EPAM University Programs

DevOps external course

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

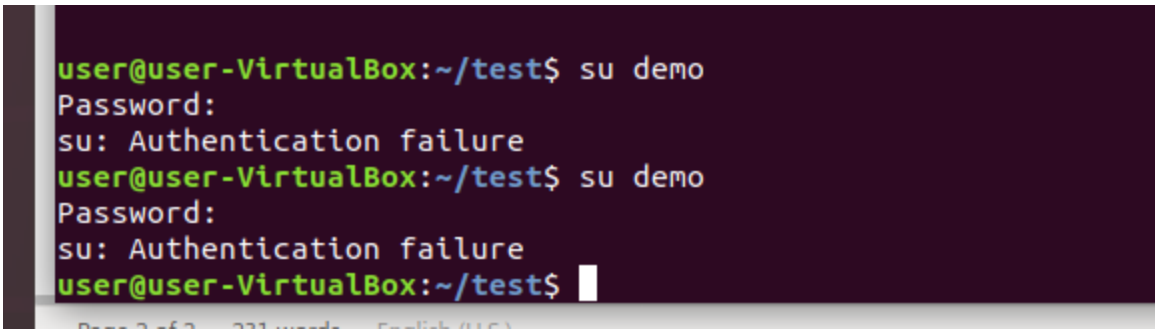
ls -ld /home/user

(ii) Log in to the system as “user” (hint use **su**).

```
user@user-VirtualBox:~/test$ sudo groupadd demo
user@user-VirtualBox:~/test$ sudo useradd -g demo -s /bin/bash -d /home/demo -m demo
user@user-VirtualBox:~/test$ passwd demo
passwd: You may not view or modify password information for demo.
user@user-VirtualBox:~/test$ sudo passwd demo
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
user@user-VirtualBox:~/test$ id demo
uid=1002(demo) gid=1002(demo) groups=1002(demo)
user@user-VirtualBox:~/test$ ls -ld /home/demo/
drwxr-xr-x 2 demo demo 4096 кві 23 23:51 /home/demo/
user@user-VirtualBox:~/test$ man su
user@user-VirtualBox:~/test$ su demo
Password:
demo@user-VirtualBox:/home/user/test$ who
user     :0           2020-04-14 23:42 (:0)
demo@user-VirtualBox:/home/user/test$ who
user     :0           2020-04-14 23:42 (:0)
demo@user-VirtualBox:/home/user/test$ whoami
demo
demo@user-VirtualBox:/home/user/test$
```

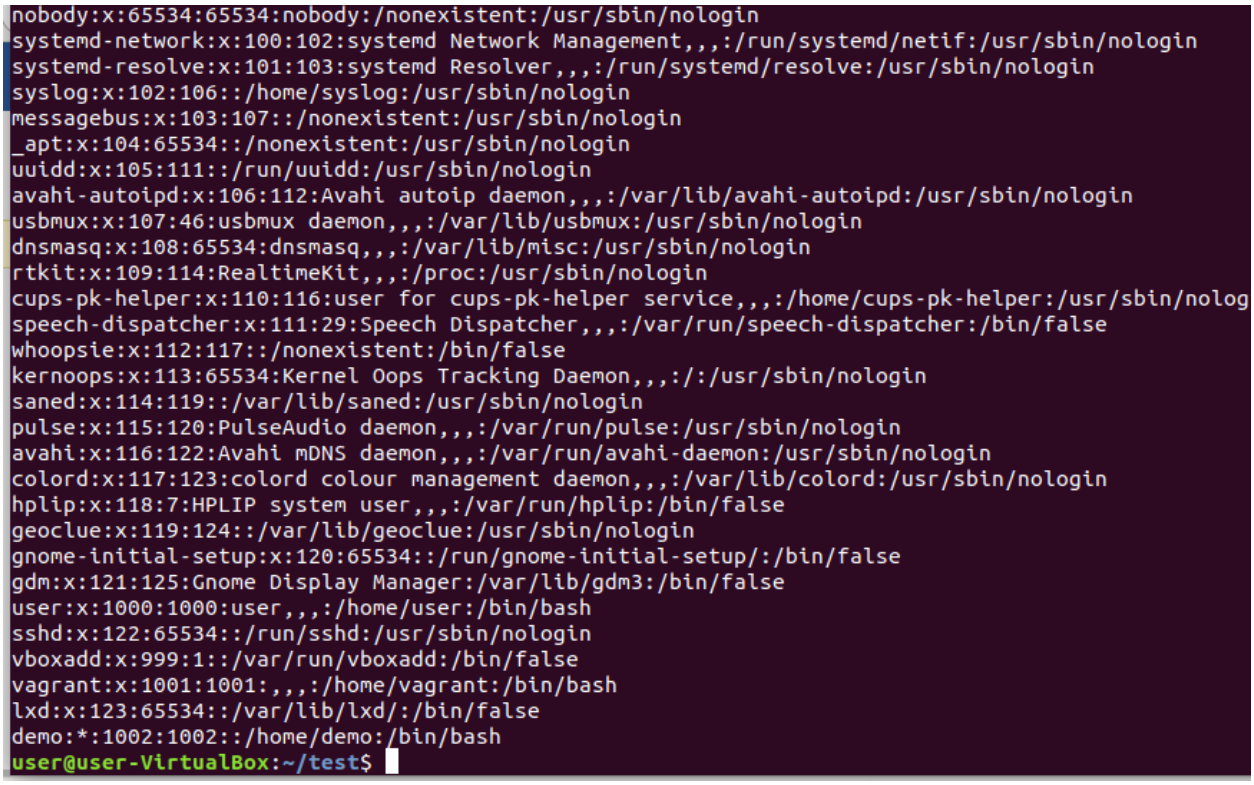
Page 2 of 2 231 words English (U.S.)

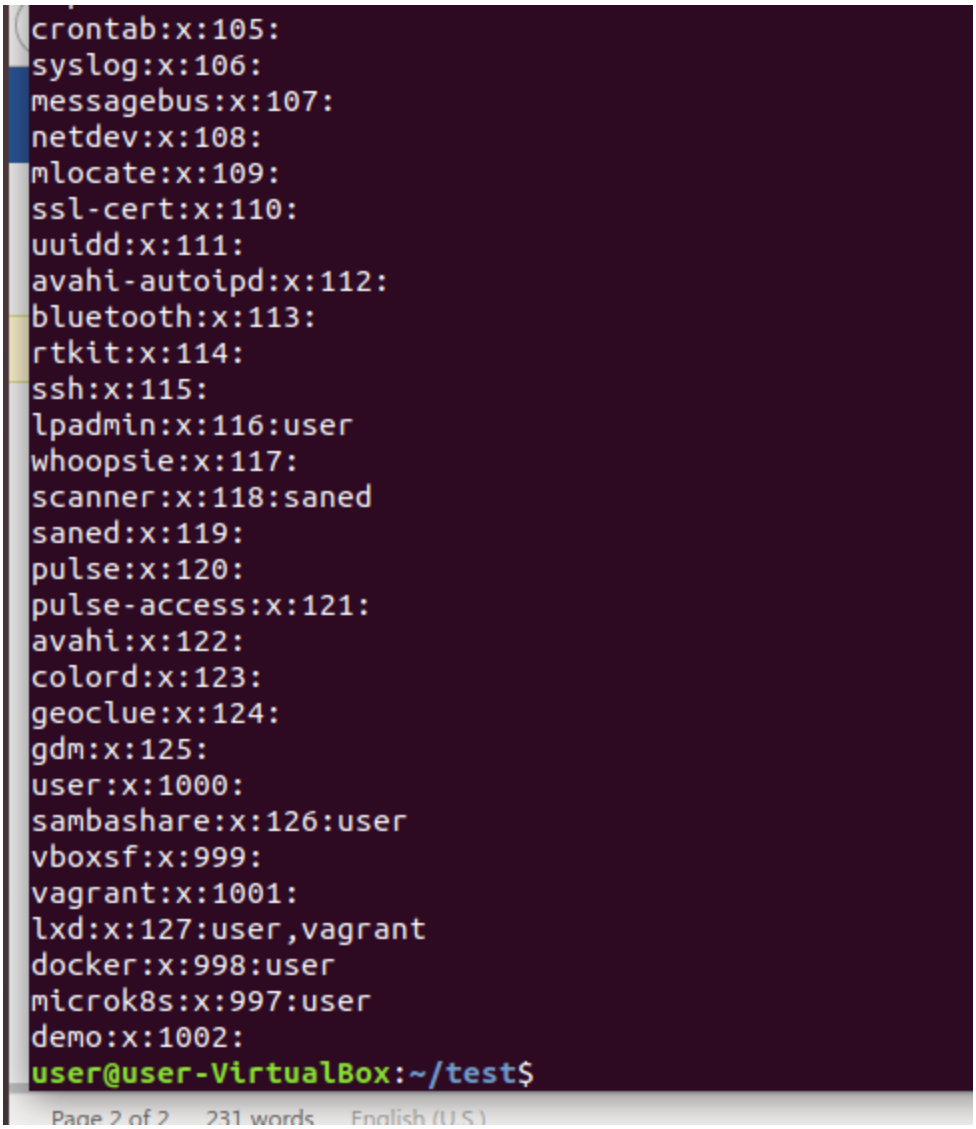
(ii) Edit **/etc/passwd** to prevent user *user* from logging in to the system.



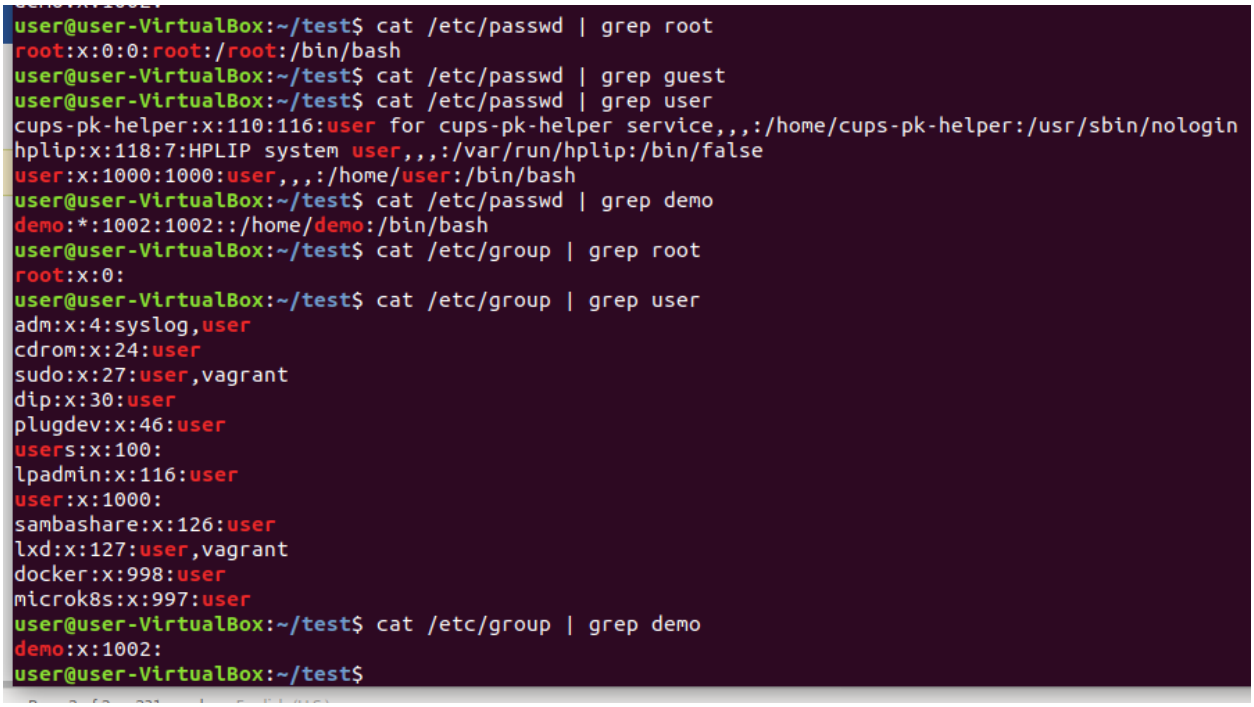
2. *Content of* **/etc/passwd** and **/etc/group**.

(i) Look through **/etc/passwd** and **/etc/group** (hint: use **less** or **cat**).


nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
uuidd:x:105:111::/run/uuidd:/usr/sbin/nologin
avahi-autoipd:x:106:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
rtkit:x:109:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
cups-pk-helper:x:110:116:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nolog
speech-dispatcher:x:111:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
whoopsie:x:112:117::/nonexistent:/bin/false
kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
saned:x:114:119::/var/lib/saned:/usr/sbin/nologin
pulse:x:115:120:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
avahi:x:116:122:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
colord:x:117:123:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:118:7:HPLIP system user,,,:/var/run/hplip:/bin/false
geoclue:x:119:124::/var/lib/geoclue:/usr/sbin/nologin
gnome-initial-setup:x:120:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:121:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
user:x:1000:1000:user,,,:/home/user:/bin/bash
sshd:x:122:65534::/run/sshd:/usr/sbin/nologin
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
vagrant:x:1001:1001:,,,:/home/vagrant:/bin/bash
lxd:x:123:65534::/var/lib/lxd/:/bin/false
demo:*:1002:1002::/home/demo:/bin/bash
user@user-VirtualBox:~/test$

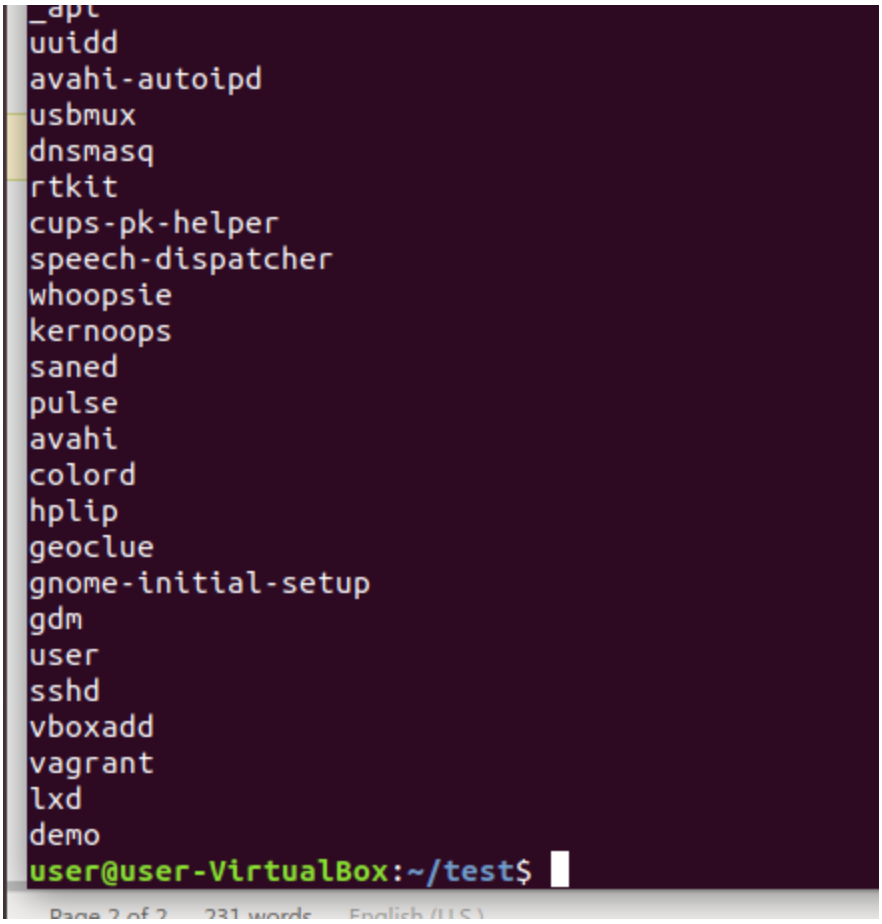


(ii) Get data from **/etc/passwd** and **/etc/group** about users: *root*, *guest*, *user* (hint: filter by **grep**).

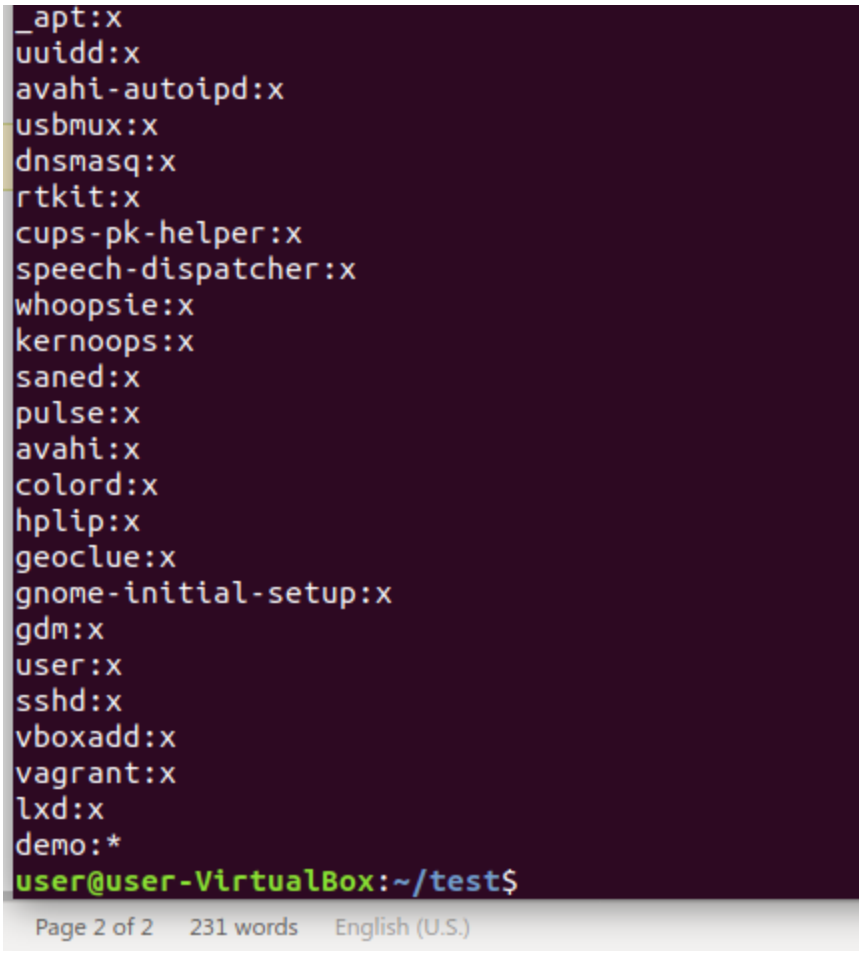


(iii)Parse **/etc/passwd** and **/etc/group** with cut.

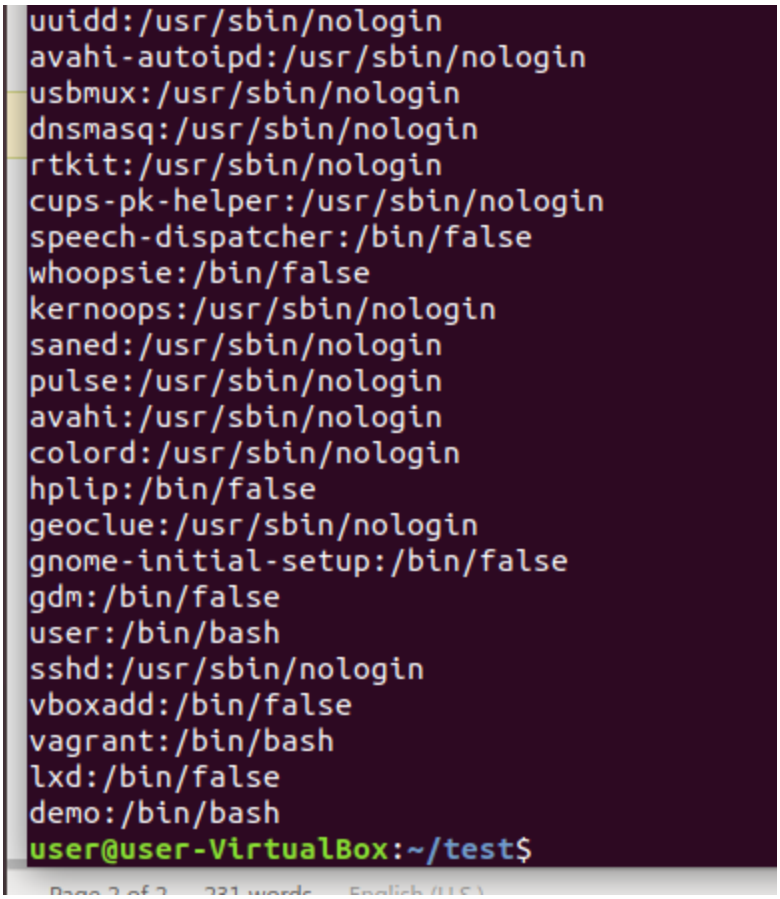
cut -f1 -d: /etc/passwd



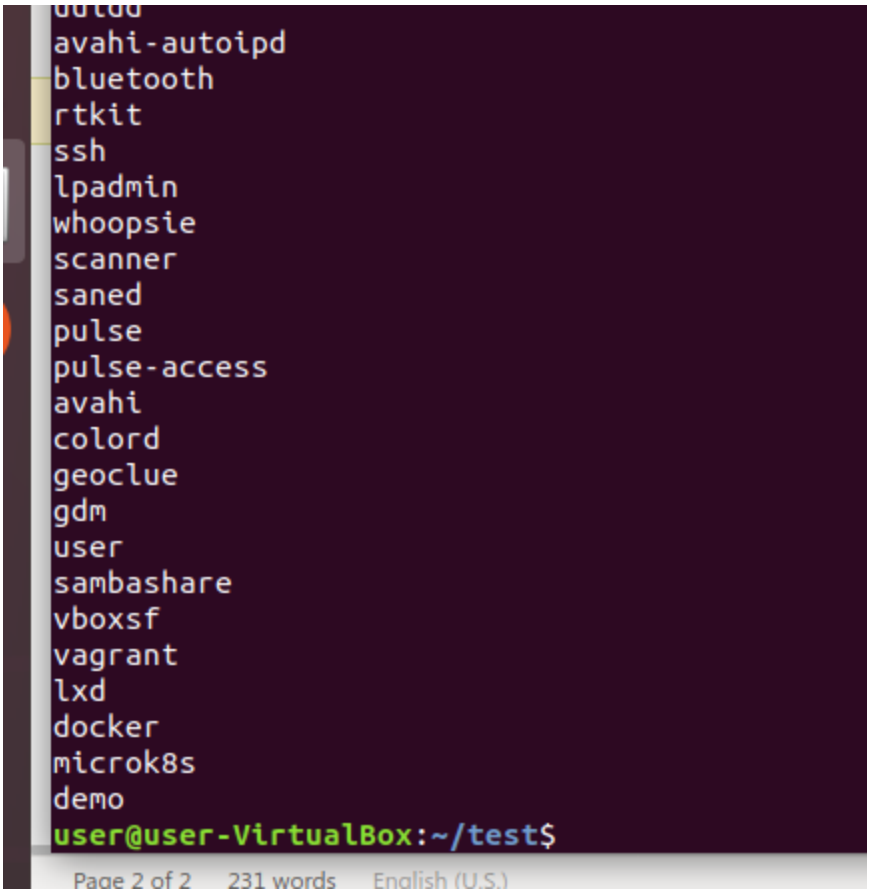
cut -f1,2 -d: /etc/passwd



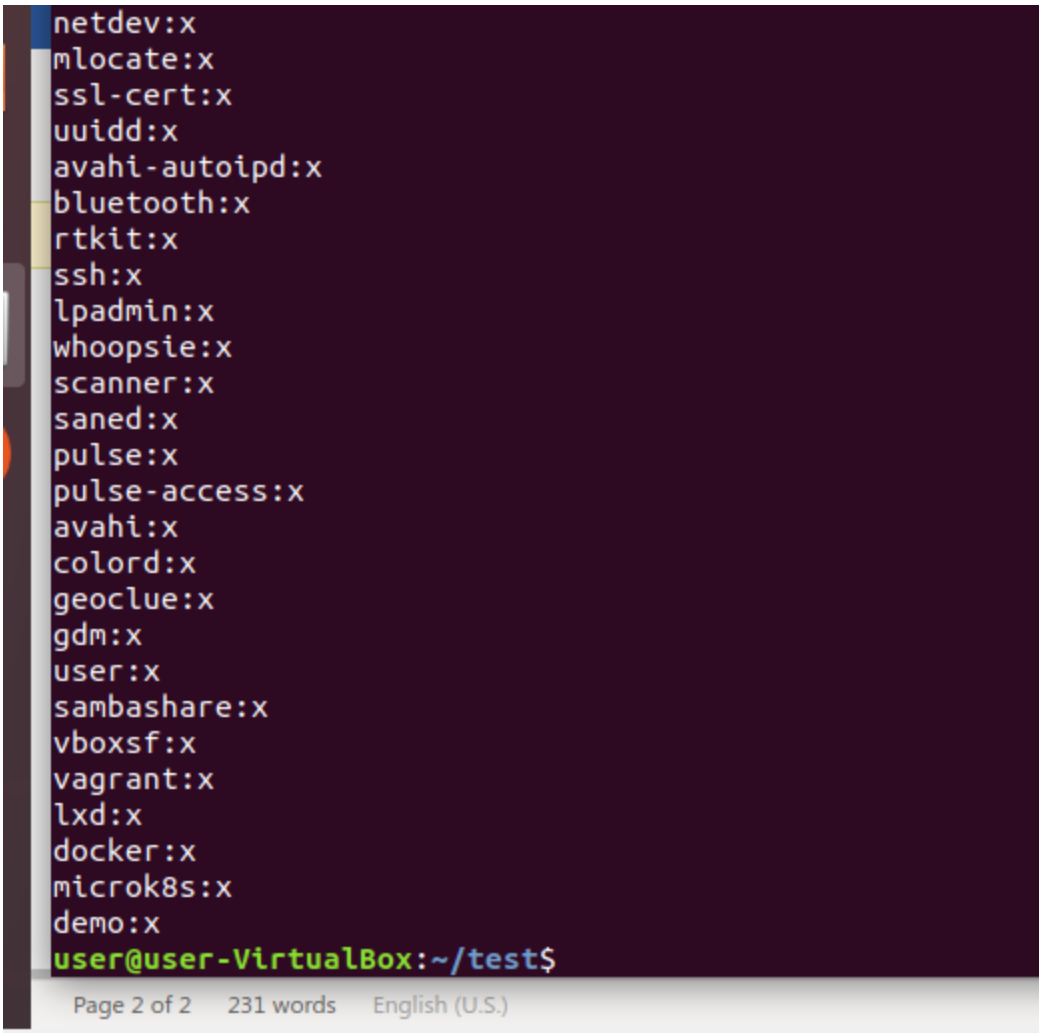
cut -f1,7 -d: /etc/passwd



cut -f1 -d: /etc/group

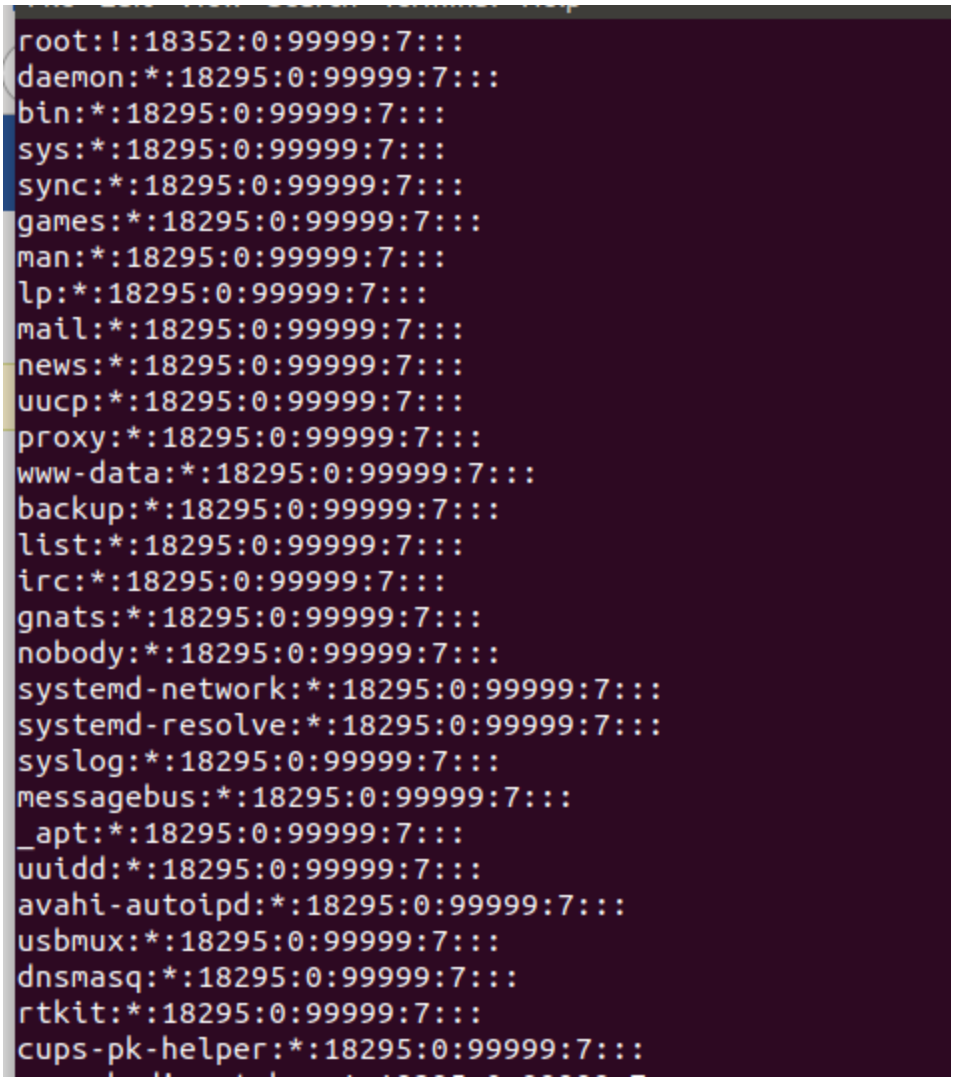


cut -f1,2 -d: /etc/group



(iv) Try to call **less** on **/etc/shadow** and invoke

sudo less /etc/shadow



man -k shadow

man 5 shadow

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

`/etc/shadow` is used to increase the security level of passwords by restricting all but highly privileged users' access to hashed password data. Typically, that data is kept in files owned by and accessible only by the super user.

With a shadowed password scheme in use, the `/etc/passwd` file typically shows a character such as '*', or 'x' in the password field for each user instead of the hashed password, and `/etc/shadow` usually contains the following user information:

- User login name
- salt and hashed password OR a status exception value e.g.:
    - "idsalt$hashed", the printable form of a password hash as produced by crypt (C), where "$id" is the algorithm used. Other Unix-like systems may have different values, like NetBSD.

    - Empty string – No password, the account has no password (reported by passwd on Solaris with "NP").[6]
    - "!", "*" – the account is password locked, user will be unable to log in via password authentication but other methods (e.g. ssh key, logging in as root) may be still allowed.[7]
    - "*LK*" – the account itself is locked, user will be unable to log in.[7]
    - "*NP*", "!!" – the password has never been set[8]
- Days since epoch of last password change
- Days until change allowed
- Days before change required
- Days warning for expiration
- Days after no logins before account is locked
- Days since epoch when account expires
- Reserved and unused

3. Dealing with **chmod**.

(i) An executable script. Open your favorite editor and put these lines into a file

#!/bin/bash

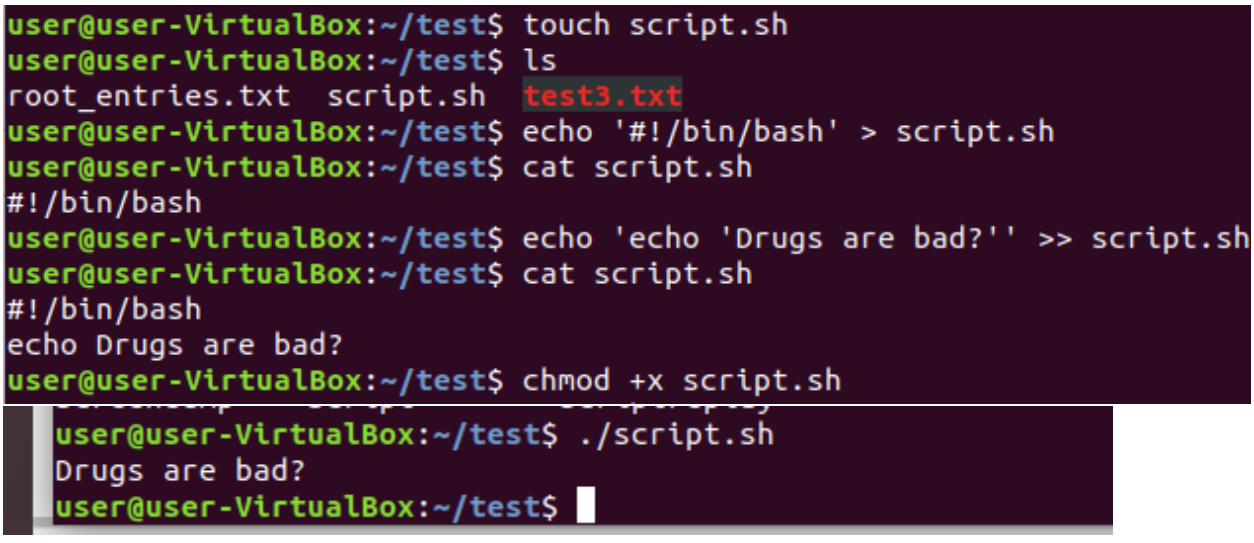
echo “Drugs are bad MKAY?”

Give name “script.sh” to the script and call to

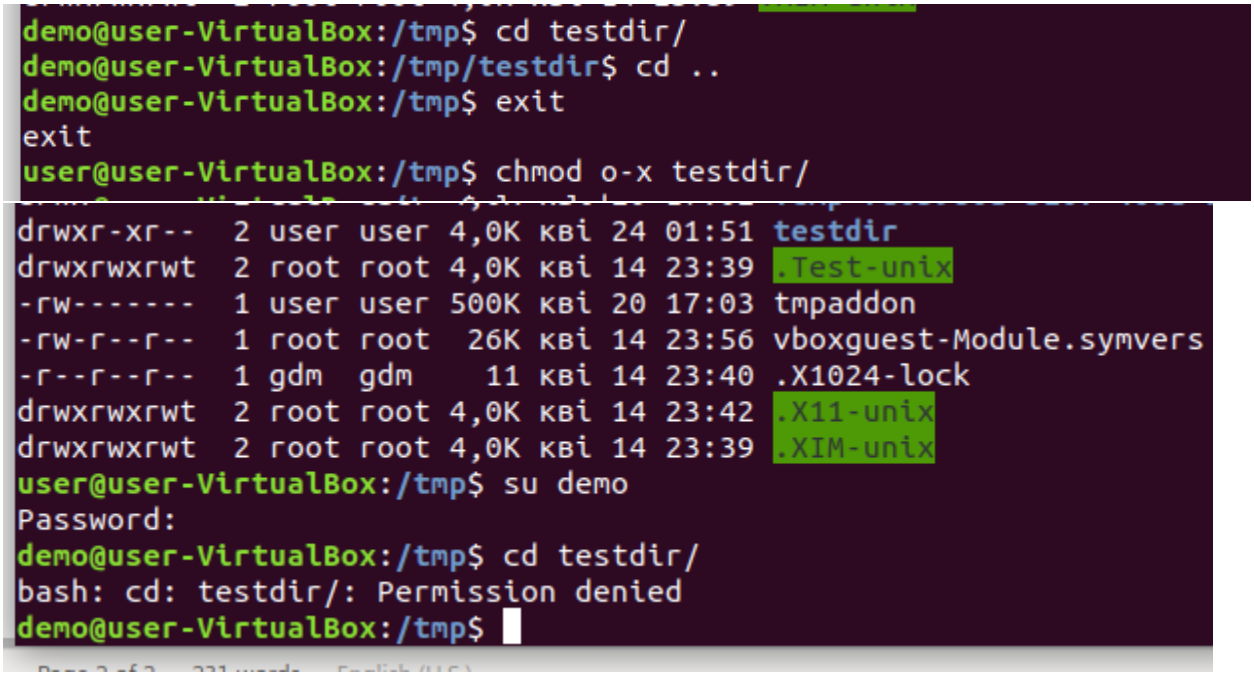
chmod +x script.sh

Then you are ready to execute the script:

./**script.sh**



(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”).



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

```
user@user-VirtualBox:/tmp/testdir$ ls -lah
total 12K
drwxr-xr--  2 user user 4,0K кві 24 01:51 .
drwxrwxrwt 20 root root 4,0K кві 24 02:02 ..
-rwxr-xr-x  1 user user   32 кві 24 01:51 script.sh
user@user-VirtualBox:/tmp/testdir$ chmod u-rw script.sh
user@user-VirtualBox:/tmp/testdir$ ls -lah
total 12K
drwxr-xr--  2 user user 4,0K кві 24 01:51 .
drwxrwxrwt 20 root root 4,0K кві 24 02:03 ..
---xr-xr-x  1 user user   32 кві 24 01:51 script.sh
user@user-VirtualBox:/tmp/testdir$ cat script.sh
cat: script.sh: Permission denied
user@user-VirtualBox:/tmp/testdir$ echo 666 >> script.sh
bash: script.sh: Permission denied
user@user-VirtualBox:/tmp/testdir$
```

Page 2 of 2 231 words English (U.S.)


```
user@user-VirtualBox:/tmp/testdir$ ls -lah
total 12K
drwxr-xr--  2 user user 4,0K кві 24 01:51 .
drwxrwxrwt 20 root root 4,0K кві 24 02:02 ..
-rwxr-xr-x  1 user user   32 кві 24 01:51 script.sh
user@user-VirtualBox:/tmp/testdir$ chmod u-rw script.sh
user@user-VirtualBox:/tmp/testdir$ ls -lah
total 12K
drwxr-xr--  2 user user 4,0K кві 24 01:51 .
drwxrwxrwt 20 root root 4,0K кві 24 02:03 ..
---xr-xr-x  1 user user   32 кві 24 01:51 script.sh
user@user-VirtualBox:/tmp/testdir$ cat script.sh
cat: script.sh: Permission denied
user@user-VirtualBox:/tmp/testdir$ echo 666 >> script.sh
bash: script.sh: Permission denied
user@user-VirtualBox:/tmp/testdir$
```

Page 2 of 2 231 words English (U.S.)