iptables : come patchare i moduli iptables del Kernel con patch−o−matic

Raoul Scarazzini − rascasoft@tiscali.it, http://web.tiscali.it/rascasoft
v 1.1, Mercoledì 09 13:45:02 CEST 2005

Questo articolo si propone di spiegare come fare a patchare i moduli iptables del kernel in modo che questo supporti le funzioni emergenti (cioè non ancora incluse nel kernel ufficiale) tramite il sistema denominato "patch−o−matic".
Nel caso che illustreremo si opererà su di una RedHat 7.3, con i sorgenti ufficiali (scaricati cioè da http://www.kernel.org) del kernel 2.4.20.
Come requisito base per la comprensione di questo testo, si richiede solo di avere un'idea del come si compili un kernel. Ho scritto un articolo in merito all'argomento. Si trova a questo indirizzo : http://web.tiscali.it/rascasoft/kernel.html.

Introduzione

iptables è l'insieme di moduli e programmi necessari per implementare un firewall in un sistema Linux. Il suo funzionamento si basa su regole scritte all'interno di "tavole" che risiedono in memoria. Quando un pacchetto viaggia attraverso una interfaccia di rete, viene confrontato con tutte le regole scritte nelle "tavole", a seconda dell'esito del confronto il pacchetto viene elaborato di conseguenza.
Le regole all'interno delle catene vengono scritte tramite il comando "iptables".
A seconda delle esigenze, è possibile quindi scrivere regole specifiche per il controllo di tutti i flussi di dati che attraversano la (o le) schede di regole. Chiaramente, più aumentano le esigenze in termini di controllo, più è necessario specializzare le regole definite.
Il problema è che alcune delle funzionalità di iptables considerate ancora emergenti (e quindi non ancora adatte ad una versione stabile) non sono incluse nei sorgenti ufficiali del kernel.
Se queste, in caso di esigenze particolari, dovessero diventare indispensabili, bisognerebbe trovare il modo di includerle nel kernel sul quale operiamo. E' proprio qui che patch−o−matic ci viene in aiuto.

L'esigenza

Partiamo da questa regola di iptables :

iptables −A FORWARD −m string −−string "Kazaa" −j DROP

Questa regola, con i sorgenti di kernel.org è inapplicabile, poiché questi non consentono di creare il modulo denominato "ipt_string.o" che appunto permette, come è facile capire, di filtrare pacchetti che contengono una specifica stringa di caratterei, nel nostro caso "Kazaa".
Se la nostra esigenza è però quella di escludere questo tipo di pacchetti, allora bisogna procedere con l'installazione di patch−o−matic.

Installare patch−o−matic ed iptables

Per prima cosa è necessario scaricare il pacchetto relativo ai sorgenti di iptables e quello relativo ai sorgenti di patch−o−matic. La scelta delle versioni, nel nostro caso è dettata da un discorso di compatibilità con la versione associata alla distribuzione. RedHat 7.3 installa di default il pacchetto iptables−1.2.7a, pertanto sarà saggio da parte nostra scaricare i sorgenti relativi a questa versione di iptables :

 # cd /usr/src
 # wget http://www.netfilter.org/files/iptables−1.2.7a.tar.bz2

Di patch−o−matic, invece, basta scaricare l'ultima versione disponibile :

 # wget http://www.netfilter.org/files/patch−o−matic−ng−20040621.tar.bz2

Scaricati i sorgenti, si può procedere con la decompressione di entrambi gli archivi :

 # tar −xjvf iptables−1.2.7a.tar.bz2
 # tar −xjvf patch−o−matic−20030107.tar.bz2

Ed alla creazione di un link simbolico denominato "iptables" che punta alla directory dei sorgenti, per standardizzare il percorso delle directory :

 # ln −s iptables−1.2.7a iptables

All'interno della directory di patch−o−matic è presente il file ./runme. Questo sarà lo strumento che ci consentirà di effettuare i vari aggiornamenti.
A questo comando è possibile passare un parametro il cui valore può essere "base", "pending" o "extra" o direttamente il nome della patch (associato alla directory) che si vuol applicare.
La cosa più saggia, salvo esigenze particolari, è lanciare il seguente comando :

 # cd patch−o−matic−ng−20040621
 # ./runme −−kernel−path=/usr/src/linux −−iptables−path=/usr/src/iptables pending

In questo modo, per ciascuna delle patch in via di inclusione nei sorgenti ufficiali del Kernel, ci verrà esposta la spiegazione, cioè in cosa consiste l'aggiornamento e se vogliamo effettuarlo o no. Le risposte possibili alla domanda sono una tra queste lettere : N/y/t/f/a/r/b/w/q/?. Premendo "?" ed invio, si otterrà la spiegazione di ciascuna lettera, quelle che a noi interessano per il momento sono "N" che sta per no, "y" per sì, "q" per quit, concludi.
Le patch in stato "pending" si possono applicare senza grosse preoccupazioni, ma è sempre bene leggere in cosa consistono e capire che nel caso la funzionalità espressa dalla patch non ci servirà, sarà bene non applicarla nemmeno.
Quello che però all'inzio ci eravamo proposti di fare però a questo punto non è stato ancora raggiunto. Infatti, la patch relativa al matching dei caratteri, è considerata "extra", pertanto per applicare questa patch o lanciamo questo comando :

 # ./runme −−kernel−path=/usr/src/linux −−iptables−path=/usr/src/iptables extra

Dove però saremo costretti a scartare tutte le patch che non ci interessano, oppure specificheremo quale patch applicare in questo modo :

 # ./runme −−kernel−path=/usr/src/linux −−iptables−path=/usr/src/iptables string

Con quest'ultimo comando utilizziamo patch−o−matic in modo che aggiorni solamente i moduli relativi a "string", che sono contenuti nella cartella /usr/src/patch−o−matic−ng−20040621/string.
A questo punto, terminata la fase di patch, è necessario compilare ed installare iptables. E' necessario quindi rimuovere il pacchetto della distribuzione, in modo da non avere conflitti sui comandi. Prima di ciò, conviene salvarsi lo script di init di questo pacchetto in modo da poter automatizzare l'avvio di iptables senza crearci uno script a mano :

 # cd
 # cp /etc/init.d/iptables ./
 # rpm −e iptables

Fatto questo, si può procedere con l'installazione di iptables nella maniera "standard" :

 # cd /usr/src/iptables
 # make BINDIR=/sbin LIBDIR=/lib KERNEL_DIR=/usr/src/linux
 # make install BINDIR=/sbin LIBDIR=/lib KERNEL_DIR=/usr/src/linux

Infine, si ripristinerà lo script di init associandolo ai runlevel 345 :

 # mv /root/iptables /etc/init.d
 # chkconfig "level 345 iptables on

Come ultima cosa, non rimane che configurare il kernel affinchè consideri i nuovi moduli e ricompilarlo :

 # cd /usr/src/linux
 # make menuconfig
−−− selezione moduli iptables x stringa : Networking options −> IP: Netfilter Configuration −> String Match Support> −−−
 # make modules
 # make modules_install
 # cp System.map /boot/System.map−2.4.20rasca

Per ulteriori dettagli su come ricompilare il kernel una volta patchato, ci si può riferire all'howto che ho scritto : http://web.tiscali.it/rascasoft/kernel.html.

Caricare il nuovo modulo

A questo punto, il comando :

 # iptables −A FORWARD −m string −−string "Kazaa" −j DROP

dovrebbe funzionare senza problemi. Si noterà come, in caso di successo nell'applicazione della regola, che nell'elenco dei moduli caricati comparirà anche il neo−creato :

Module Size Used by Tainted: P
[...]
ipt_string 2528 6 (autoclean)
[...]

Sottolineo come qualsiasi operazione di patching del kernel debba essere effettuata solamente per esigenze particolari e con la consapevolezza di quello che si sta facendo.
E' tutto, buon divertimento !

Conclusioni

In caso di problemi è sempre utile consultare i gruppi di google http://groups.google.com e di tenere come riferimento i siti : www.netfilter.org per i sorgenti e nel dettaglio http://www.netfilter.org/documentation/index.html per un'ottima dose di documentazione;

Se si riscontrano errori nel documento, si necessita di aiuto o semplicemente si vuole esprimere un commento questo è il mio indirizzo rascasoft@tiscali.it.
