ANÁLISIS FORENSE DE SISTEMAS LINUX

Juan Manuel Canelada Oset
jmcanelada@eresmas.net
Grupo de Seguridad de las Tecnologías de la Información y las Comunicaciones.
Universidad Carlos III de Madrid

RESUMEN

La facilidad de acceso a Internet y el desarrollo del mercado relacionado con los dispositivos que permiten acceder a las nuevas comunicaciones han cambiado no solo la forma en la que se pasa el tiempo libre y la forma en la que se llevan a cabo los negocios sino también la forma en la que los delincuentes comenten sus crímenes. En este panorama complejo, los profesionales de las tecnologías de la información y los profesionales de la defensa de la ley deben cooperar y trabajar juntos en la defensa, detección y procesamiento de las personas que utilizan las nuevas tecnologías para dañar individuos, organizaciones, empresas o sociedad en general.

Los ordenadores y las redes pueden verse involucrados en un crimen informático siendo las herramientas utilizadas para cometer el crimen, las víctimas del crimen o ser utilizadas para propósitos incidentales relacionados con el crimen. El **Análisis Forense de Sistemas (Computer Forensics)** comprende el proceso de extracción, conservación, identificación, documentación, interpretación y presentación de las evidencias digitales de forma que sean legalmente aceptadas en cualquier proceso legal, proporcionando las técnicas y principios que facilitan la investigación del delito.

Linux es un entorno ideal en el cual realizar tareas de análisis forense pues está dotado de gran variedad de herramientas que facilitan todas las etapas que se deben llevar a cabo en la realización de un análisis exhaustivo de un sistema comprometido.

INTRODUCCIÓN

La proliferación de redes y sistemas informáticos nos ha llevado a vivir en un mundo en el cual se trabaja y se vive globalmente conectado, se pueden mantener conversaciones, intercambiar correo o realizar transacciones monetarias con personas que se encuentran en cualquier parte del planeta de forma rápida y barata. Sin embargo, la facilidad de acceso a Internet y el desarrollo del mercado relacionado con los dispositivos que permiten acceder a las nuevas comunicaciones han cambiado no solo la forma en la que se pasa el tiempo libre y la forma en la que se llevan a cabo los negocios sino también la forma en la que los delincuentes comenten sus crímenes. La accesibilidad digital universal abre nuevas oportunidades a las personas sin escrúpulos. Según la última ***Encuesta sobre***

Seguridad y Crimen Informático del año 2004 publicada conjuntamente por el **CSI** (Computer Security Institute) y el **FBI** (Federal Bureau of Investigation) las pérdidas ocasionadas por culpa de ataque informáticos durante el año 2004 ascienden a casi ciento cincuenta millones de dólares.

La utilización de ordenadores y redes para preparar ataques violentos o para coordinar y llevar a cabo actividades terroristas que amenazan las seguridad a escala mundial, los delitos relacionados con la posesión o distribución de pornografía infantil, la falsificación y fraude de datos bancarios muestran un panorama complejo, en el cual los profesionales de las tecnologías de la información y los profesionales de la defensa de la ley deben cooperar y trabajar juntos en la defensa, detección y procesamiento de las personas que utilizan las nuevas tecnologías para dañar individuos, organizaciones, empresas o sociedad en general.

CONCEPTOS BÁSICOS

En el Décimo Congreso de las Naciones Unidas sobre la Prevención del Crimen y el Tratamiento de los Delincuentes, celebrado en Viena el año 2000, se definieron dos categorías de Crímenes Informáticos, a saber:

1. **Crimen Informático en sentido estricto**: Cualquier comportamiento ilegal, dirigido por medio de operaciones electrónicas que tengan como objetivo la seguridad de sistemas informáticos y de los datos que procesan.

2. **Crimen Informático en sentido amplio** (crímenes relacionados con la informática): Cualquier comportamiento ilegal cometido por medio o en relación con un sistema informático o una red, incluyendo crímenes como la posesión ilegal, la oferta y la distribución de información por medio de un sistema informático o de una red.

Estas definiciones no son completamente definitivas pero proporcionan un buen punto de inicio que además tiene reconocimiento y acuerdo internacional, si bien el asunto es más complejo pues una acción puede ser ilegal en un país y no serlo en otro.

Atendiendo a las definiciones expuestas anteriormente, los ordenadores y las redes pueden verse involucrados en un crimen informático de varias formas:

1. El ordenador o la red pueden ser las herramientas utilizadas para cometer el crimen.

2. El ordenador o la red pueden ser los objetivos o víctimas del crimen.

3. El ordenador o la red pueden ser utilizadas para propósitos incidentales relacionados con el crimen.

El **Análisis Forense de Sistemas (Computer Forensics)** comprende el proceso de extracción, conservación, identificación, documentación, interpretación y presentación de las evidencias digitales de forma que sean legalmente aceptadas en cualquier proceso legal (por ejemplo un juicio).

Proporciona las técnicas y principios que facilitan la investigación del delito y su metodología básica consiste en:

1. Adquirir las evidencias sin alterar ni dañar el original. La forma ideal de examinar un sistema consiste en detenerlo y examinar una copia de los datos originales, es importante tener en cuenta que no se puede examinar un sistema presuntamente comprometido utilizando las herramientas que se encuentran en dicho sistema pues estas pueden estar afectadas. La **Cadena de Custodia** documenta el proceso completo de las evidencias durante la vida del caso, quién la recogió y donde, quien y como la almacenó, quién la procesó… etc. Cada evidencia deberá ser identificada y etiquetada a ser posible en presencia de testigos, con el número del caso, una breve descripción, la firma y la fecha en que fue recogida.

2. Comprobar (Autenticar) que las evidencias recogidas y que van a ser la base de la investigación son idénticas a las abandonadas por el delincuente en la escena del crimen. Las técnicas y herramientas de control de integridad que mediante la utilización de una función ***hash*** generan una huella electrónica digital de un fichero o un disco completo constituyen una ayuda básica.

3. Analizar los datos sin modificarlos. En este punto, es crucial proteger las evidencias físicas originales trabajando con copias idénticas de forma que en caso de error se pueda recuperar la imagen original y continuar con el análisis de forma correcta. Se recomienda la realización de dos copias de los discos originales. Estas copias deben ser clones realizados bit a bit del dispositivo original, los backups normales no copian ficheros que han sido borrados ni determinadas partes de los discos que pueden contener pistas importantes para el desarrollo de la investigación. Es básico realizar siempre un control de integridad de la copia realizada antes de comenzar ningún análisis.

De los párrafos anteriores puede deducirse que las evidencias digitales presentan una serie de ventajas sobre otros conjuntos de evidencias físicas. Estas ventajas son:

1. Pueden ser duplicadas de forma exacta, pudiendo examinarse la copia como si fuera el original. Si alguien intenta destruir las evidencias se pueden tener copias igualmente válidas lejos del alcance del criminal.

2. Con la utilización de herramientas adecuadas es fácil determinar si la evidencia ha sido modificada o falsificada comparándola con la original.

3. Es relativamente difícil destruir una evidencia digital. Incluso borrándola puede ser recuperada del disco.

VENTAJAS DE LINUX COMO HERRAMIENTA DE ANÁLISIS FORENSE

El sistema operativo Linux presenta algunas características que le dotan de grandes ventajas a la hora de ser utilizado como herramienta de análisis forense de sistemas. Estas características son:

- Todo, incluido el hardware se trata y representa como un fichero.
- Soporta numerosos tipos de sistemas de archivos, mucho no reconocidos por Windows
- Permite montar los sistemas de archivos
- Permite analizar un sistema en funcionamiento de forma segura y poco invasiva.
- Permite redirigir la salida de un comando a la entrada de otro (múltiples comandos en una línea)
- Permite revisar el código fuente de la mayoría de sus utilidades
- Permite generar dispositivos de arranque
- Es gratuito, así como la mayoría de las herramientas utilizadas para el análisis forense de sistemas.

ANÁLISIS FORENSE CON LINUX

Linux es un entorno ideal en el cual realizar tareas de análisis forense pues está dotado de gran variedad de herramientas que facilitan todas las etapas que se deben llevar a cabo en la realización de un análisis exhaustivo de un sistema comprometido.

TÉCNICAS DE RECOPILACIÓN DE EVIDENCIAS

Independientemente del tipo de investigación que se esté llevando a cabo, es importante no confiar demasiado en la memoria y llevar un registro claro de la fecha y hora en la que se recogen las diferentes evidencias. Si se va a analizar un sistema comprometido en producción desde su propia consola, es recomendable ejecutar el ***comando script***, el cual captura y almacena en un fichero toda la actividad tecleada desde la consola. Su sintaxis es:

```
# script –a fichero
```

Para posteriormente realizar el análisis, es necesario disponer de un lugar en el cual almacenar los datos del sistema comprometido. Si no se dispone de un dispositivo de almacenamiento removible de gran capacidad o no se puede realizar una clonación del disco afectado, el ***comando netcat*** constituye una herramienta de gran valor pues permite transferir vía red la información del servidor afectado a otro sistema en el cual realizar el análisis. Para ello en el sistema de análisis se ejecutará el comando:

```
# nc –l –p puerto > fichero de salida
```

En el sistema comprometido se ejecutará por ejemplo el comando:

```
# cat /etc/passwd | nc maquina de análisis puerto -w 2
```

El proceso nc en la máquina de análisis se ejecutará hasta que la conexión se rompa, cerrándose el fichero de salida. La opción –w 2 indica el número de segundos que espera una vez recibido el fin de fichero para terminar la conexión.

CAPTURAS DE PANTALLA

El ***comando xwd*** de X Window permite capturar tanto ventanas de forma individual como la pantalla completa desde un servidor remoto. Para ello se ejecutará el comando:

```
# xwd –display direccionIP:0 –root > pantalla.xwd
```

Una vez capturada la pantalla, se puede ver su contenido con el ***comando xwud*** o cualquier otro visor de imágenes que soporte dicho formato.

```
# xwud –in pantalla.xwd
```

CAPTURA DE LA MEMORIA

En Linux todo se trata como un fichero, esto hace muy sencillo copiar y analizar el contenido tanto de la memoria principal analizando el ***fichero /dev/mem*** como del ***área de swap*** analizando la partición correspondiente. Sobre estos dispositivos se pueden utilizar comandos como ***strings*** o ***grep***. Por ejemplo:

```
# strings /dev/mem | more
```

Es importante tener en cuenta que la memoria es un dispositivo volátil, esto implica que es imposible verificar (por ejemplo con el ***comando md5sum***) que los datos capturados se corresponden exactamente con los originales pues el simple hecho de capturarlos hace que varíen ligeramente.

ANÁLISIS DE LAS CONEXIONES DE RED

El estado de la red proporciona información tanto de las conexiones existentes como de los procesos en ejecución. El ***comando netstat*** proporciona información sobre la actividad de red del sistema. La ejecución del siguiente comando proporciona información sobre los procesos asociados con cada conexión de red específica:

```
# netstat –pan | more
```

COPIA DE DISCOS DUROS Y SISTEMAS DE ARCHIVOS

Todas las distribuciones de Linux proporcionan un conjunto de herramientas que permiten copiar los sistemas de ficheros de forma que es posible examinarlos en una estación segura cuando no es posible apagar el sistema o quitar el disco para su clonación. Si no se dispone de un dispositivo de almacenamiento de gran capacidad, es posible copiar discos enteros, particiones o sistemas de archivos completos a un sistema remoto utilizando la ***herramienta netcat (nc)***.

El ***comando mount*** muestra los sistemas de archivos que se encuentran montados, el ***comando fdisk*** muestra las particiones existentes en cada unidad de disco estén o no montadas en ese momento.

```
# fdisk –l /dev/hda
```

El ***comando dd*** permite crear imágenes (copias bit a bit) de los sistemas de archivos. Para ello se ejecuta por ejemplo el comando:

```
# dd if=/dev/fd0 of=/tmp/disco.img
```

La ejecución del comando

```
# dd if=/dev/zero of=/dev/fd0
```

permite inicializar completamente el dispositivo sobre el que se va a almacenar la imagen.

La combinación de los comandos dd y netcat permite transferir imágenes completas de sistemas de archivos a través de la red y supone una herramienta vital en la recogida de evidencias que supone la primera fase del análisis forense de un sistema.

Una vez generada la copia es de vital importancia garantizar la autenticidad de la misma para ello es necesario realizar la comprobación, para ello se utiliza el ***comando md5sum***.

ACCESO A LOS DATOS DE UN SISTEMA DE ARCHIVOS

Una vez accesible la imagen generada con las herramientas descritas en el apartado anterior, es necesario analizar su contenido, para ello en Linux se dispone de un dispositivo virtual denominado ***loop*** que representa una abstracción que permite acceder a imágenes de sistemas de archivos. Para poder utilizarlo se crea un directorio sobre el cual montarlo:

```
# mkdir /tmp/analisis
```

A continuación se monta con el comando:

```
# mount –t ext2 –o loop -r fichero.con.imagen  /tmp/analisis
```

Una vez montado se puede tratar como cualquier otro sistema de archivos. Es muy importante montarlo en modo de lectura exclusiva lo que evitará dañar la evidencia. Linux permite trabajar con gran variedad de sistemas de ficheros, si bien en algunos casos es necesario modificar el núcleo para poder realizar el proceso.

ANÁLISIS FORENSE DE DATOS CON AUTOPSY

Autopsy es un interfaz gráfico a las herramientas en línea de comando para análisis forense ***The Sleuth Kit***. Ambos son open source, pueden ejecutarse en varias plataformas UNIX y junto ofrecen muchas de las características propias de sistemas de análisis forense comerciales. Autopsy está basado en HTML por lo que puede accederse a él desde cualquier navegador, proporcionando un gestor de ficheros que muestra información acerca de datos eliminados y estructuras del sistema de ficheros.

BIBLIOGRAFÍA

1. *CyberForensics. A field manual for collecting, examining and preserving evidence of computer crimes.* Albert J. Marcella. Auerbach Publications, 2002.

2. *Handbook of Computer Crime Investigation. Forensic Tools and Technology.* Eoghan Casey. Academic Press, 2002.

3. *Incident Response & Computer Forensic.* Kevin Mandia, Chris Prosise. McGraw-Hill, Second Edition, 2003.

4. *Computer Forensic. Incident Response Essentials.* Warren Kruse. Addison-Wesley, 2002

5. *Scene of the Cybercrime: Computer Forensic Handbook.* Debra LittleJohn Shinder. Syngress Publishing, 2002.

6. *Digital Investigation: The International Journal of Digital Forensics & Incident Response.* Elsevier. Febrero 2004.

7. *Antihacker Toolkit.* Keith Jones. McGraw-Hill, 2004.

8. *Hacking Exposed.* Stuart McClure, Joel Scambray, George Kurtz; McGraw-Hill, 1999.

9. *Criminalistics.* Richard Saferstein, Prentice-Hall, 1998

10. *Investigating Computer-Related Crime.* Peter Stephenson. CRC Press, 2000

11. *Computer Crime, A Crimefighter's Handbook.* Icove, Seger, VonStorch; O'Reilly