

Основы информационной безопасности

Лабораторная работа № 3. Дискреционное разграничение прав в Linux. Два пользователя

Сунгурова Мариян Мухсиновна

21 сентября 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Сунгкрова Мариян М.
- Студентка группы НКНбд-01-21

Вводная часть

Получение практических навыков работы в консоли с атрибутами файлов для групп пользователей.

При работе с командой `chmod` важно понимать основные права доступа, которые назначают файлам или каталогам. В Linux используется три основных типа прав доступа:

- Чтение (Read) — обозначается буквой «r». Предоставляет возможность просматривать содержимое файла или каталога.
- Запись (Write) — обозначается буквой «w». Позволяет создавать, изменять и удалять файлы внутри каталога, а также изменять содержимое файла.
- Выполнение (Execute) — обозначается буквой «x». Дает разрешение на выполнение файла или на вход в каталог.

Каждый из указанных выше типов прав доступа может быть назначен трем группам пользователей:

- Владелец (Owner) — пользователь, который является владельцем файла или каталога.
- Группа (Group) — группа пользователей, к которой принадлежит файл или каталог.
- Остальные пользователи (Others) — все остальные пользователи системы.

Комбинация этих базовых прав доступа для каждой из групп пользователей определяет полный набор прав доступа для файла или каталога.

Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы ОС создадим учетную запись пользователя guest2 и добавляем его в группу guest (рис. (fig:001?) – (fig:002?))

```
[mmsungurova@mmsungurova ~]$ sudo useradd guest2
[sudo] пароль для mmsungurova:
[mmsungurova@mmsungurova ~]$ passwd guest2
passwd: только root может выбрать имя учетной записи.
[mmsungurova@mmsungurova ~]$ sudo passwd guest2
Изменение пароля пользователя guest2.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[mmsungurova@mmsungurova ~]$
```

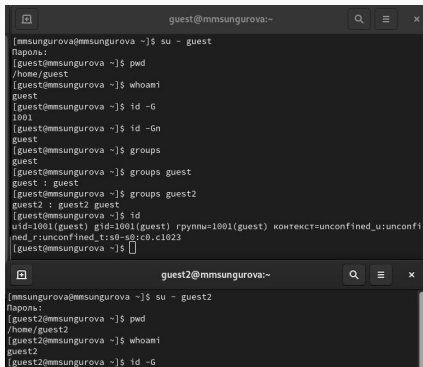
Рис. 1: Создание нового пользователя guest2 и добавление его в группу guest

```
[mmsungurova@mmsungurova ~]$ sudo gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
[mmsungurova@mmsungurova ~]$
```

Рис. 2: Создание нового пользователя guest2 и добавление его в группу guest

2. Осуществим вход в систему от двух пользователей на двух разных консолях: `guest` на первой консоли и `guest2` на второй консоли. Далее для обоих пользователей командой `pwd` определим директорию, в которой находимся. Увидим, что она совпадает с приглашениями командной строки. Увидим, что `guest` принадлежит одной группе `guet` с `id 2001`, а двум группам `guest` и `guest2` с `id 1001` и `1002`. С помощью команд `id -Gn` и `id -G` можно увидеть только `id` существующих групп и название соответственно

3. Уточним имя пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам. Определите командами `groups guest` и `groups guest2`, в какие группы входят пользователи `guest` и `guest2`. Увидим, что `guest` принадлежит одной группе `guet` с `ig 2001`, а двум группам `guest` и `guest2` с `id 1001` и `1002`. С помощью команд `id -Gn` и `id -G` можно увидеть только `id` существующих групп и название соответственно (рис. (fig:003?))



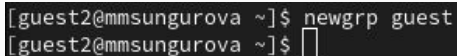
```
guest@mmsungurova:~  
[mmsungurova@mmsungurova ~]$ su - guest  
Пароль:  
[guest@mmsungurova ~]$ pwd  
/home/guest  
[guest@mmsungurova ~]$ whoami  
guest  
[guest@mmsungurova ~]$ id -G  
1001  
[guest@mmsungurova ~]$ id -Gn  
guest  
[guest@mmsungurova ~]$ groups  
guest  
[guest@mmsungurova ~]$ groups guest  
guest : guest  
[guest@mmsungurova ~]$ groups guest2  
guest2 : guest2 guest  
[guest@mmsungurova ~]$ id  
uid=1001(guest) gid=1001(guest) rpynu=1001(guest) контекст=unconfined_u:unconfi  
ned_r:unconfined_t:s0-s0:c0.c1023  
[guest@mmsungurova ~]$  
  
guest2@mmsungurova:~  
[mmsungurova@mmsungurova ~]$ su - guest2  
Пароль:  
[guest2@mmsungurova ~]$ pwd  
/home/guest2  
[guest2@mmsungurova ~]$ whoami  
guest2  
[guest2@mmsungurova ~]$ id -G
```

4. Сравним полученную информацию с содержимым файла `/etc/group`, просмотрев файл командой `cat /etc/group`

```
[guest2@mmsungurova ~]$ cat /etc/group | grep guest  
guest:x:1001:guest2  
guest2:x:1002:  
[guest2@mmsungurova ~]$
```

Рис. 4: Создание нового пользователя guest2 и добавление его в группу guest

5. От имени пользователя guest2 выполним регистрацию пользователя guest2 в группе guest командой `newgrp guest`



```
[guest2@mmsungurova ~]$ newgrp guest  
[guest2@mmsungurova ~]$
```

Рис. 5: Создание нового пользователя guest2 и добавление его в группу guest

6. От имени пользователя guest изменим права директории /home/guest, разрешив все действия для пользователей группы: `chmod g+rwx /home/guest`

```
[guest@mmsungurova ~]$ chmod 000 dir1
[guest@mmsungurova ~]$ ls -l dir1
ls: невозможно открыть каталог 'dir1': Отказано в доступе
[guest@mmsungurova ~]$ ls -l
итого 0
d----- . 2 guest guest 6 сен 11 21:14 dir1
[guest@mmsungurova ~]$
```

Рис. 6: Создание нового пользователя guest2 и добавление его в группу guest

В табл. 1 в отчете приведены данные о том, какие операции разрешены, а какие нет для владельца данных.

В табл. (tbl:tbl2?) приведены данные о том, какие минимальные права должны быть для совершения различных действий.

Таблица 1: Минимальные права для совершения операций {#tbl:tbl2}

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d(030)	(000)
Удаление файла	d(030)	(000)
Чтение файла	d(010)	(040)
Запись в файл	d(010)	(020)
Переименование файла	d(030)	(000)
Создание поддиректории	d(030)	(000)
Удаление поддиректории	d(030)	(000)

При сравнении с таблицей в лабораторной работе №2 можно увидеть, что отличие состоит только в том, что не владелец файла никогда не имеет прав на изменение его атрибутов. Менять права может владелец файла или администратор. Члены группы файла никаких особых прав на inode не имеют. Пользователь может отобрать у себя собственные права на чтение и запись в файл, но право на запись в inode (в т.ч. право на смену прав) сохраняется у владельца файла при любых обстоятельствах. Пользователь не может передать право собственности на файл другому пользователю и не может забрать право собственности на файл у другого пользователя.

Выводы

В результате выполнения данной лабораторной работы были получены практические навыки работы в консоли с атрибутами файлов для групп пользователей.