

Autopsy y Sleuthkit, Kit de Herramientas para el Forense Digital

Tras la Pista del Zorro

Sleuthkit busca en los sistemas de ficheros de Microsoft y Unix ficheros borrados y reconstruye los hechos para localizar una intrusión. Autopsy Forensic Browser [1] no es sólo fácil de usar, sino que también proporciona funciones avanzadas: este interfaz basado en web de Sleuthkit facilita y documenta el proceso de análisis forense.

Nuevos Casos

Basaremos nuestros ejemplos en el sistema de ficheros Forensic Challenge [3]. El tarball contiene la partición individual como aparece descrita en la Tabla 1.

Antes de empezar la investigación con Autopsy y Sleuthkit, los investigadores forenses tienen que abrir un nuevo caso. Para hacerlo, simplemente hay que hacer clic en el botón *New Case* al pie de la página de bienvenida.

Para determinar si un sistema está expuesto, el administrador tiene que buscar señales reveladoras y pruebas seguras, el administrador se convierte en un científico forense. Sleuthkit y Autopsy pueden ayudar con esta complicada tarea haciendo uso de una práctica interfaz Web para buscar archivos borrados y descubrir la pista de los intrusos. **POR RALF SPENNEBERG**

da de Autopsy. Haciéndolo, se abre la página de entrada para el nuevo caso (véase la Figura 2).

Una vez que se hayan rellenado todos los campos y pulsado *New Case*, Autopsy creará el directorio del caso (*/var/morgue/forensic_challenge/*) y el fichero de configuración (*/var/morgue/forensic_challenge/case.audit*), además de añadir al investigador. La herramienta muestra los resultados en otra página Web y le pide que lo confirme pulsando *OK*.

En la siguiente ventana (*Case Gallery*, Figura 3), Autopsy presenta una lista de casos seleccionables; incluso se puede acceder a esta página desde la página de bienvenida pulsando el enlace *Open Case*. El caso *forensic_challenge* está seleccionado por defecto; después de hacer clic en *OK* para confirmar la selección, es el momento de añadir las máquinas que se desean investigar en este caso.

Bajo la lupa

Para añadir un nuevo host hay que especificar el nombre de la máquina y opcionalmente se puede añadir una descripción, adicionalmente se puede indicar el huso horario y la desviación del reloj del ordenador con respecto al tiempo real, si fuera necesario. También se puede especificar, si se tiene, una base de datos hash de ficheros benignos o malignos. A continuación hay que pulsar *Add Host* y Autopsy mostrará de nuevo una página de confirmación. Púlsese *OK* para aceptar.

A continuación se muestra la *Host Gallery*, permitiendo seleccionar los hosts que van a ser procesados; otra vez hacemos clic en *OK* para confirmar antes de continuar añadiendo las imágenes de disco. Para ello, hay que seleccionar *Add Image* y teclear el nombre del fichero (véase la Figura 4).

Este formulario se utiliza también para especificar si Autopsy debe añadir un enlace simbólico para el fichero original en el directorio *morgue* o si la imagen debe ser copiada o movida. También hay que especificar el punto de montaje original, el tipo de sistema de ficheros y las opciones MD5. Autopsy calcula la suma de verificación MD5 en cada caso; si ya conoce cual debería ser dicho valor, se puede introducir aquí, para que Autopsy lo verifique con el valor de real.

Registro del 7 de Noviembre de 2000

Ahora se puede continuar con la investigación de la escala temporal de las modificaciones del sistema de ficheros seleccionando el elemento del menú *File Activity Time Lines*. Haciéndolo se cambia la apariencia de la aplicación Web, dividiendo la ventana en dos marcos. El marco

Tabla 1: Particiones de Challenge

Partition	Filesystem
<i>/dev/hda8</i>	<i>/</i>
<i>/dev/hda1</i>	<i>/boot</i>
<i>/dev/hda6</i>	<i>/home</i>
<i>/dev/hda5</i>	<i>/usr</i>
<i>/dev/hda7</i>	<i>/var</i>
<i>/dev/hda9</i>	swap

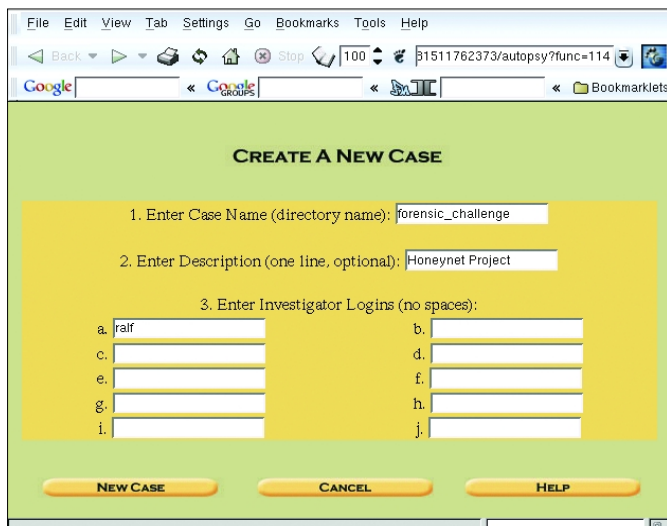


Figura 2: Hay que especificar el nombre del nuevo caso (*forensic_challenge* en nuestro ejemplo) y añadirle un login para el investigador responsable para este caso (*ralf*).

superior muestra los pasos típicos como los elementos del menú y el marco inferior se usa para las entradas y las salidas.

La Figura 5 muestra como crear el llamado fichero de “body” usando el elemento del menú *Create Data File*. Este proceso puede tardar un poco, ya que Autopsy tiene que invocar los comandos *fls* e *ils* de Sleuthkit. Después de completarse estos pasos, Autopsy automáticamente calcula las sumas de comprobación MD5 que se utilizan para comprobar la integridad de los ficheros.

menú *Create Timeline* indica con prudencia que se restrinja la ventana de tiempo que se va a investigar.

La descripción de *Forensic Challenges* indica que el 7 de Noviembre del 2000 es la fecha más probable de la intrusión. Para este ejemplo, el investigador querrá restringir la ventana del tiempo para detallar de forma más precisa las investigaciones en el período entre el 7 y el 9 de Noviembre de 2000. Para permitir a Autopsy reemplazar el UID y el GID con los nombres correspondientes cuando se cree la línea temporal, hay que establecer la

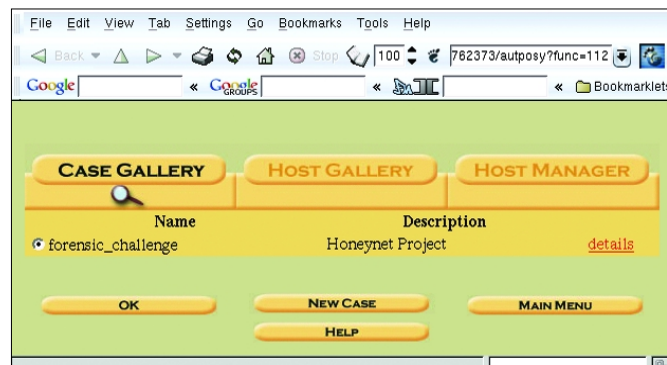


Figura 3: Autopsy organiza las investigaciones forenses en casos. Esto permite cambiar de caso sin tener que reiniciar la GUI.

A continuación Autopsy crea la línea temporal basada en el fichero “body”. El elemento del

imagen del sistema de ficheros que contenga los ficheros */etc/passwd* y */etc/group*.

La línea temporal muestra que el fichero */etc/hosts.deny* ha sido modificado, reduciendo su tamaño a 0 bytes. Unos pocos minutos después, un fichero tarball fue instalado en el directorio */usr/man/.Ci/* (véase la Figura 6). Este es el directorio en el que el investigador forense querrá concentrarse después. Unos pocos segundos antes de que esta instalación tuviera lugar, el inodo 8 133 en *hda8* fue borrado. El tamaño del fichero era de 2.129.920 bytes, y pertenecía a un usuario llamado *drosen*. Un fichero en el rootkit fue borrado después, el fichero en el inodo 109.801 con un tamaño de 1.153 bytes.

La línea temporal también muestra los accesos de lectura a las bibliotecas de

Instalación y ejecución de Autopsy

Autopsy no sólo realiza análisis, sino que también ayuda al investigador a realizar las tareas de papeleo que el análisis forense conlleva, organizando las tareas en casos y asignándole un directorio a cada uno. Es una buena idea crear un directorio padre para los directorios de los casos antes de empezar con el proceso de instalación: */var/morgue* es un buen nombre para el almacén de pruebas.

La instalación de Autopsy es algo extraña. Después de ejecutar *make*, hay que contestar una o dos preguntas. El script de instalación comprueba si una versión de Sleuthkit está instalada antes de crear los ficheros de instalación.

Cuando se lanza la herramienta, tecleando *.autopsy* en el directorio

fuente, el Autopsy Forensic Browser se activa mostrando su número de versión, una URL y

```
Terminal <3>
/opt/forensik/autopsy-1.73 # mkdir /var/morgue
/opt/forensik/autopsy-1.73 # make

Autopsy Forensic Browser Installation

perl found: /usr/bin/perl
strings found: /usr/bin/strings
Testing decimal offset flag of strings: PASS
Testing non-object file arguments: PASS
grep found: /usr/bin/grep

Enter The Sleuth Kit Directory:
/opt/forensik/sleuthkit-1.64
Sleuth Kit bin directory was found
Required version found

Do you have the NIST National Software Reference Library (NSRL)? (y/n) [n]

Enter the Evidence Locker Directory (where cases will be saved):
/var/morgue
/var/morgue already exists

Settings saved to conf.pl

/opt/forensik/autopsy-1.73 #
```

Figura 1: Tecleando *make* se compila e instala Autopsy, pero hay que estar preparado para contestar algunas preguntas. Tiene sentido crear el directorio *morgue* antes de empezar la instalación.

un mensaje indicando que se debe dejar este proceso ejecutándose durante la fase de análisis y que hay que pararlo cuando termine dicha fase pulsando [Ctrl]+[C].

A continuación, con cualquier navegador Web, se puede acceder a Autopsy. Tan sólo hay que introducir la URL mostrada anteriormente en el cuadro de texto de la barra de direcciones del navegador Web. También se pueden usar opciones de la línea de comandos para indicarle a Autopsy que se ejecute en otro puerto y dirección IP: *.autopsy <número de puerto> <dirección IP>*.

Si se prefiere usar los paquetes RPM del autor [2] para instalar Autopsy, en vez de usar los fuentes, se dará cuenta que *autopsy* se incluye en el path por defecto. Este paquete usa */var/morgue* como almacén de pruebas.

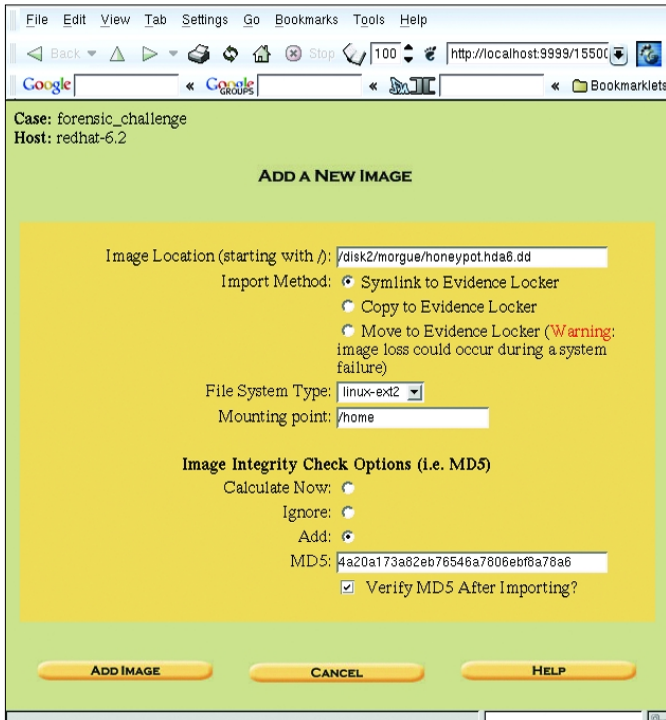


Figura 4: Antes de investigar una imagen del sistema de ficheros, el investigador ha de añadir la imagen al caso, especificando la suma de control MD5 para asegurarse que la imagen no esté dañada.

funciones. Este hecho indica que el intruso compiló una o varias aplicaciones.

Ningún Punto para Encubrir Pistas

Después de completar la instalación el intruso borró una enorme cantidad de ficheros. Parece que estos ficheros fueron creados como parte del proceso de compilación. Tras borrar los ficheros superfluos, el intruso parece que instaló una distribución SSH (véase el Listado 1).

La línea temporal también indica que el intruso usó scripts de instalación para tomar el control e instalar software. Dicha línea contiene un número de entradas que indican el borrado de ficheros que nos hace mantener esta hipótesis: *install-sshd1* y parecidos (véase el Listado 2).

Los ficheros mostrados aquí no son las únicas entradas sospechosas de la línea tem-

poral. A lo largo del curso del ataque, parece que el intruso dejó una copia del cliente “Bitch X IRC” y “eggdrops” en el disco.

Ahora la tarea del administrador-detective consiste en descubrir la naturaleza y el propósito de los ficheros instalados. Los scripts de instalación son siempre un buen punto de partida. El intruso los ha borrado, pero Autopsy no tiene ningún problema en recuperarlos.

Para recuperarlos, primero hay que cerrar la línea temporal (arriba a la

derecha *Close*) y seleccionar la partición */usr*. Tras confirmar pulsando *OK* se muestra una nueva vista, donde hay que seleccionar *File Analysis*. Este es el sitio donde se pueden mostrar los ficheros individuales, como el llamado */usr/man/.Ci/install* (véase la Figura 7).

Procesos Ocultos

Afortunadamente, Autopsy también permite el visionado de otros tipos de ficheros. Por ejemplo, */usr/man/.Ci/addps* contiene un script que obviamente ha sido usado para ocultar procesos que normalmente se muestran con los comandos *ps* o *top* para de

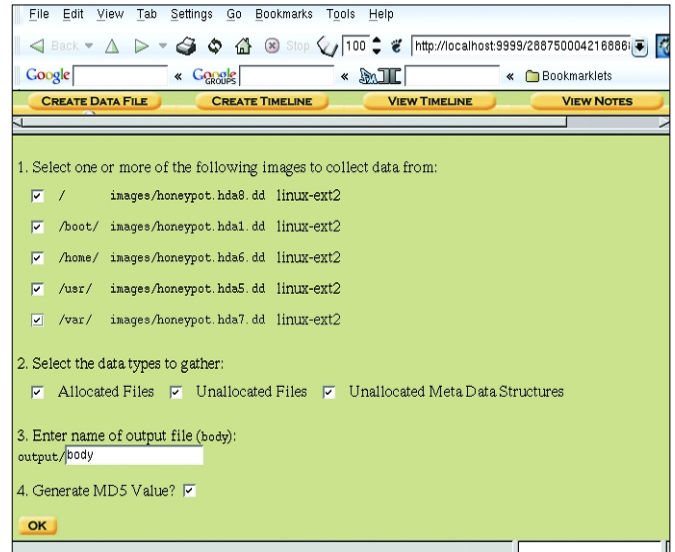


Figura 5: Autopsy crea un fichero “body” para almacenar la línea temporal para las operaciones sobre el sistema de ficheros de la imagen. El “body” se puede aplicar tanto a los ficheros borrados como a los existentes.

Listado 1: Instalación de SSH

```
01 537 m.c -/-rw----- root root 26570 /etc/ssh_host_key
02 880 .a. -/-rw-r--r-- root root 26579 /etc/ssh_config
03 512 m.c -/-rw----- root root 2048 /root/.ssh/random_seed
04 341 mac -/-rw-r--r-- root root 26578 /etc/ssh_host_key.pub
05 ...
06 604938 mac -/-rws--x--x root root 109999 /usr/local/bin/ssh1
```

Listado 2: Scripts de Instalación

```
01 1153 ..c -/-rwxr-xr-x 1010 users 109801 /usr/man/.Ci/install-sshd1 (deleted)
02 1076 ..c -/-rwxr-xr-x 1010 users 109802 /usr/man/.Ci/install-sshd (deleted)
03 80 .a. -/-rwxr-xr-x 1010 users 109803 /usr/man/.Ci/install-named (deleted)
04 71 ..c -/-rwxr-xr-x 1010 users 109867 /usr/man/.Ci/install-wu (deleted)
05 106 ..c -/-rwxr-xr-x 1010 users 109864 /usr/man/.Ci/install-statd (deleted)
06 ...
```

este modo evitar ser detectados. El atacante parece que ha reemplazado los comandos estándar del rootkit por variantes. El contenido del fichero es el siguiente:

```
#!/bin/sh
HIDE=$1
echo "hiding $HIDE from ps/top"
/bin/echo "2 $HIDE" >>/dev/ptyp
```

Los comandos *ps* y *top* modificados leen */dev/ptyp* con el objetivo de ocultar estos procesos. El fichero contiene las siguientes entradas:

```
2 slice2
2 sniff
2 pscan
2 imp
3 qd
...
```

El análisis del comando *ps* con *strings* o con la interfaz Autopsy, muestra que este comando contiene la cadena */dev/ptyp*. Esto demuestra nuestra hipótesis previa, ya que la versión original del comando *ps* no lee este archivo.

Troyanos

El servidor SSH instalado por el atacante es otro fichero interesante. */usr/local/sbin/sshd* contiene una referencia a */usr/tmp/nap*. La referencia es fácil de localizar. Tan sólo hay que mirar al carácter separador *.* */usr/tmp* es un enlace simbólico a */var/tmp*. El fichero */var/tmp/nap* contiene la siguiente información:

```
username: root password: 2
twllightz0ne hostname: 2
c871553-b.jffsn1.mo.home.com
```

En otras palabras, el servidor SSH instalado por el intruso almacena cualquier contraseña que recibe en formato texto.

Funciones Avanzadas

Autopsy proporciona un número adicional de funciones, tales como búsquedas de palabras claves, clasificación de ficheros por tipo y acceso directo al contenido de los ficheros. Una de las mayores ventajas de usar Autopsy es la posibilidad de calcular las sumas de control MD5 al vuelo y de añadir comen-

Date	Time	Permissions	Size	UID	GID	Inode	Filename
Nov 2000	14:51:37	m..-rw-r--r--	8133	drosen	drosen	8133	<honeypot.hda8.dd-dead-8133 >
Nov 2000	14:51:53	.a. -/rwxr-xr-x	1010	users	109832	109832	/usr/man/.Ci/scan/x/x
	1760	.a. -/rwxr-xr-x	1010	users	109829	109829	/usr/man/.Ci/scan/bind/ibind.sh
	15092	.a. -/rwxr-xr-x	1010	users	109836	109836	/usr/man/.Ci/scan/x/pscan
	4096	.a. d/drwxr-xr-x	1010	users	109841	109841	/usr/man/.Ci/scan/port/strobe
	1259	.a. -/rwxr-xr-x	1010	users	109834	109834	/usr/man/.Ci/scan/x/xfil
	4096	.a. d/drwxr-xr-x	1010	users	109831	109831	/usr/man/.Ci/scan/x

Figura 6: Reconstrucción de Autopsy de un rootkit. Las columnas contienen las fechas y horas, tamaños, acciones (*a* para access, *m* para modify), privilegios, UID, GID, número de inodos y nombres de los ficheros en cuestión.

File Name	Permissions	Size	Date
r/r inetd		147900	2000.06.03
r/r install-named		80	2000.06.03

Contents of File: /usr/man/.Ci/install-named

```
gunzip named.tgz;tar -xvf named.tar
cd bin
./install
cd ..
rm -rf bin named.tar
```

Figura 7: El módulo de análisis de ficheros de Autopsy permite mostrar cualquier fichero del sistema de ficheros, incluso los borrados (resaltados en rojo). El panel inferior de la derecha muestra el contenido del fichero borrado *install-named*

tarios. Un investigador tiene que ser extremadamente disciplinado para conseguir esta funcionalidad solamente haciendo uso de la línea de comandos.

Los desarrolladores de Autopsy están actualmente trabajando en rutinas de búsqueda indexadas para la característica de búsqueda de palabras claves. Tan sólo hay que crear una vez un archivo índice, para acelerar cualquier búsqueda. Una búsqueda que tarda 168 segundos actualmente, tardaría tan sólo 2 segundos con el uso de la nueva técnica.

Conclusión

La combinación de Sleuthkit con Autopsy Forensic Browser proporciona

un conjunto de herramientas bastante potentes para la realización de análisis forenses. Sus características y servicios son comparables con las herramientas comerciales. El hecho de que sea de código abierto permite a los investigadores seguir el rastro de los progresos de la herramienta en detalle.

RECURSOS

- [1] Autopsy Forensic Browser: <http://autopsy.sfn.net>
- [2] Paquetes RPM Autopsy y Sleuthkit: <http://www.spennenberg.org/Forensics/>
- [3] Ficheros del Desafío Forense: <http://project.honeynet.org/challenge/images.html>