Parlare con il postino

Breve introduzione al protocollo SMTP e Postfix

Giovanni Mascellani
<gio@debian.org>

Gruppo Utenti Linux di Pisa

Mercoledì 9 febbraio 2011

Com'è fatta un'email?

- Ci sono due parti: le intestazioni ed il corpo.
- Le intestazioni contengono tante informazioni interessanti su chi ha scritto l'email, a chi l'ha scritta, con che titolo, da dove è passata l'email durante il recapito e tanto altro.
- A volte il corpo principale ha una struttura particolare (MIME), che permette di descrivere email più complesse (firma digitale, allegati, testo HTML, ...).

- *Conviene vederli direttamente...*

Il protocollo SMTP

La posta si manda sulla porta 25.

```
$ telnet mail.gulp.linux.it 25
Trying 131.114.11.54...
Connected to mail.gulp.linux.it.
Escape character is '^]'.
220 mail.gulp.linux.it ESMTP Postfix (Debian/GNU)
```

Ora sta a noi a parlare! :-)

Un minimo di cortesia!

Il comando `HELO` serve per presentarsi.

```
220 mail.gulp.linux.it ESMTP Postfix (Debian/GNU)
HELO giovanni
250 mail.gulp.linux.it
```

Il server risponde cortesemente ed aspetta ulteriori istruzioni.

Mittente

La prima cosa da dire è chi sta mandando l'email. Si usa il comando `MAIL FROM`.

```
250 mail.gulp.linux.it
MAIL FROM:<mascellani@poisson.phc.unipi.it>
250 2.1.0 Ok
```

Ammesso che l'indirizzo fornito sia valido, perché si dovrebbe lamentare? In fin dei conti è pur sempre il suo mestiere.
Se ci saranno problemi nella consegna dell'email, il server invierà una DSN all'indirizzo specificato come mittente. L'indirizzo specificato nel testo dell'email non conta niente.

Destinatari

I destinatari si specificano con il comando `RCPT TO`. Ovviamente possono essere più di uno, ma non bisogna esagerare.

```
250 2.1.0 Ok
RCPT TO:<giovanni@gulp.linux.it>
250 2.1.5 Ok
RCPT TO:<presidente@gulp.linux.it>
250 2.1.5 Ok
```

Fin tanto che il server risponde con il codice 250, vuol dire che è contento.
Come prima, gli indirizzi specificati nel testo dell'email non contano niente. Il server utilizza unicamente quelli specificati con il comando `RCPT TO` (*indirizzo di busta*).

Testo dell'email

Alla fine bisogna passare al dunque: il corpo dell'email. Si utilizza il comando `DATA`. Il testo dell'email viene concluso con un punto su una riga da solo. Poi il comando `QUIT` permette di disconnettersi.

```
DATA
354 End data with <CR><LF>.<CR><LF>
Prova di email.
.
250 2.0.0 Ok: queued as 1EF81F0068
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
```

Appena il server risponde 250 dopo il punto su una riga da solo, vuol dire che si è preso l'incarico di consegnare l'email.

Tutto bene?

Siamo sicuri che tutto funzioni bene?

Fingersi qualcun'altro

E se avessi fatto questa cosa?

```
$ telnet mail.gulp.linux.it 25
[...]
MAIL FROM:<presidente@gulp.linux.it>
250 2.1.0 Ok
[...]
DATA
354 End data with <CR><LF>.<CR><LF>
From: Presidente del GULP <presidente@gulp.linux.it>
Subject: Devi pagare la quota di iscrizione
[...]
```

Attenzione al phishing

Il protocollo SMTP non permette di identificare con sicurezza il destinatario.

- Chiunque può mandare email a nome di chiunque altro. Questa tecnica viene spesso utilizzata per scopi fraudolenti (*phishing*).
- Per essere sicuri dell'origine di un messaggio bisogna utilizzare altre tecniche, per esempio una firma crittografica.

Email non desiderate

E che ne dite di questo?

```
$ telnet mail.gulp.linux.it 25
[...]
MAIL FROM:<v1agra@p1llz.com>
250 2.1.0 Ok
RCPT TO:<presidente@gulp.linux.it>
250 2.1.5 Ok
RCPT TO:<vicepresidente@gulp.linux.it>
250 2.1.5 Ok
RCPT TO:<consiglio@gulp.linux.it>
250 2.1.5 Ok
RCPT TO:<gulp@gulp.linux.it>
250 2.1.5 Ok
[...]
```

Attenzione allo spam

Il protocollo SMTP non permette di verificare che il messaggio sia gradito al destinatario.

- È facilissimo mandare tantissime email in blocco per scopi commerciali o fraudolenti.
- Esistono dei trucchi per difendersi: analisi statistica sul contenuto dei messaggio, blacklisting degli IP di origine, greylisting, ...
- Nessuna soluzione definitiva.

- Questi due problemi sono presenti anche nella posta tradizionale, ma sono molto meno preponderanti perché molto più costosi.

Altre cose da tenere a mente

- Normalmente i server non fanno relay pubblico: accettano un'email soltanto se è diretta ad un utente del server oppure viene dalla rete del server (a meno di configurazioni particolari).
- Filtri sul mittente: le email non vengono accettate se il mittente non ha un indirizzo valido.
- Greylisting: ritardare un po' la ricezione di un'email in modo da vedere se il mittente la vuole inviare per davvero (ci sono delle controindicazioni: il server mittente risulta più carico).
- Blacklisting: le email da indirizzi sospetti non vengono accettate (controindicazioni: si può finire per errore sulle blacklist, tipicamente quando ci sono a giro computer con virus che mandano email di spam).

Postfix!

- Postfix è un'implementazione libera di server SMTP. Il suo autore, Wietse Venema, grazie ed esso ha vinto il Free Software Foundation Award for the Advancement of Free Software per il 2008.
- Fa un sacco di cose, è molto configurabile e si può interfacciare con filtri ed altri programmi esterni. No, il caffè non lo fa, per ora.
- È molto ben documentato! :-)
- Vediamo come farci alcune delle cose che abbiamo visto.