

Лабораторная работа № 3

Дискреционное разграничение прав в Linux. Два пользователя

Абакумов Егор Александрович

Содержание

Цель работы	5
Задание	6
Теоретическое описание	7
Ход работы	9
Выводы	17
Список литературы	18

List of Figures

0.1	Добавление нового пользователя	9
0.2	pwd для guest	10
0.3	pwd для guest2	10
0.4	Группы для guest	10
0.5	Группы для guest2	11
0.6	/etc/groups	11
0.7	Регистрация guest2	12
0.8	Разрешение на домашнюю папку guest	12
0.9	Нулевые права на dir1	12
0.10	Пример ввода команд для проверки прав	13
0.11	Скрипт для guest	14
0.12	Скрипт для guest2	14
0.13	Установленные права и разрешённые действия	15

List of Tables

Цель работы

Получение практических навыков работы в консоли с атрибутами файлов для групп пользователей.

Задание

Провести эксперимент по выявлению минимально необходимых прав для совершения различных действий для групп пользователей.

Теоретическое описание

В операционной системе Linux есть много отличных функций безопасности, но она из самых важных - это система прав доступа к файлам. Linux, как последователь идеологии ядра Linux в отличие от Windows, изначально проектировался как многопользовательская система, поэтому права доступа к файлам в Linux продуманы очень хорошо.

Изначально каждый файл имел три параметра доступа [1]:

- Чтение - разрешает получать содержимое файла, но на запись нет. Для каталога позволяет получить список файлов и каталогов, расположенных в нем;
- Запись - разрешает записывать новые данные в файл или изменять существующие, а также позволяет создавать и изменять файлы и каталоги;
- Выполнение - вы не можете выполнить программу, если у нее нет флага выполнения. Этот атрибут устанавливается для всех программ и скриптов, именно с помощью него система может понять, что этот файл нужно запускать как программу.

Каждый файл имеет три категории пользователей, для которых можно устанавливать различные сочетания прав доступа:

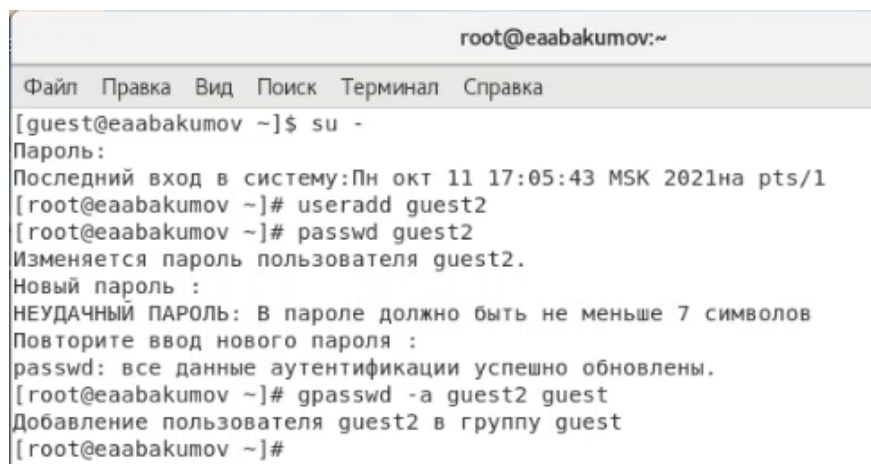
- Владелец - набор прав для владельца файла, пользователя, который его создал или сейчас установлен его владельцем. Обычно владелец имеет все права, чтение, запись и выполнение.
- Группа - любая группа пользователей, существующая в системе и привязанная к файлу. Но это может быть только одна группа и обычно это группа владельца, хотя для файла можно назначить и другую группу.

- Остальные - все пользователи, кроме владельца и пользователей, входящих в группу файла.

Для управления правами используется команда `chmod`. При использовании `chmod` вы можете устанавливать разрешения для пользователя (`user`), группы (`group`) и других (`other`). Вы можете использовать эту команду в двух режимах: относительный режим и абсолютный режим. В абсолютном режиме три цифры используются для установки основных разрешений [2].

Ход работы

1. Создаем в ОС двух новых пользователей guest и guest2. Так как первый у нас уже был, нам нужен всего один. Задаем ему пароль и добавляем его в группу guest (иллюстр. 0.1). Командой `pwd` проверяем местонахождение консоли. Видим, что guest находится в своей домашней директории, о чем свидетельствует значок тильда в приглашении командной строки (иллюстр. 0.2). Guest2 же находится в той же папке, однако для него она не домашняя, что показывает нам имя пользователя-владельца папки в приглашении командной строки (иллюстр. 0.3).

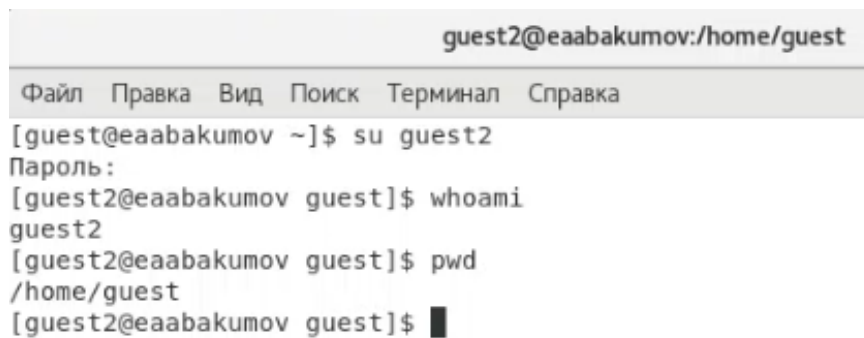


```
root@eaabakumov:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
[guest@eaabakumov ~]$ su -  
Пароль:  
Последний вход в систему: Пн окт 11 17:05:43 MSK 2021 на pts/1  
[root@eaabakumov ~]# useradd guest2  
[root@eaabakumov ~]# passwd guest2  
Изменяется пароль пользователя guest2.  
Новый пароль :  
НЕУДАЧНЫЙ ПАРОЛЬ: В пароле должно быть не меньше 7 символов  
Повторите ввод нового пароля :  
passwd: все данные аутентификации успешно обновлены.  
[root@eaabakumov ~]# gpasswd -a guest2 guest  
Добавление пользователя guest2 в группу guest  
[root@eaabakumov ~]#
```

Figure 0.1: Добавление нового пользователя

```
[guest@eaabakumov ~]$ whoami
guest
[guest@eaabakumov ~]$ pwd
/home/guest
```

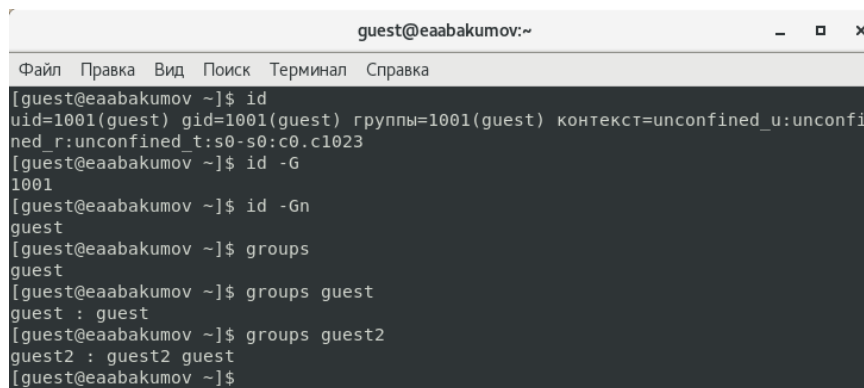
Figure 0.2: pwd для guest



```
guest2@eaabakumov:/home/guest
Файл  Правка  Вид  Поиск  Терминал  Справка
[guest@eaabakumov ~]$ su guest2
Пароль:
[guest2@eaabakumov guest]$ whoami
guest2
[guest2@eaabakumov guest]$ pwd
/home/guest
[guest2@eaabakumov guest]$
```

Figure 0.3: pwd для guest2

2. Проверяем командами `id`, `id -G`, `id -Gn` и `groups` к каким группам принадлежат пользователи. Видим, что `guest` входит только в группу `guest`, а `guest2` входит и в группу `guest`, и в группу `guest2` (иллюстр. 0.4, 0.5).



```
guest@eaabakumov:~
Файл  Правка  Вид  Поиск  Терминал  Справка
[guest@eaabakumov ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
[guest@eaabakumov ~]$ id -G
1001
[guest@eaabakumov ~]$ id -Gn
guest
[guest@eaabakumov ~]$ groups
guest
[guest@eaabakumov ~]$ groups guest
guest : guest
[guest@eaabakumov ~]$ groups guest2
guest2 : guest2 guest
[guest@eaabakumov ~]$
```

Figure 0.4: Группы для guest

```
[guest2@eaabakumov guest]$ id
uid=1002(guest2) gid=1002(guest2) группы=1002(guest2),1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest2@eaabakumov guest]$ id -G
1002 1001
[guest2@eaabakumov guest]$ id -Gn
guest2 guest
[guest2@eaabakumov guest]$ group
bash: group: команда не найдена...
[guest2@eaabakumov guest]$ groups
guest2 guest
[guest2@eaabakumov guest]$
```

Figure 0.5: Группы для guest2

3. Информация в файле `/etc/groups` так же соответствует полученным прежде данным, а именно `guest` в группе `guest`, а `guest2` в группах `guest` и `guest2` (иллюстр. 0.6). Регистрируем пользователя `guest2` в группе `guest` (иллюстр. 0.7).

```
guest@eaabakumov:~
Файл  Правка  Вид  Поиск  Терминал  Справка
unbound:x:987:
kvm:x:36:qemu
qemu:x:107:
tss:x:59:
libvirt:x:986:
usbmuxd:x:113:
geoclue:x:985:
gluster:x:984:
gdm:x:42:
rpcuser:x:29:
nfsnobody:x:65534:
gnome-initial-setup:x:983:
sshd:x:74:
slocate:x:21:
avahi:x:70:
postdrop:x:90:
postfix:x:89:
ntp:x:38:
tcpdump:x:72:
eaabakumov:x:1000:eaabakumov
vboxsf:x:982:
guest:x:1001:guest2
guest2:x:1002:
[guest@eaabakumov ~]$
```

Figure 0.6: `/etc/groups`

```
[guest2@eaabakumov guest]$ newgrp guest
[guest2@eaabakumov guest]$ █
```

Figure 0.7: Регистрация guest2

4. Изменяем права директории `/home/guest`, разрешив все действия для пользователей группы (иллюстр. 0.8). Снимаем все права с `dir1` (иллюстр. 0.9).

```

guest@eaabakumov:~
Файл  Правка  Вид  Поиск  Терминал  Справка
rfsnobody:x:65534:
gnome-initial-setup:x:983:
sshd:x:74:
locate:x:21:
avahi:x:70:
ostdrop:x:90:
ostfix:x:89:
ntp:x:38:
tcpdump:x:72:
eaabakumov:x:1000:eaabakumov
/boxsf:x:982:
guest:x:1001:guest2
guest2:x:1002:
[guest@eaabakumov ~]$ chmod g+rwX /home/guest
```

Figure 0.8: Разрешение на домашнюю папку guest

```

[guest@eaabakumov ~]$ chmod 000 dir1/
[guest@eaabakumov ~]$ ls -l
итого 0
d----- 2 guest guest 6 окт 11 18:00 dir1
drwxr-xr-x. 2 guest guest 6 сен 28 20:17 Видео
drwxr-xr-x. 2 guest guest 6 сен 28 20:17 Документы
drwxr-xr-x. 2 guest guest 6 сен 28 20:17 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 28 20:17 Изображения
drwxr-xr-x. 2 guest guest 6 сен 28 20:17 Музыка
drwxr-xr-x. 2 guest guest 6 сен 28 20:17 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 28 20:17 Рабочий стол
drwxr-xr-x. 2 guest guest 6 сен 28 20:17 Шаблоны
[guest@eaabakumov ~]$ █
```

Figure 0.9: Нулевые права на dir1

5. Следующим шагом проведем эксперимент по выявлению минимально необходимых прав для действий над файловой структурой. Для этого используем

нашу папку `dir1`, файлы внутри неё и функционал прав доступа ОС Linux. Для каждой комбинации атрибутов доступа (`r`, `w`, `x`) на папку и на файл попробуем осуществить ряд действий и таким образом выявим минимально необходимые права для каждого действия. Атрибуты используем только для группы, поэтому комбинаций будет $2^3 \cdot 2^3 = 2^6 = 64$. В каждой строчке будет по 8 действий. Проверять осуществимость функции будем следующими командами:

- `touch` для создания файла в директории;
- `rm` для удаления файла в директории;
- `echo` для записи в файл;
- `cat` для чтения из файла;
- `mv` для переименования файла;
- `chattr` для изменения атрибутов файла;
- `cd` для смены директории;
- `ls` для просмотра файлов в директории.

На иллюстрации можно увидеть вывод приведенных выше команд для первой строки таблицы (права на директорию - 000, права на файл - 000, иллюстр. 0.10).

```
[guest2@eaabakumov guest]$ ./2_gst_script
touch: невозможно выполнить touch для «/home/guest/dir1/file1»: Отказано в досту
пе
rm: невозможно удалить «/home/guest/dir1/file2»: Отказано в доступе
./2_gst_script: line 4: /home/guest/dir1/file3: Отказано в доступе
cat: /home/guest/dir1/file3: Отказано в доступе
chattr: Отказано в доступе while trying to stat /home/guest/dir1/file3
mv: не удалось получить доступ к «/home/guest/dir1/file4»: Отказано в доступе
./2_gst_script: line 8: cd: /home/guest/dir1: Отказано в доступе
ls: невозможно открыть каталог /home/guest/dir1: Отказано в доступе
[guest2@eaabakumov guest]$ █
```

Figure 0.10: Пример ввода команд для проверки прав

Для ускорения ввода команд используем два скрипта для пользователей `guest` и `guest2` соответственно (иллюстр. 0.11, 0.12).

```
1 #!/bin/bash
2 chmod 777 /home/guest/dir1
3 rm -fr /home/guest/dir1/*
4 touch /home/guest/dir1/file2 /home/guest/dir1/file3
5 chmod -R 444 /home/guest/dir1/*
6 chmod 222 /home/guest/dir1
7
```

Figure 0.11: Скрипт для guest

```
1 #!/bin/bash
2 touch /home/guest/dir1/file1
3 rm /home/guest/dir1/file2
4 echo "test_string" > /home/guest/dir1/file3
5 cat /home/guest/dir1/file3
6 chattr +d /home/guest/dir1/file3
7 mv /home/guest/dir1/file3 /home/guest/dir1/file4
8 cd /home/guest/dir1
9 ls /home/guest/dir1
```

Figure 0.12: Скрипт для guest2

Полученные результаты представлены в виде таблицы (иллюстр. 0.13).

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена атрибутов файла	Переименование файла	Смена директории	Просмотр файлов в директории
000	000	—	—	—	—	—	—	—	—
010	000	—	—	—	—	—	—	+	—
020	000	—	—	—	—	—	—	—	—
030	000	+	+	—	—	—	+	+	—
040	000	—	—	—	—	—	—	—	+
050	000	—	—	—	—	—	—	+	+
060	000	—	—	—	—	—	—	—	+
070	000	+	+	—	—	—	+	+	+
000	010	—	—	—	—	—	—	—	—
010	010	—	—	—	—	—	—	+	—
020	010	—	—	—	—	—	—	—	—
030	010	+	+	—	—	—	+	+	—
040	010	—	—	—	—	—	—	—	+
050	010	—	—	—	—	—	—	+	+
060	010	—	—	—	—	—	—	—	+
070	010	+	+	—	—	—	+	+	+
000	020	—	—	—	—	—	—	—	—
010	020	—	—	+	—	—	—	+	—
020	020	—	—	—	—	—	—	—	—
030	020	+	+	+	—	—	+	+	—
040	020	—	—	—	—	—	—	—	+
050	020	—	—	+	—	—	—	+	+
060	020	—	—	—	—	—	—	—	+
070	020	+	+	+	—	—	+	+	+
000	030	—	—	—	—	—	—	—	—
010	030	—	—	+	—	—	—	+	—
020	030	—	—	—	—	—	—	—	—
030	030	+	+	+	—	—	+	+	—
040	030	—	—	—	—	—	—	—	+
050	030	—	—	+	—	—	—	+	+
060	030	—	—	—	—	—	—	—	+
070	030	+	+	+	—	—	+	+	+
000	040	—	—	—	—	—	—	—	—
010	040	—	—	—	+	—	—	+	—
020	040	—	—	—	—	—	—	—	—
030	040	+	+	—	+	—	+	+	—
040	040	—	—	—	—	—	—	—	+
050	040	—	—	—	+	—	—	+	+
060	040	—	—	—	—	—	—	—	+
070	040	+	+	—	+	—	+	+	+
000	050	—	—	—	—	—	—	—	—
010	050	—	—	—	+	—	—	+	—
020	050	—	—	—	—	—	—	—	—
030	050	+	+	—	+	—	+	+	—
040	050	—	—	—	—	—	—	—	+
050	050	—	—	—	+	—	—	+	+
060	050	—	—	—	—	—	—	—	+
070	050	+	+	—	+	—	+	+	+
000	060	—	—	—	—	—	—	—	—
010	060	—	—	+	+	—	—	+	—
020	060	—	—	—	—	—	—	—	—
030	060	+	+	+	+	—	+	+	—
040	060	—	—	—	—	—	—	—	+
050	060	—	—	+	+	—	—	+	+
060	060	—	—	—	—	—	—	—	+
070	060	+	+	+	+	—	+	+	+
000	070	—	—	—	—	—	—	—	—
010	070	—	—	+	+	—	—	+	—
020	070	—	—	—	—	—	—	—	—
030	070	+	+	+	+	—	+	+	—
040	070	—	—	—	—	—	—	—	+
050	070	—	—	+	+	—	—	+	+
060	070	—	—	—	—	—	—	—	+
070	070	+	+	+	+	—	+	+	+
Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена атрибутов файла	Переименование файла	Смена директории	Просмотр файлов в директории

Figure 0.13: Установленные права и разрешённые действия

Таблица прав из данной работы и аналогичная таблица из предыдущей весьма похожи и имеют четкие аналогии. Тем не менее, различия также присутствуют.

На основе данных полученной выше таблицы построим вторую таблицу, иллюстрирующую минимально необходимые права для совершения определенных операций.

Операция	Мин. права на директорию	Мин. права на файл
Создание файла	030	000
Удаление файла	030	000
Чтение файла	010	040
Запись в файл	010	020
Переименование файла	030	000
Создание поддиректории	030	-
Удаление поддиректории	030	-

Выводы

В ходе работы мы успешно провели эксперимент по выявлению минимально необходимых прав для действий над файловой структурой и получили ряд практических навыков работы в консоли с атрибутами файлов для групп пользователей.

Список литературы

1. Права доступа к файлам в linux. // Losst. 2020. URL: <https://losst.ru/prava-dostupa-k-fajlam-v-linux> (дата обращения 11.10.2021).
2. Права в Linux (chown, chmod, SUID, GUID, sticky bit, ACL, umask). // habr.com. 2019. URL: <https://habr.com/ru/post/469667/> (дата обращения 11.10.2021).
3. Д. С. Кулябов, А. В. Королькова, М. Н. Геворкян. Информационная безопасность компьютерных сетей: лабораторные работы. // Факультет физико-математических и естественных наук. М.: РУДН, 2015. 64 с..