Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Ли Тимофей Александрович

Содержание

Список иллюстраций

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 лабораторной работы

Используя учетную запись root, создал нового пользователя guest1, установил для него пароль: (рис. @fig:001):

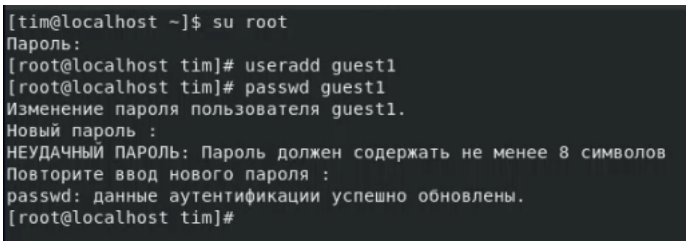

Рис. 0.1: создание пользователя

Затем, зашел в систему с новым пользователем, определил директорию, в которой нахожусь, командой pwd. Эта директория совпадает с приглашением командной строки, но не является домашней. Перешел в домашнюю директорию.

Уточнил имя пользователя командой whoami, далее, используя команду id, узнал uid (1002) и gid (1002). Ввел команду groups, получил группу guest1, что совпадает с выводом команды id.

Имя пользователя, выведенное командой id, совпадает с приглашением командной строки.

Далее посмотрел файл etc/passwd с помощью команды cat (все вышеперечисленные действия на рис. 2) (рис. @fig:002)

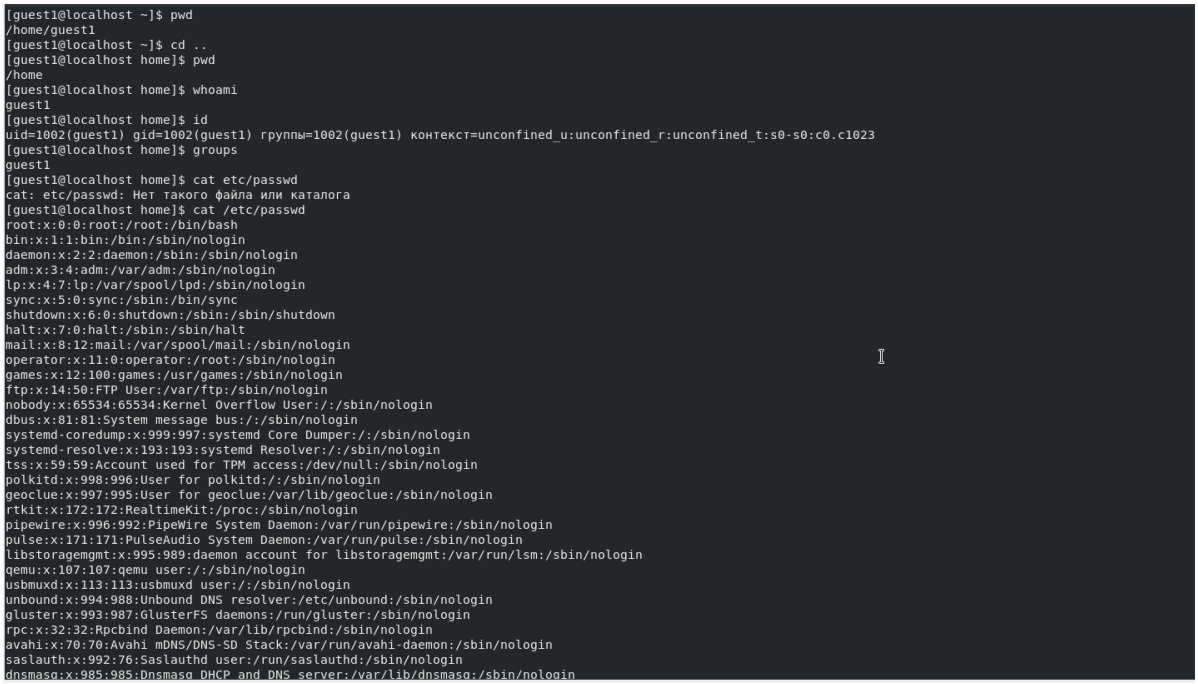

Рис. 0.2: выполненные операции

Нашел строку с данными о новом пользователе, также вывел только ее с помощью уточнения grep guest1: (рис. @fig:003)

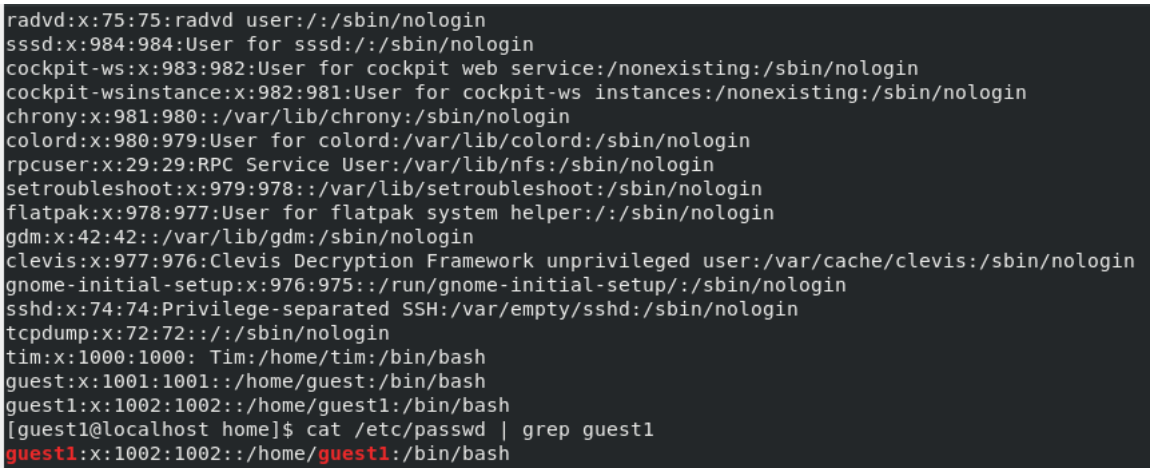

Рис. 0.3: чтение файла etc/passwd

Как видим, в файле указаны верные uid и gid (оба 1002).

Определил содержание директории home командой ls, получил список поддиректорий, на каждой из них установлены права на чтение, запись и выполнение только для владельцев.

С помощью команды lsattr посмотрел расширенные атрибуты поддиректорий. Для всех кроме guest1 мне отказано в доступе, а для guest1 никаких атрибутов не установлено.

Создал папку guest1/dir1, с помощью команд ls -l и lsattr посмотрел, какие права доступа и расширенные атрибуты у новой папки. Для нее права доступа полные, кроме записи для “прочих пользователей” и никаких расширенных атрибутов. (вышеперечисленные действия на рис. 4) (рис. @fig:004)

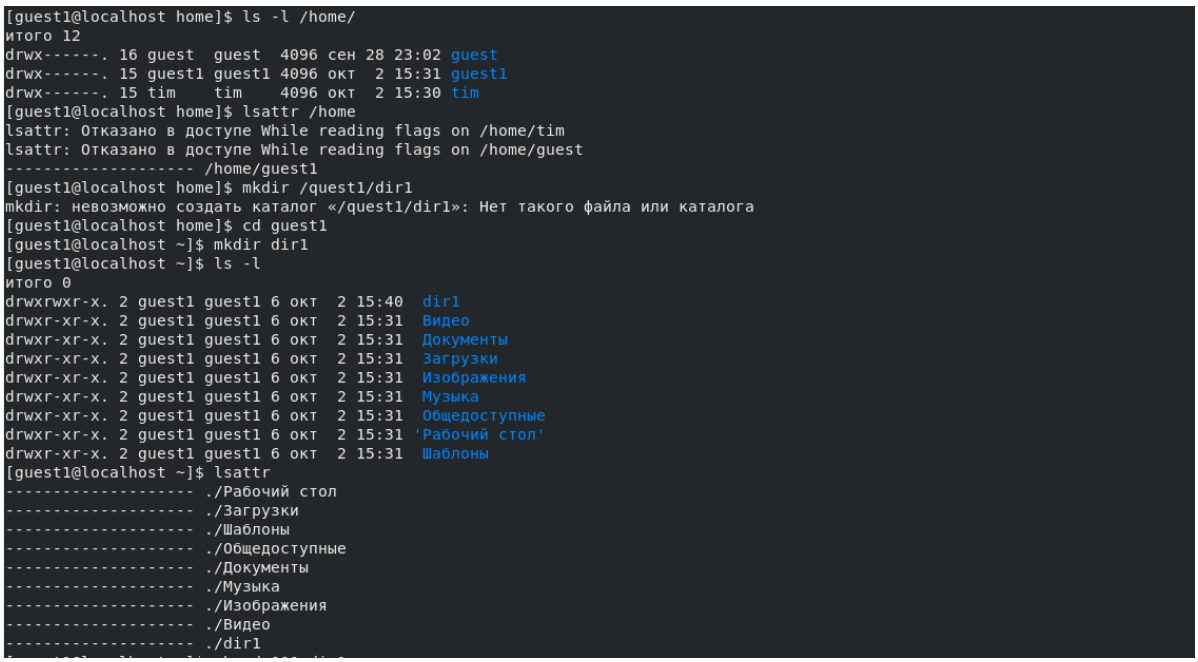

Рис. 0.4: выполненные операции

Далее я снял все права доступа с папки dir с помощью команды chmod и попытался создать в ней файл file1 с содержимым “test”. Я получил отказ, поскольку после обнуления прав доступа даже владелец не может создавать файлы в данной папке. После этого я проверил результат выполнения предыдущей операции командой ls, но

также получил отказ в доступе. В итоге я открыл файловый менеджер и убедился, что файл не создан. (вышеперечисленные действия на рис. 5) (рис. @fig:005)

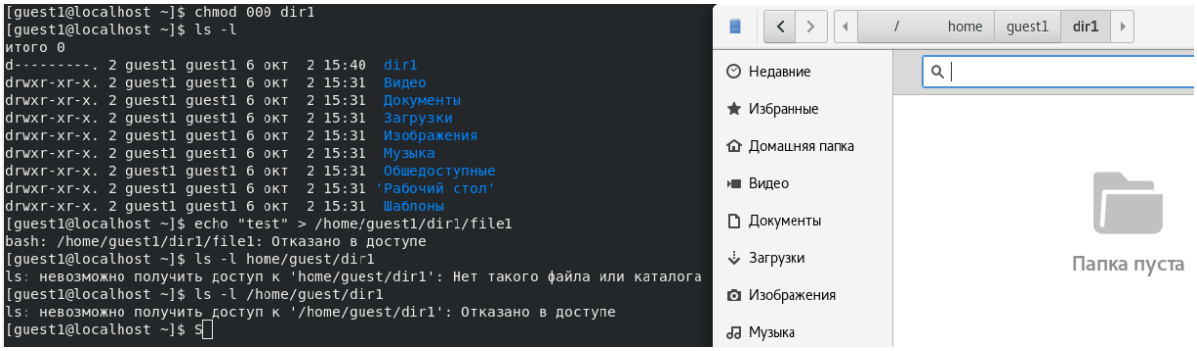

Рис. 0.5: выполненные операции

Затем, я создал в папке dir1 файл test и от имени владельца опытным путем начал проверять, какие операции разрешены, а какие нет. Для этого использовал команды cd (смена директории), touch (создание файла), rm (удаление файла), echo (запись в файл), cat (чтение файла), ls (просмотр содержимого), mv (переименование файла), chmod (смена атрибутов): (рис. @fig:006)

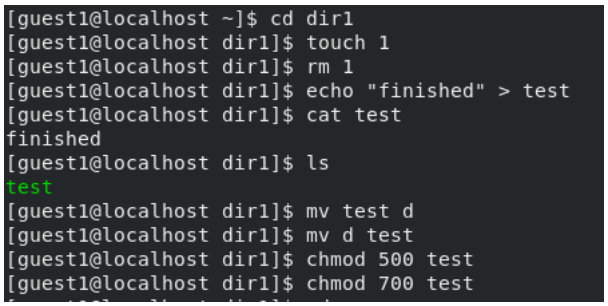

Рис. 0.6: проверка разрешений

На основе полученных ответов заполнил таблицу (таб. 2.1)

Таблица 0.1: 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)	-	-	-	-	-	-	-	-

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(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)	-	-	+	+	+	+	-	+

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(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)	+	+	+	+	+	+	+	+

Затем, на основе полученных ответов заполнил таблицу 2.2. Также для заполнения этой таблицы проверил минимальные разрешения для создания/удаления поддиректории: (рис. @fig:007):

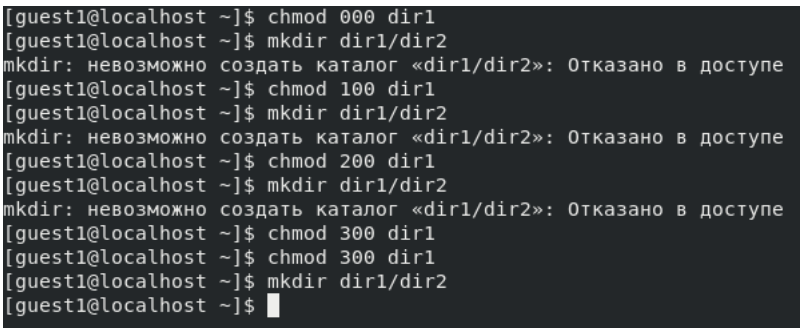

Рис. 0.7: проверка создания поддиректории

В итоге получил следующую таблицу: (таб. 2.2)

Таблица 0.2: Минимальные права для совершения операций

Операция	min права на директорию	min 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 поддиректории	d(300)	(000)
Удаление поддиректории	d(300)	(000)

Выводы

Получил практические навыки работы в консоли с атрибутами файлов, закрепил теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.