Отчет по лабораторной работе №6

Мандатное разграничение прав в Linux

Поленикова Анна Алексеевна

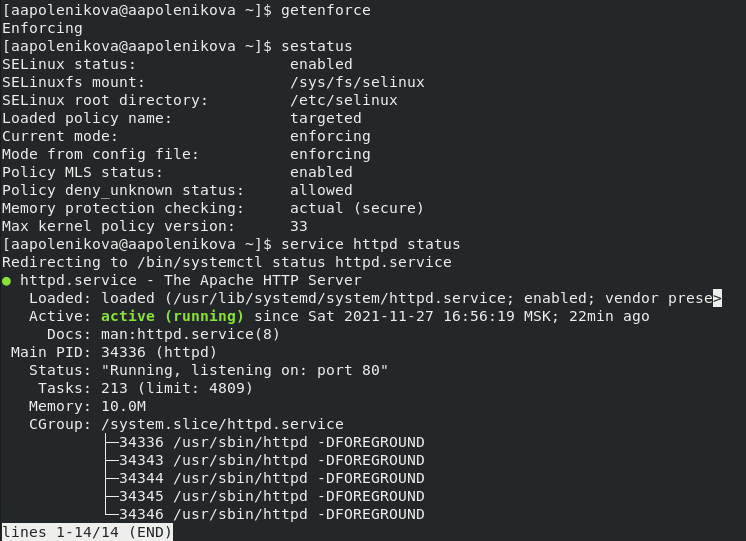
Содержание

# Цель работы

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

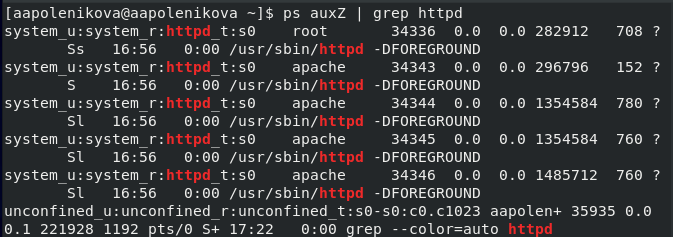
# Выполнение лабораторной работы

1. Вошла в систему и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus. Обратилась к веб-серверу, запущенному на компьютере, и убедилась, что последний работает с помощью команды service httpd status.



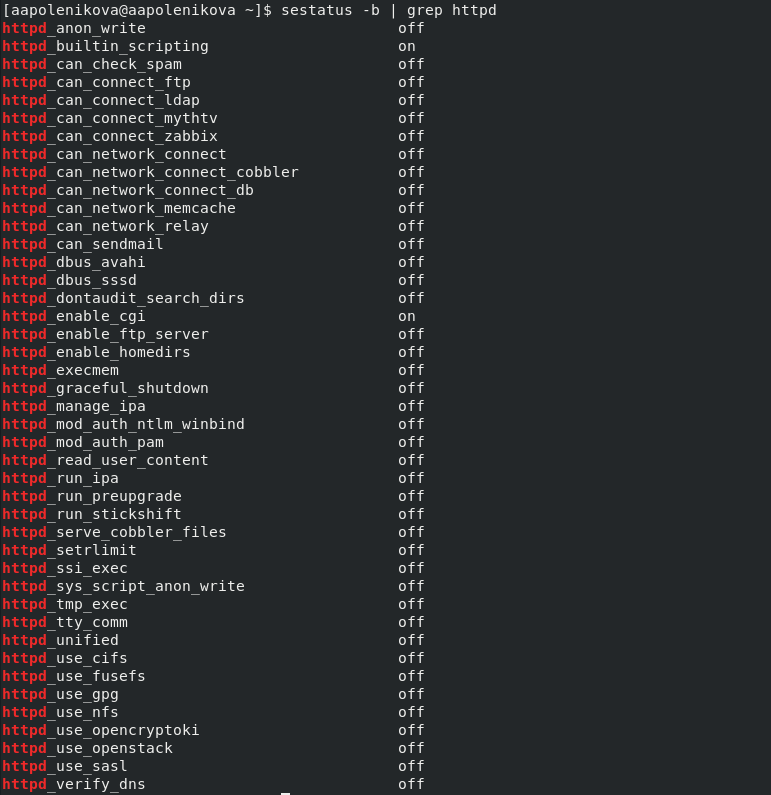
Проверка работы SELinux и веб-сервера

1. Нашла веб-сервер Apache в списке процессов и определила его контекст безопасности, использовав команду ps auxZ | grep httpd.



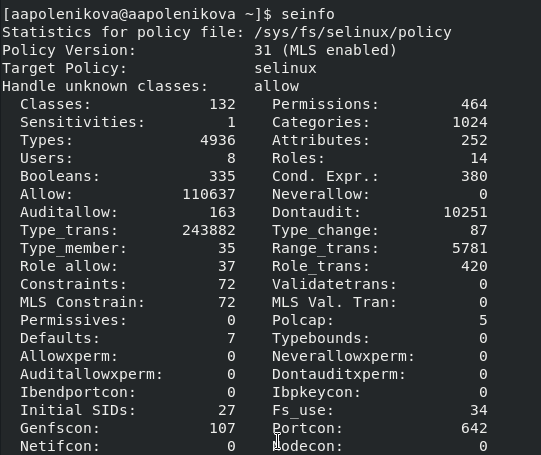
Веб-сервер Apache в списке процессов

1. Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды sestatus -b | grep httpd. Многие из них находятся в положении «off».



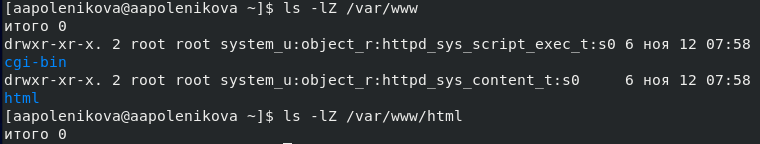
Состояние переключателей SELinux для Apache

1. Посмотрела статистику по политике с помощью команды seinfo и определила множество пользователей, ролей, типов.



Статистика

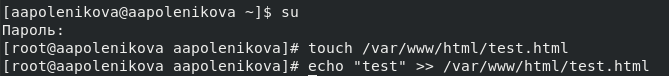
1. Определила тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www. Определила тип файлов, находящихся в директории /var/www/html с помощью команды ls -lZ /var/www/html. Создание файлов в директории /var/www/html разрешено только root пользователю.



Тип файлов и поддиректорий в директориях /var/www и /var/www/html

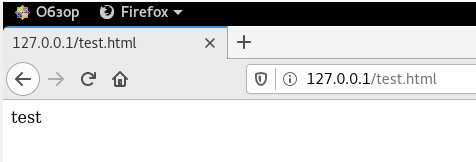
1. Создала от имени суперпользователя html-файл /var/www/html/test.html следующего содержания:

* test



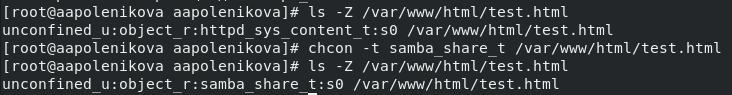
Создание html-файла /var/www/html/test.html

1. Обратилась к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Файл был успешно отображён.



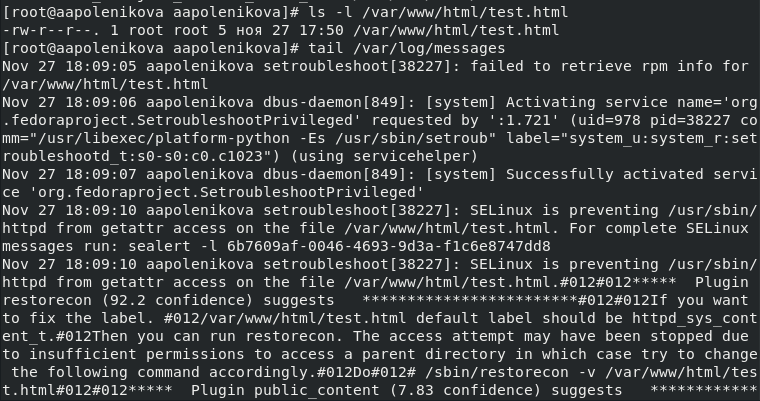
Обращение к файлу test.html через веб-сервер

1. Изучила справку man httpd\_selinux и выяснила, какие контексты файлов определены для httpd. Проверила контекст файла ls -Z /var/www/html/test.html. При выполнении команды был получен контекст httpd\_sys\_content\_t, который позволяет процессу httpd получить доступ к файлу. Изменила контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на samba\_share\_t с помощью команды chcon -t samba\_share\_t /var/www/html/test.html и проверила, что контекст поменялся с помощью команды ls -Z /var/www/html/test.html.



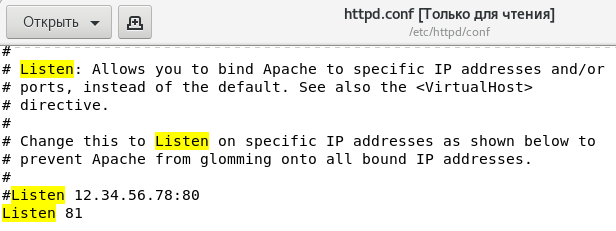
Контекст файла test.html

1. Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. При выполнении команды получила сообщение об ошибке: Forbidden You don’t have permission to access /test.html on this server.
2. Просмотрела log-файлы веб-сервера Apache с помощью команды ls -l /var/www/html/test.html. Также просмотрела системный лог-файл командой tail /var/log/messages.



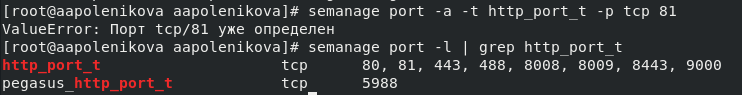
log-файлы веб-сервера Apache и системный log-файл

1. Попробовала 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 нашла строчку Listen 80 и заменила её на Listen 81.



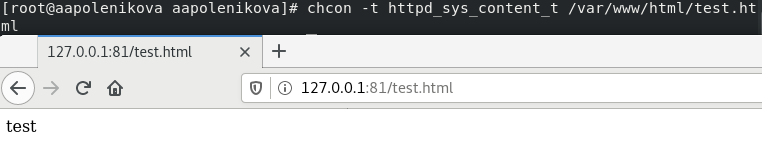
Запуск веб-сервера Apache на прослушивание ТСР-порта 81

1. Выполнила перезапуск веб-сервера Apache, при этом сбоя не произошло, поскольку порт 81 уже был определен.
2. Проанализировала лог-файлы с помощью команды tail -nl /var/log/messages. Просмотрела файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log.
3. Выполнила команду semanage port -a -t http\_port\_t -р tcp 81. После этого проверила список портов командой semanage port -l | grep http\_port\_t. Порт 81 в списке.



Вывод списка портов

1. Вернула контекст httpd\_sys\_cоntent\_t к файлу /var/www/html/test.html командой chcon -t httpd\_sys\_content\_t /var/www/html/test.html. После этого попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html.



Возвращение контекста httpd\_sys\_cоntent\_t файлу test.html

1. Исправила обратно конфигурационный файл apache, вернув Listen 80.
2. Удалила привязку http\_port\_t к 81 порту командой semanage port -d -t http\_port\_t -p tcp 81.
3. Удалила файл /var/www/html/test.html командой rm /var/www/html/test.html.

# Вывод

В ходе выполнения лабораторной работы были развиты навыки администрирования ОС Linux, получено первое практическое знакомство с технологией SELinux, а также была проверена работа SELinux на практике совместно с веб-сервером Apache.