Лабораторная работа №6

Мандатное разграничение прав в Linux

Шагабаев Давид, НПИбд-02-18"

Содержание

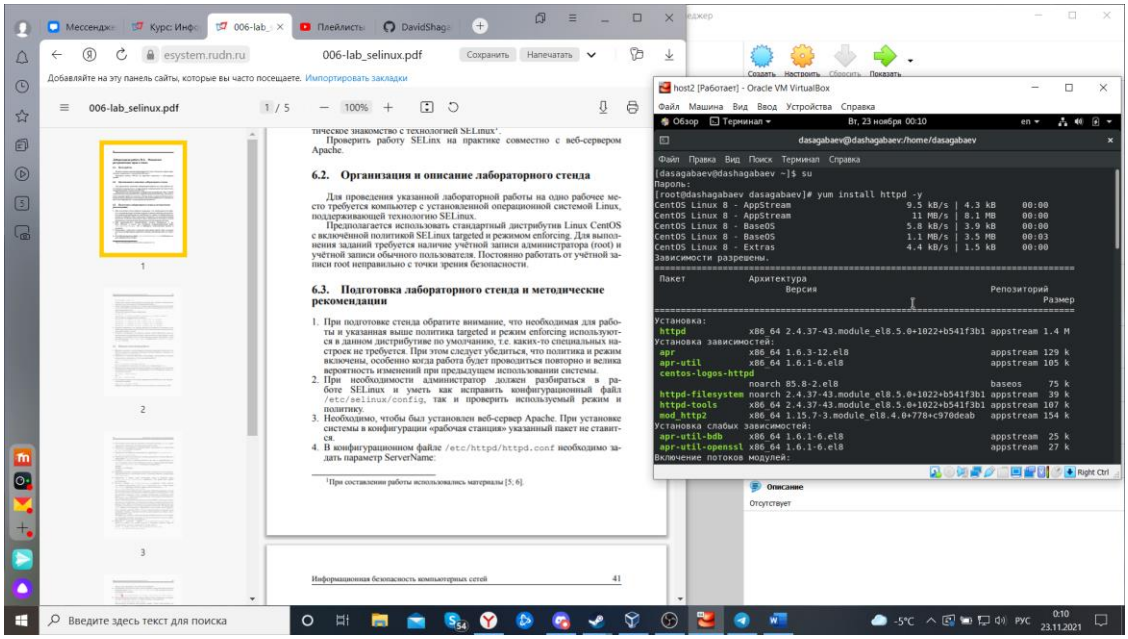
Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1 . Проверить работу SELinx на практике совместно с веб-сервером Apache.

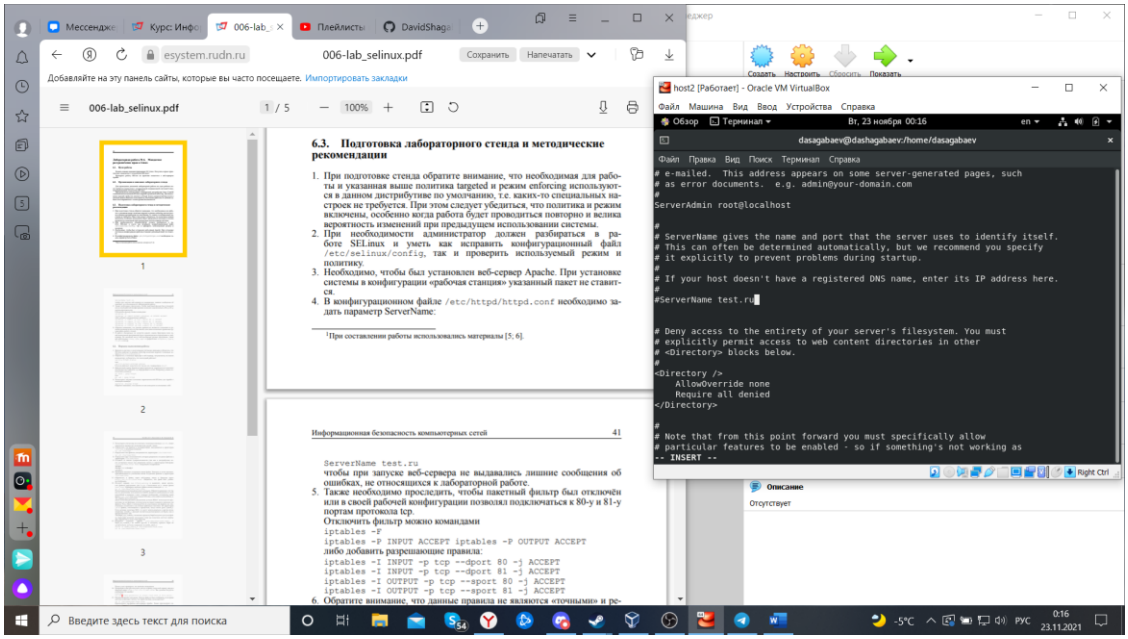
Выполнение лабораторной работы

1. Установка Apache командой

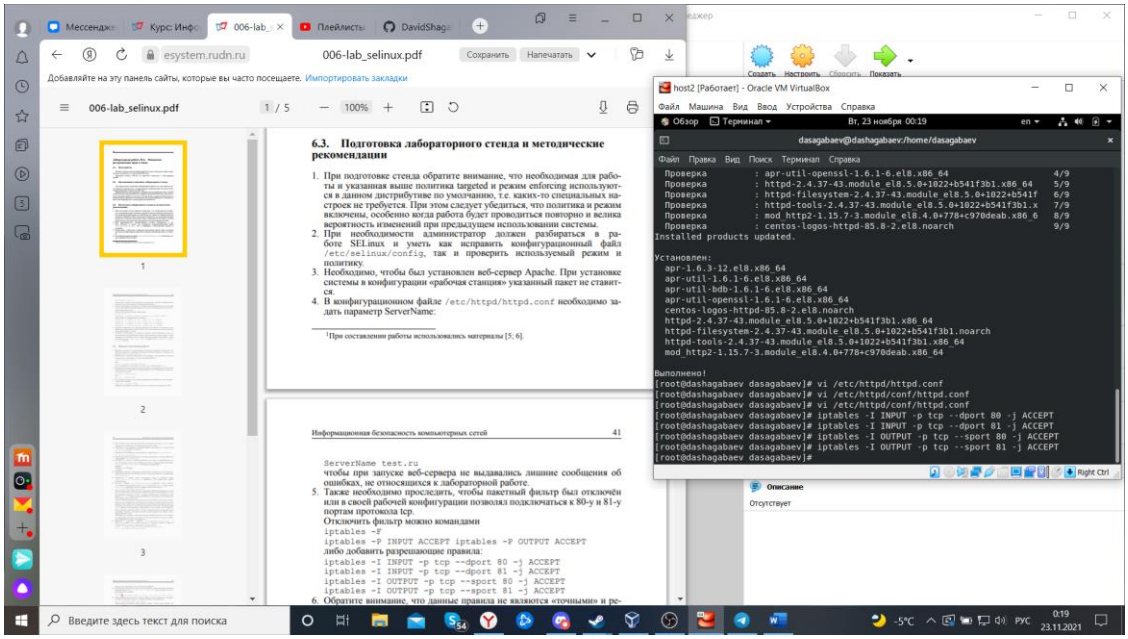
   yum install httpd -y



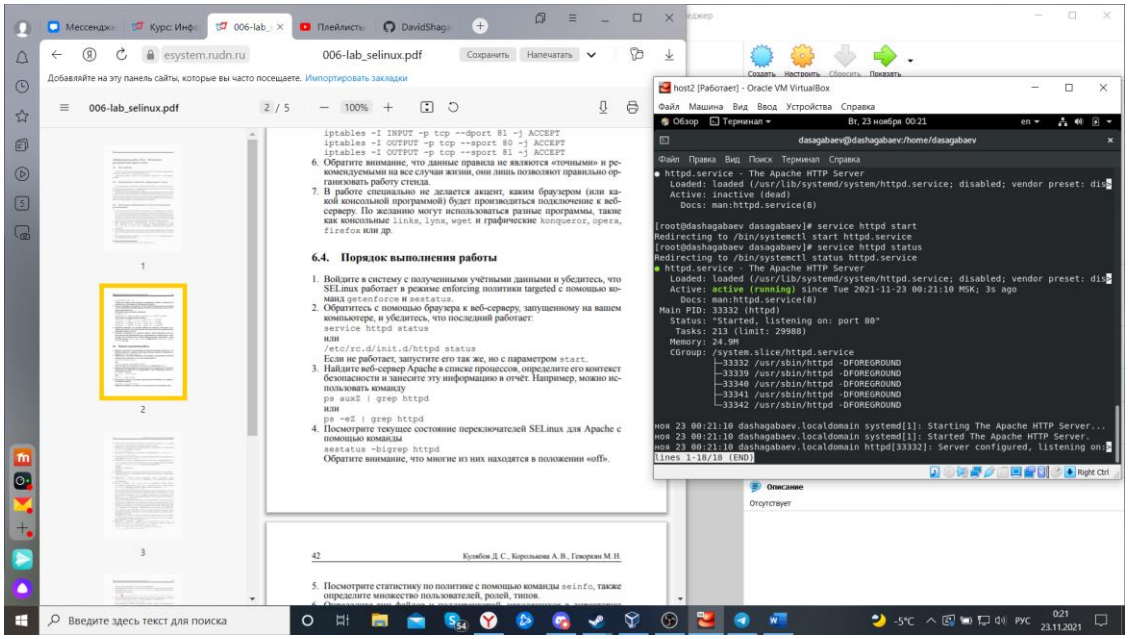
2. В конфигурационном файле /etc/httpd/httpd.conf необходимо задать параметр ServerName: ServerName test.ru



3. Также необходимо проследить, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp.

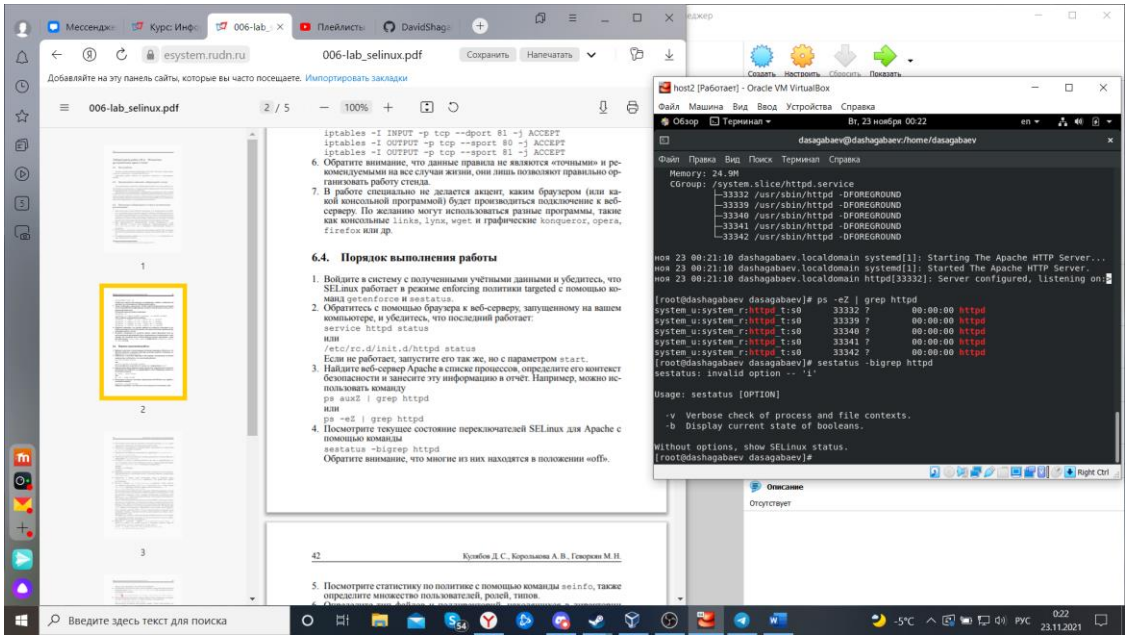


4. Запуск и проверка сервера.

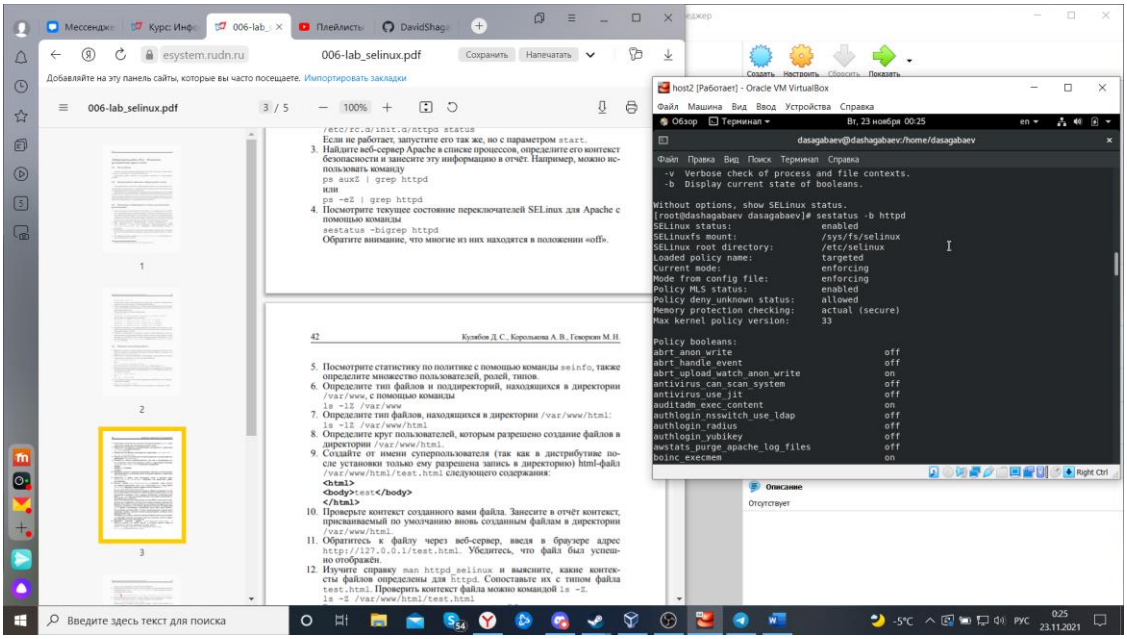


5. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду

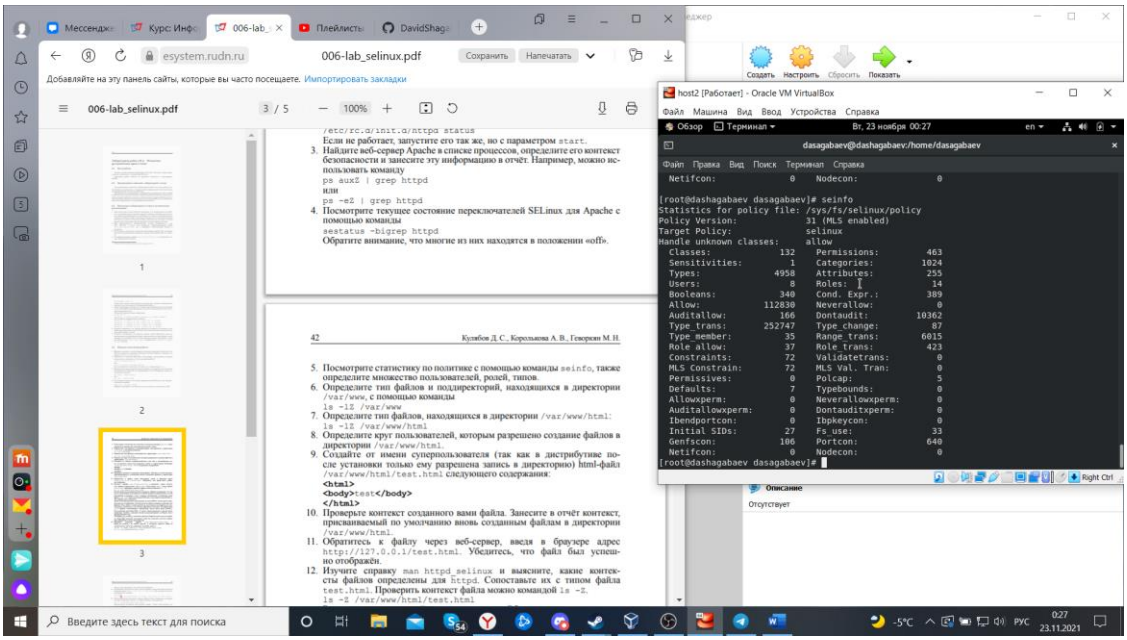
   ps -eZ | grep httpd



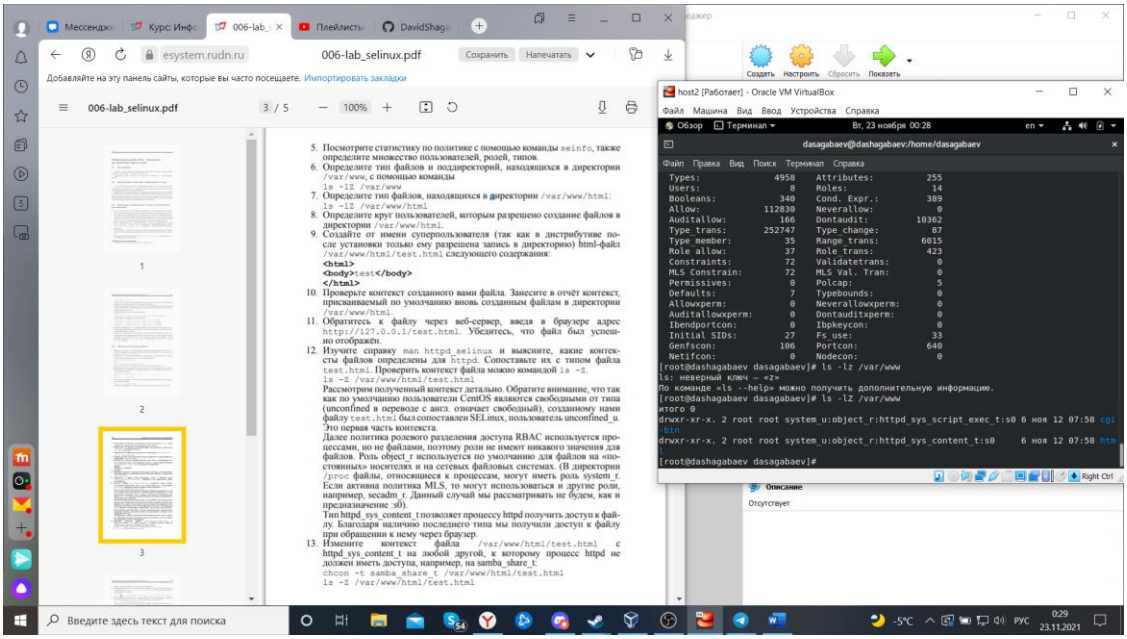
1. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды sestatus -bigrep httpd



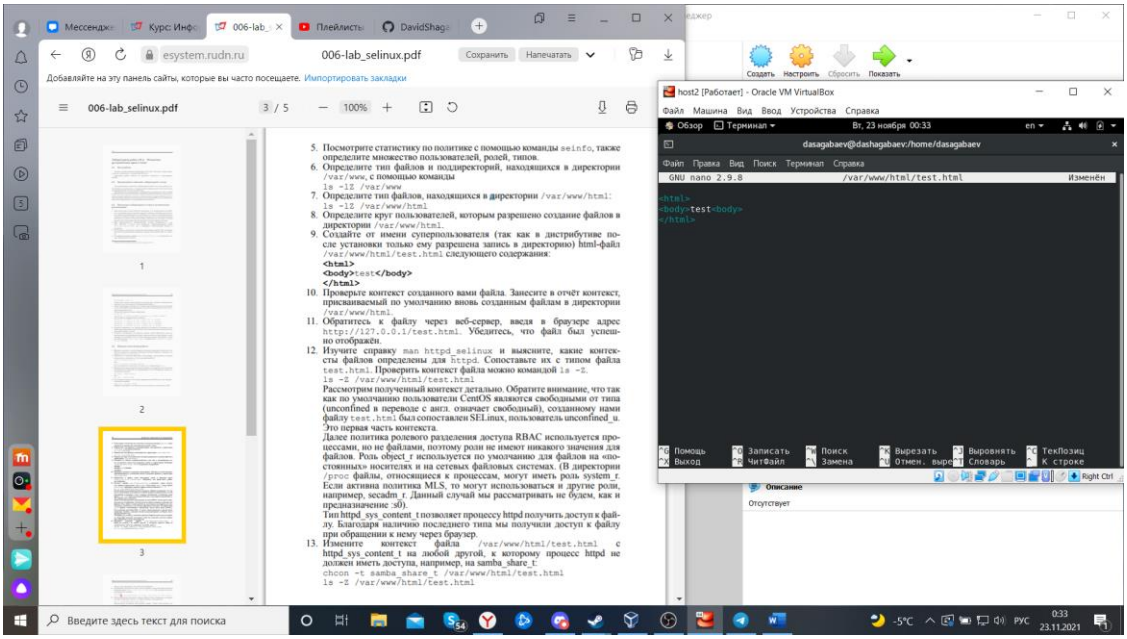
1. Посмотрите статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов.



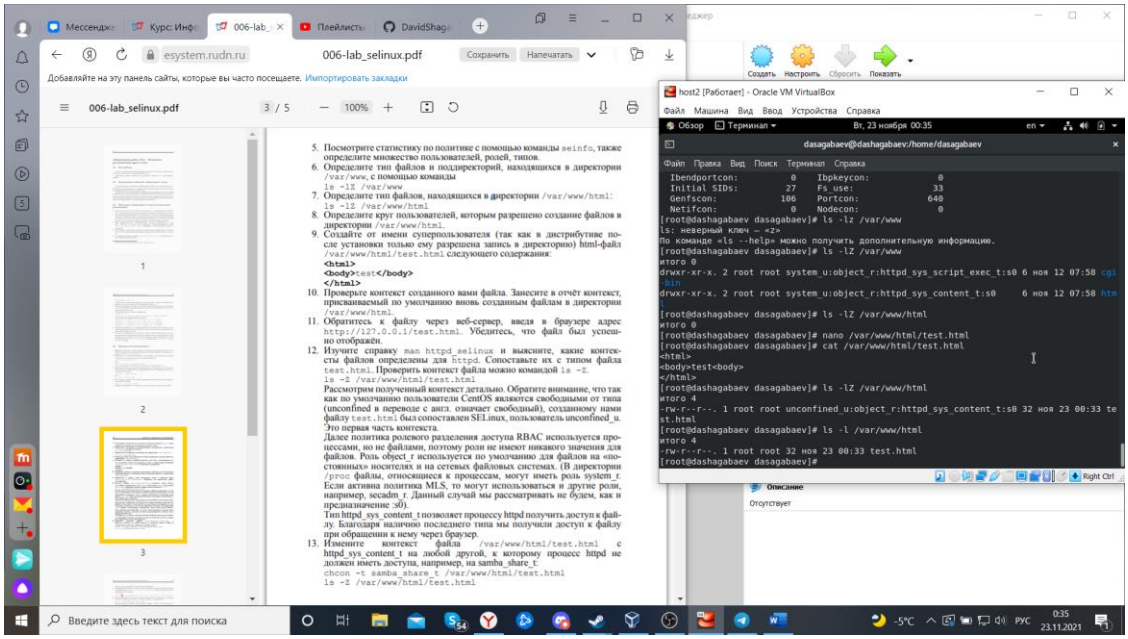
1. Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www



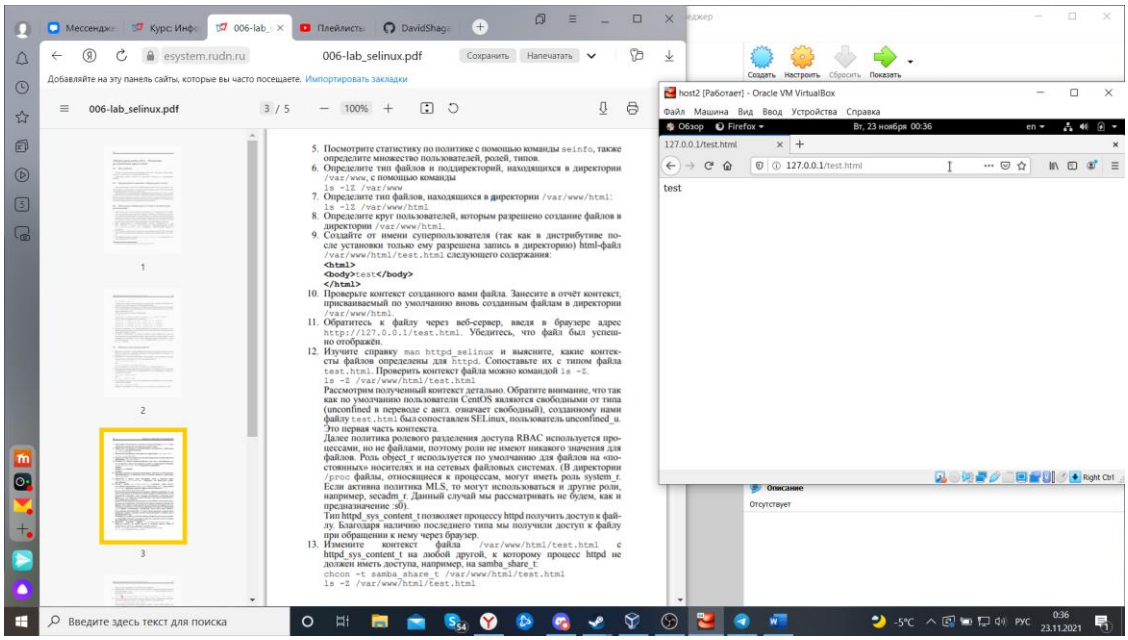
1. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания



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



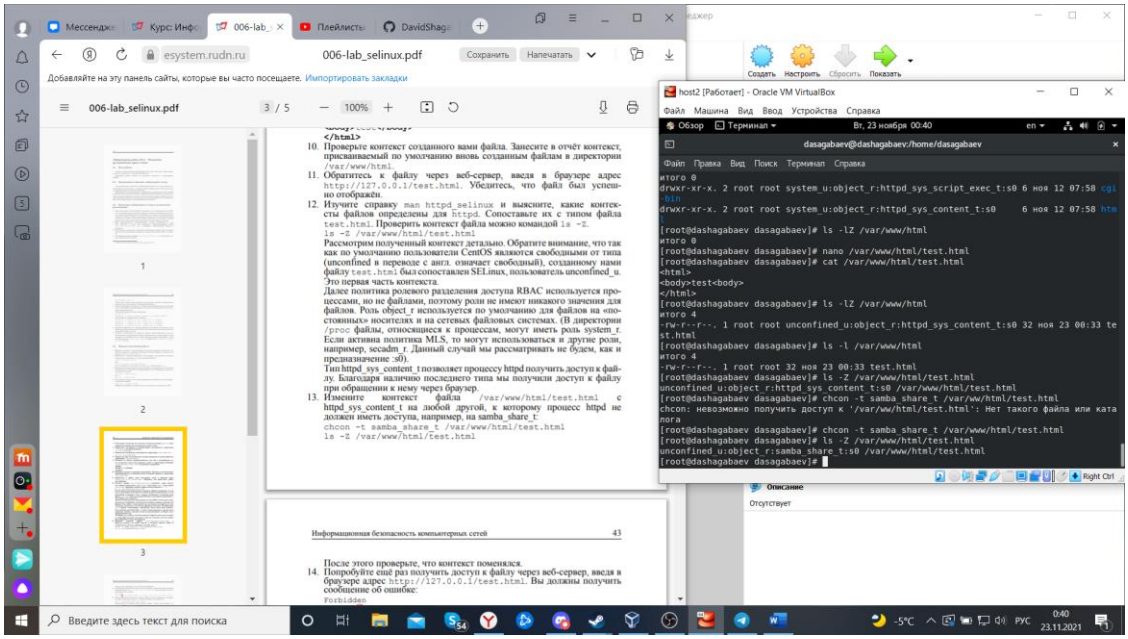
1. Обратитесь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедитесь, что файл был успешно отображён



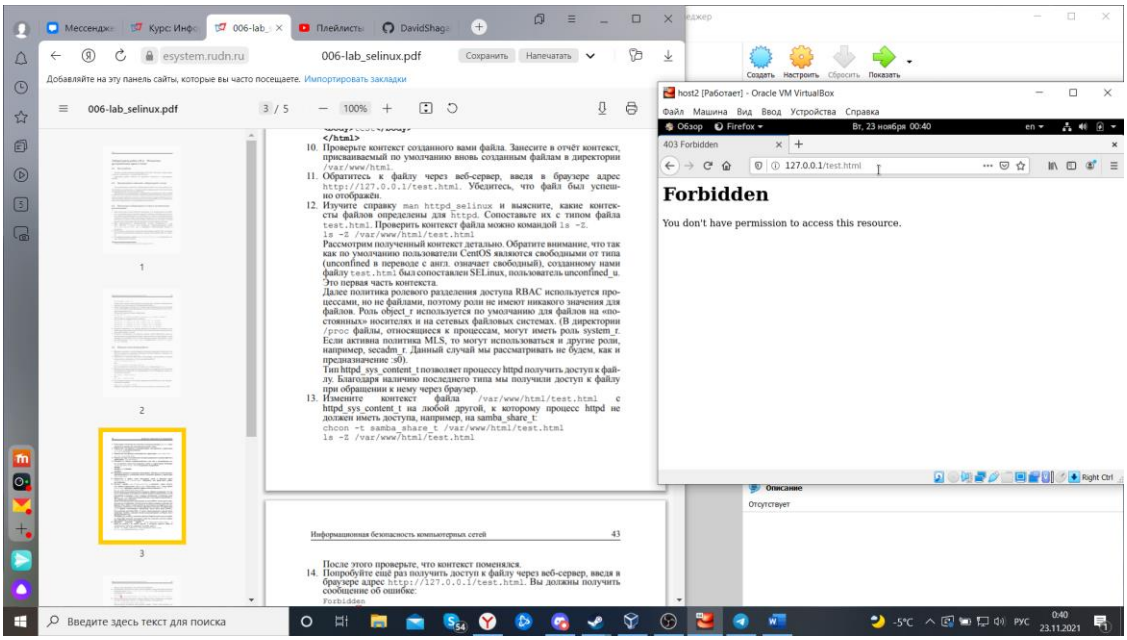
1. Изучите справку man httpd_selinux и выясните, какие контексты файлов определены для httpd. Сопоставьте их с типом файла test.html. Проверить контекст файла можно командой ls -Z. ls -Z /var/www/html/test.html

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

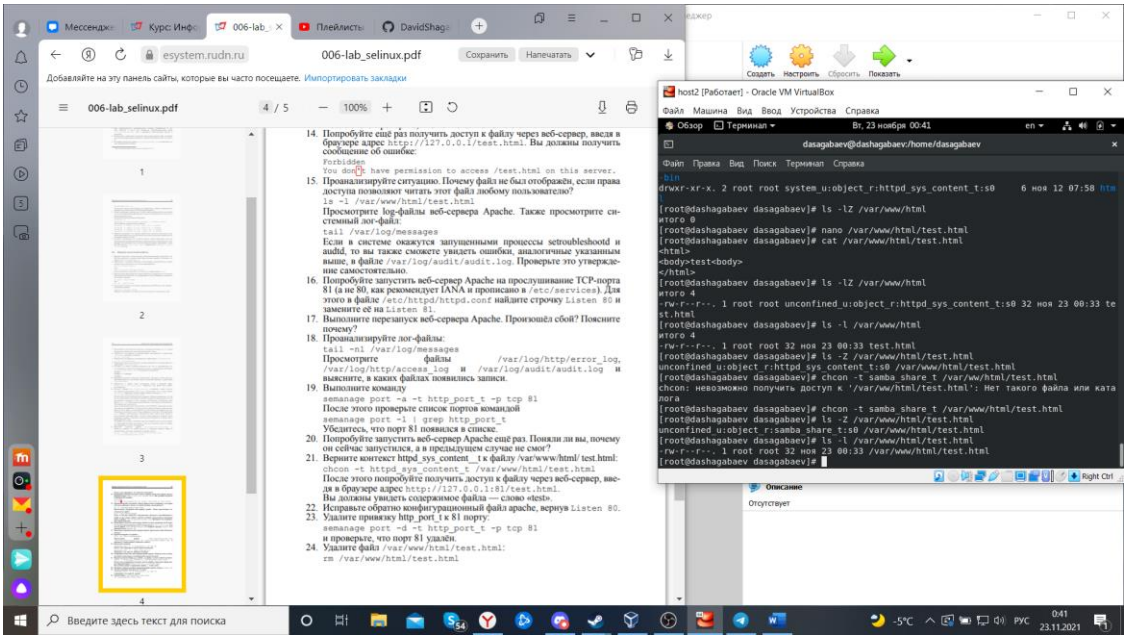
ls -Z /var/www/html/test.html



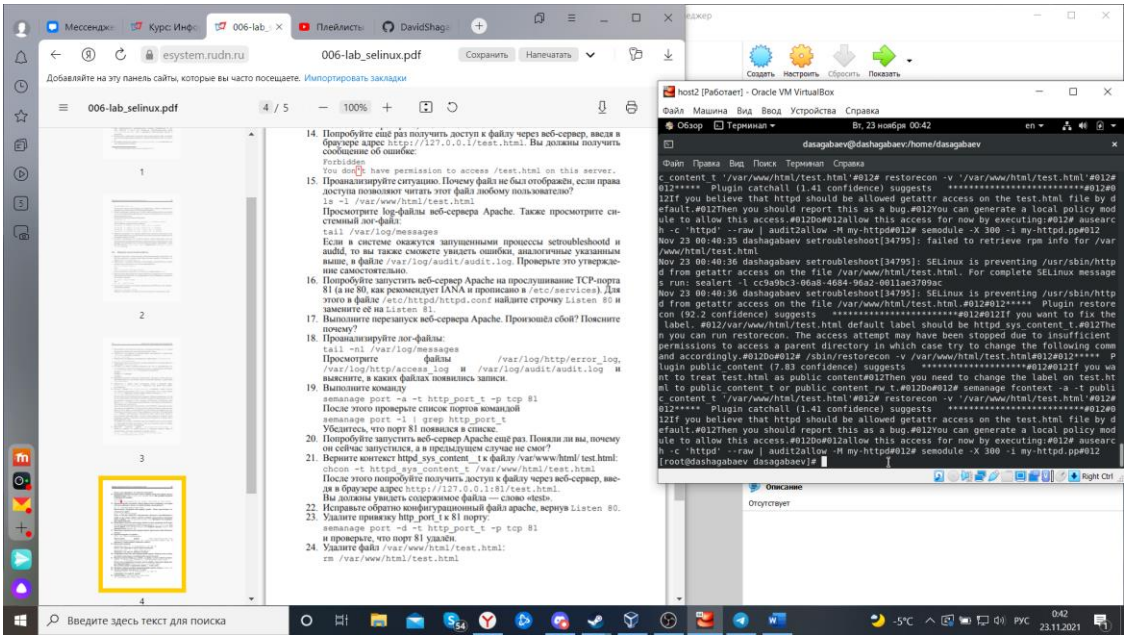
1. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Вы должны получить сообщение об ошибке



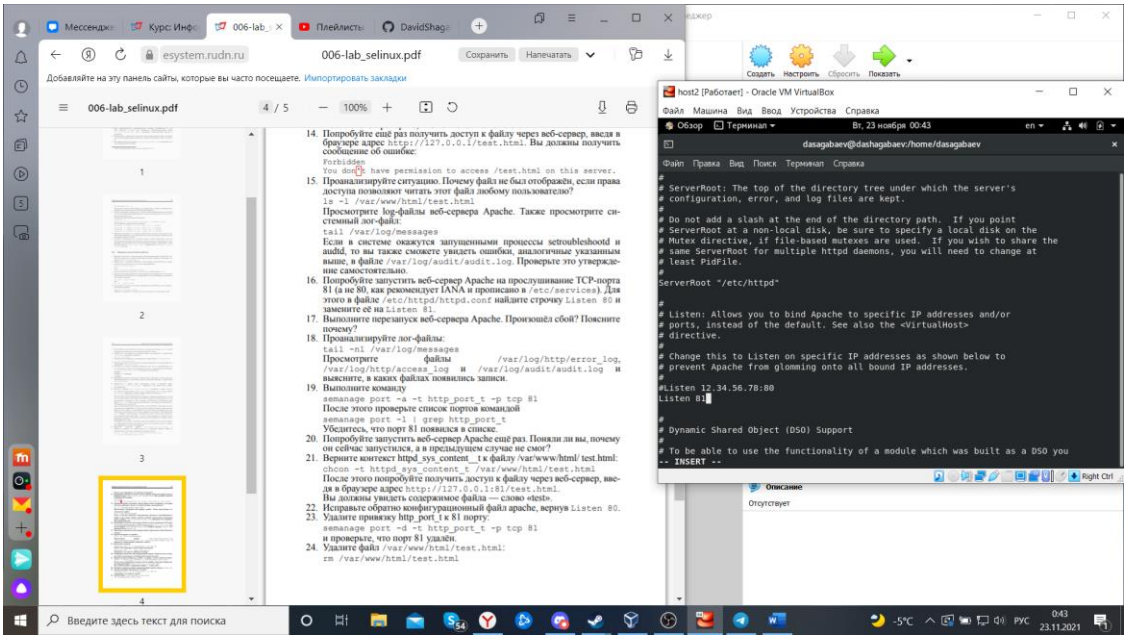
1. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? ls -l /var/www/html/test.html



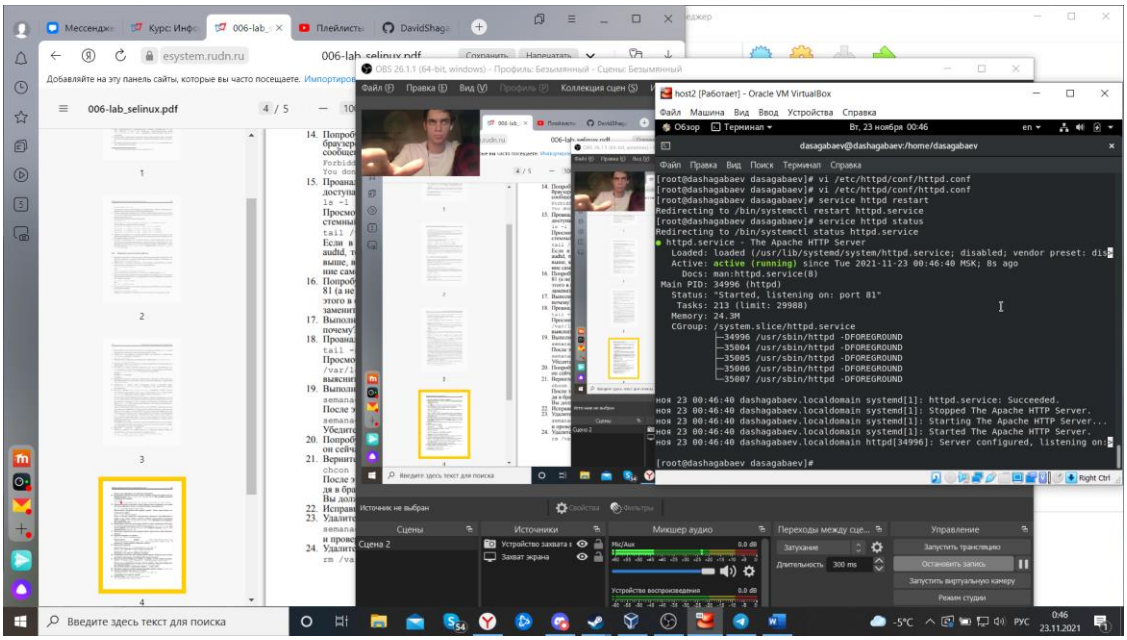
Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл:

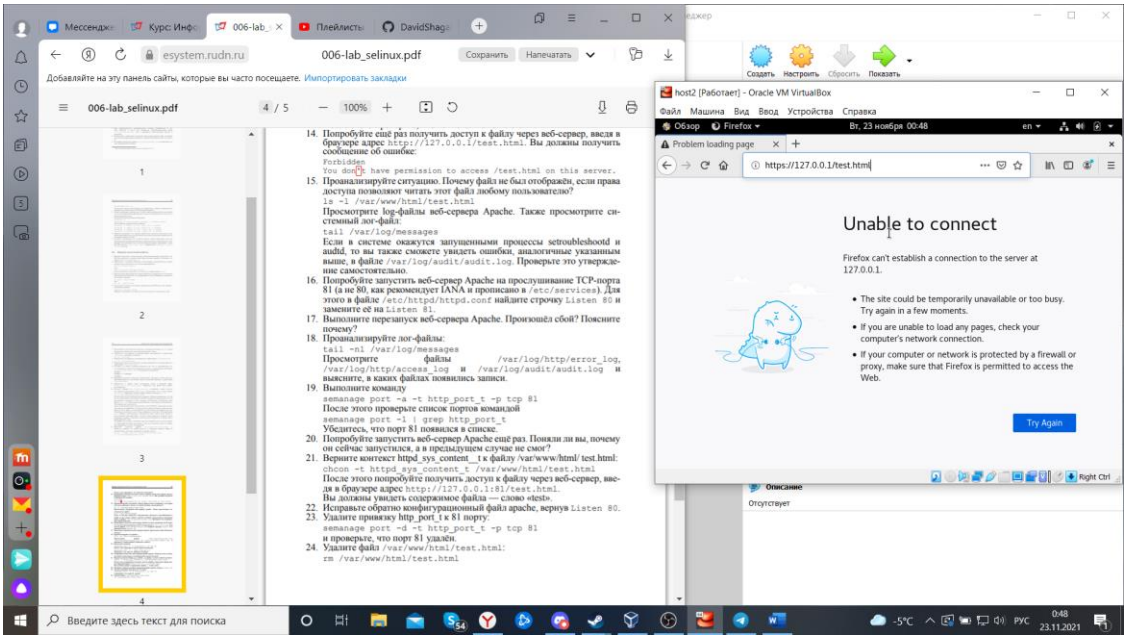


1. Попробуйте запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf найдите строчку Listen 80 и замените её на Listen 81.

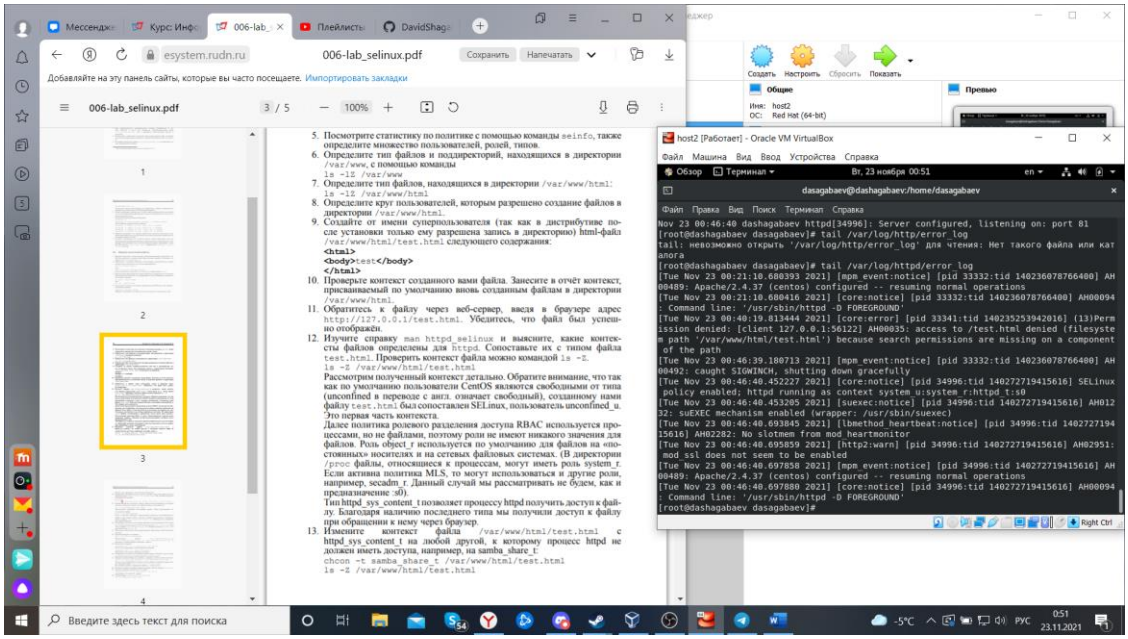


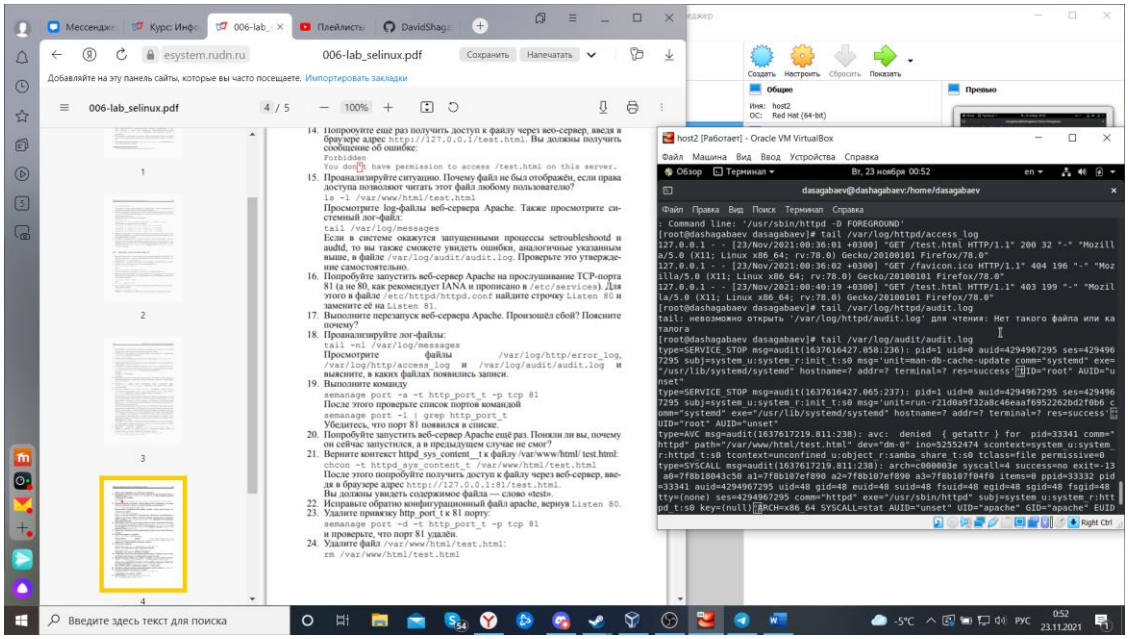
1. Выполните перезапуск веб-сервера Apache.

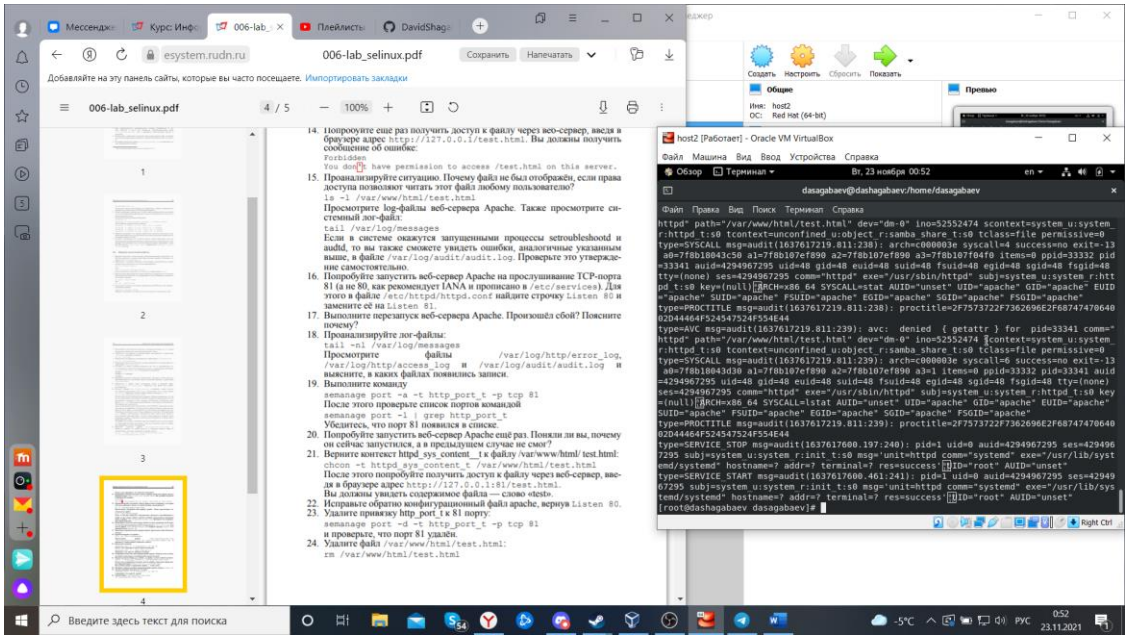




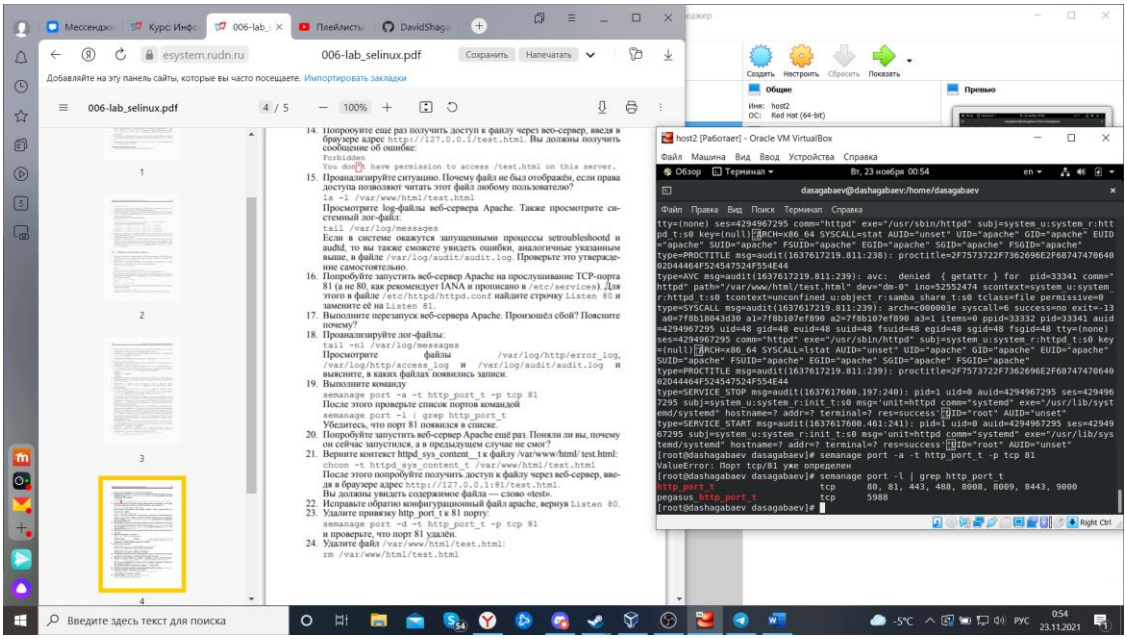
1. Проанализируйте лог-файлы: tail -nl /var/log/messages Просмотрите файлы /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log и выясните, в каких файлах появились записи.





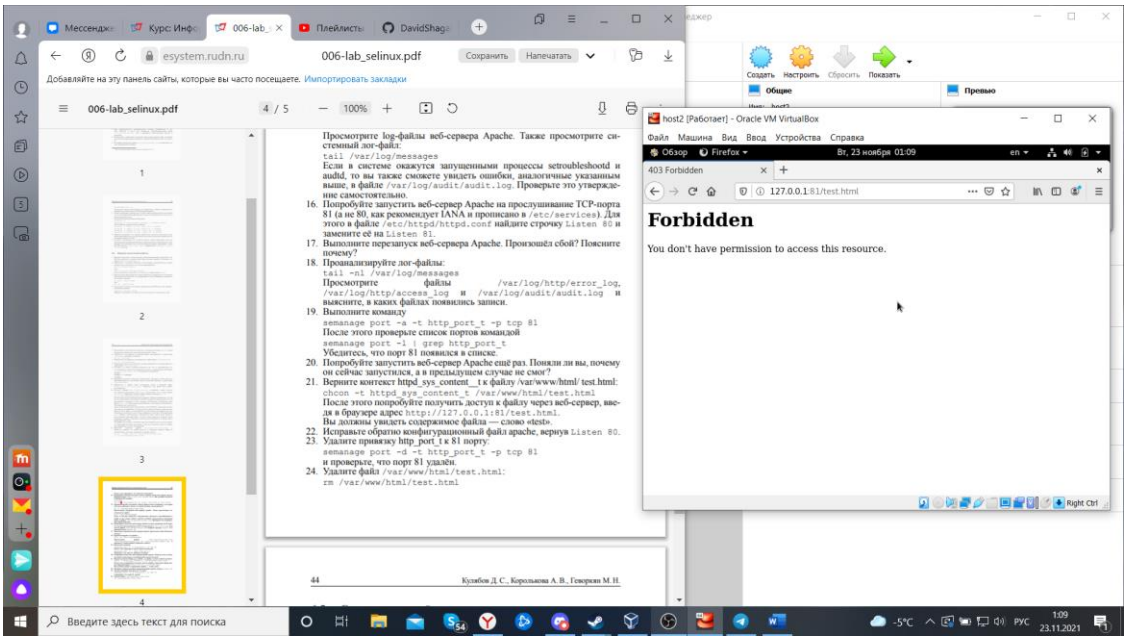


1. Выполните команду semanage port -a -t http_port_t -p tcp 81 После этого проверьте список портов командой semanage port -l | grep http_port_t Убедитесь, что порт 81 появился в списке.

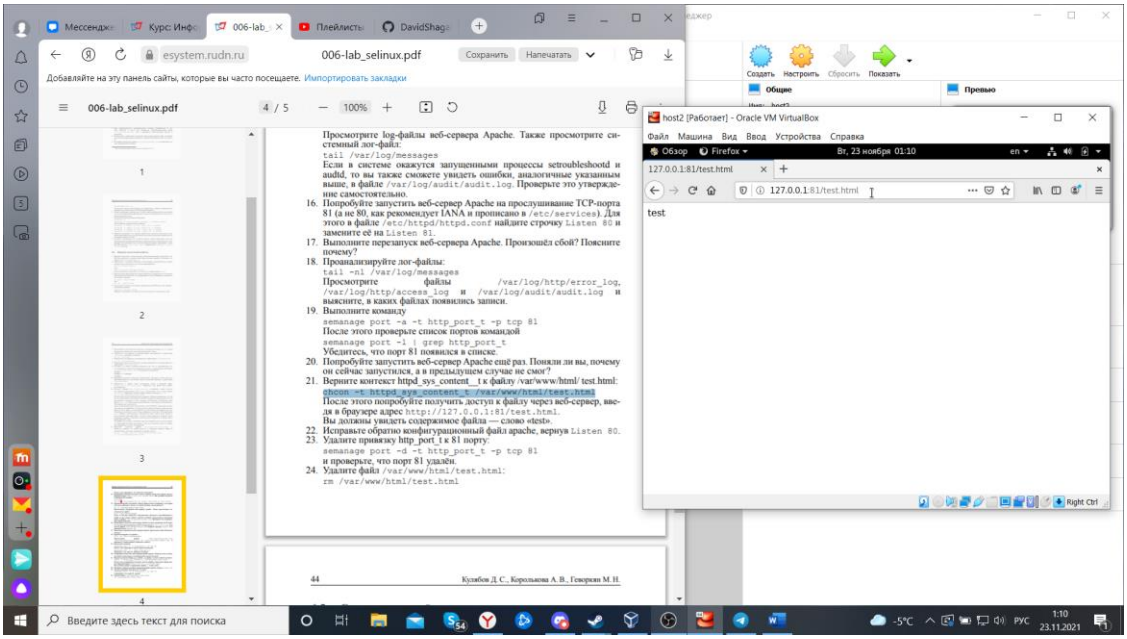


1. Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему он сейчас запустился, а в предыдущем случае не смог?

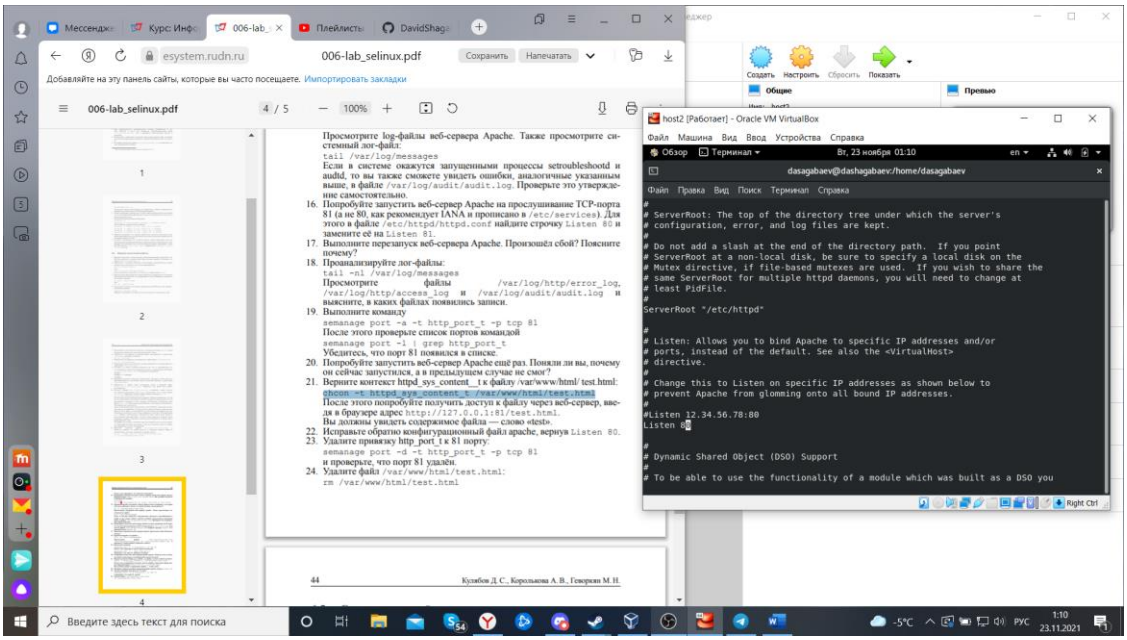
   мы добавили 81 порт, поэтому сейчас всё сработало.



1. . Верните контекст httpd_sys_content__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».

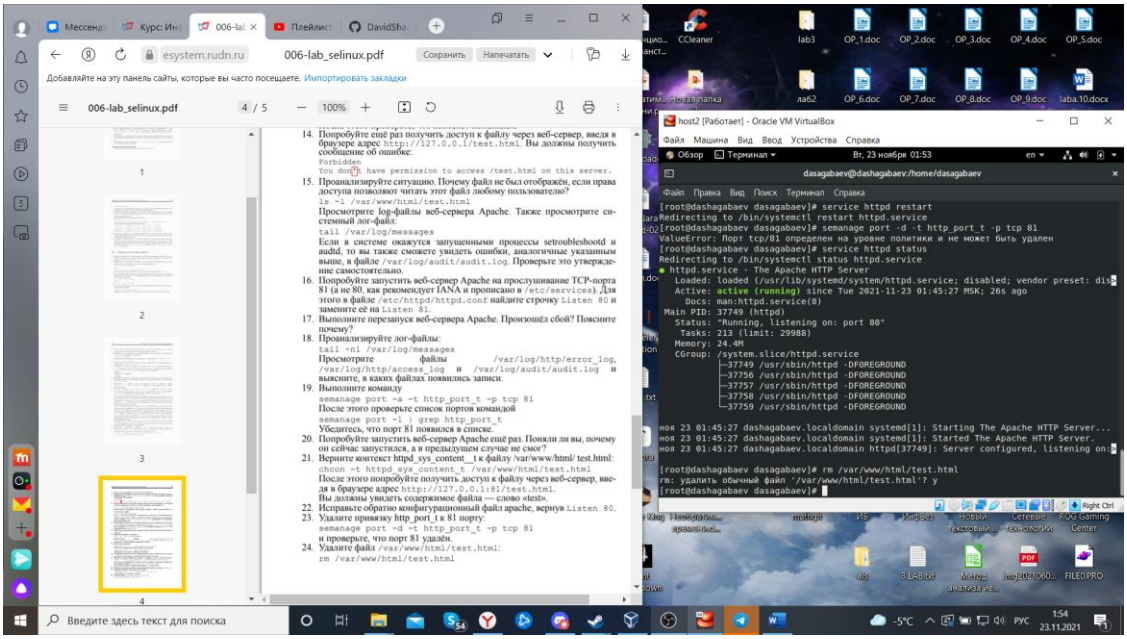


1. Исправьте обратно конфигурационный файл apache, вернув Listen 80.



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.

2. Удалите файл /var/www/html/test.html: rm /var/www/html/test.html



Выводы

Развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux1 . Проверили работу SELinx на практике совместно с веб-сервером Apache.