“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 КСМ-23А

Команда КГК:

Корольов Є.Ю.,

Горохов Д.С. та

Коваленко С.О.

Перевірила викладач

Сушанова В.С.

Київ 2024

**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:**

***Готував матеріал студент Корольов Є. та Коваленко С.***

1. \*Прочитайте короткі теоретичні відомості до лабораторної роботи та зробіть невеликий словник базових англійських термінів з питань призначення команд та їх параметрів.

|  |  |
| --- | --- |
| Термін | Опис та Команди |
| User | Користувач системи. Команда: useradd, usermod, userdel |
| Group | Група користувачів. Команда: groupadd, groupmod, groupdel |
| Password | Пароль користувача. Команда: passwd username |
| Home Directory | Домашній каталог. Параметр: -d /path/to/dir |
| Shell | Оболонка користувача. Параметр: -s /bin/bash |
| Sudo | Права адміністратора. Команда: sudo |
| Permissions | Дозволи (читання/запис/виконання). Команда: chmod, chown |
| Ownership | Власність файлів. Команда: chown user:group file |
| Authentication | Аутентифікація. Файли: /etc/passwd, /etc/shadow |
| Lock | Блокування користувача. Команда: usermod -L username |
| Unlock | Розблокування користувача. Команда: usermod -U username |
| Add to Group | Додавання до групи. Команда: usermod -aG group username |
| Delete User | Видалення користувача. Команда: userdel -r username |
| Delete Group | Видалення групи. Команда: groupdel groupname |

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

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

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

* Chapter 15 Exam
* Chapter 16 Exam

***Завдання виконувала Коваленко С.***

1. На базі розглянутого матеріалу дайте відповіді на наступні питання:
   1. Розкрийте поняття UPG, коли їх доцільно використовувати?

During the installation process, most installers create a normal user and either give this user the permission to execute administrative commands with sudo or require the root user account password be configured as part of the installation process. Most Linux systems are configured to allow for one unprivileged (non-root) user to log in, as well as have the ability to effectively execute commands as the root user, either directly or indirectly.

If the computer is to be used by only one person, then having only one regular user account might be sufficient. However, if a computer needs to be shared by multiple people, then it is desirable to have a separate account for each person who uses it. There are several advantages to individuals having their own separate accounts:

Accounts can be used to grant selective access to files or services. For example, the user of each account has a separate home directory that is generally not accessible to the other users.

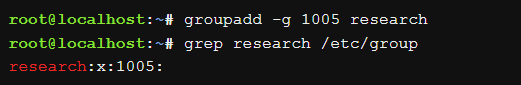
The sudo command can be configured to grant the ability to execute select administrative commands. If users are required to use the sudo command to perform administrative commands, then the system logs when users perform these commands.

Each account can have group memberships and rights associated with it allowing for greater management flexibility.

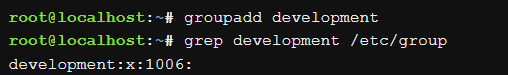
On some distributions, creating a new user account also automatically creates a group account for the user, called a User Private Group (UPG). On these systems, the group and username would be the same, and the only member of this new group would be the new user.

* 1. \*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.



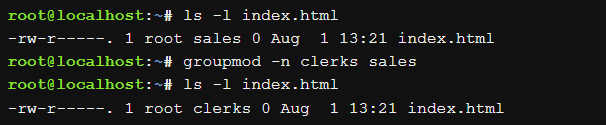
If the -g option is not provided, the groupadd command will automatically provide a GID for the new group. To accomplish this, the groupadd command looks at the /etc/group file and uses a number that is one value higher than the current highest GID number. The execution of the following commands illustrates this:



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

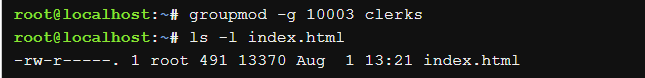
The groupmod command can be used to either change the name of a group with the -n option or change the GID for the group with the -g option.

Changing the name of the group may confuse users who were familiar with the old name and haven't been informed of the new name. However, changing the group name won't cause any problems with accessing files, since the files are owned by GIDs, not group names.



After the previous groupmod command, the index.html file has a different group owner name. However, all users who were in the sales group are now in the clerks group, so all of those users can still access the index.html file. Again, this is because the system defines the group by the GID, not the group name.

On the other hand, if you change the GID for a group, then all files that were associated with that group will no longer be associated with that group. In fact, all files that were associated with that group will no longer be associated with any group name. Instead, these files will be owned by a GID only, as shown below:



If you decide to delete a group with the groupdel command, be aware that any files that are owned by that group will become orphaned.



1. Підготувати в електронному вигляді початковий варіант звіту:

* Титульний аркуш, тема та мета роботи
* Словник термінів
* Відповіді на п.4.1 та п.4.5 з завдань для попередньої підготовки

**Хід роботи:**

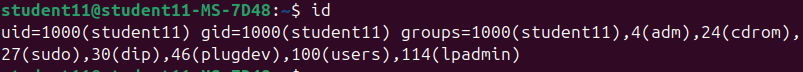
***Готував матеріал студент Корольов Є та Горохов Д(401 ауд.)***

1. Початкова робота в CLI-режимі в Linux ОС сімейства Linux:
2. Запустіть операційну систему Linux Ubuntu. Виконайте вхід в систему та запустіть термінал ***(якщо виконуєте ЛР у 401 ауд.)***.
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 |
| su | The su command allows you to run a shell as a different user. While switching to the root user is what the su command is used for most frequently, it can also switch to other users as well. |
| sudo | The sudo command allows users to execute commands as another user. Similar to the su command, the root user is assumed by default. |
| /etc/shadow | As previously mentioned, the /etc/shadow file contains account information related to the user's password. However, regular users can't view the contents of the /etc/shadow file for security reasons. To view the contents of this file, log in as the administrator (the root account |
| id | The id command is used to print user and group information for a specified user. |
| who | The 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. Through the use of options, this command is also able to display information such as the current *runlevel* (a functional state of the computer) and the time that the system was booted. |
| last | The last command reads the entire login history from the /var/log/wtmp file and displays all logins and reboot records by default. An interesting detail of the reboot records is that it displays the version of the Linux kernel that was booted instead of the login location. The /var/log/wtmp file keeps a log of all users who have logged in and out the system. |
| grep  getent | After creating or modifying a group, you can verify the changes by viewing the group configuration information in the /etc/group file with the grep command. If working with network-based authentication services, then the getent command can show you both local and network-based groups. |
| groupadd | 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 |
| groupmod | 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. |
| groupdel | If you decide to delete a group with the groupdel command, be aware that any files that are owned by that group will become orphaned. |
| passwd | The administrator can use the passwd command to either set the initial password or change the password for the account. For example, if the administrator had created the account jane, then executing passwd jane provides the administrator a prompt to set the password for the jane account. If completed successfully, then the /etc/shadow file will be updated with the user's new password. |

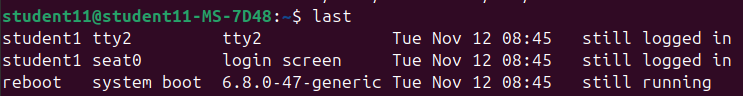
1. Виконайте наступні практичні завдання у терміналі наступні дії (продемонструвати скріншоти):

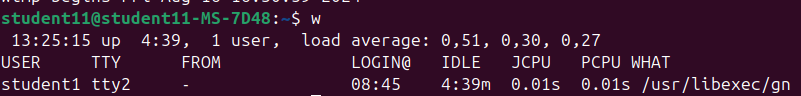
* виведіть інформацію про поточного користувача різними способами (підказка використовуйте команди id та grep);

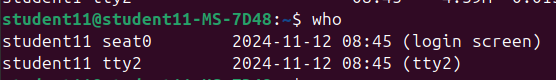




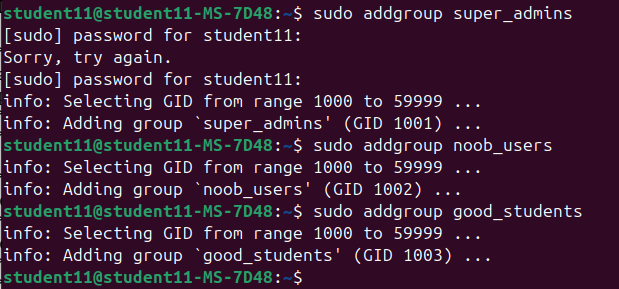
* \*попрактикуйте в терміналі команди last, w та who. Порівняйте результати виводу кожної команди, які деталі відсутні в кожній із команд порівняно з іншими?



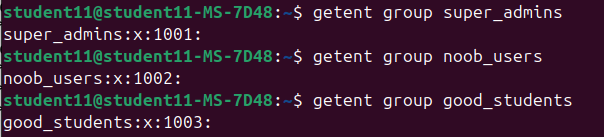




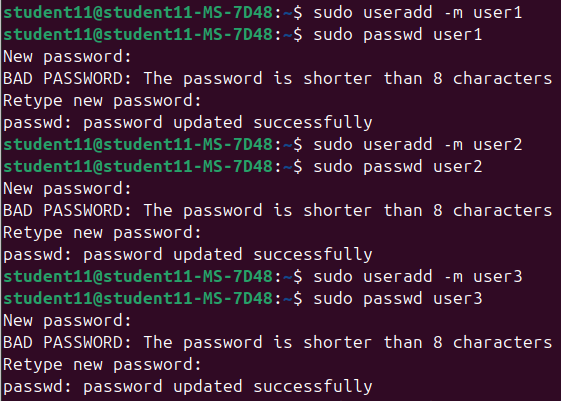
* \*створіть дві нові групи користувачів - super\_admins, noob\_users та good\_students, визначте їх ідентифікатори;

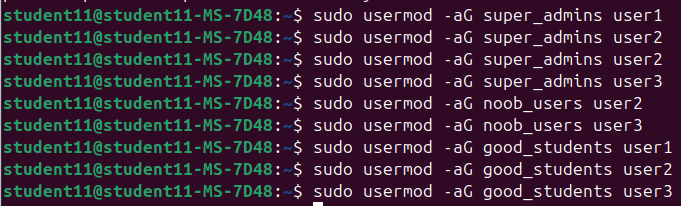


* \*для кожного члену Вашої команди за допомогою терміналу створіть нового користувача (якщо працюєте самі, то просто трьох довільних користувачів), не забудьте після створення нового користувача одразу задати йому пароль;

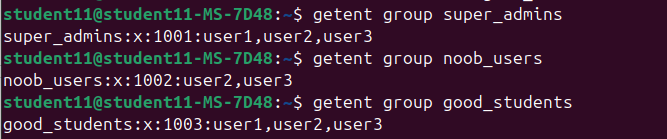


* \*\*додайте нових користувачів у створені Вами нові групи таким чином, щоб у групах super\_admins та noob\_users було по 2 користувачі, один з яких є в обох групах, у групу good\_students додайте всіх трьох користувачів;





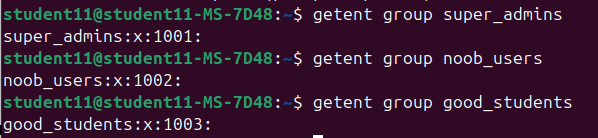
* \*\*перегляньте інформацію про групи, та які користувачі до них входять, поясніть що ви бачите;



Виведена група показує назви груп, їхні індентифікатори та імена користовувачів, які входять до цих груп.

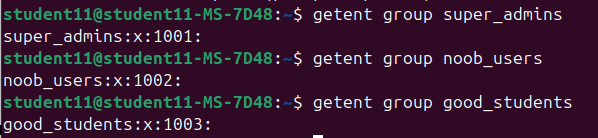
* \*\*видаліть першого створеного вами користувача, перегляньте чи залишиться інформація про нього в групах, де він перебував;





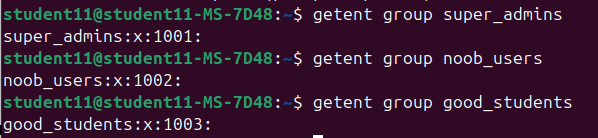
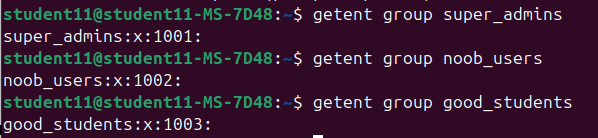
* \*\*видаліть другого користувача, перегляньте чи залишиться інформація про нього в групах, де він перебував;

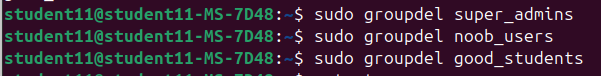




* \*\*видаліть третього користувача, перегляньте чи залишиться інформація про нього в групах, де він перебував;



* 
* \*\*перегляньте інформацію про існуючі групи користувачів;
* 
* \*\*видаліть створені Вами групи користувачів;



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





В терміналі не отримуємо жодної інформації, оскільки подані групи були видалені.

***Завдання виконувала Коваленко С.***

Контрольні запитання:

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

Passwords are not explicitly stored in configuration files for **security** reasons to protect the system and user accounts from unauthorised access. If passwords were stored explicitly, any user who gained access to the configuration file (through an error in the access rights settings or malicious actions) could easily learn the passwords. This creates a high risk of abuse.

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

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.

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

Because using the root account is potentially dangerous, you should only execute commands as root if administrative privileges are needed. If the root account is disabled, as it is on the Ubuntu distribution, then administrative commands can be executed using the sudo command. If the root account is enabled, then a regular user can execute the su command to switch accounts to the root account.

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

[sysadmin:x:1001:1001:System Administrator,,,,:/home/sysadmin:/bin/bash]

This field defines the location of the user's home directory. For regular users, this would typically be /home/username. For example, a username of bob would have a home directory of /home/bob.

The root user usually has a different place for the home directory, the /root directory.

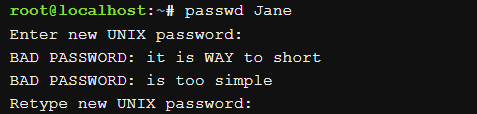
1. \*Для чого використовується команда getent?

In addition to the grep command, another technique for retrieving user information contained in the /etc/passwd and /etc/shadow files is to use the getent command. One advantage of this command is that it can retrieve account information that is defined locally, in files such as /etc/passwd and /etc/shadow, or on a network directory server.



1. \*Як можна змінити пароль користувача?

There are several ways for a user password to be changed. The user can execute the passwd command, the administrator can execute the passwd command providing the username as an argument, or graphical tools are also available.



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

If you decide to delete a group with the groupdel command, be aware that any files that are owned by that group will become orphaned.

Only supplemental groups can be deleted, so if any group that is the primary group for any user, it cannot be deleted. The administrator can modify which group is a user's primary group, so a group that was being used as a primary group can be made into a supplemental group and then can be deleted.

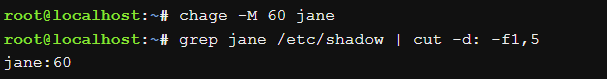
As long as the group to be deleted is not a user's primary group, deleting the group is accomplished by using the groupdel command along with the name of the group:



1. \*\*Яке призначення команди chage?

The chage command provides many options for managing the password aging information found in the /etc/shadow file.

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:



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

The usermod command offers many options for modifying an existing user account. Many of these options are also available with the useradd command at the time the account is created.

1. -g GROUP / --gid GROUP

Sets a new primary group for the user. Used when you want to change the user's primary group.

usermod -g developers alice

2. -g GROUPS / --groups GROUPS

Specifies a list of additional groups to which the user belongs. Used to grant a user additional rights or access through groups.

usermod -G sudo,adm alice

3. -a / --append

Adds a user to additional groups without removing them from other groups. Used in combination with -G to preserve a user's existing groups.

usermod -aG docker alice

4. -L / --lock

Locks the user account. Used to temporarily restrict access to an account.

usermod -L alice

5. -U / --unlock

Unlocks a previously locked account. Used to restore access to a locked account.

usermod -U alice

6. -s SHELL / --shell SHELL

Sets a new login shell for the user. Used to change the shell, for example, to /sbin/nologin to deny login.

usermod -s /bin/bash alice

7. -d HOME\_DIR / --home HOME\_DIR

Changes the user's home directory. Used when you want to move or change the location of the home directory.

usermod -d /new/home alice

Висновок:

The course covered the basic principles of system and user security in Linux, including the creation of new users and groups. The skills of working with the Bash command shell were consolidated, including the use of useradd, passwd, groupadd commands, as well as setting up access rights to system resources.

Learning how to create new users and groups, as well as how to configure them (e.g. change passwords, lock and configure groups) helped to understand how to ensure effective account management and security. This knowledge is important for administering Linux systems.