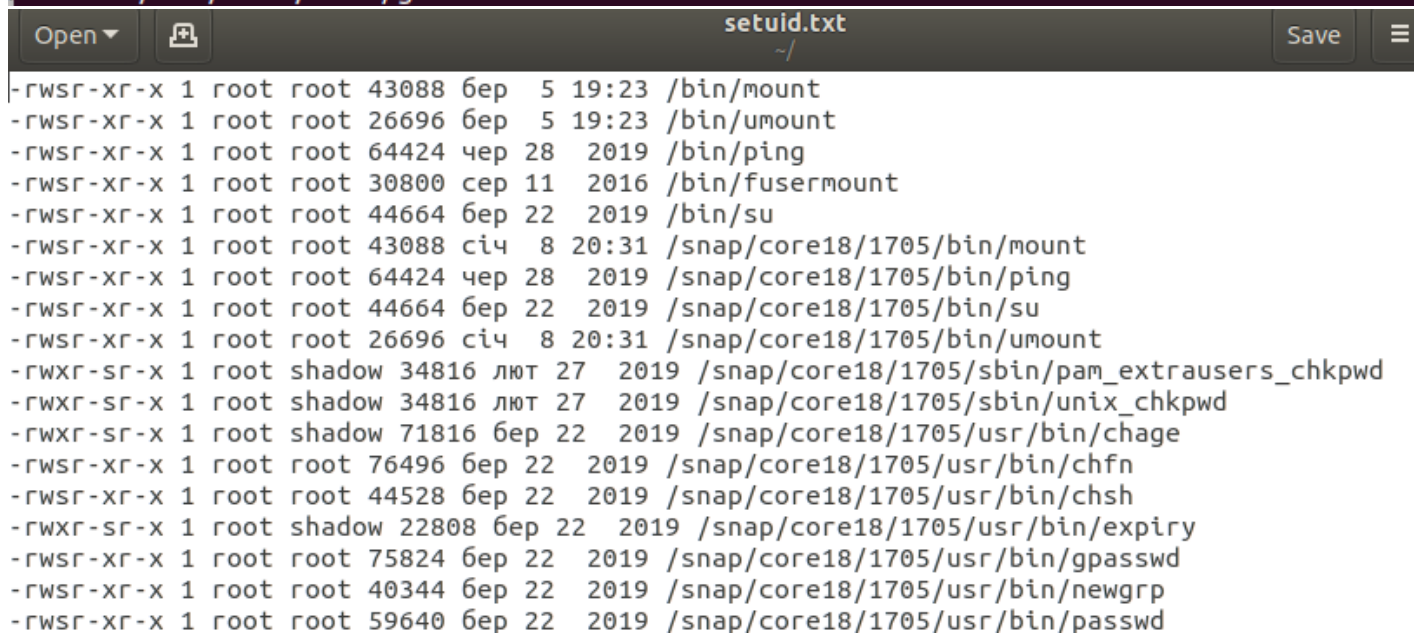


1. To discover files with active sticky bits, use the following version of the **find** command:  
**sudo find / -perm /6000 -type f -exec ls -ld {} \;** > **setuid.txt** – using this command we want to find files in root directory that have no permissions to read, write and execute either for user, 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
```



```
-rwxr-xr-x 1 root root 43088 беп 5 19:23 /bin/mount
-rwxr-xr-x 1 root root 26696 беп 5 19:23 /bin/umount
-rwxr-xr-x 1 root root 64424 чеп 28 2019 /bin/ping
-rwxr-xr-x 1 root root 30800 чеп 11 2016 /bin/fusermount
-rwxr-xr-x 1 root root 44664 беп 22 2019 /bin/su
-rwxr-xr-x 1 root root 43088 ciч 8 20:31 /snap/core18/1705/bin/mount
-rwxr-xr-x 1 root root 64424 чеп 28 2019 /snap/core18/1705/bin/ping
-rwxr-xr-x 1 root root 44664 беп 22 2019 /snap/core18/1705/bin/su
-rwxr-xr-x 1 root root 26696 ciч 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 беп 22 2019 /snap/core18/1705/usr/bin/chage
-rwxr-xr-x 1 root root 76496 беп 22 2019 /snap/core18/1705/usr/bin/chfn
-rwxr-xr-x 1 root root 44528 беп 22 2019 /snap/core18/1705/usr/bin/chsh
-rwxr-sr-x 1 root shadow 22808 беп 22 2019 /snap/core18/1705/usr/bin/expiry
-rwxr-xr-x 1 root root 75824 беп 22 2019 /snap/core18/1705/usr/bin/gpasswd
-rwxr-xr-x 1 root root 40344 беп 22 2019 /snap/core18/1705/usr/bin/newgrp
-rwxr-xr-x 1 root root 59640 беп 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

```
denis@denis-VirtualBox: ~/test
File Edit View Search Terminal Help
denis@denis-VirtualBox:~$ cd
denis@denis-VirtualBox:~$ mkdir test
denis@denis-VirtualBox:~$ cd test
denis@denis-VirtualBox:~/test$ touch test1.txt
denis@denis-VirtualBox:~/test$ echo "test1.txt" > test1.txt
denis@denis-VirtualBox:~/test$ ls -l .
total 4
-rw-r--r-- 1 denis denis 10 Kbi 16 14:39 test1.txt
denis@denis-VirtualBox:~/test$
```

(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

```
denis@denis-VirtualBox: ~/test
File Edit View Search Terminal Help
denis@denis-VirtualBox:~/test$ ln test1.txt test2.txt
denis@denis-VirtualBox:~/test$ ls -l .
total 8
-rw-r--r-- 2 denis denis 10 Kbi 16 14:39 test1.txt
-rw-r--r-- 2 denis denis 10 Kbi 16 14:39 test2.txt
denis@denis-VirtualBox:~/test$
```

(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

```
denis@denis-VirtualBox: ~/test
File Edit View Search Terminal Help
denis@denis-VirtualBox:~/test$ echo "test2.txt" > test2.txt
denis@denis-VirtualBox:~/test$ cat test1.txt test2.txt
test2.txt
test2.txt
denis@denis-VirtualBox:~/test$ rm test1.txt
denis@denis-VirtualBox:~/test$ ls -l .
total 4
-rw-r--r-- 1 denis denis 10 Kbi 16 16:15 test2.txt
denis@denis-VirtualBox:~/test$
```

*(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

```
denis@denis-VirtualBox: ~/test
File Edit View Search Terminal Help
denis@denis-VirtualBox:~/test$ ln -s test2.txt test3.txt
denis@denis-VirtualBox:~/test$ ls -l .
total 4
-rw-r--r-- 1 denis denis 10 kbi 16 16:15 test2.txt
lrwxrwxrwx 1 denis denis 9 kbi 16 16:18 test3.txt -> test2.txt
denis@denis-VirtualBox:~/test$
```

*(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

```
denis@denis-VirtualBox: ~/test
File Edit View Search Terminal Help
denis@denis-VirtualBox:~/test$ rm test2.txt
denis@denis-VirtualBox:~/test$ ls -l .
total 0
lrwxrwxrwx 1 denis denis 9 kbi 16 16:18 test3.txt -> test2.txt
denis@denis-VirtualBox:~/test$
```

### 3. I/O redirect.

Execute these commands; comment on the output.

**mount** – displays the information about current file system

```
denis@denis-VirtualBox:~$ mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,nosuid,relatime,size=4052420k,nr_inodes=1013105,mode=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,noexec,relatime,size=815356k,mode=755)
/dev/sda1 on / type ext4 (rw,relatime,errors=remount-ro)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup on /sys/fs/cgroup/unified type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,name=systemd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
cgroup on /sys/fs/cgroup/rdma type cgroup (rw,nosuid,nodev,noexec,relatime,rdma)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls,net_prio)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugetlb)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=24,pgrp=1,timeout=0,minproto=5,maxproto=5)
mqueue on /dev/mqueue type mqueue (rw,relatime)
```

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

```
denis@denis-VirtualBox: ~
File Edit View Search Terminal Help
denis@denis-VirtualBox:~$ blkid
/dev/sr0: UUID="2020-02-18-17-20-05-35" LABEL="VBox_GAs_6.1.4" TYPE="iso9660"
denis@denis-VirtualBox:~$
```

**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

```
denis@denis-VirtualBox:~$ mount | grep sda
/dev/sda1 on / type ext4 (rw,relatime,errors=remount-ro)
denis@denis-VirtualBox:~$
```

**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

```
denis@denis-VirtualBox: ~
File Edit View Search Terminal Help
denis@denis-VirtualBox:~$ dmesg | grep sda
[  2.568732] sd 2:0:0:0: [sda] 33554432 512-byte logical blocks: (17.2 GB/16.0 GiB)
[  2.568739] sd 2:0:0:0: [sda] Write Protect is off
[  2.568741] sd 2:0:0:0: [sda] Mode Sense: 00 3a 00 00
[  2.568752] sd 2:0:0:0: [sda] Write cache: enabled, read cache: enabled, does n't support DPO or FUA
[  2.606139] sda: sda1
[  2.606421] sd 2:0:0:0: [sda] Attached SCSI disk
[  4.085671] EXT4-fs (sda1): mounted filesystem with ordered data mode. Opts: (null)
[  9.049438] EXT4-fs (sda1): re-mounted. Opts: errors=remount-ro
denis@denis-VirtualBox:~$
```

**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)

```
denis@denis-VirtualBox:~$ sudo grep -R -e "root" /etc > root_entries.txt
[sudo] password for denis:
/etc/security/namespace.conf:#/tmp /tmp-inst/ level root,adm
/etc/security/namespace.conf:#/var/tmp /var/tmp/tmp-inst/ level root,adm
/etc/security/access.conf:# Disallow non-root logins on tty1
/etc/security/access.conf:#-:ALL EXCEPT root:tty1
/etc/security/access.conf:# User "root" should be allowed to get access via cron .. tty5 tty6.
/etc/security/access.conf:#+ : root : cron crond :0 tty1 tty2 tty3 tty4 tty5 tty6
/etc/security/access.conf:# User "root" should be allowed to get access from hosts with ip addresses.
/etc/security/access.conf:#+ : root : 192.168.200.1 192.168.200.4 192.168.200.9
/etc/security/access.conf:#+ : root : 127.0.0.1
/etc/security/access.conf:# User "root" should get access from network 192.168.201.
/etc/security/access.conf:#+ : root : 192.168.201.
/etc/security/access.conf:# User "root" should be able to have access from domain.
/etc/security/access.conf:#+ : root : .foo.bar.org
/etc/security/access.conf:# User "root" should be denied to get access from all other sources.
/etc/security/access.conf:#- : root : ALL
/etc/security/limits.conf:# - NOTE: group and wildcard limits are not applied to root.
/etc/security/limits.conf:# To apply a limit to the root user, <domain> must be
/etc/security/limits.conf:# the literal username root.
/etc/security/limits.conf:# - chroot - change root to directory (Debian-specific)
/etc/security/limits.conf:#root hard core 100000
/etc/security/limits.conf:#ftp - chroot /ftp
```

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)*