

# **Отчёт по лабораторной работе №2**

**Дисциплина: Основы информационной безопасности**

Мишина Анастасия Алексеевна

# Содержание

1. Цель работы	5
2. Выполнение лабораторной работы	6
3. Выводы	12
Список литературы	13

## Список иллюстраций

2.1. Создание пользователя, определение домашнего каталога . . . .	6
2.2. Команды id и groups . . . . .	7
2.3. Просмотр /etc/passwd . . . . .	7
2.4. Просмотр существующих директорий, расширенных атрибутов поддиректорий . . . . .	8
2.5. Права доступа новой директории dir1 . . . . .	8
2.6. Снятие прав доступа новой директории dir1 . . . . .	9
2.7. Попытки выполнения операций при разных правах доступа . . .	9
2.8. Попытки выполнения операций при разных правах доступа . . .	10

## Список таблиц

2.1. Установленные права и разрешенные действия . . . . .	10
2.2. Минимальные права для совершения операций . . . . .	11

# 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 [1].

## 2. Выполнение лабораторной работы

Переходим в режим суперпользователя и создаем учётную запись пользователя guest: `useradd guest`. Зададим пароль для пользователя guest (используя учётную запись ад-министратора): `passwd guest`. Далее войдем в систему от имени пользователя guest и определим директорию, в которой находимся, командой `pwd`. Директория не оказалась домашней, поэтому переходим в нее сами. Уточняем имя пользователя командой `whoami` - guest (рис. 2.1).

```
[aamishina@aamishina ~]$ su -
Password:
[root@aamishina ~]# useradd guest
[root@aamishina ~]# su guest
[guest@aamishina root]$ su -
Password:
Last login: Wed Feb 28 00:33:57 MSK 2024 on pts/0
[root@aamishina ~]# passwd guest
Changing password for user guest.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@aamishina ~]# su guest
[guest@aamishina root]$ pwd
/root
[guest@aamishina root]$ cd ~
[guest@aamishina ~]$ pwd
/home/guest
[guest@aamishina ~]$ whoami
guest
[guest@aamishina ~]$
```

Рис. 2.1.: Создание пользователя, определение домашнего каталога

Уточним имя пользователя - guest, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid` - 1001, `gid` - 1001, `group`:

guest. Вывод команды groups совпадает с выводом команды id. Полученная информация об имени пользователя с данными совпадает с данными, выводимыми в приглашении командной строки (рис. 2.2).

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

Рис. 2.2.: Команды id и groups

Просмотрим файл /etc/passwd командой cat /etc/passwd. В самом низу видим свою учетную запись, uid - 1001, gid - 1001. Значение совпадают с теми, что были получены в предыдущих пунктах (рис. 2.3).

```
[guest@aamishina ~]$ 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
cockpit-ws:x:987:986:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:986:985:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:985:984:User for flatpak system helper:/sbin/nologin
colord:x:984:983:User for colord:/var/lib/colord:/sbin/nologin
setroubleshoot:x:983:982:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
clevis:x:982:981:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:981:980:/run/gnome-initial-setup:/sbin/nologin
pesign:x:980:979:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:979:978:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:978:977:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/sbin/nologin
aamishina:x:1000:1000:aamishina:/home/aamishina:/bin/bash
guest:x:1001:1001:/home/guest:/bin/bash
[guest@aamishina ~]$
```

Рис. 2.3.: Просмотр /etc/passwd

Определим существующие в системе директории командой ls -l /home/. На ди-

ректорах установлены все права (чтение, запись, выполнение) для владельца. Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: `lsattr /home`. Удалось увидеть лишь расширенные атрибуты своей директории, потому что мы не являемся владельцем остальных (рис. 2.4).

```
[guest@aamishina ~]$ ls -l /home/
total 4
drwx-----, 14 aamishina aamishina 4096 Feb 16 23:11 aamishina
drwx-----, 4 guest guest 92 Feb 28 00:34 guest
[guest@aamishina ~]$
[guest@aamishina ~]$
[guest@aamishina ~]$
[guest@aamishina ~]$ lsattr /home
lsattr: Permission denied while reading flags on /home/aamishina
----- /home/guest
[guest@aamishina ~]$
[guest@aamishina ~]$
```

Рис. 2.4.: Просмотр существующих директорий, расширенных атрибутов поддиректорий

Создаем в домашней директории поддиректорию `dir1` командой `mkdir dir1`. Определим командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1` - `drwxr-xr-x` (рис. 2.5).

```
[guest@aamishina ~]$ ls -l /home/guest/
total 0
drwxr-xr-x, 2 guest guest 6 Feb 28 00:42 dir1
[guest@aamishina ~]$
[guest@aamishina ~]$
[guest@aamishina ~]$
[guest@aamishina ~]$ lsattr /home/guest
----- /home/guest/dir1
```

Рис. 2.5.: Права доступа новой директории `dir1`

Снимаем с директории `dir1` все атрибуты командой: `chmod 000 dir1`. Проверим с помощью команды `ls -l` правильность выполнения (рис. 2.6). Попытаемся создать в директории `dir1` файл `file1` командой `echo "test" > /home/guest/dir1/file1`, но получаем отказ, так как все права были отозваны. Файл не был создан (команда `ls -l /home/guest/dir1` также не выполняется).



```

[guest@aamishina ~]$
[guest@aamishina ~]$ chmod 000 dir1
[guest@aamishina ~]$ ls -l
total 0
d-----. 2 guest guest 6 Feb 28 00:42 dir1
[guest@aamishina ~]$
[guest@aamishina ~]$
[guest@aamishina ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@aamishina ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
[guest@aamishina ~]$

```

Рис. 2.6.: Снятие прав доступа новой директории dir1

Для заполнения таблиц 1 и 2 меняем права доступа на директорию и пытаемся производить операции (рис. 2.7), (рис. 2.8). Если операция разрешена, то заносим знак “+”, иначе - “-”.

```

[guest@aamishina ~]$
[guest@aamishina ~]$ chmod 200 dir1
[guest@aamishina ~]$ ls -l
total 0
d-w-----. 2 guest guest 6 Feb 28 00:42 dir1
[guest@aamishina ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@aamishina ~]$ cd dir1
bash: cd: dir1: Permission denied
[guest@aamishina ~]$ touch /home/guest/dir1/file1.txt
touch: cannot touch '/home/guest/dir1/file1.txt': Permission denied
[guest@aamishina ~]$
[guest@aamishina ~]$
[guest@aamishina ~]$ chmod 300 dir1
[guest@aamishina ~]$ ls -l
total 0
d-wx-----. 2 guest guest 6 Feb 28 00:42 dir1
[guest@aamishina ~]$ touch /home/guest/dir1/file1.txt
[guest@aamishina ~]$ echo "test" > /home/guest/dir1/file1.txt
[guest@aamishina ~]$ cat /home/dir1/file1.txt
cat: /home/dir1/file1.txt: No such file or directory
[guest@aamishina ~]$ cd dir1
[guest@aamishina dir1]$

```

Рис. 2.7.: Попытки выполнения операций при разных правах доступа

```

[guest@aamishina ~]$ chmod 400 dir1
[guest@aamishina ~]$ touch /home/guest/dir1/file2.txt
touch: cannot touch '/home/guest/dir1/file2.txt': Permission denied
[guest@aamishina ~]$ echo "test" > /home/guest/dir1/file2.txt
bash: /home/guest/dir1/file2.txt: Permission denied
[guest@aamishina ~]$ cd dir1
bash: cd: dir1: Permission denied
[guest@aamishina ~]$ chmod 500
chmod: missing operand after '500'
Try 'chmod --help' for more information.
[guest@aamishina ~]$ chmod 500 dir1
[guest@aamishina ~]$ touch /home/guest/dir1/file2.txt
touch: cannot touch '/home/guest/dir1/file2.txt': Permission denied
[guest@aamishina ~]$ echo "test" > /home/guest/dir1/file2.txt
bash: /home/guest/dir1/file2.txt: Permission denied
[guest@aamishina ~]$ cd dir1
[guest@aamishina dir1]$ cd ~
[guest@aamishina ~]$ chmod 600
chmod: missing operand after '600'
Try 'chmod --help' for more information.
[guest@aamishina ~]$ chmod 600 dir1
[guest@aamishina ~]$ touch /home/guest/dir1/file2.txt
touch: cannot touch '/home/guest/dir1/file2.txt': Permission denied
[guest@aamishina ~]$ echo "test" > /home/guest/dir1/file2.txt
bash: /home/guest/dir1/file2.txt: Permission denied
[guest@aamishina ~]$ cd dir1
bash: cd: dir1: Permission denied
[guest@aamishina ~]$ chmod 700 dir1
[guest@aamishina ~]$ touch /home/guest/dir1/file2.txt
[guest@aamishina ~]$ echo "test" > /home/guest/dir1/file2.txt
[guest@aamishina ~]$ cd dir1
[guest@aamishina dir1]$

```

Рис. 2.8.: Попытки выполнения операций при разных правах доступа

Заполним таблицу “Установленные права и разрешенные действия” 2.1.

Таблица 2.1.: Установленные права и разрешенные действия

Права		Смена							
ди-	Прав	Создан	Удалени	Запис	Чтени	рек-	Просмотр	Смена	
рек-	фай-	фай-	фай-	в	фай-	рек-	файлов и	атри-	
то-	фай-	фай-	фай-	файл	ла	то-	директо-	Переимен	буков
рии	ла	ла	ла	файл	ла	рии	рии	файла	файла
000	000	-	-	-	-	-	-	-	-
100	100	-	-	-	-	+	-	-	+
200	200	-	-	-	-	-	-	-	-
300	300	+	+	+	-	+	-	+	+
400	400	-	-	-	-	-	+	-	-

Права							Смена		
ди- рек- то- рии	Права фай- ла	Создание фай- ла	Удаление фай- ла	Запись в файл	Чтение фай- ла	ди- рек- то- рии	Просмотр файлов и директо- рии	Переименование файла	Смена атри- бутов файла
500	500	-	-	-	+	+	+	-	+
600	600	-	-	-	-	-	+	-	-
700	700	+	+	+	+	+	+	+	+

Заполним таблицу “Минимальные права для совершения операций” 2.2.

Таблица 2.2.: Минимальные права для совершения операций

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	300	200
Удаление файла	300	200
Чтение файла	500	400
Запись в файл	300	200
Переименование файла	300	200
Создание поддиректории	300	300
Удаление поддиректории	300	300

### **3. Выводы**

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

## Список литературы

1. Кулябов Д.С., Королькова А.В., Геворкян М.Н. Информационная безопасность компьютерных сетей. Лабораторные работы, учебное пособие. Москва: РУДН, 2015. 64 с.