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

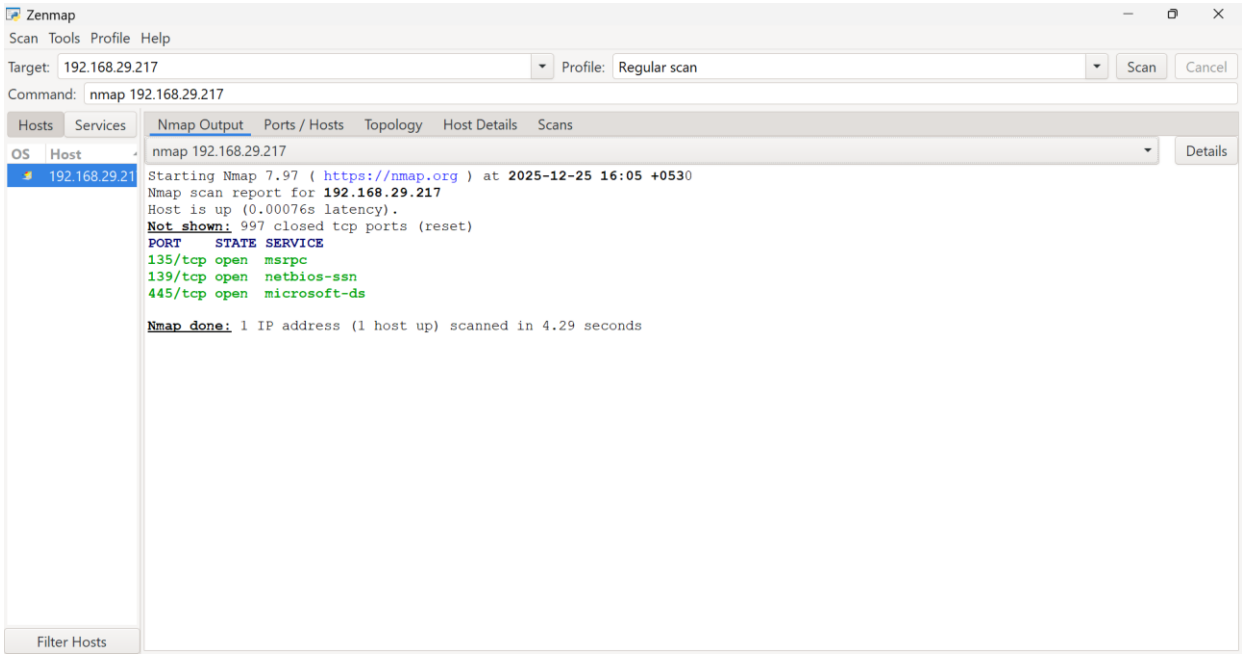

Fig 1: Screenshot of Basic Scan result

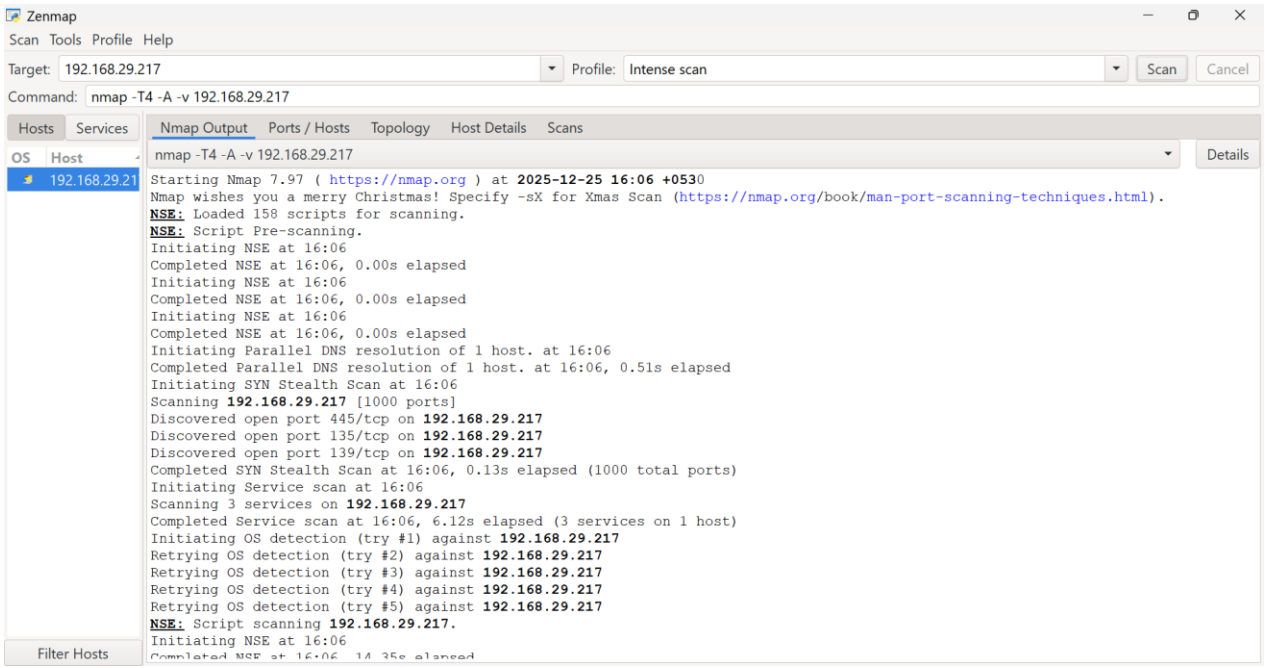

Fig 2: Screenshot of Intense Scan result

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.