

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Сабралиева М. Н.

Российский университет дружбы народов, Москва, Россия

Информация

- Сабралиева Марворид Нуралиевна
- ученица кафедры прикладной информатики и теории вероятностей НБИбд-01-22
- Российский университет дружбы народов

- Процессор **pandoc** для входного формата Markdown
- Результирующие форматы
 - pdf
 - html
- Автоматизация процесса создания: **Makefile**

Создание презентации

```
slide_level: 2  
aspectratio: 169  
section-titles: true  
theme: metropolis
```

- Используется фреймворк `reveal.js`
- Используется тема `beige`

- Тема задаётся в файле **Makefile**

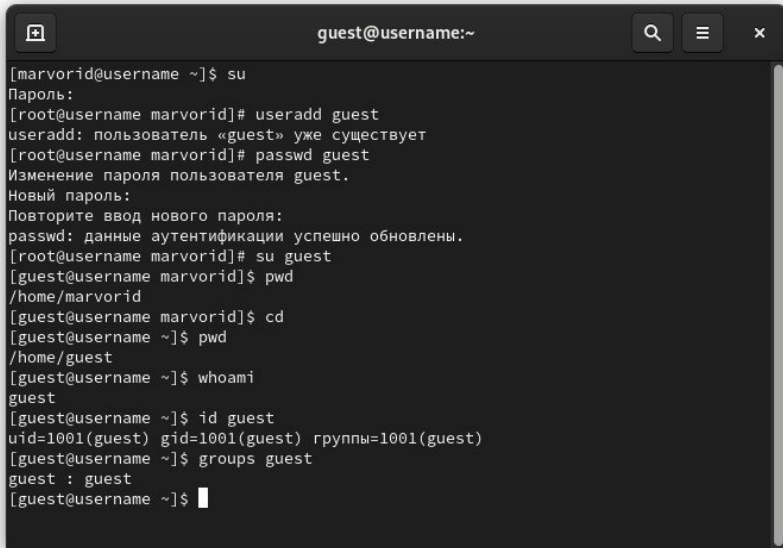
```
REVEALJS_THEME = beige
```


Элементы презентации

- 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.

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создадим учётную запись пользователя `guest` (используя учётную запись администратора): `useradd guest`
2. Зададим пароль для пользователя `guest` (используя учётную запись администратора): `passwd guest`
3. Войдем в систему от имени пользователя `guest`.
4. Определим директорию, в которой мы находимся, командой `pwd`. Сравним её с приглашением командной строки. Определим, является ли она нашей домашней директорией

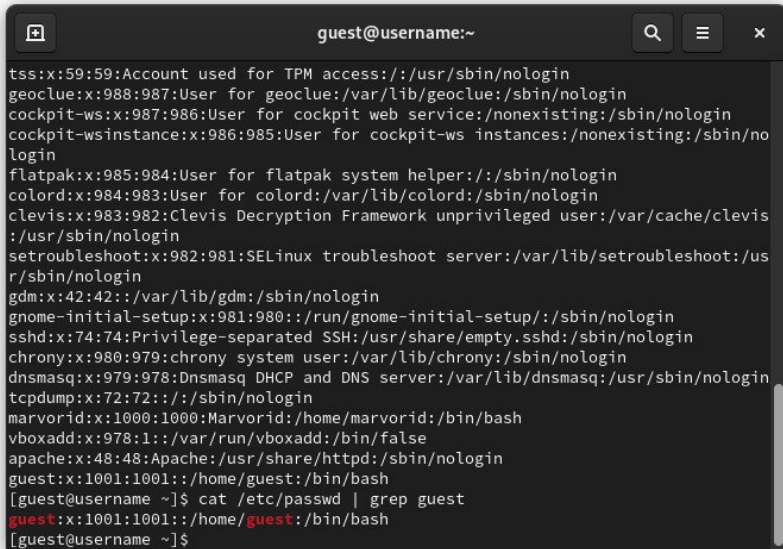
5. Уточним имя нашего пользователя командой `whoami`.
6. Уточним имя нашего пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. запомним. Сравним вывод `id` с выводом команды `groups`.
7. Сравним полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки.



```
guest@username:~  
[marvوريد@username ~]$ su  
Пароль:  
[root@username marvوريد]# useradd guest  
useradd: пользователь «guest» уже существует  
[root@username marvوريد]# passwd guest  
Изменение пароля пользователя guest.  
Новый пароль:  
Повторите ввод нового пароля:  
passwd: данные аутентификации успешно обновлены.  
[root@username marvوريد]# su guest  
[guest@username marvوريد]$ pwd  
/home/marvوريد  
[guest@username marvوريد]$ cd  
[guest@username ~]$ pwd  
/home/guest  
[guest@username ~]$ whoami  
guest  
[guest@username ~]$ id guest  
uid=1001(guest) gid=1001(guest) rгруппы=1001(guest)  
[guest@username ~]$ groups guest  
guest : guest  
[guest@username ~]$
```

Рис. 1: Первичные действия в учетной записи guest

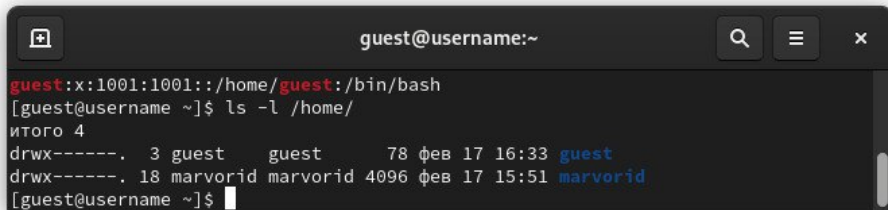
8. Просмотрим файл `/etc/passwd` командой `cat /etc/passwd` Найдём в нём свою учётную запись. Определим `uid` пользователя. Определим `gid` пользователя. Сравним найденные значения с полученными в предыдущих пунктах. `guest` имеет те же идентификаторы

A terminal window with a dark background and light text. The title bar at the top shows 'guest@username:~' and standard window controls (minimize, maximize, close). The terminal displays a list of system users and their details, followed by a command to filter the password file for the 'guest' user.

```
tss:x:59:59:Account used for TPM access:/:usr/sbin/nologin
geoclue:x:988:987:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:987:986:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:986:985:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:985:984:User for flatpak system helper:/:usr/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:/usr/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:/usr/sbin/nologin
tcpdump:x:72:72:/:usr/sbin/nologin
marvolid:x:1000:1000:Marvolid:/home/marvolid:/bin/bash
vboxadd:x:978:1:/:var/run/vboxadd:/bin/false
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
guest:x:1001:1001:/:home/guest:/bin/bash
[guest@username ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001:/:home/guest:/bin/bash
[guest@username ~]$
```

Рис. 2: команда cat

9. Определим существующие в системе директории командой `ls -l /home/`.
10. Проверим, 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.

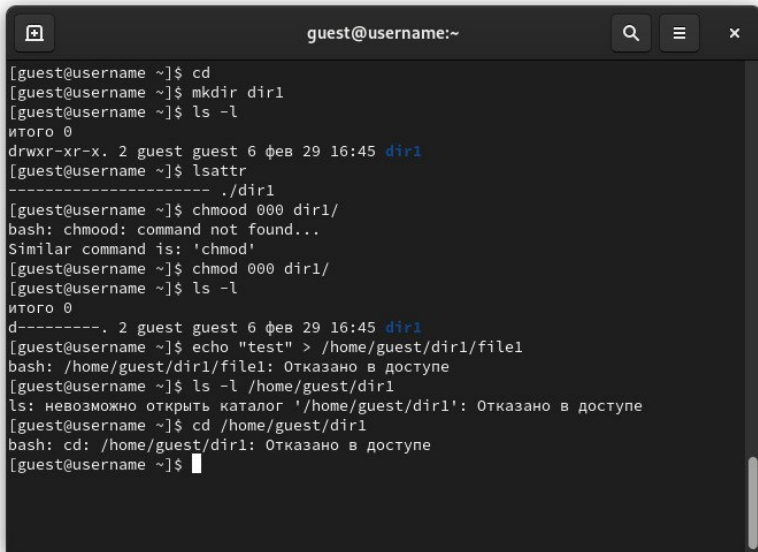


A terminal window with a dark background. The title bar shows 'guest@username:~' and standard window controls. The terminal output shows a shell prompt, a command to list files with long format, and the resulting output which includes file permissions, sizes, dates, and usernames.

```
guest@username:~$ ls -l /home/  
итого 4  
drwx-----. 3 guest    guest      78 фев 17 16:33 guest  
drwx-----. 18 marvorid marvorid 4096 фев 17 15:51 marvorid
```

Рис. 3: Расширенные атрибуты

11. 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`.
12. Снимем с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверим с её помощью правильность выполнения команды `ls -l`
13. создали в директории `dir1` файл `file1` командой `echo "test" > /home/guest/dir1/file1`. Так как ранее мы отозвали все атрибуты, то тем самым были лишены всех прав на взаимодействие с `dir1`



```
guest@username:~  
[guest@username ~]$ cd  
[guest@username ~]$ mkdir dir1  
[guest@username ~]$ ls -l  
итого 0  
drwxr-xr-x. 2 guest guest 6 фев 29 16:45 dir1  
[guest@username ~]$ lsattr  
----- ./dir1  
[guest@username ~]$ chmood 000 dir1/  
bash: chmood: command not found...  
Similar command is: 'chmod'  
[guest@username ~]$ chmod 000 dir1/  
[guest@username ~]$ ls -l  
итого 0  
d----- . 2 guest guest 6 фев 29 16:45 dir1  
[guest@username ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@username ~]$ ls -l /home/guest/dir1  
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе  
[guest@username ~]$ cd /home/guest/dir1  
bash: cd: /home/guest/dir1: Отказано в доступе  
[guest@username ~]$
```

Рис. 4: Снятие атрибутов с директории

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

```
guest@username:~  
[guest@username ~]$ echo test > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@username ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@username ~]$ chmod 200 dir1/  
[guest@username ~]$ ls -l  
итого 0  
d-w-----. 2 guest guest 6 фев 29 16:45 dir1  
[guest@username ~]$ echo test > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@username ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@username ~]$ chmod 300 dir1/  
[guest@username ~]$ ls -l  
итого 0  
d-wx-----. 2 guest guest 6 фев 29 16:45 dir1  
[guest@username ~]$ echo test > /home/guest/dir1/file1  
[guest@username ~]$ cd dir1/  
[guest@username dir1]$ cd ..  
[guest@username ~]$ chmod 400 dir1/  
[guest@username ~]$ ls -l  
итого 0  
dr-----.. 2 guest guest 19 фев 29 17:07 dir1  
[guest@username ~]$ echo test > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@username ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@username ~]$ chmod 500 dir1/  
[guest@username ~]$ ls -l  
итого 0  
dr-x-----.. 2 guest guest 19 фев 29 17:07 dir1  
[guest@username ~]$ echo test > /home/guest/dir1/file1  
[guest@username ~]$ cd dir1/  
[guest@username dir1]$ cd ..  
[guest@username ~]$
```

Рис. 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

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)	-	-	+	-	+	-	-	+

Рис. 6: Заполнение таблицы

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

Рис. 7: Заполнение таблицы

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

Рис. 8: Заполнение таблицы

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)

Рис. 9: Заполнение таблицы

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

Итоговый слайд

- Запоминается последняя фраза. © Штирлиц

...