ehack.info

Ingeniería Social – Ethical Hack - Blog

BY carlosgbr

6-8 minutos

La ingeniería social es un método no técnico para irrumpir en un sistema o red. Es el proceso de engañar a los usuarios de un sistema y convencerlos a realizar actos de utilidad para el hacker, tales como dar información que se puede utilizar para anular o evitar mecanismos de seguridad.

Es importante entender la ingeniería social porque los hackers la pueden utilizar para atacar al elemento humano de un sistema y eludir las medidas técnicas de seguridad. Este método puede ser utilizado para recoger información antes de o durante un ataque.

La parte más peligrosa de la ingeniería social es que las empresas con procesos de autenticación, cortafuegos, redes privadas virtuales y software de supervisión de la red siguen siendo vulnerables a ataques externos, ya que la ingeniería social no ataca las medidas de seguridad directamente.

El arte de la manipulación

La ingeniería social incluye la adquisición de información sensible o el acceso indebido de privilegios por un extraño, basado en la construcción de relaciones de confianza

inapropiados. Los hackers que son capaces de relacionarse y parece ser una parte de la organización son los más exitosos en los ataques de ingeniería social. Esta capacidad de mezclarse es referida comúnmente como el arte de la manipulación.

Tipos de ataques de ingeniería social

La ingeniería social se puede dividir en dos tipos comunes:

Basados en personas: Ingeniería social basada en las personas se refiere a la interacción de persona a persona para obtener la información deseada. Basada en el Cómputo: La ingeniería social basada en cómputo se refiere a tener los programas informáticos para intentar obtener la información deseada.

Ingeniería social basada en personas

Las técnicas de ingeniería social basados en personas pueden clasificarse en términos generales como sigue:

- Hacerse pasar por un empleado o usuario válido en este tipo de ataque de ingeniería social, el hacker se hace pasar por un empleado o un usuario válido en el sistema.
- Haciéndose pasar por un usuario importante en este tipo de ataque, el hacker que pretende ser un usuario importante, como un ejecutivo o gerente de alto nivel que necesita asistencia inmediata para obtener acceso a un sistema informático o archivos.
- Uso de una tercera persona utilizando el enfoque de tercera persona, un hacker pretende tener el permiso de una fuente autorizada para utilizar un sistema.
- Llamar al soporte técnico llamar al servicio de soporte técnico

es una técnica clásica de la ingeniería social.

- Shoulder surfing es una técnica de recopilación de contraseñas, mirando por encima del hombro de una persona antes de que inicie sesión en el sistema.
- Dumpster diving consiste en buscar en la basura para obtener información escrita en pedazos de papel o impresiones informáticas.
- Un método más avanzado de obtención de información ilícita se conoce como ingeniería social inversa. Usando esta técnica, un hacker crea un personaje que parece estar en una posición de autoridad para que los empleados busquen al hacker para obtener información, en lugar de a la inversa.

La ingeniería social basada en Cómputo

Los ataques de ingeniería social basados en computadora pueden incluir los siguientes:

- Adjuntos de correo electrónico
- Sitios web falsos
- Ventanas pop-up
- Ataques internos

Si un hacker no puede encontrar alguna otra manera de vulnerar una organización, la siguiente mejor opción es infiltrar la organización siendo contratado como empleado o mediante la búsqueda de un empleado descontento que ayude en el ataque. Los ataques internos pueden ser de gran alcance porque los empleados tienen acceso físico y son capaces de moverse libremente por la organización.

El robo de identidad

Un hacker puede hacerse pasar por un empleado o robar la identidad del empleado para perpetrar un ataque. La información reunida en la etapa de dumpster diving o en el Shoulder surfing en combinación con la creación de credenciales de identificación falsas puede dar acceso a los hackers en una organización.

Los ataques de phishing

El phishing consiste en el envío de un correo electrónico, por lo general se hacen pasar por un banco, compañía de tarjetas de crédito u otra organización financiera. Los correos solicitan que el destinatario confirme la información bancaria o piden restablecer las contraseñas o PIN. El usuario al hace clic en el enlace del correo electrónico se redirige a un sitio web falso.

Las estafas en línea

Algunos sitios web que hacen ofertas gratuitas u otras ofertas especiales pueden atraer a una víctima para introducir un nombre de usuario y una contraseña que puede ser los mismos que los que utilizan para tener acceso a su sistema de trabajo.

Ventanas emergentes también se pueden utilizar en los ataques de ingeniería basados en computadoras, en una situación similar al los archivos adjuntos de correo electrónico, ventanas pop-up con ofertas especiales o cosas gratis pueden animar a un usuario a instalar software malicioso sin querer.

Ofuscación de URL

En términos simples, es la dirección del sitio web. La ofuscación de URL consta en ocultar una dirección URL falsa en lo que parece ser una dirección de sitio web legítimo. Por ejemplo, un

sitio web 204.13.144.2/Citibank puede parecer ser una dirección web legítima para Citibank pero en realidad no lo es. La ofuscación de URL se utiliza en los ataques de phishing y en estafas en línea para hacer que la estafa parezca legítima.

Contramedidas de ingeniería social

Saber cómo combatir la ingeniería social es fundamental para cualquier hacker ético certificado. Hay varias maneras de hacer esto.

Políticas de seguridad documentadas y aplicadas, y programas de sensibilización de seguridad son el componente crítico en cualquier programa de seguridad de la información. Las buenas políticas y procedimientos no son eficaces si no se enseñan y refuerzan en los empleados. Las políticas deben ser comunicadas a los empleados para enfatizar su importancia y, deben ser aplicadas por la dirección.

Obtendrás **lecciones detalladas**, material adicional, recursos y asesoría vía Correo y Foro, visita https://ehack.mx/ceh para más información o ecríbenos a campus@ehack.mx

EHACK

Ethical hack

Fuente Imágenes:

- «Ingeniería Social»: Imagen cortesía by Stuart Miles en FreeDigitalPhotos.net

Créditos:

- Por Roberto C. González
- Basado parcialmente en la obra de Kimberly Graves
