

INDEX

Sr.no	Aim	Date	Page No	Sign
1	A. Use the following tools to perform footprinting and reconnaissance <ul style="list-style-type: none"> i. Recon-ng (Using Kali Linux) ii. FOCA Tool iii. Windows Command Line Utilities <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> 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 Omnipcap 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 sslltools
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”

		Path	Version	Status
	Updated	D K		
led	2020-10-13		1.1	not instal
led	2021-10-04		1.2	not instal
led	2019-06-24		1.0	not instal
led	2019-10-08		1.2	not instal
led	2019-10-08		1.1	not instal
	import/csv_file			

Step2: Use the command to install the package “marketplace install hackertarget”

D = Has dependencies. See info for details.
K = Requires keys. See info for details.

```
[recon-ng][default] > marketplace install hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules ...
[recon-ng][default] >
```

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.

```

Shell No. 1
File Actions Edit View Help
| reporting/proxifier | 1.0 | not instal
led | 2019-06-24 | | |
| reporting/pushpin | 1.0 | not instal
led | 2019-06-24 | | *
| reporting/xlsx | 1.0 | not instal
led | 2019-06-24 | | |
| reporting/xml | 1.1 | not instal
led | 2019-06-24 | | |
+-----+
D = Has dependencies. See info for details.
K = Requires keys. See info for details.

[recon-ng][default] > marketplace install hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules...
[recon-ng][default] > modules load hackertarget
[recon-ng][default][hackertarget] > show options
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|net
blocks|ports|profiles|pushpins|repositories|vulnerabilities>

[recon-ng][default][hackertarget] > options set SOURCE tesla.com
SOURCE => tesla.com
[recon-ng][default][hackertarget] >

```

Step 6: Use command run to execute the scan.

```

Shell No. 1
File Actions Edit View Help
[recon-ng][default] > modules load hackertarget
[recon-ng][default][hackertarget] > show options
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|net
blocks|ports|profiles|pushpins|repositories|vulnerabilities>

[recon-ng][default][hackertarget] > options set SOURCE tesla.com
SOURCE => tesla.com
[recon-ng][default][hackertarget] > run

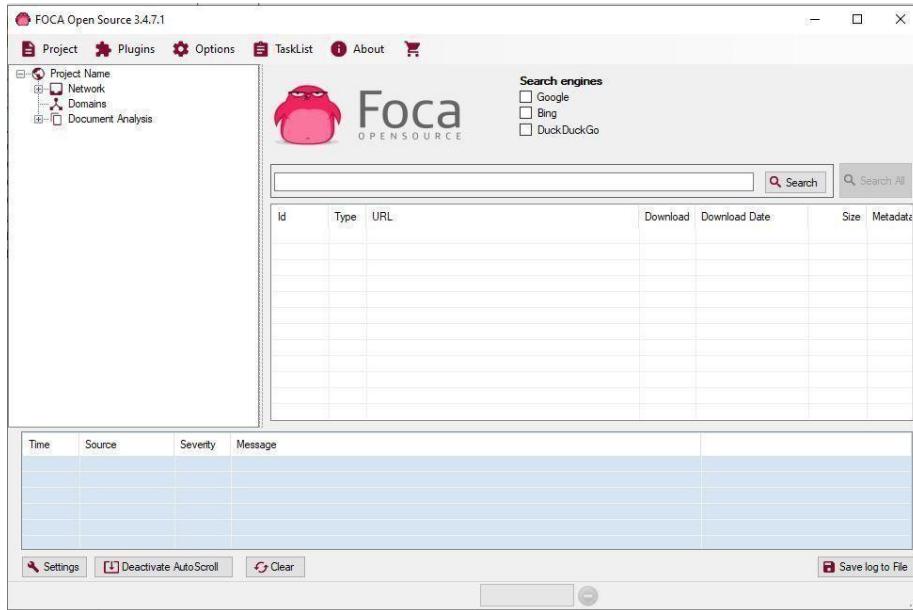
_____
TESLA.COM
_____
[*] Country: None
[*] Host: tesla.com
[*] Ip_Address: 104.85.4.91
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: apacvpn.tesla.com
[*] Ip_Address: 8.244.67.215
[*] Latitude: None
[*] Longitude: None

```

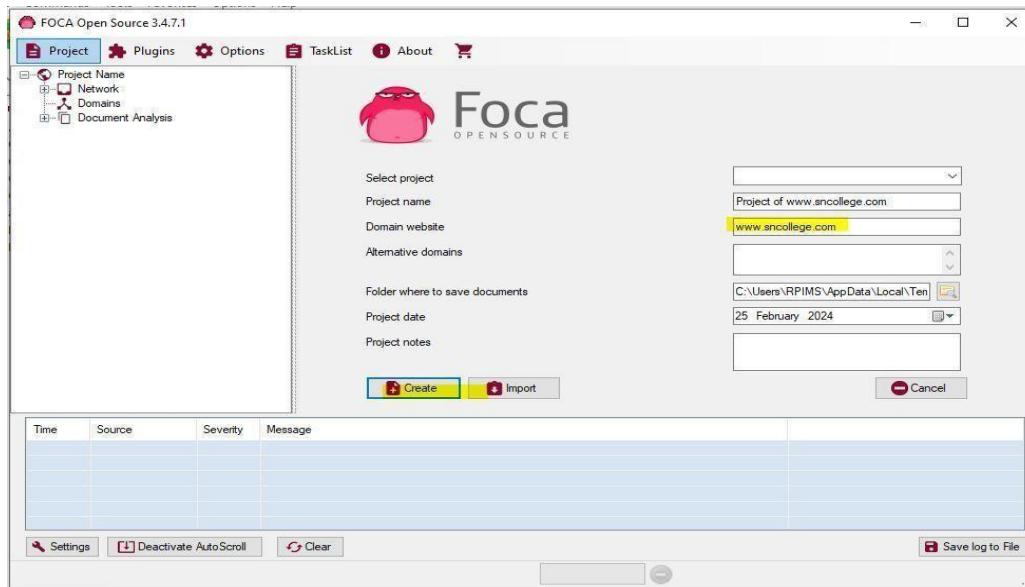
Practical no 2

Aim:- Use of FOCA Tools.

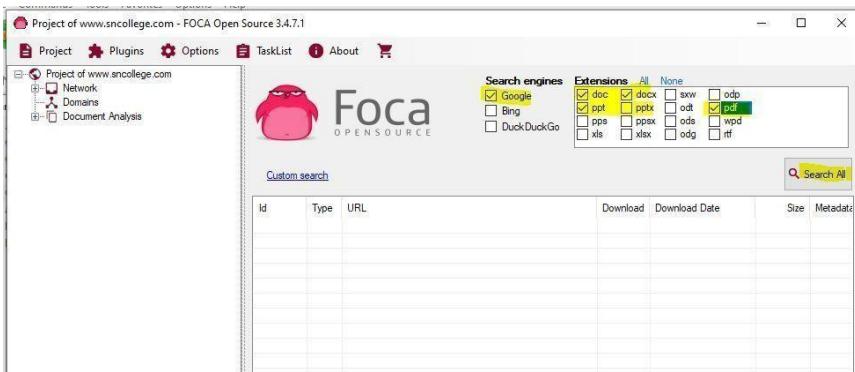
Step 1: Open FOCA Tool, goto project -> select new project.



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.

Time	Source	Severity	Message
11:30:19	MetadataSearch	medium	GoogleWeb search finished successfully!! Total found result count: 303

Practical no 3

Aim : USING TRACE ROUTE

Step 1: Open cmd prompt.

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\Sonali>
```

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

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\Sonali>cd\

C:\>
```

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

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\Sonali>cd\

C:\>tracert www.reddit.com

Tracing route to www.reddit.com [198.41.209.141]
over a maximum of 30 hops:
1  1 ms    <1 ms    <1 ms  192.168.0.1
2  1 ms    1 ms    1 ms  212-1-226-103.intechonline.net [103.226.1.212]
3  2 ms    4 ms    2 ms  249-0-226-103.intechonline.net [103.226.0.249]
4  70 ms   69 ms   68 ms  61.8.56.0
5  67 ms   66 ms   67 ms  be2.wx2.sin0.asianetcom.net [61.14.157.185]
6  65 ms   65 ms   65 ms  gi0-0-0.gw2.sin3.asianetcom.net [61.14.157.170]
7  65 ms   65 ms   65 ms  te0-0-0-4.gw3.sin3.asianetcom.net [202.147.32.10]
11
8  61 ms   61 ms   61 ms  CDF-0014.asianetcom.net [203.192.169.226]
9  63 ms   65 ms   68 ms  198.41.209.141

Trace complete.

C:\>
```

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

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\Sonali>cd\

C:\>tracert 198.41.209.142

Tracing route to 198.41.209.142 over a maximum of 30 hops
1  1 ms    1 ms    <1 ms  192.168.0.1
2  1 ms    1 ms    1 ms  212-1-226-103.intechonline.net [103.226.1.212]
3  2 ms    4 ms    22 ms  249-0-226-103.intechonline.net [103.226.0.249]
4  65 ms   67 ms   69 ms  61.8.56.0
5  65 ms   68 ms   68 ms  be2.wx2.sin0.asianetcom.net [61.14.157.185]
6  67 ms   66 ms   67 ms  te0-0-4.wr1.sin0.asianetcom.net [61.14.157.37]
7  66 ms   65 ms   66 ms  te0-0-0-0.gw3.sin3.asianetcom.net [61.14.157.130]
1
8  173 ms  311 ms  429 ms  CDF-0014.asianetcom.net [203.192.169.226]
9  64 ms   63 ms   73 ms  198.41.209.142

Trace complete.

C:\>
```

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.

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.

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

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 –I switches.
- –n means number of replies to show and –I means obtain reply from the machine in the next hop
- Open command prompt ☐
- Ping certifiedhacker.com –n 1 –I

```
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 certifiedhacker.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

```
D:\>nslookup
Default Server: UnKnown
Address: 192.168.0.1
```

- 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

```
> set type=mx
> certifiedhacker.com
Server: UnKnown
Address: 192.168.0.1

Non-authoritative answer:
certifiedhacker.com      MX preference = 10, mail exchanger = mail.certifiedhacker.com
```

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

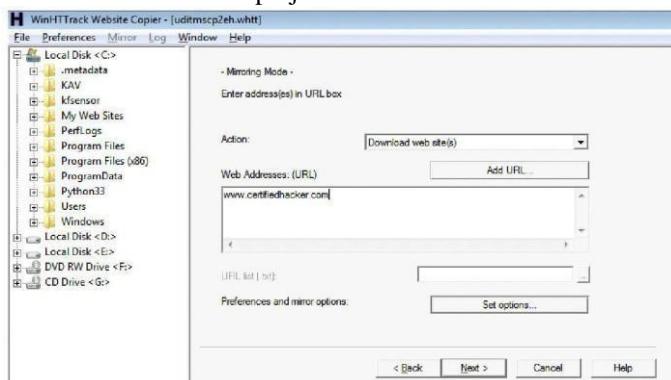
```
> set type=a
> certifiedhacker.com
Server: UnKnown
Address: 192.168.0.1

Non-authoritative answer:
Name: certifiedhacker.com
Address: 202.75.54.101
```

Aim: HTTrack Website Copier

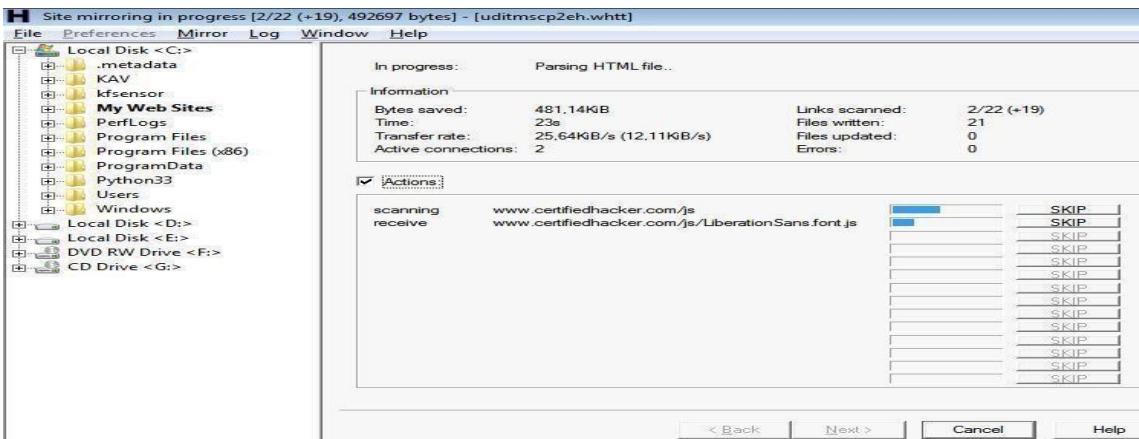
Start > Programs >

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

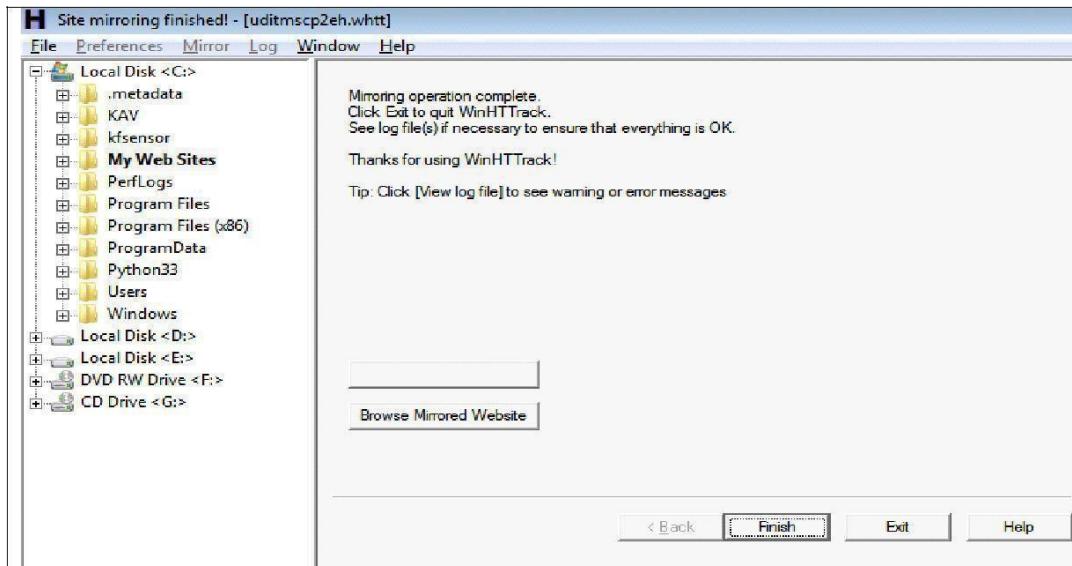


- Click on 'Add URL' and give the URL
- Any additional options that need to be set
- Then click 'Next'
- By default, the radio button will be selected for 'Please adjust connection parameters if necessary', then press FINISH to launch the mirroring operation.

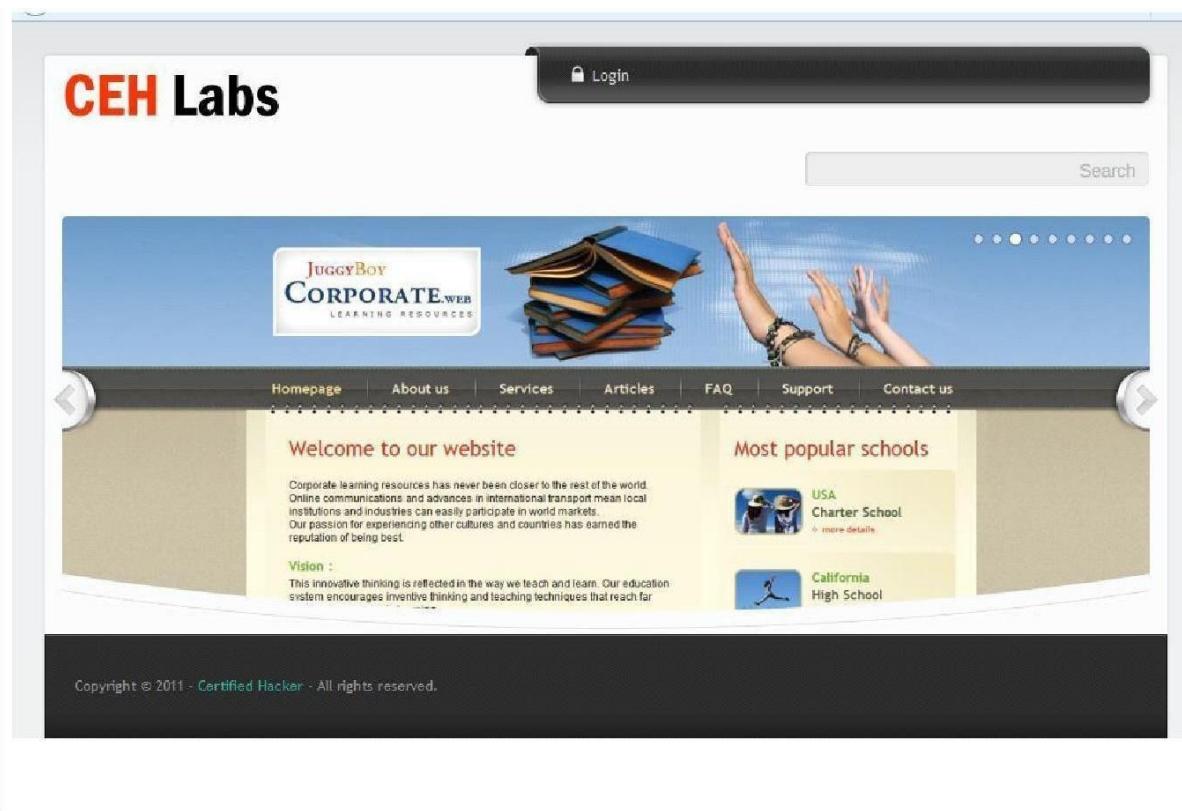
The mirroring of the site now begins. The site will be downloaded and be saved in the C:\My Web Sites\<Project Name>.



- Process of mirroring the website.

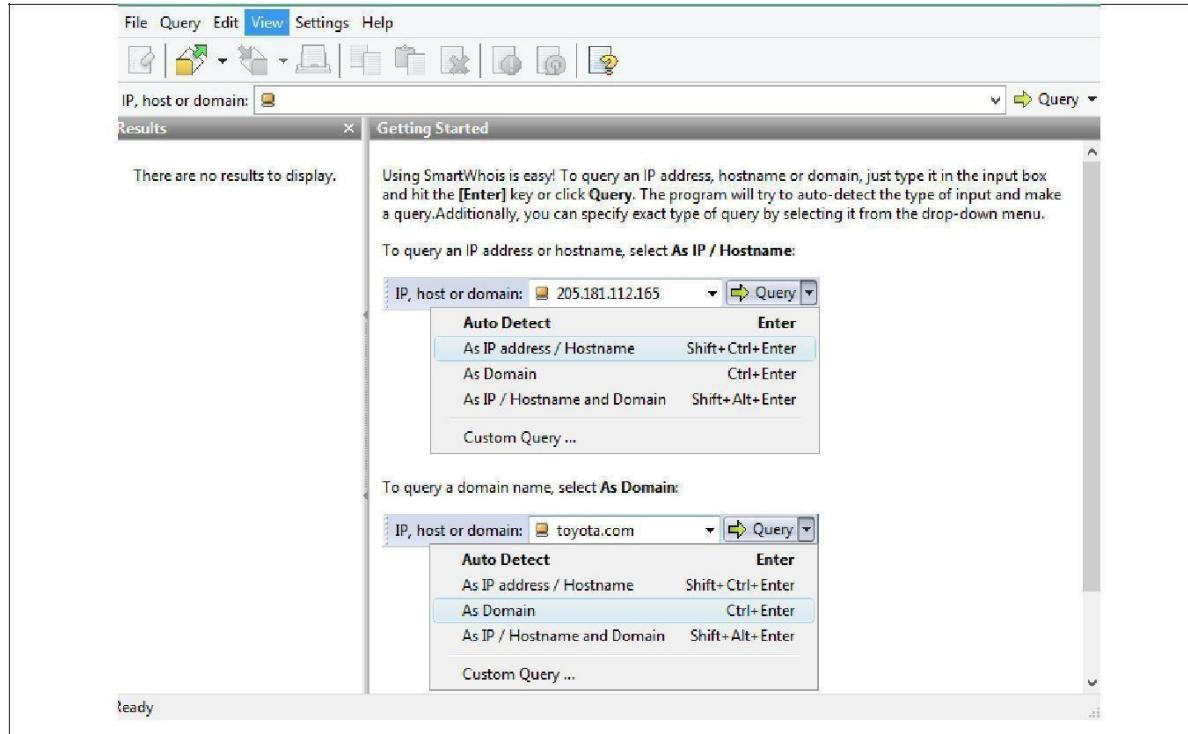


Once the Website Mirroring has been completed, you can click on the Browse Mirrored Website button and then browse the offline copy of the website. □

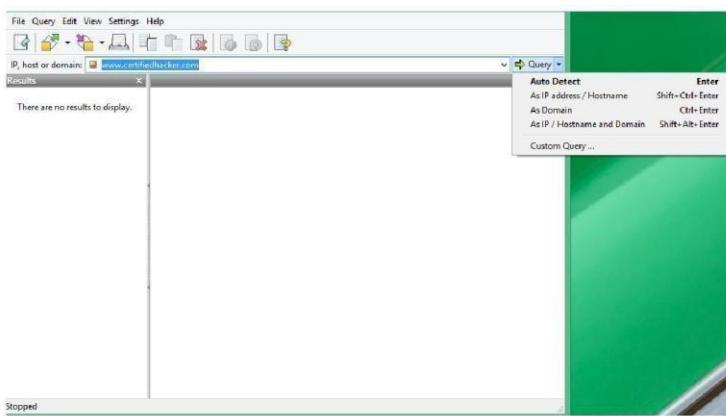


SmartWHOIs

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



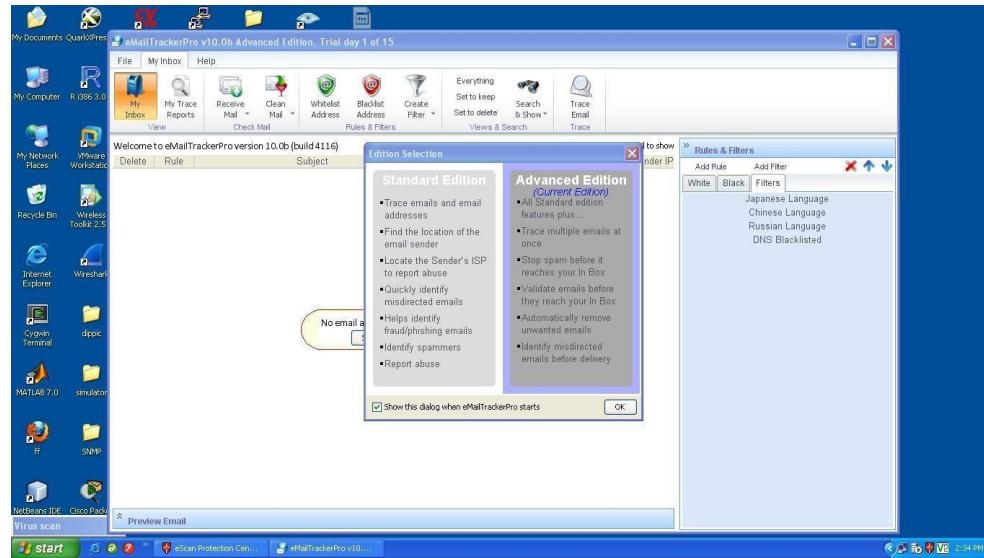
Type an IP address, hostname, or domain name in the address bar



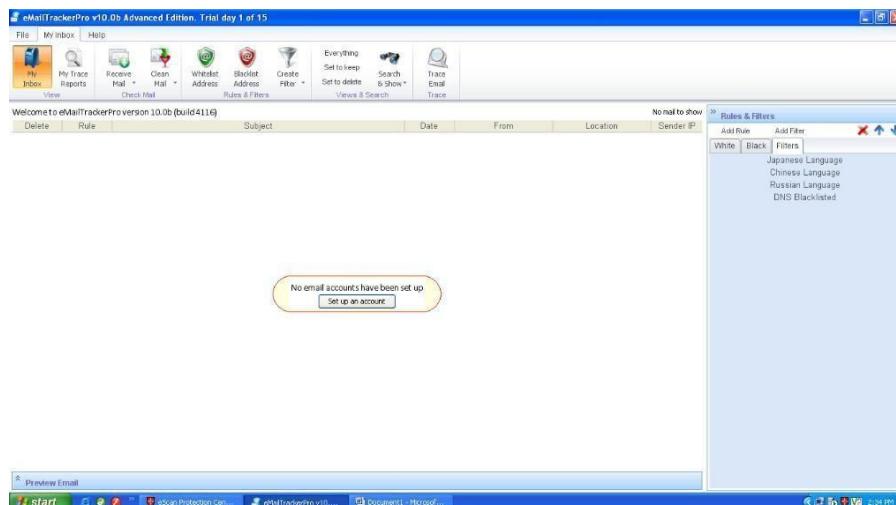
- Different queries will return different results.
- IP Address / Hostname Query results

USING EMAIL TRACKER

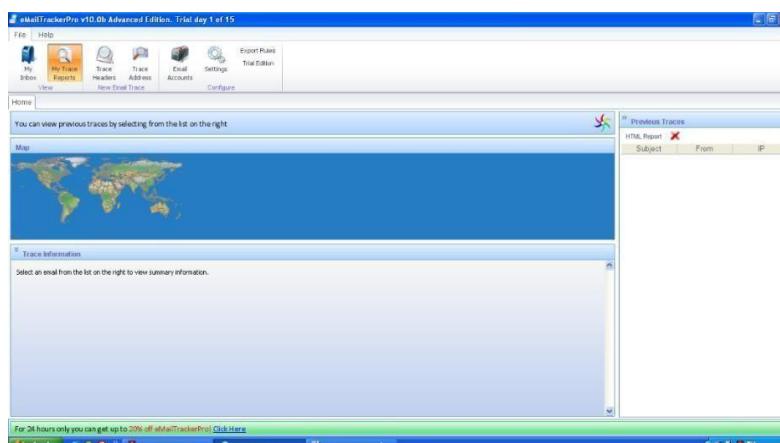
Step 1: Open emailTracker.



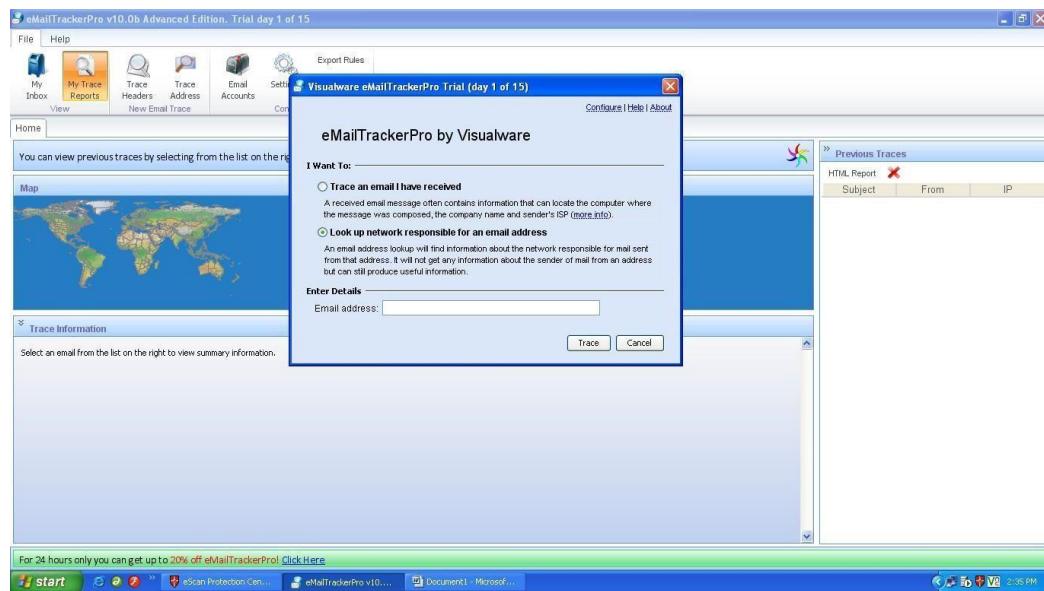
Step 2: Check if there are any reports generated previously.



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.

#	Hop IP	Hop Name	Location
1	182.74.94.9	(India)	
2	59.145.11.109	(India)	
4	72.14.232.202	[America]	
8	209.85.243.21	[America]	
10	74.125.31.27	tb-in-f27.1e100.net	Mountain View, California, USA
11	74.125.31.27	tb-in-f27.1e100.net	Mountain View, California, USA
12	74.125.31.27	tb-in-f27.1e100.net	Mountain View, California, USA

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

eMailTrackerPro Report - Mozilla Firefox

File Edit View History Bookmarks Tools Help

8 Google eMailTrackerPro Report eMailTrackerPro Report

File:///C:/Documents and Settings/Administrator/eMailTrackerPro/V8/reports/report-20140909-1459-6.html

Google

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. This 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 resellers.

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.	Domain Contact Information: The following details refer to a name registered for this address.
 Google Inc.  arin-contact@google.com  +1-650-253-0000  1600 Amphitheatre Parkway Mountain View CA 94043 US	 Administrative Contact Name: Alejandro Martinez Zarate  Administrative Contact Address: Av. Alcalde Barnils, 64-68 Modulo D 4p Administrative Contact City: San Cugat del Valles Administrative Contact Postal Code: 08174 Administrative Contact Country: Spain

start eScan Protection Cen... eh.doc - Microsoft Word eMailTrackerPro v10... tr.doc - Microsoft Word eMailTrackerPro Repo... inail/admin/login.php... 3:00 PM

eMailTrackerPro Report - Mozilla Firefox

File Edit View History Bookmarks Tools Help

8 Google eMailTrackerPro Report

File:///C:/Documents and Settings/Administrator/eMailTrackerPro/V8/reports/report-20140909-1459-6.html

Google

94043 US

City: San Cugat del Valles Administrative Contact Postal Code: 08174 Administrative Contact Country: ES Administrative Contact Email: dominics@grupointercon.com Administrative Contact Tel: +34 935 045600 Administrative Contact Fax: +34 935 045601 Technical Contact Email: 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: +34.933102360 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.



start eScan Protection Cen... eh.doc - Microsoft Word eMailTrackerPro v10... tr.doc - Microsoft Word eMailTrackerPro Repo... inail/admin/login.php... 3:00 PM

The screenshot shows a Firefox browser window displaying a report from eMailTrackerPro. The page is titled "eMailTrackerPro Report - Mozilla Firefox". It contains two main sections: "Network Route Information" and "Domain Owner Information".

Network Route Information:

Address of Hop	Name of Hop	Location
182.74.94.9		India
59.145.11.109		India
72.14.243.42		America
72.14.232.202		America
66.249.94.39		Mountain View, California, USA
209.85.243.245		America
209.85.241.81		America
209.85.243.23		America
74.125.31.27	tb-in-f27.1e100.net	Mountain View, California, USA

Domain Owner Information:

Network Owner Information	Domain Owner Information
<small>This following information refers to the network on which this system lies. This is useful information because it describes who you need to report to if someone on their network has been abusive. (How to effectively report network abuse)</small> <small># ARIN WHOIS data and services are subject to the</small>	<small>The following information describes the organization or individual who registered the domain name 1e100.net. There can be many domain contacts however Corporate and Administrator are usually the best contact references.</small> <small>NOMINALIA INTERNET S.L. - Whois Server Version 1.4</small>

The screenshot shows a Firefox browser window displaying a detailed WHOIS record for the domain **1e100.net**. The page is titled "eMailTrackerPro Report - Mozilla Firefox".

The WHOIS record includes the following details:

- Registrant:** NOMINALIA INTERNET S.L. (<http://www.nominalia.com>)
- Domain Name:** 1e100.NET
- Created On:** 2007-12-14
- Updated On:** 2014-02-07
- Expires On:** 2020-01-25
- Administrative Contact:** JOBISJOB, S.L.
- Contact:** Jobisjob, S.L.
- Registrant Address:** Av. Alcalde Barnils, 64-68 Modulo D 4p
- Registrant City:** Sant Cugat del Valles
- Registrant Postal Code:** 08174
- Registrant Country:** ES
- Administrative Contact Organization:** Alejandro Martinez Zarate
- 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 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:** INC0.DNS.MADREFACT.COM

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 different customized packets in this lab.

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

```
root@kali:~# hping3 -A 192.168.0.1
HPING 192.168.0.1 (eth0 192.168.0.1): A set, 40 headers + 0 data bytes
len=46 ip=192.168.0.1 ttl=128 DF id=24596 sport=0 flags=R seq=0 win=0 rtt=7.8 ms
len=46 ip=192.168.0.1 ttl=128 DF id=24597 sport=0 flags=R seq=1 win=0 rtt=3.7 ms
len=46 ip=192.168.0.1 ttl=128 DF id=24598 sport=0 flags=R seq=2 win=0 rtt=3.5 ms
len=46 ip=192.168.0.1 ttl=128 DF id=24599 sport=0 flags=R seq=3 win=0 rtt=3.4 ms
len=46 ip=192.168.0.1 ttl=128 DF id=24600 sport=0 flags=R seq=4 win=0 rtt=7.3 ms
len=46 ip=192.168.0.1 ttl=128 DF id=24601 sport=0 flags=R seq=5 win=0 rtt=7.2 ms
len=46 ip=192.168.0.1 ttl=128 DF id=24602 sport=0 flags=R seq=6 win=0 rtt=7.1 ms
len=46 ip=192.168.0.1 ttl=128 DF id=24603 sport=0 flags=R seq=7 win=0 rtt=7.0 ms
len=46 ip=192.168.0.1 ttl=128 DF id=24604 sport=0 flags=R seq=8 win=0 rtt=6.9 ms
len=46 ip=192.168.0.1 ttl=128 DF id=24605 sport=0 flags=R seq=9 win=0 rtt=6.7 ms
^C
--- 192.168.0.1 hping statistic ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 3.4/6.1/7.8 ms
root@kali:~#
```

- To create SYN scan against different ports:

root@kali:~# **hping3 -8 1-600 -S 10.10.50.202**

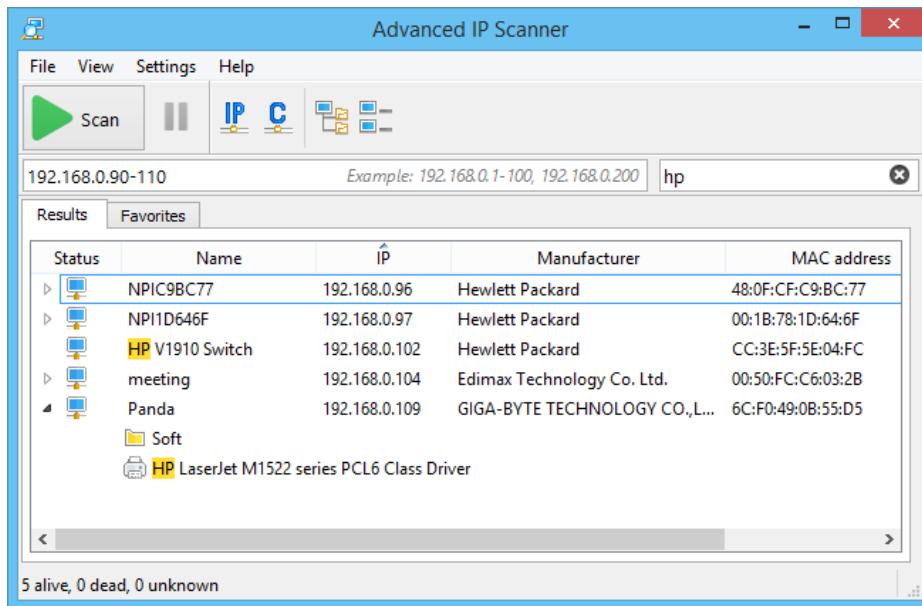
```
root@kali:~# hping3 -8 1-600 -S 10.10.50.202
Scanning 10.10.50.202 (10.10.50.202), port 1-600
600 ports to scan, use -V to see all the replies
+-----+
|port| serv name | flags | ttl| id | win | len |
+-----+
135 loc-srv : .S..A... 128 30572 8192 46
139 netbios-ssn: .S..A... 128 31596 8192 46
445 microsoft-d: .S..A... 128 35180 8192 46
554 rtsp : .S..A... 128 44652 8192 46
All replies received. Done.
Not responding ports:
root@kali:~#
```

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

```
root@kali:~# hping3 -F -P -U 10.10.50.202
HPING 10.10.50.202 (eth0 10.10.50.202): FPU set, 40 headers + 0 data bytes
len=46 ip=10.10.50.202 ttl=128 DF id=28237 sport=0 flags=RA seq=0 win=0 rtt=3.8 ms
len=46 ip=10.10.50.202 ttl=128 DF id=28238 sport=0 flags=RA seq=1 win=0 rtt=3.8 ms
len=46 ip=10.10.50.202 ttl=128 DF id=28239 sport=0 flags=RA seq=2 win=0 rtt=3.5 ms
len=46 ip=10.10.50.202 ttl=128 DF id=28240 sport=0 flags=RA seq=3 win=0 rtt=3.4 ms
len=46 ip=10.10.50.202 ttl=128 DF id=28241 sport=0 flags=RA seq=4 win=0 rtt=3.3 ms
len=46 ip=10.10.50.202 ttl=128 DF id=28242 sport=0 flags=RA seq=5 win=0 rtt=3.2 ms
len=46 ip=10.10.50.202 ttl=128 DF id=28243 sport=0 flags=RA seq=6 win=0 rtt=7.1 ms
^C
--- 10.10.50.202 hping statistic ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max = 3.2/4.0/7.1 ms
root@kali:~#
```

ii. Advanced IP Scanner

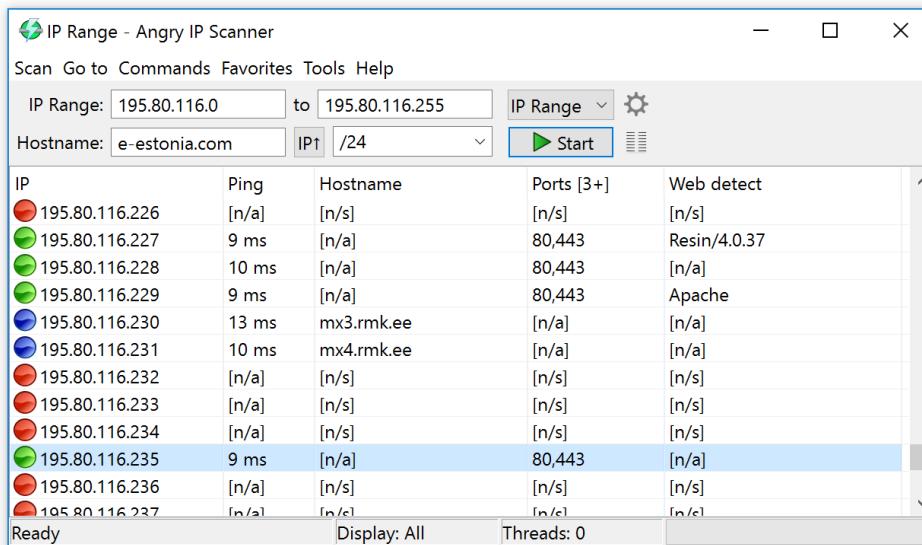
Advanced IP Scanner is a **fast and powerful network scanner with a user-friendly interface**. In seconds, Advanced IP Scanner can locate all computers on your wired or wireless local network and scan their ports. The program provides easy access to various network resources such as HTTP, HTTPS, FTP,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



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 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

i.NEET

Neet is a flexible, multi-threaded tool for network penetration testing. It runs on Linux and coordinates 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.

```
r00t@r00t-Q470C-500P4C: ~/Ktploit/neet 148x51
User Manuals
NEET(1)

NAME
    NEET - Network Enumeration and Exploitation Tool

SYNOPSIS
    neet [OPTIONS] <TARGETS> [<TARGET_RANGE>, <TARGET_RANGE> ...]

DESCRIPTION
    neet is a flexible, multi-threaded network penetration test tool which sits somewhere between manually running your own port scans and subsequent tests, and running a fully automated VA tool. It allows the user to fine-tune the test parameters, and is extensible by means of test modules and plugins. A shell ( neetshell ) is included to help make sense of the results more quickly, and is also used to control the built-in exploitation framework and other aspects of the test.

ADDRESS and PORT SPECIFICATION
    IP addresses can be specified in a couple of ways - range notation (192.168.1.1-254) or CIDR notation (192.168.1.0/24). CIDR notation will automatically exclude the network and broadcast addresses. Nested ranges are also accepted - 192.168.1.10-1.20 for example.

    Port ranges can be included and excluded, and specified in comma and hyphen-separated form. For example, 1,2,3,4-20,50-60,61-70 is acceptable (though inefficient), and will be internally mapped by neet to 1-20,50-70. The default ranges are 1-65535 for TCP scans, and 1-10000 for UDP. Specification of an initial inclusive range on the command line will override these defaults; -t 1-5000 will change the TCP scan range from 1-65535 to 1-5000 for example. Further specifications will then add to this range; -t 6000-8000,10000-11000 will make the total TCP scan range equal to 1-5000,8000-8000,10000-11000.

OPTIONS
    The options and target hosts can be specified in any order. The only rules are that parameters must immediately follow those options which require them, and that targets can be specified by IP address only - no hostnames will be accepted.

    -h, --help
        Displays usage information.

    Target HOST Specification
    -X, --exclude-host <IP_Range>
        Exclude this IP address range (may be specified more than once).
    -f, --include-hosts <File>
        Specify file containing a list of target IP addresses (may be specified more than once).
    -F, --exclude-hosts <File>
        Specify file containing a list of target IP addresses to be excluded (may be specified more than once).
    -L, --list-targets
        Print the list of targets to STDOUT, then exit.
    -O, --exclude-os
        Exclude hosts detected as running the specified operating system (may be specified more than once).

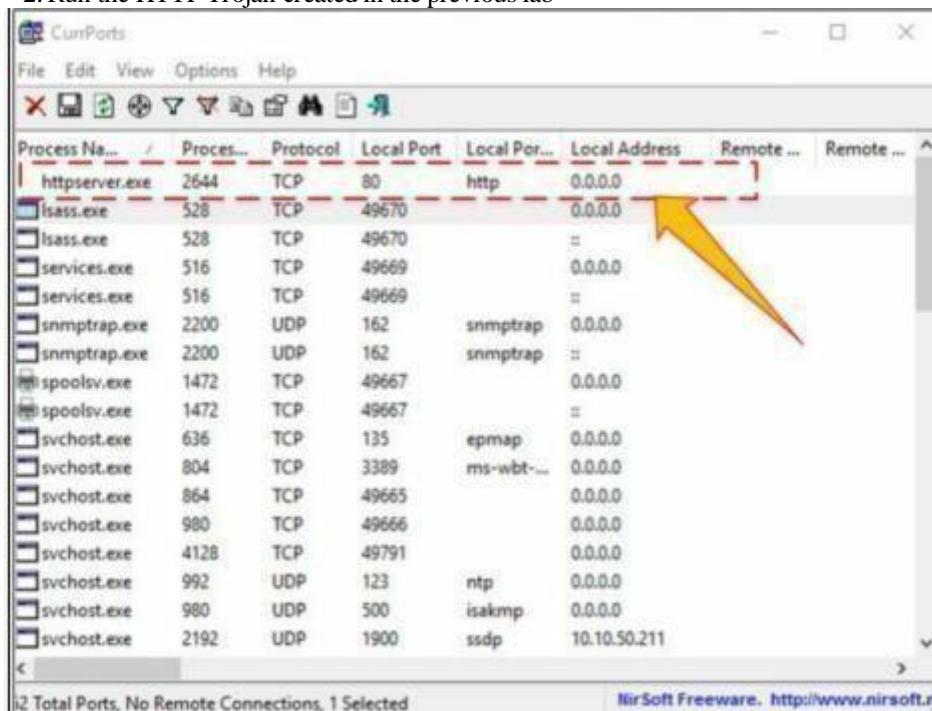
    Target and Service DISCOVERY
    Manual page neet(1) line 1/200 25% (press h for help or q to quit).
```

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:**

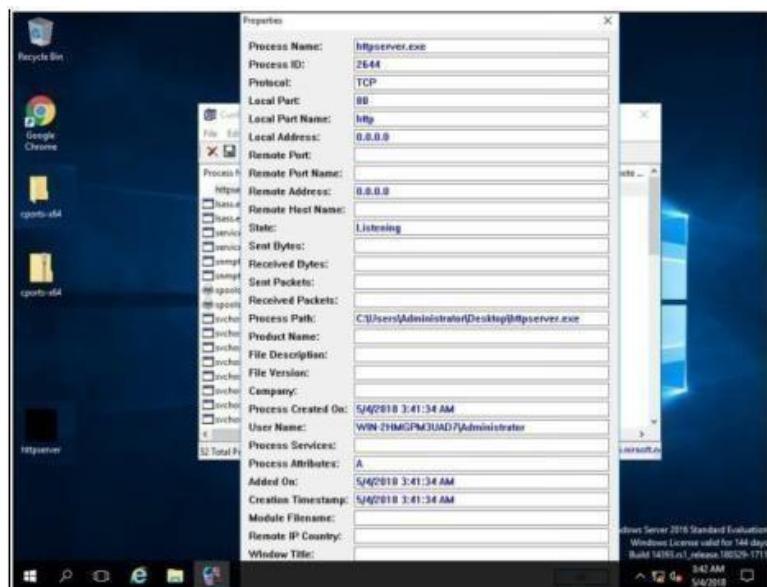
1. Run the application **CurrPorts** on Windows Server 2016 and observe the processes.
2. Run the HTTP Trojan created in the previous lab



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

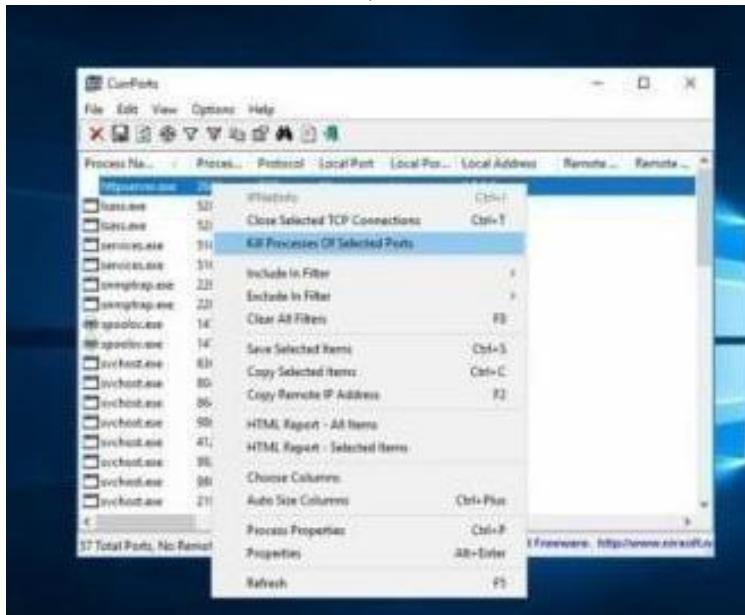


Properties are showing more details about tcp connection.

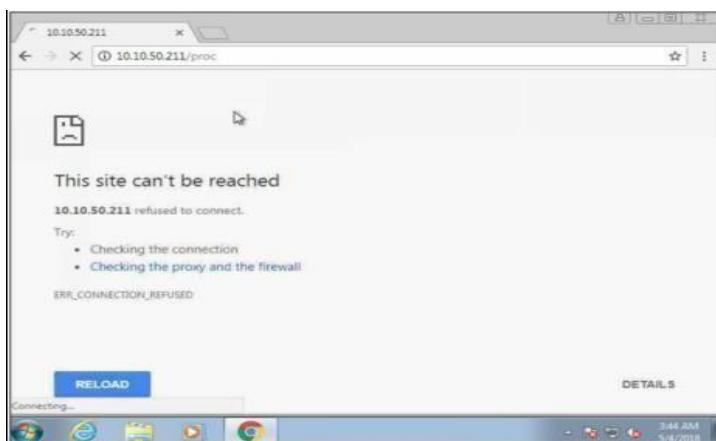
4. Go to Windows 7 machine and initiate the connection as mentioned in the previous lab using a web browser.

Connection successfully established.

5. 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 add a 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.

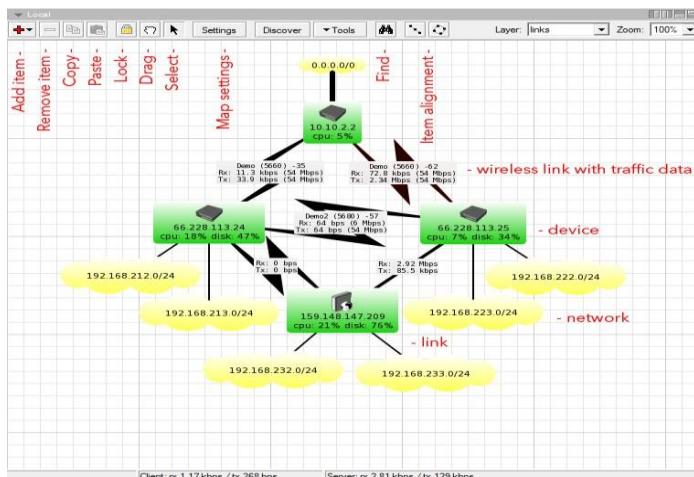
ii. The Dude

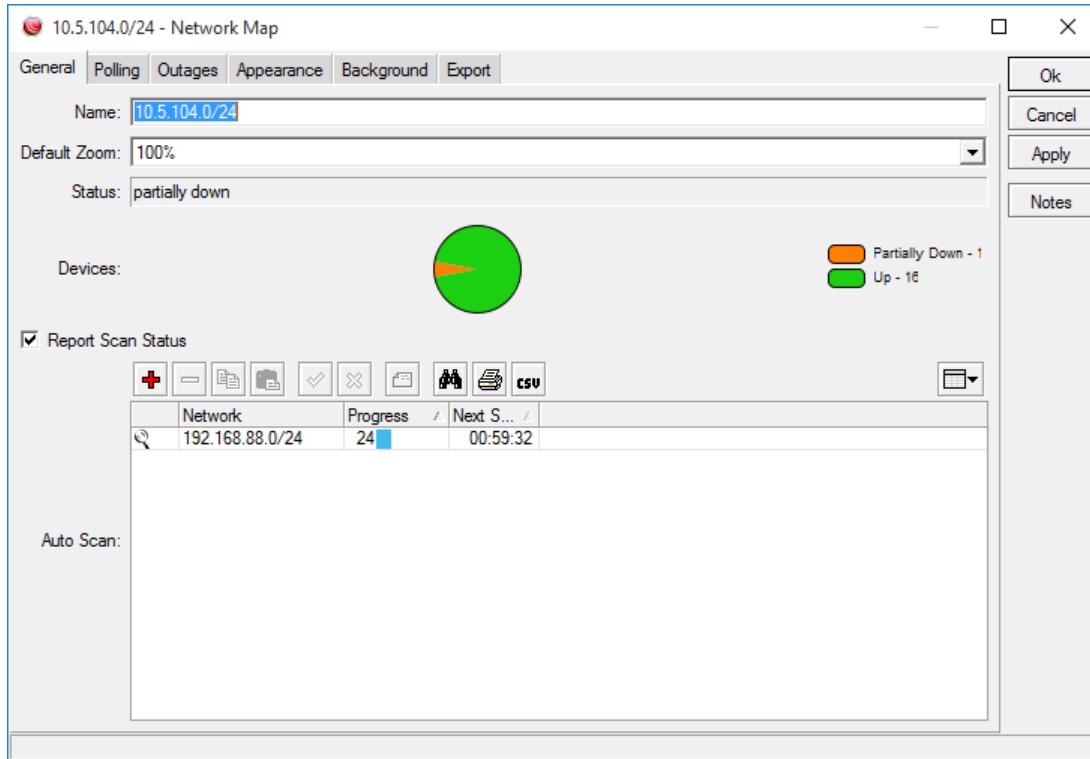
The Dude network monitor is a new application by MikroTik which can dramatically improve the way you manage your network environment. It will automatically scan all devices within specified subnets, draw and layout a map of your networks, monitor services of your devices and alert you in case some service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





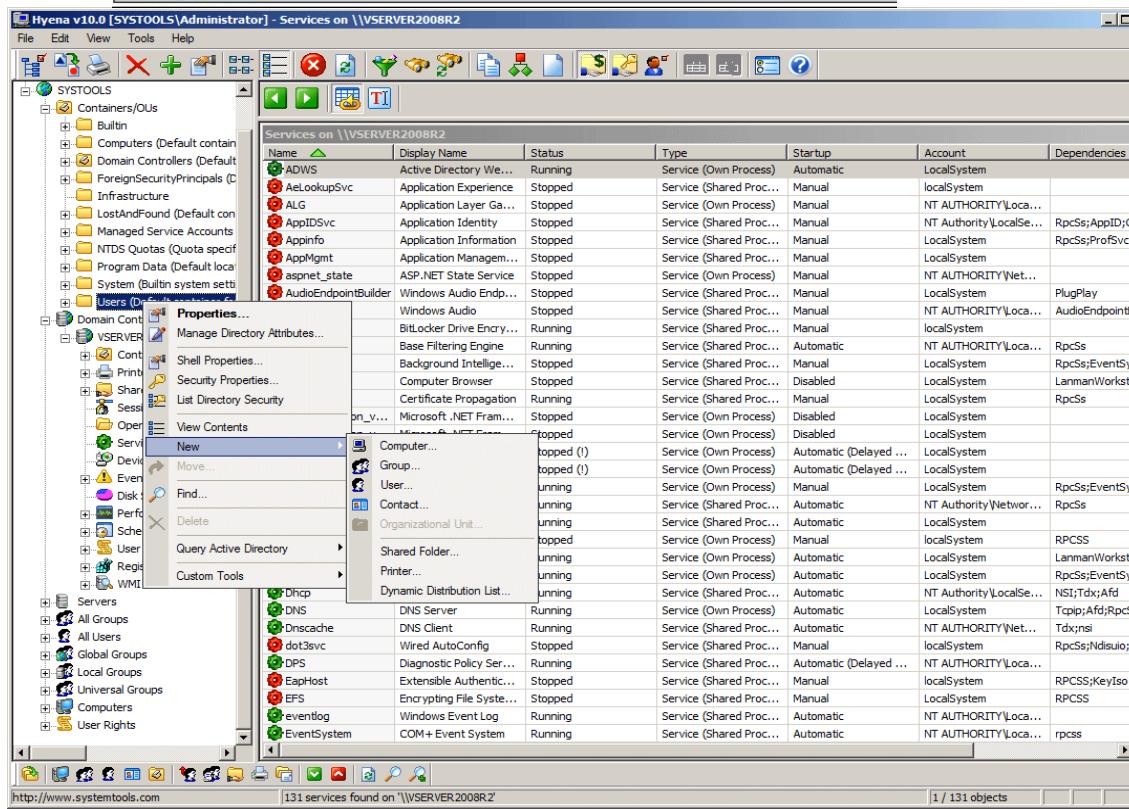
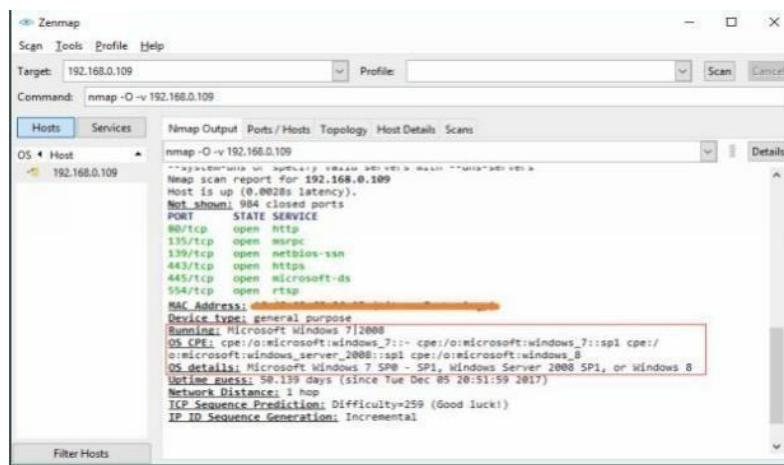
Status	Time	Duration	Device	Service
active	Dec/16 12:49:17	2d 04:39:25	gateway.lan	dns
active	Dec/16 12:49:17	2d 04:39:25	gateway.lan	radius
active	Dec/16 12:49:16	2d 04:39:26	gateway.lan	router
active	Dec/16 12:49:16	2d 04:39:26	gateway.lan	mikrotik
active	Dec/16 12:49:16	2d 04:39:26	gateway.lan	switch
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
resolved	Dec/02 11:22:34	00:03:27	nine.lan	dns

Perform Enumeration using the following tools:

i. Nmap

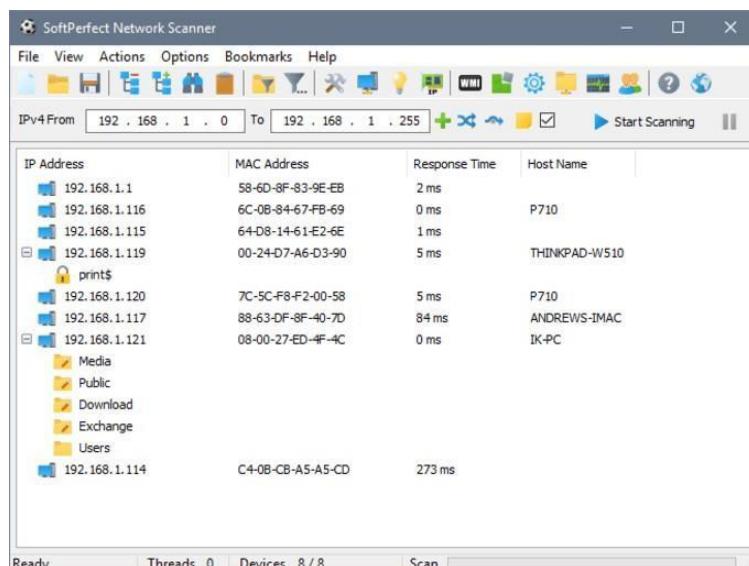
NMAP, as we know, is a powerful networking tool which supports many features and commands. Operating System detection capability allows to send TCP and UDP packet and observe the response from the targeted host. A detailed assessment of this response bring some clues regarding nature of an operating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

```
(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              del112s05-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/notifv
```



j. 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 and PowerShell.

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. OpUtils complements existing management tools by providing trouble shooting and real-time monitoring capabilities.

i. SolarWinds Engineer's Toolset

The screenshot shows the OpUtils interface with the 'Switch Port Mapper' tab selected. On the left, a tree view shows network groups like 'Default Group' and 'ME'. The main panel displays a table of switches with columns for Switch Name / IP, IP Address, DNS Name, Total, Used, Available, Transient, Usage, Status, Last Scan Time, and Sys Name. A status bar at the bottom indicates 'View 1 - 8 of 8'.

Switch Name / IP	IP Address	DNS Name	Total	Used	Available	Transient	Usage	Status	Last Scan Time	Sys Name
11.12.14.1	11.12.14.1	test.server.com	15	14	0	1	93%	Scanned	01 Feb 22, 03:12 PM	sysName
11.12.14.2	11.12.14.2	test.oputils.demo.com	15	14	0	1	93%	Scanned	01 Feb 22, 03:12 PM	sysName
11.12.14.3	11.12.14.3	test.oputils.demo3	15	14	0	1	93%	Scanned	01 Feb 22, 03:12 PM	sysName
11.12.14.4	11.12.14.4	test.demo3.com	15	14	0	1	93%	Scanned	01 Feb 22, 03:12 PM	sysName
11.12.14.5	11.12.14.5	testserver5.spu.com	15	14	0	1	93%	Scanned	01 Feb 22, 03:13 PM	sysName
11.12.14.6	11.12.14.6	oputils.demo1	15	14	0	1	93%	Scanned	01 Feb 22, 03:12 PM	sysName
11.12.14.7	11.12.14.7	test1.oputils.demo.com	15	14	0	1	93%	Scanned	01 Feb 22, 03:12 PM	sysName
11.12.14.8	11.12.14.8		15	14	0	1	93%	Scanned	01 Feb 22, 03:12 PM	sysName
11.12.14.9	11.12.14.9		15	14	0	1	93%	Scanned	01 Feb 22, 03:12 PM	sysName
11.12.14.10	11.12.14.10	switch.dns.com	15	14	0	1	93%	Scanned	01 Feb 22, 03:12 PM	sysName

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.

The screenshot shows the SolarWinds Toolset Launch Pad. The left sidebar lists categories like 'Quick Start', 'My recent tools', 'My favorites', 'All Tools', 'Network Discovery', 'Network Monitoring', 'Configuration Manager...', 'IPAM/DNS/DHCP', 'Diagnostics', 'Log Management', 'General/Other', 'Security', and 'SNMP'. The right side displays six tool cards: 'Advanced CPU Load', 'Bandwidth Gauges', 'CPU Gauges', 'Neighbor Map', 'Netflow Realtime', and 'Network Monitor'. Each card has a brief description and a 'Launch' button.

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 named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.

SECTION 2

Perform the vulnerability analysis using the following tools:

i. Nessus

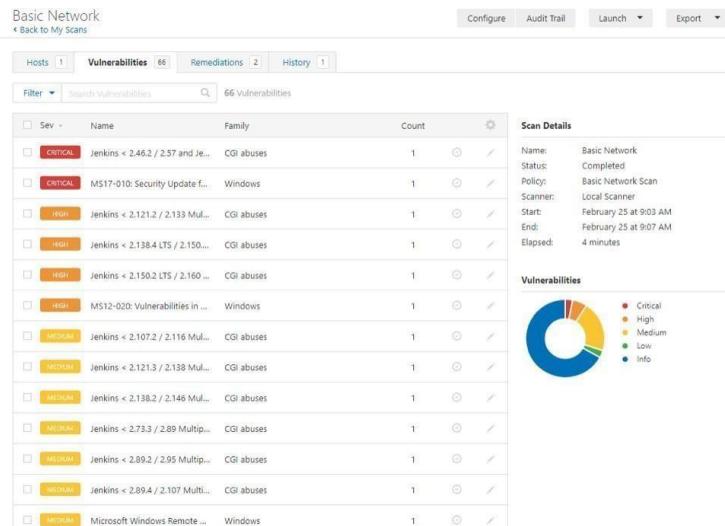
Nessus is a proprietary vulnerability scanner developed by Tenable, Inc. Tenable.io is a subscription-based service. Tenable also contains what was previously known as Nessus Cloud, which used to be Tenable's Software-as-a-Service solution. Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for 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.

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.



Open Web Vulnerability Report

HackerTarget.com

Summary

Scan Started: Wed Feb 13 04:26:48 2019 UTC
Scan Ended: Wed Feb 13 04:41:16 2019 UTC

Any HIGH and MEDIUM severity vulnerabilities should be investigated and confirmed as that named when can take place. LOW level items should not be ignored as they can be combined with other vulnerabilities to enable further attacks.

High	Medium	Low	Total
3	4	0	7
3	4	0	7

Schedule a new OpenVAS Scan

TARGET ADDRESS:
IP address(es) or Hostname(s):

Card format: 192.168.168.168 :: hostname.com :: multiple targets in list

ADD LABEL:

Optional label for identifying scan (used in results and email notifications)

SCANS:

Full Server Scan

RECORDED:

Monthly on the 3rd

00:00:00 UTC

08:00

Date of day selected on UTC, current server time is 08:53

OpenVAS Vulnerability Report

Summary
This host is running Perl/Tk Web Protocol Server and is prone to information disclosure vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method

Impact
Successful exploitation could allow remote attackers to gain sensitive information.
Impact score: 4.8 / 10

CVSS Score

CVSS Score	Impact
9.0	1
9.0	2
5.0	1
4.8	1
4.0	2

Solutions
Solution type: Remote Fix
The solution or patch was made available for at least one year prior to disclosure of this vendor-specific vulnerability.
Please provide an update. Generic exploit scripts are available to a newer version, please replace the exploit with the latest version.
A patch is present in the most recent build of the software or module.

Affected Software:
All discovered computers (OS's) or exploit software

Vulnerability Details
This flaw is due to RD's server which stores an RSA private key used for signing a terminal server's public key in the memory of servers, which allows remote attackers to capture a valid logon pre-auth token and perform a man-in-the-middle (MitM) attack to obtain sensitive information.

Vulnerability Detection Method
Details: Microsoft IIS Server Fails to Sanitize Key Information (via Secure VNC via RDP)
1.1.0.1.4.1.2.256.11.3.0.9039188
Version used: Microsoft 10409

References

- CVE: CVE-2009-1194
- BID: 33858
- Other: Microsoft Security Bulletin MS09-027

All discovered issues are given a severity rating and detailed for remediation / mitigation.

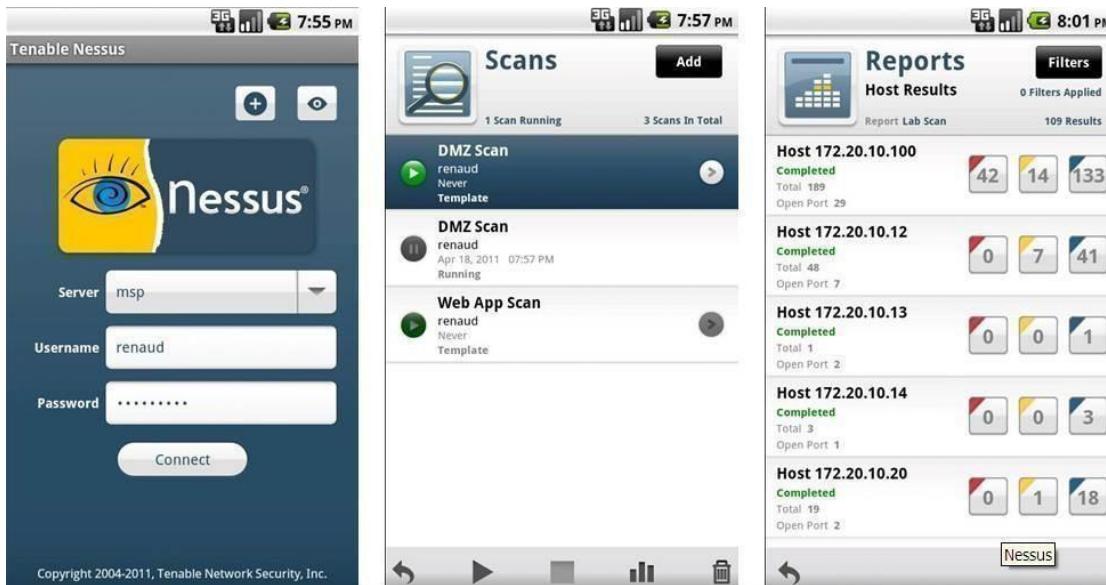
Practical No. 4

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 DeviceManagement 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**”

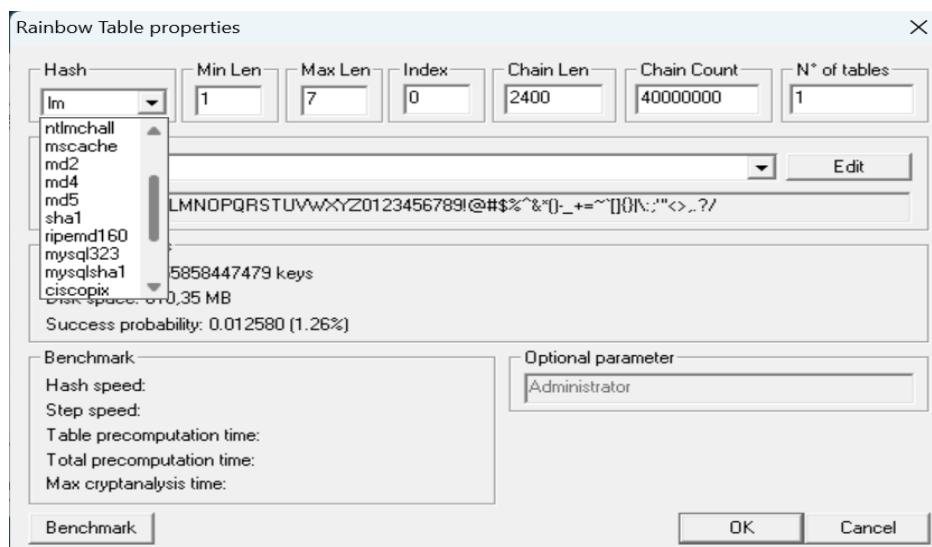
c. Perform the System Hacking using the following tools:

ii. Winrtgen

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

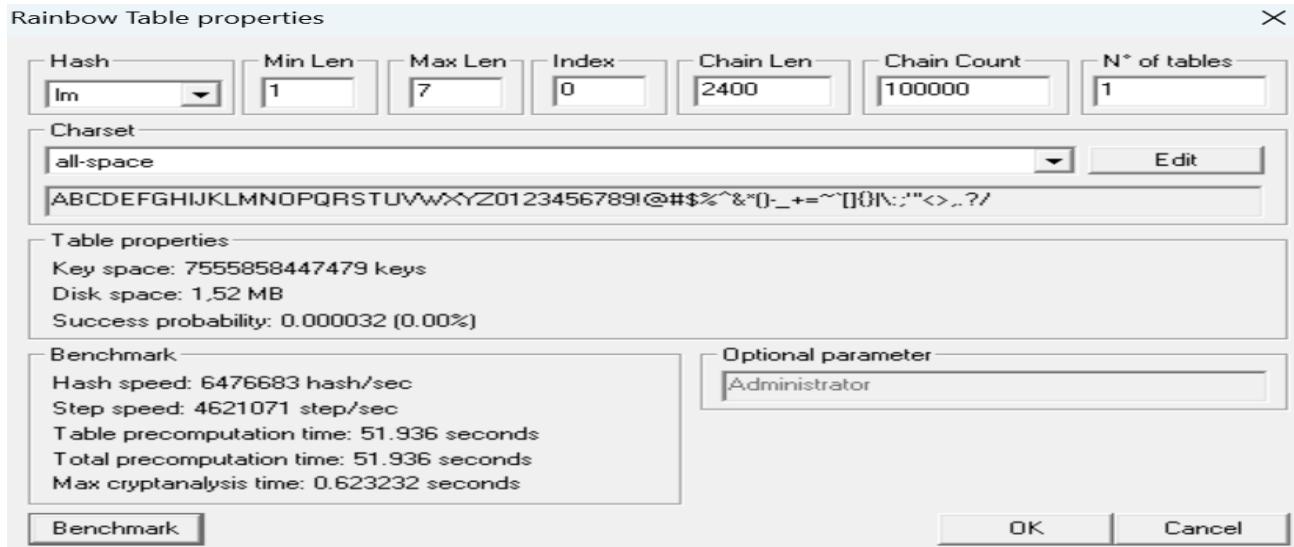
To generate rainbow tables first we will have to modify the properties of WinRTGen according to our need, and to do so Click on “**Add Table**”. After this, a new box will appear named “**Rainbow Table Properties**”

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:

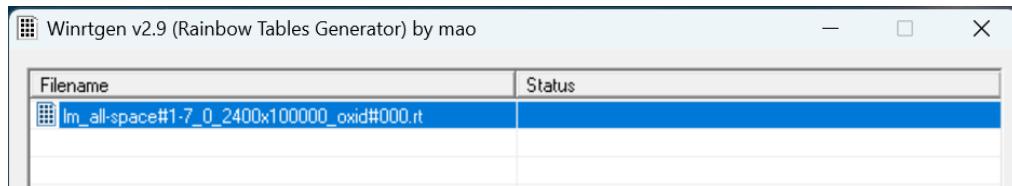


Hash: The type of encryption we want the rainbow table to be generated. For example MD5, MD4, SHA1, etc

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

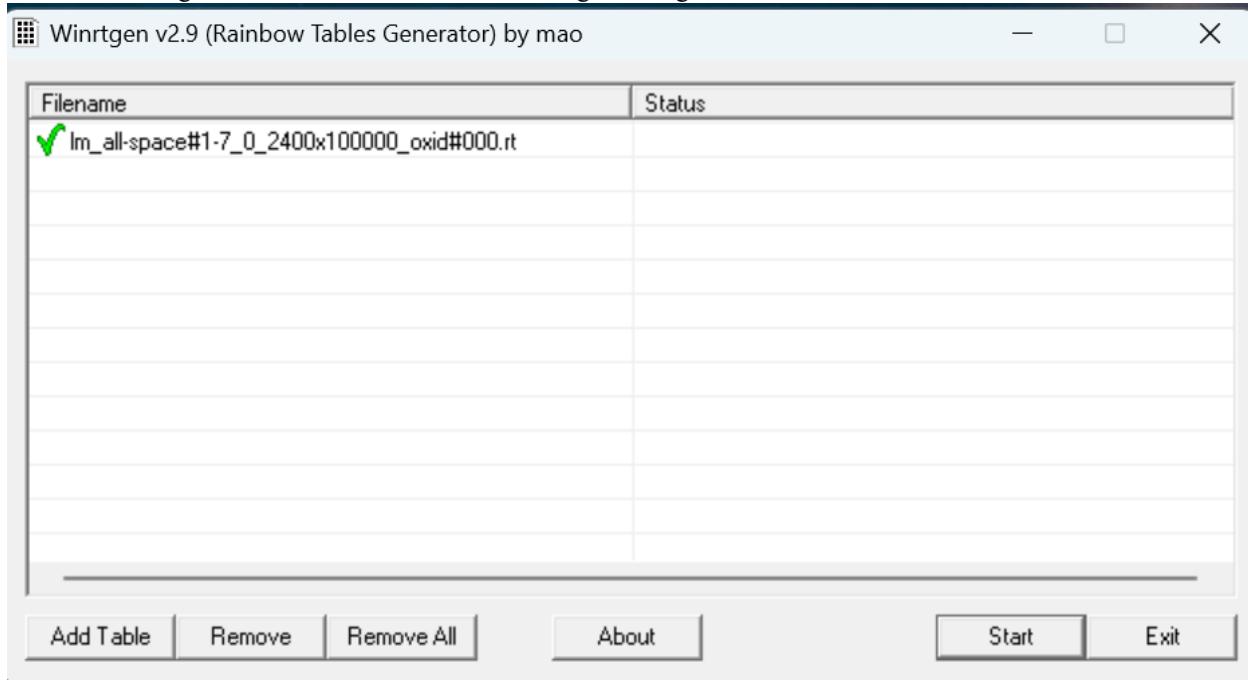


After “Benchmark” click on “Ok”. This will add the Rainbow Table to the queue in the mainwindow



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 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

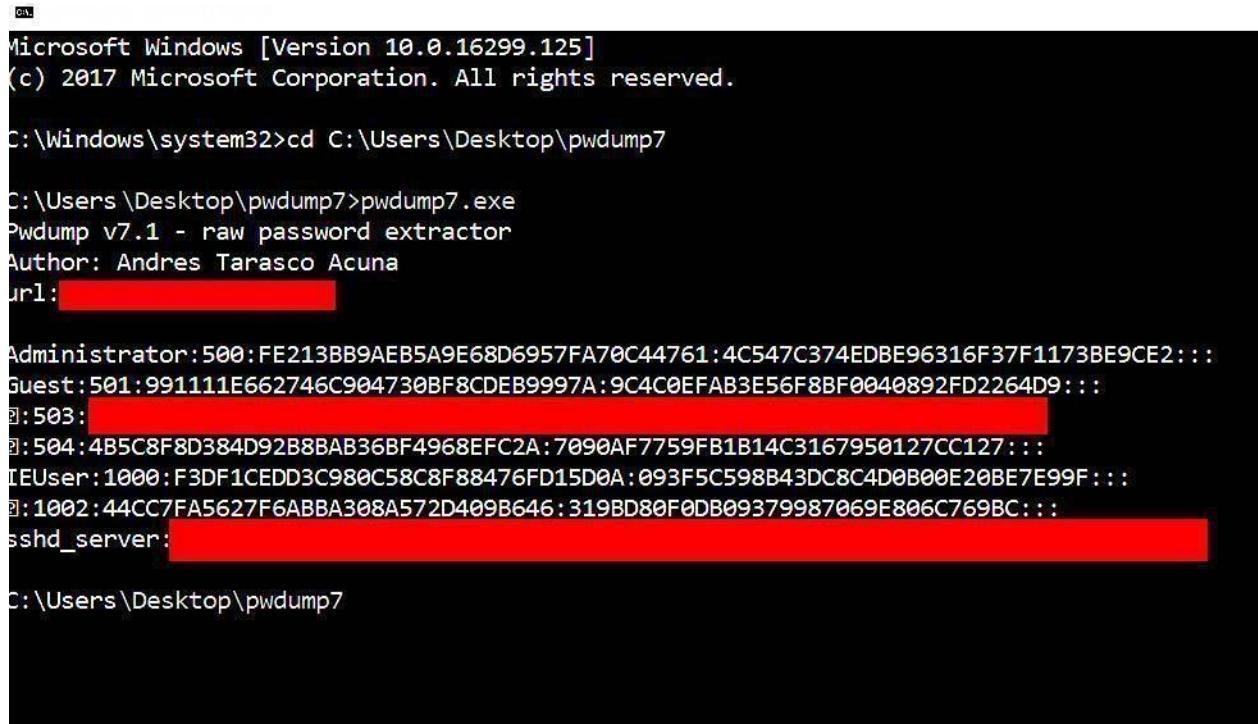
As a result, it will spill all the hashes kept in the SAM file. The next step is to use the commands below to save the registry values for the SAM file and system file in a system file:

reg save hklm\sam c:\sam

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
```



```
Microsoft Windows [Version 10.0.16299.125]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\Desktop\pwdump7

C:\Users\Desktop\pwdump7>pwdump7.exe
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: [REDACTED]

Administrator:500:FE213BB9AEB5A9E68D6957FA70C44761:4C547C374EDBE96316F37F1173BE9CE2:::
Guest:501:991111E662746C904730BF8CDEB9997A:9C4C0EFAB3E56F8BF0040892FD2264D9:::
[REDACTED]:503:[REDACTED]
[REDACTED]:504:4B5C8F8D384D92B8BAB36BF4968EFC2A:7090AF7759FB1B14C3167950127CC127:::
IEUser:1000:F3DF1CEDD3C980C58C8F88476FD15D0A:093F5C598B43DC8C4D0B00E20BE7E99F:::
[REDACTED]:1002:44CC7FA5627F6ABBA308A572D409B646:319BD80F0DB09379987069E806C769BC:::
sshd_server:[REDACTED]

C:\Users\Desktop\pwdump7
```

iv. 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.

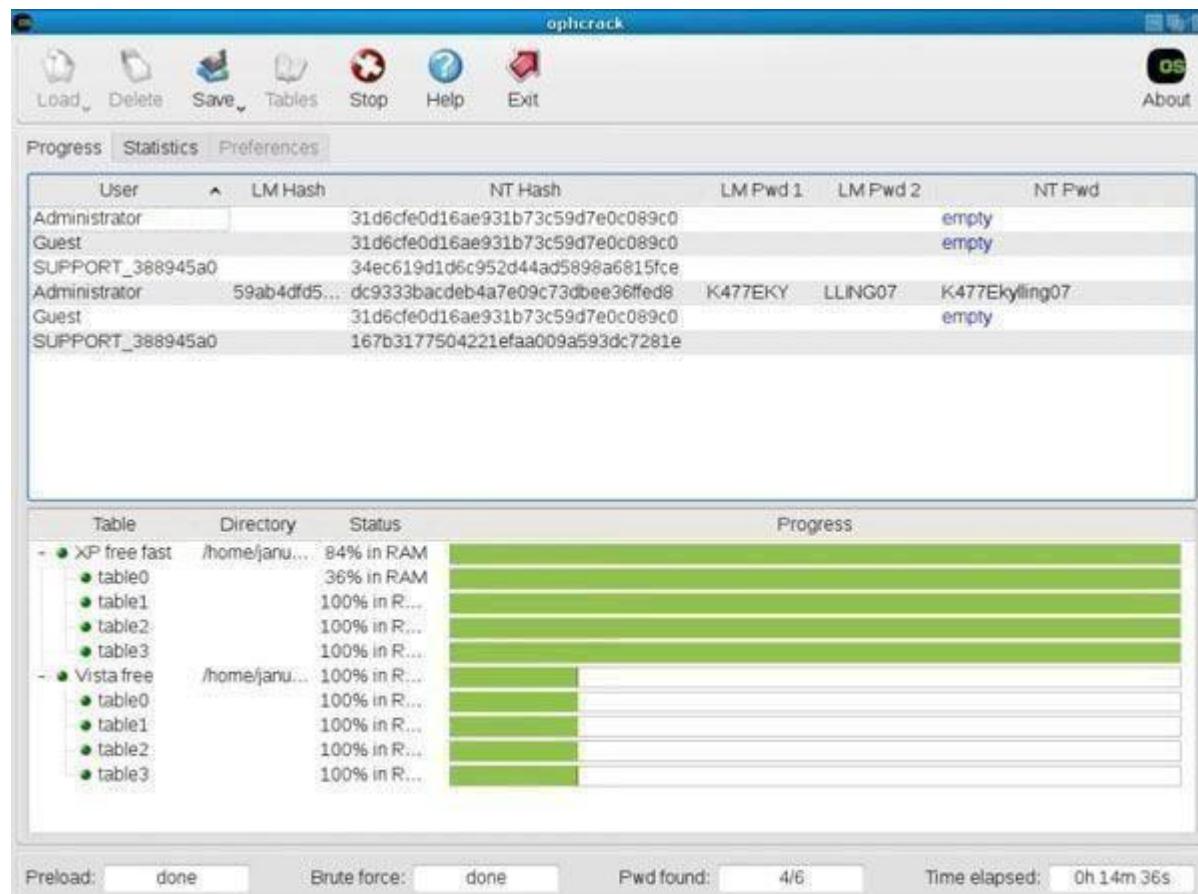
Step 4 : Remove the bootable media from the second PC and insert it into your locked Windows machine. Let the computer boot up from this media instead of the native Windows installation. This is made possible by the fact that Ophcrack itself contains a small operating system that can run independently 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 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 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 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.

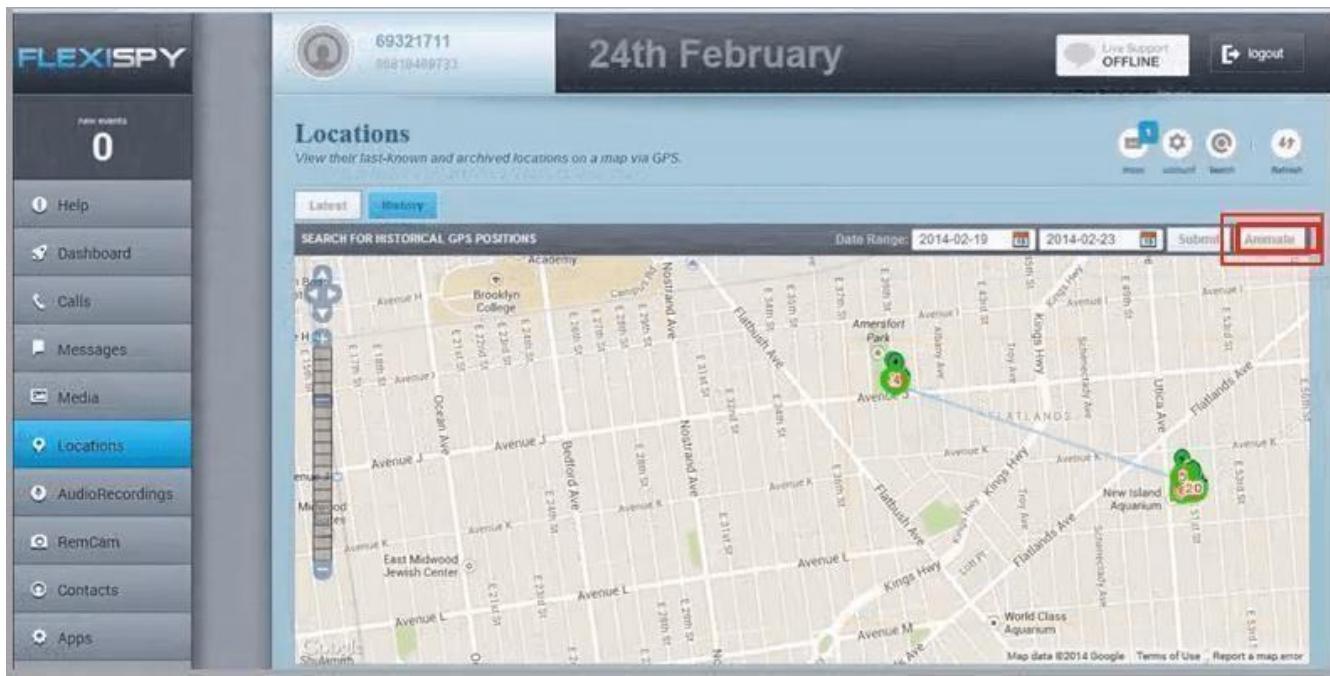


V. Flexispy

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 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.



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. 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 is in the main data stream by default. The following is the syntax of ADSs

filename.extension:alternativeName

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

C:\Windows\System32\cmd.exe

```
C:\test>echo "this is file no 1" > file_1.txt
C:\test>echo "this is hidden file inside the file_1.txt" > file_1.txt:secret.txt

C:\test>dir
Volume in drive C has no label.
Volume Serial Number is 9445-3BC5

Directory of C:\test

27-05-2022 16:01    <DIR> .
27-05-2022 16:15                22 file_1.txt
                           1 File(s)           22 bytes
                           1 Dir(s)  155,960,602,624 bytes free

C:\test>
```

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

C:\Windows\System32\cmd.exe

```
C:\test>notepad file_1.txt:secret.txt
C:\test>
```

file_1.txt:secret - Notepad

File Edit View

```
"this is hidden file inside the file_1.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
```

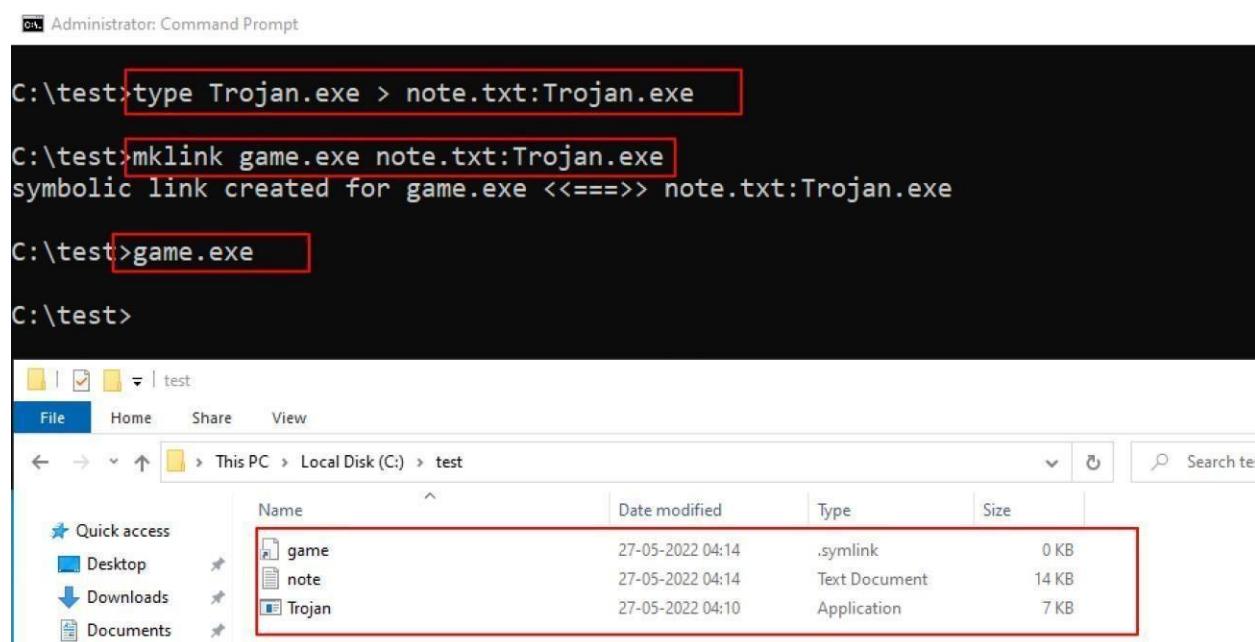
The following command has used the copy the trojan.exe into a note.txt(stream)
 C:\test>type Trojan.exe > note.txt:Trojan.exe

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 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.



The screenshot shows two windows. The top window is a Command Prompt titled 'Administrator: Command Prompt' with the following history:

```
C:\test>type Trojan.exe > note.txt:Trojan.exe
C:\test>mklink game.exe note.txt:Trojan.exe
symbolic link created for game.exe <<===>> note.txt:Trojan.exe
C:\test>game.exe
C:\test>
```

The bottom window is a File Explorer showing the contents of a 'test' folder on 'Local Disk (C:)'. The folder contains three items: 'game' (Type: .symlink, Size: 0 KB), 'note' (Type: Text Document, Size: 14 KB), and 'Trojan' (Type: Application, Size: 7 KB). The 'game' item is highlighted with a red box.

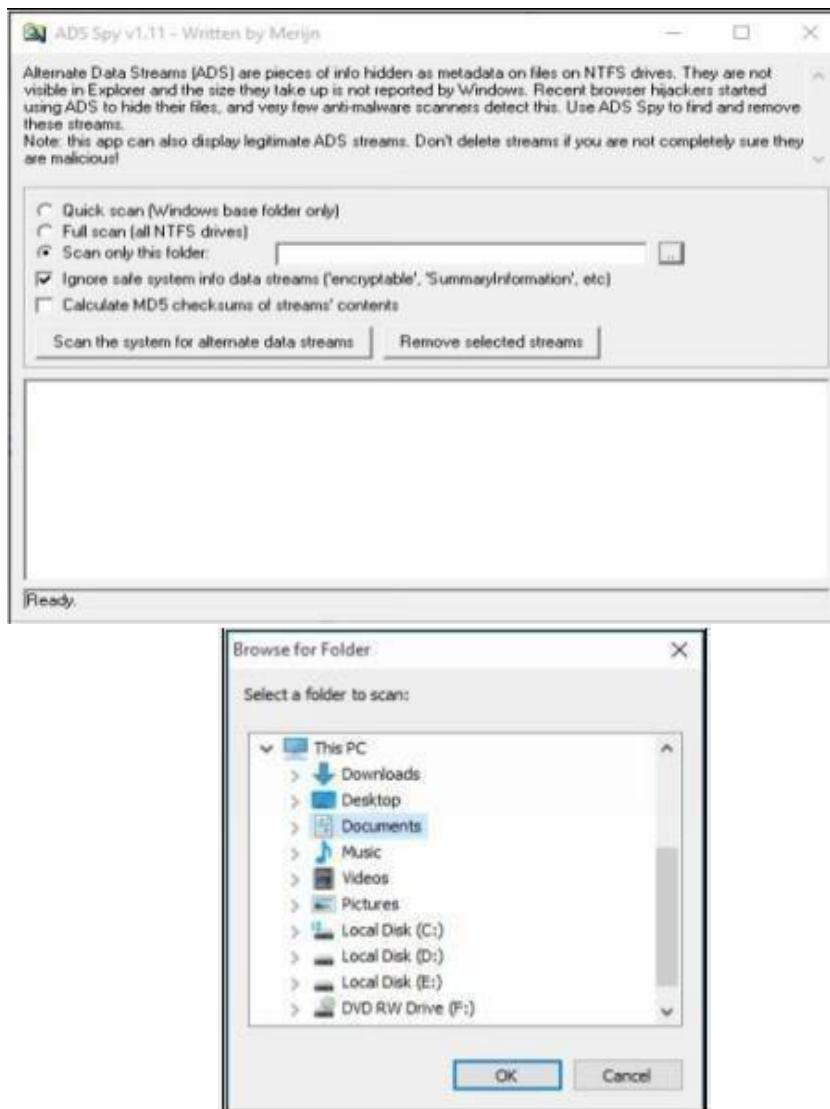
Name	Date modified	Type	Size
game	27-05-2022 04:14	.symlink	0 KB
note	27-05-2022 04:14	Text Document	14 KB
Trojan	27-05-2022 04:10	Application	7 KB

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

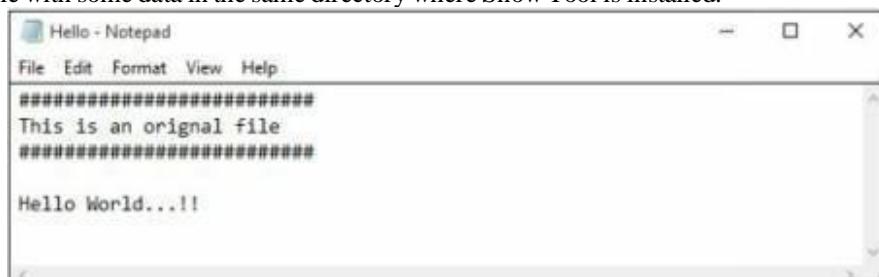
As we store the file in the Document folder, Selecting Document folder to scan particular folder only.

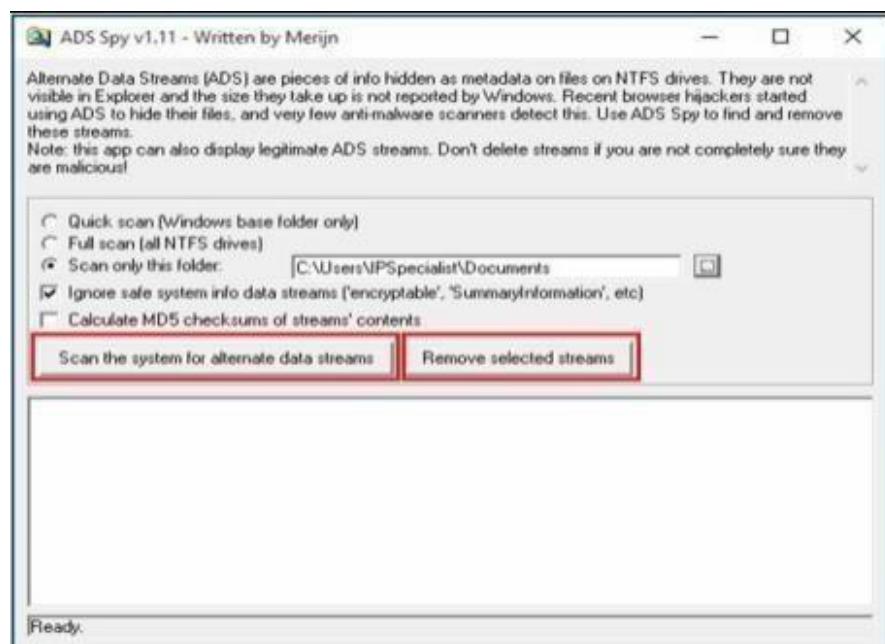


Select an Option, if you want to scan for ADS, click “Scan the system for ADS”/ or click removes button to remove the file

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 the directory.

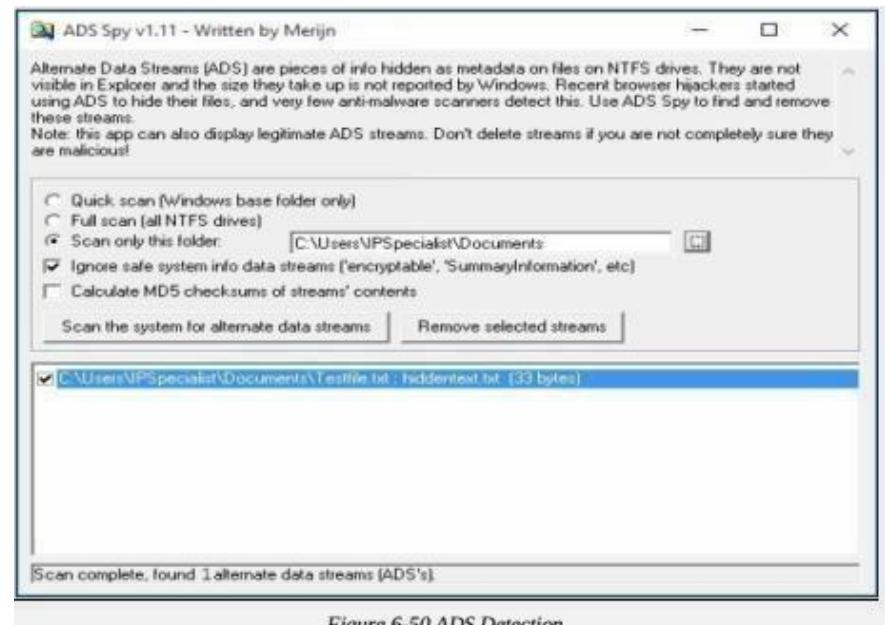


Figure 6-50 ADS Detection

Go to Command Prompt

Change the directory to run Snow tool

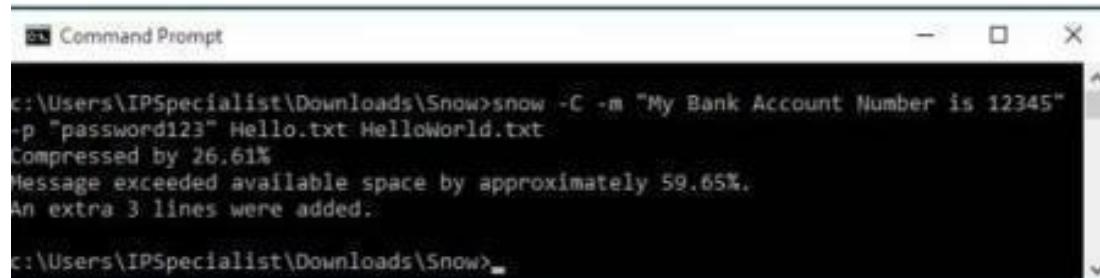
```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\IPSpecialist>cd c:\Users\IPSpecialist\Downloads\Snow\
```

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.



```
c:\Users\IPSpecialist\Downloads\Snow>snow -C -m "My Bank Account Number is 12345" -p "password123" Hello.txt HelloWorld.txt  
Compressed by 26.61%  
Message exceeded available space by approximately 59.65%.  
An extra 3 lines were added.  
c:\Users\IPSpecialist\Downloads\Snow>
```

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

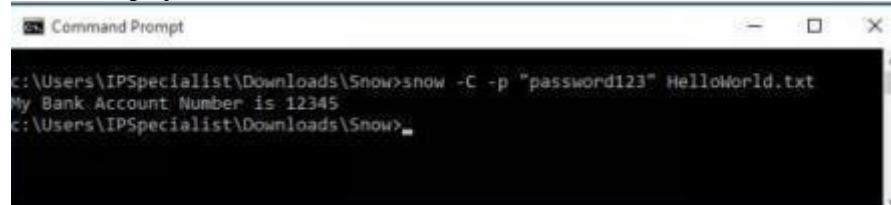


New File has the same text as an original file without any hidden information. This file can be sent to the target.

Recovering Hidden Information

On destination, Receiver can reveal information by using the command

Snow -C -p "password123" HelloWorld.txt



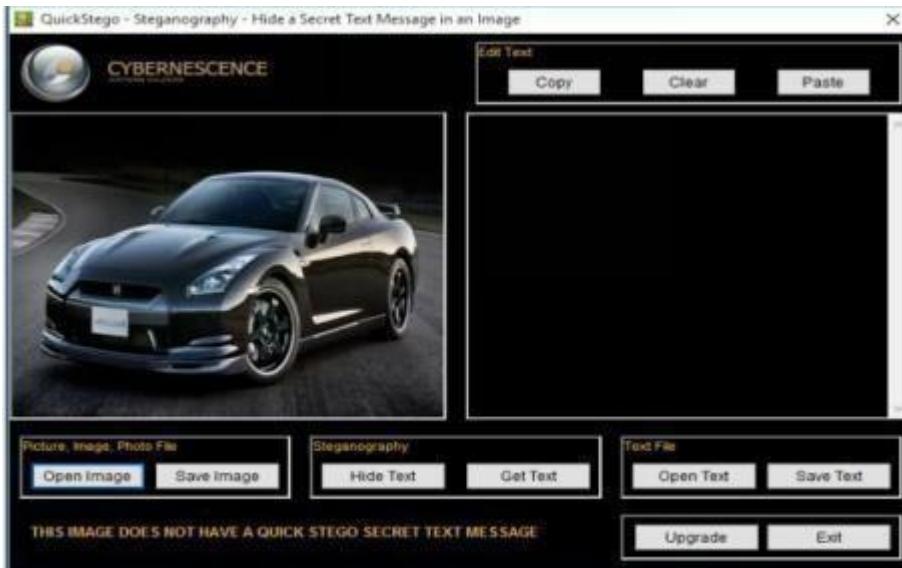
```
c:\Users\IPSpecialist\Downloads\Snow>snow -C -p "password123" HelloWorld.txt  
My Bank Account Number is 12345  
c:\Users\IPSpecialist\Downloads\Snow>
```

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

viii. Quickstego

Image Steganography using QuickStego

1. Upload an Image. This Image is termed 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 /?**

```
Administrator: Command Prompt
C:\Windows\system32>auditpol /?
Usage: AuditPol command [<sub-command><options>]

Commands (only one command permitted per execution)
/?           Help (context-sensitive)
/get          Displays the current audit policy.
/set          Sets the audit policy.
/list          Displays selectable policy elements.
/backup       Saves the audit policy to a file.
/restore      Restores the audit policy from a file.
/clear         Clears the audit policy.
/remove        Removes the per-user audit policy for a user account.
/resourceSACL Configure global resource SACLs

Use AuditPol <command> /? for details on each command
C:\Windows\system32>
```

Enter the following command to enable auditing for System and Account logon:-

C:\Windows\system32>**auditpol /set /category:"System","Accountlogon"**

/success:enable /failure:enable

```
Administrator: Command Prompt
C:\Windows\system32>auditpol /set /category:"System","Account logon" /success:enable /failure:enable
The command was successfully executed.
C:\Windows\system32>
```

To check Auditing is enabled, enter the command C:\Windows\system32>**auditpol**

logon","System"/get /category:"Account

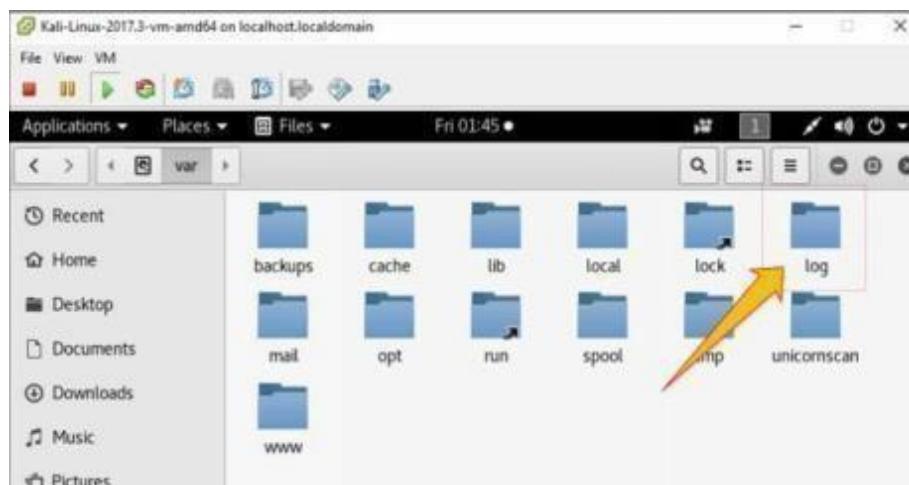
To clear Audit Policies, Enter the following command

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

Are you sure (Press N to cancel or any other key to continue)?**Y**

```
Administrator: Command Prompt
C:\Windows\system32>auditpol /get /category:"Account logon","System"
System audit policy
Category/Subcategory          Setting
System
  Security State Change       No Auditing
  IPsec Driver                No Auditing
  System Integrity             No Auditing
  Security System Extension   No Auditing
  Other System Events          No Auditing
Account Logon
  Other Account Logon Events  No Auditing
  Kerberos Service Ticket Operations  No Auditing
  Credential Validation       No Auditing
  Kerberos Authentication Service  No Auditing
C:\Windows\system32>
```

1. Go to **Logs** folder:



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

```

May 2 07:25:08 kali CRON[32135]: pam_unix(cron:session): session opened for user root
by (uid=0)
May 2 07:25:08 kali CRON[32135]: pam_unix(cron:session): session closed for user root
May 2 07:30:04 kali CRON[32149]: pam_unix(cron:session): session opened for user root
by (uid=0)
May 2 07:30:04 kali CRON[32149]: pam_unix(cron:session): session closed for user root
May 2 07:31:42 kali gdm-password: gkr-pam: unlocked login keyring
May 2 07:34:10 kali sudo:      root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/
mv /root/Desktop/Test.exe /var/www/html/share
May 2 07:34:10 kali sudo: pam_unix(sudo:session): session opened for user root by
(uid=0)
May 2 07:34:10 kali sudo: pam_unix(sudo:session): session closed for user root
May 2 07:34:23 kali sudo:      root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/
mv /root/Desktop/Test.exe /var/www/html/share
May 2 07:34:23 kali sudo: pam_unix(sudo:session): session opened for user root by
(uid=0)
May 2 07:34:23 kali sudo: pam_unix(sudo:session): session closed for user root
May 2 07:34:45 kali sudo:      root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/
mv /Desktop/Test.exe /var/www/html/share
May 2 07:34:45 kali sudo: pam_unix(sudo:session): session opened for user root by
(uid=0)
May 2 07:34:45 kali sudo: pam_unix(sudo:session): session closed for user root
May 2 07:35:09 kali CRON[32255]: pam_unix(cron:session): session opened for user root
by (uid=0)
May 2 07:35:09 kali CRON[32255]: pam_unix(cron:session): session closed for user root
May 2 07:39:04 kali CRON[32396]: pam_unix(cron:session): session opened for user root
by (uid=0)
May 2 07:39:04 kali CRON[32396]: pam_unix(cron:session): session closed for user root

```

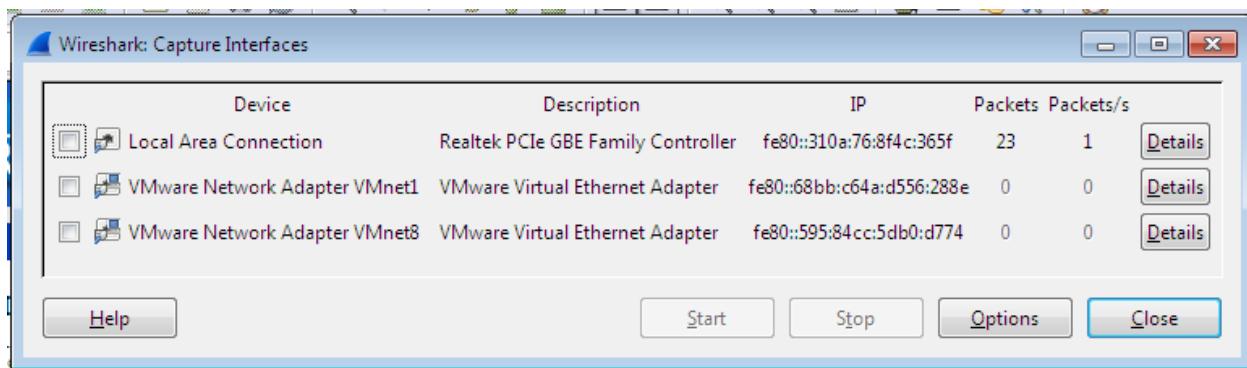
Practical No. 5

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:



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:

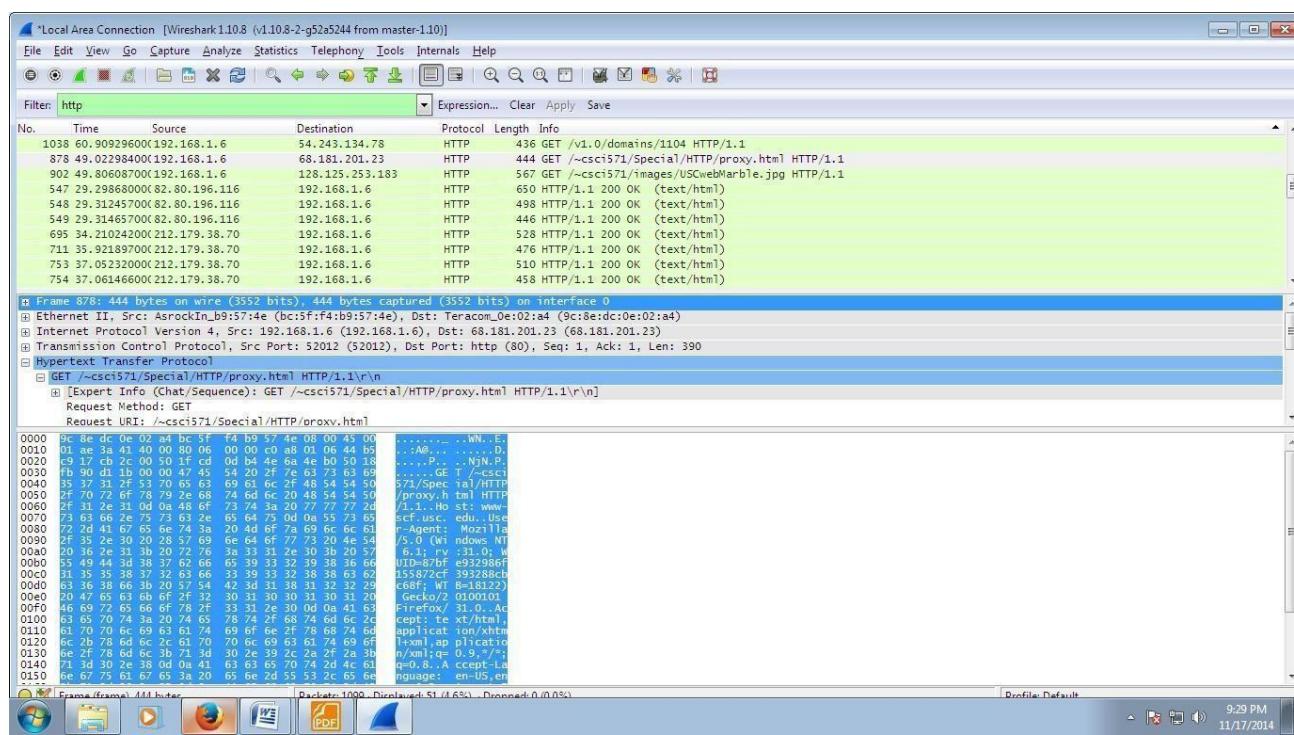


The HTTP traffic that occurs during web browsing.

- 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 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 the requested 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 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.

Figure A

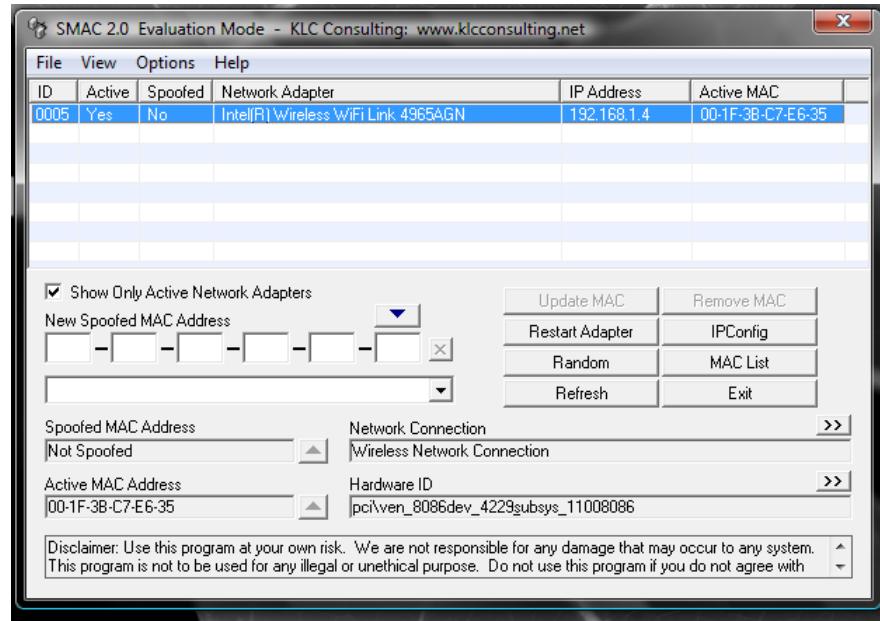
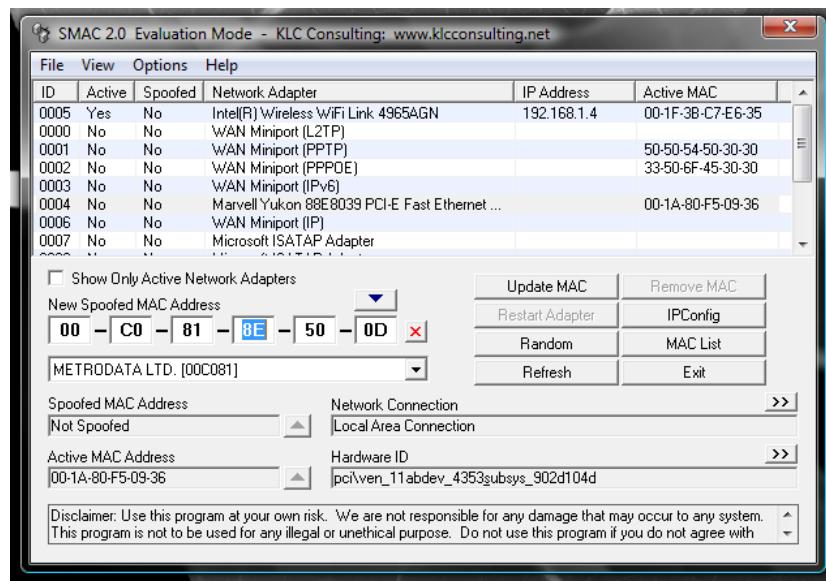


Figure C



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 (or you 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 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. 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 panel first.

Name	IP	Packets/s
<input checked="" type="checkbox"/> Local Area Connection	192.168.6.12	22
<input type="checkbox"/> Local Area Connection 2		0
<input type="checkbox"/> TAP-Win32 Adapter V9		0
<input type="checkbox"/> VMware Network Adapter VMnet1	192.168.58.1	0
<input type="checkbox"/> 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.

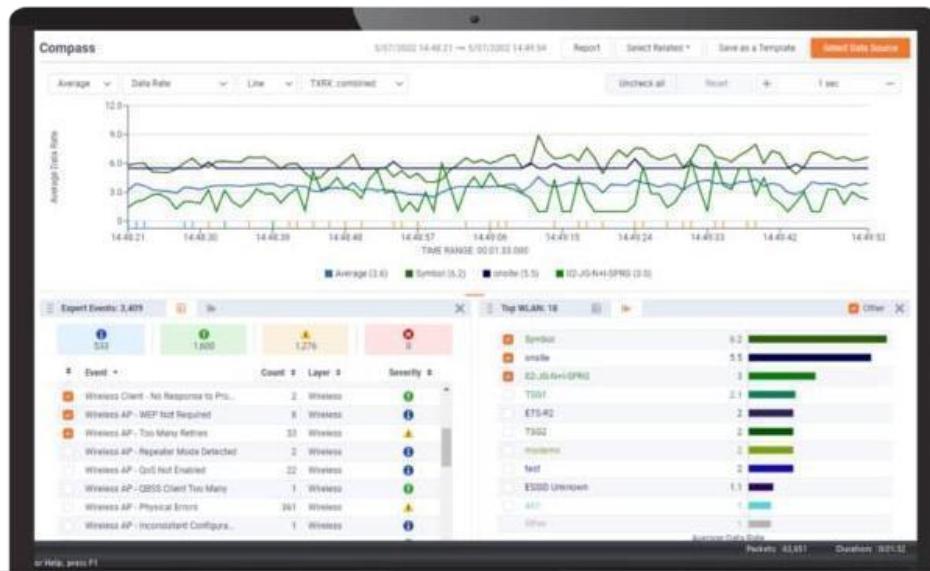
Click the big Run button to start a capture right away

Use Omnipacket Network Analyzer.

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

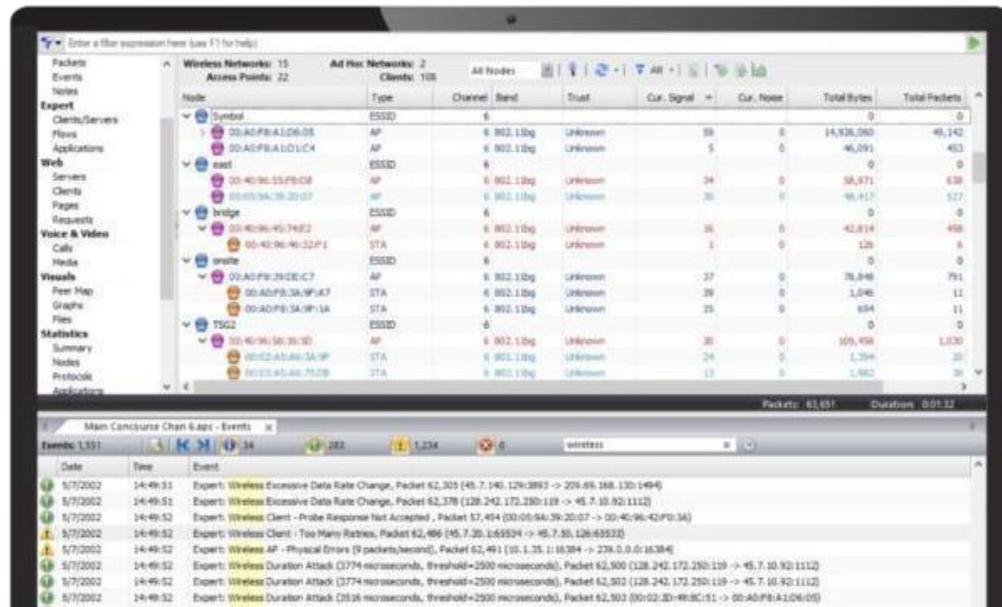
Real-Time Network Protocol Analyzer

Omnipacket 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.



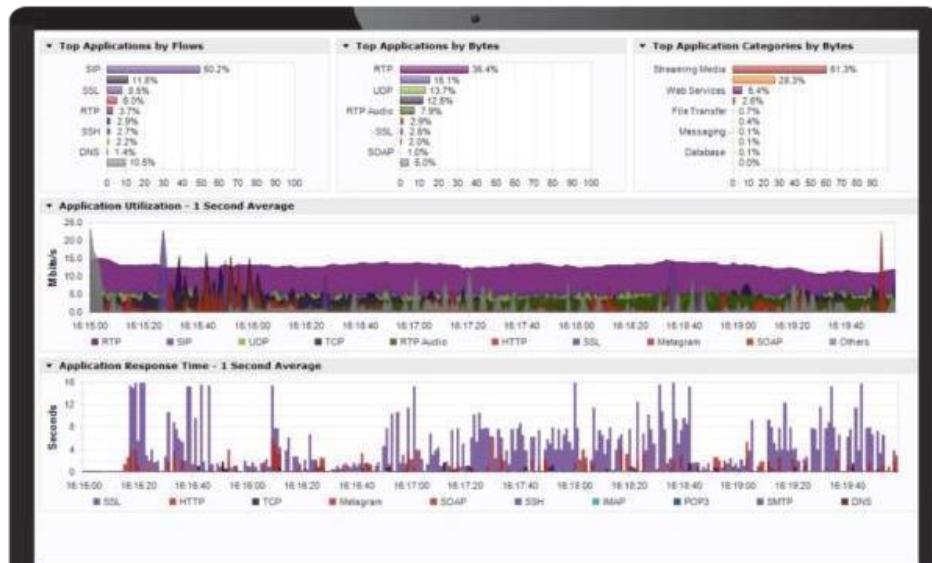
Intuitive Graphic Displays and Visualization

Omnipacket delivers intuitive visualization and effective forensics for faster resolution of network and application



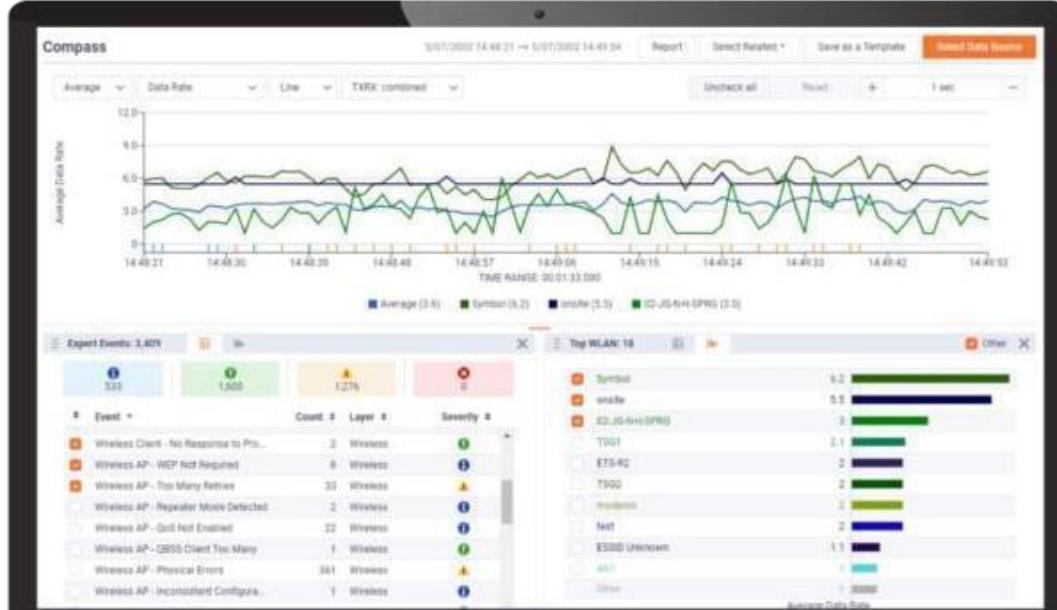
Best-In-Class Network Analysis Workflow

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 Omnipipe 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, Omnipipek extends network monitoring and visibility for troubleshooting application-level issues at remote sites and branches, WAN links, and datacenters.

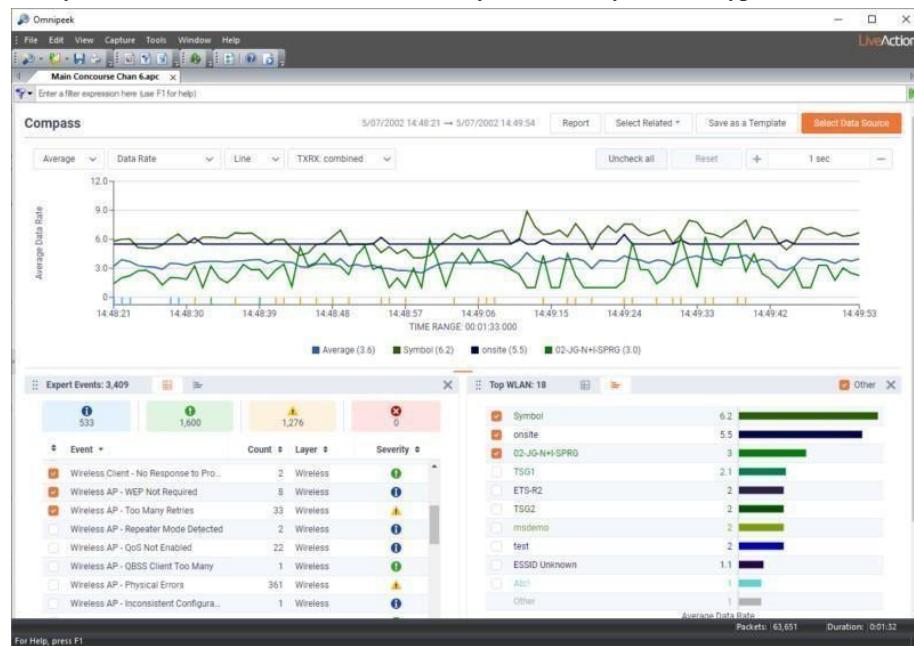


Voice and Video Monitoring and Troubleshooting

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 the need to travel to a user's location

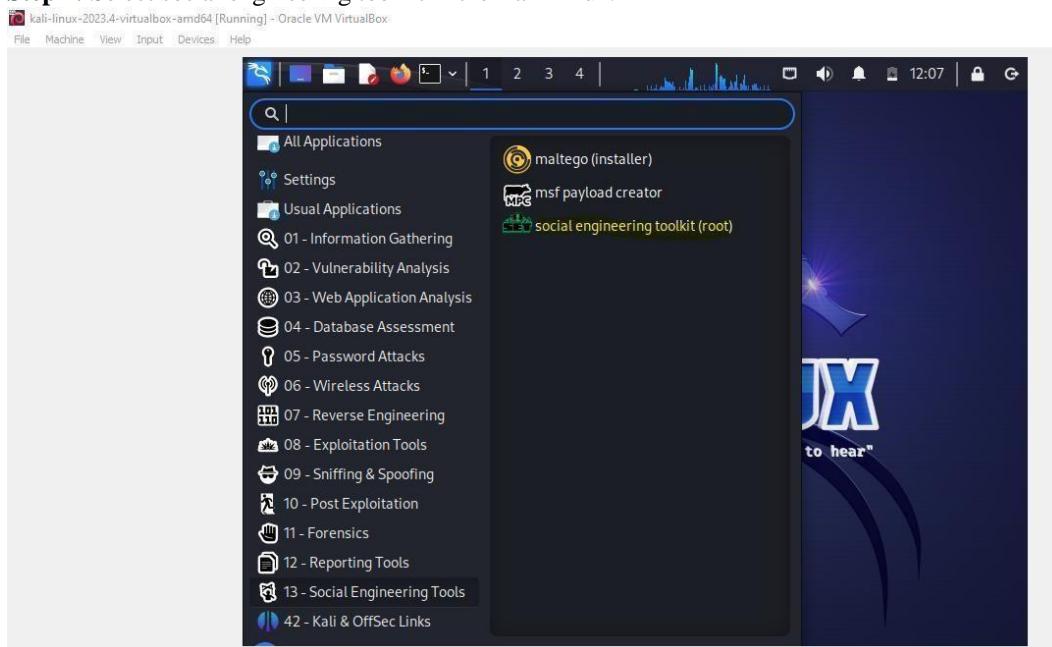


user's location

Section III A.

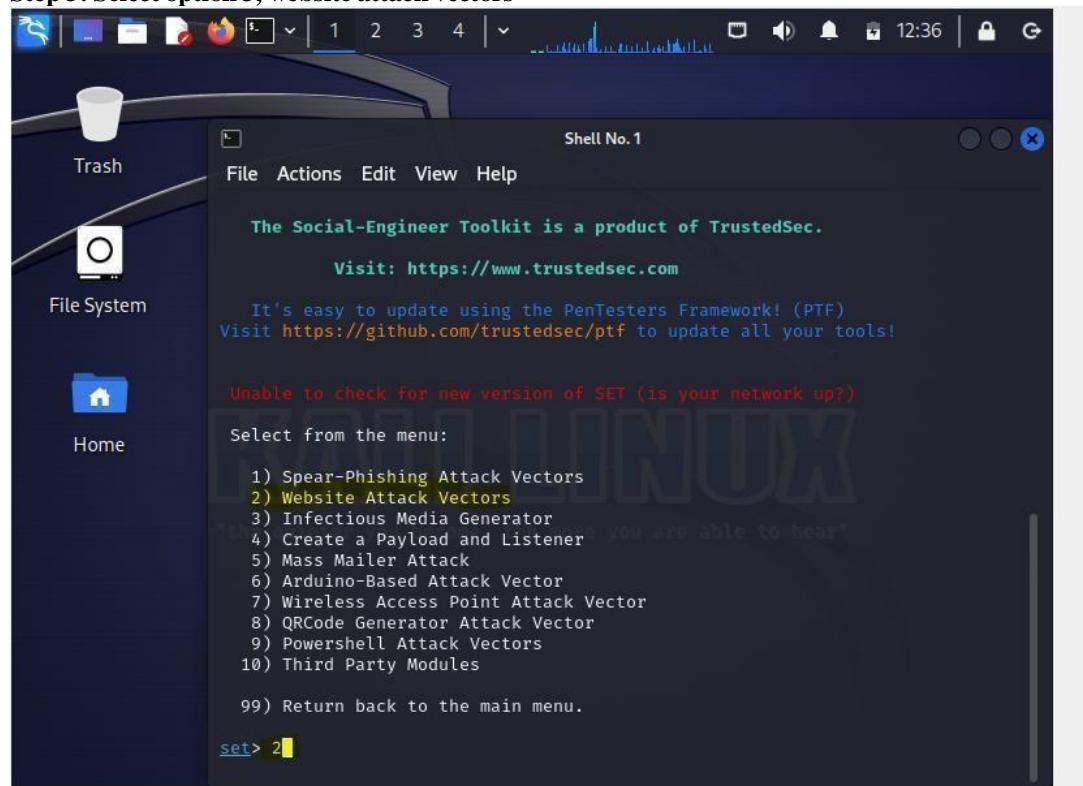
Aim: Use Social Engineering Toolkit on Kali Linux.

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

```

Shell No. 1
File Actions Edit View Help
efresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3

```

Step4: Select option 2 Site cloner.

```

Shell No. 1
File Actions Edit View Help
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

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

99) Return to Webattack Menu

set:webattack>2

```

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.

```

tro[UrP";null()])
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

LinkedIn
10.0.2.15 - - [24/Feb/2024 13:33:31] "POST /li/track HTTP/1.1" 302 -
[+] WE GOT A HIT! Printing the output:
PARAM: csrfToken=ajax:6296578694457994505
PARAM: session_key=rajat-test
PARAM: ac=0
PARAM: pkSupported=false
PARAM: sIdString=bbb5fc8-fdc2-40ea-b700-88079ab70fe2
POSSIBLE USERNAME FIELD FOUND: parentPageKey=d_checkpoint_lg_consumerLogin
POSSIBLE USERNAME FIELD FOUND: pageInstanceId=urn:li:page:checkpoint_lg_login_d
efault;Pcr1h0J2QLSRTd+v1Nd26A==
PARAM: trk=
PARAM: authUUID=
PARAM: session_redirect=
POSSIBLE USERNAME FIELD FOUND: loginCsrfParam=733d3080-4d37-48ae-8dc6-a41581a
52935
PARAM: fp_data=default
PARAM: apfc={"df":{"a":"8Gb03Wm1VcPZt9aeKM9hqw=","b":null,"c":null,"error":"
TypeError:+window.crypto[_0x561f( ... )]+is+undefined"})
PARAM: _d=
POSSIBLE USERNAME FIELD FOUND: showGoogleOneTapLogin=true
POSSIBLE USERNAME FIELD FOUND: controlId=d_checkpoint_lg_consumerLogin-login_
submit_button
POSSIBLE PASSWORD FIELD FOUND: session_password=R@123457

```

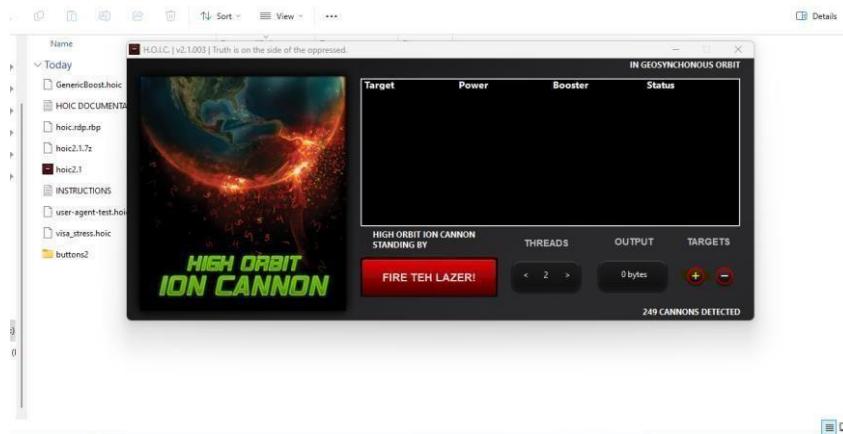
Step 8: Post the attack user is redirected to the original site:

Section III A.

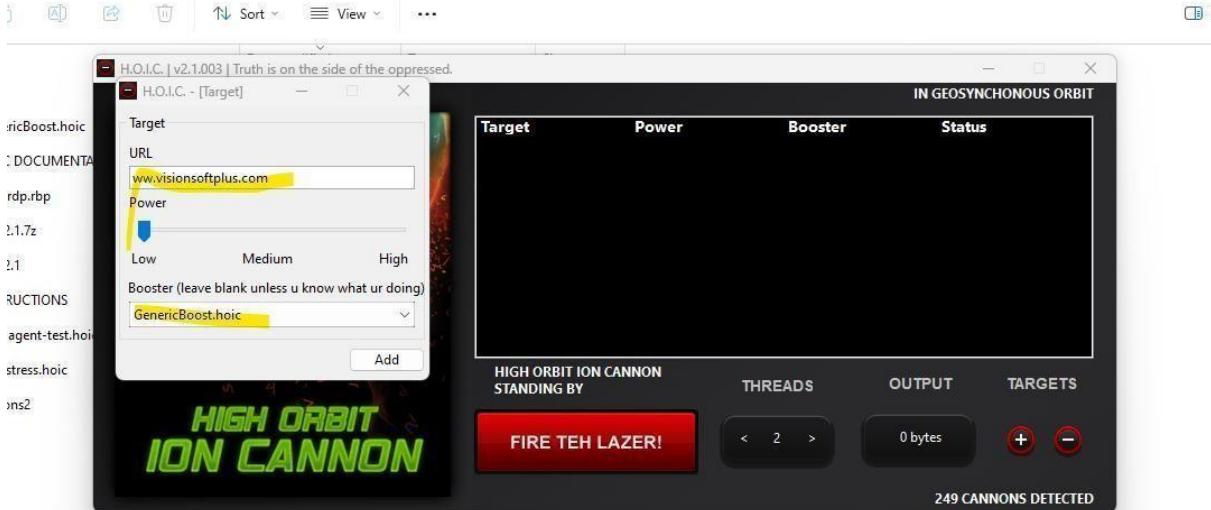
- a. Aim: Perform the DDOS attack using the following tools

I. HOIC

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

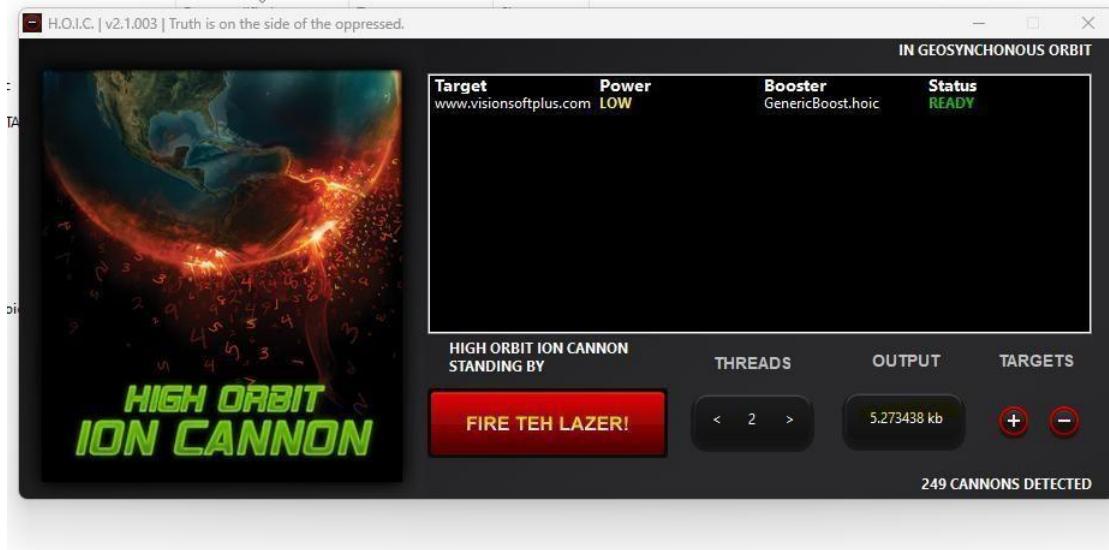


Step2: enter the url you want to attack, then click on add button.



Step 3: Click on fire button to attack

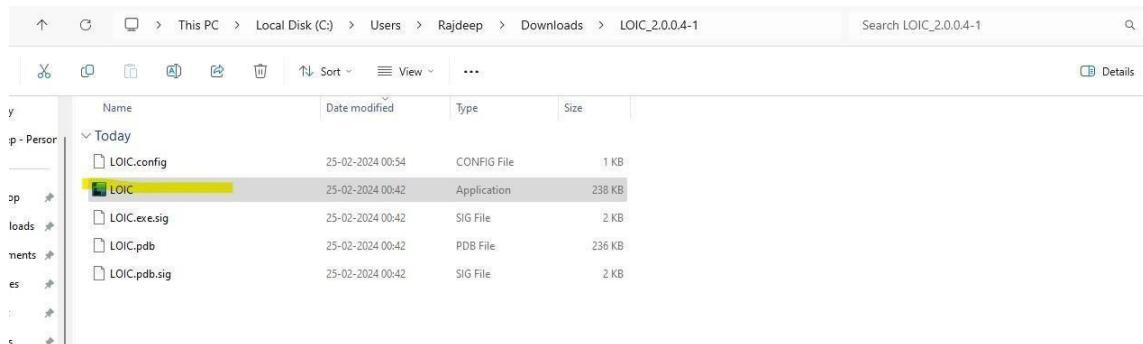
Step 4: you can see the attack is carried on and check the same on wire shark also



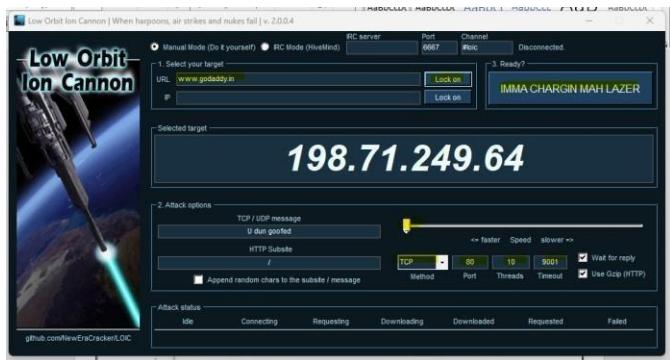
Step 5: To stop the attack again click on the Fire button.

II. LOIC

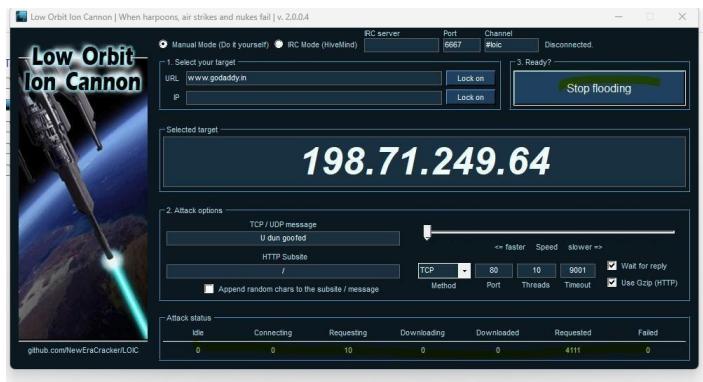
Step 1. Click on the loic.exe:



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.



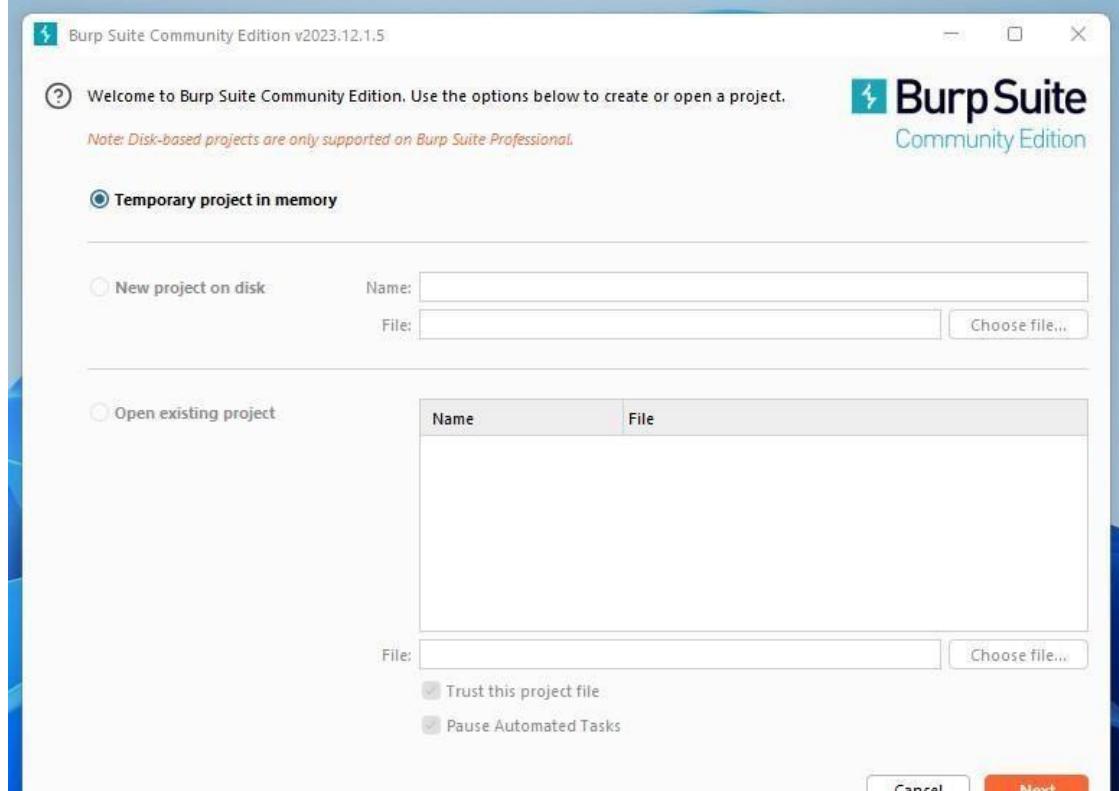
Step 3: You can see the number of requests getting hit. Click on Stop button to stop the DDOS attack.



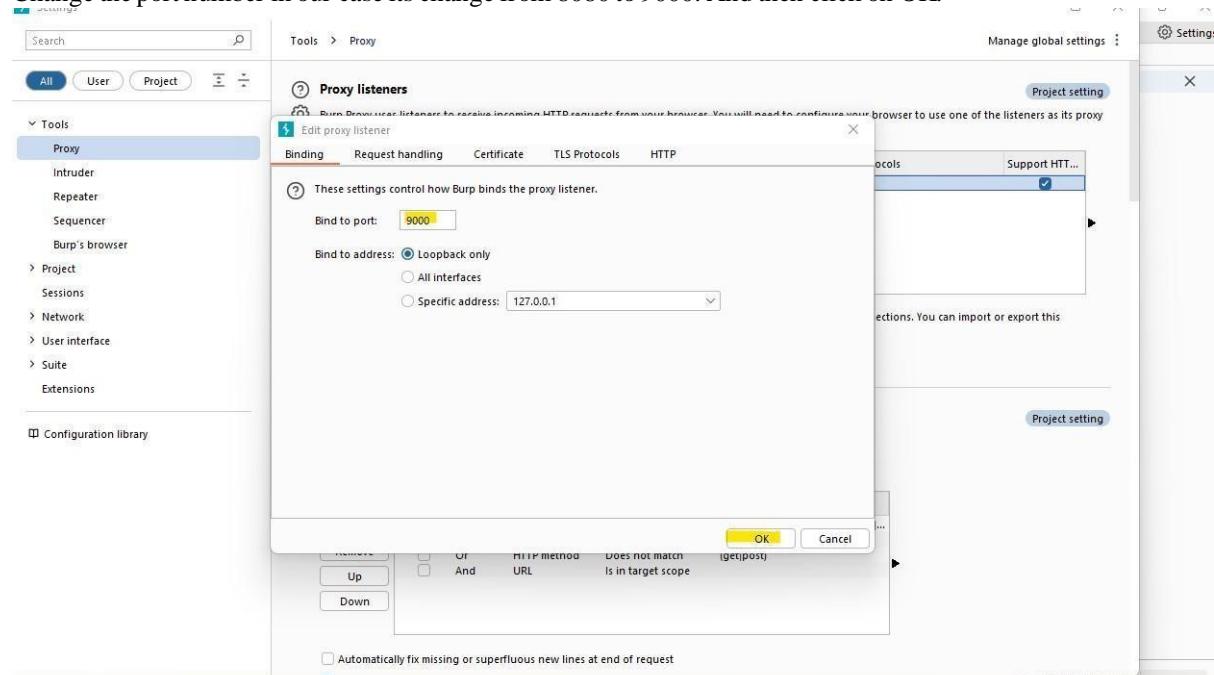
C. Aim: Using Burp Suite to inspect and modify traffic between the browser and target application

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:

The screenshot shows the Firefox settings window with the search bar containing "proxy". The "Network Settings" section is highlighted, showing options to configure how Firefox connects to the internet. A yellow box highlights the "proxy" button in the toolbar.

11. Now do the following steps:

- select manual
- Enter ip as 127.0.0.1 and port as 9000.
- select option also use this proxy for HTTPS
- 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:

The screenshot shows the Firefox about:config page with the search bar containing "network.proxy". The "network.proxy" section is expanded, showing various configuration options. The "network.proxy.allow_hijacking_localhost" option is set to "true", indicated by a yellow box. The "network.proxy.http" option is set to "127.0.0.1". The "network.proxy.ssl" option is set to "127.0.0.1". The "network.proxy.backup.ssl_port" option is set to "8080". Other options like "network.proxy.backup.ssl_version" and "network.proxy.http_port" are also visible.

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:

The screenshot shows the "All learning paths" section in the Web Security Academy. It displays three learning paths: "Server-side vulnerabilities" (Apprentice level), "SQL injection" (Practitioner level), and "API testing" (Practitioner level). Each card shows progress (e.g., 3 of 51 for Server-side vulnerabilities), a "View progress" button, and a "RESUME" button (highlighted in yellow). Below the cards is a small footer card with "My progress 0 of 17".

16. click on access Lab:

The screenshot shows the Web Security Academy platform. On the left, under 'My progress', 'Path traversal (3 of 3)' is selected from a list of vulnerabilities: Access control, Authentication, Server-side request forgery (SSRF), File upload vulnerabilities, OS command injection, and SQL injection. The main area displays the lab title 'Lab: File path traversal, simple case'. It includes a 'LAB' button, a 'Not solved' status, and a note stating: 'This lab contains a path traversal vulnerability in the display of product images. To solve the lab, retrieve the contents of the /etc/passwd file.' A large orange 'ACCESS THE LAB' button is prominent. Below it are 'Solution' and 'BACK' buttons. In the bottom right corner, there's a 'SKIP THIS LAB' button and a link to the next lab: 'Up next: What is access control?'. The top right corner features the 'Web Security Academy' logo.

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.

The screenshot shows the Burp Suite interface. The browser tab shows a failed connection to 'https://0ac600b0039964a880b3c678008500eb.web-security-academy.net'. The Burp Suite window has 'Proxy' selected in the tabs. The 'Intercept' button is highlighted in blue, indicating it is active. The 'Raw' tab of the proxy request pane shows a single line of a GET request: 'GET / HTTP/1.1'. The 'Inspector' pane on the right shows various request details like attributes, query parameters, body parameters, cookies, and headers. The status bar at the bottom indicates 'Page 8 of 8 185 words English (India) Accessibility: Investigate'.

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 burp 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:

The screenshot shows the 'ZAP Scanning Report' generated on Sun 25 Feb 2024 at 05:40:09 using ZAP Version 2.14.0. The 'Contents' section is displayed, listing various report components:

- About this report
 - Report parameters
- Summaries
 - Alert counts by risk and confidence
 - Alert counts by site and risk
 - Alert counts by alert type
- Alert counts by alert type
- Alerts
 - Risk=Medium, Confidence=High (1)
 - Risk=Medium, Confidence=Medium (1)
 - Risk=Medium, Confidence=Low (1)
 - Risk=Low, Confidence=Medium (2)
 - Risk=Informational, Confidence=Medium (2)
- Appendix
- Alert types

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)

[...](#)

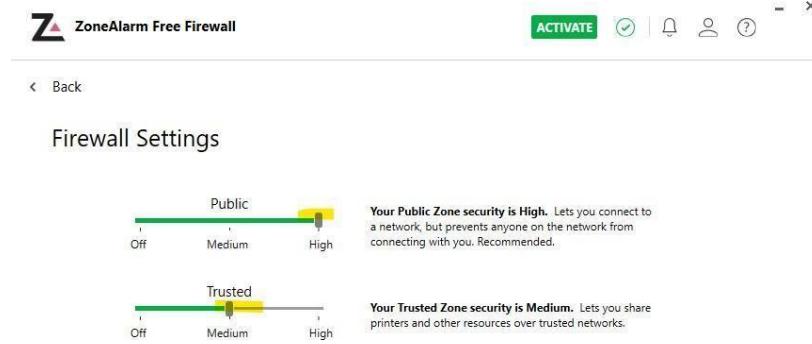
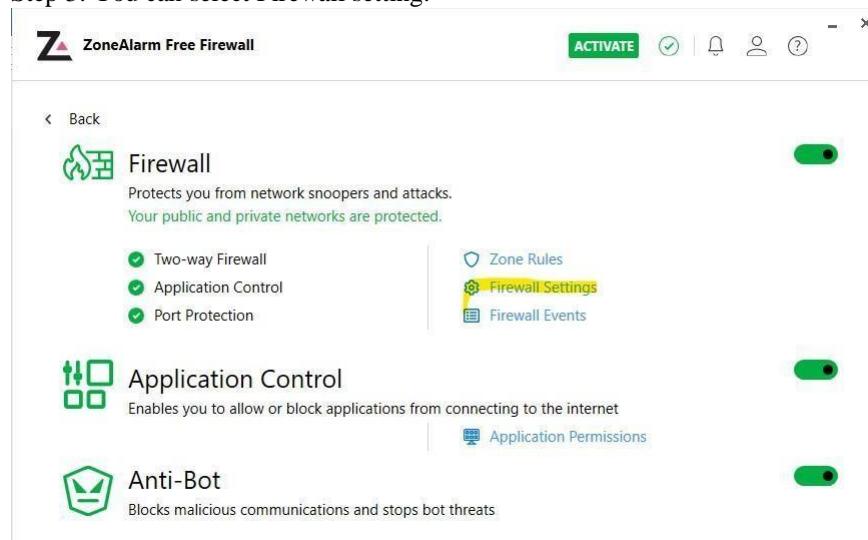
C. Demonstrate the use of the following firewalls

i. AIM: Zonealarm and analyse using Firewall Analyzer.

Step1: Open zone alarm, click on firewall:

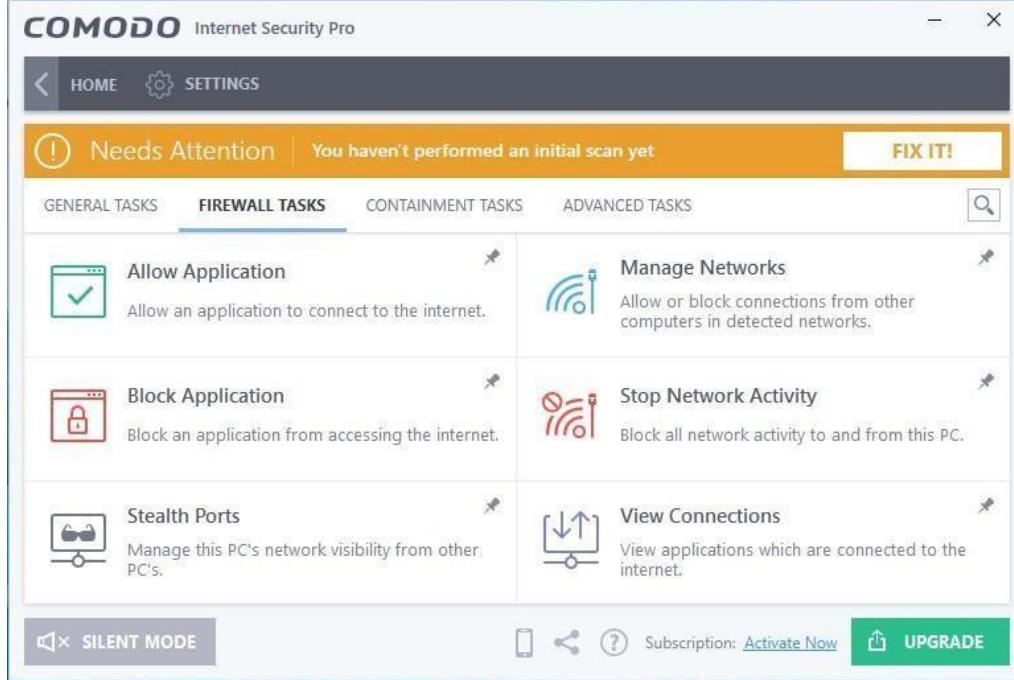
Step 2: Select Zone Rule: You can add/update new rule:

Step 3: You can select Firewall setting:



II Comodo Firewall:

Step 1: Open comodo-> go to firewall.

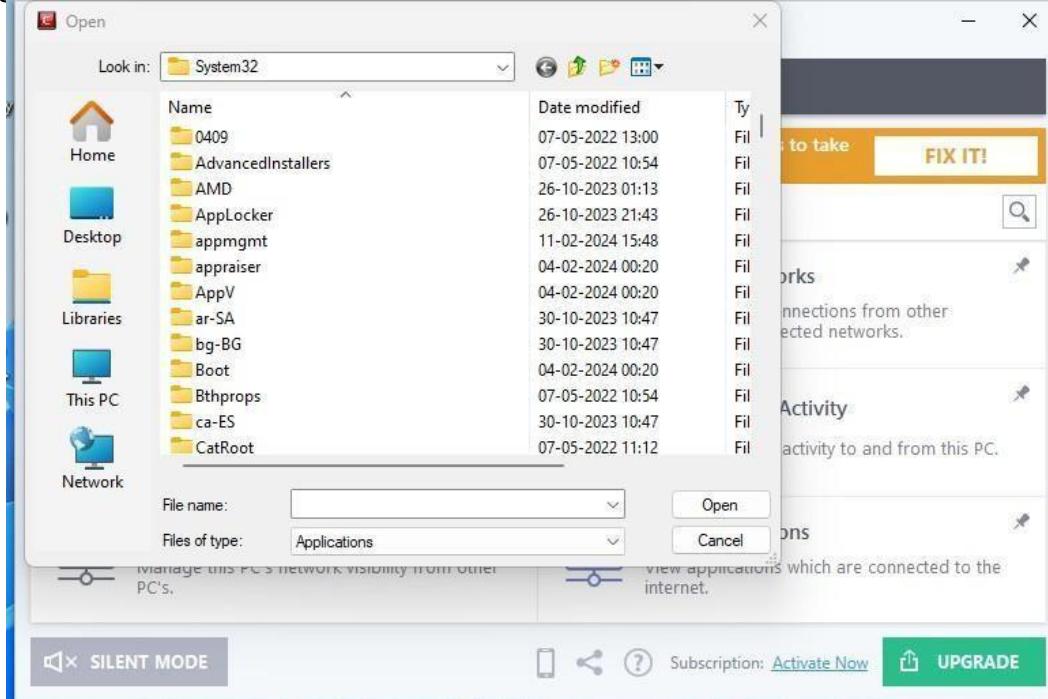


Step 2 : You can select and perform different Network activity like

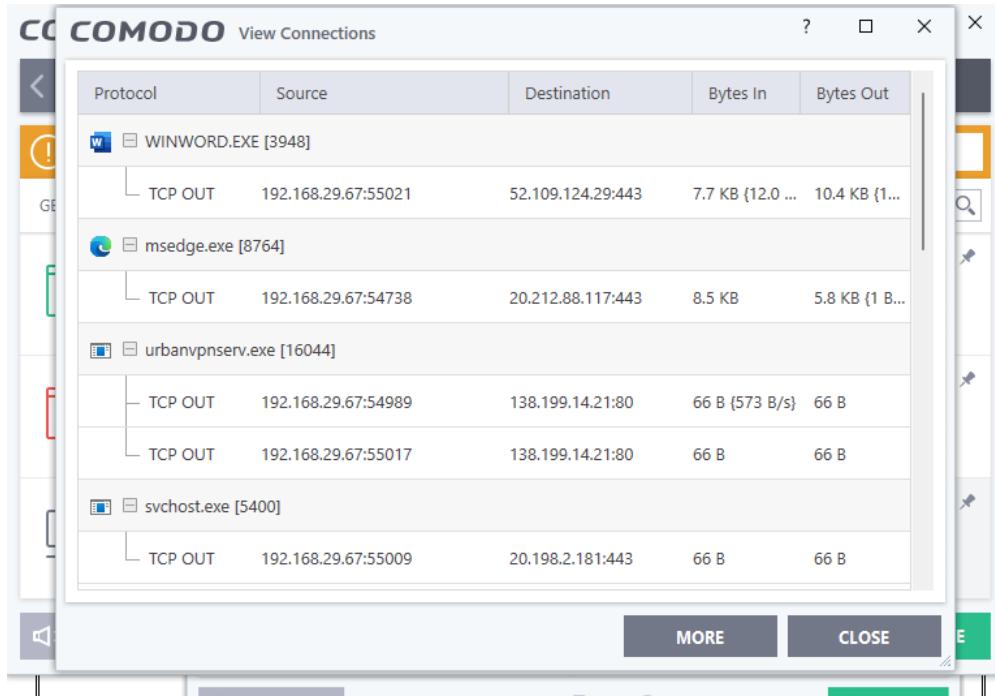
- Manage network: Like trust or block any network:



- allow or block any application by selecting application path:



- b. Allow or block network traffic in our machine:
- c. Stealth mode: allow or block on incoming network:
- d. View Connection: View all the connection in the network:



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

1. Open HoneyBot click on start icon.

	Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
Ports	26-02-2024	13:49:11	192.168.29.1	41289	192.168.29.67	7	UDP	2
Remotes	26-02-2024	13:50:41	192.168.29.1	41289	192.168.29.67	7	UDP	2

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

	Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
Ports	26-02-2024	13:49:11	192.168.29.1	41289	192.168.29.67	7	UDP	2
Remotes	26-02-2024	13:50:41	192.168.29.1	41289	192.168.29.67	7	UDP	2

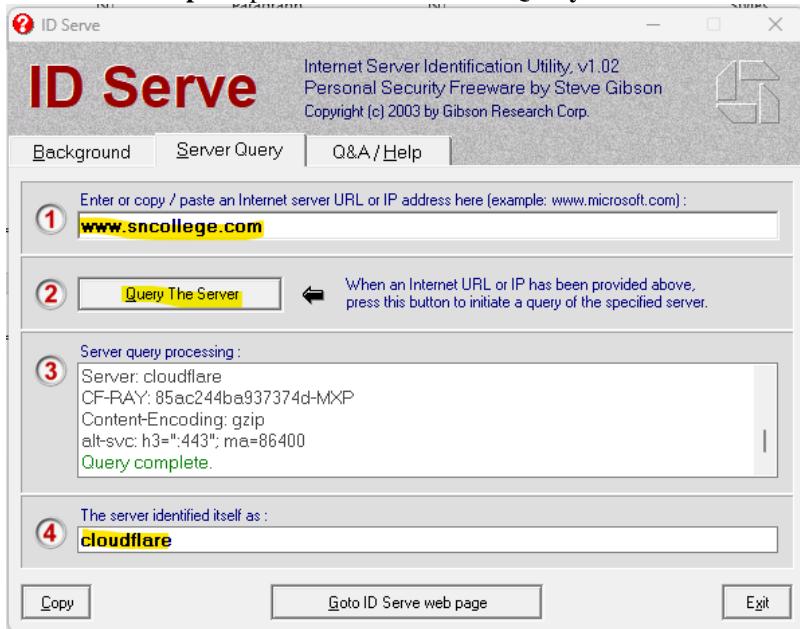
Step 3: Select any of the packet , then select from the option of text or hex format to see the output.

Time	Direction	Bytes	Data
13:49:11	RX	1	\n
13:49:11	TX	1	\n

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

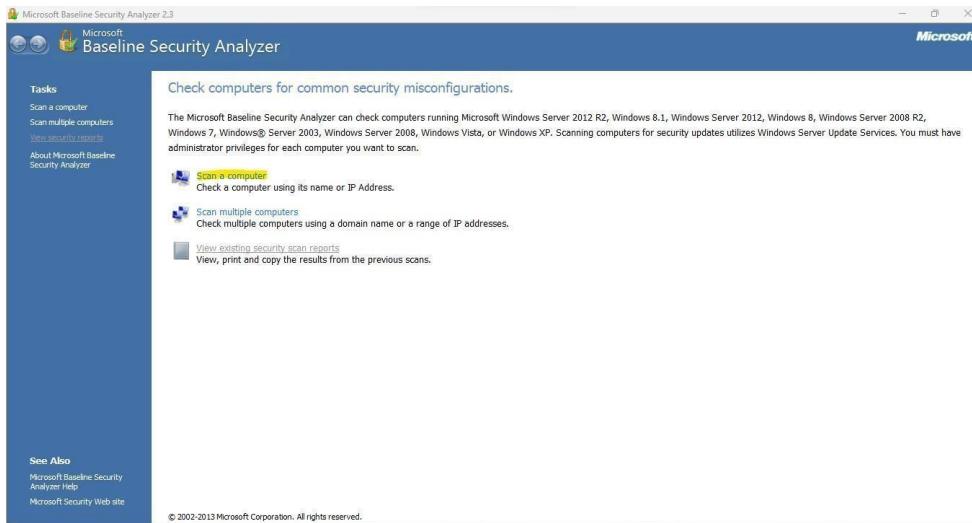
1. ID Server

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

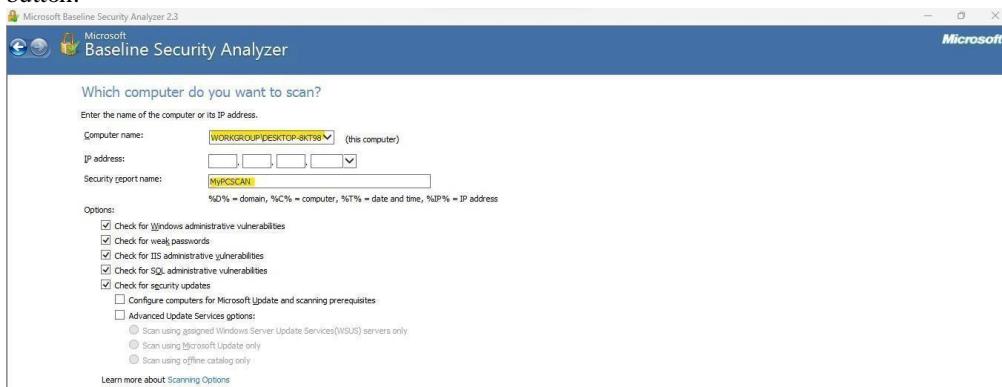


ii. Aim: Microsoft Baseline Security Analyzer

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:

Report Details for WORKGROUP - DESKTOP-8KT98Q2 (2024-02-25 02:31:17)

Security assessment:
Incomplete Scan (Could not complete one or more requested checks.)

Computer name: WORKGROUP\DESKTOP-8KT98Q2
IP address: 192.168.29.67
Security report name: MyPCSCAN
Scan date: 25-02-2024 02:31
Scanned with MBSA version: 2.3.2211.0
Catalog synchronization date: Security updates scan not performed

Sort Order: Score (worst first) ▾

Security Update Scan Results

Score	Issue	Result
!	Security Updates	Cannot load security CAB file. How to correct this

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
!	Automatic Updates	The Automatic Updates feature has not been configured on this computer. Please upgrade to the latest Service Pack to obtain the latest version of this feature and then use the Control Panel to configure Automatic Updates. What was scanned How to correct this
!	Incomplete Updates	A previous software update installation was not completed. You must restart your computer to finish the installation. If the incomplete installation was a security update, then the computer may be at risk until the computer is restarted. What was scanned How to correct this

[Print this report](#) [Copy to clipboard](#) [Previous security report](#) [Next security report](#) [OK](#)

iii. Syhunt Hybri

Step 1: Open Syhunt hunt Application -> 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.

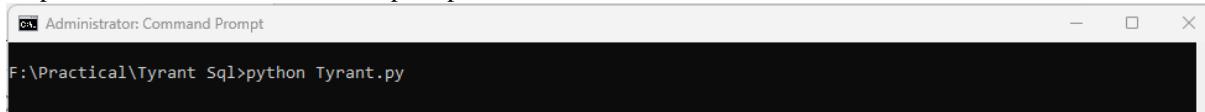
Follow the below process to run the Tyrant SQL :

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



```
F:\Practical\Tyrant_Sql>python Tyrant.py
```

Step 3: Use the vulnerable URL in target :

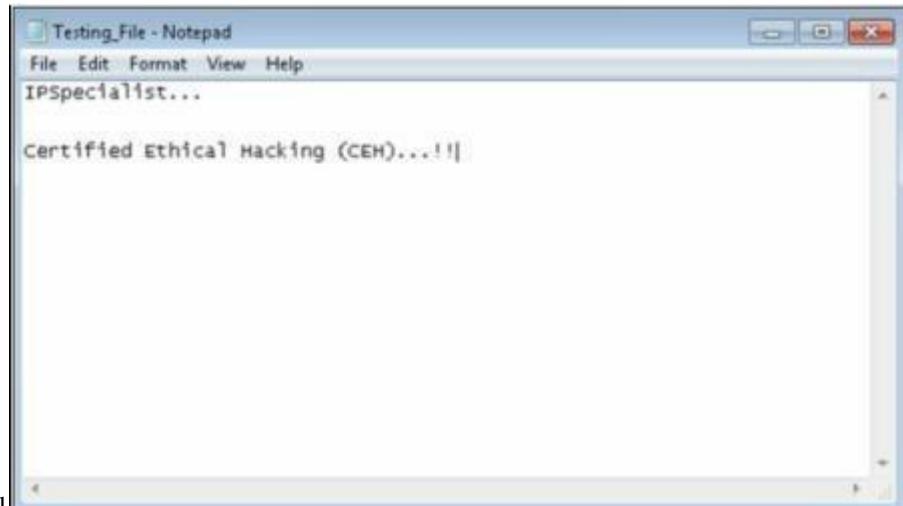
Example: <http://redtiger.labs.overthewire.org/level1.php?cat=1>

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.

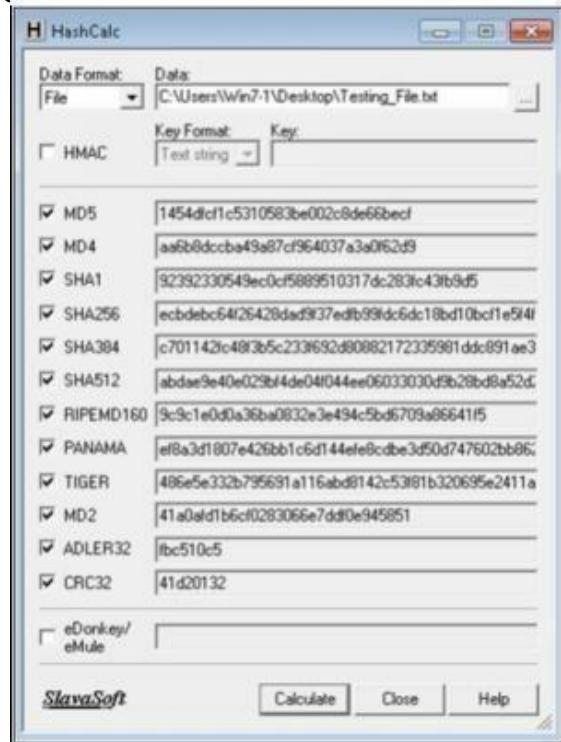
i. HashCalc

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

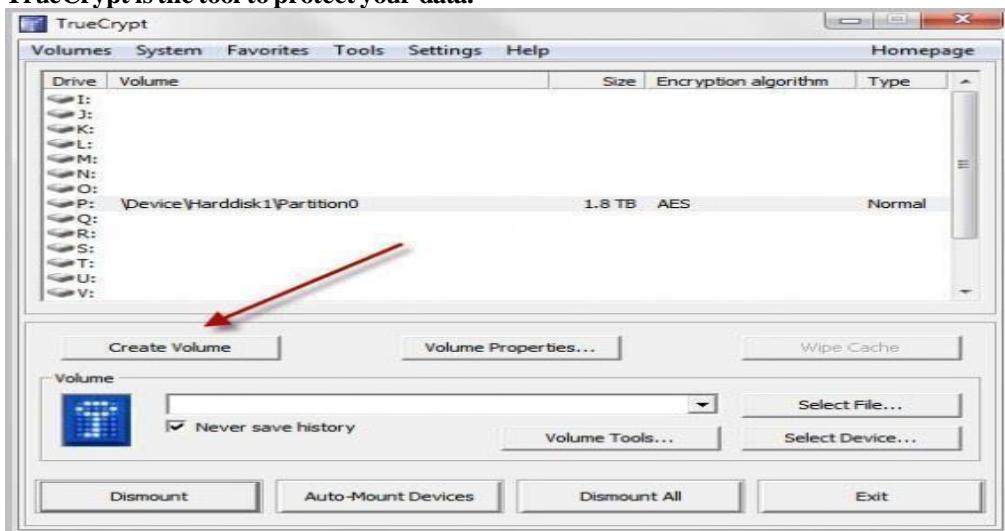
7. Now, After forwarding it to another PC, in our case, in Windows 10 PC, decrypting it using Advanced Encryption package 2017.
8. Enter password



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.

