

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты.

Кармацкий Н. С. Группа НФИбд-01-21

7 Сентября 2024

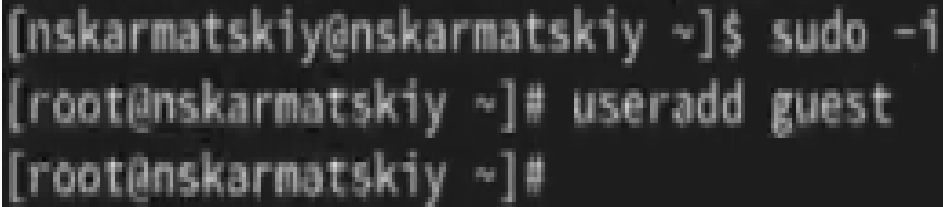
Российский университет дружбы народов, Москва, Россия

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

Теоретическая справка

Права доступа определяют, какие действия конкретный пользователь может или не может совершать с определенным файлами и каталогами. С помощью разрешений можно создать надежную среду — такую, в которой никто не может поменять содержимое ваших документов или повредить системные файлы. [2].

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создаем учётную запись пользователя guest



```
[nskarmatskiy@nskarmatskiy ~]$ sudo -i  
[root@nskarmatskiy ~]# useradd guest  
[root@nskarmatskiy ~]#
```

Рис. 1: (рис. 1. Новый пользователь guest)

2. Зададим пароль пользователя guest

```
[root@nskarmatskiy ~]# passwd guest
Изменение пароля пользователя guest.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом
Повторите ввод нового пароля:
Извините, но пароли не совпадают.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[root@nskarmatskiy ~]#
```

Рис. 2: (рис. 2. Установка пароля для пользовател guest)

3. Войдем в систему от имени пользователя guest

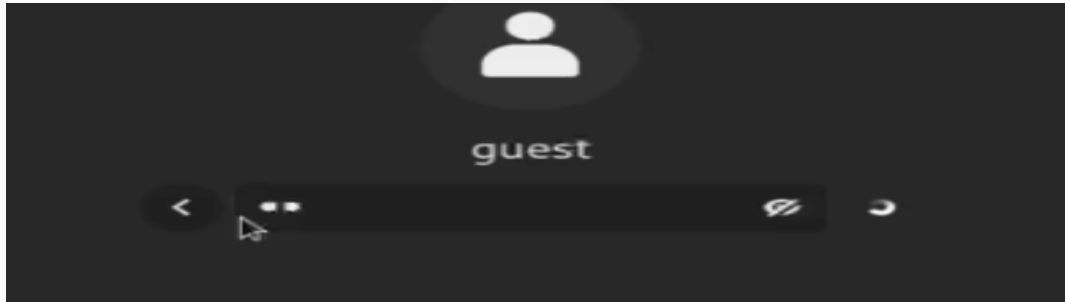


Рис. 3: (рис. 3. Вход в систему под новым пользователем)

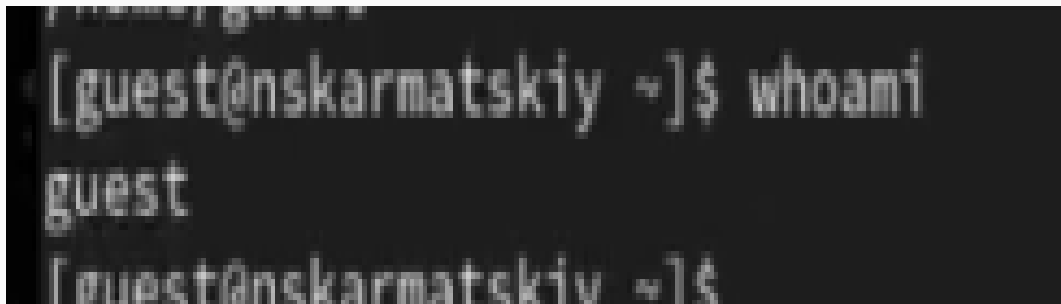
4. Определим директорию, в которой мы находимся с помощью команды `pwd`. Сравним и определим является ли она нашей домашней директорией

```
[guest@nskarmatskiy ~]$ pwd
/home/guest
[guest@nskarmatskiy ~]$ ls
Видео          Загрузки          Музыка          'Рабочий стол'
Документы      Изображения      Общедоступные  Шаблоны
[guest@nskarmatskiy ~]$ cd
[guest@nskarmatskiy ~]$ cd ~
[guest@nskarmatskiy ~]$ pwd
/home/guest
```

Рис. 4: (рис. 4. Определение директории)

Мы находимся в той же директории, что и наша домашняя

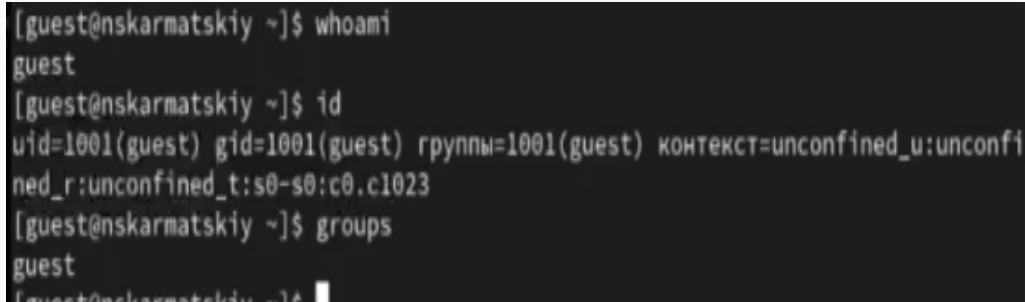
5. Уточним имя нашего пользователя командой `whoami`.

A terminal window with a black background and white text. The prompt is `[guest@nskarmatskiy ~]$`. The command `whoami` has been entered and executed, resulting in the output `guest`. The prompt `[guest@nskarmatskiy ~]$` is visible again on the next line.

```
[guest@nskarmatskiy ~]$ whoami
guest
[guest@nskarmatskiy ~]$
```

Рис. 5: (рис. 5. Уточнение имени нашего пользователя)

6. Уточним группу пользователя, а так же группы в которые входит он. Сравним вывод команды `id` с выводом команды `groups`



```
[guest@nskarmatskiy ~]$ whoami
guest
[guest@nskarmatskiy ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
[guest@nskarmatskiy ~]$ groups
guest
```

Рис. 6: (рис. 6. Уточнение группы пользователя)

Выводы двух команд идентичны, никаких разностей нет

7. Сравним полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки

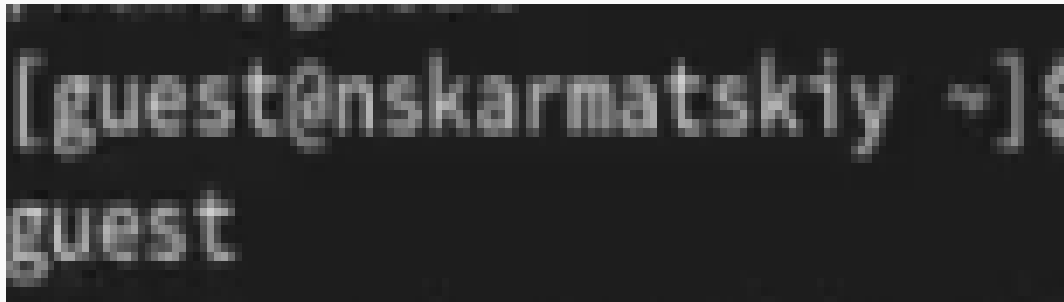
A terminal window with a black background and white text. The first line shows a shell prompt '[guest@nskarmatskiy ~]\$' followed by the command 'cat /etc/passwd'. The second line shows the output of the command, which is the line 'guest:x:1000:1000:guest:/home/guest:/bin/bash'.

Рис. 7: (рис. 7. Сравнение данных)

Все верно, данные одинаковы

8. Просмотрим файл `/etc/passwd` и найдем в нем свою учетную запись и `uid` пользователя. Так же определим `gid` пользователя. Сравним значения с вывод предыдущих пунктов



```
root@nskarmatskiy ~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
dbus:x:81:81:system message bus:/:/sbin/nologin
polkitd:x:998:996:User for polkitd:/:/sbin/nologin
avahi:x:70:70:Avahi MDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pipewire:x:997:994:PipeWire System Daemon:/run/pipewire:/usr/sbin/nologin
sssd:x:996:993:User for sssd:/:/sbin/nologin
libstoragemgmt:x:991:991:daemon account for libstoragemgmt:/:usr/sbin/nologin
taxix:x:99:59:Account used for TPM access:/:usr/sbin/nologin
geoclue:x:990:989:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:989:988:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-ws-instance:x:988:987:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:987:986:User for flatpak system helper:/:/sbin/nologin
colord:x:986:985:User for colord:/var/lib/colord:/sbin/nologin
setroubleshoot:x:985:984:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
clevvis:x:984:983:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
gdm:x:42:42:/:/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:983:982:/:run/gnome-initial-setup:/:/sbin/nologin
design:x:982:981:Group for the design signing daemon:/run/design:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
chrony:x:981:980:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:980:979:DNSmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
nskarmatskiy:x:1000:1000:nskarmatskiy:/home/nskarmatskiy:/bin/bash
guest:x:1001:1001:/:home/guest:/bin/bash
```

Рис. 8: (рис. 8. Просмотр файла `/etc/passwd`)

`gid: 1001` Значение с выводами предыдущих команд полностью идентичны

9. Определим существующие в системе директории командой. Проверим какие права установлены на директории

```
[guest@nskarmatskiy ~]$ ls -l /home/  
итого 8  
drwx-----, 14 guest      guest      4096 авг 31 19:38 guest  
drwx-----, 14 nskarmatskiy nskarmatskiy 4096 авг 31 19:00 nskarmatskiy
```

Рис. 9: (рис. 9. Права на директориях)

Права на директорию установлены только для пользователя, он может делать все в ней, для других пользователей(кроме root) действия с этим каталогом недоступны

10. Проверьте, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home

```
[guest@nskarmatskiy ~]$ ls -l
итого 0
drwxr-xr-x. 2 guest guest 6 авг 31 19:45 dir1
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Видео
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Документы
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Загрузки
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Изображения
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Музыка
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Общедоступные
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Шаблоны
```

Рис. 10: (рис. 10. Проверка прав)

10. Проверьте, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home

```
[guest@nskarmatskiy ~]$ lsattr
----- ./Рабочий стол
----- ./Загрузки
----- ./Шаблоны
----- ./Общедоступные
----- ./Документы
----- ./Музыка
----- ./Изображения
----- ./Видео
----- ./dir1
```

Рис. 11: (рис. 10.1 Проверка расширенных атрибутов)

Для всех кроме пользователя недоступна запись в каталоги

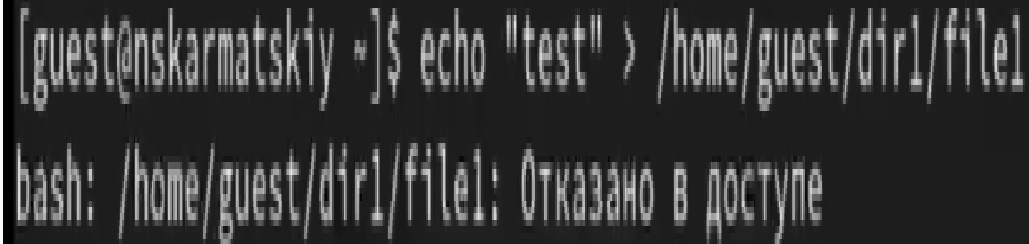
Атрибуты никакие не стоят для каталогов

11. Создаем директорию dir1 и снимаем с директории все атрибуты

```
[guest@nskarmatskiy ~]$ chmod 000 dir1/
[guest@nskarmatskiy ~]$ ls -l
итого 0
d----- . 2 guest guest 6 авг 31 19:45 dir1
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Видео
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Документы
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Загрузки
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Изображения
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Музыка
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Общедоступные
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Шаблоны
```

Рис. 12: (рис. 11. Проверка атрибутов каталога)

12. Попробуем создать файл в директории dir1

A terminal window with a black background and white text. The first line shows a shell prompt [guest@nskarmatskiy ~]\$ followed by the command echo "test" > /home/guest/dir1/file1. The second line shows the error message bash: /home/guest/dir1/file1: Отказано в доступе.

```
[guest@nskarmatskiy ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе
```

Рис. 13: (рис. 12. Попытка создания файла)

13. Заполним 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, занесем е втаблицу знак «+», если не разрешена, знак«-».

```
bash: /home/guest/dirl/: Permission denied
guest@nskarmatskiy ~]$ ls -l /home/guest/dirl/
ls: невозможно открыть каталог '/home/guest/dirl/': Отказано в доступе
guest@nskarmatskiy ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 авг 31 19:45 dirl
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Видео
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Документы
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Загрузки
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Изображения
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Музыка
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Общедоступные
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Шаблоны
guest@nskarmatskiy ~]$ cd dirl/
bash: cd: dirl/: Permission denied
guest@nskarmatskiy ~]$ chmod 700 dirl/
guest@nskarmatskiy ~]$ ls -l
total 0
drwx-----. 2 guest guest 6 авг 31 19:45 dirl
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Видео
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Документы
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Загрузки
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Изображения
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Музыка
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Общедоступные
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Шаблоны
guest@nskarmatskiy ~]$ cd dirl/
guest@nskarmatskiy dirl]$ chmod 700 dirl/
chmod: невозможно получить доступ к 'dirl/': Нет такого файла или каталога
guest@nskarmatskiy dirl]$
```

Рис. 14: (рис. 13. Проверка доступных действий)

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

Операции	Минимальные права на директорию	Минимальные права на файл
Создание файла	d(300)	(000)
Удаление файла	d(300)	(000)
Чтение файла	d(100)	(400)
Запись в файл	d(300)	(200)
Переименование файла	d(300)	(000)
Создание поддиректории	d(300)	(000)
Удаление поддиректории	d(300)	(000)

Рис. 15: Таблица 2.2 “Минимальные права для совершения операций”

Получены практических навыки работы в консоли с атрибутами файлов, закреплены теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux

1. Методические материалы курса.
2. Права доступа в ОС Linux -
<https://codechick.io/tutorials/unix-linux/unix-linux-permissions>
3. Руководство по команде lsattr -
https://rus-linux.net/MyLDP/consol/Linux_lsattr_command.html