

El Día a Día del Administrador de Sistemas: Knockd

KNOCK-KNOCK

Las historias de miedo están repletas de personajes de terror llamando a la puerta a altas horas de la noche. En Linux, llamamos a esto golpeteo de puertos y puede ser muy útil.

POR CHARLY KÜHNAST

Si prefiere no tener un puerto administrativo obvio para su cortafuegos iptables, pero necesita uno secreto, el golpeo de puertos es una opción interesante que puede desconcertar a ataques basados en script. Para los administradores ambiciosos pero reservados, la herra-

mienta a escoger es Knockd [1].

El paquete incluye dos componentes: Knock es el cliente que envía señales “knock”, que recibe el servicio Knockd.

Knocking

Para monitorizar el proceso, Knock, el cliente knocking, tan sólo necesita el número de puerto en cada llamada y la opción -v.

Por ejemplo:

```
knock -v 10.0.0.42 7000 8000 9000
```

La herramienta contesta inmediatamente con la salida en la línea de comandos mostrada en la Figura 1.

El fichero de configuración `/etc/knockd.conf` permite a los administradores de sistemas especificar qué acción realiza el servicio cuando recibe un golpe válido.

Vea el Listado 1 para un ejemplo.

En un entorno de producción es conveniente escoger un número de puerto poco usual.

Código Morse para Uso y Disfrute

Si se reconoce la señal, Knockd abre el puerto 22 para la IP solicitada, que se pasa en su propia IP (véase Figura 2).

Si se llama a los puertos en el orden equivocado, el servidor reiniciará el acceso SSH. Los administradores despistados (como yo) tienen otra opción, `knockd.conf`, que será como:

```
start_command = /usr/sbin/iptables
```

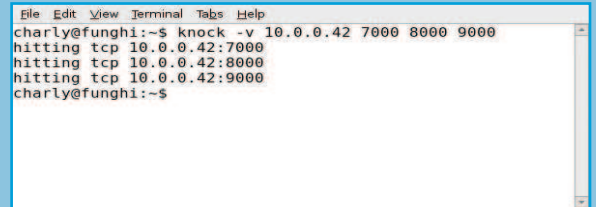


Figura 1: Si se reconoce la señal de llamada, la herramienta contesta.



Figura 2: El servicio Knockd utiliza iptables para abrir el puerto 22 de la IP solicitada, pero sólo si reconoce la señal de llamada.

```
-A INPUT
-s %IP% -p tcp -syn
-dport 22 -j ACCEPT
cmd_timeout = 10
stop_command = /usr/sbin/iptables -D INPUT
-s %IP% -p tcp -syn
-dport 22 -j ACCEPT
```

Tras golpear, el servicio lanza `start_command`, luego espera los minutos indicados en `cmd_timeout` antes de ejecutar `stop_command`.

Conclusión

A los administradores de sistemas paranoicos les gustará la opción de configurar un fichero con una secuencia de puertos. Dichas secuencias terminarán tras utilizarse.

Listado 1: /etc/knockd.conf

```
01 [options]
02 logfile = /var/log/knockd.log
03 [openSSH]
04 sequence = 7000,8000,9000
05 seq_timeout = 5
06 command = /sbin/iptables -A
  INPUT -s %IP% -p tcp -dport 22
  -j ACCEPT
07 tcpflags = syn
08 [closeSSH]
09 sequence = 9000,8000,7000
10 seq_timeout = 5
11 command = /sbin/iptables -D
  INPUT -s %IP% -p tcp -dport 22
  -j ACCEPT
12 tcpflags = syn
```

SYSADMIN

Backup64

BackupPC realiza copias de seguridad a través de la red para diversas plataformas. Aprenda más sobre este sistema de copias de seguridad de código abierto de alto rendimiento, configurable y sencillo de manejar.

RECURSOS

[1] Knockd: <http://www.zeroflux.org/cgi-bin/cvstrac.cgi/knock/wiki>