

Презентация по лабораторной работе №1

Основы информационной безопасности

Черная С.В.

8 марта 2025

Российский университет дружбы народов, Москва, Россия

Информация

- Черная София Витальевна
- студентка группы НКАбд-01-23
- Российский университет дружбы народов



Рис. 1: Черная София Витальевна

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

1. Создание новой учетной записи guest
2. Работа с атрибутами файлов
3. Работа над созданием
4. Заполнение таблицы «Установленные права и разрешённые действия»
5. Определение тех или иные минимально необходимых прав для выполнения операций внутри директории dir1

Теоретическое введение

В операционной системе Linux команда `lsattr` отображает характеристики атрибутов и их возможные значения для устройств в системе. Использование в Linux команды `lsattr`

Логическое имя устройства следует указывать с помощью флага `-l` (Name), либо использовать комбинацию одного или всех флагов `-c` (Class), `-s` (Subclass) и `-t` (Type), чтобы однозначно идентифицировать predetermined устройство. По умолчанию

На практике команда `lsattr` принимает в качестве аргументов имена файлов и каталогов для проверки. Если мы не указываем файл, он проверяет атрибуты текущего рабочего каталога.

В результате команда `lsattr` отображает по одному символу для каждого атрибута, чтобы указать, включён этот атрибут или нет:

Выполнение лабораторной работы

Задание 1

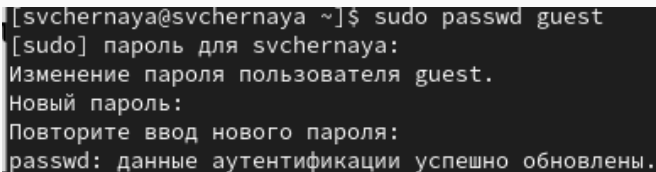
В установленной при выполнении предыдущей лабораторной работы операционной системе Rocky создаю учётную запись пользователя guest (используя учётную запись администратора): `useradd guest`

```
[svchernaya@svchernaya ~]$ sudo useradd guest  
[sudo] пароль для svchernaya:
```

Рис. 2: Guest

Задание 2

Задаю пароль для пользователя guest (использую учётную запись администратора) с помощью команды: `passwd guest`

A terminal window with a dark background and light-colored text. The text shows a user at a shell prompt running the command 'sudo passwd guest'. The prompt changes to '[sudo] пароль для svchernaya:', followed by the system message 'Изменение пароля пользователя guest.' and the prompt 'Новый пароль:'. After an invisible input, the prompt changes to 'Повторите ввод нового пароля:'. After another invisible input, the final message 'passwd: данные аутентификации успешно обновлены.' is displayed.

```
[svchernaya@svchernaya ~]$ sudo passwd guest
[sudo] пароль для svchernaya:
Изменение пароля пользователя guest.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
```

Рис. 3: Password

Задание 3

Вхожу в систему от имени пользователя guest

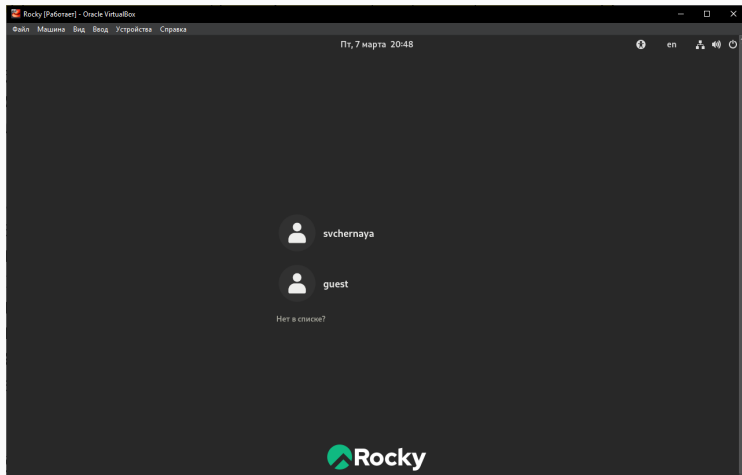
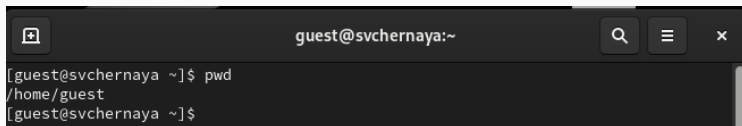


Рис. 4: Guest

Задание 4

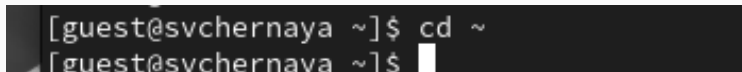
Определяю директорию, в которой я нахожусь, командой `pwd`. Результат получаю `/home/guest`. Однако в приглашении командной строки стоит знак `~`, указывающий, что данная директория является домашней

A terminal window with a dark background. The title bar shows 'guest@svchernaya:~'. The prompt is '[guest@svchernaya ~]\$'. The command 'pwd' has been entered, and the output is '/home/guest'. The prompt is now '[guest@svchernaya ~]\$' again.

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

Рис. 5: `pwd`

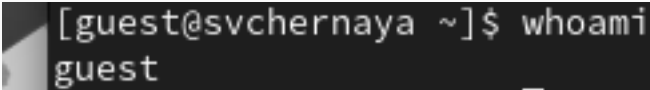
Проверяю, на всякий случай, командой перехода в домашнюю директорию : `cd ~`. Директория, в которой мы находились, не изменилась, что свидетельствует о том, что мы действительно находимся в домашней директории

A terminal window with a dark background. The prompt is '[guest@svchernaya ~]\$'. The command 'cd ~' has been entered, and the output is '[guest@svchernaya ~]\$'. The prompt is now '[guest@svchernaya ~]\$' again.

```
[guest@svchernaya ~]$ cd ~  
[guest@svchernaya ~]$
```

Задание 5

Уточняю имя моего пользователя командой whoami

A terminal window with a dark background. The prompt is [guest@svchernaya ~]\$ and the command whoami has been entered. The output guest is displayed on the line below the command.

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

Рис. 7: whoami

Задание 6

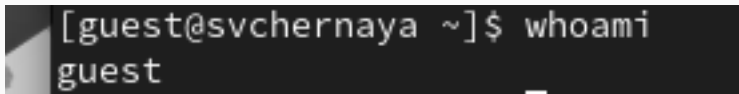
Уточняю имя моего пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. запоминаю. Сравниваю вывод `id` с выводом команды `groups`. Замечаю, что с помощью команды `id` можно узнать больше информации о пользователе `guest` и его группы

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

Рис. 8: `id`, `groups`

Задание 7

Сравниваю полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки и замечаю, что они совпадают

A terminal window with a dark background. The prompt is [guest@svchernaya ~]\$ and the command entered is whoami. The output of the command is guest.

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

Рис. 9: Guest

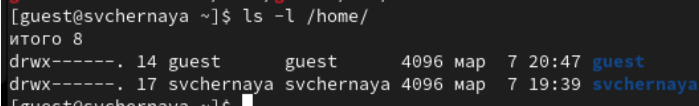
Задание 8

Просматриваю файл /etc/passwd командой `cat /etc/passwd`. Нахожу в нем свою учетную запись(выделено красным), определяю, что `uid` пользователя и `gid` пользователя равны 1001. Они совпадают с запомненными мною ранее при выводе с помощью команды `id`

```
[guest@svchernaya ~]$ 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
tss:x:59:59:Account used for TPM access:/usr/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
sssd:x:997:995:User for sssd:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
geoclue:x:996:994:User for geoclue:/var/lib/geoclue:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/sbin/nologin
pipewire:x:995:992:PipeWire System Daemon:/run/pipewire:/usr/sbin/nologin
libstoragemgmt:x:990:990:daemon account for libstoragemgmt:/usr/sbin/nologin
cockpit-wsinstance:x:989:988:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:988:987:User for flatpak system helper:/sbin/nologin
colord:x:987:986:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:986:985:clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:985:984:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
staprunpriv:x:159:159:systemtap unprivileged user:/var/lib/staprunpriv:/sbin/nologin
pesign:x:984:983:Group for the pesign signing daemon:/run/psign:/sbin/nologin
gnome-initial-setup:x:983:982:/run/gnome-initial-setup:/sbin/nologin
chrony:x:982:981:chrony system user:/var/lib/chrony:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
dnsmasq:x:981:980:dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/usr/sbin/nologin
svchernaya:x:1000:1000:svchernaya:/home/svchernaya:/bin/bash
vboxadd:x:980:1:/var/run/vboxadd:/bin/false
guest:x:1001:1001:/home/guest:/bin/bash
```

Задание 9

Вывожу список поддиректорий директории /home и их права. Замечаю, что все права есть только у создателя директории, у группы и остальных пользователей никаких прав нет



```
[guest@svchernaya ~]$ ls -l /home/  
итого 8  
drwx-----. 14 guest      guest      4096 map  7 20:47 guest  
drwx-----. 17 svchernaya svchernaya 4096 map  7 19:39 svchernaya
```

Рис. 12: Список поддиректорий директории /home

Задание 10

Проверяю есть ли какие-нибудь расширенные атрибуты на поддиректориях с помощью команды `lsattr`. Нет, никаких атрибутов у поддиректорий нет. Увидеть расширенные атрибуты у других пользователей так же не удалось

```
[guest@svchernaya ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/svchernaya
----- /home/guest
[guest@svchernaya ~]$ lsattr /home/guest/Документы
----- /home/guest/Документы/hernya.txt
[guest@svchernaya ~]$ lsattr /home/guest/Документы/hernya.txt
----- /home/guest/Документы/hernya.txt
```

Рис. 13: Просмотр атрибутов с помощью команды `lsattr`

Задание 11

Создаю в домашней директории поддиректорию `dir1` с помощью команды `mkdir`. Определяю командами `ls -l` и `lsattr` какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`. С помощью команды `ls -l` узнаю, что у создателя есть все права(на чтение, на записывание и на заход в директорию). У группы и остальных пользователей есть те же права, кроме записывания(создания файлов или удаление например). Команда `lsattr` ничего не выводит

```
[guest@svchernaya ~]$ ls -l
итого 0
drwxr-xr-x. 2 guest guest 64000 7 21:14 dir1
drwxr-xr-x. 2 guest guest 64000 7 20:47 Видео
drwxr-xr-x. 2 guest guest 24000 7 21:10 Документы
drwxr-xr-x. 2 guest guest 64000 7 20:47 Загрузки
drwxr-xr-x. 2 guest guest 64000 7 20:47 Изображения
drwxr-xr-x. 2 guest guest 64000 7 20:47 Музыка
drwxr-xr-x. 2 guest guest 64000 7 20:47 Общедоступные
drwxr-xr-x. 2 guest guest 64000 7 20:47 'Рабочий стол'
drwxr-xr-x. 2 guest guest 64000 7 20:47 Шаблоны
[guest@svchernaya ~]$ lsattr /home/guest/dir1
```

Задание 12

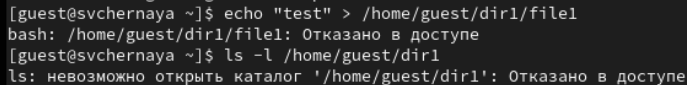
Снимаю все атрибуты с директории dir1 с помощью команды `chmod 000 dir1`.
Проверяю права доступа с помощью `ls -l`/Замечаю, что теперь у всех нет прав ни на что

```
[guest@svchernaya ~]$ chmod 000 dir1
[guest@svchernaya ~]$ ls -l
итого 0
d-----, 2 guest guest 6 map 7 21:14 dir1
drwxr-xr-x, 2 guest guest 6 map 7 20:47 видео
drwxr-xr-x, 2 guest guest 24 map 7 21:10 Документы
drwxr-xr-x, 2 guest guest 6 map 7 20:47 Загрузки
drwxr-xr-x, 2 guest guest 6 map 7 20:47 Изображения
drwxr-xr-x, 2 guest guest 6 map 7 20:47 Музыка
drwxr-xr-x, 2 guest guest 6 map 7 20:47 Общедоступные
drwxr-xr-x, 2 guest guest 6 map 7 20:47 'Рабочий стол'
drwxr-xr-x, 2 guest guest 6 map 7 20:47 Шаблоны
```

Рис. 15: `chmod 000`

Задание 13

Пытаюсь создать в директории dir1 файл fil1 командой `echo "test" > /home/guest/dir1/file1`. Отказ в доступе происходит из-за команды `chmod 000`, которая убирает все права у всех пользователей. Так же `ls -l /home/guest/dir1` показывает, что файла нет

A terminal window with a dark background and light text. It shows a user named 'guest' at a machine named 'svchernaya' in the home directory '~'. The user enters the command 'echo "test" > /home/guest/dir1/file1'. The shell returns the error 'bash: /home/guest/dir1/file1: Отказано в доступе'. The user then enters 'ls -l /home/guest/dir1'. The shell returns the error 'ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе'.

```
[guest@svchernaya ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@svchernaya ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе
```

Рис. 16: Попытка создать файл fil1 в dir1

Задание 14

Права дирек- тории	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Сме- на ди- ректо- рии	Просмотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов 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)	-	-	-	-	+	-	-

Задание 15

Операция	Минималь- ные права на директорию	Минималь- ные права на файл
Создание файла	d(300)	-
Удаление файла	d(300)	-
Чтение файла	d(100)	(400)
Запись в файл	d(100)	(200)
Переимено- вание файла	d(300)	(000)
Создание поддиректо-	d(300)	-

Выводы

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