

Лабораторная работа No 2

Дискреционное разграничение прав в Linux. Основные атрибуты

Белов Никита Дмитриевич

Содержание

1 Цель работы

1. Получение практических навыков работы в консоли с атрибутами файлов
2. Закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

2 Теоретическое введение

Здесь описываются теоретические аспекты, связанные с выполнением работы.

Например, в табл. 1 приведено краткое описание стандартных каталогов Unix.

Таблица 1: Описание некоторых каталогов файловой системы GNU Linux

| Имя каталога | Описание каталога |
|--------------|---|
| / | Корневая директория, содержащая всю файловую |
| /bin | Основные системные утилиты, необходимые как в однопользовательском режиме, так и при обычной работе всем пользователям |
| /etc | Общесистемные конфигурационные файлы и файлы конфигурации установленных программ |
| /home | Содержит домашние директории пользователей, которые, в свою очередь, содержат персональные настройки и данные пользователя |
| /media | Точки монтирования для сменных носителей |
| /root | Домашняя директория пользователя root |
| /tmp | Временные файлы |
| /usr | Вторичная иерархия для данных пользователя |

Более подробно об Unix см. в [1–6].

3 Выполнение лабораторной работы

Создаём новую учётную запись guest, используя команду `useradd guest`.

После этого задаём пароль с помощью команды `passwd guest`, используя учетную запись администратора и входим в систему от имени пользователя `guest`.

Создание учётной записи

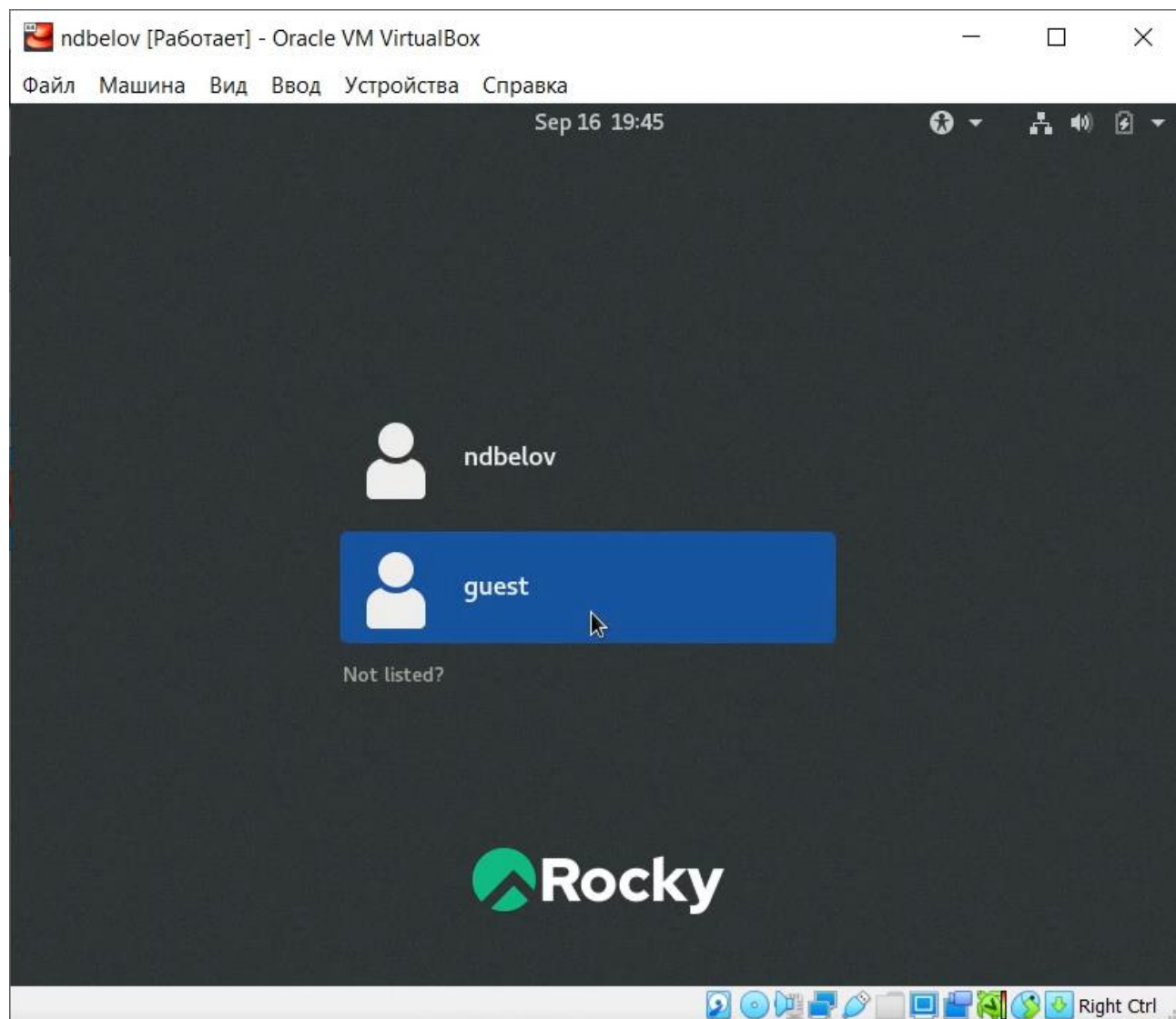


Рис. 1: Учетная запись

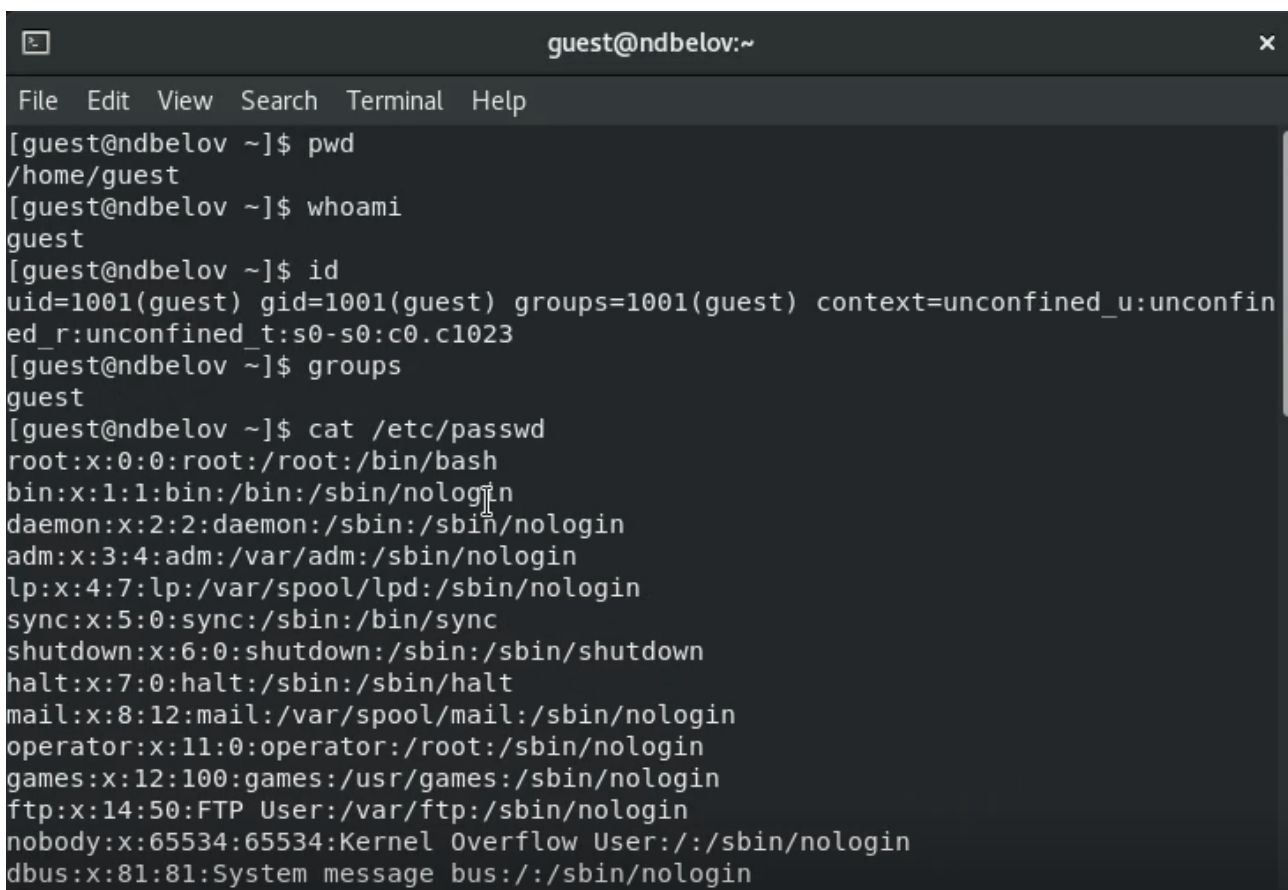
С помощью команды `pwd` убеждаемся, что директория домашняя и совпадает с приглашением командной строки.

Командой `whoami` уточняем имя пользователя - `guest`.

Уточняем имя пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Получаем результат `1001`.

Далее сравниваем вывод `id` с приглашением командной строки, имя пользователя повторяется.

Просматриваем файл `/etc/passwd` командой `cat /etc/passwd`.



```
guest@ndbelov:~  
File Edit View Search Terminal Help  
[guest@ndbelov ~]$ pwd  
/home/guest  
[guest@ndbelov ~]$ whoami  
guest  
[guest@ndbelov ~]$ id  
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@ndbelov ~]$ groups  
guest  
[guest@ndbelov ~]$ 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  
dbus:x:81:81:System message bus:/:/sbin/nologin
```

Рис. 2: *whoami*

Найдём в нём свою учётную запись. Определим `uid` пользователя. Определим `gid` пользователя. Найденные значения совпадают с полученными в предыдущих пунктах.

Определим существующие в системе директории командой `ls -l /home/`. Нам удалось получить список поддиректорий. У каждой из них установлены права на чтение, запись и выполнение только для самого пользователя.

Проверяем, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой: `lsattr /home`

Нам удалось увидеть расширенные атрибуты директории, но не удалось увидеть расширенные атрибуты директории другого пользователя.

Создаем в домашней директории поддиректорию `dir1` командой `mkdir dir1`

Определяем командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`.

Снимаем с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверяем с её помощью правильность выполнения команды `ls -l`.

```
guest@ndbelov:~  
File Edit View Search Terminal Help  
[guest@ndbelov ~]$ ls -l /home/  
total 8  
drwx-----. 15 guest  guest  4096 Sep 16 19:45 guest  
drwx-----. 15 ndbelov ndbelov 4096 Sep 16 19:35 ndbelov  
[guest@ndbelov ~]$ lsattr /home  
lsattr: Permission denied While reading flags on /home/ndbelov  
----- /home/guest  
[guest@ndbelov ~]$ mkdir dir1  
[guest@ndbelov ~]$ ls -l dir1  
total 0  
[guest@ndbelov ~]$ ls -l  
total 0  
drwxr-xr-x. 2 guest guest 6 Sep 16 19:45 Desktop  
drwxrwxr-x. 2 guest guest 6 Sep 16 19:52 dir1  
drwxr-xr-x. 2 guest guest 6 Sep 16 19:45 Documents  
drwxr-xr-x. 2 guest guest 6 Sep 16 19:45 Downloads  
drwxr-xr-x. 2 guest guest 6 Sep 16 19:45 Music  
drwxr-xr-x. 2 guest guest 6 Sep 16 19:45 Pictures  
drwxr-xr-x. 2 guest guest 6 Sep 16 19:45 Public  
drwxr-xr-x. 2 guest guest 6 Sep 16 19:45 Templates  
drwxr-xr-x. 2 guest guest 6 Sep 16 19:45 Videos  
[guest@ndbelov ~]$ lsattr  
----- ./Desktop  
----- ./Downloads  
----- ./Templates  
----- ./Public  
----- ./Documents  
----- ./Music  
----- ./Pictures  
----- ./Videos  
----- ./dir1  
[guest@ndbelov ~]$ chmod 000 dir1  
[guest@ndbelov ~]$ ls -l  
total 0  
drwxr-xr-x. 2 guest guest 6 Sep 16 19:45 Desktop  
d------. 2 guest guest 6 Sep 16 19:52 dir1  
drwxr-xr-x. 2 guest guest 6 Sep 16 19:45 Documents  
drwxr-xr-x. 2 guest guest 6 Sep 16 19:45 Downloads  
drwxr-xr-x. 2 guest guest 6 Sep 16 19:45 Music  
drwxr-xr-x. 2 guest guest 6 Sep 16 19:45 Pictures  
drwxr-xr-x. 2 guest guest 6 Sep 16 19:45 Public  
drwxr-xr-x. 2 guest guest 6 Sep 16 19:45 Templates  
drwxr-xr-x. 2 guest guest 6 Sep 16 19:45 Videos  
[guest@ndbelov ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Permission denied  
[guest@ndbelov ~]$ ls -l /home/guest/dir1  
ls: cannot open directory '/home/guest/dir1': Permission denied
```

Рис. 3: Снятие атрибутов

Пытаемся создать в директории dir1 файл file1 командой:

echo "test" > home/guest/dir1/file1, но получаем отказ от выполнения, так как шагом ранее сняли все атрибуты с директории. Проверяем, действительно ли файл не создан, с помощью команды ls -l /home/guest/dir1.

Заполняем таблицу «Установленные права и разрешённые действия».

| Права директории | Права файла | Создание файла | Удаление файла | Запись в файл | Чтение файла | Смена директории | Просмотр файлов в директории | Переименовывание файла | Смена атрибутов файла |
|------------------|----------------|----------------|----------------|---------------|--------------|------------------|------------------------------|------------------------|-----------------------|
| d----- (000) | 0 | - | - | - | - | - | - | - | - |
| d--x----- (100) | 0 | - | - | - | - | + | - | - | + |
| d-w----- (200) | 0 | - | - | - | - | - | - | - | - |
| d-wx----- (300) | 0 | + | + | - | - | + | - | + | + |
| dr----- (400) | 0 | - | - | - | - | - | + | - | - |
| dr-x----- (500) | 0 | - | - | - | - | + | + | - | + |
| drw----- (600) | 0 | - | - | - | - | - | + | - | - |
| drwx----- (700) | 0 | + | + | - | - | + | + | + | + |
| d----- (000) | --x----- (100) | - | - | - | - | - | - | - | - |
| d--x----- (100) | --x----- (100) | - | - | - | - | + | - | - | + |
| d-w----- (200) | --x----- (100) | - | - | - | - | - | - | - | - |
| d-wx----- (300) | --x----- (100) | + | + | - | - | + | - | + | + |
| dr----- (400) | --x----- (100) | - | - | - | - | - | + | - | - |
| dr-x----- (500) | --x----- (100) | - | - | - | - | + | + | - | + |
| drw----- (600) | --x----- (100) | - | - | - | - | - | + | - | - |
| drwx----- (700) | --x----- (100) | + | + | - | - | + | + | + | + |
| d----- (000) | -w----- (200) | - | - | - | - | - | - | - | - |
| d--x----- (100) | -w----- (200) | - | - | + | - | + | - | - | + |
| d-w----- (200) | -w----- (200) | - | - | - | - | - | - | - | - |
| d-wx----- (300) | -w----- (200) | + | + | + | - | + | - | + | + |
| dr----- (400) | -w----- (200) | - | - | - | - | - | + | - | - |
| dr-x----- (500) | -w----- (200) | - | - | + | - | + | + | - | + |
| drw----- (600) | -w----- (200) | - | - | - | - | - | + | - | - |
| drwx----- (700) | -w----- (200) | + | + | + | - | + | + | + | + |
| d----- (000) | -wx----- (300) | - | - | - | - | - | - | - | - |
| d--x----- (100) | -wx----- (300) | - | - | + | - | + | - | - | + |
| d-w----- (200) | -wx----- (300) | - | - | - | - | - | - | - | - |
| d-wx----- (300) | -wx----- (300) | + | + | + | - | + | - | + | + |
| dr----- (400) | -wx----- (300) | - | - | - | - | - | + | - | - |
| dr-x----- (500) | -wx----- (300) | - | - | + | - | + | + | - | + |
| drw----- (600) | -wx----- (300) | - | - | - | - | - | + | - | - |
| drwx----- (700) | -wx----- (300) | + | + | + | - | + | + | + | + |
| d----- (000) | r----- (400) | - | - | - | - | - | - | - | - |
| d--x----- (100) | r----- (400) | - | - | - | + | + | - | - | + |
| d-w----- (200) | r----- (400) | - | - | - | - | - | - | - | - |
| d-wx----- (300) | r----- (400) | + | + | - | + | + | - | + | + |
| dr----- (400) | r----- (400) | - | - | - | - | - | + | - | - |
| dr-x----- (500) | r----- (400) | - | - | - | + | + | + | - | + |
| drw----- (600) | r----- (400) | - | - | - | - | - | + | - | - |
| drwx----- (700) | r----- (400) | + | + | - | + | + | + | + | + |
| d----- (000) | r-x----- (500) | - | - | - | - | - | - | - | - |
| d--x----- (100) | r-x----- (500) | - | - | + | + | + | - | - | + |
| d-w----- (200) | r-x----- (500) | - | - | - | - | - | - | - | - |
| d-wx----- (300) | r-x----- (500) | + | + | - | + | + | - | + | + |
| dr----- (400) | r-x----- (500) | - | - | - | - | - | + | - | - |
| dr-x----- (500) | r-x----- (500) | - | - | - | + | + | + | - | + |
| drw----- (600) | r-x----- (500) | - | - | - | - | - | + | - | - |
| drwx----- (700) | r-x----- (500) | + | + | - | + | + | + | + | + |
| d----- (000) | rw----- (600) | - | - | - | - | - | - | - | - |
| d--x----- (100) | rw----- (600) | - | - | + | + | + | - | - | + |
| d-w----- (200) | rw----- (600) | - | - | - | - | - | - | - | - |
| d-wx----- (300) | rw----- (600) | + | + | + | + | + | - | + | + |
| dr----- (400) | rw----- (600) | - | - | - | - | - | + | - | - |
| dr-x----- (500) | rw----- (600) | - | - | + | + | + | + | - | + |
| drw----- (600) | rw----- (600) | - | - | - | - | - | + | - | - |
| drwx----- (700) | rw----- (600) | + | + | + | + | + | + | + | + |
| d----- (000) | rwX----- (700) | - | - | - | - | - | - | - | - |
| d--x----- (100) | rwX----- (700) | - | - | + | + | + | - | - | + |
| d-w----- (200) | rwX----- (700) | - | - | - | - | - | - | - | - |
| d-wx----- (300) | rwX----- (700) | + | + | + | + | + | - | + | + |
| dr----- (400) | rwX----- (700) | - | - | - | - | - | + | - | - |
| dr-x----- (500) | rwX----- (700) | - | - | + | + | + | + | - | + |
| drw----- (600) | rwX----- (700) | - | - | - | - | - | + | - | - |
| drwx----- (700) | rwX----- (700) | + | + | + | + | + | + | + | + |

Рис. 4: Права на действия

Заполним таблицу «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) |
| Переименовывание файла | d-wx----- (300) | ----- (000) |
| Создание поддиректории | d-wx----- (300) | ----- (000) |
| Удаление поддиректории | d-wx----- (300) | ----- (000) |

Рис. 5: Минимальные права

4 Выводы

Получили практические навыки работы в консоли с атрибутами файлов, закрепили теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux. # Список литературы{.unnumbered}

1. GNU Bash Manual [Электронный ресурс]. Free Software Foundation, 2016. URL: <https://www.gnu.org/software/bash/manual/>.
2. Newham C. [Learning the bash Shell: Unix Shell Programming](#). O'Reilly Media, 2005. 354 с.
3. Zarrelli G. Mastering Bash. Packt Publishing, 2017. 502 с.
4. Robbins A. [Bash Pocket Reference](#). O'Reilly Media, 2016. 156 с.
5. Таненбаум Э. Архитектура компьютера. 6-е изд. СПб.: Питер, 2013. 874 с.
6. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.