

# **Основы информационной безопасности**

**Лабораторная работа № 2**

Оразгелдиев Язгелди

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>8</b>
3.1	Заполнение таблицы 2.1 . . . . .	11
3.2	Заполнение таблицы 2.2 . . . . .	14
<b>4</b>	<b>Выводы</b>	<b>15</b>

## Список иллюстраций

3.1	Создание учетной записи guest . . . . .	8
3.2	Данные о guest . . . . .	9
3.3	id, gid пользователя . . . . .	9
3.4	Создание поддиректории и ее местонахождение . . . . .	10
3.5	Команды для нашего dirl . . . . .	10
3.6	Команды для нашего dirl . . . . .	11

## 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

Постарайтесь последовательно выполнить все пункты, занося ваши ответы на поставленные вопросы и замечания в отчёт. 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` 3. Войдите в систему от имени пользователя `guest`. 4. 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. 5. Уточните имя вашего пользователя командой `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`. 7. Сравните полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки. 8. 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. Замечание: в случае, когда вывод команды не умещается на одном экране монитора, используйте прокрутку вверх–вниз (удерживая клавишу `shift`, нажимайте `page up` и `page down`) либо программу `grep` в качестве фильтра для вывода только строк, содержащих определённые буквенные сочетания: `cat /etc/passwd | grep guest` 9. Определите существующие в системе директории командой `ls -l /home/` Удалось ли вам получить список поддиректо-

рий директории /home? Какие права установлены на директориях? 10. 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? 11. 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`. 12. Снимите с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверьте с её помощью правильность выполнения команды `ls -l` 13. 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`. 14. 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 «-». 15. На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения операций внутри директории `dir1`, заполните табл. 2.2.

### 3 Выполнение лабораторной работы

1. Создаем гостевую дополнительную учетную запись и входим в виртуальную машину от его имени.

```
[yazgeldi_o@localhost ~]$ useradd guest
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
[yazgeldi_o@localhost ~]$ sudo useradd guest
[sudo] password for yazgeldi_o:
[yazgeldi_o@localhost ~]$ passwd guest
passwd: Only root can specify a user name.
[yazgeldi_o@localhost ~]$ sudo passwd guest
Changing password for user guest.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[yazgeldi_o@localhost ~]$
```

Рис. 3.1: Создание учетной записи guest

2. Мы в новой учетной записи прописываем некоторые команды для того, чтобы вывести информацию о пользователе guest



```
[guest@localhost ~]$ pwd
/home/guest
[guest@localhost ~]$ whami
bash: whami: command not found...
[guest@localhost ~]$ whoami
guest
[guest@localhost ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:
s0-s0:c0.c1023
[guest@localhost ~]$ 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:997:993:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
sssd:x:996:992:User for sssd:/sbin/nologin
libstoragemgmt:x:990:990:daemon account for libstoragemgmt:/usr/sbin/nologin
systemd-oom:x:989:989:systemd Userspace OOM Killer:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/usr/sbin/nologin
geoclue:x:988:987:User for geoclue:/var/lib/geoclue:/sbin/nologin
```

Рис. 3.2: Данные о guest

### 3. Определяем uid, gid пользователя и сравниваем с предыдущими пунктами

```
[guest@localhost ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001::/home/guest:/bin/bash
[guest@localhost ~]$ ls -l /home/
total 8
drwx-----. 14 guest      guest      4096 Mar  1 21:45 guest
drwx-----. 16 yazgeldi_o yazgeldi_o 4096 Mar  1 20:42 yazgeldi_o
[guest@localhost ~]$ lsattr /home
lsattr: Permission denied while reading flags on /home/yazgeldi_o
----- /home/guest
[guest@localhost ~]$ sudo lsattr /home

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for guest:
guest is not in the sudoers file. This incident will be reported.
```

Рис. 3.3: id, gid пользователя

### 4. Создаем поддиректорию dirl

```
[guest@localhost ~]$ mkdir dirl
[guest@localhost ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Mar  1 21:45 Desktop
drwxr-xr-x. 2 guest guest 6 Mar  1 21:50 dirl
drwxr-xr-x. 2 guest guest 6 Mar  1 21:45 Documents
drwxr-xr-x. 2 guest guest 6 Mar  1 21:45 Downloads
drwxr-xr-x. 2 guest guest 6 Mar  1 21:45 Music
drwxr-xr-x. 2 guest guest 6 Mar  1 21:45 Pictures
drwxr-xr-x. 2 guest guest 6 Mar  1 21:45 Public
drwxr-xr-x. 2 guest guest 6 Mar  1 21:45 Templates
drwxr-xr-x. 2 guest guest 6 Mar  1 21:45 Videos
[guest@localhost ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dirl
```

Рис. 3.4: Создание поддиректории и ее местонахождение

5. Тестируем на поддиректории различные команды и изменяем права доступа. Проверяем работу команд

```
[guest@localhost ~]$ echo "test" > /home/guest/dirl/file1
bash: /home/guest/dirl/file1: Permission denied
[guest@localhost ~]$ ;s dirl
bash: syntax error near unexpected token `;'
[guest@localhost ~]$ ls dirl
ls: cannot open directory 'dirl': Permission denied
[guest@localhost ~]$ rm dirl/test
rm: cannot remove 'dirl/test': Permission denied
[guest@localhost ~]$ echo "test" > test
[guest@localhost ~]$ echo "test" > dirl/test
bash: dirl/test: Permission denied
[guest@localhost ~]$ cat dirl/test
cat: dirl/test: Permission denied
[guest@localhost ~]$ mv dirl/test ~
mv: cannot stat 'dirl/test': Permission denied
[guest@localhost ~]$ ls -l dirl
ls: cannot open directory 'dirl': Permission denied
[guest@localhost ~]$ mv dirl/test dirl/test10
mv: failed to access 'dirl/test10': Permission denied
[guest@localhost ~]$ chmod 100 dir/test
chmod: cannot access 'dir/test': No such file or directory
[guest@localhost ~]$ chmod 700 dirl
[guest@localhost ~]$ chmod 100 dirl/test
chmod: cannot access 'dirl/test': No such file or directory
[guest@localhost ~]$ chmod 000 dirl
[guest@localhost ~]$
```

Рис. 3.5: Команды для нашего dirl

6. Заполняем таблицу, выполняя действия от имени владельца директорий

```
[guest@localhost ~]$ mv dirl/test dirl/test10
mv: failed to access 'dirl/test10': Permission denied
[guest@localhost ~]$ chmod 100 dir/test
chmod: cannot access 'dir/test': No such file or directory
[guest@localhost ~]$ chmod 700 dirl
[guest@localhost ~]$ chmod 100 dirl/test
chmod: cannot access 'dirl/test': No such file or directory
[guest@localhost ~]$ chmod 000 dirl
[guest@localhost ~]$ chmod 000 dirl
[guest@localhost ~]$ rmdir dirl/b
rmdir: failed to remove 'dirl/b': Permission denied
[guest@localhost ~]$ chmod 100 dirl
[guest@localhost ~]$ rmdir dirl/b
```

Рис. 3.6: Команды для нашего dirl

### 3.1 Заполнение таблицы 2.1

Права ди- ректо- рии	Права файла	Со- зда- ние файла	Уда- ление файла	За- пись в файл	Чте- ние файла	Сме- на ди- ректо- рии	Про- смотр фай- лов в ди- ректо- рии	Пере- име- нова- ние файла	Сме- на 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»

## 3.2 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)
Переименова- ние файла	d(300)	(000)
Создание под- директории	d(300)	-
Удаление под- директории	d(300)	-

Таблица 2.2 “Минимальные права для совершения операций”

Пример заполнения таблицы 2.2 (рис. 16)

Проверка возможности создать поддиректорию

## 4 Выводы

Мы в ходе работы получили практические навыки работы в консоли с атрибутами файлов, закрепили теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux