Отчет по лабораторной работе 5

Дисциплина: Информационная безопасность

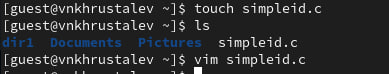
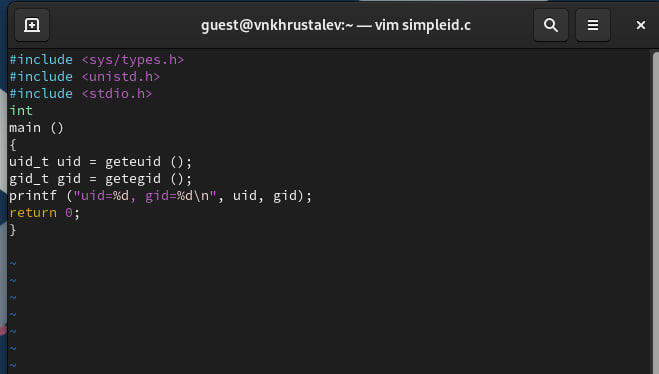
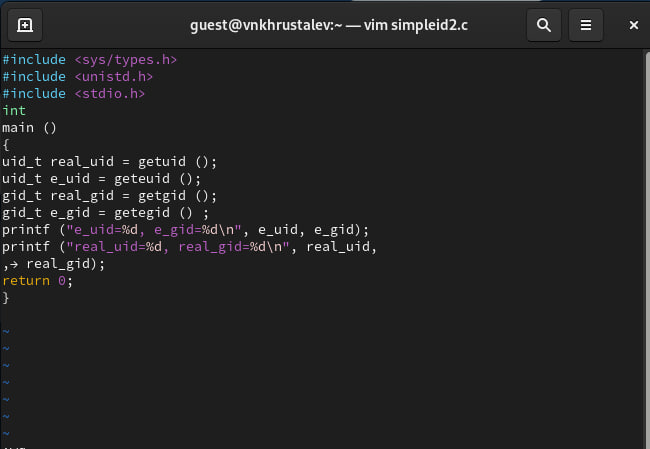
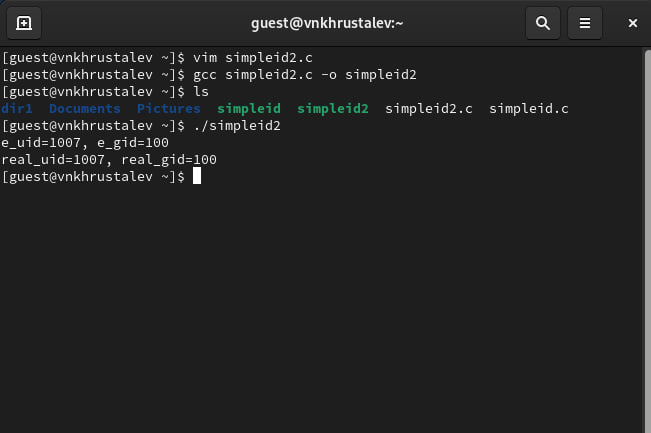
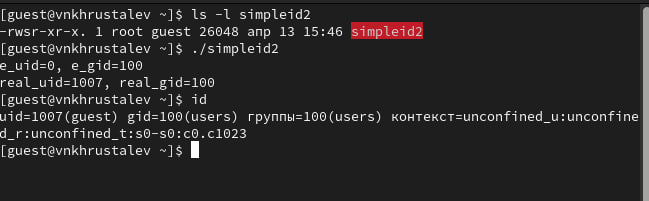
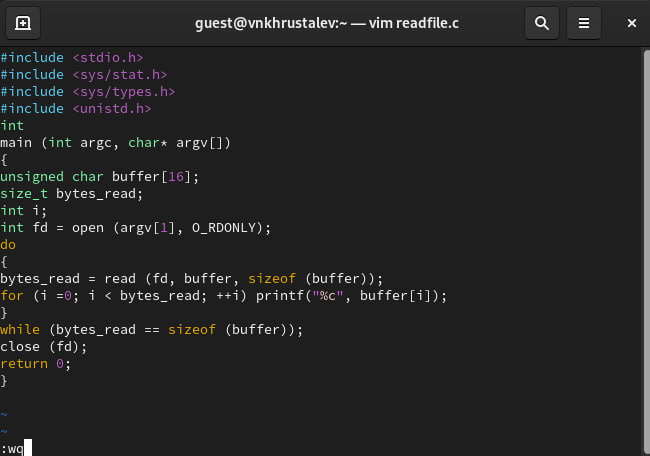
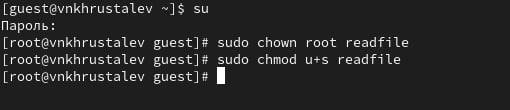
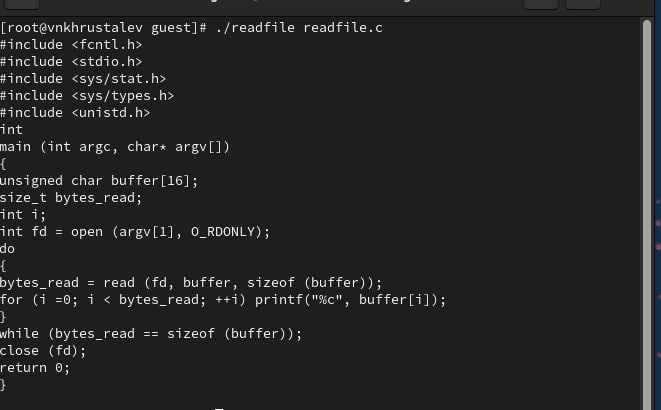
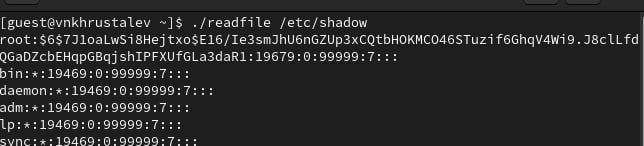
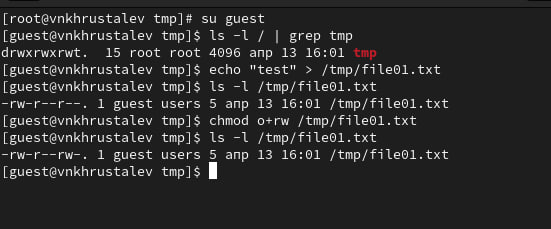
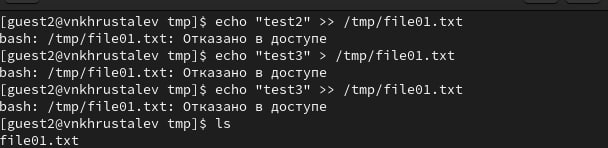
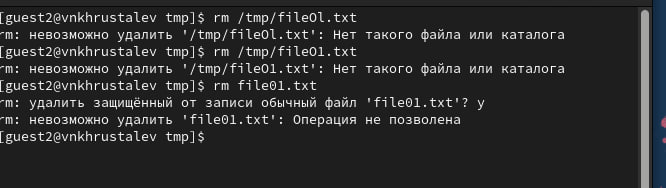
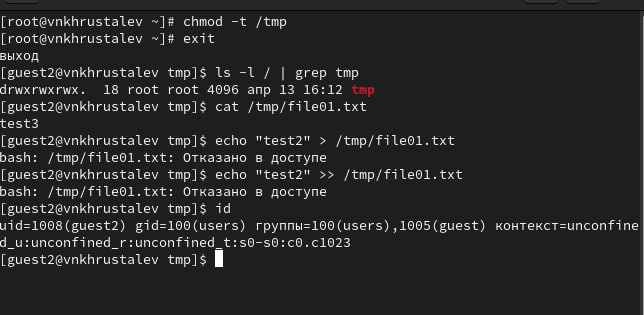
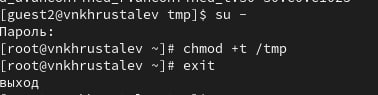
Хрусталев Влад Николаевич

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 Выполнение лабораторной работы

1. Создадим файл simpleid.c и введём в него программу  
2. Сохраним программу и сравним её работу с командой id. Как мы видим вывод верный 
3. Создадим файл simpleid2.c и введём в него программу, далее скомпилируем и запустим  
4. Изменим права доступа к файлу simpleid2, так и владельца на root. После чего запустим программу и убедимся, что вывод схож с командой id. Изменение прав и владельца simpleid2 
5. Создадим файл readfile.c и введём в него программу. Далее изменим владельца на root и изменим права доступа так, чтобы доступ к файлу был только у root.  
6. Попытаемся прочитать файл readfile.c от другого пользователя. У нас это не выйдет.(рис. **¿fig:010?**) Попытка чтения файла readfile.c от стороннего пользователя
7. Добавим бит к файлу readfile и попытаемся из него прочитать файлы, к которым у нас нет доступа. Как видим, всё выполняется, т.к. мы установили SetUID-бит.   
8. Приступаеп к следующей части работы. Создадим файл /tmp/file.01 от имени пользователя guest, изменим права, выдав доступ к чтению и записи группе OTHER. 
9. Попытаемся дописать этот файл, изменить полностью файл, удалить файл от пользователя guest2. У нас ничего этого не выйдет, т.к. guest2 в группе users, как и guest, а группе мы права не выдавали.  
10. Измененим(удалим) Sticky бит папки /tmp и повторно попытаемся выполнить предыдущик манипуляци. Опять же ничего не выйдет, по той же причине. После всех наших манипуляций, вернём Sticky бит для папки /tmp.  

# 3 Выводы

Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов, а также получение практических навыков работы в консоли с дополнительными атрибутами позволяют глубже понять принципы безопасности и управления доступом в Unix-подобных системах. Рассмотрение работы механизма смены идентификатора процессов пользователей и влияние бита Sticky на запись и удаление файлов демонстрирует важность этих аспектов для обеспечения безопасности и контроля доступа в многопользовательских средах.