

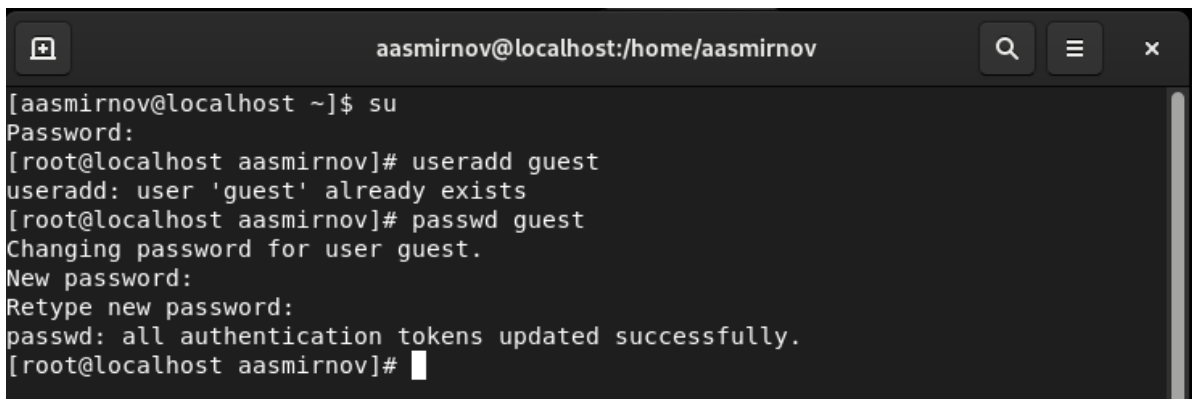
Цель работы

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

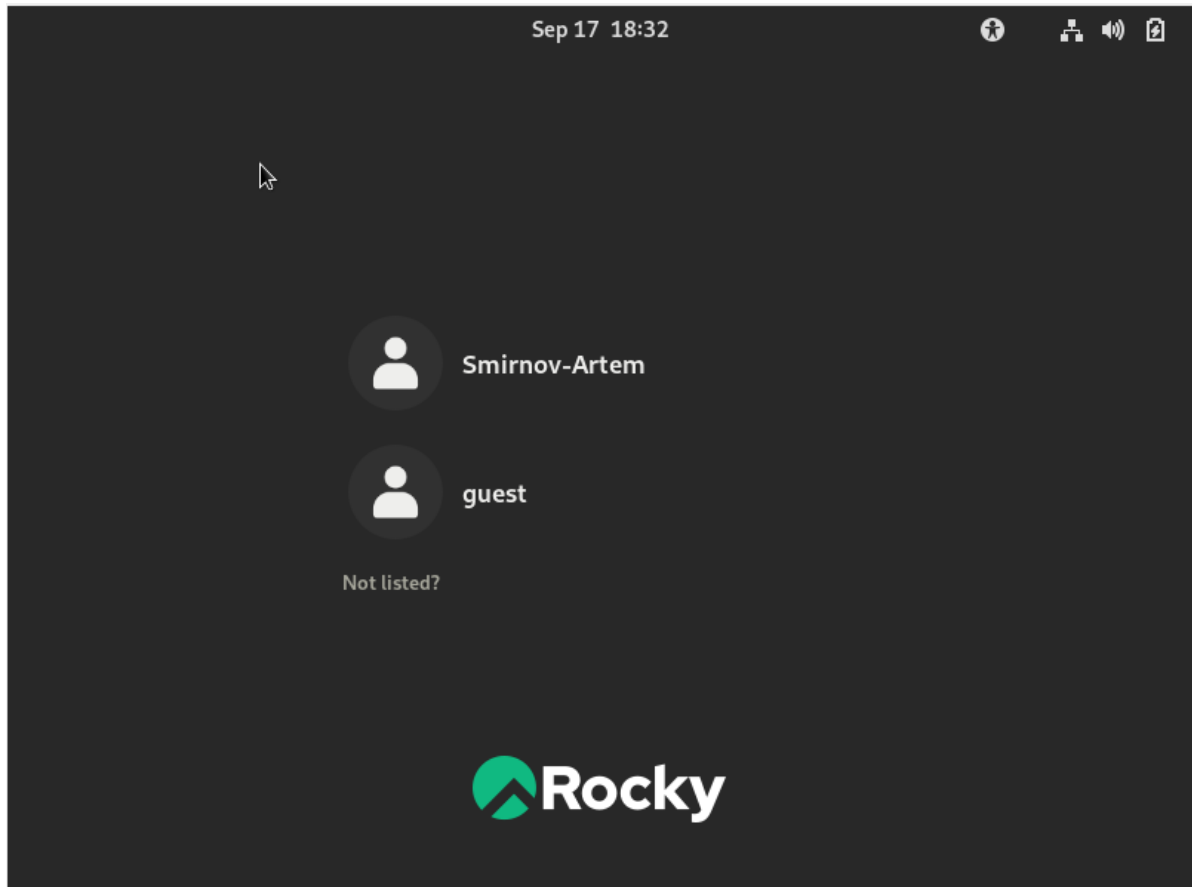
1. Создам учётную запись пользователя guest (использую учётную запись администратора).
2. Задам пароль для пользователя guest.

!

A terminal window titled 'aasmirnov@localhost:/home/aasmirnov' with search, menu, and close buttons. The command history shows: [aasmirnov@localhost ~]\$ su, Password:, [root@localhost aasmirnov]# useradd guest, useradd: user 'guest' already exists, [root@localhost aasmirnov]# passwd guest, Changing password for user guest., New password:, Retype new password:, passwd: all authentication tokens updated successfully., [root@localhost aasmirnov]#

```
[aasmirnov@localhost ~]$ su
Password:
[root@localhost aasmirnov]# useradd guest
useradd: user 'guest' already exists
[root@localhost aasmirnov]# passwd guest
Changing password for user guest.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost aasmirnov]#
```

3. Войду в систему от имени пользователя guest.



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

```
guest@localhost:~  
[guest@localhost ~]$ pwd  
/home/guest  
[guest@localhost ~]$
```

Домашняя директория.

5. Уточню имя пользователя командой whoami.

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

6. Уточню имя пользователя, его группу, а также группы, куда входит пользователь, командой id.

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

uid = 1001, gid = 1001.

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  
bash: cat /etc/passwd: No such file or directory  
[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
```

```
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
sssd:x:997:993:User for sssd:/usr/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:/usr/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:/usr/sbin/tcpdump:/sbin/nologin
aasmirnov:x:1000:1000:Smirnov-Artem:/home/aasmirnov:/bin/bash
guest:x:1001:1001:/home/guest:/bin/bash
```

uid = 1001 и gid = 1001.

9. Определим существующие в системе директории.

```
[guest@localhost ~]$ ls -l /home/
total 8
drwx-----. 14 aasmirnov aasmirnov 4096 Sep 17 17:52 aasmirnov
drwx-----. 14 guest      guest      4096 Sep 17 19:26 guest
```

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

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

```
[guest@localhost ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/aasmirnov
----- /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 17 19:31 dir1
[guest@localhost ~]$ lsattr | grep dir1
----- ./dir1
[guest@localhost ~]$
```

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
l----- . 2 guest guest 6 Sep 17 19:31 dir1
guest@localhost ~]$

```

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
[guest@localhost ~]$

```

Мне было отказано в создании файла так как ни у кого из пользователей нет прав на создание файла. 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-----	--x-----	-	-	-	-	+	-	-	+

(100)	(100)								
d-w-----	--x-----	-	-	-	-	-	-	-	-
(200)	(100)								
d-wx-----	--x-----	+	+	-	-	+	-	+	+
(300)	(100)								
dr-----	--x-----	-	-	-	-	-	+	-	-
(400)	(100)								
dr-x-----	--x-----	-	-	-	-	+	+	-	+
(500)	(100)								
drw-----	--x-----	-	-	-	-	-	+	-	-
(600)	(100)								
drwx-----	--x-----	+	+	-	-	+	+	+	+
(700)	(100)								
d-----	-w-----	-	-	-	-	-	-	-	-
(000)	(200)								
d--x-----	-w-----	-	-	+	-	+	-	-	+
(100)	(200)								
d-w-----	-w-----	-	-	-	-	-	-	-	-
(200)	(200)								
d-wx-----	-w-----	+	+	+	-	+	-	+	+
(300)	(200)								
dr-----	-w-----	-	-	-	-	-	+	-	-
(400)	(200)								

dr-x-----	-w-----	-	-	+	-	+	+	-	+
(500)	(200)								
drw-----	-w-----	-	-	-	-	-	+	-	-
(600)	(200)								
drwx-----	-w-----	+	+	+	-	+	+	+	+
(700)	(200)								
d-----	-wx-----	-	-	-	-	-	-	-	-
(000)	(300)								
d--x-----	-wx-----	-	-	+	-	+	-	-	+
(100)	(300)								
d-w-----	-wx-----	-	-	-	-	-	-	-	-
(200)	(300)								
d-wx-----	-wx-----	+	+	+	-	+	-	+	+
(300)	(300)								
dr-----	-wx-----	-	-	-	-	-	+	-	-
(400)	(300)								
dr-x-----	-wx-----	-	-	+	-	+	+	-	+
(500)	(300)								
drw-----	-wx-----	-	-	-	-	-	+	-	-
(600)	(300)								
drwx-----	-wx-----	+	+	+	-	+	+	+	+
(700)	(300)								
d-----	r-----	-	-	-	-	-	-	-	-

(000)	(400)								
d--x-----	r-----	-	-	-	+	+	-	-	+
(100)	(400)								
d-w-----	r-----	-	-	-	-	-	-	-	-
(200)	(400)								
d-wx-----	r-----	+	+	-	+	+	-	+	+
(300)	(400)								
dr-----	r-----	-	-	-	-	-	+	-	-
(400)	(400)								
dr-x-----	r-----	-	-	-	+	+	+	-	+
(500)	(400)								
drw-----	r-----	-	-	-	-	-	+	-	-
(600)	(400)								
drwx-----	r-----	+	+	-	+	+	+	+	+
(700)	(400)								
d-----	r-x-----	-	-	-	-	-	-	-	-
(000)	(500)								
d--x-----	r-x-----	-	-	-	+	+	-	-	+
(100)	(500)								
d-w-----	r-x-----	-	-	-	-	-	-	-	-
(200)	(500)								
d-wx-----	r-x-----	+	+	-	+	+	-	+	+
(300)	(500)								

dr-----	r-x-----	-	-	-	-	-	+	-	-
(400)	(500)								
dr-x-----	r-x-----	-	-	-	+	+	+	-	+
(500)	(500)								
drw-----	r-x-----	-	-	-	-	-	+	-	-
(600)	(500)								
drwx-----	r-x-----	+	+	-	+	+	+	+	+
(700)	(500)								
d-----	rw-----	-	-	-	-	-	-	-	-
(000)	(600)								
d--x-----	rw-----	-	-	+	+	+	-	-	+
(100)	(600)								
d-w-----	rw-----	-	-	-	-	-	-	-	-
(200)	(600)								
d-wx-----	rw-----	+	+	+	+	+	-	+	+
(300)	(600)								
dr-----	rw-----	-	-	-	-	-	+	-	-
(400)	(600)								
dr-x-----	rw-----	-	-	+	+	+	+	-	+
(500)	(600)								
drw-----	rw-----	-	-	-	-	-	+	-	-
(600)	(600)								
drwx-----	rw-----	+	+	+	+	+	+	+	+
(700)	(600)								

(700)	(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)
Переименовывание 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](#)