“Київський фаховий коледж зв’язку”

Циклова комісія Комп’ютерної інженерії

**ЗВІТ ПО ВИКОНАННЮ**

**ЛАБОРАТОРНОЇ РОБОТИ №10**

з дисципліни: «Операційні системи»

**Тема: “Зміна власників і прав доступу до файлів в Linux. Спеціальні каталоги тафайли в Linux”**

Виконали студенти

Групи КСМ – 13а

Команда Better Call Chekh:

Бродзінський Є.В.

Кравченко Т.І.

Тунда Р.О.

Перевірив викладач

Сушанова В.С.

Київ 2023

**Мета роботи:**

**1. Отримання практичних навиків роботи з командною оболонкою Bash.**

**2. Знайомство з базовими діями при зміні власників файлів.**

**3. Знайомство з базовими діями при зміні прав доступу до файлів**

**4. Знайомство з спеціальними каталогами та файлами в Linux.**

**Матеріальне забезпечення занять**

**1. ЕОМ типу IBM PC.**

**2. ОС сімейства Windows (Windows 7).**

**3. Віртуальна машина – Virtual Box (Oracle).**

**4. Операційна система GNU/Linux – CentOS.**

**5. Сайт мережевої академії Cisco netacad.com та його онлайн курси по Linux**

**Завдання для попередньої підготовки**

***Готував матеріал студент Бродзінський Є.В.***

1. Прочитайте короткі теоретичні відомості до лабораторної роботи та зробіть невеликий словник базових англійських термінів з питань призначення команд та їх параметрів.

| **Термін англійською** | **Термін українською** |
| --- | --- |
| File Ownership | Власність файлу |
| User Owner | Власник файлу |
| Group Owner | Груповий власник файлу |
| File and Directory Permissions | Дозволи на файли і директорії |
| FAT32, NTFS, exFAT, ReFS | Різні типи файлових систем в ОС Windows 10 |
| Streamlining | Оптимізація, спрощення |
| Administrator Actions | Дії адміністратора |
| Permissions Adjustment | Зміна дозволів |
| User Interaction Commands | Команди взаємодії користувача |
| setuid, setgid, sticky bit | Спеціальні дозволи для вирішення питань безпеки |

2. Вивчіть матеріали онлайн-курсу “NDG Linux Essentials” (netacad.com):

- Chapter 17 - Ownership and Permissions

- Chapter 18 - Special Directories and Files

3. Пройдіть тестування у курсі NDG Linux Essentials за такими темами:

- Chapter 17 Exam

- Chapter 18 Exam

4. На базі розглянутого матеріалу дайте відповіді на наступні питання:

4.1. Яке призначення команди id?

The id command displays the user identifier (UID) and the process identifier (PID).

4.2. Як переглянути які права доступу має власник файлу?

To see what access rights the owner of the file has, you need to enter the ls -l command. This command displays a list of files and directories in the current directory and their permissions.

4.3. Як змінити власника групи?

To change the owner of a group, we will use the chown command.

4.4. Як можна переглянути у терміналі який тип поточного файлу? Наведіть приклади для різних типів файлів

To view the current file type in the terminal, use the file command.

Examples:

1 Text file:

$ file test.txt

test.txt: ASCII text

2) Sound file:

$ file audio.mp3

audio.mp3: MPEG audio file

3) Video file:

$ file video.mp4

video.mp4: MPEG-4 video file

4.5. Для чого використовуються дозволи Setuid та Setgid?

Setuid and Setgid permissions are used to allow users to run executable files or open directories with the owner or group permissions of the file or directory.

4.6. Для чого в системі потрібен так званий “липкий біт” (Sticky Bit). Наведіть приклади коли цей дозвіл доцільно використовувати.

Sticky Bit is used for directories that contain temporary files, such as the /tmp directory. This allows the user to create temporary files in this directory, but does not allow the user to delete or move files created by other users.

Examples:

1) For directories that contain temporary files: Sticky Bit allows users to create temporary files in that directory, but does not allow them to delete or move files created by other users. This helps prevent important temporary files from being accidentally deleted or moved.

2) For directories that contain files that should be accessible to all users but that should not be modified: Sticky Bit allows all users to read and execute files in that directory, but does not allow them to modify them. This helps protect files from unauthorized changes.

3) For directories that contain files that should only be accessible to a specific group of users: Sticky Bit allows only users who are members of the directory's owner group to create, read, execute, and delete files in that directory. This helps protect files from unauthorized access.

5. Підготувати в електронному вигляді початковий варіант звіту:

- Титульний аркуш, тема та мета роботи

- Словник термінів

- Відповіді на п.4.1-4.6 з завдань для попередньої підготовки

**Хід роботи**

1. Початкова робота в CLI-режимі в Linux ОС сімейства Linux:

1.1. Запустіть віртуальну машину VirtualBox, оберіть CentOS та запустіть її. Виконайте вхід в систему під користувачем: CentOS, пароль для входу: reverse (якщо виконуєте ЛР у 401 ауд.) та запустіть термінал.

1.2. Запустіть віртуальну машину Ubuntu\_PC (якщо виконуєте завдання ЛР через академію netacad)

1.3. Запустіть свою операційну систему сімейства Linux (якщо працюєте на власному ПК та її встановили) та запустіть термінал.

***Готував матеріал студент Бродзінський Є.В.***

Опрацюйте всі приклади команд, що представлені у лабораторних роботах курсу NDG Linux Essentials:

- Lab 17: Ownership and Permissions

- Lab 18: Special Directories and FilesNDG Linux Essentials - Lab 15: System and User

Security

NDG Linux Essentials - Lab 17: Ownership and Permissions

| Command name | Its purpose and functionality |
| --- | --- |
| cd /tmp | Change to the /tmp directory. |
| mkdir priv-dir pub-dir | Create two directories named priv-dir and pub-dir. |
| touch priv-dir/priv-file<br>touch pub-dir/pub-file | Create two files: priv-file in priv-dir and pub-file in pub-dir. |
| ls -l priv-dir<br>ls -l pub-dir | Display details (long format) of directories priv-dir and pub-dir. |
| ls -ld priv-dir<br>ls -l priv-dir/priv-file | Display details (long format) for priv-dir and priv-file. |
| chmod o-rx priv-dir/ | Deny read and execute access for others to the priv-dir directory. |
| ls -ld priv-dir/ | Check changes in permissions for the priv-dir directory. |
| chmod a+x file<br>chmod g-w file<br>chmod go+r file<br>chmod o=rwx | Change file permissions using the symbolic method. |
| ls -ld pub-dir/<br>chmod o+w pub-dir/<br>ls -ld pub-dir/ | Allow write access for others to the pub-dir directory. |
| ls -l priv-dir/priv-file<br>chmod g-rw,o-r priv-dir/priv-file<br>ls -l priv-dir/priv-file | Deny access for the group and others to the priv-file file. |
| ls -l pub-dir/pub-file<br>chmod a=rw pub-dir/pub-file<br>ls -l pub-dir/pub-file | Grant read and write permission to everyone for the pub-file file. |
| echo "date" > test.sh | Create a file test.sh with the content "date". |
| ./test.sh | Attempt to execute the test.sh file, resulting in an error. |
| chmod u+x test.sh<br>./test.sh | Grant execute permission to the user and execute the test.sh file. |

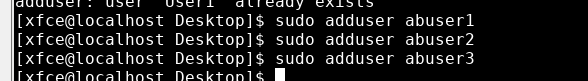
NDG Linux Essentials - Lab 18: Special Directories and Files

| ls -ld /tmp | View details of the /tmp directory. |
| --- | --- |
| ls -ld /var/tmp | View details of the /var/tmp directory. |
| ls -l /etc/shadow | View access rights for the /etc/shadow file. |
| ls -l /usr/bin/passwd | View access rights for the /usr/bin/passwd file. |
| ls -l /usr/bin/wall | View access rights for the /usr/bin/wall file. |
| echo "data" > source | Create a file named source with the content "data". |
| ls -li source | View information about the inode and details of the source file. |
| ln source hardlink | Create a hard link to the source file. |
| ls -li source hardlink | View information about the inode and details of the source and hardlink files. |
| ln hardlink hardlinktwo | Create another hard link to the source file. |
| ls -li hardlink hardlinktwo source | View information about the inode and details of the source, hardlink, and hardlinktwo files. |
| rm hardlinktwo | Remove one of the hard links (hardlinktwo). |
| ls -li source hardlink | View information about the inode and details of the source and hardlink files. |
| rm hardlink | Remove the other hard link (hardlink). |
| ls -li source | View information about the inode and details of the source file. |
| ln -s source softlink | Create a symbolic link (softlink) to the source file. |
| ls -li source softlink | View information about the inode and details of the source and softlink files. |
| ln -s /proc crossdir | Create a symbolic link (crossdir) to the /proc directory. |
| ls -l crossdir | View details of the symbolic link crossdir. |

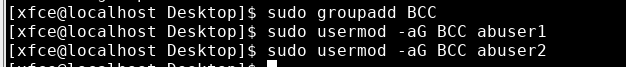
***Готував матеріал студент Тунда Р.***

4. Виконайте наступні практичні завдання у терміналі наступні дії (продемонструвати скріншоти):

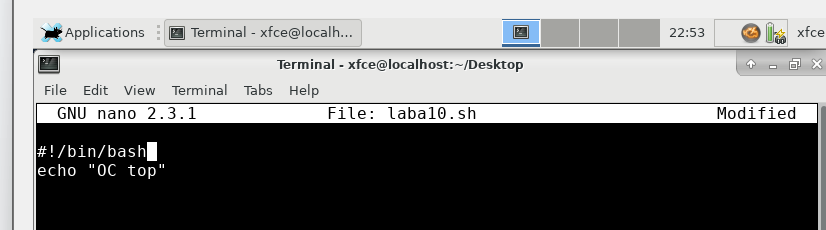
- створіть трьох нових користувачів;

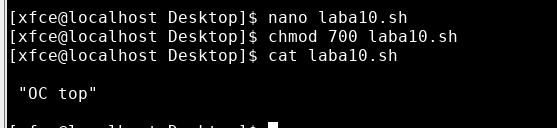


- створіть нову групу користувачів, туди додайте двох, з трьох створених користувачів;



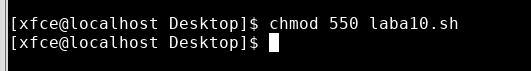
- створіть новий файл, який буде доступний на зчитування, редагування та виконання власником файлу, наприклад найпростіший скриптовий сценарій;



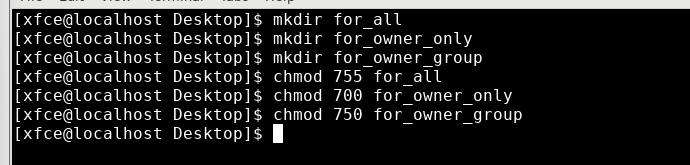


- для користувачів групи власника надайте дозволи на перегляд та виконання (без дозволу на редагування) цього файлу;

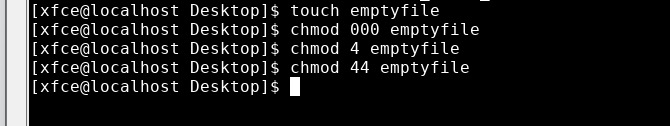
- для інших користувачів заборонити доступ до цього файлу;



- подібні дії виконайте для директорій - створіть директорію, яка буде доступна для всіх трьох користувачів, створіть директорію, яку буде доступна тільки для власника, створіть директорію, яку користувачі групи власника зможуть переглядати, але не редагувати;



- створіть порожній файл під назвою emptyfile за допомогою команди touch emptyfile. Тепер “обнуліть” дозволи для файлу з chmod 000 emptyfile. Що станеться, якщо змінити дозволи для emptyfile, передавши лише одне значення для chmod у числовому режимі, наприклад, chmod 4 emptyfile? Що буде, якщо ми використаємо два числа, наприклад chmod 44 emptyfile? Що ми можемо дізнатися про те, як chmod зчитує числове значення?



Перша команда: файл emptyfile буде існувати, але не буде доступний ні для читання, ні для запису, ні для виконання для жодного користувача

Друга команда: введене одне значення 4 встановить тільки право на читання власнику файлу. Інші права для власника, групи та інших користувачів не будуть змінені

Третя команда: введені два значення 44 встановлять права для власника та групи, але не встановлять жодних прав для інших користувачів. Це означає, що власник та користувачі групи матимуть право на читання.

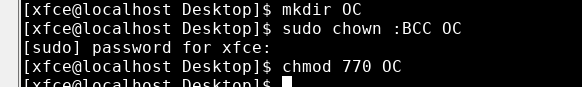
Команда chmod приймає три цифри, які представляють права доступу для власника, групи та інших користувачів. Кожна цифра в системі восьмеричного числення відповідає певному праву:

* 4 відповідає праву на читання.
* 2 відповідає праву на запис.
* 1 відповідає праву на виконання.

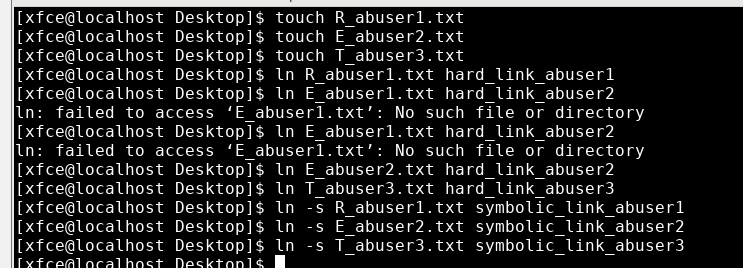
Таким чином, команда chmod 644 встановлює права на читання та запис для власника, і тільки читання для групи та інших користувачів.

Якщо ви введете лише дві цифри, команда chmod не зможе коректно інтерпретувати ці дані, оскільки потрібно три числа для представлення всіх трьох видів користувачів (власник, група, інші).

- створіть каталог під назвою, де всі файли автоматично будуть належати Вашій групі користувачів і можуть бути видалені лише користувачем, який їх створив?



- під кожним користувачем створіть по одному новому файлу, та жорстке та символічне посилання на нього;



Контрольні запитання

1. Наведіть приклади зміни прав доступу символічним методом (Symbolic Method)?

2. Наведіть приклади зміни прав доступу числовим методом (numeric method, octal method)?

3. Чи можна виконати файл, для якого є права на виконання, але не встановлені права на читання (--x)? Поясніть.

4. Яке призначення команди umask?

5. Якщо ми змінюємо права доступу та дозволи в поточній сесії чи будуть вони збережені в наступній?.

6. Чи є якийсь шаблон, яким система користується щодо прав та доступів при створенні нових файлів. Як

можна змінити права дозволу за замовчуванням?

7. Уявіть, що програмі потрібно створити одноразовий тимчасовий файл, який більше ніколи не знадобиться після закриття програми. Який правильний каталог для створення цього файлу?

8. Яким чином можна створити жорстке посилання? В яких ситуаціях їх доцільно використовувати?

9. Яким чином можна створити символічне посилання? В яких ситуаціях їх доцільно використовувати?

10. Порівняйте жорсткі та символічні посилання?

11. Є файл оригінал та для нього створено два посилання - символічне та жорстке. Що відбудеться з іншими файлами, якщо видалити:

- файл оригінал;

- символічне посилання;

- жорстке посилання.

**Conclusions:**