

Отчет по лабораторной работе №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Юрченко Артём Алексеевич

Содержание

1	Цель работы	5
1.1	### Целью данной работы является 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	5
2	Ход работы	6
3	Библиография	13
3.0.1	Методические материалы https://esystem.rudn.ru/pluginfile.php/2090273/mod_reslab_discret_attr.pdf	13

Список иллюстраций

2.1	Создание учетной записи пользователя guest	6
2.2	Создание пароля для учетной записи	6
2.3	Определение директории	7
2.4	Уточнение имени пользователя	7
2.5	Использование команды id	7
2.6	Вывод команды groups	7
2.7	Просмотр файла	8
2.8	Список поддиректорий	8
2.9	Проверка команды	8
2.10	Использование команды ls -l	9
2.11	Использование команды lsattr	9
2.12	Использование команды chmod	10
2.13	Создание файла в директории	10
2.14	Таблица «Установленные права и разрешённые действия»	11
2.15	Таблица “Минимальные права для совершения операций”	12

Список таблиц

1 Цель работы

1.1 ### Целью данной работы является 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 Ход работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создал учётную запись пользователя guest (используя учётную запись администратора) (рис. 2.1)

```
[temau@localhost ~]$ su
Пароль:
[root@localhost temau]# useradd guest
```

Рис. 2.1: Создание учетной записи пользователя guest

2. Задал пароль для пользователя guest (используя учётную запись администратора)(рис. 2.2)

```
[root@localhost temau]# passwd guest
Изменение пароля пользователя guest.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
```

Рис. 2.2: Создание пароля для учетной записи

3. Вошёл в систему от имени пользователя guest.
4. Определил директорию, в которой нахожусь, командой pwd. Определил, что она является домашней (рис. 2.3)

```
[guest@localhost ~]$ pwd
/home/guest
```

Рис. 2.3: Определение директории

5. Уточнил имя пользователя командой `whoami` (рис. 2.4)

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

Рис. 2.4: Уточнение имени пользователя

6. Уточнил имя пользователя, его группу, а также группы, куда входит пользователь, командой `id`. (рис. 2.5)

```
[guest@localhost ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
```

Рис. 2.5: Использование команды `id`

7. Сравнил вывод `id` с выводом команды `groups`. Выяснил, что на эту команду выводить только имя пользователя (рис. 2.6)

```
[guest@localhost ~]$ groups
guest
```

Рис. 2.6: Вывод команды `groups`

8. Просмотрел файл `/etc/passwd` командой `cat` и нашел в нем свою учетную запись. Определил `uid`, `gid` пользователя. Сравнил найденные значения с полученными в предыдущих пунктах. Они совпали. (рис. 2.7)

```
[guest@localhost ~]$ 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
sssd:x:997:993:User for sssd:/sbin/nologin
pipewire:x:996:992:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
libstoragemgmt:x:990:990:daemon account for libstoragemgmt:/usr/sbin/nologin
systemd-oom:x:989:989:systemd Userspace OOM Killer:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
geoclue:x:988:987:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:987:986:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:986:985:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:985:984:User for flatpak system helper:/sbin/nologin
colord:x:984:983:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:983:982:CLEVIS Decryption Framework unprivileged user:/var/cache/levis:/usr/sbin/nologin
setroubleshoot:x:982:981:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
design:x:981:980:Group for the design signing daemon:/run/design:/sbin/nologin
gnome-initial-setup:x:980:979:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:979:978:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:978:977:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72:/sbin/nologin
temau:x:1000:1000:temau:/home/temau:/bin/bash
guest:x:1001:1001:/home/guest:/bin/bash
```

Рис. 2.7: Просмотр файла

9. Определил существующие в системе директории командой `ls -l /home/` (рис. 2.8)

```
[guest@localhost ~]$ ls -l /home/
итого 8
drwx-----. 14 guest guest 4096 сен 16 18:00 guest
drwx-----. 14 temau temau 4096 сен 16 17:30 temau
```

Рис. 2.8: Список поддиректорий

10. Проверил, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой: `lsattr /home` (рис. 2.9). Так как данные права есть у администратора, информацию получить не удалось.

```
guest@localhost ~]$ lsattr /home
lsattr: Отказано в доступе while reading flags on /home/temau
----- /home/guest
guest@localhost ~]$
```

Рис. 2.9: Проверка команды

11. Создал в домашней директории поддиректорию dir1 командой `mkdir dir1`
Определил командами `ls -l` (рис. 2.10) и `lsattr` (рис. 2.11), какие права доступа и расширенные атрибуты были выставлены на директорию dir1.

```
[guest@localhost ~]$ ls -l
итого 0
drwxr-xr-x. 2 guest guest 6 сен 16 18:04 dir1
drwxr-xr-x. 2 guest guest 6 сен 16 18:00 Видео
drwxr-xr-x. 2 guest guest 6 сен 16 18:00 Документы
drwxr-xr-x. 2 guest guest 6 сен 16 18:00 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 16 18:00 Изображения
drwxr-xr-x. 2 guest guest 6 сен 16 18:00 Музыка
drwxr-xr-x. 2 guest guest 6 сен 16 18:00 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 16 18:00 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 сен 16 18:00 Шаблоны
```

Рис. 2.10: Использование команды `ls -l`

```
[guest@localhost ~]$ lsattr
----- ./Рабочий стол
----- ./Загрузки
----- ./Шаблоны
----- ./Общедоступные
----- ./Документы
----- ./Музыка
----- ./Изображения
----- ./Видео
----- ./dir1
```

Рис. 2.11: Использование команды `lsattr`

12. Снял с директории dir1 все атрибуты командой `chmod 000 dir1` и проверил с её помощью правильность выполнения команды `ls -l` (рис. 2.12)

```
[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$ ls -l
итого 0
d----- . 2 guest guest 6 сен 16 18:04 dir1
drwxr-xr-x. 2 guest guest 6 сен 16 18:00 Видео
drwxr-xr-x. 2 guest guest 6 сен 16 18:00 Документы
drwxr-xr-x. 2 guest guest 6 сен 16 18:00 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 16 18:00 Изображения
drwxr-xr-x. 2 guest guest 6 сен 16 18:00 Музыка
drwxr-xr-x. 2 guest guest 6 сен 16 18:00 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 16 18:00 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 сен 16 18:00 Шаблоны
```

Рис. 2.12: Использование команды chmod

13. Попытался создать в директории dir1 файл file1 командой echo "test" > /home/guest/dir1/file1 (рис. 2.13)

```
[guest@localhost ~]$ echo "test1" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
```

Рис. 2.13: Создание файла в директории

14. Заполнил 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, записал в таблицу знак «+», если не разрешена, знак «-».

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

Рис. 2.14: Таблица «Установленные права и разрешённые действия»

15. На основании заполненной выше таблицы определил те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполнил следующую таблицу:

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. 2.15: Таблица “Минимальные права для совершения операций”

3 Библиография

3.0.1 Методические материалы

https://esystem.rudn.ru/pluginfile.php/2090273/mod_resource/content/6/002lab_discret_attr.pdf