Лабораторная работа №6

Мандатное разграничение прав в Linux

Топонен Никита Андреевич

Содержание

# Цель работы

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

# Задание

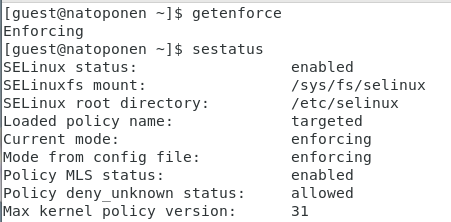
Выполнить задания из лабораторной работы и проанализировать полученные результаты.

# Теоретическое введение

Для выполнения данной лабораторной нет специальной теории. Необходимы общие знания в области компьютерных наук.

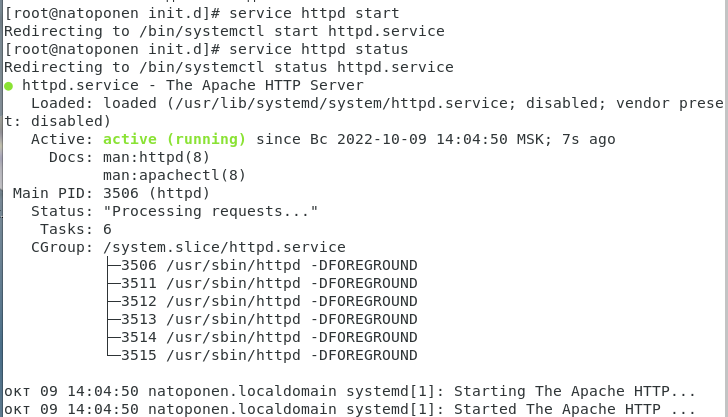
# Выполнение лабораторной работы

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



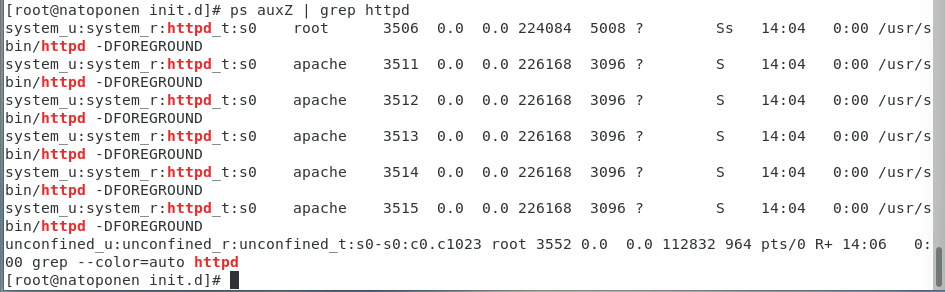
Режим и политика SELinux

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.



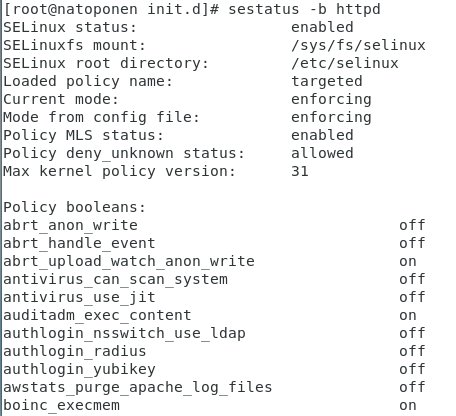
Запуск Apache web server

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



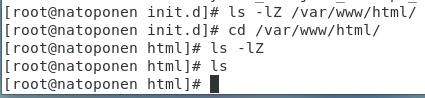
Контекст безопасности Apache web server

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



Текущее состояние переключателей SELinux для Apache

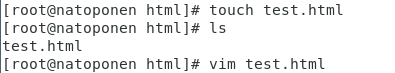
Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www



Тип файлов и поддиректорий

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>



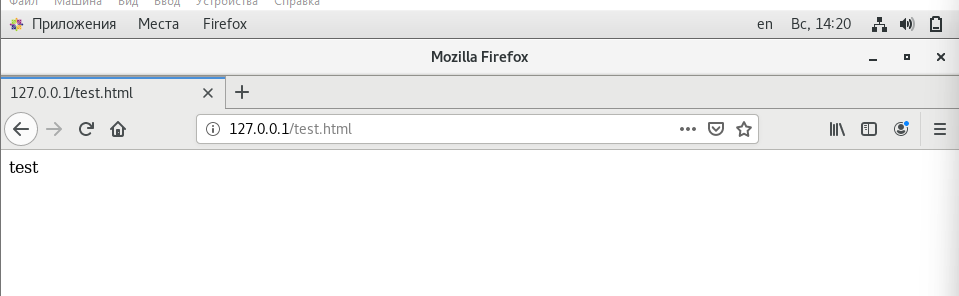
Создание файла test.html

Проверьте контекст созданного вами файла.

Контекст файла test.html

Контекст файла test.html

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



Веб страница

Проверить контекст файла можно командой ls -Z. ls -Z /var/www/html/test.html

Контекст файла test.html

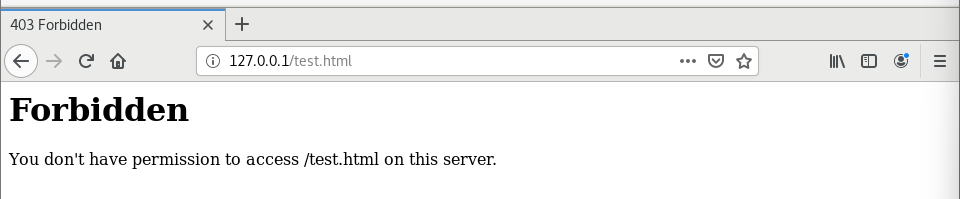
Контекст файла test.html

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

Изменения контекста файла test.html

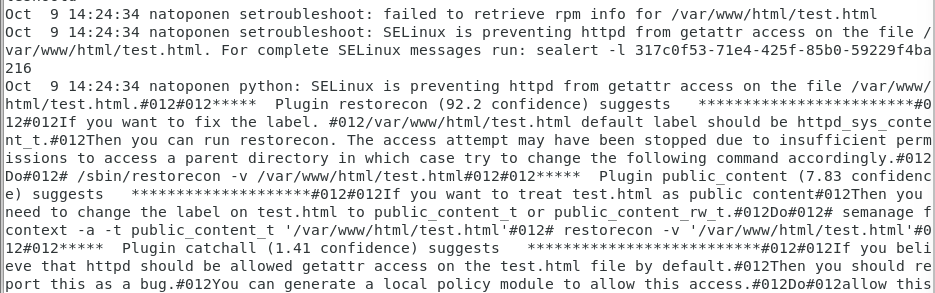
Изменения контекста файла test.html

Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html

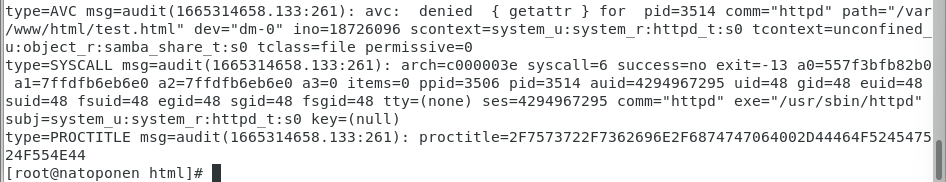


Доступ к странице запрещен

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.

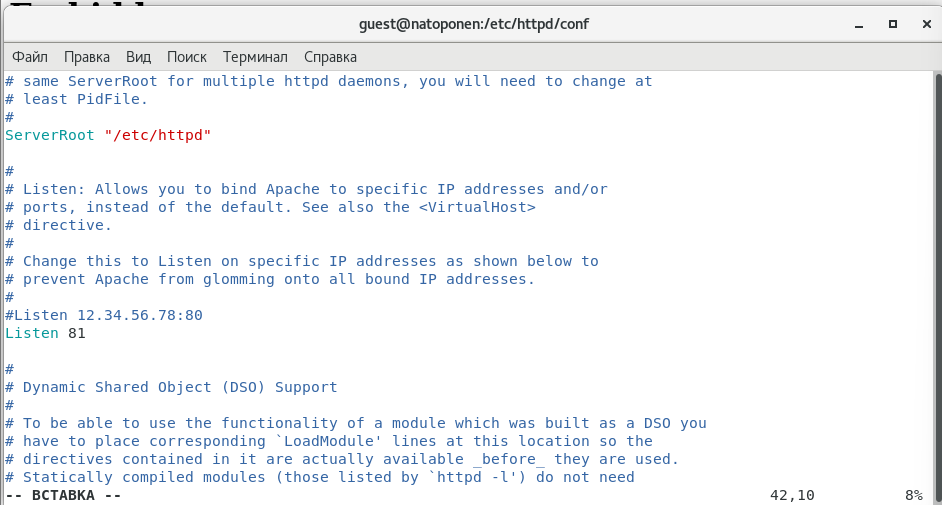


Логи веб сервера

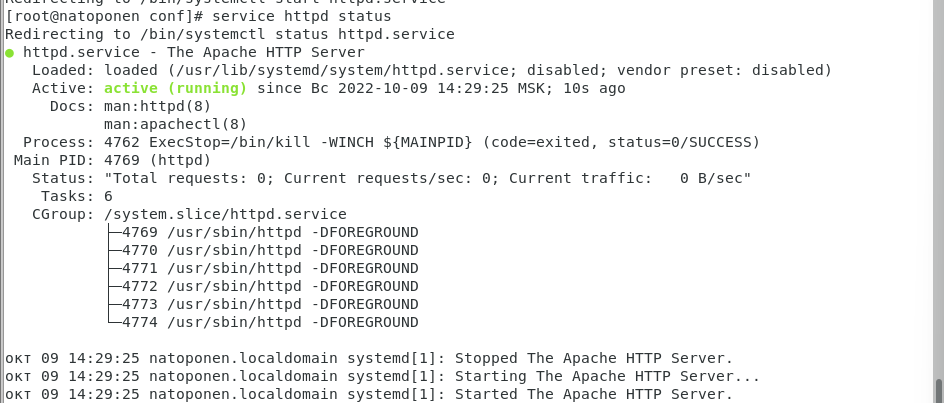


Audit логи

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.



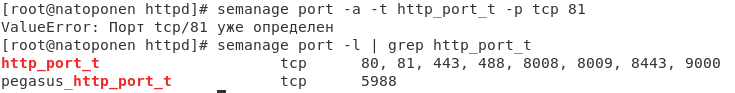
Смена порта



Запуск на 81 порту

Сервер успешно запустился на 81 порту.

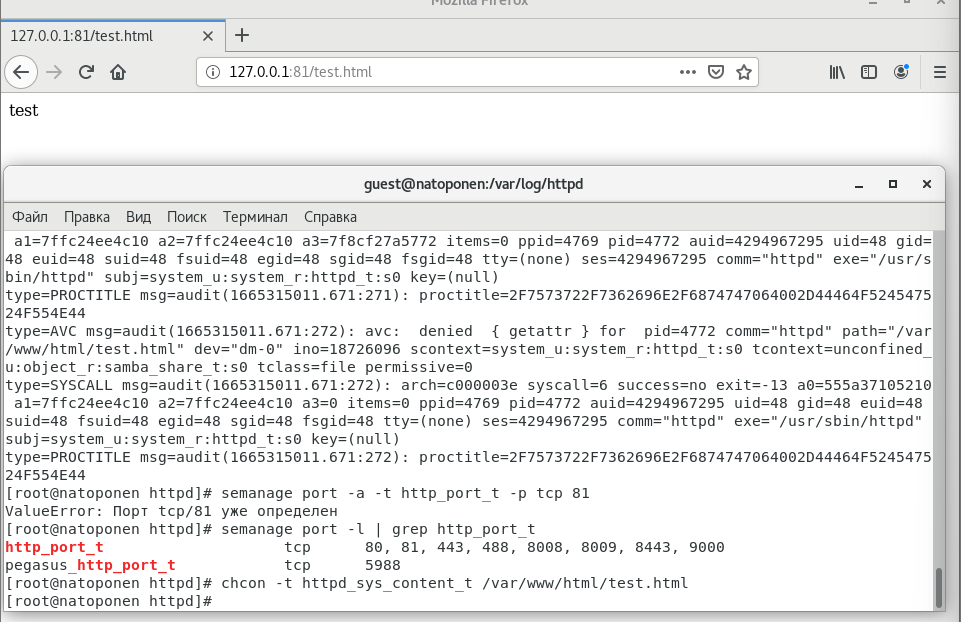
Выполните команду semanage port -a -t http\_port\_t -р tcp 81 После этого проверьте список портов командой semanage port -l | grep http\_port\_t



Установление порта

Порт уже был определен.

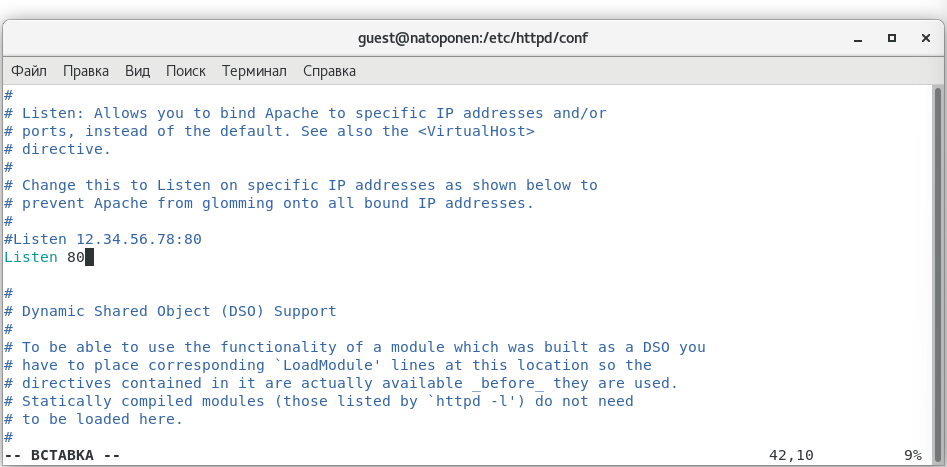
Верните контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/ test.html: chcon -t httpd\_sys\_content\_t /var/www/html/test.html После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. Вы должны увидеть содержимое файла — слово «test».



Работа веб сервера на 81 порту

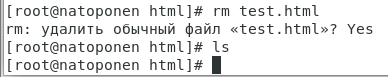
Исправьте обратно конфигурационный файл apache, вернув Listen 80.

Удалите привязку http\_port\_t к 81 порту: semanage port -d -t http\_port\_t -p tcp 81 и проверьте, что порт 81 удалён.

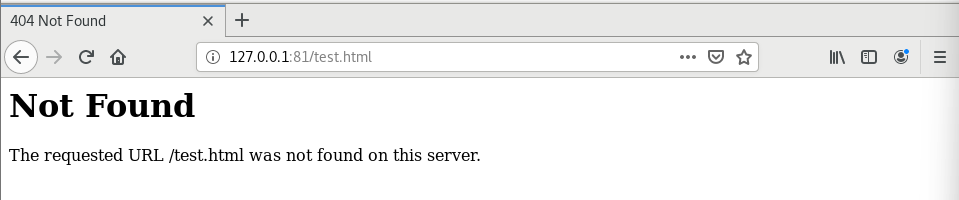


Возвращение к 80 порту

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



Удаление файла страницы



Результат работы сервера после удаления

# Выводы

В ходе данной лабораторной работы я развил навыки администрирования ОС Linux, получил первое практическое знакомство с технологией SELinux, проверил работу SELinx на практике совместно с веб-сервером Apache.

# Список литературы

* [Кулябов Д. С., Королькова А. В., Геворкян М. Н Лабораторная работа №6](https://esystem.rudn.ru/pluginfile.php/1651755/mod_resource/content/2/006-lab_selinux.pdf)