

## RE: system logging is not

---

*Source:* <http://linux.derkeiler.com/Mailing-Lists/RedHat/2006-02/msg00195.html>

---

- *From:* "Furnish, Trever G" <[TGFurnish@xxxxxxxxxxxxxxxx](mailto:TGFurnish@xxxxxxxxxxxxxxxx)>
  - *Date:* Wed, 15 Feb 2006 17:00:34 -0500
- 

Any idea why top couldn't find libncurses.so.4? I imagine that should be stored under /usr/lib – that's where it is on my RHEL3ES systems.

Why do you note that the system "can't create /var/log/messages"? Your earlier post shows /var/log/messages in the output of ls.

Do you get any errors when doing either of the following?

```
touch /var/log/messages  
echo foo >>/var/log/messages
```

After echo'ing foo into /var/log/messages, is "foo" in the file?

Looks like boot.log isn't going to be useful (since it's zero bytes), but perhaps the output of dmesg might show something helpful?

If you suspect a cracker, you might try spanning the port traffic on your switch over to another system and using ethereal to look at it. This is definitely not a guaranteed means of spotting an intrusion, of course. If you do have an intruder, he's not a very tidy one – skilled intruders don't break the system. :-)

-----Original Message-----

From: [redhat-list-bounces@xxxxxxxxxxx](mailto:redhat-list-bounces@xxxxxxxxxxx)  
[<mailto:redhat-list-bounces@xxxxxxxxxxx>] On Behalf Of Marty Landman  
Sent: Wednesday, February 15, 2006 7:28 AM  
To: General Red Hat Linux discussion list  
Subject: RE: system logging is not

At 09:50 AM 2/14/2006, McDougall, Marshall (FSH) wrote:

The fact that most of those files are empty(hacker like activity) and there are no .1, .2 etc does not look good. Did you do something at 18:04?

No, not that I can think of.

RE: system logging is not

Run a netstat and see what/who you are listening for or connected

to.

```
$ netstat -rn
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt
Iface
216.238.192.133 0.0.0.0 255.255.255.255 UH 0 0 0
ppp0
192.168.0.0 0.0.0.0 255.255.255.0 U 0 0 0
eth0
169.254.0.0 0.0.0.0 255.255.0.0 U 0 0 0
eth0
127.0.0.0 0.0.0.0 255.0.0.0 U 0 0 0
lo
0.0.0.0 216.238.192.133 0.0.0.0 UG 0 0 0
ppp0
$
```

Look normal, doesn't it?

Wtmp is time stamped 1.5 hrs later. Run last, it might tell you who was there or what id was compromised.

```
]$ sudo last
marty pts/0 nosoup4u Tue Feb 14 15:42 still logged
in
marty pts/0 nosoup4u Mon Feb 13 20:41 - 22:05 (01:24)
root pts/0 :0.0 Mon Feb 13 18:20 - 20:41 (02:20)
root :0 Mon Feb 13 18:20 - 18:46 (00:25)
reboot system boot 2.4.20-8 Mon Feb 13 18:18 (21:39)
reboot system boot 2.4.20-8 Mon Feb 13 18:14 (21:43)
marty pts/1 :0.0 Mon Feb 13 18:06 - down (00:06)
marty :0 Mon Feb 13 18:06 - down (00:06)
marty pts/0 nosoup4u Mon Feb 13 18:05 - down (00:07)
reboot system boot 2.4.20-8 Mon Feb 13 18:04 (00:08)
```

```
wtmp begins Mon Feb 13 18:04:26 2006
$
```

BTW nosoup4u is my Windows workstation - I'm ssh'd into the RH box.

Look in /tmp for anything unusual. Isolate it from your network.

```
$ ls -al /tmp
total 572
```

RE: system logging is not

RE: system logging is not

```
drwxrwxrwt 12 root root 4096 Feb 14 04:02 .
drwxr-xr-x 20 root root 4096 Feb 13 18:33 ..
drwxrwxrwt 2 root root 4096 Feb 13 18:46 .ICE-unix
-r--r--r-- 1 root root 11 Feb 13 18:46 .X0-lock
drwxrwxrwt 2 root root 4096 Feb 13 18:46 .X11-unix
srwx----- 1 root nobody 0 Feb 13 18:20 .fam_socket
drwxrwxrwt 2 xfs xfs 4096 Feb 13 18:19 .font-unix
srw-rw-rw- 1 root root 0 Feb 13 18:19 .gdm_socket
-rw-rw-rw- 1 root root 464160 Feb 10 10:04 irc.tar.gz
drwx----- 2 joel users 4096 Dec 5 16:27 orbit-joel
drwx----- 2 marty marty 12288 Feb 13 18:13 orbit-marty
drwx----- 2 root root 12288 Feb 13 18:46 orbit-root
drwxr-xr-x 2 marty marty 4096 Dec 3 15:06 samba
-rwxr--r-- 1 root root 44377 Feb 13 18:41
scrollkeeper-tempfile.0
drwx----- 2 marty marty 4096 Dec 11 18:49 ssh-XXRI9PKz
drwx----- 2 root root 4096 Jan 3 13:32 ssh-XXgHv7Ve
drwxrwxrwt 3 marty marty 4096 Jan 26 19:04 uscreens
[marty@BANYAN ~]$ ls -al /tmp/samba
total 8
drwxr-xr-x 2 marty marty 4096 Dec 3 15:06 .
drwxrwxrwt 12 root root 4096 Feb 14 04:02 ..
$
```

Good luck.

I removed everything on /tmp and rebooted, system still can't create /var/log/messages. It also is now unable to start X-Windows on the console.

What might I do next here?

Marty

-----Original Message-----

From: redhat-list-bounces@xxxxxxxxxx

[mailto:redhat-list-bounces@xxxxxxxxxx] On Behalf Of Marty Landman

Sent: Monday, February 13, 2006 8:10 PM

To: redhat-list@xxxxxxxxxx

Subject: system logging is not

My RH9 gateway suddenly seems to have developed some problems today.  
The

only thing special I recall doing was to change from a netgear hub to a

RE: system logging is not

RE: system logging is not

linksys switch and add an 8th box to my lan. There is also a netgear switch to which this box is plugged in which used to uplink to the netgear hub but now uplinks to the linksys switch. All 8 computers were

visible from my Win xp workstation after doing that btw.

Later I noticed that samba didn't seem to be working on my Win XP workstation – although it can SSH to the RH box. And it's still functioning as my LAN gateway. Saw a bunch of attempts on /var/log/samba/.log (is that a kosher name btw?) evidence of attempted break-ins from a day or two ago.

So not knowing what else to do I rebooted – windows user instinct :). Noticed during the reboot that system logging and httpd startup both FAILED. OTOH using Nautilus from the console I could find the other 7 computers on the network, but not this computer itself.

Here's some shell stuff that I think illustrates some of what's going on:

```
[marty@BANYAN ~]$ pwd
/home/marty
[marty@BANYAN ~]$ ls -al /var/log
total 324
drwxr-xr-x 2 root root 4096 Feb 13 18:46 .
drwxr-xr-x 21 root root 4096 Jul 30 2005 ..
-rw-r--r-- 1 root root 28509 Feb 13 18:46 XFree86.0.log
-rw-r--r-- 1 root root 28584 Feb 13 18:20
```

XFree86.0.log.old

```
-rw----- 1 root root 0 Feb 13 18:04 boot.log
-rw----- 1 root root 0 Feb 13 18:04 cron
-rw-r--r-- 1 root root 6532 Feb 13 18:18 dmesg
-rw-r--r-- 1 root root 65631 Feb 13 18:18 ksyms.0
-rw-r--r-- 1 root root 65631 Feb 13 18:14 ksyms.1
-rw-r--r-- 1 root root 65631 Feb 13 18:04 ksyms.2
-rw----- 1 root root 0 Feb 13 18:04 maillog
-rw----- 1 root root 0 Feb 13 18:04 messages
-rw----- 1 root root 0 Feb 13 18:04 secure
-rw----- 1 root root 0 Feb 13 18:04 spooler
-rw----- 1 root root 315 Feb 13 18:12 sudolog
-rw-rw-r-- 1 root utmp 30336 Feb 13 20:41 wtmp
[marty@BANYAN ~]$ df
Filesystem 1K-blocks Used Available Use% Mounted on
/dev/hdd1 5278644 2073532 2936972 42% /
/dev/hda1 99251 9324 84802 10% /boot
```

RE: system logging is not

RE: system logging is not

```
none 127664 0 127664 0% /dev/shm
/dev/hda2 4035432 33080 3797360 1% /mnt/kramer
/dev/hdb1 241263968 32998936 196009448 15% /mnt/maestro
[marty@BANYAN ~]$ top
top: error while loading shared libraries: libncurses.so.4: cannot open
```

shared object file: No such file or directory [marty@BANYAN ~]\$

---

At this point I wonder if my computer's been hijacked or somehow corrupted.

Either way not sure what do to next.

Thanks in advance,

Marty

Marty Landman, Face 2 Interface Inc. 845-679-9387 Webmaster's Bulletin Board: <http://bbs.face2interface.com/> Web Installed Formmail: <http://face2interface.com/formINSTal>

--  
redhat-list mailing list  
unsubscribe <mailto:redhat-list-request@xxxxxxxxxx?subject=unsubscribe>  
<https://www.redhat.com/mailman/listinfo/redhat-list>

--  
redhat-list mailing list  
unsubscribe <mailto:redhat-list-request@xxxxxxxxxx?subject=unsubscribe>  
<https://www.redhat.com/mailman/listinfo/redhat-list>

Marty Landman, Face 2 Interface Inc. 845-679-9387 Webmaster's Bulletin Board: <http://bbs.face2interface.com/> Web Installed Formmail: <http://face2interface.com/formINSTal>

--  
redhat-list mailing list  
unsubscribe <mailto:redhat-list-request@xxxxxxxxxx?subject=unsubscribe>  
<https://www.redhat.com/mailman/listinfo/redhat-list>

--  
redhat-list mailing list  
unsubscribe <mailto:redhat-list-request@xxxxxxxxxx?subject=unsubscribe>  
<https://www.redhat.com/mailman/listinfo/redhat-list>

RE: system logging is not