Лабораторная работа №2

Информационная безопасность

Банникова Екатерина Алексеевна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

1. Получение практических навыков работы с атрибутами файлов.
2. Закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

2 Теоретическое введение

Атрибуты - это набор основных девяти битов, определяющих какие из пользователей обладают правами на чтение, запись, исполнение. Первые три бита отвечают права доступа владельца, вторые - для группы пользователей, последние - для всех остальных пользователей в системе.

3 Выполнение лабораторной работы

Создаем нового пользователя guest1 командой useradd, затем устанавливаем для него пароль с помощью команды passwd guest1

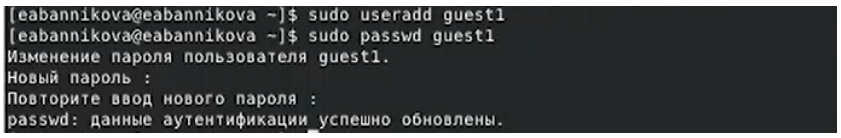

Рис. 3.1: Создание пользователя и установка пароля

Заходим в систему от имени пользователя guest1, используя только что установленный пароль.

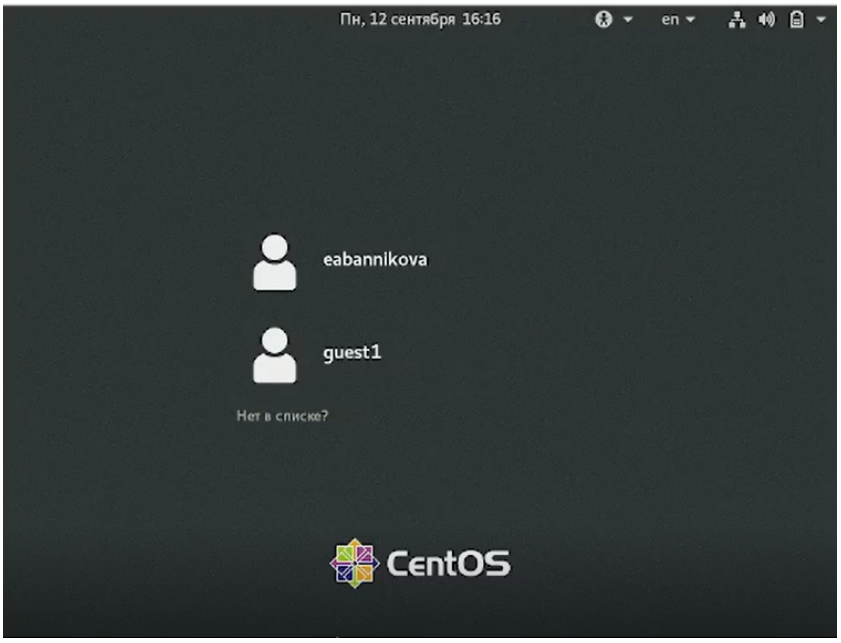

Рис. 3.2: Вход в систему пользователя guest1

Выполняем команду pwd, которая показывает, что мы находимся в домашнем каталоге пользователя guest1. Уточняем имя пользователя командой whoami, получаем вывод guest1. Уточняем имя пользователя, его группу, группы, куда входит пользователь, командой id. Вводим команду groups, видим, что группа состоит из одного пользователя guest, данные совпадают с командой id.

Рис. 3.3: Проверка данных пользователя

Посмотрим файл /etc/password командой cat /etc/password. Находим информацию о пользователе, что соотвествует данным, полученным с помощью команды id и pwd.

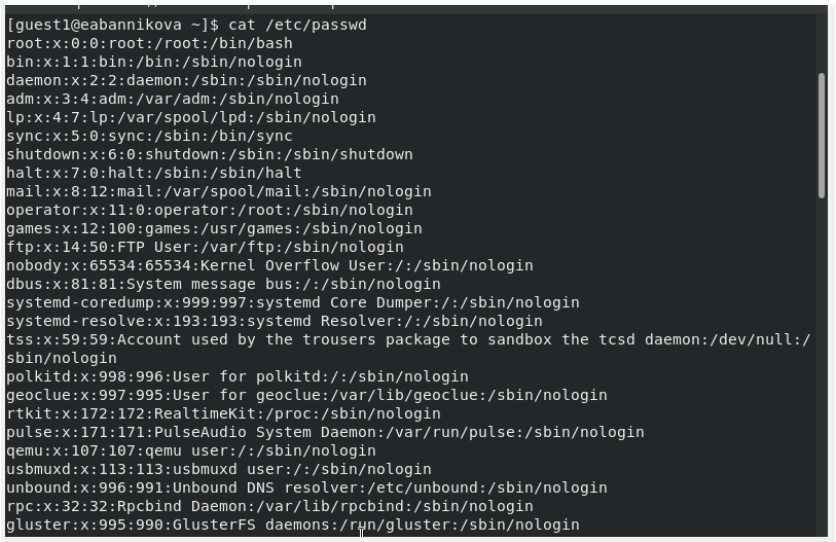

Рис. 3.4: /etc/password

Определим содержимое каталога /home. С помощью команды ls -l /home/ нам удалось получить список поддиректорий. У каждой из них установлены права на чтение, запись и выполнение только для самого пользователя. Проверяем

какие расширенные атрибуты уставновлены на поддиректориях, находящихся в директории /home, командоц lsattr /home. Нам удалось увидеть расширенные атрибуты директории, но не удалось увидеть расширенные атрибуты директорий других пользователей. Создадим в домашней директории поддиректорию dir1 командой mkdir dir1. Определим командами ls -l и lsattr, какие права доступа и расширенные атрибуты были выставлены на директорию.

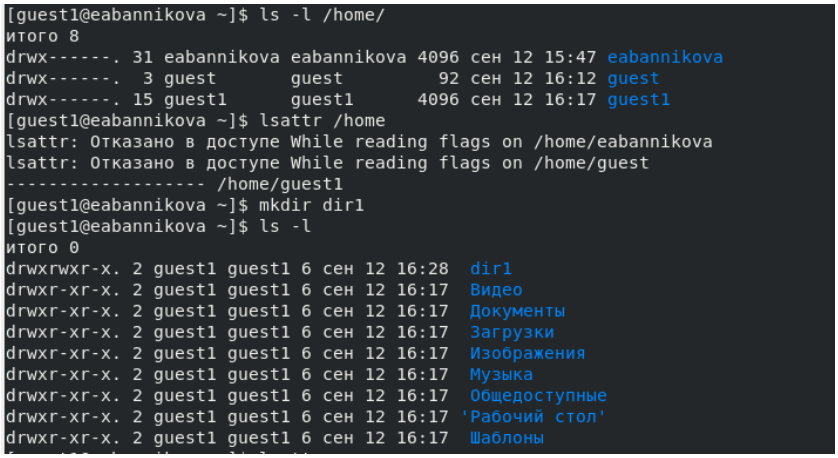

Рис. 3.5: dir1(1)

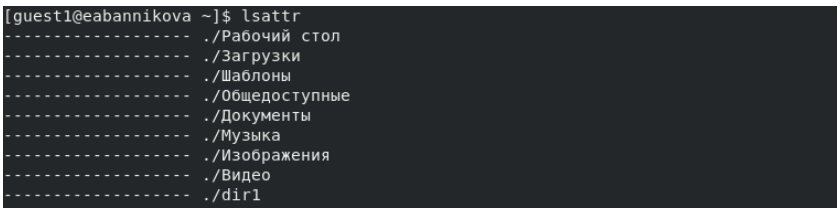

Рис. 3.6: dir1(2)

Снимем с директории dir1 все атрибуты командой chmod 000 dir1 и проверим с ее помощью правильность выполненич командой ls -l. Попытаемся создать в директории dir1 файл file, но получим отказ от выполнения, так как шагом ранее сняли все атрибуты с директории. Проверим, действительно ли файл не создался.

```
[guest1@eabannikova ~]$ chmod 000 dir1
[guest1@eabannikova ~]$ ls -l
итого 0
d---------. 2 guest1 guest1 6 сен 12 16:28  dir1
drwxr-xr-x. 2 guest1 guest1 6 сен 12 16:17  Видео
drwxr-xr-x. 2 guest1 guest1 6 сен 12 16:17  Документы
drwxr-xr-x. 2 guest1 guest1 6 сен 12 16:17  Загрузки
drwxr-xr-x. 2 guest1 guest1 6 сен 12 16:17  Изображения
drwxr-xr-x. 2 guest1 guest1 6 сен 12 16:17  Музыка
drwxr-xr-x. 2 guest1 guest1 6 сен 12 16:17  Общедоступные
drwxr-xr-x. 2 guest1 guest1 6 сен 12 16:17 'Рабочий стол'
drwxr-xr-x. 2 guest1 guest1 6 сен 12 16:17  Шаблоны
[guest1@eabannikova ~]$ echo "test" > /home/guest/dir1/filel
bash: /home/guest/dir1/filel: Отказано в доступе
[guest1@eabannikova ~]$ ls -l /home/guest/dir1
ls: невозможно получить доступ к '/home/guest/dir1': Отказано в доступе
[guest1@eabannikova ~]$
```

Рис. 3.7: Снятие атрибутов

Заполним таблицу “Установленные права и разрешенные действия”.

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименовывание файла	Смена атрибутов файла
d--------- (000)	0	-	-	-	-	-	-	-	-
d--x------ (100)	0	-	-	-	-	+	-	-	+
d-w------- (200)	0	-	-	-	-	-	-	-	-
d-wx------ (300)	0	+	+	-	-	+	-	+	+
dr-------- (400)	0	-	-	-	-	-	+	-	-
dr-x------ (500)	0	-	-	-	-	+	+	-	+
drw------- (600)	0	-	-	-	-	-	+	-	-
drwx------ (700)	0	+	+	-	-	+	+	+	+
d--------- (000)	--x------ (100)	-	-	-	-	-	-	-	-
d--x------ (100)	--x------ (100)	-	-	-	-	+	-	-	+
d-w------- (200)	--x------ (100)	-	-	-	-	-	-	-	-
d-wx------ (300)	--x------ (100)	+	+	-	-	+	-	+	+
dr-------- (400)	--x------ (100)	-	-	-	-	-	+	-	-
dr-x------ (500)	--x------ (100)	-	-	-	-	+	+	-	+
drw------- (600)	--x------ (100)	-	-	-	-	-	+	-	-
drwx------ (700)	--x------ (100)	+	+	-	-	+	+	+	+
d--------- (000)	-w------- (200)	-	-	-	-	-	-	-	-
d--x------ (100)	-w------- (200)	-	-	+	-	+	-	-	+
d-w------- (200)	-w------- (200)	-	-	-	-	-	-	-	-
d-wx------ (300)	-w------- (200)	+	+	+	-	+	-	+	+
dr-------- (400)	-w------- (200)	-	-	-	-	-	+	-	-
dr-x------ (500)	-w------- (200)	-	-	+	-	+	+	-	+
drw------- (600)	-w------- (200)	-	-	-	-	-	+	-	-
drwx------ (700)	-w------- (200)	+	+	+	-	+	+	+	+
d--------- (000)	-wx------ (300)	-	-	-	-	-	-	-	-
d--x------ (100)	-wx------ (300)	-	-	+	-	+	-	-	+
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)	+	+	+	-	+	+	+	+

Рис. 3.8: Права на действия

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)	-	-	+	+	+	+	-	+
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)	+	+	+	+	+	+	+	+

Рис. 3.9: Права на действия

Заполним таблицу “Минимальные права для совершения операций”.

Операция	**Минимальные права на директорию**	**Минимальные 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)
Переименовывание файла	d-wx------ (300)	--------- (000)
Создание поддиректории	d-wx------ (300)	--------- (000)
Удаление поддиректории	d-wx------ (300)	--------- (000)

Рис. 3.10: Минимальные права для совершения операций

4 Выводы

Получила практические навыки работы в консоли атрибутами файлов, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы