

Презентация по лабораторной работе №5

Основы информационной безопасности

Дворкина Е. В

13 апреля 2024

Российский университет дружбы народов, Москва, Россия

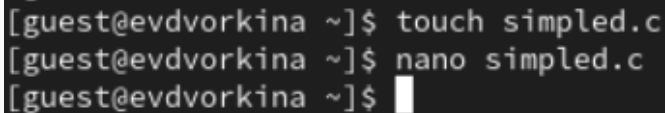
Информация

- Дворкина Ева Владимировна
- студентка группы НКАбд-01-22
- Российский университет дружбы народов
- <https://vk.com/yuri.kamori>



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

Создание файла `simplified.c` и запись в файл кода

A terminal window with a dark background and light gray text. It shows three lines of commands and their prompts. The first line is '[guest@evdvorkina ~]\$ touch simplified.c', the second is '[guest@evdvorkina ~]\$ nano simplified.c', and the third is '[guest@evdvorkina ~]\$' followed by a white cursor block.

```
[guest@evdvorkina ~]$ touch simplified.c  
[guest@evdvorkina ~]$ nano simplified.c  
[guest@evdvorkina ~]$
```

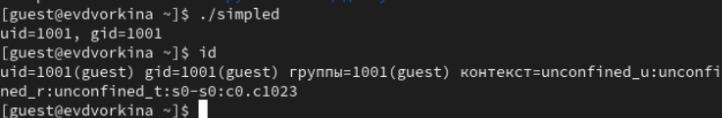
Рис. 1: Создание файла

Компилирую файл, проверяю, что он скомпилировался

```
[guest@evdvorkina ~]$ gcc simplified.c -o simplified
[guest@evdvorkina ~]$ ls
dir1      test      Видео      Изображения  'Рабочий стол'
simplified test10     Документы  Музыка        Шаблоны
simplified.c test2     Загрузки   Общедоступные
[guest@evdvorkina ~]$ ./simplified
```

Рис. 2: 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



```
[guest@evdvorkina ~]$ ./simplified
uid=1001, gid=1001
[guest@evdvorkina ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
[guest@evdvorkina ~]$
```

Рис. 3: Сравнение команд

Создание, запись в файл и компиляция файла `simplified2.c`. Запуск программы

```

[guest@evdvorkina ~]$ touch simplified2.c
[guest@evdvorkina ~]$ nano simplified2.c
[guest@evdvorkina ~]$ gcc simplified2.c -o simplified2
[guest@evdvorkina ~]$ ./simplified2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@evdvorkina ~]$

```

Рис. 4: Создание и компиляция файла

С помощью `chown` изменяю владельца файла на суперпользователя, с помощью `chmod` изменяю права доступа

```
[evdvorkina@evdvorkina ~]$ sudo chown root:guest /home/guest/simplified2  
[evdvorkina@evdvorkina ~]$ sudo chmod u+s /home/guest/simplified2  
[evdvorkina@evdvorkina ~]$ sudo ls -l /home/guest/simplified2  
-rwsr-xr-x. 1 root guest 26064 anp 13 03:57 /home/guest/simplified2  
[evdvorkina@evdvorkina ~]$
```

Рис. 5: Смена владельца файла и прав доступа к файлу

Выполнение лабораторной работы

Сравнение вывода программы и команды `id`, наша команда снова вывела только ограниченное количество информации

```
[evdvorkina@evdvorkina ~]$ sudo /home/guest/simplified2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[evdvorkina@evdvorkina ~]$ id
uid=1000(evdvorkina) gid=1000(evdvorkina) группы=1000(evdvorkina),10(wheel) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[evdvorkina@evdvorkina ~]$ sudo id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[evdvorkina@evdvorkina ~]$
```

Рис. 6: Запуск файла

Создание и компиляция файла readfile.c

```
[guest@evdvorkina ~]$ touch readfile.c
[guest@evdvorkina ~]$ nano readfile.c
[guest@evdvorkina ~]$ nano readfile.c
[guest@evdvorkina ~]$ gcc readfile.c -o readfile
[guest@evdvorkina ~]$ ls
dir1      simplified  simplified.c  test2      Загрузки   Общедоступные
readfile  simplified2 test          Видео      Изображения 'Рабочий стол'
readfile.c simplified2.c test10       Документы  Музыка     Шаблоны
```

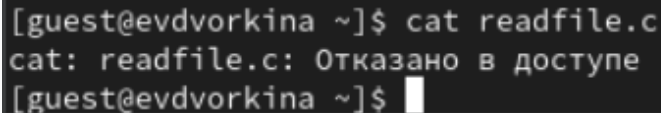
Рис. 7: Создание и компиляция файла

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

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

Рис. 8: Смена владельца файла и прав доступа к файлу

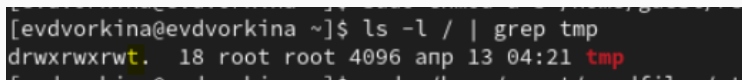
Проверка прочесть файл от имени пользователя guest. Прочесть файл не удастся

A terminal window with a black background and white text. The prompt is [guest@evdvorkina ~]\$. The user enters the command cat readfile.c. The output is cat: readfile.c: Отказано в доступе. The prompt returns to [guest@evdvorkina ~]\$.

```
[guest@evdvorkina ~]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@evdvorkina ~]$
```

Рис. 9: Попытка прочесть содержимое файла

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



```
[evdvorkina@evdvorkina ~]$ ls -l / | grep tmp
drwxrwxrwt. 18 root root 4096 apr 13 04:21 tmp
```

Рис. 11: Проверка атрибутов директории tmp

От имени пользователя guest создаю файл с текстом, добавляю права на чтение и запись для других пользователей

```
[guest@evdvorkina ~]$ echo "test" > /tmp/file01.txt
[guest@evdvorkina ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 anp 13 04:26 /tmp/file01.txt
[guest@evdvorkina ~]$ chmod o+rw /tmp/file01.txt
[guest@evdvorkina ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 anp 13 04:26 /tmp/file01.txt
[guest@evdvorkina ~]$
```

Рис. 12: Создание файла, изменение прав доступа

Выполнение лабораторной работы

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

```
[evdvorkina@evdvorkina ~]$ su guest2
Пароль:
su: Сбой при проверке подлинности
[evdvorkina@evdvorkina ~]$ su guest2
Пароль:
[guest2@evdvorkina evdvorkina]$ cat /tmp/file01.txt
test
[guest2@evdvorkina evdvorkina]$ echo 'test2' >> /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@evdvorkina evdvorkina]$ cat /tmp/file01.txt
test
[guest2@evdvorkina evdvorkina]$
```

Рис. 13: Попытка чтения файла

Также невозможно добавить в файл file01.txt новую информацию от имени пользователя guest2

```
[guest2@evdvorkina evdvorkina]$ echo 'test3' > /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@evdvorkina evdvorkina]$ cat /tmp/file01.txt
test
[guest2@evdvorkina evdvorkina]$
```

Рис. 14: Попытка записи в файл

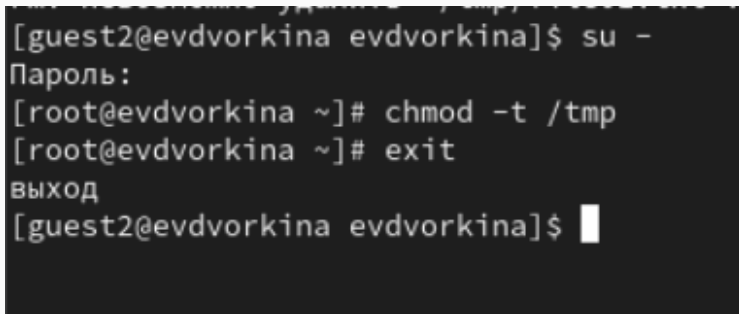
Далее пробуем удалить файл, снова получаем отказ

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

Рис. 15: Попытка удалить файл

Выполнение лабораторной работы

От имени суперпользователя снимаем с директории атрибут Sticky



```
[guest2@evdvorkina evdvorkina]$ su -  
Пароль:  
[root@evdvorkina ~]# chmod -t /tmp  
[root@evdvorkina ~]# exit  
выход  
[guest2@evdvorkina evdvorkina]$
```

Рис. 16: Смена атрибутов файла

Выполнение лабораторной работы

Далее был выполнен повтор предыдущих действий. По результатам без Sticky-бита запись в файл и дозапись в файл осталась невозможной, зато удаление файла прошло успешно

```
[guest2@evdvorkina evdvorkina]$ cat /tmp/file01.txt
test
[guest2@evdvorkina evdvorkina]$ echo 'test2' >> /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@evdvorkina evdvorkina]$ cat /tmp/file01.txt
test
[guest2@evdvorkina evdvorkina]$ echo 'test3' > /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@evdvorkina evdvorkina]$ cat /tmp/file01.txt
test
[guest2@evdvorkina evdvorkina]$ rm /tmp/file01.txt
rm: удалить защищенный от записи обычный файл '/tmp/file01.txt'? y
[guest2@evdvorkina evdvorkina]$ ls -l / | grep tmp
drwxrwxrwx. 18 root root 4096 апр 13 04:35 tmp
[guest2@evdvorkina evdvorkina]$ ls -l
ls: невозможно открыть каталог '.': Отказано в доступе
[guest2@evdvorkina evdvorkina]$ ls -l /home/guest
итого 108
drwx-----. 3 guest guest 38 map 3 01:55 dir1
-rwxr-xr-x. 1 guest guest 26008 апр 13 04:19 readfile
-rw-r--r--. 1 guest guest 402 апр 13 04:19 readfile1.c
--ws-----. 1 root guest 402 апр 13 04:08 readfile.c
-rwxr-xr-x. 1 guest guest 25960 апр 13 03:53 simplified
-rwsr-xr-x. 1 root guest 26064 апр 13 03:57 simplified2
-rw-r--r--. 1 guest guest 302 апр 13 03:56 simplified2.c
-rw-r--r--. 1 guest guest 175 апр 13 03:53 simplified.c
-rw-r--r--. 1 guest guest 5 фев 18 20:39 test
-----. 1 guest guest 5 фев 18 20:27 test10
```

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

...