

Detección de intrusiones basada en Host con Samhain

EN GUARDIA

Samhain notifica a los usuarios de los intentos de intrusión e incluso puede enviar ficheros de registro a un servidor central.

POR TIM SCHÜRMAN

Las grandes empresas no sólo cierran las puertas de noche, también contratan vigilantes de seguridad. El vigilante hace rondas regulares por las instalaciones y hace sonar la alarma si sucede algo inusual. Evidentemente, usted no va a contratar a un vigilante para que vigile a su ordenador, pero puede utilizar un cortafuegos para cerrar todas las puertas y esperar a que las actualizaciones regulares cierren cualquier posible vulnerabilidad.

Los sistemas modernos son complejos y los atacantes están encontrando constantemente puertas que se hayan podido quedar abiertas. Una vez que el atacante haya entrado en el sistema, intentará esconderse de los usuarios y administradores, normalmente instalando un rootkit. Este rootkit dejará trazas y Samhain, el vigilante electrónico, las detectará y hará sonar la alarma.

Sniffer

Samhain asegura la integridad de un sistema Linux realizando comprobaciones regulares de los ficheros para ver si han sido modificados. Para hacerlo genera una única suma de comprobación, o huella, para cada fichero que monitoriza. Esta huella cambia si el fichero es manipulado mediante malware. Samhain comprueba las huellas y otros atributos críticos de los ficheros a intervalos regulares y alerta a los administradores si encuentra alguna desviación. Si fuera

necesario, también puede monitorizar las conexiones y desconexiones de los usuarios en el sistema, buscar programas en el sistema con SUID y monitorizar el kernel en busca de cambios. Samhain también puede informar de eventos sospechosos; además de mantener un fichero de registro clásico, enviará sus registros a un servidor de registros central o los enviará por correo al administrador.

Samhain sólo monitoriza el ordenador local y funciona como un sistema de detección de intrusiones basado en host (HIDS) [1]. Al contrario que sus alternativos, los IDS basados en la red (NIDS) [2], Samhain ignora el tráfico de red entrante y saliente. La herramienta no dispara ninguna alarma hasta que el atacante haya comenzado a trastear en el sistema.

Sin embargo, esto no quiere decir que Samhain sea innecesario; si los atacantes logran pasar los controles de acceso, la única forma de identificarlos es confiando en los vigilantes que hacen sus patrullas regulares. Un HIDS es, de esta forma, la única manera de descubrir las intrusiones desde dentro de la LAN, es decir, de la gente que trabaja para nuestra empresa.

Como se puede imaginar, los delinquentes no aprecian los sistemas de detección de intrusiones y a menudo son el objetivo de los ataques. Samhain usa varias técnicas para protegerse. Por ejemplo, puede esconder su propio proceso y sólo aceptará órde-

nes con una contraseña que se haya configurado para este fin.

La Instalación

Samhain se distribuye bajo GPL y se encuentra disponible para su descarga desde el sitio web del proyecto [3]. Aunque a menudo lo encontrará en el repositorio de paquetes de su propia distribución, no es buena idea usarlos. Por un motivo, estos paquetes normalmente están obsoletos (como es el caso de, digamos, Ubuntu 9.04), y por otra razón más, es muy difícil o imposible comprobar el origen y la integridad del programa.

Si sigue las instrucciones comprobará que la instalación de Samhain es inicialmente bastante simple. Sólo hay que descomprimir el programa en el disco tras descargarlo; aparecerá el paquete con el código fuente y una firma PGP. Antes de seguir adelante sería buena idea verificar la firma PGP:

```
gpg --keyserver pgp.mit.edu --recv-key 0F571F6C
gpg --verify samhain-<versión>.tar.gz.asc
samhain-<versión>.tar.gz
```

La firma es la del autor de Samhain, Rainer Wichmann; también se puede descargar la huella desde [1]. Si todo es correcto, se puede continuar con el proceso normal:

```
./configure
make
make install
```

Si desea ejecutar Samhain directamente como un servicio que se ejecute en el inicio del sistema,

```
make install-boot
```

lo conseguirá. Desafortunadamente, esto es sólo el comienzo, como gradualmente muestra la documentación de Samhain. En la mayoría de los casos habrá que recompilarlo con diferentes opciones con el comando *configure*, especialmente si se quiere instalar en múltiples ordenadores – otra razón por la que se debe comenzar con el código fuente y no desde un paquete precompilado de la instalación. La Tabla 1 muestra los parámetros de *configure* más importantes. Antes de habilitarlos debería familiarizarse con el fichero de configuración.

Filtro de Café

Samhain monitoriza los ficheros del sistema Linux y dispara la alarma si alguno ha cambiado. Sin embargo, muchos ficheros tienen que cambiar durante su uso normal. Por ejemplo, los ficheros de registro crecen, los ficheros temporales aparecen en */tmp* y los usuarios trabajan con sus documentos OpenOffice modificando sus marcas de tiempo. Si Samhain tuviera que informar de todos estos eventos, los ataques se verían ocultos entre tantos datos de poco valor. Por tanto, es buena idea decirle qué ficheros tiene que monitorizar y de qué actividades debe informar antes de ejecutar la herra-

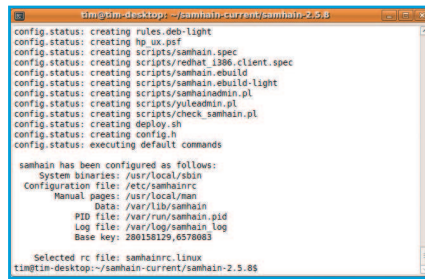


Figura 1: Cuando se compila el código fuente, configure crea una clave base, la cual se añade a cada correo electrónico que envíe. Se puede utilizar el comando "samhain -M /ruta/al/fichero" para comprobar el origen de los correos almacenados.

amienta. Para ello se utiliza el fichero de configuración */etc/samhainrc*. La plantilla por defecto parece bastante compleja, pero proporciona un punto de partida útil a partir del cual añadir nuestras propias preferencias.

Al igual que los antiguos ficheros INI de Windows, el fichero de configuración incluye secciones que comienzan con un nombre encerrado entre corchetes. Cada opción es un par *opción-valor*; Samhain ignora las líneas que comienzan con el símbolo almohadilla (#).

Para comenzar, se define dónde debe enviar Samhain los avisos. Esto nos lleva a la sección *[Log]* con la opción *...Severity* para las opciones de salida. Por ejemplo, *LogSeverity* almacena los mensajes en un fichero de registro, *MailSeverity* utiliza el correo, *PrintSeverity* imprime la información en la consola y *syslogSeverity* usa Syslog.

Para activar uno de estos posibles destinos de las notificaciones sólo hay que quitarle el

símbolo de la almohadilla y especificar cómo debe de ser de serio el mensaje para que se utilice esta opción. Por ejemplo, especificando

```
LogSeverity=err
```

el fichero de registro sólo contendrá errores, problemas críticos y los propios fallos de Samhain. La Tabla 2 lista los niveles de gravedad y sus contenidos. Si desea que Samhain envíe alertas por correo, hay que encontrar la sección *[Misc]* (cuidado: la configuración de ejemplo posee múltiples secciones con este nombre) e introducir los datos del Listado 1.

El fichero de registro se almacena en */var/log/samhain_log* por defecto. Se le puede pasar otra ruta en la etapa de configuración con la opción *—with-log-file = /ruta/al/fichero* o añadir

```
SetLogfilePath = Z
/ruta/al/fichero
```

en la sección *[Misc]*.

Políticas

El siguiente paso consiste en indicarle a Samhain cómo tiene que monitorizar los ficheros y directorios. Las siguientes líneas le indican que dispare la alarma si alguien intenta acceder a */my/file.txt*, */important/folder* o a */var/logs/a.log* por cualquier motivo excepto la lectura:

```
[ReadOnly]
dir=/important/folder
```

Tabla 1: Parámetros Configuración Relativos a la Seguridad

Parámetro	Significado
<i>--with-kcheck=/boot/System.map-\$(uname -r)</i>	Le indica a Samhain que compruebe el kernel. Supone que el fichero <i>/dev/kmem</i> es accesible.
<i>--enable-login-watch</i>	Le indica a Samhain que monitorice las conexiones y desconexiones de usuarios.
<i>--enable-suidcheck</i>	Le indica a Samhain que informe de ficheros que recientemente hayan activado el bit SUID o GID.
<i>--enable-install-name=NAME</i>	Renombra Samhain a NAME; todos los ficheros relacionados y las carpetas se renombrarán adecuadamente (<i>etc/NAMErc</i> , etc).
<i>--enable-nocl=ABC</i>	Samhain sólo ejecutará una acción si el primer argumento de la línea de comandos es ABC. Por ejemplo, <i>samhain ABC -t check</i> ejecutará una comprobación. Esto impide que otros programas puedan controlar remotamente a Samhain.
<i>--enable-micro-stealth=number</i>	Las cadenas del código fuente son invisibles para los comandos de cadena. Esto dificulta que Samhain sea encontrado por un atacante. <i>number</i> debe ser un entero comprendido entre 127 y 255.
<i>--enable-stealth=number</i>	Al contrario que <i>--enable-micro-stealth=number</i> , esta opción cambia las cadenas del fichero de registro y de la base de datos de Samhain. Para ver los ficheros de registro, hay que utilizar el comando <i>samhain -jL /ruta/al/fichero less</i> . Al mismo tiempo, el fichero de configuración se cifra esteganográficamente en un fichero de imagen PostScript. La herramienta <i>samhain_stealth</i> se encarga de ello. <i>number</i> debe ser un entero comprendido entre 127 y 255.
<i>--enable-khide=/boot/System.map-\$(uname -r)</i>	Crea un módulo del kernel que esconde todos los procesos y ficheros con la cadena <i>samhain</i> .
<i>--enable-static</i>	Enlaza Samhain estáticamente. Esto hace que el fichero sea más grande pero impide que Samhain se pueda ver comprometido por las librerías dinámicas.

```
file=/my/file.txt
file=/var/logs/a.log
```

Las rutas han de ser absolutas. [ReadOnly] le indica a Samhain que lo único que está permitido modificar de los ficheros que se listan es su fecha de acceso. Sin embargo, observe el siguiente fallo: El fichero de registro sigue creciendo; el IDS genera múltiples falsos positivos. Esto es porque hay que mover *a.log* a la sección especial [GrowingLogFiles]. El Listado 2 muestra el resultado.

Samhain se refiere a [ReadOnly] y [GrowingLogFiles] como políticas. La Tabla 3 muestra qué otras políticas tiene definida el IDS.

Si se desea que Samhain no busque por debajo de cierto nivel de anidamiento en los directorios, se puede añadir este número a la ruta:

```
dir=3/important/folder
```

Para ignorar los subdirectorios puede establecerse una profundidad recursiva de -1 en la política [IgnoreAll] del siguiente modo:

```
[IgnoreAll]
dir=-1/important/folder/exclude
```

Como se muestra al comienzo del fichero de configuración, algunas secciones pueden aparecer múltiples veces. Samhain simplemente las mezcla conforme las va evaluando, pero es buena idea mantener los directorios por defecto, ya que definen algunas reglas básicas para los ficheros más importantes del sistema Linux.

Samhain es bastante delicado con respecto a los privilegios de acceso de sus propios ficheros críticos – esto se aplica especialmente al fichero de configuración. Sólo el

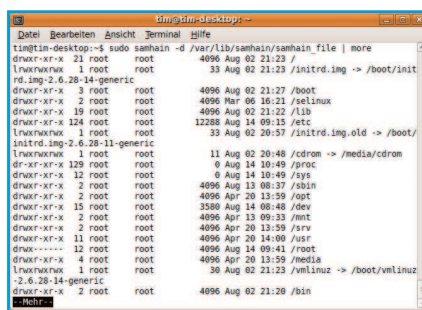


Figura 2: El comando "samhain -d /ruta/a/la/basededatos" lista el contenido de la base de datos de firmas; el formato de salida es una reminiscencia de "ls -l".

root y el usuario cuyo ID de su cuenta utiliza Samhain poseen permisos de escritura. Si necesita que alguien más modifique la configuración, habrá que configurar los usuarios "trusted" (de confianza). Para ello hay que especificar la UID con la opción de configuración `--with-trusted = 0, <uid>, <uid>, ...`. Para impedir la manipulación, se deberían mantener las opciones por defecto, es decir, el usuario root es el único que tiene los privilegios y el comando se ejecuta como root.

Cifras

Una vez que se haya completado la configuración, Samhain tiene que leer los ficheros que se desean monitorizar una vez, crear una suma de comprobación única y tomar nota de las otras características de los ficheros. El siguiente comando dispara el proceso de inicialización:

```
samhain -t init
```

Dependiendo del número de ficheros que se quieran monitorizar, probablemente desee ahora hacer un descanso y tomarse un café. La información que Samhain recolecta se almacena en la base de datos que se encuentra en `/var/lib/samhain/samhain_file` por defecto. Si este fichero existe, Samhain le añadirá al final los datos.

Dicho de otro modo, no debería usar el comando anterior para actualizar la base de datos. Un comando similar proporciona la actualización:

```
samhain -t update
```

A propósito, Samhain utiliza el algoritmo TIGER192 para calcular las sumas de comprobación. Las opciones alternativas aquí son SHA-1 y MD5; se pueden seleccionar cambiando la opción `DigestAlgo` del fichero

de configuración. El autor de Samhain sugiere que se evite MD5 debido a posibles vulnerabilidades.

Una vez que haya configurado la base de datos, se puede comprobar la integridad del sistema con el comando:

```
samhain -t check
```

Esto le indica a Samhain que analice de nuevo el sistema y, para cada fichero, se asegure de que la suma de comprobación y las propiedades de los ficheros coinciden con las entradas de la base de datos. Para automatizar esta comprobación se puede ejecutar Samhain como un servicio. Si se instaló con la opción `make install-boot`, hay que reiniciar el sistema o introducir el comando siguiente:

```
samhain -D -t check
```

El fichero de configuración establece los intervalos de comprobación para el servicio. Puede ser una entrada fija, como

```
SetFilecheckTime = segundos
```

o una entrada al estilo cron:

```
FileCheckScheduleOne = */5*****
```

Como la base de datos con las sumas de comprobación son la base para las futuras comparaciones, es importante que el sistema Linux esté limpio cuando se cree la base de datos. Un vigilante no notará una puerta abierta si está abierta desde el comienzo. Por ello, sería una buena idea instalar Samhain antes de conectar el ordenador a la red.

Listado 1: Configuración Transmisiones Correo

```
01 [Misc]
02 # Recipiente:
03 SetMailAddress =
   name@example.com
04 # Relay, si fuera necesario:
05 SetMailRelay =
   relay.example.com
06 # Siempre envía este número de
   mensajes en un único correo:
07 SetMailNum = 10
08 # Tiempo máximo de lapso (en
   segundos) antes de enviar los
   mensajes:
09 SetMailTime = 86400
10 # Asunto de los correos a
   enviar:
11 MailSubject = Subject
```

Tabla 2: Niveles de Seguridad (Ascendente)	
Nivel	Significado
debug	Errores, sólo para programadores
info	Toda la información
notice	Anuncios
warn	Avisos
mark	Marcas de tiempo
err	Errores
crit	Problemas críticos
alert	Errores que finalizan el programa Samhain
Cada nivel incluye a todos los niveles subordinados, de modo que warn también informará de los errores.	

Además, hay que asegurarse de que nadie acceda a la base de datos. Ni que se almacene en un medio de una única escritura ni en un servidor. El servidor podría recolectar todos los ficheros de registro desde todas las instalaciones de Samhain de la LAN y almacenar los ficheros de configuración por ellos. Los beneficios de esta solución para el administrador consisten en que se centraliza el almacenamiento de todos los ficheros críticos sin que ningún malware en los clientes pueda manipularlos.

Master...

Para configurar un equipo cliente-servidor, primero hay que compilar el programa Yule en el servidor. Afortunadamente, para ello se puede utilizar el código fuente de Samhain. Tan sólo hay que especificar el parámetro de configuración `--enable-network = server`:

```
./configure
--enable-network=server
make
sudo make install
```

Seguido de

```
sudo make install-user
```

para corregir un par de permisos. El servidor de registros `yule` sólo recolecta los datos de los clientes y no realiza ninguna comprobación de integridad sobre ellos. Antes de ejecutar el servidor hay que modificar la sección `[Log]` del fichero de configuración `/etc/yule`. Es idéntico en su mayoría a su equivalente `samhainrc`.

...and Servants

Si desea que sus clientes Samhain envíen sus registros al servidor, tendrá que compilar a los clientes para hacerlo. El parámetro `--enable-network = client` se encarga de esto:

```
./configure
--enable-network=client
--with-logserver=
servidor.ejemplo.com
--with-config-file=
```

Listado 2: Fichero de Configuración (Fragmento)

```
01 [ReadOnly]
02 dir=/important/folder
03 file=/my/file.txt
04
05 [GrowingLogFiles]
06 file=/var/logs/a.log
```

```
REQ_FROM_SERVER
--with-data-file=REQ_FROM
_SERVER/var/lib/samhain/
samhain_file
make
```

Pero no lo instale aún: todavía hay que hacer algo más. El resto de los parámetros de configuración le indican a Samhain que tome su configuración y su base de datos de firmas del servidor, `server.example.com`. `REQ_FROM_SERVER` apunta al servidor de registro; la ruta en `--with-data-file` apunta a la máquina local. Esta configuración es necesaria porque Samhain almacena los resultados de inicialización en un fichero (local) primero. Esta opción apunta al fichero.

Portero

Para impedir que un atacante manipule la información transferida y las firmas, el cliente y el servidor utilizan una conexión segura. Para configurar la conexión, Samhain debe autenticarse contra Yule; el programa necesita para ello una contraseña, que el siguiente comando genera en el servidor (Figura 3):

```
yule -G
```

Una vez que la clave haya sido generada, hay que ir al cliente y presentársela a Samhain:

```
./samhain_setpwd
samhain new <contraseña>
```

La utilidad `samhain_setpwd` se crea cuando se compila Samhain. Esto reemplaza la contraseña generada por Samhain con la nueva. `samhain_setpwd` en realidad modifica el programa binario `samhain` y almacena los resultados en `samhain.new`. Luego, se puede reemplazar la versión existente con este fichero:

```
mv samhain.new samhain
```

Tras completar todos estos pasos, se puede instalar finalmente el IDS en los clientes:

```
sudo make install
```

y luego construir la base de datos de firmas:

```
samhain -t init
```

A continuación hay que copiar manualmente el fichero creado (`/var/lib/samhain_file` si se ha ido siguiendo este ejemplo) a `/var/lib/yule` y renombrarlo con `file.<nombre_ordenador>`. Por ejemplo, si Samhain se está ejecutando en un ordenador llamado `client.example.com`, la base de datos de firmas debería llamarse `file.client.example.com`.

Yule tiene que saber la contraseña del cliente para poder comprobarla. El siguiente comando en el servidor se encarga de ello:

```
yule -P <password>
```

Yule crea una cadena bastante larga y críptica con un conjunto completo de credenciales de autenticación (como se muestra en la Figura 3 en la línea resaltada en negro):

```
Client=
HOSTNAME@123456789123456@
123456789ABC ?
```

Luego hay que añadir esta línea a la última sección del fichero de configuración `yulerc`, `[Clients]`, y reemplazar la cadena `HOSTNAME` con el nombre del equipo del cliente en cuestión, como en:

```
[Clients]
Client=
client.example.com@
123456789123456@123456789ABC?
```

Tabla 3: Políticas Predefinidas

Política	Significado
<code>IgnoreNone</code>	No se permiten cambios
<code>ReadOnly</code>	Sólo se permite modificar la última fecha de acceso
<code>LogFiles</code>	Pueden cambiarse las marcas de tiempo, las sumas de comprobación y el tamaño de los ficheros
<code>GrowingLogFiles</code>	El fichero puede crecer; pueden cambiarse las marcas de tiempo y las sumas de comprobación
<code>Attributes</code>	Samhain informa de los cambios en los propietarios, los grupos y los permisos
<code>IgnoreAll</code>	Samhain sólo comprueba si un fichero existe e ignora todo lo demás
<code>Prelink</code>	Como <code>ReadOnly</code> pero para programas y librerías que fueron modificadas con <code>prelink</code>



Figura 3: Yule ha generado la clave 2D1993AF832288D07, luego ha generado la entrada (resaltada en negro) para su fichero de configuración.

Todos estos pasos deben repetirse para el resto de los clientes si quiere que envíen sus datos a Yule. Finalmente, la sección *[Clients]* de *yulerc* necesita una entrada para cada cliente Samhain. Luego ya se puede ejecutar Yule como un servicio:

```
yule -D
```

Alternativamente, *make install-boot* también ejecutará Yule en el momento del arranque. Yule registra sus propios errores en */var/log/yule/yule_log* por defecto. Además, el servidor genera el fichero *yule.html* en el mismo directorio. El fichero, que se actualiza cada dos minutos, proporciona un informe de estado de los clientes que actualmente se encuentran conectados.

Código de Viena

Cuando un cliente Samhain contacta con Yule, se autentica proporcionándole su contraseña. Tras esto, las dos entidades negocian otra clave por medio de SRP (Secure Remote Password) y utilizan esta clave para el resto de las acciones a realizar. El intercambio de datos se cifra y se envía a través de TCP.

Samhain entonces toma su fichero de configuración. Yule espera que se encuentre almacenado como *rc.<nombre_host>* en */var/lib/yule*; si está siguiendo el ejemplo anterior sería *rc.client.example.com*. Lo mejor es utilizar el fichero de configuración de ejemplo como punto de partida. Para indicarle a Samhain que envíe los ficheros de registro al servidor, no hay que olvidar activar el parámetro *ExportSeverity* de la sección *[Log]*.

Tras procesar el fichero de configuración, Samhain buscará la base de datos de firmas en el directorio */var/lib/yule*. Armado con la base de datos de firmas, comprobará el sistema de forma normal, creará los ficheros de registro y se los enviará a Yule. Yule siempre grabará los ficheros de registro, sin importar qué filtros se hayan definido en */etc/yulerc*.

Para que Yule filtre los mensajes entrantes se puede utilizar la siguiente configuración en la sección *[Misc]*:

```
UseClientSeverity = yes
UseClientClass = yes
```

Esta configuración mantiene todos los ficheros de firmas críticos, los resultados de los registros y la configuración de los clientes en el servidor. Este es el corazón de sistema de monitorización de Samhain y, como tal, debe mantenerse a salvo, preferiblemente utilizando el servicio Samhain.

Avalancha de Información

Una vez que el dúo dinámico de Samhain y Yule se encuentren configurados y ejecutándose, el administrador puede darse una vuelta por el mundo real, es decir, comprobando y evaluando regularmente los ficheros de registro. La única ayuda que Samhain le dará en este punto es la opción de pasar los datos a scripts y programas externos. Si va a utilizar un analizador de ficheros de registro para procesar los registros, probablemente quiera convertirlos al formato XML. Para ello, *configure* posee el parámetro *-enable-xml-log*. Además, Samhain puede actuar como sensor para el IDS Prelude y escribir su información en una base de datos. Pero para permitir que esto ocurra, como ya habrá adivinado, hay que compilar Samhain con los parámetros -

with-prepare, *--with-database=mysql*. Además de MySQL, Samhain puede trabajar con PostgreSQL (... = *postgresql*) y Oracle (... = *oracle*).

Adicionalmente, hay que activar la salida para la base de datos si se quiere utilizar Beltane [4], la interfaz web para gestionar Yule. Disponible como un paquete independiente, ayuda a visionar los registros y a actualizar la base de datos de firmas. Como inconveniente, la interfaz de usuario requiere el entorno totalmente obsoleto PHP4, lo que es inaceptable para una herramienta de seguridad.

Para facilitar la evaluación de los ficheros de registro, especialmente en entornos mucho más complejos, hay opciones más avanzadas de filtrado. Por ejemplo, se puede especificar que sólo los eventos especiales acaben en los ficheros de registro, tales como la información de las marcas de tiempo modificadas, o incluso definir sus propias políticas y modificar las existentes.

Los ficheros de configuración de firmas de GnuPG y la base de datos de firmas proporcionan protección frente a intentos de manipular el núcleo del sistema. Antes de tocar estos controles, sería buena idea leerse detenidamente el manual. Un simple fallo es suficiente para impedir a Samhain que utilice su base de datos de firmas o que descarte pistas importantes de intrusiones, ya que los filtros son restrictivos y pueden anularse entre sí.

Conclusiones

Samhain no es la panacea contra las intrusiones, pero es una herramienta útil para utilizarla junto con un cortafuegos y un NIDS. El servidor de registros Yule actúa como un punto de recolección central de la red para mantener todo ordenado. Una vez que se haya enfrentado al proceso complejo de configuración y haya aprendido cómo leer los ficheros de registro, le agradecerá tener un vigilante tan atento que detecte las visitas inesperadas de forma rápida y silenciosa. ■

Lo que Monitoriza Samhain

- Contenido de los ficheros (por medio de sumas de comprobación)
- Tamaño de los ficheros
- Privilegios de acceso, propietarios y grupos
- Marcas de Tiempo (por ejemplo, la fecha de creación)
- Número de enlaces duros
- Número de inodo
- Número de dispositivo para los dispositivos
- Nombres de ficheros inusuales o crípticos
- Ficheros con el bit SUID o SGID (opcional)
- Actividad de carga del módulo del kernel (opcional)
- Intentos de conexiones y desconexiones de los usuarios (opcional)

RECURSOS

- [1] HIDS: http://en.wikipedia.org/wiki/Host-based_intrusion_detection_system
- [2] NIDS: http://en.wikipedia.org/wiki/Network_intrusion_detection_system
- [3] Samhain: <http://la-samhna.de/samhain/>
- [4] Beltane: <http://la-samhna.de/beltane/>