Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Seguridad con TCP Wrappers e ipchains (y III) (10448 lectures)

Per **Javi Polo**, ***DrSlump*** (http://drslump.org)

Creado el 26/07/2000 00:00 modificado el 26/07/2000 00:00

En este articulo revisamos a groso modo la configuración de los servicios ofrecidos por inetd y como usar tcp wrappers e ipchains para aumentar la seguridad de nuestro sistema. Parte III : ipchains

Anterior[1]

Pasemos ahora al uso de la herramienta ipchains

Lo primero de todo es tener el soporte de IP Firewalling en el kernel (Networking -> Network firewalls + IP: firewalling) y un kernel 2.2.0 o superior. En caso de usar una versión 2.0 del kernel de linux, deberemos usar ipfwadm. Luego, tras recompilar el kernel y reiniciar el equipo, pasemos a explicar la utilidad de esta herramienta.

Esta herramienta permite entre otras cosas gestionar la entrada y salida de paquetes de los protocolos TCP, UDP e ICMP. En resumen, nosotros le indicamos qué paquetes debe permitir entrar, pudiendo especificar si vienen de una IP o grupo de IPs concretos, a un puerto concreto, con un protocolo concreto, y todas las mezclas de opciones que se puedan hacer, y lo mismo con los paquetes que van hacia fuera.

ipchains consta de tres chains principales:

- `input`, que aplica las reglas a los paquetes entrantes
- `forward`, que coincide con los paquetes que ni proceden ni van destinados a esta máquina (aquellos que se han de reenviar)
- `output`, que coincide con los paquetes que van a a salir

Al llegar un paquete, se miran las reglas de la chain input y se hace lo que se tenga que hacer. Tras ello, si el paquete va dirigido a otra máquina y nosotros simplemente lo enrutamos, se miran las reglas de la chain forward y se toma la decisión que allí se diga. Luego, para todos los paquetes que salen de la máquina (incluido uno que enrutasemos, por ejemplo) se miran las reglas de la chain output y se toman acciones en consecuencia.

Los parámetros principales de ipchains son:

- `-P chain policy`. Especifica la politica a seguir por defecto. Las politicas disponibles son ACCEPT, DENY, y MASQ. Las primeras dos son autoexplicativas, la última solo se puede usar en la chain forward y se explicará más adelante
- `-L [chain]`. Lista las reglas. Si se especifica una chain solo lista las reglas de esa chain.
- `-F [chain]`. Borra (Flush) las reglas. Si se especifica una chain solo borra las reglas de esa chain.
- `-I chain, -A chain`. Ambos parámetros tienen la misma sintaxis, y se usan para añadir al principio (Insert) o al final (Append) de la cadena una regla. Esto tiene sentido puesto que las reglas se leen de arriba abajo, y en cuanto se encuentra una regla que coincide con el paquete a procesar, se le aplica y sanseacabó. En caso de no coincidir con ninguna regla, se aplica la politica por defecto de la cadena.
  Algunas de las subopciones de ipchains son:
  - `-s [!] ip[/mask] [puerto] , -d [!] ip[/mask] [puerto]`. Indica que la regla solo se aplica si la direccion origen (s) o destino (d) del paquete coincide con las suministradas. El ! delante de la IP indica que se aplica si es cualquier IP MENOS esa. Si se desea especificar un puerto, debe usarse tambien la opción -p. Además, se pueden indicar rangos de puertos; por ejemplo, 12:15

indicaría los puertos que van desde el 12 al 15.
- `-i interface`. La regla se aplica a los paquetes que lleguen/salgan por esa interfaz, por ejemplo, eth0.
- `-p proto`. Especifica el protocolo.
- `-j policy`. Indica la politica a seguir en esta regla.

Básicamente estos son los parámetros fundamentales, así, para permitir que las tramas lleguen a mi máquina, todas de mi misma máquina, añado la regla:

```
ipchains -I input -j ACCEPT -s 127.0.0.1
```

y para descartar los paquetes que vengan desde 123.34.22.XXX le indico:

```
ipchains -I input -j DENY -s 123.34.22.0/255.255.255.0
```

y luego si quiero denegar TODO acceso al puerto de netbios, menos para la IP 111.222.123.221, lo haría así:

```
ipchains -I input -j DENY -p tcp -s ! 111.222.123.221 -d 0/0 139
```

Ahora vamos a explicar un poco lo que es eso del masquerading.

El ip masquerading se usa por ejemplo, si tienes una red local en casa, y tienes un modem y quieres que cuando conectas a inet se pueda acceder a inet desde las máquinas de la red local. En dicho caso, linux lo que hace es mapear las conexiones de la red local y salen a internet a traves de la IP que tiene el interfaz que usamos para acceder a internet en la maquina con modem, en este caso, ppp0.
Hacer esto es tan sencillo como añadir la regla de esta forma, suponiendo que la red local sea 192.168.1.0/0

```
ipchains -I forward -j MASQ -s 192.168.1.0/0 -d ! 192.168.1.0/0
```

Ahora en las máquinas de la red local simplemente tendríamos que decirles que el gateway por defecto es la máquina con el modem, y todo listo y transparente .. :)
Por supuesto, tienes que haber puesto en el kernel la opción de ip masquerading.

Bueno, creo que eso es todo mi artículo, un poco pobre, pero mis conocimientos no llegan a más O:) Anterior[1]

Lista de enlaces de este artículo:

1. http://bulma.net/body.phtml?nIdNoticia=85&nIdComentario=-1

E-mail del autor: javipolo _ARROBA_ drslump.org
Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=86