www.eysglobal.com

MÓDULO 1

TEMA 14:
RECUPERACIÒN Y
ANÀLISIS

RECUPERACIÒN Y ANÀLISIS

En la Recuperación y el análisis de un caso en el que sea necesario el cómputo forense, hay tres roles principales que son importantes y se deben tener en cuenta: el intruso, el administrador y la infraestructura de la seguridad informática, y el investigador.

Socialicemos un poco estos roles:

RECUPERACIÒN Y ANÀLISIS

Intrusos:
El intruso es aquel que ataca un sistema, hace cambios no autorizados, manipula contraseñas o cambia configuraciones, entre otras actividades que atentan contra la seguridad de un sistema. La intención de los intrusos es un punto clave para poder analizar el caso, ya que no se puede comparar un intruso cuya motivación es el dinero con otro cuya motivación es la demostración de sus habilidades.

RECUPERACIÒN Y ANÀLISIS

Motivaciones	Ciber-Terroristas	Phreakers	Script kiddies	Crackers	Desarrollo de virus	Atacante interno
Reto		X			X	X
Ego		X	X		X	
Espionaje				X	X	X
Ideología	X					
Dinero		X		X	X	X
Venganza	X		X		X	X

Algunos intrusos y sus motivaciones

El modelo del atacante para realizar su procedimiento se explica conceptualmente por tres fases: la fase de reconocimiento, la fase de ataque y la fase de eliminación.

RECUPERACIÒN Y ANÀLISIS

Administradores y la infraestructura de la seguridad informática:

El administrador del sistema es el experto encargado de la configuración de este, de la infraestructura informática y de la seguridad del sistema. Estos administradores son los primeros en estar en contacto con la inseguridad de la información, ya sea por un atacante o por una falla interna de los equipos. Al ser los arquitectos de la infraestructura y de la seguridad de la información del sistema, son quienes primero deberían reaccionar ante un ataque, y deben proporcionar su conocimiento de la infraestructura del sistema para apoyar el caso y poder resolverlo con mayor facilidad.

RECUPERACIÒN Y ANÀLISIS

Investigador

Es un nuevo profesional que actúa como perito, criminalista digital, o informático. Comprende y conoce las nuevas tecnologías de la información, y analiza la inseguridad informática emergente en los sistemas. El perfil del investigador es nuevo y necesario en el contexto abierto informático en el que vivimos. Por lo tanto, es necesario formar personas que puedan trabajar como investigadores en la disciplina emergente de la criminalística digital y el cómputo forense.

RECUPERACIÒN Y ANÀLISIS

roles:

•Líder del caso: es aquel que planea y organiza todo el proceso de investigación digital. Debe identificar el lugar en donde se realizará la investigación, quienes serán los participantes y el tiempo necesario para esta.
•Auditor/ingeniero especialista en seguridad de la información: conoce el escenario en donde se desarrolla la investigación. Tiene el conocimiento del modelo de seguridad en el cual ocurrieron los hechos y de los usuarios y las acciones que pueden realizar en el sistema. A partir de sus conocimientos debe entregar información crítica a la investigación.

RECUPERACIÒN Y ANÀLISIS

Especialista en informática forense: es un criminalista digital que debe identificar los diferentes elementos probatorios informáticos vinculados al caso, determinando la relación entre los elementos y los hechos para descubrir el autor del delito.

Analista en informática forense: examina en detalle los datos, los elementos informáticos recogidos en la escena del crimen con el fin de extraer toda la información posible y relevante para resolver el caso.

Es importante recalcar que una misma persona puede tomar más de un rol, e incluso los cuatro, en un proceso de investigación

RECUPERACIÒN Y ANÀLISIS

Dispositivos a analizar:

Toda aquella infraestructura informática que tenga una memoria es susceptible de análisis:

- Disco duro de una Computadora o Servidor
- Documentación referente al caso.
- Tipo de sistema de telecomunicaciones.
- Dirección MAC.
- Inicios de sesiones.
- Información de los cortafuegos.
- IP, redes Proxy. LMhost, host, conexiones cruzadas, pasarelas.
- *Software* de supervisión y seguridad.
- Credenciales de autentificación.
- Rastreo de paquetes de red.

RECUPERACIÒN Y ANÀLISIS

CONSOLIDACIÓN DE ARCHIVOS SOSPECHOSOS: Como resultado del filtrado de “buenos conocidos”, se obtiene un conjunto de archivos susceptibles a análisis, este conjunto se llamará archivos sospechosos

PRIMERA CLASIFICACIÓN DE ARCHIVOS: Divide los archivos sospechosos en: Archivos “Buenos” Modificados: Son identificados en la fase de filtrado como archivos buenos

RECUPERACIÒN Y ANÀLISIS

Archivos “Malos”: Se obtienen a partir de la comparación de los archivos sospechosos contra los compendios criptográficos de archivos “malos” relacionados con el sistema operativo particular. Estos archivos representan algún tipo de riesgo para el sistema en el que se encuentran o se ejecutan, por ejemplo: sniffers, troyanos, backdoors, virus, keyloggers entre otros.

Archivos Con Extensión Modificada: Aquellos cuya extensión no es consistente con su contenido (para ello siempre es necesario verificar los encabezados de los archivos y no su extensión)

RECUPERACIÒN Y ANÀLISIS

SEGUNDA CLASIFICACIÓN DE ARCHIVOS Esta clasificación toma archivos que no han sido considerados de máxima prioridad, los examina y los evalúa respecto a dos criterios: relación de los archivos con los usuarios involucrados en la investigación y contenido relevante para el caso, derivado del marco circunstancial. De esta manera, se busca obtener información complementaria útil para la fase de análisis.

RECUPERACIÒN Y ANÀLISIS

ANÁLISIS DE LA INFORMACIÓN PRIORITARIA. Este proceso se basa en la discriminación de los archivos prioritarios con respecto a su relevancia con el caso y el criterio del investigador. Es importante resaltar que los procesos de la segunda clasificación y análisis , pueden ser iterativos con el fin de obtener más cantidad de evidencia pertinente.

RECUPERACIÒN Y ANÀLISIS

RECUPERACIÓN Y ANALISIS DE LOS ARCHIVOS BORRADOS:

Durante esta actividad se deben tratar de recuperar los archivos borrados del sistema de archivos, lo que es conveniente dado el frecuente borrado de archivos para destruir evidencia. Dependiendo de las características técnicas y del estado del sistema de archivos puede no ser posible la recuperación de la totalidad de los archivos eliminados, por ejemplo si estos han sido sobre escritos, o si se han utilizado herramientas de borrado seguro para eliminarlos.

RECUPERACIÒN Y ANÀLISIS

RECUPERACIÓN DE INFORMACIÓN ESCONDIDA:
En esta etapa se debe examinar exhaustivamente el slack space, los campos reservados en el sistema de archivos y los espacios etiquetados como dañados por el sistema de archivos. Los archivos protegidos también se tendrán en cuenta durante la fase de análisis de éste tipo de archivos

RECUPERACIÒN Y ANÀLISIS

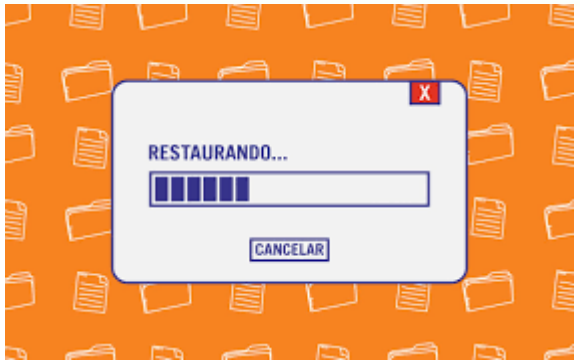
Recolección de datos:

Existen dos tendencias a la hora de realizar análisis en máquinas comprometidas:

La primera opta por no realizar ningún tipo de acción sobre la máquina con el objetivo de obtener información del estado actual.

La segunda opta por recoger información del estado actual, ya que en caso de no obtenerse en ese preciso instante, se perdería
:

RECUPERACIÒN Y ANÀLISIS



Inconvenientes de análisis en caliente:

realizar cualquier acción sobre la máquina implica que esa propia acción altera su estado y puede alterar la información, también puede implicar un aviso al atacante y que este elimine sus huellas rápidamente.

Beneficios del análisis en caliente:

la información que podemos obtener del estado de la máquina puede ser muy útil (conexiones, ficheros abiertos, programas en ejecución, estado de la memoria, etc.).