Title: Task 1: Basic Network Reconnaissance using Nmap

Prepared by: Nishant Deshmukh

Email: nishantdeshmukh996@gmail.com

Date: September 22, 2025

1. Objective

The primary objective of this task was to perform a basic network scan on my local network. The goal was to identify active devices, discover open ports on those devices, and analyze potential security risks associated with the open services.

2. Tools Used

- **Nmap (Network Mapper):** The core tool used for network discovery and security auditing.
- **Wireshark:** Used to capture and analyze the network packets generated during the scan for a deeper understanding of the process.
- **Operating System:** Kali Linux in a VirtualBox.

3. Methodology

I followed a systematic approach to scan the network and document the findings:

1. **Host Discovery:** I first performed a Ping Scan (-sn) to discover which hosts were active on my local network (192.168.43.0/24). This initial step prevents wasting time scanning inactive IPs. The command used was:

Command:

```
sudo nmap -sn 192.168.43.85/24
```

2. **Port Scanning:** After identifying the live hosts, I executed a TCP SYN scan (-sS) against the same network range. This scan is efficient for checking the most common 1000 ports on the active devices. The command used was:

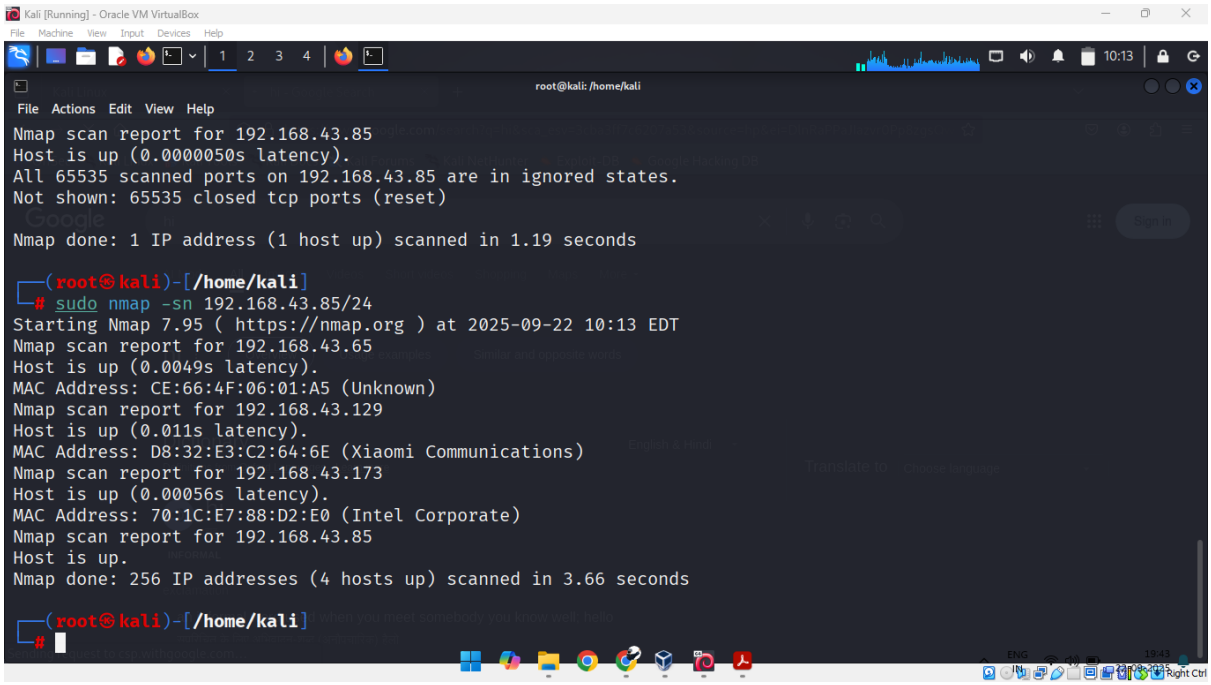
Command:

```
sudo nmap -sS 192.168.43.85/24
```

3. **Packet Analysis:** While the Nmap scans were running, I used Wireshark to capture live network traffic. This allowed me to observe the ARP requests used for host discovery and the TCP packets from the port scan in real time.
4. **Data Collection & Documentation:** I took screenshots of the scan results and Wireshark captures, then compiled them into this report for analysis.

4. Scan Results & Findings

The initial host discovery scan found 4 active devices on the network. The subsequent port scan provided details on the services running on them.

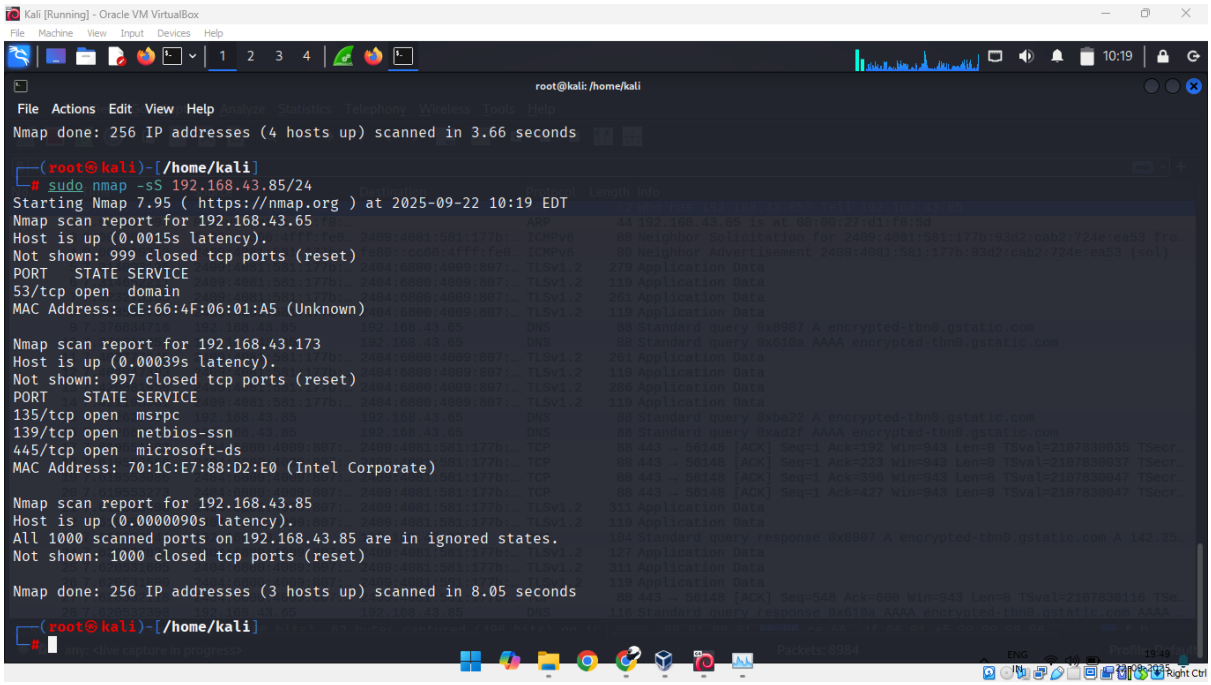


Host IP: 192.168.43.65

- **Device Details:** MAC Address CE:66:4F:06:01:A5 (Unknown Manufacturer).
- **Open Ports Found:**
    - **Port 53/tcp:** Service domain (DNS - Domain Name System).

Host IP: 192.168.43.173

- **Device Details:** MAC Address 70:1C:E7:88:D2:E0 (Intel Corporate). This is likely a Windows PC or laptop.
- **Open Ports Found:**
    - **Port 135/tcp:** Service msrpc (Microsoft Remote Procedure Call).
    - **Port 139/tcp:** Service netbios-ssn (NetBIOS Session Service).
    - **Port 445/tcp:** Service microsoft-ds (Microsoft Directory Services, used for SMB).

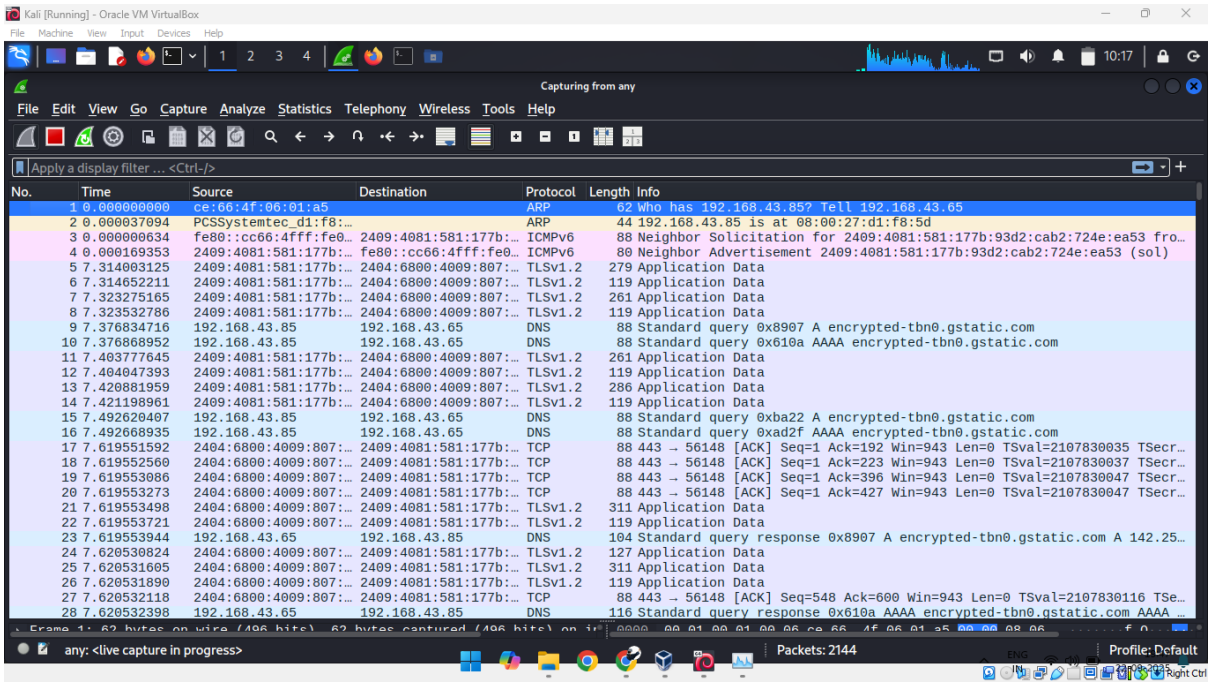


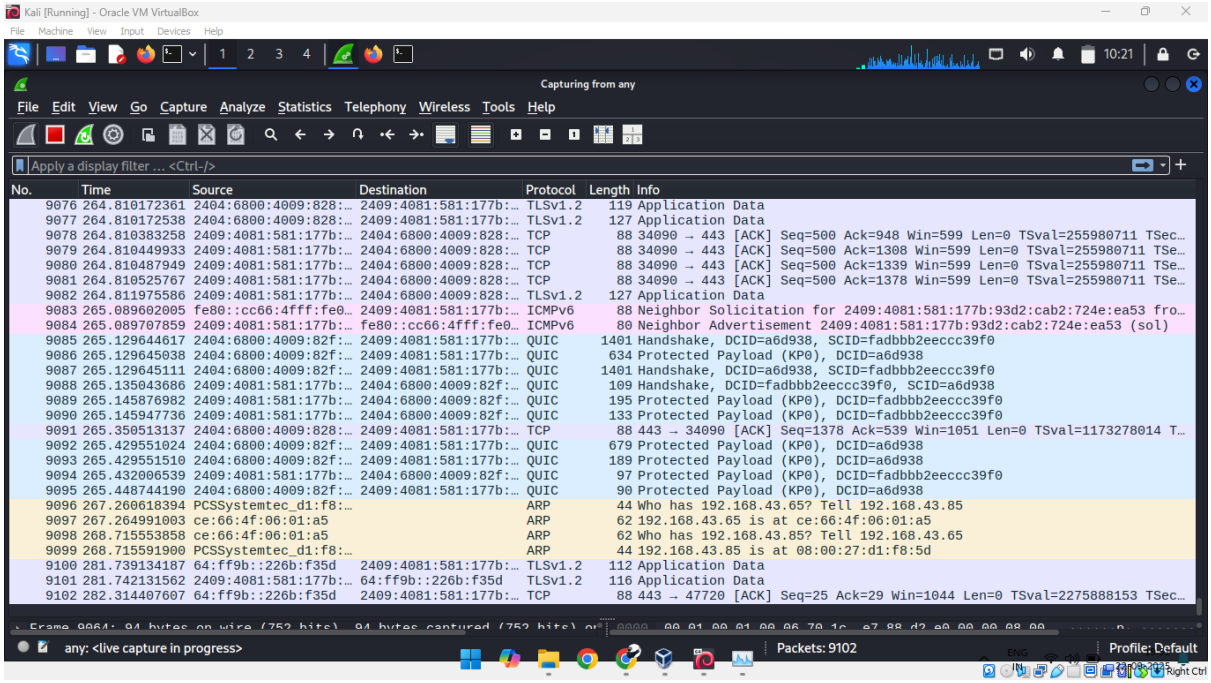
Other Hosts:

- **192.168.43.129 (Xiaomi):** This device was found to be active but did not have any of the top 1000 TCP ports open.
- **192.168.43.85 (Kali Host):** This is the machine I was scanning from.

5. Live Packet Capture Analysis

The Wireshark capture confirmed the network activity from the Nmap scans. I could clearly see the ARP requests ("Who has 192.168.43.65?") that Nmap uses to find devices, followed by TCP SYN packets sent to various ports on the target machines to check if they are open.





6. Analysis and Potential Security Risks

Based on the scan results, I identified the following potential risks:

- **Host 192.168.43.65 (DNS Server):** An open DNS port is usually normal for a router. If it's a misconfigured server, it could potentially be used in DNS-based attacks.
- **Host 192.168.43.173 (Windows Machine):** This host presents the most significant potential risk.

- The open ports **135, 139, and 445** are classic indicators of a Windows machine and are related to file and printer sharing (SMB/NetBIOS).
- The SMB protocol (Port 445) has historically been a major target for attackers. Vulnerabilities like **EternalBlue** specifically targeted this service. If this machine is not fully patched, it could be highly vulnerable to remote attacks, even within a local network.

7. Conclusion

This task was a successful practical exercise in network scanning. Using Nmap, I effectively mapped my local network, identified a Windows machine, and discovered potentially risky file-sharing services running on it. The Wireshark capture provided excellent insight into the underlying mechanics of the scanning process. This exercise highlights the critical importance of keeping all systems, especially those running services like SMB, fully updated with the latest security patches.

8.References

Websites and Youtube channels

- **GeeksforGeeks - Nmap Stealth Scan:** https://www.geeksforgeeks.org/nmap-stealth-scan-ss/
- **Varonis - What is Port 445?:** https://www.varonis.com/blog/what-is-port-445
- **YouTube - ARP Explained:** https://www.youtube.com/watch?v=pkb6VjMo6oY
- **NetworkChuck:** https://youtube.com/c/NetworkChuck
- **David Bombal:** https://youtube.com/c/DavidBombal
- **The Cyber Mentor:** https://youtube.com/c/TheCyberMentor