

Лабораторная работа №2.

Дискреционное разграничение прав в Linux. Основные атрибуты

Радикорский Павел Михайлович НФИбд-03-18

02.10.2021

RUDN University, Moscow, Russian Federation

Цели и задачи

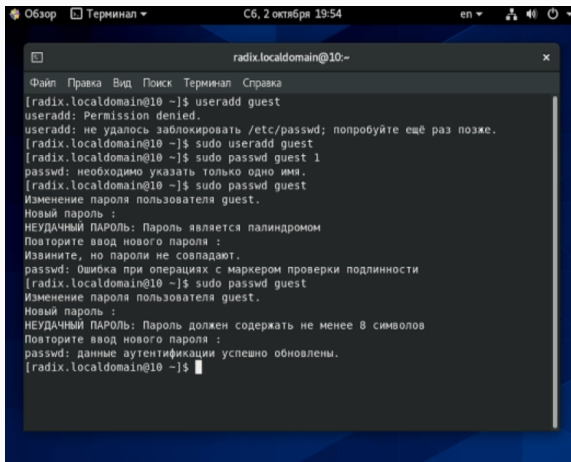
Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux

Лабораторная работа подразумевает создание гостевого пользователя, изменение и анализ прав на папки и файлы.

Выполнение

Процесс выполнения

В установленной при выполнении предыдущей лабораторной работы операционной системе создаём учётную запись пользователя guest, задаём пароль

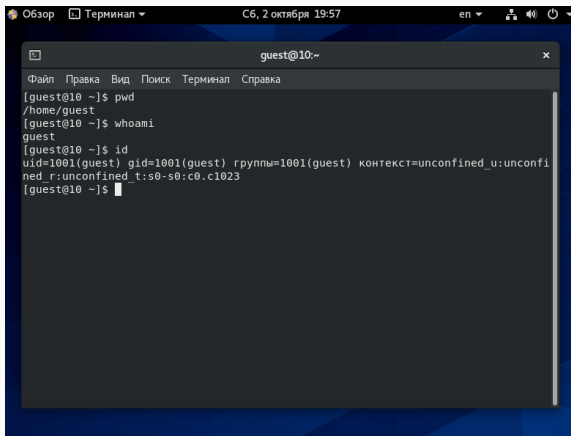


```
Обзор Терминал C6, 2 октября 19:54 en
```

```
radix.localdomain@10:~  
Файл Правка Вид Поиск Терминал Справка  
[radix.localdomain@10 ~]$ useradd guest  
useradd: Permission denied.  
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.  
[radix.localdomain@10 ~]$ sudo useradd guest  
[radix.localdomain@10 ~]$ sudo passwd guest 1  
passwd: необходимо указать только одно имя.  
[radix.localdomain@10 ~]$ sudo passwd guest  
Изменение пароля пользователя guest.  
Новый пароль :  
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом  
Повторите ввод нового пароля :  
Извините, но пароли не совпадают.  
passwd: Ошибка при операциях с маркером проверки подлинности  
[radix.localdomain@10 ~]$ sudo passwd guest  
Изменение пароля пользователя guest.  
Новый пароль :  
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов  
Повторите ввод нового пароля :  
passwd: данные аутентификации успешно обновлены.  
[radix.localdomain@10 ~]$
```

Процесс выполнения

Входим в систему через пользователя guest, проверяем директорию и уточняем имя пользователя. При сравнении группы получаем совпадение

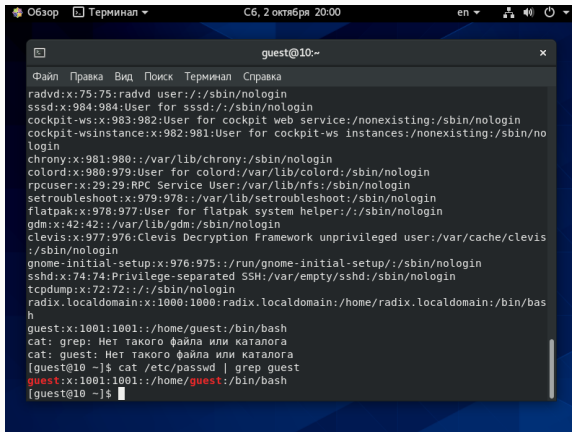


```
Обзор Терминал С6, 2 октября 19:57 en
```

```
guest@10:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@10 ~]$ pwd  
/home/guest  
[guest@10 ~]$ whoami  
guest  
[guest@10 ~]$ id  
uid=1001(guest) gid=1001(guest) rpyппы=1001(guest) контекст=unconfined_u:unconfi  
ned_r:unconfined_t:s0-s0:c0.c1023  
[guest@10 ~]$
```

Процесс выполнения

Просматриваем файл `/etc/passwd`, находим свою учётную запись, при сравнении `uid` и `gid` получаем совпадение

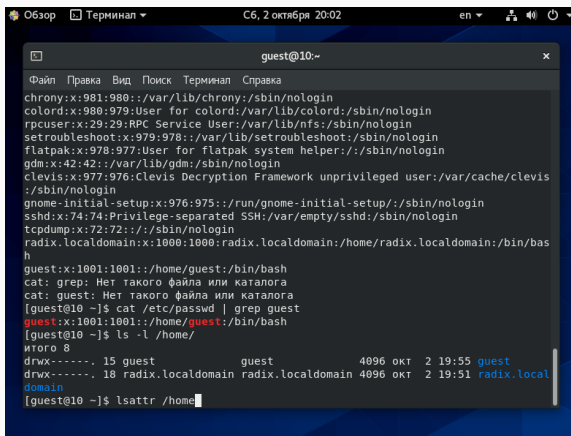


```
Обзор Терминал C6, 2 октября 20:00 en
guest@10:~
Файл Правка Вид Поиск Терминал Справка
radvd:x:75:75:radvd user:/sbin/nologin
sssd:x:984:984:User for sssd:/sbin/nologin
cockpit-ws:x:983:982:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:982:981:User for cockpit-ws instances:/nonexisting:/sbin/nologin
chrony:x:981:980:./var/lib/chrony:/sbin/nologin
colord:x:980:979:User for colord:/var/lib/colord:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
setroubleshoot:x:979:978:./var/lib/setroubleshoot:/sbin/nologin
flatpak:x:978:977:User for flatpak system helper:/sbin/nologin
gdm:x:42:42:./var/lib/gdm:/sbin/nologin
clevis:x:977:976:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/sbin/nologin
gnome-initial-setup:x:976:975:./run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72:./:/sbin/nologin
radix.localdomain:x:1000:1000:radix.localdomain:/home/radix.localdomain:/bin/bash
h
guest:x:1001:1001:~/home/guest:/bin/bash
cat: grep: Нет такого файла или каталога
cat: guest: Нет такого файла или каталога
[guest@10 ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001:~/home/guest:/bin/bash
[guest@10 ~]$
```

Рис. 3: `/etc/passwd`

Процесс выполнения

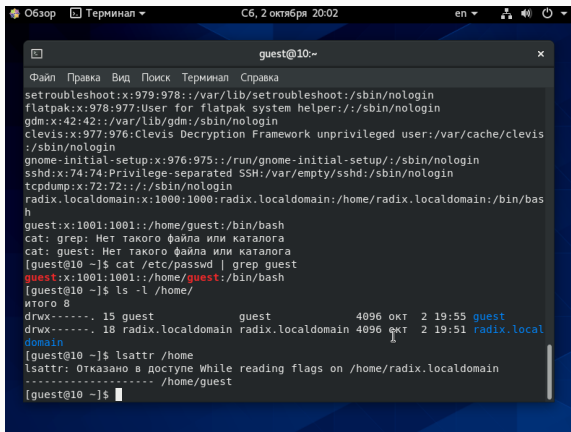
Определили существующие в системе директории. Удалось получить список, в котором полные права на доступ есть только у владельцев поддиректорий



```
guest@10:~  
Файл Правка Вид Поиск Терминал Справка  
chrony:x:981:980:./var/lib/chrony:/sbin/nologin  
colord:x:980:979:User for colord:/var/lib/colord:/sbin/nologin  
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin  
setroubleshoot:x:979:978:./var/lib/setroubleshoot:/sbin/nologin  
flatpak:x:978:977:User for flatpak system helper:/sbin/nologin  
gdm:x:42:42:./var/lib/gdm:/sbin/nologin  
clevis:x:977:976:Clevis Decryption Framework unprivileged user:/var/cache/levis  
:/sbin/nologin  
gnome-initial-setup:x:976:975:./run/gnome-initial-setup:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin  
tcpdump:x:72:72:./sbin/nologin  
radix.localdomain:x:1000:1000:radix.localdomain:/home/radix.localdomain:/bin/bas  
h  
guest:x:1001:1001:./home/guest:/bin/bash  
cat: grep: Нет такого файла или каталога  
cat: guest: Нет такого файла или каталога  
[guest@10 ~]$ cat /etc/passwd | grep guest  
guest:x:1001:1001:./home/guest:/bin/bash  
[guest@10 ~]$ ls -l /home/  
итого 8  
drwx-----, 15 guest          guest          4096 окт  2 19:55 guest  
drwx-----, 18 radix.localdomain radix.localdomain 4096 окт  2 19:51 radix.local  
domain  
[guest@10 ~]$ lsattr /home/
```

Процесс выполнения

Проверяем расширенные атрибуты. Получаем, что мы видим расширенные атрибуты только своей директории, но не остальных пользователей



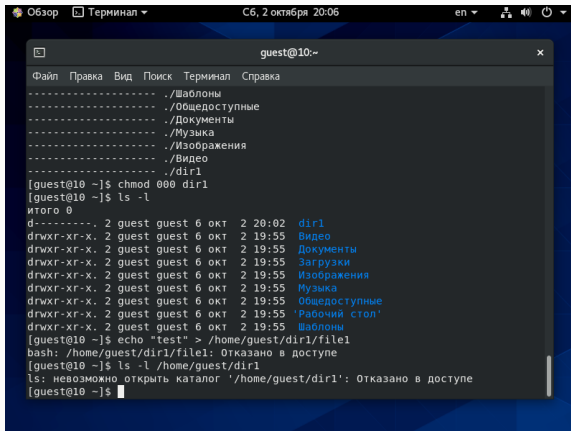
The screenshot shows a terminal window titled "guest@10:~" with a menu bar (Файл, Правка, Вид, Поиск, Терминал, Справка) and a status bar (Обзор, Терминал, C6, 2 октября 20:02, en, and system icons). The terminal output lists system users and their home directories, followed by a search for the 'guest' user in the password file, and then a directory listing and attribute check for the '/home' directory.

```
setroubleshoot:x:979:978::/var/lib/setroubleshoot:/sbin/nologin
flatpak:x:978:977:User for flatpak system helper:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
clevis:x:977:976:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/sbin/nologin
gnome-initial-setup:x:976:975::/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72::/sbin/nologin
radix.localdomain:x:1000:1000:radix.localdomain:/home/radix.localdomain:/bin/bash
h
guest:x:1001:1001::/home/guest:/bin/bash
cat: grep: Нет такого файла или каталога
cat: guest: Нет такого файла или каталога
[guest@10 ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001::/home/guest:/bin/bash
[guest@10 ~]$ ls -l /home/
итого 8
drwx----- 15 guest          guest          4096 окт  2 19:55 guest
drwx----- 18 radix.localdomain radix.localdomain 4096 окт  2 19:51 radix.localdomain
[guest@10 ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/radix.localdomain
----- /home/guest
[guest@10 ~]$
```

Рис. 5: Расширенные атрибуты

Процесс выполнения

Создали директорию dir1, сняли с директории все атрибуты. Проверили правильность выполнения команды

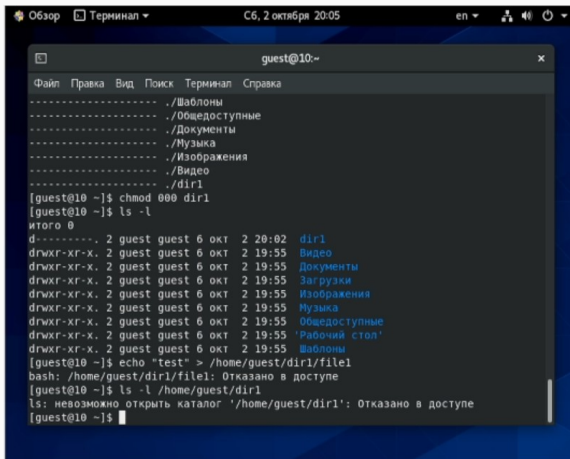


```
Обзор Терминал Сб, 2 октября 20:06 en [system icons]
guest@10:~
Файл Правка Вид Поиск Терминал Справка
-----
./Шаблоны
./Общедоступные
./Документы
./Музыка
./Изображения
./Видео
./dir1
[guest@10 ~]$ chmod 000 dir1
[guest@10 ~]$ ls -l
итого 0
d----- 2 guest guest 6 окт 2 20:02 dir1
drwxr-xr-x 2 guest guest 6 окт 2 19:55 Видео
drwxr-xr-x 2 guest guest 6 окт 2 19:55 Документы
drwxr-xr-x 2 guest guest 6 окт 2 19:55 Загрузки
drwxr-xr-x 2 guest guest 6 окт 2 19:55 Изображения
drwxr-xr-x 2 guest guest 6 окт 2 19:55 Музыка
drwxr-xr-x 2 guest guest 6 окт 2 19:55 Общедоступные
drwxr-xr-x 2 guest guest 6 окт 2 19:55 'Рабочий стол'
drwxr-xr-x 2 guest guest 6 окт 2 19:55 Шаблоны
[guest@10 ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@10 ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе
[guest@10 ~]$
```

Рис. 6: dir1

Процесс выполнения

Попытались создать в dir1 файл, получили отказ, связанный с отсутствием прав. То же самое произошло при попытке проверки наличия файлов в dir1.



```
Обзор Терминал Сб, 2 октября 20:05 en
```

```
guest@10:~  
Файл Правка Вид Поиск Терминал Справка  
-----  
./Шаблоны  
./Общедоступные  
./Документы  
./Музыка  
./Изображения  
./Видео  
./dir1  
[guest@10 ~]$ chmod 000 dir1  
[guest@10 ~]$ ls -l  
итого 0  
d-----, 2 guest guest 6 окт 2 20:02 dir1  
drwxr-xr-x, 2 guest guest 6 окт 2 19:55 Видео  
drwxr-xr-x, 2 guest guest 6 окт 2 19:55 Документы  
drwxr-xr-x, 2 guest guest 6 окт 2 19:55 Загрузки  
drwxr-xr-x, 2 guest guest 6 окт 2 19:55 Изображения  
drwxr-xr-x, 2 guest guest 6 окт 2 19:55 Музыка  
drwxr-xr-x, 2 guest guest 6 окт 2 19:55 Öffentlich  
drwxr-xr-x, 2 guest guest 6 окт 2 19:55 'Рабочий стол'  
drwxr-xr-x, 2 guest guest 6 окт 2 19:55 Шаблоны  
[guest@10 ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@10 ~]$ ls -l /home/guest/dir1  
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе  
[guest@10 ~]$
```

Процесс выполнения

Заполнили таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет

Права директории	Полна файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
d(000)	d(000)	+	+	+	+	+	+	+	+
d x(100)	d(000)	+	+	+	+	+	+	+	+
d w(200)	d(000)	+	+	+	+	+	+	+	+
d wx(300)	d(000)	+	+	+	+	+	+	+	+
dr (400)	d(000)	+	+	+	+	+	+	+	+
dr x(500)	d(000)	+	+	+	+	+	+	+	+
dwx (600)	d(000)	+	+	+	+	+	+	+	+
dwxw(700)	d(000)	+	+	+	+	+	+	+	+
d(000)	d x(100)	+	+	+	+	+	+	+	+
d x(100)	d x(100)	+	+	+	+	+	+	+	+
d w(200)	d x(100)	+	+	+	+	+	+	+	+
d wx(300)	d x(100)	+	+	+	+	+	+	+	+
dr (400)	d x(100)	+	+	+	+	+	+	+	+
dr x(500)	d x(100)	+	+	+	+	+	+	+	+
dwx (600)	d x(100)	+	+	+	+	+	+	+	+
dwxw(700)	d x(100)	+	+	+	+	+	+	+	+
d(000)	d w(200)	+	+	+	+	+	+	+	+
d x(100)	d w(200)	+	+	+	+	+	+	+	+
d w(200)	d w(200)	+	+	+	+	+	+	+	+
d wx(300)	d w(200)	+	+	+	+	+	+	+	+
dr (400)	d w(200)	+	+	+	+	+	+	+	+
dr x(500)	d w(200)	+	+	+	+	+	+	+	+
dwx (600)	d w(200)	+	+	+	+	+	+	+	+
dwxw(700)	d w(200)	+	+	+	+	+	+	+	+
d(000)	d wx(300)	+	+	+	+	+	+	+	+
d x(100)	d wx(300)	+	+	+	+	+	+	+	+
d w(200)	d wx(300)	+	+	+	+	+	+	+	+
d wx(300)	d wx(300)	+	+	+	+	+	+	+	+
dr (400)	d wx(300)	+	+	+	+	+	+	+	+
dr x(500)	d wx(300)	+	+	+	+	+	+	+	+
dwx (600)	d wx(300)	+	+	+	+	+	+	+	+
dwxw(700)	d wx(300)	+	+	+	+	+	+	+	+
d(000)	dr (400)	+	+	+	+	+	+	+	+
d x(100)	dr (400)	+	+	+	+	+	+	+	+
d w(200)	dr (400)	+	+	+	+	+	+	+	+
d wx(300)	dr (400)	+	+	+	+	+	+	+	+
dr (400)	dr (400)	+	+	+	+	+	+	+	+
dr x(500)	dr (400)	+	+	+	+	+	+	+	+
dwx (600)	dr (400)	+	+	+	+	+	+	+	+
dwxw(700)	dr (400)	+	+	+	+	+	+	+	+
d(000)	dr x(500)	+	+	+	+	+	+	+	+
d x(100)	dr x(500)	+	+	+	+	+	+	+	+
d w(200)	dr x(500)	+	+	+	+	+	+	+	+
d wx(300)	dr x(500)	+	+	+	+	+	+	+	+

Процесс выполнения

На основании заполненной таблицы определили те или иные минимально необходимые права для выполнения операций внутри директории `dir1`

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	w	-
Удаление файла	w	-
Чтение файла	-	r
Запись в файл	-	w
Переименование файла	-	w
Создание поддиректории	x	-
Удаление поддиректории	x	-

Рис. 9: Права для выполнения операций

Выводы

На основании выполненной лабораторной работы были получены практические навыки работы в консоли по изменению атрибутов файлов и папок