www.eysglobal.com

MÓDULO 1

TEMA 19:HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE PARTE 2

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

Técnicas :

para un análisis forense exitoso. Esta será la estructura del presente capítulo. Se analizarán las siguientes fases:

1. Asegurar la escena
2. Identificar y recolectar las evidencias
3. Preservar las evidencias
4. Analizar las evidencias obtenidas
5. Redactar informes sobre los resultados

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

En cada una de las técnicas se darán las mejores recomendaciones y los pasos más habituales para no cometer ningún error. Obviamente no todos los análisis forenses se producen ante hechos criminales, y por lo tanto no todos van a acabar en manos de jueces y abogados. Como ya se ha ido indicando el análisis forense tiene muchas más finalidades, puede ser simplemente una auditoría, reconstruir un sistema dañado, un proceso de aprendizaje o la toma de medidas para que no se reproduzca un determinado problema.

En todo caso, la finalidad judicial parece ser la más restrictiva y con la que más problemas nos podemos encontrar, así pues, será esta la que presente más dificultades y con la que se tenga que tener más prudencia.

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

ASEGURAR LA ESCENA

Tal vez esta técnica tenga su máxima expresión en casos criminales. No obstante, quizás con menor rigor, es importante en cualquier análisis forense. Es importante recalcar que el investigador no sólo se tiene que centrar en un análisis técnico del equipo o equipos implicados en el incidente, también debe asegurarse que la escena donde se ha producido el incidente no haya sido alterada, desde el descubrimiento del mismo hasta el inicio de su análisis. Todos los implicados en la investigación deben ser conscientes que cualquier acto que lleven a cabo puede comportar unas consecuencias posteriores, así no deben hacer nada que no tengan claro y que pueda alterar los resultados. Lo mejor es trabajar consensuando la actuación y anotando todo lo realizado en la escena.

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

IDENTIFICACIÓN Y RECOLECCIÓN DE EVIDENCIAS: Para un mayor detalle la segunda técnica se subdividirá en dos apartados, por un lado la parte relativa a la identificación de las evidencias y por otro lado la parte relativa a la recolección de las mismas

Identificación de las evidencias → **Recolección de las evidencias**

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

En la Identificación de las evidencias Llegados a este punto hay que tener en cuenta una serie de principios acerca de la identificación de las evidencias y más específicamente sobre la volatilidad de las mismas. Es vital conocer qué datos son más o menos volátiles, identificarlos correctamente y posteriormente proceder a su recolección. Entendemos por volatilidad de los datos el período de tiempo en el que estarán accesibles en el equipo. Por lo tanto, se deberán recolectar previamente aquellas pruebas más volátiles

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

Finalmente, y no menos importante, hay que recalcar unas indicaciones, a caballo entre la identificación y la recolección de las pruebas relacionadas con la privacidad. Hemos repasado en un capítulo especial la legislación legal vigente sobre este aspecto.

Es importante considerar las pautas de la empresa en cuanto a privacidad. Se suele solicitar autorización por escrito para efectuar la recolección de evidencias. Esto es muy importante ya que en ocasiones se pueden manejar datos confidenciales o incluso que la disponibilidad de los servicios quede afectada. Además, a menos que haya indicios suficientes y fundamentados no se deben recopilar datos de lugares a los que no se accede normalmente, como por ejemplo ficheros con datos personales.

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

Recolección de evidencias
Tras la correcta identificación de las evidencias se puede proceder a su recolección, para ello se pueden seguir los siguientes pasos:
Detalle etiqueta disco duro

Copia bit a bit de los discos que se quieran analizar, es decir, se requiere una copia exacta del contenido de los discos incautados. Esto incluye todos los archivos del disco, por ejemplo los temporales, los ocultos, los de configuración, los eliminados y no sobrescritos y la información relativa a la parte del disco no asignada, es lo que se conoce como copia a bajo nivel.

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

PRESERVACIÓN DE LAS EVIDENCIAS

Una mala preservación de las evidencias, un mal uso o una mala manipulación pueden invalidar toda la investigación que se lleva a cabo delante de un tribunal, este es un factor muy importante que se va repitiendo a lo largo de toda la metodología.

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

ANÁLISIS DE LAS EVIDENCIAS

La técnica de análisis no termina hasta que no se puede determinar qué o quién causó el incidente, cómo lo hizo, qué afectación ha tenido en el sistema, etc. Es decir, es el núcleo duro de la investigación y tiene que concluir con el máximo de información posible para poder proceder a elaborar unos informes con todo el suceso bien documentado.

Antes de empezar el análisis, es importante recordar unas premisas básicas que todo investigador debe tener presente en el momento de enfrontarse al incidente

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

Para ayudar al desarrollo de esta tecnica del análisis forense podemos centrarnos en varios puntos importantes que generalmente siempre deben realizarse. Cabe recordar que no existe ningún proceso estándar que ayude a la investigación y habrá que estudiar cada caso por separado teniendo en cuentas las diversas particularidades que nos podamos encontrar. No será lo mismo analizar un equipo con sistema operativo Windows o con Linux.

Tampoco será lo mismo un caso de intrusión en el correo electrónico de alguien o un ataque de denegación de servicio a una institución. De igual forma no actuaremos con los mismos pasos en un caso de instalación de un malware que destruya información de una ubicación de disco o un malware que envíe todo lo que se teclea en un equipo

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

En todo caso, se pueden destacar varios pasos, que habrá que adaptar en cada caso:

- Preparar un entorno de trabajo adaptado a las necesidades del incidente.
- Reconstruir una línea temporal con los hechos sucedidos.
- Determinar qué procedimiento se llevó a cabo por parte del atacante.
- Identificar el autor o autores de los hechos.
- Evaluar el impacto causado y si es posible la recuperación del sistema

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

Preparar un entorno de trabajo: Antes de empezar el análisis propiamente, se debe preparar un entorno para dicho análisis.

Es el momento de decidir si se va a hacer un análisis en caliente o en frío. En caso de un análisis en caliente se hará la investigación sobre los discos originales, lo que conlleva ciertos riesgos. Hay que tomar la precaución de poner el disco en modo sólo lectura, esta opción sólo está disponible en sistemas operativos Linux pero no en Windows. Si se opta por esta opción hay que operar con sumo cuidado pues cualquier error puede ser fatal y dar al traste con todo el proceso, invalidando las pruebas.

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

Creación de la línea temporal : Sea cual sea el tipo de análisis que se va a llevar a cabo, el primer paso suele ser crear una línea temporal dónde ubicar los acontecimientos que han tenido lugar en el equipo desde su primera instalación. Para crear la línea temporal, lo más sencillo es referirnos a los tiempos MACD de los archivos, es decir, las fechas de modificación, acceso, cambio y borrado, en los casos que aplique. Es importante, como ya se ha indicado en alguna ocasión tener en cuenta los husos horarios y que la fecha y hora del sistema no tienen por qué coincidir con los reales. Este dato es muy importante para poder dar crédito a las pruebas y a la investigación en general.