Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Камкина Арина Леонидовна

Содержание

Цель работы

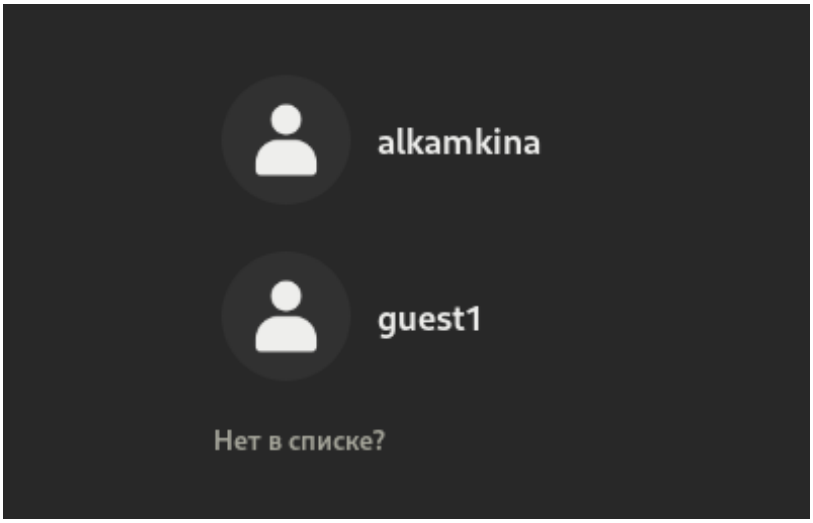
Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Теоретичсекие сведения

Есть 3 вида разрешений. Соответственно, для каждой категории указывается, какие операции с файлом ей доступны: **чтение (r)**, **запись (w)** или **выполнение (x)** — для исполняемых файлов. Для директорий параметры те же, но обозначают немного другое: **просмотр директории (r)**, **создание папок / файлов (w)** внутри директории, **переход в директорию (x)**.

Выполнение лабораторной работы

1. Создала новую учётную запись под именем guest1 и задала для неё пароль, затем вошла в систему под новым именем(рис. [-@fig:001])



Пользователь guest1

2. Командой pwd определила директорию, в которой нахожусь. Сравнив с командной строкой видим, что она совпадает с с именем пользователя, не является домашней директорией.

3. Зашла в домашнюю директоиию, уточнила имя пользователя функцией `whoami` и с помомщью команд `id` и `groups` видим имя пользователя, его id 1002 и группу, в котроую он входит - единственную(рис. [-@fig:002])

```
[guest1@alkamkina ~]$ cd ..
[guest1@alkamkina home]$ whoami
guest1
[guest1@alkamkina home]$ id
uid=1002(guest1) gid=1002(guest1) группы=1002(guest1) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest1@alkamkina home]$ groups
guest1
```

id u groups

4. Просмотрела файл командой `cat /etc/passwd`(рис. [-@fig:003])

```
[guest1@alkamkina home]$ 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
tss:x:59:59:Account used for TPM access:/:/usr/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
geoclue:x:997:995:User for geoclue:/var/lib/geoclue:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/:/sbin/nologin
stapunpriv:x:159:159:systemtap unprivileged user:/var/lib/stapunpriv:/sbin/nologin
libstoragemgmt:x:992:992:daemon account for libstoragemgmt:/:/usr/sbin/nologin
cockpit-wsinstance:x:991:991:User for cockpit-ws instances:/nonexisting:/sbin/nologin
colord:x:990:990:User for colord:/var/lib/colord:/sbin/nologin
sssd:x:989:989:User for sssd:/:/sbin/nologin
clevis:x:988:988:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:987:987:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
pipewire:x:986:986:PipeWire System Daemon:/run/pipewire:/usr/sbin/nologin
flatpak:x:985:985:User for flatpak system helper:/:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:984:983::/run/gnome-initial-setup/:/sbin/nologin
pesign:x:983:982:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
chrony:x:982:981:chrony system user:/var/lib/chrony:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
dnsmasq:x:981:980:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
alkamkina:x:1000:1000:alkamkina:/home/alkamkina:/bin/bash
vboxadd:x:980:1::/var/run/vboxadd:/bin/false
```

Файл passwd

а также нашла в нём свою учетную запись, где увидела группу, которая совпадает с тем, что видела ранее(рис. [-@fig:004])

```
guest1:x:1002:1002::/home/guest1:/bin/bash
```

Учётная запись guest1

5. Определила существующие в системе директории командой `ls -l /home/` - это alkamkina, guest1 (и guest с которым не работали), всеми правами влдеет только владелец. Также посмтотрела какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: `lsattr /home` - никакие расширеные атрибуты не установлены для guest1, для других пользователей просмотр невозможен(рис. [-@fig:005])

```
[guest1@alkamkina home]$ ls -l /home/
итого 8
drwx------. 18 alkamkina alkamkina 4096 сен 13 20:40 alkamkina
drwx------.  3 guest     guest       78 сен 13 20:45 guest
drwx------. 14 guest1    guest1    4096 сен 13 20:55 guest1
[guest1@alkamkina home]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/alkamkina
lsattr: Отказано в доступе While reading flags on /home/guest
---------------------- /home/guest1
[guest1@alkamkina home]$ mkdir dir1
mkdir: невозможно создать каталог «dir1»: Отказано в доступе
```

Права и расширенные атрибуты

6. Создала в домашней директории поддиректорию dir1 командой mkdir dir1. Определила командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию dir1: для владельца доступны все права, для остальных только чтение и вход, никаких расширенных атрибутов не установлено.(рис. [-@fig:006])

```
[guest1@alkamkina home]$ cd
[guest1@alkamkina ~]$ mkdir dir1
[guest1@alkamkina ~]$ ls -l
итого 0
drwxr-xr-x. 2 guest1 guest1 6 сен 13 21:10  dir1
drwxr-xr-x. 2 guest1 guest1 6 сен 13 20:50  Видео
drwxr-xr-x. 2 guest1 guest1 6 сен 13 20:50  Документы
drwxr-xr-x. 2 guest1 guest1 6 сен 13 20:50  Загрузки
drwxr-xr-x. 2 guest1 guest1 6 сен 13 20:50  Изображения
drwxr-xr-x. 2 guest1 guest1 6 сен 13 20:50  Музыка
drwxr-xr-x. 2 guest1 guest1 6 сен 13 20:50  Общедоступные
drwxr-xr-x. 2 guest1 guest1 6 сен 13 20:50 'Рабочий стол'
drwxr-xr-x. 2 guest1 guest1 6 сен 13 20:50  Шаблоны
[guest1@alkamkina ~]$ lsattr
---------------------- ./Рабочий стол
---------------------- ./Загрузки
---------------------- ./Шаблоны
---------------------- ./Общедоступные
---------------------- ./Документы
---------------------- ./Музыка
---------------------- ./Изображения
---------------------- ./Видео
---------------------- ./dir1
```

Поддиректория

7. Сняла с директории dir1 все атрибуты командой chmod 000 dir1 и проверила с её помощью правильность выполнения команды `ls -l`. Попыталась создать в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1`, но не получилось, так как я забрала все права на эту дирректорию - получили

отказ в создании.`ls -l /home/guest/dir1` - просмотр директории также невозможен(рис. [-@fig:007])

```
[guest1@alkamkina ~]$ chmod 000 dir1
[guest1@alkamkina ~]$ ls -l
итого 0
d---------. 2 guest1 guest1 6 сен 13 21:10  dir1
drwxr-xr-x. 2 guest1 guest1 6 сен 13 20:50  Видео
drwxr-xr-x. 2 guest1 guest1 6 сен 13 20:50  Документы
drwxr-xr-x. 2 guest1 guest1 6 сен 13 20:50  Загрузки
drwxr-xr-x. 2 guest1 guest1 6 сен 13 20:50  Изображения
drwxr-xr-x. 2 guest1 guest1 6 сен 13 20:50  Музыка
drwxr-xr-x. 2 guest1 guest1 6 сен 13 20:50  Общедоступные
drwxr-xr-x. 2 guest1 guest1 6 сен 13 20:50 'Рабочий стол'
drwxr-xr-x. 2 guest1 guest1 6 сен 13 20:50  Шаблоны
[guest1@alkamkina ~]$ echo "test" > /home/guest1/dir1
bash: /home/guest1/dir1: Это каталог
[guest1@alkamkina ~]$ echo "test" > /home/guest1/dir1/file1
bash: /home/guest1/dir1/file1: Отказано в доступе
[guest1@alkamkina ~]$ ls - l /home/guest/dir1
ls: невозможно получить доступ к '-': Нет такого файла или каталога
ls: невозможно получить доступ к 'l': Нет такого файла или каталога
ls: невозможно получить доступ к '/home/guest/dir1': Отказано в доступе
[guest1@alkamkina ~]$ ls -l /home/guest/dir1
ls: невозможно получить доступ к '/home/guest/dir1': Отказано в доступе
[guest1@alkamkina ~]$
```

Забрали все права

8. Опытным путём заполила таблицу, меняя права директории и файла(рис. [-@fig:008])

```
[guest1@alkamkina ~]$ chmod 100 dir1
[guest1@alkamkina ~]$ cd dir1
[guest1@alkamkina dir1]$ chmod 000 test
[guest1@alkamkina dir1]$ rm test
rm: удалить защищённый от записи пустой обычный файл 'test'? y
rm: невозможно удалить 'test': Отказано в доступе
[guest1@alkamkina dir1]$ ls
ls: невозможно открыть каталог '.': Отказано в доступе
[guest1@alkamkina dir1]$ echo "test" > test
bash: test: Отказано в доступе
[guest1@alkamkina dir1]$ cat test
cat: test: Отказано в доступе
[guest1@alkamkina dir1]$  mv test test1
mv: невозможно переместить 'test' в 'test1': Отказано в доступе
[guest1@alkamkina dir1]$ touch t
touch: невозможно выполнить touch для 't': Отказано в доступе
[guest1@alkamkina dir1]$ cd
[guest1@alkamkina ~]$ chmod 200 dir1
[guest1@alkamkina ~]$ cd dir1
bash: cd: dir1: Отказано в доступе
[guest1@alkamkina ~]$ chmod 300 dir1
[guest1@alkamkina ~]$ cd dir1
[guest1@alkamkina dir1]$ touch t
[guest1@alkamkina dir1]$ rm t
[guest1@alkamkina dir1]$ ls
ls: невозможно открыть каталог '.': Отказано в доступе
[guest1@alkamkina dir1]$ echo "test" > test
bash: test: Отказано в доступе
[guest1@alkamkina dir1]$ cat test
cat: test: Отказано в доступе
[guest1@alkamkina dir1]$  mv test test1
[guest1@alkamkina dir1]$ cd
[guest1@alkamkina ~]$ chmod 400 dir1
[guest1@alkamkina ~]$ cd dir1
bash: cd: dir1: Отказано в доступе
[guest1@alkamkina ~]$ ls dir1
ls: невозможно получить доступ к 'dir1/test1': Отказано в доступе
test1
[guest1@alkamkina ~]$ chmod 500 dir1
[guest1@alkamkina ~]$ cd dir1
```

Изменение прав доступа к директории

В таблице [-@tbl:tbl1] приведены данные по разрешенным и запрещенным действиям при различных правах: {#tbl:tbl1}

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
d(000)	(000)	-	-	-	-	-	-	-	-
d(100)	(000)	-	-	-	-	+	-	-	+
d(200)	(000)	-	-	-	-	-	-	-	-
d(300)	(000)	+	+	-	-	+	-	+	+
d(400)	(000)	-	-	-	-	-	+	-	-
d(500)	(000)	-	-	-	-	+	+	-	+
d(600)	(000)	-	-	-	-	-	+	-	-
d(700)	(000)	+	+	-	-	+	+	+	+
d(000)	(100)	-	-	-	-	-	-	-	-
d(100)	(100)	-	-	-	-	+	-	-	+
d(200)	(100)	-	-	-	-	-	-	-	-
d(300)	(100)	+	+	-	-	+	-	+	+
d(400)	(100)	-	-	-	-	-	+	-	-
d(500)	(100)	-	-	-	-	+	+	-	+
d(600)	(100)	-	-	-	-	-	+	-	-
d(700)	(100)	+	+	-	-	+	+	+	+
d(000)	(200)	-	-	-	-	-	-	-	-
d(100)	(20	-	-	+	-	+	-	-	+

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
	0)								
d(200)	(200)	-	-	-	-	-	-	-	-
d(300)	(200)	+	+	+	-	+	-	+	+
d(400)	(200)	-	-	-	-	-	+	-	-
d(500)	(200)	-	-	+	-	+	+	-	+
d(600)	(200)	-	-	-	-	-	+	-	-
d(700)	(200)	+	+	+	-	+	+	+	+
d(000)	(300)	-	-	-	-	-	-	-	-
d(100)	(300)	-	-	+	-	+	-	-	+
d(200)	(300)	-	-	-	-	-	-	-	-
d(300)	(300)	+	+	+	-	+	-	+	+
d(400)	(300)	-	-	-	-	-	+	-	-
d(500)	(300)	-	-	+	-	+	+	-	+
d(600)	(300)	-	-	-	-	-	+	-	-
d(700)	(300)	+	+	+	-	+	+	+	+
d(000)	(400)	-	-	-	-	-	-	-	-
d(100)	(400)	-	-	-	+	+	-	-	+
d(200)	(400)	-	-	-	-	-	-	-	-

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
d(300)	(400)	+	+	-	+	+	-	+	+
d(400)	(400)	-	-	-	-	-	+	-	-
d(500)	(400)	-	-	-	+	+	+	-	+
d(600)	(400)	-	-	-	-	-	+	-	-
d(700)	(400)	+	+	-	+	+	+	+	+
d(000)	(500)	-	-	-	-	-	-	-	-
d(100)	(500)	-	-	-	+	+	-	-	+
d(200)	(500)	-	-	-	-	-	-	-	-
d(300)	(500)	+	+	-	+	+	-	+	+
d(400)	(500)	-	-	-	-	-	+	-	-
d(500)	(500)	-	-	-	+	+	+	-	+
d(600)	(500)	-	-	-	-	-	+	-	-
d(700)	(500)	+	+	-	+	+	+	+	+
d(000)	(600)	-	-	-	-	-	-	-	-
d(100)	(600)	-	-	+	+	+	-	-	+
d(200)	(600)	-	-	-	-	-	-	-	-
d(300)	(600)	+	+	+	+	+	-	+	+
d(400)	(60	-	-	-	-	-	+	-	-

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
	0)								
d(500)	(600)	-	-	+	+	+	+	-	+
d(600)	(600)	-	-	-	-	-	+	-	-
d(700)	(600)	+	+	+	+	+	+	+	+
d(000)	(700)	-	-	-	-	-	-	-	-
d(100)	(700)	-	-	+	+	+	-	-	+
d(200)	(700)	-	-	-	-	-	-	-	-
d(300)	(700)	+	+	+	+	+	-	+	+
d(400)	(700)	-	-	-	-	-	+	-	-
d(500)	(700)	-	-	+	+	+	+	-	+
d(600)	(700)	-	-	-	-	-	+	-	-
d(700)	(700)	+	+	+	+	+	+	+	+

В таблице [-@tbl:tbl2]приведены минимальные права для совершения действий: {#tbl:tbl2}

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

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

Вывод

В ходе выполнекния работы 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.