Tema1.1.2.3.EnriqueGomezTagle

sábado, 3 de febrero de 2024 14:17

Enrique Ulises Báez Gómez Tagle – 0241823 - 0241823@up.edu.mx
UP. 2024. Ene-Jun. Hackeo Ético y Recuperación Ante Desastres – Yoel Ledo Mezquita

Instrucciones

Parte 1: Buscar vulnerabilidades en aplicaciones IoT

Utilicen su motor de búsqueda favorito para buscar vulnerabilidades de la Internet de las Cosas (IoT). Busquen un ejemplo de una vulnerabilidad IoT para cada uno de los segmentos verticales de IoT: industria, sistemas de energía, servicios de salud y gobiernos. Prepárense para debatir quiénes podrían aprovechar la vulnerabilidad y por qué, qué causó la vulnerabilidad y qué podría hacerse para limitarla.

- Recursos IoT de Cisco (en inglés)
- IoT Security Foundation (en inglés)
- Amenazas de seguridad de la IoT de Business Insider (en inglés)

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

Mientras investiguen, elijan una vulnerabilidad IoT y respondan las siguientes preguntas:

a. ¿Cuál es la vulnerabilidad?

Falta de cifrado o cifrado débil en comunicaciones entre dispositivos IoT

b. ¿Quién podría aprovecharla? Explique.

Una persona malicisa es capaz de interceptar estas comunicaciones y podría capturar o manipular datos sensibles que sean transmitidos entre estos dispositivos.

Práctica de laboratorio: Averiguar los detalles de los ataques

c. ¿Por qué existe la vulnerabilidad?

- Negligencia en la implementación de estándares de seguridad por parte de los fabricantes.
- Limitaciones de hardware
- Falta de conciencia

d. ¿Qué se puede hacer para limitar la vulnerabilidad?

- Usar protocolos de comunicación seguros como TLS para que los datos estén cifrados.
- Hacer pruebas de seguridad a los dispositivos para encontrar vulnerabilidades