Информационная безопасность

Лабораторная работа №6

Матюшкин Денис Владимирович (НПИбд-02-21)

Содержание

# 1 Цель работы

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

# 2 Теоретическое введение

VirtualBox (Oracle VM VirtualBox) — программный продукт виртуализации для операционных систем Windows, Linux, FreeBSD, macOS, Solaris/OpenSolaris, ReactOS, DOS и других [1].

Rocky Linux — дистрибутив Linux, разработанный Rocky Enterprise Software Foundation. Предполагается, что это будет полный бинарно-совместимый выпуск, использующий исходный код операционной системы Red Hat Enterprise Linux (RHEL) [2].

# 3 Ход работы

1. 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).

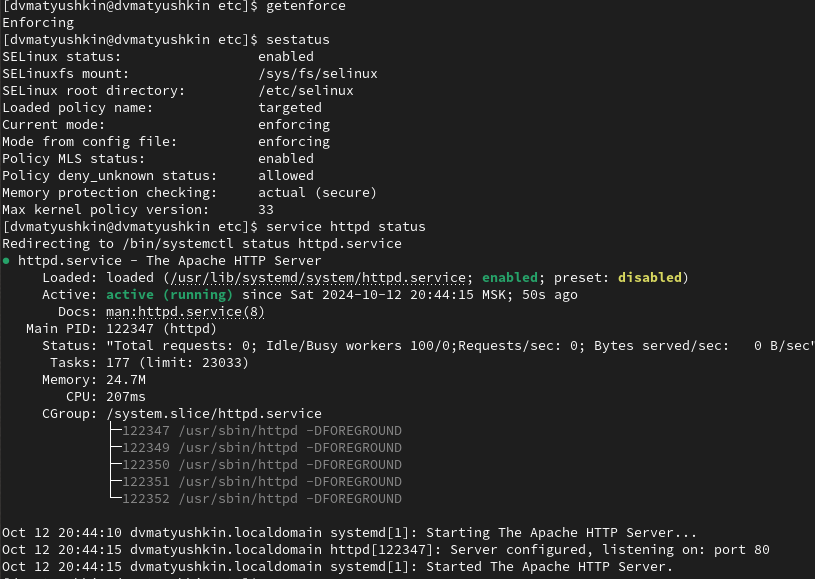


Рис. 1: Проверка работы SELinux

1. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает (рис. 2).

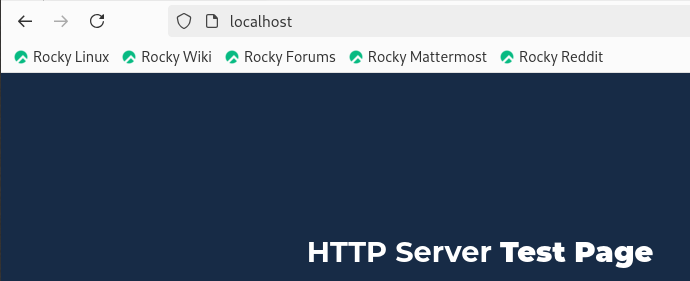


Рис. 2: localhost

1. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт (рис. 3).

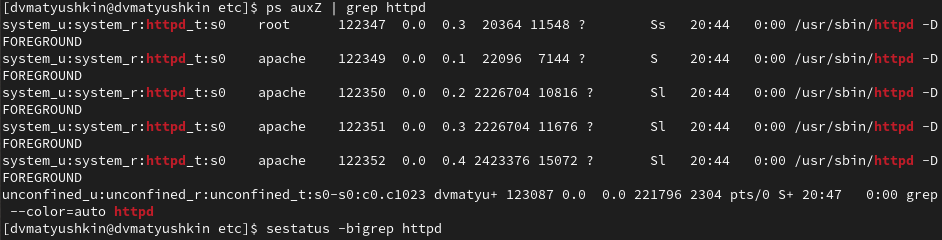


Рис. 3: Список процессов

1. Посмотрите текущее состояние переключателей SELinux для Apache (рис. 4).

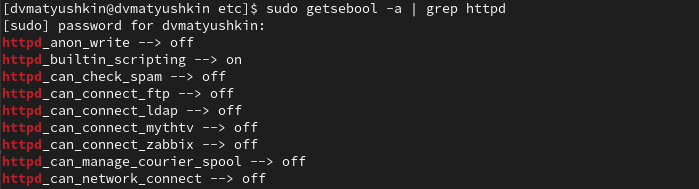


Рис. 4: Текущее состояние переключателей

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

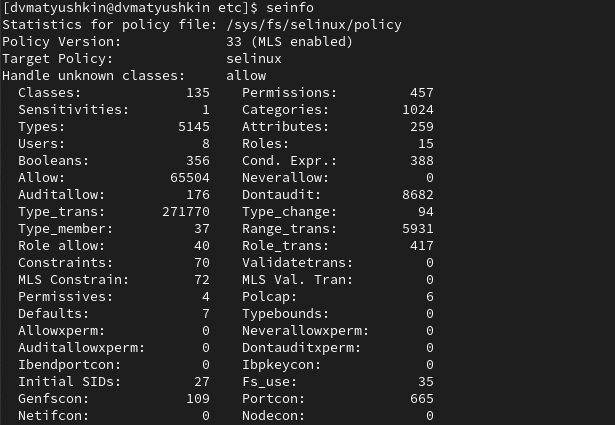


Рис. 5: Статистика по политике

1. Определите тип файлов и поддиректорий, находящихся в директории /var/www (рис. 6).
2. Определите тип файлов, находящихся в директории /var/www/html (рис. 6).
3. Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html (рис. 6).
4. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html (рис. 6).

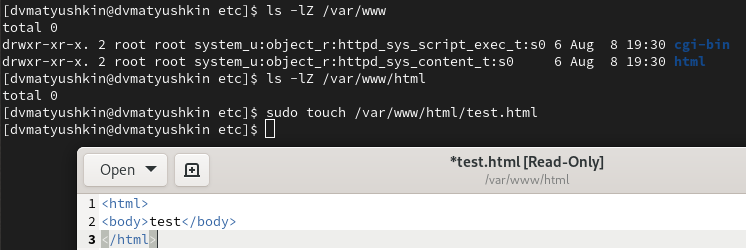


Рис. 6: Тип файлов и поддиректорий

1. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html (рис. 7).

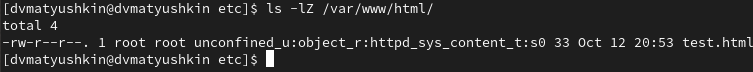


Рис. 7: Проверка контекста

1. Обратитесь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедитесь, что файл был успешно отображён (рис. 8).

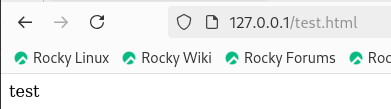


Рис. 8: Проверка

1. Изучите справку man httpd\_selinux и выясните, какие контексты файлов определены для httpd. Сопоставьте их с типом файла test.html. Проверить контекст файла можно командой ls -Z.
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 (рис. 9).

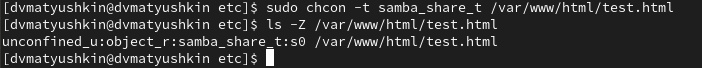


Рис. 9: Изменение контекста

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 (рис. 10).

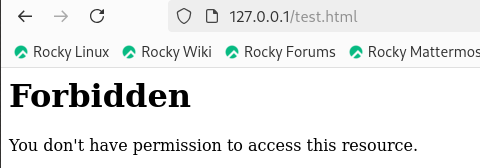


Рис. 10: Проверка

1. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: tail /var/log/messages (рис. 11).

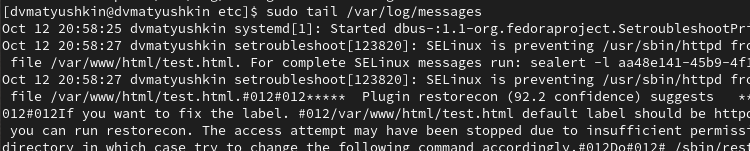


Рис. 11: Системный лог-файл

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. 12).

Рис. 12: Смена порта

Рис. 12: Смена порта

1. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему?

Сбоя не произошло, потому что порт 81 уже был в списке портов.

1. Проанализируйте лог-файлы: tail -nl /var/log/messages (рис. 13).

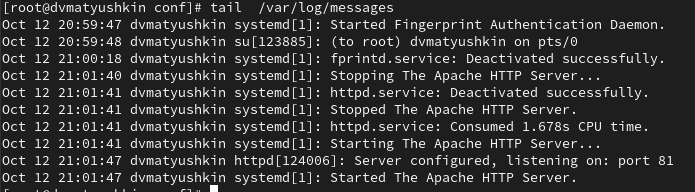


Рис. 13: Системный лог-файл

1. 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 Убедитесь, что порт 81 появился в списке (рис. 14).

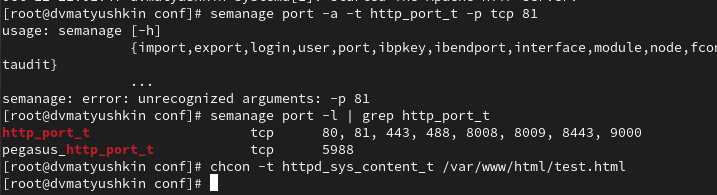


Рис. 14: Добавление порта

Порт уже был добавлен.

1. Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему он сейчас запустился, а в предыдущем случае не смог?

И в прошлый раз мог.

1. Верните контекст httpd\_sys\_cоntent\_\_t к файлу /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».
2. Исправьте обратно конфигурационный файл apache, вернув Listen 80.
3. Удалите привязку http\_port\_t к 81 порту (рис. 15).
4. Удалите файл /var/www/html/test.html (рис. 15).

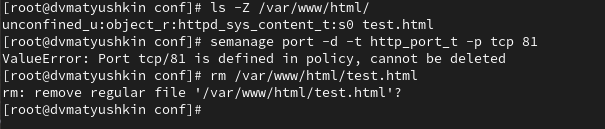


Рис. 15: Удаление привязки и файла

# 4 Выводы

В ходе данной лабораторной работы мы развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux. Проверили работу SELinx на практике совместно с веб-сервером Apache.

# Список литературы

1. VirtualBox Documentation [Электронный ресурс]. Oracle, 2024. URL: <https://www.virtualbox.org/wiki/Documentation>.

2. Rocky Documentation [Электронный ресурс]. Rocky Enterprise Software Foundation, 2024. URL: <https://docs.rockylinux.org/ru/>.