🧠 Lecture 19 – Network Scanning,N-Map,WireShark

🔍 1. What is Network Scanning?

🔹 Definition:

Network Scanning is the process of **identifying active (live) devices, open ports, and running services** on a network.

It helps a security analyst or ethical hacker understand:

- Which hosts (computers) are **alive** on the network.
- Which **ports** are **open, closed, or filtered**.
- What **operating system** and **services** are running on those hosts.
- Whether any **vulnerabilities** exist that can be exploited.

🔹 Purpose of Network Scanning:

1. **Identify Live Hosts** → Devices that are currently online and communicating.
2. **Discover Open Ports** → Find which ports accept incoming connections.
3. **Detect Running Services** → Check what application (HTTP, FTP, SSH, etc.) runs on each port.
4. **Find OS and Network Info** → Learn about the target's operating system and version.
5. **Assess Vulnerabilities** → Spot possible weaknesses in the network.

🔹 Real-Life Example:

When you connect your **Kali Linux** machine to a network and want to see which systems (like Windows or servers) are online, you'll perform a **network scan**.

If the **firewall is enabled** on a system (like a Windows Server), the scan may **not detect** that system — because the **firewall blocks incoming packets**.

👉 Therefore, to scan that system, you might need to **disable its firewall** temporarily in a controlled lab environment.

⚙️ 2. Protocols Used in Scanning

🔸 TCP (Transmission Control Protocol)

- **Connection-oriented** protocol.
- Uses the **3-Way Handshake** (SYN → SYN/ACK → ACK).
- Reliable communication (guarantees data delivery).
- Used for services like **HTTP, FTP, SSH, SMTP, Telnet**.

🔸 UDP (User Datagram Protocol)

- **Connectionless** protocol.
- No handshake process.
- Faster but **unreliable** (no confirmation of delivery).
- Used for services like **DNS, DHCP, SNMP, VoIP**.

⚙️ 3. The 3-Way Handshake (TCP Connection)

This is how TCP establishes a connection between **client** and **server**.

Step	Direction	Flag	Description
1	Client → Server	SYN	Client requests to connect.
2	Server → Client	SYN-ACK	Server acknowledges and agrees to connect.
3	Client → Server	ACK	Client confirms connection established.

✅ After these 3 steps, the connection is **established**.
If any step fails, the connection won't be made.

⚙️ 4. What is Nmap? (Network Mapper)

🔹 Definition:

Nmap (Network Mapper) is the world's most widely used **open-source network scanning tool**.
It is used to:

- Discover live hosts.
- Identify open and closed ports.
- Detect the operating system (OS) and services.
- Perform vulnerability detection.

🔹 Why Nmap is Important:

- Helps system administrators **audit network security**.
- Detect unauthorized devices on the network.
- Helps ethical hackers **map network topology** and **find weak points**.
- Used in **penetration testing**, **network inventory**, and **firewall testing**.

⚙️ 5. Nmap Basic Scanning Commands

🔸 Check Live Hosts

nmap -sn <IP address>

🔹 Example: nmap -sn 192.168.1.0/24

- Scans the whole subnet to check which systems are online (Ping Scan).
- It sends ICMP echo requests.
- If the device replies → It's "live".

🔸 **Bypass Firewall or Disable Ping Scan**

nmap <IP address> -Pn

🔹 Use this when the **firewall blocks ICMP (ping)** requests.

- Forces Nmap to treat all hosts as online and continue scanning.

🔸 **ARP Scan (Local Network Only)**

nmap -sn <IP address> -PR

🔹 Uses **ARP requests** to find live hosts.

- Works only on the **same local network**.
- Faster and more reliable than ping scans.

🔸 **Traceroute Scan**

nmap -sn --traceroute <domain>

🔹 Shows the **path packets take** from your system to the target host.

- Helps identify **network hops** and **latency** at each point.

Example:

nmap -sn --traceroute codingseekho.in

🔸 **DNS Resolution**

nmap codingseekho.in --dns-servers 1.1.1.1

🔹 Uses a specific **DNS server (Cloudflare 1.1.1.1)** to resolve hostnames faster and more securely.

- Useful when the default DNS is slow or blocked.

🔸 **Traceroute + DNS Together**

nmap --traceroute codingseekho.in --dns-servers 1.1.1.1

🔹 Performs a **combined test** for both network route and DNS resolution speed.

⚙️ **6. Port Scanning with Nmap**

🔹 **Port States in Nmap:**

State	Meaning
Open	Application is accepting connections on this port.
Closed	No service running on this port, but it's reachable.
Filtered	Firewall or security device is blocking access.
Unfiltered	Nmap cannot determine if it's open or closed.
Open/Filtered	Nmap can't decide because no response came back.
Closed/Filtered	Could be either — response unclear.

🔸 **Scan a Specific Port**

nmap -p 80 <IP>

- Scans **port 80** (HTTP).
- Shows its **state** (open/closed/filtered) and the **service**.

🔸 **Scan FTP Port**

nmap -p 21 <IP>

- Scans **port 21** (FTP).
- Checks if the FTP service is running.

🔸 Scan Common Ports (1–1024)

nmap -p 1-1024 <IP>

- Scans all **well-known ports** (common services).

🔸 Scan All Ports

nmap -p- <IP>

- Scans **all 65,535 ports** on the target machine.
- Takes longer but gives **complete port visibility**.

🔸 TCP Scan

nmap -sT <IP>

- Performs a **TCP Connect Scan** using the full 3-way handshake.
- Reliable but **slower** and **more detectable**.

🔸 UDP Scan

nmap -sU <IP>

- Scans for **UDP services** (DNS, SNMP, DHCP).
- Slower and less reliable because UDP gives no response unless open.

🔸 OS Detection Scan

nmap -O <IP>

- Detects **Operating System**, **MAC address**, and **open ports**.
- Helps identify what kind of device (Windows, Linux, Router) you're scanning.

🔸 **Aggressive Scan (Use with Caution)**

nmap -A <IP>

- Performs a **deep scan**:
  - OS detection
  - Version detection
  - Script scanning
  - Traceroute
- ⚠️ **Don't use this on public servers** — it's noisy and can get you blocked or reported.

⚙️ **7. MAC Address Spoofing & Source Port Scanning**

🔸 **Spoof MAC Address**

nmap --spoof-mac Dell -p 135 <IP>

🔹 Purpose:

- Spoofs (fakes) your **MAC address** to look like a **Dell device**.
- Used to **hide your real hardware identity** during scans.
- Helps bypass **MAC-based filtering** on some networks.

🔸 **Use Specific Source Port**

nmap --source-port 53 -p 21 <IP>

🔹 Purpose:

- Sends packets from **port 53 (DNS)** instead of a random source port.
- Helps **evade firewalls or IDS** that trust traffic from specific ports (like DNS or HTTP).
- Example: Pretending your traffic is normal DNS communication.

🧠 8. Wireshark Overview

🔹 Definition:

Wireshark is a powerful **network protocol analyzer** that captures and displays real-time data packets traveling through your network interface.

It shows:

- **Time**
- **Source**
- **Destination**
- **Protocol**
- **Length**
- **Information (details)**

🔹 How to Run Wireshark:

sudo wireshark

- sudo gives root privileges.
- Opens the GUI-based packet capture tool.

🔹 Purpose:

- Monitor **real-time network traffic**.
- Analyze **TCP handshakes**, **HTTP requests**, and **DNS queries**.
- Verify whether a **port is open** (look for SYN → SYN/ACK → ACK).
- Identify suspicious traffic or malware communication.

🔹 Example:

If Wireshark shows a **SYN-ACK** reply from a port, it means that **port is open** and responding.

⚙️ 9. Additional Notes

- **Ports Range:**
    - There are **65,535 ports** in total.
    - Common examples:
        - 21 – FTP
        - 22 – SSH
        - 23 – Telnet
        - 25 – SMTP
        - 53 – DNS
        - 80 – HTTP
        - 443 – HTTPS
- **Scanning All Ports:**
- nmap -p- <IP>

Scans all ports (1–65535) to find every open service.

- **Legal Reminder:**
  You must have **permission** before scanning any public domain or IP.
  Unauthorized scanning can be treated as a **cybercrime**.

🧩 10. Summary Table

Nmap Command	Purpose
nmap -sn <IP>	Check live hosts (Ping Scan)
nmap -Pn <IP>	Skip ping – bypass firewall
nmap -sn -PR <IP>	ARP scan in LAN
nmap -sn --traceroute <domain>	Trace path to host
nmap <domain> --dns-servers 1.1.1.1	Custom DNS resolution

Nmap Command	Purpose
nmap -p 80 <IP>	Scan HTTP port
nmap -p 1-1024 <IP>	Scan common ports
nmap -p- <IP>	Scan all ports
nmap -sT <IP>	TCP connect scan
nmap -sU <IP>	UDP scan
nmap -O <IP>	OS detection
nmap -A <IP>	Aggressive scan
nmap --spoof-mac Dell -p 135 <IP>	MAC address spoofing
nmap --source-port 53 -p 21 <IP>	Source port manipulation

✅ **Final Takeaway:**

- **Nmap** is your primary tool for **reconnaissance and vulnerability detection**.
- Always start with **basic scans**, then move to **service/OS detection**.
- **Wireshark** is used to **analyze and verify** your scan results.
- Be ethical and perform scans **only in authorized labs or networks**