NIDS & Analizadores de Logs

Sergio González González
Universidad de León, España

sergio.gonzalez@hispalinux.es

Este artículo pretende mostrar la forma de instalar y configurar, en la distribución Debian GNU/Linux, algunos programas analizadores de logs y NIDS (Network Intrusion Detection System).

Introducción

Para facilitar la vida de un administrador de sistemas, se hace imprescindible el uso de analizadores de logs, que reporten las incidencias más importantes acaecídas en un determinado equipo. En este documento se mostrarán los siguientes analizadores de logs:

- Calamaris (http://cord.de/tools/squid/calamaris/) - analizador de logs para Squid (http://www.squid-cache.org)
- AWStats (http://awstats.sourceforge.net) - Analizador de logs para Apache (http://www.apache.org)
- log2mail - Analizador de logs en busca de determinadas cadenas
- logcheck - Analizador de logs que envía las anomalías del sistema al administrador

De todos es sabido que la red es un "mundo hostil", por ello se hace necesario analizar el estado de nuestra red en busca de personajes sin escrúpulos que quieren a toda costa contactar de forma ilícita con nuestros servidores. Los programas NIDS ayudan en esta labor, aunque no son infalibles, por desgracia... Veremos a continuación algunos de los programas utilizados:

- Snort (http://www.snort.org/) - The Open Source Network Intrusion Detection System
- ippl (http://pltplp.net/ippl/) - IP protocols logger

Analizadores de logs

Sección dedicada a las herramientas analizadores de logs que actualmente se están utilizando en los servidores de la Unidad de Imagen y del laboratorio F1.

Calamaris

Calamaris es un script en Perl que genera estadísticas a partir de los archivos de log de Squid. Se ejecuta una vez al día, antes de la rotación de los logs y envía las estadísticas al administrador del sistema. Podemos ver un ejemplo de estos reportes en este enlace (http://www.cord.de/tools/squid/calamaris/calamaris-2.html).

La instalación y configuración de Calamaris es extermadamente fácil en Debian GNU/Linux. Para instalarlo ejecutaremos:

```
# apt-get install calamaris
```

Una vez se ha bajado el programa, nos hará una serie de preguntas, a las que responderemos[1] de la siguiente forma:

```
What type of proxy log files do you want to analyse? squid
How should the daily analysis of Calamaris be stored? mail
How should the weekly analysis of Calamaris be stored? mail
How should the monthly analysis of Calamaris be stored? mail
Email address to which the daily analysis should be sent -> root
```

Al finalizar la configuración, nos generará el siguiente archivo de configuración

```
# configuration file for calamaris
# by Philipp Frauenfelder <pfrauenf@debian.org>
# 1998-10-09

# There are three categories: daily, weekly and monthly. For each of these
# one line is responsible. There must be a line for each category but only
# one.

# cat: [daily|weekly|monthly]
# mailto: mailaddress, eg. root
# webto: path incl. file name, eg. /var/www/calamaris/daily.html.
#        The script does currently not check wether the directory
#        exists and fails with a rather ugly error.
# todo: [nothing|mail|web|both]
# title: try it :-)

# cat:mailto:webto:todo:title
daily:root:/var/www/calamaris/daily.html:mail:'Squid daily'
weekly:root:/var/www/calamaris/weekly.html:mail:'Squid weekly'
monthly:root:/var/www/calamaris/monthly.html:mail:'Squid monthly'
# what log files should be parsed: [auto|squid|oops]
#       auto: tries to find the log files in this order: squid, oops
#       squid: parses a squid log file if available
#       oops: parses a oops log file if available
cache=squid
```

AWStats

Advanced Web Statistics (AWStats) es un analizador de archivos de log de un servidor web escrito en Perl. Muestra todas las estadísticas, incluyendo la cantidad de visitas, páginas visitadas, hits, horas de mayor actividad, buscadores, palabras clave usadas para encontrar el sitio, robots, enlaces rotos y mucho más. Para instalarlo tenemos que teclear:

```
# apt-get install calamaris
```

La configuración se lleva a cabo en el archivo `/etc/awstats/awstats.conf` y las opciones más interesantes serían:

```
LogFormat=1
DNSLookup=1
SiteDomain="cancerbero.unileon.es"
HostAliases="cancerbero.unileon.es 193.146.99.248"
Lang="es"
DefaultFile="index.html"
```

Cancerbero posee sus propias estadísticas (http://cancerbero.unileon.es/cgi-bin/awstats.pl) generadas por AWStatas.

log2mail

log2mail es un demonio que revisa los archivos de log y envía a un correo electrónio a una determinada dirección si se da una expresión regular. Vamos a configurarlo de forma que se envíe un correo al administrador del sistema cada vez que un usuario se conecta a través de ssh al sistema o lo abandona. A continuación se muestran los archivos que se han de editar, así como su contenido:

/etc/log2mail/config/default

```
# sample config file for log2mail
# comments start with '#'
# see source code doc/Configuration for additional information

defaults
  sendtime = 20
  resendtime = 50
  maxlines = 1
  template = /etc/log2mail/mail
  fromaddr = log2mail
  sendmail = /usr/lib/sendmail -oi -t

file = /var/log/messages
  pattern = "root login"
    mailto = root

file = /var/log/auth.log
  pattern = "(ssh) session opened"
    mailto = root
```

```
  pattern = "(ssh) session closed"
    mailto = root
```

/etc/log2mail/mail

```
From: %f
To: %t
Subject: Coincidencia en: %m

Coincidencia de "%m" en "%F" %n veces:

--------------------------------------------------

%l

---------------------------------------------------
```

logcheck

Logcheck es parte del Proyecto Abacus de herramientas de seguridad. Este programa ha sido creado con la intención de ayudar en el procesado de archivos de log generados en sistemas UNIX. Logcheck encuentra las alertas de seguridad en los logs y las envía la correo del administrador. La forma de instalarlo es la siguiente:

```
# apt-get install logcheck
```

Una vez se ha bajado el programa, nos hará una serie de preguntas, que responderemos de la siguiente manera:

```
The email address to which the mails should be sent -> root
```

Esto es todo lo que tenemos que hacer, a partir de este momento, los avisos de seguridad llegarán puntualmente a nuestro correo ;-)

NIDS - Network Intrusion Detection System

Snort

Snort es un sistema detector de intrusiones en la red, capaz de hacer análisis en tiempo real y almacenar en un archivo de log los paquetes IP que han llegado a una determinada interfaz de red. La forma de instalarlo será la siguiente:

```
# apt-get install snort snort-common snort-doc snort-rules-default
```

Una vez se ha bajado el paquete, contestaremos a las preguntas realizadas de la siguiente forma:

```
 ¿Cuando debería arrancarse Snort? boot
¿En qué interfaz debería escuchar Snort? eth1 (para Cancerbero)
What address range should Snort consider to be local? 192.168.1.0/16
¿Debería deshabilitar el modo promiscuo? No
¿Deberían las reglas de Snort cambiarse de orden a Pasar|Alertar|Registrar? No
Si quiere añadir opciones adicionales a 'snort', especifiquelas aquí: "En blanco"
¿Quién debería recibir las estadísticas diarias? root
Una alerta debe aparecer más de éste número de veces para aparecer en las estadísticas. -> 1
```

Con eso es suficiente para que se ponga en marcha.

ippl

ippl es un "demonio" que guarda en archivos de log los paquetes IP enviados a un ordenador. Se ejecuta en segundo plano y muestra la información de los paquetes entrantes. Para instalarlo ejecutaremos:

```
# apt-get install ippl
```

La configuración se lleva a cabo en el archivo de configuración situado en `/etc/ippl.conf`. Ha de tener un aspecto similar al siguiente:

```
# IP protocols logger - Configuration file
# See ippl.conf(5)

# User used
# ---------
# Specify the user (declared in /etc/passwd) used to run the
# logging threads.
runas nobody

# Resolve hostnames?
# ------------------
# Uncomment the line below to disable DNS lookups
#noresolve all

# Use ident?
# ----------
# Uncomment the line below to enable IDENT lookups
#ident

# Log end of TCP connections ?
# ----------------------------
# Uncomment the line below to enable logging of closing TCP connections
# See the BUGS file.
#logclosing

# Expiration of DNS data
# ----------------------
#expire 3600

# Log in a file
# -------------
```

```
# Uncomment this line if you want to log messages into a /var/log/ippl.log
# See ippl.conf(5) for the syntax.
log-in all /var/log/ippl/all.log
log-in udp /var/log/ippl/udp.log

# Protocols logged
# ----------------
run icmp tcp
# Uncomment the line below to log UDP traffic.
# See ippl.conf(5) for recommandations.
run udp

# Logging format
# ----------------
# If you want to see the destination address, the ports, etc
# Or if you want to log the minimal information.
# See ippl.conf(5) for details.
logformat detailed all

# Filtering of packets logged
# ---------------------------

# Do not log answers to echo requests
#ignore icmp type echo_reply

# Log telnet connections using ident and name resolution
log options ident,resolve tcp port telnet

# Do not log UDP from localhost
#ignore udp from localhost

# Do not log DNS queries
#ignore udp port domain
#ignore udp srcport domain

# End of configuration
# Copyright (C) 1998-1999 Hugo Haas - Etienne Bernard
```

Más información

Si se quiere profundizar en alguno de estos programas, se invita al lector a consultar la ayuda que acompaña al programa así como las páginas principales de cada uno[2].

Sobre este documento

Se otorga permiso para copiar, distribuir y/o modificar este documento bajo los términos de la Licencia de Documentación Libre GNU, versión 1.1 o cualquier versión posterior publicada por la Free Software

Este documento ha sido escrito en formato XML utilizando la DTD de DocBook (http://www.docbook.org). Mediante este sistema, puede ser fácilmente transformado a múltiples formatos (HTML, TXT, PDF, PostScript, LaTeX, DVI, ...). Se recomienda su utilización como herramienta de documentación potente y libre.

Notas

1. Las preguntas que no aparezcan en la lista, se responderán por defecto
2. Algunas están listadas en la Introducción (./introduccion.html)