

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Щербак Маргарита Романовна, НПИбд-02-21

2024

Содержание

Цель работы	4
Теоретическое введение	5
Выполнение лабораторной работы	6
Вывод	13
Библиография	14

Список иллюстраций

1	useradd guest и passwd guest	6
2	Выполнение команд	7
3	/etc/passwd	8
4	Выполнение команд	9
5	lsattr /home	9
6	Выполнение команд	10
7	Файл	10
8	Установленные права и разрешённые действия	11
9	Минимальные права для совершения операций	12

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.

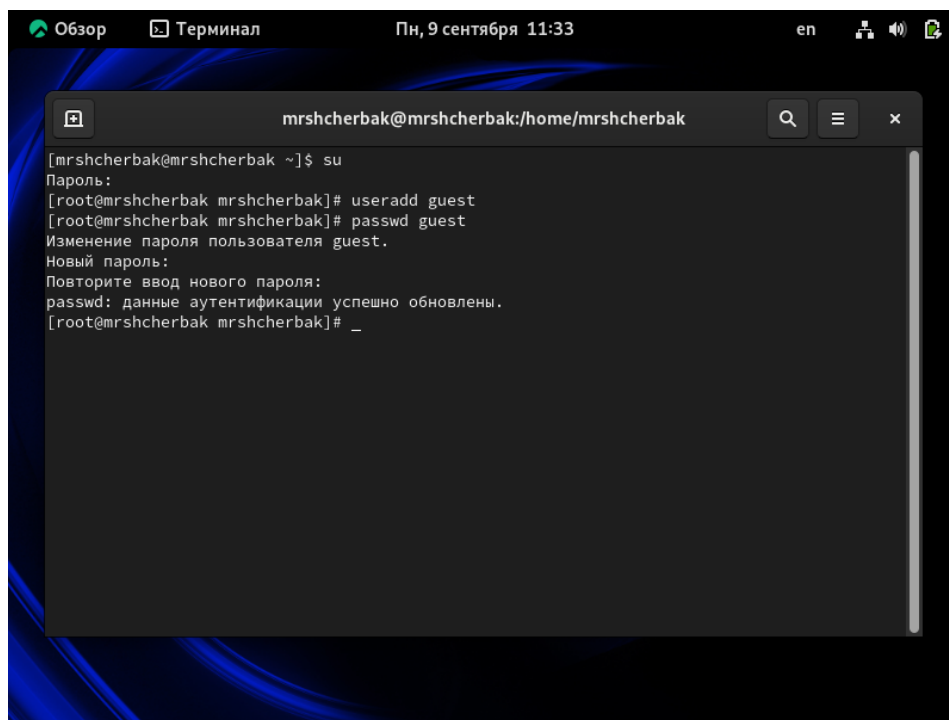
Теоретическое введение

В современных операционных системах безопасность и управление доступом к ресурсам имеют ключевое значение. Одним из базовых механизмов управления доступом является дискреционная модель разграничения доступа (DAC, Discretionary Access Control), которая позволяет владельцу ресурса (например, файла) определять, кто и каким образом может взаимодействовать с этим ресурсом. Этот метод широко используется в ОС с открытым исходным кодом, таких как Linux.

В операционной системе Linux управление правами доступа к файлам осуществляется с помощью атрибутов файлов, которые включают права на чтение, запись и выполнение для трёх категорий пользователей: владельца файла, группы и остальных пользователей. Эти атрибуты могут быть изменены и настроены с помощью команд консоли, что делает консоль важным инструментом для администрирования систем Linux [1].

Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы ОС создадим учётную запись пользователя guest (используя учётную запись администратора).
Зададим пароль для пользователя guest (используя учётную запись администратора)
(рис.1)

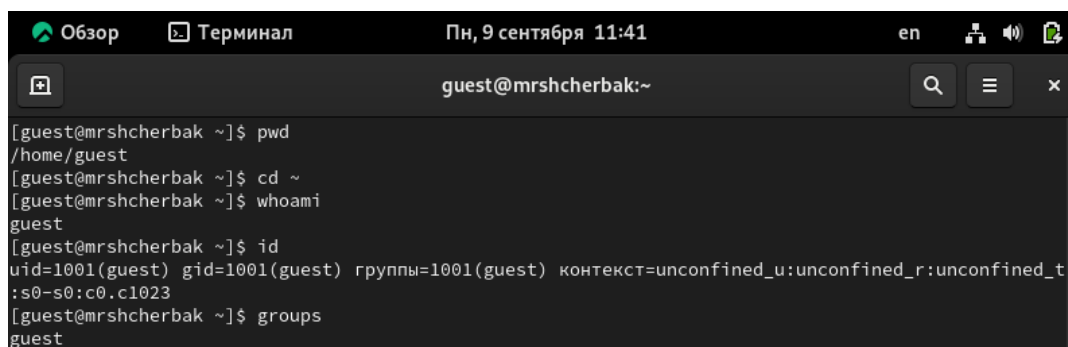


```
Обзор Терминал Пн, 9 сентября 11:33 en
mrshcherbak@mrshcherbak:/home/mrshcherbak
[mrshcherbak@mrshcherbak ~]$ su
Пароль:
[root@mrshcherbak mrshcherbak]# useradd guest
[root@mrshcherbak mrshcherbak]# passwd guest
Изменение пароля пользователя guest.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[root@mrshcherbak mrshcherbak]# _
```

Рис. 1: useradd guest и passwd guest

2. Войдём в систему от имени пользователя guest и определим директорию, в которой находимся, командой pwd. Уточним имя пользователя командой whoami. Уточним

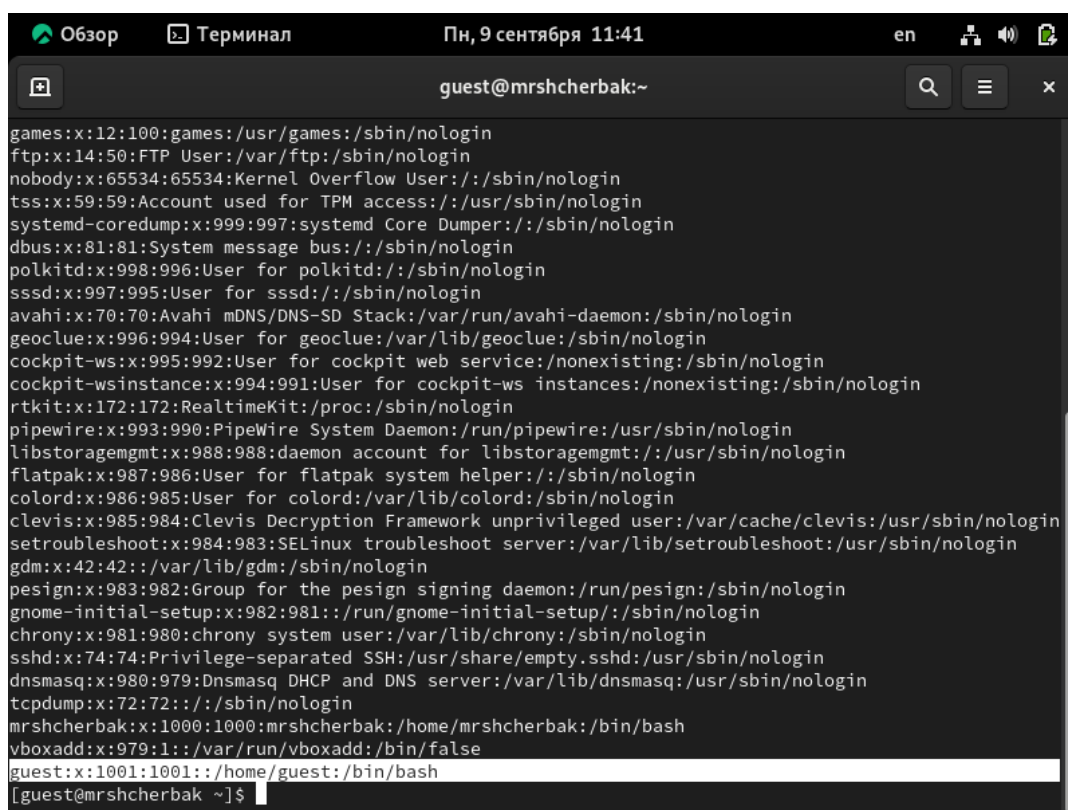
имя пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. запомним. Сравним вывод `id` с выводом команды `groups` (рис.2). Вывод команды `id` совпадает с выводом команды `groups` (`guest`).



```
Обзор Терминал Пн, 9 сентября 11:41 en
guest@mrshcherbak:~
[guest@mrshcherbak ~]$ pwd
/home/guest
[guest@mrshcherbak ~]$ cd ~
[guest@mrshcherbak ~]$ whoami
guest
[guest@mrshcherbak ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t
:s0-s0:c0.c1023
[guest@mrshcherbak ~]$ groups
guest
```

Рис. 2: Выполнение команд

3. Сравним полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки. Данные совпадают. Просмотрим файл `/etc/passwd` командой `cat /etc/passwd`. Найдём в нём свою учётную запись. Определим `uid` пользователя. Определим `gid` пользователя (рис.3). `gid` и `uid` совпадают со значениями из прошлых пунктов.



```
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
sssd:x:997:995:User for sssd:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
geoclue:x:996:994:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:995:992:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:994:991:User for cockpit-ws instances:/nonexisting:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pipewire:x:993:990:PipeWire System Daemon:/run/pipewire:/usr/sbin/nologin
libstoragemgmt:x:988:988:daemon account for libstoragemgmt:/usr/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
chrony:x:981:980:chrony system user:/var/lib/chrony:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
dnsmasq:x:980:979:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72::/sbin/nologin
mrshcherbak:x:1000:1000:mrshcherbak:/home/mrshcherbak:/bin/bash
vboxadd:x:979:1::/var/run/vboxadd:/bin/false
guest:x:1001:1001::/home/guest:/bin/bash
[guest@mrshcherbak ~]$
```

Рис. 3: /etc/passwd

4. Определим существующие в системе директории командой `ls -l /home/` (рис.4).

На директориях установлены права на чтение, запись и выполнение для владельца. Поддиректории `/home - /guest` и `/mrshcherbak`. Проверим, 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. Расширенные атрибуты директориий других пользователей удалось увидеть только от `root`.

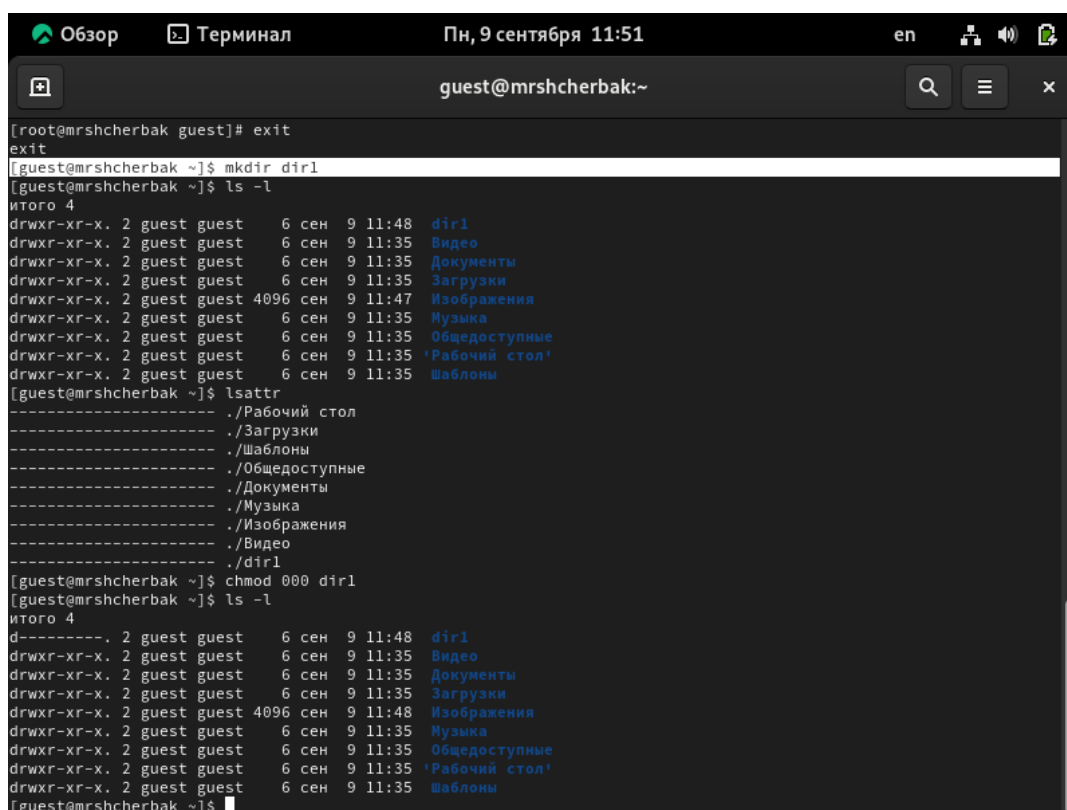

```
[guest@mrshcherbak ~]$ ls -l /home/
итого 8
drwx-----. 14 guest      guest      4096 сен  9 11:38 guest
drwx-----. 15 mrshcherbak mrshcherbak 4096 сен  9 11:33 mrshcherbak
[guest@mrshcherbak ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/mrshcherbak
----- /home/guest
```

Рис. 4: Выполнение команд

```
[guest@mrshcherbak ~]$ su
Пароль:
[root@mrshcherbak guest]# lsattr /home
----- /home/mrshcherbak
----- /home/guest
[root@mrshcherbak guest]#
```

Рис. 5: lsattr /home

5. Создадим в домашней директории поддиректорию dir1 командой `mkdir dir1`. Посмотрим командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию dir1. Снимем с директории dir1 все атрибуты командой `chmod 000 dir1` (рис.6) [2].



```
[root@mrshcherbak guest]# exit
exit
[guest@mrshcherbak ~]$ mkdir dir1
[guest@mrshcherbak ~]$ ls -l
итого 4
drwxr-xr-x. 2 guest guest 6 сен 9 11:48 dir1
drwxr-xr-x. 2 guest guest 6 сен 9 11:35 Видео
drwxr-xr-x. 2 guest guest 6 сен 9 11:35 Документы
drwxr-xr-x. 2 guest guest 6 сен 9 11:35 Загрузки
drwxr-xr-x. 2 guest guest 4096 сен 9 11:47 Изображения
drwxr-xr-x. 2 guest guest 6 сен 9 11:35 Музыка
drwxr-xr-x. 2 guest guest 6 сен 9 11:35 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 9 11:35 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 сен 9 11:35 Шаблоны
[guest@mrshcherbak ~]$ lsattr
----- ./Рабочий стол
----- ./Загрузки
----- ./Шаблоны
----- ./Общедоступные
----- ./Документы
----- ./Музыка
----- ./Изображения
----- ./Видео
----- ./dir1
[guest@mrshcherbak ~]$ chmod 000 dir1
[guest@mrshcherbak ~]$ ls -l
итого 4
d----- . 2 guest guest 6 сен 9 11:48 dir1
drwxr-xr-x. 2 guest guest 6 сен 9 11:35 Видео
drwxr-xr-x. 2 guest guest 6 сен 9 11:35 Документы
drwxr-xr-x. 2 guest guest 6 сен 9 11:35 Загрузки
drwxr-xr-x. 2 guest guest 4096 сен 9 11:48 Изображения
drwxr-xr-x. 2 guest guest 6 сен 9 11:35 Музыка
drwxr-xr-x. 2 guest guest 6 сен 9 11:35 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 9 11:35 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 сен 9 11:35 Шаблоны
[guest@mrshcherbak ~]$
```

Рис. 6: Выполнение команд

6. Попробуем создать в директории dir1 файл file1 командой echo "test" > /home/guest/dir1/file1 (рис.7). Создать файл не получилось, т.к. у папки /dir нет права на запись в неё. Файл file1 в папке /dir не создался.

```
[guest@mrshcherbak ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@mrshcherbak ~]$ ls -l /home/guest/dir1/file1
ls: невозможно получить доступ к '/home/guest/dir1/file1': Отказано в доступе
[guest@mrshcherbak ~]$
```

Рис. 7: Файл

7. Заполним 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, внесём в таблицу знак «+», если не разрешена, знак «-». (рис.8).

Права директо рии	Права файла	Созд ание файла	Удале ние файла	Запи ска файла	Чте ние файла	Смена директо рии	Просмот р файлов в директо рии	Переимено вание файла	Смена атрибу тов файла
d (000)	(000)	-	-	-	-	-	-	-	-
d-x----	(000)	-	-	-	-	+	-	-	+
d (100)	(100)	-	-	-	-	-	-	-	+
d-w-----	(000)	-	-	-	-	-	-	-	-
d-xx-----	(000)	+	+	-	-	+	-	+	+
- d (300)	(000)	-	-	-	-	-	-	-	-
gC-----	(000)	-	-	-	-	-	+	-	-
d (400)	(000)	-	-	-	-	+	-	-	+
gC-x-----	(000)	-	-	-	-	-	+	-	-
d (500)	(000)	-	-	-	-	-	+	-	-
gDx-----	(000)	-	-	-	-	-	+	-	-
d (600)	(000)	+	+	-	-	+	+	+	+
gDxx-----	(000)	+	+	-	-	+	+	+	+
- d (700)	(000)	-	-	-	-	-	-	-	-
d (000)	(100)	-	-	-	-	-	-	-	-
d-x-----	(100)	-	-	-	-	+	-	-	+
d (100)	(100)	-	-	-	-	-	-	-	-
d-w-----	(100)	-	-	-	-	-	-	-	-
d (200)	(100)	-	-	-	-	-	-	-	-
d-xx-----	(100)	+	+	-	-	+	-	+	+
- d (300)	(100)	-	-	-	-	-	-	-	-
gC-----	(100)	-	-	-	-	-	+	-	-
d (400)	(100)	-	-	-	-	+	-	-	+
gC-x-----	(100)	-	-	-	-	-	+	-	-
d (500)	(100)	-	-	-	-	-	+	-	-
gDx-----	(100)	-	-	-	-	-	+	-	-
d (600)	(100)	+	+	-	-	+	+	+	+
gDxx-----	(100)	+	+	-	-	+	+	+	+
- d (700)	(100)	-	-	-	-	-	-	-	-
d (000)	(200)	-	-	-	-	-	-	-	-
d-x-----	(200)	-	-	+	-	+	-	-	+
d (100)	(200)	-	-	-	-	-	-	-	-
d-w-----	(200)	-	-	-	-	-	-	-	-
d (200)	(200)	+	+	+	-	+	-	+	+
d-xx-----	(200)	+	+	+	-	+	-	+	+
- d (300)	(200)	-	-	-	-	-	-	-	-
gC-----	(200)	-	-	-	-	-	+	-	-
d (400)	(200)	-	-	+	-	+	-	-	+
gC-x-----	(200)	-	-	-	-	-	+	-	-
d (500)	(200)	-	-	-	-	-	+	-	-
gDx-----	(200)	-	-	-	-	-	+	-	-
d (600)	(200)	+	+	+	-	+	+	+	+
gDxx-----	(200)	+	+	+	-	+	+	+	+
- d (700)	(200)	-	-	-	-	-	-	-	-
d (000)	(300)	-	-	-	-	-	-	-	-
d-x-----	(300)	-	-	+	-	+	-	-	+
d (100)	(300)	-	-	-	-	-	-	-	-
d-w-----	(300)	-	-	-	-	-	-	-	-
d (200)	(300)	+	+	+	-	+	-	+	+
d-xx-----	(300)	+	+	+	-	+	-	+	+
- d (300)	(300)	-	-	-	-	-	-	-	-
gC-----	(300)	-	-	-	-	-	+	-	-
d (400)	(300)	-	-	+	-	+	-	-	+
gC-x-----	(300)	-	-	-	-	-	+	-	-
d (500)	(300)	-	-	-	-	-	+	-	-
gDx-----	(300)	-	-	-	-	-	+	-	-
d (600)	(300)	+	+	+	-	+	+	+	+
gDxx-----	(300)	+	+	+	-	+	+	+	+
- d (700)	(300)	-	-	-	-	-	-	-	-
d (000)	(400)	-	-	-	-	-	-	-	-
d-x-----	(400)	-	-	+	+	+	-	-	+
d (100)	(400)	-	-	-	-	-	-	-	-
d-w-----	(400)	-	-	-	-	-	-	-	-
d (200)	(400)	+	+	-	+	+	-	+	+
d-xx-----	(400)	+	+	-	+	+	-	+	+
- d (300)	(400)	-	-	-	-	-	-	-	-
gC-----	(400)	-	-	-	-	-	+	-	-
d (400)	(400)	-	-	-	+	+	-	-	+
gC-x-----	(400)	-	-	-	-	-	+	-	-
d (500)	(400)	-	-	-	-	-	+	-	-
gDx-----	(400)	-	-	-	-	-	+	-	-
d (600)	(400)	+	+	-	+	+	+	+	+
gDxx-----	(400)	+	+	-	+	+	+	+	+
- d (700)	(400)	-	-	-	-	-	-	-	-
d (000)	(500)	-	-	-	-	-	-	-	-
d-x-----	(500)	-	-	-	+	+	-	-	+
d (100)	(500)	-	-	-	-	-	-	-	-
d-w-----	(500)	-	-	-	-	-	-	-	-
d (200)	(500)	+	+	-	+	+	-	+	+
d-xx-----	(500)	+	+	-	+	+	-	+	+
- d (300)	(500)	-	-	-	-	-	-	-	-
gC-----	(500)	-	-	-	-	-	+	-	-
d (400)	(500)	-	-	-	+	+	-	-	+
gC-x-----	(500)	-	-	-	-	-	+	-	-
d (500)	(500)	-	-	-	-	-	+	-	-
gDx-----	(500)	-	-	-	-	-	+	-	-
d (600)	(500)	+	+	+	-	+	+	+	+
gDxx-----	(500)	+	+	+	-	+	+	+	+
- d (700)	(500)	-	-	-	-	-	-	-	-
d (000)	(600)	-	-	-	-	-	-	-	-
d-x-----	(600)	-	-	+	+	+	-	-	+
d (100)	(600)	-	-	-	-	-	-	-	-
d-w-----	(600)	-	-	-	-	-	-	-	-
d (200)	(600)	+	+	+	+	+	-	+	+
d-xx-----	(600)	+	+	+	+	+	-	+	+
- d (300)	(600)	-	-	-	-	-	-	-	-
gC-----	(600)	-	-	-	-	-	+	-	-
d (400)	(600)	-	-	+	+	+	-	-	+
gC-x-----	(600)	-	-	-	-	-	+	-	-
d (500)	(600)	-	-	-	-	-	+	-	-
gDx-----	(600)	+	+	+	+	+	+	+	+
gDxx-----	(600)	+	+	+	+	+	+	+	+
- d (700)	(600)	-	-	-	-	-	-	-	-
d (000)	(700)	-	-	-	-	-	-	-	-
d-x-----	(700)	-	-	+	+	+	-	-	+
d (100)	(700)	-	-	-	-	-	-	-	-
d-w-----	(700)	-	-	-	-	-	-	-	-
d (200)	(700)	+	+	+	+	+	-	+	+
d-xx-----	(700)	+	+	+	+	+	-	+	+
- d (300)	(700)	-	-	-	-	-	-	-	-
gC-----	(700)	-	-	-	-	-	+	-	-
d (400)	(700)	-	-	+	+	+	-	-	+
gC-x-----	(700)	-	-	-	-	-	+	-	-
d (500)	(700)	-	-	-	-	-	+	-	-
gDx-----	(700)	+	+	+	+	+	+	+	+
gDxx-----	(700)	+	+	+	+	+	+	+	+
- d (700)	(700)	-	-	-	-	-	-	-	-

Рис. 8: Установленные права и разрешённые действия

8. На основании заполненной таблицы определим те или иные минимально необходимые права для выполнения операций внутри директории dir1 (рис.9).

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

Рис. 9: Минимальные права для совершения операций

Вывод

В ходе ЛР№2 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.

Библиография

1. Методические материалы курса.
2. Chmod. [Электронный ресурс]. М. URL: Файловая система (Дата обращения: 09.09.2024).