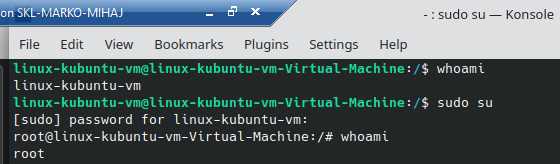
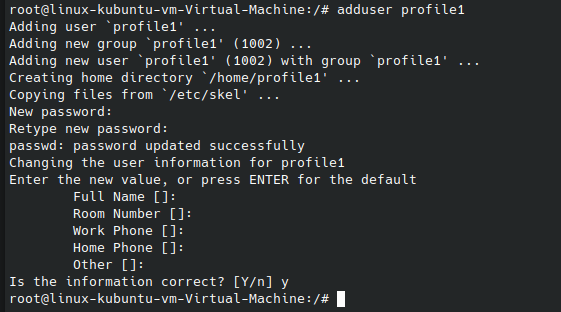
Linux Commands Part II Homework – Marko Mihajlov

1. Elevate your user access to root;

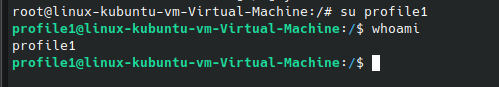


1. add a new user to your Linux OS and set a password for it;



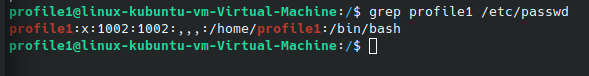
Alternatively we could user useradd with the flag -p to specify the password.

1. Test if you can log in using that user;



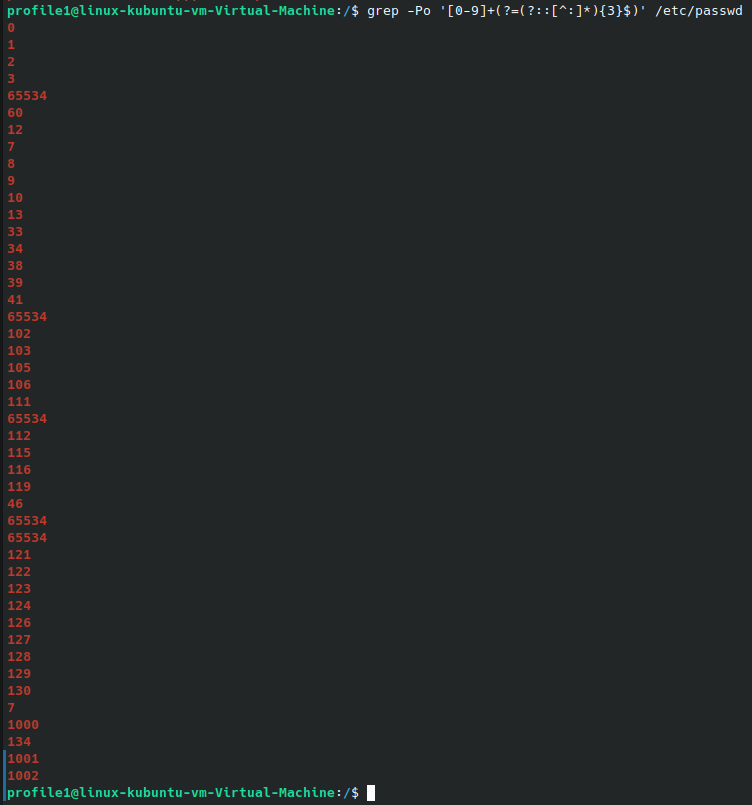
Login worked without asking for password because we were already root atm.

1. Using grep command check if the user is created;



Grep shows the whole line where “profile1” is mentioned.

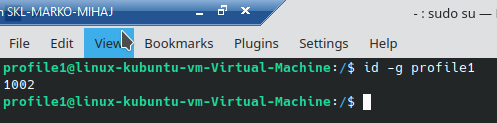
1. grep the UID of each user;



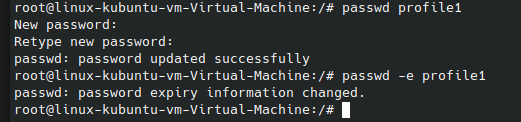
This is a very complicated way of going about it, but it was asked to do it with grep. Following is an explanation pulled from the web. – The pattern '[0-9]+(?=(?::[^:]\*){3}$)' matches one or more digits [0-9]+, followed by a positive lookahead (?=...). The positive lookahead asserts that what follows the digits is a sequence of three non-overlapping occurrences of a colon followed by any number of non-colon characters (?::[^:]\*){3}, anchored at the end of the line $.

In simpler terms, this command searches for a sequence of digits that is followed by exactly three colons (with any number of non-colon characters in between) before the end of the line, and outputs only the digits.

1. Find out the GID of the created user;

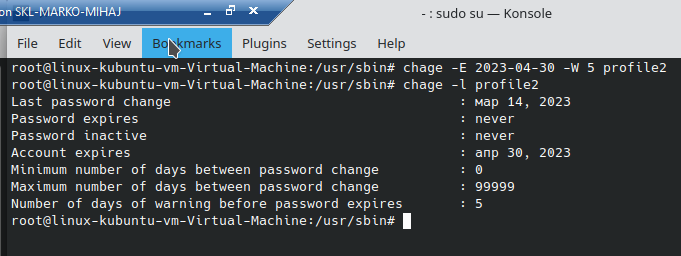


1. Change the password of the user and force it to change the pass on his next login;



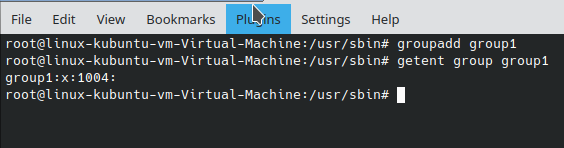
Passwd flag -e (expire password)

1. Add a new user and set an expiration date for it, with a five-day warning period;



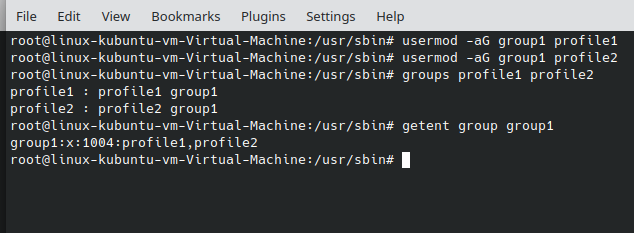
Chage – change user expiry info; flag -E (expire date), flag -W (warn days)

1. Create a new group;



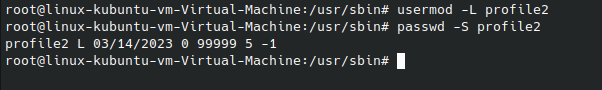
Confirming that the group is created.

1. Assign the two new users to that group;



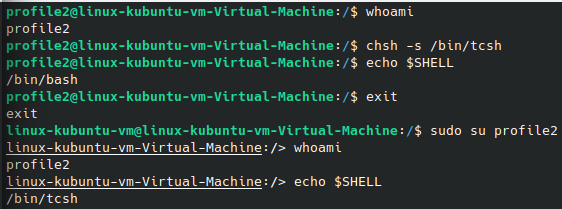
Usermod flags -a (append; add user to group) use only with -G option (groups). Confirming that users were added to said group.

1. Lock one of the user accounts;



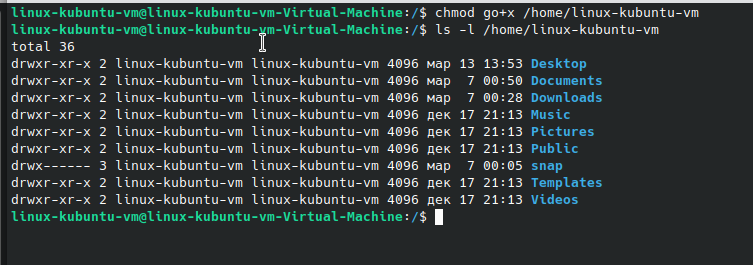
Locking profile2, then checking the state (L) – locked.

1. Change the shell of one user to tcsh;



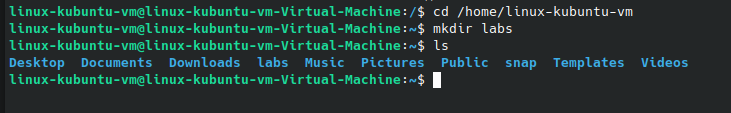
After unlocking profile2 with usermod -U and switching to it.. and installing tcsh because it was not present with sudo apt-get install tcsh.. changing the shell for the user while being logged on. Afterwards we need to re-log to perceive the changed shell env.

1. Make sure your home directory has “execute” access enabled for group and other.

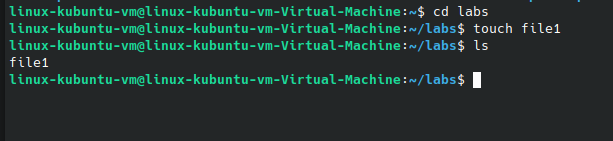


Adding the execute permission for group and other symbolized by g and o respectively. Long listing to see that group has execute/read permissions and other has execute in our Home folder. Change successful.

1. Change to your home directory, and create a directory called labs;

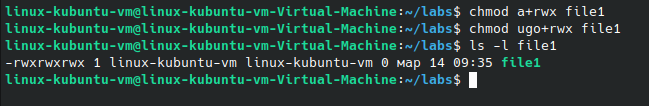


1. Create an empty file in labs directory



Creating the empty file then listing to confirm presence in folder.

1. Change permissions of file to rwx-rwx-rwx



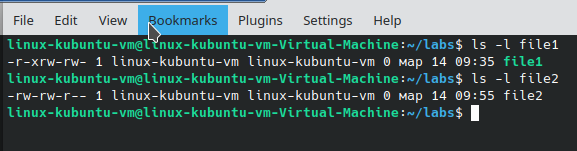
Provided 2 ways of going about it. Flag a for chmod means all permissions change to read/write/execute. Flags ugo mean u-owner/group/others all get rwx permissions. (never assigning permissions via the numbers flag route)

1. List the file. What color is the file?



File is with green colour because it has execute permission added.

1. Change the permissions back to rx-rw-rw



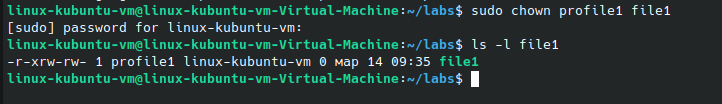
Changed permissions to rx-rw-rw although those were not the original ones when creating the file, the original ones are in the screenshot below. ( with listed example for default permissions assigned when creating a file). rw-rw-r instead of rx-rw-rw.

1. Check what owners does the file have.

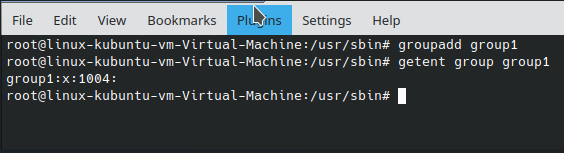


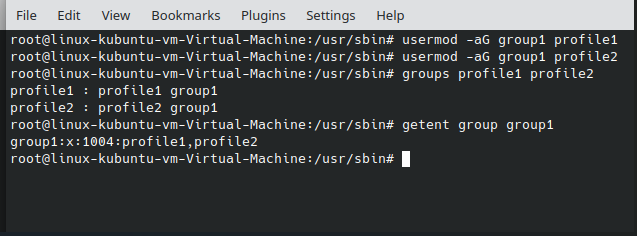
A file can have one owner – linux-kubuntu-vm user in this case.

1. Change the user ownership of the file to another user;



1. Create a group called group1 and assign two users to the group;

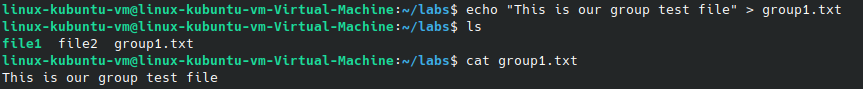




Using the group1 from before with the assigned users, as I accidentally created what is required here.

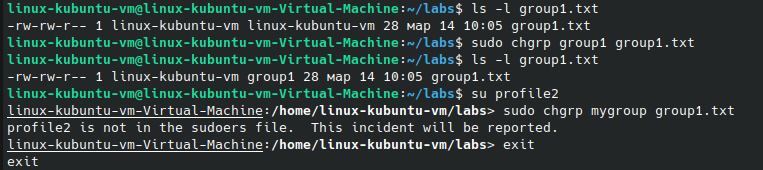
22. Create a file called group1.txt and redirect below input into the file:

“This is our group test file”.



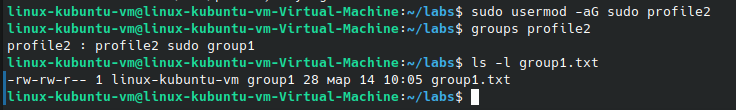
Redirecting output with > into group1.txt and listing contents of file.

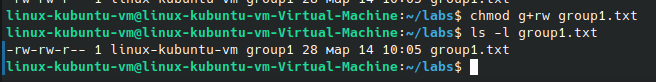
23. Change the group of the file to one of your users;



Similar to chown, chgrp changes the group ownership in this case. By default ownership from the beginning of the example above is with linux-kubuntu-vm group because when the user was created by default it created a group with that name and he the user is the only member of the group. We can change group ownership by changing with an explicitly stated group or by logging into the user that we want his group to be the group owner of the file and stating mygroup in the command.

24. Give members of the group group1 read/write access to this file?





In my case they already have it as group1 is already group owner of the file and there is r/w access for group already granted by default when creating the file. All that was needed is for the file to be in group ownership of the respective group.

End of file.