Лабораторная работа №9

Управление SELinux

Хохлачёва Полина Дмитриевна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

2 Выполнение лабораторной работы

Получаем полномочия администратора, смотрим текущую информацию о состоянии, изменение режим работы(рис. 2.1).

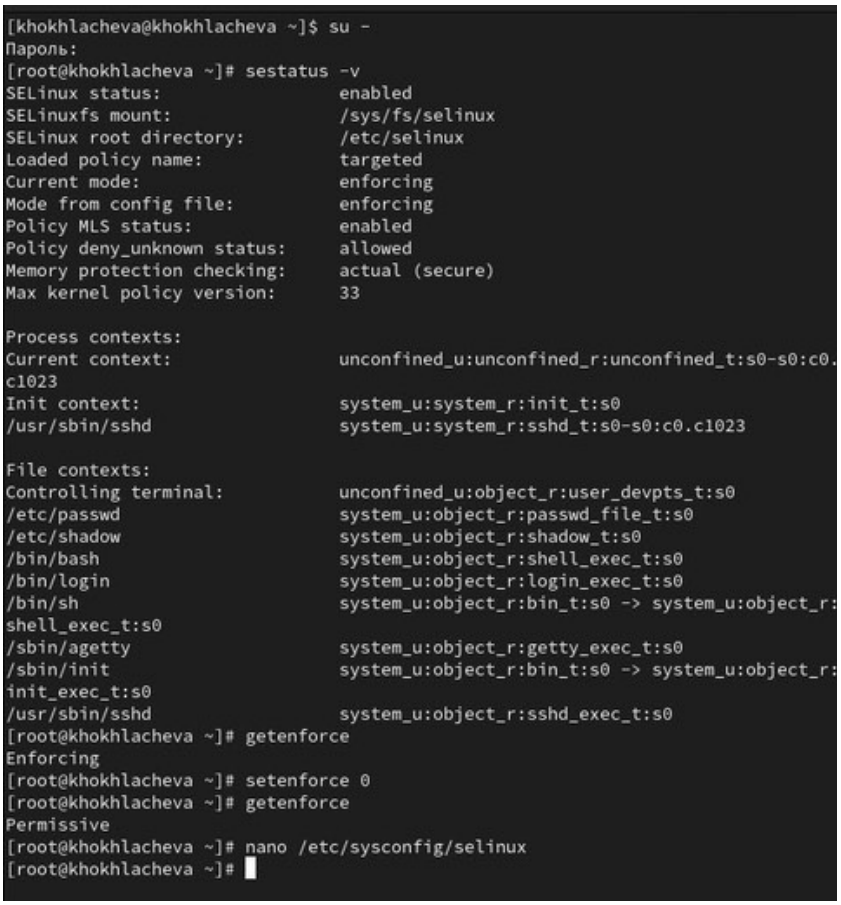

Рис. 2.1: Просмотр,изменения

Установка с помощью редактора(рис. 2.2).

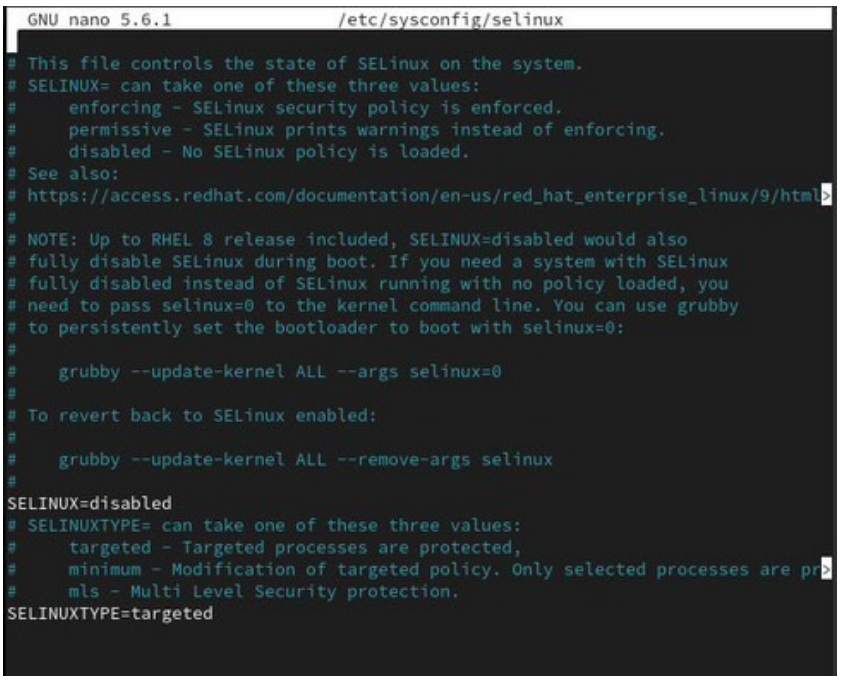

Рис. 2.2: Установка

Получаем полномочия администратора, просматриваем контекст безопасности файла, копируем файл в домашний каталоги,переписываем существенный файл, исправляем контекст безопасности, убеждаемся в этом(рис. 2.3).

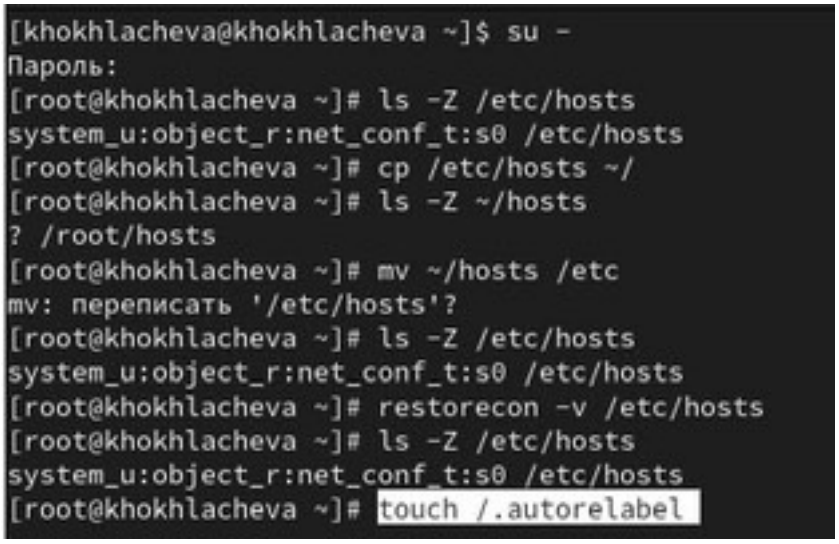

Рис. 2.3: Посматриваем,исправляем, убеждаемся

Устанавливаем необходимое программное обеспечение(рис. 2.4).

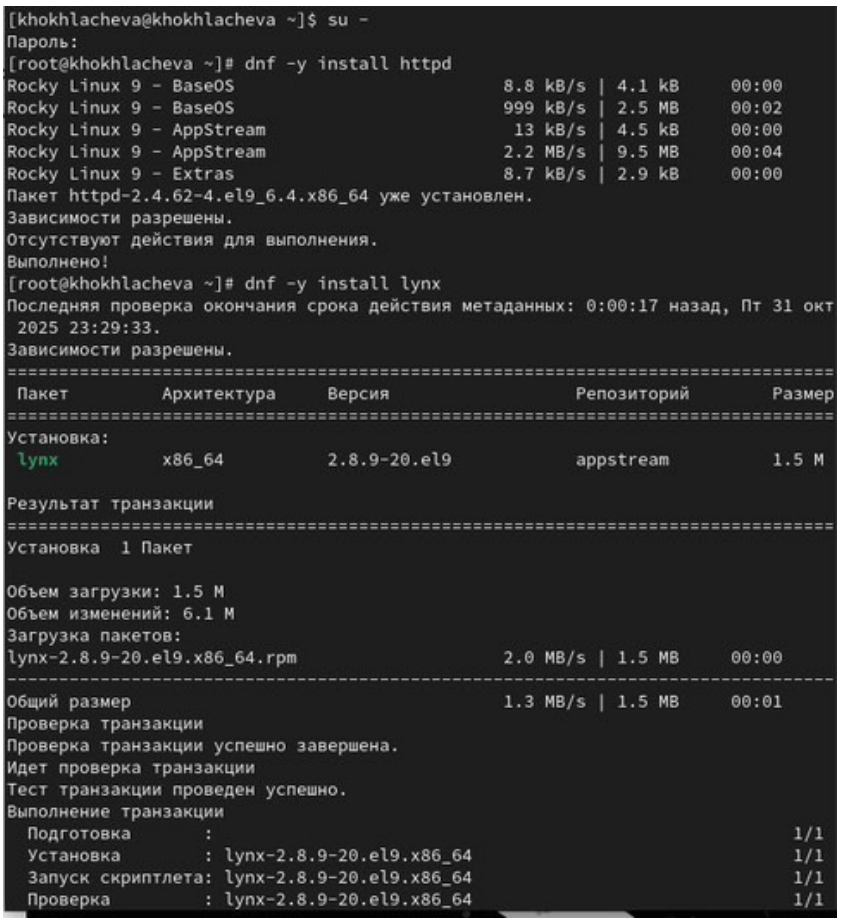

Рис. 2.4: Устанавливаем

Создаём новое хранилище, создаём файл в каталоге с контентом веб-сервера(рис. 2.5).

Рис. 2.5: Создаём

Помещаем следующий текст(рис. 2.6).

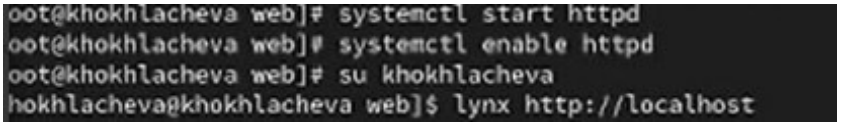

Рис. 2.6: Помещаем

Запускаем веб-сервер(рис. 2.7).

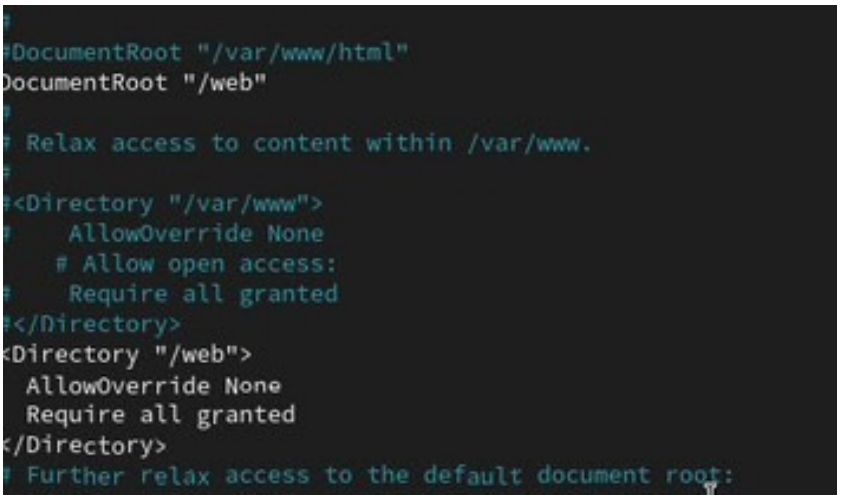

Рис. 2.7: Запускаем

Комментируем строки и добавляем следующие отделы(рис. 2.8).

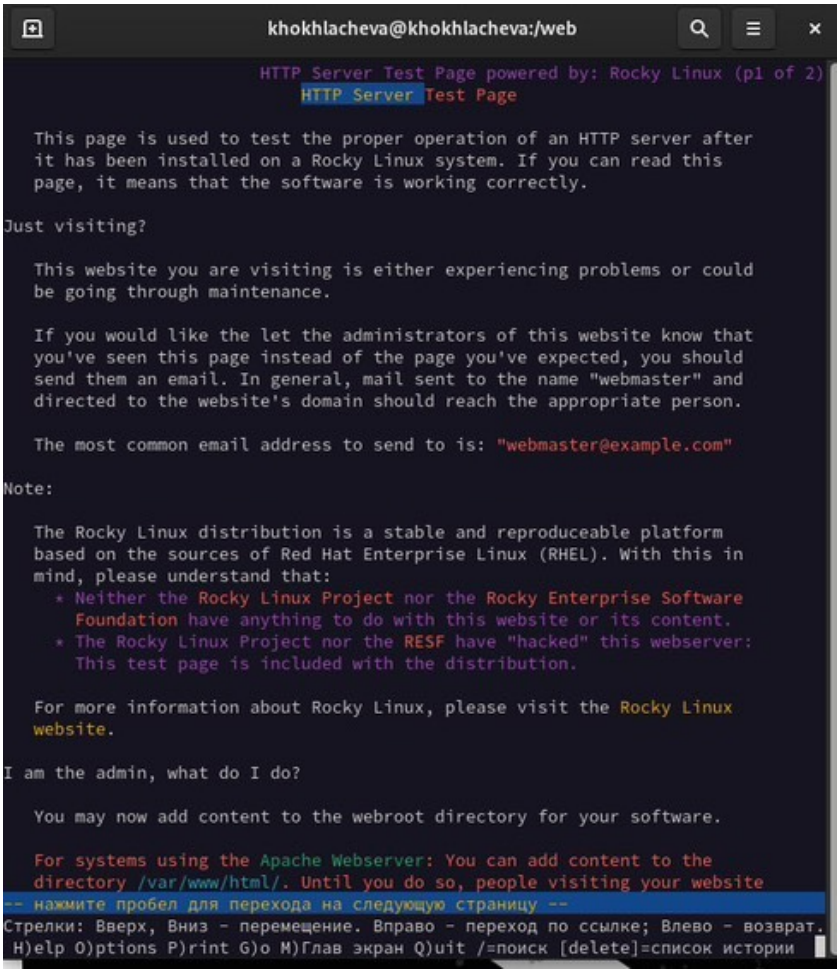

Рис. 2.8: Комментируем, добавляем

Снова обращаемся к веб-серверу(рис. 2.9).

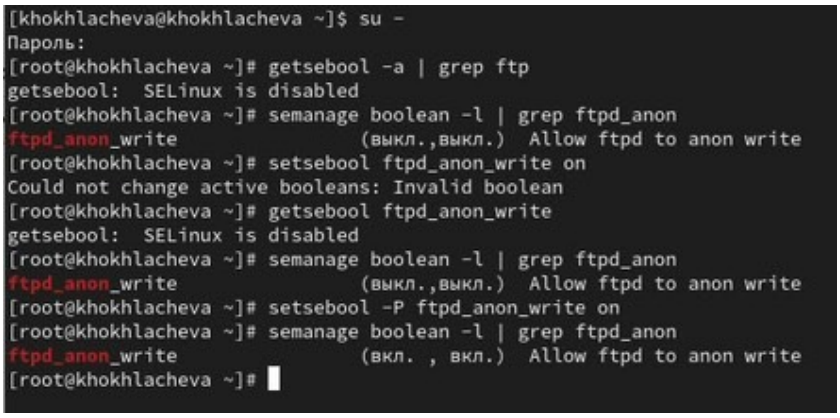

Рис. 2.9: Обращаемся

Получаем полномочия администратора, смотрим список переключателей, изменяем текущее значение переключателя для службы, повторно смотрим список, изменяем постоянное значение и снова смотри список(рис. 2.10).

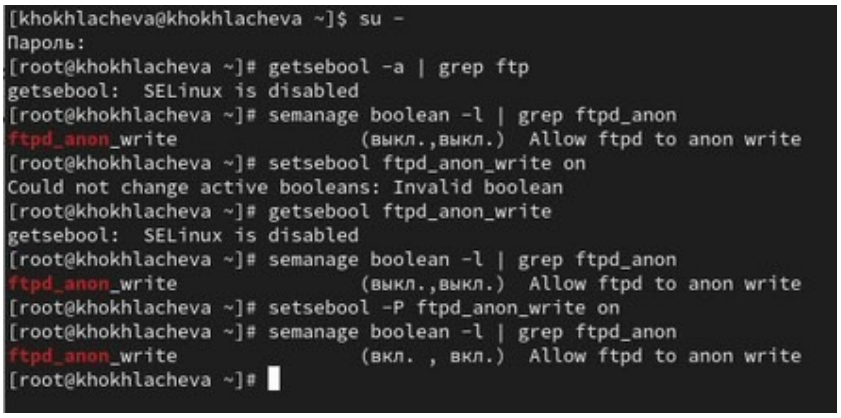

Рис. 2.10: Смотрим, изменяем

3 Ответы на вопросы

1. setenforce 0
2. getsebool -a
3. setroubleshoot-server (или setroubleshoot)
4. semanage fcontext -a -t httpd_sys_content_t “/web(/.*)?” и затем restorecon -Rv /web
5. /etc/selinux/config
6. В файле /var/log/audit/audit.log (через службу auditd)
7. semanage fcontext -l | grep ftp (или semanage fcontext -l -t ftp_t для более точного поиска)
8. Временно переключить SELinux в разрешающий режим: setenforce 0

4 Выводы

Мы получили навыки работы с контекстом безопасности и политиками SELinux.