DISICO

Instalación paso a paso de MailScanner en Linux

Manual

Instalación paso a paso de MailScanner en Linux

Los WebMasters que trabajamos con la plataforma Linux podemos proteger a nuestros usuarios de email, usando una potente aplicación: **MailScanner**.

MailScanner procesa cada mensaje que se recibe en el servidor antes de colocarlo en el fichero correspondiente al buzón del usuario de email. Si encontrara cualquier tipo de virus, eliminaría el fichero adjunto y daría aviso al emisor, al destinatario y al postmaster.

A continuación se explica detalladamente el método a seguir para realizar la compilación e instalación de MailScanner, junto con F-Prot, que es el más potente de los antivirus gratuitos para Linux:

Se instala un antivirus gratuito: F-Prot

Más información en http://linux.bankhacker.com/software/F-Prot+Antivirus+for+Linux/

```
mkdir /home/install/servicios/antivirus/
cd /home/install/servicios/antivirus/
wget "ftp://ftp.f-prot.com/pub/fp-linux_beta.tar.gz"

cd /usr/local/
tar -zxvf /home/install/servicios/antivirus/fp-linux_beta.tar.gz
ln -fs /usr/local/fp-linux_311b_beta /usr/local/f-prot
ln -fs /usr/local/f-prot/f-prot.sh /usr/local/bin/f-prot
chmod +x /usr/local/f-prot/f-prot*

/usr/local/bin/f-prot -help
```

Se instala el sistema de revisión antivirica del E-Mail: MailScanner

```
cd /home/install/servicios/antivirus/
wget "http://www.sng.ecs.soton.ac.uk/mailscanner/files/MailScanner-3.12-4.tar"

cd /usr/local/
tar -xvf /home/install/servicios/antivirus/MailScanner-3.12-4.tar
```

Configure Sendmail

```
cd /var/spool
mkdir mqueue.in
chown root mqueue.in
chgrp bin mqueue.in
chmod u=rwx,g=rx,o-rwx mqueue.in

cp -f /etc/rc.d/init.d/sendmail /etc/rc.d/init.d/sendmail.old
```

vi /etc/rc.d/init.d/sendmail
Se busca la cadena
"sendmail -bd -q15m"
ó
"daemon /usr/sbin/sendmail $(["$DAEMON" = yes] && echo -bd) $([-n "$QUEUE"] && echo -q$QUEUE)"
y se reemplaza por
"sendmail -bd -ODeliveryMode=queueonly -OQueueDirectory=/var/spool/mqueue.in ; sendmail -q15m"
ó
"daemon /usr/sbin/sendmail -bd -ODeliveryMode=queueonly -OQueueDirectory=/var/spool/mqueue.in ;
daemon /usr/sbin/sendmail $(["$DAEMON" = yes] && echo -bd) $([-n "$QUEUE"] && echo -q$QUEUE)"

Se instalan los módulos de Perl necesarios

IO-stringy (I used version 1.211)

```
### REFERENCIA: http://search.cpan.org/search?dist=IO-stringy
### REFERENCIA: http://www.cpan.org/authors/id/ERYQ/IO-stringy-2.108.tar.gz
mkdir /home/install/programacion/perl/
cd /home/install/programacion/perl/
wget "http://www.cpan.org/authors/id/ERYQ/IO-stringy-2.108.tar.gz"
cd /usr/src/
tar -zxvf /home/install/programacion/perl/IO-stringy-2.108.tar.gz
cd /usr/src/IO-stringy-2.108/
perl Makefile.PL
make
make test
make install
```

MIME-Base64 (I used version 2.11)

```
### REFERENCIA: http://search.cpan.org/search?dist=MIME-Base64
### REFERENCIA: http://www.cpan.org/authors/id/GAAS/MIME-Base64-2.12.tar.gz
mkdir /home/install/programacion/perl/
cd /home/install/programacion/perl/
wget "http://www.cpan.org/authors/id/GAAS/MIME-Base64-2.12.tar.gz"
cd /usr/src/
tar -zxvf /home/install/programacion/perl/MIME-Base64-2.12.tar.gz
cd /usr/src/MIME-Base64-2.12/
perl Makefile.PL
make
make test
make install
```

MailTools (I used version 1.1401)

```
### REFERENCIA: http://search.cpan.org/search?dist=MailTools
### REFERENCIA: http://www.cpan.org/authors/id/M/MA/MARKOV/MailTools-1.43.tar.gz
mkdir /home/install/programacion/perl/
cd /home/install/programacion/perl/
wget "http://www.cpan.org/authors/id/M/MA/MARKOV/MailTools-1.43.tar.gz"
cd /usr/src/
tar -zxvf /home/install/programacion/perl/MailTools-1.43.tar.gz
cd /usr/src/MailTools-1.43/
perl Makefile.PL
make
make test
make install
```

File-Spec (I used version 0.82)

```
### REFERENCIA: http://search.cpan.org/search?dist=File-Spec
### REFERENCIA: http://www.cpan.org/authors/id/R/RB/RBS/File-Spec-0.82.tar.gz
mkdir /home/install/programacion/perl/
cd /home/install/programacion/perl/
wget "http://www.cpan.org/authors/id/R/RB/RBS/File-Spec-0.82.tar.gz"
cd /usr/src/
tar -zxvf /home/install/programacion/perl/File-Spec-0.82.tar.gz
cd /usr/src/File-Spec-0.82/
perl Makefile.PL
make
make test
make install
```

MIME-tools (at least version 5.410, I used version 5.411)

```
### REFERENCIA: http://search.cpan.org/search?dist=MIME-tools
### REFERENCIA: http://www.cpan.org/authors/id/ERYQ/MIME-tools-5.411a.tar.gz
mkdir /home/install/programacion/perl/
cd /home/install/programacion/perl/
wget "http://www.cpan.org/authors/id/ERYQ/MIME-tools-5.411a.tar.gz"
cd /usr/src/
tar -zxvf /home/install/programacion/perl/MIME-tools-5.411a.tar.gz
cd /usr/src/MIME-tools-5.411/
perl Makefile.PL
make
make test
make install
```

Se instala el decodificador TNEF, que se encarga de transcribir los ficheros en formato RTF

```
cd /usr/src/
tar -zxvf /usr/local/MailScanner-3.12-4/mailscanner/bin/tnef-1.1.1+sizelimit.tar.gz
ln -sf tnef-1.1.1+sizelimit tnef-1.1
cd tnef-1.1
./configure
make
mv /usr/local/MailScanner-3.12-4/mailscanner/bin/tnef /usr/local/MailScanner-3.12-
4/mailscanner/bin/tnef.old
cp src/tnef /usr/local/MailScanner-3.12-4/mailscanner/bin/tnef
```

Se configura el MailScanner

```
cd /usr/local/MailScanner-3.12-4/mailscanner/etc/
rm -f mailscanner.conf
ln -fs mailscanner.conf.linux mailscanner.conf

cd /usr/local/MailScanner-3.12-4/mailscanner/
### Hay que reemplazar
### "/opt/mailscanner/"
### por
### "/usr/local/MailScanner-3.12-4/mailscanner/"
### en los siguientes ficheros:
###
###   bin/check_mailscanner:virusdir=/opt/mailscanner/bin
###   bin/check_mailscanner:config=/opt/mailscanner/etc/mailscanner.conf
###
###   bin/config.pl:my $prefix = '/opt/mailscanner';

### Hay que reemplazar
  etc/mailscanner.conf:Virus Scanner      = sophos

### por
  etc/mailscanner.conf:Virus Scanner      = f-prot

### y
  Sweep = /usr/local/Sophos/bin/sophoswrapper

### por
  Sweep = /usr/local/MailScanner-3.12-4/f-prot/f-protwrapper
```

Links de programas del sistema

ln -sf /bin/ps /usr/bin/ps
ln -sf /bin/fgrep /usr/bin/fgrep
ln -sf /bin/grep /usr/bin/grep
ln -sf /bin/sed /usr/bin/sed

Se generan algunos directorios que requiere el scanner de emails
mkdir /var/spool/MailScanner/
mkdir /var/spool/MailScanner/quarantine/
mkdir /var/spool/MailScanner/incoming/

Otros links necesarios
ln -sf /usr/local/MailScanner-3.12-4/mailscanner /usr/local/MailScanner
ln -sf /usr/local/MailScanner-3.12-4/mailscanner/etc/filename.rules.conf
/usr/local/MailScanner-3.12-4/mailscanner/etc/filename.rules

Se añade al cron estas líneas, para asegurarnos de que el mailscanner esta funcionando siempre
18/05/2000 JKF Ensure my e-mail virus scanner is still running
0,20,40 * * * * [-x /usr/local/MailScanner-3.12-4/mailscanner/bin/check_mailscanner]
&& /usr/local/MailScanner-3.12-4/mailscanner/bin/check_mailscanner >/dev/null 2>&1

Se testea el sistema

Descargamos de http://www.eicar.org/anti_virus_test_file.htm un fichero .zip (http://www.eicar.org/download/eicar_com.zip) con un virus inofensivo, para testear el sistema, y lo enviamos por email ... Si todo funciona bien, el mensaje será devuelto y se dará aviso al emisor,
al destinatario y al postmaster.

Otras direcciones interesantes:

http://linux-labs.net/docs/SendmailAntivirus.html => MailScanner y Sendmail en Debian
http://barrapunto.com/article.pl?sid=02/12/26/2139248 => Servidores de correo y antivirus