|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Attack Name** | **Vulnerability** | **How attack is mounted** | **How the attack works** | **Final Threat Posed by attack** | **Mitigation** |
| **CAM (Content Addressable Memory) table overflow** | MAC address tables in switches dynamically updated and trust the sending source MAC address in received frames | Sender will send large amounts of frames with different source MAC address | This will force the switch to update the MAC address table with false address and cause the legitimate address to be flushed out of the table | Overwhelm the network with large amounts of broadcasts as legitimate addresses are no longer in MAC address table | Configure port security on access ports,  Use manual MAC address tables rather than dynamic |
| **VLAN Hopping** | VLANs are not properly isolated from each other | Attacker sends frames with a VLAN ID that corresponds to a different VLAN | Switch forwards packets between VLANs that should not be forwarded | Access resources that should not be accessible from their own VLAN | Disable trunking on access ports |
| **VLAN double tagging** | Lack of proper validation of incoming traffic | Attacker sends packets with two VLAN tags instead of one | The switch will read the second tag and forward it as if it were untagged traffic | The hacker can send data packets to unauthorized VLANs | Disable unused ports, Use 802.1X authentication |
| **DHCP Starvation** | Limited number of IP addresses available in DHCP pool | Attacker requests multiple IP addresses from DHCP server without releasing them back to pool | Exhaust all available IP addresses in DHCP pool so that new devices cannot obtain an IP address from DHCP server | New devices cannot obtain an IP address from DHCP server and may not be able to communicate with other devices on network | Increase size of DHCP pool, Set maximum allowed users per port |
| **DHCP Spoofing** | Lack of authentication between client and server in DHCP protocol | Attacker sends fake DHCP responses to client before real server can respond | Client accepts fake response and uses attacker’s IP configuration | Attacker can intercept traffic intended for client or launch further attacks against client | Use static IP addressing for critical devices |
| **ARP**  **Spoofing / Poisoning** | Dynamic ARP Inspection not enabled | Attacker sends fake ARP messages to associate attacker’s MAC address with victim’s IP address | Victim’s traffic is sent to attacker instead of intended destination | Attacker can intercept traffic intended for victim or launch further attacks against victim | Enable Dynamic ARP Inspection (DAI),  Use static ARP entries |
| **Address Spoofing**  **(MAC and IP)** | The TCP sequence numbers that are used to construct a TCP packet can be easily guessed, and spoofed | Attacker changes the source IP address in packet headers to a trusted host’s IP address | Traffic appears to come from trusted host or network location | Attacker can bypass security mechanisms such as firewalls or IDS systems | Configure IP Source Guard (IPSG) |
| **STP Manipulation Attacks** | STP prevents network loops in a switched environment based on switch priority | Attacker connects to a switch port, and attempts to trigger an STP recalculation, becoming the root bridge. | By becoming the root bridge, the attacker can see and intercept all data that goes through the root bridge | Loss of confidentiality and integrity of network data as attacker can intercept all network data | Enable PortFast, BDPU Guard, Root Guard, Loop Guard |