Practical - 01

Aim :-

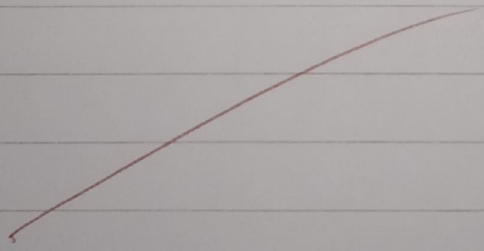
Using Google and Who.is for Reconnaissance

Step-01 :-

Open Smarsit Who is → write the website name in Ip. host or domain text field and Press enter.

Step-02 :-

It will show the various details of the website.



Practical - 02

Aim :-

Use Cryptool to encrypt and decrypt passwords using RC4 · Algorithm.

Step - 01 :-

Create one text file and save some location.

Step - 02 :-

Go to Encryption → and select the RC4 and encrypt in 16 bit.

Step - 03 :-

After Clicking encrypt you may get the converted message.

Step - 04 :-

Save the message somewhere on your desktop.

Step - 05 :-

For decryption, repeat the same procedure and select the same file.

Step - 06 :-

And Click OK to get the Output.

Practical - 03-A

Aim :-

Run and analyze the output of the following commands in linux.

Step 1 :-

If config - It displays the IP address information of any network items, including your computer.

Step 2 :-

Ping - It is used to check whether a particular IP address exists and is capable of excepting requests.

Step 3 :-

Netstat - This command shows network interface statistics (routing table, network connection).

Step 4 :-

Traceroute - It is a computer network diagnostics tool to analyze the path packets on a network. For eg : to trace the route from your router to a server for facebook. you would type trace route www.facebook.com on trace route.

Practical 3-B

Aim :-

Perform ARP Poisoning in Windows.

Step 1 :-

Download . install and open the Cain & Abel tool.

Step 2 :-

First go to sniffer & then Click on Configure select the appropriate wireless adapter Click on apply and then Click on OK Button

Step 3 :-

Activate Sniffer.

Step 4 :-

Click on + icon . Check All test - checkbox and then click on OK.

Step 5 :-

Click on ARR and then click on blank screen and then click on OK.

Step 6 :-

Select all ip address and mac address and then click on OK.

Step 7 :-

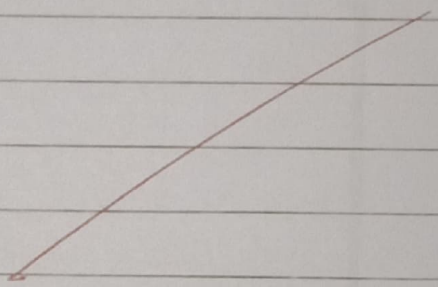
Select Apply.

Step 8 :-

It gives the status of all the device connect to wifi.

Step 9 :-

Then go to the Passwords tab it will display the passwords present.



Practical - 04

Aim :-

Using Nmap scanner to perform port scanning of various forms - ACK, SYN, FIN, NULL, XMAS.

Note :-

Install Nmap for windows and install it. After that open cmd & type "nmap" to check if it is properly installed or not. Now type the below command.

① ACK - sA (TCP ACK scan) → It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.
Command :- nmap -sA -T4 scanme.nmap.org.

② SYN (Stealth) scan (-sS) → It is the default & most popular scan option for good reason & it can be performed quickly. Scanning thousands of ports per second on a fast network not hompered by intrusive firewalls.

③ FIN Scan (-sF) → Sets just the TCP FIN bit.
Command :- nmaps -sF -T4 Para.

④ NULL Scan (-sN) → Does not set any bits - (TCP. flag header is 0)
Command :- nmap -sN -p22 sanme.nmap.org.

⑤ XMAS scan (-sX) → Sets the FIN, PSH & URG flags, lightning the packet up like a christmas tree.
Command :- nmap -sX -T4 scanme.nmap.org.

Steps :

NOTE: For using Nmap for Kali. open Terminal and type the below commands.

1) ACK -sA (TCP ACK scan)

It never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

Command: nmap -sA -T4 scanme.nmap.org

```
┌──(abhi㉿kali)-[~]
└─$ sudo su
[sudo] password for abhi:
┌──(root㉿kali)-[/home/abhi]
└─# ACK
ACK: command not found
┌──(root㉿kali)-[/home/abhi]
└─# nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-27 15:39 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00039s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.72 seconds
```

2) (Stealth) Scan (-sS)

SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls.

Command: nmap -p22,113,139 scanme.nmap.org

Practical - 05-A

Aim :-

Use Wireleshark (sniffer) to capture network traffic and analyze.

Step 1 :-

Install Wireshark.

Step 2 :-

Go to capture tab & select Interface option.

Step 3 :-

In capture Interface, select total Area Connection and click on start.

Step 4 :-

The source, destination and protocols of the packets in the LAN network are displayed.

Step 5 :-

Write http in the filter box and click on apply. It will display all the http packets.

Step 6 :-

In the browser type the Url for simple 1 html

http://www-scf.usc.edu/~csci571/special/HTTP/simple1.html

Step 7 :-

Similarly, for this Url simple 2 html

http://www-scf.usc.edu/~csci571/special/HTTP/simple2.html

Step 8 :-

For executable script

http://nunki.usc.edu:8088/eg:-bin/test-cgi

Step 9 :-

For missing file

http://www-scf-usc.edu/uscsci571/missing file.html

Step 10 :-

For birthday.html

http://nunki.usc.edu:8088/birthday.html

Step 11 :-

For secure CGI

http://nunki.usc.edu:8088/cgi-bin/secure/test-cgi

Step 12 :-

Using expressive, select the HTTP field and in it select request method.

→ select == in relation and write POST in value

Step 13 :-

Post output

Step 14 :-

404.

Practical-05-B

Aim :-

Use Nemesy to Launch SOS attack.

Step 1 :-

Open kali Linux, enter the password and users Id & open the terminal in kali Linux.

Step 2 :-

Inside the terminal, write that comment to SOS attack & appropriate IP address.

Step 3 :-

After entering the command you may show the IP is pinging with Packages.

Step 4 :-

Open the wireshark & select the interface for the sniffer the IP traffic.

Step 5 :-

Multiple TCP Protocol request has been send for the IP which is entered above.