

FAIL2BAN

INSTALLATION

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

INITIAL CONFIGURATION

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

FAIL2BAN CONFIGURATION

Open the jail.local file and edit as per the video lectures

THE SSH JAIL

Open the defaults-debian.conf file:

```
sudo nano /etc/fail2ban/jail.d/defaults-debian.conf
```

Confirm the ssh jail is enabled:

```
[sshd]
enabled = true
```

Finally, to enable the changes we have made to the various fail2ban configuration files, restart the f2b service:

```
sudo systemctl restart fail2ban
```

FAIL2BAN LOG FILES

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

```
sudo cat filename
sudo less filename
```

The cat command will display the file on the screen, that's fine if the file contains very little information.

The less command is more useful, as each page will be paused for you to peruse. You can use the following keys: HOME, END, PgUp, PgDn and your cursor keys. Pressing q will quit less and return to the prompt.

IMPORTANT NOTICE

Copying and then pasting commands from a pdf can produce errors when pasting the commands into your terminal emulator.

Confirm the accuracy & correctness of the command before pressing enter.