UNIX

Лабораторная работа №1

Учетные записи и группы пользователей Linux

ФИО студента: Готовко Алексей Владимирович
Вариант: 3
Учебная группа: P34101

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.

Выполнение работы

Пункт 1

Задание:

Создайте пользователя `sXXXXXX` (где `XXXXXX` – ваш номер ИСУ). Создайте группу пользователей `studs`, добавьте пользователя в эту группу.

```
xgodness@xgodness-pc:~$ sudo useradd s335151
xgodness@xgodness-pc:~$ sudo groupadd studs
xgodness@xgodness-pc:~$ sudo usermod -aG studs s335151
xgodness@xgodness-pc:~$ groups s335151
s335151 : s335151 studs
```

Ключи `-aG` в команде `usermod` добвляют пользователя в указанную группу, при этом не удаляя его из групп, в которых он уже состоит.

Пункт 2

Задание:

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).

```
xgodness@xgodness-pc:~$ sudo useradd admin_s335151
```

Способ 1: добавление в группу `root` с помощью команды `usermod`

```
xgodness@xgodness-pc:~$ sudo usermod -aG root admin_s335151
xgodness@xgodness-pc:~$ groups admin_s335151
admin_s335151 : admin_s335151 root
```

Способ 2: изменение файла `/etc/passwd`

Файл `/etc/passwd` хранит информацию о пользователях в системе, включая `UID` (user ID) и `GUI` (group ID). `UID` и `GUI`, равные 0, соответствуют пользователю `root` и группе `root` соответственно. Выставим пользователю `admin_s335151` значения `UID=0` и `GID=0`.

```
xgodness@xgodness-pc:~$ sudo vim /etc/passwd
<...>
admin_s335151:x:0:0::/home/admin_s335151:/bin/sh
```

Способ 3: изменение файла `/etc/sudoers`

Файл `/etc/sudoers` – это файл конфигурации, используемый командой `sudo`. Добавление записи о пользователе в этот файл позволит пользователю выполнять команды от имени других пользователей (в т.ч. от имени `root`).

```
xgodness@xgodness-pc:~$ sudo visudo
<...>
# Allow members of group sudo to execute any command
%sudo        ALL=(ALL:ALL) ALL
admin_s335151        ALL=(ALL:ALL) ALL
```

Последняя строчка означает, что пользователю `admin_s335151` выданы привелегии `root`, позволяющие выполнять любую команду от имени любого пользователя на любом хосте.

Пункт 3

Задание:

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

Сначала установим пароли новых пользователей.

```
xgodness@xgodness-pc:~$ sudo passwd admin_s335151
New password:
Retype new password:
passwd: password updated successfully
```

```
xgodness@xgodness-pc:~$ sudo passwd s335151
New password:
Retype new password:
passwd: password updated successfully
```

Отличие 1: доступ к директории `/root`

```
xgodness@xgodness-pc:~$ su s335151
Password:
$ cd /root
sh: 1: cd: can't cd to /root
$
xgodness@xgodness-pc:~$ su admin_s335151
Password:
# cd /root
# pwd
/root
```

Отличие 2: доступ к файлу `/etc/shadow`

```
xgodness@xgodness-pc:~$ su s335151
Password:
$ cat /etc/shadow
cat: /etc/shadow: Permission denied
$
xgodness@xgodness-pc:~$ su admin_s335151
Password:
# cat /etc/shadow | head -n 1
root:!:19487:0:99999:7:::
#
```

Отличие 3: возможность создания новых пользователей

```
xgodness@xgodness-pc:~$ su s335151
Password:
$ useradd test_s335151
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
$
xgodness@xgodness-pc:~$ su admin_s335151
Password:
# useradd test_s335151
# id test_s335151
uid=1002(test_s335151) gid=1004(test_s335151) groups=1004(test_s335151)
#
```

Отличие 4: доступ к диагностическим логам ядра

```
xgodness@xgodness-pc:~$ su s335151
Password:
$ dmesg
dmesg: read kernel buffer failed: Operation not permitted
$
xgodness@xgodness-pc:~$ su admin_s335151
Password:
# dmesg | head -n 1
[    0.000000] Linux version 6.8.0-40-generic (buildd@lcy02-amd64-078) (x86_64-linux-gnu-gcc-12
(Ubuntu 12.3.0-1ubuntu1~22.04) 12.3.0, GNU ld (GNU Binutils for Ubuntu) 2.38) #40~22.04.3-Ubuntu
SMP PREEMPT_DYNAMIC Tue Jul 30 17:30:19 UTC 2 (Ubuntu 6.8.0-40.40~22.04.3-generic 6.8.12)
#
```

Отличие 5: возможность установки пакетов

```
xgodness@xgodness-pc:~$ su s335151
Password:
$ apt-get install cowsay
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?
$
xgodness@xgodness-pc:~$ su admin_s335151
Password:
# apt-get install cowsay
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
<...>
Unpacking cowsay (3.03+dfsg2-8) ...
Setting up cowsay (3.03+dfsg2-8) ...
Processing triggers for man-db (2.10.2-1) ...
# cowsay Don\'t be an infosec racist! Don\'t say \'Regular phishing E-mail\',
say \'Sophisticated social engineering attack\'.
 ----------------------------------------
/ Don't be an infosec racist! Don't say \
| 'Regular phishing E-mail', say        |
| 'Sophisticated social engineering     |
\ attack'.                              /
 ----------------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
#
```

Пункт 4

Задание:
Изменить способ шифрования пароля пользователя `sXXXXXX` на `SHA512`.

Информация о шифровании паролей содержится в файле `/etc/shadow`. В поле с зашифрованным паролем, которое находится после первого двоеточия в каждой записи, первые символы обозначают способ шифрования:

- `$1$` – `MD5`;
- `$2a$` – `blowfish`;
- `$5$` – `SHA-256`;
- `$6$` – `SHA-512`;
- `$y$` (или `$7$`) – `yescrypt`;
- остальные значения – `DES`.

По умолчанию используется `yescrypt`.

```
xgodness@xgodness-pc:~$ sudo cat /etc/shadow | grep s335151 | head -n 1
s335151:$y$j9T[...]f4:19984:0:99999:7:::
```

Воспользуемся командой `chpasswd` с ключом `-c SHA512`.

```
xgodness@xgodness-pc:~$ sudo chpasswd -c SHA512
s335151:newpass
xgodness@xgodness-pc:~$ sudo cat /etc/shadow | grep s335151 | head -n 1
s335151:$6$G9g[...]X1:19984:0:99999:7:::
```

Дополнительная часть

Пункт 1

Задание:

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.

```
xgodness@xgodness-pc:~$ cat /etc/group | grep studs
studs:x:1002:s335151
xgodness@xgodness-pc:~$ sudo mkdir /studs
xgodness@xgodness-pc:~$ ll / | grep studs
drwxr-xr-x   2 root root  4096 Sep 18 16:22 studs/
xgodness@xgodness-pc:~$ sudo chown :studs /studs/
xgodness@xgodness-pc:~$ sudo chmod 770 /studs/
xgodness@xgodness-pc:~$ ll / | grep studs
drwxrwx---   2 root studs  4096 Sep 18 16:22 studs/
xgodness@xgodness-pc:~$ cd /studs
bash: cd: /studs: Permission denied
xgodness@xgodness-pc:~$ su s335151
Password:
$ cd /studs
$ pwd
/studs
```

Пункт 2

Задание:

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

Путь к домашнему каталогу новых пользователей по-умолчанию устанавливается в конфигурационном файле `/etc/default/useradd`.

```
xgodness@xgodness-pc:~$ sudo nvim /etc/default/useradd
<...>
# The default home directory. Same as DHOME for adduser
HOME=/studs
```

Создадим нового пользовател, используя флаг `-m` команды `useradd` для автоматического создания домашнего каталога.

```
xgodness@xgodness-pc:~$ sudo useradd test_s335151 -m -G studs
xgodness@xgodness-pc:~$ sudo passwd test_s335151
New password:
Retype new password:
passwd: password updated successfully
xgodness@xgodness-pc:~$ su test_s335151
Password:
$ cd
$ pwd
/studs/test_s335151
```

Пункт 3

Задание:

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.

Установим sticky bit на директорию `/studs/lab_reports`. Если sticky bit установлен, то пользователь может удалить файл, только если он является пользователем-владельцем файла или каталога, в котором содержится файл. Устанавливается sticky bit флагом `+t` или единицей перед численным значением устанавливаемых прав (например, `1770`) команды `chmod`.

```
xgodness@xgodness-pc:~$ sudo mkdir /studs/lab_reports
xgodness@xgodness-pc:~$ sudo chown :studs /studs/lab_reports
xgodness@xgodness-pc:~$ sudo chmod 1770 /studs/lab_reports
xgodness@xgodness-pc:~$ sudo ls -ld /studs/lab_reports
drwxrwx--T 2 root studs 4096 Sep 18 16:47 /studs/lab_reports
```

Протестируем права.

```
xgodness@xgodness-pc:~$ su s335151
Password:
$ touch /studs/lab_reports/testfile
$ ls -la /studs/lab_reports | grep testfile
-rw-rw-r-- 1 s335151 s335151    0 Sep 18 16:55 testfile
$ su test_s335151
Password:
$ rm /studs/lab_reports/testfile
rm: remove write-protected regular empty file '/studs/lab_reports/testfile'? y
rm: cannot remove '/studs/lab_reports/testfile': Operation not permitted
$ su s335151
Password:
$ rm /studs/lab_reports/testfile
$ ls -la /studs/lab_reports | grep testfile
$
```