

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Валиева Найля Разимовна

Содержание

| | | |
|----------|---------------------------------------|-----------|
| 1 | Цель работы | 5 |
| 2 | Задание | 6 |
| 3 | Выполнение лабораторной работы | 7 |
| 4 | Выводы | 17 |

Список таблиц

| | | |
|-----|--|----|
| 3.1 | Установленные права и разрешённые действия | 13 |
| 3.2 | Минимальные права для совершения операций | 16 |

Список иллюстраций

| | | |
|------|---|----|
| 3.1 | Создание учетной записи guest | 7 |
| 3.2 | Задание пароля для учетной записи | 8 |
| 3.3 | Вход в систему от имени пользователя guest | 8 |
| 3.4 | Определение текущей директории. Переход в домашнюю директорию | 8 |
| 3.5 | Уточнение имени пользователя | 9 |
| 3.6 | Уточнение имени, его группы | 9 |
| 3.7 | Сравнение полученной информации | 9 |
| 3.8 | Просмотр файла с помощью команды cat (часть 1) | 10 |
| 3.9 | Просмотр файла с помощью команды cat (часть 2) | 10 |
| 3.10 | Фильтрованный вывод строк | 11 |
| 3.11 | Определение существующих в системе директорий | 11 |
| 3.12 | Проверка установленных расширенных атрибутов | 11 |
| 3.13 | Создание директории dir1 | 12 |
| 3.14 | Снятие всех атрибутов с директории dir1 | 12 |
| 3.15 | Попытка создания файла file1 | 12 |

1 Цель работы

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.

2 Задание

1. Создать учетную запись пользователя guest.
2. Войти в терминал, используя созданную учетную запись, и выполнить ряд команд.
3. Заполнить таблицу “Установленные права и разрешенные действия”
4. Заполнить таблицу “Минимальные права для совершения операций”

3 Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе я создала учётную запись пользователя guest (использовала учётную запись администратора) (рис - @fig:001). Для этого использовала команду `user add guess`

```
[nrvalieva@nrvalieva ~]$ su
Пароль:
[root@nrvalieva nrvalieva]# useradd guest
useradd: пользователь «guest» уже существует
[root@nrvalieva nrvalieva]# passwd guest
Смена пароля для пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: не содержит достаточное число РАЗЛИЧНЫХ символов
Повторите ввод нового пароля :
Извините, но пароли не совпадают.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: не содержит достаточное число РАЗЛИЧНЫХ символов
Повторите ввод нового пароля :
passwd: все токены проверки подлинности успешно обновлены.
[root@nrvalieva nrvalieva]#
```

Рис. 3.1: Создание учетной записи guest

Задала пароль для пользователя guest (использовала учётную запись администратора) (рис @fig:002). Для этого использовала команду `passwd guest`

```

[nrvalieva@nrvalieva ~]$ su
Пароль:
[root@nrvalieva nrvalieva]# useradd guest
useradd: пользователь «guest» уже существует
[root@nrvalieva nrvalieva]# passwd guest
Смена пароля для пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: не содержит достаточное число РАЗЛИЧНЫХ символов
Повторите ввод нового пароля :
Извините, но пароли не совпадают.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: не содержит достаточное число РАЗЛИЧНЫХ символов
Повторите ввод нового пароля :
passwd: все токены проверки подлинности успешно обновлены.
[root@nrvalieva nrvalieva]# █

```

Рис. 3.2: Задание пароля для учетной записи

Вошла в систему от имени пользователя guest (рис @fig:003).



Рис. 3.3: Вход в систему от имени пользователя guest

2. Определила директорию, в которой я нахожусь, командой `pwd`. Она совпадает с приглашением командной строки. Определила, что она не является моей домашней директорией. Перешла в свою домашнюю директорию. (рис @fig:004)

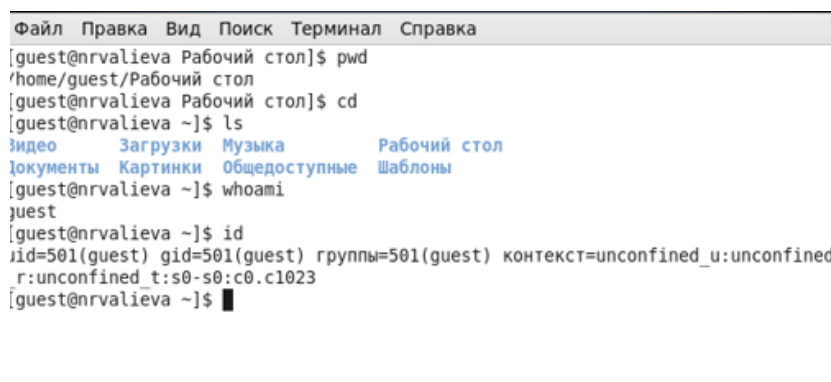


Рис. 3.4: Определение текущей директории. Переход в домашнюю директорию

Уточнила имя своего пользователя командой `whoami` (рис @fig:005).


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

Рис. 3.5: Уточнение имени пользователя

Уточнила имя своего пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. запомнила. Группы совпадают, однако вывод команды `id` объемнее (рис @fig:006).

```
[guest@nrvalieva ~]$ id  
uid=501(guest) gid=501(guest) группы=501(guest) контекст=unconfined_u:unconfined  
r:unconfined_t:s0-s0:c0.c1023  
[guest@nrvalieva ~]$
```

Рис. 3.6: Уточнение имени, его группы

Сравнила полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки (рис @fig:007). Как видно из рисунка, информация об имени пользователя, полученная командой `id` (`gid=501(guest)`), совпадает с приглашением командной строки (`guest@nrvalieva home`)

```
[guest@nrvalieva Рабочий стол]:
```

Рис. 3.7: Сравнение полученной информации


Просмотрела файл `/etc/passwd` командой `cat /etc/passwd` (рис @fig:008, рис @fig:009)

```

[guest@nrvalieva ~]$ /etc/passwd
bash: /etc/passwd: Отказано в доступе
[guest@nrvalieva ~]$ 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

```

Рис. 3.8: Просмотр файла с помощью команды cat (часть 1)



```

gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/sbin/nologin
rtkit:x:499:497:RealtimeKit:/proc:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
pulse:x:498:496:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
ntp:x:38:38:/:etc/ntp:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
saslauthd:x:497:76:Saslauthd user:/var/empty/saslauthd:/sbin/nologin
postfix:x:89:89:/:var/spool/postfix:/sbin/nologin
abrt:x:173:173:/:etc/abrt:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
gdm:x:42:42:/:var/lib/gdm:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
nrvalieva:x:500:500:nrvalieva:/home/nrvalieva:/bin/bash
guest:x:501:501:/:home/guest:/bin/bash
[guest@nrvalieva ~]$

```

Рис. 3.9: Просмотр файла с помощью команды cat (часть 2)

Нашла свою учетную запись (последняя строчка). Определила `uid` и `gid` пользователя (501 и 501 соответственно). Они совпадают со значениями `uid` и `gid`, полученными на предыдущих пунктах.

Для того, чтобы вывести только строки, содержащие определенные буквенные сочетания, необходимо воспользоваться программой `grep` в терминале (рис @fig:010)

```
[guest@nrvalieva ~]$ cat /etc/passwd | grep guest
guest:x:501:501::/home/guest:/bin/bash
```

Рис. 3.10: Фильтрованный вывод строк

Определила существующие в системе директории командой `ls -l /home/` (рис @fig:011)

```
[guest@nrvalieva ~]$ ls -l /home/
итого 8
drwx-----, 24 guest      guest      4096 Окт  2 19:05 guest
drwx-----, 29 nrvalieva nrvalieva 4096 Окт  2 18:56 nrvalieva
```

Рис. 3.11: Определение существующих в системе директорий

Мне удалось получить список поддиректорий директории `/home`. На поддиректориях установлены права на чтение (r), запись (w) и исполнение (x).

Проверила, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home` с помощью команды `lsattr /home` (рис @fig:012)

```
[guest@nrvalieva ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/nrvalieva
-----e- /home/guest
```

Рис. 3.12: Проверка установленных расширенных атрибутов

Удалось увидеть расширенные атрибуты директории `guest`. Однако не удалось увидеть расширенные атрибуты других директорий (`nrvalieva`).

Создала в домашней директории поддиректорию `dir1` командой `mkdir dir1` (рис. @fig:013)

```

[guest@nrvalieva ~]$ mkdir dir1
[guest@nrvalieva ~]$ ls
dir1  Документы  Картинки  Общедоступные  Шаблоны
Видео  Загрузки  Музыка  Рабочий стол
[guest@nrvalieva ~]$ ls -l
итого 36
drwxrwxr-x. 2 guest guest 4096 Окт  2 19:12 dir1
drwxr-xr-x. 2 guest guest 4096 Окт  2 19:05 Видео
drwxr-xr-x. 2 guest guest 4096 Окт  2 19:05 Документы
drwxr-xr-x. 2 guest guest 4096 Окт  2 19:05 Загрузки
drwxr-xr-x. 2 guest guest 4096 Окт  2 19:05 Картинки
drwxr-xr-x. 2 guest guest 4096 Окт  2 19:05 Музыка
drwxr-xr-x. 2 guest guest 4096 Окт  2 19:05 Общедоступные

```

Рис. 3.13: Создание директории dir1

Также с помощью команд `ls -l` и `lsattr` просмотрела, какие атрибуты выставлены на директорию `dir1` (`drwxrwxr-x` и `-----e-` соответственно).

Сняла с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверила правильность выполнения команды с помощью `ls -l` (рис. @fig:014)

```

[guest@nrvalieva ~]$ chmod 000 dir1
[guest@nrvalieva ~]$ ls -l
итого 36
d------. 2 guest guest 4096 Окт  2 19:12 dir1
drwxr-xr-x. 2 guest guest 4096 Окт  2 19:05 Видео
drwxr-xr-x. 2 guest guest 4096 Окт  2 19:05 Документы
drwxr-xr-x. 2 guest guest 4096 Окт  2 19:05 Загрузки
drwxr-xr-x. 2 guest guest 4096 Окт  2 19:05 Картинки
drwxr-xr-x. 2 guest guest 4096 Окт  2 19:05 Музыка
drwxr-xr-x. 2 guest guest 4096 Окт  2 19:05 Общедоступные
drwxr-xr-x. 2 guest guest 4096 Окт  2 19:05 Рабочий стол
drwxr-xr-x. 2 guest guest 4096 Окт  2 19:05 Шаблоны

```

Рис. 3.14: Снятие всех атрибутов с директории dir1

Попыталась создать в директории `dir1` файл `file1` командой `echo "test" > /home/guest/dir1/file1` (рис. @fig:015). Я получила отказ, т.к. на предыдущем шаге для директории `dir` были сняты все атрибуты.

```

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

```

Рис. 3.15: Попытка создания файла file1

С помощью команды `ls -l /home/guest/dir1` выяснила, что невозможно

получить доступ к директории `dir1`. Файл `file1` действительно не находится в директории

3. Заполнила таблицу “Установленные права и разрешенные действия”, выполняя действия от имени владельца директории (файлов), определив опытным путем, какие операции разрешены, а какие нет. “+” - операция разрешена, “-” - операция не разрешена (таб. 3.1)

Таблица 3.1: Установленные права и разрешённые действия

| Права ди- ректо- рии | Пра- ва фай- ла | Со- зда- ние фай- ла | Уда- ле- ние фай- ла | За- пись в файл | Чте- ние фай- ла | Сме- на ди- ректо- рии | Просмотр файлов в директо- рии | Пере- имено- вание файла | Смена атрибу- тов файла |
|-------------------------------|--------------------------|----------------------------------|----------------------------------|--------------------------|---------------------------|------------------------------------|---|-----------------------------------|----------------------------------|
| d(000) | (000) | - | - | - | - | - | - | - | - |
| d(000) | (100) | - | - | - | - | - | - | - | - |
| d(000) | (200) | - | - | - | - | - | - | - | - |
| d(000) | (300) | - | - | - | - | - | - | - | - |
| d(000) | (400) | - | - | - | - | - | - | - | - |
| d(000) | (500) | - | - | - | - | - | - | - | - |
| d(000) | (600) | - | - | - | - | - | - | - | - |
| d(000) | (700) | - | - | - | - | - | - | - | - |
| d(100) | (000) | - | - | - | - | - | - | - | + |
| d(100) | (100) | - | - | - | - | - | - | - | + |
| d(100) | (200) | - | - | + | - | - | - | - | + |
| d(100) | (300) | - | - | + | - | - | - | - | + |
| d(100) | (400) | - | - | - | + | - | - | - | + |
| d(100) | (500) | - | - | - | + | - | - | - | + |
| d(100) | (600) | - | - | + | + | - | - | - | + |

| Права ди- ректо- рии | Пра- ва фай- ла | Со- зда- ние фай- ла | Уда- ле- ние фай- ла | За- пись в файл | Чте- ние фай- ла | Сме- на ди- ректо- рии | Просмотр файлов в директо- рии | Пере- имено- вание файла | Смена атрибу- тов файла |
|-------------------------------|--------------------------|----------------------------------|----------------------------------|--------------------------|---------------------------|------------------------------------|---|-----------------------------------|----------------------------------|
| d(100) | (700) | - | - | + | + | - | - | - | + |
| d(200) | (000) | - | - | - | - | - | - | - | - |
| d(200) | (100) | - | - | - | - | - | - | - | - |
| d(200) | (200) | - | - | - | - | - | - | - | - |
| d(200) | (300) | - | - | - | - | - | - | - | - |
| d(200) | (400) | - | - | - | - | - | - | - | - |
| d(200) | (500) | - | - | - | - | - | - | - | - |
| d(200) | (600) | - | - | - | - | - | - | - | - |
| d(200) | (700) | - | - | - | - | - | - | - | - |
| d(300) | (000) | + | + | - | - | + | - | + | + |
| d(300) | (100) | + | + | - | - | + | - | + | + |
| d(300) | (200) | + | + | + | - | + | - | + | + |
| d(300) | (300) | + | + | + | - | + | - | + | + |
| d(300) | (400) | + | + | - | + | + | - | + | + |
| d(300) | (500) | + | + | - | + | + | - | + | + |
| d(300) | (600) | + | + | + | + | + | - | + | - |
| d(300) | (700) | + | + | + | + | + | - | + | - |
| d(400) | (000) | - | - | - | - | - | + | - | - |
| d(400) | (100) | - | - | - | - | - | + | - | - |
| d(400) | (200) | - | - | - | - | - | + | - | - |
| d(400) | (300) | - | - | - | - | - | + | - | - |
| d(400) | (400) | - | - | - | - | - | + | - | - |
| d(400) | (500) | - | - | - | - | - | + | - | - |

| Права ди- ректо- рии | Пра- ва фай- ла | Со- зда- ние фай- ла | Уда- ле- ние фай- ла | За- пись в файл | Чте- ние фай- ла | Сме- на ди- ректо- рии | Просмотр файлов в директо- рии | Пере- имено- вание файла | Смена атрибу- тов файла |
|-------------------------------|--------------------------|----------------------------------|----------------------------------|--------------------------|---------------------------|------------------------------------|---|-----------------------------------|----------------------------------|
| d(400) | (600) | - | - | - | - | - | + | - | - |
| d(400) | (700) | - | - | - | - | - | + | - | - |
| d(500) | (000) | + | - | - | - | - | + | - | + |
| d(500) | (100) | + | - | - | - | - | + | - | + |
| d(500) | (200) | + | - | + | - | - | + | - | + |
| d(500) | (300) | + | - | + | - | - | + | - | + |
| d(500) | (400) | + | - | - | + | - | + | - | + |
| d(500) | (500) | + | - | - | + | - | + | - | + |
| d(500) | (600) | + | - | + | + | - | + | - | + |
| d(500) | (700) | + | - | + | + | - | + | - | + |
| d(600) | (000) | - | - | - | - | - | + | - | - |
| d(600) | (100) | - | - | - | - | - | + | - | - |
| d(600) | (200) | - | - | - | - | - | + | - | - |
| d(600) | (300) | - | - | - | - | - | + | - | - |
| d(600) | (400) | - | - | - | - | - | + | - | - |
| d(600) | (500) | - | - | - | - | - | + | - | - |
| d(600) | (600) | - | - | - | - | - | + | - | - |
| d(600) | (700) | - | - | - | - | - | + | - | - |
| d(700) | (000) | + | + | - | - | + | + | + | + |
| d(700) | (100) | + | + | - | - | + | + | + | + |
| d(700) | (200) | + | + | + | - | + | + | + | + |
| d(700) | (300) | + | + | + | - | + | + | + | + |
| d(700) | (400) | + | + | - | + | + | + | + | + |

| Права ди- ректо- рии | Пра- ва фай- ла | Со- зда- ние фай- ла | Уда- ле- ние фай- ла | За- пись в файл | Чте- ние фай- ла | Сме- на ди- ректо- рии | Просмотр файлов в директо- рии | Пере- имено- вание файла | Смена атрибу- тов файла |
|-------------------------------|--------------------------|----------------------------------|----------------------------------|--------------------------|---------------------------|------------------------------------|---|-----------------------------------|----------------------------------|
| d(700) | (500) | + | + | - | + | + | + | + | + |
| d(700) | (600) | + | + | + | + | + | + | + | + |
| d(700) | (700) | + | + | + | + | + | + | + | + |

4. На основании заполненной выше таблицы определил те или иные минимально необходимые права для выполнения операций внутри директории `dir1`, заполняя таблицу “Установленные права и разрешенные действия” (таб. 3.2).

Таблица 3.2: Минимальные права для совершения операций

| Операция | min права на директорию | min права на файл |
|------------------------|-------------------------|-------------------|
| Создание файла | (-wx)(3) | (- - -)(0) |
| Удаление файла | (-wx)(3) | (- - -)(0) |
| Чтение файла | (- - x)(1) | (r - -)(4) |
| Запись в файл | (- - x)(1) | (-w-)(2) |
| Переименование файла | (-wx)(3) | (- - -)(0) |
| Создание поддиректории | (-wx)(3) | (- - -)(0) |
| Удаление поддиректории | (-wx)(3) | (- - -)(0) |

4 Выводы

Я получила практические навыки работы в консоли с атрибутами файлов, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.