Contents

[**Last Command:** 2](#_Toc479321759)

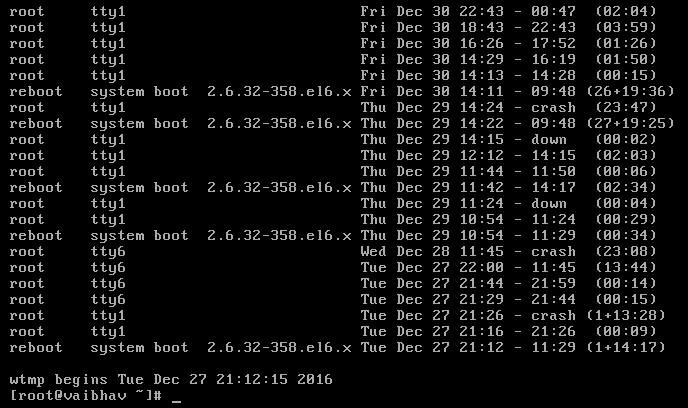
[**Last Command with more options:** 3](#_Toc479321760)

[**Lastb Command: bad logins details** 4](#_Toc479321761)

[**Lastlog command:** 5](#_Toc479321762)

# **Last Command:**

* It displays information about all users logged in/out since /var/log/wtmp file was created.
* This /var/log/wtmp file is a binary file which cannot be viewed by text editors.
* It searches back through the file /var/log/wtmp. So last command displays only successful login entries.
* File /var/log/wtmp is rotated by logrotate utility. So we can get information from last command until this file is rotated.
* Command: last



* First column represents user name.

E.g., root indicates user logged in as root user, reboot indicates user has rebooted the system. Reboot and shutdown are pseudo users. Examples: root, reboot

* Second column indicates how the user is connected. TTY means that user connect via direct connection to the computer/local terminal. PTS means user connect via remote connection such as SSH or telnet. In case, system is rebooted it shows system boot in this column. Examples: tty1, tty6,pts, system boot
* Third column indicates where the user come from.

If user connect from local computer, it shows 0.0 or nothing.

If user connect from remote computer, it shows hostname or IP address.

For reboot/shut down activity, kernel version is shown.

* Remaining columns display user log activity timing.

For an example: Tue Dec 27 21:12 - 11:29 (1+14:17)

User is logged in on Tue Dec 27 at 21:12 and logged out at 11:29.

Information in parenthesis indicates length of an event.

1+14:17 means 1 day, 14 hours and 17 minutes since last reboot/shutdown.

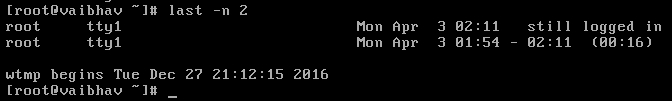
* Command last prints crash as logout time when there is no logout entry in wtmp database. wtmp has two has two entries for each user session. When a system crashes, second entry could be missing so last suppose user is still logged on when system crashes. [System crash means sudden failure of software/OS. In such cases, system stops functioning properly and exits.]
* Command last prints down when user was logged in from specific time until system is rebooted/ shut down.

## **Last Command with more options:**

* To limit number of lines shown, it will display lines from starting of output,

Command: last -n <count>

Example: last -n 2



* To hide hostname (3rd column) from output,

Command: last -R

* To display hostname (3td column) in the last column,

Command: last -a

* To display full login and log out details,

Command: last -F

* To display specific user related information,
* Command: last <username>

Example: last vbhv

* To display last reboot information,

Command: last reboot

* To display specific terminal related information,
* Command: last <tty count>

Example: last tty6

* To parse details from other than /var/log/wtmp file,

Command: last -f <filename with absolute path>

* To display state of logins at specific time,

Command: last -t YYYYMMDDHHMMSS

* To display only hostname for remote users,

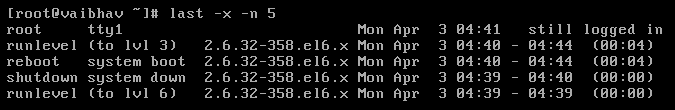
Command: last -d

* To display only IP addresses for remote users,

Command: last -i

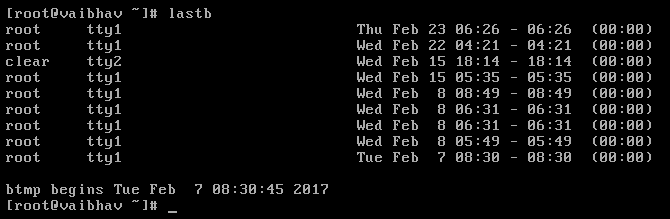
* To display rum level and shut down entry,

Command: last -x



# **Lastb Command: bad logins details**

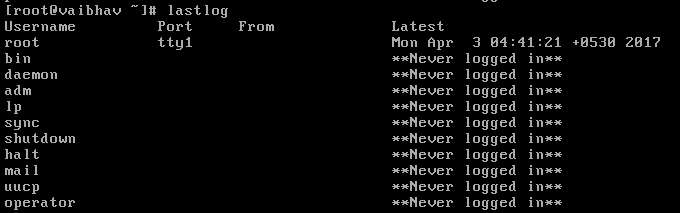
* It displays bad login attempts information.
* It retrieves information from /var/log/btmp file.
* File /var/log/btmp is rotated by logrotate utility. So we can get information from lastb command until this file is rotated.
* Command: lastb



* All options run for lastb as well which run for last command.

# **Lastlog command:**

* Lastlog command list out all users login details including users who have never logged in.
* Last command only displays successful login details whereas Lastlog command displays login details of recent successful login users, some system users’ login and users who never logged in as well.
* It retrieves information from /var/log/Lastlog file which is not rotated unlike /var/log/wtmp & /var/log/btmp files.
* Command: lastlog



* To display login details of specific users,

Command: lastlog -u <username>

* To display login details of specific users more recent than specific days,

Command: lastlog -t <count>

* To display login details of specific users older than specific days,

Command: lastlog -b <count>