escola d'enginyeria

Informe Pràctica iptables

Ramon Guimerà Ortuño - 1400214
David Cuadrado Gómez - 1391968
Grup: tai-c3

Respostes:

1. Per què creus que el *forwarding* de paquets no està activat per defecte en la majoria de distribucions *GNU/Linux*?

No està activat per defecte per ja que el *forwarding* s'utilitza en la majoria de casos per a encaminar paquets provinents d'una interfície (ex: *eth1*) cap a una altra (ex: *eth0*) tot des del mateix host. En altres paraules, la funció bàsica d'un router.
La majoria de distribucions de *GNU/Linux* estan dedicades a hosts (nodes de final de camí) i no pas routers, pel que no necessiten (per defecte) per *forwarding* de paquets.

2. Quines diferències hi ha entre els diferents tipus d'emmascarament de les *IP*'s d'origen que permet *iptables*?

iptables permet emmascarar de forma dinàmica i de forma estàtica. La diferència és que de forma dinàmica, la *IP* a emmascarar serà escollida de forma que es podrà renovar i ser agafada per un altre host si es deixa de fer servir i de forma estàtica, tots els host que provinguin de tal xarxa tindran tots la mateixa direcció *IP* d'origen.

Exemple dinàmica:
iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -o eth1 -j MASQUERADE

Exemple estàtica:
iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -o eth1 -j SNAT --to 80.58.1.14

3. Descriu un escenari per a cadascun dels possibles emmascaraments que has comentat en la pregunta anterior.

Un emmascarament estàtic es podria utilitzar en un router domèstic per a deixar a tots els hosts interns accedir a serveis externes a la xarxa domèstica i que no hi haguèssin col·lisions, ja que tindran la mateixa direcció *IP* de sortida, però amb diferents ports assignats.
Un emmascarament de tipus dinàmic, es pot utilitzar en un router d'un *ISP* i per a donar una direcció dinàmica a cada subrouter domèstic. En el cas de dinàmic, hauriem de revisar en tot moment, quina direcció genera trànsit i a quin host intern pertany, de forma estàtica, ja sabem quin host està generant tal trànsit.

4. Quines diferències bàsiques existeixen entre utilitzar un target *LOG* i un *ACCEPT*/*REJECT*?

El target *LOG* ens permet tenir un control històric dels paquets rebuts, mentre's que *ACCEPT*/*REJECT* no ens deixaria un historial de connexions realitzades.

5. Per què no podem utilitzar el target *MARK* per marcar els paquets del client?

El *MARK*, només està disponible a nivell de kernel i no per a ser propagat. En canvi, el camp de *TOS* si que pot ser modificat per a paquets o streams d'informació i ser propagat a través del a xarxa [1].

6. Mitjançant *iptables*, com ho faries per poder controlar l'accés a Internet a tots els treballadors d'una multinacional?

Es pot fer tal i com ho hem realitzat a la pràctica, asignar un valor a cada treballador de la multinacional i des dels diferents *gateways* administrar les conexions de sortida per valor del treballador.

Una altra forma es asignar valors diferents depenent de la posició en l'empresa (ex: treballadors amb 2, manager 3, etc.) i administrar els diferents accesos cap a Internet depenent del tipus de treballador.

[1] http://www.linuxtopia.org/Linux_Firewall_iptables/x4737.html