**OSI MODELS**

Its Exploits and Measures

|  |  |  |
| --- | --- | --- |
| **Layer Name** | **Attacks** | **Counter-measure** |
| Layer 7 – Application Layer | SQL Injection | WAF, input validation, parameterized queries, monitor unusual database queries in SIEM |
| Cross-Site Scripting (XSS) | Content Security Policy (CSP), input sanitization, WAF rules |
| Phishing / Malware Delivery | Email filters, sandboxing attachments, user training, SIEM alerts for malware URLs |
| DNS Tunneling | Force all DNS through trusted servers, monitor high entropy / long DNS queries, SIEM alerts |
| Layer 6 – Presentation Layer | SSL/TLS Stripping | Enforce TLS 1.2/1.3, HSTS, certificate pinning, inspect SSL traffic` |
| Malware exploiting encoding | Content inspection, decode & analyze payloads, endpoint protection |
| Layer 5 - Session Layer | Session Hijacking | Enforce MFA, session timeouts, monitor for multiple logins from different IPs, IPS |
| |  | | --- | |  |   RDP / VPN Hijacking | Network monitoring, endpoint logging, MFA, anomaly detection for sessions |
| Layer 4 – Transport Layer | |  | | --- | |  |   TCP SYN Flood | SYN cookies, rate limiting, IDS/IPS traffic anomaly detection |
| TCP Reset Injection | Firewall rules, monitor abnormal RST spikes, TLS encrypted tunnels |
| |  | | --- | |  |   UDP Flood | Rate limiting, IDS/IPS, firewall block unusual UDP traffic |
| |  | | --- | |  |   Port Scanning | IDS/IPS alerts for scanning, firewall block suspicious IPs |
| Layer 3 – Network Layer | |  | | --- | |  |   IP Spoofing | Anti-spoofing filters (BCP38), ACLs on routers, monitor unusual traffic sources |
| ICMP Flood | Rate limit ICMP, IDS/IPS detection of ICMP anomalies |
| MITM / ARP spoofing | DHCP snooping, ARP inspection, VLAN segmentation, monitor ARP table changes |
| |  | | --- | |  |   Routing Attack | |  | | --- | |  |   BGP/OSPF security, monitor route changes |
| Layer 2 – Data Link Layer | |  | | --- | |  |   ARP Spoofing | Dynamic ARP inspection, VLAN isolation, monitor MAC table changes |
| MAC Flooding | Enable port security, monitor unusual MAC addresses |
| |  | | --- | |  |   VLAN Hopping | VLAN access control, private VLANs, port-based security |
| Layer 1 – Physical Layer | |  | | --- | |  |   Cable Tapping / Sniffing | Physical security, encrypted traffic (TLS), monitor unusual network activity |
| |  | | --- | |  |   Wi-Fi Sniffing | WPA3, strong passwords, rogue AP detection, IDS/IPS for Wi-Fi |
| |  | | --- | |  |   Jamming / Rogue AP | RF monitoring, secure SSIDs, disable unused ports/APs |