Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий Фізико-технічний інститут

ОПЕРАЦІЙНІ СИСТЕМИ

Комп'ютерний практикум
Робота №2

Виконав:
студент групи ФІ-12
Завалій Олександр
Перевірив:
Кірієнко О.В.

Київ-2023

Робота №2.
Система розмежування доступу в UNIX і Linux, права доступу до файлів і керування ними

Мета:

Оволодіння практичними навичками керування правами доступу до файлів і їхній аналіз в ОС UNIX та Linux

Варіант №5

Зміст індивідуального завдання:

1. Створіть каталог **lab_2**.
2. Скопіюйте в каталог **lab_2** файл **/bin/cat** під назвою **my_cat**.
3. За допомогою файлу **my_cat**, що знаходиться в каталозі **lab_2**, перегляньте уміст файлу **.profile** (ви знаходитесь у домашньому каталозі).
4. Перегляньте список файлів у каталозі **lab_2**. Потім перегляньте список усіх файлів, включаючи приховані, з повною інформацією про файли. Зверніть увагу на права доступу, власника, дату модифікації файлу, що ви тількино скопіювали. Потім перегляньте цю інформацію про оригінальний файл (той, який копіювали) і порівняйте два результати.
5. Змініть права доступу до файлу **my_cat** так, щоб власник міг тільки читати цей файл.
6. Переконайтеся в тому, що ви зробили ці зміни і повторіть п.3.
7. Визначте права на файл **my_cat** таким чином, щоб ви могли робити з файлом усе, що завгодно, а всі інші — нічого не могли робити.
8. Поверніться в домашній каталог. Змініть права доступу до каталогу **lab_2** так, щоб ви могли його тільки читати.
9. Спробуйте переглянути простий список файлів у цьому каталозі. Спробуйте переглянути список файлів з повною інформацією про них. Спробуйте запустити і видалити файл **my_cat** з цього каталогу.
10. Поясніть отримані результати. Результати виконання п.8 можуть бути різними в різних версіях UNIX, зокрема, Linux і FreeBSD. Прокоментуйте отримані результати у висновках.
11. За допомогою команди **su <user name>**, завантажтесь в систему, користуючись обліковим записом іншого користувача. (Вам потрібно знати пароль цього користувача.) Спробуйте отримати доступ до Вашого каталогу **lab_2**. Перевірте, чи правильно зроблено завдання попереднього пункту. Створіть каталог **lab_2_2**.
12. Знову завантажтесь в систему, користуючись своїм обліковим записом. Спробуйте зробити власником каталогу **lab_2** іншого користувача. Спробуйте зробити себе власником каталогу **lab_2_2**. Поясніть результати.
13. Зайдіть у каталог **lab_2**. Зробіть так, щоб нові створені файли і каталоги діставали права доступу згідно Таблиці. Створіть новий файл і каталог і переконайтеся в правильності ваших установок. Права для файлів **«644»**. Права для каталогів **«745»**.

14. Поверніть собі права читати, писати, та переглядати вміст каталогів.

15. Створіть у каталозі **lab_2** каталог **acl_test** та у ньому файли **file1**, **file2**. Після створення **file1** додайте у нього довільний текст.

16. Виведіть ACL для **file1**.

17. Змінить права доступу на **file1** так, щоб тільки власник мав право на читання.

18. Увійдіть до системи під іншим обліковим записом та спробуйте прочитати вміст **file1**. Що отримаємо? Поверніться до свого облікового запису.

19. За допомогою команди **setfacl** додайте право на читання іншому обраному користувачу для **file1**. Перевірте, що створився новий ACL для **file1**.

20. Увійдіть до системи під іншим обліковим записом та спробуйте прочитати вміст **file1**. Що отримаємо? Поверніться до свого облікового запису.

21. За допомогою команди **setfacl** встановіть значення маски таким чином щоб дозволити читати вміст **file1** іншому користувачу. Виведіть ACL для **file1**.

22. Увійдіть до системи під іншим обліковим записом, та спробуйте прочитати вміст **file1**. Ви повинні мати таку змогу.

Task I

Створіть каталог **lab_2**.

```
alex@Oleksandr:~$ mkdir lab_2; ls
lab_2
alex@Oleksandr:~$
```

Task II

Скопіюйте в каталог **lab_2** файл /**bin**/**cat** під назвою **my_cat**.

```
alex@Oleksandr:~$ cp /bin/cat ./lab_2/my_cat; ls lab_2
my_cat
alex@Oleksandr:~$
```

Task III

За допомогою файлу **my_cat**, що знаходиться в каталозі **lab_2**, перегляньте уміст файлу **.profile** (ви знаходитесь у домашньому каталозі).

```
alex@Oleksandr:~$ lab_2/my_cat .profile
# ~/.profile: executed by the command interpreter for login shells.
# This file is not read by bash(1), if ~/.bash_profile or ~/.bash_login
# exists.
# see /usr/share/doc/bash/examples/startup-files for examples.
# the files are located in the bash-doc package.

# the default umask is set in /etc/profile; for setting the umask
# for ssh logins, install and configure the libpam-umask package.
#umask 022

# if running bash
if [ -n "$BASH_VERSION" ]; then
    # include .bashrc if it exists
    if [ -f "$HOME/.bashrc" ]; then
        . "$HOME/.bashrc"
    fi
fi

# set PATH so it includes user's private bin if it exists
if [ -d "$HOME/bin" ] ; then
    PATH="$HOME/bin:$PATH"
fi

# set PATH so it includes user's private bin if it exists
if [ -d "$HOME/.local/bin" ] ; then
    PATH="$HOME/.local/bin:$PATH"
fi
```

Task IV

Перегляньте список файлів у каталозі **lab_2**. Потім перегляньте список усіх файлів, включаючи приховані, з повною інформацією про файли. Зверніть увагу на права доступу, власника, дату модифікації файлу, що ви тількино скопіювали. Потім перегляньте цю інформацію про оригінальний файл (той, який копіювали) і порівняйте два результати.

```
alex@Oleksandr:~$ ls lab_2
my_cat
alex@Oleksandr:~$ ls -al lab_2
total 44
drwxr-xr-x 2 alex alex  4096 Feb 21 20:37 .
drwxr-x--- 5 alex alex  4096 Feb 21 20:41 ..
-rwxr-xr-x 1 alex alex 35280 Feb 21 20:37 my_cat
alex@Oleksandr:~$ ls -l /bin/cat
-rwxr-xr-x 1 root root 35280 Feb  7  2022 /bin/cat
alex@Oleksandr:~$
```

Task V

Змініть права доступу до файлу **my_cat** так, щоб власник міг тільки читати цей файл.

```
alex@Oleksandr:~$ ls -l lab_2
total 36
-r--r-xr-x 1 alex alex 35280 Feb 21 20:37 my_cat
alex@Oleksandr:~$ chmod u-wx lab_2/my_cat; ls -l lab_2
total 36
-r--r-xr-x 1 alex alex 35280 Feb 21 20:37 my_cat
alex@Oleksandr:~$
```

Task VI

Переконайтеся в тому, що ви зробили ці зміни і повторіть п.3.

```
alex@Oleksandr:~$ chmod u-wx lab_2/my_cat; ls -l lab_2
total 36
-r--r-xr-x 1 alex alex 35280 Feb 21 20:37 my_cat
alex@Oleksandr:~$ lab_2/my_cat .profile
-bash: lab_2/my_cat: Permission denied
alex@Oleksandr:~$
```

Task VII

Визначте права на файл **my_cat** таким чином, щоб ви могли робити з файлом усе, що завгодно, а всі інші — нічого не могли робити.

```
alex@Oleksandr:~$ chmod 700 lab_2/my_cat; ls -l lab_2
total 36
-rwx------ 1 alex alex 35280 Feb 21 20:37 my_cat
alex@Oleksandr:~$
```

Task VIII

Поверніться в домашній каталог. Змініть права доступу до каталогу **lab_2** так, щоб ви могли його тільки читати.

```
alex@Oleksandr:~$ ls -l
total 4
drwxr-xr-x 2 alex alex 4096 Feb 21 20:37 lab_2
alex@Oleksandr:~$ chmod u-wx lab_2; ls -l
total 4
dr--r-xr-x 2 alex alex 4096 Feb 21 20:37 lab_2
alex@Oleksandr:~$
```

Task IX

Спробуйте переглянути простий список файлів у цьому каталозі. Спробуйте переглянути список файлів з повною інформацією про них. Спробуйте запустити і видалити файл **my_cat** з цього каталогу.

```
alex@Oleksandr:~$ ls lab_2
ls: cannot access 'lab_2/my_cat': Permission denied
my_cat
alex@Oleksandr:~$ la -l lab_2
ls: cannot access 'lab_2/my_cat': Permission denied
total 0
-????????? ? ? ? ?            ? my_cat
alex@Oleksandr:~$ cat lab_2/my_cat
cat: lab_2/my_cat: Permission denied
alex@Oleksandr:~$ rm lab_2/my_cat
rm: cannot remove 'lab_2/my_cat': Permission denied
alex@Oleksandr:~$
```

Task X

Поясніть отримані результати. Результати виконання п.8 можуть бути різними в різних версіях UNIX, зокрема, Linux і FreeBSD. Прокоментуйте отримані результати у висновках.
Оскільки ми встановили права доступу для власника тільки на читання. Ми можемо переглядати(читати) вміст каталогу. Відповідно до логіки роботи ми не можемо виконувати запис та виконня для всього дерева цієї директорії.

Task XI

За допомогою команди **su <user name>**, завантажтесь в систему, користуючись обліковим записом іншого користувача. (Вам потрібно знати пароль цього користувача.) Спробуйте отримати доступ до Вашого каталогу **lab_2**. Перевірте, чи правильно зроблено завдання попереднього пункту. Створіть каталог **lab_2_2**.

```
alex@Oleksandr:~$ su test
Password:
test@Oleksandr:/home/alex$ ls -l lab_2
total 36
-rwx------ 1 alex alex 35280 Feb 21 20:37 my_cat
test@Oleksandr:/home/alex$ mkdir lab_2_2
test@Oleksandr:/home/alex$
```

Task XII

Знову завантажтесь в систему, користуючись своїм обліковим записом. Спробуйте зробити власником каталогу **lab_2** іншого користувача. Спробуйте зробити себе власником каталогу **lab_2_2**. Поясніть результати.

```
test@Oleksandr:/home/alex$ su alex
Password:
alex@Oleksandr:~$ chown test lab_2
chown: changing ownership of 'lab_2': Operation not permitted
alex@Oleksandr:~$ chown alex lab_2_2
chown: changing ownership of 'lab_2_2': Operation not permitted
```

Основна модель безпеки в Unix стосується користувачів і груп, а також їх права власності на різні файли та каталоги. Це означає, що без підвищених привілеїв (стати root або виконувати команди через sudo) жоден звичайний користувач не матиме достатніх привілеїв, щоб діяти від імені іншого користувача.

Task XIII

Зайдіть у каталог **lab_2**. Зробіть так, щоб нові створені файли і каталоги діставали права доступу згідно Таблиці. Створіть новий файл і каталог і переконайтеся в правильності ваших установок. Права для файлів **«644»**. Права для каталогів **«745»**.

```
alex@Oleksandr:~$ chmod 777 lab_2
alex@Oleksandr:~$ cd lab_2
alex@Oleksandr:~/lab_2$ umask 022
alex@Oleksandr:~/lab_2$ umask 032
alex@Oleksandr:~/lab_2$ touch test_file; mkdir test; ls -l
total 40
-rwx------ 1 alex alex 35280 Feb 21 20:37 my_cat
drwxr--r-x 2 alex alex  4096 Feb 22 19:45 test
-rw-r--r-- 1 alex alex     0 Feb 22 19:45 test_file
alex@Oleksandr:~/lab_2$
```

Task XIV

Поверніть собі права читати, писати, та переглядати вміст каталогів.

```
alex@Oleksandr:~/lab_2$ cd
alex@Oleksandr:~$ umask 0002
```

Task XV

Створіть у каталозі **lab_2** каталог **acl_test** та у ньому файли **file1**, **file2**. Після створення **file1** додайте у нього довільний текст.

```
alex@Oleksandr:~$ mkdir lab_2/acl_test && cd $_
alex@Oleksandr:~/lab_2/acl_test$ touch file1 file2
alex@Oleksandr:~/lab_2/acl_test$ nano file1
alex@Oleksandr:~/lab_2/acl_test$ cat file1
Hello, world!
alex@Oleksandr:~/lab_2/acl_test$
```

Task XVI

Виведіть ACL для **file1**.

```
alex@Oleksandr:~/labs/lab_2/acl_test$ getfacl file1
# file: file1
# owner: alex
# group: alex
user::rw-
group::rw-
other::r--
```

Task XVII

Змінить права доступу на **file1** так, щоб тільки власник мав право на читання.

```
alex@Oleksandr:~/labs/lab_2/acl_test$ ls -l
total 4
-rw-rw-r-- 1 alex alex 14 лют 23 11:49 file1
-rw-rw-r-- 1 alex alex  0 лют 23 11:49 file2
alex@Oleksandr:~/labs/lab_2/acl_test$ chmod 620  file1; ls -l
total 4
-rw--w---- 1 alex alex 14 лют 23 11:49 file1
-rw-rw-r-- 1 alex alex  0 лют 23 11:49 file2
alex@Oleksandr:~/labs/lab_2/acl_test$
```

Task XVIII

Увійдіть до системи під іншим обліковим записом та спробуйте прочитати вміст **file1**. Що отримаємо? Поверніться до свого облікового запису.

```
alex@Oleksandr:~/labs/lab_2/acl_test$ su test
Password:
test@Oleksandr:/home/alex/labs/lab_2/acl_test$ cat file1
cat: file1: Permission denied
test@Oleksandr:/home/alex/labs/lab_2/acl_test$ su alex
Password:
alex@Oleksandr:~/labs/lab_2/acl_test$
```

Task XIX

За допомогою команди **setfacl** додайте право на читання іншому обраному користувачу для **file1**. Перевірте, що створився новий ACL для **file1**.

```
alex@Oleksandr:~/labs/lab_2/acl_test$ setfacl -m u:test:r file1
alex@Oleksandr:~/labs/lab_2/acl_test$ getfacl file1
# file: file1
# owner: alex
# group: alex
user::rw-
user:test:r--
group::-w-
mask::rw-
other::---

alex@Oleksandr:~/labs/lab_2/acl_test$
```

Task XX

Увійдіть до системи під іншим обліковим записом та спробуйте прочитати вміст **file1**. Що отримаємо? Поверніться до свого облікового запису.

```
alex@Oleksandr:~/labs/lab_2/acl_test$ su test
Password:
test@Oleksandr:/home/alex/labs/lab_2/acl_test$ cat file1
Hello, world!
test@Oleksandr:/home/alex/labs/lab_2/acl_test$ su alex
Password:
alex@Oleksandr:~/labs/lab_2/acl_test$
```

Task XXI

За допомогою команди **setfacl** встановіть значення маски таким чином щоб дозволити читати вміст **file1** іншому користувачу. Виведіть ACL для **file1**.

```
alex@Oleksandr:~/labs/lab_2/acl_test$ setfacl -m u:roma:r,mask:r file1
alex@Oleksandr:~/labs/lab_2/acl_test$ getfacl file1
# file: file1
# owner: alex
# group: alex
user::rw-
user:test:r--
user:roma:r--
group::-w-                      #effective:---
mask::r--
other::---

alex@Oleksandr:~/labs/lab_2/acl_test$
```

Task XXII

Увійдіть до системи під іншим обліковим записом, та спробуйте прочитати вміст **file1**. Ви повинні мати таку змогу.

```
alex@Oleksandr:~/labs/lab_2/acl_test$ su roma
Password:
roma@Oleksandr:/home/alex/labs/lab_2/acl_test$ cat file1
Hello, world!
roma@Oleksandr:/home/alex/labs/lab_2/acl_test$
```

Висновки

З огляду вивченого матеріалу, використання команд: «ls –l», «chmod», «chown», «umask», «setfacl» та «getfacl» є незамінною частиною розмежування прав доступу до файлів і керування ними.

UNIX реалізує дискреційну модель розмежування доступу, тому для кожного файлу визначається, які права мають всі користувачі на доступ до файлу. З цього випливає легкість адміністрування і повний контроль доступу до кожного окремого файлу для всіх можливих користувачів.

Перед встановленням прав доступу потрібно чітко розуміти можливе застосування цього файлу іншими користувачами та вже наявні права доступу. Тому, щоб створювати нові файли вже по наявному шаблону можна задати маску для всіх нових файлів та директорій за домопогою команди «umask». Переглняути інформацію з таблиці індексних дескрипторів можна командою «ls –l».

В окремих випадках, для вже створеного файлу або директорії, права доступу можна редагувати командою «chmod». Команда «chown» змінює власника даного файлу або папки, яким може бути користувач або група.

Команда «setfacl» в Linux використовується для встановлення списків керування доступом (ACL) до файлів. ACL файлу визначає користувачів і групи, яким дозволено доступ до файлу, а також дозволи, які вони мають. Команду «setfacl» можна використовувати для додавання, видалення або зміни ACL файлу. Для перегляду ACL використовують «getfacl».