Curso avanzado de GNU/Linux

Netfilter

Rafael Varela Pet

Unidad de Sistemas
Área de Tecnologías de la Información y Comunicaciones
Universidad de Santiago de Compostela

Introducción: netfilter, iptables

- netfilter.org
  - *framework* para las series 2.4 y 2.6 que permite manipular tráfico de red
  - sucesor de iptables (kernel 2.2.x) e ipfwadm (kernel 2.0.x)
- componentes
  - netfilter: puntos de enganche (*hooks*) en el subsistema de red del kernel
  - iptables: herramienta para definir conjuntos de reglas de acceso
  - otros: subsistema NAT, connection tracking.

netfilter: funciones

- Filtrado de paquetes con estado (*stateful*) o sin estado (*stateless*).
- *Network Address and Port Translation* (NAT/NAPT)
- Arquitectura extensible
- Sólo funciona con protocolo IP (IPv4 e IPv6)

Netfilter: terminología

- Destinos (*targets*): Acción que se le puede aplicar a un paquete: ACCEPT, DROP, REJECT, LOG, ...
- Reglas (*rules*): define un criterio de selección de paquetes y qué destino se le va a dar a los que o cumplan.
- Cadenas (*chains*): conjunto de reglas que se aplican a un paquete.
  - Cada cadena tiene un ámbito de aplicación específico.
  - Existen cadenas predefinidas y cadenas de usuario

Netfilter: terminología

- Tablas: agrupan cadenas según un determinado propósito. Existen 4 tablas:
  - filter
  - nat
  - mangle
  - raw
- Cada tabla tiene un conjunto de cadenas predefinidas. La tabla filter tiene las cadenas INPUT, FORWARD, OUTPUT

Enfoque

- Vamos a centrarnos en el filtrado
- Usamos:
  - tabla filter
  - cadenas
    - INPUT (se aplica a paquetes que entran a nuestro sistema)
    - OUTPUT (paquetes que salen de nuestro sistema)
    - FORWARD (paquetes en tránsito)
  - Importante: Un paquete atraviesa sólo una cadena

Requisitos previos

- Disponer de soporte en el kernel

```
> grep IP_NF /boot/config-$(uname -r)
```

- Cargar el módulo

```
> modprobe ip_tables
```

- Herramientas en el espacio de usuario

```
> aptitude install iptables
```

Definición de reglas

- Añadir regla:
  - Especificamos tabla, cadena, definición de la regla y destino del paquete:

```
iptables [-t tabla]
-A CADENA
definicion_regla
-j TARGET [opciones target]
```

Match extensions

- Extensiones que amplían las capacidades de búsqueda de paquetes
- Se cargan implíticamente al usar la opción “-p” para especificar un determinado protocolo
- Se cargan explícitamente con la opción “-m”
- Algunos módulos estándar:
  - connlimit conntrack icmp
  - quota mac multiport ...

Definición de reglas

- Ejemplo: Bloquear todo el tráfico entrante por la interfaz eth0 guardando un registro previamente:
  - `iptables -t filter -A INPUT -i eth0 -j LOG --log-prefix "prohibido --"`
  - `iptables -t filter -A INPUT -i eth0 -j REJECT`
- Comprobar reglas aplicadas:
  - `iptables -t filter -L`
- Ver /var/log/syslog o ejecutar 'dmesg' para observar los mensajes de netfilter

Definición de reglas

- Borrar regla:
  `iptables [-t tabla]`
  `-D CADENA  definicion_regla`
- También se puede especificar el número de regla a borrar:
  `iptables -t filter -D prueba 2`
- Borrar todas las reglas:
  `iptables -t filter -F` (*flush*-Vacía cadenas)
  `iptables -t filter -X` (Borra cadenas de usuario)

Logging

- Empleamos el *target* -j LOG para registrar eventos a través de syslog
- Una regla con ese destino no es terminal
- Si queremos hacer log y rechazar al mismo tiempo:
  - Creamos una cadena propia con las dos reglas:

```
iptables -N logdrop
iptables -A logdrop LOG
iptables -A logdrop DROP
```

  - Cuando queramos registrar y rechazar, empleamos el *target* -j logdrop

Logging

- Ejemplo:

```
IN=eth0 OUT=
MAC=ff:ff:ff:ff:ff:ff:00:0e:83:ca:5d:cf:08:00
SRC=10.3.0.1 DST=255.255.255.255
LEN=328 TOS=0x00 PREC=0x00 TTL=255 ID=65301
PROTO=UDP SPT=67 DPT=68 LEN=308
```

- Notas:
  - `08:00` – Ethertype (protocolo IP)
  - `ff:ff:ff:ff:ff:ff` - MAC destino (broadcast)
  - `00:0e:83:ca:5d:cf` - MAC origen

Política de las cadenas

- La política determina qué es lo que hay que hacer con un paquete si no se aplica ninguna regla
- Sólo las cadenas predefinidas pueden tener política
- Ejemplo:
  - `iptables -t filter -P INPUT DROP`

Ejemplo para estación de trabajo

- Ver rc.iptables
- Para que se cargue al inicio del sistema:
  - Copiar a /etc/rc.iptables
  - Editar /etc/rc.local

Herramientas de alto nivel

- Construcción de reglas:
  - **firehol**: herramienta de consola, ficheros de texto plano
  - **firewall builder**: herramienta gráfica, ficheros XML
- Depurar reglas:
  - **sendip**: permite generar paquetes IP arbitrarios
  - Ejemplo:
    - `aptitude install sendip`
    - `sendip -v -p ipv4 -p udp -ud 22222 -d 0x12345678`

Firehol

- aptitude install firehol
- Editar /etc/firehol/firehol.conf
- Ejecutar 'firehol reload'

Referencias

- http://www.netfilter.org/
- http://iptables-tutorial.frozentux.net/iptables-tutorial.html
- http://www.earth.li/projectpurple/progs/sendip.html
- http://firehol.sourceforge.net/
- http://en.wikipedia.org/wiki/EtherType