

Лабораторная работа №3

Основы информационной безопасности

Феоктистов Владислав Сергеевич

22 сентября 2022

Российский университет дружбы народов, Москва, Россия

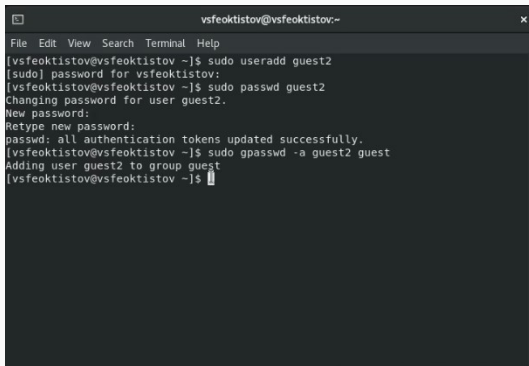
НПМбд-01-19

Целью данной работы является: приобретение практических навыков работы в консоли с правами и атрибутами файлов и каталогов для групп пользователей, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux, проверка необходимых наборов прав для выполнения различных действий над файлами и каталогами для групп пользователей, получение навыков чтения выделенных прав через консоль.

- Создать нового пользователя под именем guest2 с паролем и добавить его в группу guest;
- осуществить вход в систему от двух пользователей на двух различных консолях и получить информацию о них различными способами;
- выполнить регистрацию пользователя в группе;
- проверить и изменить права на существующие файлы и каталоги;
- заполнить таблицы разрешенных действий и минимальных прав для групп пользователей.

Ход выполнения лабораторной работы

С помощью команды `useradd` создаем нового пользователя, с помощью команды `passwd` устанавливаем для него пароль, а с помощью `gpasswd` добавляем его в другую группу.

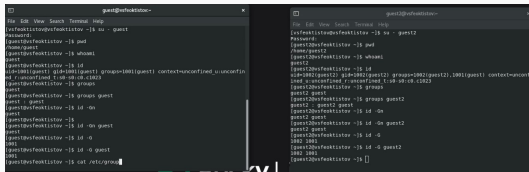
A terminal window titled 'vsfeoktistov@vsfeoktistov:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
[vsfeoktistov@vsfeoktistov ~]$ sudo useradd guest2
[sudo] password for vsfeoktistov:
[vsfeoktistov@vsfeoktistov ~]$ sudo passwd guest2
Changing password for user guest2.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[vsfeoktistov@vsfeoktistov ~]$ sudo gpasswd -a guest2 guest
Adding user guest2 to group guest
[vsfeoktistov@vsfeoktistov ~]$
```

Figure 1: Создание нового пользователя

Вход в систему и получение информации о пользователях

Осуществляем вход в систему от двух пользователей на двух разных консолях: *guest* на первой консоли и *guest2* на второй (*su - [имя пользователя]*). Получаем информацию о них: *pwd*, *id*, *groups*.



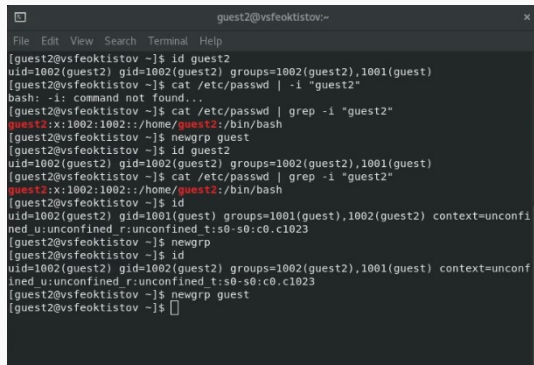
```
guest@vxfaultstor:~$ su - guest
[vsftoklist@vxfaultstor ~]$ pwd
/home/guest
[vsftoklist@vxfaultstor ~]$ whoami
guest
[vsftoklist@vxfaultstor ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[vsftoklist@vxfaultstor ~]$ groups
guest
[vsftoklist@vxfaultstor ~]$ groups guest
guest : guest
[vsftoklist@vxfaultstor ~]$ id -on
guest
[vsftoklist@vxfaultstor ~]$ id -on guest
guest
[vsftoklist@vxfaultstor ~]$ id -o
0001
[vsftoklist@vxfaultstor ~]$ id -o guest
0001
[vsftoklist@vxfaultstor ~]$ cat /etc/group
```

```
guest2@vxfaultstor:~$ su - guest2
[vsftoklist@vxfaultstor ~]$ su - guest2
Password:
[vsftoklist@vxfaultstor ~]$ pwd
/home/guest2
[vsftoklist@vxfaultstor ~]$ whoami
guest2
[vsftoklist@vxfaultstor ~]$ id
uid=1002(guest2) gid=1002(guest2) groups=1002(guest2),1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[vsftoklist@vxfaultstor ~]$ groups
guest2 guest
[vsftoklist@vxfaultstor ~]$ groups guest2
guest2 : guest2 guest
[vsftoklist@vxfaultstor ~]$ id -on
guest2 guest
[vsftoklist@vxfaultstor ~]$ id -on guest2
guest2 guest
[vsftoklist@vxfaultstor ~]$ id -o
0002 0001
[vsftoklist@vxfaultstor ~]$ id -o guest2
0002 0001
[vsftoklist@vxfaultstor ~]$
```

Figure 2: Вход в систему и получение информации о пользователях

Регистрация пользователя в группе

Регистрируем пользователя *guest2* в группе *guest* командой *newgrp*.



```
guest2@vsfeoktistov:~  
File Edit View Search Terminal Help  
[guest2@vsfeoktistov ~]$ id guest2  
uid=1002(guest2) gid=1002(guest2) groups=1002(guest2),1001(guest)  
[guest2@vsfeoktistov ~]$ cat /etc/passwd | -i "guest2"  
bash: -i: command not found...  
[guest2@vsfeoktistov ~]$ cat /etc/passwd | grep -i "guest2"  
guest2:x:1002:1002::/home/guest2:/bin/bash  
[guest2@vsfeoktistov ~]$ newgrp guest  
[guest2@vsfeoktistov ~]$ id guest2  
uid=1002(guest2) gid=1002(guest2) groups=1002(guest2),1001(guest)  
[guest2@vsfeoktistov ~]$ cat /etc/passwd | grep -i "guest2"  
guest2:x:1002:1002::/home/guest2:/bin/bash  
[guest2@vsfeoktistov ~]$ id  
uid=1002(guest2) gid=1001(guest) groups=1001(guest),1002(guest2) context=unconfi  
ned_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest2@vsfeoktistov ~]$ newgrp  
[guest2@vsfeoktistov ~]$ id  
uid=1002(guest2) gid=1002(guest2) groups=1002(guest2),1001(guest) context=unconf  
ined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest2@vsfeoktistov ~]$ newgrp guest  
[guest2@vsfeoktistov ~]$
```

Figure 3: Регистрация пользователя в группе

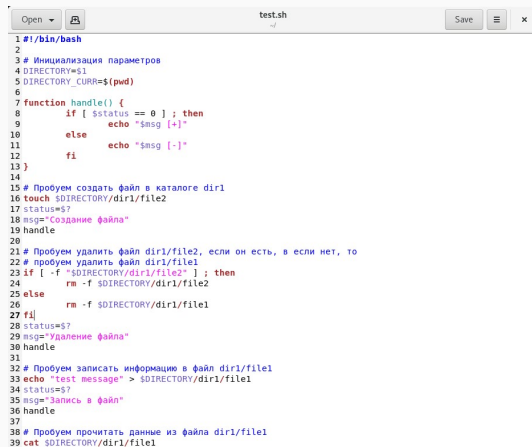
Изменение прав доступа

Изменение прав для файла/каталога осуществляется командой *chmod*. Только root, владелец файла или пользователь с привилегией *sudo* могут изменять права доступа к файлу или каталогу. Разрешения можно указывать с помощью символьного, числового или справочного режимов.

```
guest@vsfeoktistov:~  
File Edit View Search Terminal Help  
[guest@vsfeoktistov ~]$ chmod g+rwX /home/guest  
[guest@vsfeoktistov ~]$ pwd  
/home/guest  
[guest@vsfeoktistov ~]$ cd ../  
[guest@vsfeoktistov home]$ ls -l  
total 8  
drwxrwx---. 16 guest      guest      4096 Sep 21 22:41 guest  
drwx-----. 4 guest2     guest2     112 Sep 21 22:41 guest2  
drwx-----. 19 vsfeoktistov vsfeoktistov 4096 Sep 21 21:28 vsfeoktistov  
[guest@vsfeoktistov home]$ cd ~  
[guest@vsfeoktistov ~]$ ls  
Desktop  Documents  Music      Public      test.sh  
dir1     Downloads  Pictures    Templates    Videos  
[guest@vsfeoktistov ~]$ chmod 000 dir1  
[guest@vsfeoktistov ~]$ ls -l  
total 4  
drwxr-xr-x. 2 guest guest    6 Sep 17 12:13 Desktop  
d-----.. 2 guest guest    19 Sep 17 13:41 dir1  
drwxr-xr-x. 2 guest guest    6 Sep 17 12:13 Documents  
drwxr-xr-x. 2 guest guest    6 Sep 17 12:13 Downloads  
drwxr-xr-x. 2 guest guest    6 Sep 17 12:13 Music  
drwxr-xr-x. 2 guest guest    6 Sep 17 12:13 Pictures  
drwxr-xr-x. 2 guest guest    6 Sep 17 12:13 Public  
drwxr-xr-x. 2 guest guest    6 Sep 17 12:13 Templates  
-rw-rw-r--. 1 guest guest 3103 Sep 17 14:05 test.sh  
drwxr-xr-x. 2 guest guest    6 Sep 17 12:13 Videos  
[guest@vsfeoktistov ~]$
```


Автоматизация процесса проверки

Для заполнения таблицы “Установленные права и разрешенные действия для групп” можно написать bash-скрипты, которые будут создавать и выдавать права каталогу dir1 и файлу file1, а также проверять какие действия над ними можно будет совершать.



```
1 #!/bin/bash
2
3 # Инициализация параметров
4 DIRECTORY=$1
5 DIRECTORY_CURR=$(pwd)
6
7 function handle() {
8     if [ $status == 0 ]; then
9         echo "$msg [+]"
10    else
11        echo "$msg [-]"
12    fi
13 }
14
15 # Пробуем создать файл в каталоге dir1
16 touch $DIRECTORY/dir1/file2
17 status=$?
18 msg="Создание файла"
19 handle
20
21 # Пробуем удалить файл dir1/file2, если он есть, в если нет, то
22 # пробуем удалить файл dir1/file1
23 if [ -f "$DIRECTORY/dir1/file2" ]; then
24     rm -f $DIRECTORY/dir1/file2
25 else
26     rm -f $DIRECTORY/dir1/file1
27 fi
28 status=$?
29 msg="Удаление файла"
30 handle
31
32 # Пробуем записать информацию в файл dir1/file1
33 echo "test message" > $DIRECTORY/dir1/file1
34 status=$?
35 msg="Запись в файл"
36 handle
37
38 # Пробуем прочитать данные из файла dir1/file1
39 cat $DIRECTORY/dir1/file1
```

Разрешенные действия

После перебора всех атрибутов, используя `bash`-скрипт, можно заполнить такую таблицу:

		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Просмотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
Права дирек- тории	Права файла								
d----	----	-	-	-	-	-	-	-	-
(000)	(000)								
d--x-	----	-	-	-	-	+	-	-	-
(010)	(000)								
...
d-rwx-	-rwx-	+	+	+	+	+	+	+	-
(070)	(070)								

Минимальные требования

На основе предыдущей таблицы можно определить минимально необходимые права для выполнения определенных действий над файлами и директориями для групп от имени пользователей входящих в группу.

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d -wx (030)	— (000)
Удаление файла	d -wx (030)	— (000)
Чтение файла	d -x (010)	r- (040)
Запись в файл	d -x (010)	-w- (020)
Переименование файла	d -wx (030)	— (000)
Создание поддиректории	d -wx (030)	— (000)
Удаление поддиректории	d -wx (030)	— (000)

- Приобрел практические навыки работы в консоли с правами и атрибутами файлов и каталогов для групп пользователей;
- закрепил теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux;
- проверил необходимый наборов прав для выполнения различных действий над файлами и каталогами для групп пользователей;
- получил навыки чтения выделенных прав через консоль.