

Отчёта по лабораторной работе № 2

Информационная безопасность

Адебайо Ридвануллахи Айофе

Содержание

0.1	Цель работы	4
0.2	Теорическое введение	4
0.3	Выполнение лабораторной работы	5
0.4	Выводы	14
0.5	Список литературы	14

Список иллюстраций

1	Создание учётной записи пользователя	6
2	Вход в систему	6
3	Проверка Имя пользователя	7
4	Проверка Имя пользователя и его группы	7
5	Сравнение Имя пользователя	8
6	Просмотр файла /etc/passwd	8
7	Просмотр списка директорий	9
8	Просмотр расширенных атрибутов	9
9	Доступные атрибуты директории	10
10	Модификация прав	11
11	Права доступа к файлу	11
12	Заполнение таблицы(1)	12
13	Заполнение таблицы(2)	13
14	Заполнение таблицы(3)	13

Список таблиц

1	Установление права и разрешённых действий	12
2	Минимально необходимые права для выполнения операций внутри директории	14

0.1 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.

0.2 Теорическое 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

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

0.3 Выполнение лабораторной работы

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

```
[raadebayjo@raadebayjo ~]$ su
Password:
[root@raadebayjo raadebayjo]# useradd guest
[root@raadebayjo raadebayjo]# passwd guest
Changing password for user guest.
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
[root@raadebayjo raadebayjo]# passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@raadebayjo raadebayjo]#
```

Рис. 1: Создание учётной записи пользователя

3. Войдите в систему от имени пользователя guest.

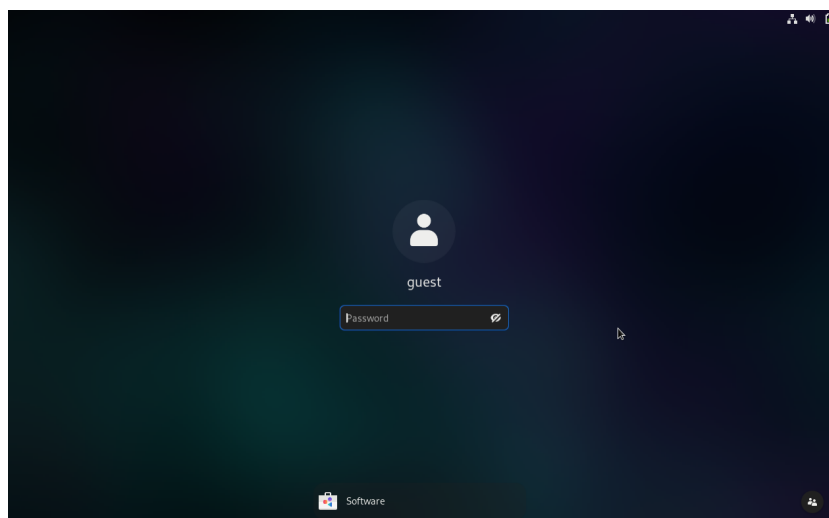


Рис. 2: Вход в систему

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.(см. рис. 3)

5. Уточните имя вашего пользователя командой `whoami`. (см. рис. 3)

```
[guest@raadebayjo ~]$ pwd
/home/guest
[guest@raadebayjo ~]$ whoami
guest
[guest@raadebayjo ~]$
```

Рис. 3: Проверка Имя пользователя

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

Рис. 4: Проверка Имя пользователя и его группы

7. Сравните полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки. **значения совпадают**

```

libstoragegmt:x:992:992:daemon account for libstoragegmt:/:usr/sbin/nologin
systemd-oom:x:991:991:systemd Userspace OOM Killer:/:usr/sbin/nologin
geoclue:x:990:990:User for geoclue:/var/lib/geoclue:/sbin/nologin
tss:x:59:59:Account used for TPM access:/:sbin/nologin
cockpit-ws:x:989:989:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:988:988:User for cockpit-ws instances:/nonexisting:/sbin/nologin
colord:x:987:987:User for colord:/var/lib/colord:/sbin/nologin
sssd:x:986:986:User for sssd:/:sbin/nologin
setroubleshoot:x:985:985:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
pipewire:x:984:984:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
flatpak:x:983:983:User for flatpak system helper:/:sbin/nologin
clevis:x:982:982: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
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:980:979:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:979:978:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/:sbin/nologin
raadebayjo:x:1000:1000:raadebayjo:/home/raadebayjo:/bin/bash
guest:x:1001:1001:/:home/guest:/bin/bash
[guest@raadebayjo ~]$

```

Рис. 5: Сравнение Имя пользователя

8. Просмотрите файл /etc/passwd командой `cat /etc/passwd`

```
cat /etc/passwd | grep guest
```

Найдите в нём свою учётную запись. Определите `uid` пользователя. Определите `gid` пользователя. Сравните найденные значения с полученными в предыдущих пунктах.

uid - 1001

gid - 1001

```

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

```

Рис. 6: Просмотр файла /etc/passwd

9. Определите существующие в системе директории командой `ls -l /home/` (см. рис. 7)

Удалось ли вам получить список поддиректорий директории /home? - **Да**
 Какие права установлены на директориях? - **все права**


```
[guest@raadebayjo ~]$ ls -l /home/
total 8
drwx-----. 14 guest      guest      4096 Sep 15 20:44 guest
drwx-----. 14 raadebayjo raadebayjo 4096 Sep 15 00:27 raadebayjo
[guest@raadebayjo ~]$
```

Рис. 7: Просмотр списка директорий

10. Проверьте, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: `lsattr /home`

Удалось ли вам увидеть расширенные атрибуты директории? - **Да**

Удалось ли вам увидеть расширенные атрибуты директорий других пользователей? - **Нет, отказ в доступ**

```
[guest@raadebayjo ~]$ lsattr /home
lsattr: Permission denied while reading flags on /home/raadebayjo
----- /home/guest
[guest@raadebayjo ~]$
```

Рис. 8: Просмотр расширенных атрибутов

11. Создайте в домашней директории поддиректорию `dir1` командой `mkdir dir1` (см. рис. 9)

Определите командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`.

```

[guest@raadebayjo ~]$ mkdir dir1
[guest@raadebayjo ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 15 20:44 Desktop
drwxr-xr-x. 2 guest guest 6 Sep 15 21:08 dir1
drwxr-xr-x. 2 guest guest 6 Sep 15 20:44 Documents
drwxr-xr-x. 2 guest guest 6 Sep 15 20:44 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 15 20:44 Music
drwxr-xr-x. 2 guest guest 6 Sep 15 20:44 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 15 20:44 Public
drwxr-xr-x. 2 guest guest 6 Sep 15 20:44 Templates
drwxr-xr-x. 2 guest guest 6 Sep 15 20:44 Videos
[guest@raadebayjo ~]$ ls -l /dir1/
ls: cannot access '/dir1/': No such file or directory
[guest@raadebayjo ~]$ ls -l /dir1
ls: cannot access '/dir1': No such file or directory
[guest@raadebayjo ~]$ ls -l dir1
total 0
[guest@raadebayjo ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
[guest@raadebayjo ~]$

```

Рис. 9: Доступные атрибуты директории

12. Снимите с директории dir1 все атрибуты командой

```
chmod 000 dir1
```

и проверьте с её помощью правильность выполнения команды `ls -l` (см. рис.

10)

```
[guest@raadebayjo ~]$ chmod 000 dir1
[guest@raadebayjo ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 15 20:44 Desktop
d------. 2 guest guest 6 Sep 15 21:08 dir1
drwxr-xr-x. 2 guest guest 6 Sep 15 20:44 Documents
drwxr-xr-x. 2 guest guest 6 Sep 15 20:44 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 15 20:44 Music
drwxr-xr-x. 2 guest guest 6 Sep 15 20:44 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 15 20:44 Public
drwxr-xr-x. 2 guest guest 6 Sep 15 20:44 Templates
drwxr-xr-x. 2 guest guest 6 Sep 15 20:44 Videos
[guest@raadebayjo ~]$
```

Рис. 10: Модификация прав

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? - **Невозможно создать файл, потому что нет прав**

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. - **Нет**

```
[guest@raadebayjo ~]$ touch file1.txt
[guest@raadebayjo ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@raadebayjo ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
[guest@raadebayjo ~]$
```

Рис. 11: Права доступа к файлу

Таблица 1: Установление права и разрешённых действий

Права директории	000	100	200	300	400	500	600	700
Права файла	000	100	200	300	400	500	600	700
Создание файла	-	-	-	+	-	-	-	+
Удаление файла	-	-	-	+	-	-	-	+
Запись в файл	-	+	-	+	-	+	-	+
Чтение файла	-	+	-	+	-	+	-	+
Смена директории	-	-	-	+	-	+	-	+
Просмотр файлов в директории	-	-	-	-	+	+	+	+
Переименование файла	-	-	-	+	-	-	-	+
Смена атрибутов файла	-	-	-	+	-	-	-	+

```

[guest@raadebayjo ~]$ chmod 100 dir1
[guest@raadebayjo ~]$ > dir1/file1
bash: dir1/file1: Permission denied
[guest@raadebayjo ~]$ chmod 200 dir1
[guest@raadebayjo ~]$ > dir1/file1
bash: dir1/file1: Permission denied
[guest@raadebayjo ~]$ chmod 300 dir1
[guest@raadebayjo ~]$ > dir1/file1
[guest@raadebayjo ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 15 20:44 Desktop
d-wx----- 2 guest guest 36 Sep 15 21:52 dir1
drwxr-xr-x. 2 guest guest 6 Sep 15 20:44 Documents
drwxr-xr-x. 2 guest guest 6 Sep 15 20:44 Downloads
-rw-r--r-- 1 guest guest 0 Sep 15 21:22 file1.txt
drwxr-xr-x. 2 guest guest 6 Sep 15 20:44 Music
drwxr-xr-x. 2 guest guest 6 Sep 15 20:44 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 15 20:44 Public
drwxr-xr-x. 2 guest guest 6 Sep 15 20:44 Templates
drwxr-xr-x. 2 guest guest 6 Sep 15 20:44 Videos
[guest@raadebayjo ~]$ chmod 400 dir1
[guest@raadebayjo ~]$ > dir1/file1
bash: dir1/file1: Permission denied
[guest@raadebayjo ~]$ chmod 500 dir1
[guest@raadebayjo ~]$ > dir1/file1
[guest@raadebayjo ~]$ cd dir1
[guest@raadebayjo dir1]$ ls
file1 file1.txt
[guest@raadebayjo dir1]$ rm file1
rm: cannot remove 'file1': Permission denied
[guest@raadebayjo dir1]$ echo "text" > file1
[guest@raadebayjo dir1]$ cat file1
text
[guest@raadebayjo dir1]$ mv file1 file2
mv: cannot move 'file1' to 'file2': Permission denied
[guest@raadebayjo dir1]$

```

Рис. 12: Заполнение таблицы(1)

```
guest@raadebayjo:~  
ls: cannot open directory 'dir1': Permission denied  
[guest@raadebayjo ~]$ > dir1/file3  
[guest@raadebayjo ~]$ rm dir1/file3  
[guest@raadebayjo ~]$ ls dir1  
ls: cannot open directory 'dir1': Permission denied  
[guest@raadebayjo ~]$ chmod 200 dir1  
[guest@raadebayjo ~]$ chmod 700 dir1  
[guest@raadebayjo ~]$ ls  
Desktop dir1 Documents Downloads file1.txt file2 Music Pictures Public Templates Videos  
[guest@raadebayjo ~]$ ls dir1  
file1 file1.txt  
[guest@raadebayjo ~]$ rm file1.txt  
[guest@raadebayjo ~]$ ls  
Desktop dir1 Documents Downloads file2 Music Pictures Public Templates Videos  
[guest@raadebayjo ~]$ ls dir1  
file1 file1.txt  
[guest@raadebayjo ~]$ rm file1  
rm: cannot remove 'file1': No such file or directory  
[guest@raadebayjo ~]$ rm dir1/file1.txt  
[guest@raadebayjo ~]$ ls dir1  
file1  
[guest@raadebayjo ~]$ chmod 200 dir1  
[guest@raadebayjo ~]$ rm dir1/file1  
rm: cannot remove 'dir1/file1': Permission denied  
[guest@raadebayjo ~]$ chmod 400 dir1  
[guest@raadebayjo ~]$ rm dir1/file1  
rm: cannot remove 'dir1/file1': Permission denied  
[guest@raadebayjo ~]$ chmod 500 dir1  
[guest@raadebayjo ~]$ rm dir1/file1  
rm: cannot remove 'dir1/file1': Permission denied  
[guest@raadebayjo ~]$ > dir1/file2  
bash: dir1/file2: Permission denied  
[guest@raadebayjo ~]$ chmod 600 dir1  
[guest@raadebayjo ~]$ rm dir1/file1  
rm: cannot remove 'dir1/file1': Permission denied  
[guest@raadebayjo ~]$
```

Рис. 13: Заполнение таблицы(2)

```
guest@raadebayjo:~  
[guest@raadebayjo ~]$ chmod 400 dir1  
[guest@raadebayjo ~]$ cd dir1  
bash: cd: dir1: Permission denied  
[guest@raadebayjo ~]$ chmod 500 dir1  
[guest@raadebayjo ~]$ cd dir1  
[guest@raadebayjo dir1]$ cd ..  
[guest@raadebayjo ~]$ chmod 300 dir1  
[guest@raadebayjo ~]$ ls dir1  
ls: cannot open directory 'dir1': Permission denied  
[guest@raadebayjo ~]$ chmod 700 dir1  
[guest@raadebayjo ~]$ ls dir1  
file1  
[guest@raadebayjo ~]$ chmod 100 dir1  
[guest@raadebayjo ~]$ mv file1 file2  
mv: cannot stat 'file1': No such file or directory  
[guest@raadebayjo ~]$ mv dir1/file1 dir1/file2  
mv: cannot move 'dir1/file1' to 'dir1/file2': Permission denied  
[guest@raadebayjo ~]$ chmod 200 dir1  
[guest@raadebayjo ~]$ mv dir1/file1 dir1/file2  
mv: failed to access 'dir1/file2': Permission denied  
[guest@raadebayjo ~]$ chmod 300 dir1  
[guest@raadebayjo ~]$ mv dir1/file1 dir1/file2  
[guest@raadebayjo ~]$ ls dir1  
ls: cannot open directory 'dir1': Permission denied  
[guest@raadebayjo ~]$ chmod 400 dir1  
[guest@raadebayjo ~]$ mv dir1/file2 dir1/file1  
mv: failed to access 'dir1/file1': Permission denied  
[guest@raadebayjo ~]$ chmod 500 dir1  
[guest@raadebayjo ~]$ mv dir1/file2 dir1/file1  
mv: cannot move 'dir1/file2' to 'dir1/file1': Permission denied  
[guest@raadebayjo ~]$ chmod 600 dir1  
[guest@raadebayjo ~]$ mv dir1/file2 dir1/file1  
mv: failed to access 'dir1/file1': Permission denied  
[guest@raadebayjo ~]$ chmod 700 dir1  
[guest@raadebayjo ~]$ mv dir1/file2 dir1/file1  
[guest@raadebayjo ~]$
```

Рис. 14: Заполнение таблицы(3)

Таблица 2: Минимально необходимые права для выполнения операций внутри директории

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)	400
Запись в файл	d -x(100)	200
Переименование файла	d -wx(300)	000
Создание поддиректории	d -wx(300)	000
Удаление поддиректории	d -wx(300)	000

0.4 Выводы

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

0.5 Список литературы

1. Кулябов Д. С. *Лабораторная работа №2*: 002-lab_discret_attr.pdf*
2. Изменение атрибутов файлов в Linux [Электронный ресурс]. 2023.URL: <https://linux-notes.org/izmenenie-atributov-flagov-na-fajlah-v-unix-linux/> (дата обращения: 14.09.2023)