Отчет по лабораторной работе №6

Мандатное разграничение прав в Linux

Гурбангельдиев Мухаммет НФИ-03-18

Содержание

# Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux.

Проверить работу SELinx на практике совместно с веб-сервером Apache.

# Последовательность выполнения работы

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus (рис. 1)

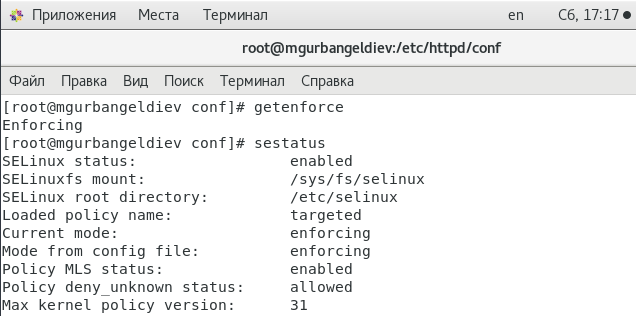


Figure 1: SELinux

1. Обратитесь с помощью браузера к веб-серверу, 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. 2)

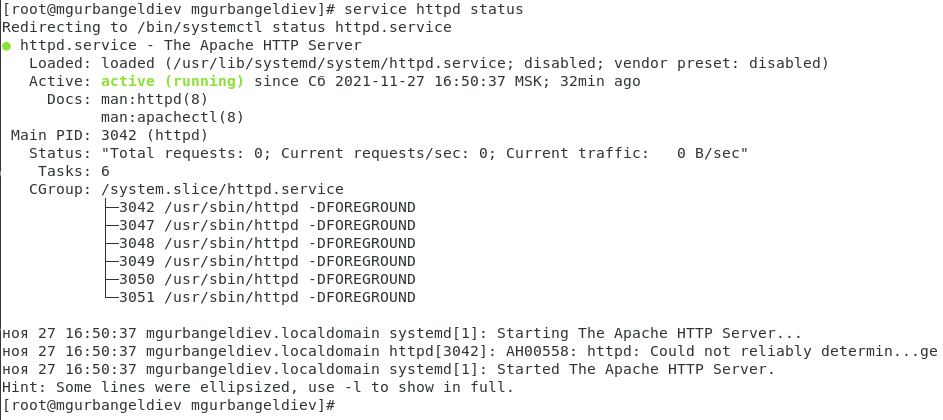


Figure 2: Apache HTTP Server

1. 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 (рис. 3)

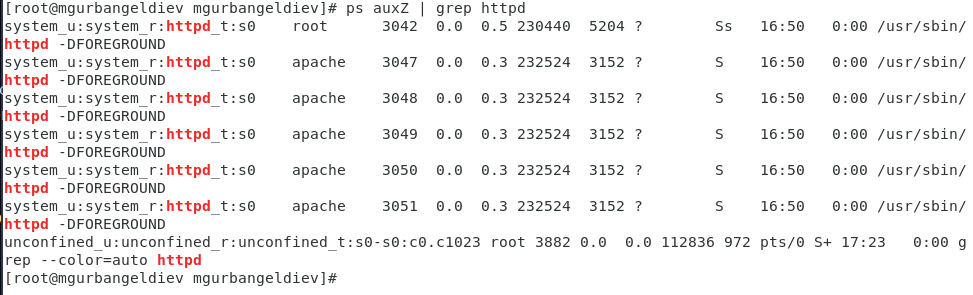


Figure 3: Apache в списке процессов

1. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды

sestatus -b | grep httpd

Обратите внимание, что многие из них находятся в положении «off». (рис. 4)

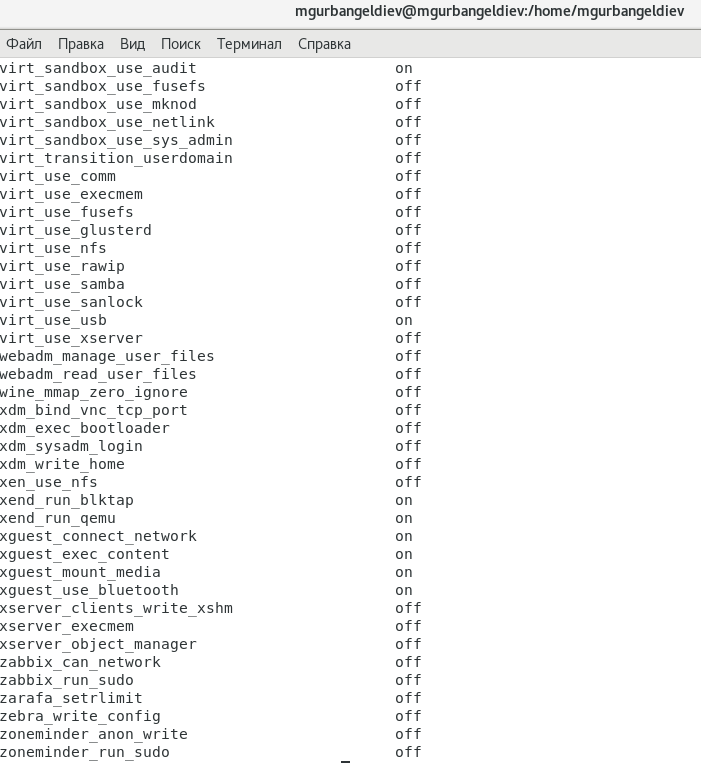


Figure 4: Текущее состояние переключателей SELinux для Apache

1. Посмотрите статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов. (рис. 5)

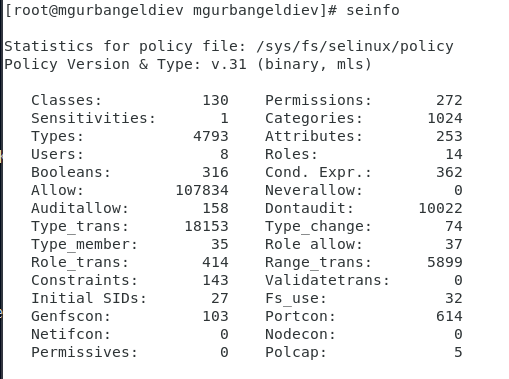


Figure 5: Статистику по политике

Множество типов: 4793. Множество пользователей: 8. Множество ролей: 14.

1. Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды (рис. 6)

ls -lZ /var/www



Figure 6: Определение типов файлов и поддиректорий

1. Определите тип файлов, находящихся в директории /var/www/html:

ls -lZ /var/www/html (рис. 7)

1. Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html.

Figure 7: Определение типов файлов и поддиректорий

Figure 7: Определение типов файлов и поддиректорий

1. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания: (рис. 8)

test

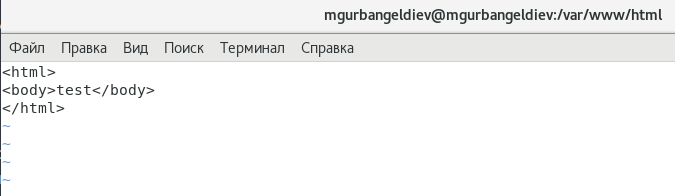


Figure 8: Файл test.html

1. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории

/var/www/html (рис. 9)



Figure 9: Контекст файла

1. Обратитесь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедитесь, что файл был успешно отображён. (рис. 10)

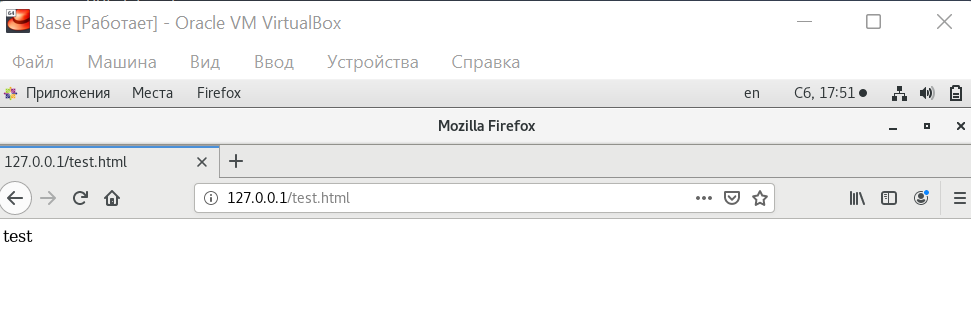


Figure 10: Обращение к файлу через браузер

1. Изучите справку man httpd\_selinux и выясните, какие контексты файлов определены для httpd. Сопоставьте их с типом файла test.html. Проверить контекст файла можно командой ls -Z.

ls -Z /var/www/html/test.html

Рассмотрим полученный контекст детально. Обратите внимание, что так как по умолчанию пользователи CentOS являются свободными от типа (unconfined в переводе с англ. означает свободный), созданному нами файлу test.html был сопоставлен SELinux, пользователь unconfined\_u. Это первая часть контекста. Далее политика ролевого разделения доступа RBAC используется процессами, но не файлами, поэтому роли не имеют никакого значения для файлов. Роль object\_r используется по умолчанию для файлов на «постоянных» носителях и на сетевых файловых системах. (В директории /ргос файлы, относящиеся к процессам, могут иметь роль system\_r. Если активна политика MLS, то могут использоваться и другие роли, например, secadm\_r. Данный случай мы рассматривать не будем, как и предназначение :s0).

Тип httpd\_sys\_content\_t позволяет процессу httpd получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер.

1. Измените контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на любой другой, к которому процесс httpd не должен иметь доступа, например, на samba\_share\_t: (рис. 11)

chcon -t samba\_share\_t /var/www/html/test.html

ls -Z /var/www/html/test.html

После этого проверьте, что контекст поменялся

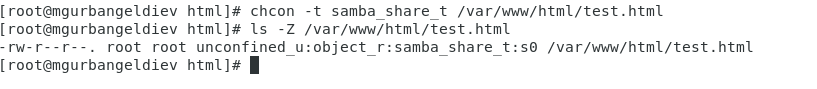


Figure 11: Изменение контекста файла

1. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Вы должны получить сообщение об ошибке: (рис. 12)

Forbidden

You don’t have permission to access /test.html on this server.



Figure 12: Обращение к файлу через браузер

1. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? (рис. 13) (рис. 14)

ls -l /var/www/html/test.html

Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл:

tail /var/log/messages

Если в системе окажутся запущенными процессы setroubleshootd и audtd, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле /var/log/audit/audit.log. Проверьте это утверждение самостоятельно.

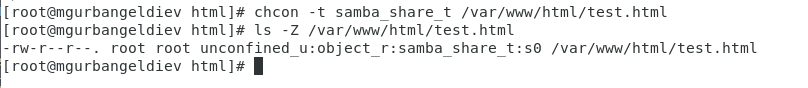


Figure 13: Права доступа

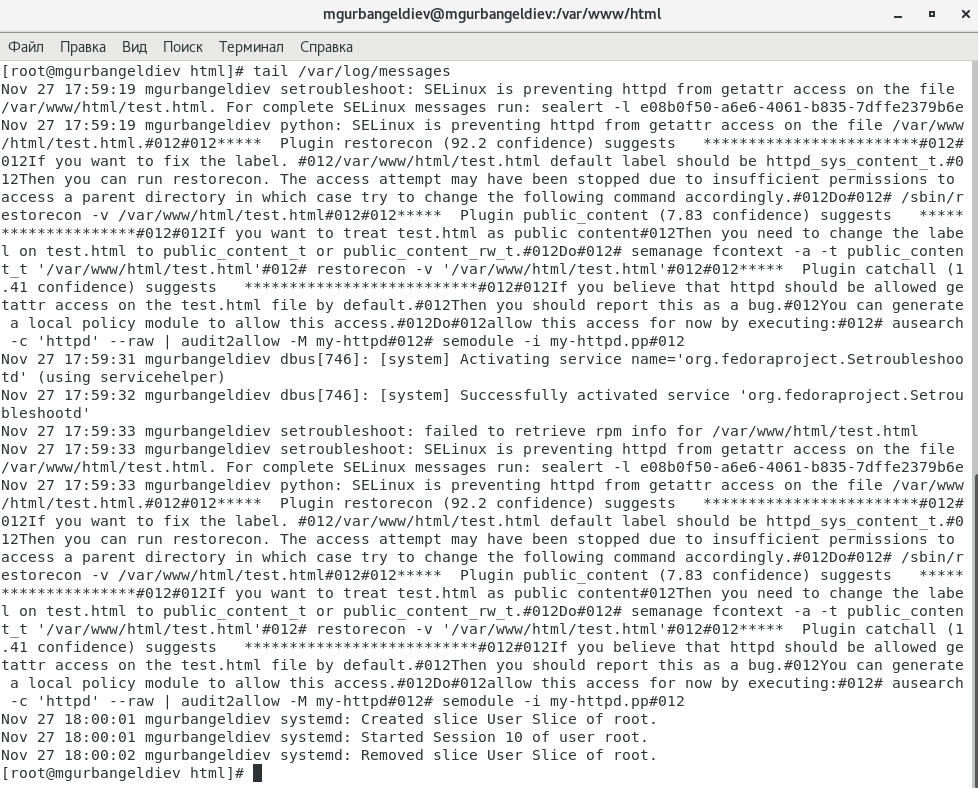


Figure 14: log-файлы веб-сервера Apache

1. Попробуйте запустить веб-сервер Apache на прослушивание ТСР-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf найдите строчку Listen 80 и замените её на Listen 81. (рис. 15)

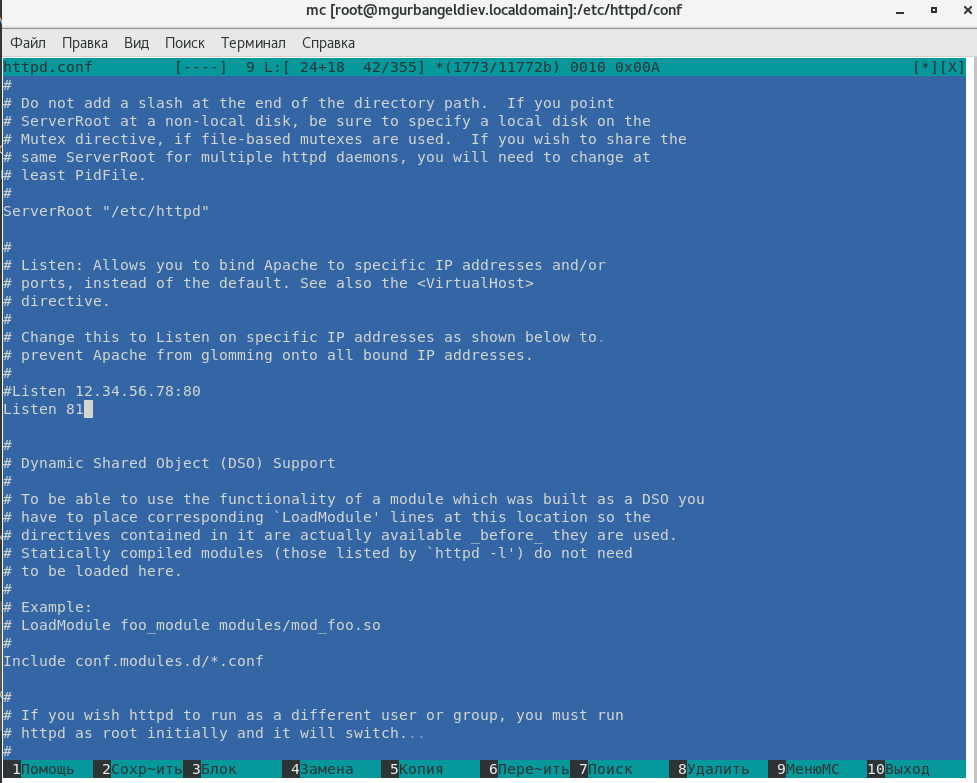


Figure 15: ТСР-порт 81

1. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему? (рис. 16)

Figure 16: Перезапуск веб-сервера Apache

Figure 16: Перезапуск веб-сервера Apache

Никакого сбоя не произошло.

1. Проанализируйте лог-файлы: (рис. 17)

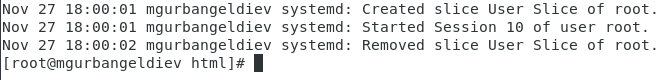


Figure 17: log-файлы веб-сервера Apache

1. Выполните команду

semanage port -a -t http\_port\_t -р tcp 81

После этого проверьте список портов командой

semanage port -l | grep http\_port\_t

Убедитесь, что порт 81 появился в списке. (рис. 18)

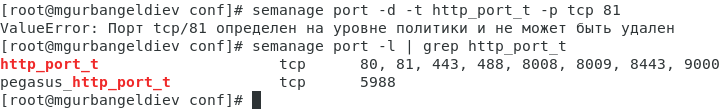


Figure 18: Проверка порта

1. Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему он сейчас запустился, а в предыдущем случае не смог? (рис. 19)

Figure 19: Презапуск веб-сервера Apache

Figure 19: Презапуск веб-сервера Apache

1. Верните контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/ test.html: (рис. 20)

chcon -t httpd\_sys\_content\_t /var/www/html/test.html

После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html.

Вы должны увидеть содержимое файла — слово «test». (рис. 21)

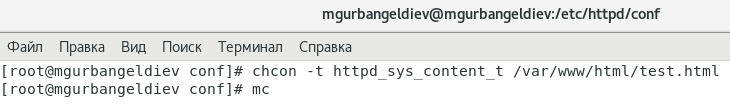


Figure 20: Изменение контекста

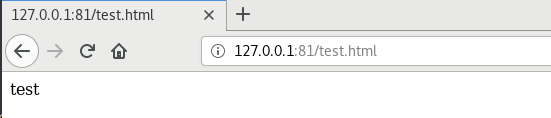


Figure 21: Обращение к файлу через браузер

1. Исправьте обратно конфигурационный файл apache, вернув Listen 80. (рис. 22)

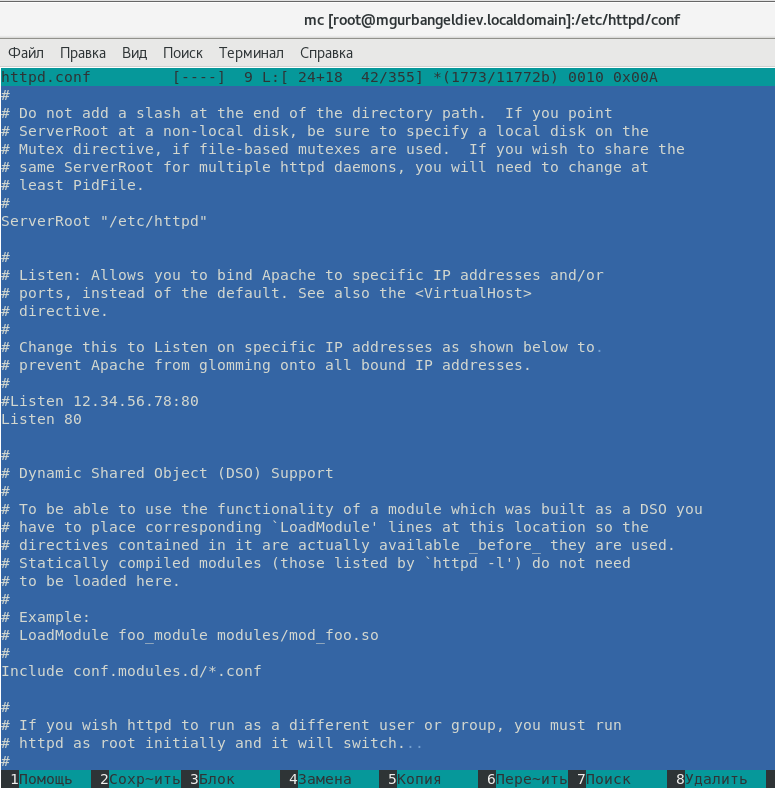


Figure 22: TCP-порт 80

1. Удалите привязку http\_port\_t к 81 порту:

semanage port -d -t http\_port\_t -p tcp 81

и проверьте, что порт 81 удалён. (рис. 23) (рис. 24)

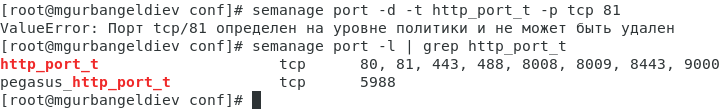


Figure 23: Удаление TCP-порта 81

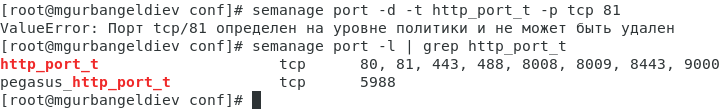


Figure 24: Удаление TCP-порта 81

1. Удалите файл /var/www/html/test.html:

rm /var/www/html/test.html (рис. 25)

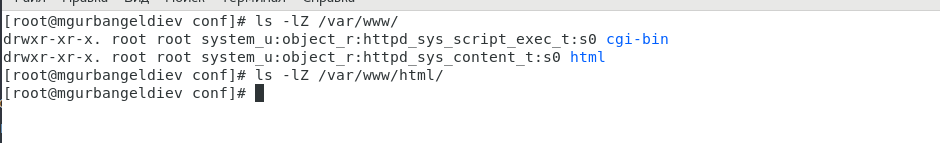


Figure 25: Удаление файла

# Выводы

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux.

Проверил работу SELinx на практике совместно с веб-сервером Apache.