

Дискреционное разграничение прав в Linux. Основные атрибуты.

Алхимова Дарья Сергеевна НБИ-01-19¹

15 сентября, 2022

¹Российский Университет Дружбы Народов

Информация

- Алхимова Дарья Сергеевна
- студентка 4 курса
- группы НБИбд-01-19
- Российский университет дружбы народов
- 1032191645@rudn.ru

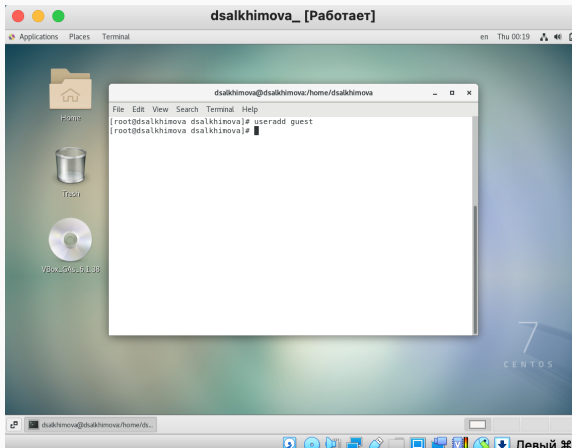
Цель работы

Целью данной работы является получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux1.

Выполнение лабораторной работы

Создала новую учетную запись

В установленной при выполнении предыдущей лабораторной работы операционной системе создала учетную запись пользователя `guest` командой `useradd guest` (рис. 1)



Задала пароль для пользователя guest

Задала пароль для пользователя guest командой `passwd guest`

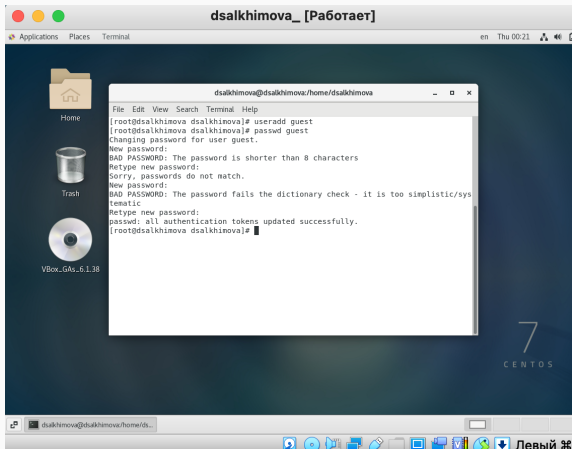


Figure 2: Установка пароля для пользователя

Авторизовалась и определила директорию, в которой я нахожусь

С помощью команды `pwd`.

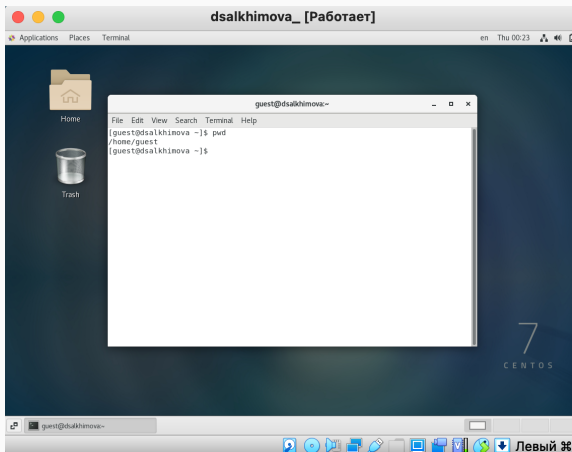


Figure 3: Проверка текущей директории

Получила имя пользователя командой `'whoami'`

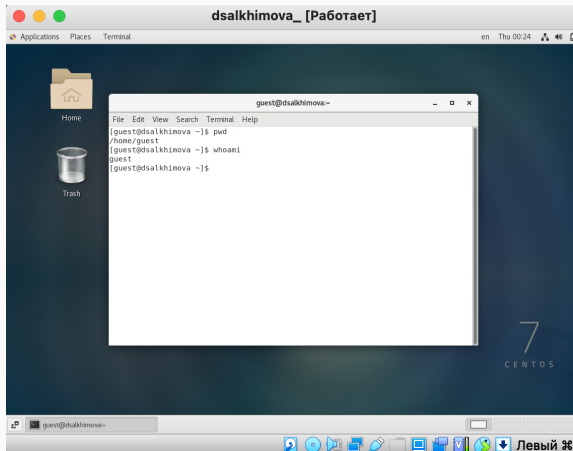


Figure 4: Имя пользователя

Уточнила имя моего пользователя, его группу, а так же группы, куда входит пользователь

С помощью команды `id`

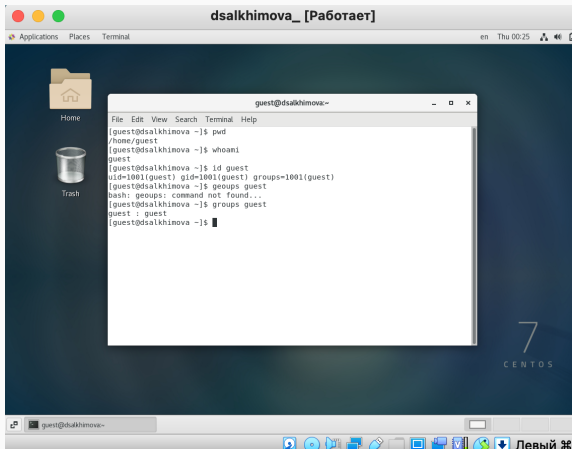
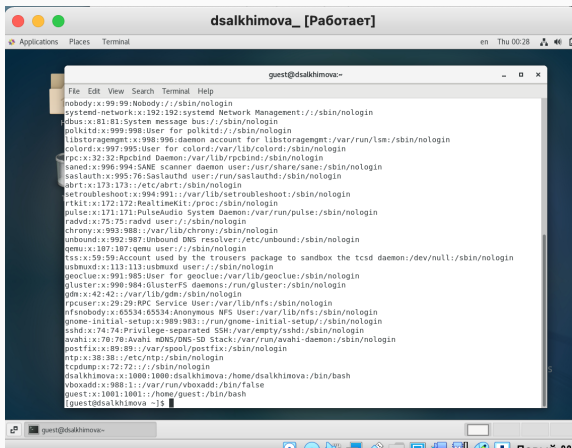


Figure 5: Информация о пользователях командой `id`

Просмотрела файл /etc/passwd командой cat
/etc/passwd

Определила uid и gid пользователя: 1001(guest).
Найденные значения совпадают с полученными в
предыдущих пунктах.



The screenshot shows a terminal window titled "dsalkhimova_ [Работает]" with a menu bar (File, Edit, View, Search, Terminal, Help) and a status bar (Applications, Places, Terminal, en, Thu 00:28). The terminal displays the output of the 'cat /etc/passwd' command, listing system users and regular users. The 'guest' user is listed at the bottom with uid 1001 and gid 1001.

```
nobody:x:99:99:Nobody:/:/sbin/nologin
system-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
libstoragemgmt:x:998:996:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
colord:x:997:995:User for colord:/var/lib/colord:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
sane:x:996:994:SANE scanner daemon user:/usr/share/sane:/sbin/nologin
sasauthd:x:995:76:Sasauthd user:/run/sasauthd:/sbin/nologin
abrt:x:173:173:/:etc/abrt:/sbin/nologin
setroubleshoot:x:994:991:/:var/lib/setroubleshoot:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
radvd:x:75:75:radvd user:/sbin/nologin
chrony:x:993:988:/:var/lib/chrony:/sbin/nologin
unbound:x:992:987:Unbound DNS resolver:/etc/unbound:/sbin/nologin
qemu:x:107:107:qemu user:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
geoclue:x:991:985:User for geoclue:/var/lib/geoclue:/sbin/nologin
gluster:x:990:984:GlusterFS daemons:/run/gluster:/sbin/nologin
gdm:x:42:42:/:var/lib/gdm:/sbin/nologin
rcpuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
gnome-initial-setup:x:989:983:/:run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
postfix:x:89:89:/:var/spool/postfix:/sbin/nologin
ntp:x:38:38:/:etc/ntp:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
dsalkhimova:x:1000:1000:dsalkhimova:/home/dsalkhimova:/bin/bash
vboxadd:x:988:1:/:var/run/vboxadd:/bin/false
guest:x:1001:1001:/:home/guest:/bin/bash
guest@dsalkhimova ~$
```

Определила существующие директории

С помощью команды `ls -l /home/`



```
guest@dsalkhinova: ~$ ls -l /home/
total 8
drwx-----, 15 dsalkhinova dsalkhinova 4096 Sep  8 08:00 dsalkhinova
drwx-----, 15 guest      guest      4096 Sep 15 00:22 guest
[guest@dsalkhinova ~]$
```

Figure 7: Определение существующих директорий

Проверила, какие расширенные атрибуты установлены на поддиректориях директории /home

Доступ к расширенным атрибутам директории, а также директории ☒ других пользователей ☒ был запрещен.

A terminal window showing a user running the command 'lsattr /home'. The output is 'lsattr: Permission denied while reading flags on /home/dsalkhimova'. The user then runs 'lsattr /home/guest' and the output is '----- /home/guest'.

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

Figure 8: Расширенные атрибуты директорий

Создала в домашней директории поддиректорию dir1

Определила командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`

```
[guest@dsalkhimova ~]$ mkdir dir1
[guest@dsalkhimova ~]$ cd dir1
[guest@dsalkhimova dir1]$ ls -l
total 0
[guest@dsalkhimova dir1]$ cd ..
[guest@dsalkhimova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Desktop
drwxrwxr-x. 2 guest guest 6 Sep 15 00:34 dir1
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Documents
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Music
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Public
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Templates
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Videos
[guest@dsalkhimova ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
[guest@dsalkhimova ~]$
```

Figure 9: Создание поддиректории

Сняла с директории dir1 все атрибуты

Права стали удалены у всех пользователей.

```
[guest@dsalkhimova ~]$ chmod 000 dir1
[guest@dsalkhimova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Desktop
d----- . 2 guest guest 6 Sep 15 00:34 dir1
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Documents
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Music
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Public
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Templates
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Videos
[guest@dsalkhimova ~]$
```

Figure 10: Снятие атрибутов директории

Попыталась создать в директории dir1 файл file1

Получила отказ в выполнении операции по созданию файла, поскольку на предыдущем шаге я убрала все права с директории dir1

```
[guest@salkhimova ~]$ chmod 000 dir1
[guest@salkhimova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Desktop
d----- 2 guest guest 6 Sep 15 00:34 dir1
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Documents
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Music
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Public
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Templates
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Videos
[guest@salkhimova ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@salkhimova ~]$ ls -l /home/guest/dir1/file1
ls: cannot access /home/guest/dir1/file1: Permission denied
[guest@salkhimova ~]$ ls -l /home/guest/dir1
ls: cannot open directory /home/guest/dir1: Permission denied
[guest@salkhimova ~]$ cd dir1
bash: cd: dir1: Permission denied
[guest@salkhimova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Desktop
d----- 2 guest guest 6 Sep 15 00:34 dir1
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Documents
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Music
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Public
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Templates
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Videos
[guest@salkhimova ~]$
```

Figure 11: Создание файла в директории

Определила минимальные права для выполнения операции

На основании анализа доступных операций с различными наборами прав на директорию и файл

Операция	Мин. права на директорию	Мин. 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 12: Минимальные права

Вывод

В процессе выполнения данной лабораторной работы я получила практические навыки работы в консоли с атрибутами файлов, а также закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux1.