# Linux Lab 2, users and groups

# Hand In: Turn in your answers for the last questions marked with \*\*

## Reading

Read the PowerPoint in Canvas entitled Linux Users and Groups

Read (or listen to) CyberAces Module 1 Linux, Session 4, Users and Groups   
Scroll down to Users and Groups <https://www.sans.org/cyberaces/introduction-to-operating-systems/?_ga=2.155066296.1056401615.1661261021-1397954398.1658280660>

Or download the PDF  
<https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt3f5717350ede5fd4/625458ad02d8144fd4daa9e3/CyberAces_Module1-Linux_4_UsersAndGroups.pdf>

Read about su and sudo in “The Linux Command Line”, from “Changing Identities” in Chapter 9 to the end of the chapter, pp 87-93 (printed version) or pp 101 - 109 in the pdf.  
The Linux Command Line website:  
<https://linuxcommand.org/tlcl.php>

Download a PDF of the book.  
<https://sourceforge.net/projects/linuxcommand/files/TLCL/19.01/TLCL-19.01.pdf/download>

## Lab

Ubuntu locks the root account for security reasons, but most other distributions do not. To give you practice in the way other distributions use the su command, we will enable the root account by giving it a password. Do not fall into the habit that Ubuntu is trying to prevent, which is running everything as the root user!

Enter this command to assign a password to the root account:  
sudo passwd root  
Then enter the password twice.  
Obviously, you want to remember the password…

1. Create a new user. I will refer to it as testuser, but you can call it whatever you want. Note: Remember that your regular user will not have the power to add users, so you will have to use sudo or switch to the root account with su - to get root privileges. Note: The Ubuntu version of adduser takes you through entering a password and GECOS information (Ubuntu decides the GECOS/comment field should include Full Name, Room Number, Work Phone, Home Phone, and Other. You will see those in the /etc/passwd file, separated by commas. The separator between the main fields of /etc/passwd like username, password, etc., is a colon (‘:’).
2. Give testuser a password, hopefully something you can remember.
3. Change to user testuser. If you are comfortable switching users at the terminal, you can just use the command  
   su - testuser  
   If you get confused over which user account you are using, log out and log back in as testuser.
4. Try to use sudo when you are logged in as test user, sudo plus some command. For example, you could use sudo ls (sudo will check your password and membership in the sudoers file, even if the command you use doesn’t require extra rights.) It should not work, because you haven’t given testuser permission to use sudo.
5. By default, in Ubuntu, members of the groups named “adm” and “sudo” have access to the sudo command; in CentOS, the “wheel” group gives access. Use a command from the slides to add testuser to the sudo group (or wheel for CentOS.) Note: there is also a command usermod, but it has a gotcha--if you are not careful, you'll give testuser membership in sudo but remove all its other groups (see \*, below). (You’ll have to add testuser to the sudo group as root. Use su - to become root, add testuser to the sudo group, and then exit to be back to testuser.)
6. Once testuser is in the group sudo (wheel for CentOS) try sudo again. You will need to exit the current terminal and open a new one to get Ubuntu to check the sudoers file. Then it should work.
7. Use su - to become root. Examine the file, /etc/sudoers, using less. You should be able to find the line that allows root to use sudo for ALL commands, and other lines that allow members of the adm and sudo groups to do the same. The sudoers file can also give users the permission to run selected commands. Some installations give all users permission to mount CD-ROMs or shutdown the computer by adding lines to /etc/sudoers.
8. Use the less command to examine the /etc/group file. You should see that the user you installed Ubuntu with is a member of adm, sudo (wheel for CentOS), and several other groups.
9. Use privileged access (either su - to get to the root account, or sudo from your own account) to remove testuser from the sudo group  
   gpasswd -d testuser sudo (from root) (CentOS remove the user from wheel) or  
   sudo gpasswd -d testuser sudo (from your account) (CentOS remove the user from wheel.)
10. Exit from root if you used su -. Test sudo for testuser to make sure it no longer works.  
      
    Hand in
11. **\*\*** How are su and sudo different?
12. **\*\*** Write down the commands you would use to:
    1. create a user called webadmin
    2. set its password to Guru0fHtml
    3. give it the same rights to the web server that the group apache has (your VM may not have an apache group, so pretend that the group exists—or, you could create a group called apache)

**Now that you are finished, lock the root password so your VM is like normal Ubuntu again.**sudo passwd -l root   (-l is a lower case "L")

# Additional Notes to describe the usermod “gotcha”

The usermod command will replace the list of supplementary groups with the new one unless you tell it to append.

[root@john ~]# usermod --help

Usage: usermod [options] LOGIN

Options:

-c, --comment COMMENT new value of the GECOS field

-d, --home HOME\_DIR new home directory for the user account

-e, --expiredate EXPIRE\_DATE set account expiration date to EXPIRE\_DATE

-f, --inactive INACTIVE set password inactive after expiration

to INACTIVE

-g, --gid GROUP force use GROUP as new primary group

-G, --groups GROUPS new list of supplementary GROUPS

-a, --append append the user to the supplemental GROUPS

mentioned by the -G option without removing

him/her from other groups

-h, --help display this help message and exit

-l, --login NEW\_LOGIN new value of the login name

-L, --lock lock the user account

-m, --move-home move contents of the home directory to the

new location (use only with -d)

-o, --non-unique allow using duplicate (non-unique) UID

-p, --password PASSWORD use encrypted password for the new password

-R, --root CHROOT\_DIR directory to chroot into

-s, --shell SHELL new login shell for the user account

-u, --uid UID new UID for the user account

-U, --unlock unlock the user account

-Z, --selinux-user SEUSER new SELinux user mapping for the user account

[root@john ~]# usermod -G wheel testuser (Removes supplementary groups, changes primary to wheel)

[root@john ~]# usermod -a -G wheel testuser (adds wheel as a supplementary group, leaves the rest unchanged)