Отчёт по лабораторной работе №6 по предмету Информационная безопасность

Мандатное разграничение прав в Linux

Саттарова Вита Викторовна

Содержание

# 1 Цели и задачи работы

**Цели:**

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

**Задачи:**

* Выполнить все пункты, указанные в методических рекомендациях к лабораторной работе.
* Ответить на вопросы, заданные в методических рекомендациях к лабораторной работе.
* Выполняя задания, познакомиться с технологией SELinux.
* Выполняя задания, поработать с SELinx с веб-сервером Apache.
* Написать отчёт, проанализировав результаты, полученные в ходе выполнения лабораторной работы.

# 2 Объект и предмет исследования

**Объект исследования:** использование SELinux и веб-сервером Apache для обеспечения безопасности.

**Предмет исследования:** администрирование, SELinux, веб-сервер Apache.

# 3 Условные обозначения и термины

**Условные обозначения**

* ОС - операционная система

**Термины**

* контекст безопасности

# 4 Задание

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus.
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.
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
4. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды sestatus -b | grep httpd 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.
6. Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www
7. Определите тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html
8. Определите круг пользователей, которым разрешено создание 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>

1. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html.
2. Обратитесь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедитесь, что файл был успешно отображён.
3. 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
4. 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.
5. 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.
6. 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.
7. 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.
8. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему?
9. 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.
10. 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.
11. Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему он сейчас запустился, а в предыдущем случае не смог?
12. 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».
13. Исправьте обратно конфигурационный файл apache, вернув Listen 80.
14. Удалите привязку http\_port\_t к 81 порту: semanage port -d -t http\_port\_t -p tcp 81 и проверьте, что порт 81 удалён.
15. Удалите файл /var/www/html/test.html: rm /var/www/html/test.html

Более подробно о работе см. в [[1]](bib/cite.bib).

# 5 Теоретическое введение

## 5.1 Организация и описание лабораторного стенда

Для проведения указанной лабораторной работы на одно рабочее место требуется компьютер с установленной операционной системой Linux, поддерживающей технологию SELinux.

Предполагается использовать стандартный дистрибутив Linux CentOS с включённой политикой SELinux targeted и режимом enforcing. Для выполнения заданий требуется наличие учётной записи администратора (root) и учётной записи обычного пользователя. Постоянно работать от учётной записи root неправильно с точки зрения безопасности.

## 5.2 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.
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.

Более подробно о работе см. в [[1]](bib/cite.bib).

# 6 Техническое оснащение и выбранные методы проведения работы

**Техническое оснащение**

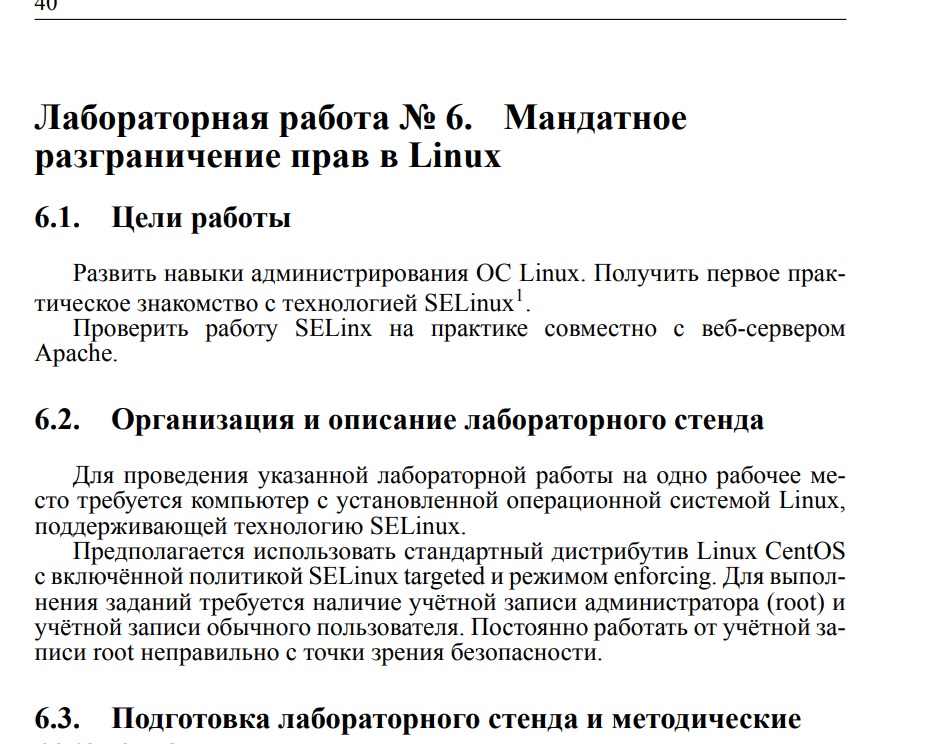
* Ноутбук
* RockyLinux
* Интернет

**Методы проведения работы**

* Изучение методической информации
* Выполнение заданий в соответствии с указаниями
* Анализ результатов
* Оветы на вопросы, заданные в задании
* Обобщение проведённой деятельности

# 7 Выполнение лабораторной работы и полученные результаты

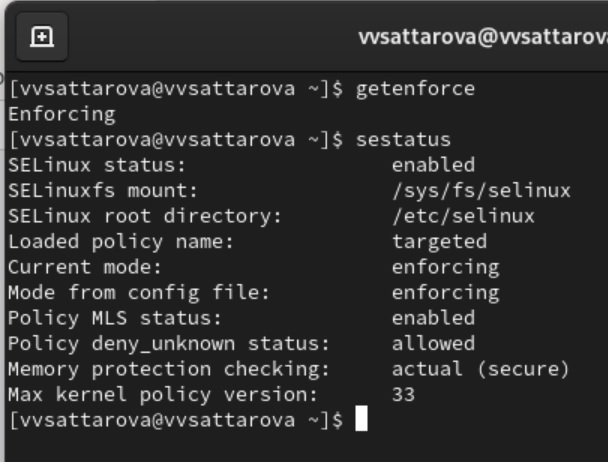
1. Скачала и ознакомилась с методическими указаниями к лабораторной работе (рис. ??).



Лабораторная работа 6

1. Выполнила следующие задания:

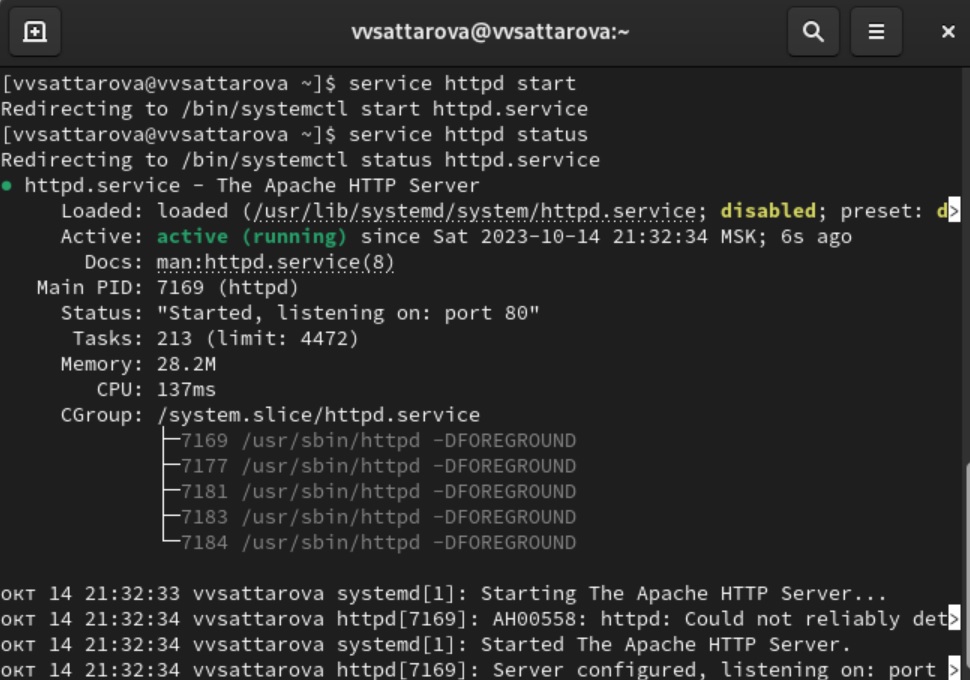
* Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus (рис. ??).



Заданиt 1

1. Выполнила следующие задания:

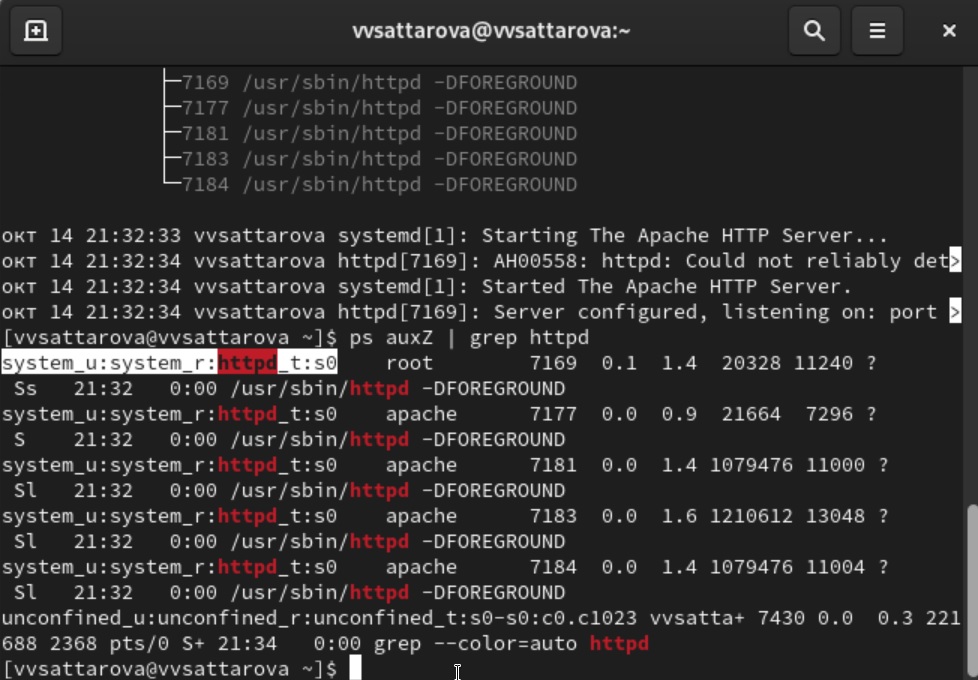
* Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: service httpd status или /etc/rc.d/init.d/httpd status Если не работает, запустите его так же, но с параметром start (рис. ??).



Заданиt 2

1. Выполнила следующие задания:

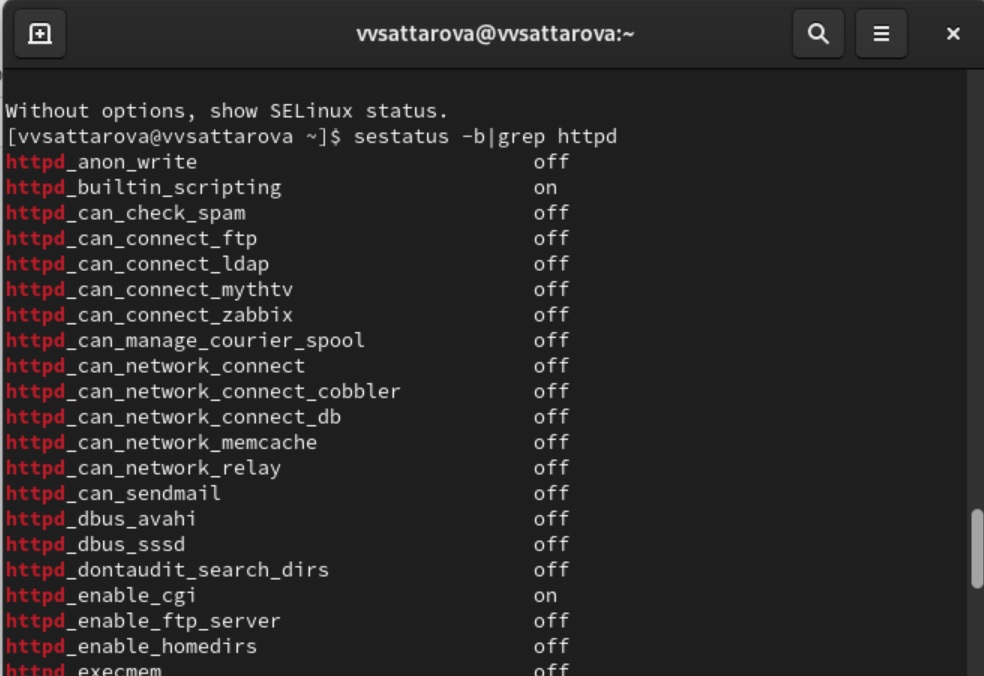
* Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду ps auxZ | grep httpd или ps -eZ | grep httpd (рис. ??).



Задание 3

1. Выполнила следующие задания:

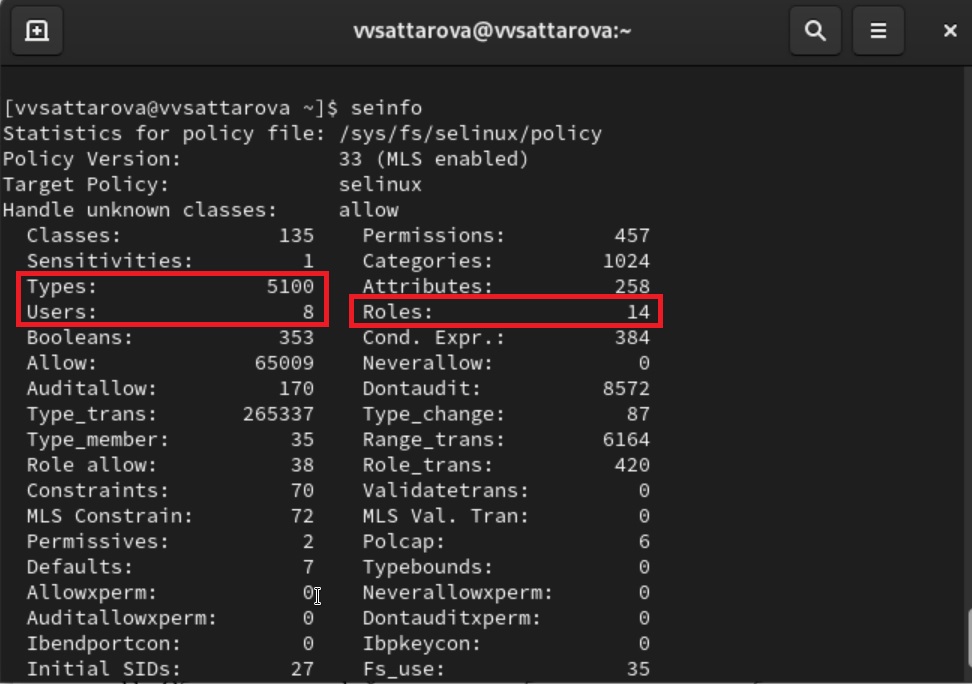
* Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды sestatus -b | grep httpd Обратите внимание, что многие из них находятся в положении «off» (рис. ??).



Задание 4

1. Выполнила следующие задания:

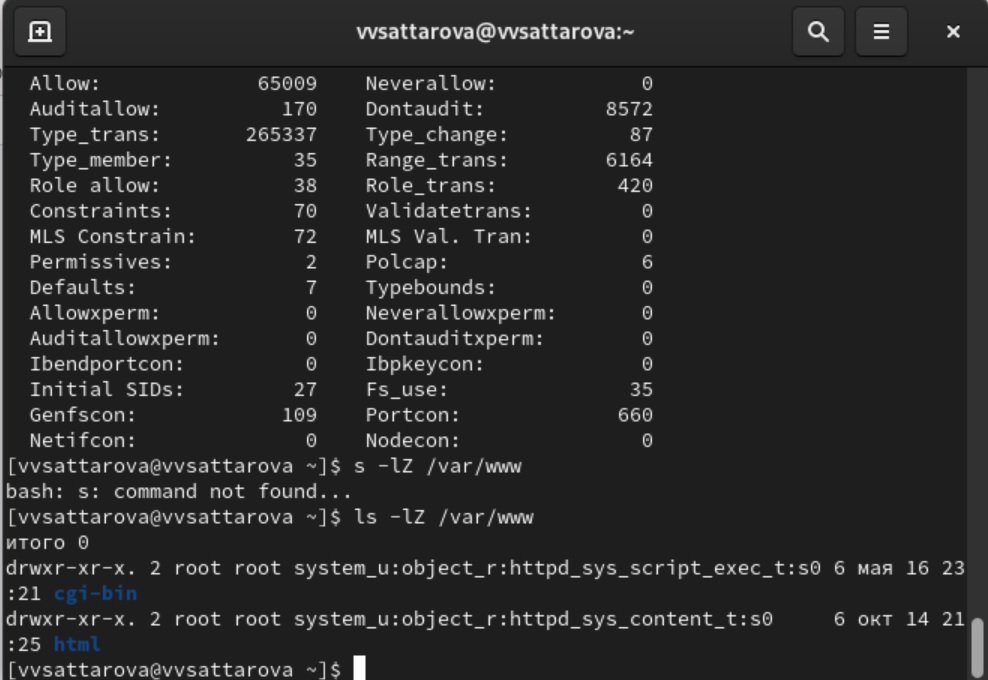
* Посмотрите статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов (рис. ??).



Задание 5

1. Выполнила следующие задания:

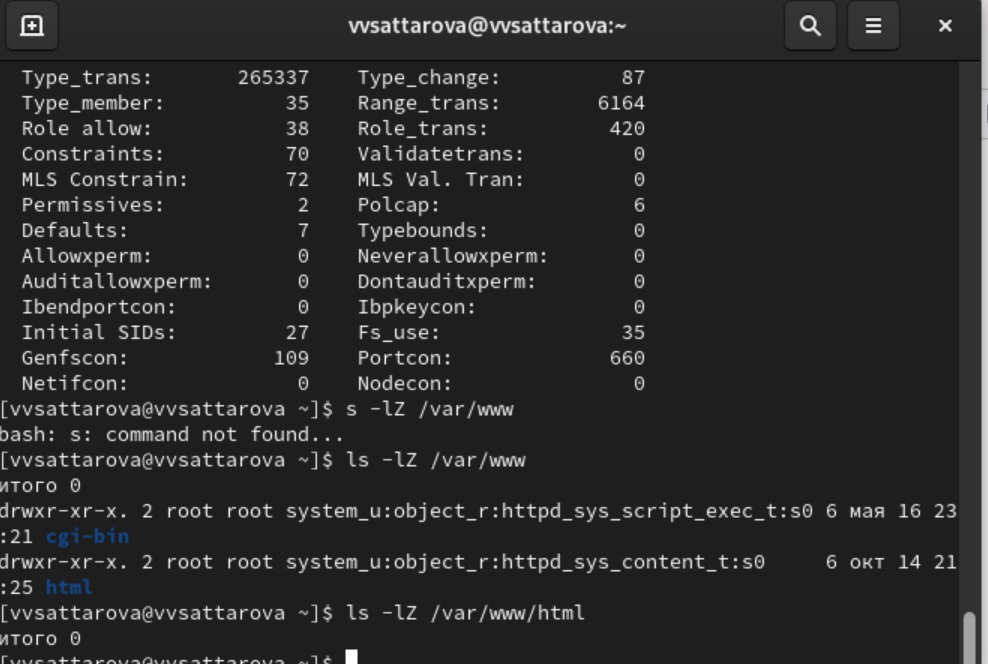
* Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www (рис. ??).



Задание 6

1. Выполнила следующие задания:

* Определите тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html
* Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html (рис. ??).



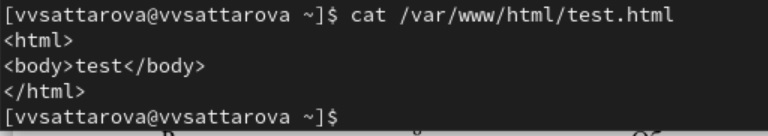
Задания 7-8

1. Выполнила следующие задания:

* 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>

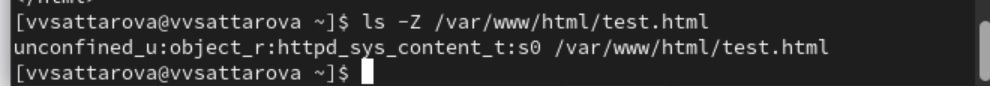
(рис. ??).



Задание 9

1. Выполнила следующие задания:

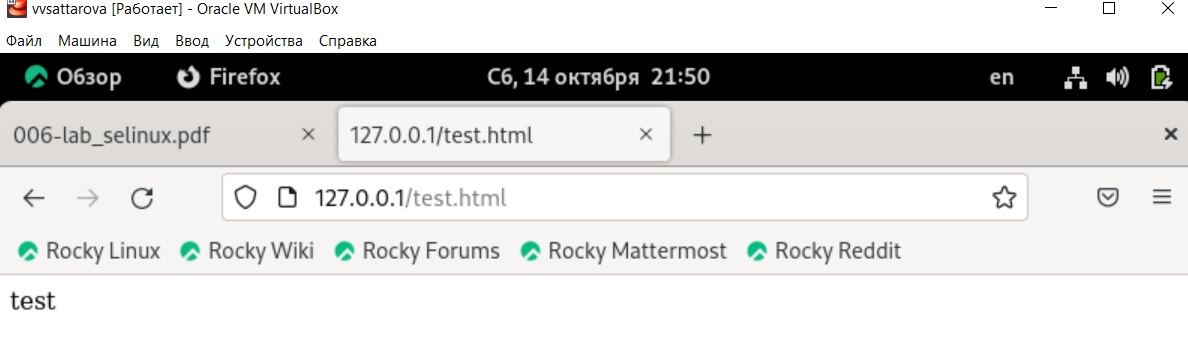
* Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html. (рис. ??).



Задание 10

1. Выполнила следующие задания:

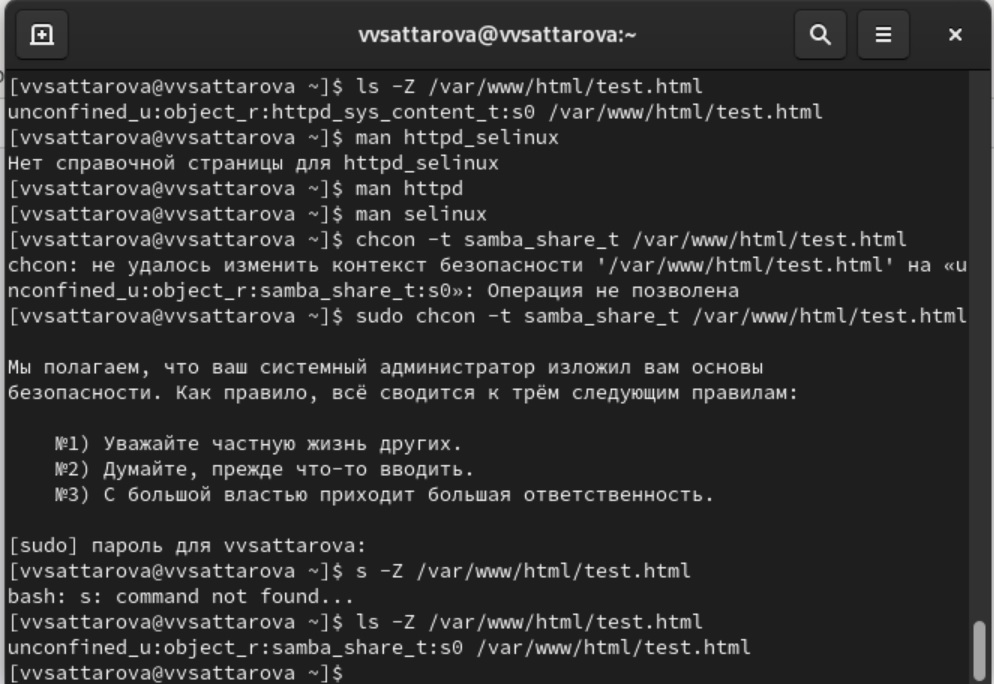
* Обратитесь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедитесь, что файл был успешно отображён (рис. ??).



Задание 11

1. Выполнила следующие задания:

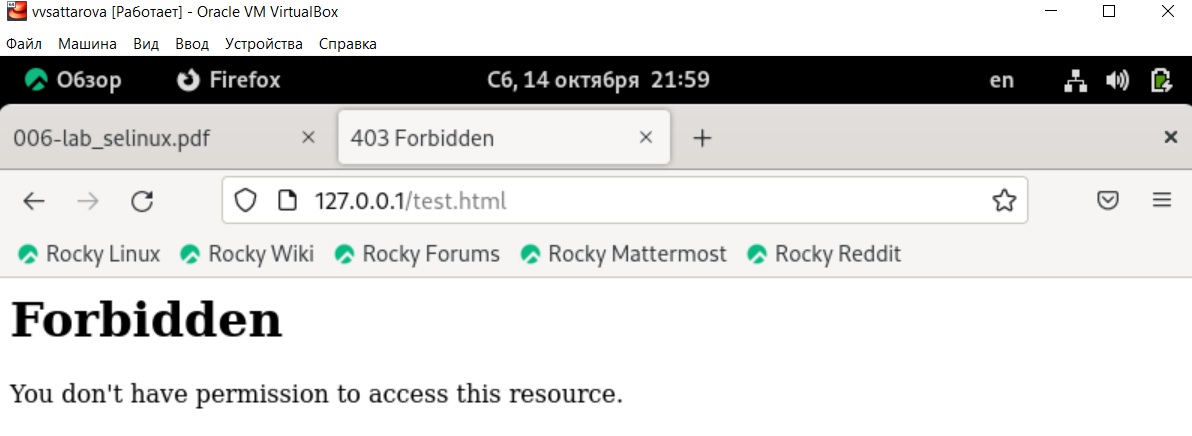
* Изучите справку man httpd\_selinux и выясните, какие контексты файлов определены для httpd. Сопоставьте их с типом файла test.html. Проверить контекст файла можно командой ls -Z. ls -Z /var/www/html/test.html
* Измените контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на любой другой, 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. ??).



Задания 12-13

1. Выполнила следующие задания:

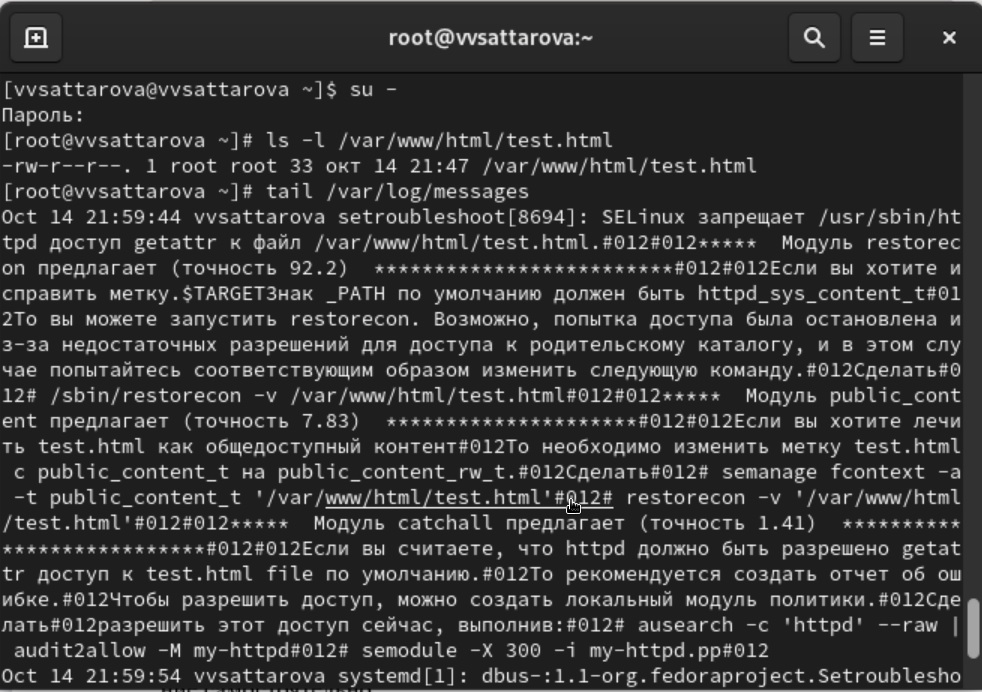
* Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Вы должны получить сообщение об ошибке (рис. ??).



Задание 14

1. Выполнила следующие задания:

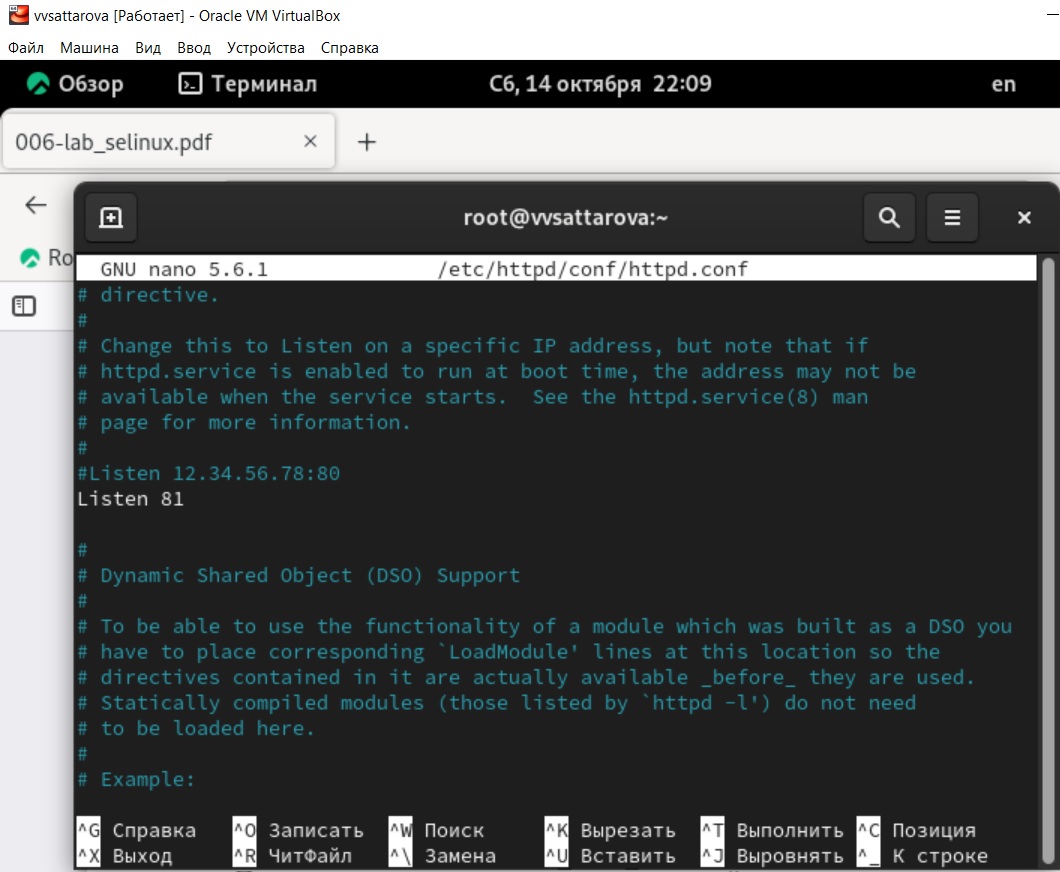
* Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? ls -l /var/www/html/test.html Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: tail /var/log/messages (рис. ??).



Задание 15

1. Выполнила следующие задания:

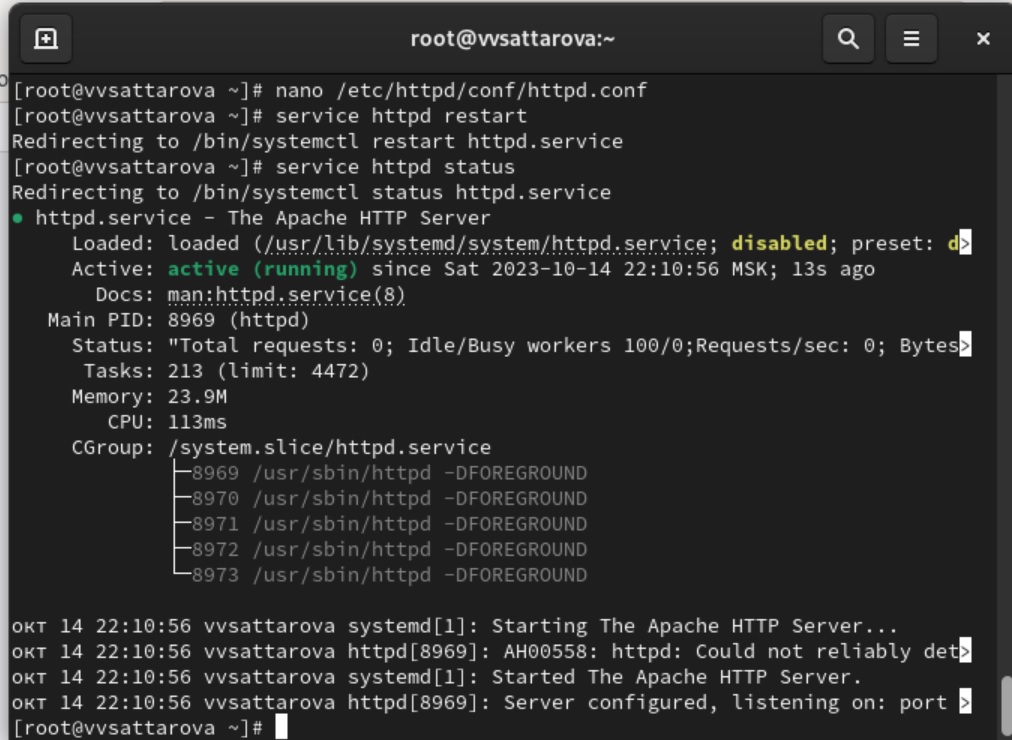
* Попробуйте запустить веб-сервер Apache на прослушивание ТСР-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf найдите строчку Listen 80 и замените её на Listen 81 (рис. ??).



Задание 16

1. Выполнила следующие задания:

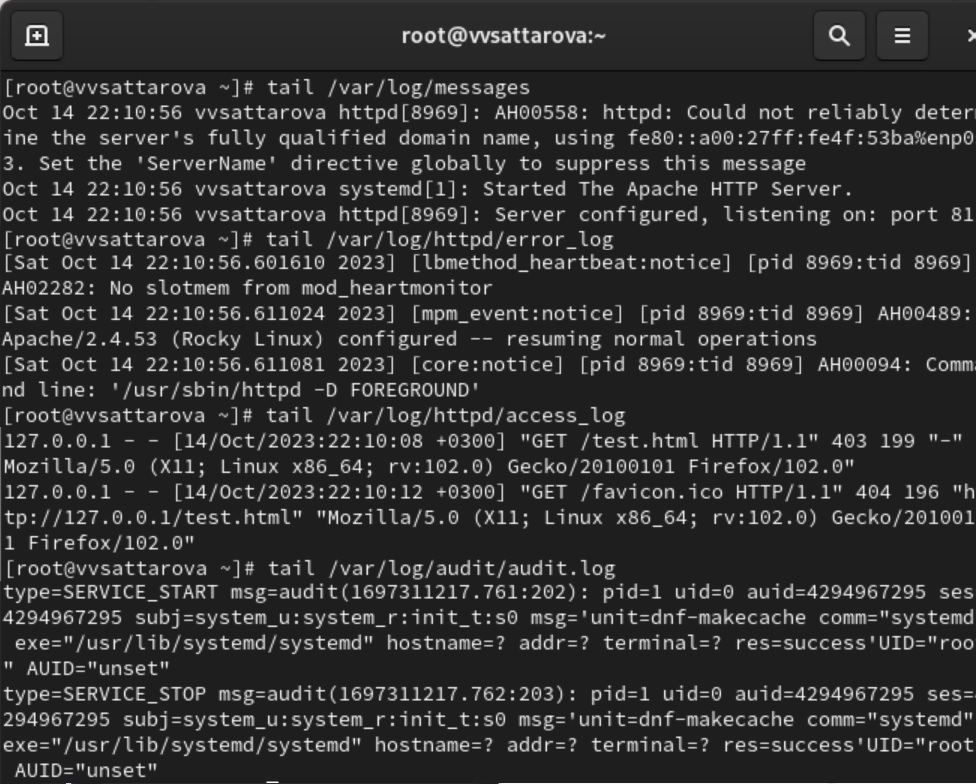
* Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему? (рис. ??).



Задание 17

1. Выполнила следующие задания:

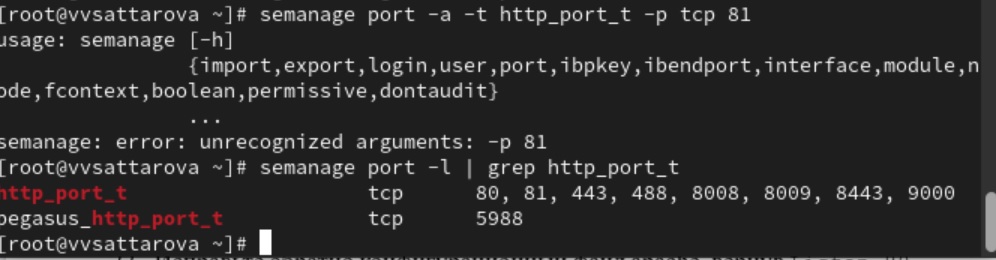
* Проанализируйте лог-файлы: tail -nl /var/log/messages. Просмотрите файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log и выясните, в каких файлах появились записи (рис. ??).



Задание 18

1. Выполнила следующие задания:

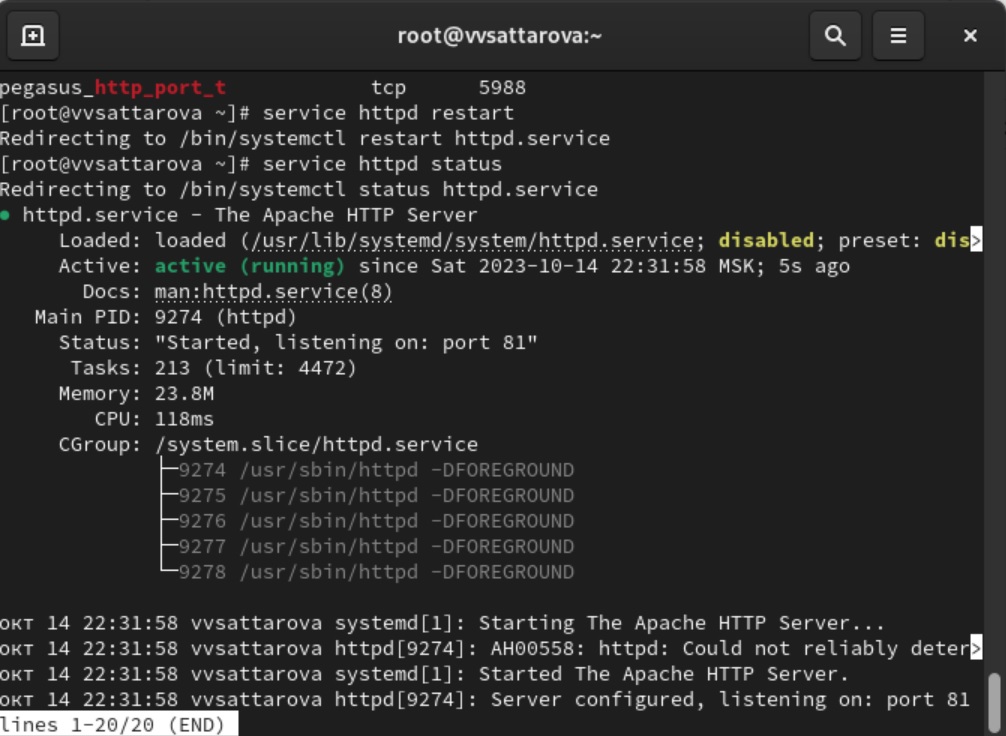
* Выполните команду semanage port -a -t http\_port\_t -р tcp 81 После этого проверьте список портов командой semanage port -l | grep http\_port\_t Убедитесь, что порт 81 появился в списке (рис. ??).



Задание 19

1. Выполнила следующие задания:

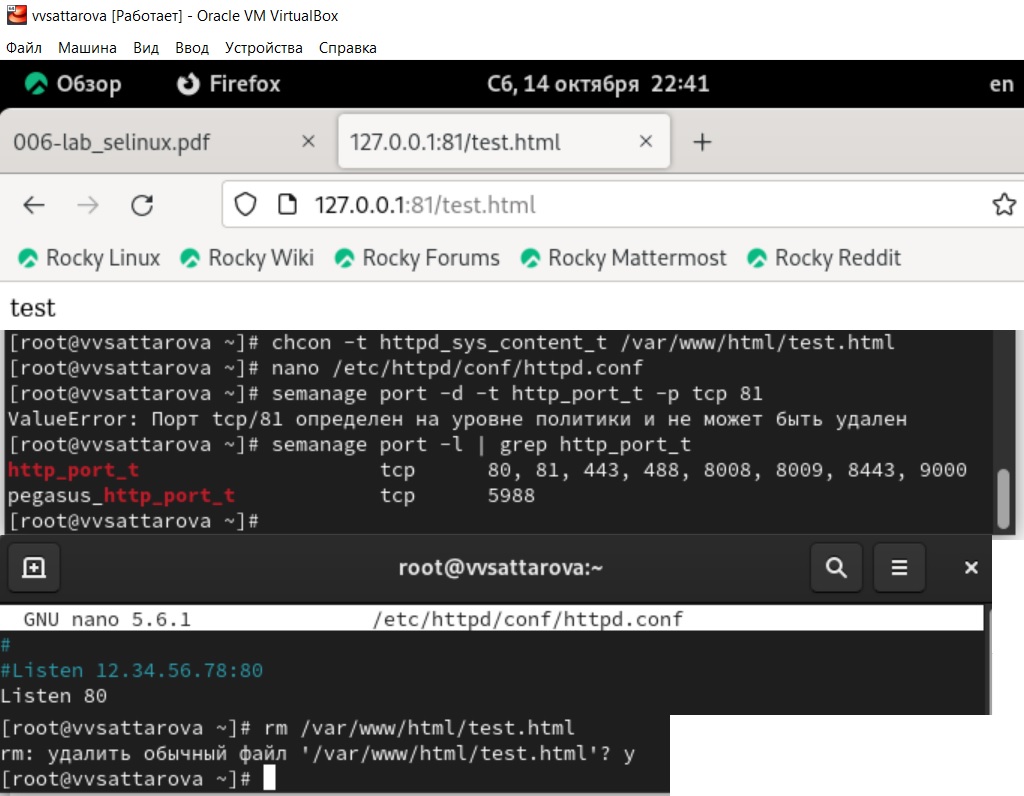
* Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему он сейчас запустился, а в предыдущем случае не смог? (рис. ??).



Задание 20

1. Выполнила следующие задания:

* 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».
* Исправьте обратно конфигурационный файл apache, вернув Listen 80.
* Удалите привязку http\_port\_t к 81 порту: semanage port -d -t http\_port\_t -p tcp 81 и проверьте, что порт 81 удалён.
* Удалите файл /var/www/html/test.html: rm /var/www/html/test.html (рис. ??).



Задания 21-24

# 8 Анализ результатов

Таким образом, были выаолнены задания по изучению администрирования, SELinux, веб-сервера Apache.

# 9 Заключение и выводы

Таким образом, в ходе выполнения лабораторной работы было сделано следующее:

* Развиты навыки администрирования ОС Linux.
* Получено первое практическое знакомство с технологией SELinux.
* Проверена работа SELinx на практике совместно с веб-сервером Apache.
* Написан отчёт к лабораторной работе.

# 10 Список литературы

[[1]](bib/cite.bib)

1. Информационная безопасность [Электронный ресурс]. Российский университет дружбы народов, 2023. URL: <https://esystem.rudn.ru/pluginfile.php/2090282/mod_resource/content/2/006-lab_selinux.pdf>.