Лабораторная работа №6

Основы информационной безопасности

Серёгина Ирина Андреевна

Содержание

# 1 Цель работы

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

# 2 Задание

1. Подготовить рабочую среду.
2. Выполнить лабораторную работу.
3. Записать вывод.

# 3 Теоретическое введение

1. При подготовке стенда обратите внимание, что необходимая для работы и указанная выше политика targeted и режим enforcing используются в данном дистрибутиве по умолчанию, т.е. каких-то специальных настроек не требуется. При этом следует убедиться, что политика и режим включены, особенно когда работа будет проводиться повторно и велика вероятность изменений при предыдущем использовании системы.
2. При необходимости администратор должен разбираться в работе SELinux и уметь как исправить конфигурационный файл /etc/selinux/config, так и проверить используемый режим и политику.
3. Необходимо, чтобы был установлен веб-сервер Apache. При установке системы в конфигурации «рабочая станция» указанный пакет не ставится.
4. В конфигурационном файле /etc/httpd/httpd.conf необходимо задать параметр ServerName: ServerName test.ru чтобы при запуске веб-сервера не выдавались лишние сообщения об ошибках, не относящихся к лабораторной работе.
5. Также необходимо проследить, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp. Отключить фильтр можно командами iptables -F iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT либо добавить разрешающие правила: iptables -I INPUT -p tcp –dport 80 -j ACCEPT iptables -I INPUT -p tcp –dport 81 -j ACCEPT iptables -I OUTPUT -p tcp –sport 80 -j ACCEPT iptables -I OUTPUT -p tcp –sport 81 -j ACCEPT
6. Обратите внимание, что данные правила не являются «точными» и рекомендуемыми на все случаи жизни, они лишь позволяют правильно организовать работу стенда.
7. В работе специально не делается акцент, каким браузером (или какой консольной программой) будет производиться подключение к вебсерверу. По желанию могут использоваться разные программы, такие как консольные links, lynx, wget и графические konqueror, opera, firefox или др.

# 4 Выполнение лабораторной работы

1. Для начала я обновила ПО, установила Apache с помощью команд yum update -y и yum install httpd -y. Затем вошла в систему и проверила, что SELinux работает в режиме enforcing (рис. [[1](#fig:001)]).

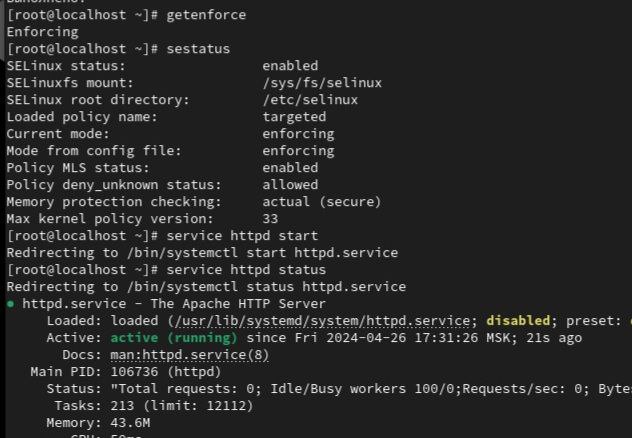


Figure 1: подготовка к работе

1. Запустила и проверила работу веб-сервера (рис. [[2](#fig:002)]).

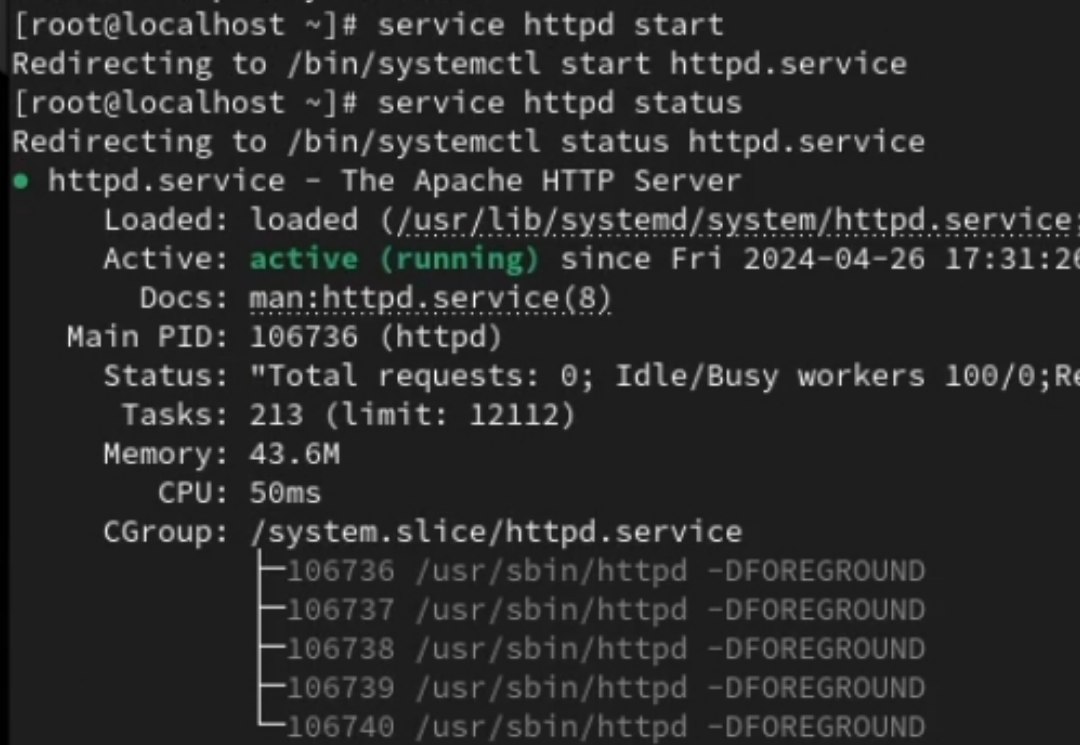


Figure 2: запуск работы Apache

1. Узнала контекст безопасности (рис. [[3](#fig:003)]).

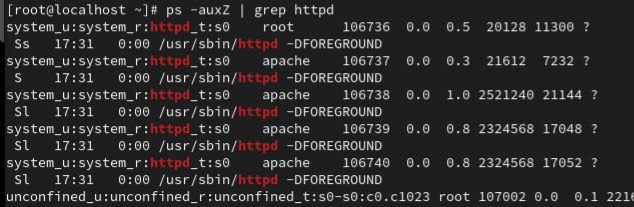


Figure 3: проверка контекста безопасности

1. Уточнила текущее состояние переключателей SELinux для Apache (рис. [[4](#fig:004)]).

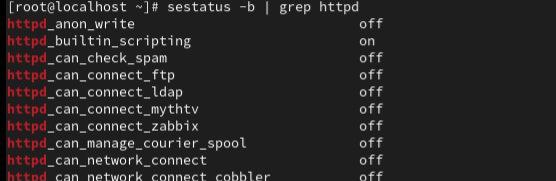


Figure 4: состояние переключателей

1. С помощью seinfo узнала статистику по политике (рис. [[5](#fig:005)]).

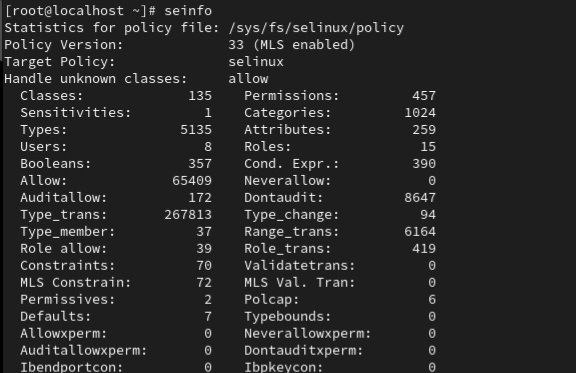


Figure 5: статистика по политике

1. Определила тип файлов и поддиректорий директории /var/www. При определении типа файлов директории /var/www/html ничего не отображается (рис. [[6](#fig:006)]).

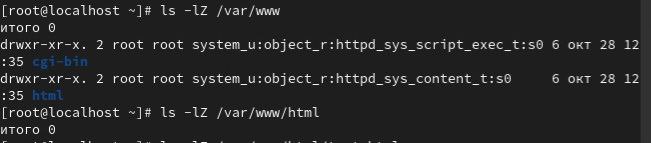


Figure 6: www

1. Создаю файл test.html, заполняю его (рис. [[7](#fig:007)]).



Figure 7: test.html

1. Проверяю контекст файла (рис. [[8](#fig:008)]).

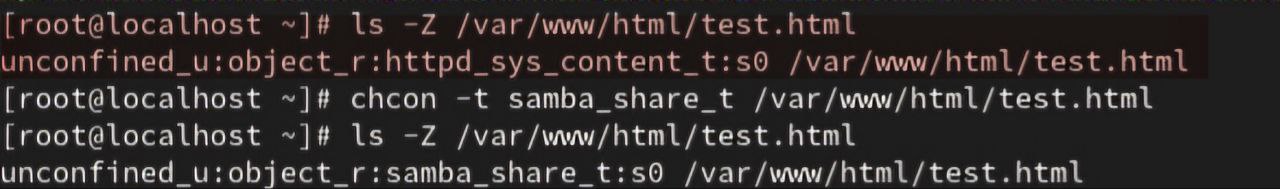


Figure 8: контекст

1. Обращаюсь к файлу через веб-сервер, его содержимое успешно отображается (рис. [[9](#fig:009)]).

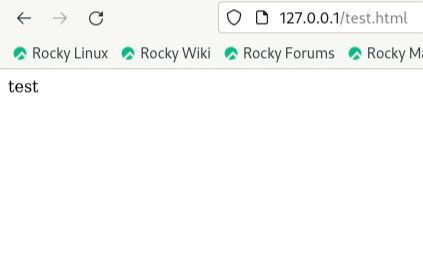


Figure 9: веб-страница файла

1. Изменяю контекст файла (рис. [[10](#fig:010)]).

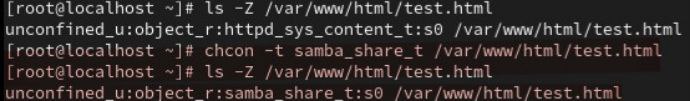


Figure 10: изменение контекста

1. После изменения контекста доступ к файлу через веб-сервер был невозможен (рис. [[11](#fig:011)]).

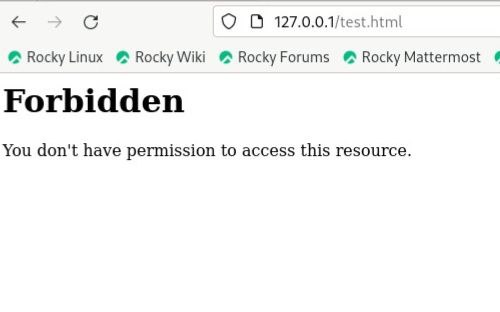


Figure 11: ошибка доступа

1. В файле меняю строку Listen 80 на Listen 81, чтобы запустить веб-сервер на прослушивание TCP-порта 81 (рис. [[12](#fig:012)]).

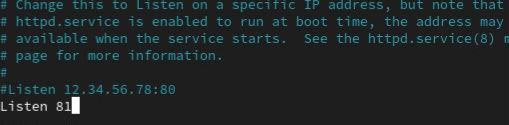


Figure 12: изменения в файле

1. Настраиваю порт (рис. [[13](#fig:013)]).

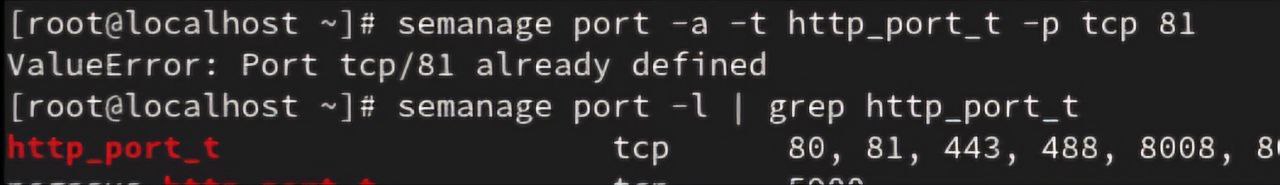


Figure 13: настройка порта 81

1. Однако даже после этого веб-сервер на отображает файл (рис. [[14](#fig:014)]).

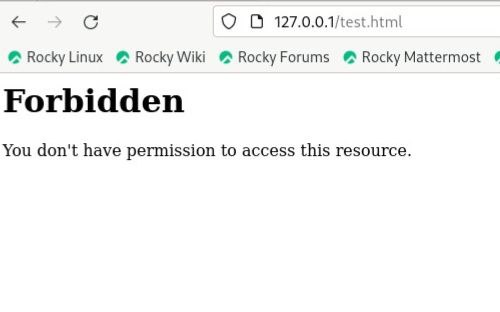


Figure 14: ошибка

1. Изменяю контекст файла обратно, после этого страница отображает все корректно (рис. [[15](#fig:015)]).

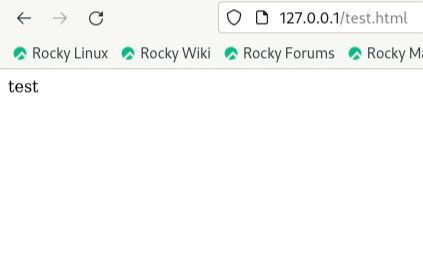


Figure 15: веб-страница

1. Убираю изменения из конфигурационного файла, пытаюсь привязку к 81 порту, но поялвяется ошибка. Удаляю ранее созданный файл (рис. [[16](#fig:016)]).



Figure 16: удаление файла

# 5 Выводы

Я развила навыки администрирования ОС Linux, получила первое практическое знакомство с технологией SELinux. Проверила работу SELinx на практике совместно с веб-сервером Apache.

# Список литературы