🛡️ Network Reconnaissance Report using Nmap

1. Objective

To perform network reconnaissance and identify open ports on a target system using Nmap, followed by an analysis of possible vulnerabilities and mitigation strategies for the discovered services.

2. Tool Used

Tool Name: Nmap (Network Mapper)

About the Tool:
Nmap is a powerful open-source network scanning tool used to discover hosts and services on a network. It supports multiple scan types, OS detection, version detection, firewall evasion, and scriptable interaction with targets using the Nmap Scripting Engine (NSE).

3. Commands Used

Scan Type	Command Used	Purpose
Basic TCP Scan	nmap <target-ip>	To detect live hosts and open ports
Stealth Scan (SYN)	nmap -sS <target-ip>	Less likely to be logged by firewall
Full Connect Scan	nmap -sT <target-ip>	Attempts full TCP connections
Version Detection	nmap -sV <target-ip>	Identifies service versions on open ports
Firewall Bypass	nmap -Pn <target-ip>	Skips host discovery (ICMP blocking bypass)
Aggressive Scan	nmap -A <target-ip>	Combines OS, version, script, traceroute
OS Detection	nmap -O <target-ip>	Tries to identify operating system

4. Scanning Results

Open Ports Identified:

Port 23 (Telnet) – Unencrypted remote login service

Port 139 (NetBIOS-SSN) – File/printer sharing (SMB-related)

Port 445 (Microsoft-DS) – SMB over TCP, Windows file sharing

5. Methodology

1. Host Discovery: ICMP and TCP probes to find live systems

2. Port Scanning: TCP SYN scan to discover open ports

3. Service Enumeration: Used version detection with -sV

4. OS Detection: Used -O flag for fingerprinting

5. Firewall Evasion: Used -Pn to bypass ICMP ping blocks

6. Manual Validation: Verified Telnet and SMB access manually

6. Learning Objectives

Gain hands-on experience with Nmap scanning

Identify critical network services running on a host

Understand risks associated with exposed ports

Learn basic defensive techniques to secure open services.

7. Exploitation & Mitigation

Port	Service	Exploitation Risk	Mitigation Strategy
23	Telnet	Unencrypted login, brute-force attacks	Disable Telnet; Use SSH with strong encryption
139	NetBIOS	Info disclosure, SMB exploits, LLMNR poisoning	Disable NetBIOS if unused; Restrict via firewall
445	SMB	EternalBlue, SMBGhost, privilege escalation	Apply Windows patches; Disable SMBv1; restrict access

8. Conclusion

The Nmap scan revealed potentially vulnerable services running on ports 23 (Telnet), 139 (NetBIOS), and 445 (SMB). These ports are often targeted in real-world attacks due to their support for remote access and file sharing. Disabling unused services and patching the system significantly reduces the attack surface and helps secure the network.