NMAP:

1. Install nmap:

```
sudo apt update
sudo apt install nmap
```

2. install Wireshark by running:

```
sudo apt install wireshark
```

3. Add your user to the wireshark group so you can run it without root privileges: (optional)

```
sudo usermod -aG wireshark $USER
```

Log out and log back in for the changes to take effect.

**Open Wireshark**:

- Type this in the terminal:

```
Wireshark
```

**Select the Network Interface**:

- In Wireshark, you will see a list of network interfaces. Choose the one that corresponds to the interface you're using (for example, eth0 for Ethernet or wlan0 for Wi-Fi).
- Double-click the interface to start capturing packets.

**Run the Nmap Command**

1. **Open another terminal** window while Wireshark is capturing traffic, and run the Nmap command:

```
sudo nmap -sS tsec.edu    or      sudo nmap -sT tsec.edu      or     sudo nmap -sU tsec.edu
-sN , -sF , -sX, -sA , -sO
```

s**udo nmap -sT tsec.edu**:

- This command performs a **TCP connect scan** on the target tsec.edu, attempting to establish a full TCP connection to each open port to determine its status.

**sudo nmap -sS tsec.edu**:

- This command conducts a **TCP SYN scan** on tsec.edu, sending SYN packets to probe open ports without completing the TCP handshake, making it faster and less detectable than a full connect scan.

**udo nmap -sN tsec.edu**

- **Explanation**: This command performs a **TCP NULL scan** on the target tsec.edu.

**Nmap (Network Mapper)**: Nmap is an open-source network scanning tool used to discover hosts and services on a computer network. It can be utilized for various purposes, including network inventory, managing service upgrade schedules, and monitoring host or service uptime.