Отчёт по лабораторной работе №6

Мандатное разграничение прав в Linux

Саргсян Арам Грачьяевич

Содержание

# 1 Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux на практике совместно с веб-сервером Apache.

# 2 Теоретическое введение

## 2.1 SELinux

SELinux (Security-Enhanced Linux) - это набор обязательных контролов доступа (MAC), разработанных для улучшения безопасности операционных систем на базе ядра Linux. SELinux предоставляет дополнительные уровни безопасности, которые работают в дополнение к стандартным системам управления доступом, таким как управление правами доступа (DAC - discretionary access control).

Основные особенности SELinux:

1. Принудительный контроль доступа (MAC): SELinux предоставляет механизм, который определяет, к каким ресурсам и операциям пользователи и процессы имеют доступ. В отличие от системы управления доступом на основе прав доступа (DAC), где пользователи могут управлять своими файлами и процессами, SELinux предписывает жесткие правила доступа на уровне ядра.
2. Политики безопасности: SELinux использует политики безопасности, определяющие, какие действия разрешены для различных объектов и субъектов (пользователей и процессов). Политики могут быть настроены и настраиваться в зависимости от потребностей системы.
3. Роли и контексты: В SELinux каждому процессу и ресурсу назначаются контексты безопасности, которые определяют его роль и права доступа. Это помогает изолировать процессы и уменьшает риск распространения атак.
4. Проверка соблюдения политик: SELinux постоянно проверяет соблюдение политик безопасности и блокирует доступ, который нарушает эти политики. Это повышает уровень безопасности, предотвращая многие типичные уязвимости.
5. Гибкость настройки: SELinux позволяет администраторам настраивать политики безопасности под конкретные потребности системы, создавать собственные политики и определять, какие действия разрешены и какие запрещены.
6. Аудит и журналирование: SELinux обеспечивает детализированный аудит и журналирование событий, что позволяет администраторам исследовать инциденты безопасности и выявлять аномалии.

SELinux является мощным инструментом для улучшения безопасности Linux-систем, но его конфигурация может быть сложной и требовать понимания принципов безопасности. В большинстве дистрибутивов Linux SELinux предоставляется как опция, и его активация и настройка зависят от конкретных потребностей системы и уровня безопасности [1].

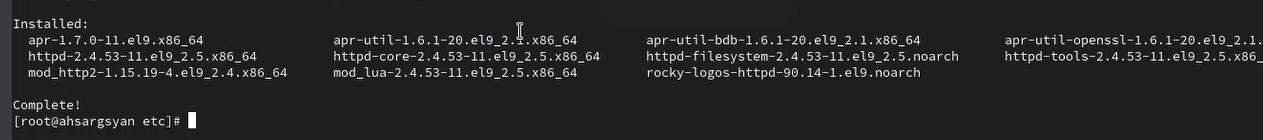
## 2.2 Apache

Apache, также известный как Apache HTTP Server, - это свободный и открытый веб-сервер, разработанный Apache Software Foundation. Этот веб-сервер является одним из самых популярных и широко используемых в мире, и он играет ключевую роль в инфраструктуре множества веб-сайтов и приложений. Вот некоторые основные характеристики и функции Apache:

1. Сервер статических и динамических контентов: Apache способен обслуживать как статические веб-страницы, так и динамические, включая страницы, создаваемые с использованием языков программирования, таких как PHP, Python, и Ruby.
2. Модульная архитектура: Apache использует модульную архитектуру, которая позволяет добавлять и настраивать разнообразные функциональные возможности, такие как аутентификация, шифрование, сжатие и многое другое с помощью модулей.
3. Открытое ПО: Apache является свободным программным обеспечением с открытым исходным кодом, что означает, что его исходный код доступен для общественности для просмотра, изменения и распространения в соответствии с лицензией Apache.
4. Поддержка множества протоколов: Apache поддерживает множество сетевых протоколов, включая HTTP, HTTPS (через модуль SSL/TLS), и другие протоколы, что делает его универсальным инструментом для обслуживания разнообразных веб-приложений.
5. Виртуальные хосты: Apache поддерживает конфигурацию виртуальных хостов, что позволяет хостить несколько сайтов на одном сервере с разными доменными именами и настройками.
6. Безопасность: Apache предоставляет множество механизмов для обеспечения безопасности, включая возможность настройки правил доступа, аутентификации и шифрования данных.
7. Логирование: Apache генерирует лог-файлы, которые записывают информацию о запросах, ошибках и активности сервера, что полезно для мониторинга и анализа.
8. Apache используется множеством организаций и индивидуальных разработчиков для развертывания веб-сайтов и веб-приложений на серверах Linux и других операционных системах. Благодаря обширному сообществу и богатой документации, Apache остается одним из наиболее надежных и гибких веб-серверов [2].

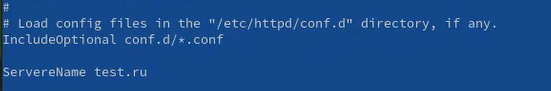
# 3 Выполнение лабораторной работы

1. Установил веб-сервис apache для дальнейшей работы (рис. ??).



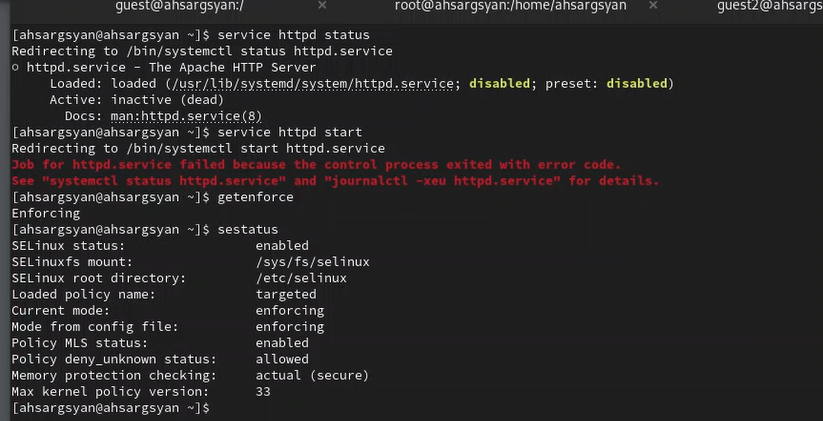
Запуск сервера

1. В конфигурационном файле /etc/httpd/httpd.conf задал параметр ServerName (рис. ??).

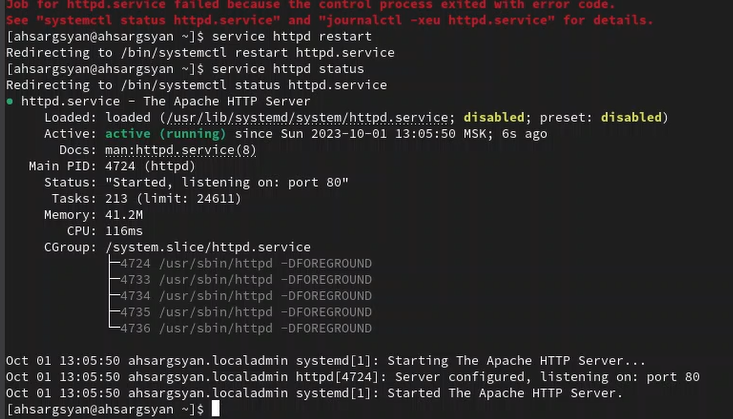


Параметр ServerName

1. Вошел в систему с полученными учётными данными и убедился, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus. Запустил веб-сервис (рис. ??, ??).

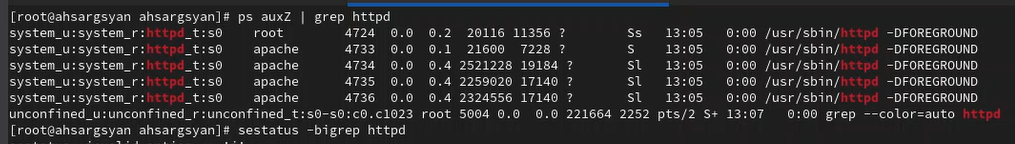


Команды getenforce и sestatus



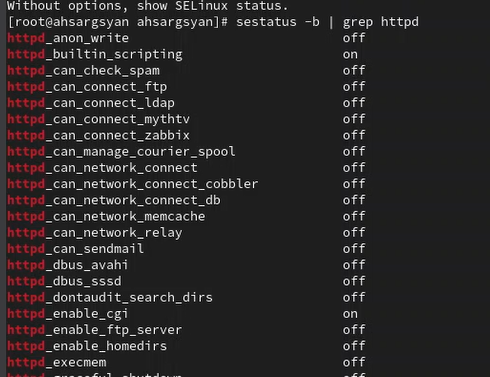
Запуск apache

1. Определил его контест безопасности (рис. ??)



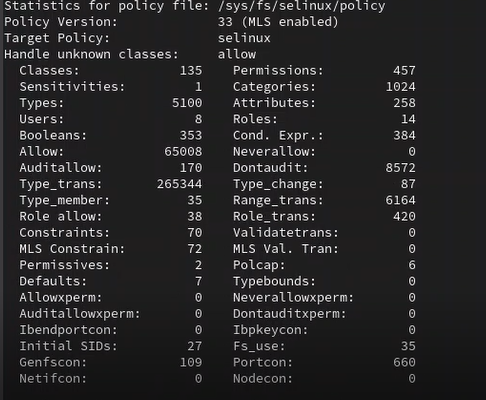
Контест безопасности

1. Посмотрел текущее состояние переключателей SELinux (рис. ??)



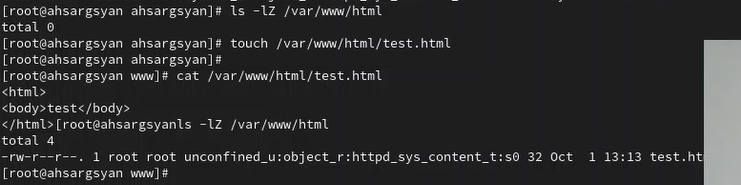
Cостояние переключателей SELinux

1. Посмотрел статистику по политике с помощью команды seinfo (рис. ??)

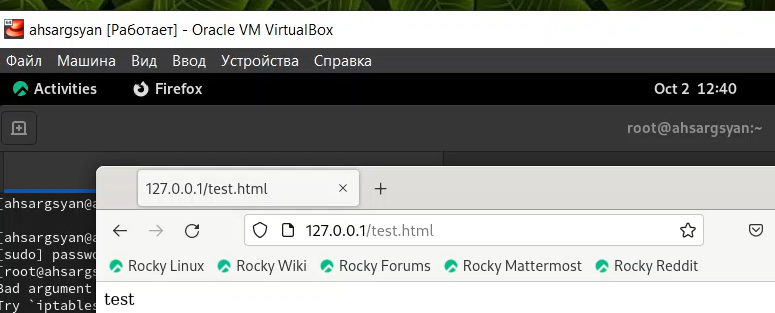


Статистика по политике

1. Определил тип файлов и поддиректорий, находящихся в директории /var/www, определил тип файлов, находящихся в директории /var/www/html, определил круг пользователей, которым разрешено создание файлов в директории /var/www/html. Создал от имени суперпользователя html-файл test.html. Проверил контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html. Обратился к файлу через веб-сервер (рис. ??, ??)

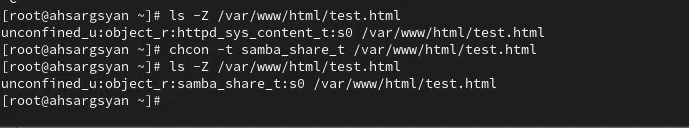


Типы файлов и поддиректории

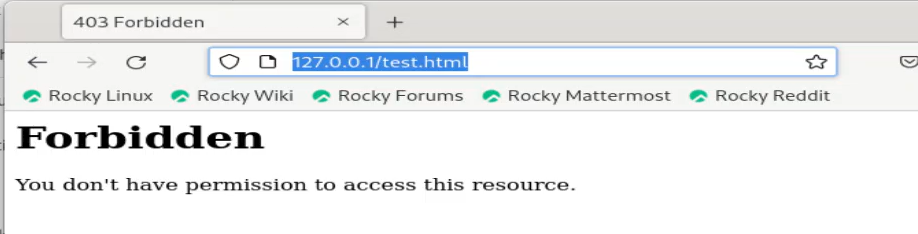


Запуск в браузере

1. Изменил контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на любой другой, к которому процесс httpd не должен иметь доступа, попробовал ещё раз получить доступ к файлу через веб-сервер (рис. ??, ??).



Изменение контеста безопасности



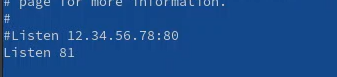
Запуск в браузере с ошибкой

1. Просмотрел log-файлы веб-сервера Apache (рис. ??)

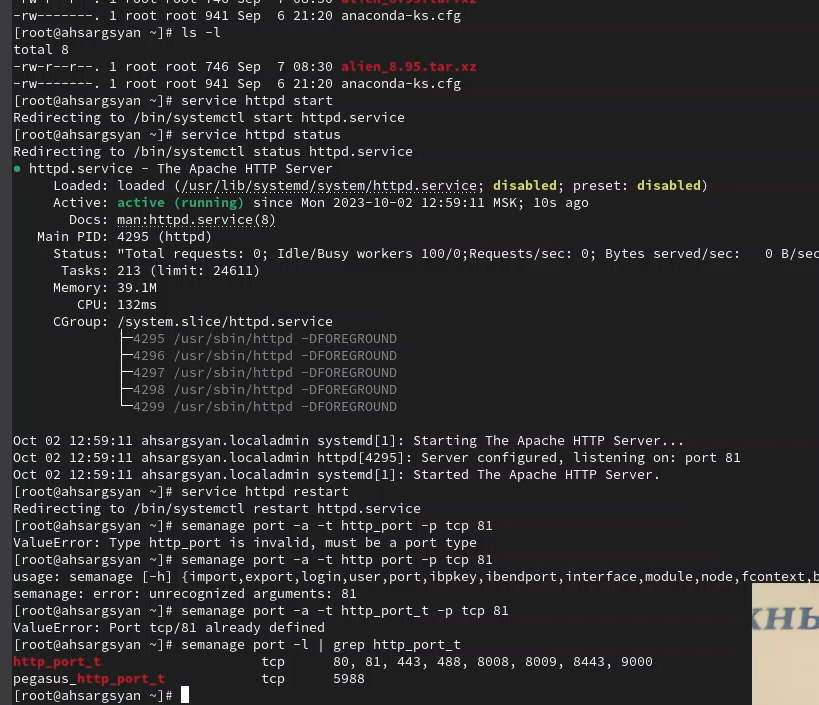


Лог файлы

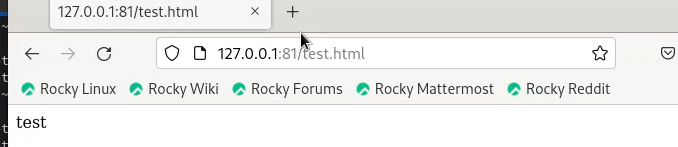
1. Открыл файл через 81 порт (рис. ??, ??, ??)



Изменение порта



Настройки



Открытие файла

# 4 Выводы

Я развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux, а также проверил работу SELinux на практике совместно с веб-сервером Apache.

# Список литературы

1. Xu W., Shehab M., Ahn G.-J. [Visualization based policy analysis](https://doi.org/10.1145/1377836.1377863) // Proceedings of the 13th ACM symposium on Access control models and technologies. ACM, 2008.

2. Laurie B. Apache. 3rd ed / под ред. Laurie P. Sebastopol: O’Reilly Media, Inc, 2007. 608 с.