Презентация по лабораторной работе №5

Основы информационной безопасности

Бережной И. А.

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Бережной Иван Александрович
- студент 2-ого курса
- Российский университет дружбы народов
- 1132236041@pfur.ru

Цель

Изучить механизмы изменения идентификаторов, применения SetUID- и Sticky-битов.

Получить практические навыки работы в консоли с дополнительными атрибутами.

Рассмотреть работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

Задачи

1. Создать программы
2. Исследовать Sticky-бит

Выполнение лабораторной работы

Выполнение лабораторной работы

Войдём в систему от имени пользователя guest и создадим программу `simpleid.c`. Скомпилируем программу и убедимся, что файл создан. Выполним программу, а также команду `id`, и сравним результаты.

```
[guest@iaberezhnoyj ~]$ ./simpleid
uid=1001, gid=1001
[guest@iaberezhnoyj ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfin
ed_r:unconfined_t:s0-s0:c0.c1023
```

Рис. 1: Сравнение simpleid и команды id

Усовершенствуем нашу программу, добавив вывод действительных идентификаторов. Скомпилируем и запустим новую программу. От имени суперпользователя меняем владельца файла на суперпользователя и меняем права с помощью `chmod`. Проверим правильность установки атрибутов.

```
[guest@iaberezhnoyj ~]$ gcc simpleid2.c -o simpleid2
[guest@iaberezhnoyj ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
```

Рис. 2: Запуск simpleid2

Выполнение лабораторной работы

Запустим `simpleid2` и `id`. Собственная команда выводит всё ещё ограниченное количество информации.

```
[iaberezhnoyj@iaberezhnoyj ~]$ sudo /home/guest/simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[iaberezhnoyj@iaberezhnoyj ~]$ id
uid=1000(iaberezhnoyj) gid=1000(iaberezhnoyj) groups=1000(iaberezhnoyj),10(wheel
) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[iaberezhnoyj@iaberezhnoyj ~]$ sudo id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfi
ned_t:s0-s0:c0.c1023
```

Рис. 3: Запуск simpleid2 и id после смены прав

Создадим программу `readfile.c`. Сменим владельца у файла `readfile.c` и изменим права так, чтобы только суперпользователь смог его прочитать. Попробуем прочитать файл от имени `guest`. Получили ошибку. Попытки прочитать файл другими путями также не увенчались успехом.

Рис. 4: Неудачные попытки чтения readfile.c

Посмотрим, установлен ли атрибует Sticky на директории /tmp. В выводе присутствует буква `t`, значит, установлен.

```
[iaberezhnoyj@iaberezhnoyj ~]$ ls -l / | grep tmp
drwxrwxrwt.  17 root root 4096 Apr 19 16:49 tmp
```

Рис. 5: Проверка Sticky-бита в /tmp

От имени пользователя guest создадим фалй `file01.txt` в директории /tmp, разрешим чтение и запись для остальных польователей. Теперь от имени пользователя guest2 попробуем прочитать файл (успешно) и дописать что-либо в него (ошибка доступа). Также не получается удалить файл.

```
[guest@iaberezhnoyj ~]$ su guest2
Password:
[guest2@iaberezhnoyj guest]$ cat /tmp/file01.txt
test
[guest2@iaberezhnoyj guest]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@iaberezhnoyj guest]$ rm /tmp/fileOl.txt
rm: cannot remove '/tmp/fileOl.txt': No such file or directory
```

Рис. 6: Попытка записи и удаления file01.txt от guest2

Повысим права до суперпользователя и снимем атрибут `t` с файла. Снова от имени пользователя guest2 повторим попытку выполнить команды. Кроме того, что получилось удалить файл, ничего не поменялось. Вернём атрибут.

```
[iaberezhnoyj@iaberezhnoyj ~]$ su -
Password:
[root@iaberezhnoyj ~]# chmod -t /tmp
[root@iaberezhnoyj ~]# su guest2
[guest2@iaberezhnoyj root]$ ls -l / | grep tmp
drwxrwxrwx.  18 root root 4096 Apr 19 16:53 tmp
```

Рис. 7: Снятие Sticky-бита с /tmp

Вывод

В результате выполнения работы мы изучили механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получили практические навыки работы в консоли с дополнительными атрибутами. Рассмотрели работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

Список литературы

[1] Основы информационной безопасности, РУДН:
https://esystem.rudn.ru/mod/resource/view.php?id=1220153