AACS2284 Operating Systems

**Practical 3: Managing Linux Permissions and Ownership**

Q1. Fill in the following commands:

|  |  |  |
| --- | --- | --- |
| Id user | Display information about a user’s UID and which groups she is assigned to |  |
| Groups user | Display information on the groups in which you are a member |  |
| sudo tail -3 /etc/passwd | User and Group Configuration Files to store information for each user such as the user name, the UID, the home directory, and the standard shell |  |
| sudo tail -3 /etc/group | User and Group Configuration Files to store group information such as the group name, the GID, the members of the group |  |
| sudo tail -3 /etc/shadow | User and Group Configuration Files to store encrypted user password and password expiration information |  |
| sudo adduser user\_1 | To create user account | Useradd option <username> |
| sudo usermod -u {UID} user | To modify settings for an existing user account | Usermod option <username> |
| sudo userdel -r user | To delete an existing user account | Userdel option <username> |
| Sudo passwd stud\_1 | To establish or change the password of a user account |  |
| Sudo groupadd -g GID newGrp | To add group account for the particular user |  |
| Sudo groupdel stud\_2 | To delete group account |  |
| sudo groupmod -g GID grpName | To modify the setting (GID, group name, users) for an existing group |  |
| usermod -g GID stud\_1 | To change the effective group of the executing user |  |
| Sudo gpasswd user\_1 | To change password for group accounts |  |
| chmod | To change file permission |  |
| umask | To modify default access permission |  |

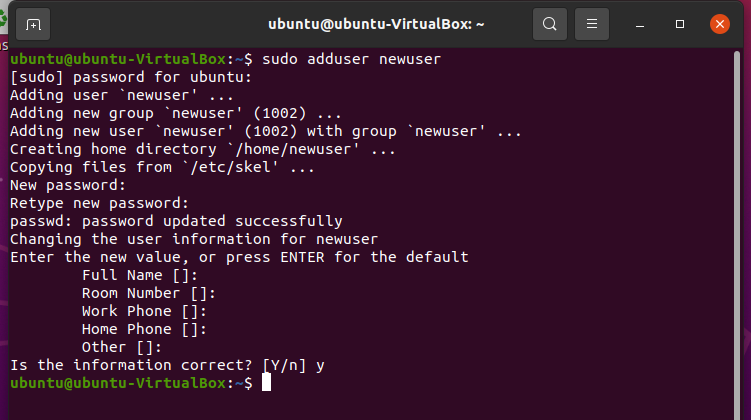
AACS2284 Operating Systems

|  |  |  |
| --- | --- | --- |
| Chown grpName file | To change the file ownership |  |
| Chgrp grpName file | To change the file ownership for group |  |

Q2. Perform the following operations in UNIX command line interface:

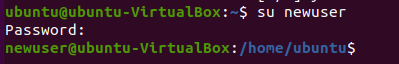
1. Add a user called “**newuser**” in the system.

Sudo adduser newuser



1. By using **su** command, switch to the **newuser** account.

Su newuser

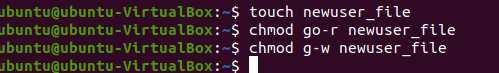


1. Create a file called “**newuser\_file**” with the following mode “**rw-------**”.

Touch newuser\_file

Chmod go-r newuser\_file

Chmod g-w newuser\_file



1. Logout **newuser** account and back to your current account.

Exit



1. Create a directory called “**currentuser\_dir**” under **/home/administrator** with the mode **“rw-r-- r--”**.

Mkdir currentuser\_dir

Chmod a-x currentuser\_dir

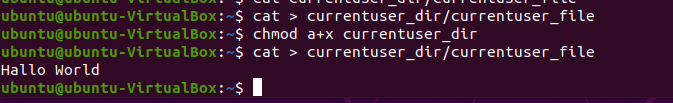


1. Create a file called “**currentuser\_file**” with default mode inside **currentuser\_dir**. Can you create the file in the directory? If not, make necessary modification on the directory’s mode. Enter “**Hallo World.**”

Cat > currentuser\_dir/currentuser\_file

Chmod a+x currentuser\_dir

Cat > currentuser\_dir/currentuser\_file



g. View **currentuser\_file**using **“cat”** command. What message did you get?

Cat currentuser\_dir/currentuser\_file



1. In the current account, view **newuser\_file** using “**cat**” command. What message did you get? Why?

Cat/home/newuser/newuser\_file

It is because the file does not given any permission to other user to views.



Q3. Change the following files, which currently have **NO** permission settings, to have the specified permissions (use ls to check your result):

|  |  |  |
| --- | --- | --- |
| **File** | **Permissions** | **Command** |
| file1 | rwxrwxrwx | Chmod a=rwx file1  OR chmod 777 file1 |
| File2 | rwxr-xr-x | Chmod u+x, g=rx,o+x file2  OR chmod 755 File2 |
| file3 | rw-r--r-- | Chmod g-w file3  OR chmod 644 file3 |
| file4 | rwx------ | Chmod u+x,g-rw,o-r file4  OR chmod 700 file4 |

AACS2284 Operating Systems

Q4. Perform the following operations:

|  |  |
| --- | --- |
| Action | Command |
| A. Change to your home directory | Cd~ |
| B. Make a directory named “myfolder” | Mkdir myfolder |
| \*\*\* C. Allow group and others to be able to read and execute on your home directory (the access rights for home directory by default is already readable and executable. This question is just to show students the purpose of dot (.)) | Chmod g=rx . |
| \*\*\* D. Allow group and others to be able to read and execute on the myfolder directory (the access rights for myfolder by default is already readable and executable. This  question is just to test students in using chmod command) | Chmod go=rx myfolder |
| E. Verify the permissions on your home directory and on myfolder | Ls-l /home  Ls -l |
| F. Use touch to create an empty file named text1.txt and text2.txtinmyfolder directory | Touch myfolder/text1.txt  Touch myfolder/text2.txt |
| G. Allow group and others to be able to write all files in the myfolder directory | Chmod go+w myfolder  Chmod go+w myfolder/\* |
| H. Verify the permissions on the file(s) in myfolder directory | Ls -l myfolder/\* |

AACS2284 Operating Systems

**Extra exercises (Optional)**

Q5.

|  |  |
| --- | --- |
| 1. | To combine **/etc/passwd** with /**etc/group** and send the output into the file **users\_groups.txt Answer:**  **Cat/etx/passwd /etc/group> user\_group.txt** |
| 2. | To create a symbolic link of **doc1** file to **softlink** in your home directory  **Answer:**  **In -s doc1 softlink** |
| 3. | Display the content of **/var/log/messages** page-by-page.  **Answer:**  **More / var/log/messages** |
| 4. | Move and rename the **/tmp/file2** file to **~/my\_file2** by using a single command. **Answer:**  **Mv /tmp/file2~/my\_file2** |
| 5. | Using wildcards token, list all the files with filenames consists of exactly 4 letters and which start with the letter “M”.  **Answer:**  **Ls -M???** |
| 6. | Find all files in the /home directory that have the word “AACS2284” as part of their filename. **Answer:**  **Find/home type f -name “AACS2284”** |
| 7. | List all the directory names that exist under the /var directory  **Answer:**  **Ls -d /var/\*** |
| 8. | The vi editor can function in 2 modes, namely :\_\_\_input\_\_\_\_\_ and \_\_command\_\_\_\_\_\_ |
| 9. | Write a command to show the date and time using each of the following formats: hh: 11mm: 24  **Answer:**  **date +"yy:%Y mm:%m dd:%d hh:%H mm:%M ss:%S"** |
| 10. | For the **umask 272**, what will the permissions on all new files and new directories be? Express your answers in octal format.  **Anwser:** New files \_\_\_404\_\_\_\_\_ and new directories\_\_\_\_505\_\_\_\_ |
| 11. | Lock the account of a user with the username **john.**  **Answer:**  usermod -L john |

AACS2284 Operating Systems

Q6. The questions below are interrelated and therefore must be done in sequence.

|  |  |  |
| --- | --- | --- |
| 1. | Create a non-empty file called **Myfile** file under your default user directory.  Create a new user called **John** | **Cat >Myfile**  **sudo adduser john** |
| 2. | Switch user to the **root user** account.  Change the ownership of **Myfile** file to **John**. | Sudo -i  ll /home/ubuntu/Myfile |
| 3. | Logout **root** user account. | Exit |
| 4. | Using a single command, switch to “**John**” account and his home directory.  Create two directories and subdirectories called **dirA/letters** and **dirB/reports** under **John** directory by using a single command. | Su - John  Mkdir -p dir A/letter dirB/reports |
| 5. | Deny all access to the “**letters**” directory by everyone except the owner. | **chmod og=-,u=- dirA/letters** |
| 6. | Change directory to **dirB/reports** using absolute pathname. Create an empty file named **OSdoc** under **dirB/reports.**  Set the permission for the file **OSdoc** to allow read and write by the file’s owner and members of the file’s owner group only. | Cd/home/John/dirB/reports  Touch Osdoc  Chmod 660 OSdoc |
| 7. | Logout **John** account and switch to your own account. | Exit |
| 8. | Change directory to John’s **dirA/letters** using relative pathname.  Can this be done? If not, why not? | Cd ../John/dirA/letters    **Cant, only owner has the permission on dirA/letters.** |