

Цель работы

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

Задание

Выполнить задания лабораторной работы и проанализировать полученные результаты.

Теоретическое введение

Дискреционное управление доступом (англ. discretionary access control, DAC) — управление доступом субъектов к объектам на основе списков управления доступом или матрицы доступа. Также используются названия избирательное управление доступом, контролируемое управление доступом и разграничительное управление доступом.

Для каждой пары (субъект — объект) должно быть задано явное и недвусмысленное перечисление допустимых типов доступа, то есть тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу (объекту).

Возможны несколько подходов к построению дискреционного управления доступом:

- Каждый объект системы имеет привязанного к нему субъекта, называемого владельцем. Именно владелец устанавливает права доступа к объекту.
- Система имеет одного выделенного субъекта — суперпользователя, который имеет право устанавливать права владения для всех остальных субъектов системы.
- Субъект с определённым правом доступа может передать это право любому другому субъекту.

Возможны и смешанные варианты построения, когда одновременно в системе присутствуют как владельцы, устанавливающие права доступа к своим объектам, так и суперпользователь, имеющий возможность изменения прав для любого объекта и/или изменения его владельца. Именно такой смешанный вариант реализован в большинстве операционных систем, например Unix.

Избирательное управление доступом является основной реализацией разграничительной политики доступа к ресурсам при обработке конфиденциальных сведений, согласно требованиям к системе защиты информации.

Выполнение лабораторной работы

При выполнении предыдущей лабораторной работы создал учётную запись пользователя `guest` и задал с помощью команды `passwd guest` пароль для пользователя `guest`.

Аналогично создал второго пользователя `guest2`:

```
[vokhudickiyj@vokhudickiyj ~]$ su
Password:
[root@vokhudickiyj vokhudickiyj]# useradd guest2
[root@vokhudickiyj vokhudickiyj]# passwd guest2
Changing password for user guest2.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Добавил пользователя `guest2` в группу `guest`:

```
[root@vokhudickiyj vokhudickiyj]# gpasswd -a guest2 guest
Adding user guest2 to group guest
[root@vokhudickiyj vokhudickiyj]#
```

Осуществил вход в систему от двух пользователей на двух разных консолях: `guest` на первой консоли и `guest2` на второй консоли. Для обоих пользователей командой `pwd` определил директорию, в которой нахожусь. Это домашняя директория, она совпадает с приглашениями командной строки:

```
[root@vokhudickiyj vokhudickiyj]# su - guest
[guest@vokhudickiyj ~]$ pwd
/home/guest
```

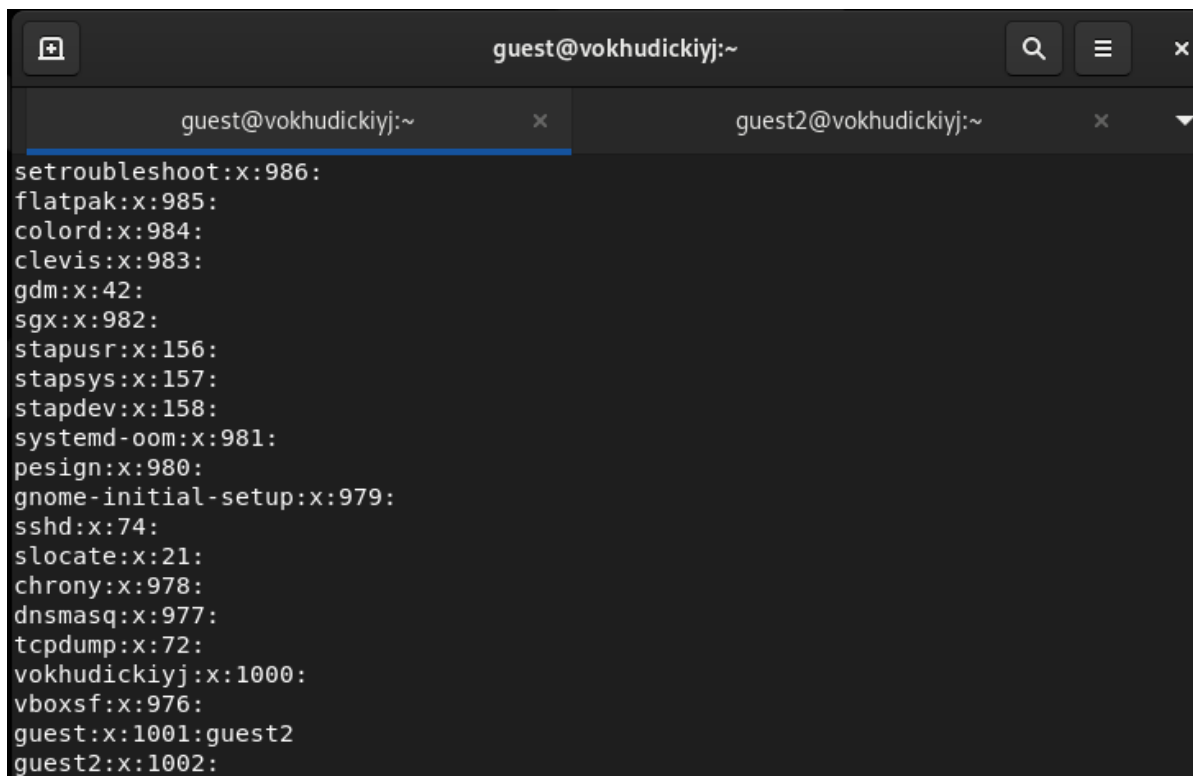
```
[vokhudickiyj@vokhudickiyj ~]$ su - guest2
Password:
[guest2@vokhudickiyj ~]$ pwd
/home/guest2
```

Уточнил имя пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам. Определил командами `groups guest` и `groups guest2`, в какие группы входят пользователи `guest` и `guest2`. Вывод команды `groups` совпадает с выводом команды `id -Gn`. `id -G` показывает gid групп.

```
[guest@vokhudickiyj ~]$ groups guest
guest : guest
[guest@vokhudickiyj ~]$ id -Gn
guest
[guest@vokhudickiyj ~]$ id -G
1001
[guest@vokhudickiyj ~]$ whoami
guest
[guest@vokhudickiyj ~]$
```

```
[guest2@vokhudickiyj ~]$ groups guest2
guest2 : guest2 guest
[guest2@vokhudickiyj ~]$ id -Gn
guest2 guest
[guest2@vokhudickiyj ~]$ id -G
1002 1001
[guest2@vokhudickiyj ~]$ whoami
guest2
[guest2@vokhudickiyj ~]$
```

Просмотрел файл `/etc/group` командой `cat /etc/group`. Найденные значения совпали с полученными в предыдущих пунктах.



```
setroubleshoot:x:986:
flatpak:x:985:
colord:x:984:
clevis:x:983:
gdm:x:42:
sgx:x:982:
stapusr:x:156:
stapsys:x:157:
stapdev:x:158:
systemd-oom:x:981:
pesign:x:980:
gnome-initial-setup:x:979:
sshd:x:74:
slocate:x:21:
chrony:x:978:
dnsmasq:x:977:
tcpdump:x:72:
vokhudickiyj:x:1000:
vboxsf:x:976:
guest:x:1001:guest2
guest2:x:1002:
```

От имени пользователя `guest2` выполнил регистрацию пользователя `guest2` в группе `guest` командой `newgrp guest`

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

От имени пользователя `guest` изменил права директории `/home/guest`, разрешив все действия для пользователей группы:

```
[guest@vokhudickiyj ~]$ chmod g+rwX /home/guest
```

От имени пользователя `guest` снял с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверил правильность снятия атрибутов командой `ls -lb` а также попытавшись создать в директории `dir1` файл `file1` командой `echo "test" > /home/guest/dir1/file1`.

```
[guest@vokhudickiyj ~]$ chmod 000 dir1
[guest@vokhudickiyj ~]$ echo "test" > /home/guest/sir1/file1
-bash: /home/guest/sir1/file1: No such file or directory
[guest@vokhudickiyj ~]$ echo "test" > /home/guest/dir1/file1
-bash: /home/guest/dir1/file1: Permission denied
[guest@vokhudickiyj ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Desktop
d------. 2 guest guest 6 Sep 17 16:09 dir1
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Documents
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Music
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Public
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Templates
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Videos
[guest@vokhudickiyj ~]$
```

Заполнил [таблицу «Установленные права и разрешённые действия»](#). Меняя атрибуты у директории dir1 и файла file1 от имени пользователя guest и делая проверку от пользователя guest2, определил опытным путём, какие операции разрешены, а какие нет.

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
d----- (000)	----- (000)	-	-	-	-	-	-	-	-
d---x--- (010)	----- (000)	-	-	-	-	+	-	-	-
d---W--- (020)	----- (000)	-	-	-	-	-	-	-	-
d---WX--- (030)	----- (000)	+	+	-	-	+	-	+	-
d---f---- (040)	----- (000)	-	-	-	-	-	+	-	-
d---f-x--- (050)	----- (000)	-	-	-	-	+	+	-	-
d---fW--- (060)	----- (000)	-	-	-	-	-	+	-	-
d---fWX--- (070)	----- (000)	+	+	-	-	+	+	+	-
d----- (000)	---x--- (010)	-	-	-	-	-	-	-	-
d---x--- (010)	---x--- (010)	-	-	-	-	+	-	-	-
d---W--- (020)	---x--- (010)	-	-	-	-	-	-	-	-
d---WX--- (030)	---x--- (010)	+	+	-	-	+	-	+	-
d---f---- (040)	---x--- (010)	-	-	-	-	-	+	-	-
d---f-x--- (050)	---x--- (010)	-	-	-	-	+	+	-	-
d---fW--- (060)	---x--- (010)	-	-	-	-	-	+	-	-
d---fWX--- (070)	---x--- (010)	+	+	-	-	+	+	+	-
d----- (000)	---W--- (020)	-	-	-	-	-	-	-	-
d---x--- (010)	---W--- (020)	-	-	+	-	+	-	-	-
d---W--- (020)	---W--- (020)	-	-	-	-	-	-	-	-
d---WX--- (030)	---W--- (020)	+	+	+	-	+	-	+	-
d---f---- (040)	---W--- (020)	-	-	-	-	+	+	-	-
d---f-x--- (050)	---W--- (020)	-	-	+	-	+	+	-	-
d---fW--- (060)	---W--- (020)	-	-	-	-	+	+	-	-
d---fWX--- (070)	---W--- (020)	+	+	+	-	+	+	+	-
d----- (000)	---WX--- (030)	-	-	-	-	-	-	-	-
d---x--- (010)	---WX--- (030)	-	-	+	-	+	-	-	-
d---W--- (020)	---WX--- (030)	-	-	-	-	-	-	-	-
d---WX--- (030)	---WX--- (030)	+	+	+	-	+	-	+	-
d---f---- (040)	---WX--- (030)	-	-	-	-	-	+	-	-
d---f-x--- (050)	---WX--- (030)	-	-	+	-	+	+	-	-
d---fW--- (060)	---WX--- (030)	-	-	-	-	-	+	-	-
d---fWX--- (070)	---WX--- (030)	+	+	+	-	+	+	+	-
d----- (000)	---f---- (040)	-	-	-	-	-	-	-	-
d---x--- (010)	---f---- (040)	-	-	-	+	+	-	-	-
d---W--- (020)	---f---- (040)	-	-	-	-	-	-	-	-
d---WX--- (030)	---f---- (040)	+	+	-	+	+	-	+	-
d---f---- (040)	---f---- (040)	-	-	-	-	-	+	-	-
d---f-x--- (050)	---f---- (040)	-	-	-	+	+	+	-	-
d---fW--- (060)	---f---- (040)	-	-	-	-	-	+	-	-
d---fWX--- (070)	---f---- (040)	+	+	-	+	+	+	+	-
d----- (000)	---f-x--- (050)	-	-	-	-	-	-	-	-
d---x--- (010)	---f-x--- (050)	-	-	-	+	+	-	-	-
d---W--- (020)	---f-x--- (050)	-	-	-	-	-	-	-	-
d---WX--- (030)	---f-x--- (050)	+	+	-	+	+	-	+	-
d---f---- (040)	---f-x--- (050)	-	-	-	+	+	+	-	-
d---f-x--- (050)	---f-x--- (050)	-	-	-	-	+	+	-	-
d---fW--- (060)	---f-x--- (050)	-	-	-	-	-	+	-	-
d---fWX--- (070)	---f-x--- (050)	+	+	-	+	+	+	+	-
d----- (000)	---fW--- (060)	-	-	-	-	-	-	-	-
d---x--- (010)	---fW--- (060)	-	-	+	+	+	-	-	-
d---W--- (020)	---fW--- (060)	-	-	-	-	-	-	-	-
d---WX--- (030)	---fW--- (060)	+	+	+	+	+	-	+	-
d---f---- (040)	---fW--- (060)	-	-	-	-	-	+	-	-
d---f-x--- (050)	---fW--- (060)	-	-	+	+	+	+	-	-
d---fW--- (060)	---fW--- (060)	-	-	-	-	-	+	-	-
d---fWX--- (070)	---fW--- (060)	+	+	+	+	+	+	+	-
d----- (000)	---fWX--- (070)	-	-	-	-	-	-	-	-
d---x--- (010)	---fWX--- (070)	-	-	+	+	+	-	-	-
d---W--- (020)	---fWX--- (070)	-	-	-	-	-	-	-	-
d---WX--- (030)	---fWX--- (070)	+	+	+	+	+	-	+	-
d---f---- (040)	---fWX--- (070)	-	-	-	-	-	+	-	-
d---f-x--- (050)	---fWX--- (070)	-	-	+	+	+	+	-	-
d---fW--- (060)	---fWX--- (070)	-	-	-	-	-	+	-	-
d---fWX--- (070)	---fWX--- (070)	+	+	+	+	+	+	+	-

На основании заполненной таблицы определил те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполнил [таблицу](#).

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)

Выводы

Я получил практические навыки работы в консоли с атрибутами файлов для групп пользователей.

Список литературы

- [Кулябов Д. С., Королькова А. В., Геворкян М. Н. Лабораторная работа №3. Дискреционное разграничение прав в Linux. Два пользователя](#)