GESTIÓN Y SOPORTE DE SEGURIDAD EN HARDWARE Y SOFTWARE

Controles de acceso

Unidad 1

ESCUELA DE CONSTRUCCIÓN E INGENIERÍA

Director: Marcelo Lucero Yañez

ELABORACIÓN

Experto disciplinar: Felipe Reyes Cáceres

Diseñador instruccional: Antonio Colmenares Prieto

Editora instruccional: María José Fonseca Palacios

VALIDACIÓN

Experto disciplinar:

Jefa de Diseño Instruccional: Alejandra San Juan Reyes

EQUIPO DE DESARROLLO

Didactic

AÑO

2022

Tabla de contenidos

Aprendizaje esperado

Configuran seguridad de acceso a switch de capa 2, considerando software y topología Packet Tracer.

Determinan acciones de implementación de seguridad en acceso para plataformas informáticas, considerando versiones y estandarizaciones vigentes.

Introducción

La dependencia tecnológica ha llevado a una mayor preocupación por la ciberseguridad gracias a las principales prácticas comerciales de las empresas que utilizan la información.

En el mundo actual altamente dependiente de la tecnología, las empresas deben ser conscientes de las amenazas que plantean las vulnerabilidades informáticas. Estos representan un riesgo significativo para sus sistemas e información.

En esta ocasión, estudiaremos lo relacionado a las vulnerabilidades y la implementación y configuraciones de elementos de seguridad.

1. Consideraciones finales de seguridad

Los profesionales de seguridad de redes deben mitigar los ataques dentro de la infraestructura de Capa 2, incluida la suplantación de direcciones MAC, la manipulación de STP, el desbordamiento de la tabla de direcciones MAC, las tormentas de LAN y los ataques de VLAN. El primer paso para mitigar tales ataques es comprender las amenazas potenciales que plantea la infraestructura de capa 2. La capa 2 puede ser un eslabón muy débil para las capas OSI más altas, porque si la capa 2 se ve comprometida, los piratas informáticos pueden ascender. Los profesionales de la ciberseguridad deben recordar que los ataques de

Capa 2 a menudo requieren acceso desde el interior, ya sean empleados o invitados. Otra consideración clave son los desbordamientos de búfer. Los desbordamientos de búfer son a menudo la fuente de ataques DoS.

La independencia de la capa 2 presenta desafíos desde el punto de vista de la seguridad, porque si una capa se ve comprometida, las otras capas no lo saben, por lo que también están expuestas. La seguridad de la red es tan segura como su eslabón más débil, que suele ser la capa de enlace de datos. Para ayudar a prevenir la explotación de la Capa 2, las aplicaciones deben validar cuidadosamente la entrada del usuario. Estos datos pueden contener datos con formato incorrecto, secuencias de control o datos excesivos, como un desbordamiento de búfer. Cabe recordar que las vulnerabilidades de desbordamiento de búfer intentan sobrescribir la memoria de la aplicación. Los desbordamientos de búfer son probablemente el método más común para atacar aplicaciones en Internet en la actualidad. Se utilizan más comúnmente para obtener privilegios de root o iniciar ataques DoS.

2. Consideraciones de seguridad de capa 2

Los switches de capa 2 funcionan a través de una tabla de direcciones de control de acceso a medios (MAC). La tabla de direcciones MAC del conmutador registra lo siguiente: la dirección MAC del hardware

aprendida y el puerto físico asociado en el que se vio la dirección por última vez. Las tramas de datos intercambian direcciones MAC solo dentro de la red LAN y no se pueden identificar fuera de la red LAN. Los conmutadores de Capa 2 pueden asignar VLAN a puertos de conmutador específicos, que a su vez existen en diferentes subredes de Capa 3.

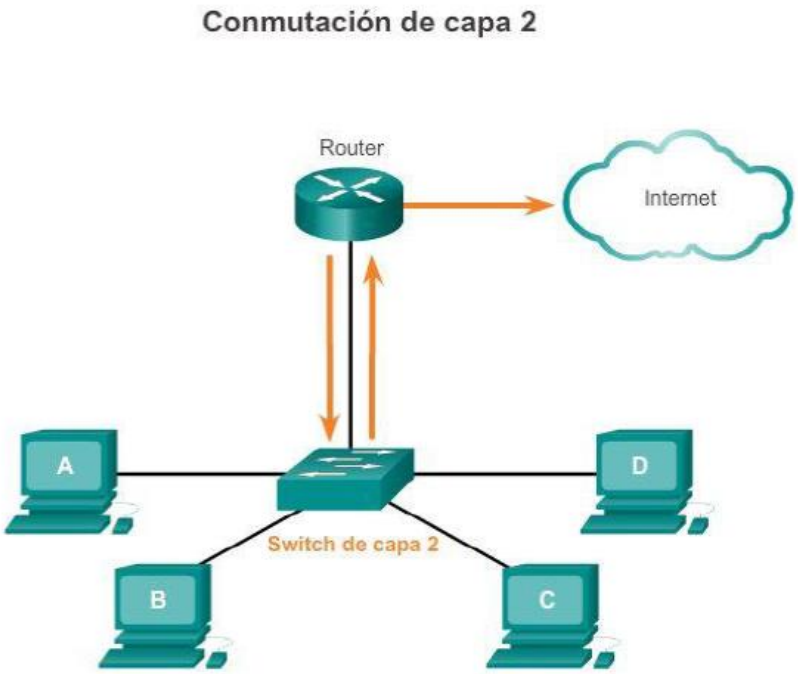

Figura 1. Conmutación de capa 2
Fuente: CCNA Security 210-260 Official Cert Guide (2016)

La capa 3 maneja el enrutamiento de paquetes a través del direccionamiento lógico y el control de subred. Los enrutadores son los dispositivos de red más comunes en la Capa 3 (concentradores, conmutadores y enrutadores). Este es responsable de enrutar los paquetes a sus respectivas direcciones IP (Protocolo de Internet) de

destino. En la capa 3, las direcciones IP de origen y destino de cada paquete se comparan con la tabla de enrutamiento de IP correspondiente y se determina el siguiente salto (a un enrutador o conmutador) en la ruta del paquete. Si la IP de destino no se encuentra en la tabla, el paquete se descartará a menos que haya un enrutador predeterminado. Esta es la razón por la que el proceso de enrutamiento suele ser sensible a la latencia.

3. Configuración de la seguridad del Switch

Ataques de Capa 2	**Descripción del ataque**	**Solución**
Ataques de Mac	Spoofing de MAC Ataques de tabla MAC	Port-Security
Manipulación de STP	Switches intrusos para romper la topologia spanning tree protocol	Port Fast Bpdu-Guard Root-Guard

Tormentas de Broadscast	Ocurren cuando: Errores en el stack del protocolo Mala configuración Ataques Dos	Storm-Control
Ataques VLAN	Vlan hopping Double Taggin Vlan Hopping	

Los Switch se utilizan para conectar dispositivos en la misma red, son los encargados de controlar el flujo de datos en la capa de acceso y de dirigirlos a los recursos de la red.

Es importante dejar claro que la seguridad básica del switch no evita los ataques malintencionados. Por ello es necesario hacer cambios en la configuración. Podemos configurar el switch, bien sea conectándonos SSH o telnet, o mediante la interfaz virtual (VLAN1) dándole una IP. En la mayoría de fabricantes esta VLAN1 viene activa de fábrica (Tomad nota, ya esta la primera cosa a desactivar y eso que llevamos poco de post).

Desbordamiento de direcciones MAC

La tabla de direcciones MAC de un switch contiene las direcciones MAC relacionadas con cada puerto físico y la VLAN asociada para cada puerto. Cuando un switch de la La capa 2 recibe una trama y el conmutador busca la dirección MAC de destino en la tabla de direcciones MAC. Si la dirección MAC tiene una entrada en la tabla, el conmutador reenvía la trama al puerto correspondiente. Si la dirección MAC no existe en la tabla de direcciones MAC, el conmutador utilizará la trama para inundar todos los puertos excepto el puerto que recibió la trama. Este es el problema, la tabla de direcciones MAC tiene un límite de tamaño y los ataques de inundación de MAC explotan este límite para sobrecargar el conmutador y utilizar direcciones MAC de origen falsas.

How to Solve

La forma más sencilla de mitigar este tipo de ataque es deshabilitar todos los puertos de conmutador no utilizados. Usando el comando show run podemos ver los puertos

Para deshabilitar una interfaz, navegamos hasta ella y la deshabilitamos:

Switch(config)#interface fastethernet 1/0

Switch(config-if)# shutdown

Si queremos inhabilitar un rango de puertos utilizamos el siguiente comando:

Switch(config)# interface range módulo primer-número - último-número

Switch(config)# interface range fastethernet 1/0 – 20/0

Switch(config-if)# shutdown

Snooping DHCP

El snooping DHCP es una familia de técnicas utilizadas para proteger la infraestructura DHCP existente. Nos permite determinar qué puertos de switch pueden responder a las solicitudes de DHCP al identificar los puertos como confiables o no confiables.

El DHCP Snooping es necesario para prevenir los ataques de tipo «man-in-the-middle».

Cuando DHCP Snooping está habilitado, todos los puertos son "no confiables" de manera predeterminada. Cuando una PC cliente envía un mensaje DHCPDISCOVER y DHCP Snooping está habilitado, el conmutador solo enviará mensajes de difusión DHCP a puertos "de confianza". Los puertos "de confianza" son los únicos puertos que permiten enviar mensajes de respuesta DHCP como DHCPOFFER.

Para configurar el snooping DHCP seguimos los siguientes pasos:

Switch(config)# ip dhcp snooping

Switch(config)# ip dhcp snooping vlan número

Switch(config-if)# ip dhcp snooping trust [limit rate pps]

Trust indica que el puerto es confiable y limit rate el limite de solicitudes DHCP falsas aceptadas en peticiones por segundo)(limit rate es opcional)

Switch# show ip dhcp snooping

#Muestra la configuracion del DHCP SNOOPING

Como adicional, se puede ver la importancia del DHCP Snooping luego de que la red de que algunas organizaciones puede ocurrir inesperadamente una denegación de servicio, uno de los factores puede ser que el servidor DHCP que el interno instaló en una de las computadoras, y que puede estar caído en la red durante algún tiempo.

Seguridad de puertos

Una buena estrategia para la seguridad de los puertos es limitar la cantidad de direcciones MAC válidas permitidas. Solo las direcciones MAC de dispositivos legítimos pueden acceder a la red. Cualquier intento no autorizado se considera una violación de la seguridad.

Existen tres maneras de configurar la seguridad de puerto:

- **Dirección MAC Estática:** Almacenada en una tabla y añadida a la configuración. [conmutador puerto-dirección mac segura dirección mac]

- **Dirección MAC dinámica:** la dirección MAC se detecta dinámicamente y se almacena solo en la tabla de direcciones. Las

direcciones MAC configuradas de esta manera se eliminan cuando se reinicia el conmutador.

• **Direcciones MAC permanentes:** estas direcciones MAC se pueden descubrir dinámicamente o configurar manualmente, luego se almacenan en la tabla de direcciones y se agregan a la configuración en ejecución.

Ataques STP

STP (Spanning Tree Protocol) Es un protocolo utilizado en redes para evitar bucles de nivel 2 en nuestra topología al conectar diferentes segmentos de red. Cada paquete STP se denomina BPDU (Unidad de datos de protocolo de puente). El switch envía la BPDU con la dirección MAC única de su puerto como MAC de origen y la dirección de multidifusión como MAC de destino.

Hay dos tipos de BPDU: configuración y notificación de cambio de topología (TCN). El primero se envía periódicamente para indicar la configuración de la red, mientras que el segundo se envía cada vez que se detecta un cambio de red (activación/desactivación de puertos).

¿Cuál es la pregunta?

• STP es confiable, sin estado y no tiene un mecanismo de autenticación fuerte.

• De forma predeterminada, el conmutador LAN acepta cualquier BPDU.

El protocolo permite que los dispositivos interconectados abran o cierren automáticamente los enlaces de conexión, lo que garantiza que la topología esté libre de bucles.

Como resultado, un atacante puede enviar tramas BPDU falsas a la red, lo que hace que el dispositivo vuelva a calcular las rutas, consume recursos, provoca inestabilidad en la red y, en última instancia, denegación de servicio. red para que parte del tráfico saliente se envíe a la computadora atacante, donde se inspecciona y se envía de regreso a la red

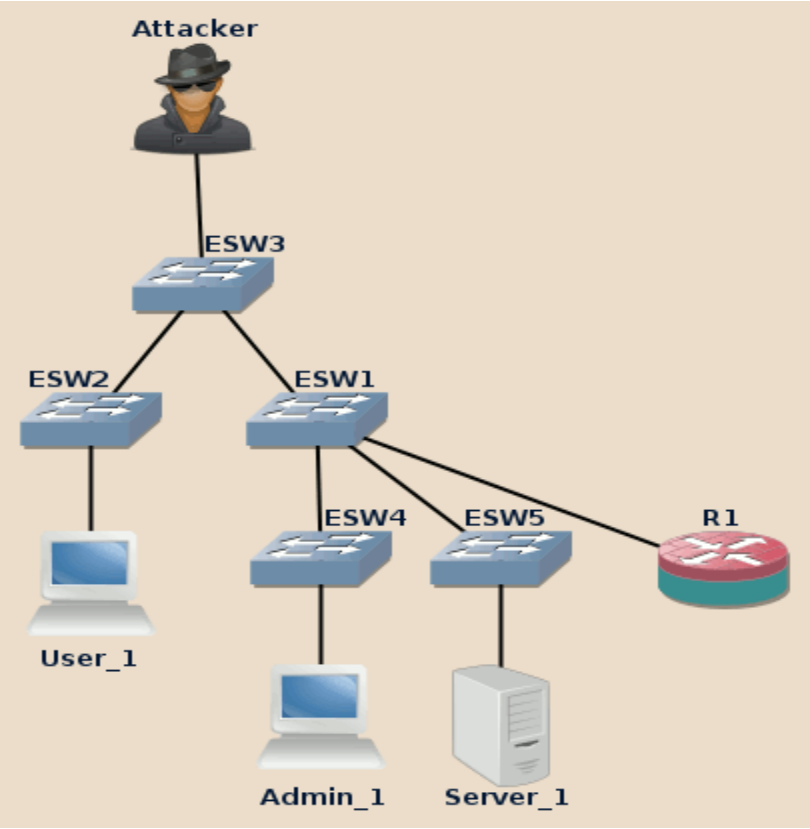

Figura 2. Conmutación de capa 2

Fuente: CCNA Security 210-260 Official Cert Guide (2016)

El protocolo establece un identificador para cada puente y selecciona el que tiene la prioridad más alta (número de prioridad más bajo) como el puente raíz. (Puente raíz) Este puente raíz establecerá la ruta de menor costo para todas las redes.

Un atacante puede enviar un mensaje BPDU anunciándose como puente con prioridad 0. De esta manera, puede ver los marcos que no debería (esto permite ataques MiM, DoS, etc.), lo que combinado con la inundación de MAC puede permitir que se capturen más marcos.

4. Configuración de protocolos Span y Rspa

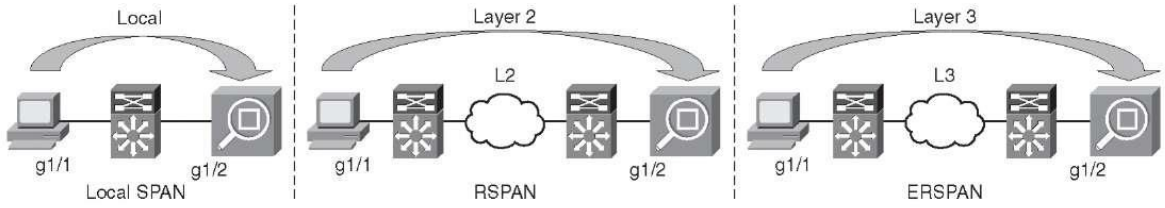

Figura 3. Configuración

Fuente: CCNA Security 210-260 Official Cert Guide (2016)

¿Cómo configurar SPAN RSAPN y ERSPAN?

Hay una respuesta simple a esta pregunta. Estos acrónimos se refieren a las diferentes capacidades de los conmutadores orientados a la gestión del tráfico. Y, gracias a ellos, se pueden realizar diferentes acciones.

¿Qué son SPAN, RSAPN y ERSPAN?

Antes de aprender a configurar SPAN, RSAPN y ERSPAN, es útil comprender qué son. SPAN (Switch Port Analyzer) le permite capturar el tráfico que ingresa y sale de los puertos de conmutación. Luego los envía a otro host conectado a su red, no importa, es un sniffer.

Por su parte, RSAPN (Remote Switch Port Analyzer) también se enfoca en capturar el tráfico y exportarlo a través de un puerto de switch, enviándolo a cualquier otro puerto de la red. Utiliza una VLAN específica llamada Remote SPAN VLAN, que mueve a los usuarios de una fuente a otra según nuestras necesidades. Es fundamental entender cómo configurar SPAN, RSAPN y ERSPAN.

ERSPAN (Encapsulating Remote Switch Port Analyzer) es una característica que solo es compatible con ciertos modelos/IOS, como Cisco Catalyst 6500 Series. Nos permite capturar el tráfico de uno o más puertos de origen o VLAN y enviarlo a cualquier otro destino. A diferencia de los otros dos tipos, con él podemos enviar usuarios a través de una red enrutada, esto hay que tenerlo en cuenta para entender cómo se configuran SPAN, RSAPN y ERSPAN.

Es importante saber la diferencia entre estos tres, ya que cada uno tiene sus propias características. De esta forma evitamos errores que pueden pasar desapercibidos al principio, pero que luego se vuelven problemáticos.

¿Cómo configurar SPAN, RSAPN y ERSPAN?

La configuración de SPAN, RSAPN y ERSPAN se divide en tres secciones, una específica para cada función. Esto hace que sea más fácil tratar con cada uno de ellos.

Ahora que sabemos qué es SPAN, veamos cómo se configura: esta función captura todo el tráfico entrante y saliente por defecto, comenzando en el puerto 1 y enviando la captura al 6. No obstante, podemos pensar en cómo configurar SPAN, RSAPN y ERSPAN con diferentes modificaciones.

A la hora de configurar SPAN, RSAPN y ERSPAN, debemos saber que con el primero podemos captar únicamente tráfico entrante o saliente. Para modificarlo, solo necesitamos ingresar el siguiente comando.

Switch#configure terminal

Switch(config)#monitor session 1 source interface Gi0/1 rx

Switch(config)#monitor session 1 source interface Gi0/1 tx

Switch(config)#monitor session 1 source interface Gi0/1 both

Al ingresar el último comando "ambos", hacemos que el conmutador acepte tanto el tráfico entrante como el saliente, es importante entender cómo se configuran SPAN, RSAPN y ERSPAN. Podemos comprobar que no hay errores en esta serie de comandos.

Switch#show monitor session all

Session 1

Type: Local Session

Source Ports:

Both: Gi0/1

Destination Ports: Gi0/6

Encapsulation: Native

Ingress: Disabled

De esta forma tan sencilla podemos realizar la configuración de SPAN especialmente en routers Cisco. Casi no lleva tiempo y es, sin duda, uno de los procesos más fáciles de ejecutar cuando se pregunta cómo configurar SPAN, RSAPN y ERSPAN.

El siguiente paso consiste en procesar la segunda de las tres funciones. La configuración es tan simple como implementar este código.

Switch1#configure terminal

Switch1(config)#vlan 999

Switch1(config-vlan)#name Remote_span_VLAN

Switch1(config-vlan)#remote-span

Switch1(config-vlan)#exit

Switch1(config)#monitor session 2 source Gi0/1

Switch1(config)#monitor session 2 destination remote vlan 999

Switch2#configure terminal

Switch2(config)#vlan 999

Switch2(config-vlan)#name Remote_span_VLAN

Switch2(config-vlan)#remote-span

Switch2(config-vlan)#exit

Switch2(config)#monitor session 5 source remote vlan 999

Switch2(config)#monitor session 5 destination interface Gi0/3

Un aspecto importante a considerar al considerar cómo configurar SPAN, RSAPN y ERSPAN es el modelo de enrutador. Si esto fue hace algunos años, es posible que nos haya pedido que configuremos el "puerto reflector", que se hace al final del comando donde indicamos la VLAN de destino. Elija siempre un destino que no esté ocupado.

Finalmente, para comprender cómo configurar SPAN, RSAPN y ERSPAN, debe saber cómo modificar ERSPAN. El proceso puede variar de

computadora a computadora, pero para evitar problemas, veremos la forma básica de hacerlo.

Switch1#configure terminal

Switch1(config)#monitor session 5 type erspan-source

Switch1(config-mon-erspan-src)#source interface Gi0/1

Switch1(config-mon-erspan-src)#destination

Switch1(config-mon-erspan-src-dst)#erspan-id 100

Switch1(config-mon-erspan-src-dst)#ip address…

Switch1(config-mon-erspan-src-dst)#origin ip address…

Con estos comandos configuramos el switch 1, que es el puerto de origen por donde saldrá el tráfico. La dirección IP que usaremos debe especificarse en el código: en la línea de dirección IP especificaremos la dirección del interruptor 2 y en la siguiente línea la dirección de la primera línea, este es un aspecto importante para entender cómo configurar SPAN , RSAPN y ERSPAN.

Así, a la hora de configurar el segundo *switch*, introduciremos este código.

Switch2#configure terminal

Switch2(config)#monitor session 5 type erspan-destination

Switch2(config-mon-erspan-dst)#destination interface Gi0/3

Switch2(config-mon-erspan-dst)#source

Switch2(config-mon-erspan-dst-src)#erspan-id 100

Switch2(config-mon-erspan-dst-src)#ip address…

5. Vulnerabilidades de acceso de cuentas de acuerdo al Sistema Operativo a Windows server

Una cuenta de Microsoft es una cuenta en línea que se utiliza para iniciar sesión en Outlook.com, Hotmail.com y otras identificaciones de correo electrónico. También se puede usar para iniciar sesión en otros servicios y dispositivos de Microsoft, como XBox Live, Windows Phone y más. Windows 8 también puede usarlo para iniciar sesión en su PC. Por lo tanto, debe proteger su cuenta de Microsoft y mantenerla segura.

Aquí hay algunas cosas que puede hacer para ayudar a proteger su cuenta de Microsoft.

1. No hace falta decir que cree una contraseña segura. Aún mejor, use caracteres ASCII para crear contraseñas y contraseñas más seguras, porque tener una contraseña segura es muy importante. No uses la misma contraseña en todas partes. Puede verificar la seguridad de su contraseña con Microsoft Password Checker o Password Security Scanner.

2. Habilite la verificación en dos pasos en su cuenta de Microsoft. La verificación en dos pasos significa que Microsoft le pedirá dos datos cada vez que acceda a su cuenta. Por ejemplo, podría ser su contraseña y un código que se enviará a su teléfono o correo electrónico registrado.

3. Habilite funciones de seguridad adicionales para su cuenta de Microsoft. Manténgase al tanto de su actividad reciente, use códigos de recuperación y opte por recibir notificaciones de seguridad.

4. Haga que su computadora con Windows 8 sea una computadora confiable.

5. Agregue la información de seguridad necesaria a su cuenta y asegúrese de que esté siempre actualizada. Obtendrá esta configuración en Contraseña e información de seguridad.

6. Manténgase alerta, manténgase alejado y evite las estafas de phishing que pueden pedirle que visite un enlace e ingrese las credenciales de su cuenta de Microsoft.

7. No revele su ID de correo electrónico principal en ningún lugar ni en ningún otro lugar. Si es necesario, cree una ID de correo electrónico secundaria si necesita distribuirla a un sitio web, correo electrónico, suscripción, etc.

8. También es posible que desee fortalecer la configuración de privacidad de su cuenta de Microsoft.

9. Consulte también estos consejos generales básicos para proteger su cuenta de correo electrónico.

6. Vulnerabilidades de acceso de cuentas de acuerdo al Sistema Operativo a Linux server

A pesar del creciente volumen de delitos cibernéticos, muchas empresas dispuestas a invertir en medidas de seguridad adecuadas están mejor protegidas hoy que en el pasado. Las soluciones y prácticas de seguridad están evolucionando rápidamente para adaptarse a las nuevas amenazas y ayudar a las empresas a mantenerse a la vanguardia.

Sin embargo, no todas las empresas están dispuestas a realizar las inversiones necesarias y, por supuesto, no todas las amenazas son vistas de la misma manera. Si bien las empresas ciertamente emplearán soluciones de seguridad básicas como firewalls y antivirus, no todos harán las inversiones necesarias en seguridad de cuentas privilegiadas y seguridad de usuarios. Para el control de inventario, muchos optan por las medidas integradas estándar proporcionadas por su software y sistemas.

Linux, en particular, tiene la reputación de ser menos vulnerable al malware, pero, de hecho, sus cuentas privilegiadas son

extremadamente vulnerables a la piratería y el abuso por parte de personas maliciosas internas. Echemos un vistazo más de cerca a cómo controlar a los usuarios privilegiados en Linux, qué medidas de seguridad proporciona Linux listas para usar para ayudar a proteger las cuentas privilegiadas y qué tan bien funcionan realmente.

Al igual que Windows, Linux presenta varios tipos de cuentas:

Superusuario o raíz: esta es una cuenta administrativa predeterminada que permite un control total del sistema, similar a la cuenta de administrador de Windows. Los privilegios de raíz de Linux permiten a un usuario ejecutar cualquier comando y controlar cualquier servicio y cualquier otra cuenta, cambiar los permisos de usuario, agregar usuarios a grupos y más.

Usuario normal: esta es una cuenta normal con un conjunto limitado de derechos de usuario de Linux. No puede acceder a ningún recurso o servicio crítico del sistema y requiere autorización de usuario root para ejecutar ciertos comandos.

Usuario del sistema: una cuenta de usuario con el mismo nivel de privilegios que un usuario normal, reservada para el uso de varias aplicaciones. Estas cuentas se utilizan para otorgar ciertos permisos a las aplicaciones o aislarlas por motivos de seguridad.

Linux proporciona una gran flexibilidad para su cuenta. Si lo desea, puede crear varias cuentas raíz de Linux y asignar diferentes permisos a cuentas o grupos de cuentas. También puede cambiar directamente los

permisos de lectura, escritura y ejecución de ciertos archivos o directorios, así como su propiedad, especificando directamente los permisos del usuario sobre estos archivos. Sin embargo, toda esta flexibilidad es una espada de doble filo, lo que facilita que los delincuentes o el malware experto en tecnología abusen o roben datos protegidos.

Al final del día, la cuenta raíz es el punto más vulnerable del sistema porque requiere acceso a archivos y configuraciones protegidos, y Linux tiene varias formas integradas para proteger dicha cuenta.

Seguridad de cuenta privilegiada

Cualquier cuenta raíz activa siempre debe estar protegida con una contraseña, Linux le pedirá que configure una durante la instalación o la primera vez que decida usar la cuenta raíz. Sin embargo, usar la cuenta raíz directamente no es la práctica más segura para una organización, especialmente si tiene varios administradores de sistemas.

Un mejor enfoque es usar una cuenta normal y usar el comando su o sudo para habilitar temporalmente los privilegios de root. Estos dos comandos realizan tareas similares: le permiten delegar derechos administrativos a cuentas normales, pero funcionan de forma ligeramente diferente. Para usar su, su administrador necesita conocer la contraseña de su propia cuenta y la contraseña de root. Si bien esto puede proporcionar una capa adicional de protección en caso de que su cuenta se vea comprometida, no es ideal desde la perspectiva de una amenaza interna.

Cualquier cuenta raíz activa siempre debe estar protegida con una contraseña, Linux le pedirá que configure una durante la instalación o la primera vez que decida usar la cuenta raíz. Sin embargo, usar la cuenta raíz directamente no es la práctica más segura para una organización, especialmente si tiene varios administradores de sistemas.

Un mejor enfoque es usar una cuenta normal y usar el comando su o sudo para habilitar temporalmente los privilegios de root. Estos dos comandos realizan tareas similares: le permiten delegar derechos administrativos a cuentas normales, pero funcionan de forma ligeramente diferente. Para usar su, su administrador necesita conocer la contraseña de su propia cuenta y la contraseña de root. Si bien esto puede proporcionar una capa adicional de protección en caso de que su cuenta se vea comprometida, no es ideal desde la perspectiva de una amenaza interna.

Herramientas de monitoreo de Linux incorporadas

Linux tiene muchos comandos que permiten a los usuarios privilegiados acceder a los registros y monitorear el uso de varios recursos del sistema. Las más básicas son herramientas de nivel superior que brindan una visión general dinámica de todos los procesos que se están ejecutando actualmente. No solo puede verificar la utilización de los recursos del sistema, sino que también puede ver todos los comandos ejecutados y otra información útil que puede brindarle una idea de lo que están haciendo los usuarios.

Linux también es conocido por su sniffer de red integrado. A diferencia de herramientas similares de Windows, no solo le permite ver el tráfico de la red en tiempo real, sino que también lo captura para un análisis posterior, lo que proporciona una buena visibilidad del uso de la red.

En general, Linux tiene capacidades de monitoreo incorporadas bastante potentes, pero está diseñado principalmente para el mantenimiento técnico y la resolución de problemas. No puede presentar datos de una manera conveniente o simplemente describir las acciones del usuario, lo que lo hace muy limitado para la detección de amenazas internas.

Si bien Linux tiene muchas herramientas integradas para controlar y proteger cuentas privilegiadas, este nivel de protección es insuficiente en un entorno de ciberseguridad moderno. Con el tiempo surgen nuevas amenazas y vulnerabilidades, y Linux no es inmune. Si realmente desea proteger su sistema Linux, debe usar una solución profesional de administración de acceso privilegiado y monitoreo de usuarios privilegiados que le permita comprender completamente quién está conectado con cuentas privilegiadas y qué están haciendo.

7. Métodos de validación de ingresos a las Plataformas TI

A continuación, se muestran todas las validaciones y las validaciones realizadas en un sistema TI. De esta manera, los programas verificados se

pueden verificar en cada paso de verificación y se intenta determinar por qué se bloqueó un intento de acceso. La lista también indica si esta validación la realiza siempre el sistema por defecto, o si ya no es posible validar (por ejemplo, deshabilitada):

• **Verificar Credenciales:** Verifica que la persona tenga una credencial de acceso registrada, no esté bloqueada y se encuentre dentro del período de vigencia.

• **Verificar Suspensión de expedientes:** Verificar en los expedientes de todo el personal si se encontraban suspendidos a la fecha de su visita. Debe haber al menos un rol activo (sin suspensión) para que el acceso sea válido.

• **Nivel de Validación:** Comprueba todos los roles de la persona para ver si algún rol no valida el nivel (en este caso, Acceso Válido). Bueno, si el dispositivo solo controla la entrada o la salida, el nivel actual de la persona debe ser igual al nivel de la fuente del dispositivo. Si el dispositivo controla ambos sentidos, el nivel actual de la persona debe ser igual al nivel de origen o de destino del dispositivo.

• **Validar Controles Anti-Passback:** Verifique todos los archivos del personal para ver si hay archivos que no validen los Controles Anti-Passback (acceso válido en este caso). Luego, verifique que el destino solicitado sea igual al último lugar que visitó la persona, es decir, donde ya estuvo la persona. Si es el mismo lugar y no ha pasado el tiempo de verificación antisubmarina, se deniega el acceso.

• **Verificar la zona horaria de la ubicación:** Verifique los archivos que se considerarán para la persona, si alguno de ellos no verifica la zona horaria de la ubicación (en este caso, acceso válido). Luego, verifique si alguno de ellos no tiene una lista de franjas horarias asociadas a la ubicación o franja horaria del día de la semana solicitado (en estos casos, el acceso no es válido). Luego verifique si la hora de la solicitud de acceso está dentro del marco de tiempo de la fecha correspondiente (o, si el día es feriado, dentro del marco de tiempo del feriado).

• **Validar horario de rol:** Verifica que alguno de los roles que se van a considerar para el individuo no valida el horario de rol (en este caso acceso válido). Luego, verifique si alguno de ellos no tiene escala, la fecha correcta para la validación o el período de tiempo definido para ese día (en estos casos, la visita no es válida).

8. Buenas prácticas de autentificación en plataformas Informáticas Windows y Linux server

El aprovechamiento de la nueva infraestructura tecnológica y maximizar la seguridad con políticas centradas en la identidad y las credenciales de PKI reducirá significativamente el riesgo de atacar con éxito sus propios sistemas o los de sus clientes. Al adoptar un enfoque centrado en la identidad para la seguridad de TI, puede bloquear sistemas y procesos

críticos y asegurarse de tener control total sobre quién puede acceder a qué infraestructura tecnológica.

• Integrar tokens OTP y credenciales basadas en certificados en los sistemas de control de acceso e identidad y ordenar su uso desde los niveles más altos de la organización. El segundo factor de autenticación solo es válido cuando se usa y solo cuando se requiere. El éxito requerirá un fuerte liderazgo de la alta dirección y una estricta aplicación de las políticas de seguridad de la empresa.

• Priorizar la implementación en función del riesgo potencial, comenzando por los administradores y ejecutivos del sistema. Bloquee las debilidades críticas, como la capacidad de crear nuevas cuentas de usuario con privilegios de administrador del sistema y otras amenazas típicas, para evitar que los atacantes entren en la infraestructura.

• Para ponerse en marcha rápidamente, comience con una contraseña de un solo uso (OTP) y evolucione rápidamente a un certificado PKI en una tarjeta cifrada. Con el tiempo, se deben completar nuevas utilidades como las firmas digitales y el cifrado de mensajes.

• Evite que las credenciales de autenticación residan en la PC mediante el uso de dispositivos portátiles de seguridad personal, como tarjetas de identificación corporativas encriptadas o contraseñas de un solo uso en tokens portátiles o móviles. La creación de la segunda línea de defensa debe ser completamente independiente de la computadora, lo que requeriría que un atacante ingrese a dos sistemas completamente

separados, ya que cualquier ataque sería inútil sin acceso a equipos auxiliares.

• Requerir autenticación de dos factores en todas las aplicaciones nuevas, ya sean remotas o en la nube. Habilita soluciones de autenticación sólidas que interactúan con sistemas de inicio de sesión único, lo que aumenta la eficiencia y la seguridad del usuario. Por ejemplo, se puede aplicar en el ámbito de las aplicaciones sanitarias de receta electrónica, cuando se trata de dispensación de medicamentos, las recetas online se pueden firmar digitalmente con certificados electrónicos, garantizando así su validez.

• Establecer un proceso de aprovisionamiento de identidad para garantizar el vínculo entre los usuarios individuales y sus credenciales personales.

• Para algunos escenarios comunes, como credenciales olvidadas, perdidas y robadas, es necesario desarrollar procedimientos seguros y completos que puedan ejecutarse de manera anormal mientras se cumplen todas las políticas para acceder a las copias de seguridad. Algunas tareas de soporte muy básicas, como el restablecimiento de PIN, deben automatizarse.

Cierre

Después de estudiado lo correspondiente a la semana, se puede destacar lo siguiente:

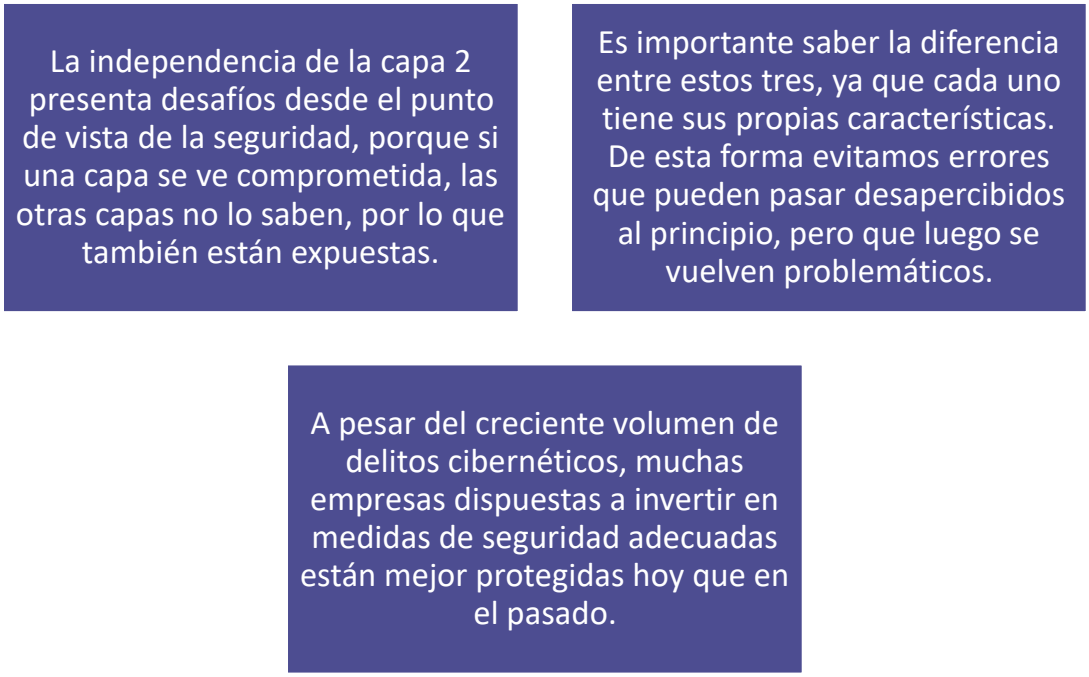

Figura 4. Ideas Claves, semana 3

Fuente: Reyes, F. (2022)

Referencias bibliográficas

CCNA Security 210-260 Official Cert Guide (Santos, Stuppi 2016)