

Menú

Estás viendo una versión traducida automáticamente de esta evaluación

Puedes volver a ver el contenido en su idioma original si lo prefieres. No perderás el progreso que hayas conseguido si cambias el idioma. **Mostrar la versión en Inglés**
Cuestionario Práctico

Desestimar ✕

Actividad: Identificar los vectores de ataque de una unidad USB

Para aprobar este tema del curso, debe obtener al menos el 100%, o 1 de 1 puntos, completando la actividad y respondiendo a una pregunta del cuestionario final. Una vez que haya completado la actividad, revise los comentarios al final de la página. Puede obtener más información sobre los ítems calificados y de práctica en la [descripción general del curso](#).

coach



Envía tu tarea

Resumen de la actividad

Reanudar tarea

En esta actividad, evaluará los vectores de ataque de una unidad USB. Considerará un escenario de hallazgo de una unidad USB en un aparcamiento tanto desde la perspectiva de un atacante como de un objetivo.

Recibe la calificación

Los USB, o unidades flash, ~~se utilizan habitualmente~~ **se utilizan habitualmente** para almacenar y transportar datos. Sin embargo, algunas características de estos pequeños y cómodos dispositivos también pueden introducir riesgos para la seguridad. Los actores de amenazas utilizan con frecuencia los USB para distribuir software malicioso, dañar otro hardware o incluso hacerse con el control de los dispositivos. **El USB baiting** es un ataque en el que un actor de amenazas deja estratégicamente una memoria USB con malware para que un empleado la encuentre e instale para infectar una red sin saberlo. Se basa en que los curiosos conecten una memoria USB desconocida que encuentren.

Asegúrese de completar esta actividad antes de continuar. El siguiente punto del curso le proporcionará un ejemplo completado para que lo compare con su propio trabajo.

 Me gusta  No me gusta  Informar de un problema

Escenario

Repase el siguiente escenario. A continuación, complete las instrucciones paso a paso.

Usted forma parte del equipo de seguridad del Hospital Retórico y llega al trabajo una mañana. En el suelo del aparcamiento, encuentra una memoria USB con el logotipo del hospital impreso en ella. No hay nadie más cerca que pueda haberlo tirado, así que decide recogerlo por curiosidad.

Lleva la memoria USB a su oficina, donde el equipo tiene instalado un software de virtualización en una estación de trabajo. El software de virtualización se puede utilizar para este mismo propósito porque es una de las únicas formas de investigar con seguridad una memoria USB desconocida. El software funciona ejecutando una instancia simulada del ordenador en la misma estación de trabajo. Esta simulación no está conectada a otros archivos o redes, por lo que la unidad USB no puede afectar a otros sistemas si resulta estar infectada con software malicioso.

Instrucciones paso a paso

Siga las instrucciones y responda a la siguiente pregunta para completar la actividad.


Paso 1: Acceder a la plantilla

Para utilizar la plantilla para este elemento del curso, haga clic en el enlace y seleccione *Utilizar plantilla*.

Enlace a la plantilla: [Ejercicio USB de aparcamiento](#)

0

Si no dispone de una cuenta de Google, puede descargar la plantilla directamente desde el siguiente archivo adjunto.

 **Parking lot USB exercise**
DOCX File