“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 та файли в Linux”**

Виконали студенти

групи РПЗ-13А та РПЗ-13Б

Eleven Two Zeroes:

Vlad Sapozhnyk

Max Karpenko

Dmytro Onufriiev

Київ 2024

Робота студентів групи РПЗ-13А та РПЗ-13Б Eleven Two Zeroes: Vlad Sapozhnyk, Max Karpenko and Dmytro Onufriiev.

**Мета роботи:**

1. Отримання практичних навиків роботи з командною оболонкою Bash.
2. Знайомство з базовими діями при зміні власників файлів, .прав доступу до файлів
3. Знайомство з спеціальними каталогами та файлами в Linux.

**Матеріальне забезпечення занять:**

1. ЕОМ типу IBM PC.
2. ОС сімейства Windows та віртуальна машина Virtual Box (Oracle).
3. ОС GNU/Linux (будь-який дистрибутив).
4. Сайт мережевої академії Cisco netacad.com та його онлайн курси по Linux

**Завдання для попередньої підготовки: *Created by Vlad Sapozhnyk***

1. **Яке призначення команди id?**

The id command is a versatile tool used to display information about the current user or a specified user, including their user ID (UID), group ID (GID), and group memberships. It's a fundamental command for understanding user privileges and group associations in Unix-like operating systems.

1. **Як переглянути які права доступу має власник файлу?**

To view the permissions for the owner of a file, you can use the ls command along with the -l (long listing) option and the file path. The owner's permissions will be represented by the first three characters of the permission string.

*ls -l [file path]*

1. **\*Як змінити власника групи?**

To change the owner of a group in Linux, you can use the chgrp command followed by the new owner's username and the group name. For example, to change the owner of the group "sales" to the user "john", you would use the following command:

*sudo chgrp john sales*

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

*file [file path]*

1. **\*\*Для чого використовуються дозволи Setuid та Setgid?**

Setuid and Setgid are special permissions in Unix-like systems that allow a program to temporarily run with the privileges of a specific user or group, typically the root user or a group with administrative privileges. These permissions are used to grant programs the necessary access to perform certain tasks that require elevated privileges, without giving the program's actual user those same privileges.

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

A "Sticky Bit" is a special permission on a file or directory in UNIX-like operating systems such as Linux. This permission has a special meaning and is intended to provide additional security and control over access to files and directories.

The main purposes of the sticky bit:

* Prevent users who are not the file owner or administrator from deleting files: When the sticky bit is set to a directory, it prevents users who are not the owner of the file or the system administrator from deleting files from that directory. This prevents other users from accidentally deleting important files.
* Ensure security in a shared directory: If several users have access to a shared directory and they store their files there, a sticky bit can prevent accidental deletion of other people's files.

Examples of using a sticky bit:

* Temporary directories that are accessible to all users: For example, a system temporary directory (/tmp) can have a sticky bit set to prevent users who are not the owner or system administrator from deleting files. This allows users to safely work in this directory without worrying about accidentally deleting files by other users.
* Shared directories for storing important files: For example, a shared directory where users store important documents or files may have a sticky bit installed to prevent other users from accidentally deleting files.

In these cases, a sticky bit helps to increase security and control over access to files and directories in shared environments where many users have access to the same resources.

**Glossary of terms**

| **Name of term** | **Explanation** |
| --- | --- |
| File ownership | A file property that determines which user and which group has access rights to a file. |
| User owner | The user who owns the file and determines the access rights of users to this file. |
| Group owner | The group to which the file belongs and determines the access rights to the file for all users belonging to this group. |
| Administrative privileges | Administrator privileges required to perform certain actions in the system, such as changing file ownership or changing access rights. |
| UID (User ID) | A unique user identifier in the system that is used to determine the owner of a file. |
| GID (Group ID) | A unique group identifier in the system that is used to determine the ownership group of a file. |
| /etc/passwd file | A text file on Unix-like systems that contains information about system users, including their identifiers and home directories. |
| id command | A command in Unix-like systems that displays information about a user and group, including the UID, username, GID of the main group, and other groups to which the user belongs. |

**Хід роботи. *Created by Max Karpenko***

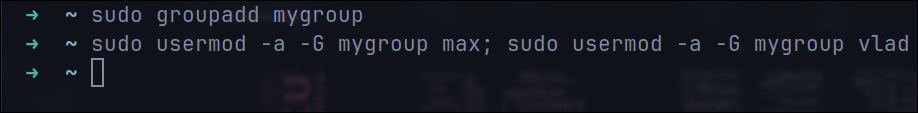
* 1. Початкова робота в CLI-режимі в Linux ОС сімейства Linux:
  2. Запустіть віртуальну машину VirtualBox, оберіть CentOS та запустіть її. Виконайте вхід в систему під користувачем: CentOS, пароль для входу: reverse ***(якщо виконуєте ЛР у 401 ауд.)*** та зпустіть термінал.
  3. Запустіть віртуальну машину Ubuntu\_PC ***(якщо виконуєте завдання ЛР через академію netacad)***
  4. Запустіть свою операційну систему сімейства Linux ***(якщо працюєте на власному ПК та її встановили)*** та запустіть термінал.
  5. Опрацюйте всі приклади команд, що представлені у лабораторних роботах курсу ***NDG Linux Essentials: Lab 17: Ownership and Permissions*** та ***Lab 18: Special Directories and Files.*** Створіть таблицю команд вивчених у п.2 ходу роботи у наступному вигляді:

| Назва команди | Її призначення та функціональність |
| --- | --- |
| ls -l | Відображає розширену інформацію про файли та директорії, включно з правами доступу, власником та групою. |
| chmod | Змінює права доступу до файлів або директорій, визначаючи, хто може читати, писати або виконувати файли. |
| chown | Змінює власника файлу або директорії, дозволяючи контролювати, хто має доступ до ресурсів. |
| chgrp | Змінює групу власності для файлів або директорій, що впливає на доступ до цих ресурсів залежно від групи користувача. |
| umask | Встановлює початкові права доступу для новостворених файлів і директорій в сесії користувача. |
| sudo | Дозволяє виконувати команди з правами суперкористувача, важлива для адміністрування системи. |
| find | Використовується для пошуку файлів в директорійній структурі на основі різних критеріїв, включаючи права доступу. |
| chmod +s | Встановлює біт setuid або setgid на виконуваних файлах, що дозволяє виконувати файл з правами власника файла або групи. |
| ln -s | Створює символьне посилання на файл або директорію, уможливлюючи легкий доступ до ресурсів через альтернативний шлях. |
| touch | Cтворює порожній файл або оновлює часові мітки існуючого файлу, часто використовується для управління файлами. |

* 1. **Виконайте наступні практичні завдання у терміналі наступні дії (продемонструвати скріншоти):**
* **створіть трьох нових користувачів;**

****

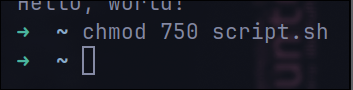
* **створіть нову групу користувачів, туди додайте двох, з трьох створених користувачів;**

****

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

****

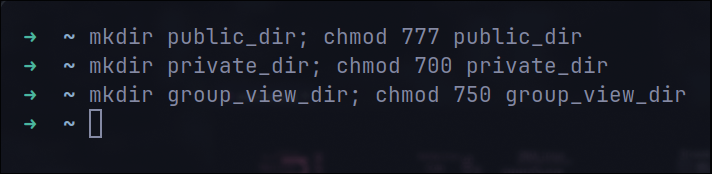
* **для користувачів групи власника надайте дозволи на перегляд та виконання (без дозволу на редагування) цього файлу;**

****

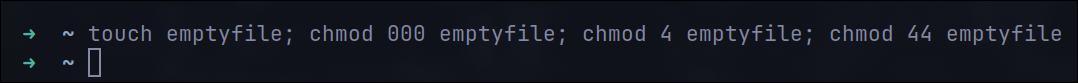
* **для інших користувачів заборонити доступ до цього файлу;**

The command above has already denied access to the file.

* **\*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;**

****

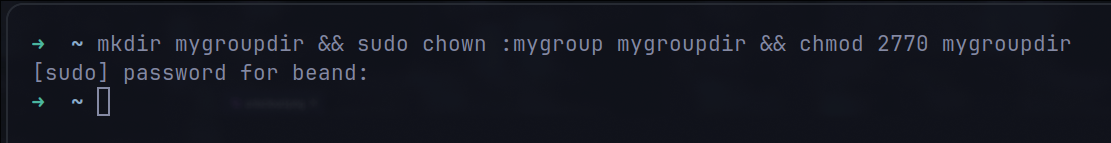
* **\*створіть порожній файл під назвою emptyfile за допомогою команди touch emptyfile. Тепер “обнуліть” дозволи для файлу з chmod 000 emptyfile. Що станеться, якщо змінити дозволи для emptyfile, передавши лише одне значення для chmod у числовому режимі, наприклад, chmod 4 emptyfile? Що буде, якщо ми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

****

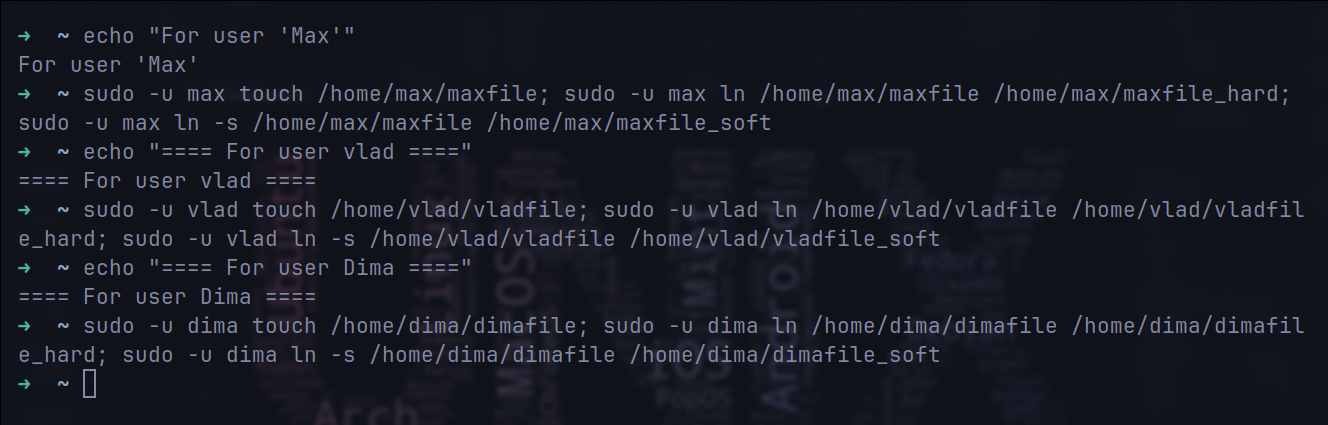
**How chmod reads a numeric value:**

chmod interprets numeric arguments as octal numbers. If fewer than three digits are specified, the missing digits are treated as leading zeros.

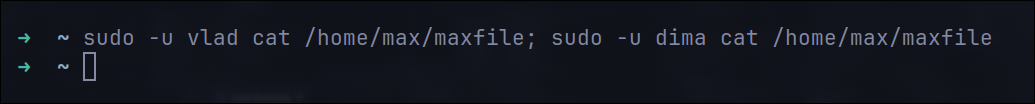
* **The first digit** from left to right corresponds to the owner's rights, the second to the group's rights, and the third to the rights of other users.
* **Each digit can be a sum:** 4 (read), 2 (write), and 1 (execute).
* **\*\*створіть каталог під назвою, де всі файли автоматично будуть належати Вашій групі користувачів і можуть бути видалені лише користувачем, який їх створив?**

****

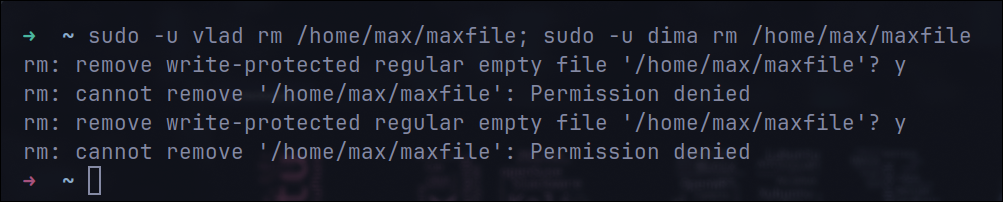
* **\*\*під кожним користувачем створіть по одному новому файлу, та жорстке та символічне посилання на нього;**

****

* **\*\*спробуйте іншими користувачами переглянути ці файли;**

****

* **\*\*спробуйте іншими користувачами видалити ці файли, зробіть висновки.**

****

**This shows that:**

* **Directory permissions on maxfile restrict users' actions -** Even if they can view files in the directory, permissions on the /home/max directory likely restrict write permissions, which is necessary to delete files.
* **Managing permissions is critical to protecting files -** Setting the proper permissions helps protect file data from improper modification or deletion, especially on multi-user systems.

**Контрольнi запитання: *Created by Dmytro Onufriiev***

**Висновок:**