

Overview

During network reconnaissance using Nmap, several common ports and services are often detected. Understanding the purpose of these services and the potential vulnerabilities they may expose is crucial for evaluating network security.

Common Ports, it's Services, and it's Risks

Port	Protocol	Service	Description	Common Security Risks
21	TCP	FTP (File Transfer Protocol)	Transfers files between systems.	- Plaintext credentials- Anonymous login- Vulnerable FTP software
22	TCP	SSH (Secure Shell)	Secure remote login.	- Brute force attacks- Weak keys/passwords- Outdated SSH versions
23	TCP	Telnet	Unsecured remote login.	- Transmits credentials in plaintext- Vulnerable to sniffing and MITM attacks
25	TCP	SMTP (Simple Mail Transfer Protocol)	Sends email messages.	- Open relay for spam- Spoofing attacks- Lack of authentication
53	TCP/UDP	DNS (Domain Name System)	Resolves domain names.	- DNS poisoning- Amplification attacks- Zone transfer exposure
80	TCP	HTTP (Hypertext Transfer Protocol)	Unsecured web traffic.	- Insecure login forms- Lack of encryption- Susceptible to XSS, CSRF
110	TCP	POP3 (Post Office Protocol)	Email retrieval.	- Plaintext transmission of credentials- Mailbox access vulnerabilities

135	TCP	Microsoft RPC	Used for DCOM services in Windows.	- DCOM vulnerabilities- Lateral movement risks
139	TCP	NetBIOS Session Service	File/printer sharing on Windows.	- SMB vulnerabilities- Information leakage- EternalBlue exploit risk
143	TCP	IMAP (Internet Message Access Protocol)	Email retrieval.	- Unencrypted logins- MITM risk
443	TCP	HTTPS (HTTP Secure)	Secure web communication.	- SSL/TLS misconfiguration- Weak ciphers/protocols
445	TCP	SMB (Server Message Block)	File sharing in Windows.	- Major target for worms/ransomware- EternalBlue, WannaCry vulnerabilities
3306	TCP	MySQL	Open-source database server.	- SQL injection- Default credentials- Unprotected access over network
3389	TCP	RDP (Remote Desktop Protocol)	Remote desktop on Windows.	- Brute-force attacks- BlueKeep vulnerability- RDP tunneling
8080	TCP	HTTP-alt / Web Proxy	Alternate HTTP port, often used for web apps.	- Same risks as port 80- Admin interfaces exposed
8443	TCP	HTTPS-alt	Alternative HTTPS port, usually for admin panels.	- Misconfigured SSL- Exposed admin interfaces

Top Threats Identified by Nmap Scans

1. Unsecured Services (Telnet, FTP, HTTP)

- Lack of encryption leads to data leakage.
- Should be replaced with secure alternatives (e.g., SSH, SFTP, HTTPS).

2. Outdated or Vulnerable Software

- Common with services like SMB (port 445), RDP (3389), MySQL (3306).
- Leads to exploits such as EternalBlue, BlueKeep.

3. Exposed Admin Interfaces

- Services on non-standard ports (e.g., 8080, 8443) may host web admin panels.
- If unprotected, can lead to full system compromise.

4. Poor Authentication

- Many services use default or weak credentials.
- Enforce strong password policies and multi-factor authentication (MFA).

5. Unfiltered Open Ports

- Unused services still accepting connections.
 - Follow the principle of least privilege; close unused ports.
-

Security Recommendations

1. **Use firewalls** to restrict access to critical services.
2. **Enforce encryption:** Use HTTPS, SFTP, and disable plaintext protocols.
3. **Disable unused services** and remove legacy applications.
4. **Patch regularly:** Keep all services and OS updated.
5. **Use IDS/IPS:** Detect and prevent abnormal network behavior.
6. **Scan regularly with tools like Nmap and Nessus** to assess security posture.

Sample Nmap Command Used

`nmap -sS -sV -p- -Pn 192.168.1.0/24 -oA network_scan`

- -sS: SYN scan
- -sV: Service/version detection
- -p-: Scan all 65535 ports
- -Pn: Skip host discovery
- -oA: Save in all formats (Nmap, XML, Grep)

Example1:

```
# Nmap 7.95 scan initiated Mon May 26 18:31:04 2025 as: /usr/lib/nmap/nmap --privileged -sS -oN report.txt 192.168.1.4/24
```

Nmap scan report for dsldevice.lan (192.168.1.1)

Host is up (0.0033s latency).

Not shown: 994 filtered tcp ports (no-response)

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https
445/tcp	closed	microsoft-ds
8008/tcp	closed	http
49156/tcp	closed	unknown
49163/tcp	closed	unknown

MAC Address: 4C:06:17:13:8A:8C (Taicang T&W Electronics)

Nmap scan report for 192.168.1.2

Host is up (0.0056s latency).

Not shown: 995 closed tcp ports (reset)

PORT	STATE	SERVICE
80/tcp	open	http
8008/tcp	open	http
8009/tcp	open	ajp13
8443/tcp	open	https-alt
9000/tcp	open	cslistener

MAC Address: 40:49:0F:23:BC:2B (Hon Hai Precision Ind.)

Nmap scan report for 192.168.1.3

Host is up (0.021s latency).

Not shown: 996 closed tcp ports (reset)

PORT	STATE	SERVICE
8008/tcp	open	http
8009/tcp	open	ajp13
8443/tcp	open	https-alt
9000/tcp	open	cslistener

MAC Address: BC:C7:DA:BB:37:06 (Earda Technologies)

Nmap scan report for 192.168.1.5

Host is up (0.00050s latency).

Not shown: 999 filtered tcp ports (no-response)

PORT STATE SERVICE

6881/tcp open bittorrent-tracker

MAC Address: 70:1A:B8:71:7E:7E (Intel Corporate)

Nmap scan report for 192.168.1.8

Host is up (0.0028s latency).

Not shown: 998 closed tcp ports (reset)

PORT STATE SERVICE

80/tcp open http

554/tcp open rtsp

MAC Address: 28:18:FD:5A:38:36 (Aditya Infotech)

Nmap scan report for 192.168.1.4

Host is up (0.0000010s latency).

All 1000 scanned ports on 192.168.1.4 are in ignored states.

Not shown: 1000 closed tcp ports (reset)

Nmap done at Mon May 26 18:31:26 2025 -- 256 IP addresses (6 hosts up) scanned in 21.77 seconds

Example2:

Nmap 7.95 scan initiated Mon May 26 18:54:37 2025 as: /usr/lib/nmap/nmap --privileged -sS

-sV -O -Pn -p- -oN report2.txt 192.168.1.4

Nmap scan report for 192.168.1.4

Host is up (0.000046s latency).

Not shown: 65533 closed tcp ports (reset)

PORT STATE SERVICE VERSION

1716/tcp open tcpwrapped

3443/tcp open ssl/http Ajenti http control panel

Device type: general purpose

Running: Linux 2.6.X|5.X

OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:6

OS details: Linux 2.6.32, Linux 5.0 - 6.2

Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at

<https://nmap.org/submit/>.

Nmap done at Mon May 26 18:54:52 2025 -- 1 IP address (1 host up) scanned in 15.33 seconds

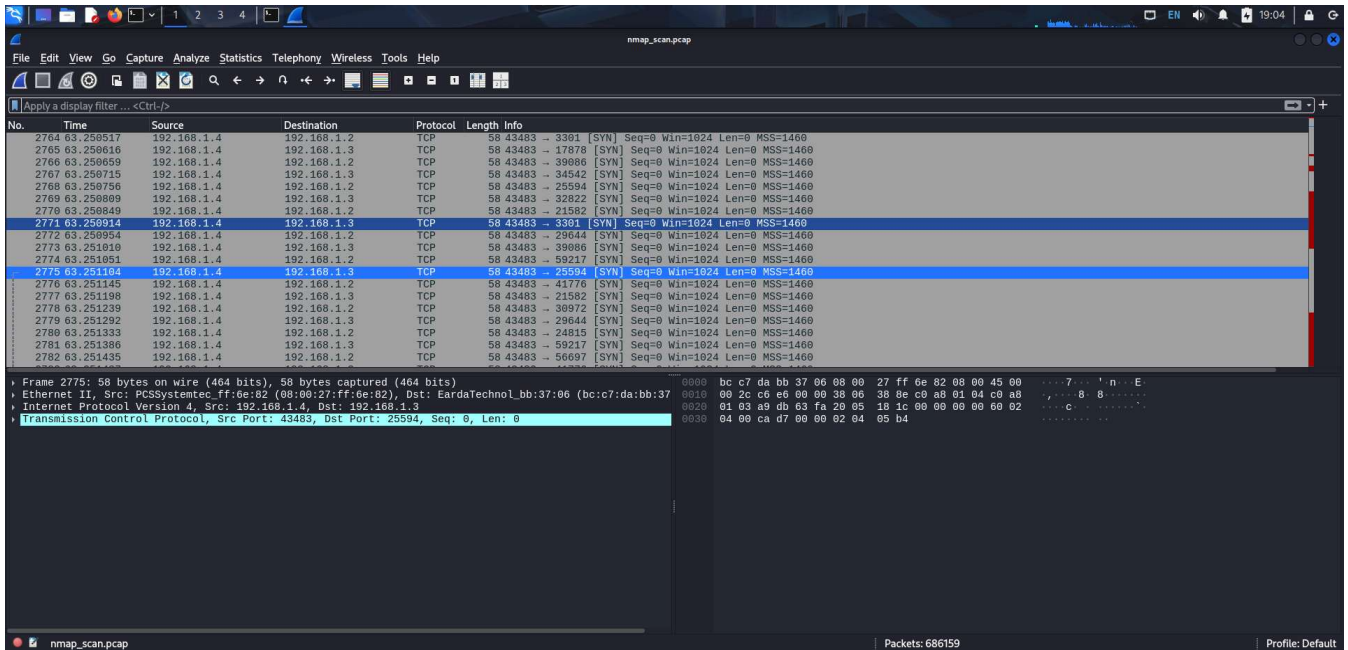
Sample Wireshark Used:

- ★ Capturing packet using tcpdump while running Nmap in another terminal.

sudo tcpdump -i eth0 -w nmap_scan.pcap

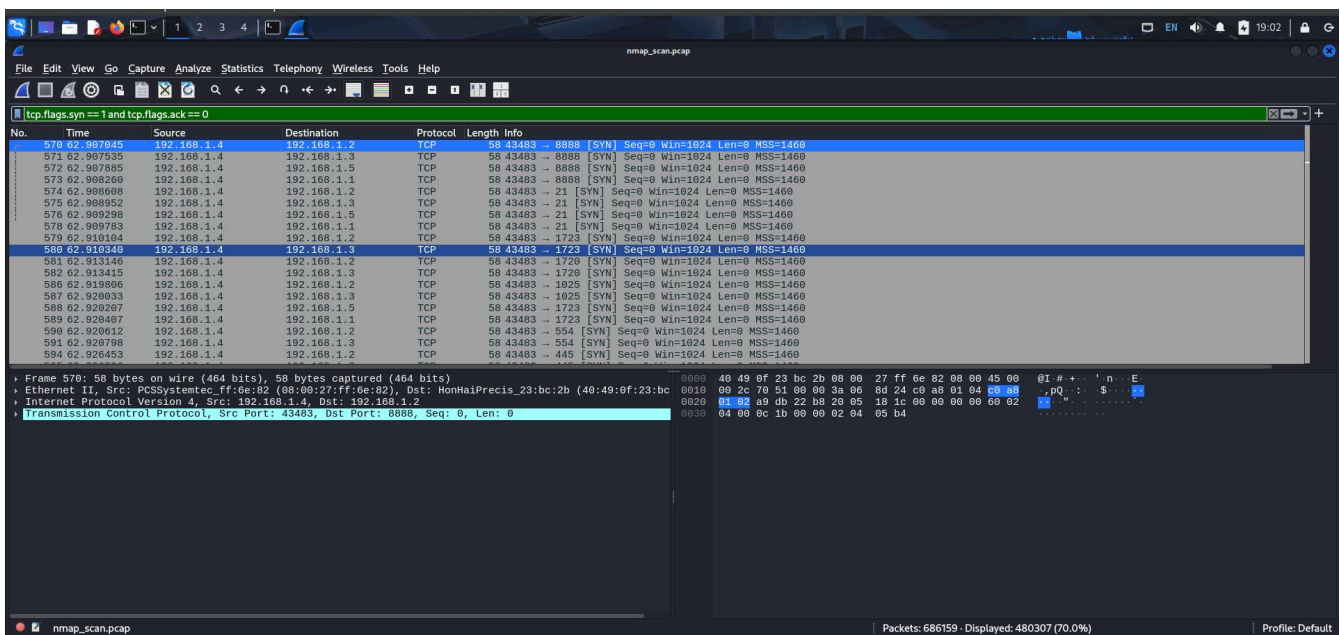
- ★ Stop **tcpdump** after the scan complete and open the capture in Wireshark:

wireshark nmap_scan.pcap



- ★ Analyzing packet capture by with Wireshark:

- Using **tcp.flags.syn == 1** and **tcp.flags.ack == 0**:
shows SYN packets (initial connection attempts)



- Using `ip.addr == 192.168.1.10:`
filters by IP

The image shows a Wireshark packet capture of network traffic. The filter bar at the top is set to `ip.addr == 192.168.1.4`. The packet list on the left shows a series of DNS queries and responses between 192.168.1.1 and 192.168.1.4. The packet details pane on the right shows the structure of a DNS query (Frame 14), including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query). The packet bytes pane on the right shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
14	24.388635	192.168.1.4	192.168.1.1	DNS	84	Standard query 0xc9f9 PTR 4.1.168.192.in-addr.arpa
15	24.393123	192.168.1.1	192.168.1.4	DNS	161	Standard query response 0xc9f9 No such name PTR 4.1.168.192.in-addr.arpa SOA prisoner.iana.org
560	62.795647	192.168.1.4	192.168.1.1	DNS	84	Standard query 0xd0eb PTR 1.1.168.192.in-addr.arpa
561	62.796264	192.168.1.4	192.168.1.1	DNS	84	Standard query 0xd0ec PTR 2.1.168.192.in-addr.arpa
562	62.796737	192.168.1.4	192.168.1.1	DNS	84	Standard query 0xd0ed PTR 3.1.168.192.in-addr.arpa
563	62.797279	192.168.1.4	192.168.1.1	DNS	84	Standard query 0xd0ee PTR 5.1.168.192.in-addr.arpa
564	62.798211	192.168.1.4	192.168.1.1	DNS	84	Standard query 0xd0ef PTR 8.1.168.192.in-addr.arpa
565	62.798436	192.168.1.1	192.168.1.4	DNS	111	Standard query response 0xd0eb PTR 1.1.168.192.in-addr.arpa PTR dsldevice.lan
566	62.803095	192.168.1.4	192.168.1.1	DNS	161	Standard query response 0xd0ec No such name PTR 2.1.168.192.in-addr.arpa SOA prisoner.iana.org
567	62.883096	192.168.1.1	192.168.1.4	DNS	161	Standard query response 0xd0ed No such name PTR 3.1.168.192.in-addr.arpa SOA prisoner.iana.org
568	62.883096	192.168.1.1	192.168.1.4	DNS	161	Standard query response 0xd0ee No such name PTR 5.1.168.192.in-addr.arpa SOA prisoner.iana.org
569	62.883096	192.168.1.1	192.168.1.4	DNS	161	Standard query response 0xd0ef No such name PTR 8.1.168.192.in-addr.arpa SOA prisoner.iana.org
570	62.907845	192.168.1.4	192.168.1.2	TCP	58	43483 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
571	62.907835	192.168.1.4	192.168.1.3	TCP	58	43483 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
572	62.907885	192.168.1.4	192.168.1.5	TCP	58	43483 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
573	62.908260	192.168.1.4	192.168.1.1	TCP	58	43483 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
574	62.908680	192.168.1.4	192.168.1.2	TCP	58	43483 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
575	62.908952	192.168.1.4	192.168.1.3	TCP	58	43483 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
576	62.909298	192.168.1.4	192.168.1.5	TCP	58	43483 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Frame 14: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface
Ethernet II, Src: PCSSystemtec ff:0e:82 (08:00:27:ff:0e:82), Dst: TaicangT&E\13:8a:8c (4c:00:17:13:8a:8c)
Internet Protocol Version 4, Src: 192.168.1.4, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 44933, Dst Port: 53
Domain Name System (query)

Packet bytes: 0000 4c 06 17 13 8a 8c 08 00 27 ff 6e 82 08 00 45 00 L n...E
0010 00 46 bc 18 40 00 40 11 fd 38 c9 a8 01 04 c0 a8 F... ..
0020 01 01 af 05 00 35 00 32 83 99 ca f9 01 00 00 01 5 2
0030 00 00 00 00 00 00 01 34 01 31 03 31 36 38 03 31 4 .1.168.1
0040 39 32 07 69 6e 2d 61 64 64 72 04 61 72 70 61 00 92 in-ad dr arpa
0050 00 0c 00 01