“Київський фаховий коледж зв’язку”

Циклова комісія комп’ютерної та програмної інженерії

**ЗВІТ ПО ВИКОНАННЮ**

**ЛАБОРАТОРНОЇ РОБОТИ №9**

з дисципліни: «Операційні системи»

**Тема: «Захист системи та користувачів у Linux. Створення користувачів та груп»**

Виконав(ла/ли) студент(ка/и)

групи: КСМ-23а

Папснази

Юхимець Д.О.Любежанін М.С

Перевірила викладач

Сушанова В.С.

Київ 2024

**Лабораторна робота №9   
 Тема:** **“Захист системи та користувачів у Linux. Створення користувачів та груп**”

**Мета роботи:**

1. Отримання практичних навиків роботи з командною оболонкою Bash.
2. Знайомство з базовими діями при створенні нових користувачів та нових груп користувачів.

**Матеріальне забезпечення занять:**

1. ЕОМ типу IBM PC.

2. ОС сімейства Windows та віртуальна машина Virtual Box (Oracle).

3. ОС GNU/Linux (будь-який дистрибутив).

4. Сайт мережевої академії Cisco netacad.com та його онлайн курси по Linux

**Завдання для попередньої підготовки:**

1. \*Прочитайте короткі теоретичні відомості до лабораторної роботи та зробіть невеликий словник базових англійських термінів з питань призначення команд та їх параметрів.
2. Вивчіть матеріали онлайн-курсу академії Cisco “NDG Linux Essentials”:

* Chapter 15 - System and User Security
* Chapter 16 - Creating Users and Groups

1. Пройдіть тестування у курсі NDG Linux Essentials за такими темами:

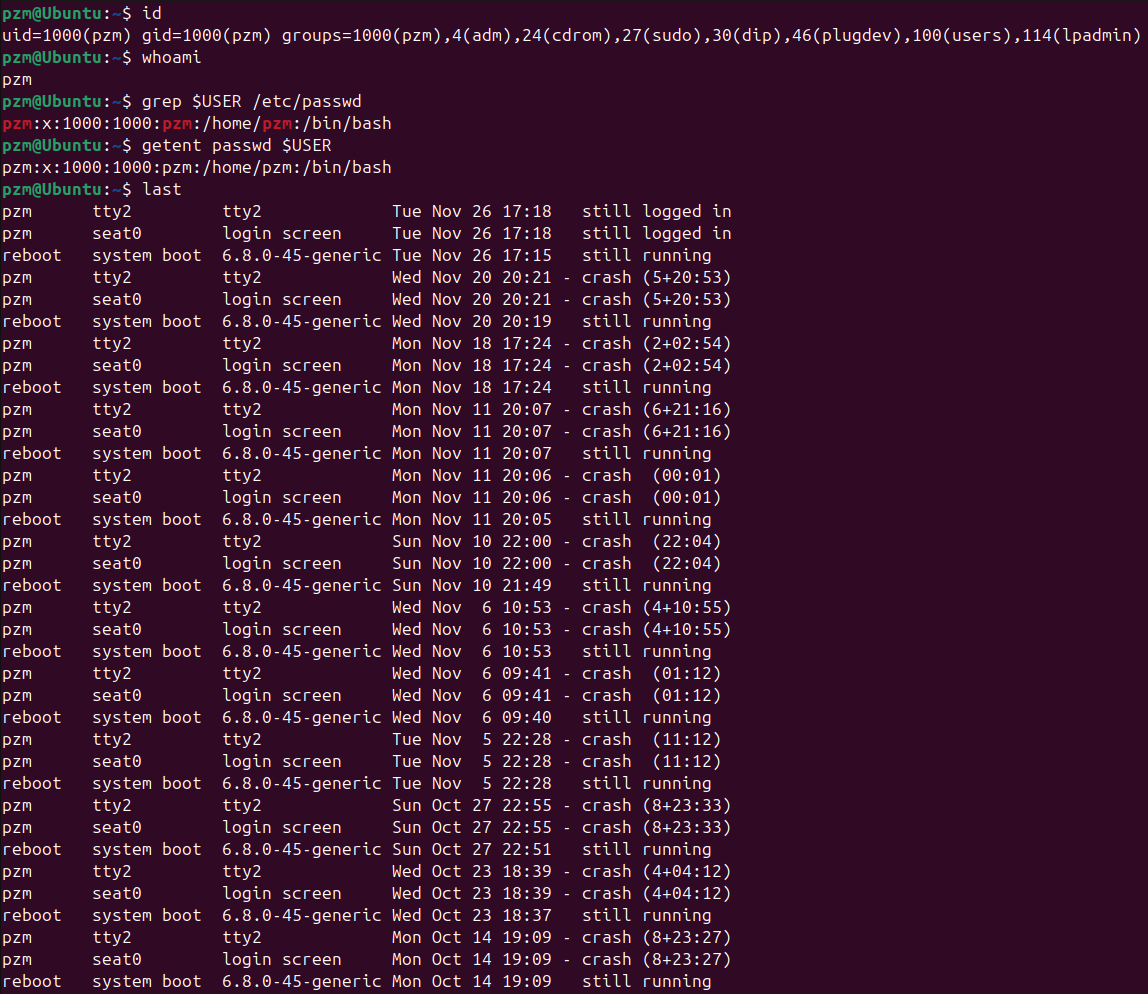
* Chapter 15 Exam
* Chapter 16 Exam

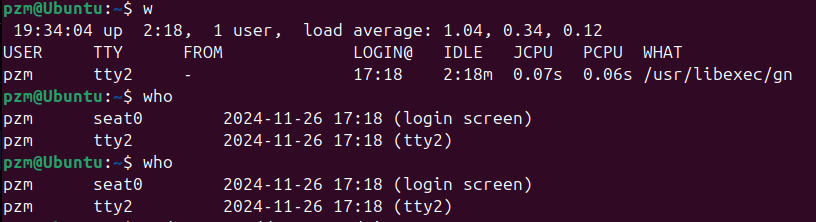
1. На базі розглянутого матеріалу дайте відповіді на наступні питання:
   1. Розкрийте поняття UPG, коли їх доцільно використовувати?
   2. \*Якими командами можна створити групи користувачів? Наведіть приклади
   3. \*\*Якими командами можна змінити налаштування груп користувачів? Наведіть приклади
2. Підготувати в електронному вигляді початковий варіант звіту:

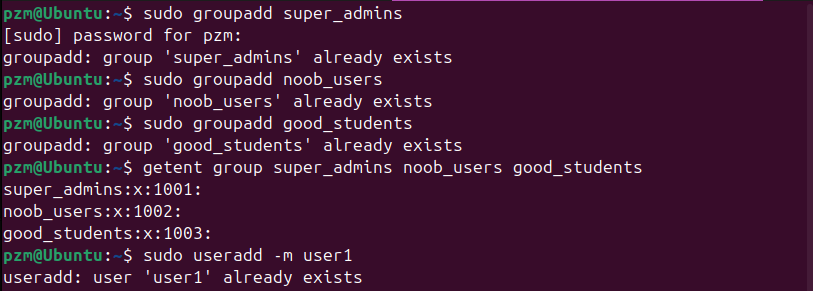
* Титульний аркуш, тема та мета роботи
* Словник термінів
* Відповіді на п.4.1 та п.4.5 з завдань для попередньої підготовки

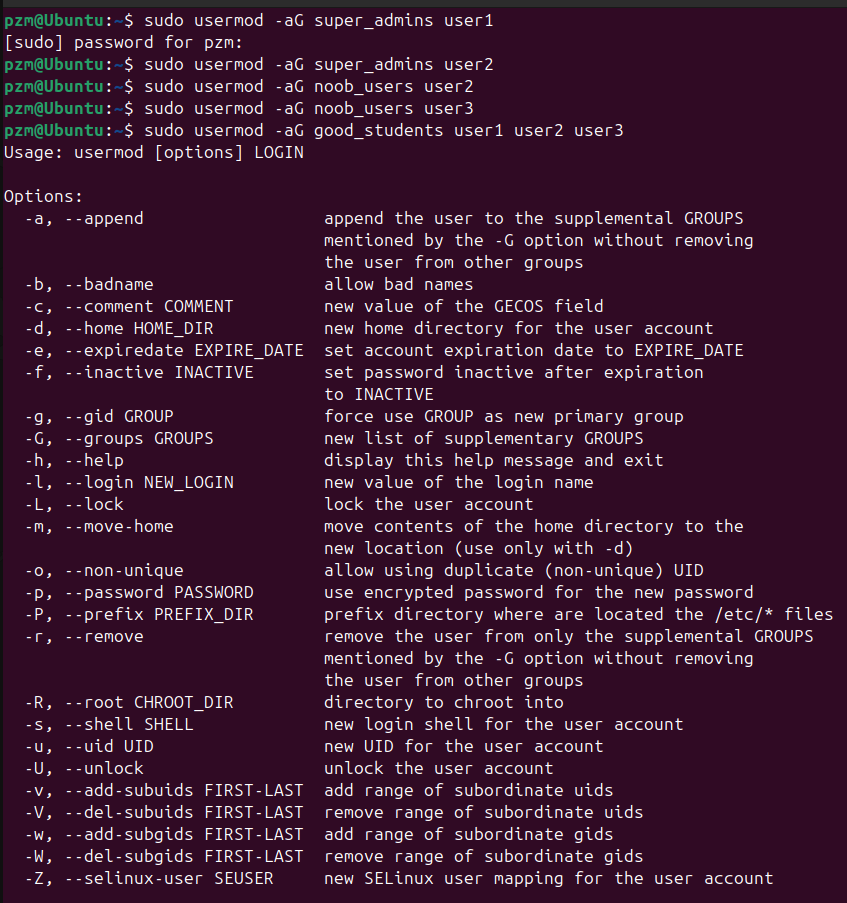
**Виконав Юхимець Дмитро**

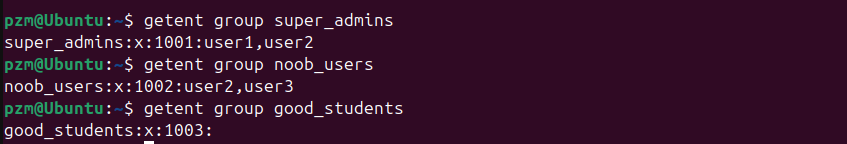
| Назва команди | Її призначення та функціональність |
| --- | --- |
| su |  |
| id | Відображення інформації про поточного користувача.Показує ідентифікатор користувача (UID), ідентифікатор групи (GID) та список додаткових груп. |
| exit | Перехід до іншого користувача.Дозволяє змінити поточного користувача в системі. За замовчуванням команда перемикає на суперкористувача (root), якщо не вказано іншого користувача. |
| head /etc/shadow | Завершення поточної сесії терміналу або завершення роботи з обліковим записом.Вихід із поточної оболонки, закриття терміналу або скасування прав суперкористувача після виконання su. |
| sudo head /etc/shadow | Вивести перші 10 рядків файлу /etc/shadow.Використовується для читання частини файлу. /etc/shadow містить зашифровані паролі користувачів. Виконати цю команду без прав суперкористувача не можна. |
| head /etc/passwd | Те саме, що і попередня команда, але з використанням привілеїв адміністратора.Дозволяє переглянути перші 10 рядків файлу /etc/shadow, якщо є дозвіл виконувати sudo. |
| grep sysadmin /etc/passwd | Вивести перші 10 рядків файлу /etc/passwd.  /etc/passwd містить інформацію про облікові записи користувачів, включаючи їхні імена, UID, GID та домашні каталоги. |
| head -3 /etc/shadow | Знайти рядки, що містять слово sysadmin, у файлі /etc/passwd. |
| ls -l /etc/shadow | Вивести перші 3 рядки файлу /etc/shadow.Показує лише обмежену частину файлу (якщо є права доступу). |
| sudo head -3 /etc/shadow | Показати інформацію про права доступу, власника, групу та розмір файлу /etc/shadow.Використовується для перевірки доступу до файлу. |
| getent passwd sysadmin | Показати перші 3 рядки файлу /etc/shadow з привілеями адміністратора.Виводить рядок із файлу /etc/passwd, якщо такий користувач існує. |
| who | Показати, хто зараз увійшов у систему.Відображає імена користувачів, час входу та термінали. |
| last | Відобразити історію входу користувачів у систему.Показує інформацію про останні сесії користувачів, включаючи час входу, виходу та використаний термінал. |

****

****

****

****

****

**Відповіді на контрольні запитання**

**Відповів Любежанін Максим  
  
  
  
1.Чому в конфігураційних файлах паролі не зберігається в явному вигляді?**Це дуже важливе питання безпеки. Ось чому паролі зазвичай не зберігаються у відкритому вигляді в конфігураційних файлах:

Ризик компрометації: Якщо зловмисник отримає доступ до файлу з відкритим текстом, він зможе легко вкрасти всі паролі.

Зручність для зловмисників: З відкритими паролями злочинцям не потрібно зламувати складні алгоритми шифрування.

Відсутність захисту від брутфорсу: З відкритими паролями атакуючі можуть легко використовувати методи грубої сили (брутфорс) для підбору паролів.  
  
**2. Чому не рекомендується виконувати повсякденні операції, використовуючи обліковий запис root?**

Обліковий запис root в операційній системі має найвищі привілеї доступу. Це означає, що користувач, який увійшов під цим обліковим записом, може виконувати будь-які дії на системі без будь-яких обмежень. Хоча це може здатися зручним, використання root-доступу для повсякденних завдань пов'язане з великими ризиками.  
  
**3. У чому відмінність механізмів отримання особливих привілеїв su і sudo?**  
  
**su (substitute user)**

**Пряме переключення користувача:** Команда su перемикає вас на інший обліковий запис, зазвичай root.

**Вимагає пароль цільового користувача:** Для переключення на інший обліковий запис необхідно ввести пароль цього облікового запису.

**Повна зміна середовища:** Після виконання команди su ви працюєте в середовищі цільового користувача з усіма його налаштуваннями та правами.  
  
**sudo (substitute user do)**

**Виконання команди з правами іншого користувача:** Команда sudo дозволяє виконати конкретну команду з правами іншого користувача, зазвичай root, без повного переключення на цей обліковий запис.

**Вимагає пароль поточного користувача:** Для виконання команди з правами sudo необхідно ввести пароль поточного користувача.

**Обмежене використання:** Можливості використання sudo зазвичай обмежуються конфігураційним файлом /etc/sudoers, який визначає, які користувачі можуть виконувати які команди з правами sudo.  
  
**4. Чому домашній каталог користувача root не розміщено в каталозі /home?  
  
Ізоляція:** Розміщення домашнього каталогу root окремо від інших користувачів створює додатковий рівень безпеки. Це зменшує ризик того, що зловмисник, отримавши доступ до системи, зможе легко знайти та модифікувати критично важливі файли root.

**Захист від випадкового видалення:** Оскільки root має найвищі привілеї, випадкове видалення важливих файлів з його домашнього каталогу може призвести до серйозних наслідків для всієї системи. Окреме розташування допомагає запобігти таким інцидентам.  
  
**Системні файли:** Домашній каталог root може містити важливі системні файли, конфігурації та журнали, які тісно пов'язані з роботою всієї системи. Розміщення їх окремо від інших користувачів полегшує управління та підтримку системи.

**Історичні причини:** З самого початку розробки Unix-подібних систем домашній каталог root розміщувався в /root, і ця традиція збереглася донині.  
  
**5. Для чого використовується команда getent?  
  
Отримання даних з різних баз даних:** За допомогою getent можна отримувати інформацію про користувачів, групи, мережеві хости, служби та інші об'єкти, які зберігаються в різних системних базах даних.

**Флексибільність:** Ця команда дозволяє задавати різні критерії пошуку, що робить її дуже зручною для адміністративних задач.

**Інтеграція з NSS:** getent тісно інтегрована з NSS, що дозволяє їй працювати з різними типами баз даних, включаючи файли, LDAP, NIS та інші.  
  
**6. Як можна змінити пароль користувача?**  
Найпростіший спосіб змінити свій власний пароль - це використати команду passwd.  
Система попросить нас ввести наший поточний пароль та два рази новий.  
  
**7. Яким чином можна видалити існуючі групи користувачів? Чи залишиться інформація про них десь у системі?**Для видалення існуючих груп користувачів в Linux використовується команда **groupdel**.  
  
**Безпосередньо в /etc/group :** Ні, запис про групу буде повністю видалений.

**В інших файлах конфігурації:** Можливо, деякі інші файли конфігурації можуть містити посилання на видалену групу. Наприклад, файли налаштування служб або програм. Тому рекомендується перевірити інші конфігураційні файли після видалення групи.

**В історії системи:** Деякі журнали систем можуть зберігати інформацію про видалену групу. Наприклад, журнали аудиту можуть містити записи про зміни в системі, пов'язані з цією групою.  
  
**8.Яке призначення команди chage?**  
  
Команда chage: Управління паролями користувачів

Команда chage в Linux використовується для управління параметрами паролів користувачів. За її допомогою можна встановлювати, змінювати та переглядати різні обмеження на паролі.  
  
**9.Які параметри команди usermod ви вважаєте найбільш використовуваними?**  
**-l new\_user:** Змінює ім'я користувача на new\_user.

**-d new\_home:** Встановлює новий домашній каталог користувача.

**-g group:** Змінює основну групу користувача на group.

**-G groups:** Додає користувача до додаткових груп (розділених комами).  
  
**-s shell:** Встановлює нову оболонку для користувача.  
  
**Висновки**   
Під час Лабораторної роботи ми ознайомились з базовими діями при створенні нових користувачів та нових груп користувачів.