GESTIÓN Y SOPORTE DE SEGURIDAD EN HARDWARE Y SOFTWARE

Unidad 3

Autenticación y protocolos de seguridad

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

Aplican protocolos de continuidad operacional y recuperación de desastres en red.

Implementan protocolos ante amenazas comunes de seguridad, considerando funcionamiento de infraestructura de red corporativa.

Introducción

Uno de los activos intangibles más importantes para cualquier organización es la información. Es evidente que sin ella cualquier empresa o institución dejaría de funcionar ya que sin duda es un elemento imprescindible en su día a día. Para asegurar que una institución cuente con información cuando la necesite ante un imprevisto, es necesario implementar un proceso preventivo conocido como "backup" o "backup".

En esta ocasión revisaremos los respaldos de información, fallas en sistemas y sus formas de respaldarlos.

1. Ventajas de poseer sistemas de respaldos acordes a la información almacenada

Para lograr este objetivo de respaldo, se debe evitar que los medios de almacenamiento sean modificados, retirados o destruidos sin autorización. Peligros adicionales están asociados con este artículo. El mantenimiento de registros y datos relacionados con el funcionamiento de una empresa, como archivos informáticos o registros, es vital para mantener el control sobre los activos. Esto incluye evitar que se alteren o destruyan documentos como facturas y contratos.

También se debe considerar el aseguramiento de que los dispositivos de entrada y salida no sean manipulados además de los datos que pueden ser sustraídos o robados de equipos como computadoras de escritorio, portátiles, impresoras y teléfonos inteligentes.

Esto sucede porque ciertas organizaciones no logran crear un proceso para eliminar datos de los dispositivos y se atrasan en la creación de controles adecuados para la eliminación de datos, esto ha tenido consecuencias negativas para estas organizaciones, la mayoría de las cuales son corporaciones, como:

- La pérdida de reputación y terreno legal.
- Los datos que carecen de control en medios de almacenamiento externo materializan amenazas, así como otros datos como amenazas potenciales.
- Daños causados por incendios, agua, contaminación y accidentes; daño al equipo; daños por polvo; corrosión; congelación; y daño físico.
- Los accidentes causados por radiaciones, como las electromagnéticas o térmicas, también entran en esta categoría.
- La manipulación de la información incluye la manipulación de software y hardware, la recuperación de datos descartados, la manipulación de hardware, el espionaje en proximidad, la recuperación de equipos de fuentes interceptadas y el compromiso de la información.

- Las fallas del sistema de información debido a problemas técnicos incluyen fallas o mal funcionamiento del equipo, así como fallas del software.

- Los grandes sistemas de información con muchos usuarios también pueden sobrepoblarse y colapsar.

- Además, exponer la confiabilidad de la mantenibilidad del sistema de información puede causar fallas en el funcionamiento.

- La falsificación del uso de software o equipos da lugar a acciones ilegítimas: la copia de software, el uso de software o hardware falsos y la corrupción de datos son ejemplos.

- El uso ilegal de datos también puede implicar el procesamiento ilegal de datos. significa mitigar el riesgo a través de controles de acuerdo con el esquema de clasificación elegido por la organización, es necesario establecer procedimientos para la gestión de los medios informáticos extraíbles.

Es adecuado desechar de manera segura y adecuada cualquier medio que ya no se necesite. Esto debe hacerse a través de los canales establecidos. Durante el transporte más allá de los límites físicos de la organización, los medios que contienen información deben protegerse contra la corrupción, el mal uso o el acceso por parte de personal no autorizado.

2. Criterios para definir la información que debe ser respaldada

La información es un activo intangible importante que muchas empresas e instituciones necesitan. Sin él, sus operaciones diarias se detendrían. Para garantizar que las organizaciones tengan acceso a este recurso necesario cuando sea necesario, deben implementar un proceso denominado "copia de seguridad" o "copia de seguridad". Este proceso no pretende simplemente copiar información de un lugar a otro; más bien, tiene la intención de crear una red de seguridad en caso de que ocurra algo catastrófico.

Las copias de seguridad son copias de datos importantes que se crean, actualizan y utilizan a lo largo del tiempo. Esta palabra también se usa para referirse a copias de datos almacenados en aplicaciones, computadoras, bases de datos, sistemas operativos y utilidades. El motivo para crear copias de seguridad es que la información se pueda restaurar si se ha eliminado, corrompido o interrumpido de alguna otra manera.

Las copias de seguridad generalmente se realizan en dispositivos de almacenamiento secundarios, como discos duros externos, CD, unidades flash y memoria adicional. Alternativamente, se pueden realizar en computadoras que están conectadas a internet o en otras computadoras locales o remotas. Establecer prácticas institucionales ideales para crear copias de seguridad puede ser vital para la existencia continua de una empresa.

Hay casos en los que las empresas han dejado de existir después de fallas en el funcionamiento de los equipos informáticos, inundaciones, incendios o incluso ataques militantes a sus sistemas. Sin respaldos y respaldos desactualizados, es difícil recuperar la información perdida durante largos períodos de tiempo (meses o incluso años) y difícil de agregar a lo que ya existe.

Es muy importante tener en cuenta que la copia de seguridad de sus archivos y bases de datos diarios es responsabilidad del administrador de sistemas. Hay algunas excepciones, teniendo las siguientes:

El usuario debe hacer una copia de seguridad de su equipo informático si quiere asegurarse de que sus datos importantes permanezcan intactos. Además, el usuario debe respaldar con frecuencia sus archivos y bases de datos que se actualizan periódicamente. Esto se debe a que la regla 3-2-1 se aplica sobre todo a los archivos en los que el usuario otorga una gran importancia.

La regla establece que las carpetas deben tener tres subcarpetas para texto, dos subcarpetas para hojas de cálculo, una subcarpeta para imágenes, una subcarpeta para videos y documentos y otra carpeta etiquetada como "otro". Los usuarios también deben aplicar esta regla a los archivos críticos creando tres carpetas etiquetadas como "texto", "hojas de cálculo" y "desconocido".

Al mantener tres copias de seguridad de un archivo, los usuarios pueden evitar perder información debido a discos duros dañados o problemas físicos. Además, deberán conservar una copia original del expediente. La copia de datos guardados

en dos dispositivos separados evita daños en cada medio de almacenamiento, como un disco duro y una tarjeta de memoria flash.

Después de un desastre, se debe mantener una copia de la información "fuera del sitio" o en un lugar diferente al lugar de trabajo. Esto puede ser en casa, un almacén o cualquier otro lugar fuera del lugar de trabajo. Si todo el equipo de cómputo se destruye en un terremoto o incendio, al menos los datos estarán seguros en otro lugar después de un desastre, es mejor mantener varias copias fuera del sitio para garantizar que la información aún se pueda recuperar.

Cambiar la información con frecuencia da como resultado copias de seguridad frecuentes. Por ejemplo, las bases de datos de nómina deben respaldarse con mayor frecuencia si se actualizan dos veces al mes. Por el contrario, no es necesario realizar copias de seguridad de las bases de datos de reservas de vuelos con tanta frecuencia, ya que se actualizan constantemente, cualquiera debería poder ver esto.

Es importante que los usuarios realicen copias de seguridad de sus datos con regularidad; lo mismo se aplica a cualquier otro archivo que mantengan en su sistema. Sin copias de seguridad regulares, cualquier falla no planificada puede causar daños irreparables. Proporcionar un seguro de respaldo ayuda a garantizar que los datos nunca se pierdan. Comprar un seguro de automóvil contra un accidente automovilístico es equivalente a hacer una copia de seguridad periódica de los archivos en un disco duro.

3. Sistemas ante falla de servidores Windows

Existen muchas herramientas incluidas con los sistemas operativos Microsoft Windows. Estas herramientas hacen que la copia de seguridad sea un proceso simple que algunas empresas aún no tienen implementado. Algunas empresas también pueden usar estas herramientas para crear un plan de respaldo básico, incluso si aún no tienen uno. Esto se debe a que la arquitectura compleja de Windows Server 2012 no garantiza el uso de una aplicación de copia de seguridad más complicada. Las herramientas de copia de seguridad de Windows Server 2012 ya que no permiten el uso de dispositivos de copia de seguridad en cinta magnética.

Esto solo se puede hacer usando discos duros físicos; ya sea interno o externo. Los datos también se pueden respaldar y copiar en cintas a través de un método secundario: Microsoft recomienda esto como una opción de respaldo terciaria. Las versiones anteriores de Windows Server permitían realizar copias de seguridad en cinta mediante dispositivos de almacenamiento magnético.

La tecnología de virtualización Hypervisor de Microsoft se basa en la misma tecnología que Virtual PC, que usaba un formato de archivo llamado .VHD o disco duro virtual. Otras tecnologías de virtualización como VirtualBox, VMWare y Citrix XenServer también admiten el formato de archivo .VHD. Este artículo creará un sistema de copia de seguridad completamente original desde cero, lo que nos permite agregarle nuevas funciones según las necesidades específicas. La instalación de estas características requiere algunos pasos.

En primer lugar, se deben realizar las tareas necesarias. Windows Server viene instalado con una copia de respaldo de sus programas en caso de que el archivo original esté dañado o falte. En la esquina inferior derecha de Windows Server 2012, acceda al comando Ejecutar con el Administrador del servidor.

Figura 1. Administrador del servidor

Fuente: Reyes, F. (2022)

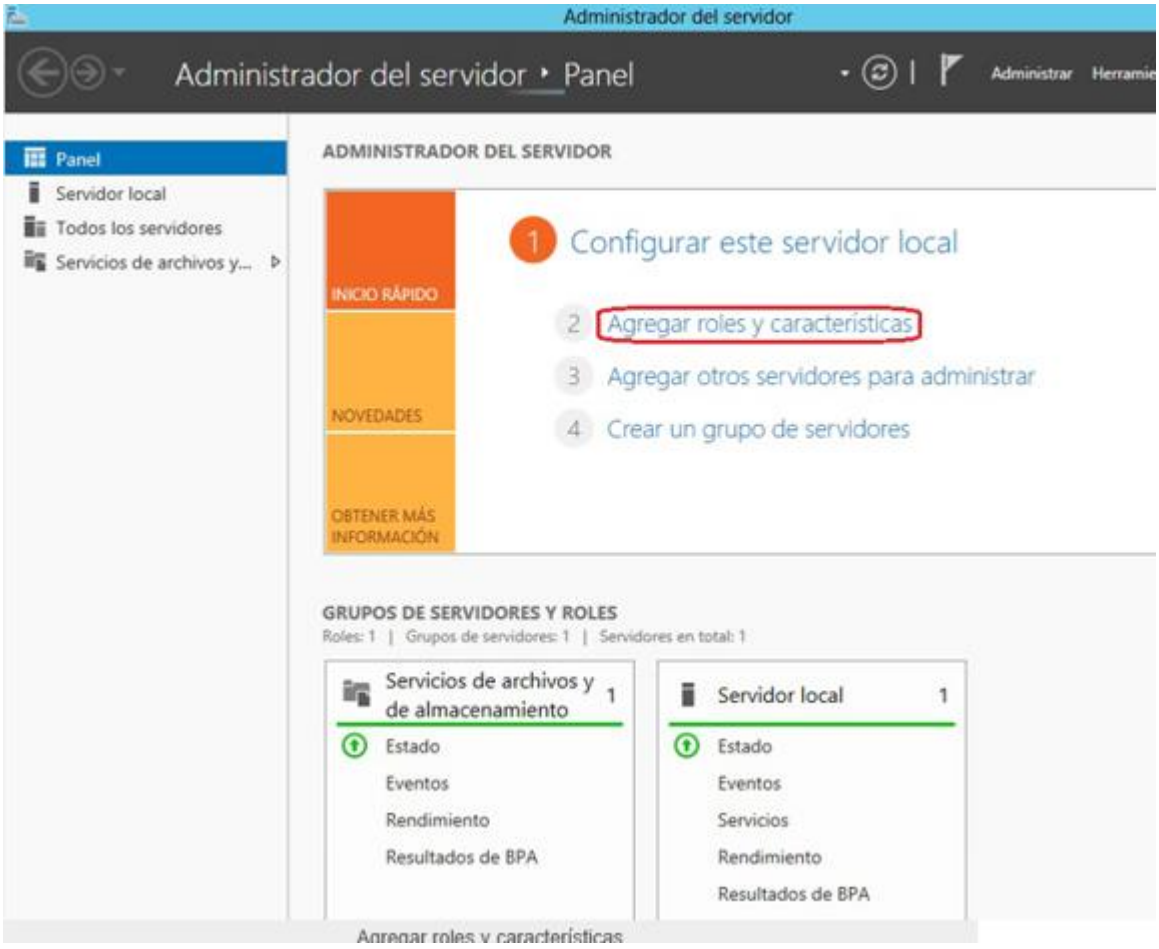

Figura 2. Agregar roles y caracteristicas

Fuente: Reyes, F. (2022)

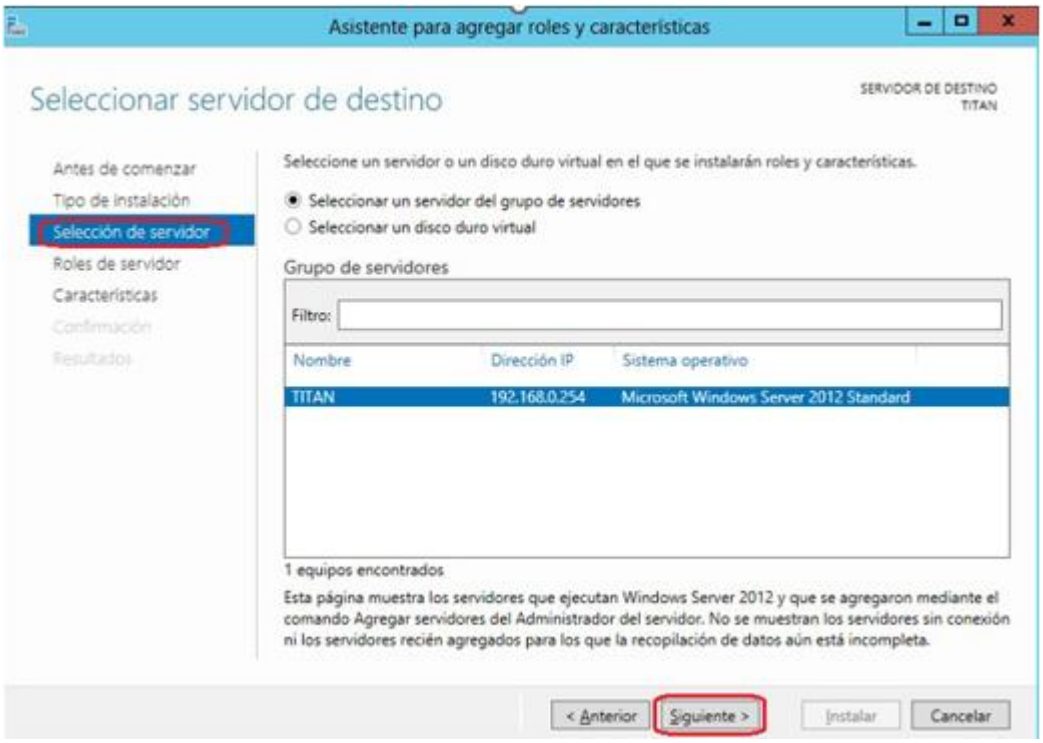

Figura 3. Asistente para agregar roles y características

Fuente: Reyes, F. (2022)

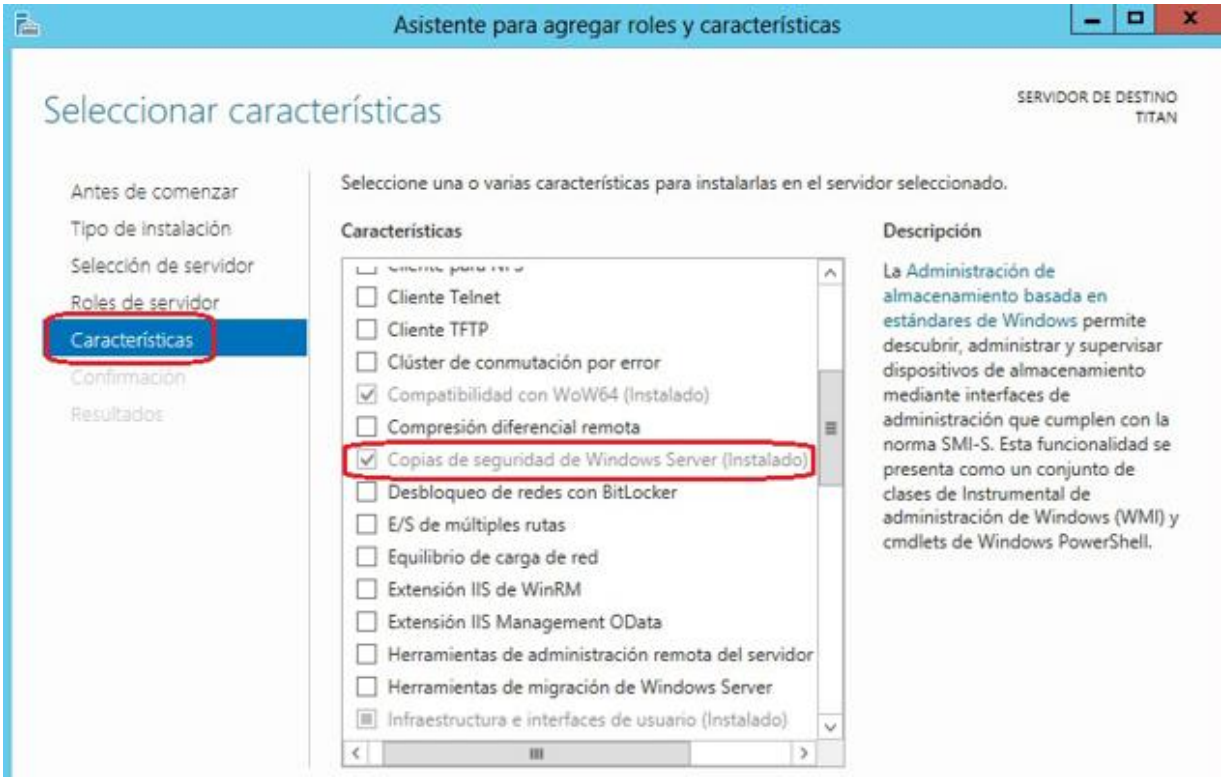

Figura 4. Selección de características

Fuente: Reyes, F. (2022)

4. Sistemas ante falla de servidores Linux

La partición raíz de un sistema Linux también se conoce como la partición "/", la unidad "/" o la partición de barra. Es donde se instala el sistema operativo y donde se deben ubicar todos los archivos del sistema. Los archivos de usuario deben ubicarse en un subdirectorio de la partición "/", mientras que cualquier otro archivo debe ubicarse en subdirectorios de /home. Pueden ocurrir problemas que son difíciles de identificar con algunas placas base cuando la partición raíz alcanza su

tamaño máximo. Esto se debe a que la partición está cerca de su capacidad máxima. Te explicamos cómo solucionar estos problemas en este tutorial. Síntomas Los problemas con los intestinos pueden causar estos síntomas: La inestabilidad del sistema es común. Es imposible reiniciar el servidor Apache. El servidor de correo electrónico no puede descargar correos electrónicos. Es imposible instalar software nuevo o actualizaciones.

Aclarar el problema requiere establecer su causa. Acceda a su servidor con SSH y use el siguiente comando para ver cuánto espacio se usa en su disco.

El motivo de la preocupación se explica en la línea misma. Acceda a su servidor a través de Secure Shell y calcule el espacio en disco con este comando:

```
df -h
```

```
Filesystem      Size  Used Avail Use% Mounted on
/dev/vda1        15G  894M   13G   7% /
tmpfs           250M     0  250M   0% /dev/shm
```

Figura 5. Cálculo de espacio

Fuente: Reyes, F. (2022)

Los problemas críticos de partición requieren atención inmediata. Si el espacio que ocupa su partición raíz alcanza o supera el 90%, debe buscar una solución. Una solución común para esto es aumentar el porcentaje de uso de su partición.

Existen muchas razones para este problema. La causa más común es cuando se está almacenando sus sitios web en una ubicación distinta de /home. Existen archivos enormes con nombres largos en el directorio /. Los programas de software grandes, como servidores para juegos en línea, se instalan en un directorio en la partición del sistema, como /usr. Por lo que se está afectado por el error mod_gzip donde pudiese existir demasiado correo electrónico en la cola para caber y los registros obsoletos se acumulan.

Además, se debe disminuir el porcentaje de archivos almacenados eliminando archivos. Mover archivos y subdirectorios en el directorio /home es todo lo que se necesita para ambos casos, además de encontrar archivos grandes que necesitan ser movidos requiere usar el comando du. Una vez encontrados, mover estos archivos se puede lograr con facilidad.

A continuación, se pueden ver algunos ejemplos del uso de du. Para ver una lista de archivos en el directorio raíz, debemos decir Supongamos que queremos ver una lista de archivos en el directorio raíz.

```
ls

a.log  b.log  c.log  d.log
```

Figura 6. Ejemplo de comando du

Fuente: Reyes, F. (2022)

El comando du proporciona el tamaño de los directorios de archivos sin reflejar sus formatos de archivo.

```
du

3411980 .
```

Figura 7. Comando du

Fuente: Reyes, F. (2022)

Cuando usamos el parámetro -chs, obtenemos un resultado más legible.

```
du -chs

3.3G    .

3.3G    total
```

Figura 8. Parámetro -chs

Fuente: Reyes, F. (2022)

El espacio total que requieren los archivos se mostrará en un formato legible con el comodín de asterisco incluido.

```
du -chs *
2.0M    a.log
30M     b.log
301M    c.log
3.0G    d.log
3.3G    total
```

Figura 9. Espacio total de archivos

Fuente: Reyes, F. (2022)

Se puede buscar el archivo más grande en un directorio ejecutando el siguiente comando.

```
ls -lh --sort=size | head -n 5
```

```
total 239.9M
-rwxr-xr-x  1 root root 85.2M Sep 22  2015 archivo1
-rwxr-xr-x  1 root root 82.7M Jul 23  2016 archivo2
-rwxr-xr-x  1 root root 37M Jul 23  2016 archivo3
-rwxr-xr-x  1 root root 35M Nov 10  2016 archivo4
```

Figura 10. Búsqueda de archivo

Fuente: Reyes, F. (2022)

5. Ataques comunes a la LAN

Una red de área local o LAN es un tipo de red que conecta computadoras y dispositivos dentro de un área específica, como un edificio u oficina. Es útil para compartir datos e información entre las computadoras de una organización; también se conoce como intranet.

El Código de la Ley de Ciberseguridad requiere que todas las redes en línea sigan protocolos de seguridad, incluidos sistemas de seguridad sólidos y controles internos estrictos. Estas prácticas ayudan a mitigar los riesgos de trabajar con estas redes. Hay amenazas de seguridad relacionadas con las redes de área local. Las brechas de seguridad pueden ser extremadamente dañinas para la reputación y las finanzas de una empresa. Incluso pueden causar la pérdida de información y datos confidenciales.

El malware también puede desencadenar la pérdida de datos, que es una de las amenazas más visibles para la seguridad de la red. Los riesgos ocultos adicionales implican: Para entender hay que escuchar:

- Alteración de datos.
- Hombre en el medio.
- Secuestro de DNS.

La creación de una red LAN segura con protocolos establecidos puede evitar la pérdida de información y datos vitales. También puede ayudar a evitar que los

atacantes accedan a información importante mediante la implementación de medidas de seguridad específicas. Las redes seguras necesitan una base sólida. Es importante seguir las normas de seguridad durante la instalación y configuración inicial del sistema, esto se debe a que los nuevos sistemas necesitan instalar una red de área local.

Es fundamental trabajar con asesores expertos al configurar un nuevo sistema, ya que se deben seguir los protocolos adecuados. Es importante tener en cuenta que tanto las empresas grandes como las pequeñas asumen la responsabilidad de la seguridad de la LAN. Deben comprender las políticas de seguridad y los niveles de seguridad presentes en cada red LAN para evitar ataques de piratas informáticos. Para mantener la seguridad, las empresas deben implementar aún más medidas de seguridad después de instalar una red LAN, esto se debe a que la instalación de una LAN no garantiza la seguridad; lo mejor que se puede hacer es agregar medidas de seguridad.

La necesidad de mantener la seguridad física de una red es necesaria, además de realizar algunas acciones que pueden fortalecer físicamente una red de área local. Estos incluyen implementar medidas de seguridad y reforzar las defensas. Para ello, se debe mantener actualizado el software y el hardware, incluidos los enrutadores y servidores.

Tambien, se debe mantener siempre actualizados todos los dispositivos con los últimos parches de seguridad. Esto mantiene una protección constante contra nuevas amenazas.

Realizar copias de seguridad de la información y los datos en un horario regular. Las contraseñas están protegidas por dos dígitos o más. Al crear una contraseña, tenga en cuenta lo siguiente cuando cree un inicio de sesión en la red o configure aplicaciones de almacenamiento o en la nube:

- Utilice al menos 8 caracteres que incluyan letras mayúsculas y minúsculas, símbolos especiales y signos de puntuación.
- Evite el uso de acrónimos para nombres o fechas que sean significativas. Tenga siempre varias contraseñas diferentes.
- Cambie siempre estas contraseñas regularmente. Para probar quién es una persona, la autenticación implica probar quién es la persona mediante la presentación de una identificación.

Se proporciona protección adicional mediante el uso de controles de seguridad biométricos como las huellas dactilares. Esto se debe a que el proceso de confirmación de las identidades de los usuarios es uno de los aspectos más comunes de una red de identidad.

Estas redes a menudo usan seguridad de nombre de usuario y contraseña como una forma de verificar a los usuarios. Soluciones de oferta de software y hardware. Cierto software y hardware pueden ayudar a que las redes se mantengan seguras, estos incluyen programas que brindan encriptación y protección contra piratas informáticos, así como hardware que evita que los usuarios reconozcan a los intrusos.

En otro orden de ideas, se debe proporcionar a los empleados un control de acceso seguro a sus lugares de trabajo, además de administrar el control de acceso permite a los administradores determinar quién está usando una red y decidir si se otorga o no acceso a una red a usuarios específicos. Los permisos para dispositivos conectados a la misma LAN, como impresoras, también se pueden administrar a través del control de acceso.

6. Ataques de reconocimiento

Los atacantes pueden atacar varios tipos de redes, incluidas aquellas con códigos maliciosos y hacks. Los programadores reconocen tres tipos específicos de ataques de red: El reconocimiento no autorizado de sistemas, servicios o vulnerabilidades se denomina ataque de exploración.

El acceso indebido a datos, sistemas o privilegios puede considerarse un ataque de acceso.

En el ataque de denegación de servicio, los atacantes dañan o apagan sistemas, redes o servicios importantes. Las utilidades nslookup y whois permiten que cualquier persona en Internet encuentre fácilmente las direcciones IP que se le han dado a una empresa o entidad específica.

Al hacer ping a las direcciones IP disponibles públicamente, un atacante puede determinar rápidamente qué direcciones IP activas se han asignado a su objetivo. Usando herramientas como gping o fping, un pirata informático malicioso puede

hacer ping en cada subred o rango de direcciones. Esto les ayuda a reducir la cantidad de esfuerzo necesario para completar este paso. Es similar a alguien que hojea una guía telefónica y llama al azar a todos los números.

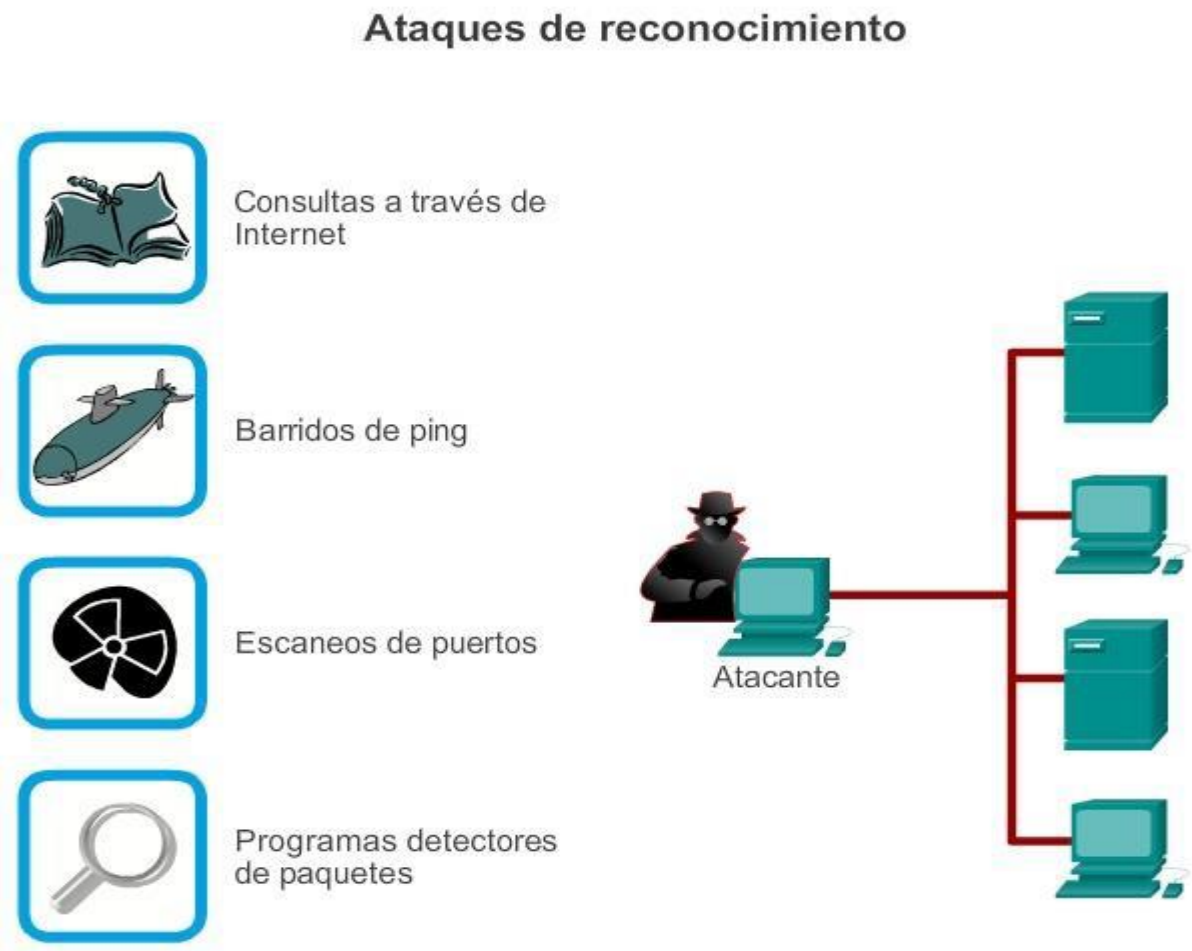

Figura 11. Ataques de reconocimiento

Fuente: ingenieriasystems.com (2017)

7. Ataques a servicios Telnet

Se necesitan mencionar algunas cosas importantes sobre Telnet al comenzar. Se refiere a la seguridad financiera y la protección contra daños. Esto a menudo incluye protocolos y procedimientos de seguridad apropiados. Un servidor Telnet se puede configurar para admitir autenticación de contraseña, autenticación AAA o ninguna autenticación.

Solo los usuarios que se han autenticado con uno de estos métodos pueden iniciar sesión e ingresar la línea de comando en el servidor. Se admite la desactivación de servicios.

Habilitar el servidor Telnet permite a los atacantes escanear fácilmente los dispositivos conectados, además de desactivar el número de puerto de escucha o desactivar el servidor Telnet por completo reduce el riesgo de que esto ocurra. Admite cambiar el número de puerto.

El número de puerto 23 es conocido como puerto de servidor Telnet, debido a esto, es vulnerable a ataques y escaneos. Cambiar el número de puerto a uno privado reduce la probabilidad de ser escaneado o atacado. Las listas de control de acceso se pueden agregar a la lista de funciones admitidas por un programa.

Los canales de línea de terminal virtual se pueden configurar mediante ACL, estas configuraciones determinan qué direcciones IP pueden conectarse a un dispositivo específico. variaciones de ataque La exploración de puertos es una actividad que consiste en examinar todos los puertos de un sistema. La información sobre el

sistema de administración de dispositivos, o NMS, puede robarse fácilmente cuando los usuarios no ocultan correctamente su actividad en la red mientras se escanean y escuchan.

Para obtener los paquetes de interacción del usuario, los atacantes escanean y escuchan en la red NMS. Los crackers de contraseñas rompen las contraseñas. Cuando un dispositivo necesita autenticarse, un atacante puede explotar el número de puerto Telnet que se descubrió y acceder al dispositivo.

Al adivinar la contraseña y eludir la autenticación, el atacante puede acceder al sistema. Interrumpir el Servicio (DoS) es un acto de negarse a aceptar una solicitud. Los servidores Telnet solo pueden admitir un número limitado de usuarios a la vez. Cuando se alcanza este límite, otros usuarios no pueden acceder al servidor, incluso si lo usan habitualmente. Esto puede suceder cuando se está utilizando el servidor o cuando está siendo atacado.

8. Ataques de saturación de tabla de conmutación

Un ataque MAC Flooding puede tener muchas formas y objetivos. Algunos se centran en los datos y las contraseñas, mientras que otros intentan que el sistema no funcione correctamente. Otros espían a los usuarios o roban información. Esto significa que debemos tener cuidado al protegernos de los ataques.

¿A qué se refiere la palabra clave MAC Flooding? Cada dispositivo que se conecta a la red tiene una dirección MAC única. Esta dirección es necesaria para identificar el enrutador y sirve como identificador. Además, es necesario poder navegar por Internet, y cada dirección MAC es única.

Una dirección física consta de seis bloques de dos dígitos hexadecimales, cuando un atacante corrompe una tabla de direcciones MAC, crea una inundación al sobrecargar los conmutadores con solicitudes entrantes. Estas solicitudes colapsan la tabla y, en última instancia, interrumpen el tráfico entre diferentes puertos. Al interceptar el tráfico entrante cada vez que atacan con éxito, este modo hace que el conmutador sature la dirección MAC de cada puerto, esto se conoce como cruce de direcciones MAC o ataque exitoso.

Las tablas de datos del switch registran direcciones MAC individuales y las asocian con puertos específicos. Esto permite que el conmutador asigne direcciones dinámicamente a medida que enruta el tráfico. Debido a que cada puerto solo reenvía datos a través de la interfaz correcta, el conmutador minimiza el tráfico en la red mientras sigue transmitiendo datos a través del canal adecuado.

El atacante inunda la mesa con miles de direcciones MAC falsas segundos después de lanzar este ciberataque. Esto obstruye rápidamente la tabla y evita que se procesen las entradas legítimas. Al cambiar a través de todos los puertos, este dispositivo expone a los usuarios a rastreadores que capturan tanto su tráfico como su privacidad. Y debido a esto, cambiar de puerto expone vulnerabilidades tanto de seguridad como de privacidad. Diferentes switches tienen diferentes tamaños

máximos de tabla de direcciones. Es importante tener esto en cuenta al crear un proyecto en la escuela. Para evitar un ataque de colapso casi seguro de Manticore, siga estos pasos.

Es crucial proteger nuestro equipo, ya que es esto es especialmente importante ya que contamos con funciones y herramientas que pueden proteger nuestros sistemas de invasiones y reducir el riesgo de ataques. Las empresas deben comprender que la privacidad y la seguridad son preocupaciones vitales. Cada estación de trabajo debe proporcionar estas funciones; de lo contrario, no son únicos.

Esto se puede encontrar en los conmutadores de red comúnmente utilizados por las empresas. existen restricciones portuarias. Esta función limita la cantidad de direcciones MAC que se pueden aprender en cada puerto para limitar el tamaño de la tabla de aprendizaje. Una vez que la tabla se llena, todas las entradas restantes se descartan para que no ocurra el ataque MAC Flooding, se asigna una dirección fija a cada Mac.

También, puede optar por configurar el conmutador para que solo procese paquetes con una dirección MAC estática. De esta manera, solo se pueden procesar paquetes de MAC específicos. Cierra los puertos que no necesitemos usar. La desactivación de puertos no utilizados proporciona el más alto nivel de seguridad, esto evita que personas no autorizadas accedan al sistema a través de la inundación del puerto. Además, les impide obtener cualquier información sobre el sistema protegido. Evite conectarse a otros dispositivos debido a los problemas

de alta saturación de direcciones MAC, necesitando encontrar una solución para aumentar la seguridad. Esto podría lograrse al no permitir que se realicen nuevas conexiones a la máquina actual.

9. Ataques VLAN

Las grandes y medianas empresas de todo el mundo se enfrentan diariamente a ciberataques con el objetivo de acceder a sus sistemas y datos. Estos hackers solo buscan robar información sensible, productos, procesos e incluso usuarios.

Un método que utilizan los atacantes para obtener acceso es el salto de VLAN. Esta técnica furtiva pasa por alto las redes corporativas saltando entre redes virtuales. La configuración incorrecta de VLAN y la falta de conocimiento sobre la administración adecuada de la red pueden dañar gravemente la reputación de una empresa y costarles miles de dólares.

En consecuencia, es vital implementar planes inmediatos de prevención, monitoreo y defensa contra fugas de datos. Para planificar una estrategia de gestión de incidentes de seguridad para el negocio de interfaces de sistemas abiertos de capa 2.

El salto de VLAN presenta una amenaza constante para las empresas de todos los tamaños. Cuando un atacante criminal viola una red de área local virtual (VLAN) para saltar entre ellos, está cometiendo un salto de VLAN. El salto de VLAN les permite atacar hosts moviéndose de VLAN a VLAN sin ser notados. Esto brinda a

los delincuentes la opción de robar datos, propagar spyware, instalar malware e incluso secuestrar otros recursos.

Durante la jornada laboral, cualquier momento en que se produzca un salto de vLAN puede permitir el acceso a cualquier perfil dentro de la red. Esto se puede lograr a través de dos vías principales: Falsificó la identidad de los interruptores cambiando a una falsificación. La forma más común de falsificación de puertos Ethernet la logra el atacante haciéndose pasar por un conmutador en la red de la víctima, esto hace que DTP cree un enlace troncal, dando al atacante acceso a todos los datos que pasan de un punto a otro y la capacidad de viajar de LAN a LAN sin ser notado.

Este tipo de ataque solo puede ocurrir cuando los puertos Ethernet están configurados en el modo de trabajo Automático o Deseable en los conmutadores de Cisco. El etiquetado doble o doble etiquetado se denomina # 2 en esta lista. Un atacante puede eludir la seguridad de la red cambiando a una nueva etiqueta de trama Ethernet.

Después de este cambio, sus etiquetas de marco se fusionan en un solo grupo. Estas etiquetas combinadas se interpretan como una VLAN, lo que permite al atacante acceder a la red corporativa y transmitir y recibir datos a su antojo. ¿Cómo se debe evitar que personas ajenas violen una red privada virtual? Cualquier intento de saltar a través de las VLAN requiere un plan sólido y un monitoreo constante. Para evitar esto, las empresas deben seguir un plan de trabajo estructurado que supervise la actividad del sistema y el cumplimiento de la seguridad en las capas

OSI. Además, es necesario fortalecer el cumplimiento de la protección de datos y las capas primarias del modelo OSI.

La implementación de soluciones de software SIEM brinda a las empresas opciones de ciberseguridad personalizables que reflejan sus características únicas. Estos programas pueden automatizar muchas operaciones de ciberseguridad, rastrear violaciones de datos, evitar que personas ajenas accedan a información segura y mejorar la gestión de TI.

Para vencer las amenazas de salto de VLAN, siga estos pasos. Para evitar la propagación de contaminantes, es imperativo que nos concentremos en la prevención, las grandes y medianas empresas incluyen gran parte de su seguridad en capas más profundas de sus sistemas. A menudo dejan abierta la dinámica de conexión entre el hardware y el software, centrándose en las capas más externas. Esto facilita que las personas atraviesen el tráfico diario.

Al coordinar los esfuerzos del software de seguridad y los especialistas de TI, se pueden implementar medidas de defensa efectivas desde el principio. El equipo de TI debe identificar cuáles son los objetivos del perpetrador mediante la consulta con el software de seguridad.

Una vez que se ha logrado esto, se pueden implementar procesos automatizados para detectar amenazas, adherirse a protocolos y fortalecer áreas específicas del sistema. Antes de cometer un delito, los ciberdelincuentes analizan el sistema de seguridad de su objetivo para encontrar vulnerabilidades. Es por eso que usar el modelo ATT&CK puede ayudar a su equipo a identificar el enfoque y la ruta de un

atacante antes de cualquier incursión en su red. Proporcionar información sobre las maniobras ofensivas. Es difícil para el software convencional identificar las etapas de reconocimiento de un atacante. Estos se realizan a través de análisis de ciberseguridad de la empresa en busca de entradas fáciles, análisis de su infraestructura y configuraciones de TI, así como análisis de sus capacidades de contraataque.

Es necesario que los especialistas en TI cierren todas las debilidades entre sus programas y dispositivos antes de que el atacante las implemente. Además de la información básica sobre la empresa, como su nombre y ubicación, se puede realizar un inventario de sus recursos y hardware para descubrir para qué los usa la gente, cuántos recursos hay disponibles y cualquier debilidad en la fábrica. Otro ejemplo es examinar los patrones de comportamiento de una empresa para determinar cómo operan.

Ciertos enrutadores tienen configuraciones predeterminadas que les otorgan acceso a toda la red. Deshabilitar estos modos es crucial, al igual que desactivar las interfaces no utilizadas. También es vital desactivar Dynamic Trunk Port, Auto y otros modos que otorgan acceso al enrutador. Al realizar un ataque de doble etiquetado, es importante utilizar una VLAN diferente para el tráfico de datos común. Realice un seguimiento del software y el hardware para detectar cualquier amenaza interna.

10. Ataques DHCP

Aunque las computadoras tienen una dirección que cambia constantemente, en algunas ocasiones no se puede acceder a la red, eso problema llama la atención, sin estar seguro de la validez de mi dirección IP o si se tiene permiso del servidor DHCP. No es posible encontrar direcciones IP ilegales si aún no las ha encontrado.

¿Cómo se llama la indagación de DHCP?

También se conoce como DHCP DHCPing. Los conmutadores de red de alto rendimiento utilizan una tecnología de seguridad de capa 2 conocida como DHCP Snooping.

Este sistema descarta todas las comunicaciones DHCP que no son aceptadas por el sistema operativo. Evita que los servidores DHCP maliciosos asignen direcciones IP a los clientes DHCP. Como resultado se producen las siguientes actividades: Los mensajes no válidos no deben filtrarse; en su lugar, utilice otros medios para confirmar que los mensajes DHCP son válidos.

Permite un fácil acceso a la información sobre hosts no seguros con arrendamientos de IP. Utilice la base de datos de vinculación de escuchas de DHCP para buscar hosts no confiables que realicen solicitudes adicionales. Los inspectores determinan sus hallazgos examinando la escuela. Para comprender cómo funciona DHCP Snooping, debemos comprender el protocolo de configuración de host dinámico o DHCP. Cuando DHCP está habilitado en una red, los dispositivos en la red sin una dirección IP interactuarán con el servidor DHCP a

través de cuatro etapas. La Figura 2 muestra dos tipos de puertos de switch: confiables y no confiables.

Los puertos de confianza provienen de servidores en los que confía el servidor DHCP; los puertos no confiables provienen de servidores no confiables. De forma predeterminada, un conmutador separa automáticamente sus interfaces en estas dos categorías. Cuando DHCP Snooping está habilitado, las ofertas de DHCP solo pueden viajar a través de puertos confiables. De lo contrario, será ignorado. Se crea una tabla de enlaces DHCP basada en el mensaje DHCPACK. Registra la dirección MAC del host, la dirección IP alquilada y el tiempo de cesión. Además, la tabla almacena información sobre la interfaz del host, como el número de VLAN y el tipo de enlace, y sus opciones de DHCP asociadas. Si se recibe un paquete DHCP posterior de un host que no es de confianza, como uno que no coincide con la información de la tabla, no se procesará.

DHCP Snooping protege contra ataques comunes al bloquearlos antes de que sucedan, un ataque de suplantación de DHCP es realizado por alguien que cambia su dirección IP para hacerse pasar por otro sistema. Un atacante puede aprovechar la suplantación de DHCP para lanzar un ataque intermedio.

Cuando responden a la solicitud de un cliente, fingen ser el enrutador o el servidor DNS, lo que les permite interceptar el tráfico de usuarios y reenviarlo a su propio destino previsto. Esto impide que los clientes utilicen los recursos de la dirección IP para ataques de denegación de servicio contra el servidor. En un ataque de inanición de DHCP, un pirata informático agota todas las direcciones DHCP

disponibles. Cuando los objetivos de un ataque de inanición de DHCP reciben una dirección de origen falsa del ataque, pueden usarla para engañar al servidor objetivo para que piense que la solicitud proviene de una fuente autorizada.

Esto hará que el servidor de destino proporcione todas las direcciones IP disponibles en su grupo. Debido a que todas estas respuestas se reenvían entre sí, esto conduce a un agotamiento del conjunto de DHCP y la posterior pérdida de funcionalidad.

¿Cómo habilitar el monitoreo DHCP?

La indagación de DHCP solo protege la red a través de puertos de acceso con una VLAN configurada en un conmutador. Al implementar esta medida de seguridad, establezca siempre un puerto que no sea de confianza antes de configurar la indagación de DHCP en las VLAN que desea utilizar. Esto se debe a que los mensajes no autorizados del servidor DHCP eluden el puerto de confianza. Esto se puede hacer tanto en la GUI web como en la interfaz de línea de comandos de Switch. Los comandos se pueden encontrar en la configuración de indagación DHCP del conmutador de la serie FS S3900.

Cierre

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

se debe considerar el aseguramiento de que los dispositivos de entrada y salida no sean manipulados además de los datos que pueden ser sustraídos o robados de equipos como computadoras de escritorio, portátiles, impresoras y teléfonos inteligentes.

La indagación de DHCP solo protege la red a través de puertos de acceso con una VLAN configurada en un conmutador.

Es necesario que los especialistas en TI cierren todas las debilidades entre sus programas y dispositivos antes de que el atacante las implemente.

Figura 12. Ideas Claves, semana 7

Fuente: Reyes, F. (2022)

Referencias bibliográficas

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