Post 6

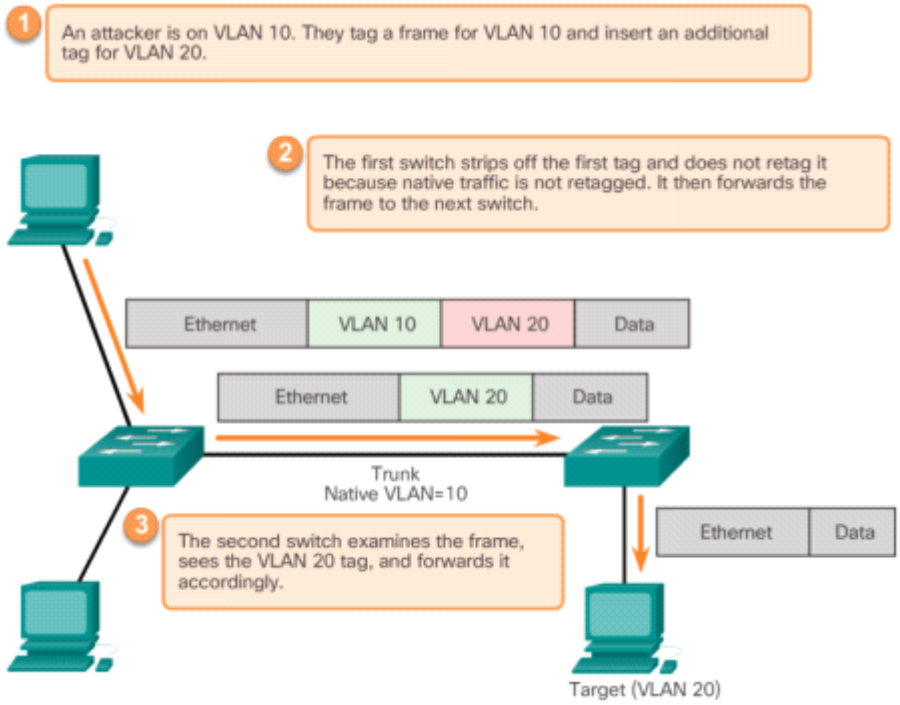
Thursday, January 24, 2019 11:11 PM

SWITCH SPOOFING ATTACKS

Switch Spoofing Attacks:

Hopping	○ Enables traffic from 1 VLAN to be seen by another VLAN ○ Trunk ports have access/pass all VLANs by default
Spoofing	▪ Attacker takes advantage of default config on switch port (dynamic auto) ▪ Takes advantage of misconfigured ports: Configures sys to spoof itself as switch ▪ Emulation of 802.1Q/DTP messages ▪ Tricks switch into thinking another switch is attempting to form trunk ▪ Allows attacker to gain access to all VLANs allowed on trunk port Mitigation: Turn off trunking all ports: Except needed: Disable DTP: Manually enable trunking

Double-Tagging (double-encapsulated) Attack



Double-tagging	▪ Takes advantage of way HW operates on switches ▪ Most only perform 1 lvl of 802.1Q de-encapsulation ▪ Embeds hidden 802.1Q tag inside frame ▪ Tag allows frame to be fwded to VLAN 802.1Q didn't specify ▪ Works **EVEN** if trunk ports disabled (host sends frame on segment not trunk) 1. Attacker sends double-tagged 802.1Q frame to switch – Outer header has VLAN tag of attacker: Same as native VLAN port – Switch processes frame received as if it were on trunk port/port w/voice VLAN – It shouldn't receive tagged eth0 frame on access port**Assume native = VLAN 10: Inner tag VLAN 20** 2. Frame arrives on switch: Looks at first 4-bytes of 802.1Q tag – Switch sees frame is destined for VLAN 10 (native) – Fwds packet out all VLAN 10 ports after stripping VLAN 10 tag – VLAN 20 tag is still intact/uninspected by 1st switch 3. Second switch only looks at inner 802.1Q tag attacker sent:

	– Sees the frame is destined for VLAN 20: Target – Second switch sends frame to victim port/floods – Depends if there is an existing MAC table entry for victim host ▪ Unidirectional: Only works when attacker is connected to port in same VLAN as native on trunk port Mitigation: Ensure native VLAN of the trunk ports is different from VLAN of user ports.

PVLAN Edge: Some apps require no traffic fwded at L2 between ports on same switch: 1 neighbor doesn't see traffic by another
PVLAN: AKA protected ports: No exchange of uni/multi/broadcast traffic between these ports on switch happens

PVLAN Edge	▪ Protected port doesn't fwd traffic (uni/multi/broadcast) to any other port also protected: Except control traffic ▪ Data traffic can't be forwarded between protected ports at L2 ▪ Fwding behavior between protected/nonprotected port proceeds as usual ▪ Protected ports must be manually config To configure PVLAN Edge: switchport protected cmd in int config no switchport protected cmd int config cmd: disable port show interfaces [*int id*] switchport (priv exec) cmd verify config of PVLAN Edge