EPAM University programs DevOps external course Oleksandr Briukhanov

Module 4 Linux & Bash Essentials (Task 4.6)

1. *User management*. Here we suppose there are at least two users, namely, root and guest.
(i) Create a new user *user*
groupadd user
useradd -g user -s /bin/bash -d /home/user -m user
passwd user
id user
ls -ld /home/user
(ii) Log in to the system as "user" (hint use **su**).
(ii) Edit **/etc/passwd** to prevent user *user* from logging in to the system.

```
root@wibob-X61:~# groupadd user
root@wibob-X61:~# useradd -g user -s /bin/bash -d /home/user -m user
root@wibob-X61:~# passwd user
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@wibob-X61:~# id user
uid=1001(user) gid=1002(user) groups=1002(user)
root@wibob-X61:~# ls -ld /home/user
drwxr-xr-x 2 user user 4096 кві 18 03:04 /home/user
root@wibob-X61:~# su user
user@wibob-X61:
user@wibob-X61:
user@wibob-X61:
user@wibob-X61: exit
You have new mail in /var/mail/root
root@wibob-X61:~# vim /etc/passwd
root@wibob-X61:~# cat /etc/passwd | grep user:
user:x:1001:1002::/home/user:/bin/false
root@wibob-X61:~#
root@wibob-X61:~# su user
root@wibob-X61:~# whoami
root
```

2. *Content of* /etc/passwd and /etc/group.
(i) Look through **/etc/passwd** and **/etc/group** (hint: use **less** or **cat**).
(ii) Get data from **/etc/passwd** and **/etc/group** about users: *root*, *guest*, *user* (hint: filter by **grep**).

## I have not user 'guest' in my system

```
root@wibob-X61:~# cat /etc/passwd | grep 'root:\|guest:\|user:'
root:x:0:0:root:/root:/bin/bash
user:x:1001:1002::/home/user:/bin/false
root@wibob-X61:~# cat /etc/group | grep 'root:\|guest:\|user:'
root:x:0:
user:x:1002:
root@wibob-X61:~#
```

(iii)Parse **/etc/passwd** and **/etc/group** with cut.

cut -f1 -d: /etc/passwd

## -f1 "cut" command get first word from every string, using ':' as a delimiter between words (option -d:)

```
root@wibob-X61:~# cut -f1 -d: /etc/passwd
root
daemon
bin
sys
sync
games
```

cut -f1,2 -d: /etc/passwd

## ,2 means how many sequential words will be cut from first

```
root@wibob-X61:~# cut -f1,2 -d: /etc/passwd
root:x
daemon:x
bin:x
sys:x
sync:x
games:x
```

cut -f1,7 -d: /etc/passwd

```
root@wibob-X61:~# cut -f1,7 -d: /etc/passwd
root:/bin/bash
daemon:/usr/sbin/nologin
bin:/usr/sbin/nologin
sys:/usr/sbin/nologin
sync:/bin/sync
games:/usr/sbin/nologin
```

cut -f1 -d: /etc/group

```
root@wibob-X61:~# cut -f1 -d: /etc/group
root
daemon
bin
sys
adm
tty
disk
```

cut -f1,2 -d: /etc/group

```
root@wibob-X61:~# cut -f1,2 -d: /etc/group
root:x
daemon:x
bin:x
sys:x
adm:x
tty:x
disk:x
```

iv) Try to call **less** on **/etc/shadow** and invoke
## Permission denied

```
bruh@wibob-X61:~$ sudo ls -l /etc/shadow
-rw-r----- 1 root shadow 1627 кві 18 03:05 /etc/shadow
```

sudo less /etc/shadow

```
root:!:18179:0:99999:7:::
daemon:*:17953:0:99999:7:::
bin:*:17953:0:99999:7:::
sys:*:17953:0:99999:7:::
sync:*:17953:0:99999:7:::
games:*:17953:0:99999:7:::
```

man -k shadow

## -k option searches keyword in all man pages and display list of this pages

```
bruh@wibob-X61:~$ man -k shadow
endspent (3)         - get shadow password file entry
fgetspent (3)        - get shadow password file entry
fgetspent_r (3)      - get shadow password file entry
getspent (3)         - get shadow password file entry
getspent_r (3)       - get shadow password file entry
getspnam (3)         - get shadow password file entry
getspnam_r (3)       - get shadow password file entry
gpasswd (1)          - administer /etc/group and /etc/gshadow
grpconv (8)          - convert to and from shadow passwords and groups
grpunconv (8)        - convert to and from shadow passwords and groups
gshadow (5)          - shadowed group file
lckpwdf (3)          - get shadow password file entry
login.defs (5)       - shadow password suite configuration
ppmshadow (1)        - add simulated shadows to a portable pixmap image
putspent (3)         - get shadow password file entry
pwconv (8)           - convert to and from shadow passwords and groups
pwunconv (8)         - convert to and from shadow passwords and groups
setspent (3)         - get shadow password file entry
sgetspent (3)        - get shadow password file entry
sgetspent_r (3)      - get shadow password file entry
shadow (5)           - shadowed password file
shadowconfig (8)     - toggle shadow passwords on and off
ulckpwdf (3)         - get shadow password file entry
update-passwd (8)    - safely update /etc/passwd, /etc/shadow and /etc/group
vigr (8)             - edit the password, group, shadow-password or shadow-group...
vipw (8)             - edit the password, group, shadow-password or shadow-group.
```

man 5 shadow

## describe structure of a shadow file strings

Analyse content of **/etc/shadow** based on what you've found in **man** 5 shadow.

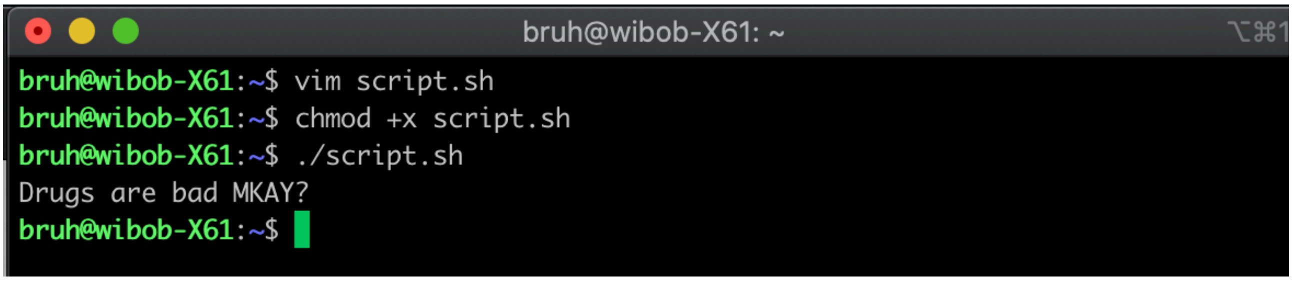
```
bruh:$6$adSgA214$j2zsqdcIHF6C1yl6DjzAx5GJVvpUU5JOdcxedB/rlCkkq2xon09tNq5XdRBIKQ7G3UoEgo/Tsbel3ubW7kyZ3.:18179:0:99999:7:::
```

This string for user bruh
This user has encrypted password
Last password changes was 01.01.1970+18179 day (not user-friendly information form)
Min age of password before user can change it - not set

Max age of password 99999 days (if that field lower than min password age, the user cannot change his password)
The number of days before a password is going to expire during which the user should be warned - 7
Password inactivity period - not set
Account expiration date - not set

3. Dealing with **chmod**.

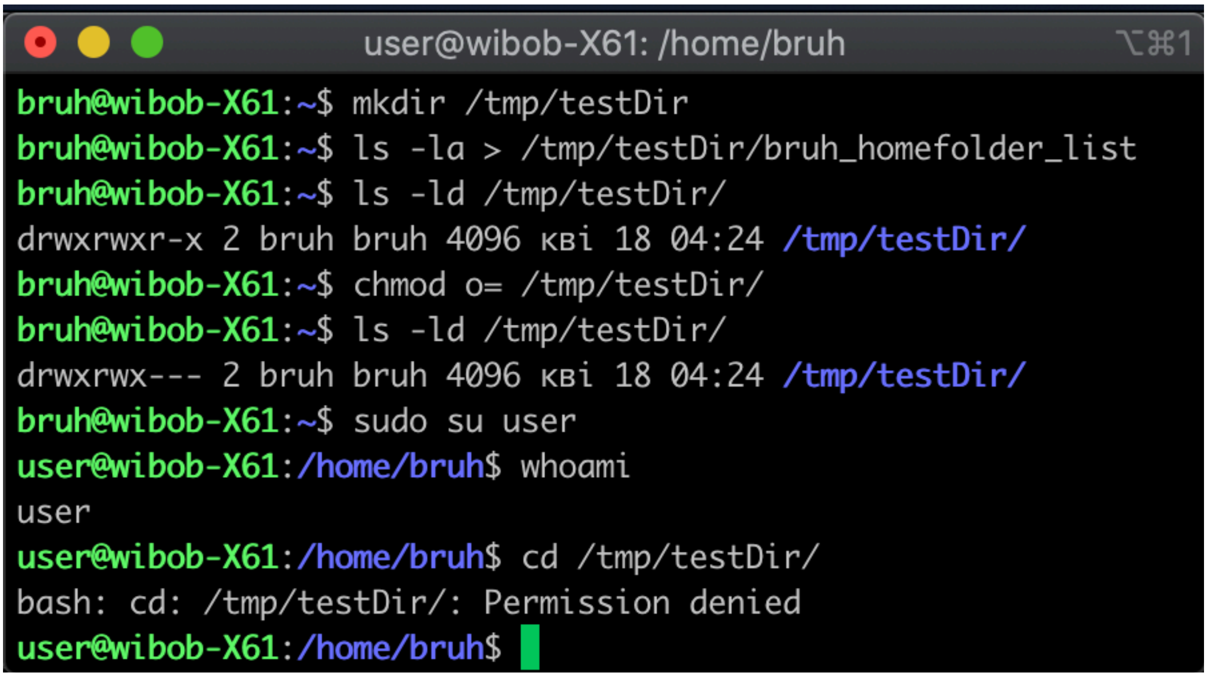
(i) An executable script. Open your favourite editor and put these lines into a file
#!/bin/bash
echo “Drugs are bad MKAY?”
Give name “script.sh” to the script and call to
chmod +x script.sh
Then you are ready to execute the script:
./script.sh



```
bruh@wibob-X61:~$ vim script.sh
bruh@wibob-X61:~$ chmod +x script.sh
bruh@wibob-X61:~$ ./script.sh
Drugs are bad MKAY?
bruh@wibob-X61:~$
```

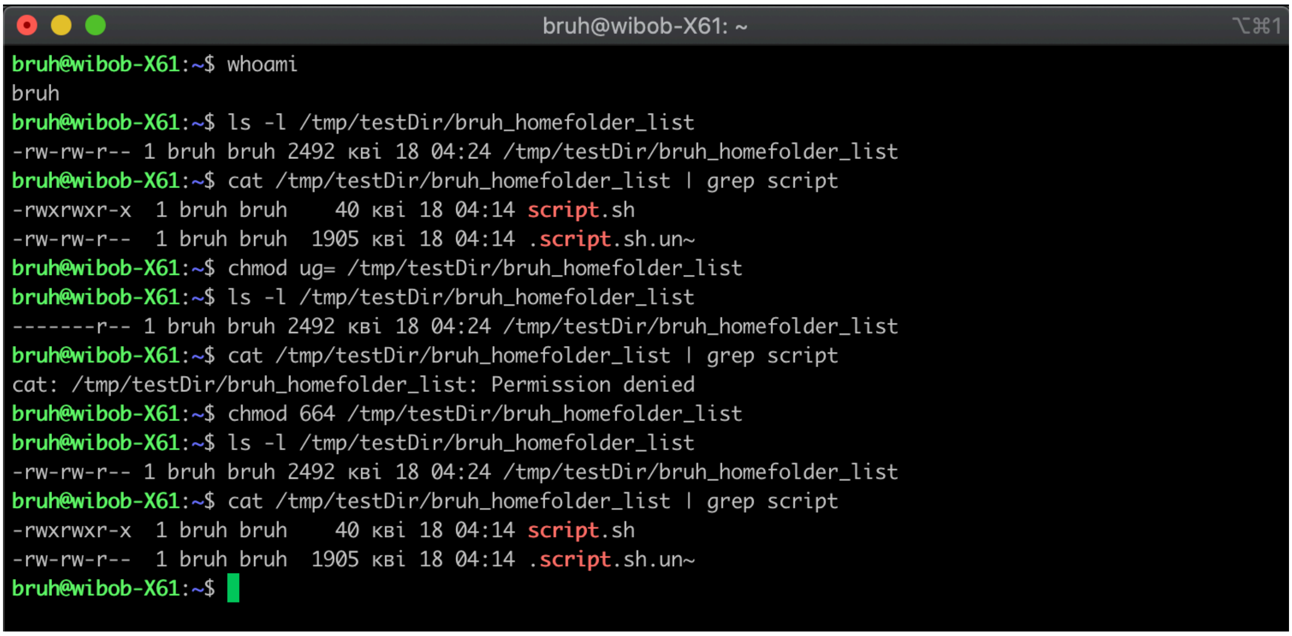
(ii) Suppose, you have logged in to the system as *guest*. Create directory “testDir” in the **/tmp**; put some file into testDir and prohibit user *user* from visiting this directory (i.e. “testDir”).

## instead of using user guest (i have not in my system) i have used user bruh



```
bruh@wibob-X61:~$ mkdir /tmp/testDir
bruh@wibob-X61:~$ ls -la > /tmp/testDir/bruh_homefolder_list
bruh@wibob-X61:~$ ls -ld /tmp/testDir/
drwxrwxr-x 2 bruh bruh 4096 кві 18 04:24 /tmp/testDir/
bruh@wibob-X61:~$ chmod o= /tmp/testDir/
bruh@wibob-X61:~$ ls -ld /tmp/testDir/
drwxrwx--- 2 bruh bruh 4096 кві 18 04:24 /tmp/testDir/
bruh@wibob-X61:~$ sudo su user
user@wibob-X61:/home/bruh$ whoami
user
user@wibob-X61:/home/bruh$ cd /tmp/testDir/
bash: cd: /tmp/testDir/: Permission denied
user@wibob-X61:/home/bruh$
```

(iii) Test, if it possible to forbid an owner of some file to read to or write from this file.



```
bruh@wibob-X61:~$ whoami
bruh
bruh@wibob-X61:~$ ls -l /tmp/testDir/bruh_homefolder_list
-rw-rw-r-- 1 bruh bruh 2492 кві 18 04:24 /tmp/testDir/bruh_homefolder_list
bruh@wibob-X61:~$ cat /tmp/testDir/bruh_homefolder_list | grep script
-rwxrwxr-x  1 bruh bruh    40 кві 18 04:14 script.sh
-rw-rw-r--  1 bruh bruh  1905 кві 18 04:14 .script.sh.un~
bruh@wibob-X61:~$ chmod ug= /tmp/testDir/bruh_homefolder_list
bruh@wibob-X61:~$ ls -l /tmp/testDir/bruh_homefolder_list
-------r-- 1 bruh bruh 2492 кві 18 04:24 /tmp/testDir/bruh_homefolder_list
bruh@wibob-X61:~$ cat /tmp/testDir/bruh_homefolder_list | grep script
cat: /tmp/testDir/bruh_homefolder_list: Permission denied
bruh@wibob-X61:~$ chmod 664 /tmp/testDir/bruh_homefolder_list
bruh@wibob-X61:~$ ls -l /tmp/testDir/bruh_homefolder_list
-rw-rw-r-- 1 bruh bruh 2492 кві 18 04:24 /tmp/testDir/bruh_homefolder_list
bruh@wibob-X61:~$ cat /tmp/testDir/bruh_homefolder_list | grep script
-rwxrwxr-x  1 bruh bruh    40 кві 18 04:14 script.sh
-rw-rw-r--  1 bruh bruh  1905 кві 18 04:14 .script.sh.un~
bruh@wibob-X61:~$ 
```

It is possible.

I was working as user bruh

1. A have successfully tried to view my file
2. with chmod ug= I cleared all permission bits for owner and his group (bruh:bruh)
3. Try to do same action from 1. But - permission was denied (despite of ownership)
4. I returned permissions with chmod 664 command to my file (I steel can do it because i'm owner)
5. And successfully got access.