

Лабораторная работа 5

Основы информационной безопасности

Симонова Полина Игоревна

2026-02-15

Содержание I

1. Информация
2. Элементы презентации
3. Выполнение лабораторной работы
4. Выводы

Раздел 1

1. Информация

1.1 Докладчик

Симонова Полина Игоревна; студент группы НКАбд-02-24

Раздел 2

2. Элементы презентации

2.1 Цели и задачи

Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов.
Получение практических навыков работы в консоли с дополнительными атрибутами.
Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

Раздел 3

3. Выполнение лабораторной работы

Для лабораторной работы необходимо проверить, установлен ли компилятор gcc, команда `gcc -V` позволяет это сделать. Также осуществляется отключение системы запретом с помощью `setenforce 0` (рис. 1).

```
pisimonova@pisimonova:~$ gcc -v
bash: gcc: команда не найдена...
Установить пакет «gcc», предоставляющий команду «gcc»? [N/y] y

* Ожидание в очереди...
* Загрузка списка пакетов...
Следующие пакеты должны быть установлены:
cpp-14.3.1-2.1.el10.x86_64      The C Preprocessor
gcc-14.3.1-2.1.el10.x86_64    Various compilers (C, C++, Objective-C, ...)
glibc-devel-2.39-58.el10_1.2.x86_64  Object files for development using standard C libraries.
kernel-headers-6.12.0-124.31.1.el10_1.x86_64  Header files for the Linux kernel for use by glibc
libxcrypt-devel-4.4.36-10.el10.x86_64  Development files for libxcrypt
Продолжить с этими изменениями? [N/y] y

* Ожидание в очереди...
* Ожидание аутентификации...
* Ожидание в очереди...
* Загрузка пакетов...
* Запрос данных...
* Проверка изменений...
* Установка пакетов...
```


Осуществляется вход от имени пользователя guest (рис. 2).

```
pisimonova@pisimonova:~$ su guest
```

Пароль :

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100

Рисунок 2: Вход от имени пользователя guest

Создание файла simpleid.c и запись в файл кода (рис. 3)

```
guest@pisimonova:~$ touch simpleid.c  
guest@pisimonova:~$ nano simpleid.c  
guest@pisimonova:~$ gcc simpleid.c -o simpleid
```

Рисунок 3: Создание файла

Компилирую файл, проверяю, что он скомпилировался (рис. 5)

```
guest@pisimonova:~$ gcc simpleid.c -o simpleid
guest@pisimonova:~$ ls
dir1          simpleid.c    Документы    Изображения  Общедоступные  Шаблоны
simpleid       Видео        Загрузки     Музыка        'Рабочий стол'
```

Рисунок 4: Компиляция файла

Запускаю исполняемый файл. В выводе файла выписаны номера пользователя и групп, от вывода при вводе `if`, они отличаются только тем, что информации меньше (рис. 6)

```
guest@pisimonova:~$ ./simpleid
uid=1001, gid=1001
guest@pisimonova:~$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Рисунок 5: Сравнение команд

Создание, запись в файл и компиляция файла simpleid2.c. Запуск программы (рис. 7)

```

guest@pisimonoa:~$ touch simpleid2.c
guest@pisimonoa:~$ nano simpleid2.c
guest@pisimonoa:~$ gcc simpleid2.c -o simpleid2
simpleid2.c: В функции «main»:
simpleid2.c:13:11: ошибка: в программе обнаружен некорректный символ «\342»
 13 | real_gid);<U+21AA><U+2192>
    |               ^~~~~~
simpleid2.c:13:12: ошибка: в программе обнаружен некорректный символ «\342»
 13 | real_gid);<U+21AA><U+2192>
    |               ^~~~~~
guest@pisimonoa:~$ nano simpleid2.c
guest@pisimonoa:~$ gcc simpleid2.c -o simpleid2
guest@pisimonoa:~$ ls
dir1      simpleid2.c  Документы  Музыка      Шаблоны
simpleid   simpleid.c   Загрузки  Общедоступные
simpleid2  Видео       Изображения 'Рабочий стол'
guest@pisimonoa:~$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001

```

Рисунок 6: Создание и компиляция файла

С помощью `chown` изменяю владельца файла на суперпользователя, с помощью `chmod` изменяю права доступа (рис. 9)

```
pisimonova@pisimonova:~$ sudo chown root:guest /home/guest/simpleid2
pisimonova@pisimonova:~$ sudo chmod u+s /home/guest/simpleid2

pisimonova@pisimonova:~$ sudo ls -l simpleid2
ls: невозможно получить доступ к 'simpleid2': Нет такого файла или каталога
pisimonova@pisimonova:~$ sudo ls -l /home/guest/simpleid2
-rwsr-xr-x. 1 root guest 16920 фев 14 14:38 /home/guest/simpleid2
```

Рисунок 7: Смена владельца файла и прав доступа к файлу

Сравнение вывода программы и команды `id`, наша команда снова вывела только ограниченное количество информации(рис. 10)

```
pisimonova@pisimonova:~$ sudo /home/guest/simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
pisimonova@pisimonova:~$ sudo id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:u
nconfined_t:s0-s0:c0.c1023
pisimonova@pisimonova:~$ su guest
```

Рисунок 8: Запуск файла

Создание и компиляция файла readfile.c (рис. 11)

```
guest@pisimonova:~$ touch readfile.c
guest@pisimonova:~$ nano readfile.c
guest@pisimonova:~$ gcc readfile.c -o readfile
guest@pisimonova:~$ ls
dir1          simpleid      simpleid.c    Загрузки     Общедоступные
readfile      simpleid2    Видео         Изображения  'Рабочий стол'
readfile.c    simpleid2.c  Документы     Музыка        Шаблоны
```

Рисунок 9: Создание и компиляция файла

Снова от имени суперпользователя меняю владельца файла readfile. Далее меняю права доступа так, чтобы пользователь guest не смог прочесть содержимое файла (рис. 13)

```
pisimonova@pisimonova:~$ sudo chown root:guest /home/guest/readfile.c
pisimonova@pisimonova:~$ sudo chmod u+s /home/guest/readfile.c
pisimonova@pisimonova:~$ sudo chmod 700 /home/guest/readfile.c
pisimonova@pisimonova:~$ sudo chmod -r /home/guest/readfile.c
pisimonova@pisimonova:~$ sudo chmod u+s /home/guest/readfile.c
pisimonova@pisimonova:~$ su guest
```

Рисунок 10: Смена владельца файла и прав доступа к файлу

Проверка прочесть файл от имени пользователя guest.Прочесть файл не удастся (рис. 14)

```
guest@pisimonova:~$ cat readfile.c
cat: readfile.c: Отказано в доступе
```

Рисунок 11: Попытка прочесть содержимое файла

Пробуем прочесть эти же файлы от имени суперпользователя и чтение файлов проходит успешно (рис. 17)

```
pisimonova@pisimonova:~$ sudo /home/guest/readfile /etc/shadow
root:$y$j9T$szYenPDDQgj0aE34FNj70aUF$gv8u9dZtGzaXbu1lf9KN3eK75PsAKe2BMP7xjB
BGibD::0:99999:7:::
bin:*:20186:0:99999:7:::
daemon:*:20186:0:99999:7:::
adm:*:20186:0:99999:7:::
lp:*:20186:0:99999:7:::
sync:*:20186:0:99999:7:::
shutdown:*:20186:0:99999:7:::
```

Рисунок 12: Чтение файла от имени суперпользователя

Проверяем папку tmp на наличие атрибута Sticky, т.к. в выводе есть буква t, то атрибут установлен (рис. 18)

```
pisimonova@pisimonova:~$ sudo ls -l / | grep tmp  
drwxrwxrwt. 18 root root 4096 фев 14 14:54 tmp
```

Рисунок 13: Проверка атрибутов директории tmp

От имени пользователя guest создаю файл с текстом, добавляю права на чтение и запись для других пользователей (рис. 19)

```

guest@pisimonova:~$ echo "test" > /tmp/file01.txt
guest@pisimonova:~$ ls
dir1      simpleid  simpleid.c  Загрузки  Общедоступные
readfile  simpleid2 Видео      Изображения 'Рабочий стол'
readfile.c simpleid2.c Документы  Музыка    Шаблоны
guest@pisimonova:~$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 фев 14 14:58 /tmp/file01.txt
guest@pisimonova:~$ chmod o+rw /tmp/file01.txt
guest@pisimonova:~$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 фев 14 14:58 /tmp/file01.txt

```

Рисунок 14: Создание файла, изменение прав доступа

Вхожу в систему от имени пользователя guest2, от его имени могу прочитать файл file01.txt, но перезаписать информацию в нем не могу (рис. 20)

```
guest@pisimonova:~$ su guest2
Пароль:
guest2@pisimonova:/home/guest$ cd
guest2@pisimonova:~$ cat /tmp/file01.txt
test
guest2@pisimonova:~$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
guest2@pisimonova:~$ cat /tmp/file01.txt
test
```

Рисунок 15: Попытка чтения файла

Далее пробуем удалить файл, снова получаем отказ (рис. 22)

```
guest2@pisimonova:~$ rm /tmp/file01.txt
rm: удалить защищённый от записи обычный файл '/tmp/file01.txt'? y
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
```

Рисунок 16: Попытка удалить файл

От имени суперпользователя снимаем с директории атрибут Sticky (рис. 23)

```
guest2@pisimonova:~$ su -  
Пароль:  
root@pisimonova:~# chmod -t /tmp  
root@pisimonova:~# exit  
ВЫХОД  
guest2@pisimonova:~$ ls -l / | grep tmp
```

Рисунок 17: Смена атрибутов файла

Раздел 4

4. Выводы

4. Выводы

Изучила механизм изменения идентификаторов, применила SetUID- и Sticky-биты. Получила практические навыки работы в консоли с дополнительными атрибутами. Рассмотрела работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.