|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Attack Name** | **Vulnerability** | **How attack is mounted** | **How the attack works** | **Final Threat Posed by attack** | **Mitigation** |
| **ICMP Sweep** | Misconfigured Network | Uses ICMP to scan hosts | Sends ICMP echo request to a range of IPs | Network discovery, reconnaissance | Block ICMP traffic |
| **ICMP Redirect** | Routing Table | Spoofs ICMP redirect message & change a victim's default gateway address to that of the attacker | Redirects traffic of a victim to a malicious host | Traffic Hijacking | Allow only gateways to send redirects |
| **Session Hijacking w/ Non-Blind Spoofing** | Weak Session Management | Send packets with the source IP set to the victim’s IP | Takes over an active session | Unauthorized Access | Employ strong session management |
| **Blind Spoofing** | Lack of Authentication | Attacker changes the source IP to a fake IP and sends malicious packets to the victim | Malicious packets are sent victim, but responses are sent to the fake IP, hiding the attacker’s real IP | Unauthorized access to network resources, data theft, data tampering | Implement IP filtering to block spoofed packets |
| **IP Spoofing w/ Source Routing** | Loose source routing | The attacker can change the source IP and also specify the route the packet takes | Allows an attacker to bypass restricted routes by setting a custom network route | Man In the Middle | Disable source routing |
| **Ping Of Death** | Packet flooding | Sends oversized ICMP (ping) packets (in MBs) that the victim cannot process | Crashes a target system | Denial of Service | Filter oversized packets, Update the OS |
| **Ping Flood** | Network Congestion | Sends a high volume of ICMP (ping) packets | Overwhelms network bandwidth | Denial of Service | Rate limit ICMP requests, Update the OS |
| **Smurf 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 IDS Signatures |
| **TTL Expiry Attack** | Path Maximum Transmission Unit | Manipulate IP packets to set their TTL value to 0 or 1, causing them to be dropped by routers along the path to their destination. | If a lot of these packets are dropped, the router has to reply to all these packets, causing it to crash | Denial of Service | Configure network devices to ignore ICMP packets with low TTL |
| **Routing Table Overflow** | Routing Table | A large number of fake routing updates are sent to a router | Leaves no room for legit routes | Denial of Service | Use static routes |
| **Routing Table Poisoning** | Routing Table | Fake routing updates with routes containing routes are sent to a router | The attacker reroutes victim traffic to its IP address | Man In the Middle | Use static routes |