Отчёт по лабораторной работе №2

Дисциплина: Основы информационной безопасности

Калашникова Ольга Сергеевна

Содержание

# 1 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.

# 2 Выполнение лабораторной работы

## 2.1 Создание учётной записи пользователя guest

В установленной при выполнении предыдущей лабораторной работы операционной системе создаём учётную запись пользователя guest (используя учётную запись администратора) (рис. 1)

Создание учётной записи пользователя guest

Рис. 1: Создание учётной записи пользователя guest

Зададим пароль для пользователя guest (рис. 2)

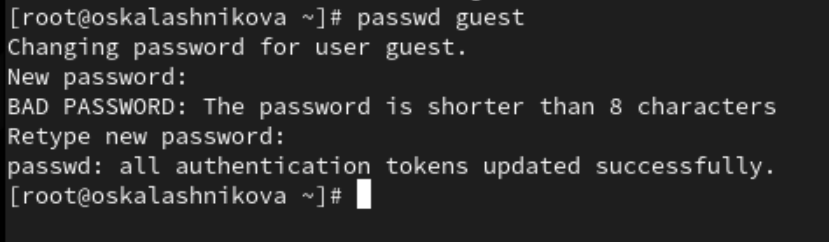


Рис. 2: Пароль для пользователя guest

Далее зайдём в систему от имени пользователя guest (рис. 3)

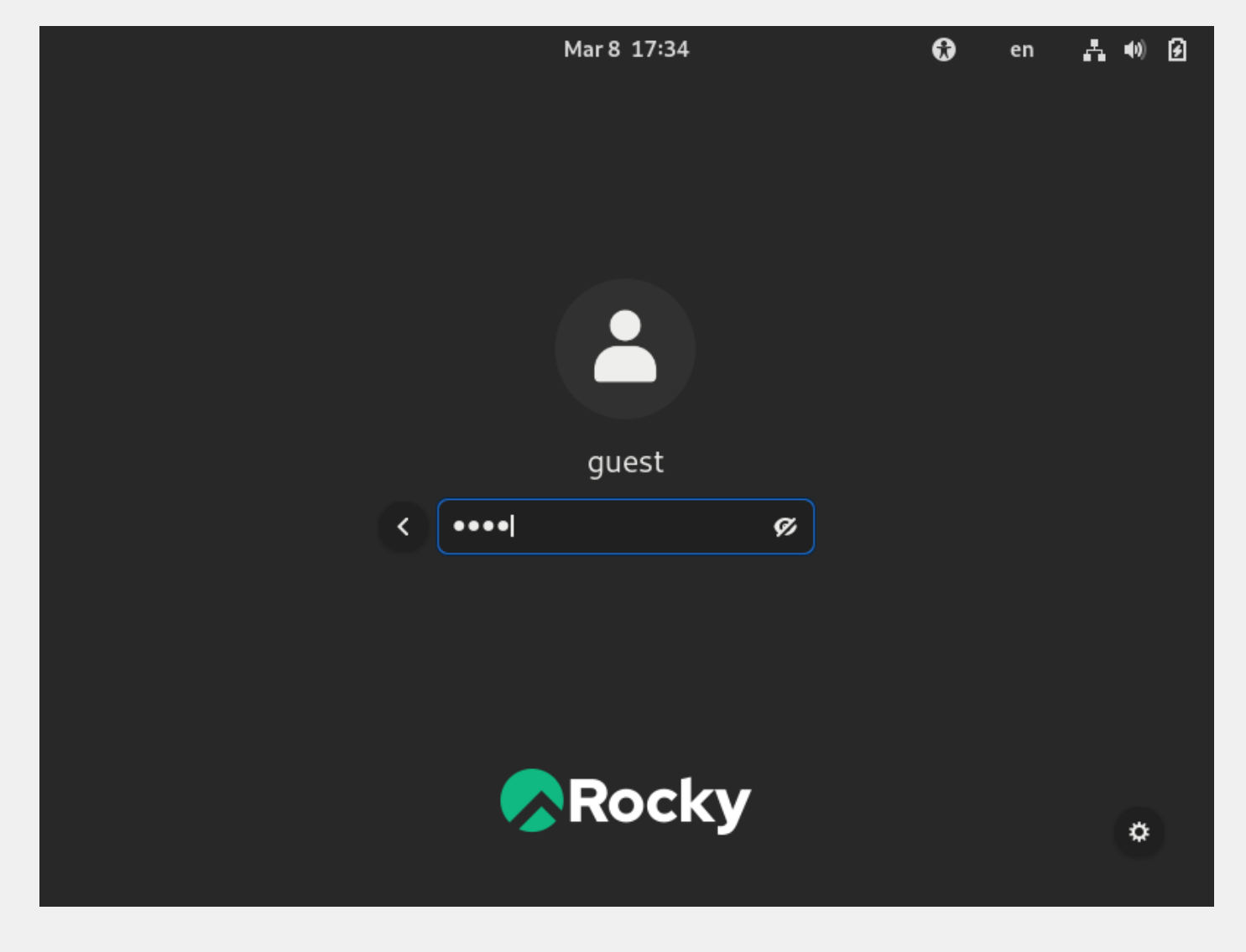


Рис. 3: Вход в учётную запись пользователя guest

## 2.2 После входа в систему от имени пользователя guest

Определим директорию, в которой мы находимся, при помощи команды *pwd* (рис. 4)

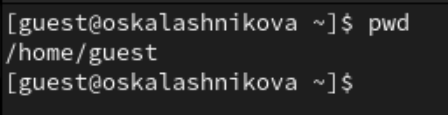


Рис. 4: Текущая директория

Уточним имя пользователя при помощи команды *whoami* (рис. 5)

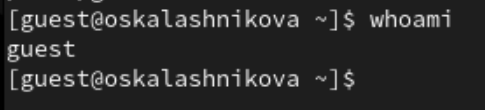


Рис. 5: Имя пользователя

Далее уточним имя пользователя, его группу, а также группы, куда входит пользователь, командой *id* (рис. 6)

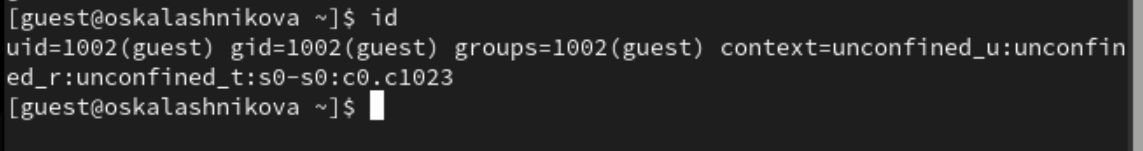


Рис. 6: Информация о пользователе через команду id

Далее сравним вывод команды *id* с выводом команды *groups*. В выводе команды *groups* информация только о названии группы, к которой относится пользователь. В выводе команды *id* больше информации: имя пользователя и имя группы, также коды имени пользователя и группы (рис. 7)

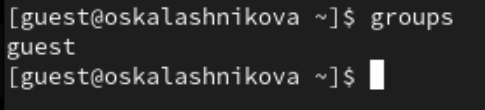


Рис. 7: Информация о пользователе через команду groups

Посмотрим файл /etc/passwd при помощи команды *cat /etc/passwd & grep guest*, чтобы найти в нём информацию об учётной записи пользователя guest, определить его uid и gid. Найденные значение совпадают с полученными в предыдущих выводах (рис. 8)

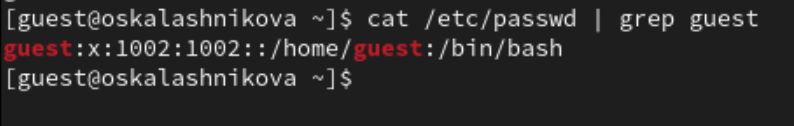


Рис. 8: Информация о пользователе в файле /etc/passwd

Определим существующие в системе директории командой *ls -l /home/*. Нам удалось получить список поддиректорий директории /home. Права у директорий oskalashnikova и guest: *drwx——* (рис. 9)

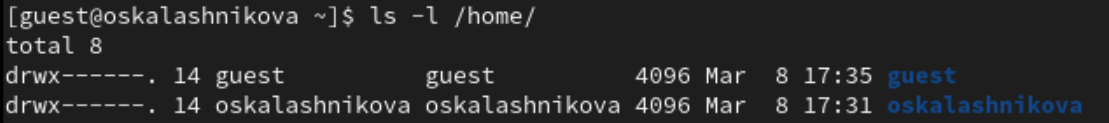


Рис. 9: Существующие в системе директории

Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой:*lsattr /home*. Увидеть расширенные атрибуты директории не удалось.(рис. 10)

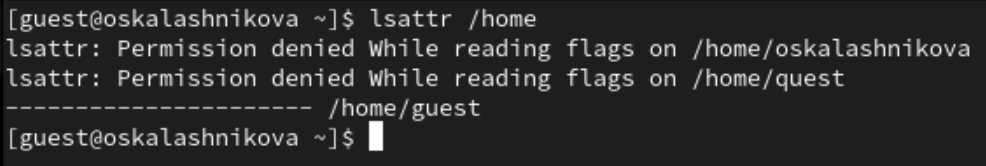


Рис. 10: Проверка расширенных атрибутов при помощи lsattr /home

Можно увидеть расширенные атрибуты директорий других пользователей при помощи команды *lsattr /home/guest* (рис. 11)

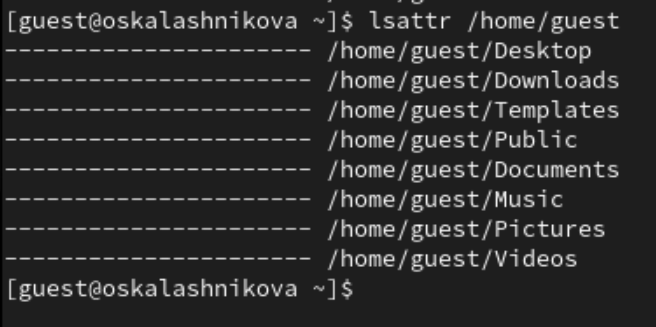


Рис. 11: Проверка расширенных атрибутов при помощи lsattr /home/guest

Далее создадим в домашней директории поддиректорию dir1 командой *mkdir dir1* (рис. 12)

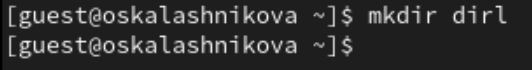


Рис. 12: Создание поддиректории dir1

Определим при помощи команды *ls -l*, какие права доступа были выставлены на директорию dir1 (рис. 13)

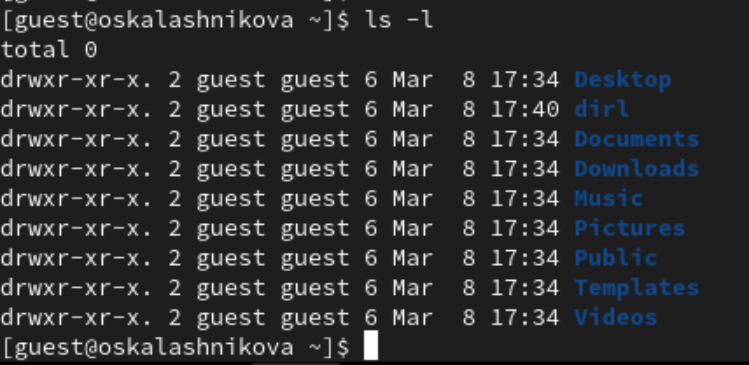


Рис. 13: Права доступа на директорию dir1

Определим при помощи команды *lsattr*, какие расширенные атрибуты были выставлены на директорию dir1 (рис. 14)

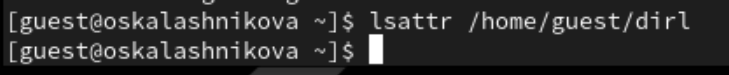


Рис. 14: Расширенные атрибуты на директорию dir1

Снимем с директории dir1 все атрибуты при помощи команды *chmod 000 dir1* (рис. 15)

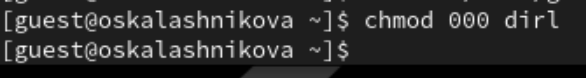


Рис. 15: Снятие всех атрибутов директории dir1

Проверим при помощи команды *ls -l* (рис. 16)

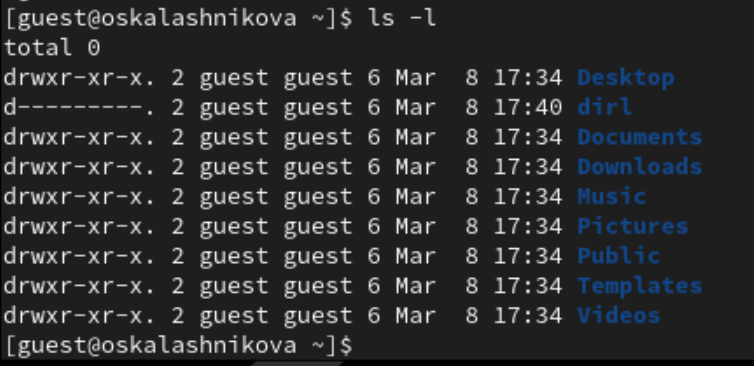


Рис. 16: Правильность выполнения команды

Попытаемся создать в директории dir1 файл file1 командой *echo “test” > /home/guest/dir1/file1*. Мы не сможем создать файл, так как у директории недостаточно прав для создания файлов (рис. 17)

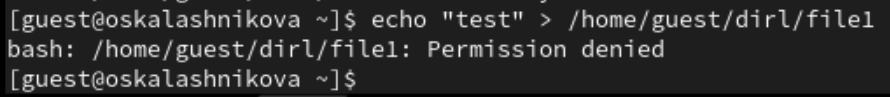


Рис. 17: Попытка создать файл в директории dir1

Далее проверим командой *ls -l /home/guest/dir1* создался ли файл. Мы сможем этого сделать, так как у директории не достаточно прав. (рис. 18)

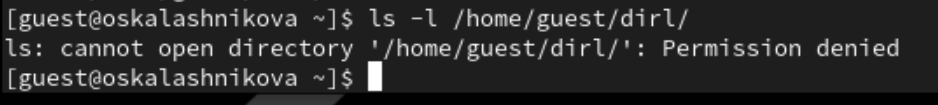


Рис. 18: Проверка содержимого директории dir1

Изменим атрибуты директории dir1 на 700 и проверим на наличие файла. Как мы видим файл не создался (рис. 19)

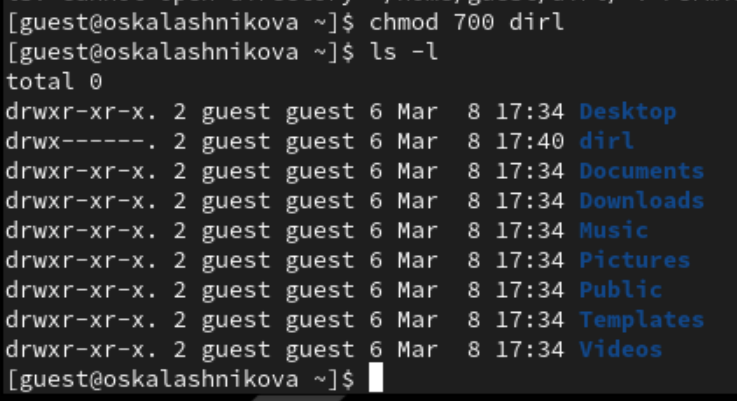


Рис. 19: Проверка содержимого директории dir1

## 2.3 Заполнение таблиц

Далее заполняем таблицу 2.1 «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, заносим в таблицу знак «+», если не разрешена, знак «-»

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) | + | + | + | + | + | + | + | + |

Далее на основании заполненной таблицы 2.1 «Установленные права и разрешённые действия» определим те или иные минимально необходимые права для выполнения операций внутри директории dir1, и заполним таблицу 2.2 «Минимальные права для совершения операций»

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) |  | - |

# 3 Выводы

В ходе выполнения лабораторной работы мы получили практические навыки работы в консоли с атрибутами файлов, закрепили теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

# 4 Список литературы

1. Лаборатораня работа №2 [Электронный ресурс] URL: https://esystem.rudn.ru/pluginfile.php/2580978/mod\_resource/content/6/002-lab\_discret\_attr.pdf