

Отчет по лабораторной работе №2

Дисциплина: Информационная безопасность

Кабанова Варвара Дмитриевна

Содержание

| | |
|--------------------------------------|---|
| Цель работы | 1 |
| Задание | 1 |
| Выполнение лабораторной работы | 1 |
| Атрибуты файлов | 1 |
| Заполнение таблицы 2.1 | 4 |
| Заполнение таблицы 2.2 | 7 |
| Выводы | 8 |
| Список литературы | 8 |

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

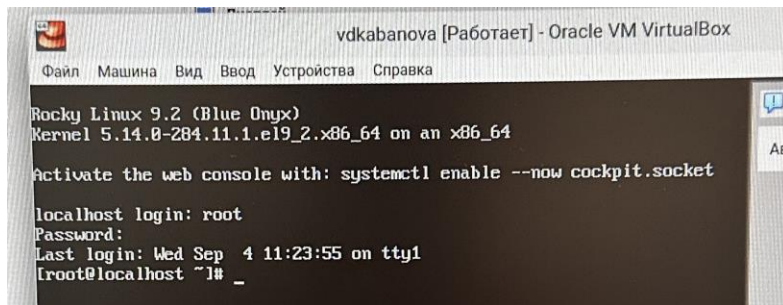
Задание

1. Работа с атрибутами файлов
2. Заполнение таблицы “Установленные права и разрешённые действия” (см. табл. 2.1)
3. Заполнение таблицы “Минимальные права для совершения операций” (см. табл. 2.2)

Выполнение лабораторной работы

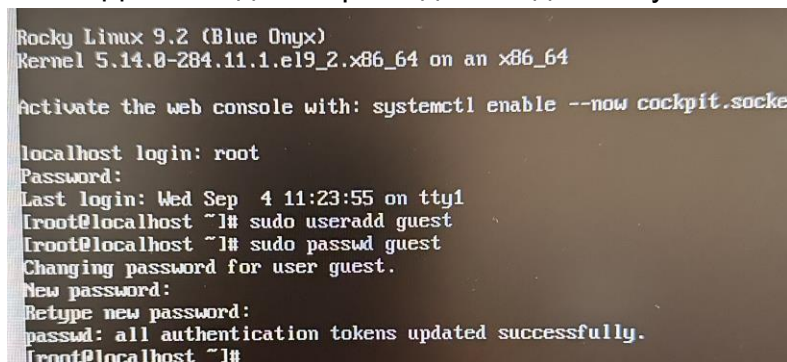
Атрибуты файлов

1. В операционной системе Rocky создаю нового пользователя guest через учетную запись администратора, задаю логин root (рис. 1).



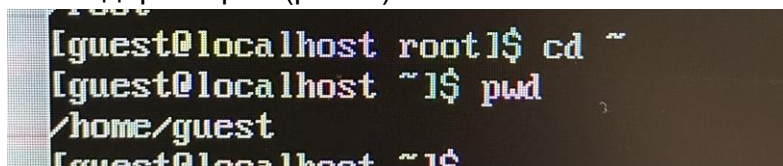
Добавление пользователя

2. Далее задаю пароль для созданной учетной записи (рис. 2).



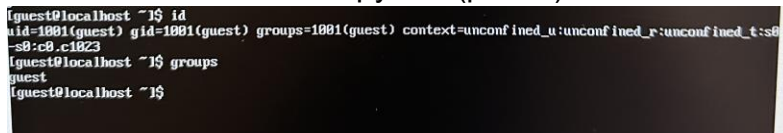
Добавление пароля для пользователя

3. Определяю с помощью команды `pwd`, что я нахожусь в директории `/home/guest/`. Эта директория является домашней, ведь в приглашении командой строкой стоит значок `~`, указывающий, что я в домашней директории (рис. 3).



Текущая директория

4. В выводе команды `groups` информация только о названии группы, к которой относится пользователь. В выводе команды `id` можно найти больше информации: имя пользователя и имя группы, также коды имени пользователя и группы (рис. 4)



Информация о пользователе

5. Имя пользователя в приглашении командной строкой совпадает с именем пользователя, которое выводит команда `whoami` (рис. 5)

```

/home/guest
[guest@localhost ~]$ whoami
guest
[guest@localhost ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001

```

Сравнение информации об имени пользователя

6. Получаю информацию о пользователе с помощью команды
`cat /etc/passwd | grep guest`

В выводе получаю коды пользователя и группы, адрес домашней директории (рис. 6).

```

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

```

Просмотр файла passwd

7. Да, список поддиректорий директории home получилось получить с помощью команды `ls -l`, если мы добавим опцию `-a`, то сможем увидеть еще и директорию пользователя root. Права у директории:

root: drwxr-xr-x,

evdvorkina и guest: drwx— (рис. 7).

```

[guest@localhost ~]$ ls -l /home/
total 0
drwx-----. 2 guest      guest      62 Sep  9 13:23 guest
drwx-----. 2 vdkabanova vdkabanova 62 Sep  4 11:28 vdkabanova
[guest@localhost ~]$ ls -la /home/
total 0
drwxr-xr-x. 4 root        root       37 Sep  9 13:23 .
dr-xr-xr-x. 18 root        root       235 Sep  4 18:53 ..
drwx-----. 2 guest      guest      62 Sep  9 13:23 guest
drwx-----. 2 vdkabanova vdkabanova 62 Sep  4 11:28 vdkabanova
[guest@localhost ~]$

```

Просмотр содержимого директории

8. Пыталась проверить расширенные атрибуты директорий. Нет, их увидеть не удалось (рис. 8). Увидеть расширенные атрибуты других пользователей, тоже не удалось, для них даже вывода списка директорий не было.

```

[guest@localhost ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/vdkabanova
-----
/home/guest
[guest@localhost ~]$ _

```

Проверка расширенных атрибутов

9. Создаю поддиректорию dir1 для домашней директории. Расширенные атрибуты командой `lsattr` просмотреть у директории не удастся, но атрибуты есть: drwxr-xr-x, их удалось просмотреть с помощью команды `ls -l` (рис. 9).

```

[guest@localhost ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/vdkabanova
----- /home/guest
[guest@localhost ~]$ mkdir dir1
[guest@localhost ~]$ ls -la
total 12
drwx-----. 3 guest guest 74 Sep  9 13:42 .
drwxr-xr-x. 4 root  root  37 Sep  9 13:23 ..
-rw-r--r--. 1 guest guest 18 Jan 24  2023 .bash_logout
-rw-r--r--. 1 guest guest 141 Jan 24  2023 .bash_profile
-rw-r--r--. 1 guest guest 492 Jan 24  2023 .bashrc
drwxr-xr-x. 2 guest guest  6 Sep  9 13:42 dir1
[guest@localhost ~]$

```

Создание поддиректории

10. Снимаю атрибуты командой `chmod 000 dir1`, при проверке с помощью команды `ls -l` видно, что теперь атрибуты действительно сняты (рис. 10).

```

drwxr-xr-x. 2 guest guest  6 Sep  9 13:42 dir1
[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$ ls -l
total 0
d-----. 2 guest guest 6 Sep  9 13:42 dir1
[guest@localhost ~]$

```

Снятие атрибутов с директории

11. Попытка создать файл в директории `dir1`. Выдает ошибку: "Отказано в доступе" (рис. 11).

```

d-----. 2 guest guest 6 Sep  9 13:42 dir1
[guest@localhost ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@localhost ~]$ _

```

{#fig:011width=70%}

Вернув права директории и используя снова команду `ls -l` можно убедиться, что файл не был создан (рис. 12).

```

bash: /home/guest/dir1/file1: Permission denied
[guest@localhost ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
[guest@localhost ~]$

```

Проверка содержимого директории

Заполнение таблицы 2.1

| Права дирек- тории | Права файла | Созда- ние файла | Удале- ние файла | Запис- ь в файл | Чтени- е файла | Смена дирек- тории | Просм- отр файло- в в дирек- тории | Переи- мено- вание файла | Смена атриб- утов 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) | - | - | - | - | + | - | - | + |
| 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) | - | - | - | - | - | + | - | - |
| 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) | + | + | - | - | + | + | + | + |
| d(700) | (200) | + | + | + | - | + | + | + | + |
| d(700) | (300) | + | + | + | - | + | + | + | + |
| d(700) | (400) | + | + | - | + | + | + | + | + |
| d(700) | (500) | + | + | - | + | + | + | + | + |
| d(700) | (600) | + | + | + | + | + | + | + | + |
| d(700) | (700) | + | + | + | + | + | + | + | + |

Таблица 2.1 «Установленные права и разрешённые действия»

Пример заполнения таблицы 2.1 (рис. 13).


```

chmod: cannot access 'dirl/test': Permission denied
lguest@localhost ~1$ ls l dirl
ls: cannot access 'l': No such file or directory
ls: cannot open directory 'dirl': Permission denied
lguest@localhost ~1$ chmod 000 dirl
lguest@localhost ~1$ rm dirl/test
rm: cannot remove 'dirl/test': Permission denied
lguest@localhost ~1$ echo 'test' > test
lguest@localhost ~1$ echo 'test' > dirl/test
bash: dirl/test: Permission denied
lguest@localhost ~1$ cat dirl/test
cat: dirl/test: Permission denied
lguest@localhost ~1$ mv dirl/test ~
mv: cannot stat 'dirl/test': Permission denied
lguest@localhost ~1$ ls -l dirl
ls: cannot open directory 'dirl': Permission denied
lguest@localhost ~1$ mv dirl/test dirl/test10
mv: failed to access 'dirl/test10': Permission denied
lguest@localhost ~1$ chmod 100 dirl/test
chmod: cannot access 'dirl/test': Permission denied
lguest@localhost ~1$ chmod 700 dirl
lguest@localhost ~1$ chmod 100 dirl/test
chmod: cannot access 'dirl/test': No such file or directory
lguest@localhost ~1$ chmod 000 dirl
lguest@localhost ~1$ chmod 000 dirl

```

Изменение прав директории и файла

Заполнение таблицы 2.2

| Операция | Минимальные права на директорию | Минимальные 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 поддиректории | d(300) | - |
| Удаление поддиректории | d(300) | - |

Таблица 2.2 “Минимальные права для совершения операций”

Пример заполнения таблицы 2.2 (рис. 14)

```

lguest@localhost ~1$ chmod 000 dirl
lguest@localhost ~1$ chmod 000 dirl
lguest@localhost ~1$ rmdir dirl/b
rmdir: failed to remove 'dirl/b': Permission denied
lguest@localhost ~1$ chmod 100 dirl
lguest@localhost ~1$ rmdir dirl/b
rmdir: failed to remove 'dirl/b': No such file or directory
lguest@localhost ~1$ chmod 300 dirl
lguest@localhost ~1$ rmdir dirl/b

```

Проверка возможности создать поддиректорию

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.

Список литературы

Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet. – НПО "Мир и семья-95", 1997. – URL:
<http://bugtraq.ru/library/books/attack1/index.html>
Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на Internet. – Издательство ДМК, 1999. – URL:
<http://bugtraq.ru/library/books/attack/index.html>
Запечников С. В. и др. Информационная безопасность открытых систем. Том 1. – М.: Горячая линия -Телеком, 2006.
Операционные системы: <https://blog.skillfactory.ru/glossary/operaczionnaya-sistema/>
Права доступа: <https://codechick.io/tutorials/unix-linux/unix-linux-permissions>