

Actividad para la cartera: Usa el Marco de Ciberseguridad del NIST para responder a un incidente de seguridad

Resumen de la actividad

En esta actividad, utilizarás los conocimientos que adquiriste sobre redes a lo largo de este curso para analizar un incidente de red. Analizarás la situación utilizando el Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST) y crearás un informe del incidente que podrás incluir como parte de la documentación de tu cartera de ciberseguridad. El CSF es un marco voluntario que consiste en estándares, pautas y mejores prácticas para administrar el riesgo de ciberseguridad. Para un repaso, revisa esta lectura sobre los [marcos del NIST y las cinco funciones del marco NIST CSF](#). Crear un informe de incidentes de ciberseguridad de calidad y aplicar el CSF puede ayudarte a generar confianza y mejorar las prácticas de seguridad dentro de tu organización.

El CSF es escalable y se puede aplicar en una amplia variedad de contextos. A medida que continúes aprendiendo más y perfeccionando tu comprensión de las habilidades clave de ciberseguridad, puedes usar las plantillas proporcionadas en esta actividad en otras situaciones. Saber identificar qué medidas de seguridad aplicar en respuesta a las necesidades de la empresa te ayudará a determinar cuáles son las mejores opciones disponibles en lo que respecta a la seguridad de red.

Asegúrate de completar esta actividad antes de continuar. En la siguiente parte del curso, podrás ver un ejemplo completo para compararlo con tu propio trabajo. También te brindará la oportunidad de responder a las preguntas de la rúbrica que te permitirán reflexionar sobre los elementos clave de tu declaración profesional. No podrás acceder a los modelos hasta que hayas finalizado esta actividad.

Escenario

Analiza el siguiente caso. Luego, completa las instrucciones paso a paso.

Eres un analista de ciberseguridad que trabaja para una empresa multimedia que ofrece servicios de diseño web, diseño gráfico y soluciones de marketing en redes sociales para pequeñas empresas. Tu organización experimentó recientemente un ataque DDoS, que comprometió la red interna durante dos horas hasta que se resolvió.

Durante el ataque, los servicios de red de tu organización dejaron de responder repentinamente debido a una avalancha de paquetes ICMP entrantes. El tráfico normal de la red interna no pudo acceder a ningún recurso de la red. El equipo de gestión de incidentes respondió bloqueando los paquetes ICMP entrantes, deteniendo todos los servicios de red no críticos fuera de línea y restableciendo los servicios de red críticos. A continuación, el equipo de ciberseguridad de la empresa investigó el incidente de seguridad. Descubrieron que un actor malicioso había enviado una avalancha de pings ICMP a la red de la empresa a través de un firewall no configurado. Esta vulnerabilidad permitió al atacante malicioso saturar la red de la empresa mediante un ataque de denegación de servicio distribuido (DDoS).

Para hacer frente a este problema de seguridad, el equipo de seguridad de red implementó:

- Una nueva regla de firewall para limitar la tasa de paquetes ICMP entrantes.
- La verificación de la dirección IP de origen en el firewall para comprobar si hay direcciones IP falsas en los paquetes ICMP entrantes.
- Un software de monitoreo de red para detectar patrones de tráfico anómalos.
- Un sistema IDS/IPS para filtrar parte del tráfico ICMP basándose en características sospechosas.

Como analista de ciberseguridad, se te asigna la tarea de utilizar este evento de seguridad para crear un plan para mejorar la seguridad de red de tu empresa, siguiendo el Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST). Utilizarás el CSF para ayudarte a navegar por los diferentes pasos del análisis de este incidente de ciberseguridad e integrar tu análisis en una estrategia general de seguridad:

- Identificar los riesgos de seguridad a través de auditorías periódicas de las redes internas, los sistemas, los dispositivos y los privilegios de acceso para identificar posibles brechas en la seguridad.
- Proteger los activos internos mediante la aplicación de políticas, procedimientos, capacitación y herramientas que ayuden a mitigar las amenazas de ciberseguridad.
- Detectar posibles incidentes de seguridad y mejorar las capacidades de monitoreo para aumentar la rapidez y la eficiencia de las detecciones.
- Responder para contener, neutralizar y analizar incidentes de seguridad; implementar mejoras en el proceso de seguridad.
- Recuperar el funcionamiento normal de los sistemas afectados y restaurar los datos y/o activos de los sistemas que se hayan visto afectados por un incidente.

W Untitled Attachment

W Untitled Attachment

Actividad: Análisis del reforzamiento de la red



Resumen de la actividad

En esta actividad, se te presentará un escenario sobre una organización de redes sociales que experimentó recientemente una importante filtración de datos causada por vulnerabilidades no detectadas. Para hacer frente a la filtración, identificarás algunas herramientas comunes de refuerzo de la red que se pueden implementar para proteger la seguridad general de la organización. Luego, seleccionarás una vulnerabilidad específica de la empresa y propondrás diferentes métodos de refuerzo de la red. Por último, explicarás cómo los métodos y herramientas elegidos serán eficaces para gestionar la vulnerabilidad y cómo evitarán posibles filtraciones en el futuro.

En el curso, aprendiste prácticas de refuerzo de la red y prácticas de refuerzo relacionadas con la seguridad de red, como el filtrado de puertos, los privilegios de acceso a la red y el cifrado en las redes. Las prácticas de refuerzo de la red ayudan a las organizaciones a monitorear amenazas y ataques potenciales en su red y a prevenir que ocurran algunos ataques. Algunas de estas prácticas se implementan todos los días, mientras que otras se ejecutan de vez en cuando, como cada dos semanas o una vez al mes. Comprender cómo utilizar las herramientas y métodos de refuerzo de la red te ayudará a monitorear mejor la actividad de la red y proteger la red de tu organización contra diversos ataques.

Asegúrate de completar esta actividad antes de continuar. En la siguiente parte del curso, podrás ver un ejemplo completo para compararlo con tu propio trabajo. No podrás acceder al modelo hasta que hayas finalizado esta actividad.

Escenario

Revisa el siguiente escenario. Luego, completa las instrucciones paso a paso.

Eres un analista de seguridad que trabaja para una organización de redes sociales. La organización experimentó recientemente una importante filtración de datos, que ha puesto en peligro la seguridad de la información personal de sus clientes, como nombres y direcciones. Tu organización quiere implementar prácticas sólidas de refuerzo de la red que puedan llevarse a cabo de forma coherente para evitar ataques y filtraciones en el futuro.

Después de inspeccionar la red de la organización, descubres cuatro vulnerabilidades importantes. Estas vulnerabilidades son las siguientes:

1. Los empleados de la organización comparten las contraseñas.
2. La contraseña del administrador de la base de datos es la predeterminada.
3. Los firewalls no tienen reglas establecidas para filtrar el tráfico que entra y sale de la red.
4. No se utiliza la autenticación multifactor (MFA).

Si no se toman medidas para abordar estas vulnerabilidades, la organización corre el riesgo de experimentar otra filtración de datos u otros ataques en el futuro.

En esta actividad, redactarás una evaluación de riesgos de seguridad para analizar el incidente y explicar qué métodos se pueden utilizar para proteger aún más la red.

Selecciona 3 herramientas y métodos de reforzamiento a implementar

1. Políticas de gestión de contraseña las cuales consten siempre de cambiar las contraseñas default además de establecer la longitud de las contraseñas de por lo menos 12 caracteres normales y 3 especiales
2. Usar la autentificación multifactor para los empleados
3. Además formar los métodos de no compartir contraseñas amenos de que sea por un canal específico y justificado
4. Implementar un SIEM para gestionar las alertas que puedan entrar y monitorear

Explica tus recomendaciones

Debido a la filtración de datos de implementarlos estos métodos ya que refuerzan la seguridad de la empresa ademas de monitorear con un SIEM lo que puede pasar , además que la autentificación multifactor para que nadie que no sea el que quiera ingresar pueda entrar, y cambiar las contraseñas que no sean las default.

Actividad: Instalación de software en una distribución de Linux

Introducción

En este lab, aprenderás a instalar y desinstalar aplicaciones en Linux. Utilizarás comandos de Linux en Bash para completar esta tarea lab. Además, utilizarás el gestor de paquetes Advanced Package Tool (APT) para instalar y desinstalar las aplicaciones Suricata y tcpdump.

Lo que harás

En este lab, tendrás múltiples tareas por realizar. En primer lugar, deberás confirmar la instalación de APT en Bash. En segundo lugar, utilizarás APT para instalar la aplicación Suricata y verificar que se haya instalado correctamente. En tercer lugar, desinstalarás la aplicación Suricata y pasarás a confirmar que se haya desinstalado. Cuarto, instalarás la aplicación tcpdump y enumerarás todas las aplicaciones actualmente instaladas. Por último, reinstalarás la aplicación Suricata y verificarás que tanto Suricata como tcpdump estén instalados correctamente.

- Confirma que APT está instalado en Bash
- Instala Suricata con APT
- Desinstala Suricata con APT
- Instala tcpdump con APT
- Reinstalla Suricata con APT

Instrucciones del lab

Antes de comenzar, puedes [revisar las instrucciones](#) de uso de este Qwiklabs.

Puedes intentar este lab un máximo de 5 veces, y tendrás 60 minutos para completarlo en cada intento.

¡Sigue adelante y haz clic en “Open Tool” (Abrir herramienta) para comenzar la actividad!

¿Completaste ya esta actividad? A veces es necesario actualizar la página de Coursera para que tu progreso se registre. Si actualizas esta página después de completar tu lab, debería aparecer la marca de verificación verde.

Este course utiliza una aplicación de terceros, Actividad: Instalación de software en una distribución de Linux, para mejorar tu experiencia de aprendizaje. La aplicación hará referencia a información básica, como tu nombre, correo electrónico e ID de Coursera.

Actividad: Mejora la autenticación, autorización y trazabilidad de una pequeña empresa



Resumen de la actividad

En esta actividad, evaluarás los controles de acceso utilizados por una empresa. Analizarás su proceso actual, identificarás problemas y harás recomendaciones para mejorar sus prácticas de seguridad.

Anteriormente, aprendiste que los controles de acceso son controles de seguridad que gestionan el acceso, la autorización y la responsabilidad de la información. Los controles de autenticación se utilizan para verificar quién es alguien, mientras que los controles de autorización se utilizan para otorgar permisos a un usuario y establecer límites en lo que se le permite hacer. Cuando se hacen bien, los controles de acceso son la clave para disminuir la probabilidad de un riesgo de seguridad.

Asegúrate de completar esta actividad antes de continuar. En la siguiente parte del curso, podrás ver un ejemplo completo para compararlo con tu propio trabajo. No podrás acceder al modelo hasta que hayas finalizado esta actividad.

Escenario

Analiza el siguiente caso. Luego, completa las instrucciones paso a paso.

Eres el primer profesional de ciberseguridad contratado por una empresa en expansión. Recientemente, la empresa realizó un ingreso en una cuenta bancaria desconocida. El gerente de finanzas dice que no se cometió ningún error. Afortunadamente, pudo detener el pago. El propietario te ha pedido que investigues qué sucedió para evitar futuros incidentes.

Para ello, tendrás que investigar un poco sobre el incidente para comprender mejor lo que sucedió. Primero, revisarás el registro de acceso del incidente. A continuación, tomarás notas que pueden ayudarte a identificar a un posible agente de amenaza. Luego, detectarás los problemas con los controles de acceso que fueron aprovechados por el usuario. Por último, recomendarás medidas para mejorar los controles de acceso de la empresa y reducir la probabilidad de que se repita el incidente.

Información del incidente

Tipo de evento: Información

AdsmEmployeeService

Categoría del evento: Ninguno

ID del evento: 1227

Fecha: 10/03/2023

Hora: 8:29:57 a. m.

Usuario: legal\administrador

Computadora: Up2-NoGud

IP: 152.207.255.255

Descripción:

FAUX_BANK

Hoja de trabajo de control de acceso

	Nota(s)	Asunto(s)	Recomendación(es)
Autorización / autenticación	<p>Objetivo: Anota 1-2 puntos clave de información relevante que puedan ayudar a identificar la amenaza:</p> <ul style="list-style-type: none"> • <i>¿Quién causó este incidente?</i> • <i>¿Cuándo ocurrió?</i> • <i>¿Qué dispositivo se utilizó?</i> <p>Objetivo: Basándote en tus notas, enumera 1-2 problemas de autorización:</p> <ul style="list-style-type: none"> • <i>¿Qué nivel de acceso tenía el usuario?</i> • <i>¿Debería estar activa su cuenta?</i> <p>Objetivo: Formula al menos 1 recomendación para evitar este tipo de incidentes:</p> <ul style="list-style-type: none"> • <i>¿Qué controles técnicos, operativos o de gestión podrían</i> 		

Administra directorios y archivos

Antes, exploraste cómo administrar el sistema de archivos utilizando comandos de Linux. Conociste los siguientes comandos: `mkdir`, `rmdir`, `touch`, `rm`, `mv` y `cp`. En esta lectura, revisarás estos comandos, así como el editor de texto nano, y aprenderás otra forma de escribir en archivos.

Cómo crear y modificar directorios

`mkdir`

El comando `mkdir` crea un directorio nuevo. Al igual que todos los comandos que presentamos en esta lectura, puedes ingresar el directorio nuevo como la ruta de archivo absoluta, que comienza desde la raíz, o como una ruta de archivo relativa, que comienza desde el directorio actual.

Por ejemplo, si quieras crear un directorio nuevo llamado `network` en tu directorio `/home/analyst/logs`, puedes ingresar `mkdir /home/analyst/logs/network` para crear este directorio nuevo. Si ya estás en el directorio `/home/analyst/logs`, también puedes crear este directorio nuevo al ingresar `mkdir network`.

Consejo profesional: Puedes usar el comando `ls` para confirmar que se agregó el directorio nuevo.

`rmdir`

El comando `rmdir` elimina o borra un directorio. Por ejemplo, al ingresar `rmdir /home/analyst/logs/network`, se eliminaría este directorio vacío del sistema de archivos.

Nota: El comando `rmdir` no puede eliminar directorios que contienen archivos o subdirectorios. Por ejemplo, si ingresas `rmdir /home/analyst`, obtendrás un mensaje de error.

Cómo crear y modificar archivos

`touch` y `rm`

El comando `touch` crea un archivo nuevo. Este archivo no tendrá ningún contenido dentro. Si tu directorio actual es `/home/analyst/reports`, al ingresar `touch permissions.txt`, se creará un archivo nuevo en el subdirectorio `reports`, llamado `permissions.txt`.

El comando `rm` elimina o borra un archivo. Este comando debe usarse con cuidado, ya que no es fácil recuperar archivos eliminados con `rm`. Para eliminar el archivo de permisos que acabas de crear, ingresa `rm permissions.txt`.

Consejo profesional: Para verificar que `permissions.txt` se haya creado o eliminado correctamente, puedes ingresar `ls`.

mv y cp

Si estás trabajando con archivos, también puedes usar `mv` y `cp`. El comando `mv` mueve un archivo o directorio a una ubicación nueva, y el comando `cp` copia un archivo o directorio a una ubicación nueva. El primer argumento después de `mv` o `cp` es el archivo o directorio que quieras mover o copiar, mientras que el segundo es la ubicación en la que quieras moverlo o copiarlo.

Para mover `permissions.txt` al subdirectorio `logs`, ingresa `mv permissions.txt /home/analyst/logs`. Al mover un archivo, se elimina de su ubicación original. Sin embargo, al copiarlo, esto no sucede. Para copiar `permissions.txt` en el subdirectorio `logs` y mantenerlo en su ubicación original, ingresa `cp permissions.txt /home/analyst/logs`.

Nota: El comando `mv` también puede usarse para cambiar el nombre de un archivo. Para hacerlo, ingresa el nombre nuevo como el segundo argumento en lugar de la ubicación nueva. Por ejemplo, al ingresar `mv permissions.txt perm.txt`, se cambia el nombre del archivo `permissions.txt` a `perm.txt`.

Editor de texto nano

Nano es un editor de archivos de línea de comandos disponible por defecto en muchas distribuciones de Linux. Muchos/as principiantes lo encuentran fácil de usar, y es muy utilizado en ciberseguridad. Puedes realizar varias tareas básicas en nano, como crear archivos nuevos y modificar contenido de archivos.

Para abrir un archivo existente en nano desde el directorio que lo contiene, ingresa `nano` seguido del nombre del archivo. Por ejemplo, al escribir `nano permissions.txt` desde el directorio `/home/analyst/reports`, se abre una nueva ventana de edición de nano con el archivo `permissions.txt` abierto para editar. También puedes proporcionar la ruta de acceso absoluta al archivo si no estás en el directorio que lo contiene.

Para crear un archivo nuevo en nano, ingresa `nano` seguido de un nombre de archivo nuevo. Por ejemplo, al ingresar `nano authorized_users.txt` desde el directorio `/home/analyst/reports`, se crea el archivo `authorized_users.txt` dentro de ese directorio y se abre en una nueva ventana de edición de nano.

Dado que no hay una función de guardado automático en nano, es importante que guardes tu trabajo antes de salir. Para guardar un archivo en nano, usa el atajo de teclado `Ctrl + O`. Se te pedirá que confirmes el nombre del archivo antes de guardarlo. Para salir de nano, utiliza el atajo de teclado `Ctrl + X`.

Nota: Otros editores de texto de línea de comandos populares son Vim y Emacs.

Redireccionamiento de salida estándar

Hay otra forma de escribir en archivos. Anteriormente, aprendiste sobre la entrada estándar y la salida estándar. La **entrada estándar** es información recibida por el sistema operativo a través de la línea de comandos, mientras que la **salida estándar** es la información devuelta por el SO a través del shell.

También aprendiste acerca del comando **pipe**, o pleca. El comando **pipe** envía la salida estándar de un comando como entrada estándar a otro comando, para su posterior procesamiento. Para usarlo, se ingresa el carácter pleca (**|**).

Además de la pleca (**|**), también puedes usar los operadores del signo “mayor que” (**>**) y el “doble mayor que” (**>>**) para redirigir la salida estándar.

Al usarlos con **echo**, los operadores **>** y **> >** pueden servir para enviar la salida de **echo** a un archivo específico en lugar de a la pantalla. La diferencia entre ambos es que **>** sobrescribe tu archivo existente, mientras que **>>** agrega tu contenido al final del archivo existente en lugar de sobrescribirlo. El operador **>** debe usarse con cuidado, ya que no es fácil recuperar archivos sobrescritos.

Cuando estés dentro del directorio que contiene el archivo **permissions.txt**, ingresa **echo "last updated date" >> permissions.txt** y agrega la cadena “last updated date” al contenido del archivo. Al ingresar **echo "time" > permissions.txt** después de este comando, se sobrescribe todo el contenido del archivo **permissions.txt** con la cadena “time”.

Nota: Los operadores **>** y **>>** crearán un archivo nuevo si todavía no existe uno con el nombre especificado.

Agentes de amenaza y tipos de hackers

Amenazas avanzadas persistentes

Una amenaza persistente avanzada (APT) es un conjunto de procesos informáticos sigilosos orquestados por un tercero con la intención y la capacidad de atacar de forma avanzada y continuada en el tiempo, un objetivo determinado. Las APT suelen investigar a sus objetivos (p. ej., grandes corporaciones u organismos de gobierno) con antelación y pueden permanecer indetectables por un período prolongado. Sus intenciones y motivaciones pueden incluir:

- Dañar infraestructura crítica, como la red eléctrica y recursos naturales
- Acceder a propiedad intelectual, como secretos comerciales o patentes

Amenazas internas

Estas abusan de su acceso autorizado para obtener datos que pueden perjudicar a la organizacion sus intenciones pueden ser.

- **Sabotaje**
- **Corrupcion**
- **Espionaje**

- **Acceso no autorizado o filtraciones de datos**

Hacktivistas

son agentes de amenaza que actuan por motivaciones politicas , abusan de la tecnologia para alcanzar sus metas las cuales pueden incluir

- **Manifestaciones**
- **Propaganda**
- **Campanas de cambio social**
- **Fama**

Tipos de hackers

Un hacker es cualquier persona o grupo que utiliza computadoras para acceder a datos sin autorizacion, puede tratarse de una persona sin experiencia o profesional, experta en la tecnologia que usan habilidades con diversos fines.

- **Hacker eticos, Respetan el codigo de etica y cumplen con la ley para realizar evaluaciones de riesgos de una organizacion. Su motivacion es proteger a las personas y a las organizaciones de los agentes de amenaza maliciosos.**
- **Hackers Semiautorizados: Se consideran investigadores, buscan vulnerabilidades pero no se aprovechan de ellas.**
- Los/las hackers no autorizados/as tambien se denominan hackers no éticos. Son agentes de amenaza maliciosos/as que no cumplen ni respetan la ley. Su objetivo es recopilar y vender informacion confidencial para obtener un beneficio financiero.
-

Amenazas riesgo y vulnerabilidades

Amenaza: es una circunstancia o evento que puede afectar negativamente a los activos

Riesgo: Es algo que puede afectar a la confidencialidad , integridad o disponibilidad de un activo.

Vulnerabilidad: Es una debilidad que puede ser aprovechada por una amenaza . Cabe recalcar que debe de haber una vulnerabilidad y una amenaza para que haya un riesgo.

Ransomware: es un ataque malicioso en que los agentes de amenazas encriptan los datos de una organizacin y exigen un pago para restaurar el acceso.

Impactos Claves de las amenazas riesgos y vulnerabilidades.

- **Financiero**
- **Robo de indentidad**
- **Dano a la reputacion de la empresa**

Analiza la comunicación en la capa de red

Escenario

Analiza el siguiente caso. Luego, completa las instrucciones paso a paso.

Eres un analista de ciberseguridad que trabaja en una empresa que se especializa en la prestación de servicios de consultoría informática. Varios clientes se pusieron en contacto con tu empresa para informar que no podían acceder al sitio web de la empresa www.yummyrecipesforme.com, y vieron el error “puerto de destino inalcanzable” después de esperar a que se cargara la página.

Tienes la tarea de analizar la situación y determinar qué protocolo de red se vio afectado durante este incidente. Para empezar, visitas el sitio web y también recibes el error “puerto de destino inalcanzable”. A continuación, cargas tu herramienta de análisis de red, tcpdump, y vuelves a cargar la página web. Esta vez, recibes una gran cantidad de paquetes en tu analizador de red. El analizador muestra que cuando envías paquetes UDP y recibes una respuesta ICMP devuelta a su host, los resultados contienen un mensaje de error: “udp port 53 unreachable.” (puerto udp 53 inalcanzable).

En el registro DNS e ICMP, encuentras la siguiente información:

1. En las dos primeras líneas del archivo de registro, ves la solicitud inicial saliente de tu computadora al servidor DNS solicitando la dirección IP de www.yummyrecipesforme.com. Esta solicitud se envía en un paquete UDP.
2. A continuación, encontrarás marcas de tiempo que indican cuándo ocurrió el evento. En el registro, esta es la primera secuencia de números que se muestra. Por ejemplo: 13:24:32.192571. Esto muestra el tiempo 1:24 p. m., 32.192571 segundos.
3. La siguiente es la dirección IP de origen y destino. En el registro de errores, esta información se muestra como: 192.51.100.15.52444 > 203.0.113.2.domain. La dirección IP a la izquierda del símbolo mayor que (>) es la dirección de origen. En este ejemplo, la fuente es la dirección IP de tu computadora. La dirección IP a la derecha del símbolo mayor que (>) es la dirección IP de destino. En este caso, es la dirección IP del servidor DNS: 203.0.113.2.domain
4. La segunda y tercera líneas del registro muestran la respuesta a tu paquete inicial de solicitud ICMP. En este caso, la línea ICMP 203.0.113.2 es el comienzo del mensaje de error que indica que el paquete ICMP no se pudo entregar en el puerto del servidor DNS.

5. A continuación, están el protocolo y el número de puerto, que muestra qué protocolo se utilizó para gestionar las comunicaciones y a qué puerto se entregó. En el registro de errores, esto aparece como “udp port 53 unreachable” (puerto udp 53 inalcanzable). Esto significa que el protocolo UDP se utilizó para solicitar una resolución de nombre de dominio utilizando la dirección del servidor DNS a través del puerto 53. El puerto 53, que se alinea con la extensión .domain en 203.0.113.2.domain, es un puerto bien conocido para el servicio DNS. La palabra “inalcanzable” en el mensaje indica que el mensaje no llegó al servidor DNS. Tu navegador no pudo obtener la dirección IP de yummyrecipesforme.com, que necesita para acceder al sitio web porque ningún servicio estaba escuchando en el puerto DNS receptor, como indica el mensaje de error ICMP “udp port 53 unreachable.” (puerto udp 53 inalcanzable).
6. Las líneas restantes del registro indican que los paquetes ICMP se enviaron dos veces más, pero se recibió el mismo error de entrega en ambas ocasiones.

Ahora que capturaste paquetes de datos utilizando una herramienta de análisis de red, tu trabajo consiste en identificar qué protocolo y servicio de red se vieron afectados por este incidente. Luego, tendrás que redactar un informe de seguimiento.

Como analista, puedes inspeccionar el tráfico de red y los datos de red para determinar qué está causando los problemas relacionados con la red durante los incidentes de ciberseguridad. Más adelante en este curso, demostrarás cómo gestionar y resolver incidentes. Por ahora, solo necesitas analizar la situación.

Mientras tanto, este incidente está siendo gestionado por ingenieros de seguridad después de que tú y otros analistas hayan informado del problema a tu supervisor directo.

Analiza los ataques a la red

Escenario

Revisa el siguiente escenario. Luego, completa las instrucciones paso a paso.

Trabajas como analista de seguridad para una agencia de viajes que anuncia ventas y promociones en el sitio web de la empresa. Los empleados de la empresa acceden regularmente a la página web de ventas de la empresa para buscar paquetes vacacionales que puedan gustar a sus clientes.

Una tarde, recibes una alerta automatizada de tu sistema de monitoreo que indica un problema con el servidor web. Intentas visitar el sitio web de la empresa, pero recibes un mensaje de error de tiempo de espera de conexión en tu navegador.

Utilizas un detector de paquetes para capturar los paquetes de datos en tránsito hacia y desde el servidor web. Observas un gran número de solicitudes TCP SYN procedentes de una dirección IP desconocida. El servidor web parece estar desbordado por el volumen de

tráfico entrante y está perdiendo su capacidad para responder al número anormalmente grande de solicitudes SYN. Sospechas que el servidor está siendo atacado por un actor malicioso.

Desconectas temporalmente el servidor para que el equipo pueda recuperarse y volver a un estado de funcionamiento normal. También configuras el firewall de la empresa para bloquear la dirección IP que estaba enviando el número anormal de solicitudes SYN. Sabes que tu solución de bloqueo de IP no durará mucho, ya que un atacante puede suplantar otras direcciones IP para eludir este bloqueo. Tienes que alertar a tu gerente sobre este problema rápidamente y discutir los siguientes pasos para detener a este atacante y evitar que este problema vuelva a ocurrir. Tendrás que estar preparado para contarle a tu jefe el tipo de ataque que descubriste y cómo estaba afectando al servidor web y a los empleados.

Logs del sistema

47	3.144521	198.51.100.23	192.0.2.1	TCP	42584->443 [SYN] Seq=0 Win=5792 Len=120...
48	3.195755	192.0.2.1	198.51.100.23	TCP	443->42584 [SYN, ACK] Seq=0 Win=5792 Len=120...
49	3.246989	198.51.100.23	192.0.2.1	TCP	42584->443 [ACK] Seq=1 Win=5792 Len=120...
50	3.298223	198.51.100.23	192.0.2.1	HTTP	GET /sales.html HTTP/1.1
51	3.349457	192.0.2.1	198.51.100.23	HTTP	HTTP/1.1 200 OK (text/html)
52	3.390692	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
53	3.441926	192.0.2.1	203.0.113.0	TCP	443->54770 [SYN, ACK] Seq=0 Win=5792 Len=120...
54	3.49316	203.0.113.0	192.0.2.1	TCP	54770->443 [ACK Seq=1 Win=5792 Len=0...
55	3.544394	198.51.100.14	192.0.2.1	TCP	14785->443 [SYN] Seq=0 Win=5792 Len=120...
56	3.599628	192.0.2.1	198.51.100.14	TCP	443->14785 [SYN, ACK] Seq=0 Win=5792 Len=120...
57	3.664863	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
58	3.730097	198.51.100.14	192.0.2.1	TCP	14785->443 [ACK] Seq=1 Win=5792 Len=120...
59	3.795332	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=120...
60	3.860567	198.51.100.14	192.0.2.1	HTTP	GET /sales.html HTTP/1.1
61	3.939499	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=120...
62	4.018431	192.0.2.1	198.51.100.14	HTTP	HTTP/1.1 200 OK (text/html)
63	4.097363	198.51.100.5	192.0.2.1	TCP	33638->443 [SYN] Seq=0 Win=5792 Len=120...
64	4.176295	192.0.2.1	203.0.113.0	TCP	443->54770 [SYN, ACK] Seq=0 Win=5792 Len=120...
65	4.255227	192.0.2.1	198.51.100.5	TCP	443->33638 [SYN, ACK] Seq=0 Win=5792 Len=120...
66	4.256159	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
67	5.235091	198.51.100.5	192.0.2.1	TCP	33638->443 [ACK] Seq=1 Win=5792 Len=120...
68	5.236023	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
69	5.236955	198.51.100.16	192.0.2.1	TCP	32641->443 [SYN] Seq=0 Win=5792 Len=120...
70	5.237887	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
71	6.228728	198.51.100.5	192.0.2.1	HTTP	GET /sales.html HTTP/1.1
72	6.229638	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
73	6.230548	192.0.2.1	198.51.100.16	TCP	443->32641 [RST, ACK] Seq=0 Win=5792 Len=120...
74	6.330539	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
75	6.330885	198.51.100.7	192.0.2.1	TCP	42584->443 [SYN] Seq=0 Win=5792 Len=0...
76	6.331231	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
77	7.330577	192.0.2.1	198.51.100.5	TCP	HTTP/1.1 504 Gateway Time-out (text/html)
78	7.351323	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
79	7.360768	198.51.100.22	192.0.2.1	TCP	6345->443 [SYN] Seq=0 Win=5792 Len=0...
80	7.380773	192.0.2.1	198.51.100.7	TCP	443->42584 [RST, ACK] Seq=1 Win=5792 Len=120...
81	7.380878	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
82	7.383879	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
83	7.482754	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
84	7.581629	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
85	7.680504	192.0.2.1	198.51.100.22	TCP	443->6345 [RST, ACK] Seq=1 Win=5792 Len=0...
86	7.709377	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
87	7.738241	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
88	7.767105	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
89	13.89597	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
90	13.91983	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
91	13.9437	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
92	13.96756	192.0.2.1	198.51.100.16	TCP	443->32641 [RST, ACK] Seq=1 Win=5792 Len=120...
93	13.99142	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
94	14.01525	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
95	14.43907	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
96	14.8629	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
97	14.88673	198.51.100.9	192.0.2.1	TCP	4631->443 [SYN] Seq=0 Win=5792 Len=0...
98	15.31055	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
99	15.73438	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
100	16.15821	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
101	16.58204	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
102	17.00586	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
103	17.42968	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...

green Conexión TCP normal (proceso de enlace)					
red Actividad de ataque					
yellow Fallo de las conexiones TCP normales debido a un ataque					
Color as No.	seconds	Source	Destination	Protocol	Info
green 47	3.144521	198.51.100.23	192.0.2.1	TCP	42584->443 [SYN] Seq=0 Win=5792 Len=120...
green 48	3.195755	192.0.2.1	198.51.100.23	TCP	443->42584 [SYN, ACK] Seq=0 Win=5792 Len=120...
green 49	3.246989	198.51.100.23	192.0.2.1	TCP	42584->443 [ACK] Seq=1 Win=5792 Len=120...
green 50	3.298223	198.51.100.23	192.0.2.1	HTTP	GET /sales.html HTTP/1.1
green 51	3.349457	192.0.2.1	198.51.100.23	HTTP	HTTP/1.1 200 OK (text/html)
red 52	3.390692	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 53	3.441926	192.0.2.1	203.0.113.0	TCP	443->54770 [SYN, ACK] Seq=0 Win=5792 Len=120...
red 54	3.49316	203.0.113.0	192.0.2.1	TCP	54770->443 [ACK Seq=1 Win=5792 Len=0...
green 55	3.544394	198.51.100.14	192.0.2.1	TCP	14785->443 [SYN] Seq=0 Win=5792 Len=120...
green 56	3.599628	192.0.2.1	198.51.100.14	TCP	443->14785 [SYN, ACK] Seq=0 Win=5792 Len=120...
red 57	3.664863	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
green 58	3.730097	198.51.100.14	192.0.2.1	TCP	14785->443 [ACK Seq=1 Win=5792 Len=120...
red 59	3.795332	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=120...
green 60	3.860567	198.51.100.14	192.0.2.1	HTTP	GET /sales.html HTTP/1.1
red 61	3.939499	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=120...
green 62	4.018431	192.0.2.1	198.51.100.14	HTTP	HTTP/1.1 200 OK (text/html)
green 63	4.097363	198.51.100.5	192.0.2.1	TCP	33638->443 [SYN] Seq=0 Win=5792 Len=120...
red 64	4.176295	192.0.2.1	203.0.113.0	TCP	443->54770 [SYN, ACK] Seq=0 Win=5792 Len=120...
green 65	4.255227	192.0.2.1	198.51.100.5	TCP	443->33638 [SYN, ACK] Seq=0 Win=5792 Len=120...
red 66	4.256159	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
green 67	5.235091	198.51.100.5	192.0.2.1	TCP	33638->443 [ACK Seq=1 Win=5792 Len=120...
red 68	5.236023	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
green 69	5.236955	198.51.100.16	192.0.2.1	TCP	32641->443 [SYN] Seq=0 Win=5792 Len=120...
red 70	5.237887	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
green 71	6.228728	198.51.100.5	192.0.2.1	HTTP	GET /sales.html HTTP/1.1
red 72	6.229638	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
yellow 73	6.230548	192.0.2.1	198.51.100.16	TCP	443->32641 [RST, ACK] Seq=0 Win=5792 Len=120...
red 74	6.330539	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
green 75	6.330885	198.51.100.7	192.0.2.1	TCP	42584->443 [SYN] Seq=0 Win=5792 Len=0...
red 76	6.331231	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
yellow 77	7.330577	192.0.2.1	198.51.100.5	TCP	HTTP/1.1 504 Gateway Time-out (text/html)
red 78	7.351323	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
green 79	7.360768	198.51.100.22	192.0.2.1	TCP	6345->443 [SYN] Seq=0 Win=5792 Len=0...
yellow 80	7.380773	192.0.2.1	198.51.100.7	TCP	443->42584 [RST, ACK] Seq=1 Win=5792 Len=120...
red 81	7.380878	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 82	7.383879	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 83	7.482754	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
red 84	7.581629	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
yellow 85	7.680504	192.0.2.1	198.51.100.22	TCP	443->6345 [RST, ACK] Seq=1 Win=5792 Len=0...
red 86	7.709377	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 87	7.738241	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 88	7.767105	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 89	13.895969	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
red 90	13.919832	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 91	13.943695	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
yellow 92	13.967558	192.0.2.1	198.51.100.16	TCP	443->32641 [RST, ACK] Seq=1 Win=5792 Len=120...
red 93	13.991421	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 94	14.015245	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
red 95	14.439072	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
red 96	14.862899	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
green 97	14.886727	198.51.100.9	192.0.2.1	TCP	4631->443 [SYN] Seq=0 Win=5792 Len=0...
red 98	15.310554	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

Informe sobre incidentes de ciberseguridad

Sección 1: Identifica el tipo de ataque que puede haber causado esta interrupción de la red

El atacante está haciendo un ataque de inundación DoS SYN por que está enviando demasiadas peticiones al servidor web el cual ya no puede resolver por lo tanto es inaccesible a este, además que es solo de una computadora por eso es DoS y no DDoS

Sección 2: Explica cómo el ataque está provocando que el sitio web no funcione como debería

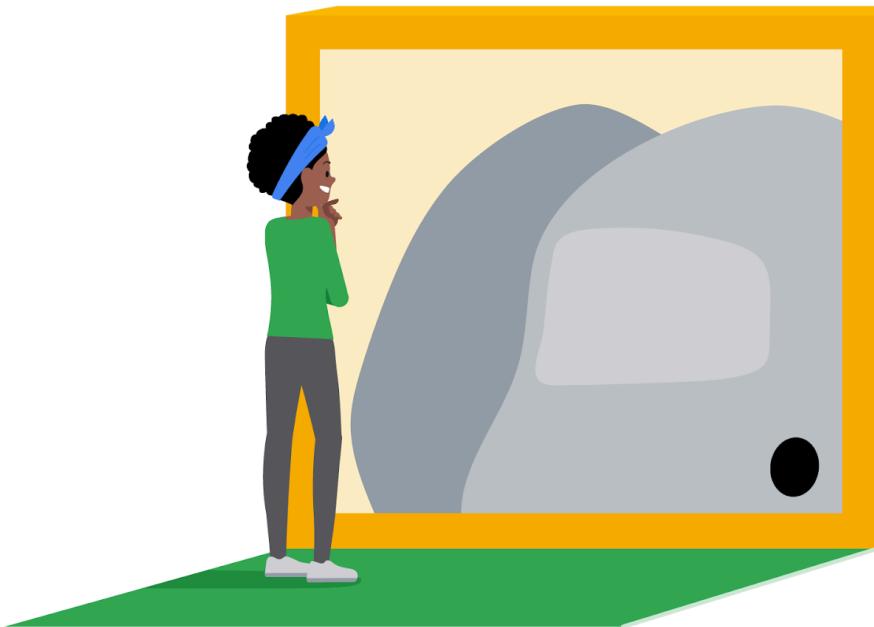
Debido al gran numero de peticiones en un periodo corto de tiempo el servidor está intentando resolver pero la capacidad no le da.

Analiza los indicadores de compromiso con herramientas de investigación

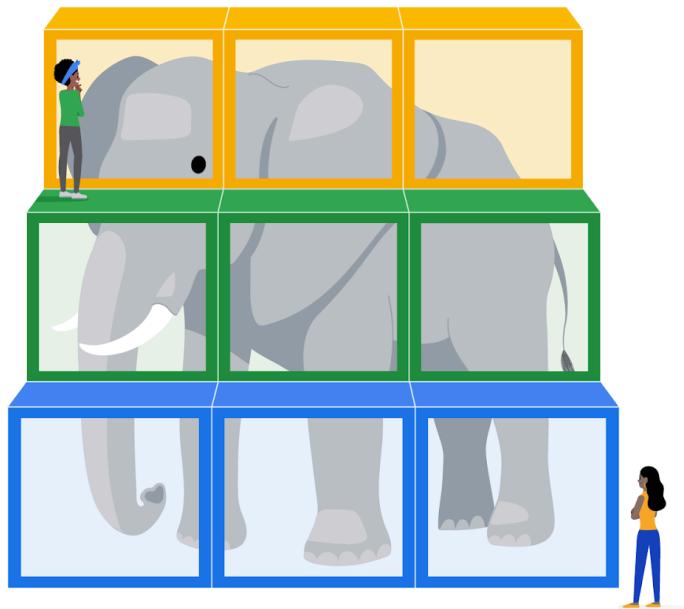
Agregar contexto a las investigaciones

Anteriormente, has aprendido sobre la pirámide del dolor, que describe la relación entre los indicadores de compromiso y el nivel de dificultad que experimentan los agentes de amenaza cuando los indicadores de compromiso son bloqueados por los equipos de seguridad. También aprendiste sobre diferentes tipos de IoC pero, como sabes, no todos los IoC son iguales. Los agentes de amenaza pueden lograr evadir la detección y continuar comprometiendo los sistemas aunque su actividad relacionada con los IoC esté bloqueada o limitada.

Por ejemplo, identificar y bloquear una sola dirección IP asociada con una actividad maliciosa no proporciona una visión amplia de un ataque, ni impide que un agente de amenaza continúe su actividad. Centrarse en una sola parte de la evidencia es como fijarse en una sola parte de un cuadro: se pierde el panorama general.



Los analistas de seguridad necesitan expandir el uso de los IoC para poder agregar contexto a las alertas. **La inteligencia sobre amenazas** es la información basada en evidencia que proporciona contexto sobre amenazas existentes o emergentes. Al acceder a información adicional relacionada con los IoC, los analistas de seguridad pueden ampliar su punto de vista para observar el panorama general y construir una narrativa que ayude a informar sus acciones de respuesta.



Al agregar contexto a un IoC, por ejemplo, mediante la identificación de otros artefactos relacionados con la dirección IP sospechosa, como comunicaciones de red dudosas o procesos inusuales, los equipos de seguridad pueden tener una imagen más concreta de un incidente. Este contexto puede ayudar a los equipos de seguridad a detectar incidentes de seguridad más rápido y adoptar un enfoque más informado en su respuesta.

El poder del "crowdsourcing" (externalización abierta de tareas)

El **crowdsourcing**, también denominado colaboración colectiva, es la práctica de recopilar información utilizando los aportes y la colaboración del público. Las plataformas de inteligencia sobre amenazas lo utilizan para reunir información de la comunidad global de ciberseguridad. Tradicionalmente, la respuesta a incidentes de una organización se realizaba de forma aislada; un equipo de seguridad recibía y analizaba una alerta, y luego procedía a remediarla, sin haber contemplado perspectivas adicionales acerca de cómo abordarla. De esta manera, sin el crowdsourcing, los atacantes podían llevar a cabo los mismos ataques contra distintas organizaciones.



Gracias al crowdsourcing, en cambio, las organizaciones aprovechan los conocimientos de millones de otros profesionales de la ciberseguridad, incluidos, entre otros, los vendedores de productos de ciberseguridad, organismos públicos y proveedores de servicios en la nube. Esta práctica permite a personas y organizaciones de la comunidad de la ciberseguridad mundial compartir y acceder abiertamente a una colección de datos de inteligencia sobre amenazas, lo cual ayuda a mejorar continuamente las tecnologías y metodologías de detección.

Entre los ejemplos de organizaciones de intercambio de información, se encuentran los Centros de Intercambio y Análisis de Información (ISAC), que se centran en recopilar inteligencia sobre amenazas dirigidas a sectores específicos y compartirla con empresas que operan en esos sectores concretos, como pueden ser los de energía o los de salud. Por su parte, la **inteligencia de fuentes abiertas (OSINT)** es la recopilación y análisis de información procedente de fuentes de acceso público para generar inteligencia utilizable. La OSINT también se puede utilizar como método para recopilar información relacionada con agentes de amenaza, amenazas, vulnerabilidades y más.

Estos datos de inteligencia sobre amenazas se utilizan para mejorar los métodos y técnicas de detección de productos de seguridad, como las herramientas de detección o el software antivirus. Por ejemplo, los atacantes suelen realizar los mismos ataques contra múltiples objetivos, con la esperanza de que uno de ellos sea exitoso. Si una organización detecta un ataque y publica inmediatamente los detalles del incidente, como archivos maliciosos, direcciones IP o URL, en herramientas como VirusTotal, esta inteligencia sobre amenazas puede ayudar a otras organizaciones a defenderse contra el mismo ataque.



VirusTotal

VirusTotal es un servicio que permite a cualquier persona analizar archivos, dominios, URL y direcciones IP sospechosos en busca de contenido malicioso. VirusTotal también ofrece servicios y herramientas adicionales para uso empresarial. Esta lectura se centra en el sitio web de VirusTotal, que está disponible para uso gratuito y no comercial.

Esta herramienta se puede utilizar para analizar archivos, direcciones IP, dominios y URL sospechosos, a fin de detectar amenazas de ciberseguridad, como el software malicioso. Los usuarios pueden enviar y verificar artefactos como hashes de archivos o direcciones IP para obtener informes de VirusTotal. Estos proporcionan información adicional sobre si un IoC se considera malicioso o no, cómo ese IoC está conectado a, o relacionado con, otros IoC en el conjunto de datos y más.

Intelligence Hunting Graph API

Sign in Sign up

VIRUSTOTAL

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE URL SEARCH

Choose file

By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the [sharing of your Sample submission with the security community](#). Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more](#).

Want to automate submissions? [Check our API](#), or access your [API key](#).

Aquí se presenta un desglose del resumen de los informes:

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b|

6 51 / 71

Community Score

1 DETECTION 2 DETAILS 3 RELATIONS 4 BEHAVIOR 5 COMMUNITY 9

① 51 security vendors and 2 sandboxes flagged this file as malicious

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
bfsvc.exe
peexe runtime-modules detect-debug-environment spreader direct-cpu-clock-access long-sleeps

430.00 KB 2022-07-26 06:23:31 UTC 5 months ago EXE

Security vendors' analysis ①

Ad-Aware	① Trojan.GenericFCA.Agent.27592	AhnLab-V3	① Malware/Win32.Generic.C4209910
Alibaba	① Backdoor:Win32/Flagpro.59f5de24	ALYac	① Trojan.Agent.Flagpro
Arcabit	① Trojan.GenericFCA.Agent.D6BC8	Avast	① Win32.Malware-gen
AVG	① Win32:Malware-gen	Avira (no cloud)	① TR/Redcap.hbtbs
BitDefender	① Trojan.GenericFCA.Agent.27592	BitDefenderTheta	① Gen:NN.Zexaf.34806.Au0@a015WTfI
Bkav Pro	① W32.AIDetect.malware2	Comodo	① Malware@#259qsws4j27nr
CrowdStrike Falcon	① Win/malicious_confidence_100% (W)	Cybereason	① Malicious.70dbeC
Cylance	① Unsafe	Cynet	① Malicious (score: 100)
Cyren	① W32/Trojan.ROHR-1168	DrWeb	① BackDoor.Flagpro.1

- Detection (Detección):** La pestaña Detection proporciona una lista de proveedores de seguridad externos y sus veredictos de detección sobre un IoC. Por ejemplo, los proveedores pueden catalogar su veredicto de detección como malicioso, sospechoso, inseguro, entre otros.

2. **Details (Detalles):** Esta pestaña proporciona información adicional extraída de un análisis estático del IoC. En esta pestaña se puede encontrar información sobre los distintos hashes, tipos de archivos, tamaños de archivo y encabezados, hora de creación y detalles sobre el primer y último envío.
3. **Relations (Relaciones):** La pestaña Relations proporciona los IoC relacionados que están conectados de alguna manera a un artefacto, como las URL, dominios, y direcciones IP contactados y los archivos soltados si el artefacto es un ejecutable.
4. **Behavior (Comportamiento):** La pestaña Behavior contiene información relacionada con la actividad y los comportamientos de un artefacto que se han observado después de ejecutarlo en un entorno controlado, como uno de pruebas (sandbox). Esta información incluye tácticas y técnicas detectadas, comunicaciones de red, acciones de sistemas de registro y archivos, procesos, entre otros.
5. **Community (Comunidad):** La pestaña Community es donde los miembros de la comunidad VirusTotal, como los profesionales de seguridad o los investigadores, pueden dejar comentarios e ideas sobre el IoC.
6. **Vendors' ratio and community Score (Ratio de proveedores y puntuación de la comunidad):** La puntuación que se muestra en la parte superior del informe es el ratio de proveedores, que indica cuántos proveedores de seguridad han marcado el IoC como malicioso. Debajo de esta puntuación también figura la de la comunidad, que se basa en los aportes de los usuarios de VirusTotal. Cuantas más detecciones tenga un archivo y mayor sea la puntuación de la comunidad, más probable es que sea malicioso.

Nota: Los datos subidos a VirusTotal se compartirán públicamente con toda la comunidad de VirusTotal. Es necesario tener cuidado al enviar información y asegurarse de no subir información personal.

Otras herramientas

Existen otras herramientas de investigación que se pueden utilizar para analizar los IoC, que también pueden compartir los datos con la comunidad.

Jotti's malware scan

[Jotti's malware scan](#) es un servicio gratuito que te permite analizar archivos sospechosos con varios programas antivirus. Hay algunas limitaciones en cuanto a la cantidad de archivos que se pueden enviar.

Urlscan.io

[Urlscan.io](#) es un servicio gratuito que escanea y analiza las URL y proporciona un informe detallado que resume la información de la URL.

CAPE Sandbox

[CAPE Sandbox](#) es un servicio de código abierto utilizado para automatizar el análisis de archivos sospechosos. En un entorno aislado, se analizan archivos maliciosos como el malware, cuyo comportamiento se describe en un informe exhaustivo.

MalwareBazaar

MalwareBazaar es un repositorio gratuito para muestras de software malicioso. Estas muestras son una gran fuente de inteligencia sobre amenazas que se puede utilizar con fines de investigación.

Aplica técnicas de reforzamiento del sistema operativo (SO)

Resumen de la actividad

En esta actividad, asumirás el papel de un analista de ciberseguridad que trabaja para una empresa que aloja el sitio web de cocina yummyrecipesforme.com. Los visitantes del sitio web experimentan un problema de seguridad al cargar la página web principal. Tu trabajo consiste en investigar, identificar, documentar y recomendar una solución al problema de seguridad.

Al investigar el evento de seguridad, revisarás un registro de tcpdump. Tendrás que identificar los protocolos de red utilizados para establecer la conexión entre el usuario y el sitio web. Los protocolos de red son las reglas y estándares de comunicación que los dispositivos en red utilizan para transmitir datos. Desafortunadamente, los actores maliciosos también pueden utilizar protocolos de red para invadir y atacar redes privadas. Saber identificar los protocolos utilizados habitualmente en los ataques te ayudará a proteger la red de tu organización contra este tipo de eventos de seguridad.

Para completar la tarea, también tendrás que documentar lo que ocurrió durante el incidente de seguridad. A continuación, recomendarás una medida de seguridad que se podría implementar para prevenir problemas de seguridad similares en el futuro.

Asegúrate de completar esta actividad antes de continuar. En la siguiente parte del curso, podrás ver un ejemplo completo para compararlo con tu propio trabajo. No podrás acceder al modelo hasta que hayas finalizado esta actividad.

Escenario

Analiza el siguiente caso. Luego, completa las instrucciones paso a paso.

Eres un analista de ciberseguridad para yummyrecipesforme.com, un sitio web que vende recetas y libros de cocina. Un panadero descontento ha decidido publicar las recetas más vendidas del sitio web para que el público pueda acceder a ellas de forma gratuita.

El panadero ejecutó un ataque de fuerza bruta para acceder al host de la web. Introdujo repetidamente varias contraseñas predeterminadas conocidas para la cuenta administrativa hasta que acertó con la correcta. Después de obtener las credenciales de acceso, pudo acceder al panel de administración y modificar el código fuente del sitio web. Incrustó una función de JavaScript en el código fuente que pedía a los visitantes que

descargaran y ejecutaran un archivo al visitar el sitio web. Tras ejecutar el archivo descargado, los clientes eran redirigidos a una versión falsa del sitio web donde las recetas del vendedor ya estaban disponibles de forma gratuita.

Varias horas después del ataque, varios clientes enviaron correos electrónicos al servicio de asistencia de [yummyrecipesforme](#). Se quejaban de que el sitio web de la empresa les había pedido que descargaran un archivo para actualizar sus navegadores. Los clientes afirmaron que, tras ejecutar el archivo, la dirección del sitio web cambió y sus computadoras personales comenzaron a funcionar más lentamente.

En respuesta a este incidente, el propietario del sitio web intenta iniciar sesión en el panel de administración, pero no lo consigue, por lo que se pone en contacto con el proveedor de alojamiento del sitio web. Tú y otros analistas de ciberseguridad reciben el encargo de investigar este incidente de seguridad.

Para abordarlo, creas un entorno sandbox para observar el comportamiento sospechoso del sitio web. Ejecuta el analizador de protocolos de red `tcpdump` y escribes la URL del sitio web, [yummyrecipesforme.com](#). En cuanto se carga el sitio web, se te pide que descargas un archivo ejecutable para actualizar tu navegador. Aceptas la descarga y permites que el archivo se ejecute. Entonces observas que tu navegador te redirige a una URL diferente, [greatrecipesforme.com](#), que está diseñada para parecerse al sitio original. Sin embargo, las recetas que vende tu empresa ahora se publican ahora gratuitamente en el nuevo sitio web.

Los registros muestran el siguiente proceso:

1. El navegador solicita una resolución DNS de la URL [yummyrecipesforme.com](#).
2. El servidor DNS responde con la dirección IP correcta.
3. El navegador inicia una solicitud HTTP para la página web.
4. El navegador inicia la descarga del malware.
5. El navegador solicita otra resolución DNS para [greatrecipesforme.com](#).
6. El servidor DNS responde con la nueva dirección IP.
7. El navegador inicia una solicitud HTTP a la nueva dirección IP.

Un analista de alto nivel confirma que el sitio web se vio comprometido. El analista verifica el código fuente del sitio web. Nota que se ha agregado código JavaScript para solicitar a los visitantes del sitio web que descarguen un archivo ejecutable. El análisis del archivo descargado encontró un script que redirige los navegadores de los visitantes de [yummyrecipesforme.com](#) a [greatrecipesforme.com](#).

El equipo de ciberseguridad informa que el servidor web se vio afectado por un ataque de fuerza bruta. El panadero descontento pudo adivinar la contraseña fácilmente porque la contraseña de administrador seguía siendo la contraseña predeterminada. Además, no había controles para prevenir un ataque de fuerza bruta.

Tu trabajo es documentar el incidente en detalle, incluida la identificación de los protocolos de red utilizados para establecer la conexión entre el usuario y el sitio web. También debes recomendar una acción de seguridad a tomar para prevenir ataques de fuerza bruta en el futuro.

oi

Que protocolo de red esta involucrado en el incidente?

Los protocolos involucrados son DNS y HTTP los cuales se usaron para re direccionar a la pagina donde venden las recetas, ademas que el puerto 80 recibia mucho trafico

Documenta el accidente

Se trato de acceder por el puerto 80 pero debido a que habia mucho trafico se redirigio a la otra pagina donde vendian las recetas

Recomienda una solucion para un ataque de fuerza bruta

Usar un gestor de contraseñas para asi poder tener mas seguridad ademas de medidas como la longitud de la contraseña y cambiarla cada periodo de tiempo

Ataque de fuerza bruta

Un ataque de fuerza bruta es un proceso de prueba y error para descubrir información privada. Algunos de los tipos de ataques de fuerza bruta que los agentes de amenaza usan para desvelar contraseñas son:

- Ataques de fuerza bruta simples. Cuando los atacantes intentan descubrir las credenciales de inicio de sesión de un usuario, se considera un ataque de fuerza bruta simple. Pueden hacerlo ingresando cualquier combinación de nombres de usuario y contraseñas hasta que encuentren la que funcione.
- Ataques de diccionario. La técnica utilizada es similar. Los atacantes utilizan una lista de uso común y credenciales robadas de ataques anteriores, para acceder a un sistema. Estos se llaman ataques de diccionario porque los atacantes originalmente usaban una lista de palabras de diccionario para dar con la contraseña correcta, antes de que las reglas de contraseña complejas se convirtieran en una práctica de seguridad común.

Evaluación de vulnerabilidades

Antes de que ocurra un ataque de fuerza bruta u otro incidente de ciberseguridad, las empresas pueden ejecutar una serie de pruebas en su red o aplicaciones web para evaluar vulnerabilidades. Los analistas pueden usar máquinas virtuales y entornos controlados (sandboxes) para probar archivos sospechosos, verificar vulnerabilidades antes de que ocurra un evento o simular un incidente de ciberseguridad.

Máquinas virtuales (VM)

Las máquinas virtuales (VM) son versiones en software de computadoras físicas. Las máquinas virtuales proporcionan una capa adicional de seguridad porque se pueden usar para ejecutar código en un entorno aislado, evitando que el código malicioso afecte al resto de la computadora o sistema. Las máquinas virtuales también se pueden eliminar y reemplazar por una imagen prístina después de probar el software malicioso.

Las máquinas virtuales son útiles cuando se investigan máquinas potencialmente infectadas o se ejecuta malware en un entorno restringido. El uso de una máquina virtual puede evitar daños en tu sistema en caso de que sus herramientas se utilicen incorrectamente. Las máquinas virtuales también te dan la capacidad de restablecer a un estado anterior. Sin embargo, aún existe un pequeño riesgo de que un programa malicioso pueda escapar de la virtualización y acceder a la máquina host.

Con máquinas virtuales, puedes probar y explorar aplicaciones fácilmente, y es fácil cambiar entre diferentes máquinas virtuales desde tu computadora. Esto también puede ayudar a agilizar muchas tareas de seguridad.

Entornos controlados (Sandboxes)

Un área de prueba o “sandbox” es un tipo de entorno que te permite ejecutar software o programas fuera de tu red. Se usan comúnmente para probar parches, identificar y abordar errores o detectar vulnerabilidades de ciberseguridad. Estas áreas de prueba también se pueden utilizar para evaluar software sospechoso o archivos que contienen código malicioso y simular escenarios de ataque.

Las áreas de prueba pueden ser computadoras físicas independientes que no están conectadas a una red; sin embargo, como entornos para un área de prueba, suele ser más rentable usar software o máquinas virtuales basadas en la nube. Ten en cuenta que quienes crean malware, por lo general, saben cómo escribir código, para detectar si el código malicioso se ejecuta en una máquina virtual o en un entorno de área de prueba. Los/los atacantes pueden programar su código malicioso para que se comporte como un software inofensivo cuando se ejecuta dentro de este tipo de entornos de prueba.

Medidas de prevención

- **Salting y hashing:** el hashing convierte la información en un valor único que luego se puede usar para determinar su integridad. Es una función unidireccional, lo que significa que es imposible descifrar y obtener el texto original. El salting agrega caracteres aleatorios a las contraseñas de hash esto aumenta la complejidad de los valores hash, haciéndolos más seguros.
- **Autenticación de múltiples factores (MFA) y autenticación de dos factores (2FA):** MFA es una medida de seguridad que requiere que un usuario verifique su identidad de dos o más maneras para acceder a un sistema o red. Esta verificación se realiza al utilizar una combinación de factores de autenticación: un nombre de usuario y contraseña, huellas dactilares, reconocimiento facial o una contraseña única (OTP) enviada a un número de teléfono o correo electrónico. 2FA es similar a MFA, pero utiliza solo dos formas de verificación.

- **CAPTCHA y reCAPTCHA:** CAPTCHA significa Prueba de Turing Pública y Automatizada para Diferenciar entre Máquinas y Humanos. Pide a los/las usuarios/as que completen una prueba simple que demuestre que son personas. Esto ayuda a evitar que el software intente forzar una contraseña. reCAPTCHA es un servicio gratuito de CAPTCHA de Google que ayuda a proteger los sitios web de bots y software malicioso.
- **Políticas de contraseña:** las organizaciones utilizan políticas de contraseña para estandarizar buenas prácticas. Estas pueden incluir pautas sobre el nivel de complejidad que debe tener una contraseña, la frecuencia con la que los/las usuarios/as deben actualizarlas y el límite de intentos de inicio de sesión por parte de un/a usuario/a antes de que se suspenda su cuenta.

Ataques de denegación de servicio (DoS)

es un ataque DoS que usa varios dispositivos o servidores en diferentes lugares para inundar la red víctima con tráfico no deseado.

¿Qué es un ataque DoS?

- Un ataque DoS inunda una red o servidor con tráfico falso, con el objetivo de sobrecargar el sistema y hacerlo colapsar.
- Esto impide que los usuarios legítimos accedan a los servicios o recursos de la red.

Tipos de ataques DoS:

- **Ataque SYN Flood:** Aprovecha el proceso de handshake TCP enviando un gran número de solicitudes SYN, saturando al servidor y bloqueando nuevas conexiones.
- **Ataque ICMP Flood:** Envía una avalancha de paquetes ICMP (ICMP es el protocolo de mensajes de control de Internet) al servidor, obligándolo a responder a cada uno de ellos y consumiendo todo el ancho de banda disponible.
- **Ataque Ping of Death:** Envía un paquete ICMP de tamaño superior al permitido, lo que puede provocar que el servidor se bloquee al intentar procesarlo.

Ataques de exfiltracion de datos

Movimiento lateral o pivoteo : Aquí explora la red con el objetivo de expandir y mantener su acceso a este y otros sistemas de red , al pivotear recorre el entorno

Ataques de seguridad pasados

Un virus informático es un código malicioso escrito para interferir con operaciones informáticas y causar daños a los datos y el software.

Malware: software diseñado para dañar dispositivos o redes.

Ataques en la nueva era:

LoveLetter: un correo que decía "I love u" para obtener las credenciales de acceso de las personas.

Fuga de información de Equifax:

Ingeniería Social es la técnica de manipulación para explotar el error humano para conseguir diferentes objetivos.

El phishing es el uso de comunicaciones digitales para engañar personas y provocar que revelen datos confidenciales o para propagar software malicioso

Phishing

Phishing es el uso de comunicaciones digitales en las que se suplanta la identidad de una persona o empresa con el objetivo de engañar a otras personas para que revelen datos confidenciales o implementen un software malicioso.

Algunos de los tipos más comunes de ataques de phishing actuales son:

- **Compromiso del correo electrónico empresarial (BEC):** el agente de amenaza envía un mensaje de correo electrónico que parece provenir de una fuente conocida, para efectuar una solicitud aparentemente legítima de información o intentar que realice una acción, con el fin de obtener un beneficio financiero.
- **Phishing localizado (Spear phishing):** un tipo de phishing focalizado en el que se envía un correo electrónico malicioso a un/a usuario/a o a un grupo de usuarios/as específicos/as, que parece provenir de una fuente confiable.
- **Ataque “caza de ballenas” (Whaling):** un tipo de phishing localizado mediante el cual los agentes de amenaza buscan acceder a los datos confidenciales de ejecutivos/as de una empresa.
- **Vishing:** un tipo de estafa por suplantación de identidad en la que se busca obtener información sensible a través de una llamada telefónica.
- **Smishing:** ataque de phishing por SMS que implica el uso de mensajes de texto para engañar a los/las usuarios/as, con el fin de obtener información confidencial o hacerse pasar por una fuente conocida.

Software malicioso

El **software malicioso** es un software diseñado para dañar dispositivos o redes. El propósito principal de quienes realizan el ataque es obtener dinero o, en algunos casos, información que pueda utilizarse en contra de una persona, una organización o un territorio.

Algunos de los tipos más comunes de ataques de software malicioso actuales son:

- **Virus informático:** un código malicioso creado para interferir con las operaciones de la computadora y dañar datos, software y hardware. El virus se instala en programas o documentos de una computadora y luego, se propaga e infecta una o más computadoras en una red.
- **Gusano:** un software malicioso que puede duplicarse y propagarse por sí mismo en los sistemas.
- **Ransomware (secuestro de datos):** un ataque malicioso en el que los agentes de amenaza cifran los datos de una organización y exigen un pago (rescate) para restablecer el acceso a ellos.
- **Spyware:** un tipo de software malicioso que se usa para recabar y vender información sin consentimiento. El spyware se puede usar para acceder a dispositivos, lo cual permite a los agentes de amenaza recopilar datos personales, como correos electrónicos, mensajes de texto, grabaciones de voz e imagen y ubicaciones de índole privada.

Ingeniería social

La **ingeniería social** es una técnica de manipulación que aprovecha errores humanos para obtener información privada, acceso a sistemas o bienes de valor. A menudo, los errores humanos se deben al exceso de confianza en alguien. La misión de un agente de amenaza que actúa como ingeniero social es crear un entorno de confianza falso y mentir para aprovecharse del mayor número posible de gente.

Algunos de los tipos más comunes de ataques de ingeniería social actuales son:

- **Ataque de suplantación de identidad en redes sociales (Phishing en redes sociales):** un tipo de ataque en el que el agente de amenaza contacta a la víctima en alguna red social, con el fin de robar información personal o tomar el control de la cuenta.
- **Ataque de “agujero de agua”:** un agente de amenaza ataca un sitio web visitado con frecuencia por un grupo específico de usuarios/as.
- **Cebo USB:** un agente de amenaza deja estratégicamente una unidad USB que contiene software malicioso para que un/a empleado/a la encuentre y la instale, con el fin de causar la infección involuntaria de una red.
- **Ingeniería social física:** un agente de amenaza se hace pasar por una persona ligada a la empresa para obtener acceso no autorizado a una ubicación física.

Principios de la ingeniería social

La ingeniería social es asombrosamente eficaz porque las personas suelen ser confiadas y tienen muy arraigado el respeto a la autoridad. La cantidad de ataques de ingeniería social

aumenta a medida que crece la cantidad de aplicaciones de redes sociales que permiten el acceso público a los datos de las personas. Aunque compartir datos personales (como tu ubicación o fotos) puede ser conveniente, también plantea un riesgo.

Los motivos por los cuales los ataques de ingeniería social son eficaces son:

- **Autoridad:** los agentes de amenaza se hacen pasar por personas con autoridad porque los individuos suelen respetarlas.
- **Intimidación:** los agentes de amenaza utilizan tácticas de hostigamiento, como asustar a las víctimas para que sigan sus órdenes.
- **Consenso/prueba social:** como las personas a veces hacen cosas convencidas de que otras también las hacen, los agentes de amenaza utilizan esta confianza en los demás para dar una impresión de legitimidad. Por ejemplo, para obtener acceso a datos privados, un agente de amenaza puede decir a un/a empleado/a que otros miembros de la empresa ya le han otorgado el acceso en otras ocasiones.
- **Escasez:** el agente de amenaza le da a entender a la persona que existe disponibilidad limitada de ciertos bienes o servicios, para convencerla de hacer algo.
- **Familiaridad:** los agentes de amenaza establecen falsos lazos emocionales con los/las usuarios/as de quienes desean aprovecharse, para lograr su objetivo.
- **Confianza:** los agentes de amenaza establecen una relación afectiva con los/las usuarios/as, que les permite aprovecharse de ellos *con el paso del tiempo*. Hacen uso de esta relación para ganarse la confianza de la víctima y acceder a su información personal.
- **Urgencia:** un agente de amenaza persuade a las personas para que respondan con rapidez sin hacer preguntas.

gestión de riesgos y seguridad.

Este se centra en definir metas y objetivos de seguridad, mitigación de riesgos, cumplimiento, continuidad del negocio y la ley, ellos pueden actualizar las leyes de seguridad de la empresa

El segundo dominio es la seguridad de los activos.

Este se centra en la seguridad de activos digitales y físicos. También se relaciona con el almacenamiento, mantenimiento, retención y destrucción de datos.

la ingeniería y arquitectura de seguridad.

Este se centra en optimizar la seguridad de los datos al asegurarse de que las herramientas, sistemas y procesos efectivos estén en su lugar.

comunicación y seguridad de la red.

Este se centra en la gestión y seguridad de las redes físicas

y las comunicaciones inalámbricas.

Como analista de seguridad,
tal vez se te pida que analices
el comportamiento de los/las usuarios/as dentro de tu organización.

gestión de acceso e identidad.

La gestión de acceso e identidad
se enfoca en mantener seguros los datos
al garantizar que se sigan políticas establecidas
para controlar y administrar activos físicos,
como espacios de oficina,
y activos lógicos, como redes y aplicaciones.
Validar las identidades de empleados/as y documentar roles de acceso
es fundamental para resguardar
la seguridad digital y física de la organización.

evaluación de seguridad y pruebas.

Este dominio se centra en realizar pruebas de control de seguridad,
recolectar y analizar datos
y realizar auditorías de seguridad
para monitorear riesgos, amenazas y vulnerabilidades.
Las/los analistas de seguridad pueden realizar auditorías periódicas
de permisos de usuario
para asegurarse de que tengan el nivel de acceso correcto.

operaciones de seguridad.

Este se dedica a realización de investigaciones
y la implementación de medidas preventivas.

seguridad de desarrollo de software.

Este se centra en el uso de prácticas seguras de codificación,
que son una serie recomendaciones
que se utilizan para crear aplicaciones y servicios seguros

Auditoria de seguridad

Las auditorías de seguridad son una revisión de los controles, políticas y procedimientos de seguridad de una organización. Las auditorías son revisiones independientes que evalúan si una compañía acata los criterios internos, como políticas y procedimientos, prácticas recomendadas y externos como el cumplimiento de normas, leyes y regulaciones federales.

Además, una auditoría de seguridad se puede utilizar para evaluar los controles de seguridad establecidos por una organización. Los controles de seguridad son medidas diseñadas para reducir riesgos de seguridad específicos.

Metas y objetivos de una auditoría

La meta de una auditoría es garantizar que las prácticas de tecnología de la información de una organización cumplan con los estándares de la industria y de la propia organización. El objetivo es identificar y abordar áreas que requieran mejoras y desarrollo. Proporcionan dirección y calidad al identificar las fallas actuales y desarrollar un plan para corregirlas. Las auditorías de seguridad deben realizarse para proteger los datos y evitar sanciones y multas por parte de las agencias gubernamentales.

Factores que determinan los tipos de auditorias que una organización debe implementar incluyen:

- Tipo de industria
- Tipo de organización
- Vínculos con las regulaciones gubernamentales
- "Ubicación geográfica de la empresa
- Decisión comercial de regirse por determinado cumplimiento normativo

El papel de los marcos y controles de las auditorias

Ademas del cumplimiento normativo es importante mencionar el papel que desempeñan los marcos y controles en las auditorias de seguridad. Como el marco de ciberseguridad (CSF) del NIST

y la serie de normas internacionales para la seguridad de cumplimiento normativo

W Untitled Attachment

Lista de control de la auditoria

Identificar el ambito de la auditoria

- La auditoría debería:
 - Enumerar los activos que se evaluarán, por ejemplo, si los cortafuegos (firewalls) están bien configurados, si la información personal de identificación (PII) es segura, si los activos físicos están bloqueados, etc..
 - Especificar de qué manera la auditoría ayudará a la organización a alcanzar sus objetivos.
 - Indicar la frecuencia con la que debería realizarse.

- Incluir una evaluación de las políticas, protocolos y procedimientos de la organización para asegurar que funcionen según lo previsto y que el personal los esté poniendo en práctica.

Completa una evaluación de riesgos

- Una evaluación de riesgos se utiliza para analizar los riesgos organizacionales identificados, relacionados con el presupuesto, los controles, los procesos internos y los estándares externos (por ejemplo, regulaciones).

Realiza una auditoría

- Al realizar una auditoría interna, evaluarás la seguridad de los activos identificados que se mencionan en el alcance de la auditoría.

Crea un plan de mitigación

- Un plan de mitigación es una estrategia implementada para reducir el nivel de riesgo y los costos potenciales, sanciones u otros problemas que puedan perjudicar la postura de seguridad de la organización.

Comunica los resultados a las partes interesadas

- El resultado final de este proceso es proporcionar un informe detallado de los hallazgos, las mejoras sugeridas necesarias para reducir el nivel de riesgo de la organización, así como las normas y los estándares de cumplimiento que la empresa debe cumplir.

Características de un modelado de amenaza eficaz

El **modelado de amenazas** es el proceso de identificación de activos, sus vulnerabilidades y cómo cada uno de ellos está expuesto a las amenazas. Es un enfoque estratégico que combina diversas actividades de seguridad, como la gestión de vulnerabilidades, el análisis de amenazas y la respuesta a incidentes. Los equipos de seguridad suelen realizar estos ejercicios para garantizar que sus sistemas estén adecuadamente protegidos. El modelado de amenazas se usa además para encontrar proactivamente formas de reducir los riesgos para cualquier sistema o proceso comercial.

Tradicionalmente, el modelado de amenazas se asocia con el campo del desarrollo de aplicaciones. En esta lectura, aprenderás sobre las metodologías comunes de modelado de amenazas que se utilizan para diseñar software capaz de resistir ataques. También te informarás acerca de la creciente necesidad de seguridad de las aplicaciones y las formas en que puedes participar.

Por qué es importante la seguridad de las aplicaciones

Las aplicaciones se han convertido en una parte esencial del éxito de muchas organizaciones. Por ejemplo, las aplicaciones basadas en la web permiten a los clientes de

cualquier parte del mundo conectarse con empresas, sus socios y otros clientes. Las aplicaciones móviles también cambiaron la forma en que las personas acceden al mundo digital. Los smartphones suelen ser la principal forma en que se intercambian datos entre los usuarios y una empresa. El volumen de datos que procesan las aplicaciones hace que asegurarlas sea clave para reducir el riesgo para las personas que se conectan a ellas.

Por ejemplo, supongamos que una aplicación utiliza bibliotecas de registro basadas en Java con la vulnerabilidad Log4Shell ([CVE-2021-44228](#)). Si esta no se parchea, puede permitir la ejecución remota de código que un atacante puede usar para obtener acceso completo a tu sistema, desde cualquier parte del mundo. Si se explota, una vulnerabilidad crítica como esta puede afectar a millones de dispositivos.

Defensa de la capa de aplicación

La defensa de la capa de aplicación requiere de pruebas adecuadas para descubrir debilidades que pueden conducir a un riesgo. El modelado de amenazas es una de las principales formas de garantizar que una aplicación cumpla con los requisitos de seguridad. Estos análisis suelen ser realizados por un equipo de DevSecOps (desarrollo, seguridad y operaciones).

Un proceso típico de modelado de amenazas se realiza en un ciclo:

- Definir el alcance
- Identificar amenazas
- Caracterizar el entorno
- Analizar amenazas
- Mitigar riesgos
- Evaluar los hallazgos



Lo ideal es que el modelado de amenazas se realice antes, durante y después del desarrollo de una aplicación. Sin embargo, realizar un análisis exhaustivo del software consume tiempo y recursos. Se debe evaluar todo: desde la arquitectura de la aplicación hasta sus fines comerciales. Como resultado, a lo largo de los años se desarrolló una serie de metodologías de modelado de amenazas para hacer que el proceso sea más sencillo.

Nota: El modelado de amenazas debe incorporarse en cada etapa del ciclo de vida del desarrollo de software (SDLC).

Marcos comunes

Al realizar un modelado de amenazas, hay varios métodos que se pueden utilizar, como los siguientes:

- STRIDE
- PASTA
- Trike
- VAST

Las organizaciones pueden usar cualquiera de estas metodologías para recopilar información y tomar decisiones que les permitan mejorar su postura de seguridad. Básicamente, el modelo “correcto” depende de la situación y los tipos de riesgos a los que una aplicación podría enfrentarse.

STRIDE

STRIDE es una metodología de modelado de amenazas desarrollada por Microsoft. Se utiliza comúnmente para identificar vulnerabilidades en seis vectores de ataque específicos. El acrónimo en inglés representa cada uno de estos vectores: suplantación, manipulación, repudio, divulgación de información, denegación de servicio y elevación de privilegios.

PASTA

El **proceso de simulación de ataques y análisis de amenazas** (PASTA, por sus siglas en inglés) es un proceso de modelado de amenazas centrado en el riesgo desarrollado por dos líderes de OWASP y respaldado por una empresa de ciberseguridad llamada VerSprite. Su enfoque principal es descubrir evidencia de amenazas viables y representar esta información como un modelo. El diseño basado en la evidencia de la metodología PASTA puede aplicarse al modelado de amenazas de una aplicación o el entorno que da soporte a esa aplicación. Su proceso de siete etapas consta de varias actividades que incorporan artefactos de seguridad relevantes del entorno, como informes de evaluación de vulnerabilidades.

Trike

Trike es una metodología y herramienta de código abierto que adopta un enfoque centrado en la seguridad para el modelado de amenazas. Se usa comúnmente para enfocarse en permisos de seguridad, casos de uso de aplicaciones, modelos de privilegios y otros elementos que propician un entorno seguro.

VAST

La metodología de modelado de amenazas visual, ágil y simple (VAST, por sus siglas en inglés) forma parte de una plataforma automatizada de modelado de amenazas llamada ThreatModeler®. Muchos equipos de seguridad optan por utilizar VAST como una forma de automatizar y optimizar sus evaluaciones de modelado de amenazas.

Cómo participar en el modelado de amenazas

El modelado de amenazas suele ser llevado a cabo por profesionales de la seguridad experimentados, pero casi nunca de forma independiente. Esto sucede sobre todo cuando se trata de asegurar aplicaciones. Los programas son sistemas complejos responsables de manejar una gran cantidad de datos y procesar una gran variedad de comandos de usuarios y otros sistemas.

Una de las claves para el modelado de amenazas es plantear las preguntas correctas:

- ¿En qué estamos trabajando?
- ¿Qué es lo que puede salir mal?
- ¿Qué estamos haciendo al respecto?
- ¿Nos hemos ocupado de todo?
- ¿Hicimos un buen trabajo?

Se necesita tiempo y práctica para aprender a trabajar con elementos como diagramas de flujo de datos y árboles de ataque. Sin embargo, todas las personas pueden aprender a realizar un modelado de amenazas efectivo. Independientemente de tu nivel de experiencia, participar en uno de estos ejercicios siempre comienza con el simple hecho de plantearse las preguntas correctas.

Clase 15 de octubre

Framework de Especialidad

NIST SP 800-53

Protección de Medio de Información

Almacenamiento de los Medios:

- Debe haber una política para el almacenamiento de los sistemas de información.
- Es importante la etiquetación de medios para los controles.

Invent

Clase 17 de octubre

Payment Card Industry Data Security (PCI DSS 4.0)

Se basa en 12 requerimientos para desarrollar software:

Crear cuentas subalternas para

La ley del mínimo privilegio es otorgar al usuario los permisos mínimos necesarios para realizar su trabajo.

Secure Control Framework SCF

El hipervisores gestiona los recursos de las maquinas.

El volcado de memoria pasa de la ram a un disco duro para saber que están haciendo.

Clase Lunes 23 sesión 7

Gestión de Riesgos

Riesgo: Se define como la posibilidad de ocurrencia de un fenómeno que pueda tener efectos negativos sobre una entidad, persona o organización, **es una posibilidad que se forme una situación adversa contra los activos.**

Riesgo de las Organizaciones

Entorno: Se refiere a lo que tenemos y que se puede perder, afectado tanto por las personas dentro como fuera de la organización.

Proceso de negocios:

Estrategia de gestión de riesgo: Es una estrategia que debe contemplar un análisis de los diferentes escenarios que puedan comprometer la operación de la organización, desde un ligero cambio hasta un cese de operaciones e incluso pérdidas humanas, centrarse en:

- **Enfoque holístico y heurístico**
- **Considerando amenazas presentes en el entorno de la organización:** Anotar y reportar todos los acontecimientos.
- **Con vista a proteger:** Los procesos de negocio y los activos sustantivos que los soportan.

Incidentes:

Estandares ISO27005

- Framework de manejo de riesgos
- Orientado al negocio
- No establece un metodología de evaluacion.

se habla de una estimación porque es subjetivo primero se establece el contexto, Riesgos: es una amenaza que impactan en los activos tanto en importancia

Clasificación de activos

Por qué es importante la gestión de los activos

Mantener los activos seguros requiere de un sistema eficiente que permita a las empresas operar sin inconvenientes. Establecer estos sistemas requiere contar con un conocimiento detallado de los activos de un entorno determinado. Por ejemplo, un banco necesita tener dinero disponible diariamente para atender a sus clientes, por lo que debe implementar equipos, dispositivos y procesos que garanticen la disponibilidad del dinero y su seguridad contra accesos no autorizados.

Las organizaciones protegen diversos tipos de activos. Algunos ejemplos podrían incluir:

- Activos digitales como datos de clientes o registros financieros.
- Sistemas de información que procesan datos, como redes o software.
- Activos físicos que pueden incluir instalaciones, equipos o suministros.
- Activos intangibles como la reputación de la marca o la propiedad intelectual.

Independientemente de su tipo, es crucial que cada activo sea clasificado y contabilizado.

Como recordarás, la **clasificación de activos** es la práctica de etiquetarlos según cuán sensibles e importantes son para una organización. Determinar estos factores puede variar, pero evaluar cuán sensible e importante es un activo generalmente requieren conocer la siguiente información:

- Lo que tienes (qué tipo de activo es)
- Dónde se encuentra ubicado
- Quién es el propietario
- Cuál es su nivel de importancia para la organización

Una organización que clasifica sus activos lo hace en función de estas características. Esto les ayuda a determinar cuán sensible es un activo y su valor.

Las clasificaciones comunes de los activos

La clasificación de activos ayuda a las organizaciones a implementar una estrategia efectiva de gestión de riesgos. También les permite priorizar los recursos de seguridad, reducir los costos de TI y cumplir con las regulaciones legales.

El esquema de clasificación más común consta de cuatro niveles: restringido, confidencial, solo interno y público.

- **Restringido** es el nivel más alto. Esta categoría está reservada a activos muy sensibles, como la información que solo se proporciona a quienes necesitan conocerla..
- El nivel **confidencial** se refiere a los activos cuya divulgación puede provocar un impacto negativo significativo en una organización.
- El nivel **solo interno** describe activos disponibles para el personal de una empresa y socios comerciales.
- **Público** es el nivel más bajo de clasificación. Estos activos no tienen consecuencias negativas para la organización si se divultan.

La forma en que se aplica este esquema depende en gran medida de las características de un activo. Puede sorprenderte saber que identificar al propietario de un activo es a veces la característica más complicada de determinar.

Desafíos de la clasificación de la información

Identificar al propietario de ciertos activos es sencillo, como en el caso de un edificio. Sin embargo, otros tipos de activos pueden ser más complicados de identificar, especialmente cuando se trata de información.

Por ejemplo, una empresa podría proporcionar una laptop a uno de sus empleados para que trabaje de forma remota. En esta situación, podríamos asumir que la organización es la propietaria del activo. Pero, ¿qué sucede si el empleado utiliza la laptop para asuntos personales, como guardar sus fotos?

La propiedad es solo una de las características que hacen que la clasificación de la información sea un desafío. Otra preocupación es que la información puede tener múltiples valores de clasificación al mismo tiempo. Por ejemplo, piensa en una carta que te envían por correo. La carta puede contener información pública que está bien compartir, como tu nombre. Sin embargo, también puede incluir información bastante confidencial que preferirías que solo estuviera disponible para ciertas personas, como tu dirección. A medida que avances en el programa, aprenderás más sobre cómo abordar estos desafíos.

Comandos de permiso

Anteriormente, exploraste los permisos de archivo y los comandos que puedes usar para mostrarlos y cambiarlos. En esta lectura, revisarás estos conceptos y también te centrarás en un ejemplo de cómo estos comandos funcionan juntos al poner en práctica el principio de mínimo privilegio.

Permisos de lectura

En Linux, los permisos se representan con una cadena de 10 caracteres. Estos son algunos permisos:

- **read** (lectura): para archivos, es la capacidad de leer el contenido de los archivos; para directorios, es la capacidad de leer todo el contenido del directorio, incluidos los archivos y subdirectorios
- **write** (escritura): para archivos, es la capacidad de realizar modificaciones en el contenido de los archivos; para directorios, es la capacidad de crear archivos nuevos en el directorio
- **execute** (ejecución): para archivos, es la capacidad de ejecutar el archivo si se trata de un programa; para directorios, es la capacidad de ingresar al directorio y acceder a sus archivos.

Estos permisos se otorgan a los siguientes tipos de propietarios:

- **user** (usuario): propietario del archivo
- **group** (grupo): un grupo más grande del que el propietario forma parte
- **other** (otros usuarios): todos los demás usuarios del sistema

Cada carácter en la cadena de 10 caracteres transmite información diferente sobre estos permisos. La siguiente tabla describe el propósito de cada carácter:

Carácter		
Ejemplo		
Significado		
1. ^º	drwxrwxrwx	<p>tipo de archivo</p> <ul style="list-style-type: none"> • d para el directorio • - para un archivo normal
2. ^º	drwxrwxrwx	<p>permisos de lectura para el usuario</p> <ul style="list-style-type: none"> • r si el usuario tiene permisos de lectura • - si el usuario no tiene permisos de lectura
3. ^º	drwxrwxrwx	<p>permisos de escritura para el usuario</p> <ul style="list-style-type: none"> • w si el usuario tiene permisos de escritura • _ si el usuario no tiene permisos de escritura
4. ^º	drwxrwxrwx	<p>permisos de ejecución para el usuario</p> <ul style="list-style-type: none"> • x si el usuario tiene permisos de ejecución • - si el usuario no tiene permisos de ejecución
5. ^º	drwxrwxrwx	<p>permisos de lectura para el grupo</p> <ul style="list-style-type: none"> • r si el grupo tiene permisos de

	lectura	
• – si el grupo no tiene permisos de lectura		
6. ^º	drwxrwxrwx	permisos de escritura para el grupo <ul style="list-style-type: none"> • w si el grupo tiene permisos de escritura • – si el grupo no tiene permisos de escritura
7. ^º	drwxrwxrwx	permisos de ejecución para el grupo <ul style="list-style-type: none"> • x si el grupo tiene permisos de ejecución • – si el grupo no tiene permisos de ejecución
8. ^º	drwxrwxrwx	permisos de lectura para otros usuarios <ul style="list-style-type: none"> • r si el otro tipo de propietario tiene permisos de lectura • – si el otro tipo de propietario no tiene permisos de lectura
9. ^º	drwxrwxrwx	permisos de escritura para otros usuarios <ul style="list-style-type: none"> • w si el otro tipo de propietario tiene permisos de escritura • – si el otro tipo de propietario no

tiene permisos de escritura		
10. ^o	drwxrwxrwx	<p>permisos de ejecución para otros usuarios</p> <ul style="list-style-type: none"> • x si el otro tipo de propietario tiene permisos de ejecución • – si el otro tipo de propietario no tiene permisos de ejecución

Exploración de los permisos existentes

Puedes usar el comando `ls` para investigar quién tiene permisos en archivos y directorios. Antes, aprendiste que `ls` muestra los nombres de los archivos y directorios en el directorio de trabajo actual.

Existen otras opciones que puedes agregar al comando `ls` para que sea más específico.

Algunas de estas opciones proporcionan detalles sobre los permisos. Estas son algunas que utilizan el comando `ls` y resultan importantes para las/los analistas de seguridad:

- `ls -a`: muestra archivos ocultos. Los archivos ocultos comienzan con un punto (.) al principio.
- `ls -l`: muestra permisos para archivos y directorios. También muestra otra información adicional, incluido el nombre del propietario, el grupo, el tamaño del archivo y la hora en que fueron modificados por última vez.
- `ls -la`: muestra los permisos de archivo y directorios, incluidos los archivos ocultos.

Se trata de una combinación de las otras dos opciones.

Cambio de permisos

El **principio de mínimo privilegio** es el concepto de otorgar solo el acceso y la autorización mínimos necesarios para ejecutar una tarea o función. En otras palabras, los/las usuarios/as no deben tener privilegios que estén más allá de lo necesario. No seguir el principio del mínimo privilegio puede crear riesgos de seguridad.

El comando `chmod` puede ayudarte a administrar esta autorización. El comando `chmod` cambia los permisos en archivos y directorios.

Cómo usar `chmod`

El comando `chmod` requiere dos argumentos. El primer argumento indica cómo cambiar los permisos, y el segundo indica el archivo o directorio para el que quieras cambiar los

permisos. Por ejemplo, el siguiente comando agregaría todos los permisos a

`login_sessions.txt`:

```
chmod u+rwx,g+rwx,o+rwx login_sessions.txt
```

Si quisieras quitar todos los permisos, podrías usar

```
chmod u-rwx,g-rwx,o-rwx login_sessions.txt
```

Otra forma de asignar estos permisos es usar el signo igual (=) en este primer argumento.

Al usar = con `chmod`, se establecen o asignan los permisos exactamente según se especificó. Por ejemplo, el siguiente comando establecería permisos de lectura para `login_sessions.txt` para usuario, grupo y otros usuarios:

```
chmod u=r,g=r,o=r login_sessions.txt
```

Este comando sobreescribe permisos existentes. Por ejemplo, si antes el usuario tenía permisos de escritura, estos permisos de escritura se eliminan después de especificar permisos de solo lectura con =.

La siguiente tabla revisa cómo se usa cada carácter dentro del primer argumento de

`chmod`:

Carácter	Descripción
u	indica que se realizarán cambios en los permisos de usuario
g	indica que se realizarán cambios en los permisos de grupo
o	indica que se realizarán cambios en los permisos de otros usuarios
+	agrega permisos al usuario, grupo u otros usuarios
-	elimina permisos del usuario, grupo u otros usuarios
=	asigna permisos para el usuario, grupo u otros usuarios

Nota: Cuando hay cambios de permiso en más de un tipo de propietario, hay que usar comas para separar los cambios para cada tipo de propietario. No se debe agregar espacios después de esas comas.

El principio de mínimo privilegio en acción

Como analista de seguridad, es posible que te encuentres en una situación como esta: hay un archivo llamado `bonuses.txt` dentro de un directorio de remuneración. El propietario de este archivo es un miembro del departamento de Recursos Humanos cuyo nombre de usuario es `hrrep1`. Se decidió que `hrrep1` necesita acceso a este archivo. Pero, dado que este archivo contiene información confidencial, nadie más en el grupo `hr` debería acceder a él.

Ejecutas `ls -l` para verificar los permisos de los archivos en el directorio de remuneración y descubres que los permisos para `bonuses.txt` son `-rw-rw----`. El tipo propietario del grupo tiene permisos de lectura y escritura que no se alinean con el principio de mínimo privilegio.

Para remediar la situación, ingresas `chmod g-rw bonuses.txt`. Ahora, solo puede acceder a este archivo el/la usuario/a que lo necesita para llevar a cabo sus responsabilidades laborales.

Comandos en linux

Grep: busca un archivo especificado y devuelve todas las líneas dentro de este archivo que contiene una cadena específica

Piping | : envía una salida estándar de un comando como entrada estándar en otro comando para procesarlo luego

grep

El comando `grep` busca un archivo especificado y devuelve todas las líneas del archivo que contienen una cadena específica. El comando `grep` suele combinarse con dos argumentos: una cadena específica a buscar y un archivo específico en el que buscar.

Por ejemplo, si ingresas `grep OS updates.txt`, obtendrás todas las líneas que contienen `OS` en el archivo `updates.txt`. En este ejemplo, `OS` es la cadena específica a buscar y `updates.txt` es el archivo específico en el que buscar.

pipe (pleca)

Para acceder a este comando, se utiliza el carácter pleca, o *pipe* (|). El comando `pipe` envía la salida estándar de un comando como entrada estándar a otro comando, para su posterior procesamiento. Como recordatorio, la **salida estándar** es la información devuelta por el sistema operativo a través del shell, mientras que la **entrada estándar** es la información recibida por el sistema operativo (SO) a través de la línea de comandos. El carácter pleca (|) puede estar en distintas partes de un teclado, pero en general, se encuentra en la misma tecla que el carácter de barra invertida (\). En algunos teclados, el carácter | puede verse diferente, con un pequeño espacio en el medio de la línea. Si no encuentras el carácter |, busca en Internet dónde está ubicado en tu teclado.

Cuando se utiliza con `grep`, la pleca puede ayudarte a encontrar directorios y archivos que contienen una palabra específica en el nombre. Por ejemplo, `ls /home/analyst/reports | grep users` devuelve los nombres de archivos y directorios en el directorio `reports` que contienen la palabra `users`. Antes de la pleca, `ls` indica que debe hacerse una lista de los nombres de los archivos y directorios en `reports`. Luego, esta salida se envía, como entrada, al comando ubicado después de la pleca. En este caso, `grep users` devolverá todos los nombres de archivos o directorios que contienen `users` de la entrada recibida.

Nota: El comando `pipe` es una forma general de redireccionamiento en Linux y puede utilizarse para múltiples tareas, además del filtrado. Puedes considerarlo como una

herramienta general a utilizar, siempre que quieras que la salida de un comando se convierta en la entrada de otro comando.

find

El comando `find` sirve para buscar directorios y archivos que cumplan con criterios especificados. Hay una amplia variedad de criterios que se pueden especificar con `find`.

Por ejemplo, puedes buscar archivos y directorios que:

- Contengan una cadena específica en el nombre;
- Tengan un determinado tamaño de archivo; o
- Se hayan modificado por última vez dentro de un período de tiempo determinado.

Cuando usas `find`, el primer argumento después de `find` indica dónde comenzar a buscar. Por ejemplo, al ingresar `find /home/analyst/projects` se busca todo lo que comienza en el directorio `projects`.

Después de este primer argumento, debes indicar tus criterios para la búsqueda. Si no incluyes un criterio de búsqueda específico con tu segundo argumento, es probable que tu búsqueda devuelva una gran cantidad de directorios y archivos.

La especificación de criterios implica opciones. Las **opciones** modifican el comportamiento de un comando y, por lo general, comienzan con un guión (-).

-name e -iname

Un criterio clave que las/los analistas podrían usar con `find` es buscar nombres de archivos o directorios que contengan una cadena específica. Debes ingresar la cadena específica que estés buscando entre comillas después de las opciones `-name` o `-iname`. La diferencia entre estas dos opciones es que `-name` distingue entre mayúsculas y minúsculas, mientras que `-iname` no lo hace.

Supongamos que quieres buscar todos los archivos en el directorio `projects` que contienen la palabra "log" en el nombre. Para hacerlo, ingresarías `find /home/analyst/projects -name "*log*"`. También podrías ingresar `find /home/analyst/projects -iname "*log*"`.

En estos ejemplos, la salida estaría conformada por todos los archivos del directorio `projects` que contengan `log` rodeada de cero o más caracteres. La parte del comando que dice `"*log*"` es el criterio de búsqueda que indica que se debe buscar la cadena "log". Cuando la opción es `-name`, no se devolverán los archivos con nombres que incluyan `Log` o `LOG`, por ejemplo, porque esta opción distingue entre mayúsculas y minúsculas. Sin embargo, sí se devolverán si la opción es `-iname`.

Nota: El asterisco (*) se usa como comodín para representar cero o más caracteres desconocidos.

-mtime

Las/los analistas de seguridad también pueden usar `find` para buscar archivos o directorios modificados por última vez, en un período de tiempo determinado. Para esta

búsqueda, se puede utilizar la opción `-mtime`. Por ejemplo, al ingresar `find /home/analyst/projects -mtime -3`, se devuelven todos los archivos y directorios del directorio `projects` que han sido modificados en los últimos tres días.

La búsqueda de la opción `-mtime` se basa en días, por lo que la entrada `-mtime +1` indica todos los archivos o directorios que se modificaron por última vez hace más de un día y la entrada `-mtime -1` indica todos los archivos o directorios que se modificaron por última vez hace menos de un día.

Nota: Si quieres basar la búsqueda en minutos en lugar de días, puedes usar la opción `-mmin` en lugar de `-mtime`.

comandos suricata

Action

```
alert http $HOME_NET any -> $EXTERNAL_NET  
any (msg:"GET on wire";  
flow:established,to_server; content:"GET";  
http_method; sid:12345; rev:3;)
```

The **action** is the first part of the signature. It determines the action to take if all conditions are met.

Actions differ across network intrusion detection system (NIDS) rule languages, but some common actions are alert, drop, pass, and reject.

Using our example, the file contains a single alert as the action. The `alert` keyword instructs to alert on selected network traffic. The IDS will inspect the traffic packets and send out an alert in case it matches.

Note that the `drop` action also generates an alert, but it drops the traffic. A `drop` action only occurs when Suricata runs in IPS mode.

The `pass` action allows the traffic to pass through the network interface. The `pass` rule can be used to override other rules. An exception to a drop rule can be made with a `pass` rule.

For example, the following rule has an identical signature to the previous example, except that it singles out a specific IP address to allow only traffic from that address to pass:

```
pass http 172.17.0.77 any -> $EXTERNAL_NET any (msg:"BAD USER-  
AGENT";flow:established,to_server;content:!Mozilla/5.0;  
http_user_agent; sid: 12365; rev:1;)
```

The rejection does not allow the traffic to pass. Instead, a TCP reset packet will be sent, and Suricata will drop the matching packet. A TCP reset packet tells computers to stop sending messages to each other.

You'll most often use the alertrule in this lab activity.

Note: Rule order refers to the order in which rules are evaluated by Suricata. Rules are loaded in the order in which they are defined in the configuration file. However, Suricata processes rules in a different default order: pass, drop, reject, and alert. Rule order affects the final verdict of a packet.

Header

```
alert http $HOME_NET any -> $EXTERNAL_NET  
any (msg:"GET on wire";  
flow:established,to_server; content:"GET";  
http_method; sid:12345; rev:3;)
```

The next part of the signature is the **header**. The header defines the signature's network traffic, which includes attributes such as protocols, source and destination IP addresses, source and destination ports, and traffic direction.

The next field after the action keyword is the protocol field. In our example, the protocol is http, which determines that the rule applies only to HTTP traffic.

The parameters to the protocol httpfield are \$HOME_NET any -> \$EXTERNAL_NET any. The arrow indicates the direction of the traffic coming from the \$HOME_NETand going to the destination IP address \$EXTERNAL_NET.

\$HOME_NETis a Suricata variable defined in /etc/suricata/suricata.yamlthat you can use in your rule definitions as a placeholder for your local or home network to identify traffic that

connects to or from systems within your organization.

In this lab \$HOME_NET is defined as the 172.21.224.0/20 subnet.

The word any means that Suricata catches traffic from any port defined in the \$HOME_NET network.

Note: The \$symbol indicates the start of a variable. Variables are used as placeholders to store values.

So far, we know that this signature triggers an alert when it detects any http traffic leaving the home network and going to the external network.

Rule options

```
alert http $HOME_NET any -> $EXTERNAL_NET
any (msg:"GET on wire";
flow:established,to_server; content:"GET";
http_method; sid:12345; rev:3;)
```

The many available **rule options** allow you to customize signatures with additional parameters. Configuring rule options helps narrow down network traffic so you can find exactly what you're looking for. As in our example, rule options are typically enclosed in a pair of parentheses and separated by semicolons.

Let's further examine the rule options in our example:

- The msg:option provides the alert text. In this case, the alert will print out the text "GET on wire", which specifies why the alert was triggered.
- The flow:established,to_server option determines that packets from the client to the server should be matched. (In this instance, a server is defined as the device responding to the initial SYN packet with a SYN-ACK packet.)
- The content:"GET" option tells Suricata to look for the word GET in the content of the http.method portion of the packet.
- The sid:12345(signature ID) option is a unique numerical value that identifies the rule.
- The rev:3 option indicates the signature's revision which is used to identify the signature's version. Here, the revision version is 3.

Task 2. Trigger a custom rule in Suricata

Now that you are familiar with the composition of the custom Suricata rule, you must trigger this rule and examine the alert logs that Suricata generates.

1. List the files in the /var/log/suricata folder:

```
ls -l /var/log/suricata
```

Copied!

content_copy

Note that before running Suricata, there are no files in the /var/log/suricata directory.

2. Run suricata using the custom.rules and sample.pcap files:

```
sudo suricata -r sample.pcap -S custom.rules -k none
```

Copied!

content_copy

This command starts the Suricata application and processes the sample.pcap file using the rules in the custom.rules file. It returns an output stating how many packets were processed by Suricata.

Note: In this lab, using sudo is required to process packet capture files with Suricata, although it may not be required in a real-world environment.

Now you'll further examine the options in the command:

- The -r sample.pcap option specifies an input file to mimic network traffic. In this case, the sample.pcap file.
- The -S custom.rules option instructs Suricata to use the rules defined in the custom.rules file.
- The -k none option instructs Suricata to disable all checksum checks.

As a refresher, checksums are a way to detect if a packet has been modified in transit.

Because you are using network traffic from a sample packet capture file, you won't need Suricata to check the integrity of the checksum.

Suricata adds a new alert line to the /var/log/suricata/fast.logfile when all the conditions in any of the rules are met.

3. List the files in the /var/log/suricata folder again:

```
ls -l /var/log/suricata
```

Copied!

content_copy

Note that after running Suricata, there are now four files in the /var/log/suricata directory, including the fast.log and eve.json files. You'll examine these files in more detail.

4. Use the cat command to display the fast.logfile generated by Suricata:

```
cat /var/log/suricata/fast.log
```

Copied!

content_copy

The output returns alert entries in the log:

```
11/23/2022-12:38:34.624866 [**] [1:12345:3] GET on wire [**]  
[Classification: (null)] [Priority: 3] {TCP} 172.21.224.2:49652 ->  
142.250.1.139:80  
11/23/2022-12:38:58.958203 [**] [1:12345:3] GET on wire [**]  
[Classification: (null)] [Priority: 3] {TCP} 172.21.224.2:58494 ->  
142.250.1.139:80
```

Each line or entry in the fast.logfile corresponds to an alert generated by Suricata when it processes a packet that meets the conditions of an alert generating rule. Each alert line includes the message that identifies the rule that triggered the alert, as well as the source, destination, and direction of the traffic.

Task 3. Examine eve.json output

In this task, you must examine the additional output that Suricata generates in the eve.json file.

As previously mentioned, this file is located in the /var/log/suricata directory.

The eve.json file is the standard and main Suricata log file and contains a lot more data than the fast.log file. This data is stored in a JSON format, which makes it much more useful for analysis and processing by other applications.

1. Use the cat command to display the entries in the eve.json file:

```
cat /var/log/suricata/eve.json
```

Copied!

content_copy

The output returns the raw content of the file. You'll notice that there is a lot of data returned that is not easy to understand in this format.

2. Use the jqcommand to display the entries in an improved format:

```
jq . /var/log/suricata/eve.json | less
```

Copied!

content_copy

Note: You can use the lowercase **f** and **b** keys to move forward or backward through the output. Also, if you enter a command incorrectly and it fails to return to the command-line prompt, you can press **CTRL+C** to stop the process and force the shell to return to the command-line prompt.

3. Press **Q** to exit the lesscommand and to return to the command-line prompt.

Note how much easier it is to read the output now as opposed to the catcommand output.

Note: The jqtool is very useful for processing JSON data, however, a full explanation of its capabilities is outside of the scope of this lab.

What is the value of the severity property for the first alert returned by the jq command?

4

3

1

0

Submit

4. Use the jqcommand to extract specific event data from the eve.jsonfile:

```
jq -c "[.timestamp,.flow_id,.alert.signature,.proto,.dest_ip]"  
/var/log/suricata/eve.json
```

Copied!

content_copy

Note: The jqcommand above extracts the fields specified in the list in the square brackets from the JSON payload. The fields selected are the timestamp (.timestamp), the flow id (.flow_id), the alert signature or msg (.alert.signature), the protocol (.proto), and the destination IP address (.dest_ip).

What is the destination IP address listed for the last event in the 'eve.json' file?

142.250.1.139

192.168.0.1

172.21.224.2

142.250.1.102

Submit

What is the alert signature for the first alert entry in the 'eve.json' file?

DROP ICMP for HOMENET

BAD USER-AGENT

GET on wire

Pass ICMP for HOMENET

Submit

The following is an example of the output of the command above. The flow_id is the long numeric field highlighted in orange in each row returned.

```
["2022-11-23T12:38:34.624866+0000",14500150016149,"GET on  
wire","TCP","142.250.1.139"]  
["2022-11-23T12:38:58.958203+0000",1647223379236084,"GET on  
wire","TCP","142.250.1.102"]
```

5. Use the jq command to display all event logs related to a specific flow_id from the eve.json file. The flow_id value is a 16-digit number and will vary for each of the log entries. Replace X with any of the flow_id values returned by the previous query:

Image here...

```
jq "select(.flow_id==X)" /var/log/suricata/eve.json
```

Copied!

content_copy

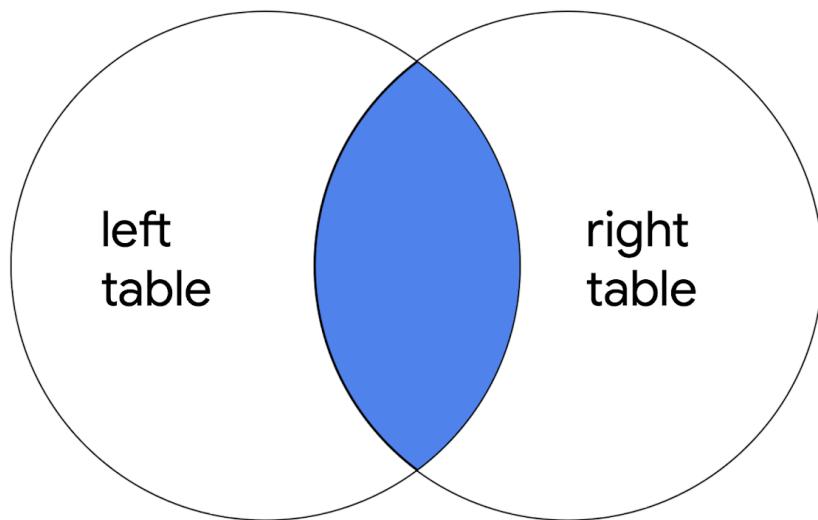
Note: A network flow refers to a sequence of packets between a source and destination that share common characteristics such as IP addresses, protocols, and more. In cybersecurity, network traffic flows help analysts understand the behavior of network traffic to identify and analyze threats. Suricata assigns a unique flow_id to each network flow. All logs from a

network flow share the same flow_id. This makes the flow_id field a useful field for correlating network traffic that belongs to the same network flows.

Compara tipos de combinaciones (Joins)

Combinaciones internas

El primer tipo de combinación que puedes ejecutar es una combinación interna. `INNER JOIN` devuelve filas que coinciden en una columna especificada que existe en más de una tabla.



Esta solo devuelve filas donde existe una coincidencia pero, como en otros tipos de combinaciones, devuelve todas las columnas especificadas de todas las tablas combinadas. Por ejemplo, si la consulta combina dos tablas con `SELECT *`, se devuelven todas las columnas en ambas tablas.

Nota: Si una columna existe en ambas tablas, esta se devuelve dos veces al usar `SELECT *`.

La sintaxis de una combinación interna

Para escribir una consulta usando `INNER JOIN`, puedes utilizar la siguiente sintaxis:

```
SELECT *  
FROM employees  
INNER JOIN machines ON employees.device_id = machines.device_id;
```

Debes especificar las dos tablas a combinar incluyendo la tabla primera o izquierda después de `FROM` y la tabla segunda o derecha después de `INNER JOIN`.

Después del nombre de la tabla derecha, usa la palabra clave `ON` y el operador `=` para indicar la columna en la que estás combinando las tablas. Es importante que especifiques

los nombres tanto de la tabla como de la columna en esta parte de la combinación colocando un punto (.) entre la tabla y la columna.

Además de seleccionar todas las columnas, puedes seleccionar solo ciertas columnas. Por ejemplo, si quieres que la combinación solo devuelva las columnas `username` (nombre de usuario), `operating_system` (sistema operativo) y `device_id` (ID de dispositivo), puedes escribir esta consulta:

```
SELECT username, operating_system, employees.device_id  
FROM employees  
INNER JOIN machines ON employees.device_id = machines.device_id;
```

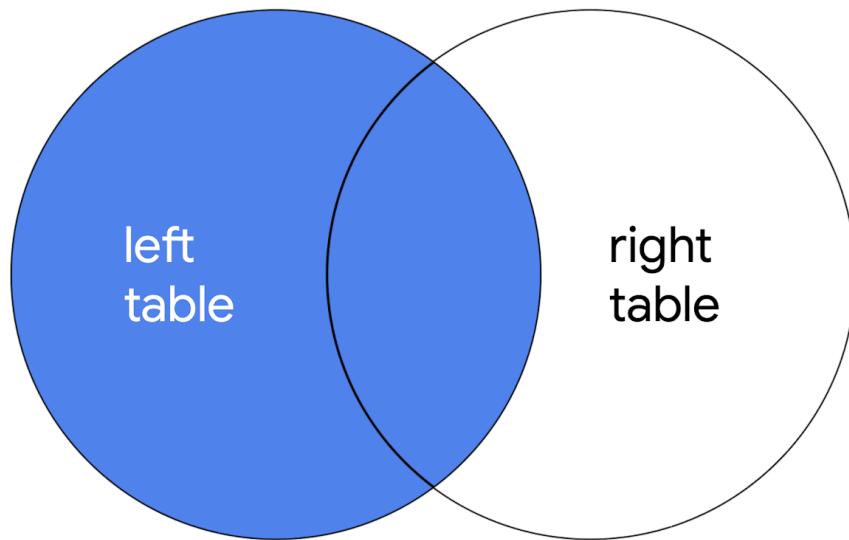
Nota: En la consulta de ejemplo, `username` (nombre de usuario) y `operating_system` (sistema operativo) solo aparecen en una de las dos tablas, por lo que se escriben solo con el nombre de la columna. Por otra parte, como `device_id` (ID de dispositivo) aparece en ambas tablas, es necesario indicar cuál devolver, especificando el nombre tanto de la tabla como de la columna (`employees.device_id`).

Combinaciones externas

Las combinaciones externas amplían lo que se devuelve a partir de una combinación. Cada tipo de combinación externa devuelve todas las filas de una o de ambas tablas.

Combinaciones izquierdas

Cuando combinas dos tablas, `LEFT JOIN` devuelve todos los registros de la primera tabla, pero solo devuelve las filas de la segunda tabla que coinciden en una columna especificada.



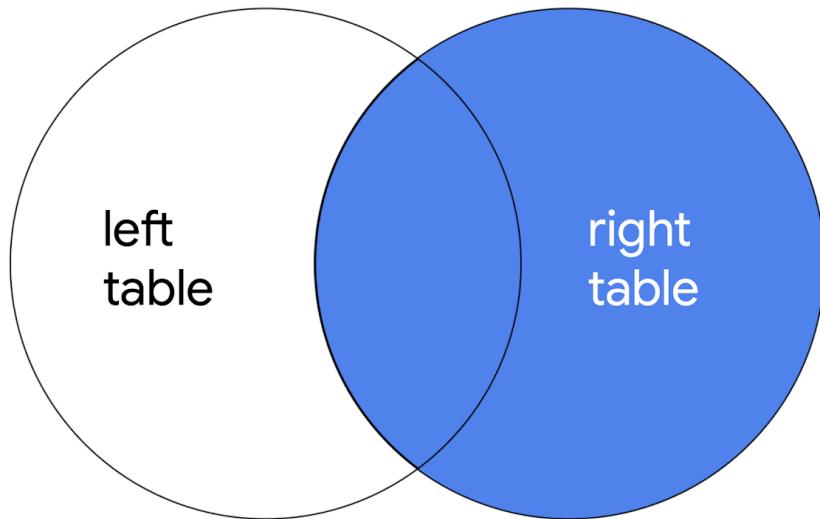
La sintaxis para usar `LEFT JOIN` se demuestra en la consulta siguiente:

```
SELECT *  
FROM employees  
LEFT JOIN machines ON employees.device_id = machines.device_id;
```

Como con todas las combinaciones, debes especificar la tabla primera o izquierda como la tabla que viene después de `FROM` y la tabla segunda o derecha como la tabla que viene después de `LEFT JOIN`. En la consulta de ejemplo, como `employees` (empleados/as) es la tabla izquierda, se devuelven todos sus registros. Solo se devuelven los registros que coinciden en la columna `device_id` (ID de dispositivo) desde la tabla derecha, `machines` (equipos).

Combinaciones derechas

Cuando combinas dos tablas, `RIGHT JOIN` devuelve todos los registros de la segunda tabla, pero solo devuelve las filas de la primera tabla que coinciden en una columna especificada.



La consulta siguiente demuestra la sintaxis para `RIGHT JOIN`:

```
SELECT *  
FROM employees  
RIGHT JOIN machines ON employees.device_id = machines.device_id;  
  
RIGHT JOIN tiene la misma sintaxis que LEFT JOIN, con la única diferencia de que la palabra clave RIGHT JOIN ordena a SQL generar resultados distintos. La consulta devuelve todos los registros de machines (equipos), que es la tabla segunda o derecha. Solo se devuelven registros coincidentes de employees (empleados/as), que es la tabla primera o izquierda.
```

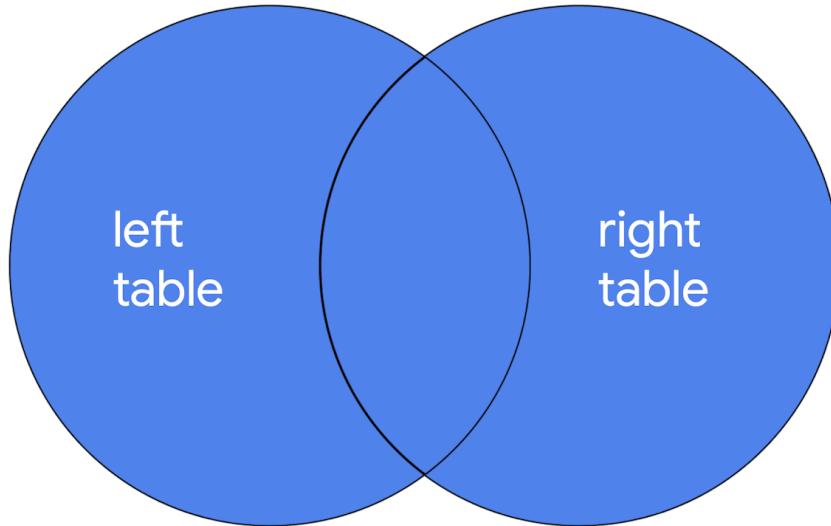
Nota: Puedes usar `LEFT JOIN` y `RIGHT JOIN` y obtener exactamente los mismos resultados si usas las tablas en orden inverso. La consulta `RIGHT JOIN` siguiente devuelve exactamente el mismo resultado que la consulta `LEFT JOIN` demostrada en la sección anterior:

```
SELECT *  
FROM machines  
RIGHT JOIN employees ON employees.device_id = machines.device_id;
```

Para cambiar de lugar las tablas izquierda y derecha, solo tienes que modificar el orden de las tablas que aparecen antes y después de la palabra clave utilizada para la combinación.

Combinaciones externas completas

FULL OUTER JOIN (Combinación externa completa) devuelve todos los registros de ambas tablas. Puedes utilizarla como una manera de fusionar totalmente dos tablas.



Puedes revisar la sintaxis para usar **FULL OUTER JOIN** en la consulta siguiente:

```
SELECT *
FROM employees
FULL OUTER JOIN machines ON employees.device_id = machines.device_id;
```

Los resultados de una consulta **FULL OUTER JOIN** incluyen todos los registros de ambas tablas. De manera similar a **INNER JOIN**, el orden de las tablas no modifica los resultados de la consulta.

Componentes de la comunicación en una capa de red

Operaciones en la capa de red

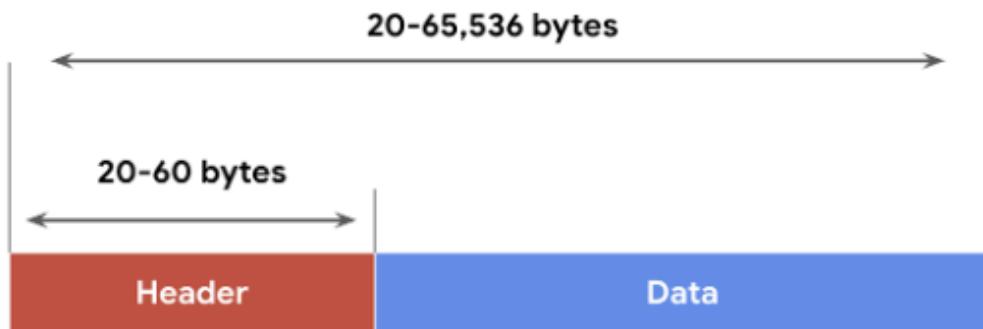
Las funciones en la capa de red organizan la dirección y la entrega de paquetes de datos a través de la red de internet desde el dispositivo host hasta el de destino. Esto incluye dirigir los paquetes de un enrutador a otro a través del internet, basándose en la dirección del protocolo de internet (IP) de la red de destino.

La dirección se almacena en tablas de enrutamiento a lo largo del camino del paquete hacia su destino, para futuros propósitos de enrutamiento.

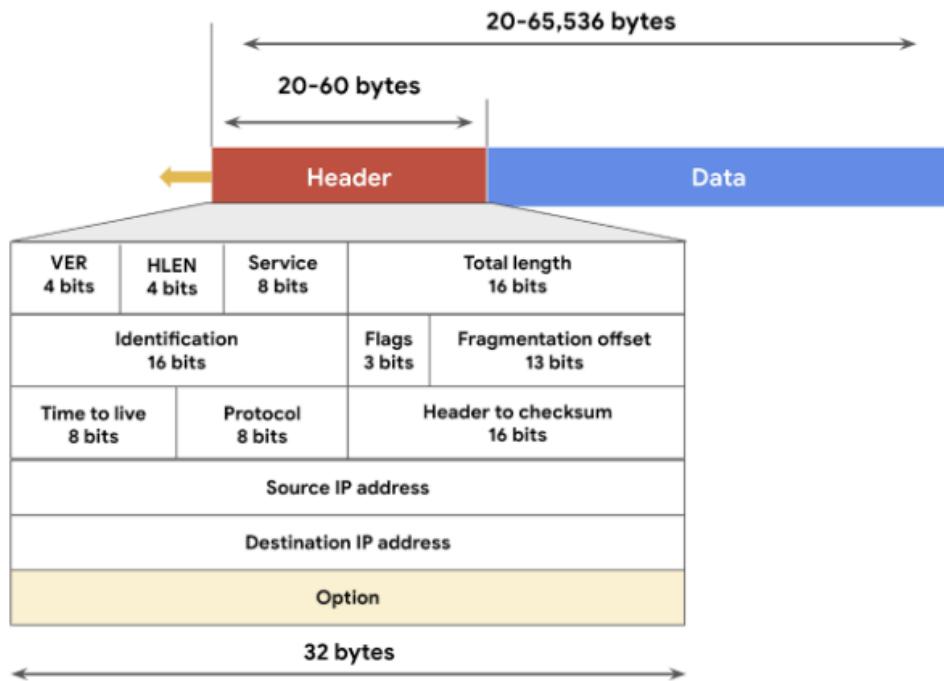
Todos los paquetes de datos incluyen una dirección IP, esto se denomina paquete IP o datagrama, lo cual lo usa el router con la IP para enrutar los paquetes entre redes, todo

esto basándose en la información contenida en el encabezado IP de un paquete de datos.

Formato de un paquete IPv4



- El tamaño del encabezado IP oscila de 20 a 60 bytes , Incluye la información de enrutamiento IP que los dispositivos utilizan para dirigir el paquete
- La longitud de la sección de datos de un paquete varía mucho pero el máximo es de 65.536 bytes



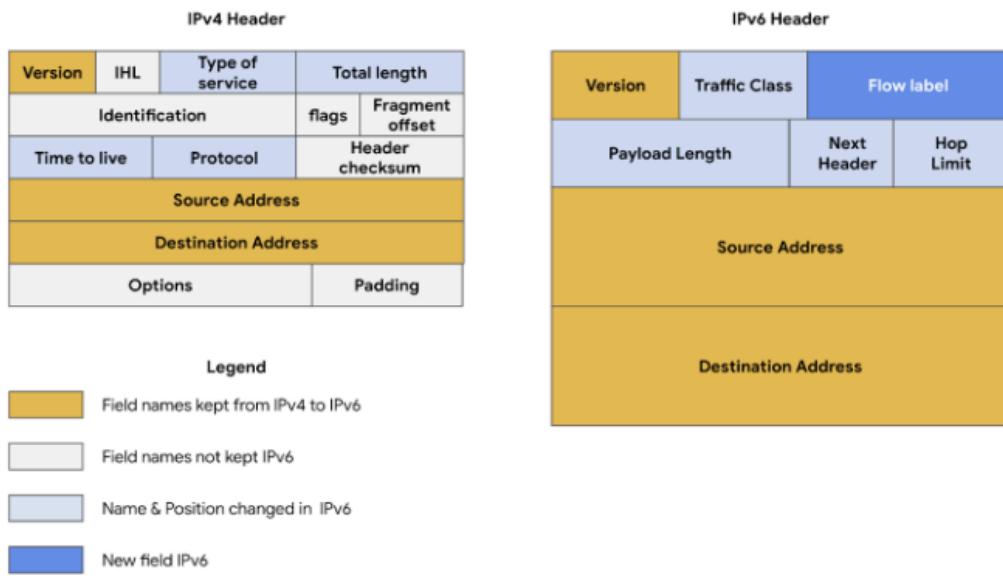
Hay 13 campos dentro del encabezado de un paquete IPv4:

- **Versión:** el primer encabezado de 4 bits indica a los dispositivos receptores qué protocolo está utilizando el paquete. El paquete utilizado en la ilustración anterior es un paquete IPv4.
- **Longitud del encabezado IP (HLEN):** HLEN es la longitud del encabezado del paquete. Este valor indica dónde termina el encabezado del paquete y comienza el segmento de datos.

- **Tipo de servicio (ToS):** los routers priorizan los paquetes a entregar con el fin de mantener la calidad del servicio en la red. El campo ToS proporciona esta información al router.
- **Longitud total:** este campo comunica la longitud total de todo el paquete IP, incluidos el encabezado y los datos. El tamaño máximo de un paquete IPv4 es de 65.535 bytes.
- **Identificación:** si el paquete IPv4 es superior a 65 535 bytes, se divide o fragmenta en paquetes IP más pequeños. El campo de identificación proporciona un identificador único para todos los fragmentos del paquete IP original para que puedan volver a ensamblarse cuando lleguen a su destino.
- **Indicadores:** este campo proporciona al dispositivo de enrutamiento más información sobre si el paquete original se fragmentó y si hay más fragmentos en tránsito.
- **Desplazamiento de fragmentación:** el campo de desplazamiento de fragmento indica a los dispositivos de enrutamiento a qué parte del paquete original pertenece el fragmento.
- **Período de vida (TTL):** evita que los routers reenvíen los paquetes de datos de manera indefinida. Contiene un contador que determina la fuente. El contador disminuye de a uno, a medida que pasa por cada router. Cuando el contador TTL llega a cero, el router descartará el paquete y enviará al emisor un mensaje de tiempo superado ICMP.
- **Protocolo:** este campo indica al dispositivo receptor qué protocolo se utilizará para el área de datos del paquete.
- **Suma de comprobación del encabezado:** este campo contiene una suma de comprobación que se puede usar para detectar si la cabecera IP en tránsito está dañada. Los paquetes dañados se descartan.
- **Dirección IP de origen:** es la dirección IPv4 del dispositivo emisor.
- **Dirección IP de destino:** es la dirección IPv4 del dispositivo receptor.
- **Opciones:** este campo permite aplicar opciones de seguridad al paquete si el valor HLEN es mayor que cinco. Además, comunica estas alternativas a los dispositivos de enrutamiento.

Diferencia entre IPv4 e IPv6

- Longitud de las direcciones IPv4 (4 bytes y 43000 millones de combinaciones posibles) y IPv6 (hexadecimales 16 bytes y 340 undecillones de direcciones (la cifra 340 seguida de 36 ceros))
- El encabezado de ipv6 es mas simple que ipv4



Componentes de Linux

Componentes principales de Linux

- El primer componente eres **tú**, el usuario. Interactúas con el sistema, iniciando tareas y comandos. Linux es un sistema multiusuario, lo que significa que varios usuarios pueden utilizarlo simultáneamente.
- Luego están las **aplicaciones**, como procesadores de texto o calculadoras, que te ayudan a realizar tareas específicas. Estas aplicaciones se suelen distribuir a través de gestores de paquetes.

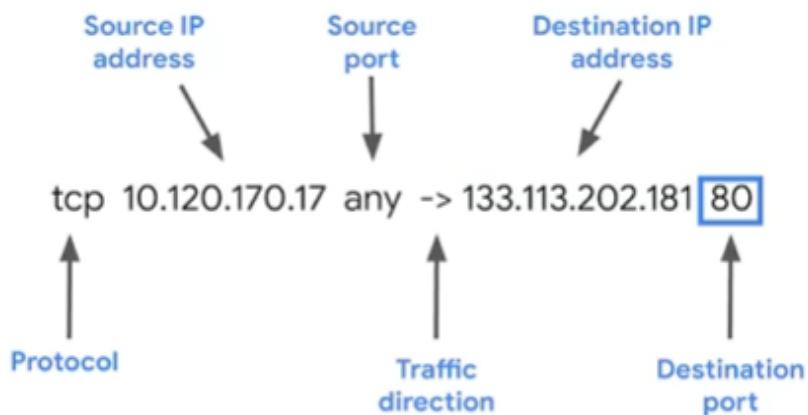
Interactuando con Linux

- Para comunicarte con Linux, utilizas el **shell**, un intérprete de línea de comandos que procesa tus instrucciones y muestra los resultados. Es como una interfaz de línea de comandos (CLI).
 - El **Estándar de Jerarquía del Sistema de Archivos (FHS)** organiza los datos como un archivador, lo que facilita al sistema encontrar y acceder a la información.
- el shell. Es importante porque permite comunicarte con el sistema. Este interpreta la línea de comandos. Procesa comandos y produce los resultados.
- el estándar de **jerarquía del sistema de archivos (FHS)**. Es el componente del SO Linux que organiza los datos. El FHS es como un archivador de datos. El FHS es la forma de almacenar datos en un sistema. Organiza los datos para encontrarlos cuando el sistema accede a ellos.

El kernel se comunica con el hardware y ejecuta comandos enviados por el shell.

Componentes de una firma de detección

1. Accion :La acción suele ser el primer elemento especificado en una firma. Esto determina la acción a realizar si se satisface la regla. Las acciones varían a través de los lenguajes de regla NIDS, pero algunas acciones comunes son: alertar, pasar o rechazar.
2. Encabezado / Header:El encabezado define el tráfico de red de la firma. Esto incluye información como direcciones IP de origen y destino, puertos de origen y destino, protocolos y dirección del tráfico. Si queremos detectar una alerta de tráfico sospechoso hacia un puerto, primero debemos definir la fuente de este tráfico en el encabezado. El tráfico sospechoso puede venir de direcciones IP fuera de la red local. También puede utilizar protocolos específicos e inusuales. Podemos especificar direcciones IP externas y estos protocolos en el encabezado. Este es un ejemplo de cómo se muestran datos del encabezado en una regla básica.
3. Opciones de Regla :permiten personalizar las firmas con parámetros adicionales. Existen diversas opciones que puedes usar. Por ejemplo, puedes crear opciones que coincidan con contenido de un paquete de red para detectar cargas maliciosas.



En este caso, la alerta imprimirá el texto:
"This is a message".

También está la opción sid, que significa ID de firma.

Esto adjunta una identificación única a cada firma.

La opción rev significa revisión.

Cuando una firma se actualiza o cambia, también lo hace el número de revisión.



Componentes Linux explicado

Explicación de la arquitectura Linux

Comprender la arquitectura Linux es importante para un/a analista de seguridad. Al entender cómo está estructurado un sistema, resulta más sencillo comprender cómo funciona. En esta lectura, explorarás con más detalle los componentes de la arquitectura Linux. El proceso de ejecución de una tarea comienza con los/las usuarios/as y continúa a través de las aplicaciones, el shell, el estándar de jerarquía del sistema de archivos (FHS), el kernel y, finalmente, el hardware.

Usuario/a

Los/las **usuarios/as** son las personas que interactúan con una computadora, siendo responsables de iniciar y administrar las tareas informáticas. En el caso de Linux, se trata de un sistema multiusuario, lo que implica que varias personas pueden utilizar los mismos recursos simultáneamente.

Aplicaciones

Una **aplicación** es un programa diseñado para realizar una tarea específica. En tu computadora, puedes encontrar diversas aplicaciones. Algunas de ellas vienen preinstaladas, como calculadoras o calendarios, mientras que otras necesitan ser instaladas, como ciertos navegadores web o clientes de correo electrónico. En el caso de

Linux, se utiliza comúnmente un gestor de paquetes para instalar aplicaciones. Un **gestor de paquetes** es una herramienta que ayuda a los/las usuarios/as a instalar, gestionar y desinstalar paquetes o aplicaciones. Vale aclarar que un **paquete** es un componente de software que puede combinarse con otros paquetes para formar una aplicación.

Shell

El **shell** es el intérprete de línea de comandos. Todo lo que se introduce en el shell se basa en texto. El shell permite a los/las usuarios/as enviar órdenes al kernel y recibir respuestas de él. Puedes pensar en el shell como un intérprete entre tú y tu computadora. Este traduce los comandos que ingreses para que la máquina pueda ejecutar las funciones que deseas.

Estándar de jerarquía del sistema de archivos (FHS)

El **estándar de jerarquía del sistema de archivos (FHS)** es el componente del sistema operativo Linux que organiza los datos. Este especifica la ubicación donde se almacenan los datos.

Un **directorio** es un archivo que organiza la ubicación de otros archivos. A veces, los directorios se llaman "carpetas" y pueden contener archivos u otros directorios. El FHS define cómo se organizan los directorios, el contenido de estos y otros elementos de almacenamiento, para que el sistema operativo sepa dónde encontrar datos específicos.

Kernel

El **kernel** es el componente del sistema operativo Linux que administra los procesos y la memoria. Se comunica con las aplicaciones para dirigir comandos. El kernel de Linux es exclusivo para este sistema operativo y desempeña un rol clave en la asignación de recursos del sistema. Este controla todas las funciones principales del hardware, lo que ayuda a acelerar la ejecución de las tareas de manera más eficiente.

Hardware

El **hardware** incluye los componentes físicos de una computadora. Es posible que estés familiarizado/a con algunos de estos, como los discos duros o las CPU. El hardware se clasifica como periférico o interno.

Dispositivos periféricos

Los **dispositivos periféricos** son componentes de hardware conectados y controlados por el sistema informático. No son componentes esenciales para el funcionamiento del sistema informático, y se pueden agregar o quitar libremente. Algunos ejemplos de dispositivos periféricos son los monitores, las impresoras, el teclado y el mouse.

Hardware interno

El **hardware interno** involucra los componentes necesarios para que funcione la computadora, como una placa de circuito principal, también denominada placa base, y todos los elementos conectados a ella. El hardware interno incluye:

- La **unidad central de procesamiento (CPU)**, que es el procesador principal de una computadora y que se utiliza para realizar tareas informáticas generales. La CPU ejecuta las instrucciones proporcionadas por los programas, permitiendo que estos se ejecuten.
- La **memoria de acceso aleatorio (RAM)**, que es un componente de hardware utilizado para la memoria a corto plazo. Es donde se almacenan temporalmente los datos mientras se realizan tareas en la computadora. Por ejemplo, si estás escribiendo un informe, los datos necesarios para que esto ocurra se almacenan en la memoria RAM. Cuando terminas de escribir el informe y cierras el programa, estos datos se eliminan de la memoria RAM. No se puede acceder a la información de la memoria RAM una vez que se ha apagado la computadora. La CPU toma los datos de la memoria RAM para ejecutar los programas.
- El **disco duro** es un componente de hardware utilizado para la memoria a largo plazo. Es donde se almacenan los programas y archivos para que la computadora pueda acceder a ellos posteriormente. Se puede acceder a la información en el disco duro incluso después de apagar y volver a encender la computadora. Una computadora puede tener varios discos duros.

Consideraciones para la continuidad del negocio

Planificación de la continuidad del negocio

Los equipos de seguridad deben estar preparados para minimizar el impacto que los incidentes de seguridad pueden tener en el desarrollo normal de un negocio. Cuando ocurre un incidente, las organizaciones pueden experimentar interrupciones significativas en la funcionalidad de sus sistemas y servicios, que pueden tener efectos graves, como perjuicios legales, financieros y de reputación. Las organizaciones deben utilizar la planificación de la continuidad del negocio para seguir operando durante cualquier interrupción importante.

Al igual que un plan de respuesta a incidentes, un **plan de continuidad del negocio (BCP)** es un documento que describe los procedimientos para mantener las operaciones comerciales durante y después de una interrupción significativa. Un BCP ayuda a las organizaciones a garantizar que las funciones comerciales críticas puedan reanudarse o restaurarse rápidamente cuando ocurre un incidente.

Los analistas de seguridad de nivel inicial no suelen ser responsables del desarrollo y las pruebas de un BCP. Sin embargo, es importante que comprendas cómo los BCP proporcionan a las organizaciones una forma estructurada de responder y recuperarse de los incidentes de seguridad.

Nota: Los planes de continuidad del negocio no son lo mismo que los *planes de recuperación ante desastres*. Estos se utilizan para recuperar sistemas de información en respuesta a un hecho grave, que puede ir desde fallas de hardware hasta la destrucción de las instalaciones por un desastre natural, como una inundación.

Los impactos del ransomware en la continuidad del negocio

Los impactos de un incidente de seguridad como el ransomware pueden ser devastadores para el funcionamiento de una organización. Los ataques de ransomware dirigidos a infraestructura crítica, como la de salud, pueden tener el potencial de causar interrupciones significativas. Dependiendo de la gravedad del ataque, pueden verse afectadas la accesibilidad, la disponibilidad y la prestación de servicios de salud esenciales. Por ejemplo, el ransomware puede cifrar datos, lo que resulta en la inhabilitación del acceso a los registros médicos y la imposibilidad de que los proveedores de atención médica accedan a los registros de los pacientes. A mayor escala, los incidentes de seguridad que tienen como objetivo los activos, sistemas y redes de infraestructura crítica también pueden comprometer la seguridad nacional y económica, y la salud y seguridad del público. La importancia de los BCP radica en que ayudan a minimizar las interrupciones en las operaciones para que se pueda acceder rápidamente a los servicios esenciales.

Estrategias de recuperación

Cuando se produce una interrupción debido a un incidente de seguridad, las organizaciones deben tener algún tipo de plan de recuperación operativo para resolver el problema y poner los sistemas en pleno funcionamiento. Los BCP pueden incluir estrategias para la recuperación que se centran en retomar las operaciones normales. La resiliencia del sitio es un ejemplo de estrategia de recuperación.

Resiliencia del sitio

La **resiliencia** es la capacidad de prepararse, responder y recuperarse de las alteraciones. Las organizaciones pueden diseñar sus sistemas para que sean resilientes y puedan continuar prestando servicios a pesar de enfrentar interrupciones. Un ejemplo es la resiliencia del sitio, que se utiliza para garantizar la disponibilidad de redes, centros de datos u otras infraestructuras cuando se produce una interrupción. Hay tres tipos de sitios de recuperación utilizados para la resiliencia del sitio:

- **Sitios calientes (Hot sites):** Instalaciones completamente operativas que replican el entorno primario de una organización. Los sitios calientes pueden activarse inmediatamente cuando el sitio principal de una organización experimenta fallas o interrupciones.
- **Sitios tibios (Warm sites):** Instalaciones que contienen una versión completamente actualizada y configurada del sitio caliente. A diferencia de estos, los sitios tibios no están completamente operativos y disponibles para su uso inmediato, pero pueden ponerse en funcionamiento rápidamente cuando se produce una falla o interrupción.

- **Sitios fríos (Cold sites)**: Instalaciones de respaldo equipadas con parte de la infraestructura necesaria para operar el sitio de una organización. Cuando se produce una interrupción o falla, los sitios fríos pueden no estar listos para su uso inmediato y tal vez requieran trabajo adicional para poder operar.

Consultas en SQL y filtros

Select	Indica que columnas devolver
From	Indica que tabla consultar

Al usar el * esto se denomina seleccionar todo

Consulta SQL básica

xisten dos palabras clave fundamentales en cualquier consulta SQL: **SELECT** y **FROM**. Las usarás cada vez que deseas consultar una base de datos SQL. Si las usas en conjunto, ayudarás a SQL a identificar los datos que necesitas de una base de datos y la tabla de la que los extraes.

El video demostró esta consulta SQL:

```
SELECT employee_id, device_id
FROM employees;
```

En lecturas y cuestionarios, este curso utiliza una base de datos de ejemplo denominada base de datos **Chinook**, para ejecutar las consultas. La base de datos **Chinook** incluye datos que se podrían crear en una empresa de medios digitales. Un/a analista de seguridad contratado/a por esta empresa puede necesitar consultar estos datos. Por ejemplo, la base de datos contiene once tablas, incluida una tabla **employees** (empleados/as), una tabla **customers** (clientes) y una tabla **invoices** (facturas). Estas tablas incluyen datos como nombres y direcciones.

A modo de ejemplo, puedes ejecutar esta consulta para obtener datos de la tabla **customers** (clientes) de la base de datos **Chinook**:

Antes de la consulta:

```
1  SELECT customerid, city, country
2  FROM customers;
```

Ejecutar

Restablecer

Después de la consulta:

CustomerId	City	Country
1	São José dos Campos	Brazil
2	Stuttgart	Germany
3	Montréal	Canada
4	Oslo	Norway
5	Prague	Czech Republic
6	Prague	Czech Republic
7	Vienne	Austria
8	Brussels	Belgium
9	Copenhagen	Denmark
10	São Paulo	Brazil
11	São Paulo	Brazil
12	Rio de Janeiro	Brazil
13	Brasília	Brazil
14	Edmonton	Canada
15	Vancouver	Canada
16	Mountain View	USA
17	Redmond	USA
18	New York	USA
19	Cupertino	USA
20	Mountain View	USA
21	Reno	USA
22	Orlando	USA
23	Boston	USA
24	Chicago	USA
25	Madison	USA

(Output limit exceeded, 25 of 59 total rows shown)

SELECT (seleccionar)

La palabra clave **SELECT** indica las columnas a devolver. Por ejemplo, puedes devolver la columna **customerid** (ID del cliente) de la base de datos **Chinook** con

```
SELECT customerid
```

También puedes seleccionar varias columnas separándolas con una coma. Por ejemplo, si quieres obtener las columnas **customerid** (ID del cliente) y **city** (ciudad), debes escribir

```
SELECT customerid, city.
```

Si quieres obtener todas las columnas en una tabla, después de la palabra clave **SELECT**, puedes escribir un asterisco (*). La primera línea de la consulta será **SELECT ***.

Nota: Si bien las tablas que estás consultando en este curso son relativamente pequeñas, no te recomendamos usar **SELECT *** cuando trabajes con bases de datos y tablas grandes; en esos casos, el resultado final puede ser difícil de entender y lento de ejecutar.

FROM (desde)

La palabra clave **SELECT** siempre viene con la palabra clave **FROM**. **FROM** indica qué tabla consultar. Para usar la palabra clave **FROM**, debes escribirla después de la palabra clave **SELECT**, generalmente en una línea nueva, y luego, escribir el nombre de la tabla que estás

consultando. Si quieras obtener todas las columnas de la tabla `customers` (clientes), puedes escribir:

```
SELECT *  
FROM customers;
```

Cuando quieras finalizar la consulta, escribe punto y coma (;) al final para indicar a SQL que la consulta está completa.

Nota: Los saltos de línea no son necesarios en consultas SQL, pero se suelen usar para facilitar la comprensión de la consulta. Si lo prefieres, también puedes escribir la consulta anterior en una línea como

```
SELECT * FROM customers;
```

ORDER BY (ordenar por)

Las tablas de bases de datos suelen ser muy complicadas, y por ello resultan útiles otras palabras clave de SQL. `ORDER BY` es una palabra clave importante para organizar los datos que extraes de una tabla.

`ORDER BY` ordena en secuencia los registros devueltos por una consulta con base en una o más columnas especificadas. Este orden puede ser ascendente o descendente.

Orden ascendente

Para usar la palabra clave `ORDER BY`, escríbela al final de la consulta y especifica una columna en la que se basará el orden. En este ejemplo, SQL devolverá las columnas `customerid` (ID del cliente), `city` (ciudad) y `country` (país) de la tabla `customers` (clientes), así como los registros se mostrarán secuencialmente en función de la columna `city` (ciudad):

```
1  SELECT customerid, city, country
2  FROM customers
3  ORDER BY city;
```

Ejecutar

Restablecer

CustomerId	City	Country
48	Amsterdam	Netherlands
59	Bangalore	India
36	Berlin	Germany
38	Berlin	Germany
42	Bordeaux	France
23	Boston	USA
13	Brasília	Brazil
8	Brussels	Belgium
45	Budapest	Hungary
56	Buenos Aires	Argentina
24	Chicago	USA
9	Copenhagen	Denmark
19	Cupertino	USA
58	Delhi	India
43	Dijon	France
46	Dublin	Ireland
54	Edinburgh	United Kingdom
14	Edmonton	Canada
26	Fort Worth	USA
37	Frankfurt	Germany
31	Halifax	Canada
44	Helsinki	Finland
34	Lisbon	Portugal
52	London	United Kingdom
53	London	United Kingdom

(Output limit exceeded, 25 of 59 total rows shown)

La palabra clave **ORDER BY** ordena los registros en función de la columna especificada después de esta palabra clave. Por defecto, como se muestra en este ejemplo, la secuencia estará en orden ascendente. Esto significa que:

- si eliges una columna que contiene datos numéricos, esta organiza los resultados de menor a mayor. Por ejemplo, si organizas en función de **customerid** (ID del cliente), los números de identificación se ordenan de menor a mayor.
- si la columna contiene caracteres alfabéticos, como en el ejemplo con la columna **city** (ciudad), esta organiza los registros de la A a la Z.

Orden descendente

También puedes usar **ORDER BY** con la palabra clave **DESC** para ordenar los datos en sentido descendente. La palabra clave **DESC** es la abreviatura de "descendente", e indica a SQL que ordene los números de mayor a menor o, en el caso de caracteres alfabéticos, de la Z a la A. Para hacerlo, después de **ORDER BY**, escribe la palabra clave **DESC**. A modo de ejemplo, puedes ejecutar esta consulta para observar cómo se diferencian los resultados cuando aplicas **DESC**:

```
1 SELECT customerid, city, country
2 FROM customers
3 ORDER BY city DESC;
```

Ejecutar

Restablecer

CustomerId	City	Country
33	Yellowknife	Canada
32	Winnipeg	Canada
49	Warsaw	Poland
7	Vienne	Austria
15	Vancouver	Canada
27	Tucson	USA
29	Toronto	Canada
10	São Paulo	Brazil
11	São Paulo	Brazil
1	São José dos Campos	Brazil
2	Stuttgart	Germany
51	Stockholm	Sweden
55	Sidney	Australia
57	Santiago	Chile
28	Salt Lake City	USA
47	Rome	Italy
12	Rio de Janeiro	Brazil
21	Reno	USA
17	Redmond	USA
5	Prague	Czech Republic
6	Prague	Czech Republic
35	Porto	Portugal
39	Paris	France
40	Paris	France
30	Ottawa	Canada

(Output limit exceeded, 25 of 59 total rows shown)

Ordenar en función de varias columnas

Adicionalmente, puedes elegir varias columnas en las que basar el orden. Por ejemplo, primero puedes elegir la columna `country` (país) y luego, la columna `city` (ciudad). A continuación, SQL ordena los resultados en función de la columna `country` (país) y, en el caso de que haya filas con el mismo valor de `country` (país), las organiza en función de la columna `city` (ciudad). Puedes practicar este ejemplo para averiguar cómo SQL muestra esto:

```

1  SELECT customerid, city, country
2  FROM customers
3  ORDER BY country, city;

```

Ejecutar
Restablecer

CustomerId	City	Country
56	Buenos Aires	Argentina
55	Sidney	Australia
7	Vienne	Austria
8	Brussels	Belgium
13	Brasília	Brazil
12	Rio de Janeiro	Brazil
1	São José dos Campos	Brazil
10	São Paulo	Brazil
11	São Paulo	Brazil
14	Edmonton	Canada
31	Halifax	Canada
3	Montréal	Canada
30	Ottawa	Canada
29	Toronto	Canada
15	Vancouver	Canada
32	Winnipeg	Canada
33	Yellowknife	Canada
57	Santiago	Chile
5	Prague	Czech Republic
6	Prague	Czech Republic
9	Copenhagen	Denmark
44	Helsinki	Finland
42	Bordeaux	France
43	Dijon	France
41	Lyon	France

(Output limit exceeded, 25 of 59 total rows shown)

Cómo ayuda el filtrado

Como analista de seguridad, a menudo deberás trabajar con registros muy voluminosos y complicados. Para encontrar la información que necesitas, con frecuencia deberás usar SQL para filtrar los registros.

En el contexto de la ciberseguridad, puedes usar filtros para identificar intentos de inicio de sesión de un usuario específico o todos los intentos de inicio de sesión realizados en el momento en que se produjo un incidente de seguridad. Como ejemplo adicional, puedes filtrar para encontrar dispositivos que están ejecutando una versión específica de una aplicación.

WHERE (dónde)

Para crear un filtro en SQL, debes usar la palabra clave **WHERE**. **WHERE** indica la condición para un filtro.

Si necesitaras enviar un correo electrónico a empleados/as con el cargo de 'IT Staff' (personal de TI), podrías usar una consulta como la del ejemplo que se presenta a continuación. Puedes ejecutar este ejemplo para examinar cuáles son los resultados:

1
2
3

SELECT firstname, lastname, title, email

```
FROM employees  
WHERE title = 'IT Staff';  
EjecutarRestablecer
```

En lugar de devolver todos los registros en la tabla **employees** (empleados/as), la cláusula **WHERE** indica a SQL que devuelva solo aquellos que contienen '**IT Staff**' (empleados/as de TI) en la columna **title** (cargo). Esta usa el operador de signo igual (=) para establecer esta condición.

Nota: Debes colocar el punto y coma (;) donde termina la consulta. Cuando agregas un filtro a una consulta básica, el punto y coma se coloca después del filtro.

Filtrado por patrones

También puedes filtrar en función de un patrón. Por ejemplo, puedes identificar las entradas que comienzan o terminan con uno o varios caracteres determinados. Filtrar en función de un patrón te exige incorporar dos elementos más en tu cláusula **WHERE**:

- un comodín
- el operador **LIKE**

Comodines

Un **comodín** es un carácter especial que se puede sustituir por cualquier otro carácter. Dos de los comodines más útiles son el signo de porcentaje (%) y el guion bajo (_):

- El signo de porcentaje puede sustituir cualquiera de los demás caracteres.
- El símbolo de guion bajo solo puede sustituir uno de los demás caracteres.

Puedes colocar estos comodines después de una cadena, antes de una cadena o en ambas ubicaciones, dependiendo del patrón según el cual estás filtrando.

La tabla siguiente incluye estos comodines aplicados a la cadena '**a**' y ejemplos de los resultados que devolverá cada patrón.

Patrón	Resultados que puede devolver
'a%'	apple123, art, a
'a_'	as, an, a7
'a__'	ant, add, a1c
'%a'	pizza, Z6ra, a
'_a'	ma, 1a, Ha
'%a%'	Again, back, a
'_a_'	Car, ban, ea7

LIKE (como)

Para aplicar comodines al filtro, debes usar el operador **LIKE** en lugar de un signo igual (=).

LIKE se usa con **WHERE** para buscar un patrón en una columna.

Por ejemplo, si quieras enviar un correo electrónico a empleados/as con el cargo '**IT Staff**' (personal de TI) o '**ITManager**' (gerente de TI), puedes usar el operador **LIKE** combinado con el comodín %:

```

1  SELECT lastname, firstname, title, email
2  FROM employees
3  WHERE title LIKE 'IT%';

```

Ejecutar
Restablecer

Lastname	Firstname	Title	Email
Mitchell	Michael	IT Manager	michael@chinookcorp.com
King	Robert	IT Staff	robert@chinookcorp.com
Callahan	Laura	IT Staff	laura@chinookcorp.com

Esta consulta devuelve todos los registros con valores en la columna **title** (cargo) que comienzan con el patrón de 'IT'. Esto significa que se devuelve tanto '**IT Staff**' (personal de TI) como '**IT Manager**' (gerente de TI).

Como ejemplo adicional, si quieras buscar en la tabla de facturas a todos/as los/las clientes ubicados en estados con la abreviatura '**NY**', '**NV**', '**NS**' o '**NT**', puedes usar el patrón '**N_**' en la columna **state** (estado):

```
1  SELECT firstname, lastname, state, country
2  FROM customers
3  WHERE state LIKE 'N_';
```

Ejecutar

Restablecer

FirstName	LastName	State	Country
Michelle	Brooks	NY	USA
Kathy	Chase	NV	USA
Martha	Silk	NS	Canada
Ellie	Sullivan	NT	Canada

criptografía

La criptografía convierte la información de forma que los no destinatarios no puedan entenderla.

ataque de fuerza bruta, un proceso de prueba y error para descubrir información privada. El otro gran defecto es que solo usa una clave.

La infraestructura de clave pública, o PKI, es un marco de cifrado que protege el intercambio de datos en línea. Es un sistema amplio que facilita y protege el acceso a la información. ¿Cómo funciona? El PKI es un proceso de dos pasos. Empieza con el intercambio de información cifrada. Esto implica cifrado asimétrico, simétrico o ambos.

Cifrado simétrico y asimétrico

Tipos de cifrado

Existen dos tipos principales de cifrado:

- **El cifrado simétrico** consiste en utilizar una única clave secreta para el intercambio de información. Debido a que emplea una sola clave tanto para el cifrado como para el descifrado, el remitente y el receptor deben conocer dicha clave para bloquear o desbloquear el cifrado.
- **El cifrado asimétrico** se basa en el uso de un par de claves: una pública, para cifrar los datos, y una privada, para descifrarlos. La clave privada solo se comparte con los usuarios con acceso autorizado.

La importancia de la longitud de la clave

Los cifrados son vulnerables a los ataques de fuerza bruta, que consisten en un proceso de prueba y error para descubrir información privada. Esta táctica es el equivalente digital de probar todas las códigos posibles de una cerradura de combinación, intentando encontrar el correcto. En el cifrado moderno, se considera que las claves más largas son más seguras. Una mayor longitud de clave implica más posibilidades que un atacante debe intentar para desbloquear un cifrado.

Una desventaja de tener claves de cifrado largas es que los tiempos de procesamiento son más lentos. Aunque las claves cortas suelen ser menos seguras, se calculan mucho más rápido. Lograr una comunicación de datos rápida en línea, manteniendo la información segura implica un delicado equilibrio.

Algoritmos aprobados

Muchas aplicaciones web utilizan una combinación de cifrado simétrico y asimétrico. De esta manera, equilibrar la experiencia de usuario con la protección de la información.

Como analista de seguridad, debes conocer cuáles son los algoritmos más utilizados.

Algoritmos simétricos

- *Triple DES (3DES)* es conocido como un cifrado por bloques debido a la forma en que convierte el texto simple, también llamado texto plano, en texto cifrado en "bloques". Sus orígenes se remontan al Data Encryption Standard (DES), que fue desarrollado a principios de la década de 1970. DES fue uno de los primeros algoritmos de cifrado simétrico que generó claves de 64 bits. Un **bit** es la unidad más pequeña de medición de datos en una computadora. Como podrás imaginar, Triple DES genera claves de 192 bits, es decir, tres veces más largas. A pesar de que las claves son más largas, muchas organizaciones están dejando de utilizar Triple DES debido a las limitaciones en la cantidad de datos que se pueden cifrar. Sin embargo, es probable que Triple DES siga utilizándose por motivos de compatibilidad con versiones anteriores.
- *Advanced Encryption Standard (AES)* es uno de los algoritmos simétricos más seguros de la actualidad. AES genera claves de 128, 192 o 256 bits. Se considera que las claves criptográficas de este tamaño están protegidas de ataques de fuerza bruta. Se estima que forzar una clave AES de 128 bits podría llevarle miles de millones de años a una computadora moderna.

Algoritmos asimétricos

- *Rivest, Shamir y Adleman (RSA)* debe su nombre a sus tres creadores, quienes lo desarrollaron en el Instituto Tecnológico de Massachusetts (MIT). RSA es uno de los primeros algoritmos de cifrado asimétrico que produce un par de claves pública y privada. Los algoritmos asimétricos, como RSA, generan longitudes de clave aún más largas. Esto se debe, en parte, al hecho de que estas funciones están creando dos claves. Los tamaños de clave RSA son 1024, 2048 o 4096 bits. RSA se utiliza principalmente para proteger datos altamente sensibles.

- *El Algoritmo de Firma Digital (DSA)* es un algoritmo asimétrico estándar que fue introducido por el Instituto Nacional de Estándares y Tecnología (NIST) a principios de la década de 1990. DSA también genera longitudes de clave de 2048 bits. Este algoritmo es ampliamente utilizado en la actualidad como complemento de RSA en infraestructuras de clave pública.

Generación de claves

Estos algoritmos deben ser implementados cuando una organización elige proteger sus datos. Una forma de hacerlo es mediante el uso de OpenSSL, que es una herramienta de línea de comandos de código abierto que se puede utilizar para generar claves públicas y privadas. OpenSSL es utilizado habitualmente en computadoras para verificar certificados digitales que se intercambian como parte de la infraestructura de clave pública.

Nota: OpenSSL es una opción entre varias herramientas disponibles que pueden generar claves utilizando cualquiera de estos algoritmos comunes.

Aunque muchas empresas utilizaban OpenSSL, ya no se recomienda su uso desde el descubrimiento del error Heartbleed en 2014.

Lo oscuro no es seguro

En el mundo de la criptografía, un cifrado debe demostrar ser invulnerable antes de afirmar que es seguro. Según el principio de Kerchoff, la criptografía debe diseñarse de tal manera que todos los detalles de un algoritmo, excepto la clave privada, puedan conocerse sin perder seguridad. Por ejemplo, puedes acceder a todos los detalles sobre cómo funciona el cifrado AES en línea y aun así sigue siendo invulnerable.

Ocasionalmente, las organizaciones implementan sus propios algoritmos de cifrado personalizados. Ha habido casos en los que estos sistemas criptográficos secretos han sido rápidamente descifrados después de hacerse públicos.

Consejo profesional: Un sistema criptográfico *no debe* considerarse seguro si su seguridad se basa en mantener en secreto su funcionamiento.

El cifrado está en todas partes

Ambos trabajan en conjunto para la seguridad con la experiencia de usuario.

Por ejemplo, los sitios web suelen emplear el cifrado asimétrico para proteger pequeños bloques de datos que son importantes, como nombres de usuario y contraseñas durante el proceso de inicio de sesión. Una vez que alguien obtiene acceso, el resto de su sesión en el sitio web suele cambiar al cifrado simétrico debido a su mayor rapidez.

Este tipo de encriptación de datos es cada vez más exigido por la ley. Regulaciones como el Estándar de Procesamiento de Información Federal (FIPS 140-3) y el Reglamento General de Protección de Datos (RGPD) establecen cómo se deben recopilar, usar y manejar los datos. Cumplir cualquiera de estas regulaciones es fundamental para demostrar a socios comerciales y gobiernos, que los datos de los clientes se manejan de manera responsable.

Cómo las intrusiones comprometen tu sistema

Ataques de interceptación de red

En los ataques de interceptación de red , se obstaculizan el trafico de red y se roba información valiosa, o se interfiere de algún modo la transmisión.

Los agentes de amenaza pueden usar herramientas de hardware o software para capturar e inspeccionar los datos de transito. Es lo que se conoce como **rastreo de paquetes (packet Sniffing)**. Ademas de ver informacion a la que no tienen derecho , los agentes de amenaza tambien pueden interceptar el trafico de red y alterarlo. Estos ataques pueden causar danos a la der de una organizacion al insertar modificaciones de codigo malicioso.

Por ejemplo, un/a atacante puede interceptar una transferencia bancaria y cambiar la cuenta que recibe los fondos por otra que esté bajo su control.

Ataques de puerta trasera

Una organizacion puede contar con muchas medidas de seguridad, como camaras, escaneres biometricos y codigos de acceso para evitar que los empleados entren y salgan sin ser vistos.

Las puertas traseras están pensadas para ayudar a los/las programadores/as a solucionar problemas o realizar tareas administrativas. Sin embargo, las/los atacantes también pueden instalarlas tras haber puesto en riesgo a una organización, para asegurarse el acceso permanente

Posibles repercusiones en una organización

Como ya aprendiste, los ataques a la red pueden tener un impacto negativo significativo en una organización. Examinemos algunas consecuencias potenciales.

- **Financieras:** cuando un sistema queda fuera de línea a causa de un ataque DoS, o si las operaciones comerciales se detienen o ralentizan por alguna otra táctica, una empresa no puede realizar las tareas que generan ingresos. Dependiendo del tamaño de la organización, la interrupción de las operaciones puede costar millones de dólares. Además, si un agente de amenaza consigue acceder a la información personal de las/los clientes, la empresa podría tener que afrontar importantes gastos en litigios y acuerdos, si las personas damnificadas recurren a la justicia.

- **Reputación:** los ataques también pueden tener un impacto negativo en la reputación de una organización. Si se hace público que una empresa ha experimentado un ataque cibernético, el público puede preocuparse por las prácticas de seguridad de la organización. Pueden dejar de confiarle su información personal y elegir a un competidor para satisfacer sus necesidades.
- **Seguridad pública:** un ataque a una red gubernamental puede afectar potencialmente a la seguridad y el bienestar de los/las ciudadanos/as de un país. En los últimos años, las agencias de defensa de todo el mundo están invirtiendo mucho en combatir las tácticas de guerra cibernética. Si un agente de amenaza consiguiera acceder a una red eléctrica, un sistema público de agua o incluso un sistema de comunicaciones militar, el público podría sufrir daños físicos, como consecuencia de un ataque de intrusión en la red.

Definición de ciberseguridad

La práctica de garantizar la confidencialidad, integridad y disponibilidad de la información protegida por redes, dispositivos, gente información de acceso no autorizado por criminales

Que protegen las personas de ciberseguridad

- Amenazas externas
- Amenazas internas : personas dentro de la organización o empleados de confianza (pueden ser accidentales o no :s)
- Que se cumplan las leyes y directrices que se requieran en los estándares de seguridad.
- Mantienen y aseguran la productividad
- Reducen costos
- Mantienen la confianza de la marca

Cumplimiento normativo (compliance) es el proceso de adhesión a normas internas y reglamentos externos que permite a las organizaciones evitar multas, auditorías y fallos de seguridad.

Marcos de seguridad son las directrices que se utilizan para elaborar planes de seguridad que ayuden a mitigar los riesgos y las amenazas a los datos y la privacidad.

Controles de seguridad son medidas diseñadas para reducir riesgos de seguridad específicos. Se utilizan junto a los marcos de seguridad para establecer una postura de seguridad sólida.

Postura de seguridad es la capacidad de una organización para administrar su defensa de activos y datos críticos y reaccionar ante los cambios. Una fuerte postura de seguridad conduce a un menor riesgo para la organización.

Agente de amenazas, o atacante malicioso, es cualquier persona o grupo que representa un riesgo para la seguridad, que puede afectar a computadoras, aplicaciones, redes o datos.

Amenaza interna es un riesgo a la seguridad producido por una persona que pertenece o perteneció a una empresa o tiene una relación directa o de confianza con ella. Por ejemplo, si un/a empleado/a hace clic accidentalmente en un enlace de correo electrónico malicioso, o si el agente de amenazas interno realiza intencionadamente una actividad de riesgo, como acceder a los datos sin autorización.

Seguridad de la red es un conjunto de prácticas que buscan evitar accesos no autorizados a la infraestructura de red de una organización. Esto incluye datos, servicios, sistemas y dispositivos que se almacenan en la red de una organización.

Seguridad en la nube es el proceso de garantizar que los activos almacenados en la nube estén configurados o establecidos correctamente, y su acceso limitado a los/as usuarios/as autorizados/as. La nube es una red formada por un conjunto de servidores o computadoras que almacenan recursos y datos en ubicaciones físicas remotas conocidas como centros de datos a los que se puede acceder a través de Internet. La seguridad en la nube es un subcampo creciente de la ciberseguridad que se centra específicamente en la protección de este tipo de datos, aplicaciones e infraestructuras.

Programación es el proceso que permite crear un conjunto específico de instrucciones para que una computadora ejecute tareas. Estas pueden incluir:

Automatización de tareas repetitivas (por ejemplo, buscar dominios maliciosos en una lista).

Revisión del tráfico web.

Alerta de actividades sospechosas.

PII (Personally Identifiable information) cualquier información usada internamente para la identidad individual. como por ejemplo:

- nombre

- fecha de nacimiento
- dirección física
- numero de teléfono
- correo electrónico
- IP

SPII sensitive personally identifiable information
informacion que se maneja con reglas estrictas
como numero de seguro,

Descripción general de las herramientas de detección

Por qué necesitas herramientas de detección

Las herramientas de detección funcionan de forma similar a los sistemas de seguridad para el hogar. Mientras que estos últimos monitorean y protegen las viviendas contra intrusiones, las herramientas de detección de ciberseguridad ayudan a las organizaciones a resguardar sus redes y sistemas contra accesos no deseados ni autorizados. Para que las organizaciones puedan proteger sus sistemas contra amenazas o ataques de seguridad, es fundamental que sean notificadas ante cualquier indicio de intrusión. Estas herramientas de detección mantienen a los profesionales de seguridad al tanto de la actividad que se desarrolla en una red o sistema. Para ello, monitorean de forma continua las redes y los sistemas en busca de cualquier actividad sospechosa. Una vez que se detecta algo inusual o sospechoso, la herramienta activa una alerta que notifica al profesional de seguridad, permitiéndole investigar y detener la posible intrusión.

Herramientas de detección

Como analista de seguridad, es probable que en algún momento te encuentres con herramientas de detección **IDS**, **IPS** y **EDR**. Por lo tanto, es importante que conozcas las diferencias que hay entre ellas. Aquí tienes una tabla comparativa que puede servirte como referencia:

Capacidad	IDS	IPS	EDR
Detecta actividad maliciosa	✓	✓	✓
Previene las intrusiones	N/A	✓	✓
Registra la actividad	✓	✓	✓
Genera alertas	✓	✓	✓
Realiza análisis de comportamiento	N/A	N/A	✓

Descripción general de las herramientas IDS

Un **sistema de detección de intrusiones (IDS)** es una aplicación que monitorea la actividad del sistema y emite alertas sobre posibles accesos no autorizados. Un IDS proporciona un seguimiento continuo de eventos de red para ayudar a protegerse contra amenazas o ataques de seguridad. El objetivo de un IDS es detectar actividades potencialmente maliciosas y generar una alerta. Un IDS *no* detiene ni previene la actividad. En su lugar, los profesionales de la seguridad investigarán la alerta y actuarán para detenerla, si es necesario.

Por ejemplo, un IDS puede enviar una alerta cuando identifica un inicio de sesión de usuario sospechoso, como una dirección IP desconocida que inicia sesión en una aplicación o un dispositivo a una hora inusual. Sin embargo, un IDS no detendrá ni impedirá acciones adicionales, como bloquear el inicio de sesión del usuario sospechoso. Algunos ejemplos de herramientas de IDS incluyen Zeek, Suricata, Snort® y Sagan.

Categorías de detección

Como analista de seguridad, investigarás las alertas que genera un IDS. Existen cuatro tipos de categorías de detección que deberías conocer:

1. **Un verdadero positivo** es el resultado de un análisis o una detección en el que un sistema de seguridad identifica correctamente un incidente real.

2. **Un verdadero negativo** es el resultado de un análisis o una detección en el que un sistema de seguridad identifica correctamente la inexistencia de incidentes. Esto ocurre cuando no existe actividad maliciosa y no se dispara ninguna alerta.
3. **Un falso positivo** es el resultado de un análisis que detecta erróneamente una amenaza y dispara una alerta. Esto ocurre cuando un IDS identifica una actividad como maliciosa, pero no lo es. Los falsos positivos son una molestia para los equipos de seguridad, porque pierden tiempo y recursos investigando una alerta ilegítima.
4. **Un falso negativo** es el resultado de un análisis que no detecta una amenaza existente y, por lo tanto, no activa una alerta. Esto ocurre cuando sucede una actividad maliciosa pero un IDS no la detecta. Los falsos negativos son peligrosos porque dejan a los equipos de seguridad sin saber de ataques legítimos a los que pueden ser vulnerables.

Descripción general de las herramientas IPS

Un **sistema de prevención de intrusiones (IPS)** es una aplicación que monitorea la actividad del sistema en busca de actividades intrusivas y toma medidas para detenerlas. Un IPS funciona de manera similar a un IDS. Sin embargo, el IPS monitorea la actividad del sistema para detectar y alertar sobre intrusiones, y también toma medidas para *prevenir* la actividad y minimizar sus efectos. Por ejemplo, un IPS puede enviar una alerta y modificar una lista de control de acceso en un router, para bloquear tráfico específico en un servidor.

Nota: Muchas herramientas IDS también pueden funcionar como IPS. Herramientas como Suricata, Snort y Sagan tienen capacidades tanto de IDS como de IPS.

Descripción general de las herramientas EDR

La **detección y respuesta de puntos de conexión (EDR)** es una aplicación que monitorea la actividad maliciosa en un punto de conexión. Las herramientas de EDR se instalan en los **puntos de conexión**, es decir, cualquier dispositivo conectado a una red. Algunos ejemplos incluyen los dispositivos de usuario final, como computadoras, teléfonos y tabletas, entre otros.

Las herramientas EDR monitorean, registran y analizan la actividad del sistema del punto de conexión para identificar, alertar y responder a actividades sospechosas. A diferencia de las herramientas de IDS o IPS, las de EDR recopilan datos de actividad del punto de conexión y realizan *análisis de comportamiento* para identificar patrones de amenazas. El análisis de comportamiento utiliza la potencia del aprendizaje automático y la inteligencia artificial para analizar el comportamiento del sistema e identificar actividades maliciosas o inusuales. Las herramientas de EDR también utilizan la *automatización* para detener los ataques sin la intervención manual de los profesionales de seguridad. Por ejemplo, si una herramienta de EDR detecta un proceso inusual que se inicia en la estación de trabajo de un usuario y que normalmente no se utiliza, puede bloquear automáticamente la ejecución del proceso.

Open EDR®, Bitdefender™ Endpoint Detection and Response y FortiEDR™ son ejemplos de herramientas de EDR.

Nota: La gestión de eventos e información de seguridad (SIEM) también tiene capacidades de detección, que verás más adelante.

Descripción general de las tácticas de interceptación

Análisis detallado del rastreo de paquetes

Es la práctica de capturar e inspeccionar paquetes de datos a través de una red, en una red privada, estos paquetes se dirigen al dispositivo de destino correspondiente de la red Tarjeta de interfaz de red (NIC)

Es un componente hardware que conecta el dispositivo a una red,

La NIC lee transmisión de datos y si conoce la dirección MAC del dispositivo acepta el paquete y lo envía al dispositivo.

La NIC se puede poner en modo promiscuo lo que significa que acepta todo el tráfico de la red.

Análisis detallado de la suplantación de IP

Tras detectar paquetes en la red, un agente de amenaza puede reemplazar las direcciones IP y MAC de dispositivos autorizados para realizar un ataque de suplantación de IP. Los cortafuegos (firewalls) pueden evitar los ataques de suplantación de IP si se los configura para que rechacen paquetes IP no autorizados y tráfico sospechoso.

Ataque en ruta

Un **ataque en ruta** se produce cuando un/a hacker intercepta la comunicación entre dos dispositivos o servidores que tienen una relación de confianza. La transmisión entre estos dos dispositivos de red de confianza podría contener información valiosa, como nombres de usuario y contraseñas que el agente de amenaza puede recopilar. Un ataque en ruta a veces se denomina **ataque de intromisión**, porque la/el hacker se esconde entre las comunicaciones de dos partes de confianza.

También puede ocurrir que la transmisión interceptada contenga una búsqueda en el sistema DNS. Recordarás de un video anterior que un servidor DNS traduce los nombres de dominio del sitio web en direcciones IP. Si un agente de amenaza intercepta una transmisión que contiene una búsqueda DNS, podría falsificar la respuesta DNS del servidor y redirigir un nombre de dominio a una dirección IP diferente, tal vez una que contenga código malicioso u otras amenazas. La forma más efectiva de protegerse contra un ataque en ruta es cifrar los datos en tránsito, por ejemplo, mediante TLS.

Ataque pitufo

Un **ataque pitufo** sucede cuando un atacante detecta la dirección IP de un usuario autorizado y la abruma con paquetes. Una vez que el paquete falsificado llega a la dirección de difusión, se envía a todos los dispositivos y servidores de la red.

En un ataque pitufo, la suplantación de IP se combina con otra técnica de denegación de servicio (DoS) para inundar la red con tráfico no deseado. Por ejemplo, el paquete falsificado podría incluir un ping del protocolo de mensajes de control de Internet (ICMP). Como aprendiste antes, ICMP se utiliza para solucionar problemas de una red. Pero si se transmiten demasiados mensajes ICMP, las respuestas de eco ICMP abruman a los servidores de la red y estos se apagan. Esto crea una denegación de servicio que puede detener las operaciones de una organización.

Una forma importante de protegerse contra un ataque pitufo es usar un cortafuegos avanzado que pueda monitorear cualquier tráfico inusual en la red. La mayoría de los cortafuegos de nueva generación (NGFW) incluyen funciones que detectan anomalías en la red para garantizar que se detecten transmisiones de gran tamaño antes de que tengan la oportunidad de derribar la red.

Ataque DoS

Como aprendiste, una vez que el agente de amenazas ha detectado el tráfico de red, puede hacerse pasar por un usuario autorizado. Un **ataque de denegación de servicio** es una clase de ataques en los que el atacante impide que el sistema comprometido realice una actividad legítima o responda al tráfico legítimo. Sin embargo, a diferencia de la suplantación de IP, el atacante no recibirá una respuesta del host objetivo. Todo lo relacionado con el paquete de datos está autorizado, incluida la dirección IP en el encabezado del paquete. En los ataques de suplantación de IP, el agente de amenazas utiliza paquetes IP que contienen direcciones falsas. Los/los atacantes siguen enviando paquetes que contienen direcciones IP falsas hasta que el servidor de red se bloquea.

Consejo profesional: Recuerda el principio de defensa en profundidad. No existe una estrategia perfecta para detener cada tipo de ataque. Puedes estratificar tu defensa mediante el uso de múltiples estrategias. En este caso, utilizar el cifrado estándar de la industria reforzará tu seguridad, además de que te permitirá defenderte de los ataques DoS en más de un nivel.

Descripción general de los formatos de archivo de registro

Previamente, aprendiste de qué manera los registros capturan eventos que ocurren en una red o sistema. En seguridad, los registros proporcionan detalles fundamentales sobre las actividades que ocurrieron en una organización, por ejemplo, quién inició sesión en una aplicación en un momento específico. Como analista de seguridad, usarás el **análisis de**

registros, que es el proceso de examinar registros para identificar eventos de interés. Saber cómo leer e interpretar los diferentes formatos de registro es importante, porque permite descubrir los detalles clave de un evento e identificar actividades inusuales o maliciosas. En esta lectura, revisaremos los siguientes formatos de registro:

- JSON
- Syslog
- XML
- CSV
- CEF

Notación de objetos JavaScript (JSON)

La notación de objetos JavaScript (JSON) es un formato de archivo que se utiliza para almacenar y transmitir datos. Es conocido por ser ligero, así como fácil de leer y escribir. Se usa para transmitir datos en tecnologías web, y también en entornos en la nube. La sintaxis de JSON deriva de la sintaxis de JavaScript. Si ya conoces JavaScript, es posible que sepas que JSON contiene componentes de JavaScript que incluyen:

- Parejas clave-valor
- Comas
- Comillas dobles
- Llaves
- Corchetes

Parejas clave-valor

Una **pareja clave-valor** es un conjunto de datos que representa dos elementos vinculados: una clave y su valor correspondiente. Consiste de una clave seguida de dos puntos y, luego, de un valor. Un ejemplo de una pareja clave-valor es `"Alert": "Malware"`.

Nota: Para que sea más fácil leerlos, se recomienda incluir un espacio después de los dos puntos para separar la clave del valor.

Comas

Las comas se utilizan para separar datos. Por ejemplo: `"Alert": "Malware", "Alert code": 1090, "severity": 10.`

Comillas dobles

Las comillas dobles se utilizan para encerrar datos de *texto*, lo cual también se conoce como cadena, por ejemplo: `"Alert": "Malware"`. Los datos que contienen números *no están* entre comillas, por ejemplo: `"Alert code": 1090`.

Llaves

Las llaves encierran un **objeto**, que es un tipo de dato que almacena datos en una lista separada por comas de parejas clave-valor. Estos objetos se suelen utilizar para describir varias propiedades para una clave determinada. Las entradas de registro JSON comienzan y terminan con una llave. En este ejemplo, `user` es el objeto que contiene varias propiedades:

```
"User"  
{  
    "id": "1234",  
    "name": "user"  
    "role": "engineer"  
}
```

Corchetes

Los corchetes se usan para encerrar un **array**, que es un tipo de datos que almacena información en una lista ordenada y separada por comas. Los arrays son útiles cuando es necesario almacenar datos, como un conjunto ordenado, por ejemplo: `["Administrators", "Users", "Engineering"]`.

Syslog

Syslog es un estándar para registrar y transmitir datos. Se puede usar para referirse a cualquiera de sus tres funciones:

1. **Protocolo:** El protocolo syslog se utiliza para transportar registros a un servidor centralizado para su gestión. Utiliza el puerto 514 para registros de texto plano y el puerto 6514 para registros cifrados.
2. **Servicio:** El servicio syslog actúa como un servicio de reenvío de registros que consolida registros de varias fuentes en una sola ubicación. Recibe y luego reenvía las entradas de registro de syslog a un servidor remoto.
3. **Formato de registro:** El formato de registro syslog es uno de los más utilizados que analizaremos. Es el formato de registro nativo utilizado en los sistemas Unix®. Consta de tres componentes: un encabezado, datos estructurados y un mensaje.

Ejemplo de registro syslog

Este es un ejemplo de entrada syslog que contiene los tres componentes: un encabezado seguido de datos estructurados y un mensaje:

```
<236>1 2022-03-21T01:11:11.003Z virtual.machine.com evntslog - ID01 [user@32473  
iut="1" eventSource="Application" eventID="9999"]
```

This is a log entry!

Encabezado

El encabezado contiene detalles, como la marca de tiempo, el nombre del host (que es el nombre del equipo que envía el registro), el nombre de la aplicación y la ID del mensaje.

- **Marca de tiempo:** en este ejemplo, es `2022-03-21T01:11:11.003z`, donde `2022-03-21` es la fecha en formato YYYY-MM-DD. Se usa `T` para separar la fecha y la hora. `01:11:11.003` es el formato de 24 horas de la hora, e incluye la cantidad de milisegundos `003`. `z` indica la zona horaria, que es Tiempo Universal Coordinado (UTC).
- **Nombre del host:** `virtual.machine.com`
- **Aplicación:** `evntslog`
- **ID del mensaje:** `ID01`

Datos estructurados

La parte de datos estructurados de la entrada de registro contiene información de registro adicional. Está encerrada entre corchetes y estructurada en parejas clave-valor. Aquí hay tres claves con valores correspondientes: `[user@32473 iut="1"`
`eventSource="Application" eventID="9999"]`.

Mensaje

Contiene un mensaje de registro detallado sobre el evento. En este caso, el mensaje es `This is a log entry!`.

Prioridad (PRI)

El campo de prioridad (PRI) indica la urgencia del evento registrado y está contenido entre los símbolos mayor y menor. En este ejemplo, el valor de prioridad es `<236>`. En general, cuanto menor sea el nivel de prioridad, más urgente es el evento.

Nota: Los encabezados syslog se pueden combinar con formatos JSON y XML. También existen formatos de registro personalizados.

XML (lenguaje de marcado extensible)

El XML (lenguaje de marcado extensible) es un lenguaje y un formato utilizado para almacenar y transmitir datos. Además, es un formato de archivo nativo utilizado en sistemas Windows. La sintaxis XML utiliza lo siguiente:

- Etiquetas
- Elementos
- Atributos

Etiquetas

XML utiliza etiquetas para almacenar e identificar datos. Las etiquetas son pares que deben contener una de inicio y una de finalización. La etiqueta de inicio encierra los datos entre símbolos de mayor y menor, por ejemplo `<tag>`, mientras que una etiqueta de finalización los encierra con símbolos de mayor y menor y una barra invertida, así: `</tag>`.

Elementos

Los elementos XML incluyen los datos contenidos dentro de una etiqueta y la etiqueta en sí. Todas las entradas XML deben contener al menos un elemento raíz. Los elementos raíz contienen otros elementos que se encuentran debajo de ellos, conocidos como elementos secundarios.

He aquí un ejemplo:

```
<Event>

<EventID>4688</EventID>

<Version>5</Version>

</Event>
```

En este ejemplo, **<Event>** es el elemento raíz, y contiene dos elementos secundarios **<EventID>** y **<Version>**. Hay datos contenidos en cada elemento secundario.

Atributos

Los elementos XML también pueden contener atributos. Se utilizan para proporcionar información adicional sobre los elementos. Además, se incluyen como la segunda parte de la etiqueta en sí misma y siempre se deben citar con comillas simples o dobles.

Por ejemplo:

```
<EventData>

<Data Name='SubjectUserSid'>S-2-3-11-160321</Data>

<Data Name='SubjectUserName'>JSMITH</Data>

<Data Name='SubjectDomainName'>ADCOMP</Data>

<Data Name='SubjectLogonId'>0x1cf1c12</Data>

<Data Name='NewProcessId'>0x1404</Data>

</EventData>
```

En la primera línea de este ejemplo, la etiqueta es **<Data>** y usa el atributo **Name='SubjectUserSid'** para describir los datos incluidos en la etiqueta **S-2-3-11-160321**.

CSV (valor separado por comas)

El CSV (valor separado por comas) utiliza comas para separar los valores de datos. En los registros CSV, la posición de los datos corresponde al nombre del campo, pero los propios nombres del campo podrían no estar incluidos en el registro. Es fundamental comprender qué campos incluye el dispositivo de origen (como un IPS, firewall, escáner, etc.) en el registro.

Ejemplo:

```
2009-11-24T21:27:09.534255,ALERT,192.168.2.7,  
1041,x.x.250.50,80,TCP,ALLOWED,1:2001999:9,"ET MALWARE BTGrab.com Spyware  
Downloading Ads",1
```

CEF (formato de evento común)

El **formato de evento común (CEF)** es un formato de registro que utiliza parejas clave-valor para estructurar datos e identificar campos y sus valores correspondientes. La sintaxis CEF contiene los siguientes campos:

```
CEF:Version|Device Vendor|Device Product|Device Version|Signature  
ID|Name|Severity|Extension
```

Todos los campos están separados por una barra vertical |, también denominada pleca.

Sin embargo, todo lo que vaya en la parte **Extension** de la entrada de registro CEF se debe escribir en un formato de clave-valor. Syslog es un método común utilizado para transportar registros como el CEF. Si se usa syslog, antes del mensaje CEF se indicarán la marca de tiempo y el nombre del host. Este es un ejemplo de una entrada de registro CEF que detalla la actividad maliciosa relacionada con una infección por un gusano:

```
Sep 29 08:26:10 host CEF:1|Security|threatmanager|1.0|100|worm  
successfully stopped|10|src=10.0.0.2 dst=2.1.2.2 spt=1232
```

Este es el desglose de cada campo:

- **Syslog Timestamp (marca de tiempo de syslog):** 29 sept 08:26:10
- **Syslog Hostname (nombre del host de syslog):** host
- **Version (versión):** CEF:1
- **Device Vendor (proveedor del dispositivo):** Seguridad
- **Device Product (producto del dispositivo):** threatmanager
- **Device Version (versión del dispositivo):** 1.0
- **Signature ID (ID de firma):** 100
- **Name (nombre):** gusano detenido exitosamente
- **Severity (gravedad):** 10
- **Extension (extensión):** Este campo contiene datos escritos como parejas clave-valor. Hay dos direcciones IP, **src=10.0.0.2** y **dst=2.1.2.2**, y un número de puerto de origen **spt=1232**. No se requieren extensiones, y agregarlas es opcional.

Esta entrada de registro contiene detalles sobre una aplicación de **Security** que se llama **threatmanager** (*gestor de amenazas*) que *detuvo con éxito* la propagación de un *gusano*.

(successfully stopped a worm) desde la red interna en 10.0.0.2 a la red externa 2.1.2.2 a través del puerto 1232. Se indica un alto nivel de gravedad de 10.

Nota: Es opcional agregar extensiones y el prefijo syslog a un registro CEF.

Descripción general de tcpdump

¿Qué es tcpdump?

Tcpdump es un analizador de protocolos de red con línea de comandos. Una **interfaz de línea de comandos (CLI)** es una interfaz de usuario basada en texto que utiliza comandos para interactuar con la computadora.

Se utiliza para capturar el tráfico de red, que puede guardarse en un **pcap**, es decir, un archivo que contiene paquetes de datos interceptados desde una interfaz o red. Al archivo pcap se puede acceder, o también puede ser analizado o compartido en otra ocasión. Los analistas utilizan tcpdump por una variedad de razones, desde la resolución de problemas de red hasta la identificación de actividades maliciosas. Tcpdump viene preinstalado en muchas distribuciones de Linux y también se puede instalar en otros sistemas operativos basados en Unix, como macOS®.

Nota: Es habitual que el tráfico de red esté cifrado, lo que significa que los datos están codificados o no se pueden leer. Inspeccionar los paquetes de red puede requerir descifrar los datos mediante las claves privadas apropiadas.

Cómo capturar paquetes con tcpdump

Anteriormente, aprendiste que un **usuario root (raíz) o superusuario de Linux** tiene privilegios importantes para modificar el sistema. También, viste que el comando **sudo** otorga temporalmente permisos importantes a usuarios específicos en Linux. Al igual que muchas otras herramientas de rastreo de paquetes, deberás tener privilegios a nivel de administrador para capturar el tráfico de red mediante tcpdump. Esto significa que tendrás que iniciar sesión como usuario root o tener la capacidad de usar el comando sudo. Aquí se muestra un desglose de la sintaxis tcpdump para capturar paquetes:

sudo tcpdump [-i interface] [option(s)] [expression(s)]

- El comando **sudo tcpdump** comienza a ejecutar tcpdump con permisos importantes como sudo.
- El parámetro **-i** especifica la interfaz de red para capturar el tráfico de red. Debes especificar una interfaz de red desde la que capturar para comenzar a capturar paquetes. Por ejemplo, si especificas **-i any**, detectarás el tráfico de todas las interfaces de red del sistema.

- Las **option(s)** son facultativas y te brindan la capacidad de alterar la ejecución del comando. Las **expression(s)** son una forma de filtrar aún más los paquetes de tráfico de red para que puedas aislarlo. En la siguiente sección, aprenderás más sobre las **option(s)** y **expression(s)**.

Nota: Antes de que puedas comenzar a capturar tráfico de red, debes identificar qué interfaz de red deseas usar para capturar paquetes. Puedes usar el indicador **-D** para enumerar las interfaces de red disponibles en un sistema.

Opciones

Con tcpdump, puedes aplicar opciones, también conocidas como indicadores, al final de los comandos para filtrar el tráfico de red. Las opciones cortas se abrevian y se representan con un guión y un solo carácter como **-i**. Las opciones largas, en tanto, se explican con un guión doble como **--interface**. Tcpdump tiene más de 50 opciones que puedes explorar a través de [la página man](#). Aquí, examinarás un par de opciones claves de tcpdump, que incluyen cómo escribir y leer archivos de captura de paquetes.

Nota: Las opciones distinguen entre mayúsculas y minúsculas. Por ejemplo, una **-w** minúscula es una opción separada con un uso diferente que la opción con una **-W** mayúscula.

Nota: Las opciones de tcpdump que se escriben mediante opciones cortas se pueden escribir con o sin un espacio entre la opción y su valor. Por ejemplo, **sudo tcpdump -i any -c 3** y **sudo tcpdump -i any -c3** son comandos equivalentes.

-w

Con el indicador **-w**, puedes escribir o guardar los paquetes de red rastreados en un archivo de captura de paquetes en lugar de solo imprimirllos en la terminal. Esto resulta de mucha utilidad porque puedes consultar este archivo guardado para su posterior análisis. En este comando, tcpdump captura el tráfico de todas las interfaces de red y lo guarda en un archivo de captura de paquetes llamado **packetcapture.pcap**:

sudo tcpdump -i any -w packetcapture.pcap

-r

Con el indicador **-r**, puedes leer un archivo de captura de paquetes especificando el nombre del archivo como parámetro. Aquí te mostramos un ejemplo de un comando tcpdump que lee un archivo llamado **packetcapture.pcap**:

sudo tcpdump -r packetcapture.pcap

-v

Como ya viste, los paquetes contienen mucha información. De forma predeterminada, tcpdump no imprimirá toda la información de un paquete. Esta opción te permite controlar la cantidad de información de paquetes que deseas que tcpdump imprima. Existen tres niveles de verbosidad que puedes usar según la cantidad de información del paquete que deseas que tcpdump imprima. Los niveles son **-v**, **-vv**, y **-vvv**. El nivel de verbosidad aumenta con cada v agregada. La opción más verbosa (abundancia de detalles) puede resultar útil si buscas información de paquetes, como los detalles de los campos de

encabezado IP. A continuación, se muestra un ejemplo de un comando tcpdump que lee el archivo **packetcapture.pcap**:

sudo tcpdump -r packetcapture.pcap -v

-c

La opción **-c** significa conteo. Esta opción te permite controlar cuántos paquetes capturará tcpdump. Por ejemplo, especificar **-c 1** imprimirá un solo paquete, mientras que **-c 10** imprimirá 10. Este ejemplo le indica a tcpdump que solo capture los primeros tres paquetes que rastrea desde **any** (cualquier) interfaz de red:

sudo tcpdump -i any -c 3

-n

De forma predeterminada, tcpdump realizará la resolución de nombres. Esto significa que tcpdump convierte automáticamente las direcciones IP en nombres. También resolverá puertos a servicios comúnmente asociados que usan estos puertos. Esto puede ser problemático porque tcpdump no siempre es preciso en la resolución de nombres. Por ejemplo, tcpdump puede capturar tráfico desde el puerto 80 y traducir automáticamente el puerto 80 a HTTP en la salida. Aun así, esto es engañoso porque el puerto 80 no siempre va a utilizar HTTP, sino que podría estar utilizando un protocolo diferente. Además, la resolución de nombres utiliza lo que se conoce como una búsqueda inversa de DNS, que es una consulta que busca el nombre de dominio asociado con una dirección IP. Si realizas una búsqueda inversa de DNS en el sistema de un atacante, puede que se les avise que los estás investigando a través de sus registros de DNS.

El uso del indicador **-n** deshabilita este mapeo automático de números a nombres y se considera la mejor práctica al rastrear o analizar el tráfico. El uso de **-n** no resolverá los nombres de host, mientras que **-nn** no resolverá *ni* los nombres de host ni los puertos.

Aquí podrás ver un ejemplo de un comando tcpdump que lee el archivo **packetcapture.pcap** con verbosidad (abundancia de detalles) y deshabilita la resolución de nombres:

sudo tcpdump -r packetcapture.pcap -v -n

Consejo profesional: Puedes combinar las opciones. Por ejemplo, **-v** y **-n** se pueden combinar como **-vn**. Pero, si una opción acepta un parámetro justo después de él como **-c 1** o **-r capture.pcap**, entonces no podrás combinarlas.

Expresiones

El uso de expresiones de filtro en comandos tcpdump también es opcional, pero puede resultar útil saber cómo y cuándo usar expresiones de filtro durante el análisis de paquetes. Existen muchas maneras de utilizar las expresiones de filtro.

Si deseas buscar tráfico de red por protocolo en específico, puedes utilizar expresiones de filtro para aislar los paquetes de red. Por ejemplo, puedes filtrar para encontrar solo tráfico IPv6 mediante la expresión de filtro **ipv6**.

También puedes usar operadores booleanos como **and** (y), **or** (o) o **not** (no) para filtrar aún más el tráfico de red para direcciones IP específicas, puertos y más. El siguiente

ejemplo lee el archivo **packetcapture.pcap** y combina dos expresiones **ipv4 and port 80** con el operador booleano **and** (y):

```
sudo tcpdump -r packetcapture.pcap -n 'ipv4 and port 80'
```

Consejo profesional: Puedes usar comillas simples o dobles para asegurarte de que tcpdump ejecute todas las expresiones. También puedes usar paréntesis para agrupar y priorizar diferentes expresiones. Agrupar expresiones es útil para comandos complejos o largos. Por ejemplo, el comando **ipv4 and (port 80 or port 443)** le indica a tcpdump que priorice la ejecución de los filtros encerrados entre paréntesis antes de filtrar para IPv4.

Interpretación de la salida

Una vez que ejecutes un comando para capturar paquetes, tcpdump imprimirá la salida del comando como los paquetes rastreados. En la salida, tcpdump imprime una línea de texto para cada paquete con cada línea, comenzando con una marca de tiempo. Aquí se muestra un ejemplo de un comando y la salida para un solo paquete TCP:

```
sudo tcpdump -i any -v -c 1
```

Este comando le indica a tcpdump que capture paquetes en interfaz de red **-i any**. La opción **-v** imprime el paquete con información detallada y la opción **-c 1** imprime solo un paquete. Esta es la salida de este comando:

Timestamp	Source IP	Source port	Destination IP	Destination port
20:00:29.538395	IP 198.168.10.1.41	>	198.111.123.1.61012	: Flags
[P.], seq 120:176, ack 1, win 501, options [nop,nop,TS val 4106659748 ecr 2979487360], length 144				

- Marca de tiempo:** La salida comienza con la marca de tiempo, que empieza con horas, minutos, segundos y fracciones de segundo.
- IP de origen:** El origen del paquete lo proporciona su dirección IP de origen.
- Puerto de origen:** Este número de puerto es donde se originó el paquete.
- IP de destino:** La dirección IP de destino es donde se transmite el paquete.
- Puerto de destino:** Este número de puerto es donde se transmite el paquete.

La salida restante contiene detalles de la conexión TCP e incluye indicadores y número de secuencia. La información de **options** es información de paquetes adicionales que proporcionó la opción **-v**.

Detalles del paquete

Protocolo de Internet (IP)

Los paquetes constituyen la base del intercambio de datos en una red, lo que significa que la detección comienza a nivel de paquetes. El **Protocolo de Internet (IP)** incluye un

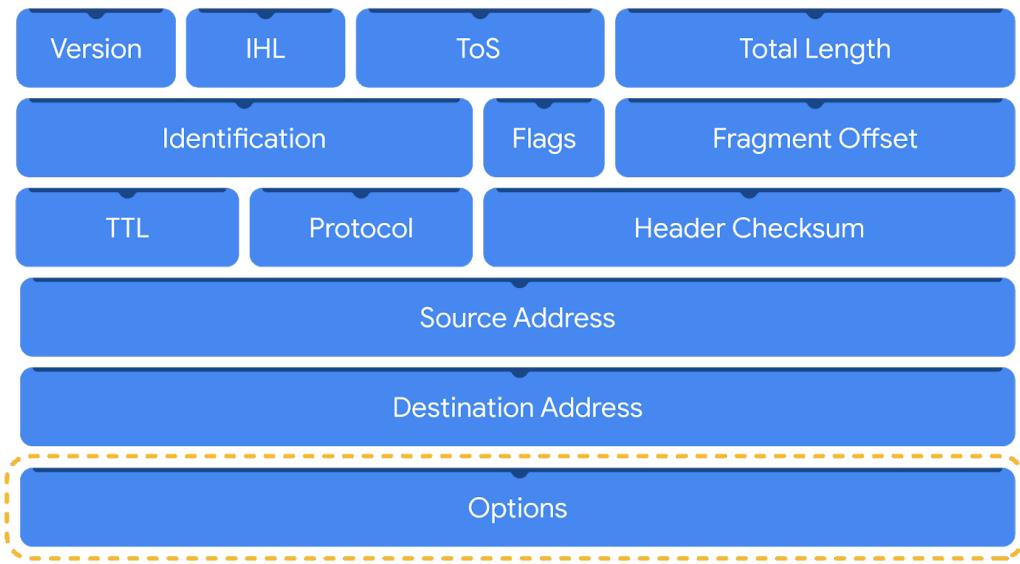
conjunto de estándares utilizados para enrutar y direccionar paquetes de datos mientras viajan de un dispositivo a otro en una red. El IP opera como la base para todas las comunicaciones a través de Internet.

El IP se encarga de garantizar que los paquetes lleguen a sus destinos. Existen dos versiones de IP en uso en la actualidad: IPv4 e IPv6. Ambas versiones utilizan encabezados diferentes para estructurar la información de los paquetes.

IPv4

IPv4 es la versión más utilizada de IP. En el encabezado hay 13 campos:

- **Versión:** Indica la versión de IP. Para un encabezado IPv4, se utiliza IPv4.
- **Longitud del encabezado de Internet (IHL):** Especifica la longitud del encabezado IPv4, incluidas las opciones.
- **Tipo de servicio (ToS):** Proporciona información sobre la prioridad del paquete para la entrega.
- **Longitud total:** Especifica la longitud total de todo el paquete IP, incluidos el encabezado y los datos.
- **Identificación:** Especifica un identificador único para fragmentos de un paquete IP original para que puedan volver a ensamblarse una vez que lleguen a su destino. Esto es así porque los paquetes que son demasiado grandes para enviar se fragmentan en piezas más pequeñas.
- **Indicadores:** Proporciona información sobre la fragmentación de paquetes, incluso si se fragmentó el paquete original y si hay más fragmentos en tránsito.
- **Desplazamiento de fragmentos:** Se utiliza para identificar la secuencia correcta de los fragmentos.
- **Tiempo de vida (TTL):** Limita el tiempo que un paquete puede circular en una red, lo que evita que los routers envíen los paquetes de forma indefinida.
- **Protocolo:** Especifica el protocolo utilizado para el área de datos del paquete.
- **Suma de comprobación de cabecera:** Especifica un valor de suma de comprobación que se utiliza para comprobar el error del encabezado.
- **Dirección de origen:** Especifica la dirección de origen del emisor.
- **Dirección de destino:** Especifica la dirección de destino del receptor.
- **Opciones:** Es opcional y se puede utilizar para aplicar opciones de seguridad a un paquete.



IPv6

Gracias a su gran espacio de direcciones, la adopción de IPv6 ha ido en aumento. Su encabezado cuenta con ocho campos:

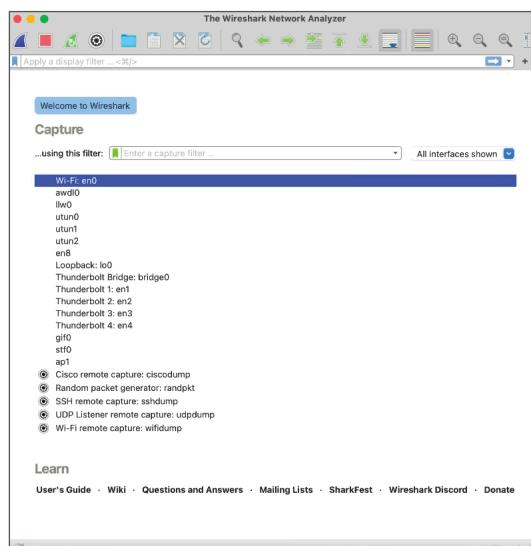
- **Versión:** Indica la versión de IP. Para un encabezado IPv6, se utiliza IPv6.
- **Clase de tráfico:** Similar al campo Tipo de servicio IPv4, proporciona información sobre la prioridad o clase del paquete para ayudar con la entrega.
- **Etiqueta de flujo:** Identifica los paquetes de un flujo. Un flujo es la secuencia de paquetes enviados desde una fuente específica.
- **Longitud de carga útil:** Especifica la longitud del área de datos del paquete.
- **Encabezado siguiente:** Indica el tipo de encabezado que sigue al encabezado IPv6, como TCP.
- **Límite de salto:** Similar al campo Tiempo de vida de IPv4, restringe el tiempo que un paquete puede viajar en una red antes de que se descarte.
- **Dirección de origen:** Especifica la dirección de origen del emisor.
- **Dirección de destino:** Especifica la dirección de destino del receptor.



Los campos de encabezado contienen información valiosa para investigaciones y herramientas como Wireshark que ayudan a mostrarlos en un formato legible para las personas.

Wireshark

Wireshark es un analizador de protocolos de red de código abierto. Utiliza una interfaz gráfica de usuario (GUI), lo que facilita la visualización de las comunicaciones de red con fines de análisis de paquetes. Wireshark tiene muchas características para explorar que no se alcanzan a cubrir en este curso. Te enfocarás en cómo usar el filtrado básico para aislar los paquetes de red de modo que puedas encontrar lo que necesitas.



Filtros de visualización

Los filtros de visualización de Wireshark te permiten aplicar filtros a archivos de captura de paquetes. Esto es útil cuando estás inspeccionando capturas de paquetes con grandes

volúmenes de información. Los filtros de visualización te ayudarán a encontrar información específica que sea relevante para tu investigación. Puedes filtrar paquetes en función de información como protocolos, direcciones IP, puertos y cualquier otra propiedad encontrada en un paquete. Aquí te centrarás en la sintaxis de filtrado de visualización y en el filtrado de protocolos, direcciones IP y puertos.

Operadores de comparación

Puedes utilizar diferentes operadores de comparación para localizar campos y valores específicos en los encabezados. Los operadores de comparación pueden expresarse utilizando abreviaturas o símbolos. Por ejemplo, este filtro que utiliza el símbolo igual == en este filtro `ip.src == 8.8.8.8` es idéntico al uso de la abreviatura eq en este filtro `ip.src eq 8.8.8.8`.

Esta tabla resume los diferentes tipos de operadores de comparación que puedes utilizar para el filtrado de visualización.

Tipo de operador	Símbolo	Abreviatura
Igual	==	eq
No es igual	!=	ne
Mayor que	>	gt
Menor que	<	lt
Mayor que o igual a	>=	ge
Menor que o igual a	<=	le

Consejo profesional: Puedes combinar operadores de comparación con operadores lógicos booleanos como `and` (y) y `or` (o) para crear filtros de visualización complejos. Los paréntesis también se pueden utilizar para agrupar expresiones y priorizar términos de búsqueda.

Operador contains

El operador `contains` se utiliza para filtrar paquetes que contienen una coincidencia exacta de una cadena de texto. Aquí, podrás ver un ejemplo de un filtro que muestra todos los flujos HTTP que coinciden con la palabra clave "moved" (movido).

The screenshot shows the Wireshark interface with a search bar at the top containing the text "http contains \"moved\"". Below the search bar is a table of network captures. The first two rows are highlighted in green, indicating they match the search criteria. The columns are labeled: No., Time, Source, Destination, Protocol, Length, and Info. The matching rows show HTTP requests from 142.250.1.139 and 142.250.1.102 to 172.21.224.2, both resulting in a "Moved Permanently" response.

No.	Time	Source	Destination	Protocol	Length	Info
69	18.036927	142.250.1.139	172.21.224.2	HTTP	648	HTTP/1.1 301 Moved Permanently (text/html)
150	42.370267	142.250.1.102	172.21.224.2	HTTP	657	HTTP/1.1 301 Moved Permanently (text/html)

Operador matches

El operador **matches** se utiliza para filtrar paquetes basados en la expresión regular (regex) que se especifica. La expresión regular es una secuencia de caracteres que forma un patrón. Más adelante en este programa, explorarás más sobre las expresiones regulares.

Barra de herramientas de filtrado

Puedes aplicar filtros a una captura de paquetes mediante la barra de herramientas de filtrado de Wireshark. En este ejemplo, **dns** es el filtro aplicado, lo que significa que Wireshark solo mostrará paquetes que contengan el protocolo DNS.

The screenshot shows the Wireshark interface with a red box highlighting the search bar at the top containing the text "dns". Below the search bar is a table of network captures. The first 10 rows are highlighted in blue, indicating they match the search criteria. The columns are labeled: No., Time, Source, Destination, Protocol, Length, and Info. The matching rows show DNS queries from various sources to 169.254.169.254, with responses ranging from 81 to 120 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
9	8.637619	172.21.224.2	169.254.169.254	DNS	81	Standard query 0x0c26 A op
10	8.637625	172.21.224.2	169.254.169.254	DNS	81	Standard query 0xd638 AAAA
11	8.641838	169.254.169.254	172.21.224.2	DNS	193	Standard query response 0x
12	8.641978	169.254.169.254	172.21.224.2	DNS	177	Standard query response 0x
19	8.644093	172.21.224.2	169.254.169.254	DNS	86	Standard query 0xb549 PTR
20	8.647339	169.254.169.254	172.21.224.2	DNS	120	Standard query response 0x
27	9.645214	172.21.224.2	169.254.169.254	DNS	86	Standard query 0x3cdc PTR
28	9.645859	169.254.169.254	172.21.224.2	DNS	120	Standard query response 0x
33	10.646715	172.21.224.2	169.254.169.254	DNS	86	Standard query 0x94d7 PTR

Filter toolbar

Consejo profesional: Wireshark utiliza diferentes colores para representar los protocolos. Puedes personalizar los colores y crear tus propios filtros.

Filtrar por protocolos

El filtrado de protocolos es una de las formas más simples de utilizar los filtros de visualización. Basta solo con ingresar el nombre del protocolo para filtrar. Por ejemplo, para filtrar paquetes DNS, escribe **dns** en la barra de herramientas de filtrado. A continuación, podrás ver una lista de algunos protocolos que puedes filtrar:

- dns
- http
- ftp
- ssh
- arp
- telnet
- icmp

Filtrar una dirección IP

Puedes utilizar filtros de visualización para localizar paquetes con una dirección IP específica.

Por ejemplo, si deseas filtrar paquetes que contienen una dirección IP específica, utiliza `ip.addr`, seguido de un espacio, el operador de comparación `== igual` y la dirección IP. A continuación se muestra un ejemplo de un filtro de visualización que filtra la dirección IP 172.21.224.2:

```
ip.addr == 172.21.224.2
```

Para filtrar paquetes que se originan desde una dirección IP de origen específica, puedes usar el filtro `ip.src`. Aquí, puedes ver un ejemplo que busca la dirección IP de origen 10.10.10.10:

```
ip.src == 10.10.10.10
```

Para filtrar los paquetes entregados a una dirección IP de destino específica, puedes utilizar el filtro `ip.dst`. Aquí, puedes ver un ejemplo que busca la dirección IP de destino 4.4.4.4:

```
ip.dst == 4.4.4.4
```

Filtrar una dirección MAC

También puedes filtrar paquetes según la **dirección de control de acceso al medio (MAC)**. Como actualización, una dirección MAC es un identificador alfanumérico único que se asigna a cada dispositivo físico en una red.

A continuación, se muestra un ejemplo:

```
eth.addr == 00:70:f4:23:18:c4
```

Filtrar por puertos

El filtrado de puertos se utiliza para filtrar paquetes en función de los números de puerto. Esto es útil cuando quieras aislar tipos específicos de tráfico. El tráfico DNS utiliza el puerto TCP o UDP 53, por lo que esto enumerará el tráfico relacionado con las consultas y respuestas de DNS únicamente.

Por ejemplo, si quieras filtrar un puerto UDP:

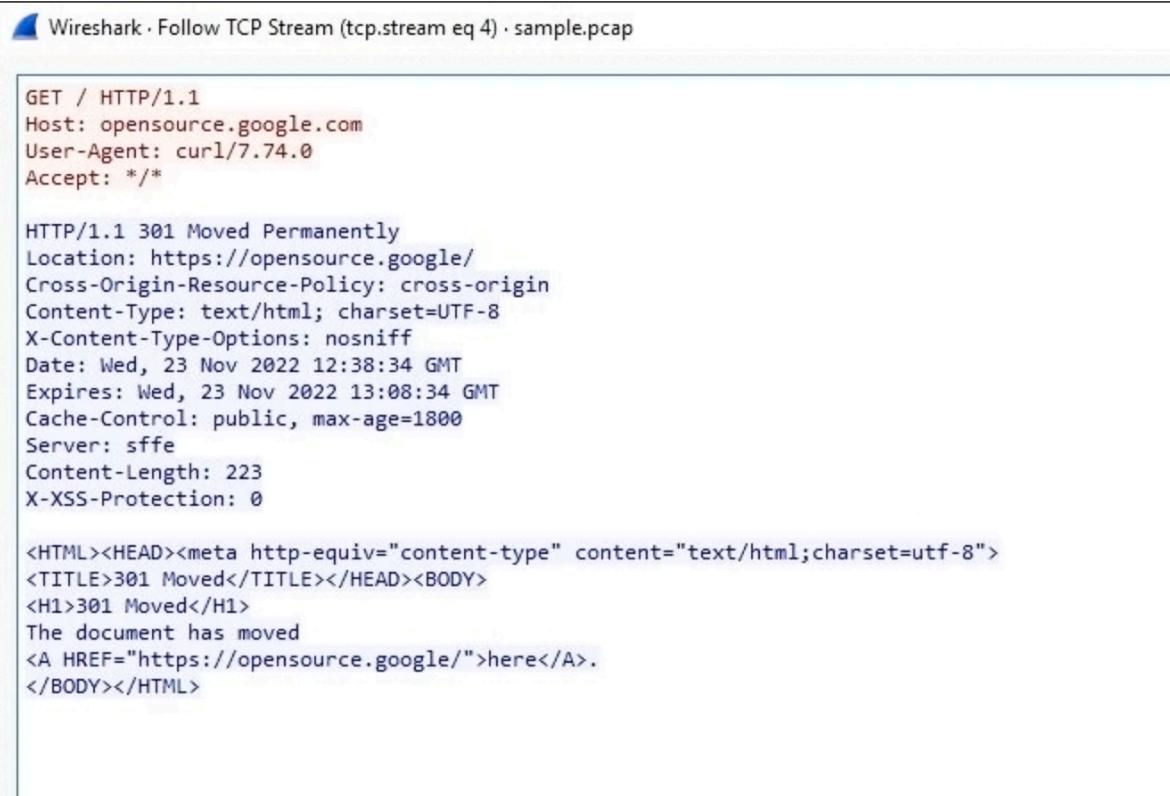
```
udp.port == 53
```

Del mismo modo, también puedes filtrar puertos TCP:

```
tcp.port == 25
```

Seguir flujos

Wireshark ofrece una función que permite filtrar paquetes específicos para un protocolo y ver flujos. Un flujo o conversación es el intercambio de datos entre dispositivos que utilizan un protocolo. Wireshark vuelve a ensamblar los datos que se transfirieron en el flujo en un formato legible.



```
Wireshark - Follow TCP Stream (tcp.stream eq 4) · sample.pcap

GET / HTTP/1.1
Host: opensource.google.com
User-Agent: curl/7.74.0
Accept: */*

HTTP/1.1 301 Moved Permanently
Location: https://opensource.google/
Cross-Origin-Resource-Policy: cross-origin
Content-Type: text/html; charset=UTF-8
X-Content-Type-Options: nosniff
Date: Wed, 23 Nov 2022 12:38:34 GMT
Expires: Wed, 23 Nov 2022 13:08:34 GMT
Cache-Control: public, max-age=1800
Server: sffe
Content-Length: 223
X-XSS-Protection: 0

<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="https://opensource.google/">here</A>.
</BODY></HTML>
```

Seguir un flujo de protocolo es útil cuando se trata de comprender los detalles de una conversación. Por ejemplo, puedes examinar los detalles de una conversación HTTP para ver el contenido de los mensajes intercambiados de solicitud y respuesta.

Conclusiones clave

En esta lectura, exploraste los filtros de visualización básicos con Wireshark. El análisis de paquetes es una habilidad fundamental que seguirás desarrollando con el tiempo en tu recorrido por el mundo de la ciberseguridad. Pon en práctica tus habilidades en la próxima actividad y explora los detalles de un archivo de captura de paquetes utilizando Wireshark.

Detección de paquetes maliciosos y Suplantación de direcciones IP

Ataque de rastreo pasivo

Los paquetes de datos se leen cuando están en tránsito, como todo el tráfico de una red es visible para cualquier host en el hub, los atacantes pueden ver los datos entrantes y salientes del dispositivo víctima

Ataque de rastreo activo

los paquetes de datos se manipulan cuando están en tránsito. Esto puede consistir en inyectar protocolos de Internet para redirigir los paquetes a otro puerto o cambiar la información que el paquete contiene.

Como protegernos?

- Usar una VPN que cifra y protege los datos al viajar por la red
- Ingresar a sitios con HTTPS como dominio usa SSL/TLS
- Evitar usar wifi públicos

los paquetes de datos se manipulan cuando están en tránsito.

Esto puede consistir en inyectar protocolos de Internet

para redirigir los paquetes a otro puerto

o cambiar la información que el paquete contiene.

Suplantación de direcciones IP

Este ataque se hace cuando un atacante cambia de IP de origen de un paquete para suplantar un sistema autorizado y acceder a una red, en este ataque el hacker finge ser otra persona para comunicarse por la red con la computadora víctima saltando reglas de firewall que evitan el tráfico exterior

un ataque en ruta

el atacante se pone en medio de una conexión autorizada e intercepta o altera los datos en tránsito.

Los atacantes en ruta acceden a la red y se ponen entre dos dispositivos, como un navegador web y un servidor web.

Luego, rastrean los datos del paquete para ver las direcciones IP y MAC de los dos dispositivos que se están comunicando. Tras tener esta información, fingen ser uno de estos dispositivos.

Ataque de repetición

Este se lleva a cabo cuando un agente de amenaza intercepta un paquete en tránsito y lo retrasa o lo repite en otro momento, esto causa problemas de conexión entre computadoras víctimas.

Ataque pitufo

Este combina un ataque DDoS con uno de suplantación de IP, el atacante detecta una dirección IP autorizada y la inunda con paquetes, esto sobrecarga la computadora y puede derribar un servidor.

Determinar el tipo de ataque

Ataque de contraseña

Tiene el propósito de acceder a dispositivos y sistemas, redes o datos protegidos por contraseña.

Algunos de los ejemplos son

- Fuerza Bruta
- Tabla arcoíris o Rainbow

Ataque de ingeniería social

Es una técnica de manipulación que aprovecha los errores humanos para obtener información probada , acceso a sistemas o bienes de valor.

Ejemplo:

- Phising suplantacion de identidad
- Smishin por mensaje SMS
- Vishing que es por llamada
- Phishing localizado (Spear phishing)
- Ataque de caza de ballena (Whaling)
- Ataque en redes sociales (Phishing en redes sociales)
- Compromiso del correo electrónico empresarial (BEC)
- Ataque de "agujero de agua"
- Cebo USB (Baiting)
- Ingeniería social física

Ataque físico

Un **ataque físico** es un incidente de seguridad que afecta no solo a los entornos digitales, sino también a los físicos en los que se produce el incidente. Algunos tipos de ataques físicos son:

- Cable USB malicioso
- Unidad flash maliciosa
- Clonación y skimming de tarjetas

Ataque a la cadena de suministro

Un **ataque a la cadena de suministro** se dirige a los sistemas, las aplicaciones, el hardware y el software con el fin de identificar una vulnerabilidad en la que instalar software malicioso. Como cada artículo que se vende pasa por un proceso que involucra a terceros, esto significa que la vulneración de seguridad puede producirse en cualquier punto de la cadena de suministro. Estos ataques resultan costosos porque pueden afectar a varias organizaciones y a las personas que trabajan para ellas. Los ataques a la cadena de suministro pertenecen a los dominios de seguridad y gestión de riesgos, arquitectura e ingeniería de seguridad y operaciones de seguridad.

En resumen, los ataques a la cadena de suministro representan una seria amenaza para las organizaciones y las personas involucradas en ellas. La seguridad y la gestión de riesgos deben ser prioridades para evitar los costosos efectos de estos ataques. La arquitectura, la ingeniería y las operaciones de seguridad juegan un papel crucial en la protección contra estos riesgos.

Ataque criptográfico

Un **ataque criptográfico** afecta a las formas seguras de comunicación protegidas por un sistema criptográfico. Algunos tipos de ataques criptográficos son:

- Cumpleaños
- Colisión
- Degradación

Los ataques criptográficos pertenecen al dominio de seguridad de las comunicaciones y las redes.

Documentación , cadena de custodia y manuales de estrategia

Beneficios de la documentación

- Transparencia
- Estandarización
- Claridad en los procesos

Cadena de custodia

Es el proceso de documentar evidencia , posesión y control durante el ciclo de vida de un incidente, Ni bien se recompila la evidencia, se produce los formularios de cadena de custodia

Cadena de custodia rota:a cual ocurre cuando hay inconsistencias en la recolección y registro de evidencia en la cadena de custodia. En los tribunales, los documentos de cadena de custodia ayudan a establecer pruebas de la integridad, confiabilidad y exactitud de la evidencia

Existen 3 tipos de manuales de estrategia

- No automatizado : que requiere acciones paso a paso realizadas por un analista.
- automatizados automatizan las tareas en procesos de respuesta a incidentes. Por ejemplo, tareas como categorizar la severidad del incidente o reunir evidencia pueden llevarse a cabo usando un manual automatizado.
- Los semiautomáticos combinan acciones humanas con automatización. Tareas tediosas, lentas o propensas al error se pueden automatizar, y así los analistas pueden dedicar más tiempo a otras tareas.Los manuales semiautomatizados pueden ayudar a aumentar la productividad y agilizar la resolución. Al responder a incidentes, se puede descubrir que un manual necesita actualizaciones o cambios.

Dominios de seguridad

Seguridad y Gestión de riesgos

Capacidad para gestionar la defensa de sus activos y datos críticos así como para reaccionar frente a los cambios. Ejemplo:

- Metas y objetivos de seguridad
- Procesos de mitigación de riesgos
- Cumplimiento normativo (compliance)
- Planes para la continuidad del negocio
- Normativa
- Ética profesional y organizacional

La seguridad de la información o InfoSec se refiere al conjunto de los procesos establecidos para proteger la información (se pueden usar guías o manuales de estrategias o procedimientos) algunos de los procesos de la InfoSec como:

- Respuesta a incidentes
- Gestión de las vulnerabilidades
- Seguridad en la aplicación
- Seguridad en la nube
- Seguridad en la infraestructura

Un ejemplo un equipo de seguridad puede tener que modificar el tratamiento de la información de identificación personal PII para cumplir el Reglamento general de Protección de Datos RGPD de la unión europea,

Seguridad en los activos:

Gestión de procesos de ciberseguridad de los activos organizacionales, lo cual incluye almacenamiento, mantenimiento, conservación y destrucción de los datos físicos y virtuales.

Dado que la perdida de activos puede ser muy grave.

Se realiza un análisis del impacto en la seguridad, establece un plan de recuperación y gestionarla exposición de los datos dependerá del nivel de riesgo asociado a cada activo.

Se pueden almacenar, mantener y conservar datos mediante la creación de copias de seguridad, para asegurarse de poder restaurar el entorno en caso de que ocurra un incidente.

Arquitectura y diseño de seguridad

Se enfoca en la gestión de la seguridad de los datos. Garantiza la existencia de herramientas , sistemas y procesos eficaces ayuda a proteger los activos y datos de una organización.

Un aspecto importante en la responsabilidad compartida , que implica que todas las personas involucradas asuman un papel activo en la reducción del riesgo durante el diseño de un sistema de seguridad. Los principios de diseño adicionales relacionados con este dominio que se tratan más adelante en el programa son:

- Simulación de amenazas
- Principio de privilegio mínimo
- Defensa en profundidad
- Fallar de forma segura
- Separación de funciones
- Simplicidad
- Confianza cero
- Confianza tras verificación
- SIEM herramienta de gestión de eventos e información de seguridad.

Seguridad de las comunicaciones y redes

Este dominio se centra en la gestión y la seguridad de las redes físicas y las comunicaciones inalámbricas , incluidas las que son en el mismo lugar remotas y en la nube.

Las organizaciones que cuentan con entornos de trabajo remotos o híbridos y presenciales deben asegurarse de que los datos permanezcan seguros y a la vez gestionar las conexiones externas y garantizar que la red de la empresa permanezca segura.

Gestión de identidades y accesos

Este dominio de gestión de identidades de accesos IAM se centra en mantener la seguridad de los datos asegurándose de que las identidades de los usuarios sean confiables y estén autenticadas y que el acceso a los activos físicos y lógicos estén autorizados realicen sus tareas.

Básicamente el IAM utiliza lo que se conoce como el principio de privilegio mínimo que es el concepto de otorgar solo el acceso y la autorización mínimos necesarios para completar una tarea.

Evaluación y pruebas de seguridad

Se enfoca en identificar y mitigar riesgos amenazas y vulnerabilidades. Las evaluaciones de seguridad se enfoca en identificar y mitigar riesgos , amenazas y vulnerabilidades. Las evaluaciones de seguridad ayudan a las empresas a determinar si sus sistemas internos son seguros o están en riesgo. Las organizaciones pueden emplear pruebas de penetración, un proceso conocido como pentesting para encontrar las vulnerabilidades que podrán aprovechar un agente de amenaza.

Operaciones de Seguridad

Se centra en la investigación de una posible filtración de datos y la implementación de medidas preventivas después de que se haya producido un incidente esto incluye el uso de estrategias

- Entrenamiento y concientización
- Informes y documentación
- Detección y prevención de intrusos
- Herramienta SIEM
- Gestión de riesgo
- Gestión de incidentes
- Manuales de estrategias
- Análisis forense posterior a una filtración
- Reflexión sobre las lecciones aprendidas

Seguridad en el desarrollo de software

El dominio de la seguridad en el desarrollo de software se enfoca en el uso de prácticas y políticas de programación para crear aplicaciones seguras . Contar con ellas ayuda a ofrecer servicios seguros y fiables y a proteger las organizaciones y sus usuarios.

Dominios de seguridad del CISSP (videos)

Seguridad y gestión de riesgo

Áreas de enfoque en definición de metas y objetivos de seguridad, mitigación de riesgos, cumplimiento normativo, continuidad al negocio y regulaciones legales.

- Pueden reducir los riesgos para activos críticos y datos

- Además de cumplir con los requisitos normativos y estándares independientes de una organización
- Continuidad de negocio : la habilidad de mantener la productividad todos los días mediante el establecimiento de planes de recuperación de desastres
-

Seguridad en los activos

Se centra en asegurar los activos físicos y digitales además de la creación modificación y eliminación de los SPII y SPI sean manejados adecuadamente.

Saber que datos tienen y quien accede a ellos

Arquitectura y diseño de seguridad

Se centra en optimizar la seguridad de los datos que haya herramientas sistemas y procesos efectivos para proteger los activos y datos de una organización.

Seguridad de las telecomunicaciones y de las redes

Se centra en proteger las redes y comunicaciones inalámbricas.

Gestión de identidades y accesos

Se centra en el acceso y autorización para proteger los datos asegurando a que los usuarios sigan las políticas de acceso y manejo de activos. limitando el acceso a los usuarios que lo necesitan y quien accesa a los datos.

Componentes de IAM

1. Identificación: es cuando alguien verifica quien brinda un nombre de usuario, una tarjeta de acceso o datos biométricos como una huella dactilar.
2. La autenticación es el proceso para verificar la identidad de alguien mediante una contraseña o pin
3. La responsabilidad : se refiere al monitoreo y registro de las acciones de los usuarios y su nivel de acceso que depende del puesto en la organización.
4. La autorización: Se da tras confirmar la identidad del usuario y su nivel de acceso que depende del puesto.

Evaluación y pruebas

Pruebas de control de seguridad, recopilar y analizar datos y realizar auditorias de seguridad para monitorear riesgos , amenazas y vulnerabilidades, con estas pruebas se busca identificar nuevas formas y mejores de mitigar amenazas, riesgos y vulnerabilidades. Esto implica examinar metas y objetivos organizacionales y evaluar si realmente se usan dichos controles para lograr esos objetivos.

Operaciones de seguridad

Se centra en investigar e implementar medidas preventivas para minimizar los riesgos de una organización.

Se realiza una investigación forense para ver cuando , donde y como ocurrió el ataque
desarrollo de software Seguro

Se centra en las prácticas de codificación segura para crear servicios o aplicaciones seguras.

en cada una de las fases de desarrollo del software.

Ejemplo: realizar la revisión de diseño seguro en la fase de diseño, revisiones del código seguro durante el desarrollo y pruebas de penetración durante la fase de implementación y despliegue.

El auge del inicio de sesión único (SSO) y la autenticación de múltiples factores (MFA)

Autenticación: El Primer Paso

- Los sistemas de autenticación verifican la identidad de cualquier persona o sistema que intente acceder a la información, esencialmente preguntando: "¿Quién eres?".
- Esta verificación puede basarse en tres factores: algo que el usuario *sabe* (como una contraseña), algo que el usuario *tiene* (como una contraseña de un solo uso), o algo que el usuario *es* (como una huella dactilar).

Mejorando la Seguridad y la Comodidad

- El inicio de sesión único (SSO) simplifica el acceso al combinar múltiples inicios de sesión en uno, lo que permite a los usuarios acceder a los recursos de la empresa más rápidamente después de una sola autenticación.

- La autenticación multifactor (MFA) mejora la seguridad al requerir múltiples factores de autenticación, como una contraseña y un código enviado a un dispositivo móvil, lo que hace que sea mucho más difícil para los actores maliciosos obtener acceso no autorizado.

Una mejor aproximación a la autenticación

El **inicio de sesión único** (SSO) es una tecnología que combina varios inicios de sesión diferentes en uno solo. Cada vez más empresas recurren al SSO como solución para sus necesidades de autenticación debido a tres razones fundamentales:

1. **Mejora la experiencia de usuario** al eliminar la necesidad de recordar múltiples nombres de usuario y contraseñas.
2. **Permite a las empresas reducir costos** al simplificar la gestión de servicios conectados.
3. **Mejora la seguridad general** al reducir la cantidad de puntos de acceso que los atacantes podrían utilizar para infiltrarse en el sistema.

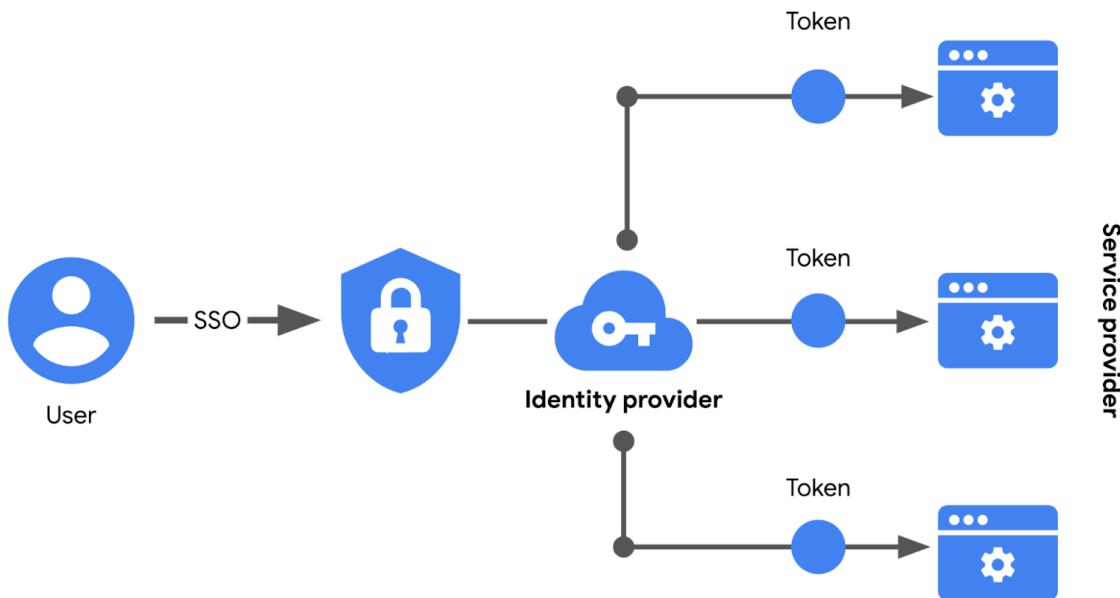
Cómo funciona el inicio de sesión único (SSO)

El inicio de sesión único (SSO) funciona automatizando el establecimiento de confianza entre un usuario y una empresa proveedora de servicios. En lugar de requerir que el empleado o cliente se encargue de la autenticación, las soluciones de SSO utilizan terceros de confianza para demostrar la identidad del usuario. Esto se logra mediante el intercambio de tokens de acceso cifrados entre el proveedor de identidad y el proveedor de servicios.

Estos tokens de acceso se intercambian utilizando protocolos específicos, al igual que ocurre con otros tipos de información digital. Las implementaciones de SSO suelen basarse en dos protocolos de autenticación diferentes: el Protocolo ligero de acceso a directorios (LDAP) y el Lenguaje de marcado para confirmaciones de seguridad (SAML). El LDAP se utiliza principalmente para transmitir información dentro de las instalaciones, mientras que el SAML se emplea sobre todo para transmitir información fuera del entorno local, como en servicios en la nube.

Nota: Los protocolos LDAP y SAML suelen utilizarse juntos.

Este es un ejemplo de cómo el SSO puede conectar a un usuario a múltiples aplicaciones con un token de acceso:



Limitaciones del inicio de sesión único (SSO)

La autenticación mediante nombres de usuario y contraseñas por sí sola no siempre es la forma más segura de proteger la información confidencial. Si bien el inicio de sesión único (SSO) ofrece ventajas útiles, aún existen riesgos asociados con el uso de una única forma de autenticación. Por ejemplo, si se pierde o roba una contraseña, podría exponerse información en múltiples servicios. Afortunadamente, existe una solución a este problema.

La autenticación de múltiples factores (MFA) al rescate

La autenticación de múltiples factores, o multifactor, (MFA) requiere que un usuario verifique su identidad de dos o más formas para acceder a un sistema o red. En cierto sentido, la MFA es similar al uso de un cajero automático para retirar dinero de la cuenta bancaria. Primero, insertas una tarjeta de débito en la máquina como forma de identificación. Luego, ingresas tu número PIN como segunda forma de identificación. Ambos pasos o factores se combinan para verificar tu identidad antes de obtener la autorización para acceder a la cuenta.



Refuerzo de la autenticación

La autenticación de múltiples factores (MFA) se basa en los beneficios del inicio de sesión único (SSO) y funciona al requerir que los usuarios demuestren que son quienes dicen ser.

Para autenticar su identidad, el usuario debe proporcionar dos factores (2FA) o tres factores (3FA). El proceso de MFA solicita que se brinden las siguientes pruebas:

- **Algo que el usuario conoce:** un nombre de usuario y contraseña, generalmente.
- **Algo que el usuario tiene:** típicamente proporcionado por una empresa proveedora de servicios, como un código de acceso de un solo uso (OTP) enviado a través de SMS.
- **Algo que el usuario es:** se refiere a las características físicas de una persona, como sus huellas dactilares o escaneos faciales.

El futuro de las herramientas SIEM

Soluciones SIEM actuales :

Una herramienta SIEM es una aplicación que recopila y analiza datos de registro para monitorear actividades críticas de una organización. Mediante el monitoreo y seguimiento en tiempo real de los riesgos de eventos de seguridad, se obtienen datos que se utilizan para realizar un análisis exhaustivo de cualquier amenaza, riesgo o vulnerabilidad de seguridad potencial identificada.

El futuro

Las herramientas funcionan y operan cada vez más en la nube, para funcionar en entornos alejados y nativos en la nube por proveedores que se encargan de mantener y administrar la infraestructura requerida.

Por otra parte, a medida que la tecnología de inteligencia artificial (IA) y aprendizaje automático (ML) progresen, las capacidades SIEM mejorarán, y podrán identificar mejor la terminología relacionada con la amenaza, así como la visualización del panel y la funcionalidad de almacenamiento de datos.

Además, la implementación de la automatización ayudará a incrementar la velocidad de respuesta de los equipos de seguridad frente a posibles incidentes, porque permite realizar numerosas acciones sin esperar una respuesta humana. Por ejemplo,

Orquestación, Automatización y Respuesta de Seguridad (SOAR) es un conjunto de aplicaciones, herramientas y flujos de trabajo que utilizan la automatización para responder a incidentes de seguridad. Al utilizarlo, el manejo de incidentes comunes relacionados con la seguridad mediante el uso de herramientas SIEM se convierte en un proceso más simplificado y con menos intervención manual. Esto es importante ya que permite que las/los analistas de seguridad puedan abocarse a incidentes más complejos y poco comunes, que no se pueden automatizar con un SOAR.

Por otra parte, se espera que las plataformas referidas a la ciberseguridad se comuniquen e interactúen entre sí, aunque si bien ya existe la tecnología que permite la comunicación entre sistemas y dispositivos interconectados, aún está en fase de desarrollo.

Splunk Enterprise, Splunk Cloud, y Chronicle

son herramientas SIEM comunes que utilizan muchas organizaciones para ayudar a proteger sus datos y sistemas.

Splunk Enterprise es una herramienta autoalojada que se utiliza para retener, analizar y buscar los datos de registro de una organización para brindar información de seguridad y alertas en tiempo real.

Splunk Cloud es una herramienta autoalojada en la nube que se utiliza para recopilar, buscar y monitorear datos de registro es útil para entornos híbridos o en la nube

Chronicle Google: es una herramienta nativa en la nube diseñada para retener, analizar y buscar datos. Ofrece un monitoreo de registros, análisis y recolección de datos.

El proceso de triaje

El proceso de triaje

Los incidentes pueden tener el potencial de causar un daño significativo a una organización. Los equipos de seguridad deben responder de manera rápida y eficiente para prevenir o limitar el impacto de un incidente antes de que sea demasiado tarde. **El triaje** es la priorización de incidentes en función de su nivel de importancia o urgencia. El proceso de triaje ayuda a los equipos de seguridad a evaluar y priorizar las alertas y asignar recursos de manera efectiva para que los problemas más críticos se atiendan primero.

El proceso de triaje consta de tres pasos:

1. Recibir y evaluar
2. Asignar prioridad
3. Recopilar y analizar

Recibir y evaluar

Durante esta primera etapa del proceso de triaje, un analista de seguridad recibe una alerta de, por ejemplo, un **sistema de detección de intrusiones** (IDS). Es posible que recuerdes que un IDS es una aplicación que monitorea la actividad del sistema y alerta sobre posibles intrusiones. Luego, el analista revisa la alerta para verificar su validez y asegurarse de que la entiende en su totalidad.

Esto implica recopilar la mayor cantidad de información posible sobre la alerta, incluidos, entre otros, los detalles sobre la actividad que desencadenó la alerta y los sistemas y activos involucrados. Aquí te presentamos algunas preguntas para tener en cuenta al verificar la validez de una alerta:

- **¿Es la alerta un falso positivo?** Los analistas de seguridad deben determinar si la alerta es un problema de seguridad genuino o un **falso positivo**, o sea, una alerta que detecta incorrectamente la presencia de una amenaza.

- **¿Se activó esta alerta en el pasado?** En caso afirmativo, ¿cómo se resolvió? El historial de una alerta puede ayudar a determinar si es un problema nuevo o recurrente.
- **¿La alerta se desencadena por una vulnerabilidad conocida?** Si una alerta es activada por una vulnerabilidad conocida, los analistas de seguridad pueden aprovechar los conocimientos existentes para determinar una respuesta adecuada y minimizar el impacto de la vulnerabilidad.
- **¿Cuál es la gravedad de la alerta?** La gravedad de una alerta puede ayudar a determinar la prioridad de la respuesta para que los problemas críticos se eleven rápidamente.

Asignar prioridad

Una vez que la alerta se ha evaluado y verificado adecuadamente como un problema de seguridad genuino, debe priorizarse en consecuencia. Los incidentes difieren en su impacto, tamaño y alcance, lo que afecta los intentos de respuesta. Para administrar el tiempo y los recursos, los equipos de seguridad deben priorizar la forma en que responden a varios incidentes, ya que no todos son iguales. A continuación, se detallan algunos factores a considerar al determinar la prioridad de un incidente:

- **Impacto funcional:** Los incidentes de seguridad que tienen como objetivo sistemas de tecnología de la información impactan el servicio que estos sistemas brindan a sus usuarios. Por ejemplo, un incidente de ransomware puede afectar gravemente la confidencialidad, disponibilidad e integridad de los sistemas. Los datos pueden ser encriptados o eliminados, haciendolos completamente inaccesibles para los usuarios. Considera cómo un incidente impacta en la funcionalidad existente para el negocio del sistema afectado.
- **Impacto de la información:** Los incidentes pueden afectar la confidencialidad, integridad y disponibilidad de los datos y la información de una organización. En un ataque de exfiltración de datos, los agentes de amenaza pueden robar datos confidenciales, que pueden pertenecer a organizaciones o usuarios externos. Considera los efectos que el compromiso de la información puede causar más allá de la organización.
- **Recuperabilidad:** La forma en que una organización se recupera de un incidente depende del tamaño y el alcance del incidente y de la cantidad de recursos disponibles. En algunos casos, la recuperación podría no ser posible, como cuando un agente de amenaza roba con éxito datos privados y los comparte públicamente. Dedicar tiempo, esfuerzo y recursos en un incidente sin recuperabilidad puede ser un desperdicio. Es importante considerar si la recuperación es posible y si merece el tiempo y el costo.

Nota: Las alertas de seguridad suelen llegar con un nivel de prioridad o gravedad asignado que clasifica la urgencia de la alerta en función de un nivel de priorización.

Recopilar y analizar

El paso final del proceso de triaje implica que el analista de seguridad realice un análisis exhaustivo del incidente. El análisis implica la recopilación de pruebas de diferentes fuentes, la realización de investigaciones externas y la documentación del proceso de investigación. El objetivo de este paso es recopilar suficiente información para tomar una decisión informada, a la hora de atender el incidente. Dependiendo de su gravedad, puede ser necesario elevarlo a un analista de nivel 2 o a un gerente. Los analistas y gerentes de nivel 2 podrían tener más conocimiento sobre el uso de técnicas avanzadas para atender el incidente.

Beneficios del triaje

Al priorizar los incidentes en función de su impacto potencial, puede reducirse el alcance del impacto en la organización, ya que garantiza una respuesta oportuna. Algunos de los beneficios que el triaje tiene para los equipos de seguridad son:

- **Gestión de recursos:** El triaje de las alertas permite a los equipos de seguridad enfocar sus recursos en las amenazas que requieren atención urgente. Esto ayuda a los miembros del equipo a evitar dedicar tiempo y recursos a tareas de menor prioridad y también podría reducir el tiempo de respuesta.
- **Enfoque estandarizado:** El triaje proporciona un enfoque estandarizado para el manejo de incidentes. La documentación del proceso, como los manuales de estrategias, ayuda a que las alertas pasen por un proceso iterativo, lo cual garantiza que se evalúen y validen correctamente. Esto hace que sean solo las alertas válidas las que pasen al siguiente nivel y sean investigadas.

El Top 10 de OWASP

A fin de prepararse para futuros riesgos, los profesionales de seguridad deben mantenerse informados. Ya aprendiste sobre la **lista CVE®**, un diccionario de acceso abierto de vulnerabilidades y exposiciones conocidas. La lista CVE® es una fuente importante de información que la comunidad de seguridad global utiliza para compartir información entre sí.

En esta lectura, aprenderás sobre otro recurso importante que los profesionales de seguridad utilizan como referencia, el Open Web Application Security Project® (Proyecto Abierto de Seguridad de Aplicaciones Web, u OWASP). Aprenderás sobre el papel de OWASP en la comunidad de seguridad global y cómo las empresas utilizan este recurso para centrar sus esfuerzos.

¿Qué es OWASP?

El Open Web Application Security Project® es una fundación sin fines de lucro que trabaja para mejorar la seguridad del software. OWASP es una plataforma abierta que los profesionales de seguridad de todo el mundo utilizan para compartir información, herramientas y eventos que se centran en proteger la web.

El Top 10 de OWASP

Uno de los recursos más valiosos de OWASP es su Top 10. Desde 2003, la organización publica esta lista como una manera de difundir el conocimiento de las vulnerabilidades más específicas de la web. El Top 10 refiere principalmente a software nuevo o por encargo. Muchas de las organizaciones más grandes del mundo consultan el Top 10 de OWASP para ayudar a garantizar que sus programas se desarrolle teniendo en cuenta los errores de seguridad más comunes.

Consejo profesional: El Top 10 de OWASP se actualiza cada algunos años, a medida que evolucionan las tecnologías. El orden se basa en la frecuencia con la que se descubren las vulnerabilidades y el nivel de riesgo que estas presentan.

Nota: Los auditores también utilizan el Top 10 de OWASP como un punto de referencia para verificar el cumplimiento normativo (compliance).

Vulnerabilidades comunes

A menudo, las empresas toman decisiones de seguridad críticas con base en las vulnerabilidades enumeradas en el Top 10 de OWASP. Este recurso influye en la forma en que las empresas diseñan el nuevo software que estará en su red, a diferencia de la lista CVE®, que las ayuda a identificar mejoras en programas ya existentes. Las vulnerabilidades que aparecen con mayor frecuencia en el ranking son:

Pérdida de control de acceso

Los controles de acceso limitan lo que los usuarios pueden hacer en una aplicación web. Por ejemplo, un blog puede permitir a sus visitantes publicar comentarios sobre un artículo reciente, pero les impide eliminar el artículo por completo. Las fallas en estos mecanismos pueden conducir a la divulgación, modificación o destrucción de información no autorizada. También pueden dar a alguien acceso no autorizado a otras aplicaciones de la empresa.

Fallas criptográficas

La información es uno de los activos más importantes que las empresas deben proteger. Las leyes de privacidad, como el Reglamento General de Protección de Datos (RGPD), requieren que los datos confidenciales estén protegidos por métodos de cifrado efectivos. Por ejemplo, pueden ocurrir vulnerabilidades cuando las empresas no cifran la información personal identifiable (PII). También, si una aplicación web utiliza un algoritmo de hashing débil, como el MD5, está más expuesta a sufrir una violación de datos.

Inyección

Un ataque de inyección se produce cuando se inserta un código malicioso en una aplicación vulnerable. Si bien la aplicación pareciera funcionar con normalidad, se

comporta de una manera diferente a la que debería. Este tipo de ataque puede dar a los agentes de amenaza una puerta trasera al sistema de información de una organización. Un objetivo habitual es el formulario de inicio de sesión de un sitio web. Si estos formularios son vulnerables a la inyección, los atacantes podrían insertar código malicioso que les permita acceder y modificar o robar credenciales de usuario.

Diseño inseguro

Las aplicaciones deben diseñarse de tal manera que sean resistentes a ataques. Cuando esto no sucede, se vuelven mucho más vulnerables a amenazas, como ataques de inyección o infecciones de malware. El diseño inseguro refiere a la carencia o deficiente implementación de una variedad de controles de seguridad, que deberían haberse programado en una aplicación durante su desarrollo.

Configuración de seguridad incorrecta

Esta vulnerabilidad se produce cuando la configuración de seguridad y su mantenimiento no se realizan correctamente. Las empresas utilizan una variedad de sistemas interconectados y los errores suelen ocurrir cuando estos no están correctamente configurados o auditados. Un ejemplo común es cuando las empresas implementan equipos, como un servidor de red, utilizando los ajustes de fábrica. Esto puede llevarlas a utilizar configuraciones que no cumplen con los objetivos de seguridad de la organización.

Componentes vulnerables y desactualizados

Se trata de una categoría que se relaciona principalmente con el desarrollo de aplicaciones. En lugar de codificar todo desde cero, la mayoría de los desarrolladores utilizan bibliotecas de código abierto para completar sus proyectos de una forma más rápida y fácil. Este software disponible públicamente lo mantienen comunidades de programadores, de forma voluntaria. Las aplicaciones que utilizan componentes vulnerables a los que no se les realizaron tareas de mantenimiento corren un mayor riesgo de ser explotadas por agentes de amenaza.

Fallas de identificación y autenticación

La identificación es la palabra clave de esta categoría de vulnerabilidad. Cuando las aplicaciones no reconocen quiénes deben tener acceso a ellas y lo que están autorizados a hacer, pueden generarse problemas graves. Por ejemplo, un router Wi-Fi doméstico suele contar únicamente con un formulario de inicio de sesión sencillo para mantener a los huéspedes no deseados fuera de la red. Si esta defensa falla, un atacante puede invadir la privacidad de un propietario.

Fallas en el software y la integridad de los datos

Se trata de instancias en que las actualizaciones o parches no se revisan adecuadamente antes de su implementación, por lo cual, los atacantes podrían explotar estas debilidades para distribuir software malicioso. Cuando eso ocurre, pueden producirse efectos graves de flujo descendente. O sea, basta con que un solo sistema se vea comprometido, para que otros sistemas también sean infectados. A este tipo de ataque se lo conoce como ataque a la cadena de suministro.

Un ejemplo famoso es el [ataque cibernético de SolarWinds \(2020\)](#), en el que un grupo de hackers inyectaron código malicioso en las actualizaciones de software que la empresa lanzó, sin saberlo, a sus clientes.

Fallas en el registro y monitoreo

En seguridad, es importante registrar eventos y rastrear su origen. Tener un registro de eventos como los intentos de inicio de sesión de usuarios es fundamental para encontrar y solucionar problemas. El monitoreo efectivo es tan importante como la respuesta a incidentes.

Falsificación de solicitudes del lado del servidor

Las empresas tienen información pública y privada almacenada en servidores web. Cuando utilizas un hipervínculo o haces clic en un botón en un sitio web, se envía una solicitud a un servidor que debe validar quién eres, obtener los datos apropiados y luego devolvértelos.



Las falsificaciones de solicitudes del lado del servidor (SSRF) suceden cuando los atacantes manipulan las operaciones normales de un servidor para leer o actualizar otros recursos de aquél. Esto es posible cuando hay una aplicación vulnerable en el servidor. Esta transporta el código malicioso a un servidor host que obtendrá datos no autorizados.

Conclusiones clave

El uso de la triada CID para proteger las organizaciones

La triada del CID es una guía que ayuda a las organizaciones a evaluar los riesgos y establecer sistemas y políticas de seguridad

Al tener esto en la empresa se establece una postura de seguridad exitosa.

Esto se refiere a la capacidad de la organización para gestionar la defensa de sus activos y datos críticos, así como reaccionar ante los cambios de manera efectiva.

Confidencialidad: se refiere a que solo los usuarios autorizados pueden acceder a los activos o datos específicos. Se puede mejorar la confidencialidad mediante la implementación de principio de diseño, como el principio de mínimo privilegio que limita el acceso de las personas solo a la información que necesitan para llevar a cabo sus tareas laborales

Integridad: Implica que los datos son verificados, autenticados y confiables. Es esencial contar con los protocolos para verificar la autenticidad de los datos y la manera de hacerlo es mediante la criptografía, que se utiliza para transformar los datos, para que las partes no autorizadas no puedan leerlos ni manipularlos. Otro ejemplo de cómo la organización podría implementar la integridad es mediante la activación de cifrado, que es un proceso de convertir los datos en un formato.

Disponibilidad: Refiera a que los datos son accesibles para aquellas personas autorizadas a usarlos , cuando el sistema cumple tanto los principios de disponibilidad como los de confidencialidad, los datos pueden utilizar cuando sean necesarios. En el entorno laboral, esto puede significar que la organización permite al personal que trabaja de forma remota acceder a su red interna para desempeñar sus tareas laborales.

El valor de la documentación y Detección de intrusos

Documentar es toda forma de contenido registrado que se utiliza con un propósito específico.

-

Tipos de documentación

- Manual de estrategias
- Diarios de gestión de incidentes
- Políticas
- Planes
- Informes finales

Un sistema de detección de intrusos (IDS)

es una aplicación que monitorear la actividad del sistema y la red genera alertas sobre posibles intrusiones.

Sistema de prevención de intrusiones (IPS)

Monitorean la actividad del sistema en busca de intrucciones y actuar para detenerlas como por ejemplo:

- Snort
- Zeek
- Kismet
- Sagan
- Suricata

Elementos de un plan de seguridad

Tiene como objetivo prepararse frente a los riesgos.

Algunos elementos del plan de seguridad son los siguientes:

- Políticas: consta de reglas que reducen el riesgo y protegen la información
- Estándares: Son referencias que informan como establecer políticas(crear un punto de referencia).
- Procedimientos: Estos son instrucciones paso a paso para realizar una tarea específica
- Abordan riesgos dividiéndolos por categorías y factores, como por ejemplo
 - Daño
 - Divulgación
 - Perdida de información

El cumplimiento normativo

es seguir los estándares internos y las normas externas. Las empresas pequeñas y grandes priorizan al máximo el cumplimiento. A un nivel alto, mantener la confianza, reputación, seguridad e integridad de los datos es un motivo para preocuparse por el cumplimiento

marco de ciberseguridad (CSF) del NIST

Esta compuesto por 3 componentes principales

- El núcleo : es una versión simple de las funciones u obligaciones del plan de seguridad
 1. Identificar
 2. Proteger
 3. Detectar
 4. Responder

5. Recuperar



- Sus niveles: Con estos, los equipos de seguridad miden el rendimiento de las cinco funciones del núcleo. Los niveles van del 1 al 4.
 - El nivel 1 (pasivo) indica que una función alcanza los estándares mínimos
 - El nivel 4 (adaptativo) indica que una función se realiza en un estándar ejemplar.
- Sus Perfiles

Implementación del CSF

Desde su creación, muchas empresas han utilizado el CSF del NIST. Como recordarás, el marco consta de tres elementos principales:

- Núcleo
- Niveles
- Perfiles

Estos tres componentes fueron diseñados para ayudar a cualquier empresa a mejorar sus operaciones de seguridad. Aunque solo hay tres elementos principales, todo el marco consta de un sistema complejo de subcategorías y procesos.

La implementación del CSF puede ser un desafío debido a su alto nivel de detalle. También puede resultar complicado determinar dónde encaja el marco. Por ejemplo, algunas empresas ya tienen planes de seguridad establecidos, lo que dificulta comprender cómo el

CSF puede beneficiarlas. Por otro lado, algunas empresas pueden estar en las etapas iniciales de elaborar sus planes y necesitar un punto de partida.

En cualquier escenario, la Agencia de Ciberseguridad y Seguridad de las Infraestructuras de los Estados Unidos (CISA) proporciona una guía detallada que cualquier organización puede utilizar para implementar el CSF. A continuación, se presenta una breve descripción y resumen de sus recomendaciones:

- **Crea un perfil actual** de las operaciones de seguridad y describe las necesidades específicas de tu empresa.
- **Realiza una evaluación de riesgos** para identificar cuáles de tus operaciones actuales cumplen con los estándares comerciales y regulatorios.
- **Analiza y prioriza las vulnerabilidades existentes** en las operaciones de seguridad que ponen en riesgo los activos de la empresa.
- **Implementa un plan de acción** para alcanzar las metas y objetivos de tu organización.

Consejo profesional: Ten siempre en cuenta las tendencias actuales en materia de riesgos, amenazas y vulnerabilidades al usar el CSF del NIST.

Industrias que adoptan el CSF

Desde su introducción en 2014, el CSF del NIST ha seguido evolucionando. Su diseño está influenciado por los estándares y las prácticas recomendadas de algunas de las empresas más grandes del mundo.

Una ventaja del marco es que se alinea con las prácticas de seguridad de muchas organizaciones en la economía global. También, facilita el cumplimiento de regulaciones que podrían ser compartidas con socios/as comerciales.

Equipo de respuesta

Equipos de respuesta a incidentes de seguridad o CSIRT

Son un grupo de profesionales capacitados en la gestión y respuesta y para prevenir diferentes ataques.

Roles de un CSIRT

- Analista de seguridad
 - Se encarga de investigar las alertas para determinar su calificación para determinar si ocurrió un incidente o no.
- Lider Tecnico

- Brinda liderazgo técnico orientando los incidentes de seguridad por su ciclo de vida , Durante ese tiempo el coordinador realiza un seguimiento y gestiona las actividades del CSIRT y otros equipos involucrados , su tarea es asegurar que sigan los procesos de respuesta y que se actualizan a los equipos sobre el estado del incidente

Evaluación de vulnerabilidades

1. Identificar: Aquí se usan herramientas de análisis y pruebas para hallar vulnerabilidades.
2. Análisis de vulnerabilidades: Aquí se ponen a prueba las vulnerabilidades identificadas, como hallar el problema.
3. Evaluación de riesgos: En esta etapa se da puntuación que se otorga por 2 factores: el grado de impacto si la vulnerabilidad se explota y la probabilidad de que esto suceda.
4. La remediación: Se abordan las vulnerabilidades que pueden afectar a la organización y la remediación depende de la puntuación de gravedad que se le asignó durante la evaluación de riesgos.

Examen

1. ¿Para qué sirven los controles de seguridad?

1 / 1 punto

- Para cifrar la información y proteger la privacidad
- Para establecer sistemas de respuesta a incidentes
- Para crear políticas y procedimientos
- Para reducir riesgos de seguridad específicos

 Correcto

2. Un suscriptor de pago de un sitio web de noticias tiene acceso a contenido exclusivo. Como propietario de los datos, ¿a qué debería estar autorizado el suscriptor para hacer con su cuenta? Selecciona tres respuestas.

1 / 1 punto

- A revisar su nombre de usuario y contraseña
- A cancelar su suscripción
- A editar artículos en el sitio web
- A actualizar sus datos de pago

 Correcto

3. ¿Qué utilizan los algoritmos de cifrado simétrico para cifrar y descifrar la información?

0 / 1 punto

- Un valor hash
- Un certificado digital
- Una única clave secreta
- Un par de claves pública y privada

 Incorrecto

Revisa [el video sobre cifrado](#).

4. ¿Para qué utilizan las funciones hash los profesionales de la seguridad? Selecciona dos respuestas.

1 / 1 pun

- Para convertir texto cifrado en texto simple
- Para determinar si dos archivos son iguales

 Correcto

- Para hacer copias de seguridad de contraseñas en una tabla Arcoíris
- Para verificar la integridad de un archivo

 Correcto

5. Completa el espacio en blanco: _____ se utiliza para demostrar la identidad de los usuarios, empresas y redes en infraestructuras de clave pública.

0 / 1 pun

- Un token de acceso
- Una firma digital
- Un certificado digital
- Una clave de acceso

 Incorrecto

Revisa [el video sobre infraestructura de clave pública \(PKI\)](#).

6. ¿Cuáles son las dos formas más comunes de identificación utilizadas por los sistemas de autenticación? Selecciona dos respuestas.

1 / 1 pun

- Escaneo facial
 - Nombre de usuario
-  Correcto
- Huella dactilar
 - Contraseña
-  Correcto

7. ¿Cuáles son algunas de las desventajas de usar la tecnología de inicio de sesión único (SSO) para la autenticación de usuarios? Selecciona dos.

0.5 / 1 punto

- Clientes, proveedores y socios comerciales son menos vulnerables a los ataques.
- Las credenciales robadas pueden dar a los atacantes acceso a múltiples recursos.

 Correcto

- La gestión de nombres de usuario y contraseñas es más complicada para los usuarios finales.

 Esto no debería estar seleccionado

Revisa el video sobre inicio de sesión único (SSO) y de múltiples factores (MFA) [\[\]](#).

- El acceso a todos los recursos conectados se detiene cuando el SSO está inactivo.

8. En un negocio una persona recibe el dinero de los clientes en la caja registradora. Al final del día, otra persona cuenta ese dinero con los artículos vendidos y lo deposita. ¿Qué principios de seguridad se están implementando en este escenario? Selecciona dos respuestas.

0.75 / 1 punto

- Autenticación de múltiples factores
- Inicio de sesión único
- segregación de funciones

 Correcto

- Mínimo privilegio

No seleccionaste todas las respuestas correctas

9. ¿Cuáles son las herramientas de autorización más comunes diseñadas teniendo en cuenta el principio de mínimo privilegio y la segregación de funciones? Selecciona tres respuestas.

0.5 / 1 punto

- SHA-256
- OAuth
- Autorización básica
- Tokens API

 Correcto

No seleccionaste todas las respuestas correctas

10. Un cliente de una empresa de venta minorista en línea se queja de que en su cuenta hay una compra no autorizada. Investiga el incidente revisando los registros de acceso. ¿Cuáles son algunos componentes de la sesión del usuario que podrías revisar? Selecciona dos respuestas.

0.5 / 1 punto

- Certificado de sesión

 Esto no debería estar seleccionado

Revisa el video sobre responsabilidad [\[\]](#).

- Algoritmo de sesión
- Cookie de sesión
- ID de sesión

 Correcto

1. ¿Qué funciones se incluirían en la categoría de controles de seguridad operativos? Selecciona dos respuestas.

0 / 1 punto

- Proporcionar entrenamiento de concienciación en materia de seguridad
- Responder a una alerta de incidente
- Generar confianza mediante certificados digitales

 **Esto no debería estar seleccionado**
Revisa [el video sobre controles de seguridad](#).

- Intercambiar información cifrada

 **Esto no debería estar seleccionado**
Revisa [el video sobre controles de seguridad](#).

2. Una gran cadena hotelera está organizando un sorteo nacional. Para participar, las personas deben dar su consentimiento para compartir su dirección de correo electrónico con los socios comerciales de la cadena, con fines de marketing. ¿Cuáles son las responsabilidades de la cadena hotelera como custodio de los datos? Selecciona tres respuestas.

0.5 / 1 punto

- Recopilar el consentimiento y los correos electrónicos de las personas

 **Correcto**

- Otorgar a los socios comerciales el consentimiento para utilizar los datos de las personas

 **Esto no debería estar seleccionado**
Revisa [el video sobre la privacidad de la información](#).

- Hacer copias de seguridad de la información de las personas

 **Correcto**

- Enviar información a los socios comerciales

3. Envías un correo electrónico a una amistad. La empresa proveedora de servicios de tu bandeja de entrada cifra todos los mensajes que envías. ¿Qué ocurre con la información de tu correo electrónico cuando está cifrada?

1 / 1 punto

- Se convierte de valor hash a texto cifrado
- Se convierte de texto cifrado a texto simple
- Se convierte de texto simple, o sin cifrar, a texto cifrado
- Se convierte de cifrado César a texto simple

 Correcto

4. ¿Para qué utilizan las funciones hash los profesionales de la seguridad? Selecciona dos respuestas.

1 / 1 punto

- Para verificar la integridad de un archivo

 Correcto

- Para hacer copias de seguridad de contraseñas en una tabla Arcoíris
- Para convertir texto cifrado en texto simple
- Para determinar si dos archivos son iguales

 Correcto

5. Completa el espacio en blanco: _____ se utiliza para demostrar la identidad de los usuarios, empresas y redes en infraestructuras de clave pública.

1 / 1 punto

- Una clave de acceso
- Un token de acceso
- Una firma digital
- Un certificado digital

 Correcto

6. Completa el espacio en blanco: El conocimiento, la posesión y la inherencia son tres factores de los sistemas _____.

1 / 1 punto

- de autorización
- de responsabilidad
- de administración
- de autenticación

 Correcto

7. ¿Cuáles son algunas de las desventajas de usar la tecnología de inicio de sesión único (SSO) para la autenticación de usuarios? Selecciona dos.

1 / 1 punto

- La gestión de nombres de usuario y contraseñas es más complicada para los usuarios finales.
- El acceso a todos los recursos conectados se detiene cuando el SSO está inactivo.

 Correcto

- Las credenciales robadas pueden dar a los atacantes acceso a múltiples recursos.

 Correcto

- Clientes, proveedores y socios comerciales son menos vulnerables a los ataques.

8. Una empresa naviera importa y exporta materiales por todo el mundo. Sus operaciones comerciales incluyen la compra de mercadería a proveedores, la recepción de envíos y la distribución de productos a minoristas. ¿Cómo debe proteger esta compañía sus activos en virtud del principio de segregación de funciones? Selecciona dos respuestas.

0 / 1 punto

- Empleando a una persona para que presente las órdenes de compra
- Empleando a una persona para que reciba los envíos y distribuya la mercadería

 Esto no debería estar seleccionado

Revisa [el video sobre la segregación de funciones](#).

- Empleando a una persona para que apruebe las órdenes de compra

- Empleando a una persona para que seleccione la mercadería y envíe los pagos

 Esto no debería estar seleccionado

Revisa [el video sobre la segregación de funciones](#).

9. ¿Qué tipo de información sobre el usuario contiene un token API? Selecciona dos respuestas.

0.5 / 1 punto

- La identidad de un usuario

 Correcto

- La contraseña de un usuario

 Esto no debería estar seleccionado

Revisa [el video sobre los tokens API](#).

- Los permisos del sitio de un usuario

- La clave secreta de un usuario

9. ¿Qué tipo de información sobre el usuario contiene un token API? Selecciona dos respuestas.

0.5 / 1 punto

La identidad de un usuario

Correcto

La contraseña de un usuario

Esto no debería estar seleccionado
Revisa [el video sobre los tokens API](#).

Los permisos del sitio de un usuario

La clave secreta de un usuario

10. ¿Cómo se conoce a la práctica de monitorear los registros de acceso de un sistema?

0 / 1 punto

Autenticación

Responsabilidad

Autorización

Auditoría

Incorrecto

Revisa [el video sobre responsabilidad](#).

Se usan muchos algoritmos de cifrado para enviar y almacenar datos en línea. Sirven para ocultar información privada, siempre y cuando sus claves estén protegidas. ¿Te imaginas tener que supervisar las claves que protegen toda tu información personal en línea? Yo tampoco. Y no es necesario, gracias a la infraestructura de clave pública. La infraestructura de clave pública, o PKI, es un marco de cifrado que protege el intercambio de datos en línea. Es un sistema amplio que facilita y protege el acceso a la información. ¿Cómo funciona? El PKI es un proceso de dos pasos. Empieza con el intercambio de información cifrada. Esto implica cifrado asimétrico, simétrico o ambos. El cifrado asimétrico usa una clave pública y una privada para cifrar y descifrar datos. Imagina que esta caja se puede abrir con dos llaves. Una llave, la clave pública, solo sirve para acceder a la ranura y meter cosas. La clave pública no sirve para eliminar cosas, se puede copiar y compartir con personas de todo el mundo para agregar cosas. Por otro lado, la segunda llave, clave privada, abre toda la caja y permite así eliminar cosas. Solo el propietario de la caja tiene la clave privada que la abre. Con la clave pública, las personas y servidores con los que te comunicas pueden ver y enviarte información cifrada que solo tú puedes descifrar con tu clave privada. Con estas dos claves, se intercambia información de forma segura con el cifrado asimétrico. Pero también se ralentiza el proceso. En cambio, el cifrado simétrico permite gestionar claves de forma rápida y simple. El cifrado simétrico usa una sola clave secreta para intercambiar información. Imagina la caja cerrada de nuevo. En lugar de dos llaves, o claves, el cifrado simétrico usa una. Con ella, el propietario puede abrir la caja, agregar cosas y cerrarla. Cuando quiere compartir el acceso, puede dar la clave a otra persona. Intercambiar una clave secreta agiliza la comunicación en línea, pero también la hace menos segura. El PKI usa el cifrado asimétrico y el cifrado simétrico, a veces en conjunto. Todo depende de si la prioridad es la velocidad o seguridad. Por ejemplo, las aplicaciones de chat móvil usan cifrado asimétrico para establecer una conexión entre

personas al comienzo de una conversación cuando la seguridad es la prioridad. Luego, cuando la velocidad del intercambio de comunicación es prioritaria, se usa el cifrado simétrico. Aunque ambos tienen sus fortalezas y debilidades, comparten una vulnerabilidad común: crear confianza entre el emisor y el receptor. Ambos procesos comparten claves que se pueden usar mal, extraviar o robar. Esto no importa al intercambiar datos en persona porque sabemos distinguir en quién confiamos y en quién no. Pero las computadoras no están naturalmente equipadas para hacer esta distinción. Ahí se aplica el segundo paso del PKI. El PKI aborda la vulnerabilidad de compartir claves creando confianza con un sistema de certificados digitales entre computadoras y redes. Un certificado digital es un archivo que verifica la identidad de un titular de clave pública. La mayoría de la información en línea se intercambia usando certificado digital. Los usuarios, empresas y redes poseen uno y los intercambian al comunicar información en línea como una forma de señalar confianza. Veamos un ejemplo de cómo se crean certificados digitales. Imagina que un negocio en línea lanzará su sitio web y quiere un certificado digital. Al registrar su dominio, la empresa de hosting envía información a una autoridad de certificación de confianza, o CA. Se trata de información básica como el nombre de la empresa y el país de sede. También se otorga una clave pública para el sitio. La CA usa estos datos para verificar la identidad de la empresa. Tras confirmarla, la CA cifra los datos con su clave privada. Finalmente, crea un certificado digital con los datos cifrados de la empresa. También contiene la firma digital de la CA para demostrar que es auténtica. Los certificados digitales son una identificación digital para restringir u otorgar el acceso a la información en línea. Así el PKI resuelve el problema de la confianza. Al combinar el cifrado asimétrico y simétrico, este enfoque de dos pasos para intercambiar datos protegidos entre fuentes confiables es lo que hace que el PKI sea un control de seguridad tan útil.

Examen de SEIM

1. ¿Qué carácter especial puedes usar para sustituir por cualquier otro carácter en el lenguaje de procesamiento de búsqueda (SPL)?

1 / 1 punto

*

|

=

!=

 **Correcto**

El carácter * también se conoce como comodín, que es un carácter especial que se puede sustituir por cualquier otro carácter.

2. ¿Cuáles de los siguientes pasos forma parte del proceso SIEM para la recopilación de datos? Selecciona tres respuestas.

1 / 1 punto

Recopilar y procesar datos.

 **Correcto**

Las herramientas SIEM recopilan, procesan e indexan datos generados por dispositivos y sistemas de todo un entorno.

Normalizar los datos para que estén listos para su lectura y análisis.

 **Correcto**

Las herramientas SIEM recopilan, procesan e indexan datos generados por dispositivos y sistemas de todo un entorno. La normalización de los datos facilita en mayor medida su lectura y análisis. Los datos sin procesar se procesan de manera que tengan un formato consistente, y solo se incluye la información del evento relevante.

Las herramientas SIEM indexan los datos para que se puedan buscar.

 **Correcto**

Las herramientas SIEM recopilan, procesan e indexan datos generados por dispositivos y sistemas de todo un entorno. Mediante la indexación, es posible acceder fácilmente a los datos a través de una búsqueda.

Supervisar la actividad y las alertas asociadas a intrusiones.

3. Completa el espacio en blanco: ____ es un lenguaje informático que se usa con el fin de crear reglas para buscar datos de registro ingeridos.

1 / 1 punto

YARA-L

EVE JSON

NIDS

SIEM

 **Correcto**

La notación de objetos JavaScript para formato de eventos extensibles (EVE JSON) es un formato de salida de Suricata para alertas y eventos. Chronicle usa el lenguaje informático YARA-L con el fin de crear reglas para buscar datos de registro ingeridos.

4. ¿Cuál de las siguientes opciones es un lenguaje de consulta de Splunk?

1 / 1 punto

SPL

IDS

UDM

SQL

 **Correcto**

Splunk usa su propio lenguaje de consulta, conocido como lenguaje de procesamiento de búsqueda (SP).

Examinar Firmar con Suricata

Examinemos una firma ya escrita en Suricata.

Este equipo Linux ejecuta Ubuntu, y Suricata ya está instalado.

Veamos algunos de sus archivos cambiando directorios al directorio etc620+ y al directorio Suricata.

Aquí se encuentran los archivos de configuración de Suricata.

Luego usaremos el comando ls para enumerar el contenido del directorio suricata.

Aquí hay un par de archivos distintos, pero revisemos la carpeta rules.

Aquí se encuentran las reglas ya escritas.

Aquí también puedes agregar firmas personalizadas.

Usaremos el comando cd seguido del nombre de la carpeta para ir a esa carpeta.

Con el comando ls, podemos ver que la carpeta contiene plantillas de reglas para diferentes protocolos y servicios.

Veamos el archivo custom.rules con el comando ls.

Para repasar, el comando ls devuelve el contenido de un archivo una página a la vez, lo que facilita avanzar y retroceder en el contenido.

Usaremos la tecla de flecha para ir hacia arriba.

```
analyst@career-certs:~$ cd /etc/suricata
analyst@career-certs:/etc/suricata$ ls
classification.config reference.config rules suricata.yaml threshold.config
analyst@career-certs:/etc/suricata$ cd rules/
analyst@career-certs:/etc/suricata/rules$ ls
app-layer-events.rules dnp3-events.rules http2-events.rules mqtt-events.rules
custom.rules dns-events.rules ipsec-events.rules nfs-events.rules
decoder-events.rules files.rules kerberos-events.rules ntp-events.rules
dhcp-events.rules http-events.rules modbus-events.rules smb-events.rules
analyst@career-certs:/etc/suricata/rules$ less custom.rules
```

```
# Custom rules example for http connection

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"GET on wire"; flow:established;
custom.rules (END)
```

Suricata format type

- EVE JSON - Extensible Event Format
JavaScript Object Notation

Suricata log types

- Alert logs
- Network telemetry logs

Los registros de alertas contienen información útil para investigaciones de seguridad. En general, es el resultado de firmas que detonaron la alerta. Por ejemplo, una firma que detecta tráfico sospechoso en toda la red genera un registro de alertas sobre detalles de ese tráfico.

Los registros de telemetría de red contienen datos de flujos de tráfico de red, la telemetría no siempre se aplica a seguridad. Solo registra los eventos de red, como una conexión que se lleva a cabo a un puerto específico.

Fuerza Bruta

Una cuestión de ensayo y error

Una forma de abrir una cerradura es probar la mayor cantidad de combinaciones posibles. A veces, los agentes de amenaza utilizan tácticas similares para obtener acceso a una

aplicación o una red.

Los atacantes utilizan diversas tácticas para ingresar en un sistema:

- En los *ataques de fuerza bruta simples*, los atacantes adivinan las credenciales de inicio de sesión de un usuario. Pueden hacerlo ingresando cualquier combinación de nombres de usuario y contraseñas que se les ocurra hasta que encuentren la que funcione.
- La de los *ataques de diccionario* es una técnica similar, excepto que en estos casos los atacantes utilizan una lista de credenciales de uso común para acceder a un sistema. Esta lista se asemeja a hacer coincidir una definición con una palabra en un diccionario.
- Los *ataques de fuerza bruta inversa* son similares a los ataques de diccionario, excepto que comienzan con una sola credencial y se prueba en varios sistemas hasta que se encuentra una coincidencia.
- El *relleno de credenciales* es una táctica en la que los atacantes usan credenciales de inicio de sesión robadas en violaciones de datos anteriores para acceder a cuentas de usuario en otra organización. Un tipo especializado de relleno de credenciales se llama *pasar el hash*. Estos ataques reutilizan credenciales hash robadas y sin salting para, de esta manera, engañar a un sistema de autenticación para que cree una nueva sesión de usuario autenticada en la red.

Nota: Además de las credenciales de acceso, la información cifrada a veces puede forzarse mediante una técnica conocida como *búsqueda exhaustiva de claves*.

Cada uno de estos métodos implica mucho trabajo para intentar adivinar. Forzar de forma bruta tu entrada en un sistema puede ser un proceso tedioso y lento, en especial cuando se realiza de forma manual. Es por eso que los agentes de amenaza a menudo utilizan herramientas para llevar a cabo sus ataques.

Herramientas del oficio

Se pueden utilizar muchísimas combinaciones para crear un solo conjunto de credenciales de inicio de sesión. La cantidad de caracteres, letras y números que se pueden mezclar es inmensa. Cuando se hace de forma manual, podría llevarle años a alguien probar todas las combinaciones posibles.

En lugar de dedicarle tiempo a esto, los atacantes suelen recurrir a software para que adivine por ellos. Estas son algunas herramientas comunes para utilizar en ataques de fuerza bruta:

- Aircrack-ng
- Hashcat
- John the Ripper
- Ophcrack
- THC Hydra

Medidas de prevención

Las organizaciones se defienden contra los ataques de fuerza bruta mediante una combinación de controles técnicos y administrativos. Cada uno hace que la ruptura de los sistemas de defensa a través de la fuerza bruta sea menos probable:

- Hashing y salting
- Autenticación de múltiples factores, o multifactor, (MFA)
- CAPTCHA
- Políticas de contraseñas

Las tecnologías como la autenticación de múltiples factores (MFA) refuerzan cada intento de inicio de sesión al requerir una segunda o tercera forma de identificación. Otras herramientas importantes son CAPTCHA y las políticas de contraseñas efectivas.

Hashing y salting

El **hashing** convierte la información en un valor único que luego se puede usar para determinar su integridad. El **salting** es una protección adicional que se utiliza para reforzar las funciones hash. Se trata de una técnica que consiste en agregar caracteres aleatorios a los datos, como contraseñas. Esto aumenta la longitud y la complejidad de los valores hash, lo que los hace más difíciles de usar y menos susceptibles a ataques de diccionario.

Autenticación de múltiples factores (MFA)

La **autenticación de múltiples factores, o multifactor**, (MFA) es una medida de seguridad que exige que un usuario verifique su identidad de dos o más formas para acceder a un sistema o red. Se trata de una estrategia de protección de la información por capas. La MFA limita las posibilidades de ataques de fuerza bruta porque, aunque una credencial se viera comprometida, es poco probable que usuarios no autorizados cumplan con cada requisito de autenticación.

CAPTCHA

CAPTCHA significa prueba de turing pública y automatizada para diferenciar entre máquinas y humanos. Se trata de un sistema de autenticación, mediante respuesta a un desafío. CAPTCHA pide a los usuarios que realicen una prueba simple para demostrar que son humanos y no un software que está intentando forzar una contraseña.

Estos son algunos ejemplos comunes de CAPTCHA:



Text CAPTCHA

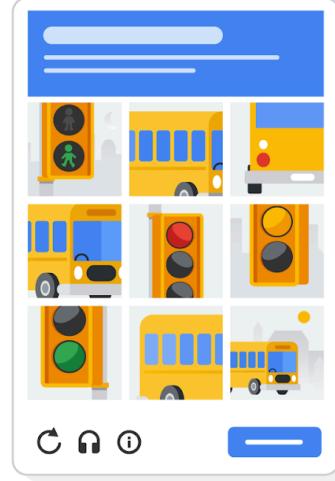


Image CAPTCHA

Existen dos tipos de pruebas de CAPTCHA. Uno desordena y distorsiona una secuencia de letras o números generada aleatoriamente y pide a los usuarios que los ingresen en una caja de texto. Otra prueba pide a los usuarios que relacionen imágenes con una palabra generada aleatoriamente. Es probable que hayas tenido que superar una prueba de CAPTCHA al acceder a un servicio web que contiene información confidencial, como una cuenta bancaria en línea.

Política de contraseñas

Las organizaciones utilizan estos controles de gestión para estandarizar las prácticas recomendadas de contraseñas en toda su empresa. Por ejemplo, una de estas políticas podría requerir que los usuarios creen contraseñas que tengan al menos ocho caracteres e incluyan una letra, un número y un símbolo. Otros requisitos comunes pueden incluir políticas de bloqueo de contraseñas. Por ejemplo, un bloqueo de contraseña puede limitar el número de intentos de inicio de sesión antes de que se suspenda el acceso a una cuenta y requerir que los usuarios creen contraseñas nuevas y únicas después de un determinado período de tiempo.

El propósito de cada uno de estos requisitos es crear la mayor cantidad de combinaciones de contraseñas posible. Esto extiende la cantidad de tiempo que tarda un atacante en encontrar una que funcione. La [Publicación especial 800-63B del Instituto Nacional de Estándares y Tecnología \(NIST\)](#) proporciona orientación detallada que las organizaciones pueden consultar al crear sus propias políticas de contraseñas.

Fuga de información

``en-note

La fuga de seguridad ha incrementado con más de **54k** casos de fuga de información. Es muy frecuente.

- **Datos no cifrados:** La mayoría de los datos no están cifrados. Denegar el acceso a los datos es esencial. - Todos los datos deberían estar cifrados. - Sin embargo, si los datos cifrados se encriptan y se pierde la llave, pueden no recuperarse. - Investigar qué es un **procesador criptográfico**.

¿Cómo se gesta una fuga de información?

1. Primero, se hace una introspección para identificar **vulnerabilidades** y qué información es vulnerable.
2. Se convoca al **equipo de respuesta**.
3. Generar una **investigación** sobre qué ocurrió.
4. Notificar y solicitar al área del **incidente**.
5. Entrar en una etapa de **recuperación**.
6. Verificar que todo esté bien para reanudar operaciones.
7. Hacer una **revisión** de lo que pasó.
8. Hacer ajustes basados en lo aprendido.

¿Qué se puede hacer?!

con el control de incidentes del nist el framework se usa

Gestión de alertas y eventos con herramientas de gestión de eventos e información de seguridad (SIEM) y orquestación, automatización y respuesta de seguridad (SOAR)

SIEM

Recopila y analiza los datos de registro para monitorear actividades de una organización, brinda a los profesionales de la seguridad información de alto nivel de lo que sucede en las redes .

Gestión de amenazas, riesgos y vulnerabilidades,

Gestión de riesgo

Un objetivo primordial de las empresas es proteger sus activos , un activo es un elemento que se percibe como valiosos para una organización, este puede ser digital o físico.

Algunos ejemplos pueden ser

- Números de seguridad Social o números únicos de identificación nacional asignados en personas
- Fechas de nacimiento
- Números de cuentas bancarias
- Direcciones postales

Ejemplos de físicos:

- Terminales de pago
- Servidores
- Computadoras de escritorio
- Espacios de oficina

Algunas estrategias habituales utilizadas para gestionar los riesgos son:

Aceptación : aceptar el riesgos para evitar interrumpir la continuidad del negocio

Prevención: crear un plan para evitar el riesgo por completo

Transferencia: transferir el riesgo a un tercero para que lo gestione.

Mitigación: Disminuir el impacto de un negocio de riesgo conocido

Además se implementan algunos marcos diferentes como Marco de gestión de riesgos (RMF) del nist

y el Health Information Trust Alliance (HITRUST)

Amenaza: Es cualquier circunstancia o evento que puede afectar negativamente a los activos estos son los mas comunes:

- Amenazas Internas: cuando miembros del personal o proveedores abusan de su acceso autorizado para obtener datos que pueden perjudicar a una organización
- Amenazas persistentes avanzadas (APT): cuando agentes de amenaza mantienen el acceso no autorizado a un sistema durante un periodo prolongado de tiempo.

Riesgo: Es todo aquello que puede afectar a la confidencialidad , integridad o disponibilidad de un activo. Una fórmula básica para determinar el nivel de riesgo es que este es igual a la probabilidad de una amenaza. Otra forma de verlo es que un riesgo es llegar tarde al trabajo y las amenazas son el tráfico o un accidente que puedan ocasionar una demora.

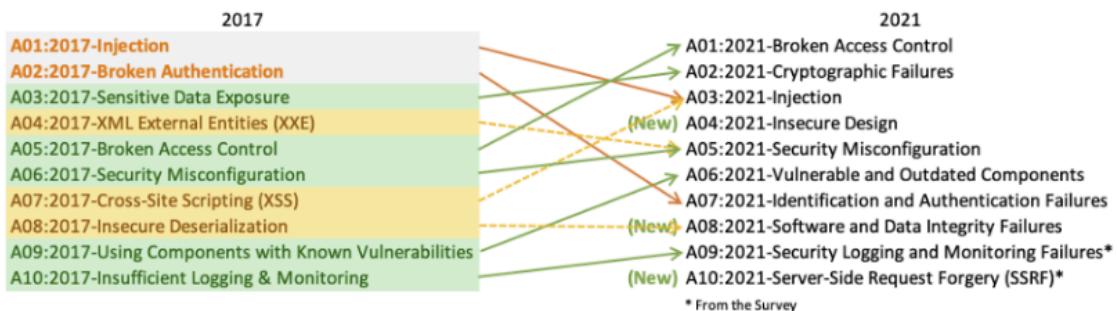
Existen diferentes tipos de riesgos:

- Riesgo Externo: se refiere a cualquier elemento, grupo o personas fuera de la organización que tienen el potencial de dañar sus activos , como agentes de amenaza que intentan acceder a información privada.
- Riesgo Interno: Se trata de colaboradores , proveedores externos o socios de confianza actuales o antiguos que pueden suponer un riesgo para la seguridad.
- Sistemas heredados: Son sistemas antiguos que si bien pueden no estar contabilizados o actualizados aun pueden afectar a los activos, como estaciones de trabajo o sistemas de mainframe antiguos.
- Riesgo de múltiples partes: Hace referencia a que , el externalizar el trabajo a terceros , pueden implicar darles acceso a propiedad intelectual, como información comercial confidencial , diseño de software y patentes.
- Cumplimiento normativo de licencias de software: Tiene que ver con el software que no esta actualizado o no cumple con la normativas o parches que no se instalan a tiempo.

Top 10 Riesgos de OWASP

Top 10 Web Application Security Risks

There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021.



Vulnerabilidades

Es una debilidad que puede ser aprovechada por una amenaza:

Vulnerabilidades:

ProxyLogon: una vulnerabilidad preautenticada que afecta un servidor de Microsoft Exchange . Esto significa que un agente de amenaza puede completar un proceso de amenaza y ingresar un código malicioso.

ZeroLogon: una vulnerabilidad en el protocolo de autenticación de Netlogon de Microsoft. Un protocolo de autenticación es una forma de verificar la identidad de una persona . Netlogon es un servicio que garantiza la identidad de un usuario antes de permitirle el acceso de un sitio web.

Log4Shell: posibilita a los atacantes ejecutar código Java en la computadora de otra persona o filtrar información confidencial. Para ello permite un atacante remoto tomar el control de dispositivos conectados a internet y ejecutar código malicioso.

- **PetitPotam:** afecta al gestor de redes de área local (LAN) de nueva tecnología de Windows (NTLM). Se trata de una técnica de robo que permite a un atacante basado en LAN iniciar una solicitud de autenticación.
- **Fallos de registro y supervisión de la seguridad:** capacidades de registro y supervisión insuficientes que dan lugar a que quienes perpetran un ataque aprovechen vulnerabilidades sin que la organización lo sepa.
- **Falsificación de solicitudes del lado del servidor:** permite a quienes perpetran un ataque manipular una aplicación del lado del servidor para que acceda a recursos backend y los actualice. También puede permitir que los agentes de amenaza roben datos.

Gestión de identidades y accesos

- El **principio de mínimo privilegio**, según el cual a un usuario solo se le otorga el nivel mínimo de acceso y autorización requerido para completar una tarea o función.
- La **segregación de funciones**, que es el principio según el cual no se debe conceder a los usuarios niveles de autorización que les permitan hacer un uso indebido de un sistema.

Estos dos principios suelen funcionar en conjunto. El mínimo privilegio establece límites en cuanto al acceso y autorización que una persona recibe, mientras que la segregación de funciones divide las responsabilidades entre varias personas para evitar que recaiga demasiado control en una sola.

Muchas empresas utilizan este modelo para implementar estos dos principios de seguridad y gestionar el acceso de los usuarios. En esta lectura, aprenderás sobre otro marco importante para gestionar el acceso de usuarios, **la gestión de identidades y accesos** (IAM, por sus siglas en inglés). Ampliarás tus conocimientos sobre las similitudes entre AAA e IAM y cómo se implementan habitualmente.

Gestión de identidades y accesos (IAM)

A medida que las organizaciones dependen cada vez más de la tecnología, los organismos reguladores aumentan su presión para que demuestren que están haciendo todo lo posible por prevenir amenazas. La **gestión de identidades y accesos** (IAM) es un conjunto de procesos y tecnologías que ayuda a las empresas a administrar las identidades digitales en su entorno. Tanto los sistemas AAA como los IAM están diseñados para autenticar usuarios, determinar sus derechos de acceso y realizar un seguimiento de sus actividades dentro de un sistema.

Cualquiera de los dos modelos utilizados por tu organización es más que un solo sistema claramente definido. Cada uno de ellos consiste en una serie de controles de seguridad que garantizan que el *usuario adecuado* tenga acceso a los *recursos correctos* en el

momento oportuno y por las razones apropiadas. Cada uno de estos cuatro factores es determinado por las políticas y procesos de la empresa para la que trabajas.

Nota: Un usuario puede ser una persona, un dispositivo o un software.

Autenticación de usuarios

Para garantizar que el usuario adecuado acceda a un recurso, se requiere algún tipo de prueba de que este es quien dice ser. En un [video sobre controles de autenticación](#), aprendiste que hay algunos factores que permiten confirmar la identidad de:

- **Conocimiento:** algo que el usuario sabe.
- **Posesión:** algo que el usuario posee.
- **Inherencia:** algo que el usuario es.

La autenticación se verifica principalmente mediante credenciales de inicio de sesión. El **inicio de sesión único** (SSO), una tecnología que combina varios inicios de sesión diferentes en uno solo, y la **autenticación de múltiples factores, o multifactor**, (MFA), una medida de seguridad que requiere que un usuario verifique su identidad de dos o más formas para acceder a un sistema o red, son otras herramientas que las organizaciones utilizan para autenticar a personas y sistemas.

Consejo profesional: La siguiente es otra forma de recordar este modelo de autenticación: algo que sabes, algo que posees y algo que eres.

Aprovisionamiento de cuentas de usuarios

Los sistemas backend deben ser capaces de verificar si la precisión de la información proporcionada por los usuario. Para lograrlo, es necesario realizar un adecuado **aprovisionamiento de usuarios**, que consiste en el proceso de crear y mantener la identidad digital de cada usuario. Por ejemplo, cuando una universidad contrata a un nuevo profesor, se crea una nueva cuenta de usuario. Esta cuenta se configura para brindar acceso a recursos exclusivos destinados a los profesores durante el período en el que están dando clases. Los analistas de seguridad suelen participar habitualmente en el aprovisionamiento de usuarios y en la asignación de sus accesos.

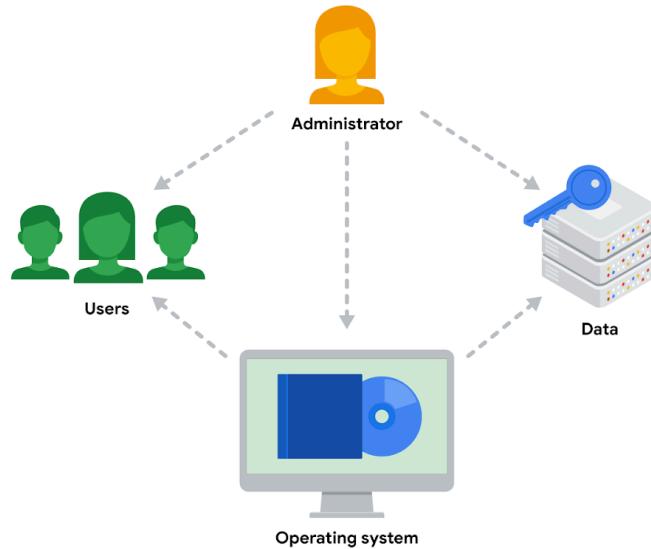
Consejo profesional: Otra función de los analistas en IAM es la de desaprovisionar usuarios. Esta es una práctica importante que elimina los derechos de acceso de un usuario cuando ya no debería tenerlos.

Concesión de autorización

Si el usuario adecuado ha sido autenticado, la red debe garantizar que los recursos correctos estén a su disposición. Existen tres marcos comunes que las organizaciones utilizan para manejar esta etapa de IAM:

- Control de acceso obligatorio (MAC).
- Control de acceso discrecional (DAC).
- Control de acceso basado en roles (RBAC).

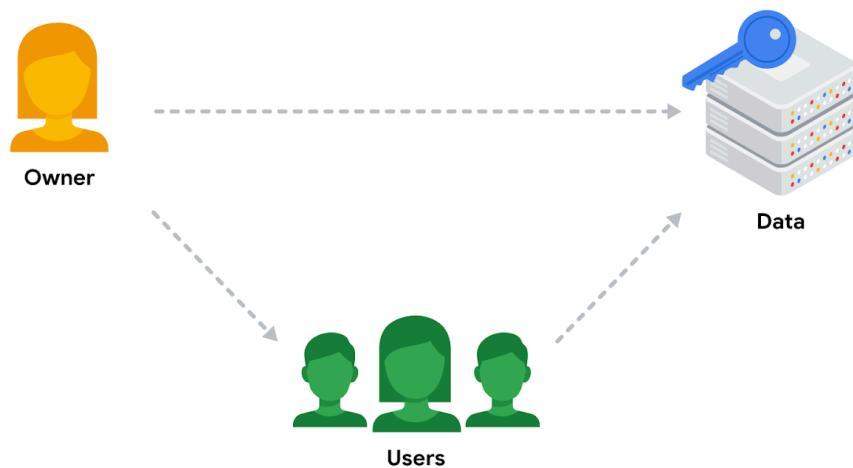
Mandatory Access Control (MAC)



Control de acceso obligatorio (MAC)

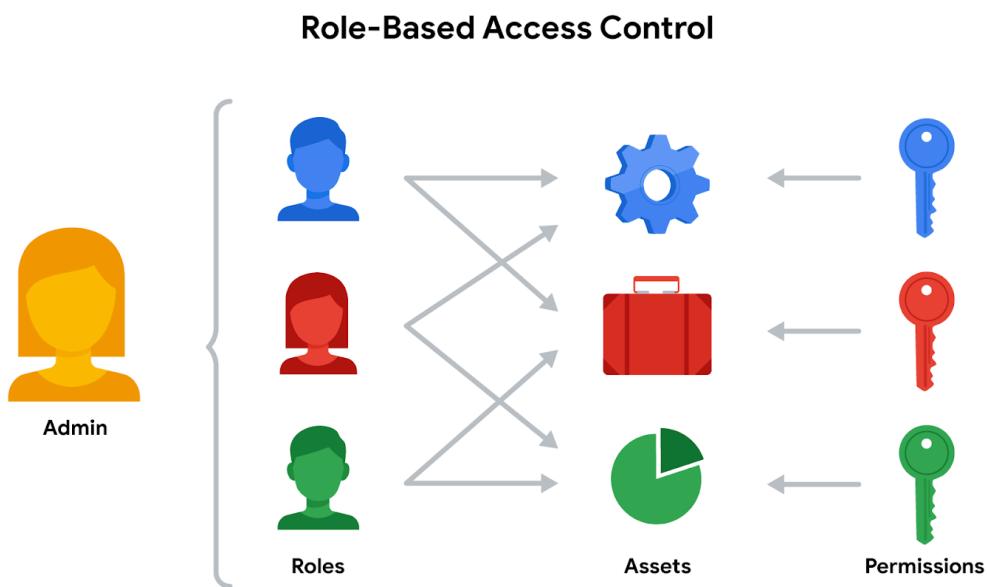
El control de acceso obligatorio (MAC) es el más estricto de los tres marcos. En este modelo, la autorización se basa en una estricta “necesidad de conocer”. El acceso a la información debe ser otorgado manualmente por una autoridad central o un administrador del sistema. Por ejemplo, MAC se aplica habitualmente en las fuerzas de seguridad, como el ejército, y otras agencias gubernamentales donde los usuarios deben solicitar acceso a través de una cadena de mando. MAC también se conoce como control no discrecional, ya que el acceso no se otorga a discreción del propietario de los datos.

Discretionary Access Control (DAC)



Control de acceso discrecional (DAC)

El control de acceso discrecional (DAC) suele aplicarse cuando el propietario de los datos decide los niveles de acceso adecuados. Un ejemplo de DAC es cuando el propietario de una carpeta de Google Drive comparte acceso con modo de editor, lector o comentador con otra persona.



Control de acceso basado en roles (RBAC)

El control de acceso basado en roles (RBAC) se utiliza cuando la autorización se determina según la función que tiene una persona dentro de una organización. Por ejemplo, alguien que se desempeña en el departamento de marketing puede tener acceso al análisis de usuarios, pero no a la administración de la red.

Tecnologías de control de acceso

Los usuarios suelen percibir la autenticación y la autorización como una experiencia unificada y fluida, en gran medida gracias a la sinergia entre las tecnologías de control de acceso que se integran entre sí. Estas herramientas ofrecen la velocidad y automatización necesarias para que los administradores supervisen y modifiquen los derechos de acceso, al mismo tiempo que reducen errores y posibles riesgos.

Algunas organizaciones desarrollan y mantienen por sí mismas tecnologías de control de acceso a través de su departamento de TI. Un sistema IAM o AAA típico consta de un directorio de usuarios, un conjunto de herramientas para administrar datos en ese directorio, un sistema de autorización y un sistema de auditoría. Estas soluciones personalizadas se crean para adaptarse a las necesidades específicas de seguridad de la organización. Sin embargo, es importante tener en cuenta que la creación de una solución interna puede requerir un alto costo en términos de tiempo y otros recursos.

En lugar de eso, muchas organizaciones optan por adquirir licencias de soluciones de terceros que ofrecen una serie de herramientas para proteger rápidamente sus sistemas de

información. Hay que tener en cuenta que la seguridad va más allá de simplemente combinar un conjunto de herramientas. Siempre es importante ajustar estas tecnologías para que contribuyan a proporcionar un entorno seguro.

Gestión del vulnerabilidades

Vulnerabilidad : Es una debilidad que puede ser explotada por una amenaza.

Los activos se protegen teniendo en cuenta sus vulnerabilidades

Exploit: Es una forma de aprovecharse de una vulnerabilidad

Gestión de vulnerabilidades : Es el proceso de buscar y aplicar parches en vulnerabilidades. Esta sirve para detener las amenazas antes de que se conviertan en un problema el cual sigue los siguientes pasos.

1. Identificar Vulnerabilidades
2. Pensar en los exploit que las vulnerabilidades pueden tener
3. Preparar defensas contra las amenazas
4. Evaluar esas defensas

Zero Day : Es un exploit que se desconocía, y se tienen cero días para arreglarlo.

Defensa a profundidad o Defensa in Depth :Es un enfoque por capas a la gestión de vulnerabilidades que reduce riesgos, tambien se le conoce Como enfoque castillo debido a como se parece a la defensa por capas de un castillo.

Defensa a profundidad estrategia:

1. Defensa perimetral : Esta capa incluye tecnologías como nombres de usuario y contraseña
2. Capa de autentificación del usuario : La cual filtra el acceso externo, su función es dar acceso solo a socios de confianza para pasar el siguiente nivel .
 - a. Capa de red : Consta de otras tecnologías como firewalls de red entre otras.
3. Punto de conexión o ENDPOINT: Los puntos de conexión son los dispositivos que poseen acceso en una red .
4. Capa de aplicación : Incluye todas las interfaces que se utilizan para interactuar con la tecnología, en esta parte se programan como parte de una aplicación.
5. Capa de datos : datos cruciales que se deben de proteger como la información personal identifiable

Glosario

Agente de amenaza: Persona o grupo de personas que representa una amenaza intencional para computadoras, aplicaciones o redes.

Adware: Tipo de software legítimo o malicioso que se utiliza para mostrar publicidad digital en las aplicaciones.

Amenaza persistente avanzada (APT): Situación en la que un agente de amenaza accede sin autorización a un sistema y permanece en él durante un periodo de tiempo prolongado.

Amenaza: Cualquier circunstancia o evento que pueda afectar negativamente a los activos.

Angler phishing: Tipo de ataque de suplantación de identidad en el que un agente de amenaza se hace pasar por representantes del servicio al cliente de una empresa en las redes sociales.

Aplicación potencialmente no deseada (PUA): Tipo de software que se incluye con programas legítimos y que puede mostrar anuncios, causar la ralentización del dispositivo o instalar otro software no deseado.

Árbol de ataque: Diagrama que muestra las amenazas a los activos y cómo se relacionan entre sí.

Ataque de “agujero de agua” (watering hole): Tipo de ataque en el que un agente de amenaza compromete un sitio web visitado con frecuencia por un grupo específico de usuarios.

Ataque de caza de ballenas (Whaling): Tipo de ataque de suplantación de identidad dirigido específicamente a personal de alto rango de una organización.

Ataque de inyección: Ataque mediante el cual se introduce un código malicioso en una aplicación vulnerable.

Ataque de secuencia de comandos en sitios cruzados, o entre sitios (XSS): Tipo de ataque de inyección que consiste en insertar código en un sitio web o aplicación web vulnerables.

Ataque de suplantación de identidad: (Consultar **Phishing**).

Ataque XSS almacenado: Tipo de ataque en el que se inyecta un script o secuencia de código malicioso directamente en el servidor.

Ataque XSS basado en DOM: Tipo de ataque en el que se inyecta un código malicioso directamente en la página web que carga un navegador.

Ataque XSS reflejado: Tipo de ataque en el que se envía un script malicioso a un servidor que se activa durante la respuesta del mismo.

Botnet: Conjunto de computadoras infectadas por software malicioso (malware), que están bajo el control de un solo agente de amenaza, conocido como el “bot-herder”.

Caballo de Troya (Troyano): Software malicioso que parece un archivo o programa legítimo.

Cebo (Baiting): Táctica de ingeniería social que incita a las personas a comprometer su seguridad.

Criptojacking: Tipo de software malicioso que instala un programa para minar criptomonedas ilegalmente.

Dropper: Tipo de troyano que instala un programa o archivo malicioso en un equipo de destino.

Exploits basados en la web: Fragmento de software o secuencia de comandos que se aprovecha de un error o vulnerabilidad de codificación en una aplicación web.

Gestión de identidad y acceso (IAM): Conjunto de procesos y tecnologías que ayuda a las organizaciones a administrar las identidades digitales en su entorno.

Gusano: Software malicioso que se reproduce por sí mismo y se propaga a través de los sistemas y redes.

Hacker: Cualquier persona o grupo de personas que utiliza computadoras para obtener acceso no autorizado a los datos. Se diferencia entre hacker ético, que es quien tiene como objetivo mejorar la seguridad y prevenir posibles ataques, y no ético o malintencionado, que es aquel que busca comprometer la seguridad de un sistema informático o de una red, con fines delictivos.

Ingeniería social: Técnica de manipulación que busca engañar a las personas con el fin de que revelen información o realicen determinadas acciones.

Inyección SQL: Tipo de ataque que consiste en ejecutar consultas maliciosas, con el fin de manipular a una base de datos y acceder a la información.

Kit de phishing: Conjunto de herramientas de software, preparado para lanzar una campaña de phishing con facilidad.

Malware sin archivos: (Consultar **Software malicioso sin archivos**).

Malware: (Consultar **Software malicioso**).

Modelado de amenazas: Proceso de identificación de activos, sus vulnerabilidades y su exposición a las amenazas, con el objetivo de planificar y optimizar las operaciones de seguridad de la red.

Phishing (Suplantación de identidad): Uso de comunicaciones digitales en las que se suplanta la identidad de una persona o empresa con el objetivo de engañar a otras personas para que revelen datos confidenciales o implementen un software malicioso.

Proceso de simulación de ataques y análisis de amenazas (PASTA): Metodología de modelado de amenazas de uso común en numerosas industrias

Quid pro quo: Tipo de cebo utilizado para engañar a una persona y hacerle creer que será recompensada si comparte un acceso, información o dinero.

Ransomware: (Consultar **Secuestro de datos**).

Rootkit: Software malicioso que proporciona acceso administrativo remoto a una computadora.

Saneamiento de entradas: Programación que valida las entradas de usuarios y de otros programas.

Scareware: Software malicioso que emplea tácticas para asustar a los usuarios con el fin de que infecten su dispositivo.

Secuestro de datos (Ransomware): Ataque malicioso que consiste en cifrar los datos de una organización para exigir el pago de un rescate para restablecer el acceso a ellos.

Sentencia preparada (Prepared Statement): Técnica de codificación que ejecuta sentencias SQL antes de pasárlas a una base de datos.

Sistema de detección de intrusiones (IDS): Aplicación que monitorea la actividad del sistema y alerta sobre posibles intrusiones.

Smishing: Tipo de ataque de suplantación de identidad (phishing) que utiliza mensajes de texto para engañar a los usuarios con el fin de obtener información confidencial.

Software malicioso (Malware): Programa diseñado para dañar dispositivos o redes.

Software malicioso sin archivos (Malware sin archivos): Tipo de software malicioso que utiliza programas legítimos que ya están instalados en una computadora para infectarla.

Phishing localizado (Spear phishing): Ataque de correo electrónico malicioso dirigido a una persona o grupo de personas específico que parece provenir de una fuente confiable

Spyware: Software malicioso que se usa para recabar y vender información sin el consentimiento de sus propietarios.

SQL, Structured Query Language (Lenguaje de consulta estructurado): Lenguaje de programación utilizado para crear, interactuar y solicitar información de una base de datos.

Tailgating: Táctica de ingeniería social en la que personas no autorizadas siguen a una persona autorizada hasta ingresar a una zona restringida.

Vishing: Tipo de estafa por suplantación de identidad en la que se busca obtener información sensible a través de una llamada telefónica.

Marcar como completo

Me gusta

No me gusta

Informar de un problema

Glosario de términos

Agente de amenaza: Persona o grupo de personas que representa una amenaza intencional para computadoras, aplicaciones o redes.

Amenaza: Cualquier circunstancia o evento que pueda afectar los activos de manera negativa.

Amenaza interna: Riesgo a la seguridad producido por una persona que pertenece o perteneció a una empresa o tiene una relación directa o de confianza con ella.

Ciberseguridad (o seguridad cibernética): Práctica de garantizar la confidencialidad, integridad y disponibilidad de la información mediante la protección de redes, dispositivos, personas y datos contra el acceso no autorizado o la explotación delictiva.

Habilidades técnicas: Competencias que requieren conocimiento de herramientas, procedimientos y políticas específicas.

Habilidades transferibles: Competencias de otras áreas que pueden aplicarse a diferentes carreras.

Información de identificación personal (PII por sus siglas en inglés): Cualquier información que pueda usarse para deducir la identidad de una persona.

Información de identificación personal sensible (SII por sus siglas en inglés): Tipo específico de Información de identificación personal que se rige por pautas de manejo más estrictas.

Seguridad de redes: Práctica de evitar accesos no autorizados a la infraestructura de red de una organización.

Cumplimiento normativo: leyes y directrices que exigen la aplicación de normas de seguridad.

Ataque de contraseña: Intento de acceder a dispositivos, sistemas, redes o datos protegidos con una contraseña.

Ataque a la cadena de suministro: Ataque que se dirige a sistemas y aplicaciones de empresas desarrolladoras y proveedoras de hardware y/o software para localizar una vulnerabilidad en la que se pueda implementar malware.

Ataque criptográfico: Ataque que afecta las formas seguras de comunicación protegidas por un sistema criptográfico.

Ataque de “agujero de agua”: Tipo de ataque en el que un agente de amenaza compromete a un sitio web visitado con frecuencia por un grupo específico de usuarios/as.

Ataque de suplantación de identidad en redes sociales (Phishing en redes sociales): Tipo de ataque en el que el agente de amenaza contacta a la víctima en alguna red social, con el fin de robar información personal o tomar el control de la cuenta.

Ataque físico: Incidente de seguridad que afecta a los entornos digitales y físicos en donde se implementa.

Autenticación: Proceso para verificar la identidad de una persona.

Cebo USB (USB Baiting): Ataque que consiste en incluir un software malicioso (malware) en una memoria USB para obtener una ventaja financiera.

Compromiso de correo electrónico empresarial (BEC): Tipo de ataque de suplantación de identidad, en el que un agente de amenaza se hace pasar por una persona conocida por la víctima e intenta que realice una acción, como enviar dinero u otorgar datos confidenciales de la compañía.

Hacker: Cualquier persona o grupo de personas que utiliza computadoras para acceder a datos sin autorización.

Ingeniería social física: Ataque en que un agente de amenaza se hace pasar por una persona ligada a la empresa para obtener acceso no autorizado a una ubicación física.

Ingeniería social: Técnica de manipulación que busca engañar a las personas con el fin de que revelen información o realicen determinadas acciones.

Inteligencia artificial (IA) antagónica: Técnica que manipula la tecnología de inteligencia artificial y aprendizaje automático para ejecutar ataques más eficientes.

Software malicioso (malware): Programa diseñado para dañar dispositivos o redes.

Phishing (Suplantación de identidad): Uso de comunicaciones digitales para engañar a las personas de manera que revelen datos confidenciales o instalen software malicioso en sus equipos.

Phishing localizado (Spear phishing): Ataque por correo electrónico malicioso dirigido a una persona o grupo de personas específico que parece provenir de una fuente confiable.

Virus: (consultar **Virus informático**).

Virus informático: Código malicioso creado para interferir en el funcionamiento de las computadoras y dañar los datos y el software

Vishing: tipo de estafa por suplantación de identidad en la que se busca obtener información sensible a través de una llamada telefónica.

Glosario Riesgos y vulnerabilidades

Términos y definiciones del curso 5, semana 1

Activo: Elemento percibido como valioso para una organización.

Amenaza: Cualquier circunstancia o evento que pueda afectar negativamente los activos.

Clasificación de activos: Práctica de etiquetar los activos en función de cuán sensibles e importantes son para una organización.

Cumplimiento normativo (Compliance): Proceso de adherirse y cumplir con las normas y reglamentos internos y externos con el fin de proteger la información y los sistemas de una empresa.

Dato: Información traducida, procesada o almacenada por una computadora.

Datos en reposo: Datos a los que no se está accediendo actualmente.

Datos en tránsito: Datos que se desplazan de un punto a otro.

Datos en uso: Datos a los que están accediendo uno/a o más usuarios/as.

Estándares: Referencias sobre los objetivos y controles exigibles en lo referente a la seguridad de la información.

Gestión de activos: Proceso de seguimiento de los activos y los riesgos que los afectan.

Inventario de activos: Catálogo de elementos valiosos que se deben proteger.

Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología

(NIST): Marco de adhesión voluntaria creado en los Estados Unidos, que incluye estándares, pautas y prácticas recomendadas para gestionar riesgos para la ciberseguridad.

Normativas: Normas establecidas por un gobierno u otra autoridad para controlar la forma en que se hace algo.

Política: Conjunto de reglas que reducen el riesgo y protegen la información.

Procedimientos: Instrucciones paso a paso para realizar una tarea de seguridad específica.

Riesgo: Cualquier hecho que pueda afectar la confidencialidad, integridad o disponibilidad de un activo.

Seguridad de la información (InfoSec): Práctica de controlar y salvaguardar los datos de una organización.

Vulnerabilidad: Debilidad que puede ser aprovechada por una amenaza.

Glosario Semana 2 activos y amenazas

Términos y definiciones del curso 5, semana 2

Algoritmo: Conjunto de instrucciones definidas, ordenadas y acotadas para resolver un problema, realizar un cálculo o desarrollar una tarea.

Algoritmo de cifrado (cipher): Algoritmo que cifra la información.

Aprovisionamiento de usuarios: Proceso de creación, actualización, modificación o eliminación de cuentas o perfiles de usuarios.

Ataque de fuerza bruta: Proceso de ensayo y error para descubrir información privada, como, por ejemplo, una contraseña.

Auditoría de seguridad: Revisión de los controles, políticas y procedimientos de seguridad de una organización.

Autenticación básica: Tecnología utilizada para establecer la solicitud de un usuario de acceder a un servidor.

Autenticación multifactor (MFA): Medida de seguridad que exige a un usuario verificar su identidad en dos o más formas para acceder a un sistema o red.

Bit: La unidad más pequeña de medición de datos en una computadora.

Cargador: Código malicioso que se inicia después de que un usuario inicia un programa dropper.

Certificado digital: Documento electrónico que verifica la identidad del titular de una clave pública.

Cifrado (encriptación): Proceso de convertir datos de un formato legible a uno codificado.

Cifrado asimétrico: Sistema criptográfico que utiliza dos claves, una pública y otra privada, para cifrar y descifrar datos.

Cifrado simétrico: Sistema criptográfico que utiliza una única clave para cifrar y descifrar datos.

Clave criptográfica: Secuencia de datos que descifra el texto cifrado o viceversa.

Colisión de hash: Situación en la que diferentes entradas comparten el mismo valor hash.

Controles de acceso: Tipo de controles de seguridad que gestionan el acceso, la autorización y el manejo de la información.

Controles de seguridad: Pautas diseñadas para abordar y eliminar riesgos de seguridad específicos, como la alteración o eliminación de información de perfiles, entre otros.

Cookie de sesión: Token que utilizan los sitios web para validar una sesión y determinar su duración.

Criptografía: (Consultar Cifrado).

Custodio de datos: Cualquier persona o entidad responsable del manejo, transporte y almacenamiento seguro de la información

Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI-DSS): Guía que define controles para la protección de los datos de titulares de tarjetas de pago y otros datos sensibles de autenticación, durante su procesamiento, almacenamiento y transmisión.

Evaluación de seguridad: Proceso de verificación que busca determinar la eficacia de las capacidades de ciberseguridad actuales contra las amenazas.

Función hash: Algoritmo que produce un código que no se puede descifrar.

Gestión de identidad y acceso (IAM): Conjunto de procesos y tecnologías que ayuda a las organizaciones a administrar las identidades digitales en su entorno.

Identificador de sesión (ID de sesión): Token único que identifica a un usuario y a su dispositivo mientras accede a un sistema.

Información de identificación personal (PII por sus siglas en inglés): Cualquier información que se pueda usar para deducir la identidad de una persona.

Información médica protegida (PHI, por sus siglas en inglés): Cualquier información relacionada con la salud, o la condición física o mental pasada, presente o futura de una persona.

Infraestructura de clave pública (PKI, por sus siglas en inglés): Marco de cifrado que garantiza la seguridad del intercambio de información en línea.

Inicio de sesión único (SSO): Solución de autenticación que combina varios inicios de sesión diferentes en uno solo.

No repudio: Concepto según el cual no se puede negar la autenticidad de una información.

OAuth “Open Authorization” (autorización abierta): Protocolo de autorización de estándar abierto que comparte el acceso designado entre aplicaciones.

Principio de mínimo privilegio: El concepto de otorgar únicamente el acceso y la autorización mínimos necesarios para ejecutar una tarea o función.

Privacidad de la información: Protección contra el acceso y la difusión de datos no autorizados.

Propietario de datos: Persona que tiene la potestad de decidir quién puede acceder a su información, editarla, usarla o destruirla.

Salting (salado): Protección adicional que se utiliza para reforzar las funciones hash que consiste en añadir un factor aleatorio a cada hash con el fin de que no se pueda predecir.

Secuestro de sesión: Ataque malicioso que consiste en obtener el identificador de sesión de un usuario legítimo.

Segregación de funciones: Principio según el cuál no se debe otorgar a una misma persona accesos a dos o más responsabilidades dentro del sistema que le permitirían hacer un uso indebido del mismo.

Sesión: Secuencia de solicitudes y respuestas de autenticación básica HTTP de red asociadas con el mismo usuario.

Tabla Arcoíris (Tabla Rainbow): Archivo de valores hash generados previamente y su texto sin cifrar asociado.

Tabla hash: Estructura de datos que se utiliza para almacenar y hacer referencia a los valores hash.

Token de interfaz de programación de aplicaciones (API): Pequeño bloque de código cifrado que contiene información sobre un usuario.

Glosario Semana 3

Términos del glosario de la semana 3

Términos y definiciones del curso 6, semana 3

Actividad posterior a un incidente: Proceso de revisión de un incidente para identificar áreas de mejora.

Análisis: Investigación y validación de alertas.

Cadena de custodia: Procedimiento documentado que permite constatar la posesión y el control de la evidencia obtenida durante el ciclo de vida de un incidente.

Caza de amenazas: Búsqueda proactiva de amenazas en una red.

Contención: Acto de limitar que un incidente se extienda para prevenir los daños adicionales que pudiera causar.

Crowdsourcing: Práctica de colaboración colectiva que consiste en recopilar información con base en aportes del público, con el fin de resolver un problema o llevar adelante una tarea.

Detección: Descubrimiento oportuno de eventos de seguridad.

Documentación: Cualquier forma de contenido que se ha registrado para un propósito específico.

Eradicación: Eliminación completa de los elementos de un incidente en todos los sistemas afectados.

Estándares: Referencias sobre los objetivos y controles exigibles en lo referente a la seguridad de la información.

Honeypot: Sistema o recurso vulnerable a los ataques creado como señuelo para atraer a posibles intrusos.

Indicadores de ataque (IoA): Serie de eventos observados que indican un incidente en tiempo real.

Indicadores de compromiso (IoC): Evidencia observable que sugiere indicios de un posible incidente de seguridad.

Informe final: Documentación que proporciona una revisión exhaustiva de un incidente.

Inteligencia de fuentes abiertas (OSINT): Recopilación y análisis de información procedente de fuentes de acceso público para generar inteligencia utilizable.

Inteligencia sobre amenazas: Información basada en evidencia que proporciona contexto sobre amenazas existentes o emergentes.

Manual de estrategias: Guía que proporciona detalles sobre cualquier acción operativa.

Plan de continuidad del negocio (BCP): Documento que describe los procedimientos para mantener las operaciones comerciales durante y después de una interrupción significativa.

Plan de respuesta a incidentes: Documento que describe los procedimientos a seguir en cada paso de la respuesta a un incidente.

Recuperación: Proceso por el que los sistemas afectados vuelven a funcionar con normalidad.

Resiliencia: Capacidad de prepararse, responder y recuperarse de las perturbaciones.

Reunión sobre lecciones aprendidas: Reunión en la que participan todas las partes implicadas tras un incidente grave.

Ruptura de la cadena de custodia: Inconsistencias en la recopilación y el registro de pruebas en la cadena de custodia.

Sistema de detección de intrusiones (IDS, por sus siglas en inglés): Aplicación que monitorea la actividad del sistema y alerta sobre posibles intrusiones.

Triaje: Clasificación y priorización de incidentes en función de su nivel de importancia o urgencia.

VirusTotal: Servicio que permite a cualquier persona analizar archivos, dominios, URL y direcciones IP sospechosas en busca de contenido malicioso.

Marcar como completo

Me gusta

No me gusta

Informar de un problema

Glosario semana 3 redes

Términos y definiciones del curso 3, semana 3

Ataque de denegación de servicio (DoS): Ataque dirigido a una red o servidor que los inunda con tráfico no deseado para inhabilitar los sistemas y servicios informáticos de

forma temporal.

Ataque de denegación de servicio distribuido (DDoS): Tipo de ataque de denegación o servicio que utiliza múltiples dispositivos o servidores situados en diferentes ubicaciones para inundar la red de destino con tráfico no deseado.

Ataque de inundación (SYN): Tipo de ataque DoS que simula una conexión TCP/IP e inunda un servidor con paquetes SYN.

Ataque de inundación del protocolo de mensajes de control Internet (inundación ICMP): Tipo de ataque DoS ejecutado por un/a atacante que envía repetidamente paquetes de solicitud ICMP a un servidor de red.

Ataque de repetición: Ataque a la red que consiste en interceptar un paquete de datos en tránsito para retrasarlo o repetirlo en otro momento.

Ataque de suplantación de IP: Ataque de red realizado cuando un/a atacante cambia la IP de origen de un paquete de datos para hacerse pasar por un sistema autorizado y obtener acceso a una red.

Ataque en ruta: Ataque en el que un agente de amenaza se coloca en medio de una conexión autorizada e intercepta o altera los datos en tránsito.

Ataque pitufo (Smurf): Ataque de red realizado cuando un atacante detecta la dirección IP de un usuario autorizado y la inunda con paquetes ICMP.

Botnet: Conjunto de computadoras infectadas por software malicioso (malware), que están bajo el control de un solo agente de amenaza, conocido como el “bot-herder”.

Rastreo activo de paquetes: Tipo de ataque en el que los paquetes de datos se manipulan en tránsito.

Rastreo de paquetes: Práctica de capturar e inspeccionar paquetes de datos a través de una red.

Rastreo pasivo de paquetes: Tipo de ataque en el que un agente de amenaza se conecta a un hub de red y observa todo el tráfico de la red.

Ping: Herramienta de la línea de comandos de prácticamente cualquier sistema operativo que posea conectividad a red. Se utiliza para probar la posibilidad de acceder a un dispositivo a través de la red. El comando envía una solicitud a un dispositivo específico mediante el uso del protocolo ICMP.

Ping de la muerte: Tipo de ataque DoS causado cuando un/a hacker hace ping a un sistema enviándole un paquete ICMP que supera los 64 KB.

Protocolo de mensajes de control de Internet (ICMP): Protocolo de Internet que utilizan los dispositivos para informarse mutuamente sobre los errores de transmisión de datos a través de la red.

Tarjeta de interfaz de red (NIC): Hardware que conecta las computadoras a una red.

GUI frente a CLI

La mayoría de las GUI incluyen estos componentes: menú de inicio con grupos de programas, barra de tareas para abrir programas, y un escritorio con íconos y accesos directos. Con estos componentes te comunicas con el sistema operativo y ejecutas tareas. En comparación, la interfaz de línea de comandos, o CLI, se basa en texto y usa comandos para interactuar con la computadora. Estos comandos se comunican con el sistema operativo y ejecutan tareas como abrir programas. La CLI tiene una estructura muy distinta a la de la GUI. Al usar la CLI, notarás la diferencia de inmediato. No hay íconos ni gráficos en la pantalla. La CLI se parece a líneas de código que usan ciertos lenguajes de texto. Una CLI es más flexible y más potente que una GUI.

Función

Estas dos interfaces también difieren en su funcionamiento. Una GUI es una interfaz que solo te permite realizar una solicitud a la vez. Sin embargo, una CLI te permite realizar múltiples solicitudes al mismo tiempo.

Ventajas de una CLI en ciberseguridad

La elección entre utilizar una GUI o una CLI se basa en parte en las preferencias personales, pero las/los analistas de seguridad deberían poder usar ambas interfaces. El uso de una CLI puede ofrecer ciertas ventajas.

Eficiencia

Algunas personas prefieren la CLI porque se puede utilizar más rápidamente, cuando se sabe cómo administrarla. Para un/a usuario/a nuevo/a, una GUI puede ser más eficiente, ya que es más fácil de navegar para principiantes.

Dado que una CLI puede aceptar múltiples solicitudes al mismo tiempo, es más potente cuando necesitas realizar múltiples tareas de manera eficiente. Por ejemplo, si tuvieras que crear varios archivos nuevos en tu sistema, podrías realizar rápidamente esta tarea en una CLI. Si estuvieras utilizando una GUI, esto podría llevar mucho más tiempo, ya que tendrías que repetir los mismos pasos para cada archivo nuevo.

Archivo de historial

Para las/los analistas de seguridad, el uso de la CLI de Linux es útil porque registra un archivo de historial de todos los comandos y acciones. Si estuvieras utilizando una GUI, tus acciones no se guardarían necesariamente en un archivo de historial.

Por ejemplo, podrías encontrarte en una situación en la que estás respondiendo a un incidente utilizando un manual de estrategias. Sus instrucciones requieren que ejecutes una serie de comandos diferentes. Si utilizas una CLI, podrías consultar el historial y asegurarte de que todos los comandos se utilizaron correctamente. Esto podría ser útil si hubiera habido problemas con el manual y tuvieras que revisar los pasos que realizaste en la línea de comandos.

Además, si sospechas que un atacante ha comprometido tu sistema, podrías rastrear sus acciones utilizando el archivo de historial.

HASHES y un ejemplo en la terminal de linux

La evolución de las funciones hash

Las funciones hash son controles importantes que forman parte de la estrategia de seguridad de todas las empresas. El hashing se utiliza ampliamente para la autenticación y el **no repudio**, que es el concepto de que la autenticidad de la información no puede ser negada.

Anteriormente, aprendiste que **las funciones hash** son algoritmos que producen un código que no se puede descifrar. Las funciones hash convierten la información en un valor único que luego puede utilizarse para determinar su integridad. En esta lectura, aprenderás sobre los orígenes de las funciones hash y cómo han cambiado con el tiempo.

Hashing Algorithm



Orígenes del hashing

Las funciones hash existen desde los inicios de la informática. Originalmente, fueron creadas como una forma de buscar datos de manera rápida. Desde el principio, estos algoritmos han sido diseñados para representar datos de cualquier tamaño como valores pequeños de tamaño fijo o compendios. Mediante el uso de una tabla hash, que es una estructura de datos utilizada para almacenar y referenciar valores hash, estos pequeños valores se convirtieron en una forma más segura y eficiente para que las computadoras accedan a los datos.

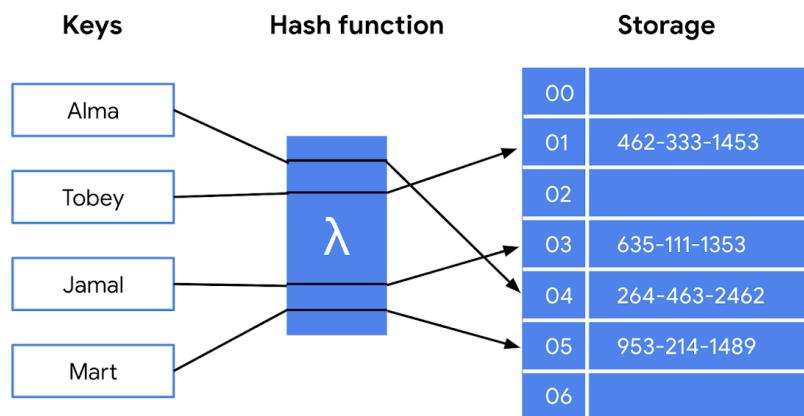
Una de las primeras funciones hash es Message Digest 5, más conocida como MD5. El profesor Ronald Rivest, del Instituto Tecnológico de Massachusetts (MIT), desarrolló MD5 a principios de la década de 1990 como una forma de verificar que un archivo enviado a través de una red coincidiera con su archivo de origen.

Ya sea utilizado para convertir un solo correo electrónico o el código fuente de una aplicación, MD5 funciona convirtiendo datos en un valor de 128 bits. Recordarás que un

bit es la unidad más pequeña de medición de datos en una computadora. Los bits pueden ser 0 o 1. En una computadora, los bits representan la entrada del usuario de una manera que las computadoras pueden interpretar. En una tabla hash, esto se muestra como una cadena de 32 caracteres. Cualquier alteración en el archivo de origen, genera un valor hash completamente nuevo.

Generalmente, cuanto más largo es el valor hash, más seguro es. Poco después de la creación de MD5, los expertos en seguridad descubrieron que los compendios de 128 bits daban lugar a una importante vulnerabilidad.

Este es un ejemplo de cómo el texto simple se convierte en valores hash:



Colisiones de hash

Una de las fallas de MD5 es, de hecho, una característica de todas las funciones hash. Los algoritmos hash asignan cualquier entrada, independientemente de su extensión, a un valor de tamaño fijo compuesto por letras y números. ¿Y cuál es el problema? Aunque existe una cantidad infinita de entradas posibles, ¡solo hay un conjunto finito de salidas disponibles!

Los valores MD5 están limitados a una extensión de 32 caracteres. Debido al tamaño de salida limitado, el algoritmo se considera vulnerable a la **colisión de hash**, una instancia en la que diferentes entradas producen el mismo valor hash. Dado que los hash se utilizan para la autenticación, una colisión de hash es similar a copiar la identidad de alguien. Los atacantes pueden llevar a cabo ataques de colisión para suplantar fraudulentamente datos auténticos.

Hashing de próxima generación

Para evitar el riesgo de colisiones de hash, se necesitaban funciones que generaran valores más largos. Las deficiencias de MD5 dieron paso a un nuevo grupo de funciones conocidas como algoritmos de hash seguro o SHA.

El Instituto Nacional de Estándares y Tecnología (NIST) aprueba cada uno de estos algoritmos. Los números junto a cada función SHA indican el tamaño de su valor hash en bits. Excepto SHA-1, que produce un compendio de 160 bits, se considera que estos algoritmos son resistentes a las colisiones. Sin embargo, eso no los hace invulnerables a otros exploits.

Cinco funciones componen la familia de algoritmos SHA:

- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

Almacenamiento seguro de contraseñas

Las contraseñas suelen almacenarse en una base de datos donde se asocian a un nombre de usuario. El servidor recibe una solicitud de autenticación que contiene las credenciales proporcionadas por el usuario. Luego, busca el nombre de usuario en la base de datos y lo compara con la contraseña brindada para verificar que coincida antes de otorgarle el acceso.

Se trata de un sistema seguro a menos que un atacante acceda a la base de datos de usuarios. Si las contraseñas se almacenan en texto sin cifrar, un atacante puede robar esa información y utilizarla para acceder a los recursos de la empresa. El hashing agrega una capa adicional de seguridad. Dado que los valores hash no pueden revertirse, un atacante no podría robar las credenciales de inicio de sesión de alguien incluso si lograra acceder a la base de datos.

Tablas Arcoíris (Tabla Rainbow)

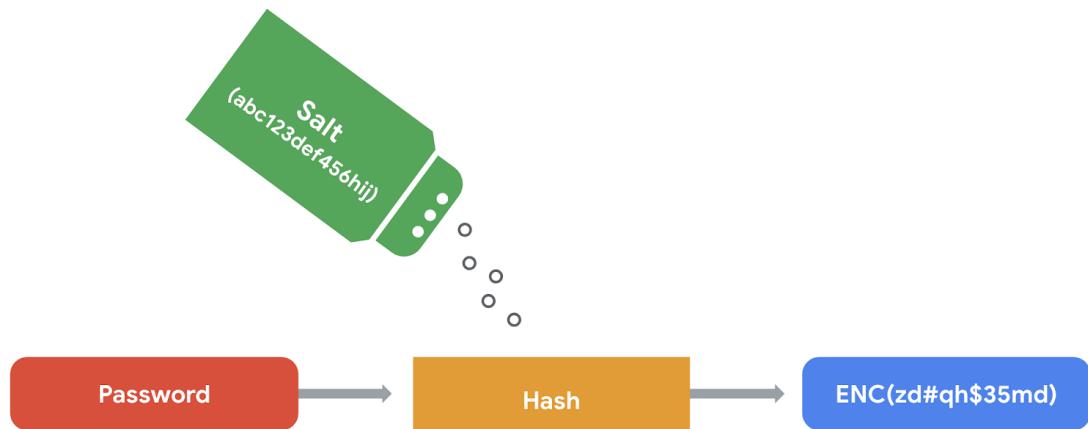
Una **tabla Arcoíris (Rainbow)** es un archivo de valores hash pregenerados y su texto sin cifrar asociado. Son como diccionarios de contraseñas poco seguras. Los atacantes capaces de obtener la base de datos de contraseñas de una organización pueden usar una tabla Arcoíris para compararlas con todos los valores posibles.

Añadir un poco de “sal”

Las funciones con compendios más grandes son menos vulnerables a los ataques de colisión y de tablas Arcoíris. Sin embargo, como ya sabes, ningún control de seguridad es perfecto.

El **salting** (salado) es una protección adicional que se utiliza para reforzar las funciones hash. Una “sal” es una cadena aleatoria de caracteres que se agrega a una entrada durante el proceso de hash. Por lo general, las “sales” se agregan al principio o al final de los datos mientras pasan por la función. Un uso cada vez más común del salting es el almacenamiento de contraseñas. Esta medida de seguridad adicional ayuda a proteger este tipo de información sin sobrecargar al usuario.

A continuación se muestra un ejemplo del proceso de salting:



Although the contents of both files appear identical when you use the `cat` command, you need to generate the hash for each file to determine if the files are actually different.

5. Use the `sha256sum` command to generate the hash of the `file1.txt` file:

```
sha256sum file1.txt
```



You now need to follow the same step for the `file2.txt` file.

6. Use the `sha256sum` command to generate the hash of the `file2.txt` file:

```
sha256sum file2.txt
```



7. Review the generated hashes of the contents of the two files:

```
analyst@4fb6d613b6b0:~$ sha256sum file1.txt
131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbd8267  file1.txt
analyst@4fb6d613b6b0:~$ sha256sum file2.txt
2558ba9a4cad1e69804ce03aa2a029526179a91a5e38cb723320e83af9ca017b  file2.txt
```

Herramientas de ciberseguridad

Herramientas de código abierto:

Suelen ser gratuitas y fáciles de usar. Su objetivo es proporcionar a los usuarios un software creado por las personas de manera colaborativa, que puede resultar más seguro. Además las herramientas de código abierto permiten una mayor personalización.

Herramientas propietarias

Estas una persona o empresa los desarrolla y los usuarios generalmente pagan por una tarifa por su uso y para su capacitación. Los dueños de las herramientas propietarias son los únicos que se pueden acceder y modificar el código fuente, esto significa que deben esperar para las actualizaciones en el software y posiblemente pagar una tarifa por estas. Como por ejemplo SIEM chronicle y splunk

Conceptos erróneos habituales

Existe la idea errónea de que las herramientas de código abierto son menos efectivas y no tan seguras de usar, en relación a las propietarias. Sin embargo, a lo largo de los años los/las desarrolladores/as han ido creando materiales de código abierto que se han convertido en estándares de la industria. Aunque es cierto que los agentes de amenaza han intentado manipular herramientas de código abierto, la realidad es que, justamente por ser de código abierto, es más difícil que las personas con intenciones maliciosas logren causar daño. La amplia exposición y el acceso inmediato al código fuente por parte de usuarios/as y profesionales bienintencionados/as e informados/as hace que sea menos probable que ocurran problemas, ya que pueden solucionarlos tan pronto como se identifican.

Ejemplos de herramientas de código abierto

En ciberseguridad, hay muchas herramientas que son de código abierto y comúnmente disponibles. Dos ejemplos son Linux y Suricata.

Herramientas SIEM

Splunk:

Splunk® Enterprise y Splunk® Cloud

Ambas nos permiten revisar datos de una organización en paneles. Esto ayuda a los profesionales de seguridad a gestionar la infraestructura interna de una organización mediante la recopilación, búsqueda, monitoreo y análisis de datos de múltiples fuentes y a observar así la totalidad de las operaciones diarias de una organización.

Panel de postura de seguridad:

Esta diseñado para los centros de operaciones de seguridad SOC, muestra los acontecimientos y tendencias destacados de una organización en cuanto a seguridad durante las últimas 24 horas y permite determinar si la infraestructura y las políticas de seguridad funcionan según lo diseñado. Lo pueden usar este panel para monitorear y investigar amenazas potenciales en tiempo real, como una actividad de red sospechosa cuyo origen es una ip específica.

Panel de resumen ejecutivo

El panel analiza y monitorea la salud en general de la organización a lo largo del tiempo, esto ayuda a los equipos de seguridad a mejorar las medidas que reducen el riesgo, se puede usar para generar reportes de incidentes y tendencias de seguridad durante un período de tiempo determinado.

Panel de revisión de incidentes

Permite identificar los patrones sospechosos que pueden ocurrir en caso de un incidente. Además destaca elementos de alto riesgo que necesitan una revisión inmediata por parte de un analista, resulta útil porque proporciona una cronología visual de los eventos que condujeron a un incidente.

Panel de análisis de riesgos:

Con este identificamos cuál es el riesgo para cada objeto de riesgo (Ejemplo: un usuario específico, una computadora o una dirección IP) muestra los cambios en la actividad o el comportamiento en una relación con el riesgo, como el inicio de sesión fuera de las horas de trabajo normales o un tráfico de red inusualmente alto desde una computadora específica, se usa para analizar el impacto potencial de las vulnerabilidades de activos críticos, lo cual ayuda a priorizar sus esfuerzos de mitigación de riesgos.

Chronicle

Es una herramienta SIEM nativa de la nube de Google que retiene, analiza y busca datos de registro para identificar posibles amenazas, riesgos y vulnerabilidades de seguridad como, por ejemplo:

- un activo específico
- un nombre de dominio
- un usuario
- una dirección IP

Panel de información empresarial (Enterprise Insights)

El panel de información empresarial muestra las alertas recientes. Identifica nombres de dominio sospechosos en los registros, conocidos como indicadores de compromiso (IOC), y cada resultado se etiqueta con una puntuación de confianza para indicar la probabilidad de una amenaza. También proporciona un nivel de gravedad, que indica la importancia de cada amenaza para la organización. Un/a analista de seguridad podría usar este panel para monitorear los intentos de inicio de sesión o acceso a datos relacionados con un activo crítico, como una aplicación o sistema, desde ubicaciones o dispositivos inusuales.

Panel de transferencia y estado de los datos

El panel de transferencia y estado de los datos muestra el número de registros de eventos, fuentes de registro y tasas de éxito de los datos que se procesan en Chronicle. Un/a

analista de seguridad podría usar este panel para asegurarse de que los orígenes de los registros estén configurados correctamente y que se reciban sin errores. Esto garantiza que el equipo de seguridad tenga acceso a los datos que se necesitan, al abordar los problemas relacionados con el registro.

El panel de coincidencias de IOC

El panel de coincidencias de IOC indica las principales amenazas, riesgos y vulnerabilidades para la organización. Las y los profesionales de seguridad utilizan este panel para observar los nombres de dominio, las direcciones IP y los IOC de los dispositivos a lo largo del tiempo, con el fin de identificar tendencias. Esta información les permite hacer foco en las principales amenazas. Por ejemplo, las/los analistas de seguridad pueden usar este panel para buscar actividad adicional asociada con una alerta, como un inicio de sesión de usuario sospechoso desde una ubicación geográfica inusual.

Panel principal

El panel principal muestra un resumen de alto nivel de la información relacionada con la ingestión de datos, las alertas y la actividad de eventos de la organización, a lo largo del tiempo. Las y los profesionales de seguridad pueden usar este panel para acceder a una cronología de eventos de seguridad, como un pico en intentos de inicio de sesión fallidos, para identificar tendencias de amenazas en fuentes de registro, dispositivos, direcciones IP y ubicaciones físicas.

Panel de detección de reglas

El panel de detección de reglas proporciona estadísticas de incidentes con el mayor índice de ocurrencias, severidades y detecciones a lo largo del tiempo. Las/los analistas de seguridad pueden usar este panel para acceder a una lista de todas las alertas activadas por una regla de detección específica, como una regla diseñada para alertar cada vez que un/a usuario/a abre un archivo adjunto malicioso conocido, desde un correo electrónico. Las/los analistas luego usan esas estadísticas para ayudar a gestionar incidentes recurrentes y establecer tácticas de mitigación, que permitan reducir el nivel de riesgo de una organización.

Panel de descripción general del acceso de usuarios

El panel de descripción general del acceso de usuarios proporciona información acerca del comportamiento de acceso de usuarios/as en toda la organización. Las/los analistas de seguridad pueden usar este panel para acceder a una lista de todos los eventos de inicio de sesión de usuarios para identificar las actividades inusuales, como el inicio de sesión de un mismo usuario desde varias ubicaciones al mismo tiempo. Esta información se usa para ayudar a mitigar las amenazas, los riesgos y las vulnerabilidades de las cuentas de usuario y las aplicaciones de la organización.

Chronicle: Herramienta nativa de la nube diseñada para conservar, analizar y buscar datos.

Información de seguridad y gestión de eventos (SIEM): Aplicación que recopila y analiza datos de registro para monitorear actividades críticas en una organización.

Manual de estrategias: Guía que proporciona detalles sobre cualquier acción operativa.

Métricas: Atributos técnicos clave, como el tiempo de respuesta, la disponibilidad y la tasa de fallos, que se utilizan para evaluar el rendimiento de una aplicación de software.

Orquestación, automatización y respuesta de seguridad (SOAR): Conjunto de aplicaciones, herramientas y flujos de trabajo que utilizan la automatización para responder a incidentes de seguridad.

Registro: Inventario de eventos que tienen lugar dentro de los sistemas de una organización.

Respuesta a incidentes: Intento rápido de una organización de identificar un ataque, contener los daños y corregir los efectos de una infracción de seguridad.

Sistema Operativo (SO): Interfaz entre la computadora y el/la usuario/a.

Splunk Cloud: Herramienta alojada en la nube que se utiliza para recopilar, buscar y monitorear datos de registro.

Splunk Enterprise: Herramienta utilizada para retener, analizar y buscar datos de registro de una organización y proporcionar información de seguridad y alertas en tiempo real.

Herramientas habituales en la ciberseguridad

Que es un log?

Un registro de eventos que ocurren dentro de los sistemas de una organización.

Ejemplo los registros de inicio de sesión de los empleados en las computadoras.

Estos ayudan a identificar vulnerabilidades y potenciales fugas de información.

SIEM (Security Information and Event Management)

Es una aplicación que se recopila y analiza datos de registro para monitorear actividades críticas de una organización. Un registro recopila eventos que ocurren dentro de los sistemas de una organización. Dependiendo de la cantidad de datos con los que se están trabajando es mas rápido.

Estas proporcionan diferentes alertas como por ejemplo: amenazas , riesgos y vulnerabilidades.

Ejemplo de herramientas

Splunk: plataforma de análisis de datos la cual busca retener analizar y buscar datos dentro del registro de una organización.

Chronicle de Google : almacena datos para su análisis y almacenan.

En ultima instancia se usan para mitigar el riesgo

Analizador de protocolo de red (Programas detectores de paquetes)

Es una herramienta diseñada para capturar y analizar el tráfico de datos en una red. Lo que quiere decir que la herramienta mantiene un registro de todos los datos que encuentran una computadora dentro de la red o organización.\

Manual de estrategia

Brinda detalles sobre cualquier acción operativa , con la forma de responder a un incidente de seguridad antes , durante y después de este. Los manuales pueden cambiar por organizaciones ya que es común que tenga diferentes cada organización.

Algunos ejemplos de manuales que se pueden seguir pueden ser:

Cadena de custodia: es el proceso para documentar la posesión y el control de la evidencia durante el ciclo de vida del incidente usando la seguridad forense , sed trabajaran con los datos involucrados.

Manual de protección y preservación de la evidencia:

es el proceso de trabajar adecuadamente con la evidencia digital,fragil y volátil. ya que existen procedimientos.

- Priorizar los datos volátiles que son los que pueden perderse si el dispositivo se apaga por lo cual se opta por hacer copias de estos mismos.

Programación

Es el proceso que se puede usar para crear un conjunto de instrucciones para que una máquina ejecute una tarea.

Se puede usar para automatizar procesos tediosos o que necesiten de una gran precisión y ayuda a reducir el riesgo de errores humanos.

Sistemas Operativos

Es la interfaz entre el hardware de la computadora y el usuario.

Vulnerabilidad de la web

Es un código o comportamiento malicioso que se utiliza para aprovechar las fallas de codificación en una aplicación web, lo cual puede explotar el acceso no autorizado, el robo de datos y la implementación de software malicioso.

Software Antivirus

es un programa utilizado para prevenir, detectar y eliminar malware y virus , dependiendo del tipo de software antivirus puede escanear la memoria de un dispositivo para encontrar patrones que indiquen la presencia de un software malicioso.

Sistema de detección de instrucciones IDS

Es una aplicación que monitorea la actividad del sistema y alerta sobre posibles instrucciones, el sistema analiza paquetes de red, que transportan pequeñas cantidades de datos a través de una red

Cifrado

Es el proceso de convertir datos de un formato legible a un formato codificado. Esto significa convertir de texto plano en texto cifrado seguro.

Pruebas de penetración

También llamadas testing son testes que simulan un ataque con el objetivo de ayudar a identificar vulnerabilidades en los sistemas, redes, sitios web, aplicaciones y procesos. Mediante el calculo de riesgo exhaustivo se pueden evaluar o identificar las amenazas externas o internas

Me entusiasma la ciberseguridad y disfruto al desarrollar, crear , contribuir y innovar soluciones que puedan ayudar al impacto positivo en una organización y a las personas a las que esta sirve\

Ademas me apasiona mucho los nuevos retos, siempre seguir aprendiendo de los demás o ser autodidacta

Tambien cuento con fortalezas como

- Comunicacion Verbal y Escrita sólida
- Gestión del Tiempo
- Programación
- Pensamiento Crítico
- Resiliencia

Me entusiasma la ciberseguridad y disfruto al desarrollar, crear , contribuir y innovar soluciones que puedan ayudar al impacto positivo en una organización y a las personas a las que esta sirve\

Ademas me apasiona mucho los nuevos retos, siempre seguir aprendiendo de los demás o ser autodidacta

Tambien cuento con fortalezas como

- Comunicacion Verbal y Escrita sólida
- Gestión del Tiempo
- Programación
- Pensamiento Crítico
- Resiliencia

Herramientas y técnicas de detección

En esta lectura, examinarás los diferentes tipos de tecnologías de sistemas de detección de intrusiones (IDS) y las alertas que estos generan. También aprenderás las dos técnicas que más suelen usar los sistemas de detección. Entender las capacidades y limitaciones de las

tecnologías IDS y sus técnicas de detección te ayudará a interpretar la información de seguridad para identificar y analizar los eventos de seguridad y responder a ellos.

Como ya sabemos, un **sistema de detección de intrusiones (IDS)** es una aplicación que monitorea la actividad del sistema y alerta sobre posibles intrusiones. Las tecnologías IDS ayudan a las organizaciones a monitorear la actividad que se desarrolla en sus sistemas y redes para poder identificar indicios de actividad maliciosa. Según dónde decidas configurar un IDS, este puede estar basado en host o en red.

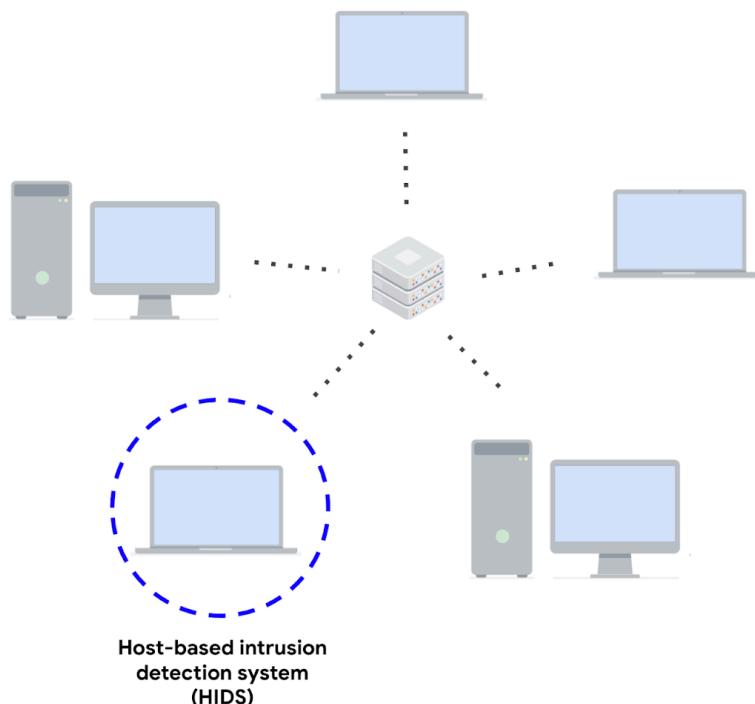
Sistema de detección de intrusiones basado en host

El **sistema de detección de intrusiones basado en host (HIDS)** es una aplicación que monitorea la actividad del host en el que está instalado. Se instala como un agente en un host. Al host también se lo conoce como **punto de conexión**, que es cualquier dispositivo conectado a una red, como una computadora o un servidor.

Por lo general, los agentes de HIDS se instalan en todos los puntos de conexión y se utilizan para controlar y detectar amenazas de seguridad. Un HIDS monitorea la actividad interna que ocurre en el host para identificar comportamientos no autorizados o anormales. Si detecta algo inusual, como la instalación de una aplicación no autorizada, el HIDS lo registra y envía una alerta.

Además de controlar los flujos de tráfico entrante y saliente, el HIDS puede tener otras capacidades, como supervisar los sistemas de archivos, el uso de los recursos del sistema, la actividad del usuario y más.

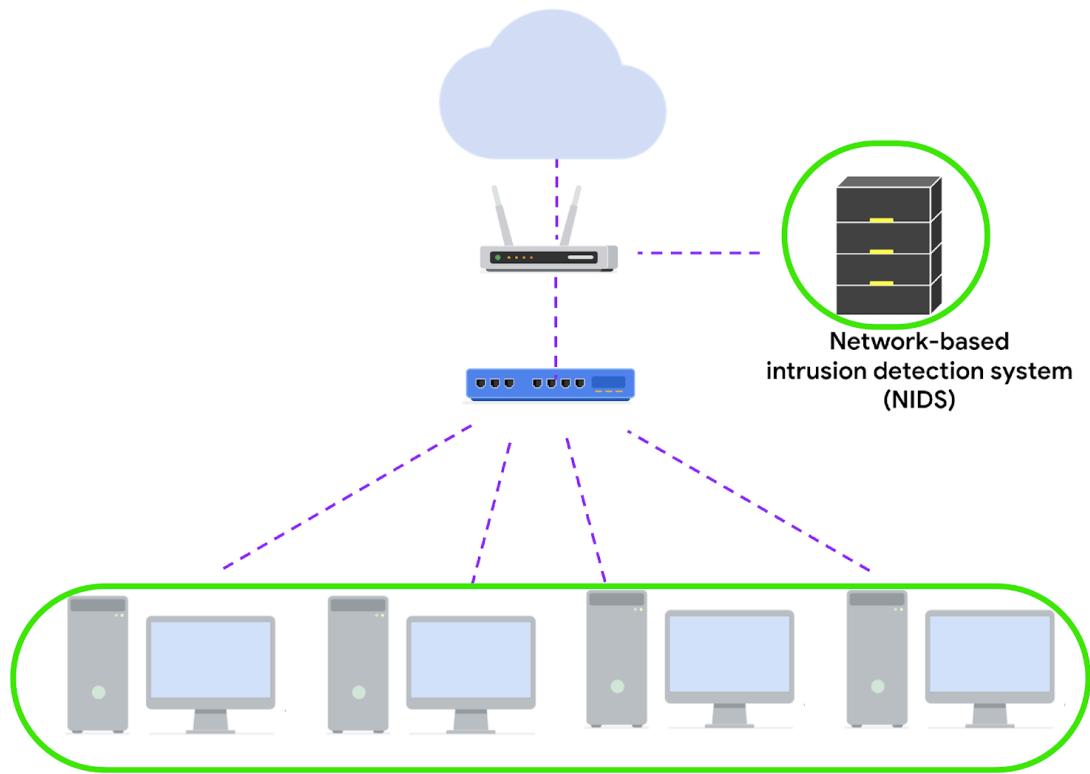
Este diagrama muestra una herramienta HIDS instalada en una computadora. El círculo punteado alrededor del host indica que solo está controlando la actividad local en esa computadora en la que está instalado.



Sistema de detección de intrusiones basado en la red

Un **sistema de detección de intrusiones basado en la red (NIDS)** es una aplicación que recopila y monitorea el tráfico de la red y sus datos. El software NIDS se instala en dispositivos ubicados en aquellas partes específicas de la red que se quiere monitorear. La aplicación NIDS inspecciona el tráfico de red desde diferentes dispositivos. Si detecta algún tráfico malicioso, lo registra y genera una alerta.

Este diagrama muestra un NIDS que está instalado en una red. El círculo resaltado alrededor del servidor y las computadoras indica que el NIDS está instalado en el servidor y está monitoreando la actividad de las computadoras.



Combinar un HIDS y un NIDS para monitorear un entorno puede ofrecer un enfoque multicapa para detectar intrusiones y darles respuesta. Ambas herramientas proporcionan una perspectiva diferente sobre la actividad que ocurre en una red y cada uno de los hosts que están conectados a ella. Esto aporta una visión integral de la actividad que se está desarrollando en un entorno.

Técnicas de detección

Los sistemas de detección pueden utilizar diferentes técnicas para detectar amenazas y ataques. Los dos tipos de técnicas de detección más utilizados por las tecnologías IDS son el análisis basado en firmas y el análisis basado en anomalías.

Análisis basado en firmas

El análisis de firmas, o análisis basado en firmas, es un método de detección que se utiliza para encontrar eventos de interés. Una **firma** es un patrón asociado con actividad maliciosa. Las firmas pueden contener patrones específicos, como una secuencia de números binarios, bytes o incluso datos específicos (como una dirección IP).

Anteriormente, exploraste la pirámide del dolor, un concepto que prioriza los diferentes tipos de **indicadores de compromiso** (IoC) asociados con un ataque o amenaza, como direcciones IP, herramientas, tácticas, técnicas y demás. Los IoC y otros indicadores de ataque pueden ser útiles para crear firmas dirigidas para detectar y bloquear ataques. Se pueden usar diferentes tipos de firmas según el tipo de amenaza o ataque que quieras detectar. Por ejemplo, una firma antimalware contiene patrones asociados con el malware. Esto puede incluir los scripts maliciosos que suele utilizar el malware. Las herramientas de IDS revisarán un entorno en busca de eventos que coincidan con los patrones definidos en esta firma de malware. Si un evento coincide con la firma, este se registra y se genera una alerta.

Ventajas

- **Baja tasa de falsos positivos:** El análisis basado en firmas es muy eficiente para detectar amenazas conocidas porque simplemente compara la actividad con las firmas y esto arroja menos falsos positivos. Recuerda que un **falso positivo** es una alerta que detecta incorrectamente la presencia de una amenaza, ya que esta no existe.

Desventajas

- **Las firmas se pueden eludir:** Al ser únicas, los atacantes pueden modificar sus comportamientos de ataque para evitarlas. Por ejemplo, pueden hacer pequeñas modificaciones en el código de malware para alterar su firma y evitar su detección.
- **Las firmas requieren actualizaciones:** El análisis basado en firmas depende de una base de datos de firmas para detectar amenazas. Cada vez que se descubre un nuevo exploit o ataque, es necesario crear nuevas firmas y agregarlas a la base de datos de firmas.
- **Es incapaz de detectar amenazas desconocidas:** El análisis basado en firmas se basa en la detección de amenazas conocidas a través de firmas. No es posible detectar amenazas desconocidas, como familias de malware nuevas o ataques de **día cero**, que son vulnerabilidades recién descubiertas.

Análisis basado en anomalías

El **análisis basado en anomalías** es un método de detección que identifica comportamiento anormal. En este tipo de análisis hay dos fases: aprendizaje y detección. Durante la fase de aprendizaje, es necesario crear un valor de referencia de lo que sería un comportamiento normal o esperado. Estos valores de referencia se desarrollan recopilando datos que corresponden al comportamiento normal del sistema. Durante la fase de detección, la actividad actual del sistema se compara con este valor de referencia. La actividad que está por fuera de ese valor se registra, y se genera una alerta.

Ventajas

- **Capacidad para detectar amenazas nuevas y en evolución:** A diferencia del análisis basado en firmas, que utiliza patrones conocidos para detectar amenazas, el análisis basado en anomalías *puede* detectar amenazas desconocidas.

Desventajas

- **Alta tasa de falsos positivos:** Cualquier comportamiento que se desvíe del valor de referencia se puede marcar como anormal, incluidos los comportamientos no maliciosos. Esto arroja una alta tasa de falsos positivos.
- **Compromiso preexistente:** La existencia de un atacante durante la fase de aprendizaje incluirá un comportamiento malicioso en el valor de referencia. Esto puede llevar a pasar por alto a un atacante preexistente.

Importancia de los flujos de tráfico de red

Que es el tráfico de red?

Es la cantidad de datos que circulan a través de una red, los datos se transmiten entre dispositivos en una red.

Indicadores de compromiso (IoC)

Son evidencia observable que sugiere signos de un potencial incidente de seguridad , como la infiltración de datos, que es la filtración no autorizada de datos desde un sistema.

Indicadores de compromiso

Indicadores de compromiso

Los **indicadores de compromiso (IoC)** son evidencias observables que sugieren indicios de un posible incidente de seguridad. Los IoC trazan piezas específicas de evidencia que están vinculadas con un ataque, como un nombre de archivo asociado con un tipo de malware. Se puede pensar en un IoC como evidencia que apunta a algo que ya ha sucedido, como notar que un objeto de valor ha sido robado del interior de un automóvil.

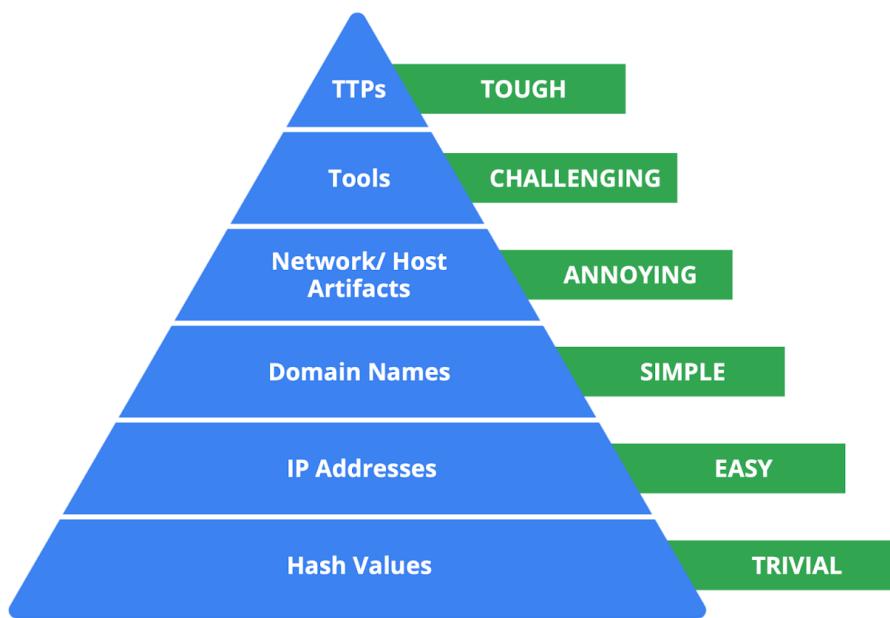
Los **indicadores de ataque (IoA)** son la serie de eventos observados que indican un incidente en tiempo real. Los IoA identifican el comportamiento de un atacante, incluidos sus métodos e intenciones.

Esencialmente, los IoC ayudan a identificar el *quién* y el *qué* de un ataque después de que haya tenido lugar, mientras que los IoA se centran en encontrar el *por qué* y el *cómo* de un ataque en curso o desconocido. Por ejemplo, observar un proceso que establece una conexión de red es un ejemplo de un IoA. El nombre de archivo del proceso y la dirección IP con la que se contactó el proceso son ejemplos de los IoC relacionados.

Nota: Los indicadores de compromiso no siempre son una confirmación de que ha ocurrido un incidente de seguridad. Los IoC pueden ser el resultado de errores humanos, mal funcionamiento del sistema y otras razones no relacionadas con la seguridad.

Pirámide del dolor

No todos los indicadores de compromiso son igual de importantes para los profesionales de seguridad y es clave que los conozcan en detalle, para poder detectarlos y responder a ellos de manera rápida y efectiva. Es por esto que el investigador de temas de seguridad David J. Bianco creó el concepto de la pirámide del dolor, que tiene el objetivo de mejorar la forma en que se utilizan los indicadores de compromiso en la detección de incidentes.



La pirámide del dolor establece la relación entre los indicadores de compromiso y el nivel de dificultad que los agentes de amenaza deben enfrentar, cuando los indicadores de compromiso son bloqueados por los equipos de seguridad. De esta manera, enumera los diferentes tipos de indicadores de compromiso que los profesionales de seguridad utilizan para identificar actividades maliciosas.

Cada tipo de indicador de compromiso se clasifica en niveles de dificultad. Estos representan los niveles de "dolor" que enfrenta un atacante cuando los equipos de seguridad bloquean la actividad asociada con el indicador de compromiso. Por ejemplo, el bloqueo de una dirección IP asociada con un agente de amenaza se etiqueta como fácil porque estos pueden usar sin dificultad distintas direcciones IP para sortear esto y así continuar con su ataque. Si los equipos de seguridad logran bloquear los IoC ubicados en la parte superior de la pirámide, más difícil se vuelve para los atacantes continuar con su misión. A continuación, se presenta un desglose de los diferentes tipos de indicadores de compromiso que se encuentran en la pirámide del dolor.

1. **Valores hash:** Hashes que corresponden a archivos maliciosos conocidos. A menudo se utilizan para proporcionar referencias únicas respecto a muestras específicas de malware o archivos involucrados en una intrusión.
2. **Direcciones IP:** Una dirección de protocolo de Internet como 192.168.1.1
3. **Nombres de dominio:** Una dirección web como www.google.com

4. **Artefactos de red:** Evidencia observable creada por agentes de amenaza en una red. Por ejemplo, la información que se encuentra en los protocolos de red, como las cadenas del agente de usuario (User-Agent strings).
5. **Artefactos de host:** Evidencia observable creada por agentes de amenaza en un host. Un host es cualquier dispositivo que esté conectado en una red. Por ejemplo, el nombre de un archivo creado por malware.
6. **Herramientas:** Software que es utilizado por un agente de amenaza para lograr su objetivo. Por ejemplo, los atacantes pueden usar herramientas de descifrado de contraseñas (password cracking) como John the Ripper para realizar ataques de contraseña y obtener acceso a una cuenta.
7. **Tácticas, técnicas y procedimientos (TTP):** Comportamiento de un agente de amenaza. Las tácticas tienen que ver con la visión general de alto nivel del comportamiento. Las técnicas proporcionan descripciones detalladas del comportamiento en relación a la táctica. Los procedimientos son descripciones muy detalladas de la técnica. Los TTP son los más difíciles de detectar.

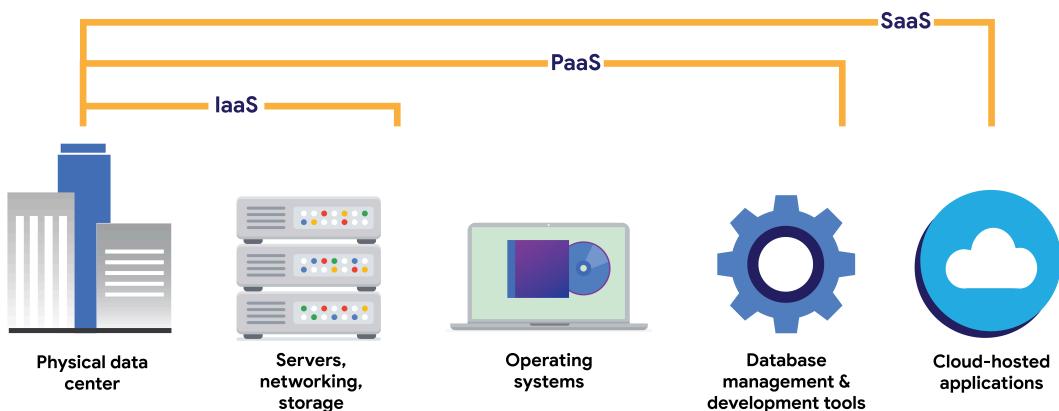
La computación en la nube

Se refiere a la práctica de utilizar servidores remotos aplicaciones y servicios de red que se alojan en internet

Un proveedor de servicios en la nube o CSP

Las empresas pagan por almacenamiento y la capacidad de procesamiento a gran escala .

- **Software como servicio (SaaS):** se refiere a suites de software operadas por el CSP que una empresa puede usar de forma remota sin alojar el software.
- **Infraestructura como servicio (IaaS):** se refiere al uso de componentes informáticos virtuales ofrecidos por el CSP. Estos incluyen almacenamiento y contenedores virtuales que se configuran de forma remota a través de la API o la consola web del CSP. Los servicios de almacenamiento y computación en la nube se pueden utilizar para operar aplicaciones existentes y otras cargas de trabajo tecnológicas sin hacer grandes modificaciones. Las aplicaciones existentes se pueden modificar para aprovechar las funcionalidades de disponibilidad, rendimiento y seguridad que son exclusivas de los servicios de proveedores en la nube.
- **Plataforma como servicio (PaaS):** se refiere a herramientas que los/las desarrolladores/as de aplicaciones pueden utilizar para diseñar aplicaciones personalizadas para su empresa. Estas aplicaciones se diseñan y alojan en la nube, y se utilizan para satisfacer las necesidades específicas del negocio de una empresa.

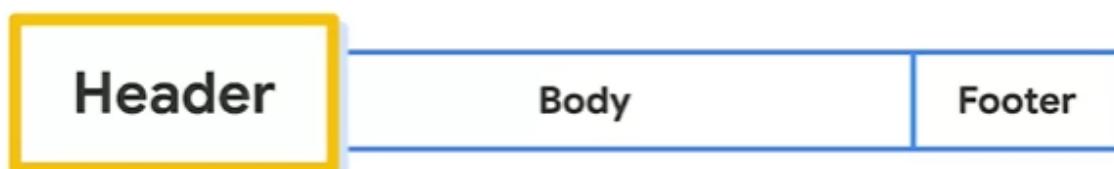


Un paquete de datos es una unidad básica de información que va de un dispositivo a otro en una red.

Al transferir datos por red de un dispositivo a otro, se envían como un paquete con información sobre su destino, su origen y el contenido del mensaje.

Como se compone un paquete de datos :

El encabezado del texto muestra la dirección IP y la MAC del dispositivo de destino. Además, contiene un número de protocolo que indica al dispositivo receptor cómo manejar la información. El texto parece ser una transcripción o descripción de una imagen. La imagen adjunta tiene un tamaño de 74 kB. Se destaca la importancia del encabezado para la transmisión de información.



IP address / MAC address / Protocol Number

El cuerpo del paquete contiene el mensaje que queremos transmitir



El pie. Similar a una firma en una carta, indica que el paquete ha sido completado.

Ancho de banda : es la cantidad de datos que un dispositivo recibe cada segundo (Se calcula dividiendo la cantidad de datos por el tiempo en segundos)
El rastreo de paquetes es capturar e inspeccionar paquetes en la red. La comunicación en la red es importante para compartir recursos y datos, permitiendo a las empresas funcionar bien. A continuación, verás más sobre los protocolos para la comunicación en red.

La fase de actividad del ciclo de vida posterior a un incidente

la fase final de la respuesta a incidentes: la actividad posterior a un incidente. Esta fase conlleva el proceso de revisar un incidente para identificar áreas de mejora en el manejo de incidentes. Durante esta fase del ciclo de vida, se actualizan o crean diferentes tipos de documentación. Uno de los más importantes que se crean es el informe final. Se trata de un documento que proporciona una revisión integral de un incidente. Incluye una línea de tiempo, detalles de todos los eventos relacionados al incidente y recomendaciones para la prevención futura.

Después del incidente, se trabaja en minimizar el riesgo de que se repita. Una forma de mejorar los procesos es la reunión sobre lecciones aprendidas. En ella participan todas las partes involucradas en el incidente, y suele llevarse a cabo dos semanas después de ocurrido. En esta reunión, se revisa el incidente para determinar qué sucedió, qué medidas se tomaron y cómo funcionaron. El informe final es también el principal documento de referencia en la reunión. El objetivo del debate en la reunión de lecciones aprendidas es compartir ideas e información sobre el incidente y ver cómo mejorar esfuerzos futuros.

Nos podemos plantear algunas de las siguientes preguntas

¿Qué pasó?

¿A qué hora sucedió?

¿Quién lo descubrió?

¿Cómo se contuvo?

¿Qué medidas se tomaron para la recuperación?

¿Qué pudo haberse hecho de otra manera?

La fase de contención, erradicación y recuperación del ciclo de vida

La importancia de las actualizaciones

Cómo corregir brechas en la seguridad

Una computadora desactualizada se parece mucho a una casa con las puertas sin llave. Los agentes de amenazas utilizan estas brechas en la seguridad de la misma manera: para obtener acceso no autorizado. Las actualizaciones de software son similares a cerrar las puertas con llave para mantenerlos fuera.

Un **parche de actualización** es una puesta al día del software y el sistema operativo que soluciona las vulnerabilidades de seguridad de un programa o producto. Por lo general, los parches contienen correcciones de errores contra vulnerabilidades y exposiciones de seguridad comunes.

Nota: Idealmente, los parches se encargan de reparar vulnerabilidades y exposiciones comunes antes de que los agentes de amenaza las descubran. Sin embargo, a veces se desarrollan como resultado de un **día cero**, que es un exploit que antes era desconocido.

Estrategias comunes de actualización

Cuando las actualizaciones de software están disponibles, los clientes y usuarios tienen dos opciones de instalación:

- Actualizaciones manuales
- Actualizaciones automáticas

Como aprenderás a continuación, cada estrategia tiene beneficios y desventajas.

Actualizaciones manuales

Una estrategia de implementación manual se basa en que los departamentos de TI o los usuarios obtengan actualizaciones de los desarrolladores. El *home office* o los entornos de pequeñas empresas pueden requerir que encuentres, descargues e instales las actualizaciones por tu cuenta. En entornos empresariales, el proceso por lo general se maneja con una herramienta de administración de configuración. Este tipo de herramienta ofrece una variedad de opciones para implementar actualizaciones, como para todos los clientes de tu red o un grupo selecto de usuarios.

Ventaja: Una ventaja de las estrategias de implementación de actualizaciones manuales es el control. Esto puede ser útil si los desarrolladores no testean bien las actualizaciones de software, lo cual puede llevar a problemas de inestabilidad.

Desventaja: Un inconveniente de las implementaciones de actualizaciones manuales es que uno puede ignorar u olvidarse por completo de alguna actualización crítica.

Actualizaciones automáticas

Una estrategia de implementación automática adopta el método opuesto. Con esta opción, el sistema o la aplicación pueden encontrar, descargar e instalar las

actualizaciones.

Consejo profesional: La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) recomienda utilizar opciones automáticas siempre que estén disponibles.

Los usuarios y los grupos de TI deben habilitar determinados permisos antes de que las actualizaciones se puedan instalar o, enviar, cuando estén disponibles. Depende de los desarrolladores testear adecuadamente sus parches antes del lanzamiento.

Ventaja: Una ventaja de las actualizaciones automáticas es que el proceso de implementación se simplifica. También mantiene los sistemas y el software actualizados con los últimos parches críticos.

Desventaja: Un inconveniente de las actualizaciones automáticas es que pueden ocurrir problemas de inestabilidad si el proveedor no testeó minuciosamente los parches. Esto puede resultar en problemas de rendimiento y una mala experiencia del usuario.

Software al final de su vida útil

A veces, las actualizaciones no están disponibles para cierto tipo de software conocido como software al final de su vida útil (End-of-Life, o EOL). Todo software tiene un ciclo de vida. Comienza cuando se produce y termina cuando se lanza una versión más nueva. En ese momento, los desarrolladores deben asignar recursos a las versiones más nuevas, lo que lleva al software EOL. Si bien el software anterior sigue siendo útil, el fabricante ya no ofrece soporte.

Nota: Los parches y actualizaciones (updates) son muy diferentes de las ampliaciones (upgrades). Las *ampliaciones* son versiones completamente nuevas de hardware o software que se pueden comprar.

CISA recomienda descontinuar el uso del software EOL porque representa un riesgo irreparable para los sistemas. Aun así, esta recomendación no siempre se sigue.

Reemplazar la tecnología EOL puede ser costoso para empresas y particulares.

Los riesgos que presenta el software EOL siguen creciendo a medida que más dispositivos conectados ingresan al mercado. Por ejemplo, existen miles de millones de dispositivos de Internet de las cosas (IoT), como bombillas de luz inteligentes, conectados a redes domésticas y de trabajo. En algunos entornos empresariales, todo lo que un atacante necesita es un solo dispositivo sin parches para obtener acceso a la red y causar problemas.

Lee registros de tcpdump

Un analizador de protocolo de red, a veces llamado sniffer de paquetes (rastreador de paquetes) o analizador de paquetes, es una herramienta usada para capturar y analizar el tráfico de datos dentro de una red. como por ejemplo:

- Analizador de tráfico NetFlow de SolarWinds
- ManageEngine OpManager

- Azure Network Watcher
- Wireshark
- tcpdump

tcpdump

Es un analizador de protocolos de red de una linea de comandos es ligero y lo pueden correr casi en cualquier lugar y usa una biblioteca de código abierto libcap.

tcpdump se basa en texto, lo que significa que todos los comandos son en terminal. muestra la dirección IP de origen, las direcciones IP de destino y los números de puerto que utilizan en las comunicaciones.

Interpretación de la salida

tcpdump imprime la salida de comando como los paquetes detectados en la linea de comandos y opcionalmente en un archivo de registro, después de ejecutar un comando. La salida de una captura de paquetes contiene mucha información importante sobre el tráfico de red.

Timestamp	Source IP	Source port	Destination IP	Destination port
20:00:29.538395	IP 198.168.10.1.41	> 198.111.123.1.61012: Flags		
	[P.], seq 120:176, ack 1, win 501, options [nop,nop,TS val			
	4106659748 ecr 2979487360], length 144			

Parte de la información que se recibe de una captura de paquetes es:

- **Marca de tiempo:** la salida comienza con la marca de tiempo, en el formato de horas, minutos, segundos y fracciones de segundo.
- **IP de origen:** el origen del paquete es proporcionado por su dirección IP de origen.
- **Puerto de origen:** el número de puerto de donde se originó el paquete.
- **IP de destino:** la dirección IP de destino es el lugar al que se transmite el paquete.
- **Puerto de destino:** el número de puerto del lugar al que se transmite el paquete.

Usos comunes

tcpdump y otros analizadores de protocolos de red se utilizan habitualmente para capturar y visualizar comunicaciones de red y para recopilar estadísticas sobre la red, por ejemplo, para solucionar problemas de rendimiento. También se pueden usar para:

- Establecer una línea de base para los patrones de tráfico de red y las métricas de utilización de la red.
- Detectar e identificar tráfico malicioso.
- Crear alertas personalizadas para enviar las notificaciones adecuadas cuando surgen problemas de red o amenazas a la seguridad.
- Localizar mensajería instantánea (IM), tráfico o puntos de acceso inalámbricos no autorizados.

Linux

Penetration testing tools in KALI LINUX ™

- Metasploit
- Burp Suite
- John the Ripper

Metasploit sirve para buscar y explotar vulnerabilidades en equipos. Con Burp Suite se buscan debilidades en apps web. Finalmente John the Ripper sirve para adivinar contraseñas.

El análisis forense digital consiste en recopilar y analizar datos para determinar qué ocurrió tras un ataque.

Digital forensics tools in KALI LINUX ™

- tcpdump
- Wireshark
- Autopsy

Tcpdump analiza paquetes de línea de comandos. Se usa para capturar el tráfico de red. Wireshark es otra herramienta usada comúnmente en la seguridad. Tiene una GUI que puede usarse para analizar tráfico de red en vivo y capturado. Un último ejemplo, Autopsy es una herramienta forense para analizar discos duros y smartphones.

Más distribuciones de Linux

Anteriormente, aprendiste sobre las diferentes distribuciones de Linux. Esto incluyó Kali Linux™. (Kali Linux™ es una marca comercial de OffSec.). Además de esta, hay otras distribuciones de Linux con las que los/las analistas de seguridad deberían estar familiarizados/as. En esta lectura, conocerás otras distribuciones de Linux.

Kali Linux™

Kali Linux™ es una distribución de Linux de código abierto que se utiliza ampliamente en la industria de la seguridad. Se basa en Debian y se caracteriza por incluir de forma preinstalada muchas herramientas útiles para pruebas de penetración y análisis forense digital. Las **pruebas de penetración** consisten en ataques simulados que ayudan a identificar vulnerabilidades en sistemas, redes, sitios web, aplicaciones y procesos. Por otro lado, el **análisis forense digital** es una práctica que implica recopilar y analizar datos para determinar qué sucedió después de un ataque. Estas actividades son claves en el ámbito de la seguridad.

Sin embargo, Kali Linux™ no es la única distribución de Linux utilizada en ciberseguridad.

Ubuntu

Ubuntu es una distribución de código abierto y fácil de usar que goza de amplia popularidad en el ámbito de la seguridad y en otros sectores. Ofrece tanto una interfaz de línea de comandos (CLI) como una interfaz gráfica de usuario (GUI). Al ser un derivado de Debian, Ubuntu incluye de forma predeterminada aplicaciones comunes. Además, los/las usuarios/as pueden descargar un gran cantidad de aplicaciones adicionales a través de un gestor de paquetes, incluyendo herramientas especializadas en seguridad. Debido a su extenso uso, Ubuntu cuenta con una gran cantidad de recursos comunitarios para brindar apoyo a los/las usuarios/as.

Ubuntu también se utiliza ampliamente en el ámbito de la computación en la nube. Por lo tanto, a medida que las organizaciones migran hacia servidores en la nube, el trabajo en ciberseguridad puede involucrar con mayor frecuencia derivados de Ubuntu.

Parrot

Parrot es una distribución de código abierto ampliamente utilizada en el ámbito de la seguridad. Al igual que Kali Linux™, Parrot viene con herramientas preinstaladas relacionadas con pruebas de penetración y análisis forense digital. Asimismo, como Kali Linux™ y Ubuntu, está basada en Debian.

Una característica destacada de Parrot es su enfoque en brindar una experiencia de uso amigable. Esto se logra mediante una interfaz gráfica de usuario (GUI) intuitiva que facilita la navegación. Además, también ofrece una interfaz de línea de comandos (CLI).

Red Hat®

Red Hat® es una distribución de Linux basada en suscripción y diseñada para su uso en empresas. A diferencia de las distribuciones mencionadas anteriormente, Red Hat no es gratuita. Debido a que está diseñada y respalda para uso corporativo, también cuenta con un equipo de soporte dedicado, al que las empresas clientes pueden consultar ante incidentes.

CentOS

CentOS es una distribución de código abierto que está estrechamente relacionada con Red Hat. Utiliza el código fuente publicado por Red Hat para proporcionar una plataforma similar. Sin embargo, no ofrece el mismo soporte corporativo y se basa en el respaldo y la colaboración de la comunidad de usuarios/as para obtener apoyo.

Los mecanismos de autorización

Separación de funciones consiste en que los usuarios no deben de recibir niveles de autorización con los que pueden abusar del sistema.

Controles de seguridad de autorización

- HTTP usa la autenticación básica envía un identificador al comunicarse con una pagina web
- OAuth es un protocolo de autorización de estándar abierto que comparte el acceso designado entre apps, usa token API para verificar el acceso entre tu y proveedor. Un token API es un pequeño bloque de código cifrado

AAA framework

- [Authentication](#)
- [Authorization](#)
- [Accounting](#)

Contabilidad en seguridad

- La contabilidad en seguridad consiste en supervisar los registros de acceso de un sistema para identificar actividades sospechosas o no autorizadas.

- Los analistas de seguridad utilizan los registros de acceso para identificar tendencias, como los intentos fallidos de inicio de sesión, descubrir a los piratas informáticos que han accedido a un sistema y detectar incidentes como las filtraciones de datos.

Sesiones y cookies

- Una sesión comienza cuando un usuario accede a un sistema y finaliza cuando cierra la sesión o se agota el tiempo de espera, y se identifica mediante un ID de sesión único.
- Las cookies de sesión son tokens que utilizan los sitios web para validar una sesión y determinar su duración, lo que hace que las sesiones web sean más seguras y eficientes al evitar el intercambio de información confidencial como nombres de usuario y contraseñas.

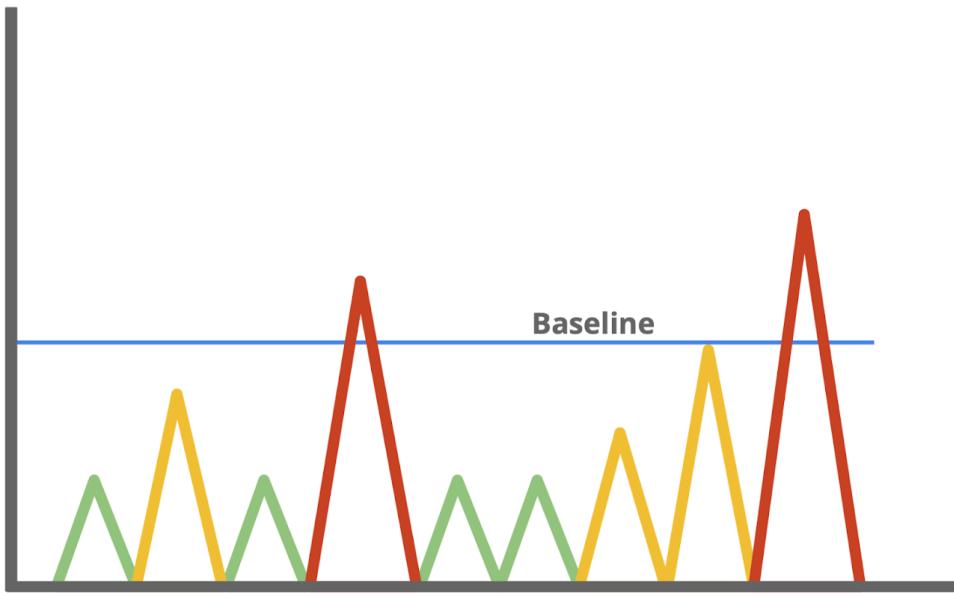
Riesgos de seguridad

- El secuestro de sesiones se produce cuando los atacantes obtienen el ID de sesión de un usuario legítimo, lo que les permite hacerse pasar por él y acceder potencialmente a información confidencial.
- La supervisión de los registros de sesión es crucial para detectar actividades inusuales que puedan indicar un acceso indebido o un robo de información.

Mantener la conciencia en el monitoreo de red

Conoce tu red

Como ya aprendiste, las redes conectan dispositivos y luego estos se comunican e intercambian datos utilizando protocolos de red. Las comunicaciones en red ofrecen información sobre conexiones, como direcciones IP de origen y destino, cantidad de datos transferidos, la fecha y la hora, y más. Esta información puede resultar valiosa para los profesionales de la seguridad al establecer **valores de referencia** de comportamiento normal o esperado.



Los valores de referencia son un punto de partida que se utiliza para la comparación. Es probable que en algún momento hayas encontrado o utilizado valores de referencia. Por ejemplo, un monto destinado a compras de alimentos en un presupuesto personal es un ejemplo que puede usarse para identificar cualquier patrón o cambio en los hábitos de gasto. En el ámbito de la seguridad, los valores de referencia ayudan a establecer un estándar de comportamiento esperado o normal para sistemas, dispositivos y redes. En esencia, al conocer los valores de referencia del comportamiento *normal* de una red, estarás en mejor posición para identificar un comportamiento de red *anormal*.

Monitorea tu red

Una vez que hayas establecido los valores de referencia, podrás monitorear una red para identificar cualquier desviación. El monitoreo implica examinar los componentes de la red para detectar actividades atípicas, como transferencias de datos grandes e inusuales. Aquí te brindamos algunos ejemplos de componentes de la red que se pueden monitorear para detectar actividad maliciosa:

Análisis de flujos

El flujo se refiere al movimiento de las comunicaciones en la red e incluye información relacionada con paquetes, protocolos y puertos. Los paquetes pueden dirigirse a puertos que reciben y transmiten comunicaciones. Con frecuencia, los puertos están asociados con los protocolos de red. Por ejemplo, el puerto 443 es comúnmente utilizado por HTTPS, que es un protocolo que proporciona cifrado de tráfico web.

Aun así, los agentes de amenaza pueden utilizar protocolos y puertos que no están comúnmente asociados, para mantener comunicaciones entre el sistema comprometido y su propia máquina. Estas comunicaciones son lo que se conoce como **comando y control (C2)**, que son las técnicas utilizadas por agentes de amenaza para mantener las comunicaciones con sistemas comprometidos.

Por ejemplo, los agentes de amenaza pueden utilizar el protocolo HTTPS sobre el puerto 8088 en lugar de su puerto comúnmente asociado, el 443, para comunicarse con sistemas comprometidos. Las organizaciones deben saber qué puertos tienen que estar abiertos y aprobados para conexiones, y estar en alerta ante cualquier desajuste entre los puertos y sus protocolos asociados.

Información de la carga útil del paquete

Los paquetes de red contienen componentes relacionados con la transmisión del paquete. Esto incluye detalles como la dirección IP de origen y destino, y la información de su carga útil, que son los datos reales que se transmiten. Con frecuencia, estos datos se cifran y requieren ser descifrados para poder ser legibles. Las organizaciones pueden monitorear la información de la carga útil de los paquetes para identificar actividades inusuales, como la transmisión de datos confidenciales fuera de la red, lo que podría indicar un posible ataque de exfiltración de datos.

Patrones temporales

Los paquetes de red contienen información relacionada con el tiempo. Esta información es útil para comprender los patrones temporales. Por ejemplo, una empresa que opera en América del Norte experimenta flujos de tráfico masivo entre las 9 am y las 5 pm, que es el valor de referencia de la actividad normal en la red. Si de pronto se observan volúmenes grandes de tráfico fuera de los horarios normales de actividad de la red, esto se considera *fuera del valor de referencia* y debe investigarse.

A través del monitoreo de la red, las organizaciones pueden detectar rápidamente intrusiones y trabajar para prevenirlas, asegurando los componentes de la red.

Protege tu red

En este programa, aprendiste sobre los **centros de operaciones de seguridad (SOC)** y su papel en el monitoreo de sistemas contra amenazas y ataques de seguridad. Las organizaciones pueden implementar un **centro de operaciones de red (NOC)**, que es una unidad organizativa encargada de supervisar el rendimiento de una red y responder a cualquier interrupción, como un fallo de red. Mientras que un SOC se centra en mantener la seguridad de una organización a través de la detección y la respuesta, un NOC es responsable de mantener el rendimiento, la disponibilidad y el tiempo de actividad de la red.



Los analistas de seguridad monitorean las redes para identificar cualquier signo de posibles incidentes de seguridad, conocidos como **indicadores de compromiso (IoC)**, y protegerlas contra los ataques o amenazas. Para hacerlo, deben comprender el entorno por el que viajan las comunicaciones de red y así poder identificar las desviaciones en el tráfico de red.

Herramientas de monitoreo de red

El monitoreo de la red se puede automatizar o realizar de forma manual. Algunas herramientas comúnmente utilizadas pueden incluir:

- **Sistemas de detección de intrusiones (IDS)**, que monitorean la actividad del sistema y alertan sobre posibles intrusiones. Un IDS identifica y alerta sobre las desviaciones que le hayas configurado para que detecte. Lo más habitual es que las herramientas IDS monitorean el contenido de la carga útil del paquete para detectar los patrones asociados con amenazas como malware o intentos de phishing.
- **Analizadores de protocolo de red**, también conocidos como rastreadores de paquetes, que son herramientas diseñadas para capturar y analizar el tráfico de datos dentro de una red. Se pueden utilizar para analizar las comunicaciones de red manualmente en detalle. Los ejemplos incluyen herramientas como tcpdump y Wireshark, que pueden utilizar los profesionales de seguridad para registrar comunicaciones de red a través de capturas de paquetes. Estas se pueden investigar para identificar las actividades potencialmente maliciosas.

Conclusiones clave

Monitorear y proteger las redes de intrusiones y ataques son responsabilidades fundamentales de los profesionales de seguridad. No se puede proteger lo que no se conoce. Como analista de seguridad, necesitarás comprender los componentes de una red y las comunicaciones que ocurren en ella, para así poder protegerla de manera más

efectiva. Los valores de referencia proporcionan una forma de comprender el tráfico de red al revelar patrones comunes que ayudan a identificar cualquier desviación de los patrones de tráfico esperados. Herramientas como los sistemas de detección de intrusiones y los analizadores de protocolos de red apoyan los esfuerzos para monitorear las actividades de la red.

Recursos

- Si deseas obtener más información sobre los componentes de red que las organizaciones pueden monitorear, consulta [tráfico de red: MITRE ATT&CK®](#)
- Los atacantes pueden aprovechar diferentes técnicas para exfiltrar datos. Si deseas obtener más información, consulta [técnicas de exfiltración de datos: MITRE ATT&CK®](#)

Manual de incidencias

La respuesta a incidentes es el intento rápido de una organización para identificar un ataque, contener el daño y corregir los efectos de una fuga de información. Un manual de respuesta a incidentes es una guía con seis fases que se usa para ayudar a mitigar y gestionar incidentes de seguridad de principio a fin.

1. Primera fase la preparación:

Las organizaciones deben prepararse para mitigar la probabilidad , el riesgo y el impacto de un incidente de seguridad, documentando procedimientos, creando planes para el personal y formando a los usuarios. La preparación sienta las bases para una respuesta a incidentes exitosa. por ejemplo las organizaciones puede crear planes y procedimientos de respuesta a incidentes que delinean roles y responsabilidades de cada miembro del equipo de seguridad.

2. Segunda fase " detección y análisis"

El objetivo es detectar y analizar eventos mediante procesos y tecnologías definidas, El uso de las herramientas y estrategias adecuada durante la fase ayuda a los demás analistas de seguridad a determinar si de produjo una fuga y analizar su posible magnitud.

3. Tercera fase "Contención "

El objetivo de la contención es prevenir el mayor daño y reducir el impacto intermedio de un incidente de seguridad , se actúa para contener el incidente de seguridad y minimizar el daño , La contención es una prioridad alta para las organizaciones por que ayuda a prevenir riesgos permanentes para dato y activos físicos

4. Cuarta fase "La erradicación y recuperación "

Esta fase implica la eliminación completa de los artefactos de un incidente, de manera que una organización pueda volver a operar con normalidad

5. Quita fase "La actividad posterior al incidente "

Aquí se documenta el incidente, se informa a los directivos de la organización y se aplican las lecciones aprendidas para garantizar que la organización esté mejor preparada para manejar futuros incidentes.

6. Sexta fase "coordinación"

Implica informar incidentes y compartir información durante todo el proceso de respuesta a incidentes en base a los estándares de la organización es importantes porque asegura que las organizaciones satisfagan los requisitos de cumplimiento y permite una respuesta y resolución coordinadas.

Manuales de estrategias, herramientas SIEM y herramientas SOAR

Manuales de estrategias y herramientas SIEM

Los manuales de estrategias son muy utilizados por los equipos de ciberseguridad ya que garantizan que, en caso de un incidente, se siga una lista consistente de acciones de una manera prescrita, independientemente de quién esté trabajando en el caso. Los manuales pueden ser muy detallados e incluir diagramas de flujo y tablas, para aclarar qué acciones tomar y en qué orden. También se utilizan para los procedimientos de recuperación, en caso de un ataque de ransomware (secuestro de datos). Los diferentes tipos de incidentes de seguridad tienen sus propios manuales de estrategias que detallan quién debe tomar qué acción y cuándo debe hacerlo.

Los manuales de estrategias suelen usarse junto con las herramientas SIEM. Si, por ejemplo, una herramienta SIEM señala el comportamiento inusual de un usuario, un manual de estrategias proporciona a los analistas instrucciones sobre cómo abordar el problema.

Manuales de estrategias y herramientas SOAR

Los manuales de estrategias también se utilizan con herramientas SOAR. Las herramientas SOAR son similares a las SIEM, ya que también se usan para el monitoreo de amenazas. SOAR es un programa informático utilizado para automatizar tareas repetitivas generadas por herramientas como las SIEM o la detección y respuesta administrada (MDR). Por ejemplo, si un/a usuario/a intentara iniciar sesión en su computadora demasiadas veces con la contraseña incorrecta, un SOAR bloquearía automáticamente su cuenta para detener una posible intrusión. Luego, los analistas consultarían el manual de estrategias para tomar medidas que permitan resolver el problema.

Marco de Gestión de Riesgo

Marco de gestión de riesgo por el nist

1. **Preparar:** Se refiere a las actividades necesarias para gestionar los riesgos de seguridad y privacidad antes de que ocurran una falla de seguridad
2. **Categorizar:** Sirve para desarrollar procesos y tareas de manejo de riesgos (se usan pensando en la confidencialidad integridad y disponibilidad de los sistemas e información pueden verse afectadas)
3. **Seleccionar :** Se refiere a elegir , personalizar y capturar la documentación de los controles que protegen una organización (ejemplo: actualizar un manual de procedimientos o gestionar otra documentación que te permita a ti y al equipo abordar los problemas de forma mas eficiente)
4. **Implementar :** Implementar planes de seguridad y privacidad para la organización , tener buenos planes es esencial para minimizar el impacto de riesgos de seguridad continuos . (ejemplo: si se nota un patrón de empleados que constantemente necesitan restablecer su password , implementar un cambio en los requisitos de contraseña para resolver este paso)
5. **Evaluar:** Se refiere a determinar si los controles establecidos se implementan correctamente , La organización siempre quiere operar con la máxima eficiencia posible, por eso tomarse el tiempo de analizar los protocolos , procedimientos y controles que se implementaron cumplen con las necesidades de la organización.
6. **Autorizar:** Significa ser responsable de los riesgos de seguridad y privacidad que pueden existir en una organización como analista este paso podría implicar generar informes, desarrollar planes de acción y establecer hitos del proyecto que estén alineados con los objetivos de seguridad de la organización.
7. **Monitorear :** Significa estar al tanto de como operan los sistemas, Evaluar y mantener las operaciones técnicas son tareas diarias de una enlista, Ver si los sistemas satisfacen los objetivos o pueden ser necesarios cambios.

Marcos

Marcos de seguridad

Los marcos de seguridad son pautas usadas para crear planes para mitigar riesgos y amenazas contra los datos y la privacidad como los ataques de ingenieria social y ransomware.

También incluye el espacio físico y virtual.

Ademas indican como prevenir o detecta y responder a las fallas de seguridad.

También existen para capacitar a los empleados contra ataques de ingeniera social.

Controles

Security controls : diseñados para reducir una brecha de seguridad diseñadas para reducir riesgos específicos.

De los cuales tenemos los 3 principales:

- Cifrado, autentificación y autorización:
 - Cifrado: es el proceso de convertir datos de un formato legible a uno codificado, suele convertir dato de texto plano a texto cifrado es un texto crudo el cual no puede ser decifrado hasta que se obtenga la clave ademas de proteger los datos sensibles (PII and PI).
 - Autentificación: El proceso de verificar quien hace algo, la forma básica de autentificación es usuario y contraseña
 - Biometricos: La identificación usando las características físicas para verificar la identidad de una persona(Ejemplos la huella dactilar, retinas, escaneo de palma).
 - El vishing es el aprovechamiento de la comunicación eléctrica de voz para obtener información sensible para hacerse pasar por una fuente conocida.
- Autorización es el concepto de conceder el conceder acceso a recursos específicos dentro del sistema. básicamente la autorización se utiliza que una persona tiene permiso para acceder a un recurso ademas se podrán obtener acceso mediante la deep web

Marcos del NIST

NIST cybersecurity Framework

El marco voluntario incluye estándares, pautas y mejores prácticas para manejar los riesgos de la ciberseguridad. Este marco es muy respetado y esencial para mantener la seguridad.

Consta de 5 Principales ramas

1. Identificar: que está relacionada con la gestión del riesgo de ciberseguridad y su efecto en las personas y activos de una organización .
2. Proteger: Es la estrategia utilizada para proteger una organización mediante la implementación de políticas, procedimientos, capacitaciones y herramientas que ayudan a mitigar las amenazas de ciberseguridad.
3. Detectar: Es identificar posibles incidentes de seguridad y mejorar las capacidades de monitoreo para aumentar la velocidad y la eficiencia de las detecciones.
4. Responder: Es tomar las medidas adecuadas para contener, neutralizar y analizar los incidentes de seguridad e implementar mejoras en el proceso de seguridad
5. Recuperar: Restaurar la operación normal de los sistemas afectados

Ventajas del framework:

que proporcionan pautas y orientaciones específicas a los profesionales de seguridad para prevenir riesgos y posibles vulnerabilidades

NIST SP 800-53

Ofrece un marco unificado para proteger los sistemas de información dentro del gobierno central de los EU

Sistema Web como herramienta de apoyo para el registro de asesoría

Más sobre los manuales de estrategias

Un manual de estrategia es una guía que brinda detalles sobre cualquier acción operativa. Basicamente proporciona una lista predefinida y actualizada de los pasos para responder a un incidente.

Siempre van acompañados de una estrategia que describe qué va a hacer cada miembro del equipo junto con las asignaciones de tareas

Los manuales de estrategia deben tratarse como documentos vivos o sea que se actualicen con frecuencia.

Los manuales se modifican cuando pasan estas cosas:

- Cuando se identifica una falla, como un descuido en las políticas y procedimientos descritos o en el manual en sí.
- Cuando hay un cambio en los estándares de la industria, por ejemplo, en las leyes o en el cumplimiento normativo.
- Cuando el panorama de la ciberseguridad cambia debido a la evolución de las tácticas y técnicas de los agentes de amenaza.

Manuales de respuesta a incidentes y vulnerabilidades

Los manuales de respuesta a incidentes y vulnerabilidades son ampliamente utilizados por profesionales de ciberseguridad de nivel inicial. Se desarrollan en función de los objetivos descritos en el plan de continuidad empresarial de una organización, que permite a una empresa recuperarse y continuar operando con normalidad. Estos manuales contienen listas predefinidas y actualizadas de pasos para responder a un incidente, garantizando el cumplimiento de estándares y protocolos legales y organizativos. Además, ayudan a minimizar errores y asegurar que las acciones importantes se realicen en un plazo determinado. Seguir estos pasos es fundamental para los profesionales de la seguridad, ya que contribuyen a la normalización de operaciones tras una interrupción como una fuga de información.

Cuando un incidente, amenaza o vulnerabilidad ocurre o se identifica, el nivel de riesgo para la organización depende del daño potencial a sus activos. Una fórmula básica para determinar el nivel de riesgo es que el riesgo es igual a la probabilidad de una amenaza.

Por esta razón, actuar rápido es fundamental. Si se lleva a cabo alguna tarea forense, también es importante seguir los pasos descritos en los manuales de estrategias, porque un mal manejo puede comprometer fácilmente estos datos y hacerlos inutilizables. Los pasos comunes incluidos en los manuales de respuesta a incidentes y vulnerabilidades incluyen:

- Preparación
- Detección
- Análisis
- Contención
- Erradicación
- Recuperación ante un incidente

Los pasos adicionales incluyen la realización de actividades posteriores al incidente y una coordinación de esfuerzos, a lo largo de las etapas de investigación y respuesta a incidentes y vulnerabilidades.

Conclusiones clave

Fase Preparacion:

Antes de que se produzcan incidentes, mitiga los impactos potenciales en la organización documentando, estableciendo planes de dotación de personal y educando a los usuarios.

Fase

Detección y análisis

Detecta y analiza eventos mediante la implementación de procesos definidos y la tecnología adecuada.

Fase

Contención

Previene daños mayores y reduce el impacto inmediato de los incidentes.

Fase

Erradicación y recuperación

Elimina completamente los artefactos del incidente para que una organización pueda volver a operar con normalidad.

Fase

Actividad posterior a un incidente

Documenta el incidente, informa a la dirección de la organización y aplica las lecciones aprendidas.

Fase

Coordinación

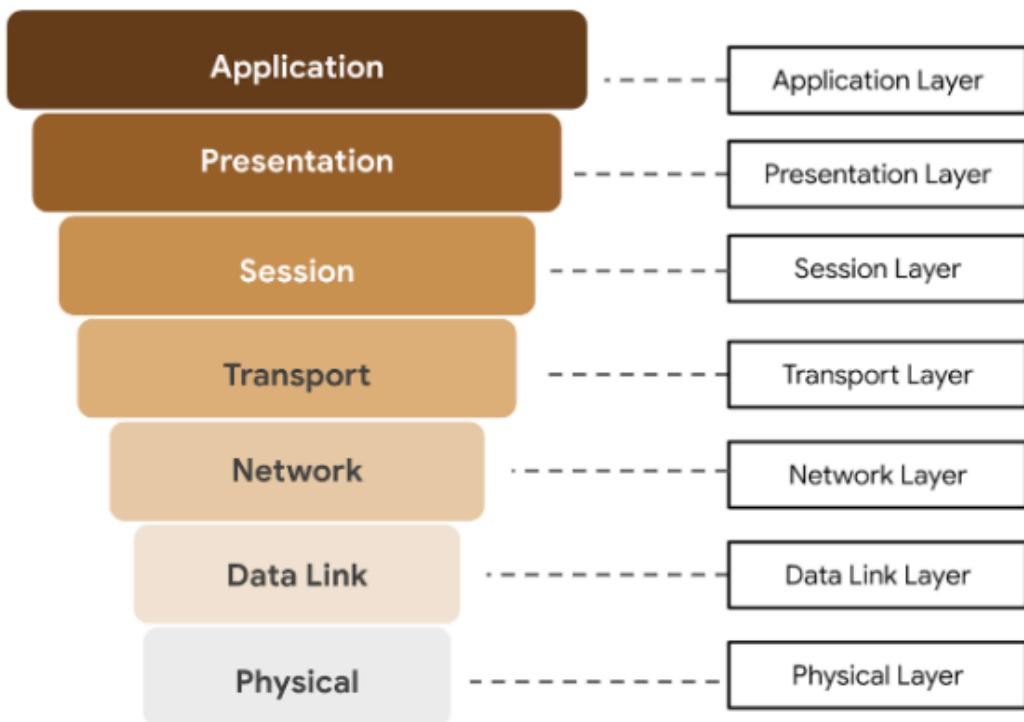
Notifica los incidentes y comparte información durante todo el proceso de respuesta, de acuerdo con los estándares establecidos.

Modelo OSI

Comparación entre el modelo TCP/IP y el modelo OSI

El modelo osi es un concepto estandarizado que describe las siete capas que las computadoras utilizan para comunicarse y enviar datos atreves de la red. Los profesionales de la seguridad suelen utilizarlo para comunicarse entre si sobre las posibles fuentes de problemas o amenazas de seguridad.

OSI Model



Capas del modelo osi

Capa 7: Capa de aplicación

La capa de aplicación incluye procesos que involucran directamente al/a la usuario/a cotidiano/a. Esta capa incluye todos los protocolos de red que las aplicaciones de software utilizan para conectarlo/a a Internet. Esta característica es la que identifica a la capa de aplicación: conexión de usuarios/as a la red a través de aplicaciones y solicitudes.

Un ejemplo de un tipo de comunicación que ocurre en la capa de aplicación es el uso de un navegador web. El navegador de Internet utiliza HTTP o HTTPS para enviar y recibir información del servidor del sitio web. La aplicación de correo electrónico utiliza el protocolo simple de transferencia de correo (SMTP) para transmitir información de correo electrónico. Además, los navegadores web utilizan el protocolo del sistema de nombres de dominio (DNS) para traducir los nombres de dominio del sitio web en direcciones IP, que identifican el servidor web que aloja la información del sitio.

Capa 6: Capa de presentación

Las funciones en la capa de presentación incluyen la traducción de datos y el cifrado para la red. Esta capa agrega y reemplaza datos con formatos que pueden ser entendidos por las aplicaciones (capa 7), en los sistemas de envío y recepción. Los formatos que están más cerca del usuario final, es decir, donde se encuentra la aplicación o dispositivo que utiliza

el/la usuario/a para interactuar con la red o recibir información, pueden ser diferentes de los del sistema receptor. Los procesos en la capa de presentación requieren el uso de un formato estandarizado.

Algunas funciones de formateo que se producen en la capa 6 incluyen cifrado, compresión y confirmación de que el conjunto de caracteres puede ser interpretado en el sistema receptor. Un ejemplo de cifrado que se da en esta capa es SSL, que cifra los datos entre los servidores web y los navegadores como parte de sitios web con HTTPS.

Capa 5: Capa de sesión

Una sesión indica cuando se establece una conexión entre dos dispositivos. Una sesión abierta permite que los dispositivos se comuniquen entre sí. El objetivo de los protocolos de la capa de sesión es mantener la sesión abierta mientras se transfieren datos y cerrarla una vez que se completa la transmisión.

La capa de sesión también es responsable de actividades como la autenticación, reconexión y establecimiento de puntos de control durante una transferencia de datos. Si la sesión se interrumpe, los puntos de control aseguran que, cuando se restablece la conexión, la transmisión se retome desde el último punto de control de la sesión. Las sesiones incluyen una solicitud y respuesta entre aplicaciones. Las funciones en la capa de sesión responden a solicitudes de servicio de procesos en la capa de presentación (capa 6) y envían solicitudes de servicios a la capa de transporte (capa 4).

Capa 4: Capa de transporte

La capa de transporte es la responsable de enviar datos entre dispositivos. Además, esta capa maneja la velocidad y el flujo de transferencia, y divide los datos en segmentos más pequeños para facilitar el envío. La segmentación es el proceso de dividir una gran transmisión de datos en piezas más pequeñas que puedan ser procesadas por el sistema receptor. Para que se puedan procesar en la capa de sesión (capa 5), estos segmentos tienen que volverse a ensamblar en su destino. La velocidad y la tasa de transmisión también tienen que coincidir con la velocidad de conexión del sistema de destino. TCP y UDP son protocolos de capa de transporte.

Capa 3: Capa de red

La capa de red supervisa la recepción de los paquetes desde la capa de enlace de datos (capa 2) y las entrega al destino previsto. El destino previsto puede encontrarse en función de la dirección que reside en el marco de los paquetes de datos. Estos paquetes incluyen direcciones IP, que indican a los routers dónde enviarlos y se enrutan desde la red de envío hacia la red de recepción.

Capa 2: Capa de enlace de datos

La capa de enlace de datos organiza el envío y la recepción de paquetes de datos dentro de una sola red. Esta capa incluye los switches en la red local y las tarjetas de interfaz de red en los dispositivos locales.

En la capa de enlace de datos se utilizan protocolos como el protocolo de control de red (NCP), el control de enlace de datos de alto nivel (HDLC) y el protocolo de control de enlace de datos sincrónico (SDLC).

Capa 1: Capa física

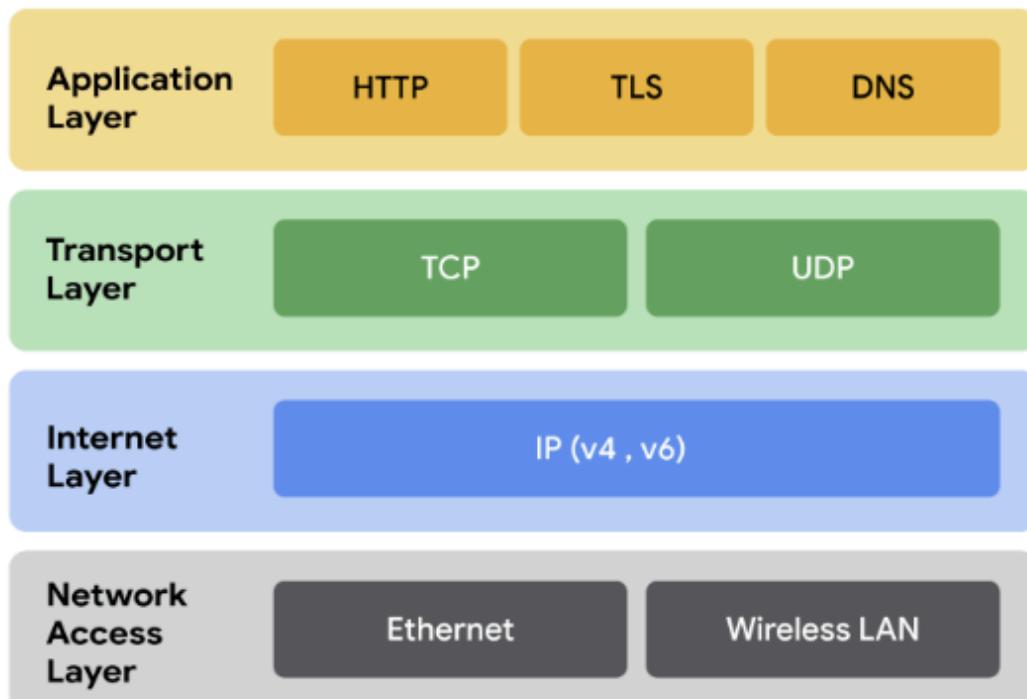
Como su nombre lo indica, la capa física corresponde al hardware físico utilizado en la transmisión de la red. Los hubs, los módems y el cableado que los conecta se consideran parte de esta capa. Para viajar a través de un cable Ethernet o coaxial, un paquete de datos debe ser traducido en una secuencia de ceros y unos, que se envía a través de los cables y conexiones físicas, se recibe y, luego, pasa a los niveles superiores del modelo OSI.

Modelo TCP/IP

Le modelo TCP/ip TPC significa (Transmission Control Protocol) es un marco utilizado para visualizar como se organizan y trasmitten los datos a través de una red esta mediante protocolos de red.

Los protocolos de red son un lenguaje que los sistemas utilizan para comunicarse entre si. Para que 2 sistemas de red se comuniquen con éxito, deben usar el mismo protocolo. Los mas comunes son TCP/IP y OSI

EL modelo TCP/IP tiene cuatro capas : acceso a la red , De internet , de transporte y de aplicación las cuales se pueden usar para saber donde ocurrió el ataque



Capas de acceso a la red

La capa de acceso a la red, llamada enlace de datos, organiza el envío y la recepción de paquetes de datos dentro de una sola red. Esta corresponde a la parte física de una red, por ejemplo (hubs, módems, cables y cableado se consideran parte de esta capa). El protocolo de resolución de direcciones ARP, por sus siglas en inglés, también forma parte de la capa de acceso a red. Esto es lo que ayuda a la IP a dirigir los paquetes y mapear direcciones IP a direcciones MAC en la misma red física.

Capa de Internet

También denominada capa de RED, es responsable de garantizar la entrega al host de destino que potencialmente puede residir en una red diferente. La capa de Internet determina qué protocolo es el encargado de entregar los paquetes de datos, como por ejemplo:

- Protocolo de internet IP: envía los paquetes de datos al destino correcto y se basa en el protocolo de control de transmisión/protocolo de datagramas de usuario (TCP/UDP) para entregarlo al servicio correspondiente. Los paquetes de IP posibilitan la comunicación entre 2 redes, ya que se enrutan desde la red origen hasta la de destino.
- Protocolo de mensajes de control de internet (ICMP)

Comparte información de errores y actualizaciones de estado de los paquetes de datos. Resulta útil para detectar y solucionar errores de red y además informa sobre paquetes que fueron descartados o desaparecieron durante el tránsito, problemas de conectividad de red y paquetes redirigidos a otros enrutadores.

Capa de transporte

Es responsable de entregar datos de manera confiable entre dos sistemas y redes. El protocolo de control de transmisión TCP y el de datagramas de usuario UDP son los protocolos que producen en esta capa

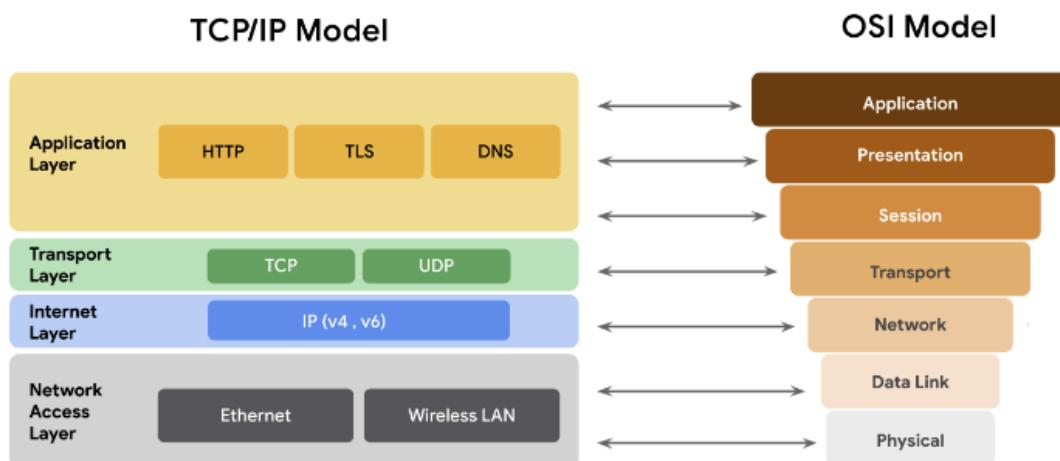
- Protocolo de control de transmisión (TCP)
 - El TCP garantiza que los datos se transmitan de forma segura al servicio de destino. Contiene el número de puerto del servicio de destino preciso, que reside en el encabezado de TCP de un paquete TCP/IP
- Protocolo de datagramas de usuario (UDP)
 - Las aplicaciones que no están afectadas por la confiabilidad de la transmisión usan el protocolo UDP. Los datos enviados a través de UDP no son un objeto de seguimiento tan exhaustivo como los enviados mediante TCP. Debido a que UDP no establece conexiones de red, se utiliza principalmente en aplicaciones sensibles al rendimiento que operan en tiempo real, como la transmisión de video.

Capa de aplicación

La capa de aplicaciones en el modelo TCP/IP es similar a las capas de aplicación, presentación y sesión del modelo OSI. Es la responsable de realizar solicitudes de red o de responder solicitudes. Además, esta capa define a qué servicios y aplicaciones de internet puede acceder cualquier usuario. Algunos de los protocolos más usados son:

- Protocolo de transferencia de hipertexto (HTTP)
- Protocolo simple de transferencia de correo (SMTP)
- Secure Shell o shell Seguro (SSH)
- Protocolo de transferencia de archivos (FTP)
- Sistema de nombres de dominio (DNS)

Comparación del modelo TCP/IP con el modelo OSI



Monitoreo de seguridad con herramientas de detección

Telemetría : Es la recopilación y transmisión de datos para el análisis. Mientras los registros realizan un inventario de eventos en sistemas, la telemetría describe los datos en sí.

IDS : es una aplicación que vigila la actividad y avisa de posibles intrusiones.

Un sistema de detección de intrusos basado en host : Para aclarar, un host es un dispositivo que se comunica con otros en una red, similar a un punto de conexión. Este tipo de sistema de detección se instala como un agente en un único host, como un equipo, laptop o servidor. Dependiendo de su configuración, los sistemas de detección

basados en host controlan el host en el que han sido instalados para detectar actividad sospechosa.

Un sistema de detección basado en red: Los sistemas de detección de intrusiones basados en la red funcionan como los rastreadores de paquetes, pues analizan tráfico y datos de red en un punto específico de la red.

Más información sobre filtros con AND, OR y NOT

Operadores lógicos

AND, **OR** y **NOT** te permiten filtrar las consultas para obtener información específica que te ayudará en tu trabajo como analista de seguridad. Todos ellos se consideran operadores lógicos.

AND (y)

En primer lugar, **AND** se usa para filtrar por dos condiciones. **AND** especifica que se deben satisfacer ambas condiciones de manera simultánea.

A modo de ejemplo, una inquietud de ciberseguridad puede afectar solo a aquellas cuentas de clientes que cumplen la condición de ser gestionadas por un/a representante de soporte con una ID de 5 y la condición de estar ubicadas en EE.UU. Para encontrar los nombres y correos electrónicos de esos/as clientes específicos/as, debes colocar las dos condiciones a cada lado del operador **AND** en la cláusula **WHERE**:

```
1  SELECT firstname, lastname, email, country, supportrepid
2  FROM customers
3  WHERE supportrepid = 5 AND country = 'USA';
```

Ejecutar

Restablecer

FirstName	LastName	Email	Country	SupportRepId
Jack	Smith	jacksmith@microsoft.com	USA	5
Kathy	Chase	kachase@hotmail.com	USA	5
Victor	Stevens	vstevens@yahoo.com	USA	5
Julia	Barnett	jubarnett@gmail.com	USA	5

OR (o)

El operador **OR** también vincula dos condiciones, pero **OR** especifica que se puede satisfacer cualquiera de las dos. Este devuelve resultados que satisfacen la primera condición, la segunda condición o ambas.

Por ejemplo, si eres responsable de encontrar a todos/as los/las clientes que se encuentran en EE.UU. o Canadá para informarles sobre una actualización de seguridad, puedes usar un operador **OR** para buscar todos los registros necesarios. Como lo demuestra la consulta siguiente, puedes colocar dos condiciones a cada lado del operador **OR** en la cláusula

WHERE:

```
1  SELECT firstname, lastname, email, country
2  FROM customers
3  WHERE country = 'Canada' OR country = 'USA';
```

Ejecutar

Restablecer

La consulta devuelve a todos los clientes que se encuentran en EE.UU. o en Canadá.

Nota: Incluso si ambas condiciones se encuentran en la misma columna, debes escribir las dos completas. Por ejemplo, la consulta del ejemplo anterior contiene el filtro `WHERE country = 'Canada' OR country = 'USA'`.

NOT (no)

A diferencia de los dos operadores anteriores, el operador **NOT** solo funciona con una sola condición y no con varias. El operador **NOT** niega una condición. Esto significa que SQL devuelve todos los registros que no coinciden con la condición especificada en la consulta.

Por ejemplo, si un problema de ciberseguridad no afecta a clientes en EE.UU. pero puede afectar a clientes en otros países, puedes obtener como resultado todos/as los/las clientes que no se encuentren en EE.UU. Esto resulta más eficiente que crear condiciones individuales para todos los demás países. Para usar el operador **NOT** en esta tarea, escribe la siguiente consulta y escribe **NOT** directamente después de **WHERE**:

```
1  SELECT firstname, lastname, email, country
2  FROM customers
3  WHERE NOT country = 'USA';
```

Combinación de operadores lógicos

Los operadores lógicos se pueden combinar en filtros. Por ejemplo, si sabes que tanto EE.UU. como Canadá no se vieron afectados por un incidente de ciberseguridad, puedes combinar operadores para obtener clientes en todos los países excepto estos dos. En la consulta siguiente, **NOT** se coloca antes de la primera condición, se combina con una segunda condición con **AND** y luego también se coloca **NOT** antes de esa segunda condición. Puedes ejecutarla para revisar los resultados:

```
1  SELECT firstname, lastname, email, country
2  FROM customers
3  WHERE NOT country = 'Canada' AND NOT country = 'USA';
```

Ejecutar

Restablecer

Métodos de búsqueda con herramientas SIEM

Anteriormente, aprendiste a usar las **herramientas de gestión de eventos e información de seguridad (SIEM)** para detectar eventos de seguridad, como intentos fallidos de inicio de sesión. SIEM es una aplicación que recopila y analiza datos de registro para monitorear actividades críticas en una organización. En esta lectura, verás cómo herramientas SIEM, como Splunk y Chronicle, utilizan diferentes métodos de búsqueda para encontrar, filtrar y transformar los resultados de búsqueda.

No todas las organizaciones utilizan la misma herramienta SIEM para recopilar y centralizar sus datos de seguridad, por lo cual tendrás que aprender a usar varias de ellas. Entender los diferentes tipos de búsquedas que puedes llevar a cabo con estas herramientas es muy importante para encontrar datos de eventos relevantes que respalden tus investigaciones de seguridad.

Búsquedas de Splunk

Como has aprendido, Splunk tiene su propio lenguaje de consulta, denominado **Search Processing Language (SPL)** (lenguaje de procesamiento de búsqueda) que se utiliza para buscar y recuperar eventos de índices mediante la aplicación de búsqueda e informes de la herramienta. Una búsqueda SPL puede contener muchos comandos y argumentos diferentes. Por ejemplo, puedes usar comandos para transformar los resultados de búsqueda en un formato de gráfico o filtrar los resultados para obtener información específica.

The screenshot shows the Splunk Cloud interface. At the top, there's a navigation bar with links for 'splunk>cloud', 'Apps', 'Messages' (with 2 notifications), 'Settings', 'Activity', and a search bar. On the right, it shows 'Splunk Cloud Admin' and a help icon. Below the navigation is a secondary menu with 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. To the right of this is a green arrow icon followed by 'Search & Reporting'. The main area is titled 'Search' and has a search bar with placeholder 'enter search here...'. It also includes filters for 'Last 24 hours', 'standard_perf (search default)', and 'Smart Mode'. A section titled 'How to Search' provides basic instructions, and another titled 'Analyze Your Data with Table Views' explains Table Views and how to create them. Buttons for 'Documentation' and 'Tutorial' are also present.

Este es un ejemplo de una búsqueda SPL básica que está consultando un índice para un evento fallido:

index=main fail

- **index=main**: Es el comienzo del comando de búsqueda que le dice a Splunk que recupere eventos de un **index** (índice) llamado **main**.
- **fail**: Es el término de búsqueda. Le dice a Splunk que devuelva los eventos que contengan el término **fail**.

Saber cómo usar el SPL de manera efectiva tiene muchos beneficios. Ayuda a acortar el tiempo que se tarda en devolver los resultados de búsqueda y también a obtener los resultados exactos que necesitas de varias fuentes de datos. El SPL admite muchos tipos diferentes de búsquedas que no se incluyen en esta lectura. Si quieres conocer más sobre SPL, puedes consultar la [Referencia de búsqueda de Splunk](#).

Pipe

Es posible que ya conozcas cómo se utiliza el comando pipe en Bash de Linux. A modo de repaso, el comando pipe envía la salida de un comando como entrada a otro comando. SPL también utiliza la barra vertical o pleca | para separar los comandos individuales en la búsqueda y para encadenar comandos juntos, de forma tal que la salida de un comando se combine en el siguiente comando. Esto es útil porque te permite refinar los datos de varias maneras para obtener los resultados que necesitas, con un solo comando.

Aquí podrás observar un ejemplo de dos comandos separados por una pleca:

index=main fail| chart count by host

- **index=main fail**: Es el comienzo del comando de búsqueda que le dice a Splunk que recupere eventos de un **index** (índice) llamado **main** para eventos que contienen el término de búsqueda **fail**.
- **|**: La pleca separa y encadena los dos comandos **index=main** y **chart count by host**. Esto significa que la salida del primer comando *index=main* se usa como la entrada del segundo comando **chart count by host**.

- **chart count by host:** Este comando le dice a Splunk que transforme los resultados de búsqueda creando un **chart** (gráfico) de acuerdo con el **count** (recuento) o la cantidad de eventos. El argumento **by host** le dice a Splunk que enumere los eventos por host, que son los nombres de los dispositivos de los que provienen los eventos. Este comando puede ser útil para identificar hosts con recuentos excesivos de errores en un entorno.

Comodín

El **comodín** es un carácter especial que se puede sustituir por cualquier otro. Se suele simbolizar con un carácter de asterisco *. Los comodines coinciden con los caracteres en los valores de una cadena. En Splunk, el comodín que uses depende del comando con el que lo estés usando. Los comodines son útiles porque pueden ayudar a encontrar eventos que contienen datos similares, pero no completamente idénticos. A continuación, verás un ejemplo de uso de un comodín para expandir los resultados de búsqueda de un término de búsqueda:

index=main fail*

- **index=main:** Este comando recupera eventos de un **index** (índice) llamado **main**.
- **fail*:** El comodín después de **fail** representa cualquier carácter. Le dice a Splunk que busque todas las terminaciones posibles que contengan el término **fail**. Esto expande los resultados de búsqueda y devolverá eventos que contengan el término **fail**, como "failed" o "failure".

Consejo profesional: Las comillas dobles se utilizan para especificar la búsqueda de una frase o cadena exacta. Por ejemplo, si solo quieres buscar eventos que contengan la frase exacta **login failure** (error de inicio de sesión), puedes colocar la frase entre comillas dobles "**login failure**". Esta búsqueda coincidirá solo con eventos que contengan la frase exacta **login failure** y no con otros eventos que contengan las palabras **failure** o **login** por separado.

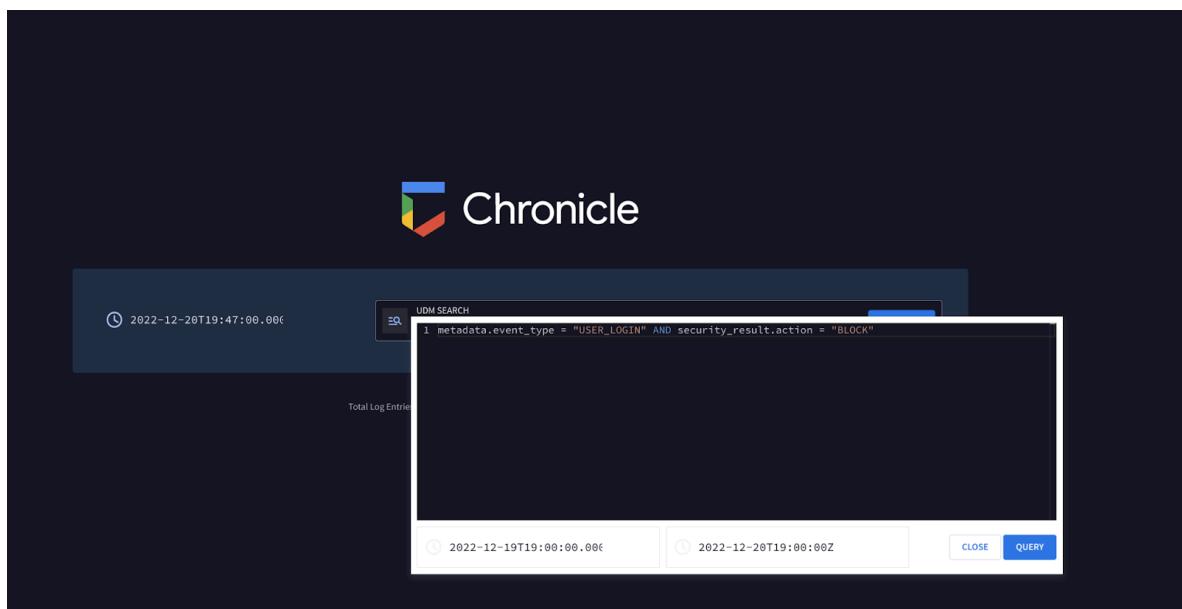
Búsquedas en Chronicle

En Chronicle, puedes buscar eventos en el campo Search (Buscar) y, además, utilizar el menú Procedural Filtering (proceso de filtrado) para aplicar filtros y refinar aún más los resultados de búsqueda. Por ejemplo, puedes usarlo para incluir o excluir resultados de búsqueda que contengan información específica relacionada a un tipo de evento o una fuente de registro. Hay dos tipos de búsqueda que puedes realizar para encontrar eventos en Chronicle: una búsqueda de modelos de datos unificados (UDM) o una búsqueda de registro sin procesar.



Búsqueda de modelos de datos unificados (UDM)

Es el tipo de búsqueda predeterminado que se utiliza en Chronicle. Para hacer una búsqueda UDM, debes escribir lo que quieras buscar, hacer clic en "Search" (Buscar) y seleccionar "UDM Search" (Búsqueda UDM). Con este tipo de búsqueda, Chronicle busca datos de seguridad que se hayan ingerido, analizado y normalizado. Una búsqueda UDM recupera los resultados de búsqueda más rápido que una búsqueda de registro sin procesar, porque busca en datos indexados y estructurados que están normalizados en UDM.



Una búsqueda UDM recupera eventos formateados en UDM, que contienen campos UDM. Hay muchos tipos diferentes de campos UDM que se pueden usar para consultar información específica de un evento. En esta lectura no los analizaremos todos, pero si deseas obtener más información, puedes consultar la [lista de campos UDM de Chronicle](#).

Todos los eventos UDM contienen un conjunto de campos comunes que incluyen:

- **Entidades:** Se las conoce también como sustantivos. Todos los eventos UDM deben contener al menos una entidad. Este campo brinda contexto adicional sobre un dispositivo, usuario o proceso que está involucrado en un evento. Por ejemplo, un evento UDM que contiene información de entidad incluye los detalles del origen de un evento, como el nombre de host, el nombre de usuario y la dirección IP del evento.

- **Metadatos del evento:** Brinda una descripción básica de un evento, incluidos el tipo de evento, las marcas de tiempo y demás.
- **Metadatos de red:** Proporciona información sobre eventos relacionados con la red y detalles del protocolo.
- **Resultados de seguridad:** Indica el resultado relacionado con la seguridad de los eventos. Un ejemplo de un resultado de seguridad puede ser un software antivirus que detecta y pone en cuarentena un archivo malicioso e informa: "virus detectado y en cuarentena".

A continuación, podrás ver un ejemplo de una búsqueda UDM simple que utiliza el campo de metadatos de eventos para localizar eventos relacionados con los inicios de sesión de los usuarios:

metadata.event_type = "USER_LOGIN"

- **metadata.event_type = "USER_LOGIN":** El campo UDM **metadata.event_type** contiene información sobre el tipo del evento. Esto incluye información como marca de tiempo, conexión de red, autenticación de usuario y demás. Aquí, el tipo de evento especifica **USER_LOGIN**, que busca eventos relacionados con la autenticación.

Si usas solo campos de metadatos, puedes comenzar rápidamente a buscar eventos.

Mientras sigues practicando la búsqueda en Chronicle con UDM Search, irás encontrando más campos. Prueba usar estos campos para realizar búsquedas específicas con el fin de localizar diferentes eventos.

Búsqueda de registros sin procesar

Si no puedes encontrar la información que necesitas en los datos normalizados, puedes usar una búsqueda de registros sin procesar, que te permitirá buscar en los registros sin analizar. Para realizar una búsqueda de registros sin procesar, deberás escribir lo que quieras buscar, hacer clic en "Search" (Buscar) y seleccionar "Raw Log Search" (Búsqueda de registro sin procesar). Buscar en registros sin procesar, lleva más tiempo que una búsqueda estructurada. En el campo Search (Buscar), puedes hacer una búsqueda de registro sin procesar si especificas información, como nombres de usuario, nombres de archivo, hashes y demás. Chronicle recuperará los eventos asociados con la búsqueda.

Consejo profesional: La búsqueda de registro sin procesar admite el uso de expresiones regulares, lo que puede ayudarte a acotar una búsqueda para que coincida con patrones específicos.

Conclusiones clave

Las herramientas SIEM, como Splunk y Chronicle, tienen sus propios métodos para buscar y recuperar datos de eventos. Como analista de seguridad, es importante comprender cómo aprovechar estas herramientas, para encontrar la información que necesitas de manera rápida y eficiente. Esto te permitirá explorar los datos para detectar amenazas y responder rápidamente a los incidentes de seguridad.

Recursos para obtener más información

Si deseas obtener más información sobre la búsqueda de eventos con Splunk y Chronicle, puedes consultar los siguientes recursos:

- [Manual de búsqueda de Splunk](#) sobre cómo utilizar el lenguaje de procesamiento de búsqueda Splunk (SPL)
- [Guía de inicio rápido de Chronicle](#) sobre los diferentes tipos de búsquedas

Marcar como completo

Me gusta

No me gusta

Informar de un problema

Métodos de detección de incidentes de ciberseguridad

Métodos de detección

Durante la **fase de detección y análisis** del ciclo de vida de respuesta a incidentes, los equipos de seguridad reciben una notificación de un posible incidente y trabajan para investigarlo y verificarlo mediante la recopilación y el análisis de datos. Como recordatorio, la **detección** es el descubrimiento rápido de eventos de seguridad, y el **análisis** implica la investigación y validación de alertas.

Como has aprendido, un sistema de detección de intrusiones (IDS) puede detectar posibles intrusiones y enviar alertas a los analistas de seguridad para que investiguen la actividad sospechosa. Estos, además, pueden utilizar las herramientas de gestión de eventos e información de seguridad (SIEM) para detectar, recopilar y analizar datos de seguridad.

También has aprendido que la detección presenta desafíos. Incluso los mejores equipos de seguridad pueden no detectar amenazas reales por distintas razones. Por ejemplo, las herramientas de detección pueden encontrar únicamente aquello que los equipos de seguridad han configurado para que monitorean. Si no están configuradas correctamente, es posible que no identifiquen actividades sospechosas, y que los sistemas queden vulnerables a ataques. Por esto, es importante que los equipos de seguridad utilicen métodos adicionales de detección para aumentar su cobertura y precisión.

Caza de amenazas

Las amenazas evolucionan y los atacantes avanzan en sus tácticas y técnicas. La detección automatizada y basada en la tecnología puede resultar insuficiente a la hora de mantenerse al día con el panorama de amenazas en constante evolución. La detección impulsada por el ser humano, como la caza de amenazas, combina el poder de la

tecnología con un elemento humano para así descubrir amenazas ocultas que las herramientas de detección no logran captar.

La caza de amenazas es la búsqueda proactiva de amenazas en una red. Los profesionales de la seguridad la utilizan para descubrir actividades maliciosas que no fueron identificadas por las herramientas de detección y como una forma de llevar a cabo un análisis más detallado de las detecciones. También se utiliza para detectar amenazas antes de que occasionen daños. Por ejemplo, para las herramientas de detección es difícil identificar el malware sin archivos. Esta es una forma de software malicioso que utiliza técnicas sofisticadas de evasión, como esconderse en la memoria en lugar de usar archivos o aplicaciones, lo que le permite eludir los métodos tradicionales de detección, como el análisis de firmas. La caza de amenazas utiliza la combinación de análisis humano activo y tecnología para identificar amenazas como el malware sin archivos.

Nota: Los especialistas en caza de amenazas son conocidos como cazadores de amenazas. Los cazadores de amenazas investigan amenazas y ataques emergentes y luego determinan la probabilidad de que una organización sea vulnerable a un ataque en particular. Para lograrlo, utilizan una combinación de inteligencia sobre amenazas, indicadores de compromiso, indicadores de ataque y aprendizaje automático para buscar amenazas en una organización.

Inteligencia sobre amenazas

Las organizaciones pueden mejorar sus capacidades de detección si están al tanto del panorama de amenazas en evolución y comprenden la relación entre su entorno y los agentes de amenaza. Para conocer mejor las amenazas se utiliza la **inteligencia sobre amenazas**, que consiste en información basada en evidencia que proporciona contexto acerca de amenazas existentes o emergentes.

La inteligencia sobre amenazas puede provenir de fuentes privadas o públicas como las siguientes:

- **Informes de la industria:** Estos, a menudo, incluyen detalles sobre las tácticas, técnicas y procedimientos (TTP) del atacante.
- **Avisos gubernamentales:** Al igual que los informes de la industria, los avisos gubernamentales ofrecen información sobre los TTP de los atacantes.
- **Fuentes de datos de amenazas:** Proporcionan información relacionada con amenazas, la cual puede utilizarse como protección contra atacantes sofisticados, como las **amenazas persistentes avanzadas (APT)**. Las APT son instancias en las que un agente de amenaza mantiene acceso no autorizado a un sistema durante un período prolongado de tiempo. Los datos suelen ser una lista de indicadores, como direcciones IP, dominios y hashes de archivos.

Nota: Las fuentes de datos de inteligencia de amenazas son importantes para agregar contexto a las detecciones, aunque no deben ser lo único que consideres a la hora de detectar y es necesario evaluarlas antes de ser utilizadas en una organización.

Ciberengaño

Se denomina ciberengaño a las técnicas que engañan deliberadamente a los agentes de amenaza con el objetivo de aumentar la detección y mejorar las estrategias defensivas. Los **honeypots** (sistemas trampa o señuelos) son un ejemplo de un mecanismo activo de defensa cibernética que utiliza tecnología del engaño. Los honeypots son sistemas o recursos que se crean como señuelos vulnerables a ataques con el propósito de atraer posibles intrusos. Por ejemplo, se puede tener un archivo falso con la etiqueta *Información de tarjetas de crédito de clientes - 2022* para engañar a los agentes de amenaza y que estos accedan al archivo porque parece legítimo. Una vez que un agente de amenaza intenta acceder a este archivo, los equipos de seguridad son alertados.

Conclusiones clave

Se pueden implementar diversos métodos de detección para identificar y localizar eventos de seguridad en un entorno. Es esencial que las organizaciones utilicen una gran variedad de métodos, herramientas y tecnologías de detección para adaptarse a un panorama de amenazas en constante evolución, y proteger mejor los activos.

Recursos para obtener información adicional

Si deseas explorar más sobre la caza de amenazas y la inteligencia sobre amenazas, puedes acudir a recursos como los siguientes:

- Un [repositorio informativo sobre la caza de amenazas](#) del Proyecto ThreatHunting
- Investigación sobre [hackers patrocinados por el estado](#) realizada por el Grupo de Análisis de Amenazas (TAG)

Métodos para el escaneo de vulnerabilidades

¿Qué es un escáner de vulnerabilidades?

Un **escáner de vulnerabilidades** es un software que compara automáticamente las vulnerabilidades y exposiciones conocidas con las tecnologías de la red. En general, estas herramientas analizan los sistemas para encontrar configuraciones erróneas o fallas de programación.

1. **Capa perimetral**, como los sistemas de autenticación que validan el acceso del usuario.
2. **Capa de red**, que se compone de tecnologías como firewalls de red y otros.
3. **Capa de punto de conexión (endpoint)**, que describe los dispositivos en una red, como computadoras portátiles yde escritorio o servidores.
4. **Capa de aplicación**, que involucra el software con el que interactúan los usuarios.
5. **Capa de datos**, que incluye cualquier información almacenada, en tránsito o en uso.

Realización de escaneos

Los escáneres de vulnerabilidad no son intrusivos. Es decir, no rompen ni se aprovechan de un sistema como lo haría un atacante, sino que simplemente escanean una superficie y te alertan sobre cualquier puerta potencialmente desbloqueada en tus sistemas.

Nota: Si bien los escáneres de vulnerabilidades no son intrusivos, existen casos en los que un análisis puede causar problemas inadvertidamente, como colapsar un sistema.

Existen varias maneras de utilizar estas herramientas para escanear una superficie. Cada una contempla uno de los caminos posibles que un agente de amenaza podría tomar. A continuación, puedes explorar cada tipo de escaneo para obtener una imagen más clara de esto.

Externo versus interno

Los escaneos externos e internos simulan la estrategia de un atacante.

Los *escaneos externos* prueban la capa perimetral fuera de la red interna. Analizan sistemas externos, como sitios web y cortafuegos (firewalls). Este tipo de análisis puede descubrir, por ejemplo, puertos de red o servidores vulnerables.

Los *escaneos internos* comienzan desde el extremo opuesto, ya que examinan los sistemas internos de una organización. Por ejemplo, este tipo de escaneo podría analizar software de aplicación, en busca de debilidades en la manera en que gestiona las entradas de usuarios.

Autenticado versus no autenticado

Los escaneos autenticados y no autenticados simulan si un usuario tiene o no acceso a un sistema.

Los *escaneos autenticados* pueden testear un sistema iniciando sesión con una cuenta de usuario real o incluso con una cuenta de administrador. Estas cuentas de servicio se utilizan para verificar vulnerabilidades, como controles de acceso rotos.

Los *análisis no autenticados* simulan agentes de amenaza externos que no tienen acceso a los recursos de tu empresa. Por ejemplo, un escaneo podría analizar los recursos compartidos de archivos dentro de la organización que se utilizan para alojar documentos internos solamente. Los usuarios no autenticados deberían recibir resultados de "acceso denegado" si intentan abrir estos archivos. Si es posible acceder a un archivo, se identificará una vulnerabilidad.

Limitado versus completo

Los escaneos limitados y completos se centran en dispositivos particulares a los que acceden usuarios internos y externos.

Los *escaneos limitados* analizan dispositivos particulares en una red, como la búsqueda de configuraciones erróneas en un firewall.

Los *análisis exhaustivos* analizan todos los dispositivos conectados a una red. Esto incluye sistemas operativos, bases de datos de usuarios y más.

Consejo profesional: antes de los escaneos limitados o completos debe realizarse un escaneo de descubrimiento. Este se utiliza para conocer las computadoras, dispositivos y

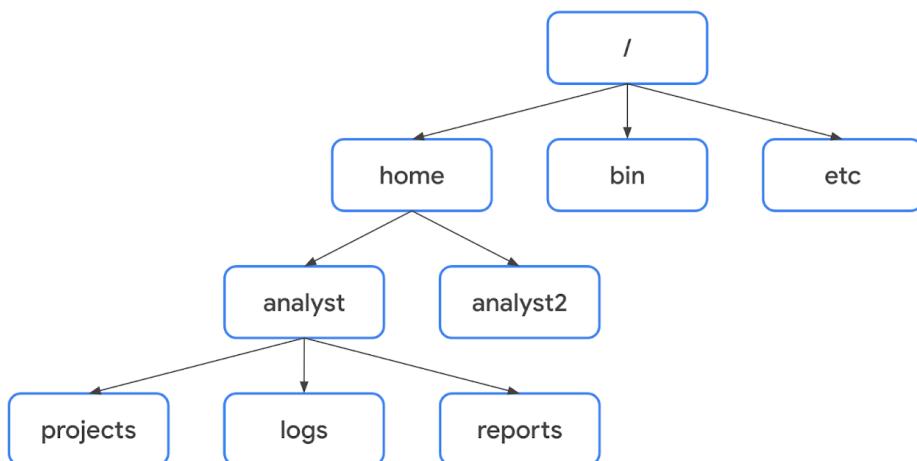
puertos abiertos que se encuentran en una red.

Navega por linux

Estándar de jerarquía del sistema de archivos (FHS)

Anteriormente, aprendiste que el **estándar de jerarquía del sistema de archivos (FHS)** es el componente de Linux que organiza los datos. El FHS es importante porque define cómo se organizan los directorios, el contenido de estos y otros tipos de almacenamiento en el sistema operativo.

Este diagrama ilustra la jerarquía de relaciones según el FHS:



Según el FHS, la ubicación de un archivo puede ser descrita por una ruta de archivo. Una **ruta de archivo** es la ubicación de un archivo o directorio. En la ruta del archivo, los diversos niveles de la jerarquía están separados por una barra (/).

Directorio raíz (o root)

El **directorio raíz** es el directorio de mayor nivel en Linux, y siempre se representa con una barra (/). Todos los subdirectorios se ramifican desde el directorio raíz y pueden continuar ramificándose a tantos niveles como sea necesario.

Directarios estándar del FHS

Justo debajo del directorio raíz, encontrarás los directorios estándar del FHS. En el diagrama, **home**, **bin** y **etc** son eso mismo. Estos son algunos ejemplos del contenido de los directorios estándar:

- **/home**: Cada usuario del sistema obtiene su propio directorio de inicio.
- **/bin**: Este directorio significa “binario” y contiene archivos binarios y otros archivos ejecutables. Los archivos ejecutables contienen una serie de comandos que una computadora debe seguir para ejecutar programas y llevar a cabo otras funciones.
- **/etc**: Este directorio almacena los archivos de configuración del sistema.

- `/tmp`: Este directorio almacena varios archivos temporales. Los/los atacantes suelen usar el directorio `/tmp` porque cualquier persona en el sistema puede modificar datos en estos archivos.
- `/mnt`: Este directorio significa “montaje” y almacena medios, como unidades USB y discos duros.

Consejo profesional: Puedes usar el comando `man hier` para obtener más información acerca del FHS y sus directorios estándar.

Subdirectorios específicos del usuario

En `home` hay subdirectorios para usuarios específicos. En el diagrama, estos usuarios son `analyst` y `analyst2`. Cada usuario tiene sus propios subdirectorios personales, como `projects`, `logs` o `reports`.

Nota: Cuando la ruta conduce a un subdirectorio debajo del directorio de inicio del usuario, este puede representarse con una virgulilla (~). Por ejemplo, `/home/analyst/logs` también puede representarse como `~/logs`.

Puedes navegar a subdirectorios específicos utilizando sus rutas de archivo absolutas o relativas. La **ruta de archivo absoluta** es la ruta completa del archivo, que comienza desde la raíz. Por ejemplo, `/home/analyst/projects` es una ruta de archivo absoluta. La **ruta de archivo relativa** comienza en el directorio actual del usuario.

Nota: Las rutas de archivo relativas pueden usar un punto (.) para representar el directorio actual, o dos puntos (..) para representar el directorio superior del directorio actual. Un ejemplo de una ruta de archivo relativa podría ser `../projects`.

Comandos clave para navegar por el sistema de archivos

Los siguientes comandos de Linux pueden utilizarse para navegar por el sistema de archivos: `pwd`, `ls` y `cd`.

`pwd`

El comando `pwd` imprime el directorio de trabajo en la pantalla. O, en otras palabras, devuelve el directorio en el que te encuentras actualmente.

La salida te da la ruta absoluta a este directorio. Por ejemplo, si estás en tu directorio `home` y tu nombre de usuario es `analyst`, al ingresar `pwd`, obtienes como resultado

`/home/analyst`.

Consejo profesional: Para saber cuál es tu nombre de usuario, usa el comando `whoami`. El comando `whoami` devuelve el nombre de usuario del usuario actual. Por ejemplo, si tu nombre de usuario es `analyst`, al ingresar `whoami` obtienes como resultado `analyst`.

`ls`

El comando `ls` muestra los nombres de los archivos y directorios en el directorio de trabajo actual. En el video, por ejemplo `ls` devolvió directorios como `logs` y un archivo llamado `updates.txt`.

Nota: Si quieres acceder al contenido de un directorio que no sea tu directorio de trabajo actual, puedes agregar un argumento después de `ls` con la ruta de archivo absoluta o relativa al directorio deseado. Por ejemplo, si estás en el directorio `/home/analyst` pero quieres enumerar el contenido de tu subdirectorio `projects`, puedes ingresar `ls /home/analyst/projects` o simplemente `ls projects`.

cd

El comando `cd` se usa para navegar entre directorios. Cuando necesites cambiar de directorio, debes usar este comando.

Para navegar a un subdirectorio del directorio actual, puedes agregar un argumento después de `cd` con el nombre del subdirectorio. Por ejemplo, si estás en el directorio `/home/analyst` y quieres navegar a tu subdirectorio `projects`, puedes ingresar `cd projects`.

También puedes navegar a cualquier directorio específico ingresando la ruta de archivo absoluta. Por ejemplo, si estás en `/home/analyst/projects`, al ingresar `cd /home/analyst/logs` cambias de tu directorio actual a `/home/analyst/logs`.

Consejo profesional: Puedes usar la ruta de archivo relativa e ingresar `cd ..` para subir un nivel en la estructura de archivos. Por ejemplo, si el directorio actual es `/home/analyst/projects`, al ingresar `cd ..` cambiarías tu directorio de trabajo a `/home/analyst`.

Comandos comunes para leer el contenido del archivo

Los siguientes comandos de Linux son útiles para leer el contenido del archivo: `cat`, `head`, `tail` y `less`.

cat

El comando `cat` muestra el contenido de un archivo. Por ejemplo, al ingresar `cat updates.txt`, se devuelve todo el contenido del archivo `updates.txt`.

head

El comando `head` muestra solo el comienzo de un archivo; 10 líneas, por defecto. El comando `head` puede ser útil cuando quieres conocer el contenido básico de un archivo pero no necesitas todo el contenido. Al ingresar `head updates.txt`, obtienes solo las primeras 10 líneas del archivo `updates.txt`.

Consejo profesional: Si quieres cambiar el número de líneas que devuelve el comando `head`, puedes incluir `-n` para especificar el número de líneas. Por ejemplo, si solo quieres que se te muestren las primeras cinco líneas del archivo `updates.txt`, ingresa `head -n 5 updates.txt`.

tail

El comando `tail` hace lo opuesto a `head`. Este comando puede usarse para mostrar solo el final de un archivo; 10 líneas, por defecto. Al ingresar `tail updates.txt`, obtienes solo las últimas 10 líneas del archivo `updates.txt`.

Consejo profesional: Puedes usar tail para leer la información más reciente en un archivo de registro.

less

El comando **less** devuelve el contenido de un archivo, una página a la vez. Por ejemplo, al escribir **less updates.txt**, se cambia la ventana de la terminal para mostrar el contenido de **updates.txt** una página a la vez. Esto te permite avanzar y retroceder por el contenido, con facilidad.

Una vez que hayas accedido a tu contenido con el comando **less**, puedes usar varios controles de teclado para moverte por el archivo:

- **Barra espaciadora**: desplazarse a la página siguiente
- **b**: desplazarse a la página anterior
- **Flecha hacia abajo**: avanzar una línea
- **Flecha hacia arriba**: retroceder una línea
- **q**: salir y volver a la ventana de terminal anterior

NIST

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1271es.pdf>

INCIDENTE :

Es un suceso inminente pone en peligro , sin autorizacion legal, la confidencialidad, integridad o disponibilidad de la informacion o de un sistema informatico o constituye una violacion o amenaza inminente de violacion de la ley

Una investigación revela información crítica sobre las cinco W de un incidente: quién desencadenó el incidente (who), qué pasó (what), cuándo ocurrió (when), dónde sucedió (where), y por qué ocurrió el incidente (why). Hacer un seguimiento de esto es clave durante una investigación, pero también al concluirla, cuando hay que escribir el informe final. Como analista, necesitarás un método para documentar y hacer referencia a esta información para acceder fácilmente cuando la necesites. La mejor manera de hacerlo es con el diario de gestión de incidentes, una documentación usada en la respuesta a incidentes. En este curso, usarás tu propio diario para registrar detalles de incidentes.

Hablaremos más sobre la documentación en las próximas lecciones.

Obtén más información sobre las capturas de paquetes

paquetes

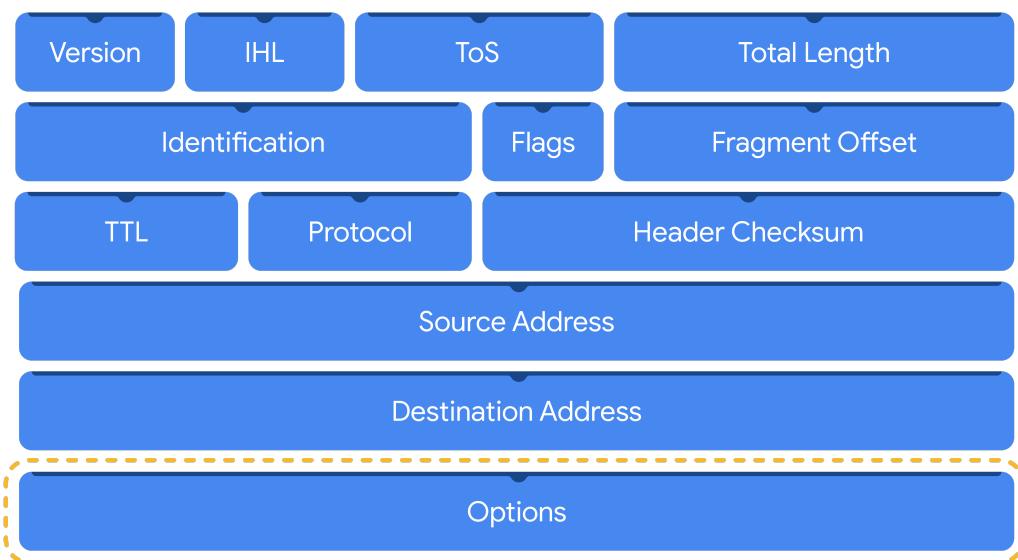
Anteriormente en el programa, aprendiste que un **paquete de datos** es una unidad básica de información que va de un dispositivo a otro dentro de una red. La detección de intrusiones en la red comienza a nivel de paquetes. Se debe a que estos constituyen la base del intercambio de información en una red. Cada vez que realizas una actividad en Internet, como visitar un sitio web, se envían y reciben paquetes entre tu computadora y el servidor del sitio web. Estos paquetes son los que ayudan a transmitir información a través de una red. Por ejemplo, al cargar una imagen en un sitio, los datos se dividen en varios paquetes, que luego se enrutan hacia el destino previsto y se vuelven a ensamblar al ser entregados.

En ciberseguridad, los paquetes proporcionan información valiosa que añade contexto a los eventos durante las investigaciones. Comprender la transferencia de información a través de paquetes no solo te ayudará a desarrollar conocimiento sobre la actividad de la red, sino también a identificar anomalías y proteger mejor las redes contra los ataques. Los paquetes tienen tres componentes: el encabezado, la carga útil y el pie. A continuación, encontrarás una descripción de cada uno.

Encabezado

Los paquetes comienzan con el componente fundamental: el encabezado. Estos pueden tener varios encabezados según los protocolos utilizados, como un encabezado Ethernet, uno de IP o uno de TCP, entre otros. Los mismos proporcionan información que se utiliza para enrutar los paquetes a su destino. Esto incluye información sobre las direcciones IP de origen y destino, la longitud del paquete, el protocolo, los números de identificación y más.

He aquí un encabezado IPv4 con la información que proporciona:



Carga útil

El componente de carga útil viene directamente después del encabezado y contiene los datos reales que se entregan. Si consideras el ejemplo de cargar una fotografía en un sitio web, la carga útil de este paquete sería la imagen en sí.

Pie

El pie, también conocido como el avance, se encuentra al final de un paquete. El protocolo Ethernet utiliza pies para brindar información de verificación de errores y determinar si los datos se dañaron. Además, puede que los paquetes de red Ethernet analizados no muestren información de pie debido a las configuraciones de red.

Nota: La mayoría de los protocolos, como el Protocolo de Internet (IP), *no* utilizan pies.

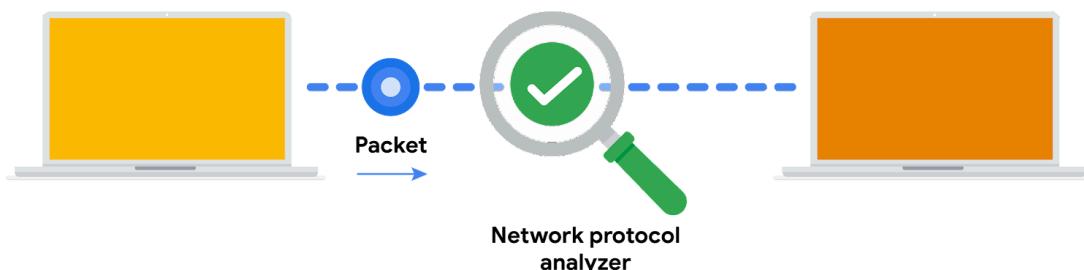
Analizadores de protocolo de red

Los analizadores de protocolo de red, o rastreadores de paquetes, son herramientas diseñadas para capturar y analizar el tráfico de datos dentro de una red. Algunos ejemplos son tcpdump, Wireshark y TShark.

Más allá de su uso en seguridad como una herramienta de investigación que monitorea redes e identifica actividades sospechosas, los analizadores de protocolo de red pueden utilizarse para recopilar estadísticas de redes, como el ancho de banda o la velocidad de conexión, y solucionar problemas de rendimiento, como las ralentizaciones.

No obstante, también se pueden utilizar con fines maliciosos. Por ejemplo, los agentes de amenaza pueden usar analizadores de protocolo de red para capturar paquetes que contienen datos confidenciales, como la información de inicio de sesión de la cuenta.

Aquí hay un diagrama de red que ilustra la transmisión de los paquetes de un emisor al receptor. Un analizador de protocolos de red se coloca en el medio de las comunicaciones para capturar los paquetes de datos que viajan a través del cable.



Cómo funcionan los analizadores de protocolo de red

Estos analizadores utilizan capacidades de software y hardware para capturar el tráfico de red y mostrarlo para que los analistas de seguridad lo examinen y analicen. A continuación, te contamos cómo lo hacen:

1. Primero, los paquetes deben recopilarse de la red a través de la **tarjeta de interfaz de red (NIC)**, que es el hardware que conecta las computadoras a una red, como un router. Las NIC reciben y transmiten tráfico de red, pero por defecto solo consideran el tráfico de red que está dirigido a ellas. Para capturar todo el tráfico que se envía a través de la red, una NIC debe ser cambiada a un modo que tenga acceso a todos los paquetes de datos de red visibles. En las interfaces inalámbricas, esto se conoce con frecuencia como modo de monitoreo, y en otros sistemas se puede llamar modo promiscuo. Este modo permite que la NIC acceda a todos los paquetes de datos de red visibles, pero no ayudará a los analistas a acceder a todos los paquetes a través de una red. Un analizador de protocolos de red debe posicionarse en un segmento de red apropiado para acceder a todo el tráfico entre diferentes hosts.
2. El analizador de protocolos de red recopila el tráfico de red en formato binario sin procesar. El formato binario consta de ceros y unos, y las personas no pueden interpretarlo con facilidad. El analizador de protocolos de red toma el formato binario y lo convierte para que se muestre en un modo legible para las personas, de modo que los analistas puedan leer y comprender la información con facilidad.

Cómo capturar paquetes

El **rastreo de paquetes** es la práctica de capturar e inspeccionar paquetes de datos a través de una red. Un archivo **pcap (captura de paquetes)** es un archivo que contiene paquetes de datos interceptados desde una interfaz o red. Estas capturas se pueden ver y analizar adicionalmente mediante analizadores de protocolo de red. Por ejemplo, puedes filtrar las capturas de paquetes para mostrar solo la información más relevante para tu investigación, como los paquetes enviados desde una dirección IP específica.

Nota: En muchos lugares, se considera ilegal utilizar analizadores de protocolo de red para interceptar y examinar las comunicaciones de red privada sin permiso.

Los archivos pcap pueden venir en diversos formatos según la biblioteca de captura de paquetes que se utilice. Cada uno tiene diferentes usos y las herramientas de red pueden utilizar o admitir formatos de archivo de captura de paquetes específicos de forma predeterminada. Te recomendamos familiarizarte con las siguientes bibliotecas y formatos:

1. **Libpcap** es una biblioteca de captura de paquetes diseñada para que la utilicen sistemas similares a Unix, como Linux y MacOS®. Las herramientas como tcpdump utilizan Libpcap como formato predeterminado de archivo de captura de paquetes.
2. **WinPcap** es una biblioteca de captura de paquetes de código abierto diseñada para dispositivos que ejecutan sistemas operativos Windows. Se considera un formato de archivo más antiguo y no se usa principalmente.
3. **Npcap** es una biblioteca diseñada por la herramienta de escaneo de puertos Nmap que se utiliza comúnmente en los sistemas operativos Windows.
4. **PCAPng** es un formato de archivo moderno que puede capturar paquetes y almacenar datos en simultáneo. Su capacidad para hacer ambas cosas explica el "ng", que significa "próxima generación".

Consejo profesional: Analizar tu red doméstica puede ser una buena manera de poner en práctica el uso de estas herramientas.

Operadores para filtrar fechas y números

Operadores de comparación

En SQL, el filtrado de datos numéricos y de fecha y hora suele involucrar operadores. Puedes usar los siguientes operadores en tus filtros, para asegurarte de obtener solo las filas que necesitas:

operador	uso
<	menor que
>	mayor que
=	igual que
<=	menor o igual que
>=	mayor o igual que
<>	no igual que

Nota: También puedes usar != como operador alternativo para no igual que.

Incorporación de operadores en filtros

Estos operadores de comparación se usan en la cláusula **WHERE** al final de una consulta. La consulta siguiente usa el operador > para filtrar la columna **birthdate** (fecha de nacimiento). Puedes ejecutar esta consulta para analizar sus resultados:

```
1  SELECT firstname, lastname, birthdate  
2  FROM employees  
3  WHERE birthdate > '1970-01-01';
```

Ejecutar

Restablecer

FirstName	LastName	BirthDate
Jane	Peacock	1973-08-29 00:00:00
Michael	Mitchell	1973-07-01 00:00:00
Robert	King	1970-05-29 00:00:00

Esta consulta devuelve el nombre y los apellidos de empleados/as que nacieron después, pero no el '1970-01-01' (o 1º de enero de 1970). Si en lugar de ese operador usaras el operador `>=`, los resultados también incluirían resultados de la fecha '1970-01-01'. En otras palabras, el operador `>` es exclusivo y el operador `>=` es inclusivo. Un **operador exclusivo** es el que no incluye el valor de comparación, en cambio un **operador inclusivo** es el que incluye el valor de comparación.

BETWEEN (entre)

Otro operador que también se usa para datos numéricos y de fecha y hora es el operador **BETWEEN**. **BETWEEN** filtra por números o fechas dentro de un rango. Por ejemplo, si quieres encontrar los nombres y apellidos de todos/as los/las empleados/as contratados/as entre el 1º de enero de 2002 y el 1º de enero de 2003, puedes usar el operador **BETWEEN** de la siguiente manera:

```
1  SELECT firstname, lastname, hiredate
2  FROM employees
3  WHERE hiredate BETWEEN '2002-01-01' AND '2003-01-01';
```

Ejecutar

Restablecer

FirstName	LastName	HireDate
Andrew	Adams	2002-08-14 00:00:00
Nancy	Edwards	2002-05-01 00:00:00
Jane	Peacock	2002-04-01 00:00:00

Task 4. Investigate logins by event ID

In this task, you need to investigate login attempts based on event ID numbers. With this query, you want to return only the `event_id`, `username`, and `login_date` fields from the `log_in_attempts` table.

Note: The `event_id` column contains numeric data; do not place numeric data in quotation marks.

1. Write a query to return login attempts with `event_id` greater than or equal to `100`.

The correct query to solve this step:

```
SELECT event_id, username, login_date
FROM log_in_attempts
WHERE event_id >= 100;
```



2. Modify the query to return only login attempts with `event_id` between 100 and 150.

The correct query to solve this step:

```
SELECT event_id, username, login_date
FROM log_in_attempts
WHERE event_id BETWEEN 100 AND 150;
```



Paquetes y captura de paquetes

Componentes de los paquetes

1. Header : información como el tipo de protocolo de red y puerto en uso
2. Carga util o payload : que contiene datos reales que se estan entregando
3. Footer : es el final del paquete

Network protocol analyzer (packed sniffer)

Es una herramienta que captura y analiza el tráfico de datos.

Packet capture (P-CAP)

Es un archivo que contiene paquetes de datos interceptados de una interfaz de red. utilies para investigar incidentes.

PASTA el proceso de modelo de ataques y análisis de amenazas

Pasta es un marco de modelado de amenazas popular que es usado en diferentes sectores, son las siglas de proceso de simulación de ataques y análisis de amenazas . El cual tiene 7 etapas

1. Definir los objetos comerciales de seguridad : antes de empezar el equipo debe definir sus objetivos.
2. Definir el alcance técnico: Aquí el equipo identifica los componentes de la aplicación que debe evaluarse (Superficie de ataque)
3. Descomponer la aplicación :Esto suele implicar trabajar en conjunto con los desarrolladores de la app para crear un diagrama de flujo de datos. El diagrama muestra cómo los datos van del dispositivo del usuario a la base de datos de la empresa. También se identificarían los controles para proteger los datos en tránsito.
4. Análisis de amenazas: Aquí el equipo adopta una mentalidad de atacante , la cual se investiga para obtener la información mas reciente sobre los tipos de ataque y prueba de vulnerabilidades
5. La quinta etapa de PASTA es crear un análisis de vulnerabilidad. Aquí, el equipo investiga en detalle las vulnerabilidades potenciales analizando la raíz del problema.
6. En la sexta etapa de PASTA, el equipo realiza el modelado de ataques y prueba las vulnerabilidades analizadas en la quinta etapa simulando ataques. Esto se hace mediante la creación de un árbol de ataque, que se parece a un diagrama de flujo.
7. Analizar el riesgo de impacto: aquí el equipo se reúne toda la información que recopilo en las etapas anteriores , entonces el equipo puede dar recomendaciones de riesgo informadas a las partes necesarias.

Permisos de archivo en Linux

W Untitled Attachment

Planes de respuesta a incidentes

1. Procedimientos de repuesta de incidentes: Son instrucciones paso a paso sobre como responder ante ellos , informacion del sistema , como los diagramas de red, diagramas de flujo de datos , registro e informacion de inventario de activos y otros documentos como listas de contactos

Practica con TCPDUMP

ask 3. Capture network traffic with tcpdump

In this task, you will use tcpdump to save the captured network data to a packet capture file.

In the previous command, you used tcpdump to stream all network traffic. Here, you will use a filter and other tcpdump configuration options to save a small sample that contains only web (TCP port 80) network packet data.

1. Capture packet data into a file called capture.pcap:

```
sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.pcap &
```

Copied!

content_copy

You must press the **ENTER** key to get your command prompt back after running this command.

This command will run tcpdump in the background with the following options:

- -i eth0: Capture data from the eth0 interface.
- -nn: Do not attempt to resolve IP addresses or ports to names. This is best practice from a security perspective, as the lookup data may not be valid. It also prevents malicious actors from being alerted to an investigation.
- -c9: Capture 9 packets of data and then exit.
- port 80: Filter only port 80 traffic. This is the default HTTP port.
- -w capture.pcap: Save the captured data to the named file.
- &: This is an instruction to the Bash shell to run the command in the background.

This command runs in the background, but some output text will appear in your terminal. The text will not affect the commands when you follow the steps for the rest of the lab.

2. Use curl to generate some HTTP (port 80) traffic:

```
curl opensource.google.com
```

Copied!

content_copy

When the curl command is used like this to open a website, it generates some HTTP (TCP port 80) traffic that can be captured.

3. Verify that packet data has been captured:

```
ls -l capture.pcap
```

Copied!

Practicas de reforzamiento del Sistema Operativo

Que es Sistema Operativo

Es la interfaz entre hardware de la computadora y el usuario

Ejemplos de practicas de seguridad:

- Actualización de parches: es una actualización de software y SO que aborda vulnerabilidades de seguridad en un programa o producto.
- Línea de base de configuración: es un conjunto de un conjunto documentado de especificaciones en un sistema que se usa como base para futuras compilaciones, versiones y actualizaciones
- Eliminación de hardware y software: debido a que no se utiliza
- Implementación de una política de contraseña segura y que sigan una serie de reglas específicas
- Autenticación de múltiples factores, o MFA :La MFA es una medida de seguridad que requiere verificar la identidad de dos o más formas para acceder a un sistema o red.

El reforzamiento de SO implica una serie de procedimientos que mantiene la seguridad del sistema operativo y la mejora.

Las medidas como privilegios de acceso y políticas de contraseña se revisan con frecuencia como parte del reforzamiento del SO

Primer examen de suricata y IDS

1. Un analista de seguridad usa un analizador de protocolos de red para capturar el tráfico HTTP con el fin de analizar patrones. ¿Qué tipo de datos está usando?

1 / 1 punto

- Basados en firmas
- Telemetría de red
- Basados en host
- Falsos positivos

Correcto

Está usando datos de telemetría de red. La telemetría de red es la recopilación y transmisión de datos de red para análisis, como el tráfico HTTP.

2. ¿Qué afirmación describe con exactitud la diferencia entre un sistema de detección de intrusiones basado en la red (NIDS) y un sistema de detección de intrusiones basado en host (HIDS)?

1 / 1 punto

- Un NIDS utiliza análisis de firmas para detectar amenazas, mientras que un HIDS utiliza agentes.
- Un NIDS solo detecta amenazas conocidas, en tanto que un HIDS detecta amenazas desconocidas.
- Un NIDS se instala en una red, en tanto que un HIDS se instala en dispositivos individuales.
- Un NIDS se instala en dispositivos individuales, en tanto que un HIDS se instala en una red.

Correcto

Un NIDS se instala en una red y se usa para recopilar y supervisar datos del tráfico de la red y de la propia red. Un HIDS se instala en un host y se usa para supervisar su actividad.

3. Completa el espacio en blanco: El componente _____ de una firma IDS incluye información del tráfico de red.

1 / 1 punto

- opciones de regla
- acción
- encabezado
- ID de firma

Correcto

El componente encabezado de una firma IDS incluye información sobre tráfico de red. Este incluye direcciones IP de origen y de destino, puertos de origen y de destino, protocolos y dirección del tráfico.

3. Completa el espacio en blanco: El componente _____ de una firma IDS incluye información del tráfico de red.

1 / 1 punto

- opciones de regla
- acción
- encabezado
- ID de firma

 Correcto

El componente encabezado de una firma IDS incluye información sobre tráfico de red. Este incluye direcciones IP de origen y de destino, puertos de origen y de destino, protocolos y dirección del tráfico.

4. Un analista de seguridad crea una firma de Suricata para identificar y detectar amenazas de seguridad en función de la dirección del tráfico de red. ¿Cuál de las siguientes opciones de regla debería usar?

1 / 1 punto

- Msg
- Flow
- Content
- Rev

 Correcto

Debería usar Flow. La opción Flow coincide con la dirección del flujo del tráfico de red.

Principio de mínimo privilegio

Reducir el acceso disminuye el riesgo

Toda empresa debe estar preparada para enfrentar el riesgo de robo, uso indebido o abuso de datos. La aplicación del principio de mínimo privilegio puede reducir significativamente el riesgo de incidentes costosos, como las filtraciones de datos, mediante las siguientes medidas:

- Limitando el acceso a la información confidencial.
- Reduciendo las posibilidades de modificación, alteración o pérdida accidental de datos.
- Facilitando la supervisión y la administración del sistema.

El principio de mínimo privilegio reduce considerablemente la probabilidad de un ataque exitoso al conectar recursos específicos a determinados usuarios y establecer límites a sus acciones. Es un control de seguridad importante que debe aplicarse a todos los activos.

Para implementar efectivamente el mínimo privilegio es fundamental empezar por definir de manera clara quiénes son los usuarios o entidades involucradas.

Determinar el acceso y la autorización

Para implementar el principio de mínimo privilegio, es necesario determinar el acceso y la autorización previamente. Para lograrlo, hay dos preguntas clave que deben responderse:

- ¿Quién es el usuario en cuestión?
- ¿Cuánto acceso requiere a un recurso específico?

Identificar un usuario suele ser un proceso sencillo. Usuario puede ser una persona (cliente, personal, proveedor) o un dispositivo o software conectado a la red empresarial. En general, cada usuario debería tener su propia cuenta, y estas cuentas, por lo general, se almacenan y gestionan dentro del servicio de directorio de la organización.

Estos son los tipos más comunes de cuentas de usuario:

- **Cuentas de invitado:** se proporcionan a usuarios externos que necesitan acceder a una red interna, como clientes, colaboradores externos o socios comerciales.
- **Cuentas de usuario:** se asignan al personal en función de sus responsabilidades laborales.
- **Cuentas de servicio:** se otorgan a aplicaciones o software que necesitan interactuar con otros programas en la red.
- **Cuentas privilegiadas:** tienen permisos elevados o acceso administrativo.

Es una buena práctica determinar un nivel de acceso inicial para cada tipo de cuenta antes de implementar el principio de mínimo privilegio. Sin embargo, el nivel de acceso apropiado puede cambiar de un momento a otro. Por ejemplo, una persona que trabaja en servicio de atención al cliente solo debería tener acceso a tu información mientras te está brindando asistencia. No obstante, cuando esta persona comience a atender a otro cliente y ya no te esté asistiendo activamente, tus datos deberían volver a quedar inaccesibles. El mínimo privilegio solo puede reducir el riesgo si las cuentas de usuario son monitoreadas de forma rutinaria y consistente.

Consejo profesional: Las contraseñas desempeñan un papel importante al implementar el principio del mínimo privilegio. Incluso si las cuentas de usuario están asignadas adecuadamente, una contraseña insegura puede comprometer los sistemas.

Auditoría de los privilegios de cuentas

Establecer las cuentas de usuario adecuadas y asignarles los derechos de acceso o privilegios apropiados es un paso inicial muy valioso. Sin embargo, realizar auditorías periódicas de estas cuentas es una parte esencial para mantener seguros los sistemas de tu empresa.

Existen tres enfoques comunes para auditar las cuentas de usuario:

- Auditorías de uso
- Auditorías de privilegios
- Auditorías de cambios de cuenta

Como profesional de seguridad, es posible que participes en cualquiera de estos procesos.

Auditorías de uso

Cuando se realiza una auditoría de uso, el equipo de seguridad revisa a qué recursos está accediendo cada cuenta y de qué forma los usuarios interactúan con estos recursos. Estas auditorías son útiles para determinar si los usuarios están cumpliendo con las políticas de seguridad de la organización. Además, permiten identificar si un usuario tiene permisos que podrían ser revocados debido a que ya no están siendo utilizados.

Auditorías de privilegios

Con el paso del tiempo, es común que los usuarios acumulen más privilegios de acceso de los que realmente necesitan, un fenómeno conocido como arrastre de privilegios. Esto puede suceder si un empleado recibe un ascenso o cambia de equipo, lo que conlleva cambios en sus responsabilidades laborales. Las auditorías de privilegios tienen como objetivo evaluar si el rol de un usuario se encuentra en consonancia con los recursos a los que actualmente tiene acceso.

Auditorías de cambios de cuentas

Los servicios de directorio de cuentas mantienen inventarios y registros asociados a cada usuario. Los cambios en una cuenta generalmente se guardan y pueden utilizarse para auditar el directorio en busca de actividades sospechosas, como múltiples intentos de cambiar la contraseña de una cuenta. Realizar auditorías de cambios de cuenta ayuda a asegurar que todas las modificaciones en las cuentas sean realizadas por usuarios autorizados.

Nota: La mayoría de los servicios de directorio se pueden configurar para alertar a quienes administran el sistema sobre actividades sospechosas.

Principios de seguridad OWASP

Open
Web
Applications
Security
Project
Principios de seguridad de owasp

- **Minimizar la superficie expuesta a ataques:** se refiere a las vulnerabilidades potenciales que podría aprovechar un agente de amenaza
- **Principio de mínimo privilegio :** significa conceder únicamente el acceso y la autorización mínimos necesarios para completar una tarea o función
- **Defensa en profundidad:** hace referencia a que las organizaciones deben disponer de varios controles de seguridad que aborden a los riesgos de amenaza de diferentes maneras
- **Separación de funciones:** refiere a que las acciones críticas deben depender de varias personas, cada una de las cuales sigue el principio del mínimo privilegio.
- **Simplificar la seguridad:** refiere a que ver con evitar soluciones innecesariamente complicadas por que la complejidad dificulta la seguridad.
- **Solucionar los problemas de seguridad correctamente:** Significa que cuando ocurren incidentes de seguridad es necesario identificar la causa , contener el impacto, detectas las vulnerabilidades y realizar pruebas para garantizar que la reparacion sea exitosa

Otros principios

Establecer configuración seguras por defecto

Este principio indica que el estado de seguridad óptimo de una aplicación también debe ser su estado predeterminado para los usuarios, ósea debería requerirse un esfuerzo adicional para hacer que la aplicación sea insegura

Fallar de forma segura:

Cuando falla o se detiene debe hacerlo restableciéndose automáticamente a la opción más segura.

No confiar en los servicios: Muchas de las organizaciones trabajan con formas asociadas o proveedoras de servicios, las cuales pueden ser diferentes a las de la empresa. Por lo tanto, la compañía no debería dar por sentado que los sistemas de estas firmas sean seguros.

Evitar la seguridad por oscuridad

La seguridad de una aplicación no debe depender de mantener el código fuente en secreto, sino que su seguridad tiene que basarse en muchos otros factores, como las políticas de contraseñas razonables, la defensa en profundidad, los límites de transacciones comerciales, una sólida arquitectura de red, y los controles de fraude y auditoría.

Privacidad de la información: Regulación y cumplimiento normativo

Seguridad de la información versus privacidad de la información

La seguridad y la privacidad son dos términos que se usan con frecuencia indistintamente fuera de este ámbito. Aunque ambos conceptos están relacionados, representan funciones específicas:

- **La privacidad de la información** se refiere a la protección contra el acceso y la difusión no autorizados de datos.
- **La seguridad de la información** (InfoSec) se refiere a la práctica de mantener los datos, en todas sus formas, alejados de usuarios no autorizados.

La diferencia clave: la privacidad consiste en proporcionar a las personas el control sobre su información personal y acerca de cómo se comparte. La seguridad, en cambio, se trata de proteger las decisiones de las personas y mantener su información a salvo de posibles amenazas.

Por qué es importante la privacidad en la seguridad

La importancia de la privacidad en la seguridad de los datos comenzó a ganar mucha atención a finales de la década de 1990. En ese momento, las empresas tecnológicas pasaron repentinamente de procesar los datos de las personas a almacenarlos y utilizarlos con fines comerciales. Por ejemplo, si una persona buscaba un producto en línea, las empresas almacenaban y compartían información sobre el historial de búsqueda de ese usuario con otras organizaciones. Esto permitía a las compañías ofrecer experiencias de compra personalizadas de forma gratuita.

Regulaciones importantes sobre privacidad

Las empresas deben cumplir con ciertas leyes para operar. Como recordarás, las **regulaciones** son normas establecidas por un gobierno u otra autoridad para controlar la forma en que se realiza algo. En particular, las regulaciones de privacidad existen para proteger a los usuarios de que su información sea recopilada, utilizada o divulgada sin su consentimiento. Además, estas regulaciones suelen describir las medidas de seguridad que deben implementarse para mantener la información privada protegida de amenazas.

Tres de las regulaciones de la industria más influyentes que todo profesional de la seguridad debe conocer son:

- Reglamento General de Protección de Datos (RGPD)
- Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI-DSS)
- Ley de Transferencia y Responsabilidad de los Seguros Médicos (HIPAA)

Reglamento General de Protección de Datos (RGPD)

El Reglamento General de Protección de Datos (RGPD) es un conjunto de normas y regulaciones desarrollado por la Unión Europea (UE) que otorga a los propietarios de los datos el control total sobre su información personal. Según el RGPD, se considera información personal el nombre, la dirección, el número de teléfono, la información financiera e información médica de una persona, entre otras.

Esta normativa es aplicable a cualquier empresa que maneje datos de ciudadanos o habitantes de la UE, sin importar dónde opere dicha compañía. Por ejemplo, una organización con sede en los Estados Unidos que maneja los datos de las visitas provenientes de la UE en su sitio web está sujeta a las disposiciones del RGPD.

Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI-DSS)

El Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI-DSS) refiere a un conjunto de normas de seguridad establecidas por importantes organizaciones de la industria financiera. Esta regulación tiene como objetivo asegurar las transacciones con tarjetas de crédito y débito contra el robo de datos y el fraude.

Ley de Transferencia y Responsabilidad de los Seguros Médicos (HIPAA)

La Ley de Transferencia y Responsabilidad de los Seguros Médicos (HIPAA) es una ley de los Estados Unidos que obliga a proteger la información sensible de salud de la gente. En virtud de la HIPAA, se prohíbe la divulgación de la información médica de una persona sin su conocimiento y consentimiento.

Nota: Estas regulaciones influyen en el manejo de datos en muchas organizaciones del mundo, a pesar de que fueron elaboradas por países o mercados específicos.

Existen otras leyes de cumplimiento normativo en materia de seguridad y privacidad.

Cuáles de ellas debe seguir tu organización dependerá de la industria y del ámbito en el que se desempeñe. Independientemente de las circunstancias, el cumplimiento normativo es importante para todas las empresas.

Evaluaciones y auditorías de seguridad

Las empresas deben cumplir con regulaciones que son importantes para el sector o industria en la que se desempeñan. Al hacerlo, validan que han alcanzado un nivel mínimo de seguridad, al mismo tiempo que demuestran su compromiso con mantener la privacidad de los datos.

El cumplimiento de las normas suele ser un proceso continuo y de dos partes, que implica auditorías y evaluaciones de seguridad:

- Una **auditoría de seguridad** es una revisión de los controles de seguridad, políticas y procedimientos de una organización frente a un conjunto de expectativas.
- Una **evaluación de seguridad** es una revisión para determinar la resistencia de las actuales medidas de seguridad frente a las amenazas.

Protección en los puntos de entrada

Superficie de ataque: incluye las vulnerabilidades potenciales que un agente de amenaza podría explotar.

Prepárate para todo

Es importante tener un plan en caso de que algo salga mal. Pero ¿cómo puedes saber qué planear? En este campo, los equipos suelen realizar simulaciones de aquello que puede salir mal como parte de su estrategia de gestión de vulnerabilidades. Una forma de hacerlo es aplicando una mentalidad de atacante a las debilidades que se descubren.

Aplicar una mentalidad de atacante es muy parecido a realizar un experimento. Se trata de causar problemas en un entorno controlado y evaluar el resultado para obtener información. Adoptar una mentalidad de atacante es una habilidad beneficiosa en el campo de seguridad, ya que ofrece una perspectiva diferente sobre los desafíos que estás tratando de resolver. Los conocimientos que obtengas pueden ser valiosos cuando llegue el momento de establecer un plan de seguridad o modificar uno ya existente.



Simulación de amenazas

Un método para aplicar una mentalidad de atacante es utilizar simulaciones de ataque. Por lo general, estas actividades se realizan de una de dos maneras: de *forma proactiva* y *reactiva*. Ambas estrategias comparten un objetivo común, que es hacer que los sistemas sean más seguros.

- Las *simulaciones proactivas* asumen el papel de un atacante al explotar las vulnerabilidades y traspasar las defensas. Esto a veces se llama un ejercicio de equipo rojo.
- Las *simulaciones reactivas* asumen el papel de un defensor que responde a un ataque. Esto a veces se llama un ejercicio de equipo azul.

Cada tipo de simulación es un esfuerzo de equipo con el que podrías involucrarte como analista.

Los equipos proactivos tienden a dedicar más tiempo a planificar sus ataques que a realizarlos. Si te encuentras involucrado en uno de estos ejercicios, es probable que tu equipo despliegue una variedad de tácticas. Por ejemplo, podrían persuadir al personal para que divulgue sus credenciales de inicio de sesión mediante el uso de correos electrónicos ficticios para evaluar cuán conscientes son en la empresa en cuanto a temas de seguridad.

Por otro lado, los equipos reactivos dedican sus esfuerzos a recopilar información sobre los activos que están protegiendo. Esto se hace comúnmente con la ayuda de herramientas de análisis de vulnerabilidades.

Cómo escanear los problemas

Quizá recuerdes que un **escáner de vulnerabilidades** es un software que compara automáticamente las vulnerabilidades y exposiciones comunes existentes con las tecnologías de la red. El escáner de vulnerabilidad se utiliza con frecuencia en el campo de

la seguridad. Los equipos emplean una variedad de técnicas de escaneo para descubrir debilidades en sus defensas. Las simulaciones reactivas suelen valerse de los resultados de un escaneo para evaluar los riesgos y determinar formas de remediar un problema.

Por ejemplo, un equipo que realiza una simulación reactiva podría realizar un análisis de vulnerabilidad externo de su red. Todo el ejercicio podría seguir los pasos que aprendiste en un video sobre evaluaciones de vulnerabilidad:

- **Identificación:** Un servidor vulnerable se marca porque está ejecutando un sistema operativo (SO) desactualizado.
- **Análisis de vulnerabilidades:** Se investiga el sistema operativo desactualizado y sus vulnerabilidades.
- **Evaluación de riesgos:** Después de haber realizado tu debida diligencia, se califica la gravedad de cada vulnerabilidad y se evalúa el impacto de no solucionarla.
- **Remediación:** Finalmente, la información que recopilaste se puede usar para abordar el problema.

Durante una actividad como esta, a menudo generarás un informe de tus hallazgos. Estos pueden presentarse ante los proveedores de servicios o supervisores. Comunicar con claridad los resultados de estos ejercicios a otros es una habilidad importante para desarrollar como profesional de la seguridad.

Encontrar soluciones innovadoras

Muchos controles de seguridad que aprendiste se crearon como una respuesta reactiva ante riesgos. Esto se debe a que los agentes de amenaza buscan continuamente formas de eludir las defensas existentes. La aplicación efectiva de una mentalidad de atacante requerirá que te mantengas al tanto de las tendencias de seguridad y las tecnologías emergentes.

Consejo profesional: Recursos como la [Base de datos nacional de vulnerabilidades \(NVD\)](#), [de NIST](#) pueden ayudarte a mantenerte al día en lo que respecta a vulnerabilidades comunes.

Protocolos de red

Se determinan como reglas que garantizan que los datos enviados lleguen a su destino, también se usan para describir el orden de entrega

Transmisión control protocolo (TCP)

protocolo de comunicación por internet permite conectar dos dispositivos y enviar datos entre ellos, verifica ambos dispositivos.

Descripción general de los protocolos de red

Es el conjunto de reglas utilizadas por dos o más dispositivos de una red para describir el orden de entrega y la estructura de los datos. Los protocolos de red funcionan como instrucciones que vienen junto con la información en el paquete de datos. Estas instrucciones indican al dispositivo receptor qué hacer con los datos. Los protocolos son como el lenguaje común que permite que los dispositivos de todo el mundo se comuniquen entre sí y se entiendan.

Las categorías de protocolos de red

Los protocolos de red se dividen en 3, los protocolos de comunicación, de gestión y de seguridad.

Protocolos de comunicación

Rigen el intercambio de información en la transmisión de redes, determinan cómo se transmiten los datos entre los dispositivos y el momento de la comunicación, también incluyen métodos para recuperar los datos perdidos durante el trayecto.

- El Protocolo de Control de Transmisión TCP es un protocolo de comunicación de internet que permite a dos dispositivos establecer una conexión y transmitir datos. El TCP usa 3 pasos.
 1. El dispositivo envía una solicitud de sincronización SYN a un servidor.
 2. Luego, el servidor responde con un paquete SYN/ACK para confirmar la recepción de la solicitud del dispositivo.
 3. Una vez que el servidor recibe el paquete ACK final desde el dispositivo, se establece la conexión TCP.
- **El protocolo de datagramas de usuario UDP** es un protocolo sin conexión que no establece un enlace entre dispositivos antes de la transmisión. Esto lo hace menos confiable que el TCP, pero también lo hace adecuado para transmisiones que requieren llegar rápidamente a su destino, como los juegos en línea.
- **El Protocolo de Transferencia de Hipertexto HTTP** es un protocolo de la capa de aplicación que proporciona un método de comunicación entre los clientes y servidores de sitios web. Este usa el puerto 80 y se considera inseguro. Por otra parte, muchos usan HTTPS, que es la versión segura.
- El sistema de nombres de dominio o DNS es un protocolo que traduce los nombres de los dominios de internet como direcciones IP cuando un equipo del cliente desea acceder a su dominio de sitio web utilizando el navegador de internet

Protocolos de gestión

Se usan para monitorear y administrar la actividad de una red, incluyen protocolos para notificar errores y optimizar el rendimiento en la red

- El protocolo simple de administración de red SNMP
 - es un protocolo de red utilizado para monitorear y gestionar los dispositivos en una red, este puede restablecer una contraseña de un dispositivo de red o cambiar la configuración básica. También puede enviar solicitudes a los dispositivos de la red para obtener un informe sobre cuánto ancho de banda de la red está siendo utilizado, en el modelo TCP/IP del SNMP se encuentra en la capa de aplicación.
- Protocolo de mensajes de control de internet (ICMP)
 - Es utilizado por dispositivos para informarse mutuamente sobre errores de transmisión de datos en la red, es utilizado por un dispositivo receptor para enviar un informe al dispositivo emisor sobre la transmisión de datos. Usado como una forma rápida de solucionar problemas de conectividad y tiempo de respuesta mediante la ejecución del comando "ping", se encuentra en la capa de internet

Protocolos de seguridad

Los protocolos de seguridad garantizan que los datos se envíen y reciban de forma segura a través de una red. Estos utilizan algoritmos de cifrado para proteger los datos durante su transmisión

- El **protocolo seguro de transferencia de hipertexto (HTTPS)** es un protocolo de red que proporciona un método de comunicación seguro entre clientes y servidores de sitios web. El HTTPS es una versión segura del HTTP que utiliza cifrado de capa de conexión segura/seguridad en la capa de transporte (SSL/TLS) en todas las transmisiones para que los/as agentes de amenaza no puedan leer la información. El HTTPS utiliza el puerto 443. En el modelo TCP/IP, el HTTPS se encuentra en la capa de aplicación.
- El **protocolo seguro de transferencia de archivos (SFTP)** es un protocolo seguro utilizado para transferir archivos de un dispositivo a otro a través de una red. El SFTP utiliza el protocolo Secure Shell (SSH), en general, a través del puerto TCP 22. El SSH utiliza un estándar de cifrado avanzado (Advanced Encryption Standard, AES) y otros tipos de encriptación para asegurar que destinatarios no deseados no puedan interceptar las transmisiones. En el modelo TCP/IP, el SFTP se encuentra en la capa de aplicación. El SFTP suele utilizarse con almacenamiento en la nube. Cada vez que un/a usuario/a carga o descarga un archivo desde el almacenamiento en la nube, el documento se transfiere utilizando el protocolo SFTP.

Traducción de direcciones de red

Los dispositivos en tu red doméstica u oficina local tienen cada uno una dirección IP privada que utilizan para comunicarse entre sí. Para que los dispositivos con direcciones IP

privadas puedan comunicarse con Internet pública, necesitan tener una dirección IP pública. De lo contrario, las respuestas no se enrutarán correctamente. En lugar de tener una dirección IP pública dedicada para cada uno de los dispositivos en la red local, el enrutador puede reemplazar la dirección IP de origen privado con su dirección IP pública y realizar la operación inversa para las respuestas. Este proceso se conoce como traducción de direcciones de red (NAT) y generalmente requiere que el enrutador o cortafuegos (firewall) se configuren específicamente para tal fin. La NAT es parte de la capa 2 (capa de Internet) y la capa 3 (capa de transporte) del modelo TCP/IP.

Direcciones IP privadas	Direcciones IP públicas
<ul style="list-style-type: none"> Las asignan los administradores de red Son únicas solo dentro de la red privada No tienen costo de uso Rangos de direcciones: <ul style="list-style-type: none"> ◦ 10.0.0.0-10.255.255.255 ◦ 172.16.0.0-172.31.255.255 ◦ 192.168.0.0-192.168.255.255 	<ul style="list-style-type: none"> Las asignan el IANA y el ISP Las direcciones son únicas en Internet a nivel mundial Alquilar una dirección IP pública tiene costo Rangos de direcciones: <ul style="list-style-type: none"> ◦ 1.0.0.0-9.255.255.255 ◦ 11.0.0.0-126.255.255.255 ◦ 128.0.0.0-172.15.255.255 ◦ 172.32.0.0-192.167.255.255 ◦ 192.169.0.0-233.255.255.255

Protocolo de configuración dinámica de host

El protocolo de configuración dinámica de host (DHCP) pertenece a la familia de los protocolos de gestión de redes. El DHCP es un protocolo de capa de aplicación utilizado en una red para configurar dispositivos. Asigna una dirección IP única y proporciona las direcciones del servidor DNS adecuado y la puerta de enlace predeterminada para cada dispositivo. Los servidores DHCP operan en el puerto UDP 67, mientras que los clientes DHCP operan en el puerto UDP 68.

Protocolo de resolución de direcciones

Para este momento, ya debes saber bastante acerca de las direcciones IP y las de control de acceso al medio (MAC). Has aprendido que cada dispositivo tiene una dirección IP que lo identifica en la red y una dirección MAC que es única para esa interfaz de red. La dirección IP de un dispositivo puede cambiar con el tiempo, pero su dirección MAC permanece. El protocolo de resolución de direcciones (ARP) es un protocolo de la capa de Internet en el modelo TCP/IP que se utiliza para traducir las direcciones IP que se encuentran en los paquetes de datos, en la dirección MAC del dispositivo de hardware.

Cada dispositivo en la red ejecuta el ARP y realiza un seguimiento de las direcciones IP y MAC coincidentes en un caché ARP. El ARP no tiene un número de puerto específico.

Telnet

Telnet es un protocolo de capa de aplicación que permite que un dispositivo se comunique con otro equipo o servidor. Telnet envía toda la información en texto claro. Si bien utiliza indicadores de línea de comando para controlar otro dispositivo similar al protocolo Secure Shell (SSH), no es tan seguro como el SSH. Telnet se puede usar para conectarse a dispositivos locales o remotos y utiliza el puerto TCP 23.

Protocolo Secure Shell (SSH)

El protocolo Secure Shell (SSH) se utiliza para crear una conexión segura con un sistema remoto. Este protocolo de capa de aplicación proporciona una alternativa para la autenticación segura y la comunicación cifrada. El SSH opera sobre el puerto TCP 22 y es un reemplazo para protocolos menos seguros, como Telnet.

Protocolo de oficina postal

El protocolo de oficina postal (POP, por Post Office Protocol) es un protocolo de capa de aplicación (capa 4 en el modelo TCP/IP) que se utiliza para gestionar y recuperar correos electrónicos de un servidor de correo. Muchas organizaciones tienen un servidor de correo dedicado que maneja el correo entrante y saliente para los/as usuarios/as en la red. Los dispositivos de usuario envían solicitudes al servidor y descargan mensajes de correo electrónico de forma local. Si alguna vez has actualizado tu aplicación de correo electrónico y has visto nuevos correos electrónicos aparecer en tu bandeja de entrada, estás experimentando el POP y el protocolo de acceso a mensajes de Internet (IMAP). La autenticación de texto no encriptada utiliza el puerto TCP/UDP 110, mientras que los correos electrónicos cifrados utilizan capa de conexión segura/seuridad en la capa de transporte (SSL/TLS) sobre el puerto TCP/UDP 995. Al usar el POP, el correo debe terminar de descargarse en un dispositivo local antes de poder leerse. Además, no permite que un/a usuario/a sincronice los correos electrónicos.

Protocolo de acceso a mensajes de Internet (IMAP)

El protocolo de acceso a mensajes de Internet (IMAP) se utiliza para correos electrónicos entrantes. Descarga sus encabezados, pero no el contenido, que permanece en el servidor, posibilitando a los/as usuarios/as acceder a su correo electrónico desde diferentes dispositivos. El IMAP utiliza el puerto TCP 143 para correos electrónicos no encriptados y el puerto TCP 993 con el protocolo TLS. El uso del IMAP permite a las personas leer parcialmente los correos electrónicos antes de que se terminen de descargar y sincronizarlos. Sin embargo, el IMAP es más lento que el POP3.

Protocolo para transferencia simple de correo (SMTP)

El protocolo para transferencia simple de correo (SMTP) se utiliza para transmitir y enrutar correos electrónicos desde el remitente hasta la dirección del/de la destinatario/a. El SMTP funciona con el software Message Transfer Agent (MTA), que consulta los servidores de sistema de nombres de dominio (DNS) para obtener las direcciones IP correspondientes a las direcciones de correo electrónico, asegurando que estos lleguen al destino previsto. El SMTP usa el puerto TCP/UDP 25 para correos electrónicos no cifrados y el puerto TCP/UDP 587 utiliza TLS para los cifrados. Con cierta frecuencia, el puerto TCP 25 se usa para el spam de alto volumen. El SMTP ayuda a filtrar el spam regulando la cantidad de correos electrónicos que una fuente puede enviar al mismo tiempo.

Protocolos y números de puerto

Recuerda que los números de puerto son utilizados por los dispositivos de red para determinar qué se debe hacer con la información contenida en cada paquete de datos una vez que lleguen a su destino. Los cortafuegos (firewalls) pueden filtrar el tráfico no deseado, basándose en los números de puerto. Por ejemplo, una empresa puede configurar un cortafuegos para permitir solo el acceso al puerto TCP 995 (POP3) a través de direcciones IP que pertenecen a la organización.

Como analista de seguridad, necesitarás conocer muchos de los protocolos y los números de puerto mencionados en este curso. Es posible que te pregunten por estos durante una entrevista laboral para evaluar tus conocimientos técnicos, así que es una buena idea memorizarlos. También aprenderás sobre nuevos protocolos mientras te desempeñas en una posición de seguridad.

Protocolo	Puerto
DHCP	Puerto UDP 67 (servidores) Puerto UDP 68 (clientes)
ARP	Ninguno
Telnet	Puerto TCP 23
SSH	Puerto TCP 22
POP3	Puerto TCP/UDP 110 (sin cifrar) Puerto TCP/UDP 995 (cifrado, SSL/TSL)
IMAP	Puerto TCP 143 (sin cifrar) Puerto TCP 993 (cifrado, SSL/TSL)
SMTP	Puerto TCP/UDP 25 (admite cifrado TSL) Puerto TCP/UDP 587 (cifrado, TSL)

Protocolos inalámbricos

IEEE 802.11 (WIFI) son estandares que definen las comunicaciones entre LAN inalambricas . En 2004 se introdujo el protocolo Acceso Wifi protegido o WPA. Es un protocolo de seguridad inalmbrica para conectarse a internet y han avanzado a WPA2 y WPA3 para tener mejoras de seguridad, como el cifrado avanzado

El termino Wifi fue propuesto como una estrategia de marketing por la Wireless Ethernet Compatibility Alliance (WECA)

Los estándares y protocolo de Wifi están basados en la familia de estándares de comunicaciones de internet 802.11 establecidos por el instituto de ingenieros eléctricos y electrónicos (IEEE)

Privacidad equivalente por cable

La privacidad equivalente por cable (WEP) es un protocolo de seguridad inalambrico usado para proporcionar a los usuarios el mismo nivel de privacidad en las conexiones de red inalambrica, que tienen por cable, el protocolo WEP fue desarrollado en 1999 y es el mas antiguo de los estandares de seguridad inlambrica.

Acceso Wi-fi protegido

o WPA fue desarrollado en 2003 para mejorar la privacidad equivalente por cable WEP, abordar problemas de seguridad que presentaba y reemplazaba. El WAP esta pensado como medida de transición para poder establecer la compatibilidad con hardware mas antiguo.

El WPA abordo esta debilidad utilizando el llamado Temporal Key Integrity Protocol (TKIP o tambien conocido como hashing de clave WEP WPA) el algoritmo de cifrado del WPA utiliza claves secretas mas extensas que las del protocolo WEP, lo que dificulta adivinar la clave mediante prueba y error.

El WPA también incluye una verificación de integridad de mensajes que agrega una etiqueta de autenticación con cada transmisión. Si un agente de amenaza intenta alterar la transmisión de alguna manera o reenviarla en otro momento, la verificación de integridad de mensajes de WPA identificará el ataque y rechazará la transmisión.

A pesar de las mejoras de seguridad del WPA, este todavía presenta vulnerabilidades. Los agentes de amenaza pueden valerse de un ataque de reinstalación de clave (o ataque KRACK) para descifrar transmisiones que utilizan WPA. Los atacantes pueden insertarse en el proceso de autenticación del WPA e introducir una nueva contraseña de cifrado en lugar

de la dinámica asignada por el WPA. Al configurar la nueva clave como todos ceros, es como si la transmisión no estuviera cifrada en absoluto.

WPA2 y WPA3

WPA2

Es la segunda version del acceso WI-Fi (WPA) lanzamiento 2004, mejora con respecto al WPA con la encripcion AES, tambien optimiza el uso del TKIP. usa el counter mode cipher chain message authentication code protocol (CCMP), que proporciona encapsulacion y garantiza la autentificacion e integridad de los mensajes, vulnerable a los ataques KRACK

Personal

El modo personal del WPA2 es el más adecuado para redes domésticas por diversas razones; es fácil de implementar y la configuración inicial lleva menos tiempo que para la versión empresarial. La frase de contraseña global para la versión personal del WPA2 debe aplicarse a cada computadora y punto de acceso individual en una red. Esto lo hace ideal para redes domésticas, pero poco práctico de gestionar en las organizaciones.

Empresarial

El modo empresarial del WPA2 es el más adecuado para aplicaciones corporativas. Proporciona la seguridad necesaria para las redes inalámbricas en entornos comerciales. Si bien la configuración inicial es más complicada que en el modo personal WPA2, el empresarial ofrece un control individualizado y centralizado sobre el acceso Wi-Fi a una red empresarial. Esto significa que quienes administren la red pueden otorgar o eliminar el acceso de los/las usuarios/as a una red en cualquier momento. Los/las usuarios/as nunca tienen acceso a las claves de cifrado, lo que evita que posibles atacantes recuperen las claves de red en computadoras individuales.

WPA3

El WPA3 es un protocolo de Wi-Fi seguro y su uso está creciendo a medida que se lanzan más dispositivos compatibles con este protocolo. Las principales diferencias entre el WPA2 y el WPA3 son:

- El WPA3 aborda la vulnerabilidad de intercambio de autenticación a los ataques KRACK, que está presente en el WPA2.
- El WPA3 utiliza la Autenticación Simultánea de Iguales (SAE, por sus siglas en inglés), un acuerdo de autenticación de contraseña y cifrado de claves. Esto evita que los atacantes descarguen datos de las conexiones de redes inalámbricas para intentar descifrarlos.
- El WPA3 incrementó el cifrado para hacer que las contraseñas sean más seguras mediante el uso de encriptación de 128 bits, mientras que el modo WPA3 empresarial ofrece un cifrado opcional de 192 bits.

Prácticas adecuadas para recopilar y gestionar registros

En esta lectura, conocerás algunas de las mejores prácticas relacionadas con la gestión, el almacenamiento y la protección de registros. Entenderlas te ayudará a perfeccionar las búsquedas de registros y te dará más recursos para identificar y resolver incidentes de seguridad.

Registros

Las fuentes de datos, como los dispositivos, generan información en forma de eventos. Un **registro** (o log) recopila los eventos que se producen dentro de los sistemas de una organización. Estos registros contienen entradas, y cada una detalla la información correspondiente a un único evento que ocurrió en un dispositivo o sistema. Originalmente, los registros servían solo para solucionar problemas tecnológicos habituales. Por ejemplo, los registros de errores proporcionan información sobre por qué ocurrió un error inesperado y ayudan a identificar el origen del error para que pueda corregirse. Hoy, prácticamente todos los dispositivos informáticos generan algún tipo de registro que brinda información valiosa y que no solo tiene que ver con la resolución de problemas. En seguridad, los profesionales usan los **análisis de registros**, que es el proceso mediante el cual se examinan los registros para identificar eventos de interés. Los registros ayudan a descubrir los detalles que responden a las 5 W de la investigación del incidente: *quién (who)* desencadenó el incidente, *qué (what)* sucedió, *cuándo (when)* ocurrió, *dónde (where)* ocurrió y *por qué (why)* se produjo.

Tipos de registros

Según la fuente de datos, se pueden producir diferentes tipos de registro. A continuación, mencionamos una lista de algunos tipos de registros comunes que las organizaciones deberían recopilar:

- **Red:** Los registros de red son generados por dispositivos de red, como firewalls, routers o switches.
- **Sistema:** Los registros de sistema son generados por sistemas operativos, como Chrome OS™, Windows, Linux o macOS®.
- **Aplicación:** Los registros de aplicación son generados por aplicaciones de software y contienen información relacionada con los eventos que ocurren dentro de la aplicación, como una aplicación en un teléfono inteligente.
- **Seguridad:** Los registros de seguridad son generados por varios dispositivos o sistemas, como el software antivirus y los sistemas de detección de intrusiones. Estos contienen información relacionada con la seguridad, como la eliminación de archivos.

- **Autenticación:** Los registros de autenticación se generan cada vez que se produce una autenticación, como un intento de inicio de sesión exitoso en una computadora.

Detalles de registro

Los registros suelen contener una fecha, una hora, una ubicación, una acción y el autor de la acción. Este es un ejemplo de un registro de autenticación:

```
Login Event [05:45:15] User1 Authenticated successfully
```

Los registros contienen información y se pueden ajustar para que incluyan aún más. El registro verbose (con abundancia de detalle) recopila información adicional y detallada que excede el registro predeterminado. Este es un ejemplo del mismo registro anterior pero registrado con abundancia de detalle (verbosidad).

```
Login Event [2022/11/16 05:45:15.892673] auth_performer.cc:470 User1
```

```
Authenticated successfully from device1 (192.168.1.2)
```

Gestión de registros

Puesto que todos los dispositivos producen registros, puede resultar complicado para las organizaciones realizar un seguimiento de cada uno de ellos. Para aprovecharlos al máximo, tienes que elegir exactamente qué registrar, saber cómo acceder a ellos fácilmente y mantenerlos seguros, mediante la gestión de registros. La **gestión de registros** es el proceso de recopilar, almacenar, analizar y eliminar los datos de registro.

Qué registrar

Lo más importante de la gestión de registros es elegir qué registrar. Cada organización es diferente, y sus requisitos de registro también pueden serlo. Es importante tener en cuenta qué fuentes de registro tienen más probabilidades de contener información útil de acuerdo al evento de interés. Esto podría implicar configurar las fuentes de registro para reducir la cantidad de datos que registran o excluir la verbosidad excesiva. Cierta información, que incluye números de teléfono, direcciones de correo electrónico y nombres, entre otros datos, constituye la información de identificación personal (PII), la cual requiere de una gestión especial. Es posible que en algunas jurisdicciones no puedan registrarse.

El problema de la saturación de registros

Desde el punto de vista de la seguridad, registrar todo puede resultar tentador. Este es el error más común que cometen las organizaciones. El hecho de que se pueda registrar no significa que *deba* registrarse. Almacenar una cantidad excesiva de registros puede suponer muchas desventajas para algunas herramientas SIEM. Por ejemplo, la saturación de registros puede aumentar los costos de almacenamiento y mantenimiento. Además, puede aumentar la carga en los sistemas, lo que puede generar problemas de rendimiento y afectar la capacidad de uso. Esto, a su vez, dificulta la búsqueda e identificación de eventos importantes.

Retención de registros

Algunas organizaciones operan en industrias con regulaciones determinadas. Por ejemplo, ciertas normativas exigen que las empresas retengan los registros durante un período

determinado. En estos casos, las organizaciones pueden implementar prácticas de retención de registros en su política de gestión.

Es posible que algunas organizaciones deban modificar su política de gestión de registros para cumplir con las regulaciones. Esto es así para las que operan en industrias como:

- Sector público, como en el caso de la Ley Federal de Modernización de la Seguridad de la Información (FISMA)
- Atención médica, como la Ley de Transferencia y Responsabilidad de los Seguros Médicos, de 1996 (HIPAA)
- Servicios financieros, como el Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS), la Ley Gramm-Leach-Bliley (GLBA) y la Ley Sarbanes-Oxley de 2002 (SOX)

Protección de registros

Junto con la gestión y la retención, la protección de los registros es vital para mantener su integridad. Suele ser habitual que los agentes de amenaza modifiquen registros con el fin de engañar a los equipos de seguridad e incluso ocultar su actividad.

Almacenar registros en un servidor de registros centralizado es una forma de mantener su integridad. Cuando estos se generan, se envían a un servidor exclusivo en vez de almacenarse en una máquina local, lo cual dificulta a los atacantes acceder a ellos.

Prácticas adecuadas para una documentación eficaz

La documentación es cualquier forma de contenido registrado que se utiliza para un propósito específico, y es esencial en el campo de la seguridad. Los equipos de seguridad utilizan la documentación para respaldar investigaciones, completar tareas y comunicar hallazgos. Esta lectura explora los beneficios de la documentación y te proporciona una lista de prácticas comunes para ayudarte a crear documentación efectiva en tu carrera en el campo de la seguridad.

Beneficios de la documentación

Anteriormente, has aprendido sobre distintos tipos de documentación de seguridad, entre ellos los manuales de estrategias y los informes finales. Además, sabes que la documentación efectiva tiene tres beneficios:

1. Transparencia
2. Estandarización
3. Claridad

Transparencia

En seguridad, la transparencia es fundamental para demostrar el cumplimiento de las normativas, regulaciones y procesos internos y dar cuenta de los requisitos vinculados con

los seguros. Además, es esencial para los procedimientos legales. El proceso de documentar la posesión y el control de evidencia durante el ciclo de vida del incidente se denomina **cadena de custodia** y es un ejemplo de cómo la documentación genera transparencia y mejora la auditoría.

Estandarización

La estandarización a través de procesos y procedimientos repetibles ayuda a la mejora continua, a transferir conocimiento y a facilitar la incorporación de nuevos miembros al equipo. Los **estándares** son referencias que informan sobre cómo establecer políticas. Previamente, has aprendido cómo NIST proporciona varios marcos de seguridad que se utilizan para mejorar las medidas de seguridad. Del mismo modo, las organizaciones establecen sus propios estándares para satisfacer las necesidades de sus negocios. El **plan de respuesta a incidentes** de una organización es un ejemplo de documentación que crea estandarización. Al describir y documentar paso a paso el proceso de respuesta a un incidente, antes de que este ocurra, el procedimiento queda estandarizado. De esta manera, ante un incidente, las personas pueden seguir el paso a paso, manteniendo, así, la consistencia con los procesos y procedimientos repetibles.

Claridad

Idealmente, la documentación debe proporcionar claridad. La documentación clara ayuda a las personas a acceder rápidamente a la información que necesitan y tomar las medidas necesarias. Los analistas de seguridad deben documentar el razonamiento que respalda cualquier medida que toman, y dejar en claro a su equipo por qué se elevó a superiores (escaló) o se cerró una alerta.

Prácticas adecuadas

En tu carrera como profesional de la seguridad, deberás aplicar las mejores prácticas de documentación. Aquí se detallan algunas pautas generales para que tengas en cuenta:

Conoce a tu público

Antes de que comiences a crear la documentación, considera a tu público y sus necesidades. Por ejemplo, un resumen de incidentes escrito para un gerente de un centro de operaciones de seguridad (SOC) estará redactado de manera diferente a uno que haya sido elaborado para un director ejecutivo (CEO). El gerente del SOC puede entender el lenguaje técnico del campo de la seguridad, pero un CEO podría no hacerlo. Por lo tanto, es necesario que adaptes tu documento para satisfacer las necesidades de tu público.

Sé conciso

Es posible que se te asigne la tarea de crear documentación larga, como un informe. Pero cuando resulta demasiado extensa, puede haber resistencia a utilizarla. Para asegurarte de que tu documentación sea útil, establece el propósito desde un comienzo. Esto ayuda a las personas a identificar rápidamente el objetivo del documento. Por ejemplo, los resúmenes ejecutivos describen los principales hechos de un incidente al comienzo de un informe final. Este resumen debe ser breve, de manera que pueda leerse por encima, fácilmente, para identificar los principales hallazgos.

Actualízalo con frecuencia

En seguridad, se descubren y explotan nuevas vulnerabilidades constantemente. La documentación debe revisarse y actualizarse regularmente para mantenerse al día con el panorama de amenazas en evolución. Por ejemplo, después de que se ha resuelto, una revisión integral de un incidente puede identificar brechas en los procesos y procedimientos que requieren cambios y actualizaciones. Al actualizar regularmente la documentación, los equipos de seguridad se mantienen bien informados y los planes de respuesta a incidentes permanecen actualizados.

Redes

De las redes tradicionales a las redes en la nube

- Tradicionalmente, las empresas eran propietarias de sus dispositivos de red y los mantenían en sus propias oficinas. Sin embargo, muchas empresas utilizan ahora proveedores externos para gestionar sus redes para ahorrar dinero y acceder a más recursos de red.
- El crecimiento de la computación en la nube está ayudando a muchas empresas a reducir costes y a agilizar sus operaciones de red.

Comprensión de las redes en la nube

- La computación en la nube es la práctica de utilizar servidores, aplicaciones y servicios de red remotos que están alojados en Internet en lugar de en dispositivos físicos locales.
- Una red en la nube es una colección de servidores u ordenadores que almacenan recursos y datos en un centro de datos remoto al que se puede acceder a través de Internet.

Importancia de la seguridad en la nube

- Los proveedores de servicios en la nube ofrecen computación en la nube para mantener aplicaciones, como almacenamiento bajo demanda y potencia de procesamiento que sus clientes sólo pagan cuando lo necesitan.
- A medida que más organizaciones trasladan sus servicios de red a la nube, la seguridad en la nube se ha convertido en un aspecto importante de la seguridad de la red.

Redes de computadora

A ¿A quién le pertenece el internet? A nadie. No es una persona o grupo, es una colección mundial de redes interconectadas que colaboran entre si para intercambiar información sobre los estándares comunes .

Redes locales

Redes SOHO(small office/ home office) nos permiten compartir recursos entre pocos usuarios locales.
dispositivos conectados

Etiquetas RFID etiquetas de identificación por radiofrecuencia puede servir para rastrear cosas

Que es datos

datos que ingresamos a nuestros dispositivos que tenemos
que tipos de datos tenemos:

Datos voluntarios: datos que ofrecemos nosotros como usuarios

Datos deducidos: datos que se generan por los que hacemos en la red.

Bit es la abreviatura de "binary digit" y representa la unidad de datos mas pequeña.

Métodos de transmisión

Señales eléctricas - La transmisión se realiza representando los datos como pulsos eléctricos que viajan por un cable de cobre.

Señales ópticas - La transmisión se realiza convirtiendo las Señales eléctricas en pulsos de luz

Señales inalámbricas- La transmisión se realiza por medio de ondas infrarrojas de microondas o de radio por aire

Ancho de banda

es la capacidad de un medio para transportar datos , lo cual se mide por la cantidad de datos que fluyen de un lugar a otro Las medidas comunes son las siguientes:

- Miles de bits por segundo (Kbps)
- Millones de bits por segundo(Mbps)
- Miles de millones de bits por segundo (Gbps)

Unidad de ancho de banda	Abreviatura	Equivalencia
Bits por segundo	bps	1 bps = unidad fundamental de ancho de banda
Kilobits por segundo	Kbps	1 Kbps = 1,000 bps = 10^3 bps
Megabits por segundo	Mbps	1 Mbps = 1,000,000 bps = 10^6 bps
Gigabits por segundo	Gbps	1 Gbps = 1,000,000,000 bps = 10^9 bps
Terabits por segundo	Tbps	1 Tbps = 1,000,000,000,000 bps = 10^{12} bps

Latencia se refiere a la cantidad de tiempo , incluidas las demoras , que le toman a los datos transferirse desde un punto determinado a otro. así como los tipos de datos y la latencias de red se combinan para hacer que el rendimiento no coincidan con el ancho de band.

Todas las Pc conectadas a una red que participan directamente en la comunicación de la red se clasifican como host . Los host pueden enviar o recibir mensajes a través de la red. Existen diferentes tipos de respuesta:

- Correo electrónico: El servidor de correo electrónico ejecuta el software del servidor de correo electrónico
- WEB: El servidor ejecuta el software del servidor web
- Archivo: el servidor de archivos almacena archivos de usuario y empresariales en una ubicación central

Redes entre pares

Cuando las PC funcionan como servidores y clientes en la red se le denomina red entre pares P2P.

La red P2P más simple consta de 2 computadoras conectadas directamente mediante una conexión por cable o inalámbrica. Ambas usan una red simple para intercambiar datos y servicios entre sí, y para ello ambas actúan como cliente y servidor.

Ventajas

- Fácil de configurar
- Menos complejo
- Menor costo, ya que es posible que se utilicen dispositivos de red sin servidores dedicados
- Se pueden utilizar para tareas sencillas como transferir archivos y compartir impresoras

Desventajas

- La administración no es centralizada
- No son tan seguras
- No son escalables
- Todos los dispositivos pueden funcionar como clientes y como servidores, lo que puede ralentizar el rendimiento

Aplicaciones P2P

Algunas de las aplicaciones usan un sistema híbrido donde se descentraliza el intercambio de recursos, pero los índices apuntan a que las ubicaciones de los recursos están almacenados en un directorio centralizado. En un sistema híbrido, cada punto accede a un servidor de índice para obtener la ubicación de un recurso almacenado en otro punto.

Infraestructura de red

Tenemos algunos dispositivos finales, dispositivos intermedios, medios de red.

Conexión ISP

La conexión ISP que conforma una red troncal de internet es una red compleja de cables de fibra óptica con comutadores y enruteadores de red.

Conexión de cable y DSL

Cable- La señal de datos de internet se transmite a través del mismo cable coaxial que transporta la señal por cable , se utiliza un modem por cable y proporciona una conexión de internet siempre activa y de un ancho de banda elevado

DSL: La línea de suscriptor digital proporciona una conexión a internet siempre activa y de un ancho de banda elevado , requiere un modem de alta velocidad que separa la señal DSL de una señal telefónica y proporciona una conexión Ethernet a un equipo host a una LAN

Se transmite a través de la línea telefónica

Dispositivos Móviles y Wi-Fi

Para conectarse a una red WiFi manualmente en un dispositivo Android, siga estos pasos:

Seleccionar Configuración > Agregar red.

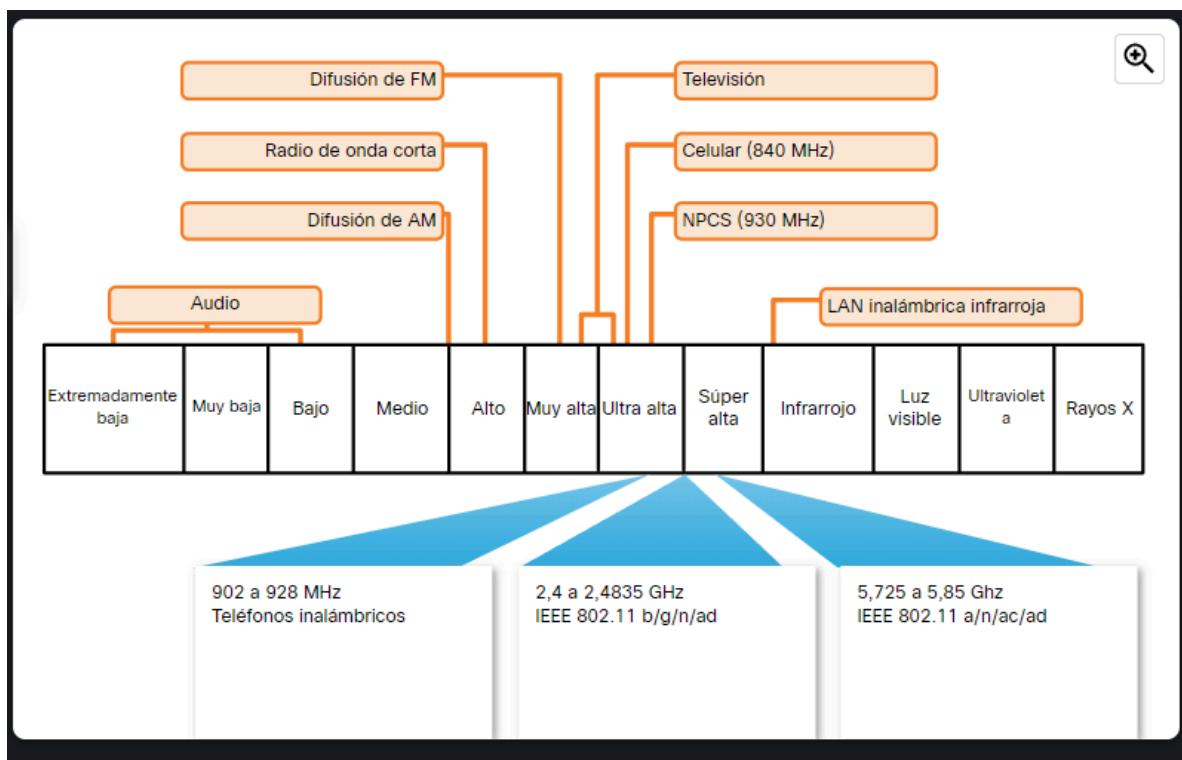
Paso 2. Ingresar el SSID de la red.

Paso 3: Tocar en Seguridad y seleccionar un tipo de seguridad.

Paso 4. Tocar en Contraseña e ingresar la contraseña.

Paso 5: Tocar en Guardar.

Frecuencias inalámbricas LAN



Tecnologías para Redes cableadas

- Cable categoria 5e: es el mas comun utilizado en LAN el cable consta de 4 pares de hilos entrelazados para reducir la interferencia electrica
- Cable coaxial: tiene un alambre interno rodeado por una capa de aislante tubular , que despues esta rodeada por un blindaje conductor tubular la mayoria de los cables coaxiales tambien tienen un aislante externo
- Cable de Fibra optica: pueden ser de vidrio o de plastico con un diametro similar al de un cabello humano, envía todo a velocidades muy largas y grandes distancias , con un ancho de banda muy alto que permite trasportar grandes cantidades de datos.

Configuracion inalambrica

- Modo de red: determina el tipo de tecnologia que se utiliza ejemplo 802.11b, 802.11g, 802.11n o Modo Mixto.
- nombre de la red: usado para identificar las WLAN todos los dispositivos que dessen participar en la WLAN deben tener el mismo SSID
- Canal Standar: especifica el canal en el que se lleva a cabo la comunicacion la configuracion esta establecida como auto para permitir al conexion mas optima

Modo de Red

Debido a la importancia de la elección del estándar 802.11 y del SSID en el entorno de red inalámbrica, es fundamental comprender su impacto en la velocidad y la seguridad. La configuración adecuada de estos componentes es esencial para garantizar un rendimiento óptimo y prevenir accesos no autorizados. Además, la implementación de un cifrado sólido es crucial para restringir el acceso no autorizado a la red inalámbrica. Es fundamental considerar estos aspectos al establecer y mantener una red inalámbrica eficiente y segura.

Protocolos de comunicación

Son necesarios para que las computadoras se comuniquen correctamente a través de la red

Características de los protocolos

- Formato de mensaje:
- Tamaño del mensaje:
- Sincronizaron: La velocidad a la que se transmiten los bits a través de la red
- Codificación: El host emisor primero convierte los bits en los mensajes enviados a través de la red
- Encapsulamiento: Cada mensaje transmitido en la red debe incluir un encabezado que contenga información de asignación de direcciones que identifique los host de origen y destino/
- Patrón de mensaje: Algunos mensajes requieren confirmación de recepción para poder enviar el siguiente mensaje

El IETF (Internet Engineering Task Force) registra y publica los estándares de Internet en documentos conocidos como: Petición de comentarios RFC

TCP/IP model

Capa del modelo TCP/IP	Descripción
Aplicación	Representa datos para el usuario más el control de codificación y de diálogo.
Transporte	Admite la comunicación entre distintos dispositivos a través de diversas redes.
Internet	Determina el mejor camino a través de una red.
Acceso a la red	Controla los dispositivos del hardware y los medios que forman la red.

Modelo de referencia OSI

Modelo de protocolo:

coincide estrechamente con la estructura de un conjunto de protocolos en familiar. Una suite de protocolos incluye el conjunto de protocolos relacionados que generalmente proporcionan toda la funcionalidad requerida para que las personas se comuniquen con la red de datos

Modelo de Referencias:

Este modelo describe las funciones que se deben completar en un modelo de referencia no pretende ofrecer un nivel de detalle en particular para definir de forma precisa la manera que cada protocolo se debe usar

Capa del modelo OSI	Descripción
7 - Aplicación	La capa de aplicación contiene protocolos utilizados para comunicaciones proceso a proceso.
6 - Presentación	La capa de presentación proporciona una representación común de los datos transferidos entre los servicios de la capa de aplicación.
5 - Sesión	La capa de sesión proporciona servicios a la capa de presentación para organizar su diálogo y administrar el intercambio de datos.
4-Transporte	La capa de transporte define los servicios para segmentar, transferir y reensamblar los datos para las comunicaciones individuales entre terminales.
3 - Red	La capa de red proporciona servicios para intercambiar los datos individuales en la red entre terminales identificados.
2 - Enlace de Datos	Los protocolos de la capa de enlace de datos describen los métodos para intercambiar tramas de datos entre dispositivos en un medio común.
1- Física	Los protocolos de la capa física describen los medios mecánicos, eléctricos, funcionales y de procedimiento para activar, mantener y desactivar conexiones físicas para una transmisión de bits hacia y desde un dispositivo de red.

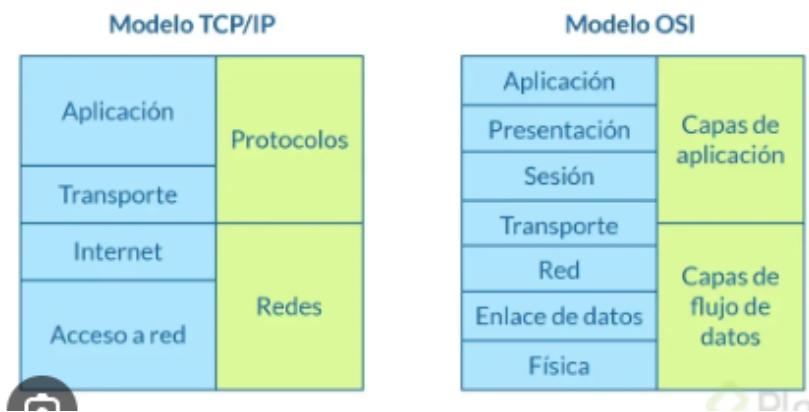
Comparación del Modelo OSI y el Modelo TCP/IP

Debido a que TCP/IP es el conjunto de protocolos en uso para las comunicaciones por Internet, ¿por qué también necesitamos aprender el modelo OSI?

En resumen, el método TCP/IP ofrece una manera de entender las interacciones de los protocolos en la suite TCP/IP, y cómo se relacionan con el modelo OSI. Aunque no abarca todos los aspectos de las comunicaciones de red, proporciona detalles específicos sobre los protocolos y las funciones que desempeñan en las capas de red, transporte y aplicación. Este enfoque detallado permite comprender mejor el funcionamiento de la suite de protocolos TCP/IP en relación con el modelo de referencia OSI.

El Protocolo de Control de Transporte (TCP) es responsable de garantizar una entrega confiable.

Los enruteadores utilizan el protocolo de Internet (IP) para reenviar mensajes



Medios de transmisión

- Hilos metálicos dentro de cables - Los datos se codifican en impulsos eléctricos.
- Fibras de vidrio o plástico (cable de fibra óptica) - Los datos se codifican como pulsos de luz.
- Transmisión inalámbrica - Los datos se codifican a través de la modulación de frecuencias específicas de ondas electromagnéticas.

CAMPOS DE LA TRAMA ETHERNET

Ethernet es la tecnología comúnmente utilizada en redes de área local. Los dispositivos acceden a la red LAN Ethernet con una Tarjeta de interfaz de red (NIC) Ethernet. Cada NIC Ethernet tiene una dirección única integrada en forma permanente en la tarjeta que se conoce como dirección de Control de acceso al medio (MAC). La dirección MAC tanto para el origen como para el destino son campos en una trama de Ethernet.

La encapsulación es el proceso de anteponer información de un protocolo con información de otro protocolo.

Cuando una trama de Ethernet envía una interfaz, la dirección MAC de destino indica la dirección MAC del dispositivo, que se encuentra en esta red, que recibirá la trama de Ethernet.

El Preámbulo y el Delimitador de Inicio de Trama (SFD) indica el comienzo de una trama de Ethernet.

Los conmutadores Ethernet deciden el reenvío en función de la dirección MAC de destino. Los switches Ethernet agregan entradas a su tabla de direcciones MAC en función de la dirección MAC de origen.

Cuando un conmutador recibe una trama de Ethernet y la dirección MAC de destino de esa trama no está en su tabla de direcciones MAC, el conmutador reenviará la trama a todos los puertos excepto al puerto de entrada.

El campo FCS se utiliza para la verificación de errores en la trama. Se calcula un valor CRC (Cyclic Redundancy Check) antes de enviar la trama y se verifica en el receptor para asegurarse de que no ocurrieron errores durante la transmisión.

determina qué interfaz se utiliza para reenviar una trama basado en la dirección MAC de destino.

Un switch de capa 2 opera en la capa de enlace de datos del modelo OSI y utiliza las direcciones MAC para decidir a qué puerto reenviar las tramas de datos.

Un switch utiliza la dirección MAC de origen y el puerto de entrada para actualizar su tabla de direcciones MAC, lo que le permite saber a qué puerto está conectado cada dispositivo en la red.

Concepto de Flooding

Cuando un switch recibe una trama de datos, verifica su tabla de direcciones MAC para determinar a qué puerto debe reenviar la trama. Si el switch no encuentra la dirección MAC de destino en su tabla, no sabe a qué puerto específico enviar la trama. En este caso, el switch realiza un flooding de la trama.

Proceso de Flooding

1. **Recepción de la Trama:** El switch recibe una trama de un dispositivo conectado a uno de sus puertos.
2. **Verificación de la Tabla MAC:** El switch examina su tabla de direcciones MAC para encontrar una coincidencia con la dirección MAC de destino.
3. **Falta de Coincidencia:** Si la dirección MAC de destino no está en la tabla (por ejemplo, porque el switch aún no ha aprendido esta dirección), el switch no sabe cuál es el puerto de salida correcto.
4. **Envío a Todos los Puertos:** El switch envía (flooding) la trama a todos los puertos, excepto al puerto por el cual la trama fue recibida originalmente. De esta manera, se asegura de que la trama llegue a su destino, sin importar en qué puerto se encuentre el dispositivo de destino.

Finalidad del Flooding

El flooding permite que los switches de red sigan enviando tramas a sus destinos correctos incluso cuando no tienen información suficiente en sus tablas de direcciones MAC. Con el tiempo, a medida que los dispositivos se comunican en la red, el switch aprenderá las direcciones MAC y sus correspondientes puertos, y podrá reenviar las tramas de manera más eficiente y específica.

Dirección de red y prefijo	Rango de direcciones privadas de RFC 1918
10.0.0.0/8	10.0.0.0 a 10.255.255.255
172.16.0.0/12	172.16.0.0 a 172.31.255.255
192.168.0.0/16	192.168.0.0 a 192.168.255.255

IPV6

IPv6 está diseñado para ser el sucesor de IPv4. IPv6 tiene un espacio de direcciones más grande de 128 bits, que proporciona 340 undecillones (es decir, 340 seguidos de 36 ceros) posibles direcciones. Sin embargo, IPv6 es más que solo direcciones más extensas.

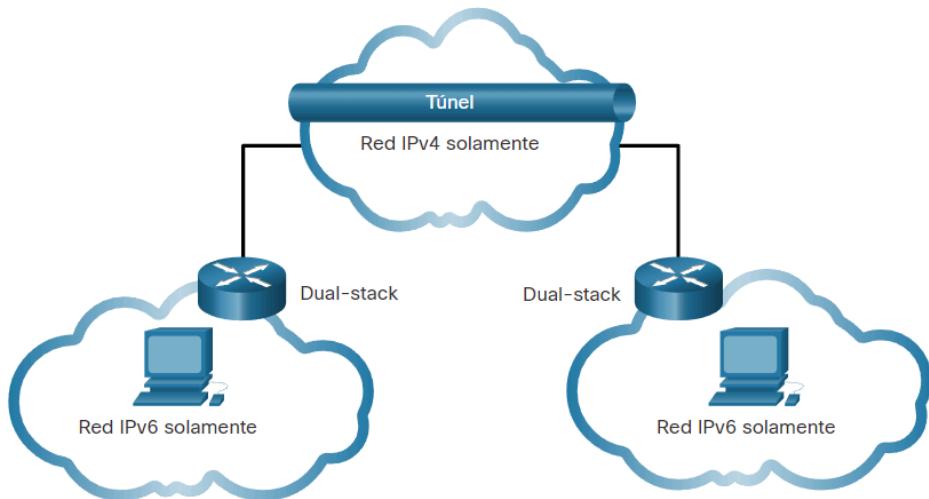
Cuando el IETF comenzó a desarrollar un sucesor de IPv4, aprovechó esta oportunidad para corregir las limitaciones de IPv4 e incluir mejoras. Un ejemplo es el Protocolo de mensajes de control de Internet versión 6 (ICMPv6), que incluye la resolución de direcciones y la configuración automática de direcciones que no se encuentran en ICMP para IPv4 (ICMPv4).

Doble pila

Doble pila permite que IPv4 e IPv6 coexistan en el mismo segmento de red. Los dispositivos dual-stack ejecutan pilas de protocolos IPv4 e IPv6 de manera simultánea. Conocido como IPv6 nativo, esto significa que la red del cliente tiene una conexión IPv6 a su ISP y puede acceder al contenido que se encuentra en Internet a través de IPv6.

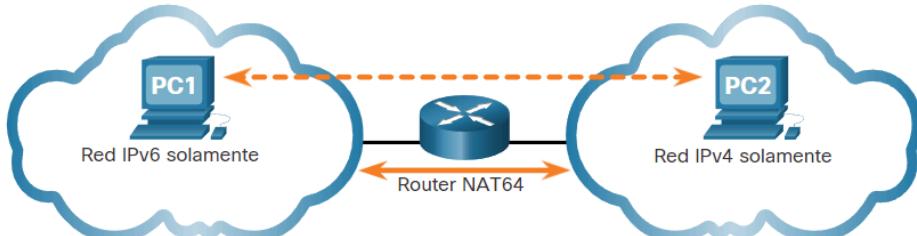
Tunelización

La tunelización es un método para transportar un paquete IPv6 a través de una red IPv4. El paquete IPv6 se encapsula dentro de un paquete IPv4, de manera similar a lo que sucede con otros tipos de datos.



Traducción

La Traducción de Direcciones de Redes 64 (NAT64) permite que los dispositivos con IPv6 habilitado se comuniquen con dispositivos con IPv4 habilitado mediante una técnica de traducción similar a la NAT para IPv4. Un paquete IPv6 se traduce a un paquete IPv4 y un paquete IPv4 se traduce a un paquete IPv6.

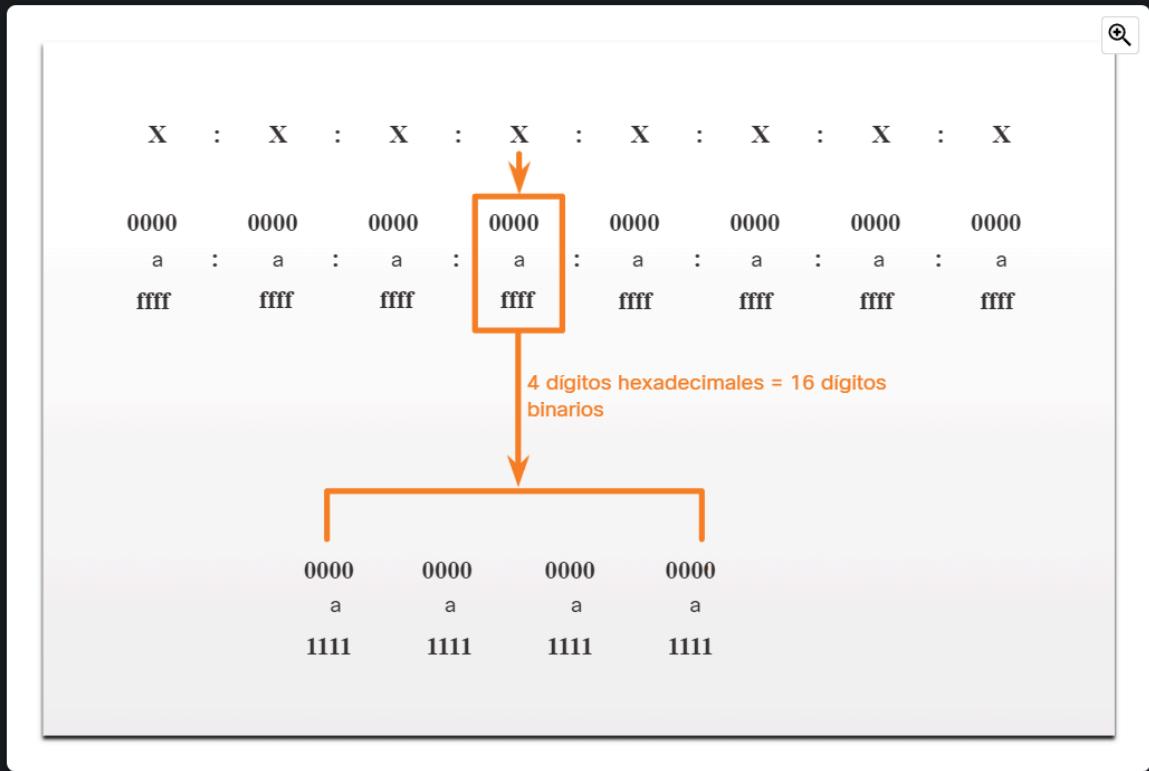


Las direcciones IPv6 usan el sistema hexadecimal

0 1 2 3 4 5 6 7 8 9 A B C D E F

Las direcciones IPv6 tienen una longitud de 128 bits y se escriben como una cadena de valores hexadecimales.

Segmentos o hextetos de 16 bits



Reglas de las direcciones ipv6

Omitir los 0 de la izquierda:

La primera regla para ayudar a reducir la notación de las direcciones IPv6 es omitir los ceros iniciales en cualquier hexteto. Aquí hay cuatro ejemplos de formas de omitir ceros a la izquierda:

- 01ab se puede representar como 1ab
- 09f0 se puede representar como 9f0
- 0a00 se puede representar como a00
- 00ab se puede representar como ab

1. un servidor DHCP que responde a la solicitud inicial de un cliente
- DHCPOFFER
1. el servidor DHCP que confirma que se ha aceptado la concesión de la dirección
- DHCPACK
1. el cliente acepta la dirección IP proporcionada por el servidor DHCP
- DHCPREQUEST
1. un cliente que inicia un mensaje para encontrar un servidor DHCP
- DHCPDISCOVER

¿Qué dos razones generalmente hacen que DHCP sea el método preferido para asignar direcciones IP a hosts en redes grandes? (Elija dos opciones)

Las dos opciones correctas son:

- Elimina la mayoría de los errores de configuración de direcciones.
- Reduce la carga del personal de soporte de la red.

Resumen:

- **Elimina la mayoría de los errores de configuración de direcciones.**
- **Reduce la carga del personal de soporte de la red.**

Enrutadores como puertas de enlace

El enrutador proporciona una puerta de enlace por la cual los hosts de una red pueden comunicarse con los hosts de diferentes redes. Cada interfaz en un enrutador está conectada a una red separada.

La dirección IPv4 asignada a la interfaz identifica qué red local está conectada directamente a ella.

Cada host de una red debe utilizar el router como gateway hacia otras redes. Por lo tanto, cada host debe conocer la dirección IPv4 de la interfaz del enrutador conectada a la red donde el host se encuentra. Esta dirección se conoce como dirección de puerta de enlace predeterminada. Puede configurarse estáticamente en el host o puede recibirse dinámicamente por DHCP.

Cuando un router inalámbrico está configurado para actuar como servidor DHCP para la red local, envía automáticamente la dirección IPv4 de la interfaz correcta a los hosts como la dirección del gateway predeterminado. De esta manera, todos los hosts de la red pueden usar esa dirección IPv4 para enviar mensajes a los hosts ubicados en el ISP y pueden obtener acceso a otros hosts en Internet. Los enrutadores inalámbricos generalmente están configurados en forma predeterminada para actuar como servidores DHCP.

La dirección IPv4 de la interfaz de router local se convierte en la dirección del gateway predeterminado para la configuración del host. La puerta de enlace predeterminada puede proporcionarse estáticamente o por DHCP.

Cuando un router inalámbrico está configurado como servidor DHCP, proporciona su propia dirección IPv4 interna como gateway predeterminado a los clientes DHCP. También les proporciona su dirección IPv4 y máscara de subred correspondientes, tal como se indica en la figura.

Para dos hosts que están en la misma red, ¿cuál de las siguientes afirmaciones es verdadera? (Escoja tres opciones).

Las tres afirmaciones verdaderas son:

1. **Ambos hosts tendrán diferentes direcciones IP.**
 - Cada host en la misma red debe tener una dirección IP única para evitar conflictos de IP.
2. **Ambos hosts tendrán la misma dirección de la puerta de enlace predeterminada.**
 - Los hosts en la misma red generalmente utilizan la misma puerta de enlace predeterminada para acceder a otras redes.
3. **Ambos hosts tendrán diferentes direcciones MAC.**

- Cada dispositivo de red tiene una dirección MAC única asignada por el fabricante.

Para dos hosts, cada uno en una red diferente, ¿cuál de las siguientes afirmaciones es verdadera? (Escoja tres opciones).

Las tres afirmaciones verdaderas son:

1. **Ambos hosts tendrán diferentes direcciones MAC.**
 - Cada dispositivo de red tiene una dirección MAC única asignada por el fabricante.
2. **Ambos hosts tendrán diferentes direcciones IP.**
 - Estar en diferentes redes implica que cada host debe tener una dirección IP única que pertenezca a su respectiva red.
3. **Ambos hosts tendrán diferentes direcciones de puerta de enlace predeterminadas.**
 - Cada red tiene su propio enrutador o puerta de enlace para conectar con otras redes, lo que significa que cada host en diferentes redes tendrá una puerta de enlace predeterminada diferente.

Pregunta 1:

Un equipo tiene que enviar un paquete a un host de destino en la misma LAN. ¿Cómo se enviará el paquete?

La respuesta correcta es:

- **El paquete se enviará directamente al host de destino.**

Pregunta 2:

Por lo general, ¿cuál dispositivo de red se usaría para realizar NAT en un entorno corporativo?

La respuesta correcta es:

- **router**

Pregunta 3:

¿Cuál de las siguientes características describe el entrada predeterminada de un equipo host?

La respuesta correcta es:

- **La dirección lógica de la interfaz del enrutador en la misma red que el equipo host.**

Pregunta 4:

¿Cuál es el propósito de configurar una dirección de gateway predeterminado en un host?

La respuesta correcta es:

- **Identificar el dispositivo que permite que las computadoras de la red local se comuniquen con dispositivos de otras redes.**

Pregunta 5:

Si el gateway predeterminado se configura de forma incorrecta en un host, ¿qué consecuencias tiene esto en las comunicaciones?

La respuesta correcta es:

- **El host no puede comunicarse con hosts en redes remotas.**

Pregunta 6:

¿Qué tres direcciones de red IPv4 son direcciones IP privadas? (Escoja tres opciones).

Las respuestas correctas son:

1. **10.0.0.0**
2. **172.16.0.0**
3. **192.168.0.0**

Cuál es el propósito de NAT?

La respuesta correcta es:

- **traducir direcciones IP privadas a una dirección IP pública registrada**

Pregunta 8:

¿Cuál es la principal ventaja de usar NAT?

La respuesta correcta es:

- **permite que un gran grupo de usuarios comparta una o más direcciones IP públicas**

Pregunta 9:

¿Qué tres configuraciones se deben configurar en una PC para que se comunique con dispositivos ubicados en Internet? (Elija tres opciones).

Las respuestas correctas son:

1. **dirección IP**
2. **máscara de subred**
3. **Dirección de puerta de enlace predeterminada (gateway)**

Pregunta 10:

¿Qué tipo de direcciones proporcionan la configuración predeterminada en un enrutador inalámbrico doméstico a los dispositivos que usan DHCP?

La respuesta correcta es:

- **direcciones IP privadas**

Pregunta 11:

¿Qué tipo de dispositivo intermediario actúa como límite entre una red inalámbrica doméstica e Internet?

La respuesta correcta es:

- **enrutador inalámbrico**

MAC y IP

¿Qué dirección MAC de destino se incluiría en una trama enviada desde un dispositivo de origen a un dispositivo de destino en la misma red local?

La respuesta correcta es:

- **La dirección MAC del dispositivo de destino.**

Pregunta 2:

¿Qué dirección MAC de destino se incluiría en una trama enviada desde un dispositivo de origen a un dispositivo de destino en una red local remota?

La respuesta correcta es:

- La dirección MAC de la interfaz del router local.

Pregunta 3:

¿Qué dos protocolos se utilizan para determinar la dirección MAC de una dirección IP de un dispositivo de destino conocido (IPv4 e IPv6)?

Las respuestas correctas son:

- ARP (Address Resolution Protocol) para IPv4
- ND (Neighbor Discovery) para IPv6

ARP

ARP utiliza un proceso de tres pasos para determinar y almacenar la dirección MAC de un host que se encuentre en la red local cuando se conoce solo la dirección IPv4 del host:

1. El host emisor crea una trama dirigida a una dirección MAC de difusión y la envía. En la trama hay un mensaje con la dirección IPv4 del host de destino que se desea encontrar.
2. Cada host de la red recibe la trama de difusión y compara la dirección IPv4 del mensaje con su dirección IPv4 configurada. El host con la dirección IPv4 coincidente envía su dirección MAC como respuesta al host emisor original.
3. El host emisor recibe el mensaje y almacena la información de la dirección MAC y la dirección IPv4 en una tabla, denominada tabla ARP.

Enrutamiento entre redes

Pregunta 1:

¿Qué información utilizan los routers para reenviar un paquete de datos hacia su destino?

La respuesta correcta es:

- dirección IP de destino

Pregunta 2:

Si el gateway predeterminado se configura de forma incorrecta en un host, ¿qué consecuencias tiene esto en las comunicaciones?

La respuesta correcta es:

- El host no puede comunicarse con hosts en redes remotas.

Pregunta 3:

¿Qué rol desempeña un router en una red?

La respuesta correcta es:

- **reenviar tramas basadas en una dirección MAC** (*la respuesta podría estar mal planteada en las opciones, ya que los routers reenvían basados en direcciones IP, no MAC*).

Pregunta 4:

¿Qué dirección debe configurarse como la dirección de puerta de enlace predeterminada de un dispositivo cliente?

La respuesta correcta es:

- **La dirección IPv4 de la interfaz del enrutador que está conectada a la red LAN.**

Pregunta 5:

¿Qué dispositivo se utiliza para transferir datos de una red local (LAN) a una red remota?

La respuesta correcta es:

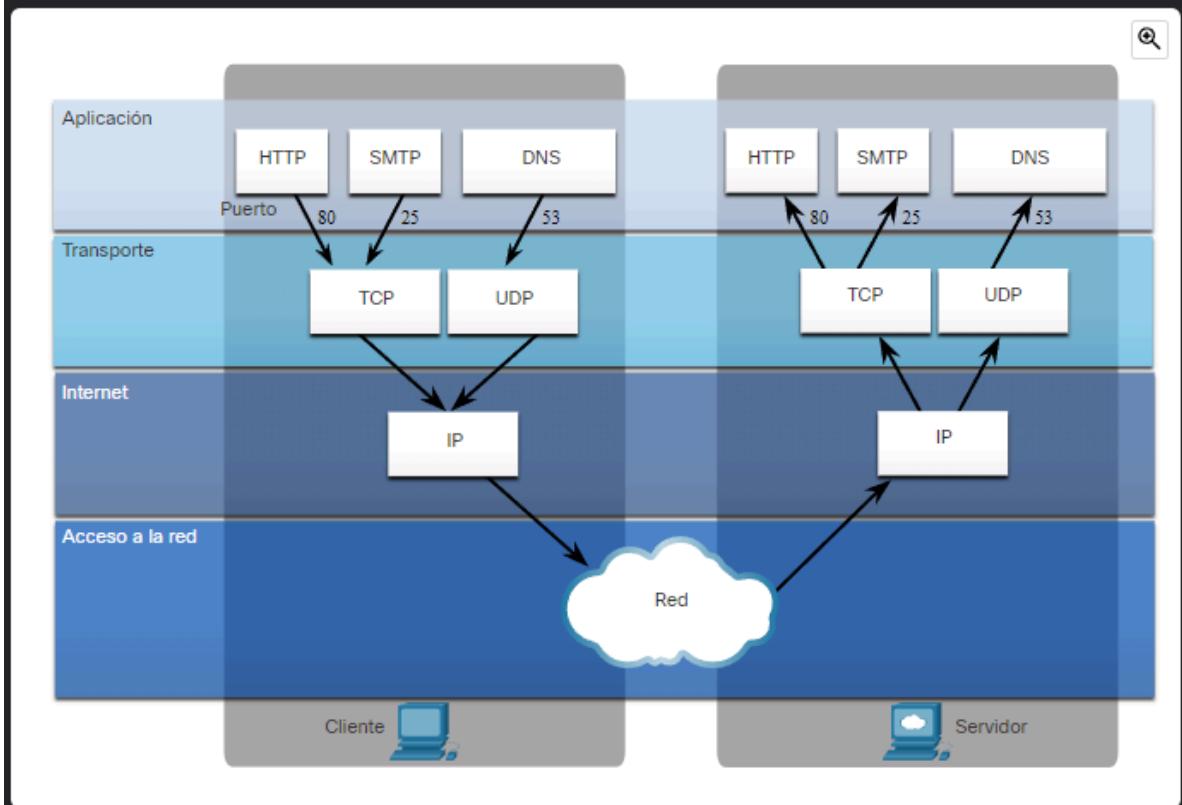
- **enrutador**

La capa de transporte en los modelos TCP/IP y OSI es responsable de garantizar que los paquetes se envíen de manera confiable y se reenvíen los paquetes faltantes.

15.2.2 Números de Puerto TCP y UDP

Accedemos a gran cantidad de servicios a través de internet durante el día. DNS, web, correo electrónico, FTP, IM y VoIP son solo algunos de estos servicios que proporcionan los sistemas cliente-servidor en todo el mundo. Estos servicios pueden ser prestados por un solo servidor o por muchos servidores en grandes centros de datos.

Cuando se entrega un mensaje mediante TCP o UDP, los protocolos y servicios solicitados se identifican mediante un número de puerto, como se muestra en la figura. Un puerto es un identificador numérico dentro de cada segmento, que se usa para llevar un seguimiento de las conversaciones específicas entre un cliente y un servidor. Cada mensaje que envía un host contiene un puerto de origen y un puerto de destino.



Cuando un servidor recibe un mensaje, tiene que poder determinar qué servicio está solicitando el cliente. Los clientes se pre-configuran para usar un puerto de destino que ya está registrado en Internet para cada servicio. Un ejemplo de esto son los clientes de navegador web que están preconfigurados para enviar solicitudes a servidores web por medio de puerto 80, el puerto conocido para servicios web de HTTP.

Los puertos son asignados y administrados por una organización conocida como la Corporación de Internet para Nombres y Números Asignados (Internet Corporation for Assigned Names and Numbers, ICANN). Los puertos se dividen en tres categorías y van de 1 a 65 535:

- **Puertos Conocidos** - Los puertos de destino que están asociados con aplicaciones de red comunes se identifican como puertos conocidos. Estos puertos están en el rango de 1 a 1023.
- **Puertos Registrados** - Los puertos 1024 a 49151 pueden usarse como puertos de origen o de destino. Las organizaciones los utilizan para registrar aplicaciones específicas, como las aplicaciones IM.
- **Puertos Privados** - Los puertos 49152 a 65535, usados frecuentemente como puertos de origen. Estos puertos pueden ser utilizados por cualquier aplicación.

La tabla muestra algunos números de puerto conocidos y sus aplicaciones asociadas.

Número de puerto	Transporte	Protocolo de aplicación
20	TCP	Protocolo de transferencia de archivos (FTP) - Datos
21	TCP	FTP - Control
22	TCP	Secure Shell (SSH)
23	TCP	Telnet
25	TCP	Protocolo simple de transferencia de correo (SMTP)
53	UDP, TCP	Servicio de nombres de dominio (DNS, Domain Name Service)
67	UDP	Protocolo de configuración dinámica de host (DHCP): servidor
68	UDP	DHCP - Cliente
69	UDP	Protocolo trivial de transferencia de archivos (TFTP)
80	TCP	Protocolo de transferencia de hipertexto (HTTP)
110	TCP	Protocolo de oficina de correos, versión 3 (POP3)
143	TCP	Protocolo de acceso a mensajes de Internet (IMAP)
161	UDP	Protocolo simple de administración de redes (SNMP)
443	TCP	Protocolo seguro de transferencia de hipertexto (HTTPS)

Pregunta 6

¿Qué información de encabezado de protocolo se utiliza en la capa de transporte para identificar una aplicación de destino?

Las opciones son:

- número de puerto
- dirección IP
- número de secuencia

- dirección MAC

Respuesta correcta: número de puerto

En la capa de transporte, los números de puerto se utilizan para identificar a qué aplicación de destino debe entregarse un segmento de datos.

Pregunta 7

¿Qué tipo de número de puerto asigna IANA a los servicios y las aplicaciones de uso común?

Las opciones son:

- puerto conocidos
- puerto registrado
- puerto dinámico
- puerto privado

Respuesta correcta: puerto conocidos

La IANA (Internet Assigned Numbers Authority) asigna números de puerto conocidos (well-known ports) a servicios y aplicaciones de uso común. Estos puertos están en el rango del 0 al 1023.

Pregunta 8

¿Cuál es el propósito de usar un número de puerto de origen en una comunicación TCP?

Las opciones son:

- para notificar al dispositivo remoto que la conversación ha terminado
- para ensamblar los segmentos que llegaron fuera de servicio
- para realizar un seguimiento de múltiples conversaciones entre dispositivos
- para consultar un segmento no recibido

Respuesta correcta: para realizar un seguimiento de múltiples conversaciones entre dispositivos

El número de puerto de origen, junto con el número de puerto de destino, permite que TCP mantenga múltiples conversaciones entre dispositivos diferentes.

Pregunta 9

¿Cuál es la ventaja de UDP sobre TCP?

Las opciones son:

- La comunicación UDP requiere menos sobrecarga.
- La comunicación UDP es más confiable.
- UDP reordena los segmentos que se reciben fuera de servicio.
- UDP acusa (confirma) los datos recibidos.

Respuesta correcta: La comunicación UDP requiere menos sobrecarga.

UDP (User Datagram Protocol) tiene una menor sobrecarga comparada con TCP, ya que no proporciona confirmaciones, reordenamiento de segmentos, o control de flujo, lo cual hace que sea más rápido pero menos confiable.

Pregunta 10

¿Cuándo se prefiere UDP a TCP?

Las opciones son:

- cuando un cliente envía un segmento a un servidor
- cuando todos los datos deben recibirse por completo antes de que cualquier parte se considere útil
- cuando una aplicación puede tolerar cierta pérdida de datos durante la transmisión
- cuando los segmentos deben llegar en una secuencia muy específica para ser procesados con éxito

Respuesta correcta: cuando una aplicación puede tolerar cierta pérdida de datos durante la transmisión

UDP se prefiere en aplicaciones donde la pérdida de algunos datos es tolerable, como en la transmisión de video o voz en tiempo real.

Pregunta 11

¿Qué enunciado describe correctamente la transmisión de datos en la capa de transporte?

Las opciones son:

- La retransmisión de paquetes perdidos es proporcionada por TCP y UDP.
- La segmentación la proporciona el campo de tamaño de ventana cuando se utiliza el protocolo TCP.
- Un solo datagrama puede incluir un encabezado TCP y UDP.
- Tanto UDP como TCP utilizan números de puerto.
- La segmentación se proporciona por números de secuencia cuando se utiliza UDP.

Respuesta correcta: Tanto UDP como TCP utilizan números de puerto.

Tanto TCP como UDP utilizan números de puerto para identificar las aplicaciones de origen y destino de los datos que se están transmitiendo.

16.1.3 URI, URN, y URL

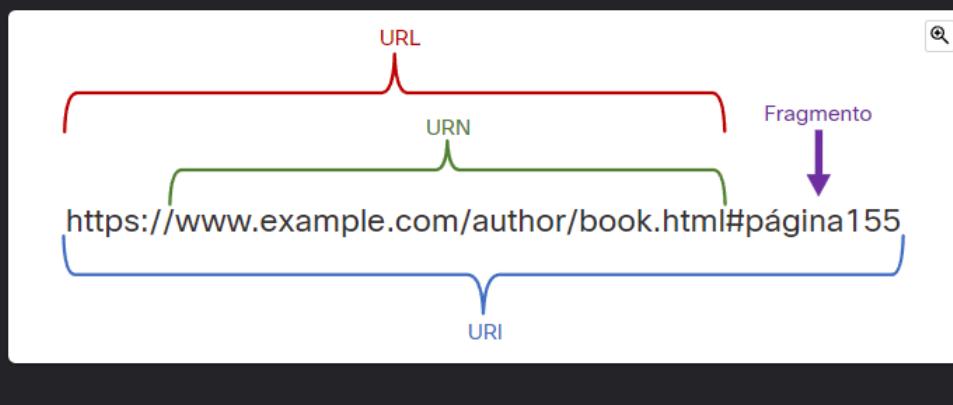
Los recursos web y los servicios web, como las API RESTful, se identifican mediante un Identificador Uniforme de Recursos (Uniform Resource Identifier, URI). Un URI es una cadena de caracteres que identifica un recurso de red específico. Como se muestra en la figura, un URI tiene dos especializaciones:

- **Nombre uniforme de recurso (URN)** - Identifica solo el espacio de nombres del recurso (página web, documento, imagen, etc.) sin referencia al protocolo.
- **Localizador uniforme de recursos (URL)** - Define la ubicación de red de un recurso específico en la red. Las URL HTTP o HTTPS se utilizan normalmente con los navegadores web. Otros protocolos como FTP, SFTP, SSH y otros pueden usarse como URL. Una URL que usa SFTP podría tener el siguiente aspecto: sftp://sftp.example.com.

Estas son las partes de un URI, tal y como se muestra en la figura:

- **Protocolo/esquema** – HTTPS u otros protocolos como FTP, SFTP, mailto y NNTP
- **Nombre de host** – www.example.com
- **Ruta y nombre de archivo** – /author/book.html
- **Fragmento** – #página155

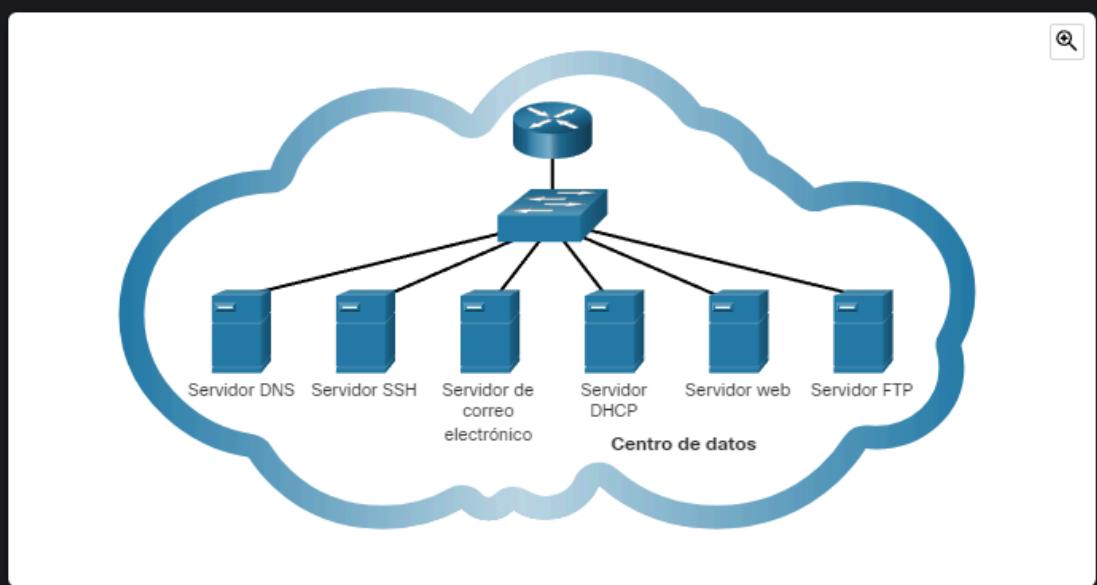
Partes de un URI



16.2.1 Servicios de Aplicaciones de Red Comunes

¿Cuáles son los servicios de Internet más comunes que utiliza periódicamente? Para la mayoría de las personas, la lista incluye servicios como búsquedas en Internet, sitios de redes sociales, transmisión de video y audio, sitios de compras en línea, correo electrónico y mensajería. Cada uno de estos servicios depende de los protocolos de la suite de protocolos TCP/IP para transmitir de manera confiable la información entre los clientes y los servidores.

Algunos de los servidores más comunes que proporcionan estos servicios se muestran en la figura. En la tabla se muestra una breve descripción de cada servicio.



Protocolo	Descripción
Sistema de nombres de dominio (DNS)	recupera los mensajes de correo electrónico de los clientes.
Secure Shell (SSH)	Se utiliza para proporcionar acceso remoto a servidores y dispositivos de red.
Protocolo simple de transferencia de correo (SMTP)	Envía mensajes de correo electrónico y archivos adjuntos de clientes a servidores y de servidores a otros servidores de correo electrónico.
Protocolo de oficina de correos (POP)	Utilizado por clientes de correo electrónico para recuperar correos electrónicos y archivos adjuntos desde un servidor remoto.
Protocolo de acceso a mensajes de Internet (IMAP)	Utilizado por clientes de correo electrónico para recuperar correos electrónicos y archivos adjuntos desde un servidor remoto.
Protocolo de configuración dinámica de host (DHCP)	Se utiliza para configurar automáticamente dispositivos con direccionamiento IP y otra información necesaria para permitirles comunicarse a través de Internet.
Protocolo de transferencia de hipertexto (HTTP)	Utilizado por los navegadores web para solicitar páginas web y servidores web para transferir los archivos que conforman las páginas web de la World Wide Web.
Protocolo de transferencia de archivos (FTP)	Se utiliza para la transferencia interactiva de archivos entre sistemas.

Redes privadas virtuales VPN

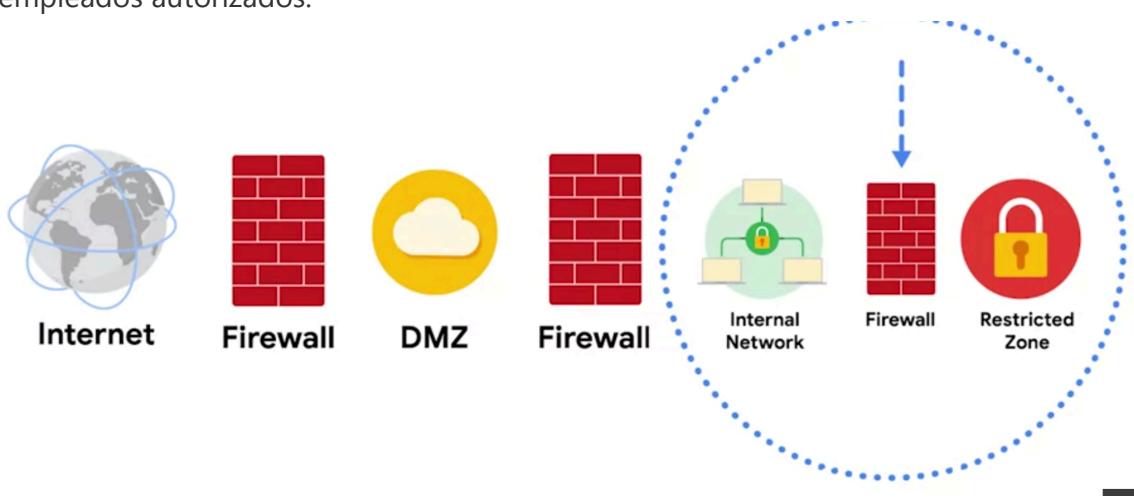
- Agregan seguridad a tu red
- Es un servicio de seguridad que cambia tu dirección IP pública y oculta tu ubicación actual por una virtual para proteger tus datos al usar una red pública como internet
- También cifra datos al transferirlos para protegerlos
- Encapsula los datos de tránsito.

Zonas de seguridad

Es un segmento de una red que protege la red interna del internet, esta forma parte de una técnica de seguridad llamada segmentación de red, que divide la red en segmentos. Cada uno tiene sus propios permisos de acceso y reglas de seguridad. Actúa como una barrera para las redes internas, protegiendo la privacidad en los grupos corporativos y evitar que los problemas se extiendan a otras redes.

Tipos de redes en la zona controlada

- Zona desmilitarizada o DMZ : la cual contiene servicios públicos que acceden al internet, incluye servidores web, servidores proxy que alojan sitios públicos y servidores DNS que asignan direcciones IP a usuarios del internet, el DMZ actúa como un perímetro de red para la red interna.
- Servidores como correo y archivos para la comunicación externa
- La red interna tiene servidores privados y datos que la empresa necesita proteger. En la red interna, hay otra zona llamada zona restringida
- Zona restringida.: Esta protege la información confidencial que solo pueden ver empleados autorizados.
-



Redes virtuales y privacidad

Protocolos de red comunes

Los protocolos de red desempeñan un papel fundamental para dirigir el tráfico hacia los dispositivos y servicios adecuados, teniendo en cuenta el tipo de comunicación que se lleva a cabo entre los dispositivos de una red. Estos protocolos son conjuntos de reglas aceptadas universalmente por todos los dispositivos de red, que establecen una base común sobre cómo se deben transferir los datos a través de una red.

Existen tres categorías principales protocolos de red: protocolos de comunicación, de gestión y de seguridad.

1. Los protocolos de comunicación se utilizan para establecer conexiones entre servidores. Algunos ejemplos son TCP, UDP y SMTP, que proporciona un marco para la comunicación por correo electrónico.
2. Los protocolos de gestión, en cambio, se utilizan para solucionar problemas de red. Un ejemplo es el protocolo de mensajes de control de Internet (ICMP).
3. En tanto, los protocolos de seguridad proporcionan cifrado para datos en tránsito. Algunos ejemplos incluyen IPSec y SSL/TLS.

A continuación, se mencionan otros protocolos de uso común:

- Protocolo de transferencia de hipertexto (HTTP). El HTTP es un protocolo de comunicación de capa de aplicación. Esto permite que el navegador y el servidor web se comuniquen entre sí.
- Sistema de nombres de dominio (DNS). El DNS es un protocolo de capa de aplicación que traduce, o mapea, nombres de host a direcciones IP.
- Protocolo de resolución de direcciones (ARP). El ARP es un protocolo de comunicación de capa de red que asigna direcciones IP a máquinas físicas o una dirección de control de acceso al medio (MAC) reconocida en la red de área local.

Wi-Fi

En esta sección del curso, también te presentamos varios protocolos de seguridad inalámbricos, incluidos la privacidad equivalente por cable (WEP), el acceso Wi-Fi protegido (WPA), el WPA2 y el WPA3. El WPA3 cifra el tráfico con el cifrado del Advanced Encryption Standard (AES) a medida que avanza desde el dispositivo hasta el punto de acceso inalámbrico. El WPA2 y el WPA3 ofrecen dos modos: personal y empresarial. El modo personal es el más adecuado para redes domésticas, mientras que el empresarial suele utilizarse para redes y aplicaciones corporativas.

Herramientas y prácticas de seguridad de redes

Cortafuegos (firewalls)

Anteriormente, aprendiste que los cortafuegos (firewalls) son dispositivos virtuales de red (NVA) o dispositivos de hardware que inspeccionan y pueden filtrar el tráfico de red antes de permitir su ingreso a la red privada. Los firewalls tradicionales se configuran con reglas que determinan qué tipos de paquetes de datos se permiten, en función del número de puerto y la dirección IP del paquete.

Existen dos categorías principales de cortafuegos (firewalls).

- **Cortafuegos Stateless (gestión sin estado):** un tipo de cortafuegos que funciona según reglas predefinidas y no hace un seguimiento a la información de los paquetes de datos.
- **Cortafuegos Stateful (gestión con estado):** un tipo de cortafuegos que hace un seguimiento de la información que pasa a través de este y filtra proactivamente las amenazas. A diferencia de los cortafuegos sin estado, que requieren que las reglas se configuren en ambas direcciones, un firewall con estado solo necesita una regla en una dirección. Esto se debe a que utiliza una "tabla de estados" para hacer un seguimiento de las conexiones, lo que le permite asociar el tráfico de retorno con una sesión existente.

Los cortafuegos de última generación (NGFW) son la protección de firewall con tecnología más avanzada. Superan la seguridad ofrecida por los cortafuegos Stateful (con estado) porque incluyen inspección profunda de paquetes (una especie de rastreo de paquetes que los examina y toma medidas si existen amenazas) y funciones de prevención de intrusiones que detectan amenazas de seguridad y notifican a quienes administran los cortafuegos. Los NGFW pueden inspeccionar el tráfico en la capa de aplicación del modelo TCP/IP y su compatibilidad suele depender de la aplicación. A diferencia de los firewalls tradicionales que bloquean el tráfico según las direcciones IP y los puertos, las reglas de los NGFW pueden configurarse para bloquear o permitir el tráfico en función de la aplicación. Algunos NGFW tienen funciones adicionales como sandboxing (entorno controlado) contra malware, antivirus de red y filtrado de URL y DNS.

Servidores proxy

Otra manera de agregar seguridad a una red privada es mediante un servidor proxy. Estos servidores utilizan la traducción de direcciones de red (NAT) para actuar como una barrera entre los clientes en la red y las amenazas externas. Los servidores proxy directos manejan consultas de clientes internos cuando acceden a recursos externos a la red. Por otro lado, los servidores proxy inversos funcionan de manera opuesta, manejando las solicitudes provenientes de sistemas externos hacia los servicios en la red interna. Además, algunos servidores proxy se pueden configurar con reglas similares a un cortafuegos. Por ejemplo, es posible crear filtros para bloquear sitios web identificados como portadores de malware.

Redes privadas virtuales (VPN)

Una VPN es un servicio que cifra los datos en tránsito y oculta la dirección IP. Utiliza un proceso llamado encapsulación, en el que los datos encriptados se envuelven en paquetes de datos sin cifrar. Esto permite que los datos se transmitan a través de la red pública de forma anónima. Las VPN se utilizan en empresas y otras organizaciones para proteger las comunicaciones entre los dispositivos de los/las usuarios/as y los recursos corporativos, como servidores o equipos virtuales que alojan aplicaciones empresariales. También se pueden usar de manera personal para aumentar la privacidad, ya que permiten a los/las usuarios/as acceder a Internet sin que nadie pueda leer la información personal ni acceder a la dirección IP privada. Cada vez más, las organizaciones están adoptando una

combinación de capacidades VPN y SD-WAN para garantizar la seguridad de sus redes. Una red de área amplia definida por software (SD-WAN) es un servicio WAN virtual que permite a las organizaciones conectar de forma segura a los/las usuarios/as con aplicaciones, en múltiples ubicaciones y a grandes distancias

Reforzamiento de seguridad

Es el proceso de reforzar un sistema para reducir su vulnerabilidad y superficie de ataque

Superficie de ataque: se le denomina a las vulnerabilidades potenciales que un atacante puede utilizar.

La seguridad se refuerza en cualquier dispositivo o sistema que pueda verse comprometido

Pentest o prueba de penetración: es un ataque simulado que identifica vulnerabilidades en un sistema, red, sitio web, aplicación y proceso.

Reforzamiento en la nube

La computación en la nube es un modelo para permitir el acceso a la red conveniente y bajo demanda de un grupo compartido de recursos informáticos configurables. Estos se pueden configurar y liberar con un mínimo esfuerzo de gestión o interacción con el proveedor de servicios.

- **Asegurar el acceso:** Controlar quién puede acceder a los recursos de la nube mediante contraseñas seguras, autenticación multifactor y gestión de identidades y accesos (IAM).
- **Cifrado de datos:** Proteger los datos en reposo y en tránsito utilizando algoritmos de cifrado robustos.
- **Protección contra malware:** Implementar soluciones antimalware para detectar y prevenir amenazas.
- **Monitoreo de seguridad:** Supervisar continuamente la actividad de la red en busca de comportamientos sospechosos y responder a los incidentes de seguridad de manera oportuna.
- **Actualizaciones de seguridad:** Mantener el software y las aplicaciones actualizadas con los últimos parches de seguridad.

Consideraciones de seguridad en la nube

Muchas organizaciones eligen usar servicios en la nube debido a la facilidad y velocidad de implementación, el ahorro de costos y la escalabilidad. La computación en la nube

presenta desafíos de seguridad únicos que las/los analistas de ciberseguridad deben tener en cuenta.

Gestión de identidad y acceso

La **gestión de identidad y acceso (IAM)** es el conjunto de procesos y tecnologías que ayuda a las organizaciones a gestionar las identidades digitales en su entorno. Este servicio también autoriza el modo en que los/las usuarios/as pueden usar diferentes recursos de la nube. Un problema común que enfrentan las organizaciones cuando usan la nube es la configuración flexible de los roles de usuario en ese entorno. Un rol de usuario configurado incorrectamente aumenta el riesgo al permitir que usuarios no autorizados tengan acceso a operaciones críticas en la nube.

Configuración

La cantidad de servicios disponibles en la nube agrega complejidad a la red. Cada servicio debe configurarse cuidadosamente para satisfacer los requisitos de seguridad y cumplimiento normativo. Esto presenta un desafío particular cuando las organizaciones realizan una migración inicial a la nube. Cuando se produce este cambio en su red, deben asegurarse de que todos los procesos trasladados a la nube se hayan configurado correctamente. Si los/las administradores/as y arquitectos/as de red no son meticulosos/as en la configuración correcta de los servicios en la nube de la organización, podrían dejar la red abierta a riesgos. La mala configuración de los en la nube son una fuente común de problemas de seguridad en ese entorno.

Superficie de ataque

Los proveedores de servicios en la nube (CSP) ofrecen a las organizaciones numerosas aplicaciones y servicios a un bajo costo.

Cada servicio o aplicación en una red conlleva su propio conjunto de riesgos y vulnerabilidades y aumenta la superficie de ataque general de una organización. Una mayor superficie de ataque debe compensarse con mayores medidas de seguridad. Las redes en la nube que utilizan varios servicios abren muchos puntos de entrada en la red de una organización. Sin embargo, si la red está diseñada correctamente, el uso de múltiples servicios no genera nuevos puntos de entrada en el diseño de la red. Estos puntos de entrada se pueden utilizar para introducir malware en la red y plantear otras vulnerabilidades de seguridad. Es importante tener en cuenta que los CSP suelen diferir de las opciones más seguras, y se los ha analizado más que a una red local tradicional.

Ataques de día cero

Los ataques de día cero son una consideración de seguridad importante para las organizaciones que utilizan soluciones de red en la nube o redes locales tradicionales. Un ataque de **día cero** es un exploit (o sea, un fragmento de software o secuencia de comandos que se aprovecha de un error o vulnerabilidad) que antes era desconocido. Los CSP tienen más probabilidades de advertir un ataque de día cero antes que una organización de TI tradicional. Los CSP tienen formas de parchear hipervisores (software capaz de crear y ejecutar máquinas virtuales) y migrar cargas de trabajo a otras máquinas virtuales. Estos métodos aseguran que los/las clientes no se vean afectados/as por el

ataque. También las organizaciones pueden usar otras herramientas disponibles como parches a nivel de sistema operativo.

Visibilidad y seguimiento

Los/las administradores/as de red tienen acceso a todos los paquetes de datos que cruzan las redes locales y de la nube. Pueden rastrear e inspeccionar paquetes de datos para obtener información sobre el rendimiento de la red o para comprobar posibles amenazas y ataques.

Este tipo de visibilidad también se ofrece en la nube a través de registros de flujo y herramientas, como la duplicación de paquetes (packet mirroring). Los CSP asumen la responsabilidad de la seguridad en la nube, pero no permiten que las organizaciones que utilizan su infraestructura monitorean el tráfico en los servidores de proveedores de servicio en la nube. Si bien muchos CSP ofrecen fuertes medidas de seguridad para proteger su infraestructura, esta situación podría ser una preocupación para las organizaciones que están acostumbradas a tener acceso completo a su red y operaciones. Los proveedores de servicio en la nube pagan por auditorías de terceros para verificar el grado de seguridad de una red e identificar posibles vulnerabilidades. Estas pueden ayudar a las organizaciones a identificar si alguna vulnerabilidad se origina en la infraestructura local y si hay fallas de cumplimiento de su CSP.

Velocidad de los cambios en la nube

Los CSP son grandes organizaciones que se esfuerzan para mantenerse al día respecto de los avances tecnológicos. Para las organizaciones que están acostumbradas a tener el control de cualquier ajuste realizado en su red, esto puede ser un posible desafío. Las actualizaciones de servicios en la nube pueden afectar la seguridad de las organizaciones que las utilizan. Por ejemplo, es posible que sea necesario cambiar las configuraciones de conexión en función de las actualizaciones del CSP.

Las organizaciones que utilizan CSP generalmente tienen que actualizar sus procesos de TI. Aunque es posible que estas sigan las mejores prácticas establecidas para cambios, configuraciones y otras consideraciones de seguridad, podrían tener que adoptar un enfoque diferente para alinearse con los cambios realizados por el CSP.

Además, las redes en la nube ofrecen varias opciones que pueden parecer atractivas para una pequeña empresa, que nunca podría permitirse construir en sus propias instalaciones. Sin embargo, es importante tener en cuenta que cada servicio agrega complejidad al perfil de seguridad de la organización, y necesitará personal de seguridad para monitorear todos los servicios en la nube.

Modelo de responsabilidad compartida

Un principio de seguridad en la nube comúnmente aceptado es el **modelo de responsabilidad compartida**. Este establece que el CSP debe asumir la responsabilidad de la seguridad que involucra la infraestructura de la nube, incluidos los centros de datos físicos, los hipervisores y los sistemas operativos host. Por su parte, la empresa que utiliza

el servicio en la nube es responsable de los activos y procesos que almacenan u operan en la nube.

El modelo de responsabilidad compartida garantiza que tanto el CSP como los/las usuarios/as estén de acuerdo acerca de dónde comienza y dónde termina su responsabilidad respecto de la seguridad. Es importante tener esto en claro porque, si las organizaciones asumen que el CSP está encargándose de una instancia de seguridad por la que ellos no se han hecho responsables, puede ser un problema. Un ejemplo de esto tiene que ver con las aplicaciones y configuraciones en la nube. El CSP asume la responsabilidad de proteger la nube, pero la organización debe encargarse de garantizar que los servicios se configuren correctamente de acuerdo con los requisitos de seguridad de su organización.

Registros y herramientas SIEM

Un registro recopila eventos que ocurren dentro de los sistemas y redes de una organización

Algunos de los tipos de registros mas comunes son:

Registros del firewall

Registros de red

Registros de servidor

Tambien se registran las conexiones entre dispositivos y servicios de la red

El registro del servidor es un registro de eventos relacionados con servicios , como sitios web, correos electronicos o archivos compartidos.Mediante el monitoreo de registros o SIEM se basa en estos para monitorear las actividades criticas de una organizacion.

Las metricas son atributos tecnicos clave como el tiempo de respuesta, la disponibilidad y la taza de errores que se usan para evaluar el rendimiento de una aplicacion de software

Retroalimentacion examen

1. ¿Qué software se usa para recopilar y enviar registros a una herramienta de gestión de datos e información de seguridad (SIEM)?

0 / 1 punto

- Reenviador
- Firewall
- Sistema de detección de intrusiones (IDS)
- Analizador de protocolos de red

 Incorrecto

Revisa el [video sobre registros](#).

2. Examina el registro siguiente:

1 / 1 punto

```
LoginEvent[2021/10/13 10:32:08.958711] auth_session_authenticator.cc:304 Regular user  
login 1
```

¿De qué tipo de registro se trata?

- Red
- Aplicación
- Ubicación
- Autenticación

 Correcto

3. Examina el registro siguiente:

0 / 1 punto

```
<111>1 2020-04-12T23:20:50.52Z my.machine.com evntslog - ID01[user@98274 iut="2"  
eventSource="Mobile" eventID="24"] [Priority@98274 class="low"] Computer A
```

¿Qué valor de campo indica el tipo de dispositivo desde el que se originó este evento?

- low
- Computer A
- my.machine.com
- Mobile

 Incorrecto

Revisa el [video sobre formatos de registro](#).

4. ¿Cuál es la diferencia entre un sistema de detección de intrusiones basado en la red (NIDS) y un sistema de detección de intrusiones basado en host (HIDS)?

1 / 1 punto

- Un NIDS monitorea la actividad del host en el que está instalado. Un HIDS utiliza análisis de firmas para analizar la actividad de la red.
- Un NIDS registra y genera alertas. Un sistema HIDS monitorea la actividad de los puntos de conexión.
- Tanto un NIDS como un HIDS supervisan sistemas y generan alertas, pero un NIDS usa agentes.
- Un NIDS recopila y supervisa el tráfico de red y los datos de red. Un HIDS monitorea la actividad del host en el que está instalado.

 Correcto

5. ¿Qué información se incluye en el encabezado de una firma? Selecciona todas las opciones que correspondan.

1 / 1 punto

- Acción
- Número de puerto
- Correcto**
- Protocolo
- Correcto**
- Dirección IP
- Correcto**

6. ¿Qué opción de regla se usa para asociación, según la dirección del tráfico de red?

1 / 1 punto

- sid
- message
- flow
- content

Correcto

7. ¿Qué tipo de datos de registro genera Suricata? Selecciona todas las opciones que correspondan.

0.25 / 1 punto

- Telemetría de red
- Correcto**
- Alerta
- Protocolo
- (X) Esto no debería estar seleccionado**
Revisa el [video sobre registros de Suricata](#).
- Firma
- (X) Esto no debería estar seleccionado**
Revisa el [video sobre registros de Suricata](#).

7. ¿Qué tipo de datos de registro genera Suricata? Selecciona todas las opciones que correspondan.

0.25 / 1 punto

Telemetría de red

Correcto

Alerta

Protocolo

(X) Esto no debería estar seleccionado

Revisa el [video sobre registros de Suricata](#).

Firma

(X) Esto no debería estar seleccionado

Revisa el [video sobre registros de Suricata](#).

8. ¿Qué lenguaje de consulta usa Splunk?

1 / 1 punto

Lenguaje de procesamiento de búsqueda

Lenguaje de procesamiento estructurado

Lenguaje de procesamiento SIEM

Lenguaje de consulta estructurado

Correcto

9. Completa el espacio en blanco: Chronicle usa _____ para definir las reglas de detección.

1 / 1 punto

YARA-L

SPL

UDM

SQL

Correcto

10. Completa el espacio en blanco: Las herramientas SIEM _____ datos sin procesar para que tengan un formato consistente.

1 / 1 punto

normalizan

recopilan

procesan

introducen

Correcto

1. ¿Cuál de las siguientes opciones hace referencia a un registro de eventos que tienen lugar en los sistemas de una organización?

1 / 1 punto

- Fuentes de registros
- Registros
- Reenviador de registros
- Sucesos

 Correcto

2. ¿Cuál es la diferencia entre un registro y un análisis de registros?

1 / 1 punto

- Un registro es un historial de eventos que tienen lugar en los sistemas de una organización. El análisis de registros es el proceso de examinar los registros para identificar eventos de interés.
- Un registro realiza un inventario de detalles en archivos de registro. El análisis de registros implica una descripción de alto nivel de todos los eventos que ocurren en la red.
- Un registro contiene detalles de archivos de registro. El análisis de registros involucra la recopilación y el almacenamiento de registros.
- Tanto un registro como un análisis de registros contienen detalles de eventos, pero registran detalles de distintas fuentes.

 Correcto

3. Completa el espacio en blanco: Una entrada de syslog contiene un encabezado, _____ y un mensaje.

0 / 1 punto

- datos estructurados
- etiqueta
- lenguaje de marcado extensible
- objeto

 Incorrecto

Revisa el [video sobre formatos de registro](#).

4. ¿Cuál es la diferencia entre un sistema de detección de intrusiones basado en la red (NIDS) y un sistema de detección de intrusiones basado en host (HIDS)?

1 / 1 punto

- Un NIDS monitorea la actividad del host en el que está instalado. Un HIDS utiliza análisis de firmas para analizar la actividad de la red.
- Un NIDS recopila y supervisa el tráfico de red y los datos de red. Un HIDS monitorea la actividad del host en el que está instalado.
- Tanto un NIDS como un HIDS supervisan sistemas y generan alertas, pero un NIDS usa agentes.
- Un NIDS registra y genera alertas. Un sistema HIDS monitorea la actividad de los puntos de conexión.

 Correcto

5. ¿Cuáles de los siguientes son ejemplos de acciones de regla que pueden encontrarse en forma de firmas? Selecciona tres respuestas.

1 / 1 punto

Pasar

Correcto

Alertar

Correcto

Rechazar

Correcto

Flujo

6. Analiza esta firma de Suricata:

1 / 1 punto

```
alert http 167.215.72.95 any -> 156.150.71.141 80 (msg:"GET on wire";
flow:established,to_server; content:"GET"; sid:12345; rev:2;)
```

¿Cuál es el puerto de destino?

2

80

141

12345

Correcto

7. ¿Qué tipo de datos de registro genera Suricata? Selecciona todas las opciones que correspondan.

1 / 1 punto

Firma

Protocolo

Telemetría de red

Correcto

Alerta

Correcto

8. ¿Qué tipo de consulta de Splunk busca en historiales de registros no estructurados?

0 / 1 punto

Búsqueda de UDM

Búsqueda de referencias

Búsqueda de registros sin procesar

Búsqueda de índice

Incorrecto

Revisa el [video sobre consulta de eventos con Splunk](#).

7. ¿Qué tipo de datos de registro genera Suricata? Selecciona todas las opciones que correspondan.

1 / 1 punto

- Firma
- Protocolo
- Telemetría de red

 Correcto

- Alerta

 Correcto

8. ¿Qué tipo de consulta de Splunk busca en historiales de registros no estructurados?

0 / 1 punto

- Búsqueda de UDM
- Búsqueda de referencias
- Búsqueda de registros sin procesar
- Búsqueda de índice

 Incorrecto

Revisa el [video sobre consulta de eventos con Splunk](#).

9. ¿Cuál es el método de búsqueda predeterminado en Chronicle?

0 / 1 punto

- UDM
- Registro sin procesar
- YARA-L
- No normalizado

 Incorrecto

Revisa el [video sobre consultas de eventos con Chronicle](#).

10. ¿Qué paso del proceso SIEM involucra el procesamiento de datos sin procesar en un formato estandarizado y estructurado?

1 / 1 punto

- Normalizar
- Indexar
- Procesar
- Recopilar

 Correcto

Revisa los campos del encabezado de un paquete

TCP/IP model es un marco que se utiliza para visualizar como los datos se organizan y transmien a traves de una red

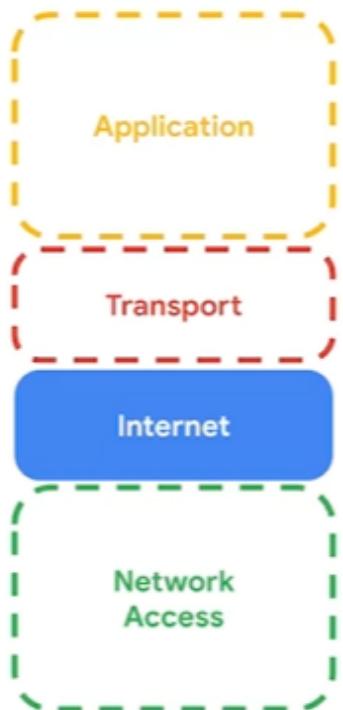
Application

Transport

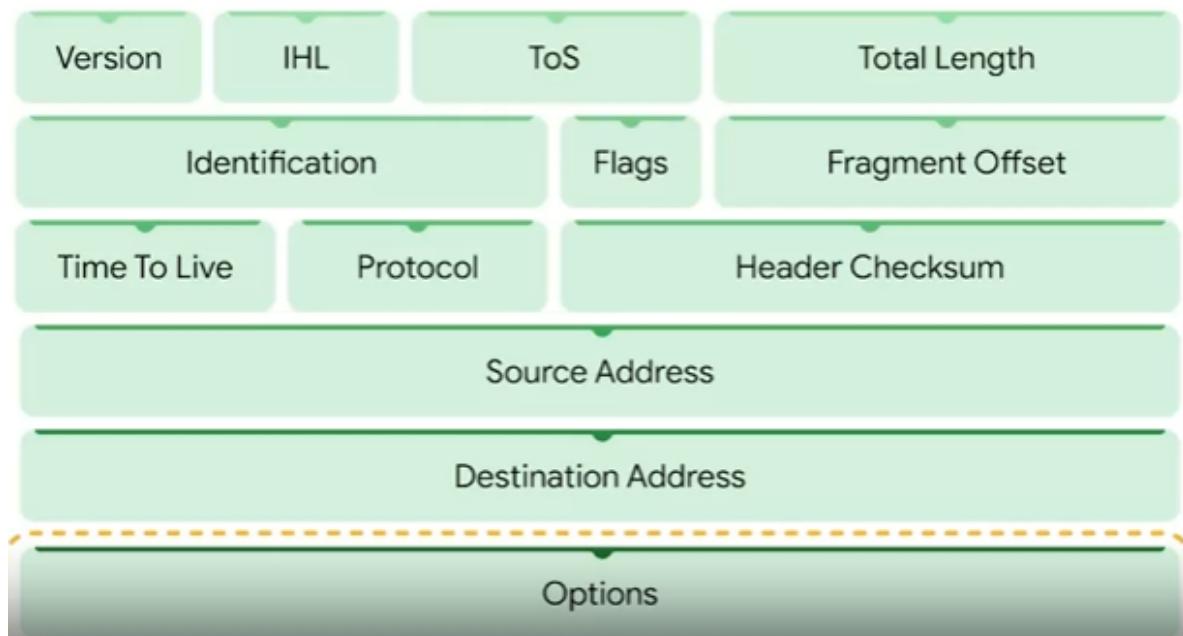
Internet

**Network
Access**

Lo que analizaremos sera la siguiente capa



IPV4



1. Versión: especifica qué versión de IP se está usando, ya sea IPv4 o IPv6.
2. IHL: representa la longitud del encabezado de internet.
3. ToS: representa el tipo de servicio, nos dice si ciertos paquetes deben tratarse de forma diferente, como una etiqueta de "frágil".
4. Longitud Total: identifica la longitud de todo el paquete, incluyendo datos y encabezados.

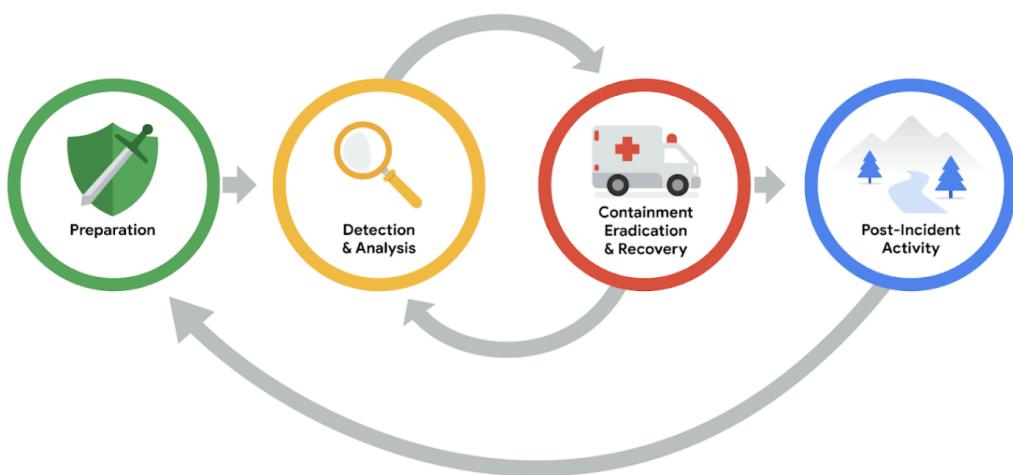
5. Identificación, Indicadores y Desplazamiento: gestionan la información relacionada con la fragmentación, que es cuando un paquete IP se divide en fragmentos, que luego se transmiten por el cable y se vuelven a ensamblar cuando llega a su destino. Estos campos indican si se usó fragmentación y cómo volver a ensamblar los paquetes fragmentados en el orden correcto.
6. TTL o time to live es el que determina cuánto puede vivir un paquete antes de ser descartado. Sin este campo, los paquetes podrían circular indefinidamente a través de los routers.
7. Protocolo: especifica el protocolo utilizado proporcionando un valor que corresponda a un protocolo. Por ejemplo, TCP representa el número 6.
8. La suma de comprobación de cabecera almacena un valor llamado suma de control, usado para determinar cualquier error ocurrido en el encabezado.
9. Dirección de origen: especifica la IP de origen del emisor.
10. Dirección de Destino: es la IP del destino.

Revisión posterior a un incidente

Anteriormente, exploraste la fase de contención, erradicación y recuperación del ciclo de vida de respuesta a incidentes del NIST. Esta lectura explora las actividades involucradas en la fase final del ciclo de vida: la **actividad posterior a un incidente**. Como analista de seguridad, es importante que te familiarices con las tareas que deben llevarse a cabo en esta fase porque cada incidente de seguridad te dará la oportunidad de aprender y mejorar tus respuestas a incidentes futuros.

Actividad posterior a un incidente

La fase de actividad posterior a un incidente del ciclo de vida de respuesta a incidentes del NIST es el proceso de revisión que permite identificar áreas a mejorar durante el manejo de incidentes.



Lecciones aprendidas

Después de que una organización ha contenido un incidente, lo ha erradicado y se ha recuperado con éxito, el incidente llega a su fin. Sin embargo, esto no significa que haya terminado el trabajo de los profesionales de la seguridad. Los incidentes brindan a las organizaciones y sus equipos de seguridad la oportunidad de aprender de lo que sucedió y priorizar formas de mejorar el proceso de manejo de incidentes.

Esto se hace generalmente a través de una **reunión sobre lecciones aprendidas**, también conocida como análisis retrospectivo o revisión post incidente (post-mortem). Una reunión sobre lecciones aprendidas convoca a todas las partes involucradas luego de un incidente importante. Dependiendo del alcance que haya tenido, se pueden programar varias reuniones para recopilar datos suficientes. El propósito de esta reunión es analizar el incidente en su totalidad, evaluar las medidas de respuesta e identificar cualquier área a mejorar. Su objetivo no es echar culpas sino ofrecer a la organización y a su personal la oportunidad de aprender y mejorar. Esta reunión debe programarse a más tardar dos semanas después de que un incidente haya sido remediado con éxito.

No todos los incidentes requieren su propia reunión sobre lecciones aprendidas. El tamaño y la gravedad de un incidente dictarán si es necesario llevarla a cabo. Los incidentes importantes, como los ataques de ransomware, sí deben revisarse en una reunión sobre lecciones aprendidas específica, a la que asisten todas las partes que intervinieron en cualquier aspecto del proceso de respuesta al incidente. Algunos ejemplos de las preguntas que se tratan en esta reunión son:

- ¿Qué sucedió?
- ¿A qué hora ocurrió?
- ¿Quién lo descubrió?
- ¿Cómo se contuvo?
- ¿Cuáles fueron las medidas que se tomaron para la recuperación?
- ¿Qué pudo haberse hecho de otra manera?

Además de tener la oportunidad de aprender del incidente, existen beneficios adicionales de llevar a cabo una reunión sobre lecciones aprendidas. Para las grandes organizaciones, ofrecen una plataforma para que los miembros del equipo en todos los departamentos comparten información y recomendaciones para la prevención futura.

Consejo profesional: Antes de que un equipo organice una reunión sobre lecciones aprendidas, los organizadores deben asegurarse de que todos los asistentes lleguen preparados. Los organizadores de la reunión generalmente desarrollan y distribuyen una agenda de la reunión de antemano, la cual contiene los temas de discusión y garantiza que los asistentes estén informados y preparados. Además, se deben asignar con anticipación las funciones de quienes participarán en la reunión, incluido un moderador que dirija y facilite la discusión y un secretario que tome notas de la reunión.

Recomendaciones

Las reuniones sobre lecciones aprendidas brindan oportunidades para el crecimiento y la mejora. Por ejemplo, los equipos de seguridad pueden identificar errores en las acciones de respuesta, brechas en los procesos y procedimientos o controles de seguridad ineficaces. Una reunión sobre lecciones aprendidas debe dar como resultado una lista de acciones prioritarias o recomendaciones prácticas destinadas a mejorar los procesos de manejo de incidentes y la postura de seguridad general de una organización. Esto garantiza que las organizaciones estén implementando las lecciones que han aprendido después de un incidente, de modo que no estén expuestas a experimentar el mismo incidente en el futuro. Algunos cambios que pueden llevarse a cabo incluyen actualizar y mejorar las instrucciones del manual de estrategias o poner en práctica nuevas herramientas y tecnologías de seguridad.

Informe final

A lo largo de este curso, exploraste la importancia que tiene la documentación en el registro de detalles durante el ciclo de vida de respuesta a incidentes. Como punto de partida, la documentación de respuesta a incidentes debe describir el incidente teniendo en cuenta las cinco preguntas fundamentales a la hora de investigar un incidente: *quién* (who), *qué* (what), *dónde* (where), *por qué* (why) y *cuándo* (when). Los detalles plasmados durante la respuesta a incidentes son importantes para desarrollar documentos adicionales al final del ciclo de vida.

Uno de los documentos fundamentales que se crea al término de un incidente es el **informe final**. Este proporciona una revisión integral del incidente. Los informes finales no están estandarizados, y sus formatos pueden variar según las organizaciones. Además, se pueden crear varios informes finales dependiendo de los públicos para los que estén escritos. Algunos ejemplos de elementos comunes que pueden encontrarse en un informe final son:

- **Resumen ejecutivo:** Un resumen de alto nivel del informe que incluye las principales conclusiones y los hechos esenciales relacionados con el incidente
- **Línea de tiempo:** Un cronograma detallado del incidente que incluye marcas de tiempo que muestran la secuencia de eventos que llevaron al incidente
- **Investigación:** Una compilación de las medidas que se tomaron durante la detección y el análisis del incidente. Por ejemplo, el análisis de un artefacto de red, como una captura de paquetes, revela información sobre qué actividades ocurren en una red.
- **Recomendaciones:** Una lista de medidas sugeridas para la prevención futura

Consejo profesional: Al escribir el informe final posterior a un incidente, considera el público para quien lo estás escribiendo. A menudo, estos informes serán leídos por ejecutivos de negocios y otros profesionales no relacionados con la seguridad, que no tienen la pericia para comprender los detalles técnicos. Tener en cuenta al público al escribir un informe final te ayudará a comunicar de manera efectiva los detalles más importantes.

ROLES DE RESPUESTA

Marco de respuesta del nist consta de 4 fases :

- Preparación
- Detección y análisis
- Contención, erradicación y recuperación
- Actividad posterior a un incidente

Mando, control y comunicación

Es un grupo de personas especializadas en seguridad , capacitadas en gestión y respuestas a incidentes , durante la respuesta a incidentes los equipos pueden enfrentar diversos desafíos . Para que la respuesta a incidentes sea efectiva y eficiente , es necesario contar con un mando claro, control y comunicación de la situación .

- El mando: se refiera a tener el liderazgo descuero y la dirección necesaria para supervisar la respuesta
- El control : se refiere a la capacidad de gestionar los aspectos técnicos durante la respuesta a incidentes como coordinar recursos y asignar tareas
- La comunicación: se refiera a la capacidad de mantener informadas a las partes interesadas.

ROLES a profundidad

analista de seguridad

El trabajo del **analista de seguridad** consiste en monitorear de manera continua un entorno en busca de posibles amenazas a la seguridad. Esto incluye:

- Analizar y clasificar las alertas.
- Realizar investigaciones de causa raíz.
- Notificar a superiores o resolver las alertas.

Si se identifica una amenaza crítica, los analistas la remiten al líder correspondiente del equipo, como el responsable técnico.

Responsable técnico

El trabajo del responsable técnico es gestionar todos los aspectos técnicos del proceso de respuesta a incidentes, como la aplicación de parches o actualizaciones de software. Para ello, primero determina la causa raíz del incidente. Luego, crea e implementa las estrategias para contener, erradicar y recuperarse del incidente. Los responsables técnicos suelen colaborar con otros equipos para asegurarse de que sus prioridades en la respuesta

a incidentes se alineen con las prioridades del negocio, como la reducción de interrupciones para los clientes o el retorno a la normalidad de las operaciones.

Coordinador de incidentes

La respuesta a un incidente también implica una colaboración interdisciplinaria con profesionales que no se especializan en seguridad. Los equipos de respuesta a incidentes de seguridad informática (CSIRT) suelen consultar y aprovechar la experiencia de miembros de departamentos externos. La persona a cargo de la coordinación de incidentes tiene la función de coordinar la tarea con los departamentos pertinentes durante un incidente de seguridad. Al hacerlo, se mantienen abiertas y claras las líneas de comunicación, y queda informado a todo el personal sobre el estado del incidente. Los coordinadores de incidentes también pueden encontrarse en otros equipos, como el Centro de Operaciones de Seguridad (SOC).

Otros roles

Dependiendo de la organización, se pueden encontrar muchos otros roles en un equipo de respuesta a incidentes de seguridad informática (CSIRT), incluyendo responsables de comunicación, de legales o de planificación, entre otros.

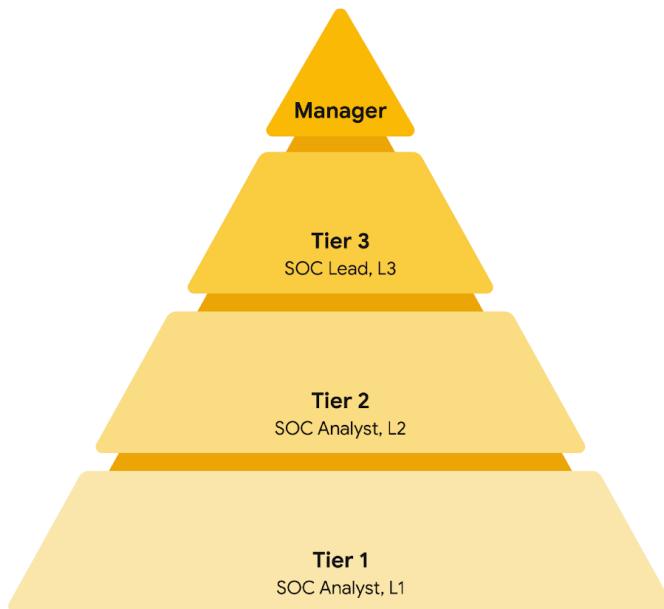
Nota: Los equipos, roles, responsabilidades y estructuras organizativas pueden variar en cada empresa. Por ejemplo, algunas funciones diferentes para la persona a cargo de la coordinación de incidentes incluyen la dirección y gerencia de incidentes.

Centro de Operaciones de Seguridad

Un **Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés)** es una unidad organizativa dedicada a monitorear redes, sistemas y dispositivos en busca de amenazas o ataques de seguridad. Estructuralmente, un SOC suele existir como unidad independiente o dentro de un CSIRT. Es posible que te hayas familiarizado con el término *equipo azul*, que se refiere a los profesionales de seguridad responsables de la defensa contra todas las amenazas y ataques a la seguridad en una organización. Un SOC participa en diversas actividades del equipo azul, como el monitoreo de redes, el análisis y la respuesta a incidentes.

Organización de un SOC

Un Centro de Operaciones de Seguridad (SOC) está compuesto por analistas, líderes y gerentes. Cada función tiene sus propias responsabilidades. Los analistas SOC se agrupan en tres niveles diferentes.



Analista SOC de nivel 1

El primer nivel está compuesto por los analistas SOC menos experimentados, conocidos como analistas de nivel 1 (L1, por level 1). Son responsables de:

- Monitorear, revisar y priorizar las alertas basándose en su criticidad o gravedad.
- Crear y cerrar alertas utilizando sistemas de tickets.
- Notificar los tickets de alerta a los niveles 2 o 3.

Analista SOC de nivel 2

El segundo nivel está formado por los analistas SOC más experimentados, o analistas de nivel 2 (L2). Son responsables de:

- Recibir tickets escalados de L1 y realizar investigaciones más profundas.
- Configurar y perfeccionar las herramientas de seguridad.
- Reportar al líder SOC.

Líder SOC de nivel 3

El tercer nivel de un SOC está compuesto por los jefes SOC o líderes de nivel 3 (L3s). Estos profesionales altamente experimentados son responsables de:

- Gestionar las operaciones de su equipo.
- Explorar métodos de detección mediante la realización de técnicas de detección avanzadas, como el análisis forense y de malware.
- Reportar al gerente SOC

Gerente SOC

El gerente SOC está en la parte superior de la pirámide y es responsable de:

- Contratar, formar y evaluar a los miembros del equipo SOC.
- Crear métricas y gestionar el rendimiento del equipo SOC.
- Desarrollar informes relacionados con incidentes, cumplimiento normativo y auditoría.
- Comunicar los resultados a las partes interesadas, como la dirección ejecutiva.

Otros roles

Los SOC también pueden contener otras funciones especializadas, como ser:

- **Investigadores forenses:** pertenecen comúnmente a L2 y L3, y recopilan, conservan y analizan pruebas digitales relacionadas con incidentes de seguridad para determinar lo sucedido.
- **Cazadores de amenazas:** suelen ser L3 que trabajan para detectar, analizar y defenderse contra amenazas de ciberseguridad nuevas y avanzadas, utilizando inteligencia de amenazas.

Nota: Al igual que los CSIRT, la estructura organizativa de un SOC puede variar dependiendo de la organización.

Seguridad en la nube

Subirse a la nube

Iniciar un negocio en línea solía ser un proceso complicado y costoso. En el pasado, las empresas debían crear y mantener sus propias soluciones internas para operar en el mercado digital. Sin embargo, gracias a la nube, en la actualidad es mucho más sencillo hacerlo, para cualquier persona.

La disponibilidad de tecnologías en la nube ha transformado radicalmente la forma en que las empresas operan en línea. Estas nuevas herramientas permiten a las empresas escalar y adaptarse rápidamente, al tiempo que reducen sus costos. Sin embargo, a pesar de estos beneficios, el cambio hacia servicios basados en la nube también ha presentado una serie de nuevos desafíos de ciberseguridad que ponen en riesgo los activos.

Servicios basados en la nube

Al hablar de "servicios basados en la nube" se hace referencia a una variedad de soluciones empresariales disponibles bajo demanda o basadas en la web. En función de las necesidades y el presupuesto con el que cuente una organización, estos servicios pueden abarcar desde el alojamiento de sitios web hasta entornos de desarrollo de aplicaciones, pasando por toda la infraestructura de backend.

Existen tres categorías principales de servicios basados en la nube:

- Software como servicio (SaaS)
- Plataforma como servicio (PaaS)
- Infraestructura como servicio (IaaS)

Software como servicio (SaaS)

El software como servicio (SaaS) hace referencia a aplicaciones de front-end a las que los/as usuarios/as acceden a través de un navegador web. Las empresas proveedoras de servicios alojan, gestionan y mantienen todos los sistemas de backend para esas aplicaciones. Algunos ejemplos comunes de servicios SaaS incluyen aplicaciones como el

servicio de correo electrónico Gmail™, la plataforma de comunicación y colaboración en equipo Slack y el software de videoconferencias Zoom.

Plataforma como servicio (PaaS)

La plataforma como servicio (PaaS) se refiere a las herramientas de desarrollo de aplicaciones de backend a las que los/as clientes/as pueden acceder en línea. Los desarrolladores utilizan estos recursos para escribir código y crear, gestionar e implementar sus propias aplicaciones. Mientras tanto, las empresas proveedoras de servicios en la nube alojan y mantienen el hardware y software de backend que las aplicaciones utilizan para funcionar. Algunos ejemplos de servicios PaaS incluyen la plataforma Google App Engine™, Heroku® y VMware Cloud Foundry.

Infraestructura como servicio (IaaS)

Los clientes de infraestructura como servicio (IaaS) obtienen acceso remoto a una variedad de sistemas de backend que son alojados por el proveedor de servicios en la nube. Esto incluye servidores de procesamiento de datos, almacenamiento, recursos de redes y más. Los recursos suelen licenciarse según las necesidades, lo que lo convierte en una alternativa rentable en comparación con la compra y el mantenimiento de infraestructura local.

Los servicios basados en la nube permiten a las empresas conectar con sus clientes, empleados y socios comerciales a través de Internet. Algunas de las organizaciones más grandes del mundo ofrecen servicios basados en la nube, como:

- Plataforma Google Cloud
- Microsoft Azure

Seguridad en la nube

Migrar aplicaciones e infraestructura a la nube puede facilitar el funcionamiento de un negocio en línea. Sin embargo, también puede complicar la tarea de mantener los datos privados y seguros. La seguridad en la nube es un campo en crecimiento dentro de la ciberseguridad, que se enfoca específicamente en la protección de datos, aplicaciones e infraestructuras en la nube.

En un modelo tradicional, las organizaciones tenían toda su infraestructura de TI en sus instalaciones. La protección de esos sistemas recaía por completo en el equipo de seguridad interno de ese entorno. No obstante, estas responsabilidades no están tan claramente definidas cuando parte o todo el entorno operativo se encuentra en la nube. Por ejemplo, un cliente de PaaS paga para acceder a los recursos que necesita para crear sus aplicaciones. En este sentido, es razonable esperar que se encargue de la seguridad de las aplicaciones que genera por su cuenta. Por otro lado, la responsabilidad de mantener la seguridad de los servidores a los que acceden debe ser de la empresa proveedora de servicios en la nube, ya que hay otros clientes que utilizan los mismos sistemas.

En seguridad en la nube, este concepto se conoce como modelo de responsabilidad compartida. Por lo general, los clientes son responsables de asegurar todo lo que esté directamente bajo su control:

- Gestión de identidades y accesos
- Configuración de recursos
- Manejo de datos

Nota: El grado de responsabilidad que se delega a un proveedor de servicios varía según el servicio que se utilice: SaaS, PaaS e IaaS.

Seguridad en los activos

Riesgo: es aquello que puede afectar a la confidencialidad, integridad o disponibilidad de un activo

Planes de seguridad:

- Activos : Es un elemento que una empresa percibe como valioso
- Amenazas : Es una circunstancia o evento que puede afectar negativamente los activos
- Vulnerabilidades: es una debilidad que de puede aprovechar por una amenaza.

OTRAS DEFINICIONES

- **Riesgo:** Cualquier hecho que pueda afectar la confidencialidad, integridad o disponibilidad de un activo.
- **Amenaza:** Cualquier circunstancia o evento que pueda afectar negativamente a los activos.
- **Vulnerabilidad:** Debilidad que puede ser aprovechada por una amenaza.

Riesgo de Seguridad

Esto depende en la forma en que una organización define el riesgo.

Se puede calcular de la siguiente manera:

Probabilidad x Impacto = Riesgo

Por ejemplo, corres el riesgo de llegar tarde cuando conduces un automóvil al trabajo. Este evento negativo es más probable que suceda si se pincha un neumático en el camino. Y el impacto podría ser grave, como perder tu empleo. Todos estos factores influyen en cómo abordas el desplazamiento al trabajo todos los días. Lo mismo ocurre con la manera en que las empresas manejan los riesgos de seguridad.

En general, en este campo calculamos el riesgo para ayudar a:

- Prevenir eventos costosos y perjudiciales
- Identificar mejoras que se pueden realizar en sistemas y procesos
- Determinar qué riesgos se pueden tolerar
- Priorizar los activos críticos que requieren atención

Factores de riesgo

A lo largo de este curso, descubrirás que en este campo existen dos amplios factores de riesgo de los que deberás preocuparte:

- Amenazas
- Vulnerabilidades

El riesgo de que un activo sufra daños o se vea perjudicado depende en gran medida de si una amenaza aprovecha las vulnerabilidades.

Aplicándolo al riesgo de llegar tarde al trabajo, una amenaza sería un clavo que perfora tu neumático, ya que los neumáticos son vulnerables a objetos afilados en la carretera. En términos de planificación de seguridad, podrías reducir la probabilidad de este riesgo conduciendo por una carretera limpia.

Categorías de amenazas

Las amenazas son circunstancias o eventos que pueden tener un impacto negativo en los activos. Existen muchos tipos diferentes de amenazas, pero generalmente se clasifican en dos categorías: intencionales e involuntarias.

Por ejemplo, una amenaza *intencional* podría ser un hacker malicioso que obtiene acceso a información confidencial al atacar una aplicación mal configurada. En cambio, una amenaza *involuntaria* podría ser un empleado que sostiene la puerta abierta para una persona desconocida y le otorga acceso a un área restringida. Ambas situaciones pueden dar lugar a un evento que requiere una respuesta adecuada.

Categorías de vulnerabilidad

Las vulnerabilidades son debilidades que pueden ser aprovechadas por las amenazas. Existen diversas vulnerabilidades, pero se pueden clasificar en dos categorías: técnicas y humanas.

Por ejemplo, una vulnerabilidad técnica podría ser un software mal configurado que permita a una persona no autorizada acceder a datos importantes. Mientras tanto, una vulnerabilidad humana podría ser un empleado olvidadizo que pierde su tarjeta de acceso en el estacionamiento. Cualquiera de estas dos situaciones puede generar riesgos.

Seguridad Frameworks

Los marcos de seguridad son pautas usadas en la creación de planes para mitigar riesgos y amenazas a los datos y la privacidad , Ofrecen un enfoque estructurado para implementar en ciclo de seguridad.

Entre sus fines están proteger la información de identificación personal, abreviada como PII,

proteger la información financiera, identificar debilidades de seguridad, manejar riesgos organizacionales y alinear los objetivos de seguridad con los de la empresa.

Fines de los marcos de seguridad:

Proteger la información de identificación personal abreviada como PII, proteger la información financiera, identificar debilidades de la seguridad, manejar riesgos de organizaciones y alinear los objetivos de seguridad con los de la empresa.

Que se centran en

- Proteger la información de identificación personal (PII)
- Proteger la información financiera
- Identificar debilidades de seguridad así como manejar los riesgos organizacionales y alinear los objetivos de seguridad con los de la empresa

Los 4 Componentes de los marcos

1. **Identificar y documentar los objetivos de seguridad**

Por ejemplo: Una organización tiene el objetivo de alinearse con el Reglamento General de Protección de Datos de la UE, también conocido como RGPD. El RGPD es una ley de protección de datos creada para dar a los ciudadanos europeos más control sobre sus datos personales.

2. **Crear pautas para alcanzar los objetivos o** Establecimiento de pautas para lograr los objetivos de seguridad

a. Por ejemplo: al implementar políticas para cumplir con el RGPD, puede que la organización deba crear nuevas políticas sobre cómo manejar solicitudes de datos de usuarios/as individuales

3. **Implementar procesos de seguridad fuertes y sólidos** :En el caso del RGPD, un/a analista que trabaja para una empresa de redes sociales puede diseñar procedimientos para cumplir con las solicitudes de datos de sus usuarios/as.

4. **los marcos de seguridad es monitorear y comunicar los resultados o Supervisión y comunicación de resultados:** puedes monitorear la red interna de la organización y reportar a tu superior o responsable de cumplimiento un problema de seguridad potencial que afecta el RGPD.

Importancia de los Controles de Seguridad en la Organización

controles de seguridad son medidas diseñadas para reducir riesgos específicos de seguridad. Por lo tanto, se utilizan junto con marcos para asegurar que los objetivos y procesos de seguridad se implementen correctamente y que las organizaciones cumplan con los requisitos regulatorios. Puede haber una directiva de que los colaboradores deben hacer una capacitación de privacidad para evitar la filtración de datos. podemos usar una herramienta de software.

Algunos frameworks utilizados son:

La CIA Triada :

Es una guía fundamental que informa como las organizaciones evalúan el riesgo y crean sistemas o políticas de seguridad es el acrónimo de CIA Confidencialidad, Integridad y Disponibilidad

- Integridad: el dato es correcto, auténticos y confiables.
- Confidencialidad:
- Disponibilidad: El dato tiene accesibilidad para quien este autorizado para verlo.

Asset o activo es un elemento percibido como valor para una organización.

Marco de ciberseguridad conocido como el CSF de NIST o

| [Marco de Gestión de Riesgos \(RMF\) del NIST](#)

Es un marco de adhesión voluntario que consiste en estándares, pautas y prácticas recomendadas para manejar riesgos de ciberseguridad

La Comisión Federal de Regulación de Energía - Corporación de Confiabilidad Eléctrica América del Norte (FERC-NERC)

La FERC-NERC es una regulación que se aplica a las organizaciones que trabajan con electricidad o que están involucradas con la red eléctrica de los Estados Unidos y América del Norte. Este tipo de organizaciones tienen la obligación de prepararse, mitigar y reportar cualquier incidente de seguridad potencial que pueda afectar negativamente a la red eléctrica. También están legalmente obligadas a cumplir con los Estándares de Confiabilidad de Protección de Infraestructura Crítica (CIP) definidos por la FERC.

Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP®)

El FedRAMP es un programa del gobierno federal de los Estados Unidos que estandariza la evaluación, autorización, monitoreo y gestión de seguridad de los servicios en la nube y las ofertas de productos. Su objetivo es proporcionar consistencia en todo el sector gubernamental y proveedores de servicios en la nube de terceros.

Centro de Seguridad en Internet (CIS®)

El CIS es una organización sin fines de lucro que se enfoca en múltiples áreas. Proporciona un conjunto de controles que pueden utilizarse para proteger sistemas y redes contra ataques. Su objetivo es ayudar a las organizaciones a establecer un mejor plan de defensa. Además, el CIS proporciona controles aplicables que las/los profesionales de seguridad pueden seguir ante un eventual incidente de seguridad.

Reglamento General de Protección de Datos (RGPD)

El RGPD es una normativa general de datos de la Unión Europea (UE) que protege el procesamiento de los datos de sus residentes y su derecho a la privacidad dentro y fuera del territorio. Por ejemplo, si una organización no es transparente en relación con los datos que posee sobre un/a ciudadano/a de la UE o la razón por la que los tiene, esto constituye una infracción que puede resultar en una multa para la organización. Además, si se produce una filtración y los datos de una persona se ven comprometidos, este debe ser informado. La organización afectada tiene 72 horas para notificarla sobre esta situación.

Estándares de seguridad de datos del sector de las tarjetas de pago (PCI DSS)

PCI DSS es un estándar de seguridad internacional destinado a garantizar que las organizaciones que almacenan, aceptan, procesan y transmiten información de tarjetas de crédito lo hagan en un entorno seguro. El objetivo de esta norma es reducir el fraude con tarjetas de crédito.

Ley de Transferencia y Responsabilidad de los Seguros Médicos (HIPAA)

La HIPAA es una ley federal de los Estados Unidos establecida en 1996 para proteger la información médica de las personas. Esta ley prohíbe que la información de un/una paciente sea compartida sin su consentimiento. Se rige por tres reglas:

1. Privacidad
2. Seguridad
3. Notificación de filtraciones

Organización Internacional para la Normalización (ISO)

La ISO fue creada para establecer estándares internacionales relacionados con la tecnología, la fabricación y la gestión en todo el mundo. Ayuda a las organizaciones a mejorar sus procesos y procedimientos en cuanto a retención del personal, planificación, gestión de residuos y servicios.

Controles de Sistemas y Organizaciones (SOC tipo 1, SOC tipo 2)

Este estándar fue desarrollado por la junta de normas de auditoría del Instituto Americano de Contables Públicos Certificados® (AICPA). Los informes SOC1 y SOC2 se enfocan en las políticas de acceso de los/as usuarios/as de una organización en diferentes niveles, tales como:

- Asociado/a
- Supervisor/a
- Gerente/a
- Ejecutivo/a
- Proveedor/a

Dos sugerencias para investigar: la Ley Gramm-Leach-Bliley y la Ley Sarbanes-Oxley.

Principios Éticos

Confidencialidad

Protección de la privacidad

Leyes

Servidores proxy

Un servidor proxy es un servidor que cumple con la solicitud de un cliente al transmitirla a otros servidores.

El servidor proxy es un servidor dedicado que está entre Internet y el resto de la red.

Cuando llega una solicitud de conexión a la red desde Internet,

el servidor proxy determinará si la solicitud de conexión es segura.

El servidor proxy es una dirección IP pública distinta de la red privada. Esto oculta la dirección IP de la red privada de agentes de amenaza y agrega una capa de seguridad.

- **Proxy Forward:** Este tipo de proxy se centra en proteger a los usuarios *dentro* de una red. Imagina que los empleados de una empresa acceden a Internet. Un proxy forward interceptaría sus solicitudes, enmascararía sus direcciones IP individuales y las enviaría a Internet. Esto hace que sea más difícil para los actores maliciosos rastrear a los usuarios individuales y sus máquinas.
- **Proxy inverso:** A diferencia del proxy forward, el proxy inverso protege los servidores *dentro* de una red del acceso externo. Piensa en un servidor web que almacena información confidencial de la empresa. Un proxy inverso actuaría como un guardián, manejando todas las solicitudes entrantes primero. Sólo las solicitudes legítimas y autorizadas se pasarían al servidor real, protegiéndolo de posibles ataques.
- **Proxy de correo electrónico:** Este tipo se especializa en la seguridad del correo electrónico. Puede filtrar los correos electrónicos no deseados o maliciosos, como el spam o los intentos de phishing, antes de que lleguen a las bandejas de entrada de los empleados. Al examinar los mensajes en busca de contenido sospechoso o remitentes bloqueados, un proxy de correo electrónico ayuda a mantener segura la comunicación por correo electrónico.

Sin título

Sin título

En 2013, la cadena minorista Target sufrió una de las violaciones de datos más grandes de la historia, que expuso la información personal y financiera de aproximadamente 40 millones de clientes. El ataque, que resultó en un costo estimado de 100 millones de dólares para la empresa, incluyó la extracción de nombres, direcciones, números de

tarjetas de crédito y códigos de seguridad. La violación ocurrió durante el periodo de compras navideñas, lo que amplificó el impacto y atrajo la atención mundial. El ataque comenzó con la vulneración de una empresa subcontratada encargada del sistema de calefacción, ventilación y aire acondicionado (HVAC) de Target, que fue utilizada como puerta de entrada para infiltrar los sistemas internos de la cadena. Los hackers instalaron malware en los puntos de venta (POS) de las tiendas, lo que les permitió interceptar los datos de las tarjetas de crédito mientras se procesaban.

La respuesta de Target fue criticada por su lentitud, ya que la empresa tardó varias semanas en identificar y notificar a los clientes afectados. Esto provocó una pérdida significativa de confianza por parte de los consumidores y dañó la reputación de la marca. Además, la violación llevó a demandas colectivas, investigaciones gubernamentales y un aumento en las normativas de ciberseguridad para las empresas.

Este incidente destacó la importancia de la seguridad en las cadenas de suministro, la gestión de accesos y el monitoreo continuo de los sistemas. Además, subrayó la necesidad de una respuesta rápida ante incidentes de seguridad para mitigar daños financieros y de reputación.

El informe del Comité de Comercio del Senado de EE.UU. sobre la violación de datos de Target en 2013 profundiza en cómo los atacantes pudieron acceder a la información personal y financiera de 110 millones de clientes a través de un proveedor externo. Los atacantes instalaron malware en los sistemas de punto de venta (POS) de Target como lo vimos en clase , logrando extraer los datos en plena temporada navideña. A pesar de haber recibido alertas de seguridad, la compañía no respondió de manera adecuada, lo que exacerbó las consecuencias. El informe critica las fallas de ciberseguridad en la cadena de suministro y la lenta reacción de la empresa. También hace hincapié en la importancia de una seguridad integral y de una respuesta rápida para mitigar los daños. Target enfrentó investigaciones, sanciones financieras y una pérdida de reputación significativa. Este incidente marcó un parte aguas en la industria minorista, donde las normas de ciberseguridad se reforzaron para prevenir ataques futuros, se aprendió de su error .

Sin título

1. Un atacante propaga software malicioso dentro de una organización, que ejecuta acciones no autorizadas en sus sistemas. ¿Qué describe este escenario?

1 / 1 punto

- Un procedimiento
- Un reglamento
- Una amenaza
- Una vulnerabilidad

 Correcto

2. Completa el espacio en blanco: Un firewall (cortafuegos) mal configurado es un ejemplo de _____ de seguridad.

1 / 1 punto

- vulnerabilidad
- activo
- exploit
- amenaza

 Correcto

3. ¿Cuáles de las siguientes afirmaciones describen correctamente la gestión de los activos de seguridad? Selecciona dos respuestas.

0.5 / 1 punto

- Disminuye las vulnerabilidades.
- Ayuda a identificar los riesgos.
- Descubre vulnerabilidades en la seguridad.
- Es un proceso que se realiza una sola vez.

 Correcto

4. ¿Cuáles de los siguientes son ejemplos de información confidencial? Selecciona dos respuestas.

0.75 / 1 punto

Contactos del personal

Esto no debería estar seleccionado
Revisa [el video sobre la clasificación de activos](#).

Estrategia de marketing

Correcto

Documentos de un proyecto

Correcto

Comunicado de prensa

5. Un juego de celular muestra anuncios a los usuarios. El juego es gratuito, siempre y cuando vean ocasionalmente anuncios de otras empresas.
¿Deberían estas otras empresas tener acceso para contactar a los usuarios del juego?

0 / 1 punto

- Tal vez, porque los usuarios pueden controlar cómo comparten su información.
- No, porque la información de los usuarios está restringida.
- Sí, porque la información de los usuarios es pública.

Incorrecto
Revisa [el video sobre la clasificación de activos](#).

6. ¿Por qué es tan difícil proteger la información digital? Selecciona dos respuestas.

0.5 / 1 punto

Hay muchos recursos que dedicar a la seguridad.

Esto no debería estar seleccionado
Revisa [el video sobre seguridad de la información](#).

La mayor parte de la información está en forma de datos.

Correcto

- No hay reglamentos que protejan la información.
- Las tecnologías están interconectadas.

7. ¿Qué es un ejemplo de datos en tránsito? Selecciona dos respuestas.

0.75 / 1 punto

Un archivo descargándose de un sitio web

 Correcto

Un sitio web con varios archivos disponibles para descargar

 **Esto no debería estar seleccionado**
Revisa [el video sobre los activos digitales ↗](#).

Una presentación de diapositivas en una memoria USB

Un correo electrónico enviándose a un colega

 Correcto

8. Completa el espacio en blanco: La mayoría de los planes de seguridad abordan los riesgos dividiéndolos en estas categorías: daños, divulgación y _____.

1 / 1 punto

eliminación

pérdida de información

fugas

supresión

 Correcto

9. ¿Cuáles de las siguientes son funciones del núcleo del Marco de Ciberseguridad (CSF) del NIST? Selecciona tres respuestas.

1 / 1 punto

Implementación

Detección

 Correcto

Protección

 Correcto

Respuesta

 Correcto

10. ¿Cuáles son algunas de las ventajas del Marco de Ciberseguridad (CSF) del NIST? Selecciona tres respuestas.

0.

El CSF ayuda a cumplir la normativa.

 Correcto

El CSF es adaptable para satisfacer las necesidades de la empresa.

 Correcto

El CSF protege a una organización de las ciberamenazas.

 **Esto no debería estar seleccionado**

Revisa [el video sobre el cumplimiento normativo y los reglamentos ↗](#).

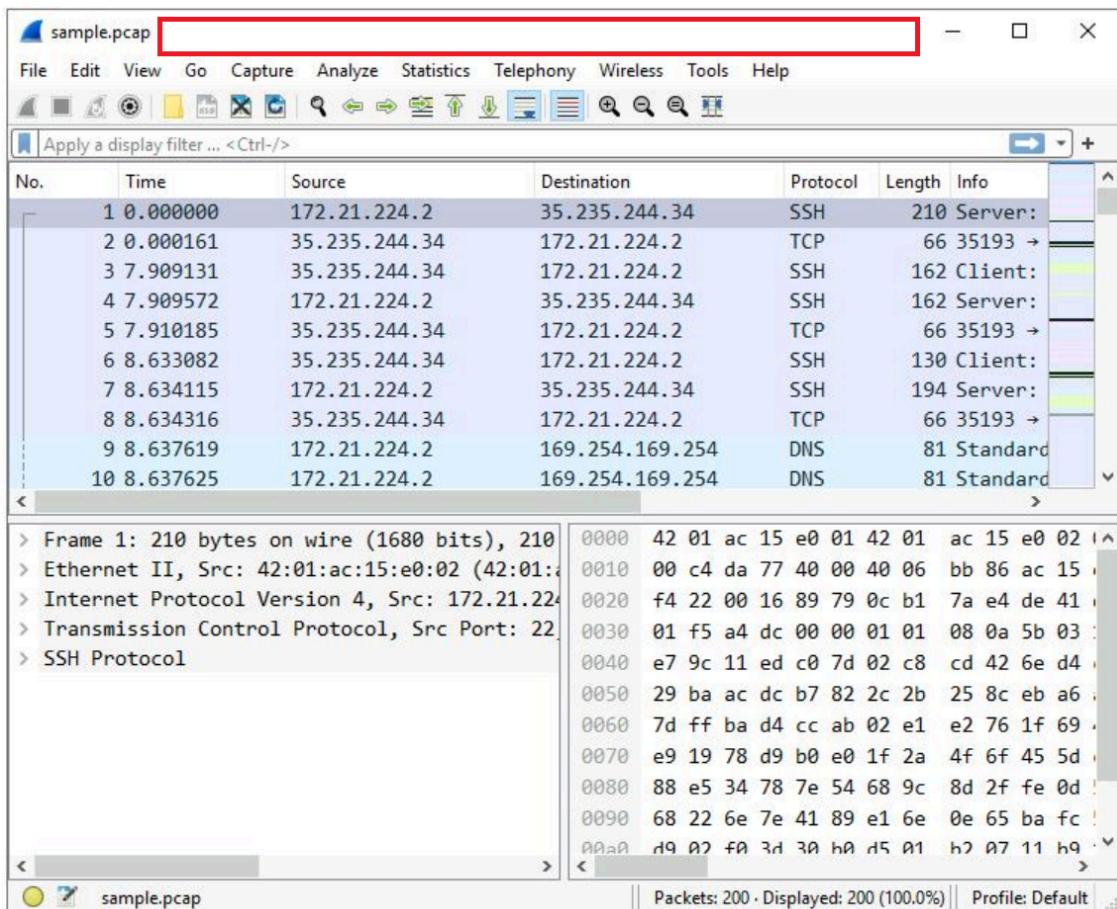
El CSF fomenta la confianza entre las empresas.

Sin título

The packet capture file has the Wireshark packet capture file icon, which shows a shark's fin swimming above three rows of binary digits. The packet capture file has a **.pcap** file extension that is hidden by default by Windows Explorer and on the desktop view.

Note: A **Software Updated** dialog box may appear, notifying you that a new version of Wireshark is available. Click **Skip this version**.

2. Double-click the Wireshark title bar next to the **sample.pcap** filename to maximize the Wireshark application window.



A lot of network packet traffic is listed, which is why you'll apply filters to find the information needed in an upcoming step.

For now, here is an overview of the key property columns listed for each packet:

- **No.:** The index number of the packet in this packet capture file
- **Time:** The timestamp of the packet
- **Source:** The source IP address

- **Destination:** The destination IP address
- **Protocol:** The protocol contained in the packet
- **Length:** The total length of the packet
- **Info:** Some information about the data in the packet (the payload) as interpreted by Wireshark

Not all the data packets are the same color. Coloring rules are used to provide high-level visual cues to help you quickly classify the different types of data. Since network packet capture files can contain large amounts of data, you can use coloring rules to quickly identify the data that is relevant to you. The example packet lists a group of light blue packets that all contain DNS traffic, followed by green packets that contain a mixture of TCP and HTTP protocol traffic.

3. Scroll down the packet list until a packet is listed where the info column starts with the words 'Echo (ping) request'.

What is the protocol of the first packet in the list where the info column starts with the words 'Echo (ping) request'?

HTTP

ICMP

TCP

SSH

Submit

Task 2. Apply a basic Wireshark filter and inspect a packet

In this task, you'll open a packet in Wireshark for more detailed exploration and filter the data to inspect the network layers and protocols contained in the packet.

1. Enter the following filter for traffic associated with a specific IP address. Enter this into the **Apply a display filter...** text box immediately above the list of packets:

```
ip.addr == 142.250.1.139
```

Copied!

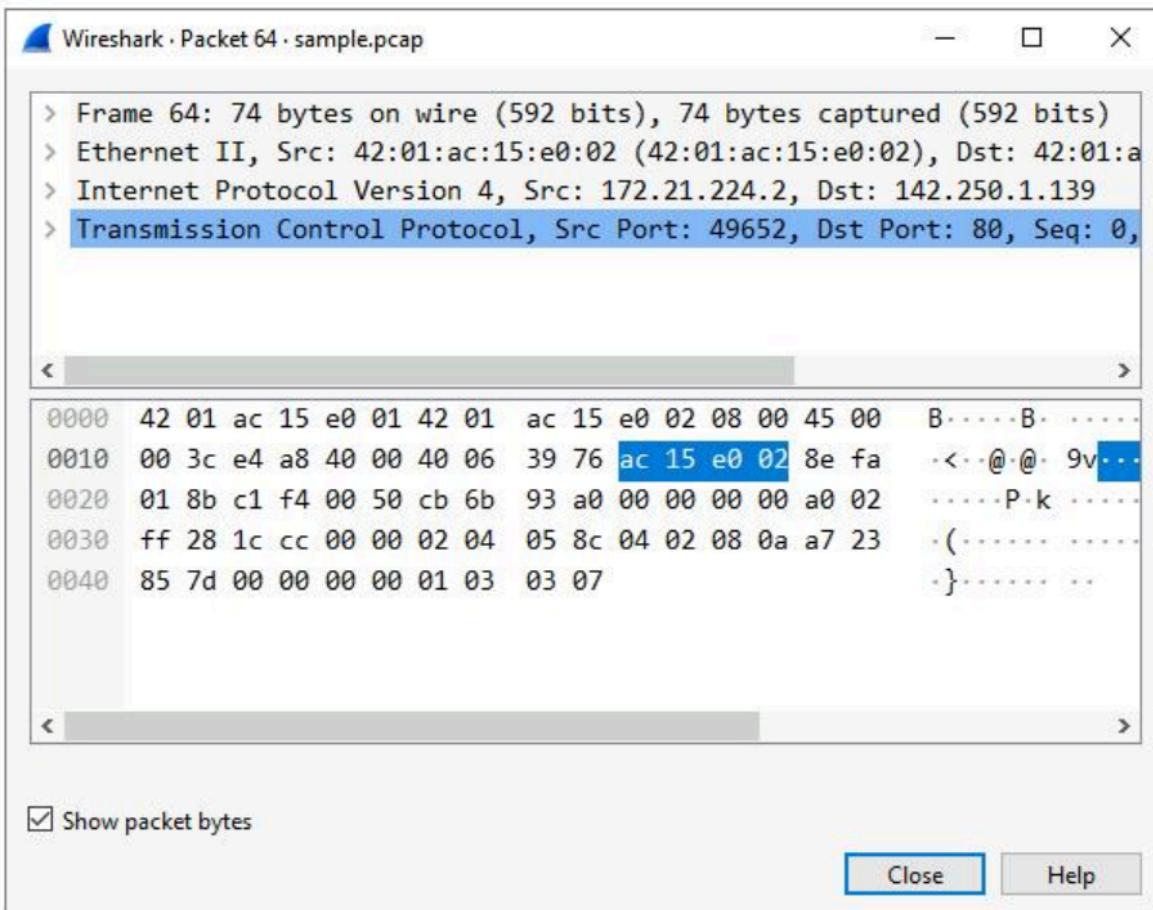
content_copy

2. Press **ENTER** or click the **Apply display filter** icon in the filter text box.

The list of packets displayed is now significantly reduced and contains only packets where either the source or the destination IP address matches the address you entered. Now only

two packet colors are used: **light pink**for ICMP protocol packets and **light green**for TCP(and HTTP, which is a subset of TCP) packets.

3. Double-click the first packet that lists **TCP**as the protocol.
This opens a packet details pane window:



The upper section of this window contains subtrees where Wireshark will provide you with an analysis of the various parts of the network packet. The lower section of the window contains the raw packet data displayed in hexadecimal and ASCII text. There is also placeholder text for fields where the character data does not apply, as indicated by the dot (".").

Note: The details pane is located at the bottom portion of the main Wireshark window. It can also be accessed in a new window by double clicking a packet.

4. Double-click the first subtree in the upper section. This starts with the word **Frame**.
This provides you with details about the overall network packet, or frame, including the frame length and the arrival time of the packet. At this level, you're viewing information about the entire packet of data.

5. Double-click **Frame** again to collapse the subtree and then double-click the **Ethernet II** subtree.

This item contains details about the packet at the Ethernet level, including the source and destination MAC addresses and the type of internal protocol that the Ethernet packet contains.

6. Double-click **Ethernet II** again to collapse that subtree and then double-click the **Internet Protocol Version 4** subtree.

This provides packet data about the Internet Protocol (IP) data contained in the Ethernet packet. It contains information such as the source and destination IP addresses and the Internal Protocol (for example, TCP or UDP), which is carried inside the IP packet.

Note: The *Internet Protocol Version 4* subtree is *Internet Protocol Version 4 (IPv4)*. The third subtree label reflects the protocol.

The source and destination IP addresses shown here match the source and destination IP addresses in the summary display for this packet in the main Wireshark window.

7. Double-click **Internet Protocol Version 4** again to collapse that subtree and then double-click the **Transmission Control Protocol** subtree.

This provides detailed information about the TCP packet, including the source and destination TCP ports, the TCP sequence numbers, and the TCP flags.

The source port and destination port listed here match the source and destination ports in the info column of the summary display for this packet in the list of all of the packets in the main Wireshark window.

What is the TCP destination port of this TCP packet?

80

53

66

200

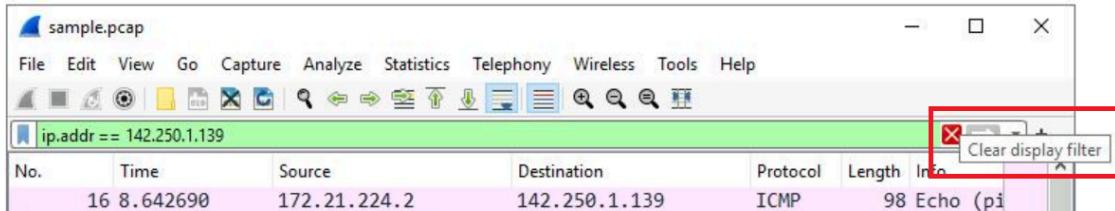
Submit

8. In the **Transmission Control Protocol** subtree, scroll down and double-click **Flags**.

This provides a detailed view of the TCP flags set in this packet.

9. Click the **X** icon to close the detailed packet inspection window.

10. Click the **X Clear display filter** icon in the Wireshark filter bar to clear the IP address filter.



All the packets have returned to the display.

If you ever accidentally close the Wireshark application, you can reopen it by double-clicking the **sample** file on the desktop.

Task 3. Use filters to select packets

In this task, you'll use filters to analyze specific network packets based on where the packets came from or where they were sent to. You'll explore how to select packets using either their physical Ethernet Media Access Control (MAC) address or their Internet Protocol (IP) address.

1. Enter the following filter to select traffic for a specific source IP address only. Enter this into the **Apply a display filter...** text box immediately above the list of packets:

```
ip.src == 142.250.1.139
```

Copied!

content_copy

2. Press **ENTER** or click the **Apply display filter** icon in the filter text box.

A filtered list is returned with fewer entries than before. It contains only packets that came from **142.250.1.139**.

3. Click the **X Clear display filter** icon in the Wireshark filter bar to clear the IP address filter.

4. Enter the following filter to select traffic for a specific destination IP address only:

```
ip.dst == 142.250.1.139
```

Copied!

content_copy

5. Press **ENTER** or click the **Apply display filter** icon in the filter text box.

A filtered list is returned that contains only packets that were sent to **142.250.1.139**.

6. Click the **X Clear display filter** icon in the Wireshark filter bar to clear the IP address filter.

7. Enter the following filter to select traffic to or from a specific Ethernet MAC address.

This filters traffic related to one MAC address, regardless of the other protocols involved:

```
eth.addr == 42:01:ac:15:e0:02
```

Copied!

content_copy

8. Press **ENTER** or click the **Apply display filter** icon in the filter text box.
9. Double-click the first packet in the list. You may need to scroll back to display the first packet in the filtered list.
10. Double-click the **Ethernet II** subtree if it is not already open.

The MAC address you specified in the filter is listed as either the source or destination address in the expanded Ethernet II subtree.

11. Double-click the **Ethernet II** subtree to close it.
12. Double-click the **Internet Protocol Version 4** subtree to expand it and scroll down until the **Time to Live** and **Protocol** fields appear.

The **Protocol** field in the **Internet Protocol Version 4** subtree indicates which IP internal protocol is contained in the packet.

What is the protocol contained in the Internet Protocol Version 4 subtree from the first packet related to MAC address 42:01:ac:15:e0:02?

ESP

ICMP

UDP

TCP

Submit

13. Click the **X** icon to close the detailed packet inspection window.
14. Click the **X Clear display filter** icon in the Wireshark filter bar to clear the MAC address filter.

Task 4. Use filters to explore DNS packets

In this task, you'll use filters to select and examine DNS traffic. Once you've selected sample DNS traffic, you'll drill down into the protocol to examine how the DNS packet data contains both queries (names of internet sites that are being looked up) and answers (IP addresses that are being sent back by a DNS server when a name is successfully resolved).

1. Enter the following filter to select UDP port **53** traffic. DNS traffic uses UDP port **53**, so this will list traffic related to DNS queries and responses only. Enter this into the **Apply a display filter...** text box immediately above the list of packets:

```
udp.port == 53
```

Copied!

content_copy

2. Press **ENTER** or click the **Apply display filter** icon in the filter text box.
3. Double-click the first packet in the list to open the detailed packet window.
4. Scroll down and double-click the **Domain Name System (query)** subtree to expand it.
5. Scroll down and double-click **Queries**.

You'll notice that the name of the website that was queried is opensource.google.com.

6. Click the **X** icon to close the detailed packet inspection window.
7. Double-click the fourth packet in the list to open the detailed packet window.
8. Scroll down and double-click the **Domain Name System (query)** subtree to expand it.
9. Scroll down and double-click **Answers**, which is in the **Domain Name System (query)** subtree.

The Answers data includes the name that was queried (opensource.google.com) and the addresses that are associated with that name.

Which of these IP addresses is displayed in the expanded Answers section for the DNS query for opensource.google.com?

169.254.169.254

172.21.224.1

139.1.250.142

142.250.1.139

Submit

10. Click the **X** icon to close the detailed packet inspection window.
11. Click the **X Clear display filter** icon in the Wireshark filter bar to clear the filter.

Task 5. Use filters to explore TCP packets

In this task, you'll use additional filters to select and examine TCP packets. You'll learn how to search for text that is present in payload data contained inside network packets. This will

locate packets based on something such as a name or some other text that is of interest to you.

1. Enter the following filter to select TCP port **80**traffic. TCP port **80**is the default port that is associated with web traffic:

```
tcp.port == 80
```

Copied!

content_copy

2. Press **ENTER**or click the **Apply display filter**icon in the filter text box.

Quite a few packets were created when the user accessed the web page

<http://opensource.google.com>.

3. Double-click the first packet in the list. The **Destination**IP address of this packet is **169.254.169.254**.

What is the Time to Live value of the packet as specified in the Internet Protocol Version 4 subtree?

64

128

32

16

Submit

What is the Frame Length of the packet as specified in the Frame subtree?

54 bytes

60 bytes

40 bytes

74 bytes

Submit

What is the Header Length of the packet as specified in the Internet Protocol Version 4 subtree?

54 bytes

60 bytes

20 bytes

74 bytes

Submit

What is the Destination Address as specified in the Internet Protocol Version 4 subtree?

169.254.169.254

172.21.224.2

142.250.1.139

239.1.250.142

Submit

4. Click the **X** icon to close the detailed packet inspection window.
5. Click the **X Clear display filter** icon in the Wireshark filter bar to clear the filter.
6. Enter the following filter to select TCP packet data that contains specific text data.

tcp contains "curl"

Copied!

content_copy

7. Press **ENTER** or click the **Apply display filter** icon in the filter text box.

This filters to packets containing web requests made with the curl command in this sample packet capture file.

Conclusion

Great work!

You now have practical experience using Wireshark to

- open saved packet capture files,
- view high-level packet data, and
- use filters to inspect detailed packet data.

This is an important milestone on your journey toward understanding how to use network packet analysis tools to examine network traffic!

Sin título

Términos de glosario de la semana 2 Zonar la alarma

Términos y definiciones del curso 6, semana 2

Analizador de protocolos de red (rastreador de paquetes): Herramienta diseñada para capturar y analizar el tráfico de datos dentro de una red..

Archivo pcap, captura de paquetes: Archivo que contiene paquetes de datos interceptados desde una interfaz o red.

Ciclo de vida de respuesta a incidentes del Instituto Nacional de Estándares y

Tecnología (NIST): Marco para la respuesta a incidentes que consta de cuatro fases: preparación, detección y análisis; contención; erradicación y recuperación; y actividad posterior a un incidente.

Comando y control (C2): Servidor o computadora que utilizan los agentes de amenaza para mantener comunicaciones con los sistemas comprometidos. De esta manera, controlan los dispositivos infectados, extraen datos, entre otras acciones.

Datos de red: Tipo de datos que se transmiten entre los dispositivos de una red.

Dirección de control de acceso al medio (MAC): Identificador alfanumérico único que se asigna a cada dispositivo físico de una red.

Exfiltración de datos: Transmisión no autorizada de datos desde un sistema.

Indicadores de compromiso (IoC): Evidencia observable que sugiere indicios de un posible incidente de seguridad.

Interfaz de línea de comandos (CLI): Interfaz de usuario basada en texto que utiliza comandos para interactuar con la computadora.

Manual de estrategias: Guía que proporciona detalles sobre cualquier acción operativa.

Paquete de datos: Unidad básica de información que se desplaza de un dispositivo a otro dentro de una red.

Protocolo de Internet (IP): Conjunto de estándares utilizados para enrutar y direccionar paquetes de datos a medida que viajan entre dispositivos en una red.

Rastreo de paquetes (packet sniffing): Práctica de capturar e inspeccionar paquetes de datos a través de una red.

Sistema de detección de intrusiones (IDS, por sus siglas en inglés): Aplicación que monitorea la actividad del sistema y alerta sobre posibles intrusiones.

Sudo: Comando que otorga temporalmente permisos elevados a usuarios específicos.

Tarjeta de interfaz de red (NIC, por sus siglas en inglés): Dispositivo que se instala en el interior de una computadora para que esta pueda conectarse a Internet.

tcpdump: Analizador de protocolos de red de línea de comandos.

Tráfico de red: Cantidad de datos que circulan por una red.

Usuario root (usuario raíz o superusuario): Usuario con amplios privilegios para modificar el sistema.

Wireshark: Analizador de protocolos de red de código abierto.

Sin título

Actividad: Realiza una consulta con Chronicle

Cuestionario Práctico. • 50 min. • 6 puntos totales disponibles.6 puntos totales

Español

Vencimiento

13 de dic. 23:59 CST

Para aprobar esta práctica, debes obtener un puntaje de al menos el 75%, o 4,6 de 6 puntos, completando la actividad y respondiendo a las preguntas correspondientes. Una vez que completes el cuestionario, revisa los comentarios. Puedes conocer más sobre las prácticas y ejercicios con calificación en la [descripción general del curso](#).



Resumen de la actividad

En esta actividad, utilizarás Chronicle, una herramienta nativa de la nube, para investigar un incidente de seguridad relacionado con la suplantación de identidad y responder a una serie de preguntas.

Anteriormente, aprendiste cómo las herramientas SIEM, como Chronicle, proporcionan una plataforma para recopilar, analizar y generar informes sobre datos de diferentes fuentes. Como analista de seguridad, usarás herramientas SIEM para identificar y responder a incidentes de seguridad.

Ten en cuenta que esta actividad es opcional y no influirá en la finalización del curso.

Escenario

Revisa el siguiente escenario. Luego, completa las instrucciones paso a paso.

Eres analista de seguridad en una empresa de servicios financieros. Te llega una alerta de que un empleado recibió un correo electrónico de phishing en su bandeja de entrada. La revisas e identificas un nombre de dominio sospechoso en el cuerpo del correo electrónico: signin.office365x24.com. Debes determinar si otros empleados han recibido correos electrónicos de phishing que contengan este dominio y si lo han visitado.

Utilizarás Chronicle para investigar este dominio.

Nota: Utiliza el diario de gestión de incidentes que iniciaste en una actividad anterior para tomar notas durante la actividad y hacer un seguimiento de tus hallazgos.

Instrucciones paso a paso

Sigue las instrucciones y responde a las preguntas para completar la actividad.

Paso 1: Inicia Chronicle

Haz clic en el enlace para iniciar [Chronicle](#).

En la página de inicio de Chronicle, encontrarás la fecha y hora actuales, una barra de búsqueda y datos sobre el número total de entradas de registro. Ya hay una cantidad significativa de eventos de registro ingeridos en la instancia de Chronicle.



Nota: Chronicle es compatible con Google Chrome. Es posible que experimentes una funcionalidad limitada si utilizas navegadores como Firefox, Edge o Safari. Para disfrutar de la mejor experiencia con Chronicle, [instala la última versión de Chrome](#).

Paso 2: Realiza una búsqueda de dominio

Para empezar, sigue estos pasos para realizar una búsqueda de dominio para el dominio contenido en el correo electrónico de phishing. A continuación, busca eventos utilizando información como nombres de host, dominios, direcciones IP, URL, direcciones de correo electrónico, nombres de usuario y hashes de archivos.

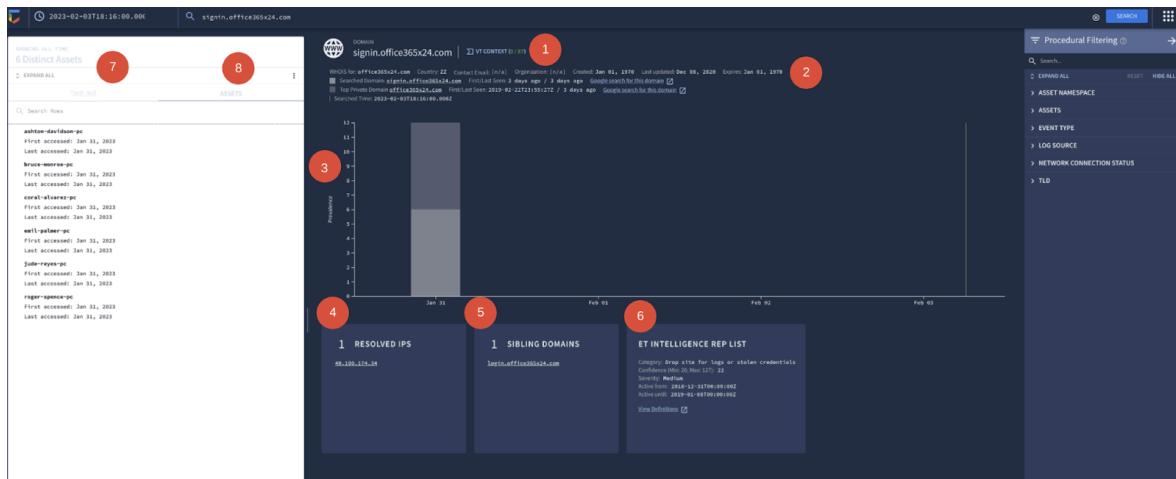
1. En la barra de búsqueda, escribe **signin.office365x24.com** y haz clic en Search (Buscar). En DOMAINS (dominios), aparecerá **signin.office365x24.com**. Esto te indica que el dominio existe en los datos ingeridos.
2. Haz clic en **signin.office365x24.com** para completar la búsqueda.
3. Haz clic en Go to Legacy View para usar la interfaz original de Chronicle.

Paso 3: Evalúa los resultados de búsqueda

Después de realizar una búsqueda de dominios, evalúa los resultados obtenidos y observa lo siguiente:

1. VT CONTEXT: Esta sección proporciona la información de VirusTotal disponible para el dominio.
2. WHOIS: Ofrece un resumen de la información sobre el dominio utilizando WHOIS, un directorio gratuito y disponible públicamente que incluye información sobre los nombres de dominio registrados, como el nombre y la información de contacto del propietario del dominio. En ciberseguridad, esta información es útil para evaluar la reputación de un dominio y determinar el origen de los sitios web maliciosos.
3. Prevalence: Esta sección proporciona un gráfico que describe la prevalencia histórica del dominio. Esto puede ser útil cuando necesitas determinar si se ha accedido al dominio anteriormente. Por lo general, los dominios menos prevalentes pueden indicar una mayor amenaza.
4. RESOLVED IPS: Esta tarjeta de información proporciona contexto adicional sobre el dominio, como la dirección IP que se asigna a **signin.office365x24.com**, que es **40.100.174.34**. Al hacer clic en esta IP se ejecutará una nueva búsqueda de la dirección IP en Chronicle. Las tarjetas de información pueden ser útiles para ampliar la investigación del dominio e investigar más a fondo un indicador para determinar si existe un compromiso más amplio.
5. SIBLING DOMAINS: Esta tarjeta de información proporciona contexto adicional sobre el dominio. Los dominios hermanos comparten un dominio superior o principal común. Por ejemplo, aquí el dominio hermano aparece como **login.office365x24.com**, que comparte el mismo dominio principal **office365x24.com** con el dominio que estás investigando: **signin.office365x24.com**.
6. ET INTELLIGENCE REP LIST: Esta tarjeta de información incluye contexto adicional sobre el dominio. Proporciona información de inteligencia de amenazas, como otras amenazas conocidas relacionadas con los dominios utilizando la Lista de representantes de inteligencia sobre amenazas emergentes (ET) de ProofPoint.
7. Haz clic en TIMELINE (línea de tiempo). Esta pestaña proporciona información sobre los eventos e interacciones realizados con este dominio. Haz clic en EXPAND ALL (expandir todo) para ver los datos sobre las solicitudes HTTP realizadas, incluidas las solicitudes **GET** y **POST**. Una solicitud **GET** recupera datos de un servidor mientras que una solicitud **POST** envía datos a un servidor.

- Haz clic en ASSETS (activos). Esta pestaña proporciona una lista de los activos que han accedido al dominio.



Paso 4: Investiga los datos de inteligencia de amenazas

Ahora, que obtuviste los resultados para el nombre de dominio, el siguiente paso es determinar si el dominio es malicioso. Chronicle proporciona un acceso rápido a los datos de inteligencia de amenazas de los resultados de búsqueda que puedes usar para ayudar en tu investigación. Sigue estos pasos para analizar los datos de inteligencia de amenazas y utiliza tu diario de gestión de incidentes para registrar los datos interesantes:

- Haz clic en VT CONTEXT para analizar la información disponible de VirusTotal sobre este dominio. No hay información de VirusTotal sobre este dominio. Para salir de la ventana de VT CONTEXT, haz clic en la X.
- En Top Private Domain (dominio privado superior), haz clic en office365x24.com para acceder a la vista del dominio de office365x24.com. Haz clic en VT CONTEXT para evaluar la información de VirusTotal sobre este dominio. En la ventana emergente, puedes observar que un proveedor ha marcado este dominio como malicioso. Sal de la ventana VT CONTEXT. Haz clic en el botón Atrás de tu navegador para volver a la vista del dominio para la búsqueda signin.office365x24.com.
- Haz clic en la tarjeta de información de ET INTELLIGENCE REP LIST (lista de representantes de inteligencia de ET) para ampliarla, si es necesario. Anota la categoría.

Paso 5: Investiga los activos y eventos afectados

La información sobre los eventos y activos relacionados con el dominio se separa en dos pestañas: TIMELINE (línea de tiempo) y ASSETS (activos). En TIMELINE se muestra la línea de tiempo de los eventos que incluye cuándo cada activo accedió al dominio. En ASSETS se enumeran los nombres de host, direcciones IP, direcciones MAC o dispositivos que han accedido al dominio.

Investiga los activos y eventos afectados explorando las pestañas:

1. ASSETS: Hay varios activos diferentes que han accedido al dominio, junto con la fecha y hora de acceso. Usando tu diario de gestión de incidentes, anota el nombre y el número de activos que han accedido al dominio.
2. TIMELINE: Haz clic en EXPAND ALL (expandir todo) para ver los datos sobre las solicitudes HTTP realizadas, incluidas las solicitudes **GET** y **POST**. La información **POST** es especialmente útil porque significa que los datos se enviaron al dominio. También sugiere un posible phishing exitoso. Usando tu diario de gestión de incidentes, toma nota de las solicitudes **POST** a la página **/login.php**. Para obtener más información sobre las conexiones, abre el visor de registros sin procesar haciendo clic en el ícono de apertura.

The screenshot shows the Chronicle interface with the following details:

- Timeline:** Shows 8 events from JAN 31, 2023 14:40 UTC.
- Assets:** Shows 14 assets.
- Raw Log:** Displays a detailed log entry for a POST request to /login.php. The log includes fields such as timestamp, source IP, user agent, and detailed security and application metadata.
- Selected:** The log entry for the POST /login.php request is selected.
- UDM Event:** A large panel on the right displays the detailed UDM event for the selected log entry, showing extensive metadata like product log ID, event timestamp, principal details, and security results.

Paso 6: Investiga la dirección IP resuelta

- 1.
- 2.
- a.
- b.
- c.

Paso 7: Responde a las preguntas sobre la investigación del dominio

Conclusiones clave

En esta actividad, utilizaste Chronicle para investigar un dominio sospechoso utilizado en un correo electrónico de phishing. Mediante la búsqueda de dominio de Chronicle, pudiste:

- Acceder a informes de inteligencia de amenazas sobre el dominio.
- Identificar los activos que accedieron al dominio.
- Evaluar los eventos HTTP asociados al dominio.
- Identificar qué activos enviaron información de inicio de sesión al dominio.
- Identificar dominios adicionales.

Tras la investigación, determinaste que el dominio sospechoso ha estado involucrado en campañas de phishing. También, que varios activos podrían haberse visto afectados por la campaña de phishing, ya que los registros mostraban que se había enviado información de inicio de sesión al dominio sospechoso a través de solicitudes **POST**. Finalmente, identificaste dos dominios adicionales relacionados con el dominio sospechoso al examinar la dirección IP resuelta.

Si deseas seguir investigando, consulta la función de chatbot en la página de inicio de Chronicle.

The screenshot displays two main sections of the Chronicle interface:

- Top Section (Domain Investigation):**
 - Left Panel:** Shows a timeline from July 08, 07:00 PM to July 09, 07:00 PM, listing 8 events related to assets (e.g., ashton-davidson-pc, jude-reyes-pc) and security vendors (e.g., alphamountain-as, e-mail-palmer-pc).
 - Middle Panel:** A central dashboard showing 12 security vendors flagged the domain as malicious. It includes tabs for Detections, IOCs, Graph, and Attribution, along with a VT Augment by VIRUSTOTAL section.
 - Right Panel:** Procedural Filtering tools for search, expand all, reset, hide all, assets, event type, log source, network connection status, and TLD.
- Bottom Section (IP Address Investigation):**
 - Left Panel:** Shows 8 distinct assets (e.g., amir-david-pc, ashton-davidson-pc, bruce-morrone-pc, corin-shaw-pc, emil-palmer-pc, jude-reyes-pc, roger-spence-pc, wanda-morris-pc) with their first and last access dates.
 - Middle Panel:** An IP ADDRESS section for 40.100.174.34, providing details like AS Name: MICROSOFT-CORP-MSN-AS-BLOCK (8075), Country: GB, Registrar: RIPE NCC, and Reverse DNS: (n/a). It also shows a presence chart from Jan 31 to Nov 27.
 - Right Panel:** ESET THREAT INTELLIGENCE report for the IP address, indicating it was blocked with high confidence and severity, active until 2023-02-23T21:50:16Z.

Se detectó una incidencia de una ip con la búsqueda en virus total podemos ver que es un sitio de phishing

The screenshot shows a web-based security analysis interface. At the top, a circular icon displays a score of 12/96. To the right, a message states "12/96 security vendors flagged this URL as malicious". Below this are sections for "DETECTION", "DETAILS", and "COMMUNITY". The "DETAILS" tab is active, showing the URL "http://signin.office365x24.com/" and its type "text/html; external-resources". Status information includes "Status 200", "Content type text/html; charset=utf-8", and "Last Analysis Date 10 hours ago". A "Community Score" of -2 is also shown. A green banner at the bottom encourages joining the community for additional insights and automation keys. The main content area is a table titled "Security vendors' analysis" comparing various vendors' findings:

			Do you want to automate checks?
alphaMountain.ai	ⓘ Phishing	BitDefender	ⓘ Phishing
CRDF	ⓘ Malicious	CyRadar	ⓘ Malicious
Fortinet	ⓘ Phishing	G-Data	ⓘ Phishing
Kaspersky	ⓘ Phishing	Lionic	ⓘ Phishing
Seclookup	ⓘ Malicious	Sophos	ⓘ Phishing
VIPRE	ⓘ Phishing	Webroot	ⓘ Malicious
Abusix	ⓘ Clean	Acronis	ⓘ Clean

Solicitudes al sistema operativo

Los sistemas operativos son un componente crítico de una computadora. Establecen conexiones entre las aplicaciones y el hardware para permitir a los/as usuarios/as realizar tareas. En esta lectura, examinarás este proceso complejo en detalle, utilizando una analogía y un nuevo ejemplo para comprenderlo mejor.

Arranque de la computadora

Cuando arrancas o enciendes tu computadora, se activa un microchip BIOS o UEFI. El **sistema básico de entrada/salida (BIOS)** es un microchip que contiene instrucciones de carga para la computadora y que es común en los sistemas más antiguos. La **interfaz de firmware extensible unificada (UEFI)** es un microchip que contiene instrucciones de carga para la computadora y reemplaza al BIOS en los sistemas más modernos.

Tanto los chips BIOS como los UEFI realizan la misma función en el arranque de una computadora. El BIOS era el chip estándar hasta 2007, cuando el uso de los chips UEFI se incrementó. Ahora, la mayoría de las computadoras nuevas incluyen un chip UEFI, que proporciona funcionalidades de seguridad mejoradas.

Los microchips BIOS o UEFI contienen una variedad de instrucciones de carga para la computadora. Por ejemplo, una de estas consiste en verificar el estado del hardware de la computadora.

La última instrucción del BIOS o UEFI activa el cargador de arranque. El **cargador de arranque** es un programa de software que inicia el sistema operativo. Una vez que el sistema operativo termina de arrancar, la computadora está lista para su uso.

Completar una tarea

Como se mencionó con anterioridad, los sistemas operativos nos ayudan a utilizar las computadoras de manera más eficiente. Cuando un equipo pasa por el proceso de arranque, para completar una tarea en una computadora se debe realizar otro proceso que contiene cuatro partes.



Muestra un proceso que va del/la usuario/a a la aplicación, a los sistemas operativos y por último, al hardware.

Usuario/a

En la primera parte está el/la usuario/a, que inicia el proceso para hacer algo con la computadora. Como tú ahora mismo, que iniciaste el proceso de acceder a esta lectura.

Aplicación

La aplicación es el programa de software con el que los/as usuarios/as interactúan para completar una tarea. Por ejemplo, si deseas hacer un cálculo, utilizarás la aplicación de la calculadora. Si deseas escribir un informe, en cambio, usarás una aplicación de procesamiento de textos. Esta es la segunda parte del proceso.

Sistema operativo

El sistema operativo recibe la solicitud del/la usuario/a desde la aplicación. Su tarea es interpretar la solicitud y dirigir el flujo. Para completar la tarea, el sistema operativo la envía a los componentes del hardware.

Hardware

El hardware es donde se realiza todo el procesamiento para completar las tareas iniciadas por el/la usuario/a. Por ejemplo, cuando una persona quiere calcular un número, la unidad central de procesamiento (CPU) realiza el cálculo. Otro ejemplo, cuando un/a usuario/a desea guardar un archivo, otro componente del hardware, el disco duro, se encarga de hacerlo.

Después de que el hardware realiza el trabajo, envía el resultado a través del sistema operativo a la aplicación para mostrárselo al/la usuario/a.

El funcionamiento del sistema operativo detrás de escena

Considera una vez más cuánto se asemeja una computadora a un automóvil. Hay procesos que alguien no observa directamente cuando maneja un vehículo, pero sí siente cómo avanza cuando pisa el acelerador. Lo mismo sucede con una computadora. Aunque no lo experimentas directamente, se lleva a cabo un trabajo importante dentro de un equipo, que involucra al sistema operativo.

Puedes explorarlo a través de otra analogía: el proceso de usar un sistema operativo también se asemeja a hacer un pedido en un restaurante. Cuando sales a comer afuera,

haces un pedido y recibes tu comida, pero no ves el paso a paso de cómo se prepara tu plato en la cocina.

Hacer un pedido de comida es similar a usar una aplicación en una computadora. Cuando haces tu pedido, mencionas algún detalle específico como “una sopa pequeña, muy caliente”. Cuando usas una aplicación, también realizas solicitudes específicas como “imprimir tres copias a doble faz de este documento”.

Puedes comparar la comida que recibes con lo que sucede cuando el hardware envía el resultado. Recibes la comida que pediste. Recibes el documento que querías imprimir. Por último, la cocina se asemeja al sistema operativo: aunque no sepas qué ocurre allí, su función es fundamental para interpretar tu solicitud y garantizar que recibas lo que pediste. Del mismo modo, si bien el trabajo del sistema operativo no es directamente visible para ti, es crucial para completar tus tareas con éxito.

Un ejemplo: descargar un archivo desde un navegador de Internet

Anteriormente, viste cómo los sistemas operativos, las aplicaciones y el hardware trabajan de manera conjunta examinando una tarea que implicaba un cálculo. Ahora, puedes ampliar esta comprensión explorando cómo el sistema operativo completa otra tarea: descarga un archivo desde un navegador de Internet:

- Primero, el/la usuario/a decide que quiere descargar un archivo que encontró en línea, por lo que hace clic en un botón de descarga cerca del archivo en la aplicación del navegador web.
- Luego, el navegador web comunica dicha acción al sistema operativo.
- El sistema operativo envía la solicitud para descargar el archivo al hardware adecuado para su procesamiento.
- El hardware comienza a descargarlo y el sistema operativo envía esta información a la aplicación del navegador. Luego, este informa al/la usuario/a cuando el archivo ha sido descargado.

Soporte en linux

Soporte integrado de Linux

Linux también tiene varios comandos que puedes usar como soporte.

man

El comando `man` muestra información sobre otros comandos y cómo funcionan. Es la abreviatura de “manual”. Para buscar información sobre un comando, ingresa el comando después de `man`. Por ejemplo, al ingresar `man chown`, obtienes información detallada sobre el comando `chown`, incluidas las diversas opciones que puedes usar con él. La salida del comando `man` también se llama “páginas `man`”.

apropos

El comando **apropos** busca una cadena especificada en las descripciones de páginas man. Las páginas man pueden ser largas y difíciles de explorar si estás buscando una palabra clave específica. Para usar **apropos**, ingresa la palabra clave después de **apropos**.

También puedes incluir la opción **-a** para buscar varias palabras. Por ejemplo, al ingresar **apropos -a graph editor**, obtienes páginas man que contienen las palabras "graph" y "editor" en sus descripciones.

whatis

El comando **whatis** muestra una descripción de un comando en una sola línea. Por ejemplo, al ingresar **whatis nano**, se obtiene una descripción de **nano**. Este comando es útil cuando no necesitas una descripción detallada, sino solo una idea general del comando. Puede servir como recordatorio, o bien una manera de obtener más información sobre un comando nuevo que conociste a través de un/a colega o un recurso en línea.

SQL

SQL significa lenguaje de consulta estructurada , es un lenguaje de programacion para crear bases de datos , interactuar con ellas y solicitarles datos.

Consulta en SQL:Es una solicitud de datos de una tabla o combinacion de tablas.

Diferencias entre el filtrado de Linux y el de SQL

Aunque tanto Linux como SQL te permiten filtrar datos, existen algunas diferencias que es necesario tener en cuenta, a la hora de elegir qué opción utilizar.

Estructura

SQL ofrece mucha más estructura que Linux, que tiene un estilo más libre y menos ordenado.

Por ejemplo, si quieras acceder a un registro de intentos de inicio de sesión de los/las empleados/as, Linux imprimirá los datos como una línea de texto sin esta organización. En cambio, SQL te entregará cada registro separado en columnas, por lo cual te facilitará el análisis de una columna específica.

En términos de estructura, SQL proporciona resultados más fáciles de leer y pueden ajustarse más rápidamente que mediante Linux.

Combinación de tablas

Algunas decisiones sobre seguridad requieren información de distintas tablas, una posibilidad que solo SQL ofrece. Mientras que con SQL, las/los analistas pueden combinar varias tablas cuando devuelve datos, Linux no tiene esa misma funcionalidad, ya que no permite que los datos se asocien con otra información que tengas en tu computadora. Para un/a analista que tiene que revisar registros de seguridad, esto resulta restrictivo.

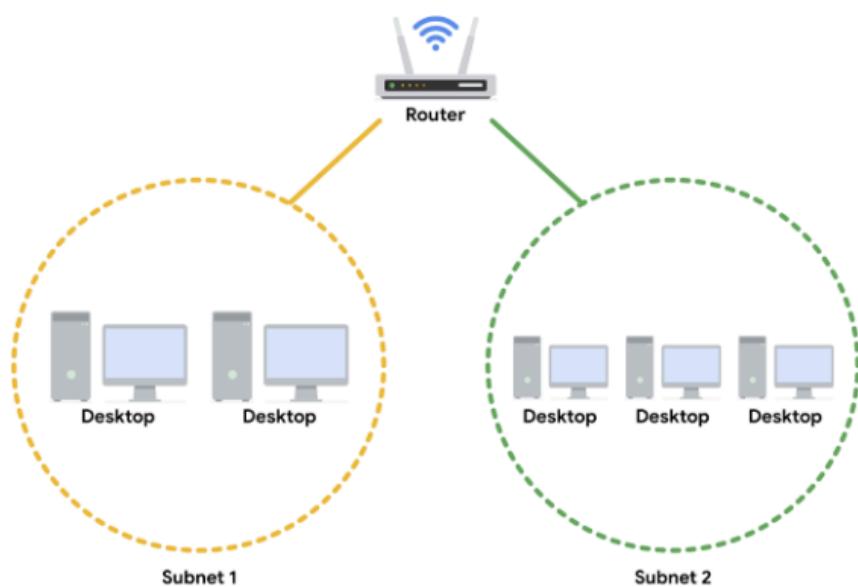
Mejores usos

Como analista de ciberseguridad, es importante que entiendas cuándo puedes usar cada herramienta. Si bien SQL posee una estructura más organizada y te permite combinar tablas, esto no significa que no haya situaciones que te exijan filtrar datos en Linux. Una gran cantidad de datos utilizados en ciberseguridad se almacenarán en un formato de base de datos que funciona con SQL. Sin embargo, otros registros pueden estar en un formato que no es compatible con este lenguaje. Por ejemplo, si los datos se almacenan en un archivo de texto, no puedes buscarlos con SQL. En esos casos, es útil saber cómo filtrar en Linux.

Subnetting y enrutamiento entre dominios sin clases (CIDR)

Descripción general del subnetting

Es la subdivisión de una red en grupos lógicos llamados subredes, lo que funciona como una red dentro de otra red. Este proceso divide el rango de direcciones de red en subredes más pequeñas dentro de la red principal. Estas subredes se forman según las direcciones IP y máscara de red de los dispositivos. También puede ser utilizado para crear zonas de seguridad. Cuando los dispositivos en la misma subred se comunican entre sí, el switch de la red cambia las transmisiones para que permanezcan en la misma subred, mejorando la velocidad y la eficiencia de las comunicaciones.



Notación del enrutamiento entre dominios sin clase (CIDR) para el subnetting

El enrutamiento entre dominios sin clase (CIDR) es un método para asignar máscaras de subred a direcciones IP con el fin de crear subredes, que remplazan al antiguo direccionamiento con clase de la clase A a la clase E.

El CIDR permite a las y los profesionales de la ciberseguridad segmentar redes clasificadas en clases en fragmentos más pequeños. Las direcciones IP en formato CIDR son similares a las direcciones IPv4, pero incluyen una barra diagonal ("/") seguida de un número al final de la dirección, conocido como el prefijo de red IP. Por ejemplo, una dirección IPv4 normal utiliza el formato 198.51.100.0, mientras que una dirección IP CIDR incluiría el prefijo de red IP al final de la dirección, 198.51.100.0/24.

Esta dirección CIDR abarca todas las direcciones IP entre 198.51.100.0 y 198.51.100.255.

El sistema de direccionamiento CIDR reduce el número de entradas en las tablas de enrutamiento y proporciona más direcciones IP disponibles dentro de las redes. Puedes probar la conversión de direcciones CIDR a direcciones IPv4 y viceversa a través de una herramienta de conversión en línea, como IPAddressGuide, para practicar y comprender mejor este concepto.

Beneficios de seguridad del subnetting

El subnetting permite a las y los profesionales y analistas crear una red dentro de su propia red sin solicitar otra dirección IP de red al proveedor de servicios de Internet. Este proceso utiliza el ancho de banda de la red de manera más eficiente y mejora el rendimiento. El subnetting es un componente para crear subredes aisladas a través del aislamiento físico, la configuración de enrutamiento y los cortafuegos (firewalls).

Sudo en linux

Uso responsable de sudo

Para administrar la autorización y la autenticación, tienes que ser un **usuario root** o un usuario con privilegios elevados para modificar el sistema. El usuario root (raíz) también puede llamarse "superusuario". Para convertirte en usuario root, debes iniciar sesión como tal. Sin embargo, no se recomienda ejecutar comandos como usuario root en Linux, ya que pueden surgir riesgos de seguridad si un agente de amenaza compromete esa cuenta.

También es fácil cometer errores irreversibles, y el sistema no puede rastrear quién ejecutó un comando. Por estas razones, en lugar de iniciar sesión como usuario root, se recomienda usar **sudo** en Linux cuando necesites privilegios elevados.

El comando `sudo` otorga temporalmente permisos elevados a usuarios específicos. El nombre de este comando proviene de “super user do” (“superusuario” y “hacer”). Para que puedan usar `sudo`, se les debe otorgar acceso a los usuarios a través de un archivo de configuración, que se llama “sudoers file”. Si bien es preferible usar `sudo` a iniciar sesión como usuario root, es importante tener en cuenta que los usuarios con permisos elevados para usar `sudo` podrían estar en mayor riesgo en caso de un ataque.

Esta situación puede compararse con la de un hotel que tiene una llave maestra. La llave maestra se puede usar para acceder a cualquier habitación del hotel. Algunos/as trabajadores necesitan esta llave para realizar su trabajo. Por ejemplo, para limpiar todas las habitaciones, la persona a cargo debería escanear la tarjeta de identificación y, luego, usar esta llave maestra. Sin embargo, si una persona ajena a la red del hotel obtuviera acceso a la tarjeta de identificación y la llave maestra de la persona a cargo de la limpieza, podría acceder a cualquier habitación del hotel. En este ejemplo, la persona a cargo de la limpieza con la llave maestra representa a un/a usuario/a que usa `sudo` para obtener privilegios elevados. Debido a los peligros que `sudo` supone, solo quienes estrictamente necesitan usarlo deben tener estos permisos.

Además, incluso si necesitas acceso a `sudo`, debes tener cuidado y usarlo solo con los comandos que necesitas. La ejecución de comandos con `sudo` permite a los/las usuarios/as eludir los controles de seguridad típicos que existen para evitar que un/a atacante obtenga acceso elevado.

Nota: Ten cuidado de no usar `sudo` si estás copiando comandos de una fuente en línea. Es importante que no uses `sudo` por accidente.

Autenticación y autorización con sudo

Puedes usar `sudo` para muchas tareas de gestión de autenticación y autorización. Como recordatorio, la **autenticación** es el proceso de verificar quién es una persona, mientras que la **autorización** es el concepto de otorgar acceso a recursos específicos en un sistema. Estos son algunos de los comandos clave que se utilizan para estas tareas:

useradd

El comando `useradd` agrega un usuario al sistema. Para agregar un usuario con el nombre de usuario `fgarcia` con `sudo`, ingresa `sudo useradd fgarcia`. Existen otras opciones que puedes usar con `useradd`:

- `-g`: Establece el grupo predeterminado del usuario, también conocido como su grupo principal.
- `-G`: Agrega al usuario a grupos adicionales, también llamados grupos complementarios o secundarios.

Para usar la opción `-g`, debe especificarse el grupo principal después de `-g`. Por ejemplo, al ingresar `sudo useradd -g security fgarcia`, se agrega a `fgarcia` como un nuevo usuario y se le asigna `security` como grupo principal.

Para usar la opción `-G`, debe incluirse el grupo complementario en el comando después de `-G`. Con la opción `-G`, puedes agregar más de un grupo complementario a la vez. Al ingresar `sudo useradd -G finance,admin fgarcia`, se agrega a `fgarcia` como usuario nuevo y se lo añade a los grupos existentes `finance` y `admin`.

usermod

El comando `usermod` modifica las cuentas de usuario existentes. Las mismas opciones `-g` y `-G` del comando `useradd` pueden utilizarse con `usermod` si el usuario ya existe.

Para cambiar el grupo principal de un usuario existente, debes usar la opción `-g`. Por ejemplo, al ingresar `sudo usermod -g executive fgarcia`, se cambiaría el grupo principal de `fgarcia` a `executive`.

Para agregar un grupo complementario para un usuario existente, debes usar la opción `-G`. También necesitas una opción `-a`, que agrega al usuario a un grupo existente y solo se usa con la opción `-G`. Por ejemplo, al ingresar `sudo usermod -a -G marketing fgarcia`, se agregaría el usuario existente `fgarcia` al grupo complementario `marketing`.

Nota: Al cambiar el grupo complementario de un usuario existente, si no incluyes la opción `-a`, `-G` reemplazará a cualquier grupo complementario existente con aquellos que se especifiquen después de `usermod`. El uso de `-a` con `-G` asegura que se agreguen los nuevos grupos, pero no se reemplaza a los grupos existentes.

Hay otras opciones que puedes usar con `usermod` para especificar cómo quieras modificar el usuario, entre ellas, las siguientes:

- `-d`: Cambia el directorio de inicio del usuario.
- `-i`: Cambia el nombre de inicio de sesión del usuario.
- `-L`: Bloquea la cuenta para que el usuario no pueda iniciar sesión.

La opción siempre va después del comando `usermod`. Por ejemplo, para cambiar el directorio de inicio de `fgarcia` a `/home/garcia_f`, ingresa `sudo usermod -d /home/garcia_f fgarcia`. La opción `-d` va justo después del comando `usermod` y antes de los otros dos argumentos necesarios.

userdel

El comando `userdel` elimina a un usuario del sistema. Por ejemplo, al ingresar `sudo userdel fgarcia`, se elimina a `fgarcia` como usuario. Ten cuidado antes de eliminar a un usuario con este comando.

El comando `userdel` no elimina los archivos en el directorio de inicio del usuario, a menos que se use la opción `-r`. Al ingresar `sudo userdel -r fgarcia`, se eliminaría a `fgarcia` como usuario y se eliminarían todos los archivos en su directorio de inicio. Antes de eliminar cualquier archivo de usuario, debes asegurarte de tener copias de seguridad en caso de que las necesites más adelante.

Nota: En lugar de eliminar al usuario, podrías considerar desactivar su cuenta con `usermod -L`. Esto le impide al usuario iniciar sesión y te otorga acceso a su cuenta y sus permisos asociados. Por ejemplo, si un usuario abandona una organización, esta opción te permitiría

identificar los archivos sobre los que tiene propiedad, por lo que podrías transferir esta propiedad a otros usuarios.

chown

El comando **chown** cambia la propiedad de un archivo o un directorio. Puedes usar **chown** para cambiar la propiedad del usuario o del grupo. Para cambiar el usuario propietario del archivo **access.txt** a **fgarcia**, ingresa **sudo chown fgarcia access.txt**. Para cambiar el grupo propietario del archivo **access.txt** a **security**, ingresa **sudo chown :security access.txt**. Tienes que ingresar dos puntos (:) antes de **security** para designarlo como un nombre de grupo.

Al igual que con **useradd**, **usermod** y **userdel**, existen otras opciones que puedes usar con **chown**.

Suricata Descripción general

Introducción a Suricata

Suricata es un sistema de detección de intrusiones de código abierto, un sistema de prevención de intrusiones y una herramienta de análisis de redes.

Características de Suricata

Suricata tiene tres funcionalidades principales:

- **Sistema de detección de intrusiones (IDS)**: Como IDS basado en la red, Suricata puede monitorear el tráfico de la red y alertar sobre intrusiones y actividades sospechosas. Además, se puede configurar como IDS basado en host para que controle el sistema y las actividades de red de un solo host, como una computadora.
- **Sistema de prevención de intrusiones (IPS)**: Suricata también puede funcionar como un sistema de prevención de intrusiones (IPS) para detectar y bloquear la actividad y el tráfico malicioso. Ejecutar Suricata en modo IPS requiere una configuración adicional, como habilitar el modo IPS.
- **Monitoreo de seguridad de red (NSM)**: En este modo, Suricata ayuda a mantener la seguridad de las redes al generar y guardar registros de red relevantes. Además, puede analizar el tráfico de red en vivo y los archivos de captura de paquetes existentes, así como crear y guardar capturas de paquetes completas o condicionales. Esto puede ser útil para análisis forenses, respuesta a incidentes y para probar firmas. Por ejemplo, puedes activar una alerta y capturar el tráfico de red en vivo para generar registros de tráfico que luego puedes analizar para refinar las firmas de detección.

Reglas

Las reglas o firmas se utilizan para identificar patrones, condiciones y comportamientos específicos del tráfico de red que podrían indicar actividad maliciosa. En Suricata, los términos regla y firma suelen ser intercambiables. Los analistas de seguridad utilizan

firmas o patrones asociados con actividades maliciosas para detectar y alertar sobre amenazas específicas. Las reglas también se pueden usar para proporcionar mayor contexto y visibilidad en sistemas y redes, lo que contribuye a identificar posibles amenazas o vulnerabilidades de seguridad.

Suricata utiliza el **análisis de firmas**, que es un método de detección utilizado para encontrar eventos de interés. Las firmas tienen tres componentes:

- **Acción:** El primer componente de una firma. Describe qué hay que hacer si la actividad de la red o del sistema coincide con la firma, por ejemplo, alertar, pasar, soltar o rechazar.
- **Encabezado:** Incluye información de tráfico de red, como direcciones IP de origen y destino, puertos de origen y destino, protocolo y dirección de tráfico.
- **Opciones de regla:** Proveen diferentes opciones para personalizar las firmas.

Este es un ejemplo de una firma de Suricata:

Action	Header	Rule options
alert	tcp 10.120.170.17 any -> 133.113.202.181 80	(msg: "Hello"; sid:1234; rev:1;)

Las opciones de regla tienen un orden específico, y cambiarlo modificaría el significado de la regla.

Nota: Los términos regla y firma son sinónimos.

Nota: El orden de reglas hace referencia al orden en que Suricata las evalúa. Las reglas se procesan en el orden en que están definidas en el archivo de configuración. Sin embargo, Suricata procesa las reglas en un orden predeterminado diferente: pass, drop, reject y alert (pasar, soltar, rechazar y alertar). El orden de las reglas afecta el veredicto final de un paquete. Por ejemplo, si las reglas con acciones en conflicto, como una regla de soltar y una regla de alertar, coinciden en el mismo paquete.

Reglas personalizadas

Aunque Suricata ya tiene reglas previamente escritas, es muy recomendable modificarlas o personalizarlas para que cumplan con los requisitos de seguridad específicos.

No hay un único enfoque para la creación y modificación de las reglas y esto se debe a que la infraestructura de TI de cada organización es diferente. Los equipos de seguridad deben probar y modificar exhaustivamente las firmas de detección de acuerdo a sus necesidades.

La creación de reglas personalizadas ayuda a personalizar la detección y el monitoreo. Además, contribuye a minimizar la cantidad de falsos positivos que los equipos de seguridad reciben. Saber cómo escribir firmas efectivas y personalizadas es muy importante para aprovechar al máximo las tecnologías de detección.

Archivo de configuración

Antes de implementar las herramientas de detección y que comiencen a monitorear sistemas y redes, es necesario configurar correctamente los ajustes, para que hagan la

tarea que se necesita. Esto se hace por medio del **archivo de configuración**, que permite configurar los ajustes de una aplicación y personalizarla. De esta manera, se indica exactamente cómo se desea que los IDS interactúen con el resto del entorno.

En Suricata, el archivo de configuración es **suricata.yaml**, que utiliza el formato de archivo YAML para la sintaxis y la estructura.

Archivos de registro

Cuando se activan las alertas, Suricata genera dos archivos de registro:

- **eve.json**: es el archivo de registro estándar de Suricata y contiene información detallada y metadatos sobre los eventos y alertas generados por Suricata, almacenados en formato JSON. Por ejemplo, los eventos en este archivo contienen un identificador único llamado `flow_id`, que se utiliza para correlacionar registros o alertas con un solo flujo de red, lo que facilita el análisis del tráfico de red. El archivo `eve.json` se utiliza para hacer un análisis más detallado, y se considera un mejor formato de archivo para el análisis sintáctico de registros y la ingestión de registros SIEM.
- **fast.log**: Se utiliza para registrar información de alerta mínima, incluida la dirección IP básica y los detalles de puerto sobre el tráfico de la red. Además, es útil para generar registros y alertas básicos, y se considera un formato de archivo heredado que no es adecuado para la respuesta a incidentes o tareas de caza de amenazas.

La principal diferencia entre ambos es el nivel de detalle que se registra en cada uno. El archivo `fast.log` registra información básica, mientras que el archivo `eve.json` contiene información detallada adicional.

Conclusiones clave

En esta lectura, exploraste algunas de las características de Suricata, su sintaxis de reglas y la importancia de su configuración. Comprender cómo configurar las tecnologías de detección y escribir reglas efectivas te dará una visión clara de la actividad que ocurre en un entorno, para que puedas mejorar la capacidad de detección y la visibilidad de la red. Podrás comenzar a practicar con Suricata en la próxima actividad.

Recursos para obtener más información

Si deseas obtener más información sobre Suricata, incluida la gestión y el rendimiento de las reglas, puedes consultar los siguientes recursos:

- [Guía de usuario de Suricata](#)
- [Características de Suricata](#)
- [Gestión de reglas](#)
- [Análisis del desempeño de las reglas](#)
- [Webinario de caza de amenazas de Suricata](#)
- [Introducción a la creación de reglas en Suricata](#)
- [Ejemplos de jq de eve.json](#)

Tipos comunes de ataques de red

Ataque de denegación de servicio (DoS)

Definición

Ataque dirigido a una red o servidor para inundarlo con tráfico de red para inhabilitar los sistemas y servicios informáticos de forma temporal.

Término

Ataque de denegación de servicio distribuido (DDoS)

Definición

Tipo de ataque de denegación de servicio que utiliza varios dispositivos o servidores en diferentes ubicaciones para inundar la red objetivo con tráfico no deseado

Término

Ataque de inundación sincronizada

Definición

Tipo de ataque DoS que simula una conexión TCP/IP e inunda un servidor con paquetes SYN.

Término

Rastreo de paquetes

Definición

Práctica consistente en capturar e inspeccionar paquetes de datos a través de una red

Término

Ataque de suplantación de IP

Definición

Ataque a la red realizado cuando un atacante cambia la IP de origen de un paquete de datos para hacerse pasar por un sistema autorizado y obtener acceso a una red

Término

Ataque en ruta

Definición

Ataque en el que un actor malicioso se coloca en medio de una conexión autorizada e intercepta o altera los datos en tránsito

Tipos de agente de amenaza

Para ser un profesional de seguridad efectivo, una habilidad importante que deberás desarrollar es poder anticiparte a los ataques. Para lograrlo, debes mantener una mentalidad abierta y flexible en cuanto a su procedencia. Antes, aprendiste sobre las **superficies de ataque**, que son todas las vulnerabilidades potenciales que un agente de amenaza podría explotar.

Las redes, los servidores, los dispositivos y el personal son ejemplos de superficies de ataque que pueden explotarse. Con frecuencia, los equipos de seguridad de todos los tamaños se encuentran defendiendo estas superficies debido al panorama digital en expansión. La clave para defender cualquiera de ellos es limitar su acceso.

En esta lectura, profundizarás en los agentes de amenaza y los tipos de riesgos que representan. También explorarás las características más comunes de una superficie de ataque que los agentes de amenaza pueden explotar.

Agentes de amenaza

Un **agente de amenaza** es cualquier persona o grupo que plantea un riesgo para la seguridad. Esta definición a grandes rasgos abarca a personas tanto dentro como fuera de una organización. También incluye a personas que intencionalmente representan una amenaza y quienes ponen en riesgo los activos por accidente. ¡Es una amplia variedad de personas!

Por lo general, los agentes de amenaza se dividen en cinco categorías según sus motivaciones:

- La **competencia** refiere a las empresas rivales que representan una amenaza porque podrían beneficiarse de la información filtrada.
- Los **actores estatales** son agencias de inteligencia del gobierno.
- Los **sindicatos criminales** son grupos organizados de personas que ganan dinero mediante actividades delictivas.
- Las **amenazas internas** pueden ser cualquier persona que tenga o haya tenido acceso autorizado a los recursos de una organización. Esto incluye a los empleados que comprometen los activos por accidente o individuos que los ponen en riesgo de manera intencional, para su propio beneficio.

- **Shadow IT** hace referencia a individuos que utilizan tecnologías que carecen de gobernanza de TI. Un ejemplo común es cuando un empleado usa su correo electrónico personal para enviar comunicaciones relacionadas con el trabajo.

En la superficie de ataque digital, estos agentes de amenaza a menudo obtienen acceso no autorizado al hackear los sistemas. Por definición, un **hacker** es cualquier persona o grupo que utiliza computadoras para acceder a datos sin autorización. Al igual que el término actor de amenazas, hacker es también un término general. Cuando se usa solo, el término no consigue captar las intenciones de un agente de amenaza.



Tipos de hackers

Debido a que la definición formal de hacker es amplia, el término puede ser un poco ambiguo. En seguridad, corresponde a tres tipos de personas en función de su intención:

1. Hackers no autorizados
2. Hackers autorizados o éticos
3. Hackers semiautorizados

Un hacker no autorizado, o hacker no ético, es un individuo que utiliza sus habilidades de programación para cometer delitos. A los hackers no autorizados también se los conoce como hackers maliciosos. El nivel de habilidad varía ampliamente dentro de esta categoría de hackers. Por ejemplo, existen hackers con habilidades limitadas que no pueden escribir su propio software malicioso, a veces llamado *script kiddies* (niñitos del script). Este tipo de hackers no autorizados llevan a cabo ataques mediante un código preescrito que obtienen de otros hackers más hábiles.

Los hackers autorizados, o éticos, son personas que utilizan sus habilidades de programación para mejorar la seguridad general de una organización. Estos incluyen a miembros internos de un equipo de seguridad que se ocupan de probar y evaluar los sistemas para asegurar la superficie de ataque. También se trata de proveedores de seguridad externos y hackers independientes que algunas empresas incentivan para

encontrar y reportar vulnerabilidades, una práctica llamada programas de **recompensas por errores**.

Por lo general, los hackers semiautorizados son individuos que podrían violar estándares éticos, pero que no son considerados como maliciosos. Por ejemplo, un **hacktivista** es una persona que podría usar sus habilidades para lograr un objetivo político. Podría explotar las vulnerabilidades de seguridad de una empresa de servicios públicos para concientizar sobre su existencia. Las intenciones de este tipo de agentes de amenaza suelen consistir en exponer los riesgos de seguridad que deben abordarse antes de que un hacker malicioso los encuentre.

Amenazas persistentes avanzadas

Muchos hackers maliciosos consiguen ingresar en un sistema, causan problemas y luego se marchan. Pero en algunas ocasiones, los agentes de amenaza se quedan. Este tipo de eventos se conocen como amenazas persistentes avanzadas, o APT.

Una **amenaza persistente avanzada (APT)** hace referencia a los casos en que un actor de amenazas mantiene el acceso no autorizado a un sistema durante un período prolongado de tiempo. El término se asocia principalmente con los estados nacionales y los agentes patrocinados por el Estado. Por lo general, una APT se ocupa de vigilar un objetivo para recopilar información. Luego esta información se utiliza para manipular los servicios gubernamentales, de defensa, financieros y de telecomunicaciones.

El hecho de que el término esté asociado con agentes estatales no significa que las empresas privadas estén a salvo de las APT. Este tipo de agentes de amenaza son sigilosos porque hackear otra agencia gubernamental o empresa de servicios públicos es costoso y consume mucho tiempo. Las APT suelen apuntar primero a organizaciones privadas como un paso hacia el acceso a entidades más grandes.

Puntos de acceso

Cada agente de amenaza tiene una motivación específica a la hora de establecer los activos de una organización como objetivo. Mantenerlos alejados requiere más que conocer sus intenciones y capacidades. También es importante reconocer los tipos de vectores de ataque que utilizarán.

En su mayor parte, los agentes de amenaza obtienen acceso a través de una de estas categorías de vectores de ataque:

- **Acceso directo**, que hace referencia a instancias en las que tienen acceso físico a un sistema.
- **Medios extraíbles**, que incluyen hardware portátil, como unidades USB.
- **Plataformas de redes sociales** que se utilizan para la comunicación y el intercambio de contenido.
- **Correo electrónico**, incluidas las cuentas personales y comerciales.
- **Redes inalámbricas** en las instalaciones.

- **Servicios en la nube** que por lo general son proporcionados por organizaciones de terceros.
- **Cadenas de suministro**, como proveedores externos que pueden presentar una puerta trasera en los sistemas.

Cualquiera de estos vectores de ataque puede proporcionar acceso a un sistema.

Reconocer las intenciones de un actor de amenazas puede ayudarte a determinar a qué puntos de acceso podrían apuntar, y cuáles podrían ser sus objetivos. Por ejemplo, es más probable que los trabajadores remotos presenten una amenaza por correo electrónico, que una amenaza de acceso directo.

Triada CID

es un modelo que ayuda los organizadores a evaluar los riesgos y configurar sistemas y políticas de seguridad

- Confidencialidad : implica que solo los usuarios autorizados tienen acceso a ciertos datos.
- Integridad: Implica que los datos sean correctos, auténticos y confiables
- Disponibilidad: Implica que solo puedan acceder a ellos quienes tengan la autorización.
-

Técnicas de reforzamiento en la red

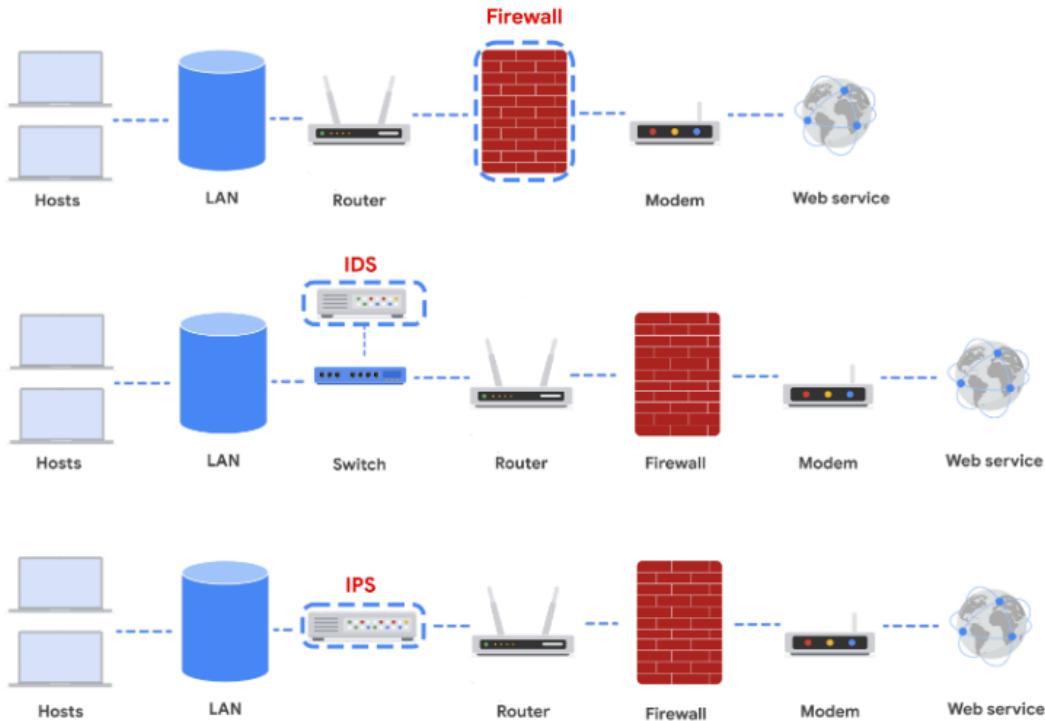
- mantenimiento de reglas del firewall
- análisis de registro de red
- actualización de parches
- respaldos del servidor

EL análisis de registro de red

es el proceso de examinar los registros de la red para identificar eventos de interés como un SIEM

Una herramienta SIEM es una aplicación que recopila y analiza datos de registro para monitorear actividades críticas en una organización. Recopila datos de seguridad de la red y los presenta en un solo panel. La interfaz del panel a veces se llama panel único.

Filtrado de puertos : Es una función que bloquea o permite ciertos números de puerto para limitar la comunicación no deseada.



Cortafuegos (firewall)

Hasta el momento en el curso, aprendiste sobre cortafuegos (firewalls) sin estado, con estado, de próxima generación (NGFW), y conociste las ventajas de seguridad de cada uno de ellos.

La mayoría de los firewalls son similares en sus funciones básicas. Todos permiten el tráfico o lo bloquean en función de un conjunto de reglas. A medida que los paquetes de datos entran en una red, se inspecciona el encabezado del paquete para permitir o denegar su acceso en función de su número de puerto. Los NGFW también pueden inspeccionar cargas útiles de paquetes. Cada sistema debe tener su propio firewall, independientemente del de la red.

Sistema de detección de intrusiones

Un **sistema de detección de intrusiones** (IDS) es una aplicación que monitorea la actividad del sistema y alerta sobre posibles intrusiones. Un IDS alerta a los/las administradores/as en función de la firma del tráfico malicioso.

El IDS está configurado para detectar ataques conocidos. Los sistemas IDS suelen detectar paquetes de datos a medida que se mueven por la red, y los analizan en busca de las características de ataques conocidos. Algunos sistemas IDS revisan no solo las firmas de ataques conocidos, sino también las anomalías que podrían ser el signo de actividad maliciosa. Cuando el IDS descubre una anomalía, envía una alerta al/ a la administrador/a de la red que luego investigará más a fondo.

La limitación de los sistemas IDS reside en que solo pueden escanear en busca de ataques conocidos o anomalías obvias. Es posible que no se detecten ataques nuevos y sofisticados. La otra limitación es que el IDS en realidad no detiene el tráfico entrante si detecta algo mal. Depende del/de la administrador/a de la red detectar la actividad maliciosa antes de que haga algo perjudicial.



Sistema de prevención de intrusiones

Un **sistema de prevención de intrusiones (IPS)** es una aplicación que monitorea la actividad del sistema en busca de actividad intrusiva y toma medidas para detenerla. Ofrece aún más protección que un IDS porque detiene activamente las anomalías cuando se detectan, a diferencia del IDS que simplemente las informa a un/a administrador/a de red.

Un IPS busca firmas de ataques conocidos y anomalías de datos a las/los analistas de seguridad y bloquea un remitente específico o deja caer paquetes de red que parecen sospechosos.



El IPS (como un IDS) se encuentra detrás del firewall en la arquitectura de red. Esto ofrece un alto nivel de seguridad porque los flujos de datos peligrosos se interrumpen incluso antes de que lleguen a partes sensibles de la red. Sin embargo, una limitación potencial es que se trata de un dispositivo inline (interpuesto en el flujo de datos), lo cual significa que el flujo de datos pasa a través de sus interfaces de red: si falla, la conexión entre la red privada e Internet deja de funcionar. Otra limitación del IPS es que se generen falsos positivos, que pueden llevar a la caída de tráfico legítimo.

Dispositivos de captura de paquetes completos

Los dispositivos de captura de paquetes completos pueden ser muy útiles para administradores de red y profesionales de seguridad. Estos dispositivos permiten registrar y analizar todos los datos que se transmiten a través de la red. También ayudan a investigar las alertas creadas por un IDS.

Gestión de eventos e información de seguridad

Un **sistema de gestión de eventos e información de seguridad (SIEM)** es una herramienta que recopila y analiza datos de registro para monitorear actividades críticas en una organización. Las herramientas SIEM funcionan en tiempo real para informar las actividades sospechosas, a través de un panel de control centralizado. Las herramientas SIEM también analizan los datos de registro de red procedentes de IDS, IPS, cortafuegos, VPN, proxies y registros de DNS. Las herramientas SIEM son una forma de agregar datos de eventos de seguridad a fin de que todo aparezca en un solo lugar para que las/los analistas de seguridad lo analicen. Esto se conoce como panel único.

A continuación, puedes analizar un ejemplo de un panel de la herramienta SIEM de Google Cloud, Chronicle. **Chronicle** es una herramienta nativa de la nube diseñada para conservar, analizar y buscar datos.

Conclusiones clave

Dispositivos/Herramientas	Ventajas	Desventajas
Cortafuegos (Firewall)	Los firewalls permiten o bloquean el tráfico en función de un conjunto de reglas.	Un firewall solo puede filtrar paquetes basándose en la información proporcionada en su encabezado.
Sistema de detección de intrusiones (SDI)	Un IDS detecta y alerta a los/las administradores/as sobre posibles intrusiones, ataques y otro tráfico malicioso.	Un IDS solo puede escanear en busca de ataques conocidos o anomalías obvias; es posible que no se detecten ataques nuevos y sofisticados. Tampoco detiene el tráfico entrante.
Sistema de prevención de intrusiones (IPS)	Un IPS monitorea la actividad del sistema en busca de intrusiones y anomalías y toma medidas para detenerlas.	Un IPS es un dispositivo inline. Si falla, la conexión entre la red privada e Internet se interrumpe. Puede detectar falsos positivos y bloquear el tráfico legítimo.
Gestión de eventos e información de seguridad (SIEM)	Una herramienta SIEM recopila y analiza datos de registro de múltiples máquinas de red. Agrega eventos de seguridad para su monitoreo en un panel de control central.	Una herramienta SIEM solo informa sobre posibles problemas de seguridad. No toma ninguna acción para detener o prevenir eventos sospechosos.

Términos del glosario de la semana 4

Términos y definiciones del Curso 6, Semana 4

Análisis basado en anomalías: Método de detección que busca identificar comportamientos atípicos a partir del análisis de un conjunto de datos.

Análisis de firmas: Método de detección que busca identificar eventos sospechosos o maliciosos.

Análisis de registros: Proceso de examinar los registros para identificar eventos de interés.

Archivo de configuración: Archivo utilizado para configurar los parámetros de una aplicación.

Array: Tipo de dato estructurado que permite almacenar un conjunto de datos homogéneo, es decir, del mismo tipo y relacionados, en una lista ordenada separada por comas.

Comodín: Carácter especial que puede sustituir a cualquier otro.

Detección y respuesta de puntos de conexión (EDR): Aplicación que monitorea un punto de conexión para detectar actividad maliciosa.

Día cero: Vulnerabilidad recién descubierta.

Falso positivo: Alerta que detecta erróneamente la presencia de una amenaza.

Firma: Patrón asociado a una actividad maliciosa.

Formato de evento común (CEF): Formato de registro que utiliza parejas clave-valor para estructurar los datos e identificar los campos y sus valores correspondientes.

Gestión de eventos e información de seguridad (SIEM, por sus siglas en inglés):

Solución de seguridad que recopila y analiza los datos de registro para monitorear actividades críticas en una organización.

Gestión de registros: Proceso de recopilación, almacenamiento, análisis y eliminación de datos de registro.

Lenguaje de procesamiento de búsqueda (SPL): Lenguaje de consulta de Splunk.

Objeto: Tipo de datos, en JavaScript, que almacena datos en una lista separada por comas de parejas clave-valor.

Pareja clave-valor: Conjunto de datos que representa dos elementos vinculados: una clave y su valor correspondiente.

Punto de conexión (endpoint): Cualquier dispositivo conectado a una red.

Registro (Log): Inventario de eventos que tienen lugar dentro de los sistemas de una organización.

Sistema de detección de intrusiones (IDS, por sus siglas en inglés): Aplicación que monitorea la actividad del sistema y alerta sobre posibles intrusiones.

Sistema de detección de intrusiones basado en la red (NIDS, por sus siglas en inglés): Aplicación que recopila y monitorea el tráfico y los datos de la red.

Sistema de detección de intrusiones basado en host (HIDS, por sus siglas en inglés):

Aplicación que monitorea la actividad del host en el que está instalada.

Suricata: Sistema de monitoreo de redes de código abierto para la detección y prevención de amenazas.

Telemetría: Recopilación y transmisión de datos para su análisis.

YARA-L: Lenguaje informático utilizado para crear reglas de búsqueda en los datos de registro ingeridos.

un modelo de amenaza

Las amenazas son toda circunstancia o evento que pueden perjudicar los activos.

1. Definir el alcance del modelo de amenaza aquí genera un inventario de activos y clasificarlos
2. Identificar amenazas : define todos los agentes de peligro potenciales
3. Caracterizar el entorno: Se adapta la mentalidad de atenuante la empresa analiza como los clientes y los empleados interactúan con el entorno.
4. Analizar las amenazas:: Aquí se examinan las protecciones existentes e identifica las brechas , luego clasifica las amenazas según la puntuación de riesgo asignadas
5. Mitigación de riesgo : El grupo crea un plan para defenderse de las amenazas . Las opciones son evitar el riesgo, transferirlo , reducirlo o aceptarlo
6. Evaluar los hallazgos: En esta etapa todo lo que se hizo se documenta, se aplica correcciones y se toma nota de cualquier éxito.

Video firewalls

El firewall es

Tipos de Firewalls

- Los firewalls de hardware son dispositivos físicos que inspeccionan cada paquete de datos antes de que pueda ingresar a una red.
- Los firewalls de software son programas instalados en computadoras o servidores que analizan el tráfico recibido y protegen los dispositivos conectados.

Funcionamiento de los Firewalls

- Los firewalls con estado rastrean la información que los atraviesa y filtran de forma proactiva las amenazas potenciales basándose en patrones sospechosos.
- Los firewalls sin estado funcionan con reglas predefinidas y no almacenan información sobre el tráfico, lo que los hace menos seguros que los firewalls con estado.

Recuerda: Los firewalls son esenciales para la seguridad de la red. ¡Comprender los diferentes tipos y cómo funcionan te ayudará a tomar decisiones informadas sobre la protección de tus propios dispositivos y redes!

Un firewall es un dispositivo de seguridad que monitorea el tráfico en la red, autoriza o bloquea el tráfico según el conjunto de reglas de seguridad.

Filtrar Puertos para bloquear o permitir ciertos número de puerto y limitar la comunicación indeseada.

Statefull es un cortafuegos que hace un seguimiento de la información que pasa a través de él y filtra proactivamente las amenazas, este busca características y comportamientos sospechosos del tráfico y evita que entre en la red, este funciona según las reglas que nosotros ponemos las reglas

Los cortafuegos de última generación o NGFW ofrece seguridad que un cortafuego stateful, hace todo el Stateful y también realiza funciones más profundas como la inspección porfunda de paquetes y protección contra intrusiones, también pueden incluir servicios de inteligencia de amenazas basados en la nube para protegerse contra las amenazas cibernéticas

Vinculación de los marcos y los controles

Se incluyen en los marcos de gestión de riesgos (RMF) y el marco de ciberseguridad (CSF)

Marcos y controles

Son pautas utilizadas para elaborar planes que ayuden a mitigar los riesgos y las amenazas a los datos y la privacidad. En el sector salud se usan los marcos para cumplir con La Ley de Transferencia y Responsabilidad de los Seguros Médicos (HIPPA)

Controles de seguridad, en tanto son medidas de protección diseñadas para reducir riesgos de seguridad específicos

Estas medidas son usadas por la organización para disminuir los riesgos y marcos de seguridad

MARCOS DE SEGURIDAD ESPECÍFICOS

Cyber Threat Framework

Fue diseñado por EU para proporcionar " un lenguaje comun para describir y comunicar informacion sobre la actividad de amenazas ciberneticas" por lo tanto ayuda a los profesionales de seguridad a analizar y compartir informacion de manera mas eficiente , esto permite a las organizaciones majorar su respuesta dado a que las tecnicas de los agentes de amenaza son multiples y por lo tanto la ciberseguridad esta en constante evolucion.

Organización Internacional de Normalización/Comisión Electrotécnica Internacional (ISO/IEC) 27001

Un marco reconocido internacionalmente y muy utilizado es el ISO/IEC 27001. El conjunto de normas ISO 27000 permite a las organizaciones de todos los sectores y tamaños gestionar la seguridad de sus activos, como la información financiera, la propiedad intelectual, los datos del personal y la información confiada a terceros. Este marco establece los requisitos para un sistema de gestión de seguridad de la información, las prácticas recomendadas y los controles que respaldan la capacidad de una organización para gestionar los riesgos. Si bien el marco ISO/IEC 27001 no exige el uso de controles específicos, proporciona una serie de controles que las empresas pueden utilizar para mejorar su postura de seguridad.

Controles

Los controles se utilizan junto con los marcos para reducir la posibilidad y el impacto de una amenaza, riesgo o vulnerabilidad de seguridad. Estos pueden ser físicos, técnicos y administrativos, y se utilizan típicamente para prevenir, detectar o corregir problemas de seguridad.

Ejemplos de controles físicos:

- Puertas, barreras y cerraduras
- Guardias de seguridad
- Vigilancia por circuito cerrado de televisión (CCTV), cámaras y detectores de movimiento
- Tarjetas de acceso o credenciales para ingresar a los espacios de la oficina

Ejemplos de controles técnicos:

- Cortafuegos (firewalls)
- Autenticación de múltiples factores (MFA)
- Software de antivirus

Ejemplos de controles administrativos:

- Separación de funciones
- Autorización
- Clasificación de activos

Para obtener más información sobre los controles, especialmente aquellos utilizados para proteger activos relacionados con la salud de diversos tipos de amenazas, consulta la [presentación sobre Control de Acceso Físico del Departamento de Salud y Servicios Humanos de los Estados Unidos.](#)

Vulnerabilidades y exposiciones comunes

Exposición: es un error que una amenaza puede explotar

Una de las bibliotecas de vulnerabilidades y exposiciones comunes o lista CVE es un diccionario de libre acceso de vulnerabilidades y exposiciones conocidas . Las empresas usan la lista CVE para mejorar sus defensas

Fue creada por la MITRE Corporation en 1999 , MITRE es una serie de control de investigación de desarrollo sin fines de lucro por el gobierno EEUU. se centran en mejorar la seguridad del mundo . El objetivo es disminuir las vulnerabilidades . Estos grupos tienen un historial probado de investigación de vulnerabilidades y capacidades de asesoría de ciberseguridad.

La lista CVE realiza pruebas con cuatro criterios que la vulnerabilidad debe tener para asignarle una identificación:

1. Independiente a otros problemas: la vulnerabilidad debe poder corregirse sin que haya que corregir otra cosa.
2. Quien la reporta debe reconocerla como riesgo potencial
3. La vulnerabilidad debe representarse como prueba de apoyo
4. La vulnerabilidad debe presentarse como pruebas de apoyo , reportada solo puede afectar una base de código

Common Vulnerability Scoring System (CVSS)

Es un sistema de medición que puntúa la gravedad de una vulnerabilidad. Los equipos usan el CVSS para calcular el impacto potencial de una vulnerabilidad de un sistema.

también se usa para ver que tan rápido puede parcharse una vulnerabilidad

Las puntuaciones reflejan el momento en que la vulnerabilidad se evalúa, y no cambian con el tiempo. En general, una puntuación CVSS menor a 4.0 se considera de bajo riesgo, y no requiere atención inmediata. En cambio, una puntuación mayor a 9.0 representa un riesgo crítico para los activos de una organización y debe abordarse de inmediato.

Vías de acceso a través de las defensas

Mentalidad del atacante

- Identificar el objetivo: puede ser un sistema, una persona , un grupo o empresa en si.
- Determinar que información hay que un atacante pude aprovechar
- Evaluar los vectores de ataque que pueden ser explotados para acceder
- Buscamos la herramientas y el método de ataque

Proteger los vectores de ataque

- Educar a los usuarios
- Aplicar el principio del mínimo privilegio
- Usar los controles de seguridad y reglas para mantener seguros
- Crear un equipo de seguridad diverso

wikilabs

Sugerencias para labs y pasos para solucionar problemas

A lo largo de esta certificación, usarás Qwiklabs y notebooks de Jupyter para completar actividades prácticas que incluyen la línea de comandos de Linux, la captura de paquetes y tareas de programación en Python. En esta lectura, abordaremos algunas sugerencias y pasos para solucionar problemas relacionados con el uso de Qwiklabs y notebooks de Jupyter en tu computadora.

Compatibilidad del navegador

Asegúrate de que tu navegador de Internet se actualice con regularidad. Qwiklabs y los notebooks de Jupyter requieren la versión más reciente de Google Chrome, Firefox o Microsoft Edge. Si tu navegador está desactualizado o utilizas uno que no es compatible con Qwiklabs o los notebooks de Jupyter, es posible que tengas problemas. Si tu navegador es uno los mencionados y lo tienes actualizado, pero sigues teniendo problemas, intenta reiniciarlo o borrar su caché y sus cookies. También puedes usar el modo Incógnito, que impide que el navegador almacene cookies y otros datos temporales.

Nota: La interfaz de usuario de Qwiklabs funciona mejor con Google Chrome.

Conexión a Internet

Qwiklabs y los notebooks de Jupyter requieren una conexión a Internet estable. Si tienes problemas para iniciarlos o para completar actividades en ellos, es posible que tu conexión a Internet sea lenta o inestable. Algunos indicadores de una conexión a Internet inestable pueden ser que las pantallas de los labs se congelen, la dificultad para conectarse a las máquinas virtuales o la imposibilidad de escribir o ingresar comandos en el entorno del lab.

Sugerencia profesional: Si no puedes completar un Qwiklab o un lab de notebooks de Jupyter en un dispositivo, intenta usar otro.

Pasos para solucionar problemas

En resumen, estos son los pasos que debes seguir para solucionar problemas con Qwiklabs o notebooks de Jupyter.

1. Asegúrate de usar la versión más reciente de un navegador compatible, como Google Chrome, Firefox o Microsoft Edge.
2. Reinicia el navegador y borra las cookies y la caché del navegador. También puedes usar el modo Incógnito.
3. Revisa tu conexión a Internet y asegúrate de que sea estable. Puedes reiniciar el router y el módem para volver a tener una conexión estable.
4. Vuelve a reiniciar Qwiklabs o los notebooks de Jupyter.
5. **Solo para Qwiklabs:** Si los problemas persisten o recibes un mensaje que indica que superaste la cuota de un Qwiklab, envía este [formulario](#) al equipo de asistencia de Qwiklabs para obtener ayuda.