

Отчёт по лабораторной работе №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Еде Мак Дональд Чуквума

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
3	Вывод	14
	Список литературы	15

List of Figures

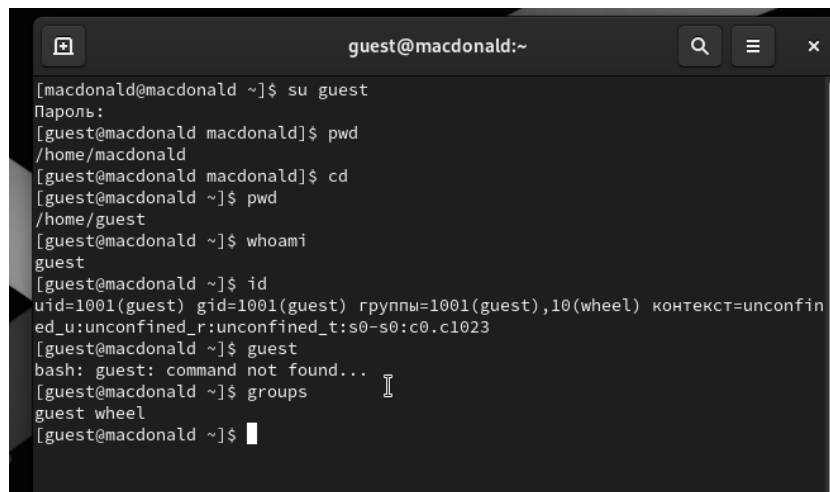
2.1	Информация о пользователе guest	6
2.2	Содержимое файла /etc/passwd	7
2.3	Расширенные атрибуты	8
2.4	Снятие атрибутов с директории	8
2.5	Заполнение таблицы	9

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

A terminal window titled 'guest@macdonald:~' with search, menu, and close icons. The terminal shows a sequence of commands and their outputs: switching to the 'guest' user, checking the password, changing the directory to the user's home, checking the current directory, running 'whoami', running 'id' to show user and group IDs, attempting to run the 'guest' command, and finally running 'groups' to show the user is in the 'wheel' group.

```
guest@macdonald:~  
[macdonald@macdonald ~]$ su guest  
Пароль:  
[guest@macdonald macdonald]$ pwd  
/home/macdonald  
[guest@macdonald macdonald]$ cd  
[guest@macdonald ~]$ pwd  
/home/guest  
[guest@macdonald ~]$ whoami  
guest  
[guest@macdonald ~]$ id  
uid=1001(guest) gid=1001(guest) rгруппы=1001(guest),10(wheel) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@macdonald ~]$ guest  
bash: guest: command not found...  
[guest@macdonald ~]$ groups  
guest wheel  
[guest@macdonald ~]$
```

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@macdonald:~$ groups
guest wheel
[guest@macdonald ~]$
[guest@macdonald ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/sbin/nologin
dbus:x:81:81:System message bus:/sbin/nologin
polkitd:x:998:996:User for polkitd:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
sssd:x:997:993:User for sssd:/sbin/nologin
pipewire:x:996:992:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
libstoragemgmt:x:990:990:daemon account for libstoragemgmt:/usr/sbin/nologin
systemd-oom:x:989:989:systemd Userspace OOM Killer:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/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:/sbin/nologin
colord:x:984:983:User for colord:/var/lib/colord:/sbin/nologin
clevvis:x:983:982:Clevis Decryption Framework unprivileged user:/var/cache/clevvis:/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
guest:x:1001:1001:guest:/home/guest:/bin/bash
macdonald:x:1002:1002:/home/macdonald:/bin/bash
[guest@macdonald ~]$
```

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@macdonald ~]$
[guest@macdonald ~]$ ls -l /home/
итого 8
drwx-----, 14 guest      guest      4096 сен 12 20:01 guest
drwx-----, 14 macdonald macdonald  4096 сен 12 19:59 macdonald
[guest@macdonald ~]$

```

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.

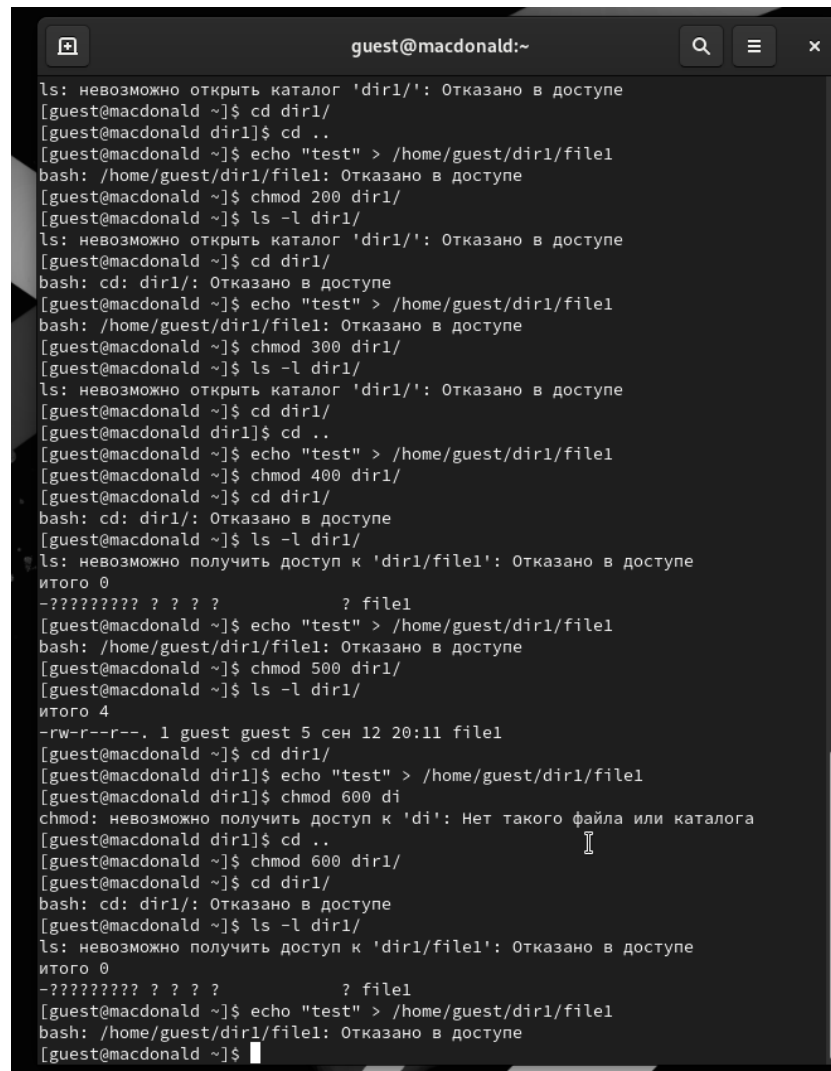
```

[guest@macdonald ~]$
[guest@macdonald ~]$ ls -l /home/
итого 8
drwx-----, 14 guest      guest      4096 сен 12 20:01 guest
drwx-----, 14 macdonald macdonald  4096 сен 12 19:59 macdonald
[guest@macdonald ~]$
[guest@macdonald ~]$
[guest@macdonald ~]$ cd
[guest@macdonald ~]$ mkdir dir1
[guest@macdonald ~]$ ls -l
итого 0
drwxr-xr-x, 2 guest guest 6 сен 12 20:08 dir1
drwxr-xr-x, 2 guest guest 6 сен 10 14:33 Видео
drwxr-xr-x, 2 guest guest 6 сен 10 14:33 Документы
drwxr-xr-x, 2 guest guest 6 сен 10 14:33 Загрузки
drwxr-xr-x, 2 guest guest 6 сен 10 14:33 Изображения
drwxr-xr-x, 2 guest guest 6 сен 10 14:33 Музыка
drwxr-xr-x, 2 guest guest 6 сен 10 14:33 Общедоступные
drwxr-xr-x, 2 guest guest 6 сен 10 14:33 'Рабочий стол'
drwxr-xr-x, 2 guest guest 6 сен 10 14:33 Шаблоны
[guest@macdonald ~]$ chmod 000 dir1/
[guest@macdonald ~]$ ls -l
итого 0
d-----, 2 guest guest 6 сен 12 20:08 dir1
drwxr-xr-x, 2 guest guest 6 сен 10 14:33 Видео
drwxr-xr-x, 2 guest guest 6 сен 10 14:33 Документы
drwxr-xr-x, 2 guest guest 6 сен 10 14:33 Загрузки
drwxr-xr-x, 2 guest guest 6 сен 10 14:33 Изображения
drwxr-xr-x, 2 guest guest 6 сен 10 14:33 Музыка
drwxr-xr-x, 2 guest guest 6 сен 10 14:33 Общедоступные
drwxr-xr-x, 2 guest guest 6 сен 10 14:33 'Рабочий стол'
drwxr-xr-x, 2 guest guest 6 сен 10 14:33 Шаблоны
[guest@macdonald ~]$ cd dir1/
bash: cd: dir1/: Отказано в доступе
[guest@macdonald ~]$

```

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@macdonald:~  
ls: невозможно открыть каталог 'dir1/': Отказано в доступе  
[guest@macdonald ~]$ cd dir1/  
[guest@macdonald dir1]$ cd ..  
[guest@macdonald ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@macdonald ~]$ chmod 200 dir1/  
[guest@macdonald ~]$ ls -l dir1/  
ls: невозможно открыть каталог 'dir1/': Отказано в доступе  
[guest@macdonald ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@macdonald ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@macdonald ~]$ chmod 300 dir1/  
[guest@macdonald ~]$ ls -l dir1/  
ls: невозможно открыть каталог 'dir1/': Отказано в доступе  
[guest@macdonald ~]$ cd dir1/  
[guest@macdonald dir1]$ cd ..  
[guest@macdonald ~]$ echo "test" > /home/guest/dir1/file1  
[guest@macdonald ~]$ chmod 400 dir1/  
[guest@macdonald ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@macdonald ~]$ ls -l dir1/  
ls: невозможно получить доступ к 'dir1/file1': Отказано в доступе  
итого 0  
-???????? ? ? ? ? ? ? file1  
[guest@macdonald ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@macdonald ~]$ chmod 500 dir1/  
[guest@macdonald ~]$ ls -l dir1/  
итого 4  
-rw-r--r--. 1 guest guest 5 сен 12 20:11 file1  
[guest@macdonald ~]$ cd dir1/  
[guest@macdonald dir1]$ echo "test" > /home/guest/dir1/file1  
[guest@macdonald dir1]$ chmod 600 di  
chmod: невозможно получить доступ к 'di': Нет такого файла или каталога  
[guest@macdonald dir1]$ cd ..  
[guest@macdonald ~]$ chmod 600 dir1/  
[guest@macdonald ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@macdonald ~]$ ls -l dir1/  
ls: невозможно получить доступ к 'dir1/file1': Отказано в доступе  
итого 0  
-???????? ? ? ? ? ? ? file1  
[guest@macdonald ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@macdonald ~]$
```

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)	-	-	+	-	+	+	-	+

Права директории	Права файла	1	2	3	4	5	6	7	8
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)	-	-	-	+	+	+	-	+
drw------(600)	-r-x------(500)	-	-	-	-	-	-	-	-
drwx------(700)	-r-x------(500)	+	+	-	+	+	+	+	+
d------(000)	-rw------(600)	-	-	-	-	-	-	-	-

Права директории	Права файла	1	2	3	4	5	6	7	8
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)
Чтение файла	d--x----- (100)	-r----- (400)
Запись в файл	d--x----- (100)	--w----- (200)
Переименование файла	d-wx----- (300)	----- (000)

Операция	Права на директорию	Права на файл
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