

Отчет №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Адабор Кристофер Твум (нкабд -03-22)

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	12

Список иллюстраций

2.1 yes 1 adduser guest.....	Error! Bookmark not defined.
2.2 пользователю пароль	5
2.3 guest	6
2.4 Домашняя директория и вывод whoami	6
2.5 id и groups	7
2.6 Пользователь	7
2.7 /etc/passwd	8
2.8 /home директория	8
2.9 lsattr /home директории.....	8
2.10 dir1.....	9
2.11 000 на dir1.....	9
2.12 Создание файла в dir1	9
2.13 “Установленные права и разрешённые действия” ч. 1	10
2.14 “Минимальные права для совершения операций”	10

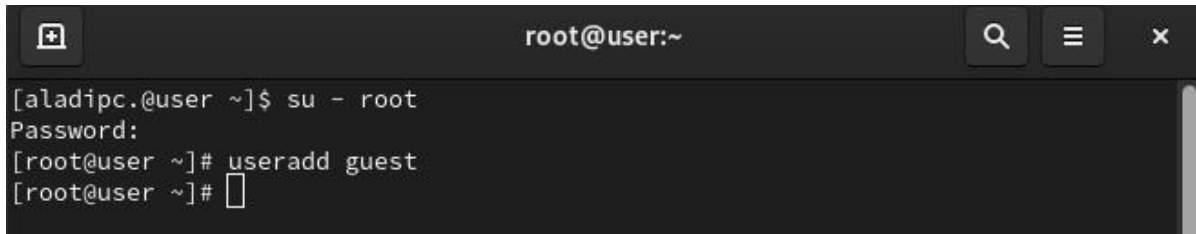
Список таблиц

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 Linux1.

Выполнение лабораторной работы

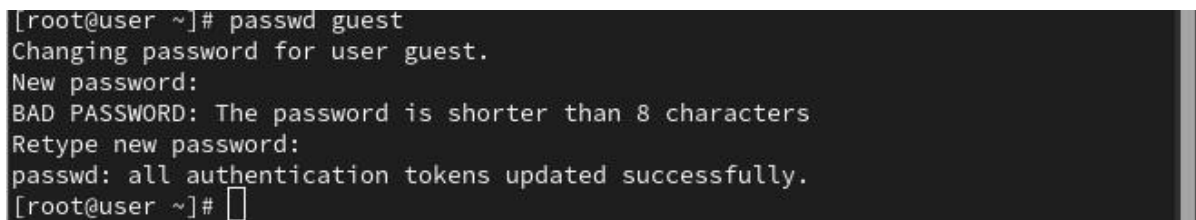
1. Создать пользователя guest. При помощи команды



```
root@user:~  
[aladipc.@user ~]$ su - root  
Password:  
[root@user ~]# useradd guest  
[root@user ~]#
```

Рис. 2.1: yes 1 |adduser guest

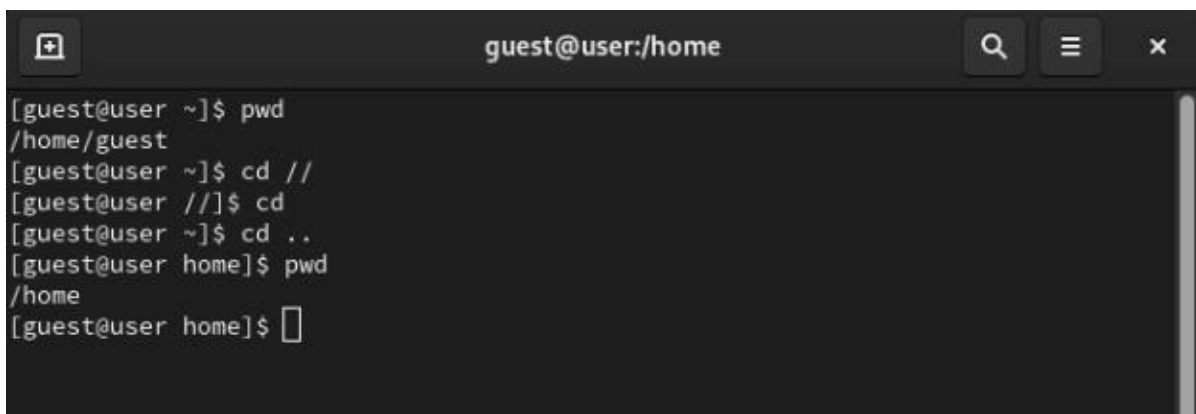
2. Задать новому пользователю пароль, при помощи утилиты passwd.



```
[root@user ~]# passwd guest  
Changing password for user guest.  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@user ~]#
```

Рис. 2.2: пользователю пароль

3. Войти в новую сессию под пользователем guest.

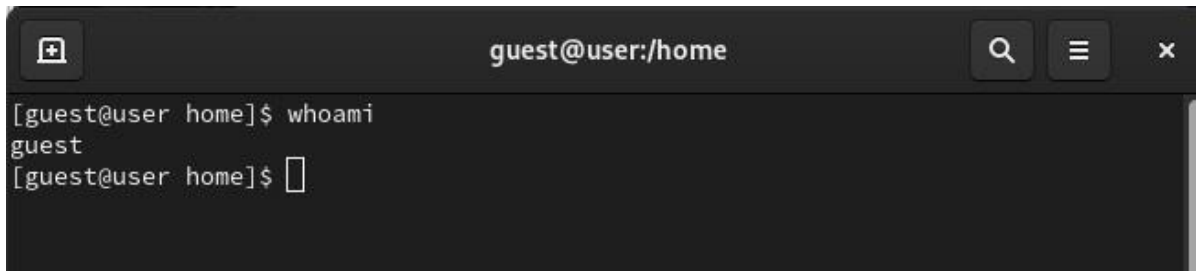


```
guest@user:/home  
[guest@user ~]$ pwd  
/home/guest  
[guest@user ~]$ cd //  
[guest@user //]$ cd  
[guest@user ~]$ cd ..  
[guest@user home]$ pwd  
/home  
[guest@user home]$
```

Рис. 2.3: guest

4. Открыть терминал и посмотреть в какой мы директории. Для этого будет использовать `pwd` (print workdir). Вывод команды можно увидеть на картинке fig.

2.1. Данная директория является домашней для пользователя `guest`.



```
guest@user:/home
[guest@user home]$ whoami
guest
[guest@user home]$
```

Рис. 2.4: Домашняя директория и вывод `whoami`

5. Для того, чтобы узнать `username` пользоваться, воспользуемся командой



```
guest@user:/home
[guest@user home]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0
-s0:c0.c1023
[guest@user home]$ groups
guest
[guest@user home]$
```

6. Посмотрим на вывод команды `id`. Там мы видим `UID`, `GID` и дополнительные метки пользователя. Вывод информации о группах сопоставим (fig. 2.2) с тем, что мы увидим, при запуске команды `groups`.

```
guest@user:/home
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pipewire:x:997:993:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
sssd:x:996:992:User for sssd:/usr/sbin/nologin
libstoragemgmt:x:990:990:daemon account for libstoragemgmt:/usr/sbin/nologin
systemd-oom:x:989:989:systemd Userspace OOM Killer:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/usr/sbin/nologin
geoclue:x:988:987:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:987:986:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:986:985:User for cockpit-ws instances:/nonexisting:/sbin/nologin
Flatpak:x:985:984:User for flatpak system helper:/usr/sbin/nologin
colord:x:984:983:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:983:982:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:982:981:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
design:x:981:980:Group for the design signing daemon:/run/psign:/sbin/nologin
gnome-initial-setup:x:980:979:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/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:/usr/sbin/nologin
aladipc:x:1000:1000:aladipc:/home/aladipc:/bin/bash
vboxadd:x:977:1:/var/run/vboxadd:/bin/false
guest:x:1001:1001:/home/guest:/bin/bash
[guest@user home]$
```

Рис. 2.5: id и groups

7. Пользователь guest и в приглашение командной строки имеет в себе username guest.

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

Рис. 2.6: Пользователь

8. В файле /etc/passwd лежит информация о всех пользователях системы (fig. 2.3). UID = 1001, GUID=1002.

```
guest@user:/home
[guest@user home]$ ls -l /home/
total 8
drwx-----, 14 aladipc. aladipc. 4096 Mar  2 12:59 aladipc.
drwx-----, 14 guest    guest    4096 Mar  2 13:10 guest
[guest@user home]$
```

Рис. 2.7: /etc/passwd

9. В директории /home/ у нас находятся все папки для каждого пользователя системы (fig. 2.4) (кроме системных пользователей). На обеих папках права выставлены 700.

```
[guest@user home]$ lsattr /home
lsattr: Permission denied While reading flags on /home/a
----- /home/guest
[guest@user home]$
```

Рис. 2.8: /home директория

10. Расширенные атрибуты удастся посмотреть только для директорий, до которых может достигаться пользователь. Потому там и появилась ошибка доступа (fig. ??).

```
[guest@user ~]$ cd
[guest@user ~]$ mkdir dir1
[guest@user ~]$ ls
Desktop dir1 Documents Downloads Music Pictures Public Templates Videos
[guest@user ~]$
```

Рис. 2.9: lsattr /home директории

11. Создадим директорию dir1 в домашнем каталоге. Посмотрим на ее права и атрибуты (fig. 2.5). На dir1 выставлены права 755.


```
guest@user:~  
[guest@user ~]$ cd  
[guest@user ~]$ mkdir dir1  
[guest@user ~]$ ls  
Desktop dir1 Documents Downloads Music Pictures Public Templates Videos  
[guest@user ~]$ ls -l dir1/  
total 0  
[guest@user ~]$ ls -l dir1  
total 0  
[guest@user ~]$ ls -l  
total 0  
drwxr-xr-x. 2 guest guest 6 Mar 2 13:10 Desktop  
drwxr-xr-x. 2 guest guest 6 Mar 2 13:33 dir1  
drwxr-xr-x. 2 guest guest 6 Mar 2 13:10 Documents  
drwxr-xr-x. 2 guest guest 6 Mar 2 13:10 Downloads  
drwxr-xr-x. 2 guest guest 6 Mar 2 13:10 Music  
drwxr-xr-x. 2 guest guest 111 Mar 2 13:33 Pictures  
drwxr-xr-x. 2 guest guest 6 Mar 2 13:10 Public  
drwxr-xr-x. 2 guest guest 6 Mar 2 13:10 Templates  
drwxr-xr-x. 2 guest guest 6 Mar 2 13:10 Videos  
[guest@user ~]$
```

Рис. 2.10: dir1

12. Обнулим (fig. 2.10) права доступа, при помощи chmod.

```
[guest@user ~]$ chmod 000 dir1  
[guest@user ~]$ ls -l  
total 0  
drwxr-xr-x. 2 guest guest 6 Mar 2 13:10 Desktop  
d------. 2 guest guest 6 Mar 2 13:33 dir1  
drwxr-xr-x. 2 guest guest 6 Mar 2 13:10 Documents  
drwxr-xr-x. 2 guest guest 6 Mar 2 13:10 Downloads  
drwxr-xr-x. 2 guest guest 6 Mar 2 13:10 Music  
drwxr-xr-x. 2 guest guest 125 Mar 2 13:36 Pictures  
drwxr-xr-x. 2 guest guest 6 Mar 2 13:10 Public  
drwxr-xr-x. 2 guest guest 6 Mar 2 13:10 Templates  
drwxr-xr-x. 2 guest guest 6 Mar 2 13:10 Videos  
[guest@user ~]$
```

Рис. 2.11: 000 на dir1

13. При попытке создать файл — получаем ошибку доступа из-за отсутствия прав для кого-либо.

```
[guest@user ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Permission denied  
[guest@user ~]$ ls -l /home/guest/dir1  
ls: cannot open directory '/home/guest/dir1': Permission denied  
[guest@user ~]$
```

Рис. 2.12: Создание файла в dir1

14. Заполним таблицу “Установленные права и разрешённые действия”.

0	0	-	-	-	-	-	-	-	-
100	0	-	-	-	-	+	-	-	+
200	0	-	-	-	-	-	-	-	-
300	0	+	+	-	-	+	-	+	+
400	0	-	-	-	-	-	+	-	-
500	0	-	-	-	-	+	+	-	+
600	0	-	-	-	-	-	+	-	-
700	0	+	+	-	-	+	+	+	+
0	100	-	-	-	-	-	-	-	-
100	100	-	-	-	-	+	-	-	+
200	100	-	-	-	-	-	-	-	-
300	100	+	+	-	-	+	-	+	+
400	100	-	-	-	-	-	+	-	-
500	100	-	-	-	-	+	+	-	+
600	100	-	-	-	-	-	+	-	-
700	100	+	+	-	-	+	+	+	+
0	200	-	-	-	-	-	-	-	-
100	200	-	-	+	-	+	-	-	+
200	200	-	-	-	-	-	-	-	-
300	200	+	+	+	-	+	-	+	+
400	200	-	-	-	-	-	+	-	-
500	200	-	-	+	-	+	+	-	+
600	200	-	-	-	-	-	+	-	-
700	200	+	+	+	-	+	+	+	+
0	300	-	-	-	-	-	-	-	-
100	300	-	-	-	-	+	-	-	+
200	300	-	-	-	-	-	-	-	-
300	300	+	+	+	-	+	-	+	+
400	300	-	-	-	-	-	+	-	-
500	300	-	-	-	-	+	+	-	+
600	300	-	-	-	-	-	+	-	-
700	300	+	+	+	-	+	+	+	+

Рис. 2.13: “Установленные права и разрешённые действия” ч. 1

15. На основе таблицы (fig. 2.8;fig. 2.9) составим таблицу с“Минимальные права для совершения операций” (fig. 2.13).

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	300	0
Удаление файла	300	0
Чтение файла	100	400
Запись в файл	100	200
Переименование файла	300	0
Создание поддиректории	300	0
Удаление поддиректории	300	0

Рис. 2.14: “Минимальные права для совершения операций”

3 Выводы

По итогам выполнения работы, я приобрел навыки работы в консоли с атрибутами файлов. :::