Университет ИТМО
Факультет программной инженерии и компьютерной техники

Информационная безопасность. Лабораторная работа №1. Учетные записи и группы пользователей Linux.

Группа: P34121
Студенты: Гиниятуллин Арслан Рафаилович
Преподаватель: Маркина Татьяна Анатольевна
Вариант: 4

2024

Содержание

1 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.

2 Требования к выполнению работы

Примечание: выполнение всех пунктов лабораторной должно сопровождаться скриншотами с результатами работы команд и изменений в конфигурационных файлах.

3 Текст задания

3.1 Основная часть

3.1.1 Этап 1. Конфигурация пользователя *sXXXXXX*

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

3.1.2 Этап 2. Конфигурация пользователя *admin_ sXXXXXX*

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).

3.1.3 Этап 3. Демонстрация различий между конфигурациями

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

3.2 По варианту

Вариант = порядковый номер в журнале % кол-во вариантов = 4 % 11 = **4**

3.2.1 Конфигурация группы

Убрать возможность создания группы по умолчанию для новых пользователей без группы.

3.3 Дополнительная часть

3.3.1

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.

3.3.2

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

3.3.3

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.

4 Этапы выполнения работы

4.1 Основная часть

4.1.1 Этап 1. Конфигурация пользователя *sXXXXXX*

Для создания пользователя воспользуемся командой *useradd*.
Далее создадим группу *studs* с помощью команды *groupadd*.
Для добавления пользователя в группу выполним следующее *sudo usermod -a -G studs s335089*

```
sudo useradd s335089;
sudo groupadd -f studs;
sudo usermod -aG studs s335089
```

-a, –append – добавить пользователя в одну или несколько дополнительных групп. Опция будет работать только вместе с опцией -G.

-G, –groups – указать список дополнительных групп, в которые должен входить пользователь. Между собой группы разделяются запятой. Если пользователь входит в дополнительную группу, которая не была указана в списке, то он будет из нее удалён. Но при использовании опции *-a* можно добавлять новые дополнительные группы, не удаляя старые.

Проверим, что изменения конфигурации применились.

```
cut -d : -f 1 /etc/passwd | grep s335089;
```

```
arslan-gin@ubuntu-vm:~/IS/unix1$ cut -d : -f 1 /etc/passwd | grep s335089
s335089
```

```
sudo cat /etc/group | grep studs;
```

```
arslan-gin@ubuntu-vm:~/IS/unix1$ sudo cat /etc/group | grep studs;
studs:x:1005:s335089
```

4.1.2 Этап 2. Конфигурация пользователя *admin_sXXXXXX*

Провернем аналогичные действия по созданию пользователя. Далее расмотрим 3 способа выдачи пользователю *root* прав.

```
sudo useradd admin_s335089;
```

```
sudo usermod -aG sudo admin_s335089; #1
```

```
sudo nano /etc/passwd; #2
```

```
postgres:x:117:124:PostgreSQL administrator,,,:/var/lib/po
s335089:x:1004:1004::/home/s335089:/bin/sh
admin_s335089:x:0:0::/home/admin_s335089:/bin/sh


^G Help        ^O Write Out   ^W Where Is    ^K Cut
^X Exit        ^R Read File   ^\ Replace     ^U Paste
```

```
sudo visudo; #3

# User privilige specification
root    ALL=(ALL:ALL) ALL

admin_s335089 ALL=(ALL:ALL) ALL
```

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

admin_s335089 ALL=(ALL:ALL) ALL
```

Проверим права пользователя

```
groups admin_s335089;
```

```
arslan-gin@ubuntu-vm:~/IS/unix1$ groups admin_s335089;
admin_s335089 : root sudo
```

4.1.3 Этап 3. Демонстрация различий между конфигурациями

1. Управление пакетами:
- *admin_s335089* может использовать *sudo apt install <package>* для установки пакетов.

```
arslan-gin@ubuntu-vm:~/IS/unix1$ sudo su admin_s335089;
# whoami
root
# sudo apt-get install python3;
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  dh-elpa-helper emacsen-common libjsoncpp25 liblldb-17 librhash0 wmdocker
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libpython3-dev libpython3-stdlib python3-dev python3-minimal python3-venv
Suggested packages:
  python3-doc
The following packages will be upgraded:
  libpython3-dev libpython3-stdlib python3 python3-dev python3-minimal python3-venv
6 upgraded, 0 newly installed, 0 to remove and 62 not upgraded.
Need to get 87.9 kB of archives.
```

- *s335089* не сможет установить пакеты через apt без повышения привилегий.

```
arslan-gin@ubuntu-vm:~/IS/unix1$ sudo su s335089
$ apt^C
$ apt-get install python3
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?
$
```

2. Доступ к защищённым файлам:
- *admin_s335089* может просматривать и изменять файлы, на которые у обычного пользователя нет прав доступа, используя sudo.

```
arslan-gin@ubuntu-vm:~/IS/unix1$ sudo su admin_s335089;
# cat root
Hello, Wolrd!
# exit
```

- *s335089* ограничен в доступе к системным и конфиденциальным файлам.

```
arslan-gin@ubuntu-vm:~/IS/unix1$ sudo su s335089;
$ cat root
cat: root: Permission denied
$
```

3. Управление пользователями:
- *admin_s335089* может создавать и удалять пользователей и группы через sudo useradd, sudo userdel.

```
arslan-gin@ubuntu-vm:~/IS/unix1$ sudo su admin_s335089;
# useradd admin_s335089_2;
# groups
root sudo
# groups admin_s335089_2;
admin_s335089_2 : admin_s335089_2
# userd: not found35089_2;
# g^CA^[[A
# ^C5:
# groups admin_s335089_2;
groups: ‘admin_s335089_2’: no such user
#
```

- *s335089* не имеет таких прав.

```
arslan-gin@ubuntu-vm:~/IS/unix1$ sudo su s335089;
$ useradd s335089_2;
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
$
```

4. Редактирование системных файлов:
   - *admin_ s335089* может использовать *sudo nano /etc/passwd* для редактирования.

```
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
uuidd:x:108:114::/run/uuidd:/usr/sbin/nologin
"/etc/passwd" 43L, 2397B                                    1,1           Top
```

   - *s335089* не сможет редактировать системные файлы, такие как */etc/passwd*, без соответствующих прав.

```
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
uuidd:x:108:114::/run/uuidd:/usr/sbin/nologin
"/etc/passwd" [readonly] 43L, 2397B                         11,1          Top
```

5. Изменение сетевых настроек:
   - *admin_ s335089* может изменять и просматривать iptable.

```
arslan-gin@ubuntu-vm:~/IS/unix1$ sudo su admin_s335089;
# iptables -L | grep 'ipv4
> ';
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
LIBVIRT_INP  all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DOCKER-USER  all  --  anywhere             anywhere
DOCKER-ISOLATION-STAGE-1  all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
```

   - *s355089* не может изменять системные сетевые настройки.

```
arslan-gin@ubuntu-vm:~/IS/unix1$ sudo su s335089;
$ iptables -L
iptables v1.8.7 (nf_tables): Could not fetch rule set generation id: Permission denied (you must be root)

$
```

4.2 По варианту

4.2.1 Конфигурация группы

Необходимо убрать возможность создания группы по умолчанию для новых пользователей без группы.
Для этого изменим содержимое конфигурационного файла */etc/login.defs* , в нем настройки добавления новых пользователей в систему.
И изменим в строчке $USERGROUPS_ENAByes, nono.$

```
sudo nano /etc/login.defs
#
```

```
# Enable setting of the umask group bits to be the same as owner bits
# (examples: 022 -> 002, 077 -> 007) for non-root users, if the uid is
# the same as gid, and username is the same as the primary group name.
#
# If set to yes, userdel will remove the user's group if it contains no
# more members, and useradd will create by default a group with the name
# of the user.
#
USERGROUPS_ENAB no
```

```
#USERDEL_CMD    /usr/sbin/userdel_local

#
# Enable setting of the umask group bits to be the same as owner bits
# (examples: 022 -> 002, 077 -> 007) for non-root users, if the uid is
# the same as gid, and username is the same as the primary group name.
#
# If set to yes, userdel will remove the user's group if it contains no
# more members, and useradd will create by default a group with the name
# of the user.
#
USERGROUPS_ENAB no

#
# Instead of the real user shell, the program specified by this parameter

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify
```

```
arslan-gin@ubuntu-vm:~/IS/unix1$ sudo useradd admin_s335089_2;
arslan-gin@ubuntu-vm:~/IS/unix1$ groups admin_s335089_2;
admin_s335089_2 : users
arslan-gin@ubuntu-vm:~/IS/unix1$
```

4.3 Дополнительная часть

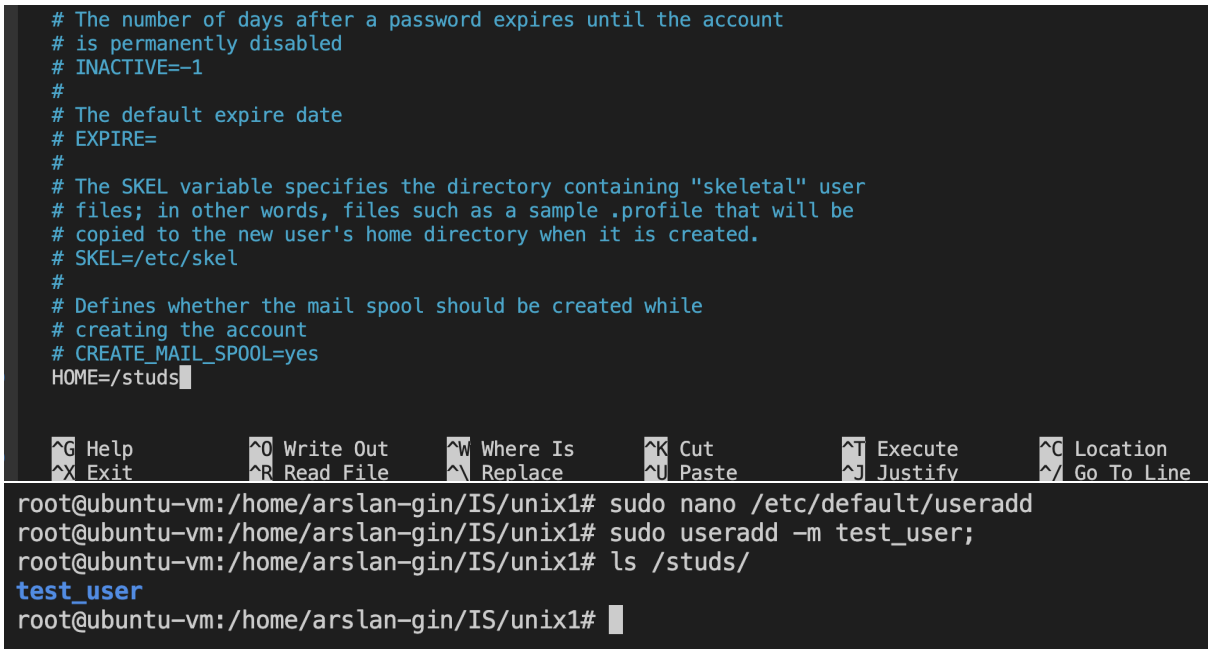
4.3.1 Этап 1. Настройка группы studs.

```
root@ubuntu-vm:/home/arslan-gin/IS/unix1# mkdir /studs
root@ubuntu-vm:/home/arslan-gin/IS/unix1# chown :studs /studs
root@ubuntu-vm:/home/arslan-gin/IS/unix1# sudo chmod 770 /studs
root@ubuntu-vm:/home/arslan-gin/IS/unix1# su s335089;
$ ls studs
ls: cannot access 'studs': No such file or directory
$ ls /studs;
$ cd /studs;
$ exit
root@ubuntu-vm:/home/arslan-gin/IS/unix1# groups s335089;
s335089 : s335089 studs
root@ubuntu-vm:/home/arslan-gin/IS/unix1# su admin_s335089;
$ ls /studs;
ls: cannot open directory '/studs': Permission denied
$ cd /studs
sh: 2: cd: can't cd to /studs
$ exit
```

4.3.2 Этап 2. Изменения конфигурации.

Добавим в конфигурационный файл */etc/default/useradd* строчку

```
# The default home directory
HOME=/studs
```



4.3.3 Этап 3. Настройка прав каталога *lab_ reports*

5 Контрольные вопросы

1. Перечислите параметры структуры записей в файлах */etc/passwd*, */etc/group* и /etc/shadow? За что отвечает каждое поле записи?
2. Какую команду следует использовать для безопасного редактирования файлов конфигурации?
3. Как UID влияет на приоритет разрешений в операционной системе?
4. Чем отличаются команды *sudo* и *su*?

Список литературы

[1] Механизмы безопасности в Linux [Электронный ресурс] / Habr. URL: https://habr.com/ru/articles/92239/

[2] Разбор файла /etc/shadow [Электронный ресурс] / itsecforu. URL: https://clck.ru/36d6Bp

[3] etc/shadow and Creating yescrypt, MD5, SHA-256, and SHA-512 Password Hashes [Электронный ресурс] / baeldung. URL: https://www.baeldung.com/linux/shadow-passwords

[4] Редактирование файла Sudoers [Электронный ресурс] / digitalocean. URL: https://www.digitalocean.com/community/tutorials/how-to-edit-the-sudoers-file-ru

[5] Разграничение прав пользователей в Ubuntu [Электронный ресурс] / baeldung. URL: https://www.baeldung.com/linux/shadow-passwords

[6] Права в Linux (chown, chmod, SUID, GUID, sticky bit, ACL, umask) [Электронный ресурс] / Habr. URL: https://habr.com/ru/articles/469667/