Name : Srinivas Atta

Cyber Security Internship Task 1:

Nmap Scan Report Introduction This report details the results of a network scan performed using Nmap 7.97 as part of the Cyber Security Internship Task 1. The scan was conducted on August 4, 2025, at 21:18:14, targeting the network range 192.168.0.0/24 using a TCP SYN scan (-sS). The scan results were saved to a file named full\tcp\scan.txt. This document provides a comprehensive analysis of the scan results, including host discovery, port states, services identified, and recommendations for securing the network. The report is structured to ensure clarity and completeness, adhering to the guidelines provided in the internship task description. Task Overview The internship task required performing a network scan and submitting the results via a GitHub repository. The scan was executed with the following command: nmap -sS -oN full\tcp\scan.txt 192.168.0.0/24

\-sS: TCP SYN scan, a stealthy scan that sends SYN packets to determine port states without completing TCP handshakes. -oN full\tcp\scan.txt: Outputs results to a file in normal format. 192.168.0.0/24: Targets the IP range 192.168.0.0 to 192.168.0.255 (256 addresses).

The scan took approximately 805.54 seconds (13.43 minutes) to complete, identifying 6 active hosts out of the 256 scanned IP addresses. Scan Results Summary

Scan Start Time: August 4, 2025, 21:18:14 Scan End Time: August 4, 2025, 21:31:40 Total IPs Scanned: 256 Hosts Up: 6 Scan Type: TCP SYN scan Output File: full\tcp\scan.txt

The scan identified six active hosts with varying port states and services. Below is a detailed breakdown of each host's scan results. Host Details

1. **Host: 192.168.0.1**

Status: Up Latency: 0.0049 seconds MAC Address: 3C:6A:D2:6F:8D:F3 (TP-Link Systems) Open Ports: 22/tcp: Open (SSH) Service: Secure Shell (SSH), typically used for secure remote access. Implications: SSH is a common target for brute-force attacks. Ensure strong passwords or key-based authentication.

23/tcp: Open (Telnet) Service: Telnet, an insecure remote access protocol. Implications: Telnet transmits data in plaintext, making it vulnerable to interception. Consider disabling Telnet and using SSH instead.

53/tcp: Open (Domain) Service: DNS (Domain Name System), used for name resolution. Implications: Exposed DNS services can be exploited for amplification attacks. Restrict access to trusted clients.

80/tcp: Open (HTTP) Service: Web server, likely hosting a web interface. Implications: Web servers are common attack vectors. Ensure the server is patched and configured securely.

1900/tcp: Open (UPnP) Service: Universal Plug and Play, used for device discovery and configuration. Implications: UPnP can be exploited for network access. Disable if not required or restrict to local network.

Closed Ports: 995 ports closed (reset) Analysis: This host appears to be a router or gateway (TP-Link Systems). The presence of Telnet and UPnP raises security concerns due to their known vulnerabilities. Immediate action is recommended to secure these services.

2**. Host: 192.168.0.3**

Status: Up Latency: 0.016 seconds MAC Address: E6:A8:32:A1:82:6B (Unknown) Open Ports: None Closed Ports: 1000 ports closed (reset) Analysis: No open ports were detected, suggesting this host may be firewalled or not running any accessible services. The unknown MAC address vendor indicates a potentially non-standard or consumer device. Further investigation is needed to identify its role on the network.

3. Host: 192.168.0.4

Status: Up Latency: 0.58 seconds MAC Address: 7E:D6:BF:03:99:45 (Unknown) Open Ports: 1213/tcp: Filtered (mpc-lifenet) Service: Unknown service associated with port 1213 (potentially MPC LifeNet). Implications: Filtered ports indicate a firewall or packet filtering. The service is unclear, requiring further investigation to determine its purpose.

Closed Ports: 999 ports closed (reset) Analysis: The high latency and filtered port suggest a device with active filtering, possibly a specialized or misconfigured system. The unknown MAC address vendor complicates identification.

4. Host: 192.168.0.6

Status: Up Latency: 0.037 seconds MAC Address: 4C:B0:4A:0E:21:21 (Intel Corporate) Open Ports: None Filtered Ports: 1000 ports filtered (no-response) Analysis: All scanned ports are filtered, indicating a strict firewall. The Intel Corporate MAC address suggests a corporate-grade device, possibly a workstation or server. Additional scans (e.g., UDP or specific port ranges) may reveal more information.

5. **Host: 192.168.0.9**

Status: Up Latency: 0.34 seconds MAC Address: 32:E4:46:EE:B0:3D (Unknown) Open Ports: None Closed Ports: 1000 ports closed (reset) Analysis: Similar to 192.168.0.3, this host has no open ports and an unknown MAC address vendor. It may be a consumer device or a system with minimal network exposure.

6. **Host: 192.168.0.17**

Status: Up Latency: 0.0000050 seconds (very low, likely local) Open Ports: 3306/tcp: Open (MySQL) Service: MySQL database server. Implications: Exposed MySQL servers are vulnerable to unauthorized access, especially if default credentials are used. Restrict access to specific IPs and enforce strong authentication.

Closed Ports: 999 ports closed (reset) Analysis: The extremely low latency suggests this is the scanning host or a closely connected device. The open MySQL port is a significant security risk if accessible externally.

Security Observations

Telnet Exposure (192.168.0.1): Telnet (port 23) is outdated and insecure. It should be disabled in favor of SSH or restricted to internal use.

UPnP Risks (192.168.0.1): UPnP (port 1900) can allow unauthorized devices to join the network. Disable unless explicitly required.

MySQL Exposure (192.168.0.17): An open MySQL port is a high-risk finding. Ensure the database is not accessible externally and uses strong credentials.

Filtered Ports (192.168.0.4, 192.168.0.6): Filtered ports indicate active firewalls, which is positive, but further scans may be needed to confirm no critical services are exposed.

Unknown Devices: Multiple hosts (192.168.0.3, 192.168.0.4, 192.168.0.9) have unknown MAC address vendors, suggesting consumer or untracked devices. Inventory and identify these devices.

Router Configuration (192.168.0.1): The router has multiple open ports, making it a prime target. Review and harden its configuration.

Recommendations

Disable Telnet: On 192.168.0.1, replace Telnet with SSH and enforce key-based authentication.

Secure MySQL: Restrict MySQL (192.168.0.17) to specific IP addresses using firewall rules. Update credentials and apply the latest patches.

Disable UPnP: Unless required, disable UPnP on 192.168.0.1 to prevent unauthorized device access.

Web Server Hardening: Ensure the HTTP service on 192.168.0.1 is running the latest software version and is protected against common vulnerabilities (e.g., XSS, SQL injection).

Device Inventory: Identify devices with unknown MAC addresses (192.168.0.3, 192.168.0.4, 192.168.0.9). Maintain a network inventory to track all devices.

Further Scanning: Perform UDP scans and targeted port scans on hosts with filtered ports (e.g., 192.168.0.6) to uncover additional services.

Network Segmentation: Implement VLANs or firewall rules to isolate critical services (e.g., MySQL) from untrusted devices.

Regular Monitoring: Schedule periodic Nmap scans to detect new devices or services on the network.

The scan took approximately 13.43 minutes and identified 6 active hosts.
Notes

All errors encountered during the scan were resolved through self-debugging.
No paid tools were used, as per task guidelines.
The report includes a comprehensive analysis of findings and security recommendations.

Conclusion

The Nmap scan revealed several security concerns, including exposed Telnet, MySQL, and UPnP services, as well as unidentified devices on the network. Immediate actions are recommended to secure the router (192.168.0.1) and MySQL server (192.168.0.17). The GitHub repository will include all necessary materials, as outlined above, to meet the submission requirements. Regular network monitoring and device inventory management are critical to maintaining a secure network environment.