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.

Violación de datos de Lifelabs

a. ¿Quiénes fueron las víctimas de los ataques?

La compañía LifeLabs, que es la compañía más grande de pruebas de laboratorio y análisis clínicos de Canadá.Se vieron afectados 15 millones de clientes, aunque la empresa asegura que fueron menos.Hasta la fecha es una de una de las mayores violaciones de datos en la historia de Canadá.

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

En el ataque se empleó un tipo de malware llamado ransomware. Es uno de los malware más frecuentes actualmente, encripta los datos y puede suponer graves pérdidas tanto para empresas como para particulares.

Se cree que los atacantes aprovecharon vulnerabilidades en el sistema de almacenamiento de datos y después con herramientas como Metasploit consiguieron escalar permisos y tomar el control de la red interna de Lifelabs.

El ransomware se difunde de diferentes formas:

-Correos phishing: Un correo que simula ser legítimo, engañan al usuario y hacen que descarguen el ransomware.

-Vulnerabilidades de software: Son fallos en aplicaciones y sistemas desactualizados, como exploits día cero.

-Descargas maliciosas: Al visitar sitios web comprometidos.

Lo más probable en el caso de LifeLabs es que fuera una combinación de técnicas de ingeniería social, unido a vulnerabilidades en los sistemas y robo de credenciales. Al no tener bien implantada la empresa la autenticación multifactor facilitó el hackeo.

c. ¿Cuándo ocurrió el ataque en la red?

El ataque comenzó en Octubre de 2019, los hackers lograron infiltrarse y robar los datos de millones de clientes.

A principios de Noviembre de ese mismo año es cuando se descubre el ataque, por amenazas y extorsiones que recibe la empresa, y contrata a expertos en ciberseguridad para evaluar el daño.

En Diciembre de 2019 la empresa paga un rescate a los atacantes para recuperar los datos y evitar su publicación.

d. ¿Cuáles fueron los sistemas objetivo?

El objetivo principal era la base de datos de los clientes. Pero también se vieron comprometidos los sistemas de facturación de la empresa y servidores internos para aplicaciones.

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

Como en casi todos los ataques de Ransomware, beneficio económico por el rescate de datos.

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

Fueron encriptados los datos de la base de datos (nombres, direcciones,correos,credenciales de acceso, fechas de nacimiento…), las aplicaciones quedaron inoperativas y la empresa perdió parcial o totalmente el control de la red interna.

Finalmente la empresa pagó por el rescate de los datos.

♥ 2018 – 2020 Cisco y/o sus filiales. Todos los derechos reservados. Información pública de Cisco