

El Día a Día del Administrador de Sistemas

BLOQUEO BRUTO

Los usuarios se conectan a servicios como SSH, FTP, SASL, POP3, IMAP, htaccess de Apache, y a muchos otros más utilizando sus nombres y sus contraseñas. Estos mecanismos de acceso son objetivos potenciales de ataques por fuerza bruta. Un buen matón se encargará de bloquear los que están basados en diccionarios.

POR CHARLY KÜHNAST

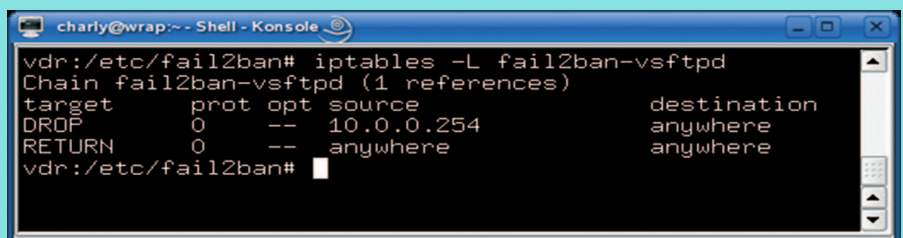
Cuando se permite a los usuarios escoger sus contraseñas por sí mismos, suelen elegir algunas bastante débiles, como el nombre de un amigo o el de alguna mascota. El predecible comportamiento humano es algo de lo que se aprovechan los hackers.

Lo único que necesita hacer un atacante es establecer un bucle en el que se intente conectar al sistema utilizando como contraseñas las palabras de un diccionario. Después de todo, hay muy pocas probabilidades de que un usuario haya escogido *4G&dP9a!* para la cuenta a la que se esté atacando.

Para contrarrestar esta vulnerabilidad inherente sería razonable restringir el número de intentos de conexión, al menos por un tiempo. Aunque *MaxAuthTries* posee un mecanismo básico para implementarlo, algunos servicios no lo tienen.

Fail2ban [1] viene a llenar este hueco. Algunas distribuciones, como Debian, Ubuntu y Gentoo lo incluyen. El código fuente y los paquetes para diversas distribuciones se encuentran disponibles en línea [2].

Fail2ban está formado por un servidor y un cliente que interpreta los ficheros de configuración central, *fail2ban.conf* y *jail.conf*, y reenvía los comandos al servidor. Analiza uno o varios ficheros de registro, comprobando cada línea en busca de expresiones regulares. Esto le permite llamar a IPtables para bloquear la dirección IP de un atacante por un período de tiempo



```

charly@wrap:~ - Shell - Konsole
vdr:/etc/fail2ban# iptables -L fail2ban-vsftpd
Chain fail2ban-vsftpd (1 references)
target      prot opt source                destination
DROP        0    --  10.0.0.254             anywhere
RETURN      0    --  anywhere               anywhere
vdr:/etc/fail2ban#

```

Figura 1: El comando de listado de IPtables muestra que Fail2ban ha hecho que el cortafuegos bloquee el equipo con dirección 10.0.0.254.

configurable tras un número definido de intentos de conexión.

Reforzando un Servidor de FTP

Como ejemplo, digamos que estoy ejecutando Vsftpd como mi servidor ftp. Tras tres intentos de conexión fallidos, se supone que el servidor tiene que bloquear la dirección IP del cliente durante cinco minutos, como se muestra en la Figura 1. El Listado 1 presenta una entrada que coincide con el fichero de configuración *jail.conf*.

Para darle cinco minutos de tranquilidad al servidor, modifiqué la entrada *bantime* desde los 600 segundos que vienen por defecto a 300 segundos. Esta cantidad de tiempo es suficiente para impedir los ataques por diccionario, pero es lo bastante corta como para no molestar a los usuarios legítimos que inadvertidamente tengan activada la tecla de bloqueo de mayúsculas.

La Figura 2 nos está mostrando que los bloqueos del programa IPtables comienzan a las 10:52 y finalizan a las 10:57, por lo que tendremos una cosa menos de lo que preocuparnos.

Listado 1: Entrada de jail.conf

```

01 [vsftpd]
02 enabled = true
03 port = ftp
04 filter = vsftpd
05 logpath = /var/log/auth.log
06 maxretry = 3
07 bantime = 300

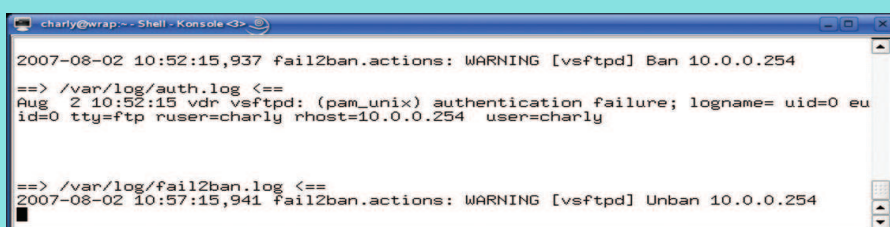
```

RECURSOS

- [1] Fail2ban: <http://www.fail2ban.org>
- [2] Código fuente y paquetes: <http://www.fail2ban.org/wiki/index.php/Downloads>

SYSADMIN

- OpenSSI..... 64**
Aprenda cómo montar un cluster OpenSSI con nivelado de carga.
- OpenSolaris68**
Seguimos aprendiendo sobre el sistema operativo de código abierto de Sun.



```

charly@wrap:~ - Shell - Konsole
2007-08-02 10:52:15,937 fail2ban.actions: WARNING [vsftpd] Ban 10.0.0.254
==> /var/log/auth.log <==
Aug 2 10:52:15 vdr vsftpd: (pan_unix) authentication failure; logname= uid=0 eu
id=0 tty=ftp ruser=charly rhost=10.0.0.254 user=charly
==> /var/log/fail2ban.log <==
2007-08-02 10:57:15,941 fail2ban.actions: WARNING [vsftpd] Unban 10.0.0.254

```

Figura 2: El bloqueo de IPtables del equipo 10.0.0.254 comenzó a las 10:52 y finalizó a las 10:57.