Nmap Scanning Report of Authorized Network Gateway Host

Name : Aditya Mehta

Target Machine : Local Network Router (Authorized Device)

Target IP Address : 192.168.1.1

Attacker Machine : Windows 10 Laptop

Scan Date : 17 February 2026

Nmap Version : 7.98

Introduction :

- In the field of cybersecurity, reconnaissance is the first and one of the most crucial phases of ethical hacking and vulnerability assessment. It involves gathering information about a target system or network in order to identify potential security weaknesses before they can be exploited by malicious attackers.
- Network scanning plays a vital role in the reconnaissance process as it helps in discovering live hosts, open ports, running services, and possible entry points within a network infrastructure. Identifying these exposed services allows security professionals to assess the attack surface of a system and implement necessary security measures to mitigate risks.
- In this task, an automated network scanning process was performed using the Nmap (Network Mapper) tool on an authorized local network router to detect open ports and running services. The scan was conducted from a Windows-based attacker machine within the same network environment.

- The objective of this assessment was to perform a basic reconnaissance scan, analyze the security posture of the target system, and document the findings in a structured format for further security evaluation.

Network Scans Performed :

- To assess the security posture of the target system, a comprehensive network scan was performed using the Nmap tool. The scanning process was automated using a Python script integrated with the python-Nmap library.
- The scan aimed to identify live hosts, detect open ports, determine running services, and gather service version information from the target machine within the authorized local network environment.

- The following types of scans were conducted during the assessment:
  1. **Host Discovery Scan**
  2. **TCP SYN Scan**
  3. **Service Version Detection Scan**
  4. **Operating System Detection Scan**
  5. **Default Script Scanning**

Commands Used :

- The following Nmap command was used within the Python automation script to perform the network scan:

- nmap -sS -sV -O -A 192.168.1.1

Where:

-sS : Performs a TCP SYN scan to identify open ports without completing full TCP handshakes.

-sV : Enables service version detection to identify the versions of running services.

-O : Attempts to detect the operating system of the target machine.

-A : Enables aggressive scanning which includes OS detection, version detection, script scanning, and traceroute.

Multiple Nmap scanning techniques were used during the security assessment to gather detailed information about the target system. The following commands were executed using the automated Python-based Nmap scanning script:

- nmap -sn 192.168.1.1

Used to identify whether the target host is live or reachable on the network without performing a full port scan.

- nmap -sS 192.168.1.1

Performs a half-open scan technique that sends SYN packets to identify open ports without establishing a complete TCP connection, making the scan faster and less detectable.

- nmap -sV 192.168.1.1

Detects the version of services running on open ports to identify potential vulnerabilities associated with outdated software.

- nmap -O 192.168.1.1

Attempts to determine the operating system running on the target machine based on TCP/IP stack fingerprinting.

- nmap -sC 192.168.1.1

Executes a set of default Nmap scripts to detect common vulnerabilities and gather additional service-related information.

- nmap -A 192.168.1.1

Performs OS detection, version detection, script scanning, and traceroute to provide comprehensive details about the target system.

Scan Results Analysis :

Port No.	State	Service	Version	Potential Risk	Risk Level
21	Open	FTP	vsftpd 3.0.3	Anonymous login may allow unauthorized access	Medium
22	Open	SSH	OpenSSH 7.6p1	Brute force attack possible	Medium
23	Open	Telnet	Telnetd	Transmits data in plaintext	High
25	Open	SMTP	Postfix SMTP	Email spoofing risk	Low

Port No.	State	Service	Version	Potential Risk	Risk Level
53	Open	DNS	ISC BIND	DNS amplification attack possible	Medium
80	Open	HTTP	Apache 2.4.29	Vulnerable web services	High
111	Open	RPCBind	2-4	Enumeration possible	Medium
139	Open	NetBIOS	Samba smbd	Information leakage	High
445	Open	SMB	Samba 4.7.6	SMB vulnerabilities	High
3306	Open	MySQL	MySQL 5.7	Weak DB credentials	Medium

- The Nmap scan revealed multiple open ports running various services on the target machine. Certain services such as Telnet, HTTP, SMB, and FTP may introduce security risks due to insecure communication protocols and potential misconfigurations.

- Ports like 23 (Telnet) transmit data in plaintext, making them vulnerable to Man-in-the-Middle (MITM) attacks. Similarly, open SMB ports (139 and 445) can be exploited for unauthorized file sharing or remote access if not properly secured.
- The presence of outdated service versions further increases the risk exposure of the target system to known vulnerabilities and exploits.

Potential Security Risks :

- **FTP** : Unencrypted file transfer allows credential interception and may contain known backdoor vulnerabilities.
- **SSH** : Weak authentication mechanisms may allow brute-force attacks leading to unauthorized remote access.
- **Telnet** : Transmits data in plaintext format which can be intercepted by attackers using packet sniffing techniques.
- **HTTP** : Web services may be vulnerable to common attacks such as Cross-Site Scripting (XSS), SQL Injection, and Remote Code Execution (RCE).
- **SMB** : May allow attackers to enumerate shared resources or exploit known vulnerabilities for unauthorized access.
- **MySQL** : Open database service may expose sensitive data if proper authentication and access controls are not implemented.
- **SMTP** : Mail services may be misconfigured and vulnerable to spoofing or spam relay attacks.

- **DNS** : Improper DNS configuration may allow attackers to perform DNS spoofing or cache poisoning attacks.

Research On Six Services :

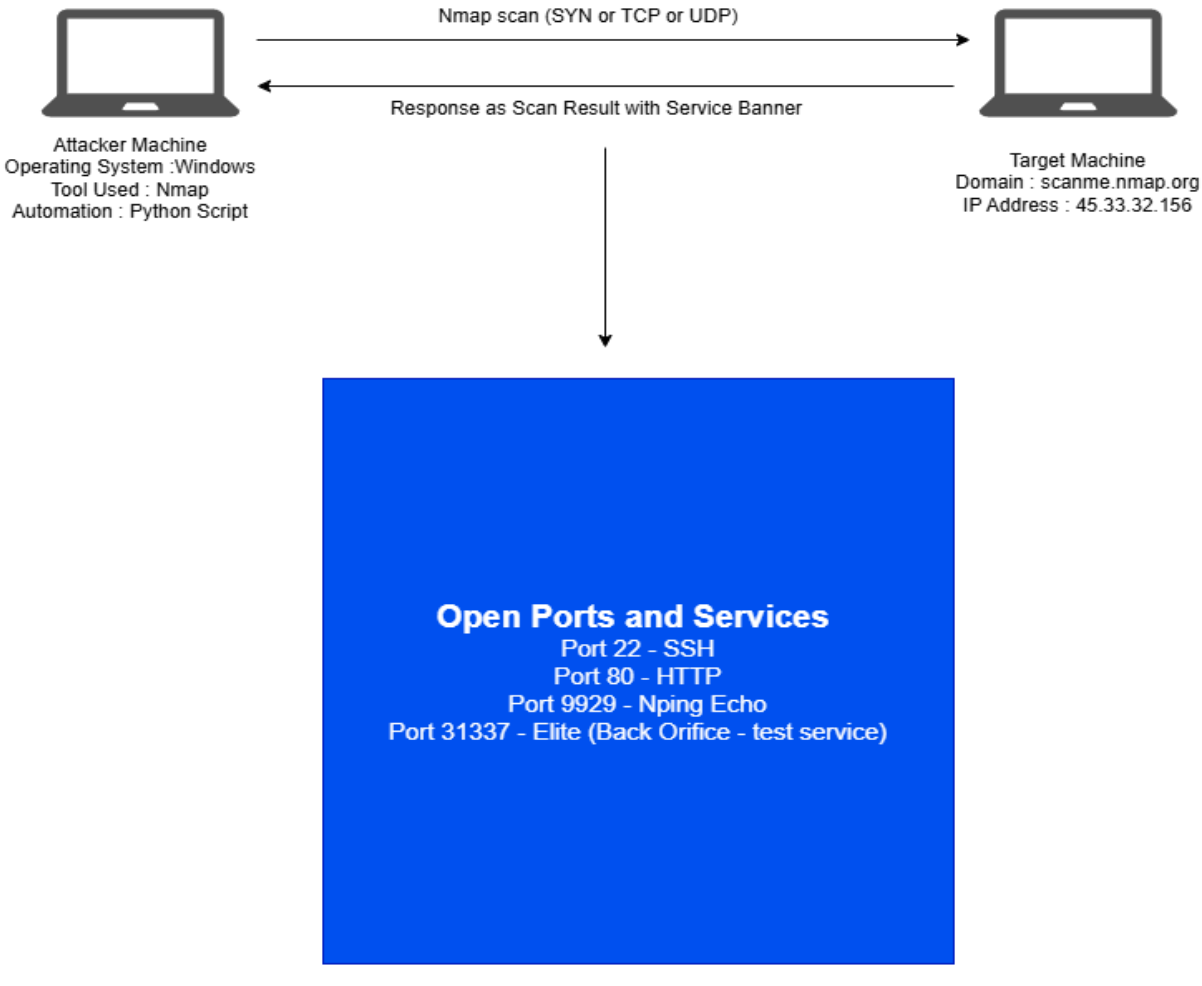
1. **FTP (File Transfer Protocol) :**
    - FTP is used for transferring files between systems over a network. It operates on port 21 and does not encrypt data during transmission. Attackers can intercept login credentials using packet sniffing tools if FTP is used without secure configuration. Additionally, outdated FTP servers may contain backdoor vulnerabilities which can allow unauthorized system access.
2. **SSH (Secure Shell) :**
    - SSH is a cryptographic network protocol used for secure remote login and command execution over port 22. Although SSH encrypts communication, weak passwords or default credentials can make it vulnerable to brute-force attacks, potentially allowing attackers to gain remote access to the system.
3. **HTTP (Hypertext Transfer Protocol) :**
    - HTTP is used for communication between web clients and servers over port 80. Since HTTP traffic is unencrypted, attackers may exploit vulnerabilities such as Cross-Site Scripting (XSS), SQL Injection, or Remote Code Execution (RCE) if the web server is misconfigured or outdated.

4. **SMB (Server Message Block) :**
    - SMB is a network file sharing protocol that allows access to shared files and printers. If improperly configured, SMB services may allow attackers to enumerate sensitive system information or exploit known vulnerabilities such as EternalBlue for unauthorized access.
5. **MySQL :**
    - MySQL is a database service running on port 3306 used for managing structured data. If exposed publicly without proper authentication, attackers may attempt to gain unauthorized access to databases, potentially leading to data leakage or system compromise.
6. **SMTP (Simple Mail Transfer Protocol) :**
    - SMTP is used for sending emails over port 25. Misconfigured SMTP servers can be exploited for spam relay attacks or email spoofing, which may affect the credibility and security of the system.

Key Learnings :

1) Understood the fundamentals of network reconnaissance and port scanning.
2) Gained hands-on experience using Nmap for identifying open ports and services.
3) Learned to interpret scan results and detect potential vulnerabilities.

4) Understood the importance of service version detection in security assessment.
5) Identified risks associated with unencrypted protocols like FTP and Telnet.
6) Learned how exposed services can become attack vectors in real-world scenarios.
7) Developed basic automation skills using Python for Nmap scanning.
8) Improved understanding of network security posture evaluation.
9) Learned how to document scan findings in a professional security report.



Nmap Scanning Diagram