

Лабораторная 5

Отчет

Карпачев Ярослав

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	9
4	Выводы	13

Список иллюстраций

3.1	Команды	9
3.2	Команды	10
3.3	Команды	10
3.4	Команды	11
3.5	Команды	11
3.6	Команды	12

Список таблиц

1 Цель работы

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

2 Задание

1. Войдите в систему от имени пользователя guest. 2. Создайте программу simpleid.c: 36 Кулябов Д. С., Королькова А. В., Геворкян М. Н. #include <sys/types.h> #include <unistd.h> #include <stdio.h> int main () { uid_t uid = getuid (); gid_t gid = getgid ();

return 0; } 3. Скомпилируйте программу и убедитесь, что файл программы создан: gcc simpleid.c -o simpleid 4. Выполните программу simpleid: ./simpleid 5. Выполните системную программу id: id и сравните полученный вами результат с данными предыдущего пункта задания. 6. Усложните программу, добавив вывод действительных идентификаторов: include <sys/types.h> include <unistd.h> include <stdio.h> int main () { uid_t real_uid = getuid (); uid_t e_uid = geteuid (); gid_t real_gid = getgid (); gid_t e_gid = getegid (); real_gid); return 0; } Получившуюся программу назовите simpleid2.c. 7. Скомпилируйте и запустите simpleid2.c: gcc simpleid2.c -o simpleid2 ./simpleid2 8. От имени суперпользователя выполните команды: Информационная безопасность компьютерных сетей 37 chown root:guest /home/guest/simpleid2 chmod u+s /home/guest/simpleid2 9. Используйте sudo или повысьте временно свои права с помощью su. Поясните, что делают эти команды. 10. Выполните проверку правильности установки новых атрибутов и смены владельца файла simpleid2: ls -l simpleid2 11. Запустите simpleid2 и id: ./simpleid2 id Сравните результаты. 12. Прodelайте тоже самое относительно SetGID-бита. 13. Создайте программу readfile.c: #include <fcntl.h> #include <stdio.h> #include <sys/stat.h> #include <sys/types.h> #include <unistd.h> int main (int argc, char* argv[]) { unsigned char buffer[16]; size_t bytes_read; int i; int fd =

```
open (argv[1], O_RDONLY); do { bytes_read = read (fd, buffer, sizeof (buffer)); for (i =0; i < bytes_read; ++i) printf("%c", buffer[i]); } while (bytes_read == sizeof (buffer)); close (fd); return 0; }
```

14. Откомпилируйте её. `gcc readfile.c -o readfile` 15. Смените владельца у файла `readfile.c` (или любого другого текстового файла в системе) и измените права так, чтобы только суперпользователь (`root`) мог прочитать его, а `guest` не мог. 16. Проверьте, что пользователь `guest` не может прочитать файл `readfile.c`. 17. Смените у программы `readfile` владельца и установите SetU'D-бит. 18. Проверьте, может ли программа `readfile` прочитать файл `readfile.c`? 19. Проверьте, может ли программа `readfile` прочитать файл `/etc/shadow`? Отрадите полученный результат и ваши объяснения в отчёте.

38 Кулябов Д. С., Королькова А. В., Геворкян М. Н. 5.3.2. Исследование Sticky-бита 1. Выясните, установлен ли атрибут Sticky на директории `/tmp`, для чего выполните команду `ls -l | grep tmp` 2. От имени пользователя `guest` создайте файл `file01.txt` в директории `/tmp` со словом `test`: `echo "test" > /tmp/file01.txt` 3. Просмотрите атрибуты у только что созданного файла и разрешите чтение и запись для категории пользователей «все остальные»: `ls -l /tmp/file01.txt` `chmod o+rw /tmp/file01.txt` `ls -l /tmp/file01.txt` 4. От пользователя `guest2` (не являющегося владельцем) попробуйте прочитать файл `/tmp/file01.txt`: `cat /tmp/file01.txt` 5. От пользователя `guest2` попробуйте дописать в файл `/tmp/file01.txt` слово `test2` командой `echo "test2" > /tmp/file01.txt` Удалось ли вам выполнить операцию? 6. Проверьте содержимое файла командой `cat /tmp/file01.txt` 7. От пользователя `guest2` попробуйте записать в файл `/tmp/file01.txt` слово `test3`, стерев при этом всю имеющуюся в файле информацию командой `echo "test3" > /tmp/file01.txt` Удалось ли вам выполнить операцию? 8. Проверьте содержимое файла командой `cat /tmp/file01.txt` 9. От пользователя `guest2` попробуйте удалить файл `/tmp/file01.txt` командой `rm /tmp/file01.txt` Удалось ли вам удалить файл? 10. Повысьте свои права до суперпользователя следующей командой `su -` и выполните после этого команду, снимающую атрибут `t` (Sticky-бит) с директории `/tmp`: `chmod -t /tmp` 11. Покиньте режим суперпользователя командой `exit` 12. От пользователя `guest2` проверьте, что атрибута `t` у

директории /tmp нет: `ls -l / | grep tmp` 13. Повторите предыдущие шаги. Какие наблюдаются изменения? 14. Удалось ли вам удалить файл от имени пользователя, не являющегося его владельцем? Ваши наблюдения занесите в отчёт. Информационная безопасность компьютерных сетей 39 15. Повысьте свои права до суперпользователя и верните атрибут t на директорию /tmp: `su - chmod +t /tmp exit`

3 Выполнение лабораторной работы

1. Выполняем команды данные в задании.

данные которые выводит программа совпадают с данными команды id, продвинутая программа единственная выводит 27(sudo) а не 1001(guest)

```
File Actions Edit View Help
$ ls
Desktop  Documents  Music      Public     Videos
dir1     Downloads  Pictures   Templates
$ touch simpleid.c
$ vim simpleid.c
$ gcc simpleid.c -o simpleid
cc1: fatal error: leid.c: No such file or directory
compilation terminated.
$ ls
Desktop  Documents  Music      Public     Templates
dir1     Downloads  Pictures   simpleid.c Videos
$ g++ simpleid.c
$ ls
a.out    dir1       Downloads  Pictures   simpleid.c Videos
Desktop  Documents  Music      Public     Templates
$ ./a.out
uid=1001, gid=1001
$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest),27(sudo)
$ vim simpleid.c
$ g++ ./simpleid
/usr/bin/ld: cannot find ./simpleid: No such file or directory
collect2: error: ld returned 1 exit status
$ g++ simpleid.c
$ ./a.out
uid=1001, gid=1001
real_uid=1001, real_gid=1001
$ sudo chown root:guest /home/guest/simpleid
[sudo] password for guest:
chown: cannot access '/home/guest/simpleid': No such file or directory
$ sudo chown root:guest /home/guest/simpleid.c
$ chmod u+s /home/guest/a.out
$ sudo chown root:guest /home/guest/a.out
$ ls -l a.out
-rwxrwxr-x 1 root guest 16160 Apr  7 04:14 a.out
$ ./a.out
uid=1001, gid=1001
real_uid=1001, real_gid=1001
$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest),27(sudo)
$ touch simpleid3.c
$ vim simpleid3.c
$ g++ simpleid3.c
cc1plus: fatal error: simpleid3.c: No such file or directory
compilation terminated.
$ ls
a.out  Desktop  dir1  Documents  Downloads  Music  Pictures  Public  simpleid3.c  simpleid.c  Templates  Videos
$ g++ simpleid3.c
$
```

Рис. 3.1: Команды

2. пишем программу readfile (simpleid3.c) и пытаемся исполнит ее с входными данными, после изменение владельца, выдается ошибка нет прав

```

$ touch simpleid3.c
$ vim simpleid3.c
$ g++ simpleid3.c
ccplus: Fatal error: simpleid3.c: No such file or directory
compilation terminated.
$ ls
a.out Desktop dir1 Documents Downloads Music Pictures Public simpleid3.c simpleid.c Templates Videos
$ g++ simpleid3.c
$ sudo chown root:root a.out
/bin/sh: 26: sudo: not found
$ sudo chown root:root a.out
$ sudo chmod 400 a.out
$ cat a.out
cat: a.out: Permission denied
$ sudo chown root a.out
$ sudo chmod u+s a.out
$ a.out
/bin/sh: 32: a.out: not found
$ ./a.out
/bin/sh: 33: ./a.out: Permission denied
$ ./a.out /etc/shadow
/bin/sh: 34: ./a.out: Permission denied
$

```

Рис. 3.2: Команды

3. подготавливаем файл file01.txt к тестам в одном пользователя а потом меняем пользователя на guest3

```

> File Actions Edit View Help
$ ls -l / | grep tmp
drwxrwxrwt 14 root root 340 Apr 7 04:32 tmp
$ echo "test" > /tmp/file01.txt
$ ls -l /tmp/file01.txt
-rw-rw-r-- 1 guest guest 5 Apr 7 04:34 /tmp/file01.txt
$ chmod o+rw /tmp/file01.txt
$ ls -l /tmp/file01.txt
-rw-rw-rw- 1 guest guest 5 Apr 7 04:34 /tmp/file01.txt
$

```

Рис. 3.3: Команды

4. со стороны guest3 все команды работают кроме удаления файла так нет прав

```

$ cat /tmp/file01.txt
test
$ echo "test2" > /tmp/file01.txt
$ cat /tmp/file01.txt
test2
$ echo "test3" >> /tmp/file01.txt
$ cat /tmp/file01.txt
test2
test3
$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': Operation not permitted
$ su -
Password:
su: Authentication failure
$ su -
Password:
su: Authentication failure
$ su chmod -t /tmp
su: invalid option -- 't'
Try 'su --help' for more information.
$ su
Password:
su: Authentication failure
$ sudo su -
[sudo] password for guest3:
guest3 is not in the sudoers file.
$

```

Рис. 3.4: Команды

5. через садуера снимаем -t

```

(yokarpachev@vbox)-[/tmp]
$ sudo chmod -t /tmp
[sudo] password for yokarpachev:
(yokarpachev@vbox)-[/tmp]
$

```

Рис. 3.5: Команды

6. проверяю команды через guest3, все работает даже удаление файла

```

$ ls -l | grep tmp
$ echo "test" >> /tmp/file01.txt
$ cat /tmp/file01.txt
test
$ echo "test2" > /tmp/file01.txt
$ cat /tmp/file01.txt
test2
$ ls /tmp
config-err-XceTds
file01.txt
ssh-1JjFgln79nqu
systemd-private-0d2711eae0d147a9b4575deebd2902a8-apache2.service-LHAsPH
systemd-private-0d2711eae0d147a9b4575deebd2902a8-colord.service-illXdd
systemd-private-0d2711eae0d147a9b4575deebd2902a8-haveged.service-06c5Lg
systemd-private-0d2711eae0d147a9b4575deebd2902a8-ModemManager.service-yAbgMK
systemd-private-0d2711eae0d147a9b4575deebd2902a8-polkit.service-eSmmNr
systemd-private-0d2711eae0d147a9b4575deebd2902a8-systemd-logind.service-oMCqZ
W
systemd-private-0d2711eae0d147a9b4575deebd2902a8-upower.service-zjpsTk
$ ls -l } grep /tmp
ls: cannot access '}': No such file or directory
ls: cannot access 'grep': No such file or directory
/tmp:
total 4
-rw----- 1 guest3 guest3  0 Apr  7 05:09 config-err-XceTds
-rw-rw-r-- 1 guest3 guest3  6 Apr  7 05:11 file01.txt
drwx----- 2 guest3 guest3 60 Apr  7 05:09 ssh-1JjFgln79nqu
drwx----- 3 root   root   60 Apr  7 05:09 systemd-private-0d2711eae0d147a9b4
575deebd2902a8-apache2.service-LHAsPH
drwx----- 3 root   root   60 Apr  7 05:09 systemd-private-0d2711eae0d147a9b4
575deebd2902a8-colord.service-illXdd
drwx----- 3 root   root   60 Apr  7 05:09 systemd-private-0d2711eae0d147a9b4
575deebd2902a8-haveged.service-06c5Lg
drwx----- 3 root   root   60 Apr  7 05:09 systemd-private-0d2711eae0d147a9b4
575deebd2902a8-ModemManager.service-yAbgMK
drwx----- 3 root   root   60 Apr  7 05:09 systemd-private-0d2711eae0d147a9b4
575deebd2902a8-polkit.service-eSmmNr
drwx----- 3 root   root   60 Apr  7 05:09 systemd-private-0d2711eae0d147a9b4
575deebd2902a8-systemd-logind.service-oMCqZW
drwx----- 3 root   root   60 Apr  7 05:09 systemd-private-0d2711eae0d147a9b4
575deebd2902a8-upower.service-zjpsTk
$ rm /tmp/file01.txt
$ █

```

Рис. 3.6: Команды

4 Выводы

Я научился применять механизмы изменения идентификаторов, применять SetUID- и Sticky-битов. ции возможны при тех или иных установленных правах. Опробовал дей- ствие на практике расширенных атрибутов «a» и «i»