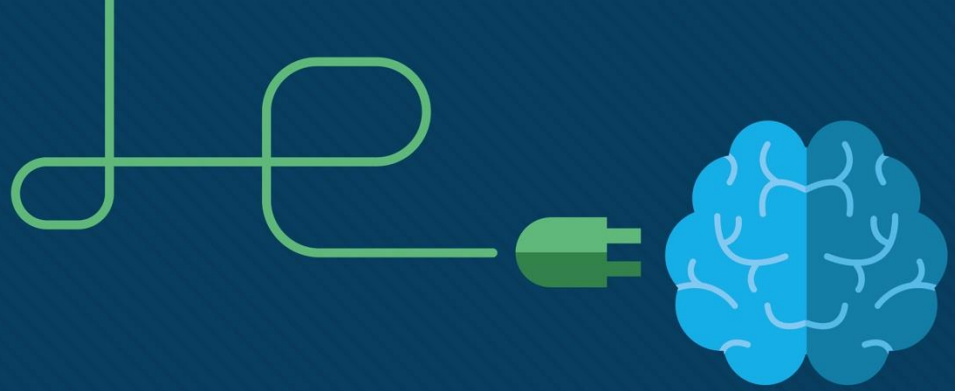
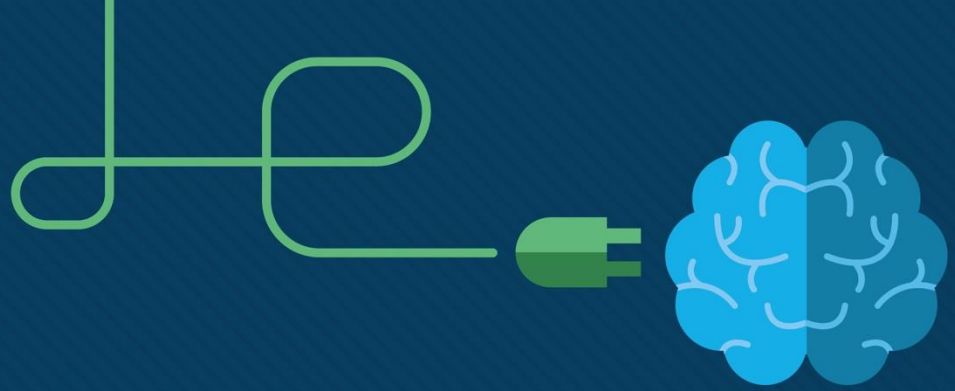


Módulo 10: Conceptos de Seguridad de LAN

Materiales del Instructor

Switching, Routing y Wireless Essentials (SRWE)



Módulo 10: Conceptos de Seguridad de LAN

Switching, Routing y Wireless Essentials (SRWE)

Objetivos del módulo

Título del Módulo: Conceptos de Seguridad de LAN

Objetivo del Módulo: Explique cómo las vulnerabilidades ponen en riesgo la seguridad de LAN.

Título del tema	Objetivo del tema
Seguridad de punto de finalización	Explique cómo usar la seguridad de para mitigar los ataques.
Control de acceso	Explique cómo se utilizan AAA y 802.1x para autenticar los terminales y los dispositivos LAN.
Amenazas a la seguridad de capa 2	Identifique vulnerabilidades de capa 2
Ataque de tablas de direcciones MAC	Explique cómo un ataque de tablas de direcciones MAC compromete la seguridad de LAN.
Ataques a la LAN	Explique cómo los ataques a la LAN comprometen la seguridad de LAN.

10.1 - Seguridad de punto final (endpoint security)

Ataques de red en la actualidad

Normalmente, los medios de comunicación cubren los ataques de red externos a redes empresariales. Sencillamente busque en el internet por "Los más nuevos ataques de red" y encontrara información actualizada de ataques actuales. Muy posiblemente, estos ataques envuelven una o más de las siguientes:

- **Denegación de servicio distribuida (DDoS)** Se trata de un ataque coordinado desde muchos dispositivos, llamados zombis, con la intención de degradar o detener el acceso público al sitio web y los recursos de una organización.
- **Data Breach**- Se trata de un ataque en el que los servidores de datos o los hosts de una organización se ven comprometidos a robar información confidencial.
- **Malware**– Este es un ataque en el que los hosts de una organización son infectados con software malicioso que causa una serie de problemas. Por ejemplo, ransomware como WannaCry, mostrado en la figura, encripta los datos en un host y bloquea el acceso hasta que se le pague un rescate.

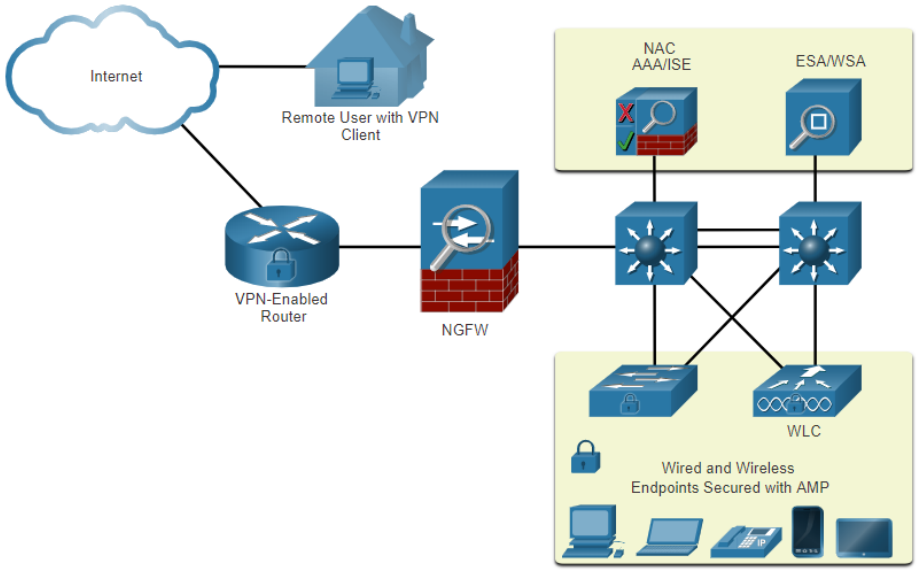
Seguridad de dispositivos de redes

Se necesitan diversos dispositivos de seguridad de la red para proteger el perímetro de la red del acceso exterior. Estos dispositivos podrían incluir lo siguiente:

- Virtual Private Network (VPN) - proporciona una conexión segura a usuarios remotos a través de una red pública y en la red empresarial. Los servicios VPN pueden ser integrados en el cortafuegos.
- Firewall de próxima generación (NGFW) - proporciona inspección de paquetes con estado, visibilidad y control de aplicaciones, un sistema de prevención de intrusos de próxima generación (NGIPS), protección avanzada contra malware (AMP) y filtrado de URL.
- Network Access Control (NAC) - incluye servicios de autenticación, autorización y contabilidad (AAA). En empresas más grandes, estos servicios podrían incorporarse en un dispositivo que pueda administrar políticas de acceso en una amplia variedad de usuarios y tipos de dispositivos. El Cisco Identity Services Engine (ISE) en un ejemplo de dispositivo NAC.

Protección de terminales

- Los puntos finales son hosts que generalmente consisten en computadoras portátiles, computadoras de escritorio, servidores y teléfonos IP, así como dispositivos propiedad de los empleados. Los puntos finales son particularmente susceptibles a ataques relacionados con malware que se originan a través del correo electrónico o la navegación web.
- Los puntos finales suelen utilizar características de seguridad tradicionales basadas en host, como antivirus antimalware, firewalls basados en host y sistemas de prevención de intrusiones (HIPS) basados en host.
- Los puntos finales de hoy están mejor protegidos por una combinación de NAC, software AMP, un dispositivo de



Cisco Email Security Appliance

El dispositivo Cisco ESA está diseñado para monitorear el Protocolo simple de transferencia de correo (SMTP). Cisco ESA se actualiza constantemente mediante datos en tiempo real de Cisco Talos, que detecta y correlaciona las amenazas con un sistema de monitoreo que utiliza una base de datos mundial. Cisco ESA extrae estos datos de inteligencia de amenazas cada tres o cinco minutos.

Estas son algunas funciones de Cisco ESA:

- Bloquear amenazas conocidas
- Remediar contra el malware invisible que evade la detección inicial
- Descartar correos electrónicos con enlaces incorrectos
- Bloquear el acceso a sitios recién infectados
- Encriptar el contenido de los correos salientes para prevenir perdida de datos.

Cisco Web Security Appliance

- Cisco Web Security Appliance (WSA) es una tecnología de mitigación para amenazas basadas en la web. Ayuda a las organizaciones a abordar los desafíos de asegurar y controlar el tráfico web.
- Cisco WSA combina protección avanzada contra malware, visibilidad y control de aplicaciones, controles de políticas de uso aceptable e informes.
- Cisco WSA proporciona un control total sobre cómo los usuarios acceden a internet. Ciertas funciones y aplicaciones, como chat, mensajería, video y audio, pueden permitirse, restringirse con límites de tiempo y ancho de banda, o bloquearse, de acuerdo con los requisitos de la organización.
- La WSA puede realizar listas negras de URL, filtrado de URL, escaneo de malware, categorización de URL, filtrado de aplicaciones web y cifrado y descifrado del tráfico web.

10.2 Control de acceso

Autenticación con una contraseña local

Muchas formas de autenticación pueden ser llevadas a cabo en dispositivos de red, y cada método ofrece diferentes niveles de seguridad.

El simple método de autenticación por acceso remoto es para configurar un inicio de sesión y contraseña combinación en consola, lineas vty, y puertos auxiliares, como se muestra en las lineas vty en el siguiente ejemplo.

```
R1(config)# line vty 0 4
R1(config-line)# password ci5c0
R1(config-line)# login
```

SSH es un tipo de acceso remoto más seguro:

- Requiere un nombre de usuario y una contraseña.
- El nombre de usuario y la contraseña se pueden autenticar localmente.

```
R1(config)# ip domain-name example.com
R1(config)# crypto key generate rsa general-keys modulus 2048
R1(config)# username Admin secret Str0ng3rPa55w0rd
R1(config)# ssh version 2
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
```

El método de base de datos local tiene algunas limitaciones:

- Las cuentas de usuario deben configurarse localmente en cada dispositivo que no sea escalable.
- El método no proporciona ningún método de autenticación alternativa.

Componentes AAA

AAA significa Autenticación, Autorización y Contabilidad, y proporciona el marco principal para configurar el control de acceso en un dispositivo de red.

AAA es un modo de controlar quién tiene permitido acceder a una red (autenticar), controlar lo que las personas pueden hacer mientras se encuentran allí (autorizar) y qué acciones realizan mientras acceden a la red (contabilizar).

Control de acceso
autenticación

Dos métodos de implementación de autenticación AAA son Local y basada en el servidor (server-based).

Autenticación AAA local:

- El método almacena nombres de usuario y contraseñas localmente en un dispositivo de red (por ejemplo, router Cisco).
- Los usuarios se autentican contra la base de datos local.
- AAA local es ideal para las redes pequeñas.

Autenticación AAA basada en el servidor:

- Con el método basado en el servidor, el enrutador accede a un servidor central AAA.
- El servidor AAA contiene los nombres de usuario y contraseñas de todos los usuarios.
- El router AAA usa el protocolo de sistema de control de acceso del controlador de acceso a terminales (TACACS+) o el protocolo de servicio de autenticación remota para usuarios de entrada telefónica (RADIUS) para comunicarse con el servidor de AAA.
- Cuando hay múltiples enrutadores y switches basado en el servidor es más apropiado.

Autorización

- La autorización es automática y no requiere que los usuarios tomen medidas adicionales después de la autenticación.

- La autorización controla lo que el usuario puede hacer o no en la red después de una autenticación satisfactoria:

- La autorización utiliza un conjunto de atributos que describe el acceso del usuario a la red. El servidor AAA utiliza estos atributos para determinar los privilegios y restricciones para ese usuario.

Contabilidad

La auditoría de AAA recopila datos de uso en los registros de AAA y los informa. La organización puede utilizar estos datos para fines como auditorías o facturación. Los datos recopilados pueden incluir la hora de inicio y finalización de la conexión, los comandos ejecutados, la cantidad de paquetes y el número de bytes.

Un uso muy implementado de la contabilidad es combinarlo con la autenticación AAA.

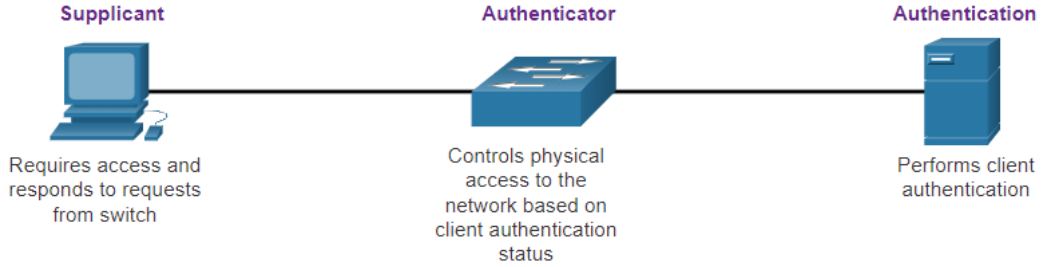
- Los servidores AAA mantienen un registro detallado de lo que el usuario autenticado hace exactamente en el dispositivo, como se muestra en la imagen Esto incluye todos los comandos EXEC y de configuración que emite el usuario.
- El registro contiene varios campos de datos, incluidos el nombre de usuario, la fecha y hora, y el comando real que introdujo el usuario. Esta información resulta útil para solucionar problemas de dispositivos También proporciona evidencia de cuándo las personas realizan actos maliciosos.

Control de acceso
802.1X

El estándar IEEE 802.1X define un control de acceso y un protocolo de autenticación basados en puertos. Evita que las estaciones de trabajo no autorizadas se conecten a una LAN a través de puertos de switch de acceso público. El servidor de autenticación autentica cada estación de trabajo que está conectada a un puerto del switch antes habilitar cualquier servicio ofrecido por el switch o la LAN.

Con la autenticación basada en el puerto 802.1X, los dispositivos en la red tienen roles específicos:

- **Cliente (Suplicante)**- Este es un dispositivo que ejecuta un software de cliente compatible con 802.1X, que está disponible para dispositivos con cable o inalámbricos.
- **Switch (Autenticador)**- El switch actúa como intermediario entre el cliente y el servidor de autenticación. Solicita la identificación de la información del cliente, verifica dicha información al servidor de autenticación y transmite una respuesta al cliente. Otro dispositivo que puede actuar como autenticador is un punto de acceso inalámbrico.
- **Servidor de autenticación:**– El servidor valida la identidad del cliente y notifica al switch o al punto de acceso inalámbrico que el cliente está o no autorizado para acceder a la LAN y a los servicios del switch.

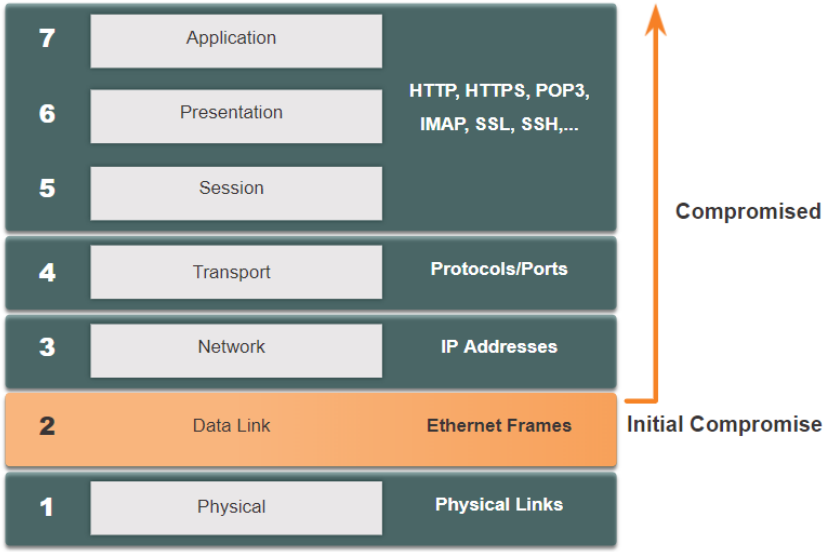


10.3 Amenazas de seguridad de capa 2

Vulnerabilidades de capa 2

Recuerde que el modelo de referencia OSI está dividido en siete capaz, las cuales trabajan de manera independiente una de otra. La figura muestra la función de cada capa los elementos de núcleo que pueden ser explotados.

Los administradores de red implementan habitualmente soluciones de seguridad para proteger los elementos en la capa 3 hasta la capa 7. Ellos usan VPNs, cortafuegos, y dispositivos IPS para proteger estos elementos Si la capa 2 se ve comprometida, todas las capas superiores también se ven afectadas. Por ejemplo, si un atacantes con acceso a la red interna captura los marcos de la Capa 2, entonces toda la seguridad implementada en las capas anteriores sería inútil. El atacante podría causar mucho daño en la infraestructura de red LAN de capa 2.



categorías de ataque en el Switch

La seguridad es solamente tan sólida como el enlace más débil en el sistema, y la capa 2 es considerada el enlace mas débil. Esto se debe a que las LAN estaban tradicionalmente bajo el control administrativo de una sola organización. Inherentemente confiamos en todas las personas y dispositivos conectados a nuestra LAN. Hoy, con BYOD y ataques más sofisticados, nuestras LAN se han vuelto más vulnerables a la penetración.

Categoría	Ejemplos
Ataques de tabla MAC	Incluye ataques de inundación de direcciones MAC.
Ataques de VLAN	Incluye ataques VLAN hopping y VLAN double-tagging. También incluye ataques entre dispositivos en una VLAN común.
Ataques de DHCP	Incluye ataques DHCP starvation y DHCP spoofing.
Ataques ARP	Incluye la suplantación de ARP y los ataques de envenenamiento de ARP.
Ataques de suplantación de direcciones	Incluye los ataques de suplantación de direcciones MAC e IP.
Ataques STP	Incluye ataques de manipulación al Protocolo de árbol de extensión

Técnicas de mitigación de ataques en el switch

Solución	Descripción
Seguridad de puertos	Previene muchos tipos de ataques, incluidos los ataques de inundación de direcciones MAC y los ataques de hambre DHCP.
Detección DHCP	Previene ataques de suplantación de identidad y de agotamiento de DHCP.
Inspección ARP dinámica (DAI)	Previene la suplantación de ARP y los ataques de envenenamiento de ARP.
Protección de IP de origen (IPSG)	Impide los ataques de suplantación de direcciones MAC e IP.

Estas soluciones de Capa 2 no serán efectivas si los protocolos de administración no están asegurados. Se recomiendan las siguientes estrategias:

- Utilice siempre variantes seguras de protocolos de administración como SSH, Protocolo de copia segura (SCP), FTP seguro (SFTP) y Seguridad de capa de sockets seguros / capa de transporte (SSL / TLS).
- Considere usar la Red de administración fuera de banda para administrar dispositivos.
- Use una VLAN de administración dedicada que solo aloje el tráfico de administración.
- Use ACL para filtrar el acceso no deseado.

10.4 Ataque de tablas de direcciones MAC

Revisión de la operación del switch

Recuerde que para tomar decisiones de reenvío, un Switch LAN de capa 2 crea una tabla basada en las direcciones MAC de origen en las tramas recibidas. Esto se llama una tabla de direcciones MAC. Las tablas de direcciones MAC se almacenan en la memoria y se usan para cambiar switch frames más eficientemente.

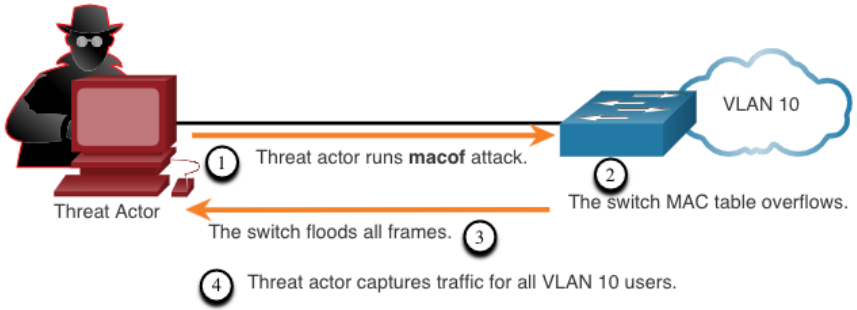
```
S1# show mac address-table dynamic
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0001.9717.22e0    DYNAMIC     Fa0/4
   1    000a.f38e.74b3    DYNAMIC     Fa0/1
   1    0090.0c23.ceca    DYNAMIC     Fa0/3
   1    00d0.ba07.8499    DYNAMIC     Fa0/2
S1#
```

Inundación de la tabla de direcciones MAC

Todas las tablas MAC tiene un tamaño fijo por lo que un interruptor puede quedarse sin espacio para guardar direcciones MAC. Los ataques de inundación de direcciones MAC aprovechan esta limitación al bombardear el switch con direcciones MAC de origen falsas hasta que la tabla de direcciones MAC del switch esté llena.

Cuando esto ocurre, el switch trata el frame como una unidifusión desconocida y comienza a inundar todo el tráfico entrante por todos los puertos en la misma VLAN sin hacer referencia a la tabla MAC. Esta condición ahora permite que un atacantes capture todas las tramas enviadas desde un host a otro en la LAN local o VLAN local.

Nota: El tráfico se inunda solo dentro de la LAN o VLAN local. El atacante solo puede capturar el tráfico dentro de la LAN o VLAN local a la que está conectado el atacante.



Mitigación de ataques de tabla de direcciones MAC

Lo que hace que herramientas como **macof**sean peligrosas, es que un atacante puede crear un ataque de desbordamiento de tabla MAC muy rápidamente. Por ejemplo, un switch Catalyst 6500 puede almacenar 132,000 direcciones MAC en su tabla de direcciones MAC. Una herramienta como **macof**puede inundar un interruptor con hasta 8,000 cuadros falsos por segundo; crear un ataque de desbordamiento de la tabla de direcciones MAC en cuestión de segundos.

Otra razón por la que estas herramientas de ataque son peligrosas es porque no sólo afectan el interruptor local sino que también afectan interruptores conectados de capa 2. Cuando la tabla de direcciones MAC de un switch está llena, comienza a desbordar todos los puertos, incluidos los conectados a otros switches de capa 2.

Para mitigar los ataques de desbordamiento de la tabla de direcciones MAC, los administradores de red deben implementar la seguridad del puerto. La seguridad de puertos (Port security) permitirá que el puerto aprenda sólo un número específico de fuentes de direcciones MAC. Seguridad de puertos (Port security) será discutido más adelante en otro módulo.

10.5 Ataques a la LAN

Video – VLAN y ataques DHCP

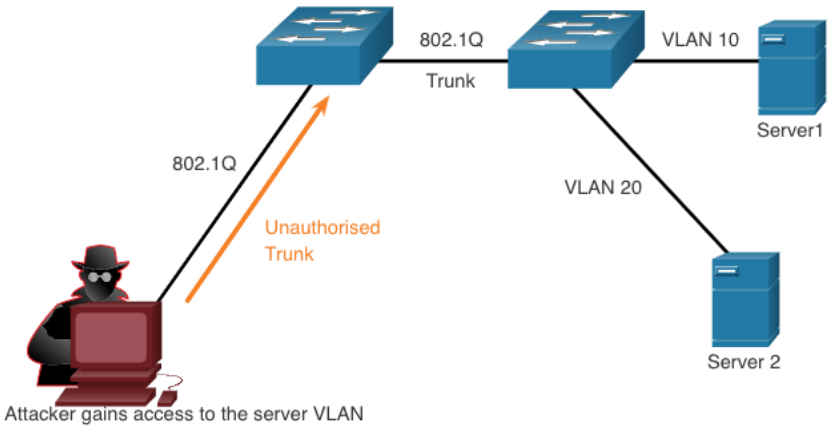
Este video cubrirá lo siguiente:

- Ataque con salto de VLAN
- Ataque de doble-etiqueta de VLAN
- Ataque por agotamiento del DHCP
- Ataque de suplantación de DHCP

Ataques de salto de VLAN

El salto de VLAN permite que otra VLAN pueda ver el tráfico de una VLAN sin cruzar primero un router. En un ataque de salto de VLAN básico, el atacante configura un host para que actúe como un switch, para aprovechar la función de puerto de enlace automático habilitada de forma predeterminada en la mayoría de los puertos del switch.

El atacante configura el host para falsificar la señalización 802.1Q y la señalización del Protocolo de enlace dinámico (DTP) propiedad de Cisco al enlace troncal con el switch de conexión. Si es exitoso, el switch establece un enlace troncal con el host, como se muestra en la figura. Ahora el actor amenazante puede acceder todas las VLANS en el switch. El atacante puede enviar y recibir tráfico en cualquier VLAN, saltando efectivamente entre las VLAN.



Ataques de doble etiquetado de VLAN

Un atacantes de situaciones específicas que podrían incrustar una etiqueta 802.1Q oculta dentro del marco que ya tiene una etiqueta 802.1Q. Esta etiqueta permite que la trama se envíe a una VLAN que la etiqueta 802.1Q externa no especificó.

- **Paso 1:** El atacante envía una trama 802.1Q de doble etiqueta al switch. El encabezado externo tiene la etiqueta VLAN del atacante, que es la misma que la VLAN nativa del puerto de enlace troncal.
- **Paso 2**: El frame llega al primer switch, que mira la primera etiqueta 802.1Q de 4 bytes. El switch ve que el frame está destinado a la VLAN nativa. El switch reenvía el paquete a todos los puertos VLAN nativos después de quitar la etiqueta VLAN. El frame no es re etiquetada porque es parte de la VLAN nativa. En este punto, la etiqueta VLAN interna todavía está intacta y no ha sido inspeccionada por el primer switch.
- **Paso 3**: La trama llega al segundo switch que no tiene conocimiento de que se suponía que era para la VLAN nativa. El switch emisor no etiqueta el tráfico de la VLAN nativa como se especifica en la especificación 802.1Q. El segundo switch solo mira la etiqueta interna 802.1Q que insertó el atacante y ve que el frame está destinado a la VLAN de destino. El segundo switch envía el paquete al puerto víctima o lo satura, dependiendo de si existe una entrada en la tabla de MAC para el host víctima.

Ataque de doble-etiqueta de VLAN (Cont.)

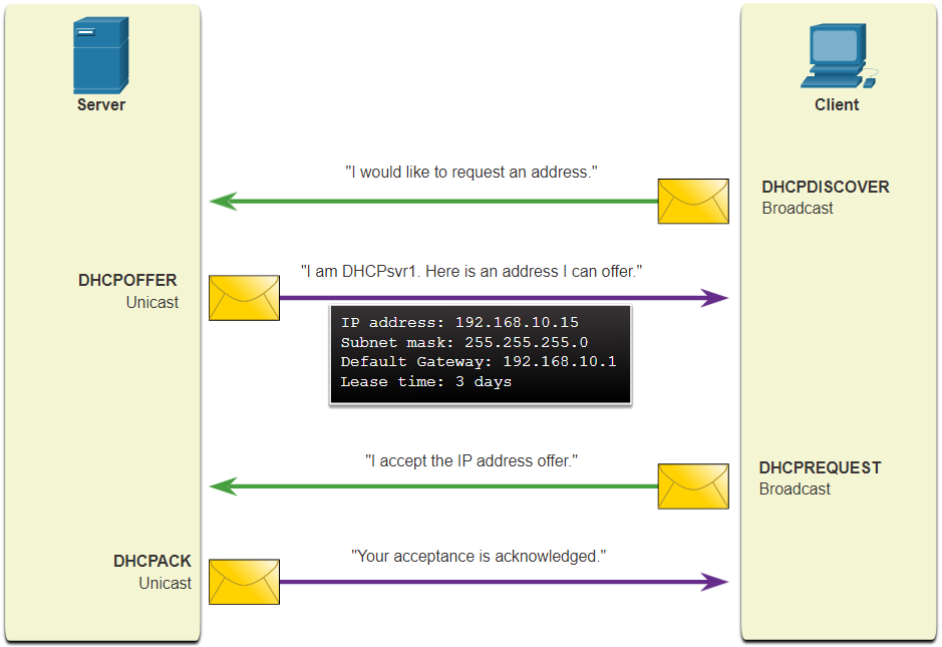
Un ataque doble-etiqueta a una VLAN es unidireccional y funciona únicamente cuando el atacante está conectado a un puerto que reside en la misma VLAN que la VLAN nativa del puerto troncal. La idea es que el doble etiquetado permite al atacante enviar datos a hosts o servidores en una VLAN que de otro modo se bloquearía por algún tipo de configuración de control de acceso. Presumiblemente, también se permitirá el tráfico de retorno, lo que le dará al atacante la capacidad de comunicarse con los dispositivos en la VLAN normalmente bloqueada.

Mitigación de ataque de VLAN: - se pueden evitar los saltos de VLAN y los ataques de doble etiquetado de VLAN mediante la implementación de las siguientes pautas de seguridad troncal, como se discutió en un módulo anterior:

- Deshabilitar troncal en todos los puertos de acceso.
- Deshabilitar troncal automático en enlaces troncales para poder habilitarlos de manera manual.
- Asegúrese de que la VLAN nativa solo se usa para los enlaces troncales.

Mensajes DHCP

Los servidores DHCP proporcionan dinámicamente la información de configuración de IP a los clientes, como la dirección IP, la máscara de subred, el gateway predeterminado, los servidores DNS y más. En la figura se muestra una revisión de la secuencia del intercambio de mensajes DH



Mensajes DHCP

Los dos tipos de ataques DHCP son inanición y suplantación de identidad. Ambos ataques pueden ser mitigados implementando DHCP snooping.

- **Ataque DHCP Starvation –** el objetivo de este ataque es crear un DoS para conectar clientes. Los ataques de agotamiento de DHCP requieren una herramienta de ataque, como Gobbler. Gobbler tiene la capacidad de ver todo el alcance de las direcciones IP alquilables e intenta alquilarlas todas. Específicamente, este crea un mensaje DHCP de descubrimiento con una dirección MAC falsa.
- **Ataque de DHCP Spoofing –** este ocurre cuando un servidor DHCP falso se conecta a la red y proporciona parámetros de configuración de IP falsos a clientes legítimos. Un servidor no autorizado puede proporcionar una variedad de información engañosa, que incluye lo siguiente:
  - **Puerta de enlace predeterminada incorrecta**- el servidor fraudulento proporciona una puerta de enlace no válida o la dirección IP de su host para crear un ataque de hombre en el medio. Esto puede pasar totalmente inadvertido, ya que el intruso intercepta el flujo de datos por la red.
  - **Servidor DNS incorrecto**- el servidor fraudulento proporciona una dirección del servidor DNS incorrecta que dirige al usuario a un sitio web malicioso.
  - **Dirección IP incorrecta**- el servidor fraudulento proporciona una dirección IP no válida que crea efectivamente un ataque DoS en el cliente DHCP.

Video – Ataques ARP, Ataques STP y Reconocimiento CDP

Este video cubrirá lo siguiente:

- Ataque por suplantación de ARP
- Ataque de envenenamiento ARP
- Ataque de STP
- Reconocimiento CDP

Mensajes DHCP

- Los hosts transmiten solicitudes ARP para determinar la dirección MAC de un host con una dirección IP de destino. Todos los hosts de la subred reciben y procesan la solicitud de ARP. El host con la dirección IP que coincide con la de la solicitud de ARP envía una respuesta de ARP.
- Un cliente puede enviar una respuesta ARP no solicitada llamada "ARP gratuito". Otros hosts en la subred almacenan la dirección MAC y la dirección IP contenidas en el ARP gratuito en sus tablas ARP.
- Un atacante puede enviar un mensaje ARP gratuito que contiene una dirección MAC falsificada a un switch, y el switch actualizaría su tabla MAC en consecuencia. En un ataque típico, un atacante envía respuestas ARP no solicitadas a otros hosts en la subred con la dirección MAC del atacante y la dirección IP de la puerta de enlace predeterminada, configurando efectivamente un ataque man-in-the-middle.
- Hay muchas herramientas disponibles en Internet para crear ataques ARP man-in-the-middle.
- IPv6 utiliza el protocolo de descubrimiento de vecinos ICMPv6 para la resolución de direcciones de capa 2. IPv6 utiliza el protocolo de descubrimiento de vecinos ICMPv6 para la resolución de direcciones de capa 2.
- La falsificación de ARP y la intoxicación por ARP se mitigan mediante la implementación de la inspección dinámica de ARP (DAI).

Ataques de suplantación de dirección

- La suplantación de direcciones IP es cuando un atacante secuestra una dirección IP válida de otro dispositivo en la subred o usa una dirección IP aleatoria. La suplantación de direcciones IP es difícil de mitigar, especialmente cuando se usa dentro de una subred a la que pertenece la IP.
- Los agentes de amenaza cambian la dirección MAC de su host para que coincida con otra dirección MAC conocida de un host de destino. El switch sobrescribe la entrada actual de la tabla MAC y asigna la dirección MAC al nuevo puerto. Luego, sin darse cuenta, reenvía las tramas destinados al host objetivo al host atacante.
- Cuando el host de destino envía tráfico, el switch corregirá el error, realineando la dirección MAC al puerto original. Para evitar que el switch devuelva la asignación del puerto a su estado correcto, el atacante puede crear un programa o script que constantemente enviará tramas al switch para que el switch mantenga la información incorrecta o falsificada.
- No hay un mecanismo de seguridad en la capa 2 que permita a un switch verificar la fuente de las direcciones MAC, que es lo que lo hace tan vulnerable a la suplantación de identidad.
- La suplantación de direcciones IP y MAC se puede mitigar mediante la

Ataques STP

- Los atacantes de red pueden manipular el Protocolo de árbol de expansión (STP) para realizar un ataque falsificando el puente raíz y cambiando la topología de una red. Los atacantes pueden capturar todo el tráfico para el dominio del switch inmediato.
- Para realizar un ataque de manipulación de STP, el host atacante transmite unidades de datos de protocolo de puente STP (BPDU) que contienen cambios de configuración y topología que forzarán los recálculos de árbol de expansión. Las BPDU enviadas por el host atacante anuncian una prioridad de puente inferior en un intento de ser elegidas como root bridge.
- Este ataque STP es mitigado implementando BPDU guard en todos los puertos de acceso. BPDU Guard se discute con más detalle más adelante en el curso.

Reconocimiento CDP

Cisco Discovery Protocol (CDP) es un protocolo de detección de enlaces de capa 2 patentado. Está habilitado en todos los dispositivos de Cisco de manera predeterminada. Los administradores de red también usan CDP para configurar dispositivos de red y solucionar problemas. La información de CDP se envía a través de puertos habilitados para CDP en transmisiones periódicas, sin cifrar y sin autenticar. La información de CDP incluye la dirección IP del dispositivo, la versión de software de IOS, la plataforma, las funcionalidades y la VLAN nativa. El dispositivo que recibe el mensaje de CDP actualiza la base de datos de CDP.

Para mitigar la explotación de CDP, se debe limitar el uso de CDP en los dispositivos o puertos. Por ejemplo, se debe deshabilitar CDP en los puertos de extremo que se conectan a dispositivos no confiables.

- Para deshabilitar CDP globalmente en un dispositivo, use el comando **no cdp run** Para habilitar CDP globalmente, use el comando **cdp run**.
- Para deshabilitar CDP en un puerto, use el comando de configuración de interfaz **no cdp enable**. Para habilitar CDP en un puerto, use el comando de configuración de interfaz **cdp enable**.

Nota: Link Layer Discovery Protocol (LLDP) también es vulnerable a los ataques de reconocimiento. Configure **no lldp run**para

10.6 Módulo de práctica y cuestionario

¿Qué aprendí en este módulo?

- Las terminales son particularmente susceptibles a ataques malware que se originan a través de correo electrónico o el navegador web, como DDOS, filtración de datos y malware. Estos puntos terminales suelen utilizar características de seguridad tradicionales basadas en host, como antivirus / antimalware, firewalls basados en host y sistemas de prevención de intrusiones (HIPS) basados en host. Los puntos terminales están mejor protegidos por una combinación de NAC, software AMP basado en host, un dispositivo de seguridad de correo electrónico (ESA) y un dispositivo de seguridad web (WSA).
- AAA es un modo de controlar quién tiene permitido acceder a una red (autenticar), controlar lo que las personas pueden hacer mientras se encuentran allí (autorizar) y qué acciones realizan mientras acceden a la red (contabilizar).
- El estándar IEEE 802.1X define un control de acceso y un protocolo de autenticación basado en puertos que evita que las estaciones de trabajo no autorizadas se conecten a una LAN a través de los puertos de switch acceso público.
- Si la capa 2 se ve comprometida, todas las capas superiores también se ven afectadas. El primer paso para mitigar los ataques a la infraestructura de capa2 es comprender el funcionamiento subyacente de la capa2 y las amenazas de la infraestructura de capa 2: Port Security, DHCP snooping, DAI, y IPSG. No funcionarán a menos que los protocolos de administración estén asegurados.

¿Qué aprendí en este módulo? (continuación)

- Los ataques por saturación de MAC se aprovechan de esta limitación con direcciones MAC de origen falsas que colman la tabla de direcciones MAC del switch y saturan el switch.
- El salto de VLAN permite que otra VLAN pueda ver el tráfico de una VLAN sin cruzar primero un router.
- Un ataque doble-etiqueta a una VLAN es unidireccional y funciona únicamente cuando el atacante está conectado a un puerto que reside en la misma VLAN que la VLAN nativa del puerto troncal.
- El salto de VLAN y los ataques de doble etiquetado de VLAN se pueden evitar mediante la implementación de las siguientes pautas de seguridad troncal:
  - Deshabilitar troncal en todos los puertos de acceso.
  - Deshabilitar troncal automático en enlaces troncales para poder habilitarlos de manera manual.
  - Asegúrese de que la VLAN nativa solo se use para los enlaces troncales.
- Los dos tipos de ataques DHCP son inanición y suplantación de identidad. Ambos ataques pueden ser mitigados implementando DHCP snooping.

¿Qué aprendí en este módulo? (continuación)

- Ataque ARP: un atacante puede enviar un mensaje ARP gratuito al switch y el switch podría actualizar su tabla MAC de acuerdo a esto. Ahora el atacante envía respuestas ARP no solicitadas a otros hosts en la subred con la dirección MAC del atacante y la dirección IP de la puerta de enlace predeterminada. La suplantación de identidad ARP y el envenenamiento ARP son mitigados implementando DAI.
- Abordando el ataque de suplantación de identidad; la suplantación de identidad de una dirección IP es cuando un atacante secuestra una dirección IP valida de otro dispositivo en la subred o usa una dirección IP AL azar. Los agentes de amenaza cambian la dirección MAC de su host para que coincida con otra dirección MAC conocida de un host de destino. La suplantación de identidad de direcciones IP y direcciones MAC puede ser mitigada implementado IPSG.
- Ataque STP; el amenazante manipula STP para conducir un ataque suplantando puente de ruta y cambiando la topología de la red. Los actores de amenazas hacen que su host aparezca como un puente de ruta; por lo tanto capturan todo el trafico para el dominio del Switch inmediato. Este ataque STP es mitigado implementando BPDU Guard en todos los puertos de acceso.
- La información de CDP se envía por los puertos con CDP habilitado en transmisiones periódicas sin encriptar. La información de CDP incluye la dirección IP del dispositivo, la versión de software de IOS, la plataforma, las funcionalidades y la VLAN nativa. El dispositivo que recibe el mensaje CDP actualiza su base de datos CDP, la información suministrada por el CDP puede también ser usada por un atacante para descubrir vulnerabilidades en la infraestructura de la red. Para mitigar la


CISCO