

Отчёт по лабораторной работе №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Пименов Михаил НБИ-01-19

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
3	Вывод	13
	Список литературы	14

List of Figures

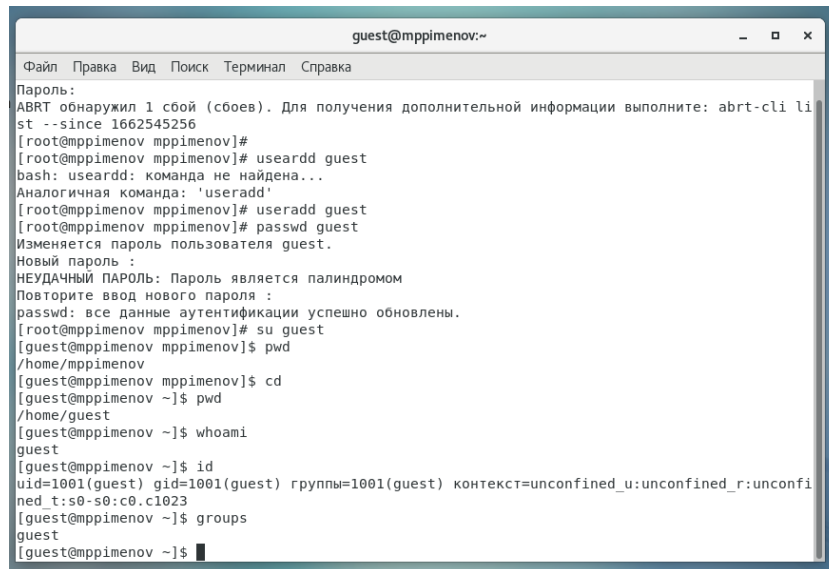
2.1	Информация о пользователе guest	6
2.2	Содержимое файла /etc/passwd	6
2.3	Расширенные атрибуты	7
2.4	Снятие атрибутов с директории	8
2.5	Заполнение таблицы	8

1 Цель 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.

2 Выполнение лабораторной работы

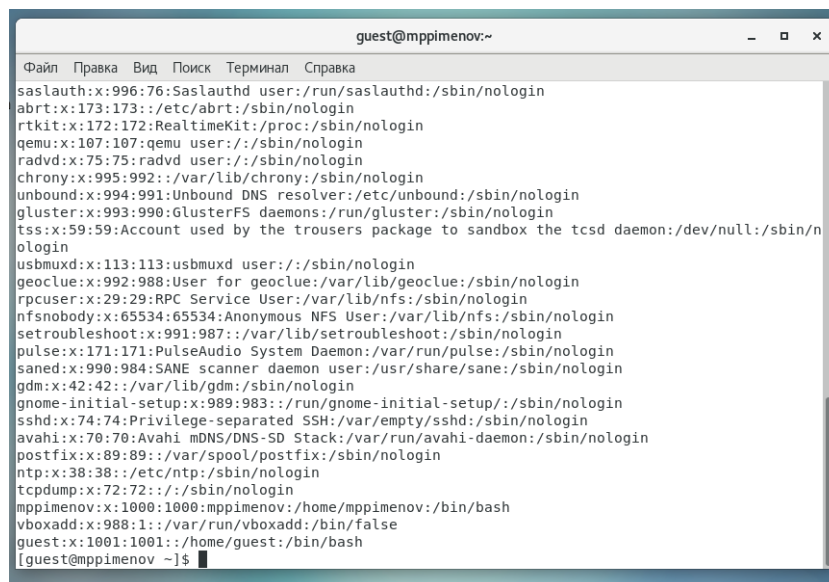
1. В установленной при выполнении предыдущей лабораторной работы операционной системе создали учётную запись пользователя `guest` (используя учётную запись администратора) и задали пароль для пользователя `guest` (используя учётную запись администратора)
2. Вошли в систему от имени пользователя `guest`
3. Командой `pwd` определили директорию, в которой находимся и определили является ли она домашней директорией
4. Уточнили имя нашего пользователя командой `whoami`:
5. 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 = `1001(guest)`
6. Сравним полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки и убедимся, что они совпадают



```
guest@mppimenov:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
Пароль:  
ABRT обнаружил 1 сбой (сбоев). Для получения дополнительной информации выполните: abrt-cli li  
st --since 1662545256  
[root@mppimenov mppimenov]#  
[root@mppimenov mppimenov]# useradd guest  
bash: useradd: команда не найдена...  
Аналогичная команда: 'useradd'  
[root@mppimenov mppimenov]# useradd guest  
[root@mppimenov mppimenov]# passwd guest  
Изменяется пароль пользователя guest.  
Новый пароль :  
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом  
Повторите ввод нового пароля :  
passwd: все данные аутентификации успешно обновлены.  
[root@mppimenov mppimenov]# su guest  
[guest@mppimenov mppimenov]# pwd  
/home/mppimenov  
[guest@mppimenov mppimenov]$ cd  
[guest@mppimenov ~]$ pwd  
/home/guest  
[guest@mppimenov ~]$ whoami  
guest  
[guest@mppimenov ~]$ id  
uid=1001(guest) gid=1001(guest) rгруппы=1001(guest) контекст=unconfined_u:unconfined_r:unconfi  
ned_t:s0-s0:c0.c1023  
[guest@mppimenov ~]$ groups  
guest  
[guest@mppimenov ~]$
```

Figure 2.1: Информация о пользователе guest

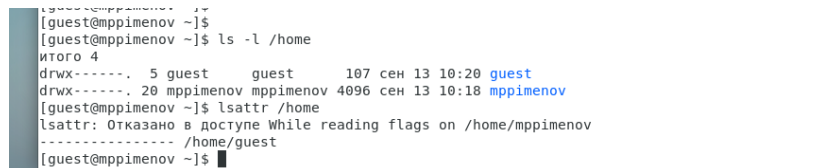
7. Просмотрим файл `/etc/passwd` Командой: `cat /etc/passwd`. Найдем в нём свою учётную запись. Определим `uid` пользователя. Определим `gid` пользователя. Сравним найденные значения с полученными в предыдущих пунктах. Guest имеет те же идентификаторы 1001, наш пользователь под идентификатором 1002.



```
guest@mppimenov:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
sasauth:x:996:76:Sasauthd user:/run/sasauthd:/sbin/nologin  
abrt:x:173:173::/etc/abrt:/sbin/nologin  
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin  
qemu:x:107:107:qemu user:/:/sbin/nologin  
radvd:x:75:75:radvd user:/:/sbin/nologin  
chrony:x:995:992::/var/lib/chrony:/sbin/nologin  
unbound:x:994:991:Unbound DNS resolver:/etc/unbound:/sbin/nologin  
gluster:x:993:990:GlusterFS daemons:/run/gluster:/sbin/nologin  
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/n  
ologin  
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin  
geoclue:x:992:988:User for geoclue:/var/lib/geoclue:/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  
setroubleshoot:x:991:987::/var/lib/setroubleshoot:/sbin/nologin  
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin  
saned:x:990:984:SANE scanner daemon user:/usr/share/sane:/sbin/nologin  
gdm:x:42:42::/var/lib/gdm:/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  
mppimenov:x:1000:1000:mppimenov:/home/mppimenov:/bin/bash  
vboxadd:x:988:1::/var/run/vboxadd:/bin/false  
guest:x:1001:1001::/home/guest:/bin/bash  
[guest@mppimenov ~]$
```

Figure 2.2: Содержимое файла `/etc/passwd`

8. Определим существующие в системе директории командой `ls -l /home/`
9. 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@mppimenov ~]$  
[guest@mppimenov ~]$ ls -l /home  
итого 4  
drwx-----, 5 guest      guest      107 сен 13 10:20 guest  
drwx-----, 20 mppimenov mppimenov 4096 сен 13 10:18 mppimenov  
[guest@mppimenov ~]$ lsattr /home  
lsattr: Отказано в доступе While reading flags on /home/mppimenov  
----- /home/guest  
[guest@mppimenov ~]$
```

Figure 2.3: Расширенные атрибуты

10. 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`.
11. Сняли с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверили с `ls -l` помощью правильность выполнения команды `chmod`.
12. 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@mppimenov:~  
Файл Правка Вид Поиск Терминал Справка  
guest:x:1001:1001:./home/guest:/bin/bash  
[guest@mppimenov ~]$  
[guest@mppimenov ~]$  
[guest@mppimenov ~]$ ls -l /home  
итого 4  
drwx-----. 5 guest guest 107 сен 13 10:20 guest  
drwx-----. 20 mppimenov mppimenov 4096 сен 13 10:18 mppimenov  
[guest@mppimenov ~]$ lsattr /home  
lsattr: Отказано в доступе While reading flags on /home/mppimenov  
----- /home/guest  
[guest@mppimenov ~]$  
[guest@mppimenov ~]$  
[guest@mppimenov ~]$ cd  
[guest@mppimenov ~]$ mkdir dir1  
[guest@mppimenov ~]$ ls -l  
итого 0  
drwxrwxr-x. 2 guest guest 6 сен 13 10:24 dir1  
[guest@mppimenov ~]$ lsattr  
----- ./dir1  
[guest@mppimenov ~]$ chmod 000 dir1  
[guest@mppimenov ~]$ ls -l  
итого 0  
d-----. 2 guest guest 6 сен 13 10:24 dir1  
[guest@mppimenov ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@mppimenov ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@mppimenov ~]$
```

Figure 2.4: Снятие атрибутов с директории

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

```
guest@mppimenov:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@mppimenov ~]$ echo "test" > /home/guest/dir1/file1  
[guest@mppimenov ~]$ cd dir1/  
[guest@mppimenov dir1]$ chmod 000 fi  
chmod: невозможно получить доступ к «fi»: Нет такого файла или каталога  
[guest@mppimenov dir1]$ ls  
ls: невозможно открыть каталог .: Отказано в доступе  
[guest@mppimenov dir1]$ chmod 000 file1  
[guest@mppimenov dir1]$ rm file 1  
rm: невозможно удалить «file»: Нет такого файла или каталога  
rm: невозможно удалить «1»: Нет такого файла или каталога  
[guest@mppimenov dir1]$ rm file1  
rm: удалить защищенный от записи обычный файл «file1»? y  
[guest@mppimenov dir1]$  
[guest@mppimenov dir1]$ ls -l  
ls: невозможно открыть каталог .: Отказано в доступе  
[guest@mppimenov dir1]$ cd ..  
[guest@mppimenov ~]$ echo "test" > /home/guest/dir1/file1  
[guest@mppimenov ~]$ chmod 400 /home/guest/dir1/file1  
[guest@mppimenov ~]$ chmod 100 dir1  
[guest@mppimenov ~]$ cat /home/guest/dir1/file1  
test  
[guest@mppimenov ~]$ chmod 200 /home/guest/dir1/file1  
[guest@mppimenov ~]$ echo "test" > /home/guest/dir1/file1  
[guest@mppimenov ~]$ chmod 300 dir1/  
[guest@mppimenov ~]$ mv dir1/file1 dir1/file2  
[guest@mppimenov ~]$ mkdir dir1/dir2  
[guest@mppimenov ~]$ rmdir dir1/dir2  
[guest@mppimenov ~]$
```

Figure 2.5: Заполнение таблицы

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

Table 2.1: Установленные права и разрешённые действия

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)	-	-	-	-	-	-	-	-

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

Права директории	Права файла	1	2	3	4	5	6	7	8
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 2.2. Для заполнения последних двух строк опытным путем проверили минимальные права.

Table 2.2: Минимальные права для совершения операций

Операция	Права на директорию	Права на файл
Создание файла	d-wx----- (300)	----- (000)
Удаление файла	d-wx----- (300)	----- (000)

Операция	Права на директорию	Права на файл
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)

3 Вывод

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

Список литературы

1. Теория разграничения прав пользователей
2. Разрешения доступа к файлам