Отчёт по лабораторной работе 6

Ду нашсименту Висенте Феликс

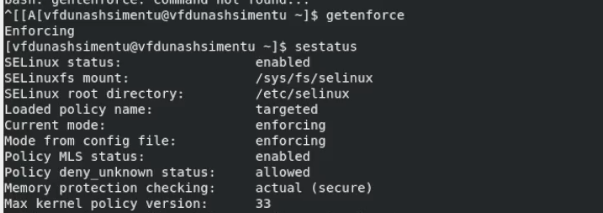
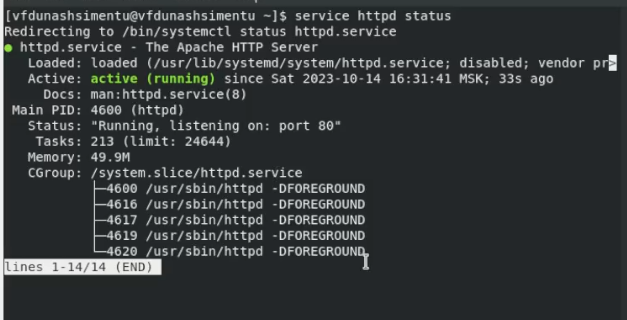
Содержание

## 6.1. Цель работы

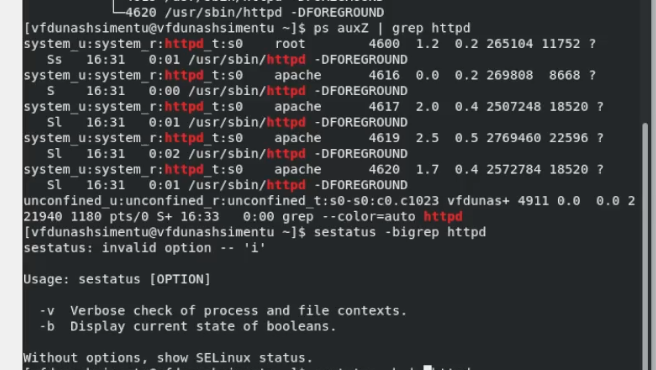
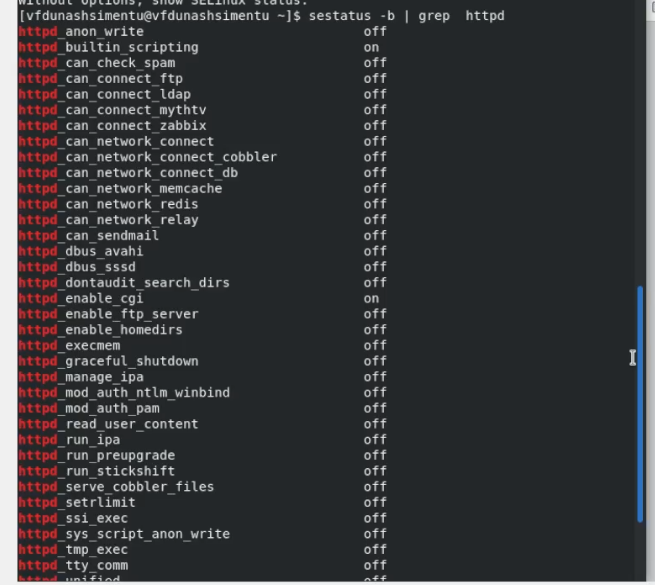
Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinx на практике совместно с веб-сервером Apache.

## 6.2. Порядок выполнения работы

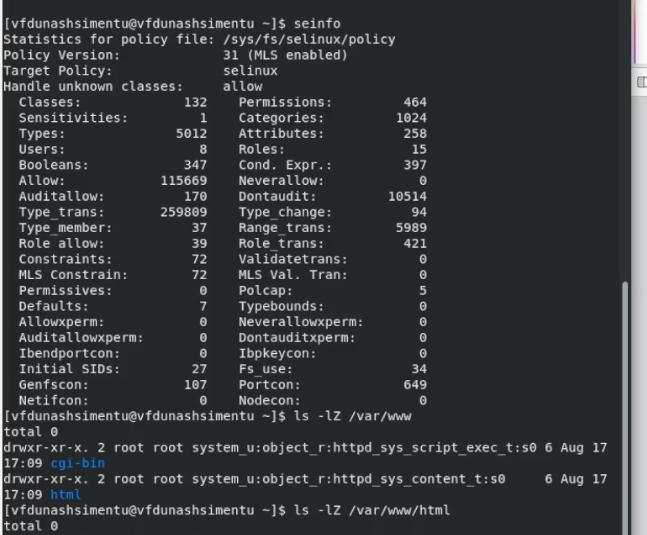
1. Вошел в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus.
2. Обратил с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: service httpd status или /etc/rc.d/init.d/httpd status Если не работает, запустите его так же, но с параметром start.

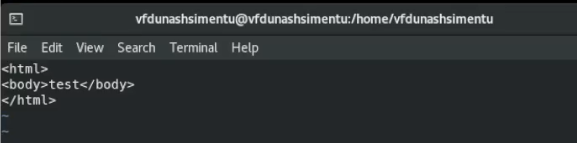
1. Нашёл веб-сервер Apache в списке процессов, определил его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду ps auxZ | grep httpd или ps -eZ | grep httpd.
2. Посмотрил текущее состояние переключателей SELinux для Apache с помощью команды sestatus -bigrep httpd Обратите внимание, что многие из них находятся в положении «off»

1. Посмотрите статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов.
2. Определите тип файлов и поддиректорий,находящихся в директории /var/www, с помощью команды ls -lZ /var/www
3. Определите тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html

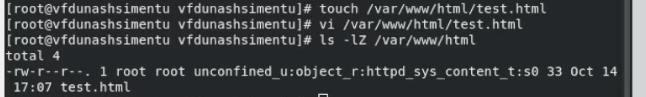
 рисунка 1.6

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



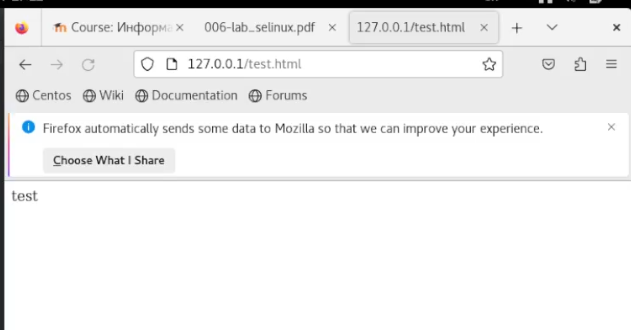
рисунка 1.7

1. Проверил контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html.



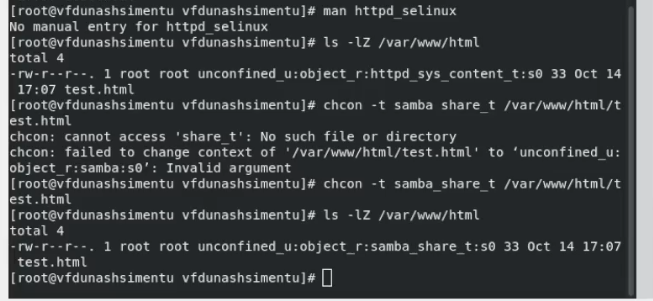
рисунка 1.8

1. Обратил к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедил, что файл был успешно отображён.

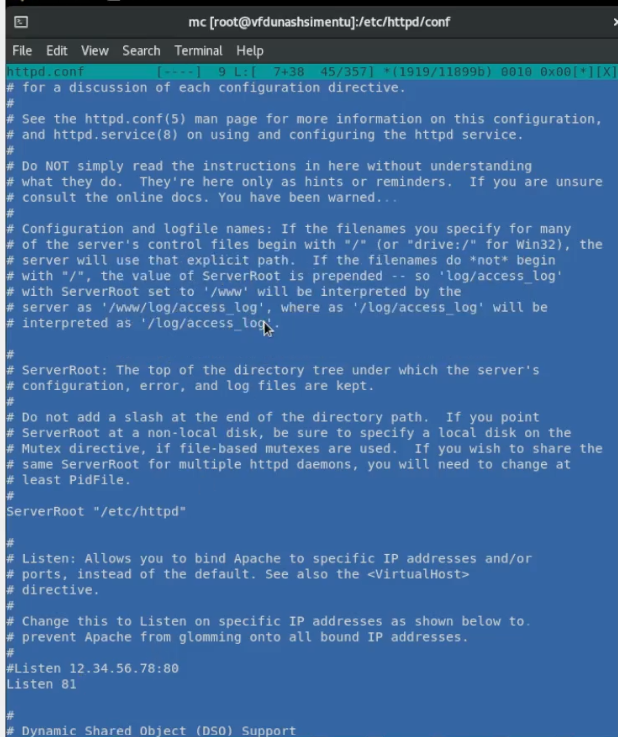


рисунка 1.9

1. Изучил справку man httpd\_selinux и выяснил, какие контексты файлов определены для httpd. Сопоставьте их с типом файла test.html. Проверил контекст файла можно командой ls -Z. ls -Z /var/www/html/test.html Рассмотрил 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.
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

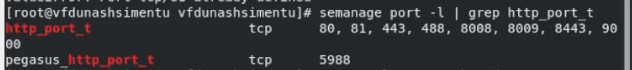
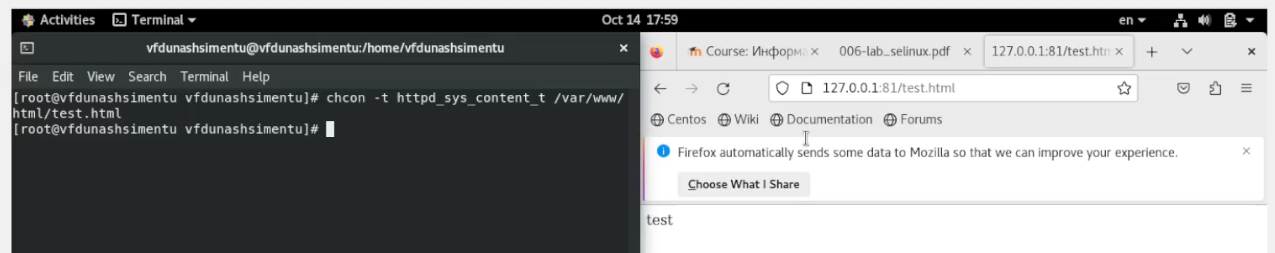
 14. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Я получил сообщение об ошибке: Forbidden You don’t have permission to access /test.html on this server.

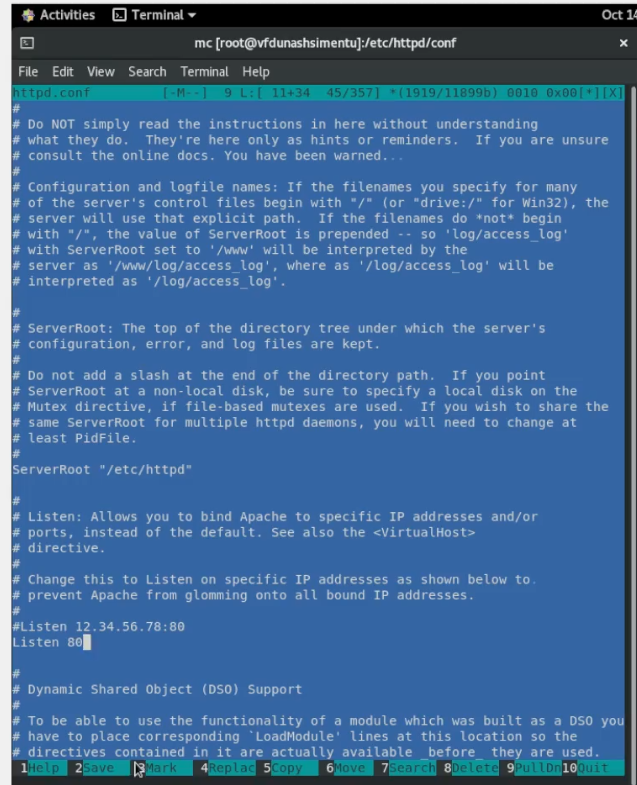
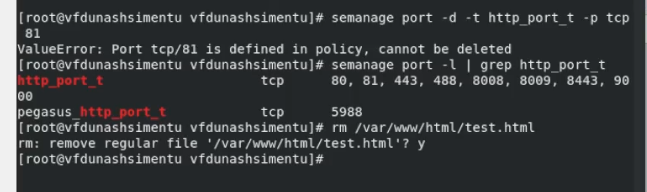
1. Попробувал запустить веб-сервер Apache на прослушивание ТСР-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf найдите строчку Listen 80 и замените её на Listen 81.



рисунка 1.11

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.

 18. Вернул контекст httpd\_sys\_cоntent\_\_t к файлу /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, введя в браузере адрес http://127.0.0.1:81/test.html. 

1. Исправил обратно конфигурационный файл apache, вернув Listen 80. 
2. Удалите привязку http\_port\_t к 81 порту: semanage port -d -t http\_port\_t -p tcp 81 и проверьте, что порт 81 удалён.
3. Удалите файл /var/www/html/test.html: rm /var/www/html/test.html 

## Выводы

SELinux предоставляет надежную и гибкую платформу для обеспечения соблюдения политик безопасности контроля доступа.