

## Re: pam, ssh, user account vulnerability

*Source:* <http://linux.derkeiler.com/Newsgroups/comp.os.linux.setup/2005-10/0111.html>

---

*From:* Lenny G. ([alengarbage\\_at\\_yahoo.com](mailto:alengarbage_at_yahoo.com))

*Date:* 10/04/05

Date: 3 Oct 2005 20:56:15 -0700

So, to give a bit of resolution: I discovered why the PAM settings didn't seem to apply. Turns out that I upgraded from a version of openssh which had pam support on by default to a version that didn't have pam support unless "UsePAM=yes" was in /etc/ssh/sshd.conf. Since my old conf file was, well, a conf file, it didn't get updated when I upgraded.

Granted, I should have been a bit more careful when upgrading, but I'd also claim that default-off is the **WRONG** way to ship a package, especially when the precedent was default-on. This was on an upgrade from Fedora Core 2 to FC 4.

And, to put your minds at ease, the system was not compromised beyond the one account. The attacker is still trying to access that account almost daily, without luck. I've verified all installed packages, and have been monitoring network traffic from another box with a sniffer. The attacker wasn't too savvy -- the hack kits installed contained readme's with lists of systems that they could compromise, most of which were linux/freebsd/solaris versions that were at least 2 years old.

I am still experiencing a nearly constant barrage of dictionary attacks on simple account names (as I have for the past 3 years), sometimes at a rate of more than one every 5 seconds, but none on any accessible accounts. I'll likely install some sentry software to automatically blacklist ips involved in these types of attacks, but am not worried enough about it right now to, well, worry about it too much.