

Лабораторная работа №2

Основы информационной безопасности

Черная София Витальевна

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	9
4.1	Заполнение таблицы 2.1	14
4.2	Заполнение таблицы 2.2	17
5	Выводы	19

Список иллюстраций

4.1	Guest	9
4.2	Password	9
4.3	Guest	10
4.4	pwd	10
4.5	cd ~	10
4.6	whoami	11
4.7	id, groups	11
4.8	Guest	11
4.9	/etc/passwd	12
4.10	Используя grep для фильтрации	12
4.11	Список поддиректорий директории /home	12
4.12	Просмотр атрибутов с помощью команды lsattr	13
4.13	Права	13
4.14	chmod 000	13
4.15	Попытка создать файл fil1 в dir1	14

Список таблиц

1 Цель работы

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.

2 Задание

1. Создание новой учетной записи `guest`
2. Работа с атрибутами файлов
3. Работа над созданием
4. Заполнение таблицы «Установленные права и разрешённые действия»
5. Определение тех или иные минимально необходимых прав для выполнения операций внутри директории `dir1`

3 Теоретическое введение

В операционной системе Linux команда `lsattr` отображает характеристики атрибутов и их возможные значения для устройств в системе. Использование в Linux команды `lsattr`

Логическое имя устройства следует указывать с помощью флага `-l` (Name), либо использовать комбинацию одного или всех флагов `-c` (Class), `-s` (Subclass) и `-t` (Type), чтобы однозначно идентифицировать предопределённое устройство. По умолчанию

На практике команда `lsattr` принимает в качестве аргументов имена файлов и каталогов для проверки. Если мы не указываем файл, он проверяет атрибуты текущего рабочего каталога.

В результате команда `lsattr` отображает по одному символу для каждого атрибута, чтобы указать, включён этот атрибут или нет:

```
oleg@mobile:~:$ lsattr abc.txt -----e---- abc.txt oleg@mobile:~:$
```

Однако `lsattr` не показывает имена атрибутов. Таким образом, нам, возможно, придётся знать значение каждого буквенного кода, чтобы интерпретировать вывод.

Права доступа делятся на три группы:

`user` — права владельца файла;

`group` — права группы, которой принадлежит файл;

`other` — права всех остальных пользователей системы.

Стандартными правами доступа являются:

для файлов – 644 (rw-r-r-);
для директорий – 755 (rwxr-xr-x).

4 Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе Rocky создаю учётную запись пользователя guest (используя учётную запись администратора): `useradd guest` (рис. 4.1).

```
[svchernaya@svchernaya ~]$ sudo useradd guest  
[sudo] пароль для svchernaya:
```

Рис. 4.1: Guest

2. Задаю пароль для пользователя guest (используя учётную запись администратора) с помощью команды: `passwd guest` (рис. 4.2).

```
[svchernaya@svchernaya ~]$ sudo passwd guest  
[sudo] пароль для svchernaya:  
Изменение пароля пользователя guest.  
Новый пароль:  
Повторите ввод нового пароля:  
passwd: данные аутентификации успешно обновлены.
```

Рис. 4.2: Password

3. Вхожу в систему от имени пользователя guest (рис. 4.3).

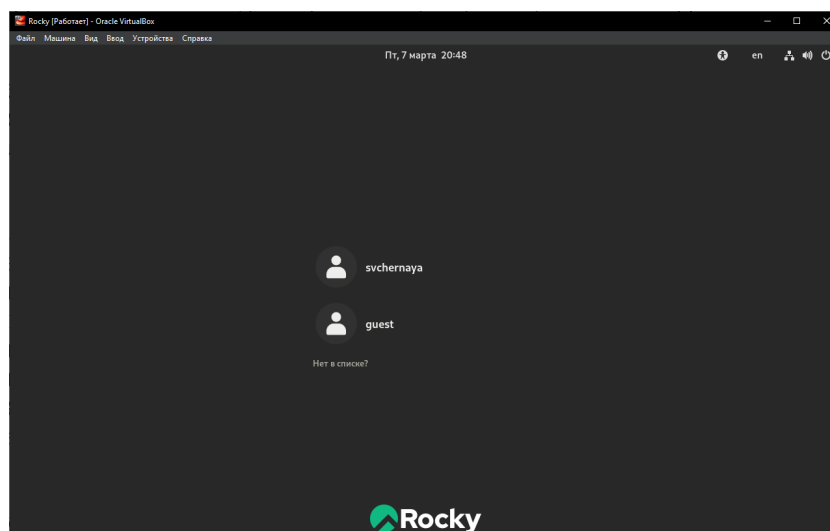


Рис. 4.3: Guest

4. Определяю директорию, в которой я нахожусь, командой `pwd`. Результат получаю : `/home/guest`. Однако в приглашении командной строки стоит знак `~` , указывающий, что данная директория является домашней.(рис. 4.4).

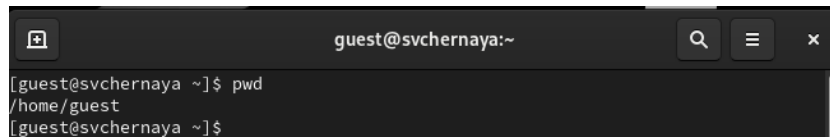


Рис. 4.4: pwd

Проверяю, на всякий случай, командой перехода в домашнюю директорию : `cd ~`. Директория, в которой мы находились, не изменилась, что свидетельствует о том, что мы действительно находимся в домашней директории(рис. 4.5).

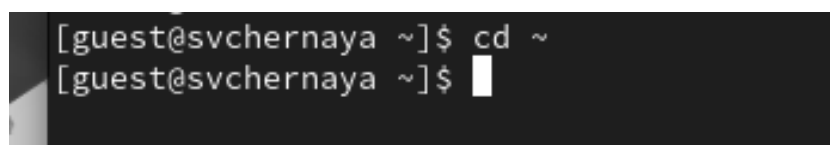


Рис. 4.5: cd ~

5. Уточняю имя моего пользователя командой `whoami`(рис. 4.6).

```
[guest@svchernaya ~]$ whoami
guest
```

Рис. 4.6: `whoami`

6. Уточняю имя моего пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. запоминаю. Сравниваю вывод `id` с выводом команды `groups`. Замечаю, что с помощью команды `id` можно узнать больше информации о пользователе `guest` и его группы(рис. 4.7).

```
[guest@svchernaya ~]$ id
uid=1001(guest) gid=1001(guest) rpynm=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@svchernaya ~]$ groups
guest
```

Рис. 4.7: `id`, `groups`

7. Сравниваю полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки и замечаю, что они совпадают.(рис. 4.6).

```
[guest@svchernaya ~]$ whoami
guest
```

Рис. 4.8: `Guest`

8. Просматриваю файл `/etc/passwd` командой `cat /etc/passwd`. Нахожу в нем свою учетную запись(выделено красным), определяю, что `uid` пользователя и `gid` пользователя равны 1001. Они совпадают с запомненными мною ранее при выводе с помощью команды `id`(рис. 4.9).

```

[guest@svchernaya ~]$ 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
tss:x:59:59:Account used for TPM access:/usr/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
sssd:x:997:995:User for sssd:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
geoclue:x:996:994:User for geoclue:/var/lib/geoclue:/sbin/nologin
rtkit:x:12:122:RealtimeKit:/sbin/nologin
pipewire:x:995:992:Pipewire System Daemon:/run/pipewire:/usr/sbin/nologin
libstoragemgmt:x:990:990:daemon account for libstoragemgmt:/usr/sbin/nologin
cockpit-ws-instance:x:989:988:User for cockpit-ws instances/nonexisting:/sbin/nologin
Flatpak:x:988:987:User for Flatpak system helper:/sbin/nologin
colord:x:987:986:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:986:985:clevis Decryption Framework unprivileged user:/var/cache/clevis/user:/sbin/nologin
setroubleshoot:x:985:984:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
stapuppriv:x:159:159:systemtap unprivileged user:/var/lib/stapuppriv:/sbin/nologin
pesign:x:984:983:Group for the pesign signing daemon:/run/psign:/sbin/nologin
gnome-initial-setup:x:983:982:/run/gnome-initial-setup:/sbin/nologin
chrony:x:982:981:chrony system user:/var/lib/chrony:/sbin/nologin
sahsi:x:74:74:Privilege-separated SSH:/usr/share/empty.ssh:/usr/sbin/nologin
dnsmasq:x:981:980:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/sbin/nologin
svchernaya:x:1000:1000:svchernaya:/home/svchernaya:/bin/bash
xoboadi:x:1001:1:/var/run/xoboadi:/bin/false
guest:x:1001:1001:/home/guest:/bin/bash

```

Рис. 4.9: /etc/passwd

Проверяю себя с помощью команды `cat /etc/passwd | grep guest`. Убеждаюсь, что я все определила верно.(рис. 4.10).

```

[guest@svchernaya ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001::/home/guest:/bin/bash

```

Рис. 4.10: Использую грейп для фильтрации

- Вывожу список поддиректорий директории /home и их права. Замечаю, что все права есть только у создателя директории, у группы и остальных пользователей никаких прав нет.(рис. 4.11).

```

[guest@svchernaya ~]$ ls -l /home/
итого 8
drwx-----. 14 guest      guest      4096 map  7 20:47 guest
drwx-----. 17 svchernaya svchernaya 4096 map  7 19:39 svchernaya

```

Рис. 4.11: Список поддиректорий директории /home

- Проверяю есть ли какие-нибудь расширенные атрибуты на поддиректориях с помощью команды `lsattr`. Нет, никаких атрибутов у поддиректорий нет. Увидеть расширенные атрибуты у других пользователей так же не удалось(рис. 4.12).

```
[guest@svchernaya ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/svchernaya
----- /home/guest
[guest@svchernaya ~]$ lsattr /home/guest/Документы
----- /home/guest/Документы/hernya.txt
[guest@svchernaya ~]$ lsattr /home/guest/Документы/hernya.txt
----- /home/guest/Документы/hernya.txt
```

Рис. 4.12: Просмотр атрибутов с помощью команды lsattr

11. Создаю в домашней директории поддиректорию dir1 с помощью команды mkdir. Определяю командами ls -l и lsattr какие права доступа и расширенные атрибуты были выставлены на директорию dir1. С помощью команды ls -l узнаю, что у создателя есть все права(на чтение, на записывание и на заход в директорию). У группы и остальных пользователей есть те же права, кроме записывания(создания файлов или удаление например). Команда lsattr ничего не выводит. (рис. 4.13).

```
[guest@svchernaya ~]$ ls -l
итого 0
drwxr-xr-x. 2 guest guest 6 map 7 21:14 dir1
drwxr-xr-x. 2 guest guest 6 map 7 20:47 Видео
drwxr-xr-x. 2 guest guest 24 map 7 21:10 Документы
drwxr-xr-x. 2 guest guest 6 map 7 20:47 Загрузки
drwxr-xr-x. 2 guest guest 6 map 7 20:47 Изображения
drwxr-xr-x. 2 guest guest 6 map 7 20:47 Музыка
drwxr-xr-x. 2 guest guest 6 map 7 20:47 Общедоступные
drwxr-xr-x. 2 guest guest 6 map 7 20:47 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 map 7 20:47 Шаблоны
[guest@svchernaya ~]$ lsattr /home/guest/dir1
```

Рис. 4.13: Права

12. Снимаю все атрибуты с директории dir1 с помощью команды chmod 000 dir1. Проверяю права доступа с помощью ls -l/Замечаю, что теперь у всех нет прав ни на что.(рис. 4.14).

```
[guest@svchernaya ~]$ chmod 000 dir1
[guest@svchernaya ~]$ ls -l
итого 0
d-----, 2 guest guest 6 map 7 21:14 dir1
drwxr-xr-x. 2 guest guest 6 map 7 20:47 Видео
drwxr-xr-x. 2 guest guest 24 map 7 21:10 Документы
drwxr-xr-x. 2 guest guest 6 map 7 20:47 Загрузки
drwxr-xr-x. 2 guest guest 6 map 7 20:47 Изображения
drwxr-xr-x. 2 guest guest 6 map 7 20:47 Музыка
drwxr-xr-x. 2 guest guest 6 map 7 20:47 Общедоступные
drwxr-xr-x. 2 guest guest 6 map 7 20:47 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 map 7 20:47 Шаблоны
```

Рис. 4.14: chmod 000

13. Пытаюсь создать в директории `dir1` файл `fil1` командой `echo "test" > /home/guest/dir1/file1`. Отказ в доступе происходит из-за команды `chmod 000`, которая убирает все права у всех пользователей. Так же `ls -l /home/guest/dir1` показывает, что файла нет. (рис. 4.15).

```
[guest@svchernaya ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@svchernaya ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе
```

Рис. 4.15: Попытка создать файл `fil1` в `dir1`

- 14.

4.1 Заполнение таблицы 2.1

Права дирек- тории	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Смена дирек- тории	Просмотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d(000)	(000)	-	-	-	-	-	-	-
d(000)	(100)	-	-	-	-	-	-	-
d(000)	(200)	-	-	-	-	-	-	-
d(000)	(300)	-	-	-	-	-	-	-
d(000)	(400)	-	-	-	-	-	-	-
d(000)	(500)	-	-	-	-	-	-	-
d(000)	(600)	-	-	-	-	-	-	-
d(000)	(700)	-	-	-	-	-	-	-
d(100)	(000)	-	-	-	-	+	-	-
d(100)	(100)	-	-	-	-	+	-	-

Права дирек- тории	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Смена дирек- тории	Просмотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d(100)	(200)	-	-	+	-	+	-	-
d(100)	(300)	-	-	+	-	+	-	-
d(100)	(400)	-	-	-	+	+	-	-
d(100)	(500)	-	-	-	+	+	-	-
d(100)	(600)	-	-	+	+	+	-	-
d(100)	(700)	-	-	+	+	+	-	-
d(200)	(000)	-	-	-	-	-	-	-
d(200)	(100)	-	-	-	-	-	-	-
d(200)	(200)	-	-	-	-	-	-	-
d(200)	(300)	-	-	-	-	-	-	-
d(200)	(400)	-	-	-	-	-	-	-
d(200)	(500)	-	-	-	-	-	-	-
d(200)	(600)	-	-	-	-	-	-	-
d(200)	(700)	-	-	-	-	-	-	-
d(300)	(000)	+	+	-	-	+	-	+
d(300)	(100)	+	+	-	-	+	-	+
d(300)	(200)	+	+	+	-	+	-	+
d(300)	(300)	+	+	+	-	+	-	+
d(300)	(400)	+	+	-	+	+	-	+
d(300)	(500)	+	+	-	+	+	-	+
d(300)	(600)	+	+	+	+	+	-	+
d(300)	(700)	+	+	+	+	+	-	+
d(400)	(000)	-	-	-	-	-	+	-
d(400)	(100)	-	-	-	-	-	+	-

Права дирек- тории	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Смена дирек- тории	Просмотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d(400)	(200)	-	-	-	-	-	+	-
d(400)	(300)	-	-	-	-	-	+	-
d(400)	(400)	-	-	-	-	-	+	-
d(400)	(500)	-	-	-	-	-	+	-
d(400)	(600)	-	-	-	-	-	+	-
d(400)	(700)	-	-	-	-	-	+	-
d(500)	(000)	-	-	-	-	+	+	-
d(500)	(100)	-	-	-	-	+	+	-
d(500)	(200)	-	-	+	-	+	+	-
d(500)	(300)	-	-	+	-	+	+	-
d(500)	(400)	-	-	-	+	+	+	-
d(500)	(500)	-	-	-	+	+	+	-
d(500)	(600)	-	-	+	+	+	+	-
d(500)	(700)	-	-	+	+	+	+	-
d(600)	(000)	-	-	-	-	-	+	-
d(600)	(100)	-	-	-	-	-	+	-
d(600)	(200)	-	-	-	-	-	+	-
d(600)	(300)	-	-	-	-	-	+	-
d(600)	(400)	-	-	-	-	-	+	-
d(600)	(500)	-	-	-	-	-	+	-
d(600)	(600)	-	-	-	-	-	+	-
d(600)	(700)	-	-	-	-	-	+	-
d(700)	(000)	+	+	-	-	+	+	+
d(700)	(100)	+	+	-	-	+	+	+

Права дирек- тории	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Смена дирек- тории	Просмотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d(700)	(200)	+	+	+	-	+	+	+
d(700)	(300)	+	+	+	-	+	+	+
d(700)	(400)	+	+	-	+	+	+	+
d(700)	(500)	+	+	-	+	+	+	+
d(700)	(600)	+	+	+	+	+	+	+
d(700)	(700)	+	+	+	+	+	+	+

15.

4.2 Заполнение таблицы 2.2

Операция	Минималь- ные права на директорию	Минималь- ные права на файл
Создание файла	d(300)	-
Удаление файла	d(300)	-
Чтение файла	d(100)	(400)
Запись в файл	d(100)	(200)

Переименование файла	d(300)	(000)
Создание под-директории	d(300)	-
Удаление под-директории	d(300)	-

5 Выводы

Были получены практические навыки работы в консоли с атрибутами файлов, закреплены теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.