“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 КСМ-13а

Команда “Viper”:

Малієнко А. М.,

Мішин А. О.

та Нерощин Д.О.

Перевірив викладач

Сушанова В.С.

Київ 2023

**Мета роботи:**

**1. Отримання практичних навиків роботи з командною оболонкою Bash.**

**2. Знайомство з базовими структурами для збереження системних даних - процеси, память, лог-файли та**

**повідомлення про стан ядра.**

**3. Знайомство зі стандартом FHS.**

**4. Знайомство з діями при налаштуванні мережі.**

**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**

***Готувала матеріал студентка Нерощин Д.***

***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.***

***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?***

***4.2. Якими командами можна створити групи користувачів? Наведіть приклади***

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

***5. Підготувати в електронному вигляді початковий варіант звіту:***

***- Титульний аркуш, тема та мета роботи***

***- Словник термінівХід 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***

***\*\*\*Скріншоти виконання команд в терміналі можна не представляти, достатньо коротко описати команди***

***в таблиці.***

***Готувала матеріал студентка Мішин А.***

***3. 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.***

***Готував матеріал студент Малієнко А.***

***Контрольні запитання***

***1. Why are passwords not stored in clear text in configuration files?***

Passwords are not stored in clear text in configuration files for security reasons. Storing passwords in plain text would expose sensitive information and pose a significant security risk. If passwords were stored in clear text, unauthorized individuals with access to the configuration files could easily read and misuse the credentials. Using cryptographic hashing or encryption methods to store passwords helps enhance security by making it more difficult for attackers to retrieve and use the actual passwords even if they gain access to the configuration files.

***2. Why is it not recommended to perform routine operations using the root account?***

It is not recommended to perform routine operations using the root account for security and safety reasons. The root account in Unix-like operating systems has elevated privileges and unrestricted access to the entire system. Performing routine operations, such as everyday tasks and running applications, under the root account increases the risk of accidental damage to critical system files and configurations.

When using the root account, there is a higher likelihood of unintentional execution of potentially harmful commands, which can lead to system instability or compromise. Additionally, if a user inadvertently runs a malicious or flawed script while logged in as root, it could have severe consequences on the system's integrity and security.

To mitigate these risks, it is advisable to use regular user accounts for routine tasks and only switch to the root account when necessary, using tools like `sudo` to execute specific commands with elevated privileges. This practice helps minimize the scope of potential errors and enhances overall system security.

***3. What is the difference between the privilege escalation mechanisms of su and sudo?***

`su` (substitute user) is used to switch to another user by entering their password, while `sudo` (superuser do) allows authorized users to execute commands with the privileges of another user (usually the root user) after authenticating with their own password.

***4. Why is the home directory of the root user not located in the /home directory?***

The home directory of the root user is typically located at `/root` to maintain a clear distinction and prevent potential conflicts with regular user home directories in the `/home` directory.

***5. What is the purpose of the getent command?***

The `getent` command is used to retrieve entries from various name service switch libraries, including passwd, group, hosts, and others. It provides a unified interface to access system databases, allowing users and administrators to query information stored in different databases configured on the system.

The primary purpose of the `getent` command is to retrieve information from various sources specified in the Name Service Switch (NSS) configuration, which defines how the system resolves different types of queries, such as user information, group information, hostnames, and more.

For example, common uses of the `getent` command include:

- `getent passwd`: Retrieve information about user accounts.

- `getent group`: Retrieve information about user groups.

- `getent hosts`: Retrieve information about hostnames and IP addresses.

By using `getent`, administrators can obtain information from multiple sources, including local files (like /etc/passwd), NIS (Network Information Service), LDAP (Lightweight Directory Access Protocol), and other configured databases, providing a flexible and unified way to access system data.

***6. How can existing user groups be deleted, and will information about them still exist in the system?***

Existing user groups can be deleted using the `groupdel` command. Information about deleted groups may still exist in system files like `/etc/group` until the file is updated or the system is rebooted.

***7. How can a user's password be changed?***

The `passwd` command is used to change a user's password. Running `passwd` without any arguments prompts the user to enter a new password.

***8. What is the purpose of the chage command?***

The `chage` command is used to change user password expiry information. It allows administrators to set and view password aging information, including password expiry dates and other related details.

***9. Which parameters of the usermod command do you consider most commonly used?***

Commonly used parameters of the `usermod` command include:

1. `-l` (or `--login`): Change the username.

2. `-c` (or `--comment`): Change the user description or comment field.

3. `-G` (or `--groups`): Add the user to supplementary groups.

4. `-s` (or `--shell`): Change the login shell for the user.

5. `-aG` (or `--append --groups`): Add the user to additional groups without removing them from existing groups.

6. `-e` (or `--expiredate`): Set the account expiration date.

7. `-L` (or `--lock`): Lock the user account, preventing login.

8. `-U` (or `--unlock`): Unlock a previously locked user account.

9. `-p` (or `--password`): Set the encrypted password for the user (not recommended for interactive use).