Prevent SSH Brute Force Dictionary Attacks

Why

As soon as it is on the Internet people will try to brute force attack your server over ssh. Basically they keep on pounding your system trying different passwords.

Just look in /var/log/auth.log to see some attackes,

```
cat /var/log/auth.log | grep "Invalid user"
Jun 19 18:18:33 myra sshd[29346]: Invalid user oracle from 210.83.86.139
Jun 19 18:18:36 myra sshd[29349]: Invalid user test from 210.83.86.139
Jun 19 18:19:02 myra sshd[29381]: Invalid user kylix from 210.83.86.139
Jun 19 18:19:09 myra sshd[29387]: Invalid user www from 210.83.86.139
```

Fail2ban makes this kind of attack more difficult. After a chosen number of failed login attempts from the same ip address, fail2ban blocks that ip address for a set period of time. As constantly changing ip addresses is not a trivial task, the attacker may move on to another system.

HOWEVER, you can still be compromised within a few days if you are only using username and password authentication. If your SSH authentication is available on the Internet, you install fail2ban (shown below) and switch to SSH Key Authentication as soon as possible.

Install Fail2ban

Install Fail2ban,

```
sudo apt-get install fail2ban
```

The fail2ban installer also starts fail2ban as a service right after installation completes.

Most of the how fail2ban works is in /etc/fail2ban/jail.conf and here are the highlights,

```
maxretry = 6 # under the ssh section you are allowed 6 retries}
bantime = 600 # 600 seconds = 10 minutes
ignoreip = 127.0.0.1 # do not block list, and CIDR list
```

The default settigs of fail2ban are usually good enough but you can also customize fail2ban to suit your needs.

After a day or so on the Internet you should start seeing people getting banned in the logs, **/var/log/fail2ban.log**. Here is an example of an ip getting banned and then after 10 minutes it unbans,

```
2009-02-15 10:29:24,108 fail2ban.actions: WARNING \[ssh\] Ban 59.63.25.158
2009-02-15 10:39:24,137 fail2ban.actions: WARNING \[ssh\] Unban
59.63.25.158
```

Unbanning

To unban a user try these instructions. I am hesitant about playing with the ip tables in any way, so I have not tried myself. I usually just wait the 10 minutes.

According to the developers, Fail2ban version 0.9 will include an unban command through it's own client program.