The Sys admin's daily grind: Fail2ban

BANNING BRUTES

Users log on to services such as SSH, ftp, SASL, POP3, IMAP, Apache htaccess, and many more using their names and passwords. These popular access mechanisms are a potential target for brute-force attacks. An attentive bouncer will keep dictionary attacks at bay. **BY CHARLY KÜHNAST**

When users are allowed to choose passwords of their own volition, they often choose something fairly weak, like the name of a friend or pet. This predictable human behavior is something that the bad guys relish.

All an attacker needs to do is set up a loop of login attempts that references a dictionary list of passwords. After all, chances are very slight that the user has set up a password like *4G&dP9a!* for the account under attack.

To counteract this inherent vulnerability, it makes sense to restrict the number of login attempts – at least for part of the time. Although *MaxAuthTries* has a basic mechanism for doing this, some legacy services don't.

Fail2ban [1] closes this gap. Some distributions, such as Debian, Ubuntu, and Gentoo, include Fail2ban. The source code and packages for a couple of other distributions are available online [2].

Fail2Ban comprises a server daemon and a client that interprets the central configuration files, *fail2ban.conf* and *jail.conf*, and forwards commands to the server. Fail2ban parses one or multiple logfiles and checks each line against regular expressions. This lets Fail2Ban call IPtables to block an attacker's IP address for a configurable period of time when a definable number of login attempts has been made.

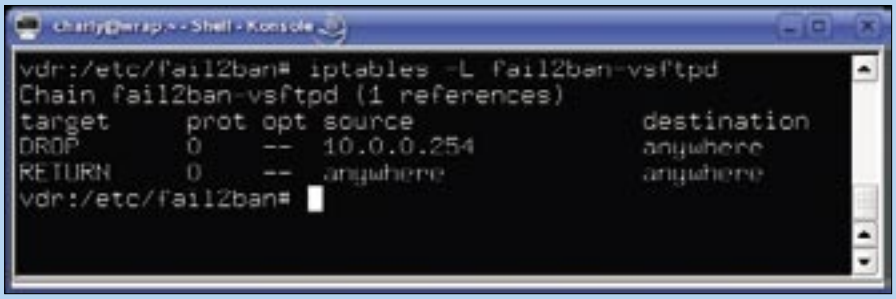

Figure 1: The IPtables list command shows that Fail2ban has caused the firewall to block the host at 10.0.0.254.

Hardening an ftp Server

As an example, say I run Vsftpd as my ftp server. After three unsuccessful login attempts, the host is supposed to block the client's IP address for five minutes, as shown in Figure 1. Listing 1 shows a matching entry in the *jail.conf* configuration file.

To give the server five minutes of peace, I changed the *bantime* entry from the default of 600 to 300 seconds. This amount of time is sufficient to prevent dictionary attacks but is still short enough to avoid annoying legitimate users who have inadvertently pressed the Caps lock key.

Figure 2 shows that the IPtables blockade starts at 10:52am and ends at 10:57am – this makes one less thing to worry about. ■

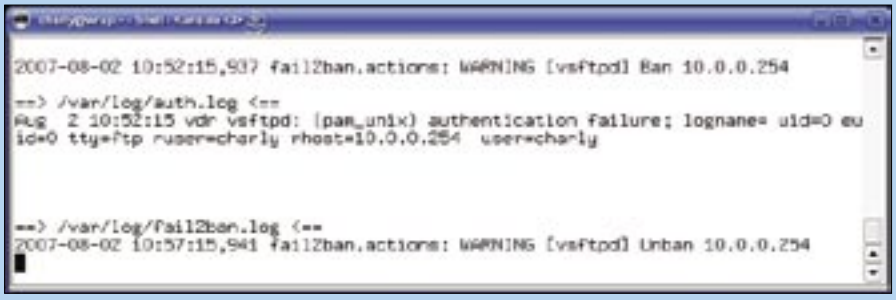

Figure 2: The IPtables blockade against the host at 10.0.0.254 started at 10:52am and ended at 10:57am.

Listing 1: jail.conf Entry

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

INFO

[1] Fail2ban: *http://www.fail2ban.org*

[2] Source code and packages: *http://www.fail2ban.org/wiki/index.php/Downloads*

SYSADMIN

OpenSSI 64
Learn how to set up load-leveling in the OpenSSI clustering solution.

THE AUTHOR

Charly Kühnast is a Unix System Manager at the data center in Moers, near Germany's famous River Rhine. His tasks include ensuring firewall security and availability and taking care of the DMZ (demilitarized zone).