**"Kyiv Vocational College of Communication"**

**Cyclic Commission of Computer Engineering**

**EXECUTION REPORT**

**LABORATORY WORK No. 9**

from the discipline: "Operating systems"

**Topic: "System and user protection in Linux. Creating users and groups"**

**Performed by students of the group:**

Барабаш Матвій  
Погребняк Ілля

Целуйко Станіслав

**Checked by the teacher**

Sushanova V.S

**Work of group students КСМ-13Б Team:** **PMC wolf group**

**The goal of the work:**

1. Getting practical skills for working with the Bash command shell.

2. Familiarity with basic file system navigation commands.

3. Familiarity with basic commands for managing files and directories.

**Material provision of classes**

1. IBM PC type computer.

2. OS family Windows (Windows 7).

3. Virtual machine - Virtual Box (Oracle).

4. GNU/Linux operating system - CentOS.

5. Cisco network academy site netacad.com and its online Linux courses

**Tasks for preliminary preparation:**

**Ilya Pogrebnyak was looking for material**

**4.1. Explain the concept of UPG, when it is appropriate to use them?**

UPG (User and Group Profiles) are user and group profiles used to manage access rights to files and directories on Linux systems. UPGs contain information about users and groups, including their names, default groups, group IDs, and file and directory permissions.

**\* UPG should be used in the following cases:**

- For centralized management of access rights to files and directories on the system.

- To ensure system security by restricting user access rights to files and directories.

- To simplify system administration by reducing the number of commands that must be used to manage access rights.

**4.2. What commands can be used to create user groups? Give examples**

- To create a user group in Linux systems, the following commands are used:

\* groupadd <groupname> - creates a group with the name <groupname>.

\* groupadd -g <gid> - creates a group with the name <groupname> and the group ID <gid>.

**- For example, to create a group with the name "developers" and a group ID of 1000, you can use the following command:**

groupadd -g 1000 developers

**4.3. What commands can be used to change user group settings? Give examples**

**- To change the settings of user groups in Linux systems, the following commands are used:**

\* groupmod -n <newname> <groupname> - changes the name of the group <groupname> to <newname>.

\* groupmod -g <gid> - changes the ID of the group <groupname> to <gid>.

\* groupmod -a <username> <groupname> - adds user <username> to group <groupname>.

\* groupmod -d <username> <groupname> - removes user <username> from group <groupname>.

**- For example, to change the name of the group "developers" to "dev" you can use the following command:**

\* groupmod -n dev developers

**- To change the ID of the "developers" group to 2000, you can use the following command:**

\* groupmod -g 2000 developers

**- To add the user "johndoe" to the "developers" group, you can use the following command:**

\* gpasswd -a johndoe developers

**Progress  
1)** **The table was made by Barabash Matviy**

|  |  |
| --- | --- |
| passwd | Changes the password for the current account. |
| chage | Changes the password settings for the current account. |
| useradd | Creates a new account. |
| usermod | Modifies an existing account. |
| userdel | Deletes an existing account. |
| groupadd | Creates a new group. |
| groupmod | Modifies an existing group. |
| groupdel | Deletes an existing group. |
| gpasswd | Adds or removes group members. |
| chgrp | Changes the owner group of a file or directory. |
| chown | Changes the owner of a file or directory. |
| sudo | Allows a user to execute commands with superuser privileges. |
| sudoers | A file that contains a list of users who have access to sudo. |
| passwd -l <username> | Locks the account. |
| passwd -u <username> | Unlocks the account. |
| passwd -x <username> | Removes the password for the account. |
| passwd -S <username> | View account status. |
| useradd -g <groupname> <username> | Creates an account with the default group. |
| useradd -G <group1>, <group2> <username> | Creates an account with additional groups. |
| useradd -m <username> | Creates an account from the home folder. |
| useradd -s <shell> | Creates an account with the given shell. |
| usermod -g <groupname> <username> | Changes the default group for an account. |
| usermod -G <group1>, <group2> <username> | Adds an account to additional groups. |
| userdel <username> | Deletes an account. |
| groupadd <groupname> | Creates a group. |
| groupmod -g <gid> <groupname> | Changes the group ID. |
| groupmod -n <newname> <groupname> | Changes the group name. |
| groupdel <groupname> | Deletes a group. |
| gpasswd -a <username> <groupname> | Adds a user to a group. |
| gpasswd -d <username> <groupname> | Removes a user from a group |
| chgrp <groupname> <filename> | Changes the group of the owner of the file. |
| chown <username> <filename> | Changes the owner of a file. |

**Control questions:**

**The answers to the control questions were given by Stanislav Tseluiko**

**1. Why is the password not stored explicitly in the configuration files?**

- Passwords are not stored explicitly in configuration files for security reasons. If the password is stored in the clear, it can be easily read by any user who has access to the file.

- Hash functions are used to store passwords in configuration files. A hash function turns a password into a string of characters that cannot be restored to its original form.

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

- The root account has full system access rights. This means that any mistake made in root mode can lead to serious problems with the system.

- For everyday operations that do not require full access rights, it is recommended to use a regular user account. This will help protect the system from unintentional errors.

**3. What is the difference between the mechanisms for obtaining su and sudo special privileges?**

- Both commands allow the user to obtain special privileges that are necessary to execute commands with superuser rights. However, there are some differences between them:

\* The su command switches the user to the root account. This means that all subsequent commands will be executed with superuser rights.

\* The sudo command allows a user to execute one or more commands with superuser privileges. After completing the commands, the user is returned to their normal account.

**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 placed in the /home directory for security reasons. This is due to the fact that the /home directory is publicly accessible to all users of the system.

- The root user's home directory is located in the /root directory, which has more limited access. This helps protect the root user's files from unauthorized access.

**5. What is the getent command used for?**

- The getent command is used to retrieve information from databases stored in the system.

For example, the getent group command allows you to get a list of all user groups.

**6. How can existing user groups be deleted? Will information about them remain somewhere in the system?**

- You can use the groupdel command to delete an existing user group. This command will remove the group from the system and all files belonging to that group.

- Information about the deleted group will remain in the /etc/group file. This file contains a list of all user groups that exist on the system.

**7. How can you change a user's password?**

- You can use the passwd command to change the user's password. This command allows you to change the password for the current account or for any other account.

\* To change the password for the current account, you can use the following command: passwd

\* To change the password for another account, you can use the following command: passwd <username>

- When changing the password, the user will be asked to enter the old password, the new password and confirm the new password.

**Conclusion:**

During the execution of the LB, I learned about new commands and what they mean, but unfortunately it did not work out in practice, because of problems with the terminal