

Презентация по лабораторной работе №5

Информационная безопасность

Акандзо Жордани Лади Гаэл.

03 Октября 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Акондзо Жордани Лади Гаэл.
- студент 4-го курса группы НКНбд-01-21
- 1032215649
- Российский университет дружбы народов
- GitHub

Вводная часть

- Обеспечение безопасности
- Предотвращение пересечений между пользовательскими аккаунтами
- Совместный доступ к файлам

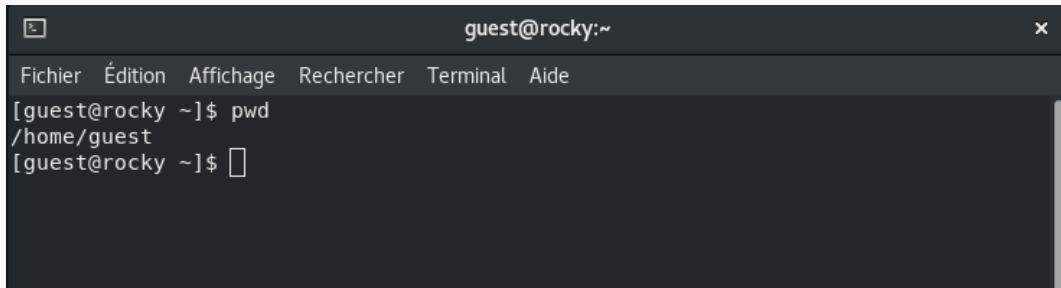
- Закрепление практических навыков работы в консоли с атрибутами файлов
- Закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux
- Изучение механизмов изменения идентификаторов, применение SetUID- и SetGID-битов.
- Изучение действия Sticky-бита на запись и удаление файлов в общей директории.

- Веб-сервис **GitHub** для работы с репозиториями
- Программа для виртуализации ОС **VirtualBox**
- Процессор **pandoc** для входного формата Markdown
- Результирующие форматы
 - pdf
 - docx
- Автоматизация процесса создания: **Makefile**

Выполнение лабораторной работы

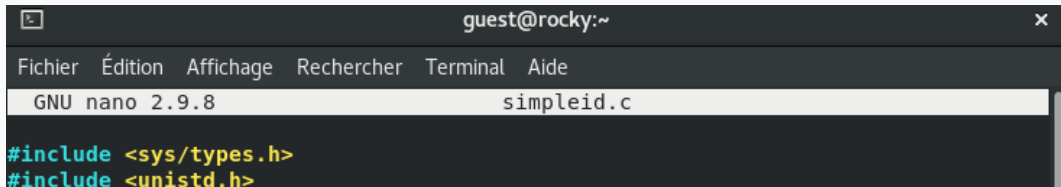
Часть 1: Изучение SetUID- и SetGID-битов

Вход в систему.



```
guest@rocky:~  
Fichier  Édition  Affichage  Rechercher  Terminal  Aide  
[guest@rocky ~]$ pwd  
/home/guest  
[guest@rocky ~]$
```

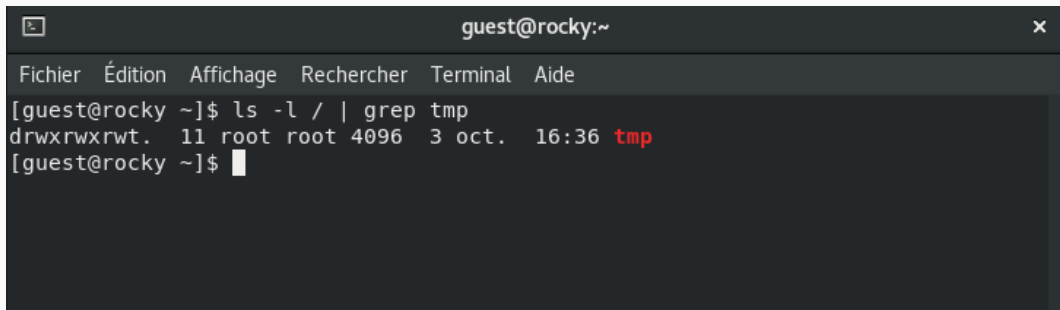
Создание программы `simpleid.c` и её компиляция:



```
guest@rocky:~  
Fichier  Édition  Affichage  Rechercher  Terminal  Aide  
GNU nano 2.9.8 simpleid.c  
  
#include <sys/types.h>  
#include <unistd.h>
```

Часть 2: Исследование Sticky-бита

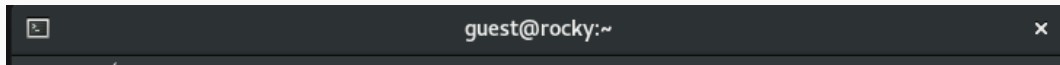
Проверка наличия Sticky-бита на директории /tmp:



```
guest@rocky:~  
Fichier  Édition  Affichage  Rechercher  Terminal  Aide  
[guest@rocky ~]$ ls -l / | grep tmp  
drwxrwxrwt. 11 root root 4096 3 oct. 16:36 tmp  
[guest@rocky ~]$
```

- Sticky-бит (t) указывает, что только владелец файла или root может удалить его, даже если у других пользователей есть права на запись.

Создание файла в /tmp и изменение прав доступа:**



```
guest@rocky:~  
touch /tmp/test  
touch: /tmp/test: Permission denied  
[guest@rocky ~]$
```

Выводы

В ходе этой лабораторной работы было продемонстрировано, как использование **SetUID**, **SetGID**, и **Sticky-бита** позволяет управлять доступом и правами пользователей в системе Linux. **SetUID** и **SetGID** позволяют временно выполнять программы с правами владельца файла или его группы, что полезно для выполнения привилегированных задач. **Sticky-бит** защищает файлы в общих директориях, таких как **/tmp**, от удаления пользователями, не являющимися владельцами, что предотвращает потенциальные конфликты и нарушения безопасности.