Práctica 1. Análisis forense de sistemas Linux.

Extracción de evidencias en caliente.

Como bien sabemos, hay dos tipos de análisis forense: en vivo y post mortem.

El primero ocurre cuando el sistema todavía está activo durante el análisis. En este escenario, es posible adquirir datos volátiles, como RAM, procesos en ejecución, conexiones a Internet y archivos temporales. Si se utiliza el cifrado de disco, con este análisis, el sistema de archivos se puede descifrar con la clave en caché. Por otro lado, este tipo de análisis requiere más experiencia y el sistema modifica constantemente sus datos, lo que puede perjudicar la admisibilidad judicial.

El analista tampoco debe confiar en ninguna herramienta proporcionada en el sistema, dado que puede haberse manipulado deliberadamente.

Objetivo:

- Realizar un script desde donde obtener las evidencias que se indican a continuación.

Materiales

- Cualquier distribución Linux con la que cuentes en tu sistema informático.

La idea es confeccionar un SCRIPT a medida que pueda ser ejecutado desde una unidad USB externa conectada a la computadora. Este script realizará funciones como copiar registros a la unidad USB externa y recopilar información como fecha, hora, usuarios registrados, árbol de procesos, tiempo de actividad del sistema, etc.

Algunas de las labores que debe realizar el:

- Copiar el contenido de las carpetas de "registro" (logs)
- Determinar la fecha en el sistema
- Determinar el nombre de host del sistema
- Información sobre la CPU del sistema
- Determinar los usuarios registrados en el sistema
- Determinar los procesos en ejecución en el sistema.
- Determinar el árbol de procesos (y argumentos)
- Determinar los discos / elementos montados

- Revisar la salida de la utilidad de particionado disco (particiones)
- Obtener estadísticas de uso de discos.
- Determinar las extensiones de kernel cargadas.
- Obtener los parámetros de arranque del kernel.
- Determinar el tiempo de actividad del sistema
- Determinar el entorno del sistema (versión de SO, kernel que se está usando y si es 32 o 64 bits)
- Determinar las variables entorno del sistema
- Determinar el uso de la memoria del proceso en ejecución
- Determinar los servicios en ejecución
- Determinar todos los módulos cargados
- Determinar los últimos inicios de sesión
- Revisar el contenido de usuarios (/etc/passwd)
- Revisar el contenido de grupos (/etc/group)
- Determinar el último inicio de sesión por usuario
- Determinar "quién" es el usuario que inició sesión
- Determinar con qué usuario se inició sesión (logname)
- Determinar grupos a los que pertenece el usuario (id)
-
- Revise .bash_history para cada usuario
- Determinar las conexiones de red actuales
- Compruebe adaptadores/interfaces de red.
- Determinar estadísticas de sockets
- Determinar la lista de puertos abiertos.
- Determine la tabla de enrutamiento

- Determinar tabla ARP
- Determinar la información de la interfaz de red
- Revisar los hosts permitidos
- Revisar los hosts denegados
- Obtener la resolución DNS estática.
- Obtener información de gateway y DNS dinámicos que se usen.
- Buscar ficheros que tengan activo los permisos SUID o GUID (2000 y 4000)