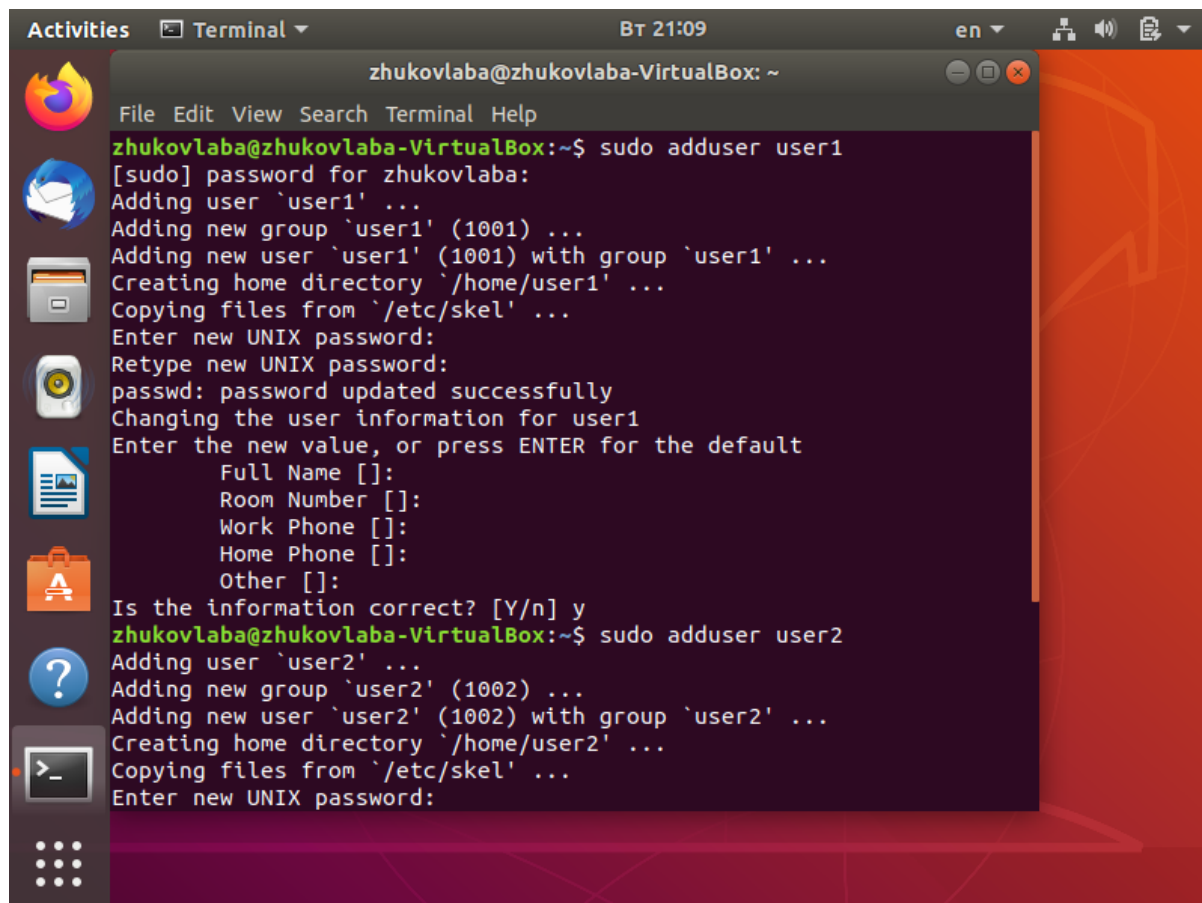


Кекеев Алексей Баатрович СКБ 181.

1. Создание пользователей. Задание паролей. Сброс пароля пользователя.

а. Создать две учетные записи пользователей: user1, user2.

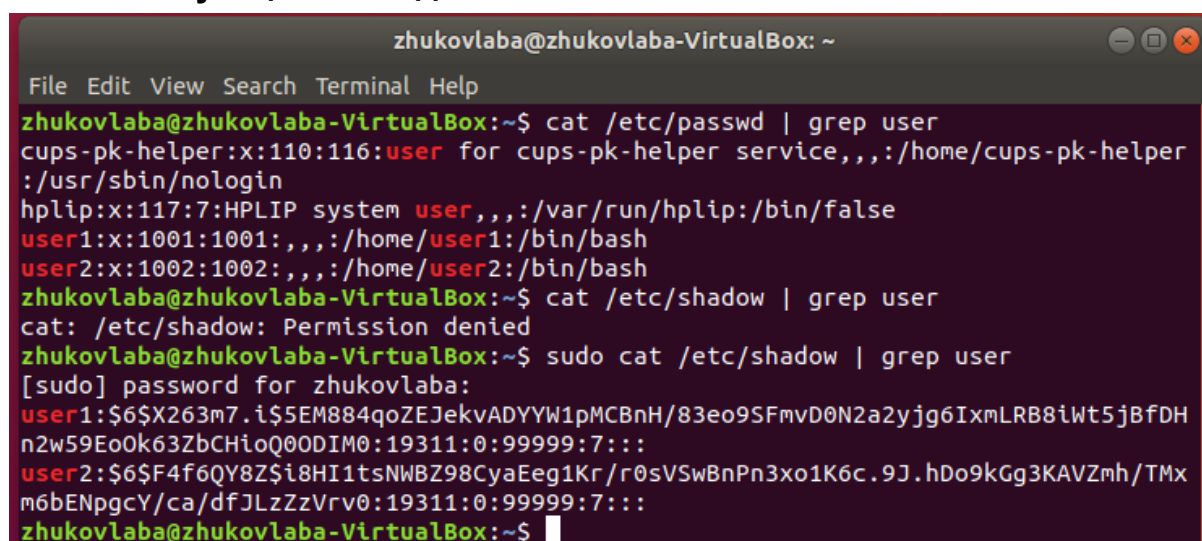


```
zhukovlaba@zhukovlaba-VirtualBox: ~  
File Edit View Search Terminal Help  
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo adduser user1  
[sudo] password for zhukovlaba:  
Adding user `user1' ...  
Adding new group `user1' (1001) ...  
Adding new user `user1' (1001) with group `user1' ...  
Creating home directory `/home/user1' ...  
Copying files from `/etc/skel' ...  
Enter new UNIX password:  
Retype new UNIX password:  
passwd: password updated successfully  
Changing the user information for user1  
Enter the new value, or press ENTER for the default  
Full Name []:  
Room Number []:  
Work Phone []:  
Home Phone []:  
Other []:  
Is the information correct? [Y/n] y  
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo adduser user2  
Adding user `user2' ...  
Adding new group `user2' (1002) ...  
Adding new user `user2' (1002) with group `user2' ...  
Creating home directory `/home/user2' ...  
Copying files from `/etc/skel' ...  
Enter new UNIX password:
```

б. Задать пользователям одинаковые пароли.

Пароли заданы. У обоих пароль:user.

с. Проанализировать файл /etc/shadow и /etc/passwd. Сделать соответствующие выводы.



```
zhukovlaba@zhukovlaba-VirtualBox: ~  
File Edit View Search Terminal Help  
zhukovlaba@zhukovlaba-VirtualBox:~$ cat /etc/passwd | grep user  
cups-pk-helper:x:110:116:user for cups-pk-helper service,,,:/home/cups-pk-helper  
:/usr/sbin/nologin  
hplip:x:117:7:HPLIP system user,,,:/var/run/hplip:/bin/false  
user1:x:1001:1001:,,,:/home/user1:/bin/bash  
user2:x:1002:1002:,,,:/home/user2:/bin/bash  
zhukovlaba@zhukovlaba-VirtualBox:~$ cat /etc/shadow | grep user  
cat: /etc/shadow: Permission denied  
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo cat /etc/shadow | grep user  
[sudo] password for zhukovlaba:  
user1:$6$X263m7.i$EM884qoZEJekvADYYW1pMCBnH/83eo9SFmVD0N2a2yJg6IxmLRB8iWt5jBfDH  
n2w59Eo0k63ZbCHioQ00DIM0:19311:0:99999:7:::  
user2:$6$F4f6QY8Z$i8HI1tsNBWZ98CyaEeg1Kr/r0sVSwBnPN3xo1K6c.9J.hDo9kGg3KAVZmh/TMx  
m6bENpgcY/ca/dfJLzZzVrv0:19311:0:99999:7:::  
zhukovlaba@zhukovlaba-VirtualBox:~$
```

Хеши паролей пользователей различны, однако их пароли одинаковы. Это обуславливается тем фактом, что при хешировании паролей используется специальная соль, которая хранится после id алгоритма хеширования.

d. Из файла /etc/shadow удалить свертку пароля пользователя user1.

Изменения проводил через nano.(sudo nano /etc/shadow)

```
zhukovlaba@zhukovlaba-VirtualBox: ~  
File Edit View Search Terminal Help  
GNU nano 2.9.3 /etc/shadow Modified  
whoopsie:*:18885:0:99999:7:::  
kernoops:*:18885:0:99999:7:::  
saned:*:18885:0:99999:7:::  
avahi:*:18885:0:99999:7:::  
colord:*:18885:0:99999:7:::  
hplip:*:18885:0:99999:7:::  
geoclue:*:18885:0:99999:7:::  
pulse:*:18885:0:99999:7:::  
gnome-initial-setup:*:18885:0:99999:7:::  
gdm:*:18885:0:99999:7:::  
zhukovlaba:$6$T1n7M7M2$K2JZYrneP4HsG39jS3DVM0pA5XwPVBntK6ysfImysRfSdLk3mCzLMYRv0hyKIph0568zQipDGR/UwmmKsvZWN0:19311:0:99999:7:::  
user1:$19311:0:99999:7:::  
user2:$6$F4f6QY8Z$18HI1tsNWBZ98CyaEeg1Kr/r0sVSwBnPN3xo1K6c.9J.hDo9kGg3KAVZmh/TMxm6bENpgcY/ca/dfJLzZzVrv0:19311:0:99999:7:::  
vboxadd!:19311:0:99999:7:::  
  
zhukovlaba@zhukovlaba-VirtualBox: ~  
File Edit View Search Terminal Help  
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo nano /etc/shadow  
[sudo] password for zhukovlaba:  
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo nano /etc/shadow  
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo nano /etc/shadow  
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo cat /etc/shadow | grep user  
user1::19311:0:99999:7:::  
user2:$6$F4f6QY8Z$18HI1tsNWBZ98CyaEeg1Kr/r0sVSwBnPN3xo1K6c.9J.hDo9kGg3KAVZmh/TMxm6bENpgcY/ca/dfJLzZzVrv0:19311:0:99999:7:::  
zhukovlaba@zhukovlaba-VirtualBox:~$
```

e. Проверить, каким образом user1 войдет в систему. Сделать выводы.

```
zhukovlaba@zhukovlaba-VirtualBox: ~  
File Edit View Search Terminal Help  
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo nano /etc/shadow  
[sudo] password for zhukovlaba:  
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo nano /etc/shadow  
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo nano /etc/shadow  
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo cat /etc/shadow | grep user  
user1::19311:0:99999:7:::  
user2:$6$F4f6QY8Z$18HI1tsNWBZ98CyaEeg1Kr/r0sVSwBnPN3xo1K6c.9J.hDo9kGg3KAVZmh/TMxm6bENpgcY/ca/dfJLzZzVrv0:19311:0:99999:7:::  
zhukovlaba@zhukovlaba-VirtualBox:~$ su user1  
Password:  
su: Authentication failure  
zhukovlaba@zhukovlaba-VirtualBox:~$
```

Под user1 нельзя войти. Вывод: в ubuntu 18.04 запрещен вход без пароля.

f. В файле /etc/shadow заменить свертку пароля для пользователя user1 сверткой пароля user2.

```
zhukovlaba@zhukovlaba-VirtualBox: ~
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/shadow Modified
whoopsie:*:18885:0:99999:7:::
kernoops:*:18885:0:99999:7:::
saned:*:18885:0:99999:7:::
avahi:*:18885:0:99999:7:::
colord:*:18885:0:99999:7:::
hplip:*:18885:0:99999:7:::
geoclue:*:18885:0:99999:7:::
pulse:*:18885:0:99999:7:::
gnome-initial-setup:*:18885:0:99999:7:::
gdm:*:18885:0:99999:7:::
zhukovlaba:$6$T1n7M7M2$K2JZYrneP4HsG39j53DVM0pA5XwPVBntK6ysfmysRfSdLk3mCzLMYRv0hyKIph0568zQipDGR/UwwmKsvZWN0:19311:0:99999:7:::
user1:$6$F4f6QY8Z$18HI1tsNWBZ98CyaEeg1Kr/r0sVSwBn3xo1K6c.9J.hDo9kGg3KAVZmh/TMxm6bENpgcY/ca/dfJLzZzVrv0:19311:0:99999:7:::
user2:$6$F4f6QY8Z$18HI1tsNWBZ98CyaEeg1Kr/r0sVSwBn3xo1K6c.9J.hDo9kGg3KAVZmh/TMxm6bENpgcY/ca/dfJLzZzVrv0:19311:0:99999:7:::
vboxadd!:19311:0:99999:7:::

zhukovlaba@zhukovlaba-VirtualBox: ~
File Edit View Search Terminal Help
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo nano /etc/shadow
[sudo] password for zhukovlaba:
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo nano /etc/shadow
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo nano /etc/shadow
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo cat /etc/shadow | grep user
user1::19311:0:99999:7:::
user2:$6$F4f6QY8Z$18HI1tsNWBZ98CyaEeg1Kr/r0sVSwBn3xo1K6c.9J.hDo9kGg3KAVZmh/TMxm6bENpgcY/ca/dfJLzZzVrv0:19311:0:99999:7:::
zhukovlaba@zhukovlaba-VirtualBox:~$ su user1
Password:
su: Authentication failure
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo nano /etc/shadow
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo cat /etc/shadow | grep user
user1:$6$F4f6QY8Z$18HI1tsNWBZ98CyaEeg1Kr/r0sVSwBn3xo1K6c.9J.hDo9kGg3KAVZmh/TMxm6bENpgcY/ca/dfJLzZzVrv0:19311:0:99999:7:::
user2:$6$F4f6QY8Z$18HI1tsNWBZ98CyaEeg1Kr/r0sVSwBn3xo1K6c.9J.hDo9kGg3KAVZmh/TMxm6bENpgcY/ca/dfJLzZzVrv0:19311:0:99999:7:::
zhukovlaba@zhukovlaba-VirtualBox:~$
```

g. Проверить, каким образом user1 войдет в систему. Сделать выводы.

```
user1@zhukovlaba-VirtualBox: /home/zhukovlaba
File Edit View Search Terminal Help
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo nano /etc/shadow
[sudo] password for zhukovlaba:
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo nano /etc/shadow
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo nano /etc/shadow
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo cat /etc/shadow | grep user
user1::19311:0:99999:7:::
user2:$6$F4f6QY8Z$18HI1tsNWBZ98CyaEeg1Kr/r0sVSwBn3xo1K6c.9J.hDo9kGg3KAVZmh/TMxm6bENpgcY/ca/dfJLzZzVrv0:19311:0:99999:7:::
zhukovlaba@zhukovlaba-VirtualBox:~$ su user1
Password:
su: Authentication failure
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo nano /etc/shadow
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo cat /etc/shadow | grep user
user1:$6$F4f6QY8Z$18HI1tsNWBZ98CyaEeg1Kr/r0sVSwBn3xo1K6c.9J.hDo9kGg3KAVZmh/TMxm6bENpgcY/ca/dfJLzZzVrv0:19311:0:99999:7:::
user2:$6$F4f6QY8Z$18HI1tsNWBZ98CyaEeg1Kr/r0sVSwBn3xo1K6c.9J.hDo9kGg3KAVZmh/TMxm6bENpgcY/ca/dfJLzZzVrv0:19311:0:99999:7:::
zhukovlaba@zhukovlaba-VirtualBox:~$ su user1
Password:
user1@zhukovlaba-VirtualBox: /home/zhukovlaba$
```

Через user1 можно снова войти с паролем user. Вывод: пароль пользователя можно вручную изменить в файле /etc/shadow.

2. Создание пользователей вручную.

а. Вручную (без использования команды useradd или adduser) добавить пользователя user3.

б. Пароль пользователя задать вручную (без использования команды passwd).

```
user3@zhukovlaba-VirtualBox:~$ sudo nano /etc/passwd
[sudo] password for zhukovlaba:
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo nano /etc/passwd
[sudo] password for zhukovlaba:
zhukovlaba@zhukovlaba-VirtualBox:~$ su user3
Password:
su: Authentication failure
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo nano /etc/shadow
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo nano /etc/shadow
zhukovlaba@zhukovlaba-VirtualBox:~$ su user3
Password:
groups: cannot find name for group ID 1003
user3@zhukovlaba-VirtualBox:/home/zhukovlaba$ cd ..
user3@zhukovlaba-VirtualBox:/home$ ls
user1 user2 user3 zhukovlaba
user3@zhukovlaba-VirtualBox:/home$ cat /etc/passwd
```

Все изменения проводились внутри /etc/passwd и /etc/shadow.

с. Задать ограничения на пароль вручную, время действия пароля 3 дня (без использования команды passwd).

d. Задать ограничения на пароль вручную, предупреждать о смене пароля за 5 дней (без использования команды passwd), убедиться в наличии предупреждений.

Создавать юзера и менять пароли можно в /etc/shadow и /etc/passwd.

Есть интересные моменты:

- 1) Когда пароль скопирован из старых пользователей(которые были созданы > недели назад).

```
user3@zhukovlaba-VirtualBox: /home/zhukovlaba
File Edit View Search Terminal Help
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo nano /etc/shadow
[sudo] password for zhukovlaba:
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo cat /etc/shadow | grep user
user1:$6$F4f6QY8Z5i8HI1tsNWBZ98CyaEeg1Kr/r0sV5wBnPN3xo1K6c.9J.hDo9kGg3KAVZmh/TMxn6bENpgcY/ca/dfJLzZzVrv0:19311:0:99999:7:::
user2:$6$F4f6QY8Z5i8HI1tsNWBZ98CyaEeg1Kr/r0sV5wBnPN3xo1K6c.9J.hDo9kGg3KAVZmh/TMxn6bENpgcY/ca/dfJLzZzVrv0:19311:0:99999:7:::
user3:$6$F4f6QY8Z5i8HI1tsNWBZ98CyaEeg1Kr/r0sV5wBnPN3xo1K6c.9J.hDo9kGg3KAVZmh/TMxn6bENpgcY/ca/dfJLzZzVrv0:19311:0:3:5:::
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo cat /etc/passwd | grep user
cups-pk-helper:x:110:116:user for cups-pk-helper service,,:/home/cups-pk-helper:/usr/sbin/nologin
hplip:x:117:7:HPLIP system user,,:/var/run/hplip:/bin/false
user1:x:1001:1001:,,:/home/user1:/bin/bash
user2:x:1002:1002:,,:/home/user2:/bin/bash
user3:x:1003:1003:,,:/home/user3:/bin/bash
zhukovlaba@zhukovlaba-VirtualBox:~$ su user3
Password:
You are required to change your password immediately (password aged)
Changing password for user3.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
Password unchanged
Enter new UNIX password:
Retype new UNIX password:
Password unchanged
Enter new UNIX password:
Retype new UNIX password:
Password unchanged
su: Authentication token manipulation error
zhukovlaba@zhukovlaba-VirtualBox:~$ su user3
Password:
You are required to change your password immediately (password aged)
Changing password for user3.
(current) UNIX password:
su: Authentication token manipulation error
zhukovlaba@zhukovlaba-VirtualBox:~$ su user3
Password:
You are required to change your password immediately (password aged)
Changing password for user3.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
Bad: new password is just a wrapped version of the old one
Enter new UNIX password:
Retype new UNIX password:
```

- 2) Когда пароль новый.

```
user3@zhukovlaba-VirtualBox: /home/zhukovlaba$  
File Edit View Search Terminal Help  
zhukovlaba@zhukovlaba-VirtualBox:~$ openssl passwd -6 -salt user user  
$6$user$DF63QDLZmI1r005EbLo5EuFZXkmK0jxALJNp9KAGizMQ1gq5cs0/u.vGkiDe/yJYv9V7foRMx6LyDwSKed9xv0  
  
user1:$6$F4f6QY8Z$18HI1tsNBWZ98CyaEeg1Kr/r0sVSwBnPN3xo1K6c.9J.hDo9kGg3KAVZmh/TMxm6bENpgcY/ca/dfJLzZzVrv0:19311:0:99999:7:::  
user2:$6$F4f6QY8Z$18HI1tsNBWZ98CyaEeg1Kr/r0sVSwBnPN3xo1K6c.9J.hDo9kGg3KAVZmh/TMxm6bENpgcY/ca/dfJLzZzVrv0:19311:0:99999:7:::  
user3:$6$ncA4Vh.ySPd9zZy/8xUjerS11hTtUw4P98uQUEXFGNFRhNuGHxMTQ4N7PNK/j1ir8XAuMc7RFXpcj5lnfhsV2ruN/9kjIS0:19317:0:3:5:::  
vboxadd!:19311:~::~:  
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo vipw  
vipw: /etc/passwd is unchanged  
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo nano /etc/shadow  
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo cat /etc/shadow | grep user  
user1:$6$F4f6QY8Z$18HI1tsNBWZ98CyaEeg1Kr/r0sVSwBnPN3xo1K6c.9J.hDo9kGg3KAVZmh/TMxm6bENpgcY/ca/dfJLzZzVrv0:19311:0:99999:7:::  
user2:$6$F4f6QY8Z$18HI1tsNBWZ98CyaEeg1Kr/r0sVSwBnPN3xo1K6c.9J.hDo9kGg3KAVZmh/TMxm6bENpgcY/ca/dfJLzZzVrv0:19311:0:99999:7:::  
user3:$6$user$DF63QDLZmI1r005EbLo5EuFZXkmK0jxALJNp9KAGizMQ1gq5cs0/u.vGkiDe/yJYv9V7foRMx6LyDwSKed9xv0:19317:0:3:5:::  
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo nano /etc/passwd  
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo cat /etc/passwd | grep user  
cups-pk-helper:x:110:116:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin  
hplip:x:117:7:HPLIP system user,,,:/var/run/hplip:/bin/false  
user1:x:1001:1001:,,,:/home/user1:/bin/bash  
user2:x:1002:1002:,,,:/home/user2:/bin/bash  
user3:x:1003:1003:,,,:/home/user3:/bin/bash  
zhukovlaba@zhukovlaba-VirtualBox:~$ su user3  
Password:  
Warning: your password will expire in 3 days  
groups: cannot find name for group ID 1003  
user3@zhukovlaba-VirtualBox: /home/zhukovlaba$
```

Если пароль старый(или срок истёк), то потребует сменить, иначе - выдаст предупреждение.

3. Добавление пользователей в привилегированную группу (sudoers).

а. Добавить пользователю user3 возможность выполнять команды от имени пользователя user1 с запросом пароля.

```
zhukovlaba@zhukovlaba-VirtualBox: ~  
File Edit View Search Terminal Help  
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo visudo  
[sudo] password for zhukovlaba:  
visudo: /etc/sudoers.tmp unchanged  
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo cat /etc/sudoers | grep user3  
user3 ALL=(user1) ALL  
zhukovlaba@zhukovlaba-VirtualBox:~$
```

б. Убедиться в возможности выполнения команд от имени пользователя user1


```
user3@zhukovlaba-VirtualBox: /home/zhukovlaba
File Edit View Search Terminal Help
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo visudo
[sudo] password for zhukovlaba:
visudo: /etc/sudoers.tmp unchanged
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo cat /etc/sudoers | grep user3
user3 ALL=(user1) ALL
zhukovlaba@zhukovlaba-VirtualBox:~$ su user3
Password:
Warning: your password will expire in 3 days
groups: cannot find name for group ID 1003
user3@zhukovlaba-VirtualBox:/home/zhukovlaba$ sudo -l
[sudo] password for user3:
Matching Defaults entries for user3 on zhukovlaba-VirtualBox:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User user3 may run the following commands on zhukovlaba-VirtualBox:
    (user1) ALL
user3@zhukovlaba-VirtualBox:/home/zhukovlaba$ sudo -u user1 whoami
user1
user3@zhukovlaba-VirtualBox:/home/zhukovlaba$
```

с. Добавить пользователю user3 возможность выполнять команды от имени пользователя user2 без запроса пароля.

```
zhukovlaba@zhukovlaba-VirtualBox: ~
File Edit View Search Terminal Help
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo visudo
[sudo] password for zhukovlaba:
>>> /etc/sudoers: syntax error near line 32 <<<
What now? sudo visudo
Options are:
  (e)dit sudoers file again
  e(x)it without saving changes to sudoers file
  (Q)uit and save changes to sudoers file (DANGER!)

What now? e
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo cat /etc/sudoers | grep user3
user3 ALL=(user1) ALL
user3 ALL=(user2)NOPASSWD: ALL
zhukovlaba@zhukovlaba-VirtualBox:~$
```

```
user3@zhukovlaba-VirtualBox: /home/zhukovlaba
File Edit View Search Terminal Help
(e)dit sudoers file again
e(x)it without saving changes to sudoers file
(Q)uit and save changes to sudoers file (DANGER!)

What now? e
zhukovlaba@zhukovlaba-VirtualBox:~$ sudo cat /etc/sudoers | grep user3
user3 ALL=(user1) ALL
user3 ALL=(user2)NOPASSWD: ALL
zhukovlaba@zhukovlaba-VirtualBox:~$ su user3
Password:
Warning: your password will expire in 3 days
groups: cannot find name for group ID 1003
user3@zhukovlaba-VirtualBox:/home/zhukovlaba$ sudo -l
Matching Defaults entries for user3 on zhukovlaba-VirtualBox:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User user3 may run the following commands on zhukovlaba-VirtualBox:
    (user1) ALL
    (user2) NOPASSWD: ALL
user3@zhukovlaba-VirtualBox:/home/zhukovlaba$ sudo -u user2 whoami
user2
user3@zhukovlaba-VirtualBox:/home/zhukovlaba$
```

4. Разграничение прав пользователей.

a. Создать двух пользователей user1 и user2.

Они созданы в пункте 1.

b. В директории /tmp создать файл file.

c. Настроить его ACL таким образом, чтобы user1 имел полный доступ к файлу, а user2 мог только читать из него.

d. Убедиться, что права настроены правильно, для этого записать от имени user1 данные файл, а затем считать их от имени user2. Затем попробовать записать от имени user2 и убедиться, что это сделать невозможно.

```
user2@zhukovlaba-Vir
File Edit View Search Terminal Help
zhukovlaba@zhukovlaba-VirtualBox:~$ cd /tmp
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ touch file
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ setfacl -m u:user1:rwx file
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ setfacl -m u:user2:r file
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ getfacl file
# file: file
# owner: zhukovlaba
# group: zhukovlaba
user::rw-
user:user1:rwx
user:user2:r--
group::rw-
mask::rwx
other::r--

zhukovlaba@zhukovlaba-VirtualBox:/tmp$ su user1
Password:
user1@zhukovlaba-VirtualBox:/tmp$ echo a>file
user1@zhukovlaba-VirtualBox:/tmp$ su user2
Password:
user2@zhukovlaba-VirtualBox:/tmp$ cat file
a
user2@zhukovlaba-VirtualBox:/tmp$ echo qwerty>file
bash: file: Permission denied
user2@zhukovlaba-VirtualBox:/tmp$
```

5. Рекурсивная настройка прав директорий.

а. В директории /tmp создать следующую структуру файлов:

```
recursive/
└─ subdir
```

```
zhukovlaba@zhukovlaba-VirtualBox:~$ cd /tmp
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ cd recursive
zhukovlaba@zhukovlaba-VirtualBox:/tmp/recursive$ cd subdir
zhukovlaba@zhukovlaba-VirtualBox:/tmp/recursive/subdir$ cd ..
zhukovlaba@zhukovlaba-VirtualBox:/tmp/recursive$ cd ..
```

б. Рекурсивно установить ACL права на всю указанную выше структуру так, чтобы user1 мог писать в каждую поддиректорию.


```

zhukovlaba@zhukovlaba-VirtualBox:/tmp$ setfacl -R -m u:user1:w recursive/
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ getfacl recursive
# file: recursive
# owner: zhukovlaba
# group: zhukovlaba
user::rwx
user:user1:-w-
group::rwx
mask::rwx
other::r-x

zhukovlaba@zhukovlaba-VirtualBox:/tmp$ getfacl recursive/subdir
# file: recursive/subdir
# owner: zhukovlaba
# group: zhukovlaba
user::rwx
user:user1:-w-
group::rwx
mask::rwx
other::r-x

```

с. Убедится в правильности установки прав, создав следующую структуру от имени user1:

```

recursive/
├── file
└── subdir
    └── file

```

```

user1@zhukovlaba-VirtualBox:/tmp$ getfacl recursive/subdir file
getfacl: recursive/subdir: Permission denied
getfacl: file: No such file or directory
user1@zhukovlaba-VirtualBox:/tmp$ getfacl recursive/subdir/file
getfacl: recursive/subdir/file: Permission denied
user1@zhukovlaba-VirtualBox:/tmp$ exit
exit
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ setfacl -R -m u:user1:wx recursive/
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ su user1
Password:
user1@zhukovlaba-VirtualBox:/tmp$ touch recursive/file
user1@zhukovlaba-VirtualBox:/tmp$ touch recursive/subdir/file
user1@zhukovlaba-VirtualBox:/tmp$ █

```

Увы, отобразить это через tree не получилось, так как все время выводит ошибку при открытии директории. Права выставлены обычные.

6. ACL по умолчанию.

- a. В директории /tmp создать поддиректорию test.
- b. Установить на эту директорию ACL по умолчанию таким образом, чтобы user1 мог только читать файлы, размещенные в нем, а user2 мог только записывать в файлы в нём.

```
zhukovlaba@zhukovlaba-V
File Edit View Search Terminal Help
zhukovlaba@zhukovlaba-VirtualBox:~$ cd /tmp
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ mkdir test
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ cd test
zhukovlaba@zhukovlaba-VirtualBox:/tmp/test$ cd ..
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ setfacl -d -m u:user1:r test
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ setfacl -d -m u:user2:w test
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ getfacl test
# file: test
# owner: zhukovlaba
# group: zhukovlaba
user::rwx
group::rwx
other::r-x
default:user::rwx
default:user:user1:r--
default:user:user2:-w-
default:group::rwx
default:mask::rwx
default:other::r-x

zhukovlaba@zhukovlaba-VirtualBox:/tmp$
```

с. Убедиться, что права настроены правильно, для этого создать файл file в этой директории и попробовать записать в него данные сначала от имени user1, убедиться, что это невозможно, а затем от имени user2. Аналогично, попробовать считать данные по очереди за каждого из созданных пользователей.

```
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ cd test
zhukovlaba@zhukovlaba-VirtualBox:/tmp/test$ touch file
zhukovlaba@zhukovlaba-VirtualBox:/tmp/test$ ls
file
zhukovlaba@zhukovlaba-VirtualBox:/tmp/test$ su user1
Password:
user1@zhukovlaba-VirtualBox:/tmp/test$ echo abcd>file
bash: file: Permission denied
user1@zhukovlaba-VirtualBox:/tmp/test$ su user2
Password:
user2@zhukovlaba-VirtualBox:/tmp/test$ echo efghi>file
user2@zhukovlaba-VirtualBox:/tmp/test$ cat file
cat: file: Permission denied
user2@zhukovlaba-VirtualBox:/tmp/test$ su user1
Password:
user1@zhukovlaba-VirtualBox:/tmp/test$ cat file
efghi
user1@zhukovlaba-VirtualBox:/tmp/test$ touch file1
touch: cannot touch 'file1': Permission denied
user1@zhukovlaba-VirtualBox:/tmp/test$ exit
```

d. Создать ещё один файл file2 в tmp. Установить его права в ACL так, чтобы user2 мог из него читать. Убедиться, что user2 имеет возможность читать из file2. Для этого от имени user2 записать в него данные, а затем вывести его содержимое на экран.

```
exit
zhukovlaba@zhukovlaba-VirtualBox:/tmp/test$ touch file1
zhukovlaba@zhukovlaba-VirtualBox:/tmp/test$ ls
file file1
zhukovlaba@zhukovlaba-VirtualBox:/tmp/test$ setfacl -m u:user2:r file1
zhukovlaba@zhukovlaba-VirtualBox:/tmp/test$ su user2
Password:
user2@zhukovlaba-VirtualBox:/tmp/test$ echo sdek>file1
bash: file1: Permission denied
user2@zhukovlaba-VirtualBox:/tmp/test$ cat file1
user2@zhukovlaba-VirtualBox:/tmp/test$
```

7. Эффективная маска.

a. Создать в директории /tmp файл mask и записать в него произвольный текст.

```
zhukovlaba@zhukovlaba-VirtualBox: /t
File Edit View Search Terminal Help
zhukovlaba@zhukovlaba-VirtualBox:~$ cd /tmp
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ echo zhukov>mask
```

b. Модифицировать ACL: дать пользователю user1 право на чтение и запись в mask.

```
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ setfacl -m u:user1:rw mask
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ su user1
Password:
user1@zhukovlaba-VirtualBox:/tmp$ cat mask
zhukov
user1@zhukovlaba-VirtualBox:/tmp$ echo noneklimsanych>mask
user1@zhukovlaba-VirtualBox:/tmp$ cat mask
noneklimsanych
user1@zhukovlaba-VirtualBox:/tmp$
```

c. Установить в ACL этого файла эффективную маску так, чтобы никто не мог записывать в файл.

d. Убедиться в том, что user1 не может ничего записать в mask, но может из него считать.

```
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ setfacl -m m:r mask
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ su user1
Password:
user1@zhukovlaba-VirtualBox:/tmp$ echo koomi2.0>mask
bash: mask: Permission denied
user1@zhukovlaba-VirtualBox:/tmp$ cat mask
noneklimsanych
user1@zhukovlaba-VirtualBox:/tmp$
```

8. Копирование ACL.

- a. Создать в директории /tmp файлы source и dest и записать в них текстовую информацию. Установить этим файлам стандартные UNIX-права 660, чтобы user1 и user2 не имели доступа к файлам.
- b. Настроить ACL правила source так, чтобы user1 мог читать из него, а правила dest так, чтобы из него мог читать user2.
- c. Убедиться, что каждый из пользователей может читать из соответствующего файла.
- d. Скопировать ACL из файла source в файл dest.
- e. Убедиться, что из файла dest может читать только пользователь user1.

```
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ echo zos>source
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ echo zpd>dest
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ chmod 660 source
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ chmod 660 dest
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ setfacl -m u:user1:r source
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ setfacl -m u:user2:r dest
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ su user1
Password:
user1@zhukovlaba-VirtualBox:/tmp$ cat source
zos
user1@zhukovlaba-VirtualBox:/tmp$ su user2
Password:
user2@zhukovlaba-VirtualBox:/tmp$ cat dest
zpd
user2@zhukovlaba-VirtualBox:/tmp$ exit
exit
user1@zhukovlaba-VirtualBox:/tmp$ getfacl source | setfacl --set-file=- dest
setfacl: dest: Operation not permitted
user1@zhukovlaba-VirtualBox:/tmp$ exit
exit
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ getfacl source | setfacl --set-file=- dest
zhukovlaba@zhukovlaba-VirtualBox:/tmp$ su user1
Password:
user1@zhukovlaba-VirtualBox:/tmp$ cat dest
zpd
user1@zhukovlaba-VirtualBox:/tmp$ su user2
Password:
user2@zhukovlaba-VirtualBox:/tmp$ cat dest
cat: dest: Permission denied
user2@zhukovlaba-VirtualBox:/tmp$
```

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Перечислите основные команды для работы с пользователями и группами.

adduser/useradd
deluser/userdel
groups
addgroup/groupadd
sudo
su

passwd

2. Почему нужны два разных файла /etc/passwd и /etc/shadow, почему нельзя использовать один из них?

В файле /etc/passwd хранится общая информация о пользователях.

В файле /etc/shadow хранится информация о паролях пользователей.

Некоторые командам нужна информация о пользователях, например для нахождения UID по именам пользователей. Файл `/etc/passwd` общедоступен и каждый его может прочитать. А критически важная информация уже хранится в `/etc/shadow` и доступ к ней имеет только root.

3. Зачем нужны SUID и SGID и Stickybit?

SUID: Пусть пользователь хочет сменить пароль, тогда ему для этого нужны права для записи в файл `/etc/shadow`. Однако, файл `/etc/shadow` доступен только root. Так, пользователь не смог бы сменить пароль. Но благодаря SUID-биту установленному для команды `passwd`, эта команда запускается от имени root, что позволяет пользователю изменить пароль. Так, при использовании команды `passwd` с этим битом, пользователь временно получает права root.

SGID: похож на SUID — файл будет запущен от имени группы владельца файла. Обычно его используют для директорий, чтобы автоматически устанавливать группу владельца для поддиректорий такой же как у главной директории.

Sticky bit: Например, мы создали общую папку для пользователей. Пользователь имеет право туда писать. Однако, так, он также может удалить абсолютно всё из этой папки. Но, установив sticky бит на эту директорию, пользователь в этой директории сможет удалить только те файлы, владельцем которых он является.

4. Зачем в Linux были введены списки контроля доступа?

Потому что с обычными правами невозможно задать права для нескольких пользователей или групп сразу.

5. Какие базовые утилиты используются для управления ACL?

`getfacl` — предназначена для получения информации об установленных ACL.

`setfacl` — предназначена для установки, модификации и удаления ACL.

6. Зачем нужны ACL по умолчанию?

Для того, чтобы файлы без ACL, содержащиеся в директории, "наследовали" ACL по умолчанию этой директории.

7. Как понять, что для файла установлен ACL?

Вызвать команду `ls -l`, в конце файла будет символ `+`.

8. Чем лучше воспользоваться, когда необходимо разрешить выполнение конкретного исполняемого файла конкретному пользователю ACL или прописать правило в sudoers?

В случае, если выполнение нужно было бы от имени root, я бы воспользовался ACL, так как, удалив файл, удалятся и привилегии. А, если мы удалили этот исполняемый

файл, но sudoers не изменили, то можно создать файл и запустить его. С точки зрения пентеста.

В ином случае, лучше воспользоваться sudoers.