

Основы информационной безопасности

**Лабораторная работа № 2. Дискреционное разграничение прав в Linux.
Основные атрибуты**

Смирнов-Мальцев Егор Дмитриевич

Содержание

1	Цель работы	4
2	Теоретическое введение	5
3	Выполнение лабораторной работы	6
4	Выводы	13
	Список литературы	14

Список иллюстраций

3.1	Добавления гостевого пользователя	6
3.2	Домашняя папка гостевого пользователя	6
3.3	Информация о гостевом пользователе	7
3.4	Информация о пользователях	7
3.5	Попытка зайти в домашнюю папку другого пользователя	7
3.6	Создание директории	8
3.7	Создание файла	8

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 Теоретическое введение

Всего есть 2 вида моделей разграничения доступа: дискреционная и мандатная. Эта модель в том или ином виде реализована почти во всех современных *nix-системах. В англоязычных ресурсах можно встретить название DAC (Discretionary Access Control). |

Более подробно про Unix см. в [1–3,[tanenbaum_book_modern-os_ru?](#)].

3 Выполнение лабораторной работы

Добавил гостевого пользователя (рис. 3.1).

```
[edsmirnovmaljce@edsmirnovmaljce ~]$ 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 edsmirnovmaljce:
[edsmirnovmaljce@edsmirnovmaljce ~]$ passwd guest
passwd: Only root can specify a user name.
[edsmirnovmaljce@edsmirnovmaljce ~]$ useradd guest
useradd: user 'guest' already exists
[edsmirnovmaljce@edsmirnovmaljce ~]$ sudo passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
```

Рис. 3.1: Добавления гостевого пользователя

Перешел в учетную запись гостевого пользователя (рис. 3.2).

```
[edsmirnovmaljce@edsmirnovmaljce ~]$ su - guest
Password:
[guest@edsmirnovmaljce ~]$ pwd
/home/guest
```

Рис. 3.2: Домашняя папка гостевого пользователя

Просмотрел кто я, свое id и группу (рис. 3.3).

```

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

```

Рис. 3.3: Информация о гостевом пользователе

Проверил файл /etc/passwd (рис. 3.4).

```

[guest@edsmirnovmaljce ~]$ 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
sssd:x:997:994:User for sssd:/sbin/nologin
libstoragemgmt:x:992:992:daemon account for libstoragemgmt:/usr/sbin/nologin
setroubleshoot:x:991:991:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
cockpit-ws:x:990:990:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:989:989:User for cockpit-ws instances:/nonexisting:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
chrony:x:988:988:chrony system user:/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72:/sbin/nologin
edsmirnovmaljce:x:1000:1000:edsmirnovmaljce:/home/edsmirnovmaljce:/bin/bash
guest:x:1001:1001:/home/guest:/bin/bash

```

Рис. 3.4: Информация о пользователях

Проверил есть ли права на просмотр других директорий (рис. 3.5).

```

[guest@edsmirnovmaljce ~]$ ls -l /home/
total 0
drwx-----. 2 edsmirnovmaljce edsmirnovmaljce 62 Sep 11 12:07 edsmirnovmaljce
drwx-----. 2 guest guest 62 Sep 11 12:59 guest
[guest@edsmirnovmaljce ~]$ ls -l /home/guest
total 0
[guest@edsmirnovmaljce ~]$ ls -l /home/edsmirnovmaljce
ls: cannot open directory '/home/edsmirnovmaljce': Permission denied
[guest@edsmirnovmaljce ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/edsmirnovmaljce
----- /home/guest

```

Рис. 3.5: Попытка зайти в домашнюю папку другого пользователя

Создал директорию и изменил ее права (рис. 3.6).

```
lguest@edsmirnovmaljce ~1$ mkdir dir1
lguest@edsmirnovmaljce ~1$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 11 13:11 dir1
lguest@edsmirnovmaljce ~1$ lsattr
----- ./dir1
lguest@edsmirnovmaljce ~1$ chmod 000 dir1
lguest@edsmirnovmaljce ~1$ ls -l
total 0
d-----. 2 guest guest 6 Sep 11 13:11 dir1
```

Рис. 3.6: Создание директории

Попробовал создать файл в директории (рис. 3.7).

```
lguest@edsmirnovmaljce ~1$ echo "test" > /home/guest/dir1/file1
-bash: /home/guest/dir1/file1: Permission denied
lguest@edsmirnovmaljce ~1$ ls -l dir1
ls: cannot open directory 'dir1': Permission denied
```

Рис. 3.7: Создание файла

В табл. [3.1] приведены данные о том, какие операции разрешены, а какие нет для владельца данных.

Таблица 3.1: Установленные права и разрешённые действия

		Прочитывать		Писать		См. атрибуты		См. метаданные	
		См.	Уда.	Зап.	Чте.	См.	Файл.	Име.	Атриб.
		здание	ление	пись	ние	ди-рек-	ди-рек-	вание	бутов
Права директории	Права файла	файла	файла	в файл	файла	тории	тории	файла	файла
d(000)	(000)	-	-	-	-	-	-	-	-
d(100)	(000)	-	-	-	-	+	-	-	+
d(200)	(000)	-	-	-	-	-	-	-	-
d(300)	(000)	+	+	-	-	+	-	+	+
d(400)	(000)	-	-	-	-	-	+	-	-

Права директории	Права файла	Про- Пе- Сме- смотр ре- на Сме- фай- име- ат- на лов в но- ри- зда- ле- За- Чте- ди- ди- ва- бу- ние ние пись ние рек- рек- ние тов фай- фай- в фай- то- то- фай- фай- ла ла файл ла рии рии ла ла							
		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- рек- то- рии	Про- смотр фай- лов в ди- рек- то- рии	Пе- ре- име- но- ва- ние фай- ла	Сме- на ат- ри- бу- тов фай- ла
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)	(200)	-	-	+	-	+	-	-	+
d(200)	(200)	-	-	-	-	-	-	-	-
d(300)	(200)	+	+	+	-	+	-	+	+
d(400)	(200)	-	-	-	-	-	+	-	-
d(500)	(200)	-	-	+	-	+	+	-	+
d(600)	(200)	-	-	-	-	-	+	-	-
d(700)	(200)	+	+	+	-	+	+	+	+
d(000)	(300)	-	-	-	-	-	-	-	-
d(100)	(300)	-	-	+	-	+	-	-	+

Права директории	Права файла	<div> <div>Про- Пе- Сме-</div> <div>смотр ре- на</div> <div>Сме- фай- име- ат-</div> <div>на лов в но- ри-</div> <div>ди- ди- ва- бу-</div> <div>рек- рек- ние тов</div> </div>							
		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	ди- рек- то- рии	ди- рек- то- рии	фай- ла	фай- ла
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)	-	-	-	-	-	-	-	-
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)	-	-	-	-	-	+	-	-

							Про- смотр	Пе- ре-	Сме- на	
							Сме- на	фай- лов в	име- но-	ат- ри-
		Со- зда- ние	Уда- ле- ние	За- пись	Чте- ние	ди- рек- то-	ди- рек- то-	ва- ние	ри- бу-	
Права директории	Права файла	фай- ла	фай- ла	в файл	фай- ла	рии	рии	фай- ла	фай- ла	
d(700)	(500)	+	+	-	+	+	+	+	+	
d(000)	(600)	-	-	-	-	-	-	-	-	
d(100)	(600)	-	-	+	+	+	-	-	+	
d(200)	(600)	-	-	-	-	-	-	-	-	
d(300)	(600)	+	+	+	+	+	-	+	+	
d(400)	(600)	-	-	-	-	-	+	-	-	
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 табл. [3.2] приведены данные о том, какие минимальные права должны быть для совершения различных действий.

Таблица 3.2: Минимальные права для совершения операций

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 поддиректории	d(300)	(000)
Удаление поддиректории	d(300)	(000)

4 Выводы

Получена информация о доступе к файлам.

Список литературы

1. Robbins A. Bash Pocket Reference. O'Reilly Media, 2016. 156 с.
2. Zarrelli G. Mastering Bash. Packt Publishing, 2017. 502 с.
3. Newham C. Learning the bash Shell: Unix Shell Programming. O'Reilly Media, 2005. 354 с.