To install Fail2ban

Sudo apt-get install fail2ban

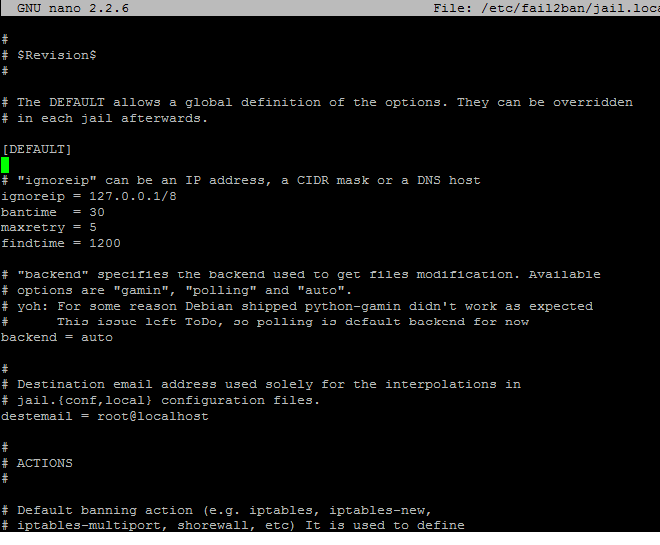
Fail2ban has a default configuration file and is located at /etc/fail2ban/jail.conf. This file should be left alone and the configurationwork should be done in a local copy of that file. So we use the command:

Sudo cp /etc/fail2ban/jail.conf /etc /etc/fail2ban/jail.local

Now open up the jail.local file

Sudo nano /etc/fail2ban/jail.local

When the file is opened u see a default page, we’ve changed some value’s and added few.



Just below the [DEFAULT] rule there’s ignoreip, bantime and maxretry in the default page.  
We’ve adjusted the bantime from 600 seconds to 30 seconds because it’s a working project and it would be annoying if everyone gets banned once in a while.

We’ve added the line findtime = 1200  
It might come in handy to know what these lines mean.  
**Bantime** is the actual time the user that tries to bruteforce your server or typed their password incorrectly is banned. As explained above it’s just for 30 seconds now because it would take more time to unban our developers than to wait the 30 seconds.  
**maxretry** means the amount of time a user may get there password wrong or the amount of time a user could try to bruteforce your server.  
If the user has generated the “maxretry” within the last “**findtime**” the user gets banned.  
So the “findtime” is basically the amount of time the user gets to enter as many incorrect passwords as the value of “maxretry”

Now restart fail2ban

Sudo service fail2ban restart