“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 Linux. Створення користувачів та груп”**

Виконали студенти

групи РПЗ-13А та РПЗ-13Б

Eleven Two Zeroes:

Vlad Sapozhnyk

Max Karpenko

Dmytro Onufriiev

Київ 2024

Робота студентів групи РПЗ-13А та РПЗ-13Б Eleven Two Zeroes: Vlad Sapozhnyk, Max Karpenko and Dmytro Onufriiev.

**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: *Created by Vlad Sapozhnyk***

1. Розкрийте поняття UPG, коли їх доцільно використовувати?

A User Private Group (UPG) is a specific group that is automatically created when a new user account is added on certain operating systems.

Features of UPG:

* Uniqueness: Each user is assigned a unique UPG with a name identical to the username.
* Sole member: The user is the only member of his/her UPG. No other users are added to this group.
* Permission preferences: UPGs are primarily used to simplify the management of permissions for newly created files and directories. By default, these files and directories are granted read/write access for both the user and their UPG.

Advantages of UPG:

* Simpler permissions: UPGs eliminate the need to explicitly assign group ownership to new files, making permission management clearer.
* More secure defaults: With a UPG, even if the system's default mask (the value that determines the initial permissions of files) restricts write access to others, the user and their UPG can still modify their files.

When are UPGs useful?

* UPGs are especially useful on systems where users frequently create and manage their own files and directories.
* They simplify the management of permissions, especially for individual users who mostly work with their own files.

Are there any drawbacks to UPGs?

UPGs may not be optimal for collaborative environments where multiple users need to access and modify each other's files. In such cases, separate group memberships may be more appropriate.

1. \*Якими командами можна створити групи користувачів? Наведіть приклади

* groupadd: This command is used to create a new group.

*sudo groupadd groupname*

* usermod: This command is used to add users to an existing group.

*sudo usermod -G group\_name username*

* groups: Use this command to view the groups to which a user belongs.

*groups username*

* gpasswd: This command allows you to manage user membership in groups.

*sudo gpasswd username group\_name*

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

* groupmod: This command is used to modify the settings of an existing group.

sudo groupmod -o options -g new\_GID group\_name

* chgrp: This command is used to change the primary user group.

sudo chgrp group name username

Glossary of Terms

| Name of term | Explanation |
| --- | --- |
| User Account | A record in the operating system that identifies a specific user and grants them access to the system's resources. |
| Root user | The user with the highest level of privileges and access on a Linux system. |
| sudo | A command-line tool that allows a user to execute commands with the privileges of another user, typically the root user. |
| Home directory | directory in the file system that is assigned to a specific user and typically contains their personal files and configuration settings. |
| Group | A collection of users that can be assigned specific permissions to access files and resources. |
| User Private Group (UPG) | A special type of group created automatically for a new user on some Linux distributions. |
| Primary group | The default group associated with a user account. |

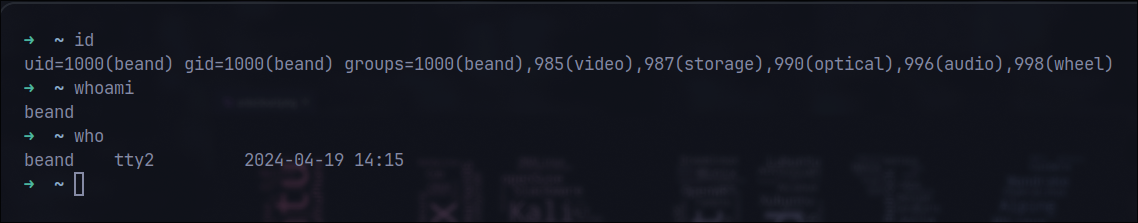
**Хід роботи. *Created by Max Karpenko***

**Хід роботи:**

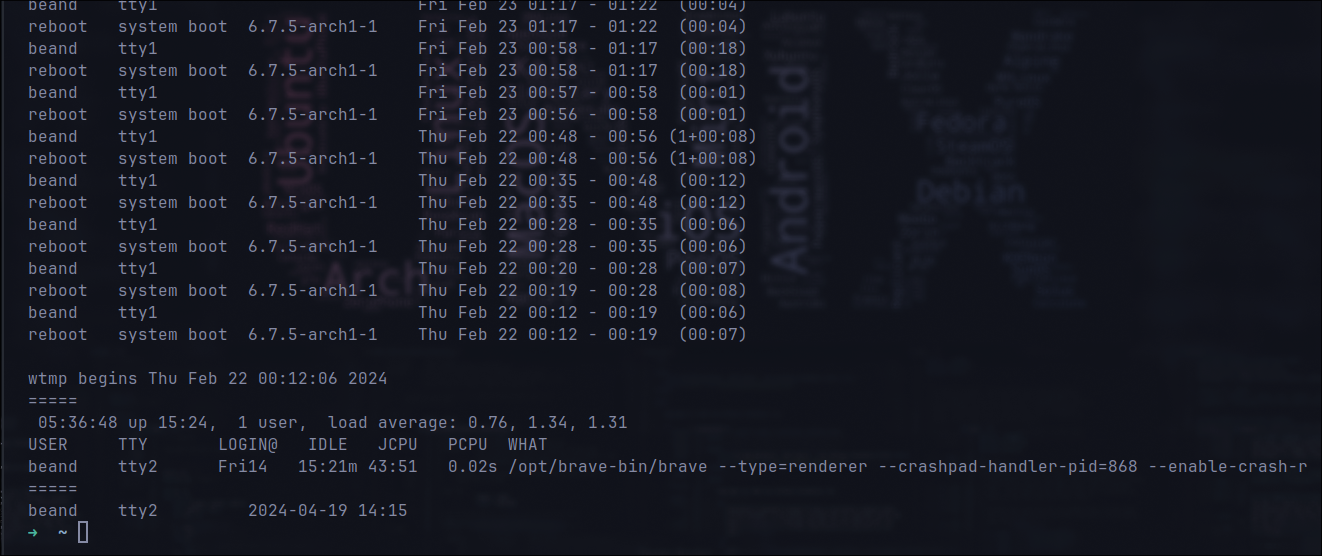
* 1. Початкова робота в CLI-режимі в Linux ОС сімейства Linux:
  2. Запустіть віртуальну машину VirtualBox, оберіть CentOS та запустіть її. Виконайте вхід в систему під користувачем: CentOS, пароль для входу: reverse ***(якщо виконуєте ЛР у 401 ауд.)*** та запустіть термінал.
  3. Запустіть віртуальну машину Ubuntu\_PC ***(якщо виконуєте завдання ЛР через академію netacad)***
  4. Запустіть свою операційну систему сімейства Linux ***(якщо працюєте на власному ПК та її встановили)*** та запустіть термінал.
  5. 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

| Назва команди | Її призначення та функціональність |
| --- | --- |
| passwd | Змінює або оновлює пароль користувача. Користується для забезпечення безпеки акаунтів шляхом оновлення паролів. |
| useradd | Створює новий користувацький акаунт. Дозволяє налаштувати початкові параметри для нового користувача. |
| userdel | Видаляє користувацький акаунт. Використовується для управління користувачами в системі. |
| groupadd | Створює нову групу користувачів. Дозволяє адміністраторам групувати користувачів за певними критеріями. |
| groupdel | Видаляє групу користувачів. Використовується для управління групами в системі. |
| chmod | Змінює права доступу до файлів або директорій. Важлива команда для налаштування контролю доступу до ресурсів. |
| chown | Змінює власника файлу або директорії. Дозволяє адміністраторам керувати правами на файли та директорії. |
| chgrp | Змінює групу файлу або директорії. Використовується для керування доступом до файлів за допомогою груп. |
| umask | Встановлює маску створення файлу за замовчуванням, що впливає на права доступу створених файлів і директорій. |
| su | Переключає поточного користувача на іншого користувача (часто на root), надаючи можливість виконувати команди з іншими правами. |

* 1. **Виконайте наступні практичні завдання у терміналі наступні дії (продемонструвати скріншоти):**
* **виведіть інформацію про поточного користувача різними способами (підказка використовуйте команди id та grep);**

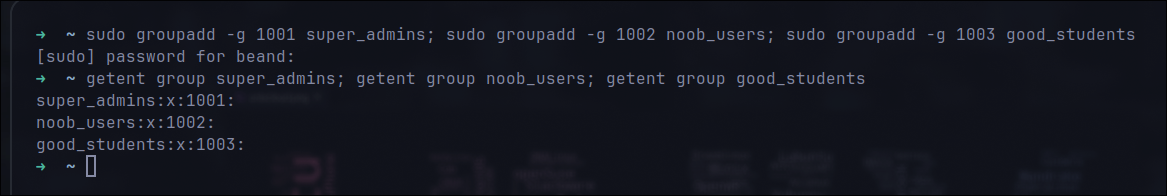
****

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

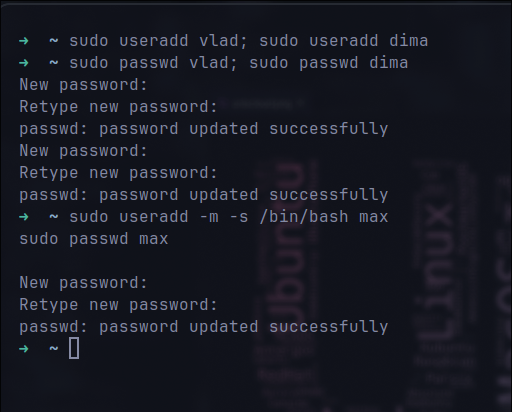
****

**Comparison**

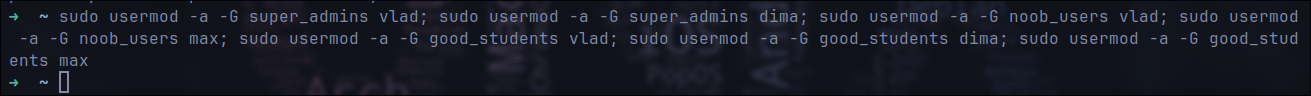
* **Login history details:** The last command provides a complete history of user logins with details about the time of login, logout, and the terminal used.
* **Active users and their sessions:** The w command displays the active users and their sessions, along with terminals, login times, and active processes.
* **List of logged in users:** The who command provides only a list of logged-in users and terminals, without any additional details.
* **\*створіть дві нові групи користувачів - super\_admins, noob\_users та good\_students, визначте їх ідентифікатори;**

****

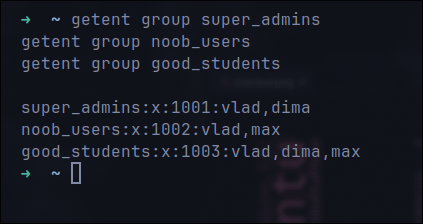
* **\*для кожного члену Вашої команди за допомогою терміналу створіть нового користувача (якщо працюєте самі, то просто трьох довільних користувачів), не забудьте після створення нового користувача одразу задати йому пароль;**

****

* **\*\*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;**

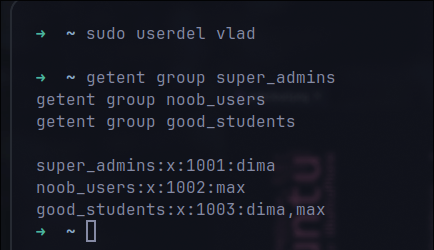
****

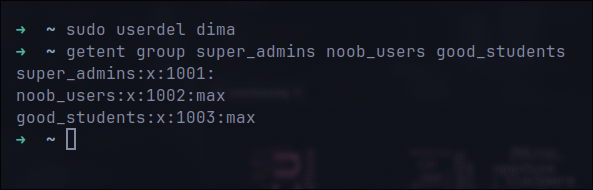
* **\*\*перегляньте інформацію про групи, та які користувачі до них входять, поясніть що ви бачите;**

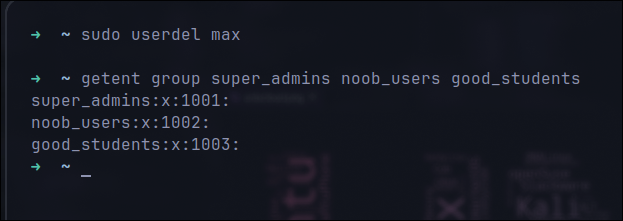
****

**Explanation.**

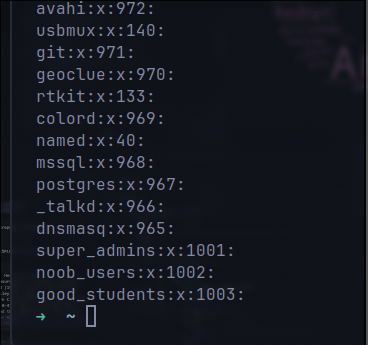
* **super\_admins:** You should see that the group includes users vlad and dima. This means that both users have administrator privileges that can be granted through this group.
* **noob\_users:** This group should contain users vlad and max. This may mean that these users are restricted in some rights or capabilities if the group has appropriate policies set.
* **good\_students:** This group should contain all three users: vlad, dima, and max. This may indicate that these users are jointly involved in certain educational or training activities.
* **\*\*видаліть першого створеного вами користувача, перегляньте чи залишиться інформація про нього в групах, де він перебував;**

****

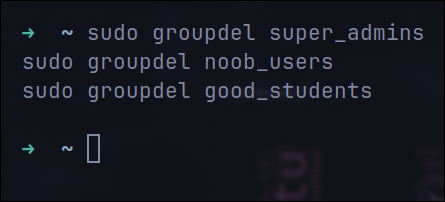
* **\*\*видаліть другого користувача, перегляньте чи залишиться інформація про нього в групах, де він перебував;**
* ****
* **\*\*видаліть третього користувача, перегляньте чи залишиться інформація про нього в групах, де він перебував;**

****

* **\*\*перегляньте інформацію про існуючі групи користувачів;**

****

* **\*\*видаліть створені Вами групи користувачів;**

****

* **\*\*перегляньте інформацію про існуючі групи користувачів.**

****

**Контрольнi запитання: *Created by Dmytro Onufriiev***

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

Storing passwords explicitly makes them vulnerable to theft. If an attacker gains access to the configuration file, they can easily see all the passwords stored there. This can lead to serious security issues, such as compromised accounts, data theft, or even loss of control of the system.

Instead of storing passwords explicitly, they are usually hashed. Hashing is the process of converting a password into an irreversible string of characters called a hash. Even if an attacker gains access to the password hash, they won't be able to decrypt it to get the original password. This makes passwords much more resistant to theft.

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

The root account has the highest level of permissions on a Linux system. This means that the root user can do anything they want with the system, including deleting important files, changing critical settings, and even granting access to the system to other users. If an attacker gains access to the root account, they can cause serious damage to the system.

Using the root account for daily operations can lead to system instability. This is because the root user can easily make mistakes that can lead to system crashes or damage.

If you make a mistake while using the root account, it can be difficult to restore the system. That's because you won't have access to the root account if you accidentally delete it or change its password.

1. **\*У чому відмінність механізмів отримання особливих привілеїв su і sudo?**

su:

su is used to completely switch to another user account. This means that you have access to that user's environment and files, as well as their rights and privileges.

To use su, you will be required to enter the password of the target user you want to switch to. This can be risky because you gain full control over that account.

Because of the risks involved in completely switching to another account, su is not recommended for general use, especially for granting administrator (root) privileges.

sudo:

sudo is used to execute individual commands as another user, usually root.

Instead of the target user's password, sudo requires your current user's password. This makes it more secure because you don't reveal your administrator password.

Access control and permissions for sudo are configured in the /etc/sudoers file. This allows you to clearly define which users can execute which commands with root or other administrator privileges.

sudo is the best choice for granting users rights to perform administrative tasks because it gives them access to only certain commands without giving them full control of the root account.

Translated with DeepL.com (free version)

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

Placing the root directory in /home increases the risk that an attacker who has access to another user account on the system will also be able to access the root files. By keeping the root directory in a different location, we make it more secure. If the root directory were placed in /home, an attacker who gained access to it could potentially cause significant damage to the system.By isolating the root directory, we limit the possible scope of damage.

1. **\*Для чого використовується команда getent?**

The getent command is used to retrieve information from system databases about users, groups, network services, and other system resources.

1. **\*Як можна змінити пароль користувача?**

1. To use the passwd command

Open a terminal. Type the passwd command and press Enter. The system prompts you to enter your current password. Enter it and press Enter. The system prompts you to enter a new password. Enter it and press Enter. The system prompts you again for a new password. Enter it again for confirmation and press Enter. Your password is now changed.

2. To use the sudo command

Open a terminal. Enter the sudo passwd [user] command, replacing [user] with the name of the user whose password you want to change. The system prompts you to enter the password. Type the root or sudo password and press Enter. The system prompts you to enter a new password for [user]. Enter it and press Enter. The system prompts you again for the new password. Enter it again for confirmation and press Enter. The user's password is changed.

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

To remove existing user groups in Linux, use the groupdel command. It removes a user group from the system. For example:

*sudo groupdel <group\_name>*

Note that to remove a group, may be needed to remove all users who belong to it. Group information can be stored in the /etc/group file. When deleting a group, this information will be removed from this file. Also, some system files may refer to a group, and these references may remain, but they will not refer to the existing group.

1. **\*\*Яке призначення команди chage?**

The chage command in Linux is used to change the attributes of a user's password. It is typically used to set the password expiration date or to set other parameters of the user's password.

1. **\*\*Які параметри команди usermod ви вважаєте найбільш використовуваними?**

The most commonly used options for the usermod command on Linux typically:

-a, --append, adds a user to additional groups without changing their main group.

-c, --comment, allows you to set a comment or information about the user.

-d, --home, sets the user's home directory.

-g, --gid, sets the user's main group ID.

-G, --groups, sets the list of additional groups to which the user belongs.

-l, --login, changes the user's login name.

-p, --password, sets the user's password (typically used to import a hashed password).

-s, --shell, sets the user's login shell.

**Висновок:**

In this group activity, we learned the basic steps for creating new users and new user groups in the Bash shell. Learning Linux commands for managing users and groups is an important part of system administration skills.

We learned how to create new users (useradd), assign them groups and passwords, and how to create new user groups (groupadd). In addition, we learned how to delete existing groups (groupdel) and how to modify user account attributes using the usermod command.