Лабораторная работа № 9. Управление SELinux

Отчёт

Сергеев Даниил Олегович

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux. [1]

2 Задание

- Продемонстрировать навыки по управлению режимами SELinux
- Продемонстрировать навыки по восстановлению контекста безопасности SELinux
- Настроить контекст безопасности для нестандартного расположения файлов веб-службы
- Продемонстрировать навыки работы с переключателями SELinux

3 Ход выполнения лабораторной работы

3.1 Управление режимами SELinux

Запустим терминал, получим права администратора (su -) и просмотрим текущую информацию о состоянии SELinux с помощью команды sestatus -v.

Опишем информацию, выведенную на экран:

- SELinux status - статус работы службы SELinux;
- SELinuxfs mount - временная точка монтирования файловой системы SELinux;
- SELinux root directory - расположение файлов конфигурации SELinux;
- Loaded policy name - тип загруженной на данный момент политики SELinux;
- Current mode - текущий режим работы SELinux (Enforcing - блокировка нарушений и их фиксация, permissive - только фиксация нарушений, disabled - SELinux отключен);
- Mode from config file - режим работы, указанный в файле конфигурации /etc/selinux/config;
- Policy MLS status - статус политики MLS;
- Policy deny_unknown status - статус переключателя (флага) deny_unknown в текущей политике;
- Memory protection checking - режим работы защиты памяти;

- Max kernel policy version - максимальная версия политики, поддерживаемая ядром Linux.

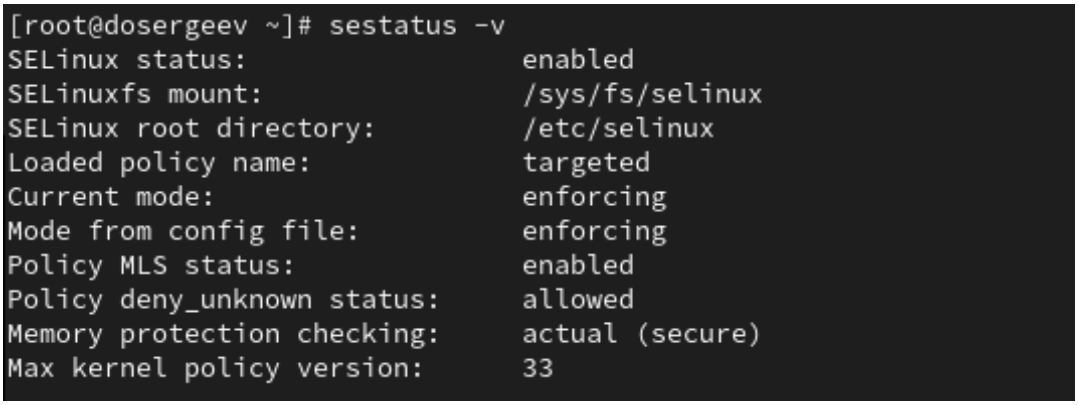

Рис. 3.1: Вывод команды sestatus -v (1)

- Process contexts - контексты безопасности процессов из конфига /etc/sestatus.conf.

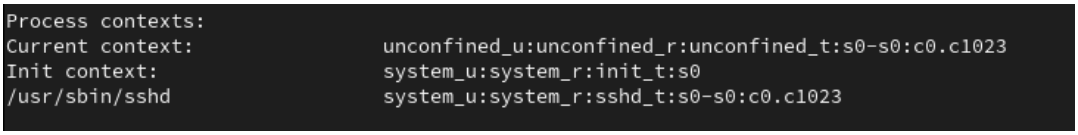

Рис. 3.2: Вывод команды sestatus -v (2)

- File contexts - контексты безопасности файлов из конфига /etc/sestatus.conf.

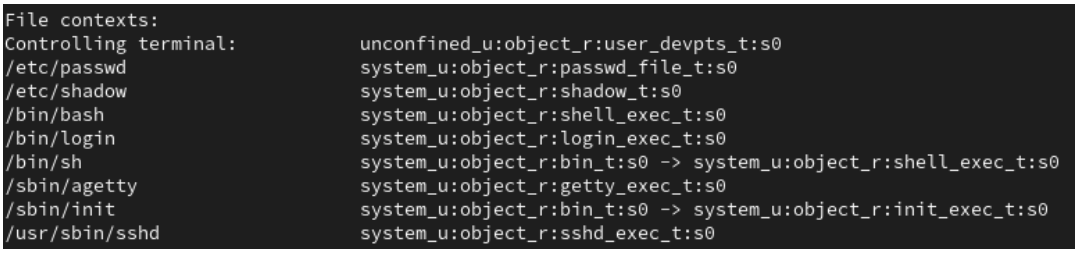

Рис. 3.3: Вывод команды sestatus -v (3)

Используя команду getenforce посмотрим, в каком режиме работает SELINUX. На данный момент он находится в режиме Enforcing. Изменим режим работы на

Permissive: setenforce 0; И снова проверим режим: на этот раз он изменился на Permissive.

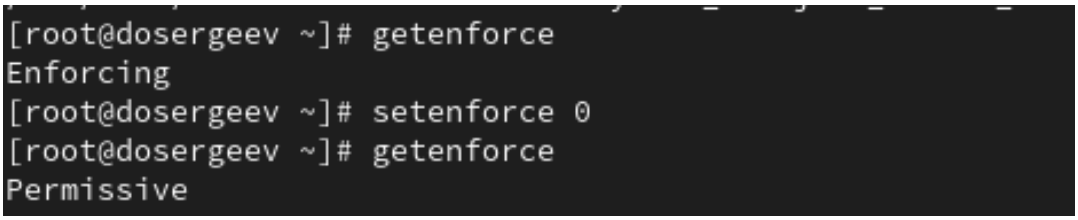

Рис. 3.4: Изменение режимов SELinux с помощью setenforce

В файле /etc/sysconfig/selinux изменим состояние режима на disabled и перезапустим систему.

Рис. 3.5: Установка режима SELINUX=disabled

После перезагрузки запустим терминал под учетной записью root и посмотрим текущий статус. Вывелась строка Disabled - значит SELinux отключен. Попробуем переключить режим работы на enforcing (setenforce 1). Так как SELinux отключен, на экран вывелась ошибка

- setenforce: SELinux is disabled

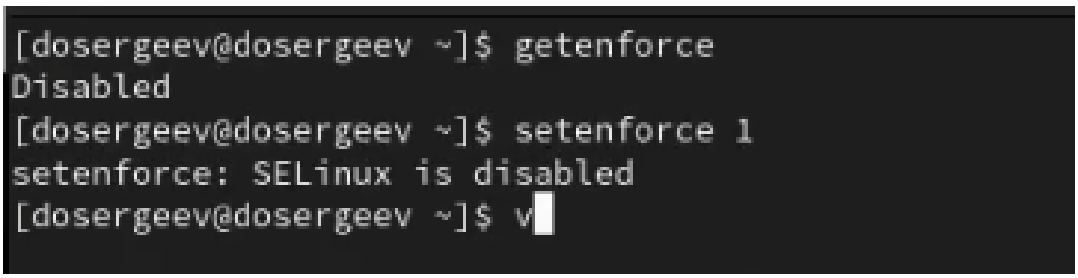

Рис. 3.6: Попытка переключение режима SELinux

Снова откроем файл /etc/sysconfig/selinux с помощью редактора и установим режим SELINUX=enforcing вручную. Перезагрузим систему.

Во время загрузки выводится предупреждающее сообщение о восстановлении меток SElinux.

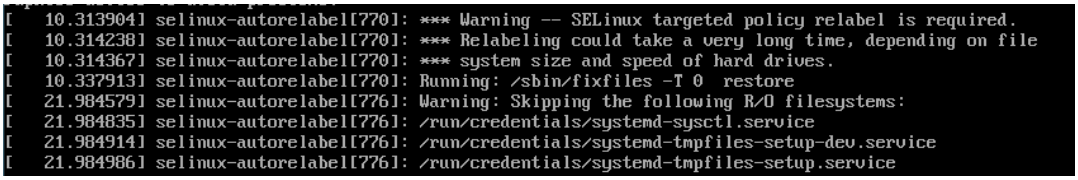

Рис. 3.7: Восстановление меток SELinux после перезапуска

После перезапуска снова введем команду sestatus -v, чтобы проверить режим: теперь выводится принудительный режим Enforcing, как и было запланировано.

3.2 Использование restorecon для восстановления контекста безопасности

Просмотрим контекст безопасности файла /etc/hosts. У файла наблюдается отметка контекста: net_conf_t. Скопируем этот файл в домашний каталог и снова проверим контекст. На этот раз установлено: admin_home_t.

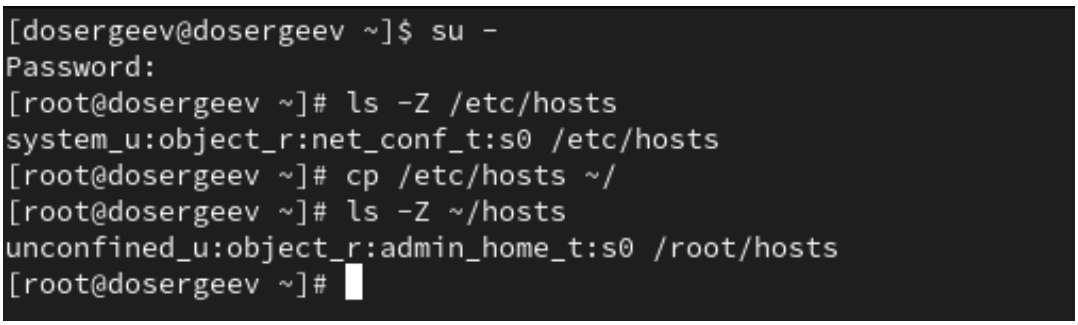

Рис. 3.8: Контекст безопасности файла после копирования

Попытаемся перезаписать файл /etc/hosts уже существующим файлом из домашнего каталога и убедимся, что контекст изменился. Так как он действительно изменился, исправим все до прежних настроек, использовав restorecon -v /etc/hosts. Теперь контекст снова равен net_conf_t.

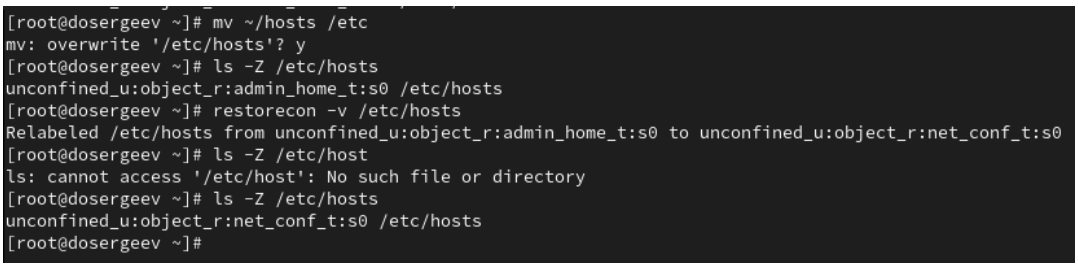

Рис. 3.9: Восстановление контекста безопасности /etc/hosts

Для массового исправления контекста создадим файл .autorelabel в корневом каталоге и перезапустим систему. Во время перезагрузки нажмем Esc, чтобы проверить загрузочные сообщение. SELinux запустил автоматическую перемаркировку контекста.

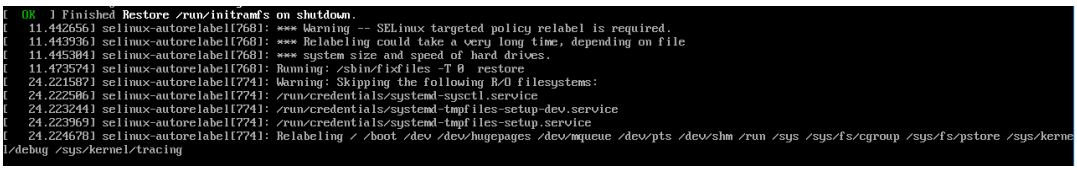

Рис. 3.10: Автоматическая перемаркировка SELinux во время перезапуска системы

3.3 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

Проверим установку пакетов httpd и lynx.

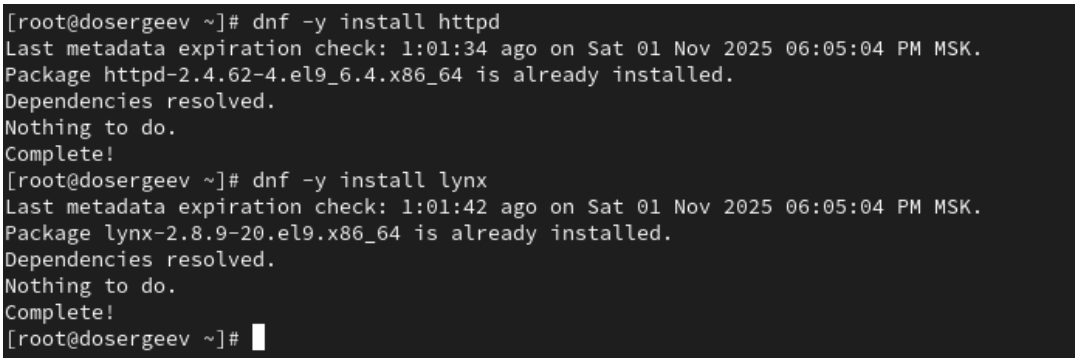

Рис. 3.11: Проверка патеков httpd, lynx

Так как они установлены, приступим к следующему заданию.

Создадим новое хранилище для файлов веб-сервера: mkdir /web; Также создадим индекс (в новом каталоге): touch index.html.

В индекс запишем сообщение - Welcome to my web-server.

Откроем файл /etc/httpd/conf/httpd.conf на редактирование. Закомментируем строку DocumentRoot и тег (раздел) Directory, после чего добавим те же строки, заменив пути /var/www/html и /var/www на /web.

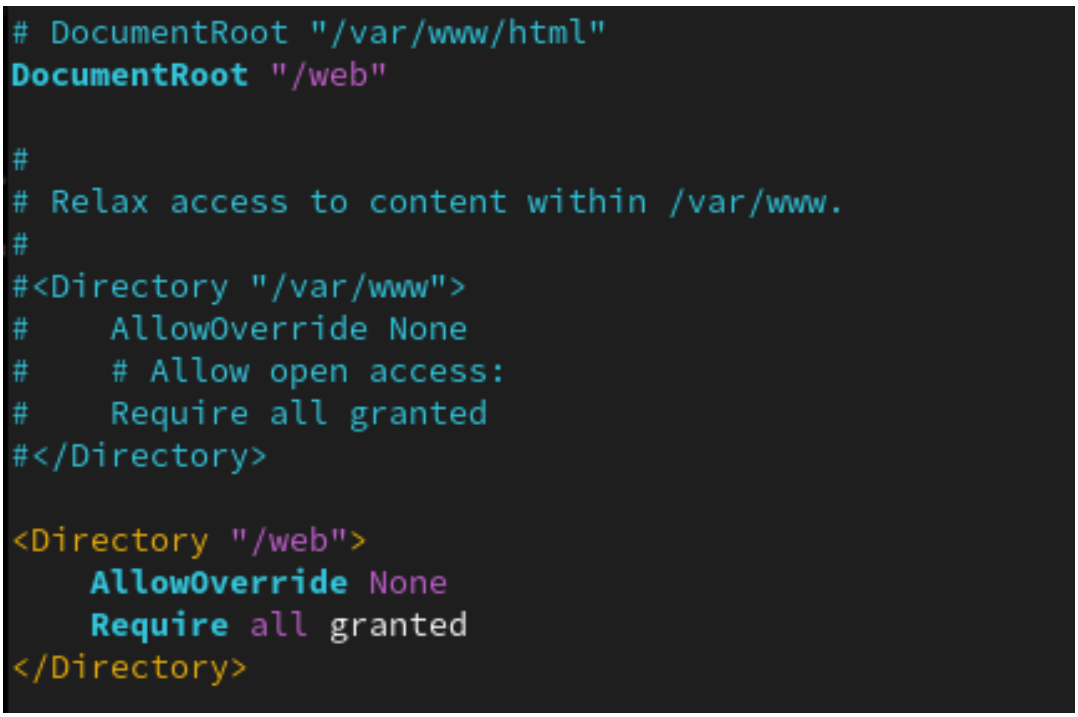

Рис. 3.12: Изменение конфигурации httpd

Запустим веб-сервер и службу httpd.

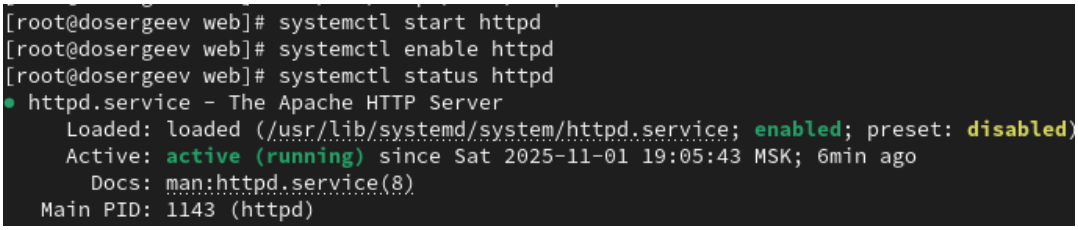

Рис. 3.13: Запуск httpd

Откроем терминал под своей основной учетной записью и обратимся к веб-серверу по адресу localhost в текстовом браузере lynx. Так как контекст безопасности не настроен, выводится веб-страница Red Hat по умолчанию, а не содержимое index.html

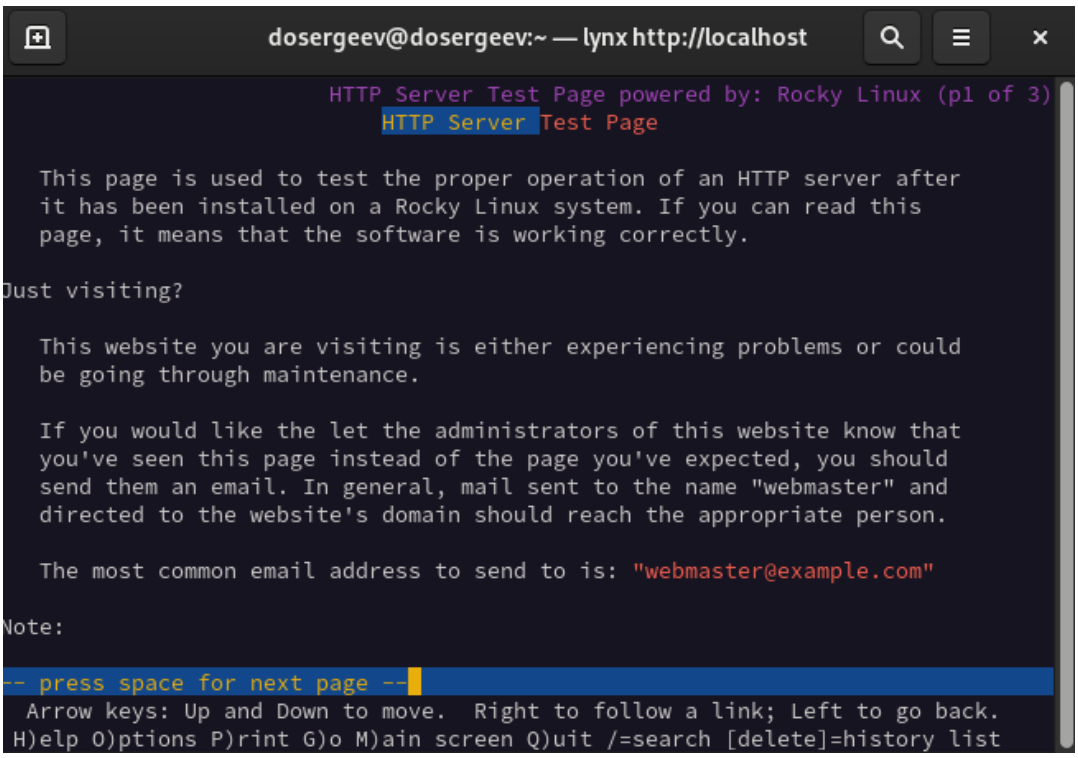

Рис. 3.14: Веб-страница до настройки контекста безопасности

В терминале с полномочиями администратора установим новую метку контекста к /web и восстановим контекст безопасности.

```
[root@dosergeev web]# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
[root@dosergeev web]# restorecon -R -v /web
Relabeled /web from unconfined_u:object_r:default_t:s0 to unconfined_u:object_r:httpd_sys_conten
t_t:s0
Relabeled /web/index.html from unconfined_u:object_r:default_t:s0 to unconfined_u:object_r:httpd
_sys_content_t:s0
[root@dosergeev web]#
```

Рис. 3.15: Настройка контекста для веб-сервера

Попробуем снова обратится к странице. Она не обновилась, поэтому перезапустим систему чтобы обновить настройки SELinux.

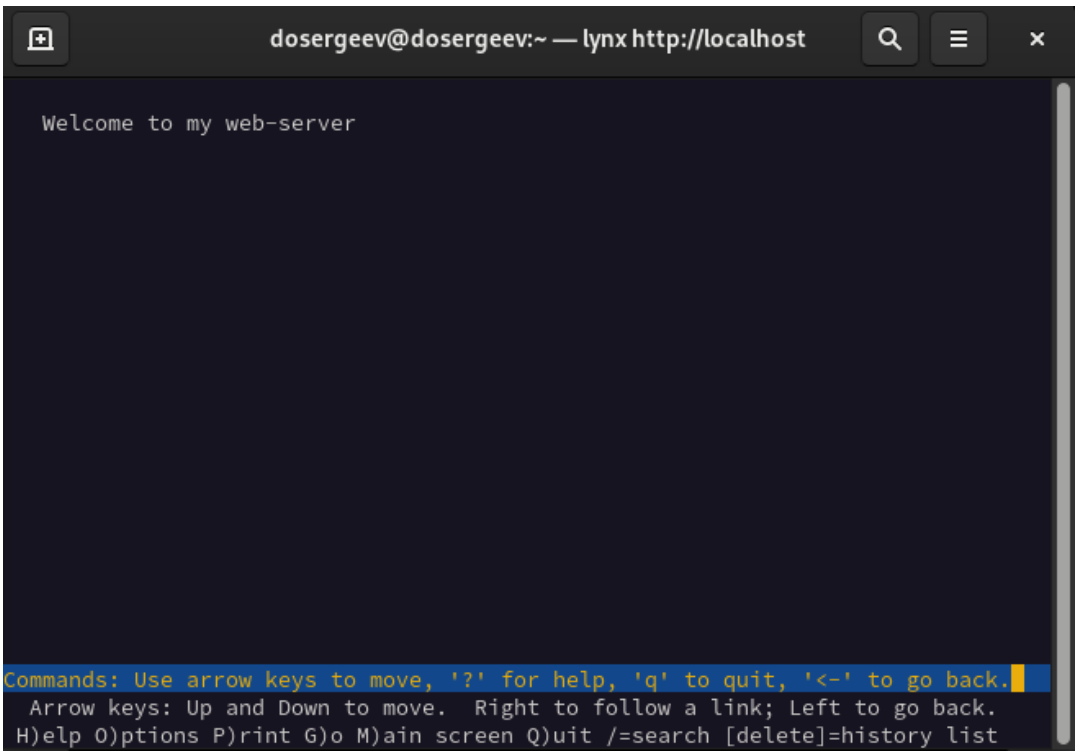

Рис. 3.16: Обновленная веб-страница

Теперь на экране отображена запись “Welcome to my web-server”.

3.4 Работа с переключателями SELinux

Снова запустим терминал под учетной записью root и посмотрим список переключателей SELinux для службы ftp. Отметим, что параметр ftpd_anon_write имеет значение off. Просмотрим список переключателей с пояснением для службы ftpd_anon.

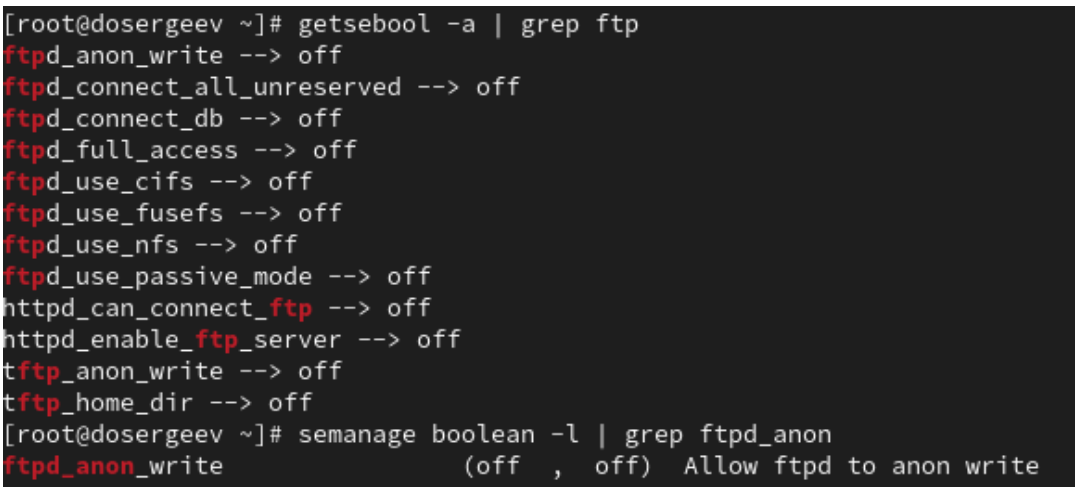

Рис. 3.17: Переключатели для службы ftp, ftpd_anon

Вывелся только один переключатель: ftpd_anon_write. Он имеет параметры (off - настройка времени выполнения отключена, off - постоянная настройка отключена) и краткое описание: “Позволить ftpd анонимную запись”.

Изменим текущее значение переключателя ftpd_anon_write с off на on: setsebool ftpd_anon_write on; Повторно посмотрим список переключателей (в том числе и с пояснением): getsebool ftpd_anon_write.

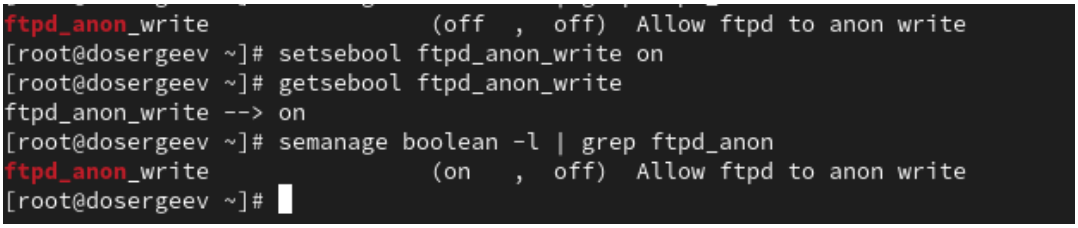

Рис. 3.18: Переключатель для службы ftpd_anon после изменения значения

Настройка времени выполнения включена, но постоянная настройка по-прежнему отключена.

Изменим постоянное значение переключателя с off на on: setsebool-P ftpd_anon_write on; Посмотрим список: semanage boolean-l | grep ftpd_anon

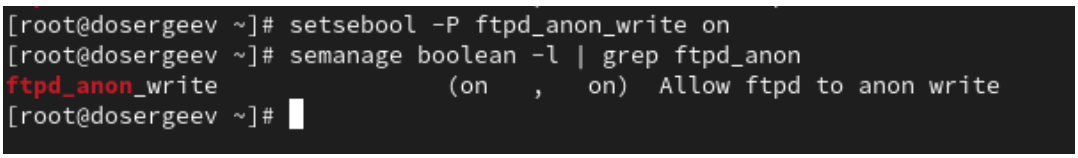

Рис. 3.19: Переключатели для службы ftp, ftpd_anon

Теперь переключатель имеет состояние (on , on). Это значит, что теперь он включен как постоянная настройка и как настройка времени выполнения.

4 Ответы на контрольные вопросы

1. Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете?

- setenforce 0

2. Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете?

- getsebool -a

3. Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита?

- setroubleshoot

4. Какие команды вам нужно выполнить, чтобы применить тип контекста httpd_sys_content_t к каталогу /web?

- semanage fcontext-a-t httpd_sys_content_t “/web(/.*)?” - добавляет правило в политику
- restorecon -R -v /web - обновляет политику

5. Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux?

- /etc/selinux/config или /etc/sysconfig/selinux

6. Где SELinux регистрирует все свои сообщения?

- /var/log/audit/audit.log

7. Вы не знаете, какие типы контекстов доступны для службы ftp. Какая команда позволяет получить более конкретную информацию?

- seinfo -t | grep ftp

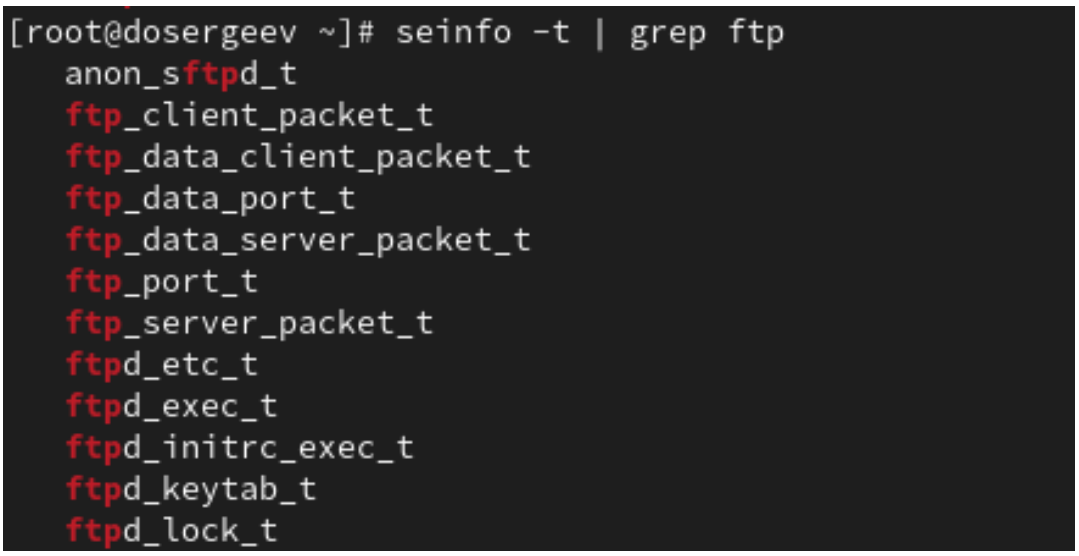

Рис. 4.1: Вывод seinfo

8. Ваш сервис работает не так, как ожидалось, и вы хотите узнать, связано ли это с SELinux или чем-то ещё. Какой самый простой способ узнать?

- Можно перевести SELinux в разрешающий режим (setenforce 0). Таким образом, если проблема связана с SELinux, то сервис перестанет блокироваться политикой, возобновив свою работу. Для дальнейшего анализа можно просмотреть журналы, ведь в режиме permissive SELinux все ещё отправляет логи.

5 Вывод

В результате выполнения лабораторной работы я получил навыки работы с контекстом безопасности и политиками SELinux, научился настраивать контекст безопасности для нестандартного расположения файлов веб сервера и переключатели для служб на примере ftp.

Список литературы

1. Kulyabov, Korolykova. Лабораторная работа № 9. Управление SELinux. https://esystem.rudn.ru/pluginfile.php/2843497/mod_resource/content/4/010-selinux.pdf; RUDN.