

Отчёт по лабораторной работе №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Дарья Эдуардовна Ибатулина

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	8
4	Выполнение лабораторной работы	10
5	Выводы	17
	Список литературы	18

Список иллюстраций

4.1	Создание учётной записи нового пользователя	10
4.2	Здание пароля нового пользователя	10
4.3	Вход в систему под пользователем <i>guest</i>	10
4.4	Определение текущей директории	11
4.5	Определение имени текущего пользователя	11
4.6	Уточнение имени пользователя, его группы и других групп, в кото- рые он входит	11
4.7	Просмотр файла <i>/etc/passwd</i>	11
4.8	Существующие в системе директории	12
4.9	Проверка расширенных атрибутов	12
4.10	Создание новой директории, просмотр прав доступа и расширен- ных атрибутов на неё	12
4.11	Снятие всех атрибутов с новой директории	13
4.12	Попытка создания файла в новой директории	13

Список таблиц

4.1	Установленные права и разрешённые действия	13
4.1	Установленные права и разрешённые действия	14
4.1	Установленные права и разрешённые действия	15
4.1	Установленные права и разрешённые действия	16
4.2	Минимальные права для совершения операций	16

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 Задание

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создайте учётную запись пользователя `guest` (используя учётную запись администратора): `useradd guest`
2. Задайте пароль для пользователя `guest` (используя учётную запись администратора): `passwd guest`
3. Войдите в систему от имени пользователя `guest`.
4. Определите директорию, в которой вы находитесь, командой `pwd`. Сравните её с приглашением командной строки. Определите, является ли она вашей домашней директорией? Если нет, зайдите в домашнюю директорию.
5. Уточните имя вашего пользователя командой `whoami`.
6. Уточните имя вашего пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. запомните. Сравните вывод `id` с выводом команды `groups`.
7. Сравните полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки.
8. Просмотрите файл `/etc/passwd` командой `cat /etc/passwd`. Найдите в нём свою учётную запись. Определите `uid` пользователя. Определите `gid` пользователя. Сравните найденные значения с полученными в предыдущих пунктах. Замечание: в случае, когда вывод команды не умещается на одном экране монитора, используйте прокрутку вверх–вниз (удерживая клавишу `shift`, нажимайте `page up` и `page down`) либо качестве фильтра для вывода только строк, содержащих определённые буквенные сочетания: `cat`

`/etc/passwd | grep guest`

9. Определите существующие в системе директории командой `ls -l /home/`
Удалось ли вам получить список поддиректорий директории `/home`? Какие права установлены на директориях?
10. Проверьте, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой: `lsattr /home` Удалось ли вам увидеть расширенные атрибуты директории? Удалось ли вам увидеть расширенные атрибуты директорий других пользователей?
11. Создайте в домашней директории поддиректорию `dir1` командой `mkdir dir1` Определите командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`.
12. Снимите с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверьте с её помощью правильность выполнения команды `ls -l`
13. Попробуйте создать в директории `dir1` файл `file1` командой `echo "test" > /home/guest/dir1/file1` Объясните, почему вы получили отказ в выполнении операции по созданию файла? Оцените, как сообщение об ошибке отразилось на создании файла? Проверьте командой `ls -l /home/guest/dir1` действительно ли файл `file1` не находится внутри директории `dir1`.
14. Заполните 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, занесите в таблицу знак “+”, если не разрешена, то “-”.
15. На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения операций внутри директории `dir1`, заполните таблицу “Минимальные права для совершения операций”.

3 Теоретическое введение

В основе механизмов разграничения прав доступа лежат имена пользователей и имена групп пользователей. В Linux каждый пользователь имеет уникальное имя, под которым он входит в систему (логинится). Кроме того, в системе создается некоторое число групп пользователей, причем каждый пользователь может быть включен в одну или несколько групп.

Создает и удаляет группы системный администратор (суперпользователь), он же может изменять состав участников той или иной группы. Члены разных групп могут иметь разные права по доступу к файлам Linux.

Права доступа подразделяются на три типа:

- чтение — r (сокращение от read);
- запись — w (сокращение от write);
- выполнение — x (сокращение от execute). Эти типы прав доступа могут быть предоставлены трем классам пользователей: владельцу файла, группе, в которую входит владелец, и всем (прочим) пользователям. Владельца и группу файла в дальнейшем можно поменять с помощью команд `chown` и `chgrp`.

Разрешение на чтение позволяет пользователю читать содержимое файлов, а в случае каталогов — просматривать перечень имен файлов в каталоге (используя, например, команду `ls`).

Разрешение на запись позволяет пользователю писать в файл и изменять его. Для каталогов это дает право создавать в каталоге новые файлы и каталоги, или удалять файлы в этом каталоге.

Разрешение на выполнение позволяет пользователю выполнять файлы (как бинарные программы, так и командные файлы). Разрешение на выполнение применительно к каталогам означает возможность выполнять команды, например, `cd`.

4 Выполнение лабораторной работы

Используя учётную запись администратора, создадим учётную запись пользователя *guest* (рис. [4.1]).

```
[deibatulina@deibatulina ~]$ sudo -i
[sudo] пароль для deibatulina:
[root@deibatulina ~]# useradd guest
[root@deibatulina ~]#
```

Рис. 4.1: Создание учётной записи нового пользователя

Используя учётную запись администратора, зададим пароль нового пользователя (рис. [4.2]).

```
[root@deibatulina ~]# passwd guest
Изменение пароля пользователя guest.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - на основе слова из словаря
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[root@deibatulina ~]#
```

Рис. 4.2: Задание пароля нового пользователя

Войдём в систему под новым пользователем *guest* (рис. [4.3]).

```
[root@deibatulina ~]# exit
выход
[deibatulina@deibatulina ~]$ su guest
Пароль:
[guest@deibatulina deibatulina]$
```

Рис. 4.3: Вход в систему под пользователем *guest*

Определяю директорию, в которой нахожусь - это есть домашняя директория (рис. [4.4]).

```
[guest@deibatulina deibatulina]$ pwd
/home/deibatulina
[guest@deibatulina deibatulina]$
```

Рис. 4.4: Определение текущей директории

Уточним, под какой учётной записью произведён вход в систему (рис. [4.5]).

```
[guest@deibatulina deibatulina]$ whoami
guest
[guest@deibatulina deibatulina]$
```

Рис. 4.5: Определение имени текущего пользователя

Уточним имя пользователя, его группу и другие группы, в которые он входит (рис. [4.6]). Сравним полученные значения с выводом команды *groups*.

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

Рис. 4.6: Уточнение имени пользователя, его группы и других групп, в которые он входит

Имя пользователя совпадает с приглашением командной строки. Просмотрим файл */etc/passwd* (рис. [4.7]).

```
[guest@deibatulina deibatulina]$ cat /etc/passwd | grep guest
guest:x:1001:1001::/home/guest:/bin/bash
[guest@deibatulina deibatulina]$
```

Рис. 4.7: Просмотр файла */etc/passwd*

Определим *uid* пользователя. Определим *gid* пользователя. Сравнив найденные значения с полученными в предыдущих пунктах, можем заключить, что они совпадают.

Определим существующие в системе директории (рис. [4.8]).

```
[guest@deibatulina deibatulina]$ ls -l /home/
итого 4
drwx-----. 18 deibatulina deibatulina 4096 фев 15 12:39 deibatulina
drwx-----.  4 guest      guest      133 фев 15 13:11 guest
[guest@deibatulina deibatulina]$
```

Рис. 4.8: Существующие в системе директории

Список поддиректорий директории */home* получить удалось. Права, установленные на них: *drwx* для пользователя *deibatulina*, для пользователя *guest* такие же права: *drwx*.

Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории */home* (рис. [4.9]).

```
[guest@deibatulina ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/deibatulina
----- /home/guest
[guest@deibatulina ~]$
```

Рис. 4.9: Проверка расширенных атрибутов

Список расширенных атрибутов посмотреть мне, к сожалению, не удалось. Не удалось посмотреть и список расширенных атрибутов директорий других пользователей.

Создаём новую директорию, проверим, какие расширенные атрибуты и права доступа на неё установлены (рис. [4.10]).

```
[guest@deibatulina ~]$ mkdir dir1
[guest@deibatulina ~]$ ls -l dir1
итого 0
[guest@deibatulina ~]$ lsattr /dir1
lsattr: Нет такого файла или каталога while trying to stat /dir1
[guest@deibatulina ~]$ lsattr dir1
[guest@deibatulina ~]$ ls -la dir1
итого 0
drwxr-xr-x. 2 guest guest   6 фев 15 13:29 .
drwx-----. 5 guest guest 145 фев 15 13:29 ..
[guest@deibatulina ~]$
```

Рис. 4.10: Создание новой директории, просмотр прав доступа и расширенных атрибутов на неё

Снимаем с этой директории все атрибуты (рис. [4.11]).

```
[guest@deibatulina ~]$ chmod 000 dir1
[guest@deibatulina ~]$ ls -l
итого 0
d-----, 2 guest guest 6 фев 15 13:29 dir1
[guest@deibatulina ~]$
```

Рис. 4.11: Снятие всех атрибутов с новой директории

Попытаемся создать новый файл в новой директории (рис. [4.12]).

```
[guest@deibatulina ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@deibatulina ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе
[guest@deibatulina ~]$
```

Рис. 4.12: Попытка создания файла в новой директории

Видим сообщение об ошибке: Отказано в доступе. Ошибку выдало, так как ранее я сняла все расширенные атрибуты.

Приступаю к заполнению таблицы [4.1] “Установленные права и разрешённые действия”.

Таблица 4.1: Установленные права и разрешённые действия

Права	Права	Со-	Уда-	За-	Чте-	Сме-	Про-	Пере-	Сме-
ди-	файла	зда-	ление	пись	ние	на	смотр	име-	на
ректо-		ние	файла	в	файла	ди-	фай-	нова-	атри-
рии		файла		файл		ректо-	лов в	ние	бутов
						рии	ди-	файла	файла
							ректо-		
							рии		
d(000)	(000)	-	-	-	-	-	-	-	-
d(000)	(100)	-	-	-	-	-	-	-	-
d(000)	(200)	-	-	-	-	-	-	-	-
d(000)	(300)	-	-	-	-	-	-	-	-
d(000)	(400)	-	-	-	-	-	-	-	-
d(000)	(500)	-	-	-	-	-	-	-	-

Таблица 4.1: Установленные права и разрешённые действия

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)	-	-	-	-	-	+	-	-

Таблица 4.1: Установленные права и разрешённые действия

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)	+	+	+	-	+	+	+	+

Таблица 4.1: Установленные права и разрешённые действия

d(700)	(400)	+	+	-	+	+	+	+	+
d(700)	(500)	+	+	-	+	+	+	+	+
d(700)	(600)	+	+	+	+	+	+	+	+
d(700)	(700)	+	+	+	+	+	+	+	+

Приступаю к заполнению таблицы [4.2] “Минимальные права для совершения операций”.

Таблица 4.2: Минимальные права для совершения операций

Операция	Минималь- ные права на директорию	Минималь- ные права на файл
Создание файла	d(300)	-
Удаление файла	d(300)	-
Чтение файла	d(100)	(400)
Запись в файл	d(100)	(200)
Переименова- ние файла	d(300)	(000)
Создание под- директории	d(300)	-
Удаление под- директории	d(300)	-

5 Выводы

В результате выполнения лабораторной работы №2 я научилась просматривать и снимать атрибуты директорий, вспомнила некоторые команды работы с командной строкой, а также узнала теоретические основы дискреционного разграничения доступа в ОС Linux.

Список литературы