|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Attack Name** | **Vulnerability** | **How attack is mounted** | **How the attack works** | **Final Threat Posed by attack** | **Mitigation** |
| **TCP Port Scans** | Open network ports | A port scanner | TCP packets are sent to check if a server is alive | Network discovery, reconnaissance | Close unneeded ports |
| **Stealth TCP Port Scans** | Open network ports | Port scanning software with stealth mode enabled | Uses FIN, SYN-FIN, NULL, PUSH, or fragmented packets to stay undetected | Network discovery, reconnaissance | Use IDS/IPS systems, configure firewalls |
| **TCP Host Sweeps** | Live hosts on a network | A port scanner that supports range IP scanning | TCP Port Scan a range of IPs | Network discovery, reconnaissance | Use network segmentation, limit network access |
| **OS Fingerprinting** | Operating System Headers | TCP packets are sent and the response headers are analyzed | Identifies the type of operating system running | Information about (potentially outdated) OS versions | Configure systems to avoid disclosing info |
| **TCP Hijacking Attacks** | User session information | The victim’s IP is spoofed (using sequence numbers prediction) | Hijacking a TCP session by intercepting and modifying packets in transit | Unauthorized Access | Update the OS, random seq numbers |
| **TCP SYN Flood** | Low Network bandwidth | Floods a target system with a large number of TCP SYN packets | Every SYN request is saved in the 'incomplete connection queue' until acknowledged. This queue will overload if many SYNs are sent | Denial of Service | Use firewalls and IDS/IPS |
| **UDP Flood Attack** | Amplification Attack | A large number of pings are sent to a network's broadcast address, using a spoofed source IP address that belongs to the network | This will cause all hosts on the network to reply to the ping, flooding the victim's network (DOS) | Denial of Service | Block directed broadcasts, use load balancers |
| **UDP Bomb Attack** | Buffer Overflow | The length specified in the UDP header is less than the length specified in the IP header | The server allocates memory according to the UDP length, but writes data according to the IP length. A buffer will overflow if both lengths aren’t the same | Information disclosure, Denial of Service | Validate UDP/IP length headers before processing |