Subject: Re: Any way to limit SSH bruteforce scanning of VPS's on the node?
Posted by Ales on Wed, 21 Dec 2011 11:47:28 GMT
View Forum Message <> Reply to Message

I understand that you need a good solution with as little per VPS configuration as possible, but I don't know if that's easily achievable. Custom iptable rules seem the best approach in your case.

That aside, I think the most effective solutions would be changing the sshd port and using fail2ban.

There are other tools similar to fail2ban, like denyhosts and BlockHosts. Last time I made comparisons, fail2ban was the most versatile one and it seems most widely used.

If you go for fail2ban, make sure to patch it's init script on the hardware node, since it interferes with the fail2ban services on the VMs. Patch can be found somewhere in Red Hat's bugzilla, just search for fail2ban.

I'd recommend using both, different sshd port and one of these tools, at the same time. Just changing the port is a trivial obstacle to overcome if someone is targeting your server specifically.