Actividad: Identifica los vectores de ataque de una unidad USB

Resumen de la actividad

En esta actividad, evaluarás los vectores de ataque de una unidad USB. Considerarás un escenario en el que te encuentras una unidad USB en un estacionamiento tanto desde la perspectiva de un atacante como de un objetivo.
Las unidades USB o unidades flash se usan habitualmente para almacenar y transportar datos. Sin embargo, algunas características de estos pequeños y prácticos dispositivos también pueden introducir riesgos para la seguridad. Los agentes de amenaza suelen usar las unidades USB para distribuir software malicioso, dañar otro hardware o incluso hacerse con el control de los dispositivos. El cebo USB es un ataque en el que un agente de amenaza deja estratégicamente una unidad USB que contiene malware para que un empleado la encuentre y la instale, con el fin de causar la infección involuntaria de una red. Se basa en las personas curiosas que conectan una unidad flash desconocida que se encuentran por casualidad.
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.

Escenario

Revisa el siguiente escenario. Luego, completa las instrucciones paso a paso.
Formas parte del equipo de seguridad del Rhetorical Hospital y llegas al trabajo una mañana. En el suelo del estacionamiento, te encuentras una memoria USB con el logotipo del hospital impreso en ella. No hay nadie más alrededor que pueda haberla dejado caer, así que decides recogerla por curiosidad.
Llevas la unidad USB a tu oficina, donde el equipo tiene instalado un software de virtualización en una estación de trabajo. El software de virtualización se puede usar para este mismo propósito, ya que es una de las únicas maneras de investigar con seguridad el contenido de una memoria USB desconocida. El software funciona ejecutando una instancia simulada de la computadora 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 está infectada con software malicioso.

Respuesta

Contenido	• La unidad USB de Jorge Bailey contiene una combinación de archivos personales y laborales, incluyendo fotos de familiares, una carta de contratación y un horario de turnos de empleados. Esta mezcla de información puede incluir datos de identificación personal (PII) y documentos sensibles relacionados con el trabajo, lo que plantea riesgos significativos si se expone o se utiliza indebidamente. Almacenar archivos personales junto con documentos laborales puede resultar en una falta de seguridad y privacidad.
Mentalidad del atacante	• Un atacante podría utilizar la información contenida en la unidad USB para extorsionar a Jorge o comprometer al hospital. Por ejemplo, al acceder a la carta de contratación, podría obtener información sobre nuevos empleados y usarlos como puntos de ataque. Además, podría utilizar fotos familiares para crear un perfil de Jorge, aumentando el riesgo de ataques dirigidos, como el phishing o el acoso.
Análisis de riesgos	• *Los dispositivos USB pueden estar infectados con diversos tipos de malware, como troyanos, ransomware o keyloggers, que pueden comprometer la seguridad de la red del hospital si son conectados a un sistema. Si otro empleado descubriera un dispositivo USB infectado, podría permitir la entrada de un atacante al sistema de la organización, causando pérdida de datos o interrupción de servicios. La información sensible, como horarios de empleados y datos personales, podría ser utilizada para realizar ataques de ingeniería social o acceder a sistemas internos. Para mitigar estos riesgos, es esencial implementar políticas de seguridad que incluyan el uso de software antivirus actualizado, la capacitación de los empleados sobre los riesgos de los dispositivos USB y la segregación de datos personales y laborales en diferentes dispositivos.*