Tarea online AFI04.

Título de la tarea: Análisis de IoT

Ciclo formativo y módulo: Curso de especialización en ciberseguridad en entornos de las tecnologías de la información - Análisis Forense Informático.

¿Qué contenidos o resultados de aprendizaje trabajaremos?

Resultados de aprendizaje

- **RA4.** Realiza análisis forense en dispositivos del IoT, aplicando metodologías establecidas, actualizadas y reconocidas.

Contenidos

1.- Realización de análisis forenses en Internet of Things (IoT).
- 1.1.- Identificar los dispositivos a analizar.
- 1.2.- Adquirir, analizar y extraer las evidencias.
- 1.3.- Línea temporal y cadena de custodia
- 1.4.- Elaborar, Presentar y Exponer las conclusiones.

1.- Descripción de la tarea.

Caso práctico

María se enfrente a uno de sus mayores retos, en la escena de un posible delito encuentran una cámara IP que podría haber almacenado información valiosa sobre lo sucedido.

El problema es que María no sabe que tipo de sistema operativo o sistema de ficheros usa este dispositivo o que tipo de servicios o conexiones realizar por lo que analiza su firmware para tener más detalles de dónde, qué y cómo buscar.

Pixabay (Dominio público)

¿Qué te pedimos que hagas?

- **Apartado 1: Análisis de IoT**
  Esta tarea nos enfrentaremos a uno de los principales retos que tenemos cuando tenemos que analizar un dispositivo de IoT que desconocemos su funcionamiento.
  - PREGUNTA 1: ¿Qué información podemos obtener del firmware de la siguiente de la bombilla (dispositivo IoT)? ¿Por qué sucede esto? ¿Qué supone para el análisis forense esta situación?
    - Link firmware https://drive.google.com/drive/folders/1U7vZameivlfhaOiSLYfbujV1ZOOMhrIb
  - PREGUNTA 2: ¿Qué información podemos obtener del firmware de la cámara XIAOMI IMI Home Security Camera 1080P ? ¿Qué sistema operativo usa?
    - https://drive.google.com/file/d/1pB_XqoHGLN9yA51HgD9QHoxpx588Kn1v/view?usp=sharing
  - PREGUNTA 3: ¿Qué sistema de ficheros usa?
  - PREGUNTA 4: ¿Puedes decir algunos servicios que use?
  - PREGUNTA 5: ¿Podrías decirnos que usuarios tiene?
  - PREGUNTA 6: ¿Cómo se llama este tipo de análisis?

NOTA IMPORTANTE

Para todos los apartados es necesario entregar las capturas de pantalla de los principales pasos realizados, explicando el proceso seguido en cada uno de ellos. Las capturas de pantalla realizadas deben tener como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil. Aquellos apartados/subapartados que no cumplan esta condición no serán corregidos.

2.- Información de interés.

Recursos necesarios y recomendaciones

Recursos necesarios

- Ordenador personal con, al menos, 4 Gigabytes de memoria RAM
- Conexión a Internet para consultar ejemplos de la Unidad 1.
- Navegador web.
- Consola de comandos en Linux o Windows (recomendado)

Recomendaciones

- Antes de abordar la tarea:
  - Lee con detenimiento la unidad, consulta los enlaces para saber más, examina el material proporcionado por el profesor y aclara las dudas que te surjan con él.
  - Realiza el examen online de la unidad, y consulta nuevamente las dudas que te surjan. Solo cuando lo tengas todo claro, debes abordar la realización de la tarea.
- Te recomendamos usar un sistema operativo Linux pero es igualmente realizable en entornos Windows
- Aunque no es obligatorio el ejercicio puede resolverse desde una consola de comandos
- Algunas de las herramientas necesarias son: file, binwalk, firmwalker

Indicaciones de entrega

Una vez realizada la tarea, el envío se realizará a través de la plataforma. El archivo se nombrará siguiendo las siguientes pautas:

Apellido1_Apellido2_Nombre_AFI04_Tarea

Asegúrate que el nombre no contenga la letra ñ, tildes ni caracteres especiales extraños. Así por ejemplo la alumna **Begoña Sánchez Mañas para la cuarta unidad del MP de AFI**, debería nombrar esta tarea como...

sanchez_manas_begona_AFI04_Tarea

3.- Evaluación de la tarea.

Criterios de evaluación implicados

Criterios de evaluación RA4

- a. Se han identificado los dispositivos a analizar garantizando la preservación de las evidencias.
- b. Se han utilizado mecanismos y herramientas adecuadas para la adquisición y extracción de evidencias.
- c. Se ha garantizado la autenticidad, completitud, fiabilidad y legalidad de las evidencias extraídas.
- d. Se han realizado análisis de evidencias de manera manual y mediante herramientas.
- e. Se ha documentado el proceso de manera metódica y detallada.
- f. Se ha considerado la línea temporal de las evidencias.
- g. Se ha mantenido la cadena de custodia.
- h. Se ha elaborado un informe de conclusiones a nivel técnico y ejecutivo.
- i. Se han presentado y expuesto las conclusiones del análisis forense realizado.

¿Cómo valoramos y puntuamos tu tarea?

Rúbrica de la tarea	
Apartado 1.a: ¿Qué información podemos obtener del firmware de la siguiente de la bombilla (dispositivo IoT)? ¿Por qué sucede esto? ¿Qué supone para el análisis forense esta situación?	2 puntos
Apartado 1.b: ¿Qué información podemos obtener de la imagen de la cámara XIAOMI? ¿Qué sistema operativo usa?	1 punto
Apartado 1.c: ¿Puedes decir qué sistema de ficheros usa?	1 punto
Apartado 1.d: ¿Puedes decir algunos servicios que use?	2 puntos

Apartado 1.e: ¿Podrías decirnos que usuarios tiene?	2 puntos
Apartado 1.f: ¿Cómo se llama este tipo de análisis?	2 puntos

NOTA IMPORTANTE

Aquellos apartados/subapartados en los que las capturas de pantalla no sean claras o no tengan como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil, no serán corregidos.