Task 1: Scan Your Local Network for Open Ports

Cybersecurity Lab Report

KANDI TEJASREE
ELEVATE LABS

Task 1:

Scan Your Local Network for Open Ports

Index:

Installation of Nmap from official website.

Finding local IP range.

Running: nmap -sS 192.168.183.0/24 to perform TCP SYN scan.

Note of IP addresses and open ports found.

Analyzing packet capture with Wireshark.

Research on common services running on those ports.

Identifying potential security risks from the open ports.

Objective:

To discover open ports and active devices within the local network and analyze possible security risks using tools like Nmap and Wireshark.

Tools Used

Nmap (Network Mapper)

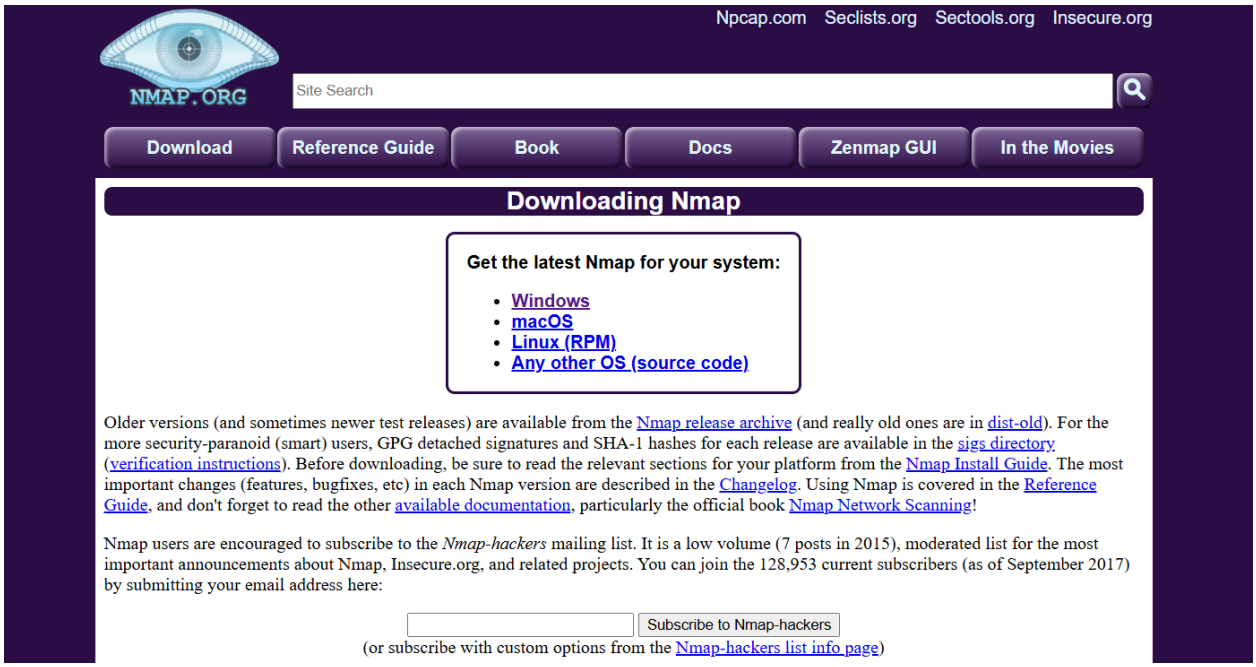
Wireshark (optional)

Environment Setup

Operating System: Linux
Local IP Address: 192.168.183.1
Netmask: 255.255.255.0
Local IP Range: 192.168.183.0/24

Steps Performed:

Installation of Nmap from official website.



Finding Local IP Range

Used ipconfig command to determine:

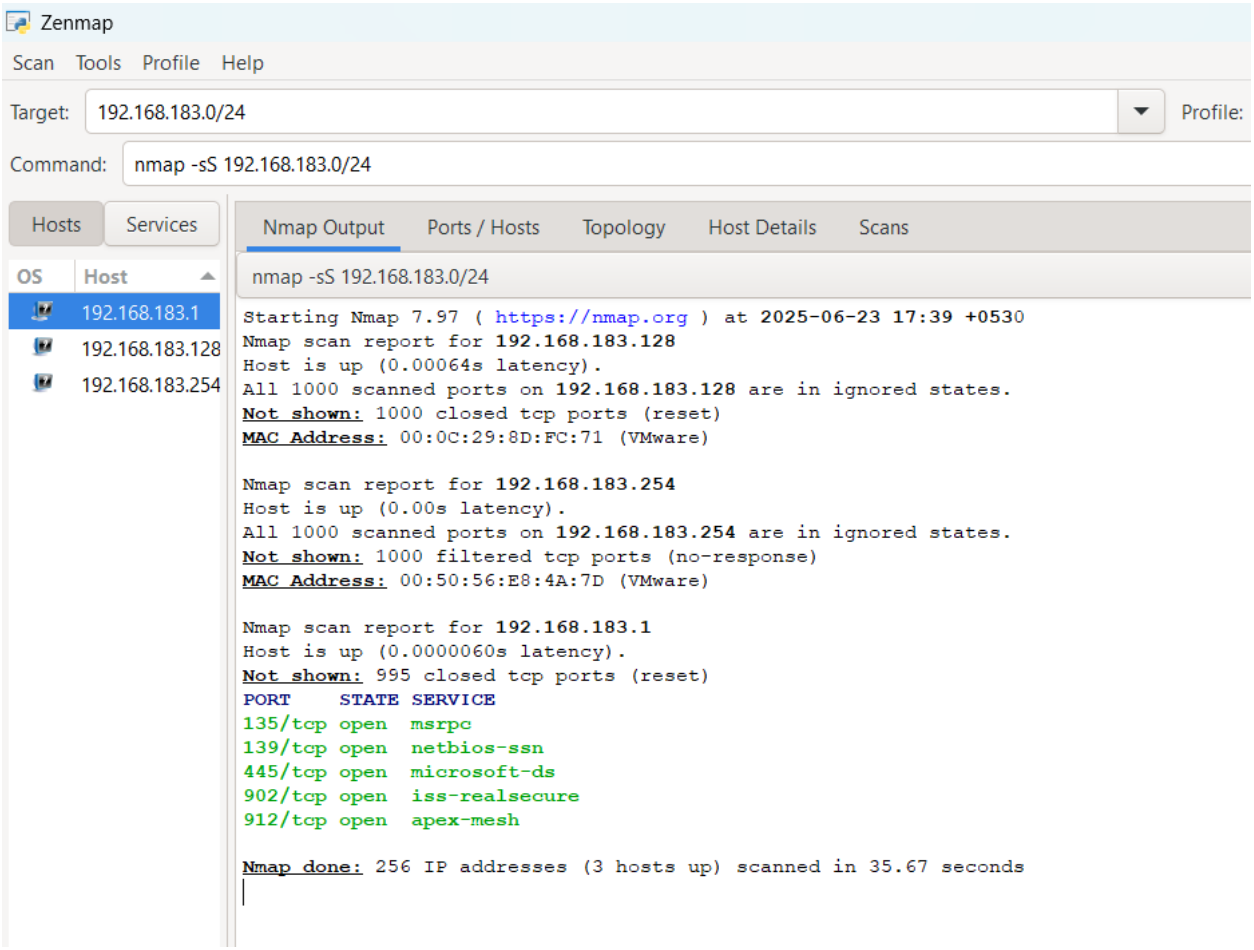
IP: 192.168.183.1

Subnet Mask: 255.255.255.0 → CIDR: /24

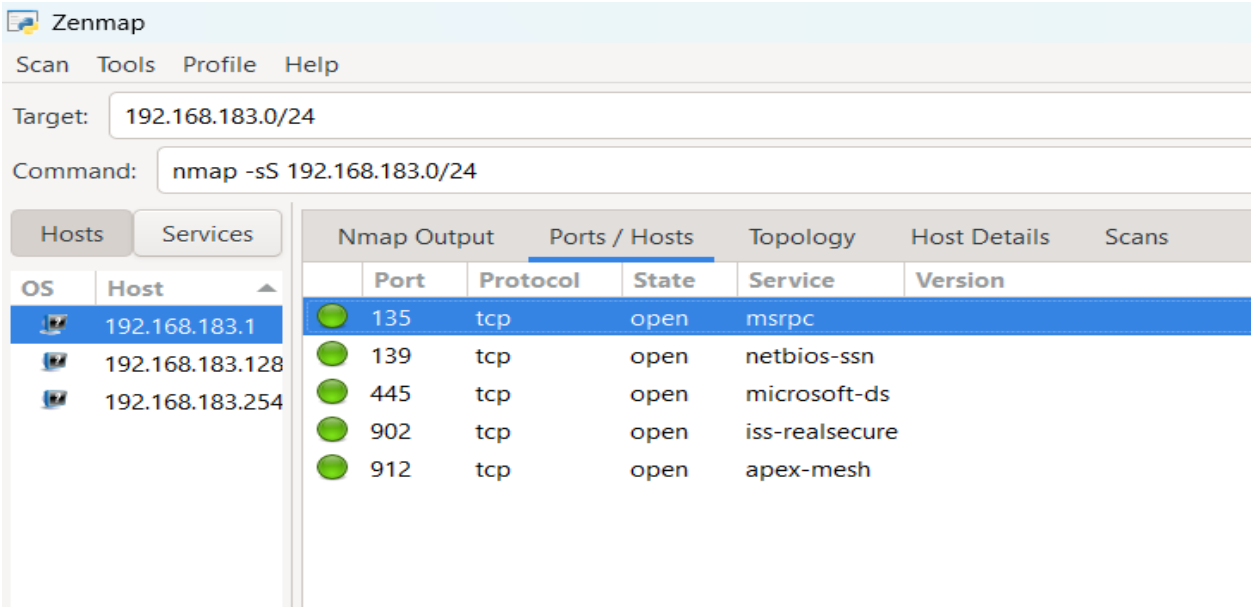
IP Range: 192.168.183.0/24

```
Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::80a8:8d8c:e973:696b%19
   IPv4 Address. . . . . . . . . . . : 192.168.183.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9af2:cf55:4dd1:5a86%10
   IPv4 Address. . . . . . . . . . . : 10.68.20.196
   Subnet Mask . . . . . . . . . . . : 255.255.224.0
   Default Gateway . . . . . . . . . : 10.68.0.1

Ethernet adapter Bluetooth Network Connection:
```

Running: nmap -sS 192.168.183.0/24 **to perform TCP SYN scan.**



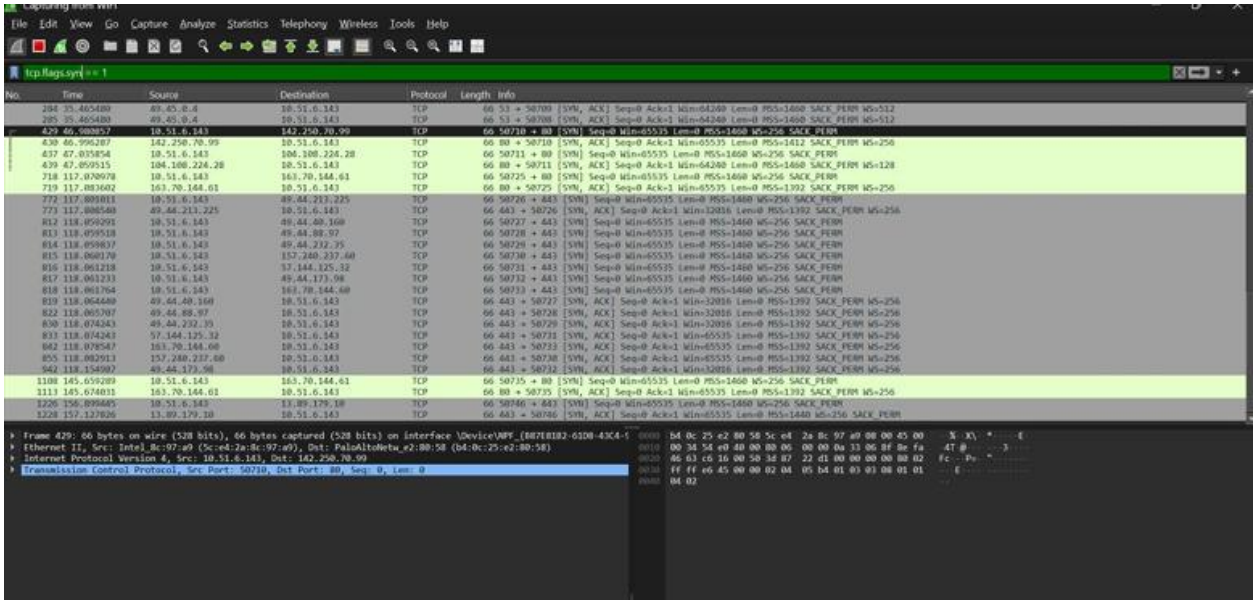
Result:



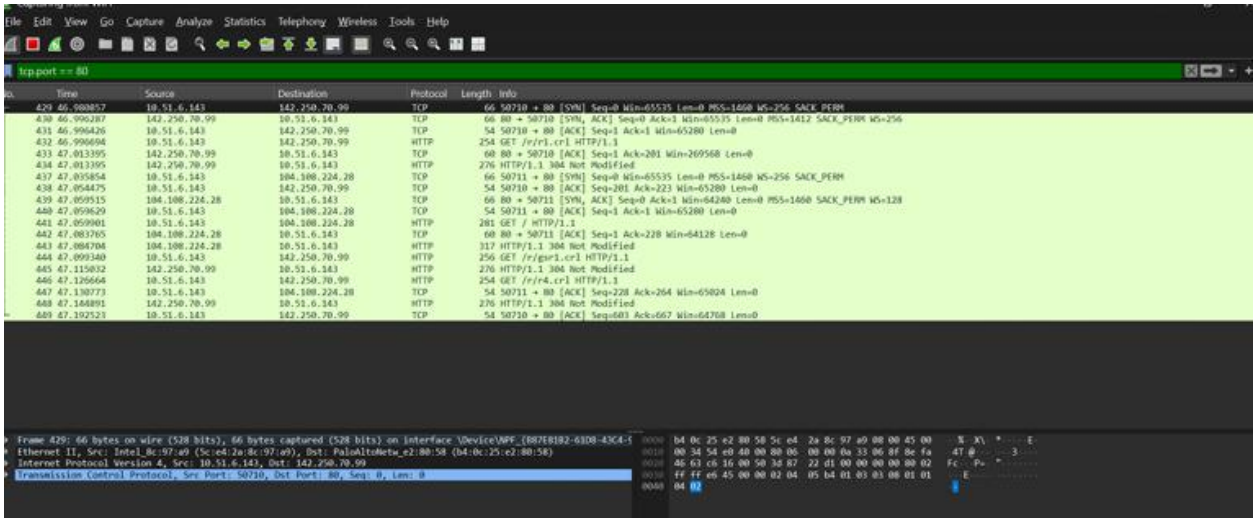
Analyzing packet capture with Wireshark

Started packet capture during Nmap scan. Applied filters such as:

- tcp.port.syn == 1



- tcp.port == 80



Identified Services

Identified the following services through the scan I performed using Nmap on my local network. These open ports revealed which services were running on the devices connected to the network:

Common ports and services identified:

Port	Protocol	Service Name	Description
135	TCP	msrpc	Microsoft RPC service
139	TCP	netbios-ssn	NetBIOS Session Service (Windows)
445	TCP	microsoft-ds	SMB file sharing
902	TCP	iss-realsecular	VM ware remote console
912	TCP	apex-mesh	Monitoring

Security Analysis:

- **Port 135 (msrpc):**

Risk: Can be abused for DCOM/RPC-based attacks.

Recommendation: Block this port on external interfaces; monitor for RPC activity internally.

- **Port 139/445 (NetBIOS/SMB):**

Risk: Common target for malware and lateral movement.

Recommendation: Disable if file sharing isn't needed; restrict access using firewall rules.

- **Port 902 (VMware Remote Console / VMCI)**

Risk: Can be exploited to gain unauthorized access to VMware ESXi hosts or VM's

Recommendation: Restrict to trusted IPs; block on external interfaces; keep VMware components patched.

- **Port 915 (Unassigned / Custom Use)**

Risk: Typically unused by standard services; may be used by custom or rogue applications.

Recommendation: Investigate active services; block unless explicitly needed; monitor for suspicious activity.

Conclusion:

Using **Nmap**, I scanned my local network and identified active devices and open TCP ports, gaining insight into exposed services. To deepen my understanding, I analyzed the scan traffic with **Wireshark**, which revealed how scanning works at the packet level. This exercise highlighted the importance of regularly auditing internal network services to maintain security and proper configuration.