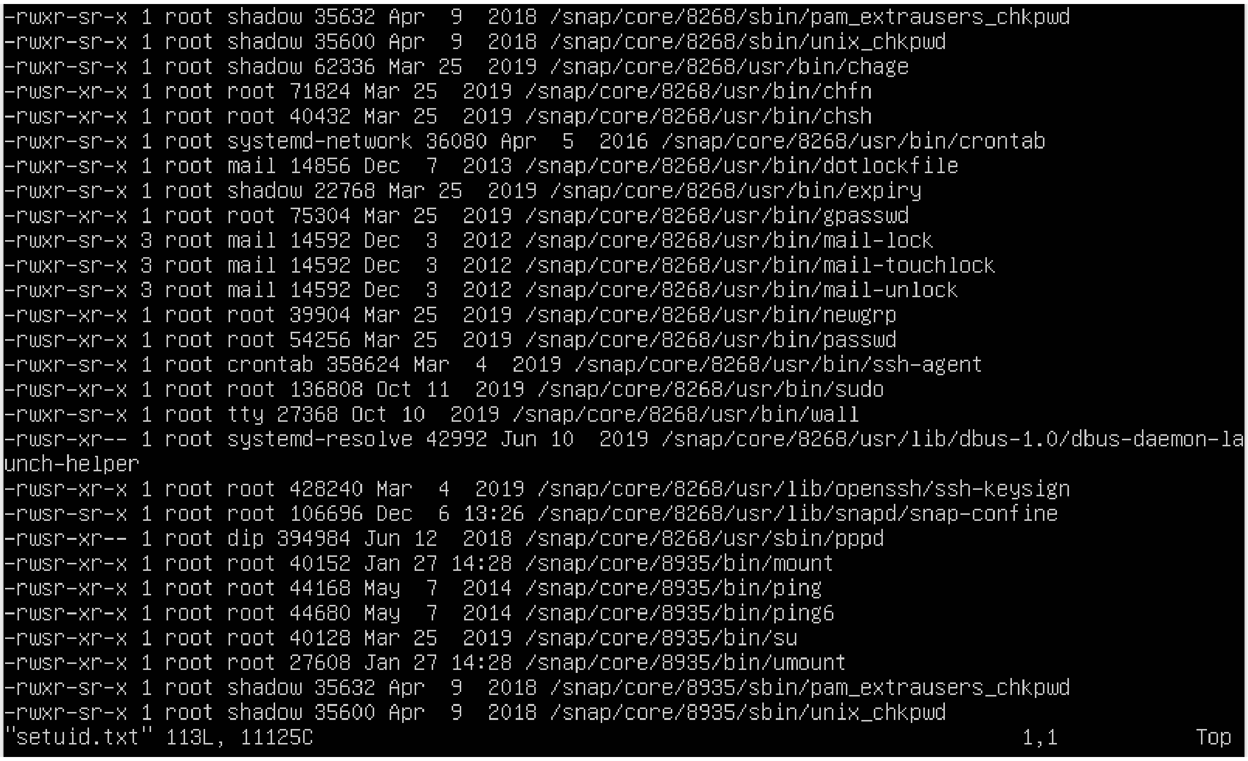
EPAM University Programs
DevOps external course
Module 4 Linux & Bash Essentials
TASK 4.5

1. To discover files with active sticky bits, use the following version of the **find** command:
sudo find / -perm /6000 -type f -exec ls -ld {} \;>setuid.txt
Put into your report a fragment of setuid.txt file. Explain meaning of parameters of the above **find** command (hint: use find’s man page).



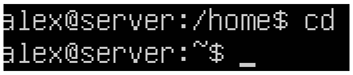
```
-rwxr-sr-x 1 root shadow 35632 Apr  9  2018 /snap/core/8268/sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root shadow 35600 Apr  9  2018 /snap/core/8268/sbin/unix_chkpwd
-rwxr-sr-x 1 root shadow 62336 Mar 25  2019 /snap/core/8268/usr/bin/chage
-rwsr-xr-x 1 root root 71824 Mar 25  2019 /snap/core/8268/usr/bin/chfn
-rwsr-xr-x 1 root root 40432 Mar 25  2019 /snap/core/8268/usr/bin/chsh
-rwxr-sr-x 1 root systemd-network 36080 Apr  5  2016 /snap/core/8268/usr/bin/crontab
-rwxr-sr-x 1 root mail 14856 Dec  7  2013 /snap/core/8268/usr/bin/dotlockfile
-rwxr-sr-x 1 root shadow 22768 Mar 25  2019 /snap/core/8268/usr/bin/expiry
-rwsr-xr-x 1 root root 75304 Mar 25  2019 /snap/core/8268/usr/bin/gpasswd
-rwxr-sr-x 3 root mail 14592 Dec  3  2012 /snap/core/8268/usr/bin/mail-lock
-rwxr-sr-x 3 root mail 14592 Dec  3  2012 /snap/core/8268/usr/bin/mail-touchlock
-rwxr-sr-x 3 root mail 14592 Dec  3  2012 /snap/core/8268/usr/bin/mail-unlock
-rwsr-xr-x 1 root root 39904 Mar 25  2019 /snap/core/8268/usr/bin/newgrp
-rwsr-xr-x 1 root root 54256 Mar 25  2019 /snap/core/8268/usr/bin/passwd
-rwxr-sr-x 1 root crontab 358624 Mar  4  2019 /snap/core/8268/usr/bin/ssh-agent
-rwsr-xr-x 1 root root 136808 Oct 11  2019 /snap/core/8268/usr/bin/sudo
-rwxr-sr-x 1 root tty 27368 Oct 10  2019 /snap/core/8268/usr/bin/wall
-rwsr-xr-- 1 root systemd-resolve 42992 Jun 10  2019 /snap/core/8268/usr/lib/dbus-1.0/dbus-daemon-la
unch-helper
-rwsr-xr-x 1 root root 428240 Mar  4  2019 /snap/core/8268/usr/lib/openssh/ssh-keysign
-rwsr-sr-x 1 root root 106696 Dec  6 13:26 /snap/core/8268/usr/lib/snapd/snap-confine
-rwsr-xr-- 1 root dip 394984 Jun 12  2018 /snap/core/8268/usr/sbin/pppd
-rwsr-xr-x 1 root root 40152 Jan 27 14:28 /snap/core/8935/bin/mount
-rwsr-xr-x 1 root root 44168 May  7  2014 /snap/core/8935/bin/ping
-rwsr-xr-x 1 root root 44680 May  7  2014 /snap/core/8935/bin/ping6
-rwsr-xr-x 1 root root 40128 Mar 25  2019 /snap/core/8935/bin/su
-rwsr-xr-x 1 root root 27608 Jan 27 14:28 /snap/core/8935/bin/umount
-rwxr-sr-x 1 root shadow 35632 Apr  9  2018 /snap/core/8935/sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root shadow 35600 Apr  9  2018 /snap/core/8935/sbin/unix_chkpwd
"setuid.txt" 113L, 11125C                                                      1,1          Top
```

Answer: In all directories of system find (**find /**) files with permissions setgid and setuid(**-perm /6000**). Find only files, not directories (**-type f**). With sorted files run command in directory, where we find files - / (**-exec ls –ld {}\;**). Save results of the command in file setuid.txt(**>setuid.txt**)

2. Discovering soft and hard links.

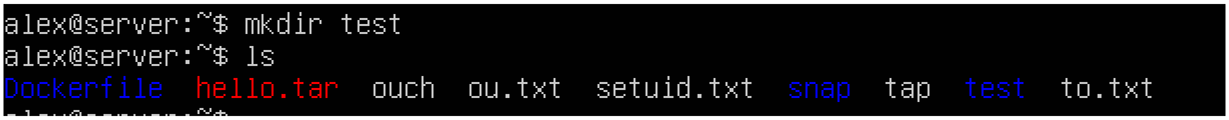
Comment on results of these commands (place the output into your report):

cd – change current directory to home directory of user alex



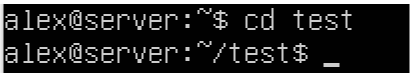
```
alex@server:/home$ cd
alex@server:~$ _
```

mkdir test – create directory test



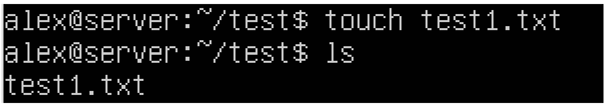
```
alex@server:~$ mkdir test
alex@server:~$ ls
Dockerfile  hello.tar  ouch  ou.txt  setuid.txt  snap  tap  test  to.txt
```

cd test – change current directory from /home/alex to ~/test



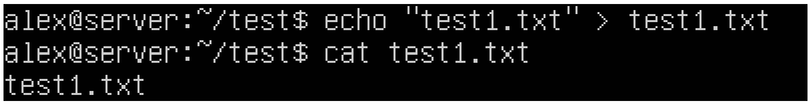
```
alex@server:~$ cd test
alex@server:~/test$ _
```

touch test1.txt – create a new empty file



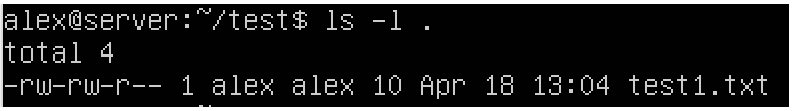
```
alex@server:~/test$ touch test1.txt
alex@server:~/test$ ls
test1.txt
```

echo “test1.txt” > test1.txt – save result of the echo “test1.txt” command to file test1.txt



```
alex@server:~/test$ echo "test1.txt" > test1.txt
alex@server:~/test$ cat test1.txt
test1.txt
```

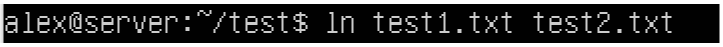
ls -l . – to list files of current directory in long



```
alex@server:~/test$ ls -l .
total 4
-rw-rw-r-- 1 alex alex 10 Apr 18 13:04 test1.txt
```

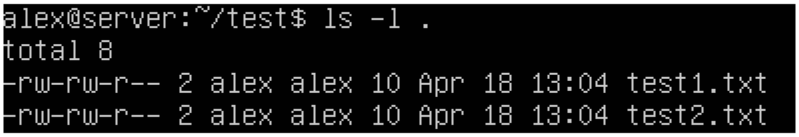
(a hard link) - 1

ln test1.txt test2.txt – create a hard link with name test2.txt of file test1.txt



```
alex@server:~/test$ ln test1.txt test2.txt
```

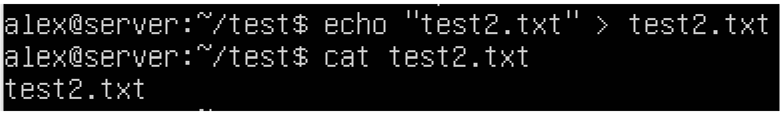
ls -l . - to list files of current directory in long



```
alex@server:~/test$ ls -l .
total 8
-rw-rw-r-- 2 alex alex 10 Apr 18 13:04 test1.txt
-rw-rw-r-- 2 alex alex 10 Apr 18 13:04 test2.txt
```

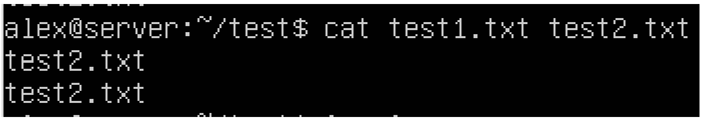
(pay attention to the number of links to test1.txt and test2.txt) - 2

echo “test2.txt” > test2.txt – save result of the echo “test2.txt” command to file test2.txt



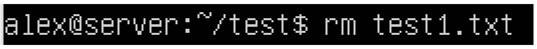
```
alex@server:~/test$ echo "test2.txt" > test2.txt
alex@server:~/test$ cat test2.txt
test2.txt
```

cat test1.txt test2.txt – to show info that contains in both files test1.txt and test2.txt



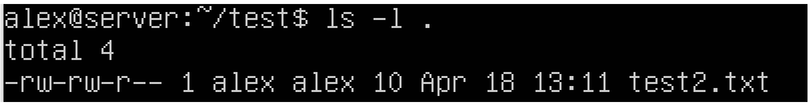
```
alex@server:~/test$ cat test1.txt test2.txt
test2.txt
test2.txt
```

rm test1.txt – to delete file test1.txt



```
alex@server:~/test$ rm test1.txt
```

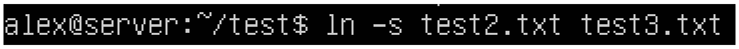
ls -l . – to list files of current directory in long



```
alex@server:~/test$ ls -l .
total 4
-rw-rw-r-- 1 alex alex 10 Apr 18 13:11 test2.txt
```

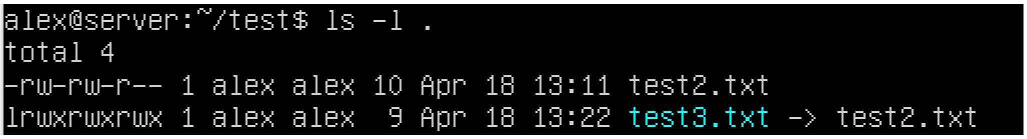
(now a soft link)

ln -s test2.txt test3.txt – to create a symbolic link test3.txt of file test2.txt



```
alex@server:~/test$ ln -s test2.txt test3.txt
```

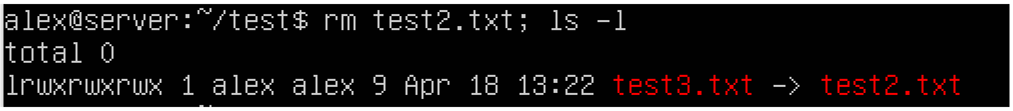
ls -l . – to list files of current directory in long



```
alex@server:~/test$ ls -l .
total 4
-rw-rw-r-- 1 alex alex 10 Apr 18 13:11 test2.txt
lrwxrwxrwx 1 alex alex  9 Apr 18 13:22 test3.txt -> test2.txt
```

(pay attention to the number of links to the created files) – both 1

rm test2.txt; **ls** -l . – to delete file test1.txt and after that list files of current directory in long

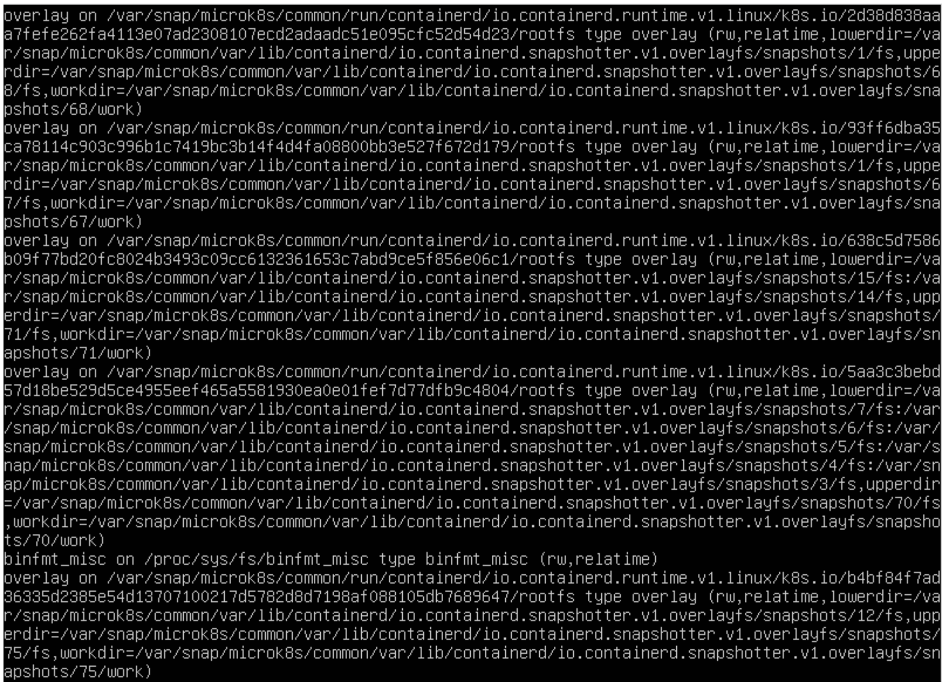


```
alex@server:~/test$ rm test2.txt; ls -l
total 0
lrwxrwxrwx 1 alex alex 9 Apr 18 13:22 test3.txt -> test2.txt
```

3. I/O redirect.

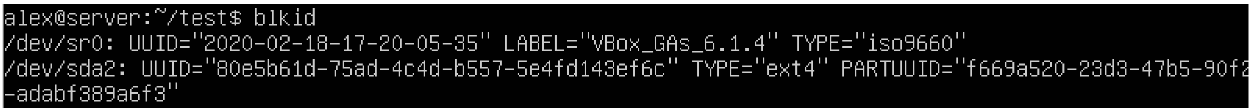
Execute these commands; comment on the output.

mount - to check status file system of OS



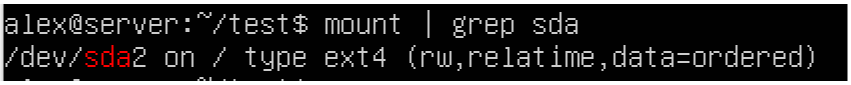
```
overlay on /var/snap/microk8s/common/run/containerd/io.containerd.runtime.v1.linux/k8s.io/2d38d838aa
a7fefe262fa4113e07ad2308107ecd2adaadc51e095cfc52d54d23/rootfs type overlay (rw,relatime,lowerdir=/va
r/snap/microk8s/common/var/lib/containerd/io.containerd.snapshotter.v1.overlayfs/snapshots/1/fs,uppe
rdir=/var/snap/microk8s/common/var/lib/containerd/io.containerd.snapshotter.v1.overlayfs/snapshots/6
8/fs,workdir=/var/snap/microk8s/common/var/lib/containerd/io.containerd.snapshotter.v1.overlayfs/sna
pshots/68/work)
overlay on /var/snap/microk8s/common/run/containerd/io.containerd.runtime.v1.linux/k8s.io/93ff6dba35
ca78114c903c996b1c7419bc3b14f4d4fa08800bb3e527f672d179/rootfs type overlay (rw,relatime,lowerdir=/va
r/snap/microk8s/common/var/lib/containerd/io.containerd.snapshotter.v1.overlayfs/snapshots/1/fs,uppe
rdir=/var/snap/microk8s/common/var/lib/containerd/io.containerd.snapshotter.v1.overlayfs/snapshots/6
7/fs,workdir=/var/snap/microk8s/common/var/lib/containerd/io.containerd.snapshotter.v1.overlayfs/sna
pshots/67/work)
overlay on /var/snap/microk8s/common/run/containerd/io.containerd.runtime.v1.linux/k8s.io/638c5d7586
b09f77bd20fc8024b3493c09cc6132361653c7abd9ce5f856e06c1/rootfs type overlay (rw,relatime,lowerdir=/va
r/snap/microk8s/common/var/lib/containerd/io.containerd.snapshotter.v1.overlayfs/snapshots/15/fs:/va
r/snap/microk8s/common/var/lib/containerd/io.containerd.snapshotter.v1.overlayfs/snapshots/14/fs,upp
erdir=/var/snap/microk8s/common/var/lib/containerd/io.containerd.snapshotter.v1.overlayfs/snapshots/
71/fs,workdir=/var/snap/microk8s/common/var/lib/containerd/io.containerd.snapshotter.v1.overlayfs/sn
apshots/71/work)
overlay on /var/snap/microk8s/common/run/containerd/io.containerd.runtime.v1.linux/k8s.io/5aa3c3bebd
57d18be529d5ce4955eef465a5581930ea0e01fef7d77dfb9c4804/rootfs type overlay (rw,relatime,lowerdir=/va
r/snap/microk8s/common/var/lib/containerd/io.containerd.snapshotter.v1.overlayfs/snapshots/7/fs:/var
/snap/microk8s/common/var/lib/containerd/io.containerd.snapshotter.v1.overlayfs/snapshots/6/fs:/var/
snap/microk8s/common/var/lib/containerd/io.containerd.snapshotter.v1.overlayfs/snapshots/5/fs:/var/s
nap/microk8s/common/var/lib/containerd/io.containerd.snapshotter.v1.overlayfs/snapshots/4/fs:/var/sn
ap/microk8s/common/var/lib/containerd/io.containerd.snapshotter.v1.overlayfs/snapshots/3/fs,upperdir
=/var/snap/microk8s/common/var/lib/containerd/io.containerd.snapshotter.v1.overlayfs/snapshots/70/fs
,workdir=/var/snap/microk8s/common/var/lib/containerd/io.containerd.snapshotter.v1.overlayfs/snapsho
ts/70/work)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,relatime)
overlay on /var/snap/microk8s/common/run/containerd/io.containerd.runtime.v1.linux/k8s.io/b4bf84f7ad
36335d2385e54d13707100217d5782d8d7198af088105db7689647/rootfs type overlay (rw,relatime,lowerdir=/va
r/snap/microk8s/common/var/lib/containerd/io.containerd.snapshotter.v1.overlayfs/snapshots/12/fs,upp
erdir=/var/snap/microk8s/common/var/lib/containerd/io.containerd.snapshotter.v1.overlayfs/snapshots/
75/fs,workdir=/var/snap/microk8s/common/var/lib/containerd/io.containerd.snapshotter.v1.overlayfs/sn
apshots/75/work)
```

blkid – to show list of devices that connected to the system and to know their names of file systems and identifications of UUID



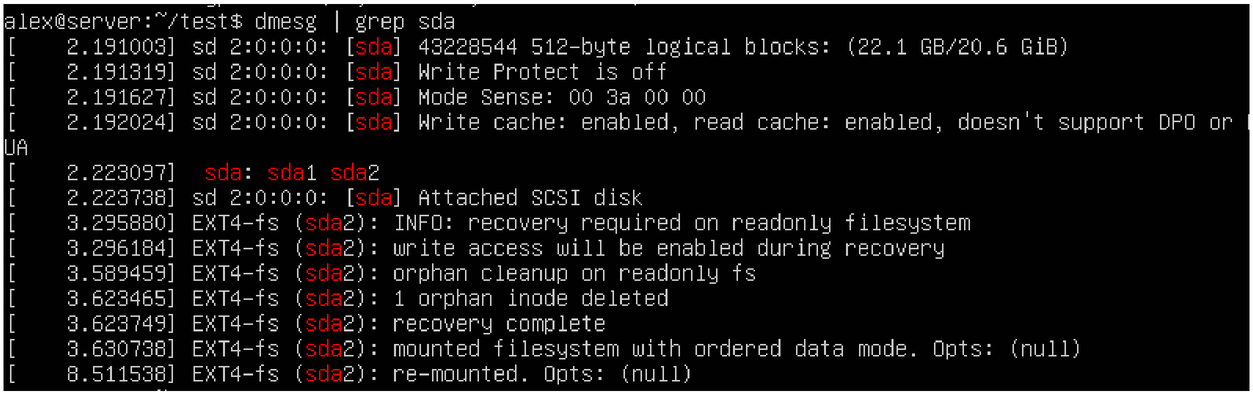
```
alex@server:~/test$ blkid
/dev/sr0: UUID="2020-02-18-17-20-05-35" LABEL="VBox_GAs_6.1.4" TYPE="iso9660"
/dev/sda2: UUID="80e5b61d-75ad-4c4d-b557-5e4fd143ef6c" TYPE="ext4" PARTUUID="f669a520-23d3-47b5-90f2
-adabf389a6f3"
```

mount | **grep** sda – to show status file system of system drive(sata, scsi, usb) my VM or PC



```
alex@server:~/test$ mount | grep sda
/dev/sda2 on / type ext4 (rw,relatime,data=ordered)
```

dmesg | **grep** sda - to show messages from kernel that have any connections to the any hard drive sda

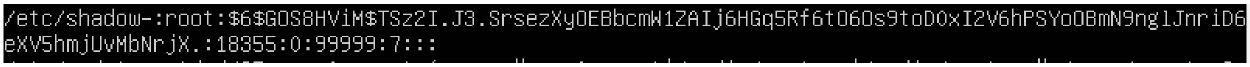


```
alex@server:~/test$ dmesg | grep sda
[    2.191003] sd 2:0:0:0: [sda] 43228544 512-byte logical blocks: (22.1 GB/20.6 GiB)
[    2.191319] sd 2:0:0:0: [sda] Write Protect is off
[    2.191627] sd 2:0:0:0: [sda] Mode Sense: 00 3a 00 00
[    2.192024] sd 2:0:0:0: [sda] Write cache: enabled, read cache: enabled, doesn't support DPO or 
UA
[    2.223097]  sda: sda1 sda2
[    2.223738] sd 2:0:0:0: [sda] Attached SCSI disk
[    3.295880] EXT4-fs (sda2): INFO: recovery required on readonly filesystem
[    3.296184] EXT4-fs (sda2): write access will be enabled during recovery
[    3.589459] EXT4-fs (sda2): orphan cleanup on readonly fs
[    3.623465] EXT4-fs (sda2): 1 orphan inode deleted
[    3.623749] EXT4-fs (sda2): recovery complete
[    3.630738] EXT4-fs (sda2): mounted filesystem with ordered data mode. Opts: (null)
[    8.511538] EXT4-fs (sda2): re-mounted. Opts: (null)
```

sudo grep -R -e “root” /etc > root_entries.txt

(place only a reasonable fragment of root_entries.txt into your report)

To find encrypted password of user root and to know time of last change to be sure that someone didn’t change password of the root user



```
/etc/shadow-:root:$6$GOS8HViM$TSz2I.J3.SrsezXyOEBbcmW1ZAIj6HGq5Rf6tO6Os9toDOxI2V6hPSYoOBmN9nglJnriD6
eXV5hmjUvMbNrjX.:18355:0:99999:7:::
```