Отчёт по лабораторной работе №6

дисциплина: Информационная безопасность

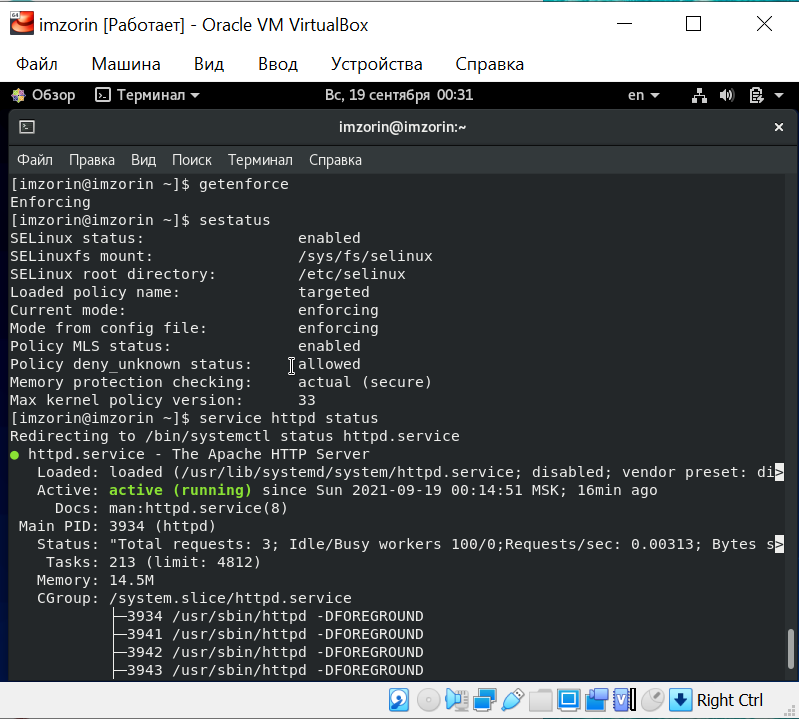
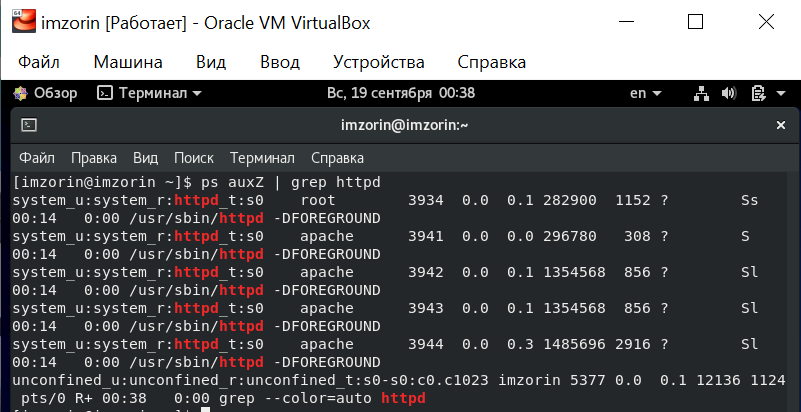
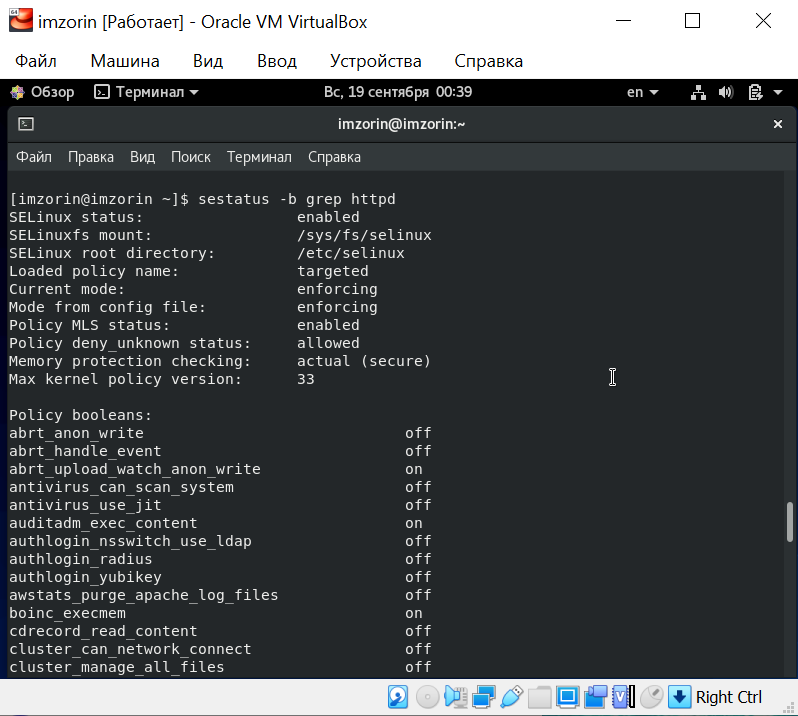
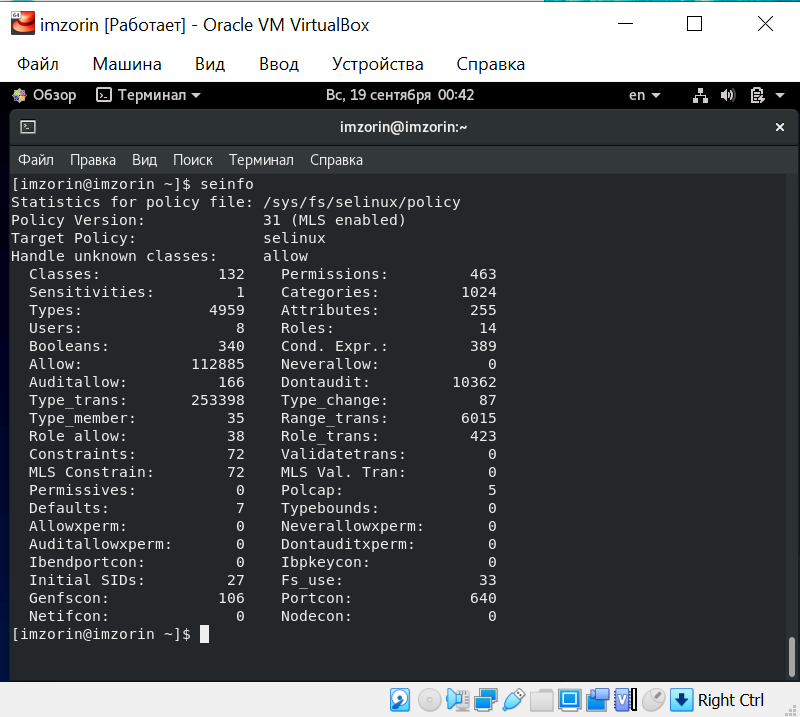
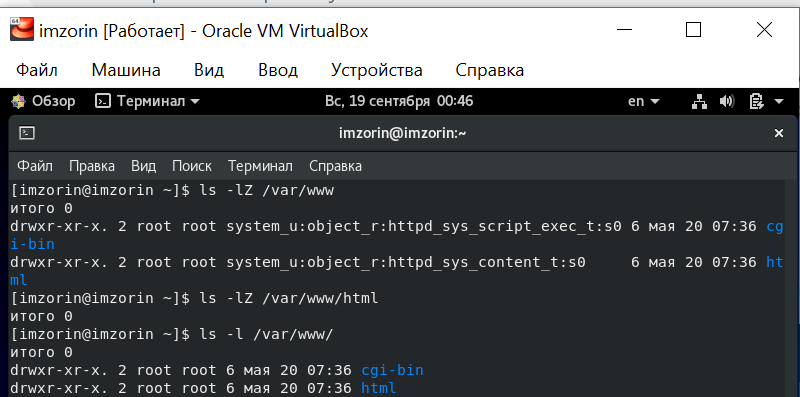
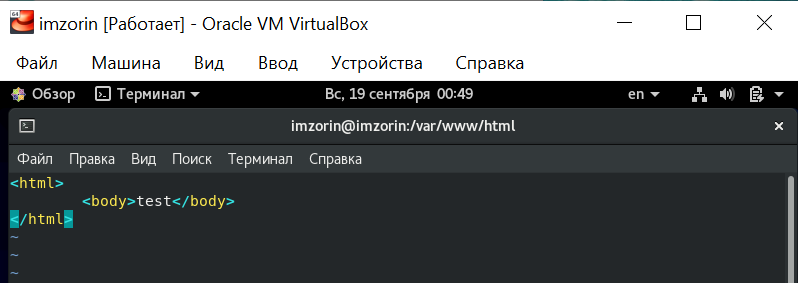
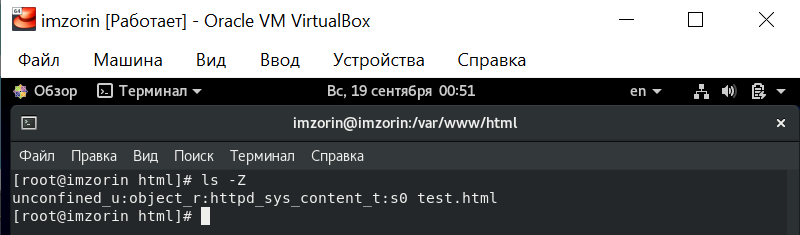
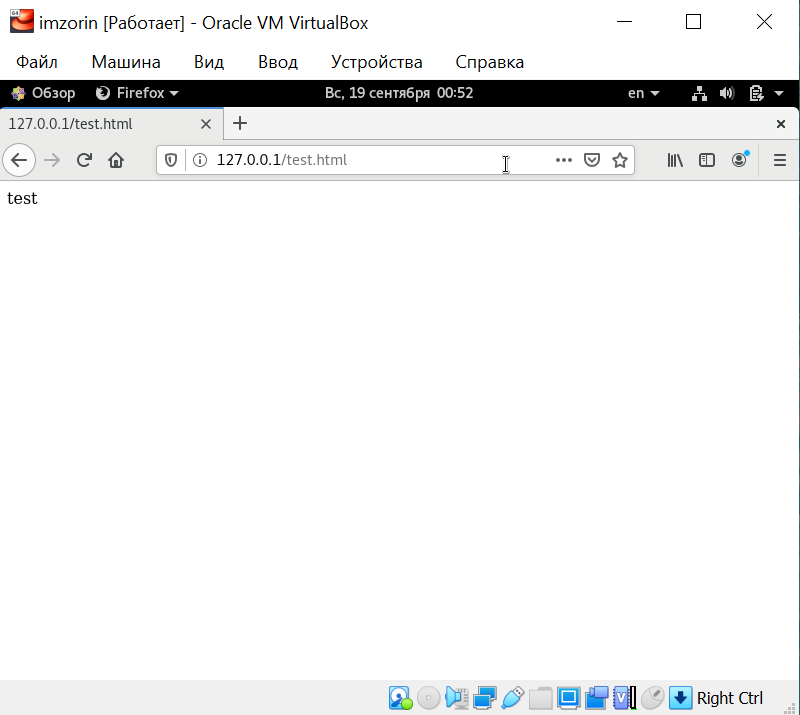
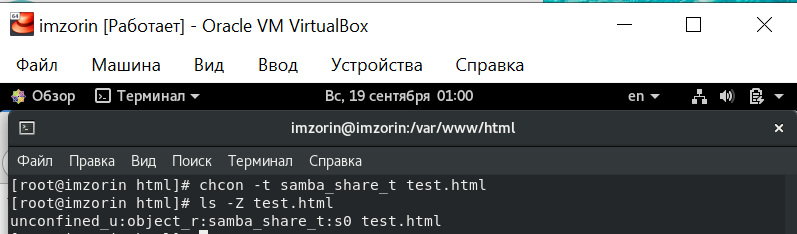
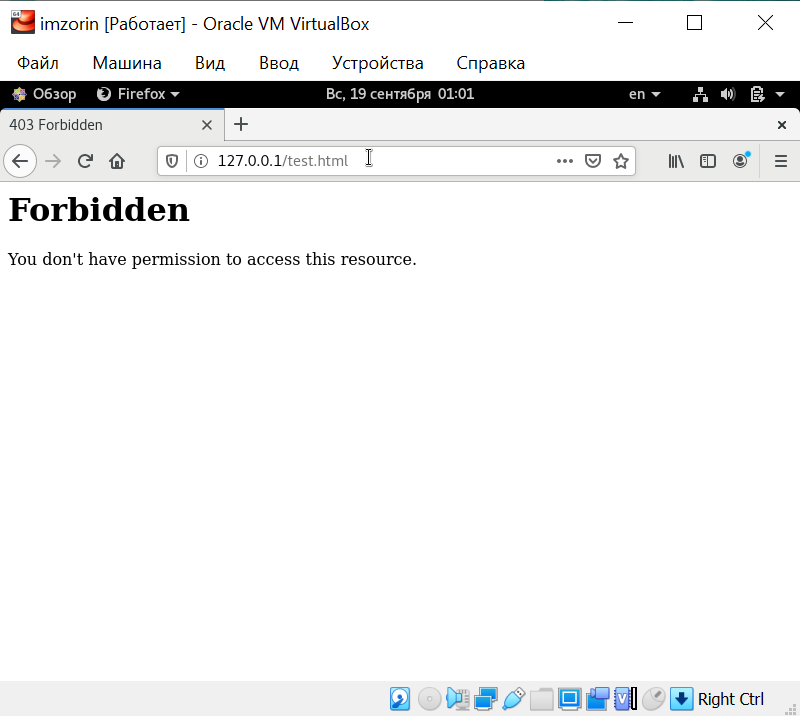
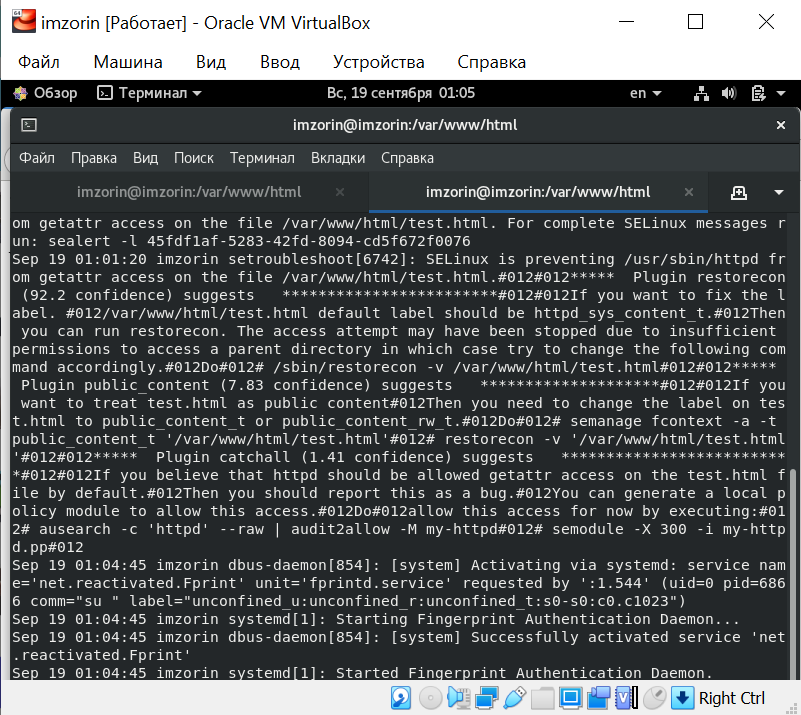
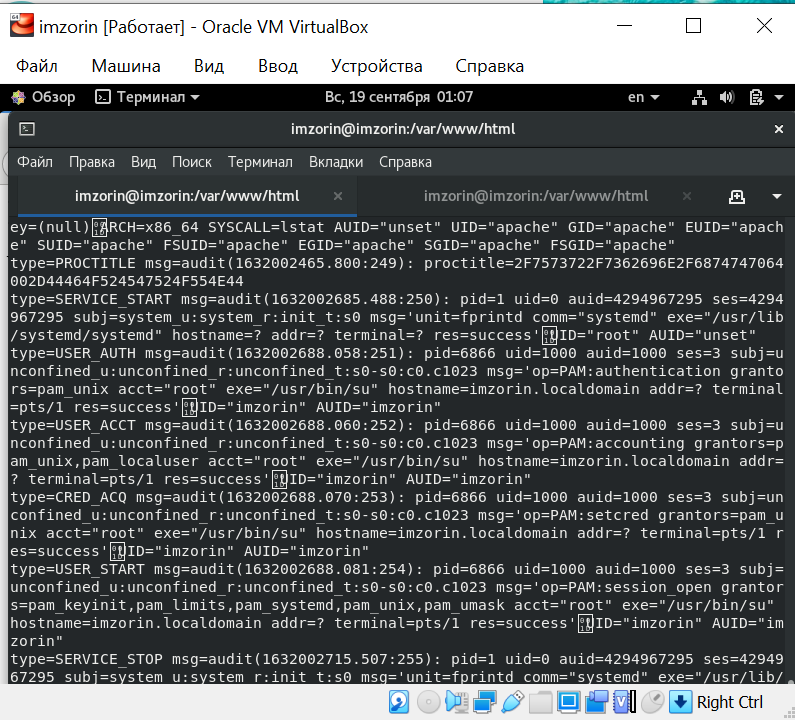
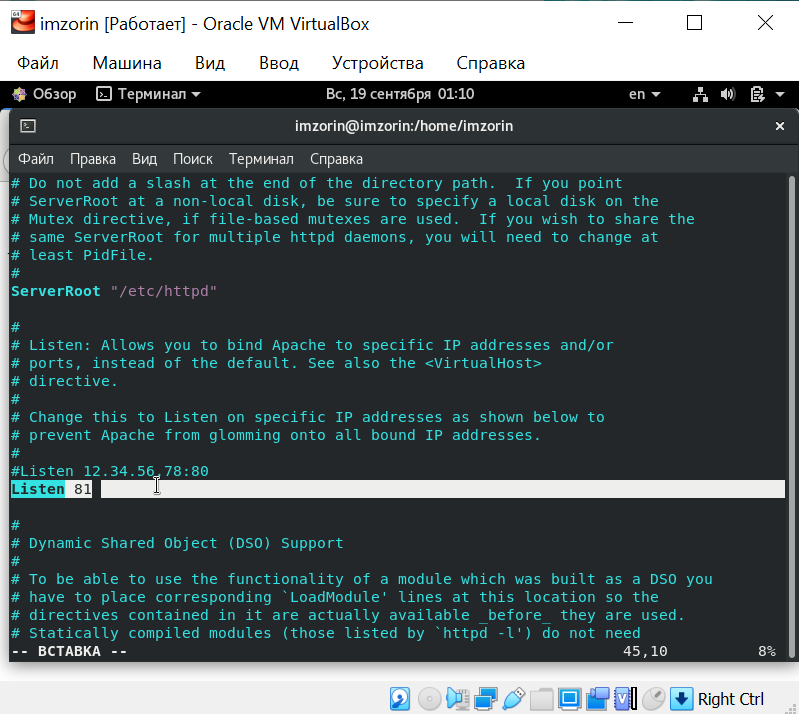
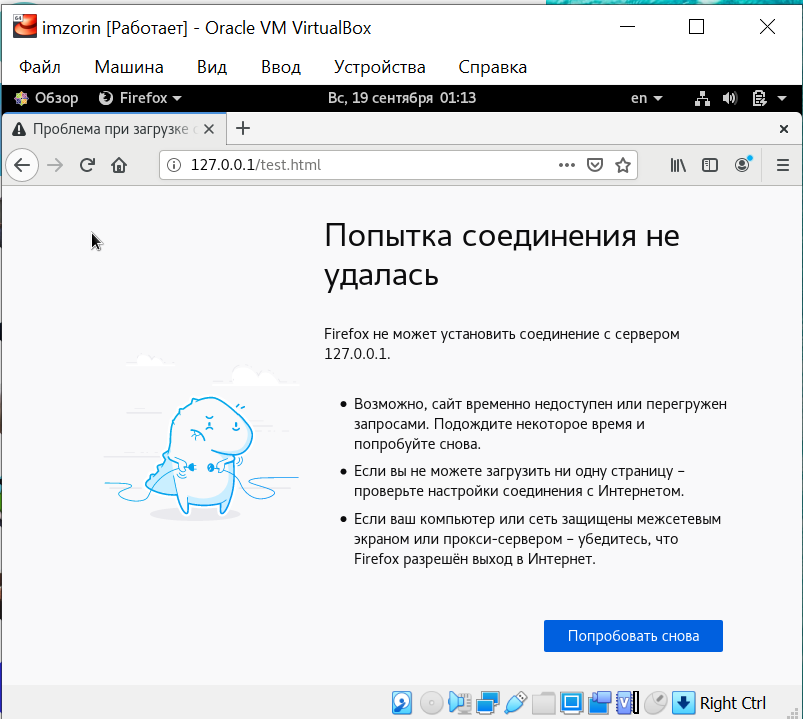
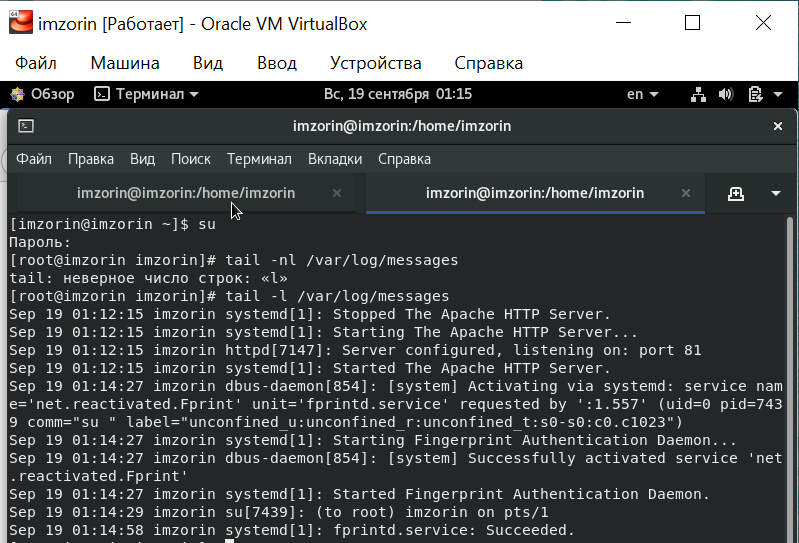
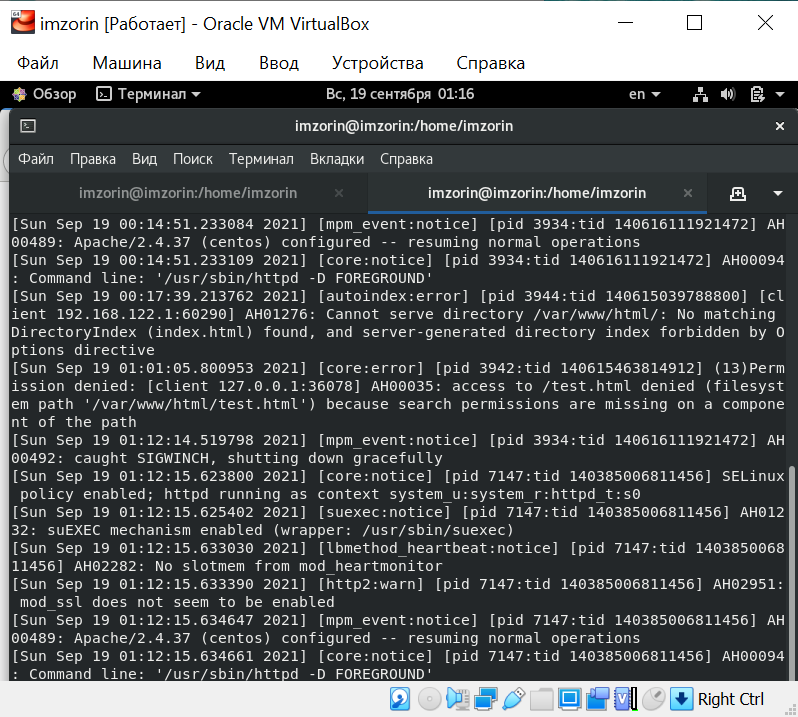
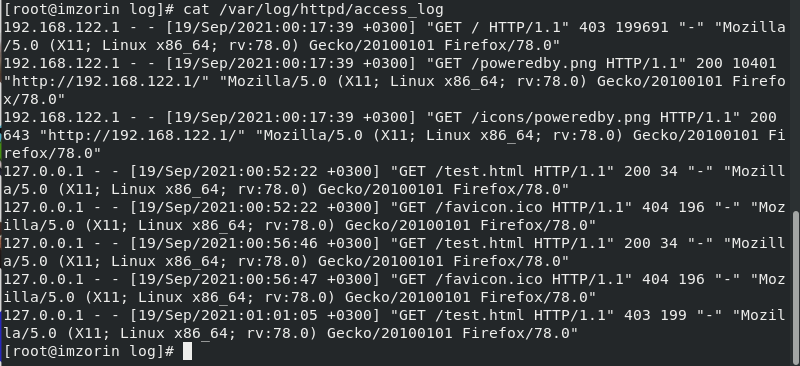
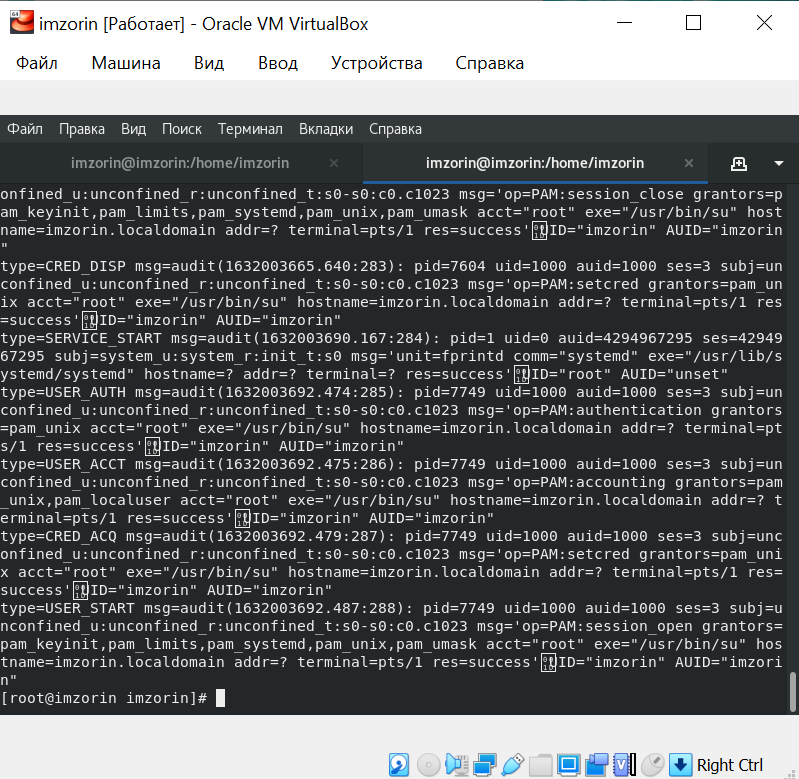
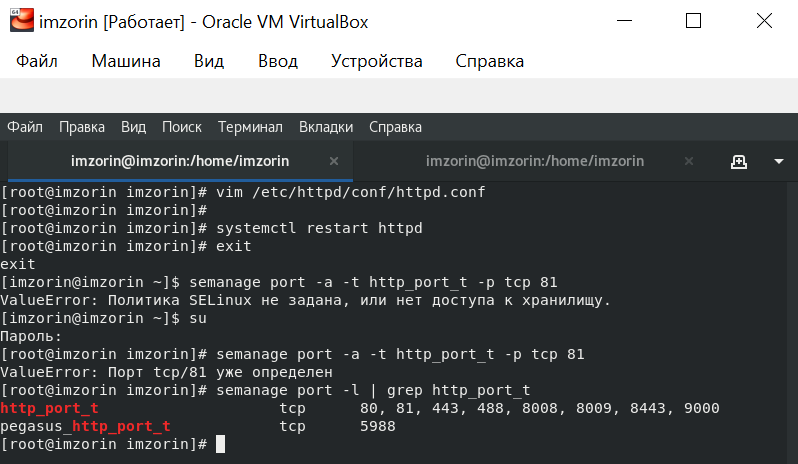
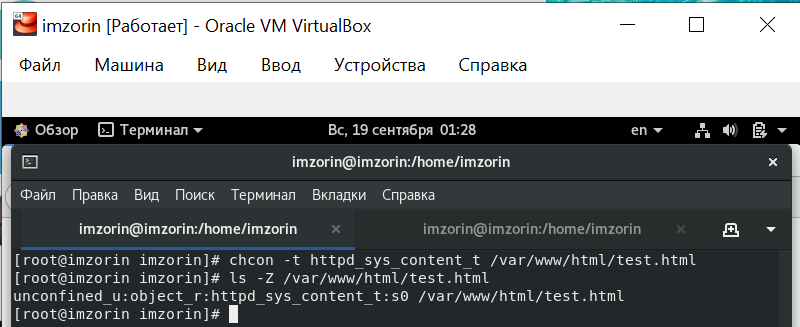
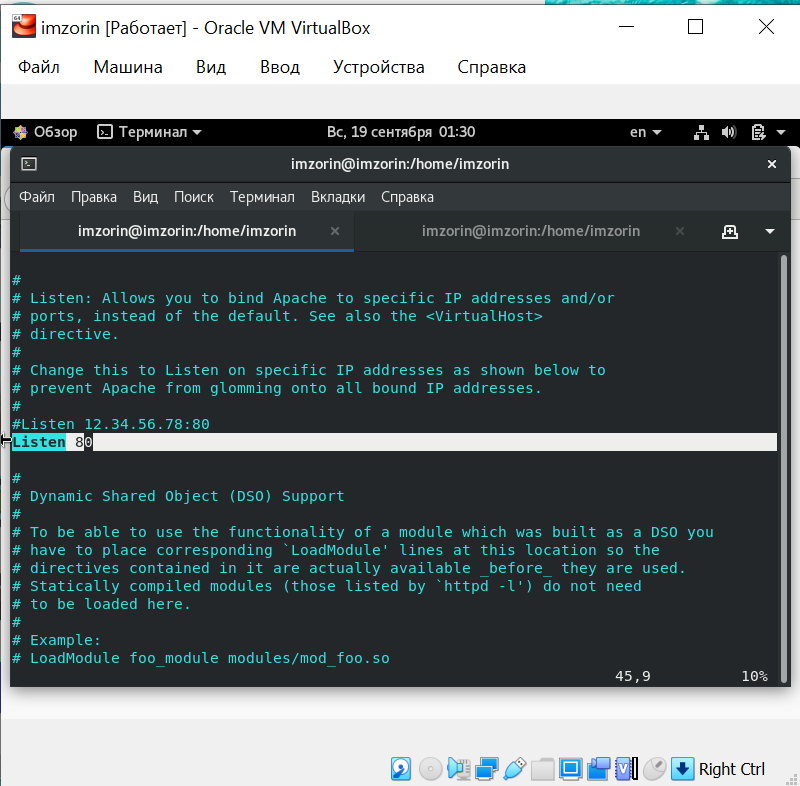
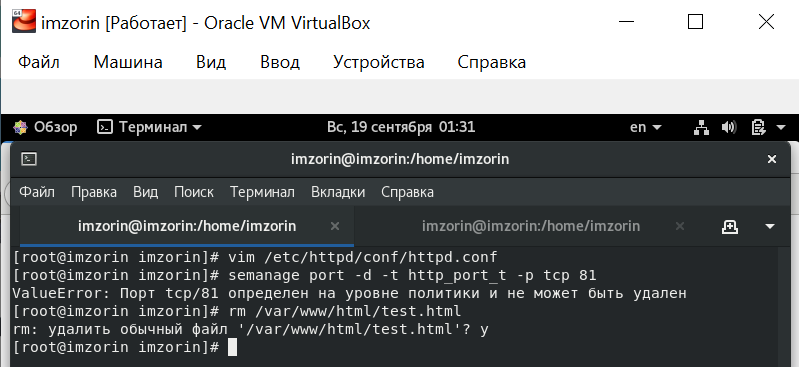
Зорин Илья Михайлович

Содержание

# Цель работы

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

# Выполнение лабораторной работы

1. Вошёл в систему с полученными учётными данными и убедился, что SELinux работает в режиме enforcing политики targeted. Обратился с помощью браузера к веб-серверу, запущенному на компьютере, и убедился, что последний работает (рис. 1). 
2. Нашёл веб-сервер Apache в списке процессов, определил его контекст безопасности и занёс эту информацию в отчёт (рис. 2).  
   
3. Посмотрел текущее состояние переключателей SELinux для Apache (рис. 3). 
4. Посмотрел статистику по политике с помощью команды seinfo, также определил множество пользователей, ролей, типов (рис. 4). 
5. Определил тип файлов и поддиректорий, находящихся в директории /var/www. Определил тип файлов, находящихся в директории /var/www/html. Определил круг пользователей, которым разрешено создание файлов в директории (рис. 5). 
6. Создал от имени суперпользователя html-файл (рис. 6). 
7. Проверил контекст созданного файла. Контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html: httpd\_sys\_content (рис. 7). 
8. Обратился к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедился, что файл успешно отображён (рис. 8). 
9. Изменил контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на samba\_share\_t. После этого проверил, что контекст поменялся (рис. 9). 
10. Попробовал ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html (рис. 10). 
11. Проанализировал ситуацию. Почему файл не был отображён,если права доступа позволяют читать этот файл любому пользователю? Просмотрел log-файлы веб-сервера Apache. Также просмотрите системный лог-файл. 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. 11-12).  
12. Попробовал запустить веб-сервер Apache на прослушивание ТСР-порта 81. Для этого в файле /etc/httpd/httpd.conf нашёл строчку Listen 80 и заменил её на Listen 81 (рис. 13). 
13. Выполнил перезапуск веб-сервера Apache. Произошёл сбой. Поясните почему? (рис. 14). 
14. Проанализировал лог-файлы. Просмотрел 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. 15-18).    
15. Выполнил команду semanage port -a -t http\_port\_t -р tcp 81. После этого проверил список портов. Убедился, что порт 81 появился в списке (рис. 19). 
16. Вернул контекст httpd\_sys\_cоntent\_\_t к файлу/var/www/html/test.html (рис. 20). 
17. Исправил обратно конфигурационный файл apache, вернув Listen80 (рис. 21). 
18. Удалил привязку http\_port\_t к 81 порту и проверил, что порт 81 удалён. Удалил файл /var/www/html/test.html (рис. 22). 

# Выводы

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinx на практике совместно с веб-сервером Apache.