# Информационная безопасность

## Лабораторная работа №5

## Презентация

Кузнецов Юрий Владимирович

### 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.

### Ход работы:

1. Войдите в систему от имени пользователя guest.

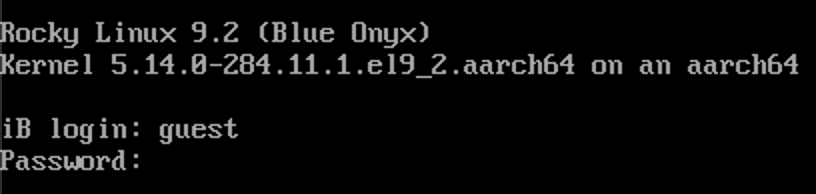


рис.1

1. Создайте программу simpleid.c:

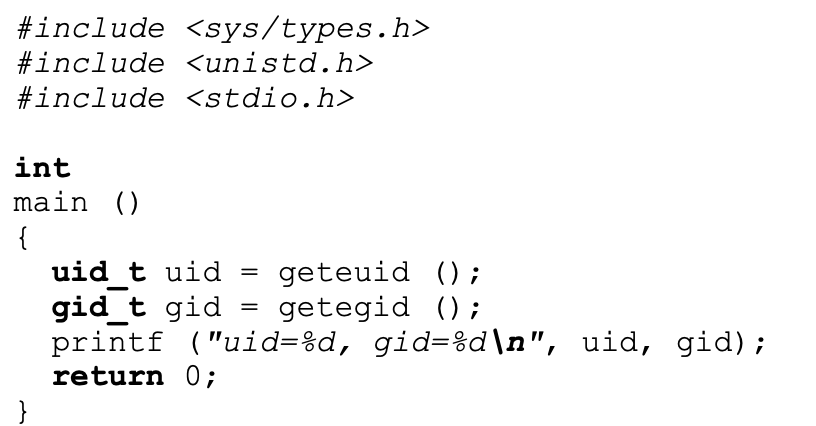


рис.2

1. Скомплилируйте программу и убедитесь, что файл программы создан: gcc simpleid.c -o simpleid

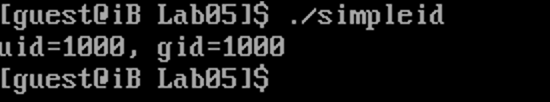


рис.3

1. Выполните программу simpleid:

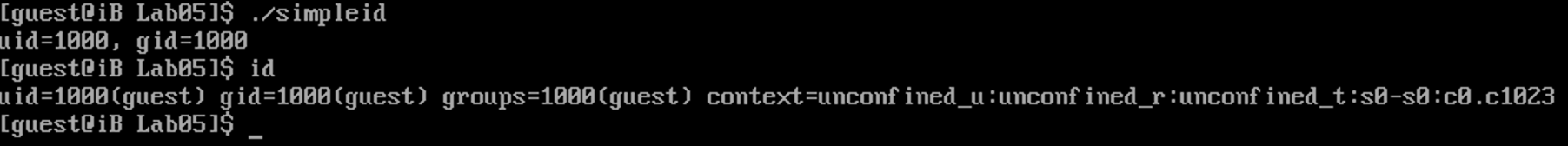


рис.4

1. Выполните системную программу id: id и сравните полученный вами результат с данными предыдущего пункта задания.

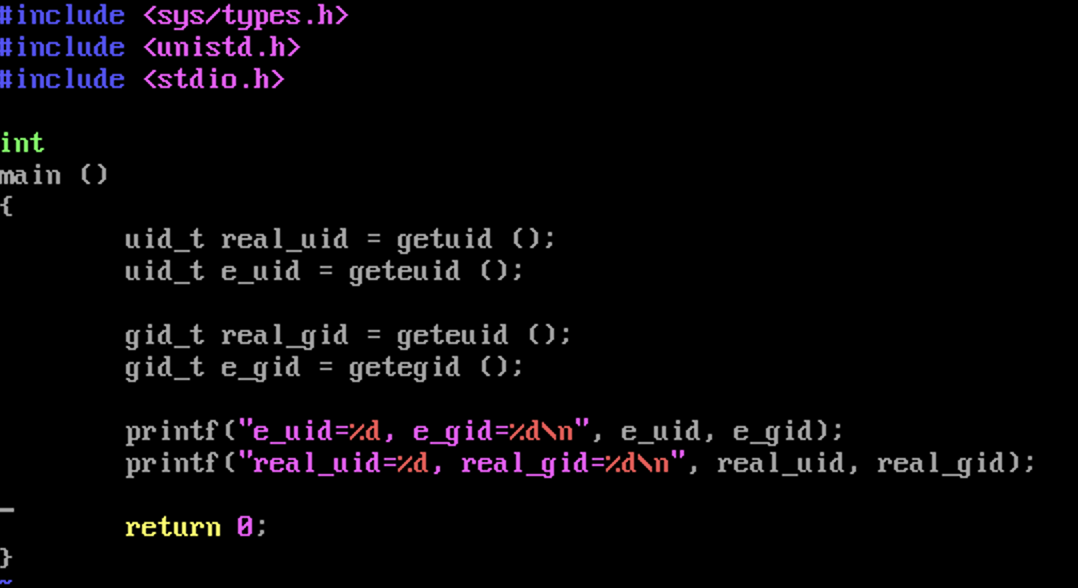


рис.5

1. Усложните программу, добавив вывод действительных идентификато- ров:

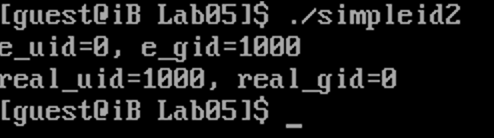


рис.6

1. Скомпилируйте и запустите simpleid2.c: gcc simpleid2.c -o simpleid2 ./simpleid2
2. От имени суперпользователя выполните команды: chown root:guest /home/guest/simpleid2 chmod u+s /home/guest/simpleid2
3. Используйте sudo или повысьте временно свои права с помощью su. Поясните, что делают эти команды.
4. Выполнитепроверкуправильностиустановкиновыхатрибутовисмены владельца файла simpleid2: ls -l simpleid2
5. Запустите simpleid2 и id: ./simpleid2 id
6. Проделайте тоже самое относительно SetGID-бита.
7. Создайте программу readfile.c:
8. Откомпилируйте её. gcc readfile.c -o readfile
9. Смените владельца у файла readfile.c (или любого другого текстового файла в системе) и измените права так, чтобы только суперпользователь (root) мог прочитать его, a guest не мог.
10. Проверьте, что пользователь guest не может прочитать файл readfile.c.
11. Смените у программы readfile владельца и установите SetU’D-бит.
12. Проверьте, может ли программа readfile прочитать файл readfile.c?
13. Проверьте, может ли программа readfile прочитать файл /etc/shadow? Отразите полученный результат и ваши объяснения в отчёте.
14. Выясните, установлен ли атрибут Sticky на директории /tmp, для чего выполните команду ls -l / | grep tmp
15. Отименипользователяguestсоздайтефайлfile01.txtвдиректории/tmp со словом test: echo “test” > /tmp/file01.txt
16. Просмотрите атрибуты у только что созданного файла и разрешите чте- ние и запись для категории пользователей «все остальные»: ls -l /tmp/file01.txt chmod o+rw /tmp/file01.txt ls -l /tmp/file01.txt
17. От пользователя guest2 (не являющегося владельцем) попробуйте про- читать файл /tmp/file01.txt: cat /tmp/file01.txt
18. От пользователя guest2 попробуйте дозаписать в файл /tmp/file01.txt слово test2 командой echo “test2” > /tmp/file01.txt Удалось ли вам выполнить операцию?
19. Проверьте содержимое файла командой cat /tmp/file01.txt
20. От пользователя guest2 попробуйте записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию ко- мандой echo “test3” > /tmp/file01.txt Удалось ли вам выполнить операцию?
21. Проверьте содержимое файла командой cat /tmp/file01.txt
22. Отпользователяguest2попробуйтеудалитьфайл/tmp/file01.txtко- мандой rm /tmp/fileOl.txt Удалось ли вам удалить файл?
23. Повысьте свои права до суперпользователя следующей командой su - и выполните после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp: chmod -t /tmp
24. Покиньте режим суперпользователя командой exit
25. От пользователя guest2 проверьте, что атрибута t у директории /tmp нет: ls -l / | grep tmp
26. Повторите предыдущие шаги. Какие наблюдаются изменения?
27. Удалось ли вам удалить файл от имени пользователя, не являющегося его владельцем? Ваши наблюдения занесите в отчёт.
28. Повысьте свои права до суперпользователя и верните атрибут t на ди- ректорию /tmp: su - chmod +t /tmp exit

### Вывод:

Мы изучили 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.