

Отчёт по лабораторной работе №2

Информационная безопасность

Дискреционное разграничение прав в Linux.

Выполнил: Мальков Роман Сергеевич,
НФИбд-02-21, 1032217048

Содержание

Цель работы	4
Выполнение	5
Заключение	13

Список иллюстраций

1	Создаем учетную запись	5
2	Задаем новый пароль	5
3	Переход в новую учетную запись	6
4	Команды pwd,whoami,id,groups	6
5	passwd	7
6	passwd с grep	7
7	ls -l /home/	7
8	lsattr /home	7
9	mkdir dir1	8
10	ls -l grep dir1	8
11	lsattr grep dir1	8
12	chmod 000 dir1	8
13	echo "test" > /home/guest/dir1/file1	8
14	Проверяем созданся ли файл	8

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.

Выполнение

Создаем новую учетную запись guest

```
[rsmaljkov@localhost ~]$ sudo useradd guest  
  
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.
```

Рис. 1: Создаем учетную запись

Задаем новый пароль для созданной учетной записи

```
[rsmaljkov@localhost ~]$ sudo passwd guest  
Changing password for user guest.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.
```

Рис. 2: Задаем новый пароль

Переходим в новую учетную запись.

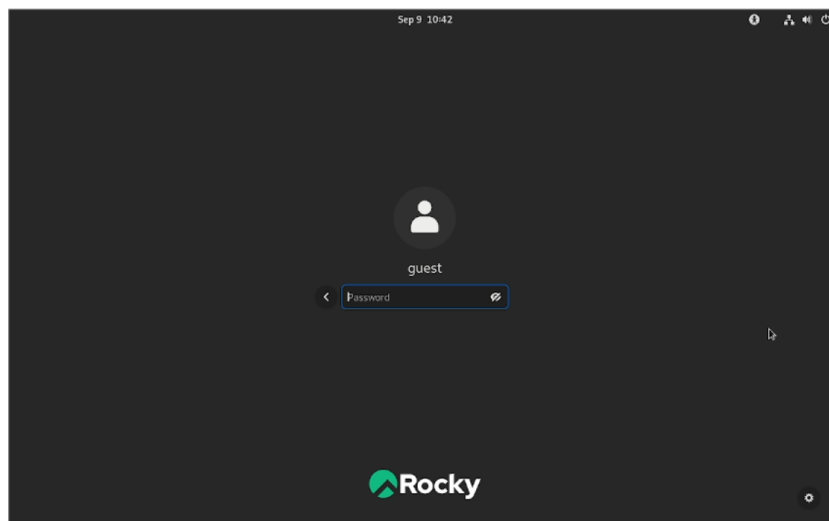


Рис. 3: Переход в новую учетную запись

Вводим команду `pwd`, смотрим находимся ли в домашней директории. Вводим команду `whoami`, чтобы узнать имя текущего пользователя. Вводим команду `id` и команду `groups`, сравниваем. На скриншоте видно, что команды показывают группу `guest`.

```
[guest@localhost ~]$ pwd
/home/guest
[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 ~]$ groups
guest
```

Рис. 4: Команды `pwd`, `whoami`, `id`, `groups`

Просматриваем файл `/etc/passwd`.

```
[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:997:994:PipeWire System Daemon:/run/pipewire:/usr/sbin/nologin
```

Рис. 5: passwd

Применяем команду с фильтром, чтобы получить информацию о пользователе.

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

Рис. 6: passwd с grep

Определяем директории в home. Как мы видим установлены права для пользователей, на чтение запись и исполнение.

```
[guest@localhost ~]$ ls -l /home/
total 8
drwx-----, 14 guest      guest      4096 Sep  9 10:42 guest
drwx-----, 14 rsmaljkov  rsmaljkov 4096 Sep  2 13:58 rsmaljkov
```

Рис. 7: ls -l /home/

Смотрим атрибуты, просмотр атрибутов для основного пользователя не доступен, атрибуты же для директории guest не установлены.

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

Рис. 8: lsattr /home

Создаем поддиректорию dir1 в домашней директории.

```
[guest@localhost ~]$ mkdir dir1
[guest@localhost ~]$ ls
Desktop  dir1  Documents  Downloads  Music  Pictures  Public  Templates  Videos
```

Рис. 9: mkdir dir1

Смотрим права и атрибуты для dir1. Атрибуты не установлены, права доступа на чтение запись и выполнение.

```
[guest@localhost ~]$ ls -l | grep dir1
drwxr-xr-x. 2 guest guest 6 Sep  9 10:58 dir1
```

Рис. 10: ls -l |grep dir1

```
[guest@localhost ~]$ lsattr | grep dir1
----- ./dir1
```

Рис. 11: lsattr |grep dir1

Воспользуемся командой chmod 000 dir1. Проверим правильность выполнения командой ls -l |grep dir1.

```
[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$ lsattr | grep dir1
lsattr: Permission denied while reading flags on ./dir1
[guest@localhost ~]$ ls -l | grep dir1
d-----, 2 guest guest 6 Sep  9 10:58 dir1
```

Рис. 12: chmod 000 dir1

Попробуем создать файл в директории dir1. Проверяем наличие файла.

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

Рис. 13: echo "test" > /home/guest/dir1/file1

```
[guest@localhost ~]$ chmod -u+r dir1
[guest@localhost ~]$ ls -l /home/guest/dir1
total 0
```

Рис. 14: Проверяем созданся ли файл

Заполняем таблицу 2.1

Права дирек- тории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена дирек- тории	Просмотр фай- лов в дирек- тории	Переиме- вание 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»

Заполняем таблицу 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	d(300)	(000)
поддиректории		
Удаление	d(300)	(000)
поддиректории		

Таблица 2.2 “Минимальные права для совершения операций”

Заключение

Были получены навыки работы в консоли с атрибутами файлов, были закреплены теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.