FAIL2BAN

INSTALLATION

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

INITIAL CONFIGURATION

```
cd /etc/fail2ban

sudo cp jail.conf jail.local
```

At this stage of the course, the only jail that concerns us is the SSH jail and this is enabled by default.

Protecting SSH access to your server is just one layer in protecting your server.

FAIL2BAN LOG FILES

Fail2ban has its own log file, located in the following directory: /var/log/fail2ban.log

Ownership

The fail2ban.log is owned by the user root and the group admin. From a previous lecture, group owners are used to organize users.

```
-rw-r----- 1 root   adm     2815 Jul  3 06:33 fail2ban.log
```

Permissions

The permissions are as follows:

```
fail2ban.log 640
```

That means the owner can read and write to the files, the group can read and other users have no permissions on the files. Currently your user is the other user, so you have no permissions of these files.

Add your user to the admin group. That will give you read permissions on the log files.

```
sudo usermod –a –G admin $USER
```

To enable the above change, you need to log out and then login to your server.

Now, you can view the contents of a log file. To view the contents of a log file, you can use any of the following commands, followed by the log file name.

```
cat | less | tail –f
```