

Лабораторная работа номер 2

Malkov Roman Sergeevich

09.09.2024

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.

Создаем новую учетную запись guest

```
[rsmaljkov@localhost ~]$ sudo useradd guest  
  
We trust you have received the usual lecture from the local System  
Administrator. It usually boils down to these three things:  
  
#1) Respect the privacy of others.  
#2) Think before you type.  
#3) With great power comes great responsibility.
```

Рис. 1: Создаем учетную запись

```
[rsmaljkov@localhost ~]$ sudo passwd guest
Changing password for user guest.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Рис. 2: Задаем новый пароль

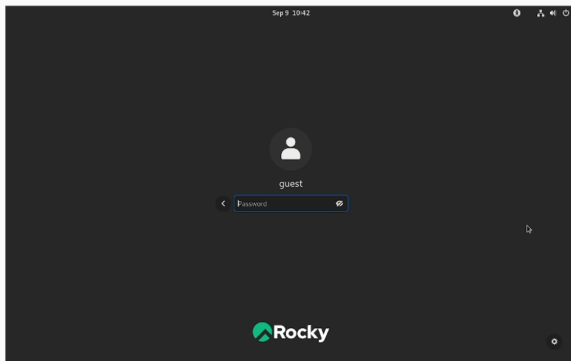


Рис. 3: Переход в новую учетную запись

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

Рис. 4: Команды pwd,whoami,id,groups

```
[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
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:997:994:PipeWire System Daemon:/run/pipewire:/usr/sbin/nologin
```

Рис. 5: passwd

```
[guest@localhost ~]$ cat etc/passwd | grep guest  
guest:x:1001:1001::/home/guest:/bin/bash  
[guest@localhost ~]$
```

Рис. 6: passwd с grep


```
[guest@localhost ~]$ ls -l /home/  
total 8  
drwx-----, 14 guest      guest      4096 Sep  9 10:42 guest  
drwx-----, 14 rsmaljkov  rsmaljkov 4096 Sep  2 13:58 rsmaljkov
```

Рис. 7: ls -l /home/

```
[guest@localhost ~]$ lsattr /home  
lsattr: Permission denied while reading flags on /home/rsmaljkov  
/home/guest
```

Рис. 8: lsattr /home

```
[guest@localhost ~]$ mkdir dir1  
[guest@localhost ~]$ ls  
Desktop dir1 Documents Downloads Music Pictures Public Templates Videos
```

Рис. 9: mkdir dir1

```
[guest@localhost ~]$ ls -l | grep dir1  
drwxr-xr-x. 2 guest guest 6 Sep  9 10:58 dir1
```

Рис. 10: `ls -l |grep dir1`

```
[guest@localhost ~]$ lsattr | grep dir1  
----- ./dir1
```

Рис. 11: lsattr |grep dir1

```
[guest@localhost ~]$ chmod 000 dir1  
[guest@localhost ~]$ lsattr | grep dir1  
lsattr: Permission denied while reading flags on ./dir1  
[guest@localhost ~]$ ls -l | grep dir1  
d-----, 2 guest guest 6 Sep  9 10:58 dir1
```

Рис. 12: chmod 000 dir1

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

Рис. 13: echo "test" > /home/guest/dir1/file1

```
[guest@localhost ~]$ chmod -u+r dir1  
[guest@localhost ~]$ ls -l /home/guest/dir1  
total 0
```

Рис. 14: Проверяем созданся ли файл

| Права дирек- тории | Права файла | Создание файла | Удаление файла | Изменение файла | Чтение файла | Смена дирек- тории | Просмотр фай- лов в дирек- тории | Изменение файла | Атри- бутов 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) | (300) | - | - | + | - | + | - | - | + |
| d(100) | (400) | - | - | - | + | + | - | - | + |
| d(100) | (500) | - | - | - | + | + | - | - | + |
| d(100) | (600) | - | - | + | + | + | - | - | + |
| d(100) | (700) | - | - | + | + | + | - | - | + |
| d(200) | (000) | - | - | - | - | - | - | - | - |
| d(200) | (100) | - | - | - | - | - | - | - | - |
| d(200) | (200) | - | - | - | - | - | - | - | - |
| d(200) | (300) | - | - | - | - | - | - | - | - |
| d(200) | (400) | - | - | - | - | - | - | - | - |
| d(200) | (500) | - | - | - | - | - | - | - | - |

Рис. 15: Пример заполнения таблицы 2.1

Таблица 2.1 «Установленные права и разрешённые действия»

Заполняем таблицу 2.2

| 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) |

11

Рис. 16: Пример заполнения таблицы 2.2

Были получены навыки работы в консоли с атрибутами файлов, были закреплены теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.