МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное автономное образовательное учреждение высшего образования “Национальный исследовательский университет ИТМО”

ФАКУЛЬТЕТ ПРОГРАММНОЙ ИНЖЕНЕРИИ И КОМПЬЮТЕРНОЙ ТЕХНИКИ

ЛАБОРАТОРНАЯ РАБОТА №1

“Учетные записи и группы пользователей Linux”

по дисциплине

“Информационная безопасность”

Вариант 11

Выполнил:

Иванов Матвей Сергеевич

группа P34111

Преподаватель:

Маркина Татьяна Анатольевна

г. 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.

Ход выполнения:

1) Создайте пользователя sXXXXXX(где XXXXXX - ваш номер ису). Создайте группу пользователей studs, добавьте пользователя в эту группу.

```
root@v132798:~# useradd s335105
root@v132798:~# groupadd studs
root@v132798:~# usermod -aG studs s335105
root@v132798:~# id s335105
uid=1000(s335105) gid=1000(s335105) groups=1000(s335105),1001(studs)
root@v132798:~#
```

2) Создайте пользователя admin_sXXXXXX(где XXXXXX - ваш номер ису). Предоставьте пользователю root-права. Опишите все способы, которыми можно это сделать и продемонстрируйте их. (минимум 3 способа).

Способы:

1. Создать пользователя и добавить пользователя в группу root с помощью команды usermod

```
root@v132798:~# useradd admin_s335105
root@v132798:~# usermod -aG root admin_s335105
root@v132798:~# id admin_s335105
uid=1001(admin_s335105) gid=1002(admin_s335105) groups=1002(admin_s335105),0(root)
root@v132798:~#
```

2. Создать пользователя сразу в группе root с помощью аргументов команды useradd

```
root@v132798:~# useradd -ou 0 -g 0 admin_s335105
root@v132798:~# id admin_s335105
uid=0(root) gid=0(root) groups=0(root)
root@v132798:~#
```

   Аргументы -ou указывает на UID пользователя, а -g на группу (для root всё будет 0)

3. Создать пользователя и отредактировать файл /etc/passwd изменив UID и GID пользователя:

```
[root@v132798:~# useradd admin_s335105
[root@v132798:~# vipw --passwd
You have modified /etc/passwd.
You may need to modify /etc/shadow for consistency.
Please use the command 'vipw -s' to do so.
[root@v132798:~# id admin_s335105
uid=0(root) gid=0(root) groups=0(root)
```

Было:

```
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
s335105:x:1000:1000::/home/s335105:/bin/sh
admin_s335105:x:1001:1002::/home/admin_s335105:/bin/sh
```

Стало:

```
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
s335105:x:1000:1000::/home/s335105:/bin/sh
admin_s335105:x:0:0::/home/admin_s335105:/bin/sh
```

4. Создать пользователя и дать ему доступ ко всем привилегиям в /etc/sudoers

```
[root@v132798:~# useradd admin_s335105
[root@v132798:~# visudo
[root@v132798:~# id admin_s335105
uid=1001(admin_s335105) gid=1002(admin_s335105) groups=1002(admin_s335105)
root@v132798:~#
```

```
# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

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

admin_s335105   ALL=(ALL:ALL) ALL
```

3) Продемонстрируйте, что пользователь admin_sXXXXXX(где XXXXXX - ваш номер ису), теперь имеет больше привилегий, по сравнению с пользователем user_sXXXXXX. Предоставьте минимум 5 отличий.

Я остановился на варианте 2 прошлого пункта для создания пользователя admin_s335105. Также создадим домашние директории для каждого из пользователей:

```
root@v132798:~# mkhomedir_helper admin_s335105
root@v132798:~# mkhomedir_helper s335105
```

Отличия:

1. Зайдем на пользователя admin_s335105 и попробуем изменить пароль пользователя s335105 - у нас это успешно получается, так как у admin_s335105 все права root.

   При этом, если мы зайдем на пользователя s335105 и попробуем изменить пароль admin_s335105 у нас не выйдет, так как недостаточно прав для такого действия

   ```
   root@v132798:~# su admin_s335105
   # passwd s335105
   New password:
   Retype new password:
   passwd: password updated successfully
   #
   root@v132798:~# su s335105
   $ passwd admin_s335105
   passwd: You may not view or modify password information for admin_s335105.
   $
   root@v132798:~#
   ```

2. Создадим папку с файлом в домашних директориях пользователей:

   ```
   root@v132798:~# su admin_s335105
   # cd ~
   # pwd
   /home/admin_s335105
   # mkdir test
   # touch test/test.file
   # ls -l
   total 4
   drwxr-xr-x 2 root root 4096 Sep 22 13:41 test
   # ls -l test
   total 0
   -rw-r--r-- 1 root root 0 Sep 22 13:41 test.file
   #
   ```

```
root@v132798:~# su s335105
$ cd ~
$ pwd
/home/s335105
$ mkdir test
$ touch test/test.file
$ ls -l
total 4
drwxrwxr-x 2 s335105 s335105 4096 Sep 22 13:43 test
$ ls -l test
total 0
-rw-rw-r-- 1 s335105 s335105 0 Sep 22 13:43 test.file
$
```

Теперь, как видно из вывода ls -l, все пользователи имеют доступ на чтение к этим директориям и файлам, но на редактирование только сами пользователи. Зайдем за пользователя s335105 и попробуем создать файл в папке созданной admin_s335105 - получаем ошибку доступа. Но если мы зайдём за пользователя admin_s335105 и попробуем создать файл в папке созданной s335105, то у нас всё получится, так как root имеет доступ ко всем файлам системы.

```
root@v132798:~# su s335105
$ ls /home/admin_s335105/test
test.file
$ cat /home/admin_s335105/test/test.file
$ touch /home/admin_s335105/test/new_test.file
touch: cannot touch '/home/admin_s335105/test/new_test.file': Permission denied
$
root@v132798:~# su admin_s335105
# ls /home/s335105/test
test.file
# cat /home/s335105/test/test.file
# touch /home/s335105/test/new_test.file
# ls /home/s335105/test
new_test.file  test.file
#
```

3. В продолжение прошлого пункта, попробуем изменить доступы к директориям и файлам. Попробуем изменить доступы с пользователя s335105 директории test и файла test.file пользователя admin_s335105:

```
root@v132798:~# su s335105
$ chmod 000 -R /home/admin_s335105/test
chmod: changing permissions of '/home/admin_s335105/test': Operation not permitted
chmod: changing permissions of '/home/admin_s335105/test/test.file': Operation not permitted
$
```

Как видно, он не сможет этого сделать. Теперь попробуем сделать наоборот:

```
root@v132798:~# su admin_s335105
# chmod 000 -R /home/s335105/test
# ls -l /home/s335105/
total 4
d--------- 2 s335105 s335105 4096 Sep 22 13:47 test
# ls -l /home/s335105/test
total 0
---------- 1 root    root    0 Sep 22 13:47 new_test.file
---------- 1 s335105 s335105 0 Sep 22 13:43 test.file
# cat /home/s335105/test/test.file
#
```

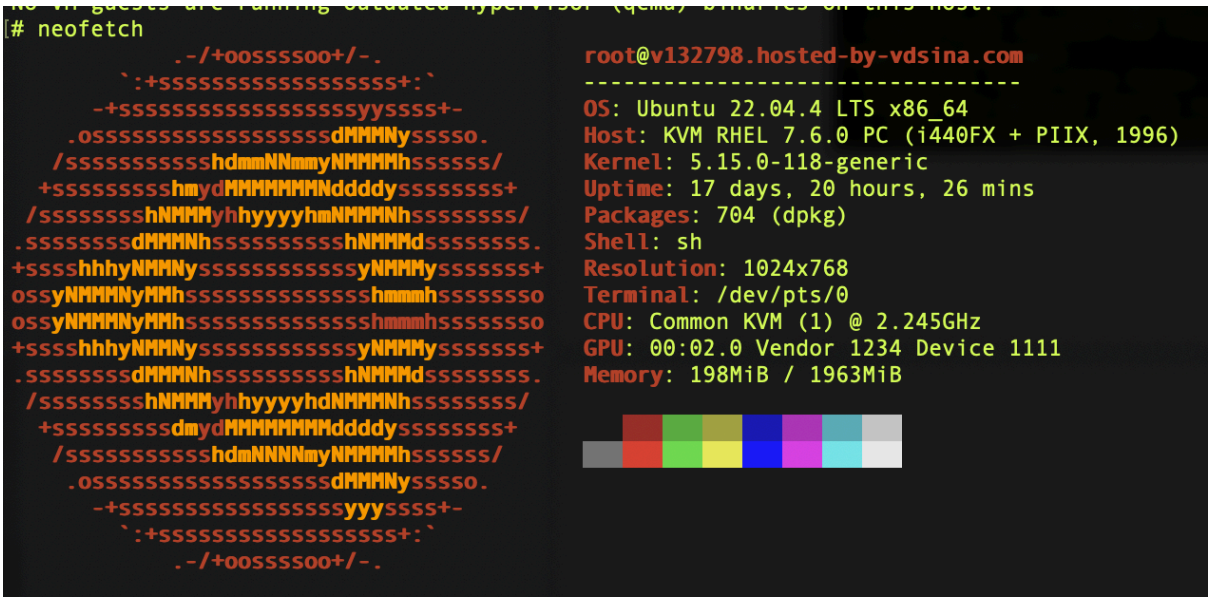
Доступы успешно изменены (удалены все доступы), при том root всё ещё имеет доступ к директориям и файлам. При том сам владелец этих файлов s335105 больше не имеет доступа к ним:

```
root@v132798:~# su s335105
$ cd ~
$ pwd
/home/s335105
$ ls test
ls: cannot open directory 'test': Permission denied
$ cat test/test.file
cat: test/test.file: Permission denied
$
```

4. Установка новых пакетов через apt (apt-get):

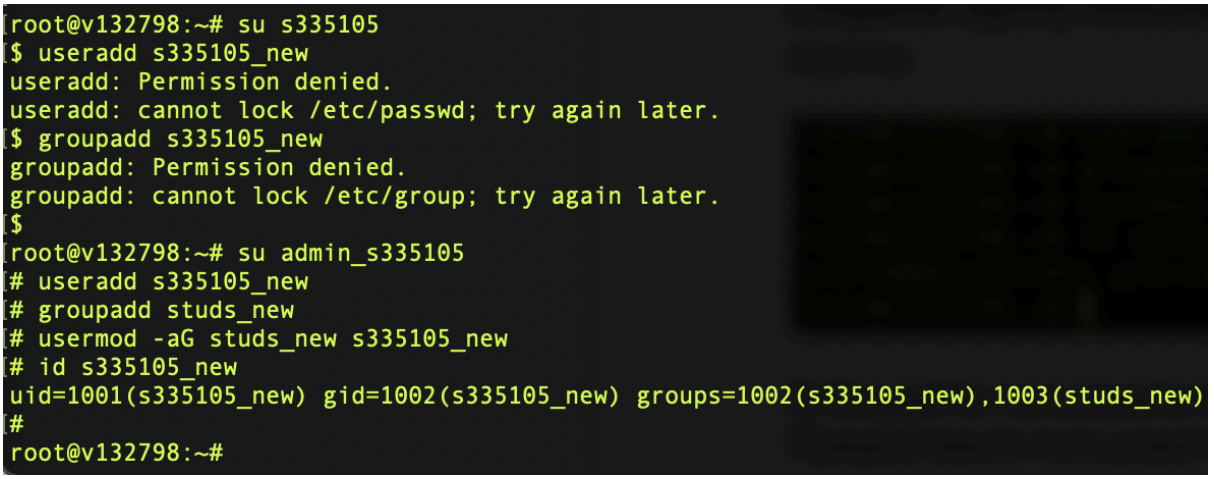
   Пользователь s335105 не имеет доступа к установке пакетов, при том что у пользователя admin_s335105 доступ есть:

```
root@v132798:~# su s335105
$ apt-get install neofetch
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), are you root?
$
root@v132798:~# su admin_s335105
# apt-get install neofetch
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  bzip2 caca-utils chafa fontconfig fontconfig-config fonts-dejavu-core fonts-droid-fallba
  imagemagick-6.q16 jp2a libaom3 libavahi-client3 libavahi-common-data libavahi-common3 li
  libdjvulibre21 libfftw3-double3 libfontconfig1 libgc1 libgif7 libgomp1 libgraphite2-3 li
  libjbig2dec0 libjpeg-turbo8 libjpeg8 libjxr-tools libjxr0 liblcms2-2 liblqr-1-0 libltdl7
  libpango-1.0-0 libpangocairo-1.0-0 libpangoft2-1.0-0 libpaper-utils libpaper1 libpixman-
  libx11-xcb1 libx265-199 libxcb-render0 libxcb-shm0 libxrender1 netpbm poppler-data toile
Suggested packages:
  bzip2-doc fonts-noto fonts-freefont-otf | fonts-freefont-ttf fonts-texgyre ghostscript-x
  libwmf-bin mplayer povray radiance sane-utils texlive-base-bin transfig ufraw-batch xdg-
  | fonts-ipafont-mincho fonts-japanese-gothic | fonts-ipafont-gothic fonts-arphic-ukai fo
```



5. Создание пользователей и групп.

   Пользователь admin_s335105 может создать, редактировать и удалять нового пользователя или группу, а пользователь s335105 этого сделать не может.



Задание по варианту:

11) Задайте диапазон UID для создания новых пользователей, отличный от диапазона по умолчанию.

Отредактируем параметры UID_MIN и UID_MAX в файле /etc/login.defs:

Было:

```
#
# Min/max values for automatic uid selection in useradd
#
UID_MIN                  1000
UID_MAX                 60000
# System accounts
#SYS_UID_MIN               100
#SYS_UID_MAX               999
```

Стало:

```
#
# Min/max values for automatic uid selection in useradd
#
UID_MIN                 60000
UID_MAX                 62000
# System accounts
#SYS_UID_MIN               100
#SYS_UID_MAX               999
```

Создадим нового пользователя, чтобы проверить, что UID теперь выбирается из нового диапазона:

```
root@v132798:~# useradd s335105_new
root@v132798:~# id s335105_new
uid=60000(s335105_new) gid=60000(s335105_new) groups=60000(s335105_new)
root@v132798:~# useradd s335105_new2
root@v132798:~# id s335105_new2
uid=60001(s335105_new2) gid=1002(s335105_new2) groups=1002(s335105_new2)
root@v132798:~#
```

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.

Создаём директорию и файл внутри в домашней директории пользователя s335105. Устанавливаем группу и доступ только для владельца и группы.

```
[root@v132798:~# su s335105
 $ cd /home/s335105
[$ mkdir studs
[$ echo 'TEST' > studs/check.file
[$ ls -l
 total 8
 drwxrwxr-x 2 s335105 s335105 4096 Sep 22 14:20 studs
 d--------- 2 s335105 s335105 4096 Sep 22 13:47 test
[$ ls -l studs
 total 4
 -rw-rw-r-- 1 s335105 s335105 5 Sep 22 14:20 check.file
[$ chgrp -R studs studs/
[$ chmod -R 770 studs/
[$ ls -l
 total 8
 drwxrwx--- 2 s335105 studs   4096 Sep 22 14:20 studs
 d--------- 2 s335105 s335105 4096 Sep 22 13:47 test
[$ ls -l studs
 total 4
 -rwxrwx--- 1 s335105 studs 5 Sep 22 14:20 check.file
[$ cat studs/check.file
 TEST
 $
```

Из прошлого задания у нас есть пользователи s335105_new и s335105_new2. Добавим пользователя s335105_new в группу studs и проверим что есть доступ к директории и файлу.

```
[root@v132798:~# usermod -aG studs s335105_new
[root@v132798:~# id s335105_new
 uid=60000(s335105_new) gid=60000(s335105_new) groups=60000(s335105_new),1001(studs)
[root@v132798:~# su s335105_new
[$ cd /home/s335105
[$ ls studs
 check.file
[$ cat studs/check.file
 TEST
[$
```

Доступ есть. Теперь проверим доступ к этой же директории и файлу пользователя s335105_new2, не добавляя его в группу studs.

```
[root@v132798:~# id s335105_new2
 uid=60001(s335105_new2) gid=1002(s335105_new2) groups=1002(s335105_new2)
[root@v132798:~# su s335105_new2
[$ cd /home/s335105
[$ ls studs
 ls: cannot open directory 'studs': Permission denied
[$ cat studs/check.file
 cat: studs/check.file: Permission denied
[$
```

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

Отредактируем параметр DHOME в файле /etc/adduser.conf

```
root@v132798:~# nano /etc/adduser.conf
```

Было:

```
# The DHOME variable specifies the directory containing users' home
# directories.
DHOME=/home
```

Стало:

```
# The DHOME variable specifies the directory containing users' home
# directories.
DHOME=/studs
```

Аналогично отредактируем /etc/default/useradd файл

Было:

```
#
# The default home directory. Same as DHOME for adduser
# HOME=/home
#
```

Стало:

```
#
# The default home directory. Same as DHOME for adduser
HOME=/studs
#
```

Попробуем создать нового пользователя с домашней директорией:

```
root@v132798:~# useradd -m s335105_new3
root@v132798:~# ls /studs
s335105_new3
root@v132798:~# ls /home
admin_s335105  s335105
root@v132798:~#
```

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.

Создадим директорию и зададим на неё права. Первая цифра в chmod 1 означает sticky bit, который как раз таки даст пользователям возможность удалять и переименовывать только свои файлы.

```
root@v132798:~# mkdir /studs/lab_reports
root@v132798:~# chmod 1777 /studs/lab_reports
root@v132798:~# ls -ld /studs/lab_reports
drwxrwxrwt 2 root root 4096 Sep 22 14:44 /studs/lab_reports
root@v132798:~#
```

Проверим, создадим файл от лица пользователя s335105 и попробуем его удалить от лица пользователя s335105_new:

```
root@v132798:~# su s335105
$ echo 'My report' > /studs/lab_reports/report.txt
$ ls /studs/lab_reports/
report.txt
$
```

```
root@v132798:~# su s335105_new
$ ls -l /studs/lab_reports/
total 4
-rw-rw-r-- 1 s335105 s335105 10 Sep 22 14:48 report.txt
$ rm -rf /studs/lab_reports/report.txt
rm: cannot remove '/studs/lab_reports/report.txt': Operation not permitted
$ cat /studs/lab_reports/report.txt
My report
$
```

При том, как видно, прочитать этот файл пользователь s335105_new может, но не удалить. Удалим файл от лица пользователя s335105

```
root@v132798:~# su s335105
$ ls -l /studs/lab_reports/
total 4
-rw-rw-r-- 1 s335105 s335105 10 Sep 22 14:48 report.txt
$ rm -rf /studs/lab_reports/report.txt
$ ls -l /studs/lab_reports/
total 0
$
```

Всё получилось.