

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Монастырская Кристина Владимировна

Содержание

Цель работы	5
Выполнение лабораторной работы	6
Выводы	14
Список литературы	15

Список иллюстраций

1	Создание нового пользователя	6
2	Определение текущей директории, имени пользователя и групп пользователя	7
3	Файл /etc/passwd	7
4	Существующие директории	8
5	Атрибуты поддиректорий	8
6	Создание поддиректории и установка прав	9
7	Попытка создать файл	9

Список таблиц

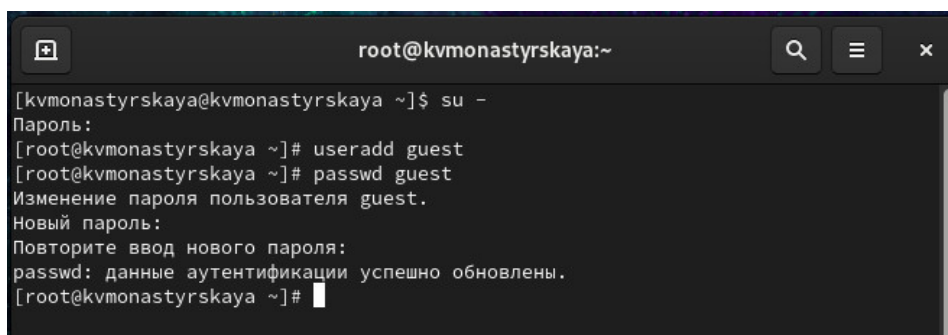
1	Установленные права и разрешённые действия	10
2	Минимальные права для совершения операций	13

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[1].

Выполнение лабораторной работы

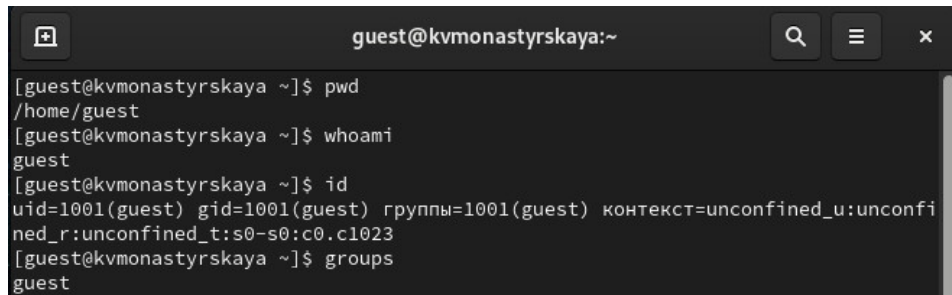
1. Создала учётную запись пользователя guest (использую учётную запись администратора): `useradd guest`. Задала пароль для пользователя guest (использую учётную запись администратора): `passwd guest` (рис. -@fig:001)



```
root@kvmonastyrskaya:~  
[kvmonastyrskaya@kvmonastyrskaya ~]$ su -  
Пароль:  
[root@kvmonastyrskaya ~]# useradd guest  
[root@kvmonastyrskaya ~]# passwd guest  
Изменение пароля пользователя guest.  
Новый пароль:  
Повторите ввод нового пароля:  
passwd: данные аутентификации успешно обновлены.  
[root@kvmonastyrskaya ~]#
```

Рис. 1: Создание нового пользователя

2. Вошла в систему от имени пользователя guest
3. Определила директорию, в которой нахожусь, командой `pwd` (рис. -@fig:002)
Директория `/home/имя_пользователя` является домашней директорией, в нашем случае это директория `home/guest`. Уточнила имя пользователя командой `whoami`. (рис. -@fig:004) Уточнила имя пользователя, его группу, а также группы, куда входит пользователь, командой `id` (рис. -@fig:005)

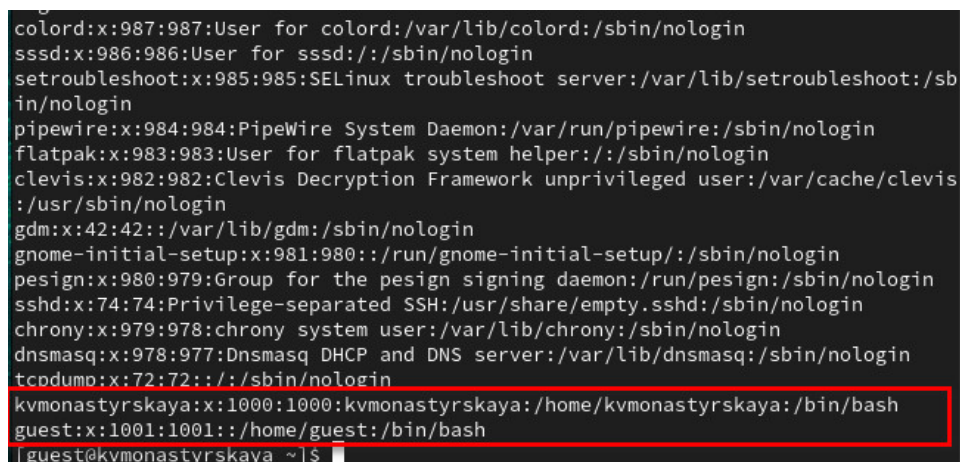
A terminal window titled 'guest@kvmonastyrskaya:~' with search, menu, and close icons. It shows the execution of 'pwd', 'whoami', 'id', and 'groups' commands.

```
guest@kvmonastyrskaya ~]$ pwd
/home/guest
guest@kvmonastyrskaya ~]$ whoami
guest
guest@kvmonastyrskaya ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
guest@kvmonastyrskaya ~]$ groups
guest
```

Рис. 2: Определение текущей директории, имени пользователя и групп пользо-
вателя

Сравним вывод `id` с выводом команды `groups`: `id` вывело номер группы 1001 и её название `guest`, `groups` также вывело название `guest`.

4. Просмотрела файл `/etc/passwd` командой `cat /etc/passwd`. Нашла в нём свою учётную запись (рис. -@fig:003)

A terminal window showing the output of 'cat /etc/passwd'. The entry for 'guest' is highlighted with a red box.

```
colord:x:987:987:User for colord:/var/lib/colord:/sbin/nologin
sssd:x:986:986:User for sssd:/:/sbin/nologin
setroubleshoot:x:985:985:SELinux troubleshoot server:/var/lib/setroubleshoot:/sb
in/nologin
pipewire:x:984:984:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
flatpak:x:983:983:User for flatpak system helper:/:/sbin/nologin
clevis:x:982:982:Clevis Decryption Framework unprivileged user:/var/cache/clevis
:/usr/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:981:980::/run/gnome-initial-setup:/sbin/nologin
pesign:x:980:979:Group for the pesign signing daemon:/run/pesign:/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:/sbin/nologin
tcdump:x:72:72::/:/sbin/nologin
kvmonastyrskaya:x:1000:1000:kvmonastyrskaya:/home/kvmonastyrskaya:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
[guest@kvmonastyrskaya ~]$
```

Рис. 3: Файл `/etc/passwd`

`uid = 1001 gid = 1001`

5. Определила существующие в системе директории командой `ls -l /home/` (рис. -@fig:004)

```

guest:x:1001:1001::/home/guest:/bin/bash
[guest@kvmonastyrskaya ~]$ ls -l /home
итого 8
drwx-----. 14 guest          guest          4096 дек 15 14:28 guest
drwx-----. 14 kvmonastyrskaya kvmonastyrskaya 4096 дек 15 13:59 kvmonastyrskaya
[guest@kvmonastyrskaya ~]$

```

Рис. 4: Существующие директории

Получили список поддиректорий, в нем директории двух пользователей: kvmonastyrskaya и guest, с правами на чтение, запись и переход в директорию для владельца.

6. Проверила, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: lsattr /home (рис. -@fig:005)

```

[guest@kvmonastyrskaya ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/kvmonastyrskaya
----- /home/guest
[guest@kvmonastyrskaya ~]$

```

Рис. 5: Атрибуты поддиректорий

Можно видеть расширенные атрибуты своей директории, но нельзя увидеть атрибуты других.

7. Создала в домашней директории поддиректорию dir1 командой mkdir dir1. Определила командами ls -l и lsattr, какие права доступа и расширенные атрибуты были выставлены на директорию dir1: все права для владельца, право на чтение и вход для группы и остальных. Сняла с директории dir1 все атрибуты командой chmod 000 dir1 и проверила с её помощью правильность выполнения команды ls -l (рис. -@fig:006)


```
[guest@kvmonastyrskaya ~]$ mkdir dir1
[guest@kvmonastyrskaya ~]$ chmod 000 dir1
[guest@kvmonastyrskaya ~]$ ls -l
итого 0
d-----, 2 guest guest 6 дек 15 14:40 dir1
drwxr-xr-x, 2 guest guest 6 дек 15 14:28 Видео
drwxr-xr-x, 2 guest guest 6 дек 15 14:28 Документы
drwxr-xr-x, 2 guest guest 6 дек 15 14:28 Загрузки
drwxr-xr-x, 2 guest guest 6 дек 15 14:28 Изображения
drwxr-xr-x, 2 guest guest 6 дек 15 14:28 Музыка
drwxr-xr-x, 2 guest guest 6 дек 15 14:28 Общедоступные
drwxr-xr-x, 2 guest guest 6 дек 15 14:28 'Рабочий стол'
drwxr-xr-x, 2 guest guest 6 дек 15 14:28 Шаблоны
[guest@kvmonastyrskaya ~]$
```

Рис. 6: Создание поддиректории и установка прав

8. Попыталась создать в директории dir1 файл file1 командой echo "test" > /home/guest/dir1/file1. (рис. -@fig:007)

```
[guest@kvmonastyrskaya ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@kvmonastyrskaya ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе
[guest@kvmonastyrskaya ~]$
```

Рис. 7: Попытка создать файл

Так как мы закрыли владельцу доступ на запись в директорию, мы не смогли создать файл.

Попробовала командой ls -l /home/guest/dir1 проверить действительно ли файл file1 не находится внутри директории dir1 (рис. -@fig:012)

9. Заполнила таблицу «Установленные права и разрешённые действия» (табл. 1), выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, заносила в таблицу знак «+», если не разрешена, знак «-».

Таблица 1: Установленные права и разрешённые действия

		Про- смотр							
Права		Со-		За-	Чте-	Сме-	фай-	Пере-	Сме-
ди-		зда-	Уда-	пись	ние	на	лов в	име-	на
ректо-	Права	ние	ление	в	из	ректо-	ректо-	нова-	атри-
рии	файла	файла	файла	файл	файла	рии	рии	файла	бутов
									файла
d---	----	-	-	-	-	-	-	-	-
d--x	----	-	-	-	-	+	-	-	+
d-w-	----	-	-	-	-	-	-	-	-
d-wx	----	+	+	-	-	+	-	+	+
dr--	----	-	-	-	-	-	-	-	-
dr-x	----	-	-	-	-	+	+	-	+
drw-	----	-	-	-	-	-	-	-	-
drwx	----	+	+	-	-	+	+	+	+
d---	---x	-	-	-	-	-	-	-	-
d--x	---x	-	-	-	-	+	-	-	+
d-w-	---x	-	-	-	-	-	-	-	-
d-wx	---x	+	+	-	-	+	-	+	+
dr--	---x	-	-	-	-	-	-	-	-
dr-x	---x	-	-	-	-	+	+	-	+
drw-	---x	-	-	-	-	-	-	-	-
drwx	---x	+	+	-	-	+	+	+	+
d---	--w-	-	-	-	-	-	-	-	-
d--x	--w-	-	-	+	-	+	-	-	+
d-w-	--w-	-	-	-	-	-	-	-	-
d-wx	--w-	+	+	+	-	+	-	+	+

		Про- смотр							
Права		Со-		За-	Чте-	Сме-	фай-	Пере-	Сме-
ди-		зда-	Уда-	пись	ние	на	лов в	име-	на
ректо-	Права	ние	ление	в	из	ректо-	ректо-	ние	атри-
рии	файла	файла	файла	файл	файла	рии	рии	файла	бутов
									файла
dr--	--w-	-	-	-	-	-	-	-	-
dr-x	--w-	-	-	+	-	+	+	-	+
drw-	--w-	-	-	-	-	-	-	-	-
drwx	--w-	+	+	+	-	+	+	+	+
d---	--wx	-	-	-	-	-	-	-	-
d--x	--wx	-	-	+	-	+	-	-	+
d-w-	--wx	-	-	-	-	-	-	-	-
d-wx	--wx	+	+	+	-	+	-	+	+
dr--	--wx	-	-	-	-	-	-	-	-
dr-x	--wx	-	-	+	-	+	+	-	+
drw-	--wx	-	-	-	-	-	-	-	-
drwx	--wx	+	+	+	-	+	+	+	+
d---	-r--	-	-	-	-	-	-	-	-
d--x	-r--	-	-	-	+	+	-	-	+
d-w-	-r--	-	-	-	-	-	-	-	-
d-wx	-r--	+	+	-	+	+	-	+	+
dr--	-r--	-	-	-	-	-	-	-	-
dr-x	-r--	-	-	-	+	+	+	-	+
drw-	-r--	-	-	-	-	-	-	-	-
drwx	-r--	+	+	-	+	+	+	+	+
d---	-r-x	-	-	-	-	-	-	-	-
d--x	-r-x	-	-	-	+	+	-	-	+

Про- смотр									
Права		Со-		За-	Чте-	Сме-	фай-	Пере-	Сме-
ди-		зда-	Уда-	пись	ние	на	лов в	име-	на
ректо-	Права	ние	ление	в	из	ректо-	ректо-	нова-	атри-
рии	файла	файла	файла	файл	файла	рии	рии	файла	бутов
									файла
d-w-	-r-x	-	-	-	-	-	-	-	-
d-wx	-r-x	+	+	-	+	+	-	+	+
dr--	-r-x	-	-	-	-	-	-	-	-
dr-x	-r-x	-	-	-	+	+	+	-	+
drw-	-r-x	-	-	-	-	-	-	-	-
drwx	-r-x	+	+	-	+	+	+	+	+
d---	-rw-	-	-	-	-	-	-	-	-
d--x	-rw-	-	-	+	+	+	-	-	+
d-w-	-rw-	-	-	-	-	-	-	-	-
d-wx	-rw-	+	+	+	+	+	-	+	+
dr--	-rw-	-	-	-	-	-	-	-	-
dr-x	-rw-	-	-	+	+	+	+	-	+
drw-	-rw-	-	-	-	-	-	-	-	-
drwx	-rw-	+	+	+	+	+	+	+	+
d---	-rwx	-	-	-	-	-	-	-	-
d--x	-rwx	-	-	+	+	+	-	-	+
d-w-	-rwx	-	-	-	-	-	-	-	-
d-wx	-rwx	+	+	+	+	+	-	+	+
dr--	-rwx	-	-	-	-	-	-	-	-
dr-x	-rwx	-	-	+	+	+	+	-	+
drw-	-rwx	-	-	-	-	-	-	-	-

		Про- смотр							
Права		Со-	За-	Чте-	Сме-	фай-	Пере-	Сме-	
ди-		зда-	Уда-	пись	на	лов в	име-	на	
ректо-	Права	ние	ление	в	из	ректо-	ректо-	нове-	атри-
рии	файла	файла	файла	файл	файла	рии	рии	файла	бутов
									файла
drwx	-rwx	+	+	+	+	+	+	+	+

10. На основании заполненной таблицы определила те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполнила табл. 2

Таблица 2: Минимальные права для совершения операций

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

Выводы

Научились работать в консоли с атрибутами файлов, закрепили теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы

1. Основы безопасности информационных систем : Учеб. пособие для студентов вузов, обучающихся по специальностям “Компьютер. безопасность” и “Комплекс. обеспечение информ. безопасности автоматизир. систем” / Д.А. Зегжда, А.М. Ивашко. - М. : Горячая линия - Телеком, 2000. - 449, [2] с. : ил., табл.; 21 см.; ISBN 5-93517-018-3.