

Основы информационной безопасности

Лабораторная работа № 2. Дискреционное разграничение прав в Linux. Основы атрибуты

Абдеррахим Мугари.

28 февраля 2024ю

Российский университет дружбы народов, Москва, Россия

Информация

- Абдеррахим Мугари
- Студент
- Российский университет дружбы народов
- 1032215692@pfur.ru
- <https://github.com/iragoum>



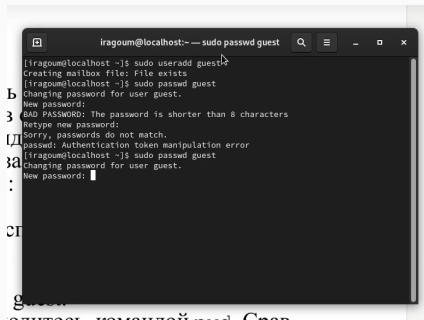
- Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

- Терминал Unix

Ход работы:

создание гостевой учетной записи и ее настройка

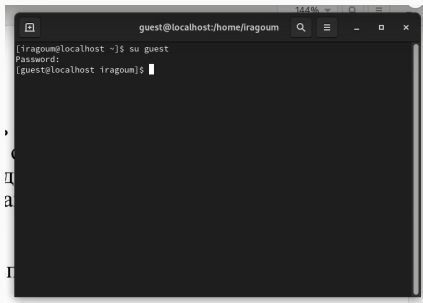
- Здесь мы создали учетную запись гостевого пользователя, используя нашу учетную запись администратора, используя команду **user addguest**, а затем мы установили пароль для гостевого пользователя, используя команду **passwd guest**.



```
iragoum@localhost:~ — sudo passwd guest
[iragoum@localhost ~]$ sudo useradd guest
Creating mailbox file: File exists
[iragoum@localhost ~]$ sudo passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
[iragoum@localhost ~]$ sudo passwd guest
Changing password for user guest.
New password:
```

Рис. 1: создание гостевой учетной записи и ее настройка

- Затем мы вошли в систему как гостевой пользователь, используя команду `su guest`.

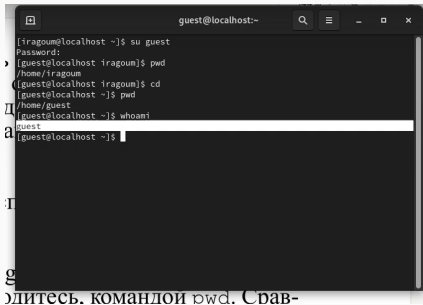


```
guest@localhost:/home/iragoum
[iragoum@localhost ~]$ su guest
Password:
[guest@localhost iragoum]$
```

Рис. 2: вход в гостевую учетную запись

определяя путь, по которому мы находились, и учетную запись пользователя, которую мы использовали

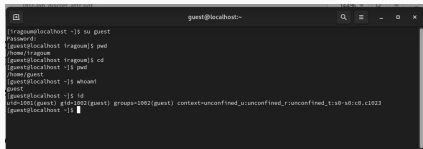
- Здесь мы определили каталог, в котором мы находились, с помощью команды **pwd**. После сравнения мы обнаружили, что мы не были расположены в домашнем каталоге гостя, и нам пришлось перейти к нему, после чего мы использовали команду **whoami** для определения учетной записи пользователя, в которую мы вошли.



```
guest@localhost:~  
[iragoum@localhost ~]$ su guest  
Password:  
[guest@localhost iragoum]$ pwd  
/home/iragoum  
[guest@localhost iragoum]$ cd /home/guest  
[guest@localhost ~]$ pwd  
/home/guest  
[guest@localhost ~]$ whoami  
guest  
[guest@localhost ~]$
```

Рис. 3: определяя путь, по которому мы находились, и учетную запись пользователя, которую мы

- здесь мы указали имя нашего пользователя, его группу, а также группы, в которые входит пользователь, с помощью команды `id`.



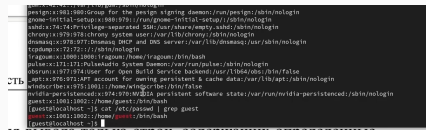
```
guest@localhost:~  
[iragum@localhost ~]$ su guest  
Password:  
[guest@localhost ~]$ pwd  
/home/iragum  
[guest@localhost ~]$ cd  
[guest@localhost ~]$ pwd  
/home/guest  
[guest@localhost ~]$ whoami  
guest  
[guest@localhost ~]$ id  
uid=1001(guest) gid=1002(guest) groups=1002(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@localhost ~]$
```

Рис. 4: указание имени пользователя, его группы, а также групп, в которые входит пользователь

- мы обнаружили, что данные идентичны.

сравнение данных гостя в файле passwd

- затем мы прочитали файл `/etc/passwd`, используя команду `cat`, и после этого, используя команду `cat /etc/passwd | grep guest`, мы выделили все слова, содержащие слово `guest`, мы нашли те же данные, которые получили ранее



```
design:x:981:980:Group for the design signing daemon:/run/design:/sbin/nologin
grom-initial-setup:x:988:979:/:run/grom-initial-setup:/sbin/nologin
sahd:x:74:74:Privilege-separated SSH:/usr/share/empty.sahd:/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:/usr/sbin/nologin
tcpdump:x:72:72:1:/sbin/nologin
fragum:x:1000:1000:fragum:/home/fragum:/bin/bash
pulse:x:171:171:Pulseaudio System Daemon:/var/run/pulse:/sbin/nologin
obrun:x:977:974:user for Open Build Service backend:/usr/lib4/jobd:/bin/false
_wpt:x:976:973:APT account for owning persistent & cache data:/var/lib/apt:/sbin/nologin
windscribe:x:975:1001:/:home/windscribe:/bin/false
nvidia-persistenced:x:974:970:NVIDIA persistent software state:/var/run/nvidia-persistenced:/sbin/nologin
guest:x:1001:1002:/:home/guest:/bin/bash
[guest@localhost ~]$ cat /etc/passwd | grep guest
guest:x:1001:1002:/:home/guest:/bin/bash
[guest@localhost ~]$
```

Рис. 5: сравнение данных гостя в файле passwd

- Затем мы определили существующие каталоги в системе с помощью команды `ls -l /home/`.

```
[guest@localhost ~]$ ls -l /home/
total 4
drwx-----. 3 guest  guest   98 Feb 24 17:50 guest
drwx-----. 19 iragoum iragoum 4096 Feb 24 17:39 iragoum
[guest@localhost ~]$
```

существующие в системе директории командой

Рис. 6: идентификация существующих каталогов

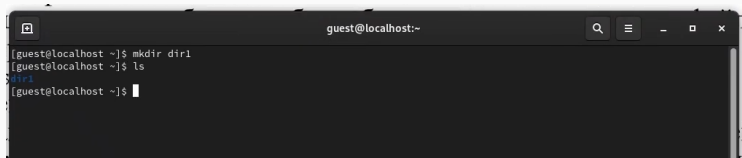
- да, мы смогли получить существующие подкаталоги каталога `/home`, у них права `d(drwx)`

- затем мы проверили, какие расширенные атрибуты установлены в подкаталогах, расположенных в каталоге /home, с помощью команды: `lsattr /home` и обнаружили, что у них нет расширенных атрибутов.

```
[guest@localhost ~]$ lsattr /home/  
lsattr: Permission denied While reading flags on /home/iragoum  
----- /home/guest
```

Рис. 7: проверка расширенных атрибутов

- здесь мы создали каталог dir1, используя команду `mkdir`.

A terminal window with a dark background and light text. The title bar at the top reads 'guest@localhost:~'. The terminal shows the following commands and output:

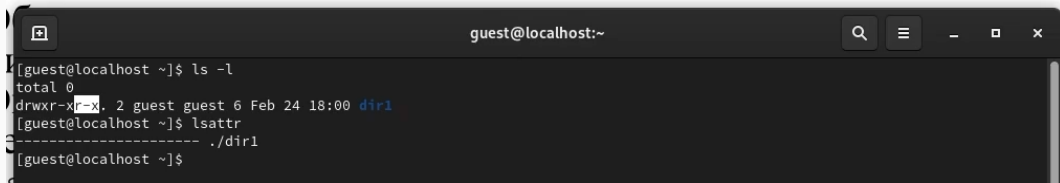
```
[guest@localhost ~]$ mkdir dir1
[guest@localhost ~]$ ls
dir1
[guest@localhost ~]$
```

The directory 'dir1' is listed in blue text after the 'ls' command.

Рис. 8: создание каталога dir1

определение прав доступа и расширенных атрибутов каталога dir1

- Используя команды `ls -l` и `lsattr`, мы определили, какие права доступа и расширенные атрибуты были установлены для каталога *dir1*.



```
guest@localhost:~  
[guest@localhost ~]$ ls -l  
total 0  
drwxr-xr-x. 2 guest guest 6 Feb 24 18:00 dir1  
[guest@localhost ~]$ lsattr  
----- ./dir1  
[guest@localhost ~]$
```

Рис. 9: определение прав доступа и расширенных атрибутов каталога dir1

- затем мы удалили все атрибуты из каталога *dir1* командой `chmod 000 dir1`.

```
[guest@localhost ~]$ chmod 000 dir1/
[guest@localhost ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Feb 24 18:00 dir1
[guest@localhost ~]$ cd
```

Рис. 10: удаление прав на каталог dir1

создание file1 внутри каталога dir1

- здесь мы попытались создать файл file 1 в каталоге dir1 с помощью команды `echo "test" > /home/guest/dir1/file1`, но у нас не было разрешения на это, потому что у нас нет прав в каталог *dir1*

```
[guest@localhost ~]$ cd dir1/  
bash: cd: dir1/: Permission denied  
[guest@localhost ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Permission denied  
[guest@localhost ~]$
```

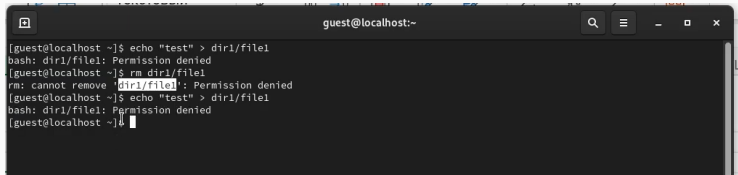
е атрибу-
дельца».

Рис. 11: создание file1 внутри каталога dir1

- нет, *file1* не находится внутри каталога *dir1*, потому что он даже не был создан.

Заполнение таблицы установленных прав и разрешенных действий

- здесь мы приступили к заполнению таблицы “Установленные права и разрешенные действия” (см. таблицу 2.1), выполняя действия от имени владельца каталога.



```
guest@localhost:~  
[guest@localhost ~]$ echo "test" > dir1/file1  
bash: dir1/file1: Permission denied  
[guest@localhost ~]$ rm dir1/file1  
rm: cannot remove 'dir1/file1': Permission denied  
[guest@localhost ~]$ echo "test" > dir1/file1  
bash: dir1/file1: Permission denied  
[guest@localhost ~]$
```

Рис. 12: заполнение таблицы установленных прав и разрешенных действий

Заполнение таблицы установленных прав и разрешенных действий

	A	B	C	D	E	F	
1	Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смеи
2	d(000)	000	-	-	-	-	
3	d-x----- d(100)	000	-	-	-	-	
4	d-w----- d(200)	000	-	-	-	-	
5	d-wx----- d(300)	000					
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							

Рис. 13: заполнение таблицы установленных прав и разрешенных действий

таблица минимально необходимых прав для выполнения операций внутри каталога

- основываясь на заполненной таблице, мы смогли определить определенные минимально необходимые права для выполнения операций внутри каталога dir1, заполнив таблицу 2.2.

	A	B	C	D
1	Операция	Минимальные права на директорию	Минимальные права на файл	
2	Создание файла	d-wx----- d(300)	---(000)	
3	Удаление файла	d-wx----- d(300)	---(000)	
4	Чтение файла	d--x----- d(100)	r--(400)	
5	Запись в файл	d--x----- d(100)	-w-(200)	
6	Переименование файла	d-wx----- d(300)	---(000)	
7				
8				

Рис. 14: таблица минимально необходимых прав для выполнения операций внутри каталога

Выводы, согласованные с целью
работы:

Выводы, согласованные с целью работы:

- В рамках данной лабораторной работы мы получили практические навыки работы с атрибутами файлов в консоли Linux, а также закрепили теоретические основы дискреционного разграничения доступа.