...E liberaci dallo spam quotidiano ...

Tanti anni fa' ....

...alcune compagnie di comunicazioni cominciarono a regalare connessioni ad internet al semplice costo della telefonata urbana. Fu praticamente un boom, ed il successo notevolissimo. Era sufficiente una registrazione presso un provider, ed in pochi minuti si disponeva di un account valido e di una casella di posta elettronica.
Visto il successo di tale iniziativa era prassi comune registrarsi presso parecchi provider, per provare le differenze di servizio, oppure solo per curiosita'. Ovviamente ad ogni registrazione veniva assegnata una ulteriore casella di posta elettronica. Non era assolutamente raro che una stessa persona fosse titolare di una decina di indirizzi email.
Adesso con le moderne ADSL la cosa si e' enfatizzata. Non solo (quasi) tutti gli indirizzi mail registrati in passato son ancora validi, ma altri possono venire assegnati sempre in modo gratuito, oppure a pagamento per chi necessita di funzionalità' particolari. La seccatura e' leggere tutti gli indirizzi !!
Inoltre dobbiamo fare i conti con virus, spam, dialer et similia.
Noi adepti del pinguino abbiamo pochi problemi, nessun virus ci impensierisce, nessun dialer ci tocca, basta settare bene alcune cose tipo il firewall e siamo felici. Solo lo spam e' una seccatura, ma abbiamo gli strumenti per combatterlo. E gia' che ci siamo daremo una mano ai nostri cugini windowsiani. In fondo non e' colpa loro se win e' piu' fragile di Linux.
Cosa vogliamo realizzare ? Semplicemente un sistema che legga per noi tutte le caselle di posta che indicheremo, passi all'anti virus ed all'antispam il tutto e depositi il materiale su una directory del nostro pc. Noi con calma visioneremo tutto cio' che e' sopravvissuto a questo tour-de-force.
Ovviamente possiamo mettere il tutto in cron e dare una cadenza di 5 minuti, o qualcosa di analogo.
Come lo realizziamo ? Cominciamo col formattare un pc ed installare l'insuperabile slackware 10.1, successivamente ...

ci procuriamo il software:

razor-agents-sdk-2.04.tar.gz
razor-agents-2.72.tar.gz

li troviamo presso

http://razor.sourceforge.net

Il pacchetto

HTML-Parser-3.45.tar.gz

lo scarichiamo da:

http://search.cpan.org/dist/HTML-Parser/lib/HTML/Entities.pm

Il pacchetto

Mail-SpamAssassin-3.0.4.tar.bz2

lo scarichiamo da:

http://mirror.tomato.it/apache/spamassassin/source/

Il pacchetto

clamav-0.86.1.tar.gz

lo scarichiamo da:

http://www.clamav.net/stable.php#pagestart

Come avrete gia' capito faremo tutto il lavoro partendo dai sorgenti e compilando il tutto a manina. Saro' fissato ma credo sia il modo migliore di lavorare con Linux ed i *NIX in genere. Non ho provato -per pigrizia- a creare i pacchetti tgz con checkinstall. Se qualcuno volesse fare tale prova e postarmi i risultati mi fara' cosa gradita.

Al lavoro:

Il tutto e' molto semplice e lineare. Cominciamo con razor-agents-sdk-2.04.tar.gz . Ipotizziamo di lavorare in /tmp/ ; quindi (ovviamente come root):

```
tar zxvf razor-agents-sdk-2.04.tar.gz -C /tmp/
cd /tmp/azor-agents-sdk-2.04
perl Makefile.pl
make all
make install
```

Ora tocca a razor-agents-2.72.tar.gz. Ripetiamo il tutto:

```
tar zxvf razor-agents-2.72.tar.gz -C /tmp/
cd /tmp/razor-agents-2.72
perl Makefile.pl
make all
make install
```

Il prossimo sara' HTML-Parser-3.45.tar.gz :

```
tar zxvf HTML-Parser-3.45.tar.gz -C /tmp/
```

```
cd /tmp/HTML-Parser-3.45
perl Makefile.pl
make all
make install
```

Passiamo ora a spamassassin:

```
tar jxvf Mail-SpamAssassin-3.0.4.tar.bz2 -C /tmp/
cd /tmp/Mail-SpamAssassin-3.0.4
perl Makefile.pl
make all
make install
```

Per ultimo installiamo l'ottimo anti virus clamav :

```
tar zxvf clamav-0.86.1.tar.gz -C /tmp/
cd /tmp/clamav-0.86.1
groupadd clamav
useradd -s/bin/false -g clamav clamav
./configure
make
make install
```

adesso dobbiamo editare il file di configurazione locato in /usr/local/etc/fresclam.conf. Cercate la riga

```
EXAMPLE
```

e commentatela come segue:

```
#EXAMPLE
```

Salviamo ed aggiorniamo l'anti virus col comando

```
freshclam
```

C**onfigurazione del sistema:**

Aggiungiamo un utente qualora gia' non lo avessimo fatto. Il nostro utente fittizio e' “pinguino” .

```
adduser pinguino
.............
.............
.............
```

Creiamo la cartella /home/pinguino/.getmail (notate il punto .getmail)

mkdir /home/pinguino/.getmail

All'interno di /home/pinguino/.getmail/ creiamo il file di configurazione di getmail dal nome getmailrc. A titolo di esempio utilizziamo quello qui sotto riportato in corsivo :

[options]
verbose = 2
read_all = true
delete = true
message_log = /home/pinguino/.getmail/getmail.log

[retriever]
type = SimplePOP3Retriever
server = xxxxxxxxxx
port = 110
username = yyyyyyyyyyy
password = zzzzzzzzzzzz

[filter-1]
type = Filter_external
path = /usr/bin/spamc

[filter-2]
type = Filter_classifier
path = /usr/local/bin/clamscan
arguments = ("--stdout", "--no-summary", "--mbox", "--infected", "-")
exitcodes_drop = (1,)

[destination]
type = Mboxrd
path = /var/spool/mail/pinguino
user = pinguino

Se abbiamo creato la cartella /home/pinguino/.getmail come root, allora dobbiamo dare a tale cartella i giusti permessi:

chown -R pinguino:users /home/pinguino/.getmail

Creiamo il file di log dichiarato nella prima sezione del file /home/pinguino/.getmail/getmailrc :

touch /home/pinguino/.getmail/getmail.log

Ovviamente controllate i permessi e la possibilità' di scrittura sul file da parte dell'user pinguino.
Creiamo il file che ricevera' fisicamente la posta, nel formato mailbox:

touch /var/spool/mail/pinguino
chown pinguino:users /var/spool/mail/pinguino

Editiamo il file /etc/inetd.conf e decommentiamo la riga inerente al servizio

popa3d. In pratica la seguente riga:

```
#pop3    stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/popa3d
```

diventera' cosi' :

```
pop3    stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/popa3d
```

Stoppiamo il supervisore inetd:

```
killall inetd
```

e lo riavviamo:

```
inetd
```

Ancora qualche dettaglio sul file getmailrc: nella sezione

```
[retriever]
```

dovete inserire i vostri login + username corretti per l'accesso alla casella mail che vogliamo leggere. Non mi dilungo oltre sulla configurazione di getmail, poiche' nella directory /usr/share/doc/getmail.x.x.x c'e' materiale a sufficienza per qualche settimana. Inoltre vi sono diversi esempi di settaggio. Abbiamo quasi finito: ricontrolliamo per puro scrupolo di avere clamav aggiornato; poi facciamo partire spamassassin in modalita' demone, tramite il flag -d

```
spamd -d
```

Ovviamente da root. Il comando spamd -d deve essere esguito ogni qualvolta desideriamo il controllo della posta elettronica. Una buona soluzione potrebbe essere quella di mettere nel file /etc/rc.c/rc.local i comandi adeguati alla partenza del servizio. Invece i pinguini piu' smaliziati creeranno un vero e proprio script di avvio dal nome ipotetico rc.antispam e lo posizioneranno in /etc/rc.d . Sara' /etc/rc.d/rc.M a controllare cosa fare partire tramita il flag di eseguibilita'. E' la soluzione ottimale poiche' rispetta l'ordine e la pulizia della slackware.

E adesso ...?

Adesso abbiamo un potente sistema anti-spam ed antivirus, dello stesso calibro di quelli utilizzati dai provider. Come lo utilizziamo? Col semplice comando

```
getmail
```

Sara' l'utente pinguino a dovere eseguire tale comando. Il nostro getmail obbediente obbediente leggera' il file /home/pinguino/.getmail/getmailrc ,

si colleghera' al pop indicato, scarichera' tutte le mail , le passera' a spamAssassin ed a clamav, infine sistemera' il tutto nel formato mailbox e precisamente in /var/spool/mail/pinguino. Non ci resta che prelevare il tutto con il nostro programma di posta elettronica preferito. Come sarebbe a dire “ come facciamo?” Semplicemente nel nostro programma di posta elettronica aggiungiamo un account il cui login e' “ pinguino “ , la password sara' quella dell'utente pinguino, il server pop sara' l'indirizzo ip della linux-box su cui abbiamo appena finito di lavorare, il server smtp ... usate quello valido del vostro provider .
Per completezza segnalo anche un'altra possibile configurazione di getmailrc: nella sezione

```
[filter-1]
type = Filter_external
path = /usr/bin/spamc
```

e' possibile la variante:

```
[filter-1]
type = Filter_external
path = /usr/bin/spamassassin
```

In questo caso getmail puo' essere invocato senza mandare in esecuzione il demone di spamassassin. In pratica non serve lanciare il comando

```
spamd -d
```

Nelle mie prove tutte e due le configurazioni hanno funzionato.

Utilizzo intenso

Tutto questo e' buono e giusto, ma troppo macchinoso per l'utenza casalinga. Chi legge 3/5 caselle di posta ha poco vantaggio rispetto all'uso dei filtri et similia. Le cose cambiano in azienda: Quando occorre tenere sotto controllo 25 caselle di posta, ecco che il lavoro speso per mettere in piedi quanto sopra diventa ben speso. La nostra slackware fedele e docile fara' tutto il lavoro al posto nostro. Per ogni casella basta creare un user, un file di configurazione per getmail, che deve essere posizionato in /home/utente/.getmail/ , mettere il tutto in cron ... ed il gioco e' fatto.

Hardware di test:

I tests sono stati eseguiti su un pentium 2 350 mhz, 384 mb ram, disco fisso IDE da 20 gb , lettore cdrom, sk video ati rage 4 mb (vecchiotta) , sk rete 10/100 realtek ed ovviamente slackware 10.1

ringraziamenti:

Matteo Spigolon , bimbo@slackware-italia.com , che mi ha prestato

l'idea. Non solo, ma con pazienza e tenacia ha letto le mie mail e prontamente evaso i miei quesiti.

Marco Porro , bugs84@libero.it , esperto di sicurezza informatica , il quale in pochi istanti ha trovato il link ai software necessari, inoltre ha corretto un errore di procedimento al quale io non avevo fatto caso.