**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

***Изображение выглядит как черный, темнота

Автоматически созданное описание***

**Факультет Программной Инженерии и Компьютерной Техники**

**Дисциплина:**

**«*Информационная безопасность*»**

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №2   
«Политики безопасности Linux»**

*Вариант 9*

**Выполнил:**

Студент гр. P34151 *Соловьев Артемий Александрович*

**Преподаватель:**

*Маркина Татьяна Анатольевна*

Санкт-Петербург

2024г.

# Задание:

## Основная часть:

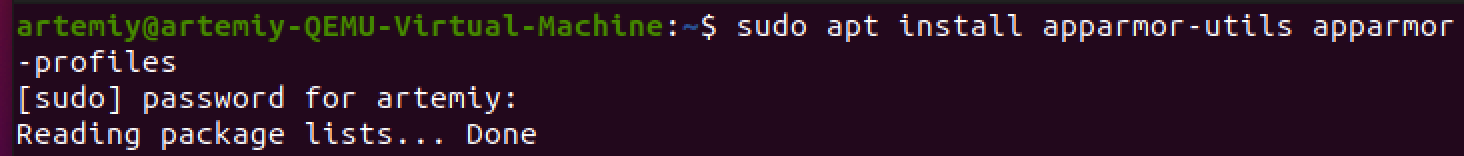
1. Установите утилиту AppArmor  
   sudo apt install apparmor-utils apparmor-profiles  
   Напишите bash-скрипт который будет создавать файл в директории log , записывать в него что-то, читать из него и затем удалять.
2. Создайте директорию log. Выдайте файлу права на исполнение. Запустите файл, покажите вывод ./file
3. Создайте профиль безопасности для данной программы  
   sudo aa-genprof ./file  
   Покажите результат выполнения программы
4. Запустите утилиту aa-logprof и настройте разрешения так, чтобы при выполнении программы не было ошибок. Запустите файл еще раз. Покажите, что теперь ошибок нет.
5. В программе, измените местоположение создаваемого файла с /log на /logs.
6. Создайте директорию logs. Запустите программу, покажите, что AppArmor блокирует попытку получить доступ к пути за пределами границ.
7. Верните изначальное значение /log. Покажите, что программа работает корректно.
8. Отключите и удалите профиль безопасности из системы.

## Дополнительная часть:

1. Опишите отличия SELinux vs AppArmor?
2. Опишите режимы профилей Enforce и Complain? Их различия для чего нужны?

# Выполнение

## Установка утилиты AppArmor



## Bash-скрипт для создания, записи, чтения и удаления файла в директории log

Команды для создания

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Содержимое файла file.sh

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

## Создание директории log, выдача прав на исполнения для bash-скрипта и его исполнение

Создадим директорию /log.

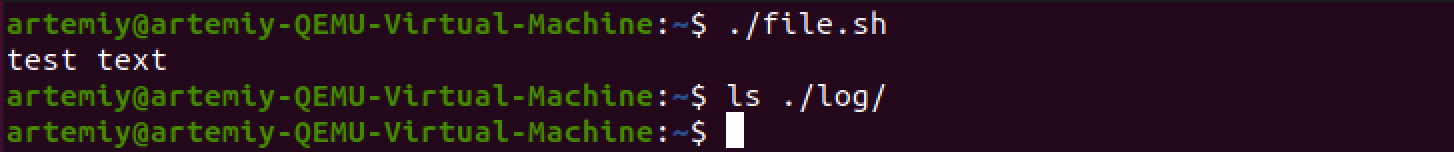
Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Выдадим права на исполнения файла file.shИзображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Запустим скрипт и проверим вывод



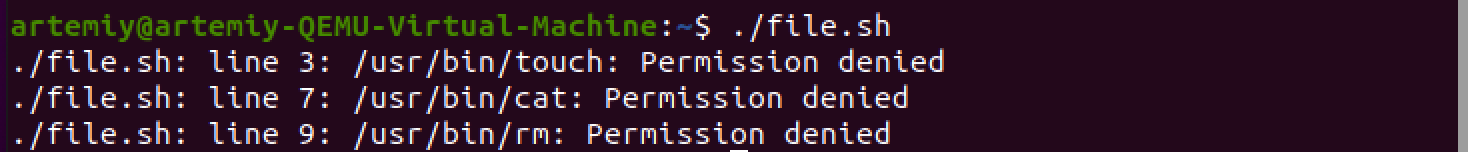
## Создание профиля безопасности для file.sh

При выполнении команды *sudo aa-genprof ./file.sh* мы видим такое окно с логами операций.

Изображение выглядит как текст, снимок экрана, программное обеспечение

Автоматически созданное описание

Пробуем запустить файл file.sh



## Настройка разрешений через aa-logprof

## Изображение выглядит как текст, снимок экрана, Шрифт Автоматически созданное описание

На скриншоте выше мы выдали разрешения для файла

Проверка, что разрешения выданы:

Изображение выглядит как текст, снимок экрана, Шрифт, Графика

Автоматически созданное описание

## Изменение метаположения создаваемого файла на /logs

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

## Создание директории logs и запуск программы

## Изображение выглядит как текст, снимок экрана, Шрифт Автоматически созданное описание

Ожидаемо, доступ заблокирован.

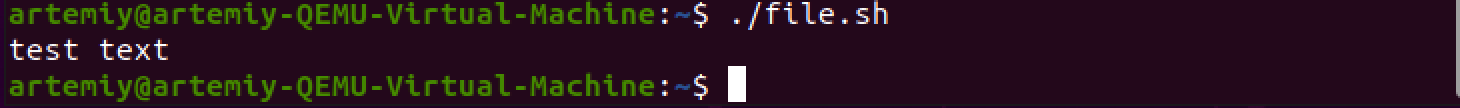
## Возвращаем скрипт в начальный вид

nano file.txt

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

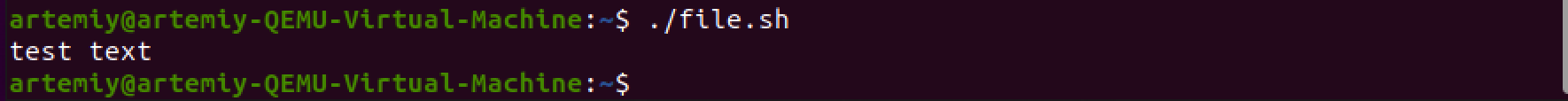
Проверяем работоспособность скрипта



## Отключение и удаления профиля безопасности

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание



# Дополнительная часть

## Отличия SELinux vs AppArmor

|  |  |  |
| --- | --- | --- |
| Критерий | SELinux | AppArmor |
| Контроль доступа | Использует профили безопасности на основе меток файлов | Использует профили безопасности, основанные на путях |
| Сложность в освоении | Сложная настройка и администрирование | Простая настройка и администрирование |
| Требуется сложная конфигурация | Да | Нет |
| Влияние на производительность | Из-за сложных проверок может несильно замедлить систему | Небольшое влияние во время запуска |

## Режимы профилей Enforce и Complain. Сравнение и для чего нужны

Режим профиля определяет обработку правил во время выполнения, если произойдет соответствующее событие.

### Описание профилей

1. Enforce:   
   Система применяет правила, сообщает о нарушении и записывает его в системный журнал.   
   Мы используем этот режим, чтобы запретить программе выполнять определенные вызовы.
2. Complain: Система не применяет правила, но записывает нарушения в журнал.

### Для чего нужны

1. Enforce:   
   Используется, чтобы запретить программе выполнять определенные вызовы
2. Complain:  
   Этот режим полезен, если мы хотим обнаружить вызовы, которые делает программа

# Вывод

В ходе выполнения лабораторной работы были созданы (а в последствии удалены) политики безопасности по средствам утилиты AppArmor, а также была проведена сравнительная характеристика AppArmor и SELinux.