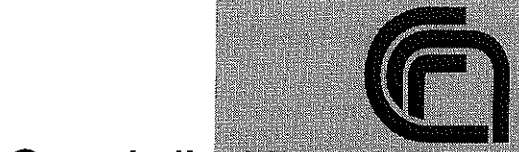

Consiglio Nazionale delle Ricerche

*T*CP Wrapper: un programma per controllare e filtrare l'accesso ai servizi di rete

Massimo Martinelli

B4-34
dic-1998

TCP Wrapper: un programma per controllare e filtrare l'accesso ai servizi di rete

M. Martinelli

Dicembre 1998

Introduzione

TCP Wrapper è un pacchetto software utile per controllare e filtrare le richieste di accesso ai servizi di rete offerti da macchine con sistema operativo UNIX, come telnet e ftp.
Consente di registrare il nome dell' *host* cliente e il servizio di rete richiesto al *server*. Inoltre, impostando corrette regole di sicurezza, consente l'accesso ai servizi solo da determinati *host*.

Il programma è prelevabile al seguente indirizzo:
ftp://ftp.win.tue.nl/pub/security/tcp_wrappers_7.6.tar.gz

Di seguito saranno fornite indicazioni utili alla configurazione del pacchetto software relativamente alla versione 7.6, con un cenno al software incluso nella versione UNIX relativa all HP-UX 10.20.

Il funzionamento

Normalmente un singolo processo, inetd, si occupa di attendere le richieste di connessione ai servizi di rete. Ogni volta che arriva una richiesta inetd attiva il processo *server* relativo, che, successivamente, attiva un'applicazione: se, ad esempio, arriva una richiesta tramite il comando telnet, inetd attiva il processo telnetd che successivamente attiva l'applicazione "remote login".
Con TCP Wrapper inetd non attiva un processo *server* bensì una procedura *wrapper* che registra nel file di *log* il nome dell' *host* cliente e del servizio richiesto; successivamente attiva il processo *server* solo se il richiedente rispetta le condizioni impostate tramite regole di sicurezza, altrimenti termina la connessione.

Configurazione

E' possibile configurare il pacchetto software spostando le procedure *server* in un'altra directory e copiare al loro posto i programmi *wrapper*.
Si consiglia però di configurare modificando il file */etc/inetd.conf*: volendo controllare il servizio telnet, supponendo di aver installato il TCP Wrapper in */usr/local/sbin*, modificare la seguente linea

telnet stream tcp nowait root /usr/sbin/in.telnetd in.telnetd

come segue

telnet stream tcp nowait root /usr/local/sbin/tcpd in.telnetd

Effettuare la stessa modifica per tutti i servizi che si intendono controllare.
Far ripartire il processo inetd con il comando "kill -HUP *pid_syslogd*".

Logging

Per *default* le informazioni relative ai *log* vengono registrate nel file */var/log/syslog*.
Il TCP Wrapper registra le informazioni nello stesso file in cui le registra il *sendmail*.
E' possibile cambiare questa impostazione modificando il file */etc/syslog.conf* e facendo ripartire il processo syslogd tramite il comando "kill -HUP *pid_syslogd*".
Nelle versioni di Solaris 2.x il syslogd dipende dal preprocessore m4 installato come parte del pacchetto di sviluppo.
Le versioni più recenti di syslog supportano livelli di priorità (*debug, info, notice, alert, emerg, ...*) e classi di messaggi (*mail, kern, daemon, auth, news, ...*).

Ad esempio, la seguente linea nel file */etc/syslog.conf*

mail.debug ifdef('LOGHOST', /var/adm/syslog, @loghost)

fa si che i messaggi di classe *mail* di priorità *debug* o più urgente vengano registrati nel file */var/log/syslog* del *loghost*. Il *loghost* è definito nel file */etc/hosts* e corrisponde alla macchina su cui stiamo lavorando. In presenza di un *server* NIS/NIS+ (Network Information Service / Plus) si possono registrare i file di *log* su una sola macchina definendo il *logmaster* nei file */etc/hosts* dei vari computer come in figura 1.

Figura 1: esempio di file /etc/hosts

```
# Hosts table
127.0.0.1        localhost
131.114.200.20   bibli    bibli.iei.pi.cnr.it  loghost
131.114.200.250  nisserv  logmaster
```

Filtraggio degli accessi

TCP Wrapper, di *default*, è configurato per consultare due file: */etc/hosts.allow* e */etc/hosts.deny*, il primo contenente regole per consentire l'accesso ai servizi il secondo per negarlo.

I due file possono essere costituiti da zero, una o più righe con il seguente formato:

daemon_list : client_list [: shell_command]

dove

daemon_list è una lista di uno o più nomi di processi, separati da uno spazio o una virgola;

client_list è una lista di uno o più nomi o indirizzi di *host*, separati da uno spazio o una virgola;

shell_command è un comando di shell (è opzionale, viene eseguito se la condizione impostata dai due parametri precedenti è valida).

Se, ad esempio, il file */etc/hosts.allow* è composto dalle seguenti righe

in.ftpd in.telnetd : 131.114.200.

in.fingerd : 131.114.200.2

e il file */etc/hosts.deny* dalla seguente riga

ALL : ALL

l'accesso ai servizi ftp e telnet è consentito solo dagli *host* con indirizzo 131.114.200.x, che corrispondono a tutte le macchine del dominio iei.pi.cnr.it, l'accesso al servizio finger è possibile solo dall'*host* con indirizzo 131.114.200.2. Ogni altro accesso è negato.

In figura 2 sono elencati alcuni esempi di *client_list*.

Figura 2: alcuni esempi di *client_list*:

```
131.114.200.7 galileo.iei.pi.cnr.it # due macchine
.iei.pi.cnr.it      # le macchine del dominio iei.pi.cnr.it
131.114.            # le macchine con indirizzo compreso tra
                    # 131.114.0.0 e 131.114.255.255
131.114.200.0/255.255.254.0
     # 255.255.254.0 rappresenta la netmask quindi tutte le
     # macchine con indirizzo compreso tra 131.114.200.0 e
     # 131.114.201.255
ALL EXCEPT 131.114.216.
     # tutte le macchine eccetto quelle di indirizzo compreso
     # tra 131.114.216.0 e 131.114.216.255
```

In assenza di regole o dei file */etc/hosts.allow* e */etc/hosts.deny* l'accesso è sempre consentito. TCP Wrapper consulta prima il file */etc/hosts.allow* poi */etc/hosts.deny*, non appena verifica una regola valida la consultazione termina.

E' possibile regolare l'accesso ai servizi con il solo file */etc/hosts.allow*, utilizzando le parole chiave *ALLOW* e *DENY*.
Se impostiamo le seguenti regole

ALL : 131.114.200. : ALLOW
ALL : ALL : DENY

l'accesso ai servizi è possibile solo dalle macchine con indirizzo 131.114.200.x
Nell'esempio successivo viene negato l'accesso dalle macchine appartenenti al dominio *bad.domain* e accettato l'accesso da tutte le altre macchine:

ALL : bad.domain : DENY
ALL : ALL : ALLOW

HP-UX 10.20

Il sistema operativo HP-UX 10.20 offre la possibilità di filtrare gli accessi tramite il file */var/adm/inetd.sec*, il cui formato non differisce molto dalle regole del TCP Wrapper:

daemon_list <*allow* / *deny*> *client_list*

Per negare l'accesso al servizio telnet dalle macchine 131.114.216.x
basta inserire la seguente riga

*telnet deny 131.114.216.**

Bibliografia

1) "*TCP/IP daemon wrapper package 7.6 version*". Wietse Venema.

2) "Unix security Cookbook". Starlink System Note 67. http://star-www.rl.ac.uk

3) "*Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network*". Macmillan Computer Publishing. http://www.mcp.com

4) HP-UX 10.20 online manual