Министерство образования и науки РФ

Федеральное государственное автономное

образовательное учреждение высшего образования

«Национальный исследовательский университет ИТМО»

**факультет программной инженерии и компьютерной техники**

**ЛАБОРАТОРНАЯ РАБОТА**

**“**Политики безопасности Linux”

по дисциплине

‘Информационная безопасность’

***Выполнили:***

Студент группы P34312

Соболев Иван Александрович

***Преподаватель:***

Маркина Татьяна Анатольевна



Санкт-Петербург, 2024

Оглавление

[Установка утилиты AppArmor и создание скрипта bash 3](#_Toc178417091)

[Запуск bash-скрипта 3](#_Toc178417092)

[Создание профиля безопасности 4](#_Toc178417093)

[Настройка разрешений утилитой aa-logprof 5](#_Toc178417094)

[Изменение местоположения создаваемого файла 6](#_Toc178417095)

[Запуск appArmor с измененным местоположением 6](#_Toc178417096)

[Изменение местоположения на изначальное 6](#_Toc178417097)

[Отключение и удаление профиля безопасности 7](#_Toc178417098)

[Дополнительная часть 7](#_Toc178417099)

# Установка утилиты AppArmor и создание скрипта bash



Рисунок 1 - Установка утилиты

Содержимое скрипта:  
A screenshot of a computer

Description automatically generated

Рисунок 2 - Содержимое скрипта

# Запуск bash-скрипта

Выдача прав на исполнение:



Рисунок 3 - Права

Запуск:

A close up of a sign

Description automatically generated

Рисунок 4 - Тестирование

# Создание профиля безопасности

A screenshot of a computer program

Description automatically generated

Рисунок 5 - Профиль безопасности

Вывод результата выполнения программы:  
A computer code with white text

Description automatically generated

Рисунок 6 - Вывод программы

# Настройка разрешений утилитой aa-logprof

Часть с выдачей разрешений на чтение и запись файлов в директории test.log

A screenshot of a computer program

Description automatically generated

Рисунок 7 - Разрешения

Вывод работы скрипта в процессе работы над политикой безопасности

A screenshot of a computer program

Description automatically generated

Рисунок 8 - Работа скрипта

# Изменение местоположения создаваемого файла

A screenshot of a computer program

Description automatically generated

Рисунок 9 - Изменение местоположения

# Запуск appArmor с измененным местоположением

A screenshot of a computer program

Description automatically generated

Рисунок 10 - Запуск скрипта

# Изменение местоположения на изначальное

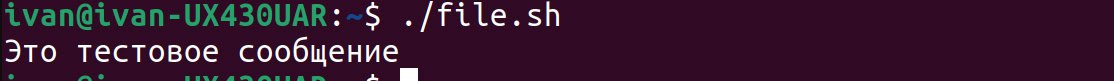


Рисунок 11 - Изменение местоположения

# Отключение и удаление профиля безопасности

Проверка наличия профиля:  
A screenshot of a computer

Description automatically generated

Рисунок 12 - Проверка наличия профиля

Отключение профиля:

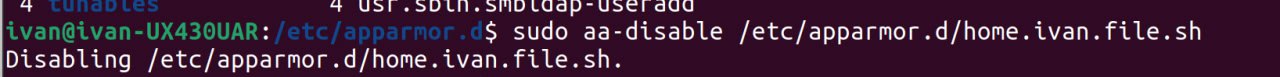


Рисунок 13 - Удаление профиля безопасности

Удаление профиля:  
A computer screen with white text

Description automatically generated

Рисунок 14- Удаление профиля безопасности

# Дополнительная часть

1. Отличия SELinux vs AppArmor

SELinux (Security-Enhanced Linux) и AppArmor — это две разные системы управления доступом на уровне ядра в Linux.

SELinux основан на реализации мандатного управления доступом (MANDATORY ACCESS CONTROL, MAC). Каждому процессу и объекту в системе назначается контекст безопасности, и доступ основывается на этих контекстах.

AppArmor работает на уровне приложений и позволяет задавать конкретные правила для каждого приложения, контролируя доступ только к тем ресурсам, которые необходимы для работы.

2. Режимы профилей Enforce и Complain

Enforce (Принуждение):

В этом режиме профили соблюдаются строго. Если приложение пытается выполнить операцию, которая не разрешена, то доступ отклоняется, и действие не выполняется.

Complain (Жалоба):

В этом режиме профили также применяются, но если приложение нарушает правила, то действие не блокируется. Вместо этого в журнале записывается информация о нарушении. Это позволяет администраторам наблюдать за потенциальными проблемами, не ограничивая функциональность программ.