

Firewalls e IPTables for n00bs

Boris Quiroz Q.

borisq22@gmail.com

<http://g00fy.homelinux.org>

cc by-nc-sa/2.0/cl



Generalidades

- La seguridad **no es** un problema técnico.
- Defectos de diseño y programación:
 - Buffer Overflow.
 - Mala selección de contraseñas.
- Una red será tan segura como su **eslabón más débil**.
- ¿Qué asegurar? ¿Porqué asegurarlo?

¿Qué es un Firewall?

- Dispositivo que **controla las conexiones** que entran y salen de una red.
- **RFC 2979** define su comportamiento y funcionamiento.
- Proporciona:
 - **Protección.**
 - **Confidencialidad.**

Funcionamiento de un Firewall

- **Analiza las conexiones** que entran y salen.
- Examina el origen y el destino del paquete.
- Métodos de control:
 - Filtro de paquetes.
 - Inspección de estado.

Políticas de Seguridad

- Permitir todo:
 - Filtra lo explícitamente especificado.
 - Fácil de administrar.
 - Bajo control de puertos abiertos.
- Denegar todo:
 - Deja pasar solo lo indicado.
 - Administración un poco más compleja.
 - Mayor control de qué está abierto y porqué.

Netfilter e IPTables

- Módulo del Kernel 2.4+
- **Analiza los headers** antes de hacer algo.
- IPTables:
 - Herramienta de filtrado y revisión TCP/IP.
 - Sucesor de ipchains.
 - Es parte del módulo netfilter

Terminología

- Tablas:
 - Conjunto de Cadenas.
- Cadenas:
 - Conjunto de Reglas.
- Reglas:
 - A quién aplico lo que quiero hacer.
- Targets:
 - Qué quiero hacer.

Sintaxis Básica

iptables

<tabla>

<comando cadena>

<regla>

<target>

Tablas

- filter:
 - **Filtrado** de paquetes.
- nat:
 - **Manipulación** de direcciones y puertos.
- mangle:
 - **Alteración** especializada.
- raw:
 - **Evitar seguimiento** de conexiones.

Comandos

- **Agregar**
- **Insertar**
- **Reemplazar**
- **Delete**
- **Flush**
- **Listar**
- **Política**
- **Nueva**

Cadenas: filter y nat

- filter:
 - Input: **hacia** el equipo.
 - Output: **desde** el equipo.
 - Forward: **a través** del equipo.
- nat:
 - Prerouting: DNAT.
 - Output: paquetes locales.
 - Postrouting: SNAT/MASQUERADE.

Ejemplos

```
# iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

```
# iptables -A INPUT -p ICMP -j REJECT
```

```
# iptables -t nat -L
```

Reglas

- Definen **sobre qué** vamos a actuar.
- Ejemplos:
 - -p tcp –dport 80
 - -s 192.168.1.0/24
 - -d 0.0.0.0/0
 - -i eth0
 - -m state –state NEW

Targets

- ACCEPT
 - REJECT
 - DROP
-

- SNAT / MASQUERADE
 - DNAT
-

- LOG

Ejemplos

- Nat en nuestra red:
 - # iptables -t nat -A POSTROUTING -s 192.168.1.0/24 – 0.0.0.0/0 -j MASQUERADE
- Forwarding:
 - # iptables -A FORWARD -i eth1 -o eth1 -j ACCEPT
- Bloqueo del ping:
 - # iptables -A INPUT -p ICMP -j REJECT

Más ejemplos...

- Permitir acceso ssh solo a una ip:
 - # iptables -A INPUT -p TCP -s 192.168.1.4 –dport 22 -j ACCEPT
- Bloquear el resto:
 - # iptables -A INPUT -p TCP -s 0.0.0.0/0 –dport 22 -j DROP || REJECT
- Bloquear rangos de puertos:
 - # iptables -A INPUT -p TCP -i eth0 –dport 135:139 -j DROP || REJECT

Optimización

- Objetivo: **minimizar** el número de reglas por las que un paquete debe pasar.
- **Armar bloques** mediante cadenas de usuario.
- **Agrupar condiciones comunes.**

Mauricio Campiglia
<http://campiglia.org>

Links de Interés

- Manual de iptables, Matías Bellone, AR.
 - <http://www.enespanol.com.ar/files/iptables.pdf>
- RFC 2979:
 - <http://tools.ietf.org/html/rfc2979>
- Mauricio Campiglia:
 - <http://campiglia.org>
- Boris Quiroz:
 - <http://g00fy.homelinux.org>

netfilter.org

¿Preguntas?

Linux no es poco
amigable...

Boris Quiroz Q.

<http://g00fy.homelinux.org>

borisq22@gmail.com

cc by-nc-sa/2.0/cl



...Solo elige muy bien a sus
amigos.