

Отчет по лабораторной работе №6

Информационная безопасность

Евдокимова Юлия Константиновна НПИбд-01-18

Содержание

1 Цель работы	4
2 Выполнение лабораторной работы	5
3 Выводы	22

List of Figures

2.1	SELinux	5
2.2	Отключение фильтра	6
2.3	Режим SELinux	7
2.4	Проверка	7
2.5	веб-сервер Apache	8
2.6	Просмотр состояния переключателей SELinux для Apache	9
2.7	Получение информации	10
2.8	Получение информации	10
2.9	Создание файла	11
2.10	Проверка	11
2.11	Получение доступа к файлу через браузер	12
2.12	Получение доступа к файлу через браузер	13
2.13	Просмотр системного лог-файла	14
2.14	Просмотр системного лог-файла	14
2.15	Изменение порта 80 на 81	15
2.16	Анализ лог-файла	16
2.17	Анализ файла	16
2.18	Анализ файла	17
2.19	Выполнение и проверка	18
2.20	Возвращение контекста	19
2.21	Получение доступа к файлу через браузер	19
2.22	Исправление конфигурационного файл apache	20
2.23	Удаление привязки http_port_t к 81 порту	20
2.24	Удаление файла /var/www/html/test.html	21

1 Цель работы

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

2 Выполнение лабораторной работы

1. Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus.

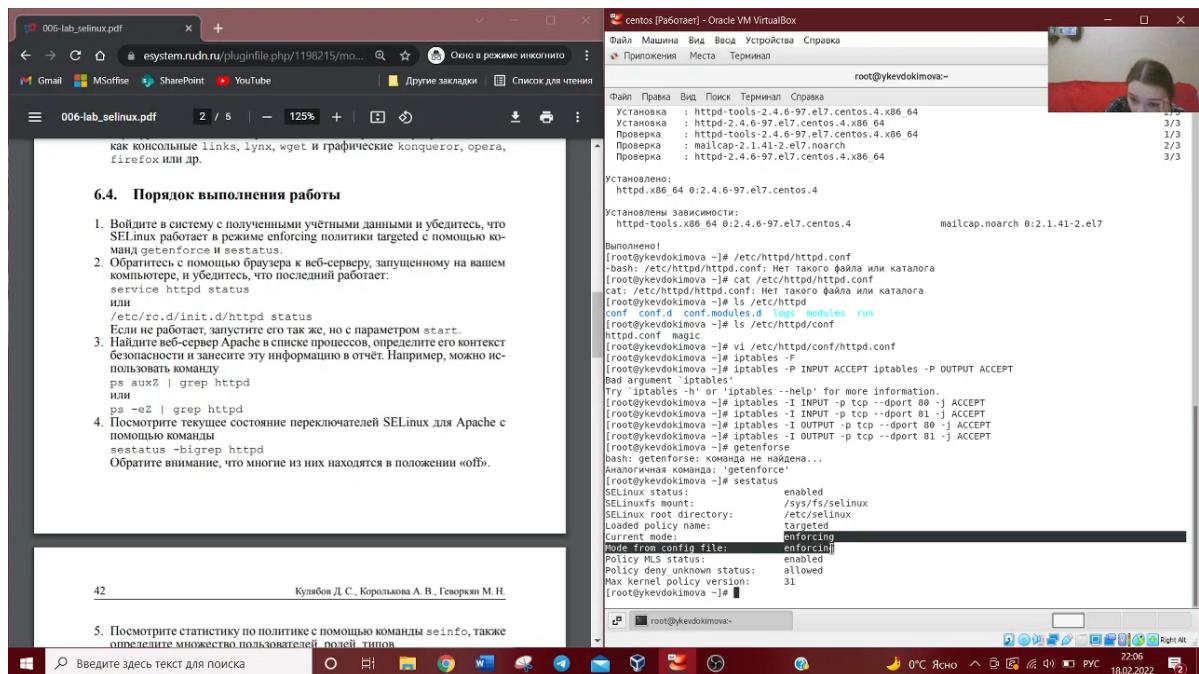


Figure 2.1: SELinux

2. Также проследила, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp. Отключила фильтр командами: iptables -F, iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT. Так же добавила разрешающие правила.

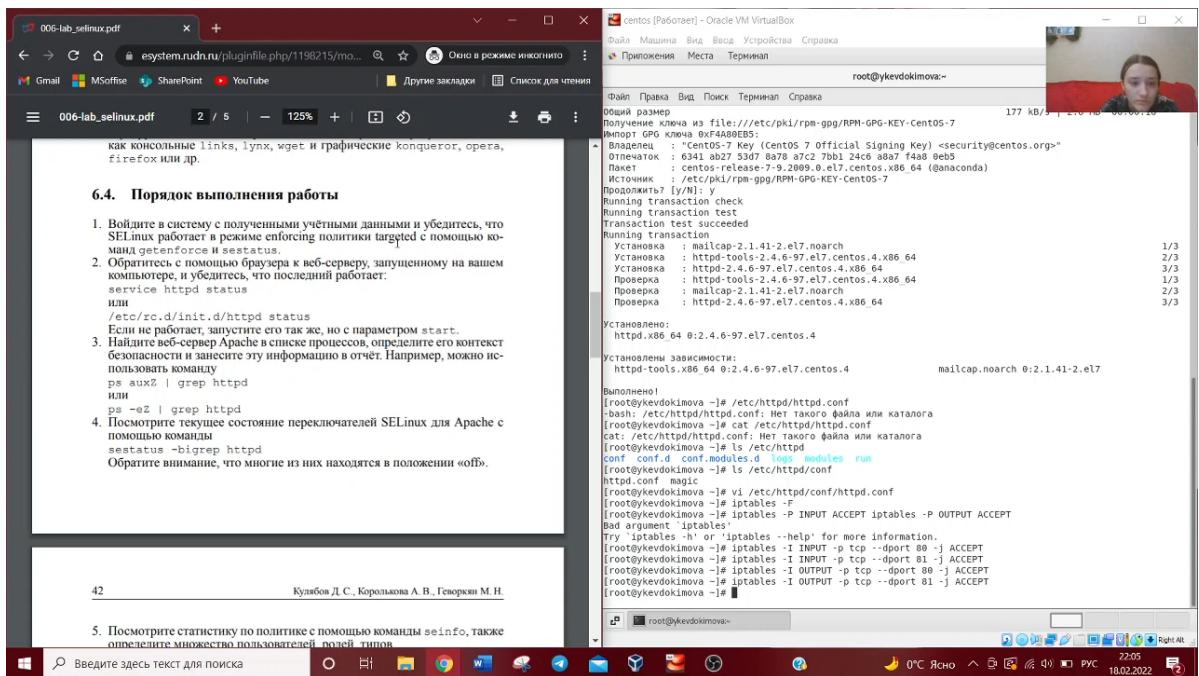


Figure 2.2: Отключение фильтра

3. Вшла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus.

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`.
3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и запишите эту информацию в отчёте. Например, можно использовать команду
`ps auxZ | grep httpd`
4. Помогите текущее состояние переключателей SELinux для Apache с помощью команды
`sestatus -bigrep httpd`
 Обратите внимание, что многие из них находятся в положении «off».

42 Кульбов Д.С., Королькова А.В., Геворкян М.Н.

5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей разной типов

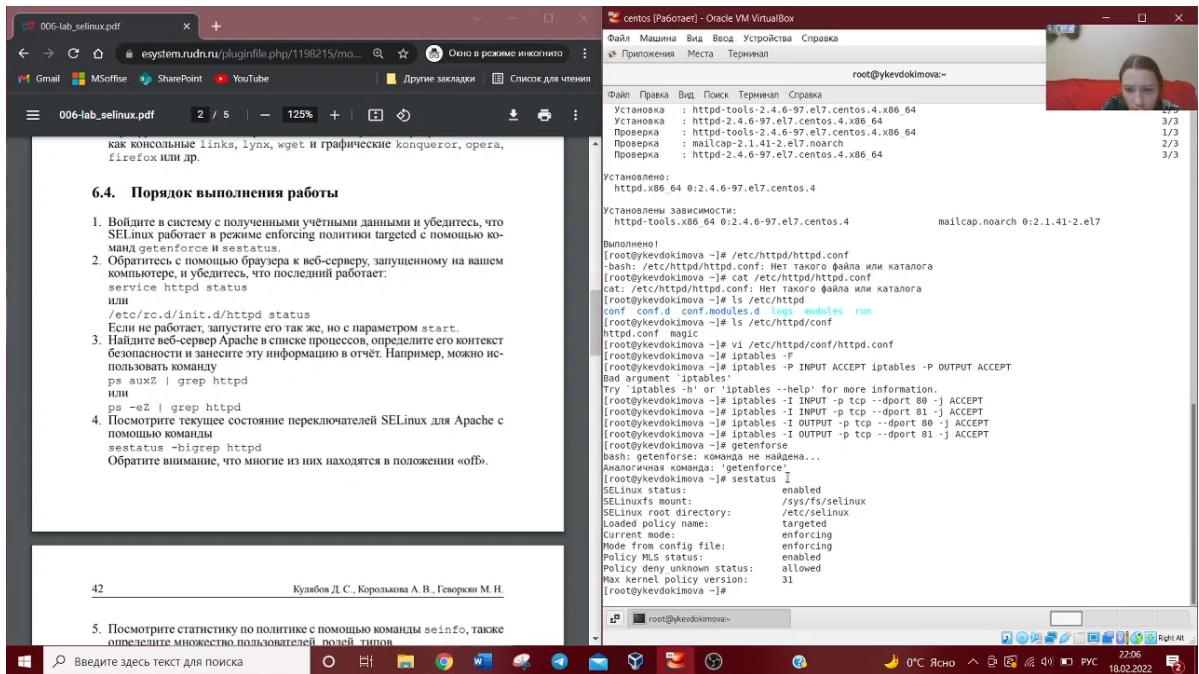


Figure 2.3: Режим SELinux

4. Убедилась, что сервер работает: service httpd status.

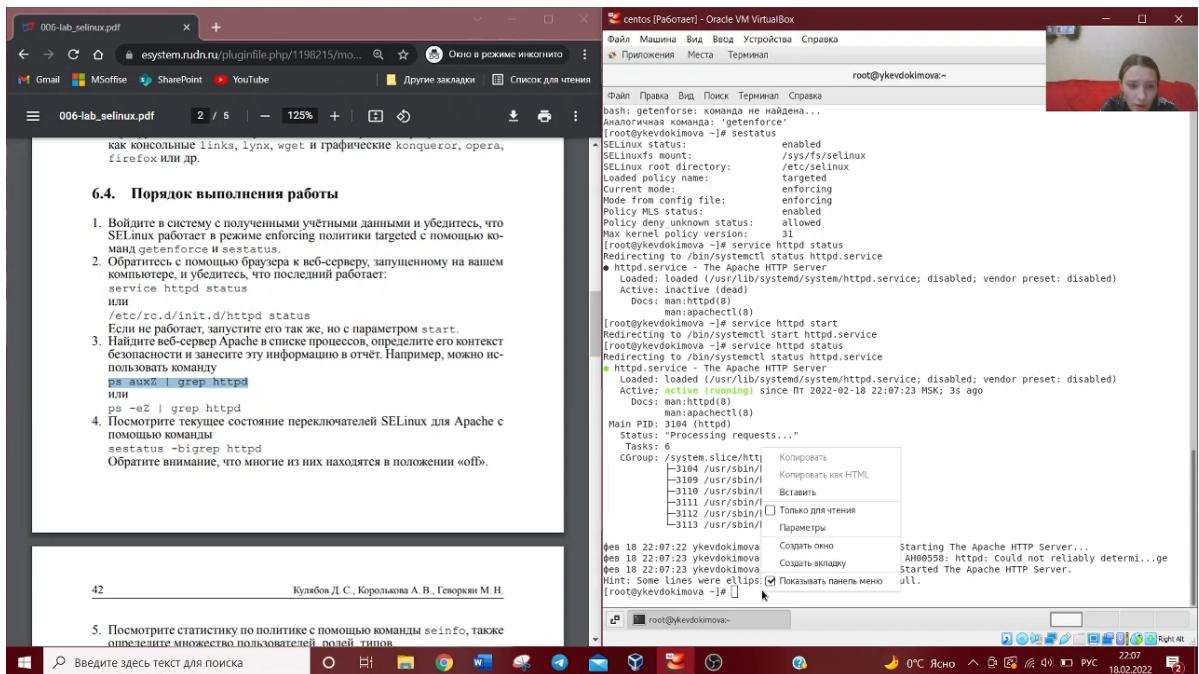


Figure 2.4: Проверка

5. Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности.

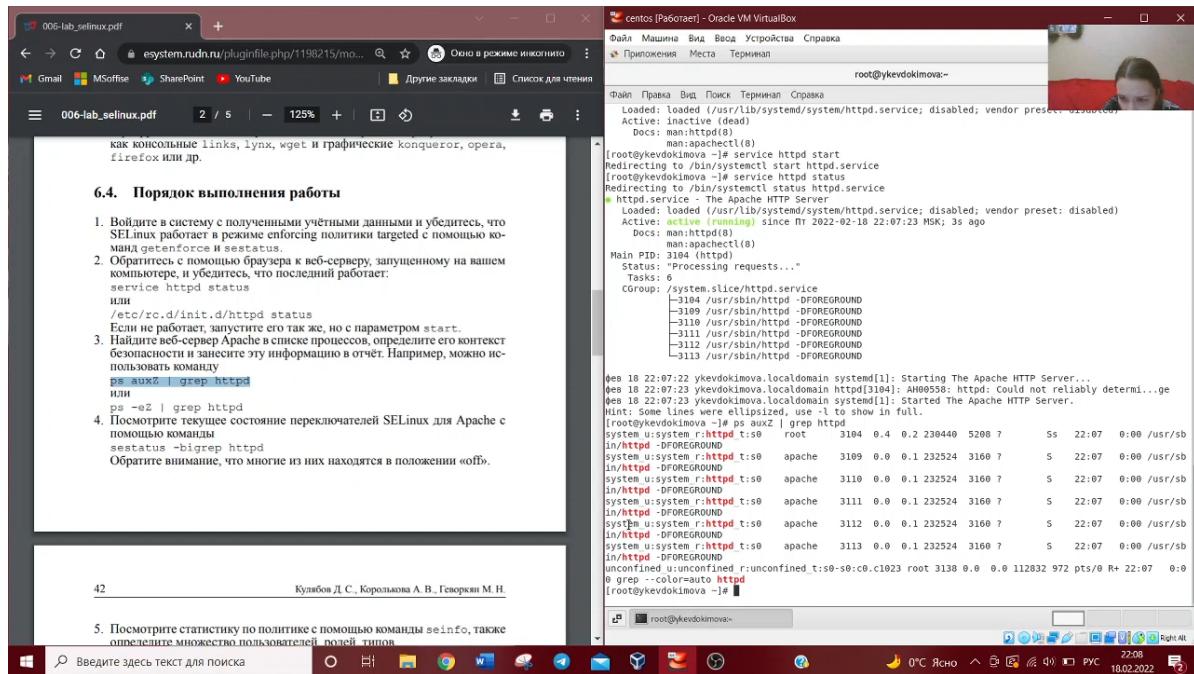


Figure 2.5: веб-сервер Apache

6. Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды: sestatus -bigrep httpd. Обратила внимание, что многие из них находятся в положении «off».

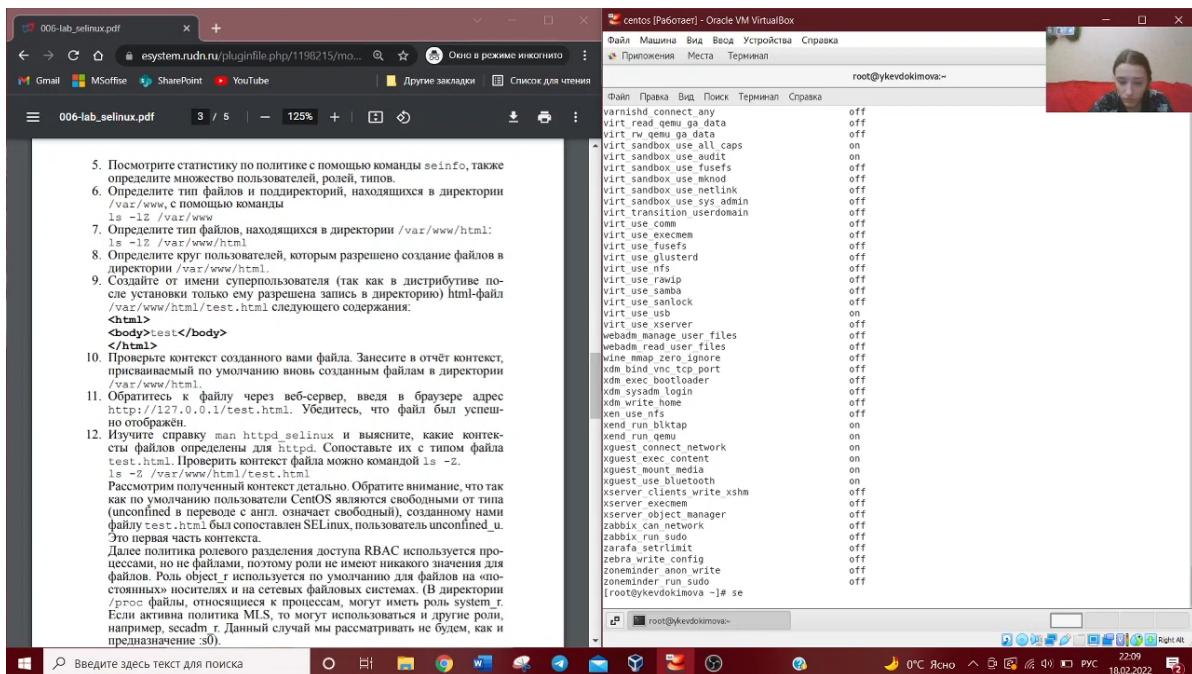


Figure 2.6: Просмотр состояния переключателей SELinux для Apache

7. Посмотрела статистику по политике с помощью команды `seinfo`, также определила множество пользователей, ролей, типов. Определила тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды: `ls -lZ /var/www`. Определила тип файлов, находящихся в директории `/var/www/html`: `ls -lZ /var/www/html`. Определила круг пользователей, которым разрешено создание файлов в директории `/var/www/html`.

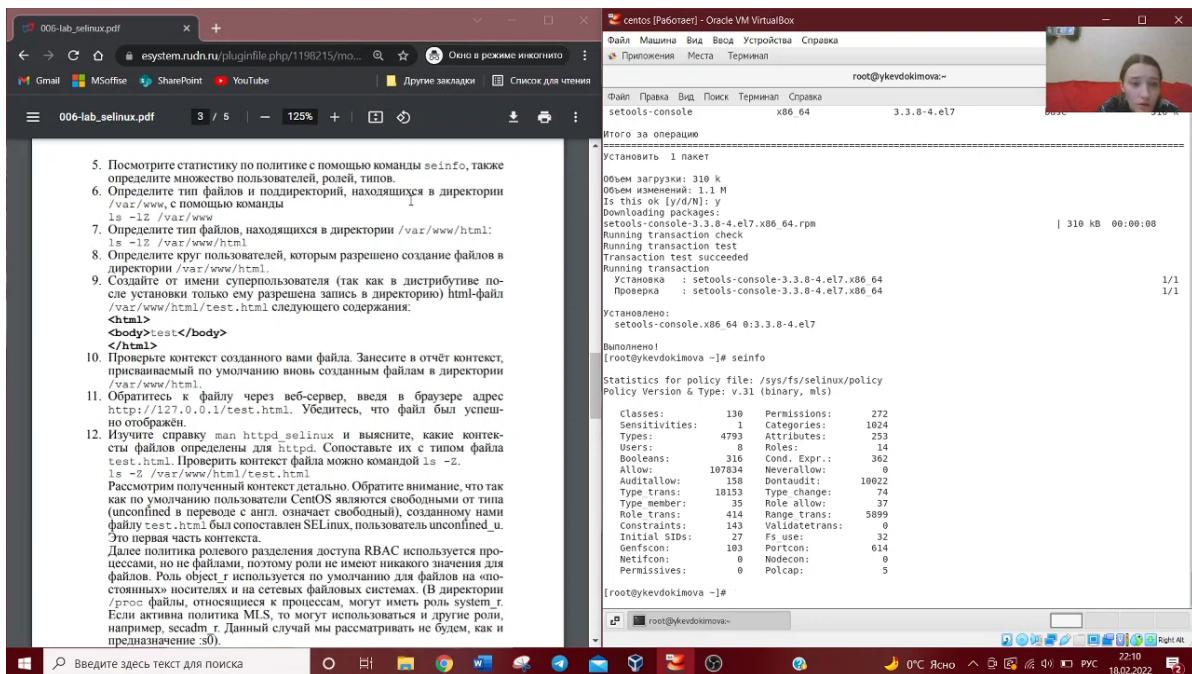


Figure 2.7: Получение информации

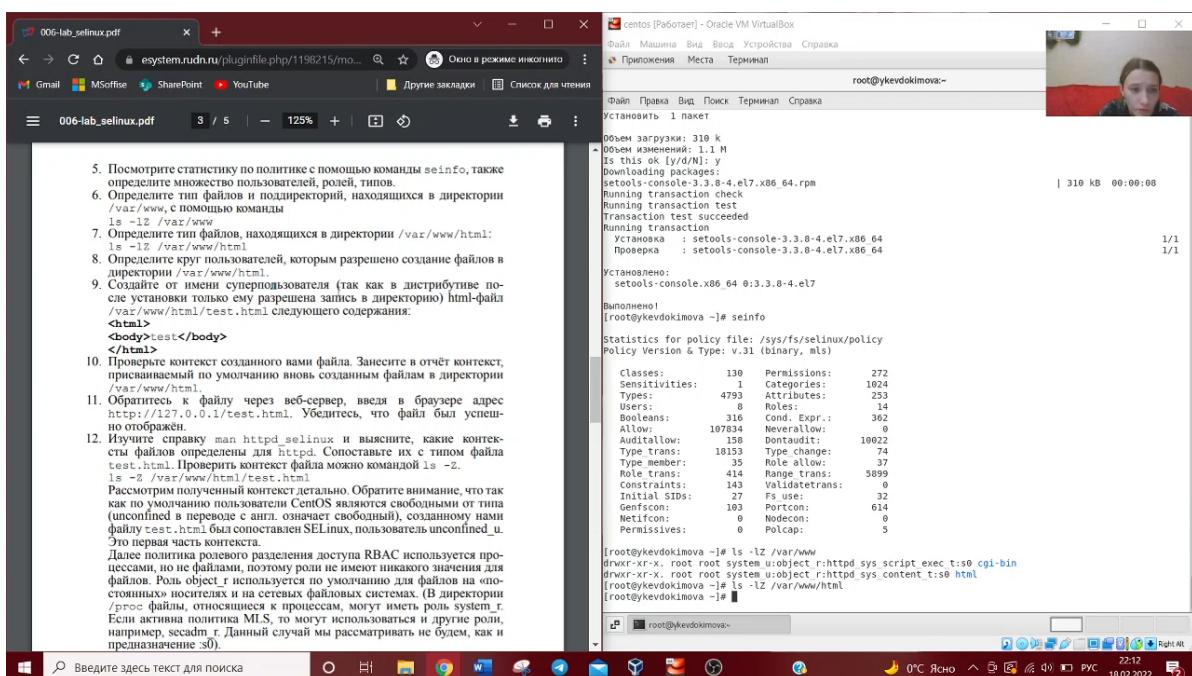


Figure 2.8: Получение информации

8. Создала от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл

/var/www/html/test.html.

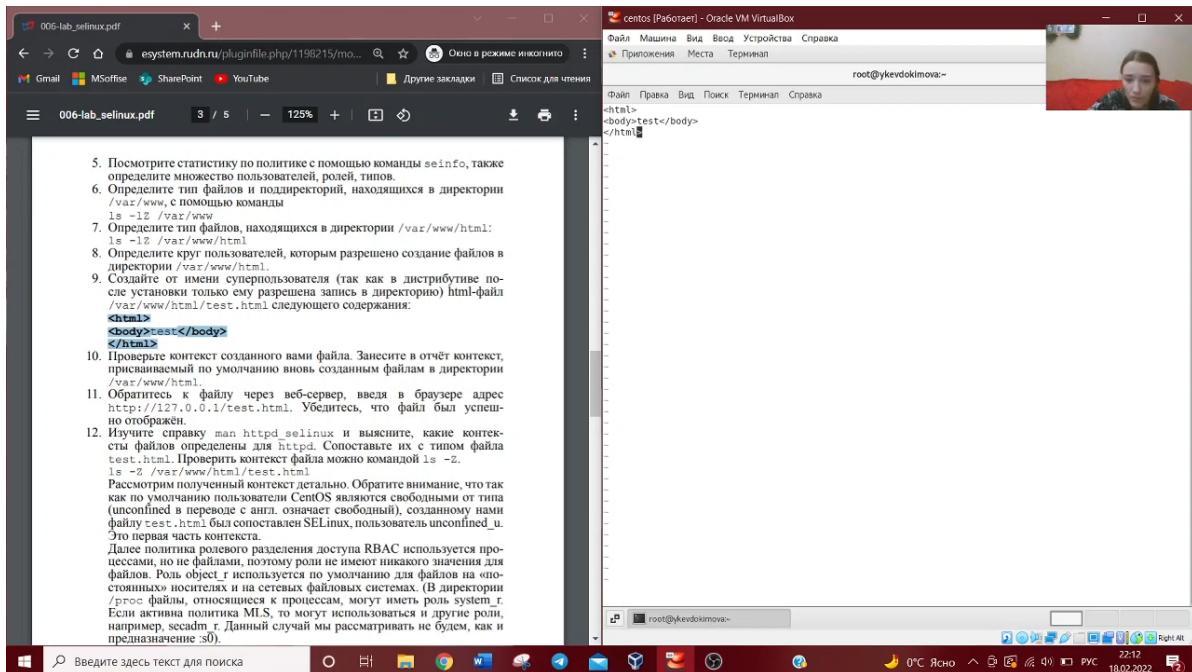


Figure 2.9: Создание файла

9. Проверила контекст созданного файла. httpd_sys_content_t.

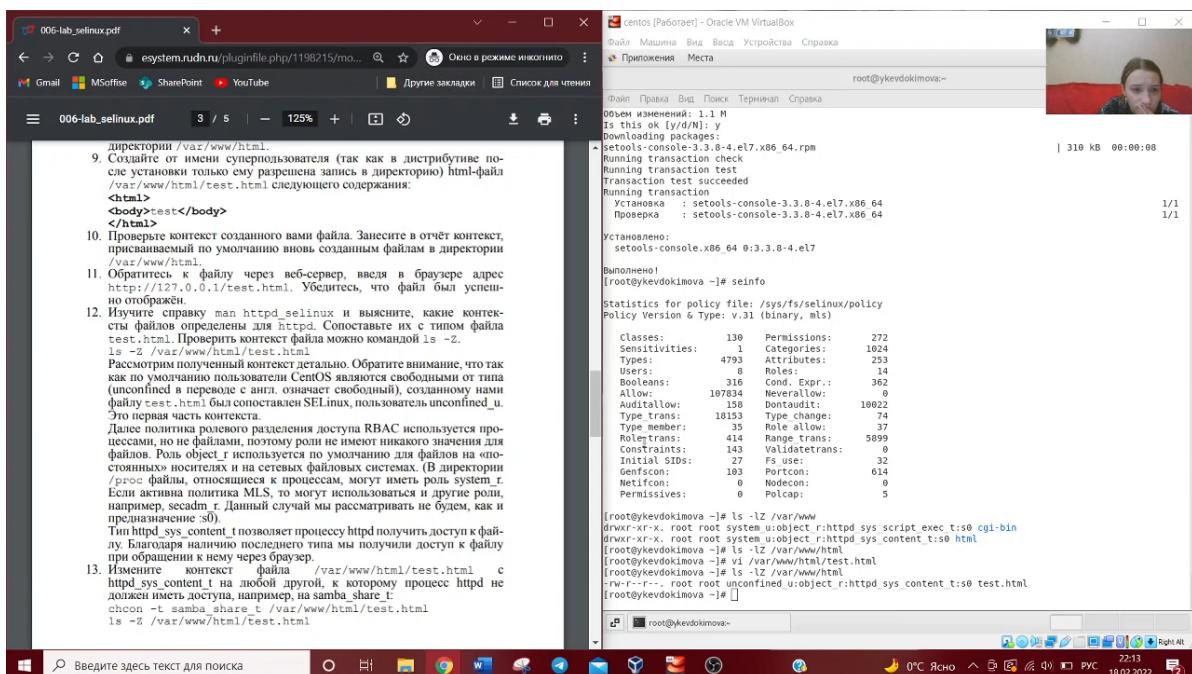


Figure 2.10: Проверка

10. Обратилась к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>.

Убедилась, что файл был успешно отображён.

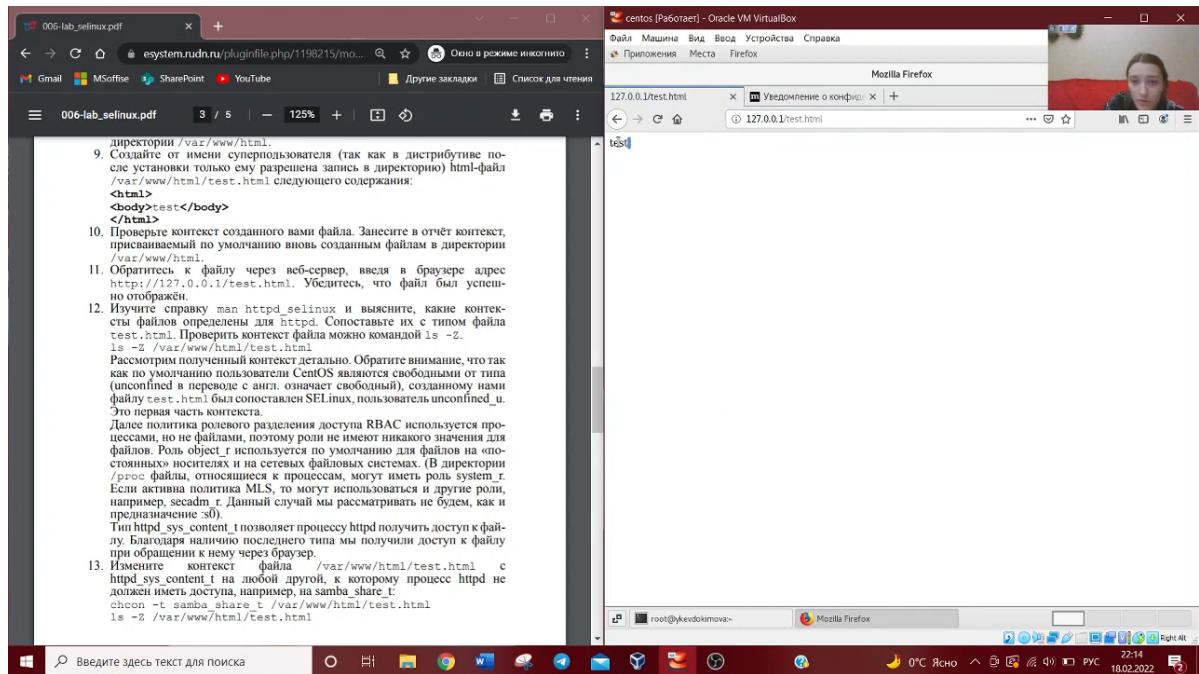


Figure 2.11: Получение доступа к файлу через браузер

11. Изменила контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t`. После этого проверила, что контекст поменялся. Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Получили сообщение об ошибке.

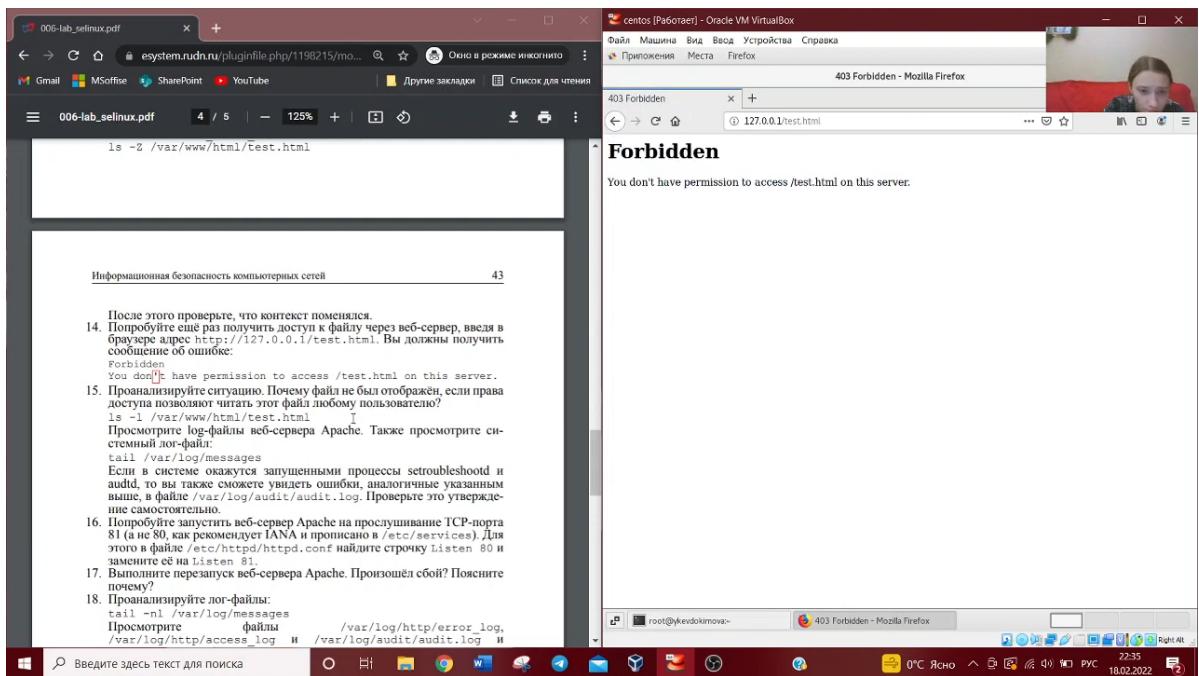


Figure 2.12: Получение доступа к файлу через браузер

12. Проанализировала ситуацию. Файл не был отображён потому что мы изменили контекст файла. Просмотрела log-файлы веб-сервера Apache. Также просмотрела системный лог-файл: tail /var/log/messages.

Figure 2.13: Просмотр системного лог-файла

После этого проверьте, что контекст поменялся.

14. Попробуйте сабз 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.
```

15. Проверяйте ситуацию. Почему файл не был отображен, если права доступа позволяют читать этот файл любому пользователю?

```
ls -l /var/www/html/test.html
```

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

```
tail /var/log/messages
```

Если в системе окажутся запущенными процессы `setroubleshield` и `auditd`, то вы также сумеете увидеть ошибки, аналогичные указанным выше, в файле `/var/log/audit/audit.log`. Проверьте это утверждение.

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

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

18. Проверяйте лог-файлы:

```
tail -nL 1 /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.

19. Выполните команду

```
semanage port -a -t http_port_t -p tcp 81
```

После этого проверьте список портов коммандой

```
semanage port -l | grep http_port_t
```

и убедитесь, что порт 81 now ported.

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

21. Верните контекст `http_sys_content_t` к файлу `/var/www/html/test.html`:

```
chcon -t http_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>.

Figure 2.14: Просмотр системного лог-файла

13. Попробовала 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 нашла строчку Listen 80 и замените её на Listen 81.

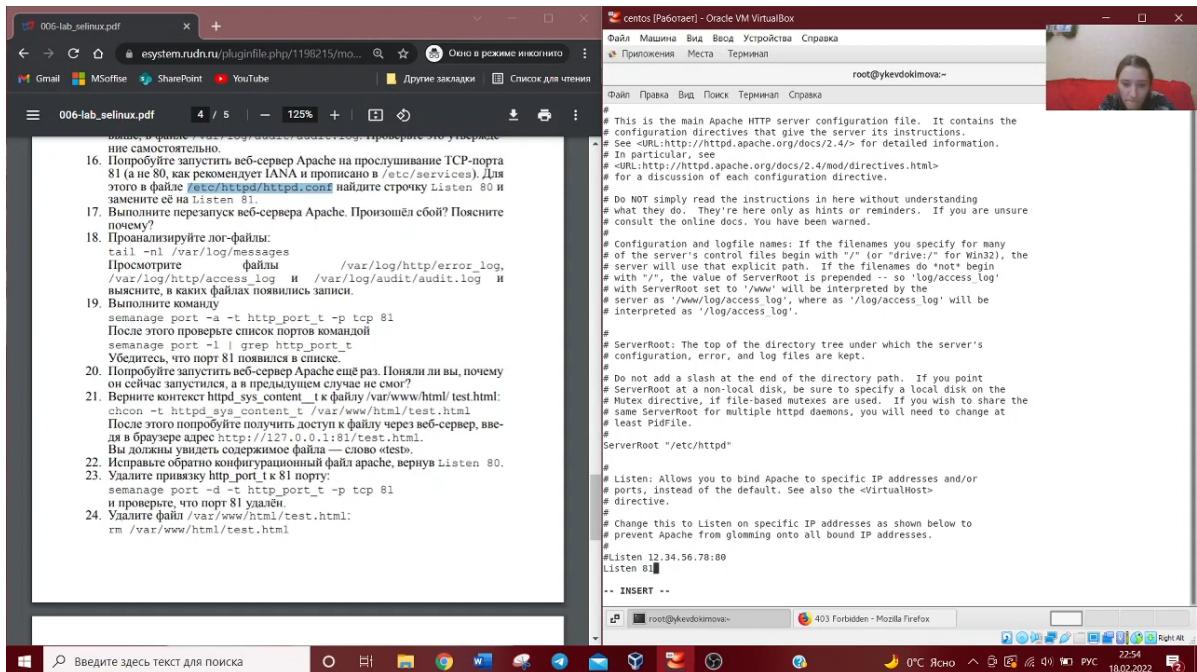


Figure 2.15: Изменение порта 80 на 81

14. Проанализировала лог-файлы. Просмотрела файлы /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log.

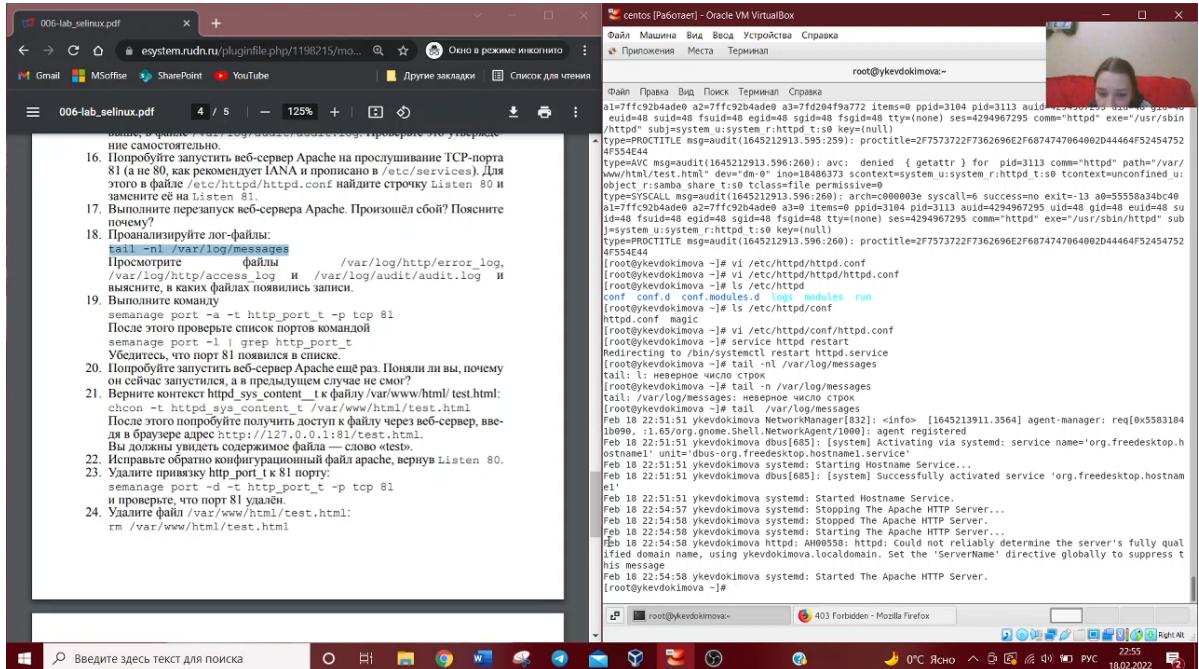


Figure 2.16: Анализ лог-файла

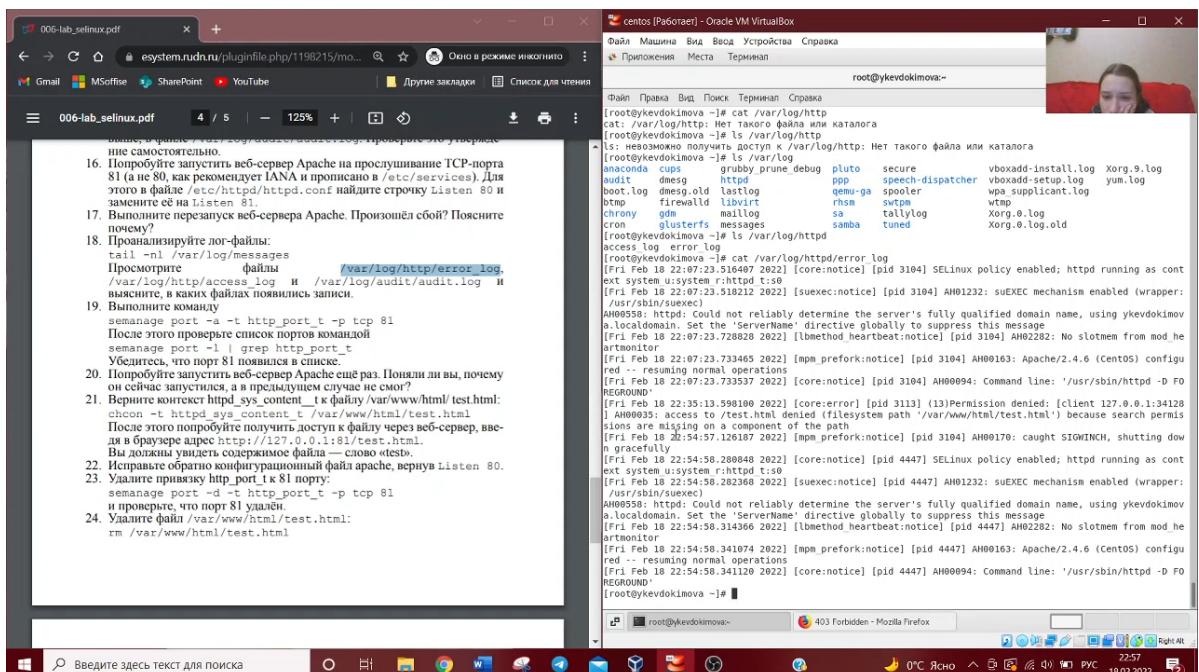


Figure 2.17: Анализ файла

The screenshot shows a Windows desktop environment with two terminal windows open. The left terminal window displays a PDF document titled '006-lab_selinux.pdf' which contains a numbered list of 24 SELinux configuration steps. The right terminal window is running on a CentOS VM in Oracle VM VirtualBox, showing a root shell. The terminal output includes SELinux audit logs and command-line history related to SELinux policy changes and Apache configuration.

Figure 2.18: Анализ файла

15. Выполнила команду: `semanage port -a -t http_port_t -p tcp 81`. После этого проверила список портов командой: `semanage port -l | grep http_port_t`. Убедилась, что порт 81 появился в списке.

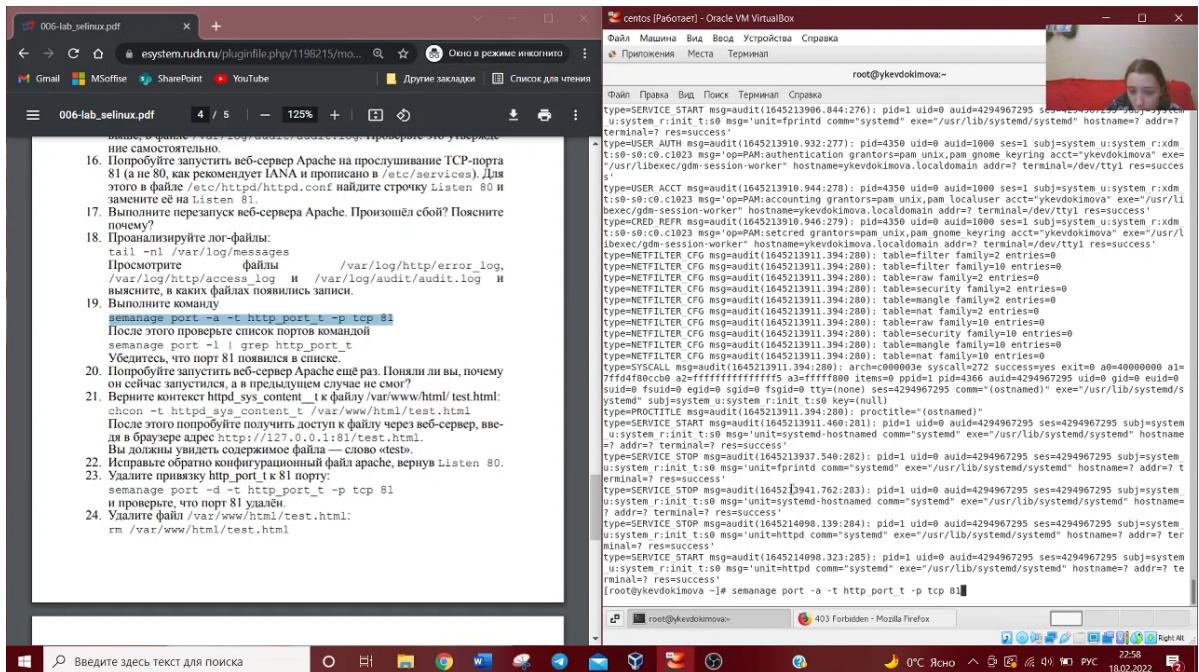


Figure 2.19: Выполнение и проверка

16. Вернула 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 попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. Увидели содержимое файла — слово «test».

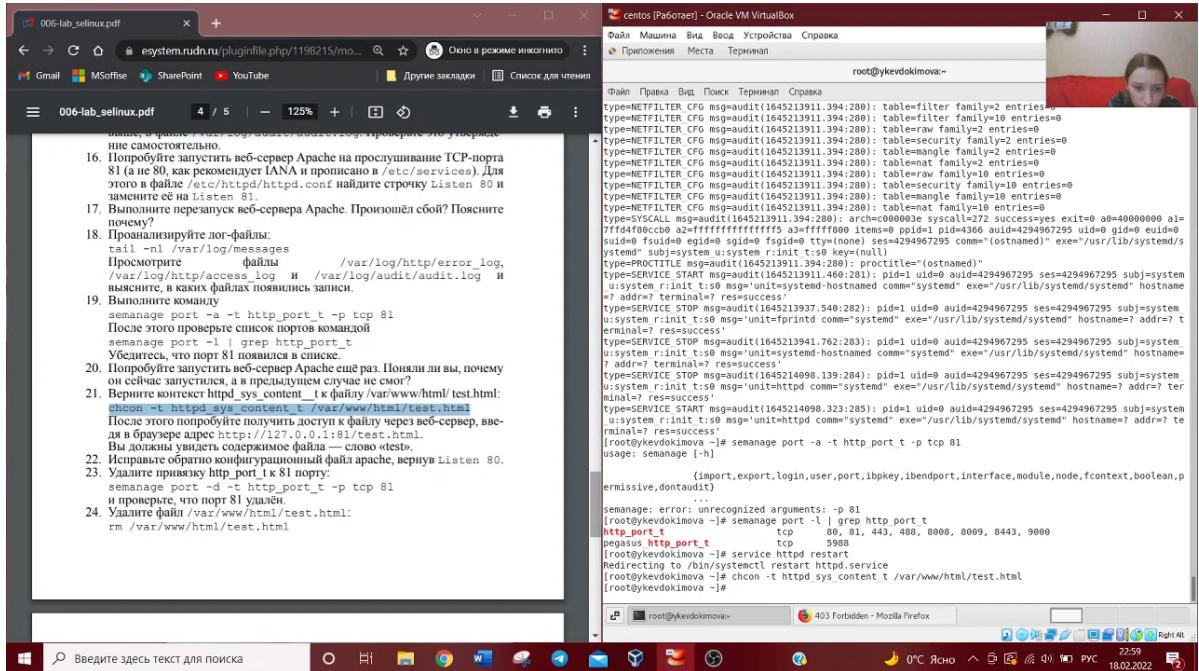


Figure 2.20: Возвращение контекста

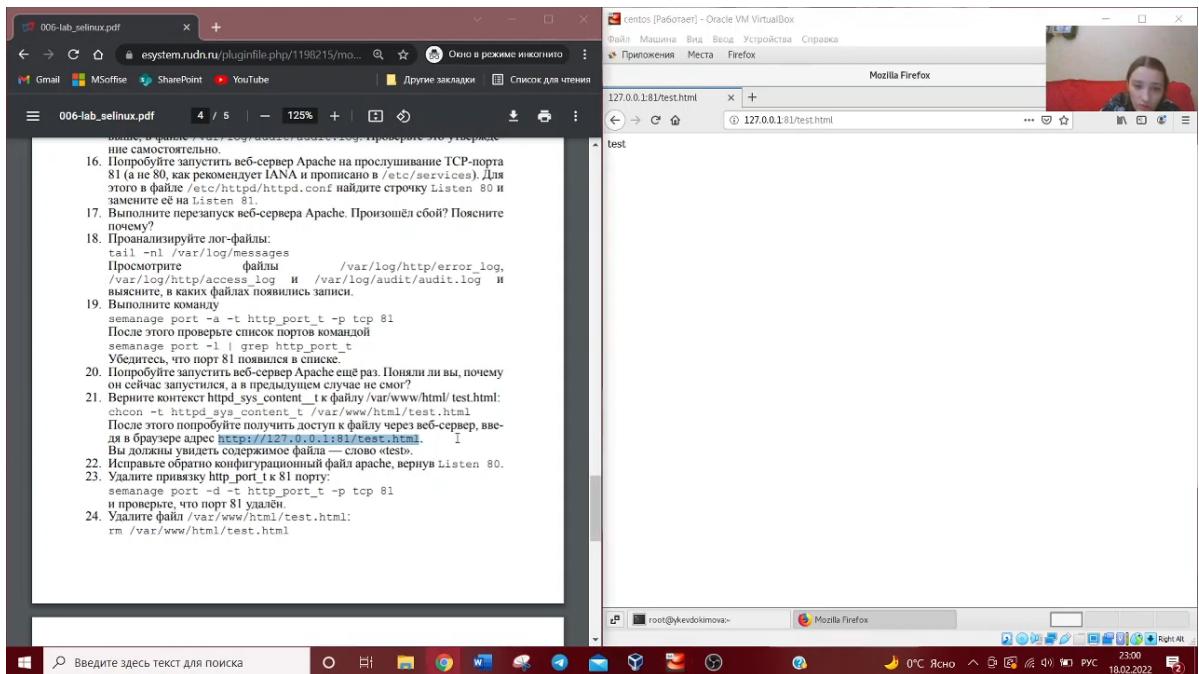


Figure 2.21: Получение доступа к файлу через браузер

17. Исправила обратно конфигурационный файл apache, вернув Listen 80.

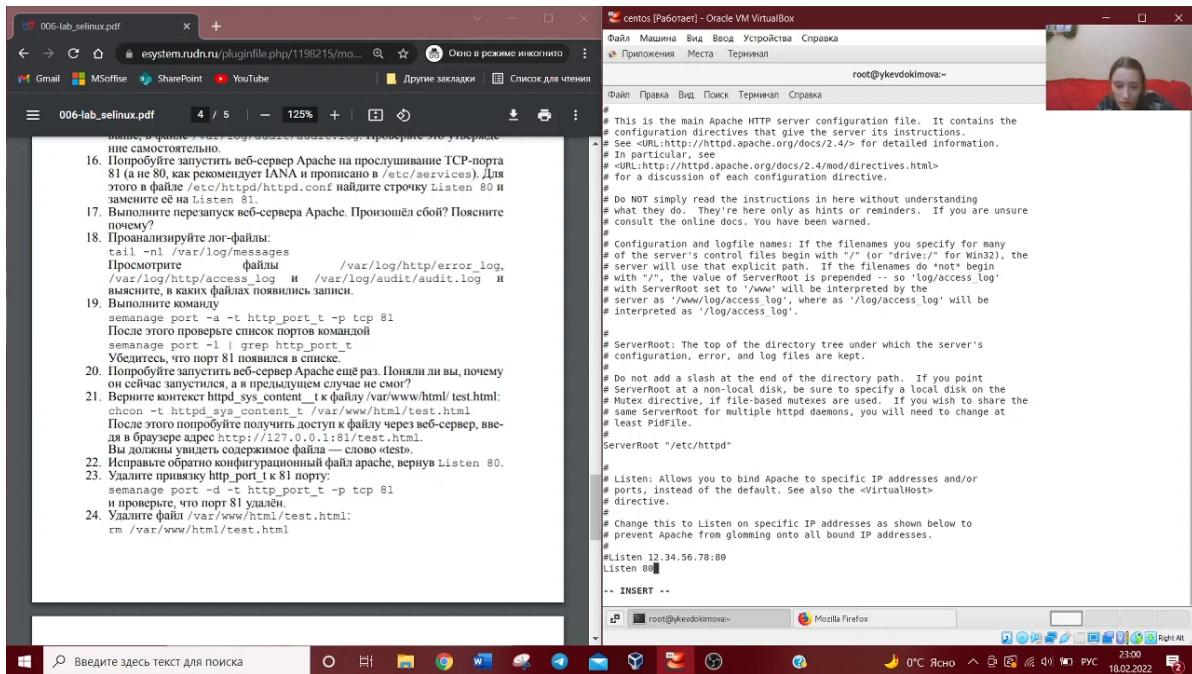


Figure 2.22: Исправление конфигурационного файла apache

18. Удалила привязку http_port_t к 81 порту.

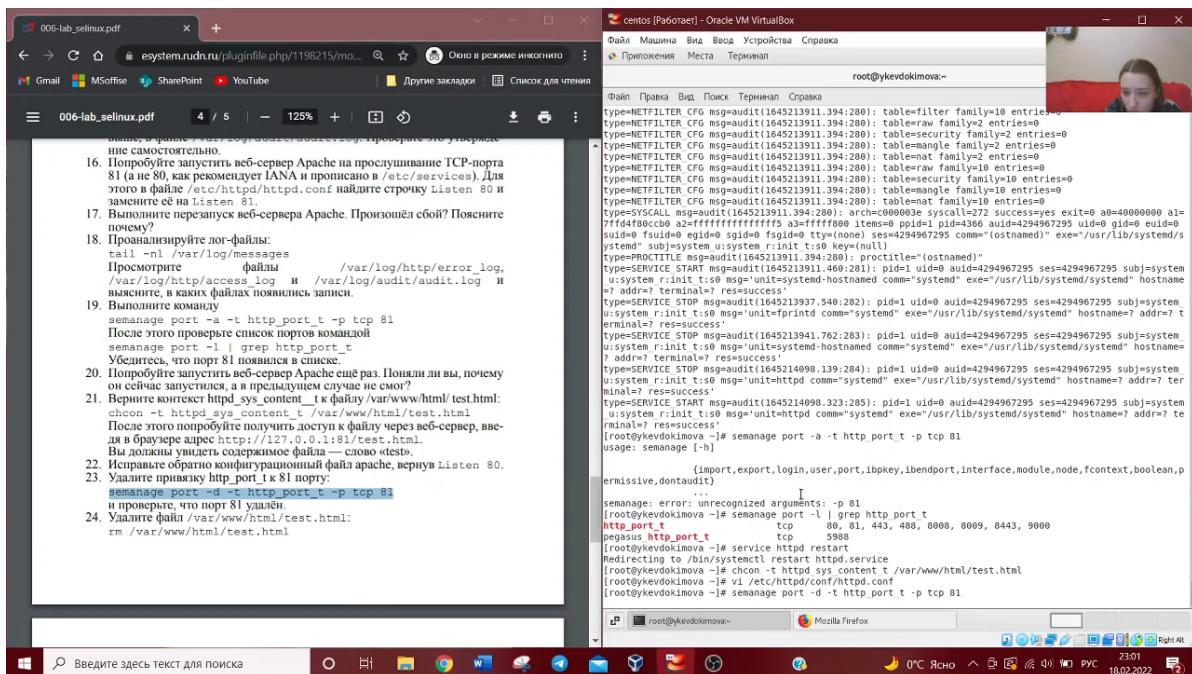


Figure 2.23: Удаление привязки http_port_t к 81 порту

19. Удалила файл /var/www/html/test.html.

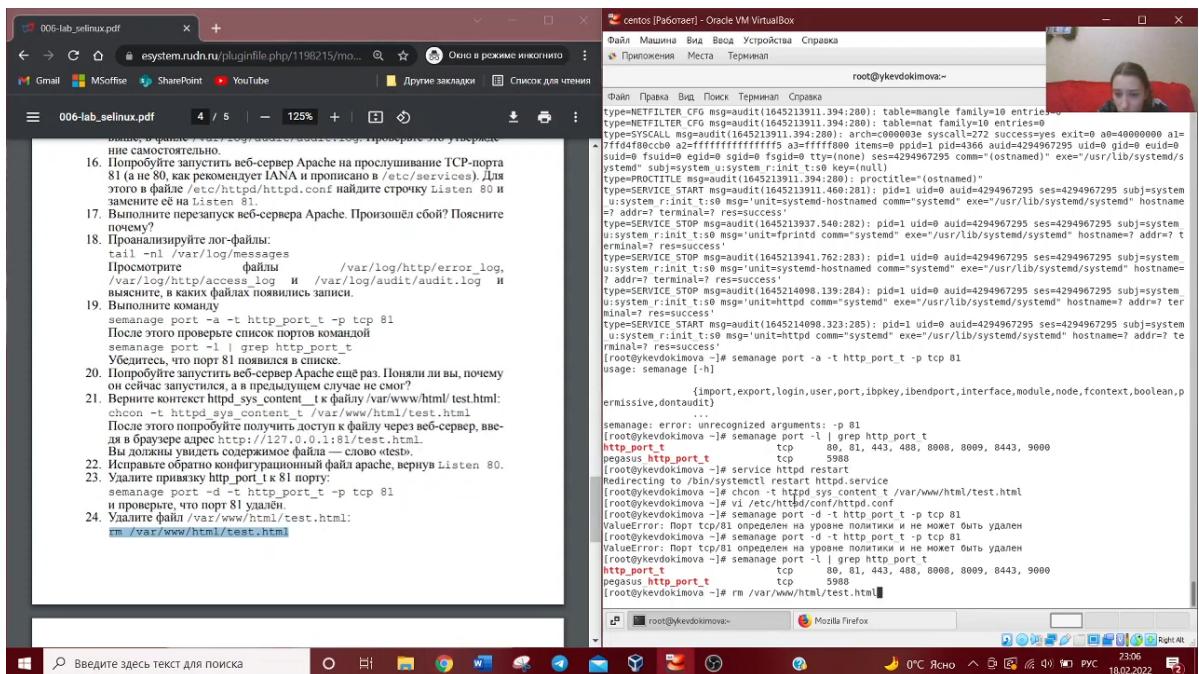


Figure 2.24: Удаление файла /var/www/html/test.html

3 Выводы

На основе проделанной работы развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux. Проверила работу SELinux на практике совместно с веб-сервером Apache.