

# Лабораторная работа №2

## Основы информационной безопасности

Подъярова Ксения Витальевна | НПМбд-02-21

### 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.

### Теоретическое введение

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

## 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”. Вошла в систему от имени пользователя guest.

image/Pasted image 20240909175851.png

Командой “pwd” определила, что нахожусь в директории /home/guest, которая и является моей домашней директорией. С приглашением командной строки совпадает. Уточнила имя моего пользователя командой “whoami” и получила вывод: guest. С помощью команды “id” определила имя своего пользователя - всё так же guest, uid = 1001 (guest), gid = 1001 (guest). Затем сравнила полученную информацию с выводом команды “groups”, которая вывела “guest”. Мой пользователь входит только в одну группу, состоящую из него самого, поэтому вывод обеих команд “id” и “groups” совпадает. Данные, выводимые в приглашении командной строки, совпадают с полученной информацией.

```
[guest@kvpodjhyarova ~]$ pwd
/home/guest
[guest@kvpodjhyarova ~]$ whoami
guest
[guest@kvpodjhyarova ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@kvpodjhyarova ~]$ groups
guest
```

Затем просмотрела файл /etc/passwd командой “cat /etc/passwd”. Нашла в нём свою учётную запись в самом конце. Uid = 1001, gid = 1001, то есть они совпадают с тем, что

мы получили ранее.

```
[guest@kvpodjhyarova ~]$ 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
kvpodjhyarova:x:1000:1000:kvpodjhyarova:/home/kvpodjhyarova:/bin/bash
guest:x:1001:1001:/home/guest:/bin/bash
[guest@kvpodjhyarova ~]$
```

Посмотрела, какие директории существуют в системе командой “ls -l /home/” . Список поддиректорий директории /home получить удалось. На директориях установлены права чтения, записи и выполнения для самого пользователя (для группы и остальных пользователей никаких прав доступа не установлено). Проверила, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой “lsattr /home”. Удалось увидеть расширенные атрибуты только директории того пользователя, от имени которого я нахожусь в системе.

```
[guest@kvpodjhyarova ~]$ ls -l /home/
total 8
drwx-----. 14 guest          guest          4096 Sep  9 18:00 guest
drwx-----. 14 kvpodjhyarova kvpodjhyarova 4096 Sep  9 17:10 kvpodjhyarova
[guest@kvpodjhyarova ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/kvpodjhyarova
----- /home/guest
```

Создала в домашней директории поддиректорию dir1 командой “mkdir dir1” и определила, какие права доступа и расширенные атрибуты были на неё выставлены:

чтение, запись и выполнение доступны для самого пользователя и для группы, для остальных - только чтение и выполнение, расширенных атрибутов не установлено

```
[guest@kvpodjhyarova ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@kvpodjhyarova ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
[guest@kvpodjhyarova ~]$ chmod 700 dir1
[guest@kvpodjhyarova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep  9 18:00 Desktop
drwx-----. 2 guest guest 6 Sep  9 18:07 dir1
drwxr-xr-x. 2 guest guest 6 Sep  9 18:00 Documents
drwxr-xr-x. 2 guest guest 6 Sep  9 18:00 Downloads
drwxr-xr-x. 2 guest guest 6 Sep  9 18:00 Music
drwxr-xr-x. 2 guest guest 6 Sep  9 18:00 Pictures
drwxr-xr-x. 2 guest guest 6 Sep  9 18:00 Public
drwxr-xr-x. 2 guest guest 6 Sep  9 18:00 Templates
drwxr-xr-x. 2 guest guest 6 Sep  9 18:00 Videos
[guest@kvpodjhyarova ~]$ ls -l /home/guest/dir1
total 0
[guest@kvpodjhyarova ~]$ cd dir1
[guest@kvpodjhyarova dir1]$ ls
[guest@kvpodjhyarova dir1]$ cd ../
[guest@kvpodjhyarova ~]$ chmod 000 dir1
[guest@kvpodjhyarova ~]$
```

Сняла с директории dir1 все атрибуты командой “chmod 000 dir1” и проверила с её помощью правильность выполнения команды “ls -l”. Действительно, все атрибуты были сняты. Попыталась создать в директории dir1 файл file1 командой echo “test” > /home/guest/dir1/file1. Этого сделать не получилось, т.к. предыдущим действием мы убрали право доступа на запись в директории. В итоге файл не был создан (открыть директорию с помощью команды “ls -l /home/guest/dir1” изначально тоже не удалось по той же причине, поэтому я поменяла права доступа и снова воспользовалась этой командой, и тогда смогла просмотреть содержимое директории, убедившись, что файл не был создан).

Заполним таблицу «Установленные права и разрешённые действия» 2.1. Создание файла: “echo”text” > /home/guest/dir1/file2” Удаление файла: “rm -r /home/guest/dir1/file1” Запись в файл: “echo”textnew” > /home/guest/dir1/file1” Чтение файла: “cat /home/guest/dir1/file1” Смена директории: “cd dir1” Просмотр файлов в директории: “ls dir1” Переименование файла: “mv /home/guest/dir1/file1 filenew” Смена атрибутов файла: “chattr -a /home/guest/dir1/file1”

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)
Создание поддиректории	d -wx (300)	(000)
Удаление поддиректории	d -wx (300)	(000)

## 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.