OSI Model

The **OSI (Open Systems Interconnection) Model** is a conceptual framework that describes how data moves through a network in **7 layers**:

1. **Physical** – Hardware, cables, signals
2. **Data Link** – MAC addresses, switches
3. **Network** – IP addresses, routing
4. **Transport** – TCP/UDP, ports
5. **Session** – Connections between apps
6. **Presentation** – Data formatting/encryption
7. **Application** – User-facing services (HTTP, DNS)

Why It Matters: Helps you understand where issues or attacks occur in the network stack.

TCP/IP

The **TCP/IP model** is a simplified version of OSI used in real-world networking. It has **4 layers**:

1. **Link** – Physical and data link
2. **Internet** – IP addressing and routing
3. **Transport** – TCP/UDP
4. **Application** – Protocols like HTTP, DNS, FTP

Why It Matters: It's the foundation of how the internet works.

DNS (Domain Name System)

DNS translates **human-readable domain names** (like google.com) into **IP addresses** (like 142.250.72.14).

Why It Matters: Attackers often abuse DNS for data exfiltration or command-and-control (C2) channels.

HTTP/HTTPS

- **HTTP (HyperText Transfer Protocol)** – Used for web communication.
- **HTTPS** – Secure version using encryption (TLS/SSL).

Why It Matters: Many attacks (like phishing or data theft) happen over HTTP/S. Understanding headers and requests helps in detection.

VPNs (Virtual Private Networks)

VPNs create **encrypted tunnels** between your device and a remote server, hiding your IP and securing your traffic.

Why It Matters: Used for privacy, but attackers may use VPNs to hide their origin.

Firewalls

Firewalls monitor and control **incoming/outgoing traffic** based on security rules.

Network firewalls – Protect entire networks

Host-based firewalls – Protect individual devices

Why It Matters: They're your first line of defense against unauthorized access.

Wireshark

Wireshark is a **network protocol analyzer** that lets you capture and inspect packets in real time.

What You Can Do:

- See TCP handshakes
- Analyze DNS queries
- Detect suspicious HTTP requests
- Spot malformed or malicious packets

Why It Matters: It's a must-have tool for network troubleshooting and threat hunting.