Antivirus under Linux

Paolo Subiaco
psubiaco@creasol.it
http://www.creasol.it

25 agosto 2002

Sommario

Con questo documento intendo descrivere brevemente come installare gli antivirus in Linux per filtrare le email e lo scambio di dati attraverso proxy e samba.

La trattazione ha uno scopo puramente illustrativo: ulteriore documentazione è indicata nelle note bibliografiche.

1 Filtraggio della posta con Postfix/AMaViS

Attraverso il procedimento sottoriportato si potrà filtrare la posta che transita attraverso il MTA Postfix[1] sfruttando uno script Perl, AMaViS-perl[2], il quale viene richiamato da Postfix alla ricezione di ogni mail e si occupa di estrarre dalla mail ogni singolo attachment per poi farlo processare da uno o più programmi antivirus installati.

La peculiarità di AMaViS-perl è la possibilità di gestire veramente molti antivirus, alcuni OpenSource (come ad esempio ScannerDaemon [3]), altri Freeware (come F-Prot [4]), altri commerciali e quindi con tutto il supporto di aggiornamento dei virus signature, quali TrendMicro [5], Sophos [6], eccetera.

AMaViS è inoltre disponibile come demone (programma sempre residente che in questo caso si chiamerà AMaViSd): in quest'ultimo caso l'esecuzione risulterà velocizzata dalla non necessità di caricare in memoria l'interprete perl e lo script AMaViS-perl alla ricezione di ogni mail. AMaViSd è scritto in Perl ed in C, e pertanto richiede la configurazione, compilazione ed installazione come indicato nella sezione 3.

2 Installazione di AMaViS-perl

L'installazione di AMaViS può risultare critica perché richiede la ricompilazione dell'interprete Perl per l'inserimento di alcuni moduli. Tuttavia l'aggiunta dei moduli può avvenire grazie all'utilizzo di CPAN, e quindi in forma abbastanza automatizzata seguendo le indicazioni riportate nel file README distribuito con AMaViS.

È tuttavia necessaria la modifica del file *amavis* che verrà installato in */usr/sbin* per indicare il percorso degli antivirus installati e per correggere alcuni problemi (loop ricorsivi nell'estrazione di archivi). Il file *amavis* già configurato per l'uso degli antivirus f-prot e ScannerDaemon è disponibile in http://www.ir3ip.net/iw3grx/sw/.

Inoltre è necessaria la configurazione dei file *main.cf* e *master.cf* presenti nella directory di configurazione di Postfix affinché sia richiamato AMaViS alla ricezione di ogni mail dal server in ascolto nella porta 25, e sia attivato un altro server SMTP in ascolto sulla porta 10025 dell'interfaccia localhost.

Le linee da aggiungere in *main.cf* sono

```
content_filter = vscan:
soft_bounce = yes
```

mentre le linee da aggiungere in *master.cf* sono:

```
# enable virus scanning thorugh amavis
vscan unix - n n - 10 pipe user=vscan argv=/usr/sbin/amavis ${sender} ${recipient}
localhost:10025 inet n - n - - smtpd -o content_filter=
flush unix - - n 1000? 0 flush
```

Infine, è necessario creare l'utente *vscan*, magari disabilitandone il login, e creare le directory */var/virusmails* e */var/amavis* che dovranno essere di proprietà dell'utente *vscan* ed avere possibilmente i diritti *700*.

2.1 Installazione di F-Prot

Finché sarà possibile utilizzarlo liberamente in Linux, conviene installare l'antivirus F-Prot [4]: l'installazione non necessita di particolari accorgimenti. È inoltre possibile prelevare gli aggiornamenti in modo automatizzato sfruttando lo script sottoriportato, che può inoltre essere inserito nel crontab affinché sia richiamato quotidianamente.

```
#! /bin/bash
FPROT_DIR=/usr/local/f-prot
mkdir $FPROT_DIR/new 2>/dev/null
cd $FPROT_DIR/new
rm -f *
ncftpget -V ftp://ftp.f-prot.com/pub/fp-def.zip
sleep 30
ncftpget -V ftp://ftp.f-prot.com/pub/macrdef2.zip
unzip fp-def.zip
unzip macrdef2.zip
ls -lt |grep -v zip
mv -f *.DEF ..
rm -f *zip
```

2.2 Installazione di ScannerDaemon

Si tratta di un antivirus basato sul riconoscimento del pattern dei virus, distribuito con licenza GPL e quindi liberamente scaricabile ed utilizzabile.

L'installazione non necessita di particolari accorgimenti, essendo il programma scritto in Java; è richiesto l'uso dell'ambiente JRE, scaricabile dal sito della Sun Microsystem [7].

Si tratta di un demone, ovvero un programma residente, che rimarrà in ascolto in una porta TCP dell'interfaccia localhost; dovrà essere eseguito digitando il comando
java -jar /usr/local/bin/ScannerDaemon.jar /usr/local/bin/virussignatures.txt.signed >/dev/tty12 2>&1 &
e lo stesso comando dovrà essere anche richiamato dal file di startup */etc/rc.d/rc.local.*

Essendo un programma OpenSource, sviluppato durante i ritagli di tempo, non sarà certamente aggiornato, e pertanto verrà richiamato da AMaViS prima di F-Prot al fine di individuare eventuali virus riconosciuti dagli altri antivirus commerciali ma non da ScannerDaemon: in questo modo sarà successivamente possibile ricercare il virus signature attraverso l'utility *PatternFinder* [3] per poi inserirlo in *virussignatures.txt.signed* e distribuirlo agli autori di ScannerDaemon.

3 Installazione di AMaViSd

In questa sezione saranno elencati sinteticamente i passi per l'installazione del demone amavisd; sono da considerarsi *prerequisite* le informazioni riportate in sezione 2.

- Prelievo dell'ultima versione aggiornata dal sito http://www.amavis.org
- Scompattazione dell'archivio con il comando tar xvzf amavisd-snapshot*gz

- ./configure –enable-postfix –with-amavisuser=vscan
- make
- su
- make install

Deve inoltre essere modificato l'init file da cui viene richiamato il MTA utilizzato (postfix nel mio caso): nelle distribuzioni Mandrake basta editare il file */etc/rc.d/init.d/postfix* aggiungendo le linee in grassetto:

```
case "$1" in
start)
# start amavis
echo -n "Start amavis... "
su vscan -c '/usr/sbin/amavisd >/dev/null 2>&1'
# Start daemons.
echo -n "Starting postfix: "
......etc
;;
stop)
# Stop daemons.
echo -n "Shutting down postfix: "
/usr/sbin/postfix stop 2>/dev/null
echo postfix
rm -f /var/lock/subsys/postfix
echo "Shutting down amavisd"
killall amavisd
sleep 1
killall -9 amavisd
;;
restart)
```

A questo punto è sufficiente digitare */etc/rc.d/init.d/postfix restart* per ricaricare il demone AMaViSd ed il MTA.

3.1 Eventuali problemi

Durante la fase di configurazione sono ricercati alcune applicazioni per scomprimere archivi con estensione arc, rar, eccetera.... Sono applicazioni reperibili in internet, magari necessitano di qualche patch [2] affinché risultino compilabili.
È possibile temporaneamente risolvere il problema creando uno script che non fa assolutamente nulla, che sia eseguibile, chiamandolo /usr/bin/arc, linkandolo poi a /usr/bin/unrar, /usr/bin/zoo, eccetera.

Riferimenti bibliografici

[1] Postfix: http://www.postfix.org

[2] AMaViS: http://www.amavis.org

[3] ScannerDaemon: http://www.openantivirus.org

[4] F-Prot: http://www.f-prot.com

[5] Trend Micro Antivirus: http://www.antivirus.com

[6] Sophos Antivirus: http://www.sophos.com

[7] Sun Microsystem & Java: http://www.sun.com