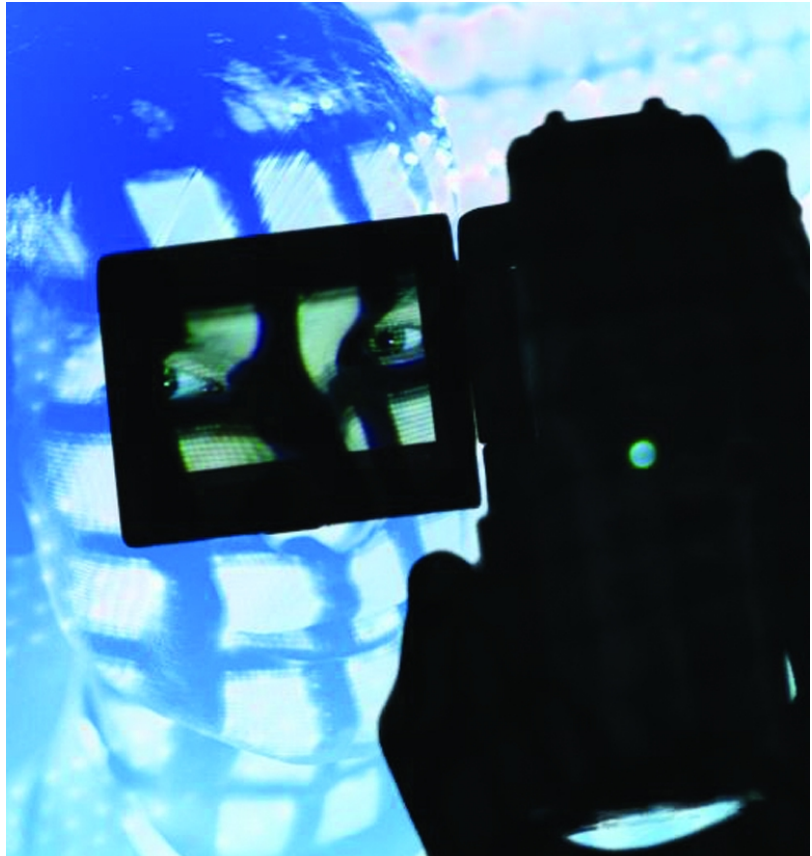


Herramientas de Análisis para Ficheros de Registros de Cortafuegos

Análisis Final

El cortafuegos Netfilter crea ficheros de registros muy detallados que realmente nadie quiere inspeccionar a mano. Las herramientas de análisis de ficheros de registros como IPTables Log Analyzer, Wallfire Wflogs y FWlogwatch ayudan a los administradores a seguir la pista de acontecimientos y de filtros para mensajes importantes.

POR RALF SPENNEBERG



En un entorno protegido por un cortafuegos, el administrador debe seguir la pista de los acontecimientos mediante el registro de tantas transacciones como sean posibles. Al mismo tiempo, los administradores quieren evitar inspeccionar ficheros de registros de cientos de megabytes porque sólo están interesados en algunos en concreto.

Asistentes para los Ficheros de Registros

Las herramientas de análisis de protocolo proporcionan una solución a este dilema. Los usuarios de Linux tienen varias opciones a la hora de elegir un programa de análisis de cortafuegos. En

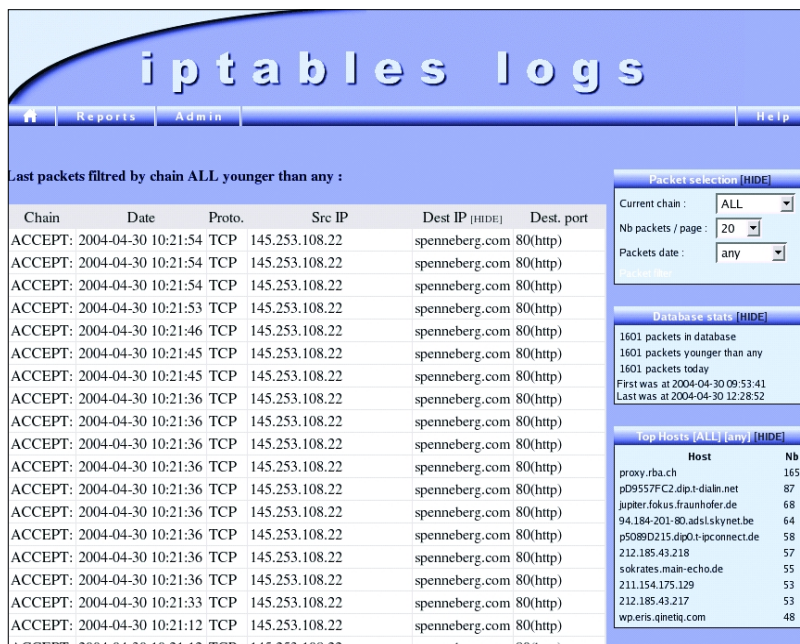
este artículo, veremos tres alternativas: IPTables Log Analyzer [1], WFlogs del proyecto Wallfire [2] y FWlogwatch [3]. Los tres programas soportan una amplia gama de protocolos y muestran los resultados como páginas HTML muy bien formateadas; WFlogs y FWlogwatch además tienen modos en tiempo real. IPTables Log Analyzer es la única herramienta que utiliza bases de datos para el almacenamiento de mensajes.

IPTables Log Analyzer se basa en un sistema de entrada especial. Ulogd de Harald Weltes [4] maneja esto de forma nativa, sustituyendo el sistema de syslog que trae por defecto. Desafortunadamente, las herramientas de análisis gratuitas que soportan las bases de

datos Ulog son raras. Ulogd-php [5] es uno de los primeros. Al contrario que los otros sistemas de registros, Ulogd puede registrar los eventos que causaron una alerta en el cortafuegos en su base de datos.

IPTables Log Analyzer

IPTables Log Analyzer presta servicio a los registros de IPTables para Linux 2.4 o 2.6 en formato de páginas HTML (Ver Figura 1). La herramienta incluye tres componentes. El sistema de entrada de la base de datos almacena los eventos en una base de datos MySQL; los administradores pueden usar el interfaz web para acceder a la base de datos. El sistema de entrada de la base de datos, la



Chain	Date	Proto.	Src IP	Dest IP [HIDE]	Dest. port
ACCEPT	2004-04-30 10:21:54	TCP	145.253.108.22	spenneberg.com	80(http)
ACCEPT	2004-04-30 10:21:54	TCP	145.253.108.22	spenneberg.com	80(http)
ACCEPT	2004-04-30 10:21:54	TCP	145.253.108.22	spenneberg.com	80(http)
ACCEPT	2004-04-30 10:21:53	TCP	145.253.108.22	spenneberg.com	80(http)
ACCEPT	2004-04-30 10:21:45	TCP	145.253.108.22	spenneberg.com	80(http)
ACCEPT	2004-04-30 10:21:45	TCP	145.253.108.22	spenneberg.com	80(http)
ACCEPT	2004-04-30 10:21:36	TCP	145.253.108.22	spenneberg.com	80(http)
ACCEPT	2004-04-30 10:21:36	TCP	145.253.108.22	spenneberg.com	80(http)
ACCEPT	2004-04-30 10:21:36	TCP	145.253.108.22	spenneberg.com	80(http)
ACCEPT	2004-04-30 10:21:36	TCP	145.253.108.22	spenneberg.com	80(http)
ACCEPT	2004-04-30 10:21:36	TCP	145.253.108.22	spenneberg.com	80(http)
ACCEPT	2004-04-30 10:21:36	TCP	145.253.108.22	spenneberg.com	80(http)
ACCEPT	2004-04-30 10:21:36	TCP	145.253.108.22	spenneberg.com	80(http)
ACCEPT	2004-04-30 10:21:36	TCP	145.253.108.22	spenneberg.com	80(http)
ACCEPT	2004-04-30 10:21:36	TCP	145.253.108.22	spenneberg.com	80(http)
ACCEPT	2004-04-30 10:21:33	TCP	145.253.108.22	spenneberg.com	80(http)
ACCEPT	2004-04-30 10:21:12	TCP	145.253.108.22	spenneberg.com	80(http)

Figura 1: IPTables Log Analyzer da al administrador una clara visión de los ficheros de registros del cortafuegos.

base de datos y el interfaz web pueden ejecutarse todos en la misma máquina o en máquinas distintas. Por otro lado, la base de datos puede almacenar ficheros de registros de varios cortafuegos.

Después de decidir la arquitectura, el administrador necesita crear una base de datos MySQL denominada *iptables*, permitir a los usuarios el acceso a *iptables_admin* e *iptables_user* y generar tablas en la base de datos (Listado 1). También es necesario definir las reglas de IPTables. Dos cadenas definidas por el usuario es la mejor forma (Listado 2).

Creando Cadenas

En vez de *-j ACCEPT*, IPTables ahora usará *-j LOG_ACCEPT*. Estas modificaciones no son necesarias para Shorewall [6] o Suse Firewall en CD [7]. Sin embargo Suse dice que no dará soporte a su producto de cortafuegos en el futuro, que es otra razón para que los administradores escojan herramientas y actualizaciones del mundo de código abierto.

El siguiente paso es instalar el interfaz web. Para hacer esto, el administrador necesita mover el directorio *web* al directorio raíz del servidor web y modificar *config.php* para reflejar los

parámetros de la base de datos y la configuración del servidor web (usuario, password, URL). El último paso es instalar y activar el sistema de entrada de la base de datos. Será necesario de nuevo modificar las credenciales de los usuarios de la base de datos.

IPTables Log Analyzer tiene tres variantes del sistema de entrada de la base de datos denominadas *feed_db.pl*, *feed_db-shore-wall.pl* y *feed_db-suse.php*. Para lanzar el sistema de entrada automáticamente, el administrador necesita mover el script de arranque, *scripts/iptableslog*, a */etc/init.d* y crear los enlaces en *rc*.

WFlogs

WFlogs es la herramienta de análisis que pertenece al proyecto Wallfire [2], aunque puede usarse independientemente. El módulo del programa analiza y procesa Netfilter, Ipchains, IPfilter, Cisco PIX, Cisco IOS y ficheros de registro Snort, mostrando los resultados como texto, HTML, XML o en tiempo real. WFlogs no tiene soporte de base de datos, pero puede convertir formatos de ficheros de registros entre Netfilter, IPchains e IPfilter.

Instalar WFlogs en Debian es muy fácil. Debian Sid incluye WFlogs y los

Listado 1: Base de Datos MySQL

```
01 # mysql -u root -p
02 mysql> create database
03     iptables;
04 mysql> grant
05     create,select,insert
06     on
07     iptables.* to
08     iptables_admin@localhost
09     identified by
10     'g3h31m';
11 mysql> grant create,select on
12     iptables.* to
13     iptables_user@localhost
14     identified by
15     'auchgeheim';
16 mysql> quit
17 # cat sql/db.sql | mysql -u
18     iptables_admin -p
19     iptables
```

paquetes para Woody están disponibles en [8]. Los usuarios de otras distribuciones pueden compilar WFlogs desde el código fuente. WFlogs también necesita la biblioteca WFnetobjs, otro componente de Wallfire [2]. La librería alternativa DNS, *adns* [9], también se recomienda para la resolución de nombres de forma asíncrona DNS.

Para compilar Wflogs, se siguen los pasos típicos *./configure; make; make install*; se necesitará especificar el directorio de *WFnetobjs* en los pasos de configuración.

De Netfilter a HTML

WFlogs puede procesar los registros del cortafuegos de forma online u offline. Los siguientes comandos crean una vista en formato HTML de un fichero de registro de Netfilter (Figura 2):

```
wflogs -i netfilter -o html >
netfilter.log > logs.html
```

En el modo tiempo real, WFlogs analiza las nuevas entradas del fichero de registros y muestra por pantalla estas entradas. Los administradores pueden usar la shell para modificar interactivamente el comportamiento de WFlogs. Los siguientes comandos le dicen a

WFlogs que monitorice interactivamente un fichero denominado `/var/log/warn` en tiempo real:

```
wflogs -RI -o human
/var/log/warn
```

La opción `-P` le dice a WFlogs que procese los mensajes más antiguos del fichero. WFlogs no se lanza por mensajes que no sean del cortafuegos.

Filtrado

Las opciones de filtrado pueden restringir la salida a mensajes específicos. El filtro siguiente es de la documentación de WFlogs; lista las conexiones Telnet y SSH denegadas para los últimos tres días de la red 10.0.0.0/8:

```
wflogs -f '$start_time >=
this 3 days ago' && '$start_time <
[this 2 days ago]' &&
$chainlabel =~ /(DROP|REJECT)/
&& $sipaddr == 10.0.0.0/8 &&
$protocol == tcp && ($dport ==
ssh || $dport == telnet) &&
($tcpflags & SYN) -i
netfilter -o text
--summary=no
```

FWlogwatch

Boris Wesslowski desarrolló FWlogwatch para RUS-CERT en la Universidad de Stuttgart, Alemania. La versión 1.0 [3] de la herramienta de análisis ahora ha sido lanzada bajo licencia GPL.

FWlogwatch tiene tres modos de operación: Modo Log Summary, Modo Interactive Report y Modo Realtime Response. En el modo Log Summary, el programa genera texto o páginas HTML con el resumen del análisis de los ficheros de registros del cortafuegos (Figura 3). En el modo Interactive Report, FWlogwatch genera automáticamente informes de incidencias que los administradores pueden reenviar a quienes hayan sido afectados por el incidente.

En el modo Realtime, FWlogwatch responde a ataques ejecutando scripts,

wflogs summary									
Generated on Fri Apr 30 12:29:37 CEST 2004 by spenneb.									
#	start	end	interval	loghost	chain	input interface	output interface	proto	source
13	Apr 30 10:45:24	Apr 30 10:46:26	00:00:01:02	P15097491	ACCEPT: HTTP-Zugriff	eth0	-	tcp	62.52.55.227
15	Apr 30 10:34:17	Apr 30 10:34:20	00:00:00:03	P15097491	ACCEPT: HTTPS-Zugriff	eth0	-	tcp	62.59.233.212
2	Apr 30 11:25:51	Apr 30 11:25:52	00:00:00:01	P15097491	ACCEPT: HTTPS-Zugriff	eth0	-	tcp	62.94.244.202
6	Apr 30 10:26:56	Apr 30 10:27:37	00:00:00:41	P15097491	ACCEPT: HTTP-Zugriff	eth0	-	tcp	62.101.126.222
15	Apr 30 10:44:47	Apr 30 10:47:02	00:00:02:15	P15097491	ACCEPT: HTTPS-Zugriff	eth0	-	tcp	62.108.18.44
18	Apr 30 10:45:01	Apr 30 10:47:10	00:00:02:09	P15097491	ACCEPT: HTTP-Zugriff	eth0	-	tcp	62.108.18.44
38	Apr 30 10:27:03	Apr 30 10:50:29	00:00:23:26	P15097491	ACCEPT: HTTP-Zugriff	eth0	-	tcp	62.159.148.131
55	Apr 30 10:35:06	Apr 30 10:38:14	00:00:03:08	P15097491	ACCEPT: HTTP-Zugriff	eth0	-	tcp	62.159.226.12
8	Apr 30 10:22:12	Apr 30 10:22:42	00:00:00:30	P15097491	ACCEPT: HTTP-Zugriff	eth0	-	tcp	62.238.255.223
7	Apr 30 10:22:12	Apr 30 10:22:42	00:00:00:30	P15097491	ACCEPT: HTTP-Zugriff	eth0	-	tcp	62.238.255.223

Figura 2: La página del Resumen de WFlogs muestra cuantos paquetes han sido registrados para cada fuente.

enviando mensajes de correo o automáticamente modificando las reglas del cortafuegos.

Los administradores pueden usar el servidor web integrado para supervisar el estado de FWlogwatch desde un navegador web.

FWlogwatch soporta IPchains (opción *i*), Netfilter (*n*), Ipfiler (*f*), IPFW (*b*), Cisco IOS (*c*), Cisco PIX (*p*), Netscreen (*e*), Windows XP (*w*), Elsa Lancom (*l*) y formatos Snort (*s*). La instalación es tan fácil como lanzar los

procesos `make && make install && make install-config`. Boris Wesslowski tiene los paquetes para Red Hat y Debian en la página principal del sitio web de FWlogwatch.

Los administradores pueden configurar el comportamiento de FWlogwatch usando el archivo de configuración, que viene sumamente comentado. También pueden configurar FWlogwatch mediante la línea de comandos. En las páginas de ayuda (comando *man*) vienen explicadas las opciones. Por ejemplo, el siguiente comando ejecuta FWlogwatch en modo resumen:

```
fwlogwatch -b -Pn -U
'Spenneberg.Com' -p -n -N -o
output.html -t -w
/var/log/messages
```

La opción `-Pn` habilita el analizador de Netfilter. `-U` permite al usuario especificar una cabecera para el resumen. La opción `-o` especifica el fichero de salida; `-w` estipula la salida HTML. `-n` y `-N` permite la resolución de nombres de hosts y servicios. El resultado es un resumen en formato HTML del fichero de registros del cortafuegos.

Respuesta Rápida

La opción de ejecución de FWlogwatch en modo tiempo real permite a los administradores reaccionar ante mensajes del fichero de registros y a la vez mostrar el estado actual en la ventana del navegador. FWlogwatch se ejecuta en segundo plano como un servicio y monitoriza el fichero de registros, analizando de nuevo el archivo de configuración si se recibe un SIGHUP. SIGUSR1 le indica al servicio que vuelva a abrir el fichero de registros. Esta característica es útil para ir rotando ficheros de registros, por ejemplo.

Los administradores pueden especificar el valor umbral para que FWlogwatch reaccione a mensajes del fichero de registros disparando alarmas o respondiendo con scripts. Hay dos

Listado 2: Analizador de Registros de IPTables

```
01 iptables -N LOG_DROP
02 iptables -A LOG_DROP -j LOG
--
03 log-tcp-options
--log-iptoptions
04 --log-prefix
05 '[IPTABLES DROP] : '
06 iptables -A LOG_DROP -j DROP
07 iptables -N LOG_ACCEPT
08 iptables -A LOG_ACCEPT -j LOG
--log-tcp-options
--log-iptoptions
10 --log-prefix
11 '[IPTABLES ACCEPT] : '
12 iptables -A LOG_ACCEPT -j
13 ACCEPT
```

opciones de configuración importantes: *recent (-l)* define el período de tiempo a monitorizar y *alert_threshold (-a)* define el número de eventos que en este tiempo tienen que suceder para lanzar una respuesta. El Listado 3 muestra su configuración. Este ejemplo configura Fwlogwatch para el modo en tiempo real

Listado 3: Fwlogwatch en Modo Tiempo Real

```
01 realtime_response = yes
02 parser = n
03 run_as = fwloguser
04 recent = 600
05 alert_threshold = 5
06 notify = yes
07 notification_script = /usr/
08     sbin/fwlv_notify
09 server_status = yes
10 bind_to = 127.0.0.1
11 listen_port = 8888
12 status_user = ralf
13 status_password =
14     iOQ1Am0g4PrAA
15 refresh = 10
```

fwlogwatch status

[Information | Options | Packet cache | Host status | Reload]

Information

```
Daemon start time: Freitag April 30 20:03:49 CEST 2004
Current time: Freitag April 30 20:06:48 CEST 2004
Running time: 00:00:02:59
Response mode: Log
Lines seen: 10843
Hits: 74
Old/excluded/malformed: 10667
Entries in packet cache: 5
Entries in host status: 4
```

[Information | Options | Packet cache | Host status | Reload]

fwlogwatch 1.0 2004/04/25 © Boris Wesslowski

Figura 4: El servidor web integrado en Fwlogwatch permite a los administradores monitorizar el estado actual del cortafuegos.

fwlogwatch status

[Information | Options | Packet cache | Host status | Reload]

Options

Parameter	Decrease	Current	Increase
Alert threshold:	≤	4	≥
Discard timeout:	≤	00:00:10:00	≥
Minimum count in packet cache:	≤	1	≥
Top amount of entries in packet cache:	≤	-	≥
Refresh time:	≤	-	≥

[Information | Options | Packet cache | Host status | Reload]

fwlogwatch 1.0 2004/04/25 © Boris Wesslowski

Figura 5: Los administradores pueden utilizar un navegador para configurar Fwlogwatch. El Alert Threshold especifica el número de mensajes necesarios para lanzar la respuesta de Fwlogwatch.

```
ureserver.info) port 80 (http) with TCP flags SYN
at Apr 30 12:28:48, 1 packet logged on host P15097491: chain IPTABLES ACCEPT: HT
TP-Zugriff, on input interface eth0, source mac address 00:00:5a:9d:10:ba, desti
nation mac address 00:20:ed:2f:ed:68, protocol tcp, from 80.58.0.172 (unknown ho
stname) (80.58.0.0/16 RIMA (Red IP Multi Acceso) AS3352 Internet Access Network
of TDE) port 50651 (unknown service name) to 217.160.128.61 (p15097491.pureserve
r.info) port 80 (http) with TCP flags SYN
at Apr 30 12:28:52, 1 packet logged on host P15097491: chain IPTABLES ACCEPT: SS
H-Zugriff, on input interface eth0, source mac address 00:00:5a:9d:10:ba, desti
nation mac address 00:20:ed:2f:ed:68, protocol tcp, from 212.204.17.133 (iD4CC118
5.versanet.de) port 64541 (unknown service name) to 217.160.128.61 (p15097491.pu
reserver.info) port 22 (ssh) with TCP flags SYN
/var/log/messages:3250: warning: line format matches none of the specified modul
e(s): netfilter
wflogs> help
help          Display this text.
?             Synonym for 'help'.
quit         Quit.
exit         Synonym for 'quit'.
beep         Set beep mode: [on|off|?]. Beep for every log entry displayed.
filter       Set filter expression: [expression|unset].
realtime     Set realtime mode: [on|off|?]. Monitor new log entries..
verbose      Set verbosity level: [level].
wflogs>
```

Figura 3: En Modo Resumen, Fwlogwatch da a los administradores una vista de la actividad del fichero de registro del cortafuegos.

con el analizador Netfilter. El proceso se ejecuta bajo la identificación de usuario *fwloguser*.

Si se excede el umbral de cinco conexiones en 600 segundos, Fwlogwatch realiza una acción configurable. Fwlogwatch monta un servidor de web en 127.0.0.1:8888, donde un usuario *ralf* puede conectarse con la contraseña *password*. Fwlogwatch utiliza contraseñas encriptadas con DES, que pueden generarse tecleando *htpasswd -nb usuario*

contraseña. Cuando el usuario se registra en esta página, aparece lo mostrado en la Figura 4. Esta página conduce a otras páginas con una amplia gama de opciones de configuración de Fwlogwatch (Figura 5).

Opciones

Fwlogwatch tiene una enorme variedad de características, que van desde un simple resumen hasta un modo en tiempo real con respuestas configurables. Pero las otras herramientas que se comentan en este artículo merecen también una buena consideración. Si necesita filtros potentes, WFlogs puede ser una buena opción para su red. El IPTables Log Analyzer es una opción interesante para algunas situaciones por su soporte de base de datos.

El IPTables Log Analyzer da a los administradores de sistemas la opción de utilización de sentencias SQL para buscar los mensajes del cortafuegos, en vez de tener que lanzar las búsquedas desde una interfaz web.

INFO

- [1] IPTables Log Analyzer: <http://www.gege.org/iptables/>
- [2] Proyecto Wallfire (WFlogs y WFnetobjs): <http://www.wallfire.org>
- [3] Fwlogwatch: <http://fwlogwatch.inside-security.de>
- [4] Ulogd: <http://gnumonks.org/projects/ulogd>
- [5] Ulogd PHP: <http://www.inl.fr/download/ulog-php.html>
- [6] Cortafuegos Shorewall: <http://shorewall.sourceforge.net>
- [7] Cortafuegos Suse: http://www.suse.de/en/business/products/suse_business/firewall/
- [8] Paquetes WFlogs, Debian Woody: <http://people.debian.org/~kelbert/>
- [9] GNU adns: <http://www.chiark.greenend.org.uk/~ian/adns/>

EL AUTOR

Ralf Spenneberg es un freelance de Unix/Linux, profesor y autor. El año pasado vió la luz su primer libro: "Sistemas de Intrusión y Detección para Servidores Linux". Ralf también ha desarrollado varios trabajos de educación.