OSI Model Quick Reference Guide

For Ethical Hackers

The 7 Layers (Bottom to Top)

1. Physical Layer

- **Function:** Physical connections, cables, signals
- **Examples:** Ethernet cables, Wi-Fi signals, fiber optic
- **Security Risks:** Physical tampering, cable tapping
- **Common Ports:** N/A (hardware level)

2. Data Link Layer

- **Function:** Frame data, error detection within local network
- **Examples:** MAC addresses, Ethernet frames, switches
- **Security Risks:** MAC spoofing, ARP poisoning
- **Protocols:** ARP, PPP

3. Network Layer

- **Function:** Routing between networks, logical addressing
- **Examples:** IP addresses, routers, packet forwarding
- **Security Risks:** IP spoofing, routing attacks
- **Protocols:** IP, ICMP, OSPF

4. Transport Layer

- **Function:** Reliable data delivery, flow control
- **Examples:** Port numbers, data segments
- **Security Risks:** Port scanning, SYN flooding
- **Protocols:** TCP (reliable), UDP (fast)
- **Common Ports:** 80 (HTTP), 443 (HTTPS), 22 (SSH), 21 (FTP)

5. Session Layer

- **Function:** Manage sessions between applications
- **Examples:** Login sessions, API connections
- **Security Risks:** Session hijacking, session fixation
- **Protocols:** NetBIOS, RPC, PPTP

6. Presentation Layer

- **Function:** Data encryption, compression, formatting
- **Examples:** SSL/TLS encryption, JPEG, MPEG
- **Security Risks:** Weak encryption, data exposure
- **Protocols:** SSL/TLS, MIME

7. Application Layer

- **Function:** User interface, network services
- **Examples:** Web browsers, email clients, file transfer
- **Security Risks:** Application vulnerabilities, malware
- **Protocols:** HTTP/HTTPS, FTP, SMTP, DNS, DHCP
- **Common Ports:** 25 (SMTP), 53 (DNS), 110 (POP3)

Memory Trick

"Please Do Not Throw Sausage Pizza Away"

- **P**hysical
- **D**ata Link
- **N**etwork
- **T**ransport
- **S**ession
- **P**resentation
- **A**pplication

Key Protocol Summary

Protocol	Layer	Port	Purpose
HTTP	Application	80	Web browsing
HTTPS	Application	443	Secure web browsing
FTP	Application	21	File transfer
SSH	Application	22	Secure remote access
DNS	Application	53	Domain name resolution
SMTP	Application	25	Email sending
TCP	Transport	N/A	Reliable delivery
UDP	Transport	N/A	Fast delivery
IP	Network	N/A	Addressing & routing

Ethical Hacker Focus

Bottom Layers (1-3): Infrastructure attacks

- Physical access, network mapping, routing manipulation

Middle Layers (4-5): Connection attacks

- Port scanning, session management, traffic analysis

Top Layers (6-7): Application attacks

- Web vulnerabilities, encryption weaknesses, service exploitation

---

Quick Analysis Framework

When analyzing any network issue or attack:

1. **Identify the layer** involved
2. **Check common vulnerabilities** for that layer
3. **Use appropriate tools** for that layer
4. **Apply security measures** specific to that layer

This systematic approach helps you think like both an attacker and defender.