DANS GUARDIAN

1.Qué es DansGuardian.

La herramienta DansGuardian es código abierto, está desarrollada en C++ y permite una configuración flexible adaptándose a las necesidades del usuario.

Al instalar el paquete la configuración por defecto ya limita las visitas a páginas prohibidas para menores, pero dispone de gran cantidad de archivos de configuración para llevar a cabo un ajuste del servicio mas personalizado.

El mecanismo es el siguiente: los clientes mediante sus navegadores web hacen peticiones de páginas que son recibidas por DansGuardian y sólo son redireccionadas al servidor proxy SQUID aquellas que superan la fase de filtrado.

En realidad DansGuardian se ejecuta como un demonio independiente del proxy, acepta peticiones en el puerto 8080 y las redirecciona al proxy SQUID, que escucha en el puerto 3128.

Por lo tanto, cuando una petición entra por el puerto 8080, DansGuardian la filtra y la pasa al Proxy SQUID por el puerto 3128. Es importante, en consecuencia, que ningún otro servicio esté utilizando el puerto 8080.

Si el resultado del filtrado (dependiendo de los filtros configurados) es una denegación de acceso a una determinada página web se muestra al usuario el mensaje correspondiente al 'Acceso Denegado'. Si DansGuardian está en la máquina que hace de cortafuegos y se configura un proxy transparente en SQUID, habrá que redireccionar todo el tráfico de la LAN hacia el puerto 80 al puerto 8080, donde DansGuardian escucha. Es decir, se capturan todas las peticiones que se hagan a un servidor http (petición de páginas web) y se envían a DansGuardian (8080) para que se encargue del filtrado.

iptables -t nat A PREROUTING -i eth0 -p tcp --dport 3128 –j REDIRECT --to-port 8080

En el caso de acceder a páginas seguras que utilizan el protocolo https (puerto 443) también deberán ser redirigidas.

2.Instalar clamav

Instalamos en primer lugar el antivirus clamav.

sudo apt-get install clamavdaemon clamavfreshclam

3.Instalar DansGuardian

sudo apt-get install dansguardian

4.Configurando DansGuardian

El archivo de configuración es /etc/dansguardian/dansguardian.conf
Pasos para la configuración:

Establecer la línea que contiene la directiva #UNCONFIGURED como un comentario. Para ello añadir al principio de la línea el carácter '#'. Si no lo hacemos así, DansGuardian pensará que no nos hemos molestado en configurarlo.

#UNCONFIGURED - Please remove this line after configuration
En la sección 'Network Settings' comprobar que están las líneas siguientes:

filterip = <ip donde escucha dansguardian>
filterport = 8080
proxyip = 127.0.0.1
proxyport = 3128

Modificar el idioma por defecto. Para ello sustituir el inglés por 'spanish' y dejar las líneas como sigue:

languagedir = '/etc/dansguardian/languages'

 # language to use from languagedir.

language = 'spanish'

Para que DansGuardian se sincronice con el antivirus Clamav, debemos descomentar la siguiente línea:

#contentscanner = '/etc/dansguardian/contentscanners/clamav.conf'
Salir de gedit salvando los cambios y reiniciar el servicio dansguardian ejecutando la orden:

$sudo /etc/init.d/dansguardian restart

5.Cuidado con los descuidos

Tal y como lo hemos dejado, alguien que sencillamente no ataque al puerto 8080 no pasará por el filtro de DansGuardian. Debemos por tanto forzar a que el tráfico http sea redirigido al puerto 8080.

iptables –t nat –A PREROUTING –i eth0 –p tcp --dport 3128 –j REDIRECT --toport 8080

iptables –t nat –A PREROUTING –i eth0 –p tcp –dport 80 –j REDIRECT --toport 8080

¿Para qué sirve la primera regla? ¿Y la segunda?

Si estamos redireccionando, necesitaremos definir squid como transparente.

6.Ficheros de filtros en DansGuardian

Archivos de filtros en /etc/dansguardian/
Archivo Descripción

bannedphraselist contiene una lista de frases prohibidas. Las frases deben estar entre <>. Por defecto incluye una lista ejemplo en inglés. Las frases pueden contener espacios.

Se puede también utilizar combinaciones de frases, que si se encuentran en una página, serán bloqueadas.

Archivos de filtros en /etc/dansguardian/

bannedmimetypelist contiene una lista de tipos MIME prohibidos. Si una URL devuelve un tipo MIME incluido en la lista, quedará bloqueada. Por defecto se incluyen algunos ejemplos de tipos MIME que serán bloqueados.
bannedextensionlist contiene una lista de extensiones de archivos no permitidas. Si una URL termina con

alguna extensión contenida en esta lista, será bloqueada. Por defecto se incluye un archivo ejemplo que muestra como denegar extensiones.

bannedregexpurllist contiene una lista de expresiones regulares3 que si se cumplen sobre la URL ésta será bloqueada.

bannedsitelist contiene una lista de sitios prohibidos. Si se indica un nombre de dominio todo él será bloqueado. Si se quiere sólo bloquear partes de un sitio hay que utilizar el archivo bannedurllist. También se pueden bloquear los sitios indicados exeptuando los dados en el archivo exceptionsitelist. Existe la posibilidad de descargarse listas negras tanto de sitios como de URLs y situarlas en los archivos correspondientes. Están disponibles en http://dansguardian.org/?page=extras.

bannedurllist permite bloquear partes específicas de un sitio web.

bannedsitelist bloquea todo el sitio web y ésta sólo bloquea una parte.

banneduserlist lista de los nombres de usuario que estarán bloqueados.

Archivos de excepciones en /etc/dansguardian/

Archivo Descripción

exceptionsitelist contiene una lista de los nombres de dominio que no serán filtrados Es importante tener en cuenta que el nombre de dominio no debe incluir http:// o www.

exceptioniplist contiene una lista de las direcciones IP de los clientes a los que se permite el acceso sin restricciones. este sería el caso de la dirección IP del administrator.

exceptionuserlist lista de los nombres de usuarios que no serán filtrados en el caso de utilizar control de acceso por usuario. Requiere autenticación básica o "ident".

exceptionphraselist lista de las frases que, si aparecen en una página web, pasará el filtro.

7. Definir grupos

Puede que queramos definir ciertas reglas de filtrado dependiendo del usuario. Para ello seguiremos los siguientes pasos (en nuestro ejemplo usaremos dos grupos, aunque todo esto es generalizable hasta 99 grupos, lo que es imposible de mantener).

Primero vamos a crear dos directorios, uno para cada grupo, a saber:

/etc/dansguardian/f1
/etc/dansguardian/f2

Dentro de cada uno de estos directorios, pondremos las reglas de filtrado específicas para cada grupo:

cp -r /etc/dansguardian/lists /etc/dansguardian/f1
cp –r /etc/dansguardian/lists /etc/dansguardian/f2

Ahora, para no aligerar un poco el directorio /etc/dansguardian, vamos a meter los directorios f1 y f2 en /etc/dansguarian/lists.

mv /etc/dansguardian/f1 /etc/dansguardian/lists/
mv /etc/dansguaridian/f2 /etc/dansguardia/lists/

También vamos a crear los ficheros de configuración de cada grupo. Inicialmente ya existe dansguardianf1.conf (para el grupo 1, por defecto). A partir de este vamos a crear el segundo.

cp /etc/dansguardian/dansguardianf1.conf /etc/dansguardian/dansguardianf2.conf

Debemos modificar el contenido de dansguardianf1.conf y dansguardianf2.conf, para que importen las reglas desde /etc/dansguardian/lists/f1 y /etc/dansguardian/lists/f2 respectivamente.

Podemos hacer esto utilizando gedit.

Ahora, vamos a modificar el fichero dansguardian.conf para lo siguiente:
1. Que dansguardian sepa que hay dos grupos.
2. Para poder establecer una equivalencia entre ciertas ips y cada uno de los grupos.
Modificamos las siguientes líneas en /etc/dansguardian/dansguardian.conf
filtergroups=2
authplugin = '/etc/dansguardian/authplugins/ip.conf' # descomentar esta línea. Ahora solo queda asociar cada ip a cada grupo. Esto podemos hacerlo en el fichero que se indica en /etc/dansguardian/authplugins/ip.conf, es decir en /etc/dansguardian/lists/authplugins/ipgroups.

Allí escribiremos algo como lo siguiente:

172.16.0.51=filter1
172.16.0.52=filter2

Hecho esto, reiniciamos DansGuardian, y debería diferenciar entre los dos grupos. Para comprobarlo, añadiremos en las reglas de cada grupo, un sitio diferente. Por ejemplo, añadir en /etc/dansguardian/lists/f1/bannedsitelist la siguiente línea

sitio1.com

Ahora añadiremos la siguiente línea en

/etc/dansguardian/lists/f2/bannedsitelist:

sitio2.com

Reiniciamos Dansguardian, y a hacer pruebas.

NOTA: este manual es de internet solo lo aporto para compartir conocimientos con la comunidad de taringa.....Viva el software libre