

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ  
“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. ІГОРЯ СІКОРСЬКОГО”  
КАФЕДРА АВТОМАТИЗОВАНИХ СИСТЕМ ОБРОБКИ ІНФОРМАЦІЇ І УПРАВЛІННЯ

Комп’ютерний практикум № 8  
з дисципліни  
“Основи захисту інформації”  
Варіант 11

Виконав:  
студент групи ІС-72  
Кривохижа Р. А.

Перевірив:  
асистент  
Ільїн К.І.

**Тема:** Механізми захисту операційних систем.

**Мета:** Ознайомитись із вбудованими засобами захисту в операційних системах Windows та Linux.

**Хід роботи:**

Для ОС Linux Debian виконайте послідовність дій та поясніть одержані на кожному кроці результати. Для довідки використовуйте команду `man ім'я_команди`

```
user@user-pc:~$ sudo adduser kryvokhyzha1
Adding user `kryvokhyzha1' ...
Adding new group `kryvokhyzha1' (1003) ...
Adding new user `kryvokhyzha1' (1001) with group `kryvokhyzha1' ...
Creating home directory `/home/kryvokhyzha1' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for kryvokhyzha1
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
```

Було створено нового користувача

```
user@user-pc:~$ > file
user@user-pc:~$ ls -l
total 32
drwxr-xr-x 2 user user 4096 rpy 6 00:06 Desktop
drwxr-xr-x 2 user user 4096 rpy 6 00:06 Documents
drwxr-xr-x 2 user user 4096 rpy 6 00:06 Downloads
-rw-r--r-- 1 user user 0 rpy 6 00:18 file
drwxr-xr-x 2 user user 4096 rpy 6 00:06 Music
drwxr-xr-x 2 user user 4096 rpy 6 00:06 Pictures
drwxr-xr-x 2 user user 4096 rpy 6 00:06 Public
drwxr-xr-x 2 user user 4096 rpy 6 00:06 Templates
drwxr-xr-x 2 user user 4096 rpy 6 00:06 Videos
```

Створено файл `file` та показано вміст директорії командою `ls`.

```

user@user-pc:~$ chmod 777 file
user@user-pc:~$ ls -l
total 32
drwxr-xr-x 2 user user 4096 rpy 6 00:06 Desktop
drwxr-xr-x 2 user user 4096 rpy 6 00:06 Documents
drwxr-xr-x 2 user user 4096 rpy 6 00:06 Downloads
-rwxrwxrwx 1 user user 0 rpy 6 00:18 file
drwxr-xr-x 2 user user 4096 rpy 6 00:06 Music
drwxr-xr-x 2 user user 4096 rpy 6 00:06 Pictures
drwxr-xr-x 2 user user 4096 rpy 6 00:06 Public
drwxr-xr-x 2 user user 4096 rpy 6 00:06 Templates
drwxr-xr-x 2 user user 4096 rpy 6 00:06 Videos

```

Надання всім користувачам та групам доступ на читання та виконання.

```

pop-os@pop-os:~$ vim &
[3] 4378

```

Запускаємо vim.

```

user@user-pc:~$ sudo adduser kryvokhyzha2
Adding user `kryvokhyzha2' ...
Adding new group `kryvokhyzha2' (1004) ...
Adding new user `kryvokhyzha2' (1002) with group `kryvokhyzha2' ...
Creating home directory `/home/kryvokhyzha2' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for kryvokhyzha2
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y

```

Створимо нового користувача.

```

user@user-pc:~$ su kryvokhyzha2
Password:
kryvokhyzha2@user-pc: /home/user$

```

Перейдемо на нового користувача.

```

rkuser1@pop-os: /home/kryvokhyzha$ cat file
rkuser1@pop-os: /home/kryvokhyzha$ less file
rkuser1@pop-os: /home/kryvokhyzha$ more file

```

Кожна з цих трьох команд виконує

виведення вмісту файлу.

```
kryvokhyzha2@user-pc:/home/user$ chown kryvokhyzha2:kryvokhyzha2 file
chown: changing ownership of 'file': Operation not permitted
kryvokhyzha2@user-pc:/home/user$ sudo chown kryvokhyzha2:kryvokhyzha2 file

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for kryvokhyzha2:
kryvokhyzha2 is not in the sudoers file. This incident will be reported.
```

Змінюємо користувача та групу для файлу (поточний користувач не має прав на здійснення даної операції).

```
kryvokhyzha2@user-pc:/home/user$ chmod 777 file
chmod: changing permissions of 'file': Operation not permitted
kryvokhyzha2@user-pc:/home/user$ sudo chmod 777 file
[sudo] password for kryvokhyzha2:
kryvokhyzha2 is not in the sudoers file. This incident will be reported.
kryvokhyzha2@user-pc:/home/user$
```

Надання всім користувачам та групам права на читання, запис та виконання.

```
kryvokhyzha2@user-pc:/home/user$ echo "test" >> file
```

Записуємо текст “test” у файл.

```
kryvokhyzha2@user-pc:/home/user$ mv file /home/kryvokhyzha2
mv: cannot move 'file' to '/home/kryvokhyzha2/file': Permission denied
```

Переміщення файлу в іншу директорію.

```
kryvokhyzha2@user-pc:/home/user$ cp file file2
cp: cannot create regular file 'file2': Permission denied
```

Копіюємо file та перейменуємо його у file2.



```
kryvokhyzha2@user-pc:/home/user$ touch file
kryvokhyzha2@user-pc:/home/user$ ls -l
total 36
drwxr-xr-x 2 user user 4096 rpy 6 00:06 Desktop
drwxr-xr-x 2 user user 4096 rpy 6 00:06 Documents
drwxr-xr-x 2 user user 4096 rpy 6 00:06 Downloads
-rwxrwxrwx 1 user user 5 rpy 6 00:28 file
drwxr-xr-x 2 user user 4096 rpy 6 00:06 Music
drwxr-xr-x 2 user user 4096 rpy 6 00:06 Pictures
drwxr-xr-x 2 user user 4096 rpy 6 00:06 Public
drwxr-xr-x 2 user user 4096 rpy 6 00:06 Templates
drwxr-xr-x 2 user user 4096 rpy 6 00:06 Videos
```

Створено файл та показано вміст директорії.

```
kryvokhyzha2@user-pc:/home/user$ ps auxx | grep test1
kryvokh+ 2052 0.0 0.0 9028 888 pts/0 S+ 00:29 0:00 grep test1
```

Шукаємо всі процеси, які містять в описі “test1”.

```
kryvokhyzha2@user-pc:/home/user$ killall -u kryvokhyzha2
```

Закінчуємо всі процеси користувача kryvokhyzha2

```
kryvokhyzha2@user-pc:/home/user$ su kryvokhyzha1
Password:
kryvokhyzha1@user-pc:/home/user$
```

Переходимо на користувача kryvokhyzha1

```
kryvokhyzha1@user-pc:/home/user$ ls -la /etc/init.d/
total 136
drwxr-xr-x 2 root root 4096 rpy 5 23:55 .
drwxr-xr-x 122 root root 4096 rpy 6 00:20 ..
-rwxr-xr-x 1 root root 2269 лис 22 2018 acpid
-rwxr-xr-x 1 root root 5336 бер 30 2019 alsa-utils
-rwxr-xr-x 1 root root 2055 тра 19 2019 anacron
-rwxr-xr-x 1 root root 3740 бер 30 2019 apparmor
-rwxr-xr-x 1 root root 2401 кві 27 2018 avahi-daemon
-rwxr-xr-x 1 root root 2948 бер 22 2020 bluetooth
-rwxr-xr-x 1 root root 1232 сер 15 2019 console-setup.sh
-rwxr-xr-x 1 root root 3059 жов 11 2019 cron
-rwxr-xr-x 1 root root 937 сер 26 2019 cryptdisks
-rwxr-xr-x 1 root root 896 сер 26 2019 cryptdisks-early
-rwxr-xr-x 1 root root 2813 лип 5 19:10 dbus
-rwxr-xr-x 1 root root 3033 лют 9 2019 gdm3
-rwxr-xr-x 1 root root 3809 січ 10 2019 hwclock.sh
-rwxr-xr-x 1 root root 1479 жов 10 2016 keyboard-setup.sh
-rwxr-xr-x 1 root root 2044 лют 10 2019 kmod
-rwxr-xr-x 1 root root 4445 сер 25 2018 networking
-rwxr-xr-x 1 root root 1942 жов 4 2019 network-manager
-rwxr-xr-x 1 root root 1366 кві 8 2019 plymouth
-rwxr-xr-x 1 root root 752 кві 8 2019 plymouth-log
-rwxr-xr-x 1 root root 612 лют 20 2020 pppd-dns
-rwxr-xr-x 1 root root 924 тра 31 2018 procps
-rwxr-xr-x 1 root root 2864 лют 26 2019 rsyslog
-rwxr-xr-x 1 root root 2224 кві 15 2018 saned
-rwxr-xr-x 1 root root 1960 тра 2 2020 speech-dispatcher
-rwxr-xr-x 1 root root 1030 лют 2 2020 sudo
-rwxr-xr-x 1 root root 6872 кві 27 2020 udev
-rwxr-xr-x 1 root root 1391 чер 8 2019 unattended-upgrades
-rwxr-xr-x 1 root root 1306 січ 10 2019 uuidd
-rwxr-xr-x 1 root root 2757 лис 23 2016 x11-common
```

Як бачимо “/etc/init.d/ssh” файлу не існує. Аналогічна ситуація для “/var/run/bind”.

```
user@user-pc:~/folder$ touch file.txt
user@user-pc:~/folder$ ls -la
total 8
drwxr-xr-x  2 user user 4096 rpy  6 00:47 .
drwxr-xr-x 16 user user 4096 rpy  6 00:47 ..
-rw-r--r--  1 user user   0 rpy  6 00:47 file.txt
user@user-pc:~/folder$ chmod u+s file.txt
user@user-pc:~/folder$ ls -la
total 8
drwxr-xr-x  2 user user 4096 rpy  6 00:47 .
drwxr-xr-x 16 user user 4096 rpy  6 00:47 ..
-rwSr--r--  1 user user   0 rpy  6 00:47 file.txt
user@user-pc:~/folder$ chmod g+s file.txt
user@user-pc:~/folder$ ls -la
total 8
drwxr-xr-x  2 user user 4096 rpy  6 00:47 .
drwxr-xr-x 16 user user 4096 rpy  6 00:47 ..
-rwSr-Sr--  1 user user   0 rpy  6 00:47 file.txt
```

Створимо файл та встановимо для нього відповідні флаги SUID, SGID. SUID дає можливість на час виконання файлу (запущеного їм процесу) привілейованому користувачеві отримати права користувача - власника файлу, в даному випадку - root. Біт SGID аналогічний SUID, але встановлюються права не користувача файлу, а групи - власника файлу. Так само, всі файли, створювані в каталозі з установленим SGID отримуватимуть ідентифікатор групи - власника каталогу, а не власника файлу. Нові каталоги, створювані в каталозі з установленим SGID будуть його наслідувати від каталогу-батька.

```
GNU nano 3.2 /etc/sudoers
Defaults    secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
# Host alias specification
# User alias specification
# Cmnd alias specification
# User privilege specification
root    ALL=(ALL:ALL) ALL
# Allow members of group sudo to execute any command
%sudo    ALL=(ALL:ALL) ALL
# See sudoers(5) for more information on "#include" directives:
#include_dir /etc/sudoers.d

^G Get Help      ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos      ^U Undo
^X Exit          ^R Read File    ^_ Replace      ^U Uncut Text  ^T To Spell     ^G Go To Line   ^M-E Redo
```

Переглянули вміст файлу `\etc\sudoers`.

```
# Псевдоніми для факультета інформатики та обчислювальної техніки
Host_Alias CS= tigger, pandao, piper, sigi
Host_Alias INFORMATICS = hostel, eprince, honda
```

```
# Набір команд
Cmnd_Alias    DUMP = /sbin/dump, /sbin/restore
Cmnd_Alias    PRINTING = /usr/sbin/lpc, /usr/bin/lprm
Cmnd_Alias    SHELLS = /bin/sh, /bin/tcsh, /bin/csh, /bin/bash, /bin/ash,
```

```
# Права доступу
alex, ed      INFORMATICS = ALL,
syncmaster    CS = /usr/sbin/tcpdump : INFORMATICS = (operator) DUMP
Lynda         ALL = (ALL) ALL, !SHELLS
%fruit        ALL, !INFORMATICS = NOPASSWD: PRINTING
```

Лінда не зможе запускати інтерпретатор. Так, вимагається введення паролю.

## Висновок:

### Додаткові запитання

1. Якими будуть результати дії команди `chmod 750 file`?

*Дана команда надає поточному користувачу права на читання, запис та виконання файлу; група користувачів не може виконувати запис до файлу; інші користувачі не мають права на читання, запис та виконання.*

2. Якими будуть результати дії команди `umask 127 file`?

*Дана команда надає власнику файлу право на виконання файлу; групі – право на запис до файлу, іншим користувачам права на читання, запис та виконання файлу.*

3. Де ОС Windows зберігає паролі, та які способи захисту їх застосовує?

*Образи паролів зберігаються в спеціальному розділі реєстру, при цьому використовуються два типи хеш-функцій: за алгоритмом MD4 (NT-hash) та менш стійка з використанням DES (LM-hash), остання для сумісності з клієнтами попередньої серверної ОС Microsoft — Lan Manager.*

4. Яким чином ОС Windows захищає журнал безпеки?

*Вбудований антивірус "Захисник Windows" в Windows 10 веде і захищає журнал захисту про знайдені загрози.*

5. Назвіть основні відмінності в системі розмежування доступу ОС Windows 8 та ОС Linux Debian.

*Windows 8 реалізує дискреційну модель розмежування доступу. Матриця доступу в даній ОС, таким чином, зберігається у вигляді множини списків контролю доступу об'єктів. Останні, на відміну від ОС Linux Debian, мають нефіксовану довжину і можуть містити довільну кількість елементів контролю доступу (Access Control Entry, ACE).*

**Висновок:** в даній лабораторній роботі ми навчилися працювати з вбудованими засобами захисту операційних систем, навчилися працювати з правами доступу, розмежовувати його для користувачів та познайомились з основними командами ОС Linux Debian 10.