

Отчет по лабораторной работе №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Alexander O. Vorobyov¹

13 September, 2022

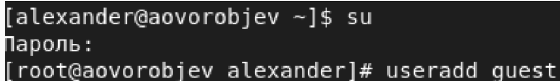
¹RUDN University, Moscow, Russian Federation

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

Выполнение работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создайте учётную запись пользователя guest (используя учётную запись администратора): `useradd guest`.

A terminal window with a dark background. The first line shows a user prompt: [alexander@aovorobjev ~]\$ su. The second line shows the password prompt: Пароль:. The third line shows the root prompt: [root@aovorobjev alexander]# useradd guest.

```
[alexander@aovorobjev ~]$ su
Пароль:
[root@aovorobjev alexander]# useradd guest
```

Figure 1: Добавление пользователя

2. Задайте пароль для пользователя guest (использую учётную запись администратора): `passwd guest`.

```
[root@aovorobjev alexander]# 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.
```

Figure 2: Установка пароля

3. Войдите в систему от имени пользователя guest.

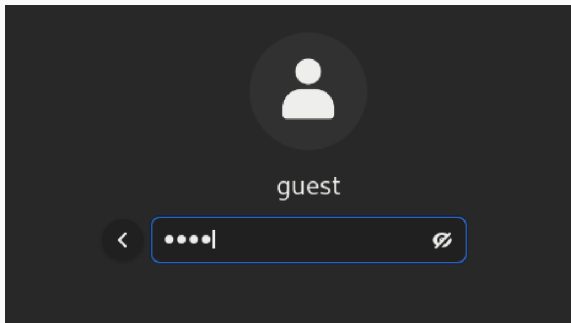


Figure 3: Вход в систему

4. Определите директорию, в которой вы находитесь, командой `pwd`.

```
[guest@aovorobjev ~]$ pwd  
/home/guest
```

Figure 4: Определение директории

5. Уточните имя вашего пользователя командой whoami.

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

Figure 5: Уточнение имени пользователя

6. Уточните имя вашего пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. запомните. Сравните вывод `id` с выводом команды `groups`.

```
[guest@aovorobjev ~]$ id
uid=1002(guest) gid=1002(guest) группы=1002(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
[guest@aovorobjev ~]$ groups
guest
```

Figure 6: Уточнение имени, группы пользователя командами `id`, `groups`

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

8. Просмотрите файл /etc/passwd командой cat /etc/passwd.

```
(guest@aovorobjev ~)$ 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
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
sssd:x:997:993:User for sssd:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
pipewire:x:996:992:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
libstoragemgmt:x:995:991:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
geoclue:x:994:989:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:993:988:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:992:987:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:991:986:User for flatpak system helper:/sbin/nologin
colord:x:990:985:User for colord:/var/lib/colord:/sbin/nologin
setroubleshoot:x:989:984:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/nologin
clevis:x:988:983:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:987:982:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:986:981:/var/lib/chrony:/sbin/nologin
dnsmasq:x:985:980:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72:/sbin/nologin
systemd-oom:x:978:978:systemd Userspace OOM Killer:/usr/sbin/nologin
alexander:x:1000:1000:Alexander:/home/alexander:/bin/bash
aovorobjev:x:1001:1001:/home/aovorobjev:/bin/bash
guest:x:1002:1002:/home/guest:/bin/bash
```

Figure 7: Просмотр файла /etc/passwd

9. Определите существующие в системе директории командой `ls -l /home/`.

```
[guest@aovorobjev ~]$ ls -l /home/
итого 8
drwx-----. 14 alexander alexander 4096 сен 6 19:17 alexander
drwx-----.  3 aovorobjev aovorobjev  78 сен 6 19:13 aovorobjev
drwx-----. 14 guest      guest    4096 сен 12 21:08 guest
```

Figure 8: Определение существующих директорий

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

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

Figure 9: Проверка расширенных атрибутов

11. Создайте в домашней директории поддиректорию dir1 командой mkdir dir1.

```
[guest@aovorobjev ~]$ cd
[guest@aovorobjev ~]$ mkdir dir1
[guest@aovorobjev ~]$ ls -l /dir
ls: невозможно получить доступ к '/dir': Нет такого файла или каталога
[guest@aovorobjev ~]$ ls -l /dir1
ls: невозможно получить доступ к '/dir1': Нет такого файла или каталога
[guest@aovorobjev ~]$ ls -l /dir1/
ls: невозможно получить доступ к '/dir1/': Нет такого файла или каталога
[guest@aovorobjev ~]$ ls -l /home/dir1
ls: невозможно получить доступ к '/home/dir1': Нет такого файла или каталога
[guest@aovorobjev ~]$ ls
dir1 Видео Документы Загрузки Изображения Музыка Общедоступные
[guest@aovorobjev ~]$ ls -l dir1
итого 0
[guest@aovorobjev ~]$ lsattr dir1
```

Figure 10: Создание директории

12. Снимите с директории dir1 все атрибуты командой `chmod 000 dir1`.

```
[guest@aovorobjev ~]$ chmod 000 dir1
[guest@aovorobjev ~]$ ls -l dir1
ls: невозможно открыть каталог 'dir1': Отказано в доступе
[guest@aovorobjev ~]$ ls -l
итого 0
d----- . 2 guest guest 6 сен 12 21:17 dir1
drwxr-xr-x. 2 guest guest 6 сен 12 21:08 Видео
drwxr-xr-x. 2 guest guest 6 сен 12 21:08 Документы
drwxr-xr-x. 2 guest guest 6 сен 12 21:08 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 12 21:08 Изображения
drwxr-xr-x. 2 guest guest 6 сен 12 21:08 Музыка
drwxr-xr-x. 2 guest guest 6 сен 12 21:08 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 12 21:08 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 сен 12 21:08 Шаблоны
```

Figure 11: Снятие атрибутов с созданной директории

13. Попробуйте создать в директории `dir1` файл `file1` командой `echo "test" > /home/guest/dir1/file1`.

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

Figure 12: Попытка создания файла

14. Заполните 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, занесите в таблицу знак «+», если не разрешена, знак «-».

Права директории	Права файла	Создание файла	Удаление файла	Запись файла	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
d(000)	(000)	-	-	-	-	-	-	-	-
d-x-----	(100)	-	-	-	-	+	-	-	+
d-w-----	(200)	+	+	+	-	-	-	+	-
d-wx-----	(300)	+	+	+	-	+	-	+	+
Dg-----	(400)	-	-	-	+	-	+	-	-
Dg-x-----	(500)	-	-	-	+	+	-	-	+
Dgw-----	(600)	+	+	+	+	-	+	+	-
Dgwx-----	(700)	+	+	+	+	+	+	+	+

Figure 13: Таблица 1

15. На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполните таблицу.

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d-w-----	(200)
Удаление файла	d-w-----	(200)
Чтение файла	dr-----	(400)
Запись в файл	d-w-----	(200)
Переименование файла	d-w-----	(200)
Создание поддиректории	d-x-----	(100)
Удаление поддиректории	d-x-----	(100)

Figure 14: Таблица 2

Выводы

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