**"КИЇВСЬКИЙ ФАХОВИЙ КОЛЕДЖ ЗВ’ЯЗКУ"**

**Лабораторна робота 10**

з дисципліни «Операційні системи»

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

файли в Linux”

Виконали: студенти **3** курсу, групи **КСМ-13А**

**Засенко Олександр**

(прізвище та ініціали)

**Дзюбенко Дмитро**

(прізвище та ініціали)

**Сторожук Костянтин**

(прізвище та ініціали)

Київ  2023

**ЗМІСТ**

1 …………………………………………………………………………………...

2 ……………………………….

Conclusions……………………………………………………..16

**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

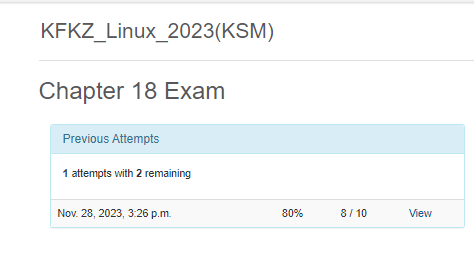
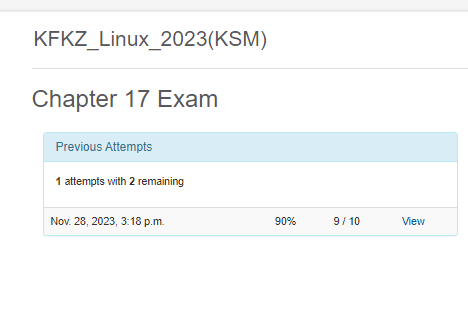
**Завдання для попередньої підготовки**

***Готував матеріал студент Zasenko***

Невеликий словник базових англійських термінів з питань призначення команд та їх параметрів.

|  |  |
| --- | --- |
| File Ownership | By default, users own the files that they create. While this ownership can be changed, this function requires  administrative privileges. Although most commands usually show the user owner as a name, the operating system is  associating the user ownership with the UID for that username. |
| Changing Groups | If you know that the file you are about to create should belong to a group different from your current primary  group, then you can use the newgrp command to change your current primary group. |
| Setuid | When the setuid permission is set on an executable binary file (a program) the binary file is run as the owner  of the file, not as the user who executed it. This permission is set on a handful of system utilities so that they can be  run by normal users, but executed with the permissions of root, providing access to system files that the normal user  doesn&#39;t normally have access to. |
| Setgid | The setgid permission is similar to setuid, but it makes use of the group owner permissions. There are two  forms of setgid permissions: setgid on a file and setgid on a directory. The behavior of setgid depends on whether it is  set on a file or directory. |

**Пройдіть тестування у курсі NDG Linux Essentials за такими темами:**



4.1. Призначення команди id:

Команда id виводить інформацію про ідентифікатор користувача (UID), групу користувача (GID) та додаткові групи користувача.

4.2. Як переглянути права доступу власника файлу:

Використовуйте команду ls -l та зверніть увагу на перші три символи виводу, які вказують на права доступу власника файлу.

4.3. Як змінити власника групи:

Використовуйте команду chown з опцією -R для зміни власника групи для всіх файлів у директорії. Приклад:

chown -R новий\_власник:нова\_група /шлях\_до\_директорії\_або\_файлу

4.4. Як переглянути тип поточного файлу:

Використовуйте команду file. Наприклад:

file текстовий\_файл.txt

file програмний\_файл

file директорія

4.5. Дозволи Setuid та Setgid:

Setuid (SUID): Дозволяє виконувати програму з правами власника файлу, незалежно від того, хто запустив програму.

Setgid (SGID): Застосовується до директорій і дозволяє новим файлам у цій директорії успадковувати групу від батьківської директорії.

4.6. "Липкий біт" (Sticky Bit):

Sticky Bit застосовується до директорій і унеможливлює видалення або перейменування файлів користувачами, крім власника файлу або адміністратора. Зазвичай використовується в директоріях, таких як /tmp, де кілька користувачів може створювати файли, і мета - унеможливити іншим користувачам випадкове видалення чи модифікацію файлів інших користувачів.

**Хід роботи  
*Готував матеріал студент Dziubenko***

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 зпустіть 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.

1. Опрацюйте всі приклади команд, що представлені у лабораторних роботах курсу NDG Linux

Essentials:

- Lab 17: Ownership and Permissions

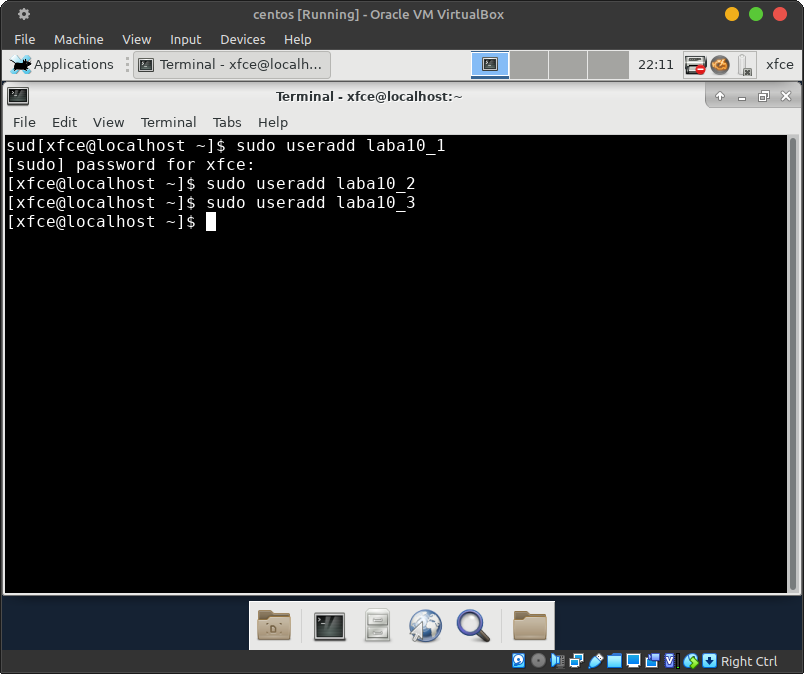
- Lab 18: Special Directories and Files

1. Створіть таблицю команд вивчених у п.2 ходу роботи у наступному вигляді:

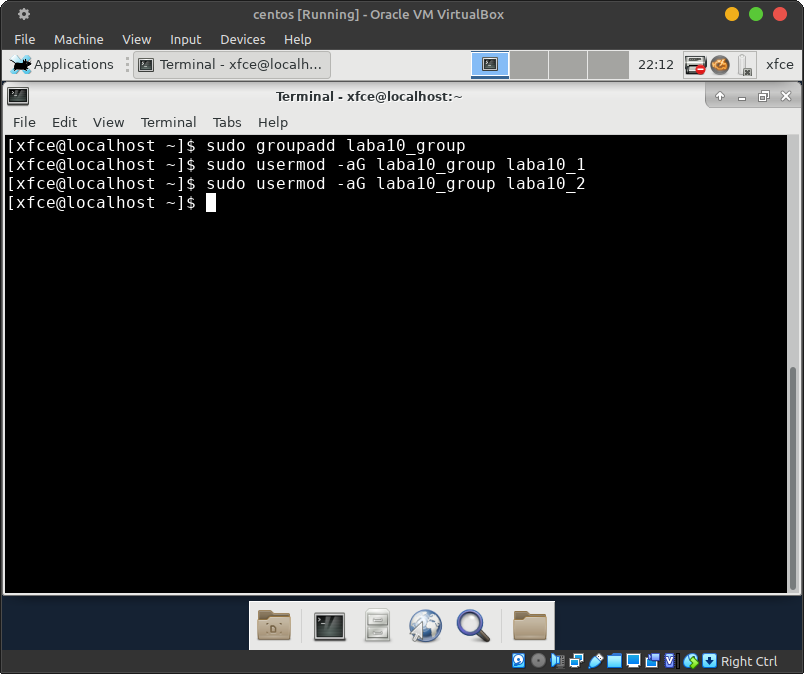
|  |  |
| --- | --- |
| Назва команди | Її призначення та функціональність |
| cd | Перехід до директорії |
| mkdir | Створення каталогу |
| touch | Створення пустого текстового документа |
| ls | Вивід на екран вміст каталогу |
| chmod | Додавання повноважень файлу |
| echo | Вивід на екран повідомлення користувачу |
| ./test.sh | Запуск виповнюваного скрипта |
| stat | Вивід статистики файлу |
| chown | Зміна користувача або групи на супер-користувача(чів) |
| chgrp | Зміна групи користувачів всіх файлів на директорію структури |
| ln | Створення посилання на файл або директорію |
| rm | Видалення файлу або каталогу |

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

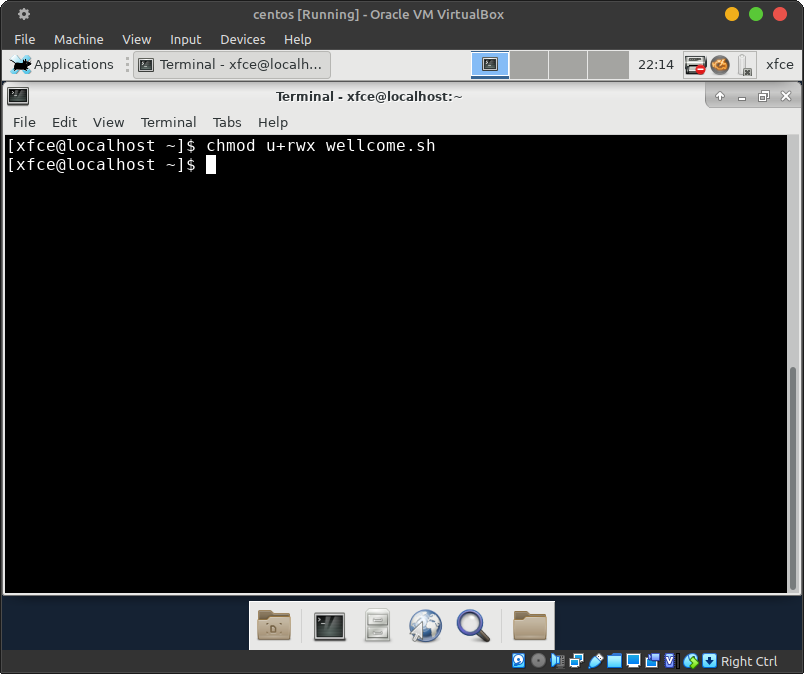
- створіть трьох нових користувачів;



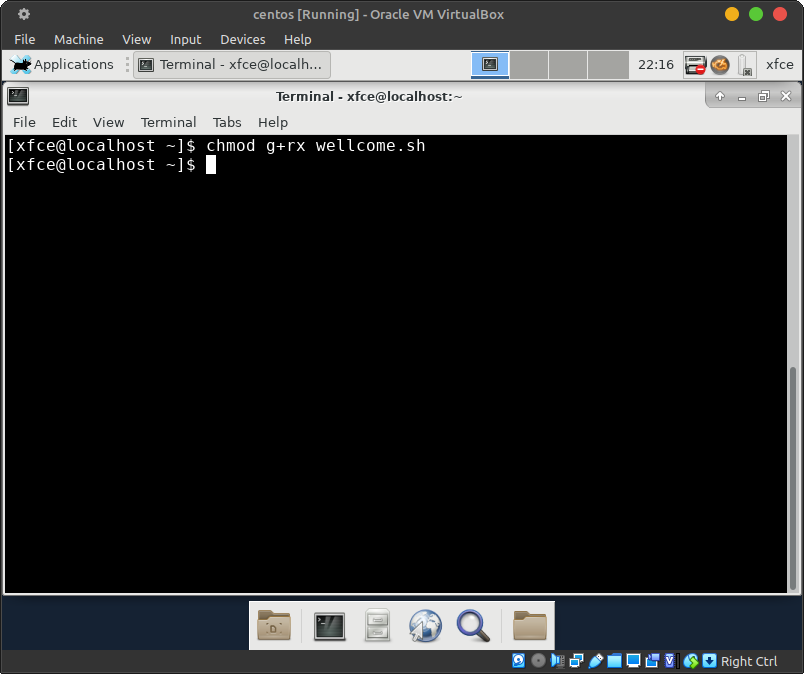
- створіть нову групу користувачів, туди додайте двох, з трьох створених користувачів;



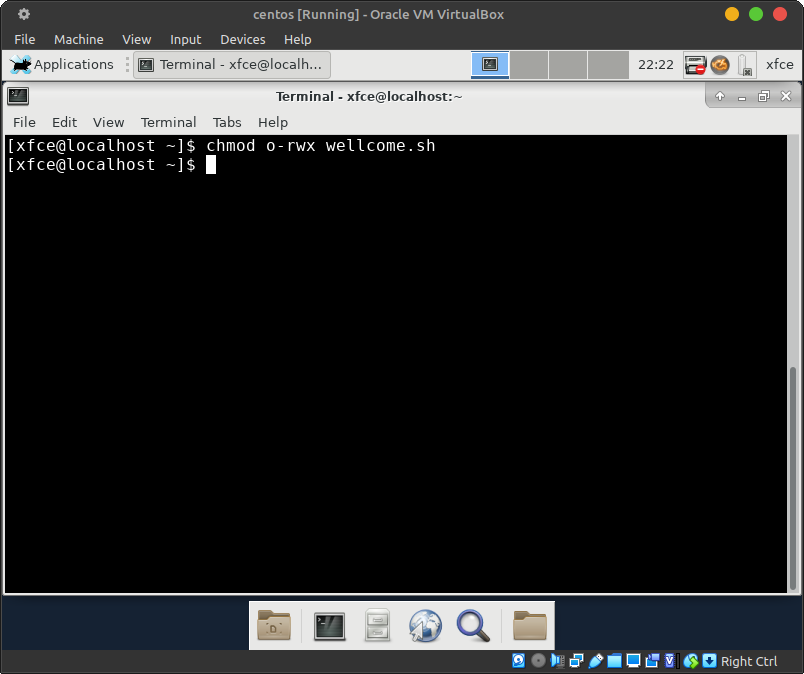
- створіть новий файл, який буде доступний на зчитування, редагування та виконання власником файлу, наприклад найпростіший скриптовий сценарій;



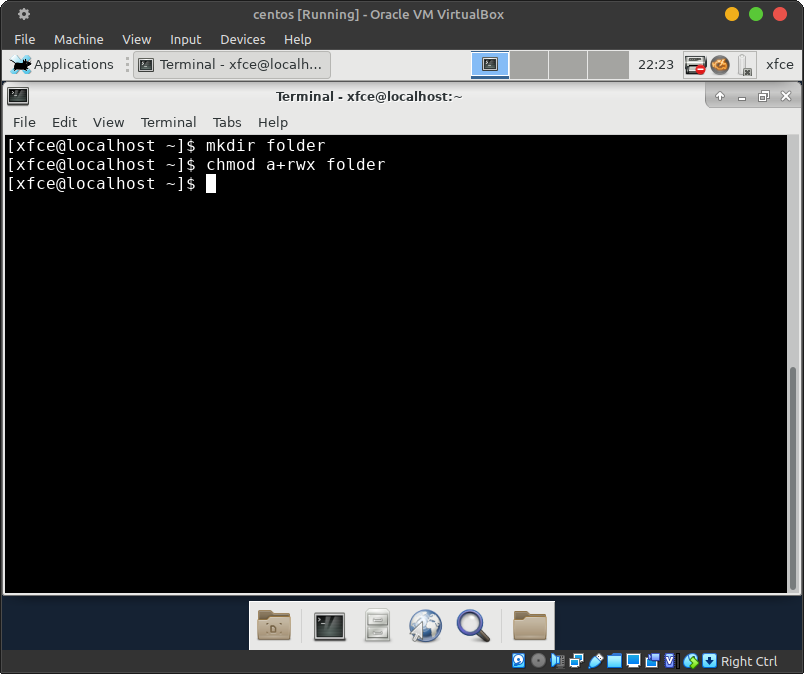
- для користувачів групи власника надайте дозволи на перегляд та виконання (без дозволу на редагування) цього файлу;

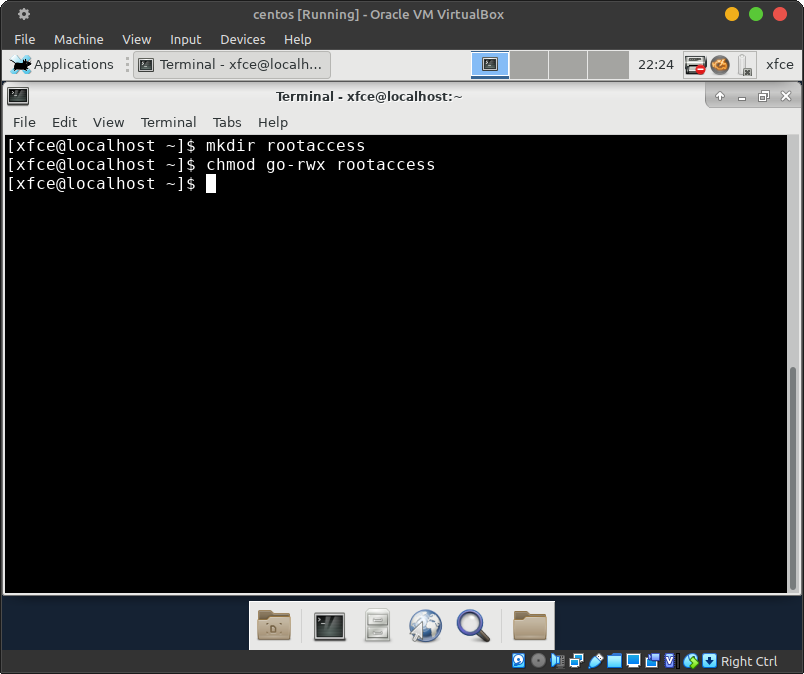


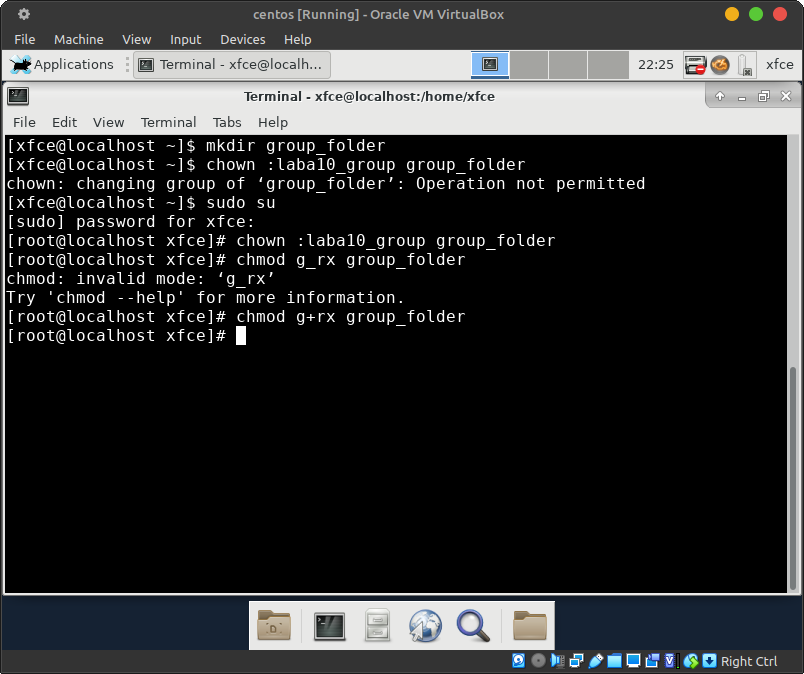
- для інших користувачів заборонити доступ до цього файлу;



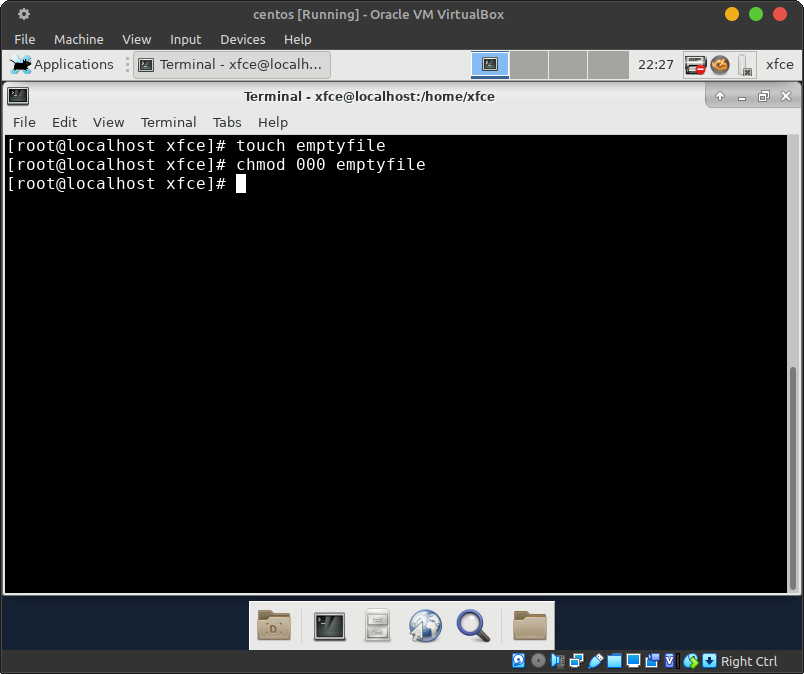
- подібні дії виконайте для директорій - створіть директорію, яка буде доступна для всіх трьох користувачів, створіть директорію, яку буде доступна тільки для власника, створіть директорію, яку користувачі групи власника зможуть переглядати, але не редагувати;

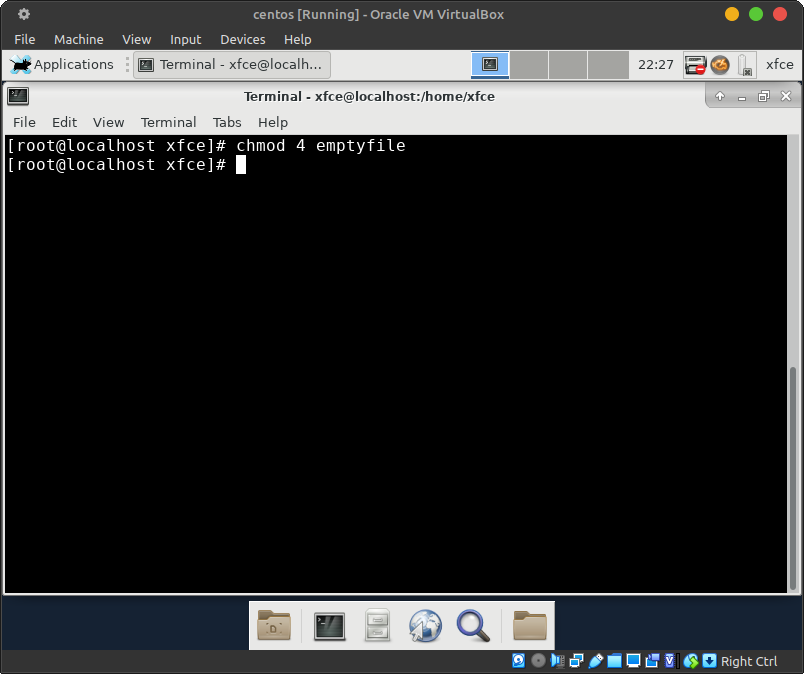




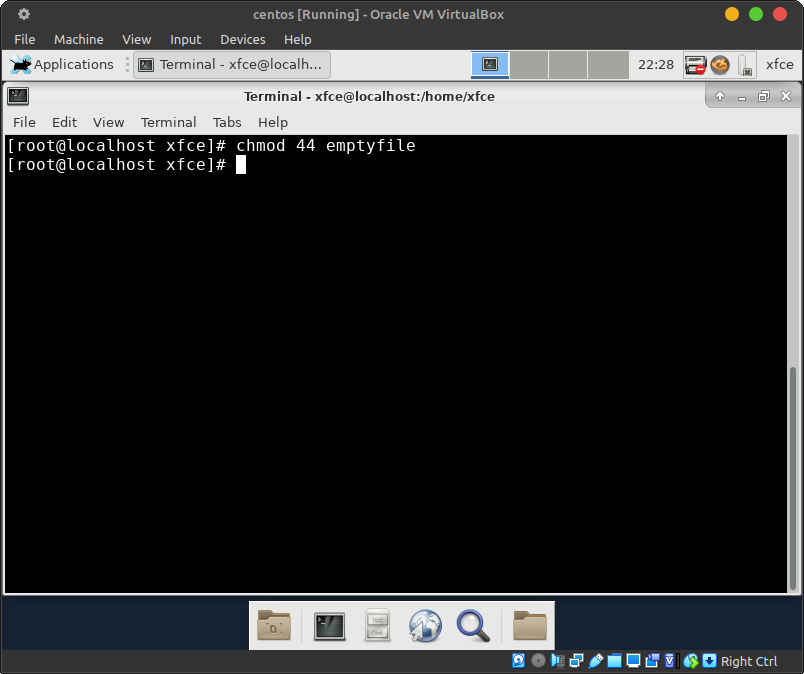


- створіть порожній файл під назвою emptyfile за допомогою команди touch emptyfile. Тепер “обнуліть” дозволи для файлу з chmod 000 emptyfile. Що станеться, якщо змінити дозволи для emptyfile, передавши лише одне значення для chmod у числовому режимі, наприклад, chmod 4 emptyfile? Що буде, якщо ми використаємо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



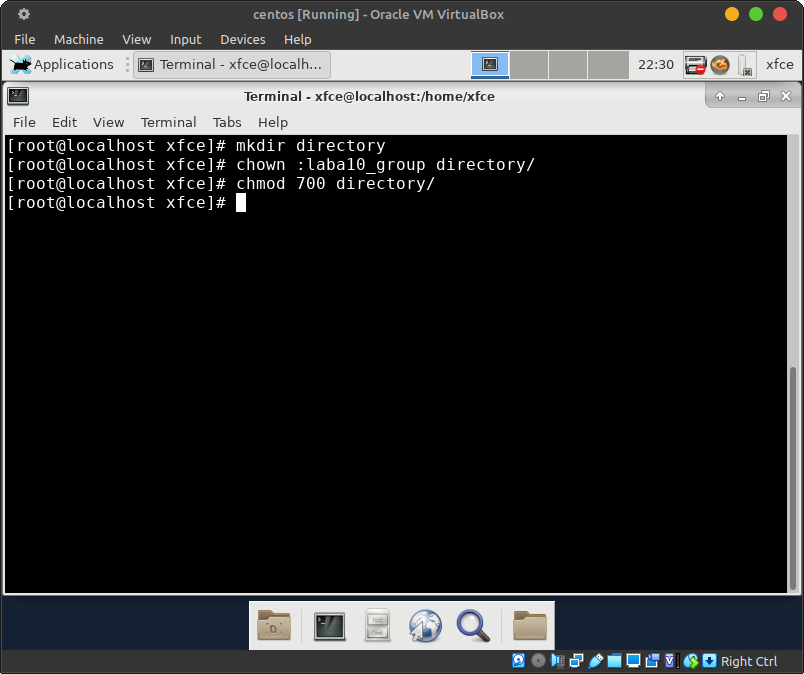


Це надасть власнику файлу право на читання, а інші дозволи будуть вимкнені для всіх користувачів.

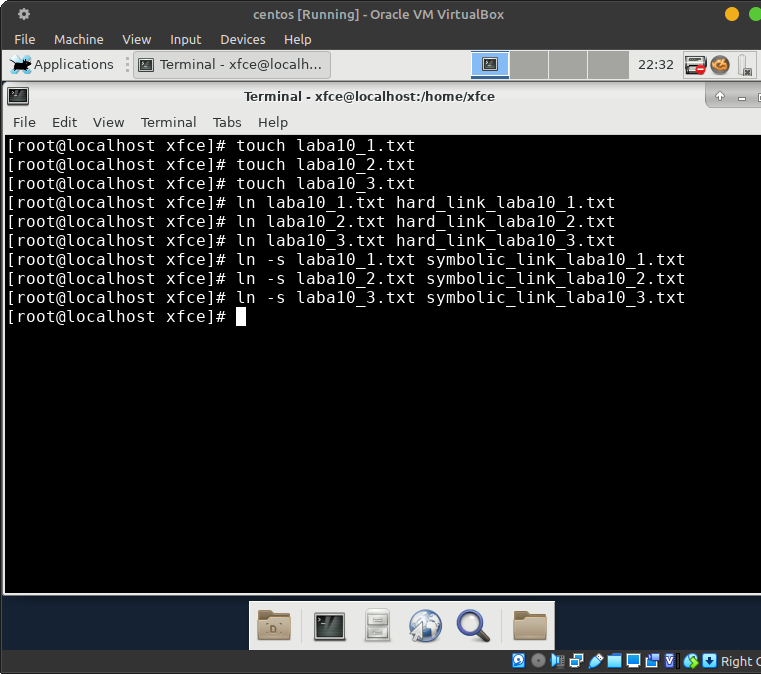


Теж надасть права на читання як власнику, так і групі. Але ці дозволи для інших користувачів залишаться нульовими.

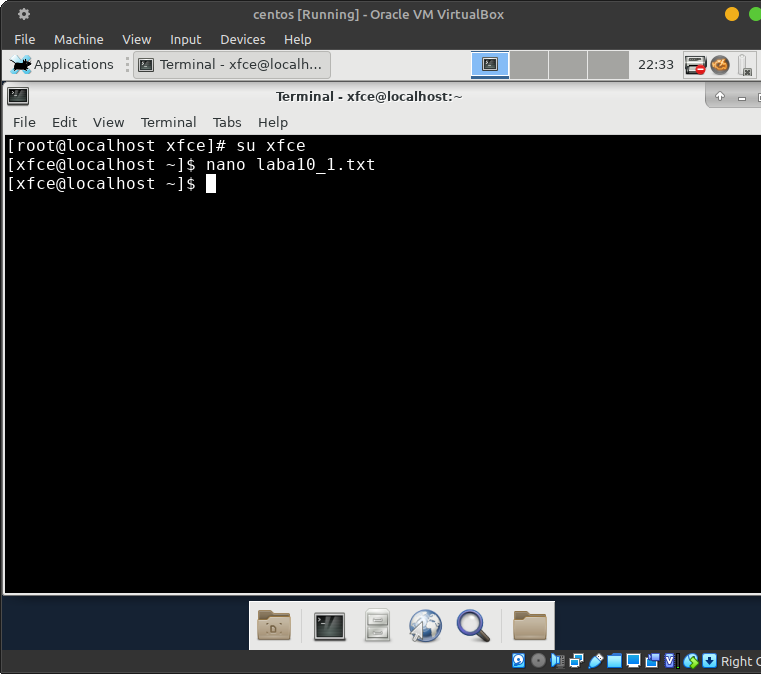
- створіть каталог під назвою, де всі файли автоматично будуть належати Вашій групі користувачів і можуть бути видалені лише користувачем, який їх створив?



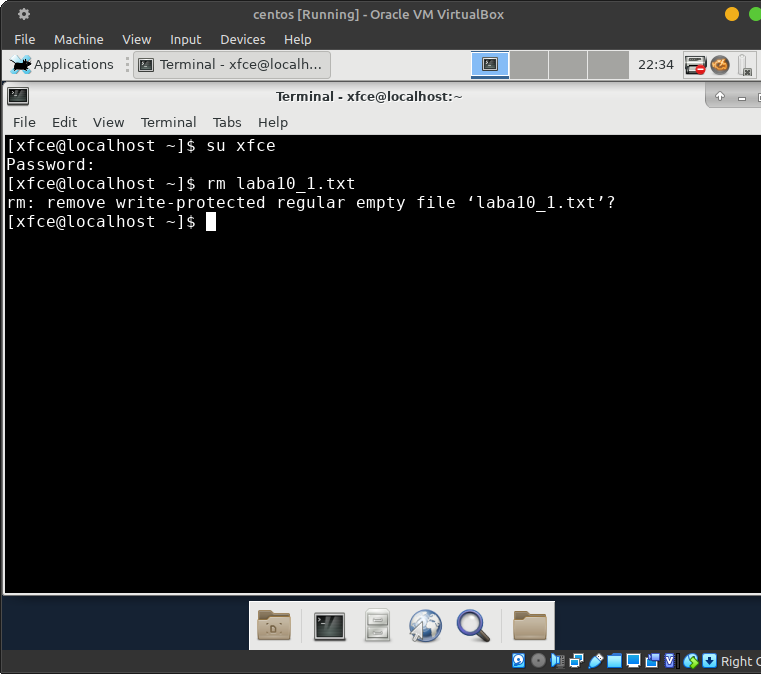
- під кожним користувачем створіть по одному новому файлу, та жорстке та символічне посилання на нього;



- спробуйте іншими користувачами переглянути ці файли;



- спробуйте іншими користувачами видалити ці файли, зробіть висновки.



Здебільшого користувачі можуть видаляти свої файли та посилання, але не можуть видаляти файли інших користувачів, які мають встановлені адекватні права доступу.

**Контрольні запитання:**

**Conclusions**