Práctica de laboratorio: Casos prácticos de ciberseguridad Objetivos

Investigar y analizar incidentes de ciberseguridad

Parte 1: Realice una búsqueda de ciberataques de alto perfil

Parte 2: Escriba un análisis de un ciberataque

Antecedentes / Escenario

Los gobiernos, las empresas y los usuarios individuales cada vez son más propensos a ser víctimas de ciberataques y los expertos predicen que en el futuro probablemente haya más ataques. La educación en ciberseguridad es la máxima prioridad internacional ya que los incidentes de alto nivel relacionados con ciberseguridad aumentan los temores de que los ataques puedan amenazar a la economía global. El centro de estrategia y estudios internacionales estima que el costo de los cibercrimenes en la economía global es más de $600 billones anuales. En esta práctica de laboratorio estudiarán cuatro ciberataques de alto perfil y se prepararán para analizar el quién, qué, por qué y cómo de cada ataque.

Recursos necesarios

• Computadora personal o dispositivo móvil con acceso a internet

Instrucciones

Parte 1: Buscar ciberataques de alto perfil

a. Utilicen su motor de búsqueda favorito para buscar cada uno de los ciberataques que se mencionan a continuación. En su búsqueda probablemente encuentren varios resultados que pueden ser desde noticias hasta artículos técnicos.

- El virus Stuxnet
- Violación de datos Marriott
- Violación de datos de las Naciones Unidas
- Violación de la base de datos de soporte al cliente de Microsoft
- Violación de datos de Lifelabs

Nota: Puede utilizar el navegador web de la máquina virtual instalada en una práctica de laboratorio anterior para investigar el hack. Si utilizan la máquina virtual, pueden impedir que se instale malware en su computadora.

b. Lean los artículos que encontraron en sus búsquedas del paso 1a y prepárense para analizar y compartir sus búsquedas con respecto al quién, qué, cuándo, dónde y por qué de cada ataque.

Parte 2: Redactar un análisis de un ciberataque

Seleccionen uno de los ciberataques de alto perfil del paso 1a y redacten un análisis del ataque en el que se incluyan respuestas para las siguientes preguntas.

a. ¿Quiénes fueron las víctimas de los ataques?

Una planta nuclear en Bushehr, en Irán. En concreto afectó a mil máquinas centrifugadoras reprogramandolas

Práctica de laboratorio: Casos prácticos de ciberseguridad

b. ¿Qué tecnologías y herramientas se utilizaron en el ataque?

El ataque fue en forma malware a través de un gusano. Este se introdujo a través de un USB en un equipo conectado a la red y desde ahí se propagó por esta. El gusano tenía órdenes de tomar el control del software que controla las centrifugadoras

c. ¿Cuándo ocurrió el ataque en la red?

En enero de 2010

d. ¿Cuáles fueron los sistemas objetivo?

Equipos con Windows . PLC ´S . Equipos con Sistemas de control SIEMENS

e. ¿Qué motivó a los atacantes en este caso? ¿Qué esperaban lograr?

Inutilizar maquinaria de central nuclear mediante la toma de control de sus máquinas.

f. ¿Cuál fue el resultado del ataque? (datos robados, rescate, daños en el sistema, etc.)

Alterar maquinaria industrial. Miles de activos infectados. Principalmente en Irán.

