

Отчёт по лабораторной работе №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Булаев Максим Александрович НПИбд-01-19

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	5
2.2	Содержимое файла /etc/passwd	6
2.3	Расширенные атрибуты	6
2.4	Снятие атрибутов с директории	7

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 создал учётную запись пользователя guest (используя учётную запись администратора) и задал пароль для пользователя guest (используя учётную запись администратора).
2. Вошёл в систему от имени пользователя guest.
3. Командой `pwd` определил директорию, в которой нахожусь и определил, является ли она домашней директорией.
4. Уточнил имя моего пользователя командой `whoami`.
5. Уточнил имя пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. Сравнил вывод `id` с выводом команды `groups`. Видим, что `gid` и группы = 1001(guest).
6. Сравнил полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки и убедился, что они совпадают.

```
[guest@mabulaev ~]$ pwd
/home/guest
[guest@mabulaev ~]$ whoami
guest
[guest@mabulaev ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@mabulaev ~]$ groups
guest
[guest@mabulaev ~]$ █
```

Figure 2.1: Информация о пользователе guest

7. Просмотрел файл `/etc/passwd` Командой: `cat /etc/passwd`. Нашёл в нём свою учётную запись. Определил `uid` пользователя. Определил `gid` пользователя. Сравнил найденные значения с полученными в предыдущих пунктах. `Guest` имеет те же идентификаторы 1001, мой пользователь под идентификатором 1002.

```
polkitd:x:998:996:User for polkitd:/:sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:sbin/nologin
sssd:x:997:993:User for sssd:/:sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:sbin/nologin
pipewire:x:996:992:PipeWire System Daemon:/var/run/pipewire:sbin/nologin
libstoragemgmt:x:995:991:daemon account for libstoragemgmt:/var/run/lsm:sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:sbin/nologin
geoclue:x:994:989:User for geoclue:/var/lib/geoclue:sbin/nologin
cockpit-ws:x:993:988:User for cockpit web service:/nonexisting:sbin/nologin
cockpit-wsinstance:x:992:987:User for cockpit-ws instances:/nonexisting:sbin/nologin
setroubleshoot:x:991:986:SELinux troubleshoot server:/var/lib/setroubleshoot:sbin/nologin
flatpak:x:990:985:User for flatpak system helper:/:sbin/nologin
colord:x:989:984:User for colord:/var/lib/colord:sbin/nologin
clevis:x:988:983:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
gdm:x:42:42:/:/var/lib/gdm:sbin/nologin
systemd-oom:x:981:981:systemd Userspace OOM Killer:/usr/sbin/nologin
design:x:980:980:Group for the design signing daemon:/run/design:sbin/nologin
gnome-initial-setup:x:979:979:/:/run/gnome-initial-setup:sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:sbin/nologin
chrony:x:978:978:/:/var/lib/chrony:sbin/nologin
dnsmasq:x:977:977:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:sbin/nologin
tcpdump:x:72:72:/:sbin/nologin
mabulaev:x:1000:1000:mabulaev:/home/mabulaev:/bin/bash
vboxadd:x:976:1:/:/var/run/vboxadd:/bin/false
guest:x:1001:1001:/:/home/guest:/bin/bash
[guest@mabulaev ~]$
```

Figure 2.2: Содержимое файла `/etc/passwd`

8. Определил существующие в системе директории командой `ls -l /home/`.
9. Проверил, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой: `lsattr /home`. Мне не удалось увидеть расширенные атрибуты директорий других пользователей, только своей домашней директории.

```
[guest@mabulaev ~]$ ls -l /home/
total 8
drwx-----. 14 guest      guest      4096 Sep 17 15:47 guest
drwx-----. 14 mabulaev  mabulaev  4096 Sep 17 15:43 mabulaev
[guest@mabulaev ~]$ lsattr /home
lsattr: Permission denied while reading flags on /home/mabulaev
----- /home/guest
[guest@mabulaev ~]$
```

Figure 2.3: Расширенные атрибуты

10. Создал в домашней директории поддиректорию dir1 командой `mkdir dir1`.
Определил командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию dir1.
11. Снял с директории dir1 все атрибуты командой `chmod 000 dir1` и проверил с помощью `ls -l` правильность выполнения команды `chmod`.
12. Создал в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1`.
Поскольку ранее я отозвал все атрибуты, то тем самым лишил всех прав на взаимодействие с dir1.

```
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Videos
[guest@mabulaev ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
[guest@mabulaev ~]$ chmod 000 dir1
[guest@mabulaev ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Desktop
d----- . 2 guest guest 6 Sep 17 16:00 dir1
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Documents
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Music
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Public
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Templates
drwxr-xr-x. 2 guest guest 6 Sep 17 15:46 Videos
[guest@mabulaev ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@mabulaev ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
[guest@mabulaev ~]$
```

Figure 2.4: Снятие атрибутов с директории

13. Заполнил таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определил опытным путём, какие операции разрешены, а какие нет. Если операция была

разрешена, заносил в таблицу знак «+», если не была разрешена, знак «-».

- 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)	+	+	-	-	+	+	+	+

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

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

14. На основании таблицы выше определил минимально необходимые права для выполнения операций внутри директории dir1 и заполнил таблицу 2.2. Для заполнения последних двух строк опытным путем проверил 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

Таким образом, в ходе выполнения лабораторной работы я получил навыки работы с атрибутами файлов и сведения о разграничении доступа.

Список литературы

1. Теория разграничения прав пользователей
2. Разрешения доступа к файлам