**"КИЇВСЬКИЙ ФАХОВИЙ КОЛЕДЖ ЗВ’ЯЗКУ"**

**Лабораторна робота 9**

з дисципліни «Операційні системи»

**Тема:**  
“Захист системи та користувачів у Linux. Створення користувачів та груп”

Виконали: студенти **3** курсу,

групи **КСМ-13А**

**Засенко Олександр**

(прізвище та ініціали)

**Дзюбенко Дмитро**

(прізвище та ініціали)

**Сторожук Костянтин**

(прізвище та ініціали)

Київ  2023

**ЗМІСТ**

Мета роботи…………………………………………………………………….…3

Хід роботи…………………………………………………………………………5

Контрольні запитання……………………………………………………………12

Conclusions……………………………………………………………………..…14

**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

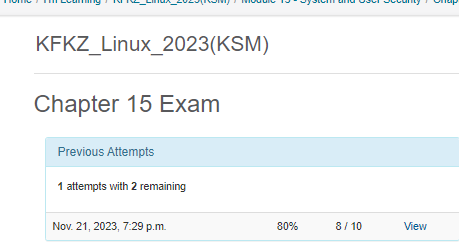
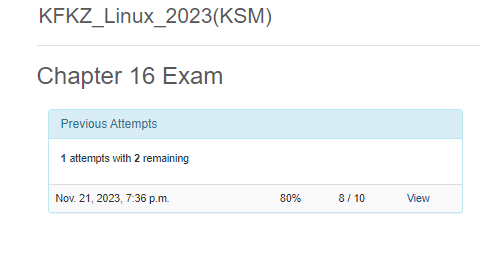
**Завдання для попередньої підготовки**

***Готував матеріал студент Zasenko***

Невеликий словник базових англійських термінів з питань призначення команд та їх параметрів.

|  |  |
| --- | --- |
| User Accounts | There are several text files in the /etc directory that contain the account data of the users and groups defined on  the system. For example, to see if a specific user account has been defined on the system, then the place to check is the  /etc/passwd file. |
| System Accounts | Users log into the system using regular user accounts. Typically, these accounts have UID values of greater  than 500 (on some systems 1,000). The root user has special access to the system. This access is provided to the  account with a UID of 0. |
| Group Accounts | Your level of access to a system is not determined solely by your user account. Each user can be a member of  one or more groups, which can also affect the level of access to the system. |
| Administrative Accounts | There are many different ways to execute a command that requires administrative or root privileges. Logging  in to the system as the root user allows you to execute commands as the administrator. This access is potentially  dangerous because you may forget that you are logged in as root and might run a command that could cause problems  on the system. As a result, it is not recommended to log in as the root user directly. |

**Пройдіть тестування у курсі NDG Linux Essentials за такими темами:**



4.1. UPG (User Profile Generator): UPG - is a tool or system designed to automate the creation and management of user profiles in information systems. It is typically used in areas where you need to quickly create many users with different access rights or characteristics. UPG can provide effective user management, security policy, and facilitate audit and monitoring processes.4.2. Створення груп користувачів:

1) Add a new group: **groupadd group\_name**

2. Add a user to the group: **usermod -aG groupname username**

4.3. Change user group settings:

1. Change the name of the group: **groupmod -n new\_group\_name old\_name**

2. Change the group identifier (GID): **groupmod -g new\_GID old\_group\_name**

**Хід роботи**

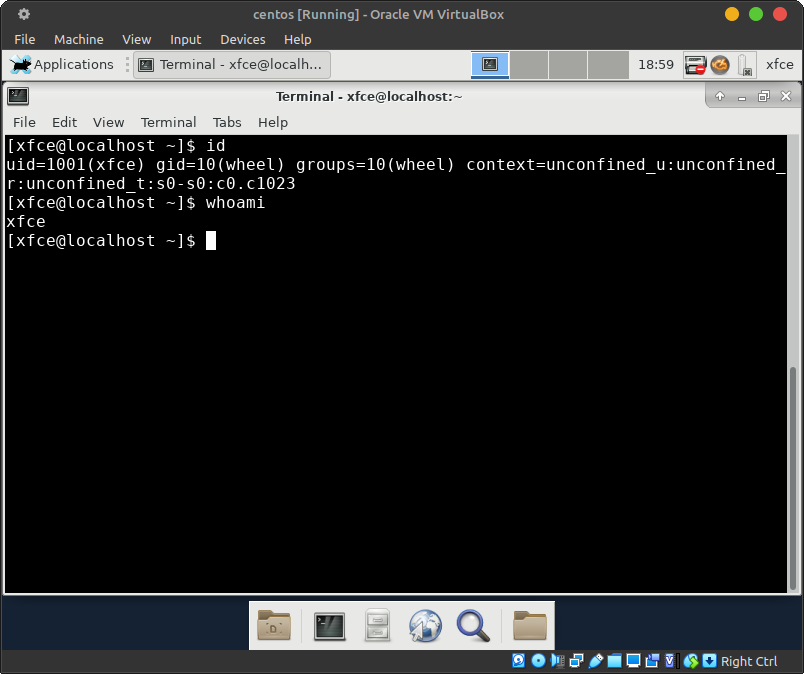
***Готував матеріал студент Dziubenko***

1. .

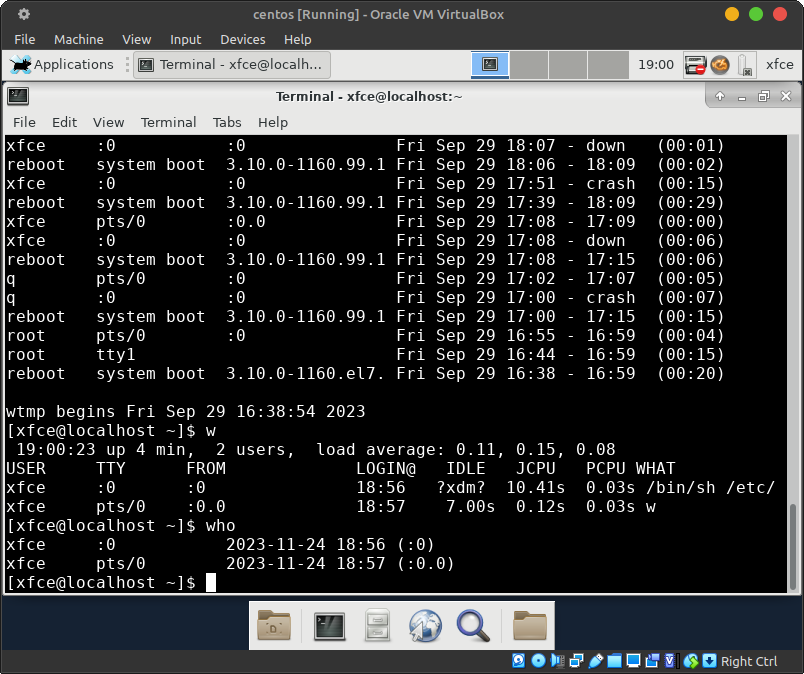
|  |  |
| --- | --- |
| Team name | Its purpose and functionality |
| su | Changing a user |
| id | Display information about a user or group |
| exit | Log out of the current session |
| head | Display the first lines of a file |
| grep | Search for text in a file or data stream |
| ls | View the contents of the current directory |
| getent | Displaying info. from the system database |
| man | Displaying help information by command |
| who | Displaying information about remote users |
| w | Displaying information about active users |
| groupadd | Adding groups |
| groupmod | Changing groups |
| groupdel | Deleting groups |
| useradd | Add a user |
| nano | Open a text editor |
| passwd | Change a user's password |

3.

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

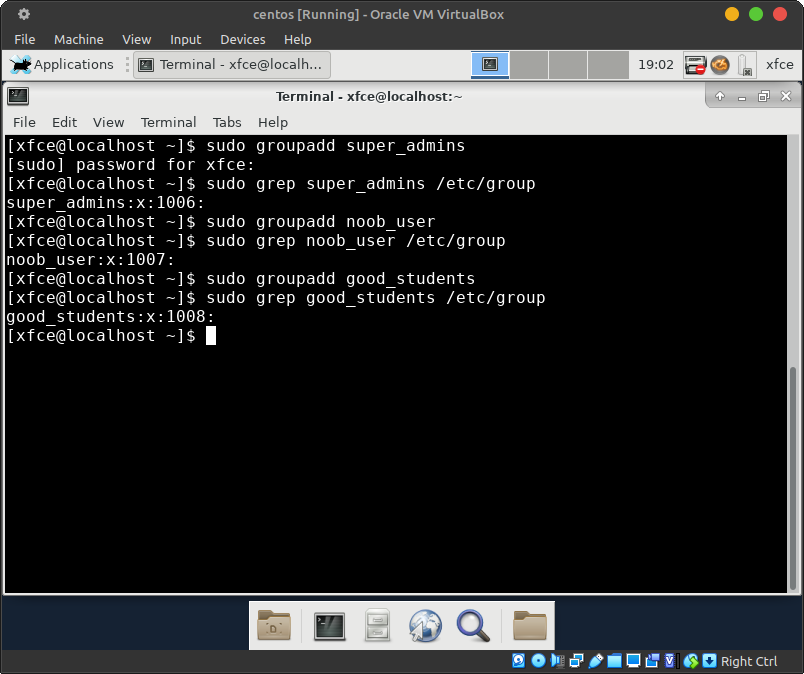


1. попрактикуйте в терміналі команди last, w та who. Порівняйте результати виводу кожної команди, які деталі відсутні в кожній із команд порівняно з іншими?

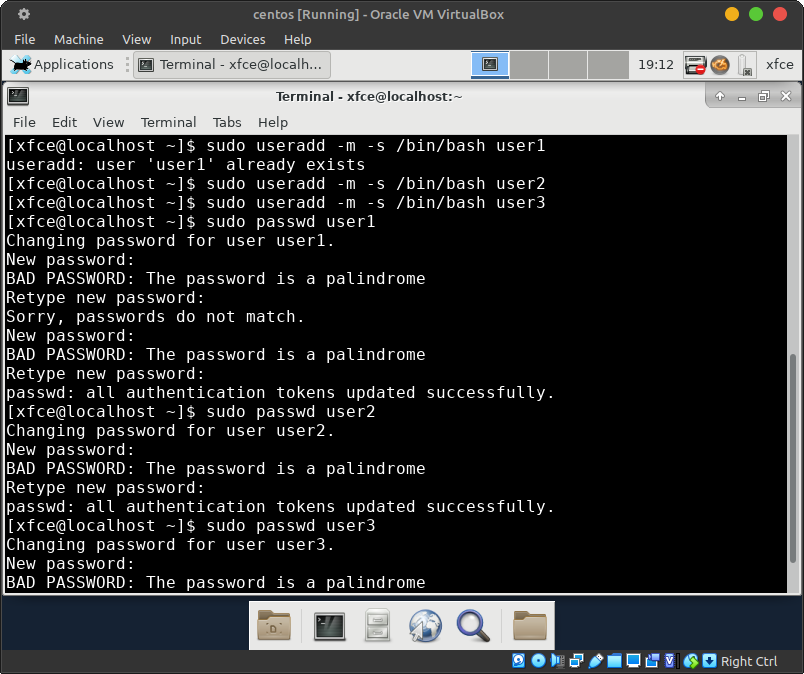


The difference between them is mainly that last displays the history of logins and logouts, w provides more details about current users, and who gives a shorter view. Each of these commands serves a different purpose and can be used depending on the context.

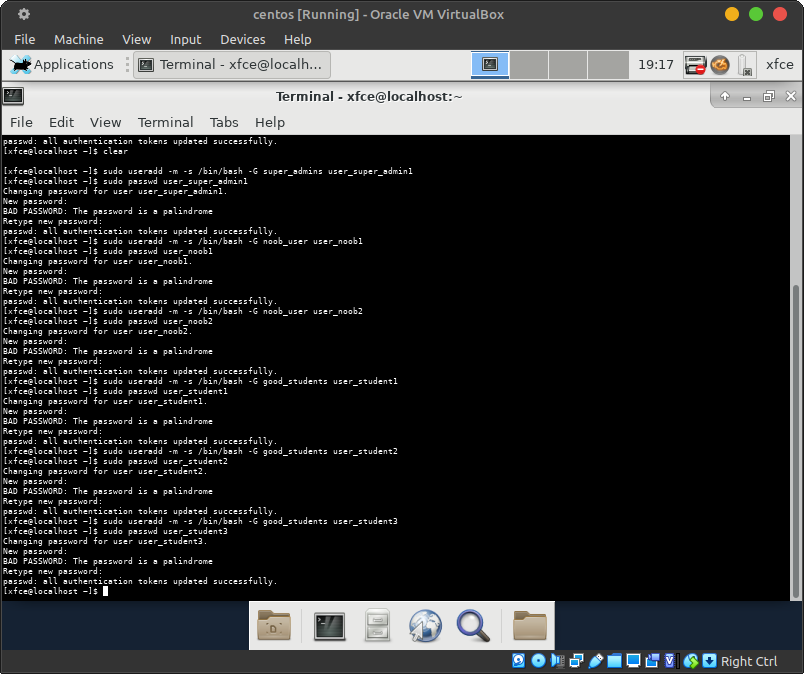
1. створіть дві нові групи користувачів - super\_admins, noob\_users та good\_students, визначте їх ідентифікатори;



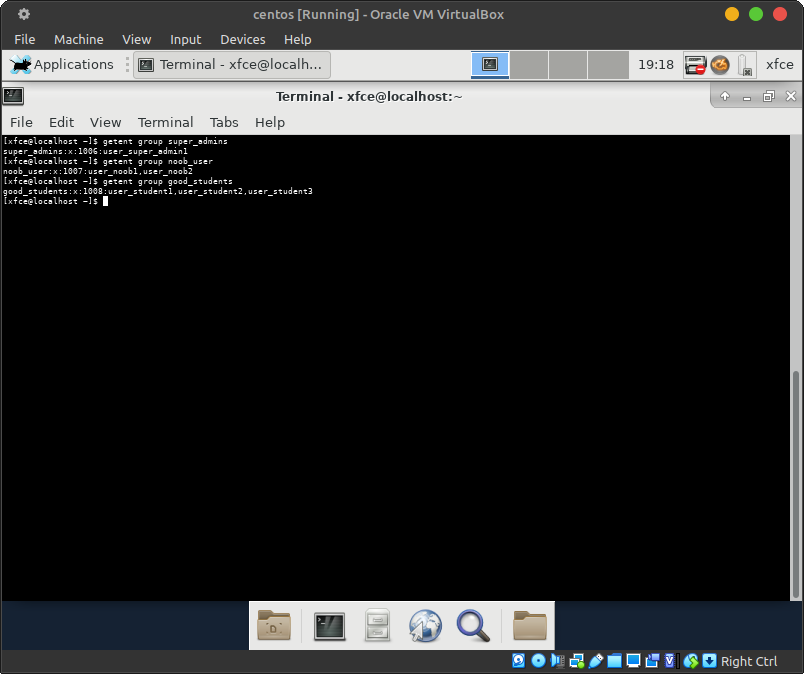
1. для кожного члену Вашої команди за допомогою терміналу створіть нового користувача (якщо працюєте самі, то просто трьох довільних користувачів), не забудьте після створення нового користувача одразу задати йому пароль;



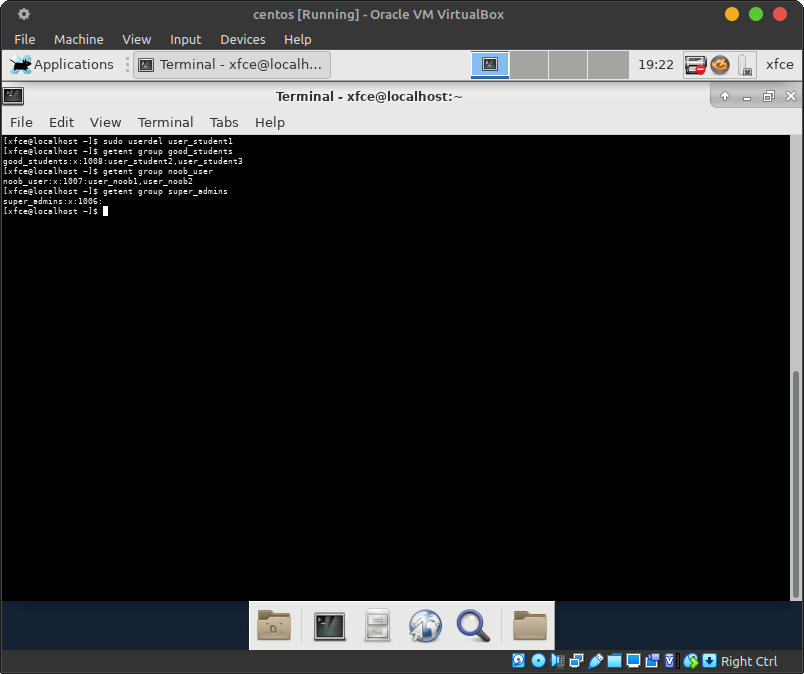
1. додайте нових користувачів у створені Вами нові групи таким чином, щоб у групах super\_admins та noob\_users було по 2 користувачі, один з яких є в обох групах, у групу good\_students додайте всіх трьох користувачів;



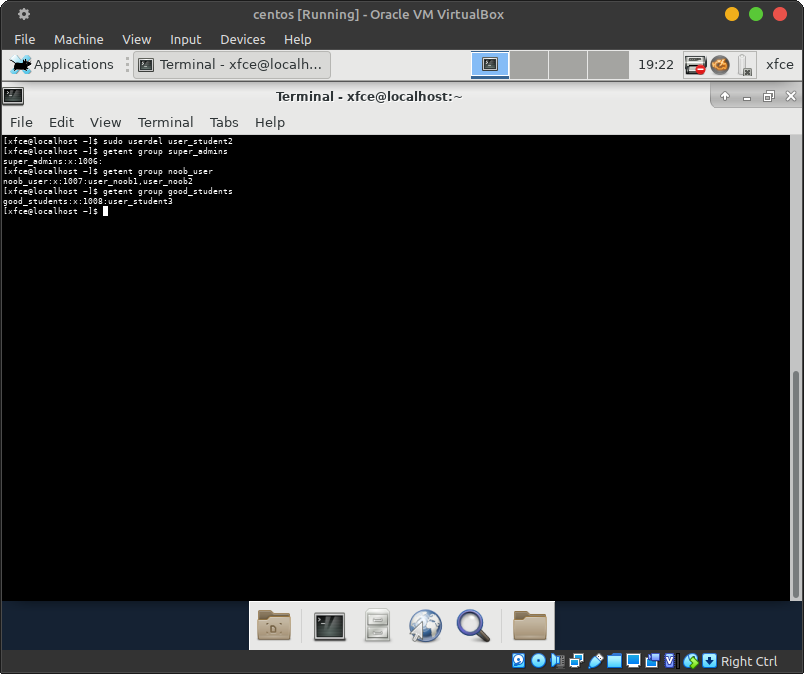
1. перегляньте інформацію про групи, та які користувачі до них входять, поясніть що ви бачите;



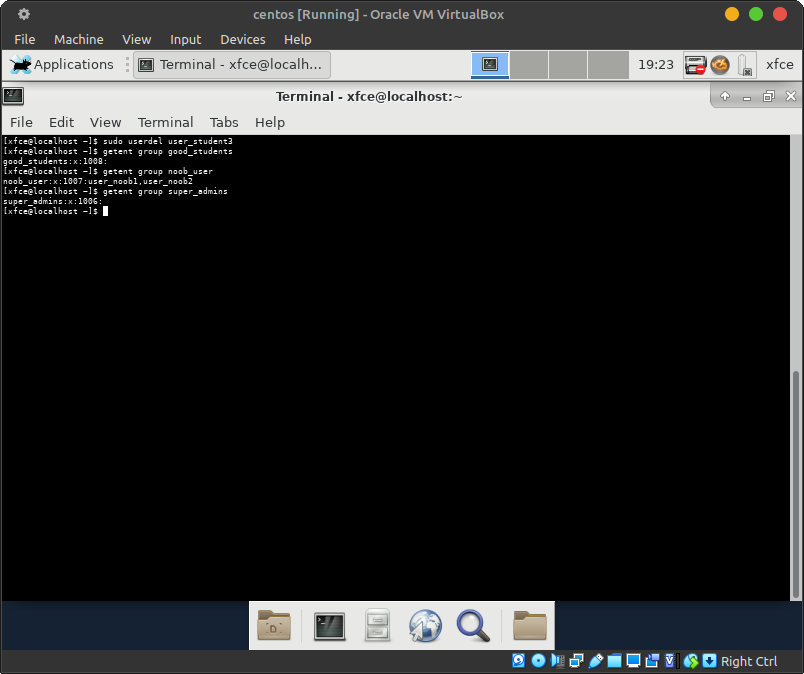
1. видаліть першого створеного вами користувача, перегляньте чи залишиться інформація про нього в групах, де він перебував;



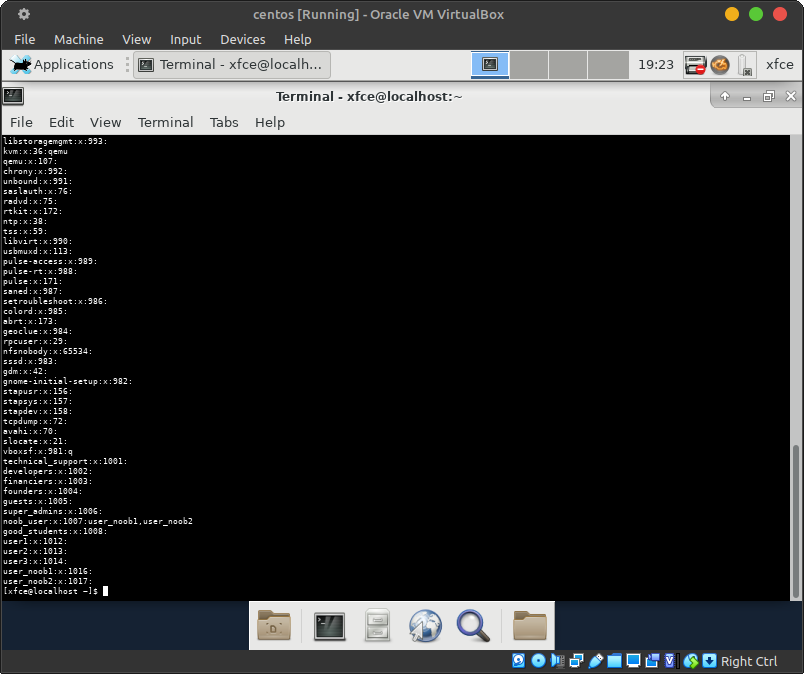
1. видаліть другого користувача, перегляньте чи залишиться інформація про нього в групах, де він перебував;



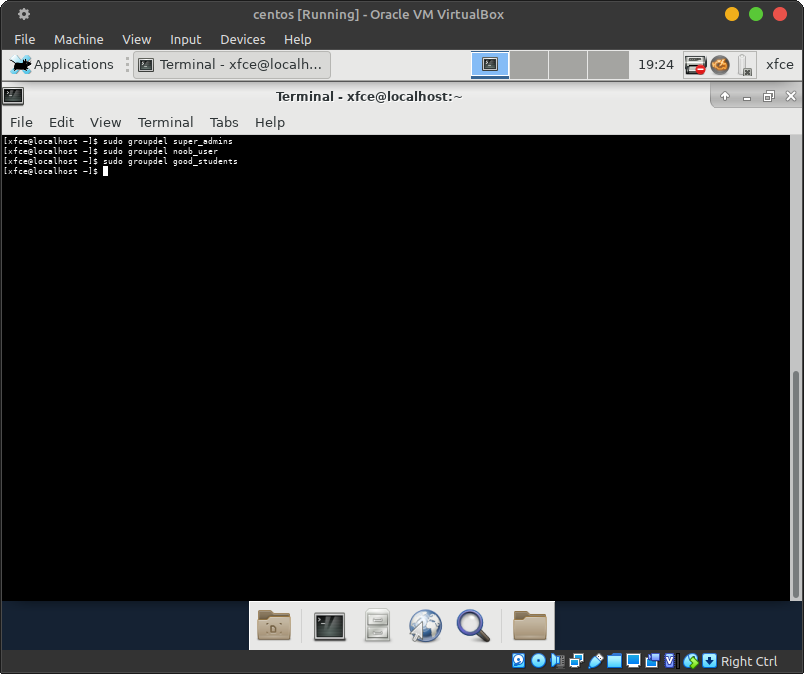
1. видаліть третього користувача, перегляньте чи залишиться інформація про нього в групах, де він перебував;



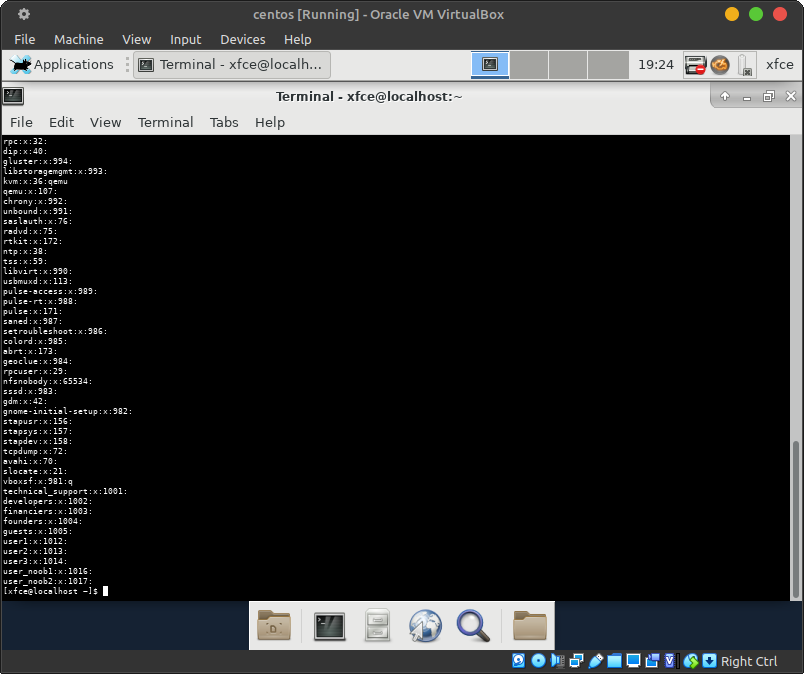
1. перегляньте інформацію про існуючі групи користувачів;



1. видаліть створені Вами групи користувачів;



1. перегляньте інформацію про існуючі групи користувачів.



**Контрольні запитання**

***The material was prepared by student Storozhuk***

1. Passwords are not explicitly stored in configuration files for several reasons:

* Security. If the password is stored explicitly, it can be easily read by anyone who has access to the configuration file. This can lead to a compromise of system or network security.
* Convenience. Creating and using passwords in configuration files explicitly can be cumbersome and inefficient. Users need to memorize or store passwords in a safe place.
* Changing passwords. If the password needs to be changed, you need to make changes to the configuration file. This can be difficult and dangerous if the password is long or complex.

1. It is not recommended to perform day-to-day operations using the root account for several reasons:

* Security: The root account has full control over the system, including the ability to change system configuration, install software, and create new users. If the root account is compromised, the attacker will have full control of the system.
* Convenience: The root account has unlimited access to all files and directories on the system. This can make it difficult to keep track of what changes have been made to the system and can lead to errors or unintended consequences.
* Efficiency: Root accounts usually have a limited lifespan. This means that you will need to log out of the root account and log in to your regular user account to complete any tasks that do not require full root access. This can be cumbersome and inefficient.

1. The su and sudo commands are used to gain special privileges on Unix-like systems. However, there are some key differences between them.

The su command, which means "substitute user," allows a user to switch to another user account, including the root account. When a user runs su, they are asked to enter the password of the account they want to switch to. After entering the correct password, they will have full access to the account they have switched to.

The sudo command, which means "super user do," allows a user to execute a single command with the privileges of another user, including the root account. When a user runs sudo, they are asked to enter their own password. If the user's password is correct, they will be able to execute the specified command with the privileges of the specified user.

1. The root user's home directory is not placed in the /home directory because the root account is the most powerful user account on a Unix-like system. Using the /root home directory for the root account helps protect the system from unintentional or malicious actions.

If the root user's home directory were placed in the /home directory, users with lesser privileges could easily access files and directories contained in the root home directory. This could lead to a compromise of system security, as the root account has access to all files and directories on the system.

1. The getent command can be used to obtain information about the following databases:

* passwd: The user database.
* group: Group database.
* services: The services database.
* networks: Networks database.
* protocols: The protocols database.
* rpc: The RPC database.
* aliases: Database of email aliases.
* netgroup: Database of network groups.

1. To delete an existing user group, you can use the groupdel command. This command takes as an argument the name of the group you want to delete. For example, to delete the users group, you can run the command **groupdel users**

This command will delete the users group record from the system group database. However, information about the group may remain in other places on the system, such as in application configuration files or in user home directory files.

1. To change a user's password, you can use the passwd command. This command takes as an argument the name of the user whose password you want to change. For example **passwd user**.
2. The chage command is used to change user password information in the system. This information includes:

* The date the password was last changed.
* The number of days left before the password expires.
* The date when the password should be changed.
* The date when the user account will be locked if the password is not changed.

1. The most commonly used parameters of the usermod command are:

* -c - sets the full user name.
* -g - sets the default user group.
* -d - sets the user's home directory.
* -m - creates the user's home directory if it does not exist.

**Conclusions**

***The material was prepared by student Storozhuk***

In this lab, we learned the basic steps for creating new users and user groups, as well as new information about administrator rights, and performed several tasks in practice. No problems were encountered during the task.