📡 OSI MODEL CHEAT SHEET (Definitions + Attacks)

🔹 Layer 7 – Application Layer

Role:
Provides network services directly to end-user applications and defines how applications communicate over a network.

Protocols: HTTP, FTP, SMTP, DNS

Attacks:

- **Buffer Overflow:** Excess input overwrites memory to execute unintended code
- **XSS:** Malicious scripts injected into trusted web applications
- **DDoS:** Multiple systems flood an application to make it unavailable

---

🔹 Layer 6 – Presentation Layer

Role:
Handles data format, encoding, compression, and encryption.

Attacks:

- **Unicode Vulnerability:** Exploits encoding issues to bypass security checks
- **SSL Strip:** Downgrades HTTPS to HTTP to intercept sensitive data

---

🔹 Layer 5 – Session Layer

Role:
Establishes, manages, and terminates communication sessions.

Attacks:

- **Session Hijacking:** Attacker takes control of an active session
- **DNS Poisoning:** Corrupts DNS cache to redirect users to malicious sites

---

🔹 Layer 4 – Transport Layer

Role:
Provides end-to-end data delivery using ports, flow control, and error handling.

Protocols: TCP, UDP

Attacks:

- **SYN Flood:** Exhausts server resources with half-open TCP connections
- **Invalid TCP Flags:** Uses malformed TCP packets to crash systems
- **UDP Flood:** Floods target with UDP packets to exhaust bandwidth

---

🔹 Layer 3 – Network Layer

Role:
Handles logical addressing and routing of packets.

Protocols: IP, ICMP

Attacks:

- **ICMP Flood:** Overwhelms system with ICMP packets
- **OS Fingerprinting:** Identifies OS via network response analysis
- **IP Spoofing:** Fakes source IP address to impersonate a device
- **Routing Table Poisoning:** Injects false routing information

---

🔹 Layer 2 – Data Link Layer

Role:
Provides MAC addressing, framing, and error detection.

Technologies: Ethernet, ARP, Switches

Attacks:

- **Sniffing:** Passive capture of network traffic
- **ARP Cache Poisoning:** Links attacker's MAC to victim's IP
- **MACOF:** Floods switch with fake MACs to disable switching

---

🔹 Layer 1 – Physical Layer

Role:
Transmits raw bits over physical media.

Attacks:

- **Cutting Cables:** Physical disruption of network connectivity

- **Jamming:** Interferes with wireless signals
- **Keystroke Logging:** Records keyboard input to steal credentials

---