

Отчет по лабораторной работе 2

Даниил Генералов, 1032212280

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	14

Список иллюстраций

3.1	useradd/pwd	7
3.2	whoami/id	8
3.3	etc/passwd	9
3.4	ls /home	10
3.5	mkdir	11

Список таблиц

1 Цель работы

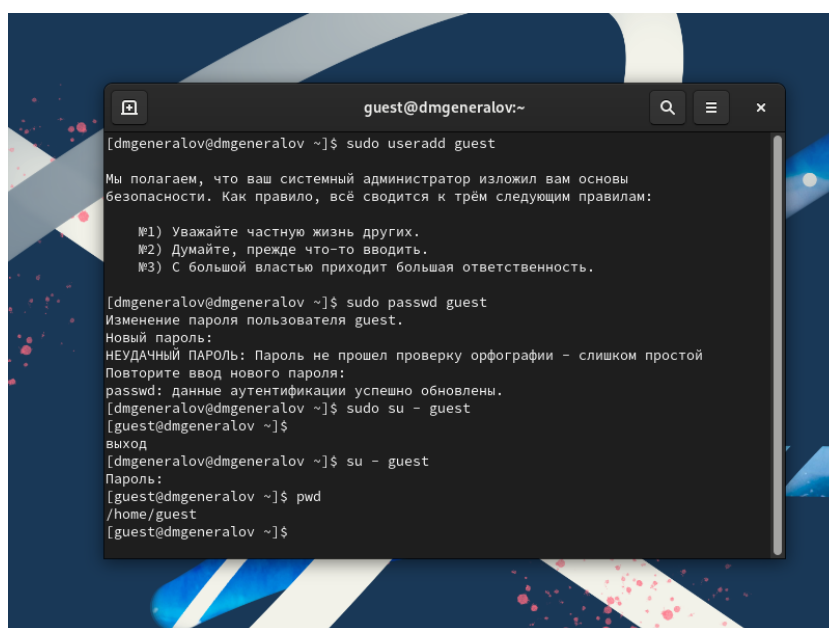
Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

2 Задание

Постарайтесь последовательно выполнить все пункты, занося ваши ответы на поставленные вопросы и замечания в отчёт.

3 Выполнение лабораторной работы

Сначала нужно создать нового пользователя по имени guest, задать его пароль и зайти в систему от его имени (рис. 3.1).

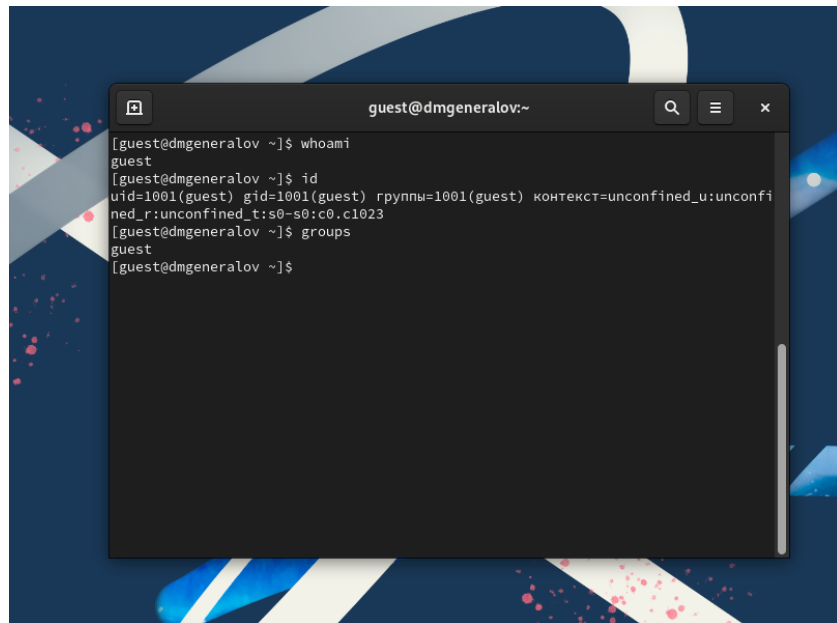


```
guest@dmgeneralov:~  
[dmgeneralov@dmgeneralov ~]$ sudo useradd guest  
Мы полагаем, что ваш системный администратор изложил вам основы  
безопасности. Как правило, всё сводится к трём следующим правилам:  
  
№1) Уважайте частную жизнь других.  
№2) Думайте, прежде что-то вводить.  
№3) С большой властью приходит большая ответственность.  
  
[dmgeneralov@dmgeneralov ~]$ sudo passwd guest  
Изменение пароля пользователя guest.  
Новый пароль:  
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - слишком простой  
Повторите ввод нового пароля:  
passwd: данные аутентификации успешно обновлены.  
[dmgeneralov@dmgeneralov ~]$ sudo su - guest  
[guest@dmgeneralov ~]$  
выход  
[dmgeneralov@dmgeneralov ~]$ su - guest  
Пароль:  
[guest@dmgeneralov ~]$ pwd  
/home/guest  
[guest@dmgeneralov ~]$
```

Рис. 3.1: useradd/pwd

Этот пользователь оказался в папке /home/guest – по умолчанию домашняя папка пользователя /home/<имя_пользователя>. Эта папка выглядит не так в приглашении командной строки – там, домашняя папка пользователя сокращается до ~.

После этого мы выясняем информацию про самого этого пользователя (рис. 3.2).

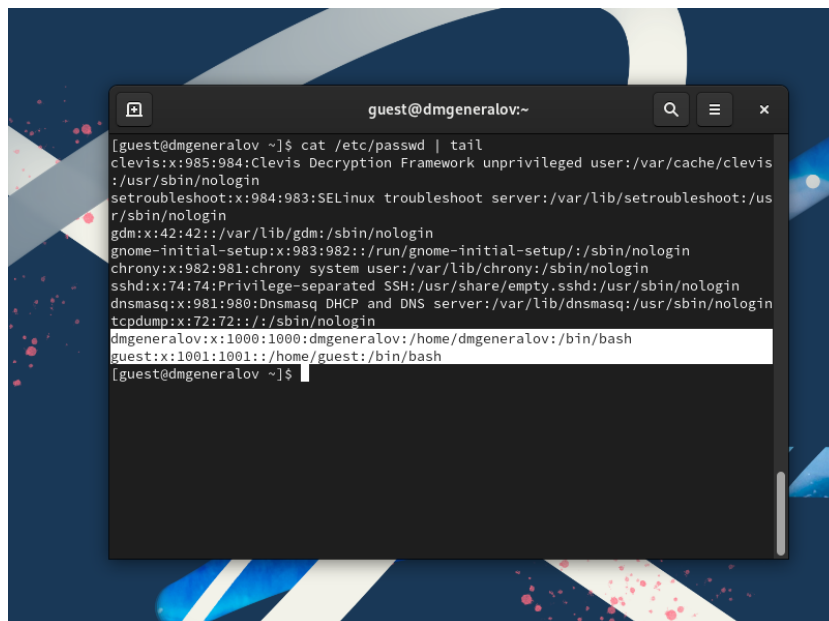
A terminal window titled 'guest@dmgeneralov:~' with search, menu, and close icons. The terminal shows the following commands and their outputs:

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

Рис. 3.2: whoami/id

В выводе этой команды видно, что имя пользователя равно `guest` – это соответствует первой части приглашения командной строки, до символа `@`. С помощью команды `id` мы узнали, что этот пользователь имеет UID 1001 и GID 1001, а также принадлежит к единственной группе с UID 1001 – `guest` (об этом также сообщает команда `groups`).

Эту же информацию можно определить, посмотрев в системную базу данных пользователей – `/etc/passwd` (рис. 3.3).

A terminal window titled 'guest@dmgeneralov:~' with search, menu, and close icons. The command '[guest@dmgeneralov ~]\$ cat /etc/passwd | tail' has been executed. The output lists system users and the 'guest' user. The 'guest' user entry is highlighted: 'guest:x:1001:1001::/home/guest:/bin/bash'.

```
[guest@dmgeneralov ~]$ cat /etc/passwd | tail
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:/u
sr/sbin/nologin
gdm:x:42:42:/:/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:983:982:/:run/gnome-initial-setup:/sbin/nologin
chrony:x:982:981:chrony system user:/var/lib/chrony:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
dnsmasq:x:981:980:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
dmgeneralov:x:1000:1000:dmgeneralov:/home/dmgeneralov:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
[guest@dmgeneralov ~]$
```

Рис. 3.3: `/etc/passwd`

Здесь видно, что пользователь `guest` имеет пароль `x` (то есть, он хранится в `/etc/shadow`), UID 1001 и GID 1001, не имеет полного имени пользователя, имеет домашнюю директорию `/home/guest` и интерпретатор `/bin/bash`.

Попытавшись посмотреть на информацию о папке `/home`, мы видим результат на рис. 3.4.

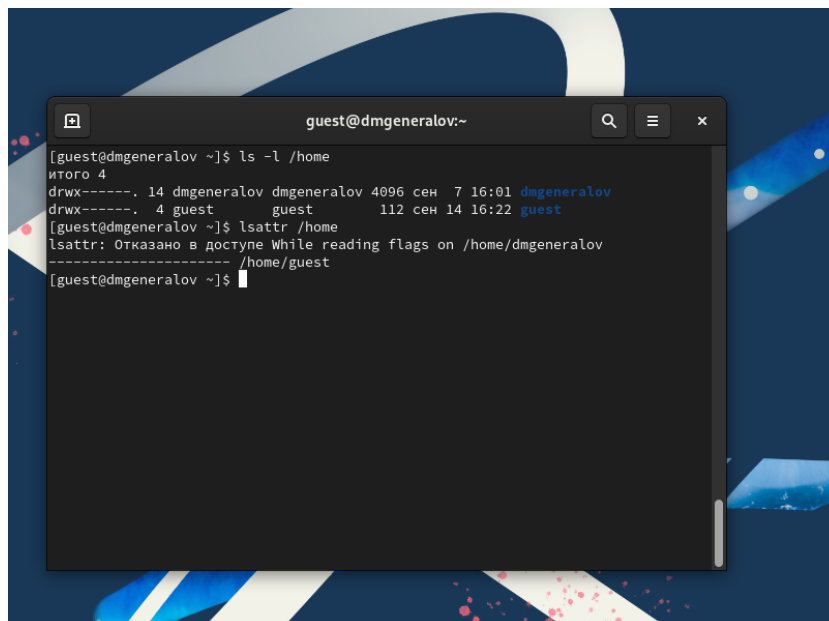


Рис. 3.4: ls /home

Базовая информация о папках в /home доступна: мы видим домашнюю папку для dmgeneralov и для guest, и они обе имеют права, которые разрешают владельцу все действия, а остальным – никакие. В частности, остальные пользователи не могут выполнять lsattr на них, потому что происходит ошибка разрешений при чтении этой информации про /home/dmgeneralov, но эта информация (пустая) возвращается для guest.

Затем мы создаем папку, настраиваем разрешения для нее, и пытаемся использовать ее (рис. 3.5).

```
guest@dmgeneralov:~$ mkdir dir1
guest@dmgeneralov:~$ ls -l
итого 0
drwxr-xr-x. 2 guest guest 6 сен 14 16:39 dir1
guest@dmgeneralov:~$ lsattr .
----- ./dir1
guest@dmgeneralov:~$ chmod 000 dir1
guest@dmgeneralov:~$ ls -l
итого 0
d-----. 2 guest guest 6 сен 14 16:39 dir1
guest@dmgeneralov:~$ lsattr .
lsattr: Отказано в доступе While reading flags on ./dir1
guest@dmgeneralov:~$ echo "test" > /home/guest/dir1/file1
-bash: /home/guest/dir1/file1: Отказано в доступе
guest@dmgeneralov:~$ ls -l /home/guest/dir1
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе
guest@dmgeneralov:~$ su
Пароль:
[root@dmgeneralov guest]# ls -l /home/guest/dir1
итого 0
[root@dmgeneralov guest]#
exit
guest@dmgeneralov:~$
```

Рис. 3.5: mkdir

Сначала папка имеет права для чтения-записи для владельца, и только чтения для остальных, и мы можем использовать ее (в том числе читать `lsattr`). После этого мы меняем разрешения с помощью `chmod`, так что никто не имеет никаких прав на доступ к ней. Как результат, мы не можем создать файл в этой папке, и он действительно не создается (что можно подтвердить, посмотрев на эту папку от пользователя `root`).

В выводе команды `ls -l` в начале пишется шифр, который обозначает права на этот файл или папку. В случае папок, этот шифр имеет следующий смысл:

		Запись		Просмотр					
Права	Права	Создание	Удаление	Чтение	Смена	в	Переименование	атрибутов	
директорий	файла	файла	файла	файла	директорий	директорий	файла	файла	
d---	----	-	-	-	-	-	-	-	-
(000)	(000)								
d-x-	-x--	-	-	-	+	-	-	+	
(100)	(100)								

		Запись			Просмотр				
Права	Права	Создание	Удаление	Чтение	Смена	в	Переименование	Смена	атрибутов
директории	файла	файла	файла	файла	директории	директории	файла	файла	файла
d-	-w----	-	-	+	-	-	-	-	-
w----	(200)								
(200)									
d-	-wx---	+	+	+	-	+	-	+	+
wx---	(300)								
(300)									
dr---	-r----	-	-	-	+	-	-	-	-
(400)	(400)								
dr-	-r-	-	-	-	+	+	+	-	-
x---	x---								
(500)	(500)								
drw---	-	-	-	+	+	-	-	-	-
(600)	rw----								
	(600)								
drwx---	-	+	+	+	+	+	+	+	+
(700)	rwx---								
	(700)								

На основании этих данных можно определить минимальные права, которые нужно поставить на файл или папку, если мы хотим разрешить кому-то делать определенные операции с ними:

Операция	Права на директорию	Права на файл
Создание файла	-wx	???
Удаление файла	-wx	—

Операция	Права на директорию	Права на файл
Чтение файла	-x	r-
Запись в файл	-x	-w-
Переименование файла	-wx	—
Создание поддиректории	-wx	???
Удаление поддиректории	-wx	???

4 Выводы

Мы изучили, как использовать базовый дискреционный контроль доступа в Linux, и определили, какие атрибуты позволяют выполнять какие действия над папками или файлами.