

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

ОТЧЕТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ № 2

Дисциплина: Информационная безопасность

*Тема: Дискреционное разграничение прав в Linux. Основные
атрибуты*

Студент: Ломакина София Васильевна

Группа: НФИбд-02-19

МОСКВА

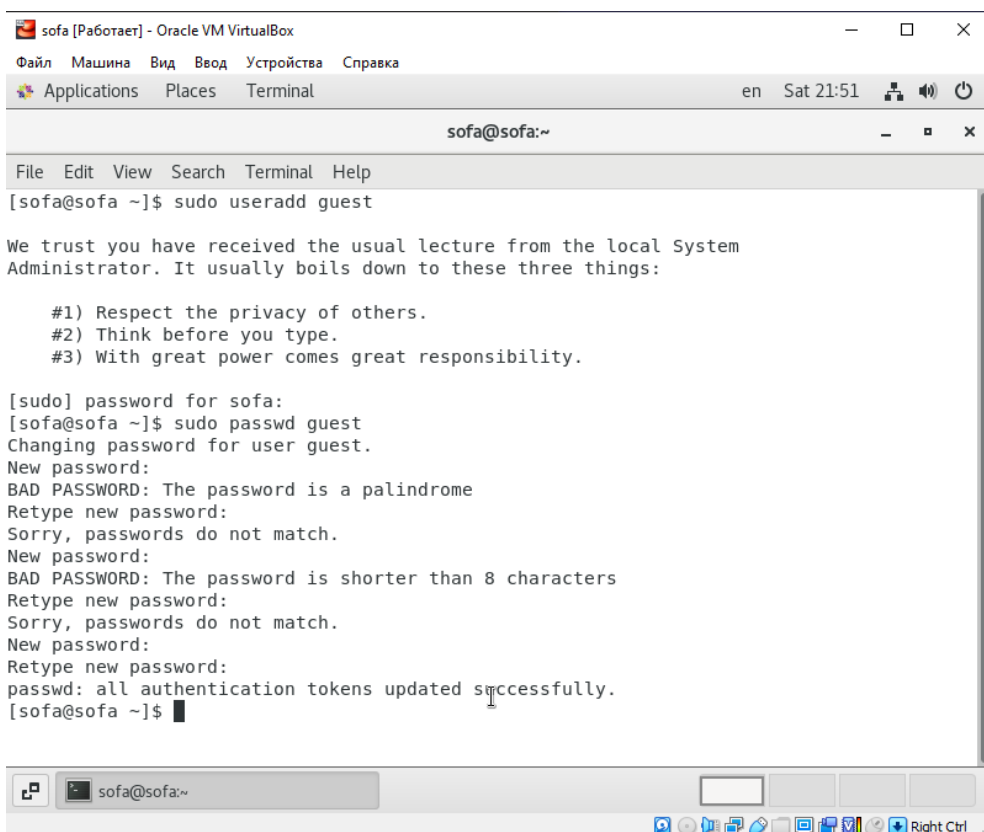
2022 г.

Цель работы

Цель лабораторной работы No2 - 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.

Выполнение лабораторной работы

В установленной при выполнении предыдущей лабораторной работы операционной системе создали учетную запись пользователя guest (используя учетную запись администратора) с помощью команды `useradd guest` и задали пароль для пользователя guest (используя учетную запись администратора) с помощью команды `passwd guest`.



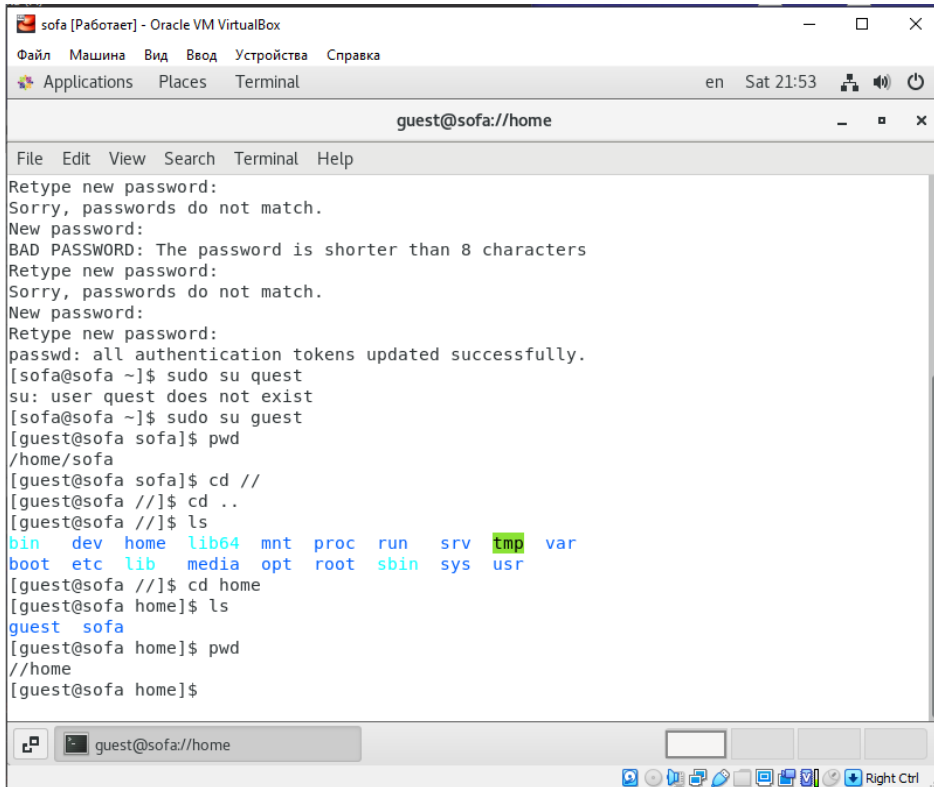
```
sofa [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Applications  Places  Terminal  en  Sat 21:51
sofa@sofa:~
File Edit View Search Terminal Help
[sofa@sofa ~]$ sudo useradd guest

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.

[sudo] password for sofa:
[sofa@sofa ~]$ sudo passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[sofa@sofa ~]$
```

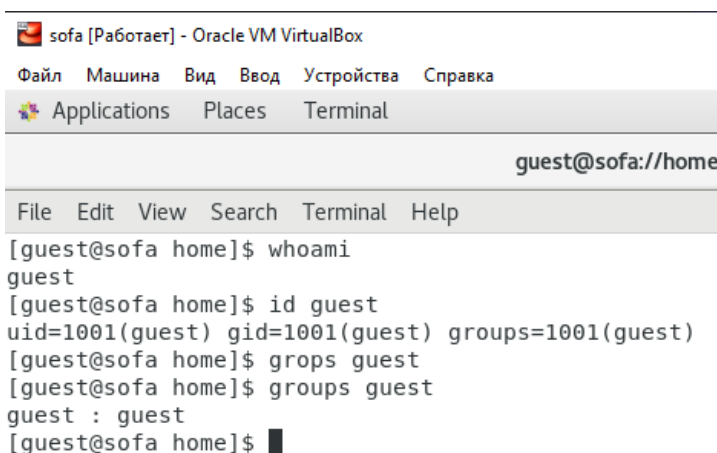
Вошли в систему от имени пользователя `guest` и командой `pwd` определили директорию, в которой находимся и определили является ли она домашней директорией.



```
sofa [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Applications  Places  Terminal  en  Sat 21:53
guest@sofa://home
File Edit View Search Terminal Help
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[sofa@sofa ~]$ sudo su quest
su: user quest does not exist
[sofa@sofa ~]$ sudo su guest
[guest@sofa sofa]$ pwd
/home/sofa
[guest@sofa sofa]$ cd ../
[guest@sofa //]$ cd ..
[guest@sofa //]$ ls
bin  dev  home  lib64  mnt  proc  run  srv  tmp  var
boot  etc  lib  media  opt  root  sbin  sys  usr
[guest@sofa //]$ cd home
[guest@sofa home]$ ls
guest  sofa
[guest@sofa home]$ pwd
//home
[guest@sofa home]$
```

Уточнили имя пользователя командой `whoami`.

Уточнили имя пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Сравнили вывод `id` с выводом команды `groups`. Видим, что `uid`, `gid` и группы = 1001(guest).



```
sofa [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Applications  Places  Terminal
guest@sofa://home
File Edit View Search Terminal Help
[guest@sofa home]$ whoami
guest
[guest@sofa home]$ id guest
uid=1001(guest) gid=1001(guest) groups=1001(guest)
[guest@sofa home]$ groups guest
[guest@sofa home]$ groups guest
guest : guest
[guest@sofa home]$
```

Сравнили полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки и убедились, что они совпадают. Просмотрели файл `/etc/passwd` с помощью команды `cat /etc/passwd`. Нашли в нём свою учётную запись. Определили `uid` и `gid` пользователя. Guest имеет те же идентификаторы 1001, которые также были получены в предыдущих пунктах.

```
sofa [Работаer] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Applications  Places  Terminal
en  Sat 21:57
guest@sofa:/home
File Edit View Search Terminal Help
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
rpcuser: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/sshd:/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
sofa:x:1000:1000:sofa:/home/sofa:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
[guest@sofa home]$
```

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

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

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@sofa home]$ ls -l /home/
total 4
drwx-----. 5 guest guest 107 Sep 17 21:51 guest
drwx-----. 15 sofa sofa 4096 Sep 17 21:13 sofa
[guest@sofa home]$
```

```
[guest@sofa home]$ lsattr /home
lsattr: Permission denied While reading flags on /home/sofa
----- /home/guest
[guest@sofa home]$ █
```

Создали в домашней директории поддиректорию dir1 командой `mkdir dir1`.

Определили с помощью команд `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию dir1.

```
[guest@sofa home]$ cd quest
bash: cd: quest: No such file or directory
[guest@sofa home]$ cd ~
[guest@sofa ~]$ ls
[guest@sofa ~]$ mkdir dir1
[guest@sofa ~]$ ls
dir1
[guest@sofa ~]$ ls -l dir1
total 0

[guest@sofa ~]$ ls -l
total 0
drwxrwxr-x. 2 guest guest 6 Sep 17 22:10 dir1
[guest@sofa ~]$ lsattr /home/guest/dir1
[guest@sofa ~]$ lsattr /home/guest
----- /home/guest/dir1
[guest@sofa ~]$ ls
dir1
[guest@sofa ~]$ █
```

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

```
[guest@sofa ~]$ chmod 000 dir1
[guest@sofa ~]$ ls -l
total 0
d----- . 2 guest guest 6 Sep 17 22:10 dir1
[guest@sofa ~]$ █
```

Попытались создать в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1`. Поскольку ранее мы отозвали все атрибуты, то тем самым

лишили пользователя всех прав на взаимодействие с dir1, в том числе и на создание файлов.

```
[guest@sofa ~]$ echo "test" > /home/quest/dir1/file1
bash: /home/quest/dir1/file1: No such file or directory
[guest@sofa ~]$ ls -l /home/quest/dir1
ls: cannot open directory /home/quest/dir1: Permission denied
[guest@sofa ~]$ ls
dir1
[guest@sofa ~]$ cd dir1
bash: cd: dir1: Permission denied
[guest@sofa ~]$ ls
dir1
—
```

Заполним таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определяем опытным путем, какие операции разрешены, а какие нет. Если операция разрешена, заносим в таблицу знак «+», если не разрешена, знак «-».

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

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)	-	-	+	-	+	-	-	+
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)	-	-	-	-	-	-	-	-
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)	+	+	+	+	+	+	+	+

На основании таблицы выше определили минимально необходимые права для выполнения операций внутри директории dir1 и заполнили таблицу минимальных прав для совершения операций. Для заполнения последних двух строк опытным путем проверили минимальные права.

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)