“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”**

Виконав(ла/ли) студент(ка/и)

групи КСМ-13а

European TRO: Козаченко

М.О., Савіч М.М.

Перевірив викладач

Сушанова В.С.

Київ 2023

**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 (Windows 7).

3. Віртуальна машина – Virtual Box (Oracle).

4. Операційна система GNU/Linux – CentOS.

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

**Завдання для попередньої підготовки**

***Готував матеріал студент Савіч Матвій.***

1. Прочитайте короткі теоретичні відомості до лабораторної роботи та зробіть невеликий словник базових англійських термінів з питань призначення команд та їх параметрів.

|  |  |
| --- | --- |
| Термін англійською | Термін українською |
| Administrative Accounts | Адміністративні облікові записи |
| Root user | Користувач з правами адміністратора |
| Primary Group | Основна група |
| Viewing User Information | Перегляд інформації про користувача |
| Group Accounts | Групові облікові записи |
| Supplemental/Secondary Group | Додаткова група |
| UID (User ID) | Ідентифікатор користувача |

1. На базі розглянутого матеріалу дайте відповіді на наступні питання:
   1. Розкрийте поняття UPG, коли їх доцільно використовувати?

UPG (User Private Group) – це концепція в UNIX-подібних операційних системах, таких як Linux, яка автоматично створює окрему групу для кожного нового користувача з ідентичною назвою.

Доцільно використовувати UPG у таких випадках:

1. Підтримка безпеки. Уникнення можливості конфліктів доступу до файлів. Кожен користувач має свою власну групу, у якій він єдиний учасник, тому доступ до файлів обмежений для інших користувачів.
2. Забезпечення приватності користувача. Кожен користувач має свою власну групу, що дозволяє зберігати особисті файли в приватному режимі, обмежуючи доступ інших користувачів.
3. Легке управління доступом. Група UPG автоматично створюється при створенні нового користувача, що полегшує управління правами доступу до файлів та спільних ресурсів для цього користувача.
4. Зручність у роботі з файлами та спільними проектами. Якщо кілька користувачів працюють над спільними проектами, можна створити окремі групи UPG для кожного користувача. Це спрощує керування спільними ресурсами та спільною роботою над проектами.
   1. Якими командами можна створити групи користувачів? Наведіть приклади
5. groupadd – ця команда дозволяє створити нову групу в системі.

sudo groupadd \*назва групи\*.

Команда sudo використовують для тимчасового підвищення своїх привілегій на виконання завдань, що вимагають адміністративних прав.

1. addgroup - ця команда також створює нову групу користувачів.

sudo addgroup \*назва групи\*

* 1. Якими командами можна змінити налаштування груп користувачів? Наведіть приклади.

1. groupmod – ця команда дозволяє змінювати властивості і параметри існуючої групи користувачів.

sudo groupmod -n newname oldname

1. gpasswd – ця команда дозволяє управляти паролем групи або додавати/видаляти користувачів з групи.

sudo gpasswd -a username groupname

1. chgrp - ця команда змінює власника файлу або каталогу на іншу групу.

sudo chgrp newgroup filename

**Хід роботи**

***Готував матеріал студент Козаченко Микита.***

1. Початкова робота в CLI-режимі в Linux ОС сімейства Linux:

1.1. Запустіть віртуальну машину VirtualBox, оберіть CentOS та запустіть її. Виконайте вхід в систему під користувачем: CentOS, пароль для входу: reverse (якщо виконуєте ЛР у 401 ауд.) та запустіть термінал.

1.2. Запустіть віртуальну машину Ubuntu\_PC (якщо виконуєте завдання ЛР через академію netacad)

1.3. Запустіть свою операційну систему сімейства Linux (якщо працюєте на власному ПК та її встановили) та запустіть термінал.

2. Опрацюйте всі приклади команд, що представлені у лабораторних роботах курсу NDG Linux Essentials - Lab 15: System and User Security та Lab 16: Creating Users and Groups. Створіть таблицю для опису цих команд.

**\*Табл\***

3. Виконайте наступні практичні завдання у терміналі наступні дії (продемонструвати скріншоти):

- 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?

- 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;

- 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;

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

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

- перегляньте інформацію про існуючі групи користувачів;

- видаліть створені Вами групи користувачів;

- перегляньте інформацію про існуючі групи користувачів.

**Відповіді на контрольні запитання**

***Готував матеріал студент Савіч Матвій.***

* 1. Чому в конфігураційних файлах паролі не зберігається в явному вигляді?

Зберігання паролів в конфігураційних файлах в явному вигляді є небезпечним з точки зору безпеки і може стати причиною серйозних проблем з безпекою системи.

* 1. Чому не рекомендується виконувати повсякденні операції, використовуючи обліковий запис root?

1. Під час роботи в системі з правами root, ви можете випадково виконати команди або внести зміни, які можуть призвести до серйозних проблем для стабільності та функціональності системи.
2. Використання облікового запису root надає повний доступ до всіх системних ресурсів. Це означає, що якщо ваш обліковий запис скомпрометований або використовується необережно, це може стати причиною серйозних безпекових проблем, включаючи можливість несанкціонованого доступу зовнішніх атакувальників до системи.
3. Виконання операцій з правами root може призвести до видалення або модифікації важливих файлів або структур, що може призвести до втрати даних або навіть пошкодження файлової системи.
4. Якщо ви використовуєте обліковий запис root для повсякденних операцій, це ускладнює відстеження та аудит дій, виконаних вами чи іншими користувачами. Це може призвести до складнощів у виявленні помилок чи проблем.
   1. У чому відмінність механізмів отримання особливих привілеїв su і sudo?

Механізми su і sudo призначені для отримання особливих привілеїв в операційних системах подібних до Unix.

Відмінності:

1) su:

su дозволяє вам логуватися як інший користувач (зазвичай як root або інший користувач) шляхом введення його пароля.

Команда su переведе вас до облікового запису, який ви вказали, і до тих пір, поки не введете exit або Ctrl+D, ви залишаєтесь у цьому обліковому записі.

Вимагає від вас пароль облікового запису, до якого ви хочете змінити.

Використовується для тимчасового отримання прав користувача або адміністратора.

2) sudo:

sudo дозволяє користувачам виконувати окремі команди або скрипти з адміністративними привілеями, зазвичай без необхідності вводити пароль root.

Щоб використовувати sudo, користувач повинен мати право на його використання, і йому дозволяється виконувати команди, які вказані в файлі конфігурації sudoers.

Існує можливість налаштувати sudo для того, щоб користувачі могли виконувати певні команди без введення пароля.

sudo використовується для тимчасового отримання адміністративних прав для конкретної команди або серії команд без необхідності зміни користувача в цілому.

* 1. Чому домашній каталог користувача root не розміщено в каталозі /home?

1) Розділення домашнього каталогу користувача root допомагає уникнути плутанини між даними і робочими файли, які належать користувачеві root, і даними інших користувачів системи. Це зменшує ризик непередбачених змін чи видалення важливих даних користувачів.

2) Користувачі з обмеженими правами зазвичай не мають доступу до домашнього каталогу користувача root. Розміщення його в окремому місці допомагає утримати ці директорії від доступу неуповноважених користувачів.

3) У деяких системах архітектура файлової системи може бути такою, що користувач root має власний розділ або файлову систему, окрім загальної /home, з метою кращого управління правами доступу та збереженням важливих даних адміністратора.

* 1. Для чого використовується команда getent?

Команда getent використовується для отримання інформації про бази даних та сервіси, які використовуються для різноманітних операцій в системі. Вона дозволяє отримати дані з різних системних баз даних, таких як /etc/passwd, /etc/group, /etc/hosts і багатьох інших, які зберігаються в або використовуються операційною системою.

* 1. Яким чином можна видалити існуючі групи користувачів? Чи залишиться інформація про них десь у системі?

Для видалення існуючої групи користувачів використовується команда groupdel у більшості систем на базі Unix/Linux. Проте, перед видаленням групи необхідно впевнитися, що жоден користувач не є її членом, оскільки це може призвести до проблем доступу до файлів, які мають власника цієї групи.

Щодо інформації про видалені групи: після видалення групи її інформація прибирається з файлів /etc/group та /etc/gshadow. Однак, якщо ви створювали файли або встановлювали деякі права доступу, які були пов'язані з цією групою, ці відповідність файлів з видаленою групою також може бути видалена.

* 1. Як можна змінити пароль користувача?

Для зміни пароля користувача використовується команда passwd. Якщо ви хочете змінити пароль для іншого користувача, введіть: sudo passwd \*ім'я користувача\*.

* 1. Яке призначення команди chage?

Команда chage використовується для зміни параметрів терміну дії паролю користувача в системах Unix/Linux. Ця команда дозволяє адміністраторам налаштовувати та керувати політикою паролів для користувачів.

Основні функції команди chage:

1. Адміністратор може встановлювати термін дії паролю, після якого потрібно змінити пароль.
2. Команда chage також може встановлювати минулий час зміни паролю, після якого вимагається змінити пароль.
3. За допомогою команди chage можна встановити повідомлення, яке буде відображатися при вході користувача в систему перед закінченням терміну дії паролю.
   1. Які параметри команди usermod ви вважаєте найбільш використовуваними?

Команда `usermod` використовується для зміни налаштувань користувача в системі Unix/Linux.

Найбільш використовуванні:

1. -l, --login NEW\_LOGIN: Зміна логіну користувача на новий. Цей параметр дозволяє змінювати ім'я входу користувача.

2. -c, --comment COMMENT: Додавання коментаря до облікового запису користувача. Це поле може містити короткий опис або іншу інформацію про користувача.

3. -u, --uid UID: Зміна ідентифікатора користувача (UID). Цей параметр використовується для зміни числового ідентифікатора користувача.

4. -g, --gid GROUP: Зміна ідентифікатора групи (GID). Цей параметр використовується для зміни основної групи користувача.

5. -G, --groups GROUPS: Додавання користувача до додаткових груп. Цей параметр дозволяє вказати список груп, до яких користувач може належати, відділяючи їх комами.

6. -a, --append: Додавання користувача до додаткових груп без заміни існуючих груп.

7. -e, --expiredate EXPIRE\_DATE: Встановлення дати закінчення терміну дії облікового запису користувача. Це поле визначає дату, після якої обліковий запис буде вважатися неактивним.

8. -d, --home HOME\_DIR: Зміна домашнього каталогу користувача. Цей параметр використовується для зміни шляху до домашнього каталогу користувача.

9. -s, --shell SHELL: Зміна оболонки користувача. Цей параметр встановлює шлях до оболонки, яку користувач використовує при вході в систему.

**Висновки**

a