

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

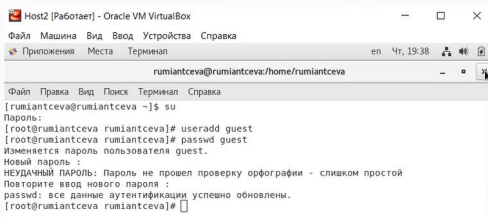
Румянцева Александра Сергеевна

1 октября, 2021

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.

Лабораторная работа подразумевает изучение установленных прав и разрешённых действий над файлами и директориями опытным путем, определение минимальных прав для операций.

1-2. Создала учётную запись пользователя guest и задала пароль для него (рис. 1).



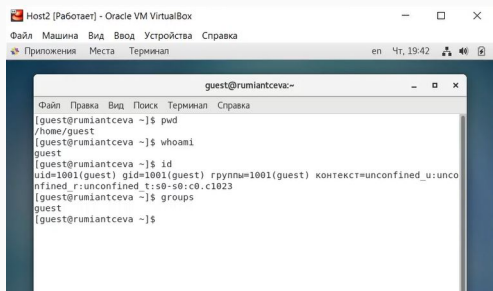
```
Host2 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Приложения  Места  Терминал
en  Чт, 19:38
rumiantceva@rumiantceva:/home/rumiantceva

Файл  Правка  Вид  Поиск  Терминал  Справка
[rumiantceva@rumiantceva ~]$ su
Пароль:
[root@rumiantceva rumiantceva]# useradd guest
[root@rumiantceva rumiantceva]# passwd guest
Изменяется пароль пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - слишком простой
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@rumiantceva rumiantceva]#
```

Figure 1: рис.1. Создание пользователя guest и задание для него пароля.

3. Вошла в систему от имени пользователя guest.

4-7. Определила директорию, в которой нахожусь, командой `pwd`. Уточнила имя пользователя командой `whoami`. Уточнила имя пользователя, его группу, а также группы, куда входит пользователь, командой `id` (рис. 2).

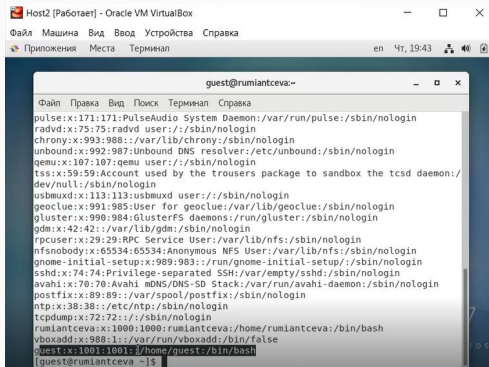


```
Host2 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Приложения  Места  Терминал  en  Чт, 19:42

guest@rumiantceva:~
Файл  Правка  Вид  Поиск  Терминал  Справка
[guest@rumiantceva ~]$ pwd
/home/guest
[guest@rumiantceva ~]$ whoami
guest
[guest@rumiantceva ~]$ id
uid=1001(guest) gid=1001(guest) rpyyny=1001(guest) контекст=unconfined_u:unco
nfinied_r:unconfined_t:s0-s0:c0.c1023
[guest@rumiantceva ~]$ groups
guest
[guest@rumiantceva ~]$
```

Figure 2: рис.2. Выполнение команды `pwd`, `whoami`, `id` и `groups`.

8. Просмотрела файл `/etc/passwd` командой `cat /etc/passwd`. Нашла в нём свою учётную запись (рис. 3). `uid` пользователя равен 1001, `gid` пользователя равен 1001, что совпадает с результатами выполнения команд, которые мы получили в предыдущих пунктах.

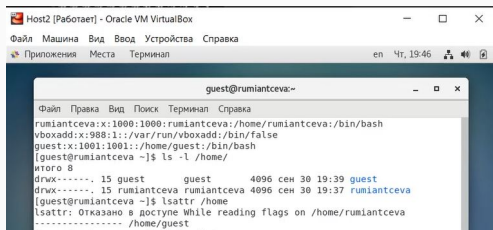


```
Host2 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Приложения  Места  Терминал  en  Чт, 19:43  [иконки]

guest@rumiantceva:~
Файл  Правка  Вид  Поиск  Терминал  Справка
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
rfcuser: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
sshdx: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
ntpd:x:38:38:/etc/ntp:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
rumiantceva:x:1000:1000:rumiantceva:/home/rumiantceva:/bin/bash
vboxadd:x:988:1:/var/run/vboxadd:/bin/false
guest:x:1001:1001:/home/guest:/bin/bash
guest@rumiantceva ~$
```

Figure 3: рис.3. Результат выполнения команды `cat /etc/passwd`. Учётная запись `guest`.

9-10. Определила существующие в системе директории командой `ls -l /home/` и проверила, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой `lsattr /home` (рис. 4).

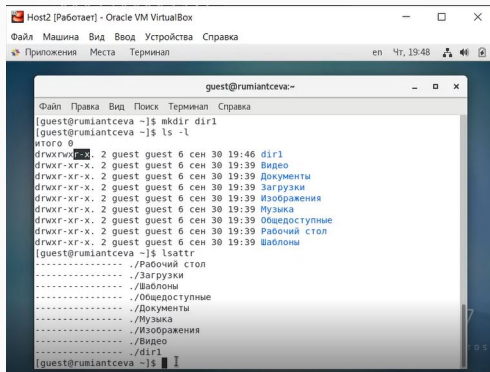


```
Host2 [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Приложения Места Терминал en Чт, 19:46

guest@rumiantceva:~
Файл Правка Вид Поиск Терминал Справка
rumiantceva:x:1000:1000:rumiantceva:/home/rumiantceva:/bin/bash
vboxadd:x:988:1::/var/run/vboxadd:/bin/false
guest:x:1001:1001::/home/guest:/bin/bash
[guest@rumiantceva ~]$ ls -l /home/
итого 8
drwx-----. 15 guest      guest      4096 сен 30 19:39 guest
drwx-----. 15 rumiantceva rumiantceva 4096 сен 30 19:37 rumiantceva
[guest@rumiantceva ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/rumiantceva
----- /home/guest
```

Figure 4: рис.4. Результат выполнения команды `ls -l /home/` и `lsattr /home`

11. Создала в домашней директории поддиректорию dir1 командой `mkdir dir1`. С помощью команд `ls -l` и `lsattr` посмотрела, какие права доступа и расширенные атрибуты были выставлены на директорию dir1 (рис.5).

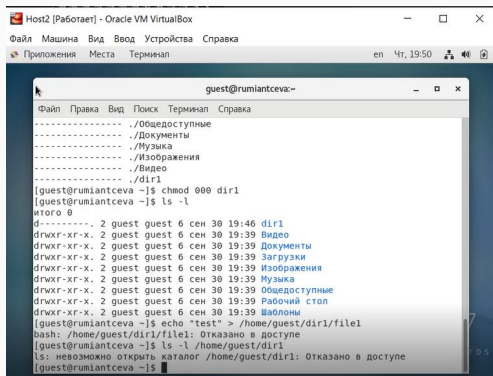


```
Host2 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройство  Справка
Приложения  Места  Терминал  en  Чт, 19:48

guest@rumiantceva:~$ mkdir dir1
guest@rumiantceva ~]$ ls -l
итого 0
drwxrwxr-x. 2 guest guest 6 сен 30 19:46 dir1
drwxr-xr-x. 2 guest guest 6 сен 30 19:39 Видео
drwxr-xr-x. 2 guest guest 6 сен 30 19:39 Документы
drwxr-xr-x. 2 guest guest 6 сен 30 19:39 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 30 19:39 Изображения
drwxr-xr-x. 2 guest guest 6 сен 30 19:39 Музыка
drwxr-xr-x. 2 guest guest 6 сен 30 19:39 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 30 19:39 Рабочий стол
drwxr-xr-x. 2 guest guest 6 сен 30 19:39 Шаблоны
guest@rumiantceva ~]$ lsattr
-----
./Рабочий стол
./Загрузки
./Шаблоны
./Общедоступные
./Документы
./Музыка
./Изображения
./Видео
./dir1
guest@rumiantceva ~]$
```

Figure 5: рис.5. Выполнение команд `mkdir dir1`, `ls -l` и `lsattr`

12-13. Сняла с директории dir1 все атрибуты. Попыталась создать в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1`. Данное действие выполнить не удалось из-за отсутствия доступа (рис. 6).



```
Host2 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Приложения  Места  Терминал  en  Чт, 19:50

guest@rumiantceva:~
Файл  Правка  Вид  Поиск  Терминал  Справка
-----
./Общедоступные
./Документы
./Музыка
./Изображения
./Видео
./dir1
[guest@rumiantceva ~]$ chmod 000 dir1
[guest@rumiantceva ~]$ ls -l
итого 0
d-----. 2 guest guest 6 сен 30 19:46 dir1
dwxr-xr-x. 2 guest guest 6 сен 30 19:39 Видео
dwxr-xr-x. 2 guest guest 6 сен 30 19:39 Документы
dwxr-xr-x. 2 guest guest 6 сен 30 19:39 Загрузки
dwxr-xr-x. 2 guest guest 6 сен 30 19:39 Изображения
dwxr-xr-x. 2 guest guest 6 сен 30 19:39 Музыка
dwxr-xr-x. 2 guest guest 6 сен 30 19:39 Общедоступные
dwxr-xr-x. 2 guest guest 6 сен 30 19:39 Рабочий стол
dwxr-xr-x. 2 guest guest 6 сен 30 19:39 Шаблоны
[guest@rumiantceva ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@rumiantceva ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог /home/guest/dir1: Отказано в доступе
[guest@rumiantceva ~]$
```

Figure 6: рис.6. Результат команд `chmod 000 dir1`, `ls -l` и `echo "test" > /home/guest/dir1/file1`.

14. Заполнила таблицу 1 опытным путём.

Команды для проверки, которые я использовала: - touch - проверка на создание файла - rm - проверка на удаление файла - echo - проверка на запись в файл - cat - проверка на чтение файла - cd - проверка на доступ в директорию - ls - проверка на просмотр файлов в директории - mv - проверка на переименование файла - chattr - проверка добавление атрибутов

Для смены и задания прав на файл или директорию я использовала команду chmod.

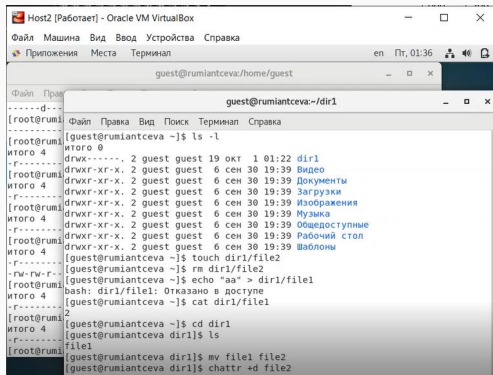


Figure 7: рис.7. Пример выполнения команд для заполнения таблицы установленных прав и разрешённых действий над файлами и директориями для случая 700 / 400.

«Установленные права и разрешённые действия»

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
000	000	-	-	-	-	-	-	-	-
100	000	-	-	-	-	+	-	-	-
200	000	-	-	-	-	-	+	-	-
300	000	+	+	-	-	+	-	+	-
400	000	-	-	-	-	-	+	-	-
500	000	-	-	-	-	+	+	-	-
600	000	-	-	-	-	-	+	-	-
700	000	+	+	-	-	+	+	+	-
000	100	-	-	-	-	-	-	-	-
100	100	-	-	-	-	+	-	-	-
200	100	-	-	-	-	-	-	-	-
300	100	+	+	-	-	+	-	+	-
400	100	-	-	-	-	-	+	-	-
500	100	-	-	-	-	-	+	-	-
600	100	-	-	-	-	-	+	-	-
700	100	+	+	-	-	+	+	+	-
000	200	-	-	-	-	-	-	-	-
100	200	-	-	+	-	+	-	-	-
200	200	-	-	-	-	+	-	-	-
300	200	+	+	+	-	+	-	+	-
400	200	-	-	-	-	-	+	-	-
500	200	-	-	+	-	+	+	-	-
600	200	-	-	-	-	-	+	-	-
700	200	+	+	+	-	+	+	+	-
000	300	-	-	-	-	-	-	-	-
100	300	-	-	+	-	+	-	-	-
200	300	-	-	-	-	-	-	-	-
300	300	+	+	+	+	+	-	+	-
400	300	-	-	-	-	-	+	-	-
500	300	-	-	+	-	+	+	-	-
600	300	-	-	-	-	-	+	-	-
700	300	+	+	+	-	+	+	+	-
000	400	-	-	-	-	-	-	-	-
100	400	-	-	-	+	+	-	-	+
200	400	-	-	-	-	-	-	-	-
300	400	+	+	-	+	+	-	+	+
400	400	-	-	-	-	-	-	-	-
500	400	-	-	-	+	+	+	-	+
600	400	-	-	-	-	-	+	-	-
700	400	+	+	-	+	+	+	+	+
000	500	-	-	-	-	-	-	-	-
100	500	-	-	-	+	+	-	-	+
200	500	-	-	-	-	-	-	-	-
300	500	+	+	-	+	+	-	+	+
400	500	-	-	-	-	+	+	-	+
500	500	-	-	-	+	+	+	-	+
600	500	-	-	-	-	-	+	-	-
700	500	+	+	-	+	+	+	+	+
000	600	-	-	-	-	-	-	-	-
100	600	-	-	+	+	+	-	-	+
200	600	-	-	-	-	-	-	-	-
300	600	+	+	+	+	+	-	+	+
400	600	-	-	-	-	-	+	-	-
500	600	-	-	-	+	+	+	-	+
600	600	-	-	-	-	-	+	-	-
700	600	+	+	+	+	+	+	+	+
000	700	-	-	-	-	-	-	-	-
100	700	-	-	-	+	+	-	-	+
200	700	-	-	-	+	+	-	-	+
300	700	+	+	+	+	+	-	+	+
400	700	-	-	-	-	+	-	-	-
500	700	-	-	+	+	+	+	-	+
600	700	-	-	-	-	-	+	-	-
700	700	+	+	+	+	+	+	+	+

Figure 8: рис.8. Таблица «Установленные права и разрешённые действия».

15. На основании заполненной таблицы определяю минимально необходимые права для выполнения операций внутри директории dir1.

Операция	Мин. права на директорию	Мин. права на файл
Создание файла	300	000
Удаление файла	300	000
Чтение файла	100	400
Запись в файл	300	200
Переименование файла	300	000
Создание поддиректории	300	-
Удаление поддиректории	300	-

Я получила практические навыки работы в консоли с атрибутами файлов, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux1.