Módulo 1 (Curso 2020/21):

Trabajos en Grupo

Auditoría Informática II

1. Análisis forense de ordenador Windows & Linux (5-7 grupos)

a. Objetivo
   i. Toma de evidencias volátiles.
   ii. Toma de evidencias no volátiles
   iii. Análisis de una imagen de disco duro de un equipo con S.O. Windows a escoger de "forma libre" por el grupo (instalado en un sistema virtual) y de un equipo con S.O. Linux (por ejemplo: Kali Linux).

b. Documentación principal
   i. INCIBE-CERT: "Guía de toma de evidencias en entorno Windows" (www.incibe-cert.es)
   ii. Herramienta Autopsy
   iii. Forensic Analysis with Autopsy in Kali Linux (https://www.youtube.com/watch?v=9AyiRITI9HI&t=441s)

c. Documentación auxiliar
   i. A definir por el alumno

d. Entregable: informe de auditoría según el modelo de la asignatura con:
   i. Descripción del método y escenario de investigación.
   ii. Explicación de las fases del proceso de análisis forense realizadas.
   iii. Explicación razonada y detallada de cada respuesta y tabla de esfuerzos.

e. Exposición al final del segundo cuatrimestre.

Procedimiento de Trabajo:

FASE I

1. Se instalará en un sistema virtual un sistema operativo Windows. Con el sistema arrancado se realizarán distintas operaciones como:
   a. Dar de altas distintas cuentas de usuario con distintas propiedades.
   b. Instalar más de seis programas de hacking ético o informática forense.
   c. Borrar distintos ficheros (gráficos, vídeo, audio, texto y comprimidos), programas ejecutables, etc. De ellos eliminar algunos de la "Papelera".
   d. Navegar y acceder a distintas páginas comprobando que se generan "cookies".
   e. Enviar correos electrónicos desde alguna de las cuentas de usuario.
2. Se obtendrá una imagen forense del sistema Windows a analizar instalado en una máquina virtual ("copia de disco principal") en formato "Encase® E01" o "raw (dd) files" (admitido por Autopsy). Para ello se investigará sobre las herramientas o sistemas disponibles y se explicará de una forma motivada cuál se ha escogido, por qué y el procedimiento seguido para obtener la imagen forense.

FASE II

3. Utilizando un kit de herramientas definidas previamente por el equipo auditor, se procederá a la toma de evidencias (volátiles y no volátiles) según la guía de INCIBE.
4. Utilizando Autopsy se procederá a analizar la evidencia no volátil "copia de disco principal". En este análisis se responderá de forma razonada (explicando el método seguido de análisis), preguntas siguientes:
   a) ¿Cuál es el hash de la imagen? ¿Coincide la adquisición con la verificación?
   b) ¿Qué sistema operativo fue usado en el ordenador?
   c) ¿Cuándo fue la fecha de instalación?
   d) ¿Cuál es la configuración de la zona horaria?
   e) ¿Quién es el propietario registrado?
   f) ¿Cuál es el nombre de la cuenta del ordenador?

g) ¿Cuál es el nombre del dominio principal o grupo?
h) ¿Cuándo fue la última vez que se apagó el ordenador (fecha y hora)?
i) ¿Cuándo fue la última vez que se arrancó el ordenador (fecha y hora)?
j) ¿Cuántas cuentas de usuario hay recogidas (Número total)?
k) ¿Cuál es el nombre de cuenta de usuario que más veces ha usado el ordenador?
l) ¿Cuál es la fecha de último acceso de cada usuario existente en el sistema?
m) ¿Quién fue el último usuario en iniciar sesión en el ordenador?
n) ¿Cuáles es la lista de las tarjetas de red usadas por el ordenador y sus direcciones IP y MAC?
o) Encuentra al menos 4 programas que se usen para hacking.
p) ¿Cuál es la dirección SMTP de los usuarios del sistema?
q) ¿Cuántos archivos ejecutables hay en la papelera de reciclaje? ¿Cuáles son?
r) ¿Están los archivos realmente borrados?
s) ¿Cuántos archivos están esperando a ser borrados?
t) ¿Cuántas cookies y cuál es su contenido se encuentran en el sistema?

FASE III

5. Haciendo uso de una imagen de un S.O. Linux que previamente haya sido modificada (se podrá usar algunas de las acciones de la FASE I), se utilizará AUTOPSY en vuestra distribución LINUX para realizar el siguiente análisis:

a) Obtener 5 evidencias (pueden ser volátiles o no).
b) ¿Cuál es el sistema de ficheros usado en la imagen que se está analizando?.
c) ¿Cuál es el hash de la imagen?. ¿Coincide la adquisición con la verificación?.
d) Realizar una búsqueda de evidencia por palabra clave.
e) Realizar el análisis de metadatos de 3 ficheros (formatos: .pdf, .docx y .jpg/.png).

Informe de análisis forense a redactar y enviar por el CV (máximo 30 páginas)
Se incluirá al menos:

1. Descripción del laboratorio de análisis forense utilizado.
2. Descripción de las herramientas de análisis forense utilizadas y del uso que se ha dado de las mismas con los resultados y su interpretación.
3. Descripción detallada de cada una de las fases del proceso de análisis forense realizado y herramienta usada en cada fase.
4. Tabla de esfuerzo y tareas realizadas por cada uno de los integrantes del equipo forense.

Fechas a tener en cuenta:
Entrega final: 16-05-2021
Presentación: 18-05-2021 & 26-05-2021