13.4.2 Switch Attack Facts

The following table lists attacks that are commonly perpetrated against switches:

Attack	Description
MAC Flooding	*MAC flooding* overloads the switch's MAC forwarding table to make the switch function like a hub. MAC flooding attacks are performed as follows: 1. The attacker floods the switch with packets, each containing different source MAC addresses. 2. The flood of packets fills up the forwarding table and consumes so much of the switch's memory that it causes the switch to enter a state called *fail open mode*, in which all incoming packets are broadcast out all ports (as with a hub) instead of to the correct ports as per normal operation. 3. The attacker captures all the traffic with a protocol analyzer.

ARP Spoofing/Poisoning	*ARP spoofing/poisoning* associates the attacker's MAC address with the IP address of victim devices.
	▪ When computers send an ARP request for the MAC address of a known IP address, the attacker's system responds with its own MAC address.
	▪ The source device sends frames to the attacker's MAC address instead of the correct device.
	▪ Switches are indirectly involved in the attack because they do not verify the MAC address and IP address association.
	▪ A default gateway is a prime target because local traffic goes through a default gateway to get to non-local destinations, like the internet. When the attacker's MAC address is associated with the IP address of the default gateway:
	  ▪ Traffic can be forwarded to the actual default gateway (passive sniffing).
	  ▪ Data can be modified before it is forwarded (man-in-the-middle).

MAC Spoofing	*MAC spoofing* changes the source MAC address on frames sent by the attacker.
	▪ MAC spoofing is typically used to bypass 802.1x port-based security. It can also be used to bypass wireless MAC filtering.
	▪ MAC spoofing can hide the identity of the attacker's computer or impersonate another device on the network.
	▪ The attacker's system sends frames with the spoofed MAC address. The switch reads the source address contained in the frames and associates the MAC address with the port where the attacker is connected.
	▪ MAC spoofing can be used to:
	  ▪ Impersonate another device on the network and capture frames addressed to it.
	  ▪ Impersonate a valid device on the network to gain network access. It can be used to gain access when the switch uses MAC addresses to allow or deny a network connection.
	  ▪ Modify data before it is forwarded (man-in-the-middle).

VLAN Hopping	*VLAN hopping* occurs when an attacking host on a VLAN attempts to access traffic on another VLAN that it should not have access to. Two primary ways an attacker can execute a VLAN hopping exploit are: ▪ Switch spoofing. The attacker uses special software to manipulate VLAN tagging and trunking to make it appear that the computer is a trunking switch. ▪ Double tagging attack. The attacking host adds two VLAN tags to the header of the frames it transmits. The first tag identifies the VLAN of the attacker's computer. When the frame arrives at the first switch, the first tag is stripped off, making the second VLAN tag in the frame header visible. The second VLAN tag falsely indicates that the frame is a member of the target VLAN.