

Re: pam, ssh, user account vulnerability

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.setup/2005-09/0629.html>

From: Rick Moen (rick_at_linuxmafia.com)

Date: 09/28/05

Date: Wed, 28 Sep 2005 04:54:53 -0400

Peter T. Breuer <ptb@oboe.it.uc3m.es> wrote:

- > *Yes – it does sound a little as though he has an adore module*
- > *installed. He DOES want to boot from a live cd, get chkrootkit,*
- > *and run it on the disk, mounted under /mnt.*

Les, what Peter's saying is that he suspects the intruder used his remote ssh access to the "michael" account to crack root access (some privilege escalation or other), and then installed trojan-horse code as a Linux kernel module -- which, while running in kernelspace on your system, will not show up in runtime checks and can act to protect itself against discovery. He therefore suggests booting a known-uncompromised Linux boot disc (such as a Knoppix disc), mounting your HD's filesystems to make them accessible, and then -- while you're sure that nothing from your HD has been loaded into RAM and executed -- running a pattern-checking "rootkit detector" such as chkrootkit or rkhunter (or both) to search your HD known instances of intruders' bad juju.

One of the implications to note from the above is that, unless you're really good at system administration, your system probably harbours a number of local vulnerabilities usable for escalation from regular-user to root authority. When intruders break into your system masquerading as a legitimate user (e.g., the guy who broke in as michael/michael on yours), he/she will probably run, in his/her first ten minutes, a canned toolkit that tries, rapid-fire, a dozen or two recently popular local-escalation techniques. All he/she needs is one achieving success, then a rootkit (such as the "LKM" = Linux kernel module-type rootkit Peter alluded to) goes in to hide his/her presence from you, from that point forward.

- > *He wants to avoid his normal init sequence, as the files will have been*
- > *doctored to install the module at each boot. A simple ls -lr on the*
- > *init scripts can show the trail, but it's generally sysklogd's script*
- > *which has had the extra lines added.*

And you might want to look there and elsewhere in /etc/init.d/ , to see if something stands out. As I mentioned before, the "excellent

question" is how much scrutiny of your system is enough, before you can reasonably decide it's `_not_` compromised.

As you'll see if you read my (aforementioned) `_Linux Gazette_` article, installing and diligently configuring a file-based IDS `_before_` you suspect you have an intruder is one way to deal with that problem.

> *Makes sense. But if it's an `adore` module the checksums will be correct*
> *anyway. Neither he nor the checksummer will see the REAL files.*

What Peter is saying is: `_If_` there's an LKM rootkit, then it's in a perfect position (`_if_` and only if you boot through your normal boot sequence as opposed to booting a Knoppix disc) to make your scrutiny of your system pointless — by causing it to lie to you and tell you nothing bad was found.

That's why he stressed `_not_` booting your system as part of checking it.

Me, I still go back to what I was saying previously: If you have `_any_` reason to think your system might be compromised, then assume it is and do a clean rebuild as I outlined earlier. It's painful, but not as painful as realising that, say, your entire system and everything in or out of or on it has been spied on, interfered with, and/or corrupted by unauthorised personnel.

Adjust your paranoia to suit local norms. ;-> But don't forget that, 999 times out of 1000, the intruder neither knows nor cares about you or your affairs: Odds are, the entire process of intrusion was the activity of completely automated attack scripts strobing up and down publicly accessible IP addresses. (Thus, don't ever relax your guard on grounds of "I'm not significant enough to attack.")

--

Cheers,

Rick Moen
rick@linuxmafia.com

Mark Moraes: "Usenet is not a right."
Edward Vielmetti: "Usenet is a right, a left, a jab,
and a sharp uppercut to the jaw.
The postman hits! You have new mail."