Building Cisco Multilayer Switched Networks (BCMSN)

Layer 2 Security

http://www.INE.com

Attack Mitigation Overview

- What are common types of attacks?
  - Layer 2 attacks?
  - Layer 3 attacks?
  - Application attacks?
- How do we detect them?
- How do we stop them?

VLAN Hopping Attack

- Attacking host attached to Ethernet network sends 802.1Q / ISL tagged frames into switched network in order to hop over VLAN barriers
- Two variations
  - Host runs Dynamic Trunking Protocol (DTP) to actually form a trunk link with the adjacent switch
  - Host sends frames double tagged with 802.1q headers
    - Outside header is padding
    - Inside header is tagged with destination VLAN of victim

VLAN Hopping Mitigation

- Host facing interfaces should not be dynamic ports
  - **`switchport mode access`**
- Don't use VLAN 1, ***ever!***
  - Unused ports should be assigned to unused non VLAN 1 VLAN
  - Native VLAN should be changed to new administrative VLAN

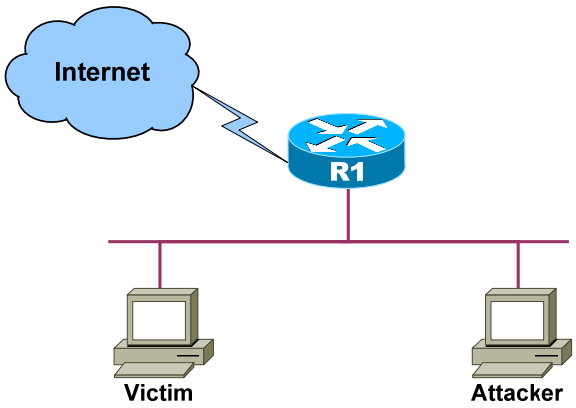
CAM Table Attacks

- Switch's Content Addressable Memory (CAM) table associates destination MAC address with outgoing interface
- If CAM table is full all unknown entries are treated like broadcast traffic
  - Forward out all ports in VLAN except the one it was received on
- Attacker floods frames with random source MAC addresses until CAM table fills up
- VLAN essentially turns into a hub

CAM Attack Mitigation

- Port Security
  - Limit the amount of source MAC addresses on a port
  - Limit the specific MAC address allowed on a port
  - Shut down the port or filter traffic if a violation occurs
  - Generate a syslog or SNMP trap for notification

Man-in-the-Middle (MiM) Attack



DHCP Starvation Attack

- DHCP server has finite IP address scope
- Attacker sends flood of DHCP requests with spoofed source MAC addresses
- DHCP server leases one IP address per MAC address until pool is depleted
- Victim hosts are “starved” of a DHCP lease

DHCP Starvation Mitigation

- Port Security
  - Limit the amount of source MAC addresses on a port
  - Limit the specific MAC address allowed on a port
  - Shut down the port or filter traffic if a violation occurs
  - Generate a syslog or SNMP trap for notification

DHCP Starvation Variation

- Port security can be used to limit number of MAC addresses on an interface
- Attacker can't generate DHCP requests with lots of source MAC addresses
- Some DHCP implementation don't use client source MAC address but instead use "Client Hardware Address" inside DHCP request payload
- Attacker can keep source MAC address in Ethernet frame the same but change the source MAC address in the DHCP packet
- Port security sees only one source MAC address - same starvation attack result

DHCP Starvation Mitigation

- DHCP Snooping
- Listens for DHCP traffic between client and server
- Builds IP to MAC mapping on a per interface basis
- Additional DHCP requests are dropped on interfaces that already have IP to MAC binding in the snooping table

Rogue DHCP Server Attack

- DHCP requests are layer 2 broadcasts within the VLAN
- By default anyone could reply to a host's DHCP request
- Can facilitate simple DoS, or worse, MiM attack
- For MiM attacker replies to host's request with…
  - Itself as default gateway
    - Sniff all traffic then forward to correct gateway
    - Transparent from victim perspective
  - Itself as DNS server
    - Redirect www.cisco.com to phishing website

Rogue DHCP Server Mitigation

- DHCP Snooping
  - Port connected to DHCP server is in snooping "trust" state
  - DHCP replies denied in all other ports

Rogue DHCP Server Mitigation

- If switches don't support snooping…
  - DHCP request uses UDP port 67
  - DHCP reply users UDP 68
  - Filter DHCP replies from all sources except DHCP server
- Can use port ACLs but VACLs would be more efficient

ARP Spoofing Attacks

- ARP is normally request / reply protocol
  - What is 1.2.3.4's MAC address?
  - I'm 1.2.3.4, my MAC address is…
- Gratuitous is an unsolicited ARP reply
  - Legitimate use is to refresh neighbors' ARP cache
  - Illegitimate use is to spoof someone else's MAC address
  - Can be used to facilitate MiM attack

ARP Attack Mitigation

- DHCP Snooping & Dynamic ARP Inspection
  - DHCP snooping builds IP and MAC binding table
  - When ARP replies are received the snooping table is checked to see if IP source and MAC address in ARP match
  - Malformed replies are dropped

MAC Spoofing Attack

- Attacker simply modifies source MAC and/or IP address to look like someone else
- From victim's perspective it looks like legitimate host

MAC Spoofing Mitigation

- IP Source Guard
  - Works like Dynamic ARP Inspection but checks all packets instead of just ARP
  - Consults DHCP snooping table
  - If source IP address and MAC don't match snooping table traffic is dropped

MAC Spoofing Mitigation

- If switches don't support IP Source Guard…
  - Port security can be used to allow only specific source MAC address or limit number of MAC addresses allowed in the interface

802.1X Authentication

- Used for username / password authentication between client and switch
- Uses AAA w/ RADIUS for authentication
- Stops illegitimate hosts from joining the network in the first place

Private VLANs

- Allow for layer 2 isolation and access control between ports within the same VLAN
- Can span multiple switches
- Example:
  - Device A, B, C and D are in VLAN 10
  - Device A should be allowed to communicate with device B, C, and D
  - Device B and C should be allowed to communicate with device A and each other
  - Device D should only be allowed to communicate with device A

Private VLANs (cont.)

- Private VLANs use “sub-VLANs” within the primary VLAN for the layer 2 isolation
  - Community
  - Isolated
- Sub VLANs contain port types…
  - Promiscuous
    - Can talk to all ports in the VLAN
  - Isolated
    - Can talk only to promiscuous ports
  - Community
    - Can talk to other ports in the same community and to promiscuous ports