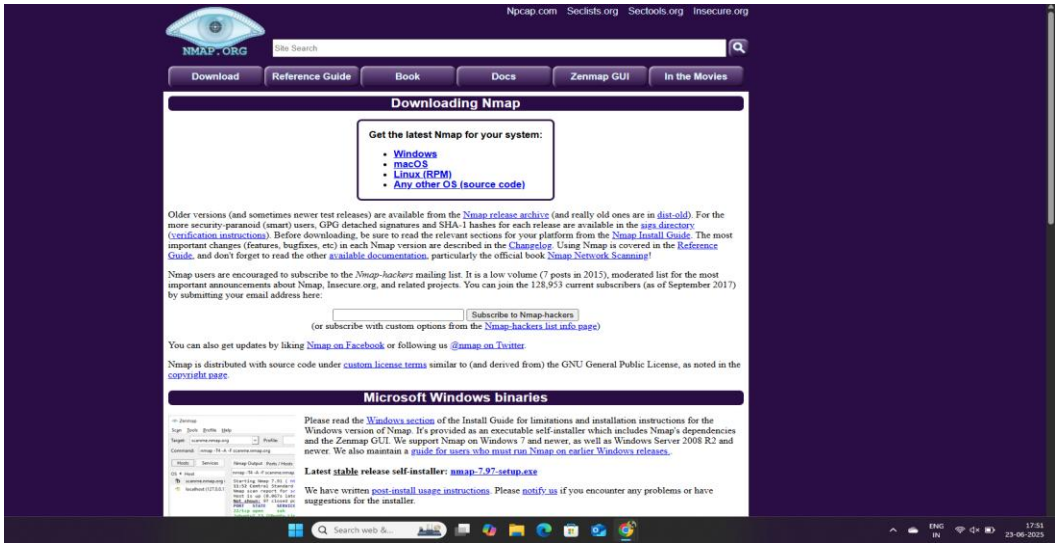
CYBER SECURITY INTERNSHIP

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)

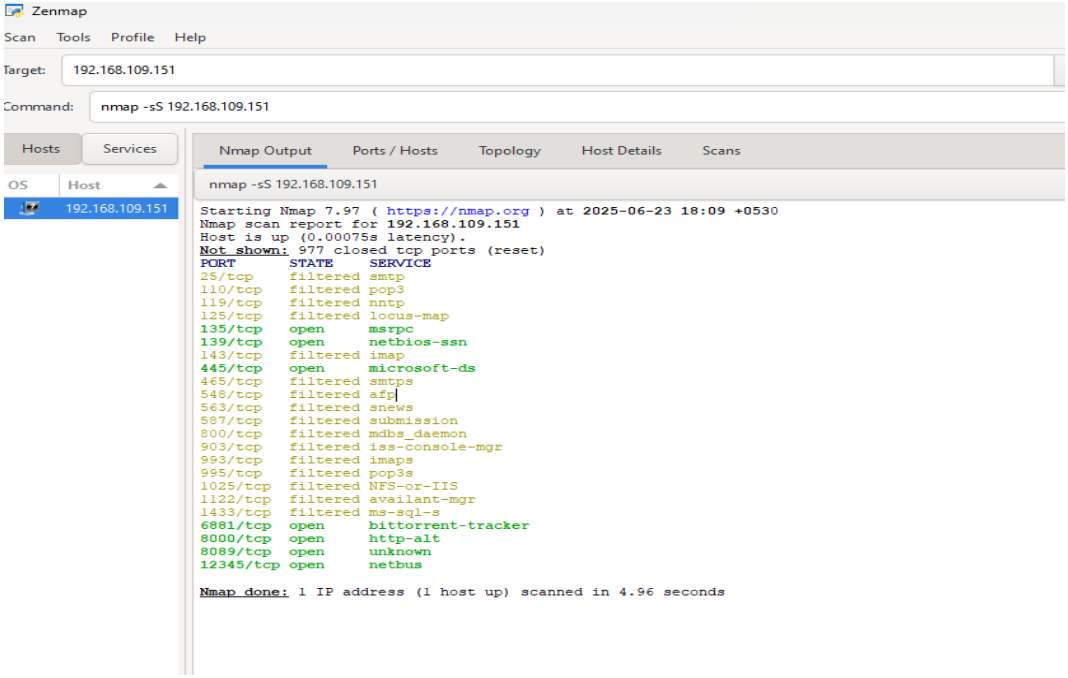
1.Insta l Nmap from official website



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>
```

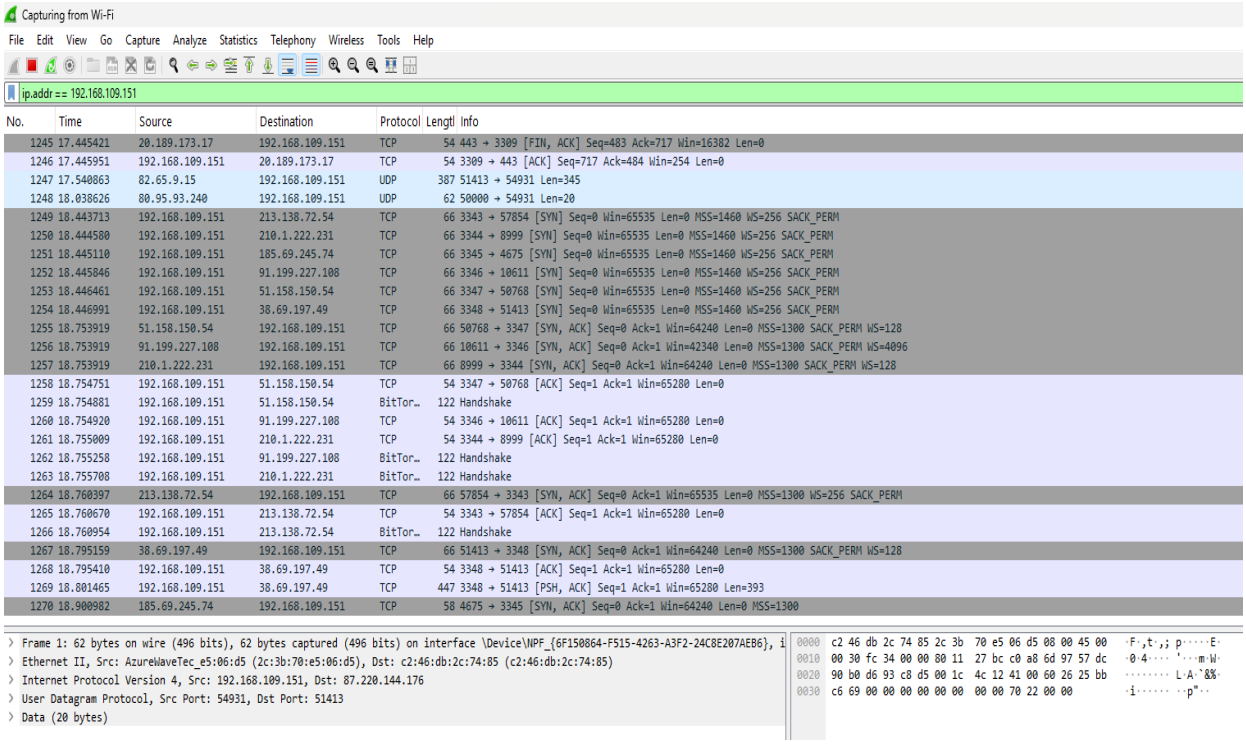
3.Run: nmap -sS 192.168.1.0/24 to perform TCP SYN scan:



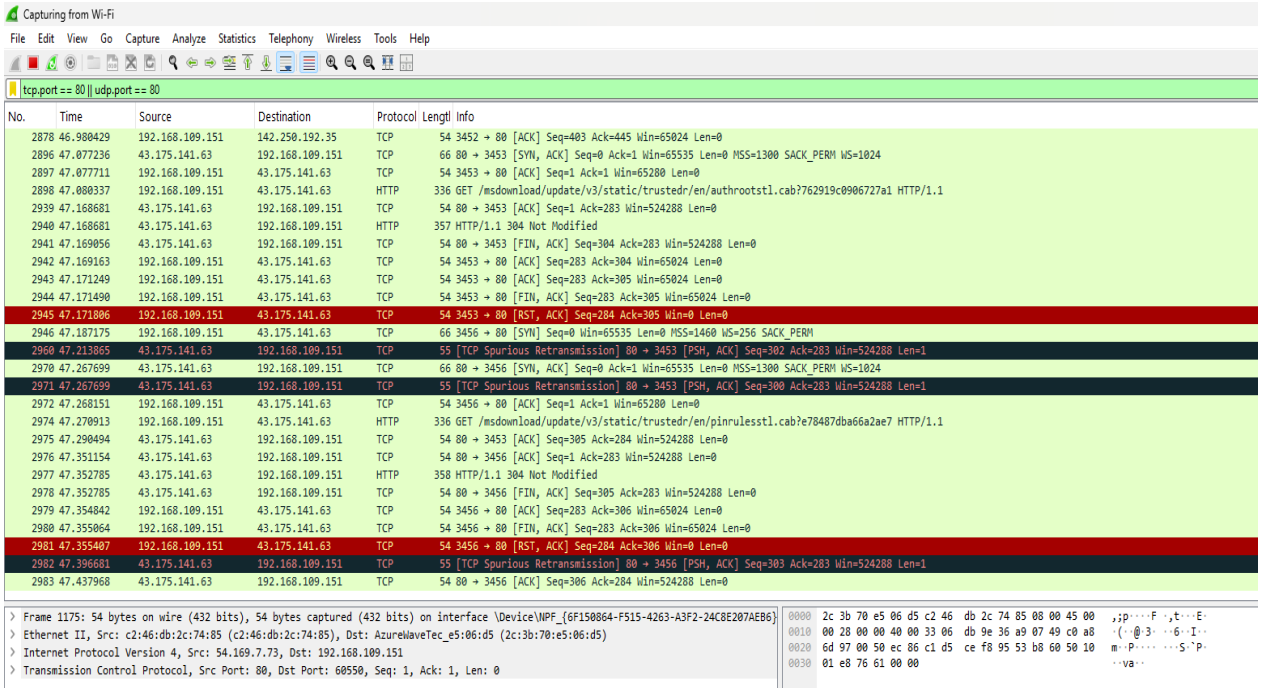
4. IP addresses and open ports found:

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

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



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



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: