Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

ОПЕРАЦІЙНІ СИСТЕМИ

Комп’ютерний практикум

Робота № 2

Виконав
студент гр. ФЕ-01 Дорошенко В. О.
Перевірив
Кіреєнко О. В.

Київ - 2022

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 6 Залікова книжка ФЕ-0108

Інформація о системі

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.el7.x86_64 on an x86_64
```

1. Створіть каталог lab_2. 2. Скопіюйте в каталог lab_2 файл /bin/cat під назвою my_cat.

```
[vl@localhost ~]$ mkdir lab_2
[vl@localhost ~]$ cp /bin/cat lab_2/my_cat
```

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

```
[vl@localhost ~]$ ./lab_2/my_cat /etc/profile | less_
```

```
# /etc/profile

# System wide environment and startup programs, for login setup
# Functions and aliases go in /etc/bashrc

# It's NOT a good idea to change this file unless you know what you
# are doing. It's much better to create a custom.sh shell script in
# /etc/profile.d/ to make custom changes to your environment, as this
# will prevent the need for merging in future updates.

pathmunge () {
    case ":${PATH}:" in
        *:"$1":*)
            ;;
        *)
            if [ "$2" = "after" ] ; then
                PATH=$PATH:$1
            else
                PATH=$1:$PATH
            fi
    esac
}


if [ -x /usr/bin/id ]; then
    if [ -z "$EUID" ]; then
        # ksh workaround
        EUID=`/usr/bin/id -u`
        UID=`/usr/bin/id -ru`
    fi
    USER="`/usr/bin/id -un`"
    LOGNAME=$USER
    MAIL="/var/spool/mail/$USER"
fi

# Path manipulation
:
```

```
# Path manipulation
if [ "$EUID" = "0" ]; then
    pathmunge /usr/sbin
    pathmunge /usr/local/sbin
else
    pathmunge /usr/local/sbin after
    pathmunge /usr/sbin after
fi

HOSTNAME=`/usr/bin/hostname 2>/dev/null`
HISTSIZE=1000
if [ "$HISTCONTROL" = "ignorespace" ] ; then
    export HISTCONTROL=ignoreboth
else
    export HISTCONTROL=ignoredups
fi

export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE HISTCONTROL

# By default, we want umask to get set. This sets it for login shell
# Current threshold for system reserved uid/gids is 200
# You could check uidgid reservation validity in
# /usr/share/doc/setup-*/uidgid file
if [ $UID -gt 199 ] && [ "`/usr/bin/id -gn`" = "`/usr/bin/id -un`" ]; then
    umask 002
else
    umask 022
fi

for i in /etc/profile.d/*.sh /etc/profile.d/sh.local ; do
    if [ -r "$i" ]; then
        if [ "${-#*i}" != "$-" ]; then
            . "$i"
        else
            . "$i" >/dev/null
        fi
:_
```

```
    fi
done

unset i
unset -f pathmunge
(END)
```

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.

```
[vl@localhost ~]$ ls lab_2/
my_cat
[vl@localhost ~]$ ls -la lab_2/
total 60
drwxrwxr-x.  2 vl vl    20 Feb 17 10:33 .
drwx------. 17 vl vl  4096 Feb 17 10:38 ..
-rwxr-xr-x.  1 vl vl 54080 Feb 17 10:33 my_cat
[vl@localhost ~]$ ls -la /bin/cat
-rwxr-xr-x. 1 root root 54080 Aug 20  2019 /bin/cat
[vl@localhost ~]$ _
```

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.

```
[vl@localhost ~]$ chmod u=r lab_2/my_cat
[vl@localhost ~]$ ls -la lab_2/
total 60
drwxrwxr-x.  2 vl vl    20 Feb 17 10:33 .
drwx------. 17 vl vl  4096 Feb 17 10:38 ..
-r--r-xr-x.  1 vl vl 54080 Feb 17 10:33 my_cat
```

```
[vl@localhost ~]$ ./lab_2/my_cat /etc/profile
-bash: ./lab_2/my_cat: Permission denied
```

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.

```
[vl@localhost ~]$ ./lab_2/my_cat /etc/profile
-bash: ./lab_2/my_cat: Permission denied
[vl@localhost ~]$ chmod 700 lab_2/my_cat
[vl@localhost ~]$ ls -la lab_2/my_cat
-rwx------. 1 vl vl 54080 Feb 17 10:33 lab_2/my_cat
```

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

```
[vl@localhost ~]$ chmod 400 lab_2
```

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.

```
[vl@localhost ~]$ ls lab_2/
ls: cannot access lab_2/my_cat: Permission denied
my_cat
[vl@localhost ~]$ ls -la lab_2/
ls: cannot access lab_2/.: Permission denied
ls: cannot access lab_2/..: Permission denied
ls: cannot access lab_2/my_cat: Permission denied
total 0
d????????? ? ? ? ?            ? .
d????????? ? ? ? ?            ? ..
-????????? ? ? ? ?            ? my_cat
```

```
[vl@localhost ~]$ ./lab_2/my_cat /etc/profile
-bash: ./lab_2/my_cat: Permission denied
```

```
[vl@localhost ~]$ rm lab_2/my_cat
rm: cannot remove ‘lab_2/my_cat’: Permission denie
```

10. Я не можу перейти, переглянути, записати в каталог lab_2 оскільки в мене відсутні права на виконання (неможливо отримати інформацію з таблиці індексних дескрипторів) та запис файлів.

11. За допомогою команди su , 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.

```
localhost login: test
Password:
Last login: Thu Feb 17 11:40:34 on tty3
[test@localhost ~]$ ls /home/vl/lab_2
ls: cannot access /home/vl/lab_2: Permission denied
```

```
[test@localhost ~]$ mkdir lab_2_2
```

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

```
[vl@localhost ~]$ chown test lab_2
chown: changing ownership of ‘lab_2’: Operation not permitted
```

```
[vl@localhost ~]$ chown vl /home/test/lab_2_2
chown: changing ownership of ‘/home/test/lab_2_2’: Operation not permitted
```

Для забезпечення безпеки власника каталога чи файлу може змінюзати лише адміністратор.

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.

```
[vl@localhost ~]$ cd lab_2/
-bash: cd: lab_2/: Permission denied
[vl@localhost ~]$ chmod 777 lab_2/
[vl@localhost ~]$ cd lab_2/
```

```
[vl@localhost lab_2]$ umask 013
[vl@localhost lab_2]$ mkdir dir1
[vl@localhost lab_2]$ touch file1
[vl@localhost lab_2]$ ls -la
total 60
drwxrwxrwx.  3 vl vl    45 Feb 17 12:22 .
drwx------. 17 vl vl  4096 Feb 17 10:58 ..
drwxrw-r--.  2 vl vl     6 Feb 17 12:22 dir1
-rw-rw-r--.  1 vl vl     0 Feb 17 12:22 file1
-rwx------.  1 vl vl 54080 Feb 17 10:33 my_cat
[vl@localhost lab_2]$
```

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

```
[vl@localhost lab_2]$ umask 0002
```

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

```
[vl@localhost lab_2]$ mkdir acl_test
[vl@localhost lab_2]$ echo "123123" > acl_test/file1
[vl@localhost lab_2]$ touch acl_test/file2
```

```
[vl@localhost lab_2]$ getfacl acl_test/file1
# file: acl_test/file1
# owner: vl
# group: vl
user::rw-
group::rw-
other::r--
```

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

```
[vl@localhost lab_2]$ chmod 400 acl_test/file1
```

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

```
[test@localhost ~]$ cat /home/vl/lab_2/acl_test/file1
cat: /home/vl/lab_2/acl_test/file1: Permission denied
```

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

```
[sudo] password for vl:
[vl@localhost lab_2]$ setfacl -m u:test:r acl_test/file1
```

```
[vl@localhost lab_2]$ getfacl acl_test/file1
# file: acl_test/file1
# owner: vl
# group: vl
user::r--
user:test:r--
group::---
mask::r--
other::---
```

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

```
[vl@localhost lab_2]$ su test
Password:
[test@localhost lab_2]$ cat acl_test/file1
123123
```

Висновки:

В Linux реалізує дискреційну модель розмежування доступу. Встановити права для користувач, групи, інших можна за допомогою chmod . Списки ACL мають більшу гнучкість в встановленні потрібних правил доступу. ACL можна встановлювати утилітами “setfact” та “getfacl”.