

Отчёт по лабораторной работе № 2

Дисциплина: Основы информационной безопасности

Перелыгин Сергей Викторович

Содержание

1	Цель работы	4
2	Задание	5
3	Теоретическое введение	6
4	Выполнение лабораторной работы	8
5	Выводы	23
6	Библиография	24

Список иллюстраций

4.1	Рисунок 1	8
4.2	Рисунок 2	9
4.3	Рисунок 3	10
4.4	Рисунок 4	11
4.5	Рисунок 5	11
4.6	Рисунок 6	12
4.7	Рисунок 7	13
4.8	Рисунок 8	14
4.9	Рисунок 9	14
4.10	Рисунок 10	15

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

- Сделать отчёт по лабораторной работе в формате Markdown.
- В качестве отчёта предоставить отчёты в 3 форматах: pdf, docx и md.

3 Теоретическое введение

В операционной системе Linux есть много отличных функций безопасности, но одна из самых важных - это система прав доступа к файлам. Изначально каждый файл имел три параметра доступа. Вот они:

- Чтение - разрешает получать содержимое файла, но на запись нет. Для каталога позволяет получить список файлов и каталогов, расположенных в нем
- Запись - разрешает записывать новые данные в файл или изменять существующие, а также позволяет создавать и изменять файлы и каталоги
- Выполнение - невозможно выполнить программу, если у нее нет флага выполнения. Этот атрибут устанавливается для всех программ и скриптов, именно с помощью него система может понять, что этот файл нужно запускать как программу

Каждый файл имеет три категории пользователей, для которых можно устанавливать различные сочетания прав доступа:

- Владелец - набор прав для владельца файла, пользователя, который его создал или сейчас установлен его владельцем. Обычно владелец имеет все права, чтение, запись и выполнение
- Группа - любая группа пользователей, существующая в системе и привязанная к файлу. Но это может быть только одна группа и обычно это группа владельца, хотя для файла можно назначить и другую группу
- Остальные - все пользователи, кроме владельца и пользователей, входящих в группу файла

Команды, которые могут понадобиться при работе с правами доступа:

- “ls -l” - для просмотра прав доступа к файлам и каталогам
- “chmod категория действие флаг файл или каталог” - для изменения прав доступа к файлам и каталогам (категорию действие и флаг можно заменить на набор из трех цифр от 0 до

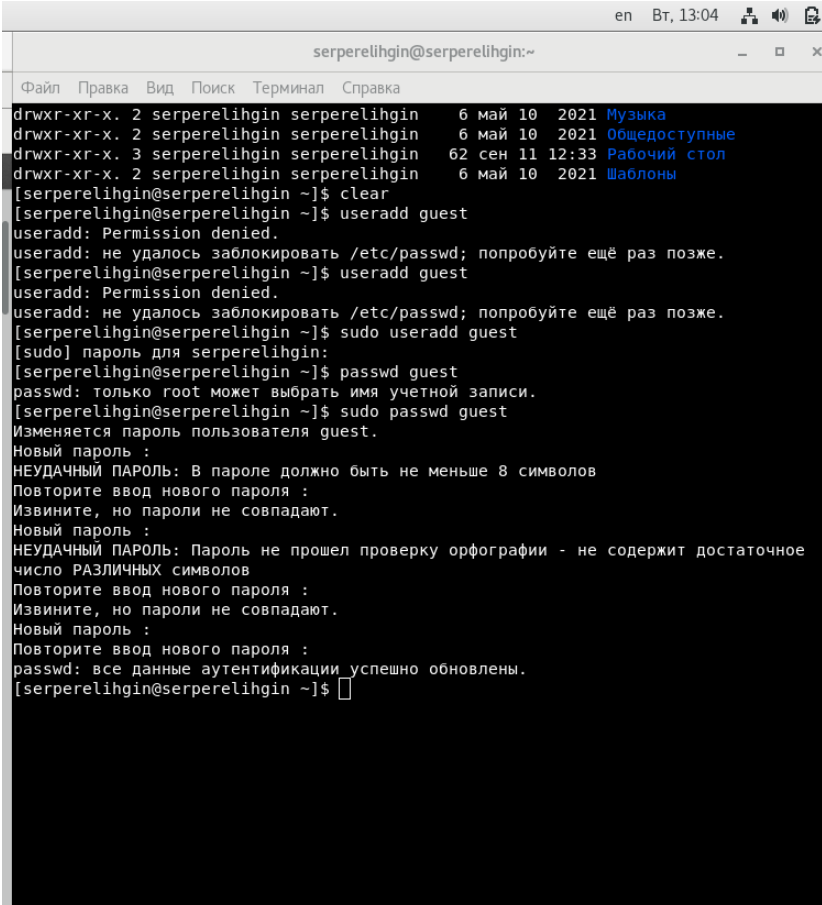
7)

Значения флагов прав:

- — - нет никаких прав
- -x - разрешено только выполнение файла, как программы, но не изменение и не чтение
- -w- - разрешена только запись и изменение файла
- -wx - разрешено изменение и выполнение, но в случае с каталогом, невозможно посмотреть его содержимое
- r- - права только на чтение
- r-x - только чтение и выполнение, без права на запись
- rw- - права на чтение и запись, но без выполнения
- rwx - все права

4 Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создаю учётную запись пользователя guest (используя учётную запись администратора): `sudo useradd guest` и задаю пароль для этого пользователя командой “`sudo passwd guest`” (рис. 1).



```
serperelihgin@serperelihgin:~$ clear
serperelihgin@serperelihgin ~]$ useradd guest
useradd: Permission denied.
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.
serperelihgin@serperelihgin ~]$ useradd guest
useradd: Permission denied.
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.
serperelihgin@serperelihgin ~]$ sudo useradd guest
[sudo] пароль для serperelihgin:
serperelihgin@serperelihgin ~]$ passwd guest
passwd: только root может выбрать имя учетной записи.
serperelihgin@serperelihgin ~]$ sudo passwd guest
Изменяется пароль пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: В пароле должно быть не меньше 8 символов
Повторите ввод нового пароля :
Извините, но пароли не совпадают.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - не содержит достаточное
число РАЗЛИЧНЫХ символов
Повторите ввод нового пароля :
Извините, но пароли не совпадают.
Новый пароль :
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
serperelihgin@serperelihgin ~]$
```

Рис. 4.1: Рисунок 1

2. Далее я зашел в систему от имени пользователя guest (рис. 2).

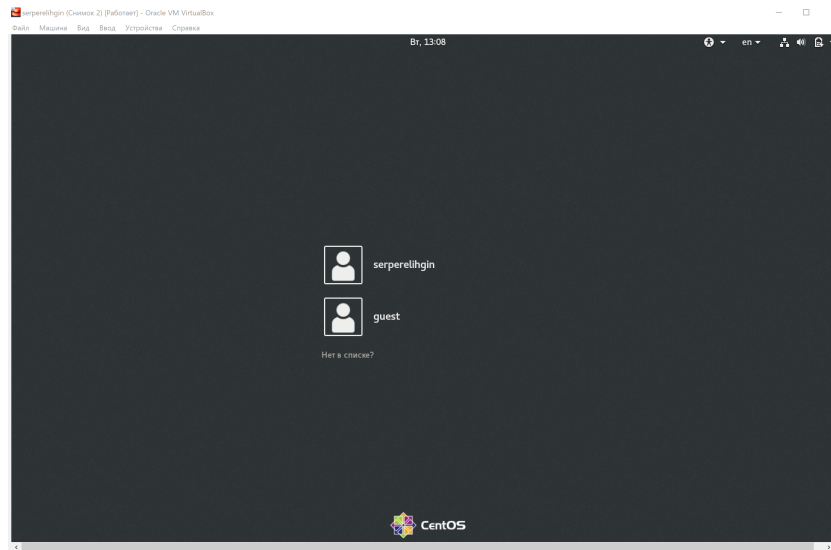
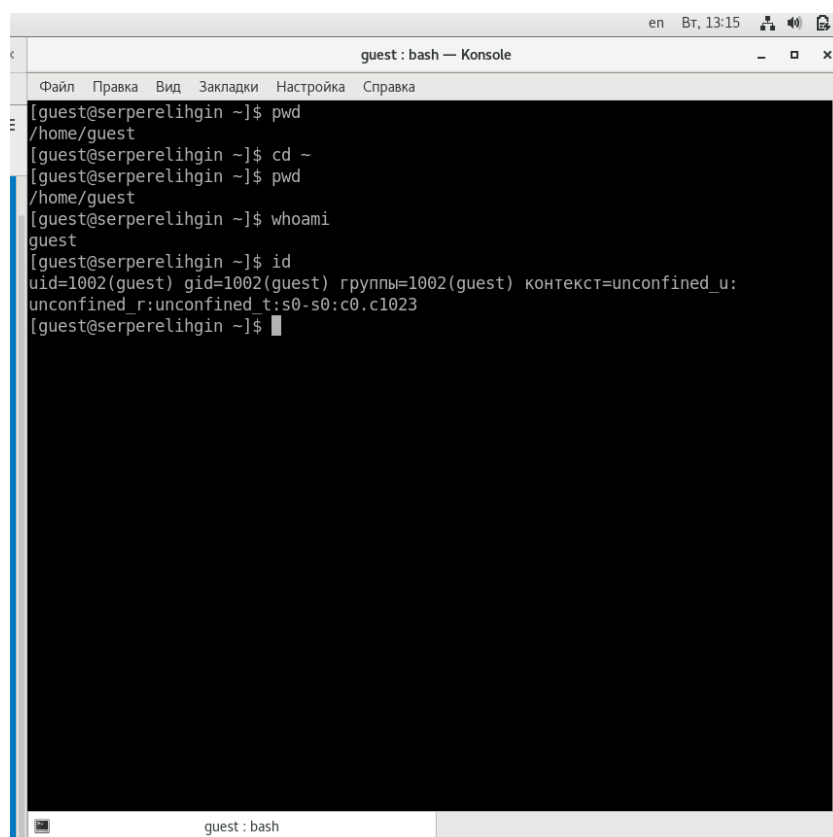


Рис. 4.2: Рисунок 2

3. Командой `pwd` определил директорию, в которой нахожусь. Сравнил её с приглашением командной строки: является моей домашней директорией (рис. 3).
4. Уточнил имя моего пользователя командой `whoami` и получил вывод: `guest` (рис. 3).
5. С помощью команды `id` определил имя своего пользователя - всё так же `guest`, `uid = 1002 (guest)`, `gid = 1002 (guest)` (рис. 3).



```
guest : bash — Konsole
Файл  Правка  Вид  Закладки  Настройка  Справка

[guest@serperelihgin ~]$ pwd
/home/guest
[guest@serperelihgin ~]$ cd ~
[guest@serperelihgin ~]$ pwd
/home/guest
[guest@serperelihgin ~]$ whoami
guest
[guest@serperelihgin ~]$ id
uid=1002(guest) gid=1002(guest) группы=1002(guest) контекст=unconfined_u:
unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@serperelihgin ~]$
```

Рис. 4.3: Рисунок 3

6. Затем сравнил полученную информацию с выводом команды “groups”, которая вывела “guest”. Мой пользователь входит только в одну группу, состоящую из него самого, поэтому вывод обеих команд “id” и “groups” совпадает (рис. 4). Данные, выводимые в приглашении командной строки, совпадают с полученной информацией (рис. 4).

Затем просмотрел файл /etc/passwd командой “cat /etc/passwd” (рис. 4).

```
Приложения Места guest: bash — Konsole en Br, 13:20
guest: bash — Konsole
Файл Правка Вид Закладки Настройка Справка
[guest@serperelighin ~]$ pwd
/home/guest
[guest@serperelighin ~]$ whoami
guest
[guest@serperelighin ~]$ id
uid=1002(guest) gid=1002(guest) группы=1002(guest) контекст=unconfined_u:
unconfined_r:unconfined_t:s8-sb:c0.c1023
[guest@serperelighin ~]$ groups
guest
[guest@serperelighin ~]$ 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:99:99:nobody:/:/sbin/nologin
systemd-network:x:102:102:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:system message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
libstoragemgmt:x:998:996:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nolo
gin
colord:x:997:995:User for colord:/var/lib/colord:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
sane:x:996:994:SANE Scanner daemon user:/usr/share/sane:/sbin/nologin
sasauthd:x:995:76:sasauthd user:/run/sasauthd:/sbin/nologin
abrt:x:173:173:/etc/abrt:/sbin/nologin
```

Рис. 4.4: Рисунок 4

7. Нашел в нём свою учётную запись в самом конце (рис. 5). Uid = 1002, gid = 1002, то есть они совпадают с тем, что мы получили ранее.

```
Приложения Места guest: bash — Konsole en Br, 13:21
guest: bash — Konsole
Файл Правка Вид Закладки Настройка Справка
sasauthd:x:995:76:sasauthd user:/run/sasauthd:/sbin/nologin
abrt:x:173:173:/etc/abrt:/sbin/nologin
setroubleshoot:x:994:991:/var/lib/setroubleshoot:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
radvd:x:75:75:radvd user:/:/sbin/nologin
chrony:x:993:988:/var/lib/chrony:/sbin/nologin
unbound:x:992:987:Unbound DNS resolver:/etc/unbound:/sbin/nologin
qemu:x:107:107:qemu user:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/n
ull:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
geoclue:x:991:985:User for geoclue:/var/lib/geoclue:/sbin/nologin
gluster:x:990:984:GlusterFS daemons:/run/gluster:/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
gnome-initial-setup:x:989:983:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
postfix:x:89:89:/var/spool/postfix:/sbin/nologin
ntp:x:38:38:/etc/ntp:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
serperelighin:x:1000:1000:serperelighin:/home/serperelighin:/bin/bash
vboxadd:x:988:1:/var/run/vboxadd:/bin/false
mysql:x:27:27:MySQL Server:/var/lib/mysql:/sbin/nologin
sssd:x:987:981:User for sssd:/:/sbin/nologin
vboxsf:x:1001:1000:/home/vboxsf:/bin/bash
guest:x:1002:1002:/home/guest:/bin/bash
[guest@serperelighin ~]$
```

Рис. 4.5: Рисунок 5

Также использовал для поиска команду `cat /etc/passwd | grep guest` (рис. 6).

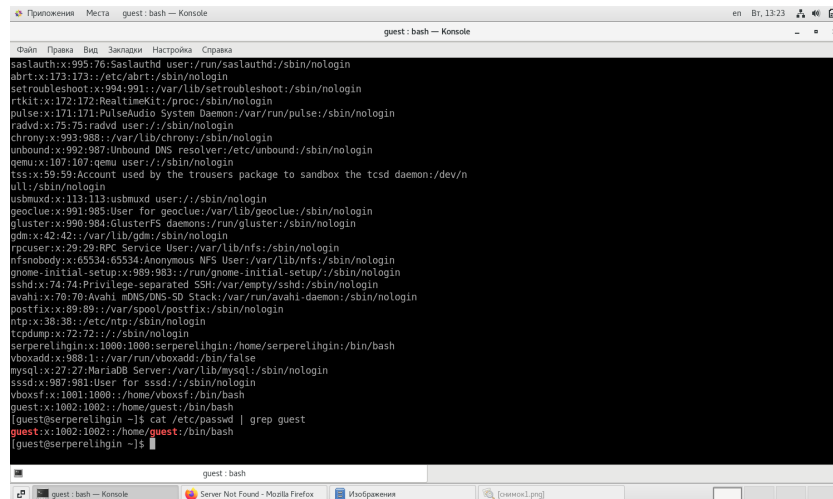


Рис. 4.6: Рисунок 6

8. Посмотрел, какие директории существуют в системе командой “ls -l /home/” (рис. 7). Список поддиректорий директории /home получить удалось. На директориях установлены права чтения, записи и выполнения для самого пользователя (для группы и остальных пользователей никаких прав доступа не установлено). Проверил, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой “lsattr /home” (рис. 7). Удалось увидеть расширенные атрибуты только директории того пользователя, от имени которого я нахожусь в системе. Создал в домашней директории поддиректорию dir1 командой “mkdir dir1” и определил, какие права доступа и расширенные атрибуты были на неё выставлены: чтение, запись и выполнение доступны для самого пользователя и для группы, для остальных - только чтение и выполнение, расширенных атрибутов не установлено (рис. 7).

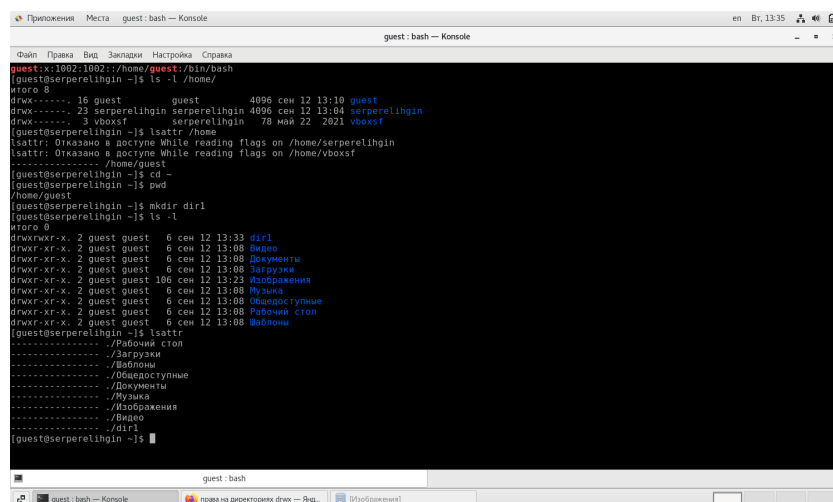


Рис. 4.7: Рисунок 7

9. Снял с директории `dir1` все атрибуты командой `“chmod 000 dir1”` и проверил с её помощью правильность выполнения команды `“ls -l”`. Действительно, все атрибуты были сняты (рис. 8). Попытался создать в директории `dir1` файл `file1` командой `echo “test” > /home/guest/dir1/file1` (рис. 8). Этого сделать не получилось, т.к. предыдущим действием мы убрали право доступа на запись в директории. В итоге файл не был создан (открыть директорию с помощью команды `“ls -l /home/guest/dir1”` изначально тоже не удалось по той же причине, поэтому я поменял права доступа и снова воспользовался этой командой, и тогда смог просмотреть содержимое директории, убедившись, что файл не был создан).

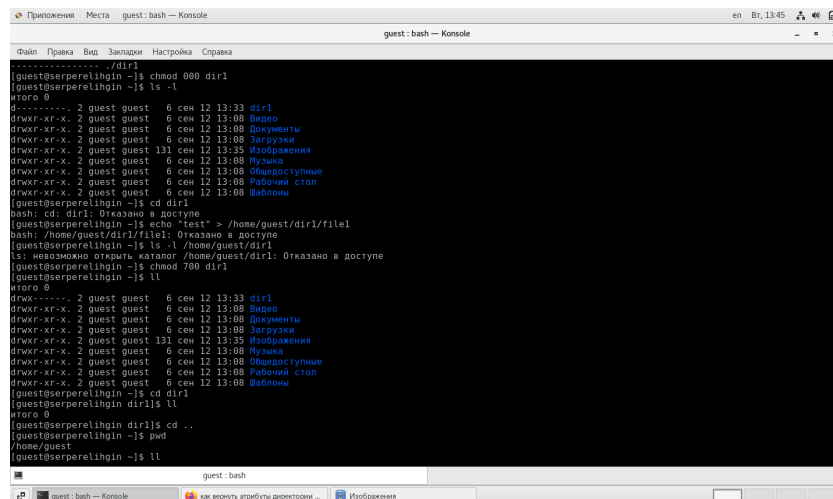


Рис. 4.8: Рисунок 8

10. Заполним таблицу «Установленные права и разрешённые действия»(рис. 9-10). Создание файла: “echo”text” > /home/guest/dir1/file2” Удаление файла: “rm -r /home/guest/dir1/file2” Запись в файл: “echo”text_2” > /home/guest/dir1/file2” Чтение файла: “cat /home/guest/dir1/file1” Смена директории: “cd dir1” Просмотр файлов в директории: “ls dir1” Переименование файла: “mv /home/guest/dir1/file1 file2” Смена атрибутов файла: “chattr -a /home/guest/dir1/file1”

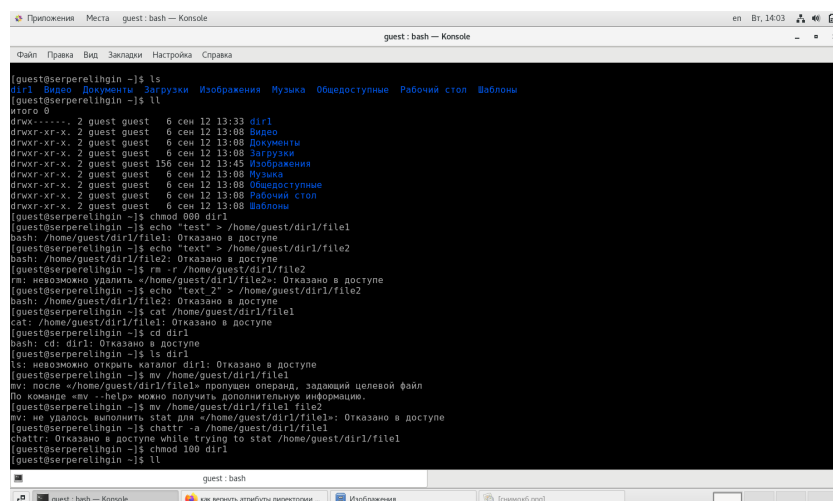


Рис. 4.9: Рисунок 9

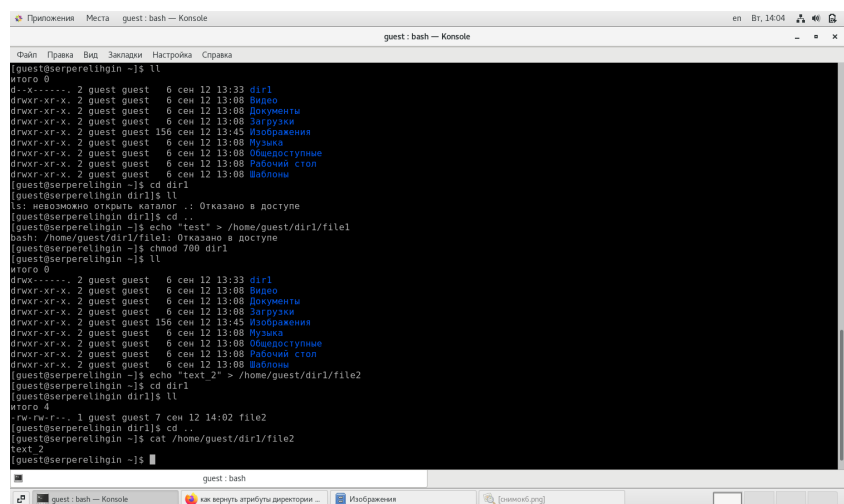


Рис. 4.10: Рисунок 10

11. Заполним таблицы.

В случае успеха будет записывать +, в случае ошибки доступа будем записывать -. Соберём данные в таблицу 1.

Таблица 4.1: Установленные права и разрешённые действия {табл. 1}

Смена									
ат-									
ри-									
бу-									
Просмотр									
файлов									
Запись									
Смена									
в									
Переименование									
Права	Права	Создание	Удаление	в	Чтение	Смена	в	Переименование	файла
директории	файла	файла	файла	файл	файла	директории	директории	файла	файла
d (000)	(000)	-	-	-	-	-	-	-	-
d -x	(000)	-	-	-	-	+	-	-	-
(100)									
d -w-	(000)	-	-	-	-	-	-	-	-
(200)									
d -wx	(000)	+	+	-	-	+	-	+	-
(300)									

									Смена
									ат-
									ри-
									бу-
									Смена
Права	Права	Создание	Удаление	Запись	Чтение	Смена	Просмотр	Переименование	Смена
директории	файла	файла	файла	файл	файла	директории	файлов	файла	файла
d r-	(000)	-	-	-	-	-	+	-	-
(400)									
d r-x	(000)	-	-	-	-	+	+	-	-
(500)									
d rw-	(000)	-	-	-	-	-	+	-	-
(600)									
d rwx	(000)	+	+	-	-	+	+	+	-
(700)									
d (000)	-x	-	-	-	-	-	-	-	-
	(100)								
d -x	-x	-	-	-	-	+	-	-	-
(100)	(100)								
d -w-	-x	-	-	-	-	-	-	-	-
(200)	(100)								
d -wx	-x	+	+	-	-	+	-	+	-
(300)	(100)								
d r-	-x	-	-	-	-	-	+	-	-
(400)	(100)								
d r-x	-x	-	-	-	-	+	+	-	-
(500)	(100)								
d rw-	-x	-	-	-	-	-	+	-	-
(600)	(100)								

									Смена
									ат-
									ри-
									бу-
									Смена
Права	Права	Создание	Удаление	Запись	Чтение	Смена	Просмотр	Переименование	Смена
директории	файла	файла	файла	файл	файла	директории	директории	файла	файла
d rwx	-x	+	+	-	-	+	+	+	-
(700)	(100)								
d (000)	-w-	-	-	-	-	-	-	-	-
	(200)								
d -x	-w-	-	-	+	-	+	-	-	-
(100)	(200)								
d -w-	-w-	-	-	-	-	-	-	-	-
(200)	(200)								
d -wx	-w-	+	+	+	-	+	-	+	-
(300)	(200)								
d r-	-w-	-	-	-	-	-	+	-	-
(400)	(200)								
d r-x	-w-	-	-	+	-	+	+	-	-
(500)	(200)								
d rw-	-w-	-	-	-	-	-	+	-	-
(600)	(200)								
d rwx	-w-	+	+	+	-	+	+	+	-
(700)	(200)								
d (000)	-wx	-	-	-	-	-	-	-	-
	(300)								
d -x	-wx	-	-	+	-	+	-	-	-
(100)	(300)								

									Смена
									ат-
									ри-
									бу-
									Смена
Права	Права	Создание	Удаление	Запись	Чтение	Смена	Просмотр	Переименование	Смена
директории	файла	файла	файла	файл	файла	директории	директории	файла	файла
d -w-	-wx	-	-	-	-	-	-	-	-
(200)	(300)								
d -wx	-wx	+	+	+	-	+	-	+	-
(300)	(300)								
d r-	-wx	-	-	-	-	-	+	-	-
(400)	(300)								
d r-x	-wx	-	-	+	-	+	+	-	-
(500)	(300)								
d rw-	-wx	-	-	-	-	-	+	-	-
(600)	(300)								
d rwx	-wx	+	+	+	-	+	+	+	-
(700)	(300)								
d (000)	r-	-	-	-	-	-	-	-	-
	(400)								
d -x	r-	-	-	-	+	+	-	-	+
(100)	(400)								
d -w-	r-	-	-	-	-	-	-	-	-
(200)	(400)								
d -wx	r-	+	+	-	+	+	-	+	+
(300)	(400)								
d r-	r-	-	-	-	-	-	+	-	-
(400)	(400)								

									Смена
									ат-
									ри-
									бу-
									Смена
Права	Права	Создание	Удаление	Запись	Чтение	Смена	Просмотр	Переименование	Смена
директории	файла	файла	файла	файл	файла	директории	директории	файла	файла
d r-x	r-	-	-	-	+	+	+	-	+
(500)	(400)								
d rw-	r-	-	-	-	-	-	+	-	-
(600)	(400)								
d rwx	r-	+	+	-	+	+	+	+	+
(700)	(400)								
d (000)	r-x	-	-	-	-	-	-	-	-
	(500)								
d -x	r-x	-	-	-	+	+	-	-	+
(100)	(500)								
d -w-	r-x	-	-	-	-	-	-	-	-
(200)	(500)								
d -wx	r-x	+	+	-	+	+	-	+	+
(300)	(500)								
d r-	r-x	-	-	-	-	-	+	-	-
(400)	(500)								
d r-x	r-x	-	-	-	+	+	+	-	+
(500)	(500)								
d rw-	r-x	-	-	-	-	-	+	-	-
(600)	(500)								
d rwx	r-x	+	+	-	+	+	+	+	+
(700)	(500)								

									Смена
									ат-
									ри-
									бу-
									Смена
Права	Права	Создание	Удаление	Запись	Чтение	Смена	Просмотр	Переименование	Смена
директории	файла	файла	файла	файл	файла	директории	директории	файла	файла
d (000)	rw-	-	-	-	-	-	-	-	-
	(600)								
d -x	rw-	-	-	+	+	+	-	-	+
(100)	(600)								
d -w-	rw-	-	-	-	-	-	-	-	-
(200)	(600)								
d -wx	rw-	+	+	+	+	+	-	+	+
(300)	(600)								
d r-	rw-	-	-	-	-	-	+	-	-
(400)	(600)								
d r-x	rw-	-	-	+	+	+	+	-	+
(500)	(600)								
d rw-	rw-	-	-	-	-	-	+	-	-
(600)	(600)								
d rwx	rw-	+	+	+	+	+	+	+	+
(700)	(600)								
d (000)	rwX	-	-	-	-	-	-	-	-
	(700)								
d -x	rwX	-	-	+	+	+	-	-	+
(100)	(700)								
d -w-	rwX	-	-	-	-	-	-	-	-
(200)	(700)								

Права директории	Права файла	Создание файла	Удаление файла	Запись файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена ат- ри- бу- ции
d -wx (300)	rwX (700)	+	+	+	+	+	-	+	+
d r- (400)	rwX (700)	-	-	-	-	-	+	-	-
d r-x (500)	rwX (700)	-	-	+	+	+	+	-	+
d rw- (600)	rwX (700)	-	-	-	-	-	+	-	-
d rwx (700)	rwX (700)	+	+	+	+	+	+	+	+

На основании этой таблицы создадим другую, в которой опишем минимальные требования на права и директорию для выполнения тех или иных действий. Внесём проанализированные данные в таблицу 2.

Таблица 4.2: Минимальные права для совершения операций {табл. 2}

Операция	Минимальные права на директорию	Минимальные 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)

Операция	Минимальные права на директорию	Минимальные права на файл
Удаление поддиректории	d -wx (300)	— (000)

5 Выводы

Вывод: В ходе выполнения данной лабораторной работы я приобрел практические навыки работы в консоли с атрибутами файлов, закрепил теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

6 Библиография

- 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.
- Введение в информационную безопасность. Типы уязвимостей. (Д.Гамаюнов, МГУ)
- Практические аспекты сетевой безопасности. Вводная лекция. Сетевая безопасность. Стек протоколов TCP/IP. (Д. Гамаюнов, МГУ)
- Практические аспекты сетевой безопасности. Сетевая безопасность. Межсетевые экраны. (В. Иванов, МГУ)
- Практические аспекты сетевой безопасности. Сетевая безопасность. Системы обнаружения и фильтрации компьютерных атак (IDS/IPS). (Д. Гамаюнов, МГУ)
- Практические аспекты сетевой безопасности. Контроль нормального поведения приложений. Security Enhanced Linux (SELinux) (В. Сахаров, МГУ)