

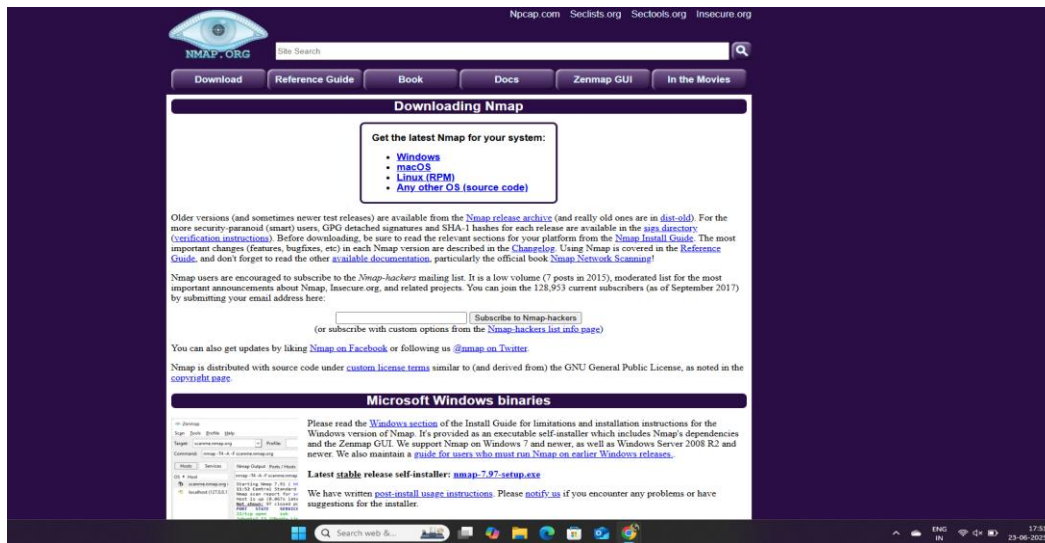
# CYBER SECURITY INTERNSHIP

## Task 1: Scan Your Local Network for Open Ports

**Objective:** Learn to discover open ports on devices in your local network to understand network exposure.

**Tools:** Nmap (free), Wireshark (optional)

### 1. Install Nmap from official website



### 2. Find your local IP range: use command: ipconfig to get ip range

```
C:\Users\divak>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Unknown adapter Local Area Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

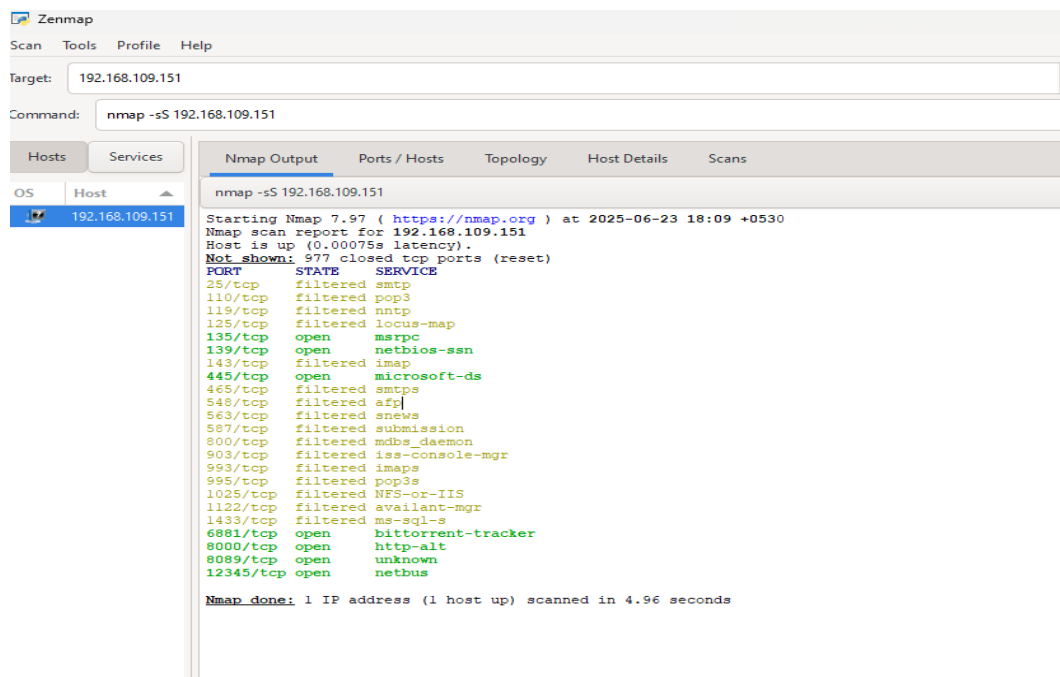
    Connection-specific DNS Suffix  . :
    IPv4 Address. . . . . : 192.168.109.151
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.109.228

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\divak>
```

### 3.Run: nmap -sS 192.168.1.0/24 to perform TCP SYN scan:



Zenmap

Scan Tools Profile Help

Target: 192.168.109.151

Command: nmap -sS 192.168.109.151

Hosts Services

OS Host

192.168.109.151

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sS 192.168.109.151

Starting Nmap 7.97 ( <https://nmap.org> ) at 2025-06-23 18:09 +0530  
Nmap scan report for 192.168.109.151  
Host is up (0.00075s latency).  
Not shown: 977 closed tcp ports (reset)

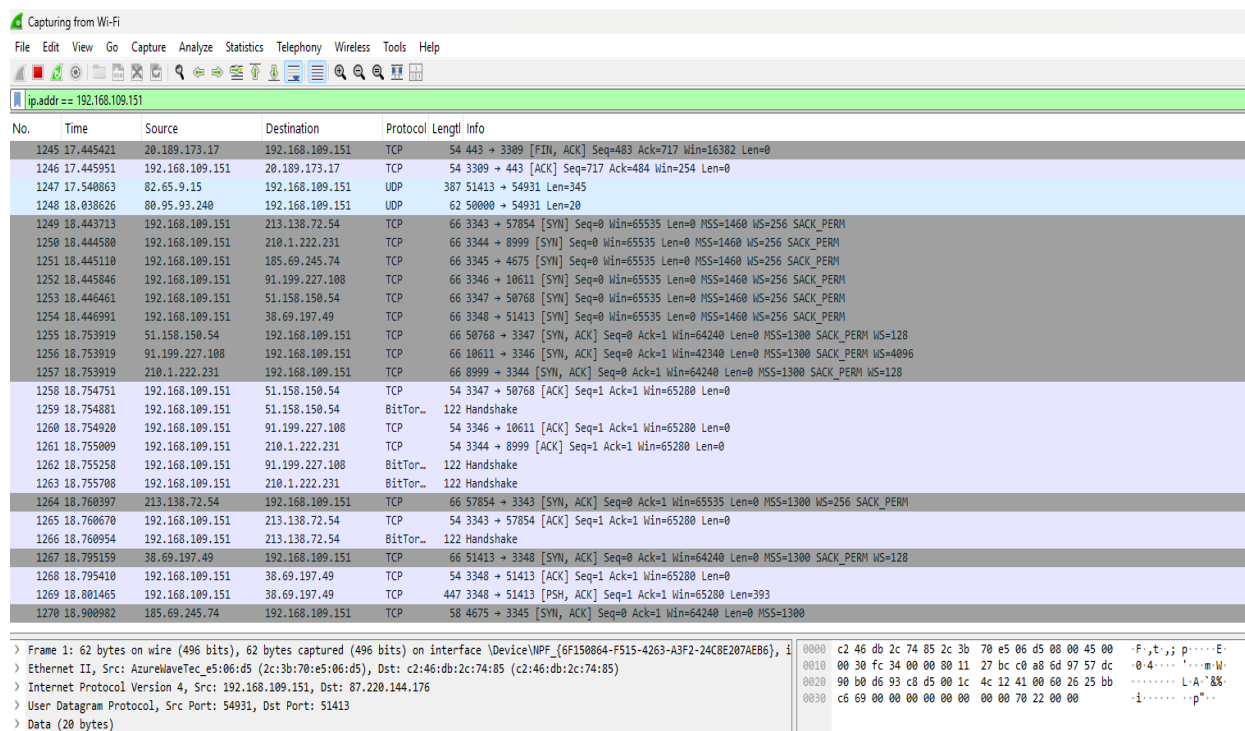
PORT	STATE	SERVICE
25/tcp	filtered	smtp
110/tcp	filtered	pop3
119/tcp	filtered	nntp
125/tcp	filtered	locus-map
135/tcp	open	marpc
139/tcp	open	netbios-ssn
143/tcp	filtered	imap
445/tcp	open	microsoft-ds
465/tcp	filtered	smtps
548/tcp	filtered	afp
563/tcp	filtered	snews
587/tcp	filtered	submission
800/tcp	filtered	mdbs_daemon
903/tcp	filtered	iss-Console-mgr
993/tcp	filtered	imaps
995/tcp	filtered	pop3s
1025/tcp	filtered	NFS-or-IIS
1122/tcp	filtered	avallant-mgr
1433/tcp	filtered	ms-sql-s
6881/tcp	open	bittorrent-tracker
8000/tcp	open	http-alt
8089/tcp	open	unknown
12345/tcp	open	netbus

Nmap done: 1 IP address (1 host up) scanned in 4.96 seconds

### 4. IP addresses and open ports found:

Open Ports: 135,139,445,6881,8000,8089,12345

### 5. analyze packet capture with Wireshark: use filter ip.addr== <ip address>



Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.109.151

No.	Time	Source	Destination	Protocol	Length	Info
1245	17.445421	20.189.173.17	192.168.109.151	TCP	54	443 → 3309 [FIN, ACK] Seq=483 Ack=717 Win=16382 Len=0
1246	17.445951	192.168.109.151	20.189.173.17	TCP	54	3309 → 443 [ACK] Seq=717 Ack=484 Win=254 Len=0
1247	17.540863	82.65.9.15	192.168.109.151	UDP	387	51413 → 54931 Len=345
1248	18.038626	80.95.93.240	192.168.109.151	UDP	62	50000 → 54931 Len=20
1249	18.443713	192.168.109.151	213.138.72.54	TCP	66	3343 → 57854 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1250	18.444580	192.168.109.151	210.1.222.231	TCP	66	3344 → 8999 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1251	18.445110	192.168.109.151	185.69.245.74	TCP	66	3345 → 4675 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1252	18.445846	192.168.109.151	91.199.227.108	TCP	66	3346 → 10611 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1253	18.446461	192.168.109.151	51.158.150.54	TCP	66	3347 → 50768 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1254	18.446991	192.168.109.151	38.69.197.49	TCP	66	3348 → 51413 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1255	18.753919	51.158.150.54	192.168.109.151	TCP	66	50768 → 3347 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1300 SACK_PERM WS=128
1256	18.753919	91.199.227.108	192.168.109.151	TCP	66	10611 → 3346 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1300 SACK_PERM WS=4096
1257	18.753919	210.1.222.231	192.168.109.151	TCP	66	8999 → 3344 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1300 SACK_PERM WS=128
1258	18.754751	192.168.109.151	51.158.150.54	TCP	54	3347 → 50768 [ACK] Seq=1 Ack=1 Win=65280 Len=0
1259	18.754881	192.168.109.151	51.158.150.54	BitTor...	122	Handshake
1260	18.754920	192.168.109.151	91.199.227.108	TCP	54	3346 → 10611 [ACK] Seq=1 Ack=1 Win=65280 Len=0
1261	18.755009	192.168.109.151	210.1.222.231	TCP	54	3344 → 8999 [ACK] Seq=1 Ack=1 Win=65280 Len=0
1262	18.755258	192.168.109.151	91.199.227.108	BitTor...	122	Handshake
1263	18.755708	192.168.109.151	210.1.222.231	BitTor...	122	Handshake
1264	18.760397	213.138.72.54	192.168.109.151	TCP	66	57854 → 3343 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 WS=256 SACK_PERM
1265	18.760670	192.168.109.151	213.138.72.54	TCP	54	3343 → 57854 [ACK] Seq=1 Ack=1 Win=65280 Len=0
1266	18.760954	192.168.109.151	213.138.72.54	BitTor...	122	Handshake
1267	18.795159	38.69.197.49	192.168.109.151	TCP	66	51413 → 3348 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1300 SACK_PERM WS=128
1268	18.795410	192.168.109.151	38.69.197.49	TCP	54	3348 → 51413 [ACK] Seq=1 Ack=1 Win=65280 Len=0
1269	18.801465	192.168.109.151	38.69.197.49	TCP	447	3348 → 51413 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=393
1270	18.900982	185.69.245.74	192.168.109.151	TCP	58	4675 → 3345 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1300

> Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface \Device\NPF\_{6F150864-F515-4263-A3F2-24C8E207AEB6}, i

> Ethernet II, Src: AzurelaviTec\_e5:06:d5 (2c:3b:70:e5:06:d5), Dst: c2:46:db:2c:74:85 (c2:46:db:2c:74:85)

> Internet Protocol Version 4, Src: 192.168.109.151, Dst: 87.220.144.176

> User Datagram Protocol, Src Port: 54931, Dst Port: 51413

> Data (20 bytes)

0000 c2 46 db 2c 74 85 2c 3b 70 e5 06 d5 00 00 45 00 ·F,t,; p····E·  
0010 00 30 fc 34 00 00 80 11 27 bc c0 a8 6d 97 57 dc ·0.4....'··m·W·  
0020 90 b0 d6 93 c8 d5 00 1c 4c 12 41 00 60 26 25 bb ······L·A··8%·  
0030 c6 69 00 00 00 00 00 00 00 00 70 22 00 00 ·i······p···

## Use filter tcp.port == <port> || udp.port == <port>

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 80 || udp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
2878	46.980429	192.168.109.151	142.250.192.35	TCP	54	3452 → 80 [ACK] Seq=403 Ack=445 Win=65024 Len=0
2896	47.077236	43.175.141.63	192.168.109.151	TCP	66	80 → 3453 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 SACK_PERM WS=1024
2897	47.077711	192.168.109.151	43.175.141.63	TCP	54	3453 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
2898	47.080337	192.168.109.151	43.175.141.63	HTTP	336	GET /msdownload/update/v3/static/trusted/en/authrootstl.cab?762919c0906727a1 HTTP/1.1
2939	47.168681	43.175.141.63	192.168.109.151	TCP	54	80 → 3453 [ACK] Seq=1 Ack=283 Win=524288 Len=0
2940	47.168681	43.175.141.63	192.168.109.151	HTTP	357	HTTP/1.1 304 Not Modified
2941	47.169856	43.175.141.63	192.168.109.151	TCP	54	80 → 3453 [FIN, ACK] Seq=304 Ack=283 Win=524288 Len=0
2942	47.169163	192.168.109.151	43.175.141.63	TCP	54	3453 → 80 [ACK] Seq=283 Ack=304 Win=65024 Len=0
2943	47.171249	192.168.109.151	43.175.141.63	TCP	54	3453 → 80 [ACK] Seq=283 Ack=305 Win=65024 Len=0
2944	47.171490	192.168.109.151	43.175.141.63	TCP	54	3453 → 80 [FIN, ACK] Seq=283 Ack=305 Win=65024 Len=0
2945	47.171806	192.168.109.151	43.175.141.63	TCP	54	3453 → 80 [RST, ACK] Seq=284 Ack=305 Win=0 Len=0
2946	47.187175	192.168.109.151	43.175.141.63	TCP	66	3456 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2960	47.213865	43.175.141.63	192.168.109.151	TCP	55	[TCP Spurious Retransmission] 80 → 3453 [PSH, ACK] Seq=302 Ack=283 Win=524288 Len=1
2978	47.267699	43.175.141.63	192.168.109.151	TCP	66	80 → 3456 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 SACK_PERM WS=1024
2971	47.267699	43.175.141.63	192.168.109.151	TCP	55	[TCP Spurious Retransmission] 80 → 3453 [PSH, ACK] Seq=300 Ack=283 Win=524288 Len=1
2972	47.268151	192.168.109.151	43.175.141.63	TCP	54	3456 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
2974	47.270913	192.168.109.151	43.175.141.63	HTTP	336	GET /msdownload/update/v3/static/trusted/en/pinrulesstl.cab?e78487dba66a2ae7 HTTP/1.1
2975	47.290494	43.175.141.63	192.168.109.151	TCP	54	80 → 3453 [ACK] Seq=305 Ack=284 Win=524288 Len=0
2976	47.351154	43.175.141.63	192.168.109.151	TCP	54	80 → 3456 [ACK] Seq=1 Ack=283 Win=524288 Len=0
2977	47.352785	43.175.141.63	192.168.109.151	HTTP	358	HTTP/1.1 304 Not Modified
2978	47.352785	43.175.141.63	192.168.109.151	TCP	54	80 → 3456 [FIN, ACK] Seq=305 Ack=283 Win=524288 Len=0
2979	47.354842	192.168.109.151	43.175.141.63	TCP	54	3456 → 80 [ACK] Seq=283 Ack=306 Win=65024 Len=0
2980	47.355064	192.168.109.151	43.175.141.63	TCP	54	3456 → 80 [FIN, ACK] Seq=283 Ack=306 Win=65024 Len=0
2981	47.355407	192.168.109.151	43.175.141.63	TCP	54	3456 → 80 [RST, ACK] Seq=284 Ack=306 Win=0 Len=0
2982	47.396601	43.175.141.63	192.168.109.151	TCP	55	[TCP Spurious Retransmission] 80 → 3456 [PSH, ACK] Seq=303 Ack=283 Win=524288 Len=1
2983	47.437968	43.175.141.63	192.168.109.151	TCP	54	80 → 3456 [ACK] Seq=306 Ack=284 Win=524288 Len=0

> Frame 1175: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{6F150864-F515-4263-A3F2-24C8E207AE86}

> Ethernet II, Src: c2:46:db:2c:74:85 (c2:46:db:2c:74:85), Dst: AzureWaveTec\_e5:06:d5 (2c:3b:70:e5:06:d5)

> Internet Protocol Version 4, Src: 54.169.7.73, Dst: 192.168.109.151

> Transmission Control Protocol, Src Port: 80, Dst Port: 60550, Seq: 1, Ack: 1, Len: 0

0000 2c 3b 70 e5 06 d5 c2 46 db 2c 74 85 08 00 45 00 :p....F...E..  
0010 00 28 00 00 40 00 33 06 db 9e 36 a9 07 49 c0 a8 :(.@:3...6..I..  
0020 6d 97 00 50 ec 86 c1 d5 ce f8 95 53 b8 60 50 10 m:P.....S.P..  
0030 01 e8 76 61 00 00 :va..

## 6. Research common services running on those ports:

### Open Ports and Their Services

These ports are accessible and are likely running the listed services:

Port	Protocol	Service	Notes
135/tcp	TCP	Microsoft RPC (msrpc)	Common on Windows; used for DCOM
139/tcp	TCP	NetBIOS-SSN	Windows file/printer sharing
445/tcp	TCP	Microsoft-DS (SMB)	Used for file sharing; common attack vector
6881/tcp	TCP	BitTorrent-Tracker	Used for P2P file sharing
8000/tcp	TCP	HTTP-alt	Alternate HTTP; often custom apps or dashboards
8089/tcp	TCP	Unknown	Needs further probing to identify the service
12345/tcp	TCP	NetBus	Malware/Trojan backdoor, highly suspicious

## 🚫 Filtered Ports and Their Common Services

These ports are filtered (likely firewalled), and may or may not have services running behind them:

Port	Protocol	Common Service
25/tcp	TCP	SMTP (email sending)
110/tcp	TCP	POP3 (email receiving)
119/tcp	TCP	NNTP (Usenet)
125/tcp	TCP	Locus-Map
143/tcp	TCP	IMAP
465/tcp	TCP	SMTPS (secure SMTP)
548/tcp	TCP	AFP (Apple Filing Protocol)
563/tcp	TCP	SNEWS (Secure NNTP)
587/tcp	TCP	Submission (SMTP)
800/tcp	TCP	MDBS_Daemon
903/tcp	TCP	ISS Console Manager
993/tcp	TCP	IMAPS (Secure IMAP)
995/tcp	TCP	POP3S (Secure POP3)
1025/tcp	TCP	NFS/IIS (varies)
1122/tcp	TCP	Availant Manager
1433/tcp	TCP	Microsoft SQL Server

## 7. potential security risks from open ports:

### General Risks of Open Ports

#### 1. Unauthorized Access

- Any open port is a potential entry point.
- If a service behind an open port is misconfigured, lacks authentication, or has weak credentials, attackers can gain access to the system.

#### 2. Service Enumeration

- Attackers use open ports to learn about the services, software versions, and OS in use.
- This reconnaissance phase helps them choose targeted exploits.

### **3. Exploitation of Vulnerabilities**

- Services listening on open ports may have known vulnerabilities (e.g., buffer overflows, RCE bugs).
- Unpatched services can be compromised with publicly available exploits.

### **4. Malware and Backdoor Communication**

- Malware often uses specific ports (like 12345 for NetBus) to receive commands or exfiltrate data.
- Open ports can facilitate C2 (Command & Control) communication.

### **5. Denial of Service (DoS) Attacks**

- Open ports expose services that may be overwhelmed with requests, causing them to crash or become unresponsive.

### **6. Data Leakage**

- Some services (e.g., SMB, SNMP) may inadvertently expose sensitive data like usernames, shares, network info.
- Misconfigured web services can leak internal paths, APIs, or configuration files.

### **7. Lateral Movement**

- In internal networks, attackers can exploit open ports to move laterally from one host to another, escalating privileges.

### **8. Botnet Recruitment**

- Internet-facing systems with open ports can be compromised and recruited into botnets for spam, DDoS, or crypto mining.

### **135/tcp – Microsoft RPC (msrpc)**

- Risk: Exposed DCOM/RPC services on Windows can be exploited remotely.
- Common Exploits: DCOM vulnerabilities, Blaster worm, privilege escalation.
- Mitigation: Restrict to local/internal networks via firewall.

### **139/tcp – NetBIOS Session Service**

- Risk: Leaks information about file shares and can enable unauthorized access to Windows systems.

- Common Exploits: Enumeration of shared resources, Man-in-the-Middle (MitM) attacks, credential harvesting.
- Mitigation: Disable if not needed; block at perimeter firewall.

#### **445/tcp – Microsoft-DS (SMB)**

- Risk: Frequently targeted for remote code execution and lateral movement.
- Common Exploits: EternalBlue, WannaCry ransomware, SMBRelay attacks.
- Mitigation: Keep Windows patched, disable SMBv1, use strong authentication, restrict access.

#### **6881/tcp – BitTorrent Tracker**

- Risk: P2P services can expose the system to unauthorized access, DoS, and bandwidth abuse.
- Common Exploits: Peer flooding, IP leakage, propagation of malware.
- Mitigation: Disable if not used for legitimate reasons; monitor traffic.

#### **8000/tcp – HTTP-alt (Custom Web Services)**

- Risk: May host vulnerable or outdated web applications.
- Common Exploits: XSS, SQL injection, remote file inclusion.
- Mitigation: Identify the app, ensure it's updated, apply web hardening best practices.

#### **8089/tcp – Unknown Service**

- Risk: Unidentified services can mask backdoors or misconfigured applications.
- Mitigation: Investigate with tools like nmap -sV, netstat, or ss; disable or secure the service.

#### **12345/tcp – NetBus (Backdoor Trojan)**

- Risk: High! This port is used by NetBus, a known backdoor Trojan.
- Threats: Complete remote control of the system, data theft, keylogging, spyware.
- Mitigation:
  - Immediately disconnect the system from the network.
  - Run a full antivirus/malware scan.
  - Investigate for indicators of compromise (IoCs).
  - Consider reimaging the system if compromise is confirmed.

### Overall Security Recommendations

- Close unnecessary ports via host-based or network firewall.
- Audit running services and stop unused ones.
- Harden services by patching and using secure configurations.
- Use network segmentation to limit access to internal services.
- Monitor logs and enable intrusion detection systems (IDS).

### 8.Save scan results as a text or HTML file:

