Лабораторная работа №6.

Мандатное разграничение прав в Linux.

Яссин.М.А

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

SELinux (англ. Security-Enhanced Linux — Linux с улучшенной безопасностью) — реализация системы принудительного контроля доступа, которая может работать параллельно с классической избирательной системой контроля доступа. [2]

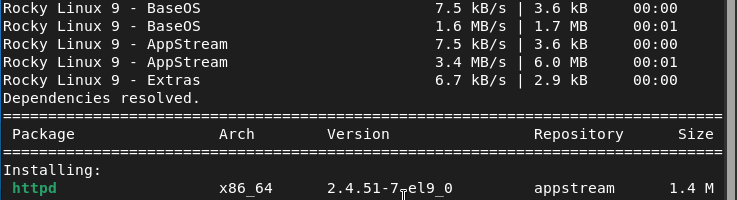
Apache HTTP-сервер — свободный веб-сервер. Apache является кроссплатформенным ПО, поддерживает операционные системы Linux, BSD, macOS, Microsoft Windows, Novell NetWare, BeOS.

Основными достоинствами Apache считаются надёжность и гибкость конфигурации. Он позволяет подключать внешние модули для предоставления данных, использовать СУБД для аутентификации пользователей, модифицировать сообщения об ошибках и т. д. Поддерживает IPv4. [3]

# 3 Выполнение лабораторной работы

## 3.1 Подготовка лабораторного стенда

1. Установили httpd. (??)



Установка httpd

1. В конфигурационном файле /etc/httpd/httpd.conf необходимо задали параметр ServerName. (??)

Задача параметра ServerName

Задача параметра ServerName

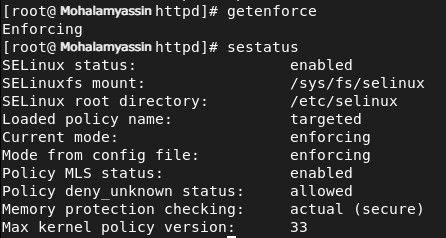
1. Отключили фильтры. (??)

Отключение фильтров

Отключение фильтров

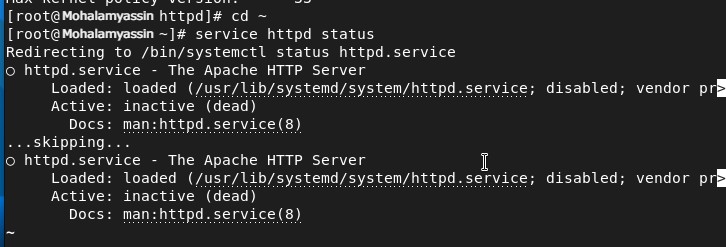
## 3.2 Основная часть

1. Убедились, что SELinux работает в режиме enforcing политики targeted. (??)

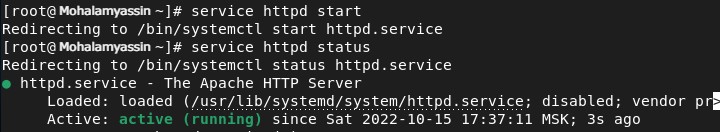


Режим работы SELinux

1. Увидели, что сервер не работает и запустили его. (??, ?? )

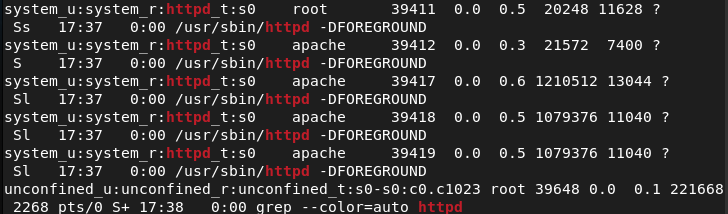


Проверка работы сервера



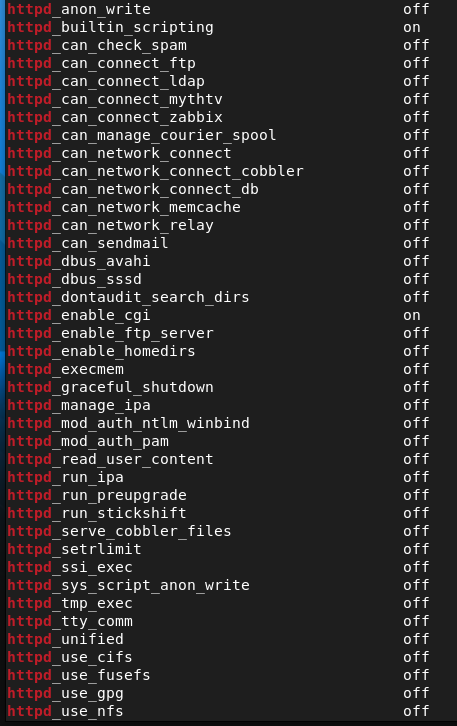
Запуск сервера

1. Определили контекст безопасности Appache - unconfined\_u:unconfined\_r:unconfined\_t. (??)



Определение контекста безопасности

1. Посмотрели текущее состояние переключателей SELinux для Apache. (??)



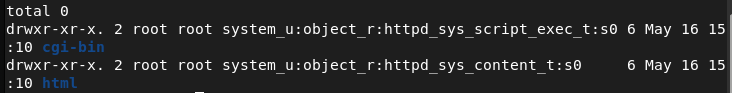
Текущее состояние переключателей SELinux для Apache

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



Статистика по политике

1. Определили тип файлов и поддиректорий, находящихся в директории /var/www. (??)



Тип файлов и поддиректорий в /var/www

1. Определили тип файлов и поддиректорий, находящихся в директории /var/www/html. (??)

Тип файлов и поддиректорий в /var/www/html

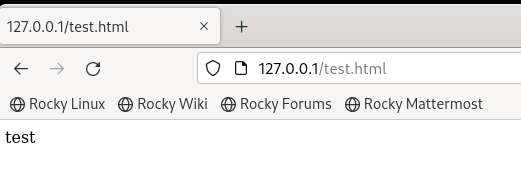
Тип файлов и поддиректорий в /var/www/html

1. Создали файл test.html и проверили его контест. (??)



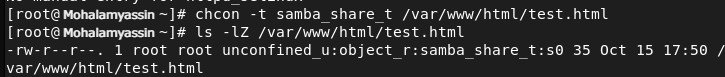
Создание test.html

1. Обратились к файлу через веб-сервер. (??)



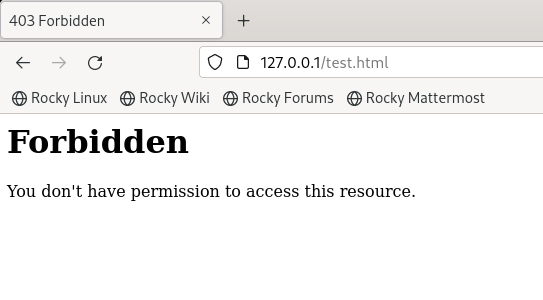
Обращение к файлу через браузер

1. Изменили контекст файла и проверили что он поменялся. (??)



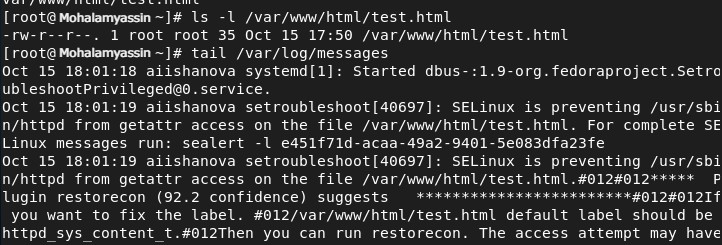
Смена контекста test.html

1. Попробовали получить доступ к файлу через браузер. (??)



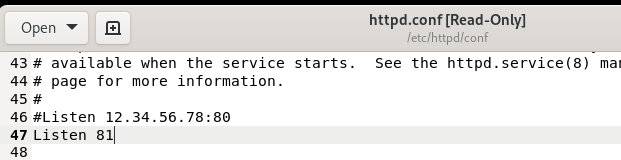
Обращение к файлу через браузер после смены контекста

1. Просмотрели системный лог-файл. Увидели, что проблема в смененном контексте. (??)



Просмотр системного лог-файла

1. Поменяли прослушивание TCP-порта на 81. (??)



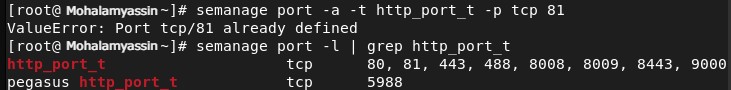
Изменение прослушивания TCP-порта

1. Перезапустили Apache, не получили ошибки. (??)



Перезапуск Apache

1. Добавили порт 81 и проверили, что он появился в списке. (??)



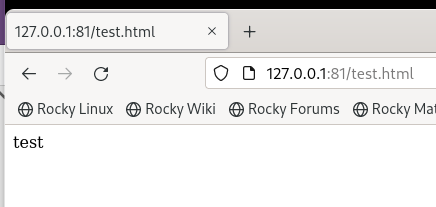
Добавление порта 81

1. Перезапустили Apache, вернули изначальный контекст test.html. (??)

Перезапуск Apache, возвращение изначального контекста test.html

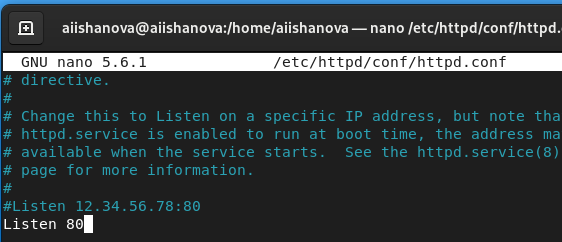
Перезапуск Apache, возвращение изначального контекста test.html

1. Обратились к файлу через веб-сервер. (??)



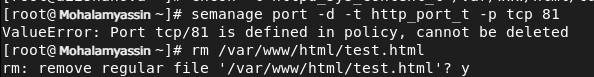
Обращение к файлу через браузер после возвращения контекста

1. Вернули порт 80. (??)



Возвращение порта 80 в httpd.conf

1. Ввели команду для удаления порта 81 из списка. Удалили файл test.html. (??)



Работа команды удаления порта 81 и удаление test.html

# 4 Вывод

В ходе выполнения лабораторной работы были развиты навыки администрирования ОС Linux и проверена работа SELinux на практике совместно с веб-сервером Apache.

# 5 Библиография

1. Методические материалы курса.
2. Wikipedia: SELinux (URL: https://ru.wikipedia.org/wiki/SELinux)
3. Wikipedia: Apache HTTP Server (URL: https://ru.wikipedia.org/wiki/Apache\_HTTP\_Server)