Міністерство освіти і науки України

Національний авіаційний університет

Факультет кібербезпеки, комп’ютерної та програмної інженерії

Кафедра інженерії програмного забезпечення

*Операційні системи*

**Лабораторна робота №6**

**«Права доступу до файлів та каталогів»**

Розробив: студент ПІ-322

Царук С.О.

Перевірив:

Лосєв Є.О.

Київ 2021

**Мета:** Визначення понять і аналіз роботи нижче названих об’єктів та процесів, які відбуваються при доступі процесів до файлів і каталогів.

**Завдання**

Опрацювання роботи команд:

1. Визначення ідентифікатора користувача та членства в групах.
2. Права доступу до файлів та каталогів
3. Утиліти роботи із жорсткими посланнями на каталоги.
4. Обмеження доступу до повної таблиці процесів.
5. Доступ до повної таблиці процесів: група proc.
6. Знищення чужого файлу з незручним ім’ям.
7. Робота з файлами в каталозі який розділяється.
8. Робота з чужими файлами в своєму каталозі.
9. Робота з використанням SetUid.

Зміст

[Хід роботи 3](#_Toc67498302)

[1. Визначення ідентифікатора користувача та членства в групах. 3](#_Toc67498303)

[2. Права доступу до файлів та каталогів 3](#_Toc67498304)

[3. Утиліти роботи із жорсткими посланнями на каталоги. 3](#_Toc67498305)

[4. Обмеження доступу до повної таблиці процесів. 4](#_Toc67498306)

[5. Доступ до повної таблиці процесів: група proc. 5](#_Toc67498307)

[6. Знищення чужого файлу з незручним ім’ям. 5](#_Toc67498308)

[7. Робота з файлами в каталозі який розділяється. 5](#_Toc67498309)

[8. Робота з чужими файлами в своєму каталозі. 6](#_Toc67498310)

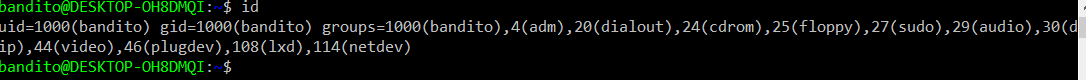
[9. Робота з використанням SetUid. 7](#_Toc67498311)

[Висновок 9](#_Toc67498312)

# Хід роботи

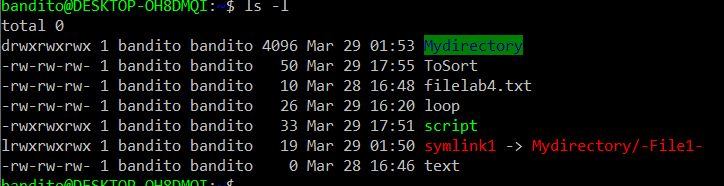
## Визначення ідентифікатора користувача та членства в групах.

***Ідентифікатор користувача*** (***UID***) – обов’язкова властивість любого процесу Linux.Права доступу до файлів та каталогів. Утиліта ***id***, якою ми скористалися, виводить наше **вхідне ім’я** і відповідний нам ***UID***, а також **групу за замовченням** і повний список **груп**, членами яких ми є.



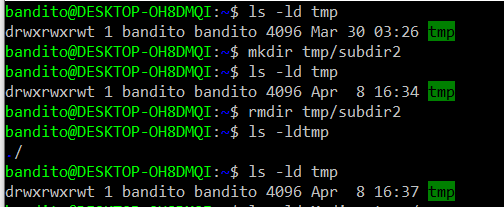
## Права доступу до файлів та каталогів

При *утворенні* об’єктів файлової системи – файлів, каталогів і тому подібне, – кожному, обов’язковому порядку приписується **ярлик**. Ярлик включає в себе ***UID*** ідентифікатор користувача-*хозяїна* файлу, ***GID*** – ідентифікатор групи, до якої належить файл, тип об’єкту і набір, так званих, **атрибутів**, а також деяку додаткову інформацію. **Атрибути** визначають, хто і що з файлом має право робити, і описані нижче



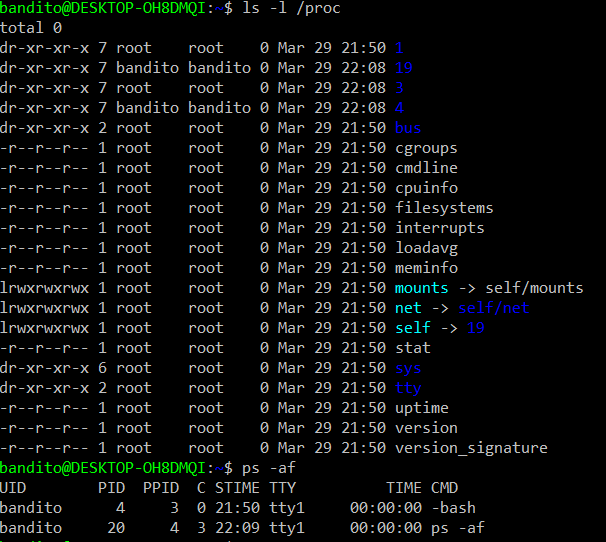
## Утиліти роботи із жорсткими посланнями на каталоги.

Не дивлячись на те, що утворення *жорстких посилань* на каталог не можливо, поле «кількість жорстких посилань» для *усіх* каталогів прикладу дорівнює *двом*, а не одному. Насамперед, цього і слід було очікувати, тому, що *любий* каталог файлової системи Linux завжди має не менше двох імен: особисте (наприклад, ***tmp***) і ім’я «**.**» у самому каталозі (**tmp/.**). Якщо у каталозі утворити підкаталог, кількість жорстких посилань на цей каталог збільшиться на 1 за рахунок імені «**..**» у підкаталозі (***tmp/subdir1/..***)



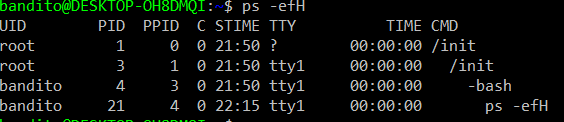
## Обмеження доступу до повної таблиці процесів.

B Linux майже завжди використовується **віртуальна файлова система */proc*** – каталог, у якому у вигляді підкаталогів і файлів подана інформація з **таблиці процесів**. Ім’я підкаталогу ***/proc*** співпадає з ***PID*** відповідного процесу, а вміст цього каталогу відображає властивості процесу. *Хазяїном* такого підкаталогу буде хазяїн процесу (з правами на читання і використання), тому *любий* користувач може продивитися інформацію про свої процеси. Саме каталогом ***/proc*** користується утиліта ***ps***.



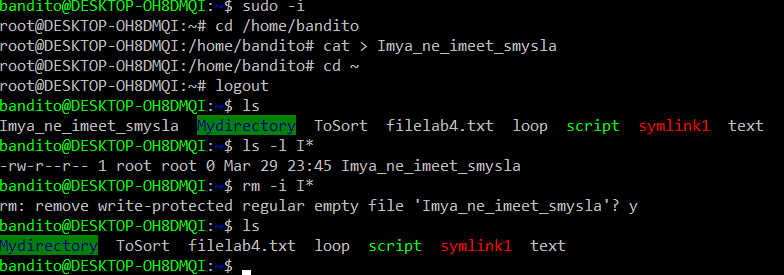
## Доступ до повної таблиці процесів: група proc.

Команда ***ps -а*** виводить інформацію про *всі* процеси запущені «живими» (а не системними користувачами). Для перегляду усіх процесів адміністратор запускає ***ps –efH***



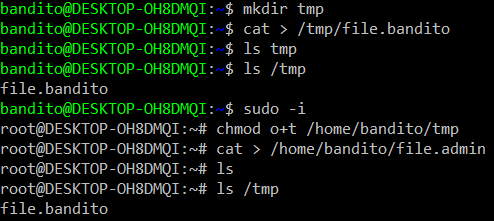
## Знищення чужого файлу з незручним ім’ям.

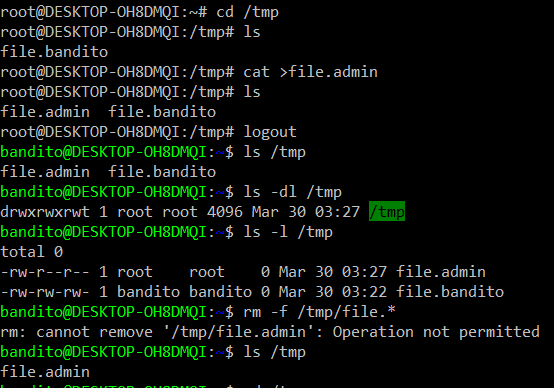
Ми вирішили не набирати ім’я файлу,який знищується, з клавіатури, а скористатися *шаблоном* і ключем «***-і***» *(****i****nteractive*) команди ***rm***, щоби та очікувала підтвердження перед тим, як знищувати черговий файл. Не дивлячись на відсутність доступу до самого файлу, знищити його виявилося можливим.



## Робота з файлами в каталозі який розділяється.

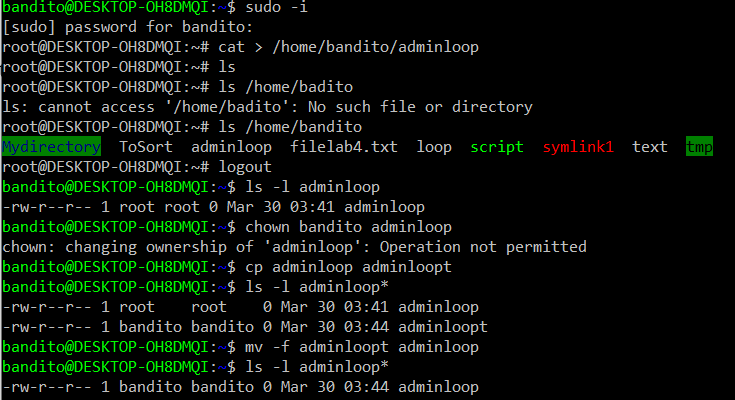
Oдну особливість атрибутів каталогу ***/tmp***: замість «***х***» у трійці «для сторонніх» ***ls*** видав «***t***». Це – *ще* один атрибут каталогу, наявність якого якраз і забороняє користувачеві знищувати звідти файли, яким ми не хазяї. Таким чином, права запису у каталог з ярликом ***drwxrwxrwt*** ***група хазяїн*** і для членів групи *група*, і для сторонніх обмежені їх особистими файлами, тільки *хазяїн* має право змінювати список файлів у каталозі, як йому заманеться. Такі каталоги називаються тими, що **розділяються**, тому що призначені вони, як правило, для сумісної роботи усіх користувачів у системі, обміну інформацією тощо. За допомогою прав адміністратора ми присвоїли атрибут «***t***» каталогу ***/tmp.***





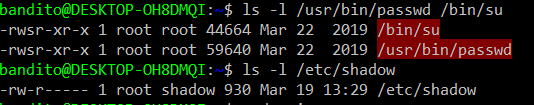
## Робота з чужими файлами в своєму каталозі.

Хтось замінив файлу ***adminloop*** хазяїна, що тепер ми можемо тільки читати його але на змінювати. Знищувати цей файл дуже просто, але хочеться повернути старі права на нього. Це нескладно: чужий файл можна перейменувати (це дія над каталогом а не файлом), скопіювати перейменований файл у файл з іменем старого (доступ на читання відкрито), на кінець, знищити чужий файл. Ключ «***-f***» (**f***orce*, «силоміць»)дозволяє утиліті ***mv*** робити свою справу, не питаючи підтверджень. Зокрема. Побачивши, що файл з іменем, в яке необхідно перейменувати існує, навіть чужий, навіть недоступний на запис, ***mv*** спокійно знищує його і виконує операцію перейменування.



## Робота з використанням SetUid.

У багатьох дистрибутивах Linux і ***/bin/su***, і ***/usr/bin/passwd*** мають встановлений ***SetUID*** і користувачу ***root***, що дозволяє ***su*** запускати процеси з правами цього користувача (це означає і любого іншого), а ***passwd*** – модифікувати файл ***/etc/shadow***, який вміщує у таких системах відомості про *усі* облікові записи. Як правило, ***SetUID***-ні файли доступні звичайним користувачам тільки на виконання, щоби не провокувати цих звичайних користувачів розглядати вміст цих файлів і досліджувати їхні *не документовані можливості*.



# **Висновок**

В ході виконання даної лабораторної роботи я визначив поняття і аналіз роботи нижче названих об’єктів та процесів, які відбуваються при доступі процесів до файлів і каталогів. Було опрацьовано команди роботи з каталогами і доступом до них.