Лабораторная работа № 6

Мандатное разграничение прав в Linux

Аксёнова Алина Владимировна

Содержание

# Цель работы

Развить навыки администрирования ОС Linux.Проверить работу SELinx на практике совместно с веб-сервером Apache.

# Задание

Получить первое практическое знакомство с технологией SELinux

# Теоретическое введение

Для разграничения доступа субъектов — программ к объектам — файлам дерева каталогов используют так называемый мандатный (от англ, mandatory — обязательный или принудительный) подход (MAC, mandotary access control), предполагающий следование обязательным правилам доступа к файлам, назначаемым администраторами системы. Правила доступа строятся на основе знания о внутреннем устройстве программ и представляют собой описание набора минимально необходимых условий их целевого функционирования. Таким образом, в мандатных правилах, ограничивающих доступ к SSH-ключам пользователя, только программе ssh должен быть разрешен доступ для непосредственного выполнения своих прямых функций, а программам firefox и skype в доступе к SSH-ключам должно быть отказано.

# Ход работы

1. Входим в систему и убеждаемся, что SELinux работает в режиме enforcing политики targeted. (Рис. 1).

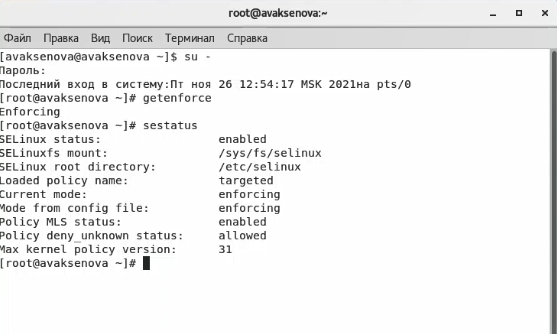


Figure 1: Проверка режима и политики SELinux

1. Проверяем работу веб-сервера. (Рис. 2).

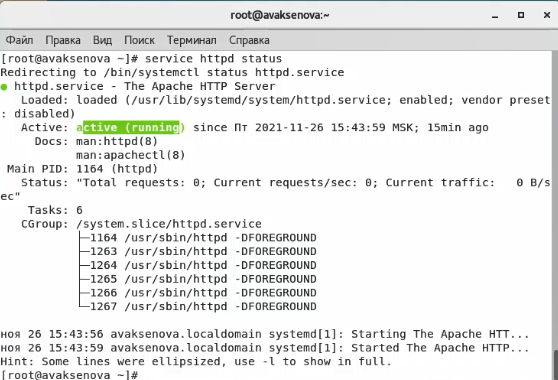


Figure 2: Проверка статуса веб-сервера

1. Определяем контекст безопасности веб-сервера.(Рис. 3).

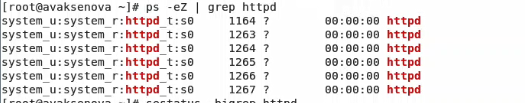


Figure 3: Определение контекста безопасности

1. Теперь посмотрим текущее состояние SELinux переключателей. Как можно заметить, практически все переключатели выключены. (Рис. 4).

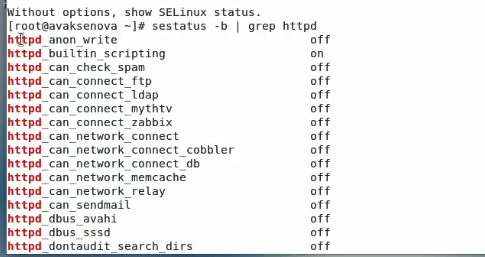


Figure 4: Состояние переключателей

1. Посмотрели статистику по политике. Кроме того, определили множество польхователей, ролей, типов (Рис. 5).

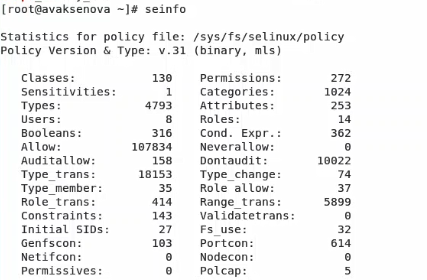


Figure 5: Статистика по политике

6.Определили тип файлов и поддиректорий, находящихся в директории /var/www. Тип файлов, находящихся в директории /var/www/html, определить не удалось, т.к. директория не сожержит файлов. Кроме того, определили круг пользователей, которым разрешено создание файлов в данной директории. Оказалось, что только суперпользователь имеет такое право. (Рис. 6).

Figure 6: Определяем типы

Figure 6: Определяем типы

1. Создали от имени суперпользователя html-файл. (Рис. 7).

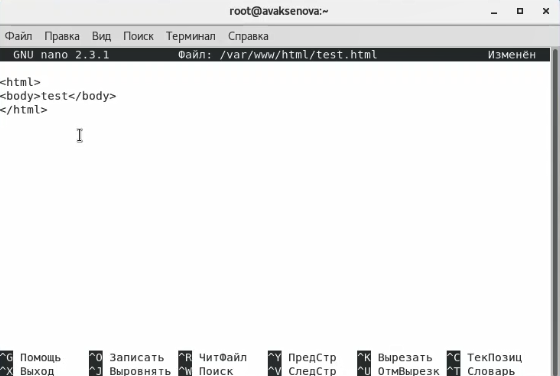


Figure 7: Создание html-файла

1. Проверили контекст созданного файла и обратились к файлу через веб-сервер (Рис. 8, -fig. 9]).

Figure 8: Проверка контекста файла

Figure 8: Проверка контекста файла

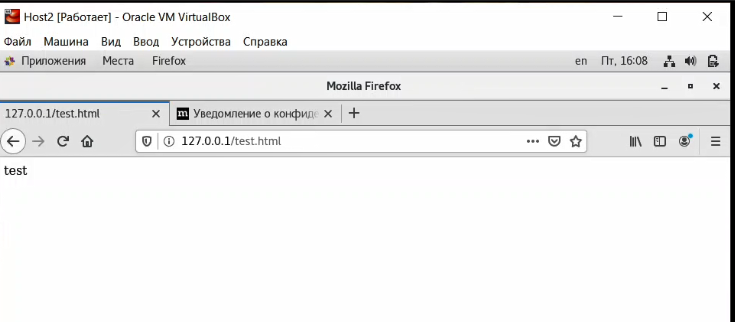


Figure 9: Обращение через веб-сервер

1. Изучили справку man httpd\_selinux и сопоставили их с типом файла test. (Рис. 10).

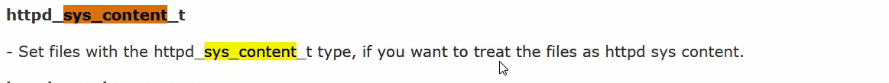


Figure 10: Тип файла

1. Изменили контекст файла на samba\_share\_t и проверили, что контекст поменялся. После этого в браузере получили сообщение об ошибке. Это произошло, поскольку SELinux запретил доступ к файлу (Рис. 11, 12).

Figure 11: Изменение контекста

Figure 11: Изменение контекста

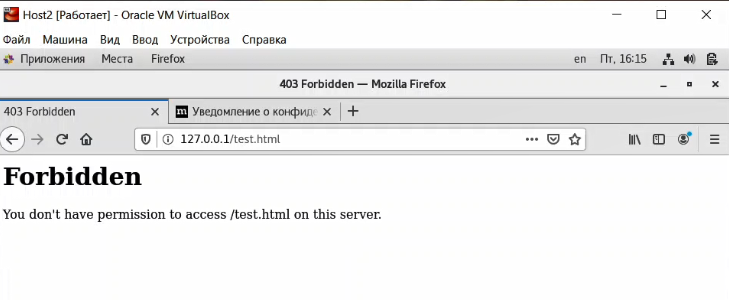


Figure 12: Повторный просмотр файла в браузере

1. Запустили веб-сервер Apache на прослушивание ТСР-порта 81. После чего перезапустили веб-сервер и проанализировали log-файлы. Также проверили список портов (Рис. 13, 14).

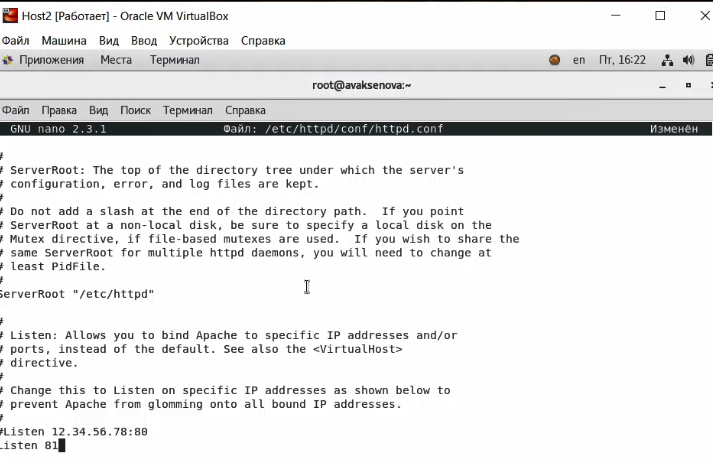


Figure 13: Запуск веб-сервера

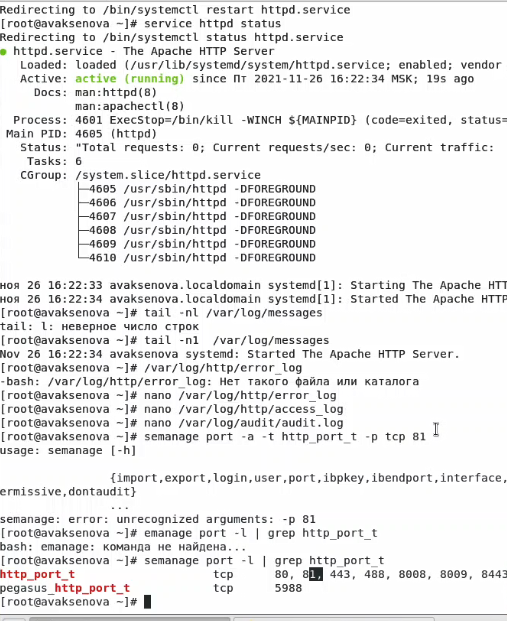


Figure 14: Анализ лог-файлов

1. Снова запустили веб-сервер Apache и вернули контекст httpd\_sys\_cоntent\_\_t к файлу, а затем попробовали получить доступ к файлу через браузер. В результате увидели содержимое файла (Рис. 15, 16).

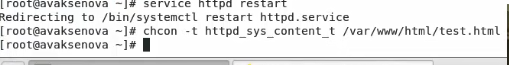


Figure 15: Запуск веб-сервера

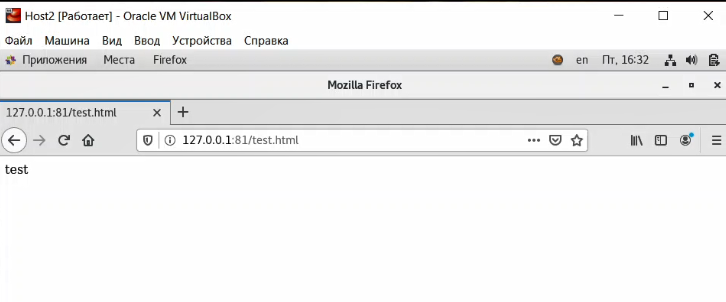


Figure 16: Доступ к файлу

1. Исправили обратно конфигурационный файл apache, вернув Listen 80 и попытались удалите привязку http\_port\_t к 81 порту. Вылезла ошибка, поскольку порт 81 определен на уровне политики. После этого удилили html-файл (Рис. 17, 18).

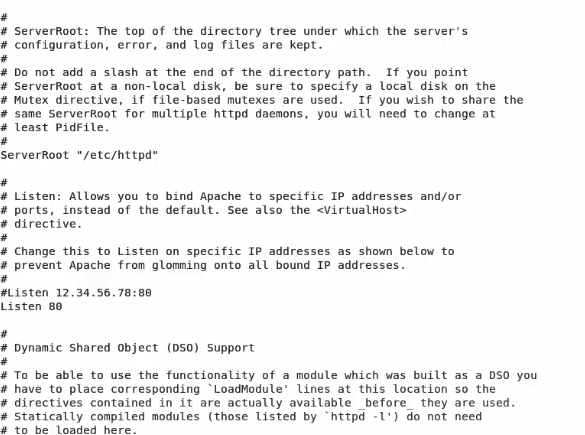


Figure 17: Исправление конфигурационного файла

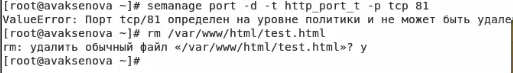


Figure 18: Удаление привезки и файла html

# Выводы

В результате выполнения данной работы была изучена технология SELinux, а также проверена работа SELinux с веб-сервером Apache.

# Библиографический список

1. Острейковский В. А. Информатика: учеб. для вузов / В. А. Острейковский. - 4-е изд., стер. - М.: Высш. шк., 2007. - 511 с.
2. Права в Linux [Электронный ресурс]. – Режим доступа : https://habr.com/ru/post/469667/, свободный. – Загл. с экрана.
3. Мандатное (принудительное) разграничение доступа Linux [Электронный ресурс]. – Режим доступа : https://debianinstall.ru/mandatnoe-prinuditelnoe-razgranichenie-dostupa-linux/, свободный. – Загл. с экрана.
4. Права доступа Unix, SUID, SGID, Sticky биты [Электронный ресурс]. – Режим доступа : https://help.ubuntu.ru/wiki/%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%BD%D1%8B%D0%B5\_%D0%BF%D1%80%D0%B0%D0%B2%D0%B0\_unix, свободный. – Загл. с экрана.