Отчет по лабораторной работе №1
“Учетные записи и группы пользователей Linux”
по дисциплине
“Информационная безопасность”

Выполнил:
студент группы P34131
Бусыгин Дмитрий Алексеевич
Преподаватель:
Маркина Татьяна Анатольевна

Санкт-Петербург
2024

Цель работы

Изучить параметры учетных записей пользователей в Linux. Ознакомиться с процессом конфигурации и изменения учетных записей по умолчанию. Изучить процесс разграничения доступа к данным и модификации прав доступа.

Основная часть

Пункт 1.

Создание пользователя и группы.

```
busygind02@ubuntu-vm:~$ sudo useradd s335103
busygind02@ubuntu-vm:~$ sudo groupadd studs
busygind02@ubuntu-vm:~$ sudo usermod -aG studs s335103
busygind02@ubuntu-vm:~$ groups s335103
s335103 : s335103 studs
```

Пункт 2.

Создание root-пользователя

```
busygind02@ubuntu-vm:~$ sudo useradd admin_s335103
```

Способы выдачи root-прав

Способ 1: изменение файла /etc/passwd

```
busygind02@ubuntu-vm:~$ sudo vim /etc/passwd
...
admin_s335103:x:0:0::/home/admin_s335103:/bin/sh
...
```

В файле /etc/passwd хранится информация о пользователях, в т.ч. UID (user ID) и GID (group ID). UID и GID, равные 0, соответствуют пользователю root и группе root соответственно. Выставим пользователю admin_s335103 значения UID=0 и GID=0.

Способ 2: добавление пользователя в группу root

```
busygind02@ubuntu-vm:~$ sudo usermod -aG root admin_s335103
busygind02@ubuntu-vm:~$ groups admin_s335103
admin_s335103 : root
```

Способ 3: добавление пользователя в конфигурационный файл /etc/sudoers

```
busygind02@ubuntu-vm:~$ sudo visudo
...
```

```
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
admin_s335103 ALL=(ALL:ALL) ALL
```

Запись "ALL=(ALL:ALL) ALL" означает, что пользователю выданы привилегии root, позволяющие выполнять любую команду от имени любого пользователя на любом хосте

Пункт 3.

Демонстрация root-привилегий

Переопределим пароли для ранее созданных пользователей:

```
busygind02@ubuntu-vm:~$ sudo passwd s335103
New password:
Retype new password:
passwd: password updated successfully
busygind02@ubuntu-vm:~$ sudo passwd admin_s335103
New password:
Retype new password:
passwd: password updated successfully
```

Отличие 1. доступ к /etc/shadow

```
busygind02@ubuntu-vm:~$ su s335103
Password:
$ cat /etc/shadow
cat: /etc/shadow: Permission denied
busygind02@ubuntu-vm:~$ su admin_s335103
Password:
# cat /etc/shadow
root:!:19866:0:99999:7:::
...
```

Отличие 2. доступ к директории /root

```
busygind02@ubuntu-vm:~$ su s335103
Password:
$ cd /root
sh: 1: cd: can't cd to /root
busygind02@ubuntu-vm:~$ su admin_s335103
Password:
# cd /root
# ls -l
total 0
```

Отличие 3. возможность установки новых пакетов

```
busygind02@ubuntu-vm:~$ su s335103
Password:
$ apt-get install colima
E: Could not open lock file /var/lib/dpkg/lock-frontend - open (13:
Permission denied)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontend)
busygind02@ubuntu-vm:~$ su admin_s335103
# apt-get install colima
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
...
```

Отличие 4. возможность управления правами других пользователей

```
busygind02@ubuntu-vm:~$ su s335103
Password:
$ chmod o-x $(which echo)
chmod: changing permissions of '/usr/bin/echo': Operation not permitted
busygind02@ubuntu-vm:~$ su admin_s335103
Password:
# chmod o-x $(which echo)
...
```

Отличие 5. возможность создания/удаления пользователей

```
busygind02@ubuntu-vm:~$ su s335103
Password:
$ useradd test
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
busygind02@ubuntu-vm:~$ su admin_s335103
Password:
# useradd test
...
```

Пункт 4.

Задание по варианту

Порядковый номер в группе - 4

Задание: убрать возможность создания группы по умолчанию для новых пользователей без группы.

```
busygind02@ubuntu-vm:~$ sudo vim /etc/login.defs
...
USERGROUPS_ENAB no
busygind02@ubuntu-vm:~$ sudo useradd test1
```

```
busygind02@ubuntu-vm:~$ sudo su test1
$ groups
users
```

По умолчанию в UNIX-системах каждому новому пользователю создается primary группа с названием, идентичным названию пользователя. Это может быть чревато сложностью настройки прав для новых пользователей, т.к у них нет общей группы.

В конфигурационном файле `/etc/login.defs` параметр `USERGROUPS_ENAB` отвечает как раз за создание primary групп. После его отключения новым пользователям будет присваиваться только группа users (GID:100)

Дополнительная часть

1. Создайте каталог /studs. Настройте группу studs так, чтобы только у ее членов был доступ к этому каталогу. Продемонстрируйте, что у других групп нет доступа к этому каталогу.

```
busygind02@ubuntu-vm:~$ sudo mkdir /studs
busygind02@ubuntu-vm:~$ ls -l / | grep studs
drwxr-xr-x   2 root root  4096 Oct  5 23:49 studs
busygind02@ubuntu-vm:~$ sudo chown :studs /studs/
busygind02@ubuntu-vm:~$ sudo chmod 770 /studs/
busygind02@ubuntu-vm:~$ ls -l / | grep studs
drwxrwx---   2 root studs  4096 Oct  5 23:49 studs
busygind02@ubuntu-vm:~$ cd /studs
-bash: cd: /studs: Permission denied
busygind02@ubuntu-vm:~$ su s335103
Password:
$ cd /studs
$ ls -l
total 0
```

2. Измените конфигурацию таким образом, чтобы у всех пользователей домашний каталог создавался в /studs/… Продемонстрируйте выполнение, создав тестового пользователя.

```
busygind02@ubuntu-vm:~$ sudo vim /etc/default/useradd
<...>
# The default home directory. Same as DHOME for adduser
HOME=/studs

busygind02@ubuntu-vm:~$ sudo useradd test_homedir -m -G studs
busygind02@ubuntu-vm:~$ sudo passwd test_homedir
New password:
Retype new password:
passwd: password updated successfully
```

```
busygind02@ubuntu-vm:~$ su test_homedir
Password:
$ cd
$ pwd
/studs/test_homedir
```

3. Создайте каталог /studs/lab_reports. Настройте права так, чтобы файлы из этого каталога могли удалять только те пользователи, которые эти файлы создали. Продемонстрируйте изменения, создав новый файл и удалив его, как другой пользователь.

```
busygind02@ubuntu-vm:~$ sudo mkdir /studs/lab_reports
busygind02@ubuntu-vm:~$ sudo chown :studs /studs/lab_reports
busygind02@ubuntu-vm:~$ sudo chmod 1770 /studs/lab_reports
busygind02@ubuntu-vm:~$ sudo ls -ld /studs/lab_reports
drwxrwx--T 2 root studs 4096 Oct  6 00:27 /studs/lab_reports
busygind02@ubuntu-vm:~$ su s335103
Password:
$ touch /studs/lab_reports/test_report
$ ls -la /studs/lab_reports | grep test_report
-rw-r--r-- 1 s335103 s335103    0 Oct  6 00:28 test_report

busygind02@ubuntu-vm:~$ sudo su test1
$ rm /studs/lab_reports/test_report
rm: cannot remove '/studs/lab_reports/test_report': Permission denied
$
busygind02@ubuntu-vm:~$ su s335103
Password:
$ rm /studs/lab_reports/test_report
$ ls -la /studs/lab_reports | grep test_report
$
```

Специфицировать права на удаление конкретным пользователем можно с помощью sticky bit на директорию. Если он установлен, то файл можно удалить только пользователю, который является владельцем файла или каталога, в котором содержится файл.

Вывод:

В процессе выполнения лабораторной работы я освоил на практике способы задания прав в UNIX, ознакомился с привилегиями root-пользователей и конфигурационными файлами /etc/shadow, /etc/passwd, /etc/group и другими.