Лабораторная работа №6

Оснновы информационной безопасности

Сабралиева Марворид Нуралиевна

Содержание

# 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

## 2.1 Подготовка

1. Установили httpd
2. Задали имя сервера
3. Открыли порты для работы с протоколом http

## 2.2 Изучение механики SetUID

1. Войдем в систему с полученными учётными данными и убедимся, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus.
2. Обратимся с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедимся, что последний работает: service httpd status или /etc/rc.d/init.d/httpd status Если не работает, запустить его можно так же, но с параметром start.

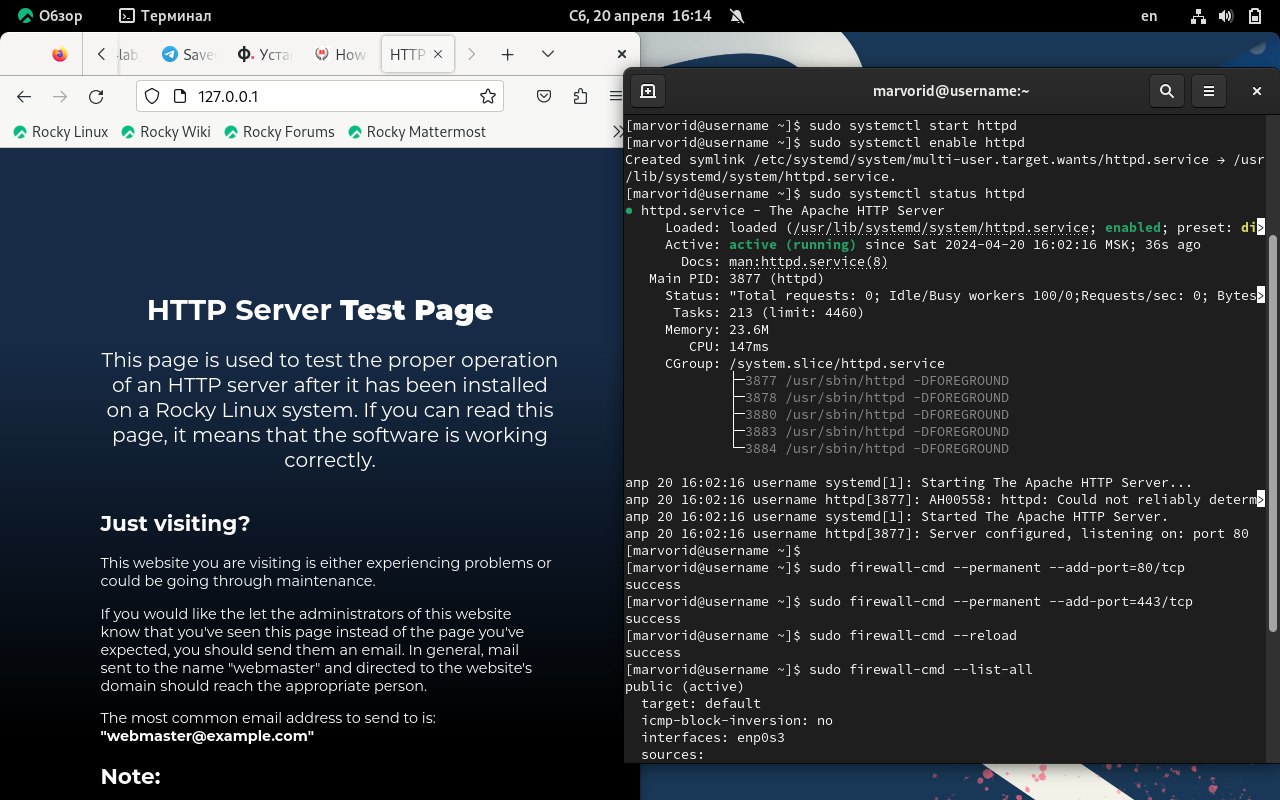


Figure 1: запуск http

1. Найдем веб-сервер Apache в списке процессов, определите его контекст безопасности. Например, можно использовать команду ps auxZ | grep httpd или ps -eZ | grep httpd (рис. [2](#fig:002)).

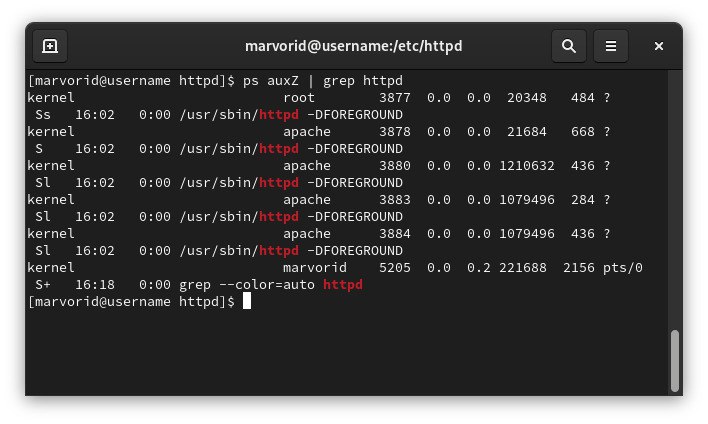


Figure 2: контекст безопасности http

1. Посмотрим текущее состояние переключателей SELinux для Apache с помощью команды sestatus -bigrep httpd. Обратим внимание, что многие из них находятся в положении «off». (рис. [3](#fig:003)).

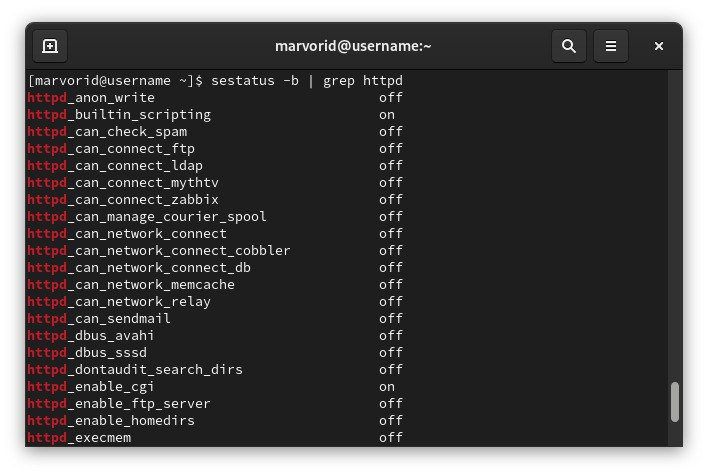


Figure 3: переключатели SELinux для http

1. Посмотрим статистику по политике с помощью команды seinfo, также определим множество пользователей, ролей, типов. (рис. [4](#fig:004)).

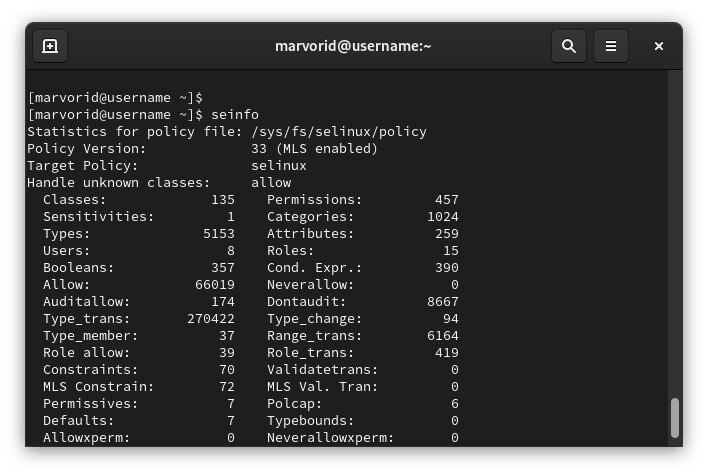


Figure 4: статистика по политике

1. Определим тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www
2. Определим тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html
3. Определим круг пользователей, которым разрешено создание файлов в директории /var/www/html.
4. Создадим от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания:

* test

1. Проверьте контекст созданного вами файла.
2. Обратитимся к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Файл был успешно отображён.

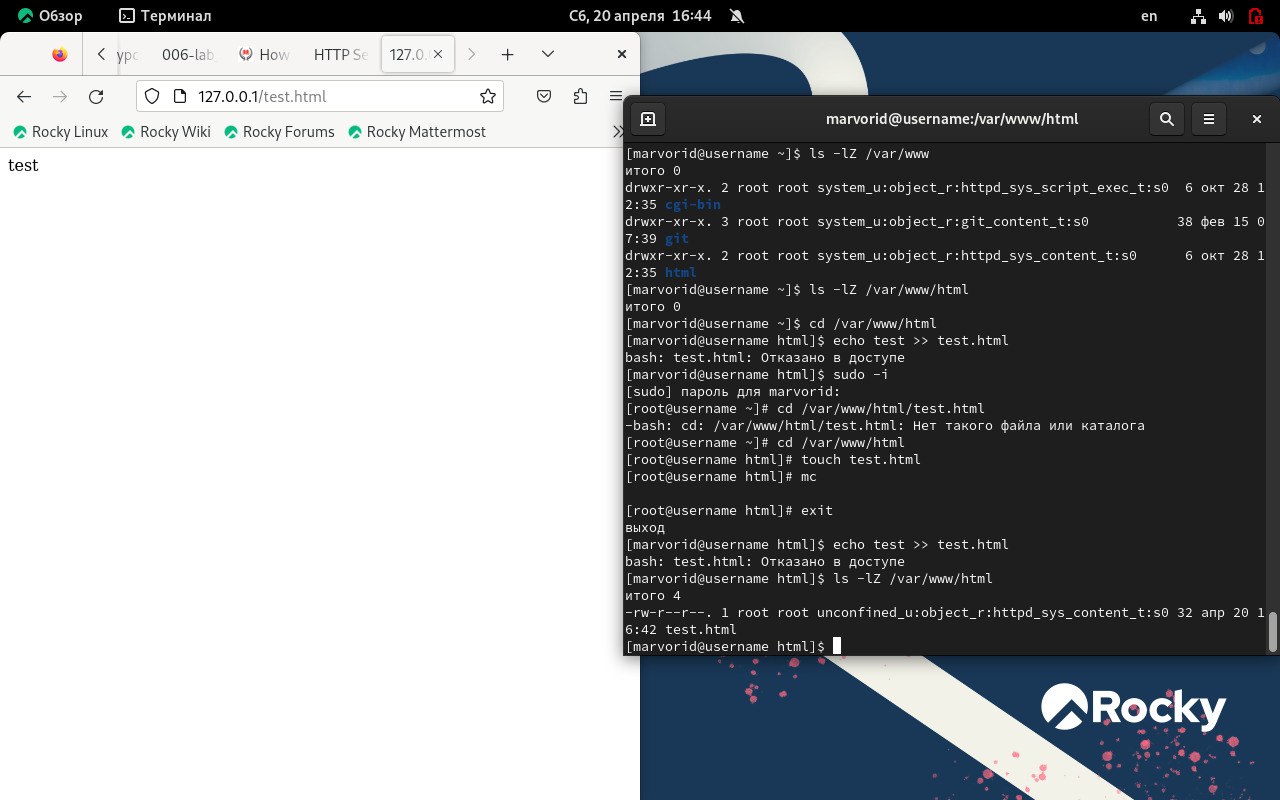


Figure 5: тип файлов и поддиректорий

1. Изучите справку man httpd\_selinux и выясните, какие контек- сты файлов определены для httpd. Сопоставьте их с типом файла test.html. (рис. [6](#fig:006)). Проверить контекст файла можно командой ls -Z. 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. Это первая часть контекста. Далее политика ролевого разделения доступа RBAC используется процессами, но не файлами, поэтому роли не имеют никакого значения для файлов. Роль object\_r используется по умолчанию для файлов на «постоянных» носителях и на сетевых файловых системах. (В директории к/ргос файлы, относящиеся к процессам, могут иметь роль system\_r. Если активна политика MLS, то могут использоваться и другие роли, например, secadm\_r. Данный случай мы рассматривать не будем, как и предназначение :s0). Тип httpd\_sys\_content\_t позволяет процессу httpd получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер.
2. 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. [7](#fig:007)).

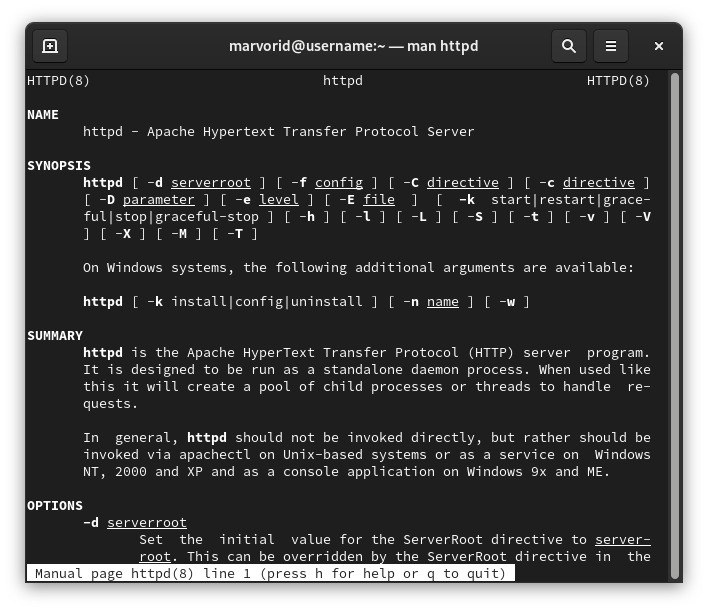


Figure 6: man httpd\_selinux

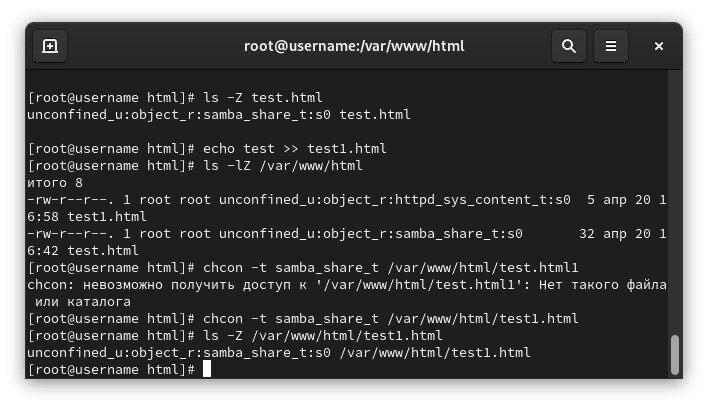


Figure 7: Изменение контекста файла

1. 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.
2. 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.

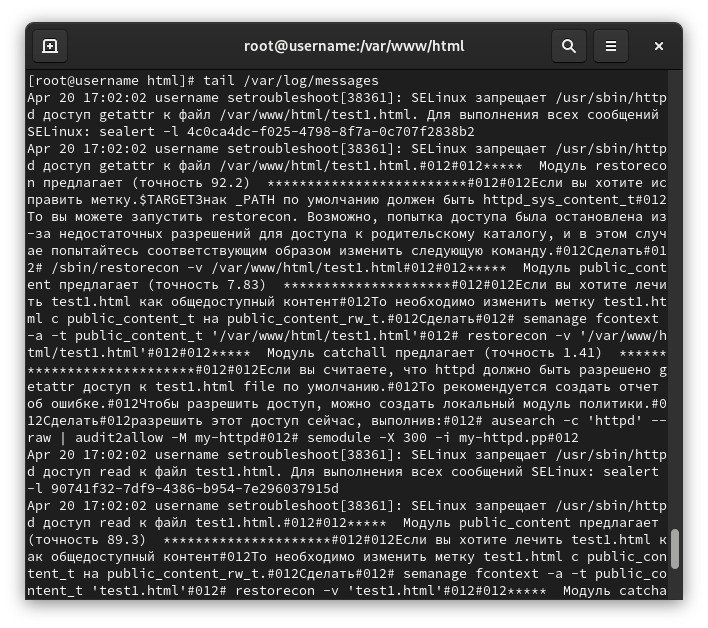


Figure 8: лог ошибок

1. 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. (рис. [9](#fig:009)).

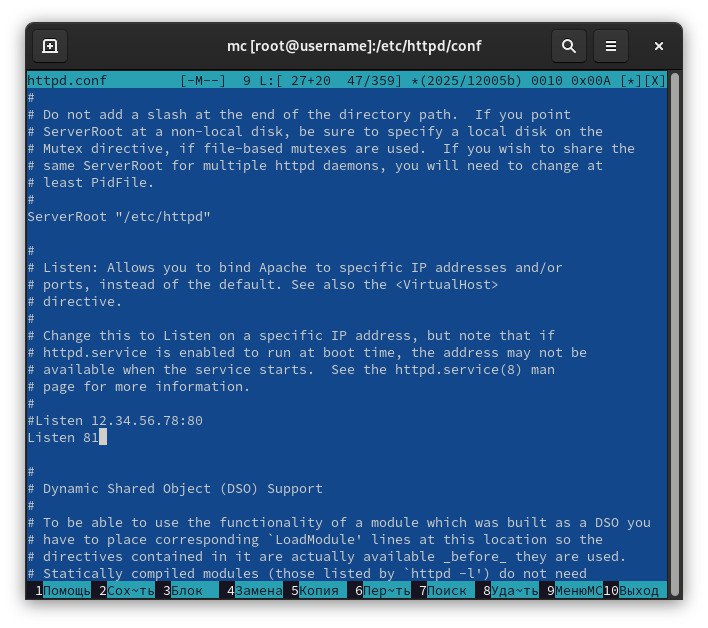


Figure 9: переключение порта

1. Выполним перезапуск веб-сервера Apache. Произошёл сбой? Сбой не происходит, порт 81 уже вписан в разрешенные
2. 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.
3. Выполним команду semanage port -a -t http\_port\_t -р tcp 81 После этого проверьте список портов командой semanage port -l | grep http\_port\_t Убедимся, что порт 81 появился в списке.
4. Попробуем запустить веб-сервер Apache ещё раз.
5. Вернем 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».

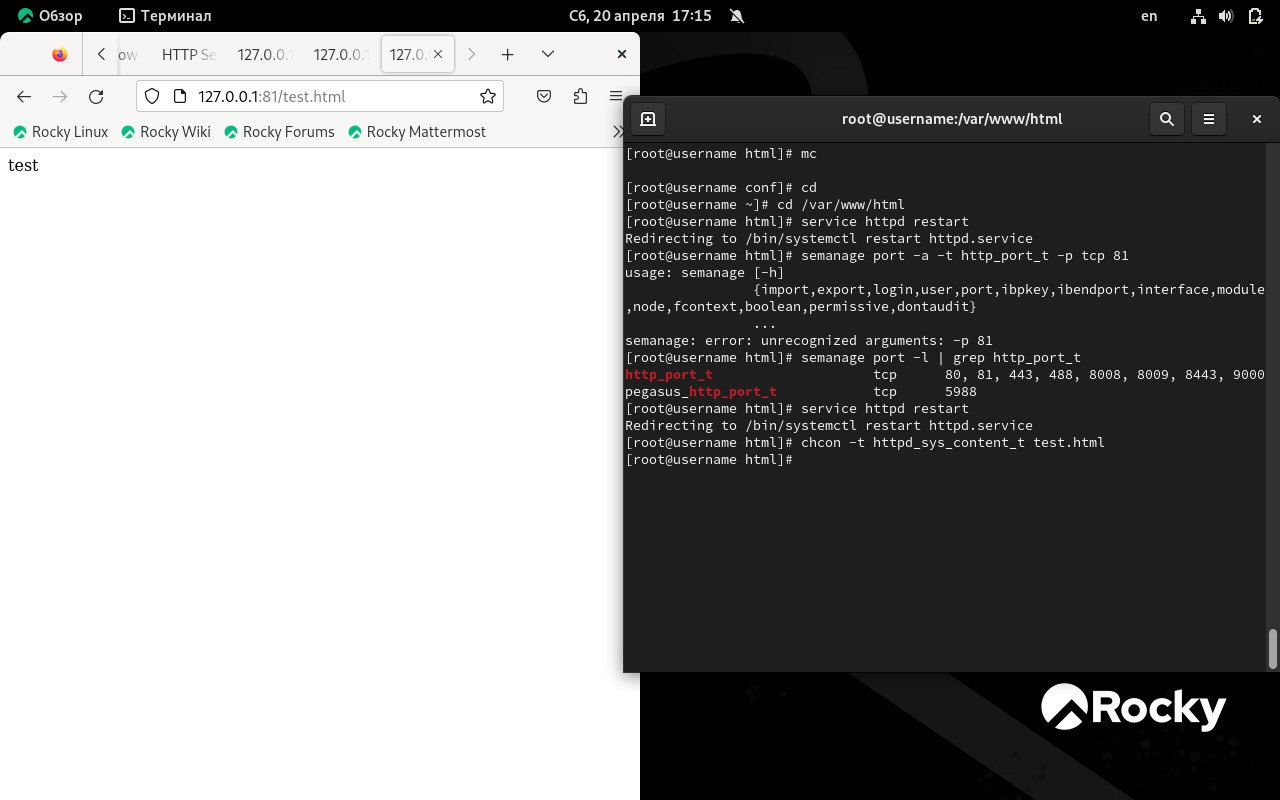


Figure 10: доступ по http на 81 порт

1. Исправьте обратно конфигурационный файл apache, вернув Listen 80.
2. Удалите привязку http\_port\_t к 81 порту: semanage port -d -t http\_port\_t -p tcp 81 и проверьте, что порт 81 удалён.
3. Удалите файл /var/www/html/test.html: rm /var/www/html/test.html



Figure 11: Удаление файлов

# 3 Выводы

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

# Список литературы