Homework 4.6

by Alexander Krupskiy

```
ak@ubuntu01:~$ sudo groupadd user
[sudo] password for ak:
ak@ubuntu01:~$ sudo useradd -g user -s /bin/bash -d /home/user -m user
ak@ubuntu01:~$ sudo passwd user
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
ak@ubuntu01:~$ id user
uid=1001(user) gid=1001(user) groups=1001(user)
ak@ubuntu01:~$ sudo ls -ld /home/user
drwxr-xr-x 2 user user 4096 Apr 23 19:39 /home/user
ak@ubuntu01:~$ su - user
Password:
user@ubuntu01:~$ pwd
/home/user
user@ubuntu01:~$ exit
logout
ak@ubuntu01:~$ sudo nano /etc/passwd
ak@ubuntu01:~$ su - user
Password:
su: Authentication failure
ak@ubuntu01:~$ cat /etc/passwd | grep user
user::1001:1001::/home/user:/bin/bash
```

```
ak@ubuntu01:~$ cat /etc/passwd | grep root
root:x:0:0:root:/root:/bin/bash
ak@ubuntu01:~$ cat /etc/passwd | grep ak
ak:x:1000:1000:ak,,,:/home/ak:/bin/bash
ak@ubuntu01:~$ cat /etc/passwd | grep user
user::1001:1001::/home/user:/bin/bash
ak@ubuntu01:~$ cut -f1,2,7 -d: /etc/passwd
root:x:/bin/bash
daemon:x:/usr/sbin/nologin
bin:x:/usr/sbin/nologin
sys:x:/usr/sbin/nologin
sync:x:/bin/sync
games:x:/usr/sbin/nologin
man:x:/usr/sbin/nologin
lp:x:/usr/sbin/nologin
mail:x:/usr/sbin/nologin
news:x:/usr/sbin/nologin
uucp:x:/usr/sbin/nologin
proxy:x:/usr/sbin/nologin
www-data:x:/usr/sbin/nologin
backup:x:/usr/sbin/nologin
list:x:/usr/sbin/nologin
irc:x:/usr/sbin/nologin
gnats:x:/usr/sbin/nologin
nobody:x:/usr/sbin/nologin
systemd-network:x:/usr/sbin/nologin
systemd-resolve:x:/usr/sbin/nologin
syslog:x:/usr/sbin/nologin
messagebus:x:/usr/sbin/nologin
_apt:x:/usr/sbin/nologin
```

```
lxd:x:/bin/false
uuidd:x:/usr/sbin/nologin
dnsmasq:x:/usr/sbin/nologin
landscape:x:/usr/sbin/nologin
sshd:x:/usr/sbin/nologin
pollinate:x:/bin/false
ak:x:/bin/bash
vboxadd:x:/bin/false
user::/bin/bash
ak@ubuntu01:~$ cut -f1,2 -d: /etc/group
root:x
daemon:x
bin:x
sys:x
adm:x
tty:x
disk:x
lp:x
mail:x
news:x
uucp:x
man:x
proxy:x
kmem:x
dialout:x
fax:x
voice:x
cdrom:x
floppy:x
tape:x
sudo:x
audio:x
dip:x
www-data:x
backup:x
operator:x
list:x
irc:x
src:x
gnats:x
shadow:x
utmp:x
video:x
sasl:x
plugdev:x
staff:x
games:x
users:x
nogroup:x
systemd-journal:x
systemd-network:x
systemd-resolve:x
input:x
crontab:x
syslog:x
messagebus:x
lxd:x
mlocate:x
uuidd:x
ssh:x
```

```
landscape:x
ak:x
lpadmin:x
sambashare:x
vboxsf:x
user:x
ak@ubuntu01:~$ less /etc/shadow
/etc/shadow: Permission denied
ak@ubuntu01:~$ sudo less /etc/shadow
root:!:18348:0:99999:7:::
daemon:*:18295:0:99999:7:::
bin:*:18295:0:99999:7:::
sys:*:18295:0:99999:7:::
sync:*:18295:0:99999:7:::
games:*:18295:0:99999:7:::
man:*:18295:0:99999:7:::
lp:*:18295:0:99999:7:::
mail:*:18295:0:99999:7:::
news:*:18295:0:99999:7:::
uucp:*:18295:0:99999:7:::
proxy:*:18295:0:99999:7:::
www-data:*:18295:0:99999:7:::
backup:*:18295:0:99999:7:::
list:*:18295:0:99999:7:::
irc:*:18295:0:99999:7:::
gnats:*:18295:0:99999:7:::
nobody:*:18295:0:99999:7:::
systemd-network:*:18295:0:99999:7:::
systemd-resolve:*:18295:0:99999:7:::
syslog:*:18295:0:99999:7:::
messagebus:*:18295:0:99999:7:::
_apt:*:18295:0:99999:7:::
lxd:*:18348:0:99999:7:::
uuidd:*:18348:0:99999:7:::
dnsmasq:*:18348:0:99999:7:::
landscape:*:18348:0:99999:7:::
sshd:*:18348:0:99999:7:::
pollinate:*:18348:0:99999:7:::
ak:$1$kwEnNVhb$teKuGSbPTQ/I6MWDjliz1t6uUvX34cdilE2zcWuFu9be2ygaShJb/itRKwurB95yieX3omMRDfaSaui
igxjfa0:18348:0:99999:7:::
vboxadd:!:18348::::::
user:$6$T6qzHX9X$4W3pVRSV63xyZQeK3uwdnaiyNgHtvIOtKwe1pUQ4HPYm.UkKF3fL.UfkZd2f.2RzaDCDL0CG4SQgz
QrtXv2Yv/:18375:0:99999:7:::
vnstat:*:18375:0:99999:7:::
/etc/shadow (END)
```

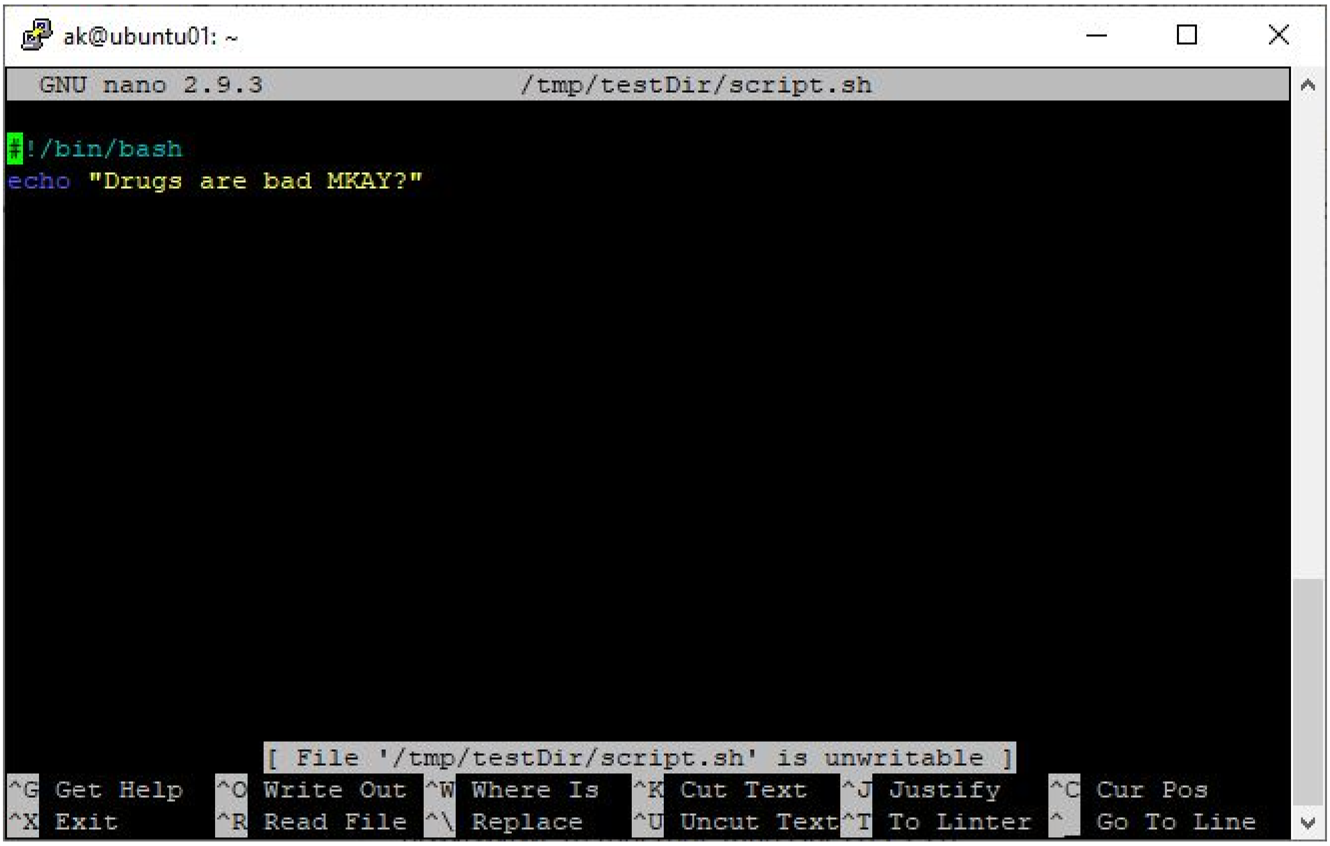
‘/etc/shadow’ is a file which contains the password information for the system's accounts and optional aging information. This file must not be readable by regular users if password security is to be maintained. Each line of this file contains 9 fields, separated by colons (“:”)

For example we take one line from /etc/shadow with username ‘ak’ and describe all fields:

1. ‘ak’ - login name
2. encrypted password, If the password field contains some string that is not a valid result of crypt, for instance ! or *, the user will not be able to use a unix password to log in (but the user may log in the system by other means)
3. ‘18348’ - date of last password change since Jan 1, 1970 count in days. The value 0 has a special meaning, which is that the user should change her password the next time she will log in the system.
4. ‘0’ - minimum password age, is the number of days the user will have to wait before he/she will be allowed to change her password again

5. ‘99999’ - maximum password age, is the number of days after which the user will have to change his/her password the next time he/she will log in. An empty field means that there are no maximum password age, no password warning period, and no password inactivity period
6. ‘7’ - password warning period, the number of days before a password is going to expire during which the user should be warned. An empty field and value 0 mean that there are no password warning period
7. empty field - password inactivity period, the number of days after a password has expired during which the password should still be accepted. After expiration of the password and this expiration period is elapsed, no login is possible using the current user's password. An empty field means that there are no enforcement of an inactivity period
8. empty field - account expiration date, the date of expiration of the account, expressed as the number of days since Jan 1, 1970. An empty field means that the account will never expire
9. empty field - this field is reserved for future use

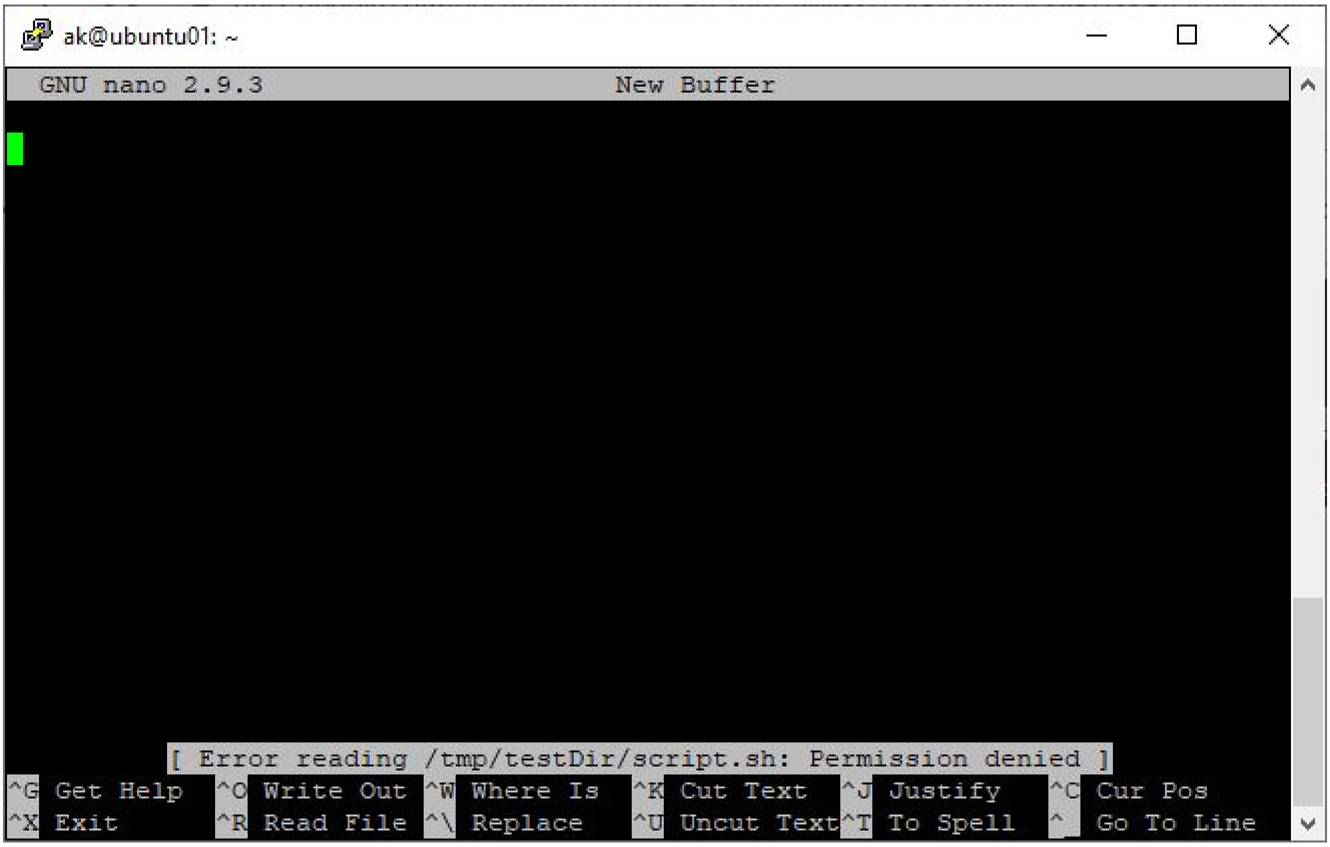
```
ak@ubuntu01:~$ nano ./script.sh
ak@ubuntu01:~$ ls -l
total 4
-rw-rw-r-- 1 ak ak 39 Apr 23 21:18 script.sh
ak@ubuntu01:~$ chmod +x ./script.sh
ak@ubuntu01:~$ ls -l
total 4
-rwxrwxr-x 1 ak ak 39 Apr 23 21:18 script.sh
ak@ubuntu01:~$ ./script.sh
Drugs are bad MKAY?
ak@ubuntu01:~$ mkdir /tmp/testDir
ak@ubuntu01:~$ cp ./script.sh /tmp/testDir/
ak@ubuntu01:~$ ls -la /tmp/testDir/
total 12
drwxrwxr-x  2 ak   ak   4096 Apr 23 21:24 .
drwxrwxrwt 10 root root 4096 Apr 23 21:24 ..
-rwxrwxr-x  1 ak   ak     39 Apr 23 21:24 script.sh
ak@ubuntu01:~$ chmod 770 /tmp/testDir
ak@ubuntu01:~$ ls -la /tmp/testDir/
total 12
drwxrwx---  2 ak   ak   4096 Apr 23 21:24 .
drwxrwxrwt 10 root root 4096 Apr 23 21:26 ..
-rwxrwxr-x  1 ak   ak     39 Apr 23 21:24 script.sh
ak@ubuntu01:~$ su - user
Password:
user@ubuntu01:~$ cd /tmp/testDir/
-su: cd: /tmp/testDir/: Permission denied
ak@ubuntu01:~$ chmod 460 /tmp/testDir/script.sh
ak@ubuntu01:~$ ls -l /tmp/testDir/script.sh
-r--rw---- 1 ak ak 39 Apr 23 21:24 /tmp/testDir/script.sh
```



```
#!/bin/bash
echo "Drugs are bad MKAY?"
```

```
[ File '/tmp/testDir/script.sh' is unwritable ]
```

```
ak@ubuntu01:~$ chmod 060 /tmp/testDir/script.sh
ak@ubuntu01:~$ ls -l /tmp/testDir/script.sh
----rw---- 1 ak ak 39 Apr 23 21:24 /tmp/testDir/script.sh
```



```
[ Error reading /tmp/testDir/script.sh: Permission denied ]
```