# Лабораторная работа №6

## Дискреционное разграничение прав в Linux. Основные атрибуты

**Выполнила:** Накова Амина Михайловна, НПИбд-02-23

### 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

#### 1 . Для проведения указанной лабораторной работы на одно рабочее место

требуется компьютер с установленной операционной системой Linux, поддерживающей технологию SELinux. Предполагается использовать стандартный дистрибутив Linux CentOS с включённой политикой SELinux targeted и режимом enforcing. Для выполнения заданий требуется наличие учётной записи администратора (root) и учётной записи обычного пользователя. Постоянно работать от учётной записи root неправильно с точки зрения безопасности /home/guest/dir1/file1 командой ([рис. @fig-001]).

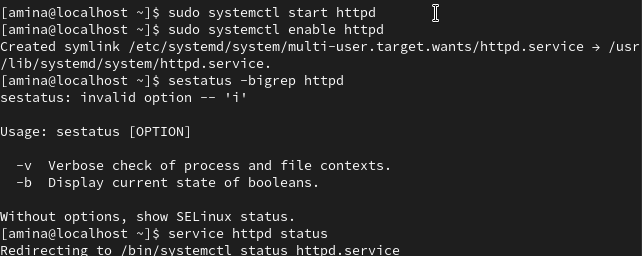


рис.1.1

#### 2. Войдите в систему с полученными учётными данными и убедитесь, что

SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus. Обратитесь с помощью браузера к вебсерверу, запущенному на вашем компьютере, и убедитесь, что последний работает: service httpd status или /etc/rc.d/init.d/httpd status. Если не работает, запустите его так же, но с параметром start ([рис. @fig-002]).

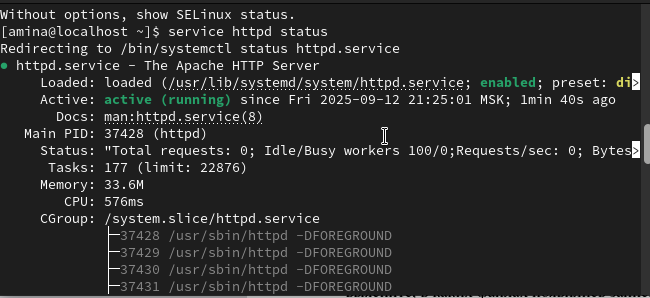


рис.2.1

#### 3. Найдите веб-сервер Apache в списке процессов, определите его контекст

безопасности и занесите эту информацию в отчёт. Например, можно использовать команду ps auxZ | grep httpd или ps -eZ | grep httpd Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды sestatus -bigrep httpd. Обратите внимание, что многие из них находятся в положении «off».([рис. @fig-003]).

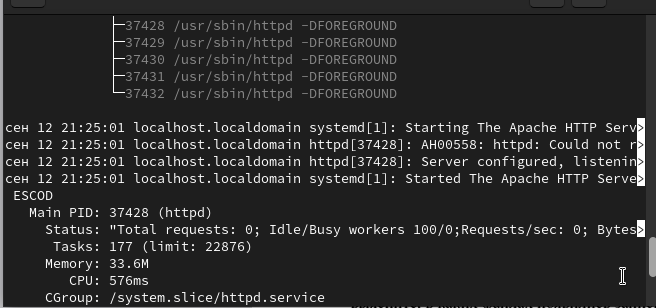


рис.3.1

#### 4. Посмотрите статистику по политике с помощью команды seinfo, также

определите множество пользователей, ролей, типов. Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www Определите тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html ([рис. @fig-004]).

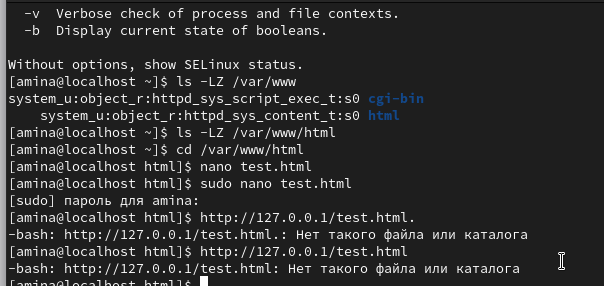


рис.4.1

#### Выводы:

В ходе лабораторной работы было получено практическое знакомство с технологией SELinux. Были изучены основные механизмы мандатного разграничения доступа в Linux, работа с контекстами безопасности, портами и политиками. Исследование показало, что: SELinux обеспечивает дополнительный уровень безопасности поверх стандартных прав доступа Контексты безопасности определяют, какие процессы могут обращаться к каким ресурсам Изменение контекста файла может заблокировать доступ к нему, даже если стандартные права доступа разрешают чтение Для работы служб на нестандартных портах необходимо явно добавлять эти порты в политику SELinux Работа позволила получить практические навыки администрирования SELinux и понимание важности мандатного контроля доступа в современных операционных системах.