CHAPTER 1

Cisco Layer 2 Security

This Quick Reference Guide provides a handy reference for students studying for the Cisco Securing Networks with Cisco Routers and Switches exam and is a great refresher on general Cisco router and switch security.

This Quick Reference is mapped to the requirements of the 642-504 SNRS exam.

This opening section of this Quick Reference to the Cisco SNRS exam provides an overview of Layer 2 security and the features within Cisco IOS that can mitigate the risk from the associated Layer 2 attacks.

Section 1: Cisco Layer 2 Security

A lot of attention is paid to securing the higher layers of the OSI reference model with network-level devices such as firewalls and intrusion protection systems (IPS) and applications such as antivirus and host-based intrusion protection (HIPS).

Layer 2 attacks occur, as you would expect, at Layer 2 of the OSI model. We know that switching operates at Layer 2, and therefore most of these attacks need to be mitigated in the switches that you deploy in your network.

Types of Layer 2 Attacks

We cover several types of Layer 2 attacks in this section. This section also explains how to mitigate these attacks by implementing the correct control in Cisco IOS.

The main types of Layer 2 attacks are as follows:

- CAM overflow
- VLAN hopping
- MAC spoofing

- Private VLAN attacks
- DHCP attacks

CAM Overflow

Switches operate by building a reference table of MAC addresses and corresponding switch ports. Based on the destination MAC address, the switch knows to which port to forward the frames. This table is called the context-addressable memory (CAM) table.

The switch can hold only a specific number of MAC addresses in this table, depending on the resources available to the switch.

A CAM overflow attack is where an attacker connects to a single or multiple switch ports and then runs a tool that s the existence of thousands of random MAC addresses on those switch ports. The switch enters these into the CAM table, and eventually the CAM table fills to capacity. When a switch is in this state, no more new MAC addresses can be learned, and therefore the switch starts to flood any traffic from new hosts out of all ports on the switch.

A CAM overflow attack turns a switch into a hub, which enables the attacker to eavesdrop on a conversation and perform man-in-the-middle attacks.

Cisco implemented a technology into IOS called Port Security that mitigates the risk of a Layer 2 CAM overflow attack.

Port Security

Port Security on a Cisco switch enables you to control how the switch port handles the learning and storing of MAC addresses on a per-interface basis. The main use of this command is to set a limit as to the maximum number of MAC addresses that can be learned and allocated to the individual switch port.

If a machine starts broadcasting multiple MAC addresses in what appears to be a CAM overflow attack, the default action of Port Security is to shut down the switch interface, although you can configure the switch just to discard any frames received from the bogus MAC addresses.

Configuring Port Security

Port Security has to be configured at the interface configuration level on a Cisco IOS switch.

It is recommended that you enable Port Security on static access ports rather than dynamic access or trunk ports.

Note

Using a setting of 1 for the maximum allowed MAC addresses sounds good from a security point of view, but might produce unwanted support overhead in all but the most locked-down environments.

For illustrative purposes, this section shows a common Port Security configuration. We will configure Port Security to dynamically allow three MAC addresses on the configured port. We will also make these connections sticky.

We will start by ensuring that the switch port is a static access port:

```
Switch(config-if)# switchport mode access
```

The next step is to enable Port Security on the switch interface and to configure a maximum of three MAC addresses for the interface:

```
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 3
```

The switch will learn the MAC addresses that are connected on the switch port and allow the first three it finds. In most cases, it will just be a single end-user workstation connected to the switch, and it should see only a single MAC address. The switch has to go through this process whenever the switch is rebooted. You can enable sticky mode for Port Security so that the MAC addresses that the switch learns about are stored when the configuration is saved so that they do not have to be relearned when the switch is rebooted. To enable sticky learning, enter the following command:

```
Switch(config-if)# switchport port-security mac-address sticky
```

We have just reviewed a common configuration scenario in which the switch dynamically learns and remembers the MAC address of the devices connected to it. The other, and more secure mechanism is to configure static Port Security by manually specifying the MAC address of the host connected to it.

If we have a switch port with the host MAC address 00:16:cb:96:95:94 connected to it, we can enter the following command to ensure that only this host can be connected to the switch port:

```
Switch(config-if)# switchport port-security mac-address 0016.cb96.9594
```

Note

When statically assigning MAC addresses, be careful of the possible support overhead that will be required for any moves or changes to the end-user infrastructure.

VLAN Hopping

Switches implement virtual LANs (VLAN). Users are connected to access ports that are members of a VLAN as specified in the configuration. VLAN hopping is where a user is able to gain access to a VLAN that is not assigned to the switch port to which the user is connected.

A user can achieve this in two ways against the default configuration of a Cisco switch port. The first and most commonly used VLAN hopping method is where the attacker makes his workstation act as a trunk port. Most switches, in the default configuration, need only one side of a connection to announce themselves as a trunk, then the switch automatically trunks all available VLANs over the switch port. This results in the attacker being able to see all traffic across all VLANs.

The second way an attacker can hop VLANs is by using what is called double tagging. With double tagging, the attacker inserts a second 802.1q tag in front of the existing 802.1q tag. This relies on the switch stripping off only the first 802.1q tag and leaving itself vulnerable to the second tag. This is not as common a method of VLAN hopping as using trunking.

To ensure you do not fall foul of a VLAN hopping attack, you have to ensure that all your user ports are assigned as access mode ports. Any unused ports should be disabled, and set as access mode ports by default.

To set a switch port to access mode, use the following configuration command from interface configuration mode:

```
Switch(config-if)# switchport mode access
```

MAC Spoofing

MAC spoofing attacks are attacks launched by clients on a Layer 2 network. Attackers spoofs their MAC address to perform what is known as a man-in-the-middle (MiTM) attack.

In one common attack, the attacker pretends to be the default gateway and sends out a gratuitous Address Resolution Protocol (ARP) to the network so that users send their traffic through the attacker rather than the default gateway. The attacker then forwards user traffic to the real default gateway. An attacker on a fast enough host can forward packets such that victims do not notice any change in their network access. Many tools available for download from the Internet can accomplish such a task, and preventing such attacks is quite problematic.

One way to mitigate this threat is to use Port Security. For this to work, however, the maximum MAC address setting must be 1, and the support headache associated with using this setting would probably be greater than the risk of this type of an attack occurring.

Private VLAN Attacks

Private VLANs (PVLAN) are special VLANs that can be used to further segment an existing Layer 2 VLAN into what are known as isolated and community ports. PVLANs are common on demilitarized zone (DMZ) segments, where the mail server does not need to communicate to the web server or similar, for example. In these instances, even though the web server and the mail server are on the same VLAN, the use of PVLANs can isolate the traffic between them so that the mail server cannot communicate with the web server unless the communication is through the default gateway.