**Incident Response Procedures, Forensics and Forensics Analysis Lab**

A picture containing text, screenshot, electronics

Description automatically generated

Figure 1.1

In this lab, the main aim is to find out the artifacts which are present in the Victim Machine. We will exploit the remote system first and analyse web logs and at last perform incident response on the compromised host.

Graphical user interface

Description automatically generated

Figure 1.2

Logging into the Windows 8.1 machine and accessing cmd, we are going to find the open ports on the firewall using nmap as seen in **figure 1.2.**

Graphical user interface, text, application

Description automatically generated

Figure 1.3

Using Zenmap, the target id – 203.0.113.100 is entered and the command – **nmap -T4 -A -v 203.0.113.100** is used for the intense scan

T4 - Aggressive (4) speeds scans, assumes reasonably fast and reliable network

A - Enables OS detection, version detection, script scanning, and traceroute

Graphical user interface, text, application, email

Description automatically generated

Figure 1.4

Once the scan is completed, we found the open ports and in figure 1.4, we can see that FTP is a Microsoft Service.

Graphical user interface, application

Description automatically generated

Figure 1.5

Using Bruter, we are going to find the password of FTP service. The target id is 203.0.113.000 and the port is 21. As we can see the password is found out using the dictionary combination.

Graphical user interface

Description automatically generated

Figure 1.6

To find the RDP is open, nmap is opened and the following command is used:

**nmap 203.0.113.100 -p 3389**

A screenshot of a computer

Description automatically generated with medium confidence

Figure 1.7

The Microsoft Terminal Service is opened using mstsc. The RDP is opened.

Text

Description automatically generated

Figure 1.8

Logging into 192.168.1.10 server, the following command is used to add the incident responder to the IR.txt file: **echo Incident Responder Gowtham > IR.TXT**

The date and time command are used to add date to the IR.txt file. It is checked by using the type command.

Ipconfig /all >> IR.TXT command is used to add ip address information to the IR.txt file. To add the connection information to the incident response text file, the following command is used : **netstat -ano >> ir.txt** as seen in **figure 1.10.Text

Description automatically generated**

Figure 1.9

Text

Description automatically generated

Figure 1.10

The following command is used to add the process information to the IR.txt file : **tasklist >> ir.txt**

To view the svchost processes in the incident response text file, the following command is used:

**type ir.txt | find “svchost”**

Text

Description automatically generated

Figure 1.11

To add information about the logged-on users to the incident response text file, the following command is used : **psloggedon >> ir.txt**

To view the administrator account in the IR.txt file, the following command is used :

**type ir.txt | find “administrator”**

The user account information is added to the IR.txt file and the guest account are viewed. To hash the incident respond file and send the output to the hash.txt file, the following command is used :

**md5sum ir.txt >> hash.txt**

The file is checked by using **type hash.txt** command.