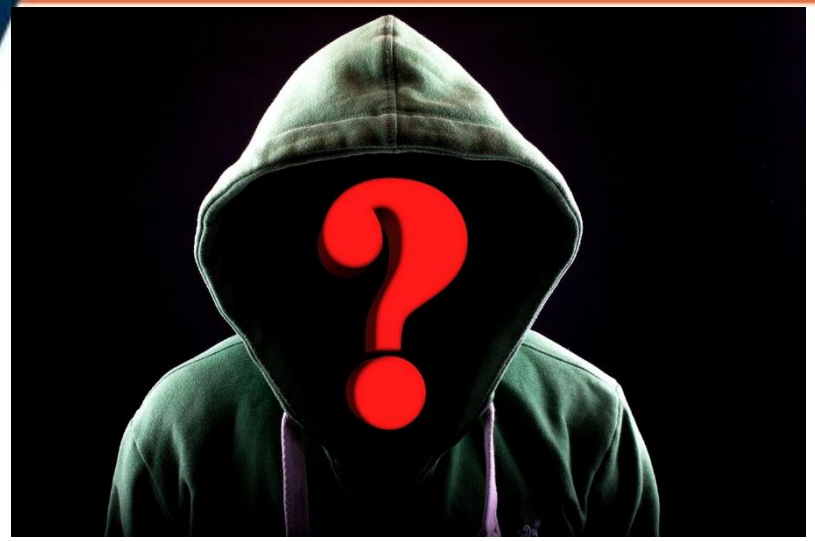
www.eysglobal.com

MÓDULO 1
TEMA 8:IDENTIFICACIÒN DE OBJETIVOS

IDENTIFICACIÒN DE OBJETIVOS

Si ya ha logrado averiguar cómo entraron en sus sistemas, ahora le toca saber quién o quiénes lo hicieron. Para este propósito le será de utilidad consultar nuevamente algunas evidencias volátiles que recopiló en las primeras fases, revise las conexiones que estaban abiertas, en qué puertos y qué direcciones IP las solicitaron, además busque entre las entradas a los logs de conexiones. También puede indagar entre los archivos borrados que recuperó por si el atacante eliminó alguna huella que quedaba en ellos.

IDENTIFICACIÒN DE OBJETIVOS



También puede emplear técnicas hacker, eso sí ¡DE FORMA ÉTICA!, para identificar a su atacante, piense que si este dejó ejecutándose en el equipo comprometido “un regalito” como una puerta trasera o un troyano, está claro que en el equipo del atacante deberán estar a la escucha esos programas y en los puertos correspondientes, bien esperando noticias o buscando nuevas víctimas. Aquí entra en juego nuevamente nuestro ordenador “conejillo de indias”.

IDENTIFICACIÓN DE OBJETIVOS

Otro aspecto que le interesaría averiguar es el perfil de sus atacantes, aunque sin entrar en detalles podrá encontrarse con los siguientes tipos de “tipos”:

IDENTIFICACIÓN DE OBJETIVOS

Evaluación del impacto causado al sistema

Para poder evaluar el impacto causado al sistema, el análisis forense le ofrece la posibilidad de investigar qué es lo que han hecho los atacantes una vez que accedieron a sus sistemas. Esto le permitirá evaluar el compromiso de sus equipos y realizar una estimación del impacto causado. Generalmente se pueden dar dos tipos de ataques:

INVESTIGACIÓN FORENSE, A INCIDENTES EN DISPOSITIVOS MÓVILES

Teniendo en cuenta que el uso del celular se ha convertido en una herramienta masiva de comunicación por sus facilidades en la portabilidad, servicios y bajos costos.

Los servicios que prestan los nuevos modelos de *Smartphone* (transmisión de vídeo, fotografía, GPS, Wi-fi, manejo de documentos, aplicaciones, entre otros) hacen que estos dispositivos se utilicen para algo más que hacer y recibir llamadas.

PROCEDIMIENTOS Y ESTÁNDARES PARA ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

En una investigación forense de carácter digital, se pueden seguir los patrones de una investigación forense de carácter estándar; sin embargo, teniendo en cuenta lo sensible de la evidencia en esta rama de investigación, se hace necesaria la aplicación de procedimientos más cuidadosos, desde el momento en que se recolecta la evidencia, hasta que se obtienen resultados posteriores a la investigación

PRESERVACIÓN DE LA EVIDENCIA:

Para preservar la evidencia es necesario mantener el dispositivo móvil con alimentación eléctrica para evitar cambios en la memoria volátil del equipo.

ANALISIS DE EVIDENCIA

En esta fase de la investigación, se pueden encontrar grandes cantidades de información. En esta fase, seguramente se requerirá que haga uso de un “*toolkit*” especializado, para que no se produzcan cambios en la evidencia original, y haga expedito el trabajo del investigador, para encontrar más fácilmente rastros y producir informes de forma clara y precisa.

PRESENTACIÓN DE UN INFORME FORENSE

Finalmente culmina la investigación y en este paso se presentan los resultados por parte del investigador sobre su búsqueda y análisis de los medios, lo que se encontró en la fase de análisis de la evidencia, así como la información puntual de los hechos previamente sugeridos para investigar y posibles responsables.