Lab - Explore Técnicas de ingeniería social

Objetivos

Parte 1: Explorar Técnicas de ingeniería social

Parte 2: Crear un póster de Concientización sobre ciberseguridad

Introducción

La ciberseguridad es fundamental porque implica proteger el acceso no autorizado a datos confidenciales, información de identificación personal (PII), información de salud protegida (PHI), información personal, propiedad intelectual (IP) y sistemas confidenciales. La ingeniería social es la manipulación a las personas para que realicen acciones o divulguen información confidencial. En esta práctica de laboratorio, explorará técnicas de ingeniería social, a veces denominadas hacking humano, que es una categoría amplia para los diferentes tipos de ataques.

Recursos necesarios

Computadora personal o dispositivo móvil con acceso a internet

Aspectos básicos/Situación

Investigaciones recientes revelan que los tipos más comunes de ataques cibernéticos son cada vez más sofisticados y que los objetivos de ataque están creciendo. El propósito de un ataque es robar información, deshabilitar sistemas o servicios críticos, interrumpir sistemas, actividades y operaciones. Algunos ataques están diseñados para destruir información o sistemas de información, controlar maliciosamente un entorno informático o su infraestructura, o destruir la integridad de datos y / o sistemas de información. Una de las maneras más eficaces en que un atacante puede obtener acceso a la red de una organización es mediante un simple engaño. En el mundo de la ciberseguridad, esto se denomina ingeniería social.

Ataques de ingeniería social

Los ataques de ingeniería social son muy eficaces porque las personas quieren confiar en otras personas y los ataques de ingeniería social no son el tipo de ataque contra el que se protege el usuario promedio; los usuarios están preocupados por botnets, robo de identidad o ransomware. Estas son grandes amenazas externas, por lo que no piensan en cuestionar lo que parece ser un mensaje de aspecto legítimo.

Hostigamiento

La carnada depende de la curiosidad o la codicia de la víctima. Lo que distingue a los cebos de otros tipos de ingeniería social es la promesa de un artículo o bien que los hackers utilizan para atraer a las víctimas. Baiters puede ofrecer a los usuarios descargas gratuitas de música o películas si los usuarios entregan sus credenciales de inicio de sesión a un sitio determinado. Los ataques de cebo no se limitan a los esquemas en línea. Los atacantes pueden aprovechar la curiosidad humana con medios físicos como unidades USB.

Espiar por encima del hombro

La navegación de hombro es, literalmente, mirar por encima del hombro de alguien para obtener información. La navegación de hombro es una forma eficaz de obtener información en lugares con mucha gente, ya que es relativamente fácil pararse junto a alguien y observar cómo completan un formulario o ingresan un número PIN en un cajero automático. La navegación de hombro también puede realizarse a larga distancia con la ayuda de teléfonos celulares modernos, binoculares u otros dispositivos para mejorar la visión. Para evitar que se hundan los hombros, los expertos recomiendan proteger la documentación o el teclado mediante el cuerpo o la mano. Incluso hay protectores de pantalla que dificultan mucho la navegación por el hombro.

Pretexto

Pretexto es utilizar el engaño para crear un escenario para convencer a las víctimas de divulgar información que no deben divulgar. Los pretexto a menudo se usan contra organizaciones que conservan datos de clientes, como datos financieros, números de tarjetas de crédito, números de cuentas de servicios públicos y otra información confidencial. A menudo, los pretextos solicitan información a las personas de una organización mediante la suplantación de un supervisor, un empleado del servicio de asistencia o un cliente, generalmente por teléfono, correo electrónico o mensaje de texto.

Suplantación de identidad, suplantación de identidad y ataques de caza de ballenas

En los ataques de suplantación de identidad, los atacantes intentan obtener información personal o datos, como nombre de usuario, contraseña y datos de tarjetas de crédito, disfrazándose de entidades confiables. La suplantación de identidad se realiza principalmente a través de correos electrónicos y llamadas telefónicas. El Spear Phishing es una versión más específica de la suplantación de identidad (phishing) en la que un atacante elige individuos o empresas específicos y luego personaliza el ataque de suplantación de identidad (phishing) a sus víctimas para que sea menos visible. La caza de ballenas es cuando el objetivo específico es un empleado de alto perfil, como un CEO o CFO.

Scareware y ransomware

Los ataques de ransomware implican la inyección de malware que cifra los datos críticos de una víctima. The cyber criminals request a ransom to be paid to decrypt the data. Sin embargo, incluso si se paga un rescate, no hay garantía de que los ciberdelincuentes descifren la información. El ransomware es uno de los tipos de ataque cibernético de más rápido crecimiento y ha afectado a miles de organizaciones financieras, agencias gubernamentales, centros de salud, incluso escuelas y nuestros sistemas educativos.

El scareware aprovecha el temor de un usuario para convencerlo de que instale un software antivirus falso.

Infiltración (tailgating)

El seguimiento ilegal engaña a la víctima para que ayude al atacante a obtener acceso no autorizado a las instalaciones físicas de la organización. El atacante busca entrar en un área restringida donde el acceso está controlado por dispositivos electrónicos basados en software o guardias humanos. El seguimiento ilegal también puede implicar que el atacante siga de cerca a un empleado para atravesar una puerta cerrada antes de que la puerta se cierre detrás del empleado.

Hurgar en la basura

En el mundo de la ingeniería social, el buceo con contenedores de basura es una técnica utilizada para recuperar información desechada que se arroja a la basura para llevar a cabo un ataque contra una persona u organización. Bucear en el contenedor no se limita a buscar en la basura tesoros obvios, como códigos de acceso o contraseñas escritas en notas adhesivas, sino que también puede incluir información electrónica que se deja en los equipos de escritorio o se almacena en unidades USB.

Parte 1. Explore las técnicas de ingeniería social

Paso 1: Explore la carnada, la navegación de hombro y la predisposición.

El Centro de soporte nacional para la seguridad de los sistemas y el aseguramiento de la información (CSSIA) organiza una actividad interactiva de ingeniería social. El enlace actual al sitio es https://www.cssia.org/social_engineering/. Sin embargo, si el enlace cambia, intente buscar "CSSIA Social Engineering Interactive".

Haga clic en Siguiente en la actividad interactiva y luego utilice el contenido para responder las siguientes preguntas.

¿Qué es la carnada? ¿Hizo clic en la unidad USB? ¿Qué sucedió con el sistema de la víctima?

¿Qué es espiar por encima del hombro? ¿Qué dispositivo se utilizó para espiar por encima del hombro? ¿Qué información se obtuvo?

¿Qué es Pretextar (pretexting)? ¿Qué tipo de información solicitó el ciberdelincuente? ¿Caería como víctima?

Paso 2: Explore el Pishing, el Spear Phishing y la caza de ballenas

La suplantación de identidad (Phishing) está diseñada para que las víctimas hagan clic en enlaces a sitios web maliciosos, abran archivos adjuntos que contengan malware o revelen información confidencial. Utilice la actividad interactiva para explorar diferentes técnicas de suplantación de identidad.

En este ejemplo de suplantación de identidad, ¿cuál es la táctica que utiliza el atacante para engañar a la víctima para que visite el sitio web de la trampa? ¿Para qué se utiliza el sitio web de trap?

¿Cuál es la diferencia entre Phishing y Spear Phishing o caza de ballenas?

Paso 3: Explore Scareware y Ransomware

Scareware es cuando las víctimas son engañadas al pensar que su sistema está infectado con malware y reciben falsas alarmas que les instan a instalar software que no es necesario o es en sí mismo malware. El ransomware es un tipo de malware que amenaza con publicar los datos de la víctima o encripta los datos de la víctima impidiendo el acceso o la capacidad de usar los datos. Las víctimas no pueden acceder a su sistema o a sus archivos personales hasta que realicen un pago de rescate para recuperar el acceso.

¿Qué datos afirma tener el atacante en este ejemplo? ¿Caería usted en este engaño?

¿Qué solicita el atacante que haga la víctima para recuperar los datos?

¿Qué es la infiltración (tailgating)?

¿De tres maneras de prevenir ataques de ingeniería social?

Parte 2. Crear un póster de Concientización sobre ciberseguridad

Utilice PowerPoint para crear un póster que haga que otros conozcan las diferentes técnicas de ingeniería social utilizadas para obtener acceso no autorizado a una organización o a los datos de la organización.

Elija entre: hostigamiento, navegación de hombro, pretexto, suplantación de identidad (phishing), Scareware, ransomware, infiltración o buceo en el contenedor.

El póster debe mostrar las técnicas utilizadas y cómo los usuarios pueden evitar uno de estos ataques de ingeniería social. También incluya instrucciones sobre dónde debe colocarse el póster dentro de la organización.