ЛАБОРАТОРНАЯ РАБОТА 2

Королев Федор,
НПМбд-02-21

Contents

Лабораторная Работа 2

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 Теоретическая Справка

В операционной системе Linux есть много отличных функций безопасности, но одна из самых важных - это система прав доступа к файлам. Изначально каждый файл имел три параметра доступа. Вот они:
• Чтение - разрешает получать содержимое файла, но на запись нет. Для каталога позволяет получить список файлов и каталогов, расположенных в нем
• Запись - разрешает записывать новые данные в файл или изменять существующие, а также позволяет создавать и изменять файлы и каталоги
• Выполнение - невозможно выполнить программу, если у нее нет флага выполнения. Этот атрибут устанавливается для всех программ и скриптов, именно с помощью него система может понять, что этот файл нужно запускать как программу
Каждый файл имеет три категории пользователей, для которых можно устанавливать различные сочетания прав доступа:
• Владелец - набор прав для владельца файла, пользователя, который его создал или сейчас установлен его владельцем. Обычно владелец имеет все права, чтение, запись и выполнение
• Группа - любая группа пользователей, существующая в системе и привязанная к файлу. Но это может быть только одна группа и обычно это группа владельца, хотя для файла можно назначить и другую группу

• Остальные - все пользователи, кроме владельца и пользователей, входящих в группу файла
Команды, которые могут понадобиться при работе с правами доступа:
• “ls -l” - для просмотра прав доступа к файлам и каталогам
• “chmod категория действие флаг файл или каталог” - для изменения прав доступа к файлам и каталогам (категорию действие и флаг можно заменить на набор из трех цифр от 0 до 7)
Значения флагов прав:
• — - нет никаких прав
• –x - разрешено только выполнение файла, как программы, но не изменение и не чтение • -w- - разрешена только запись и изменение файла
• -wx - разрешено изменение и выполнение, но в случае с каталогом, невозможно посмотреть его содержимое
• r– - права только на чтение
• r-x - только чтение и выполнение, без права на запись
• rw- - права на чтение и запись, но без выполнения
• rwx - все права

3 Выполнение Лабораторной Работы

В установленной при выполнении предыдущей лабораторной работы ОС создала учётную запись пользователя guest с помощью команды “sudo useradd guest” и задала пароль для этого пользователя командой “sudo passwd guest”

```
[fedor@localhost ~]$ sudo useradd guest

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for fedor:
[fedor@localhost ~]$ sudo useradd guest
useradd: user 'guest' already exists
[fedor@localhost ~]$ passwd guest
passwd: Only root can specify a user name.
[fedor@localhost ~]$ sudo passwd guest
Changing password for user guest.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Начальная дирректория является домашней:

```
[guest@localhost ~]$ pwd
/home/guest
[guest@localhost ~]$ cd ~
[guest@localhost ~]$ pwd
/home/guest
[guest@localhost ~]$
```

```
[guest@localhost ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@localhost ~]$ echo uid=1001(guest) gid=1001(guest) > remember.txt
bash: syntax error near unexpected token `('
[guest@localhost ~]$ echo "uid=1001(guest) gid=1001(guest") > remember.txt
bash: syntax error near unexpected token `)'
[guest@localhost ~]$ echo "uid=1001(guest) gid=1001(guest)" > remember.txt
[guest@localhost ~]$ ls -l
total 4
drwxr-xr-x. 2 guest guest  6 Sep  6 19:47 Desktop
drwxr-xr-x. 2 guest guest  6 Sep  6 19:47 Documents
drwxr-xr-x. 2 guest guest  6 Sep  6 19:47 Downloads
drwxr-xr-x. 2 guest guest  6 Sep  6 19:47 Music
drwxr-xr-x. 2 guest guest  6 Sep  6 19:47 Pictures
drwxr-xr-x. 2 guest guest  6 Sep  6 19:47 Public
-rw-r--r--. 1 guest guest 32 Sep  6 19:52 remember.txt
drwxr-xr-x. 2 guest guest  6 Sep  6 19:47 Templates
drwxr-xr-x. 2 guest guest  6 Sep  6 19:47 Videos
[guest@localhost ~]$ groups
guest
```

id отличается от *groups* тем, что выводит только guest.

Смотрим учетные записи, находим в них свою:

```
[guest@localhost ~]$ 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
tss:x:59:59: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-wsinstance: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
clevis:x:985:984:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:984:983:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
pesign:x:983:982:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
gnome-initial-setup:x:982:981::/run/gnome-initial-setup/:/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
fedor:x:1000:1000:fedor:/home/fedor:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
```

Сравниваем *uid* и *gid* с раннее запомненными - совпадает:

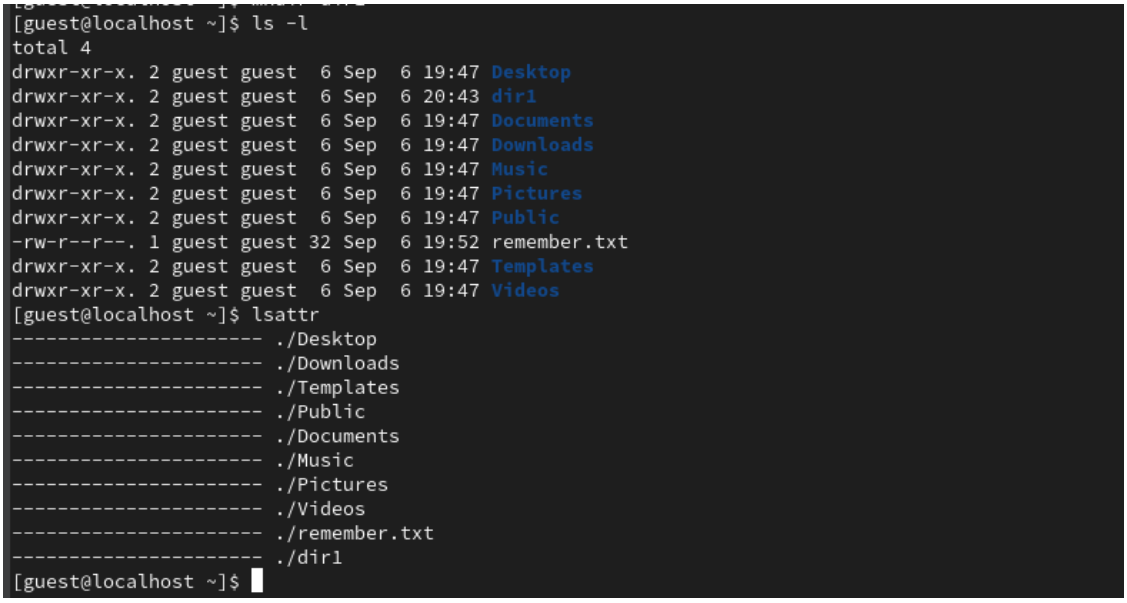
```
guest:x:1001:1001::/home/guest:/bin/bash
[guest@localhost ~]$ cat remember.txt
uid=1001(guest) gid=1001(guest)
[guest@localhost ~]$
```

на обоих пользователях установлены одинаковые права: исполнение, чтение, запись для владельца:

```
[guest@localhost ~]$ ls -l /home/
total 8
drwx------. 14 fedor fedor 4096 Sep  6 19:10 fedor
drwx------. 14 guest guest 4096 Sep  6 19:52 guest
```

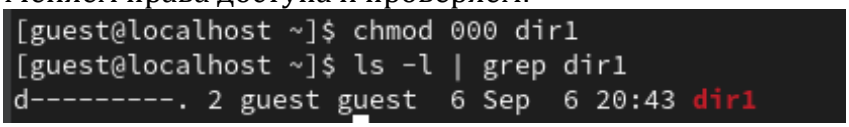
у пользователя *guest* нет прав для исполнения этой команды:

```
[guest@localhost ~]$ sudo lsattr /home

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for guest:
guest is not in the sudoers file.  This incident will be reported.
[guest@localhost ~]$
```

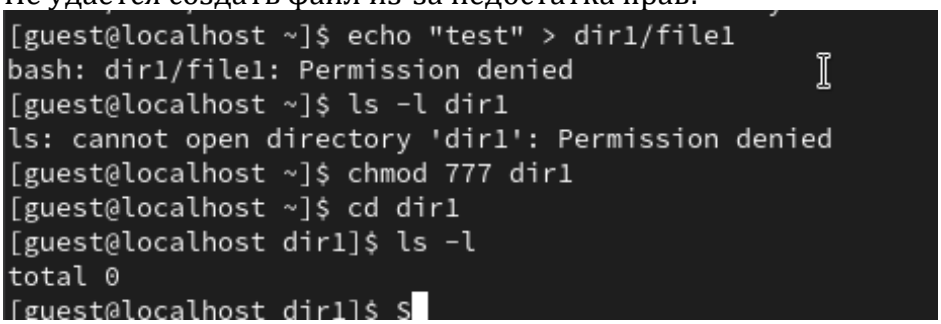


Были выставлены стандартные права для пользователя, исполнение, чтение для группы и исполнение для остальных.

Меняем права доступа и проверяем:



Не удается создать файл из-за недостатка прав:



из-за отстутсвия необходимых прав невозможно даже проверить что на находится внутри дирректории, изменив права убеждаемся, что внутри ничего нет.

Права директории, права файла, создание файла, удаление файла, запись в файл, чтение файла, смена директории, просмотр файлов в директории, премеивание файла, смена атрибутов файла соответственно ниже:

d
(000)
(000) - - - - - - - -
d –x
(100)
(000) - - - - + - - -
d -w-
(200)
(000) - - - - - - - -

d -wx
(300)
(000) + + - - + - + -
d r–
(400)
(000) - - - - - + - -
d r-x
(500)
(000) - - - - + + - -
d rw-
(600)
(000) - - - - - + - -
d rwx
(700)
(000) + + - - + + + -
d
(000)
(100) - - - - - - - -
d –x
(100)
(100) - - - - + - - -
d -w-
(200)
(100) - - - - - - - -
d -wx
(300)
(100) + + - - + - + -
d r–
(400)
(100) - - - - - + - -
d r-x
(500)
(100) - - - - + + - -
d rw-
(600)
(100) - - - - - + - -
d rwx
(700)
(100) + + - - + + + -
d
(000)
(200) - - - - - - - -
d –x
(100)
(200) - - + - + - - -
d -w-
(200)
(200) - - - - - - - -

d -wx
(300)
(200) + + + - + - + -
d r–
(400)
(200) - - - - - + - -
d r-x
(500)
(200) - - + - + + - -
d rw-
(600)
(200) - - - - - + - -
d rwx
(700)
(200) + + + - + + + -
d
(000)
(300) - - - - - - - -
d –x
(100)
(300) - - + - + - - -
d -w-
(200)
(300) - - - - - - - -
d -wx
(300)
(300) + + - + + - + -
d r–
(400)
(300) - - - - - + - -
d r-x
(500)
(300) - - + - + + - -
d rw-
(600)
(300) - - - - - + - -
d rwx
(700)
(300) + + + - + + + -
d
(000)
(400) - - - - - - - -
d –x
(100)
(400) - - - + + - - +
d -w-
(200)
(400) - - - - - - - -

d -wx
(300)
(400) + + - + + - + +
d r–
(400)
(400) - - - - - + - -
d r-x
(500)
(400) - - - + + + - +
d rw-
(600)
(400) - - - - - + - -
d rwx
(700)
(400) + + - + + + + +
d
(000)
(500) - - - - - - - -
d –x
(100)
(500) - - - + + - - +
d -w-
(200)
(500) - - - - - - - -
d -wx
(300)
(500) + + - + + - + +
d r–
(400)
(500) - - - - - + - -
d r-x
(500)
(500) - - - + + + - +
d rw-
(600)
(500) - - - - - + - -
d rwx
(700)
(500) + + - + + + + +
d
(000)
(600) - - - - - - - -
d –x
(100)
(600) - - + + + - - +
d -w-
(200)
(600) - - - - - - - -

d -wx
(300)
(600) + + + + + - + +
d r–
(400)
(600) - - - - - + - -
d r-x
(500)
(600) - - + + + + - +
d rw-
(600)
(600) - - - - - + - -
d rwx
(700)
(600) + + + + + + + +
d
(000)
(700) - - - - - - - -
d –x
(100)
(700) - - + + + - - +
d -w-
(200)
(700) - - - - - - - -
d -wx
(300)
(700) + + + + + - + +
d r–
(400)
(700) - - - - - + - -
d r-x
(500)
(700) - - + + + + - +
d rw-
(600)
(700) - - - - - + - -
d rwx
(700)
(700) + + + + + + + +

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d -wd (300)	(000)
Удаление файла	d -wx (300)	(000)
Чтение файла	d --x (100)	(400)
Запись в файл	d --x (100)	(200)
Переименование файла	d -wx (300)	(000)

Операция	Минимальные права на директорию	Минимальные права на файл
Создание поддиректории	d -wx (300)	(000)
Удаление поддиректории	d -wx (300)	(000)

4 Вывод

В ходе выполнения данной лабораторной работы я приобрела практические навыки работы в консоли с атрибутами файлов, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.