Лабораторная работа №6

Мандатное разграничение прав в Linux

Лебедева Ольга Андреевна

Содержание

# Цель работы

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

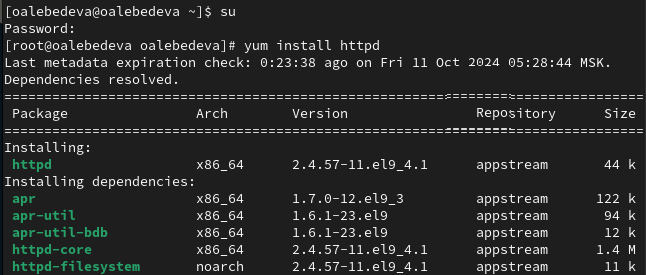
# Теоретическое введение

Мандатное управление доступом (Mandatory Access Control, MAC) предназначено для обеспечения большего уровня безопасности и контроля над доступом к ресурсам системы.

Мандатное разграничение доступа применяется в совокупности с дискреционным разграничением доступа. Оно определяет правила доступа на основе атрибутов объектов и субъектов, которые затем при проверке определяют разрешен ли доступ. Объект в данной модели – это то, над чем совершаются какие-либо действия, а субъект – исполнитель этого действия. Значение уровня доступа субъекта или объекта называется меткой. Метка может быть символьной или числовой. Проверка полномочий определяется при помощи сопоставления меток объекта и субъекта. Пользователи системы не могут самостоятельно определять доступ субъектов к объектам. Управление доступом субъектов к объектам осуществляют только администраторы[1].

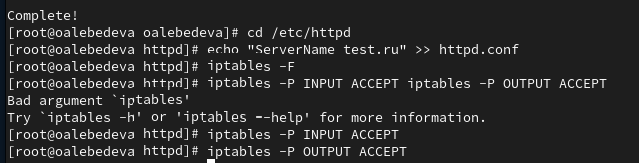
# Выполнение лабораторной работы

Перед выполнением лабораторной работы подготовим рабочее пространство и скачаем httpd: Cм. [рис. 1](#fig:001)



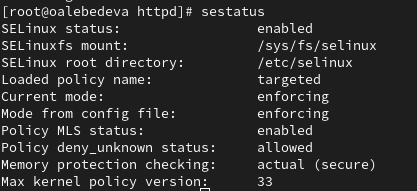
Скачивание httpd

В конфигурационном файле задаем ServerName и отключаем пакетный фильтр: Cм. [рис. 2](#fig:002)



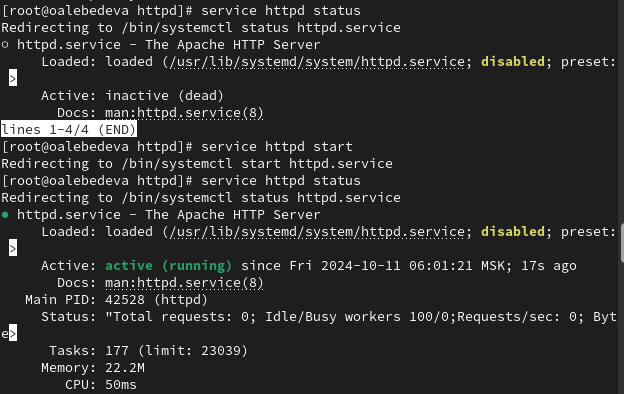
ServerName

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted: Cм. [рис. 3](#fig:003)



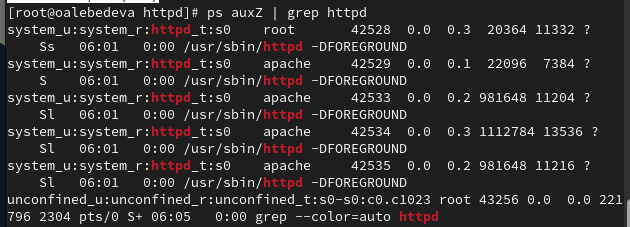
Вход в систему

1. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: Cм. [рис. 4](#fig:004)



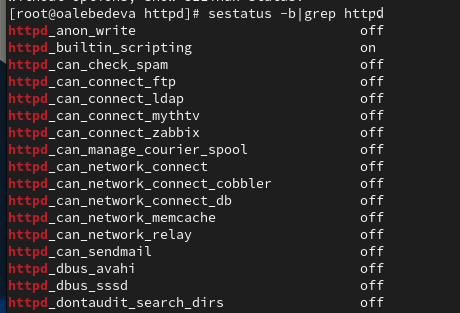
Обращение к веб-серверу

1. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт: Cм. [рис. 5](#fig:005)



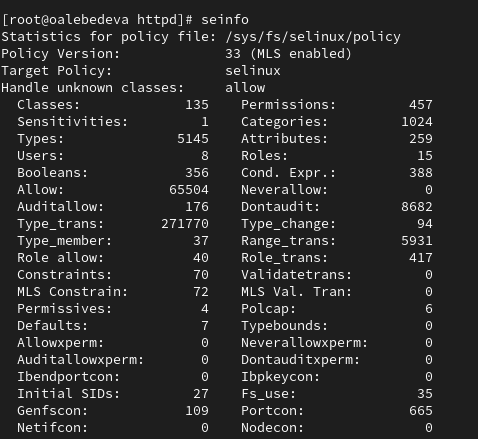
Контекст безопасности

1. Посмотрите текущее состояние переключателей SELinux для Apache: Cм. [рис. 6](#fig:006)



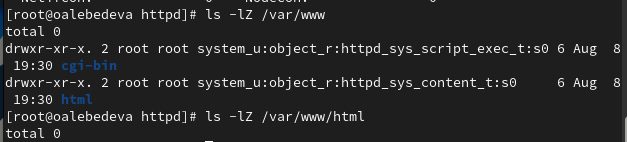
Состояние переключателей SELinux

Посмотрите статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов: Cм. [рис. 7](#fig:007)



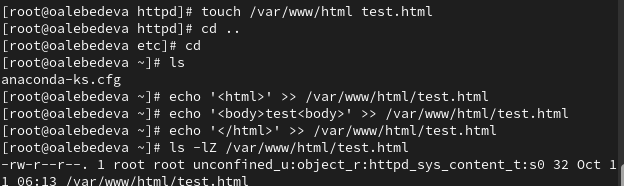
Статистика по политике

1. Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www
2. Определите тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html: Cм. [рис. 8](#fig:008)



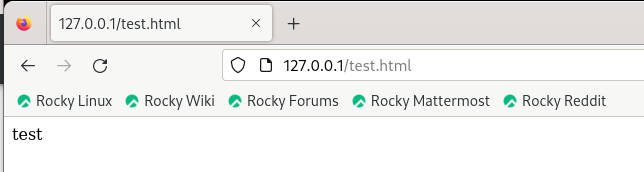
Определение типа файлов и директорий

1. Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html.
2. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html.
3. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html.: Cм. [рис. 9](#fig:009)



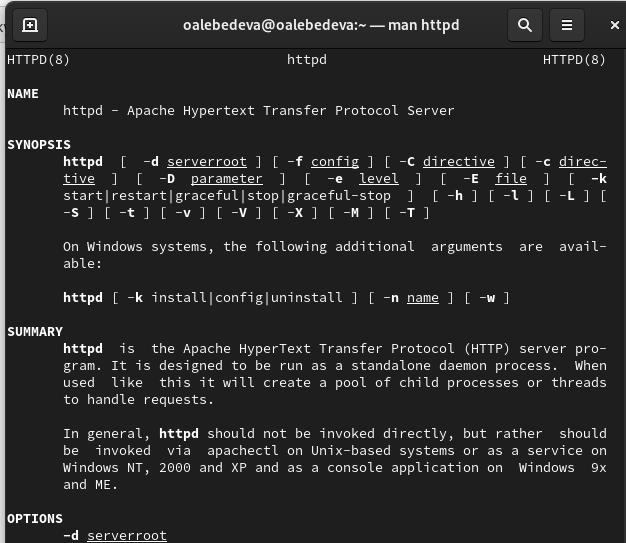
Создание файла test.html

1. Обратитесь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедитесь, что файл был успешно отображён: Cм. [рис. 10](#fig:010)



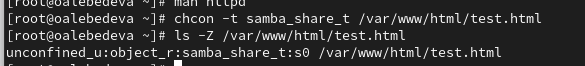
Просмотр файла через веб-сервер

1. Изучите справку man httpd\_selinux и выясните, какие контексты файлов определены для httpd: Cм. [рис. 11](#fig:011)



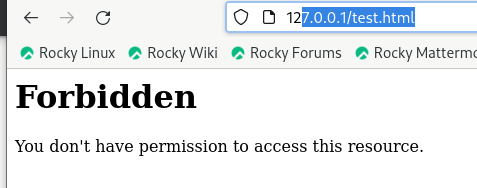
Контексты файлов для httpd

1. 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. Cм. [рис. 12](#fig:012)



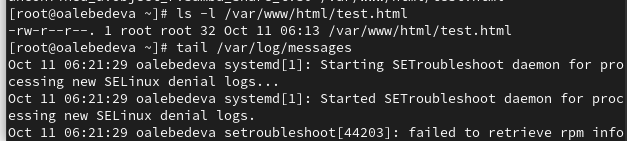
Изменение контекста

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: Cм. [рис. 13](#fig:013)



Ошибка доступа

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. Cм. [рис. 14](#fig:014)



Просмотр log-файлов

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. Cм. [рис. 15](#fig:015)

Замена порта на 81

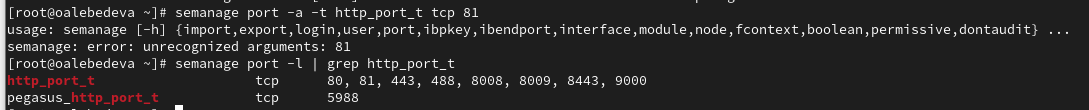
Замена порта на 81

1. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему?
2. Проанализируйте лог-файлы. Cм. [рис. 16](#fig:016)

Лог-файлы

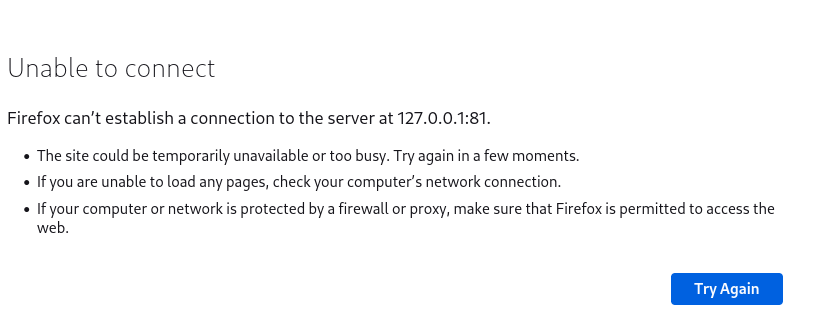
Лог-файлы

1. Выполните команду semanage port -a -t http\_port\_t -р tcp 81. После этого проверьте список портов. Убедитесь, что порт 81 появился в списке. Cм. [рис. 17](#fig:017)



Проверка порта

1. Попробуйте запустить веб-сервер Apache ещё раз. Cм. [рис. 18](#fig:018)



Запуск сервера

1. Верните 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». Cм. [рис. 19](#fig:019)

Возврат контекста

Возврат контекста

1. Исправьте обратно конфигурационный файл apache, вернув Listen 80.
2. Удалите привязку http\_port\_t к 81 порту и проверьте, что порт 81 удалён. Cм. [рис. 20](#fig:020)

Удаление привязки к 81 порту

Удаление привязки к 81 порту

1. Удалите файл /var/www/html/test.html: Cм. [рис. 21](#fig:021)

Удаление файла

Удаление файла

# Заключение

Развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux1. Проверили работу SELinx на практике совместно с веб-сервером Apache.

# Библиографическая справка

[1] Мандатное управление: https://itcloud-edu.ru/info/articles/upravlenie-dostupom-v-gnu-linux/