**Федеральное государственное автономное образовательное учреждение высшего образования**

**«РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ»**

**(РУДН)**

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 № 1032205641

Сатлихана Петрити

(Подпись)

Москва 2024

# Список содержания

[Список содержания 2](#_Toc179221088)

[Список изображений 3](#_Toc179221089)

[Цель работы 4](#_Toc179221090)

[*Последовательность выполнения работы* 4](#_Toc179221091)

[Выводы 12](#_Toc179221092)

# Список изображений

[рис. 1 Политика SELinux и режим Enforcing 5](#_Toc179221013)

[рис. 2 Установка и настройка веб-сервера Apache 5](#_Toc179221014)

[рис. 3 Добавьте строку 6](#_Toc179221015)

[рис. 4 Настройка пакета фильтра (iptables) 6](#_Toc179221016)

[рис. 5 Выбор браузера 6](#_Toc179221017)

[рис. 6 Вход в систему и проверка режима SELinux 7](#_Toc179221018)

[рис. 7 статус веб-сервера 7](#_Toc179221019)

[рис. 8 Если сервер не запущен, запустите его 7](#_Toc179221020)

[рис. 9 Определение контекста безопасности веб-сервера Apache 8](#_Toc179221021)

[рис. 10 Просмотр переключателей SELinux для Apache 8](#_Toc179221022)

[рис. 11 Просмотр статистики по политике SELinux 8](#_Toc179221023)

[рис. 12 Определение типов файлов и директорий в /var/www 9](#_Toc179221024)

[рис. 13 Определение типов файлов в /var/www/html 9](#_Toc179221025)

[рис. 14 Проверка прав создания файлов в директории /var/www/html 9](#_Toc179221026)

[рис. 15 Создание HTML-файла 9](#_Toc179221027)

[рис. 16 Проверка контекста созданного файла 9](#_Toc179221028)

[рис. 17 файл отображается корректно 10](#_Toc179221029)

[рис. 18 Изменение контекста файла 10](#_Toc179221030)

[рис. 19 Проверка доступа к файлу после изменения контекста 11](#_Toc179221031)

[рис. 20 Анализ логов 11](#_Toc179221032)

[рис. 21 Запуск Apache на порту 81 11](#_Toc179221033)

[рис. 22 Перезапуск веб-сервера 12](#_Toc179221034)

[рис. 23 Анализ логов после изменения порта 12](#_Toc179221035)

[рис. 24 Добавление нового порта в SELinux 12](#_Toc179221036)

[рис. 25 Восстановление контекста файла 13](#_Toc179221037)

[рис. 26 Перезапуск веб-сервера Apache 13](#_Toc179221038)

[рис. 27 Возвращение Apache на порт 80 13](#_Toc179221039)

[рис. 28 Удаление порта 81 из списка SELinux 13](#_Toc179221040)

[рис. 29 Удаление файла 13](#_Toc179221041)

Цель работы  
Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux.

Проверить работу SELinx на практике совместно с веб-сервером Apache.

*Последовательность выполнения работы*

6.3. 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.

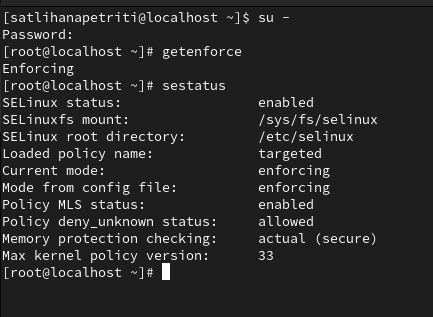


рис. 1 Политика SELinux и режим Enforcing

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

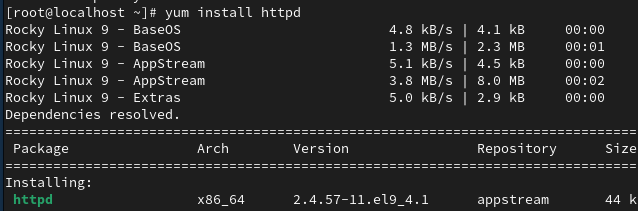
системы в конфигурации «рабочая станция» указанный пакет не ставится. 

рис. 2 Установка и настройка веб-сервера Apache

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.

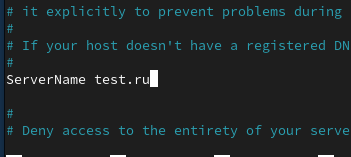


рис. 3 Добавьте строку

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

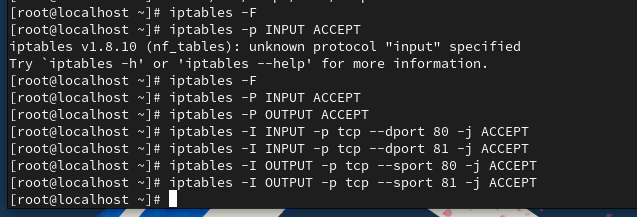


рис. 4 Настройка пакета фильтра (iptables)

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.

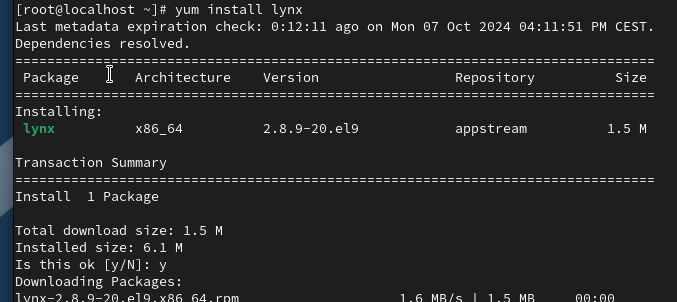


рис. 5 Выбор браузера

6.4. 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.

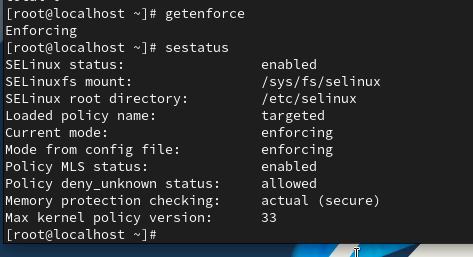


рис. 6 Вход в систему и проверка режима SELinux

2. 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.

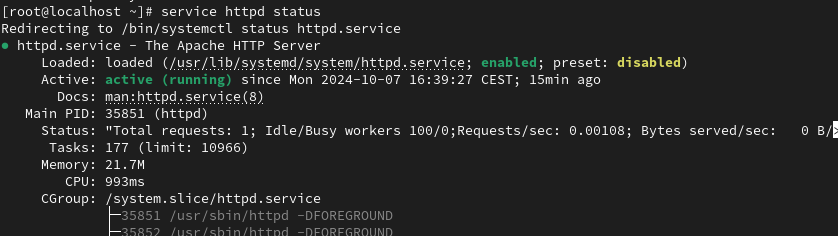


рис. 7 статус веб-сервера

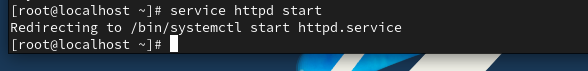


рис. 8 Если сервер не запущен, запустите его

3. 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

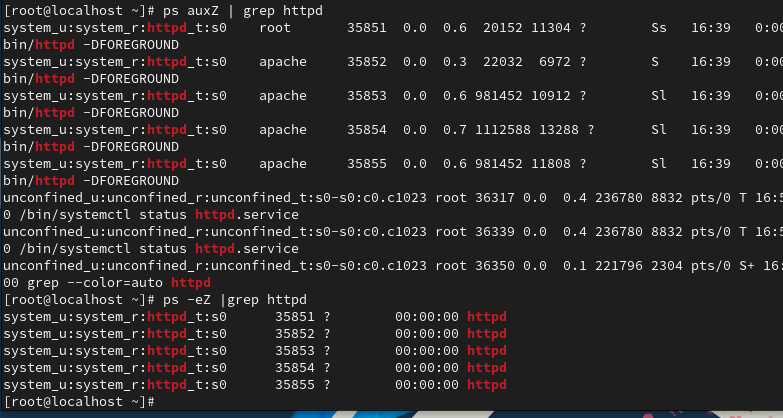


рис. 9 Определение контекста безопасности веб-сервера Apache

4. Посмотрите текущее состояние переключателей SELinux для Apache с

помощью команды

sestatus -bigrep httpd

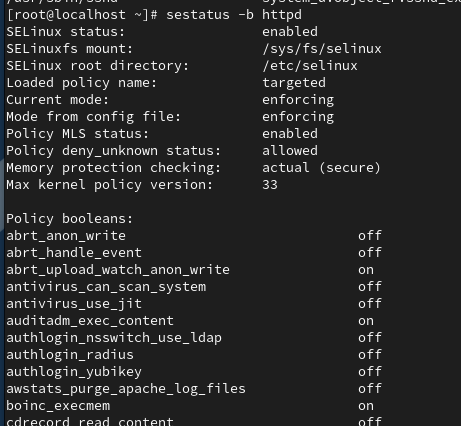


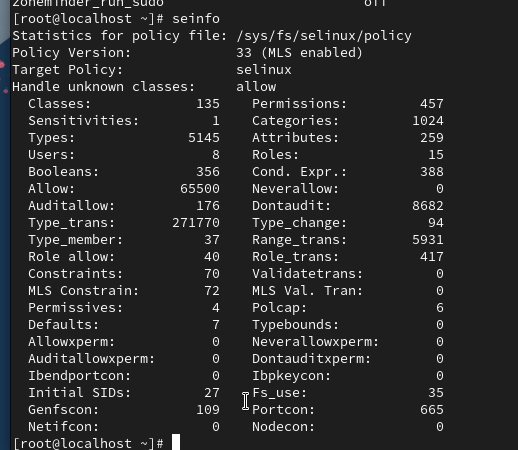
рис. 10 Просмотр переключателей SELinux для Apache

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

5. Посмотрите статистику по политике с помощью команды seinfo, также

определите множество пользователей, ролей, типов.

рис. 11 Просмотр статистики по политике SELinux



6. Определите тип файлов и поддиректорий, находящихся в директории

/var/www, с помощью команды

ls -lZ /var/www

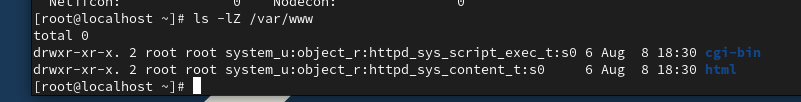


рис. 12 Определение типов файлов и директорий в /var/www

7. Определите тип файлов, находящихся в директории /var/www/html:

ls -lZ /var/www/html

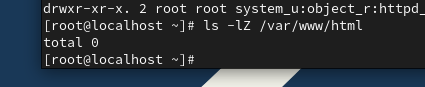


рис. 13 Определение типов файлов в /var/www/html

8. Определите круг пользователей, которым разрешено создание файлов в

директории /var/www/html.



рис. 14 Проверка прав создания файлов в директории /var/www/html

9. 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:

**<html> <body>**test**</body>**

**</html>**

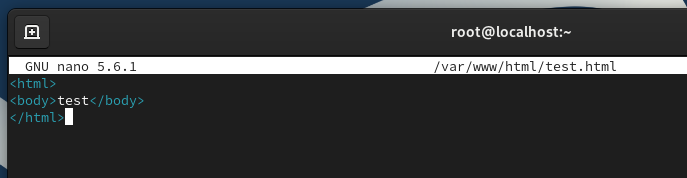


рис. 15 Создание HTML-файла

10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст,

присваиваемый по умолчанию вновь созданным файлам в директории

/var/www/html.

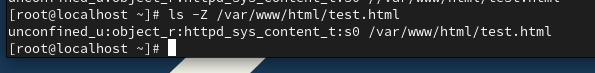


рис. 16 Проверка контекста созданного файла

11. Обратитесь к файлу через веб-сервер, введя в браузере адрес

http://127.0.0.1/test.html. Убедитесь, что файл был успешно отображён.

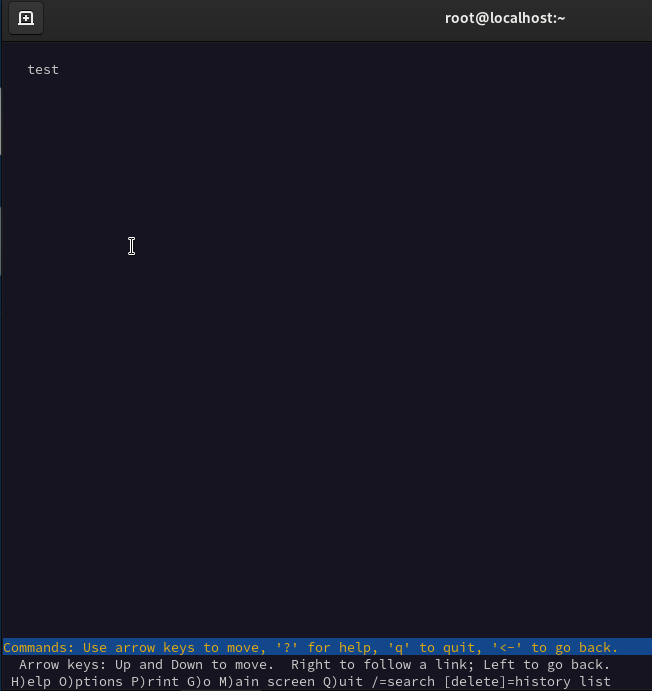


рис. 17 файл отображается корректно

12. 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.

13. 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.

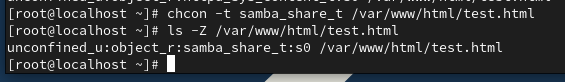


рис. 18 Изменение контекста файла

14. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в

браузере адрес 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.

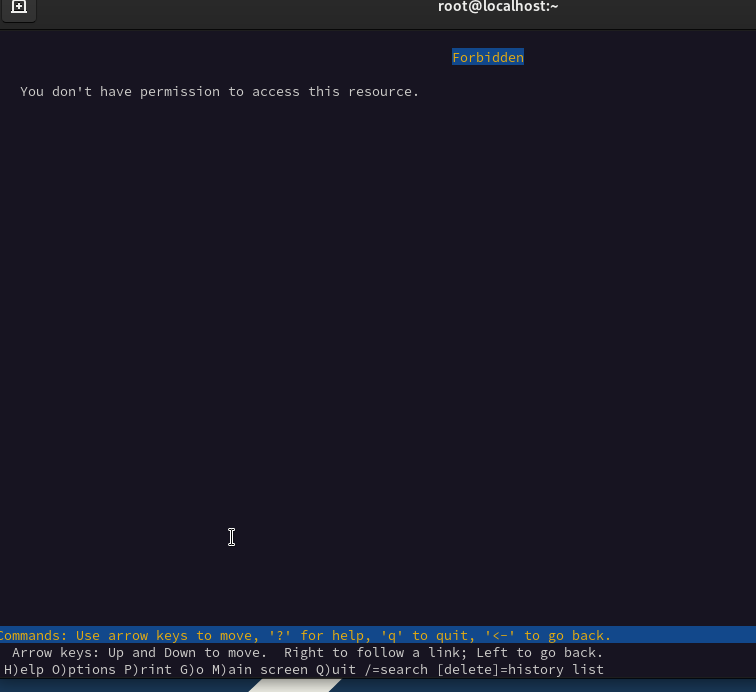


рис. 19 Проверка доступа к файлу после изменения контекста

15. 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.

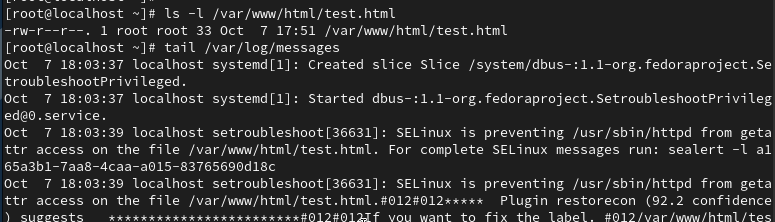


рис. 20 Анализ логов

16. 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.

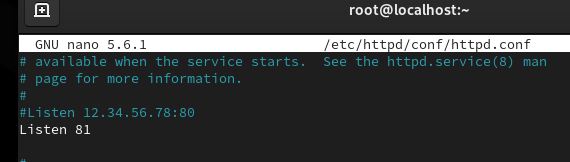


рис. 21 Запуск Apache на порту 81

17. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните

почему?

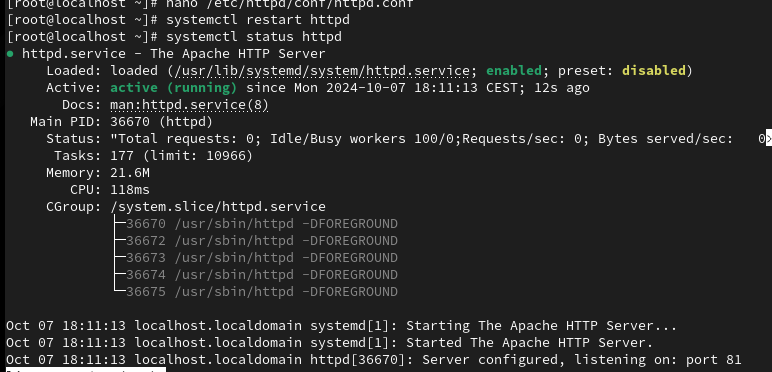


рис. 22 Перезапуск веб-сервера

18. Проанализируйте лог-файлы:

tail -nl /var/log/messages

|  |  |  |
| --- | --- | --- |
| Просмотрите | файлы | /var/log/http/error\_log, |
| /var/log/http/access\_log | и | /var/log/audit/audit.log | и |

выясните, в каких файлах появились записи.

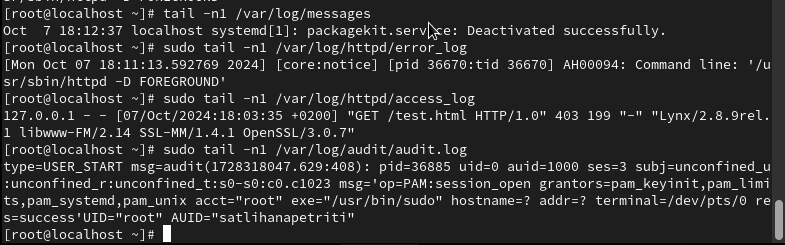


рис. 23 Анализ логов после изменения порта

19. 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.

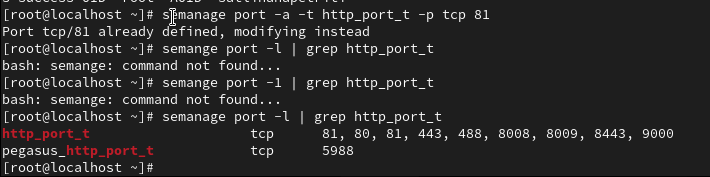


рис. 24 Добавление нового порта в SELinux

20. Попробуйте запустить веб-сервер Apache ещё раз.

http://127.0.0.1:81/test.html

21. 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. 25 Восстановление контекста файла

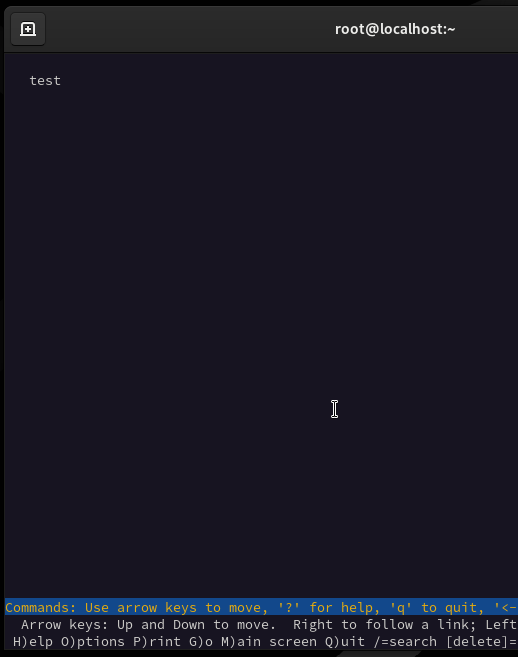


рис. 26 Перезапуск веб-сервера Apache

22. Исправьте обратно конфигурационный файл apache, вернув Listen 80.

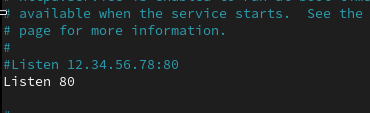


рис. 27 Возвращение Apache на порт 80

23. 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. 28 Удаление порта 81 из списка SELinux

24. Удалите файл /var/www/html/test.html:

rm /var/www/html/test.html



рис. 29 Удаление файла

Выводы

В этой лабораторной работе мы исследовали конфигурацию и механизмы безопасности веб-сервера Apache в среде SELinux. Мы убедились, что служба Apache активна и правильно настроена для прослушивания определённых портов, таких как 80 и 81.

Изучая контексты SELinux и разрешения пользователей, мы поняли, как управляются доступы к файлам и каталогам в корневом каталоге веб-сервера. Мы столкнулись с проблемами, связанными с политиками SELinux, что подчеркнуло важность понимания взаимодействия SELinux с сетевыми службами.