

## Re: What is this? A hacker?

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.misc/2002-05/0616.html>

---

**From:** Kevin Buhr ([buhr@telus.net](mailto:buhr@telus.net))

**Date:** 05/27/02

From: Kevin Buhr <[buhr@telus.net](mailto:buhr@telus.net)>

Date: Mon, 27 May 2002 16:03:49 GMT

"@lex" <[alexandros@sklavos.de](mailto:alexandros@sklavos.de)> writes:

>

> *Recently my system (linux SuSE 7.3) crashed several times...*

> *I found following, quite interesting entry in last:*

>

> \*\*\*\*\*0\*\*\*\*\*0\*\*\* *Thu Jan 1 01:00 – crash (11831-01:24*

"last" works by reading the "wtmp" file (which is probably located in "/var/log" or "/var/adm"). This file just contains a long list of coded entries, and these entries mean things like "bob logged in at 4:00 from foohost", "sally logged in at 4:30 from console", "sally logged out at 4:30 from console", "bob logged out at 6:00 from foohost", "the system was rebooted at 10:30", and "the system came back up at 10:33".

Entries are added to "wtmp" behind the user's back by system programs like "init", "login", and "sessreg".

"last" just reads this linear history of system activity, tries to guess what it means, and displays the results. In particular, if there's a garbage entry that says "<binary crap user> logged in at 12:00am on January 1, 1970 GMT (time zero on many Unix hosts, and a Thursday, by the way) from <binary crap host>" without a matching logout entry followed by a "system came back up at 3:00" without a previous "system was rebooted" entry, then you're going to see an entry telling you that "\*\*\*\*\*" logged in from "0\*\*\*\*\*0\*\*\*" on Thursday, January 1 (1970, that is) at 1:00am local time and was logged in for 11,831 days, 1 hour, and 24 minutes before the computer crashed.

Most likely, there's no shadowy figure logged in to your computer right now. It's just a corrupt "wtmp" file that resulted from one of the crashes. As "root", you can move the file out of the way and create a blank one to start over:

```
cd /var/log
```

comp.security.misc: Re: What is this? A hacker?

```
mv wtmp wtmp-saveme
> wtmp
last # should give an empty list
```

--

Kevin Buhr <[buhr@telus.net](mailto:buhr@telus.net)>

---

- *Next message:* [Jerry Leslie: "Re: Unhackable Network ?"](#)
- *Previous message:* [Bill Unruh: "Re: What is this? A hacker?"](#)
- *In reply to:* [@lex: "What is this? A hacker?"](#)
- *Next in thread:* [@lexandros: "Re: What is this? A hacker?"](#)
- *Messages sorted by:* [\[ date \] \[ thread \] \[ subject \] \[ author \] \[ attachment \]](#)