LAN Security Attacks

Tags	
Klaar	JA
Week	Week 5

CDP Reconnaissance Attack

CDP information can be used by an attacker

Use the `no cdp run` global configuration command to disable CDP globally.

Use the `no cdp enable` interface configuration command to disable CDP on a port.

Telnet Attacks

There are two types of Telnet attacks:
Brute Force Password Attack - trial-and-error method used to obtain the administrative password.
Telnet DoS Attack - Attacker continuously requests Telnet connections in an attempt to render the Telnet service unavailable.
To mitigate these attacks:
Use SSH
Use strong passwords that are changed frequently.
Limit access to the vty lines using an access control list (ACL)

MAC Address Table Flooding Attack

Common LAN switch attack is the MAC address table flooding attack.
An attacker sends fake source MAC addresses until the switch MAC address table is full and the switch is overwhelmed.
Switch is then in fail-open mode and broadcasts all frames, allowing the attacker to capture those frames.

To mitigate this attack:

Enable port security to prevent MAC table flooding attacks.
Port security allows an administrator to do the following:
statically specify MAC addresses for a port.
permit the switch to dynamically learn a limited number of MAC addresses.
when the maximum number of MAC addresses is reached, any additional attempts to connect by unknown MAC addresses will generate a security violation.

VLAN Attacks

Switch spoofing attack - an example of a VLAN attack.
Attacker can gain VLAN access by configuring a host to spoof a switch and use the 802.1Q trunking protocol and DTP to trunk with the connecting switch.
Methods to mitigate VLAN attacks:

Disable DTP (auto trunking) negotiations on non-trunk ports and use switchport mode access.
Manually enable trunk links using switchport mode trunk.
Disable DTP (auto trunking) negotiations on trunking and non-trunking ports using switchport nonegotiate.
Change the native VLAN from VLAN 1.
Disable unused ports and assign them to an unused VLAN.

DHCP Attacks

DHCP spoofing attack - An attacker configures a fake DHCP server on the network to issue IP addresses to clients.
DHCP starvation attack - An attacker floods the DHCP server with bogus DHCP requests and leases all of the available IP addresses. This results in a denial-of-service

(DoS) attack as new clients cannot obtain an IP address.

Methods to mitigate DHCP attacks:

With DHCP snooping enabled on an interface, the switch will deny packets containing:
Unauthorized DHCP server messages coming from an untrusted port.
Unauthorized DHCP client messages not adhering to the DHCP Snooping Binding Database or rate limits.
DHCP snooping recognizes two types of ports:
Trusted DHCP ports - Only ports connecting to upstream DHCP servers should be trusted.
Untrusted ports - These ports connect to hosts that should not be providing DHCP server messages.

Administrative Access using AAA

Local AAA Authentication

Client establishes a connection with the router.
AAA router prompts the user for username and password.
Router authenticates the username and password using the local database, and allows user access.

Server-Based AAA Authentication

Client establishes a connection with the router.
AAA router prompts the user for a username and password.
The router authenticates the username and password using a remote AAA server.