“Київський фаховий коледж зв’язку”

Циклова комісія комп’ютерної та програмної інженерії

**ЗВІТ ПО ВИКОНАННЮ**

**ЛАБОРАТОРНОЇ РОБОТИ №9**  
з дисципліни: «Операційні системи»  
Тема: “Захист системи та користувачів у Linux. Створення користувачів та груп”

Виконали студенти

групи БІКС-13

Команда JRSY: Андрущик П.С   
Бурбан Д.Ю.  
Перевірив викладач

Сушанова В.С.

Київ 2024

**The goal of the work: (робила студентка Андрущик Поліна)**1. Getting hands-on skills with the Bash shell.  
2. Getting to know the basic actions when creating new users and new user groups.  
  
**1. \*Read the short theoretical information for the laboratory work and make a small dictionary of basic English terms for the assignment of commands and their parameters.**

|  |  |
| --- | --- |
| **Term in English** | **Term in Ukrainian** |
| Root User | Обліковий запис суперкористувача в системах Nyh/Linux з повними правами адміністратора. |
| Administrative Privileges | Дозволи, що дозволяють користувачам виконувати команди з підвищеними привілеями. |
| Graphical Environment | Інтерфейс користувача, який включає графічні елементи, такі як вікна, значки, кнопки тощо. |
| Unprivileged User | Додаткові групи, до яких може належати користувач, визначені у файлі /etc/group. |
| Groupmod | Команда для зміни властивостей групи, таких як ім’я або GID (ідентифікатор групи). |

**2. On the basis of the considered material, answer the following questions:  
Explain the concept of UPG, when it is appropriate to use them?**User Private Groups (UPGs) are groups automatically created for each user on some Unix/Linux systems, typically having the same name as the user. They are useful in scenarios where multiple users need to collaborate on shared files or projects while maintaining individual file access permissions. UPGs simplify file sharing and access management by ensuring that each user has a dedicated group, allowing administrators to grant group-level permissions without affecting other users. This enhances security and facilitates efficient collaboration among users on the system.

**\*What commands can be used to create user groups? Enter examples**You can use the groupadd command to create user groups. For example, to create a group with the name "developers", the command sudo groupadd developers is used. You can also specify a group ID if needed with the -g option. For example, sudo groupadd -g 1001 developers.

**\*\*What commands can be used to change user group settings? Enter examples**To change the settings of user groups, you can use the groupadd command to create a new group and the groupmod command to change the parameters of an existing group. For example, groupadd developers will create a new group named "developers", and groupmod -n newname oldname will change the group name from "oldname" to "newname".

2. Work through all the command examples presented in the labs of the NDG Linux Essentials course - Lab 15: System and User Security and Lab 16: Creating Users and Groups. Create a table to describe these commands(робив студент Бурбан Данило)

| **Command** | **Purpose and Functionality** |
| --- | --- |
| **su** | **command is used to switch users. By default, it switches the user to root**  **(or another specified user), if not otherwise specified.** |
| **sudo** | **allows users to execute commands with the privileges of another user, typically root.** |
| **id** | **command displays information about user and group identifiers, including the real and effective user**  **identifier (UID) as well as a list of groups to which the user belongs.** |
| **head** | **is designed to output the first few lines of a file or standard input.** |
| **getent** | **command allows retrieving information about users, groups, hosts, and other configuration data**  **from system files.** |
| **last** | **shows a list of recent logins to the system.** |
| **w** | **displays who is logged into the system and their activities.** |
| **groupadd** | **command is used to create a new user group.** |
| **groupdel** | **is used to delete an existing user group.** |
| **useradd** | **command allows administrators to create new users on the system.** |
| **chage** | **is used to change password expiration parameters for a user.** |
| **userdel** | **command removes a user from the system, deleting their entry from the user and group files.** |

3. Perform the following practical tasks in the terminal following actions (show screenshots):

display information about the current user in various ways (hint, use the id and grep commands);

\*practice the last, w, and who commands in the terminal. Compare the output of each command, what details are missing from each command compared to the others?

\*create two new user groups - super\_admins, noob\_users and good\_students, define their identifiers;

\*for each member of your team, use the terminal to create a new user (if you work alone, just three arbitrary users), do not forget to immediately set a password for the new user after creating it;

\*\*add new users to the new groups you created so that there are 2 users in the super\_admins and noob\_users groups, one of which is in both groups, add all three users to the good\_students group;

\*\*view information about groups and which users belong to them, explain what you see;

\*\*delete the first user you created, see if information about him remains in the groups where he was;

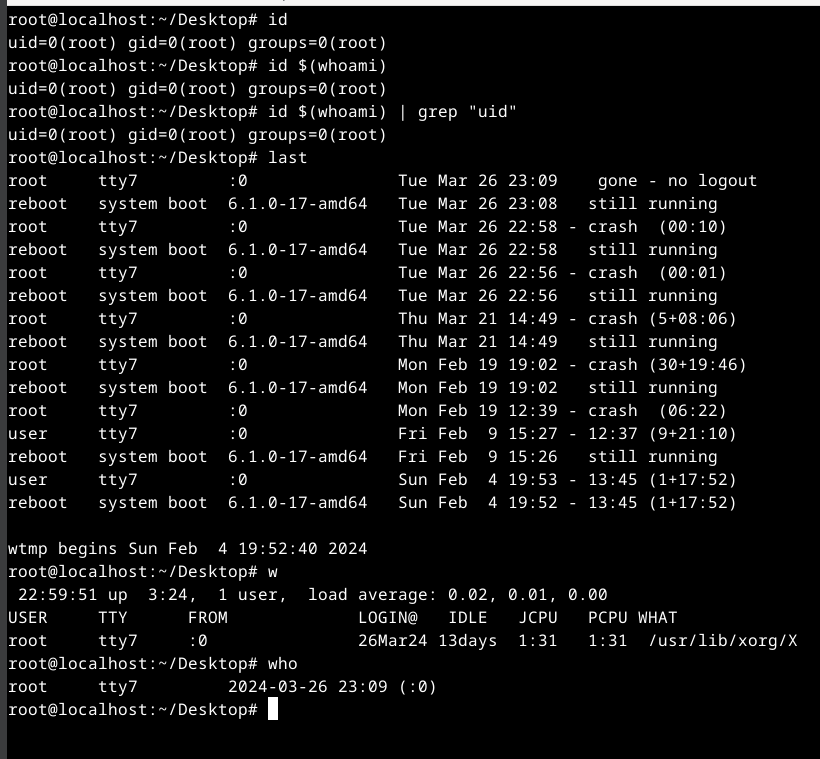
\*\*delete the second user, see if information about him remains in the groups where he was;

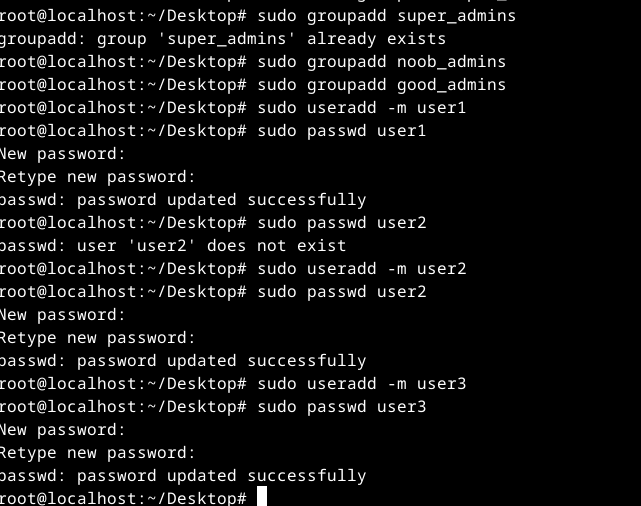
\*\*delete the third user, check whether information about him remains in the groups where he was;

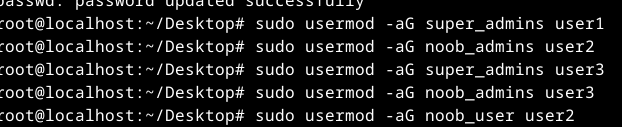
\*\*view information about existing user groups;

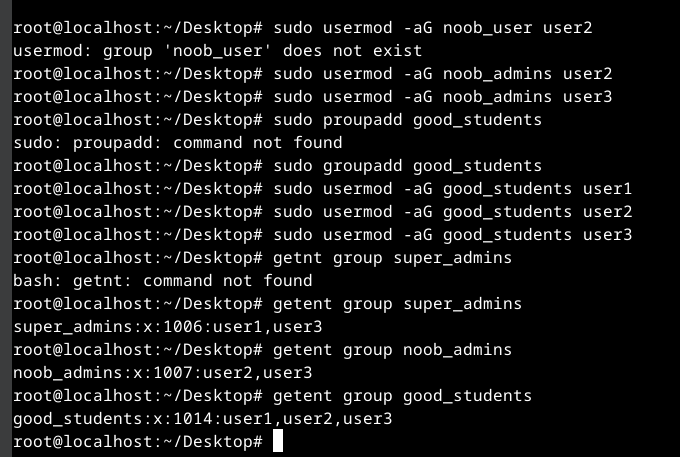
\*\*delete user groups created by you;

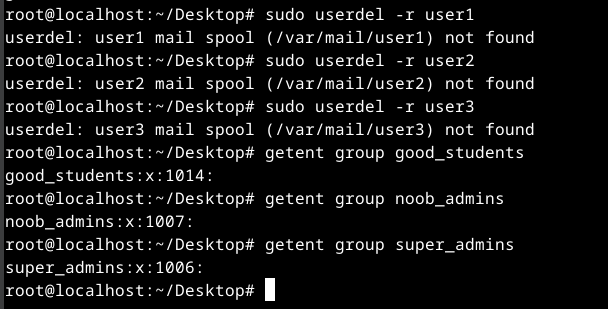
\*\*view information about existing user groups.



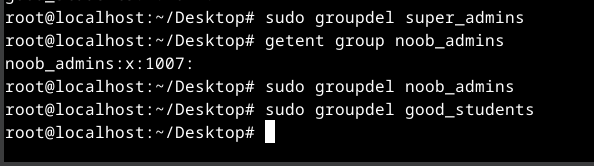














**Answers to control questions: (робив студент Бурбан Данило)  
1. Why is the password not stored explicitly in the configuration files?**Passwords are not explicitly stored in configuration files for security purposes. If passwords were stored in clear text, anyone with access to these files could easily gain access to critical system resources. Instead, password hashes are usually stored, which are an encrypted version of the password that cannot be read directly. This approach provides an additional level of security, because even in case of access to the configuration file, an attacker will not be able to simply look at the password in its open form.

**2. Why is it not recommended to perform daily operations using the root account?**It is not recommended to perform day-to-day operations using the root account, as this may lead to a major security risk. While running the system as root, the user can recklessly execute a command that can cause serious problems or even damage the system. Also, by remaining logged in as root, the user runs the risk of accidentally running dangerous programs, such as browsers or mail clients, which may have full access to the system. Therefore, it is better to use a regular user account for day-to-day tasks and use the root account only for necessary administrative tasks.

**3. \*What is the difference between the mechanisms for obtaining su and sudo special privileges?**The main difference between su and sudo special privilege mechanisms is the way they are used. The su command allows the user to switch to another account, usually root, provided the password for that account is entered. While sudo provides the ability to execute commands with administrative privileges, but with the user's own password that has the right to execute those commands. Thus, sudo provides a more flexible and secure privilege management mechanism, allowing fine-grained control over access to administrative commands.

**4. \*Why is the home directory of the root user not located in the /home directory?**The home directory of the root user is not located in the /home directory for security and isolation reasons. Because root has full access to the entire system and can execute any commands, its home directory is usually placed in a separate directory such as /root to avoid accidental deletion or modification of root user data and to maximize system security.

**5. \*What is the getent command used for?**The getent command is used to retrieve information about users, groups, and other records from various databases such as /etc/passwd, /etc/group, and, depending on the system configuration, from network authentication services such as LDAP or NIS . This command allows you to view information about users and groups that may not be available through direct access to the /etc/passwd and /etc/group files, and to use information found in network databases.

**6. \*How can you change a user's password?**To change a user's password in Unix/Linux systems, you can use the passwd command, which allows you to change the password of the current user or specify the name of the user whose password you want to change. Just enter the command passwd, or passwd username, where username is the name of the user whose password you want to change, and follow the instructions that appear on the screen to enter a new password.

**7. \*\*How can existing user groups be deleted? Will information about them remain somewhere in the system?**Existing user groups can be deleted using the groupdel command in a Unix/Linux environment. After you delete a group, the information about it will still remain in the system, but it will be removed from the /etc/group file, which contains information about user groups.

**8. \*\*What is the purpose of the chage command?**The chage command is used to change user password expiration settings on a Unix/Linux system. This command allows administrators to configure password expiration dates, including last modified date, maximum and minimum expiration dates, and expiration notifications. Such settings help increase system security by changing passwords at regular intervals and controlling their use.

**9. \*\*Which options of the usermod command do you think are the most used?**The most used options of the usermod command include -a (add user to additional groups), -G (change user's primary and secondary groups), -l (change user name), -p (set user password), -u (change user ID user) and -e (set user account expiration date).  
  
**Conclusion:**During the laboratory work, we studied in detail the issues of system and user protection in the Linux environment, as well as the process of creating users and groups. Explored various aspects of account administration, such as using administrative privileges, managing groups, and configuring access rights. Learned the basic commands for creating, changing and deleting users and groups, as well as the parameters of these commands. Understand the importance of using administrative accounts with caution and restricting root access to ensure system security.