Лабораторная работа №3

Дисциплина: Информационная безопасность

Боровикова Карина Владимировна

Содержание

# 1 Цель работы

Получение практических навыков работы в консоли с атрибутами файлов для групп пользователей, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

# 2 Задание

* Произвести работу в консоли с атрибутами файлов для групп пользователей от имени пользователя *guest* и *guest2*;
* Сотавить опытным путем таблицы “Установленные права и разрешенные действия” и “Минимальные права для совершения операций”.

# 3 Теоретическое введение

В данной лабораторной работе нам предстоит поработать с правами доступа файлов и директорий. **Права доступа** определяют, какие действия конкретный пользователь может или не может совершать с определенным файлами и каталогами.

Есть 3 вида разрешений. Они определяют права пользователя на 3 действия: чтение, запись и выполнение. В Linux эти действия обозначаются вот так:

* **r** — read (чтение) — право просматривать содержимое файла;
* **w** — write (запись) — право изменять содержимое файла;
* **x** — execute (выполнение) — право запускать файл, если это программа или скрипт.

У каждого файла есть 3 группы пользователей, для которых можно устанавливать права доступа.

* **owner** (владелец) — отдельный человек, который владеет файлом. Обычно это тот, кто создал файл, но владельцем можно сделать и кого-то другого.
* **group** (группа) — пользователи с общими заданными правами.
* **others** (другие) — все остальные пользователи, не относящиеся к группе и не являющиеся владельцами.[**01?**]

Чтобы увидеть текущие назначения владельца, вы можете использовать команду ls -l. Эта команда показывает пользователя и группу-владельца.

С помощью команды ls вы можете отобразить владельца файлов в данном каталоге. Иногда может оказаться полезным получить список всех файлов в системе, в которых в качестве владельца указан данный пользователь или группа. Для этого вы можете использовать find. Аргумент find -user может быть использован для этой цели.

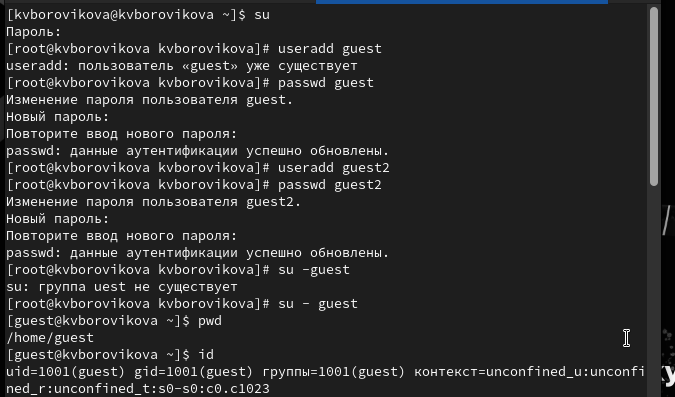
Чтобы применить соответствующие разрешения, первое, что нужно учитывать, это владение. Для этого есть команда chown.[**02?**]

Для того, чтобы позволить обычным пользователям выполнять программы от имени суперпользователя без знания его пароля была придумана такая вещь, как SUID и SGID биты. Рассмотрим эти полномочия подробнее.

* **SUID** - если этот бит установлен, то при выполнении программы, id пользователя, от которого она запущена заменяется на id владельца файла. Фактически, это позволяет обычным пользователям запускать программы от имени суперпользователя;
* **SGID** - этот флаг работает аналогичным образом, только разница в том, что пользователь считается членом группы, с которой связан файл, а не групп, к которым он действительно принадлежит. Если SGID флаг установлен на каталог, все файлы, созданные в нем, будут связаны с группой каталога, а не пользователя. Такое поведение используется для организации общих папок;
* **Sticky-bit** - этот бит тоже используется для создания общих папок. Если он установлен, то пользователи могут только создавать, читать и выполнять файлы, но не могут удалять файлы, принадлежащие другим пользователям.

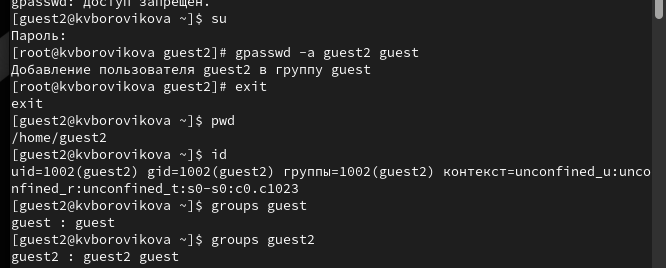
# 4 Выполнение лабораторной работы

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



Создание учетной записи guest

1. Зададим пароль для пользователя guest (использую учётную запись администратора) (рис. ??): passwd guest.
2. Аналогично создадим второго пользователя guest2. (рис. ??): useradd guest2, passwd guest
3. Добавим пользователя guest2 в группу guest: (рис. ??) `gpasswd -a guest2 guest



Добавление пользователя guest2 в группу guest

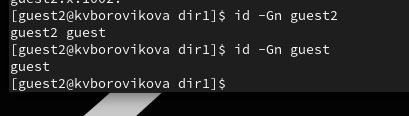
1. Осуществим вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли. (рис. ?? - ??) su - guest, su - guest2
2. Определим директорию, в которой находимся, командой pwd(рис. ?? - ??). Сравним её с приглашением командной строки. В командной строке видим символ ~, что свидетельствует о том, что **мы находимся в своей домашней директории.**
3. Уточним имя пользователя, его группу, а также группы, куда входит пользователь, командой id (рис. ?? - ??).

Видим следующие данные для пользователя guest: uid = 1001(guest), gid = 1001(guest), groups = 1001(guest).

Видим следующие данные для пользователя guest2: uid = 1002(guest2), gid = 1002(guest), groups = 1002(guest2).

Определите командами groups guest и groups guest2 (рис. ??), в какие группы входят пользователи guest и guest2. Сравните вывод команды groups с выводом команд id -Gn и id -G.

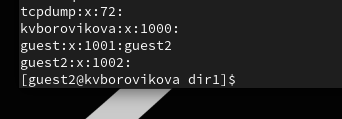
Видим, что информация для groups guest и groups guest2 совпадает с действительностью, для пользователя guest группа guest, для пользователя guest2 группы guest и guest2, так как мы этого пользователя добавили в группу guest. Аналогично, совпадает и для команд id -Gn и id -G. (рис. ?? - ??)



Проверка групп для пользователей guest и guest2

1. Сравним полученную информацию с содержимым файла /etc/group. Просмотрите файл командой

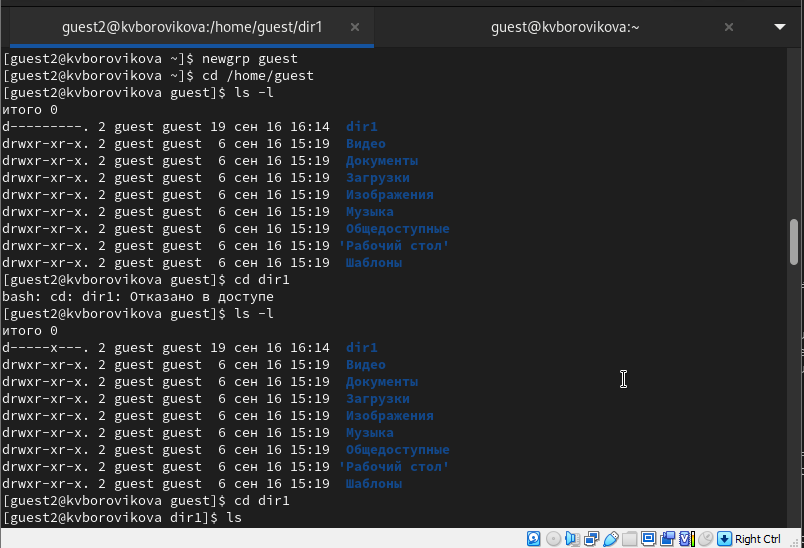
cat /etc/group



Файл /etc/group

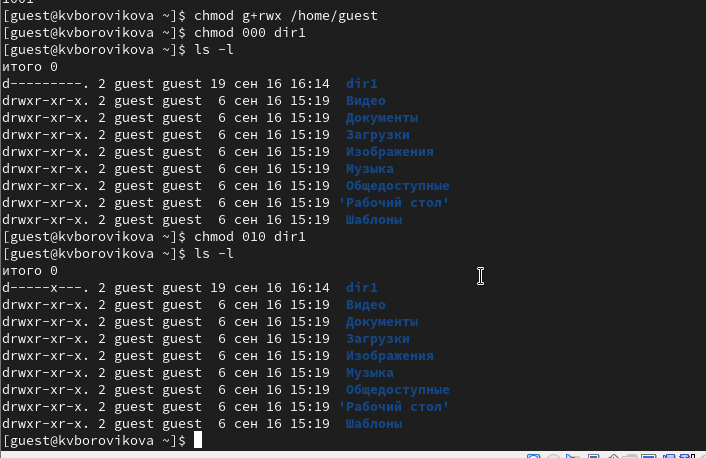
Найдем в нем последние 2 записи - записи о пользователях guest и guest2. Данные строки показывают, что для guest gid = 1001 и guest2, что соответствует результатам предыдущих команд.

1. От имени пользователя guest2 выполним регистрацию пользователя guest2 в группе guest командой newgrp guest (рис. ??)



регистрация пользователя guest2 в группе guest

1. От имени пользователя guest изменим права директории /home/guest, разрешив все действия для пользователей группы: chmod g+rwx /home/guest (рис. ??)



Изменяем права директории разрешив все действия для пользователей группы

1. От имени пользователя guest снимем с директории /home/guest/dir1 все атрибуты командой chmod 000 dirl и проверим правильность снятия атрибутов. (рис. ??)

Видим, что теперь на директорию dir1 нет никаких прав.

1. Заполните 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, занесите в таблицу знак «+», если не разрешена, знак «-».

Для опрделения опытным путем будем использовать следующие действияв соответствие со столбцами таблицы:

* cd dir1 - смена директории;
* touch <новый\_файл> - создание файла;
* rm <новый\_файл> - удаление файла;
* ls -l (dir1) - просмотр файлов в директории;
* echo "test" > <файл\_с\_установленными\_правами> - запись в файл;
* cat <файл\_с\_установленными\_правами> - чтение файла;
* mv <файл\_с\_установленными\_правами> <переименование> - переименование файла;
* chattr <атрибуты> <файл\_с\_установленными\_правами> смена атрибутов файла.

Остальные действия можно найти в видеозаписи к лабораторной работе.

Заполненная табл. [1](#tbl:01) краткого описания стандартных каталогов Unix.

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------ (010) | - | - | - | - | - | - | - | - |
| --------- (000) | -w------- (020) | - | - | - | - | - | - | - | - |
| --------- (000) | -wx------ (030) | - | - | - | - | - | - | - | - |
| --------- (000) | r-------- (040) | - | - | - | - | - | - | - | - |
| --------- (000) | r-x------ (050) | - | - | - | - | - | - | - | - |
| --------- (000) | rw------- (060) | - | - | - | - | - | - | - | - |
| --------- (000) | rwx------ (070) | - | - | - | - | - | - | - | - |
| --x------ (010) | --x------ (010) | - | - | - | - | + | - | - | - |
| --x------ (010) | -w------- (020) | - | - | + | - | + | - | - | - |
| --x------ (010) | -wx------ (030) | - | - | + | - | + | - | - | - |
| --x------ (010) | r-------- (040) | - | - | - | + | + | - | - | + |
| --x------ (010) | r-x------ (050) | - | - | - | + | + | - | - | + |
| --x------ (010) | rw------- (060) | - | - | + | + | + | - | - | + |
| --x------ (010) | rwx------ (070) | - | - | + | + | + | - | - | + |
| --x------ (010) | --------- (000) | - | - | - | - | + | - | - | - |
| -w------- (020) | --------- (000) | - | - | - | - | - | - | - | - |
| -w------- (020) | --x------ (010) | - | - | - | - | - | - | - | - |
| -w------- (020) | -w------- (020) | - | - | - | - | - | - | - | - |
| -w------- (020) | -wx------ (030) | - | - | - | - | - | - | - | - |
| -w------- (020) | r-------- (040) | - | - | - | - | - | - | - | - |
| -w------- (020) | r-x------ (050) | - | - | - | - | - | - | - | - |
| -w------- (020) | rw------- (060) | - | - | - | - | - | - | - | - |
| -w------- (020) | rwx------ (070) | - | - | - | - | - | - | - | - |
| -wx------ (030) | --------- (000) | + | + | - | - | + | - | + | - |
| -wx------ (030) | --x------ (010) | + | + | - | - | + | - | + | - |
| -wx------ (030) | -w------- (020) | + | + | + | - | + | - | + | - |
| -wx------ (030) | -wx------ (030) | + | + | + | - | + | - | + | - |
| -wx------ (030) | r-------- (040) | + | + | - | + | + | - | + | + |
| -wx------ (030) | r-x------ (050) | + | + | - | + | + | - | + | + |
| -wx------ (030) | rw------- (060) | + | + | + | + | + | - | + | + |
| -wx------ (030) | rwx------ (070) | + | + | + | + | + | - | + | + |
| r-------- (040) | --------- (000) | - | - | - | - | - | + | - | - |
| r-------- (040) | --x------ (010) | - | - | - | - | - | + | - | - |
| r-------- (040) | -w------- (020) | - | - | - | - | - | + | - | - |
| r-------- (040) | -wx------ (030) | - | - | - | - | - | + | - | - |
| r-------- (040) | r-------- (040) | - | - | - | - | - | + | - | - |
| r-------- (040) | r-x------ (050) | - | - | - | - | - | + | - | - |
| r-------- (040) | rw------- (060) | - | - | - | - | - | + | - | - |
| r-------- (040) | rwx------ (070) | - | - | - | - | - | + | - | - |
| r-x------ (050) | --------- (000) | - | - | - | - | + | + | - | - |
| r-x------ (050) | --x------ (010) | - | - | - | - | + | + | - | - |
| r-x------ (050) | -w------- (020) | - | - | + | - | + | + | - | - |
| r-x------ (050) | -wx------ (030) | - | - | + | - | + | + | - | - |
| r-x------ (050) | r-------- (040) | - | - | - | + | + | + | - | + |
| r-x------ (050) | r-x------ (050) | - | - | - | + | + | + | - | + |
| r-x------ (050) | rw------- (060) | - | - | + | + | + | + | - | + |
| r-x------ (050) | rwx------ (070) | - | - | + | + | + | + | - | + |
| rw------- (060) | --------- (000) | - | - | - | - | - | + | - | - |
| rw------- (060) | --x------ (010) | - | - | - | - | - | + | - | - |
| rw------- (060) | -w------- (020) | - | - | - | - | - | + | - | - |
| rw------- (060) | -wx------ (030) | - | - | - | - | - | + | - | - |
| rw------- (060) | r-------- (040) | - | - | - | - | - | + | - | - |
| rw------- (060) | r-x------ (050) | - | - | - | - | - | + | - | - |
| rw------- (060) | rw------- (060) | - | - | - | - | - | + | - | - |
| rw------- (060) | rwx------ (070) | - | - | - | - | - | + | - | - |
| rwx------ (070) | --------- (000) | + | + | - | - | + | + | + | - |
| rwx------ (070) | --x------ (010) | + | + | - | - | + | + | + | - |
| rwx------ (070) | -w------- (020) | + | + | + | - | + | + | + | - |
| rwx------ (070) | -wx------ (030) | + | + | + | - | + | + | + | - |
| rwx------ (070) | r-------- (040) | + | + | - | + | + | + | + | + |
| rwx------ (070) | r-x------ (050) | + | + | - | + | + | + | + | + |
| rwx------ (070) | rw------- (060) | + | + | + | + | + | + | + | + |
| rwx------ (070) | rwx------ (070) | + | + | + | + | + | + | + | + |

1. На основании заполненной таблицы [1](#tbl:01) определите те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполните табл. [2](#tbl:02).

Table 2: Минимальные права для совершения операций

| Операция | Минимальные права на директорию | Минимальные права на файл |
| --- | --- | --- |
| Создание файла | d-wx——(030) | ———-(000) |
| Удаление файла | d-wx——(030) | ———-(000) |
| Чтение файла | d–x——(010) | -r——–(040) |
| Запись в файл | d–x——(010) | –w——-(020) |
| Переименование файла | d-wx——(030) | ———-(000) |
| Создание поддиректории | d-wx——(030) | ———-(000) |
| Удаление поддиректории | d-wx——(030) | ———-(000) |

# 5 Выводы

Получила практические навыки работы в консоли с атрибутами файлов для групп пользователей, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux. Заполнила опытным путем таблицы “Установленные права и разрешенные действия” и “Минимальные права для совершения операций”.

# Список литературы