

Лабораторная работа №3

Дискреционное разграничение прав в Linux. Два пользователя

Ильин А.В.

23 сентября 2023

Российский университет дружбы народов, Москва, Россия

Информация

- Ильин Андрей Владимирович
- НФИбд-01-20
- 1032201656
- Российский Университет Дружбы Народов
- 1032201656@pfur.ru
- <https://github.com/av-ilin>



Вводная часть

- Приобрести необходимые в современном научном сообществе навыки администрирования систем и информационной безопасности.

- Получение практических навыков работы в консоли с атрибутами файлов для групп пользователей. Закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

1. Создать пользователей `guest` и `guest2`. Добавить пользователя `guest2` в группу `guest`.
2. Уточнить информацию о пользователях.
3. Заполнить таблицы “Установленные права и разрешённые действия для групп” и “Минимальные права для совершения операций от имени пользователей входящих в группу”, меняя атрибуты у директории `dir1` и файла `file1` от имени пользователя `guest` и делая проверку от пользователя `guest2`.

- Rocky Linux
- Git
- VirtualBox

Выполнение работы

Пользователь guest2

```
aviljin login: root
Password:
Last login: Sat Sep 23 19:52:09 on tty1
[root@aviljin ~]# useradd guest2
[root@aviljin ~]# passwd guest2
Changing password for user guest2.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@aviljin ~]# gpasswd -a guest2 guest
Adding user guest2 to group guest
[root@aviljin ~]# cat /etc/passwd | grep guest
guest:x:1001:1001::/home/guest:/bin/bash
guest2:x:1002:1002::/home/guest2:/bin/bash
```

Рис. 1: Пользователь guest2

Изучение пользователя

```
aviljin login: guest2
Password:
Last login: Sat Sep 23 20:01:09 on tty3
[guest2@aviljin ~]$ pwd
/home/guest2
[guest2@aviljin ~]$ whoami
guest2
[guest2@aviljin ~]$ groups guest2
guest2 : guest2 guest
[guest2@aviljin ~]$ id
uid=1002(guest2) gid=1002(guest2) groups=1002(guest2),1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest2@aviljin ~]$ id -G
1002 1001
[guest2@aviljin ~]$ id -Gn
guest2 guest
[guest2@aviljin ~]$
```

Рис. 2: Изучение пользователя guest2

```
[root@aviljin ~]# cat /etc/group | grep guest
guest:x:1001:guest2
guest2:x:1002:
[root@aviljin ~]#
```

Рис. 3: Просмотр `cat /etc/passwd`

```
[quest2@aviljin ~]$ newgrp guest  
[quest2@aviljin ~]$
```

Рис. 4: Регистрация пользователя guest2 в группе guest

```
[quest@aviljin ~]$ chmod g+rwx /home/guest  
[quest@aviljin ~]$ ls -l /home  
total 0  
drwx-----, 2 aviljin aviljin 83 Sep 16 19:31 aviljin  
drwxrwx---, 3 guest guest 95 Sep 23 19:49 guest  
drwx-----, 2 guest2 guest2 83 Sep 23 20:09 guest2  
[quest@aviljin ~]$ ls  
dir1  
[quest@aviljin ~]$ chmod 000 dir1  
[quest@aviljin ~]$ ls -l  
total 0  
d-----, 2 guest guest 19 Sep 16 20:46 dir1  
[quest@aviljin ~]$
```

Рис. 5: Изменения права директории /home/guest и /home/guest/dir1

Эксперименты с правами доступа

```
lguest@aviljin ~]$ chmod 020 dir1
lguest@aviljin ~]$ ls -l
total 0
d----w----, 2 guest guest 6 Sep 23 20:22 dir1
lguest@aviljin ~]$ _
```

tty2

```
lguest2@aviljin ~]$ touch /home/guest/dir1/file1
touch: cannot touch '/home/guest/dir1/file1': Permission denied
lguest2@aviljin ~]$ cd /home/guest/dir1/file1
bash: cd: /home/guest/dir1/file1: Permission denied
lguest2@aviljin ~]$ ls /home/guest/dir1/file1
ls: cannot access '/home/guest/dir1/file1': Permission denied
lguest2@aviljin ~]$
```

tty3

Рис. 6: Эксперименты с правами доступа (1)

```
lguest@aviljin ~]$ chmod 030 dir1
lguest@aviljin ~]$ ls -l
total 0
d----wx---, 2 guest guest 6 Sep 23 20:22 dir1
lguest@aviljin ~]$ _
lguest2@aviljin ~]$ touch /home/guest/dir1/file1
lguest2@aviljin ~]$ chmod 000 /home/guest/dir1/file1
lguest2@aviljin ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
lguest2@aviljin ~]$ cat /home/guest/dir1/file1
cat: /home/guest/dir1/file1: Permission denied
lguest2@aviljin ~]$ cd /home/guest/dir1/
lguest2@aviljin dir1]$ ls
ls: cannot open directory '.': Permission denied
lguest2@aviljin dir1]$ mv file1 file2
lguest2@aviljin dir1]$ ls
ls: cannot open directory '.': Permission denied
lguest2@aviljin dir1]$ chattr +i file1
chattr: Permission denied while reading flags on file1
lguest2@aviljin dir1]$ rm file2
rm: remove write-protected regular empty file 'file2'? y
```

tty2

tty3

Рис. 7: Эксперименты с правами доступа (2)

Установленные права и разрешённые действия для групп

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
000	000	-	-	-	-	-	-	-	-
010	000	-	-	-	-	-	+	-	+
020	000	-	-	-	-	-	-	-	-
030	000	+	+	-	-	+	-	+	-
040	000	-	-	-	-	-	+	-	-
050	000	-	-	-	-	+	+	-	-
060	000	-	-	-	-	-	+	-	-
070	000	+	+	-	-	+	+	+	-
000	010	-	-	-	-	-	-	-	-
010	010	-	-	-	-	+	-	-	+
020	010	-	-	-	-	-	-	-	-
030	010	+	+	-	-	+	-	+	-
040	010	-	-	-	-	-	+	-	-
050	010	-	-	-	-	+	+	-	-
060	010	-	-	-	-	-	+	-	-
070	010	+	+	-	-	+	+	+	-
000	020	-	-	-	-	-	-	-	-

Рис. 8: Фрагмент таблицы «Установленные права и разрешённые действия для групп»11/13

Минимальные права для совершения операций от имени пользователей входящих в группу

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	030	000
Удаление файла	030	000
Чтение файла	010	040
Запись в файл	010	020
Переименование файла	030	000
Создание поддиректории	030	000
Удаление поддиректории	030	000

Рис. 9: Таблица «Минимальные права для совершения операций от имени пользователей входящих в группу»

Результаты

В рамках лабораторной работы был создан новый пользователь `guest2`, который был добавлен в группу пользователя `guest`. На примере данных пользователей мы разобрали базовые команды и права доступа для групп.

Спасибо за внимание!