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 descargues 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.

Informe incidente ciberseguridad

Sección 1: Identificar el protocolo de red involucrado en el incidente
En la investigación del incidente, se identificaron dos protocolos principales: **HTTP** y **DNS**. El protocolo **DNS** se utilizó para resolver los nombres de dominio, primero para el sitio original (*yummyrecipesforme.com*) y luego para el sitio malicioso (*greatrecipesforme.com*). El protocolo **HTTP** se utilizó para establecer las conexiones entre el navegador y ambos sitios web, lo que permitió la descarga del archivo malicioso y la redirección posterior.

Sección 2: Documentar el incidente
El incidente de seguridad ocurrió cuando un panadero descontento lanzó un ataque de fuerza bruta para adivinar la contraseña administrativa del sitio *yummyrecipesforme.com*, que aún usaba su contraseña predeterminada. Tras

obtener acceso, el atacante modificó el código fuente del sitio web, incrustando un código JavaScript que solicitaba a los usuarios descargar un archivo para supuestamente actualizar sus navegadores.

Al aceptar y ejecutar el archivo, los usuarios eran redirigidos automáticamente al sitio *greatrecipesforme.com*, un sitio web malicioso que imitaba al original y ofrecía gratuitamente las recetas que *yummyrecipesforme.com* vendía. Los registros de red muestran cómo el navegador del usuario primero realiza una resolución DNS de *yummyrecipesforme.com*, carga el sitio web, descarga el archivo malicioso, y luego resuelve la dirección DNS de *greatrecipesforme.com*, estableciendo una nueva conexión HTTP con este sitio malicioso.

El ataque fue posible debido a la falta de medidas de seguridad adecuadas, como la protección contra ataques de fuerza bruta, lo que permitió al atacante obtener las credenciales administrativas.

Sección 3: Recomendación de una medida para prevenir ataques de fuerza bruta
Para prevenir futuros ataques de fuerza bruta, se recomienda implementar **autenticación multifactor (MFA)** en todas las cuentas administrativas. La MFA requeriría que los usuarios verifiquen su identidad utilizando al menos dos métodos (por ejemplo, contraseña y código enviado a un dispositivo móvil), lo que dificultaría significativamente que los atacantes accedieran a las cuentas administrativas, incluso si logran adivinar o robar una contraseña.