

Отчет по лабораторной работе №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Поленикова Анна Алексеевна

Содержание

Цель работы	4
Выполнение лабораторной работы	5
Вывод	11

Список иллюстраций

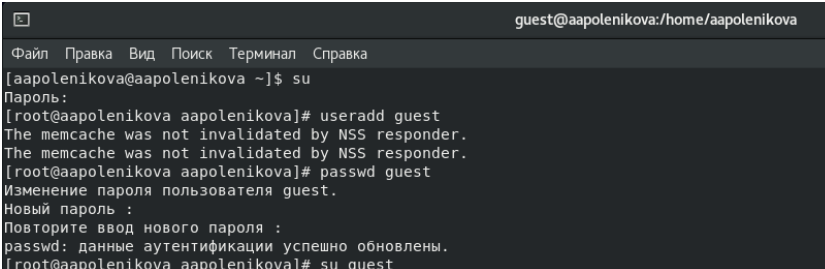
0.1	Создание учетной записи пользователя guest и вход	5
0.2	Информация о пользователе guest	6
0.3	Содержимое файла /etc/passwd	6
0.4	Расширенные атрибуты	6
0.5	Работа с директорией dir1	7

Цель работы

Цель лабораторной работы №2 - 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.

Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создали учётную запись пользователя guest (используя учётную запись администратора) с помощью команды `useradd guest` и задали пароль для пользователя guest (используя учётную запись администратора) с помощью команды `passwd guest`.
2. Вошли в систему от имени пользователя guest

A screenshot of a terminal window with a dark background. The title bar shows 'guest@aapolenikova:/home/aapolenikova'. The terminal content shows a sequence of commands and their outputs: a user switches to root via 'su', then runs 'useradd guest' (which shows memcache warnings), then 'passwd guest' (which prompts for and sets a password), and finally switches back to the guest user with 'su guest'.

```
guest@aapolenikova:/home/aapolenikova
Файл Правка Вид Поиск Терминал Справка
[aapolenikova@aapolenikova ~]$ su
Пароль:
[root@aapolenikova aapolenikova]# useradd guest
The memcache was not invalidated by NSS responder.
The memcache was not invalidated by NSS responder.
[root@aapolenikova aapolenikova]# passwd guest
Изменение пароля пользователя guest.
Новый пароль :
Повторите ввод нового пароля :
passwd: данные аутентификации успешно обновлены.
[root@aapolenikova aapolenikova]# su guest
```

Рис. 0.1: Создание учетной записи пользователя guest и вход

3. Командой `pwd` определили директорию, в которой находимся и определили является ли она домашней директорией.
4. Уточнили имя пользователя командой `whoami`.
5. Уточнили имя пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Сравнили вывод `id` с выводом команды `groups`. Видим, что `uid`, `gid` и группы = 1001(guest)

```
[guest@aapolenikova aapolenikova]$ whoami
guest
[guest@aapolenikova aapolenikova]$ id
uid=1001(guest) gid=1001(guest) rгруппы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@aapolenikova aapolenikova]$ groups
guest
```

Рис. 0.2: Информация о пользователе guest

6. Сравнили полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки и убедились, что они совпадают.
7. Просмотрели файл `/etc/passwd` с помощью команды `cat /etc/passwd`. Нашли в нём свою учётную запись. Определили `uid` и `gid` пользователя. Guest имеет те же идентификаторы 1001, которые также были получены в предыдущих пунктах.

```
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
aapolenikova:x:1000:1000:aapolenikova:/home/aapolenikova:/bin/bash
quest:x:1001:1001:./home/guest:/bin/bash
```

Рис. 0.3: Содержимое файла `/etc/passwd`

8. Определили существующие в системе директории командой `ls -l /home/`
9. Проверили, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой: `lsattr /home`. Нам не удалось увидеть расширенные атрибуты директорий других пользователей, только своей домашней директории.

```
[guest@aapolenikova aapolenikova]$ ls -l /home/
итого 4
drwx----- 15 aapolenikova aapolenikova 4096 окт  2 13:23 aapolenikova
drwx-----  3 guest      guest      78 окт  2 13:57 guest
[guest@aapolenikova aapolenikova]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/aapolenikova
----- /home/guest
```

Рис. 0.4: Расширенные атрибуты

10. Создали в домашней директории поддиректорию `dir1` командой `mkdir dir1`. Определили с помощью команд `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`.

11. Сняли с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверили с `ls -l` помощью правильность выполнения предыдущей команды.
12. Попытались создать в директории `dir1` файл `file1` командой `echo "test" > /home/guest/dir1/file1`. Поскольку ранее мы отозвали все атрибуты, то тем самым лишили пользователя всех прав на взаимодействие с `dir1`, в том числе и на создание файлов.

```
[guest@aapolenikova aapolenikova]$ mkdir /home/guest/dir1
[guest@aapolenikova aapolenikova]$ ls -l /home/guest
итого 0
drwxrwxr-x. 2 guest guest 6 окт  2 15:29 dir1
[guest@aapolenikova aapolenikova]$ lsattr /home/guest
----- /home/guest/dir1
[guest@aapolenikova aapolenikova]$ chmod 000 /home/guest/dir1
[guest@aapolenikova aapolenikova]$ ls -l /home/guest
итого 0
d----- . 2 guest guest 6 окт  2 15:29 dir1
[guest@aapolenikova aapolenikova]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@aapolenikova aapolenikova]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе
[guest@aapolenikova aapolenikova]$
```

Рис. 0.5: Работа с директорией `dir1`

13. Заполним таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определим опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, заносим в таблицу знак «+», если не разрешена, знак «-».

- 1 - Создание файла
- 2- Удаление файла
- 3- Запись в файл
- 4- Чтение файла
- 5- Смена директории
- 6- Просмотр файлов в директории
- 7 - Переименование файла
- 8- Смена атрибутов файла

Таблица 0.1: Установленные права и разрешённые действия {#tbl:rig-act}

Права директории	Права файла	1	2	3	4	5	6	7	8
d-----(000)	-----(000)	-	-	-	-	-	-	-	-
d--x-----(100)	-----(000)	-	-	-	-	+	-	-	+
d-w-----(200)	-----(000)	-	-	-	-	-	-	-	-
d-wx-----(300)	-----(000)	+	+	-	-	+	-	+	+
dr-----(400)	-----(000)	-	-	-	-	-	-	-	-
dr-x-----(500)	-----(000)	-	-	-	-	+	+	-	+
drw-----(600)	-----(000)	-	-	-	-	-	-	-	-
drwx-----(700)	-----(000)	+	+	-	-	+	+	+	+
d-----x(000)	---x-----(100)	-	-	-	-	-	-	-	-
d--x-----x(100)	---x-----x(100)	-	-	-	-	+	-	-	+
d-w-----x(200)	---x-----x(100)	-	-	-	-	-	-	-	-
d-wx-----x(300)	---x-----x(100)	+	+	-	-	+	-	+	+
dr-----x(400)	---x-----x(100)	-	-	-	-	-	-	-	-
dr-x-----x(500)	---x-----x(100)	-	-	-	-	+	+	-	+
drw-----x(600)	---x-----x(100)	-	-	-	-	-	-	-	-
drwx-----x(700)	---x-----x(100)	+	+	-	-	+	+	+	+
d-----w(000)	--w-----x(200)	-	-	-	-	-	-	-	-
d--x-----w(100)	--w-----x(200)	-	-	+	-	+	-	-	+
d-w-----w(200)	--w-----x(200)	-	-	-	-	-	-	-	-
d-wx-----w(300)	--w-----x(200)	+	+	+	-	+	-	+	+
dr-----w(400)	--w-----x(200)	-	-	-	-	-	-	-	-
dr-x-----w(500)	--w-----x(200)	-	-	+	-	+	+	-	+
drw-----w(600)	--w-----x(200)	-	-	-	-	-	-	-	-
drwx-----w(700)	--w-----x(200)	+	+	+	-	+	+	+	+
d-----wx(000)	--wx-----x(300)	-	-	-	-	-	-	-	-
d--x-----wx(100)	--wx-----x(300)	-	-	+	-	+	-	-	+

Права директории	Права файла	1	2	3	4	5	6	7	8
d-w-----(200)	--wx-----(300)	-	-	-	-	-	-	-	-
d-wx-----(300)	--wx-----(300)	+	+	+	-	+	-	+	+
dr----- (400)	--wx-----(300)	-	-	-	-	-	-	-	-
dr-x----- (500)	--wx-----(300)	-	-	+	-	+	+	-	+
drw----- (600)	--wx-----(300)	-	-	-	-	-	-	-	-
drwx----- (700)	--wx-----(300)	+	+	+	-	+	+	+	+
d----- (000)	-r----- (400)	-	-	-	-	-	-	-	-
d--x----- (100)	-r----- (400)	-	-	-	+	+	-	-	+
d-w----- (200)	-r----- (400)	-	-	-	-	-	-	-	-
d-wx----- (300)	-r----- (400)	+	+	-	+	+	-	+	+
dr----- (400)	-r----- (400)	-	-	-	-	-	-	-	-
dr-x----- (500)	-r----- (400)	-	-	-	+	+	+	-	+
drw----- (600)	-r----- (400)	-	-	-	-	-	-	-	-
drwx----- (700)	-r----- (400)	+	+	-	+	+	+	+	+
d----- (000)	-r-x----- (500)	-	-	-	-	-	-	-	-
d--x----- (100)	-r-x----- (500)	-	-	-	+	+	-	-	+
d-w----- (200)	-r-x----- (500)	-	-	-	-	-	-	-	-
d-wx----- (300)	-r-x----- (500)	+	+	-	+	+	-	+	+
dr----- (400)	-r-x----- (500)	-	-	-	-	-	-	-	-
dr-x----- (500)	-r-x----- (500)	-	-	-	+	+	+	-	+
drw----- (600)	-r-x----- (500)	-	-	-	-	-	-	-	-
drwx----- (700)	-r-x----- (500)	+	+	-	+	+	+	+	+
d----- (000)	-rw----- (600)	-	-	-	-	-	-	-	-
d--x----- (100)	-rw----- (600)	-	-	+	+	+	-	-	+
d-w----- (200)	-rw----- (600)	-	-	-	-	-	-	-	-
d-wx----- (300)	-rw----- (600)	+	+	+	+	+	-	+	+
dr----- (400)	-rw----- (600)	-	-	-	-	-	-	-	-
dr-x----- (500)	-rw----- (600)	-	-	+	+	+	+	-	+

Права директории	Права файла	1	2	3	4	5	6	7	8
drw-----(600)	-rw-----(600)	-	-	-	-	-	-	-	-
drwx-----(700)	-rw-----(600)	+	+	+	+	+	+	+	+
d----- (000)	-rwx----- (700)	-	-	-	-	-	-	-	-
d--x----- (100)	-rwx----- (700)	-	-	+	+	+	-	-	+
d-w----- (200)	-rwx----- (700)	-	-	-	-	-	-	-	-
d-wx----- (300)	-rwx----- (700)	+	+	+	+	+	-	+	+
dr----- (400)	-rwx----- (700)	-	-	-	-	-	-	-	-
dr-x----- (500)	-rwx----- (700)	-	-	+	+	+	+	-	+
drw----- (600)	-rwx----- (700)	-	-	-	-	-	-	-	-
drwx----- (700)	-rwx----- (700)	+	+	+	+	+	+	+	+

На основании таблицы выше определили минимально необходимые права для выполнения операций внутри директории `dir1` и заполнили таблицу `[-@tbl:min-rig]`. Для заполнения последних двух строк опытным путем проверили минимальные права.

Таблица 0.2: Минимальные права для совершения операций `{#tbl:min-rig}`

Операция	Права на директорию	Права на файл
Создание файла	d-wx----- (300)	----- (000)
Удаление файла	d-wx----- (300)	----- (000)
Чтение файла	d--x----- (100)	-r----- (400)
Запись в файл	d--x----- (100)	--w----- (200)
Переименование файла	d-wx----- (300)	----- (000)
Создание поддиректории	d-wx----- (300)	----- (000)
Удаление поддиректории	d-wx----- (300)	----- (000)

Вывод

В ходе выполнения лабораторной работы были получены практические навыки работы в консоли с атрибутами файлов, а также закреплены теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.