Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Карпова Есения Алексеевна

Содержание

1 Цель работы

Получение практических навыков работы в консоли с атрибутами фай- лов, закрепление теоретических основ дискреционного разграничения до- ступа в современных системах с открытым кодом на базе ОС Linux

2 Задания

1. Ознакомление с основными командами терминала
2. Заполнение таблицы «Установленные права и разрешённые действия»
3. Заполнение таблицы «Минимальные права для совершения операций»

3 Теоретическое введение

Права доступа в Linux определяют, кто и каким образом может взаимодействовать с файлами и директориями в системе. Каждый файл и директория имеют ассоциированные с ними права, которые указывают на возможность чтения, записи и выполнения. Эти права назначаются для трех категорий пользователей: владельца файла, группы пользователей и всех остальных пользователей.

Система управления правами доступа в Linux основана на трех основных типах разрешений: “r” (чтение), “w” (запись) и “x” (выполнение). Владельцы файлов могут изменять права доступа с помощью команд, таких как chmod, а также настраивать владельца и группу через команды chown и chgrp. Это позволяет администраторам систем эффективно управлять безопасностью и конфиденциальностью данных.

Правильная настройка прав доступа критически важна для защиты систем от несанкционированного доступа и обеспечения безопасности пользовательских данных. Неправильно установленное разрешение может привести к компрометации системы, поэтому важно по умолчанию применять наименее привилегированные разрешения к файлам и директориям.

4 Выполнение лабораторной работы

4.1 Ознакомление с основными командами терминала

1. Создаю учетную запись guest и меняю пароль (рис. 1).

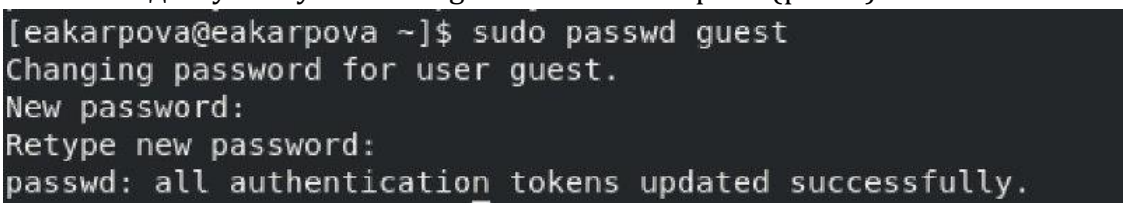

Рис. 1: Создание учетной записи guest

2. Вхожу в систему от имени пользователя guest (рис. 2).

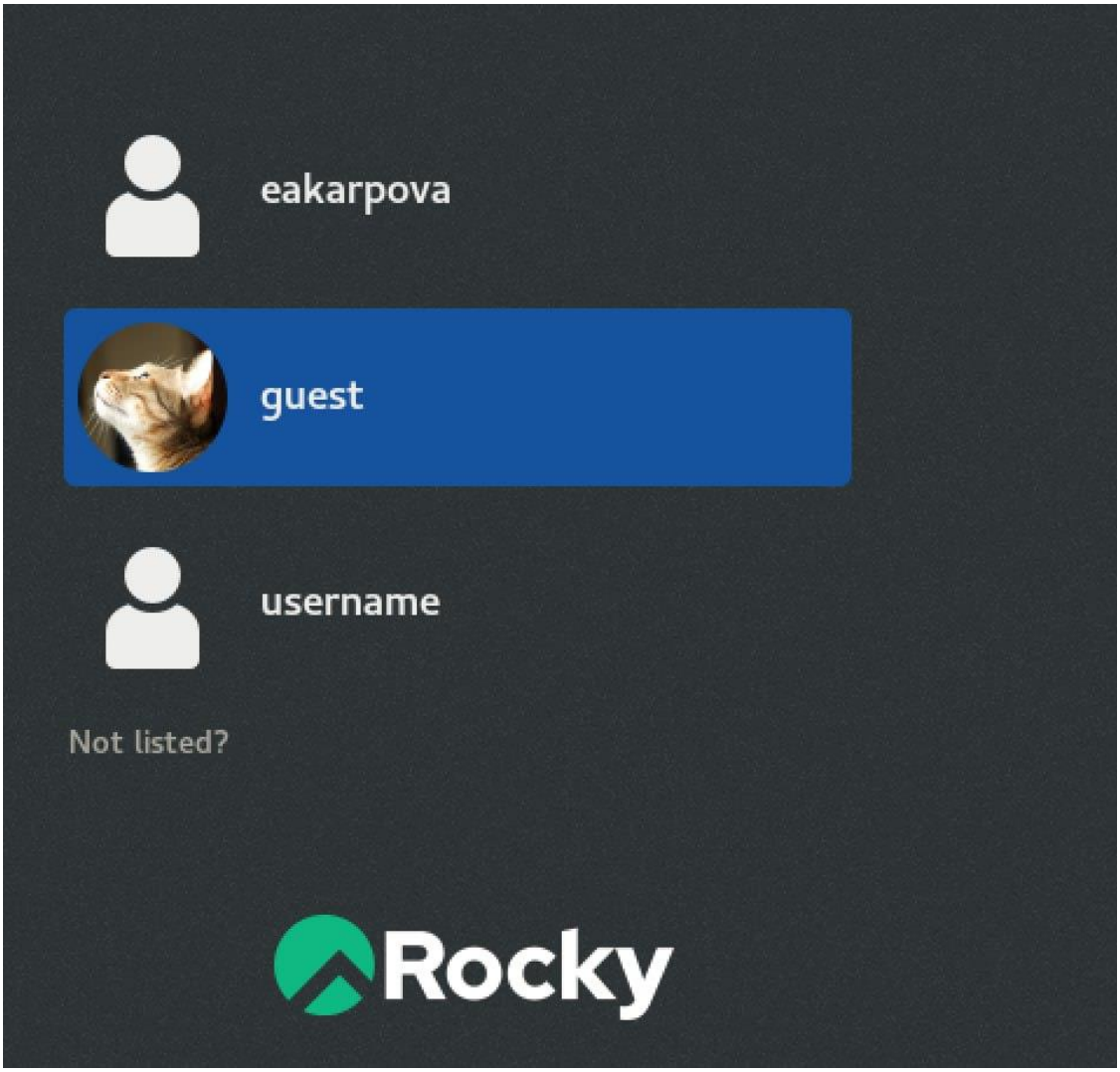

Рис. 2: Вход в систему от имени пользователя guest

3. Определяю директорию, в которой нахожусь, командой pwd. Она является домашней директорией. (рис. 3).

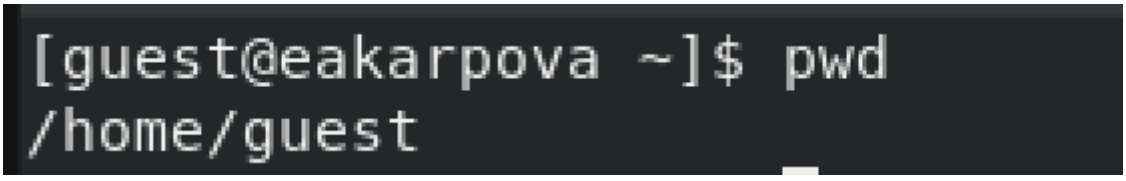

Рис. 3: Команда pwd

4. Уточняю имя пользователя командой whoami (рис. 4).

```
[guest@eakarpova ~]$ id
uid=1002(guest) gid=1002(guest) groups=1002(guest),10(wheel) context=unconfined_
u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@eakarpova ~]$ groups
guest wheel
```

Рис. 4: Команда whoami

5. Уточняю имя пользователя, его группу, а также группы, куда входит пользователь, командой id. Сравниваю вывод id с выводом команды groups (рис. 5).

```
[guest@eakarpova ~]$ 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
dbus:x:81:81:System message bus:/:/sbin/nologin
```

Рис. 5: Команды id и groups

6. Командой cat /etc/passwd просматриваю файл /etc/passwd (рис. 6).

Так как вывод команды не умещается на одном экране монитора программу grep в качестве фильтра для вывода только строк, содержащих определённые буквенные сочетания: cat /etc/passwd | grep guest

Определяю uid и gid пользователя. Они совпадают со значениями, полученные в предыдущих пунктах (1002)

```
[guest@eakarpova ~]$ cat /etc/passwd | grep guest
guest:x:1002:1002::/home/guest:/bin/bash
```

Рис. 6: Нахождение uid и gid

7. Определяю существующие в системе директории командой ls -l /home/ Мне удалось получить список поддиректорий директории /home. На них установлены права drwx—— (700), то есть только я (пользователь) могу писать и читать указанные файлы (рис. 7).

```
[guest@eakarpova ~]$ ls -l /home/
total 8
drwx------. 15 eakarpova eakarpova 4096 Feb 15 09:08 eakarpova
drwx------. 15 guest     guest     4096 Feb 18 19:07 guest
drwx------.  3 username  username    78 Feb 14 23:16 username
```

Рис. 7: Команда ls

8. Проверяю, какие расширенные атрибуты установлены на поддиректо- риях, находящихся в директории /home, командой: lsattr /home Мне не удалось увидеть расширенные атрибуты директории как своего, так и других пользователей (рис. 8).

```
[guest@eakarpova ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/eakarpova
lsattr: Permission denied While reading flags on /home/username
-------------------- /home/guest
```

Рис. 8: Проверка расширенных атрибутов

9. Создаю в домашней директории поддиректорию dir1 командой mkdir dir1 Определяю, какие права доступа и расширенные атрибуты были выставлены на директорию dir1, командами ls -l и lsattr (рис. 9).

```
[guest@eakarpova ~]$ mkdir dir1
[guest@eakarpova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest  6 Feb 18 19:07 Desktop
drwxrwxr-x. 2 guest guest  6 Feb 18 19:17 dir1
drwxr-xr-x. 2 guest guest  6 Feb 18 19:07 Documents
drwxr-xr-x. 2 guest guest  6 Feb 18 19:07 Downloads
drwxr-xr-x. 2 guest guest  6 Feb 18 19:07 Music
drwxr-xr-x. 2 guest guest 53 Feb 18 19:11 Pictures
drwxr-xr-x. 2 guest guest  6 Feb 18 19:07 Public
drwxr-xr-x. 2 guest guest  6 Feb 18 19:07 Templates
drwxr-xr-x. 2 guest guest  6 Feb 18 19:07 Videos
[guest@eakarpova ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/eakarpova
lsattr: Permission denied While reading flags on /home/username
-------------------- /home/guest
```

Рис. 9: Определение прав доступа

10. Снимаю с директории dir1 все атрибуты командой chmod 000 dir1 и проверяю её правильность, выполненяя команду ls -l (рис. 10).

```
[guest@eakarpova ~]$ chmod 000 dir1
[guest@eakarpova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest  6 Feb 18 19:07 Desktop
d---------. 2 guest guest  6 Feb 18 19:17 dir1
drwxr-xr-x. 2 guest guest  6 Feb 18 19:07 Documents
drwxr-xr-x. 2 guest guest  6 Feb 18 19:07 Downloads
drwxr-xr-x. 2 guest guest  6 Feb 18 19:07 Music
drwxr-xr-x. 2 guest guest 53 Feb 18 19:11 Pictures
drwxr-xr-x. 2 guest guest  6 Feb 18 19:07 Public
drwxr-xr-x. 2 guest guest  6 Feb 18 19:07 Templates
drwxr-xr-x. 2 guest guest  6 Feb 18 19:07 Videos
```

Рис. 10: Команда chmod

11. Пытаюсь создать в директории dir1 файл file1 командой echo “test” > /home/guest/dir1/file1 Я получаю сообщение об ошибке, так как в предыдущем пункте поменяла права пользователя для данной директории. Проверяю, как сообщение об ошибке отразилось на создании файла, с помощью команды ls -l /home/guest/dir1 (рис. 11).

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

Рис. 11: Создание файла

4.2 Заполнение таблицы «Установленные права и разрешённые действия»

Заполняю таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории, определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, я заношу в таблицу знак «+», если не разрешена, знак «-» (рис. 12).

```
[guest@eakarpova ~]$ chmod 100 dir1
[guest@eakarpova ~]$ chmod  100 ~/dir1 test
[guest@eakarpova ~]$ echo 'test' > dir1/test
bash: dir1/test: Permission denied
[guest@eakarpova ~]$ rm ~/dir1/test
rm: remove write-protected regular empty file '/home/guest/dir1/test'? n
[guest@eakarpova ~]$ rm ~/dir1/test
rm: remove write-protected regular empty file '/home/guest/dir1/test'? y
rm: cannot remove '/home/guest/dir1/test': Permission denied
[guest@eakarpova ~]$ cat  ~/dir1/test
cat: /home/guest/dir1/test: Permission denied
[guest@eakarpova ~]$ mv  ~/dir1/test ~
mv: replace '/home/guest/test', overriding mode 0100 (--x------)? y
mv: cannot move '/home/guest/dir1/test' to '/home/guest/test': Permission denied
[guest@eakarpova ~]$ ls dir1
ls: cannot open directory 'dir1': Permission denied
[guest@eakarpova ~]$ cd  ~/dir1/test ~
bash: cd: too many arguments
[guest@eakarpova ~]$ cd  ~/dir1/test
bash: cd: /home/guest/dir1/test: Not a directory
[guest@eakarpova ~]$ cd  ~/dir1
```

Рис. 12: Заполнение таблицы

Таблица 2.1 «Установленные права и разрешённые действия»

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов 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)	+	+	+	+	+	+	+	+

4.3 Заполнение таблицы «Минимальные права для совершения операций»

Таблица 2.2 “Минимальные права для совершения операций”

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

5 Выводы

В ходе 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