Local Network Port Scan & Risk Assessment Report

Scan Tool: Nmap 7.94SVN

Scan Type: TCP SYN Scan (-sS)

Command Executed:

```
nmap -sS -oN scan_results.txt 172.X.X.X/24
```

1. Summary

A reconnaissance scan was performed on the internal subnet to identify exposed services and evaluate potential security risks. Two live hosts were discovered:

Host	Exposed Ports	Risk Summary
172.X.X.1	21 (FTP), 53 (DNS)	High – legacy & misconfigured services
172.X.X.3	135, 139, 445 (Filtered)	Medium – Windows SMB stack, protected by firewall

Primary concerns include insecure services (FTP & DNS) and legacy Windows SMB services that could be exploited if firewall rules change.

2. Host-Level Findings

2.1 Host: 172.X.X.1

MAC: Unknown vendor

Open Ports:

Port	Service	Security Concern
21/tcp	FTP	Transmits credentials in plaintext, risk of anonymous logins
53/tcp	DNS	May allow DNS amplification or internal zone disclosure

Analysis

FTP (Port 21)

- Legacy, insecure protocol

- Credentials transmitted unencrypted
- Possible anonymous access exploitation

DNS (Port 53)

- Risk of DNS amplification attacks
- Misconfiguration may allow zone transfers
- Internal network data exposure

2.2 Host: 172.X.X.3

MAC: Intel Corporate (Indicates Windows-based host)

Filtered Ports:

Port	Service
135/tcp	MS RPC
139/tcp	NetBIOS
445/tcp	SMB

Analysis

- Services associated with historical exploits such as EternalBlue (MS17-010)
- Firewall filtering reduces immediate exposure
- Risk increases if rules are relaxed or host is misconfigured

---

3. Risk Rating

Host	Severity	Reason
172.X.X.1	High	Exposed & insecure FTP, DNS services
172.X.X.3	Medium	SMB/RPC stack present but firewalled

---

4. Recommendations

For Host 172.X.X.1

- Replace FTP with SFTP or FTPS
- Restrict port exposure using firewall rules
- Disable anonymous FTP access
- Validate DNS configuration and disable zone transfers
- Perform software version scan using:

For Host X.X.X.3

- Maintain firewall rules
- Disable SMBv1
- Apply Windows security patches
- Run periodic vulnerability assessments:

5. Keywords & Definitions

Keyword	Definition
FTP (File Transfer Protocol)	A legacy protocol used to transfer files between client and server over TCP (usually port 21). It sends credentials and data in plaintext, making it vulnerable to sniffing and credential theft on untrusted networks.
DNS (Domain Name System)	The service that translates human-readable domain names into IP addresses (commonly on port 53). Misconfigured DNS can leak internal information (via zone transfers) or be abused for amplification and reflection attacks in DDoS campaigns.
Filtered Ports	Ports where a firewall or filtering device drops or blocks probe packets instead of explicitly accepting or rejecting them. This indicates some protection is in place, but the underlying service may still be reachable from other networks or misconfigurations.
MS RPC (Microsoft Remote Procedure Call)	A Windows service (often on port 135) used for DCOM, remote management, and inter-process communication. Historically, MS RPC has been a target for remote code execution exploits and lateral movement inside Windows environments.
NetBIOS (Network Basic Input/Output System)	A legacy Windows networking protocol (commonly on port 139) used for name resolution and file/printer sharing. It is largely superseded but still present on many systems and can expose hostnames and shares to attackers.
SMB (Server Message Block)	A file and printer sharing protocol used by Windows (commonly on port 445). Vulnerabilities in SMB (e.g., EternalBlue) have been used for wormable attacks, ransomware propagation, and lateral movement within networks.
EternalBlue	A highly critical SMBv1 exploit (MS17-010) used by malware such as WannaCry and NotPetya to achieve remote code execution and worm-like spread. Systems with unpatched SMBv1 and exposed port 445 are at severe risk from this class of attacks.

6. Conclusion

The performed scan highlighted one vulnerable host (likely IoT/router) exposing FTP and DNS, and one Windows system running SMB but properly firewalled. Immediate attention is required for Host 172.X.X.1 to prevent credential leakage, internal reconnaissance, and potential exploitation.

Overall Network Exposure: Moderate

Priority Action: Harden or isolate Host 172.X.X.1 immediately.