🧷 OSI Model – Security Quick Card

Layer 7 – Application

What it does: User-facing services (HTTP, DNS, SMTP, RDP).
Common vulns:

- Injection (SQLi, LDAPi, OS command)
- XSS / CSRF
- Directory traversal
- Insecure deserialization
- Weak authentication
  Security controls: WAF, input validation, MFA, secure coding, patching.

Layer 6 – Presentation

What it does: Encoding/decoding, encryption (TLS).
Common vulns:

- Weak encryption (TLS 1.0/1.1, SSL)
- Improper certificate validation
  Security controls: Disable weak ciphers, enforce TLS 1.2/1.3, cert pinning.

Layer 5 – Session

What it does: Handles sessions, connections.
Common vulns:

- Session hijacking
- Session fixation
- Poor timeout controls
  Security controls: Secure cookies, short session tokens, rotate tokens, TLS.

Layer 4 – Transport

What it does: TCP/UDP ports, segmentation, reliability.
Common vulns:

- SYN floods (DoS)
- UDP amplification attacks
- Port scanning / enumeration
  Security controls: Firewalls, rate limiting, TCP SYN cookies, IDS/IPS.

Layer 3 – Network

What it does: IP addresses, routing.
Common vulns:

- IP spoofing

- Routing attacks
- ICMP flooding / Smurf attacks
  Security controls: ACLs, anti-spoofing filters, router hardening.

Layer 2 – Data Link

What it does: MAC addresses, switching.
Common vulns:

- MAC spoofing
- ARP poisoning (Man-in-the-Middle)
- VLAN hopping
  Security controls: Dynamic ARP inspection, port security, VLAN segmentation.

Layer 1 – Physical

What it does: Cables, WiFi signals, hardware.
Common vulns:

- Physical tampering
- Signal jamming
- Cable tapping
  Security controls: Locks, CCTV, biometric access, EMI shielding.

🛡️ **High-Yield Exam & SOC Tips**

- **Most cyber-attacks start or end at Layer 7 (apps).**
- **MITM = Usually Layer 2 (ARP spoofing) or Layer 3 (IP spoofing).**
- **DDoS = Primarily Layer 3 & 4.**
- **WAF protects Layer 7, Firewalls protect Layer 3/4.**
- **TLS operates at Layer 6 but *implemented* at Layer 4 (TCP handshake extended).**
- **Industrial attacks (e.g., cable cut, jamming) = Layer 1.**