Лабораторная работа № 6

Мандатное разграничение прав в Linux

Юрченко Артём Алексеевич

Содержание

## 0.1 Цели

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

## 0.2 Задачи

1. Настроить и запустить сервер Apache.
2. Исследовать влияние параметров сервера на его работу.

## 0.3 Ход работы

Войдем в систему с полученными учётными данными и убедимся, что SELinux работает в режиме enforcing политики targeted.

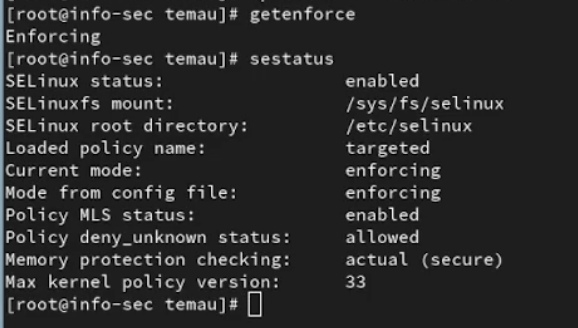


Figure 1: Конфигурация SELinux

## 0.4 Ход работы

Обратимся с помощью браузера к веб-серверу, запущенному на нашем компьютере, и убедимся, что последний работает.

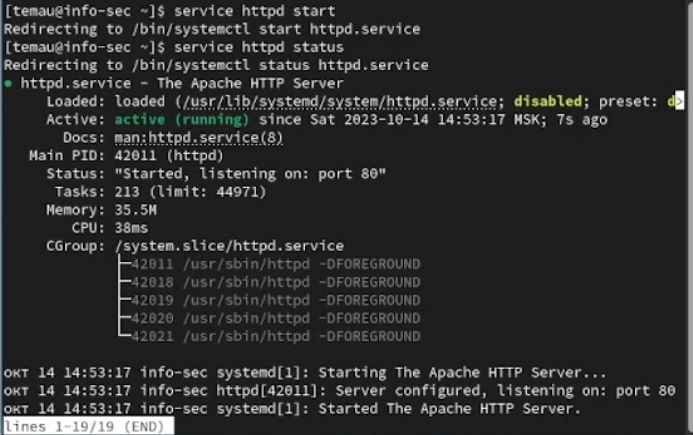


Figure 2: Обращение к веб-серверу

## 0.5 Ход работы

Найдем веб-сервер Apache в списке процессов, определим его контекст безопасности.

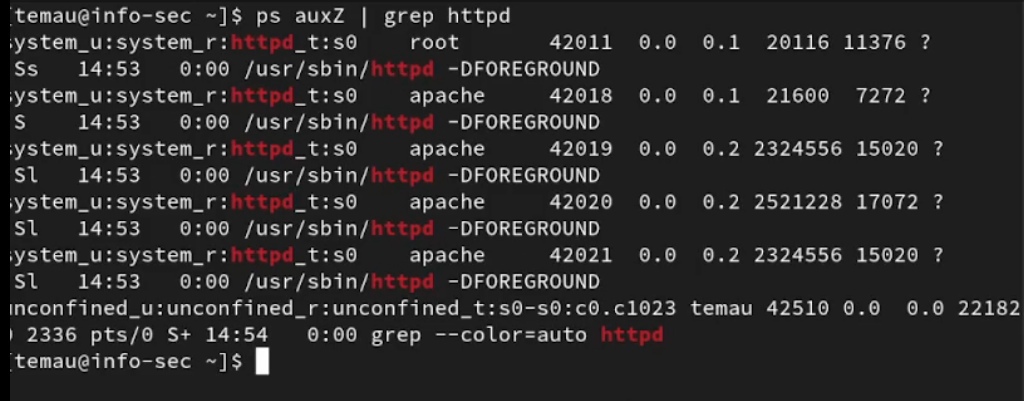


Figure 3: Контекст безопасности веб-сервера Apache

## 0.6 Ход работы

Посмотрим текущее состояние переключателей SELinux для Apache.

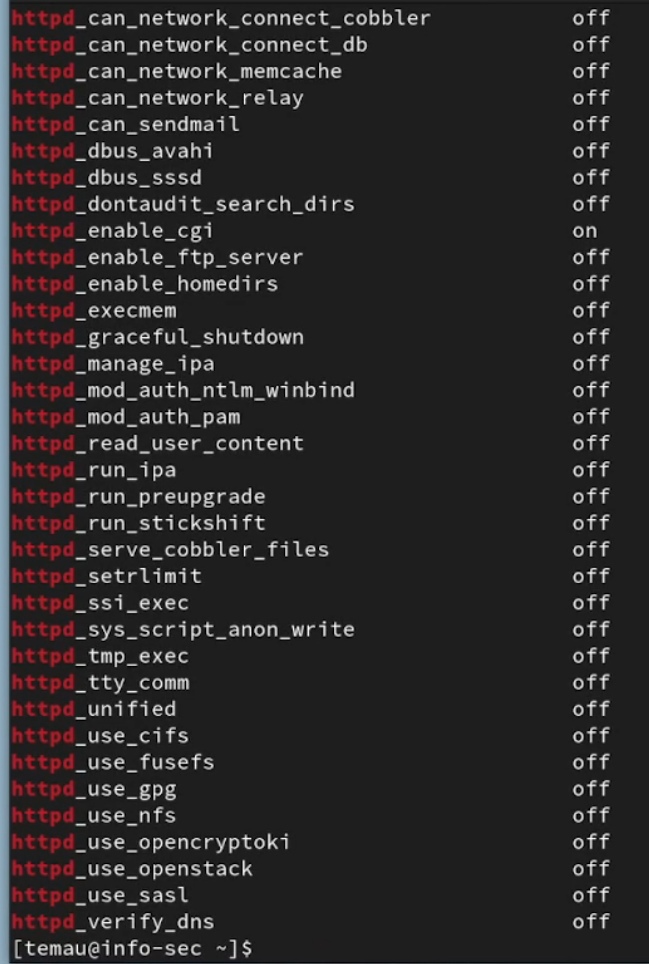


Figure 4: Текущее состояние переключателей SELinux для Apache

## 0.7 Ход работы

Посмотрим статистику по политике с помощью команды seinfo.

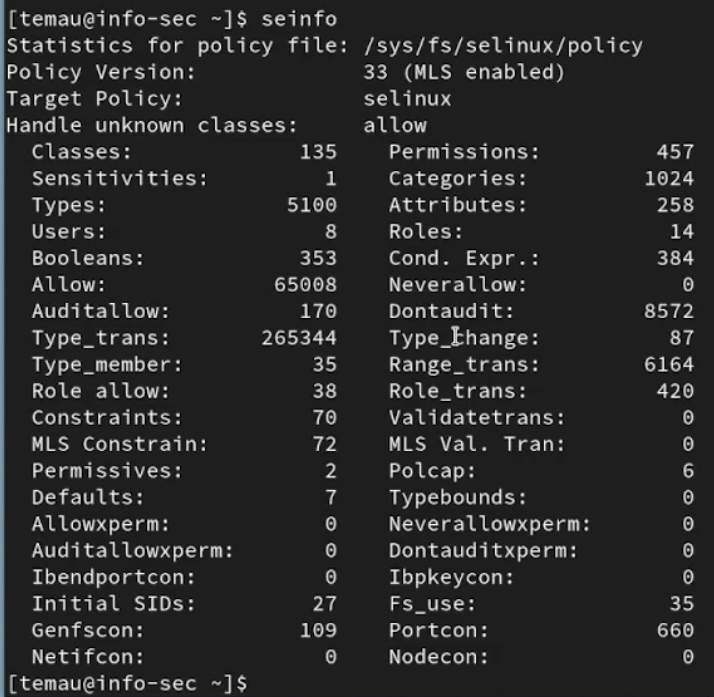


Figure 5: Статистика по политике

## 0.8 Ход работы

Определим тип файлов и поддиректорий, находящихся в директории /var/www.

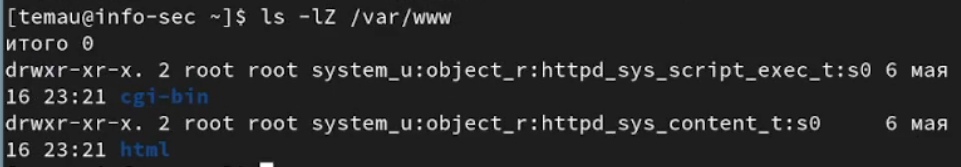


Figure 6: Тип файлов и поддиректорий, находящихся в директории /var/www

## 0.9 Ход работы

Определим тип файлов, находящихся в директории /var/www/html.

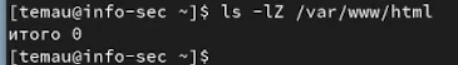


Figure 7: Тип файлов, находящихся в директории /var/www/html

## 0.10 Ход работы

Определим круг пользователей, которым разрешено создание файлов в директории /var/www/html.

Figure 8: Круг пользователей, которым разрешено создание файлов в директории /var/www/html

Figure 8: Круг пользователей, которым разрешено создание файлов в директории /var/www/html

## 0.11 Ход работы

Создадим от имени суперпользователя html-файл /var/www/html/test.html.

Figure 9: Создание файла /var/www/html/test.html

Figure 9: Создание файла /var/www/html/test.html

Заполним его следующим содержимым:

<html>  
<body>test</body>  
</html>

## 0.12 Ход работы

Проверим контекст созданного нами файла.



Figure 10: Работа с параметрами readfile

Как видим по умолчанию присваивается контекст unconfined\_u:object\_r:httpd\_sys\_content\_t:s0

## 0.13 Ход работы

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

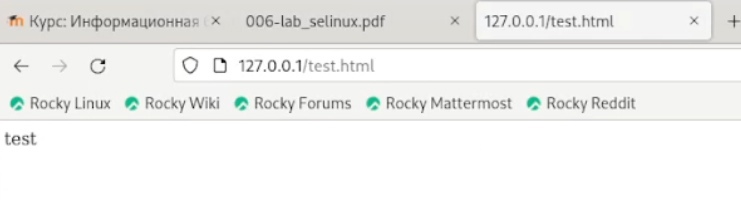


Figure 11: Файл test.html в браузере

## 0.14 Ход работы

Изучим справку man httpd\_selinux и выясним, какие контексты файлов определены для httpd. Сопоставим их с типом файла test.html.

Figure 12: Вызов справки и тип файла test.html

Figure 12: Вызов справки и тип файла test.html

## 0.15 Ход работы

Изменим контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на samba\_share\_t.

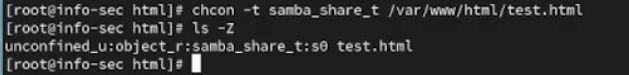


Figure 13: Изменение контекста

## 0.16 Ход работы

Попробуем ещё раз получить доступ к файлу через веб-сервер.

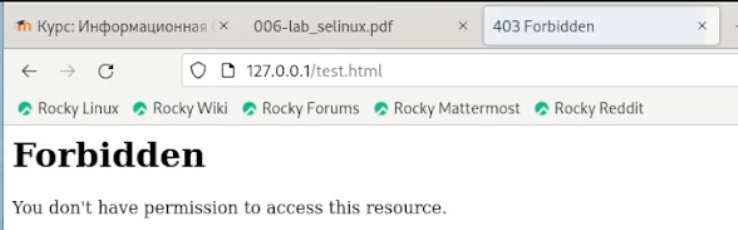


Figure 14: Файл test.html в браузере после изменения контекста

## 0.17 Ход работы

Просмотрим log-файлы веб-сервера Apache и системный лог-файл.

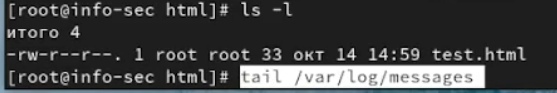


Figure 15: Содержимое логов

Как видим, нам не удалось получить доступ к файлу как раз из-за измененного контекста.

## 0.18 Ход работы

Попробуем запустить веб-сервер Apache на прослушивание ТСР-порта 81.

Figure 16: Изменение содержимого файла /etc/httpd/httpd.conf

Figure 16: Изменение содержимого файла /etc/httpd/httpd.conf

## 0.19 Ход работы

Выполним перезапуск веб-сервера. Сбоя не произошло.

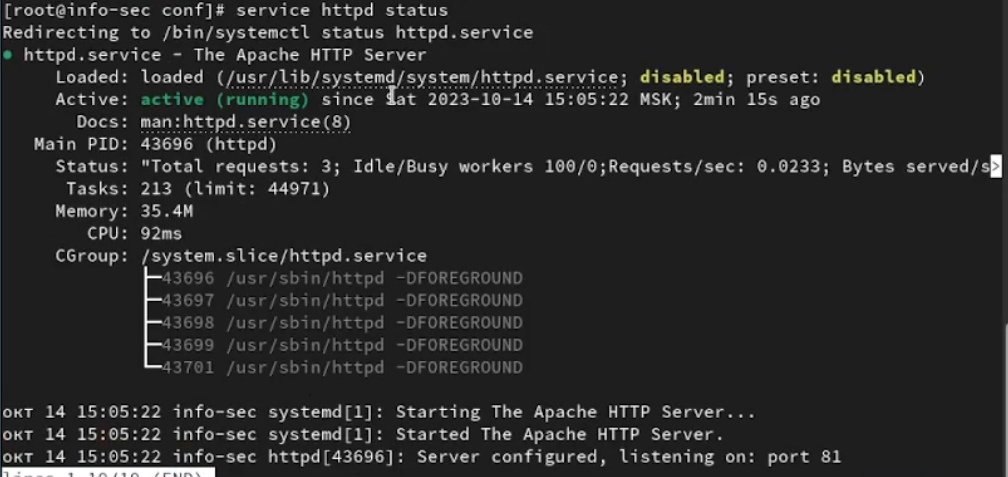


Figure 17: Перезапуск веб-сервера

## 0.20 Ход работы

Проанализируем лог-файлы.

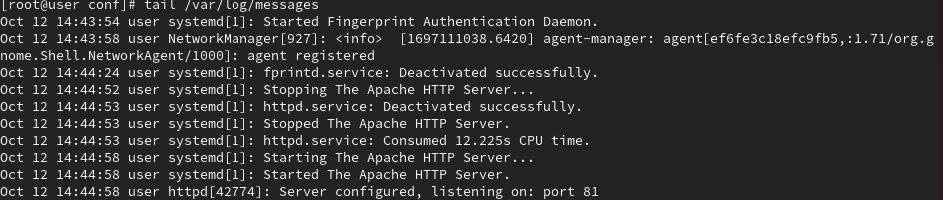


Figure 18: Лог-файл tail -nl /var/log/messages

## 0.21 Ход работы

Выполним команду semanage port -a -t http\_port\_t -р tcp 81. После этого проверим список портов командой semanage port -l | grep http\_port\_t Убедимся, что порт 81 есть в списке.

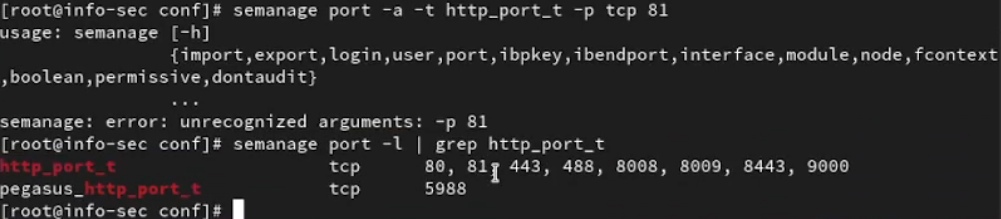


Figure 19: Попытка добавления порта 81 в список и вывод списка допустимых портов

## 0.22 Ход работы

Попробуем запустить веб-сервер Apache ещё раз.

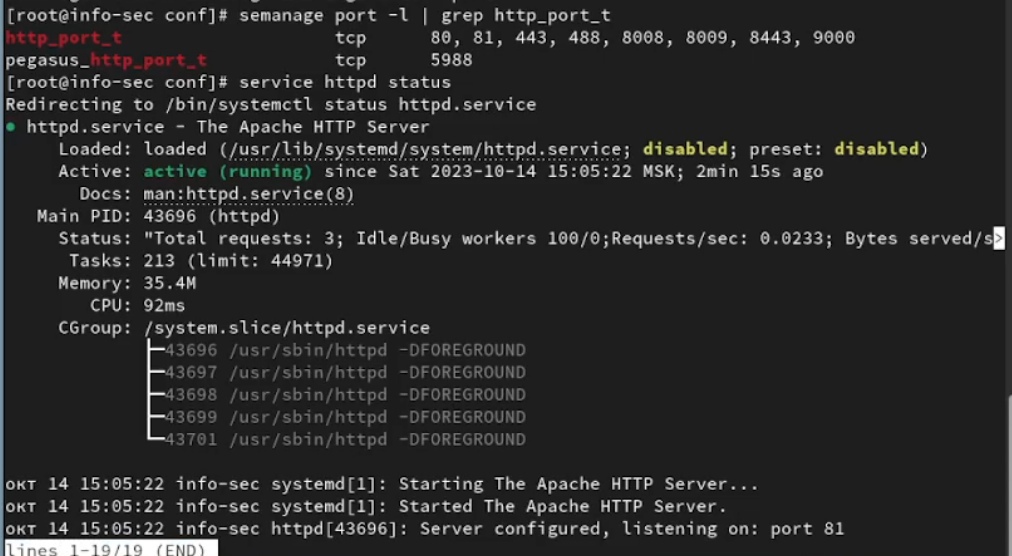


Figure 20: Повторный запуск веб-сервера

## 0.23 Ход работы

Вернем контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/ test.html. Попробуем получить доступ к файлу через веб-сервер.

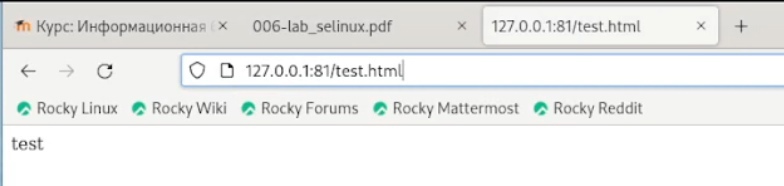


Figure 21: Файл test.html в браузере после возвращения контекста

## 0.24 Ход работы

Исправим обратно конфигурационный файл apache, вернув Listen 80.

Figure 22: Параметр Listen после возвращения значения

Figure 22: Параметр Listen после возвращения значения

## 0.25 Ход работы

Попробуем удалить привязку http\_port\_t к 81. Удаление невозможно.

Figure 23: Попытка удаления привязки к порту 81

Figure 23: Попытка удаления привязки к порту 81

## 0.26 Ход работы

Удалим файл /var/www/html/test.html.

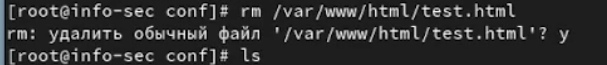


Figure 24: Удаление файла /var/www/html/test.html

## 0.27 Результаты

В рамках данной лабораторной работы были развиты навыки администрирования ОС Linux. Получено первое практическое знакомство с технологией SELinux1. Проверена работа SELinx на практике совместно с веб-сервером Apache.