NETWORK SCANNING REPORT:

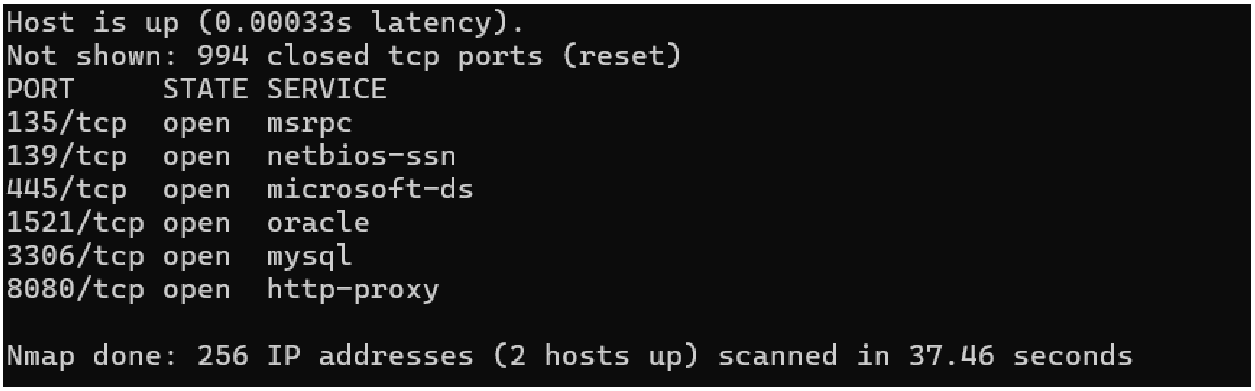
- ## Objective:
  - The purpose of this task was to perform a TCP SYN scan on a local network using Nmap to
    1. Discover active hosts with subnet
    2. Identify open TCP ports and services running on them
    3. Evaluate potential risks
- ## NOTE:
  - IP addresses will not be shown completely for security reasons
- ## Tools & Environment:

TOOLS	PURPOSE
NMAP	Network discovery and port scanning
Wireshark	Packet capture& Traffic analysis
OS	Windows

- ## Methodology:
  - Install Nmap from the official website
  - Identify the local IP range using ipconfig/ifconfig (e.g., 192.168.1.0/24)
  - Execute the following command: nmap -sS 192.168.1.0/24 to perform a TCP SYN scan
  - Capture packets with Wireshark using the display filter: tcp.flags.syn == 1 && tcp.flags.ack == 0 to observe SYN packets
- ## Results:

HOST IP ADDR	STATUS	OPEN PORTS	COMMON SERVICES
10.106.x.x	open	445	Microsoft-ds
10.106.x.x	open	8080	Http-proxy
10.106.x.x	open	1521	oracle

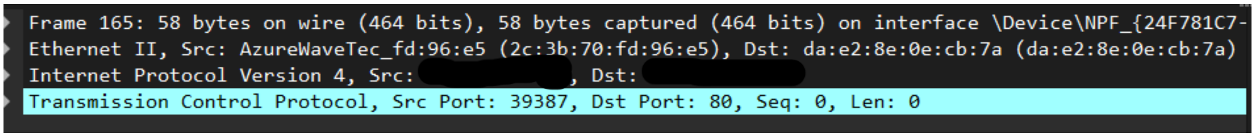
- Nmap Scan:



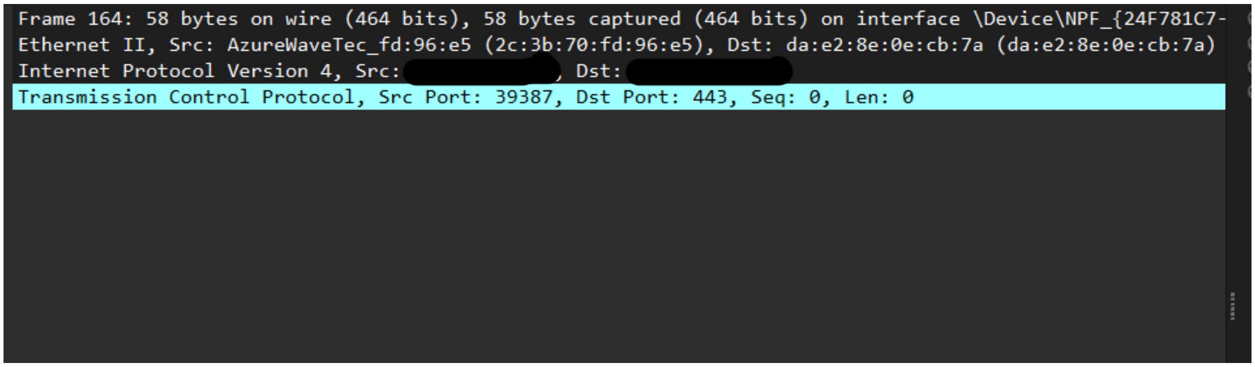
```
Host is up (0.00033s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1521/tcp open  oracle
3306/tcp open  mysql
8080/tcp open  http-proxy

Nmap done: 256 IP addresses (2 hosts up) scanned in 37.46 seconds
```

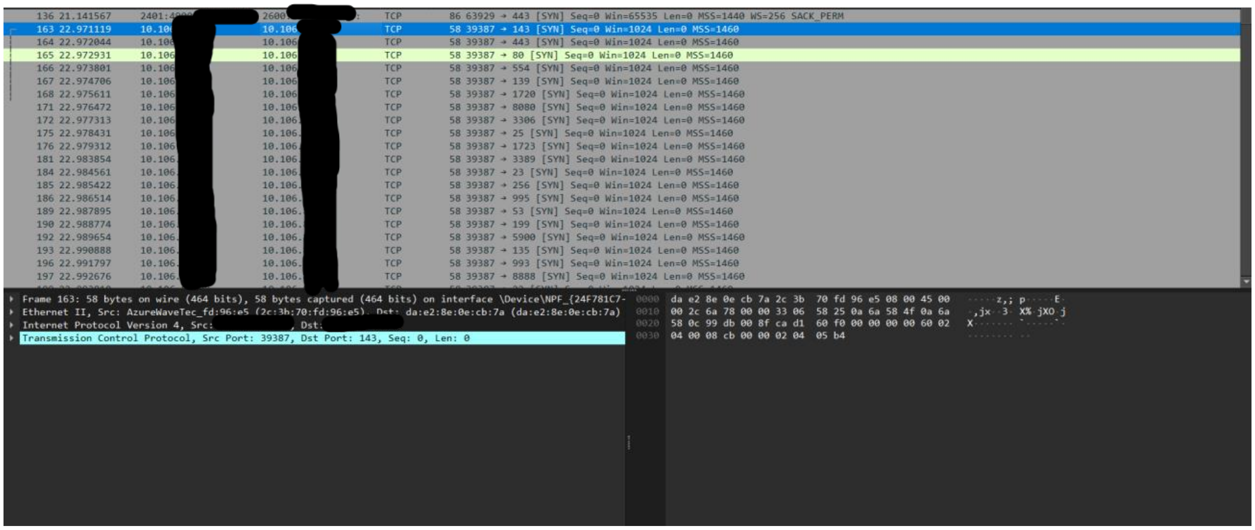
- Wireshark analysis:



```
Frame 165: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface \Device\NPF_{24F781C7-
Ethernet II, Src: AzureWaveTec_fd:96:e5 (2c:3b:70:fd:96:e5), Dst: da:e2:8e:0e:cb:7a (da:e2:8e:0e:cb:7a)
Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
Transmission Control Protocol, Src Port: 39387, Dst Port: 80, Seq: 0, Len: 0
```



```
Frame 164: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface \Device\NPF_{24F781C7-
Ethernet II, Src: AzureWaveTec_fd:96:e5 (2c:3b:70:fd:96:e5), Dst: da:e2:8e:0e:cb:7a (da:e2:8e:0e:cb:7a)
Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
Transmission Control Protocol, Src Port: 39387, Dst Port: 443, Seq: 0, Len: 0
```



```
136 21.141567  2401:4[redacted]  2600[redacted]  TCP  86 63929 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
163 22.971119  10.106        10.106        TCP  58 39387 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
164 22.972044  10.106        10.106        TCP  58 39387 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
165 22.972931  10.106        10.106        TCP  58 39387 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
166 22.973801  10.106        10.106        TCP  58 39387 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
167 22.974706  10.106        10.106        TCP  58 39387 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
168 22.975611  10.106        10.106        TCP  58 39387 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
171 22.976472  10.106        10.106        TCP  58 39387 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
172 22.977313  10.106        10.106.       TCP  58 39387 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
175 22.978431  10.106        10.106.       TCP  58 39387 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
176 22.979312  10.106        10.106.       TCP  58 39387 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
181 22.983854  10.106.       10.106.       TCP  58 39387 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
184 22.984561  10.106.       10.106.       TCP  58 39387 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
185 22.985422  10.106.       10.106.       TCP  58 39387 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
186 22.986514  10.106.       10.106.       TCP  58 39387 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
189 22.987895  10.106.       10.106.       TCP  58 39387 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
190 22.988774  10.106.       10.106.       TCP  58 39387 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192 22.989654  10.106.       10.106.       TCP  58 39387 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
193 22.990888  10.106.       10.106.       TCP  58 39387 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
196 22.991797  10.106.       10.106.       TCP  58 39387 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
197 22.992676  10.106.       10.106.       TCP  58 39387 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

```
Frame 163: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface \Device\NPF_{24F781C7-
Ethernet II, Src: AzureWaveTec_fd:96:e5 (2c:3b:70:fd:96:e5), Dst: da:e2:8e:0e:cb:7a (da:e2:8e:0e:cb:7a)
Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
Transmission Control Protocol, Src Port: 39387, Dst Port: 143, Seq: 0, Len: 0
```

```
0000  da e2 8e 0e cb 7a 2c 3b  70 fd 96 e5 08 00 45 00   ·····z,; p·····E·
0010  00 2c 6a 78 00 00 33 06  58 25 0a 6a 58 4f 0a 6a   ·,jx··3· X%·jXO·j
0020  58 0c 99 db 00 8f ca d1  60 f0 00 00 00 00 60 02   X······· `·····`·
0030  04 00 08 cb 00 00 02 04  05 b4                     ········ ··
```

- Analysis of Common services:

1. **HTTP Proxy (Port 8080)**
   An HTTP proxy forwards client requests to external servers for caching or filtering
2. **Oracle Database Listener (Port 1521)**
   This service accepts client connections to Oracle databases
3. **Microsoft-DS / SMB (Port 445)**
   Used for file sharing and Active Directory communication in Windows environments.

- Risks & vulnerabilities:
  1. **HTTP Proxy**
     If left open or unauthenticated, attackers can relay traffic through the proxy for malicious activity such as spam or phishing, creating legal and reputational risks.
  2. **Oracle Database Listener**
     Default configurations or weak database credentials can allow unauthorized database access, while outdated Oracle versions may contain critical vulnerabilities.
  3. **Microsoft-DS / SMB**
     This service has been exploited by ransomware campaigns such as WannaCry (EternalBlue/MS17-010) and can expose sensitive files if shares are misconfigured.
- Recommendation:
  1. **HTTP Proxy**
     Recommendation: require authentication, restrict usage to trusted internal networks, and monitor logs for abnormal traffic.
  2. **Oracle Database Listener**
     Recommendation: disable default/sample accounts, enable listener password authentication, restrict access by IP, and apply Oracle Critical Patch Updates regularly.
  3. **Microsoft-DS / SMB**
     Recommendation: disable SMBv1, apply the latest Windows security patches, enforce strong authentication (Kerberos/NTLMv2), and limit share permissions.
  4. Close or disable unused ports/services.

5. Enforce strong passwords and enable multi-factor authentication. • Keep firmware and software up to date.
6. Use a firewall to restrict unnecessary inbound/outbound traffic.

- conclusion:

  1. The TCP SYN scan successfully identified active hosts and open services within the local subnet. Implementing the recommended security measures will help reduce the attack surface and protect network resources.