

Лабораторная работа №2

Основы информационной безопасности

Волгин Иван Алексеевич

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	9
4	Выводы	16

Список иллюстраций

3.1	создание пользователя guest	9
3.2	создание пароля для пользователя guest	9
3.3	вход в систему под новым пользователем	10
3.4	проверка текущей директории	10
3.5	имя пользователя	10
3.6	информация команды id	11
3.7	информация команды groups	11
3.8	просмотр файла /etc/passwd	11
3.9	информация о пользователе	11
3.10	существующие в системе директории	11
3.11	расширенные атрибуты установлены поддиректорий	12
3.12	создание директории dir1	12
3.13	права доступа директории dir1	12
3.14	разрешенные атрибуты директории dir1	12
3.15	снятие прав доступа с dir1	13
3.16	попытка создания файла file1	13
3.17	проверка его нахождения в dir1	13
3.18	Таблицу «Установленные права и разрешённые действия» ч.1 . . .	14
3.19	Таблицу «Установленные права и разрешённые действия» ч.2 . . .	14
3.20	Таблицу «Установленные права и разрешённые действия» ч.3 . . .	15
3.21	Таблицу «Установленные права и разрешённые действия» ч.4 . . .	15
3.22	Таблица минимально необходимых прав для выполнения операций внутри директории dir1	15

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

2 Задание

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создайте учётную запись пользователя `guest` (используя учётную запись администратора): `useradd guest`
2. Задайте пароль для пользователя `guest` (используя учётную запись администратора): `passwd guest`
3. Войдите в систему от имени пользователя `guest`.
4. Определите директорию, в которой вы находитесь, командой `pwd`. Сравните её с приглашением командной строки. Определите, является ли она вашей домашней директорией? Если нет, зайдите в домашнюю директорию.
5. Уточните имя вашего пользователя командой `whoami`.
6. Уточните имя вашего пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. запомните. Сравните вывод `id` с выводом команды `groups`.
7. Просмотрите файл `/etc/passwd` командой `cat /etc/passwd`. Найдите в нём свою учётную запись. Определите `uid` пользователя. Определите `gid` пользователя. Сравните найденные значения с полученными в предыдущих пунктах. Замечание: в случае, когда вывод команды не умещается на одном экране монитора, используйте прокрутку вверх–вниз (удерживая клавишу `shift`, нажимайте `page up` и `page down`) либо программу `grep` в качестве фильтра для вывода только строк, содержащих определённые буквенные сочетания: `cat /etc/passwd | grep guest`
8. Определите существующие в системе директории командой `ls -l /home/`

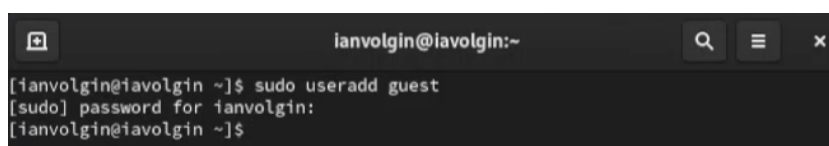
- Удалось ли вам получить список поддиректорий директории /home? Какие права установлены на директориях?
9. Проверьте, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: `lsattr /home` Удалось ли вам увидеть расширенные атрибуты директории? Удалось ли вам увидеть расширенные атрибуты директорий других пользователей?
 10. Создайте в домашней директории поддиректорию `dir1` командой `mkdir dir1` Определите командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`.
 11. Снимите с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверьте с её помощью правильность выполнения команды `ls -l`
 12. Попробуйте создать в директории `dir1` файл `file1` командой `echo "test" > /home/guest/dir1/file1` Объясните, почему вы получили отказ в выполнении операции по созданию файла? Оцените, как сообщение об ошибке отразилось на создании файла? Проверьте командой `ls -l /home/guest/dir1` действительно ли файл `file1` не находится внутри директории `dir1`
 13. Заполните таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесите в таблицу знак «+», если не разрешена, знак «-». Замечание 1: при заполнении табл. 2.1 рассматриваются не все атрибуты файлов и директорий, а лишь «первые три»: `g`, `w`, `x`, для «владельца». Остальные атрибуты также важны (особенно при использовании доступа от имени разных пользователей, входящих в те или иные группы). Проверка всех атрибутов при всех условиях значительно увеличила бы таблицу: так 9 атрибутов на директорию и 9 атрибутов на файл дают 218 строк без учёта дополнительных атрибутов, плюс таблица была бы расширена по количеству столбцов, так как все приведённые операции необходимо было бы повторить ещё как минимум для двух пользователей: входящего в группу владельца файла и не

входящего в неё. После полного заполнения табл. 2.1 и анализа полученных данных нам удалось бы выяснить, что заполнение её в таком виде излишне. Можно разделить большую таблицу на несколько малых независимых таблиц. В данном примере предлагается рассмотреть 3 + 3 атрибута, т.е. $2^6 = 64$ варианта. Замечание 2: в ряде действий при выполнении команды удаления файла вы можете столкнуться с вопросом: «удалить защищённый от записи пустой обычный файл dir1/file1?» Обратите внимание, что наличие этого вопроса не позволяет сделать правильный вывод о том, что файл можно удалить. В ряде случаев, при ответе «у» (да) на указанный вопрос, возможно получить другое сообщение: «невозможно удалить dir1 /file1: Отказано в доступе».

14. На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения операций внутри директории dir1.

3 Выполнение лабораторной работы

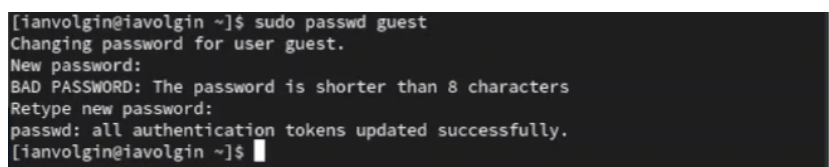
1. Создаю учетную запись пользователя guest (рис. 3.1).



```
ianvolgin@iavolgin:~  
[ianvolgin@iavolgin ~]$ sudo useradd guest  
[sudo] password for ianvolgin:  
[ianvolgin@iavolgin ~]$
```

Рис. 3.1: создание пользователя guest

2. Далее задаю пароль для пользователя guest (рис. 3.2).



```
[ianvolgin@iavolgin ~]$ sudo 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.  
[ianvolgin@iavolgin ~]$
```

Рис. 3.2: создание пароля для пользователя guest

3. Затем вхожу в систему под пользователем guest (рис. 3.3).

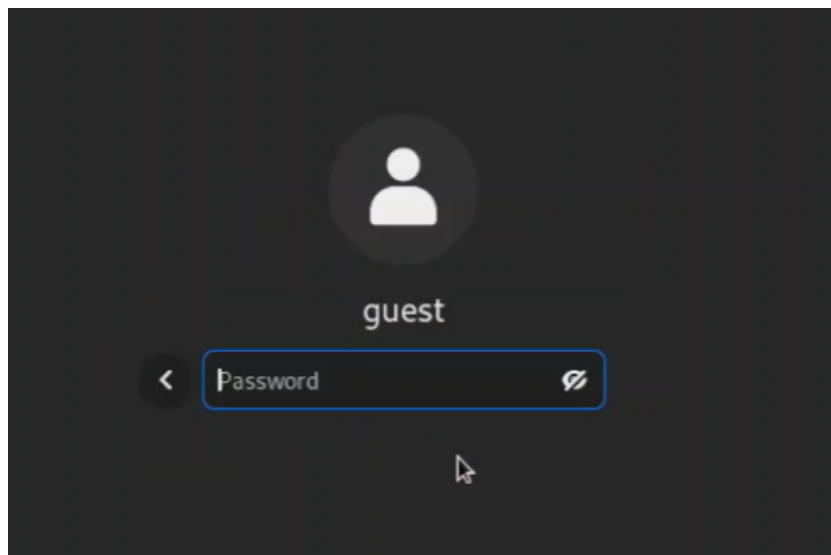


Рис. 3.3: вход в систему под новым пользователем

4. После этого нужно было проверить в какой директории я нахожусь с помощью команды `pwd` (рис. 3.4).

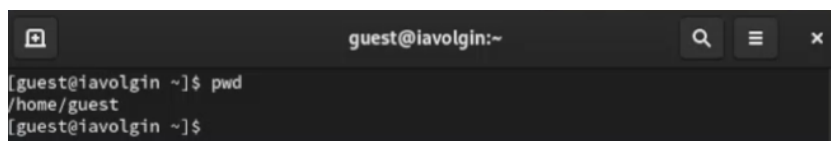


Рис. 3.4: проверка текущей директории

5. Далее уточняю имя пользователя, используя команду `whoami` (рис. 3.5).



Рис. 3.5: имя пользователя

6. Затем с помощью команды `id` уточняю имя моего пользователя, его группу, а также группы, куда он входит (рис. 3.6) и сравниваю с выводом команды `groups` (рис. 3.7). Команда `groups` выводит только имя пользователя в то время, как команда `id` дает более расширенную информацию о нем.

```
[guest@iavolgin ~]$ id
uid=1003(guest) gid=1003(guest) groups=1003(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@iavolgin ~]$
```

Рис. 3.6: информация команды id

```
[guest@iavolgin ~]$ id
uid=1003(guest) gid=1003(guest) groups=1003(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@iavolgin ~]$ groups
guest
[guest@iavolgin ~]$
```

Рис. 3.7: информация команды groups

- Далее нужно было просмотреть файл /etc/passwd командой cat /etc/passwd (рис. 3.8) и найти там информацию о моей учетной записи, я сделал это с помощью команды cat /etc/passwd | grep guest (рис. 3.9). uid и gid пользователя совпадают с теми, что я получил в прошлых пунктах.

```
[guest@iavolgin ~]$ 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
```

Рис. 3.8: просмотр файла /etc/passwd

```
[guest@iavolgin ~]$ cat /etc/passwd | grep guest
guest:x:1003:1003::/home/guest:/bin/bash
[guest@iavolgin ~]$
```

Рис. 3.9: информация о пользователе

- После этого нужно было определить существующие в системе директории командой ls -l /home/ (рис. 3.10)

```
[guest@iavolgin ~]$ ls -l /home/
total 8
drwx-----. 14 guest      guest      4096 Feb 23 16:36 guest
drwx-----. 14 ianvolgin ianvolgin 4096 Feb 23 16:36 ianvolgin
[guest@iavolgin ~]$
```

Рис. 3.10: существующие в системе директории

9. Затем я проверил, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: `lsattr /home` (рис. 3.11).

```
[guest@iavolgin ~]$ lsattr /home
lsattr: Permission denied while reading flags on /home/iavolgin
----- /home/guest
[guest@iavolgin ~]$
```

Рис. 3.11: расширенные атрибуты установлены поддиректорий

10. Далее я создаю домашней директории поддиректорию `dir1` командой `mkdir dir1` (рис. 3.12) и определяю командами `ls -l` (рис. 3.13) и `lsattr` (рис. 3.14), какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`.

```
[guest@iavolgin ~]$ mkdir dir1
[guest@iavolgin ~]$
```

Рис. 3.12: создание директории `dir1`

```
[guest@iavolgin ~]$ ls -l /home/guest
total 0
drwxr-xr-x. 2 guest guest 6 Feb 23 16:36 Desktop
drwxr-xr-x. 2 guest guest 6 Feb 23 16:45 dir1
drwxr-xr-x. 2 guest guest 6 Feb 23 16:36 Documents
drwxr-xr-x. 2 guest guest 6 Feb 23 16:36 Downloads
drwxr-xr-x. 2 guest guest 6 Feb 23 16:36 Music
drwxr-xr-x. 2 guest guest 6 Feb 23 16:36 Pictures
drwxr-xr-x. 2 guest guest 6 Feb 23 16:36 Public
drwxr-xr-x. 2 guest guest 6 Feb 23 16:36 Templates
drwxr-xr-x. 2 guest guest 6 Feb 23 16:36 Videos
[guest@iavolgin ~]$
```

Рис. 3.13: права доступа директории `dir1`

```
[guest@iavolgin ~]$ 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
----- /home/guest/dir1
[guest@iavolgin ~]$
```

Рис. 3.14: разрешенные атрибуты директории `dir1`

11. Затем я снимаю с директории dir1 все атрибуты командой `chmod 000 dir1` и проверяю с её помощью правильность выполнения команды `ls -l` (рис. 3.15)

```
[guest@iavolgin ~]$ chmod 000 dir1
[guest@iavolgin ~]$ ls -l /home/guest
total 0
drwxr-xr-x. 2 guest guest 6 Feb 23 16:36 Desktop
d----- . 2 guest guest 6 Feb 23 16:45 dir1
drwxr-xr-x. 2 guest guest 6 Feb 23 16:36 Documents
drwxr-xr-x. 2 guest guest 6 Feb 23 16:36 Downloads
drwxr-xr-x. 2 guest guest 6 Feb 23 16:36 Music
drwxr-xr-x. 2 guest guest 6 Feb 23 16:36 Pictures
drwxr-xr-x. 2 guest guest 6 Feb 23 16:36 Public
drwxr-xr-x. 2 guest guest 6 Feb 23 16:36 Templates
drwxr-xr-x. 2 guest guest 6 Feb 23 16:36 Videos
[guest@iavolgin ~]$
```

Рис. 3.15: снятие прав доступа с dir1

12. После этого я пытаюсь создать в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1` (должно быть отказано в доступе) (рис. 3.16) и проверяю командой `ls -l /home/guest/dir1` действительно ли файл file1 не находится внутри директории dir1 (тоже отказано в доступе) (рис. 3.17)

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

Рис. 3.16: попытка создания файла file1

```
[guest@iavolgin ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
[guest@iavolgin ~]$
```

Рис. 3.17: проверка его нахождения в dir1

13. Заполняю таблицу «Установленные права и разрешённые действия» (рис. 3.18) (рис. 3.19) (рис. 3.20) (рис. 3.21)

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переимено- вание файла	Смена атрибутов файла
d(000)	(000)	-	-	-	-	-	-	-	-
d(000)	(100)	-	-	-	-	-	-	-	-
d(000)	(200)	-	-	-	-	-	-	-	-
d(000)	(300)	-	-	-	-	-	-	-	-
d(000)	(400)	-	-	-	-	-	-	-	-
d(000)	(500)	-	-	-	-	-	-	-	-
d(000)	(600)	-	-	-	-	-	-	-	-
d(000)	(700)	-	-	-	-	-	-	-	-
d(100)	(000)	-	-	-	-	+	-	-	+
d(100)	(100)	-	-	-	-	+	-	-	+
d(100)	(200)	-	-	+	-	+	-	-	+
d(100)	(300)	-	-	+	-	+	-	-	+
d(100)	(400)	-	-	-	+	+	-	-	+
d(100)	(500)	-	-	-	+	+	-	-	+
d(100)	(600)	-	-	+	+	+	-	-	+
d(100)	(700)	-	-	+	+	+	-	-	+
d(200)	(000)	-	-	-	-	-	-	-	-
d(200)	(100)	-	-	-	-	-	-	-	-
d(200)	(200)	-	-	-	-	-	-	-	-
d(200)	(300)	-	-	-	-	-	-	-	-
d(200)	(400)	-	-	-	-	-	-	-	-

Рис. 3.18: Таблицу «Установленные права и разрешённые действия» ч.1

d(200)	(500)	-	-	-	-	-	-	-	-
d(200)	(600)	-	-	-	-	-	-	-	-
d(200)	(700)	-	-	-	-	-	-	-	-
d(300)	(000)	+	+	-	-	+	-	+	+
d(300)	(100)	+	+	-	-	+	-	+	+
d(300)	(200)	+	+	+	-	+	-	+	+
d(300)	(300)	+	+	+	-	+	-	+	+
d(300)	(400)	+	+	-	+	+	-	+	+
d(300)	(500)	+	+	-	+	+	-	+	+
d(300)	(600)	+	+	+	+	+	-	+	+
d(300)	(700)	+	+	+	+	+	-	+	+
d(400)	(000)	-	-	-	-	-	+	-	-
d(400)	(100)	-	-	-	-	-	+	-	-
d(400)	(200)	-	-	-	-	-	+	-	-
d(400)	(300)	-	-	-	-	-	+	-	-
d(400)	(400)	-	-	-	-	-	+	-	-

Рис. 3.19: Таблицу «Установленные права и разрешённые действия» ч.2

d(400)	(500)	-	-	-	-	-	+	-	-
d(400)	(600)	-	-	-	-	-	+	-	-
d(400)	(700)	-	-	-	-	-	+	-	-
d(500)	(000)	-	-	-	-	+	+	-	+
d(500)	(100)	-	-	-	-	+	+	-	+
d(500)	(200)	-	-	+	-	+	+	-	+
d(500)	(300)	-	-	+	-	+	+	-	+
d(500)	(400)	-	-	-	+	+	+	-	+
d(500)	(500)	-	-	-	+	+	+	-	+
d(500)	(600)	-	-	+	+	+	+	-	+
d(500)	(700)	-	-	+	+	+	+	-	+
d(600)	(000)	-	-	-	-	-	+	-	-
d(600)	(100)	-	-	-	-	-	+	-	-
d(600)	(200)	-	-	-	-	-	+	-	-
d(600)	(300)	-	-	-	-	-	+	-	-
d(600)	(400)	-	-	-	-	-	+	-	-
d(600)	(500)	-	-	-	-	-	+	-	-
d(600)	(600)	-	-	-	-	-	+	-	-
d(600)	(700)	-	-	-	-	-	+	-	-
d(700)	(000)	+	+	-	-	+	+	+	+
d(700)	(100)	+	+	-	-	+	+	+	+
d(700)	(200)	+	+	+	-	+	+	+	+

Рис. 3.20: Таблицу «Установленные права и разрешённые действия» ч.3

d(700)	(300)	+	+	+	-	+	+	+	+
d(700)	(400)	+	+	-	+	+	+	+	+
d(700)	(500)	+	+	-	+	+	+	+	+
d(700)	(600)	+	+	+	+	+	+	+	+
d(700)	(700)	+	+	+	+	+	+	+	+

Рис. 3.21: Таблицу «Установленные права и разрешённые действия» ч.4

14. Затем на основании заполненной таблицы определяю те или иные минимально необходимые права для выполнения операций внутри директории dir1 (рис. 3.22)

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d(300)	(000)
Удаление файла	d(300)	(000)
Чтение файла	d(100)	(400)
Запись в файл	d(100)	(200)
Переименование файла	d(300)	(000)
Создание поддиректории	d(300)	(000)
Удаление поддиректории	d(300)	(000)

Рис. 3.22: Таблица минимально необходимых прав для выполнения операций внутри директории dir1

4 Выводы

В ходе выполнения данной лабораторной работы я получил практические навыки работы в консоли с атрибутами файлов, закрепил теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.