Índice

Contenido

Ejemplo de evaluación de controles

Activos actuales

Entre los activos administrados por el departamento de TI se encuentran los siguientes:

- Equipos en las instalaciones para las necesidades comerciales en la oficina.
- Equipos del personal: dispositivos de usuario final (computadoras de escritorio/portátiles, teléfonos inteligentes), estaciones de trabajo remotas, auriculares, cables, teclados, mouse, estaciones de acoplamiento, cámaras de vigilancia, etc.
- Gestión de sistemas, software y servicios: contabilidad, telecomunicaciones, bases de datos, seguridad, comercio electrónico y gestión de inventario.
- Acceso a Internet.
- Red interna.
- Gestión de acceso a proveedores.
- Servicios de alojamiento del centro de datos.
- Retención y almacenamiento de datos.
- Lectores de tarjetas de identificación.
- Mantenimiento de sistemas heredados: sistemas obsoletos que requieren supervisión humana.

Controles administrativos			
Nombre de control	**Tipo de control y explicación**	**Se tiene que implementar (X)**	**Prioridad**
Principios de mínimo privilegio	Preventivo. Reducir el riesgo asegurándose de que proveedores y el personal no autorizado solo tengan acceso a los activos/datos que necesitan para realizar	X	Alto

Controles administrativos			
	su trabajo.		
Planes de recuperación ante incidentes	Correctivo. Garantizar la continuidad del negocio, asegurando que los sistemas puedan ejecutarse en caso de incidentes, que no haya pérdida de productividad por tiempo de inactividad ni impacto en los componentes del sistema, que incluyen, entorno de la sala de computadoras (aire acondicionado, fuentes de alimentación, etc.), hardware (servidores, equipos de empleados), conectividad (red interna, inalámbrica), aplicaciones (correo electrónico, datos electrónicos), así como datos y restauración.	X	Alto
Políticas de contraseñas	Preventivo. Establecer requisitos de seguridad de contraseñas para reducir la probabilidad de comprometer la cuenta debido a técnicas de ataque por fuerza bruta o diccionario.	X	Alto
Políticas de control de acceso	Preventivo. Aumentar la confidencialidad e integridad de los datos.	X	Alto
Políticas de gestión de cuentas	Preventivo. Reducir la superficie expuesta a ataques y limita el impacto general de ex empleados/as disconformes.	X	Alto/ Medio

Controles administrativos			
Separación de funciones	Preventivo. Garantizar que nadie tenga tanto acceso que pueda abusar del sistema para obtener beneficios personales.	X	Alto

Controles técnicos			
Nombre de control	**Tipo de control y explicación**	**Se tiene que implementar (X)**	**Prioridad**
Cortafuegos (firewall)	Preventivo. Ya hay instalados firewalls para filtrar el tráfico no deseado/malicioso que ingresa a la red interna.	N/D	N/D
Sistema de detección de intrusiones (IDS)	De detección. Permitir al equipo de TI identificar posibles intrusiones (por ejemplo, tráfico anómalo) rápidamente.	X	Alto
Cifrado	Disuasivo. Garantizar que la información y los datos confidenciales sean más seguros (por ejemplo, transacciones de pago en el sitio web).	X	Alto/ Medio
Copias de seguridad	Correctivo. Permitir la continuidad del negocio y mantener la productividad en caso de incidentes, al mantener los sistemas funcionando	X	Alto

Gestión de contraseñas	Correctivo. Recuperar y restablecer contraseñas, bloqueo de notificaciones.	X	Alto/ Medio
Software de antivirus (AV)	Correctivo. Detectar amenazas conocidas y aislarlas.	X	Alto
Monitoreo manual, mantenimiento e intervención	Preventivo/correctivo. Necesario para que los sistemas heredados identifiquen y mitiguen posibles amenazas, riesgos y vulnerabilidades.	X	Alto

Controles físicos			
Nombre de control	**Tipo de control y objetivo**	**Se tiene que implementar (X)**	**Prioridad**
Caja fuerte con control de tiempo	Disuasivo. Reducir la superficie expuesta a ataque y el impacto de las amenazas físicas.	X	Medio/ Bajo
Iluminación adecuada	Disuasivo. Limitar los lugares "ocultos" para disuadir las amenazas.	X	Medio/ Bajo
Vigilancia del circuito cerrado de televisión (CCTV)	Preventivo/De detección. Reducir el riesgo de ciertos eventos y ver qué sucedió después del incidente, al llevar a cabo una investigación.	X	Alto/ Medio

Cerradura de gabinetes (para equipos de red)	Preventivo. Aumentar la integridad al evitar que personas no autorizadas accedan físicamente o modifiquen el equipo de infraestructura de la red.	X	Medio
Carteles que indican el nombre de la empresa proveedora del servicio de alarmas	Disuasivo. Reducir la probabilidad de éxito de ciertos tipos de amenazas al dar la apariencia de que un ataque exitoso es poco probable.	X	Bajo
Cerraduras	Preventivo. Lograr que los activos físicos y digitales estén más seguros.	X	Alto
Detección y prevención de incendios (alarma de incendios, sistema de rociadores, entre otros)	De detección/Preventivo. Detectar incendios en la ubicación física de la juguetería para evitar daños en el inventario, servidores, entre otros.	X	Medio/ Bajo

Ejemplo de la lista de control de cumplimiento normativo

Para revisar las regulaciones y estándares de cumplimiento, lee el documento sobre controles, marcos y cumplimiento normativo.

_____ La Comisión Federal Reguladora de Energía, Corporación de Confiabilidad Eléctrica América del Norte (FERC-NERC)

La normativa FERC-NERC se aplica a organizaciones que trabajan con electricidad o que están involucradas con la red eléctrica de los Estados Unidos y América del Norte. Las empresas 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.

Explicación: no disponible

__X__ Reglamento General de Protección de Datos (RGPD)

El RGPD es una regulación 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. Además, si se produce una filtración y los datos de una persona se ven comprometidos, esto debe ser informado en un plazo de 72 horas posteriores al incidente.

Explicación: Botium Toys debe cumplir con el RGPD porque trabaja con personas (y recopila su información) de todo el mundo, incluida la UE.

__X__ Estándares de seguridad de datos del sector de las tarjetas de pago (PCI DSS)

PCI DSS es un estándar internacional destinado a garantizar que las organizaciones que almacenan, aceptan, procesan y transmiten información de tarjetas de crédito lo hagan en un entorno seguro.

Explicación: Botium Toys debe cumplir con las PCI DSS porque almacena, acepta, procesa y transmite información de tarjetas de crédito tanto de forma presencial como en línea.

_____ 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/a paciente se comparta sin su consentimiento. Las organizaciones tienen la obligación legal de

informar a los/as pacientes en caso de que esta información se filtre.

Explicación: no disponible

__X__ Controles de Sistemas y Organizaciones (SOC tipo 1, SOC tipo 2)

El SOC1 y el SOC2 se enfocan en las políticas de acceso de las usuarias y los usuarios de una organización en los diferentes niveles. Se utilizan para evaluar el cumplimiento financiero de una organización, así como los niveles de riesgo asociados. También abordan aspectos críticos como la confidencialidad, privacidad, integridad, disponibilidad, seguridad y protección general de los datos. Es importante destacar que cualquier falla en el control de estos aspectos puede resultar en posibles fraudes.

Explicación: Es necesario que Botium Toys cree y haga cumplir el acceso adecuado del personal interno y externo (proveedores externos), a fin de mitigar los riesgos y garantizar la seguridad de los datos.

Material de apoyo:

- https://d3c33hcgiwev3.cloudfront.net/MB29ozNEQYWwg5V_Yi-hCw_1afea47ea75b495facfb6ab5a32201f1_Portfolio-Activity-Conduct-a-security-audit-Part-1_Botium-Toys_-Audit-scope-and-goals.docx?Expires=1703721600&Signature=X-1xmDCERlXhBQ0-5U-fONMBO2d4C7kiplXtZYN9QajI7bhWFPdWXI2myGsSy4nral~Pkq9ItJfurtH1HoBuP4vSIjlX5BuegZULEsWT24knGSaI-TRauiYj-2b8KMqnH7BDwGvYh6LlmrEx0RYOPccPlJeKO1w1kT5JIdbc42s_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A
- https://d3c33hcgiwev3.cloudfront.net/XsOZ1JafRSSTcHMiXzvZrA_b502e8ba736d43a9a88e488b29b472f1_Portfolio-Activity-Conduct-a-security-audit-Part-1_Botium-Toys_-Risk-assessment.docx?Expires=1703721600&Signature=R12yDMPVRn9C0GxeK6SP2tQlXRblZ2shi~u-fmdq0zv2~F8oSFgClgNCR6mg5DaEfLvBd8AES3ujEGRwFhrOGYvqkvbc~rTPSBX-wJFIBk2OSelhsy~Ajqhq-

Cgqp7A6g8pScK8ugynexS~~QONFwHNtoiAl~MHbH0nnyrANPZ4_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A

Memorándum para las partes interesadas

PARA: Gerente de TI, partes interesadas
DE: Alvarado Carlos
FECHA: 10 de Noviembre del 2023
ASUNTO: Hallazgos y recomendaciones de la auditoría interna de TI

Estimados/as compañeros/as:

Revise la siguiente información sobre el alcance, los objetivos, los hallazgos críticos, el resumen y las recomendaciones de la auditoría interna de Botium Toys.

Alcance:

- Los siguientes sistemas están dentro del alcance: contabilidad, detección de puntos finales, firewalls, sistema de detección de intrusiones, herramienta SIEM. Los sistemas serán evaluados para:
    - Permisos de usuario actuales
    - Controles implementados actualmente
    - Procedimientos y protocolos actuales
- Asegúrese de que los permisos, controles, procedimientos y protocolos de usuario actuales estén alineados con los requisitos de cumplimiento de PCI DSS y GDPR.
- Asegúrese de que la tecnología actual tenga en cuenta tanto el acceso al hardware como al sistema.

Objetivos:

- Adhiérase al NIST CSF.

- Establecer un mejor proceso para sus sistemas para garantizar que cumplan.
- Fortalecer los controles del sistema.
- Adáptese al concepto de permisos mínimos cuando se trata de gestión de credenciales de usuario.
- Establecer sus políticas y procedimientos, que incluyen sus manuales.
- Asegúrese de que cumplan con los requisitos de cumplimiento.

Hallazgos críticos (deben abordarse de inmediato):

- Es necesario desarrollar e implementar múltiples controles para cumplir con los objetivos de la auditoría, incluyendo:
    - Control de privilegios mínimos y separación de funciones
    - Planes de recuperación de desastres
    - Políticas de contraseñas, control de acceso y gestión de cuentas, incluida la implementación de un sistema de gestión de contraseñas.
    - Cifrado (para transacciones seguras en sitios web)
    - identificación
    - Copias de seguridad
    - software audiovisual
    - circuito cerrado de televisión
    - Cerraduras
    - Monitoreo, mantenimiento e intervención manuales para sistemas heredados
    - Sistemas de detección y prevención de incendios.
- Es necesario desarrollar e implementar políticas para cumplir con los requisitos de PCI DSS y GDPR.
- Es necesario desarrollar e implementar políticas para alinearse con las pautas SOC1 y SOC2 relacionadas con las

políticas de acceso de los usuarios y la seguridad general de los datos.

Hallazgos (deben abordarse, pero no son necesarios de inmediato):

- Cuando sea posible, se deben implementar los siguientes controles:
    - Caja fuerte con control de tiempo
    - Iluminación adecuada
    - Gabinetes con cerradura
    - Señalización que indica proveedor de servicios de alarma

Resumen/Recomendaciones: Se recomienda que los hallazgos críticos relacionados con el cumplimiento de PCI DSS y GDPR se aborden de inmediato, ya que Botium Toys acepta pagos en línea de clientes de todo el mundo, incluida la UE. Además, dado que uno de los objetivos de la auditoría es adaptarse al concepto. de permisos mínimos, se deben utilizar las pautas SOC1 y SOC2 relacionadas con las políticas de acceso de los usuarios y la seguridad general de los datos para desarrollar políticas y procedimientos apropiados. Tener planes de recuperación ante desastres y copias de seguridad también es fundamental porque respaldan la continuidad del negocio en caso de un incidente. La integración de un software IDS y AV en los sistemas actuales respaldará nuestra capacidad para identificar y mitigar riesgos potenciales y podría ayudar con la detección de intrusiones, ya que los sistemas heredados existentes requieren monitoreo e intervención manuales. Para proteger aún más los activos alojados en la ubicación física única de Botium Toys, se deben utilizar cerraduras y CCTV para proteger los activos físicos (incluido el equipo) y para monitorear e investigar amenazas potenciales. Si bien no es necesario de inmediato, el uso de cifrado y tener una caja fuerte con control de tiempo, iluminación adecuada,

gabinetes con cerradura, sistemas de detección y prevención de incendios y señalización que indique el proveedor de servicios de alarma mejorarán aún más la postura de seguridad de Botium Toys.

Material de apoyo:

- https://d3c33hcgiwev3.cloudfront.net/gaqNNHrJTfCdL12dkxA94Q_f19527180fec4652b22d7eb50612a6f1_Portfolio-Activity-Conduct-a-security-audit-Part-2_Botium-Toys_-Audit-scope-and-goals.docx?Expires=1703721600&Signature=Xf5hqrLlFiCR3O0OhlUOXs0ASAdPfehm08UAlzCOV2Yx4Z6AjGTs-rKbkxS7hzKsFyZ71bJqooqRHeubL0dK0K1MYThdrzP7fI7MiH94rcY4QsLZfT8c3qcIOGu10mOGqrd--9wia4z-ah7aBlC4CnAOqEy-N7TOmke3EFhA8Uk_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A

Informe sobre incidentes de ciberseguridad: Análisis del tráfico de red

Parte 1: Proporciona un resumen del problema encontrado en el registro de tráfico DNS e ICMP	**Explicación**
A. El protocolo UDP revela que el servidor DNS está caído o inaccesible. B. Como evidencian los resultados del análisis de la red, la respuesta de eco ICMP devolvió el mensaje de error "udp port 53 unreachable" (puerto udp 53 inaccesible). C. El puerto 53 se usa habitualmente	A. **Ofrece un breve resumen del análisis de los registros DNS e ICMP.** Siguiendo las instrucciones, deberías haber identificado "qué protocolo y servicio de red se vieron afectados por este incidente". En el escenario se indica: "[El archivo de registro] muestra qué protocolo se utilizó para gestionar las comunicaciones y a qué puerto se entregó. En el registro de errores, esto se muestra como "udp port 53 unreachable" (puerto udp 53 inaccesible). Esto significa que el protocolo UDP se usó para solicitar una resolución de nombre de dominio utilizando la dirección para el servidor DNS a través del puerto 53". B. **Proporciona algunos detalles sobre lo que se indicó en los registros:** La sección Escenario indica que realizaste un análisis de red utilizando tcpdump, que registró paquetes ICMP desde tu computadora de origen a la dirección IP y el puerto del sitio web (203.0.113.2.domain). También registró las respuestas ICMP desde el sitio web hacia tu computadora. Si revisas el registro de errores DNS e ICMP, las respuestas ICMP incluyen un tipo de mensaje de error, que tcpdump representa como "udp port 53

para el tráfico del protocolo DNS. Es muy probable que el servidor DNS no responda.	unreachable" (puerto udp 53 inaccesible). C. **Interpreta los problemas encontrados en los registros.** La sección Escenario (o una búsqueda rápida en Internet de "puerto 53") mostrará que este número de puerto se usa habitualmente para comunicaciones del protocolo DNS. Dado que el puerto 53 es inaccesible y que ese puerto se usa comúnmente para las comunicaciones del servidor DNS, puedes concluir que el servidor DNS es inaccesible o "no responde". Esto podría ser causado por un ataque DoS contra el servidor DNS, por ejemplo.

Parte 2: Explica tu análisis de los datos y proporciona una solución para implementar	**Explicación**
D. El incidente ocurrió hoy a la 1:23 p. m.	D. **Indica cuándo se notificó el problema por primera vez:** Esta información se obtuvo de las marcas de fecha y hora del archivo de registro. En el registro, esta es la primera secuencia de números que se muestra: 13:24:32.192571. Esto muestra la hora 1:24 p. m., 32.192571 segundos, con la hora en formato de 24 horas. El Escenario indica que este evento ocurrió hoy.
E. Las/los clientes llamaron a la	E. **Proporciona el escenario, los eventos y los síntomas identificados**

organización para notificar al equipo de TI que recibían el mensaje "puerto de destino inaccesible" cuando intentaban visitar el sitio web.	**cuando se informó por primera vez del evento:** El Escenario establece que "Un puñado de clientes se comunicaron con tu empresa para reportar que no podían acceder al sitio web de la compañía y vieron el error "puerto de destino inaccesible" después de esperar que la página se cargara".
F. Las/los profesionales de seguridad de la red de la organización están investigando el problema para que las/los clientes puedan acceder al sitio web nuevamente.	F. **Explica el estado actual del problema:** El Escenario establece que: "Este incidente, mientras tanto, está siendo manejado por ingenieros de seguridad después de que tanto tú como otros analistas hayan informado del problema a tu supervisor directo".
G. En nuestra investigación del problema, realizamos pruebas de rastreo de paquetes utilizando tcpdump. En el archivo de registro resultante, encontramos que el puerto DNS 53 era inaccesible.	G. **Describe la información descubierta en la investigación del problema hasta este momento:** Proporciona un resumen conciso de lo que hiciste para investigar el problema. El Escenario dice: "Visitas el sitio web y también recibes el error 'puerto de destino inaccesible'". 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. En el analizador, envías paquetes UDP y recibes una respuesta ICMP para regresar al host. Los resultados contienen un mensaje de error: "udp port 53 unreachable" (puerto udp 53 inaccesible).
H. El siguiente paso es identificar si el servidor DNS está caído o si el tráfico al puerto 53 está bloqueado por el cortafuegos.	H. **Enumera los siguientes pasos para solucionar el problema:** El siguiente paso para solucionar el problema es determinar si el servidor DNS no funciona correctamente. Si el servidor DNS está bien, el equipo debe verificar la configuración del cortafuegos (firewall)

I. El servidor DNS podría estar caído debido a un ataque de denegación de servicio exitoso o una configuración incorrecta.	para ver si alguien cambió la configuración para bloquear el tráfico de red en el puerto 53. Los firewalls ofrecen la capacidad de bloquear el tráfico de red en puertos específicos. El bloqueo de puertos se puede utilizar para detener o prevenir un ataque. I. **Proporciona la presunta causa raíz del problema:** Anteriormente, aprendiste acerca de varios tipos de ataques de denegación de servicio (DoS). El objetivo de un ataque DoS es enviar una gran cantidad de información a un dispositivo de red, como un servidor DNS, para bloquearlo o hacer que sea incapaz de responder al tráfico de red legítimo. Es posible que un/a atacante haya desactivado el servidor DNS con un ataque DoS. Otra posibilidad es que alguien de tu equipo haya realizado un cambio de configuración en el firewall que resultó en el bloqueo del puerto 53.

Material de apoyo:

- https://d3c33hcgiwev3.cloudfront.net/zBxAlhYBRWWI-s0nIAg6dQ_b65755de106540099e6c1af8ae0b04f1_Activity-Analyze-network-layer-communication_Cybersecurity-incident-report-network-traffic-analysis.docx?Expires=1703721600&Signature=SsJvOLE1TypVdxBHXTL-BJmxkmeWiOv7B7DicVeDEOgfijW0fCxCW7OLAoz3tjynCOOtDuFVh6~ug~618s6l5UDdvBL1s~VHHz43TjqMaIn7TNk7J86FRHMomvVBdbI1EysS~tjoTKb9W-~YCpG9Dmufq2rBWQIIdBUwn8-Vu9Y_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A

- https://d3c33hcgiwev3.cloudfront.net/riBQkqggSm2jtGJBnQ9goA_1d7c9cd3a5cb495fbb345f63fca561f1_Activity-Analyze-network-layer-communication_DNS-ICMP-traffic-log.docx?Expires=1703721600&Signature=L9a0tFJIE~ncGMnvtabxF80JukYpQhKczGNjhvcf0q8tpDObWO8YEQN5ROZ09~eHYupthjDq34jA61GA~c5l6Kbvplib4cpdr4WWU26b5TcAEigA6v6W5q76qtyrB5HKiWoLHawJJEheUcVb7n2V3SsJHAZ~llrf6HTae0MLQ8U_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A
- https://d3c33hcgiwev3.cloudfront.net/t-ObQyVXRcGAElbBgcRn-Q_4853cd085a964b8d8324e25be1e2c6f1_Activity-Analyze-network-layer-communication_Example-of-a-Cybersecurity-Incident-Report.docx?Expires=1703721600&Signature=Jq4lFj3DLevOTHH1hq-78-8zkBSDIOWfH0Nn7Ey-XRFQ5E1py2gayAdf04ZFdTk8VNMSzd6R5aJLaoX64WrDufjDZgMHMERbmkSjBcYszyF3~YpjcRaBm22e3eXMdb6c2TyX2c6QiQEwggNBdRfRaX0VfJJ4jnhVjoBFIsAee9A_&Key-Pair-Id=APKAJLTNE6QMUY6HB

Informe sobre incidentes de ciberseguridad:

Análisis del tráfico de red

Parte 1: Proporciona un resumen del problema encontrado en el registro de tráfico DNS e ICMP.
El protocolo UDP revela que el servidor DNS está caído o inaccesible. Como se desprende de los resultados del análisis de red, la respuesta de eco ICMP devolvió el mensaje de error "udp port 53 unreachable" (puerto udp 53 inaccesible). El puerto 53 se usa habitualmente para el tráfico del protocolo DNS. Es muy probable que el servidor DNS no esté respondiendo.

Parte 2: Explica tu análisis de los datos y proporciona una solución para implementar.
El incidente ocurrió hoy a la 1:23 p.m. Las/los clientes llamaron a la organización para notificar al equipo de TI que recibían el mensaje "puerto de destino inaccesible" cuando intentaban visitar el sitio web. Las/los profesionales de seguridad de la red de la organización están investigando el problema para que las/los clientes puedan acceder al sitio web nuevamente. En nuestra investigación del problema, realizamos pruebas de rastreo de paquetes utilizando tcpdump. En el archivo de registro resultante, encontramos que el puerto DNS 53 era inaccesible. El siguiente paso es identificar si el servidor DNS está caído o si el tráfico al puerto 53 está bloqueado por el cortafuegos. El servidor DNS podría estar caído debido a un ataque de denegación de servicio exitoso o una configuración incorrecta.

Material de apoyo:

- https://d3c33hcgiwev3.cloudfront.net/XF1UJiDRRgeMEZ-vXEV3Sg_07de10fc69724af0a748c139c8b9d9f1_Activity-Analyze-network-attacks_Cybersecurity-incident-

report.docx?Expires=1703721600&Signature=YEa~WcHriQvr7DXsyF8VYdARJfO9ZpjVW0N9vO294p69hVuMg6EwJc14tUiHGuBj3SzRRgZCtkeIfum1HkF6CHE07JeRwhMxvqKZ4oXaln-prYMjsi5-R3CeYpEWiLi6pFDKNRUiCl00RmTFSfH4xpaGrPIY9MWJMdhpQOoUlml_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A

- https://d3c33hcgiwev3.cloudfront.net/_plk--pBQUm3r7bw54Y-bA_5982de12131d4f3e9bb99e09522db4f1_Activity-Analyze-network-attacks_Wireshark-TCP_HTTP-log.xlsx?Expires=1703721600&Signature=hFmkKq22wO~TJCHnSbQWWYNfaChcYbhTE95kpQx99XqqoRlYkxlMhiCz6JETSH-982VNOJsKVEwAjPwzq39qLgoJq4T7hmfpCNXwl5qF6R4yw0VNkKVXQnTPmxL3H3KrEttphh50MCihnA7zlQ2UcGJ8S-HK0QcunQ9BAobLC~M_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A
- https://d3c33hcgiwev3.cloudfront.net/-KcB8dTMSLupwW-Y85Wzpg_319f94dbd6bb45e2a71e75eb836e45f1_Activity-Analyze-network-attacks_How-to-read-the-Wireshark-TCP_HTTP-log.docx?Expires=1703721600&Signature=VpumxsOKGKsgOU5gz1AasV03yh3nG0o1jooNikUfVxsJls13205gJZ6lnmlEreYTqpPBRUMGUwGjMWzrSRuMPGzlpQ6UsPfjUtdlXiaxAnxP589m78MHZh9me8cQWMDDaOkwUggsxnO9CJf2PBxz3PmcYxpyVC8YrqyKIThaTpc_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A

Actividad de ejemplo: Aplica técnicas de reforzamiento del SO

Sección 1: Identifica el protocolo de red involucrado en el incidente
El protocolo afectado en el incidente es el protocolo de transferencia de hipertexto (HTTP). La ejecución de tcpdump y el acceso al sitio web yummyrecipesforme.com para detectar el problema y capturar el protocolo y la actividad de tráfico en un archivo de registro de tráfico DNS y HTTP proporcionó la evidencia necesaria para llegar a esta conclusión. Se observa que el archivo malicioso se transporta a las computadoras de los/las usuarios/as utilizando el protocolo HTTP en la capa de aplicación.

Sección 2: Documenta el incidente
Varios/as clientes se pusieron en contacto con el/la propietario/a del sitio web indicando que, al visitar dicho sitio, se les pidió descargar y ejecutar un archivo que les pedía que actualizaran sus navegadores. Sus computadoras personales funcionan con lentitud desde entonces. El/la propietario/a del sitio web intentó iniciar sesión en el servidor web, pero advirtió que sus cuentas estaban bloqueadas. La/el analista de ciberseguridad utilizó un entorno controlado (sandbox) para probar el sitio web sin afectar la red de la empresa. Luego, ejecutó tcpdump para capturar los paquetes de tráfico de red y protocolo producidos al interactuar con el sitio web. Se le pidió que descargara un archivo que supuestamente actualizaría el navegador del usuario, este/a aceptó la descarga y lo ejecutó. El navegador luego redirigió al/a la analista a un sitio web falso (greatrecipesforme.com) que se veía idéntico al sitio original (yummyrecipesforme.com). El/la analista de ciberseguridad inspeccionó el registro de tcpdump y observó que, inicialmente, el navegador solicitó la dirección IP para el sitio web yummyrecipesforme.com. Una vez que se estableció la conexión con el sitio web a través del protocolo HTTP, el/la analista recordó descargar y ejecutar el archivo. Los registros mostraron un

cambio repentino en el tráfico de red cuando el navegador solicitó una nueva resolución IP para la URL greatrecipesforme.com. El tráfico de red fue redirigido a la nueva dirección IP para el sitio web greatrecipesforme.com. El/la profesional sénior de ciberseguridad analizó el código fuente de los sitios web y el archivo descargado. El/la analista descubrió que un/a atacante había manipulado el sitio web para agregar código que llevó a los/las usuarios/as a descargar un archivo malicioso disfrazado de actualización del navegador. Como el/la propietario/a del sitio web declaró que le habían bloqueado su cuenta de administrador, el equipo cree que la/el responsable utilizó un ataque de fuerza bruta para acceder a la cuenta y cambiar la contraseña del administrador. La ejecución del archivo malicioso comprometió las computadoras de los/las usuarios/as finales.

Sección 3: Recomienda una solución para los ataques de fuerza bruta
Una medida de seguridad que el equipo planea implementar para protegerse contra los ataques de fuerza bruta es la autenticación de dos factores (2FA). Este plan 2FA incluirá un requisito adicional para que los/las usuarios/as validen su identificación confirmando una contraseña única (OTP) enviada a su correo electrónico o teléfono. Una vez que el/la usuario/a confirme su identidad a través de sus credenciales de inicio de sesión y la OTP, obtendrá acceso al sistema. Cualquier agente de amenaza que intente un ataque de fuerza bruta probablemente no obtendrá acceso al sistema porque requiere autorización adicional.

Explicación del ejemplo: Informe del incidente de seguridad

Sección 1: Identifica del protocolo de red involucrado en el incidente
El protocolo afectado en el incidente es el protocolo de transferencia de hipertexto (HTTP). La ejecución de tcpdump y el acceso al sitio web yummyrecipesforme.com para detectar el problema y capturar el protocolo y la actividad de tráfico en un archivo de registro de tráfico DNS y HTTP proporcionó la evidencia necesaria para llegar a esta conclusión. Se observa que el archivo malicioso se transporta a las computadoras de los/las usuarios/as utilizando el protocolo HTTP en la capa de aplicación.

Sección 2: Documenta el incidente
Varios/as clientes se pusieron en contacto con el/la propietario/a del sitio web indicando que, al visitar dicho sitio, se les pidió descargar y ejecutar un archivo que les pedía que actualizaran sus navegadores. Sus computadoras personales funcionan con lentitud desde entonces. El/la propietario/a del sitio web intentó iniciar sesión en el servidor web, pero advirtió que sus cuentas estaban bloqueadas. La/el analista de ciberseguridad utilizó un entorno controlado (sandbox) para probar el sitio web sin afectar la red de la empresa. Luego, ejecutó tcpdump para capturar los paquetes de tráfico de red y protocolo producidos al interactuar con el sitio web. Se le pidió al/ a la analista que descargara un archivo que supuestamente actualizaría el navegador del usuario, este/a aceptó la descarga y lo ejecutó. El navegador luego redirigió al/a la analista a un sitio web falso (greatrecipesforme.com) que se veía idéntico al sitio original (yummyrecipesforme.com).

El/la analista de ciberseguridad inspeccionó el registro de tcpdump y observó que, inicialmente, el navegador solicitó la dirección IP para el sitio web yummyrecipesforme.com. Una vez que se estableció la conexión con el sitio web a través del protocolo HTTP, el/la analista recordó descargar y ejecutar el archivo. Los registros mostraron un cambio repentino en el tráfico de red cuando el navegador solicitó una nueva resolución IP para la URL greatrecipesforme.com. El tráfico de red fue redirigido a la nueva dirección IP para el sitio web greatrecipesforme.com.

El/la profesional sénior de ciberseguridad analizó el código fuente de los sitios web y el archivo descargado. El/la analista descubrió que un/a atacante había manipulado el sitio web para agregar código que llevó a los/las usuarios/as a descargar un archivo malicioso disfrazado de actualización del navegador. Como el/la propietario/a del sitio web declaró que le habían bloqueado su cuenta de administrador, el equipo cree que la/el responsable utilizó un ataque de fuerza bruta para acceder a la cuenta y cambiar la contraseña del administrador. La ejecución del archivo malicioso comprometió las computadoras de los/las usuarios/as finales.

Sección 3: Recomienda una solución para los ataques de fuerza bruta
Una medida de seguridad que el equipo planea implementar para protegerse contra los ataques de fuerza bruta es la autenticación de dos factores (2FA). Este plan 2FA incluirá un requisito adicional para que los/las usuarios/as validen su identificación confirmando una contraseña única (OTP) enviada a su correo electrónico o teléfono. Una vez que el/la usuario/a confirme su identidad a través de sus credenciales de inicio de sesión y la OTP, obtendrá acceso al sistema. Cualquier agente de amenaza que intente un ataque de fuerza bruta probablemente no obtendrá acceso al sistema porque requiere autorización adicional.

Material de apoyo:

- https://d3c33hcgiwev3.cloudfront.net/gmwPHX36SjaMnn-l1t4ZEg_096805058d0f42f9a23b043bbdf7fbf1_Activity-Apply-OS-hardening-techniques_Security-incident-report-template.docx?Expires=1703721600&Signature=kr23eNZvXTsZ8OKI-jVrV3Q9ZuSs8hkZAqE3FSF7TRnQEHCRYtYq8H8OzAOLwvx1WXq5du~OhIlsFcGvdvTC480fksbqkXU1~u6VnS0raZjkQ~FIgojCZ-0hzl0B6nPzo0J0JmBJYeOJgSuxWkne~MGsGtkstuV9DYyAIiipsvQ_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A
- https://d3c33hcgiwev3.cloudfront.net/YtPq1UL2SY6e-LB8Faf8uQ_988d4ffa4dde4936a5b61b41643a02f1_Activity-Apply-OS-hardening-techniques_DNS-HTTP-traffic-log.docx?Expires=1703721600&Signature=EUxh-La3WWLQ7RNWDO-KLUA27jPFg1ZBuKwVJmZHWi0Y-6XFgReiKOz3yVTTbgLl8DDRjNJ86DeomHxDKnoOKLteomMEiKll7Ro1Tp47Ad5PVSh8xn2fLTrkkrEhUBFmTEjZwNgYY0lti~Sho6wYvu1eEpJRWvURBsaUmctsYiA_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A
- https://d3c33hcgiwev3.cloudfront.net/tssao9SLSguBUCuqDPLX3Q_2509fca74ea642feb59398bfdc2e72f1_Activity-Apply-OS-hardening-techniques_How-to-read-the-DNS-HTTP-traffic-log.docx?Expires=1703721600&Signature=EcJk8YekH411pubsP0ptDi7DFNdO6-h5RBdo4tht1TDtpt-P1KTovnGU3a0Q0nY4BQlu5o4iSiieMMTloLyKgQkxh1f~UmXjyMVRBLPJwPHSzwkKaSf95aeZHAJzaNmtSQOlwDS086YgAE1LqfI3-IqbyLMN1Jjv5aVUXIJRYjs_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A

Análisis del informe del incidente

Resumen	Esta mañana, una pasante informó al departamento de TI que no pudo iniciar sesión en su cuenta de red interna. Los registros de acceso indican que su cuenta ha estado accediendo activamente a los registros de la base de datos de clientes, a pesar de estar bloqueada. La pasante indicó que recibió un correo electrónico esta mañana pidiéndole que se dirija a un sitio web externo e inicie sesión con sus credenciales de red interna para recuperar un mensaje. Creemos que este es el método utilizado por un agente de amenaza para obtener acceso a nuestra red y base de datos de clientes. Otros/as empleados/as han advertido que faltan varios registros de clientes o que contienen datos incorrectos. Parece que no solo se expusieron los datos de las/los clientes a un agente de amenaza, sino que también se eliminaron o manipularon algunos datos.
Identificar	El equipo de gestión de incidentes auditó los sistemas, dispositivos y políticas de acceso involucrados en el ataque para identificar las brechas de seguridad o fugas de datos. El equipo descubrió que el inicio de sesión y la contraseña de una pasante fueron obtenidos por un agente de amenaza y utilizados para acceder a los datos de nuestra base de datos de clientes. Tras la revisión inicial,

	parece que algunos datos de clientes se eliminaron de la base de datos.
Proteger	El equipo ha implementado nuevas políticas de autenticación para prevenir futuros ataques: autenticación de múltiples factores (MFA), límite de solo tres intentos para el inicio de sesión y capacitación para todos/as los/las empleados acerca de cómo proteger las credenciales de inicio de sesión. Además, implementaremos una nueva configuración de firewall para protección e invertiremos en un sistema de prevención de intrusiones (IPS).
Detectar	Para detectar nuevos ataques de acceso no autorizados en el futuro, el equipo utilizará una herramienta de registro por firewall y un sistema de detección de intrusiones (IDS) para monitorear todo el tráfico entrante de Internet.
Responder	El equipo deshabilitó la cuenta de red de la pasante. Brindamos capacitación a pasantes y empleados/as sobre cómo proteger las credenciales de inicio de sesión en el futuro. Informamos a la alta dirección de este evento y se pondrán en contacto con nuestros/as clientes por correo para informarles sobre la filtración de datos. La administración también deberá informar a las fuerzas del orden y otras organizaciones según lo exijan las leyes locales.

Recuperar	El equipo recuperará los datos eliminados restaurando la base de datos de la copia de seguridad completa realizada la noche anterior. Hemos informado al personal de que cualquier información de clientes que se haya ingresado o cambiado esta mañana no se registraría en la copia de seguridad. Por lo tanto, deberán volver a ingresar esa información en la base de datos una vez que esta se haya restaurado desde la copia de seguridad.

Reflexiones/Notas:

Material de apoyo:

- https://d3c33hcgiwev3.cloudfront.net/ywmyo7zYSteaM60lHjKuWA_394679b5b27a47d19ce03d9d11fda5f1_Portfolio-Activity-Use-the-NIST-Cybersecurity-Framework-to-respond-to-a-security-incident_Incident-report-analysis.docx?Expires=1703721600&Signature=SgPA~vpJGFaMSEcwkNjt98XwsPj4AYMFXnDZVJ9ZjgKGVB~LhBejRpekRpeDBZFiT5k2usk9ljQqbw2F1BZHzwGEkUkdc6zAE3T2sdEWXm~ntX8bq3l97TR8~lX9uMIe7~~A0VmSjAL9plF6KMS3ykci3HPDjVRd03JqxpIglT8_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A

- https://d3c33hcgiwev3.cloudfront.net/ZEMJ6rETQrqMcf0GXWMF1Q_b2c964a148034a47ab91bb969d9b34f1_Portfolio-Activity-Use-the-NIST-Cybersecurity-Framework-to-respond-to-a-security-incident__Applying-the-NIST-CSF-

.docx?Expires=1703721600&Signature=LYEq2Odw8CwSHDgho8h0TnbNY1RwlH4DfdCHWA5cXVS9IxlXn42LsF~NaiPyiY8heq~Gg3pYuOxCKnayEFLdCHr1yF1vwicfkeaB8M42OLum0-C88FE3QViVfOfVdB0sK3~IJkPhVAYbZDHcFDu-L7C80W6KxF-PwXBCep6vemc_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A

Permisos de archivo en Linux

Descripción del proyecto

El equipo de investigación de mi organización necesita actualizar los permisos de archivo para ciertos archivos y directorios dentro del directorio projects. Actualmente, los permisos no reflejan el nivel de autorización que debe otorgarse. Revisar y actualizar estos permisos ayudará a mantener el sistema seguro. Para completar esta tarea, realicé las siguientes acciones:

Comprobar detalles del archivo y del directorio

El siguiente código muestra cómo utilicé los comandos de Linux para determinar los permisos que se establecieron para un directorio específico en el sistema de archivos.

```
researcher2@5d738f0f927b:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Dec  2 15:27 .
drwxr-xr-x 3 researcher2 research_team 4096 Dec  2 15:27 ..
-rw--w---- 1 researcher2 research_team   46 Dec  2 15:27 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Dec  2 15:27 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Dec  2 15:27 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Dec  2 15:27 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 15:27 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 15:27 project_t.txt
researcher2@5d738f0f927b:~/projects$
```

La primera línea de la captura de pantalla muestra el comando que ingresé, y las otras líneas muestran la salida. El código enumera todos los contenidos del directorio `projects`. Utilicé el comando `ls` con la opción `-la` para mostrar una lista detallada de los contenidos de los archivos que también arrojó archivos ocultos. La salida de mi comando indica que hay un directorio llamado `drafts`, un archivo oculto llamado `.project_x.txt` y otros cinco archivos de proyecto. La cadena de 10 caracteres en la primera columna representa los permisos establecidos en cada archivo o directorio.

Describir la cadena de permisos

La cadena de 10 caracteres se puede desglosar para determinar quién tiene autorización para acceder al archivo y qué permisos específicos tiene. Los caracteres y lo que representan son los siguientes:

- **1º carácter**: es una `d` o un guion (`-`) e indica el tipo de archivo. Si es una `d`, se trata de un directorio. Si es un guion (`-`), se trata de un archivo normal.
- **2.º al 4.º carácter**: indican los permisos de lectura (`r`), escritura (`w`) y ejecución (`x`) para el usuario. Cuando uno de estos caracteres es un guion (`-`) en lugar de una letra, indica que no se le ha concedido este permiso al usuario.
- **5.º al 7.º carácter:** indican los permisos de lectura (`r`), escritura (`w`) y ejecución (`x`) para el grupo. Cuando uno de estos caracteres es un guion (`-`) en lugar de una letra, indica que este permiso no está concedido al grupo.

- **8.º al 10.º carácter:** indican los permisos de lectura (r), escritura (w) y ejecución (x) para otros usuarios. Este tipo de propietario está compuesto por todos los demás usuarios del sistema, aparte del usuario y el grupo. Cuando uno de estos caracteres es un guion (-) en lugar de una letra, eso indica que este permiso no está concedido a otros usuarios.

Supongamos que los permisos de archivo para project_t.txt son -rw-rw-r--. Dado que el primer carácter es un guion (-), esto indica que project_t.txt es un archivo, no un directorio. Tanto el segundo como el quinto y el octavo carácter son r. Esto indica que el usuario, el grupo y otros usuarios tienen permisos de lectura. El tercer carácter y el sexto son w, lo que indica que solo el usuario y el grupo tienen permisos de escritura. Nadie tiene permisos de ejecución para project_t.txt.

Cambiar permisos de archivo

La organización determinó que otros usuarios no deberían tener acceso de escritura a ninguno de sus archivos. Para cumplir con esto, me basé en los permisos de archivo que había obtenido como resultado. Determiné que debía eliminar el permiso de escritura de otros usuarios para project_k.txt.

El siguiente código muestra cómo usé los comandos de Linux para hacer esto:

```
researcher2@5d738f0f927b:~/projects$ chmod o-w project_k.txt
researcher2@5d738f0f927b:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Dec  2 15:27 .
drwxr-xr-x 3 researcher2 research_team 4096 Dec  2 15:27 ..
-rw--w---- 1 researcher2 research_team   46 Dec  2 15:27 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Dec  2 15:27 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 15:27 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Dec  2 15:27 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 15:27 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 15:27 project_t.txt
researcher2@5d738f0f927b:~/projects$
```

Las dos primeras líneas de la captura de pantalla muestran los comandos que ingresé, mientras que las demás líneas muestran la salida del segundo comando. El comando chmod cambia los permisos en archivos y directorios. El primer argumento indica qué permisos se deben cambiar y el segundo argumento especifica el archivo o directorio. En este ejemplo, eliminé los permisos de escritura de otros para el archivo project_k.txt. Luego, utilicé ls-la para revisar las actualizaciones que había hecho.

Cambiar permisos de archivo en un archivo oculto

Recientemente, el equipo de investigación de mi organización archivó `project_x.txt`. No quieren que nadie tenga acceso de escritura a este proyecto, pero el usuario y el grupo deben tener acceso de lectura.

El siguiente código muestra cómo utilicé los comandos de Linux para cambiar los permisos:

```
researcher2@3213bbc1d047:~/projects$ chmod u-w,g-w,g+r .project_x.txt
researcher2@3213bbc1d047:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Dec 20 15:36 .
drwxr-xr-x 3 researcher2 research_team 4096 Dec 20 15:36 ..
-r--r----- 1 researcher2 research_team   46 Dec 20 15:36 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Dec 20 15:36 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Dec 20 15:36 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Dec 20 15:36 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec 20 15:36 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec 20 15:36 project_t.txt
researcher2@3213bbc1d047:~/projects$
```

Las dos primeras líneas de la captura de pantalla muestran los comandos que ingresé, y las otras líneas muestran la salida del segundo comando. Sé que `.project_x.txt` es un archivo oculto porque comienza con un punto (`.`). En este ejemplo, eliminé los permisos de escritura del usuario y el grupo, y agregué permisos de lectura para el grupo. Eliminé los permisos de escritura del usuario con `u-w`. Luego, eliminé los permisos de escritura del grupo con `g-w` y agregué permisos de lectura para el grupo con `g+r`.

Cambiar permisos de directorio

Mi organización solo quiere que el usuario `researcher2` tenga acceso al directorio `drafts` y sus contenidos. Esto significa que nadie más que `researcher2` debe tener permisos de ejecución.

El siguiente código muestra cómo utilicé los comandos de Linux para cambiar los permisos:

```
researcher2@5d738f0f927b:~/projects$ chmod g-x drafts
researcher2@5d738f0f927b:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Dec  2 15:27 .
drwxr-xr-x 3 researcher2 research_team 4096 Dec  2 15:27 ..
-r--r----- 1 researcher2 research_team   46 Dec  2 15:27 .project_x.txt
drwx------ 2 researcher2 research_team 4096 Dec  2 15:27 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 15:27 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Dec  2 15:27 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 15:27 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 15:27 project_t.txt
researcher2@5d738f0f927b:~/projects$
```

Las dos primeras líneas de la captura de pantalla muestran los comandos que ingresé. Las otras líneas muestran la salida del segundo comando. Antes había determinado que el grupo tenía permisos de ejecución, así que utilicé el comando `chmod` para eliminar estos permisos. El usuario `researcher2` ya tenía permisos de ejecución, por lo que no era necesario agregarlos.

Resumen

Cambié varios permisos para que coincidieran con el nivel de autorización que mi organización quería para archivos y directorios en el directorio `projects`. El primer paso en esto fue usar `ls-la` para verificar los permisos para el directorio. En esta información basé mis decisiones para los siguientes pasos. Luego, usé el comando `chmod` varias veces para cambiar los permisos en archivos y directorios.

Material de apoyo:

- https://d3c33hcgiwev3.cloudfront.net/ItMR0BSVSX26Nqp0vLg4Zw_4c71dadcb7a9437f8eb880acc3c575f1_Portfolio-Activity-Use-Linux-commands-to-manage-file-permissionsFile-permissions-in-Linux.docx?Expires=1703721600&Signature=bqyqBgu9s2ot3v7mMj0nJitglif5GIV3yZDdELXNUh3ahXIQRxEha~q~iZq1E5PWI2G1nSCZmueEiP4Qr2hQThq0zPVyz7irPEBOiIlU9TRLwgcrDnTsxJVKpZ~Q0ipRprsSF53zTRbQ50o6am5GmjeOUu6riX3C3BnT-uNQ~u0_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A
- https://d3c33hcgiwev3.cloudfront.net/G0jYC_3qTO61PefqRIMPZA_4215da130b6b437593a4beb7ea8799f1_Portfolio-

Activity-Use-Linux-commands-to-manage-file-permissions_Instructions-for-including-Linux-commands.docx?Expires=1703721600&Signature=H-nFEbeS7gXqRWwpdh9bxLYIsZ-JFlQ-DQFNHvtLQm-3adeqPtAw9NDVY4rS3rc5aWgXxU9ffIXkmfrTDl8FV~BzuwnU2PvkzsW7JA3sNv8wgYHcE~qtZBp6TitNmXblB6UdV~O~67dCSi9TaFSSy41ef1YVas6JLFohVJvMagI_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A

- https://d3c33hcgiwev3.cloudfront.net/sugq7qAkSUG1wR4EjBRGcQ_67cdbd042f944ee3836d49b98c323ef1_Portfolio-Activity-Use-Linux-commands-to-manage-file-permissions_Current-file-permissions.docx?Expires=1703721600&Signature=dPB1g3nTgqt40hLPfoFKkJCcHXwTXfsPj4CLO5PP65QKRgwZ-DiI2acm~mQuy6WN5A0inDqorUDToK8nYpSFLm6O2dDd3EOjqnW-jxRZ0KKnj8MIzGuSksslUMoapbMuGcHCEJdtaArPIn2ia9MZX9V7iygAgH-3ZXkAPKlaKJc_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A

Aplicación de filtros a consultas SQL

Descripción del proyecto

Mi organización está trabajando para que su sistema sea más seguro. Mi labor consiste en garantizar que el sistema esté protegido, investigar todos los posibles problemas de seguridad y actualizar las computadoras de los/las empleados/as según sea necesario. Los pasos siguientes ofrecen ejemplos de cómo usé SQL con filtros para realizar tareas de seguridad.

Recupera intentos de inicio de sesión fallidos después del horario laboral

Se produjo un posible incidente de seguridad después del horario laboral (después de las 18:00). Fue necesario investigar todos los intentos de inicio de sesión fallidos después del horario laboral.

El código siguiente demuestra cómo creé una consulta SQL para filtrar por los intentos de inicio de sesión fallidos que tuvieron lugar después del horario laboral.

```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_time > '18:00' AND success = FALSE;
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12  |       0 |
|       18 | pwashing | 2022-05-11 | 19:28:50   | US      | 192.168.66.142  |       0 |
|       20 | tshah    | 2022-05-12 | 18:56:36   | MEXICO  | 192.168.109.50  |       0 |
```

La primera parte de la captura de pantalla es mi consulta, y la segunda es un fragmento del resultado. Esta consulta filtra por inicios de sesión fallidos que se produjeron después de las 18:00. En primer lugar, comencé por seleccionar todos los datos de la tabla log_in_attempts (intentos de inicio de sesión). A continuación, usé una cláusula WHERE con un operador AND para filtrar mis resultados, de manera de obtener solo los intentos de inicio de sesión fallidos que tuvieron lugar después de las 18:00. La primera condición es login_time > '18:00', que filtra por los intentos de inicio de sesión que se produjeron después de las 18:00. La segunda condición es success = FALSE, que filtra por los intentos de inicio de sesión fallidos.

Recupera intentos de inicio de sesión en fechas específicas

El 09-05-2022 se produjo un evento sospechoso. Es necesario investigar toda la actividad registrada el 09-05-2022 o el día anterior.

El código a continuación demuestra cómo creé una consulta SQL para filtrar por intentos de inicio de sesión que tuvieron lugar en fechas específicas.

```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_date = '2022-05-09' OR login_date = '2022-05-08';
+----------+----------+------------+------------+---------+----------------+---------+
| event_id | username | login_date | login_time | country | ip_address     | success |
+----------+----------+------------+------------+---------+----------------+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.140 |       0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |       0 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.71  |       0 |
```

La primera parte de la captura de pantalla es mi consulta, y la segunda es un fragmento del resultado. Esa consulta devuelve todos los intentos de inicio de sesión que tuvieron lugar el 09-05-2022 o el 08-05-2022. En primer lugar, comencé por seleccionar todos los datos de la tabla log_in_attempts (intentos de inicio de sesión). A continuación, usé una cláusula WHERE con un operador OR para filtrar mis resultados, con el fin de obtener solo los intentos de inicio de sesión que tuvieron lugar el 09-05-2022 o el 08-05-2022. La primera condición es login_date = '2022-05-09', que filtra por los inicios de sesión ocurridos el 09-05-2022. La segunda condición es login_date = '2022-05-08', que filtra por los inicios de sesión ocurridos el 08-05-2022.

Recupera intentos de inicio de sesión fuera de México

Luego de haber investigado los datos de intentos de inicio de sesión en la organización, sospecho que existe un problema con los intentos de inicio de sesión realizados fuera de México. Estos intentos de inicio de sesión deben ser investigados..

El código siguiente demuestra cómo creé una consulta SQL para filtrar por intentos de inicio de sesión ocurridos fuera de México.

```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE NOT country LIKE 'MEX%';
+----------+----------+------------+------------+---------+----------------+---------+
| event_id | username | login_date | login_time | country | ip_address     | success |
+----------+----------+------------+------------+---------+----------------+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.140 |       0 |
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12  |       0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |       0 |
```

La primera parte de la captura de pantalla es mi consulta, y la segunda es un fragmento del resultado. Esta consulta devuelve todos los intentos de inicio de sesión que tuvieron lugar fuera de México. En primer lugar, comencé por seleccionar todos los datos de la tabla log_in_attempts (intentos de inicio de sesión). A continuación, usé una cláusula WHERE con NOT para filtrar por países

que no son México. Usé LIKE con MEX% como el patrón de coincidencia, porque el conjunto de datos (dataset) representa a México como MEX y MEXICO. El signo de porcentaje (%) representa cualquier número de caracteres no especificados cuando se usan con LIKE.

Recupera empleados/as en Marketing

Mi equipo quiere actualizar las computadoras para ciertos/as empleados/as del departamento de Marketing. Para hacerlo, necesito obtener información sobre los equipos de los/las empleados/as que debo actualizar.

El código siguiente demuestra cómo creé una consulta SQL para filtrar por equipo de empleados/as en el departamento de Marketing en el edificio Este (East).

```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department = 'Marketing' AND office LIKE 'East%';
+-------------+-------------+----------+------------+----------+
| employee_id | device_id   | username | department | office   |
+-------------+-------------+----------+------------+----------+
|        1000 | a320b137c219 | elarson  | Marketing  | East-170 |
|        1052 | a192b174c940 | jdarosa  | Marketing  | East-195 |
|        1075 | x573y883z772 | fbautist | Marketing  | East-267 |
```

La primera parte de la captura de pantalla es mi consulta, y la segunda es un fragmento del resultado. Esta consulta devuelve a todos/as los/las empleados/as del departamento de Marketing en el edificio Este. En primer lugar, comencé por seleccionar todos los datos de la tabla employees (empleados/as). A continuación usé una cláusula WHERE con AND para filtrar por empleados/as que trabajan en el departamento de Marketing en el edificio Este (East). Usé LIKE con East% como el patrón de coincidencia porque los datos en la columna office (oficina) representan el edificio Este (East) con el número específico de la oficina. La primera condición es el fragmento department = 'Marketing', que filtra por empleados en el departamento de Marketing. La segunda condición es el fragmento office LIKE 'East%', que filtra por empleados en el edificio Este (East).

Recupera empleados/as en Finanzas o Ventas

También es necesario actualizar los equipos de los/las empleados/as de los departamentos de Finanzas y Ventas. Como se necesita una actualización de seguridad distinta, solo debo obtener información de empleados/as de esos dos departamentos.

El código siguiente demuestra cómo creé una consulta SQL para filtrar por equipos de empleados de los departamentos de Finanzas o Ventas.

```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department = 'Finance' OR department = 'Sales';
+-------------+-------------+----------+------------+-------------+
| employee_id | device_id   | username | department | office      |
+-------------+-------------+----------+------------+-------------+
|        1003 | d394e816f943 | sgilmore | Finance    | South-153   |
|        1007 | h174i497j413 | wjaffrey | Finance    | North-406   |
|        1008 | i858j583k571 | abernard | Finance    | South-170   |
```

La primera parte de la captura de pantalla es mi consulta, y la segunda es un fragmento del resultado. Esta consulta devuelve todos/as los/as empleados/as de los departamentos de Finanzas y Ventas. En primer lugar, comencé por seleccionar todos los datos de la tabla `employees` (empleados/as). A continuación, usé una cláusula `WHERE` con `OR` para filtrar por empleados/as que trabajan en los departamentos de Finanzas y Ventas. Usé el operador `OR` en lugar de `AND` porque quería obtener todos/as los/las empleados/as de ambos departamentos. La primera condición es `department = 'Finance'`, que filtra por empleados/as del departamento de Finanzas. La segunda condición es `department = 'Sales'`, que filtra por empleados/as del departamento de Ventas.

Recupera a todos/as los/las empleados/as que no trabajan en TI

Mi equipo necesita realizar otra actualización de seguridad para empleados/as que no trabajan en el departamento de Tecnología de la Información. Para realizar la actualización, primero debo obtener información sobre estos/as empleados/as.

A continuación, demuestro cómo creé una consulta SQL para filtrar por equipos de empleados/as que no trabajan en el departamento de Tecnología de la Información.

```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE NOT department = 'Information Technology';
+-------------+-------------+----------+-----------------+-------------+
| employee_id | device_id   | username | department      | office      |
+-------------+-------------+----------+-----------------+-------------+
|        1000 | a320b137c219 | elarson  | Marketing       | East-170    |
|        1001 | b239c825d303 | bmoreno  | Marketing       | Central-276 |
|        1002 | c116d593e558 | tshah    | Human Resources | North-434   |
```

La primera parte de la captura de pantalla es mi consulta, y la segunda es un fragmento del resultado. La consulta devuelve todos/as los/las empleados/as que no trabajan en el departamento de Tecnología de la Información. En primer lugar, comencé por seleccionar todos los datos de la tabla employees (empleados/as). A continuación, usé una cláusula WHERE con NOT para filtrar por empleados/as que no trabajan en este departamento.

Resumen

Apliqué filtros a consultas SQL para obtener información específica sobre los intentos de inicio de sesión y los equipos de los/las empleados/as. Utilicé dos tablas distintas, log_in_attempts (intentos de inicio de sesión) y employees (empleados/as). Usé los operadores AND, OR y NOT para filtrar por la información específica que necesitaba para cada tarea. También utilicé LIKE y el comodín de signo de porcentaje (%) para filtrar por patrones.

Material de apoyo:

- https://d3c33hcgiwev3.cloudfront.net/qr7ka9-JQvKRmZ0wretPPA_c3db71138047404b8d9b6604c7039ff1_Portfolio-Activity-Apply-filters-to-SQL-queries_Instructions-for-including-SQL-queries.docx?Expires=1703721600&Signature=Zvkqmb3i-KgPp6J1~Pce8cMLPLE9JKBex0lagTMr-dOoHiuzXBBgPF1TskiogRMiGMye5gvtMf04MoxkffAvVuzJvOr

unFAGUYQR8ZBICG5KuvSGJiombbps1UtyhpnyOiirDIMQzwbERFD9YyJevPxBSnm8ifyravdMs8G2GvE_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A

- https://d3c33hcgiwev3.cloudfront.net/jS8rHT__SXiJvSOX8op1MA_d4fd5d3cc3b24d73897fb2eda833f8f1_Portfolio-Activity-Apply-filters-to-SQL-queries_Table-formats.docx?Expires=1703721600&Signature=PU7A0McZv~8WPW8EZKtAORoNa-5YgVIsX4KxDBxjQDTOz8GL6a69qGzFVWp0PVPg0j~E3vnWkitxC21W4DTxF9ahN2b~ZfxdQL26b4oRGcnjCjGz3D5vdC1QoAMQBxYW3pRQEzrA2PTWnpoE-o9YbQ-QQ11Od2hzVwo4RLyLywg_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A
- https://docs.google.com/document/d/1QLYj8sdBCYtcZv3ZF1RlcPft8Uh-fscWSZsiT_6QVy0/template/preview

Inventario de activos

Activo	Acceso a la red	Dueño	Ubicación	Notas	Sensibilidad
Router	*Continuo*	*Proveedor de servicios de Internet (ISP)*	*Local*	*Tiene una conexión de 2.4 GHz y 5 GHz.*	*Confidencial*

				Todos los dispositivos en la red doméstica se conectan a la frecuencia de 5 GHz.	
Equipo de escritorio	*Ocasional*	*Propietario*	*Local*	*Contiene información privada, como fotos.*	*Restringida*
Smartphone invitado	*Ocasional*	*Amigo*	*Local y externa*	*Se conecta a mi red doméstica.*	*Solo interna*
Disco duro externo	Ocasional	Propietario	Local	Contiene música y películas.	Confidencial
Reproductor multimedia	Continuo	Propietario	Local	La información de la tarjeta de pago se almacena para el alquiler de películas.	Solo interna
Consola de juegos portátil	Ocasional	Amigo	Local y externa	Tiene una cámara y un micrófono.	Solo interna

Categorías	Designación de acceso
Ninguno	Ninguna relación
Pública	Cualquiera
Confidencial	Limitado a usuarios específicos

Restringida	Es necesario saber

Material de apoyo:

- https://d3c33hcgiwev3.cloudfront.net/mbXlYr-NS7GDk8CKD2J2QA_967d9776575a48e0875af856b836a0f1_Activity-Classify-the-assets-connected-to-a-home-network_Home-asset-inventory.xlsx?Expires=1703721600&Signature=I4KPDYoNy-sAQsv8YuReaqYzwpXrk1UgGao39SAq1469TvHBVTsdP9M9pfcAYD-4NEZi4z~GIC257oVKjyVx6V9dtgelCwLMdsaYrtEaOZN5XJlJNP22Re-VsG8CdYYB3gPBDWhosaAlCX~3l3kONpib3HpLCe19X5oO0ampesM_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A

Hoja de trabajo de control de acceso

	Nota(s)	Asunto(s)	Recomendación (es)
Autorización / autenticación	• *El evento ocurrió el 10/03/23.* • *El usuario es legal / administrador.* • *La dirección IP del equipo utilizado para iniciar sesión es 152.207.255.255.*	• *Robert Taylor Jr. no es administrador.* • *Su contrato finalizó en 2019, pero su cuenta accedió a los sistemas de nómina en 2023.*	• *Las cuentas de usuario deben expirar después de 30 días.* • *Los colaboradores externos deben tener acceso limitado a los recursos de la empresa.* • *Habilitar la autenticación de múltiples factores.*

Material de apoyo:

- https://d3c33hcgiwev3.cloudfront.net/KzwTlo5zSD-I9_FYoQO8Dw_07246ddf3a754e5182812985ac6037f1_Activity-Improve-authentication-authorization-and-business_Activity-Template_-Access-control-worksheet.docx?Expires=1703721600&Signature=ftdc1Dy8c9cWMAFTKbBGAWIsk0hqMGvhvitdFEBNvNGJOmpS39mHbtT5WnhFD01FLsuALqg2PQY0RCjlrVFErISCevzZ73NH5GxxecJYH5taOeqaW9r8rrx1Hwqnp-u2o6pJcz8m8uaEsITMmEQBRlysSK0rcb9pWPMGuFTw3Ys_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A
- https://d3c33hcgiwev3.cloudfront.net/OVA-3571SAyvmgO_QNPbZA_ad7d8d663ec54a88a491099e6ed375f1_Activity-Improve-authentication-authorization-and-accounting-for-a-small-business_Accounting-exercise.xlsx?Expires=1703721600&Signature=TJ3VXimixaWS-

IJIB0IE9uTDTWKn1j9VoLdeEPb9qLWFO-cMKBpUAeCxey6SE7-4cBq4nuwpOgunGyt5ZaheuEiYI5v4G8HqSCw9NRFFnmlI5IYN~8Vq~89Gd83vrU3t54XaFIS-kh7okC4hE15x1667G-GZPzL3uAnc6gfWOlw_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A

Ejercicio sobre USB abandonado en estacionamiento

Contenido	*Algunos documentos parecen contener información personal que Jorge no querría que se hiciera pública. Los archivos de trabajo incluyen la PII de otras personas. También contienen información sobre las operaciones del hospital.*
Mentalidad de atacante	*Las planillas horarias pueden proporcionar información de un atacante sobre otras personas con las que Jorge trabaja. Se podría utilizar la información laboral o personal para engañar a Jorge. Por ejemplo, se puede crear un correo electrónico malicioso para que parezca que proviene de un compañero de trabajo o pariente.*
Análisis de riesgos	*Cómo promover la conciencia de los empleados sobre este tipo de ataques y qué hacer cuando una unidad USB sospechosa es un control gerencial que puede reducir el riesgo de un incidente negativo. La configuración de análisis antivirus de rutina es un control operativo que se puede implementar. Otra línea de defensa podría ser un control técnico, como deshabilitar la reproducción automática en las PC de la empresa que evitará que una computadora ejecute automáticamente un código malicioso cuando se conecta una unidad USB.*

Material de apoyo:

- https://d3c33hcgiwev3.cloudfront.net/X63QaePSSYyg1iPwKBILNg_3e97c11bbb024d9083e5ed7b63e6f5f1_Activity-Identify-the-attack-vectors-of-a-USB-drive_Parking-lot-USB-exercise.docx?Expires=1703721600&Signature=J6WSFoaaezMK6KFS1jh1Hk4w4NQ8CY5O2Yx39pW93wHTbAJf1NdFKTX2HRaGDd06SZkT0NwDptfbStHMRLJdSYxDdK55zNt~4OfEktlKoMTRNUxfqlLQm7Py1jz0mtEJf0PD5LpsTi6wtrKcdkPgktHpZMviElANJPLTvCxYXc4_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A

Diario de gestión de incidentes

Fecha: 23 de noviembre de	**Entrada:** N.º 1

2023	
Descripción	Documentar un incidente de ciberseguridad Este incidente ocurrió en las dos fases: 1. **Detección y análisis**: El escenario describe cómo la organización detectó por primera vez el incidente de ransomware. Para la etapa de análisis, la empresa se puso en contacto con varias organizaciones para obtener asistencia técnica. 2. **Contención, erradicación y recuperación**: El escenario detalla algunos pasos que implementó la organización para contener el incidente. Por ejemplo, apagó los sistemas informáticos. Sin embargo, como no podían erradicar y recuperarse del incidente por su cuenta, contactaron a varias otras organizaciones para obtener ayuda.
Herramienta(s) utilizada(s)	Ninguna
Las 5 W	● **Quién (who)**: Un grupo organizado de hackers poco éticos. ● **Qué (what)**: Un incidente de seguridad de ransomware. ● **Dónde (where)**: En una empresa de atención médica. ● **Cuándo (when)**: Martes 9:00 a.m. ● **Por qué (why)**: El incidente ocurrió porque hackers poco éticos pudieron acceder a los sistemas de la compañía mediante un ataque de phishing. Acto seguido, los atacantes lanzaron su ransomware en los sistemas de la compañía y cifraron archivos críticos. Su motivación parecía ser financiera porque la nota de rescate exigía una gran suma de dinero a cambio de la clave para descifrar los archivos.
Notas complementarias	1. ¿De qué manera la compañía de atención médica podría evitar que vuelva a ocurrir un incidente como este? 2. ¿La empresa debería pagar el rescate para recuperar la clave de descifrado?

Fecha: 25 de noviembre de 2023	**Entrada:** N.º 2
Descripción	Análisis de un archivo de captura de paquetes
Herramienta(s) utilizada(s)	Para esta actividad, utilicé Wireshark para analizar un archivo de captura de paquetes. Wireshark es un analizador de protocolos de red que utiliza una interfaz gráfica de usuario. El valor de Wireshark en ciberseguridad es que permite a los analistas capturar y analizar el tráfico de red. Esto puede ayudar a detectar e investigar actividades maliciosas.
Las 5 W	● **Quién (who)**: N/D ● **Qué (what)**: N/D ● **Dónde (where)**: N/D ● **Cuándo (when)**: N/D ● **Por qué (why)**: N/D
Notas complementarias	Antes nunca había usado Wireshark, así que me interesaba mucho comenzar este ejercicio y analizar un archivo de captura de paquetes. A primera vista, la interfaz era muy abrumadora. Ahora entiendo por qué es una herramienta tan poderosa para comprender el tráfico de red.

Fecha: 25 de noviembre de 2023	**Entrada:** N.º 3
Descripción	Capturar mi primer paquete
Herramienta(s) utilizada(s)	Para esta actividad, utilicé tcpdump para capturar y analizar el tráfico de red. Tcpdump es un analizador de protocolos de red al que se accede mediante la interfaz de línea de comandos. Al igual que Wireshark, el valor de tcpdump en ciberseguridad es que permite a los analistas capturar, filtrar y analizar el tráfico de red.

Las 5 W	● **Quién (who)**: N/D ● **Qué (what)**: N/D ● **Dónde (where)**: N/D ● **Cuándo (when)**: N/D ● **Por qué (why)**: N/D
Notas complementarias	Aún no domino el uso de la interfaz de línea de comandos, por lo que usarla para capturar y filtrar el tráfico de red me supuso un desafío. Me atasqué algunas veces porque usé los comandos equivocados. Pero después de seguir cuidadosamente las instrucciones y rehacer algunos pasos, pude superar esta actividad y capturar el tráfico de la red.

Fecha: 27 de noviembre de 2023	**Entrada:** N.º 4
Descripción	Investigar un hash de archivo sospechoso
Herramienta(s) utilizada(s)	Para esta actividad, utilicé VirusTotal, que es una herramienta de investigación que analiza archivos y URL en busca de contenido malicioso, como virus, gusanos, troyanos y más. Es una herramienta muy útil si lo que necesitas es verificar rápidamente si otros integrantes de la comunidad de ciberseguridad denunciaron como malicioso un indicador de compromiso (como un sitio web o archivo). Para esta actividad, utilicé VirusTotal con el fin de analizar un hash de archivo que se reportó como malicioso. Este incidente ocurrió en la fase de **detección y análisis**. Tuve que asumir el rol de un analista de seguridad en un SOC que investiga un hash de archivo sospechoso. Después de que los sistemas de seguridad detectaron el archivo sospechoso, tuve que realizar un análisis y una investigación más profundos para determinar si la alerta era una amenaza real.

Las 5 W	● **Quién (who)**: Un agente de amenaza desconocido. ● **Qué (what)**: Un correo electrónico enviado a un empleado contenía un archivo adjunto malicioso con el hash de archivo SHA-256 de 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b. ● **Dónde (where)**: La computadora de un empleado de una compañía de servicios financieros. ● **Cuándo (where)**: A la 1:20 p.m., se envió una alerta al SOC de la organización después de que el sistema de detección de intrusiones detectara el archivo. ● **Por qué (why)**: Un empleado pudo descargar y ejecutar un archivo adjunto malicioso que recibió por correo electrónico.
Notas complementarias	¿Cómo se puede prevenir este incidente en el futuro? ¿Deberíamos considerar mejorar la capacitación en concientización de seguridad para que los empleados tengan cuidado con dónde hacen clic?

Reflexiones/Notas:

1. **¿Hubo alguna actividad específica que te haya resultado desafiante? ¿Por qué sí o por qué no?**

La actividad con tcpdump me resultó verdaderamente desafiante. Aún no domino el uso de la línea de comandos, y aprender la sintaxis de una herramienta como tcpdump fue un gran proceso de aprendizaje. Al principio, me resultó muy frustrante porque no lograba el resultado correcto. Repetí la actividad y me di cuenta de dónde me había equivocado. Aprendí que tengo que leer las instrucciones con atención e ir avanzando en el proceso paso a paso.

2. **Después de completar este curso, ¿entiendes mejor el proceso de detectar y dar respuesta a incidentes?**

Sí, definitivamente, después de completar el curso comprendo mejor la detección y respuesta a incidentes. Al comenzar el curso, tenía un conocimiento básico de lo que implicaba el proceso de detección y respuesta, pero no llegaba a comprender toda su complejidad. A medida que fui avanzando, aprendí sobre el ciclo de vida de un

incidente y de la importancia de los planes, los procesos y las personas, así como las herramientas utilizadas. En general, siento que ahora lo entiendo mejor y que cuento con más conocimientos para detectar incidentes y dar respuesta a ellos.

3. **¿Hubo alguna herramienta o concepto específico que te haya gustado más? ¿Por qué?**

Disfruté mucho de aprender sobre el análisis del tráfico de red y aplicar los conocimientos mediante las herramientas del analizador de protocolos de red. Era la primera vez que aprendía sobre análisis de tráfico de red, por lo que fue desafiante y emocionante. Me fascinó el hecho de haber podido usar herramientas para capturar el tráfico de la red y analizarlo en tiempo real. Definitivamente, me interesa aprender más sobre este tema y espero algún día poder dominar las herramientas de los analizadores de protocolos de red.

Material de apoyo:

- wZN6fLQXR-GqszuaADvueg_565a65a18f524a9a934b627cbd05d1f1_Portfolio-Activity-Finalize-your-incident-handler_s-journal_Incident-handler-s-journal-.docx (live.com)

Actualizar un archivo a través de un algoritmo de Python

Descripción del proyecto

En mi organización, el acceso a contenido restringido se controla con una lista de direcciones IP permitidas. El archivo "allow_list.txt" identifica estas direcciones IP. Una lista de eliminación independiente identifica las direcciones IP que ya no deberían tener acceso a este contenido. Creé un algoritmo para automatizar la actualización del archivo "allow_list.txt" y eliminar estas direcciones IP que ya no deberían tener acceso.

Abrir el archivo con la lista de permisos

Para la primera parte del algoritmo, abrí el archivo "allow_list.txt". Primero, asigné este nombre de archivo como una cadena a la variable import_file:

```
# Assign `import_file` to the name of the file

import_file = "allow_list.txt"
```

Luego, utilicé una sentencia with para abrir el archivo:

```
# Build `with` statement to read in the initial contents of the file

with open(import_file, "r") as file:
```

En mi algoritmo, la sentencia with se usa con la función .open() en modo de lectura para abrir el archivo de lista de permitidos con el fin de leerlo. El propósito de abrir el archivo es permitirme acceder a las direcciones IP almacenadas en el archivo de la lista de permitidos. La palabra clave with ayudará a administrar

los recursos al cerrar el archivo después de salir de la sentencia with. En el código with open(import_file, "r") as file:, la función open() tiene dos parámetros. El primero identifica el archivo a importar, y el segundo, lo que quiero hacer con el archivo. En este caso, "r" indica que quiero leerlo. El código también usa la palabra clave as para asignar una variable llamada file; file almacena la salida de la función .open() mientras trabajo dentro de la sentencia with.

Leer el contenido del archivo

Para leer el contenido del archivo, utilicé el método .read() para convertirlo en la cadena.

```
with open(import_file, "r") as file:

  # Use `.read()` to read the imported file and store it in a variable named `ip_addresses`

  ip_addresses = file.read()
```

Al usar una función .open() que incluye el argumento "r" para "read", puedo llamar a la función .read() en el cuerpo de la sentencia with. El método .read() convierte el archivo en una cadena y me permite leerlo. Apliqué el método .read() a la variable file identificada en la sentencia with. Luego, asigné la salida de cadena de este método a la variable ip_addresses.

En resumen, este código lee el contenido del archivo "allow_list.txt" en un formato de cadena que me permite usar más tarde la cadena para organizar y extraer datos en mi programa Python.

Convertir la cadena en una lista

Para eliminar direcciones IP individuales de la lista de permisos, necesitaba que estuviera en formato de lista. Por lo tanto, utilicé el método .split() para convertir la cadena ip_addresses en una lista:

```
# Use `.split()` to convert `ip_addresses` from a string to a list

ip_addresses = ip_addresses.split()
```

Se llama a la función .split() al agregarla a una variable de cadena. Lo que hace es convertir el contenido de una cadena en una lista. El propósito de dividir ip_addresses en una lista es facilitar la eliminación de direcciones IP de la lista de permitidos. De forma predeterminada, la función .split() separa el texto por espacios en blanco en elementos de lista. En este algoritmo, la función .split() toma los datos almacenados en la variable ip_addresses (que es una cadena de direcciones IP que están separadas por un espacio en blanco) y convierte esta cadena en una lista de direcciones IP. Para almacenar esta lista, la reasigné a la variable ip_addresses.

Iterar a través de la lista de eliminación

Una parte clave de mi algoritmo consiste en iterar a través de las direcciones IP que son elementos de remove_list. Para hacer esto, incorporé un bucle for:

```
# Build iterative statement
# Name loop variable `element`
# Loop through `remove_list`

for element in remove_list:
```

El bucle for en Python repite el código para una secuencia especificada. El propósito general del bucle for en un algoritmo de Python como este es aplicar sentencias de código específicas a todos los elementos de una secuencia. La palabra clave for inicia el bucle for. Le sigue la variable del bucle element y la palabra clave in. La palabra clave in indica iterar a través de la secuencia ip_addresses y asignar cada valor a la variable de bucle element.

Eliminar direcciones IP que están en la lista de eliminación

Mi algoritmo requiere eliminar las direcciones IP de la lista de permitidos ip_addresses, que también estén en remove_list. Puesto que todos los elementos de remove_list también están en la lista ip_addresses y que la lista ip_addresses no contiene duplicados, pude incorporar el método .remove() en el cuerpo de mi bucle for de la siguiente manera:

```
for element in remove_list:

  # use the `.remove()` method to remove
  # elements from `ip_addresses`

  ip_addresses.remove(element)
```

Debido a que las direcciones IP en remove_list se deben eliminar de la lista ip_addresses, apliqué .remove() a ip_addresses. Pasé la variable de bucle element como argumento para que cada dirección IP que estaba en remove_list se eliminara de ip_addresses.

Actualizar el archivo con la lista revisada de direcciones IP

Como paso final en mi algoritmo, necesitaba actualizar el archivo de la lista de permitidos con la lista revisada de direcciones IP. Para ello, primero tuve que convertir la lista de nuevo en una cadena. Para hacerlo, usé el método .join():

```
# Convert `ip_addresses` back to a string so that it can be written into the text file

ip_addresses = " ".join(ip_addresses)
```

El método .join() combina todos los elementos de un iterable en una cadena. Se aplica a una cadena que contiene caracteres que separarán los elementos en el iterable una vez unidos en una cadena. En este algoritmo, utilicé el método .join() para crear una cadena a partir de la lista ip_addresses para poder pasarla como argumento al método .write() al escribir en el archivo "allow_list.txt". Utilicé un solo espacio (" ") como separador.

Luego, utilicé otra sentencia with y el método .write() para actualizar el archivo:

```
# Build `with` statement to rewrite the original file

with open(import_file, "w") as file:

  # Rewrite the file, replacing its contents with `ip_addresses`

  file.write(ip_addresses)
```

Esta vez, utilicé un segundo argumento "w" con la función open() en mi sentencia with. Este argumento indica que quiero abrir un archivo para escribir en su contenido. Al usar este argumento "w", puedo llamar a la función .write() en el cuerpo de la sentencia with. La función .write() escribe los datos de la

cadena en un archivo especificado y reemplaza el contenido de archivo existente.

En este caso, quería escribir la lista de permisos actualizada como una cadena en el archivo "allow_list.txt". De esta manera, las direcciones IP que se hayan eliminado de la lista de permitidos ya no podrán acceder al contenido restringido. Para reescribir el archivo, agregué la función .write() al objeto de archivo file que identifiqué en la sentencia with. Pasé la variable ip_addresses como argumento para especificar que el contenido del archivo especificado en la sentencia with se reemplace con los datos de esta variable.

Resumen

Creé un algoritmo que elimina las direcciones IP identificadas en una variable remove_list del archivo "allow_list.txt" con las direcciones IP aprobadas. Este algoritmo implicaba abrir el archivo, convertirlo en una cadena para leerlo y, luego, convertir esta cadena en una lista almacenada en la variable ip_addresses. A continuación, iteré a través de las direcciones IP en remove_list y eliminé las direcciones IP de la lista ip_addresses con el método .remove(). Posteriormente, utilicé el método .join() para volver a convertir ip_addresses en una cadena para poder sobrescribir el contenido del archivo "allow_list.txt" con la lista revisada de direcciones IP.

Material de apoyo:

- https://d3c33hcgiwev3.cloudfront.net/y2LYMJHeQDutSgwXoatbMg_3abc5449e8fd4c6296a81f4f3d6686f1_Portfolio-Activity-Update-a-file-through-a-Python-algorithm_Algorithm-for-file-updates-in-Python.docx?Expires=1703721600&Signature=Rz8IOOvWD529IxVQrlQ8P0fQisTWPutJeUG38VnGKUYCXFXSLIcemMbKoIroZ

MAY2s5e9~VezUI6cw3Cg7R6Spk0Gym4xEAs2H08aJQCgoemrLLilZo7wfmEHkmRUqjmUx2QyvX1WcEjzNtetnBbfsgaUxtcEehpytOdiF~rqms_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A