Servidor de seguridad perimetral II

Por. Daniel Vazart

Proxy + filtro de contenidos + estadísticas

- **Squid** (http://www.squid-cache.org/): Squid es un Servidor Intermediario (Proxy) de alto desempeño que se ha venido desarrollando desde hace varios años y es hoy en día un muy popular y ampliamente utilizado entre los sistemas operativos como GNU/Linux y derivados de Unix®. Es muy confiable, robusto y versátil y se distribuye bajo los términos de la Licencia Pública General GNU (GNU/GPL).

Proxy + filtro de contenidos + estadísticas

- **Dansguardian** (http://dansguardian.org/):
  Dansguardian es un Proxy con filtro de contenidos para sistemas Unix como: Linux, FreeBSD, OpenBSD, NetBSD, Mac OS X, HP-UX y Solaris que pueden correr Squid como WEB Proxy.
  Dansguardian realiza el filtrado por diferentes métodos como el filtrado de URL y nombres de dominio, filtrado de frases en el contenido de una pagina, filtrado por PICS, filtro por tipos de archivos y filtros por POST.
  El filtrado de frases en el contenido chequea las paginas en busca de palabras obscenas, pornográficas y otras no deseadas. El filtrado de POSTS permite bloquear o limitar la subida de archivos por Internet. El filtro de URL y de nombres de dominio, permite manejar grandes listas y es considerablemente mas rápido que SquidGuard.

Proxy + filtro de contenidos + estadísticas

- **SARG** (http://sarg.sourceforge.net): Es un analizador de logs para Squid que genera reportes WEB sobre la navegación a través del proxy.

Requerimientos del sistema

- Dansguardian requiere un mínimo de 150 MHz de procesador y 32 MB de memoria RAM por cada 50 usuarios concurrentes.
- Para sitios con un mayor trafico, se recomienda tener un servidor dedicado con por lo menos 256 MB de memoria RAM y 1 Ghz de procesador.

1. Configurar el firewall para el proxy transparente.

- En primer lugar, es importante habilitar la opción del kernel que permite el fordward de IP para que NAT funcione correctamente:

```
ono:~# echo 1 > /proc/sys/net/ipv4/ip_forward
ono:~#
```

- Para que el proxy sea realmente transparente, se pueden redirigir las peticiones por el puerto 80 al puerto donde trabaja dansguardian:

```
ono:~# iptables -t nat -A PREROUTING -m tcp -p tcp --dport 80 -j REDIRECT --to-port 8080
ono:~#
```

1. Configurar el firewall para el proxy transparente.

- Evitar que los usuarios de la red configuren directamente el proxy para saltarse el filtro de contenidos !

```
ono:~# iptables -A INPUT -m tcp -p tcp -s ! 127.0.0.1 --dport 3128 -j DROP
ono:~#
```

2. Instalar y configurar el proxy.

```
ono:~# apt-get install squid
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes extras:
  squid-common
Paquetes sugeridos:
  squidclient squid-cgi logcheck-database resolvconf winbind smbclient
Se instalarán los siguientes paquetes NUEVOS:
  squid squid-common
0 actualizados, 2 se instalarán, 0 para eliminar y 236 no actualizados.
Necesito descargar 963kB de archivos.
Se utilizarán 6005kB de espacio de disco adicional después de desempaquetar.
¿Desea continuar? [S/n]
Des:1 http://http.us.debian.org stable/main squid-common 2.5.9-10sarge2 [195kB]
Des:2 http://http.us.debian.org stable/main squid 2.5.9-10sarge2 [768kB]
Descargados 963kB en 21s (44,9kB/s)
Preconfigurando paquetes ...
Seleccionando el paquete squid-common previamente no seleccionado.
(Leyendo la base de datos ...
144211 ficheros y directorios instalados actualmente.)
Desempaquetando squid-common (de .../squid-common_2.5.9-10sarge2_all.deb) ...
Seleccionando el paquete squid previamente no seleccionado.
Desempaquetando squid (de .../squid_2.5.9-10sarge2_i386.deb) ...
Configurando squid-common (2.5.9-10sarge2) ...
Configurando squid (2.5.9-10sarge2) ...
Starting proxy server: squid.

ono:~#
```

2. Instalar y configurar el proxy.

```
ono:~# nmap localhost

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2006-09-29 08:59 COT
Interesting ports on localhost.localdomain (127.0.0.1):
(The 1645 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
111/tcp  open  rpcbind
143/tcp  open  imap
443/tcp  open  https
783/tcp  open  hp-alarm-mgr
788/tcp  open  unknown
953/tcp  open  rndc
993/tcp  open  imaps
995/tcp  open  pop3s
3128/tcp open  squid-http
3306/tcp open  mysql
5432/tcp open  postgres
6002/tcp open  X11:2

Nmap finished: 1 IP address (1 host up) scanned in 0.237 seconds
ono:~#
```

2. Instalar y configurar el proxy.

- El archivo de configuración de Squid esta ubicado en: **/etc/squid/squid.conf**
- Para editarlo solo es necesario abrirlo con nano: **nano /etc/squid/squid.conf**
- Despues de editar la configuración de Squid, recuerde reiniciar el servicio con: **/etc/init.d/squid restart**

2. Instalar y configurar el proxy.

- Squid está lleno de opciones interesantes, pero para nuestra aplicación nos interesa tomar unas pocas para que el proxy funcione correctamente, estas opciones son:
- **http_port:** Es el puerto por el cual navegarán los usuarios.
- **Las siguientes opciones no son obligatorias, solo se configuran si se quiere hacer un cache de las paginas que se naveguen:**
- **cache_mem:** Es la cantidad de memoria que se destinará para los objetos en transito.
- **cache_dir:** Aquí se define el tamaño y el directorio que guardará el cache.

3. Instalar y configurar Dansguardian.

```
ono:~# apt-get install dansguardian
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  dansguardian
0 actualizados, 1 se instalarán, 0 para eliminar y 236 no actualizados.
Necesito descargar 238kB de archivos.
Se utilizarán 967kB de espacio de disco adicional después de desempaquetar.
Des:1 http://http.us.debian.org stable/main dansguardian 2.8.0.4-2 [238kB]
Descargados 238kB en 4s (58,3kB/s)
Seleccionando el paquete dansguardian previamente no seleccionado.
(Leyendo la base de datos ...
145226 ficheros y directorios instalados actualmente.)
Desempaquetando dansguardian (de .../dansguardian_2.8.0.4-2_i386.deb) ...
Configurando dansguardian (2.8.0.4-2) ...
adduser: Aviso: El directorio home que Usted especificó ya existe.
Añadiendo usuario del sistema dansguardian...
Adding new group `dansguardian' (119).
Adding new user `dansguardian' (119) with group `dansguardian'.
El directorio home /var/log/dansguardian ya existe.
        DansGuardian has not been configured!
        Please edit /etc/dansguardian/dansguardian.conf manually then rerun
        this script.

ono:~#
```

3. Instalar y configurar Dansguardian.

- El archivo de configuración de Dansguardian esta ubicado en: **/etc/dansguardian/dansguardian.conf**
- Para editarlo solo es necesario abrirlo con nano: **nano /etc/dansguardian/dansguardian.conf**
- Despues de editar la configuración de Dansguardian, recuerde reiniciar el servicio con: **/etc/init.d/dansguardian restart**

3. Instalar y configurar Dansguardian.

```
# DansGuardian config file for version 2.8.0

# **NOTE** as of version 2.7.5 most of the list files are now in dansguardianf1.conf


# Comment this line out once you have modified this file to suit your needs
#UNCONFIGURED


# Web Access Denied Reporting (does not affect logging)
#
# -1 = log, but do not block - Stealth mode
#  0 = just say 'Access Denied'
#  1 = report why but not what denied phrase
#  2 = report fully
#  3 = use HTML template file (accessdeniedaddress ignored) - recommended
#
reportinglevel = 0

# Language dir where languages are stored for internationalisation.
# The HTML template within this dir is only used when reportinglevel
# is set to 3. When used, DansGuardian will display the HTML file instead of
# using the perl cgi script.  This option is faster, cleaner
# and easier to customise the access denied page.
# The language file is used no matter what setting however.
#
```

3. Instalar y configurar Dansguardian.

```
# the page gets let through.  Can be useful for diagnosing
# why a site gets through the filter.  on | off
logexceptionhits = on

# Log File Format
# 1 = DansGuardian format        2 = CSV-style format
# 3 = Squid Log File Format      4 = Tab delimited
logfileformat = 3


# Log file location
#
# Defines the log directory and filename.
#loglocation = '/var/log/dansguardian/access.log'


# Network Settings
#
# the IP that DansGuardian listens on.  If left blank DansGuardian will
# listen on all IPs.  That would include all NICs, loopback, modem, etc.
# Normally you would have your firewall protecting this, but if you want
# you can limit it to only 1 IP.  Yes only one.
filterip =

# the port that DansGuardian listens to.
filterport = 8080
```

3. Instalar y configurar Dansguardian.

```
# Network Settings
#
# the IP that DansGuardian listens on.  If left blank DansGuardian will
# listen on all IPs.  That would include all NICs, loopback, modem, etc.
# Normally you would have your firewall protecting this, but if you want
# you can limit it to only 1 IP.  Yes only one.
filterip =

# the port that DansGuardian listens to.
filterport = 8080

# the ip of the proxy (default is the loopback - i.e. this server)
proxyip = 127.0.0.1

# the port DansGuardian connects to proxy on
proxyport = 3128
```

3. Instalar y configurar Dansguardian.

```
ono:~# /etc/init.d/dansguardian start
Starting DansGuardian: dansguardian.
ono:~# nmap localhost

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2006-09-29 11:04 COT
Interesting ports on localhost.localdomain (127.0.0.1):
(The 1644 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
111/tcp  open  rpcbind
143/tcp  open  imap
443/tcp  open  https
783/tcp  open  hp-alarm-mgr
788/tcp  open  unknown
953/tcp  open  rndc
993/tcp  open  imaps
995/tcp  open  pop3s
3128/tcp open  squid-http
3306/tcp open  mysql
5432/tcp open  postgres
6002/tcp open  X11:2
8080/tcp open  http-proxy

Nmap finished: 1 IP address (1 host up) scanned in 0.238 seconds
ono:~#
```

4. Configuración de los filtros

- Para realizar la actualización de las listas de bloqueo por frases, puede descargarlas de la pagina: **http://contentfilter.futuragts.com/phraselists/**
- Descomprima el archivo y reemplace el contenido del directorio **/etc/dansguardian/phraselists/** por el contenido del archivo descargado. Luego deberá reemplazar los archivos: **bannedphraselist**, **bannedregexpurllist**, **exceptionphraselist** y **weightedphraselist**; por sus iguales en el archivo descargado.

4. Configuración de los filtros

- **Bannedextensionlist**: Extensiones de archivo no permitidas.
- **Bannedmimetypelist**: Tipos MIME no permitidos.
- **Bannedsitelist**: Sitios no permitidos.
- **Exceptioniplist**: IP no filtradas.
- **Exceptionsitelist**: Sitios no filtrados.
- **Bannediplist**: IP sin derechos de navegación.

4. Configuración de los filtros

```
ono:~/filtros# wget http://contentfilter.futuragts.com/phraselists/phraselistsmay31.tar
.gz
--13:32:43--  http://contentfilter.futuragts.com/phraselists/phraselistsmay31.tar.gz
           => `phraselistsmay31.tar.gz'
Resolviendo contentfilter.futuragts.com... 24.79.172.191
Conectando con contentfilter.futuragts.com[24.79.172.191]:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 55,958 [application/x-gzip]

100%[==========================================>] 55,958        20.96K/s

13:32:46 (20.91 KB/s) - `phraselistsmay31.tar.gz' guardado [55958/55958]

ono:~/filtros#
```

```
ono:~/filtros# ls
phraselistsmay31.tar.gz
ono:~/filtros# gunzip phraselistsmay31.tar.gz
ono:~/filtros# tar -xpf phraselistsmay31.tar
ono:~/filtros# ls
phraselists  phraselistsmay31.tar
ono:~/filtros#
```

4. Configuración de los filtros

```
ono:~/filtros# cd /etc/dansguardian/
ono:/etc/dansguardian# ls
bannedextensionlist  bannedurllist       exceptionphraselist  greyurllist
bannediplist         banneduserlist      exceptionsitelist    languages
bannedmimetypelist   contentregexplist    exceptionurllist     phraselists
bannedphraselist     dansguardian.conf   exceptionuserlist    pics
bannedregexpurllist  dansguardianf1.conf  filtergroupslist     transparent1x1.gif
bannedsitelist       exceptioniplist     greysitelist         weightedphraselist
ono:/etc/dansguardian# mv phraselists/ phraselists.viejas
ono:/etc/dansguardian# ls
bannedextensionlist  bannedurllist       exceptionphraselist  greyurllist
bannediplist         banneduserlist      exceptionsitelist    languages
bannedmimetypelist   contentregexplist    exceptionurllist     phraselists.viejas
bannedphraselist     dansguardian.conf   exceptionuserlist    pics
bannedregexpurllist  dansguardianf1.conf  filtergroupslist     transparent1x1.gif
bannedsitelist       exceptioniplist     greysitelist         weightedphraselist
ono:/etc/dansguardian# mv /root/filtros/phraselists /etc/dansguardian/
ono:/etc/dansguardian# ls
bannedextensionlist  banneduserlist      exceptionurllist   phraselists.viejas
bannediplist         contentregexplist   exceptionuserlist  pics
bannedmimetypelist   dansguardian.conf   filtergroupslist   transparent1x1.gif
bannedphraselist     dansguardianf1.conf  greysitelist      weightedphraselist
bannedregexpurllist  exceptioniplist     greyurllist
bannedsitelist       exceptionphraselist  languages
bannedurllist        exceptionsitelist    phraselists
ono:/etc/dansguardian#
```

4. Configuración de los filtros

```
ono:/etc/dansguardian# ls
bannedextensionlist  banneduserlist      exceptionurllist   phraselists.viejas
bannediplist         contentregexplist   exceptionuserlist  pics
bannedmimetypelist   dansguardian.conf   filtergroupslist   transparent1x1.gif
bannedphraselist     dansguardianf1.conf greysitelist       weightedphraselist
bannedregexpurllist  exceptioniplist     greyurllist
bannedsitelist       exceptionphraselist languages
bannedurllist        exceptionsitelist   phraselists
ono:/etc/dansguardian# mv bannedphraselist bannedphraselist.vieja
ono:/etc/dansguardian# mv bannedregexpurllist bannedregexpurllist.vieja
ono:/etc/dansguardian# mv exceptionphraselist exceptionphraselist.vieja
ono:/etc/dansguardian# mv weightedphraselist weightedphraselist.vieja
ono:/etc/dansguardian# ls
bannedextensionlist        dansguardian.conf         greyurllist
bannediplist               dansguardianf1.conf       languages
bannedmimetypelist         exceptioniplist           phraselists
bannedphraselist.vieja     exceptionphraselist.vieja phraselists.viejas
bannedregexpurllist.vieja  exceptionsitelist         pics
bannedsitelist             exceptionurllist          transparent1x1.gif
bannedurllist              exceptionuserlist         weightedphraselist.vieja
banneduserlist             filtergroupslist
contentregexplist          greysitelist
ono:/etc/dansguardian#
```

4. Configuración de los filtros

```
ono:/etc/dansguardian# cd phraselists
ono:/etc/dansguardian/phraselists# ls
badwords              games           news                          violence
bannedphraselist      goodphrases     notes for creating lists.txt  warezhacking
bannedregexpurllist   googlesearches  nudism                        weapons
chat                  gore            peer2peer                     webmail
drugadvocacy          illegaldrugs    personals                     weightedphraselist
exceptionphraselist   intolerance     pornography
forums                legaldrugs      proxies
gambling              malware         sport
ono:/etc/dansguardian/phraselists# mv bannedphraselist /etc/dansguardian/
ono:/etc/dansguardian/phraselists# mv bannedregexpurllist /etc/dansguardian/
ono:/etc/dansguardian/phraselists# mv exceptionphraselist /etc/dansguardian/
ono:/etc/dansguardian/phraselists# mv weightedphraselist /etc/dansguardian/
ono:/etc/dansguardian/phraselists#
```

CONTINUARÁ...