**LAN Attacks**

**I. VLAN Hopping Attacks**

- VLAN Hopping attacks are a category of network attacks aimed at gaining unauthorized access to traffic within different Virtual Local Area Networks (VLANs) that a user or device should not have access to.

- There are three main types:

+ Switch Spoofing (or Trunk Spoofing)

+ Double Tagging

+ VTP (VLAN Trunking Protocol) Attacks

**II. Switch Spoofing Attack**

- The Setup:

* The attacker connects their device (a computer, for example) to a switch port.
* The attacker's device is configured to send DTP (Dynamic Trunking Protocol) messages.

- The Attack:

* DTP is designed to automatically negotiate trunk links between switches.
* The attacker's device sends DTP messages that mimic a switch requesting a trunk link.
* If the target switch is configured for automatic trunking (often the default), it responds and establishes a trunk link with the attacker's device.

- The Result:

* The attacker's device now acts as if it's connected to all VLANs allowed on the trunk.
* The attacker can send and receive traffic from any of those VLANs, effectively "hopping" between them.

iii. Double Tagging Attack

- **The Setup:**

* The attacker's device is connected to a switch port.
* The attacker crafts Ethernet frames with two 802.1Q VLAN tags.

- **The Attack:**

* The attacker adds two VLAN tags to the Ethernet frame.
* The outer tag (the first one) is the native VLAN of the switch the attacker is connected to.
* The inner tag (the second one) is the VLAN the attacker wants to target.
* When the first switch receives the frame, it only sees the outer tag. Because the outer tag matches the native vlan, the switch strips the outer tag, and forwards the frame.
* The second switch recieves the frame, and now the first tag that it sees, is the inner tag, which is the target vlan, and it forwards the packet to the target vlan.

- **The Result:**

* The packet is delivered to the target vlan, without the first switch knowing that it was delivered to the target vlan.
* This attack only works if the attacker is on the same vlan as the native vlan of the trunk port.

**IV. DHCP Message Attack**

- **Goal:** Disrupt network connectivity or manipulate client network settings.

- **Types:**

* **DHCP Starvation:** Flooding server with requests to exhaust IP pool (DoS).
* **Rogue DHCP Server:** Attacker's server provides malicious IP/config to clients (man-in-the-middle).
* **DHCP Spoofing:** Forging DHCP messages to manipulate client network configuration.

- **Vulnerabilities:** Lack of DHCP authentication, default insecure configs.

- **Mitigation:**

* DHCP Snooping (switch feature to filter DHCP messages).
* Port Security (limit MAC addresses per port).
* Network Segmentation (limit attack scope).
* Network monitoring.

**V. ARP Spoofing & ARP Poisoning Attacks**

- Core: Attack that exploits ARP (IP to MAC address mapping) within a LAN.

- How:

* Attacker sends forged ARP replies, linking their MAC to another's IP.
* Devices update their ARP caches with this false info.

- Goal: Intercept/manipulate network traffic (man-in-the-middle attacks).

- Vulnerability: ARP lacks built-in authentication.

- Result: Attacker becomes the "middleman," seeing/changing data.

- Essentially: Falsifying the "phonebook" of network devices.

1. **Address spoofing attacks** occur when the threat actor **changes the MAC and/or IP addres**s of the threat actor’s device to pose as another legitimate device, such as the default gateway.  
2. A threat actor sending **BPDU** messages with a priority of 0 is trying to becoming the root bridge in the **STP** topology.  
3. **DHCP starvation** attacks occur when a threat actor **requests and receives all the available IP address** for a subnet.  
4. A threat actor can send a **gratuitous ARP** reply causing all devices to believe that the threat actor’s device is a legitimate device, such as the **default gateway.**  
5. A threat actor can effectively **hop VLANs** if the threat actor’s device belongs to the **native VLAN and trunks with the switch.**  
6. A threat actor can use packet sniffing software, such as Wireshark, to view the contents of CDP messages, which are sent unencrypted and include a variety of device information including the IOS version and IP addresses.