Отчет по лабораторной работе №2

Дискреционные разграничения прав в Linux. Основные атрибуты

Евсеева Дарья Олеговна

17 сентября, 2022

Содержание

Список иллюстраций

Цель работы

Целью данной работы является 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.

Задание

1. Создать гостевого пользователя.
2. Провести работу с директориями от имени гостевого пользователя.
3. Заполнить таблицы прав доступа.

Теоретическое введение

Дискреционное разграничение доступа — подход к разграничению доступа, предполагающий назначение владельцев объектов, которые по собственному усмотрению определяют права доступа субъектов (других пользователей) к объектам (файлам), которыми владеют.

Дискреционные механизмы разграничения доступа используются для разграничения прав доступа процессов как обычных пользователей, так и для ограничения прав системных программ (например, служб операционной системы), которые работают от лица псевдопользовательских учетных записей.

Выполнение лабораторной работы

Выполнять работу будем в операционной системе, установленной при выполнении предыдущей лабораторной работы.

1. Создание пользователя

Для начала, используя учетную запись администратора, создадим пользователя guest с помощью команды useradd.

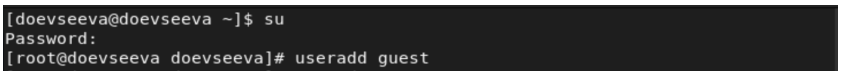

Рис. 1: Создание пользователя guest

Дале установим пароль для созданного пользователя.

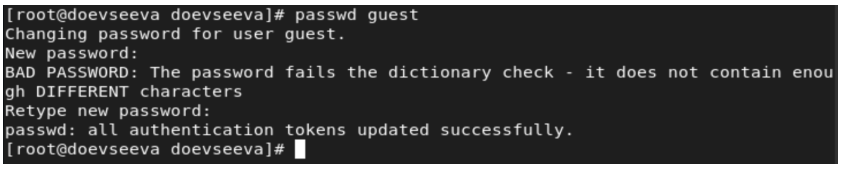

Рис. 2: Установка пароля для пользователя guest

Войдем в систему от имени созданного пользователя guest.

Рис. 3: Вход в систему через пользователя guest

Выполним команду pwd, чтобы определить текущую директорию.

Рис. 4: Определение текущей директории

Мы видим, что директория является домашней директорией для пользователя guest и совпадает с приглашением командной строки.

Выполним команду whoami для уточнения имени пользователя.

Рис. 5: Уточнение имени пользователя

Далее выполним команду id для просмотра информации о пользователе. Также проверим вывод команды groups.

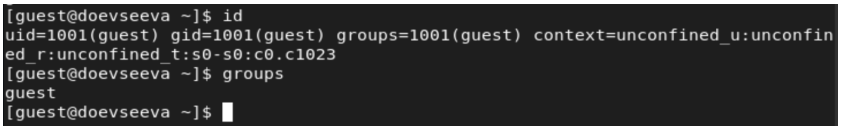

Рис. 6: Просмотр информации о пользователе

Здесь мы видим, что имя пользователя — guest, значение uid равняется 1001(guest), значение gid равняется 1001(guest), также пользователь входит в единственную группу — 1001(guest). Выводы обеих команд соотносятся друг с другом.

Полученные данные также соответствуют данным в приглашении командной строки.

Посмотрим содержимое файла /etc/passwd.

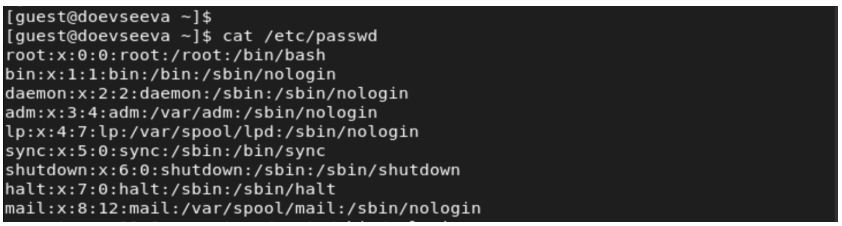

Рис. 7: Просмотр файла /etc/passwd (1)

Рис. 8: Просмотр файла /etc/passwd (2)

Мы видим, что в последней строке вывода содержится информация о текущем пользователе guest. Значение uid равняется 1001 и значение gid равняется 1001, что совпадает с данными , полученными ранее.

2. Работа с директориями

Определим существующие в системе директории.

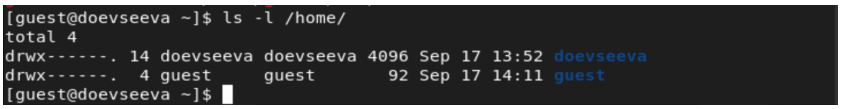

Рис. 9: Просмотр директорий в системе

Нам удалось получить список поддиректорий директории /home, и мы видим, что в системе есть домашние директории пользователей doevseeva и guest. У обеих директорий установлены права на чтение, запись и исполнение для пользователя.

Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home.

Рис. 10: Просмотр расширенных атрибутов

Нам удалось получить только данные о домашней директории текущего пользователя guest, и можно видеть, что установленных расширенных атрибутов нет. Данные о домашней директории пользователя doevseeva не были получены.

Создадим в домашней директории поддиректорию dir1.

Рис. 11: Создание поддиректории dir1

Далее определим, какие права доступа и расширенные атрибуты были выставлены на созданную директорию.

Рис. 12: Проверка прав доступа и расширенных атрибутов dir1

Снимем с созданной директории все атрибуты.

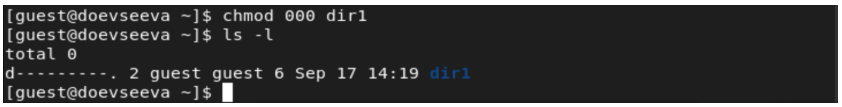

Рис. 13: Снятие атрибутов с директории

Далее попытаемся создать внутри директории файл.

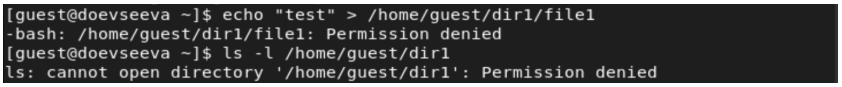

Рис. 14: Проверка возможности создания файла

Как мы видим, в доступе было отказано, так как мы сняли все атрибуты с директории, также из-за этого мы не можем увидеть, действительно ли не создался файл.

Добавим к директории право на чтение и проверим список файлов в ней.

Рис. 15: Проверка наличия файла в директории

Мы видим, что директория действительно пуста.

3. Заполнение таблиц прав доступа.

Заполним таблицу “Установленные права и разрешенные действия”, выполняя действия от имени владельца директории (файлов), определив опытным путем, какие операции разрешены, а какие нет.

Для начала вернем директории все права доступа для пользователя и создадим в ней файл для дальнейшей проверки действий. Затем приступим к заполнению таблицы.

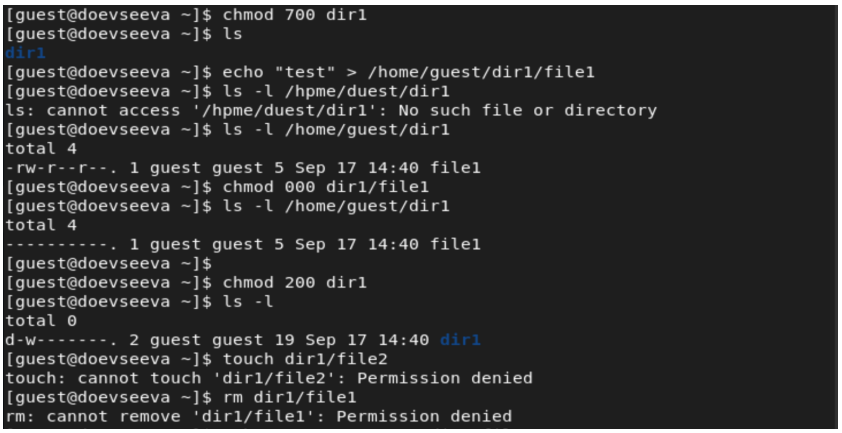

Рис. 16: Создание файла и проверка прав и действий

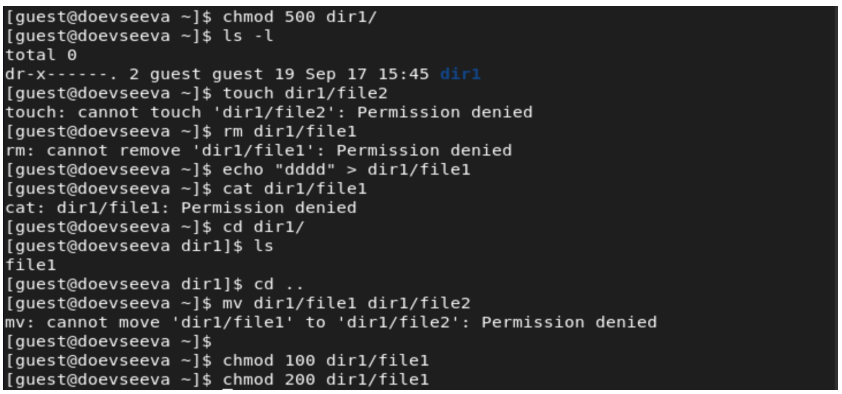

Рис. 17: Проверка прав и действий (1)

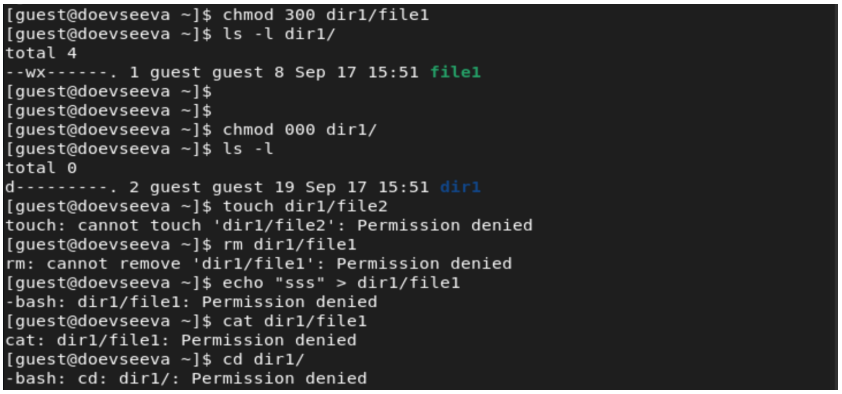

Рис. 18: Проверка прав и действий (2)

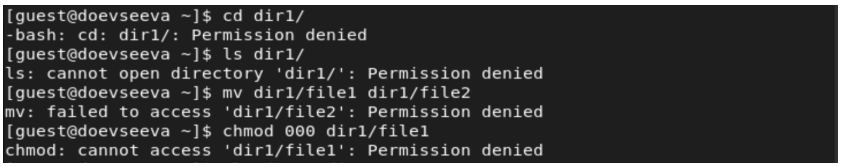

Рис. 19: Проверка прав и действий (3)

```
[guest@doevseeva ~]$ chmod 700 dir1/
[guest@doevseeva ~]$ ls -l
total 0
drwx------. 2 guest guest 19 Sep 17 16:51 dir1
[guest@doevseeva ~]$ touch dir1/file2
[guest@doevseeva ~]$ rm dir1/file2
[guest@doevseeva ~]$ echo "oooool" > dir1/file1
[guest@doevseeva ~]$ cat dir1/file1
oooool
[guest@doevseeva ~]$ cd dir1/
[guest@doevseeva dir1]$ ls
file1
[guest@doevseeva dir1]$ cd ..
[guest@doevseeva ~]$ mv dir1/file1 dir1/file2
[guest@doevseeva ~]$ mv dir1/file2 dir1/file1
[guest@doevseeva ~]$ chmod 000 dir1/file1
[guest@doevseeva ~]$
```

Рис. 20: Проверка прав и действий (4)

Итак, закончим заполнение таблицы “Установленные права и действия”.

Установленные права и разрешенные 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--x------ (100)	- --------- (000)	-	-	-	-	+	-	-	+
d-w------- (200)	- --------- (000)	-	-	-	-	-	-	-	-
d-wx------ (300)	- --------- (000)	+	+	-	-	+	-	+	+
dr-------- (400)	- --------- (000)	-	-	-	-	-	+	-	-
d-x------ (500)	- --------- (000)	+	-	-	-	+	+	-	+
drw------- (600)	- --------- (000)	-	-	-	-	-	+	-	-
drwx------ (700)	- --------- (000)	+	+	-	-	+	+	+	+
d--------- (000)	- --x------ (100)	-	-	-	-	-	-	-	-
d--x------ (100)	- --x------ (100)	-	-	-	-	+	-	-	+
d-w------- (200)	- --x------ (100)	-	-	-	-	-	-	-	-
d-wx------ (300)	- --x------ (100)	+	+	-	-	+	-	+	+
dr-------- (400)	- --x------ (100)	-	-	-	-	-	+	-	-
d-x------ (500)	- --x------ (100)	-	-	-	-	+	+	-	+
drw------- (600)	- --x------ (100)	-	-	-	-	-	+	-	-
drwx------ (700)	- --x------ (100)	+	+	-	-	+	+	+	+

Рис. 21: Установленные права и действия (1)

d--------- (000)	- -w------- (200)	-	-	-	-	-	-	-	-
d--x------ (100)	- -w------- (200)	-	-	+	-	+	-	-	+
d-w------- (200)	- -w------- (200)	-	-	-	-	-	-	-	-
d-wx------ (300)	- -w------- (200)	+	+	+	+	+	-	+	+
dr-------- (400)	- -w------- (200)	-	-	-	-	-	+	-	-
d-x------ (500)	- -w------- (200)	-	-	+	-	+	+	-	+
drw------- (600)	- -w------- (200)	-	-	-	-	-	+	-	-
drwx------ (700)	- -w------- (200)	+	+	+	-	+	+	+	+
d--------- (000)	- -wx------ (300)	-	-	-	-	-	-	-	-
d--x------ (100)	- -wx------ (300)	-	-	+	-	+	-	-	+
d-w------- (200)	- -wx------ (300)	-	-	-	-	-	-	-	-
d-wx------ (300)	- -wx------ (300)	+	+	+	-	+	-	+	+
dr-------- (400)	- -wx------ (300)	-	-	-	-	-	+	-	-
d-x------ (500)	- -wx------ (300)	-	-	+	-	+	+	-	+
drw------- (600)	- -wx------ (300)	-	-	-	-	-	+	-	-
drwx------ (700)	- -wx------ (300)	+	+	+	-	+	+	+	+
d--------- (000)	- r-------- (400)	-	-	-	-	-	-	-	-
d--x------ (100)	- r-------- (400)	-	-	-	+	+	-	-	+

Рис. 22: Установленные права и действия (2)

d-w------- (200)	- r-------- (400)	-	-	-	-	-	-	-	-
d-wx------ (300)	- r-------- (400)	+	+	-	+	+	-	+	+
dr-------- (400)	- r-------- (400)	-	-	-	-	-	+	-	-
d-x------ (500)	- r-------- (400)	-	-	-	+	+	+	-	+
drw------- (600)	- r-------- (400)	-	-	-	-	-	+	-	-
drwx------ (700)	- r-------- (400)	+	+	-	+	+	+	+	+
d--------- (000)	- r-x------ (500)	-	-	-	-	-	-	-	-
d--x------ (100)	- r-x------ (500)	-	-	-	+	+	-	-	+
d-w------- (200)	- r-x------ (500)	-	-	-	-	-	-	-	-
d-wx------ (300)	- r-x------ (500)	+	+	-	+	+	-	+	+
dr-------- (400)	- r-x------ (500)	-	-	-	-	-	+	-	-
d-x------ (500)	- r-x------ (500)	-	-	-	+	+	+	-	+
drw------- (600)	- r-x------ (500)	-	-	-	-	-	+	-	-
drwx------ (700)	- r-x------ (500)	+	+	-	+	+	+	+	+
d--------- (000)	- rw------- (600)	-	-	-	-	-	-	-	-
d--x------ (100)	- rw------- (600)	-	-	+	+	+	-	-	+
d-w------- (200)	- rw------- (600)	-	-	-	-	-	-	-	-
d-wx------ (300)	- rw------- (600)	+	+	+	+	+	-	+	+

Рис. 23: Установленные права и действия (3)

dr-------- (400)	- rw------- (600)	-	-	-	-	-	+	-	-
d-x------ (500)	- rw------- (600)	-	-	+	+	+	+	-	+
drw------- (600)	- rw------- (600)	-	-	-	-	-	+	-	-
drwx------ (700)	- rw------- (600)	+	+	+	+	+	+	+	+
d--------- (000)	- rwx------ (700)	-	-	-	-	-	-	-	-
d--x------ (100)	- rwx------ (700)	-	-	+	+	+	-	-	+
d-w------- (200)	- rwx------ (700)	-	-	-	-	-	-	-	-
d-wx------ (300)	- rwx------ (700)	+	+	+	+	+	-	+	+
dr-------- (400)	- rwx------ (700)	-	-	-	-	-	+	-	-
d-x------ (500)	- rwx------ (700)	-	-	+	+	+	+	-	+
drw------- (600)	- rwx------ (700)	-	-	-	-	-	+	-	-
drwx------ (700)	- rwx------ (700)	+	+	+	+	+	+	+	+

Рис. 24: Установленные права и действия (4)

Теперь, на основании заполненной таблицы определим те или иные минимально необходимые права для выполнения операций внутри директории и заполним таблицу “Минимальные права для совершения операций”.

Минимальные права для совершения операций

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	300	000
Удаление файла	300	000
Чтение файла	100	200
Запись в файл	100	200
Переименование файла	300	000
Создание поддиректории	300	000
Удаление поддиректории	300	000

Рис. 25: Минимальные права для совершения операций

Выводы

В результате проделанной работы мы приобрели практические навыки работы в консоли с атрибутами файлов и закрепили теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы

- Методические материалы к лабораторной работе, представленные на сайте “ТУИС РУДН” https://esystem.rudn.ru/