Лабораторная работа № 6

Мандатное разграничение прав в Linux

Заболотная Кристина Александровна

Содержание

1 Цель работы 1
2 Выполнение лабораторной работы 1
3 Выводы 7
Список литературы 7

1 Цель работы

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

2 Выполнение лабораторной работы

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

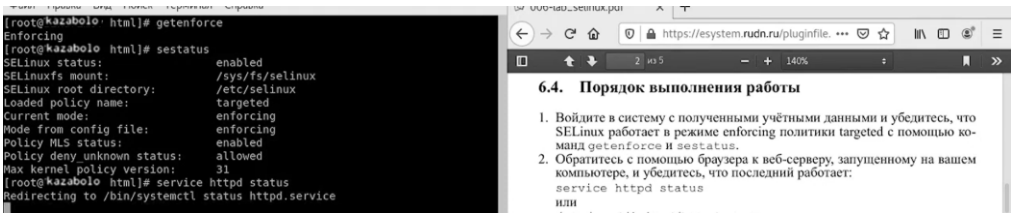

Рис. 1: getenforce, sestatus

Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: service httpd status

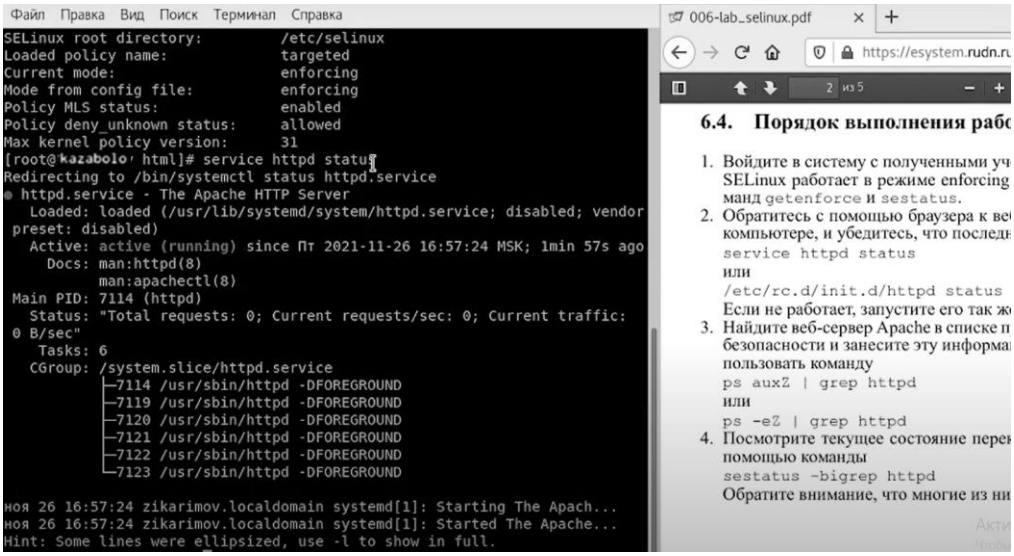

Рис. 2: service httpd status

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

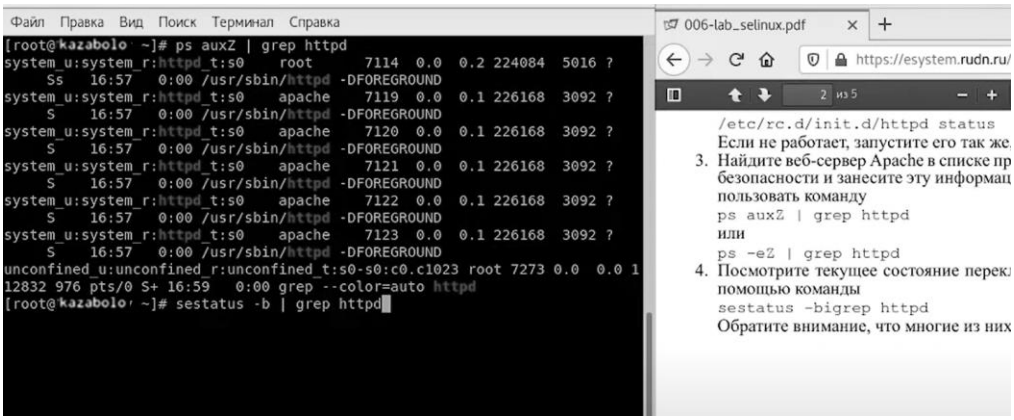

Рис. 3: ps auxZ | grep httpd

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

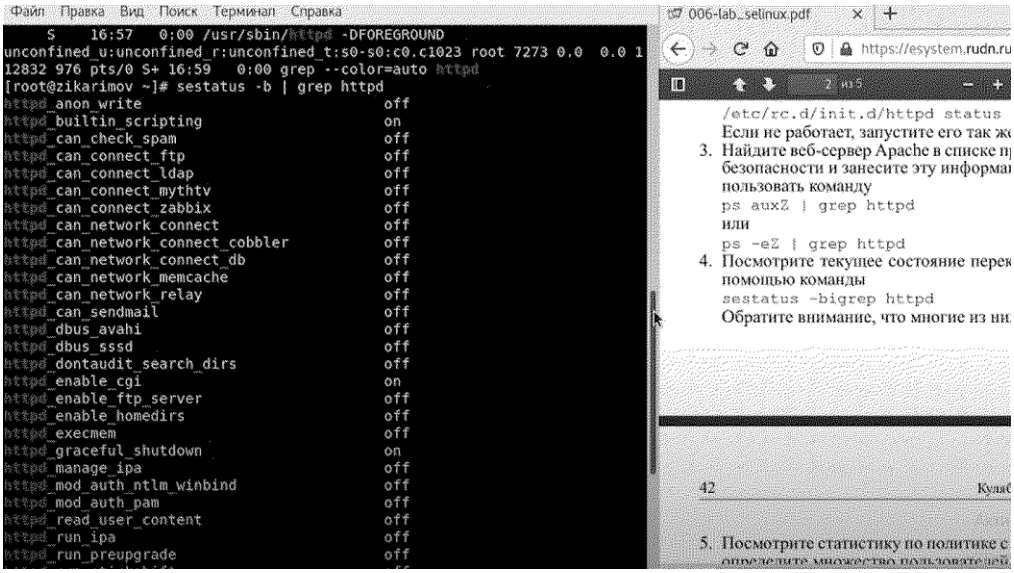

Рис. 4: ps auxZ | grep httpd

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

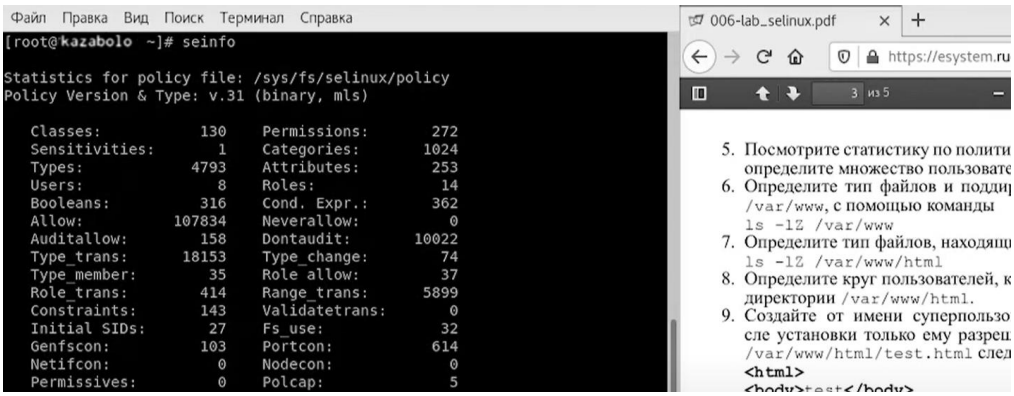

Рис. 5: seinfo

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

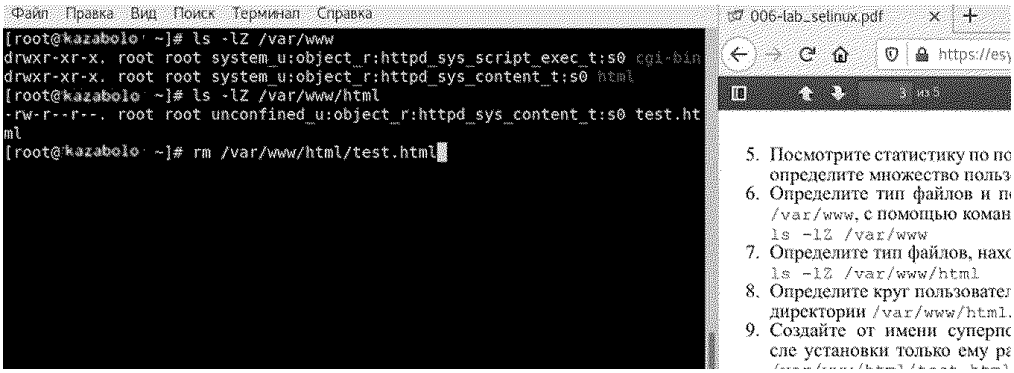

Рис. 6: /var/www

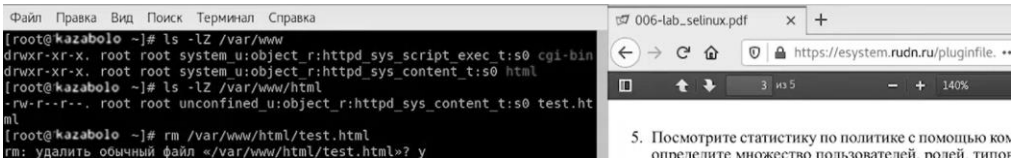

Рис. 7: /var/www

Рис. 8: /var/www

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

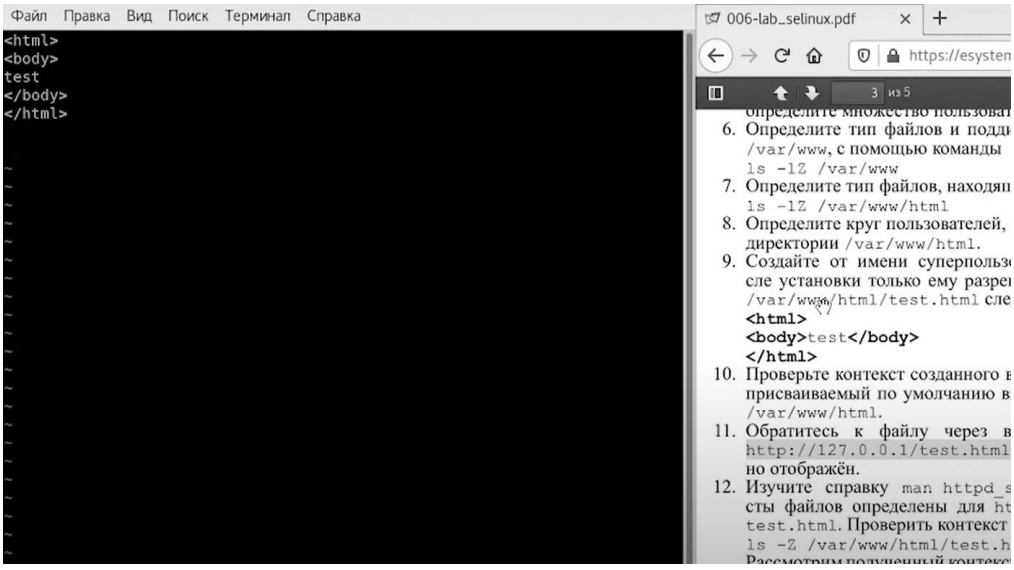

Рис. 9: /var/www/html/test.html

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

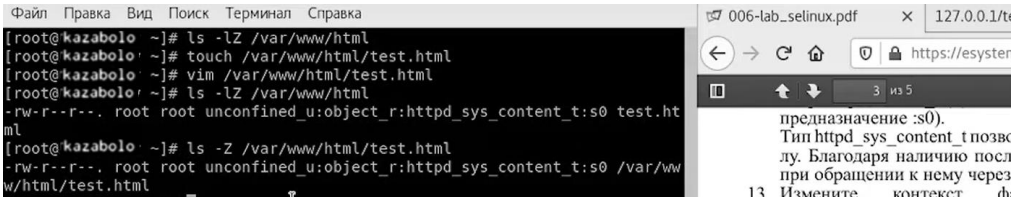

Рис. 10: /var/www/html

chon -t samba_share_t /var/www/html/test/html

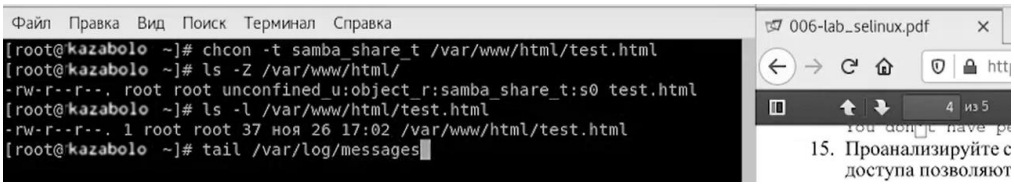

Рис. 11: chon -t samba_share_t /var/www/html/test/html

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

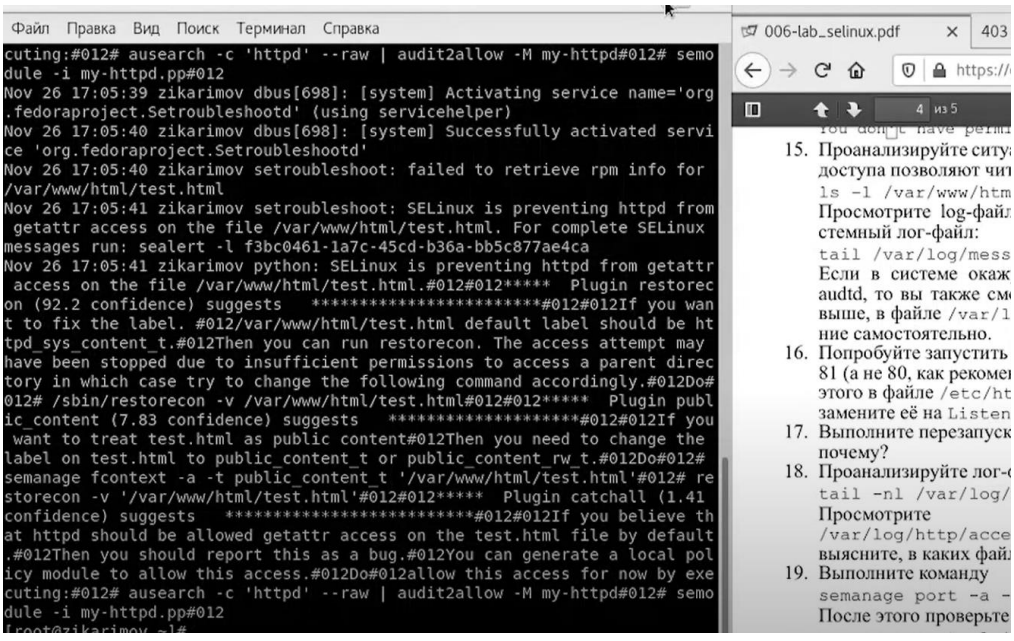

Рис. 12: result

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

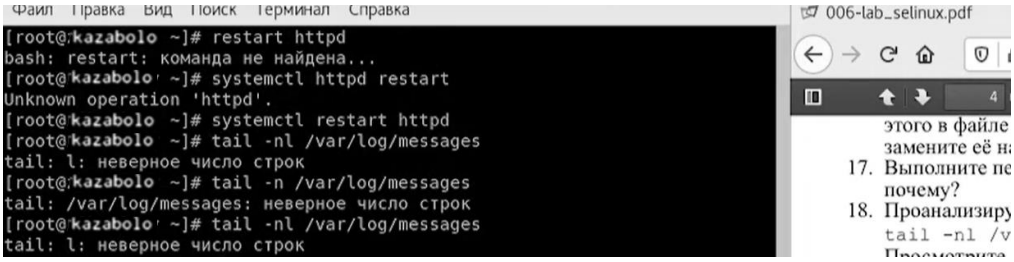

Рис. 13: tail /var/log/messages

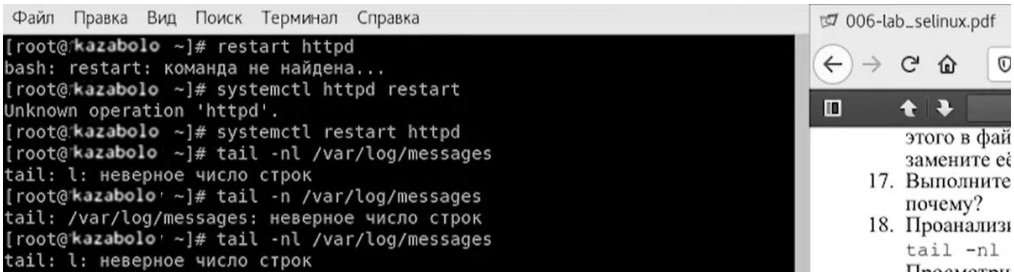

Рис. 14: tail /var/log/messages

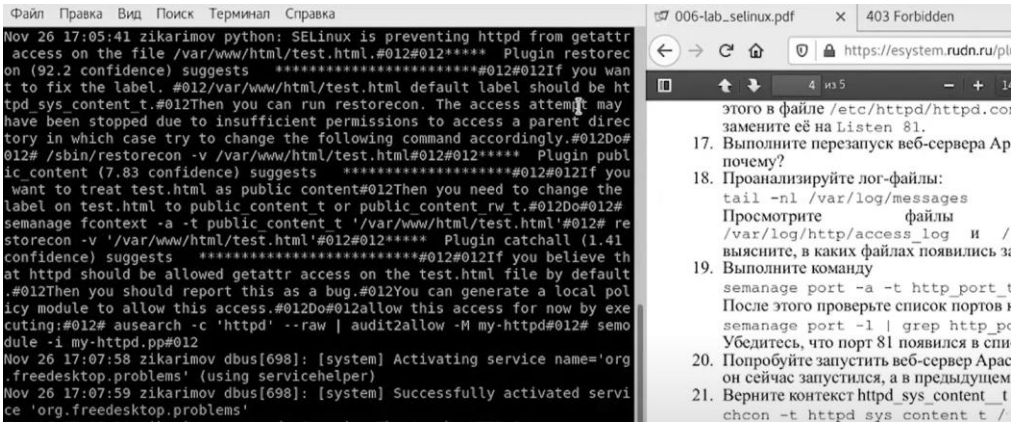

Рис. 15: result

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.htm.

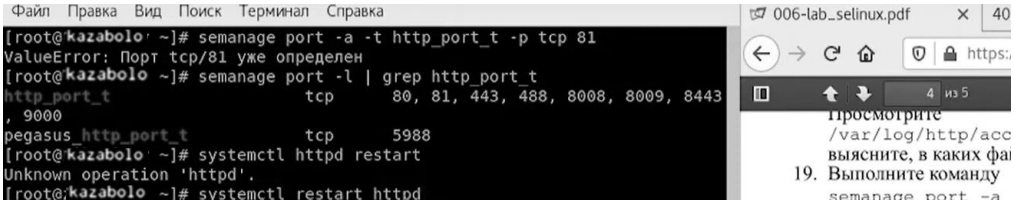

Рис. 16: semanage port -d -t http_port_t -p tcp 81

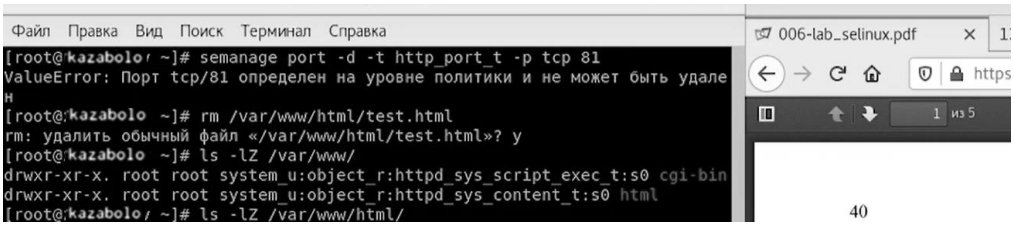

Рис. 17: ls -lz /var/www/html

3 Выводы

В ходе выполнения данной лабораторной работы были развиты навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinx на практике совместно с веб-сервером Apache.

Список литературы