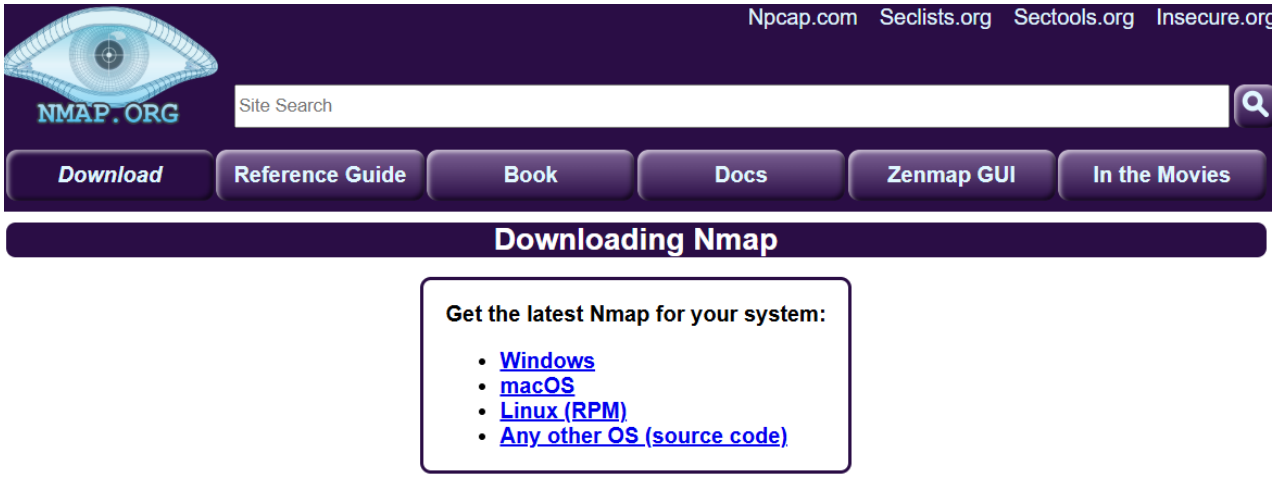
Vaibhav Dhonde
Cyber Security

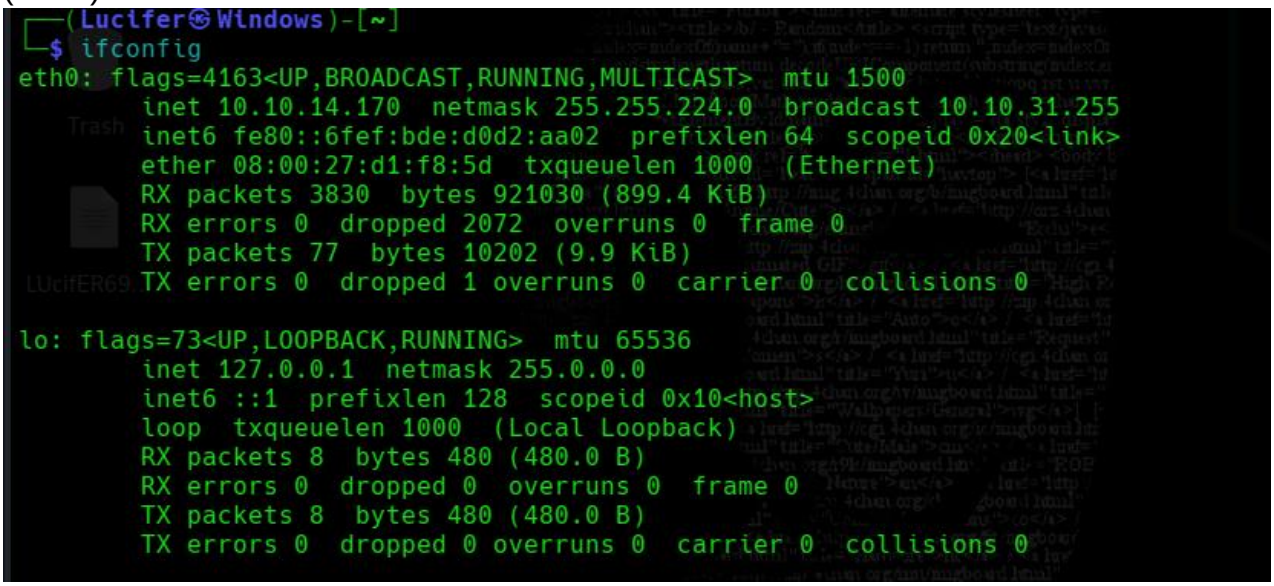
Nmap Scan & Wireshark Analysis Report

1. **Install Nmap:**
Download and install Nmap from official website: https://nmap.org/download.html



2. **Find Local IP Range:**

Command to check IP:
• ipconfig (Windows)
• ifconfig or ip addr
(Linux)



Example: 10.10.0.0/19

3. **Perform TCP SYN Scan:**
Command:
nmap -sS [Target ip-address]

```
┌──(Lucifer㉿Windows)-[~]
└─$ sudo nmap -sS  10.10.18.168
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 09:48 EDT
Nmap scan report for 10.10.18.168
Host is up (0.0042s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:69:AD:3C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

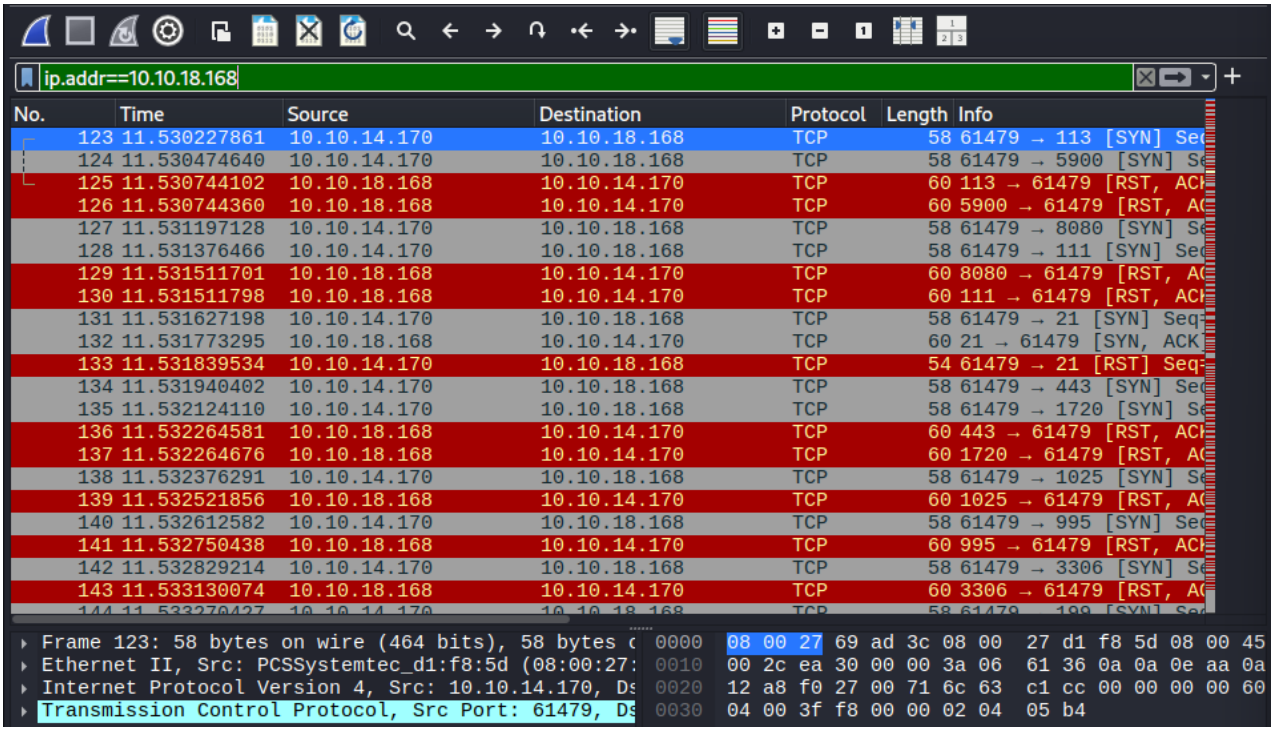
4. **Scan Results:**

10.10.14.116 - Ports: 21(FTP), 22 (SSH) and 80 (HTTP)

```
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:69:AD:3C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

5. **Wireshark Analysis:**
Captured packets during scan.



6. **Common Services on Ports:**
Port 80 → HTTP (Web Server)
Port 22 → SSH (Secure Shell)
Port 21 → FTP (File Transfer Protocol)

7. **Potential Security Risks:**
Port 80 (HTTP): No encryption, vulnerable to sniffing.
Port 22 (SSH): Brute-force risk with weak passwords.
Port 21 (FTP): Transmits data in plain text, making it vulnerable to sniffing, credential theft, and man-in-the-middle attacks.

8. **Save Scan Results:**
Exported scan results as text or HTML.