MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL

SERVICIO PÚBLICO DE EMPLEO ESTATAL
SEPE
SERVEI PÚBLIC D'OCUPACIÓ ESTATAL

MINISTERIO DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y DEPORTES

Generalitat de Catalunya
SOC Servei d'Ocupació de Catalunya

IRON HACK SPAIN

Gestión de incidentes de seguridad informática

IFCT0109 – Seguridad informática

MF0488_3 (90 horas)

Análisis forense informático

- Introducción
- Conceptos generales y objetivos del análisis forense
- Exposición del principio de Locard
- Guía para la recogida de evidencias electrónicas
- Guía para el análisis de las evidencias electrónicas recogidas, incluyendo el estudio de ficheros y directorios ocultos, información oculta de sistema y la recuperación de ficheros borrados
- Guía para la selección de las herramientas de análisis forense
- Resumen

Análisis forense informático

Introducción

La evolución de las Tecnologías de la Información y la Comunicación (TIC) proporciona a las organizaciones diversas herramientas para la gestión de la información, convirtiéndola en uno de sus principales activos.

Esto ha hecho que la información de empresas y organizaciones sea un objetivo atractivo para atacantes, quienes buscan generar intrusiones y usos indebidos con diversos propósitos.

Aunque se cuente con la cantidad adecuada de herramientas y sistemas de protección, siempre existe la posibilidad de que ocurra un incidente. Por tanto, es crucial detectar al responsable para reclamarle exigencias legales y económicas, si corresponde.

El análisis forense informático emerge como una herramienta fundamental en esta tarea, dedicándose a obtener evidencias en los incidentes para identificar al culpable de manera justificada.

Este capítulo detalla el concepto de informática forense, sus procesos y las mejores herramientas para lograr resultados efectivos, adaptados al sistema operativo utilizado.

Conceptos generales y objetivos del análisis forense

Introducción

El análisis forense, también conocido como ciencia forense digital, es una disciplina dentro de la seguridad informática que se encarga de analizar los incidentes de seguridad a posteriori. Su objetivo principal es reconstruir los hechos para responder preguntas como:

- ¿Quién ha sido el atacante?
- ¿Cómo se ha producido el incidente de seguridad?
- ¿Cuáles han sido las vulnerabilidades explotadas?
- ¿Cuáles fueron las acciones del intruso cuando consiguió acceder al sistema?

Importancia y crecimiento del análisis forense

El Instituto Nacional de Ciberseguridad de España (INCIBE) gestionó más de 118.000 incidentes de ciberseguridad durante 2022, lo que representa un aumento del 9% en comparación con el año anterior.

Del total de incidentes, más de 110.100 afectaron a ciudadanos y empresas, 546 a operadores estratégicos y 7.980 a la Red Académica y de Investigación Española (RedIRIS). En cuanto a los incidentes más frecuentes, destacan el phishing con casi 17.000 incidentes, seguido del malware con más de 14.000 y, por último, el ransomware, con casi 450 incidentes.

Conceptos generales y objetivos del análisis forense

Este crecimiento de la incidencia se debe a diversos factores, como:

- El auge del cibercrimen como actividad ilícita altamente rentable.
- La aparición de plataformas MaaS (Malware as a Service) que facilitan la ejecución de ciberataques.
- La falta de formación en ciberseguridad entre los usuarios, que los convierte en el eslabón más débil de la cadena.

Ante este panorama, es crucial que las empresas inviertan en:

- Herramientas de análisis forense para identificar y combatir las amenazas.
- Formación en ciberseguridad para sus empleados, con el objetivo de concienciarlos sobre los riesgos y las medidas de prevención.

Conceptos generales y objetivos del análisis forense

Metodología del análisis forense informático

La informática forense, también conocida como ciencia forense digital, es una disciplina que se encarga de capturar, procesar e investigar la información de los sistemas informáticos en búsqueda de evidencias.

Objetivos: El objetivo principal de la informática forense es reunir pruebas digitales que puedan ser utilizadas en un proceso legal. Entre sus objetivos secundarios se encuentran:

- Compensar los daños causados por los intrusos.
- Perseguir y aplicar medidas judiciales a los atacantes.
- Crear e implantar medidas para prevenir incidentes futuros similares.

Usos: La informática forense tiene una amplia gama de aplicaciones, incluyendo:

- Persecución criminal: obtener evidencias que incriminen a los culpables de delitos como fraudes financieros, tráfico de drogas, pornografía infantil, etc.
- Litigación civil: aportar pruebas en la resolución de conflictos como divorcios, fraudes, problemas de discriminación, etc.
- Investigación de seguros: detectar casos de fraude a compañías de seguros.
- Mantenimiento de la ley: realizar búsquedas iniciales en investigaciones con órdenes judiciales.
- Usuario final: recuperar archivos eliminados, encriptar archivos y datos, rastrear correos electrónicos, etc.
- Organizaciones y temas corporativos: obtener evidencias y perseguir delitos relacionados con el uso malintencionado o la apropiación de información confidencial, así como el espionaje industrial.

Conceptos generales y objetivos del análisis forense

Metodología del análisis forense informático

El análisis forense informático es una disciplina que se encarga de identificar, preservar, analizar y presentar evidencias digitales en un contexto legal.

Fases del análisis forense

Fase 1: Estudio preliminar.

- Se realiza un estudio inicial para identificar las fuentes de información relevantes.
- Se realizan entrevistas y se revisa la documentación inicial del incidente.

Fase 2: Adquisición de datos y recopilación de evidencias

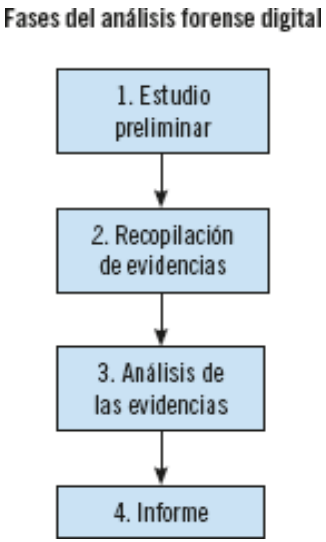
- Se recopilan y obtienen los distintos tipos de evidencias e información fundamental para la investigación.
- Se recomienda realizar copias de los dispositivos implicados para su análisis posterior.

Fase 3: Análisis e investigación de las evidencias

- Se realiza un análisis exhaustivo de las evidencias para reconstruir la línea temporal del ataque.
- Se busca identificar al atacante y determinar el origen del ataque.

Fase 4: Confirmación de las pruebas y elaboración del informe

- Se documenta todo el procedimiento en un informe.
- El informe se remite a la dirección o responsables de seguridad de la organización.
- En caso de delito digital, el informe puede ser utilizado como prueba legal.



Conceptos generales y objetivos del análisis forense

Metodología del análisis forense informático

Las herramientas de análisis forense digital permiten:

- Automatizar tareas repetitivas y tediosas.
- Agilizar el proceso de análisis.
- Encontrar información que podría pasar desapercibida.
- Presentar las pruebas de forma clara y concisa.

Las herramientas de análisis forense digital proporcionan los siguientes beneficios:

- Precisión y confiabilidad en los resultados.
- Reducción del tiempo de análisis.
- Mejora de la eficiencia en la gestión de incidentes.
- Mayor capacidad para identificar y combatir las amenazas.

Exposición del principio de Locard

Introducción

La ciencia forense se fundamenta en principios y técnicas para investigar cualquier delito criminal. En otras palabras, esta ciencia incluye los principios y técnicas que se utilizarán para identificar, recuperar, reconstruir y analizar las evidencias que forman parte de un delito.

En cuanto a los principios, todo procedimiento de recolección y análisis de evidencias debe tener en cuenta y llevar a cabo los siguientes aspectos:

- Recogida y examen de las huellas dactilares y ADN.
- Recuperación de los documentos de los dispositivos dañados.
- Realización de copias exactas de las evidencias digitales detectadas.
- Generación de una huella digital de los textos y evidencias para asegurarse que no se modifican.
- Utilización de la firma digital para confirmar la autenticidad de los documentos y mantener la cadena de custodia de evidencias.

La cadena de custodia de una evidencia es un procedimiento controlado de recolección y análisis de evidencias que tiene como finalidad la preservación de su integridad, evitando que su manejo no provoque vicios o alteraciones.

Exposición del principio de Locard

Introducción

Los forenses en general, y más concretamente los informáticos, se encargan de aplicar su conocimiento para ayudar a los investigadores a encontrar evidencias y pistas y así poder reconstruir el crimen.

Utilizando un método científico crean hipótesis sobre lo que ha sucedido mediante el análisis de las evidencias, pruebas adicionales y una serie de controles que confirmen o invaliden las hipótesis formuladas.

Los forenses informáticos no pueden conocer todo el pasado, simplemente pueden formular hipótesis y teorías de qué ha podido ocurrir en función de la información limitada de la que se dispone.

El principio de Locard, también conocido como principio de intercambio, establece que cada contacto entre dos objetos deja una traza. Esto significa que en la escena del crimen, el criminal, la víctima y el entorno intercambian material, como pelos, fibras, huellas dactilares o ADN.

Los forenses utilizan este principio para buscar y analizar las evidencias que puedan ayudar a identificar al culpable o a reconstruir los hechos del crimen.

Exposición del principio de Locard

El principio de intercambio o transferencia de Locard

Edmond Locard, pionero en criminología, enunció el principio de intercambio o transferencia de Locard:

Siempre que dos objetos entran en contacto, hay una transferencia de material de uno al otro.

En la escena del crimen, esto significa que:

- El criminal deja rastros (pelos, sudor, huellas dactilares) en la escena o en la víctima.
- El criminal se lleva algo consigo (barro, olores, fibras) de la escena del crimen.

Cada contacto deja un rastro

Tipos de evidencias físicas:

- Evidencias transitorias: temperatura, olor (desaparecen en poco tiempo).
- Evidencias de curso o patrones: muebles cambiados de sitio, trayectoria de una bala.
- Evidencias condicionales: ventanas abiertas o cerradas, televisión encendida/apagada.
- Evidencias transferidas: pelos, fibras, huellas dactilares.

El análisis de estas evidencias permite:

- Relacionar al criminal con el crimen.
- Reconstruir los hechos del crimen.

El principio de Locard es una herramienta fundamental en la investigación criminal.

Exposición del principio de Locard

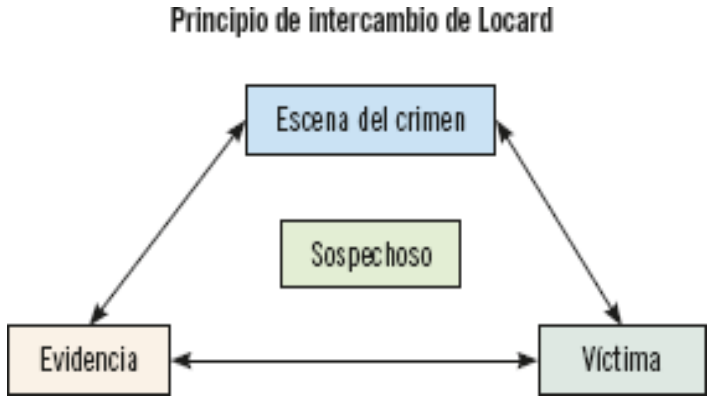
El principio de intercambio o transferencia de Locard

Se basa en tres ideas:

- El criminal se lleva rastros de la escena y la víctima.
- El criminal deja rastros en la víctima y viceversa.
- El criminal deja rastros en la escena del crimen.

El objetivo es establecer relaciones entre:

- La víctima
- El sospechoso
- La evidencia
- La escena del crimen



La relación entre estos elementos es fundamental para resolver el crimen.

Tipos de transferencia de evidencia:

- Transferencia directa: sin intermediarios.
- Transferencia indirecta: con un paso intermedio.

El éxito de la investigación depende de descubrir la relación entre los elementos del crimen. El principio de intercambio de Locard se basa en el concepto de relación.

Exposición del principio de Locard

Aplicación del principio de Locard al análisis forense digital

El principio de Locard se aplica al análisis forense digital:

- El atacante deja una "huella digital" en el sitio atacado.
- El atacante se lleva algo consigo.

El análisis de las huellas digitales y las evidencias permite:

- Reconstruir lo que ha ocurrido.
- Relacionar al atacante con la víctima y la escena del crimen (equipos o dispositivos afectados).

Preguntas clave:

- ¿Cómo ha sucedido?
- ¿Dónde ha sucedido?
- ¿Qué se ha afectado?

Detección y relación de las evidencias digitales:

Quién fue la última persona que escribió en un archivo relacionado con una intrusión.
Análisis de las alertas emitidas por los dispositivos y equipos monitorizados.
Histórico de las conexiones realizadas.
Trazado de ruta de las conexiones realizadas.
Relación entre el atacante, la víctima y el equipo: Archivos utilizados y/o modificados por ambos.

Exposición del principio de Locard

Aplicación del principio de Locard al análisis forense digital

Evidencia digital:

- Cualquier documento, fichero, registro, etc. en un soporte informático o digital.
- Ejemplos: documentos de ofimática, imágenes, BBDD, registros de actividad, comunicaciones digitales.

Las evidencias digitales son:

- Pilares de la informática forense.
- De gran valor en las investigaciones.
- Aportables en procesos judiciales.

La recopilación de evidencias electrónicas es una fase crucial del análisis forense digital. Si se realiza mal, todo el análisis posterior puede invalidarse, con información incorrecta y resultados erróneos.

Por lo tanto, la recogida de evidencias electrónicas debe ser meticulosa:

- No se debe realizar ningún cambio en las evidencias.
- Se deben tener en cuenta conceptos clave:
  - Evidencias volátiles y no volátiles.
  - Etiquetado de evidencias.
  - Cadena de custodia.
  - Ficheros y directorios ocultos.
  - Recuperación de ficheros borrados.

Guía para la recogida de evidencias electrónicas

Evidencias volátiles y no volátiles.

Clasificación:

- Evidencias volátiles: se pierden al apagar el equipo (memoria, procesos).
- Evidencias no volátiles: se almacenan en el sistema de archivos (aplicaciones, configuraciones).

Decisión crucial: apagar o no el equipo.

- Apagarlo elimina las evidencias volátiles.
- Mantenerlo encendido puede comprometer la seguridad del equipo.

Recomendación: preservar las evidencias volátiles primero.

Orden de preservación:

- Registros, memoria caché, memoria de periféricos
- Memoria física
- Estado de las conexiones de red
- Ficheros temporales del sistema
- Procesos en ejecución
- Discos duros
- Archivos de backups
- Registros y datos de monitorización remotos
- Configuración física y topología de la red
- CD-ROM, impresiones

Las evidencias volátiles son cruciales en el análisis forense digital. Se recomienda preservarlas primero siguiendo el orden de preservación.

La decisión de apagar o no el equipo debe tomarse con cuidado, considerando la seguridad y la volatilidad de las pruebas.

Guía para la recogida de evidencias electrónicas

Etiquetado de Evidencias

Requisitos para la admisión de evidencias:

- Conservación del estado original o lo más cercano posible al estado en el que se encontraron.
- Copia exacta de la evidencia original. Sobre las copias se realizarán los trabajos de análisis e investigación.
- Medios estériles para las copias. Medios que no hayan contenido datos previamente.
- Etiquetado y documentación en la cadena de custodia. Cada acción realizada debe documentarse con detalle.
- Documentación de las acciones con firmas digitales. Garantizando la autoría de las acciones.

Categorías de las evidencias digitales:

- Registros generados por ordenador: inalterables por el usuario (logs).
- Registros almacenados por ordenadores: generados por el usuario (documentos).
- Registros híbridos: combinan acciones del usuario y del equipo.
- Registros de cada servidor: sistema y programas en ejecución.
- Registros de tráfico de red: actividad de red del equipo.
- Registros de aplicación: acceso de usuarios, errores y acciones.

Guía para la recogida de evidencias electrónicas

Etiquetado de Evidencias

Criterios de admisibilidad de las evidencias electrónicas:

Criterios de admisibilidad de evidencias electrónicas	
Autenticidad	La evidencia debe haber sido generada y registrada en la escena del crimen y debe mostrar que los medios utilizados no se han modificado.
Confiabilidad	Las evidencias serán confiables si el sistema que las produjo no ha sido violado y estaba funcionando correctamente cuando se recibió, almacenó o generó la prueba.
Completitud o suficiencia	La evidencia debe estar completa, tiene que haberse mantenido su integridad.
Respeto por las leyes	Las técnicas de recolección y tratamiento de la evidencia deben cumplir las normativas legales vigentes en el ordenamiento jurídico.

Guía para la recogida de evidencias electrónicas

Cadena de custodia

La cadena de custodia es un conjunto de procedimientos y documentos que documentan el manejo de las evidencias desde su recolección hasta su análisis final. Su objetivo es garantizar la integridad y autenticidad de las pruebas para evitar errores en los resultados del análisis.

Importancia: La cadena de custodia es fundamental en todas las fases del análisis forense digital, desde la recolección hasta la emisión del informe final. Es especialmente importante desde un punto de vista legal, ya que la pérdida de integridad o la alteración de datos en las pruebas puede invalidarlas en un proceso judicial.

Requisitos:

- Métodos adecuados para la identificación, documentación, etiquetado y almacenamiento de las evidencias.
- Protección de las evidencias de factores ambientales.
- Manejo de las evidencias por profesionales con conocimientos especializados.
- Documentación precisa de cada acción realizada sobre las evidencias.

Objetivos:

- Reducir al mínimo la cantidad de personas que manipulan las evidencias.
- Mantener la identidad de las personas involucradas en el proceso.
- Asegurar la seguridad de las evidencias durante su almacenamiento.
- Registrar el historial de manejo de las evidencias para identificar a los responsables en cada momento.

Guía para la recogida de evidencias electrónicas

Ficheros y directorios ocultos

Importancia en la Recolección de Evidencias: Los ficheros y directorios ocultos pueden contener información crucial para una investigación forense digital. Los atacantes a menudo los utilizan para ocultar su presencia y actividad en un sistema.

Localización: Es fundamental conocer la ubicación de los archivos y directorios ocultos para poder examinarlos y determinar si contienen evidencias relevantes.

Existen diferentes métodos para buscar archivos y directorios ocultos:

- Utilizar herramientas de análisis forense digital para automatizar la búsqueda y análisis de archivos ocultos.
- Algunos sistemas operativos tienen comandos específicos para mostrar archivos ocultos.
- Exploradores de archivos con opciones para mostrar archivos ocultos: Algunos exploradores de archivos permiten activar la visualización de archivos ocultos.

Tipos de archivos ocultos:

- Archivos del sistema: Son archivos utilizados por el sistema operativo y no suelen ser relevantes para una investigación.
- Archivos de configuración: Contienen información sobre la configuración de aplicaciones o del sistema.
- Archivos temporales: Son archivos creados por las aplicaciones y que se eliminan automáticamente.
- Archivos ocultos por el usuario: Son archivos que el usuario ha ocultado deliberadamente.

Guía para la recogida de evidencias electrónicas

Ficheros y directorios ocultos

Análisis:

Es importante analizar los archivos y directorios ocultos para determinar si contienen evidencias relevantes. Algunos indicadores de que un archivo puede ser una evidencia incluyen:

- Nombres inusuales o sospechosos.
- Modificaciones recientes en la fecha o hora del archivo.
- Contenido que coincide con las características de un ataque conocido.

Información oculta del sistema

La información oculta del sistema puede ser crucial para una investigación forense digital. Esta información puede incluir:

- Parámetros del sistema: Configuración del sistema operativo, software instalado, usuarios y grupos, etc.
- Información de eventos: Registros de eventos del sistema, registros de aplicaciones, etc.
- Información de red: Registros de conexiones de red, historial de navegación web, etc.

Existen herramientas especializadas que permiten localizar y analizar la información oculta del sistema. Estas herramientas pueden: (Sysinternals Suite)

- Extraer la información oculta del sistema.
- Analizar la información para detectar anomalías o modificaciones sospechosas.
- Identificar posibles evidencias digitales.

Guía para la recogida de evidencias electrónicas

Recuperación de archivos borrados:

Existen herramientas que permiten recuperar archivos borrados del disco duro. Estas herramientas funcionan buscando archivos marcados como espacio disponible y restaurando su contenido.

Buscar en la papelera de reciclaje. El primer paso es buscar el archivo en la papelera de reciclaje. Si el archivo está en la papelera de reciclaje, puedes restaurarlo fácilmente haciendo clic derecho sobre él y seleccionando "Restaurar".

Usar una herramienta de recuperación de archivos. Estas herramientas funcionan buscando archivos que han sido marcados como espacio disponible en el disco duro.

Hay muchos tipos diferentes de herramientas de recuperación de archivos disponibles. Algunas son gratuitas, mientras que otras requieren una licencia.

Guía para la recogida de evidencias electrónicas

Recuperación de archivos borrados:

Consejos para recuperar archivos borrados.

- Deja de usar el dispositivo inmediatamente después de eliminar el archivo. Cuanto más uses el dispositivo, mayor será la probabilidad de que los datos del archivo borrado se sobrescriban y se pierdan para siempre.
- Descarga e instala la herramienta de recuperación de archivos en un disco duro diferente al que contiene el archivo borrado. Esto ayudará a evitar que la herramienta de recuperación de archivos sobrescriba los datos del archivo borrado.
- Escanea el dispositivo con la herramienta de recuperación de archivos. La herramienta de recuperación de archivos escaneará el dispositivo en busca de archivos que puedan ser recuperados.
- Previsualiza los archivos encontrados. La mayoría de las herramientas de recuperación de archivos te permiten previsualizar los archivos encontrados antes de restaurarlos. Esto te ayudará a asegurarte de que estás restaurando el archivo correcto.
- Restaura el archivo. Una vez que hayas encontrado el archivo que deseas recuperar, puedes restaurarlo a su ubicación original o a una ubicación diferente.

Si no puedes recuperar el archivo con una herramienta de recuperación de archivos, es posible que el archivo se haya perdido para siempre. En este caso, puedes intentar contactar con un servicio profesional de recuperación de datos.

Guía para el análisis de las evidencias electrónicas recogidas, incluyendo el estudio de ficheros y directorios ocultos, información oculta de sistema y la recuperación de ficheros borrados

Introducción

El objetivo es reconstruir y determinar la secuencia temporal de los hechos ocurridos, identificar al responsable, el método de ataque, el objetivo y las circunstancias del mismo.

Preparación del Entorno de Trabajo:
No tocar los dispositivos originales. Trabajar con copias de las evidencias.

Preparar dos estaciones de trabajo:

- Estación 1:
  - Un disco duro con el sistema operativo para el análisis.
  - Otro disco duro con la imagen del disco duro del equipo atacado.
- Estación 2:
  - Sistema operativo configurado exactamente igual que el equipo atacado.

Guía para el análisis de las evidencias electrónicas recogidas, incluyendo el estudio de ficheros y directorios ocultos, información oculta de sistema y la recuperación de ficheros borrados

Reconstrucción de la Secuencia Temporal del Ataque:

- Análisis de la información de los ficheros:
- Tamaño y tipo de fichero.
- Usuarios y grupos.
- Permisos de acceso.
- Estado de borrado.
- Ruta completa.
- Marcas de tiempo: creación, modificación, borrado y acceso.

Objetivo:

- Llegar al origen del ataque.
- Localizar al atacante.
- Conocer los pasos del ataque.
- Obtener pruebas para medidas legales.

Búsqueda de Ficheros y Directorios:

- Visibles y ocultos.
- Creados, modificados o eliminados recientemente.
- En rutas poco comunes.
- Prestar especial atención a archivos ocultos y eliminados.
- Recuperar archivos eliminados en la medida de lo posible.
- Analizar archivos ocultos e información oculta del sistema.

Guía para el análisis de las evidencias electrónicas recogidas, incluyendo el estudio de ficheros y directorios ocultos, información oculta de sistema y la recuperación de ficheros borrados

Determinación de cómo se realizó el ataque

Una vez establecida la secuencia temporal del ataque, el siguiente paso es determinar cómo se llevó a cabo. Esto implica:

Identificar el punto de entrada:

Vulnerabilidades explotadas: Investigar las vulnerabilidades del sistema que el atacante pudo aprovechar para acceder.
Fallas de administración: Analizar si el acceso se logró por errores en la gestión del sistema.
Herramientas utilizadas:
Consultas y análisis de archivos: Revisar logs, registros, cuentas de usuario y otros archivos para identificar las herramientas del atacante.

Análisis de Vulnerabilidades:

1. Tipos de vulnerabilidades:
   - Software: Errores en el código de programas o aplicaciones.
   - Hardware: Defectos en los componentes físicos del sistema.
   - Configuración: Errores en la configuración del sistema o de las aplicaciones.
2. Recursos para la identificación de vulnerabilidades:
   - Bases de datos de vulnerabilidades: CVE Details, NVD.
   - Herramientas de escaneo de vulnerabilidades: Nessus, OpenVAS.

Guía para el análisis de las evidencias electrónicas recogidas, incluyendo el estudio de ficheros y directorios ocultos, información oculta de sistema y la recuperación de ficheros borrados

Determinación de cómo se realizó el ataque

Análisis de Herramientas del Atacante:

1. Tipos de herramientas:
   - Malware: Software malicioso que infecta el sistema.
   - Exploits: Programas que aprovechan vulnerabilidades específicas.
   - Herramientas de hacking: Software para obtener acceso no autorizado a sistemas.
2. Técnicas de análisis:
   - Análisis de logs: Buscar entradas que indiquen la actividad del atacante.
   - Análisis de archivos: Buscar archivos sospechosos o modificados por el atacante.
   - Análisis de la memoria: Buscar rastros de herramientas en la memoria del sistema.

Recursos para la identificación de herramientas:

- Bases de datos de herramientas de hacking: VirusTotal, ThreatExpert.
- Informes de inteligencia sobre amenazas: MITRE ATT&CK.

Guía para el análisis de las evidencias electrónicas recogidas, incluyendo el estudio de ficheros y directorios ocultos, información oculta de sistema y la recuperación de ficheros borrados

Identificación del atacante o atacantes

La identificación del atacante o atacantes es crucial, especialmente si la organización desea tomar acciones legales.

Métodos de identificación:

- Análisis de la dirección IP del atacante: Revisar los registros de conexiones de red.
- Análisis de las evidencias volátiles: Buscar información sobre conexiones fallidas, archivos temporales, archivos eliminados, información sobre correos electrónicos, etc.
- Análisis de otras evidencias: Logs del sistema, registros de aplicaciones, información de cuentas de usuario.

Herramientas para la identificación:

- Herramientas de análisis de logs: Splunk, ELK Stack.
- Herramientas de análisis de malware: VirusTotal, Cuckoo Sandbox.
- Herramientas de análisis de redes: Wireshark, Nmap.

Consideraciones:

La identificación del atacante puede ser compleja y no siempre es posible obtener resultados concluyentes.

Guía para el análisis de las evidencias electrónicas recogidas, incluyendo el estudio de ficheros y directorios ocultos, información oculta de sistema y la recuperación de ficheros borrados

Evaluación del Impacto Causado

Objetivos:

- Determinar qué han hecho los atacantes una vez han accedido al sistema.
- Evaluar si el ataque ha comprometido la información de los equipos.
- Determinar el impacto real y potencial del ataque.

Tipos de ataques:

- Activos: Modifican la información del sistema, afectando su funcionamiento.
- Pasivos: Obtienen información del sistema sin modificarlo.

Metodología de evaluación:

- Análisis de las evidencias: Buscar información sobre las acciones del atacante, los datos a los que ha accedido y los daños causados.
- Análisis de los sistemas afectados: Evaluar el impacto del ataque en el funcionamiento de los sistemas.
- Análisis del impacto en la información: Evaluar si la información confidencial ha sido comprometida.

Herramientas para la evaluación:

- Herramientas de análisis forense digital: EnCase, FTK Imager.
- Herramientas de análisis de vulnerabilidades: Nessus, OpenVAS.
- Herramientas de análisis de riesgos: RiskWatch, MegaCorp.

Guía para el análisis de las evidencias electrónicas recogidas, incluyendo el estudio de ficheros y directorios ocultos, información oculta de sistema y la recuperación de ficheros borrados

Documentación del Ataque

La documentación precisa y completa del ataque es fundamental para:

- Garantizar la eficiencia del análisis forense.
- Disminuir las posibilidades de error.
- Facilitar la consulta del histórico de incidentes.
- Demostrar la existencia del ataque en caso de acciones legales.

Información a documentar:

- Cadena de custodia de las evidencias.
- Identificación de los equipos, componentes y dispositivos afectados.
- Ataques tipificados.
- Metodología de recolección y almacenamiento de las evidencias.
- Resultados del análisis forense.

Herramientas para la documentación:

- Formularios predefinidos.
- Herramientas de gestión de incidentes.
- Sistemas de gestión de tickets.

Guía para el análisis de las evidencias electrónicas recogidas, incluyendo el estudio de ficheros y directorios ocultos, información oculta de sistema y la recuperación de ficheros borrados

Documentación del Ataque

Consideraciones:

- La documentación debe ser clara, concisa y precisa.
- Debe ser realizada por personal con formación en análisis forense digital.
- Debe ser actualizada a medida que se avanza en la investigación del ataque.

Recomendaciones:

- Establecer un protocolo de actuación para la documentación de los ataques.
- Utilizar formularios predefinidos para facilitar la recopilación de información.
- Almacenar la documentación de forma segura y accesible.
- Capacitar al personal en la importancia de la documentación de los ataques.

Guía para el análisis de las evidencias electrónicas recogidas, incluyendo el estudio de ficheros y directorios ocultos, información oculta de sistema y la recuperación de ficheros borrados

Elaboración del informe

Una vez finalizado el análisis de las evidencias y obtenidos los detalles de los ataques, se debe elaborar un informe que documente el proceso y los hallazgos.

Contenido del Informe:

- Antecedentes del ataque: Fecha, hora, tipo de ataque, sistemas afectados, etc.
- Recolección previa de datos y evidencias: Descripción de las fuentes de información y las técnicas de recolección utilizadas.
- Descripción de la evidencia: Tipo de evidencia, ubicación, formato, etc.
- Herramientas utilizadas en el análisis: Software y hardware utilizados para analizar las evidencias.
- Análisis de la evidencia: Resultados del análisis de cada evidencia, incluyendo información sobre los equipos y dispositivos analizados.
- Descripción de los hallazgos encontrados: Huellas del ataque, vulnerabilidades explotadas, origen del ataque, alcance, etc.
- Cronología del ataque: Secuencia de eventos del ataque.
- Conclusiones: Resumen de los hallazgos y su impacto en la organización.
- Recomendaciones: Medidas para prevenir futuros ataques y mitigar el impacto del ataque actual.

Guía para el análisis de las evidencias electrónicas recogidas, incluyendo el estudio de ficheros y directorios ocultos, información oculta de sistema y la recuperación de ficheros borrados

Elaboración del informe

Estructura del Informe:

- Introducción: Resumen ejecutivo del informe.
- Metodología: Descripción de las técnicas y herramientas utilizadas.
- Resultados: Presentación detallada de los hallazgos.
- Conclusiones: Interpretación de los resultados y su impacto.
- Recomendaciones: Medidas a tomar para prevenir futuros ataques.
- Anexos: Documentación adicional, como imágenes, capturas de pantalla, etc.

Consideraciones:

- El informe debe ser claro, conciso y preciso.
- Debe estar escrito en un lenguaje comprensible para la audiencia objetivo.
- Debe ser objetivo e imparcial.
- Debe ser presentado de forma profesional.

Recomendaciones:

- Utilizar una plantilla predefinida para la elaboración del informe.
- Revisar y corregir el informe cuidadosamente antes de su presentación.
- Solicitar la revisión de un experto en análisis forense digital.

Guía para el análisis de las evidencias electrónicas recogidas, incluyendo el estudio de ficheros y directorios ocultos, información oculta de sistema y la recuperación de ficheros borrados

Elaboración del informe

Preservación de la Cadena de Custodia:

Es fundamental preservar la cadena de custodia en todas las fases del análisis de las evidencias. Esto significa mantener un registro de:

- Quién ha tenido acceso a la evidencia.
- Qué se ha hecho con la evidencia.
- Cuándo se ha hecho algo con la evidencia.
- La preservación de la cadena de custodia es esencial para garantizar la integridad de las evidencias y la admisibilidad de los resultados del análisis en un proceso legal

Guía para la selección de las herramientas de análisis forense

Introducción

Los atacantes continuamente emplean técnicas más sofisticadas en sus ataques, haciendo que la detección y análisis de evidencias sea una tarea tediosa para los investigadores que no disponen de herramientas específicas. La elección de la herramienta adecuada dependerá del sistema operativo, presupuesto y preferencias entre software comercial y libre.

Criterios de selección:

- Sistema operativo: Algunas herramientas solo funcionan en sistemas operativos específicos (Windows, macOS, Linux).
- Costo: Software comercial vs. gratuito.
- Funcionalidades: Análisis de discos duros, recuperación de archivos, análisis de archivos, búsqueda de archivos, generación de informes, etc.
- Facilidad de uso: Interfaz intuitiva y curva de aprendizaje.
- Compatibilidad con formatos de archivos: Soporte para diferentes tipos de archivos y sistemas de archivos.
- Soporte y actualizaciones: Disponibilidad de actualizaciones, documentación y comunidad de usuarios.

Guía para la selección de las herramientas de análisis forense

Herramientas destacadas:

EnCase:

- Software comercial de pago.
- Análisis de medios de comunicación digitales.
- Recopilación de datos, recuperación de archivos, análisis y búsqueda de archivos.
- Versión en español disponible.
- Limitaciones: Alto costo, no es de código abierto.

The Sleuth Kit y Autopsy:

- Conjunto de herramientas forenses gratuitas.
- Funciona en Windows, macOS y Linux.
- Análisis de datos de evidencias de unidades de disco.
- Acceso a archivos eliminados, generación de línea temporal de actividad, creación de informes y notas.
- Ventajas: Gratis, código abierto, multiplataforma, amplia gama de funcionalidades.
- Limitaciones: Interfaz menos intuitiva que EnCase, requiere mayor conocimiento técnico.

Guía para la selección de las herramientas de análisis forense

Otras herramientas:

- FTK Imager: Herramienta gratuita para la creación de imágenes de disco.
- Wireshark: Analizador de redes para la captura y análisis de tráfico de red.
- Volatility Framework: Análisis de memoria volátil en sistemas Windows y Linux.
- Binja: Desensamblador de código binario para la identificación de malware.

Recomendaciones:

- Evaluar las necesidades específicas de la investigación.
- Probar diferentes herramientas antes de tomar una decisión.
- Considerar la relación costo-beneficio.
- Buscar herramientas con una comunidad activa de usuarios.
- Mantenerse actualizado con las últimas versiones y herramientas disponibles.

Resumen

Introducción:

El aumento de los incidentes de seguridad ha impulsado el desarrollo del análisis forense digital, una disciplina dentro de la seguridad informática que se encarga de analizar a posteriori los incidentes de seguridad y los delitos digitales.

Objetivos:

- Reconstruir los hechos del incidente.
- Detectar al atacante.
- Averiguar cómo se accedió a los equipos.

Aplicaciones:

- Aportar pruebas en investigaciones de fraude.
- Realizar investigaciones con orden judicial.
- Entre otras.

Metodología:

- Estudio preliminar.
- Recopilación de evidencias.
- Análisis de evidencias.
- Elaboración de informes con los resultados.

Cadena de custodia:

- Es fundamental para mantener la integridad de las evidencias.
- Permite descubrir el origen del ataque y localizar al atacante.

Resumen

Herramientas:

- Existen herramientas de pago, gratuitas y para varios sistemas operativos.
- Ayudan a recopilar evidencias y detectar al culpable.

Conclusión:

El análisis forense digital es una herramienta crucial para combatir los delitos informáticos. La correcta aplicación de la metodología y el uso de las herramientas adecuadas pueden ayudar a identificar a los responsables y llevarlos ante la justicia.