

Отчёт по лабораторной работе №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Руслан Кайкы НБИ-01-20

Содержание

1	Цель работы	1
2	Выполнение лабораторной работы.....	1
3	Вывод.....	10
Список литературы		Ошибка! Закладка не определена.

1 Цель работы

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

2 Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создали учётную запись пользователя guest (используя учётную запись администратора) и задали пароль для пользователя guest (используя учётную запись администратора)
2. Вошли в систему от имени пользователя guest
3. Командой `pwd` определили директорию, в которой находимся и определили является ли она домашней директорией
4. Уточнили имя нашего пользователя командой `whoami`:
5. Уточнили имя пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. Сравнили вывод `id` с выводом команды `groups`. Видим, что `gid` и группы = `1001(guest)`
6. Сравним полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки и убедимся, что они совпадают

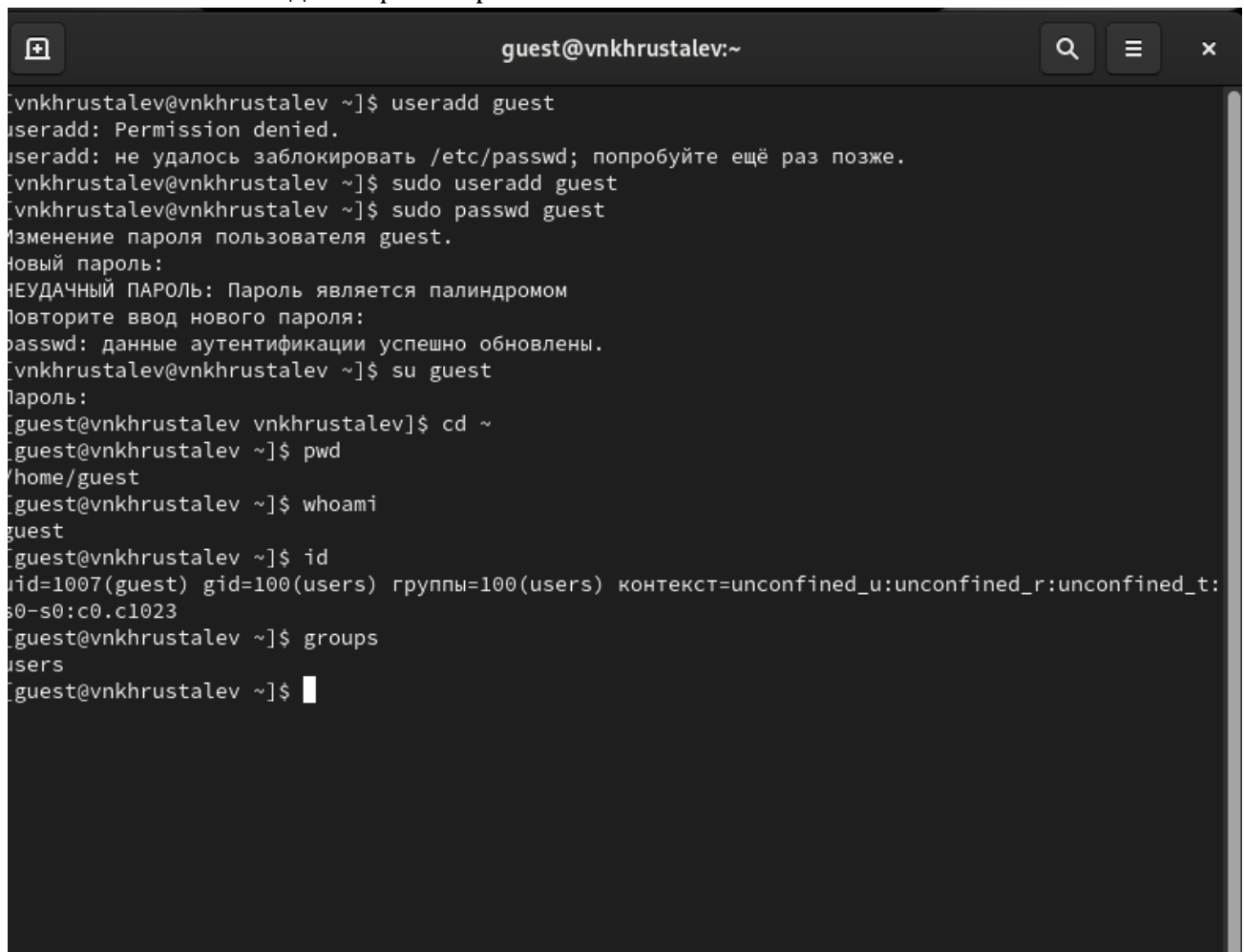
```

[vnkhurstalev@vnkhurstalev ~]$ useradd guest
useradd: Permission denied.
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.
[vnkhurstalev@vnkhurstalev ~]$ sudo useradd guest
[vnkhurstalev@vnkhurstalev ~]$ sudo passwd guest
Изменение пароля пользователя guest.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[vnkhurstalev@vnkhurstalev ~]$

```

Figure 1: Информация о пользователе guest

7. Просмотрим файл `/etc/passwd` Командой: `cat /etc/passwd`. Найдем в нём свою учётную запись. Определим `uid` пользователя. Определим `gid` пользователя. Сравним найденные значения с полученными в предыдущих пунктах. Guest имеет те же идентификаторы 1007



```

guest@vnkhurstalev:~
[vnkhurstalev@vnkhurstalev ~]$ useradd guest
useradd: Permission denied.
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.
[vnkhurstalev@vnkhurstalev ~]$ sudo useradd guest
[vnkhurstalev@vnkhurstalev ~]$ sudo passwd guest
Изменение пароля пользователя guest.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[vnkhurstalev@vnkhurstalev ~]$ su guest
Пароль:
[guest@vnkhurstalev vnkhurstalev]$ cd ~
[guest@vnkhurstalev ~]$ pwd
/home/guest
[guest@vnkhurstalev ~]$ whoami
guest
[guest@vnkhurstalev ~]$ id
uid=1007(guest) gid=100(users) группы=100(users) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@vnkhurstalev ~]$ groups
users
[guest@vnkhurstalev ~]$

```

Figure 2: Содержимое файла `/etc/passwd`

8. Определим существующие в системе директории командой `ls -l /home/`

9. Проверили, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: `lsattr /home`. Нам не удалось увидеть расширенные атрибуты директорий других пользователей, только своей домашней директории.

```
guest@vnkhrustalev:~  
[vnkhrustalev@vnkhrustalev ~]$ useradd guest  
useradd: Permission denied.  
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.  
[vnkhrustalev@vnkhrustalev ~]$ sudo useradd guest  
[vnkhrustalev@vnkhrustalev ~]$ sudo passwd guest  
Изменение пароля пользователя guest.  
Новый пароль:  
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом  
Повторите ввод нового пароля:  
passwd: данные аутентификации успешно обновлены.  
[vnkhrustalev@vnkhrustalev ~]$ su guest  
Пароль:  
[guest@vnkhrustalev vnkhrustalev]$ cd ~  
[guest@vnkhrustalev ~]$ pwd  
/home/guest  
[guest@vnkhrustalev ~]$ whoami  
guest  
[guest@vnkhrustalev ~]$ id  
uid=1007(guest) gid=100(users) группы=100(users) контекст=unconfined_u:unconfined_r:unconfined_t:  
s0-s0:c0.c1023  
[guest@vnkhrustalev ~]$ groups  
users  
[guest@vnkhrustalev ~]$
```

```

guest@vnkhrustalev ~]$ 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
sssd:x:997:993:User for sssd:/:/sbin/nologin
pipewire:x:996:992:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
libstoragemgmt:x:990:990:daemon account for libstoragemgmt:/:usr/sbin/nologin
systemd-oom:x:989:989:systemd Userspace OOM Killer:/:usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
geoclue:x:988:987:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:987:986:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:986:985:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:985:984:User for flatpak system helper:/:/sbin/nologin
colord:x:984:983:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:983:982:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
n
setroubleshoot:x:982:981:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/nologin
gdm:x:42:42:/:/var/lib/gdm:/sbin/nologin
pesign:x:981:980:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
gnome-initial-setup:x:980:979:/:run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:979:978:chrony system user:/var/lib/chrony:/sbin/nologin

```

Figure 3: Расширенные атрибуты

10. Создали в домашней директории поддиректорию dir1 командой `mkdir dir1`. Определим командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию dir1.
11. Сняли с директории dir1 все атрибуты командой `chmod 000 dir1` и проверили с `ls -l` помощью правильность выполнения команды `chmod`.
12. Создали в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1`. Поскольку ранее мы отозвали все атрибуты, то тем самым лишили всех прав на взаимодействие с dir1.

```

setroubleshoot:x:982:981:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/nologin
gdm:x:42:42:./var/lib/gdm:/sbin/nologin
pesign:x:981:980:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
gnome-initial-setup:x:980:979:./run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:979:978:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:978:977:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72:./sbin/nologin
vnkhrustalev:x:1000:1000:vnkhrustalev:/home/vnkhrustalev:/bin/bash
vboxadd:x:977:1:./var/run/vboxadd:/bin/false
alice:x:1001:1001:./home/alice:/bin/bash
bob:x:1002:1002:./home/bob:/bin/bash
carol:x:1003:100:./home/carol:/bin/bash
dan:x:1004:100:./home/dan:/bin/bash
dave:x:1005:100:./home/dave:/bin/bash
david:x:1006:100:./home/david:/bin/bash
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
guest:x:1007:100:./home/guest:/bin/bash
[guest@vnkhrustalev ~]$ s

```

```

[guest@vnkhrustalev ~]$ ls -l /home/
итого 4
drwx-----.  4 alice      alice      113 сен 23 17:20 alice
drwx-----.  4 bob        bob        113 сен 23 17:20 bob
drwx-----.  6 carol      users      183 сен 23 17:26 carol
drwx-----.  5 dan        users      149 сен 16 14:28 dan
drwx-----.  5 dave       users      149 сен 16 14:28 dave
drwx-----.  5 david      users      149 сен 16 14:28 david
drwx-----.  5 guest      users      169 мар  2 21:52 guest
drwx-----. 14 vnkhrustalev vnkhrustalev 4096 мар  2 21:15 vnkhrustalev
[guest@vnkhrustalev ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/vnkhrustalev
lsattr: Отказано в доступе While reading flags on /home/alice
lsattr: Отказано в доступе While reading flags on /home/bob
lsattr: Отказано в доступе While reading flags on /home/carol
lsattr: Отказано в доступе While reading flags on /home/dan
lsattr: Отказано в доступе While reading flags on /home/dave
lsattr: Отказано в доступе While reading flags on /home/david
----- /home/guest

```

Figure 4: Снятие атрибутов с директории

13. Заполним таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определим опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, заносим в таблицу знак «+», если не разрешена, знак «-».

```

[guest@vnkhrustalev ~]$ mkdir dir1
[guest@vnkhrustalev ~]$ ls -al
итого 40
drwx-----. 6 guest users 181 мар  2 21:58 .
drwxr-xr-x. 10 root root 112 мар  2 21:45 ..
-rw-r--r--. 1 guest users 18 янв 24 2023 .bash_logout
-rw-r--r--. 1 guest users 141 янв 24 2023 .bash_profile
-rw-r--r--. 1 guest users 519 сен 16 14:20 .bashrc
-rw-r--r--. 1 guest users 12288 сен 16 14:19 .bashrc.swo
-rw-r--r--. 1 guest users 12288 сен 16 14:15 .bashrc.swp
drwxr-xr-x. 2 guest users  6 мар  2 21:58 dir1
drwxr-xr-x. 2 guest users  6 сен 16 14:13 Documents
drwxr-xr-x. 4 guest users 39 сен  9 14:44 .mozilla
drwxr-xr-x. 2 guest users  6 сен 16 14:13 Pictures
-rw-----. 1 guest users 136 мар  2 21:52 .xauthmhN8yT
[guest@vnkhrustalev ~]$

```

Figure 5: Заполнение таблицы

```

[guest@vnkhrustalev ~]$ chmod 000 dir1
[guest@vnkhrustalev ~]$ ls -al
итого 40
drwx-----. 6 guest users 181 мар  2 21:58 .
drwxr-xr-x. 10 root root 112 мар  2 21:45 ..
-rw-r--r--. 1 guest users 18 янв 24 2023 .bash_logout
-rw-r--r--. 1 guest users 141 янв 24 2023 .bash_profile
-rw-r--r--. 1 guest users 519 сен 16 14:20 .bashrc
-rw-r--r--. 1 guest users 12288 сен 16 14:19 .bashrc.swo
-rw-r--r--. 1 guest users 12288 сен 16 14:15 .bashrc.swp
d------. 2 guest users  6 мар  2 21:58 dir1
drwxr-xr-x. 2 guest users  6 сен 16 14:13 Documents
drwxr-xr-x. 4 guest users 39 сен  9 14:44 .mozilla
drwxr-xr-x. 2 guest users  6 сен 16 14:13 Pictures
-rw-----. 1 guest users 136 мар  2 21:52 .xauthmhN8yT
[guest@vnkhrustalev ~]$

```

```

[guest@vnkhrustalev ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@vnkhrustalev ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе
[guest@vnkhrustalev ~]$

```

- 1 - Создание файла
- 2- Удаление файла
- 3- Запись в файл
- 4- Чтение файла
- 5- Смена директории
- 6- Просмотр файлов в директории

7 - Переименование файла

8- Смена атрибутов файла

Table 1: Установленные права и разрешённые действия

Права директории	Права файла	1	2	3	4	5	6	7	8
d-----(000)	----- (000)	-	-	-	-	-	-	-	-
d--x----- (100)	----- (000)	-	-	-	-	+	-	-	+
d-w----- (200)	----- (000)	-	-	-	-	-	-	-	-
d-wx----- (300)	----- (000)	+	+	-	-	+	-	+	+
dr----- (400)	----- (000)	-	-	-	-	-	-	-	-
dr-x----- (500)	----- (000)	-	-	-	-	+	+	-	+
drw----- (600)	----- (000)	-	-	-	-	-	-	-	-
drwx----- (700)	----- (000)	+	+	-	-	+	+	+	+
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)	+	+	+	+	+	+	+	+

На основании таблицы выше определили минимально необходимые права для выполнения операций внутри директории dir1 и заполнили таблицу 2. Для заполнения последних двух строк опытным путем проверили минимальные права.

Table 2: Минимальные права для совершения операций

Операция	Права на директорию	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)
Переименование файла	d-wx----- (300)	----- (000)
Создание поддиректории	d-wx----- (300)	----- (000)
Удаление поддиректории	d-wx----- (300)	----- (000)

3 Вывод

В ходе выполнения лабораторной работы были получены навыки работы с атрибутами файлов и сведения о разграничении доступа.

1.