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.

Informe de evaluación de riesgos de seguridad

Parte 1: Selección de hasta tres herramientas y métodos de refuerzo
Autenticación Multifactor (MFA): Implementar la autenticación multifactor garantizará que los usuarios verifiquen su identidad mediante dos o más métodos (como contraseñas,

huellas dactilares o códigos OTP) antes de acceder a sistemas o datos críticos. Esto añade una capa adicional de seguridad y reduce significativamente la probabilidad de accesos no autorizados, incluso si las contraseñas se ven comprometidas.

Políticas de Contraseñas:

Establecer políticas de contraseñas que exijan el uso de contraseñas únicas, "salteadas" y "hasheadas" puede ayudar a proteger contra ataques de fuerza bruta y evitar que los usuarios compartan o reutilicen contraseñas débiles. También asegura que se cumplan los requisitos de complejidad de contraseñas sin sobrecargar a los usuarios con cambios frecuentes.

Mantenimiento del Firewall y Filtrado de Puertos:

El mantenimiento regular del firewall y la implementación de reglas de filtrado de puertos adecuadas permitirán a la organización controlar el tráfico entrante y saliente, evitando accesos no autorizados y mitigando el riesgo de posibles ataques. Bloquear puertos no utilizados o vulnerables es crucial para minimizar la exposición de la red.

Parte 2: Explicación de las recomendaciones

Autenticación Multifactor (MFA):

La MFA es una técnica eficaz porque proporciona una capa adicional de seguridad. Incluso si un actor malicioso obtiene acceso a una contraseña, necesitaría un segundo método de autenticación para ingresar al sistema, lo que dificulta mucho la posibilidad de comprometer las cuentas. La MFA debe implementarse de manera continua y mantenerse de forma regular, con actualizaciones periódicas de los métodos de autenticación según evolucionen las amenazas.

Políticas de Contraseñas:

Una política de contraseñas sólida es eficaz para mitigar los riesgos asociados con contraseñas débiles o reutilizadas. La implementación de técnicas de "hashing" y "salting" de contraseñas garantiza que, incluso si las bases de datos de contraseñas se exponen, sea difícil recuperar las contraseñas reales. Es

recomendable revisar las políticas de contraseñas periódicamente para asegurarse de que cumplan con los estándares de seguridad actuales y las necesidades de la organización, pero deben diseñarse para minimizar la carga de los usuarios, lo que fomenta su cumplimiento.

Mantenimiento del Firewall y Filtrado de Puertos:

Las reglas del firewall y el filtrado de puertos ayudan a limitar la exposición de la red restringiendo el acceso solo a los servicios necesarios, evitando el tráfico no autorizado que entra o sale de la red. Es fundamental realizar auditorías periódicas del firewall y actualizar las reglas para adaptarse a nuevas amenazas y vulnerabilidades. Esta práctica debe ser parte de la postura de seguridad continua y revisarse regularmente para asegurar su efectividad, especialmente después de cambios importantes en la infraestructura de la red.

Estas medidas, aplicadas de manera conjunta, abordan varias vulnerabilidades clave dentro de la organización, proporcionando capas de protección que dificultan considerablemente el acceso de los atacantes a la red. La aplicación regular de estas prácticas ayudará a prevenir futuras filtraciones y garantizar la seguridad continua de la red de la organización.