

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Крутова Екатерина Дмитриевна

Содержание

Цель работы	5
Выполнение лабораторной работы	6
Выводы	13
Список литературы	14

Список иллюстраций

1	Создание учётной записи пользователя guest	6
2	Пароль пользователя guest	6
3	Вход от имени пользователя guest	6
4	Определение директории (домашняя)	6
5	Имя пользователя	7
6	имя пользователя, его группа, а также группы, куда входит пользователь	7
7	Просмотр файла /etc/passwd	7
8	Существующие в системе директории	7
9	Расширенные атрибуты	8
10	Создание в домашней директории поддиректории dir1	8
11	Снятие с директории dir1 всех атрибутов	8
12	Попытка создать в директории dir1 файл file1	8

Список таблиц

Цель работы

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

Выполнение лабораторной работы

1. Выполнение пунктов (рис. [-@fig:001] - [-@fig:0012]).

```
[edkrutova@edkrutova ~]$ su -  
Password:  
[root@edkrutova ~]# useradd guest  
[root@edkrutova ~]#
```

Рис. 1: Создание учётной записи пользователя guest

```
[root@edkrutova ~]# passwd guest  
Changing password for user guest.  
New password:  
BAD PASSWORD: The password is a palindrome  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@edkrutova ~]#
```

Рис. 2: Пароль пользователя guest

```
[root@edkrutova ~]# su - guest  
[guest@edkrutova ~]$
```

Рис. 3: Вход от имени пользователя guest

```
[guest@edkrutova ~]$ pwd  
/home/guest  
[guest@edkrutova ~]$ -
```

Рис. 4: Определение директории (домашняя)

```
[guest@edkrutova ~]$ whoami
guest
[guest@edkrutova ~]$
```

Рис. 5: Имя пользователя

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

Рис. 6: имя пользователя, его группа, а также группы, куда входит пользователь

Команда `id` вывела больше информации.

```
polkitd:x:998:996:User for polkitd:/usr/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/usr/sbin/nologin
rtkit:x:172:172:RealtimeKit:/usr/sbin/nologin
pipewire:x:997:994:PipeWire System Daemon:/usr/sbin/nologin
sssd:x:996:993:User for sssd:/usr/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:/usr/lib/geoclue:/usr/sbin/nologin
cockpit-ws:x:989:988:User for cockpit web service:/usr/sbin/nologin
cockpit-wsinstance:x:988:987:User for cockpit-ws instances:/usr/sbin/nologin
flatpak:x:987:986:User for flatpak system helper:/usr/sbin/nologin
colord:x:986:985:User for colord:/usr/lib/colord:/usr/sbin/nologin
clevis:x:985:984:Clevis Decryption Framework unprivileged user:/usr/sbin/nologin
setroubleshoot:x:984:983:SELinux troubleshoot server:/usr/lib/setroubleshoot:/usr/sbin/nologin
gdm:x:42:42:/usr/lib/gdm:/usr/sbin/nologin
gnome-initial-setup:x:983:982:/usr/bin/gnome-initial-setup:/usr/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
chrony:x:982:981:chrony system user:/usr/lib/chrony:/usr/sbin/nologin
dnsmasq:x:981:980:Dnsmasq DHCP and DNS server:/usr/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/usr/sbin/nologin
edkrutova:x:1000:1000:edkrutova:/home/edkrutova:/bin/bash
guest:x:1001:1001:/home/guest:/bin/bash
[guest@edkrutova ~]$
```

Рис. 7: Просмотр файла `/etc/passwd`

`uid` пользователя 1001, `gid` пользователя 1001, совпадает.

```
[guest@edkrutova ~]$ ls -l /home/
total 4
drwx-----, 14 edkrutova edkrutova 4096 Sep  7 17:15 edkrutova
drwx-----,  4 guest      guest    92 Sep 14 19:10 guest
[guest@edkrutova ~]$
```

Рис. 8: Существующие в системе директории

Права 700

```
[guest@edkrutova ~]$ lsattr /home/  
lsattr: Permission denied While reading flags on /home/edkrutova  
----- /home/guest  
[guest@edkrutova ~]$
```

Рис. 9: Расширенные атрибуты

```
[guest@edkrutova ~]$ mkdir dir1  
[guest@edkrutova ~]$ ls -l dir1/  
total 0  
[guest@edkrutova ~]$ lsattr dir1/
```

Рис. 10: Создание в домашней директории поддиректории dir1

```
[guest@edkrutova ~]$ chmod 000 dir1/  
[guest@edkrutova ~]$ ls -l dir1/  
ls: cannot open directory 'dir1/': Permission denied  
[guest@edkrutova ~]$
```

Рис. 11: Снятие с директории dir1 всех атрибутов

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

Рис. 12: Попытка создать в директории dir1 файл file1

Отказано в доступе

2. Заполненные таблицы

Права дирек- тории	Права файла	Созда- ние файла	Удале- ние файла	За- пись в файл	Чте- ние файла	Смена дирек- тории	Про- смотр фай- лов в дирек- тории	Переиме- нование файла	Смена атри- бутов файла
d(000)	(000)	-	-	-	-	-	-	-	-
d(000)	(100)	-	-	-	-	-	-	-	-
d(000)	(200)	-	-	-	-	-	-	-	-
d(000)	(300)	-	-	-	-	-	-	-	-
d(000)	(400)	-	-	-	-	-	-	-	-
d(000)	(500)	-	-	-	-	-	-	-	-
d(000)	(600)	-	-	-	-	-	-	-	-
d(000)	(700)	-	-	-	-	-	-	-	-
d(100)	(000)	-	-	-	-	+	-	-	+
d(100)	(100)	-	-	-	-	+	-	-	+
d(100)	(200)	-	-	+	-	+	-	-	+
d(100)	(300)	-	-	+	-	+	-	-	+
d(100)	(400)	-	-	-	+	+	-	-	+
d(100)	(500)	-	-	-	+	+	-	-	+
d(100)	(600)	-	-	+	+	+	-	-	+
d(100)	(700)	-	-	+	+	+	-	-	+
d(200)	(000)	-	-	-	-	-	-	-	-
d(200)	(100)	-	-	-	-	-	-	-	-
d(200)	(200)	-	-	-	-	-	-	-	-
d(200)	(300)	-	-	-	-	-	-	-	-
d(200)	(400)	-	-	-	-	-	-	-	-
d(200)	(500)	-	-	-	-	-	-	-	-

d(200)	(600)	-	-	-	-	-	-	-	-
d(200)	(700)	-	-	-	-	-	-	-	-
d(300)	(000)	+	+	-	-	+	-	+	+
d(300)	(100)	+	+	-	-	+	-	+	+
d(300)	(200)	+	+	+	-	+	-	+	+
d(300)	(300)	+	+	+	-	+	-	+	+
d(300)	(400)	+	+	-	+	+	-	+	+
d(300)	(500)	+	+	-	+	+	-	+	+
d(300)	(600)	+	+	+	+	+	-	+	+
d(300)	(700)	+	+	+	+	+	-	+	+
d(400)	(000)	-	-	-	-	-	+	-	-
d(400)	(100)	-	-	-	-	-	+	-	-
d(400)	(200)	-	-	-	-	-	+	-	-
d(400)	(300)	-	-	-	-	-	+	-	-
d(400)	(400)	-	-	-	-	-	+	-	-
d(400)	(500)	-	-	-	-	-	+	-	-
d(400)	(600)	-	-	-	-	-	+	-	-
d(400)	(700)	-	-	-	-	-	+	-	-
d(500)	(000)	-	-	-	-	+	+	-	+
d(500)	(100)	-	-	-	-	+	+	-	+
d(500)	(200)	-	-	+	-	+	+	-	+
d(500)	(300)	-	-	+	-	+	+	-	+
d(500)	(400)	-	-	-	+	+	+	-	+
d(500)	(500)	-	-	-	+	+	+	-	+
d(500)	(600)	-	-	+	+	+	+	-	+
d(500)	(700)	-	-	+	+	+	+	-	+
d(600)	(000)	-	-	-	-	-	+	-	-
d(600)	(100)	-	-	-	-	-	+	-	-

d(600)	(200)	-	-	-	-	-	+	-	-
d(600)	(300)	-	-	-	-	-	+	-	-
d(600)	(400)	-	-	-	-	-	+	-	-
d(600)	(500)	-	-	-	-	-	+	-	-
d(600)	(600)	-	-	-	-	-	+	-	-
d(600)	(700)	-	-	-	-	-	+	-	-
d(700)	(000)	+	+	-	-	+	+	+	+
d(700)	(100)	+	+	-	-	+	+	+	+
d(700)	(200)	+	+	+	-	+	+	+	+
d(700)	(300)	+	+	+	-	+	+	+	+
d(700)	(400)	+	+	-	+	+	+	+	+
d(700)	(500)	+	+	-	+	+	+	+	+
d(700)	(600)	+	+	+	+	+	+	+	+
d(700)	(700)	+	+	+	+	+	+	+	+

Таблица 2.1 «Установленные права и разрешённые действия»

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)
Переименова- ние файла	d(300)	(000)
Создание поддиректории	d(300)	(000)

Удаление	d(300)	(000)
поддиректории		

Таблица 2.2 “Минимальные права для совершения операций”

Выводы

Я приобрела практические навыки работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы