

Отчёт по лабораторной работе №2.

Информационная безопасность

Дискреционное разграничение прав в Linux. Основные атрибуты

Выполнила: Данзанова Саяна, НПИбд-01-21, 1032217624

Содержание

Цель работы	4
Теоретическое введение	5
Выполнение лабораторной работы	6
Атрибуты файлов	6
Заполнение таблицы 2.1	10
Заполнение таблицы 2.2	14
Вывод	16
Список литературы. Библиография	17

Список иллюстраций

1	(рис. 1. useradd guest, passwd guest)	6
2	(рис. 2. log in)	7
3	(рис. 3. pwd)	7
4	(рис. 4. whoami)	7
5	(рис. 5. id и groups)	8
6	(рис. 6. cat /etc/passwd)	8
7	(рис. 7. ls -l /home/)	9
8	(рис. 8. lsattr /home)	9
9	(рис. 9. mkdir dir1)	9
10	(рис. 10. chmod 000 dir1)	10
11	(рис. 11. “test” > /home/guest/dir1/file1)	10
12	(рис. 12. Проверка директории d(000) и d(100) с правами файла 000) . . .	13
13	(рис. 13. Проверка на минимальные необходимы права на создание под- директории)	15

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

Теоретическое введение

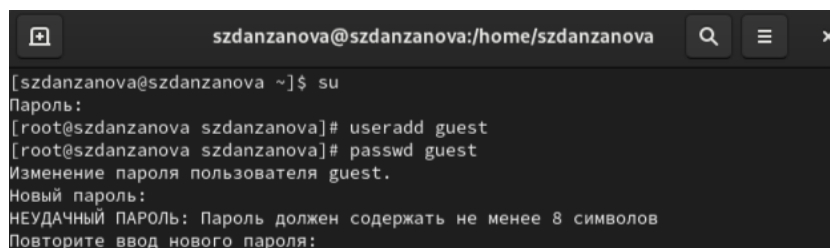
Операционная система — то комплекс программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем [1].

Права доступа определяют, какие действия конкретный пользователь может или не может совершать с определенными файлами и каталогами. С помощью разрешений можно создать надежную среду — такую, в которой никто не может поменять содержимое ваших документов или повредить системные файлы. [2].

Выполнение лабораторной работы

Атрибуты файлов

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создайте учётную запись пользователя guest (используя учётную запись администратора): `useradd guest`
2. Задайте пароль для пользователя guest (используя учётную запись администратора): `passwd guest`



```
szdanzanova@szdanzanova:/home/szdanzanova
[szdanzanova@szdanzanova ~]$ su
Пароль:
[root@szdanzanova szdanzanova]# useradd guest
[root@szdanzanova szdanzanova]# passwd guest
Изменение пароля пользователя guest.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
```

Рис. 1: (рис. 1. `useradd guest`, `passwd guest`)

2. Войдите в систему от имени пользователя guest.

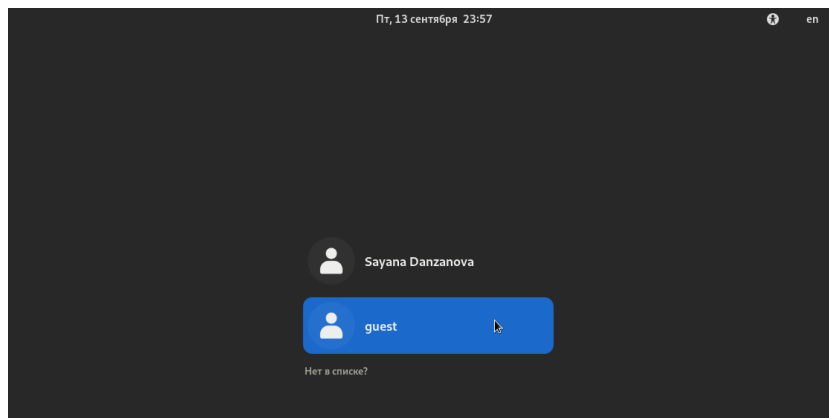


Рис. 2: (рис. 2. log in)

3. Определите директорию, в которой вы находитесь, командой `pwd`. Сравните её с приглашением командной строки. Определите, является ли она вашей домашней директорией? Если нет, зайдите в домашнюю директорию.

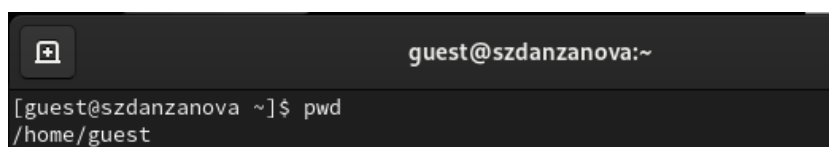


Рис. 3: (рис. 3. pwd)

5. Уточните имя вашего пользователя командой `whoami`.

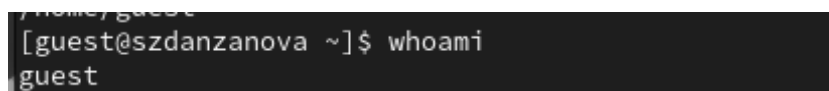


Рис. 4: (рис. 4. whoami)

6. Уточните имя вашего пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. запомните. Сравните вывод `id` с выводом команды `groups`.

```
[guest@szdanzanova ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
[guest@szdanzanova ~]$ groups
guest
```

Рис. 5: (рис. 5. id и groups)

7. Просмотрите файл /etc/passwd командой cat /etc/passwd Найдите в нём свою учётную запись. Определите uid пользователя. Определите gid пользователя. Сравните найденные значения с полученными в предыдущих пунктах.

```
[guest@szdanzanova ~]$ 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
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
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pipewire:x:997:994:PipeWire System Daemon:/run/pipewire:/usr/sbin/nologin
sssd:x:996:993:User for sssd:/sbin/nologin
libstoragemgmt:x:991:991:daemon account for libstoragemgmt:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/usr/sbin/nologin
geoclue:x:990:989:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:989:988:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:988:987:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:987:986:User for flatpak system helper:/sbin/nologin
colord:x:986:985:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:985:984:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:984:983:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
pesign:x:983:982:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
gnome-initial-setup:x:982:981:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
chrony:x:981:980:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:980:979:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/sbin/nologin
szdanzanova:x:1000:1000:Sayana Danzanova:/home/szdanzanova:/bin/bash
guest:x:1001:1001:/home/guest:/bin/bash
```

Рис. 6: (рис. 6. cat /etc/passwd)

8. Определите существующие в системе директории командой ls -l /home/ Удалось ли вам получить список поддиректорий директории /home? Какие права установлены на директориях?


```
[guest@szdanzanova ~]$ is -l /home/
bash: is: команда не найдена...
[guest@szdanzanova ~]$ ls -l /home/
итого 8
drwx-----. 14 guest      guest      4096 сен 13 23:58 guest
drwx-----. 16 szdanzanova szdanzanova 4096 сен  8 18:26 szdanzanova
```

Рис. 7: (рис. 7. ls -l /home/)

9. Проверьте, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: lsattr /home. Удалось ли вам увидеть расширенные атрибуты директории? Удалось ли вам увидеть расширенные атрибуты директорий других пользователей?

```
[guest@szdanzanova ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/szdanzanova
----- /home/guest
```

Рис. 8: (рис. 8. lsattr /home)

10. Создайте в домашней директории поддиректорию dir1 командой mkdir dir1. Определите командами ls -l и lsattr, какие права доступа и расширенные атрибуты были выставлены на директорию dir1.

```
[guest@szdanzanova ~]$ mkdir dir1
[guest@szdanzanova ~]$ ls -l
итого 0
drwxr-xr-x. 2 guest guest 6 сен 14 00:06 dir1
drwxr-xr-x. 2 guest guest 6 сен 13 23:58 Видео
drwxr-xr-x. 2 guest guest 6 сен 13 23:58 Документы
drwxr-xr-x. 2 guest guest 6 сен 13 23:58 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 13 23:58 Изображения
drwxr-xr-x. 2 guest guest 6 сен 13 23:58 Музыка
drwxr-xr-x. 2 guest guest 6 сен 13 23:58 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 13 23:58 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 сен 13 23:58 Шаблоны
```

Рис. 9: (рис. 9. mkdir dir1)

11. Снимите с директории dir1 все атрибуты командой chmod 000 dir1 и проверьте с её помощью правильность выполнения команды ls -l

```
[guest@szdanzanova ~]$ chmod 000 dir1
[guest@szdanzanova ~]$ ls -l
итого 0
d----- . 2 guest guest 6 сен 14 00:06 dir1
drwxr-xr-x. 2 guest guest 6 сен 13 23:58 Видео
drwxr-xr-x. 2 guest guest 6 сен 13 23:58 Документы
drwxr-xr-x. 2 guest guest 6 сен 13 23:58 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 13 23:58 Изображения
drwxr-xr-x. 2 guest guest 6 сен 13 23:58 Музыка
drwxr-xr-x. 2 guest guest 6 сен 13 23:58 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 13 23:58 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 сен 13 23:58 Шаблоны
```

Рис. 10: (рис. 10. chmod 000 dir1)

12. Попробуйте создать в директории dir1 файл file1 командой echo “test” > /home/guest/dir1/file1. Объясните, почему вы получили отказ в выполнении операции по созданию файла? Оцените, как сообщение об ошибке отразилось на создании файла? Проверьте командой ls -l /home/guest/dir1 действительно ли файл file1 не находится внутри директории dir1.

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

Рис. 11: (рис. 11. “test” > /home/guest/dir1/file1)

Заполнение таблицы 2.1

13. Заполните таблицу «Установленные права и разрешённые действия» (см. табл. 2.1), выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесите в таблицу знак «+», если не разрешена, знак «-».

Права дирек- тории	Права файла	Созда- ние файла	Удале- ние файла	За- пись в файл	Чте- ние файла	Смена дирек- тории	Про- смотр фай- лов в дирек- тории	Переиме- нование файла	Смена атри- бутов 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:

```
[guest@szdanzanova dirl]$ touch test
touch: невозможно выполнить touch для 'test': Отказано в доступе
[guest@szdanzanova dirl]$ chmod 000 test
chmod: невозможно получить доступ к 'test': Нет такого файла или каталога
[guest@szdanzanova dirl]$ chmod 000 test1
chmod: невозможно получить доступ к 'test1': Нет такого файла или каталога
[guest@szdanzanova dirl]$ touch test1
touch: невозможно выполнить touch для 'test1': Отказано в доступе
[guest@szdanzanova dirl]$ rm test
rm: невозможно удалить 'test': Нет такого файла или каталога
[guest@szdanzanova dirl]$ echo 'test' > test
bash: test: Отказано в доступе
[guest@szdanzanova dirl]$ cat test
cat: test: Нет такого файла или каталога
[guest@szdanzanova dirl]$ ls -l /home/guest/dirl/
ls: невозможно открыть каталог '/home/guest/dirl/': Отказано в доступе
[guest@szdanzanova dirl]$ mv test test1
mv: не удалось выполнить stat для 'test': Нет такого файла или каталога
[guest@szdanzanova dirl]$ chmod 100 test
chmod: невозможно получить доступ к 'test': Нет такого файла или каталога
[guest@szdanzanova dirl]$
```

Рис. 12: (рис. 12. Проверка директории d(000) и d(100) с правами файла 000)

Заполнение таблицы 2.2

14. На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения операций внутри директории `dir1`, заполните табл. 2.2.

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d(300)	(000)
Удаление файла	d(300)	(000)
Чтение файла	d(100)	(400)
Запись в файл	d(100)	(200)
Переименование файла	d(300)	(000)
Создание поддиректории	d(300)	(000)
Удаление поддиректории	d(300)	(000)

Таблица 2.2 “Минимальные права для совершения операций”

Пример заполнения таблицы 2.2:

```
[guest@szdanzanova dirl]$ cd
[guest@szdanzanova ~]$ chmod 000 dirl
[guest@szdanzanova ~]$ mk dirl/dir2
bash: mk: команда не найдена...
[guest@szdanzanova ~]$ mkdir dirl/dir2
mkdir: невозможно создать каталог «dirl/dir2»: Отказано в доступе
[guest@szdanzanova ~]$ chmod 100 dirl
[guest@szdanzanova ~]$ mkdir dirl/dir2
mkdir: невозможно создать каталог «dirl/dir2»: Отказано в доступе
[guest@szdanzanova ~]$ chmod 200 dirl
[guest@szdanzanova ~]$ mkdir dirl/dir2
mkdir: невозможно создать каталог «dirl/dir2»: Отказано в доступе
[guest@szdanzanova ~]$ chmod 300 dirl
[guest@szdanzanova ~]$ mkdir dirl/dir2
[guest@szdanzanova ~]$
```

Рис. 13: (рис. 13. Проверка на минимальные необходимы права на создание поддиректории)

Вывод

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. Библиография

[1] Операционные системы: <https://blog.skillfactory.ru/glossary/operaczionnaya-sistema/>

[2] Права доступа: <https://codechick.io/tutorials/unix-linux/unix-linux-permissions>