Resumen de la actividad

En esta actividad, considerarás un escenario en el que un cliente de la empresa para la que trabajas experimenta un problema de seguridad al acceder al sitio web de la empresa. Identificarás la causa probable de la interrupción del servicio. A continuación, explicarás cómo se produjo el ataque y el impacto negativo que tuvo en el sitio web.

En este curso, has aprendido sobre varios ataques de red comunes. Aprendiste sus nombres, cómo se llevan a cabo y las características de cada ataque desde la perspectiva del objetivo. Comprender cómo afectan los ataques a una red te ayudará a solucionar problemas en la red de tu organización. También te ayudará a tomar medidas para mitigar los daños y proteger una red de futuros 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.

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.

Cybersecurity Incident Report

Sección 1: Identificar el tipo de ataque que ha causado esta interrupción de la red
Basado en el análisis de los síntomas y el registro de Wireshark, parece que la red está experimentando un **ataque de Denegación de Servicio Distribuida (DDoS)**. Un ataque DDoS inunda un servidor o red objetivo con una gran cantidad de tráfico malicioso proveniente de múltiples fuentes, lo que provoca una interrupción significativa en los servicios. En este caso, el sitio web presenta tiempos de carga extremadamente lentos y errores de "tiempo de espera de conexión agotado". Estos son síntomas clásicos de un ataque DDoS, donde los usuarios legítimos no pueden acceder al servicio debido a que el servidor está sobrecargado con una avalancha de solicitudes. Los registros de Wireshark muestran patrones inusuales de tráfico provenientes de una gran cantidad de direcciones IP en un corto período de tiempo, todas apuntando al mismo servidor web. El volumen y la distribución del tráfico indican un ataque coordinado desde varias fuentes, lo que confirma un ataque DDoS.

Sección 2: Explicación de cómo el ataque está afectando el funcionamiento del sitio web
El ataque DDoS está afectando el sitio web al sobrecargar el servidor con solicitudes falsas o maliciosas, lo que impide que los usuarios legítimos

accedan a la página. El servidor no puede procesar todas las solicitudes simultáneas, lo que causa retrasos y, eventualmente, el agotamiento de recursos del sistema, resultando en errores de tiempo de espera.

Este tipo de ataque afecta negativamente al rendimiento de la red, ya que el tráfico legítimo no puede ser procesado debido a la congestión artificial creada por los atacantes. Las consecuencias de este ataque incluyen la interrupción de los servicios en línea de la organización, pérdida de ingresos, daño a la reputación y posibles costos de recuperación y mitigación.

Es crucial implementar medidas de defensa como el uso de firewalls avanzados, herramientas de monitoreo de tráfico, y sistemas de mitigación de DDoS para prevenir futuros incidentes similares.