

Отчёт по лабораторной работе №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Магамадов Асхаб Ахиатович НБИбд-02-22

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

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.

```
cockpit-ws:instance:x:980:983:User for cockpit-ws:/usr/share/cockpit-ws:/usr/sbin/nologin  
flatpak:x:985:984:User for flatpak system helper:/usr/share/flatpak:/usr/sbin/nologin  
colord:x:984:983:User for colord:/usr/share/colord:/usr/sbin/nologin  
clevis:x:983:982:clevis Decryption Framework unprivileged user:/usr/share/colord:/usr/sbin/nologin  
setroubleshoot:x:982:981:SELinux troubleshoot server:/usr/share/colord:/usr/sbin/nologin  
gdm:x:42:42:GDM User:/usr/share/gdm:/usr/sbin/nologin  
gnome-initial-setup:x:981:980:Gnome Initial Setup:/usr/share/gnome-initial-setup:/usr/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty:/usr/sbin/nologin  
chrony:x:980:979:chrony system user:/usr/share/chrony:/usr/sbin/nologin  
dnsmasq:x:979:978:dnsmasq DHCP and DNS server:/usr/share/dnsmasq:/usr/sbin/nologin  
tcpdump:x:72:72:tcpdump:/usr/share/tcpdump:/usr/sbin/nologin  
aamagamadov:x:1000:1000:/home/aamagamadov:/bin/bash  
guest:x:1001:1001:/home/guest:/bin/bash  
[guest@aamagamadov ~]$
```

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.

```
dnsmasq:x:979:978:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72:::/sbin/nologin
aamagamadov:x:1000:1000::/home/aamagamadov:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
[guest@aamagamadov ~]$
[guest@aamagamadov ~]$ ls -l /home/
итого 4
drwx-----. 14 aamagamadov aamagamadov 4096 фев 21 12:04 aamagamadov
drwx-----. 3 guest guest 78 фев 21 12:06 guest
[guest@aamagamadov ~]$
```

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@aamagamadov ~]$
[guest@aamagamadov ~]$ cd
[guest@aamagamadov ~]$ mkdir dir1
[guest@aamagamadov ~]$ ls -l
итого 0
drwxr-xr-x. 2 guest guest 6 фев 21 12:12 dir1
[guest@aamagamadov ~]$ chmod 000 dir1/
[guest@aamagamadov ~]$ ls -l
итого 0
d-----. 2 guest guest 6 фев 21 12:12 dir1
[guest@aamagamadov ~]$ echo test > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@aamagamadov ~]$ cd dir1/
bash: cd: dir1/: Отказано в доступе
[guest@aamagamadov ~]$
```

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@aamagamadov:~
итого 0
d--x-----, 2 guest guest 6 фев 21 12:12 dir1
[guest@aamagamadov ~]$ echo test > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@aamagamadov ~]$ cd dir1/
[guest@aamagamadov dir1]$ cd ..
[guest@aamagamadov ~]$ chmod 200 dir1/
[guest@aamagamadov ~]$ ls -l
итого 0
d-w-----, 2 guest guest 6 фев 21 12:12 dir1
[guest@aamagamadov ~]$ echo test > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@aamagamadov ~]$ cd dir1/
bash: cd: dir1/: Отказано в доступе
[guest@aamagamadov ~]$ chmod 300 dir1/
[guest@aamagamadov ~]$ ls -l
итого 0
d-wx-----, 2 guest guest 6 фев 21 12:12 dir1
[guest@aamagamadov ~]$ echo test > /home/guest/dir1/file1
[guest@aamagamadov ~]$ cd dir1/
[guest@aamagamadov dir1]$ cd ..
[guest@aamagamadov ~]$ chmod 400 dir1/
[guest@aamagamadov ~]$ ls -l
итого 0
dr-----, 2 guest guest 19 фев 21 12:15 dir1
[guest@aamagamadov ~]$ echo test > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@aamagamadov ~]$ cd dir1/
bash: cd: dir1/: Отказано в доступе
[guest@aamagamadov ~]$ chmod 500 dir1/
[guest@aamagamadov ~]$ ls -l
итого 0
dr-x-----, 2 guest guest 19 фев 21 12:15 dir1
[guest@aamagamadov ~]$ echo test > /home/guest/dir1/file1
[guest@aamagamadov ~]$ cd dir1/
[guest@aamagamadov dir1]$ cd ..
[guest@aamagamadov ~]$
```

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