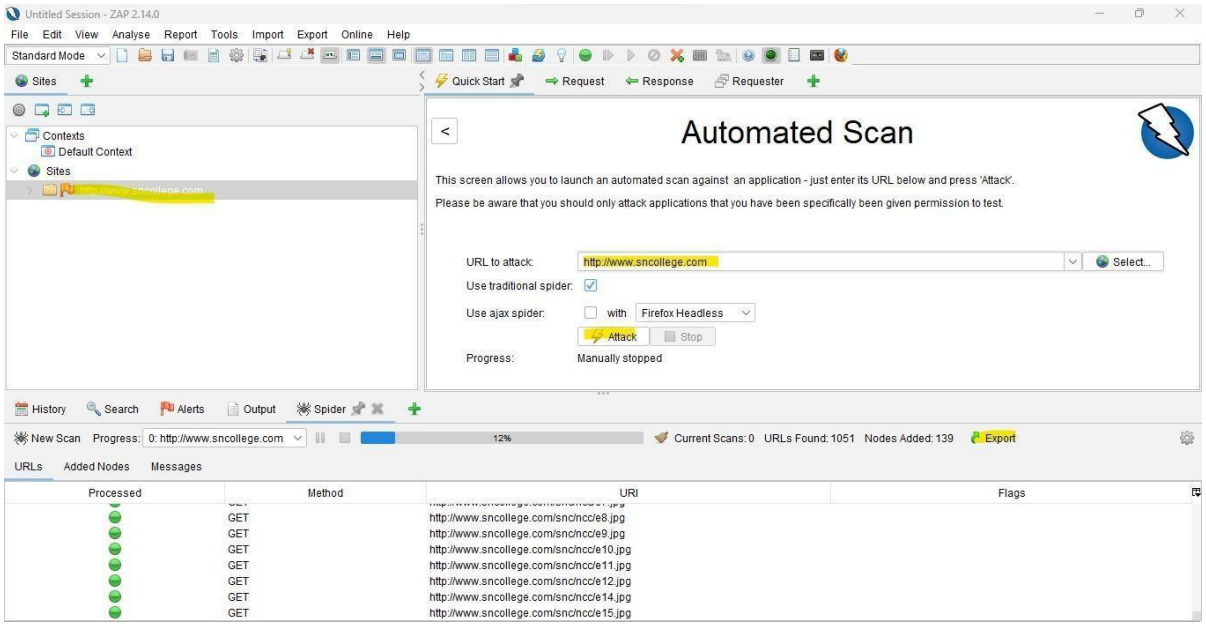


4. Then click on forward you will observe, page for item 3 will open instead of 1.

Section 3 B.

a. a. Perform Web App Scanning using OWASP Zed Proxy.

Step 1. Open Zed Proxy, click on quick start enter he URL and click on attack.



Step 2: go to report generate report, click on generate report:

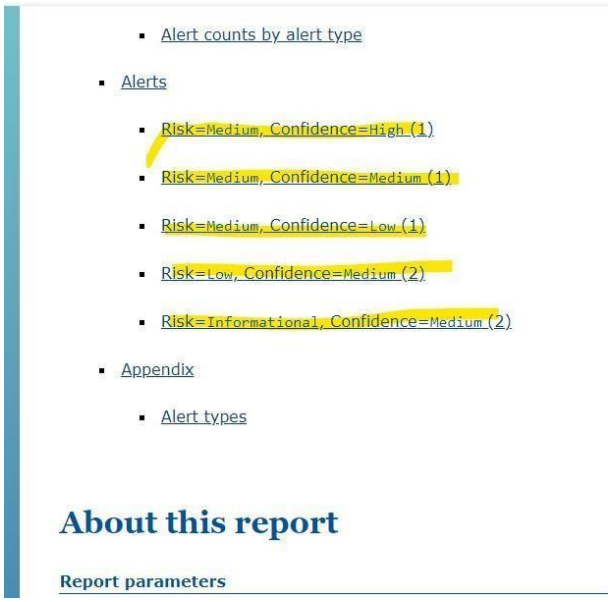
Step 3: Output:

ZAP Scanning Report

Generated with ZAP on Sun 25 Feb 2024, at 05:40:09

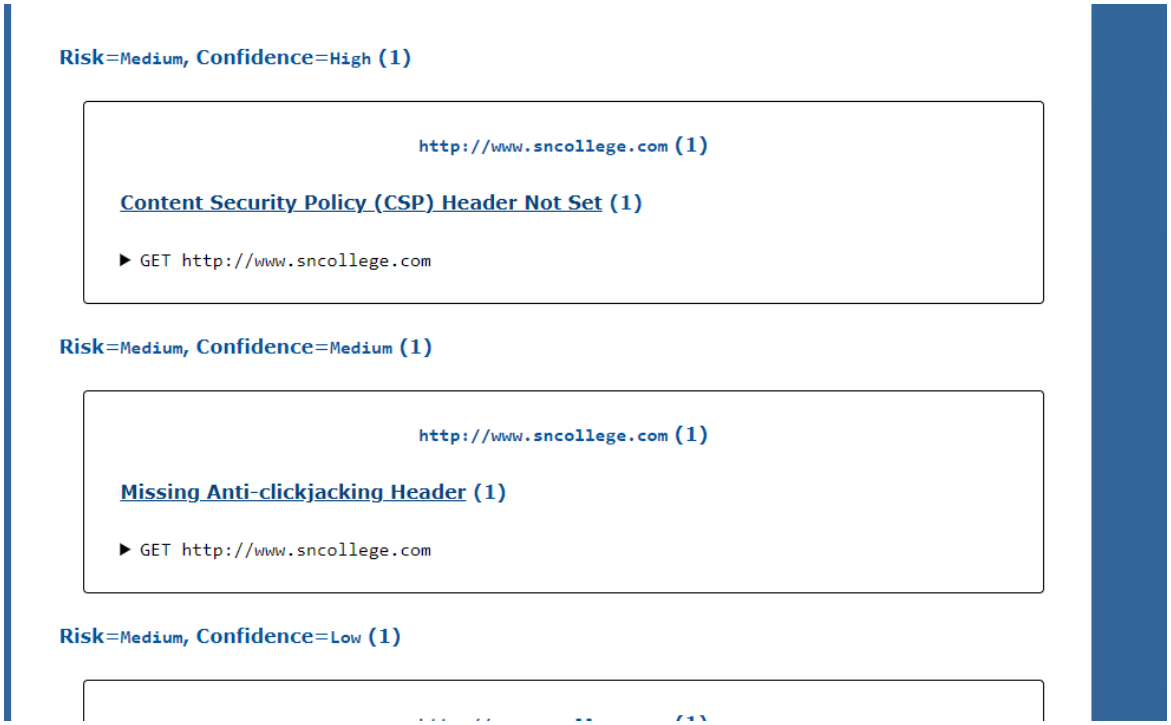
ZAP Version: 2.14.0

Contents



About this report

Report parameters



Risk=Medium, Confidence=High (1)

http://www.sncollege.com (1)

Content Security Policy (CSP) Header Not Set (1)

▶ GET http://www.sncollege.com

Risk=Medium, Confidence=Medium (1)

http://www.sncollege.com (1)

Missing Anti-clickjacking Header (1)

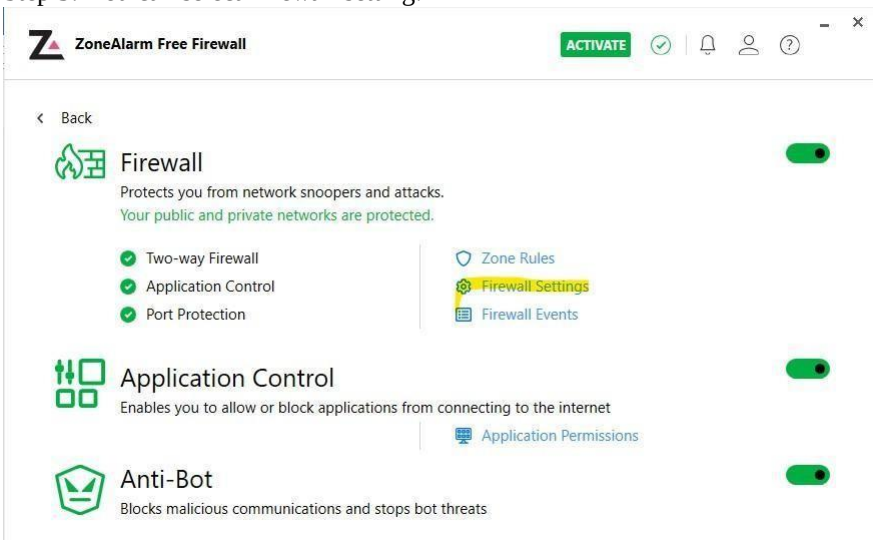
▶ GET http://www.sncollege.com

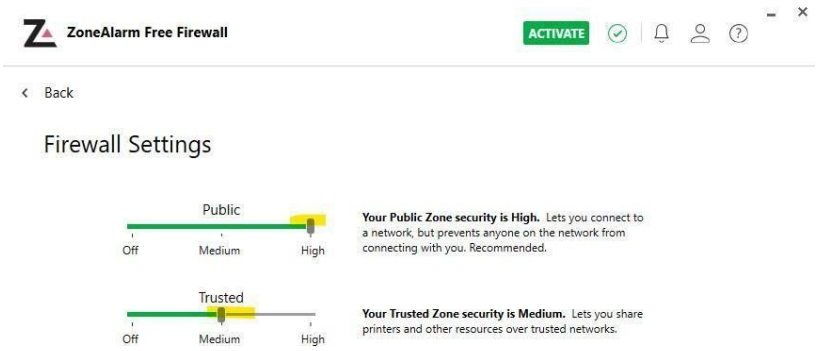
Risk=Medium, Confidence=Low (1)

C. Demonstrate the use of the following firewalls

i. AIM: Zonealarm and analyse using Firewall Analyzer.

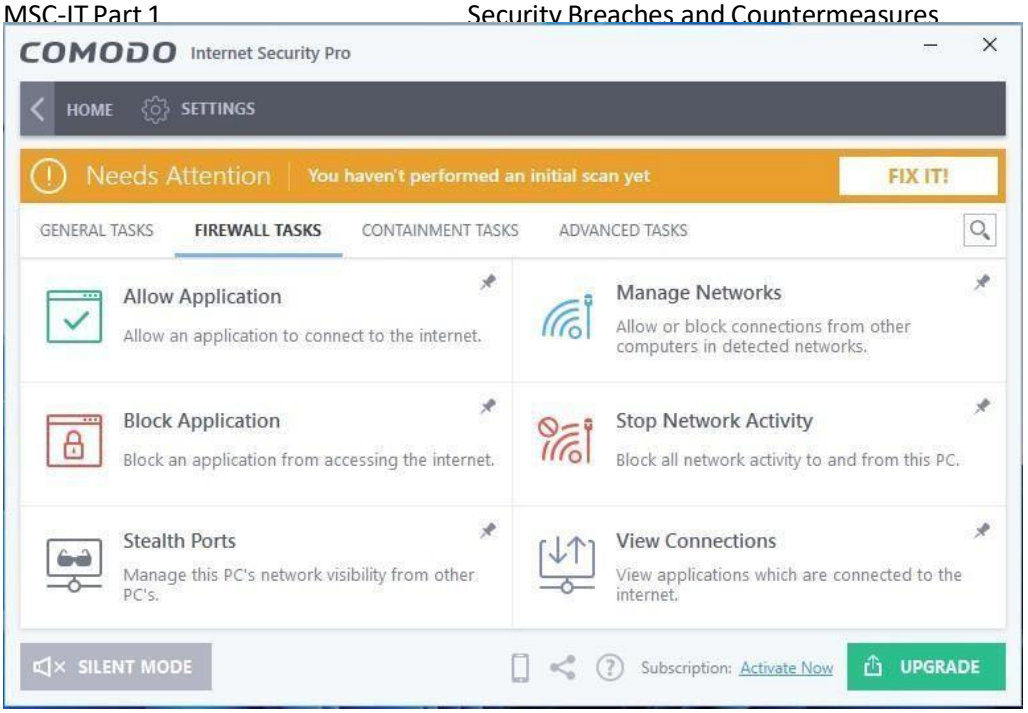
Step1: Open zone alarm, click on firewall:
Step 2: Select Zone Rule: You can add/update new rule:
Step 3: You can select Firewall setting:





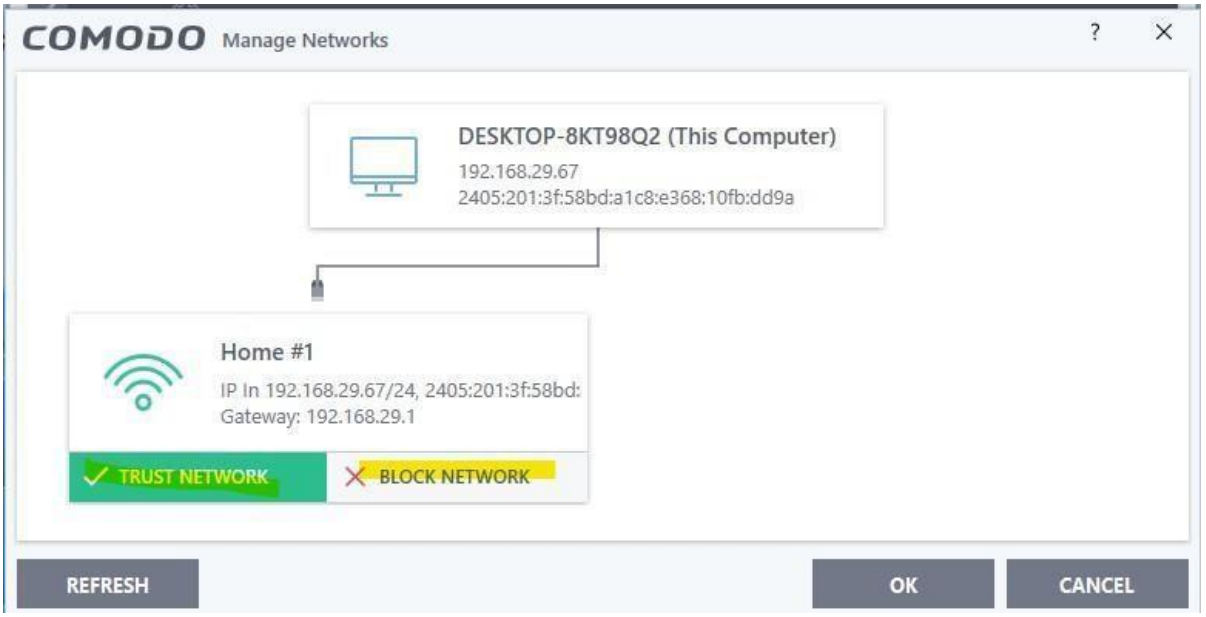
II **Comodo Firewall:**

Step 1: Open comodo-> go to firewall.

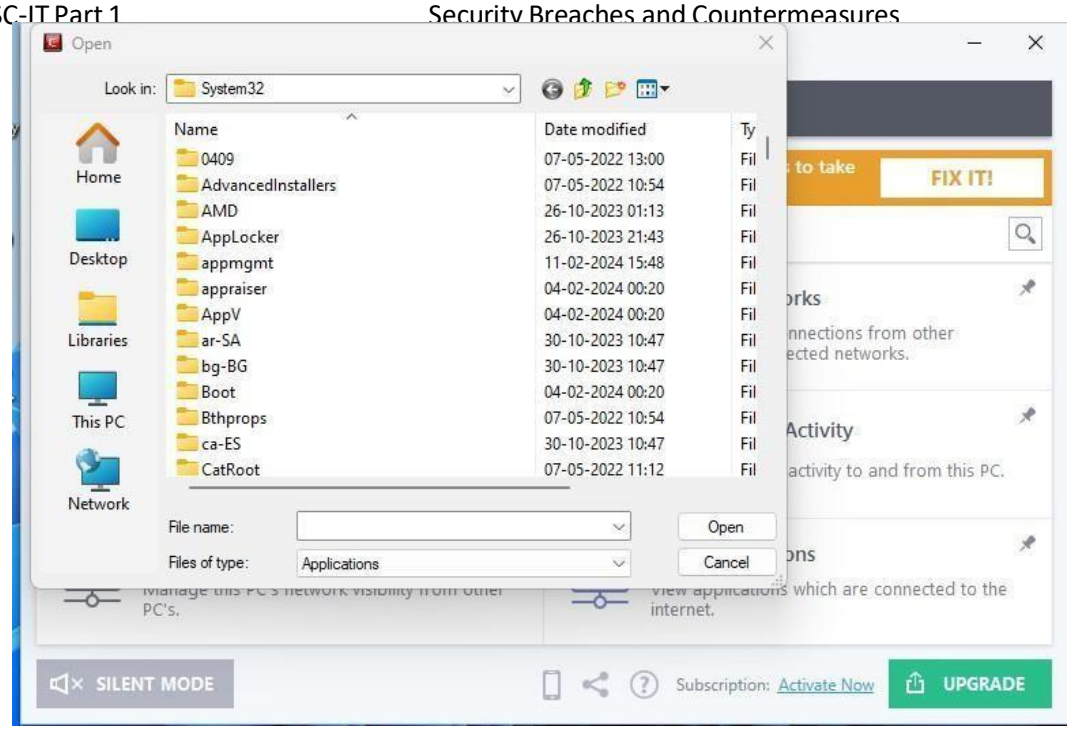


Step 2 : You can select and perform different Network activity like

a. Manage network: Like trust or block any network:



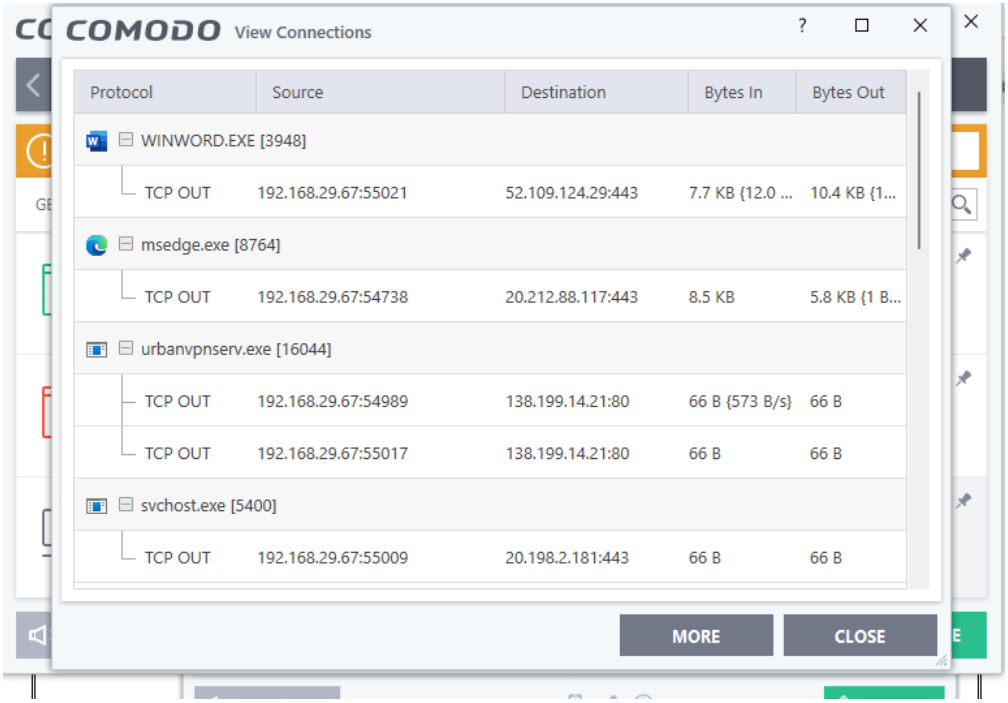
B. allow or block any application by selecting application path:



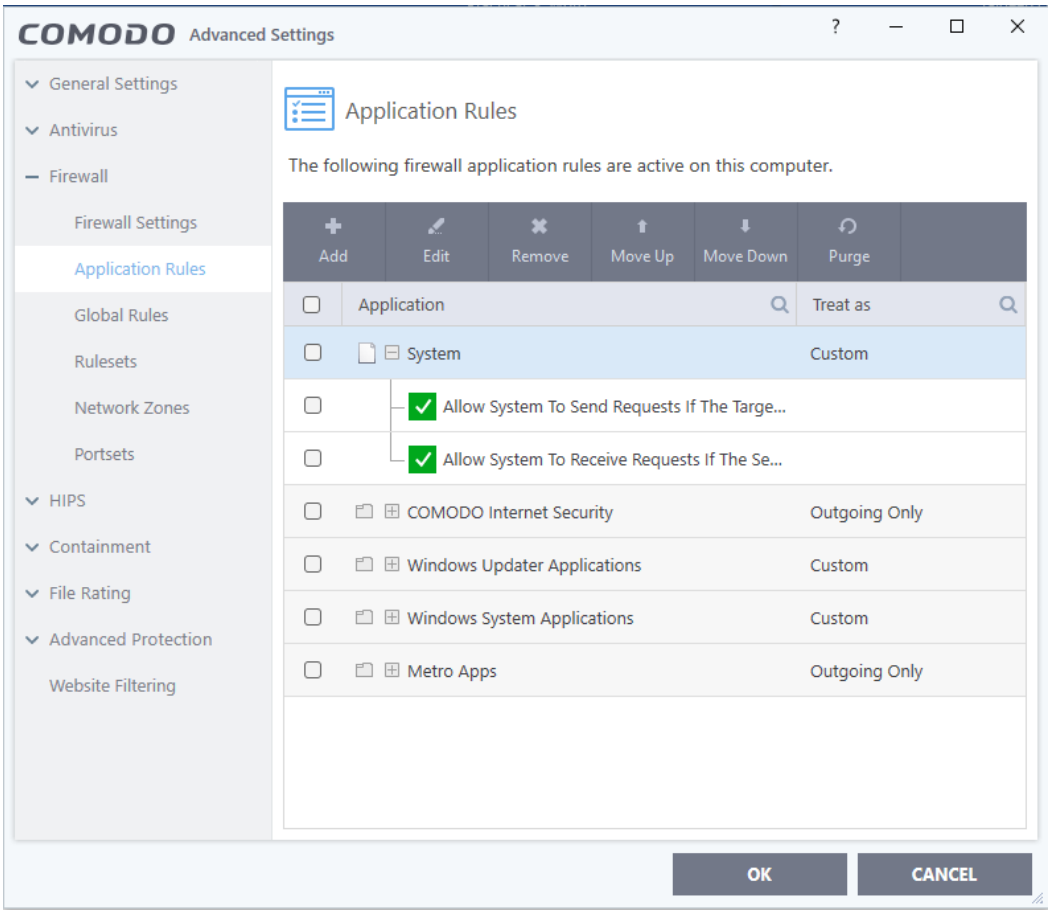
b. Allow or block network traffic in our machine:

c. Sealth mode: allow or block on incoming network:

d. View Connection: View all the connection in the network:

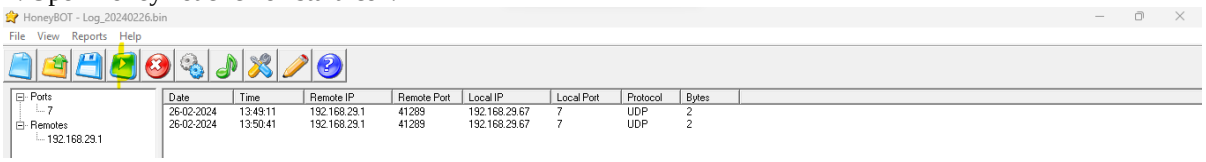


Step 3: Go to firewall setting:

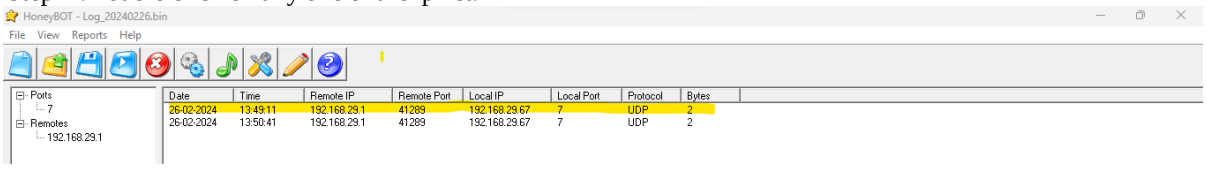


d. Aim: Use HoneyBOT to capture malicious network traffic.

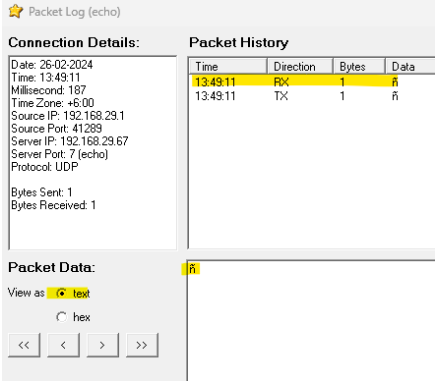
1. Open HoneyBot click on start icon.



Step 2 :Double click on any one of the ip list:



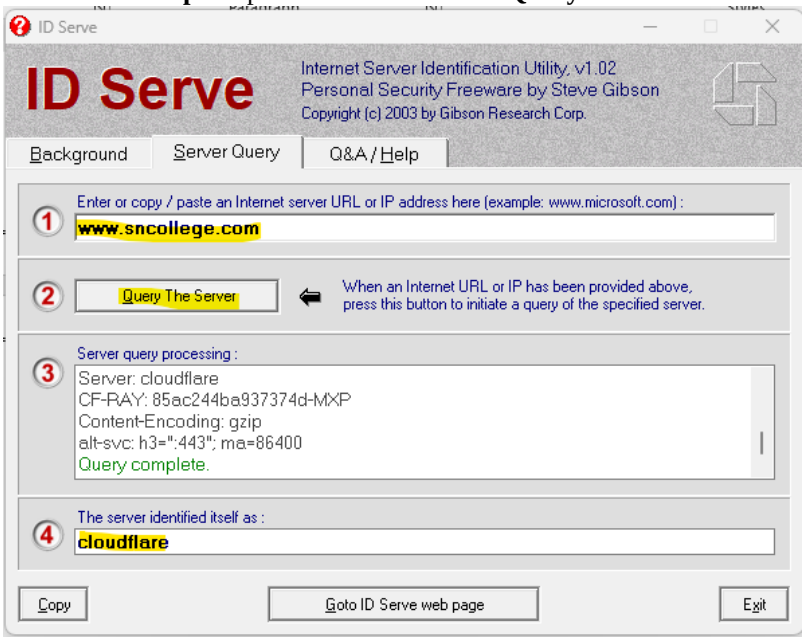
Step 3: Select any of the packet , then select from the option of text or hex format to see the output.



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

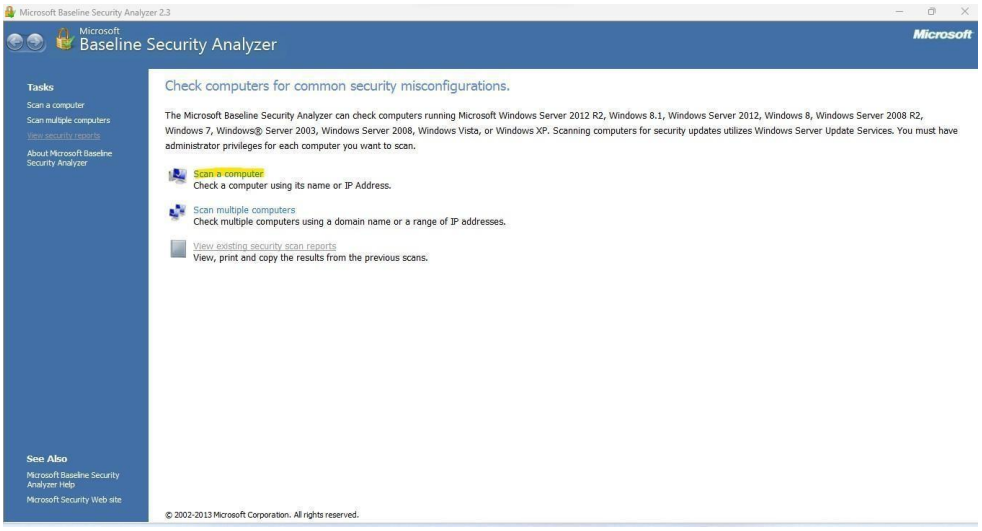
1. **ID Server**

Step 1. Open ID server. Click on "**Query the Server**" button and you will get the server details.



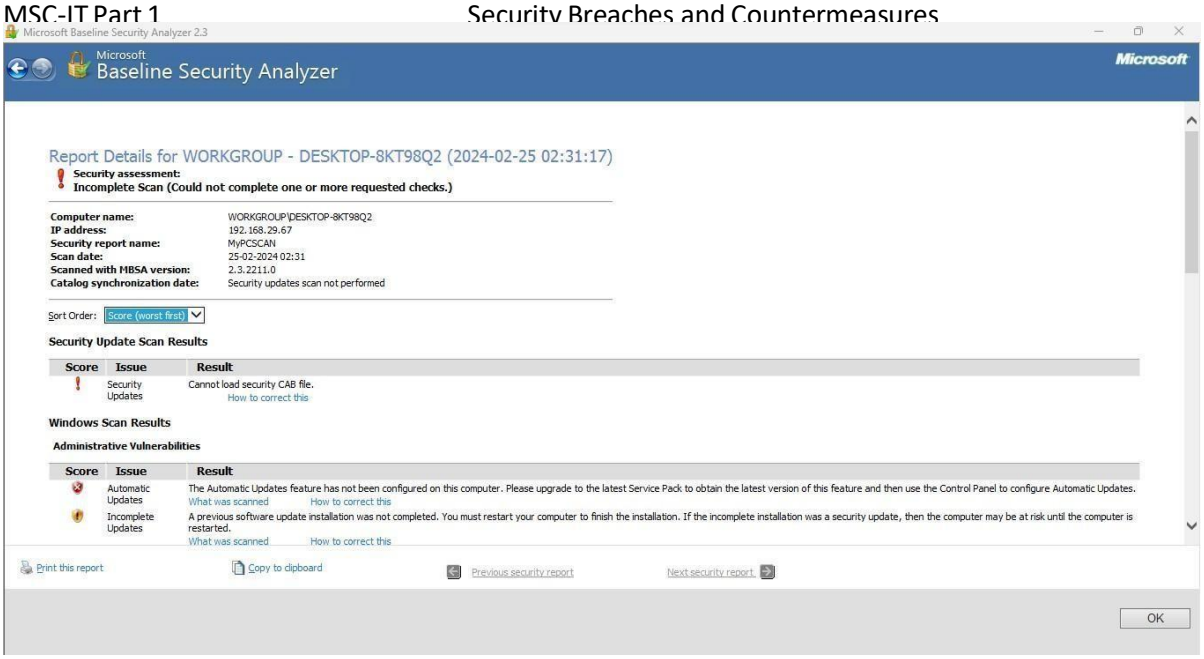
ii. Aim: Microsoft Baseline Security Analyzer

Step 1. Open Microsoft Baseline Security application and click on scan a computer:



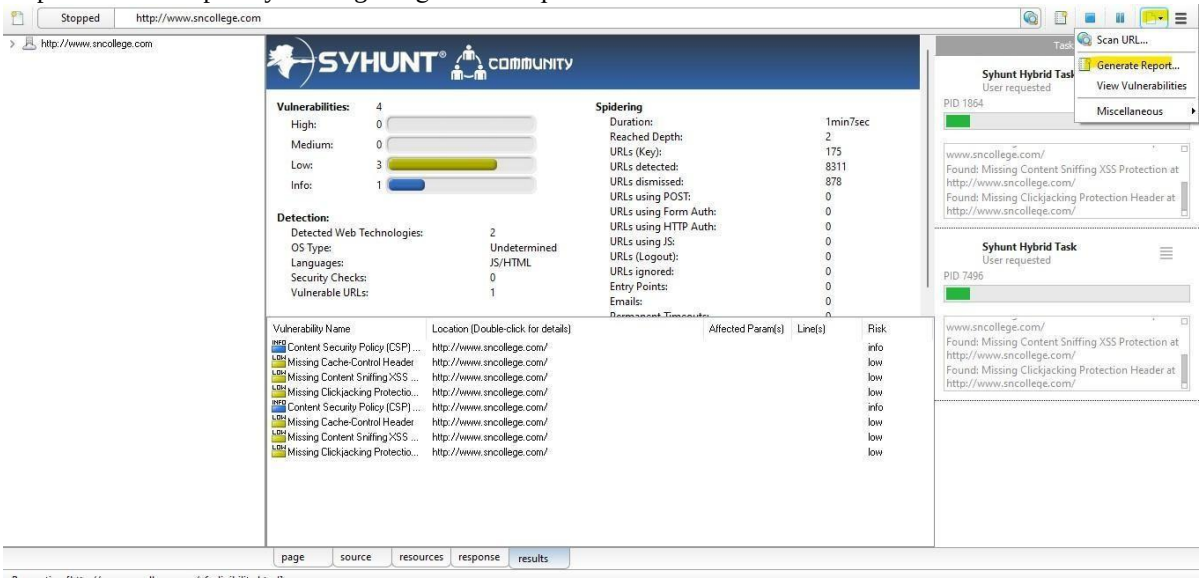
Step 2: Scan the computer or any computer in the network by providing IP, and giving report name. then click on start scan button:

Output: You will get Report for the Scan:

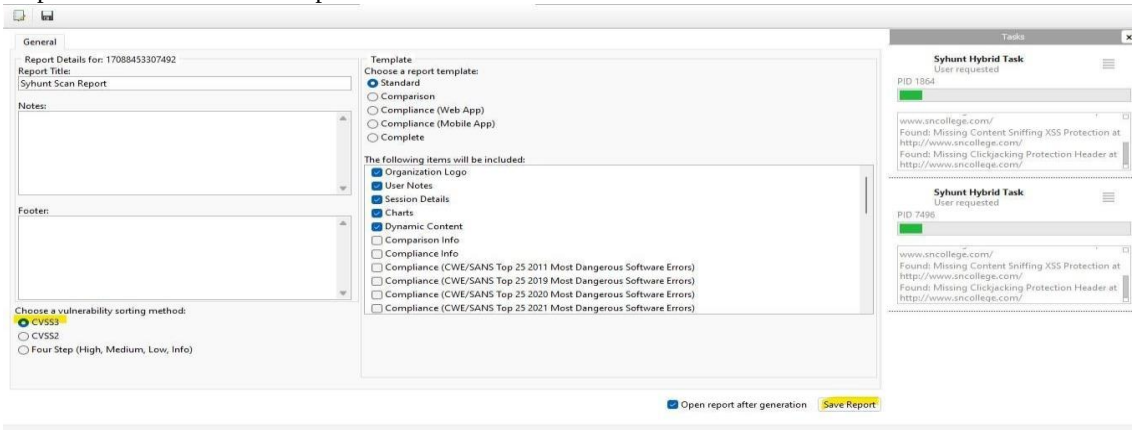


iii. Syhunt Hybri

Step 1: Open Syhunt hunt Appliation -> go to Dynamic Scanner,
Step 2: Insert URL you need to scan and click on “Start” button:
Step 3: Scanning in progress can be seen:
Step 4: Generate report by clicking on “generate Report” button:



Step 5: Select the format or repot and click on Save:



Section 3B

a. Tyrant SQL
Tyrant SQL is a Havij based cross-platform. It's Sqlmap's gui version.
Follow the below process to run the Tyrant SQL :
Step 1. Install below software and package:

->Python 2.7 Site: http://www.python.org/download/releases/2.7.5/

->PySide 1.2.0 Site: http://qt-project.org/wiki/Category:LanguageBindings::PySide::Downloads

Step 2: Run the file from command prompt

Step 3: Use the vulnerable URL in target :
Example: http://redtiger.labs.overthewire.org/level1.php?cat=1

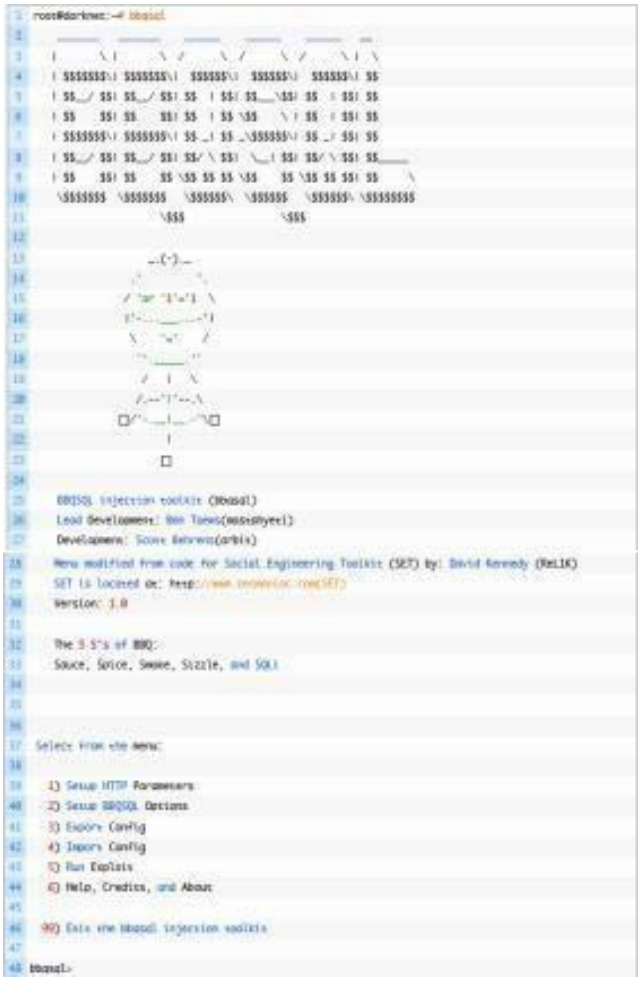
b. **Havij** : Open the Havij Application, in the target add any of the vulnerabilities site. We will be using below venerable URL: http://redtiger.labs.overthewire.org/level1.php?cat=1

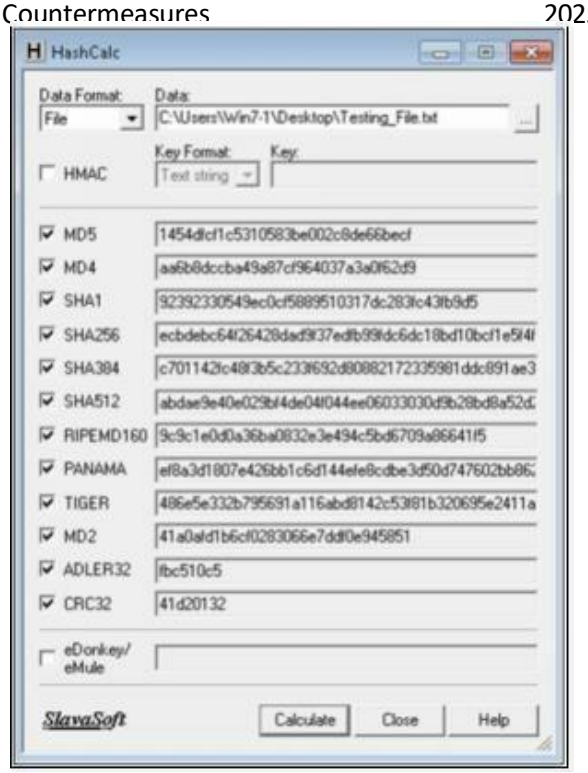
Aim: Use the following tools for cryptography.

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…**"**"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

7. 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.

TrueCrypt:
TrueCrypt is the tool to protect your data.

iv. CrypTool

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