Elevate Labs
Cybersecurity Internship Report

Task 1: Scanning Local Network for Open TCP Ports using Nmap

Submitted by: Namita Rana

Role: Cybersecurity Intern

Company: Elevate Labs

Internship Duration: 04 August 2025 – 18 September 2025

Date of Submission: 04 August 2025

Privacy & Ethical Use Notice

All IP addresses, services, and host information used in this report are collected from a private local area network (LAN) strictly for educational and internship project purposes. No external or unauthorized systems were scanned.

Any MAC addresses or device names included have been anonymized or masked to preserve privacy. This report complies with ethical scanning practices and contains no personally identifiable information (PII) or exploitable data.

Unauthorized use, distribution, or modification of this report outside the intended academic or internship context is strictly prohibited.

Acknowledgement

I would like to express my sincere gratitude to **Elevate Labs** for providing me the opportunity to undertake an internship and work on real-world cybersecurity tasks. The chance to work on this project, has been an invaluable learning experience that has significantly enriched my practical knowledge in network reconnaissance and vulnerability analysis.

I extend my appreciation to the entire security team at **Elevate Labs** for fostering a professional learning environment and providing access to the necessary tools, systems, and documentation that facilitated hands-on experience with industry-standard scanning techniques.

This project not only improved my technical abilities with tools like **Nmap**, but also enhanced my analytical thinking, documentation skills, and understanding of real-time security practices. It reinforced the importance of ethical scanning, risk evaluation, and the need for ongoing security vigilance in modern networks.

— Namita Rana

Table of Contents

Chapter 1. Introduction

1.1 Objective

The objective of this task is to conduct a network host and port discovery using a **TCP SYN scan** via **Nmap** on a **Windows-based system**. This type of scan is particularly useful for identifying open TCP ports on remote devices without completing the full TCP handshake, making it stealthier than a full connection scan.

Key goals of this task include:

- Identifying live devices on the network.
- Determining which TCP ports are open on those hosts.
- Gaining insights into potential services running on the discovered hosts.
- Providing groundwork for further enumeration or security testing.
- Verifying firewall rules and host configurations.

SYN scanning is more suitable for active port discovery than ARP or ICMP scans, especially when dealing with firewall or IDS configurations. It is often referred to as **half-open scanning** since it does not complete the TCP handshake, reducing the likelihood of detection.

1.2 Tools and Environment Used

1.2.1 Tool: Nmap (Network Mapper)

- Nmap is an open-source network scanning utility used to discover devices, ports, and services.
- The -sS option is used to perform a SYN scan.
- Nmap attempts to initiate a TCP handshake by sending a SYN packet and listening for SYN-ACK responses.

1.2.2 Operating System: Windows 11

- Nmap was installed using the official setup executable from: https://nmap.org/download.html
- Commands were executed via Command Prompt in administrator mode.

1.2.3 Network Configuration

- Local IP and subnet details were obtained using:

```
ipconfig
```

- Subnet range was determined based on the IP address and subnet mask. For example, if the IP is 192.168.10.10 with subnet 255.255.255.0, the target becomes 192.168.10.0/24.

Note : *All IP Addresses listed in the report are from a local private network used for testing purpose only***.**

1.2.4 Output Management

- Scan results were saved in text format for documentation using:

```
nmap -sn 192.168.10.0/24 -oN arp_scan_results.txt
```

Chapter 2. Methodology

2.1 Step-by-Step Procedure

This section details the process followed to perform a TCP SYN scan on the local network using Nmap on Windows.

Step 1: Install Nmap on Windows

- Download Nmap from https://nmap.org/download.html
- Run the setup (nmap-setup.exe)
- Select the CLI and Zenmap options during installation

Step 2: Identify Local IP and Subnet Range

1. Open Command Prompt
2. Enter:

```
ipconfig
```

3. Note the IPv4 Address and Subnet Mask
   Example:
   - IP: 192.168.31.37
   - Subnet: 255.255.255.0
     Range: 192.168.31.0/24

Note : *All IP Addresses listed in the report are from a local private network used for testing purpose only.*

Step 3: Perform the SYN Scan

1. Open Command Prompt as Administrator
2. Run the command:

```
nmap -sS 192.168.31.0/24
```

   - -sS: Initiates a TCP SYN scan
   - This scan sends SYN packets and identifies open ports via SYN-ACK responses

---

Step 4: Save the Results

To save the scan output for documentation:

```
nmap -sS 192.168.0.0/24 -oN arp_scan_results.txt
```

This stores the output in a text file named arp_scan_results.txt in the same directory.

Step 5: Analyze Results

After the scan completes:

- Note which IPs responded with open ports
- Review detected port numbers and inferred services
- Classify any unexpected services for further security analysis

---

Chapter 3. Scan Results

3.1 Command Executed

To perform a SYN scan across the subnet, the following command was executed:

```
nmap -sS 192.168.31.0/24
```

This scan probes each IP in the range and attempts to detect which TCP ports are open by sending SYN packets.

3.2 Output

Below is a sample of the output received from the SYN scan. This reflects how Nmap reports live hosts with their IP and Open Ports :

Starting Nmap 7.95 (https://nmap.org) at 2025-08-04 19:51 IST

Nmap scan report for Router (192.168.31.1)

Host is up (0.022s latency).

Not shown: 994 closed tcp ports (reset)

PORT STATE SERVICE

53/tcp open domain

80/tcp open http

443/tcp open https

7443/tcp open oracleas-https

8080/tcp open http-proxy

8443/tcp open https-alt

MAC Address: 98:87:4C:xx:xx:xx (Vendor Hidden)

Nmap scan report for Android Tablet (192.168.31.38)

Host is up (0.11s latency).

Not shown: 998 closed tcp ports (reset)

PORT STATE SERVICE

787/tcp filtered qsc

8193/tcp filtered sophos

MAC Address: E2:EB:47:xx:xx:xx (Vendor Hidden)

Nmap scan report for Smartphone Device (192.168.31.209)

Host is up (0.0039s latency).

All 1000 scanned ports on 192.168.31.209 are in ignored states.

Not shown: 1000 closed tcp ports (reset)

MAC Address: A2:7F:76:xx:xx:xx (Vendor Hidden)

Nmap scan report for Windows Laptop (192.168.31.37)

Host is up (0.00037s latency).

Not shown: 995 closed tcp ports (reset)

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

2869/tcp open icslap

3306/tcp open mysql

Nmap done: 256 IP addresses (4 hosts up) scanned in 291.58 seconds

Note : *MAC address partially masked for privacy.*

3.3 Summary Table

IP Address	Open Ports	Common Services	Status
192.168.31.1	53,80, 443, 7443, 8080, 8443	Domain, HTTP, HTTPS, Oracleas-HTTPS, HTTP-proxy, HTTPS-alt	Online
192.168.31.37	135, 139, 445, 2869, 3306	MSRPC, NetBIOS-SSN, Microsoft-ds, ICSLAP, MySQL	Online
192.168.31.38	787, 8293	QSC, SOPHOS	Online
192.168.31.209	Not visible.	Not scanned.	Online

The Command scanned 4 Hosts and their details in 291.58 seconds.

Chapter 4. Device Identification & Host Profiling

4.1 Purpose of Host Identification

After identifying active hosts and their open ports using the **SYN scan**, the next step is to **profile each device** to better understand its:

- **Type** (e.g., router, PC, server, mobile, IoT)
- **Services** it exposes (via open TCP ports)
- **Potential role** within the network environment

This step is crucial for:

- Establishing a **network asset inventory**
- Detecting **unauthorized** or **unexpected** devices or services
- Planning **further scans**, such as version detection or vulnerability assessment
- Enforcing **network security policies** based on device roles

SYN scan results go beyond just finding active devices — they help classify endpoints by observing which ports they expose and what services they potentially host.

4.2 Identification Criteria

Each discovered host was analysed based on the following:

4.2.1 Open TCP Ports & Service Patterns

Common service-port associations help in recognizing device types. For example:

- Port 80/443/8080/8443: Indicates HTTP/HTTPS web interface (often routers or admin consoles)
- Port 53: DNS service, typically used by routers or DNS servers
- Port 135/139/445: Common on Windows systems for file sharing and RPC
- Port 3306: MySQL database, indicating development or service-oriented systems

4.2.2 Port Fingerprinting and OS Clues

Although version detection was not enabled (-sV or -O), the combination of open ports gives strong hints:

- Devices with 80, 443, 7443, 8080, 8443 and 53 suggest a router or network gateway
- Ports like 135, 139, 445, and 2869 imply a Windows-based workstation
- Filtered or stealthy ports (filtered) typically appear in mobile or IoT devices

4.2.3 Latency & Response Behaviour

- Devices with low latency responses are often stable systems such as routers, laptops, or servers
- Higher or inconsistent latencies indicate mobile phones or IoT devices

4.2.4 Internal IP Assignments

- 192.168.31.1 is typically reserved for default gateways or router interfaces
- Other IPs like 192.168.31.38 or 192.168.31.37 are usually assigned dynamically via DHCP

4.3 Device Profiles

IP Address	Open Ports	Likely Device Type	Remarks
192.168.31.1	53, 80, 443, 7443, 8080, 8443	Router / Gateway	Web admin interfaces and DNS exposed
192.168.31.37	135, 139, 445, 2869, 3306	Windows Laptop	SMB, RPC, and MySQL services detected
192.168.31.38	787, 8193 (filtered)	Android Tablet (IoT)	Likely mobile or tablet with filtered ports
192.168.31.209	All ports closed	Mobile Device	No active services, likely smartphone

These profiles were derived using standard port-to-service inference techniques and analysis of the Nmap SYN scan results.

4.4 Importance of Device Profiling

Understanding device roles via SYN scan enhances:

- Security segmentation — for instance, isolating IoT or mobile devices from core systems
- Host risk classification — based on services exposed
- Firewall rule planning — targeted rules per device type
- Detection of misconfigurations or rogue devices, such as:
    - A personal laptop running a MySQL database unintentionally
    - A router exposing multiple HTTPS interfaces unnecessarily

In summary, device profiling from SYN scans uncovers not just online presence, but operational roles and potential security implications, vital for network hardening and policy enforcement.

Chapter 5. Security Risk Analysis & Saving the Scan Report

5.1 Security Risk Analysis

The SYN scan output provided detailed visibility into active TCP services running on devices within the local subnet. Although no version detection was performed, the exposure of specific ports still enables a meaningful security evaluation. By identifying open ports and host roles, it becomes possible to uncover potential vulnerabilities, misconfigurations, and gaps in network segmentation.

5.1.1 Key Observations from SYN Scan

Open Ports Exposing Critical Services

- The host 192.168.31.1 (likely the router) exposes multiple web-facing ports (80, 443, 7443, 8080, 8443), potentially increasing the surface for attacks targeting router admin panels or misconfigured services.
- Host 192.168.31.37 exposes 445 (SMB), 139 (NetBIOS), and 3306 (MySQL) — services that are commonly targeted in lateral movement or database enumeration attacks.

Unauthorized or Unnecessary Services

- May indicate a development environment or a misconfigured installation..
- IoT or mobile devices like 192.168.31.38 showed filtered ports (787, 8193), indicating either firewall blocking or potentially suspicious remote services.

Firewall / Access Control Gaps

- Multiple devices responded to SYN probes, suggesting either no host-based firewalls or permissive ACLs.
- The flat structure of the subnet (same IP range) without segmentation implies higher lateral movement risk.

Invisibility of Some Devices

- Host 192.168.31.209 responded but revealed no open ports, likely due to strict firewall rules or mobile OS network behaviour — a positive security posture if intentional.

5.1.2 Recommendations Based on SYN Scan

Area	Recommendation
Open Ports on Workstations	Disable unnecessary services (e.g., SMB, MySQL)

Router/Web Interfaces	Harden router interfaces and restrict access via firewall rules
Network Segmentation	Isolate IoT, mobile, and guest devices from critical infrastructure
Port Monitoring	Regularly scan and baseline open ports for all devices
Access Control Lists	Implement stricter rules to limit access to internal services
Patch Management	Keep services like SMB, MySQL, and HTTP up to date
Security Tooling	Deploy host-based firewalls, and consider using IDS tools

---

5.2 Saving the Scan Report

Documenting scan results is a best practice for future audits, comparisons, and investigations.

5.2.1 Save SYN Scan Output in Text Format

To save the scan result for reference:

bash

CopyEdit

nmap -sS 192.168.31.0/24 -oN syn_scan_results.txt

- -sS: Performs a TCP SYN scan.
- -oN: Saves output in a human-readable text format.

This command will store all live hosts and their detected open TCP ports in the file syn_scan_results.txt.

Chapter 6. Outcome & Conclusion

6.1 Outcome

The task of performing a TCP SYN scan using **Nmap 7.95** on a Windows system was successfully completed. The scan explored 256 IPs within the subnet 192.168.31.0/24 and identified four active hosts.

Key outcomes of the scan:

- Identified **active devices** responding to TCP SYN probes.
- Detected **open TCP ports** and inferred likely services on hosts such as:
    - Web interfaces on router (192.168.31.1)
    - SMB and MySQL on Windows laptop (192.168.31.37)
- **Classified host types** (router, laptop, mobile, IoT) based on port patterns.
- Gained hands-on experience with **stealth scanning** using half-open TCP handshakes.
- Understood how **open ports expose service surfaces**, increasing risk if unmonitored.
- Saved the scan output for future analysis and reporting.

This scan provided **deeper network visibility** than ARP scans, moving beyond device detection to understanding device behaviour and potential vulnerabilities.

6.2 Conclusion

This project delivered valuable practical experience in **active port scanning using TCP SYN probes**. It bridged theoretical learning with real-world network reconnaissance.

Key takeaways:

- SYN scans help identify **services and roles** of hosts without fully connecting to them.
- Network services like HTTP, SMB, or MySQL — if exposed unintentionally — can become **entry points for attackers**.
- Proper segmentation and firewall policies are essential to **minimize exposure and mitigate risks**.

Compared to ARP scans, SYN scans offer **deeper insight into host activity**, making them essential for vulnerability assessments and network security audits.

6.3 Final Takeaway

This SYN scan–based exercise not only enhanced my technical skills in **network mapping and service enumeration**, but also strengthened my understanding of **risk analysis and security policy planning**.

The experience lays a solid foundation for future cybersecurity tasks such as:

- Designing **port-based firewall rules**
- Conducting **version detection** and **vulnerability scanning** using advanced Nmap options (-sV, --script)
- Performing **OS fingerprinting** and **penetration testing**

This marks a key step in my journey toward becoming a **competent cybersecurity analyst**, capable of interpreting network behaviour and securing enterprise systems.

Appendix A: GitHub Sharing Disclaimer

This project report is shared publicly on GitHub for academic reference purposes only. All scanned IP addresses are from a private local network and were part of a controlled environment used for cybersecurity learning.

Sensitive data such as device MAC addresses and hostnames have been masked to maintain privacy. No external networks or unauthorized systems were scanned during this task.

The tools used (e.g., Nmap) are intended for ethical use only. Please do not replicate any scans or commands on networks without explicit permission.

Unauthorized use of this report, or using the techniques described here in for illegal purposes, is strictly prohibited.