

Re: firewall setup and whois for blacklisting IP's

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/questions/2005-01/1412.html>

From: Louis LeBlanc (*FreeBSD_at_keyslapper.org*)

Date: 01/10/05

Date: Mon, 10 Jan 2005 14:16:52 -0500

To: dave <dmehler26@woh.rr.com>

On 01/10/05 01:34 PM, dave sat at the `puter and typed:

> *Hello,*
> *For your setup of blacklisting IP's do you use any cron scripts for*
> *procedure automation?*
> *I'm assuming for your firewall block table that you store that in a*
> *separate file? Can you send that file my way? I've tried to come up with a*
> *perl script to get whois information out of a maillog, i'm gettin ssh*
> *attempts that corespond to mail relaying atempts so i thought that would be*
> *best, however there seems to be difference in the way certain servers*
> *return whois information, do you have any experience with this?*
> *When you email an abuse contact approximately what percentage of them*
> *write you back? I've emailed several providers comcast mostly in the US, but*
> *i have not heard anything back from the person. Is there some sort of*
> *standard email template you follow?*
> *Thanks.*
> *Dave.*

Good questions. I don't use any automation, I just look at the auth logs on a regular basis. The reason is that I don't want to block every network that attempts my system. I haven't found any of the security settings to include illegal user attempts in the security mailing – though I'd think that would be there, and on by default. If it were there, I'd use that as a more reliable alert.

Also, I don't typically do anything at all with Amsterdam IPs, mostly because I haven't decided whether there's anything legitimate to be expected. I know there's a lot of porn sites, and this could easily be a starting point for a lot of these attempts, but it's a fairly open society, and I don't know whether the ISPs would really care about them. They may well care in those that I do block, but my experience has shown that they typically won't make much effort. Giving the benefit of the doubt, it's probably more of a language barrier than a lack of interest.

When I used ipfw, I did keep the blocked lists in a separate file, /etc/rc.firewall.blocked contained a rule for each CIDR block I rejected. Now I keep it in a table definition in /etc/pf.conf. So far, in the last month, this is the full table definition for my pf firewall:

