Subject: Re: Any way to limit SSH bruteforce scanning of VPS's on the node?
Posted by Ales on Thu, 22 Dec 2011 01:54:18 GMT
View Forum Message <> Reply to Message

I agree, a solid iptables solution that's on the HN side only is the most clean approach. Especially if you don't have complete control over VMs or need to keep resource consumption as low as possible.

I'd start by looking at existing stateful firewalls to see how they limit access to sshd. Just to get some more ideas about possible iptables rules and policies.

I'm afraid I don't have a more specific suggestion than this. Perhaps someone else has done more research in this direction and can chip in.

Just to note, fail2ban's memory consumption is caused by a large default stack size on linux (ie. 10MB on SL6). I believe fail2ban would be quite happy with 256kB but it would need a small patch to put this into effect on SL/CentOS/RHEL. This would lower fail2ban's memory consumption at least tenfold.

It's worth looking into if you are using it on some nodes end would need to lower its memory footprint.

Also, when I mentioned patching its init script (fail2ban from EPEL 6) for openvz, I meant this: currently, when attempting to start the program, its init script simply looks for any running fail2ban processes and if it sees any, it won't start fail2ban.

This is a problem when you try to run fail2ban on the HN while it's already running in some VM, since this VM process is visible on the HN and the init script incorrectly assumes fail2ban is already running on the HN itself.

There is a bug open about this at EPEL but I don't think they'll act on it since the patch provided is openvz specific. Anyway, a patch is provided in the bug report and it works just fine.

It's a bit unrelated to what you're asking but I thought I'd mention it since you said you use fail2ban too.