

Отчёт по лабораторной работе №3

Дискреционное разграничение прав в Linux. Два пользователя

Алламе Ормиз НФИбд-01-21

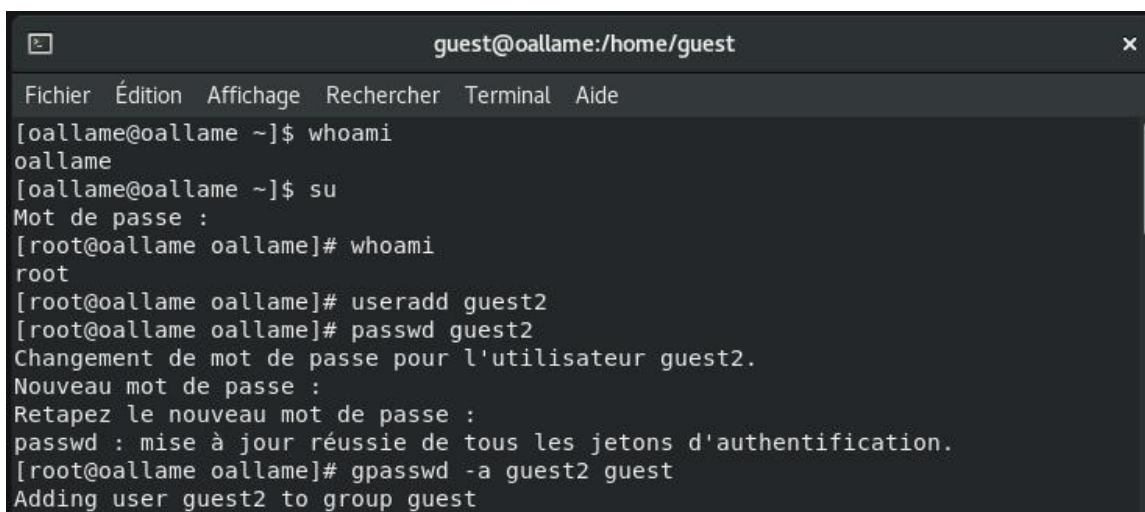
Содержание

1 Цель работы

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

2 Выполнение работы

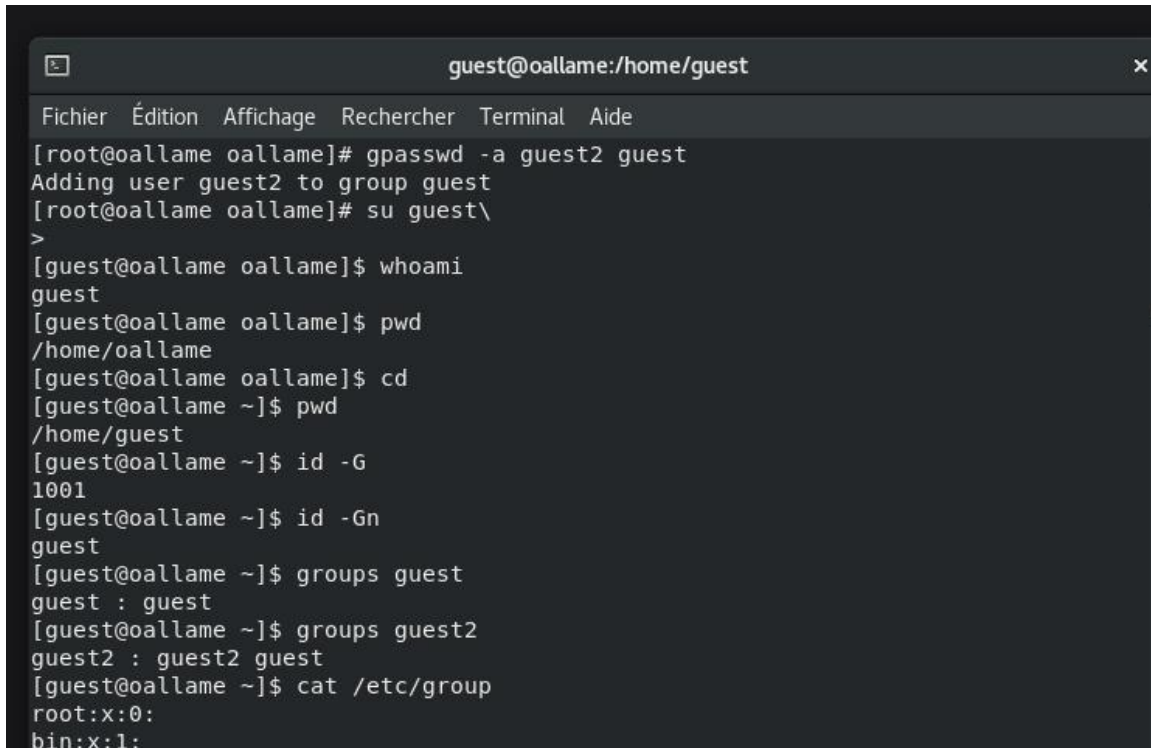
1. В предыдущей работе в установленной операционной системе создали учетную запись пользователя `guest` и задали пароль для пользователя (используя учетную запись администратора) и зашла в эту учетную запись
2. Аналогично создали второго пользователя `guest2` и выполнили вход в эту учетную запись
3. Добавили пользователя `guest2` в группу `guest` используя команду: `Gpasswd -a guest2 guest`



```
guest@oallame:/home/guest
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
[oallame@oallame ~]$ whoami
oallame
[oallame@oallame ~]$ su
Mot de passe :
[root@oallame oallame]# whoami
root
[root@oallame oallame]# useradd guest2
[root@oallame oallame]# passwd guest2
Changement de mot de passe pour l'utilisateur guest2.
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mise à jour réussie de tous les jetons d'authentification.
[root@oallame oallame]# gpasswd -a guest2 guest
Adding user guest2 to group guest
```

Figure 1: Добавление пользователей в группу

4. Выполнили вход в две учетные записи guest guest2 на разных консолях
5. Для обоих пользователей командой Pwd определили директорию, в которой находимся. Сравнили ее с приглашением командой строки.
6. Уточнили имя нашего пользователя, его группу, кто входит в нее и к каким группам принадлежит он сам. Определили командами groups guest и groups guest2, в какие группы входят пользователи guest и guest2. Сравнили выводы команды groups с выводом команд id -Gn и id -G.



```
guest@oallame:/home/guest
Fichier Édition Affichage Rechercher Terminal Aide
[root@oallame oallame]# gpasswd -a guest2 guest
Adding user guest2 to group guest
[root@oallame oallame]# su guest\
>
[guest@oallame oallame]$ whoami
guest
[guest@oallame oallame]$ pwd
/home/oallame
[guest@oallame oallame]$ cd
[guest@oallame ~]$ pwd
/home/guest
[guest@oallame ~]$ id -G
1001
[guest@oallame ~]$ id -Gn
guest
[guest@oallame ~]$ groups guest
guest : guest
[guest@oallame ~]$ groups guest2
guest2 : guest2 guest
[guest@oallame ~]$ cat /etc/group
root:x:0:
bin:x:1:
```

Figure 2: Информация о пользователях

7. Сравнили полученную информацию с содержимым файла /etc/group. Посмотрели файл командой cat /etc/group.
8. От имени пользователя guest2 выполнили регистрацию пользователя guest2 в группе guest командой newgrp guest

```
guest@oallame:/home/guest
Fichier Édition Affichage Rechercher Terminal Aide
guest2 : guest2 guest
[guest@oallame ~]$ 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:oallame
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:
```

```
guest@oallame:/home/guest
Fichier Édition Affichage Rechercher Terminal Aide
sssd:x:981:
libvirt:x:980:
cockpit-ws:x:979:
cockpit-wsinstance:x:978:
flatpak:x:977:
stapusr:x:156:
stapusr:x:157:
stapdev:x:158:
colord:x:976:
rpcuser:x:29:
gdm:x:42:
gnome-initial-setup:x:975:
pesign:x:974:
sshd:x:74:
avahi:x:70:
slocate:x:21:
tcpdump:x:72:
oallame:x:1000:
vboxsf:x:973:
vboxdrmpc:x:972:
guest:x:1001:guest2
guest2:x:1002:
```

Figure 3: Содержимое файла /etc/group и регистрация в группе

9. От имени пользователя guest изменили права директории /home/guest, разрешив все действия для пользователей группы: `chmod g+rwX /home/guest`. И также от имени пользователя guest сняли с директории /home/guest/dir1 все атрибуты командой `chmod 000 dir1` и проверили правильность снятия атрибутов

```
guest@oallame:/home/guest
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
guest:x:1001:guest2
guest2:x:1002:
[guest@oallame ~]$ newgrp guest
[guest@oallame ~]$ cd
[guest@oallame ~]$ chmod g+rwX /home/guest
[guest@oallame ~]$ mkdir dir1
mkdir: impossible de créer le répertoire « dir1 »: File exists
[guest@oallame ~]$ chmod 000 dir1
[guest@oallame ~]$ ls -l
total 0
d----- . 2 guest guest 19 14 sept. 13:14 dir1
[guest@oallame ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@oallame ~]$ cd dir1
bash: cd: dir1: Permission denied
[guest@oallame ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
```

Figure 4: Изменение прав у директории

Меняя атрибуты у директории `dir1` и файла `file1` от имени пользователя `guest` и делая проверку от пользователя `guest2`, заполнили табл. 2, определили опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесли в таблицу знак «+», если не разрешена, знак «-». На основании заполненной таблицы определили те или иные минимально необходимые права для выполнения пользователем `guest2` операций внутри директории `dir1` и заполнили табл. 1.

```

guest@oallame:/home/guest
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
avahi:x:70:
slocate:x:21:
tcpdump:x:72:
oallame:x:1000:
vboxsf:x:973:
vboxdrmipc:x:972:
guest:x:1001:guest2
guest2:x:1002:
[guest@oallame ~]$ newgrp guest
[guest@oallame ~]$ cd
[guest@oallame ~]$ chmod g+rwX /home/guest
[guest@oallame ~]$ mkdir dir1
mkdir: impossible de créer le répertoire « dir1 »: File exists
[guest@oallame ~]$ chmod 000 dir1
[guest@oallame ~]$ ls -l
total 0
d----- . 2 guest guest 19 14 sept. 13:14 dir1
[guest@oallame ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@oallame ~]$ cd dir1
bash: cd: dir1: Permission denied
[guest@oallame ~]$ echo "test" > /home/guest/dir1/file1

```

Figure 5: Заполнение таблицы

Обозначения в таблице:

- (1) Создание файла
- (2) Удаление файла
- (3) Запись в файл
- (4) Чтение файла
- (5) Смена директории
- (6) Просмотр файлов в директории
- (7) Переименование файл
- (8) Смена атрибутов файла

Table 1: Установленные права и разрешённые действия для групп

Права директории	Права файла	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
d----- (000)	----- (000)	-	-	-	-	-	-	-	-
d----x--- (010)	----- (000)	-	-	-	-	+	-	-	+
d----w---- (020)	----- (000)	-	-	-	-	-	-	-	-
d----wx--- (030)	----- (000)	+	+	-	-	+	-	+	+
d---r----- (040)	----- (000)	-	-	-	-	-	+	-	-
d---r-x--- (050)	----- (000)	-	-	-	-	+	+	-	+
d---rw---- (060)	----- (000)	-	-	-	-	-	+	-	-
d---rwx--- (070)	----- (000)	+	+	-	-	+	+	+	+

d----- (000)	-----x--- (010)	-	-	-	-	-	-	-	-
d----x--- (010)	-----x--- (010)	-	-	-	-	+	-	-	+
d----w---- (020)	-----x--- (010)	-	-	-	-	-	-	-	-
d---wx--- (030)	-----x--- (010)	+	+	-	-	+	-	+	+
d---r----- (040)	-----x--- (010)	-	-	-	-	-	+	-	-
d---r-x--- (050)	-----x--- (010)	-	-	-	-	+	+	-	+
d---rw---- (060)	-----x--- (010)	-	-	-	-	-	+	-	-
d---rwx--- (070)	-----x--- (010)	+	+	-	-	+	+	+	+
d----- (000)	-----w---- (020)	-	-	-	-	-	-	-	-
d----x--- (010)	-----w---- (020)	-	-	+	-	+	-	-	+
d----w---- (020)	-----w---- (020)	-	-	-	-	-	-	-	-
d---wx--- (030)	-----w---- (020)	+	+	+	-	+	-	+	+
d---r----- (040)	-----w---- (020)	-	-	-	-	-	+	-	-
d---r-x--- (050)	-----w---- (020)	-	-	+	-	+	+	-	+
d---rw---- (060)	-----w---- (020)	-	-	-	-	-	+	-	-
d---rwx--- (070)	-----w---- (020)	+	+	+	-	+	+	+	+
d----- (000)	-----wx--- (030)	-	-	-	-	-	-	-	-
d----x--- (010)	-----wx--- (030)	-	-	+	-	+	-	-	+
d----w---- (020)	-----wx--- (030)	-	-	-	-	-	-	-	-
d---wx--- (030)	-----wx--- (030)	+	+	+	-	+	-	+	+
d---r----- (040)	-----wx--- (030)	-	-	-	-	-	+	-	-
d---r-x--- (050)	-----wx--- (030)	-	-	+	-	+	+	-	+
d---rw---- (060)	-----wx--- (030)	-	-	-	-	-	+	-	-
d---rwx--- (070)	-----wx--- (030)	+	+	+	-	+	+	+	+
d----- (000)	----r----- (040)	-	-	-	-	-	-	-	-
d----x--- (010)	----r----- (040)	-	-	-	+	+	-	-	+
d----w---- (020)	----r----- (040)	-	-	-	-	-	-	-	-
d---wx--- (030)	----r----- (040)	+	+	-	+	+	-	+	+
d---r----- (040)	----r----- (040)	-	-	-	-	-	+	-	-
d---r-x--- (050)	----r----- (040)	-	-	-	+	+	+	-	+
d---rw---- (060)	----r----- (040)	-	-	-	-	-	+	-	-
d---rwx--- (070)	----r----- (040)	+	+	-	+	+	+	+	+
d----- (000)	----r-x--- (050)	-	-	-	-	-	-	-	-
d----x--- (010)	----r-x--- (050)	-	-	-	+	+	-	-	+
d----w---- (020)	----r-x--- (050)	-	-	-	-	-	-	-	-
d---wx--- (030)	----r-x--- (050)	+	+	-	+	+	-	+	+
d---r----- (040)	----r-x--- (050)	-	-	-	-	-	+	-	-

d---r-x--- (050)	----r-x--- (050)	-	-	-	+	+	+	-	+
d---rw---- (060)	----r-x--- (050)	-	-	-	-	-	+	-	-
d---rwx--- (070)	----r-x--- (050)	+	+	-	+	+	+	+	+
d----- (000)	----rw---- (060)	-	-	-	-	-	-	-	-
d----x--- (010)	----rw---- (060)	-	-	+	+	+	-	-	+
d----w---- (020)	----rw---- (060)	-	-	-	-	-	-	-	-
d----wx--- (030)	----rw---- (060)	+	+	+	+	+	-	+	+
d---r----- (040)	----rw---- (060)	-	-	-	-	-	+	-	-
d---r-x--- (050)	----rw---- (060)	-	-	+	+	+	+	-	+
d---rw---- (060)	----rw---- (060)	-	-	-	-	-	+	-	-
d---rwx--- (070)	----rw---- (060)	+	+	+	+	+	+	+	+
d----- (000)	----rwx--- (070)	-	-	-	-	-	-	-	-
d----x--- (010)	----rwx--- (070)	-	-	+	+	+	-	-	+
d----w---- (020)	----rwx--- (070)	-	-	-	-	-	-	-	-
d----wx--- (030)	----rwx--- (070)	+	+	+	+	+	-	+	+
d---r----- (040)	----rwx--- (070)	-	-	-	-	-	+	-	-
d---r-x--- (050)	----rwx--- (070)	-	-	+	+	+	+	-	+
d---rw---- (060)	----rwx--- (070)	-	-	-	-	-	+	-	-
d---rwx--- (070)	----rwx--- (070)	+	+	+	+	+	+	+	+

На основании заполненной таблицы я определила те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1 и заполнила таблицу 2. Для заполнения последних двух строк опытным путем проверила минимальные права для создания и удаления поддиректории. (рис. 7)

Table 2: Минимальные права для совершения операций

Операция	права на директорию	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)

Сравнивая таблицу 3.1. с такой же таблицей из предыдущей лабораторной работы, могу сказать, что они одинаковы. Единственное различие только в том, что в предыдущий раз я присваивала права владельцу, а в этот раз группе.

3 Выводы

В ходе выполнения работы, мы смогли приобрести практические навыки работы в консоли с атрибутами файлов для групп пользователей.

Список литературы

1. Теория разграничения прав пользователей
2. Разрешения доступа к файлам