Estudio de caso: Archivos ocultos – informática forense

Cuestionario de examen

1. Esboce el significado de los siguientes términos.

(a) *cookie* *[2 puntos]*

Una cookie es un conjunto de datos almacenados localmente que usan algunos sitios web para mantener datos entre sesiones como, por ejemplo, recordar los detalles del usuario activo.

2

(b) *espacio de archivo desperdiciado* *[2 puntos]*

El espacio de archivo desperdiciado se produce cuando un archivo es más pequeño que el tamaño total de los clústeres que tiene asignado. Es el espacio entre el final de los datos del archivo y el próximo clúster.

2

2. Las empresas que reciclan sus computadores y los venden a terceros deberían borrar todos los datos de los discos duros. Esta operación, no obstante, puede fallar en ocasiones.

(a) Esboce cómo el formateo del disco podría no conseguir el objetivo propuesto.

[4 puntos]

Un archivo se almacena en un disco duro como la información contenida dentro del archivo, pero también metainformación sobre el mismo, como la fecha de creación y la ubicación de los contenidos del archivo en el disco. [Almacenado en el directorio raíz y la FAT] Normalmente, cuando se borra un archivo el espacio que ocupan los contenidos se marca como disponible para que se sobrescriba cuando sea necesario. [Explicación] Cuando se formatea un disco, el proceso concreto dependerá de la herramienta utilizada. [Es necesario incluir más detalles. El formateo normal (p. ej. en Windows o DOS) borraría los datos del directorio raíz y de la FAT. Una "limpieza forense", sin embargo, normalmente escribe varios caracteres idénticos (p. ej. ceros) en cada sector]. Es probable que solo se elimine la referencia al archivo, al igual que con la eliminación y, por tanto, los contenidos del archivo aún permanezcan. [Para conseguir el cuarto punto, el alumno debe distinguir entre los distintos tipos de formateo (referencia a la "herramienta" usada) ya que la elección del formateo ocasionaría distintos resultados].

3

(b) Esboce los posibles efectos sobre la privacidad si **no** se borran todos los datos.

[4 puntos]

Es probable que el usuario de un computador haya registrado información confidencial para la compañía, como datos de los clientes, estrategias de marketing, etc. Si estos datos no se borran completamente, estarían disponibles para los nuevos propietarios de la unidad de disco. Se suele asumir que la privacidad es un derecho y que la pérdida de la misma mediante la divulgación involuntaria de datos es un problema ético. [No añade valor a la respuesta] Si la información del cliente se facilita a otra compañía, esta podría acceder a información comprometedora para el cliente, como registros sanitarios o legales.

4

3. Durante la práctica, John se centró en conseguir el disco duro del computador del sospechoso.

Explique por qué se podría haber obviado alguna prueba adicional al concentrarse sólo en el disco duro. *[6 puntos]*

Los datos almacenados en un computador no residen completamente en el disco duro, ya que la memoria principal del computador (RAM) también contiene datos temporales. Si se toma el disco duro como el centro de la investigación, cualquier prueba que se almacene en la RAM se podría perder al apagar el sistema. Los programas actualmente abiertos podrían ser relevantes para la investigación, al igual que cualquier información contenida en los mismos. Es probable que esta información solo se almacene en la memoria del computador y, por tanto, si nos centramos solo en el disco duro se podría perder alguna prueba. [La respuesta es correcta, pero hay que prestar atención a no alterar pruebas importantes como fechas y horas al utilizar el computador]

Si el usuario del sistema ha tomado contramedidas forenses como la encriptación de datos del disco duro, centrarse solo en el disco duro podría producir pérdidas de datos que sirvan como pruebas. Si el disco duro está encriptado, la clave para desencriptarlo solo podría almacenarse en la RAM y se perdería al no investigar los contenidos de la memoria del sistema. El entorno podría contener unidades flash o medios ópticos que también podrían contener claves de encriptación. Si estas fuentes de datos no se investigan, también se podrían perder pruebas en forma de archivos o datos almacenados en el interior. [La respuesta es correcta, pero hay que prestar atención a no alterar pruebas importantes como fechas y horas al utilizar el computador]

El disco duro es el sitio más lógico para encontrar pruebas y, por tanto, si el usuario ha toma contramedidas forenses básicas, cualquier dato del disco duro podría estar oculto y, por tanto, la búsqueda de archivos podría requerir mucho tiempo. Además, la búsqueda en memoria y en el entorno podría generar pruebas inculpatorias (o exculpatorias) incluso más fácilmente.

La respuesta demuestra un muy buen nivel de conocimientos y desarrolla varias ideas rigurosamente. La extensión de la respuesta (259 palabras) es adecuada.

6

4. Discuta los métodos usados por los criminales para ocultar o camuflar archivos. Para cada método, identifique la contramedida que podría tomar un científico forense informático.

[12 puntos]

Si un criminal conoce la informática forense y las técnicas usadas, podría intentar ocultar o camuflar sus actividades o datos incriminatorios. Para localizar estas actividades habría que realizar un esfuerzo adicional.

A partir de un estudio independiente basado en Anti-Forensics y en la visita del colegio al Dr. McBride en la Universidad De Montfort [prueba de investigación], una forma posible de ocultar información delictiva inculpatoria es encriptar los datos en el disco duro o encriptar archivos individuales en todo el disco. Esto vuelve ilegible el contenido del archivo a menos que tengamos la clave de encriptación, aunque esto podría verse como evitar el acceso y no como ocultación de datos y podría llamar la atención. [Fuera de tema, no añade ningún valor a la respuesta]

A partir de la investigación en Forensics Wiki, [investigación: no se requiere la URL, la información va más allá del estudio de caso, así que se considera investigación] la esteganografía **[M1]** es la acción de ocultar información o archivos dentro de otros archivos en apariencia inofensivos, como ocultar un archivo de texto dentro de una imagen. Las imágenes suelen contener información sobre las propias imágenes, como la cámara que tomó la foto. Este espacio se puede usar para almacenar datos no relacionados, como un archivo de texto. Mientras que el archivo oculto se almacene en texto plano, una búsqueda de una cadena de texto con las palabras clave relevantes para la investigación debería encontrar la información. En cambio, si la información está encriptada, la búsqueda es mucho más difícil. También sería posible buscar irregularidades en archivos que muestren el uso de software esteganográfico común **[CM1]**, como grandes cantidades de datos redundantes que no están relacionados con la imagen y podría ser información encriptada como, por ejemplo, búsquedas con 'stegdetect' de signaturas comunes de programas esteganográficos. [Excelente conocimiento basado en una investigación que va mucho más allá de la información del estudio de caso]

Cambiar la extensión **[M2]** podría contribuir a ocultar los archivos, ya que no estarían visibles para las búsquedas simples de algún tipo de archivos. En el estudio de caso, por ejemplo, se podría detener una búsqueda de imágenes cambiando la extensión de cualquier imagen incriminatoria, por ejemplo, un archivo .jpg por un archivo .doc. Una contramedida adecuada para esta situación sería buscar imágenes por el contenido del archivo **[CM2]**. Como los tipos de

archivo suelen tener una cabecera estándar que los identifica como imágenes, se podría dirigir una búsqueda hacia estas cabeceras, lo cual sería más fiable para localizar imágenes aunque requiera más tiempo.

Además, cambiar el nombre de los archivos **[M3]** puede ocultar los contenidos haciendo que sea más difícil de encontrar los archivos relevantes para la investigación, como por ejemplo, poner nombres no significativos a archivos relevantes para que no se pueda sospechar que los contenidos tienen ninguna información relevante para el caso. Una contramedida **[CM3]** es no centrarse en los nombres de los archivos, sino en los contenidos, usando búsquedas diseñadas para encontrar palabras relevantes para la investigación independientemente de su ubicación en el disco duro.

Hay varios métodos que los criminales pueden usar para ocultar cualquier prueba incriminatoria, aunque la mayoría se podría superar buscando cadenas concretas en el disco duro. [Buen resumen] La información de Anti-Forensics y la visita del colegio al Dr. McBride de la Universidad De Montfort demostraron cómo encontrar la mayoría de información sin importar cuánto se camuflen nombres o extensiones de archivos. [Conclusión relacionada con el análisis y la investigación] No obstante, si se usa la encriptación, se debe encontrar la clave empleando otros medios para conseguir cualquier dato. Existen contramedidas sencillas para los métodos básicos de ocultar o camuflar archivos y, en la mayoría de los casos, no es probable que se use la encriptación. Incluso cuando se usa, es bastante probable encontrar en los registros de actividad pruebas que han pasado desapercibidas y que no se han encriptado.

Una respuesta bien investigada y meticulosa que abarca tres medidas y contramedidas con la profundidad adecuada. El párrafo final unifica la respuesta y ofrece una conclusión adecuada. La respuesta va claramente más allá de la información del estudio de caso y ofrece una prueba clara de que se ha realizado una investigación amplia.

Hay una leve confusión en la respuesta sobre encriptación y cuando afirma que no oculta o camufla archivos, sino que solo dificulta el acceso a los mismos, pero el alumno habría conseguido la máxima puntuación sin ella, así que no se le penaliza por salirse del tema.

12

Recursos (solo con fines informativos)

http://archive.cabinetoffice.gov.uk/e-government/resources/handbook/html/4-7.asp

- Información en profundidad sobre las cookies. Es demasiado detallada, pero la introducción proporciona un buen resumen acerca de las cookies y trata el tema de la privacidad. [En inglés].

http://www.anti-forensics.com/

- Proporciona el punto de vista opuesto y es útil para mostrar algunas de las técnicas utilizadas para burlar la informática forense. [En inglés].

http://en.wikipedia.org/wiki/Computer_forensics#The_Forensic_Process

- No es fiable puesto que se trata de la Wikipedia, pero ofrece una perspectiva general del proceso forense y ayuda a comprender cómo se desarrolla una investigación. [En inglés. La versión en español de este artículo se encuentra en http://es.wikipedia.org/wiki/Cómputo_forense]

http://www.forensicswiki.org/wiki/Main_Page

- Principalmente útil para encontrar el significado de palabras clave. No proporciona tanta información acerca del proceso forense. [En inglés].

http://www.daemon.be/maarten/forensics.html

- Proporciona información acerca del proceso forense y además da ejemplos específicos de las técnicas utilizadas. [En inglés].

http://www.outguess.org/detection.php

- Programa utilizado para detectar información esteganográfica en archivos de imagen. [En inglés].