Análisis forense en sistemas operativos Linux utilizando The Coroner's Toolkit

Yupanqui Chipana Enrique
Universidad Mayor De San Andrés
Carrera De Informática
Simulación de Sistemas
rique_toolate@hotmail.com

RESUMEN

En este artículo se tratará sobre cómo Linux se esta volviendo una herramienta más amplia en el aspecto de resguardo de evidencia forense, en general, y como la suite The Coroners's Toolkit provee lo necesario para cumplir con los pasos que sigue la informática forense, con el fin que la misma persigue.

Palabras clave

Análisis, evidencia digital, resguardo, captura, daño, sistema informático.

1. INTRODUCCIÓN

Cientos de ordenadores pierden información que al principio resulta parecer no tener importancia, cuando en realidad la falta de esta información puede ser la causa de la quiebra de empresas que reportan perdidas por esta situación.

Los investigadores de informática forenses se encargan de reunir los datos necesarios para encontrar a los causantes del robo de información lo cual realizan gracias a metodologías y herramientas que los apoyan en esta área. Los intrusos cada vez más mejoran las técnicas de intromisión a sistemas sin dejar huellas, borrando pruebas lo cual hace más difícil poder seguirles sin una investigación minuciosa.

De esta manera, el análisis forense se trata en esencia de la extracción, conservación identificación, documentación, interpretación y presentación de las evidencias digitales de tal manera que sean legitimas para cualquier procedimiento legal.

El análisis forense de sistemas informáticos en la época actual juega un papel importante para reunir información y pruebas necesarias, en el campo de la ciencia forense en este caso la escena del crimen al que nos referimos es un ordenador y la red a la cual está conectada (posiblemente), la cual es utilizada para operaciones fraudulentas y delictivas como la distribución de pornografía infantil, la falsificación y fraude de datos bancarios, robo de información que puede dañar tanto a individuos o empresas a las que se relacionan

2. LINUX EN LA INFORMÁTICA FORENSE

Primero veamos algunas ventajas que conlleva utilizar Linux para el uso como herramienta forense de sistemas estas son las siguientes.

Linux es de libre utilización al igual que las herramientas utilizadas para el análisis.

Linux acepta el montaje de archivos

El software como el hardware se interpreta como un fichero.

Soporta muchos tipos de archivos, algunos no reconocidos por los sistemas Windows

Acepta el análisis de un sistema en funcionamiento de forma segura y casi sin dificultades por la invasión.

Acepta el re direccionamiento de salida de un comando a la entrada de otro comando

3. CONCEPTOS FUNDAMENTALES

Al margen de que método de recopilación de la información se esté utilizando se debe tomar nota de la fecha y hora en que se realice la revisión. Además para guardar la información si se utiliza la consola en Linux existe una opción que lo permite y es el comando script el que almacena en un fichero la información de la consola.

Su sintaxis:

```
# script  -a  nombredefichero
```

Para realizar un análisis de óptimo es necesario almacenar una copia de seguridad del sistema afectado, para lo cual se recomienda un dispositivo extraíble de almacenamiento, o realizar un clon del sistema. Si no se tuviera alguna de las opciones podemos utilizar la opción netcat que permite transferir vía red la información del servidor afectado

Su sintaxis:

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

En Linux existen diferentes técnicas para la recopilación de la información y/o evidencias, en este artículo se mencionara las siguientes.

3.1. Captura de Pantalla

En Linux se utiliza el comandoxwd de Windows que captura las ventanas en forma individual, tanto como las pantallas completas su sintaxis es la siguiente:

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

Y para ver el contenido se utiliza el comando xwud o algún comando que soporte el formato del archivo.

xwud –in pantalla.xwd

3.2. Captura de la Memoria

Todo se trata como un fichero en Linux lo que facilita el copiar y analizar el contenido tanto de la memoria principal, como del área de swap realizando el análisis en la partición correspondiente, también se puede utilizar los comandos string o grep cuya sintaxis es:

strings /dev/mem | more

Es de gran importancia estar enterado que la memoria el dispositivo es volátil, por esto es imposible verificar que la captura de datos es exactamente igual al original, porque en realidad al capturar los datos ya se modifican en una pequeña proporción.

3.3. Análisis de Conexiones de Red

Al analizar la red nos puede proporcionar información importante acerca de las conexiones y los procesos en ejecución. Para esto en Linux existe un comando netstat que muestra la información de la red del sistema, y la información de los procesos asociados a la conexión de red se utiliza el siguiente comando con la siguiente sintaxis.

netstat –pan | more

3.4. Copia de Sistemas de Archivos

En Linux existen herramientas que nos son útiles para realizar la copia de los sistemas de archivos como del disco duro, lo que permitirá el análisis de forma segura, si no es posible apagar el disco duro o sacar una copia en un dispositivo extraíble, o al no disponer de un dispositivo de almacenamiento de gran capacidad, Linux nos da la opción de poder realizar la copia del disco duro, particiones y sistemas de archivos a un sistema remoto utilizando el comando netcat o también nc. El comando mount nos permite ver los archivos actualmente montados en el sistema.

El comando fdisk lo que hace es desplegar en pantalla las particiones de cada unidad de disco y si están montadas o no actualmente, cuya sintaxis es:

fdisk –l /dev/hda

Y el comando dd que crea copias bit a bit de los sistemas de archivos, su sintaxis es:

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

Y la combinación de los comandos dd y netcat permite transferir imágenes completas de sistemas atreves de la red, y para verificar que la copia generada es autentica podemos utilizar el comando md5sum.

3.5. Acceso a los datos del Sistema de Archivos

Al tener la imagen generada de los archivos de sistema, Linux nos permite analizar el contenido, Linux posee un dispositivo virtual que permite acceder a las imágenes de los archivos de sistemas. Para poder utilizar este dispositivo es necesario crear un archivo en donde se debe montar, con la siguiente sintaxis.

mkdir /tmp/analisis

//y para montar

mount –t ext2 –o loop -r fichero.con.imagen /tmp/análisis

Al finalizar este procedimiento el sistema puede ser tratado como cualquier otro sistema de archivos, se debe tomar nota de que se debe cargar en forma de lectura exclusiva pues evitara dañar la evidencia.

4. CORONER'S TOOLKIT TCT

Coroner's Toolkit (o el "TCT") es una suite de aplicaciones escritas por Dan Farmer y Wietse Venema para IBM sobre un estudio forense de equipos comprometidos. El cual se divide en diferentes aplicaciones.

grave-robber. Una utilidad para capturar información sobre datos, para luego pueda ser procesada por el programa mactime del mismo toolkit.

unrm y lazarus. Herramientas para la recuperación de archivos borrados (logs, RAM, swap, etc.). Estas aplicaciones identifican y recuperan la información oculta en los sectores del disco duro.

mactime. El programa para visualizar los ficheros/directorios su timestamp MAC (Modification, Access, y Change).

Las herramientas son muy útiles para el análisis, la función más simple de grave-robber es la de escanear los ficheros con la función stat(), para obtener la información de los archivos. Para realizar esta función primero crea una carpeta /data en un directorio nombrado como el host de la maquina, allí almacena los datos recolectados. Luego el programa mactime ordena los resultados y los despliega en pantalla, según el tiempo y así crear un listado. Y desde el mismo podremos sacar algunas conclusiones sobre la actividad que ha sido afectada por el intruso o los movimientos que realizo el mismo durante el tiempo que estuvieron en el sistema, algo de lo que podríamos verificar es por ejemplo la instalación de caballos de troya, backdoors, sustitución de ficheros del sistema operativo legítimos, también la creación de directorios ocultos, compilación de aplicaciones, etc.

5. SU INSTALACIÓN

Ahora se describirá paso a paso el funcionamiento del sistema

Primero debemos instalar la aplicación en una unidad con suficiente espacio para poder trabajar con libertad.

Luego realizamos la limpieza de la distribución con el comando make all.

Realizamos el montaje de la partición a analizar en modo solo lectura

mount -r /dev/hdd2 /mnt

Después empezamos activando la herramienta graver-robber para empezar a analizar el sistema utilizando la siguiente sintaxis

bin/grave-robber -m /mnt

Se iniciara con el análisis de todas las carpetas que están en el $Path y la partición montada. Después del análisis se debe realizar la copia de los ficheros passwd y group al directorio tct-1.09/ para utilizarlos mas adelante.

Luego se ejecuta la herramienta mactime dándole una fecha anterior a la del suceso, los resultados se deben copiar a un fichero para facilitar el análisis , cuya sintaxis es la siguiente:

bin/mactime -p passwd.victim -g group.victim /mnt 06/01/2000 > victim.mactime

Se observa que se guarda con el nombre victim.mactime, realizamos una copia de seguridad para empezar el análisis que llevara el nombre de victim.mactime.evidence, utilizando algún editor de texto empecemos a analizar el mismo.

Ejemplo : Análisis de fichero

Feb 13 2000 01:10:50 50148 mca -rwxr-xr-x root root /x/dev/.

Feb 13 2000 01:10:52 564 m.c -rw-r--r-- root root /x/etc/profile

Feb 13 2000 01:11:00 5 mac -rw-r--r-- root root /x/lib/sp

18110 .a. -rw-r--r-- root root /x/lib/tp

[MARK]

Feb 13 2000 01:12:08 0 ..c -rw-r--r-- root root /x/dev/ttyag

25 ..c -rwxr-xr-x root root /x/dev/ttyfg

23 ..c -rwxr-xr-x root root /x/dev/ttypg

373176 ..c -rws--x--x root root /x/lib/...

8268 ..c -rwxr-xr-x root root /x/lib/go

20164 ..c -rwsr-xr-x root root /x/usr/bin/xcat

183780 ..c -rwxr-xr-x root root /x/usr/sbin/find

Feb 13 2000 01:30:00 8268 .a. -rwxr-xr-x root root /x/lib/go

Feb 14 2000 10:42:03 1166856 .a. -rw-r--r-- root root /x/var/log/boot.log

[MARK]

Feb 14 2000 10:45:35 18110 m.c -rw-r--r-- root root /x/lib/tp

Feb 14 2000 10:57:42 2998 m.c -rw-r--r-- root root /x/etc/inetd.conf~

Feb 14 2000 11:01:47 168 .a. -rw-rw-r-- root root /x/root/.saves-1380-dragon~

Feb 14 2000 11:18:38 160 m.c -rw-r--r-- root root /x/etc/hosts.allow.old

Feb 14 2000 11:18:55 347 m.c -rw-r--r-- root root /x/etc/hosts.deny.old

Feb 14 2000 11:19:08 8 m.c -rw-r--r-- root root /x/etc/hosts.deny

Feb 14 2000 11:22:53 168 m.c -rw-rw-r-- root root /x/root/.saves-1380-dragon~

Feb 14 2000 11:30:30 2998 .a. -rw-r--r-- root root /x/etc/inetd.conf~

[MARK]

Feb 14 2000 11:31:25 20164 .a. -rwsr-xr-x root root /x/usr/bin/xcat

Feb 14 2000 11:34:10 868 m.c -rwxr-xr-x root root /x/etc/rc.d/rc.local

Puede que no descubramos nada al principio pero después de una búsqueda exhaustiva, mediante cambios de fecha durante varios intentos un buen tiempo de búsqueda, posiblemente se hallará lo que se sospechaba: una intrusión.

Podemos mencionar que esta herramienta ya es utilizada en al ámbito de la investigación forense informática.

6. CONCLUSIONES

Con la finalidad de lograr una recogida óptima y rápida de la evidencia digital, que puede ser sometida al borrado intencionado o no, se ha considerado que no necesariamente herramientas compatible con software propietario sean utilizados para este tipo de procedimientos, sino también se han ido desarrollando herramientas de código abierto que cubren áreas que normalmente no se consideran, un ejemplo de herramienta es la que se ha descrito en este artículo.

7. REFERENCIAS

[1]BurnEye Nivel1 http://www.activalink.com/reviews/elf.php y http://www.phrack.com/show.php?p=58

[2]Brian Carrier “File System Forensic” Analysis

[3]Brian Carrier "TCTUTILS"/"TASK" http://www.cerias.purdue.edu/homes/carrier/forensics/

[4]Peter Stephenson .Investigating ComputerRelated Crime. In Linux.