“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»**

Виконали

студенти

групи БІКС-13

Команда «chipichapa»:

Ємець В.О.,

Лапчик С.С.,

Савустьян М.В.

Перевірив викладач

Сушанова В.С.

Робота студентів групи БІКС-13 Команда «chipichapa»: Ємець В., Лапчик С., Савустьян М.

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:**

***Готувала матеріал студентка Лапчик Софія***

1. \*Прочитайте короткі теоретичні відомості до лабораторної роботи та зробіть невеликий словник базових англійських термінів з питань призначення команд та їх параметрів.  
   sudo – administrative commands can be executed usinf this command.

su – command to switch accounts to the root account.

id – command is used to print user and group information for a specified user.

-g – to print only the user's primary group.

who – displays a list of users who are currently logged into the system, where they are logged in from, and when they logged in.

last – reads the entire login history from the /var/log/wtmp file and displays all logins and reboot records by default.

groupadd – create a new group.

groupmod – make changes to groups.

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

UPG (Universal Password Generator) is a password generator that uses a cryptographically strong algorithm to generate random, complex and unique passwords. It is designed to increase the security of online accounts by making them more resistant to hacking.  
Used to: create passwords for new accounts, replace weak or repetitive passwords, improve overall security.

* 1. \*Якими командами можна створити групи користувачів? Наведіть приклади

groupadd to create a new group.

* 1. \*\*Якими командами можна змінити налаштування груп користувачів? Наведіть приклади  
     groupmod to make changes to groups.  
     The groupdel command can be used to delete either of the groups, as long as neither of them have been made the primary group for a use r.  
     Use the getent command to retrieve information about the new research group.  
     Use the grep command to retrieve information about the new sales group.

**Хід роботи:**

***Готувала матеріал студентка Лапчик Софія***

1. Початкова робота в CLI-режимі в Linux ОС сімейства Linux:
   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.
   2. Запустіть віртуальну машину Ubuntu\_PC ***(якщо виконуєте завдання ЛР через академію netacad)***
   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 |
| sudo | administrative commands can be executed usinf this command |
| su | command to switch accounts to the root account |
| id | command is used to print user and group information for a specified user |
| groupadd | to create a new group |
| groupmod | to make changes to groups |
| useradd | create a new user |
| passwd | set and reset a user's password |
| usermod | make changes to the user account |
| groupdel | used to delete either of the groups, as long as neither of them have been made the primary group for a use r |
| grep | to retrieve information about the new sales group |
| who | displays a list of users who are currently logged into the system, where they are logged in from, and when they logged in |
| last | reads the entire login history from the /var/log/wtmp file and displays all logins and reboot records by default |
| getent | to retrieve information about the new research group |

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;
* \*\*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.

**Контрольні запитання:**

***Готувала матеріал студентка Ємець Валерія***

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

1) Configuration files are often accessible to multiple users on the system. If passwords were stored in plaintext within these files, anyone with access to the configuration could easily retrieve them.

2) Storing passwords in plaintext poses a significant security risk. If an attacker gains access to the configuration files (due to misconfigurations, vulnerabilities, or other reasons), they would immediately have access to sensitive credentials.

3) Modern systems separate user account information (including password hashes) from the public user database.

4) In Linux, passwords are stored in a separate file called `/etc/shadow`. This file is only readable by the system's superuser (root) and contains hashed versions of passwords, making it more secure than storing plaintext passwords in `/etc/passwd`.

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

Using the root account for everyday operations is not recommended due to several important reasons:

1. If an attacker gains access to your system, they can cause significant damage if they have root privileges.
2. If you running `rm -rf /` (which recursively removes everything) as root, the consequences will be catastrophic.
3. \*У чому відмінність механізмів отримання особливих привілеїв su і sudo?

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. Additionally, it is advisable to stick to sudo when performing tasks that require root privileges. By doing so, the current user is only granted privileged for the specified command. On the other hand, su switches to the root user completely, exposing the entire system to potential accidental modification.

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

1) /home is mounted on a different drive)

2) composability

You want to build/diagnose/repair a system using that same system, so it makes sense to keep the next upper layer (multi-user features) independent from the lower layers. Many systems to this day equate recovery with single-user: not a special mode, but a merely a lack of some features built on top of it. And if /home is part of a layer on top of single-user systems, it cannot contain single-user essentials.

3) privacy

You should keep personal data separated from system data. Enforcing this separation even when not also expressed in distributing across different mounts makes sense to simplify safe defaults for common operations: Only multi-user directories require explicit exclusion when doing a system backup - the root users directory being considered system, not personal data here.

1. \*Для чого використовується команда getent?

getent is a Linux command that helps the user to get the entries in a number of important text files called databases. This includes the passwd and the group of databases which stores the user information. Hence getent is a common way to look up in user details on Linux. Since getent uses the same name of service as the system, getent will be going to show all information, including that gained from the network information sources such as LDAP. The databases it usually searches in are: ahosts, ahostsv4, ahostsv6, aliases, ethers (Ethernet addresses), group, gshadow, hosts, netgroup, networks, passwd, protocols, rpc, services, and shadow.

1. \*Як можна змінити пароль користувача?
2. In Ubuntu and other Linux distributions you can change the password of a user account with the passwd command.
3. The user you are logged in as must have sudo privileges to be able to change or reset another user’s passwords. To change the password of another user account, run the passwd command followed by the username.
4. \*\*Яким чином можна видалити існуючі групи користувачів? Чи залишиться інформація про них десь у системі?

To delete existing user groups, follow these steps:

1) Click on the folder associated with the user group you want to delete.

2) Click on Properties.

3) Navigate to the Security tab and click Edit.

4) In the Permissions for <folder name> dialog box, click Add.

5) Enter your user name and then click Check names > Ok.

6) Select your user name and check the Full control checkbox in the Allow column.

7) Click Apply > Ok.

If the folder size is equal to or greater than 10 GB, deleting the folder will remove the data within it. However, if the folder contains less data, remnants may still exist. It’s essential to verify the folder size before deletion.

1. \*\*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.

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

1) The `-a -G` options allow you to add an existing user to a secondary group.

2) The `-g` option lets you change a user's primary group.

3) The `-c` option allows you to add or modify the GECOS (full name) information for a user.

4) Use the `-d` option to change a user's home directory. By default, content isn't moved to the new directory. To move content, add the `-m` option.

5) The `-s` option sets the user's default shell.

**Висновок:** we gained practical skills in working with the Bash command shell and learnt the basic steps in creating new users and new user groups.