root@kishori-virtual-machine:/var# cd /var/log

root@kishori-virtual-machine:/var/log# ls -l

total 6136

-rw-r--r-- 1 root root 29034 Sep 6 16:48 alternatives.log

-rw-r----- 1 root adm 0 Sep 8 16:25 apport.log

-rw-r----- 1 root adm 1748 Sep 7 17:53 apport.log.1

drwxr-xr-x 2 root root 4096 Sep 6 20:03 apt

-rw-r----- 1 syslog adm 63112 Sep 9 18:54 auth.log

-rw------- 1 root root 8687 Sep 9 18:45 boot.log

-rw------- 1 root root 27657 Sep 8 16:25 boot.log.1

-rw------- 1 root root 27109 Sep 7 17:47 boot.log.2

-rw-r--r-- 1 root root 108494 Aug 8 04:23 bootstrap.log

-rw-rw---- 1 root utmp 3072 Sep 3 15:40 btmp

drwxr-xr-x 2 root root 4096 Sep 9 10:07 cups

drwxr-xr-x 2 root root 4096 Aug 2 21:23 dist-upgrade

-rw-r----- 1 root adm 131147 Sep 9 18:45 dmesg

-rw-r----- 1 root adm 131651 Sep 7 19:10 dmesg.0

-rw-r----- 1 root adm 25082 Sep 7 17:56 dmesg.1.gz

-rw-r----- 1 root adm 25581 Sep 7 17:53 dmesg.2.gz

-rw-r----- 1 root adm 25698 Sep 7 17:47 dmesg.3.gz

-rw-r----- 1 root adm 25409 Sep 6 16:10 dmesg.4.gz

-rw-r--r-- 1 root root 1054552 Sep 6 20:04 dpkg.log

-rw-r--r-- 1 root root 32064 Sep 6 19:53 faillog

-rw-r--r-- 1 root root 11056 Sep 3 14:37 fontconfig.log

drwx--x--x 2 root gdm 4096 Sep 3 14:40 gdm3

-rw-r--r-- 1 root root 1297 Sep 9 18:45 gpu-manager.log

drwxr-xr-x 3 root root 4096 Aug 8 04:24 hp

drwxrwxr-x 2 root root 4096 Sep 3 14:39 installer

drwxr-sr-x+ 3 root systemd-journal 4096 Sep 3 14:40 journal

-rw-r----- 1 syslog adm 1342484 Sep 9 18:51 kern.log

-rw-rw-r-- 1 root utmp 292584 Sep 6 19:53 lastlog

drwxr-xr-x 2 root root 4096 Jul 14 2022 openvpn

drwx------ 2 root root 4096 Aug 8 04:22 private

drwx------ 2 speech-dispatcher root 4096 May 23 12:59 speech-dispatcher

-rw-r----- 1 syslog adm 3075030 Sep 9 18:53 syslog

-rw-r--r-- 1 root root 3171 Sep 9 11:17 ubuntu-advantage.log

drwxr-x--- 2 root adm 4096 Sep 6 16:46 unattended-upgrades

-rw-r--r-- 1 root root 217 Sep 7 17:47 vmware-network.1.log

-rw-r--r-- 1 root root 0 Sep 7 17:55 vmware-network.log

-rw------- 1 root root 4911 Sep 9 14:05 vmware-vmsvc-root.1.log

-rw------- 1 root root 1921 Sep 7 17:56 vmware-vmsvc-root.2.log

-rw------- 1 root root 2133 Sep 7 17:55 vmware-vmsvc-root.3.log

-rw------- 1 root root 1921 Sep 9 18:45 vmware-vmsvc-root.log

-rw------- 1 root root 3752 Sep 9 18:45 vmware-vmtoolsd-root.log

-rw-rw-r-- 1 root utmp 9984 Sep 9 18:51 wtmp

root@kishori-virtual-machine:/var/log# man last

root@kishori-virtual-machine:/var/log# last -s -5days -file -auth.log

last: invalid option -- 'u'

Try 'last --help' for more information.

root@kishori-virtual-machine:/var/log# last -s -5days -f auth.log

sudo:ses hori-virtual r user root(uid= Mon May 5 22:09 gone - no logout

kishori er:session): p 9 18:51:29 ki Tue Oct 29 10:02 gone - no logout

: stashe rtual-machin in open session

Sun Jul 13 13:38 gone - no logout

ect path me :1.38 [/u Kit1/Authenticat Sun Nov 16 01:35 gone - no logout

p 9 18: for user gd chine systemd-lo Tue Nov 25 22:22 gone - no logout

-machine at0.

Sep 9 tching system bu Fri Jan 6 21:21 gone - no logout

ix(su:se 4 kishori-vi or user root(uid Fri Jul 1 06:14 gone - no logout

ecret Se ne gnome-key lized

Sep 9 13: Sun Mar 25 12:27 gone - no logout

machine =0)

Sep 9 1 gnome-keyring-da Fri Nov 21 20:08 gone - no logout

kishori ater in open sword]: pam\_unix Mon Mar 17 11:01 gone - no logout

tication (authority=l c2 (system bus n Tue Oct 29 10:02 gone - no logout

12:30:01 session clos CRON[2870]: pam Thu May 8 23:10 gone - no logout

sion ope N[2835]: pam by (uid=0)

Sep Fri Nov 28 23:29 gone - no logout

root

Sep n:session): tual-machine CRO Sun Apr 6 08:03 gone - no logout

kishori- t(uid=0) by 9]: pam\_unix(cro Fri May 16 12:44 gone - no logout

ed for u pam\_unix(cro kishori-virtual Fri Feb 25 20:07 gone - no logout

hority=l kishori-vir entication Agent Sat Sep 27 15:21 gone - no logout

1 compon ome-keyring- zed

Sep 7 19:10 Fri Mar 30 00:49 gone - no logout

c1 (syst thentication bin/gnome-shell] Sun Jan 25 20:19 gone - no logout

): sessi \_unix(gdm-la id=128) by (uid= Sun Aug 15 16:09 gone - no logout

835]: Ne hori-virtual 10:19 kishori-vi Sun Jul 13 13:38 gone - no logout

-virtual ) by (uid=0) ty=local): Regis Mon Mar 17 11:01 gone - no logout

:51 kish 78]: Removed launch-environme Tue May 20 21:29 gone - no logout

: [syste ori-virtual- rvice 'org.bluez Sun Sep 10 00:38 gone - no logout

master p 836]: couldn PIN is incorrec Fri Nov 28 23:29 gone - no logout

by kisho session open 1 kishori-virtua Sun Mar 23 17:05 gone - no logout

tual-mac rom bus)

Sep Y=pts/0 ; PWD=/h Sat Jan 17 11:07 gone - no logout

Waiting -logind[778] Sep 7 18:27:19 Mon May 3 19:39 gone - no logout

led to a chine dbus-d ez': timed out ( Mon Feb 28 02:05 gone - no logout

ent, loc edesktop/Pol 05 kishori-virtu Tue Oct 29 10:58 gone - no logout

l file

S -pam: unable irtual-machine g Sat Dec 9 19:32 gone - no logout

udo: pam 7 18:17:28 k ession closed fo Tue Oct 29 10:58 gone - no logout

=root ; shori : TTY= 18:01:00 kishor Sun Aug 15 16:09 gone - no logout

sion c1 ual-machine processes to exi Thu May 8 22:07 gone - no logout

ep 7 17 rted properl achine gnome-key Tue Oct 9 11:32 gone - no logout

ate serv aemon[736]: ut (service\_star Sun Nov 3 08:07 gone - no logout

ching sy ual-machine ut/event1 (AT Tr Sun Sep 17 14:50 - 22:07 (963+07:17)

system b tication Age th /org/freedesk Sat Dec 11 07:22 gone - no logout

\_unix(gd machine gdm- sion): session c Thu Jan 15 09:17 gone - no logout

chine gn d

Sep 7 17: : The Secret Ser Tue Nov 25 22:22 gone - no logout

: /home/ n[1513]: Gkm ngs/login.keyrin Tue Oct 29 19:52 gone - no logout

md: pam\_ :53:06 kisho n): session open Sun Nov 16 01:34 gone - no logout

stemd-lo 17:53:05 ki em buttons on /d Wed Mar 28 08:18 gone - no logout

577]: [s ishori-virtu ] Failed to acti Fri May 28 19:21 gone - no logout

ile, dat 566]: Gkm: c nx/.local/share/ Sat Jan 10 02:03 gone - no logout

n contro rd]: gkr-pam ishori-virtual-m Thu Jan 15 09:17 gone - no logout

Agent f ty=local): R em bus name :1.3 Tue Nov 14 11:18 gone - no logout

shori : 14 kishori-v ers near line 1 Thu Apr 15 01:28 gone - no logout

ned for u: pam\_unix( (uid=0)

Sep 6 2 Mon May 19 13:04 gone - no logout

Sep 6 TTY=pts/1 ; l-machine sudo: Sun Sep 17 09:39 gone - no logout

0) by ro ): session o 0:11 kishori-vir Fri May 16 12:44 gone - no logout

osed for : pam\_unix(s 11 kishori-virtu Sun May 11 23:25 gone - no logout

ishori(u ion opened f shori-virtual-ma Wed Sep 4 04:50 gone - no logout

=0) by ( n): session 2 kishori-virtua Sun Jan 25 20:19 gone - no logout

n): sess l-machine su

Sep 6 22:08:10 Sun Jul 13 13:38 gone - no logout

0:55 kis =1001) by ki N[17569]: pam\_un Sat Dec 2 17:47 gone - no logout

virtual- ser=kishori

3 incorrect pas Fri Jan 23 00:11 gone - no logout

1 kishor oot(uid=0) b 7343]: pam\_unix( Fri Jan 23 00:11 gone - no logout

\_unix(su 58 kishori-v losed for user r Sat Aug 11 22:01 gone - no logout

ishori-v COMMAND=/bi \_unix(sudo-i:ses Mon May 19 13:04 gone - no logout

; USER= do: kishori

Sep 6 20:04:36 Thu Mar 22 11:47 gone - no logout

6 20:04: : session cl ne pkexec: pam\_u Wed Mar 28 08:18 gone - no logout

n closed do: pam\_unix :03:56 kishori-v Sun Jul 13 13:38 gone - no logout

-machine est'

Sep 6 inx' to shadow g Sat Sep 9 19:36 gone - no logout

: gkr-pa ishori-virtu g

Sep 6 19:53:2 Sun Aug 15 16:09 gone - no logout

on opene 6927]: pam\_u y (uid=0)

Sep 6 Mon Mar 17 14:05 gone - no logout

ame=test 16921]: grou 59 kishori-virtu Fri Mar 30 19:48 gone - no logout

pam\_uni :21:04 kisho on opened for us Sat Oct 30 00:03 gone - no logout

ine CRON Sep 6 19:05 ession): session Sun May 11 23:25 gone - no logout

by (uid session ope ori-virtual-mach Wed May 26 18:13 gone - no logout

Sep 6 1 for user ro machine pkexec[1 Fri Nov 28 23:29 gone - no logout

06 kisho t(uid=0) by c[9877]: kishori Sat Feb 13 14:50 gone - no logout

machine =0)

Sep 6 1 n:session): sess Mon Jan 19 23:48 gone - no logout

Sep 6 d for user r -machine CRON[26 Fri Jan 23 18:41 gone - no logout

machine 00)

Sep 6 1 xecuting command Thu Jan 15 09:17 gone - no logout

ting for ind[777]: Se 6 16:11:13 kish Tue Nov 25 22:22 gone - no logout

Authenti olkitd(autho ssion:2 (system Wed Oct 3 07:53 gone - no logout

virtual- ked keyring

emon[1490]: The Sat Jan 24 12:10 gone - no logout

: timed iled to acti ut=25000ms)

Sep Tue Aug 21 22:18 gone - no logout

pened fo nix(systemd- uid=0)

Sep 6 16 Sun Mar 25 12:27 gone - no logout

p 3 20: nd[765]: Sys chine sudo: pam\_ Wed Oct 3 07:53 gone - no logout

7:01 kis oot(uid=0) b N[3522]: pam\_uni Sun Sep 17 14:50 gone - no logout

1000 eui uthenticatio =kishori rhost= Fri Feb 25 20:07 gone - no logout

7 kishor isconnected aemon[720]: [sys Tue Dec 5 05:36 gone - no logout

ocal): R -virtual-mac Agent for unix- Sat Dec 9 01:03 gone - no logout

14:41:2 properly and e gnome-keyring- Tue Nov 25 22:23 gone - no logout

kishori( d:session): 3 14:41:20 kis Tue Aug 21 22:18 gone - no logout

ervice ' [720]: [syst ervice\_start\_tim Tue Oct 29 19:52 gone - no logout

ession): ine systemd: gdm(uid=128) by Wed Oct 3 07:53 gone - no logout

system achine syste ent1 (AT Transla Mon Jan 29 17:02 gone - no logout