Управление SELinux

Майоров Дмитрий Андреевич

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 SELinux. SELinux включен(enabled) и находится в принудительном режиме работы (enforcing). Тип политики: targeted. Конфигурационный режим: enforcing. Состояние политики: MS status не задан, deny_unknown разрешен. Проверка защиты памяти активна. Версия ядра политики: 33

Рисунок 2.1

Смотрим, в каком режиме работает SELinux.Он раюотает в принудительном режиме. Изменяем режим работы на разрешающий.

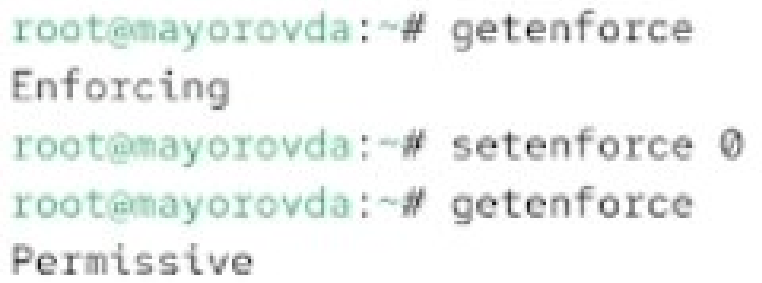

Рисунок 2.2

Открываем файл /etc/sysconfig/selinux для редактирования и устанавливаем следующий параметр. Перезагружаем систему

Рисунок 2.3

Смотрим статус SELinux. Видим, что он отключен. Пробуем переключить режим работы. Система говорит, что SELInux отключен. Мы не можем переключаться между отключённым и принудительным режимом без перезагрузки системы

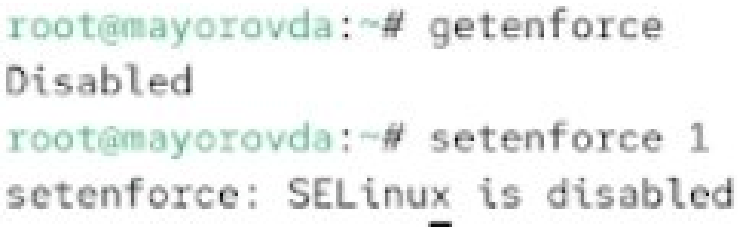

Рисунок 2.4

Открываем файл /etc/sysconfig/selinux для редактирования и устанавливаем следующий параметр. Перезагружаем систему

Рисунок 2.5

Смотрим текущую информацию о SELinux. Убеждаемся, что он работает в принудительном режиме

Рисунок 2.6

Смотрм контекст безопасности файла /etc/hosts. Копируем его в домашний каталог. Проверяем контект файла. Параметр контекста изменился на admin_home_t

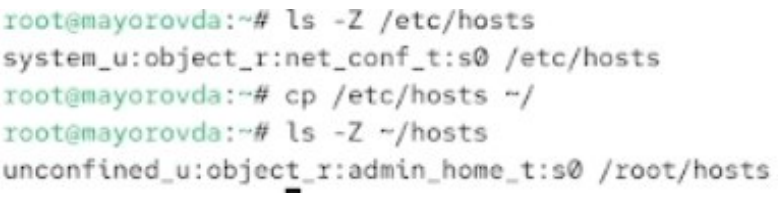

Рисунок 2.7

Пытаемся перезаписать существующий файл hosts из домашнего каталога в каталог /etc. Убеждаемся, что тип контекста по-прежнему установлен на admin_home_t

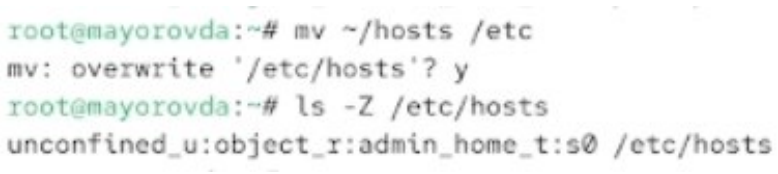

Рисунок 2.8

Исправляем контекст безопасности. Убеждаемся, что он изменился

Рисунок 2.9

Для массового исправления контекста безопасности на файловой системе ввоодим следующую команду и перезагружаем систему. При перезагрузке смотрим загрузочные сообщения. Видим, что файловая система перемаркирована

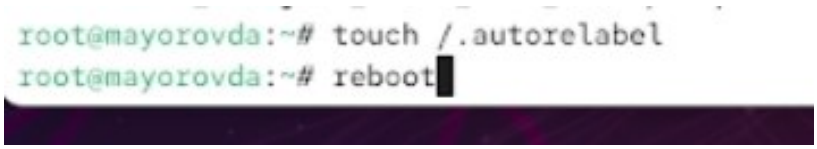

Рисунок 2.10

Рисунок 2.11

Устанавливаем необходимое программное обеспечение

Рисунок 2.12

Создаем новое хранилище для файлов web-сервера. Создаем файл index.html

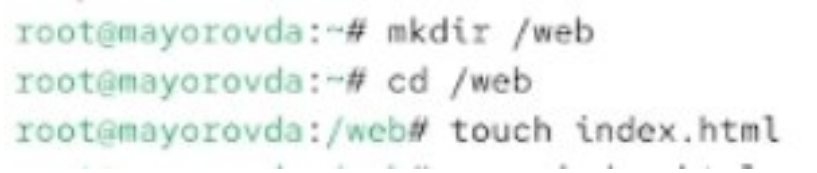

Рисунок 2.13

Открываем этот файл для редактирования и помещаем туда следующий текст

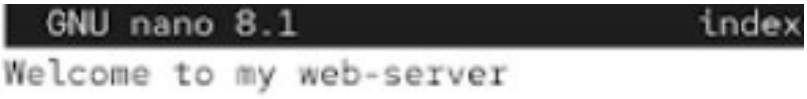

Рисунок 2.14

В файле /etc/httpd/conf/httpd.conf комментируем строку DocumentRoot «/var/www/html» и ниже добавляем строку DocumentRoot «/web»

Рисунок 2.15

Также ниже комментируем раздел и добавляем другой раздел, определяющий правила доступа

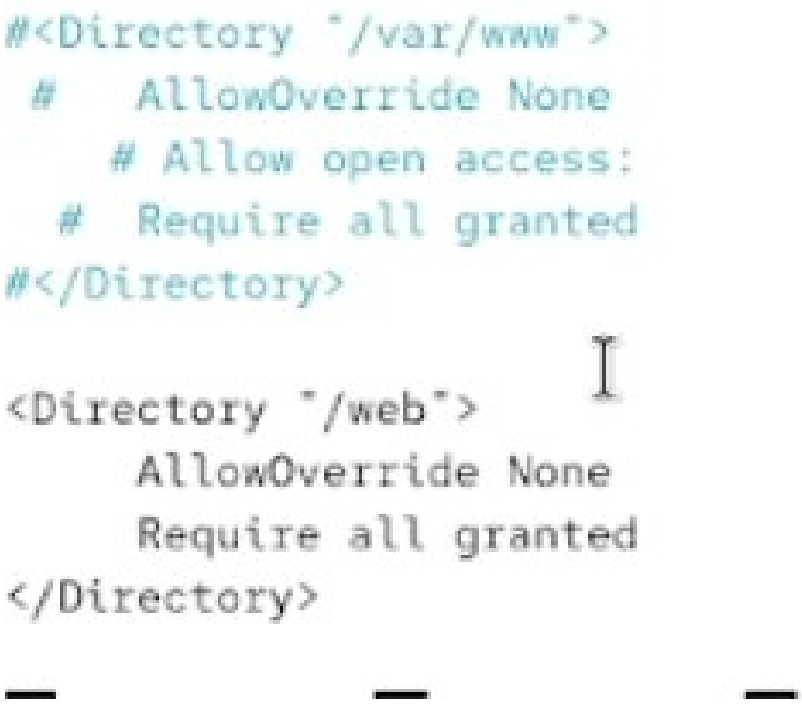

Рисунок 2.16

Запусткаем веб-сервер и службу httpd

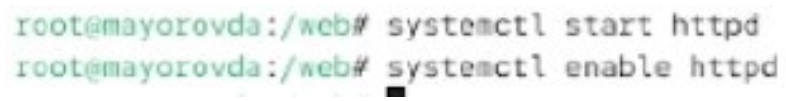

Рисунок 2.17

Открваем веб-сервер в текстовом браузере. Видим страницу REd Hat по умолчанию

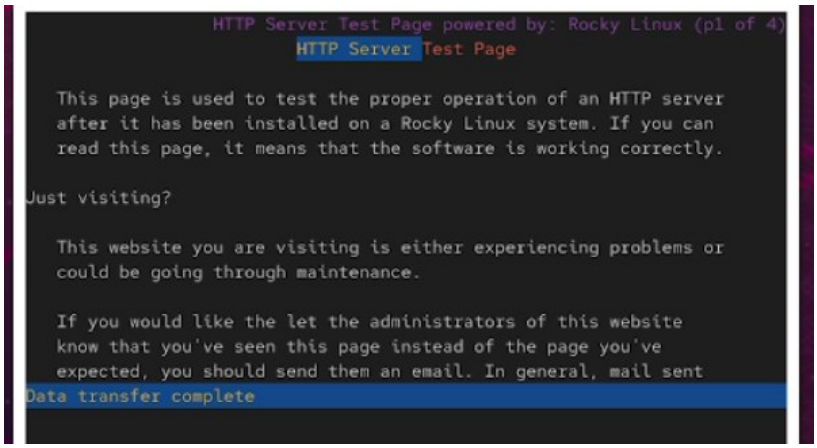

Рисунок 2.18

Применяем новую метку контекста к /web и восстанавливаем контекст безопастности

```
root@mayorovda:~# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?
"
root@mayorovda:~# restorecon -R -v /web
```

Рисунок 2.19

Перезагружаем систему и снова обращаемся к веб серверу. Теперь видим там запись, которую мы оставляли в файле index.html

Рисунок 2.20

Смотрим список переключателей SELinux для службы ftp

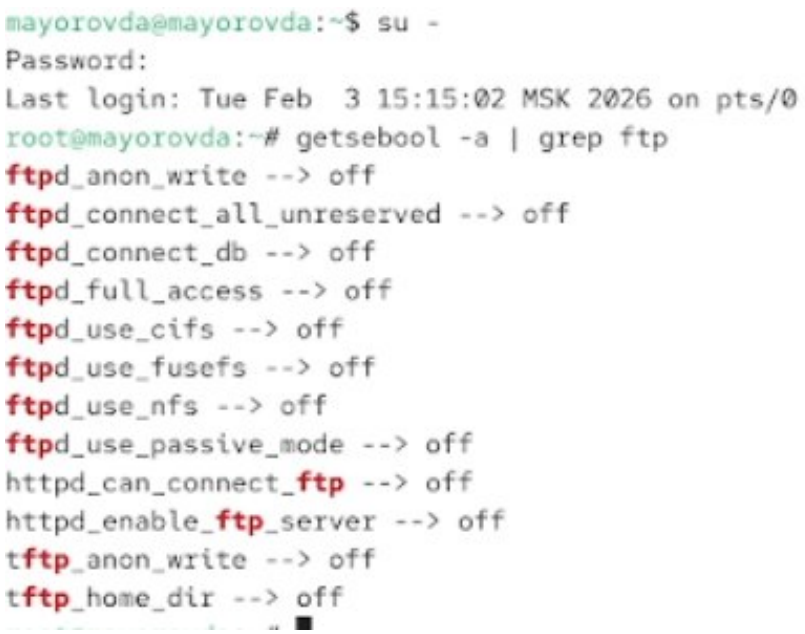

Рисунок 2.21

Для службы ftpd_anon смотрим список переключателей с пояснением, за что отвечает каждый переключатель, включён он или выключен

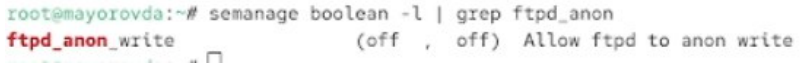

Рисунок 2.22

Изменяем текущее значение переключателя для службы ftpd_anon_write с off на on. Снова смотрим список переключателей для службы ftpd_anon. Смотрим список всех переключататателей

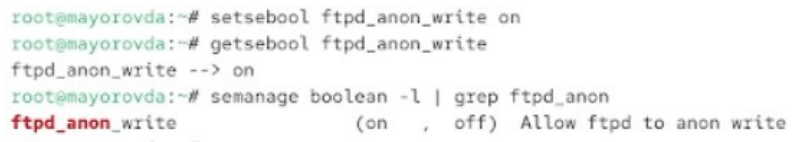

Рисунок 2.23

Изменяем постоянное значение переключателя для службы ftpd_anon_write с off на on. Смотрим список переключателей. Видим, что переключатель включен

3 Выводы

Получены навыки работы с контекстом безопасности и политиками SELinux.