Task 1:Scanning local network for open ports

Open Ports

Discovered open port 53/tcp on 192.168.0.1

Discovered open port 443/tcp on 192.168.0.1

Discovered open port 135/tcp on 192.168.0.164

Discovered open port 135/tcp on 192.168.0.202

Discovered open port 135/tcp on 192.168.0.89

Discovered open port 80/tcp on 192.168.0.1

Discovered open port 135/tcp on 192.168.0.209

Discovered open port 445/tcp on 192.168.0.209

Discovered open port 3306/tcp on 192.168.0.202

Discovered open port 139/tcp on 192.168.0.209

Discovered open port 445/tcp on 192.168.0.202

Discovered open port 139/tcp on 192.168.0.202

Discovered open port 445/tcp on 192.168.0.89

Discovered open port 445/tcp on 192.168.0.164

Discovered open port 139/tcp on 192.168.0.89

Wireshark Analysis: Open HTTP Port 80

1. Findings

Open Port Detected:

IP: 192.168.0.1

Port: 80/TCP (HTTP)

Evidence: Server responded with [SYN, ACK] (Packet 209), confirming the port is open and accepting connections.

Closed/Filtered Ports:

All other scanned IPs (192.168.0.98, 192.168.0.19, etc.) responded with [RST, ACK], indicating no active HTTP service or firewall blocking.

Anomalous Behavior:

Source IP 192.168.0.153 sent rapid [SYN] packets to multiple hosts (resembling a port scan).

Abrupt [RST, ACK] response to 192.168.0.1 (Packet 212) suggests intentional connection termination (e.g., scanning tool or misconfiguration).

2. Technical Analysis

TCP Handshake Observed:

plaintext

192.168.0.153 → 192.168.0.1: [SYN] (Connection initiation)

192.168.0.1 → 192.168.0.153: [SYN, ACK] (Port 80 open)

192.168.0.153 → 192.168.0.1: [RST, ACK] (Connection reset)

The expected [ACK] to complete the handshake was missing, implying an incomplete connection.

Scanning Indicators:

Reuse of source port 46273 across multiple targets.

High frequency of [SYN] packets (millisecond intervals).

3. Security Implications

Risk:

An open HTTP port (80) on 192.168.0.1 could expose unencrypted web traffic or vulnerable services.

Recommendations:

For 192.168.0.1:

Disable HTTP (port 80) if unnecessary, or enforce HTTPS (port 443).

Audit the web server for vulnerabilities (e.g., outdated software).

Network Monitoring:

Log and alert on repeated port scans.

Implement firewall rules to block suspicious SYN floods.

4. Conclusion

192.168.0.1:80 is the only active HTTP service in the scanned subnet.

Potential Risks from Open Ports

1. Risks Associated with Open HTTP Port (80/TCP)

An open HTTP port (80) on 192.168.0.1 introduces several security risks:

A. Information Exposure

Unencrypted Traffic: HTTP transmits data in plaintext, allowing attackers to intercept sensitive information (e.g., credentials, cookies)

Server Banner Leakage: Web servers (e.g., Apache, Nginx) often expose version details, aiding attackers in exploiting known vulnerabilities.

B. Exploitation of Known Vulnerabilities

Outdated Software: If the web server or applications are unpatched, attackers can exploit CVEs (e.g., Log4j, Heartbleed for older systems).

Default Configurations: Misconfigured servers may allow directory listing, unauthorized access, or admin panel exposure.

C. Attack Vectors

Brute Force Attacks: Weak login pages (e.g., /admin, /wp-login.php) can be targeted.

Cross-Site Scripting (XSS) / SQL Injection: Vulnerable web apps may allow code injection or database breaches.

DDoS Amplification: Open ports can be abused in reflection attacks (e.g., HTTP flood).

2. Risks from Port Scanning Activity (192.168.0.153)

The scan behavior (SYN packets to multiple IPs) suggests:

Reconnaissance Phase: An attacker may be mapping the network for weak points.

Follow-Up Attacks: Potential next steps:

Exploitation: Targeting 192.168.0.1:80 with web app attacks.

Lateral Movement: If compromised, pivoting to other internal systems.

3. Additional Risks from Other Open Ports (Hypothetical)

While only port 80 was detected here, other common open ports pose risks:

Port	Service	Potential Risks
22/TCP	SSH	Brute force attacks, unauthorized remote access if weak credentials are used.
443/TCP	HTTPS	SSL/TLS vulnerabilities (e.g., expired certificates, Heartbleed).
3389/TCP	RDP	Credential theft, ransomware attacks.
21/TCP	FTP	Data interception (plaintext), anonymous login exploits.

4. Mitigation Strategies

For Open HTTP Port 80 (192.168.0.1)

Enforce HTTPS: Redirect HTTP → HTTPS (port 443) and use TLS 1.2+/1.3.

Web Server Hardening

Remove unnecessary headers (e.g., Server: Apache/2.4.1).

Use WAF (Web Application Firewall) to block injection attacks.

Regular Patching: Update the web server (e.g., Apache/Nginx) and backend apps (e.g., PHP, WordPress).

For Port Scanning Activity

Block Unauthorized Scans:

Firewall rules to throttle SYN floods (e.g., iptables/Windows Firewall).

Implement IDS/IPS (e.g., Snort, Suricata) to detect scans.

Investigate Source (192.168.0.153):

Check logs for malware (e.g., netstat -ano, process monitoring).

Verify if scanning was authorized (e.g., IT security team).

General Best Practices

Network Segmentation: Isolate critical systems (e.g., place 192.168.0.1 in a DMZ).

Port Auditing: Regularly scan for unintended open ports (e.g., nmap -sV 192.168.0.0/24).

Least Privilege: Restrict access to port 80 via IP whitelisting if possible.