Servidor de Seguridad Perimetral II (continuación)

Por. Daniel Vazart P.

Resumen de la clase pasada.

1. Reglas del firewall.
2. Instalación de Squid.
3. Instalación de Dansguardian.
4. Actualización de los filtros de navegación.

5. Instalar Sarg

- Para instalar Sarg es necesario tener un servidor WEB corriendo en la maquina, en este caso utilizaremos Apache2, también es necesario tener el procesador de PHP instalado y corriendo con Apache para poder procesar las paginas .php de Sarg.
- El procedimiento de instalación de Apache es: apt-get install apache2
- El procedimiento de instalación de PHP es: apt-get install php4

5. Instalar Sarg

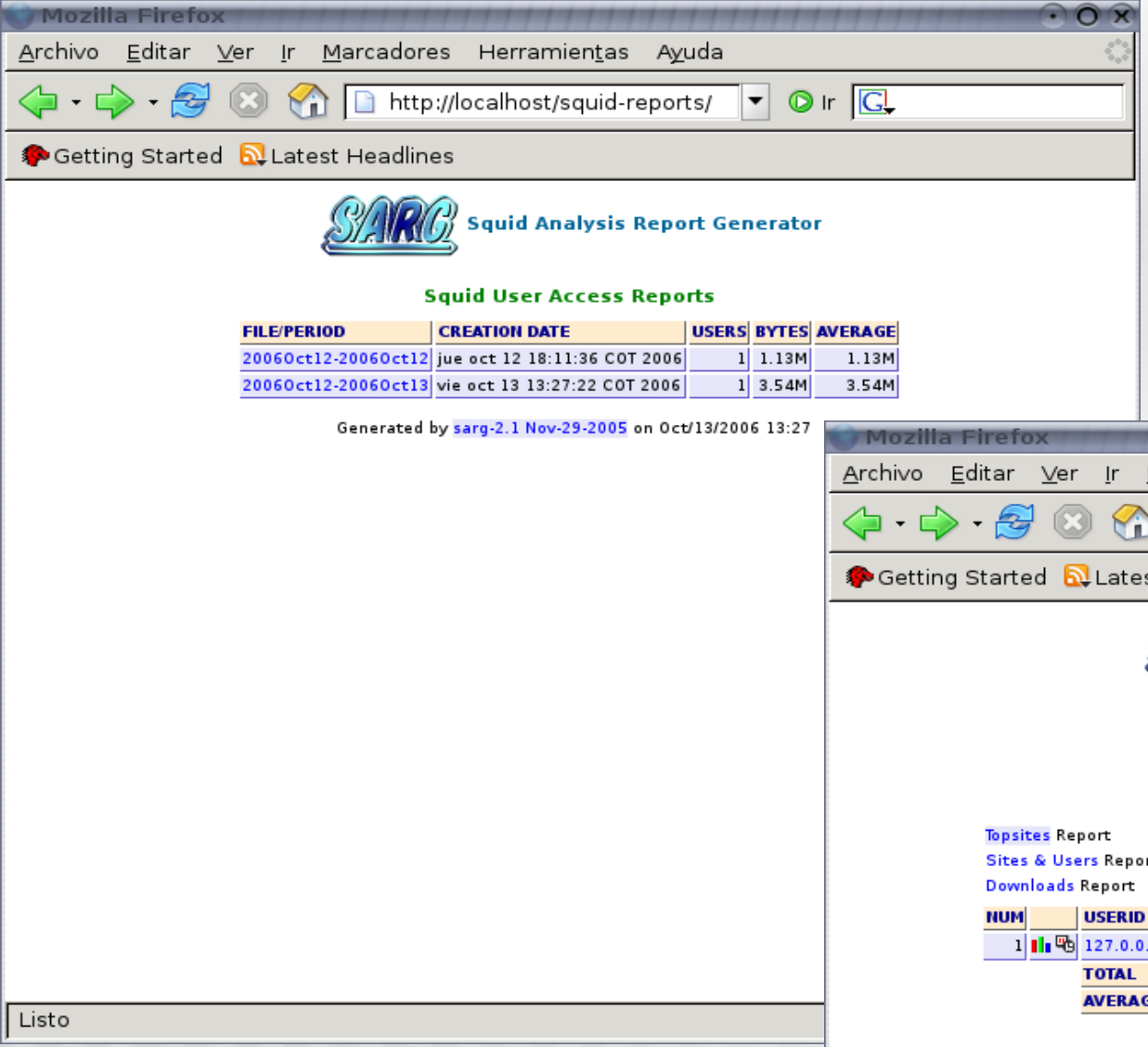
```
root@D3NI4L:/# apt-get install sarg
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  sarg
0 actualizados, 1 se instalarán, 0 para eliminar y 959 no actualizados.
Necesito descargar 300kB de archivos.
Se utilizarán 954kB de espacio de disco adicional después de desempaquetar.
Des:1 http://co.archive.ubuntu.com dapper/universe sarg 2.1-2 [300kB]
Descargados 300kB en 13s (21,6kB/s)

Preconfigurando paquetes ...
Seleccionando el paquete sarg previamente no seleccionado.
(Leyendo la base de datos ...
81758 ficheros y directorios instalados actualmente.)
Desempaquetando sarg (de .../archives/sarg_2.1-2_i386.deb) ...
Configurando sarg (2.1-2) ...

root@D3NI4L:/#
```

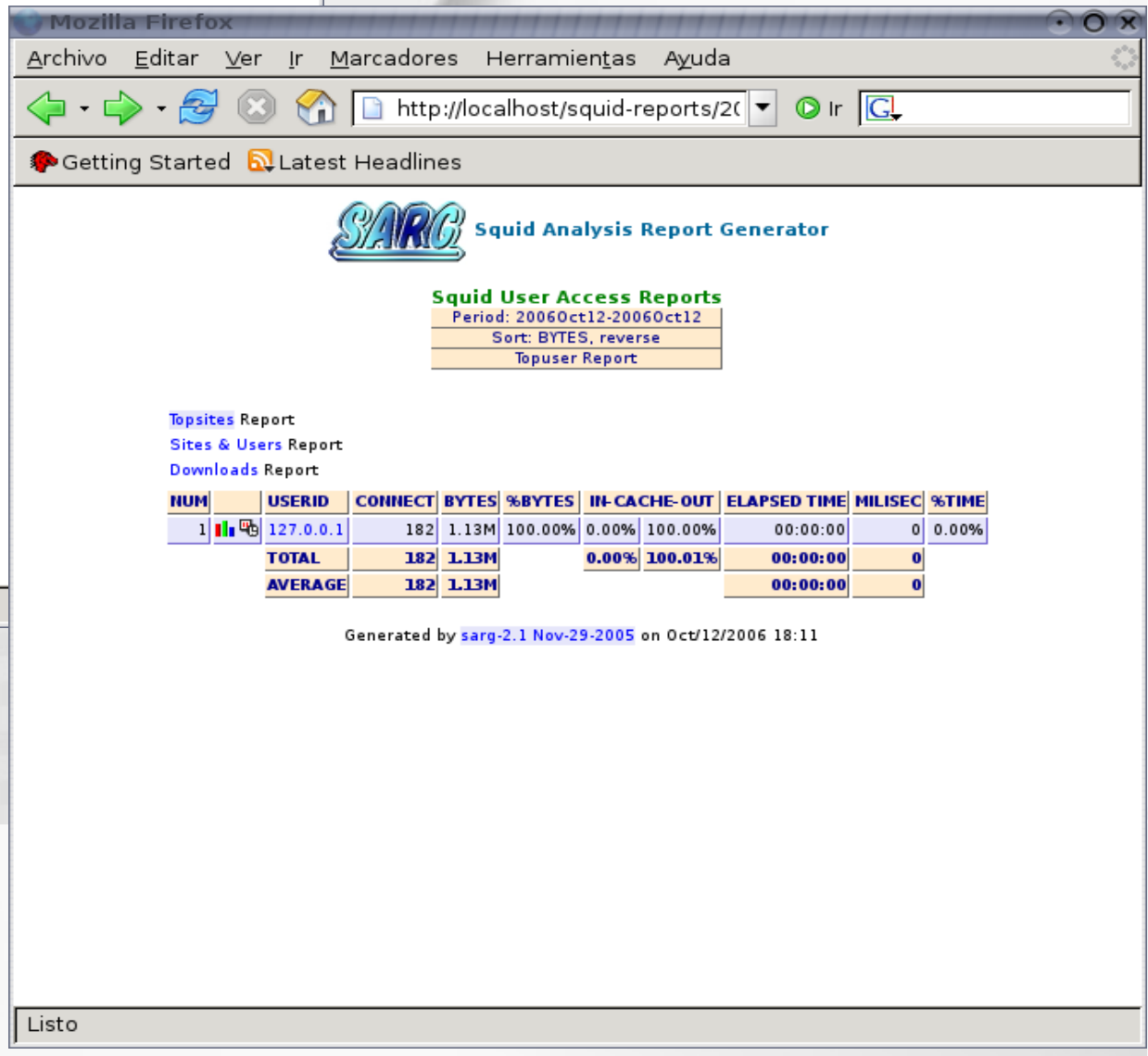
5. Instalar Sarg

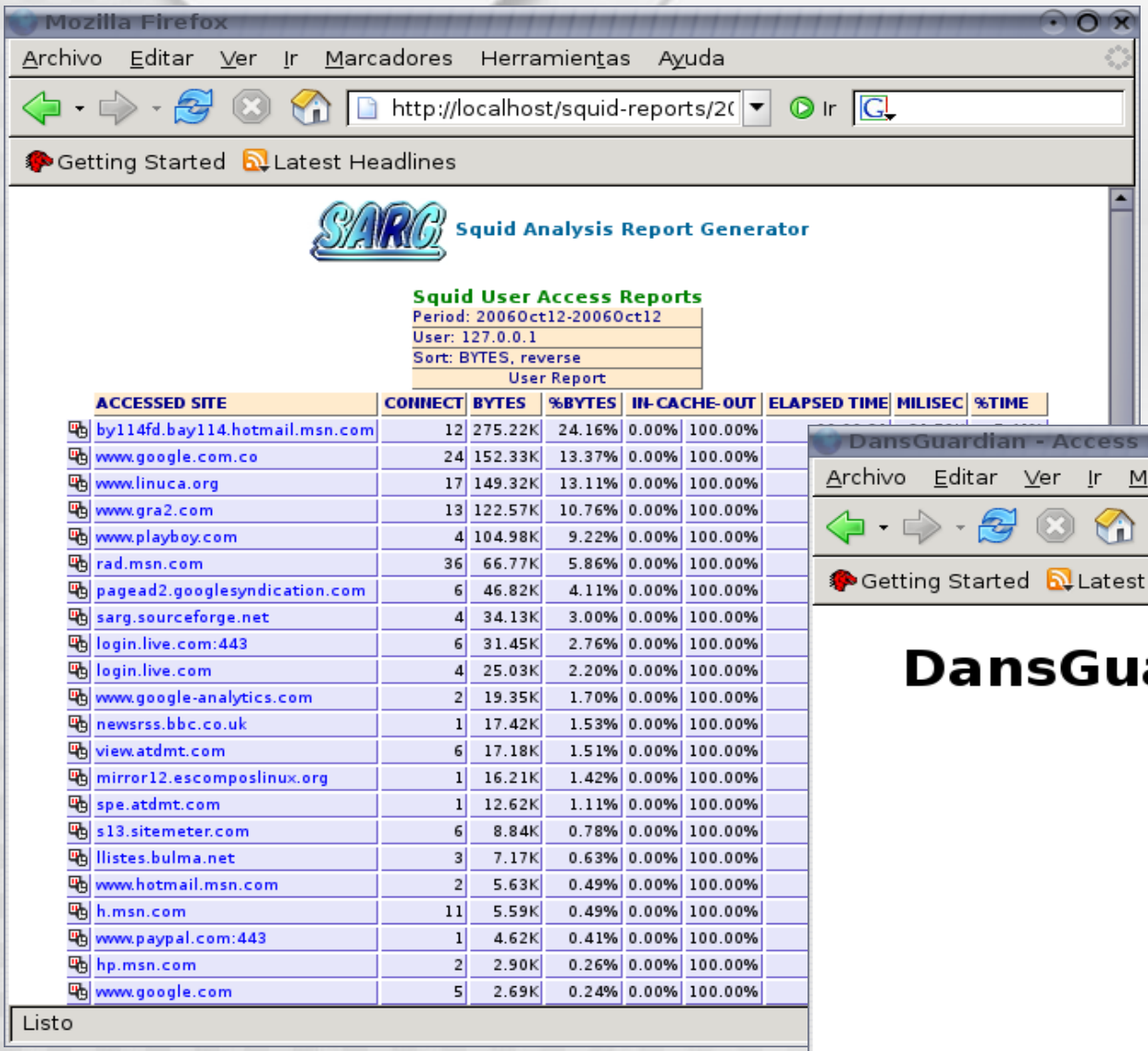
- Una vez instalado, se debe ejecutar el programa para que lea los archivos de registro del proxy y genere el reporte en WEB.

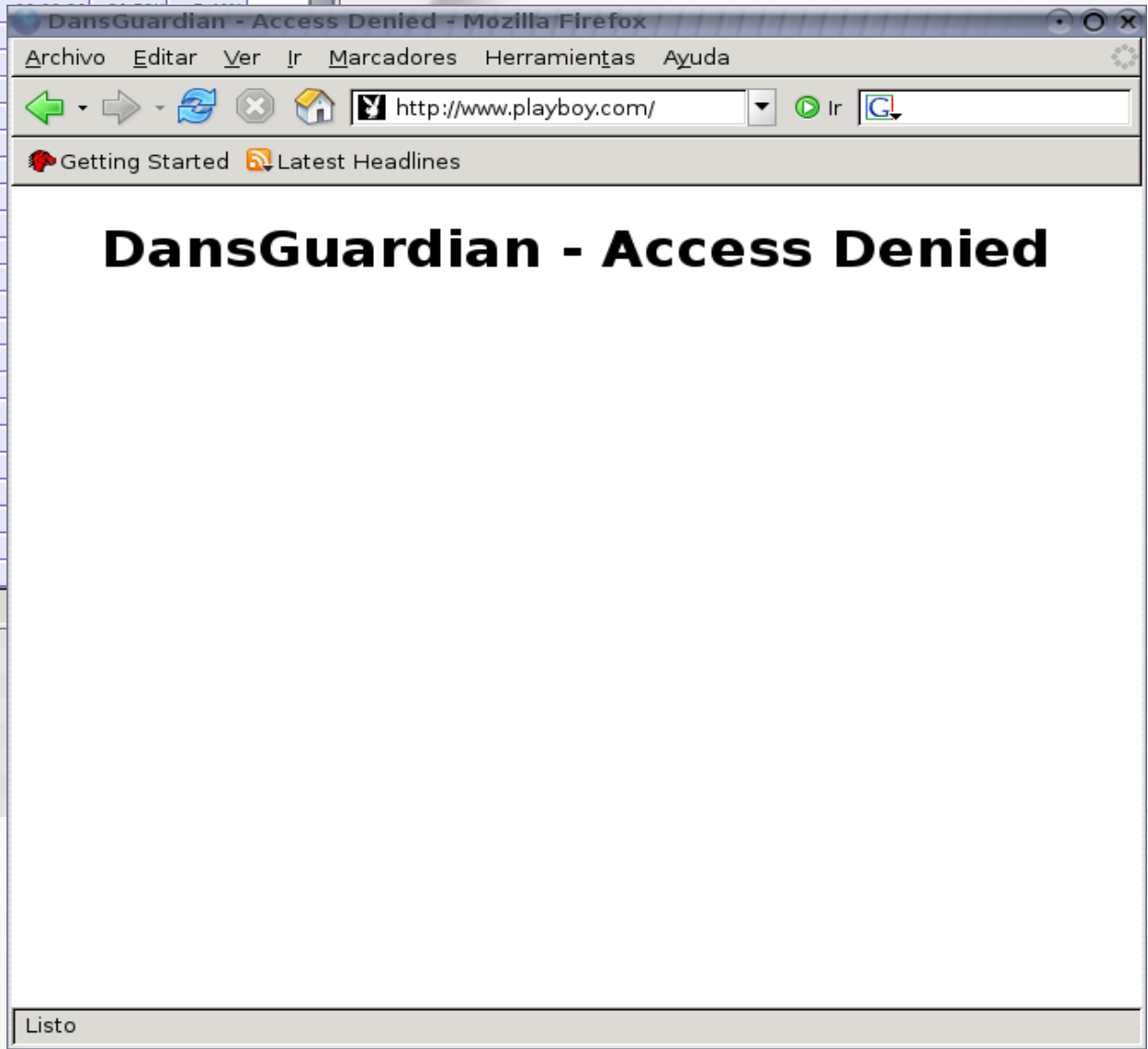
```
root@D3NI4L:~# sarg
root@D3NI4L:~#
```

- El reporte se genera en un directorio llamado squid-reports dentro de la raiz del servidor WEB:
  http://localhost/squid-reports/


Mozilla Firefox
Archivo Editar Ver Ir Marcadores Herramientas Ayuda
http://localhost/squid-reports/
Ir
Getting Started
Latest Headlines
Squid Analysis Report Generator
Squid User Access Reports
FILE/PERIOD
CREATION DATE
USERS
BYTES
AVERAGE
20060ct12-20060ct12
jue oct 12 18:11:36 COT 2006
1
1.13M
1.13M
20060ct12-20060ct13
vie oct 13 13:27:22 COT 2006
1
3.54M
3.54M
Generated by sarg-2.1 Nov-29-2005 on Oct/13/2006 13:27
Listo


Mozilla Firefox
Archivo Editar Ver Ir Marcadores Herramientas Ayuda
http://localhost/squid-reports/2(
Ir
Getting Started
Latest Headlines
Squid Analysis Report Generator
Squid User Access Reports
Period: 20060ct12-20060ct12
Sort: BYTES, reverse
Topuser Report
Topsites Report
Sites & Users Report
Downloads Report
NUM
USERID
CONNECT
BYTES
%BYTES
IN-CACHE-OUT
ELAPSED TIME
MILISEC
%TIME
1
127.0.0.1
182
1.13M
100.00%
0.00%
100.00%
00:00:00
0
0.00%
TOTAL
182
1.13M
0.00%
100.01%
00:00:00
0
AVERAGE
182
1.13M
00:00:00
0
Generated by sarg-2.1 Nov-29-2005 on Oct/12/2006 18:11
Listo


Mozilla Firefox
Archivo Editar Ver Ir Marcadores Herramientas Ayuda
http://localhost/squid-reports/2(
Ir
Getting Started
Latest Headlines
SARG
Squid Analysis Report Generator
Squid User Access Reports
Period: 20060ct12-20060ct12
User: 127.0.0.1
Sort: BYTES, reverse
User Report
ACCESSED SITE
CONNECT
BYTES
%BYTES
IN-CACHE-OUT
ELAPSED TIME
MILISEC
%TIME
by114fd.bay114.hotmail.msn.com 12 275.22K 24.16% 0.00% 100.00%
www.google.com.co 24 152.33K 13.37% 0.00% 100.00%
www.linuca.org 17 149.32K 13.11% 0.00% 100.00%
www.gra2.com 13 122.57K 10.76% 0.00% 100.00%
www.playboy.com 4 104.98K 9.22% 0.00% 100.00%
rad.msn.com 36 66.77K 5.86% 0.00% 100.00%
pagead2.googlesyndication.com 6 46.82K 4.11% 0.00% 100.00%
sarg.sourceforge.net 4 34.13K 3.00% 0.00% 100.00%
login.live.com:443 6 31.45K 2.76% 0.00% 100.00%
login.live.com 4 25.03K 2.20% 0.00% 100.00%
www.google-analytics.com 2 19.35K 1.70% 0.00% 100.00%
newsrss.bbc.co.uk 1 17.42K 1.53% 0.00% 100.00%
view.atdmt.com 6 17.18K 1.51% 0.00% 100.00%
mirror12.escomposlinux.org 1 16.21K 1.42% 0.00% 100.00%
spe.atdmt.com 1 12.62K 1.11% 0.00% 100.00%
s13.sitemeter.com 6 8.84K 0.78% 0.00% 100.00%
llistes.bulma.net 3 7.17K 0.63% 0.00% 100.00%
www.hotmail.msn.com 2 5.63K 0.49% 0.00% 100.00%
h.msn.com 11 5.59K 0.49% 0.00% 100.00%
www.paypal.com:443 1 4.62K 0.41% 0.00% 100.00%
hp.msn.com 2 2.90K 0.26% 0.00% 100.00%
www.google.com 5 2.69K 0.24% 0.00% 100.00%
Listo


DansGuardian - Access Denied - Mozilla Firefox
Archivo Editar Ver Ir Marcadores Herramientas Ayuda
http://www.playboy.com/
Ir
Getting Started
Latest Headlines
DansGuardian - Access Denied
Listo