UD3. Seguridad en switches

Índice

Ataques a Switches

ataque por desbordamiento de MACs

Cuando un host envía una trama en una LAN no hay nada que le impida poner la dirección MAC de origen que desee Incluso puede poner una dirección diferente en cada trama.

Con un sencillo programa un host puede enviar miles de tramas por segundo con direcciones MAC diferentes, todas falsas, de ese modo rápidamente desbordará la tabla CAM de cualquier conmutador

A partir de ese momento el conmutador difundirá todo el tráfico por inundación, actuando como si fuera un hub.

Con un programa de análisis de tráfico (sniffer o similar) el ordenador atacante, o cualquier otro de la red, podrá a partir de ese momento capturar el tráfico de otros ordenadores, incluidas las combinaciones usuario/contraseña utilizadas por los usuarios para acceder a los servicios (por ejemplo para leer el correo)

Soluciones al ataque por desbordamiento

Algunos conmutadores permiten limitar por configuración el número de direcciones MAC asociadas a cada puerto. En ese caso cuando el conmutador recibe por un puerto mas MACs diferentes que las permitidas deshabilita el puerto (lo pone en modo shutdown)

En una LAN en estrella, los conmutadores del final deberían limitar los puertos de usuario a 1 MAC por puerto ya que contendrán solamente ordenadores conectados a ellos y no otros conmutadores.

```
switch(config)# interface f0/2
switch(config-if)# switchport port-security maximum 1
```

También se pueden configurar en el conmutador las MACs que se permiten en cada puerto, es decir construir de forma estática la tabla CAM. Esto es lo más seguro, pero impide la movilidad de equipos por lo que no suele hacerse.

ataque por envenenamiento

Si las tramas ‘envenenadas’ (con direcciones de origen falsas) llevan como destino la dirección broadcast o cualquier dirección inexistente se distribuyen por toda la LAN, con lo que un solo host puede desbordar las tablas CAM de todos los conmutadores.

El host atacante puede husmear el tráfico de cualquier otro host en la LAN

Además el rendimiento de la red disminuye considerablemente, pues todos los puertos reciben todo el tráfico. La red funciona como un medio compartido.

Deshabilitar puertos en desuso

Un método simple que muchos administradores usan para contribuir a la seguridad de la red ante accesos no autorizados es inhabilitar todos los puertos del switch que no se utilizan. Por ejemplo, si un switch Catalyst 2960 tiene 24 puertos y hay tres conexiones Fast Ethernet en uso, es aconsejable inhabilitar los 21 puertos que no se utilizan. Navegue hasta todos los puertos que no se utilizan y emita el comando **shutdown** de Cisco IOS. Si más adelante se debe reactivar un puerto, este se puede habilitar con el comando **no shutdown**. La figura muestra el resultado parcial para esta configuración.

Realizar cambios de configuración a varios puertos de un switch es sencillo. Si se debe configurar un rango de puertos, use el comando **interface range**.

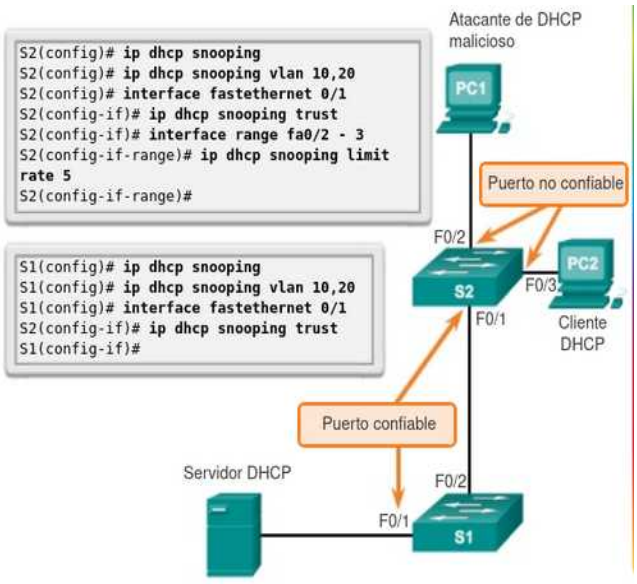
Switch(config)# **interface range *primer-número – último-número***

El proceso de habilitación e inhabilitación de puertos puede llevar mucho tiempo, pero mejora la seguridad de la red y vale la pena el esfuerzo.

Snooping DHCP

El snooping DHCP es una función que determina cuáles son los puertos de switch que pueden responder a solicitudes de DHCP. Los puertos se identifican como confiables o no confiables. Los puertos confiables pueden recibir todos los mensajes de DHCP, incluidos los paquetes de oferta de DHCP y de acuse de recibo de DHCP; los puertos no confiables solo pueden recibir solicitudes. Los puertos confiables de los hosts se alojan en el servidor de DHCP o pueden ser un enlace hacia dicho servidor. Si un dispositivo no autorizado en un puerto no confiable intenta enviar un paquete de oferta de DHCP a la red, el puerto se desactiva. Esta función puede unirse con las opciones de DHCP donde la información del switch, como el ID de puerto o la solicitud de DHCP pueden insertarse en el paquete de solicitudes de DHCP

Los puertos no confiables son aquellos que no están configurados explícitamente como confiables. Se construye una tabla enlazada de DHCP para los puertos no confiables. Cada entrada contiene una dirección MAC cliente, una dirección IP, un tiempo de arrendamiento, un número de VLAN y una ID de puerto registrados como clientes que realizan solicitudes de DHCP. Se utiliza entonces la tabla para filtrar el tráfico de DHCP subsiguiente. Desde la perspectiva de la detección de DHCP, los puertos de acceso no confiables no deben enviar mensajes de servidor de DHCP.



DHCP Starvation (DoS atack)

Un atacante envía tramas de DHCP Discover con CHADDR MAC's aleatorias consiguiendo que se le asignen IP's hasta acabar con el pool de direcciones del servidor DHCP lo que lleva a una denegación de servicio a los clientes legítimos.

El CHADDR (Client Host Address) es necesario por si la trama viene de un relay, por eso el servidor DHCP no se fija en la MAC de la trama sinó en la que va dentro del paquete.

DHCP Poisoning (M-i-t-M)

Similar al ARP poisoning, un servidor DHCP espúreo responde a los mensajes de discover de los clientes asignándoles ip's y de paso hace que los clientes lo usen a él como default gateway. El atacante puede examinar entonces todos sus paquetes o incluso modificarlos.

Funcionamiento

DHCP Snooping diferencia entre mensajes DHCP Server (Offer, ACK y NACK) y mensajes DHCP Cliente (DISCOVER y REQUEST, Release, Decline)

Los mensajes de Servidor son prohibidos en los puertos untrust y los cliente son investigados para ver si son legítimos o no.

- Si se recibe un mensaje en un puerto trusted se reenvía sin inspección

- si se recibe un mensaje en un puerto untrusted se inspecciona:

    - si es un mensaje de servidor se descarta

    - si es un mensaje de cliente se inspeccionan las MAC de origen y se reenvía guardando las MAC en la tabla de binding, se asegura que las ip's están en consonancia con las interfaces

Para habilitar el DHCP snooping:

Paso 1. Habilita la detección de DHCP mediante el comando **ip dhcp snooping** del modo de configuración global.

Paso 2. Habilita la detección de DHCP para VLAN específicas mediante el comando **ip dhcp snooping vlan número**. Es necesario el paso anterior, no llega con éste sólo

Paso 3. Definimos los puertos como confiables en el nivel de la interfaz mediante la identificación de los puertos confiables con el comando **ip dhcp snooping trust**.

Paso 4. (Optativo) Limitamos la velocidad a la que un atacante puede enviar solicitudes de DHCP falsas de manera continua a través de puertos no confiables al servidor de DHCP mediante el comando **ip dhcp snooping limit rate velocidad**. Por ejemplo ip dhcp snooping limit rate 1 limita a 1 mensaje DHCP por segundo, si se supera esta ratio el puerto será puesto en err-disabled con lo que tendremos que deshabilitarlo y habilitarlo como en port-security. También se puede hacer que se recupere automaticamente con **errdisable recovery cause dhcp-rate-limit** del modo de configuración global .

Pondremos también para evitar problemas con relay agentes **no ip dhcp snooping information option**

Con **show errdisable recovery** vemos los modos que tenemos habilitados. Vemos que hay un tiempo de espera hasta que se recupere.

Paso 5. Ver la tabla con **ip dhcp snooping trust**

Port Security

La seguridad de puerto limita la cantidad de direcciones MAC válidas permitidas en el puerto. Se permite el acceso a las direcciones MAC de los dispositivos legítimos, mientras que otras direcciones MAC se rechazan.

La seguridad de puertos se puede configurar para permitir una o más direcciones MAC. Si la cantidad de direcciones MAC permitidas en el puerto se limita a una, solo el dispositivo con esa dirección MAC específica puede conectarse correctamente al puerto. **switchport port-security** Habilita la seguridad **switchport port-security maximum 10**. Hablita 10 direcciones MAC

Si se configura un puerto como seguro y se alcanza la cantidad máxima de direcciones MAC, cualquier intento adicional de conexión de las direcciones MAC desconocidas genera una violación de seguridad.

Tipos de direcciones MAC seguras

Existen varias maneras de configurar la seguridad de puerto. El tipo de dirección segura se basa en la configuración e incluye lo siguiente:

Direcciones MAC seguras **estáticas**: son direcciones MAC que se configuran manualmente en un puerto mediante el comando **switchport port-security mac-address dirección-mac** del modo de configuración de interfaz. Las direcciones MAC configuradas de esta forma se almacenan en la tabla de direcciones y se agregan a la configuración en ejecución del switch. La podemos guardar.

Direcciones MAC seguras **dinámicas**: son direcciones MAC detectadas dinámicamente y se almacenan solamente en la tabla de direcciones. Las direcciones MAC configuradas de esta manera se eliminan cuando el switch se reinicia. Solo hay que haber habilitado el port-security.

Direcciones MAC seguras **persistentes**: son direcciones MAC que pueden detectarse de forma dinámica o configurarse de forma manual, y que después se almacenan en la tabla de direcciones y se agregan a la configuración en ejecución. Hay que insertarlas son la clave sticky

Direcciones MAC seguras persistentes

Para configurar una interfaz a fin de convertir las direcciones MAC detectadas dinámicamente en direcciones MAC seguras persistentes y agregarlas a la configuración en ejecución, debe habilitar el aprendizaje por persistencia. El aprendizaje por persistencia se habilita en una interfaz mediante el comando **switchport port-security mac-address sticky** del modo de configuración de interfaz.

Cuando se introduce este comando, el switch convierte todas las direcciones MAC detectadas dinámicamente en direcciones MAC seguras persistentes, incluso las que se detectaron dinámicamente antes de que se habilitara el aprendizaje por persistencia. Todas las direcciones MAC seguras persistentes se agregan a la tabla de direcciones y a la configuración en ejecución.

Las direcciones MAC seguras persistentes también se pueden definir manualmente. Cuando se configuran direcciones MAC seguras persistentes mediante el comando **switchport port-security mac-address sticky dirección-mac** del modo de configuración de interfaz, todas las direcciones especificadas se agregan a la tabla de direcciones y a la configuración en ejecución.

Si se guardan las direcciones MAC seguras persistentes en el archivo de configuración de inicio, cuando el switch se reinicia o la interfaz se desactiva, la interfaz no necesita volver a aprender las direcciones. Si no se guardan las direcciones seguras persistentes, estas se pierden.

Si se inhabilita el aprendizaje por persistencia mediante el comando **no switchport port-security mac-address sticky** del modo de configuración de interfaz, las direcciones MAC seguras persistentes siguen formando parte de la tabla de direcciones, pero se eliminan de la configuración en ejecución.

Observe que la característica de seguridad de puertos no funciona hasta que se habilita la seguridad de puertos en la interfaz mediante el comando **switchport port-security**.

Modos de violación de seguridad

Existe una violación de seguridad cuando se produce cualquiera de estas situaciones:

Se agregó la cantidad máxima de direcciones MAC seguras a la tabla de direcciones para esa interfaz, y una estación cuya dirección MAC no figura en la tabla de direcciones intenta acceder a la interfaz.

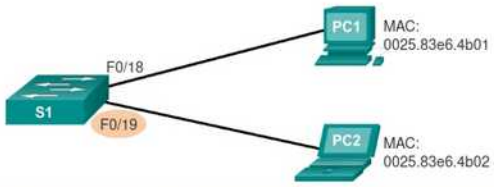
Una dirección aprendida o configurada en una interfaz segura puede verse en otra interfaz segura de la misma VLAN.

Se puede configurar una interfaz para uno de tres modos de violación, con la acción específica que se debe realizar si se produce una violación. La figura muestra los tipos de tráficos de datos que se envían cuando se configura en el puerto uno de los siguientes modos de violación de seguridad.

Especifica la interfaz que se debe configurar para la seguridad de puertos.	`S1(config)# interface fastethernet 0/18`
Establece la interfaz en modo de acceso.	`S1(config-if)# switchport mode access`
Establezca la seguridad de puerto en la interfaz.	`S1(config-if)# switchport port-security`

Protect (Proteger): cuando la cantidad de direcciones MAC seguras alcanza el límite permitido para el puerto, los paquetes con direcciones de origen desconocidas se descartan hasta que se elimine una cantidad suficiente de direcciones MAC seguras o se aumente la cantidad máxima de direcciones permitidas. No hay ninguna notificación de que se produjo una violación de seguridad.

Restrict (Restringir): cuando la cantidad de direcciones MAC seguras alcanza el límite permitido para el puerto, los paquetes con direcciones de origen desconocidas se descartan hasta que se elimine una cantidad suficiente de direcciones MAC seguras o se aumente la cantidad máxima de direcciones permitidas. En este modo, hay una notificación de que se produjo una violación de seguridad.



Comandos de CLI de Cisco IOS

Especifica la interfaz que se debe configurar para la seguridad de puertos.	`S1(config)# interface fastethernet 0/19`
Establece la interfaz en modo de acceso.	`S1(config-if)# switchport mode access`
Establezca la seguridad de puerto en la interfaz.	`S1(config-if)# switchport port-security`
Establece la cantidad máxima de direcciones seguras permitidas en el puerto.	`S1(config-if)# switchport port-security maximum 50`
Habilita el aprendizaje por persistencia.	`S1(config-if)# switchport port-security mac-address sticky`

Shutdown (Desactivar): en este modo de violación (predeterminado), una violación de seguridad de puerto produce que la interfaz se inhabilite de inmediato por errores y que se apague el LED del puerto. Aumenta el contador de violaciones. Cuando hay un puerto seguro en estado inhabilitado por errores, se lo puede sacar de dicho estado mediante la introducción de los comandos **shutdown** y **no shutdown** del modo de configuración de interfaz.

Para cambiar el modo de violación en un puerto de switch, use el comando del modo de configuración de interfaz **switchport port-security violation {protect | restrict | shutdown}.**

Verificar la seguridad de puerto

Después de configurar la seguridad de puertos en un switch, revise cada interfaz para verificar que la seguridad de puertos y las direcciones MAC estáticas se configuraron correctamente.

Verificar los parámetros de seguridad de puerto

Para mostrar la configuración de seguridad de puertos para el switch o la interfaz especificada, use el comando **show port-security [interface ID-de-interfaz].** El resultado de la configuración de la seguridad del puerto dinámico se muestra en la figura. De manera predeterminada, se permite una dirección MAC en este puerto.

```
S1# show port-security interface fastethernet 0/18
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0025.83e6.4b01:1
Security Violation Count   : 0
```

El resultado que se muestra en la figura muestra los valores de la configuración de seguridad del puerto persistente. La cantidad máxima de direcciones se estableció en 50, como se configuró.

Nota: la dirección MAC se identifica como sticky MAC (MAC persistente).

```
S1# show port-security interface fastethernet 0/19
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 50
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
```

Las direcciones MAC persistentes se agregan a la tabla de direcciones MAC y a la configuración en ejecución. Como se muestra en la figura 3, la dirección MAC persistente del PC2 se agregó a la configuración en ejecución para S1.

```
S1# show run | begin FastEthernet 0/19
interface FastEthernet0/19
 switchport mode access
 switchport port-security maximum 50
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0025.83e6.4b02
```

Verificar las direcciones MAC seguras

Para mostrar todas las direcciones MAC seguras configuradas en todas las interfaces del switch o en una interfaz especificada con la información de vencimiento para cada una, use el comando **show port-security address**. Como se muestra en la figura las direcciones MAC seguras se indican junto con los tipos.

```
S1# show port-security address
Secure Mac Address Table
------------------------------------------------------------
Vlan   Mac Address     Type           Ports   Remaining Age
                                                 (mins)
----   -----------     ----           -----   -------------
1      0025.83e6.4b01  SecureDynamic  Fa0/18      -
1      0025.83e6.4b02  SecureSticky   Fa0/19      -
------------------------------------------------------------
```

Cuando se configura un puerto con seguridad de puertos, una violación puede provocar que el puerto se inhabilite por errores. Cuando un puerto se inhabilita por errores, se desactiva eficazmente, y no se envía ni se recibe tráfico en ese puerto.

El estado del enlace y del protocolo del puerto cambia a down (inactivo). El LED del puerto cambia a color naranja. El comando show interfaces identifica el estado del puerto como err-disabled. El resultado del comando show port-security interface ahora muestra el estado del puerto como secure-shutdown. Debido a que el modo de violación de seguridad de puertos está establecido en shutdown, el puerto que experimenta la violación de seguridad pasa al estado de inhabilitación por errores.

Tambien podemos ver el running-config las estáticas y las sticky