Gentoo – Deny Hosts

If you find your ssh server is getting hit by a lot of brute force attempts from the internet, and want to do something to defend yourself against them then denyhosts is for you! It helps to alleviate some of the stress on your server that occurs when someone or lots of someones are trying to hack their way into your ssh server. Basically the service watches your ssh traffic, and if it sees an IP address hitting a threshold of failed attempts it adds the address to your /etc/hosts.deny file so that it is blocked from future access attempts.

Simply install the package through emerge:

The initial configuration in /etc/denyhosts.conf should suffice, however it is well commented and you can edit it to suit your needs. You may want to add your email address in the ADMIN_EMAIL = variable so that denyhosts can email you alerts.

Once it is installed and configured start it up and add it to the default runlevel:

Thats it! Your server will now block an IP address after 3 failed ssh login attempts.

But what do I do if I accidentally lock out a valid IP address? Glad you asked!

You need to remove the wrongfully accused IP address from the following files using this process:

First stop the denyhosts service:

Then remove the IP from the following files:

/etc/hosts.deny

```
/var/lib/denyhosts/hosts
/var/lib/denyhosts/hosts-restricted
/var/lib/denyhosts/hosts-root
/var/lib/denyhosts/hosts-valid
```

Now restart the service:

You should now be able to ssh from the blocked IP address once again.