“Київський фаховий коледж зв’язку”

Циклова комісія Комп’ютерної інженерії

**ЗВІТ ПО ВИКОНАННЮ**

**ЛАБОРАТОРНОЇ РОБОТИ №9**

з дисципліни: «Операційні системи»

**Тема: “Захист системи та користувачів у Linux. Створення користувачів та груп”**

Виконали студенти

Групи БІКС-13

Береза Артем

Когут Ігор

Перевірив викладач

Сушанова В.С.

Київ 2024

**Завдання для попередньої підготовки:**

1. UPG (User Private Group) - це механізм управління групами користувачів у Linux-системах, при якому для кожного нового користувача створюється окрема група з тим самим ім'ям, що і користувач. Це дозволяє автоматично надавати користувачеві права доступу до власних файлів та ресурсів, забезпечуючи при цьому зручне керування правами доступу.

2. Для створення груп користувачів можна використовувати команду `groupadd`. Наприклад: sudo groupadd mygroup

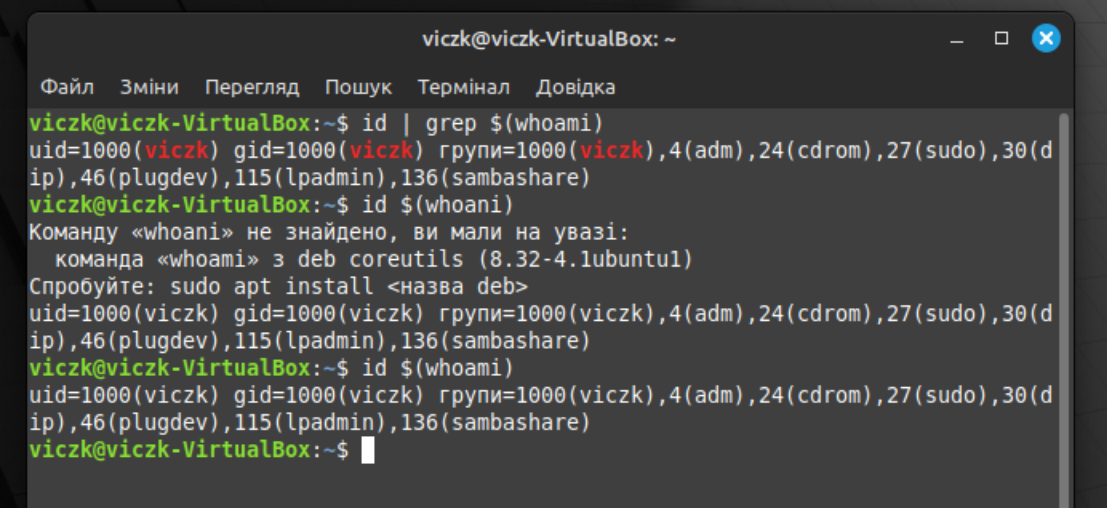
3. Налаштування груп користувачів можна змінювати за допомогою команди `groupmod`. Наприклад, для зміни імені групи:

sudo groupmod -n newgroup oldgroup

Де `newgroup` - нове ім'я групи, а `oldgroup` - поточне ім'я групи.

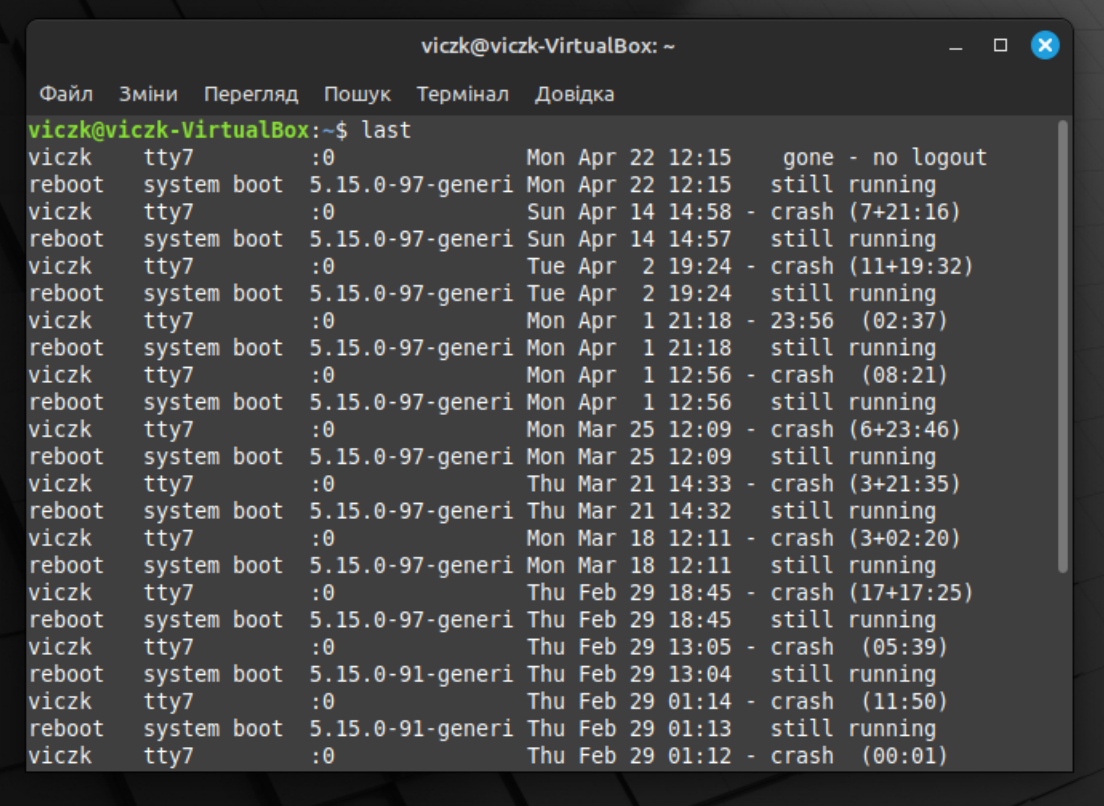
Хід роботи:

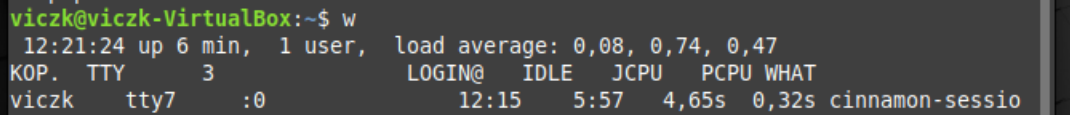
виведіть інформацію про поточного користувача різними способами (підказка використовуйте команди id та grep);



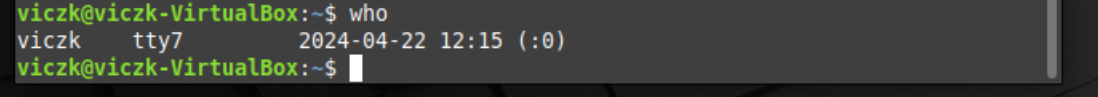
попрактикуйте в терміналі команди last, w та who. Порівняйте результати виводу кожної команди, які деталі відсутні в кожній із команд порівняно з іншими?

* Команда last виводить історію входів користувачів, включаючи ім'я користувача, термінал, IP-адресу, час входу та вихід. Ця команда відображає всі входи та виходи, включаючи ребут та вимкнення системи.



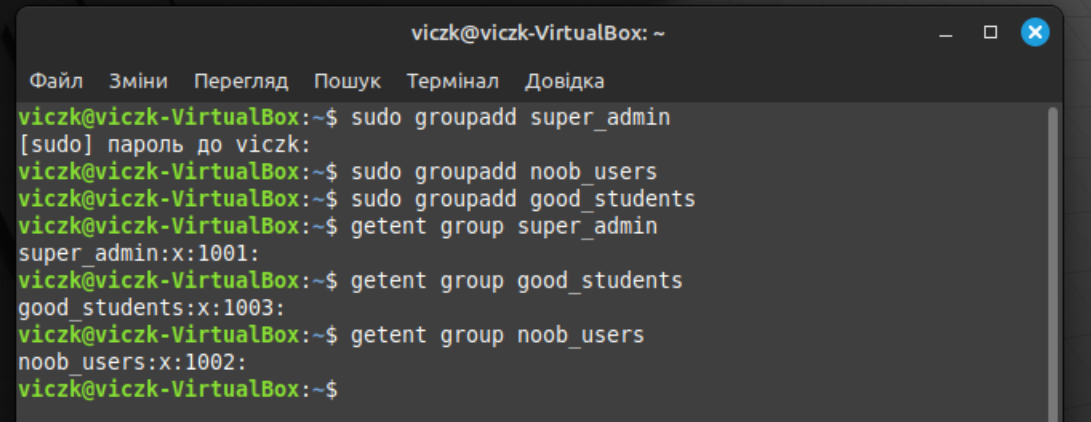
Команда w показує відомості про поточних користувачів, які зараз ввійшли в систему, разом з інформацією про їх активність, час входу та інші деталі.

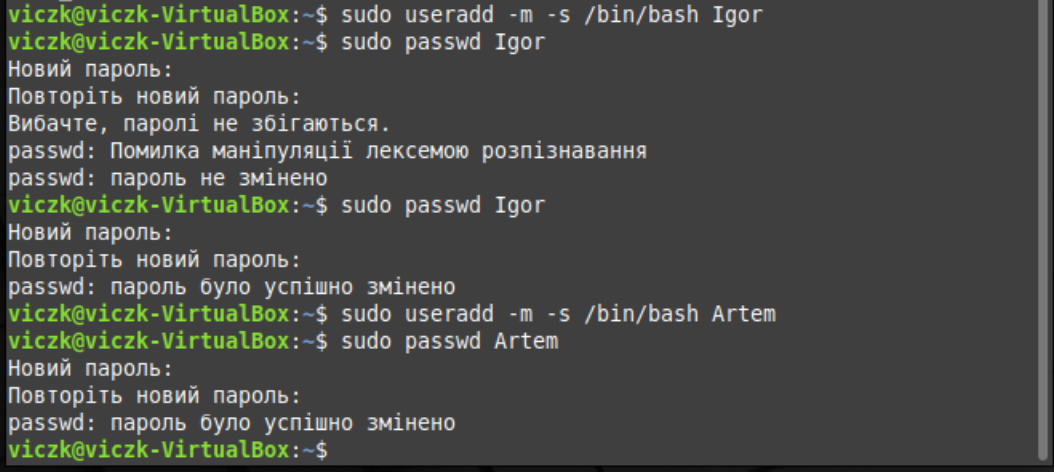
* Команда who також виводить інформацію про ввійшли в систему користувачів, включаючи ім'я, термінал та час входу.



створіть дві нові групи користувачів - super\_admins, noob\_users та good\_students, визначте їх ідентифікатори;

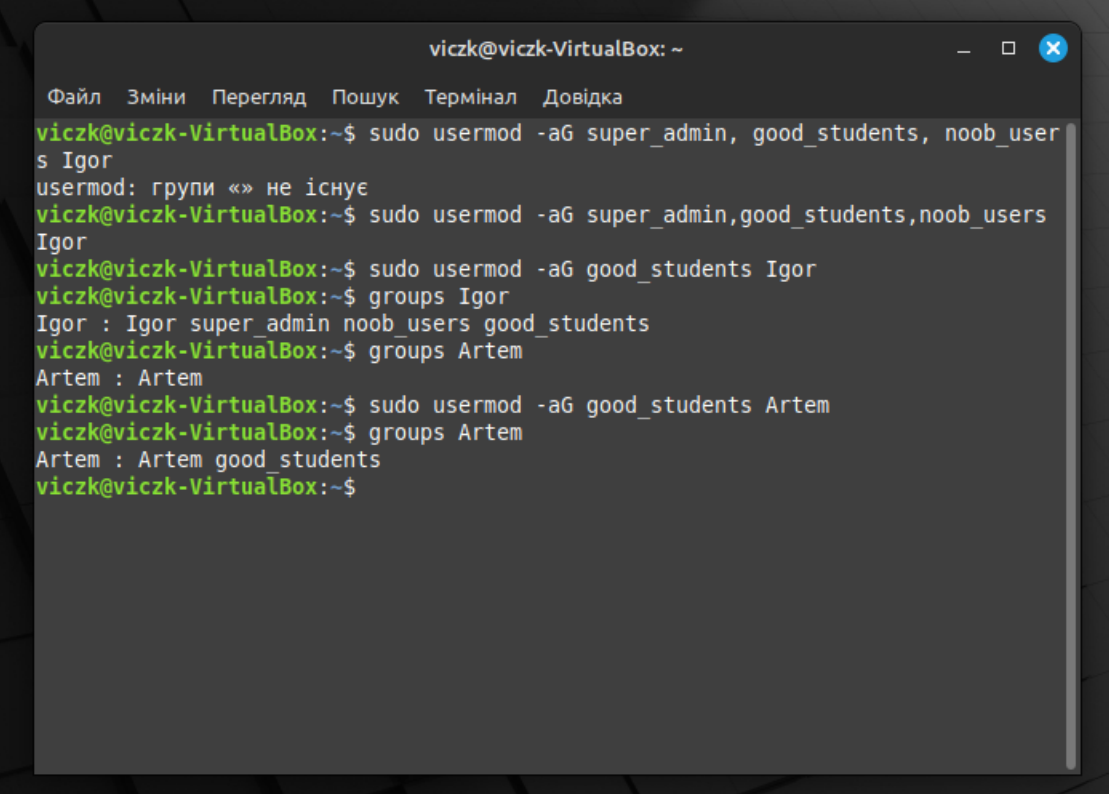
для кожного члену Вашої команди за допомогою терміналу створіть нового користувача (якщо працюєте самі, то просто трьох довільних користувачів), не забудьте після створення нового користувача одразу задати йому пароль;



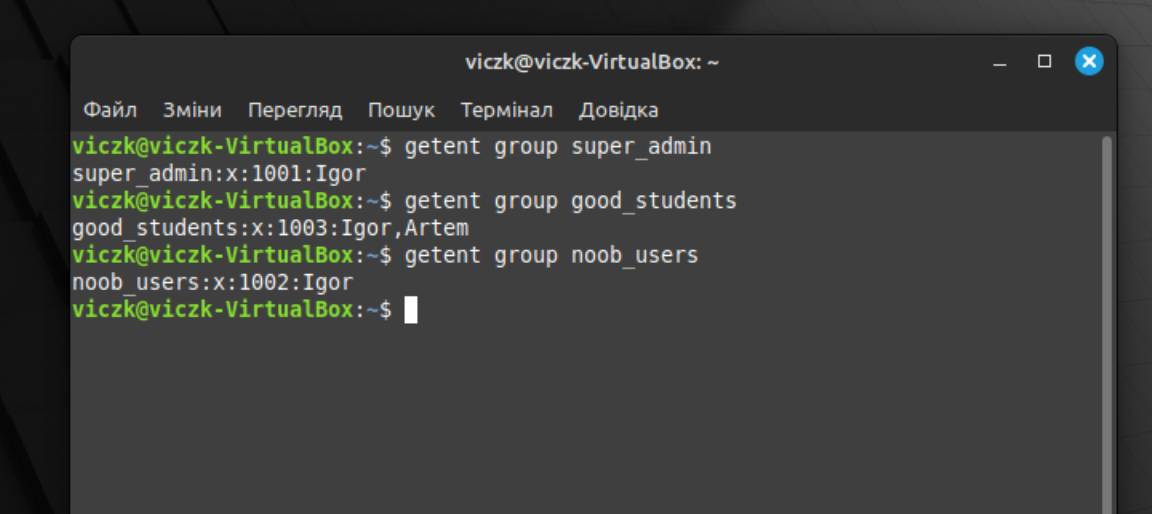


- додайте нових користувачів у створені Вами нові групи таким чином, щоб у групах super\_admins та noob\_users було по 2 користувачі, один з яких є в обох групах, у групу good\_students додайте всіх трьох користувачів;

додайте нових користувачів у створені Вами нові групи таким чином, щоб у групах super\_admins та noob\_users було по 2 користувачі, один з яких є в обох групах, у групу good\_students додайте всіх трьох користувачів;

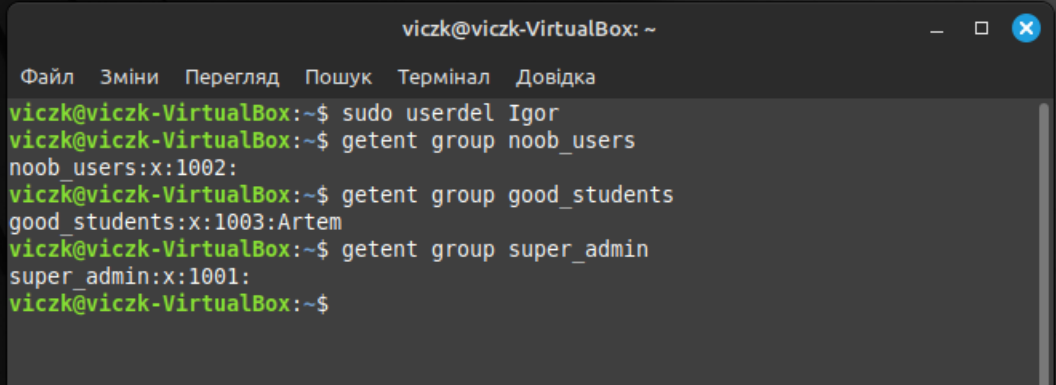


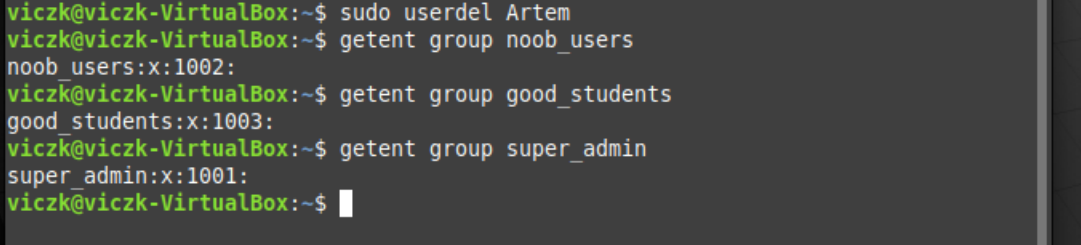
- перегляньте інформацію про групи, та які користувачі до них входять, поясніть що ви бачите;



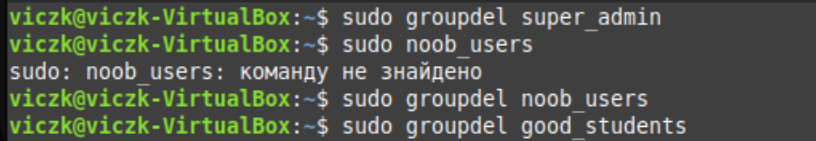
- видаліть першого створеного вами користувача, перегляньте чи залишиться інформація про нього в групах, де він перебував;

Як ми бачимо,з усіх груп він зник:

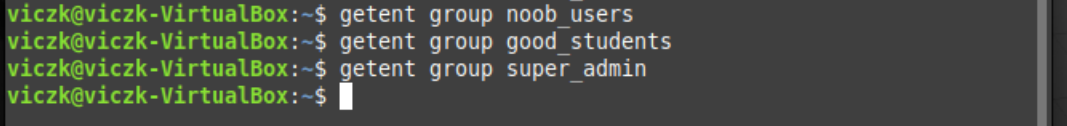




- видаліть створені Вами групи користувачів;



- перегляньте інформацію про існуючі групи користувачів.



Контрольні запитання:

1. Паролі не зберігаються в явному вигляді в конфігураційних файлах з міркувань безпеки. Якщо паролі зберігатимуться в текстових файлах у відкритому вигляді, вони можуть бути зламані або викрадені, що може призвести до компрометації системи та конфіденційної інформації.

2. Виконання повсякденних операцій, використовуючи обліковий запис root, не рекомендується з міркувань безпеки. Обліковий запис root має повний доступ до всіх системних ресурсів і може виконувати будь-які дії, включаючи потенційно небезпечні або ризиковані. Використання облікового запису root повинно бути обмеженим лише до необхідних адміністративних завдань.

3. Механізми отримання особливих привілеїв su і sudo відрізняються основним чином в тому, як вони перевіряють доступ користувача до підвищених привілеїв. Команда su дозволяє користувачеві змінити ідентифікатор користувача на інший (root), вимагаючи введення пароля цього користувача. У той час як команда sudo дозволяє користувачам виконувати окремі команди з підвищеними привілеями, використовуючи свій власний пароль, а не пароль root.

4. Домашній каталог користувача root зазвичай не розміщений в каталозі /home з міркувань безпеки. Каталог /home зазвичай містить домашні каталоги для звичайних користувачів, і розміщення домашнього каталогу root там може створити потенційні ризики безпеки.

5. Команда getent використовується для отримання інформації з різних джерел аутентифікації та авторизації в системі. Вона може використовуватися для отримання інформації про користувачів, групи, паролі та інші аутентифікаційні дані з різних джерел, таких як /etc/passwd, /etc/group, /etc/shadow тощо.

6. Змінити пароль користувача можна за допомогою команди passwd.

7. Щоб видалити існуючі групи користувачів, можна використовувати команду groupdel.

ів може залишитися у файлі /etc/group, але вони будуть видалені з системи та втратять свої права доступу.

8. Команда chage використовується для зміни параметрів пароля користувача. Вона дозволяє налаштувати термін дії пароля, інтервал для зміни пароля та інші параметри.

9. Параметри команди usermod, які найчастіше використовуються, включають зміну імені користувача, додавання або видалення користувача з груп, зміну домашнього каталогу тощо.