“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»

Виконала студентка
групи РПЗ-13б
Дімітрова С.П.
Перевірив викладач
Сушанова В.С.

Київ 2024

Робота студентки групи РПЗ-13б Дімітрової Софії

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.

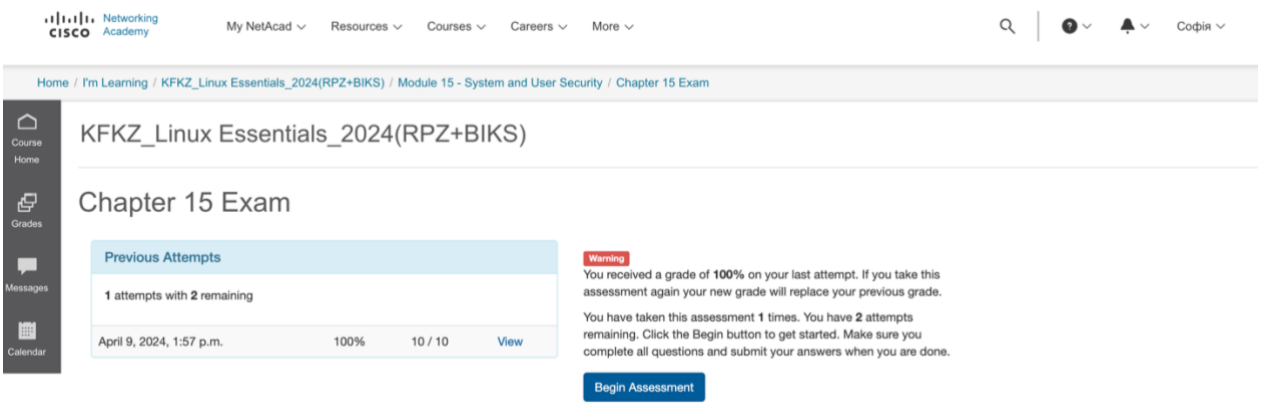
Термін англійською	Термін українською
permission	дозвіл
primary group	основна група
collaborate	співпрацювати
access	доступ
selective access	обмежений доступ
efficient	ефективний
standard user	звичайний користувач
UID	ідентифікатор користувача
group ID (GID)	ідентифікатор групи
group membership	членство в групі
unprivileged user (non-root)	непривілейований користувач
network-based authentication	автентифікація в мережі

2. Вивчіть матеріали онлайн-курсу академії Cisco “NDG Linux Essentials”:

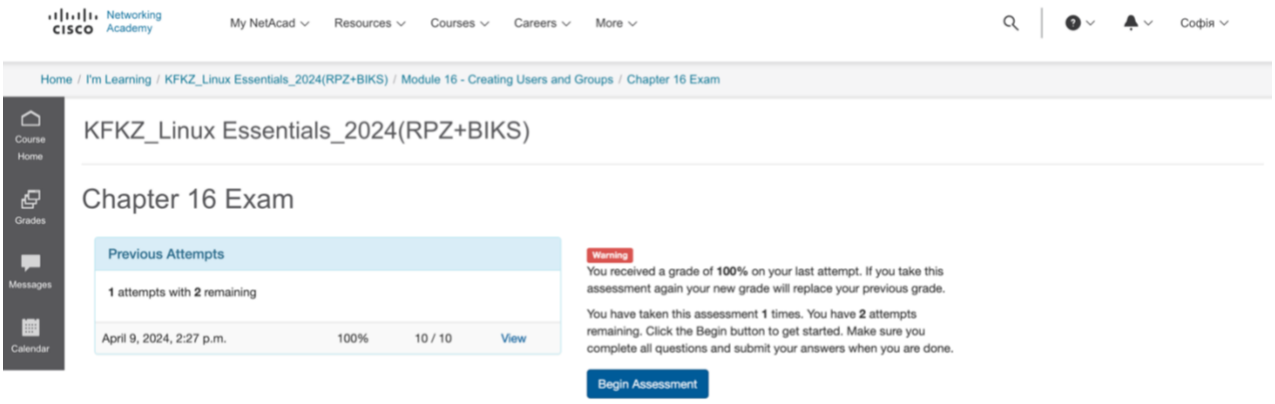
- Chapter 15 - System and User Security
- Chapter 16 - Creating Users and Groups

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

- Chapter 15 Exam



- Chapter 16 Exam



4. На базі розглянутого матеріалу дайте відповіді на наступні питання:

4.1 Розкрийте поняття UPG, коли їх доцільно використовувати?

UPGs (User Private Groups) are special user groups that are automatically created when a new user is created on some Linux distributions. In these groups, the username is the same as the group name, and the user automatically becomes the only member of this group. UPGs are useful when you need to provide isolated access to files and services for individual users who do not share resources with other users. This can be useful in environments where data security and access restrictions are important.

4.2 *Якими командами можна створити групи користувачів? Наведіть приклади

The *groupadd* command can be executed by the *root user* to create a new group. The command requires only the name of the group to be created.

The *-g* option can be used to specify a group id for the new group. If the *-g* option is not provided, the *groupadd* command will automatically provide a GID for the new group.

4.3 **Якими командами можна змінити налаштування груп користувачів? Наведіть приклади

The *groupmod* command can be used to either change the name of a group with the *-n* option or change the GID for the group with the *-g* option.

Хід роботи:

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.

Назва команди	**Її призначення та функціональність**
NDG Linux Essentials - Lab 15: System and User Security	
su	Command that allows users to run a shell as a different user.
sudo	Command that allows users to execute commands as another user.
su -	Command used to switch users to the root account.
id	Command used to print user and group information for a specified user.
exit	Return to your original shell. Exiting the shell is important to avoid executing commands as root that could damage the system.
sudo head /etc/shadow	If the current user is part of the sudo group, the command will be executed. /etc/shadow - file that contains account information related to the user's password.
head /etc/passwd	View the first ten lines from the /etc/passwd file. /etc/passwd - file that defines some of the account information for user accounts.
grep sysadmin /etc/passwd	View the record for your sysadmin account. By using the grep command, the output only includes the account information for that one username.
sudo head -3 /etc/shadow	View the first few lines of the /etc/shadow file.
getent passwd sysadmin	Use the getent command to retrieve the information about the sysadmin.
who	Command displays a list of users who are currently logged into the system, where they are logged in from, and when they logged in.
w	Command provides a detailed list about the users currently on the system and a summary of the system status.

last	View the /var/log/wtmp file which keeps a log of all users who have logged in and out the system.
NDG Linux Essentials - Lab 16: Creating Users and Groups	
groupadd	Command used to create new groups.
groupadd -r research groupadd -r sales	Command to create groups called research and sales. The research and sales groups that were just added were added in the reserved range (between 1-999) because the -r option was used.
getent group research	Command to retrieve information about the new research group.
grep sales /etc/group	Command to retrieve information about the new sales group. /etc/group - file that contains group configuration information.
groupmod	Command used to make changes to groups.
groupmod -n clerks sales	groupmod command with the -n option changes the name of the sales group.
groupmod -g 10003 clerks	groupmod command with the -g option changes the GID for the group.
grep clerks /etc/group	Use the grep command to verify the changes made above.
groupdel	The groupdel command can be used to delete a group.
groupdel clerks	Delete the clerks group
grep clerks /etc/group	Verify that the clerks group has been removed
useradd	Command used to create new users.
useradd -D	The -D option to the useradd command will allow you to view or change some of the default values.
useradd -D -f 30	The -f 30 option specifies that users who have expired passwords can still log in for up to thirty days before their accounts are inactivated.
useradd -G research -c 'Linux Student' -m student	The command will create a new user named student, add it to the research group, set its description to Linux Student, and create a home directory for it. -G research: adds the new user to the ‘research’ group.

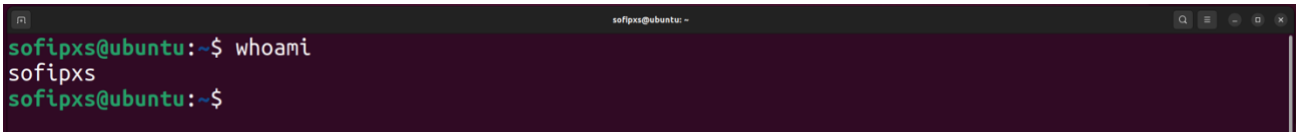
	-c 'Linux Student': sets the comment for the user to ‘Linux Student’. -m: creates the home directory for the user.
usermod	Command used to make changes to the user account.
usermod -aG research sysadmin	Use the usermod command to add the research group as a secondary group for the sysadmin user. The -a (append) option is used with -G to prevent the user from being removed from other groups.
getent passwd student getent shadow student	Show the passwd and shadow databases for the student user.
passwd	Command used to set or update user passwords.
last student	Command is used to display the last login of the user ‘student’.
userdel -r student	Delete the student account and remove the user's home directory. Using the -r option with the userdel command removes the user's home directory and mail, in addition to deleting the user's account.
grep student /etc/group	Command to verify the student user has been removed.

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

     - The *id* command is used to print user and group information.

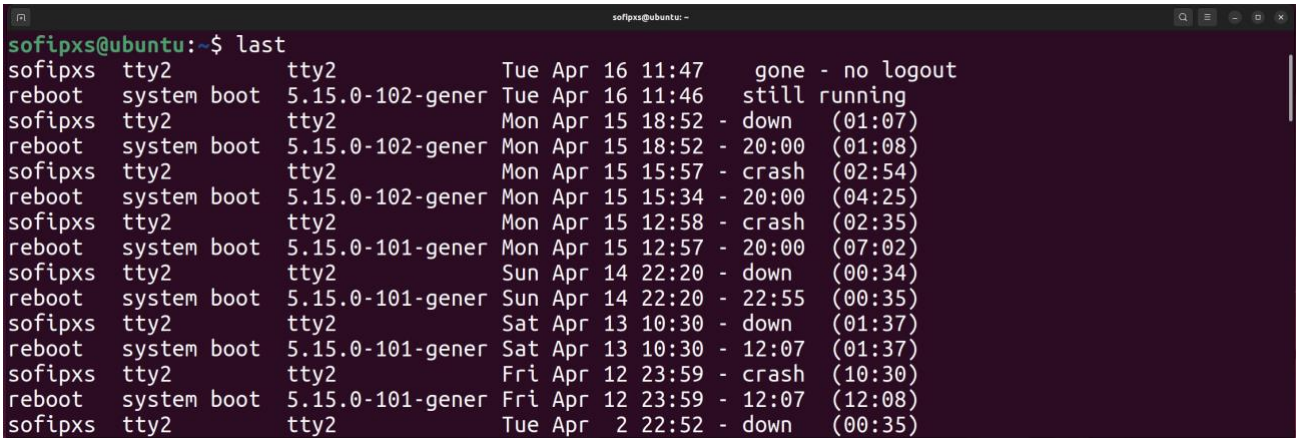
     - By using the *grep* command, the output only includes the account information for that one username.

     - The *whoami* command: displays the name of the current user.

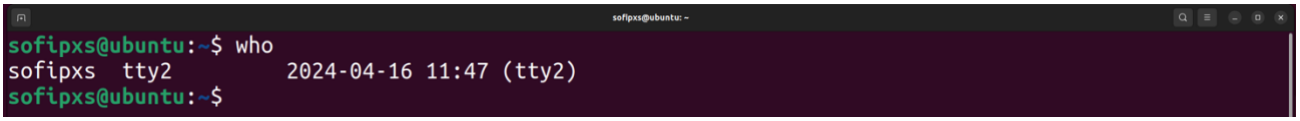


- *попрактикуйте в терміналі команди last, w та who. Порівняйте результати виводу кожної команди, які деталі відсутні в кожній із команд порівняно з іншими?

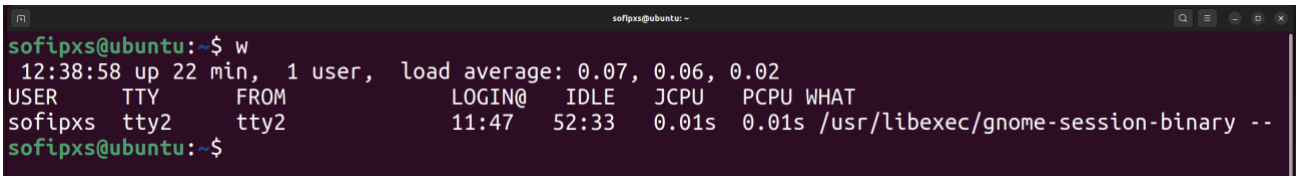
  - The *last* command reads the /var/log/wtmp file all login records. Shows previous login sessions as well as current login information.



  - The *who* command lists users who are currently logged in, as well as where and when they logged in.



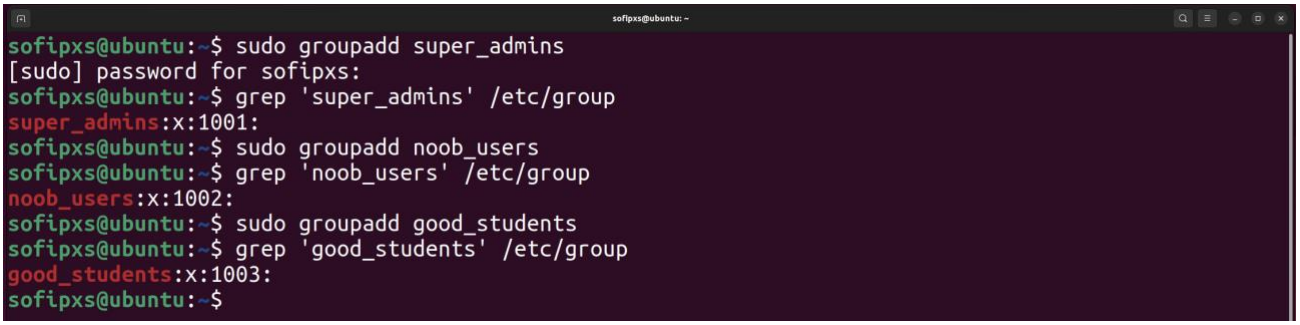
  - The *w* command provides more detailed information about users currently on the system. Provides info about system status.



The main difference between them is that *last* shows the history of logins and logouts, *w* gives more details about current users, and *who* gives a shorter view. Each of these commands serves a different purpose and can be used in different contexts.

- *створіть дві нові групи користувачів - super_admins, noob_users та good_students, визначте їх ідентифікатори;

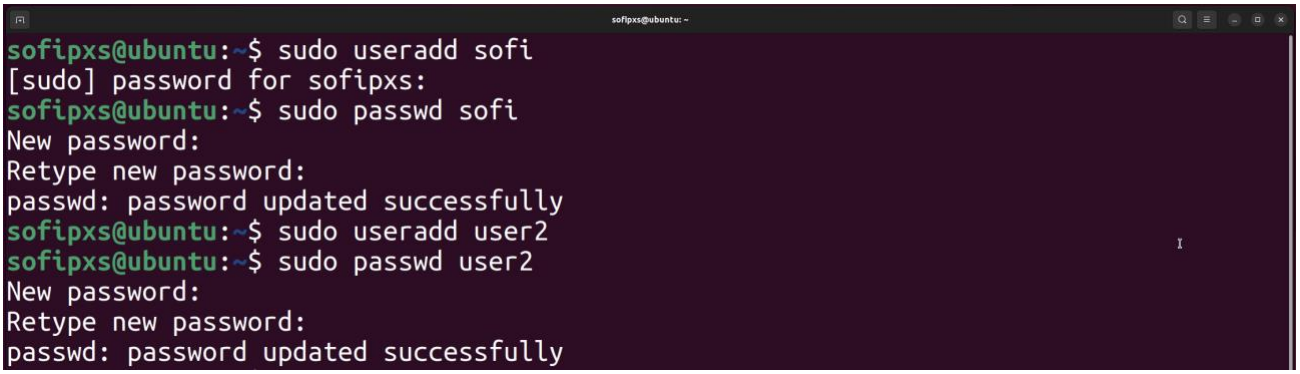
To create new user groups, use the *groupadd* command. To determine the identifiers of these groups, use the *grep* command to search for the group name in the */etc/group* file, which contains information about all groups.



Also, group IDs can be found using command *getent group*:

- *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;

To create new users, use the *useradd* command. And to set a password for a new user, use the *passwd* command.



```
sofipxs@ubuntu:~$ sudo useradd user3
sofipxs@ubuntu:~$ sudo passwd user3
New password:
Retype new password:
passwd: password updated successfully
sofipxs@ubuntu:~$
```

- **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;

  Use the *usermod* command to add users to groups:

```
sofipxs@ubuntu:~$ sudo usermod -aG super_admins sofi
sofipxs@ubuntu:~$ sudo usermod -aG super_admins user2
sofipxs@ubuntu:~$ sudo usermod -aG noob_users sofi
sofipxs@ubuntu:~$ sudo usermod -aG noob_users user3
sofipxs@ubuntu:~$ sudo usermod -aG good_students sofi && sudo usermod -aG good_studen
ts user2 && sudo usermod -aG good_students user3
sofipxs@ubuntu:~$
```

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

  To view information about groups and their members, use the *getent group groupname* command.

```
sofipxs@ubuntu:~$ getent group super_admins
super_admins:x:1001:sofi,user2
sofipxs@ubuntu:~$ getent group noob_users
noob_users:x:1002:sofi,user3
sofipxs@ubuntu:~$ getent group good_students
good_students:x:1003:sofi,user2,user3
sofipxs@ubuntu:~$
```

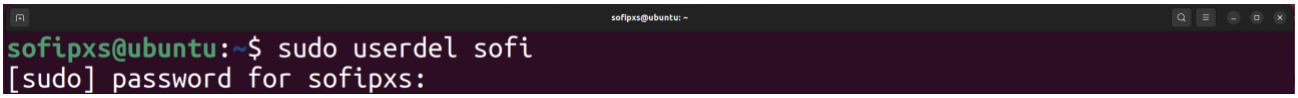
After executing this command in the terminal, we will get the group, its identifier, and the users who are members of it.

super_admins:x:1001:sofi,user2 — group:password:GID:user(s)

- group is the group's name
- password is the encrypted group password, empty field signifies no password, x bit signifies the password is in the file /etc/gshadow
- GID is the Group ID
- user(s) is the list of users member of this group, empty means this group has no member.

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

To delete a user use the *sudo userdel username* command:

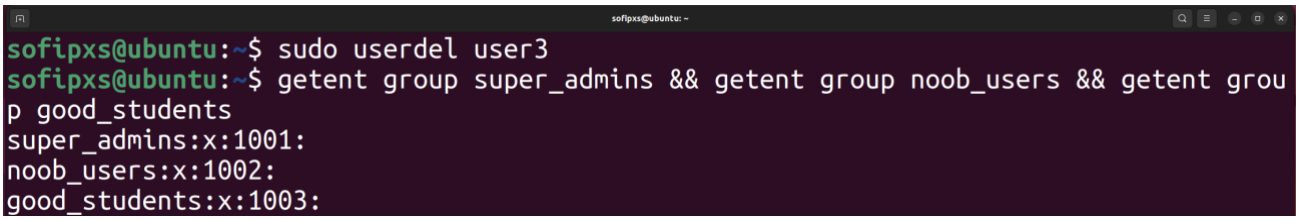


To delete a user along with his home directory, use the command sudo userdel -r user1. When a users are deleted from the system, their information should be removed from all groups to which they belonged. As we can see, there is no longer a *sofi* user in the groups.

- **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;

Again, use the *getent* command to view information about the groups. As we can see, the deleted users no longer appear in the list of group members.



- **перегляньте інформацію про існуючі групи користувачів;

To view information about existing user groups, use the getent group command in the terminal. This command displays a list of user groups, their identifiers, and a list of users who belong to them.

```
sofipxs@ubuntu:~$ getent group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,sofipxs
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
sssd:x:129:
scanner:x:130:saned
saned:x:131:
colord:x:132:
geoclue:x:133:
pulse:x:134:
pulse-access:x:135:
gdm:x:136:
sambashare:x:137:
super_admins:x:1001:
noob_users:x:1002:
good_students:x:1003:
sofipxs@ubuntu:~$
```

- **видаліть створені Вами групи користувачів;

  To delete groups use the *sudo groupdel* command:

```
sofipxs@ubuntu:~$ sudo groupdel super_admins && sudo groupdel noob_users && sudo groupdel good_students
[sudo] password for sofipxs:
sofipxs@ubuntu:~$
```

- **перегляньте інформацію про існуючі групи користувачів.

```
sofipxs@ubuntu:~$ getent group super_admins && getent group noob_users && getent group good_students
sofipxs@ubuntu:~$ getent group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,sofipxs
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
colord:x:132:
geoclue:x:133:
pulse:x:134:
pulse-access:x:135:
gdm:x:136:
sambashare:x:137:
sofipxs@ubuntu:~$
```

Відповіді на контрольні запитання:

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

Passwords in configuration files are not stored explicitly for security reasons. If a password is stored explicitly, anyone who has access to the file can read the password. This could lead to unauthorised access. Therefore, passwords are usually stored as hashes. A hash function converts a password into a unique set of fixed-length characters. This process is one-way, meaning that the original password cannot be recovered from the hash. When a user enters his or her password, the system converts it into a hash and compares this hash with the hash stored in the system. If both hashes match, the password is considered correct.

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

Since the root account has full access and control, any mistakes you make can have serious consequences for the system. Forgetting you're logged in as root and running the wrong command could cause data loss or system instability. Most everyday tasks don't require full administrative privileges. Using the root account for simple things like browsing the web or checking email gives those programs unnecessary access to your system, potentially increasing the security risk if they were compromised by malware.

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

   - su: The su (or "switch user") command is used to switch to another user. If you use su without arguments, you will switch to the root user. To do this, you need to enter the password of the user you want to switch to.
   - sudo: The sudo (or "superuser do") command allows you to run commands as root without changing your current user. You execute the command as root by entering your own password, not the root password.

The main difference between the two is that su requires the password of the target account, while sudo requires the password of the current user. Therefore, it is much safer to use sudo since it doesn’t include exchanging sensitive information.

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

The root user's home directory is usually placed in /root, not /home, for security reasons. If the system is experiencing problems and /home cannot be mounted, the root user should be able to log in and fix the problem. This is possible if his home directory is in the root directory /.

5. *Для чого використовується команда getent?

The *getent* command is used to retrieve information from various system databases, such as /etc/passwd, /etc/group, and others. It allows you to access information about users, groups, hosts, and other system data.

- get information about the user user1: *getent passwd user1*;
- list all groups in the system: *getent group*.

6. *Як можна змінити пароль користувача?

The user's password can be changed using the *passwd* command. Simply enter this command and follow the on-screen instructions to change the password. This command takes as an argument the name of the user whose password you want to change. For example: *passwd user1*.

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

The *groupdel* command can be used to delete a group. Files in the deleted group will become orphaned. Only supplementary groups can be deleted. When a group is deleted, information about it usually disappears from the system. However, sometimes a trace of the group may remain in certain configuration or log files. For example, if a group has been granted access rights to certain files or directories, its GID might remain in these file attributes. However, in most cases, once a group is deleted, its information is no longer available to the system.

8. **Яке призначення команди chage?

The chage command is used to view and change the user password expiry information. This command is used when the login is to be provided for a user for a limited amount of time or when it is necessary to change the login password from time to time. With the help of this command, we can view the ageing information of an account, the date when the password was previously changed, set the password changing time, lock an account after a certain amount of time etc. A good example of the *chage* command would be to change the maximum number of days that an individual's password is valid to be 60 days*: chage -M 60 jane*

9. **Які параметри команди usermod ви вважаєте найбільш використовуваними?

The most commonly used parameters of the usermod command include:

- -a, --append - add the user to one or more additional groups. The option will only work in conjunction with the -G option.
- -G, --groups - specify a list of additional groups to which the user should belong. The groups are separated by a comma. If a user enters an additional group that

was not specified in the list, the user will be removed from it. But if you use the -a option, you can add new additional groups without deleting the old ones.

- -d, --home - specify the new location of the user's home directory. If the -m option is used, the contents of the current home directory will be moved to the new location.
- -l, --login - change the user's username to the new one. This option does not affect any other data. This means that the name of the home directory and mail will have to be changed manually to match the new user name.
- -L, --lock - lock user password. This option places the symbol ! (exclamation mark) in front of the password in encrypted form, disabling it.

Висновки:

In the course of the laboratory work, I studied the main aspects of system and user security in the Linux environment. The concept of User Private Group (UPG), which allows you to automatically create private groups for new users, simplifying access control to files and resources, was studied in more detail. I gained practical skills in working with teams to create and manage user groups, and learnt the process of creating new groups, assigning identifiers to them, and adding users to these groups.