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.

Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создам учётную запись пользователя guest (использую учётную запись администратора): useradd guest.

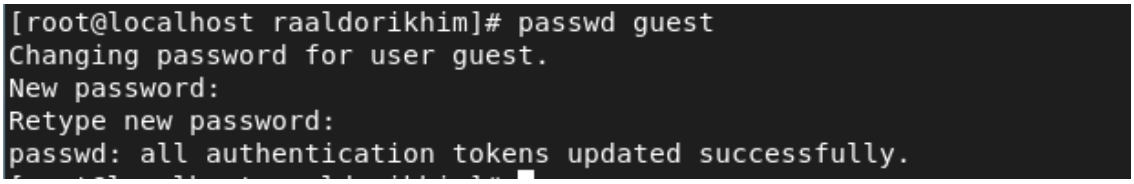
   Получение прав администратора:

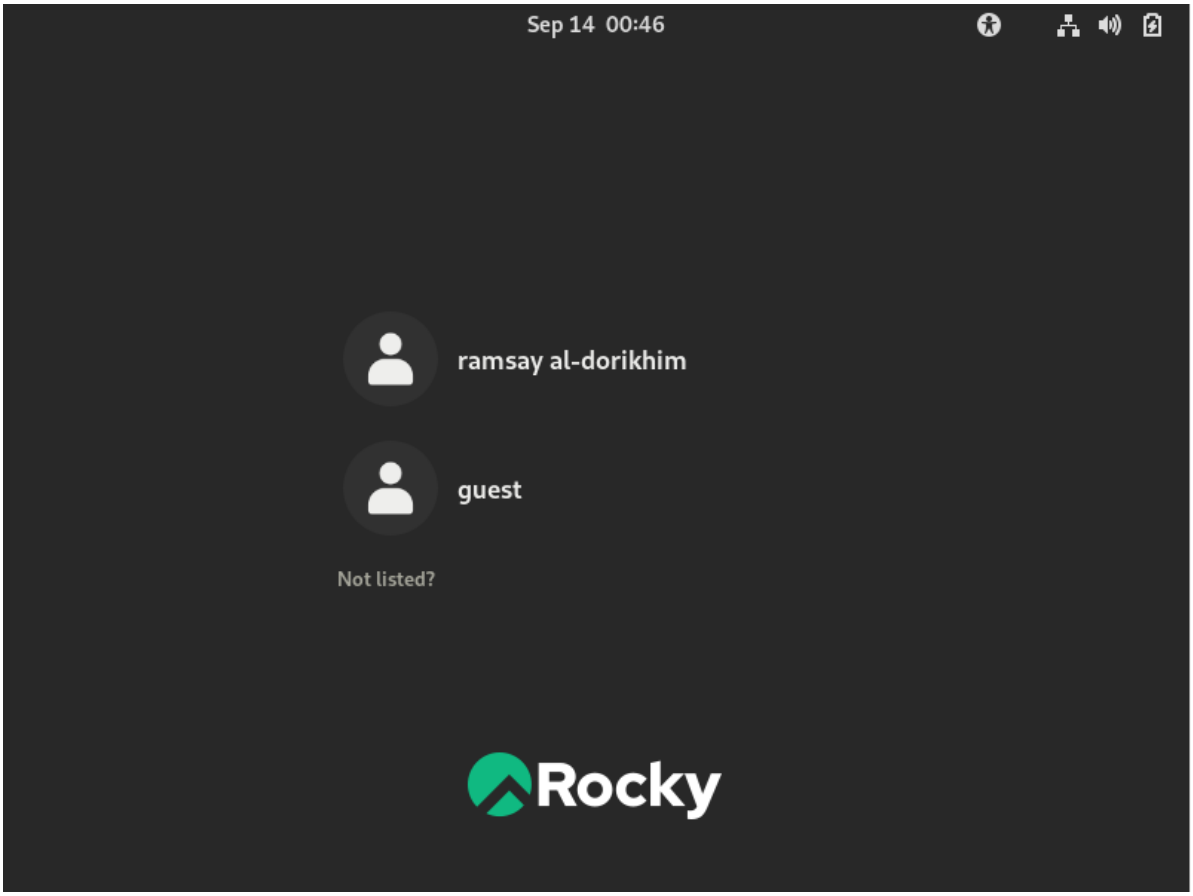
   Создание пользователя:

```
[root@localhost raaldorikhim]# useradd guest
[root@localhost raaldorikhim]# passwd guest
```

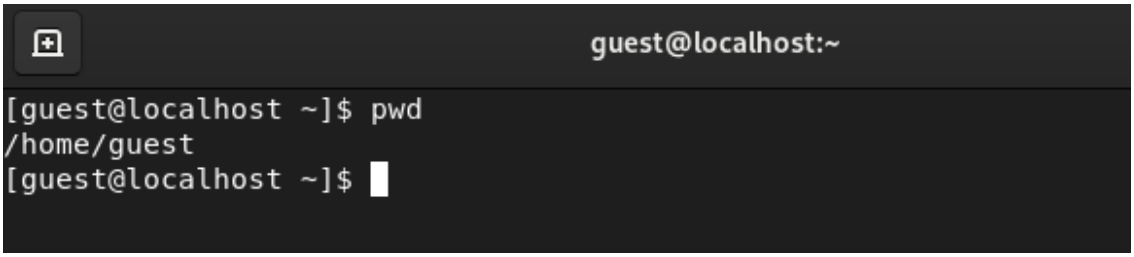
2. Задам пароль для пользователя guest (использую учётную запись администратора): passwd guest.

3. Войдите в систему от имени пользователя guest.

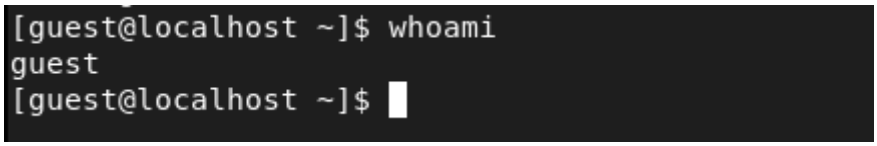


4. Определю директорию, в которой я нахожусь, командой pwd.

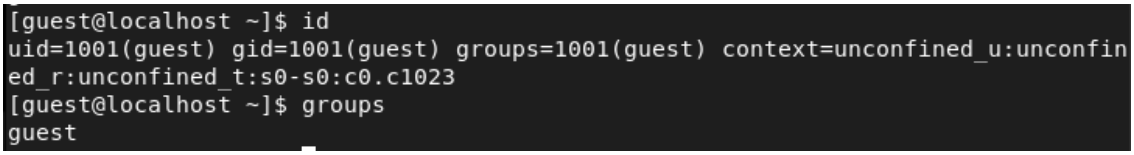


Это домашняя директория.

5. Уточню имя моего пользователя командой whoami.



6. Уточню имя моего пользователя, его группу, а также группы, куда входит пользователь, командой id. Выведенные значения uid, gid и др. запомним. Сравним вывод id с выводом команды groups.



uid = 1001, gid = 1001.

Если сравнивать вывод id с выводом команды groups, то очевидно, что команда id выводит много больше информации.

7. Полученная информация об имени пользователя совпадает с данными, выводимыми в приглашении командной строки.

8. Просмотрим файл /etc/passwd командой cat /etc/passwd Найдем в нём свою учётную запись. Определим uid пользователя. Определим gid пользователя. Сравним найденные значения с полученными в предыдущих пунктах.

```
[guest@localhost ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:998:996:User for polkitd:/:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
sssd:x:997:993:User for sssd:/:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
pipewire:x:996:992:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
libstoragemgmt:x:995:991:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
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/nologin
setroubleshoot:x:991:986:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/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
raaldorikhim:x:1000:1000:ramsay al-dorikhim:/home/raaldorikhim:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
```

uid = 1001 и gid = 1001, как и в предыдущих пунктах.

9. Определю существующие в системе директории командой ls -l /home/ .

```
[guest@localhost ~]$ ls -l /home/
total 8
drwx------. 14 guest        guest        4096 Sep 14 00:46 guest
drwx------. 14 raaldorikhim raaldorikhim 4096 Sep  8 16:48 raaldorikhim
```

Мне удалось получить список поддиректорий директории /home. У пользователя, создавшего директорию (raaldorikhim/guest) есть права на чтение (r), запись (w) и выполнение (x) файлов в директории. У остальных пользователей никаких прав нет.

10. Проверю, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: lsattr /home.

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

Мне не удалось увидеть расширенные атрибуты как текущей директории, так и директории другого пользователя.

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

```
[guest@localhost ~]$ mkdir dir1
[guest@localhost ~]$ ls -l | grep dir1
drwxrwxr-x. 2 guest guest  6 Sep 14 01:07 dir1
[guest@localhost ~]$ lsattr | grep dir1
---------------------- ./dir1
```

У всех есть права на чтение и выполнение, но только у создателя и группы создателя есть права на запись. Расширенные атрибуты просмотреть не удалось.

12. Сниму с директории dir1 все атрибуты командой chmod 000 dir1 и проверю с её помощью правильность выполнения команды ls -l.

```
[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$ ls -l | grep dir1
d---------. 2 guest guest  6 Sep 14 01:07 dir1
```

13. Попытаюсь создать в директории dir1 файл file1 командой echo "test" > /home/guest/dir1/file1.

```
[guest@localhost ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
```

Мне было отказано в создании файла в связи с тем, что ни у кого из пользователей нет прав на создание файла, это видно по скриншоту из предыдущего пункта. Проверю наличие файла file1 в директории dir1.

```
[guest@localhost ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
```

Поскольку права на просмотр директории закрыты, я не смог просмотреть файлы директории.

14. Заполню таблицу «Установленные права и разрешенные действия».

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)	+	-	-	+	+	+	+	+

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
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)	-	+	+	+	+	-	+	+

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
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. Заполню таблицу «Минимальные права для совершения операций».

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)

Вывод

В ходе данной лабораторной работы мы получили практические навыки работы в консоли с атрибутами файлов, закрепили теоретические основы разграничения доступа на базе ОС Linux

Список литературы

- `Кулябов Д. С., Королькова А. В., Геворкян М. Н Лабораторная работа №2`