EXERCISE I

1. To perform DNS scan using “**dnsenum**” Tool and extract useful artifacts.

AIM :

To perform DNS scan using “**dnsenum**” Tool and extract useful artifacts.

ALGORITHM :

Step – 1 : Start the Process.

Step – 2 : Start the Virtual box Kali linux machine.

Step – 3 : Open the terminal app and start the dnsenum tool with the command and targeted URL:

```
>>> sudo dnsenum <URL>
```

Step – 4 : Write the full output in the observation.

Step – 5 : Stop the Process.

OUTPUT :

RESULT : Scanning for targeted URL with DNSENUM is done successfully.

EXERCISE II

2. To perform DNS scan using "dnsrecon" Tool and extract IP address of the server machine.

AIM :

To perform DNS scan using "dnsrecon" Tool and extract IP address of the server machine.

ALGORITHM :

Step – 1 : Start the Process.

Step – 2 : Start the Virtual box Kali linux machine.

Step – 3 : Open the terminal app and start the dnsenum tool with the command and targeted URL:

```
>>>sudo dnsrecon -d <URL>
```

Step – 4 : Write the full output in the observation.

Step – 5 : Stop the Process.

OUTPUT :

RESULT : Scanning for targeted URL with DNSRECON is successfully done.

EXERCISE III

3. To perform Nmap Scan on the IP address of a server and find open ports.

AIM :

To perform Nmap Scan on the IP address of a server and find open ports.

ALGORITHM :

Step – 1 : Start the Process.

Step – 2 : Start the Virtual box Kali linux machine.

Step – 3 : Open the terminal app and start the nmap tool with the command and targeted IP_ADDRESS:

```
>>>sudo nmap –vv <IP_ADDRESS>
```

Step – 4 : Use –sV tag for service enumeration.

```
>>>sudo nmap –vv –sV <IP_ADDRESS>
```

Step – 5 : Use –A tag for service enumeration.

```
>>>sudo nmap –vv –sV –A <IP_ADDRESS>
```

Step – 6 : Use –O tag for service enumeration.

```
>>>sudo nmap –vv –sV –A –O <IP_ADDRESS>
```

Step – 7 : Write the full output in the observation.

Step – 8 : Stop the Process.

OUTPUT :

RESULT : Nmap Scan on the IP address of a server and find open ports are successfully done.

EXERCISE IV

4. To perform Directory scan on the server with the tool "Gobuster".

AIM :

To perform Directory scan on the server with the tool "Gobuster".

ALGORITHM :

Step – 1 : Start the Process.

Step – 2 : Start the Virtual box Kali linux machine.

Step – 3 : Open the terminal app and start the gobuster tool and targeted URL:

```
>>>sudo gobuster dir -u <IP ADDRESS>  -w  /usr/share/wordlists/dirb/common.txt
```

Step – 4: Write the full output in the observation.

Step – 5: Stop the Process.

OUTPUT :

Write the output of the gobuster tool finding the database tables.

RESULT : Directory scan on the server is successfully done.

EXERCISE V

5. To perform Intruder attack with BurpSuite.

AIM :

To perform Intruder attack with BurpSuite.

Step – 1 : Start the Process.

Step – 2 : Start the Virtual box Kali linux machine.

Step – 3 : Open the Burpsuite with super user privilege for that type in the terminal:

>>>sudo burpsuite

Step – 4 : Navigate to Proxy :

>>>Proxy

Step – 5 : Select Intercept the Proxy:

>>>Proxy> Intercept on >

Step – 6 : Enter the target URL to be scanned in Search Engine:

>>> <URL>

Step – 7 : Configure with lightweight scanning.

Step – 8 : Write the Critical vulnerabilities in the Observation.

Step – 9 : Stop the Process.

OUTPUT :

RESULT:

Performing Intruder attack is successfully done.

EXERCISE VI

6. To perform Web crawling with OWASP-ZAP.

AIM:

To perform Web crawling with OWASP-ZAP.

ALGORITHM:

Step – 1: Start the Process.

Step – 2: Start the Virtual box Kali linux machine.

Step – 3: Open the terminal app and start the ZAP tool and enter targeted URL:

```
>>> <URL>
```

Step – 4: Write the full output in the observation.

Step – 5: Stop the Process.

OUTPUT :

Write the directory the tool scanned for :

Write the files present in the database :

RESULT :

Web crawling with ZAP is performed successfully.

EXERCISE VII

7. To perform exploit search with "search-sploit" tool.

AIM :

To perform exploit search with "search-sploit" tool.

ALGORITHM :

Step – 1 : Start the Process.

Step – 2 : Start the Virtual box Kali linux machine.

Step – 3 : Open the terminal app and start the searchsploit tool with the comment:

```
>>>sudo searchsploit  qdpm 9.2
```

Step – 4 : Write the output of the identified vulnerability in the Observation.

Step – 5 : Stop the Process.

OUTPUT :

RESULT : Exploit search with "search-sploit" tool is done successfully.

EXERCISE VIII

8. To perform Protocol (TCP, FTP, UDP) scanning with Metasploit framework.

AIM :

To perform Protocol (TCP, FTP, UDP) scanning with Metasploit framework

ALGORITHM :

Step – 1 : Start the Process.

Step – 2 : Start the Virtual box Kali linux machine.

Step – 3 : Open the terminal app and start the Metasploit tool with the command:

```
>>>sudo msfconsole
```

Step – 4 : Set TCP scan tunnel and meterpreter shell.

```
>>>use exploit/multi/handler
>>>show options
```

Step – 4 : Set FTP/FTPD scan tunnel and meterpreter shell.

```
>>>use exploit/FTPD/reverse_shell
>>>show options
```

Step – 4 : Set UDP scan tunnel and meterpreter shell.

```
>>>use exploit/UDP/reverse_shell
>>>show options
```

Step – 5 : Write the full output in the observation.

Step – 6 : Stop the Process.

OUTPUT :

Write the output of the TCP, FTP and UDP scans from the meterpreter shell.

RESULT :

Scanning for TCP, FTP and UDP services is successfully completed.

EXERCISE IX

9. To perform SSH Login attack using Metasploit framework.

AIM :

To perform SSH Login attack using Metasploit framework.

ALGORITHM :

Step – 1: Start the Process.

Step – 2: Start the Virtual box Kali linux machine.

Step – 3: Open the terminal app and type the ssh command to access and login with user and password:

```
>>>sudo ssh <USERNAME@IP_ADDRESS> -p <PASSWORD>
```

Step – 4: Use Metasploit to set a SSH reverse shell as command and control center:

```
>>>sudo msfconsole
```

Step – 5: set SSH login exploit with reverse shell access:

```
>>>use exploit/ssh/reverse_shell
```

Step – 6: Write the full output in the observation.

Step – 7: Stop the Process.

OUTPUT :

Write the command to setup the Metasploit and the revers shell access vulnerability file path.

RESULT :

Performing a SSH login attack is successfully done.

EXERCISE X

10. To perform Pentesting on the given ICA vulnerable machine to find Password of the database using pentesting tools.

AIM :

To perform Pentesting on the given ICA vulnerable machine to find Password of the database using pentesting tools.

ALGORITHM:

Step – 1 : Start the Process.

Step – 2 : Start the Virtual box Kali linux machine.

Step – 3 : Find the IP_ADDRESS of the ICA machine with netdiscover:

Step – 4 : Perform initial full in depth scan with nmap.

Step – 4 : Find the vulnerability in the database with search sploit.

Step – 4 : Use mysql to remotely login and find the database username and password.

Step – 4 : Use reverse ssh shell to escalate privilege to the default user and login as super user.

Step – 5 : Write the full output in the observation.

Step – 6 : Stop the Process.

OUTPUT :

Write the Contents of the database tables : USER AND LOGIN

RESULT :

Exploit and study of the ICA machine is successfully accomplished.