Presentación

Nombre: Moisés Ricardo

Apellido: Zabala Bueno

Matricula: 20200927

Materia: Seguridad Informática

Trabajo: Resumen ejecutivo #7

Docente: Ernesto Wachsmann

En la clase pasada continuamos viendo el tema de informática forense, estos son algunos de los subtemas que aprendí.

1. Particionado de discos: Se refiere al proceso de dividir un disco duro en secciones lógicas separadas conocidas como particiones. Cada partición funciona como si fuera un disco duro independiente, con su propio sistema de archivos y espacio de almacenamiento. El particionado de discos permite organizar y gestionar de manera más eficiente los datos en un disco duro, facilitando la instalación de varios sistemas operativos en una misma máquina o permitiendo separar los datos del sistema operativo de los datos personales.

2. Información hexadecimal en investigación forense: La información hexadecimal es una representación numérica de datos en base 16, que utiliza dígitos del 0 al 9 y letras de la A a la F para representar valores del 0 al 15. En la investigación forense, la información hexadecimal puede ser útil para examinar y analizar datos binarios, como archivos o registros de sistemas informáticos, ya que proporciona una representación legible de los datos en forma de cadenas de caracteres hexadecimales.

3. Offset: Es la medida de desplazamiento o distancia entre el inicio de un archivo o una estructura de datos y un punto de referencia específico. En términos más simples, el offset indica la ubicación relativa de un dato dentro de un archivo o una unidad de almacenamiento. El offset se expresa generalmente en bytes y se utiliza en diversos campos, como la programación, la investigación forense y la recuperación de datos.

4. Detectar incidentes: Hace referencia al proceso de identificar y reconocer actividades inusuales, anómalas o maliciosas en un entorno informático o de red que puedan indicar la presencia de un incidente de seguridad. Esto implica el monitoreo activo de los sistemas y redes, así como el análisis de registros y eventos en busca de patrones o comportamientos sospechosos.

5. Equipos encendidos vs. equipos apagados: En el contexto de la seguridad informática y la investigación forense, "equipos encendidos" se refiere a sistemas informáticos que están en funcionamiento y operativos, mientras que "equipos apagados" se refiere a sistemas que están desconectados o sin energía. Durante una investigación forense, los equipos encendidos pueden ser analizados de forma activa y en tiempo real, permitiendo la adquisición de datos en vivo y la recopilación de información sobre la actividad actual del sistema.

6. Recuperación de desastres por incidente o ciberdelito: Es el proceso de restaurar la operatividad normal de un sistema informático o una red después de un incidente grave de seguridad, como un ataque cibernético o un desastre natural. La recuperación de desastres generalmente implica la implementación de planes de continuidad del negocio y la colaboración entre equipos de seguridad, administradores de sistemas y expertos forenses para mitigar los efectos de los incidentes y restaurar la operatividad normal lo más rápido posible.