Лабораторная работа №2

Дисциплина: Основы информационной безопасности

Аветисян Давид Артурович

Содержание

# 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

1. В прошлой лабораторной работе мы установили операционную систему Rocky Linux. С помощью команды useradd guest создаём в этой операционной системе ещё одного пользователя - guest. С помощью команды passwd guest устанавливаем пароль для пользователя guest (fig. 1). Перед всеми командами мы прописываем sudo, что даёт нам права суперпользователя.

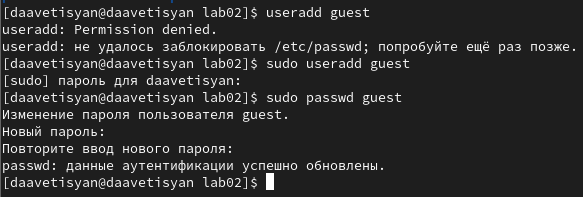


Figure 1: Создание нового пользователя

1. Выходим из нашего пользователя и входим от имени пользователя guest (fig. 2, fig. 3).

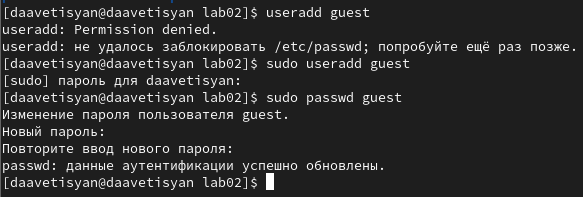


Figure 2: Вход от имени guest

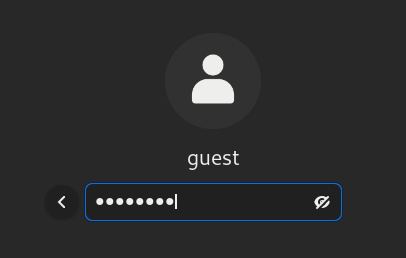


Figure 3: Вход от имени guest

1. Зашли от имени пользователя guest. Открыли терминал. Пишем команду pwd, которая покажет нам директорию, в которой мы находимся. Мы находимся в директории /home/guest. С приглашением командной строки совпадает. Мы находимся в домашней директории. С помощью команды whoami мы уточняем имя нашего пользователя. Имя - guest. Вывод команды id покажет нам имя пользователя, его группу, а также группы, куда входит пользователь (uid, gid и др.). Запомним вывод этой команды. Команда groups выводит нам группы, в которых мы состоим (fig. 4). Сравниваем полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки. Они совпадают.

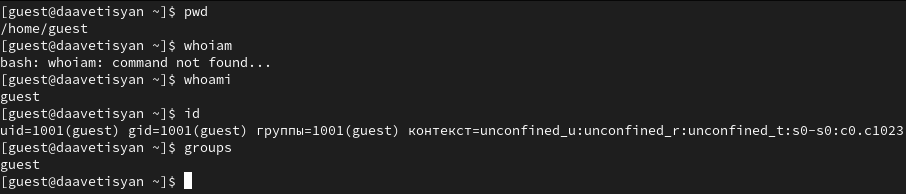


Figure 4: Команды, которые показывают информацию о пользователе

1. Просматриваем файл /etc/passwd с помощью cat (fig. 5). Наш пользователь guest находится внизу списка. uid и gid пользователя совпадает с выводом прошлых команд. Чтобы вывести только нашего пользователя guest, проще применить после команду grep, которая делает поиск по файлу (fig. 6).

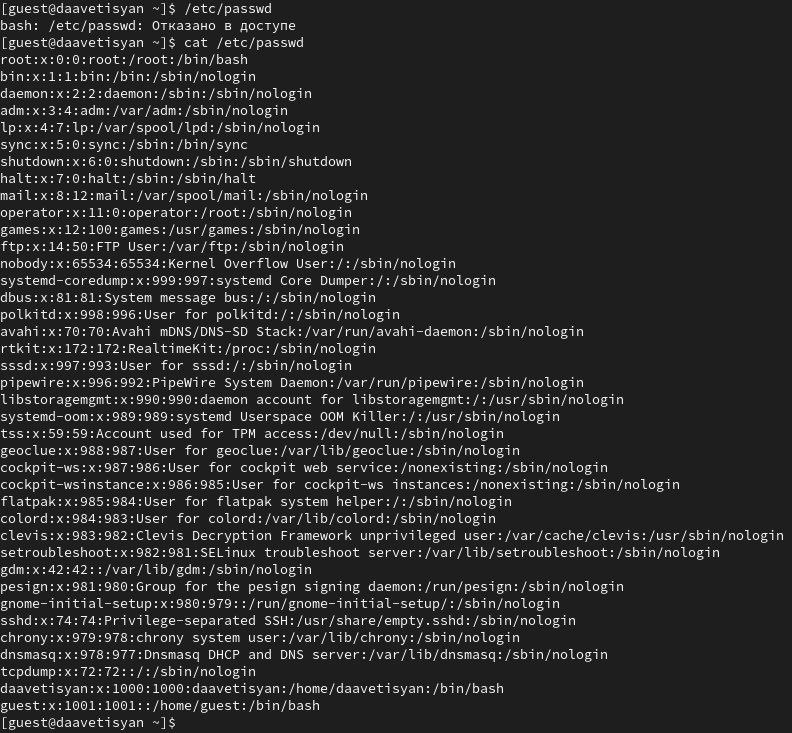


Figure 5: Просмотр /etc/passwd

Команда grep - поиск по файлу

Figure 6: Команда grep - поиск по файлу

1. С помощью команды ls -l /home/ смотрим директории в нашей системе. Видим две директории: одна гостевая (guest), другая моя (daavetisyan). Мне удалось получить список поддиректорий директории /home. На директориях установлены права чтения, записи и выполнения для самого пользователя(для группы и остальных пользователей никаких прав доступа не установлено). С помощью команды lsattr /home посмотрим, какие расширенные атрибуты стоят на директориях (fig. 7). И мне сразу выдаёт, что у меня, как у гостя, нет таких прав.

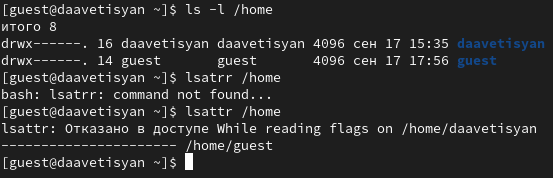


Figure 7: Директории в системе

1. Создаём директорию dir1 с помощью команды mkdir. С помощью команды ls -l посмотрим, какие права доступа и расширенные атрибуты были выставлены на директорию (fig. 8). Чтение, запись и выполнение доступны для самого пользователя и для группы, для остальных - только чтение и выполнение, расширенных атрибутов не установлено.

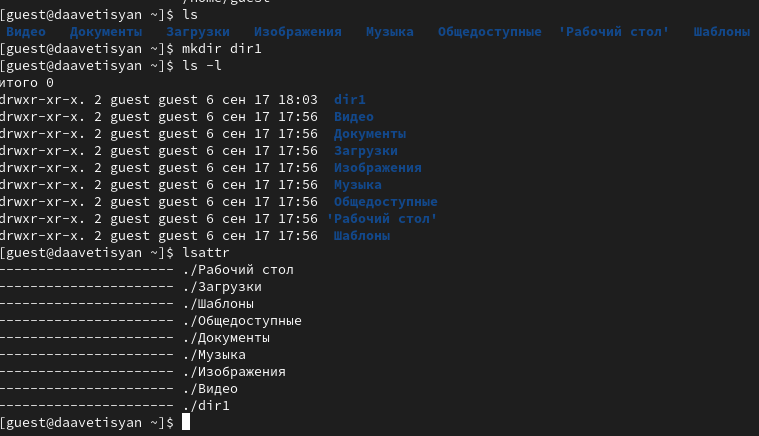


Figure 8: Новая директория

1. Снимаем с директории dir1 все атрибуты командой chmod. И сразу же посмотрим, что изменилось с помощью команды ls -l (fig. 9). Как мы видим, мы убрали права с файла. А именно: чтение, запись и выполнение.

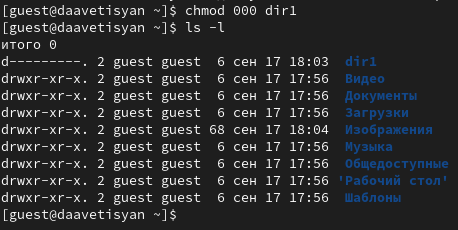


Figure 9: Права на файл

1. Пытаемся создать в директории dir1 файл file1 командой echo “test” > /home/guest/dir1/file1 (fig. 10). Как мы видим, ничего не получается, так как в прошлом пункте мы забрали право на запись в директории. Стоит отметить, что в саму директорию теперь зайти также нельзя, по той же причине. Чтобы убедиться в том, что файл не был создан, дадим право на чтение директории (fig. 11). Просмотрев директорию, мы не обнаруживаем там файла, который мы пытались создать.

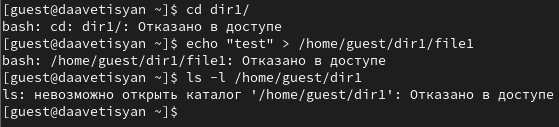


Figure 10: Попытка создать файл

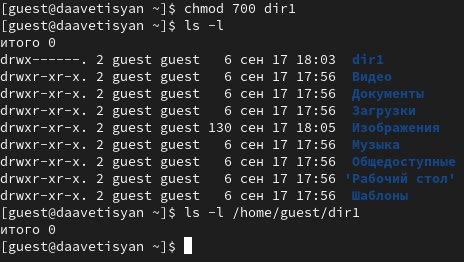


Figure 11: Проверка

9 )Заполним таблицу “Установленные права и разрешённые действия”. Нужно заполнить 64 ячейки.

Создание файла: echo”text” > /home/guest/dir1/file2. Удаление файла: rm -r /home/guest/dir1/file1. Запись в файл: echo”textnew” > /home/guest/dir1/file1. Чтение файла: cat /home/guest/dir1/file1. Смена директории: cd dir1. Просмотр файлов в директории: ls dir1. Переименование файла: mv /home/guest/dir1/file1 filenew. Смена атрибутов файла: chattr -a /home/guest/dir1/file1.

| 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) | + | + | - | - | + | - | + | - |
| d r– (400) | (000) | - | - | - | - | - | + | - | - |
| d r-x (500) | (000) | - | - | - | - | + | + | - | - |
| d rw- (600) | (000) | - | - | - | - | - | + | - | - |
| d rwx (700) | (000) | + | + | - | - | + | + | + | - |
| —————— | ————- | —————- | —————- | ————— | ————– | —————— | —————————— | ———————- | ———————– |
| d (000) | (100) | - | - | - | - | - | - | - | - |
| d –x (100) | (100) | - | - | - | - | + | - | - | - |
| d -w- (200) | (100) | - | - | - | - | - | - | - | - |
| d -wx (300) | (100) | + | + | - | - | + | - | + | - |
| d r– (400) | (100) | - | - | - | - | - | + | - | - |
| d r-x (500) | (100) | - | - | - | - | + | + | - | - |
| d rw- (600) | (100) | - | - | - | - | - | + | - | - |
| d rwx (700) | (100) | + | + | - | - | + | + | + | - |
| —————— | ————- | —————- | —————- | ————— | ————– | —————— | —————————— | ———————- | ———————– |
| d (000) | (200) | - | - | - | - | - | - | - | - |
| d –x (100) | (200) | - | - | + | - | + | - | - | - |
| d -w- (200) | (200) | - | - | - | - | - | - | - | - |
| d -wx (300) | (200) | + | + | + | - | + | - | + | - |
| d r– (400) | (200) | - | - | - | - | - | + | - | - |
| d r-x (500) | (200) | - | - | + | - | + | + | - | - |
| d rw- (600) | (200) | - | - | - | - | - | + | - | - |
| d rwx (700) | (200) | + | + | + | - | + | + | + | - |
| —————— | ————- | —————- | —————- | ————— | ————– | —————— | —————————— | ———————- | ———————– |
| d (000) | (300) | - | - | - | - | - | - | - | - |
| d –x (100) | (300) | - | - | + | - | + | - | - | - |
| d -w- (200) | (300) | - | - | - | - | - | - | - | - |
| d -wx (300) | (300) | + | + | - | + | + | - | + | - |
| d r– (400) | (300) | - | - | - | - | - | + | - | - |
| d r-x (500) | (300) | - | - | + | - | + | + | - | - |
| d rw- (600) | (300) | - | - | - | - | - | + | - | - |
| d rwx (700) | (300) | + | + | + | - | + | + | + | - |
| —————— | ————- | —————- | —————- | ————— | ————– | —————— | —————————— | ———————- | ———————– |
| d (000) | (400) | - | - | - | - | - | - | - | - |
| d –x (100) | (400) | - | - | - | + | + | - | - | + |
| d -w- (200) | (400) | - | - | - | - | - | - | - | - |
| d -wx (300) | (400) | + | + | - | + | + | - | + | + |
| d r– (400) | (400) | - | - | - | - | - | + | - | - |
| d r-x (500) | (400) | - | - | - | + | + | + | - | + |
| d rw- (600) | (400) | - | - | - | - | - | + | - | - |
| d rwx (700) | (400) | + | + | - | + | + | + | + | + |
| —————— | ————- | —————- | —————- | ————— | ————– | —————— | —————————— | ———————- | ———————– |
| d (000) | (500) | - | - | - | - | - | - | - | - |
| d –x (100) | (500) | - | - | - | + | + | - | - | + |
| d -w- (200) | (500) | - | - | - | - | - | - | - | - |
| d -wx (300) | (500) | + | + | - | + | + | - | + | + |
| d r– (400) | (500) | - | - | - | - | - | + | - | - |
| d r-x (500) | (500) | - | - | - | + | + | + | - | + |
| d rw- (600) | (500) | - | - | - | - | - | + | - | - |
| d rwx (700) | (500) | + | + | - | + | + | + | + | + |
| —————— | ————- | —————- | —————- | ————— | ————– | —————— | —————————— | ———————- | ———————– |
| d (000) | (600) | - | - | - | - | - | - | - | - |
| d –x (100) | (600) | - | - | + | + | + | - | - | + |
| d -w- (200) | (600) | - | - | - | - | - | - | - | - |
| d -wx (300) | (600) | + | + | + | + | + | - | + | + |
| d r– (400) | (600) | - | - | - | - | - | + | - | - |
| d r-x (500) | (600) | - | - | + | + | + | + | - | + |
| d rw- (600) | (600) | - | - | - | - | - | + | - | - |
| d rwx (700) | (600) | + | + | + | + | + | + | + | + |
| —————— | ————- | —————- | —————- | ————— | ————– | —————— | —————————— | ———————- | ———————– |
| d (000) | (700) | - | - | - | - | - | - | - | - |
| d –x (100) | (700) | - | - | + | + | + | - | - | + |
| d -w- (200) | (700) | - | - | - | - | - | - | - | - |
| d -wx (300) | (700) | + | + | + | + | + | - | + | + |
| d r– (400) | (700) | - | - | - | - | - | + | - | - |
| d r-x (500) | (700) | - | - | + | + | + | + | - | + |
| d rw- (600) | (700) | - | - | - | - | - | + | - | - |
| d rwx (700) | (700) | + | + | + | + | + | + | + | + |

1. Заполним таблицу “Минимальные права для совершения операций”.

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

# Выводы

Я 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.

# Список литературы

* Права доступа к файлам в Linux [Электронный ресурс]. 2019. URL: https://losst.ru/prava-dostupa-k-fajlam-v-linux.