Отчет по лабораторной работе №6

Мандатное разграничение прав в Linux

Александр Олегович Воробьев

Содержание

# 1 Цель работы

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

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

# 2 Последовательность выполнения работы

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью ко- манд getenforce и sestatus.

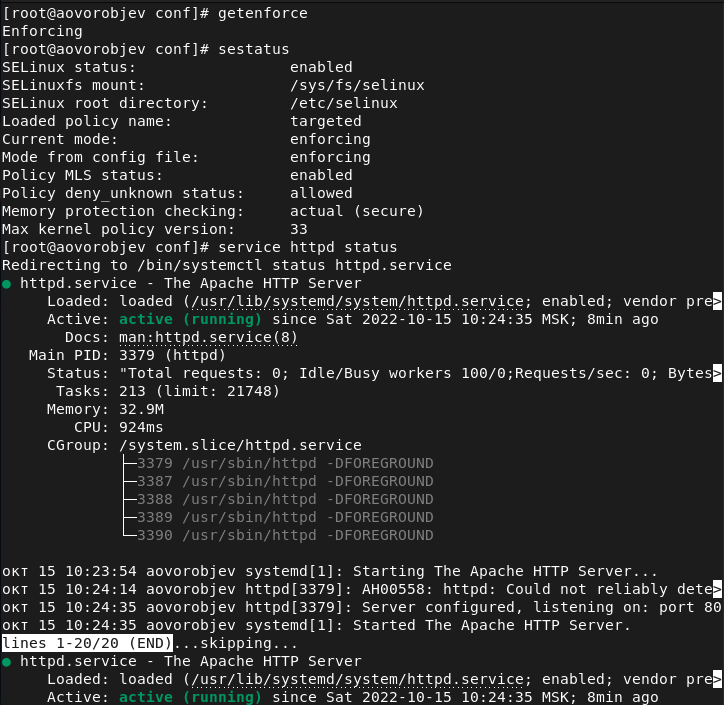


Figure 1: Выполнение команд

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.
2. Найдитевеб-серверApacheвспискепроцессов,определитеегоконтекст безопасности и занесите эту информацию в отчёт. Например, можно ис- пользовать команду  
   ps auxZ | grep httpd  
   или  
   ps -eZ | grep httpd
3. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды sestatus -bigrep httpd  
   Обратите внимание, что многие из них находятся в положении «off».

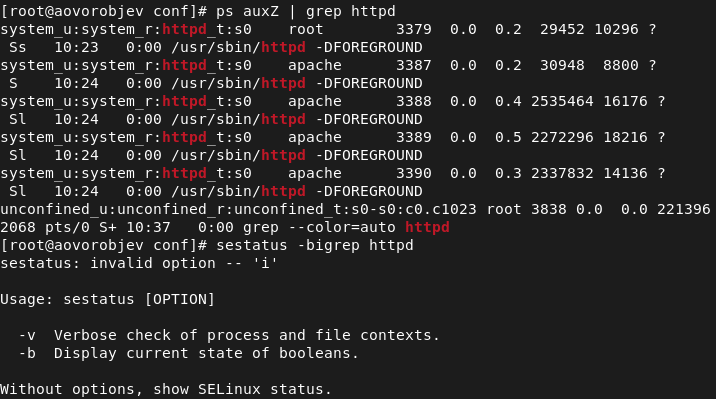


Figure 2: поиск веб-сервера в списке процессов

1. Посмотритестатистикупополитикеспомощьюкомандыseinfo,также определите множество пользователей, ролей, типов.

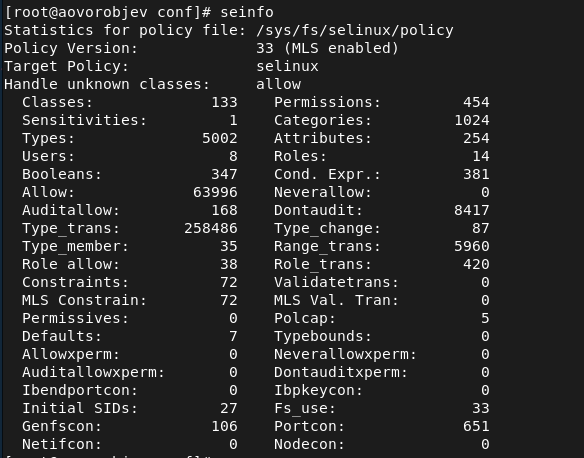


Figure 3: Статистика

1. Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды  
   ls -lZ /var/www
2. Определите тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html
3. Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html.
4. Создайте от имени суперпользователя (так как в дистрибутиве по- сле установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания:

* test

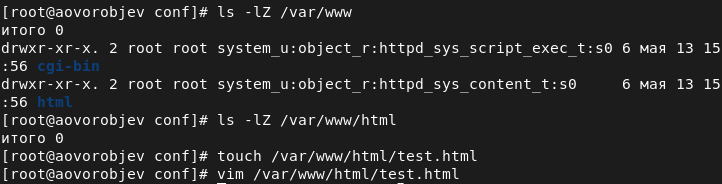


Figure 4: Выполнение команд

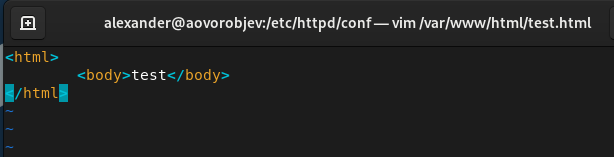


Figure 5: Текст файла

1. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html.
2. Обратитесь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедитесь, что файл был успеш- но отображён.

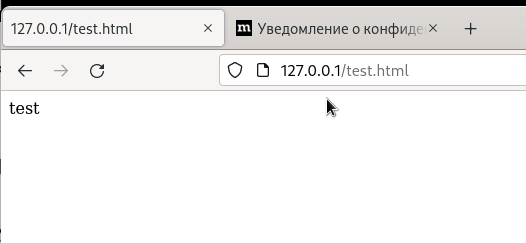


Figure 6: Отображение файла

1. Изучите справку man httpd\_selinux и выясните, какие контек- сты 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 про- цессами, но не файлами, поэтому роли не имеют никакого значения для файлов. Роль object\_r используется по умолчанию для файлов на «по- стоянных» 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 фай- лу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер.
2. 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:  
   chcon -t samba\_share\_t /var/www/html/test.html  
   ls -Z /var/www/html/test.html

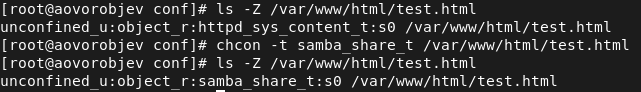


Figure 7: Проверка и изменение контекста

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

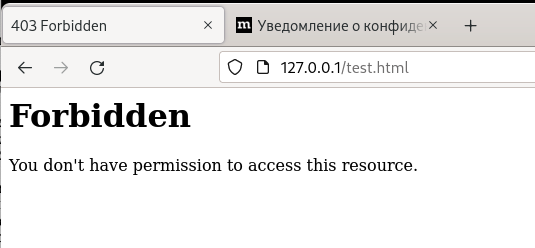


Figure 8: Попытка получить доступ к файлу

1. Проанализируйтеситуацию.Почемуфайлнебылотображён,еслиправа доступа позволяют читать этот файл любому пользователю? ls -l /var/www/html/test.html Просмотрите log-файлы веб-сервера Apache. Также просмотрите си- стемный 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 утвержде- ние самостоятельно.

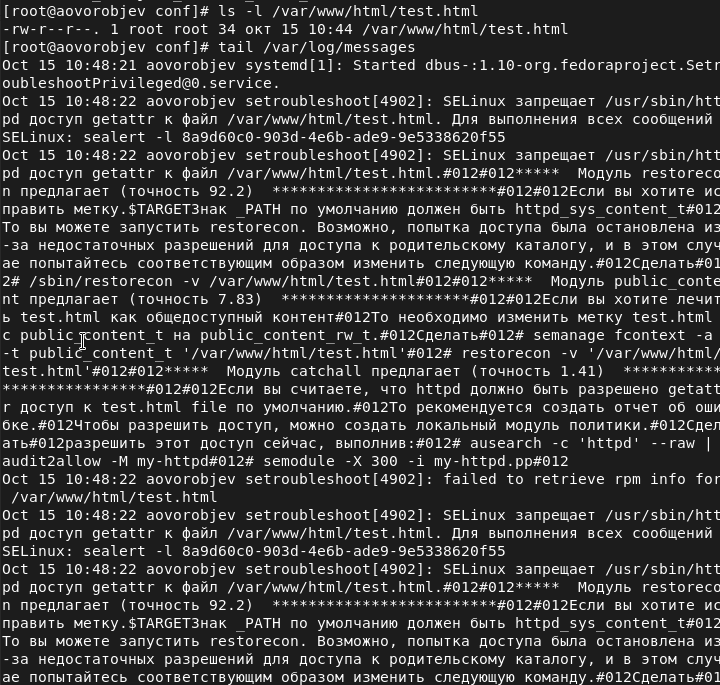


Figure 9: Проверка log-файлов

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.

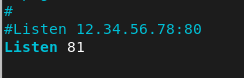


Figure 10: Изменение порта

1. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему?

Figure 11: Перезапуск веб-сервера

Figure 11: Перезапуск веб-сервера

1. Проанализируйте лог-файлы:  
   tail -nl /var/log/messages  
   Просмотрите файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log и выясните, в каких файлах появились записи.

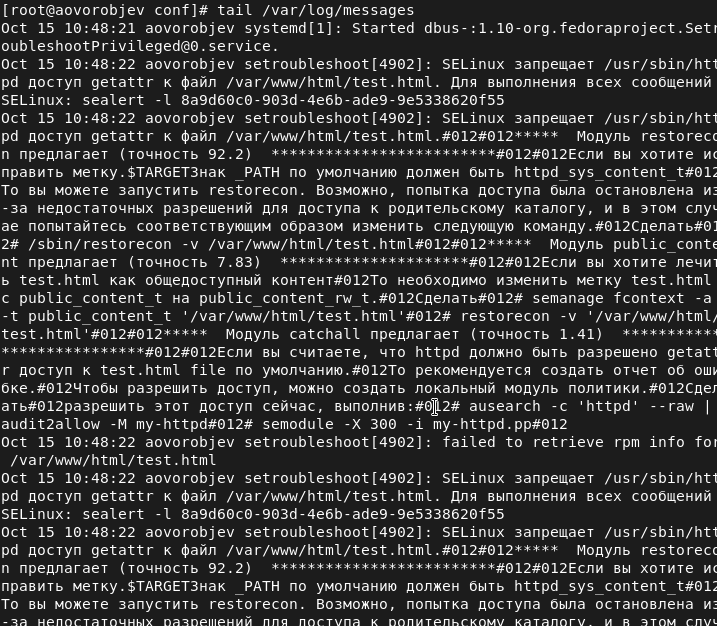


Figure 12: Проверка log-файлов

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.

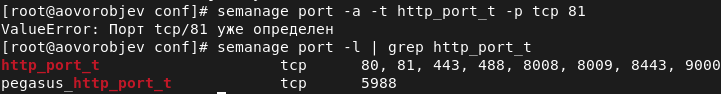


Figure 13: Выполнение команд

1. Попробуйтезапуститьвеб-серверApacheещёраз.Понялиливы,почему он сейчас запустился, а в предыдущем случае не смог?
2. Вернитеконтекстhttpd\_sys\_cоntent\_\_tкфайлу/var/www/html/test.html: chcon -t httpd\_sys\_content\_t /var/www/html/test.html После этого попробуйте получить доступ к файлу через веб-сервер, вве- дя в браузере адрес http://127.0.0.1:81/test.html. Вы должны увидеть содержимое файла — слово «test».

Figure 14: Перезапуск веб-сервера

Figure 14: Перезапуск веб-сервера

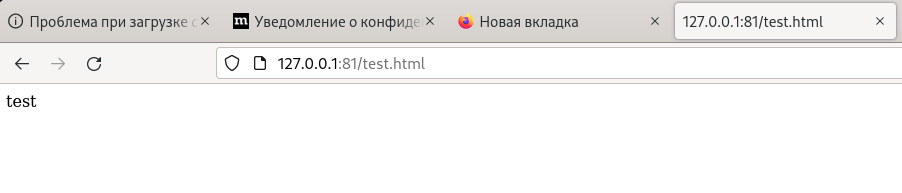


Figure 15: Проверка отображения файла

1. Исправьтеобратноконфигурационныйфайлapache,вернувListen80.

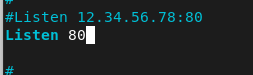


Figure 16: Изменение порта

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.
2. Удалитефайл/var/www/html/test.html: rm /var/www/html/test.html

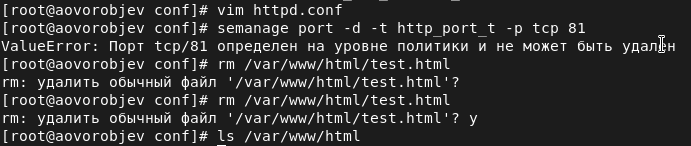


Figure 17: Удаление привязки и файла

# 3 Выводы

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