“Київський фаховий коледж зв’язку”

Циклова комісія Комп’ютерної та програмної 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 КСМ 13А**

**Команда ВВС**

**Панчук О.С**

**Петрик С.С.**

**Перевірив викладач**

**Сушанова В.С.**

Київ 2023

**Мета роботи:**

1. Отримання практичних навиків роботи з командною оболонкою Bash.

2. Знайомство знайомство з базовими діями при роботі зі скриптовими сценаріями.

**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.

**Завдання для попередньої підготовки**

***Готував матеріал студент Панчук О.С***

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 |
| Setgid | Сетгід |
| To add the setuid permission symbolically, run:  chmod u+s file | Щоб символічно додати дозвіл setuid, виконайте:  chmod u+s file |
| According | За словами |
| groups you belong | групи, до яких ви належите |
| new shell; | нову оболонку; |
| GID becomes | GID стає |
| sysadmin attempts | спроби системного адміністратора |
| Setuid та Setgid? | Setuid та Setgid? |
| "sticky bit" | "липкий біт" |

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 in the Linux operating system displays information about user and group identifiers. When you execute this command in a terminal, it displays the user's user ID (UID), group ID (GID), and a list of additional groups to which the user belongs.

4.2. Як переглянути які права доступу має власник файлу?

To view the access rights of a file owner in Linux, use the ls command with the -l option. The main output of this command contains information about the access rights, owner, group, and other attributes of the file. Access rights are specified in the form of characters that define the capabilities of the file owner.

4.3. Як змінити власника групи?

To change the owner of a group in Linux, use the chown command

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

To view the type of the current file in the terminal, use the file command. This command determines the type of file and can also provide additional information about its contents.

4.5. Для чого використовуються дозволи Setuid та Setgid?

The Setuid (Set User ID) and Setgid (Set Group ID) permissions are special attributes that can be set for executable files on UNIX and similar operating systems such as Linux. These attributes affect how the file is executed and what privileges are used when it is executed.

Setuid (SUID):

When a file has the SUID bit set, it executes in the context of the file's owner, not the person who started it.

This is usually used to grant temporary execution privileges to specific users.

Most often, SUID is set on executable files that interact with system resources and may require elevated privileges (for example, a password reset program).

Setgid (SGID):

When a file has the SGID bit set, it is executed in the context of the file owner's group, not the group of the person who ran it.

This can be useful, for example, when users in the same group share files and need to share them.

SGIDs can also be used on directories so that new files created in that directory belong to the owner's group, not the group of the user who created them.

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

"The Sticky Bit is a special permission in UNIX and similar operating systems such as Linux. This bit is applied to directories and has specific functions.

The main function of the sticky bit is that it restricts the ability to delete or move files in a directory. That is, in a directory where the sticky bit is set, files can only be deleted or moved by the file owner, the owner of the directory, or the superuser.

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**

***2.Готував матеріал студент Панчук О.С.***

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

Essentials:

- Lab 17: Ownership and Permissions

- Lab 18: Special Directories and Files

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

|  |  |
| --- | --- |
| **Назва команди** | **Її призначення** |
| cd /tmp | is used to change the current working directory |
| ls -la | displays a detailed list of files and directories in the current directory, including hidden files |
| echo "date" > test.sh | you create a file called test.sh and write the line "date" into it. Note, however, that you used double quotes, so the contents of the file will be the word "date" and not the output of the date command. |
| stat test.sh | is used to display detailed information about a file or directory in the system. |
| su - | used to switch the user to another account |
| chown root:root pub-dir  ls -ld pub-dir | The chown root:root pub-dir command sets the owner and group for the pub-dir directory to the user and group root. |
| ls -ld /tmp  ls -ld /var/tmp | The ls -ld /tmp and ls -ld /var/tmp commands display information about the properties of two different temporary directories on the system. |
| cd | The cd command is used to change the current working directory in the terminal. |

***4. Готував матеріал студент Петрик С.С.***

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?

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

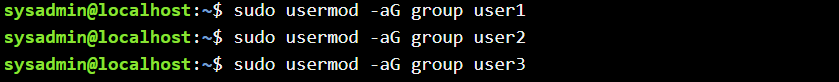
- під кожним користувачем створіть по одному новому файлу, та жорстке та символічне посилання на нього;

- спробуйте іншими користувачами переглянути ці файли;

- спробуйте іншими користувачами видалити ці файли, зробіть висновки.

***Зображення, що містить текст, знімок екрана, Шрифт

Автоматично згенерований опис***

******

***Зображення, що містить текст, знімок екрана, Шрифт

Автоматично згенерований опис***

******

For the numeric chmod mode, the first number indicates permission for the owner, the second for the group, and the third for other users. For example, a chmod 4 file will grant read-only permission to the owner, a chmod 44 file will grant read-only permission to the owner and the group. This mode allows you to change permissions for different categories of users.

******

***Зображення, що містить текст, знімок екрана, Шрифт

Автоматично згенерований опис***

***Зображення, що містить текст, знімок екрана, Шрифт

Автоматично згенерований опис***

Conclusions:

Files and links created using the ln command may be restricted from being viewed or deleted by other users who are not the owners of these objects due to access rights restrictions. To change the access rights to files for other users, you need to use access rights change commands, such as chmod, or change the owner of the file.

***Готував матеріал студент Петрик С.С.***

***Контрольні запитання:***

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

Changing permissions using the symbolic method uses the chmod command along with a symbolic representation of the permissions of files or directories. The symbolic method allows you to change individual aspects of access rights, such as owner, group, and other user rights.

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

The numeric method, also known as the octal method, uses numbers to represent access rights to files or directories. Each number corresponds to a specific set of access rights (read, write, execute) for the owner, group, and other users.

The numeric method uses values from 0 to 7, where:

0 - corresponds to no permission (no rights)

1 - corresponds to the right to execute

2 - corresponds to the right to write

4 - corresponds to the right to read

Combining these values gives different combinations of access rights.

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

Yes, you can execute a file that has execute privileges but no read privileges. On Unix-like systems, if a file has execute (--x) permissions but no read (r--) permissions, it can be executed.

Read permissions (r) indicate whether the user can view the contents of the file. Execution rights (x) indicate whether the file can be executed as a program or script. If a file has execute permissions, the operating system will be able to execute it even if it does not have read permissions.

This can be useful in cases where the file is executable program code, but the author/owner of the file does not want users to be able to read or view the contents of the file directly because of the read permissions denied. This approach can provide a certain level of security by keeping sensitive data within the program.

4. Яке призначення команди umask?

The umask command in UNIX-like operating systems sets or shows the mask level for creating permissions for new files and directories.

In mask mode, umask tells the operating system which access rights bits should be subtracted from the default permissions when creating a new file or directory. That is, it defines those rights that will not be set for newly created files and directories.

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

Changes to access rights and permissions that you make in the current session do not persist after the session ends. They apply only to the files and processes that exist at the time you make these changes. If you log out of the current session or reboot the system, the changes to access rights revert to the default values for the corresponding files and directories.

6. Чи є якийсь шаблон, яким система користується щодо прав та доступів при створенні нових файлів. Як можна змінити права дозволу за замовчуванням?

umask is a template that defines which permissions will be subtracted from the standard permissions when creating new files and directories. These values set the default permissions.

To change this pattern (umask conditions) and set different default permissions for creating files and directories, use the umask command followed by an octal number, for example umask 022

Here, 022 indicates that when creating new files and directories, the group and other users will not be allowed to write, but they will have read access.

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

It is best to use a system directory for temporary files, such as /tmp (or /var/tmp on some systems), to create a temporary file.

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

Hard links can be created using the ln command on many UNIX-like systems. It is done like this: ln existingfile linkname

existingfile is an existing file, and linkname is the name for the new hard link you are creating.

Hard links point to the same data in the file system, meaning they point to the same inode node as the main file. They are used to create many names for the same data.

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

To create a symbolic link on the command line on many UNIX-like systems, use the ln command with the -s option.

Symbolic links point to the path to the original file or directory, providing flexibility in working with the file system. Here are the situations when it is advisable to use them:

10. Порівняйте жорсткі та символічні посилання?

The main difference between the two is how they reference the source file and how they interact with the file system. Symbolic links are more flexible because they allow you to link to different resources and file systems, but they are vulnerable to deletion of the source file. Hard links are less flexible, but provide resistance to deletion of the source file because they refer to an inode node.

Hard links:

Point directly to the inode node of the original file in the file system.

They can't point to another file system or directory.

If the original file is deleted, the hard link will continue to work.

You cannot create a hard link for a directory.

Symbolic links:

Refers to the path to a file, not directly linked to an inode node.

They can pass links to other file systems and directories.

If the source file is deleted, the symbolic link loses its connection.

You can create a symbolic link for a directory.

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.

If you delete:

The original file: All references to this file will remain, but will point to nothing (no file).

Symbolic link: Deleting a symbolic link won't affect the original file or any other links.

Hard link: A hard link will have the same information as the original file. However, when a deleted file is restored from a backup or a new file with the same name is created, the hard link will still point to the updated copy of the file, not the previous version.

***Готував матеріал студент Панчук О.С.***

***Висновки***

important goals and objectives set out in the work statement were achieved. The acquired practical skills in working with the Bash command shell will contribute to the development of competencies in the field of Linux system administration. Familiarity with the basic operations of changing owners and access rights to files will allow you to more effectively manage security levels and access to information. Additionally, the study of special directories and files in Linux will expand the understanding of the file structure of the operating system.