

OSI Model by Morphine

The OSI Model (Open Systems Interconnection) has 7 layers.

It explains how data moves from one device to another and where attack happens.

✂ OSI Model : 1 Line Summary

| | |
|---------------------|----------------------------------|
| Application | What the user sees (Web/FTP/SSH) |
| Presentation | Encryption/formatting |
| Session | Session control & auth |
| Transport | Ports, TCP/UDP, connections |
| Network | IP Address, Routing |
| Data Link | MAC, ARP, VLANs |
| Physical | Cables, Signals, Hardware |

✂ Tools

| Tool | Primary Layer | Purpose |
|-------------|---------------|------------------------------|
| Wireshark | L2 - L7 | Packet capture + analysis |
| Nmap | L3 - L4 | Scanning, reconnaissance |
| Netcat | L4 | Manual TCP/UDP communication |
| Aircrack-ng | L1 - L2 | Wireless cracking |
| Burp Suite | L5 - L7 | Web hacking |
| SSLStrip | L6 | HTTPS downgrade |
| Scapy | L2 - L4 | Custom packets |

Layer 7 : Application Layer

Final interface for the user. App use it to send or receive data.

Examples :

- HTTP/HTTPS (Websites)
- DNS (Domain Lookup)
- SMTP (Email)
- FTP (File transfer)
- SSH (remote login)

Cyber attacks on this layer :

- SQL Injection
- Cross-site scripting (XSS)
- CSRF
- Directory Traversal
- Email spoofing
- DNS Poisoning (Partly L7 and L3)

Tools :

- Burp Suite
- OWASP ZAP
- SQLMap
- Nikto
- Gobuster
- Dirsearch
- Wfuzz

Layer 6 : Presentation Layer

Formats and encrypts data before sending.

Functions :

- Encryption (SSL/TLS)
- Compression
- Encoding (ASCII/UTF-8)

Cyber Attacks :

- SSL Stripping
- Weak encryption attacks
- Man-in-the-middle attack (Breaking TLS)

Tools :

- OpenSSL
- SSLStrip
- mitmproxy
- Burp Suite (intercepts HTTPS traffic)

Layer 5 : Session Layer

Creates, maintains, ends communication between devices.

Think : "Session Management"

Examples :

- Online login sessions.
- API sessions.
- Web sessions (Cookies / tokens)

Cyber Attacks :

- Session hijacking
- Session fixation
- Cookie stealing
- Replaying sessions tokens

Tools :

- Burp Suite (session token manipulation)
- OWASP ZAP
- Wireshark (cookie hunting)
- Bettercap

Layer 4 : Transport Layer

Handles end-to-end data transfers.

Protocols :

- TCP (Reliable)
- UD (Fast but not guaranteed)

TCP 3-Way Handshake :

SYN → SYNK/ACK → ACK

Cyber Attacks :

- SYN Flood (DoS)
- UDP Flood
- TCP Reset Attack
- Port scanning (Nmap uses this layer heavily)

Tools :

- Nmap (port scan, version scan)
- Netcat ("Swiss army knife", TCP/UDP)
- Hping (TCP flag manipulation)
- Wireshark

Layer 3 : Network Layer

Moves packet across different networks.

Key Concepts :

- IP Addressing
- Routing
- Packets
- NAT

Devices :

- Router
- Layer 3 switches

Cyber Attacks :

- IP Spoofing
- Route hijacking
- BGP attacks
- ICMP tunneling
- Packet fragmentation attacks

Tools :

- Nmap (scanning, ping sweepps)
- Hping3 (crafting packets, DDoS testing)
- Traceroute
- Wireshark (analysis)

Layer 2: Data Link Layer

Moves data **inside the same network** (LAN).

Key Concepts :

- MAC addresses
- Ethernet
- Frames
- Switches
- VLANs

Cyber Attacks :

- MAC Flooding
- ARP Spoofing
- VLAN Hopping
- STP manipulation

- CAM table attacks

Tools :

- Ettercap (ARP spoofing, MITM)
- Bettercap
- Cain & Abel
- Scapy (custom frames)
- Yersinia (attacking STP, CDP, DHCP)

Layer 1: Physical Layer

Handles the **raw signals**.

Examples:

- Cables
- WiFi signals
- Hubs
- Voltage
- Bits (0/1)

Cyber Attacks:

- Wiretapping
- Signal jamming
- Device tampering
- Hardware keyloggers
- Signal Jamming
- Cable Tapping
- EMI Attacks

Tools:

- Wi-Fi Jammers
- Spectrum analyzers

- Hardware sniffers
- Aircrack-ng (monitoring RF behavior)