

Отчёт по лабораторной работе №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Альхаддад Рашид Мухаммед Отман

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
3	Вывод	12
	Список литературы	13

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@rashidalhaddad:~  
/home/guest  
rashidalhaddad@rashidalhaddad:~$ su guest  
Пароль:  
guest@rashidalhaddad:/home/rashidalhaddad$ pwd  
/home/rashidalhaddad  
guest@rashidalhaddad:/home/rashidalhaddad$ cd  
guest@rashidalhaddad:~$ pwd  
/home/guest  
guest@rashidalhaddad:~$ id  
uid=1001(guest) gid=1001(guest) rpyнпы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined  
_t:s0-s0:c0.c1023  
guest@rashidalhaddad:~$ whoami  
guest  
guest@rashidalhaddad:~$ groups  
guest  
guest@rashidalhaddad:~$ █
```

Figure 2.1: Информация о пользователе guest

7. 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 1001, наш пользователь под идентификатором 1002.

```
guest@rashidalhaddad:~  
/home/guest  
systemd-oom:x:999:999:systemd Userspace OOM Killer:/:/sbin/nologin  
polkitd:x:114:114:User for polkitd:/:/sbin/nologin  
colord:x:998:997:User for colord:/var/lib/colord:/sbin/nologin  
stapunpriv:x:159:159:systemtap unprivileged user:/var/lib/stapunpriv:/sbin/nologin  
rtkit:x:172:172:RealtimeKit:/:/sbin/nologin  
geoclue:x:997:996:User for geoclue:/var/lib/geoclue:/sbin/nologin  
sssd:x:996:995:User for sssd:/run/sss:/sbin/nologin  
libstoragemgmt:x:994:994:daemon account for libstoragemgmt:/:/usr/sbin/nologin  
systemd-coredump:x:993:993:systemd Core Dumper:/:/usr/sbin/nologin  
wsdd:x:992:992:Web Services Dynamic Discovery host daemon:/:/sbin/nologin  
clevis:x:991:991:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin  
setroubleshoot:x:990:990:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin  
pipewire:x:989:989:PipeWire System Daemon:/run/pipewire:/usr/sbin/nologin  
flatpak:x:988:988:Flatpak system helper:/:/usr/sbin/nologin  
gdm:x:42:42:GNOME Display Manager:/var/lib/gdm:/usr/sbin/nologin  
gnome-initial-setup:x:987:986:/:/run/gnome-initial-setup:/sbin/nologin  
dnsmasq:x:986:985:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin  
pesign:x:985:984:Group for the pesign signing daemon:/run/pesign:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin  
chrony:x:984:983:chrony system user:/var/lib/chrony:/sbin/nologin  
tcpdump:x:72:72:tcpdump:/:/usr/sbin/nologin  
gnome-remote-desktop:x:981:981:GNOME Remote Desktop:/var/lib/gnome-remote-desktop:/usr/sbin/nologin  
guest:x:1001:1001:/:/home/guest:/bin/bash  
rashidalhaddad:x:1002:1002:/:/home/rashidalhaddad:/bin/bash  
guest@rashidalhaddad:~$ █
```

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@rashidalhaddad:~$  
guest@rashidalhaddad:~$  
guest@rashidalhaddad:~$ ls -l /home  
итого 8  
drwx-----, 3 guest      guest      78 фев 5 2025 guest  
drwx-----, 14 rashidalhaddad rashidalhaddad 4096 авг 30 14:44 rashidalhaddad  
drwx-----, 14          1000      1000 4096 фев 5 2025 user  
guest@rashidalhaddad:~$
```

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@rashidalhaddad:~$  
guest@rashidalhaddad:~$ cd  
guest@rashidalhaddad:~$ mkdir dir1  
guest@rashidalhaddad:~$ ls -l | grep dir1/  
guest@rashidalhaddad:~$ ls -l | grep dir1  
drwxr-xr-x. 2 guest guest 6 авг 30 14:46 dir1  
guest@rashidalhaddad:~$ chmod 000 dir1/  
guest@rashidalhaddad:~$ ls -l | grep dir1  
d-----, 2 guest guest 6 авг 30 14:46 dir1  
guest@rashidalhaddad:~$ echo test > dir1/file1  
bash: dir1/file1: Отказано в доступе  
guest@rashidalhaddad:~$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
guest@rashidalhaddad:~$
```

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@rashidalhaddad:~  
/home/guest  
  
guest@rashidalhaddad:~$ ls -l | grep dir1  
d--x----- . 2 guest guest 6 авг 30 14:46 dir1  
guest@rashidalhaddad:~$ cd dir1/  
guest@rashidalhaddad:~/dir1$ cd ..  
guest@rashidalhaddad:~$ echo test > dir1/file1  
bash: dir1/file1: Отказано в доступе  
guest@rashidalhaddad:~$ chmod 200 dir1/  
guest@rashidalhaddad:~$ ls -l | grep dir1  
d-w----- . 2 guest guest 6 авг 30 14:46 dir1  
guest@rashidalhaddad:~$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
guest@rashidalhaddad:~$ echo test > dir1/file1  
bash: dir1/file1: Отказано в доступе  
guest@rashidalhaddad:~$ chmod 300 dir1/  
guest@rashidalhaddad:~$ ls -l | grep dir1  
d-wx----- . 2 guest guest 6 авг 30 14:46 dir1  
guest@rashidalhaddad:~$ cd dir1/  
guest@rashidalhaddad:~/dir1$ cd ..  
guest@rashidalhaddad:~$ echo test > dir1/file1  
guest@rashidalhaddad:~$ chmod 400 dir1/  
guest@rashidalhaddad:~$ ls -l | grep dir1  
dr----- . 2 guest guest 19 авг 30 14:48 dir1  
guest@rashidalhaddad:~$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
guest@rashidalhaddad:~$ echo test > dir1/file1  
bash: dir1/file1: Отказано в доступе  
guest@rashidalhaddad:~$
```

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)	+	+	+	-	+	+	+	+
d------(000)	--wx------(300)	-	-	-	-	-	-	-	-
d--x------(100)	--wx------(300)	-	-	+	-	+	-	-	+

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)	-	-	-	-	-	-	-	-

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)	+	+	+	+	+	+	+	+

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)
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