**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКИЙ**

**УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

Факультет физико-математических и естественных наук

Кафедра информационных технологий

ОТЧЕТ по лабораторной работе 6

ТЕМА «**Мандатное разграничение прав в Linux**»

**по дисциплине «Информационная безопасность»**

**Выполнил:**

Студент группы НПИбд-02-21

Студенческий билет № 1032205421

Стелина Петрити

# Список содержания

**Список содержания Список изображений** Цель работы

Последовательность выполнения работы

* 1. Подготовка лабораторного стенда и методические рекомендации
  2. Порядок выполнения работы Вывод

# Список изображений

рис. 1 SELinux и Enforcing рис. 2 Установка httpd

рис. 3 Добавьте строку ServerName test.ru рис. 4 Настройка пакета iptables

рис. 5 Выбор браузера lynx

рис. 6 Вход в систему и проверка режима SELinux

рис. 7 статус веб-сервера, eсли сервер не запущен, запустите c start рис. 8 Определение контекста безопасности Apache

рис. 9 Просмотр состояние переключателей SELinux для Apache рис. 10 статистики по политике SELinux

рис. 11 Определение типов файлов и директорий рис. 12 Определение типов файлов в /var/www/html рис. 13 Проверка прав создания файлов

рис. 14 Создание HTML-файла рис. 15 контекст созданного файла

рис. 16 файл отображается корректно рис. 17 Изменение контекста файла рис. 18 Проверка доступа к файлу рис. 19 Анализ логов

рис. 20 Запуск Apache на порту 81 рис. 21 Перезапуск веб-сервера

рис. 22 Анализ логов после изменения порта рис. 23 Добавление нового порта в SELinux рис. 24 Восстановление контекста файла рис. 25 Перезапуск веб-сервера Apache

рис. 26 Возвращение Apache на порт 80

рис. 27 Удаление порта 81 из списка SELinux рис. 28 Удаление файла

## Цель работы

Развить навыки управления операционной системой Linux, получив практический опыт работы с технологией SELinux.

Исследовать работу SELinux на практике в сочетании с веб-сервером Apache.

## Последовательность выполнения работы

* 1. **Подготовка лабораторного стенда и**

## методические рекомендации

* + 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

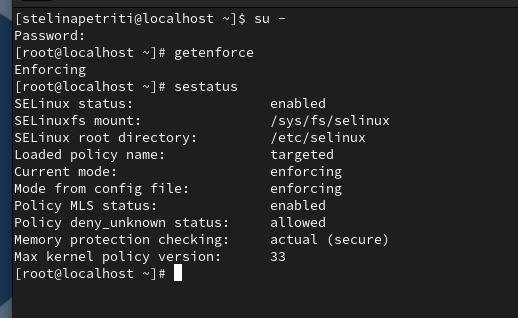


рис. 1 SELinux и Enforcing

* + 1. При необходимости администратор должен разбираться в работе SELinux и уметь как исправить конфигурационный файл /etc/selinux/config, так и проверить используемый режим и политику.
    2. Необходимо, чтобы был установлен веб-сервер Apache. При установке системы в конфигурации «рабочая станция» указанный пакет не ставится.

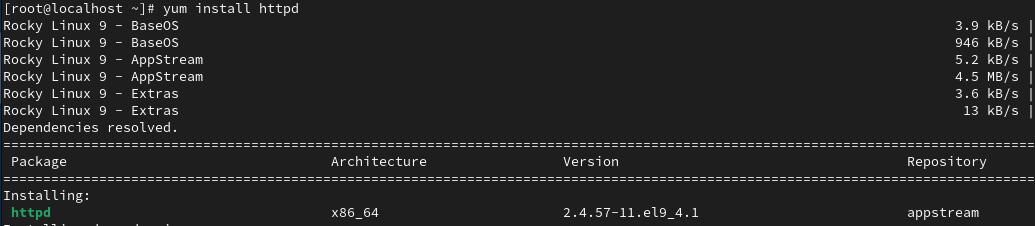


рис. 2 Установка httpd

* + 1. 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.

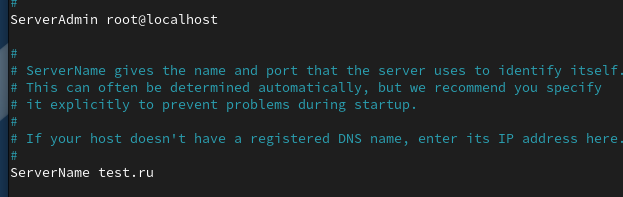


рис. 3 Добавьте строку ServerName test.ru

* + 1. 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

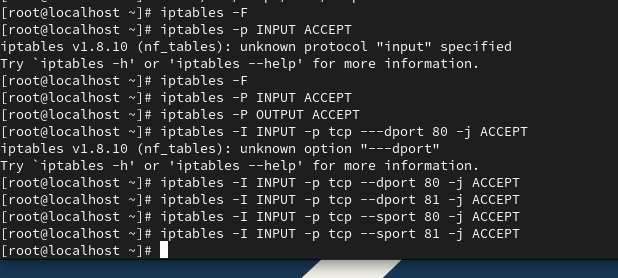


рис. 4 Настройка пакета iptables

* + 1. Обратите внимание, что данные правила не являются «точными» и рекомендуемыми на все случаи жизни, они лишь позволяют правильно организовать работу стенда.
    2. В работе специально не делается акцент, каким браузером (или какой консольной программой) будет производиться подключение к веб-серверу. По желанию могут

использоваться разные программы, такие как консольные links, lynx, wget и графические

konqueror, opera, firefox или др.

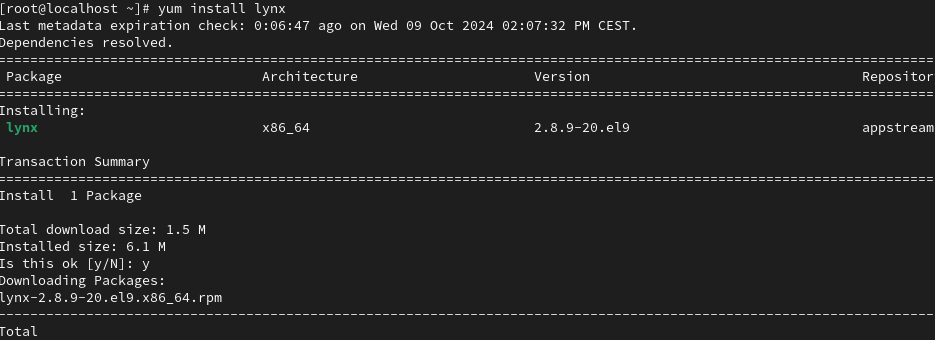


рис. 5 Выбор браузера lynx

## Порядок выполнения работы

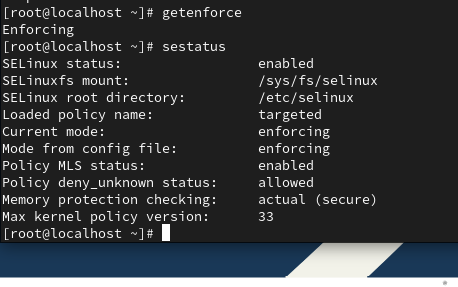
* + 1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus.

рис. 6 Вход в систему и проверка

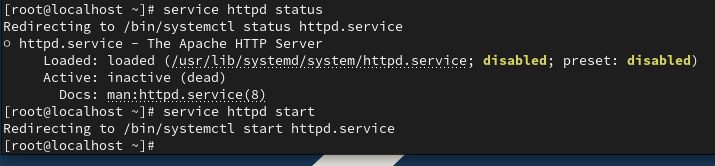
* + 1. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: service httpd status или /etc/rc.d/init.d/httpd status Если не работает, запустите его так же, но с параметром start.

рис. 7 статус веб-сервера, eсли сервер не запущен, запустите c start

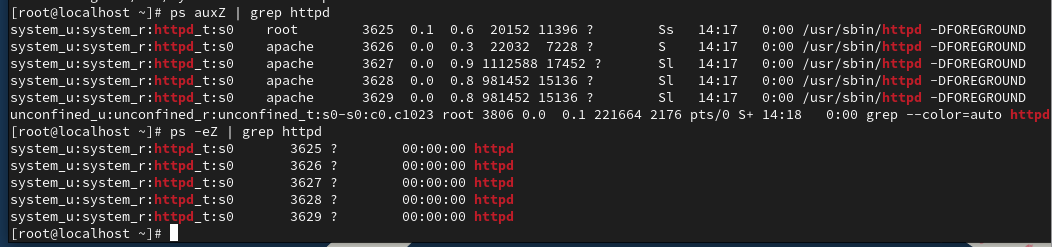
* + 1. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду ps auxZ | grep httpd или ps -eZ | grep httpd

рис. 8 Определение контекста безопасности Apache

* + 1. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды

sestatus -bigrep httpd

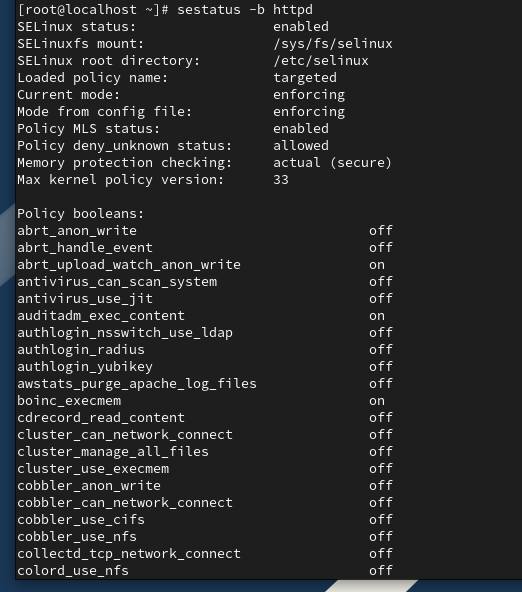


рис. 9 Просмотр состояние переключателей SELinux для Apache

Обратите внимание, что многие из них находятся в положении «off».

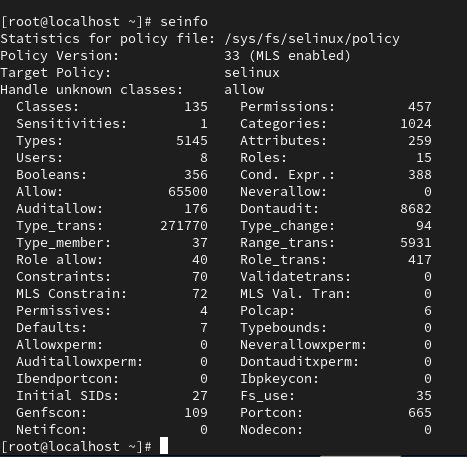
* + 1. Посмотрите статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов.

рис. 10 статистики по политике SELinux

* + 1. Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www

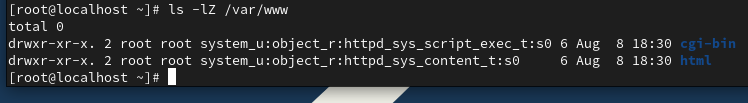


рис. 11 Определение типов файлов и директорий

* + 1. Определите тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html

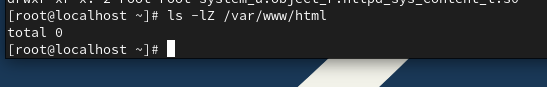


рис. 12 Определение типов файлов в /var/www/html

* + 1. Определите круг пользователей, которым разрешено создание файлов в директории

/var/www/html.

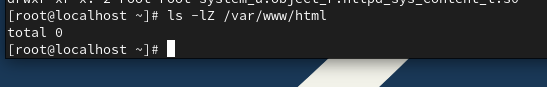


рис. 13 Проверка прав создания файлов

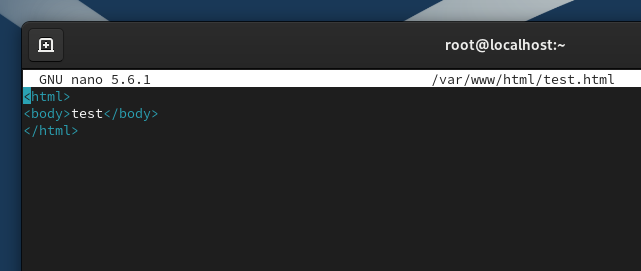
* + 1. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания: test

рис. 14 Создание HTML-файла

* + 1. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html.

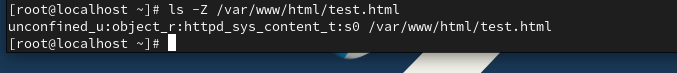


рис. 15 контекст созданного файла

* + 1. Обратитесь к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>.

Убедитесь, что файл был успешно отображён.

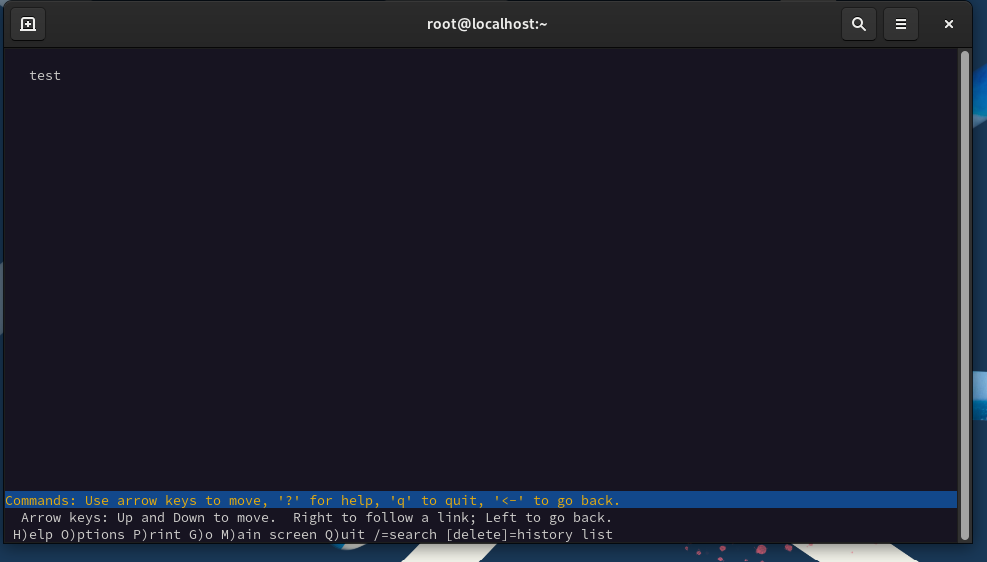


рис. 16 файл отображается корректно

* + 1. Изучите справку man httpd\_selinux и выясните, какие контексты файлов определены для httpd. Сопоставьте их с типом файла test.html. Проверить контекст файла можно командой ls -Z. ls -Z /var/www/html/test.html

Рассмотрим полученный контекст детально. Обратите внимание, что так как по умолчанию

пользователи CentOS являются свободными от типа (unconfined в переводе с англ. означает свободный), созданному нами файлу test.html был сопоставлен SELinux, пользователь unconfined\_u. Это первая часть контекста. Далее политика ролевого разделения доступа RBAC используется процессами, но не файлами, поэтому роли не имеют никакого значения для

файлов. Роль object\_r используется по умолчанию для файлов на «постоянных» носителях и на сетевых файловых системах. (В директории /ргос файлы, относящиеся к процессам, могут иметь роль system\_r. Если активна политика MLS, то могут использоваться и другие роли, например, secadm\_r. Данный случай мы рассматривать не будем, как и предназначение :s0). Тип httpd\_sys\_content\_t позволяет процессу httpd получить доступ к файлу. Благодаря наличию

последнего типа мы получили доступ к файлу при обращении к нему через браузер.

* + 1. Измените контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на любой другой, к которому процесс httpd не должен иметь доступа, например, на samba\_share\_t: chcon -t samba\_share\_t /var/www/html/test.html ls -Z /var/www/html/test.html. После этого

проверьте, что контекст поменялся.

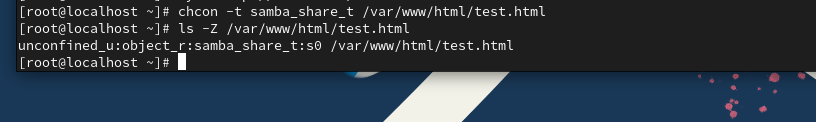


рис. 17 Изменение контекста файла

* + 1. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес [htt](http://127.0.0.1/test.html) [p://127.0.0.1/test.html](http://127.0.0.1/test.html). Вы должны получить сообщение об ошибке: Forbidden You don't have permission to access /test.html on this server.

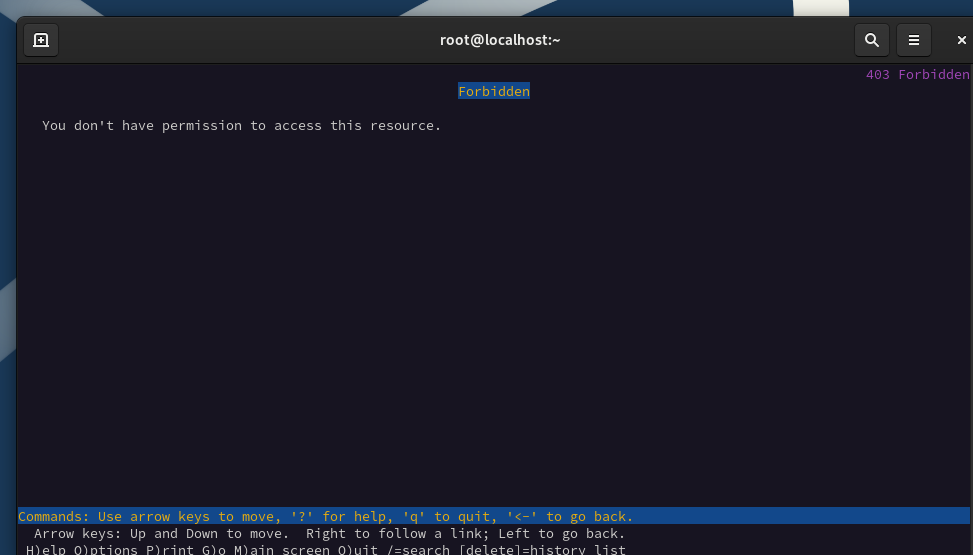


рис. 18 Проверка доступа к файлу

* + 1. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? ls -l /var/www/html/test.html Просмотрите log-

файлы веб-сервера Apache. Также просмотрите системный лог-файл: tail /var/log/messages Если в системе окажутся запущенными процессы setroubleshootd и audtd, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле /var/log/audit/audit.log.

Проверьте это утверждение самостоятельно.

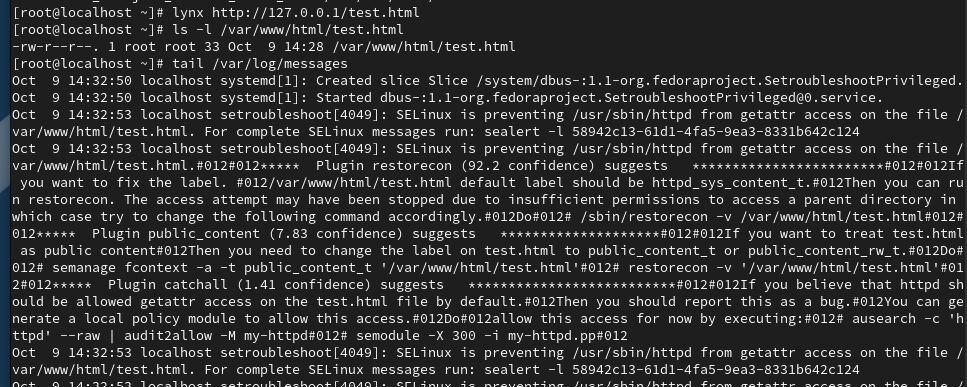


рис. 19 Анализ логов

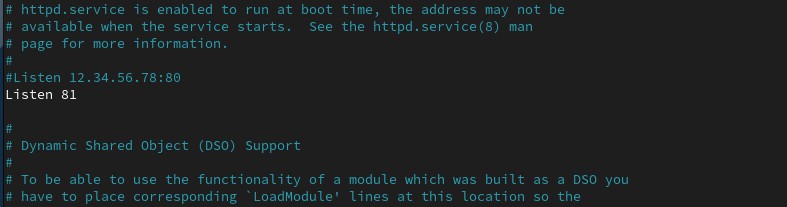
* + 1. Попробуйте запустить веб-сервер Apache на прослушивание ТСР-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf найдите строчку Listen 80 и замените её на Listen 81.

рис. 20 Запуск Apache на порту 81

* + 1. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему?

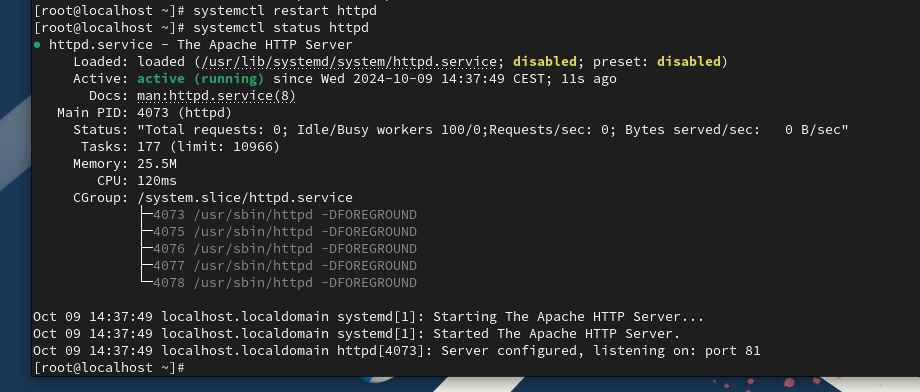


рис. 21 Перезапуск веб-сервера

* + 1. Проанализируйте лог-файлы: tail -nl /var/log/messages, /var/log/http/access\_log

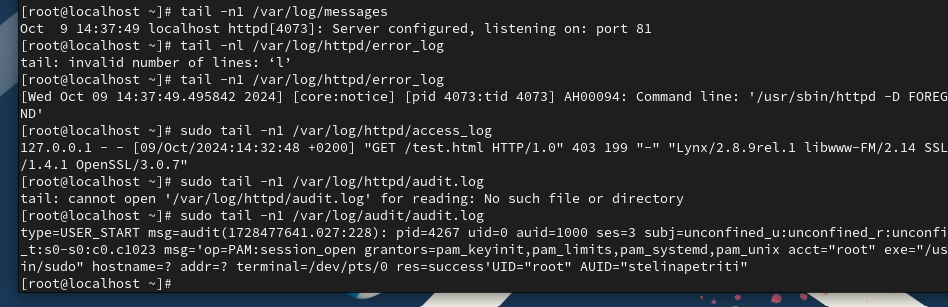


рис. 22 Анализ логов после изменения порта

* + 1. Выполните команду semanage port -a -t http\_port\_t -р tcp 81. После этого проверьте список портов командой semanage port -l | grep http\_port\_t Убедитесь, что порт 81 появился в списке.

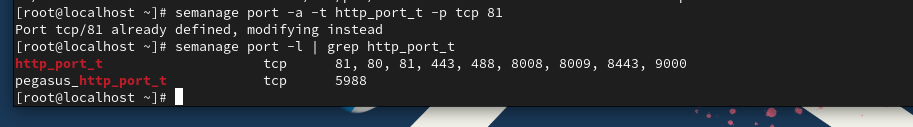


рис. 23 Добавление нового порта в SELinux

* + 1. Попробуйте запустить веб-сервер Apache ещё раз. http://127.0.0.1:81/test.html
    2. Верните контекст httpd\_sys\_cоntent t к файлу /var/www/html/ test.html: chcon -t httpd\_sys\_content\_t /var/www/html/test.html После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. Вы должны увидеть содержимое файла — слово «test».



рис. 24 Восстановление контекста файла

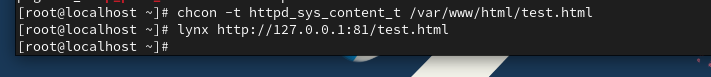


рис. 25 Перезапуск веб-сервера Apache

* + 1. Исправьте обратно конфигурационный файл apache, вернув Listen 80.

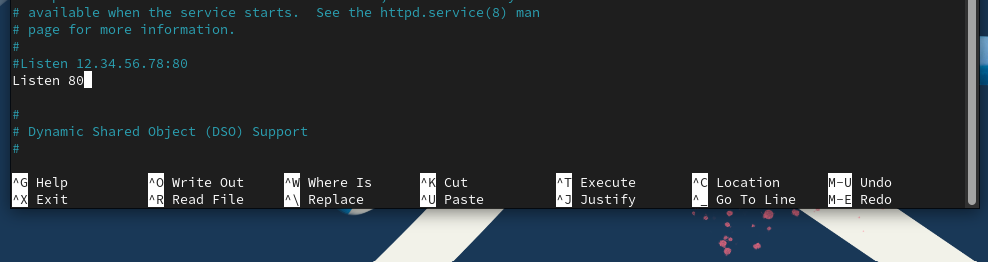


рис. 26 Возвращение Apache на порт 80

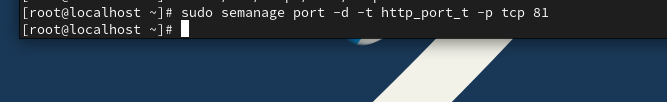
* + 1. Удалите привязку http\_port\_t к 81 порту: semanage port -d -t http\_port\_t -p tcp 81 и проверьте, что порт 81 удалён.

рис. 27 Удаление порта 81 из списка SELinux

* + 1. Удалите файл /var/www/html/test.html: rm /var/www/html/test.html

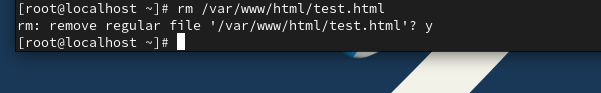


рис. 28 Удаление файла

## Вывод

В данной лабораторной работе мы изучили настройку и механизмы безопасности веб-сервера Apache в среде SELinux. Мы проверили активность службы Apache и убедились, что она корректно настроена для прослушивания на определённых портах, таких как 80 и 81.

Анализируя контексты SELinux и права доступа пользователей, мы поняли, как SELinux управляет доступом к файлам и каталогам в корневом каталоге веб-сервера. Возникшие проблемы,

связанные с политиками SELinux, показали важность глубокого понимания взаимодействия этой системы безопасности с сетевыми службами, что ещё раз подчеркнуло необходимость детального изучения SELinux в реальных условиях.