🖥️NETWORKING

🔷 1. What is Networking? (Expanded)

Networking is the art of **connecting computers and devices** to communicate and share resources like **data, files, internet, and printers**. It's the **digital backbone** of everything from WhatsApp messages to YouTube videos.

🧠 Why Should a Hacker Learn Networking First?

Imagine trying to break into a system, but you don't even know how data flows. Networking teaches:

- How systems are structured
- Where security is applied
- How vulnerabilities can be found

🖧 Real World Example:

- When you open Instagram, your phone contacts a **web server**.
- The server sends back **encrypted data** using **HTTPS**.
- Your phone **receives, decrypts, and displays** the content.
- All this involves networking: DNS, TCP, SSL, routing, etc.

> 💡 Without networking, there's no internet. No internet = nothing to hack.

🔧 2. KEY COMPONENTS OF NETWORKING (FULLY EXPANDED)

Understanding these components is like learning the **parts of a house before you break in ethically** — doors, windows, locks, alarms. Here, we'll break down the **hardware, software, and protocol-based components** that make up any network.

✅ 1. IP Address (Internet Protocol Address)

🔍 What It Is:

An **IP address** is a **unique ID assigned to each device** connected to a network. It's like the **home address** of a device — so data knows where to go.

🧠 Types:

- **IPv4** – Most common (e.g., `192.168.1.100`)
- **IPv6** – Newer, more addresses (e.g., `2001:0db8:85a3:0000:0000:8a2e:0370:7334`)

🧪 Dynamic vs Static IP:

- **Static IP**: Manually set, doesn't change. Used for servers.
- **Dynamic IP**: Assigned by DHCP (Dynamic Host Configuration Protocol). It changes.

🛡️ Hacker Usage:

- Scan for **active IPs** in a range (network scanning)
- Find **misconfigured or open IPs** to exploit
- Target **public IPs** exposed online using **tools like Shodan**

✅ 2. MAC Address (Media Access Control)

🔍 What It Is:

A **MAC address** is a **hardware identifier** burned into your device's network card.
Looks like: `00:0A:E6:3E:FD:E1`

🔐 Why It's Unique:

Every network device — laptop, router, phone — has a **globally unique MAC**.

🧠 Example:

- **MAC of Laptop**: `A4:CF:12:44:DE:2A`
- **MAC of Smartphone**: `B7:33:FF:91:29:8D`

🛡️ Hacker Usage:

- **MAC Spoofing**: Change MAC to bypass Wi-Fi filters
- **Identify Devices** on a LAN using tools like `arp -a`
- Used in **man-in-the-middle (MITM)** attacks on local networks

---

✅ 3. Router

🔍 What It Is:

A **router** connects **multiple networks** together, typically your local network (LAN) to the **Internet (WAN)**.

> Think of a router as a post office: it forwards your data to the right address.

🛠️ Functions:

- Assigns IP addresses (via **DHCP**)
- Connects LAN to the internet (via **NAT**)
- Applies basic **firewall rules**
- Often acts as a **gateway** to external traffic

🛡️ Hacker Usage:

- **Default credentials** (`admin:admin`) still used on many routers
- **Router exploits** like:
  - Remote Code Execution (RCE)
  - DNS Hijacking
- **Router fingerprinting** using tools like **Nmap** or **RouterSploit**

✅ 4. Switch

🔍 What It Is:

A **switch** connects multiple devices **within the same network (LAN)**. It forwards data **only to the intended device** using MAC addresses.

> Switches are like a smart delivery person who gives the package only to the right door.

🛠️ Key Features:

- Operates at **Layer 2 (Data Link Layer)** of OSI
- Maintains a **MAC address table**
- Helps reduce network collisions

🛡️ Hacker Usage:

- If **port mirroring** is enabled, hackers can sniff traffic
- **ARP spoofing** can be used to poison MAC tables
- Used to launch **MITM attacks** inside a LAN

✅ 5. Firewall

🔍 What It Is:

A **firewall** is a **security filter** that allows or blocks traffic based on pre-set rules.

> Think of it as a digital security guard that decides who enters or exits.

🛠️ Types of Firewalls:

- **Software Firewall** (e.g., Windows Defender Firewall)
- **Hardware Firewall** (e.g., Cisco ASA, FortiGate)
- **Next-Gen Firewalls** (NGFWs) — inspect applications & behavior

🧠 Rule Examples:

- Allow only **port 443 (HTTPS)** to the internet
- Block all **outbound FTP traffic**
- Drop packets from a **blacklisted IP**

🛡️ Hacker Usage:

- Fingerprinting firewalls to identify vendor (e.g., Palo Alto, Cisco)
- Finding **misconfigured rules** (e.g., port 22 open to the world)
- Use **evasion techniques** to bypass firewalls (e.g., fragmenting payloads)

✅ 6. Access Point (AP)

🔍 What It Is:

A wireless **Access Point** allows Wi-Fi devices to connect to a **wired network**.

> Think of it as a Wi-Fi hub for your home, office, or cafe.

🛠️ Features:

- Supports wireless standards: **802.11 a/b/g/n/ac/ax**

- Often built into **routers**
- Can be **open or encrypted** (WEP, WPA, WPA2, WPA3)

🛡️ Hacker Usage:

- **Wi-Fi sniffing** with tools like **Kismet, Aircrack-ng**
- Cracking **WEP/WPA passwords**
- Creating **fake APs** to trap users (Evil Twin attack)

✅ 7. Server

🔍 What It Is:

A **server** is a computer that provides services or resources to other devices (clients) in a network.

> Web server, mail server, database server — they all serve content or handle requests.

🔗 Examples:

- **Web Server**: Hosts websites (Apache, Nginx)
- **Database Server**: Stores data (MySQL, MongoDB)
- **DNS Server**: Resolves domain names
- **File Server**: Stores files on LAN

🛡️ Hacker Usage:

- **Web server exploits** (e.g., RFI, LFI, XSS)
- **Database extraction** (via SQL Injection)
- **Privilege escalation** on misconfigured or outdated servers

---

✅ 8. Client

🔍 What It Is:

A **client** is any device (e.g., laptop, phone) that requests services from a server.

> Your browser is a client when visiting a website.

🧠 Clients Run:

- Web browsers (Chrome, Firefox)
- Email clients (Outlook, Thunderbird)
- VPN clients
- Remote desktop clients

🛡️ Hacker Usage:

- **Social engineering** attacks target clients (phishing)
- Exploiting **client-side vulnerabilities** (e.g., Flash, JavaScript)
- Malware delivery via fake client apps

⚠️ BONUS: NAT & DHCP

🔄 NAT (Network Address Translation):

- Translates **private IPs** (like `192.168.1.10`) to a **public IP** when going online.
- Protects internal network structure.

> Hackers might try to exploit NAT routers to access internal devices.

🔄 DHCP (Dynamic Host Configuration Protocol):

- Automatically assigns IP addresses to devices in a network.
- Removes the need to manually set IPs.

> DHCP starvation attacks can crash a network by exhausting all IP addresses.

✅ Summary Table

Component	Main Use	Hacker Angle
IP Address	Identify devices	Scanning, targeting
MAC Address	Identify hardware	Spoofing, MITM
Router	Connect networks	Exploitation, DNS hijack
Switch	Connect devices	MITM, sniffing
Firewall	Block unwanted traffic	Evasion, fingerprinting

Access Point	Wireless connectivity	Cracking, Evil Twin
Server	Provide resources	Exploits, lateral movement
Client	Request resources	Malware, phishing

🔷 3. Types of Networks (Expanded)

Understanding network types helps you choose the right tools and **attack vectors**.

🏠 LAN (Local Area Network)

- Covers homes, offices, schools.
- Devices are **physically close** (10m to 100m).
- Uses **private IPs** (e.g., `192.168.x.x`).

Hacker Target:

- **Wi-Fi attacks**, **ARP spoofing**, **packet sniffing** (e.g., stealing passwords using Wireshark).

🌐 WAN (Wide Area Network)

- Connects multiple LANs across cities/countries.
- The Internet is the largest WAN.
- Uses **public IPs** for access.

Hacker Target:

- Scanning large IP ranges (e.g., using Nmap + Shodan)
- Finding **exposed ports**, **services**, **IoT devices**

📱 PAN (Personal Area Network)

- Range of 1–10 meters.
- Devices like phones, smartwatches, Bluetooth headphones.

Hacker Target:

- Bluetooth sniffing (e.g., **BlueBorne** attack), **MITM on tethered devices**

🌆 MAN (Metropolitan Area Network)

- Covers city or campus.
- Often used by ISPs, universities, or government.

Hacker Target:

- Infrastructure vulnerabilities (e.g., exploiting shared routers or switches in a building)

🛡️ VPN (Virtual Private Network)

- Creates an **encrypted tunnel** between client and server.
- Protects your IP and data from being seen.

Hacker Target:

- Weak VPN implementations, credential stuffing attacks.

🔷 4. Ports & Protocols (Expanded)

Ports = **entry and exit points** for network traffic.

Protocols = **rules** for communication.

Port	Protocol	Use	Hacker Threat
21	FTP	File Transfer	Unencrypted FTP can be sniffed
22	SSH	Secure Shell (remote login)	Brute-force attacks, misconfigurations
23	Telnet	Remote login (insecure)	Common target for IoT hacks
25	SMTP	Email sending	Spamming or email spoofing
53	DNS	Domain resolution	DNS poisoning or tunneling
80	HTTP	Website (insecure)	MITM, injections
443	HTTPS	Secure websites	SSL stripping, cert spoofing
3306	MySQL	Database service	SQL injection, DB hacking
3389	RDP	Remote Desktop	Exploiting RDP flaws

> 🧠 Ports are doors. Scanning them reveals services that can be exploited.

TCP vs UDP (Analogy)

Protocol	Analogy	Hacker Use
TCP	Sending a **registered post** – slow but confirms delivery	Used for **web**, **FTP**, **SSH**
UDP	Sending a **postcard** – fast, no delivery confirmation	Used in **DDoS attacks**, **VoIP exploits**

💡 Lesson: OSI Model (Open Systems Interconnection)

🔷 What is the OSI Model?

The **OSI Model** (Open Systems Interconnection) is a **conceptual framework** that describes how data moves through a network in **seven layers**, from the physical hardware to the application the user sees.

> Think of it as a 7-layer sandwich—each layer adds or processes something before passing it to the next one.

📊 The 7 Layers of the OSI Model

Layer	Name	Function	Protocols/Devices	Hacker Perspective
7	Application	End-user interface	HTTP, DNS, FTP	Social Engineering, Phishing
6	Presentation	Data translation/encryption	SSL/TLS, JPEG, MP3	SSL Stripping, Encoding attacks
5	Session	Start/manage/end communication	NetBIOS, RPC, SQL Sessions	Session Hijacking
4	Transport	Reliable delivery (port management)	TCP, UDP	Port Scanning, DoS
3	Network	Routing data (logical addressing)	IP, ICMP	IP Spoofing, DDoS
2	Data Link	MAC addressing, framing	ARP, Switches	ARP Poisoning, MITM
1	Physical	Actual hardware transmission	Ethernet, Wi-Fi	Sniffing, Jamming

🔷 Layer 1 – Physical Layer

🧠 Role:

Deals with the **physical medium** — wires, signals, cables.

📦 Real-World:

- Ethernet cables

- Wi-Fi radio signals
- Fiber optics
- Hubs

🛠️ Protocols:

None (pure hardware)

👨‍💻 Hacker Usage:

- **Wiretapping**, **packet sniffing** with hardware
- **Wi-Fi jamming** using tools like `aireplay-ng`
- **Disrupt physical access** to networks

🔷 Layer 2 – Data Link Layer

🧠 Role:

Transmits data between two nodes on the same network using **MAC addresses**.

📦 Real-World:

- Switches
- Network cards
- ARP

🛠️ Protocols:

- Ethernet
- ARP (Address Resolution Protocol)
- PPP

👨‍💻 Hacker Usage:

- **ARP Spoofing / Poisoning** for MITM
- MAC flooding attacks
- Use tools like `ettercap`, `arpspoof`

🔷 Layer 3 – Network Layer

🧠 Role:

Handles **routing** and logical addressing using **IP addresses**.

📦 Real-World:

- Routers
- IP Packets

🛠️ Protocols:

- IP (IPv4, IPv6)
- ICMP (used in ping)
- OSPF, BGP (routing)

👨‍💻 Hacker Usage:

- **IP Spoofing**
- **Ping of Death** (ICMP flood)
- **Network scanning** with Nmap

🔷 Layer 4 – Transport Layer

🧠 Role:

Ensures **reliable or fast** delivery of data using **ports**.

📦 Real-World:

- Ports: 80 (HTTP), 443 (HTTPS), 22 (SSH)

🛠️ Protocols:

- TCP (reliable, 3-way handshake)
- UDP (fast, no guarantee)

👨‍💻 Hacker Usage:

- **Port Scanning** (e.g., with Nmap, Masscan)
- **TCP SYN Flood** (Denial of Service)
- **UDP Floods**

🔷 Layer 5 – Session Layer

🧠 Role:

Manages and **controls sessions** (connections) between devices.

📦 Real-World:

- Remote logins
- Database sessions

🛠️ Protocols:

- NetBIOS
- PPTP
- RPC
- SQL Sessions

👨‍💻 Hacker Usage:

- **Session Hijacking**
- Exploit **long-lived sessions** to impersonate users
- Token theft

🔷 Layer 6 – Presentation Layer

🧠 Role:

Handles **data formatting**, **encryption**, and **compression**.

📦 Real-World:

- SSL/TLS (data encryption)
- File formats: PDF, JPEG, MP3

🛠️ Protocols:

- SSL/TLS
- ASCII, JPEG, MPEG

👨‍💻 Hacker Usage:

- **SSL Stripping** (convert HTTPS to HTTP)
- Encoding payloads (Base64, Hex) to bypass filters
- TLS downgrade attacks

🔷 Layer 7 – Application Layer

🧠 Role:

The layer that users interact with — web browsers, email, etc.

📦 Real-World:

- Google Chrome, Outlook, Zoom

🛠️ Protocols:

- HTTP, HTTPS
- FTP
- DNS
- SMTP

👨‍💻 Hacker Usage:

- **Phishing**
- **DNS Spoofing**
- **XSS, SQL Injection**
- Command and control (C2) servers

🔑 Simple Analogy: Sending a Parcel

Layer	Analogy
7	You write a letter (App)
6	You translate it to the recipient's language (Presentation)
5	You start a call to let them know it's coming (Session)
4	You pack it into a box, add tracking number (Transport)
3	You put the address label on it (Network)
2	The postman organizes delivery by name & apartment (Data Link)
1	The delivery truck physically takes it to the house (Physical)

🛠️ Tools for OSI Understanding in Hacking:

Layer	Tool
1	Wireshark (Packet Sniffing), Aircrack-ng
2	Arpspoof, Ettercap
3	Nmap, Hping
4	Netcat, TCPdump

5	Burp Suite, Session Hijacker
6	SSLStrip, Wireshark
7	OWASP ZAP, Metasploit, sqlmap

✅ Summary (Mnemonic)

Mnemonic to remember OSI layers (Top to Bottom):

🔷 **"All People Seem To Need Data Processing"**

Layer	Mnemonic Word
7	Application – All
6	Presentation – People
5	Session – Seem
4	Transport – To
3	Network – Need
2	Data Link – Data
1	Physical – Processing

🔚 Summary: Why This Depth Maters

Topic	Hacker's Reason
Networking basics	Foundation of **every attack**
Devices/components	Know the **attack surface**
Network types	Know **what's vulnerable** in each context
Ports & Protocols	Reveal **entry points**
OSI Model	Shows **where attacks happen**