THE OSI MODEL

LAYER	PROTOCOL DATA UNIT (PDU)	PURPOSES	PROTOCOLS SUPPORTED	DEVICES/ SERVICES	ATTACKS
APPLICATION (7) — How application uses network	DATA	- Resource sharing - Remote file access - Remote resource access - Directory services - Network management - Emails - Virtual terminals	HTTP/S FTP SMTP POP3 Telnet LPD (Linux)	DNS server	**EXPLOIT** Malware SMTP attack FTP Bounce Data attack Ransomware
PRESENTATION (6) — Represent and display data	DATA	(a) Translation → characters & numbers to binary format (0's and 1's) (b) Bit-reduction/ compression → loss / lossless — Data conversion and compression (c) Encryption	ASCII UNICODE TIFF JPEG SSL		**PHISHING**
SESSION (5) — Establish communication	DATA	DIALOG CONTROLLER: (a) Full duplex - 2way communication between 2 devices at the same time (b) Half duplex - 1way communication at a time SESSION MANAGEMENT - establish session - terminate - Maintenance - support Authentication, authorization, tracking of files downloaded.	SQL NFS RPC	APIs Net BIOS	**HIJACKING** - Cross site scripting - session side jacking - Malware cookie hijacking
TRANSPORT (4) — Provide reliable delivery	SEGMENTS	SEGMENTATION - source and destination portnos. - sequencing FLOW CONTROL ERROR CONTROL - checksums CONNECTION ORIENTED TRANSMISSION → TCP CONNECTION LESS TRANSMISSION → UDP	TCP: WWW, Email, FTP UDP: TFTP, DNS, online streaming		→ SYN flood → SYN packets → smurf attacks DDOS attacks Reconnaissance attacks

SOFTWARE LAYERS

HEART OF OSI

OSI MODEL (cont'd)

HARDWARE LAYERS

LAYER	PDU	PURPOSES	PROTOCOLS	DEVICES/ SERVICES	ATTACKS.
NETWORK (3) Address assigning and packet forwarding	Packets	LOGICAL ADDRESSING PATH DETERMINATION ROUTING	IPv4, IPv6 Masking OSPF BGP IS-IS ICMP ARP Routing protocols	ROUTERS	SPOOFING IP spoofing DOS and DDOS Attacks MITM attacks ICMP flooding Ping of death
DATA LINK (2) organizing data and transmitting	FRAMES	FRAMING (MAC1 | MAC2 | IP1 IP2 | SEGMENT | TAIL) PHYSICAL ADDRESSING - Media access control ERROR CONTROL FLOW CONTROL (Address resolution)	ATM CDP ARP (IP-MAC address, linking) FDDI Frame relay IEEE 802.11 MPLS	switches Bridges NIC Device drivers of host machines	MAC-SPOOFING MAC flooding Misconfigured devices Vulnerable old firmware ARP poisoning DNS spoofing DHCP starvation
PHYSICAL (1) Transmitting bits	BITS	BIT SYCHRONIZATION BIT RATE CONTROL PHYSICAL TOPOLOGIES (STAR, BUS, MESH) TRANSMISSION MODE (SIMPLEX, HALF DUPLEX, DUPLEX) ELECTRICAL SIGNALS TO BITS Fiber optics → PHOTONS Electrical voltage → ETHERNET Radio frequencies → WIRELESS	- Digital subscriber line - Infrared data association - USB - Bluetooth - Ethernet	Hubs Repeaters Modems cables (coax, fiber)	SNIFFING ATTACKS Alter data bits. Environmental & Physical threats — Dust — water — power outage — rodents Vandalism Eavesdropping SNIFFING Hub-inserting