

ЛР №3. Дискреционное разграничение прав в Linux. Два пользователя

Дисциплина: Информационная безопасность

Доборщук Владимир Владимирович, НФИбд-01-18

16 октября 2021

Цель работы

Цель работы

Получение практических навыков работы в консоли с атрибутами файлов для групп пользователей.

Задачи:

- анализ атрибутов директорий/файлов от пользователя из определенной группы;
- укрепление навыков манипуляции учетными записями;
- укрепление навыков взаимодействия с файловой системой.


Выполнение лабораторной работы

Выполнение лабораторной работы

Зайдя в терминал, мы сделали следующие вещи:

- создали учетную запись для `guest` и `guest2`;
- задали пароль для `guest` и `guest2`;
- вошли в систему от лица `guest` и `guest2`;
- определили домашнюю директорию для каждого пользователя;
- определили группы, к которым они принадлежат (команды `groups` и `id`).

Выполнение лабораторной работы

```
1 vvdoborschuk@wxco... 2 guest@wxcore:~ 3 guest2@wxcore:~ +   
[vvdoborschuk@wxcore ~]$ useradd guest  
useradd: Permission denied.  
useradd: cannot lock /etc/passwd; try again later.  
[vvdoborschuk@wxcore ~]$ sudo useradd guest  
[sudo] password for vvdoborschuk:  
[vvdoborschuk@wxcore ~]$ sudo passwd guest  
Changing password for user guest.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[vvdoborschuk@wxcore ~]$ sudo useradd guest2  
[vvdoborschuk@wxcore ~]$ sudo passwd guest2  
Changing password for user guest2.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[vvdoborschuk@wxcore ~]$ sudo gpasswd -a guest2 guest  
Adding user guest2 to group guest  
[vvdoborschuk@wxcore ~]$ pwd  
/home/vvdoborschuk  
[vvdoborschuk@wxcore ~]$ |
```

Выполнение лабораторной работы

```
[guest@wxcore ~]$ pwd
/home/guest
[guest@wxcore ~]$ groups guest
guest : guest
[guest@wxcore ~]$ id -Gn; id -G
guest
1001
```

Рис. 1: Информация о пользователе guest

Выполнение лабораторной работы

```
[guest2@wxcore ~]$ pwd
/home/guest2
[guest2@wxcore ~]$ groups guest2
guest2 : guest2 guest
[guest2@wxcore ~]$ id -Gn; id -G
guest2 guest
1002 1001
[guest2@wxcore ~]$ id -G
1002 1001
```

Рис. 2: Информация о пользователе guest

Выполнение лабораторной работы

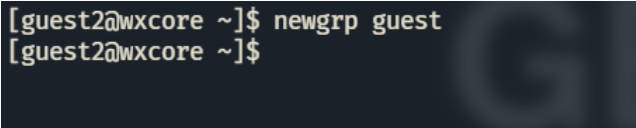
Видим, что пользователь `guest2` у нас также принадлежит к группе `guest`, помимо своей, которая создается при заведении пользователя. Эти же данные мы видим из файла `/etc/passwd`.

Выполнение лабораторной работы

```
[guest@wxcore ~]$ cat /etc/group
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:vdoborschuk
cdrom:x:11:
mail:x:12:
man:x:15:
dialout:x:18:
floppy:x:19:
games:x:20:
tape:x:33:
video:x:39:
ftp:x:50:
lock:x:54:
audio:x:63:
users:x:100:
nobody:x:65534:
utmp:x:22:
utempter:x:35:
dbus:x:81:
input:x:999:
kvm:x:36:
render:x:998:
systemd-journal:x:190:
systemd-coredump:x:997:
systemd-resolve:x:193:
vdoborschuk:x:1000:
tss:x:59:
unbound:x:996:
guest:x:1001:guest2
```

Выполнение лабораторной работы

От имени пользователя `guest2` выполнили регистрацию в группе `guest`.



```
[guest2@wxcore ~]$ newgrp guest  
[guest2@wxcore ~]$
```

Рис. 4: Регистрация `guest2`

Выполнение лабораторной работы

От имени пользователя `guest` мы дали полный набор прав на директорию `/home/guest` для групп с помощью `g+rwX`.

Также наложили ограничения на директорию `/home/guest/dir1` с помощью `chmod`.

```
[guest@wxcore ~]$ chmod g+rwX /home/guest
[guest@wxcore ~]$ ls -l /home/guest
total 0
[guest@wxcore ~]$ ls -l /home/
total 12
drwxrwx--- 2 guest      guest      4096 Oct 16 22:21 guest
drwx----- 2 guest2     guest2     4096 Oct 16 22:21 guest2
drwx----- 3 vvdoborschuk vvdoborschuk 4096 Oct 16 21:26 vvdoborschuk
[guest@wxcore ~]$ mkdir dir1
[guest@wxcore ~]$ chmod 000 dir1
[guest@wxcore ~]$ ls -l
total 4
d----- 2 guest guest 4096 Oct 16 22:30 dir1
[guest@wxcore ~]$
```

Рис. 5: Работа с каталогом `dir1`

Выполнение лабораторной работы

Очевидно, что ни одно действие внутри каталога от лица `guest2` мы сделать не сможем.

Перед заполнением таблицы, мы экспериментально проверили все возможные варианты атрибутов для индивидуального пользователя.

Выполнение лабораторной работы

```
[guest2@wxcore guest]$ cd dir1/  
[guest2@wxcore dir1]$ touch file1  
touch: cannot touch 'file1': Permission denied  
[guest2@wxcore dir1]$ rm file1  
rm: cannot remove 'file1': No such file or directory  
[guest2@wxcore dir1]$ echo "test" > file1  
bash: file1: Permission denied  
[guest2@wxcore dir1]$ ls  
ls: cannot open directory '.': Permission denied  
[guest2@wxcore dir1]$ mv  
mv: missing file operand  
Try 'mv --help' for more information.  
[guest2@wxcore dir1]$
```

Рис. 6: Атрибуты 010

Выполнение лабораторной работы

```
[guest2@wxcore guest]$ touch dir1/file3
touch: cannot touch 'dir1/file3': Permission denied
[guest2@wxcore guest]$ rm dir1/file2
rm: cannot remove 'dir1/file2': Permission denied
[guest2@wxcore guest]$ echo "test" > dir1/file3
bash: dir1/file3: Permission denied
[guest2@wxcore guest]$ ls dir1/file2
ls: cannot access 'dir1/file2': Permission denied
[guest2@wxcore guest]$ cd dir1/
bash: cd: dir1/: Permission denied
[guest2@wxcore guest]$ ls -l dir1/
ls: cannot open directory 'dir1/': Permission denied
[guest2@wxcore guest]$ chmod 777 dir1/*
chmod: cannot access 'dir1/*': Permission denied
[guest2@wxcore guest]$ |
```

Рис. 7: Атрибуты 020

Выполнение лабораторной работы

```
[guest2@wxcore guest]$ echo "test3" > dir1/file3
[guest2@wxcore guest]$ rm dir1/file3
[guest2@wxcore guest]$ cat dir1/file2
test2
[guest2@wxcore guest]$ cd dir1/
[guest2@wxcore dir1]$ ls -l
ls: cannot open directory '.': Permission denied
[guest2@wxcore dir1]$ mv file2 file22
[guest2@wxcore dir1]$ chmod 777 file22
chmod: changing permissions of 'file22': Operation not permitted
[guest2@wxcore dir1]$ mv file22 file2
[guest2@wxcore dir1]$ cd ..
```

Рис. 8: Атрибуты 030

Выполнение лабораторной работы

```
[guest2@wxcore guest]$ echo "test3" > dir1/file3
bash: dir1/file3: Permission denied
[guest2@wxcore guest]$ rm dir1/file2
rm: cannot remove 'dir1/file2': Permission denied
[guest2@wxcore guest]$ cat dir1/file2
cat: dir1/file2: Permission denied
[guest2@wxcore guest]$ cd dir1/
bash: cd: dir1/: Permission denied
[guest2@wxcore guest]$ ls -l dir1/
ls: cannot access 'dir1/file2': Permission denied
ls: cannot access 'dir1/file1': Permission denied
total 0
-????????? ? ? ?          ? file1
-????????? ? ? ?          ? file2
[guest2@wxcore guest]$ mv dir1/file2
mv: missing destination file operand after 'dir1/file2'
Try 'mv --help' for more information.
[guest2@wxcore guest]$ mv dir1/file2 dir1/file3
mv: failed to access 'dir1/file3': Permission denied
[guest2@wxcore guest]$ chmod 777 dir1/file`
> ^C
[guest2@wxcore guest]$ chmod 777 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest2@wxcore guest]$
```

Рис. 9: Атрибуты 040

Выполнение лабораторной работы

```
[guest2@wxcore guest]$ echo "test3" dir1/file3
test3 dir1/file3
[guest2@wxcore guest]$ echo "test3" > dir1/file3
bash: dir1/file3: Permission denied
[guest2@wxcore guest]$ rm dir1/file2
rm: cannot remove 'dir1/file2': Permission denied
[guest2@wxcore guest]$ cat dir1/file2
test2
[guest2@wxcore guest]$ cd dir1/
[guest2@wxcore dir1]$ echo "test3" >> dir1/file2
bash: dir1/file2: No such file or directory
[guest2@wxcore dir1]$ echo "test3" >> file2
[guest2@wxcore dir1]$ ls -l
total 8
-rwxrwxrwx 1 guest guest  5 Oct 16 22:36 file1
-rwxrwxrwx 1 guest guest 12 Oct 16 22:45 file2
[guest2@wxcore dir1]$ mv file1 file3
mv: cannot move 'file1' to 'file3': Permission denied
[guest2@wxcore dir1]$ chmod 600 file1
chmod: changing permissions of 'file1': Operation not permitted
```

Рис. 10: Атрибуты 050

Выполнение лабораторной работы

```
[guest2@wxcore guest]$ echo "test3" > dir1/file3
bash: dir1/file3: Permission denied
[guest2@wxcore guest]$ echo "test3" >> dir1/file2
bash: dir1/file2: Permission denied
[guest2@wxcore guest]$ rm dir1/file2
rm: cannot remove 'dir1/file2': Permission denied
[guest2@wxcore guest]$ cat dir1/file2
cat: dir1/file2: Permission denied
[guest2@wxcore guest]$ cd dir1/
bash: cd: dir1/: Permission denied
[guest2@wxcore guest]$ ls -l dir1/
ls: cannot access 'dir1/file2': Permission denied
ls: cannot access 'dir1/file1': Permission denied
total 0
-?????????? ? ? ?           ? file1
-?????????? ? ? ?           ? file2
[guest2@wxcore guest]$ mv dir1/file2 dir1/file3
mv: failed to access 'dir1/file3': Permission denied
[guest2@wxcore guest]$ chmod 060 dir1/file2
chmod: cannot access 'dir1/file2': Permission denied
[guest2@wxcore guest]$
```

Выполнение лабораторной работы

Таблица 1. Установленные права и разрешённые действия

Права						Смена		Просмотр фай- лов в	Смена атри- бу-
ди-	рек-	Прав	Создан	Удален	Запись	Чтение	ди-	рек-	Переем
то-	то-	фай-	фай-	фай-	в	фай-	то-	то-	фай-
рии	рии	ла	ла	ла	файл	ла	рии	рии	ла
d	---	-----	-	-	-	-	-	-	-
(000)	(000)								
d	---	x-----	-	-	-	+	-	-	+
(010)	(000)								

Выполнение лабораторной работы

Таблица 2. Минимальные права для совершения операция

Операции	Мин. права на директорию	Мин. права на файл
Создание файла	d - - - - wx - - - (030)	- - - - - wx - - - (030)
Удаление файла	d - - - - wx - - - (030)	- - - - - x - - - (010)
Чтение файла	d - - - - wx - - - (030)	- - - - r - - - - (040)
Запись в файл	d - - - - wx - - - (030)	- - - - rw - - - - (050)
Переименование файла	d - - - - wx - - - (030)	- - - - rw - - - - (050)
Создание поддиректории	d - - - rwx - - - (070)	- - - - - x - - - (010)
Удаление поддиректории	d - - - rwx - - - (070)	- - - - - x - - - (010)

Заключение

Мы получили практические навыки работы в консоли с атрибутами файлов для групп пользователей.