Лабораторная работа №3

Дисциплина: Информационная безопасность

Новосельцев Данила Сергеевич

Содержание

# 1 Цели и задачи работы

## 1.1 Цель

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.

## 1.2 Задачи

1. Создать двух новых пользователей (гостевых аккаунтов) виртуальной машины;
2. Через гостевые аккаунту выполнить задания лабораторной работы;
3. Заполнить таблицы об уровнях доступа и действиях с файлами/директориями.

# 3 Теоретическое введение [1]

Для разграничения действий над файлами определены три базовых права доступа (базовые разрешения):

* чтение r — «read»,
* запись w — «write» и
* выполнение х — «execute»,

соответствующие разрешению выполнять системные вызовы read, write и execve (точнее, системному вызову open с флагами O\_RDONLY и O\_WRONLY, но для простоты можно считать r — read, a w — write).

Каждое из базовых прав назначается на файл тому или иному пользователю или группе, разрешая соответствующую операцию.

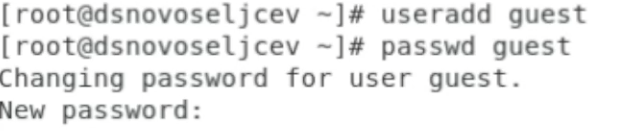
В наследии классической UNIX определены только три субъекта, которым назначаются базовые права — пользователь-владелец (owner), группа-владелец (group owner) и все остальные (others). Совокупность их базовых прав называется режимом доступа (access mode) к файлу.

Базовое право может быть назначено r, w или х или отозвано —, поэтому в метаданных файла представляется одним битом, а для режима доступа требуется девять бит: по три бита прав на каждый из трех субъектов доступа.

Компактно режим доступа может быть записан соответствующим числом в восьмеричной системе счисления rw-r–r– .

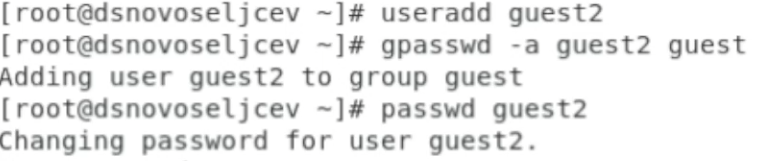
# 3 Выполнение лабораторной работы [2]

1. В установленной ОС создаю учётную запись пользователя guest (??)
2. Задаём пароль для пользователя guest (??)



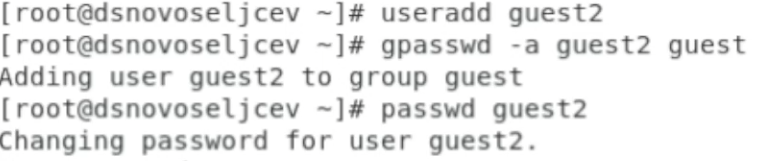
Задание пароля для пользователя guest

1. Аналогично пунктам 1 и 2 создаю пользователя guest2 (??)



Cоздание учетной запись пользователя guest2 и задание пароля

1. С помощью команды gpasswd -a guest2 guest добавляю пользователя guest2 в группу guest (??)



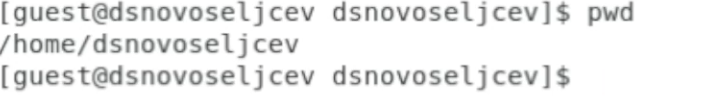
Команда gpasswd -a guest2 guest

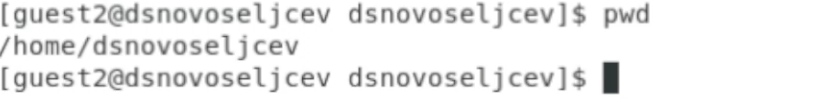
1. Захожу в две консоли, в каждую от разных пользователей (guest и guest2) (??)



Две консоли

1. С помощью команды pwd определить, в какой директории находятся пользователи (??)





В какой директории находятся пользователи?

1. Уточняю информацию о пользователях с помощью команды id, определяем группы с помощью команды groups для обоих пользователей (??).

По результатам выполнения команд id -G, id -Gn и groups видно, что первая выводит только ID групп, в которых состоит пользователь, вторая — названия групп, в которых состоит пользователь, и третья выводит строку вида

<username> : <groupname> <groupname> <groupname> <groupname>

1. Сравниваем информацию о пользователях с содержанием файла /etc/group (??, ??)
2. От имени пользователя guest2 регистрируем этого пользователя в группе
3. От имени пользователя guest разрешаем все действия для группы в папке /home/guest (??)
4. От имени пользователя guest снимаем все атрибуты с директории /home/guest/dir1 командой chmod 000 dir1 (??)

Далее пробуем выполнять различные действия от лица пользователя guest2 с папкой dir1 в домашней директории пользователя guest и, по результатам выполнения, заполняем таблицы [1](#tbl:access_1) и [2](#tbl:access_2).

## 4.1 Таблицы ([1](#tbl:access_1) и [2](#tbl:access_2))

Table 1: Установленные права и разрешённые действия

| Права директории | Права файла | Создание файла | Удаление файла | Запись файла | Чтение файла | Смена директории | Просмотр файлов в директории | Переименование файла | Смена атрибутов файла |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| d(000) | (000) | - | - | - | - | - | - | - | - |
| d(000) | (010) | - | - | - | - | - | - | - | - |
| d(000) | (020) | - | - | - | - | - | - | - | - |
| d(000) | (030) | - | - | - | - | - | - | - | - |
| d(000) | (040) | - | - | - | - | - | - | - | - |
| d(000) | (050) | - | - | - | - | - | - | - | - |
| d(000) | (060) | - | - | - | - | - | - | - | - |
| d(000) | (070) | - | - | - | - | - | - | - | - |
| —————————– | ————- | —————- | —————- | ————– | ————– | —————— | —————————— | ———————- | ———————– |
| d—–x— | (000) | - | - | - | - | + | - | - | - |
| d—–x— | (010) | - | - | - | - | + | - | - | - |
| d—–x— | (020) | - | - | + | - | + | - | - | - |
| d—–x— | (030) | - | - | + | - | + | - | - | - |
| d—–x— | (040) | - | - | - | + | + | - | - | - |
| d—–x— | (050) | - | - | - | + | + | - | - | - |
| d—–x— | (060) | - | - | + | + | + | - | - | - |
| d—–x— | (070) | - | - | + | + | + | - | - | - |
| —————————– | ————- | —————- | —————- | ————– | ————– | —————— | —————————— | ———————- | ———————– |
| d—-w—- | (000) | - | - | - | - | - | - | - | - |
| d—-w—- | (010) | - | - | - | - | - | - | - | - |
| d—-w—- | (020) | - | - | - | - | - | - | - | - |
| d—-w—- | (030) | - | - | - | - | - | - | - | - |
| d—-w—- | (040) | - | - | - | - | - | - | - | - |
| d—-w—- | (050) | - | - | - | - | - | - | - | - |
| d—-w—- | (060) | - | - | - | - | - | - | - | - |
| d—-w—- | (070) | - | - | - | - | - | - | - | - |
| —————————– | ————- | —————- | —————- | ————– | ————– | —————— | —————————— | ———————- | ———————– |
| d—-wx— | (000) | + | + | - | - | + | - | + | - |
| d—-wx— | (010) | + | + | - | - | + | - | + | - |
| d—-wx— | (020) | + | + | + | - | + | - | + | - |
| d—-wx— | (030) | + | + | + | - | + | - | + | - |
| d—-wx— | (040) | + | + | - | + | + | - | + | + |
| d—-wx— | (050) | + | + | - | + | + | - | + | + |
| d—-wx— | (060) | + | + | + | + | + | - | + | + |
| d—-wx— | (070) | + | + | + | + | + | - | + | + |
| —————————– | ————- | —————- | —————- | ————– | ————– | —————— | —————————— | ———————- | ———————– |
| d—r—– | (000) | - | - | - | - | - | + | - | - |
| d—r—– | (010) | - | - | - | - | - | + | - | - |
| d—r—– | (020) | - | - | - | - | - | + | - | - |
| d—r—– | (030) | - | - | - | - | - | + | - | - |
| d—r—– | (040) | - | - | - | - | - | + | - | - |
| d—r—– | (050) | - | - | - | - | - | + | - | - |
| d—r—– | (060) | - | - | - | - | - | + | - | - |
| d—r—– | (070) | - | - | - | - | - | + | - | - |
| —————————– | ————- | —————- | —————- | ————– | ————– | —————— | —————————— | ———————- | ———————– |
| d—r-x— | (000) | - | - | - | - | + | + | - | - |
| d—r-x— | (010) | - | - | - | - | + | + | - | - |
| d—r-x— | (020) | - | - | + | - | + | + | - | - |
| d—r-x— | (030) | - | - | + | - | + | + | - | - |
| d—r-x— | (040) | - | - | - | + | + | + | - | - |
| d—r-x— | (050) | - | - | - | + | + | + | - | - |
| d—r-x— | (060) | - | - | + | + | + | + | - | - |
| d—r-x— | (070) | - | - | + | + | + | + | - | - |
| —————————– | ————- | —————- | —————- | ————– | ————– | —————— | —————————— | ———————- | ———————– |
| d—rw—- | (000) | - | - | - | - | - | + | - | - |
| d—rw—- | (010) | - | - | - | - | - | + | - | - |
| d—rw—- | (020) | - | - | - | - | - | + | - | - |
| d—rw—- | (030) | - | - | - | - | - | + | - | - |
| d—rw—- | (040) | - | - | - | - | - | + | - | - |
| d—rw—- | (050) | - | - | - | - | - | + | - | - |
| d—rw—- | (060) | - | - | - | - | - | + | - | - |
| d—rw—- | (070) | - | - | - | - | - | + | - | - |
| —————————– | ————- | —————- | —————- | ————– | ————– | —————— | —————————— | ———————- | ———————– |
| d—rwx— | (000) | + | + | - | - | + | + | + | - |
| d—rwx— | (010) | + | + | - | - | + | + | + | - |
| d—rwx— | (020) | + | + | + | - | + | + | + | - |
| d—rwx— | (030) | + | + | + | - | + | + | + | - |
| d—rwx— | (040) | + | + | - | + | + | + | + | + |
| d—rwx— | (050) | + | + | - | + | + | + | + | + |
| d—rwx— | (060) | + | + | + | + | + | + | + | + |
| d—rwx— | (070) | + | + | + | + | + | + | + | + |

Table 2: Минимальные права для совершения операций

| Операция | Минимальные права на директорию | Минимальные права на файл |
| --- | --- | --- |
| Создание файла | d—-wx— | (000) |
| Удаление файла | d—-wx— | (000) |
| Чтение файла | d—–x— | (040) |
| Запись в файл | d—–x— | (020) |
| Переименование файла | d—-wx— | (000) |
| Создание поддиректории | d—-wx— | (000) |
| Удаление поддиректории | d—-wx— | (000) |

# 5 Выводы по проделанной работе

## 5.1 Сравнения таблиц [1](#tbl:access_1) и [2](#tbl:access_2) с аналогичными таблицами из лабораторной работы №2 [3].

Если сравнивать получившиеся результаты в виде сводных таблиц, то можно легко заметить, что права действуют по одним и тем же принципам как в случае, если они выданы владельцу файла, так и в случае, если они даны пользователям из группы владельца файла. Главное, отслеживать, какие права выданы пользователю, который пытается получить доступ к файлу, а уже исходя из этого легко предсказать, как себя поведёт та или иная функция в зависимости от выданных прав.

## 5.2 Общий вывод

В результате выполнения работы мы ознакомились с основными этапами установки виртуальных машин и их настроек, а также создали виртуальную среду для выполнения последующих лабораторных работ.