23/10/22

Experiment :- 5

Session Hijacking

Cookie Hijacking

Hijack Amazon Account

→ Go to Amazon.com

→ Login from one computer

→ Press F12 key

→ Go for application → cookies

→ Look for
copy the value of x-acbin and at-acbin

→ Send this information on another computer

→ open any web browser with url :-
www. Amazon.com

→ Now again press F12

→ Go to application → cookies

→ Add x-acbin and paste value

→ Add at-acbin and paste value

Hijacking Facebook Account

Yes, it is possible to Hijack Facebook Account from :-

→ Login from one computer.
→ Press F12 key.
→ go for application → cookies
→ Look for C-user and xS
→ Copy the value for C-user and xS
→ Send this ~~f~~ info ~~on~~ another computer.
→ open any web browser with URL:
www. facebook.com
→ Now again press F12
→ Go for application → cookies
→ Add C-user and copy its value
→ Add x.s and copy its value.

3/11/22

Experiment no:- 6

Information Gathering:-

- Information gathering is the act of gathering of dlt kinds Of information against the targeted victim on system

- It is the first step or the beginning stage of ethical hacking.

- Attacker will first gather information like domain name, IP address, IP range, operating system, services, control panel, vulnerable services etc and later on explore it.

Tools in Kali Linux
nmap

→ Dmitry (Deep Magic Information gathering Tool) is a UNIX (GNU) Linux command line application coded in C.

→ Dmitry has the Ability to gather as much information as possible about a host.

→ Base functionality is able to gather possible sub domains email address, uptime information, tcp port scan, who is lookups and more.

Output

Deep magic informationgathering tool

Host IP : 169.255.28.23

Host Name: 169.255.28.233.technasolution.co.za

The following is a list f the current features:-

→ An open source project.
→ Perform an internet numbers who is lookup.
→ Retreive possible uptime, data, system and service data.
→ perform an E-mall address search on a target host.
→ A modular program allowing user specified modules

```
$ sudo dmitry  - i169.255.28.29
$ sudo dmitry  - w  www.facebook.com
$ sudo dmitry  - s   amazon.in
```

Output:-

```
Text entered :- Hello Piyush
After ceaser encryption
Encrypted text:- Ifmmp Qjzvti
After decryption
Text : Hello Piyush
```

10/11/22

Experiment no:- 7

Encryption and Decryption

Installing Cryptool

Step 1:- To download the cryptool 1:
https://www.cryptool.org/en/ct-1-downloads

Step 2:- Follow the step of installation by clicking next

Step 3:- agreement of license. I agree

Step 4:- What type of installation you need install for anyone using this computer.

Step 5:- Set up the path in which you want to download the cryptool 1

Step 6:- we get the wizard page.

Step 7:- Click on new to create a workspace.

Step 8:- After creating the workspace copy or write a text message.

Entered msg :- Hello Piyush

17/11/22

Experiment :- 8

Installation rootkit and study about the variety of options.

Procedure:-

Step 1:- Download Rootkit tool from GMER website www.gmer.net

Step 2:- This display the process, modules, services, files, registry, rootkit/malwares, autostart, and of localhost.

Step 3:- Select process menu and kill any unwanted process if any

Step 4:- Modules menu displays the various system files like .sys, dll.

Step 5: Services menu displays the complete services running with Autostart, Enable, Disable, System, Boot.

Step 6:- Files menu displays full files on Hard Disk Volumes.

Step 7: Registry displays ~~full files on~~ H Hkey_Current_User and Hkey_Local_Machine.

Step8:- Rootkits / Malwares scans the local drives selected.

Step9:- Autostart displays the registry base autostart application.

Step10: CMD allows the user to interact with command line utilities or Registry.