EPAM University Programs
DevOps external course
Module 4 Linux & Bash Essentials
Найда Д.В.
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* – using this command we want to find files in root directory that have no permissions to read, write and execute either for user, or for group user, or other; then we execute *ls* command for directories where found matching files and then we make output in file setuid.txt

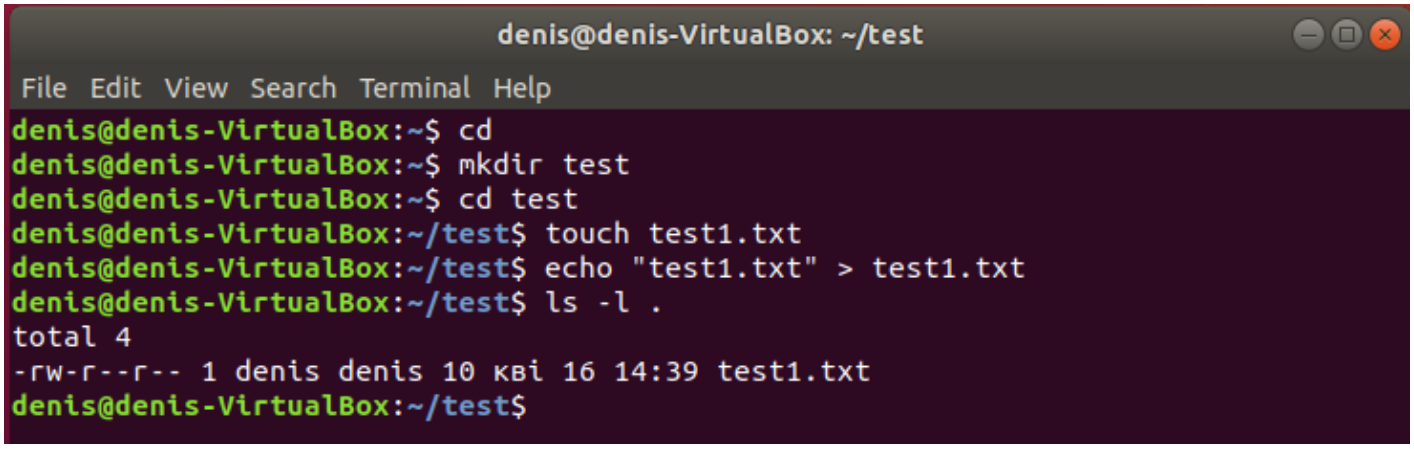
```
denis@denis-VirtualBox:~$ sudo find / -perm /6000 -type f -exec ls -ld {} \; > s
etuid.txt
find: ‘/proc/16329/task/16329/fdinfo/6’: No such file or directory
find: ‘/proc/16329/fdinfo/5’: No such file or directory
find: ‘/run/user/1000/gvfs’: Permission denied
```

Open ▾ | setuid.txt ~/ | Save

```
-rwsr-xr-x 1 root root 43088 бер  5 19:23 /bin/mount
-rwsr-xr-x 1 root root 26696 бер  5 19:23 /bin/umount
-rwsr-xr-x 1 root root 64424 чер 28  2019 /bin/ping
-rwsr-xr-x 1 root root 30800 сер 11  2016 /bin/fusermount
-rwsr-xr-x 1 root root 44664 бер 22  2019 /bin/su
-rwsr-xr-x 1 root root 43088 січ  8 20:31 /snap/core18/1705/bin/mount
-rwsr-xr-x 1 root root 64424 чер 28  2019 /snap/core18/1705/bin/ping
-rwsr-xr-x 1 root root 44664 бер 22  2019 /snap/core18/1705/bin/su
-rwsr-xr-x 1 root root 26696 січ  8 20:31 /snap/core18/1705/bin/umount
-rwxr-sr-x 1 root shadow 34816 лют 27  2019 /snap/core18/1705/sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root shadow 34816 лют 27  2019 /snap/core18/1705/sbin/unix_chkpwd
-rwxr-sr-x 1 root shadow 71816 бер 22  2019 /snap/core18/1705/usr/bin/chage
-rwsr-xr-x 1 root root 76496 бер 22  2019 /snap/core18/1705/usr/bin/chfn
-rwsr-xr-x 1 root root 44528 бер 22  2019 /snap/core18/1705/usr/bin/chsh
-rwxr-sr-x 1 root shadow 22808 бер 22  2019 /snap/core18/1705/usr/bin/expiry
-rwsr-xr-x 1 root root 75824 бер 22  2019 /snap/core18/1705/usr/bin/gpasswd
-rwsr-xr-x 1 root root 40344 бер 22  2019 /snap/core18/1705/usr/bin/newgrp
-rwsr-xr-x 1 root root 59640 бер 22  2019 /snap/core18/1705/usr/bin/passwd
```

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).

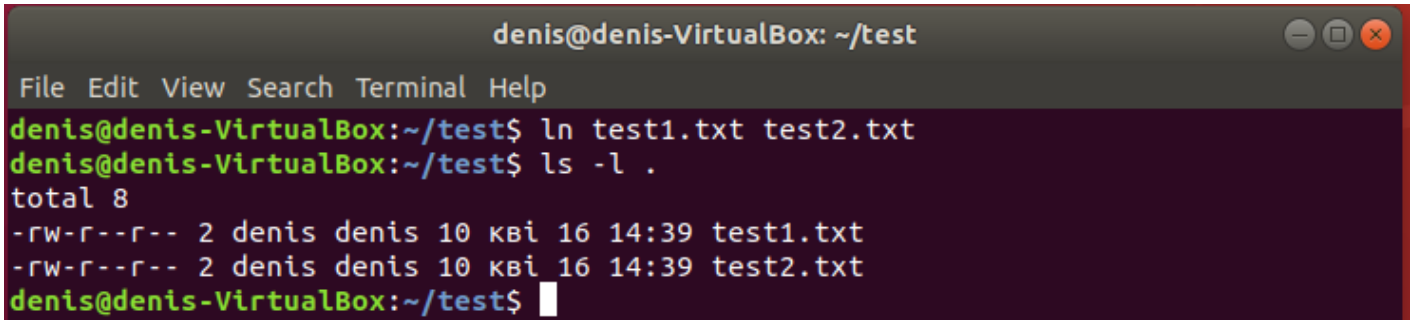
2. Discovering soft and hard links.
Comment on results of these commands (place the output into your report):
cd – changes current directory to *home* directory
mkdir test – creates *test* directory in current directory
cd test – changes current directory to *test* directory
touch test1.txt – creates empty file test1.txt in current directory
echo “test1.txt” > test1.txt – outputs the text *test1.txt* in file test1.txt
ls -l . – shows long information about current directory



(a hard link)

ln test1.txt test2.txt – makes a hard link *test2.txt* that refers to file *test1.txt* and content of both files will be the same even if one of them will be changed

ls -l . – shows long information about current directory



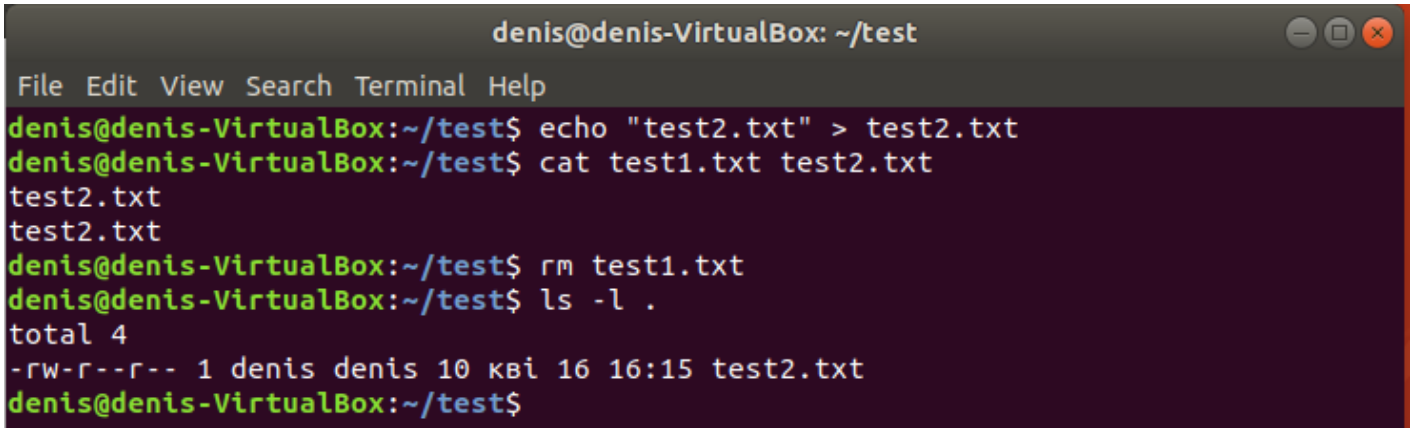
(pay attention to the number of links to test1.txt and test2.txt)

echo “test2.txt” > test2.txt - outputs the text *test2.txt* in file test2.txt

cat test1.txt test2.txt – displays content of the both files test1.txt and test2.txt

rm test1.txt – removes file test1.txt

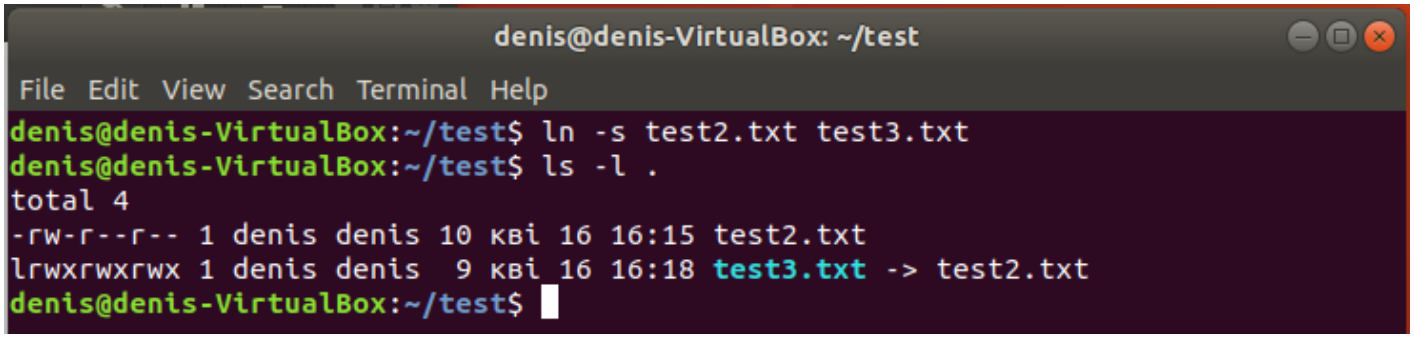
ls -l . – shows long information about current directory



(now a soft link)

ln -s test2.txt test3.txt – creates soft link test3.txt that refers to file test2.txt, number of links stays

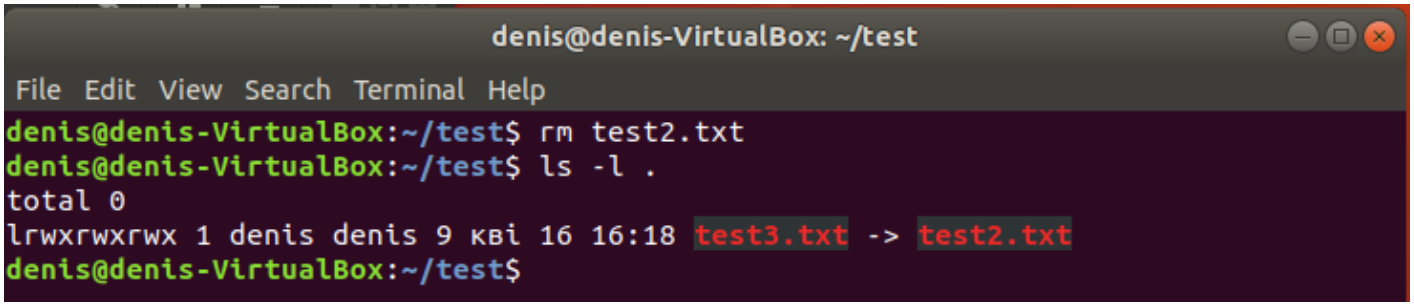
ls -l . – shows long information about current directory



(pay attention to the number of links to the created files)

rm test2.txt – removes file test2.txt

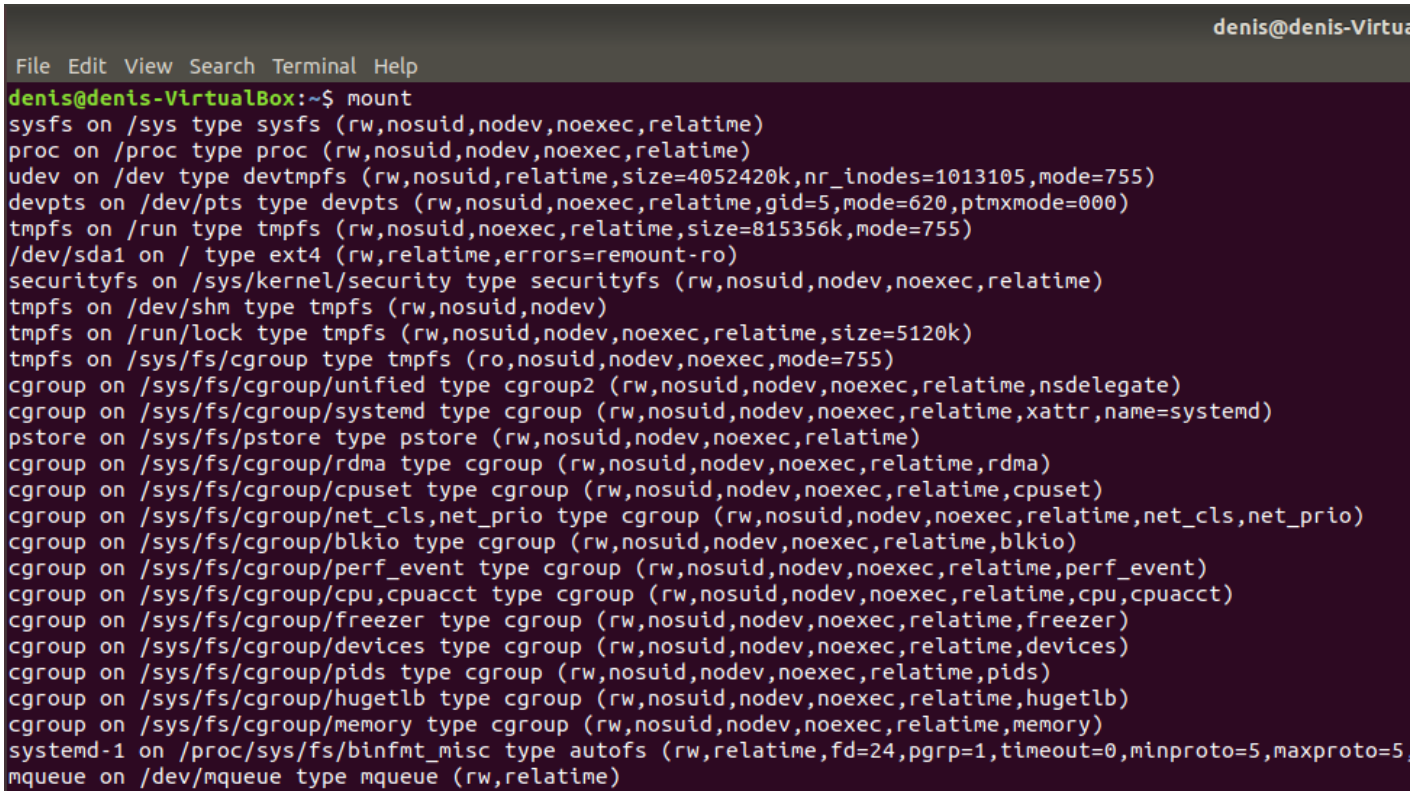
ls -l . – shows long information about current directory; test3.txt became unreadable because of deletion of the original file



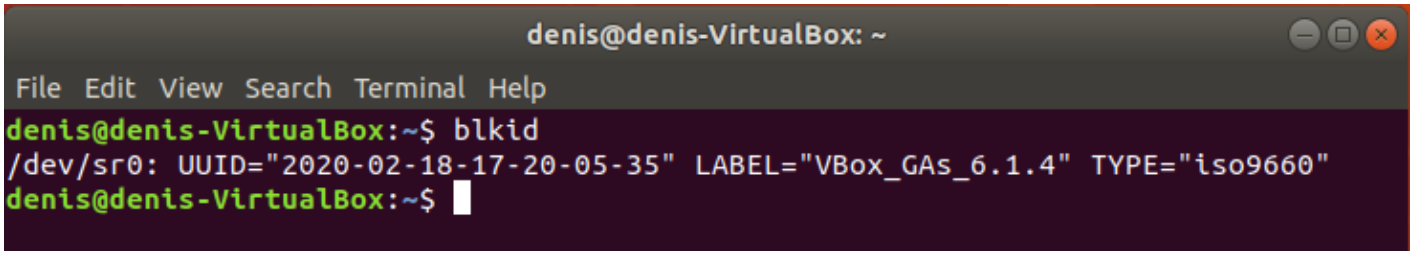
3. I/O redirect.

Execute these commands; comment on the output.

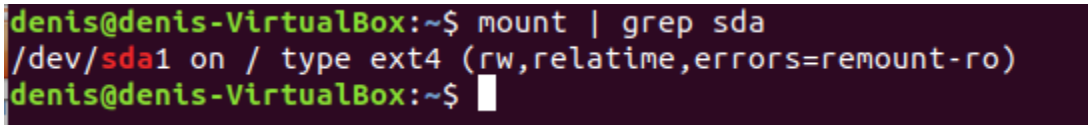
mount – displays the information about current file system



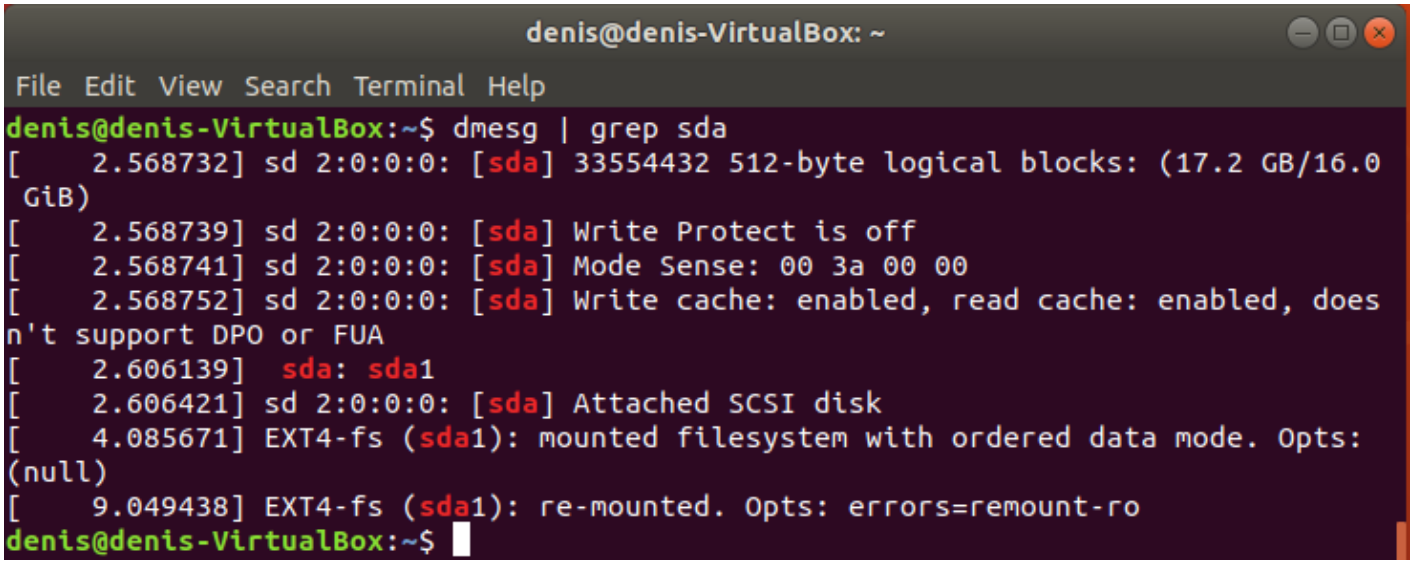
blkid – displays the list of devices, their UUID, type of the file system



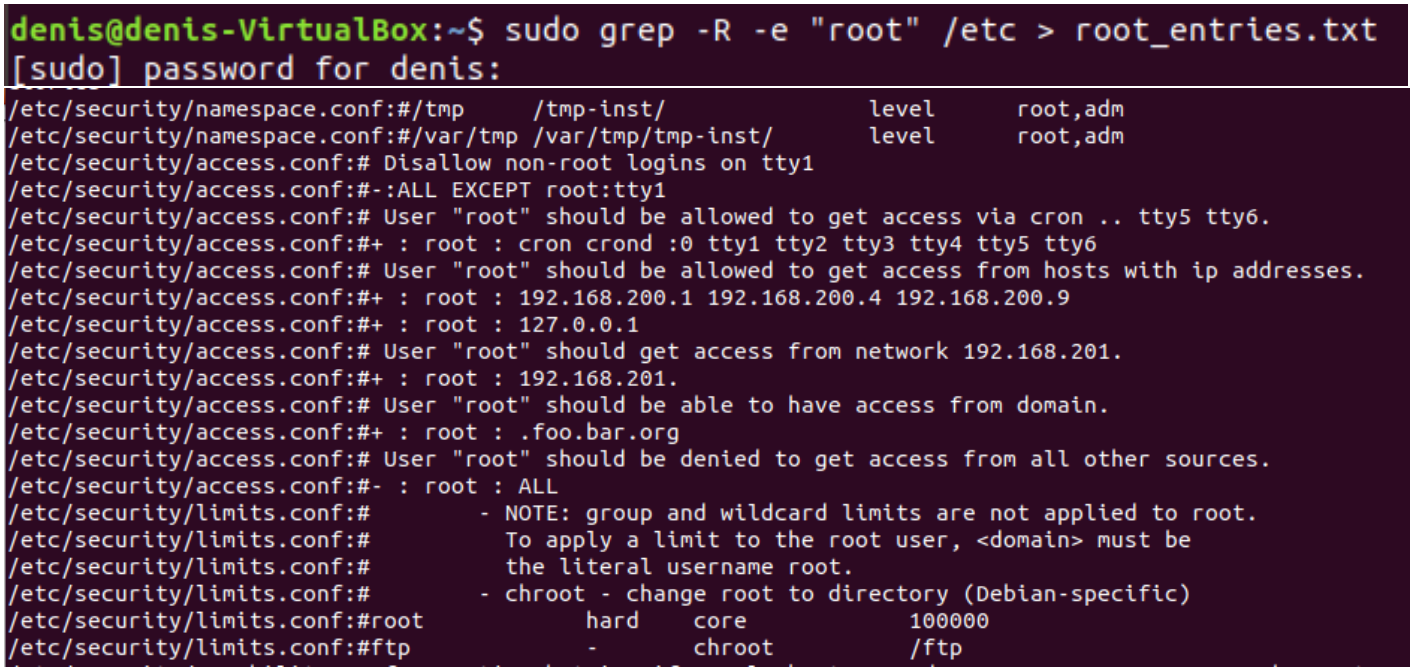
mount | **grep** sda - displays the information about current file system and then finds matches in it using text “sda”, that allows to see information about first hard disk detected



dmesg | **grep** sda – displays the information about all devices that were detected by kernel and then finds matches in it using text “sda”, that allows to see information about first hard disk



sudo grep -R -e “root” /etc > root_entries.txt – displays all entries of text “root” in /etc directory and all it’s subdirectories (-R allows to find entries recursively following all symlinks and -e means that “root” must be used only like example for search)



This fragment of root_entries.txt shows what permissions have root users, for example what virtual terminals can be used. Also, it shows information about request limits – for root users they are not applied.

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