https://blueteamresources.blogspot.com/2022/01/osi-model.html

| OSI Layer | Functions | Devices | Protocols | Protocol Data Unit | Attacks | Mitigations |
|---|---|---|---|---|---|---|
| **7. Application** | Responsible for creating the data for the packets. Acts as the interface between the user and the network. | PC, Phone, Server, Host Firewall, NIPS, HIPS, WAF, Gateways | HTTP, SMTP, FTP, DNS, SNMP, Telnet, DHCP, POP3, IMAP | Data | Exploit (malware), DDoS, HTTP Floods, SQL injection, Cross-site Scripting | Use WAF and Secure Gateways (web), Application Monitoring, AV. |
| **6. Presentation** | Data is translated, compressed, encoded, encrypted (if enabled) in such a way that the receiving application can understand and can be transported over the network | - | JPEG, MP3, SSL, TLS | Data | Phishing, SSL Hijacking, Encryption Downgrade, Decryption attacks. | Keeping AV and signatures up-to-date, SSL offloading and inspection. |
| **5. Session** | Establishment, maintenance, encryption, security, and termination of sessions is handled by this layer. | Circuit Level Gateway | NetBIOS, RPC, SMB | Data | Session Hijacking, Man-in-the-Browser | Vulnerabilities should be patched. |
| **4. Transport** | Responsible for end-to-end communication (process-to-process) and for error and flow control of segments. | Gateways, Firewall, NIPS | TCP, UDP | Segments-TCP, Datagram-UDP | Reconnaissance such as Host Discovery, Port Scanning, TCP/UDP Flood, and UDP Amplification. | Use Firewall, IPS, detect based on Thresholds and block at ISP level. |
| **3. Network** | Creates a routing path for packet delivery for devices in different networks and can also select between routing paths. | Router, N/W Firewall, NIPS | IP, ICMP, RIP, OSPF, IPsec | Packets | Man-in-the-middle (MITM), IP Spoofing, ICMP Attacks, Smurf Attack, Packet Sniffing. | Use Firewall, IPS (Packet Filtering), Enable logging, Encrypt Traffic, Configure Routers. |
| **2. Data Link** | Responsible for delivery to and from hosts on local network through communication media. Also does framing, error and flow control. Consists of LLC and MAC sub-layers | Switch, Bridge, NIC. | ARP, ATM, MAC, VLAN, PPP, PPTP | Frames | ARP Spoofing, MAC Cloning, DoS, VLAN Hopping. | Configure Switches, Port locking or Port Level Security, Static ARP. |
| **1. Physical** | It acts as the communication media and responsible for the actual physical communication between devices. | Hubs, Cables, Modems, Repeaters | 802.11, Ethernet BASE | Bits | Data Sniffing, Unauthorized access, Physical Damage. | Access Control, Tracking/Securing Physical Assets. |