Отчёт по лабораторной работе №5

Дисциплина: Информационная безопасность

Евдокимов Иван Андреевич

Содержание

# Техническое оснащение:

* Персональный компьютер с операционной системой Windows 10;
* OBS Studio, использующийся для записи скринкаста лабораторной работы;
* Приложение Visual Studio Code для редактирования файлов формата *md*, а также для конвертации файлов отчётов и презентаций;

# 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).

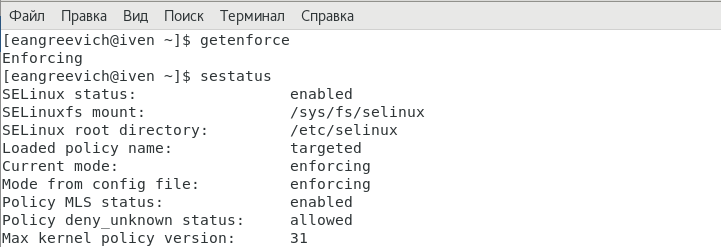


Рис. 1

1. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: service httpd status, запустил его так же, но с параметром start.(рис. 2).

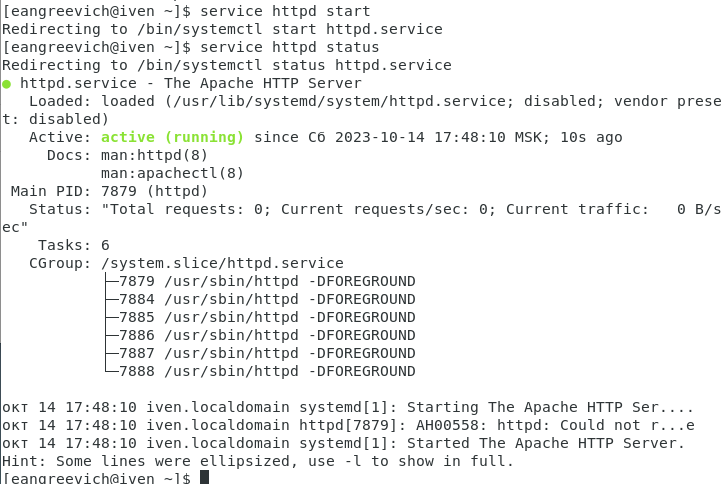


Рис. 2

1. Найшёл веб-сервер Apache в списке процессов, определил его контекст безопасности , использовав командуps auxZ | grep httpd (рис. 3).

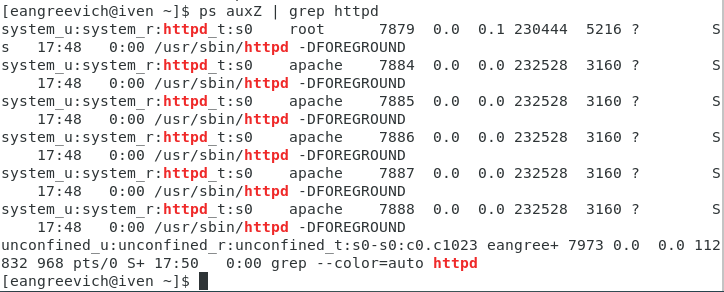


Рис. 3

1. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды sestatus -b | grep httpd (рис. 4)

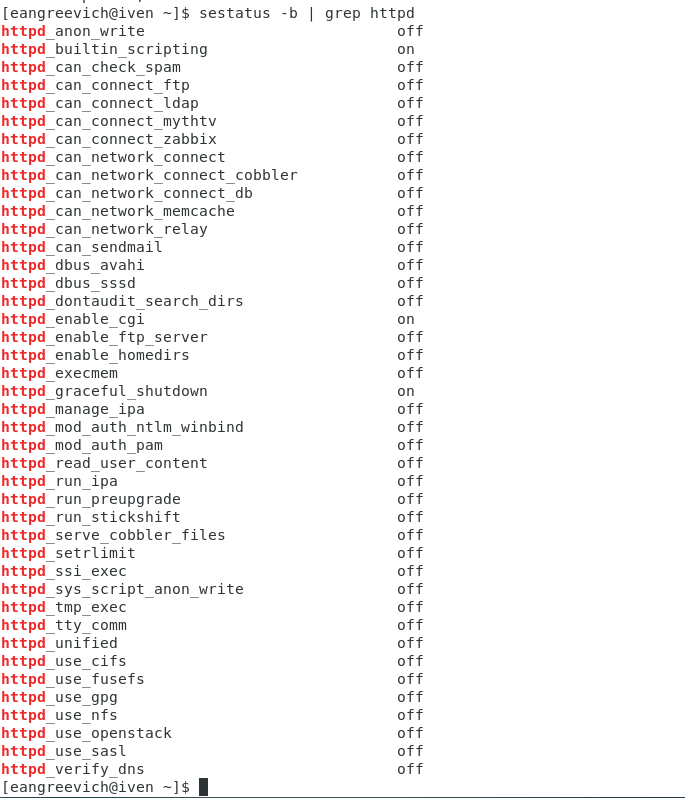


Рис. 4

1. Посмотрел статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов. (рис. 5).

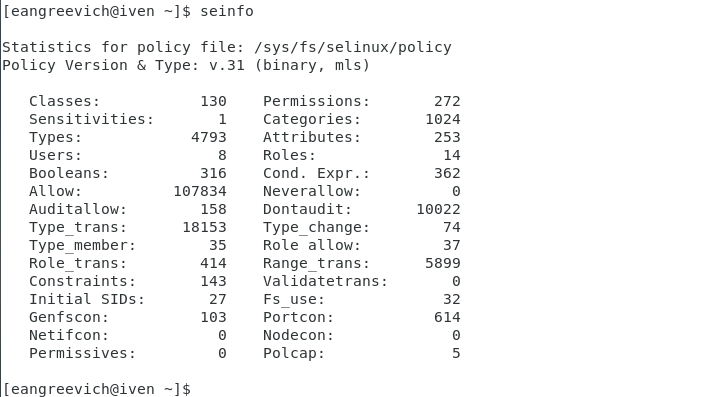


Рис. 5

1. Определил тип файлов и поддиректорий, находящихся в директории/var/www, с помощью команды ls -lZ /var/www (рис. 6).



Рис. 6

1. Определил тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html (рис. 7).

Рис. 7

Рис. 7

1. Определил круг пользователей, которым разрешено создание файлов в директории /var/www/html. (рис. 8).

Рис. 8

Рис. 8

1. Создал от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html (рис. 9).



Рис. 9

1. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html. (рис. 10).

Рис. 10

Рис. 10

1. Обратился к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедился, что файл был успешно отображён. (рис. 11).

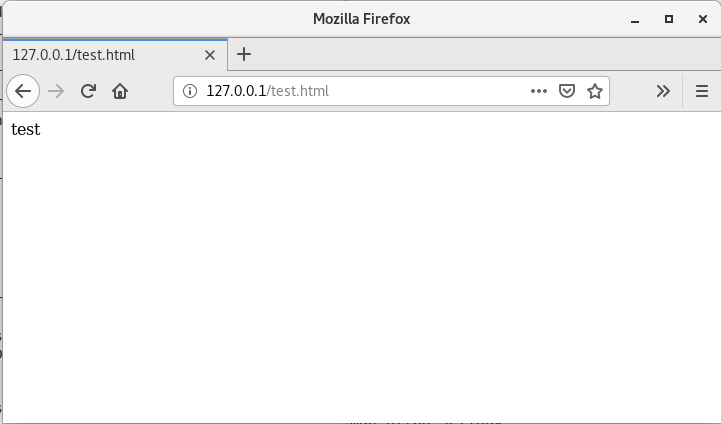


Рис. 11

1. Изучил справку man httpd\_selinux и выясните, какие контексты файлов определены для httpd. Сопоставил их с типом файла test.html. Проверить контекст файла можно командой ls -Z. ls -Z /var/www/html/test.html (рис. 12).

Рис. 12

Рис. 12

1. Изменил контекст файла /var/www/html/test.html 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 После этого проверил, что контекст поменялся.(рис. 13).

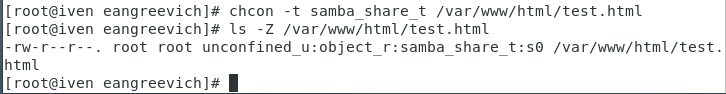


Рис. 13

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. (рис. 14).



Рис. 14

1. Проанализировал 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 просмотрел системный лог-файл: tail /var/log/messages (рис. 15).



Рис. 15

1. Попробовал 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. 16).

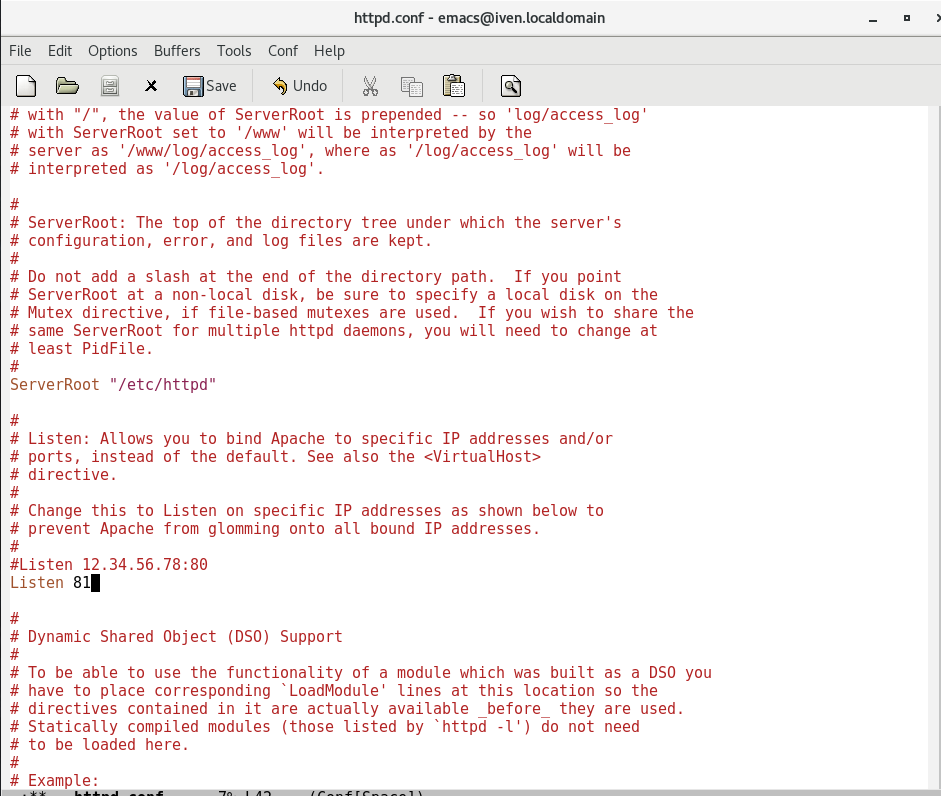


Рис. 16

1. Выполните перезапуск веб-сервера Apache. Произошёл сбой (рис. 17).

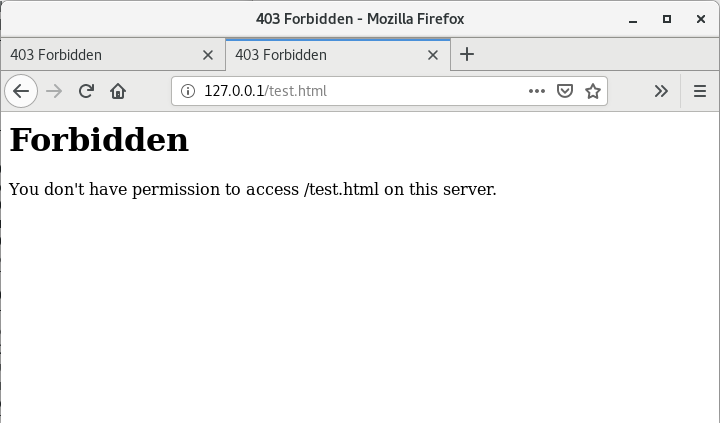


Рис. 17

1. Проанализировал лог-файлы: tail -nl /var/log/messages Просмотрел файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log и выяснил, в каких файлах появились записи (рис. 18).



Рис. 18

1. Выполнил команду semanage port -a -t http\_port\_t -р tcp 81 После этого проверил список портов командой semanage port -l | grep http\_port\_t Убедился, что порт 81 появился в списке(рис. 19).

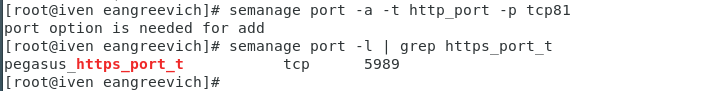
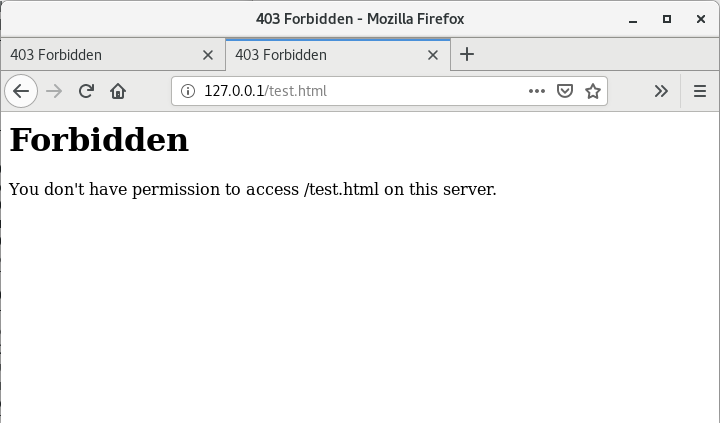
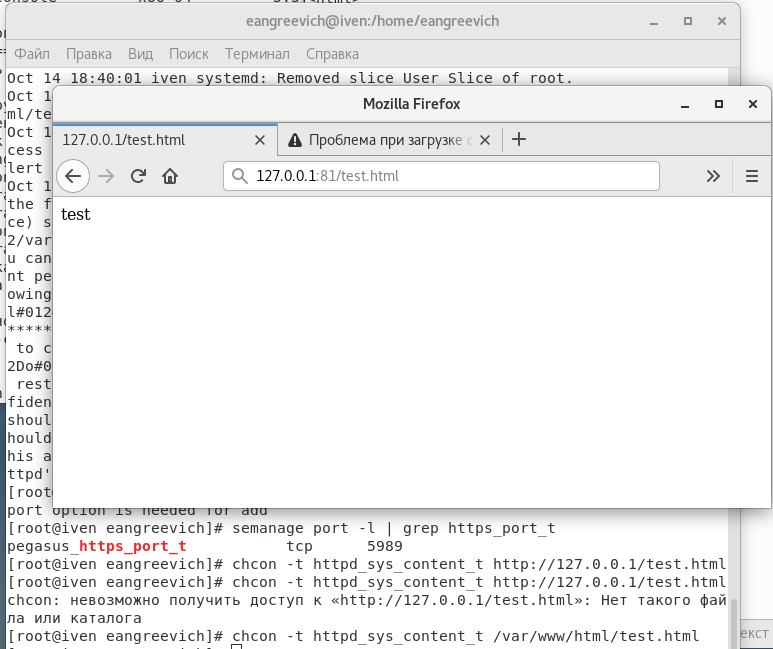


Рис. 19

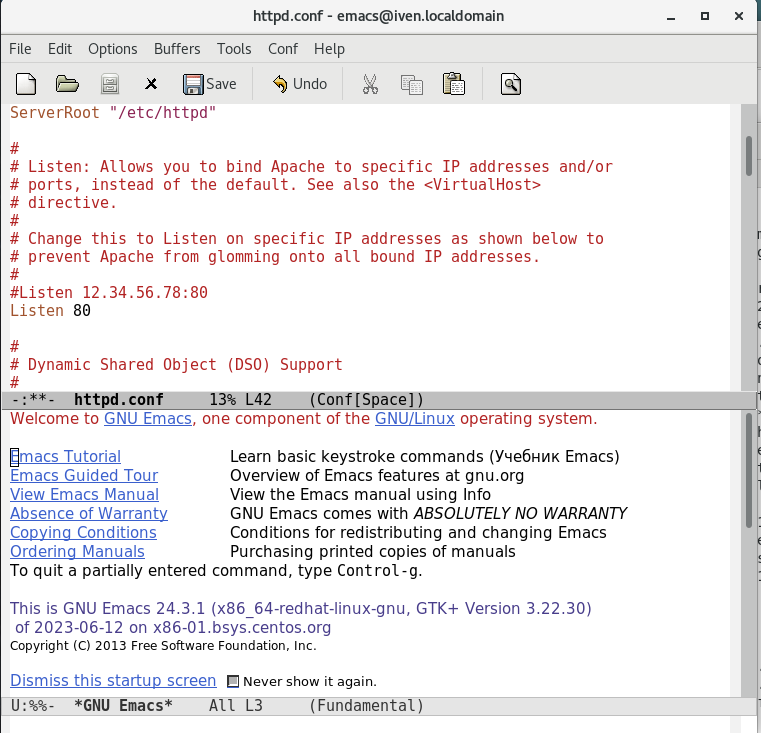
1. Пробую запустить веб-сервер Apache ещё раз (рис. 20).

.

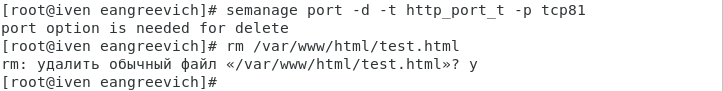
1. Вернул контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/ test.html: chcon -t httpd\_sys\_content\_t /var/www/html/test.html После этого попробовал получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. Увидеть содержимое файла — слово «test»(рис. 21).

.

1. . Исправил обратно конфигурационный файл apache, вернув Listen 80 (рис. 22).

.

1. Удалил привязку http\_port\_t к 81 порту: semanage port -d -t http\_port\_t -p tcp 81 и проверил, что порт 81 удалён,затем удалил файл /var/www/html/test.html: rm /var/www/html/test.html

.

**Выводы:**

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

# Список литературы

1. [Официальный сайт VirtualBox](https://www.virtualbox.org/)
2. [Материал для выполнения лабораторной](https://esystem.rudn.ru/pluginfile.php/2090282/mod_resource/content/2/006-lab_selinux.pdf)
3. [Официальный сайт CentOS](https://www.centos.org/)