**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 (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.**

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

**Хід роботи.**

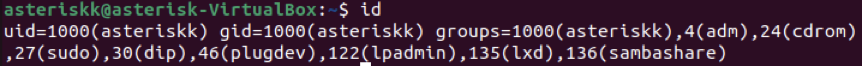
1. Опрацюйте всі приклади команд, що представлені у лабораторних роботах курсу ***NDG Linux Essentials - Lab 15: System and User Security*** та ***Lab 16: Creating Users and Groups.*** Створіть таблицю для опису цих команд\*\*\*

| Назва команди | Її призначення та функціональність |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

\*\*\***Скріншоти** виконання команд в терміналі можна **не представляти**, достатньо **коротко описати команди в таблиці**.

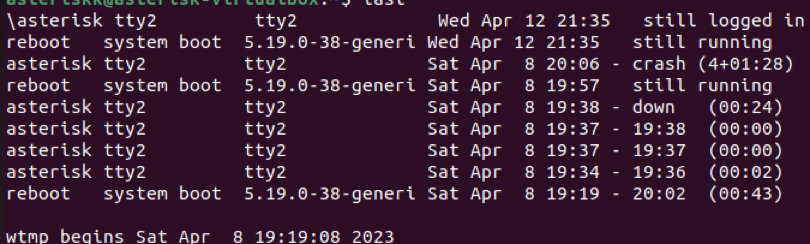
1. Виконайте наступні практичні завдання у терміналі наступні дії (продемонструвати скріншоти):

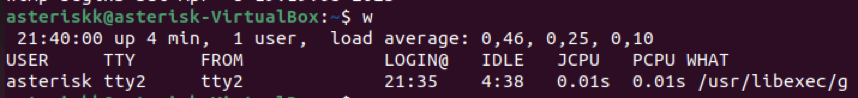
* виведіть інформацію про поточного користувача різними способами (підказка використовуйте команди id та grep);

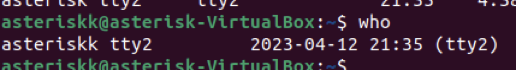




* попрактикуйте в терміналі команди last, w та who. Порівняйте результати виводу кожної команди, які деталі відсутні в кожній із команд порівняно з іншими?

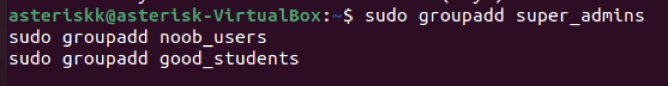


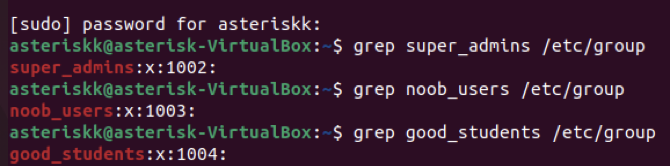




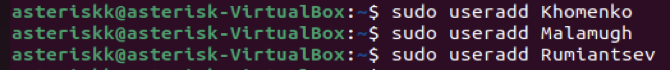
1. Команда last виводить інформацію про останні входи користувачів у систему. Крім імені користувача та дати часу та входу, вона також надає інформацію про тривалість сесії та IP-адресу, з якою було здійснено вхід. Однак ця команда не виводить поточну інформацію про користувачів.
2. Команда w виводить поточну інформацію про користувачів, які зараз залогінені в системі. Інформація містить ім’я користувача, термінал, на який він зареєструвався, час входу та завантаження в систему, а також процеси, які застосовуються в терміналі. Однак ця команда не виводить інформацію про попередні входи користувачів.
3. Команда, who виводить інформацію про поточні залогінені сесії. Інформація містить ім’я користувача, термінал, на який він зареєструвався, дату та час входу. Відмінність від команди виникла в тому, що вона не виводить деталі про процеси та завантаження в систему.

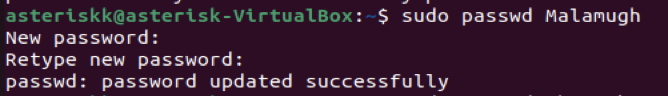
* створіть дві нові групи користувачів - super\_admins, noob\_users та good\_students, визначте їх ідентифікатори;



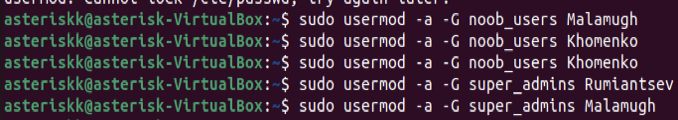


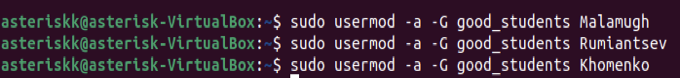
* для кожного члену Вашої команди за допомогою терміналу створіть нового користувача (якщо працюєте самі, то просто трьох довільних користувачів), не забудьте після створення нового користувача одразу задати йому пароль;



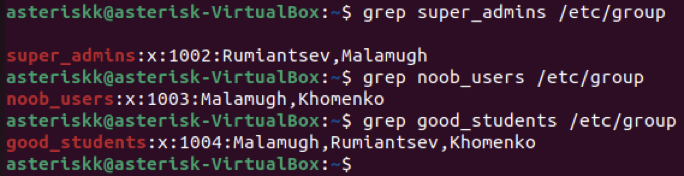


* додайте нових користувачів у створені Вами нові групи таким чином, щоб у групах super\_admins та noob\_users було по 2 користувачі, один з яких є в обох групах, у групу good\_students додайте всіх трьох користувачів;



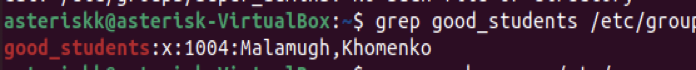


* перегляньте інформацію про групи, та які користувачі до них входять, поясніть що ви бачите;

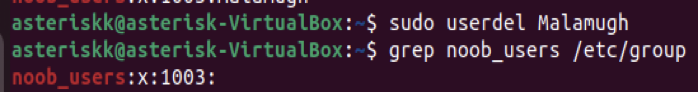


* видаліть першого створеного вами користувача, перегляньте чи залишиться інформація про нього в групах, де він перебував;





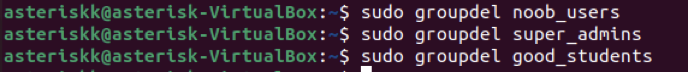
* видаліть третього користувача, перегляньте чи залишиться інформація про нього в групах, де він перебував;



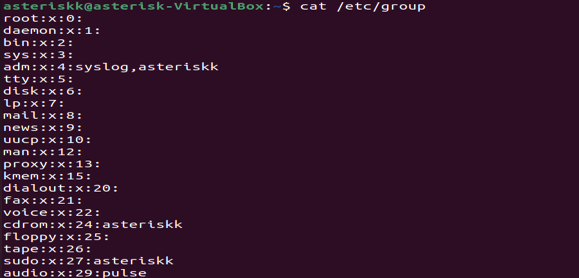
* перегляньте інформацію про існуючі групи користувачів;



* видаліть створені Вами групи користувачів;



* перегляньте інформацію про існуючі групи користувачів.



**Контрольні запитання**

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

Passwords are not explicitly stored in configuration files in Linux for security reasons. If passwords were stored in plain text in configuration files, they could be easily accessed by unauthorized users or attackers who gain access to the file. This could compromise the security of the system and any sensitive data that it holds.

Instead, Linux uses a technique called password hashing to store passwords. When a user creates a password, it is encrypted using a one-way cryptographic function called a hashing algorithm, and the resulting hash value is stored in a file called the "shadow file". The actual password is never stored in the shadow file, only its hashed value.

When a user logs in, the system hashes the password that the user enters and compares it to the hashed value stored in the shadow file. If the hashes match, the user is granted access to the system. This approach ensures that the actual password is never stored in plain text, making it much more difficult for attackers to access the password and compromise the system.

In addition to password hashing, Linux also uses other security measures such as file permissions, access controls, and audit logs to protect the system and monitor any attempts to access sensitive data, including passwords.Чому не рекомендується виконувати повсякденні операції, використовуючи обліковий запис root?

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

su and sudo are two commands that allow users to execute commands with elevated privileges on a Linux or Unix-based system, but there are some key differences between the two.

The su command stands for "switch user" or "substitute user". It allows a user to log in as another user, typically the root user, and execute commands with that user's privileges. When you use the su command, you are prompted to enter the password of the user account that you want to switch to. Once you have entered the correct password, you will be granted the same level of privileges as that user. You can then execute any commands with that user's permissions.

On the other hand, the sudo command stands for "superuser do". It allows a user to execute a single command with elevated privileges, without having to log in as another user. When you use the sudo command, you are prompted to enter your own password, not the password of the root user. If your account has been granted permission to execute the command with elevated privileges, the command will be executed as if you were the root user.

The key difference between the two commands is that su allows you to switch to another user's account and run commands with their privileges, while sudo allows you to run a single command with elevated privileges using your own account. sudo is typically considered more secure, as it limits the scope of the commands that can be run with elevated privileges and avoids the need to log in as the root user. However, su can be useful in some situations where you need to execute a series of commands as another user, or if you need to log in as the root user to perform system maintenance tasks.

3. Для чого використовується команда getent?

The getent command in Linux is used to retrieve information about system accounts and services from various sources including files, databases, and network services.

The getent command allows you to query system databases such as /etc/passwd, /etc/group, and /etc/hosts as well as network services such as LDAP and NIS to retrieve information about users, groups, hosts, and other system entities.

For example, you can use the getent passwd command to retrieve a list of all user accounts on the system, including information such as the username, user ID, group ID, home directory, and shell. Similarly, the getent group command can be used to retrieve information about all the groups on the system, including the group name, group ID, and list of members.

The getent command is often used in shell scripts and other automation tasks to retrieve system information programmatically. It can also be useful for troubleshooting network issues, as it allows you to verify information about network services such as LDAP or NIS.

In summary, the getent command is a powerful tool that allows you to retrieve system information from various sources and can be useful for managing user accounts, groups, and network services on a Linux system.

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

In Linux, you can delete existing user groups using the groupdel command. The groupdel command is used to remove a group from the system, including its associated group ID (GID) and any membership information.

To delete a group, you can use the following command:

sudo groupdel <groupname>

Replace <groupname> with the name of the group that you want to delete.

When you run the groupdel command, it will remove the group from the system and all associated information, including group membership information. Any files or directories that were owned by the group will have their group ownership changed to the group with GID 0, typically the root group.

Note that while the group and its associated information will be removed from the system, there may be some residual information left in system logs or other files. Additionally, any files or directories that were owned by the group before it was deleted will still contain that group's GID in their metadata, even though the group no longer exists. However, this should not cause any functional issues on the system.

You can delete existing user groups using the groupdel command in Linux. This will remove the group from the system and all associated information, although some residual information may remain in system logs or other files.

5. Як можна змінити пароль користувача?

To change your password, follow these steps:

Open a terminal window.

* Type the following command and press Enter: passwd
* You will be prompted to enter your current password.
* After entering your current password, you will be prompted to enter your new password twice.
* Follow the prompts to enter your new password and confirm it.

6.Яке призначення команди chage?

The chage command in Linux is used to configure the aging policy for user passwords. It allows administrators to set various password expiration policies for user accounts, such as the maximum age of the password, minimum age of the password, and the number of days before the password expires that the user will receive a warning message.

The chage command is useful for enhancing the security of the system by ensuring that users change their passwords periodically and that the passwords are sufficiently complex. By setting password aging policies, you can enforce good password hygiene and reduce the risk of unauthorized access to the system.

7.Які параметри команди usermod ви вважаєте найбільш використовуваними?

The usermod command in Linux is used to modify user account settings, such as the user's login name, home directory, default shell, and group membership. Here are some of the most commonly used parameters of the usermod command:

-l, --login: This option is used to change the user login name. For example, if you want to change the login name of the user "jdoe" to "johndoe", you would use the following command: sudo usermod -l johndoe jdoe.

-d, --home: This option is used to change the user's home directory. For example, if you want to change the home directory of the user "jdoe" to "/home/johndoe", you would use the following command: sudo usermod -d /home/johndoe jdoe.

-s, --shell: This option is used to change the user's default shell. For example, if you want to change the default shell of the user "jdoe" to "/bin/bash", you would use the following command: sudo usermod -s /bin/bash jdoe.

-aG, --append: This option is used to add a user to a supplementary group. For example, if you want to add the user "jdoe" to the "wheel" group, you would use the following command: sudo usermod -aG wheel jdoe.

-u, --uid: This option is used to change the user's UID (user ID). For example, if you want to change the UID of the user "jdoe" to 1001, you would use the following command: sudo usermod -u 1001 jdoe.

**Оформлення звіту:**

1. Титульний аркуш
2. Тема та мета роботи
3. Завдання попередньої підготовки
4. Основні позиції ходу роботи
5. Відповіді на контрольні запитання
6. Висновки за результатами роботи **(обов’язково!!!)**