Отчёт по лабораторной работе №6

Мандатное разграничение прав в Linux

Волков Тимофей Евгеньевич

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.

# Выполнение лабораторной работы

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

Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает:  
service httpd status  
Если не работает, запустите его так же, но с параметром start (fig. 1).

Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт (fig. 1). Например, можно использовать команду  
ps auxZ | grep httpd

Контекст безопасности - system\_u:system\_r:httpd\_t

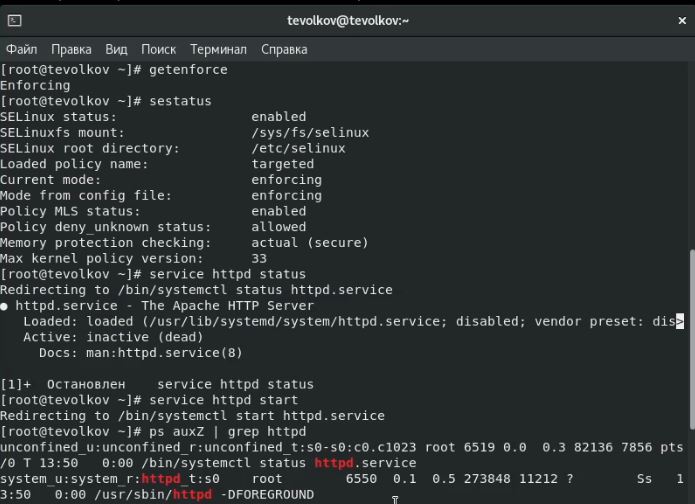


Figure 1: Начало работs с apache

Посмотрите текущее состояние переключателей SELinux для Apache (fig. 2) с помощью команды  
sestatus -b httpd

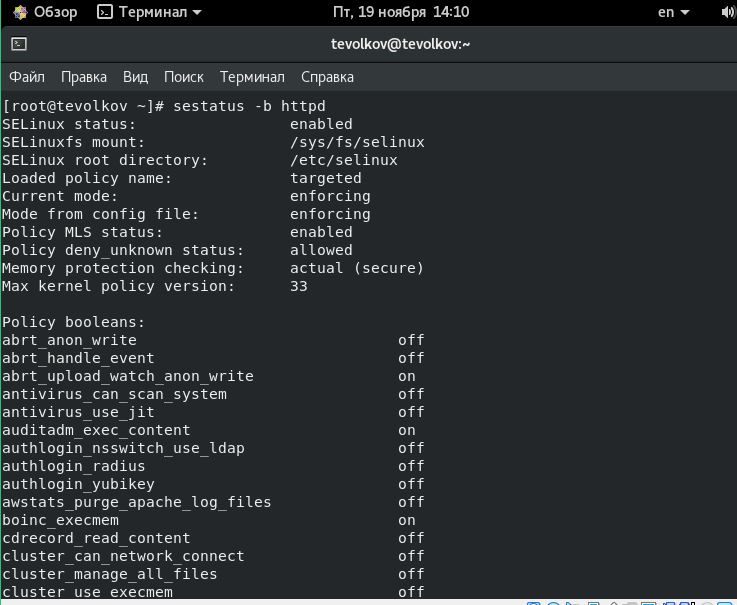


Figure 2: Состояние переключателей

Посмотрите статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов (fig. 3).

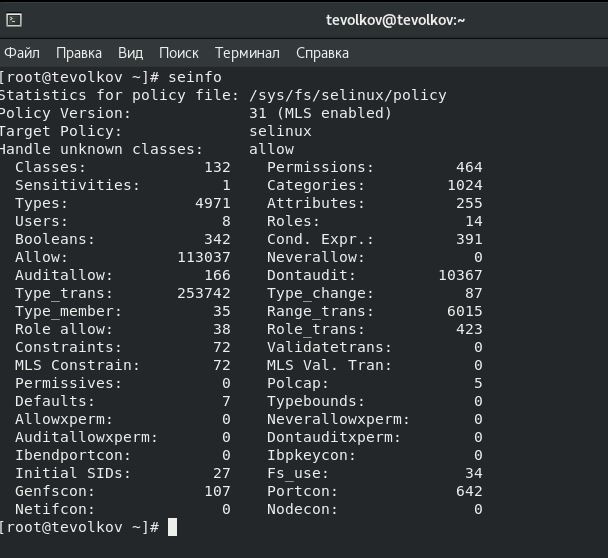


Figure 3: Статистика по политике

Определите тип файлов и поддиректорий, находящихся в директории /var/www (fig. 4), с помощью команды  
ls -lZ /var/www

Определите тип файлов, находящихся в директории /var/www/html (fig. 4):  
ls -lZ /var/www/html

Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html. Позволено только владельцу.

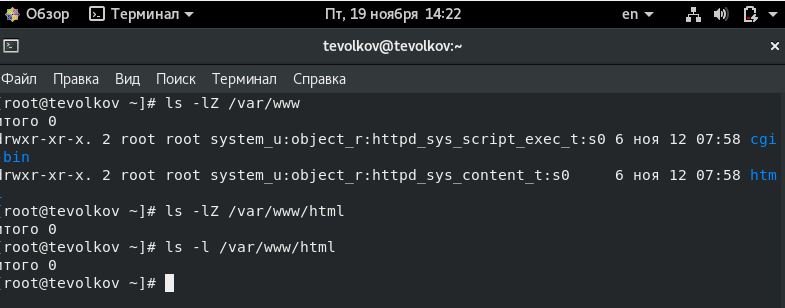


Figure 4: Тип файлов и поддерикторий

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 (fig. 5):

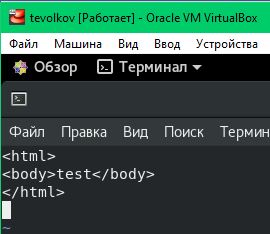


Figure 5: Файл test.html

Проверьте контекст созданного вами файла.  
unconfined\_u:object\_r:httpd\_sys\_content\_t - контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html (fig. 6).



Figure 6: Проверка контеста

Обратитесь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедитесь, что файл был успешно отображён (fig. 7).

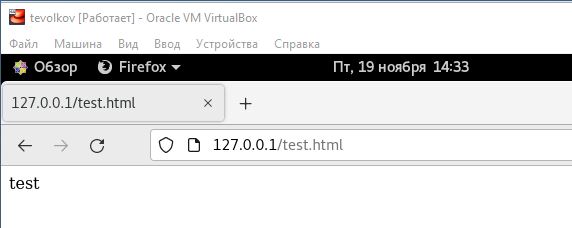


Figure 7: Вывод файла

Изучите справку man httpd и выясните, какие контексты файлов определены для httpd. Сопоставьте их с типом файла test.html. Контектсы совпадают. Проверить контекст файла можно командой ls -Z (fig. 8).  
ls -Z /var/www/html/test.html

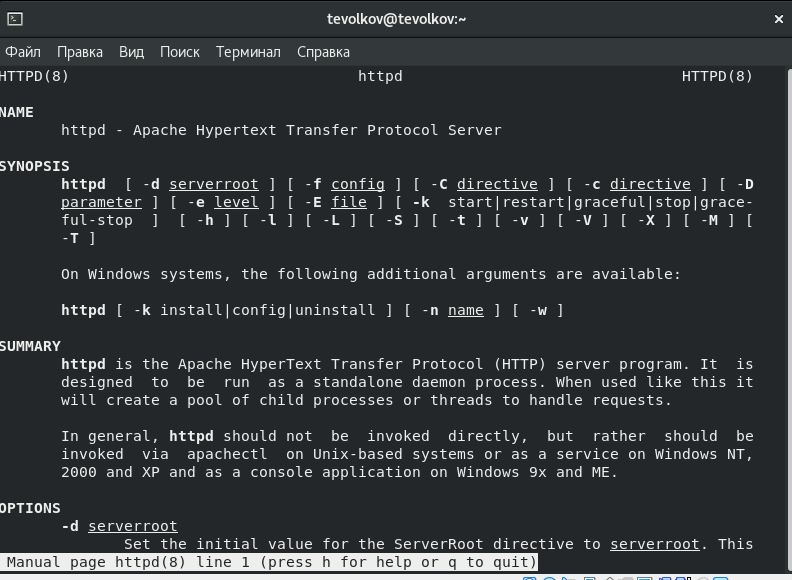


Figure 8: Справка по apache

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 (fig. 9):  
chcon -t samba\_share\_t /var/www/html/test.html  
ls -Z /var/www/html/test.html  
После этого проверьте, что контекст поменялся.

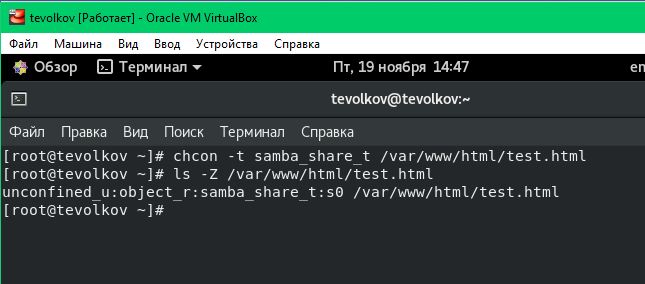


Figure 9: Изменение контекста файла

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 (fig. 10).

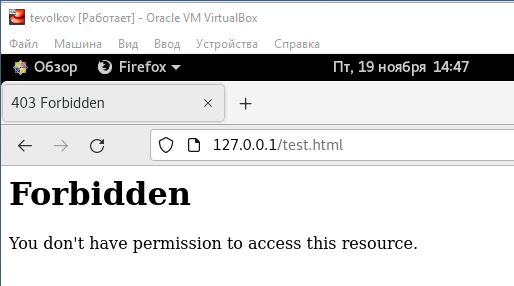


Figure 10: Ошибка доступа

Файл не был отображён так как у httpd не было доступа к измененному контексту. Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл (fig. 11):  
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 (fig. 11).

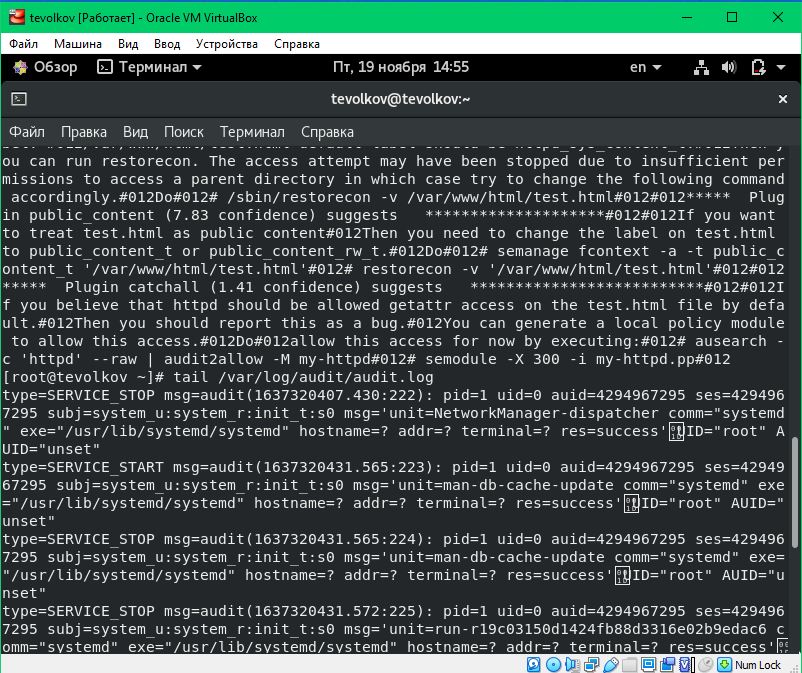


Figure 11: log-файлы

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.

Выполните перезапуск веб-сервера Apache (fig. 12).

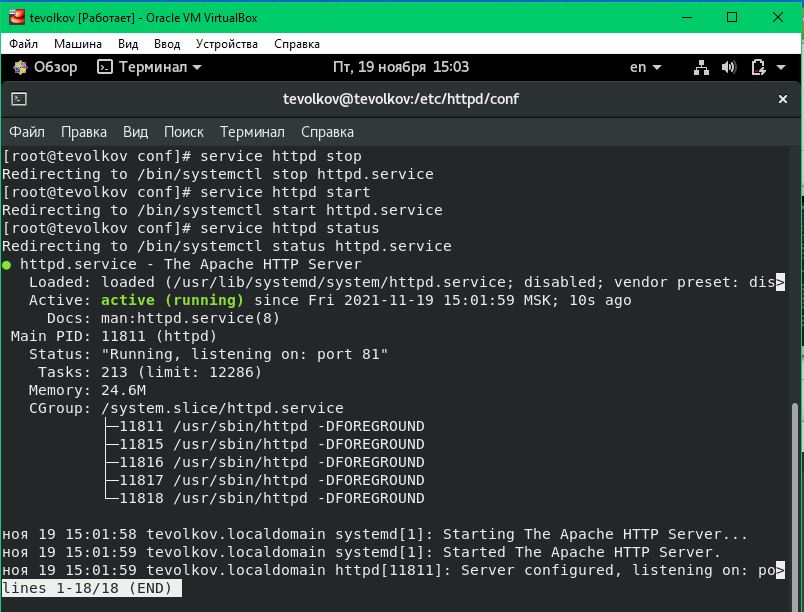


Figure 12: Перезапуск веб-сервера Apache

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 (fig. 13).

Попробуйте запустить веб-сервер Apache ещё раз (fig. 13).

Верните контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/test.html (fig. 13):  
chcon -t httpd\_sys\_content\_t /var/www/html/test.html

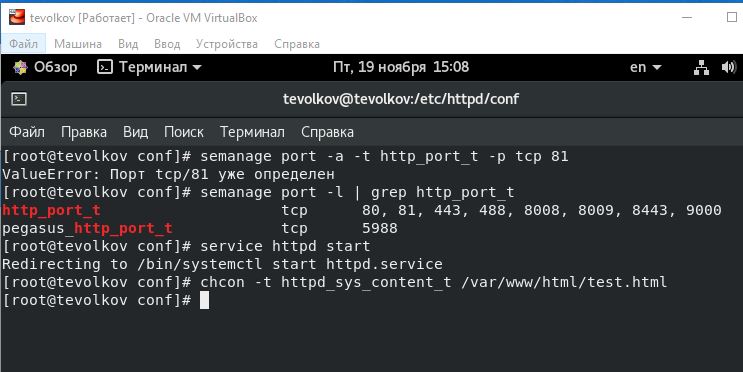


Figure 13: Подготовка к запуску файла test.html

После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html (fig. 14).  
Вы должны увидеть содержимое файла — слово «test»

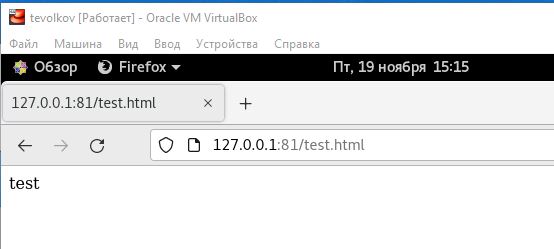


Figure 14: Вывод файла

Исправьте обратно конфигурационный файл apache, вернув Listen 80.

Удалите привязку http\_port\_t к 81 порту: semanage port -d -t http\_port\_t -p tcp 81

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

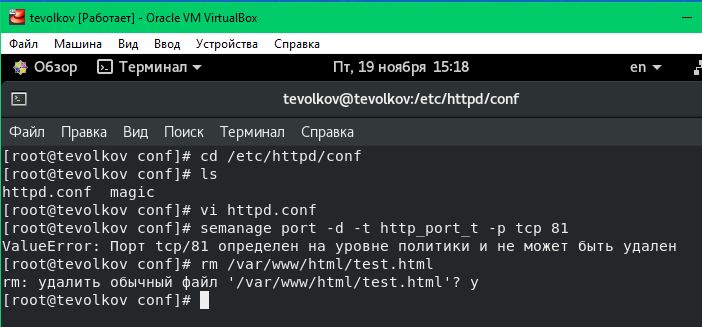


Figure 15: Возврат к начальным настройкам

# Выводы

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinx на практике совместно с веб-сервером Apache.