

Отчёт по лабораторной работе №2

Управление пользователями и группами

Руслан Алиев

Содержание

1 Цель работы	5
2 Выполнение	6
2.1 Переключение учётных записей пользователей	6
2.2 Работа с файлом /etc/sudoers	7
2.3 Создание пользователей alice и bob	8
2.4 Настройка параметров создания пользователей	10
2.5 Создание и анализ пользователя carol	11
2.6 Работа с группами	13
3 Контрольные вопросы	14
4 Заключение	16

Список иллюстраций

2.1	Определение текущего пользователя и его идентификаторов	6
2.2	Переключение на пользователя root	7
2.3	Просмотр файла /etc/sudoers	8
2.4	Создание пользователя alice и проверка групп	9
2.5	Создание пользователя bob	9
2.6	Редактирование файла /etc/login.defs	10
2.7	Изменение файла .bashrc	11
2.8	Домашний каталог пользователя carol	12
2.9	Изменение параметров пароля пользователя carol	12
2.10	Проверка групп пользователей	13

Список таблиц

1 Цель работы

Получить представление о работе с учётными записями пользователей и группами пользователей в операционной системе типа Linux.

2 Выполнение

2.1 Переключение учётных записей пользователей

1. Работа была начата под обычной учётной записью пользователя.

Для определения текущего пользователя была использована команда **whoami**, после чего для получения расширенной информации применялась команда **id**.

В результате отображены следующие данные:

- **uid** – уникальный идентификатор пользователя в системе
- **gid** – идентификатор основной группы пользователя
- **groups** – список всех групп, в которые входит пользователь
- **context** – контекст безопасности SELinux

```
raliev@raliev:~$ whoami
raliev
raliev@raliev:~$ id
uid=1000(raliev) gid=1000(raliev) groups=1000(raliev),10(wheel) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
raliev@raliev:~$ su
Password:
root@raliev:/home/raliev# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
root@raliev:/home/raliev#
exit
raliev@raliev:~$
```

Рис. 2.1: Определение текущего пользователя и его идентификаторов

2. Для получения прав суперпользователя была использована команда **su**.

После ввода пароля пользователя root повторно выполнена команда **id**.

Вывод команды показывает, что пользователь root имеет идентификаторы **uid=0** и **gid=0**, что означает наличие полных административных прав в системе. Также отсутствуют ограничения по группам, а контекст SELinux указывает на неограниченный режим.

```
raliev@raliev:~$ whoami
raliev
raliev@raliev:~$ id
uid=1000(raliev) gid=1000(raliev) groups=1000(raliev),10(wheel) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
raliev@raliev:~$ su
Password:
root@raliev:/home/raliev# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
root@raliev:/home/raliev#
exit
raliev@raliev:~$
```

Рис. 2.2: Переключение на пользователя root

3. Возврат к исходной учётной записи был выполнен с помощью команды **exit**.

2.2 Работа с файлом /etc/sudoers

4. Для просмотра и редактирования файла **/etc/sudoers** использовалась команда **sudo -i visudo**.

Использование утилиты **visudo** является обязательным, так как она:

- проверяет синтаксис файла перед сохранением
- предотвращает сохранение некорректных изменений
- защищает систему от потери доступа к sudo

```
# Defaults    env_keep += "HOME"

Defaults    secure_path = /sbin:/bin:/usr/sbin:/usr/bin

## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##       user      MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root      ALL=(ALL)      ALL

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys  ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS

## Allows people in group wheel to run all commands
%wheel    ALL=(ALL)      ALL

## Same thing without a password
# %wheel      ALL=(ALL)      NOPASSWD: ALL

## Allows members of the users group to mount and umount the
## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users  localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#includedir /etc/sudoers.d
```

Рис. 2.3: Просмотр файла /etc/sudoers

5. В файле /etc/sudoers присутствует строка `%wheel ALL=(ALL) ALL`.

Данная запись означает, что все пользователи, входящие в группу **wheel**, имеют право выполнять любые команды от имени любого пользователя с использованием механизма sudo. Группа **wheel** применяется для разграничения административных привилегий.

2.3 Создание пользователей **alice** и **bob**

6. Был создан пользователь **alice**, включённый в группу **wheel**.

Проверка принадлежности к группе выполнена с помощью команды **id alice**.

```
-----  
raliev@raliev:~$ sudo -i visudo  
[sudo] password for raliev:  
raliev@raliev:~$  
raliev@raliev:~$ sudo -i useradd -G wheel alice  
raliev@raliev:~$ id alice  
uid=1001(alice) gid=1001(alice) groups=1001(alice),10(wheel)  
raliev@raliev:~$ sudo -i passwd alice  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
passwd: password updated successfully  
-----
```

Рис. 2.4: Создание пользователя alice и проверка групп

7. Для пользователя **alice** был установлен пароль стандартным способом.
8. Выполнено переключение на учётную запись пользователя **alice**.
9. Под пользователем **alice** был создан пользователь **bob**, после чего ему также был назначен пароль.

Проверка существования пользователя выполнена командой **id bob**.

```
raliev@raliev:~$ su alice  
Password:  
alice@raliev:/home/raliev$ sudo useradd bob  
  
We trust you have received the usual lecture from the local System  
Administrator. It usually boils down to these three things:  
  
#1) Respect the privacy of others.  
#2) Think before you type.  
#3) With great power comes great responsibility.  
  
For security reasons, the password you type will not be visible.  
  
[sudo] password for alice:  
alice@raliev:/home/raliev$ sudo passwd bob  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
passwd: password updated successfully  
alice@raliev:/home/raliev$ id bob  
uid=1002(bob) gid=1002(bob) groups=1002(bob)  
-----
```

Рис. 2.5: Создание пользователя bob

2.4 Настройка параметров создания пользователей

10. Под учётной записью root был открыт файл конфигурации `/etc/login.defs`.

В файле были изменены параметры:

- `CREATE_HOME` установлен в значение `yes`, что обеспечивает автоматическое создание домашнего каталога пользователя
- `USERGROUPS_ENAB` установлен в значение `no`, что запрещает создание персональной группы с именем пользователя и позволяет использовать общую группу `users`

```
# the user to be removed (passed as the first argument).
#USERDEL_CMD    /usr/sbin/userdel_local

#
# Enables userdel(8) to remove user groups if no members exist.
#
USERGROUPS_ENAB no

#
# If set to a non-zero number, the shadow utilities will make sure that
# groups never have more than this number of users on one line.
# This permits to support split groups (groups split into multiple lines,
# with the same group ID, to avoid limitation of the line length in the
# group file).
#
# 0 is the default value and disables this feature.
#
#MAX_MEMBERS_PER_GROUP  0

#
# If useradd(8) should create home directories for users by default (non
# system users only).
# This option is overridden with the -M or -m flags on the useradd(8)
# command-line.
#
CREATE_HOME yes

#
# Force use shadow, even if shadow passwd & shadow group files are
# missing.
#
#FORCE_SHADOW yes

#
# Select the HMAC cryptography algorithm.
```

Рис. 2.6: Редактирование файла `/etc/login.defs`

11. В каталоге `/etc/skel` были созданы каталоги **Pictures** и **Documents**, которые автоматически копируются в домашние каталоги новых пользователей.

12. В файл .bashrc, находящийся в каталоге /etc/skel, была добавлена переменная окружения EDITOR, указывающая редактор по умолчанию.



```
# .bashrc

# Source global definitions
if [ -f /etc/bashrc ]; then
    . /etc/bashrc
fi

# User specific environment
if ! [[ "$PATH" =~ "$HOME/.local/bin:$HOME/bin:" ]]; then
    PATH="$HOME/.local/bin:$HOME/bin:$PATH"
fi
export PATH

# Uncomment the following line if you don't like systemctl's auto-paging feature:
# export SYSTEMD_PAGER=

# User specific aliases and functions
if [ -d ~/.bashrc.d ]; then
    for rc in ~/.bashrc.d/*; do
        if [ -f "$rc" ]; then
            . "$rc"
        fi
    done
fi
unset rc
export EDITOR=/usr/bin/vim
~
```

Рис. 2.7: Изменение файла .bashrc

2.5 Создание и анализ пользователя carol

13. Под пользователем **alice** был создан пользователь **carol**, после чего ему был назначен пароль.
14. После переключения на пользователя **carol** были проверены его идентификаторы и содержимое домашнего каталога.

Установлено, что:

- основной группой пользователя является **users**
- каталоги **Pictures** и **Documents** были созданы автоматически

```

root@raliev:/etc/skel# su alice
alice@raliev:/etc/skel$ sudo -i useradd carol
alice@raliev:/etc/skel$ sudo passwd carol
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
alice@raliev:/etc/skel$ su carol
Password:
carol@raliev:/etc/skel$ id
uid=1003(carol) gid=100(users) groups=100(users) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
carol@raliev:/etc/skel$ cd
carol@raliev:~$ ls -Al
total 12
-rw-r--r--. 1 carol users 18 Oct 29 2024 .bash_logout
-rw-r--r--. 1 carol users 144 Oct 29 2024 .bash_profile
-rw-r--r--. 1 carol users 549 Dec 14 11:27 .bashrc
drwxr-xr-x. 2 carol users 6 Dec 14 11:26 Documents
drwxr-xr-x. 4 carol users 39 Oct 2 18:52 mozilla
drwxr-xr-x. 2 carol users 6 Dec 14 11:26 Pictures
carol@raliev:~$ █

```

Рис. 2.8: Домашний каталог пользователя carol

15. В файле `/etc/shadow` была просмотрена строка, относящаяся к пользователю **carol**.

Данная строка содержит зашифрованный пароль, дату последнего изменения пароля, а также параметры, определяющие срок его действия.

16. Были изменены параметры пароля пользователя **carol**: минимальный срок действия, срок действия пароля и период предупреждения об истечении срока.

```

alice@raliev:/etc/skel$ sudo cat /etc/shadow | grep carol
carol:$y$j9T$kf00eKV3Hk0WSPLRDUSvl.$EhupcKwKTMDT8r6BDRQGdT/CKKsRm5Q0059KPHB3zPlA:20436:0:99999:7:::
alice@raliev:/etc/skel$ sudo passwd -n 30 -w 3 -x 90 carol
passwd: password changed.
alice@raliev:/etc/skel$ sudo cat /etc/shadow | grep carol
carol:$y$j9T$kf00eKV3Hk0WSPLRDUSvl.$EhupcKwKTMDT8r6BDRQGdT/CKKsRm5Q0059KPHB3zPlA:20436:30:90:3:::
alice@raliev:/etc/skel$ sudo grep alice /etc/passwd /etc/shadow /etc/group
/etc/passwd:alice:x:1001:1001::/home/alice:/bin/bash
/etc/shadow:alice:$y$j9T$NN0VCQbu/malVuIzdia.w/$MA2tWxe/2g8JiCEcWkgqRs8RhkeybY.mb1fDX8DCwh4:20436:0:99999:7:::
/etc/group:wheel:x:10:raliev,alice
/etc/group:alice:x:1001:
alice@raliev:/etc/skel$ sudo grep carol /etc/passwd /etc/shadow /etc/group
/etc/passwd:carol:x:1003:100::/home/carol:/bin/bash
/etc/shadow:carol:$y$j9T$kf00eKV3Hk0WSPLRDUSvl.$EhupcKwKTMDT8r6BDRQGdT/CKKsRm5Q0059KPHB3zPlA:20436:30:90:3:::
alice@raliev:/etc/skel$ █

```

Рис. 2.9: Изменение параметров пароля пользователя carol

17. Повторная проверка файла `/etc/shadow` подтвердила применение новых параметров.
18. Выполнена проверка наличия записей о пользователях **alice** и **carol** в файлах `/etc/passwd`, `/etc/shadow` и `/etc/group`.

2.6 Работа с группами

19. Под учётной записью пользователя **alice** были созданы группы **main** и **third**.
20. Пользователи **alice** и **bob** были добавлены в группу **main**, а пользователь **carol** – в группу **third**.
21. С помощью команды **id** подтверждено, что пользователь **carol** имеет основную группу **users** и вторичную группу **third**.

Также определены группы, в которые входят остальные созданные пользователи.

```
alice@raliev:/etc/skel$ sudo groupadd main
alice@raliev:/etc/skel$ sudo groupadd third
alice@raliev:/etc/skel$ sudo usermod -aG main alice
alice@raliev:/etc/skel$ sudo usermod -aG main bob
alice@raliev:/etc/skel$ sudo usermod -aG third carol
alice@raliev:/etc/skel$ id carol
uid=1003(carol) gid=100(users) groups=100(users),1004(third)
alice@raliev:/etc/skel$ id bob
uid=1002(bob) gid=1002(bob) groups=1002(bob),1003(main)
alice@raliev:/etc/skel$ id alice
uid=1001(alice) gid=1001(alice) groups=1001(alice),10(wheel),1003(main)
alice@raliev:/etc/skel$ █
```

Рис. 2.10: Проверка групп пользователей

3 Контрольные вопросы

1. Информацию об идентификаторе пользователя и группах, в которые он включён, можно получить с помощью команд **whoami** и **id**.

Команда **whoami** выводит имя текущего пользователя, а команда **id** отображает UID пользователя, его основной GID и список всех групп, в которые он входит.

2. Пользователь **root** имеет идентификатор **UID = 0**.

Узнать UID пользователя можно с помощью команды **id**. Например, при выполнении команды **id root** в выводе будет указано **uid=0**, что подтверждает принадлежность пользователя к суперпользователям.

3. Команда **su** используется для полного переключения на другую учётную запись и запуска новой оболочки от имени другого пользователя.

Команда **sudo** позволяет выполнять отдельные команды с повышенными привилегиями, не переключаясь полностью на другую учётную запись. При этом используются собственные учётные данные пользователя.

4. Параметры работы утилиты sudo определяются в конфигурационном файле **/etc/sudoers**, а также в дополнительных файлах, подключаемых из каталога **/etc/sudoers.d**.

5. Для безопасного изменения конфигурации sudo следует использовать команду **visudo**.

Она выполняет проверку синтаксиса перед сохранением файла и предот-

вращает повреждение конфигурации, которое может привести к потере доступа к sudo.

6. Для предоставления пользователю доступа ко всем административным командам через sudo он должен быть членом группы **wheel**.

Это обеспечивается строкой `%wheel ALL=(ALL) ALL` в файле `/etc/sudoers`.

7. Параметры, используемые при создании учётных записей пользователей, определяются в файле `/etc/login.defs` и каталоге `/etc/skel`.

В файле `/etc/login.defs` задаются, например, параметры автоматического создания домашнего каталога и политики групп, а каталог `/etc/skel` содержит файлы и каталоги, которые копируются в домашний каталог нового пользователя.

8. Информация о первичной и дополнительных группах пользователей хранится в файлах `/etc/passwd` и `/etc/group`.

В файле `/etc/passwd` для пользователя **alice** указывается его UID, основной GID и домашний каталог.

В файле `/etc/group` перечислены группы, в которых пользователь **alice** указан как член вторичной группы, например группы **wheel** или **main**.

9. Для изменения информации о пароле пользователя, включая срок его действия, используются команды **passwd** с дополнительными параметрами.

С их помощью можно задать минимальный и максимальный срок действия пароля, а также период предупреждения пользователя об истечении срока действия.

10. Для прямого изменения информации в файле `/etc/group` следует использовать команду **vigr**.

Она обеспечивает безопасное редактирование файла групп, выполняет блокировку файла на время изменения и предотвращает возможные ошибки конфигурации.

4 Заключение

В ходе лабораторной работы были изучены механизмы управления пользователями и группами в операционной системе Linux. Освоены приёмы переключения между учётными записями, предоставления административных прав с помощью sudo, создания и настройки пользователей, а также управления группами и параметрами паролей. Полученные навыки позволяют эффективно администрировать систему и контролировать доступ пользователей к ресурсам ОС.