

Отчёт по лабораторной работе №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Дурдалыев Максат

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 | 7 |
| 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@mdurdaliev:~  
[mdurdaliev@mdurdaliev ~]$ su  
Пароль:  
[root@mdurdaliev mdurdaliev]# useradd guest  
Создание почтового ящика: Файл существует  
[root@mdurdaliev mdurdaliev]# passwd guest  
Изменение пароля пользователя guest.  
Новый пароль:  
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом  
Повторите ввод нового пароля:  
passwd: данные аутентификации успешно обновлены.  
[root@mdurdaliev mdurdaliev]#  
[root@mdurdaliev mdurdaliev]# su guest  
[guest@mdurdaliev mdurdaliev]$ pwd  
/home/mdurdaliev  
[guest@mdurdaliev mdurdaliev]$ cd  
[guest@mdurdaliev ~]$ pwd  
/home/guest  
[guest@mdurdaliev ~]$ whoami  
guest  
[guest@mdurdaliev ~]$ id guest  
uid=1001(guest) gid=1001(guest) rгруппы=1001(guest)  
[guest@mdurdaliev ~]$ groups guest  
guest : guest  
[guest@mdurdaliev ~]$
```

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.

```
cockpit-wsinstance:x:986:985:User for cockpit-ws instances:/nonexisting:/sbin/nologin  
flatpak:x:985:984:User for flatpak system helper:/sbin/nologin  
colord:x:984:983:User for colord:/var/lib/colord:/sbin/nologin  
clevis:x:983:982:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin  
setroubleshoot:x:982:981:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/nologin  
gdm:x:42:42::/var/lib/gdm:/sbin/nologin  
gnome-initial-setup:x:981:980::/run/gnome-initial-setup:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin  
chrony:x:980:979:chrony system user:/var/lib/chrony:/sbin/nologin  
dnsmasq:x:979:978:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin  
tcpdump:x:72:72::/sbin/nologin  
mdurdaliev:x:1000:1000::/home/mdurdaliev:/bin/bash  
guest:x:1001:1001::/home/guest:/bin/bash  
[guest@mdurdaliev ~]$
```

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.

```
emrony:x:1000:1000:emrony:/var/lib/emrony:/sbin/nologin
dnsmasq:x:979:978:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72:::/sbin/nologin
mdurdaliev:x:1000:1000::/home/mdurdaliev:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
[guest@mdurdaliev ~]$
[guest@mdurdaliev ~]$ ls -l /home
итого 4
drwx-----. 3 guest guest 78 фев 21 12:48 guest
drwx-----. 14 mdurdaliev mdurdaliev 4096 фев 21 12:46 mdurdaliev
[guest@mdurdaliev ~]$
```

Figure 2.3: Расширенные атрибуты

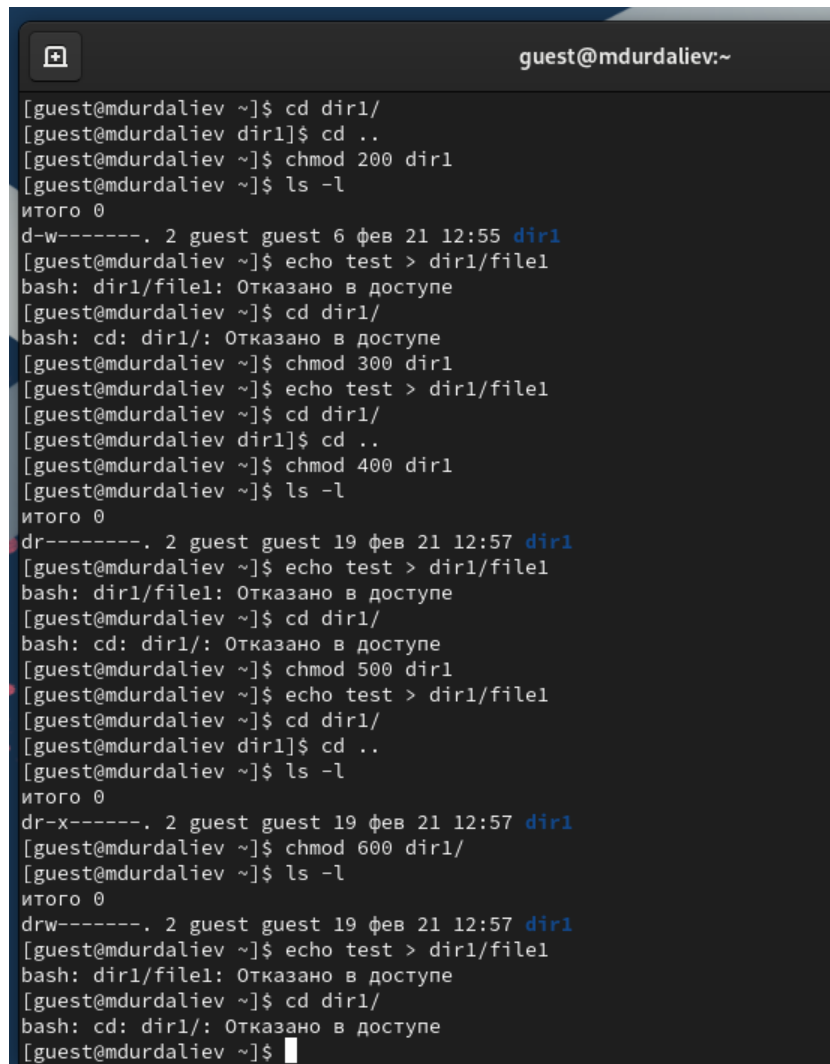
10. Создали в домашней директории поддиректорию dir1 командой `mkdir dir1`. Определим командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию dir1.
11. Сняли с директории dir1 все атрибуты командой `chmod 000 dir1` и проверили с `ls -l` помощью правильность 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@mdurdaliev ~]$
[guest@mdurdaliev ~]$ cd
[guest@mdurdaliev ~]$ mkdir dir1
[guest@mdurdaliev ~]$ ls -l
итого 0
drwxr-xr-x. 2 guest guest 6 фев 21 12:55 dir1
[guest@mdurdaliev ~]$ chmod 000 dir1
[guest@mdurdaliev ~]$ ls -l
итого 0
d------. 2 guest guest 6 фев 21 12:55 dir1
[guest@mdurdaliev ~]$ echo test > dir1/file1
bash: dir1/file1: Отказано в доступе
[guest@mdurdaliev ~]$ cd dir1/
bash: cd: dir1/: Отказано в доступе
[guest@mdurdaliev ~]$
```

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@mdurdaliev:~  
[guest@mdurdaliev ~]$ cd dir1/  
[guest@mdurdaliev dir1]$ cd ..  
[guest@mdurdaliev ~]$ chmod 200 dir1  
[guest@mdurdaliev ~]$ ls -l  
итого 0  
d-w-----. 2 guest guest 6 фев 21 12:55 dir1  
[guest@mdurdaliev ~]$ echo test > dir1/file1  
bash: dir1/file1: Отказано в доступе  
[guest@mdurdaliev ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@mdurdaliev ~]$ chmod 300 dir1  
[guest@mdurdaliev ~]$ echo test > dir1/file1  
[guest@mdurdaliev ~]$ cd dir1/  
[guest@mdurdaliev dir1]$ cd ..  
[guest@mdurdaliev ~]$ chmod 400 dir1  
[guest@mdurdaliev ~]$ ls -l  
итого 0  
dr-----. 2 guest guest 19 фев 21 12:57 dir1  
[guest@mdurdaliev ~]$ echo test > dir1/file1  
bash: dir1/file1: Отказано в доступе  
[guest@mdurdaliev ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@mdurdaliev ~]$ chmod 500 dir1  
[guest@mdurdaliev ~]$ echo test > dir1/file1  
[guest@mdurdaliev ~]$ cd dir1/  
[guest@mdurdaliev dir1]$ cd ..  
[guest@mdurdaliev ~]$ ls -l  
итого 0  
dr-x-----. 2 guest guest 19 фев 21 12:57 dir1  
[guest@mdurdaliev ~]$ chmod 600 dir1/  
[guest@mdurdaliev ~]$ ls -l  
итого 0  
drw-----. 2 guest guest 19 фев 21 12:57 dir1  
[guest@mdurdaliev ~]$ echo test > dir1/file1  
bash: dir1/file1: Отказано в доступе  
[guest@mdurdaliev ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@mdurdaliev ~]$
```

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) | - | - | - | - | - | - | - | - |
| d-wx------(300) | --w------(200) | + | + | + | - | + | - | + | + |
| dr------(400) | --w------(200) | - | - | - | - | - | - | - | - |
| dr-x------(500) | --w------(200) | - | - | + | - | + | + | - | + |
| drw------(600) | --w------(200) | - | - | - | - | - | - | - | - |
| drwx------(700) | --w------(200) | + | + | + | - | + | + | + | + |

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

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

| Операция | Права на директорию | Права на файл |
|------------------------|---------------------|---------------|
| 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