LAYER 2 ATTACKS

Switches
Networking devices called switches forward packages to other nodes in the network. Switches can connect to numerous machines since they have numerous ports. For instance, you might have numerous PCs linked to a switch, which is connected to a router.

ARP Poisoning Attacks

What is ARP?
An IP address's corresponding MAC address can be determined via the Address Resolution Protocol (ARP). What MAC address is associated with IP? is the question that a device broadcasts over its local network segment when it wishes to know the MAC address connected with an IP. Only the device with the IP is expected to respond, broadcasting its MAC address in response. All other devices on the network segment receive this broadcast.

Poisoning ARP
You might be able to spot a problem in how ARP functions because it wasn't developed with security in mind: Only the device with the right IP is expected to respond when a request is made, but there is nothing to stop an attacker from responding instead by giving their own MAC address, which would cause data to be delivered to that MAC address rather than the intended recipient. ARP poisoning is used for a variety of purposes, such as man-in-the-middle attacks and denial of service.

MAC Attacks
MAC addresses have already been mentioned, but now is a good opportunity to examine them in greater detail. Network interfaces are given a hardware address called MAC, which stands for Media Access Control. Since MAC addresses are designed to be unique, no two pieces of hardware should ever have the same MAC address.

Layer 2 protocols use MAC addresses to direct data to the appropriate device.

MAC Spoofing
The initial 24 bits of a MAC address are used to identify the manufacturer, while the final 24 bits operate as a unique ID for that manufacturer. Officially, MAC addresses are divided into two 24-bit portions. However, MAC spoofing—the practice of devices "lying" about their MAC address—is entirely conceivable.

The method of MAC spoofing is NOT complicated, and security precautions like maintaining a deny-list of MAC addresses can be readily gotten through.

MAC Flooding

Switches on a network are the target of the attack known as MAC Flooding. Devices can connect to a switch's various ports, and for data to be sent to its intended location, the switch needs to know which MAC addresses go with which ports. This data is stored in the memory of switches. By bombarding the switch with data that seems to come from many distinct MAC addresses, MAC flooding tries to make the switch run out of space for storing MAC addresses.

Conclusion

Numerous low-level network protocols are weak points for attacks since they were not created with security in mind. These assaults may be intended to disrupt the victim's network or steal information.