How to get full host and IP address of last month logged in users on GNU / Linux

Author : admin

This post might be a bit trivial for the Linux gurus, but for novices Linux users hopefully helpful. I bet, all Linux users know and use the so common used **last** command.

last cmd provides information on last logged in users over the last 1 month time as well as shows if at present time of execution there are logged in users. It has plenty of options and is quite useful. The problem with it I have often, since I don't get into the habit to use it with arguments different from the so classical and often used:

last | less

back in time when learning Linux, is that whether run it like this I can't see full hostname of users who logged in or is currently logged in from remote hosts consisting of longer host names strings than 16 characters.

To show you what I mean, here is a chunk of **last | less** output taken from my home router *pc-freak.net*.

```
 # last|less
root     pts/1        ip156-108-174-82 Fri Dec 21 13:20   still logged in
root     pts/0        ip156-108-174-82 Fri Dec 21 13:18   still logged in
hipo     pts/0        ip156-108-174-82 Thu Dec 20 23:14 - 23:50  (00:36)
root     pts/0        g45066.upc-g.che Thu Dec 20 22:31 - 22:42  (00:11)
root     pts/0        g45066.upc-g.che Thu Dec 20 21:56 - 21:56  (00:00)
play     pts/2        vexploit.net.s1. Thu Dec 20 17:30 - 17:31  (00:00)
play     pts/2        vexploit.net.s1. Thu Dec 20 17:29 - 17:30  (00:00)
play     pts/1        vexploit.net.s1. Thu Dec 20 17:27 - 17:29  (00:01)
play     pts/1        vexploit.net.s1. Thu Dec 20 17:23 - 17:27  (00:03)
play     pts/1        vexploit.net.s1. Thu Dec 20 17:21 - 17:23  (00:02)
root     pts/0        ip156-108-174-82 Thu Dec 20 13:42 - 19:39  (05:56)
reboot   system boot  2.6.32-5-amd64   Thu Dec 20 11:29 - 13:57 (1+02:27)
root     pts/0        e59234.upc-e.che Wed Dec 19 20:53 - 23:24  (02:31)
```

The hostname *last* cmd output as you can see is sliced, so one cannot see full hostname. This is quite inconvenient, especially, if you have on your system some users who logged in with suspicious hostnames like the user play which is a user, I've opened for people to be able to play my system installed Cool Linux ASCII (text) Games. In normal means, I would skip worrying about the **vexploit.net.s1.....** user, however as I've noticed *one of the ascii games similar to nethack called hunt was kept hanging on the system putting a load of about 50% on the CPU* and was run with the **play** user and according to logs, the last logged in username with play was containing a hostname with "vexploit.net" as a hostname.

This looked to me very much like a script kiddie, attempt to root my system, so I killed *hunt, huntd and*

HUNT hanging processes and decided investigate on the case.

I wanted to do whois on the host, but since the host was showing incomplete in *last* | less, I needed a way to get the full host. The first idea I got is to get the info from binary file **/var/log/wtmp** - storing the hostname records for all logged in users:

```
# strings /var/log/wtmp | grep -i vexploit | uniq
vexploit.net.s1.fti.net
```

To get in a bit raw format, all the hostnames and IPs (whether IP did not have a PTR record assigned):

```
 strings /var/log/wtmp|grep -i 'ts/' -A 1|less
```

Another way to get the full host info is to check in **/var/log/auth.log** - this is the Debian Linux file storing ssh user login info; in Fedora and CentOS the file is **/var/log/secure**.

```
# grep -i vexploit auth.log
Dec 20 17:30:22 pcfreak sshd[13073]: pam_unix(sshd:auth): authentication failure; logname= uid=0
euid=0 tty=ssh ruser= rhost=vexploit.net.s1.fti.net  user=play
```

Finally, I decided to also check **last** man page and see if ***last is capable of showing full hostname or IPS of previously logged in hosts***. It appears, last is having already an argument for that so my upper suggested methods, turned to be useless overcomplexity. To show full hostname of all hosts logged in on Linux over the last month:

```
# last -a |less

root     pts/2        Fri Dec 21 14:04   still logged in    ip156-108-174-82.adsl2.static.versatel.nl
root     pts/1        Fri Dec 21 13:20   still logged in    ip156-108-174-82.adsl2.static.versatel.nl
root     pts/0        Fri Dec 21 13:18   still logged in    ip156-108-174-82.adsl2.static.versatel.nl
hipo     pts/0        Thu Dec 20 23:14 - 23:50  (00:36)     ip156-108-174-82.adsl2.static.versatel.nl
root     pts/0        Thu Dec 20 22:31 - 22:42  (00:11)     g45066.upc-g.chello.nl
root     pts/0        Thu Dec 20 21:56 - 21:56  (00:00)     g45066.upc-g.chello.nl
play     pts/2        Thu Dec 20 17:30 - 17:31  (00:00)     vexploit.net.s1.fti.net
play     pts/2        Thu Dec 20 17:29 - 17:30  (00:00)     vexploit.net.s1.fti.net
play     pts/1        Thu Dec 20 17:27 - 17:29  (00:01)     vexploit.net.s1.fti.net
play     pts/1        Thu Dec 20 17:23 - 17:27  (00:03)     vexploit.net.s1.fti.net
play     pts/1        Thu Dec 20 17:21 - 17:23  (00:02)     vexploit.net.s1.fti.net
root     pts/0        Thu Dec 20 13:42 - 19:39  (05:56)     ip156-108-174-82.adsl2.static.versatel.nl
reboot   system boot  Thu Dec 20 11:29 - 14:58 (1+03:28)    2.6.32-5-amd64
root     pts/0        Wed Dec 19 20:53 - 23:24  (02:31)     e59234.upc-e.chello.nl
```

Listing all logged in users remote host IPs (only) is done with *last's "-i" argument*:

```
 # last -i
root     pts/2        82.174.108.156   Fri Dec 21 14:04   still logged in
root     pts/1        82.174.108.156   Fri Dec 21 13:20   still logged in
root     pts/0        82.174.108.156   Fri Dec 21 13:18   still logged in
hipo     pts/0        82.174.108.156   Thu Dec 20 23:14 - 23:50  (00:36)
root     pts/0        80.57.45.66      Thu Dec 20 22:31 - 22:42  (00:11)
root     pts/0        80.57.45.66      Thu Dec 20 21:56 - 21:56  (00:00)
play     pts/2        193.252.149.203  Thu Dec 20 17:30 - 17:31  (00:00)
play     pts/2        193.252.149.203  Thu Dec 20 17:29 - 17:30  (00:00)
play     pts/1        193.252.149.203  Thu Dec 20 17:27 - 17:29  (00:01)
play     pts/1        193.252.149.203  Thu Dec 20 17:23 - 17:27  (00:03)
play     pts/1        193.252.149.203  Thu Dec 20 17:21 - 17:23  (00:02)
root     pts/0        82.174.108.156   Thu Dec 20 13:42 - 19:39  (05:56)
reboot   system boot  0.0.0.0          Thu Dec 20 11:29 - 15:01 (1+03:31)
```

One note to make here is on every 1st number of month **last** *command clear ups the records storing for user logins in* ***/var/log/wtmp*** *and nullifies the file.*

Though the other 2 suggested, methods are not necessary, as they are provided in last argument. They're surely a mus do routine, t when checking a system for which doubting it could have been intruded (hacked). Checking both */var/log/wtmp* and */var/log/auth.log* / and /var/log/auth.log.1 content and comparing if the records on user logins match is a good way to check if your login logs are not forged. It is not a 100% guarantee however, since sometimes attacker scripts wipe out their records from both files. Out of security interest some time, ago I've written a small script to clean logged in user recordfrom /var/log/wtmp and /var/log/auth.log - log_cleaner.sh - the script has to be run as a super to have write access to */var/log/wtmp* and */var/log/auth.log*. It is good to mention for those who don't know, that last reads and displays its records from */var/log/wtmp* file, thus altering records in this files will alter **last** displayed login info.

Thanks God in my case after examing this files as well as super users in /etc/passwd, there was no "signs", of any succesful breach.