

Лабораторная работа №2

Основы информационной безопасности

Бекназарова Виктория Тиграновна

29 февраля 2024

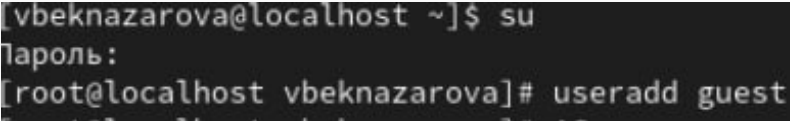
Российский университет дружбы народов, Москва, Россия

Целью данной работы является приобретение практических навыков установки операционной системы на виртуальную машину, настройки минимально необходимых для дальнейшей работы сервисов.

Научиться работать в консоли.

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.

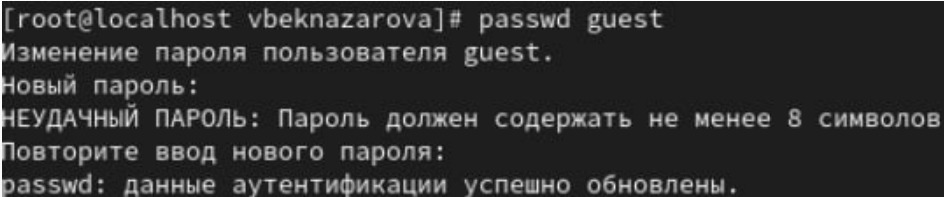
1. В установленной при выполнении предыдущей лабораторной работы операционной системе создаю учётную запись пользователя guest.

A terminal window with a dark background and light-colored text. The first line shows the prompt '[vbeknazarova@localhost ~]\$' followed by the command 'su'. The second line shows the prompt 'Пароль:' (Password:). The third line shows the prompt '[root@localhost vbeknazarova]#' followed by the command 'useradd guest'.

```
[vbeknazarova@localhost ~]$ su
Пароль:
[root@localhost vbeknazarova]# useradd guest
```

Рис. 1: Создание учетной записи для пользователя guest

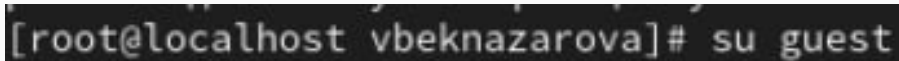
2. Задаю пароль для пользователя guest.

A terminal window with a black background and white text. The prompt is [root@localhost vbeknazarova]#. The command 'passwd guest' has been entered. The output shows the password change process for the user 'guest', including a warning about password strength and a confirmation message.

```
[root@localhost vbeknazarova]# passwd guest
Изменение пароля пользователя guest.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
```

Рис. 2: Создание пароля для пользователя guest

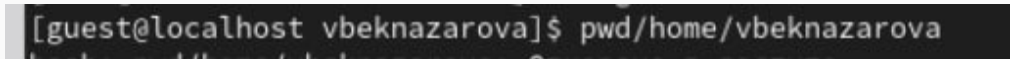
3. Входим в систему от имени пользователя guest.



```
[root@localhost vbeknazarova]# su guest
```

Рис. 3: Входим в систему от пользователя guest

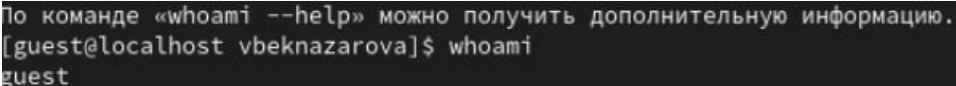
4. Определяем директорию, в которой мы находимся, командой `pwd`. Также определили, что она является домашней директорией.

A terminal window with a dark background. The prompt is [guest@localhost vbeknazarova]\$ and the command pwd/home/vbeknazarova has been entered. The output of the command is visible on the next line.

```
[guest@localhost vbeknazarova]$ pwd/home/vbeknazarova
```

Рис. 4: Домашняя директория

5. Уточняем имя пользователя командой `whoami`.

A terminal window with a black background and white text. The first line shows a command prompt and the command: `[guest@localhost vbeknazarova]$ whoami`. The second line shows the output of the command: `guest`.

```
По команде «whoami --help» можно получить дополнительную информацию.  
[guest@localhost vbeknazarova]$ whoami  
guest
```

Рис. 5: Командой `whoami` уточнили имя пользователя

6. Уточняем имя пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Сравниваем вывод `id` с выводом команды `groups`.

```
[guest@localhost vbeknazarova]$ id guest
uid=1001(guest) gid=1001(guest) группы=1001(guest)
[guest@localhost vbeknazarova]$ cat /etc/passwd
```

Рис. 6: Сравнили две команды

7. Сравниваем полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки.

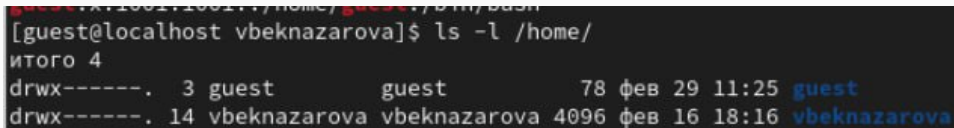
8. Просматриваем файл `/etc/passwd` командой `cat /etc/passwd`. Найдём в нём свою учётную запись. Определим `uid` пользователя. Определим `gid` пользователя. Сравним найденные значения с полученными в предыдущих пунктах. `Guest` имеет те же идентификаторы 1001, наш пользователь под идентификатором 1002.

```
[guest@localhost vbeknazarova]$ id guest
uid=1001(guest) gid=1001(guest) группы=1001(guest)
[guest@localhost vbeknazarova]$ 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
```

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

Рис. 8: Программа grep

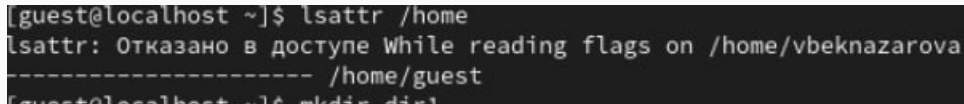
9. Определяем существующие в системе директории командой `ls -l /home/`.



```
guest@192.168.1.1: /home/ guest@192.168.1.1: /bin/bash
[guest@localhost vbeknazarova]$ ls -l /home/
итого 4
drwx-----.  3 guest          guest          78 фев 29 11:25 guest
drwx-----. 14 vbeknazarova vbeknazarova 4096 фев 16 18:16 vbeknazarova
```

Рис. 9: Существующие директории

10. Проверяем, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: `lsattr /home`. Нам не удалось увидеть расширенные атрибуты директорий других пользователей, только своей домашней директории.



```
[guest@localhost ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/vbknazarova
----- /home/guest
[guest@localhost ~]$ lsattr /home/guest
```

Рис. 10: Расширенные атрибуты

11. Создаём 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`.

```
[guest@localhost ~]$ mkdir dir1
[guest@localhost ~]$ ls -l
итого 0
drwxr-xr-x. 2 guest guest 6 фев 29 12:29 dir1
[guest@localhost ~]$
```

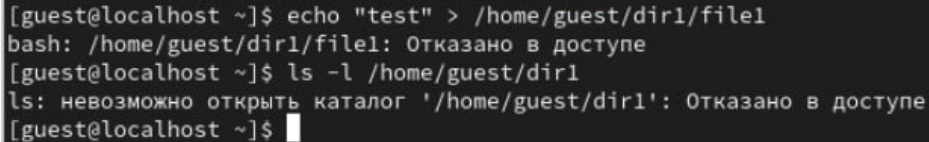
Рис. 11: Создаём поддиректорию

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

```
[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$ ls -l
итого 0
d----- . 2 guest guest 6 фев 29 12:29 dir1
```

Рис. 12: Снимаем все атрибуты

13. Создаем в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1`.
Поскольку ранее мы сняли все атрибуты, то тем самым лишили всех прав на взаимодействие с dir1.

A terminal window with a dark background and light-colored text. It shows a user named 'guest' at 'localhost' 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 'ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе'. The prompt returns to the user.

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

Рис. 13: Создаем файл

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

Создание файла - 1 Удаление файла - 2 Запись в файл - 3 Чтение файла - 4 Смена директории
- 5 Просмотр файлов в директории - 6 Переименование файла - 7 Смена атрибутов файла - 8

```
[root@localhost ~]# chmod 200 dir1/
[root@localhost ~]# ls -l
итого 4
-rw-----. 1 root root 1049 фев 15 20:47 anaconda-ks.cfg
d-w-----. 2 root root    6 фев 29 13:22 dir1
[root@localhost ~]# chmod 300 dir1/
[root@localhost ~]# ls -l
итого 4
-rw-----. 1 root root 1049 фев 15 20:47 anaconda-ks.cfg
d-wx-----. 2 root root    6 фев 29 13:22 dir1
[root@localhost ~]# chmod 400 dir1/
[root@localhost ~]# ls -l
итого 4
-rw-----. 1 root root 1049 фев 15 20:47 anaconda-ks.cfg
dr-----. 2 root root    6 фев 29 13:22 dir1
[root@localhost ~]# chmod 500 dir1/
[root@localhost ~]# ls -l
итого 4
-rw-----. 1 root root 1049 фев 15 20:47 anaconda-ks.cfg
dr-x-----. 2 root root    6 фев 29 13:22 dir1
[root@localhost ~]#
```

Рис. 14: Заполняем таблицу

Права директории	Права файла	1	2	3	4	5	6	7	8
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)	-	-	-	-	+	+	-	+
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)	-	-	+	-	+	-	-	+

Рис. 15: Установленные права и разрешенные действия

Права директории	Права файла	1	2	3	4	5	6	7	8
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)	-	-	-	+	+	+	-	+
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)	-	-	-	-	-	-	-	-

Рис. 16: Установленные права и разрешенные действия

Права директории	Права файла	1	2	3	4	5	6	7	8
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)	+	+	+	+	+	+	+	+

Рис. 17: Установленные права и разрешенные действия

Операция	Права на директорию	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)

Рис. 18: Минимальные права для совершения операций

В ходе выполнения лабораторной работы я получила практические навыки работы в консоли с атрибутами файлов, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Я научилась пользоваться консолью.