

[SLE] Hacked?

Source: <http://linux.derkeiler.com/Mailing-Lists/SuSE/2004-04/2040.html>

From: Lucky Leavell (susemisc_at_UniXpress.com)

Date: 04/28/04

Date: Wed, 28 Apr 2004 09:53:32 -0400 (EDT)

To: "[SLE]" <suse-linux-e@suse.com>

OS: SuSE 9.0

This is a new FTP installation updated via YOU. During the install, one non-root user was created and used successfully for about a week. First sign of trouble: we couldn't login with error indicating an incorrect password. AS root we reset the password and can now login on a character screen but when logging in under KDE, receive the following error:

There was an error setting up inter-process communications with KDE. The message returned by the system was:

```
Could not read network connection list
/home/<user>/DCOPserver_HBADMIN_0
```

Please check that the dcopserver program is running.

A quick check of running processes shows no such process.

The KDE login fails and returns to a login screen. All other users can login just fine.

Further, we tried removing this user and his home directory along with all files/subdirectories but were unable to even list the following directories:

```
cannot access /home/<user>/qt (permission denied)
cannot access /home/<user>/kde (permission denied)
cannot access /home/<user>/wine (permission denied)
cannot access /home/<user>/Desktop (permission denied)
```

even as root.

Could this system have been hacked or compromised in some way? (How would I go about checking this?) If so, what should we do about it?

(I did enable SuSEfirewall2 closing all ports to the outside world.)

SuSE: [SLE] Hacked?

Thank you,
Lucky Leavell

--

Check the headers for your unsubscribe address
For additional commands send e-mail to suse-linux-e-help@suse.com
Also check the archives at <http://lists.suse.com>
Please read the FAQs: suse-linux-e-faq@suse.com