**ОТЧЕТ**

По дисциплине: Информационная безопасность.

Лабораторная работа № 6. Мандатное разграничение прав в Linux.

Нгуен Чау Ки Ань

1032185287

НБИбд-01-18

6.1. Цели работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1.

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

6.2. 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.

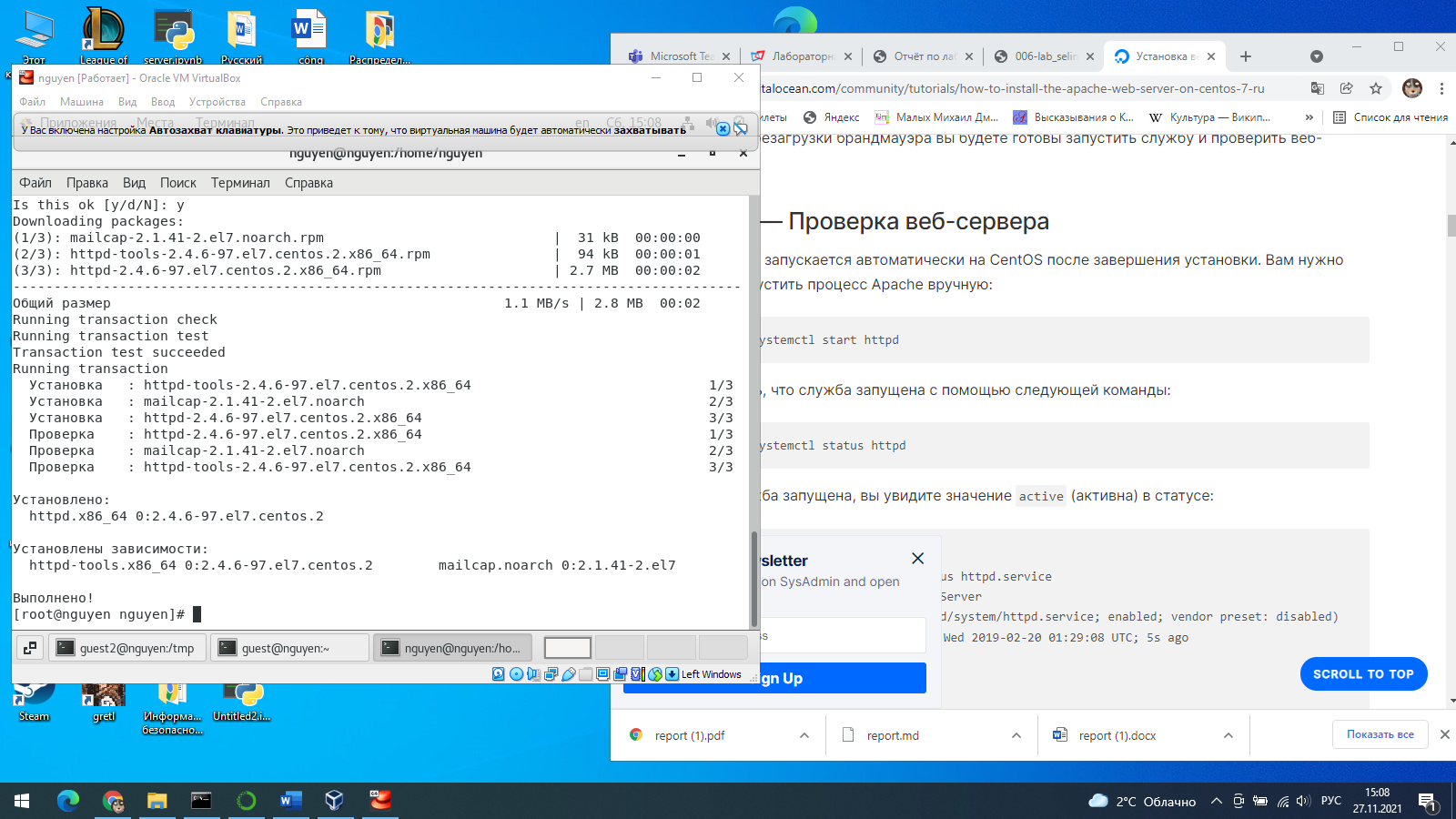


Figure 1: подготовка к задаче

4. В конфигурационном файле /etc/httpd/httpd.conf необходимо задать параметр ServerName:

1При составлении работы использовались материалы [5; 6].

ServerName test.ru

чтобы при запуске веб-сервера не выдавались лишние сообщения об

ошибках, не относящихся к лабораторной работе.

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.

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.

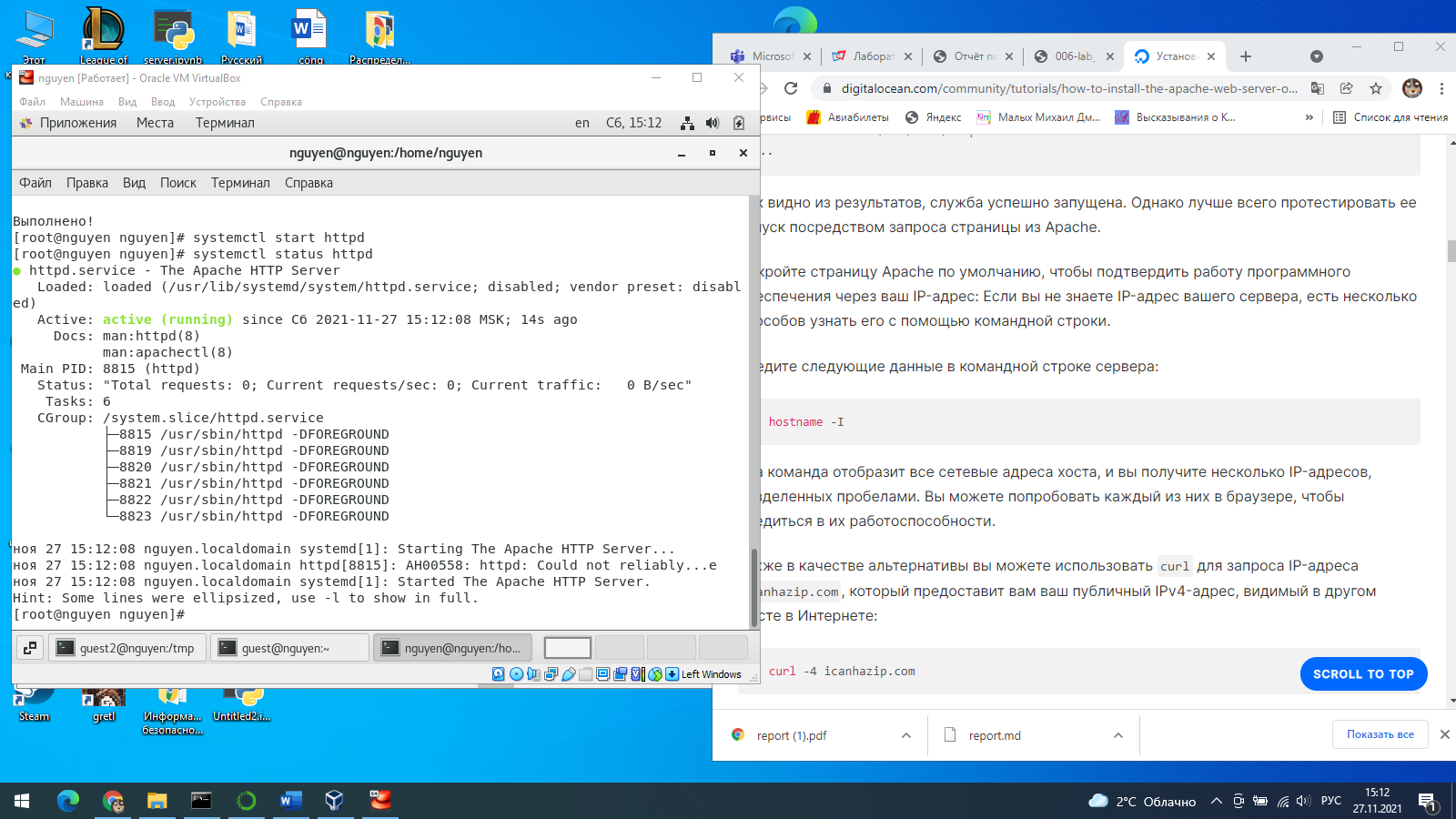


Figure 2: запуск http

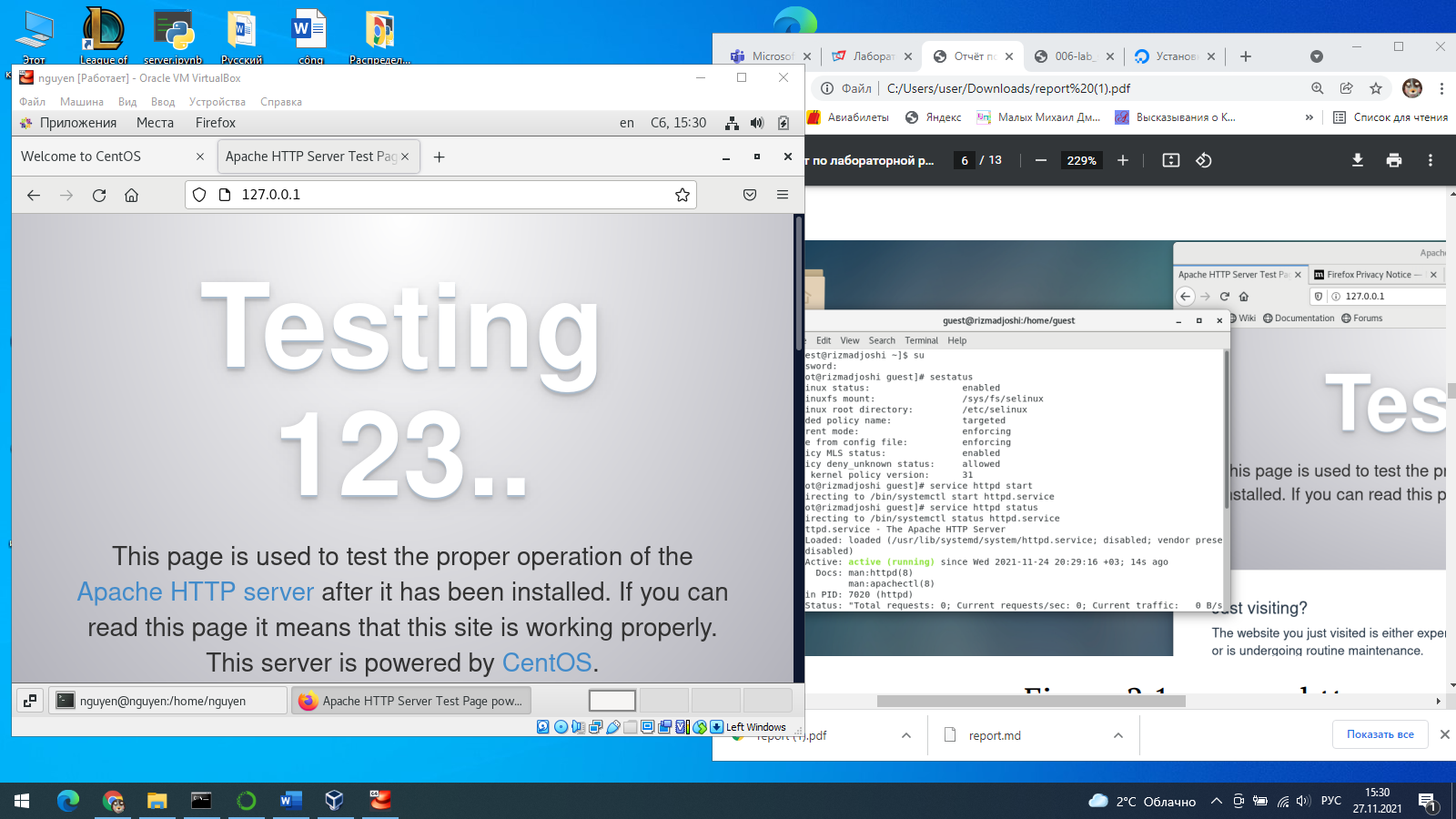


Figure 3: запуск http

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

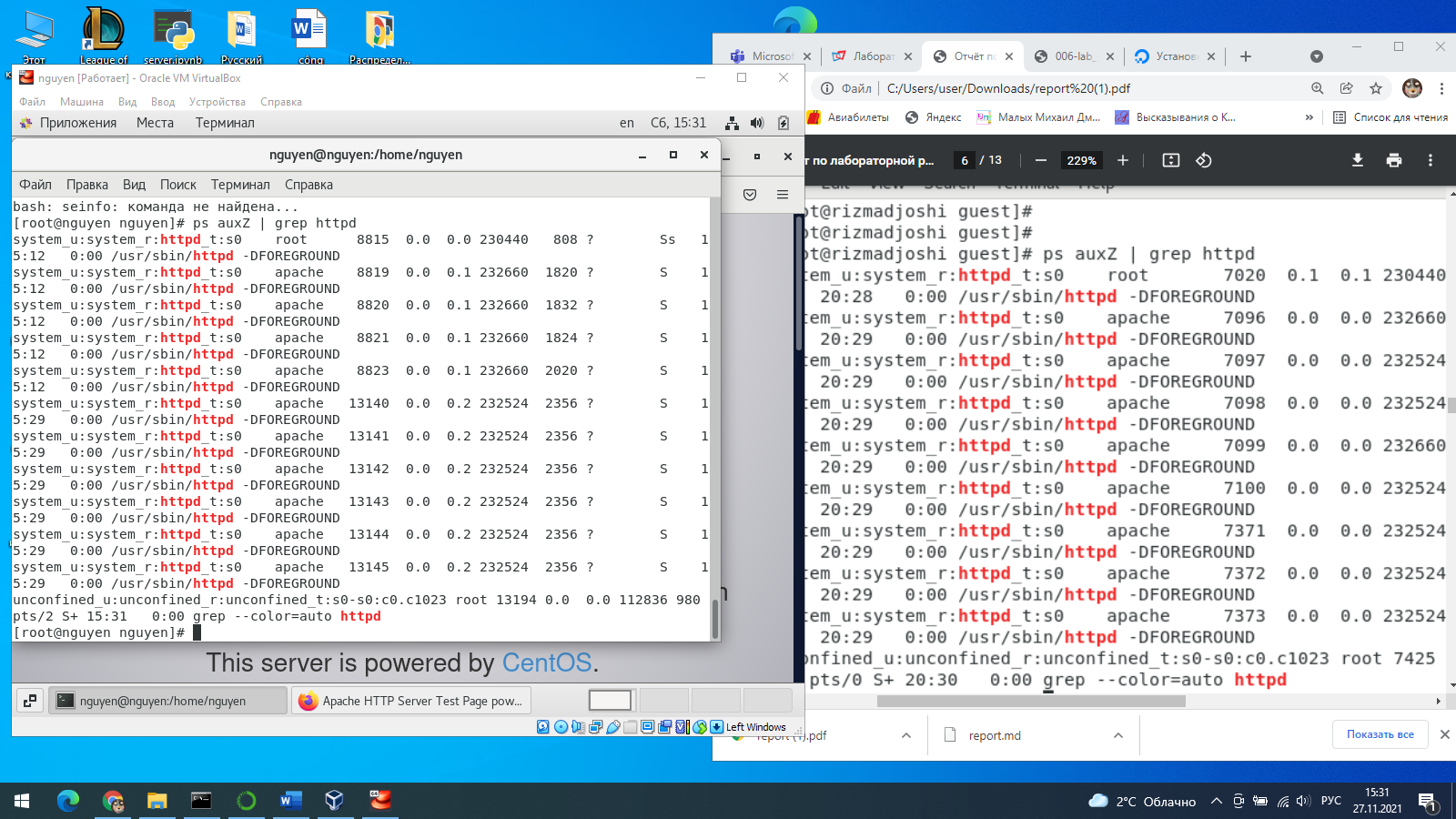


Figure 4: ps auxZ | grep httpd

4. Посмотрите текущее состояние переключателей SELinux для Apache с

помощью команды

sestatus -bigrep httpd

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

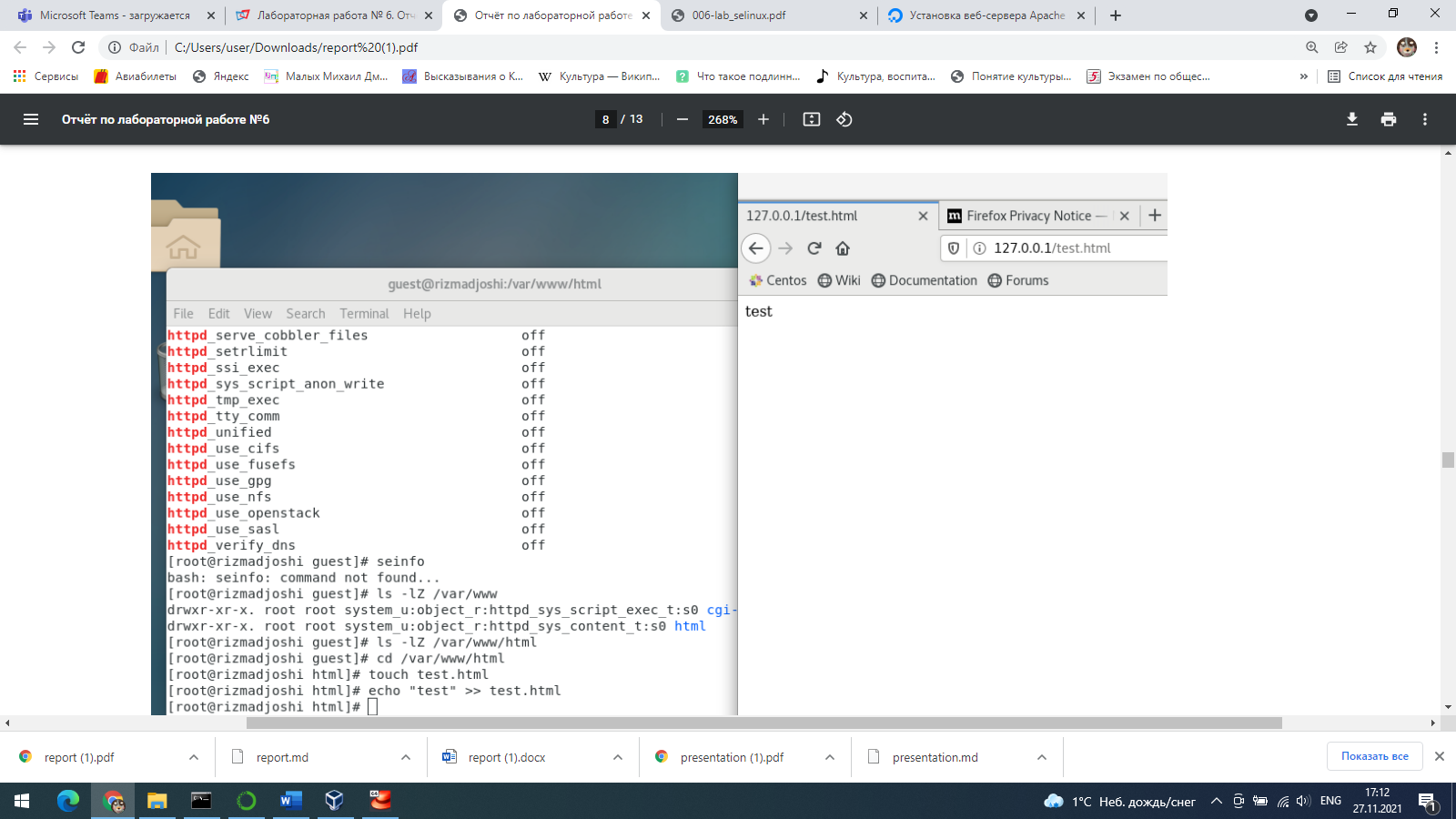


Figure 5: sestatus -bigrep httpd

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>

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

присваиваемый по умолчанию вновь созданным файлам в директории

/var/www/html.

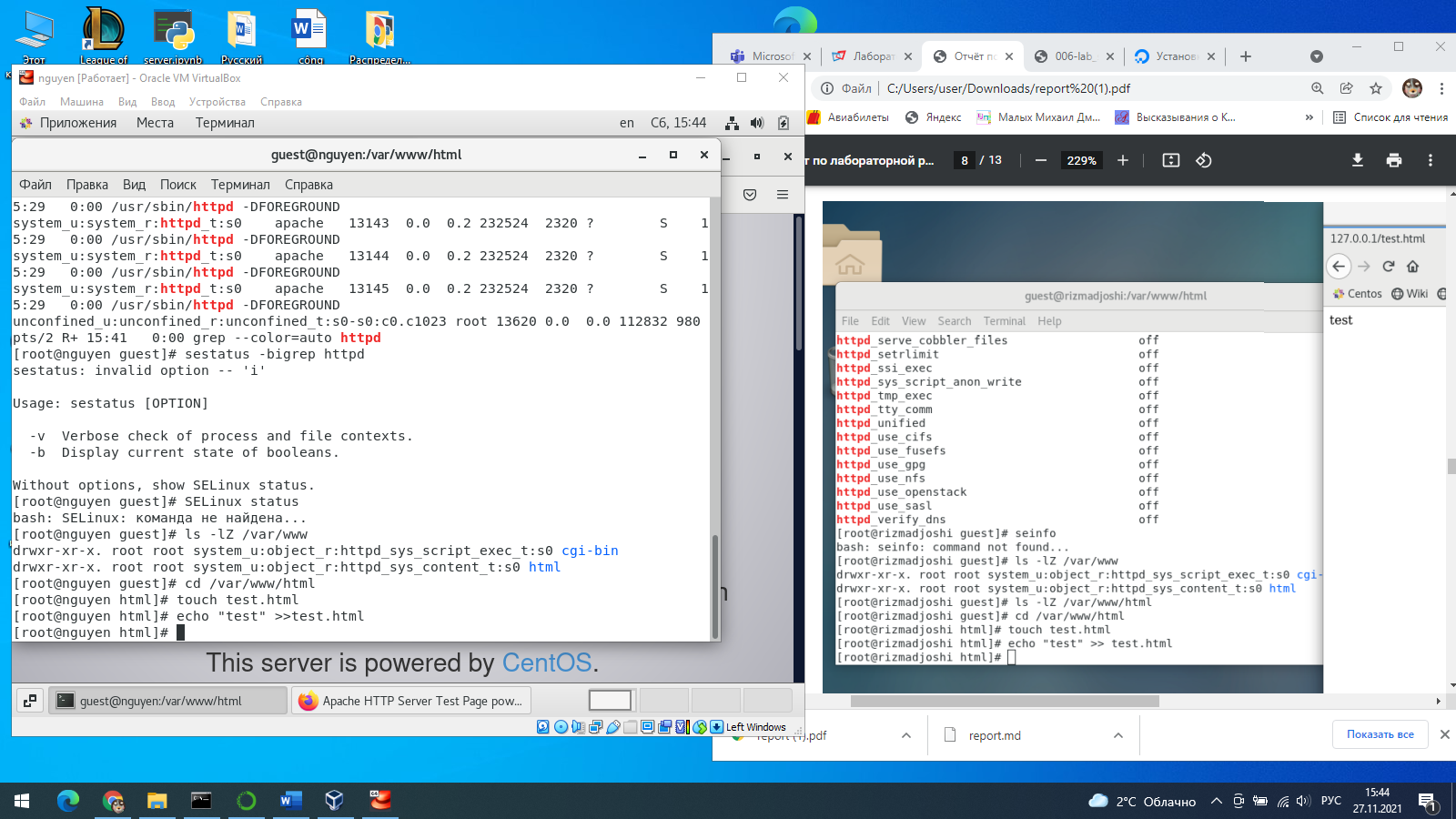


Figure 6: test.html

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

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

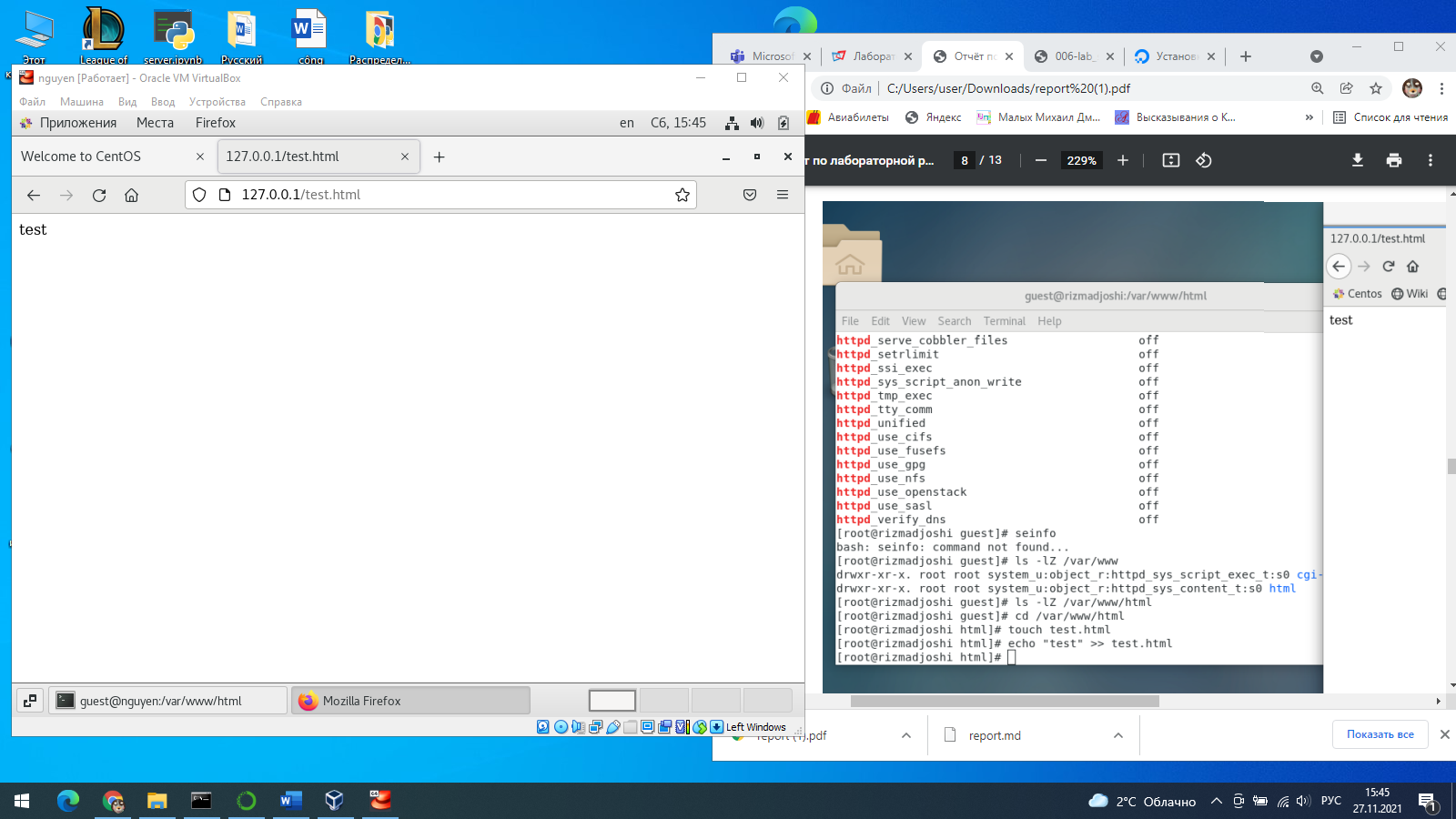


Figure 7: отображен текст

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.

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

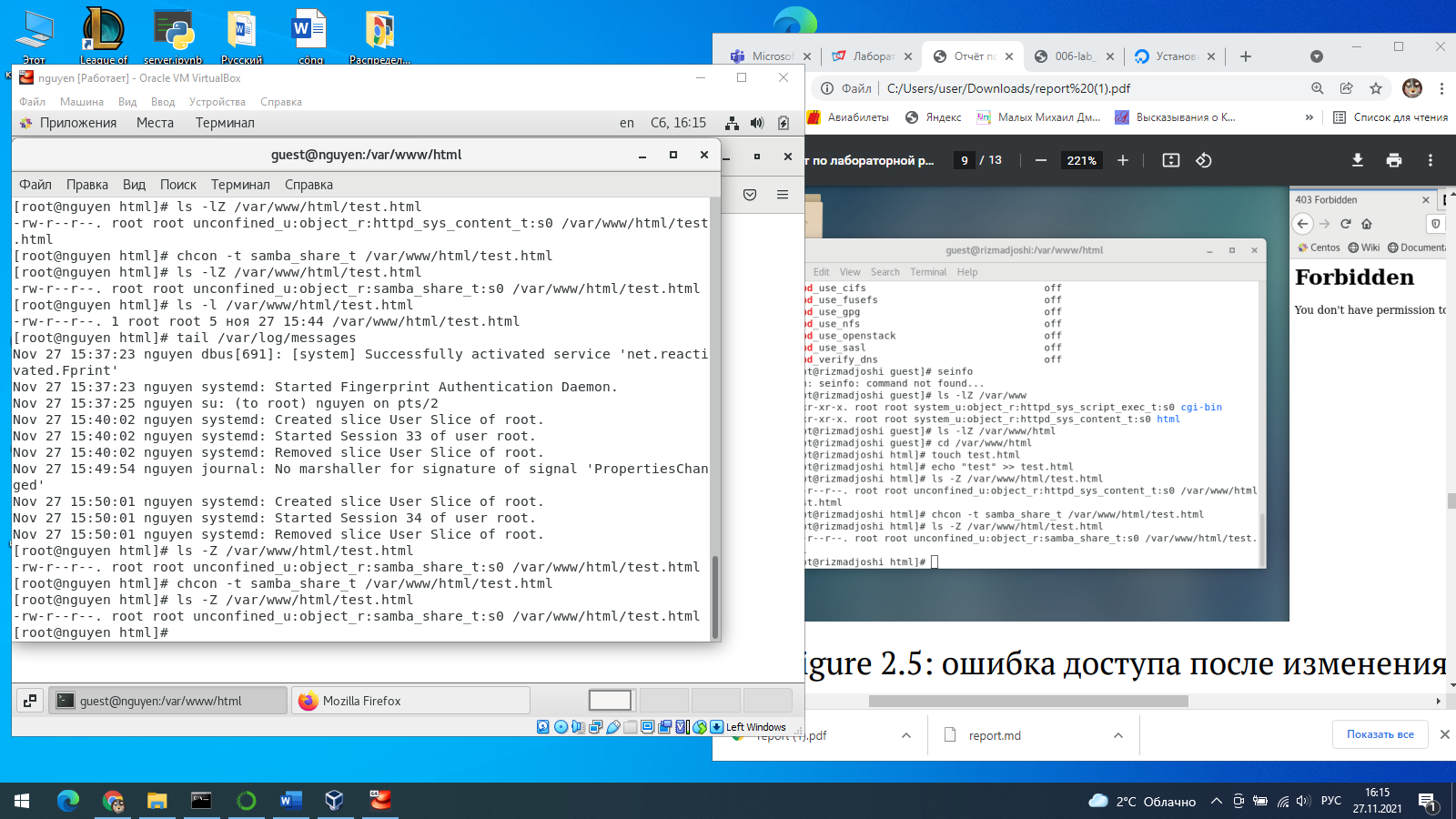


Figure 8: Пункт 12 +13.

После этого проверьте, что контекст поменялся.

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.

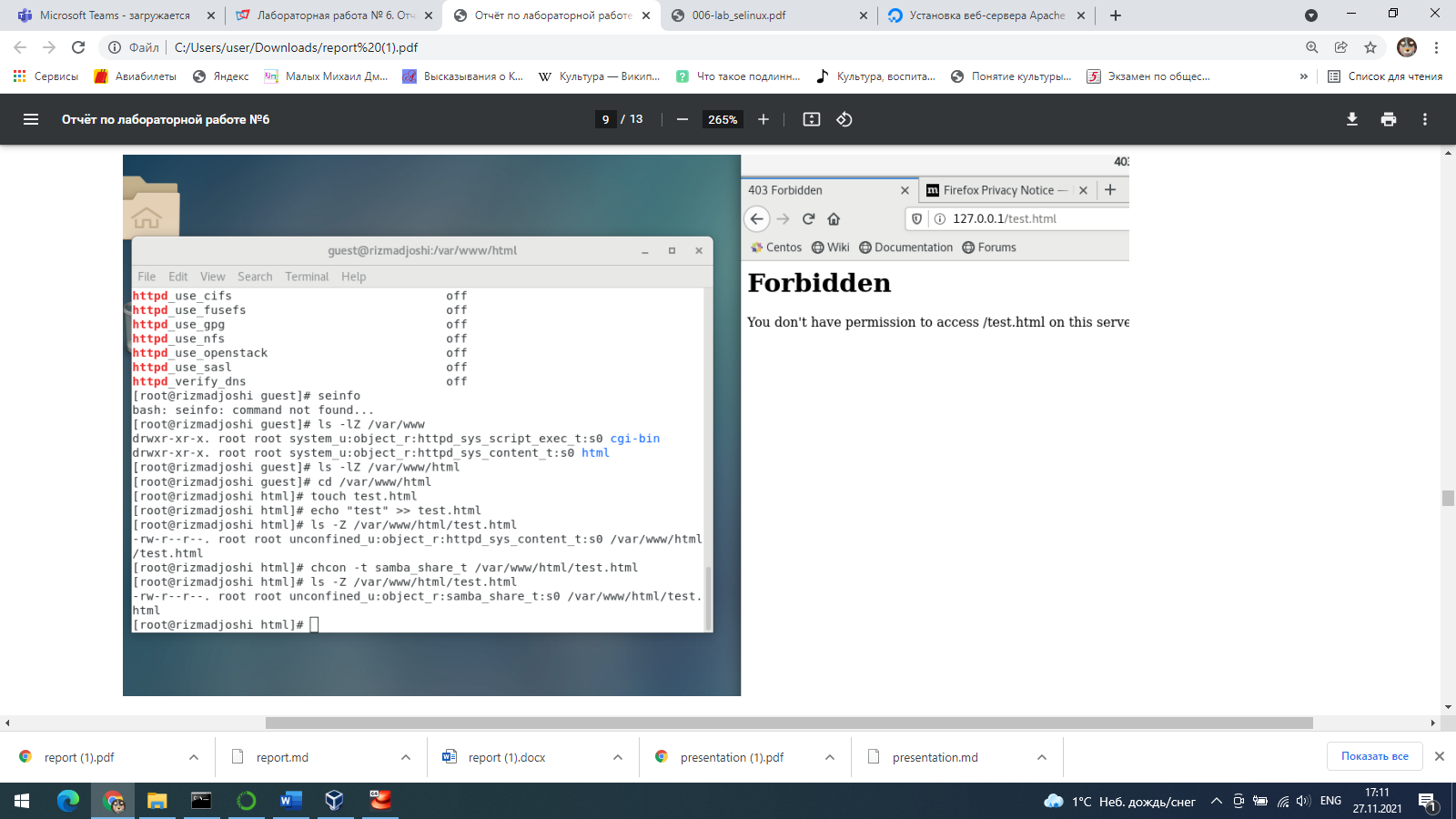


Figure 9: пункт 14

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.

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.

17. Выполнила перезапуск веб-сервера Apache. Сбой не происходит, порт 81 уже вписан в разрешенные

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.

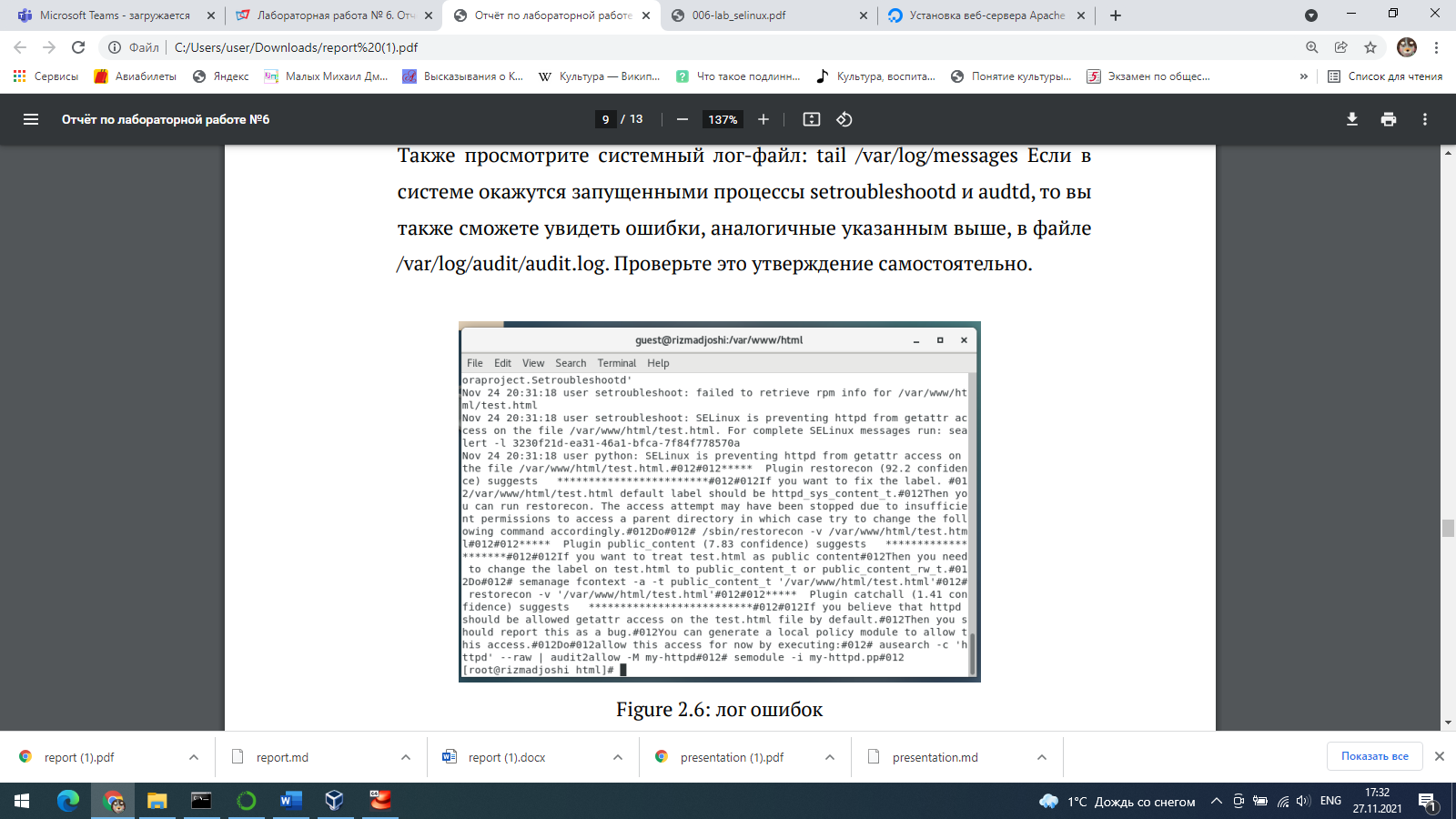


Figure 10: log error

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.

20. Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему

он сейчас запустился, а в предыдущем случае не смог?

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».

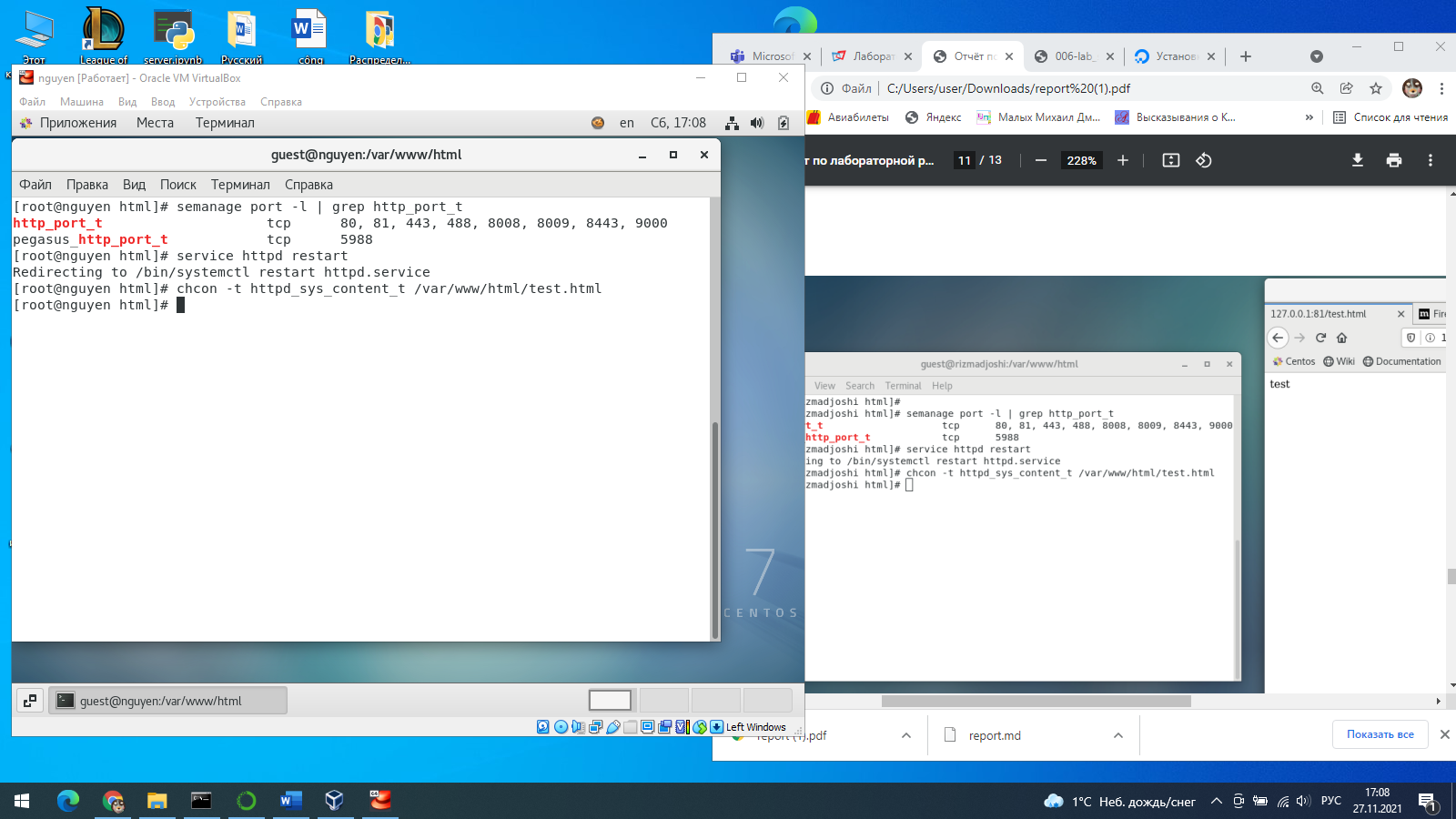


Figure 11: пункт 19+20+21

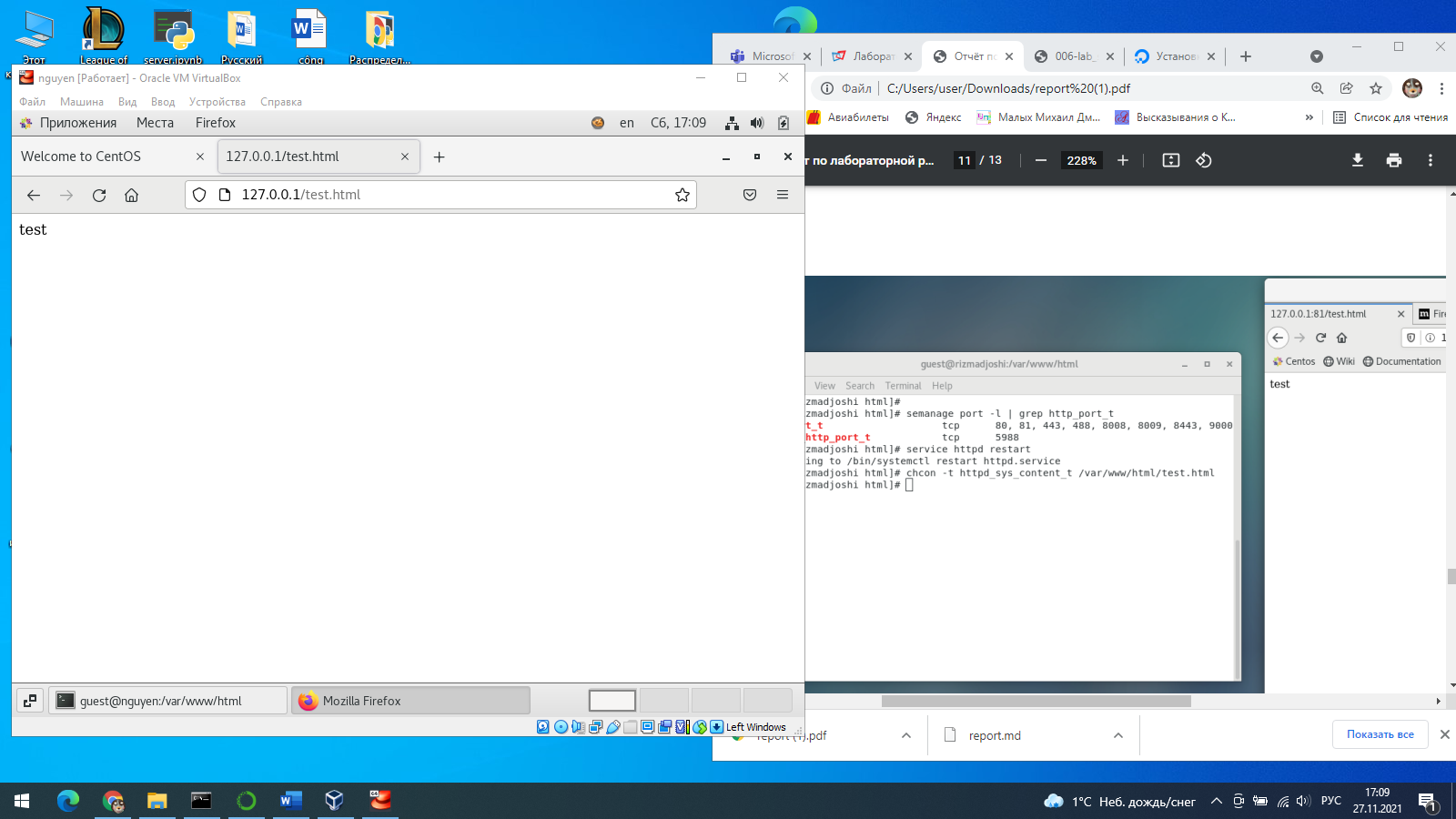


Figure 12: пункт 19+20+21

22. Исправьте обратно конфигурационный файл apache, вернув Listen 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.

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

rm /var/www/html/test.html

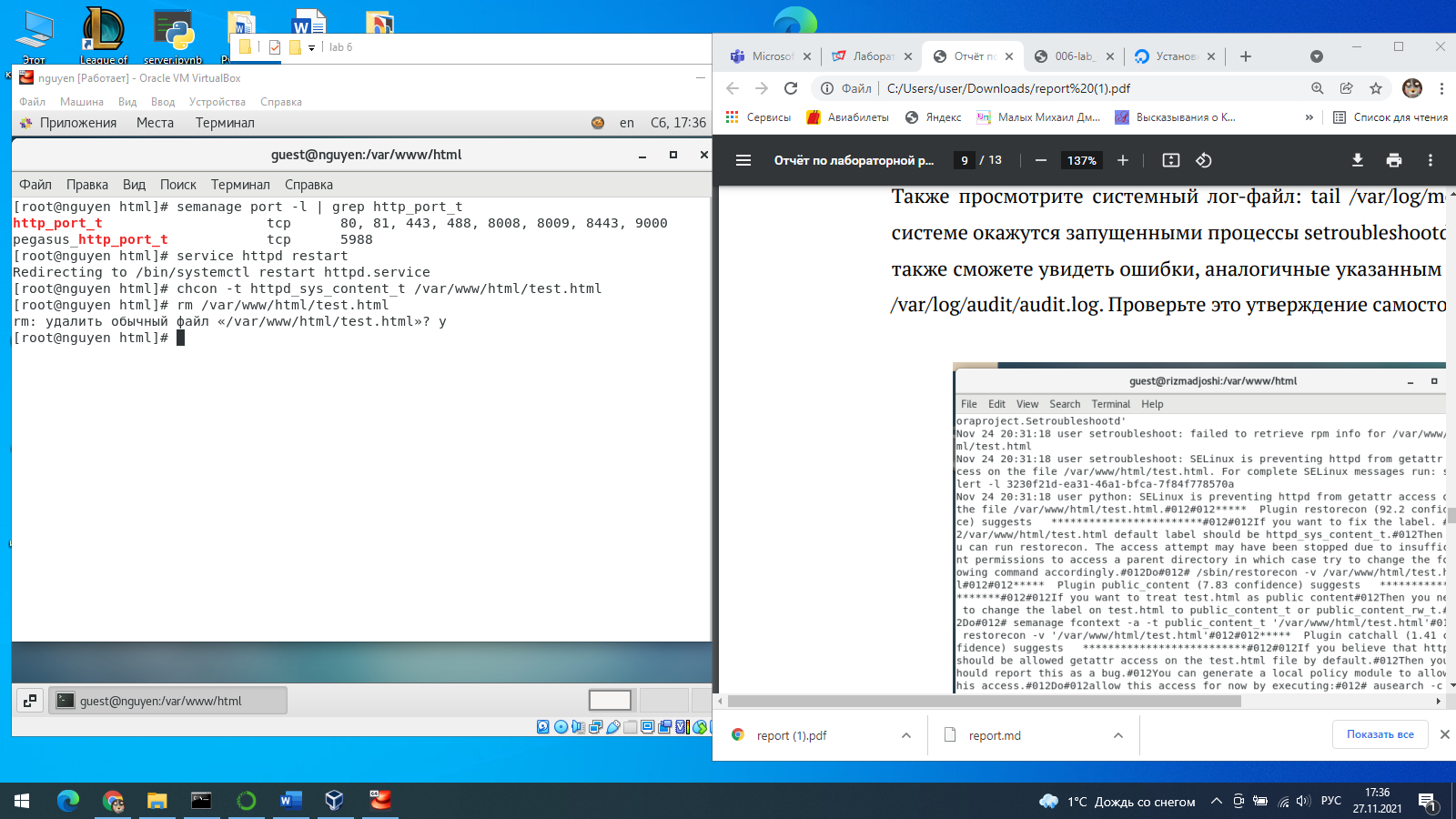


Figure 13: пункт 22+23+24

**Выводы**

В процессе выполнения лабораторной работы мною были получены базовые навыки работы с технологией seLinux.