Лабораторная работа №5

Основы информационной безопасности

Анастасия Андреевна Кондрашова

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. Вошли в систему от имени пользователя guest2.
2. Создали программу simpleid.c.
3. Скомплилируйте программу и убедитесь, что файл программы создан с помощью команды gcc simpleid.c -o simpleid.
4. Выполните программу simpleid.
5. Выполните системную программу id и сравнили полученный нами результат с данными предыдущего пункта. Данные иденичны.

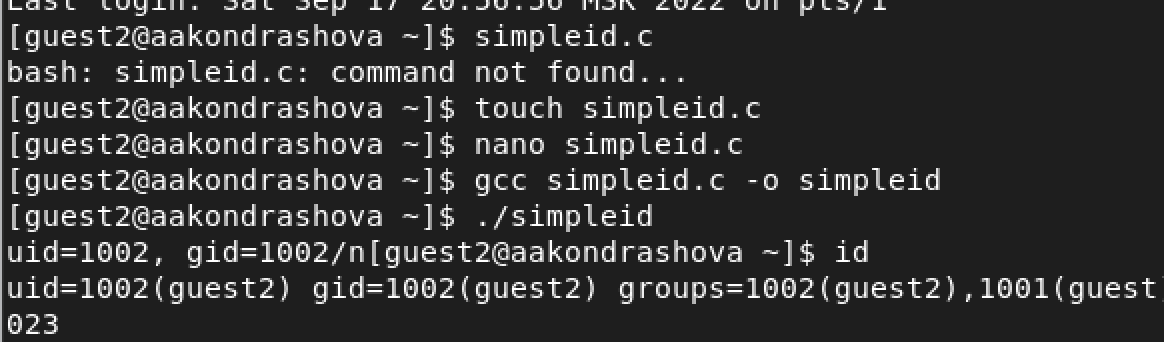


Рис. 1: Выполнение программы simpleid

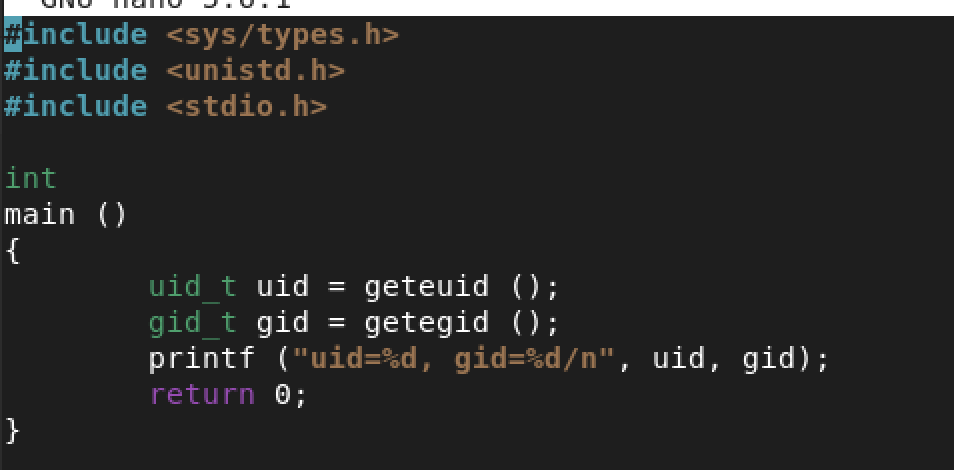


Рис. 2: Программа simpleid

1. Усложнили программу, добавив вывод действительных идентификаторов.Получившуюся программу назвали simpleid2.c.
2. Скомпилируйте и запустили simpleid2.c с помощью команды gcc simpleid2.c -o simpleid2.

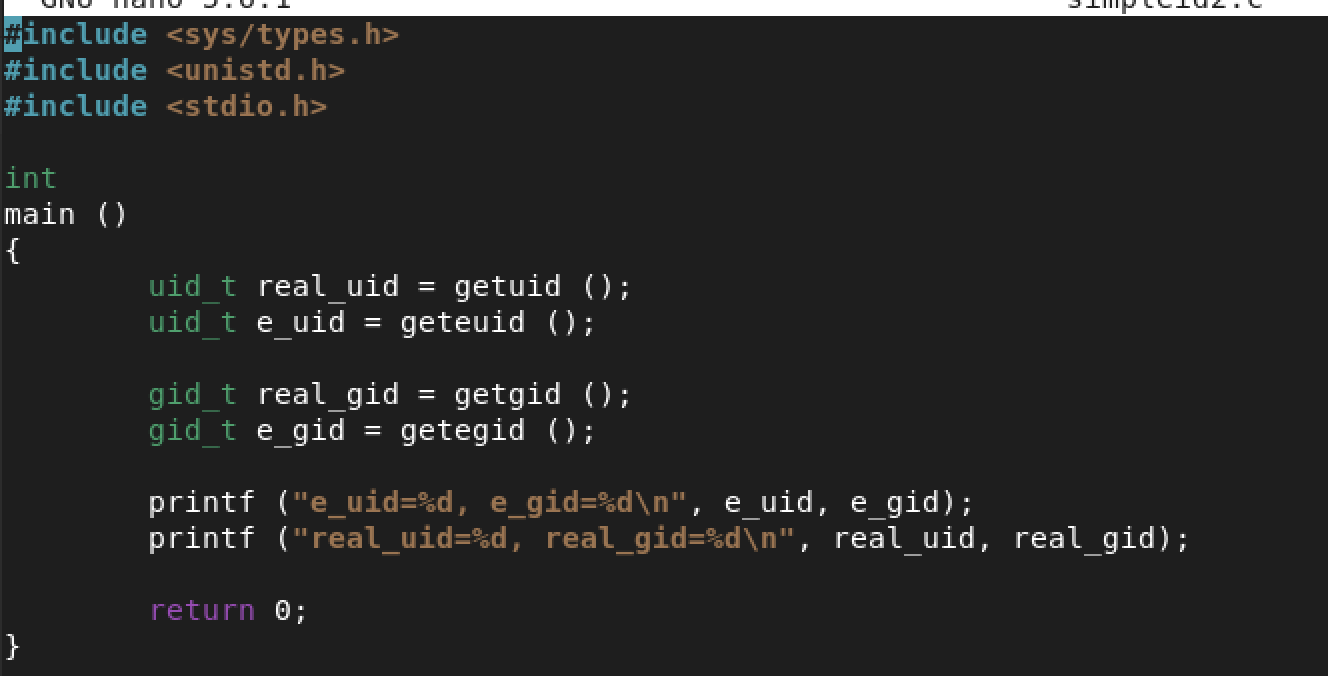


Рис. 3: Программа simpleid2

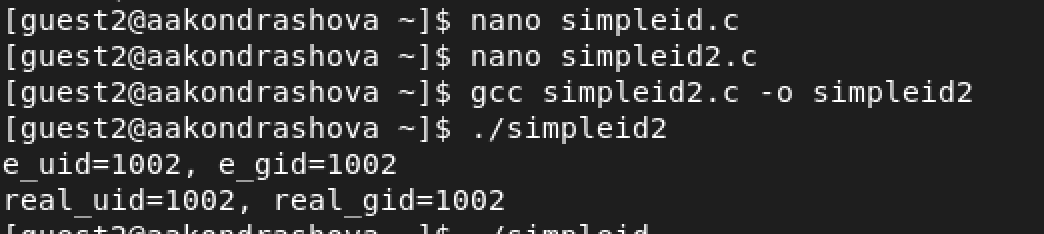


Рис. 4: Выполнение программы simpleid2

1. От имени суперпользователя выполнили команды (для этого исползовали повышение своих прав с помощью sudo): chown root:guest /home/guest/simpleid2 chmod u+s /home/guest/simpleid2
2. Выполнили проверку правильности установки новых атрибутов и смены владельца файла simpleid2.
3. Запустите simpleid2 и id.

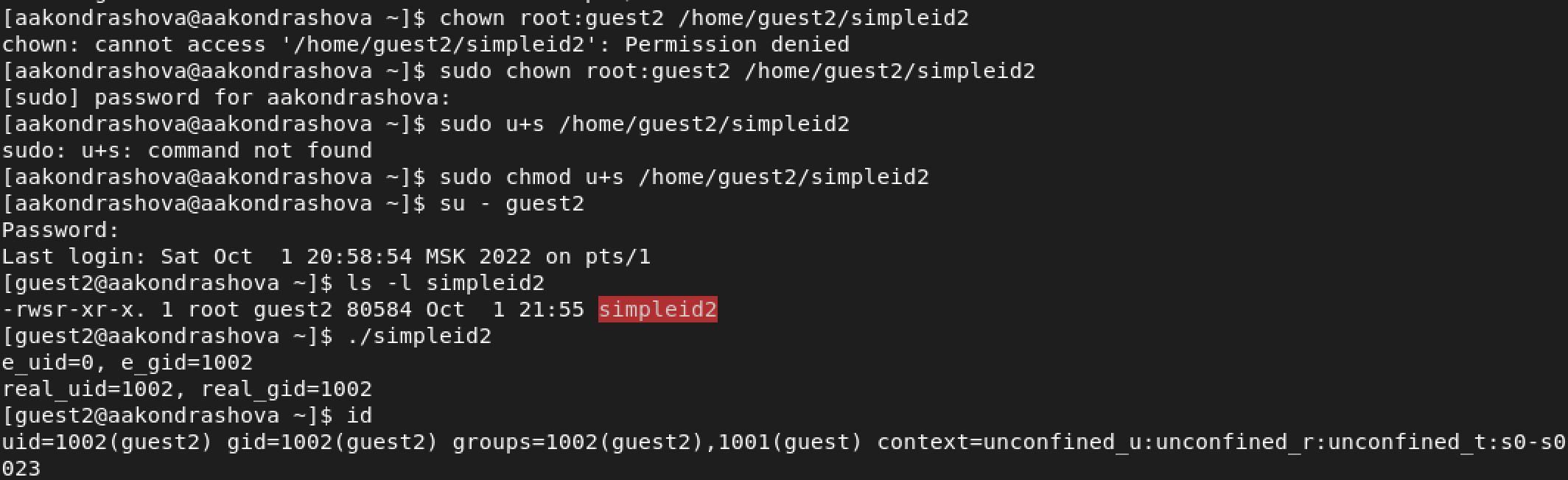


Рис. 5: Выполнение программы simpleid2

1. Создали программу readfile.c:
2. Откомпилировали её.

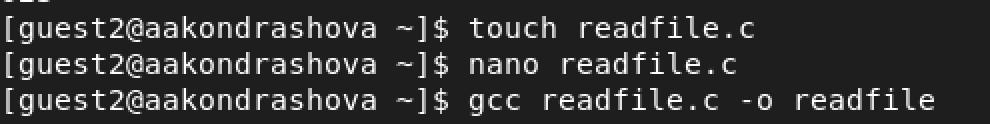


Рис. 6: Создание программы readfile.c



Рис. 7: Программа readfile.c

1. Сменили владельца у файла readfile.c и изменили права так, чтобы только суперпользователь (root) мог прочитать его, a guest2 не мог.

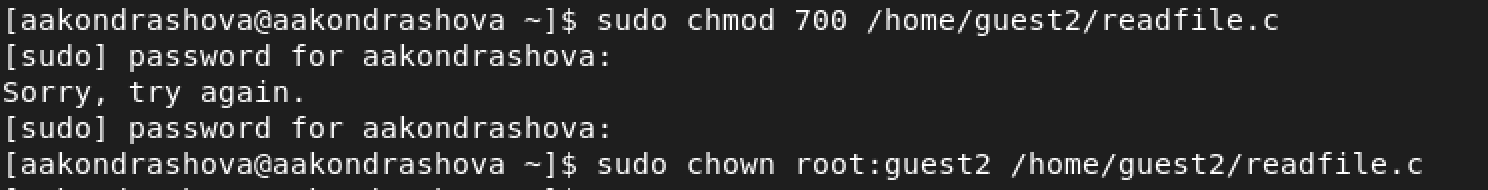


Рис. 8: Смена прав

1. Проверили, что пользователь guest2 не может прочитать файл readfile.c.

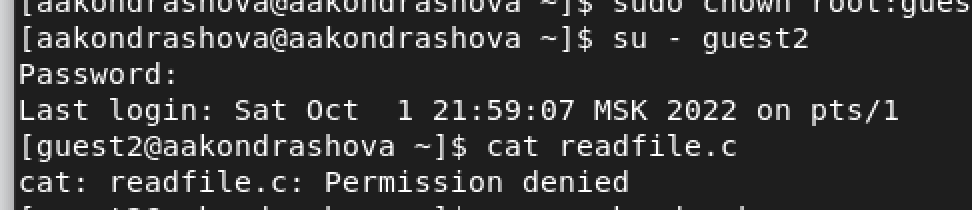


Рис. 9: Проверка невозможности чтения

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

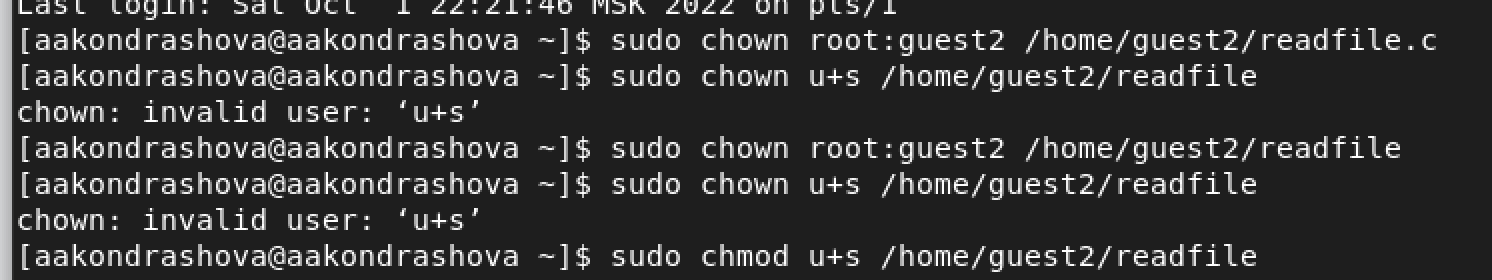


Рис. 10: Смена владельца и установка SetU’D-бит

1. Проверили, что программа readfile может прочитать файл readfile.c

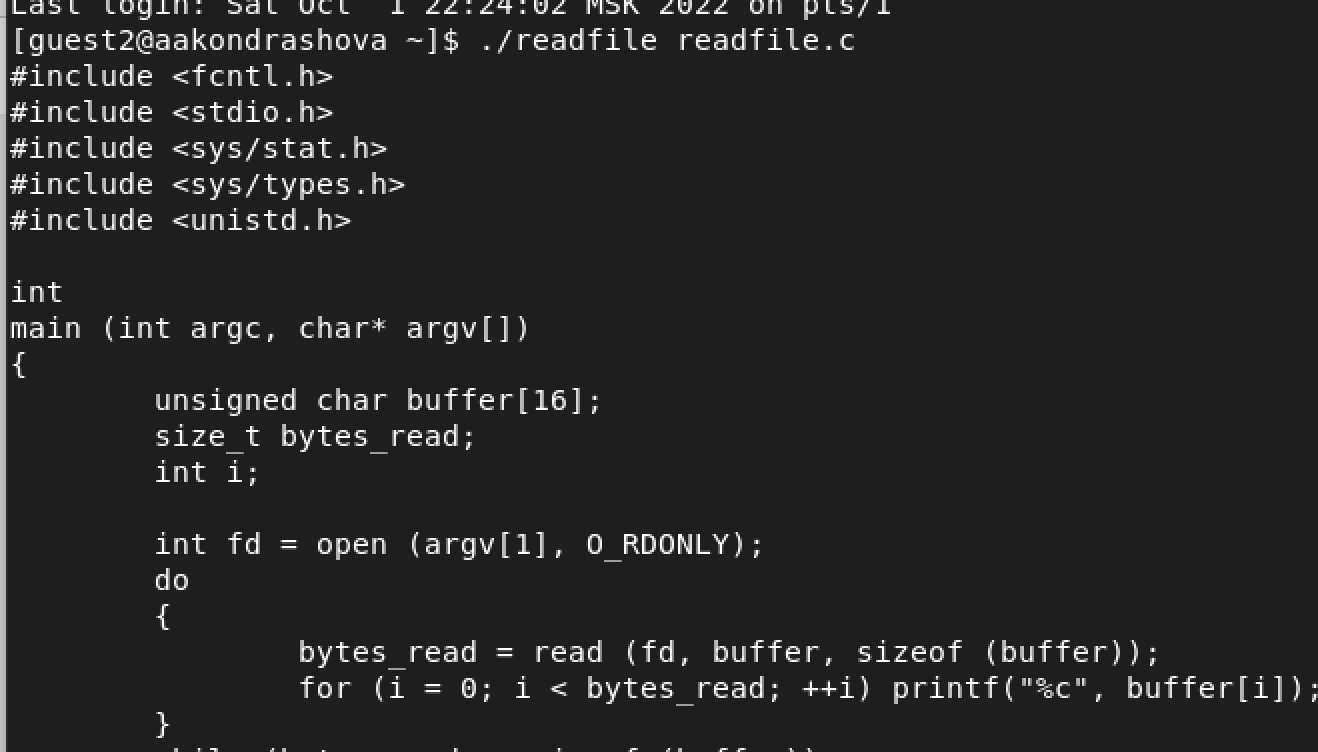


Рис. 11: Проверка возможности чтения файла readfile.c

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



Рис. 12: Проверка возможности чтения файла /etc/shadow

* Исследование Sticky-бита

1. Выяснили, установлен ли атрибут Sticky на директории /tmp, для чего выполнили команду ls -l / | grep tmp
2. От имени пользователя guest создали файл file01.txt в директории /tmp со словом test.
3. Просмотрели атрибуты у только что созданниого файла и разрешили чтение и запись для категории пользователей «все остальные».

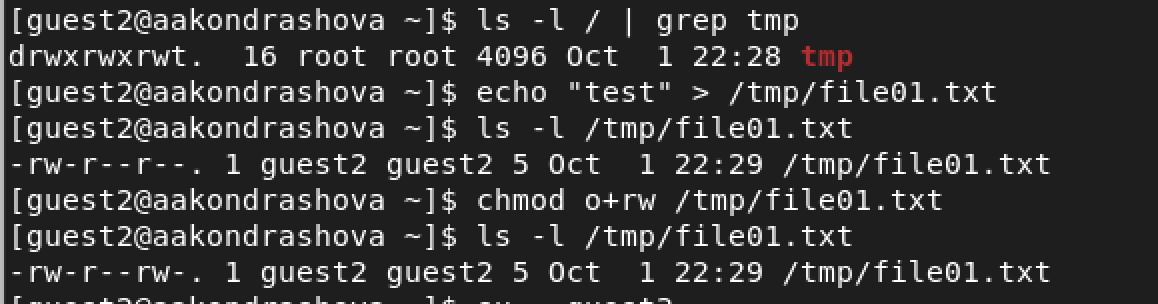


Рис. 13: Атрибуты на директории /tmp и файла file01.txt

1. От пользователя guest3 (не являющегося владельцем) попробовали прочитать файл /tmp/file01.txt. Нам это удалось.
2. От пользователя guest3 попробовали дозаписать в файл /tmp/file01.txt слово test2. Слово перезаписалось, а не дозаписалось.
3. От пользователя guest3 попробовали перезаписать в файл /tmp/file01.txt слово test3. Слово перезаписалось.
4. От пользователя guest3 попробовали удалить файл /tmp/file01.txt командой
5. Повысили свои права до суперпользователя и выполнили после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp.

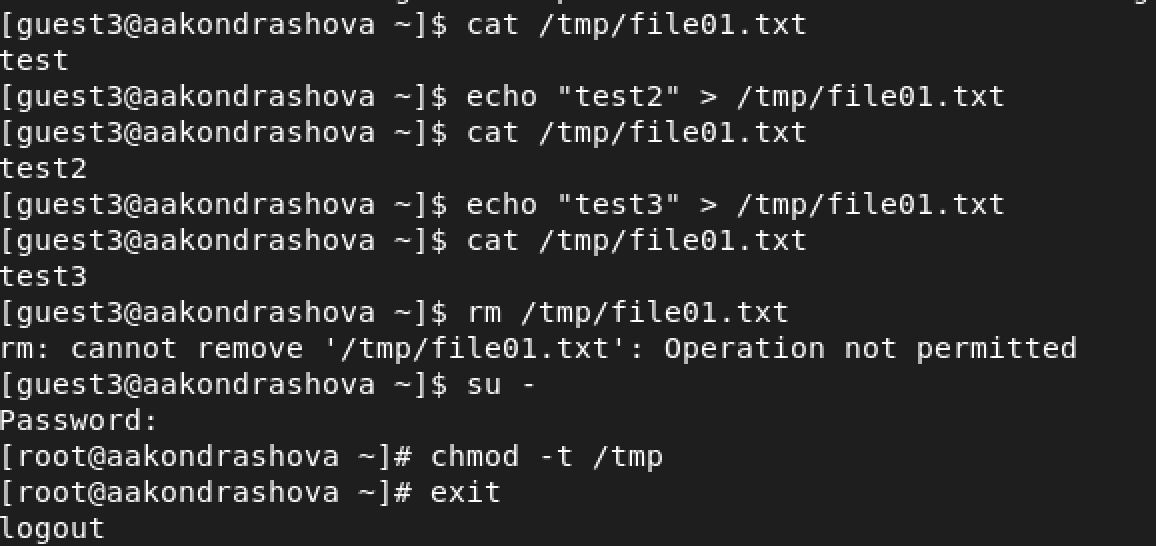


Рис. 14: Пункты 4-8

1. От пользователя guest3 проверили, что атрибута t у директории /tmp нет.
2. Повторили предыдущие шаги, удалось удалить файл.
3. Повысили свои права до суперпользователя и вернули атрибут t на директорию /tmp:

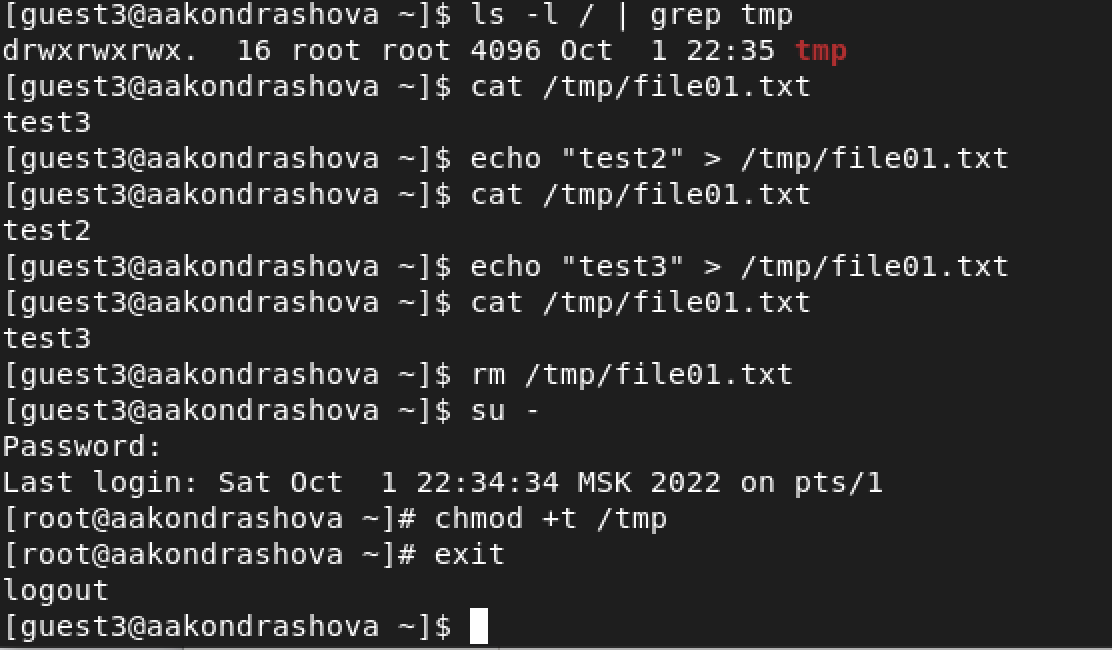


Рис. 15: Пункты 9-11

# 3 Выводы

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.