Homework 4.5
by Alexander Krupskiy

```
ak@ubuntu01:~$ sudo find / -perm /6000 -type f -exec ls -ld {} \;>setuid.txt
[sudo] password for ak:
find: ‘/proc/1945/task/1945/fdinfo/6’: No such file or directory
find: ‘/proc/1945/fdinfo/5’: No such file or directory
ak@ubuntu01:~$ cat ./setuid.txt
-rwsr-xr-x 1 root root 22520 Mar 27  2019 /usr/bin/pkexec
-rwxr-sr-x 1 root tty 14328 Jan 17  2018 /usr/bin/bsd-write
-rwxr-sr-x 1 root tty 30800 Mar  5 19:23 /usr/bin/wall
-rwsr-xr-x 1 root root 76496 Mar 22  2019 /usr/bin/chfn
-rwsr-xr-x 1 root root 44528 Mar 22  2019 /usr/bin/chsh
-rwxr-sr-x 1 root ssh 362640 Mar  4  2019 /usr/bin/ssh-agent
-rwsr-xr-x 1 root root 75824 Mar 22  2019 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 18448 Jun 28  2019 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 40344 Mar 22  2019 /usr/bin/newgrp
-rwsr-sr-x 1 daemon daemon 51464 Feb 20  2018 /usr/bin/at
-rwsr-xr-x 1 root root 37136 Mar 22  2019 /usr/bin/newuidmap
-rwsr-xr-x 1 root root 59640 Mar 22  2019 /usr/bin/passwd
-rwxr-sr-x 1 root shadow 71816 Mar 22  2019 /usr/bin/chage
-rwsr-xr-x 1 root root 37136 Mar 22  2019 /usr/bin/newgidmap
-rwsr-xr-x 1 root root 149080 Jan 31 19:18 /usr/bin/sudo
-rwxr-sr-x 1 root mlocate 43088 Mar  1  2018 /usr/bin/mlocate
-rwxr-sr-x 1 root crontab 39352 Nov 16  2017 /usr/bin/crontab
-rwxr-sr-x 1 root shadow 22808 Mar 22  2019 /usr/bin/expiry
-rwsr-xr-x 1 root root 100760 Nov 23  2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
-rwxr-sr-x 1 root utmp 10232 Mar 11  2016 /usr/lib/x86_64-linux-gnu/utempter/utempter
-rwsr-xr-x 1 root root 10232 Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-sr-x 1 root root 109432 Oct 30 14:17 /usr/lib/snapd/snap-confine
-rwxr-sr-x 1 root tty 10232 Aug  5  2017 /usr/lib/mc/cons.saver
-rwsr-xr-x 1 root root 14328 Mar 27  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 436552 Mar  4  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-- 1 root messagebus 42992 Jun 10  2019 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 30800 Aug 11  2016 /bin/fusermount
-rwsr-xr-x 1 root root 64424 Jun 28  2019 /bin/ping
-rwsr-xr-x 1 root root 44664 Mar 22  2019 /bin/su
-rwsr-xr-x 1 root root 26696 Mar  5 19:23 /bin/umount
-rwsr-xr-x 1 root root 43088 Mar  5 19:23 /bin/mount
-rwxr-sr-x 1 root shadow 34816 Feb 27  2019 /sbin/unix_chkpwd
-rwxr-sr-x 1 root shadow 34816 Feb 27  2019 /sbin/pam_extrausers_chkpwd
```

Explanation of the output of `find` command: find all elements that match ‘regular file’ type that allow execute it with privileges of owning user or group under the ‘/’ directory and then execute `ls -ld` command on each find entry. As we search only ‘regular file’ type, so the command `ls -l` gives the same execution result.

```
ak@ubuntu01:~$ cd
```
#Change the current directory to $HOME variable value.

```
ak@ubuntu01:~$ mkdir test
```
#Create new ‘test’ directory at current directory location.

```
ak@ubuntu01:~$ cd test
```
#Change current directory to ‘test’ directory.

```
ak@ubuntu01:~/test$ touch test1.txt
```
#Create new file named ‘test1.txt’ at the current directory.

```
ak@ubuntu01:~/test$ echo “test1.txt” > test1.txt
```
#Echo value ‘test1.txt’ to file ‘test1.txt’ at the current directory.

```
ak@ubuntu01:~/test$ ls -l .
total 4
-rw-rw-r-- 1 ak ak 16 Apr 20 15:36 test1.txt
```
#List info about the files in the current directory.

```
ak@ubuntu01:~/test$ ln test1.txt test2.txt
```
#Create a ‘hard link’ named ‘test2.txt’ to file named ‘test1.txt’ at the current directory.

```
ak@ubuntu01:~/test$ ls -l .
total 8
-rw-rw-r-- 2 ak ak 16 Apr 20 15:36 test1.txt
-rw-rw-r-- 2 ak ak 16 Apr 20 15:36 test2.txt
```
#List info about the files in the current directory. As we can see there is two files that have ‘hard link count’ set to value of ‘2’ (after the access attributes). Each hard linked file is assigned the same Inode value as the original, therefore they reference the same physical file location. Hard links remain linked even if the original or linked files are moved throughout the file system, although hard links are unable to cross different file systems.

```
ak@ubuntu01:~/test$ echo “test2.txt” > test2.txt
```
#Echo value ‘test2.txt’ to file ‘test2.txt’ that was hardlinked with the file ‘test1.txt’.

```
ak@ubuntu01:~/test$ cat test1.txt test2.txt
“test2.txt”
“test2.txt”
```
#As hardlinked files have actual file contents, we can see the same output of ‘test1.txt’ and ‘test2.txt’ files.

```
ak@ubuntu01:~/test$ rm test1.txt
```
#Delete ‘test1.txt’ file from current directory.

```
ak@ubuntu01:~/test$ ls -l .
total 4
-rw-rw-r-- 1 ak ak 16 Apr 20 15:39 test2.txt
```
#List info about the files in the current directory. As we can see the counter of hard link is decreased, because we have removed one of the hardlinked files.

```
ak@ubuntu01:~/test$ ln -s test2.txt test3.txt
```
#Create a ‘soft link’ named ‘test3.txt’ to the file ‘test2.txt’ at the current directory.

```
ak@ubuntu01:~/test$ ls -l .
total 4
-rw-rw-r-- 1 ak ak 16 Apr 20 15:39 test2.txt
lrwxrwxrwx 1 ak ak  9 Apr 20 15:41 test3.txt -> test2.txt
```
#List info about the files in the current directory. As we can see ‘test3.txt’ entry is a soft link to the file ‘test2.txt’. The ‘l’ access attribute and the graphical output show that fact.

```
ak@ubuntu01:~/test$ rm test2.txt; ls -l .
total 0
lrwxrwxrwx 1 ak ak 9 Apr 20 15:41 test3.txt -> test2.txt
```
#Delete file ‘test2.txt’ from the current directory and then list info about the files in the current directory. As we can see the soft link is still remains, but it linked to nonexistent file ‘test2.txt’.

```
ak@ubuntu01:~/test$ 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=472828k,nr_inodes=118207,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=100884k,mode=755)
/dev/sda2 on / type ext4 (rw,relatime,errors=remount-ro,data=ordered)
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)
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/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
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/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
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/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/rdma type cgroup (rw,nosuid,nodev,noexec,relatime,rdma)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs
(rw,relatime,fd=25,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=13561)
mqueue on /dev/mqueue type mqueue (rw,relatime)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,pagesize=2M)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
fusectl on /sys/fs/fuse/connections type fusectl (rw,relatime)
configfs on /sys/kernel/config type configfs (rw,relatime)
/dev/sda1 on /boot type ext4 (rw,relatime,data=ordered)
lxcfs on /var/lib/lxcfs type fuse.lxcfs
(rw,nosuid,nodev,relatime,user_id=0,group_id=0,allow_other)
tmpfs on /run/user/1000 type tmpfs
(rw,nosuid,nodev,relatime,size=100880k,mode=700,uid=1000,gid=1000)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,relatime)
tracefs on /sys/kernel/debug/tracing type tracefs (rw,relatime)
```

‘mount’ command serves to attach the filesystem found on some device to the big file tree. If the ‘mount’ command executes without any parameter, it lists all mounted filesystems. For example we can see that filesystem from ‘/dev/sda1’ block device is ‘ext4’ type and mounted under the ‘/boot’ directory with ‘rw’ attributes, filesystem from ‘/dev/sda2’ block device is also ‘etx4’ and mounted under the root directory (‘/’) with ‘rw’ attributes.

```
root@ubuntu01:~# blkid
/dev/sda1: UUID="b69cb2c0-8a9b-4be3-aab6-992d5ed28ca4" TYPE="ext4" PARTUUID="4e084d54-01"
/dev/sda2: UUID="5d691983-9cfb-4c67-b36b-6583dcd76ce3" TYPE="ext4" PARTUUID="4e084d54-02"
```

‘blkid’ command allow to locate/print block device attributes. As we can see /dev/sda1 block device has ‘b69cb2c0-8a9b-4be3-aab6-992d5ed28ca4’ unique identifier, filesystem type ‘ext4’ and ‘4e084d54-01’ is the GUID from the GPT partition table.

```
root@ubuntu01:~# mount | grep sda
/dev/sda2 on / type ext4 (rw,relatime,errors=remount-ro,data=ordered)
/dev/sda1 on /boot type ext4 (rw,relatime,data=ordered)
```

‘grep’ command searches for pattern in each file. If no file is given, recursive searches examine the working directory, and nonrecursive searches read standard input. By default, grep prints the matching lines. As we can see in the output ‘grep sda’ command filter output of ‘mount’ command and prints only line that matched ‘sda’ pattern.

```
root@ubuntu01:~# dmesg | grep sda
[    3.115618] sd 2:0:0:0: [sda] 20971520 512-byte logical blocks: (10.7 GB/10.0 GiB)
[    3.117353] sd 2:0:0:0: [sda] Write Protect is off
[    3.118027] sd 2:0:0:0: [sda] Mode Sense: 00 3a 00 00
[    3.118141] sd 2:0:0:0: [sda] Write cache: enabled, read cache: enabled, doesn't support
DPO or FUA
[    3.122965]  sda: sda1 sda2
[    3.124656] sd 2:0:0:0: [sda] Attached SCSI disk
[    3.993592] EXT4-fs (sda2): mounted filesystem with ordered data mode. Opts: (null)
[    5.053741] EXT4-fs (sda2): re-mounted. Opts: errors=remount-ro
[    7.358973] EXT4-fs (sda1): mounted filesystem with ordered data mode. Opts: (null)
```

‘dmesg’ command is used to examine or control the kernel ring buffer. The default action is to display all messages from the kernel ring buffer. With ‘grep sda’ command we can see only lines that match ‘sda’ pattern. In our case it shows lines that concern to ‘sda’, ‘sda1’ and ‘sda2’ block devices.

```
ak@ubuntu01:~/test$ sudo grep -R -e “root” /etc > root_entries.txt
[sudo] password for ak:
ak@ubuntu01:~/test$ cat ./root_entries.txt
/etc/gshadow:root:*::
...
/etc/subuid:root:100000:65536
...
/etc/shadow:root:!:18348:0:99999:7:::
...
/etc/group:root:x:0:
...
/etc/sudoers:root       ALL=(ALL:ALL) ALL
...
/etc/passwd:root:x:0:0:root:/root:/bin/bash
...
/etc/crontab:17 *       * * *   root    cd / && run-parts --report /etc/cron.hourly
/etc/crontab:25 6       * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts
--report /etc/cron.daily )
/etc/crontab:47 6       * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts
--report /etc/cron.weekly )
/etc/crontab:52 6       1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts
--report /etc/cron.monthly )
...
```

This command examine the ‘/etc’ directory for pattern ‘root’ in each file with ‘root’ user access permissions and redirect the output to ‘root_entries.txt’ file. Also with ‘-R’ option it read all files under each directory, recursively and follow all symbolic links.
As we can see at the partial output of the ‘root_entries.txt’ file, ‘root’ entries can be found at such files:

- /etc/gshadow: shadowed group file;
- /etc/subuid: the subordinate uid file (each line contains a user name and a range of subordinate user ids that user is allowed to use);
- /etc/shadow: shadowed password file (each line contains the password information for the system's accounts and optional aging information);
- /etc/group: a text file that defines the groups on the system (one entry per line, with the following format: group_name:password:GID:user_list);
- /etc/sudoers: the policy file of ‘sudo’ security policy plugin;

- /etc/passwd: the password file that contains one line for each user account, with seven fields delimited by colons (“:”), These fields are: login name, optional encrypted password, numerical user ID, numerical group ID, user name or comment field, user home directory, optional user command interpreter;
- /etc/crontab: file contains instructions to the cron daemon of the general form: ``run this command at this time on this date''.