Objetivos

Investigar e identificar ataques de ingeniería social

Aspectos básicos / Escenario

Los ataques de ingeniería social tienen como objetivo lograr que una víctima introduzca información personal o confidencial; este tipo de ataque puede ser realizado por un delincuente que está utilizando un capturador de teclas, correos electrónicos de phishing o un método físico. En esta práctica de laboratorio tendrán que investigar la ingeniería social e identificar formas de reconocerla e impedirla.

Recursos necesarios

Dispositivo móvil con acceso a internet

Instrucciones

Utilizando un navegador web, encontrar el artículo "Methods for Understanding and Reducing Social Engineering Attacks" en el sitio web del Instituto SANS. Un motor de búsqueda debe encontrar fácilmente el artículo.

El Instituto SANS es una organización cooperativa de investigación y educación que ofrece capacitación en seguridad de la información y certificación en seguridad. La Sala de lectura SANS tiene muchos artículos que son relevantes para la práctica de análisis de ciberseguridad. Podemos unirnos a la comunidad SANS creando una cuenta de usuario gratuita para acceder a los artículos más recientes, o bien puede acceder a los artículos más antiguos sin una cuenta de usuario.

Lea el artículo o escoja otro artículo sobre ingeniería social, léalo y responda las siguientes preguntas:

a. ¿Cuáles son tres métodos que se utilizan en la ingeniería social para obtener acceso a la información?
b. ¿Cuáles son tres ejemplos de ataques de ingeniería social?
c. ¿Por qué las redes sociales son una amenaza de ingeniería social?

d. ¿Qué puede hacer una organización para defenderse de ataques de ingeniería social?

e. ¿Qué es el SANS Institute, quién es el autor de este artículo?

Alumno: Julián Gordon

A) Cuáles son tres métodos que se utilizan en la ingeniería social para obtener acceso a la información?

Los tres metodos que se usan en la ingenieria social para obtener información son, acceso electronico , acceso físico y Redes sociales que mezcla acceso electronico y acceso fisico.

B) Cuáles son tres ejemplos de ataques de ingeniería social?

Podríamos citar como ejemplos el Phishing que es una técnica de ingeniería social que consiste en el envío de correos electrónicos que suplantan la identidad de compañías u organismos públicos y solicitan información personal y/o bancaria al usuario.

El Baiting consiste en un ataque informático de ingeniería social en el que el atacante presenta una oportunidad tentadora, ya sea para obtener un beneficio o por simple curiosidad, y la usa para atraer a la víctima a sufrir un ataque.Básicamente consiste en poner un cebo para atraer a la víctima hacia una trampa.

El pretexting es la base de cualquier ataque de ingeniería social. Consiste en crear elaborar un escenario o historia ficticia, donde el atacante tratará que la víctima comparta información que, en circunstancias normales, no revelaría.

C) ¿Por qué las redes sociales son una amenaza de ingeniería social?

Porque en las redes sociales las personas suelen compartir información personal, como nombres, ubicación, fechas de graduacion, nacimiento, estudios realizados, gustos personales, interes por determinados asuntos.

Esto puede brindar información muy útil a ciberdelincuentes para realizar ataques personalizados, intentar romper contraseñas, descubrir información personal e intentar hacerse pasar por otras personas.

D)¿Qué puede hacer una organización para defenderse de ataques de ingeniería social?

En primer lugar concienciar a los trabajadores sobre la seguridad interna y hacer un plan de capacitación personalizada para disminuir la probabilidad de que caigan en ataques de ingenieria social. Este plan debe planificarse, ser diseñado, implementado y medido.

Debe estar “integrado” en los procesos cotidianos de la organización hasta que se convierta en parte de la cultura de la organización.

Para eso podremos citar ejemplos como:

Asegurarse que todos los trabajadores aprendan las políticas de seguridad y procedimientos.

Que se reduzca el uso de internet en 30% para asuntos personales.

E) ¿Qué es el SANS Institute, quién es el autor de este artículo?

El SANS institute es es una institución con ánimo de lucro fundada en 1989, con sede en Bethesda (Maryland, Estados Unidos) que agrupa a 165.000 profesionales de la seguridad informática. Este instituto brinda recursos muy confiables para capacitación, certificaciones e investigación en ciberseguridad.

El autor de este artículo es Michael Alexander,miembro del SANS institute.