Guía de aprendizaje 1: Identificación de vulnerabilidades y amenazas

Introducción

Ahora bien, en el documento se presenta una clasificación de las amenazas de acuerdo con el modelo CIA (confidencialidad, integridad, y disponibilidad) y queremos complementarlo con otra clasificación, de acuerdo con las capas de seguridad.

- Amenazas a nivel de software: Se refiere a toda amenaza que se aprovecha de:
    - Defectos que derivan en errores
    - Defectos que son producto de explotaciones
    - Programas maliciosos como virus, gusanos, troyanos, puertas traseras
    - Bots (programa de software que corre tareas automáticas)
    - Ataques de autenticación (cuando un ciberdelincuente intenta obtener nuestras credenciales por la fuerza)
    - Explotación de configuraciones erróneas
- Amenazas humanas: Son aquellas amenazas que presentamos los humanos o por la interacción entre nosotros los humanos como:
    - Ingeniería social: Es una forma de engañar a las personas para que proporcionen información sensible como contraseñas o información sobre tarjetas de crédito.
    - Ataques por hackers o ciberdelincuentes
    - Extorsiones
    - Espionaje

Vamos a profundizar un poco en la ingeniería social porque para los ciberdelincuentes es la forma más fácil de cometer délitos y obtener lo que quieren. La ingeniería social puede presentarse de diferentes maneras:

- Espiar sobre el hombro: Es la práctica de espiar la contraseña o PIN de una persona mientras la escribe en el dispositivo para acceder de manera ilegal a su información personal. Esto puede ser en una oficina o un lugar público como una cafetería. El aumento en el uso de computadoras y teléfonos ha permitido que esta técnica sea más frecuente.
- Persuación: En esta, el atacante presiona a la persona para que proporcione información personal intentando convencerla que está actuando de buena fé sobre lo que pasaría si la persona no le proporciona la información solicitada.
- Uso de “pretextos”: Un pretexto es un propósito o motivo que esconde las intenciones reales. En cuanto a ingeniería social, pretexto es básicamente impersonificación. Es decir, el atacante pretende ser alguién más para ganarse la confianza y obtener información.

Ejercicios

Ahora se presentan algunos escenarios en los que debe identificar qué tipo de amenaza y/o vulnerabilidad se presenta. Para clasificar las amenazas puede hacerlo basado en cualquiera de los dos modelos presentados, de acuerdo con CIA o con las capas de seguridad. Algunos de los escenarios pueden abarcar más de una categoría de clasificación.

- En tu trabajo tienes un (a) compañero (a) en el cual confías mucho y has decidido compartir tu nombre de usuario y contraseña para ingresar al ordenador.
- Utilizas una complejidad de contraseña débil para acceder a una cuenta.
- Estas a punto de eliminar una serie de archivos y directorios, pero sin darte cuenta has seleccionado otros archivos que no deberías. Accidentalmente eliminas la información permanentemente.
- Recibes una llamada telefónica de una persona que se identifica como personal de una entidad bancaria. La persona te indica que sucede algo extraño con una cuenta y que necesita confirmar cierta información para poder hacer una revisión. Entre la información que solicita es tu nombre de usuario y la pregunta favorita que has configurado para ingresar a la plataforma.
- Alguien accede a una de tus cuentas en línea debido a un error en la aplicación.
- Estas en un espacio público utilizando tu ordenador y observas un comportamiento anómalo de una persona quien constantemente está observando lo que haces.
- Te ha llegado un correo electrónico con un adjunto que parece un documento. En realidad el documento era un programa malicioso (ingenioso por parte del atacante) que se ha instalado en el ordenador. El programa malicioso ha encriptado los directorios, al cual ya no tienes acceso. El mensaje que se muestra es que debes depositar dinero para recuperar el acceso a tu información.