**ЛАБОРАТОРНАЯ РАБОТА №2**

**“**Политики безопасности Linux”

по дисциплине

‘Информационная безопасность’

***Выполнил:***

Соболев Иван Александрович

**Группа:** P34312

***Преподаватель:***

Маркина Татьяна Анатольевна

Санкт-Петербург, 2024

# Цель работы:

Ознакомиться с процессом работы с утилитой AppArmor. Изучить отличия утилиты AppArmor от SELinux.

# Программные и аппаратные средства

Для выполнения лабораторной работы был использован компьютер со следующими характеристиками:

* Процессор: Intel i5 8250U
* Видеокарта: Intel UHD Graphics 620
* Объем оперативной памяти: 8GB
* Использована операционная система Ubuntu 22.04.3 LTS.

# Основная часть

# Установка утилиты AppArmor и создание скрипта bash



Содержимое скрипта:  
A screenshot of a computer

Description automatically generated

# Запуск bash-скрипта

Выдача прав на исполнение:



Запуск:

A close up of a sign

Description automatically generated

# Создание профиля безопасности

A screenshot of a computer program

Description automatically generated

Вывод результата выполнения программы:  
A computer code with white text

Description automatically generated

# 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

Вывод работы скрипта в процессе работы над политикой безопасности:A screenshot of a computer program

Description automatically generated

# Изменение местоположения создаваемого файла

A screenshot of a computer program

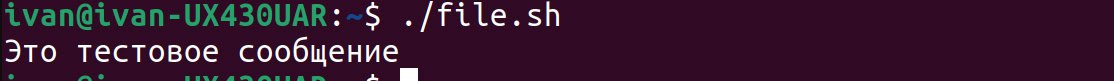
Description automatically generated

# Запуск appArmor с измененным местоположением

A screenshot of a computer program

Description automatically generated

# Запуск скрипта с начальным местоположением

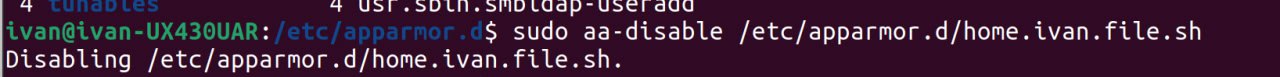


# Отключение и удаление профиля безопасности

Проверка наличия профиля:  
A screenshot of a computer

Description automatically generated

Отключение профиля:

  
Удаление профиля:  
A computer screen with white text

Description automatically generated

# Дополнительная часть

1. Отличия SELinux vs AppArmor

SELinux и AppArmor — это две разные системы управления доступом в Linux.

Ключевое отличие AppArmor от SELinux заключается в том, что AppArmor привязывает политику к пути, а SELinux опирается на дескриптор файла. Если заблокировать исполнение файла и потом переместить его, то AppArmor позволит файлу запуститься, а SELinux ― нет. Если же файл перезапишут по исходному пути, то уже AppArmor заблокирует его, а SELinux разрешит выполнение.

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.

**Выводы:**   
Я изучил работу с политиками безопасности с помощью утилиты AppArmor. Также познакомился с SELinux и сформулировал отличия SELinux от AppArmor.