

Лабораторная работа № 2

Дискреционное разграничение прав в Linux. Основные атрибуты

Абу Сувейлим Мухаммед Мунифович

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	8
5	Выводы	17
	Список литературы	18

Список иллюстраций

4.1	Имя и пароль пользователя	8
4.2	Домашняя директория	8
4.3	Команда whoami	9
4.4	Команда id	9
4.5	Команда groups	9
4.6	Команда grep guest	10
4.7	Команда ls -l	10
4.8	Команда lsattr	10
4.9	Поддиректория dir1	11
4.10	Команда chmod	11
4.11	Команда echo	12

Список таблиц

table №1	Установленные права и разрешённые действия	12
table №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

Заполнить таблицу «Установленные права и разрешённые действия».

3 Теоретическое введение

В метаданных каждого объекта (в inode файла/директории) содержится список разрешений на доступ к нему для разных категорий субъектов [1].

Атрибуты Minimal ACL поддерживают три базовых класса субъектов доступа к файлу (класс All объединяет все три класса):

User access (u) – доступ для владельца файла; Group access (g) – доступ для группы, владеющей файлом; Other access (o) – доступ для остальных пользователей (кроме пользователя root). All access (a) – доступ для всех субъектов доступа (u, g, o). Для каждого из этих классов определены три типа разрешений:

На чтение содержимого файла (read) – символ «r». На запись внутри файла или изменения его содержимого (write) – символ «w». На исполнение файла (если это бинарный исполняемый файл или файл сценария интерпретатора (execute)) – символ «x» [2].

4 Выполнение лабораторной работы

В установленной при выполнении предыдущей лабораторной работы операционной системе создад учётную запись пользователя guest (используя учётную запись администратора) и задал пароль для пользователя guest (используя учётную запись администратора) (рис. 4.1):

```
[smabu@smabu ~]$ su
Пароль:
[root@smabu smabu]# useradd guest
[root@smabu smabu]# passwd guest
Изменение пароля пользователя guest.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[root@smabu smabu]#
```

Рис. 4.1: Имя и пароль пользователя

Войшел в систему от имени пользователя guest. Определил директорию, в которой мы находимся, командой pwd (рис. 4.2):

```
[guest@smabu ~]$ pwd
/home/guest
[guest@smabu ~]$ cd ~
[guest@smabu ~]$ pwd
/home/guest
[guest@smabu ~]$
```

Рис. 4.2: Домашняя директория

Уточнил имя пользователя командой (рис. 4.3):

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

Рис. 4.3: Команда whoami

Уточнил имя пользователя, его группы, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др сравнил с выводом командой `groups` (рис. 4.4, 4.5):

```
[guest@smabu ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest)
```

Рис. 4.4: Команда id

```
[guest@smabu ~]$ groups
guest
[guest@smabu ~]$ id -G
1001
[guest@smabu ~]$ id -nG
guest
[guest@smabu ~]$
```

Рис. 4.5: Команда groups

Находил свою учётную запись. Определил `uid` пользователя. Определил `gid` пользователя и сравнил найденные значения с полученными в предыдущих пунктах (рис. 4.6):

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

Рис. 4.6: Команда grep guest

Определил существующие в системе директории командой (рис. 4.7)

```
[guest@smabu ~]$ ls -l /home/
итого 8
drwx-----. 14 guest guest 4096 сен 13 23:22 guest
drwx-----. 14 smabu smabu 4096 сен  6 21:37 smabu
[guest@smabu ~]$
```

Рис. 4.7: Команда ls -l

Проверил, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой (рис. 4.8):

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

Рис. 4.8: Команда lsattr

Создал в домашней директории поддиректорию dir1 командой (рис. 4.9):

```

[guest@smabu ~]$ mkdir dir1
[guest@smabu ~]$ ls -l
dir1
Видео
Документы
Загрузки
Изображения
Музыка
Общедоступные
'Рабочий стол'
Шаблоны
[guest@smabu ~]$ lsattr
bash: lsattr: команда не найдена...
[guest@smabu ~]$ lsattr
----- ./Рабочий стол
----- ./Загрузки
----- ./Шаблоны
----- ./Общедоступные
----- ./Документы
----- ./Музыка
----- ./Изображения
----- ./Видео
----- ./dir1
[guest@smabu ~]$ █

```

Рис. 4.9: Поддиректория dir1

Снял с директории dir1 все атрибуты командой (рис. 4.10):

```

[guest@smabu ~]$ chmod 000 dir1
[guest@smabu ~]$ ls -l
dir1
Видео
Документы
Загрузки
Изображения
Музыка
Общедоступные
'Рабочий стол'
Шаблоны
[guest@smabu ~]$ ls -l dir1
ls: невозможно открыть каталог 'dir1': Отказано в доступе
[guest@smabu ~]$ █

```

Рис. 4.10: Команда chmod

Попытался создать в директории dir1 файл file1 командой (рис. 4.11):

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

Рис. 4.11: Команда echo

но получил отказ в выполнении операции по созданию файла.

Заполнил таблицу «Установленные права и разрешённые действия» (см. табл. 2.1), выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занес в таблицу знак «+», если не разрешена, знак «-».

Установленные права и разрешённые действия									
Права директории	Права файла	Права файла							
		Про- смотр	Пе- ре- име- но- ва- ние	Сме- на фай- лов в ди- рек- то- рии	Сме- на ди- рек- то- рии	Созда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла
d(000)	(000)	-	-	-	-	-	-	-	-
d(100)	(000)	-	-	-	+	-	-	-	+
d(200)	(000)	-	-	-	-	-	-	-	-
d(300)	(000)	+	+	-	+	-	+	-	+
d(400)	(000)	-	-	-	-	+	-	-	-
d(500)	(000)	-	-	-	+	+	-	-	+
d(600)	(000)	-	-	-	-	+	-	-	-
d(700)	(000)	+	+	-	+	+	+	-	+
d(000)	(100)	-	-	-	-	-	-	-	-

Права директории	Права файла								
		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(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)	-	-	+	-	+	-	-	+
d(200)	(300)	-	-	-	-	-	-	-	-
d(300)	(300)	+	+	+	-	+	-	+	+
d(400)	(300)	-	-	-	-	-	+	-	-
d(500)	(300)	-	-	+	-	+	+	-	+

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

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

На основании заполненной таблицы определил те или иные минимально необходимые права для выполнения операций внутри директории dir1.

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)

5 Выводы

Получил 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

1. // skillbox.ru.
2. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.