Отчет по лабораторной работе №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Александр Олегович Воробьев

Содержание

# 1 Цель работы

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.

# 2 Последовательность выполнения работы

## 2.1 Подготовка лабораторного стенда

1. Установка gcc

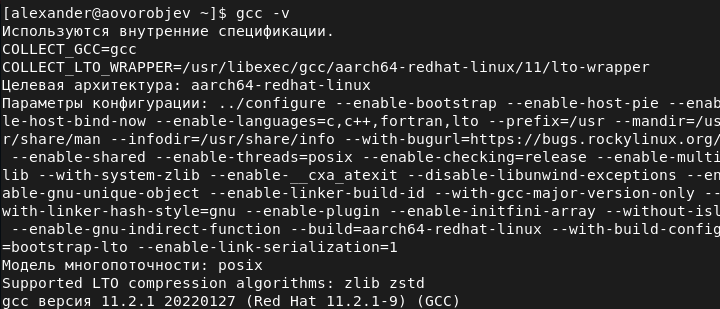


Figure 1: Установка gcc

## 2.2 Создание программы

1. Войдите в систему от имени пользователя guest.
2. Создайте программу simpleid.c:

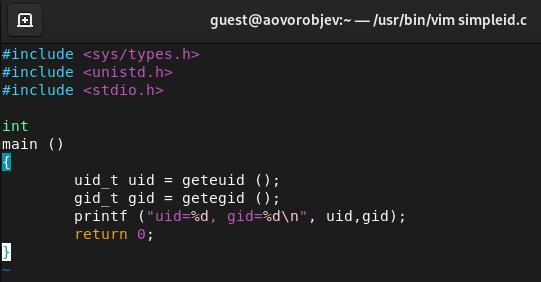


Figure 2: Создание программы

1. Скомплилируйте программу и убедитесь, что файл программы создан:  
   gcc simpleid.c -o simpleid
2. Выполните программу simpleid:  
   ./simpleid
3. Выполните системную программу id:  
   id  
   и сравните полученный вами результат с данными предыдущего пункта задания.

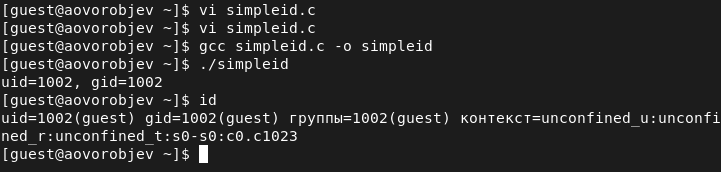


Figure 3: Компиляция программы

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

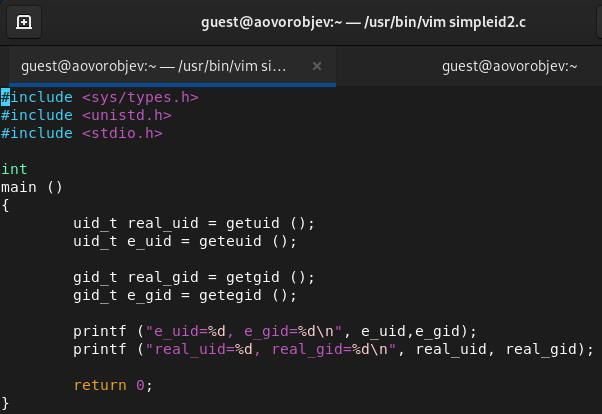


Figure 4: Усложненная программа

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  
   Сравните результаты.
6. Проделайте тоже самое относительно SetGID-бита.

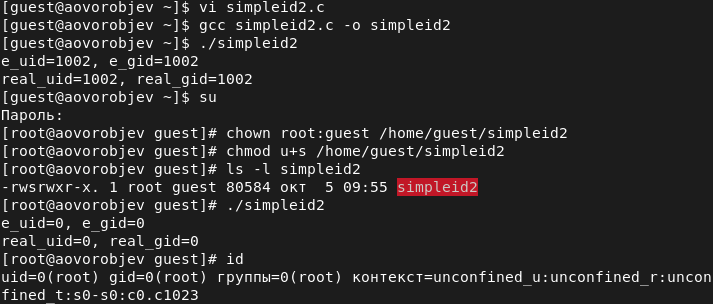


Figure 5: Компиляция усложненной программы, сравнение результатов

1. Создайте программу readfile.c:
2. Откомпилируйте её.  
   gcc readfile.c -o readfile

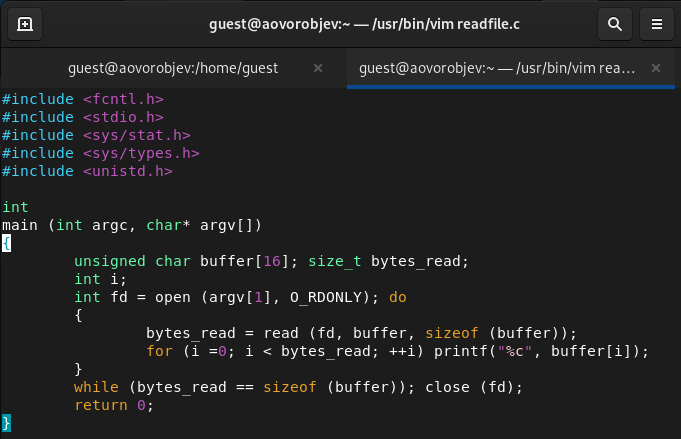


Figure 6: Создание новой программы

1. 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.

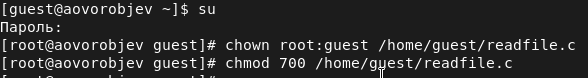


Figure 7: Смена владельца у файла

1. Проверьте, что пользователь guest не может прочитать файл readfile.c.

Figure 8: Проверка условия

Figure 8: Проверка условия

1. Смените у программы readfile владельца и установите SetU’D-бит.

Figure 9: смена владельца у файла

Figure 9: смена владельца у файла

1. Проверьте, может ли программа readfile прочитать файл readfile.c?



Figure 10: Проверка

1. Проверьте, может ли программа readfile прочитать файл /etc/shadow?



Figure 11: Проверка

## 2.3 Исследование Sticky-бита

1. Выясните, установлен ли атрибут Sticky на директории /tmp, для чего выполните команду  
   ls -l / | grep tmp
2. Отименипользователяguestсоздайтефайлfile01.txtвдиректории/tmp со словом test: echo “test” > /tmp/file01.txt
3. 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



Figure 12: Проверка атрибута

1. От пользователя guest2 (не являющегося владельцем) попробуйте про- читать файл /tmp/file01.txt:  
   cat /tmp/file01.txt
2. От пользователя guest2 попробуйте дозаписать в файл /tmp/file01.txt слово test2 командой  
   echo “test2” > /tmp/file01.txt  
   Удалось ли вам выполнить операцию?
3. Проверьте содержимое файла командой  
   cat /tmp/file01.txt
4. 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?
5. Проверьте содержимое файла командой  
   cat /tmp/file01.txt
6. Отпользователяguest2попробуйтеудалитьфайл/tmp/file01.txtкомандой  
   rm /tmp/fileOl.txt

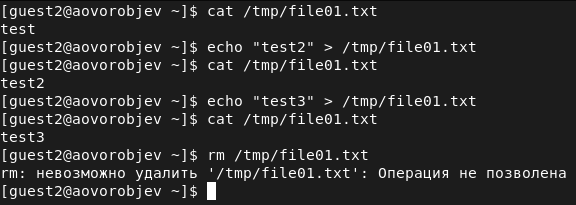
  
10. Повысьте свои права до суперпользователя следующей командой  
su -  
и выполните после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp: chmod -t /tmp  
11. Покиньте режим суперпользователя командой  
exit  
12. От пользователя guest2 проверьте, что атрибута t у директории /tmp нет: ls -l / | grep tmp

Figure 13: Повышение прав, проверка отсутствия атрибута

Figure 13: Повышение прав, проверка отсутствия атрибута

1. Повторите предыдущие шаги. Какие наблюдаются изменения?
2. Удалось ли вам удалить файл от имени пользователя, не являющегося его владельцем? Ваши наблюдения занесите в отчёт.

Figure 14: Повторение предыдущих шагов

Figure 14: Повторение предыдущих шагов

1. Повысьте свои права до суперпользователя и верните атрибут t на ди- ректорию /tmp:  
   su -  
   chmod +t /tmp  
   exit

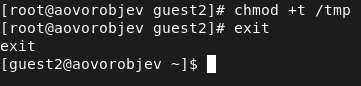


Figure 15: Возвращение атрибута

# 3 Выводы

Изучил механизмы изменения идентификаторов, примененив SetUID- и Sticky-биты. Получил практические навыкы работы в консоли с дополнительными атрибутами. Рассмотрел работы механизмов смены идентификаторов процесса пользователей, а также влияние бита Sticky на запись и удаление файлов.