

Отчёт по лабораторной работе 2

Дискреционное разграничение прав в Linux. Основные атрибуты

Аристова Арина Олеговна

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	15
	Список литературы	16

Список иллюстраций

2.1	Создание пользователя guest.	6
2.2	Создание пароля для пользователя guest.	6
2.3	Выбор пользователя guest.	7
2.4	Определение директории, в которой нахожусь.	7
2.5	Уточнение имени пользователя.	8
2.6	Уточнение имени пользователя и его групп.	8
2.7	Получение информации о группах.	8
2.8	Определение uid и gid пользователя.	9
2.9	Фильтр по поиску.	9
2.10	Определение существующих в системе директорий.	10
2.11	Проверка расширенных атрибутов.	10
2.12	Создание каталога dir1.	10
2.13	Проверка прав доступа на вновь созданную директорию.	11
2.14	Снятие атрибутов с директории.	12
2.15	Попытка создать файл в директории без прав.	12
2.16	Создание файла в директории с правами на чтение и запись для владельца.	13

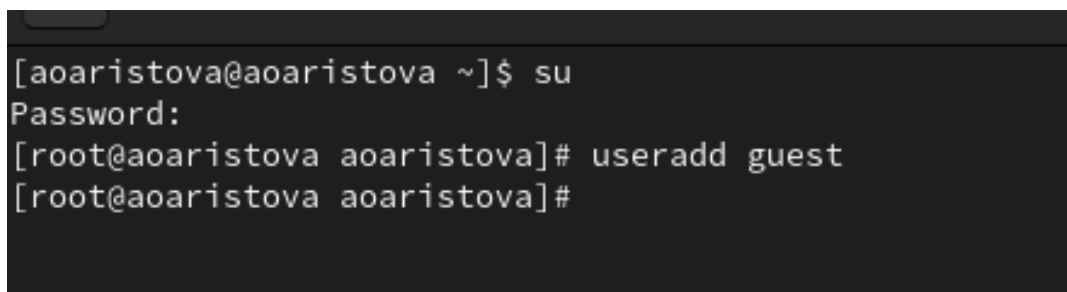
Список таблиц

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 Linux.

2 Выполнение лабораторной работы

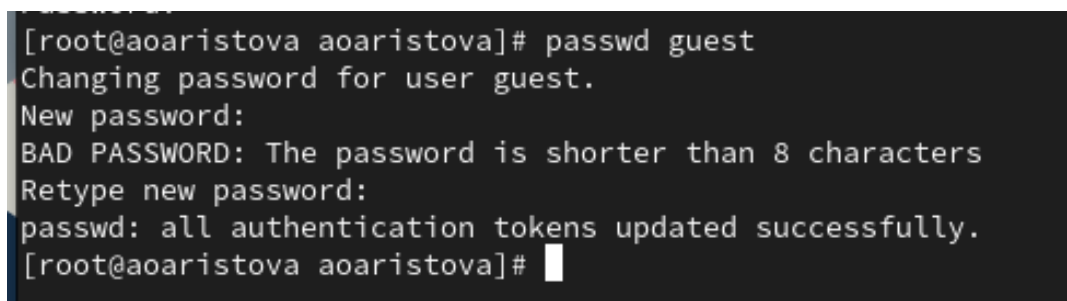
Запускаю виртуальную машину, настроенную в рамках предыдущей лабораторной работы. Открываю терминал и, используя учетную запись администратора создаю учетную запись пользователя с помощью команды: *useradd guest*



```
[aoaristova@aoaristova ~]$ su
Password:
[root@aoaristova aoaristova]# useradd guest
[root@aoaristova aoaristova]#
```

Рис. 2.1: Создание пользователя guest.

Задаю пароль для нового пользователя guest с помощью команды *passwd guest*:



```
[root@aoaristova aoaristova]# 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@aoaristova aoaristova]#
```

Рис. 2.2: Создание пароля для пользователя guest.

Перезагружаю машину и вижу возможность войти от имени пользователя guest, делаю это:

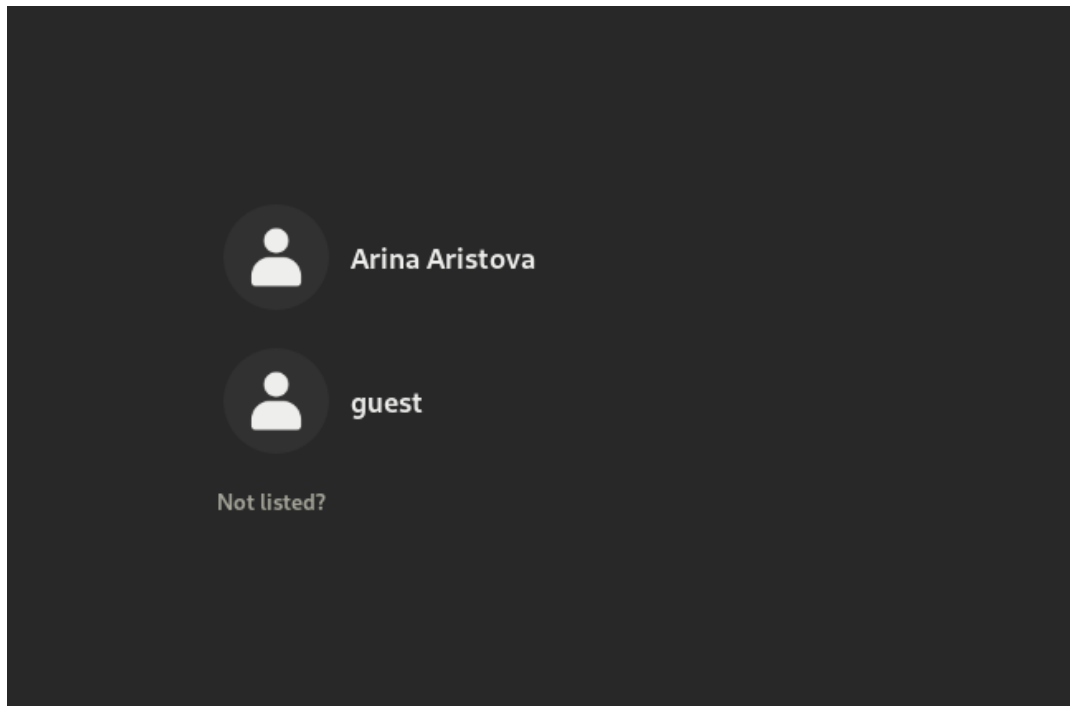


Рис. 2.3: Выбор пользователя guest.

С помощью команды *pwd* определяю директорию, в которой нахожусь. Сравнив результат с приглашением командной строки выявляю: они одинаковы. Я нахожусь в домашней директории.

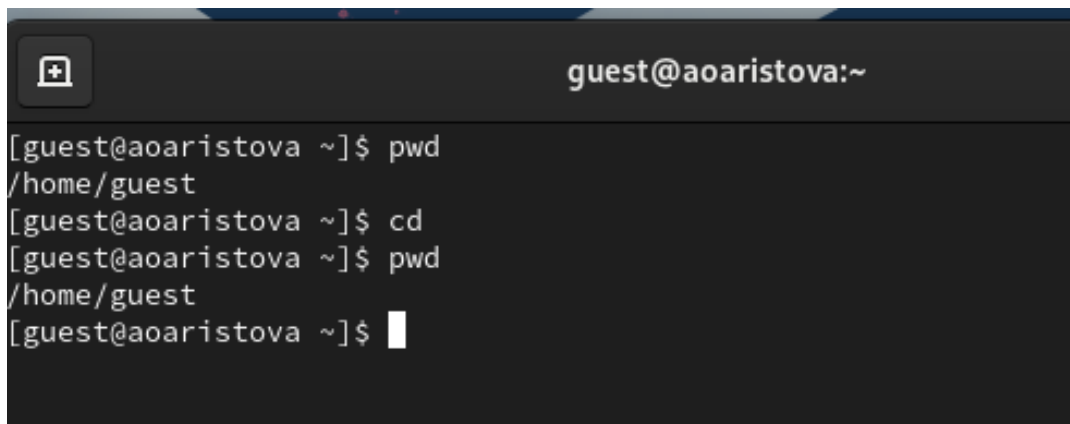


Рис. 2.4: Определение директории, в которой нахожусь.

С помощью команды *whoami* определяю имя пользователя, от имени которого произошел вход.

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

Рис. 2.5: Уточнение имени пользователя.

Командой *id* уточняю имя пользователя, его группы куда входит пользователь.

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

Рис. 2.6: Уточнение имени пользователя и его групп.

Затем выполняю команду *groups*, чтобы узнать информацию о группах. Видим, что полученная информация сходится с полученной в прошлом пункте информации о группах.

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

Рис. 2.7: Получение информации о группах.

Сравнив полученный результат с приглашением командной строки, убеждаемся в том, что в приглашении указано имя пользователя.

Просматриваю файл */etc/passwd* командой *cat /etc/passwd* Нахожу в нём свою учётную запись. Определяю *uid* пользователя. Определяю *gid* пользователя.


```
[guest@aoaristova ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/sbin/nologin
dbus:x:81:81:System message bus:/sbin/nologin
polkitd:x:998:996:User for polkitd:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pipewire:x:997:994:PipeWire System Daemon:/run/pipewire:/usr/sbin/nologin
sssd:x:996:993:User for sssd:/sbin/nologin
libstoragemgmt:x:991:991:daemon account for libstoragemgmt:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/usr/sbin/nologin
geoclue:x:990:989:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:989:988:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:988:987:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:987:986:User for flatpak system helper:/sbin/nologin
colord:x:986:985:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:985:984:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:984:983:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
pesign:x:983:982:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
gnome-initial-setup:x:982:981:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
chrony:x:981:980:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:980:979:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/sbin/nologin
aoaristova:x:1000:1000:Arina Aristova:/home/aoaristova:/bin/bash
guest:x:1001:1001:/home/guest:/bin/bash
[guest@aoaristova ~]$
```

Рис. 2.8: Определение uid и gid пользователя.

Для более понятного результата использую команду грег:

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

Рис. 2.9: Фильтр по поиску.

Определяю существующие в системе директории с помощью команды `ls -l /home/`:

На директория установлены следующие права: владельцы могут читать, записывать и выполнять, а группа и остальные ничего из перечисленного.

```
[guest@aoaristova ~]$ ls -l /home
total 8
drwx-----. 15 aoaristova aoaristova 4096 Sep  7 17:13 aoaristova
drwx-----. 14 guest      guest      4096 Sep  9 11:06 guest
[guest@aoaristova ~]$
```

Рис. 2.10: Определение существующих в системе директорий.

Проверяю, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: *lsattr /home*: Удалось ли вам увидеть расширенные атрибуты директории? - НЕТ Удалось ли вам увидеть расширенные атрибуты директорий других пользователей? - НЕТ

```
[guest@aoaristova ~]$ lsattr /home/
lsattr: Permission denied While reading flags on /home/aoaristova
----- /home/guest
[guest@aoaristova ~]$ lsattr /home/guest/
----- /home/guest/Desktop
----- /home/guest/Downloads
----- /home/guest/Templates
----- /home/guest/Public
----- /home/guest/Documents
----- /home/guest/Music
----- /home/guest/Pictures
----- /home/guest/Videos
[guest@aoaristova ~]$ lsattr /home/aoaristova/
[guest@aoaristova ~]$
```

Рис. 2.11: Проверка расширенных атрибутов.

Затем создаю в домашнем каталоге каталог dir1.

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

Рис. 2.12: Создание каталога dir1.

Затем с помощью команды *ls* я проверяю права доступа на эту директорию: владелец может читать, записывать выполнять, члены группы только записывать и выполнять, а остальные только выполнять

С помощью команды *lsattr* узнаем о расширенных атрибутах.

```

guest@aoaristova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep  9 11:04 Desktop
drwxr-xr-x. 2 guest guest 6 Sep  9 11:23 dir1
drwxr-xr-x. 2 guest guest 6 Sep  9 11:04 Documents
drwxr-xr-x. 2 guest guest 6 Sep  9 11:04 Downloads
drwxr-xr-x. 2 guest guest 6 Sep  9 11:04 Music
drwxr-xr-x. 2 guest guest 6 Sep  9 11:04 Pictures
drwxr-xr-x. 2 guest guest 6 Sep  9 11:04 Public
drwxr-xr-x. 2 guest guest 6 Sep  9 11:04 Templates
drwxr-xr-x. 2 guest guest 6 Sep  9 11:04 Videos
guest@aoaristova ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
guest@aoaristova ~]$

```

Рис. 2.13: Проверка прав доступа на вновь созданную директорию.

С помощью команды *chmod 000 dir1* снимаем с директории *dir1*, а затем проверяю выполненные действия с помощью команды *ls -l*.

```

[guest@aoaristova ~]$ chmod 000 dir1
[guest@aoaristova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep  9 11:04 Desktop
d----- . 2 guest guest 6 Sep  9 11:23 dir1
drwxr-xr-x. 2 guest guest 6 Sep  9 11:04 Documents
drwxr-xr-x. 2 guest guest 6 Sep  9 11:04 Downloads
drwxr-xr-x. 2 guest guest 6 Sep  9 11:04 Music
drwxr-xr-x. 2 guest guest 6 Sep  9 11:04 Pictures
drwxr-xr-x. 2 guest guest 6 Sep  9 11:04 Public
drwxr-xr-x. 2 guest guest 6 Sep  9 11:04 Templates
drwxr-xr-x. 2 guest guest 6 Sep  9 11:04 Videos
[guest@aoaristova ~]$

```

Рис. 2.14: Снятие атрибутов с директории.

Пытаюсь создать в директории `dir1` файл `file1` командой `echo "test" > /home/guest/dir1/file1`. Я получаю отказ в выполнении этого действия, так как даже у владельца директории нет прав на запись. Файл действительно не находится внутри директории.

```

[guest@aoaristova ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@aoaristova ~]$ ls -l /home/guest/dir1/
ls: cannot open directory '/home/guest/dir1/': Permission denied
[guest@aoaristova ~]$ chmod u+x dir1/
[guest@aoaristova ~]$ ls -l dir1/
ls: cannot open directory 'dir1/': Permission denied
[guest@aoaristova ~]$

```

Рис. 2.15: Попытка создать файл в директории без прав.

Проделываю те же действия, предварительно дав пользователю права на чтение и запись директории, таким образом создание файла заканчивается успехом. Эти действия выполняются для последующего заполнения таблицы.

```
Activities Terminal Sep 9 14:40
guest@aoaristova:~
[guest@aoaristova ~]$ chmod u+wrdir1
chmod: missing operand after 'u+wrdir1'
Try 'chmod --help' for more information.
[guest@aoaristova ~]$ chmod u+wr dir1
[guest@aoaristova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 9 11:04 Desktop
drwx----- 2 guest guest 19 Sep 9 14:38 dir1
drwxr-xr-x. 2 guest guest 6 Sep 9 11:04 Documents
drwxr-xr-x. 2 guest guest 6 Sep 9 11:04 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 9 11:04 Music
drwxr-xr-x. 2 guest guest 6 Sep 9 11:04 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 9 11:04 Public
drwxr-xr-x. 2 guest guest 6 Sep 9 11:04 Templates
drwxr-xr-x. 2 guest guest 6 Sep 9 11:04 Videos
[guest@aoaristova ~]$ touch dir1/file2
[guest@aoaristova ~]$ nano dir1/file2
[guest@aoaristova ~]$ nano dir1/file2
[guest@aoaristova ~]$ nano dir1/file2
[guest@aoaristova ~]$ rm dir1/file2
[guest@aoaristova ~]$ ls dir1
file1
[guest@aoaristova ~]$ mv dir/file1 dir2/file2
mv: cannot stat 'dir/file1': No such file or directory
[guest@aoaristova ~]$ mv dir1/file1 dir2/file2
mv: cannot move 'dir1/file1' to 'dir2/file2': No such file or directory
[guest@aoaristova ~]$ mv dir/file1 Documents
mv: cannot stat 'dir/file1': No such file or directory
[guest@aoaristova ~]$ mv dir1/file1 Documents
[guest@aoaristova ~]$ ls D
ls: cannot access 'D': No such file or directory
[guest@aoaristova ~]$ ls Do
Documents/ Downloads/
[guest@aoaristova ~]$ ls Documents/
file1
[guest@aoaristova ~]$ rm Documents/file1
rm: remove write-protected regular empty file 'Documents/file1'? y
[guest@aoaristova ~]$ ls Documents/
[guest@aoaristova ~]$ ls -l dir1/
total 0
[guest@aoaristova ~]$
```

Рис. 2.16: Создание файла в директории с правами на чтение и запись для владельца.

Теперь заполним таблицу “Установленные права и разрешенные действия”.

Права					Смена				
ди-	Соз-	Удале-	За-	Чте-	ди-	Просмотр	Переи-	Смена	
рек-	Права	дание	ние	пись	рек-	файлов в	менова-	атри-	
то-	фай-	фай-	фай-	в	то-	директо-	ние	бутов	
рии	ла	ла	ла	файл	рии	рии	файла	файла	
d	(000)	-	-	-	-	-	-	-	
(000)									

Права		Смена							
ди- рек- то- рии	Права фай- ла	Соз- дание фай- ла	Удале- ние фай- ла	За- пись в файл	Чте- ние фай- ла	ди- рек- то- рии	Просмотр файлов в директо- рии	Переи- менова- ние файла	Смена атри- бутов файла
d-x— — (100)	(000)	-	-	-	-	+	-	-	-
drwx— — (700)	(700)	+	+	+	+	+	+	+	+

3 Выводы

В ходе выполнения лабораторной работы мною были получены навыки работы в консоли с атрибутами файлов, закреплены теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы

- Описание лабораторной работы