Цель работы

Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

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:

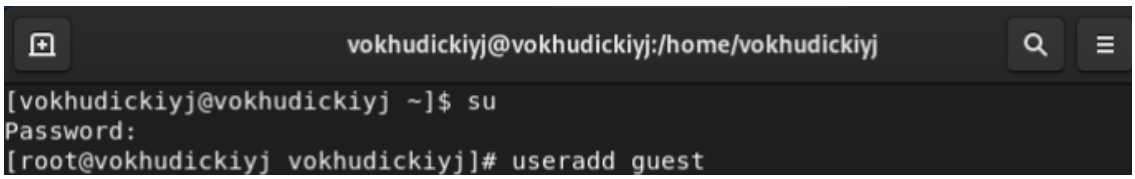
- Каждый объект системы имеет привязанного к нему субъекта, называемого владельцем. Именно владелец устанавливает права доступа к объекту.
- Система имеет одного выделенного субъекта — суперпользователя, который имеет право устанавливать права владения для всех остальных субъектов системы.
- Субъект 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.

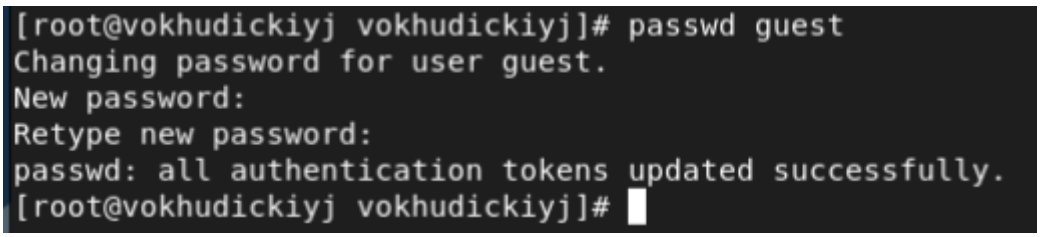
Избирательное управление доступом является основной реализацией разграничительной политики доступа к ресурсам при обработке конфиденциальных сведений, согласно требованиям к системе защиты информации.

Выполнение лабораторной работы

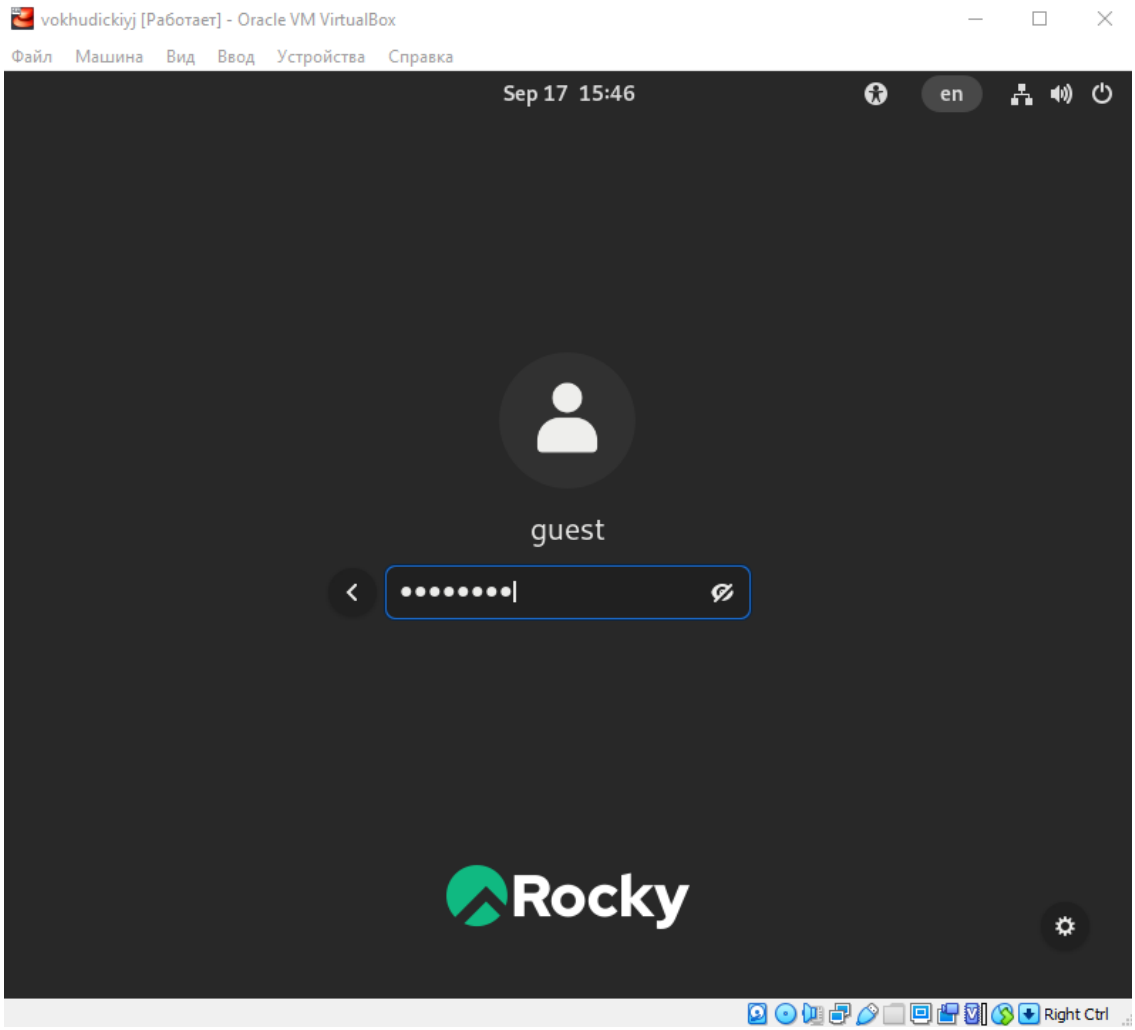
1. В установленной при выполнении предыдущей лабораторной работы операционной системе с помощью команды *useradd guest* создал учётную запись пользователя guest:



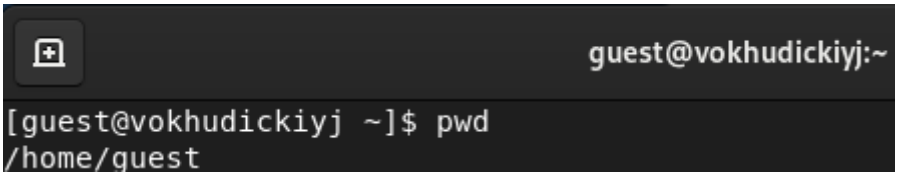
2. Задал с помощью команды *passwd guest* пароль для пользователя guest:



3. Вошёл в систему от имени пользователя guest:



4. Определил директорию, в которой я нахожусь, с помощью команды *pwd*. Она совпадает с приглашением командной строки и является домашней для guest:



5. Уточнил имя пользователя командой *whoami*:

```
[guest@vokhudickiyj ~]$ whoami
guest
[guest@vokhudickiyj ~]$
```

6. Уточнил имя пользователя, его группу, а также группы, куда входит пользователь, командой *id*. Сравнил вывод *id* с выводом команды *groups*, названия групп совпали совпали.

```
[guest@vokhudickiyj ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfin
ed_r:unconfined_t:s0-s0:c0.c1023
[guest@vokhudickiyj ~]$
```

```
[guest@vokhudickiyj ~]$ groups
guest
```

7. Сравнил полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки. Имя пользователя совпало с приглашением командной строки.

8. Просмотрел файл /etc/passwd командой *cat /etc/passwd*. Нашёл в нём свою учётную запись. Определил uid и gid пользователя. Найденные значения совпали с полученными в предыдущих пунктах.

```
guest@vokhudickiyj:~
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
geoclue:x:994:989:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:993:988:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:992:987:User for cockpit-ws instances:/nonexisting:/sbin/no
login
setroubleshoot:x:991:986:SELinux troubleshoot server:/var/lib/setroubleshoot:/sb
in/nologin
flatpak:x:990:985:User for flatpak system helper:/:/sbin/nologin
colord:x:989:984:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:988:983:Clevis Decryption Framework unprivileged user:/var/cache/clevis
:/usr/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
systemd-oom:x:981:981:systemd Userspace OOM Killer:/:/usr/sbin/nologin
pesign:x:980:980:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
gnome-initial-setup:x:979:979::/run/gnome-initial-setup/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:978:978::/var/lib/chrony:/sbin/nologin
dnsmasq:x:977:977:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
vokhudickiyj:x:1000:1000:vokhudickiyj:/home/vokhudickiyj:/bin/bash
vboxadd:x:976:1::/var/run/vboxadd:/bin/false
guest:x:1001:1001::/home/guest:/bin/bash
```

9. Определил существующие в системе директории командой *ls -l /home/*. Только владельцы папок имеют все права на директориях.

```
[guest@vokhudickiyj ~]$ ls -l /home/
total 8
drwx------. 14 guest        guest        4096 Sep 17 15:47 guest
drwx------. 14 vokhudickiyj vokhudickiyj 4096 Sep 17 14:56 vokhudickiyj
[guest@vokhudickiyj ~]$
```

10. Проверил, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой *lsattr /home*. Удалось увидеть только атрибуты директории пользователя guest:

```
[guest@vokhudickiyj ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/vokhudickiyj
---------------------- /home/guest
```

11. Создал в домашней директории поддиректорию dir1 командой *mkdir dir1*. Определил командами *ls -l* и *lsattr*, какие права доступа и расширенные атрибуты были выставлены на директорию dir1:

```
[guest@vokhudickiyj ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Desktop
drwxrwxr-x. 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 ~]$ lsattr
---------------------- ./Desktop
---------------------- ./Downloads
---------------------- ./Templates
---------------------- ./Public
---------------------- ./Documents
---------------------- ./Music
---------------------- ./Pictures
---------------------- ./Videos
---------------------- ./dir1
[guest@vokhudickiyj ~]$
```

12. Снял с директории dir1 все атрибуты командой *chmod 000 dir1* и проверил с её помощью правильность выполнения команды *ls -l*.

```
[guest@vokhudickiyj ~]$ chmod 000 dir1
[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 ~]$
```

13. Попытался создать в директории dir1 файл file1 командой *echo "test" > /home/guest/dir1/file1*. Получил отказ, так как теперь у меня нет прав на директорию dir1. Попытался проверить создание файла командой *ls -l /home/guest/dir1*, но получил отказ из-за отсутствия прав:

```
[guest@vokhudickiyj ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@vokhudickiyj ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
[guest@vokhudickiyj ~]$
```

14. Заполнил таблицу «Установленные права и разрешённые действия». Выполняя действия от имени владельца директории (файлов), 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------ (100)	--------- (000)	-	-	-	-	+	-	-	+
d-w------- (200)	--------- (000)	-	-	-	-	-	-	-	-
d-wx------ (300)	--------- (000)	+	+	-	-	+	-	+	+
dr-------- (400)	--------- (000)	-	-	-	-	-	+	-	-
dr-x------ (500)	--------- (000)	-	-	-	-	+	+	-	+
drw------- (600)	--------- (000)	-	-	-	-	-	+	-	-
drwx------ (700)	--------- (000)	+	+	-	-	+	+	+	+
d--------- (000)	--x------ (100)	-	-	-	-	-	-	-	-
d--x------ (100)	--x------ (100)	-	-	-	-	+	-	-	+
d-w------- (200)	--x------ (100)	-	-	-	-	-	-	-	-
d-wx------ (300)	--x------ (100)	+	+	-	-	+	-	+	+
dr-------- (400)	--x------ (100)	-	-	-	-	-	+	-	-
dr-x------ (500)	--x------ (100)	-	-	-	-	+	+	-	+
drw------- (600)	--x------ (100)	-	-	-	-	-	+	-	-
drwx------ (700)	--x------ (100)	+	+	-	-	+	+	+	+
d--------- (000)	-w------- (200)	-	-	-	-	-	-	-	-
d--x------ (100)	-w------- (200)	-	-	+	-	+	-	-	+
d-w------- (200)	-w------- (200)	-	-	-	-	-	-	-	-
d-wx------ (300)	-w------- (200)	+	+	+	-	+	-	+	+
dr-------- (400)	-w------- (200)	-	-	-	-	-	+	-	-
dr-x------ (500)	-w------- (200)	-	-	+	-	+	+	-	+
drw------- (600)	-w------- (200)	-	-	-	-	-	+	-	-
drwx------ (700)	-w------- (200)	+	+	+	-	+	+	+	+
d--------- (000)	-wx------ (300)	-	-	-	-	-	-	-	-
d--x------ (100)	-wx------ (300)	-	-	+	-	+	-	-	+
d-w------- (200)	-wx------ (300)	-	-	-	-	-	-	-	-
d-wx------ (300)	-wx------ (300)	+	+	+	-	+	-	+	+
dr-------- (400)	-wx------ (300)	-	-	-	-	-	+	-	-
dr-x------ (500)	-wx------ (300)	-	-	+	-	+	+	-	+
drw------- (600)	-wx------ (300)	-	-	-	-	-	+	-	-
drwx------ (700)	-wx------ (300)	+	+	+	-	+	+	+	+
d--------- (000)	r-------- (400)	-	-	-	-	-	-	-	-
d--x------ (100)	r-------- (400)	-	-	-	+	+	-	-	+
d-w------- (200)	r-------- (400)	-	-	-	-	-	-	-	-
d-wx------ (300)	r-------- (400)	+	+	-	+	+	-	+	+
dr-------- (400)	r-------- (400)	-	-	-	-	-	+	-	-
dr-x------ (500)	r-------- (400)	-	-	-	+	+	+	-	+
drw------- (600)	r-------- (400)	-	-	-	-	-	+	-	-
drwx------ (700)	r-------- (400)	+	+	-	+	+	+	+	+
d--------- (000)	r-x------ (500)	-	-	-	-	-	-	-	-
d--x------ (100)	r-x------ (500)	-	-	-	+	+	-	-	+
d-w------- (200)	r-x------ (500)	-	-	-	-	-	-	-	-
d-wx------ (300)	r-x------ (500)	+	+	-	+	+	-	+	+
dr-------- (400)	r-x------ (500)	-	-	-	-	-	+	-	-
dr-x------ (500)	r-x------ (500)	-	-	-	+	+	+	-	+
drw------- (600)	r-x------ (500)	-	-	-	-	-	+	-	-
drwx------ (700)	r-x------ (500)	+	+	-	+	+	+	+	+
d--------- (000)	rw------- (600)	-	-	-	-	-	-	-	-
d--x------ (100)	rw------- (600)	-	-	+	+	+	-	-	+
d-w------- (200)	rw------- (600)	-	-	-	-	-	-	-	-
d-wx------ (300)	rw------- (600)	+	+	+	+	+	-	+	+
dr-------- (400)	rw------- (600)	-	-	-	-	-	+	-	-
dr-x------ (500)	rw------- (600)	-	-	+	+	+	+	-	+
drw------- (600)	rw------- (600)	-	-	-	-	-	+	-	-
drwx------ (700)	rw------- (600)	+	+	+	+	+	+	+	+
d--------- (000)	rwx------ (700)	-	-	-	-	-	-	-	-
d--x------ (100)	rwx------ (700)	-	-	+	+	+	-	-	+
d-w------- (200)	rwx------ (700)	-	-	-	-	-	-	-	-
d-wx------ (300)	rwx------ (700)	+	+	+	+	+	-	+	+
dr-------- (400)	rwx------ (700)	-	-	-	-	-	+	-	-
dr-x------ (500)	rwx------ (700)	-	-	+	+	+	+	-	+
drw------- (600)	rwx------ (700)	-	-	-	-	-	+	-	-
drwx------ (700)	rwx------ (700)	+	+	+	+	+	+	+	+

15. 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------ (300)	--------- (000)
Удаление файла	d-wx------ (300)	--------- (000)
Чтение файла	d--x------ (100)	r-------- (400)
Запись в файл	d--x------ (100)	-w------- (200)
Переименование файла	d-wx------ (300)	--------- (000)
Создание поддиректории	d-wx------ (300)	--------- (000)
Удаление поддиректории	d-wx------ (300)	--------- (000)

Выводы

Я получил практические навыки работы в консоли с атрибутами файлов и закрепил теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы

- Кулябов Д. С., Королькова А. В., Геворкян М. Н Лабораторная работа №2. Дискреционное разграничение прав в Linux. Основные атрибуты