TASK 1: SCAN YOUR LOCAL NETWORK FOR OPEN PORTS

Cybersecurity Lab Report

VOONNA VENKATESH
ELEVATE LABS

Task 1:

Scan Your Local Network for Open Ports

Index

1. Installation of Nmap from official website.
2. Finding local IP range.
3. Running: nmap -sS 192.168.1.0/24 to perform TCP SYN scan.
4. Note of IP addresses and open ports found.
5. Analyzing packet capture with Wireshark.
6. Research on common services running on those ports.
7. Identifing 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)

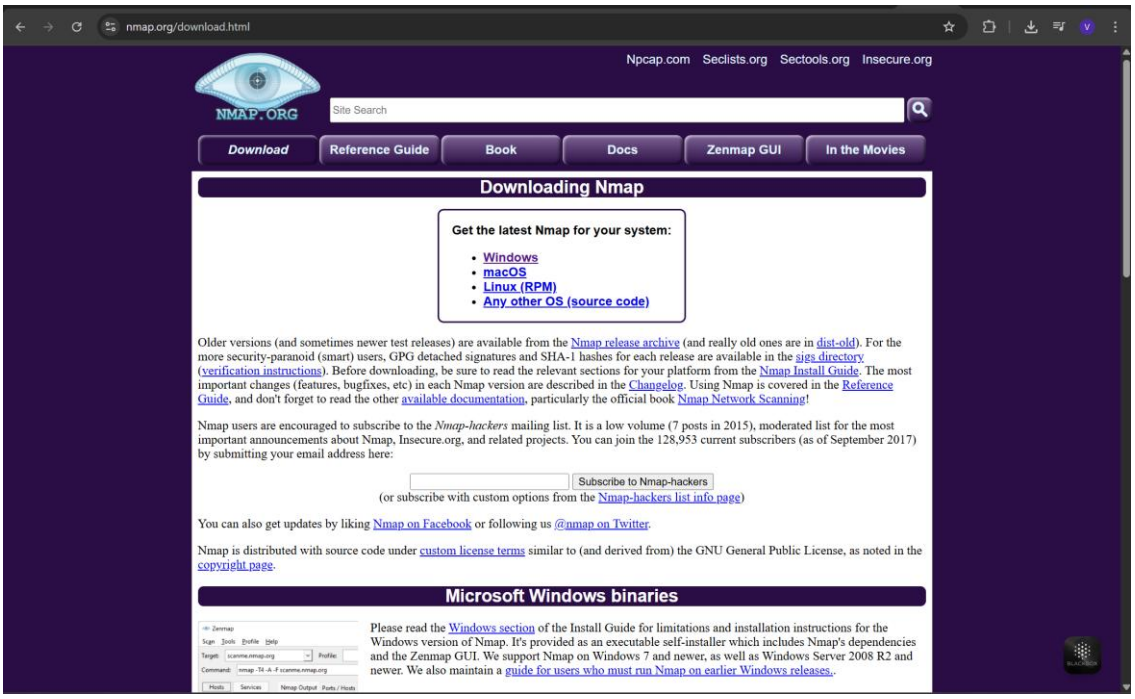
Environment Setup

Operating System: Linux
Local IP Address: 192.168.15.132
Netmask: 255.255.255.0
Local IP Range: 192.168.15.0/24

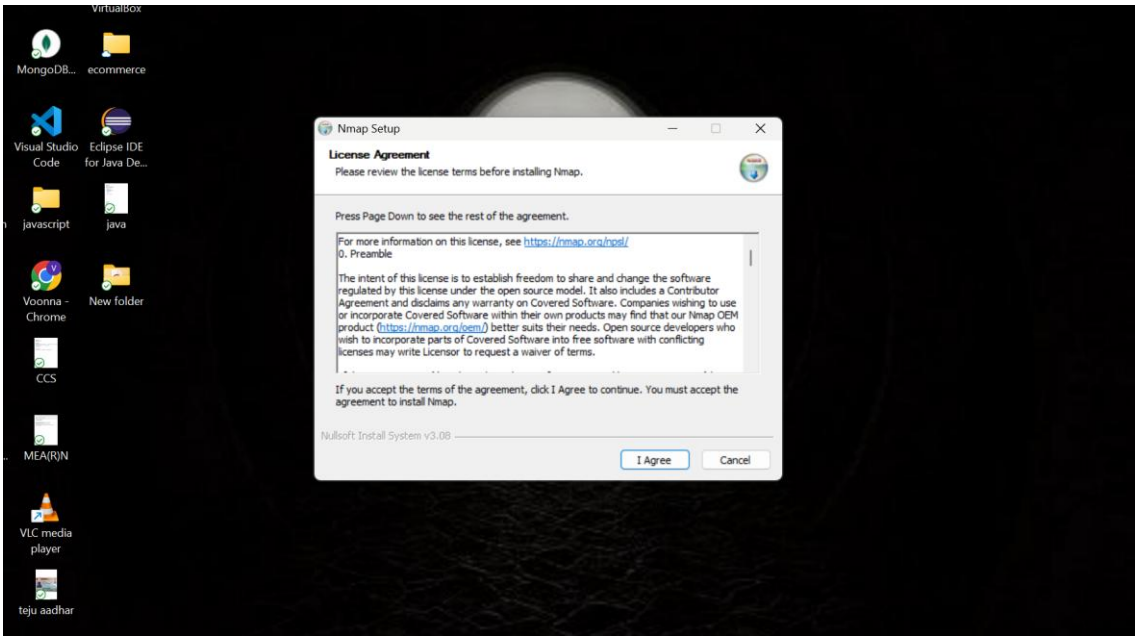
Steps Performed:

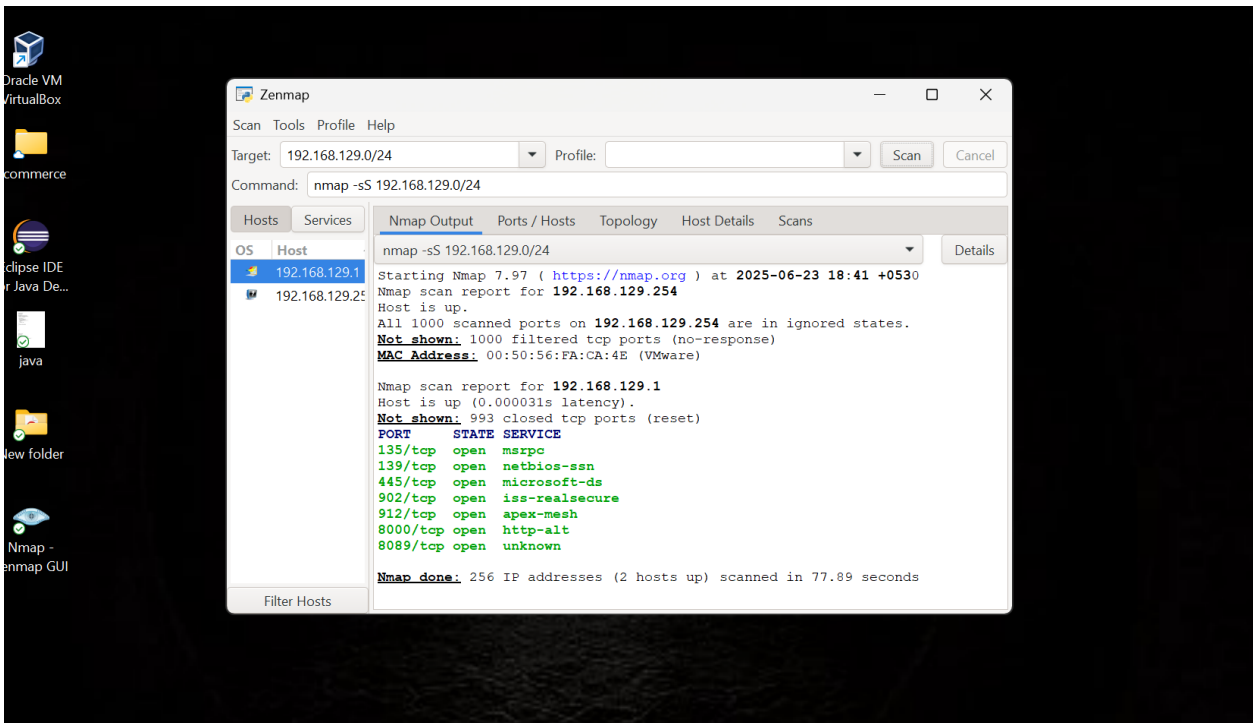
1. Installation of Nmap from official website.

Windows:



Complete the setup:

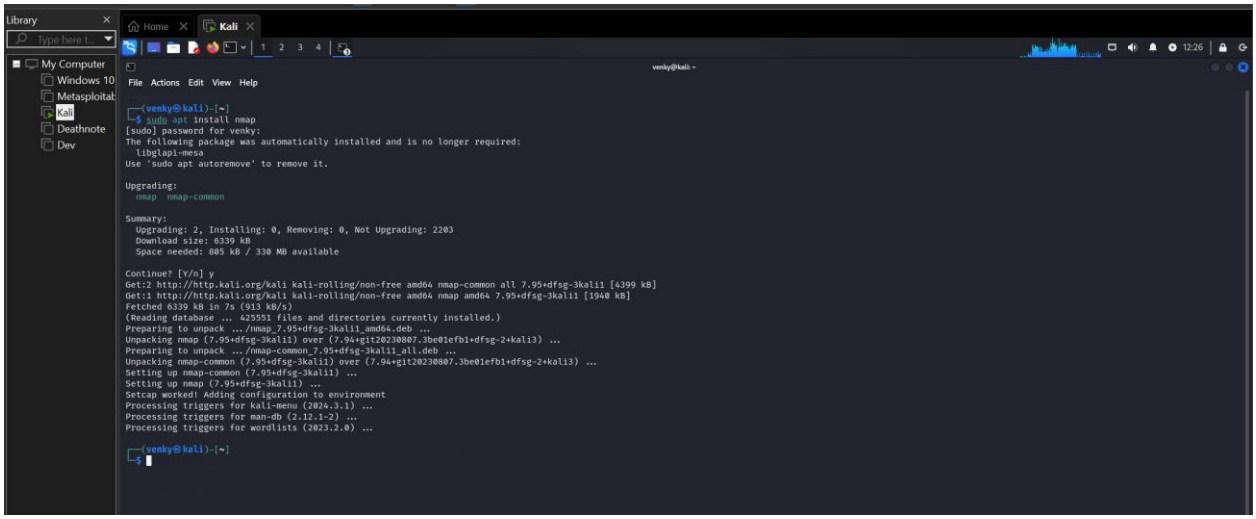




(Or)

Linux:

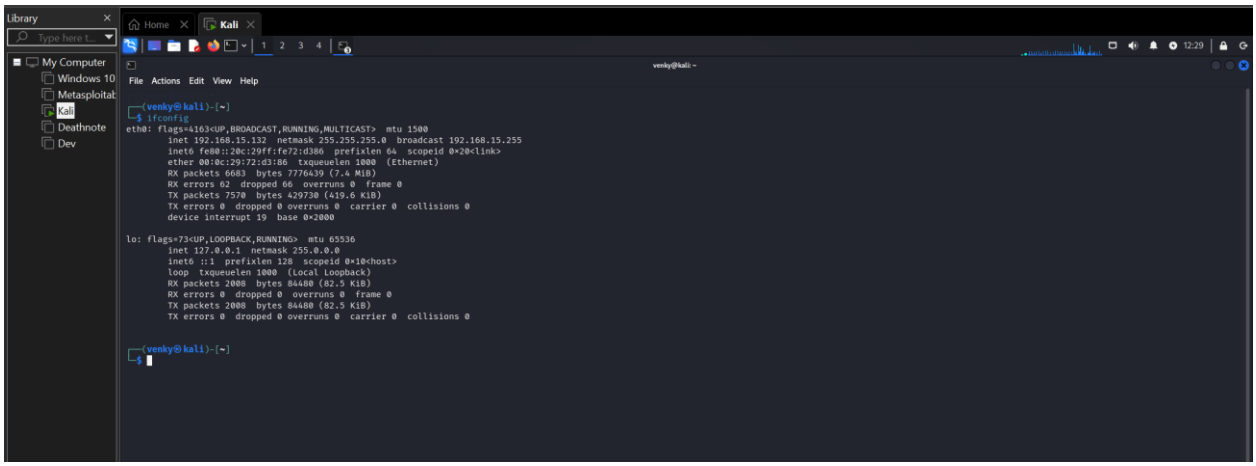
Sudo apt install nmap



2. Finding Local IP Range

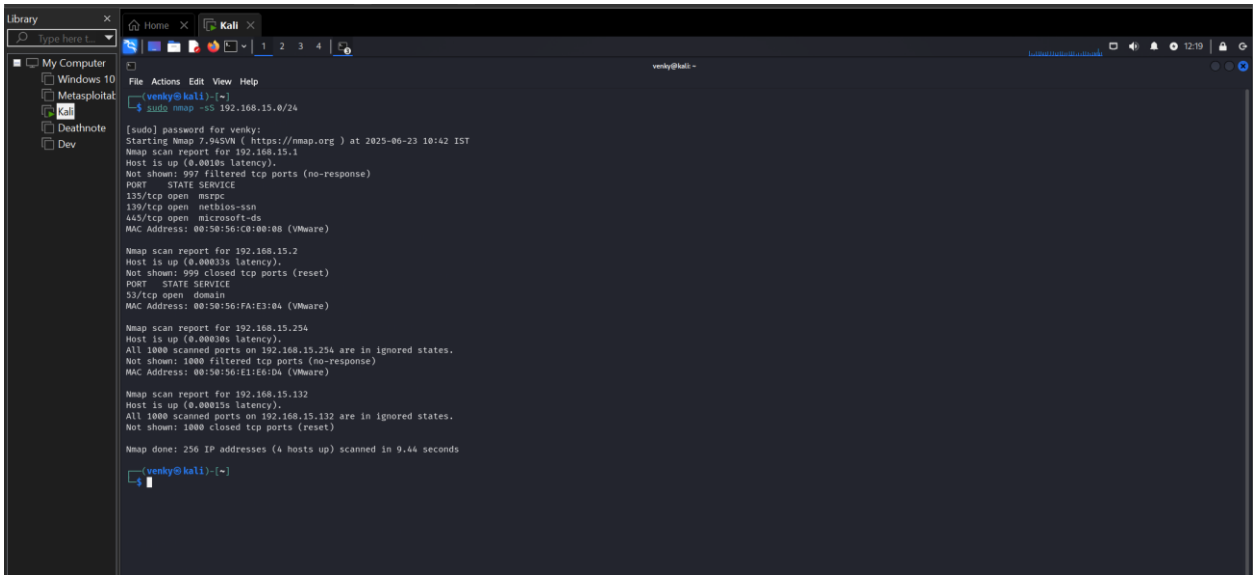
Used ifconfig command to determine:

- IP: 192.168.15.132
- Subnet Mask: 255.255.255.0 → CIDR: /24
- IP Range: 192.168.15.0/24



3. Running: nmap -sS 192.168.1.0/24 to perform TCP SYN scan.

```
nmap -sS 192.168.15.0/24
```



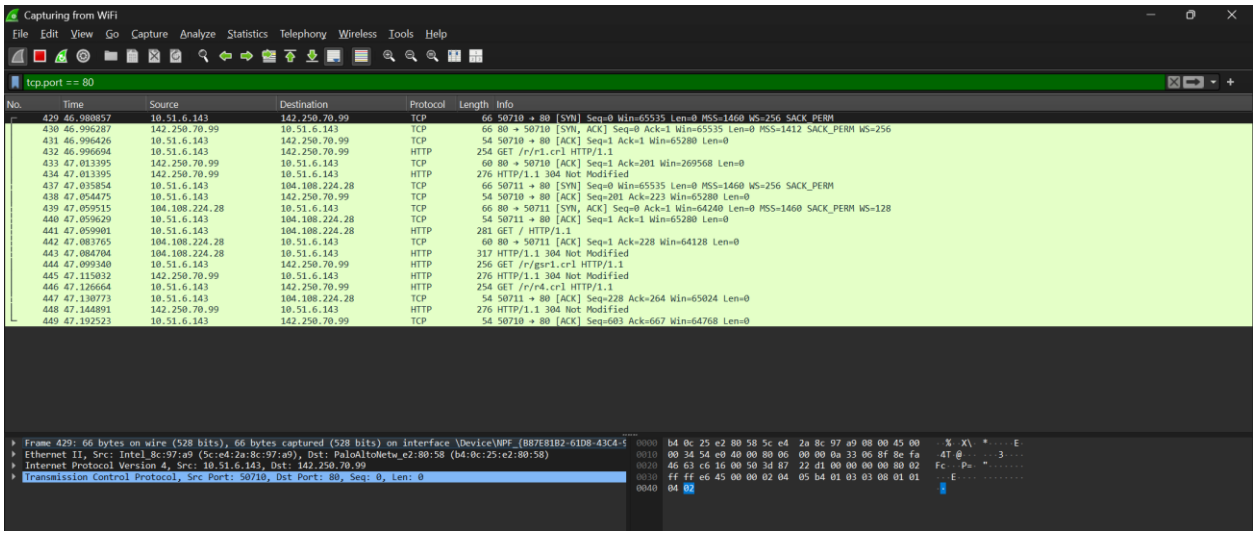
Result:

```
PORT      STATE   SERVICE
135/tcp   open    msrpc
139/tcp   open    netbios-ssn
445/tcp   open    microsoft-ds
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.15.2
Host is up (0.0018s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE   SERVICE
53/tcp    open    domain
MAC Address: 00:50:56:FA:E3:04 (VMware)

Nmap scan report for 192.168.15.254
Host is up (0.00037s latency).
All 1000 scanned ports on 192.168.15.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E1:E6:D4 (VMware)

Nmap scan report for 192.168.15.132
```

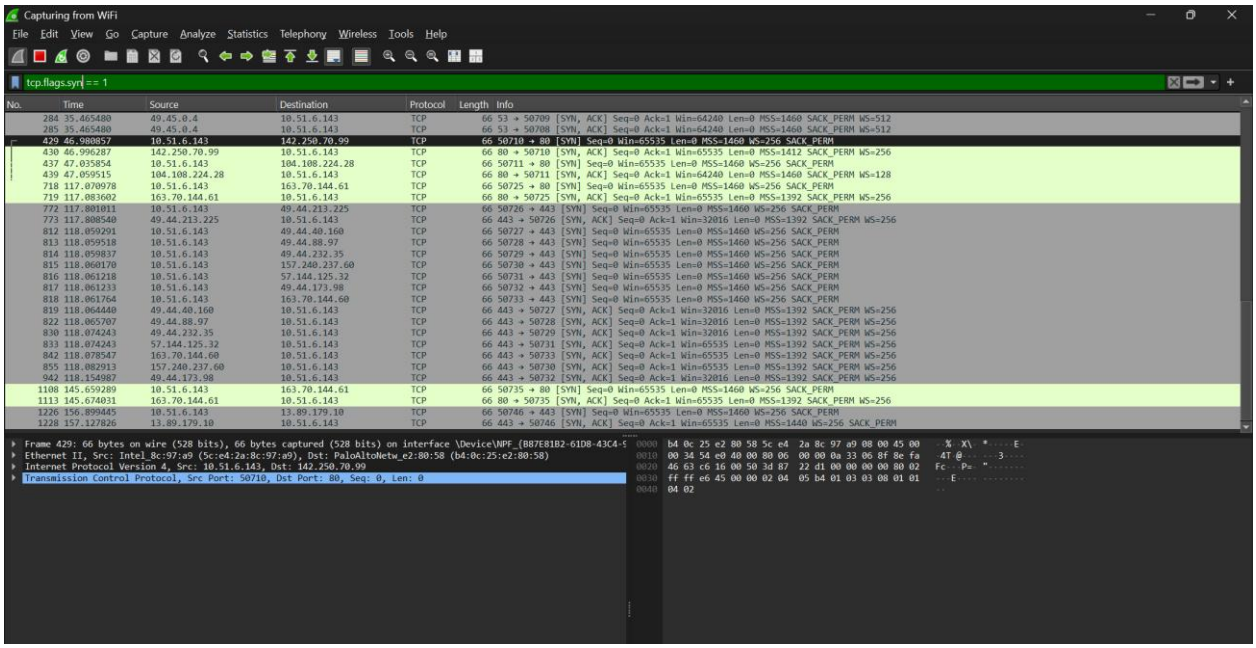
4. Analyzing packet capture with Wireshark

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

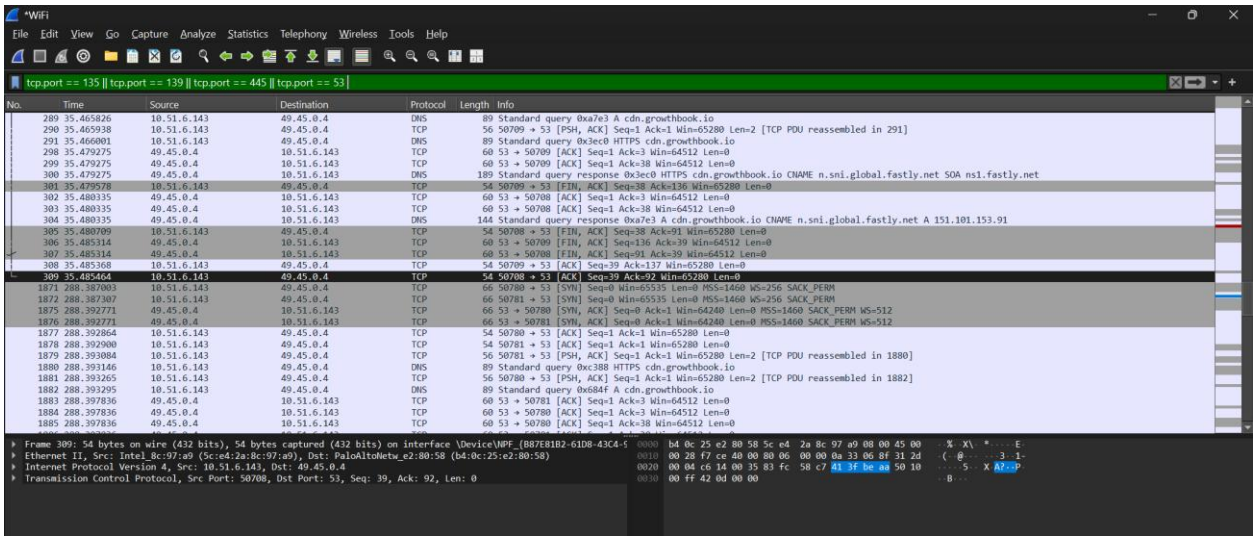
```
tcp.port == 80
```



tcp.port.syn == 1



tcp.port == 135 || tcp.port == 139 || tcp.port == 445 || tcp.port == 53



5. 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
53	TCP	domain	DNS service

6. 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 53 (DNS):

- Risk: If open to the internet, may be used for DNS amplification attacks.
- Recommendation: Ensure it is only accessible internally; use secure DNS configurations.

Conclusion:

During this task, I used Nmap to scan my local network and successfully discovered active devices along with their open TCP ports. Among the services I identified were MSRPC (port 135), NetBIOS/SMB (ports 139 and 445), and DNS (port 53). While these services are important for Windows-based network operations, they can also introduce security risks if they’re not properly secured or configured.

To better understand the network activity during the scan, we also used Wireshark to analyze packet-level traffic. This gave us deeper insight into how the scanning process works behind the scenes.

Overall, this exercise highlighted how essential it is to regularly scan and review internal network services. Identifying open ports and understanding the services behind them is a key part of maintaining a secure and well-managed network environment.