

Дискреционное разграничение прав в Linux. Основные атрибуты

Виноградова Варвара НФИбд-01-18¹

02 октября, 2021, Москва, Россия

¹Российский Университет Дружбы Народов

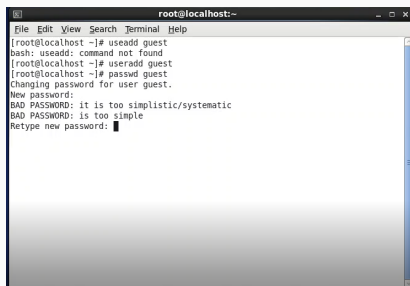
Цели и задачи работы

Цель лабораторной работы

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

Процесс выполнения лабораторной работы

В установленной при выполнении предыдущей лабораторной работы операционной системе создали учётную запись пользователя guest (используя учётную запись администратора) и задали пароль для пользователя guest (используя учётную запись администратора)



```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# useadd guest  
bash: useadd: command not found  
[root@localhost ~]# useradd guest  
[root@localhost ~]# passwd guest  
Changing password for user guest.  
New password:  
BAD PASSWORD: it is too simplistic/systematic  
BAD PASSWORD: it is too simple  
Retype new password:
```

Figure 1: Создала пользователя guest

Процесс выполнения лабораторной работы

Вошли в систему от имени пользователя guest

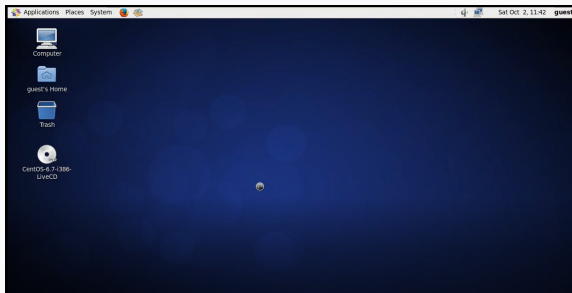
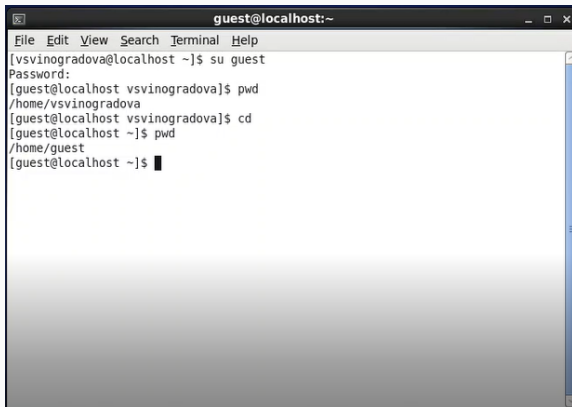


Figure 2: Рабочий экран guest

Процесс выполнения лабораторной работы

Командой `pwd` определили директорию, в которой находимся и определили является ли она домашней директорией

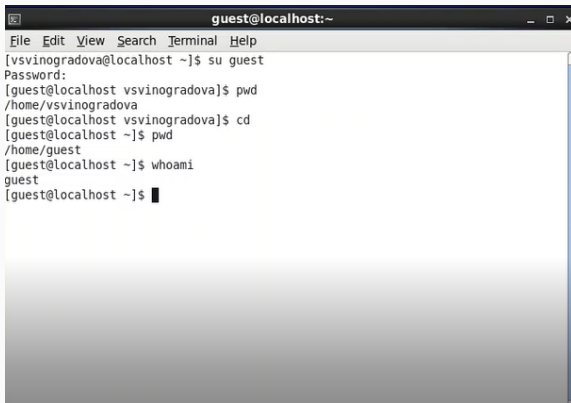


```
guest@localhost:~  
File Edit View Search Terminal Help  
[vsvinogradova@localhost ~]$ su guest  
Password:  
[guest@localhost vsvinogradova]$ pwd  
/home/vsvinogradova  
[guest@localhost vsvinogradova]$ cd  
[guest@localhost ~]$ pwd  
/home/guest  
[guest@localhost ~]$
```

Figure 3: Команда `pwd` и `cd`

Процесс выполнения лабораторной работы

Уточнили имя нашего пользователя командой `whoami`:

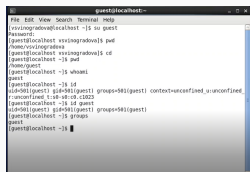
A terminal window titled 'guest@localhost:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows a sequence of commands and their outputs: switching to the 'guest' user, verifying the current directory with 'pwd' (output: /home/vsvinogradova), changing to the user's home directory with 'cd' (output: /home/guest), and finally running 'whoami' (output: guest).

```
guest@localhost:~  
File Edit View Search Terminal Help  
[vsvinogradova@localhost ~]$ su guest  
Password:  
[guest@localhost vsvinogradova]$ pwd  
/home/vsvinogradova  
[guest@localhost vsvinogradova]$ cd  
[guest@localhost ~]$ pwd  
/home/guest  
[guest@localhost ~]$ whoami  
guest  
[guest@localhost ~]$
```

Figure 4: Команда `whoami`

Процесс выполнения лабораторной работы

Уточнили имя пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. Сравнили вывод `id` с выводом команды `groups`. Видим, что `gid` и группы = 501(guest). Сравним полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки и убедимся, что они совпадают



```
guest@localhost:~$ id
uid=501(guest) gid=501(guest) groups=501(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0-c0-c0
guest@localhost:~$
```

Figure 5: Информация о пользователе guest

Процесс выполнения лабораторной работы

Посмотрим 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` имеет те же идентификаторы 501, наш пользователь под идентификатором 500.

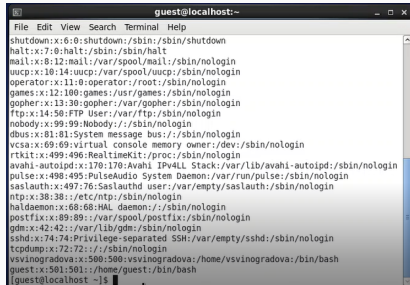
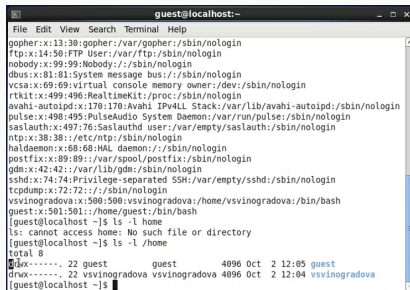
A screenshot of a terminal window titled 'guest@localhost:~'. The terminal displays the output of the 'cat /etc/passwd' command, showing a list of system and user accounts. The accounts listed are: shutdown, halt, mail, uucp, operator, games, gopher, ftp, nobody, dbus, vcsa, rtkit, avahi-autoipd, pulse, saslauthd, ntp, haldaemon, postfix, gdm, sshd, tcpdump, vsvinogradova, and guest. Each entry follows the format 'username:x:uid:gid:gecos:home:shell'. The 'guest' user is the last entry, with uid 501 and gid 501, and a home directory of /home/guest and shell of /bin/bash. The prompt at the bottom is '[guest@localhost ~]\$'.

Figure 6: Содержимое файла `/etc/passwd`

Процесс выполнения лабораторной работы

Определим существующие в системе директории командой
`ls -l /home/`

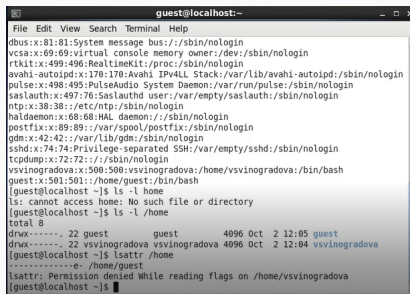


```
guest@localhost:~  
File Edit View Search Terminal Help  
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin  
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin  
nobody:x:99:99:Nobody:/:/sbin/nologin  
dbus:x:81:81:System message bus:/:/sbin/nologin  
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin  
rtkit:x:499:496:RealtimeKit:/proc:/sbin/nologin  
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin  
pulse:x:498:495:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin  
saslauth:x:497:76:Saslauthd user:/var/empty/saslauth:/sbin/nologin  
ntp:x:38:38:/:etc/ntp:/sbin/nologin  
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin  
postfix:x:89:89:/:var/spool/postfix:/sbin/nologin  
gdm:x:42:42:/:var/lib/gdm:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin  
tcpdump:x:72:72:/:/sbin/nologin  
vsvinogradova:x:500:500:vsvinogradova:/home/vsvinogradova:/bin/bash  
guest:x:501:501:/:home/guest:/bin/bash  
[guest@localhost ~]$ ls -l /home  
ls: cannot access /home: No such file or directory  
[guest@localhost ~]$ ls -l /home  
total 8  
drwx----- 22 guest      guest      4096 Oct 2 12:05 guest  
drwx----- 22 vsvinogradova vsvinogradova 4096 Oct 2 12:04 vsvinogradova  
[guest@localhost ~]$
```

Figure 7: Команда `ls -l /home/`

Процесс выполнения лабораторной работы

Проверили, 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:~  
File Edit View Search Terminal Help  
dbus:x:81:81:System message bus:/:/sbin/nologin  
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin  
rtkit:x:499:496:RealtimeKit:/proc:/sbin/nologin  
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin  
pulse:x:498:495:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin  
saslauth:x:497:76:Saslauthd user:/var/empty/saslauth:/sbin/nologin  
ntp:x:38:38:::/etc/ntp:/sbin/nologin  
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin  
postfix:x:89:89::/var/spool/postfix:/sbin/nologin  
gdm:x:42:42::/var/lib/gdm:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin  
tcpdump:x:72:72:::/sbin/nologin  
vsvinogradova:x:500:500:vsvinogradova:/home/vsvinogradova:/bin/bash  
guest:x:501:501::/home/guest:/bin/bash  
[guest@localhost ~]$ ls -l /home  
ls: cannot access /home: No such file or directory  
[guest@localhost ~]$ ls -l /home  
total 8  
drwx----- 22 guest      guest      4096 Oct  2 12:05 guest  
drwx----- 22 vsvinogradova vsvinogradova 4096 Oct  2 12:04 vsvinogradova  
[guest@localhost ~]$ lsattr /home  
-----e- /home/guest  
lsattr: Permission denied while reading flags on /home/vsvinogradova  
[guest@localhost ~]$
```

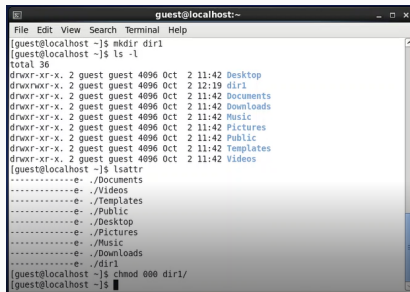
Figure 8: Расширенные атрибуты

Создали 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`.

Сняли с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверили с `ls -l` помощью правильность выполнения команды `chmod`.

Процесс выполнения лабораторной работы

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



```
guest@localhost:~  
File Edit View Search Terminal Help  
[guest@localhost ~]$ mkdir dir1  
[guest@localhost ~]$ ls -l  
total 36  
drwxr-xr-x. 2 guest guest 4096 Oct 2 11:42 Desktop  
drwxr-xr-x. 2 guest guest 4096 Oct 2 12:19 dir1  
drwxr-xr-x. 2 guest guest 4096 Oct 2 11:42 Documents  
drwxr-xr-x. 2 guest guest 4096 Oct 2 11:42 Downloads  
drwxr-xr-x. 2 guest guest 4096 Oct 2 11:42 Music  
drwxr-xr-x. 2 guest guest 4096 Oct 2 11:42 Pictures  
drwxr-xr-x. 2 guest guest 4096 Oct 2 11:42 Public  
drwxr-xr-x. 2 guest guest 4096 Oct 2 11:42 Templates  
drwxr-xr-x. 2 guest guest 4096 Oct 2 11:42 Videos  
[guest@localhost ~]$ lsattr  
-----e- ./Documents  
-----e- ./Videos  
-----e- ./Templates  
-----e- ./Public  
-----e- ./Desktop  
-----e- ./Pictures  
-----e- ./Music  
-----e- ./Downloads  
-----e- ./dir1  
[guest@localhost ~]$ chmod 000 dir1/  
[guest@localhost ~]$
```

Figure 9: Снятие атрибутов с директории

Права и разрешённые 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)

Figure 10: Минимальные права для совершения операций

Выводы по проделанной работе

В ходе выполнения лабораторной работы были получены навыки работы с атрибутами файлов и сведения о разграничении доступа.