

Лабораторная работа № 2.

Дискреционное разграничение прав в Linux. Основные атрибуты

Абакумова Олеся Максимовна, НКАбд-01-22

Содержание

Цель работы	1
Задание	1
Теоретическое введение	1
Выполнение лабораторной работы.....	1
Выводы	13
Список литературы	13

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 Linux1 .

Задание

Поэтапное выполнение всех пунктов данной лабораторной работы.

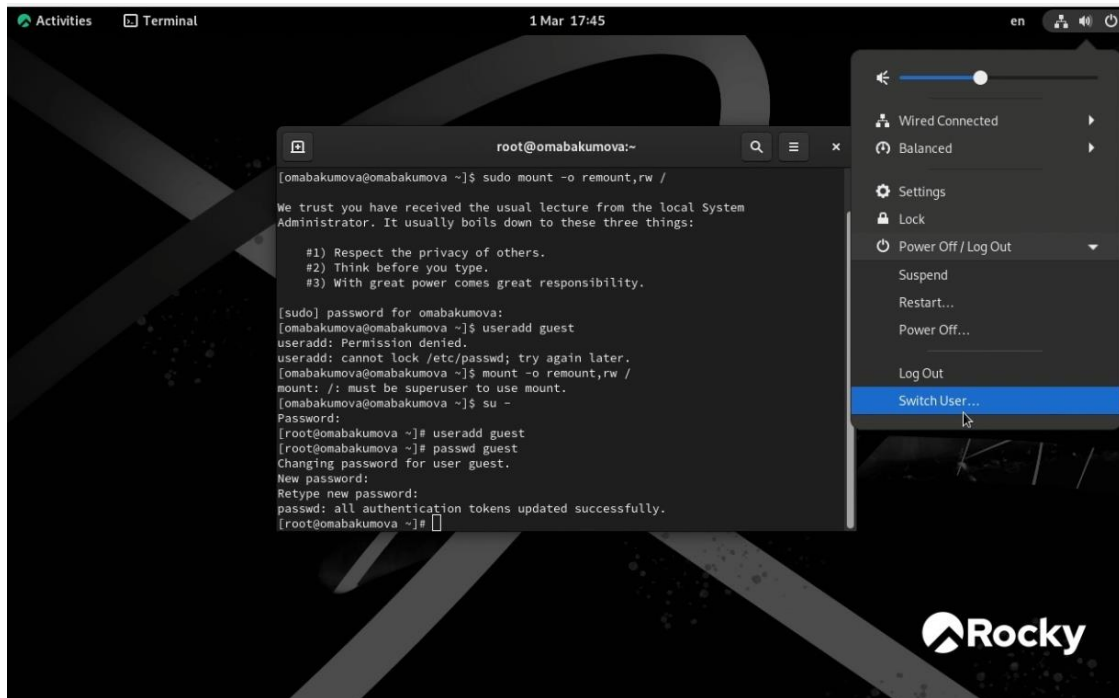
Теоретическое введение

Дискреционное управление доступом - права доступа состоят из трех компонентов: владелец файла, группа владельца и остальные пользователи. Каждому компоненту присваивается разрешение на чтение (r), запись (w) и выполнение (x). Для управления правами доступа в Linux используются команды `chmod`, `chown` и `chgrp`.

Выполнение лабораторной работы

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

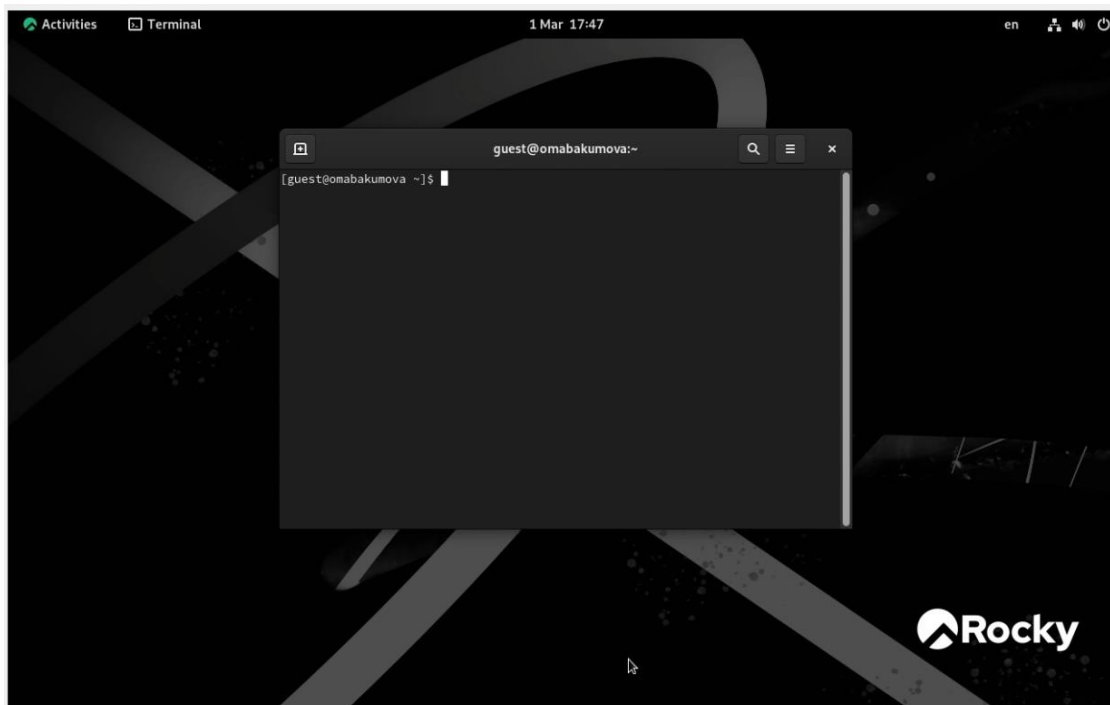
2. Задаем пароль для пользователя guest (используя учётную запись администратора): `passwd guest`



Команда `useradd guest`

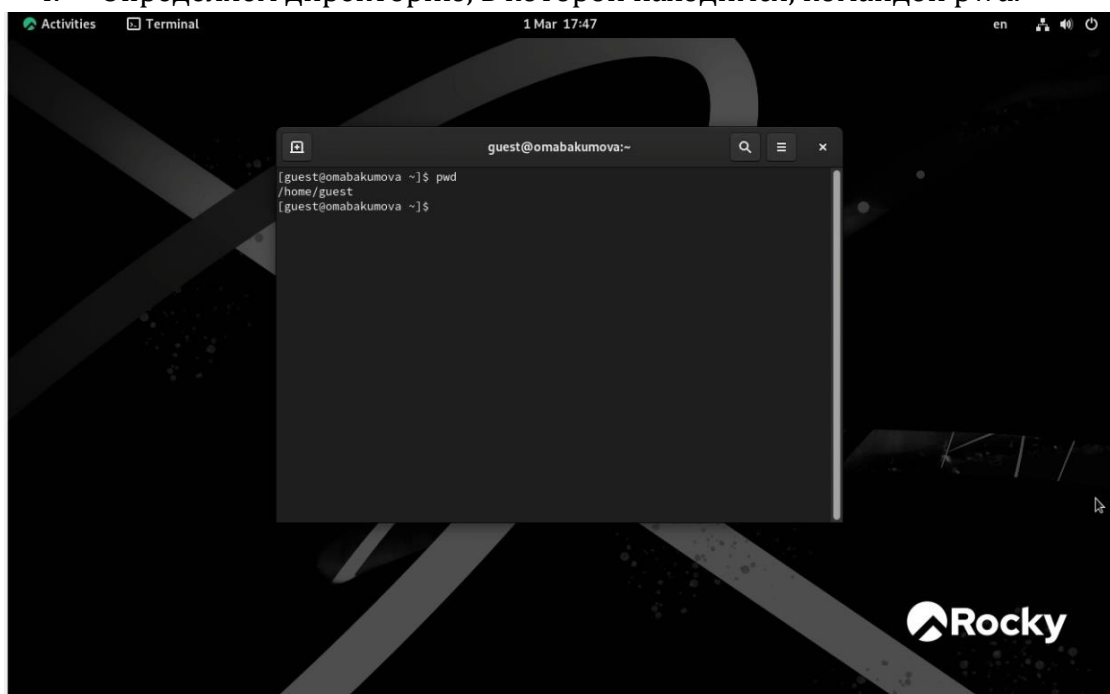
Далее, переходим с учетной записи на которой находились на новую, созданную учетную запись.

3. Входим в систему от имени пользователя guest.



Успешный вход в новую учетную запись и переход в терминал

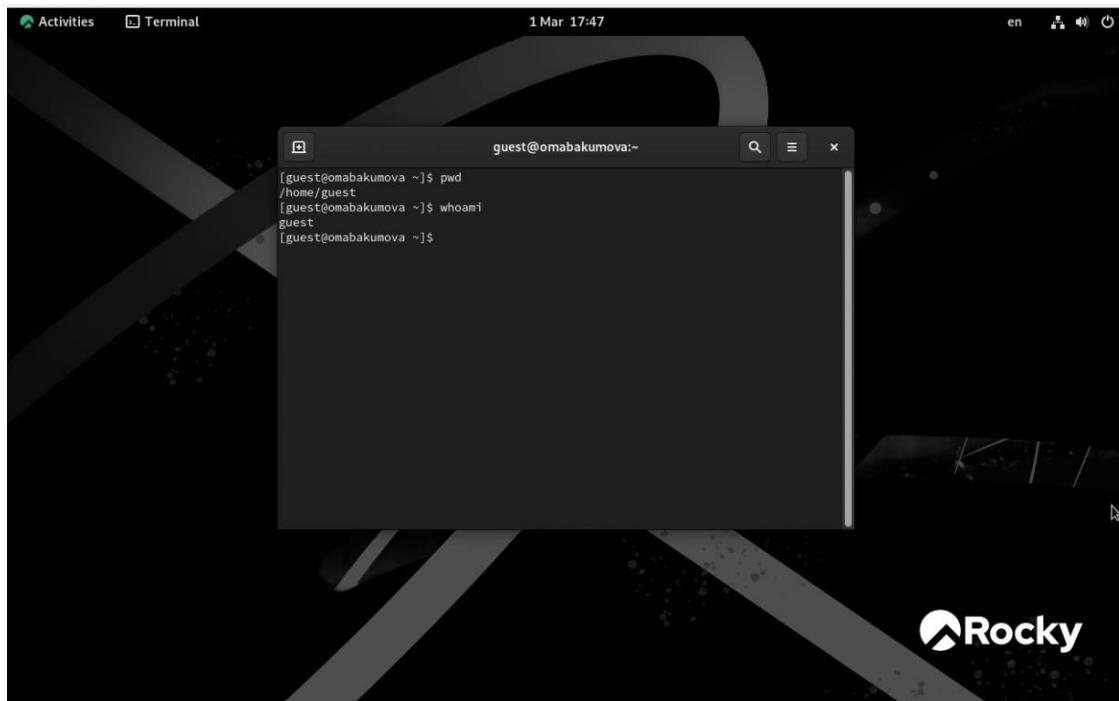
4. Определяем директорию, в которой находимся, командой `pwd`.



Использование команды `pwd`

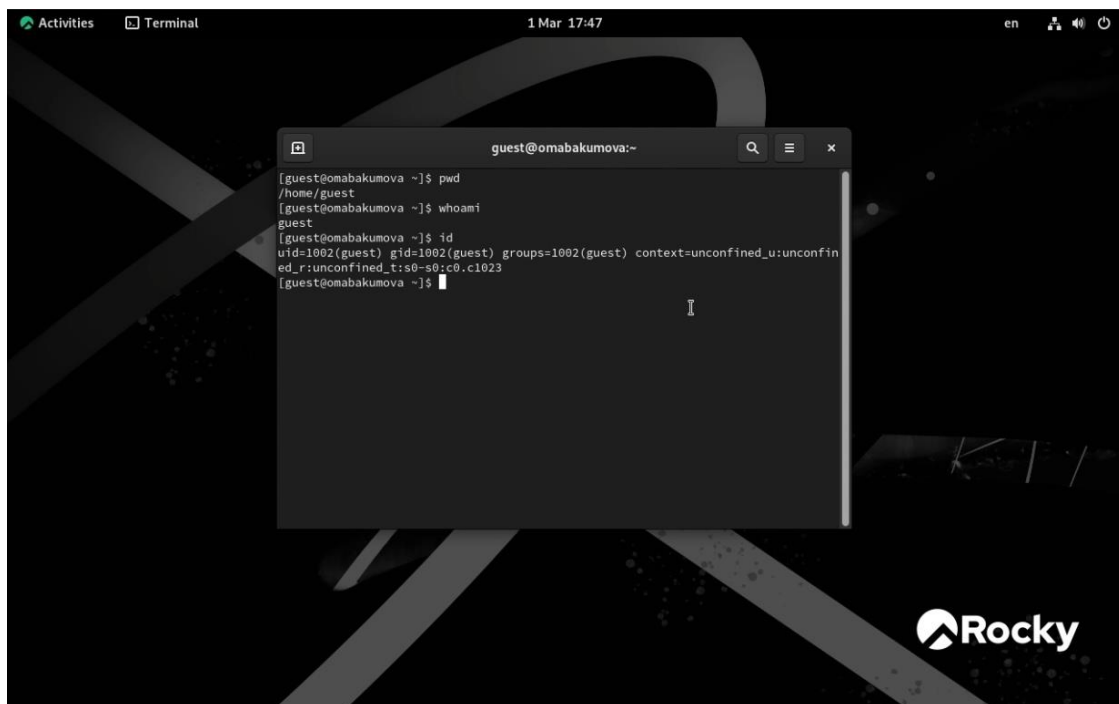
Директория является домашней.

5. Уточняем имя пользователя командой `whoami`.



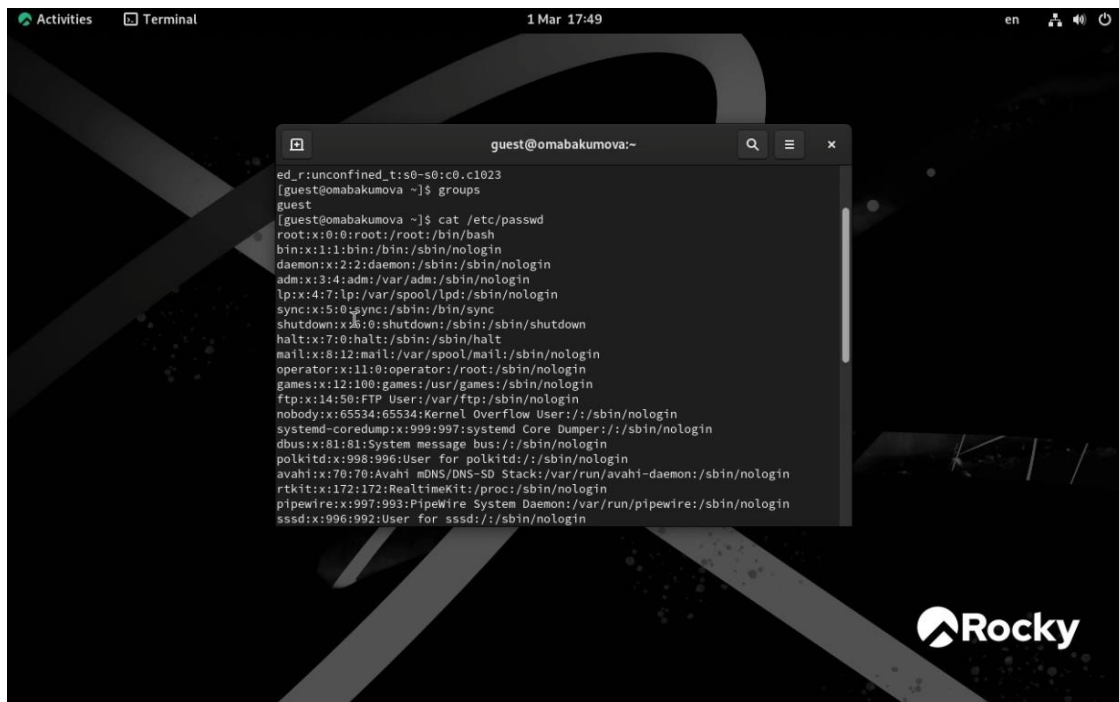
Использование команды *whoami*

6. Уточняем имя пользователя, его группу, а также группы, куда входит пользователь, командой *id*. Выведенные значения *uid*, *gid* и др. запоминаем.



При вводе команды *groups* нам дают более конкретную информацию о пользователе, в случае с *id* мы получаем более подробную о пользователе.

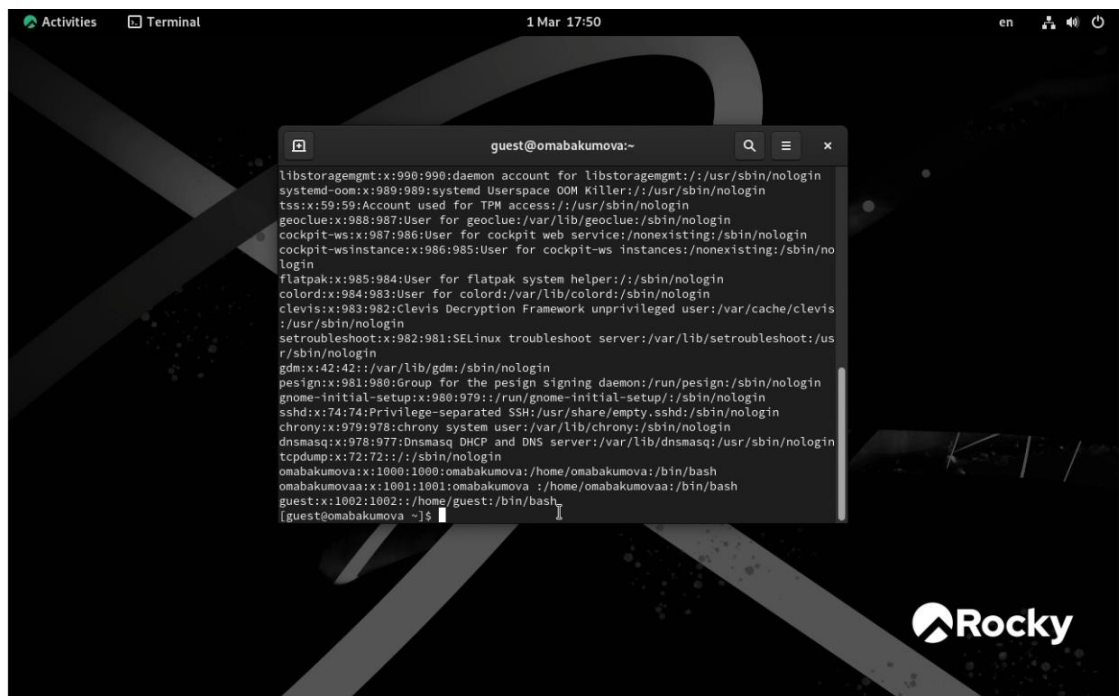
7. Просматриваем файл */etc/passwd* командой *cat /etc/passwd*



The terminal window shows the command `groups` being executed. The output lists the groups for the `guest` user, including `root`, `bin`, `daemon`, `adm`, `lp`, `sync`, `shutdown`, `halt`, `mail`, `operator`, `games`, `ftp`, `nobody`, `systemd-coredump`, `dbus`, `polkitd`, `avahi`, `rtkit`, `pipewire`, and `sssd`.

```
ed_r:unconfined_t:s0-s0:c0.c1023
[guest@omabakumova ~]$ groups
guest
[guest@omabakumova ~]$ 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
avahi:x:70:70:avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pipewire:x:997:993:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
sssd:x:996:992:User for sssd:/sbin/nologin
```

Используем команду `cat /etc/passwd` и находим нашу учетную запись, `uid,gid`(часть1)



The terminal window shows the command `cat /etc/passwd` being executed. The output lists all system and user accounts, including `libstoragemgmt`, `systemd-oom`, `tss`, `geoclue`, `cockpit-ws`, `cockpit-wsinstance`, `flatpak`, `colord`, `clevis`, `setroubleshoot`, `gdm`, `pesign`, `gnome-initial-setup`, `sshd`, `chrony`, `dnsmasq`, `tcpdump`, `omabakumova`, `omabakumovaa`, and `guest`.

```
libstoragemgmt:x:990:990:daemon account for libstoragemgmt:/usr/sbin/nologin
systemd-oom:x:989:989:systemd Userspace OOM Killer:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/usr/sbin/nologin
geoclue:x:988:987:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:987:986:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:986:985:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:985:984:User for flatpak system helper:/sbin/nologin
colord:x:984:983:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:983:982:Clevis Decryption Framework unprivileged user:/var/cache/levis:/usr/sbin/nologin
setroubleshoot:x:982:981:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
pesign:x:981:980:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
gnome-initial-setup:x:980:979:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:979:978:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:978:977:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/sbin/nologin
omabakumova:x:1000:1000:omabakumova:/home/omabakumova:/bin/bash
omabakumovaa:x:1001:1001:omabakumovaa:/home/omabakumovaa:/bin/bash
guest:x:1002:1002:/home/guest:/bin/bash
[guest@omabakumova ~]$
```

Используем команду `cat /etc/passwd` и находим нашу учетную запись, `uid,gid`(часть2)

Дополнительно используем команду `cat /etc/passwd | grep guest` в качестве фильтра для вывода только строк, содержащих определённые буквенные сочетания

```

[guest@omabakumova ~]$ cat /etc/passwd | grep guest
guest:x:1002:1002::/home/guest:/bin/bash
[guest@omabakumova ~]$

```

Используем команду *grep*

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

```

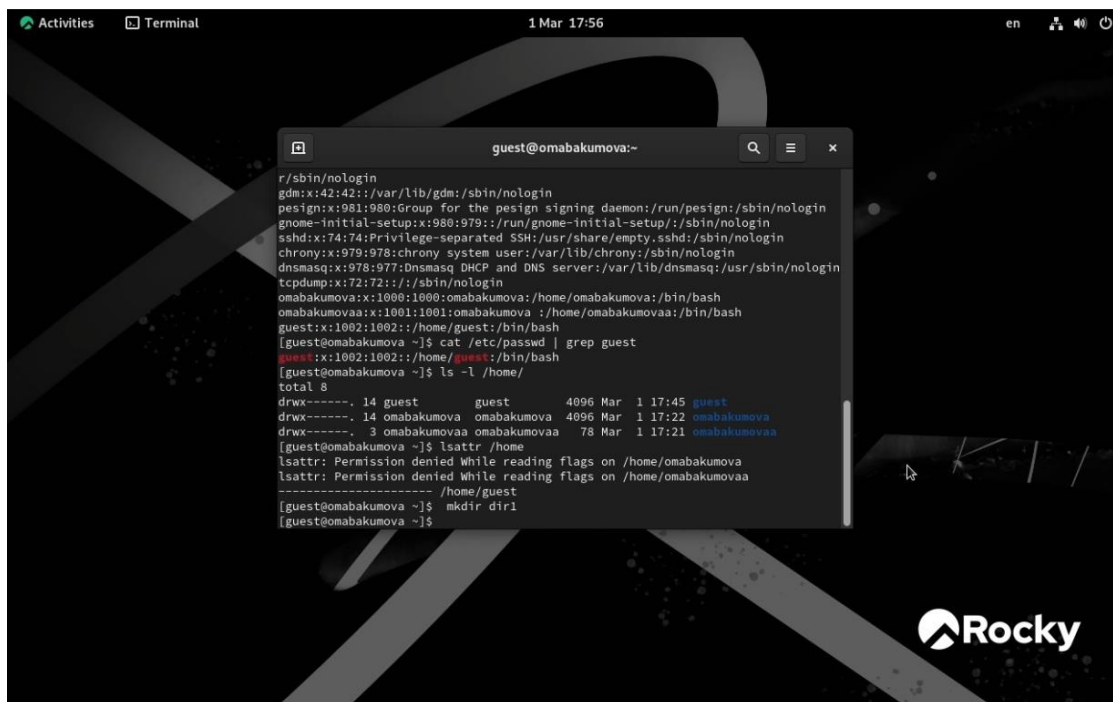
guest@omabakumova:~
flatpak:x:985:984:User for flatpak system helper:/usr/sbin/nologin
colord:x:984:983:User for colord:/usr/lib/colord:/usr/sbin/nologin
clevis:x:983:982:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:982:981:SELinux troubleshoot server:/usr/lib/setroubleshoot:/usr/sbin/nologin
gdm:x:42:42:/usr/lib/gdm:/usr/sbin/nologin
pesign:x:981:980:Group for the pesign signing daemon:/run/pesign:/usr/sbin/nologin
gnome-initial-setup:x:980:979:/usr/share/empty:/usr/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty:/usr/sbin/nologin
chrony:x:979:978:chrony system user:/usr/lib/chrony:/usr/sbin/nologin
dnsmasq:x:978:977:Dnsmasq DHCP and DNS server:/usr/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/usr/sbin/nologin
omabakumova:x:1000:1000:omabakumova:/home/omabakumova:/bin/bash
omabakumovaa:x:1001:1001:omabakumovaa:/home/omabakumovaa:/bin/bash
guest:x:1002:1002:/home/guest:/bin/bash
[guest@omabakumova ~]$ cat /etc/passwd | grep guest
guest:x:1002:1002:/home/guest:/bin/bash
[guest@omabakumova ~]$ ls -l /home/
total 8
drwx----- 14 guest      guest      4096 Mar 1 17:45 guest
drwx----- 14 omabakumova omabakumova 4096 Mar 1 17:22 omabakumova
drwx-----  3 omabakumovaa omabakumovaa 78 Mar 1 17:21 omabakumovaa
[guest@omabakumova ~]$

```

Используем команду *ls -l /home/*

Мы получили необходимую нам информацию о директориях и о правах.

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



Используем команды lsattr /home

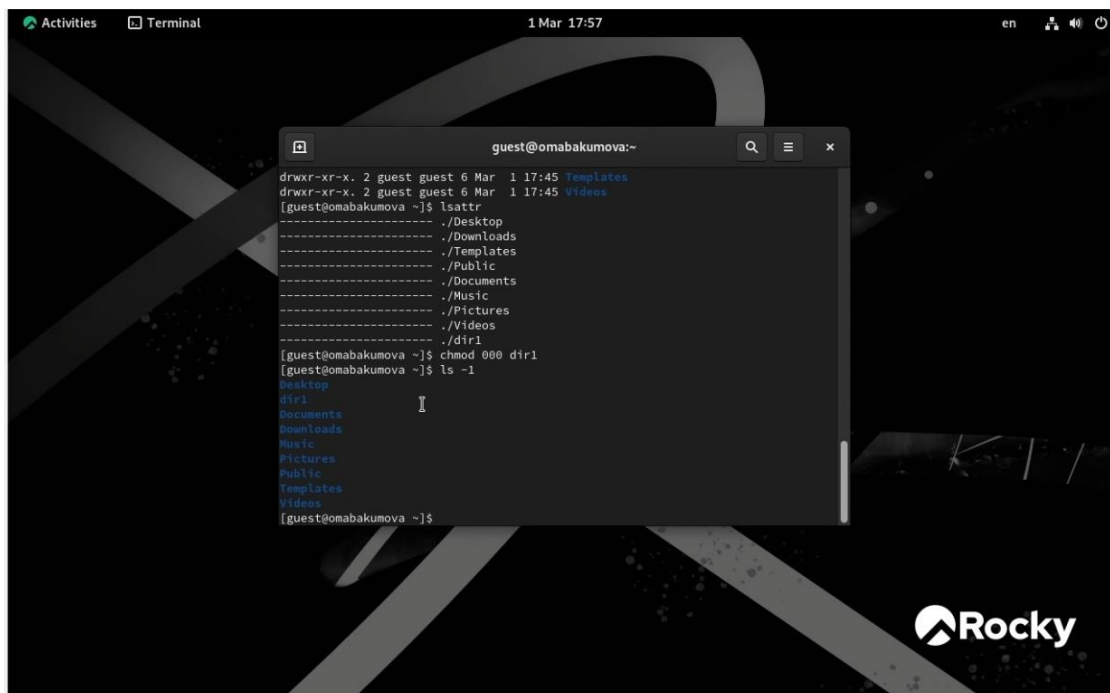
Нам запрещен доступ.

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



Создаем поддиректорию dir1 командой mkdir dir1, задействуем команды ls -l и lsattr

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



Использование команд `chmod 000 dir1` и `ls -l`

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

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

Использование команды `echo "test" > /home/guest/dir1/file1`.

Мы получили отказ в связи с тем, что сняли все атрибуты с этой директории в прошлом пункте.

Проверка командой `ls -l /home/guest/dir1`

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

Использование команды `ls -l /home/guest/dir1`

14. Заполняем таблицу «Установленные права и разрешённые действия» (см. табл. 2.1), выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, заносим в таблицу знак «+», если не разрешена, знак «-».

Таблица 2.1

Установленные права и разрешённые 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)	-	-	-	-	+	-	-	+
drwx----- (700)	rw-x----- (700)	+	+	+	+	+	+	+	+

Пример таблицы "Установленные права и разрешённые 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(000)	(100)	-	-	-	-	-	-	-	-
d(000)	(200)	-	-	-	-	-	-	-	-
d(000)	(300)	-	-	-	-	-	-	-	-
d(000)	(400)	-	-	-	-	-	-	-	-
d(000)	(500)	-	-	-	-	-	-	-	-
d(000)	(600)	-	-	-	-	-	-	-	-
d(000)	(700)	-	-	-	-	-	-	-	-
d(100)	(000)	-	-	-	-	+	-	-	+
d(100)	(100)	-	-	-	-	+	-	-	+
d(100)	(200)	-	-	+	-	-	-	-	-

d(100)	(30 0)	-	-	+	-	+	-	-	+
d(100)	(40 0)	-	-	-	+	-	-	-	-
d(100)	(50 0)	-	-	-	+	+	-	-	+
d(100)	(60 0)	-	-	+	+	+	-	-	+
d(100)	(70 0)	-	-	+	+	+	-	-	+
d(200)	(00 0)	-	-	-	-	-	-	-	-
d(200)	(10 0)	-	-	-	-	-	-	-	-
d(200)	(20 0)	-	-	-	-	-	-	-	-
d(200)	(30 0)	-	-	-	-	-	-	-	-
d(200)	(40 0)	-	-	-	-	-	-	-	-
d(200)	(50 0)	-	-	-	-	-	-	-	-
d(200)	(60 0)	-	-	-	-	-	-	-	-
d(200)	(70 0)	-	-	-	-	-	-	-	-
d(300)	(00 0)	+	+	-	-	+	-	+	+
d(300)	(10 0)	+	+	-	-	+	-	+	+
d(300)	(20 0)	+	+	+	-	+	-	+	+
d(300)	(30 0)	+	+	+	-	+	-	+	+
d(300)	(40 0)	+	+	-	+	+	-	+	+
d(300)	(50 0)	+	+	-	+	+	-	+	+
d(300)	(60 0)	+	+	+	+	+	-	+	+

d(300)	(70 0)	+	+	+	+	+	-	+	+
d(400)	(00 0)	-	-	-	-	-	+	-	-
d(400)	(10 0)	-	-	-	-	-	+	-	-
d(400)	(20 0)	-	-	-	-	-	+	-	-
d(400)	(30 0)	-	-	-	-	-	+	-	-
d(400)	(40 0)	-	-	-	-	-	+	-	-
d(400)	(50 0)	-	-	-	-	-	+	-	-
d(400)	(60 0)	-	-	-	-	-	+	-	-
d(400)	(70 0)	-	-	-	-	-	+	-	-
d(500)	(00 0)	-	-	-	-	+	+	-	+
d(500)	(10 0)	-	-	-	-	+	+	-	+
d(500)	(20 0)	-	-	+	-	+	+	-	+
d(500)	(30 0)	-	-	+	-	+	+	-	+
d(500)	(40 0)	-	-	-	+	+	+	-	+
d(500)	(50 0)	-	-	-	+	+	+	-	+
d(500)	(60 0)	-	-	+	+	+	+	-	+
d(500)	(70 0)	-	-	+	+	+	+	-	+
d(600)	(00 0)	-	-	-	-	-	+	-	-
d(600)	(10 0)	-	-	-	-	-	+	-	-
d(600)	(20 0)	-	-	-	-	-	+	-	-

d(600)	(30 0)	-	-	-	-	-	+	-	-
d(600)	(40 0)	-	-	-	-	-	+	-	-
d(600)	(50 0)	-	-	-	-	-	+	-	-
d(600)	(60 0)	-	-	-	-	-	+	-	-
d(600)	(70 0)	-	-	-	-	-	+	-	-
d(700)	(00 0)	+	+	-	-	+	+	+	+
d(700)	(10 0)	+	+	-	-	+	+	+	+
d(700)	(20 0)	+	+	+	-	+	+	+	+
d(700)	(30 0)	+	+	+	-	+	+	+	+
d(700)	(40 0)	+	+	-	+	+	+	+	+
d(700)	(50 0)	+	+	-	+	+	+	+	+
d(700)	(60 0)	+	+	+	+	+	+	+	+
d(700)	(70 0)	+	+	+	+	+	+	+	+

15. На основании заполненной таблицы определяем те или иные минимально необходимые права для выполнения операций внутри директории dir1.

Таблица 2.2

Минимальные права для совершения операций

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла		
Удаление файла		
Чтение файла		
Запись в файл		
Переименование файла		
Создание поддиректории		
Удаление поддиректории		

Пример таблицы “Минимальные права для совершения операций”

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла		d(300) (000)
Удаление файла		d(300) (000)
Чтение файла		d(100) (400)
Запись в файл		d(100) (200)
Переименование файла		d(300) (000)
Создание поддиректории		d(300) (000)
Удаление поддиректории		d(300) (000)

Выводы

Выполняя данную лабораторную работы, мы получили практические навыки работы в консоли с атрибутами файлов и закрепили теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы

1.О правах доступа в ОС 2.Подробнее о дискреционном разграничении прав