

BASIC NETWORK SCANNING REPORT USING NMAP

Target IP: 192.168.29.217

Tool Used: Nmap

Objective

The goal of this task was to perform a basic and an intense network scan using Nmap/Zenmap to identify open ports, running services, OS details, and system behaviour on the target machine 192.168.29.217. This helps understand the system's exposure and potential attack surface.

Scan Types Performed

1. Basic Scan

- Command used: nmap 192.168.29.217
- This scan quickly identified which ports on the target machine are open.
- This scan is quick and useful for getting an overview of active ports.
- **Results:** Open ports found were 135/tcp, 139/tcp, and 445/tcp.
 - **Port 135 (msrpc):** Microsoft RPC (Remote Procedure Call) – used for communication between software programs.
 - **Port 139 (netbios-ssn):** NetBIOS Session Service – used for file and printer sharing over Windows networks.
 - **Port 445 (microsoft-ds):** Microsoft Directory Services – used for SMB (Server Message Block) file sharing.

2. Intense Scan

- Command used: nmap -T4 -A -v 192.168.29.217
- This scan is more detailed and performs OS detection, version detection, script scanning, and traceroute.
- **Results:** Confirmed the same open ports: 135/tcp, 139/tcp, 445/tcp.
 - 135/tcp → Microsoft Windows RPC
 - 139/tcp → Microsoft Windows NetBIOS-SSN
 - 445/tcp → Microsoft Windows SMB
- OS Detection: The target machine is running a Windows OS.

- Uptime guess: The system has been up for approximately 12 days.
- Network distance: Local network (0 hops).
- This scan provides detailed information about the system, helping in security assessment.

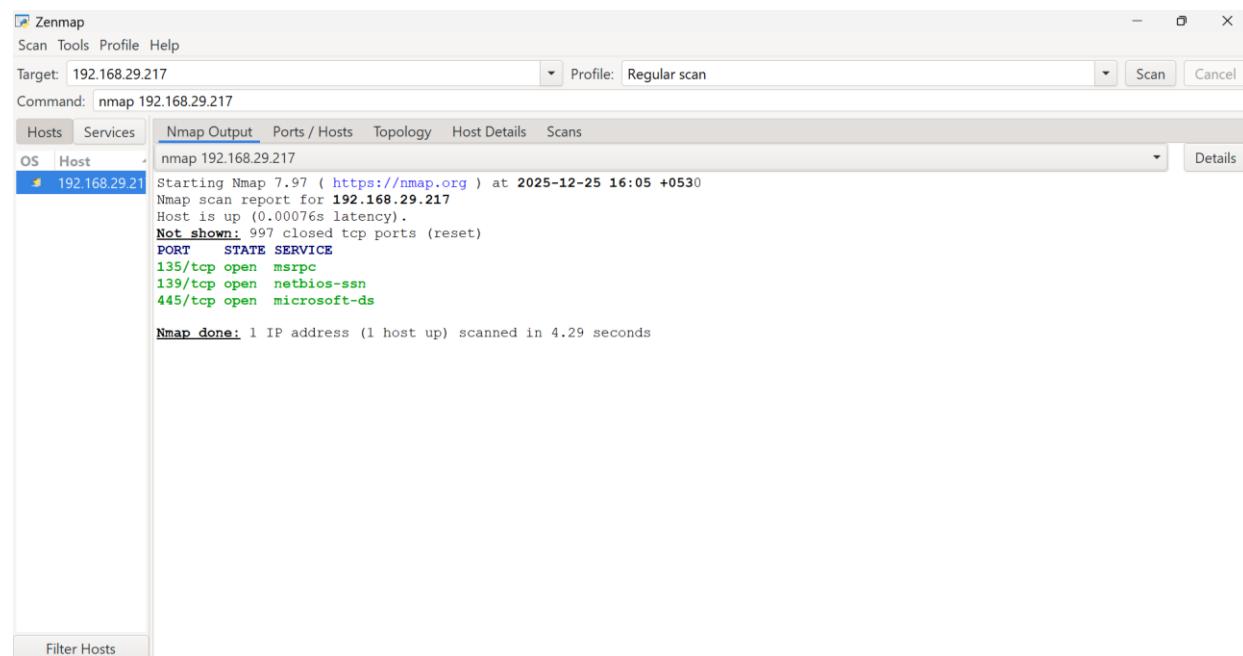
Findings

1. Three open ports identified: 135 (RPC), 139 (NetBIOS), 445 (SMB).
2. System is running essential Windows network services (RPC, NetBIOS, SMB).
3. Target OS detected as Windows with noticeable uptime.

Significance

1. SMB/RPC ports are commonly targeted for remote exploitation.
2. NetBIOS may reveal system information useful to attackers.
3. SMB signing is not enforced, which increases the risk of tampering attacks.

Attachments



The screenshot shows the Zenmap interface with the following details:

- Target:** 192.168.29.217
- Profile:** Regular scan
- Command:** nmap 192.168.29.217
- Hosts:** Host 192.168.29.217
- Services:** Nmap Output tab selected, showing the following output:

```

Starting Nmap 7.97 ( https://nmap.org ) at 2025-12-25 16:05 +0530
Nmap scan report for 192.168.29.217
Host is up (0.00076s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
Nmap done: 1 IP address (1 host up) scanned in 4.29 seconds

```

Fig 1: Screenshot of Basic Scan result

The screenshot shows the Zenmap interface with the following details:

- Target:** 192.168.29.217
- Profile:** Intense scan
- Command:** nmap -T4 -A -v 192.168.29.217
- Hosts:** 192.168.29.217
- Services:** Nmap Output (selected), Ports / Hosts, Topology, Host Details, Scans
- OS:** Host
- Details:** Shows the Nmap command and its output, including the results of the SYN Stealth Scan, service detection, and OS detection.

```
Starting Nmap 7.97 ( https://nmap.org ) at 2025-12-25 16:06 +0530
Nmap wishes you a merry Christmas! Specify -sX for Xmas Scan (https://nmap.org/book/man-port-scanning-techniques.html).
NSE: Loaded 158 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:06
Completed NSE at 16:06, 0.00s elapsed
Initiating NSE at 16:06
Completed NSE at 16:06, 0.00s elapsed
Initiating NSE at 16:06
Completed NSE at 16:06, 0.00s elapsed
Initiating NSE at 16:06
Completed NSE at 16:06, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 16:06
Completed Parallel DNS resolution of 1 host. at 16:06, 0.51s elapsed
Initiating SYN Stealth Scan at 16:06
Scanning 192.168.29.217 [1000 ports]
Discovered open port 445/tcp on 192.168.29.217
Discovered open port 135/tcp on 192.168.29.217
Discovered open port 139/tcp on 192.168.29.217
Completed SYN Stealth Scan at 16:06, 0.13s elapsed (1000 total ports)
Initiating Service scan at 16:06
Scanning 3 services on 192.168.29.217
Completed Service scan at 16:06, 6.12s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 192.168.29.217
Retrying OS detection (try #2) against 192.168.29.217
Retrying OS detection (try #3) against 192.168.29.217
Retrying OS detection (try #4) against 192.168.29.217
Retrying OS detection (try #5) against 192.168.29.217
NSE: Script scanning 192.168.29.217.
Initiating NSE at 16:06
Completed NSE at 16:06, 14.25s elapsed
```

Fig 2: Screenshot of Intense Scan result

Conclusion

The Nmap scans provided clear visibility into the target system's open ports and running services. Both scans confirmed the presence of key Windows network services, making the system potentially vulnerable if not properly secured. These results help highlight security gaps and guide future mitigation steps.