Отчёт по лабораторной работе №2

дисциплина: Информационная безопасность

Быстров Глеб Андреевич

Содержание

# 1 Цель работы

В данной лабораторной работе мне будет необходимо получить практические навыки работы в консоли с атрибутами файлов, закрепить теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

# 2 Задание

Последовательно выполнить пункты по настройке доступа через команды в терминале для нового пользователя.

# 3 Теоретическое введение

В Linux у каждого файла и каждого каталога есть два владельца: пользователь и группа.

Эти владельцы устанавливаются при создании файла или каталога. Пользователь, который создаёт файл становится владельцем этого файла, а первичная группа, в которую входит этот же пользователь, так же становится владельцем этого файла. Чтобы определить, есть ли у вас как у пользователя права доступа к файлу или каталогу, оболочка проверяет владение ими. [1].

Выделяют три категории пользователей, которым могут предоставляться права на файл:

* Сам владелец (u – user) объекта – конкретный пользователь, чье имя числится в атрибутах файла как имя владельца этого файла. Обычно если пользователь создает файл, то он автоматически записывается как его владелец.
* Группа (g – group), к которой принадлежит владелец файла. Когда в Linux создается пользователь, то для него создается одноименная группа. Однако средствами администрирования системы можно объединять пользователей в различные группы. При этом конкретный пользователь может входить в состав нескольких групп. Группы позволяют предоставлять права доступа к ресурсам сразу нескольким людям, но при этом ограниченному кругу лиц.
* Все остальные (o – other) – это все те, кто не является владельцем файла и не принадлежит к группе владельца файла. То есть любой посторонний пользователь.

Чтение, запись, выполнение – это то, что можно делать с существующим файлом, возможные действия над ним. У каждой категории пользователей (владельца, группы, остальных) должны быть свои права на каждое вышеупомянутое действие.

* Право на чтение (r – read) означает, что файл можно просматривать. Например, открыть файл и, если он текстовый, прочитать содержащийся в нем текст. Если это файл изображения, то можно посмотреть изображение. Наличие права только на чтение не позволяет изменять файл. То есть нельзя будет исправить текст или подрисовать что-то к картинке.
* Право на запись (w – write) позволяет изменять файл, то есть дописывать в него информацию или заменять ее другой.
* Право на исполнение (x – execution) имеет смысл не для всех файлов, хотя может быть установлено для любого. Это право позволяет исполнять файл как программу, при этом в файле должны быть записаны инструкции для процессора, то есть файл должен быть исполняемой программой.

Первые три записи – это права владельца, вторые три записи – права группы, последняя тройка – права на файл для всех остальных. Если обозначить каждое право соответствующей буквой, и все права всем предоставляются, то получится такая запись: rwxrwxrwx [2].

Рассмотрим подробнее, что значат условные значения флагов прав:

— - нет прав, совсем;

–x - разрешено только выполнение файла, как программы но не изменение и не чтение;

-w- - разрешена только запись и изменение файла;

-wx - разрешено изменение и выполнение, но в случае с каталогом, вы не можете посмотреть его содержимое;

r– - права только на чтение;

r-x - только чтение и выполнение, без права на запись;

rw- - права на чтение и запись, но без выполнения;

rwx - все права;

–s - установлен SUID или SGID бит, первый отображается в поле для владельца, второй для группы;

–t - установлен sticky-bit, а значит пользователи не могут удалить этот файл [3].

Использование команды ls с опцией -l выведет на экран «длинную» распечатку, в которой будут, среди прочего, отражены права доступа к файлу [4].

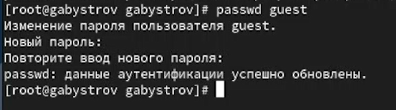
# 4 Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создал учётную запись пользователя guest (использовал учётную запись администратора): useradd guest (рис. ??).

Создание новой учетной записи

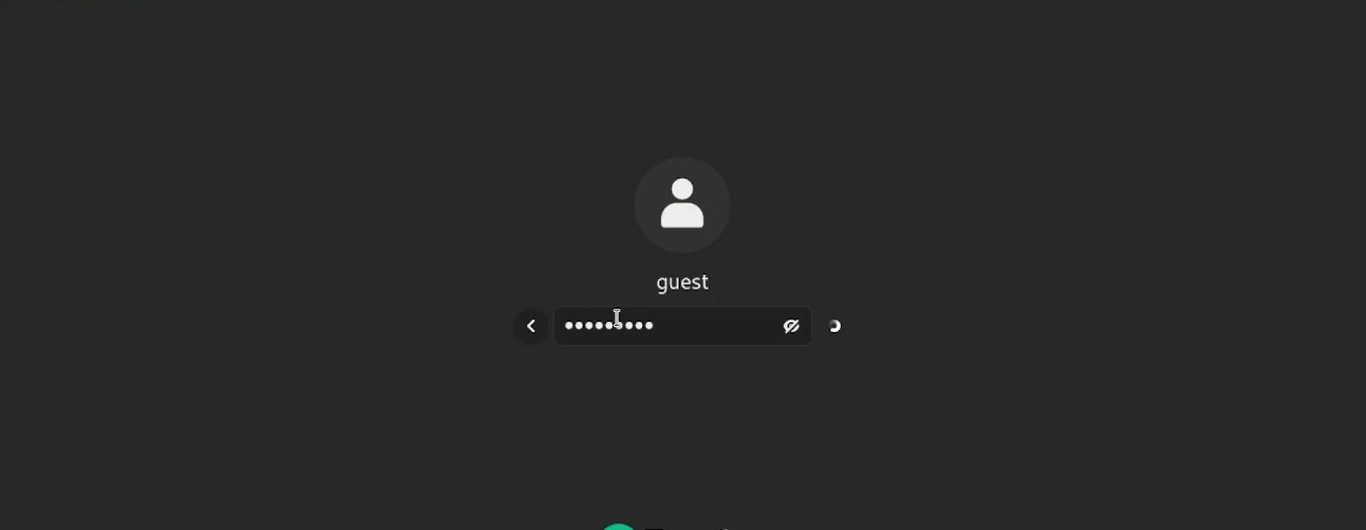
Создание новой учетной записи

1. Задал пароль для пользователя guest (использовал учётную запись администратора): passwd guest (рис. ??).



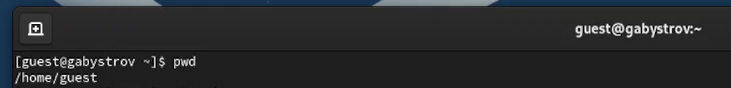
Создание пароля

1. Вошёл в систему от имени пользователя guest (рис. ??).



Вход в систему

1. Определил директорию, в которой нахожусь, командой pwd. С приглашением командной строки совпадает. Является домашней директорией (рис. ??).



Определение дирректории

1. Уточнил имя пользователя командой whoami. (рис. ??).

Уточнение пользователя

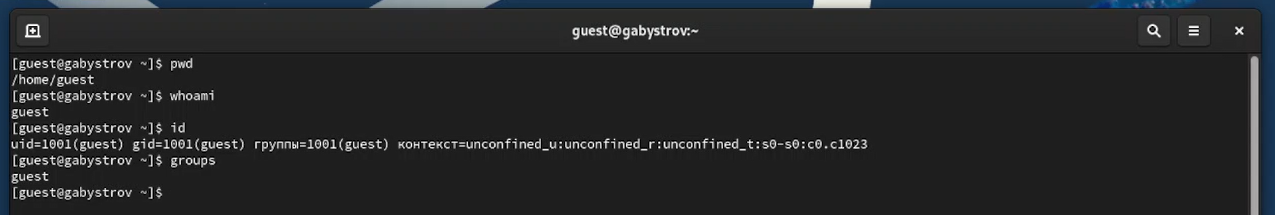
Уточнение пользователя

1. Уточнил имя пользователя, его группу, а также группы, куда входит пользователь, командой id. Выведенные значения с выводом команды groups совпадают (рис. ??).



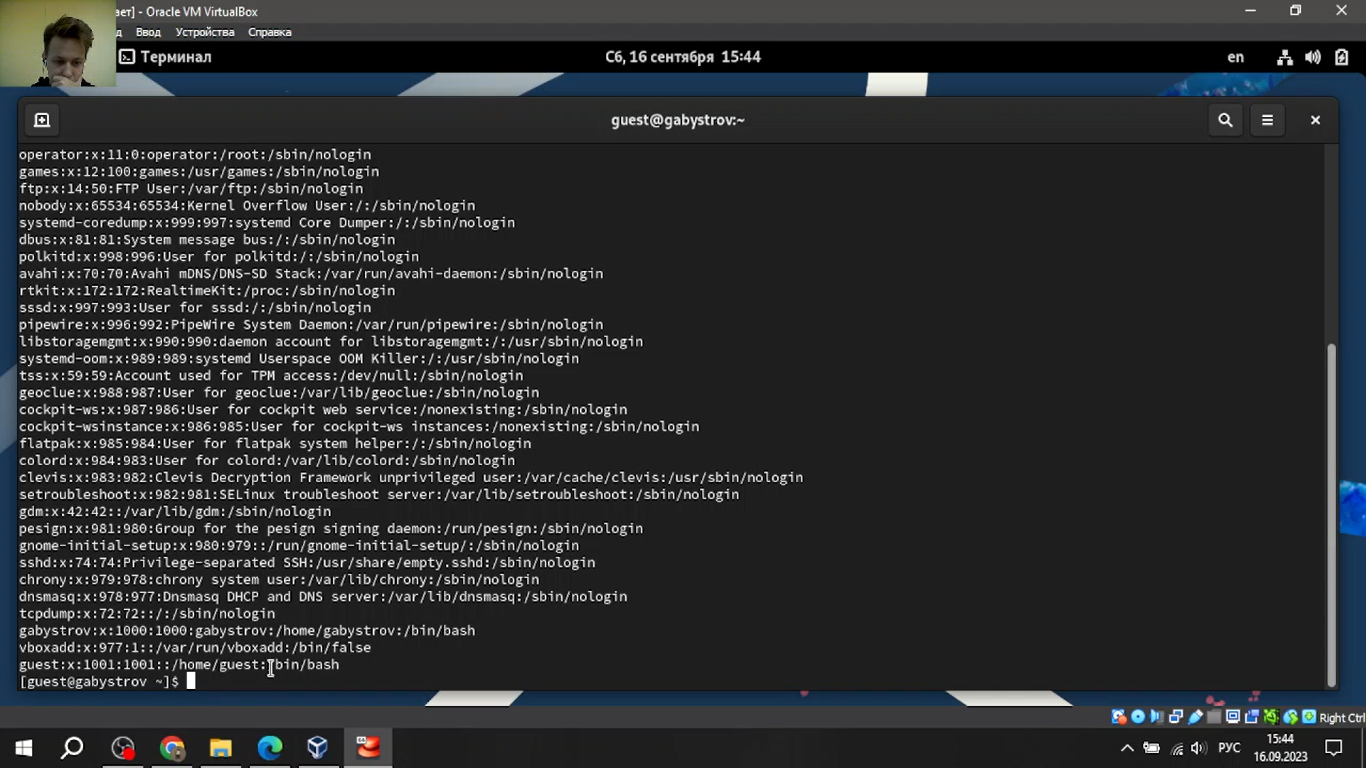
Команды id и group

1. Полученная информация об имени пользователя с данными, выводимыми в приглашении командной строки совпадает (рис. ??).



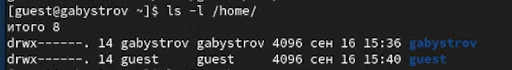
Приглашение командной строки

1. Просмотел файл /etc/passwd командой cat /etc/passwd. Нашёл в нём свою учётную запись. Определил uid пользователя (1001). Определил gid пользователя (1001). Найденные значения совпадают с полученными в предыдущих пунктах (рис. ??).



Просмотр файла

1. Определил существующие в системе директории командой ls -l /home/. Удалось получить список поддиректорий директории /home. На директориях установлены права для чтения, записи и выполнения только для пользователя (рис. ??).



Существующие в системе директории

1. Проверил какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: lsattr /home. Удалось увидеть расширенные атрибуты директории только для пользователя. Не удалось увидеть расширенные атрибуты директорий других пользователей? (рис. ??).

Расширенные атрибуты установлены на поддиректориях

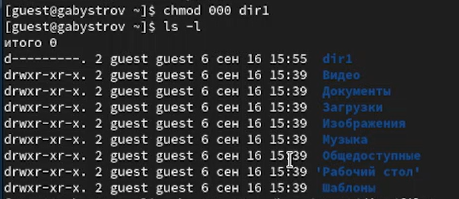
Расширенные атрибуты установлены на поддиректориях

1. Создал в домашней директории поддиректорию dir1 командой mkdir dir1. Определил командами ls -l и lsattr, какие права доступа и расширенные атрибуты были выставлены на директорию dir1: чтение, запись и выполнение для пользователя и групп. Чтение и выполнение для остальных. Расширенных атрибутов нет (рис. ??).



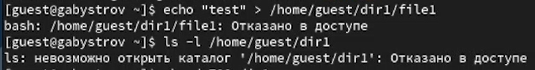
Работа с поддиректорией

1. Снял с директории dir1 все атрибуты командой chmod 000 dir1 и проверил с её помощью правильность выполнения команды ls -l. Все было верно(рис. ??).



Снятие атрибутов и проверка ls -l

1. Попытался создать в директории dir1 файл file1 командой echo “test” > /home/guest/dir1/file1. Получил отказ в выполнении операции по созданию файла так как до этого убрал данное право. Оценил, как сообщение об ошибке отразилось на создании файла. Файл не создался. Проверил командой ls -l /home/guest/dir1 действительно ли файл file1 не находится внутри директории dir1. (рис. ??).



Работа с файлом в дирректории

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

Table 1: Установленные права и разрешенные действия

| Права директории | Права файла | Создание файла | Удаление файла | Запись в файл | Чтение файла | Смена директории | Просмотр файлов директории | Переименование файла | Смена аттрибутов файла |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| --------- (000) | --------- (000) | - | - | - | - | - | - | - | - |
| --------- (000) | --x------ (100) | - | - | - | - | - | - | - | - |
| --------- (000) | -w------- (200) | - | - | - | - | - | - | - | - |
| --------- (000) | -wx------ (300) | - | - | - | - | - | - | - | - |
| --------- (000) | r-------- (400) | - | - | - | - | - | - | - | - |
| --------- (000) | r-x------ (500) | - | - | - | - | - | - | - | - |
| --------- (000) | rw------- (600) | - | - | - | - | - | - | - | - |
| --------- (000) | rwx------ (700) | - | - | - | - | - | - | - | - |
| --x------ (100) | --------- (000) | - | - | - | - | + | - | - | - |
| --x------ (100) | --x------ (100) | - | - | - | - | + | - | - | - |
| --x------ (100) | -w------- (200) | - | - | + | - | + | - | - | - |
| --x------ (100) | -wx------ (300) | - | - | + | - | + | - | - | - |
| --x------ (100) | r-------- (400) | - | - | - | + | + | - | - | + |
| --x------ (100) | r-x------ (500) | - | - | - | + | + | - | - | + |
| --x------ (100) | rw------- (600) | - | - | + | + | + | - | - | + |
| --x------ (100) | rwx------ (700) | - | - | + | + | + | - | - | + |
| -w------- (200) | --------- (000) | - | - | - | - | - | - | - | - |
| -w------- (200) | --x------ (100) | - | - | - | - | - | - | - | - |
| -w------- (200) | -w------- (200) | - | - | - | - | - | - | - | - |
| -w------- (200) | -wx------ (300) | - | - | - | - | - | - | - | - |
| -w------- (200) | r-------- (400) | - | - | - | - | - | - | - | - |
| -w------- (200) | r-x------ (500) | - | - | - | - | - | - | - | - |
| -w------- (200) | rw------- (600) | - | - | - | - | - | - | - | - |
| -w------- (200) | rwx------ (700) | - | - | - | - | - | - | - | - |
| -wx------ (300) | --------- (000) | + | + | - | - | + | - | + | - |
| -wx------ (300) | --x------ (100) | + | + | - | - | + | - | + | - |
| -wx------ (300) | -w------- (200) | + | + | + | - | + | - | + | - |
| -wx------ (300) | -wx------ (300) | + | + | + | - | + | - | + | - |
| -wx------ (300) | r-------- (400) | + | + | - | + | + | - | + | + |
| -wx------ (300) | r-x------ (500) | + | + | - | + | + | - | + | + |
| -wx------ (300) | rw------- (600) | + | + | + | + | + | - | + | + |
| -wx------ (300) | rwx------ (700) | + | + | + | + | + | - | + | + |
| r-------- (400) | --------- (000) | - | - | - | - | - | + | - | - |
| r-------- (400) | --x------ (100) | - | - | - | - | - | + | - | - |
| r-------- (400) | -w------- (200) | - | - | - | - | - | + | - | - |
| r-------- (400) | -wx------ (300) | - | - | - | - | - | + | - | - |
| r-------- (400) | r-------- (400) | - | - | - | - | - | + | - | - |
| r-------- (400) | r-x------ (500) | - | - | - | - | - | + | - | - |
| r-------- (400) | rw------- (600) | - | - | - | - | - | + | - | - |
| r-------- (400) | rwx------ (700) | - | - | - | - | - | + | - | - |
| r-x------ (500) | --------- (000) | - | - | - | - | + | + | - | - |
| r-x------ (500) | --x------ (100) | - | - | - | - | + | + | - | - |
| r-x------ (500) | -w------- (200) | - | - | + | - | + | + | - | - |
| r-x------ (500) | -wx------ (300) | - | - | + | - | + | + | - | - |
| r-x------ (500) | r-------- (400) | - | - | - | + | + | + | - | + |
| r-x------ (500) | r-x------ (500) | - | - | - | + | + | + | - | + |
| r-x------ (500) | rw------- (600) | - | - | + | + | + | + | - | + |
| r-x------ (500) | rwx------ (700) | - | - | + | + | + | + | - | + |
| rw------- (600) | --------- (000) | - | - | - | - | - | + | - | - |
| rw------- (600) | --x------ (100) | - | - | - | - | - | + | - | - |
| rw------- (600) | -w------- (200) | - | - | - | - | - | + | - | - |
| rw------- (600) | -wx------ (300) | - | - | - | - | - | + | - | - |
| rw------- (600) | r-------- (400) | - | - | - | - | - | + | - | - |
| rw------- (600) | r-x------ (500) | - | - | - | - | - | + | - | - |
| rw------- (600) | rw------- (600) | - | - | - | - | - | + | - | - |
| rw------- (600) | rwx------ (700) | - | - | - | - | - | + | - | - |
| rwx------ (700) | --------- (000) | + | + | - | - | + | + | + | - |
| rwx------ (700) | --x------ (100) | + | + | - | - | + | + | + | - |
| rwx------ (700) | -w------- (200) | + | + | + | - | + | + | + | - |
| rwx------ (700) | -wx------ (300) | + | + | + | - | + | + | + | - |
| rwx------ (700) | r-------- (400) | + | + | - | + | + | + | + | + |
| rwx------ (700) | r-x------ (500) | + | + | - | + | + | + | + | + |
| rwx------ (700) | rw------- (600) | + | + | + | + | + | + | + | + |
| rwx------ (700) | rwx------ (700) | + | + | + | + | + | + | + | + |

1. На основании заполненной таблицы определил те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполнил таблицу.

Table 2: 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) | -r——–(400) |
| Запись в файл | d–x——(100) | –w——-(200) |
| Переименование файла | d-wx——(300) | ———-(000) |
| Создание поддиректории | d-wx——(300) | ———-(000) |
| Удаление поддиректории | d-wx——(300) | ———-(000) |

# 5 Выводы

В данной лабораторной работе мне успешно удалось получить практические навыки работы в консоли с атрибутами файлов, закрепить теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

# Список литературы

1. Права в Linux (chown, chmod, SUID, GUID, sticky bit, ACL, umask) [Электронный ресурс]. 2023. URL: <https://habr.com/ru/articles/469667/>.

2. Права доступа к файлам и каталогам [Электронный ресурс]. 2023. URL: <https://younglinux.info/bash/rwx>.

3. Права доступа к файлам в Linux [Электронный ресурс]. 2023. URL: <https://losst.pro/prava-dostupa-k-fajlam-v-linux>.

4. Права доступа к файлам [Электронный ресурс]. 2023. URL: <https://docs.altlinux.org/ru-RU/archive/2.3/html-single/junior/alt-docs-extras-linuxnovice/ch02s08.html>.