Install and Configure Fail2Ban on Ubuntu 18.04

Installing fail2ban can be done with a single command:

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

When that command finishes, fail2ban is ready to go. You'll want to start and enable the service with the commands:

```
sudo systemctl start fail2ban
```

```
sudo systemctl enable fail2ban
```

Configuring a jail

Next we're going to configure a jail for SSH login attempts. In the */etc/fail2ban* directory, you'll find the jail.conf file. Do not edit this file. Instead, we'll create a new file, jail.local by copying the jail.conf to it, and override any similar settings in jail.conf. Our new jail configuration will monitor */var/log/auth.log*, use the fail2ban sshd filter, set the SSH port to 22, and set the maximum retry to 3. To do this, issue the command:

```
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

locate the [sshd] section, and edit to match the following contents:

```
[sshd]
enabled = true
port = 22
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 604800 # ban for 7 days
```

Next, locate and uncomment the ignoreip variable and set it as below where 192.xxx.xxx.xxx is your IP address. Enter multiple addresses and/or networks separated by a space:

```
ignoreip = 127.0.0.1/8 ::1 192.xxx.xxx.xxx
```

Save and close that file. Restart fail2ban with the command:

```
sudo systemctl restart fail2ban
```

At this point, if anyone attempts to log into your Ubuntu Server via SSH, and fails three times, they will be prevented from entry, by way of iptables blocking their IP Address.

Testing and unbanning

You can test to make sure the new jail works by failing three attempts at logging into the server, via ssh. After the third failed attempt, the connection will hang. Hit [Ctrl]+[c] to escape and then attempt to SSH back into the server. You should no longer be able to SSH into that server from the IP address you were using.

You can then unban your test IP address with the following command:

```
sudo fail2ban-client set sshd unbanip IP_ADDRESS
```

where IP_ADDRESS is the banned IP Address.

You should now be able to log back into the server with SSH.

Revision #1
Created 1 December 2020 19:54:31 by Dino Edwards
Updated 6 December 2021 19:09:56 by Dino Edwards