Práctica de laboratorio: Ingeniería social

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

- Computadora personal o 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 de los primeros dos métodos del Paso 2a?

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?