www.eysglobal.com

MÓDULO 1

TEMA 19:HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE PARTE 3

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

Continuemos adquiriendo conocimiento en como utilizamos estas técnicas en un análisis para culminar con éxito un caso:

Determinar cómo se actuó : Para determinar cómo se actuó es importante llevar a cabo una investigación sobre la memoria del equipo. Es interesante realizar un volcado de memoria para la obtención de cierta información. Con programas destinados a tal fin podremos ver que procesos se están ejecutando en el momento concreto y también aquellos que hayan sido ocultados para no levantar sospechas. Con esta información podremos saber qué ejecutables inician los procesos en ejecución y qué librerías se ven involucradas. Llegados aquí se puede proceder a realizar volcados de los ejecutables y de dichas librerías para poder analizar si contienen cadenas sospechosas o si, por lo contrario, son archivos legítimos. Sabiendo los procesos que se ejecutan y su naturaleza podemos obtener pistas de cómo se actuó para comprometer el equipo.

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

A menudo nos deberemos fijar en procesos en ejecución aparentemente inofensivos, habituales y legítimos en los sistemas operativos. No es extraño que determinados procesos con fines malintencionados se camuflen con procesos legítimos. Para ello deberemos observar que muchas veces estos se encuentran sin un proceso padre, cuando lo más habitual es que dependan de otros. En otras ocasiones simplemente se camuflan con nombres muy parecidos a otros para pasar desapercibidos

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

Identificación de autores: Para poder realizar una identificación del autor o autores del incidente, otra información importante que nos puede dar el volcado de memoria son las conexiones de red abiertas y las que están preparadas para enviar o recibir datos. Con esto podremos relacionar el posible origen del ataque buscando datos como la dirección IP en Internet. Hay que actuar con prudencia puesto que en ocasiones se utilizan técnicas para distribuir los ataques o falsear la dirección IP. Hay que ser crítico con la información que se obtiene y contrastarla correctamente. No siempre se obtendrá la respuesta al primer intento y posiblemente en ocasiones sea muy difícil averiguar el origen de un incidente

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

Impacto causado: El impacto causado se puede calcular en base a distintos factores y no hay un método único para su cálculo, ni una fórmula que nos dé un importe económico. Aun así para estos cálculos puede servir ayudarse de métodos como BIA (Business Impact Analysis) que determinan el impacto de ciertos eventos ayudando a valorar los daños económicamente.

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

REDACCIÓN DE INFORMES La última técnica de un análisis forense queda para redactar los informes que documenten los antecedentes del evento, todo el trabajo realizado, el método seguido y las conclusiones e impacto que se ha derivado de todo el incidente. Para ello se redactarán dos informes, a saber, el informe técnico y el ejecutivo. En esencia en ambos informes se explican los mismos hechos pero varía su enfoque y el grado de detalle con que se expone el asunto.

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

- En el informe ejecutivo se usará un lenguaje claro y sin tecnicismos, se debe evitar usar terminología propia de la ciencia e ingeniería y expresiones confusas para gente no ducha en el tema. Hay que pensar que el público lector de estos informes serán jueces y gerentes que seguramente estén poco relacionados con el tema y además tengan poco tiempo para dedicarle. Se les debe facilitar la tarea al máximo.

- En el informe técnico, por el contrario, el público final será técnico y con conocimientos de la materia que se expone. Aquí se detallarán todos los procesos, los programas utilizados, las técnicas, etcétera. Debemos crear un documento que pueda servir de guía para repetir todo el proceso que se ha realizado en caso necesario

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

El informe ejecutivo Entrando más en detalle en este tipo de informes, cabe destacar que será un resumen de toda la tarea que se ha llevado a cabo con las evidencias digitales. Aunque será un documento de poca extensión, al menos comparado con el informe técnico, éste deberá contener al menos los siguientes apartados:

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

Motivos de la intrusión.
¿Por qué se ha producido el incidente? ¿Qué finalidad tenía el atacante?

Desarrollo de la intrusión. ¿Cómo lo ha logrado? ¿Qué ha realizado en los sistemas?

Resultados del análisis. ¿Qué ha pasado? ¿Qué daños se han producido o se prevén que se producirán? ¿Es denunciable? ¿Quién es el autor o autores?

Recomendaciones. ¿Qué pasos dar a continuación? ¿Cómo protegerse para no repetir los hechos?

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

El informe técnico

El informe técnico será más largo que el anterior y contendrá mucho más detalle. Se hará una exposición muy detallada de todo el análisis con profundidad en la tecnología usada y los hallazgos. En este caso se deberá redactar, al menos:

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

Antecedentes del incidente.

- Puesta en situación de cómo se encontraba la situación anteriormente al incidente.

Recolección de datos.

- ¿Cómo se ha llevado a cabo el proceso?
- ¿Qué se ha recolectado?

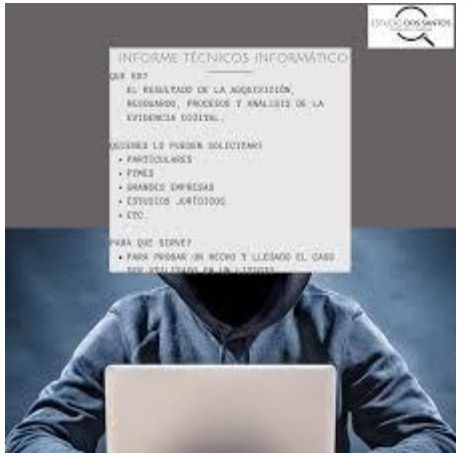
Descripción de la evidencia.

- Detalles técnicos de las evidencias recolectadas, su estado, su contenido, etc.

Entorno de trabajo del análisis.

- ¿Qué herramientas se han usado?
- ¿Cómo se han usado?

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE



Análisis de las evidencias

- Se deberá informar del sistema analizado aportando datos como las características del sistema operativo, las aplicaciones instaladas en el equipo, los servicios en ejecución, las vulnerabilidades que se han detectado y la metodología usada.

Descripción de los resultados.

- ¿Qué herramientas ha usado el atacante?
- ¿Qué alcance ha tenido el incidente?
- Determinar el origen del mismo y como se ha encontrado.

Dar la línea temporal de los hechos ocurridos con todo detalle. Redactar unas conclusiones con las valoraciones que se crean oportunas a la vista de todo el análisis realizado.