Лабораторная работа №6: Дискреционное разграничение прав в Linux. Расширенные атрибуты

*дисциплина: Информационная безопасность*

Швец Сергей Сергеевич

2021, 27 november

# Цель работы

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

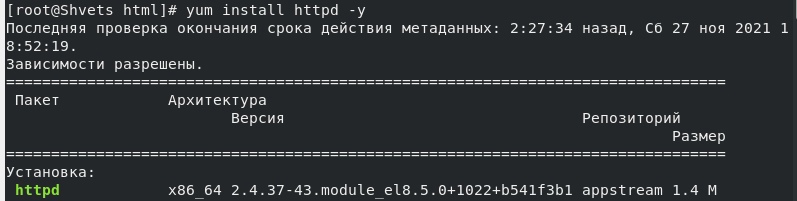
**Установка httpd**

Figure 1: httpd

**Вход в систему**Войдите в систему с полученными учётными данными и убедитесь, что

SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus.

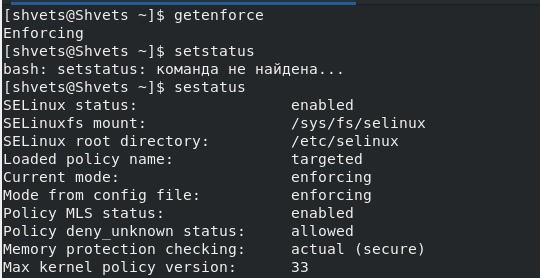


Figure 2: вход

## Обращение

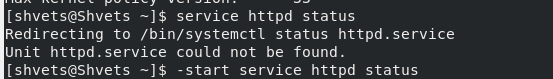
Обращение с помощью браузера к веб-серверу, запущенному на компьютере  
  


Figure 3: обращение к веб-серверу

## Контекст

Определение контекста безопасности.



Figure 4: Контекст безопасности

## Состояние

Текущее состояние переключателей SELinux для Apache.

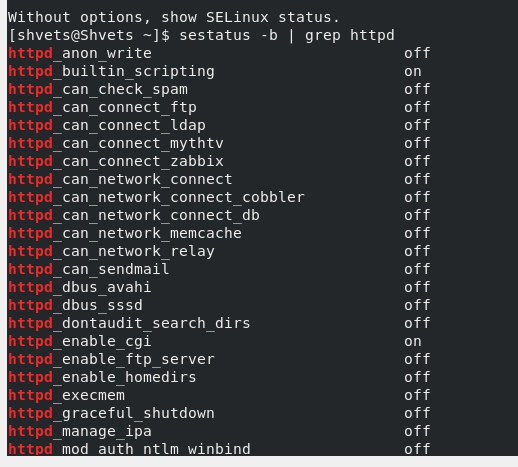


Figure 5: просмотр состояния

**Файлы и поддиректории**Определение типа файлов и поддиректорий, находящихся в директории.



Figure 6: Расширенные атрибуты

**Создание файла test.html**Создание файла test.html

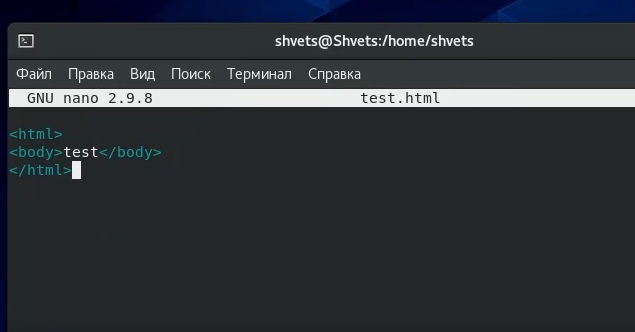


Figure 7: test.html

## Log-файл

Просмотр системного log-файла.

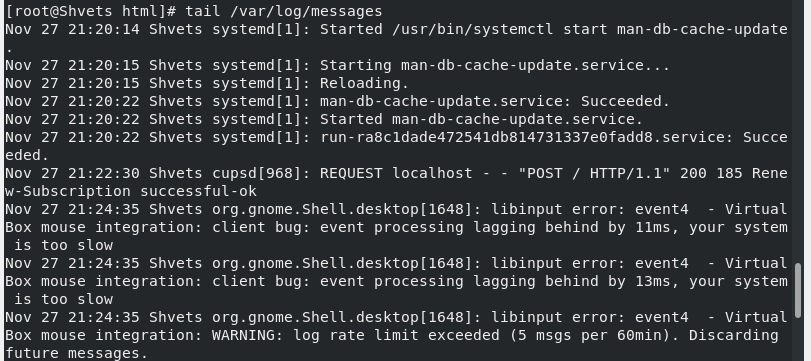
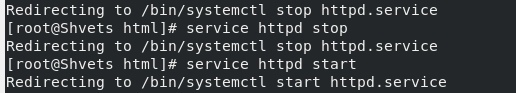


Figure 8: log-файл

## Попытка перезапуска

Попытка перезапуска сервера  


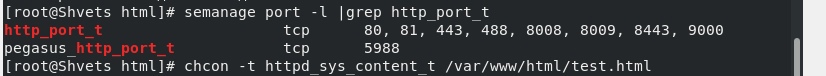
## Log-файлы

tail -nl /var/log/messages.



## Список портов

semanage port -l | grep http\_port\_t.



# Выводы

Я ознакомился с базовыми с технологией SELinux. Развил навыки одминистратора и проверил работу SELinux на практике.