Task 1 – Nmap Scanning and Service Enumeration Report

Submitted by:
Shashanka U N
SOC Intern – Cyber Security

Submitted to:
CyArt Tech

Date:
19th August 2025

Introduction:

With the increasing number of cyber threats targeting systems and applications, understanding how attackers gather information has become essential. One of the first steps in a cyberattack is reconnaissance, where attackers scan networks and systems to identify open ports, services, and potential vulnerabilities.

This task focuses on using **Nmap**, a powerful and widely used network scanning tool, to enumerate the open ports and running services of a given target system. By performing such scans, we can simulate the perspective of an attacker, identify weaknesses, and recommend security measures to mitigate risks.

The objective of this task is to:

- Perform a network scan using Nmap.
- Identify active services and their versions.
- Analyze potential security risks associated with these services.
- Document findings in a structured report with supporting diagrams.

Methodology

The following methodology was adopted to complete Task:

1. Environment Setup

- The internship-provided virtual machine (AttackBox/VM) was used as the scanning system.
- The target IP/host was identified and documented for scanning.

2. Tool Used

- **Nmap (Network Mapper):** An open-source tool for network discovery and security auditing.
- Version: Nmap 7.94 (latest stable release at the time of testing).

3. Scanning Approach

- A **basic host discovery** scan was performed to verify if the target was live.
- A **SYN Scan (-sS)** was used for fast detection of open ports.
- A **Service and Version Detection (-sV)** scan was performed to identify services running on the discovered ports.

- An **Aggressive Scan (-A)** was used in some cases to gather additional information like OS detection and traceroute.

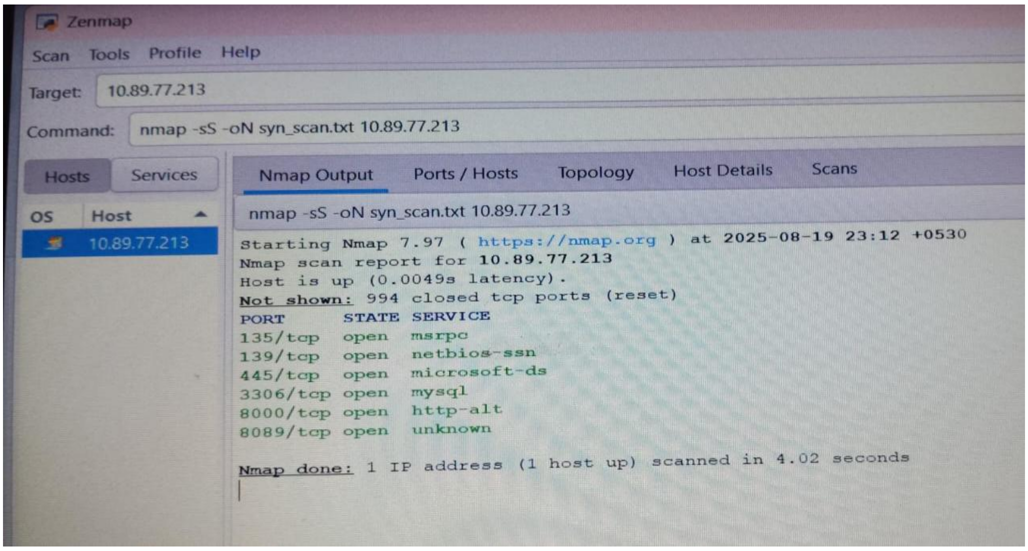
4. Steps Followed

1. Verified connectivity with a simple **ping test**.
2. Conducted an initial **Nmap scan** to identify open ports.
3. Performed **service enumeration** to determine versions and applications.
4. Documented findings with screenshots of the commands and results.
5. Designed a **network diagram** to visualize open ports and services.

Scan Results & Observations:

Target IP (Host): 10.89.77.213

1. **SYN Scan (-sS):**
   Command used: nmap -sS -oN syn_scan.txt 10.89.77.213
   Results:



Target: 10.89.77.213

Command: nmap -sS -oN syn_scan.txt 10.89.77.213

```
nmap -sS -oN syn_scan.txt 10.89.77.213
Starting Nmap 7.97 ( https://nmap.org ) at 2025-08-19 23:12 +0530
Nmap scan report for 10.89.77.213
Host is up (0.0049s 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
3306/tcp open  mysql
8000/tcp open  http-alt
8089/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.02 seconds
```

Port	State	Service
135/tcp	Open	Marpo
139/tcp	Open	Netdios-ssn
445/tcp	Open	Microsoft-ds
3306/tcp	Open	Mysql
8000/tcp	Open	Http-alt
8089/tcp	Open	unknown

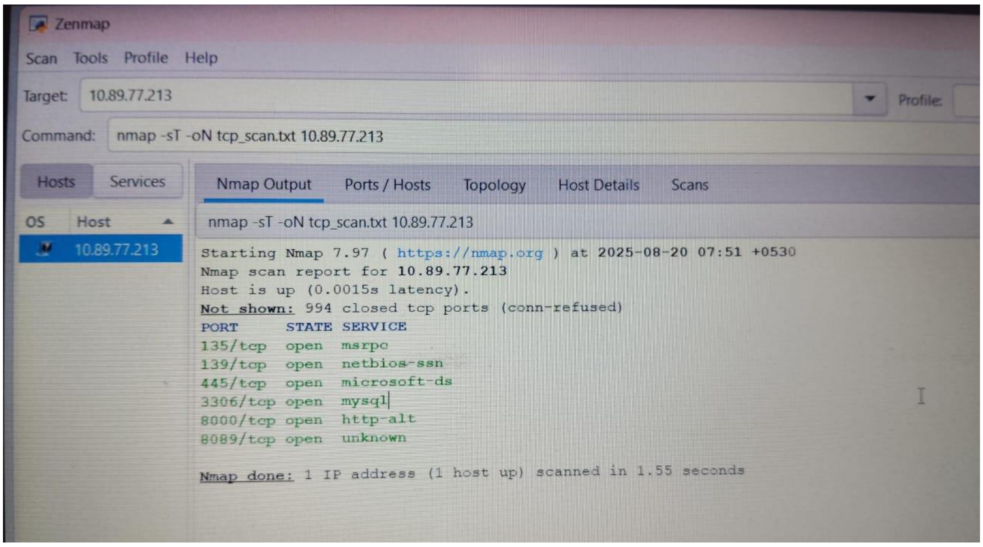
Analysis:

- The presence of SMB ports (139, 445) indicates potential for SMB-related vulnerabilities.
- MySQL (3306) being open may expose database services, requiring authentication checks.
- HTTP ports (8000, 8089) could be hosting web applications that should be tested for common web vulnerabilities.
- The unknown service on 8089 requires banner grabbing or version detection to identify the application.

2. **TCP Connect Scan (-sT):**

Command used: nmap -sT -oN tcp_scan.txt 10.89.77.213

Results:



Target: 10.89.77.213

Command: nmap -sT -oN tcp_scan.txt 10.89.77.213

10.89.77.213

```
nmap -sT -oN tcp_scan.txt 10.89.77.213
Starting Nmap 7.97 ( https://nmap.org ) at 2025-08-20 07:51 +0530
Nmap scan report for 10.89.77.213
Host is up (0.0015s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp open  mysql
8000/tcp open  http-alt
8089/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.55 seconds
```

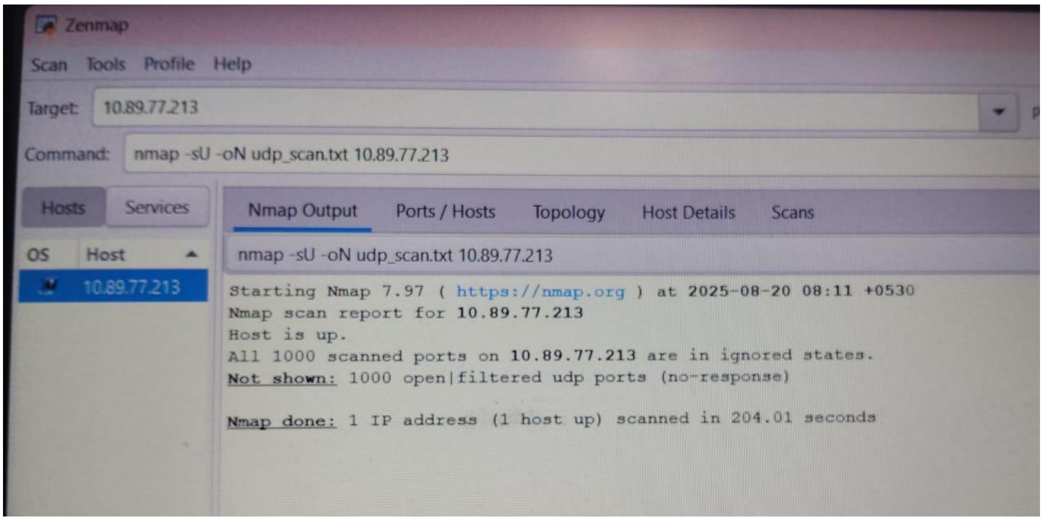
Port	State	Service
135/tcp	Open	Marpo
139/tcp	Open	Netdios-ssn
445/tcp	Open	Microsoft-ds
3306/tcp	Open	Mysql
8000/tcp	Open	Http-alt
8089/tcp	Open	unknown

Analysis:

- The presence of SMB ports (139, 445) indicates potential for SMB-related vulnerabilities.
- MySQL (3306) being open may expose database services, requiring authentication checks.

- HTTP ports (8000, 8089) could be hosting web applications that should be tested for common web vulnerabilities.
- The unknown service on 8089 requires banner grabbing or version detection to identify the application.

3. **UDP Scan (-sU):**
   Command used: nmap -sT -oN tcp_scan.txt 10.89.77.213
   Results:



Target: 10.89.77.213

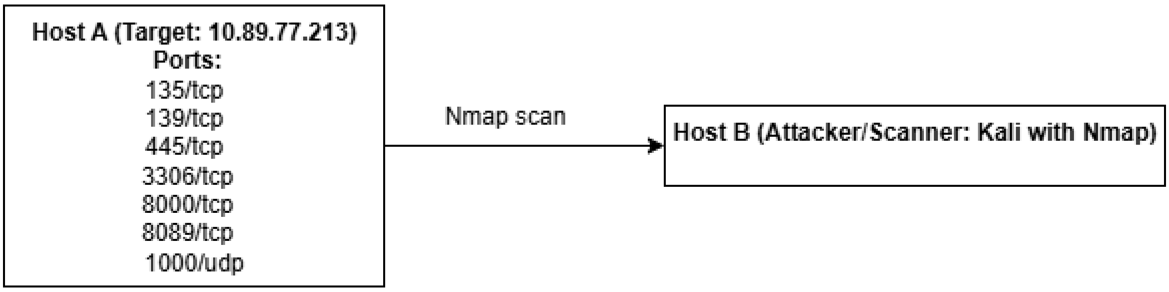
Command: nmap -sU -oN udp_scan.txt 10.89.77.213

```
nmap -sU -oN udp_scan.txt 10.89.77.213

Starting Nmap 7.97 ( https://nmap.org ) at 2025-08-20 08:11 +0530
Nmap scan report for 10.89.77.213
Host is up.
All 1000 scanned ports on 10.89.77.213 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 204.01 seconds
```

Analysis:

- Host is **up**.
- **All 1000 UDP ports** are shown as open|filtered (Nmap couldn’t confirm if they’re open, because UDP doesn’t reply unless there’s a service running).
- No specific service was identified.

Network Diagram for Above results:


Host A (Target: 10.89.77.213)
Ports:
135/tcp
139/tcp
445/tcp
3306/tcp
8000/tcp
8089/tcp
1000/udp
Nmap scan
Host B (Attacker/Scanner: Kali with Nmap)

135,139,445,3306,8000,8089 = TCP ports
1000 = UDP ports
Arrow shows scanning direction

Two Researched Services:

1. SMB / Microsoft Services (Ports 139, 445)

- **Ports:** 139 (NetBIOS-SSN), 445 (Microsoft-DS)
- **Purpose:**
  - Provide file and printer sharing in Windows networks.
  - Enable remote access to shared resources and services.
- **Common Vulnerabilities:**
  - **SMBv1**: Vulnerable to **WannaCry**/EternalBlue attacks.
  - **Unauthorized access**: Weak or misconfigured shares can allow attackers to read/write files.
- **Security Notes:**
  - Ensure SMBv1 is disabled on modern systems.
  - Use strong passwords and proper access controls.

2. MySQL Database (Port 3306)

- **Port:** 3306 (MySQL)
- **Purpose:**
  - Provides database services for storing and managing structured data.
- **Common Vulnerabilities:**
  - **Weak/default credentials**: Can allow attackers to log in and dump or modify databases.
  - **SQL Injection**: If applications accessing MySQL are vulnerable, attackers can manipulate data.
- **Security Notes:**
  - Always use strong passwords for database users.
  - Restrict remote access and enable firewall rules.