Лабораторная работа №6

Дисциплина: Информационная безопасность

Манаева Варвара Евгеньевна

Содержание

# 1 Техническое оснащение:

* Персональный компьютер с операционной системой Windows 10;
* Планшет для записи видеосопровождения и голосовых комментариев;
* Microsoft Teams, использующийся для записи скринкаста лабораторной работы;
* Приложение Pycharm для редактирования файлов формата *md*;
* *pandoc* для конвертации файлов отчётов и презентаций.

# 2 Цели и задачи работы

## 2.1 Цель

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

## 2.2 Задачи

1. Подготовить лабораторный стенд;
2. Запустить Apache в системе;
3. Создать небольшой веб-сервер;
4. Посмотреть различные варианты настроек сервера и изучить реакции на изменение этих настроек.

# 3 Теоретическое введение и подготовка лабораторного стенда

HTTP-сервер Apache — самый широко используемый веб-сервер в мире. Он имеет множество мощных функций, включая динамически загружаемые модули, надежную поддержку различных медиаформатов и интеграцию с другим популярным программным обеспечением.

Apache доступен в используемых по умолчанию репозиториях программного обеспечения CentOS, т. е. вы можете установить его с помощью менеджера пакетов yum.

Порядок настройки машины для использования Apache:

sudo yum update httpd  
sudo yum install httpd  
sudo yum install firewalld  
sudo systemctl start firewalld  
sudo firewall-cmd --permanent --add-service=ssh  
sudo firewall-cmd --permanent --add-service=http  
sudo firewall-cmd --permanent --add-service=https  
sudo firewall-cmd --reload  
sudo systemctl enable firewalld

В файле /etc/httpd/httpd.conf необходимо задать:

ServerName test.ru

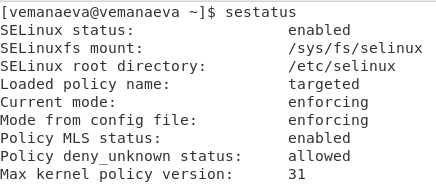
Также необходимо проследить, чтобы пакетный фильтр был отключён. Отключить фильтр можно командами:

sudo iptables -F  
sudo iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT

# 4 Выполнение лабораторной работы [1]

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

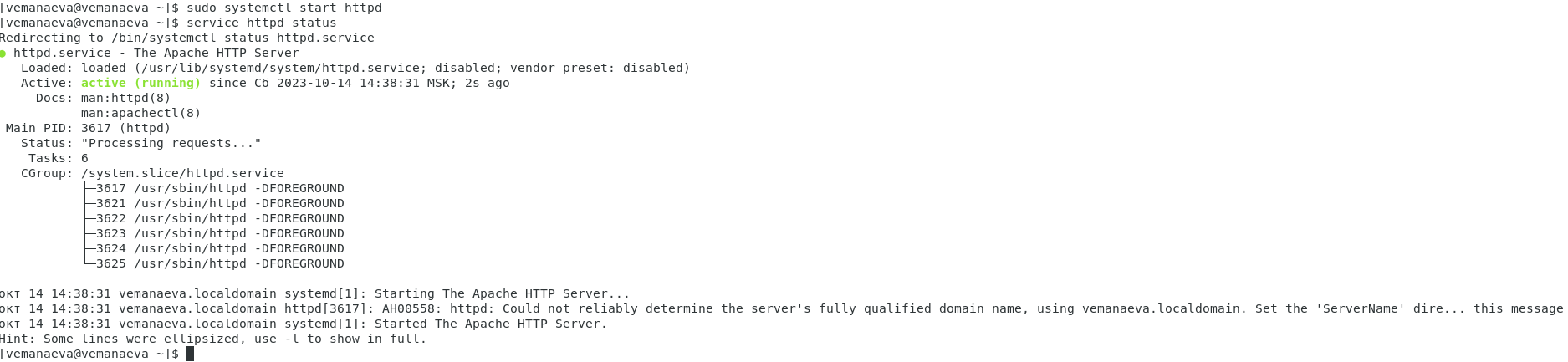
sestatus



Проверим SELinux

1. Обратимся с помощью браузера к веб-серверу, запущенному на компьютере, и убедимся, что последний работает (??)

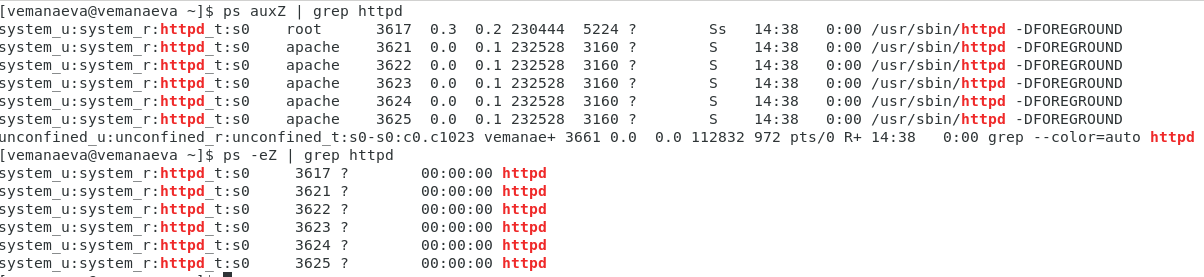
sudo systemctl start httpd  
service httpd status



Проверяем

1. Найдём веб-сервер Apache в списке процессов и определим его контекст безопасности (??)

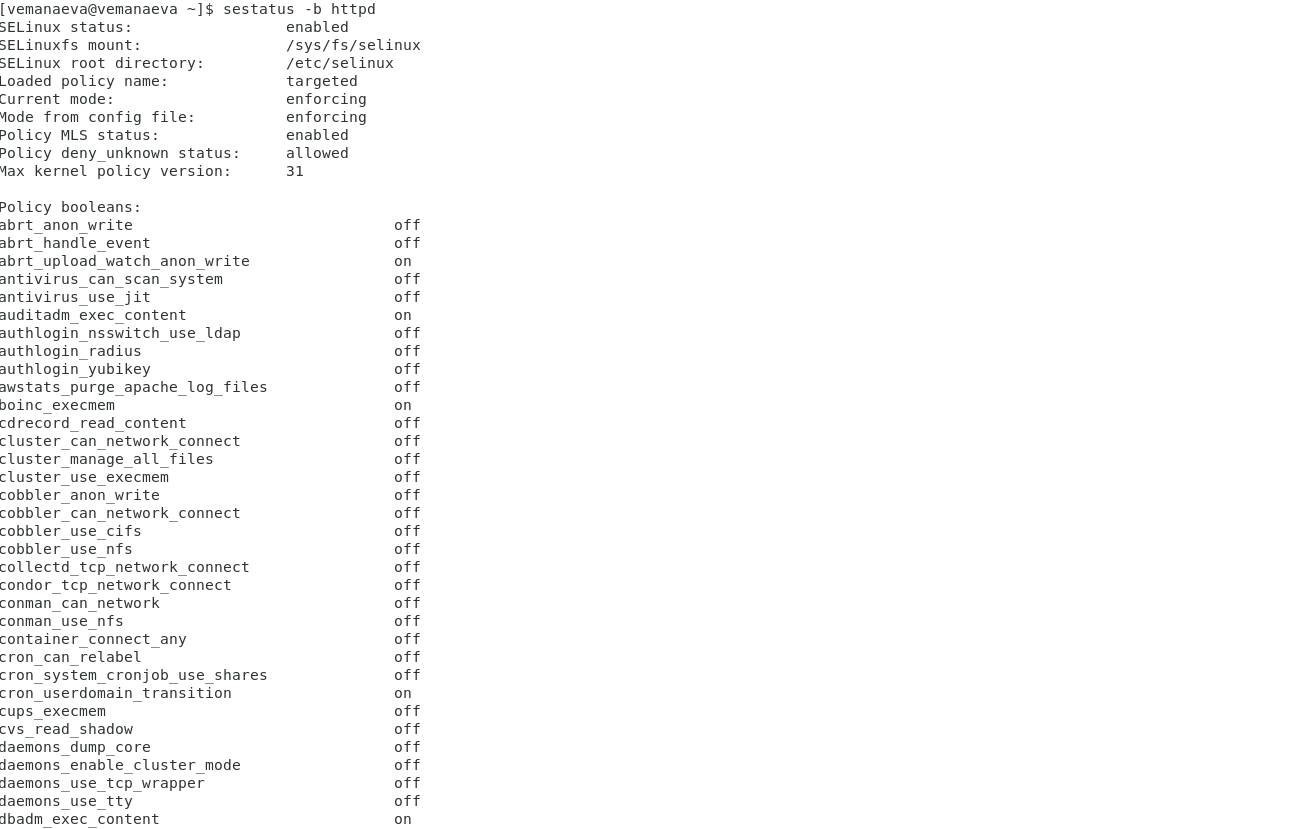
ps auxZ | grep httpd  
ps -eZ | grep httpd



Контекст безопасности

1. Посмотрим текущее состояние переключателей SELinux для Apache (??)

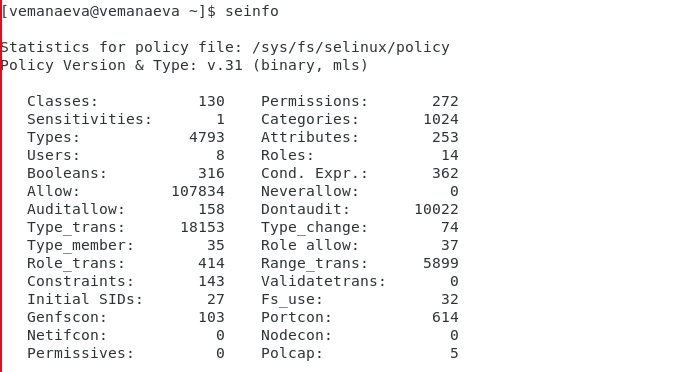
sestatus -bigrep httpd



Текущее состояние переключателей SELinux для Apache

1. Посмотрим статистику по политике, а также определим множество пользователей, ролей и типов (??)

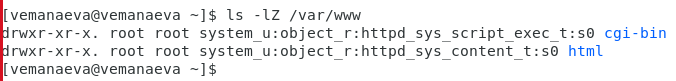
seinfo



Статистика по политике

1. Определим тип файлов и поддиректорий, находящихся в директории /var/www (??)

ls -lZ /var/www



Типы поддиректорий и файлов в директории /var/www

1. Определим тип файлов, находящихся в директории /var/www/html (??)

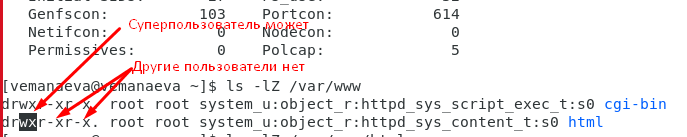
ls -lZ /var/www/html

Тип файлов в директории /var/www/html

Тип файлов в директории /var/www/html

1. Определим круг пользователей, которым разрешено создание файлов в директории /var/www/html (только суперпользователь) (??)

ls -l /var/www



Определим права на файл

1. Создадим от имени суперпользователя html-файл /var/www/html/test.html (??)

sudo nano /var/www/html/test.html

<html>  
<body>test</body>  
</hmtl>



Создадим файл

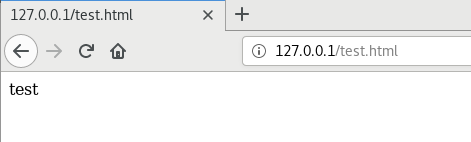
1. Проверим контекст созданного файла. (??)

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

Определим контекст

Определим контекст

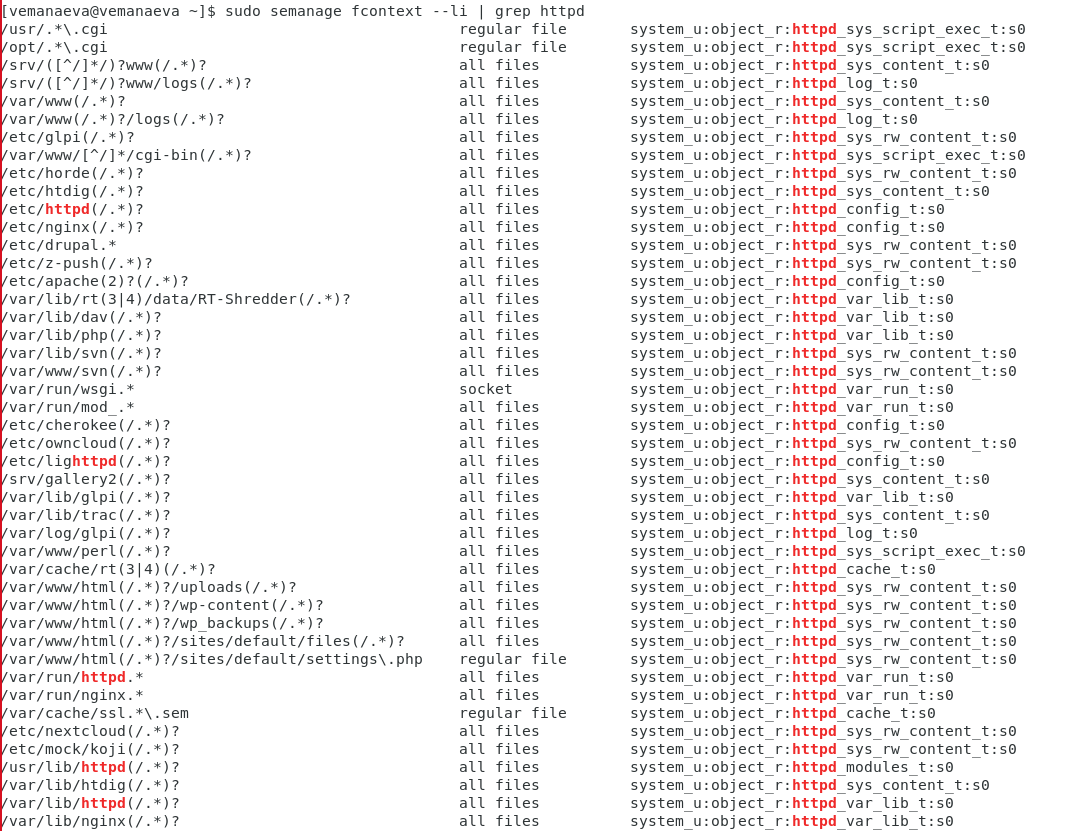
1. Обратимся к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html”. Убедимся, что файл был успешно отображён. (??)



http://127.0.0.1/test.html

1. Изучим справку и выясните, какие контексты файлов определены для httpd. Сопоставим их с типом файла test.html, проверив контекст файла (??)

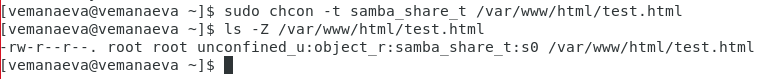
man httpd\_selinux  
ls -Z /var/www/html/test.html



Контексты файлов, определённые для SELinux

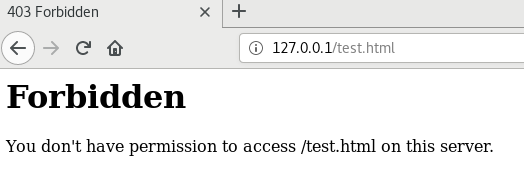
1. Измените контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на любой другой, к которому процесс httpd не должен иметь доступа (??)

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



Изменяем контекст файла

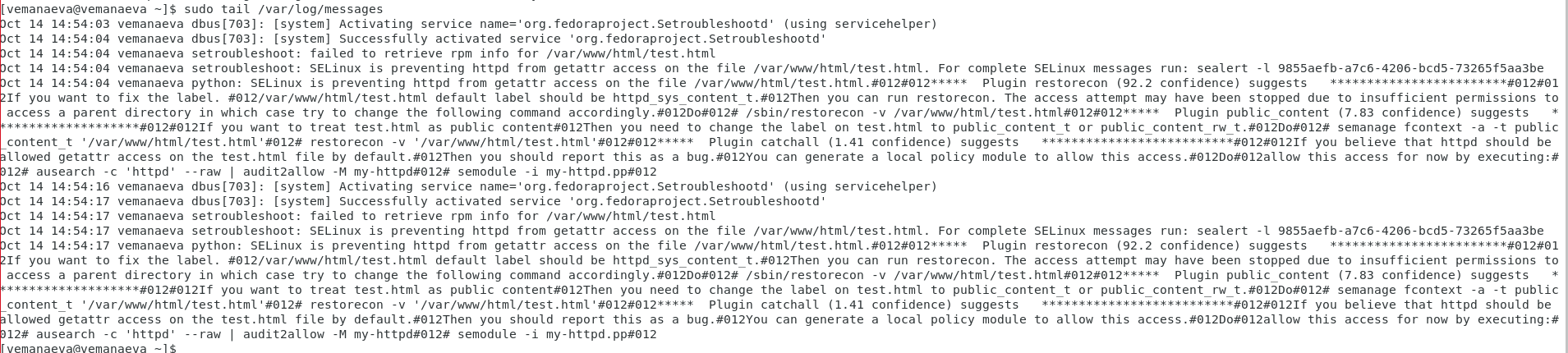
1. Попробуем ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html”. И получаем сообщение об ошибке Forbidden. (??)



http://127.0.0.1/test.html

1. Проанализируем ситуацию. Просмотрим log-файлы веб-сервера Apache. (??)

ls -l /var/www/html/test.html  
tail /var/log/messages



log-файлы

1. Запустим 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 (??)

nano /etc/httpd/httpd.conf



Замена строки

1. Выполним перезапуск веб-сервера Apache (??)

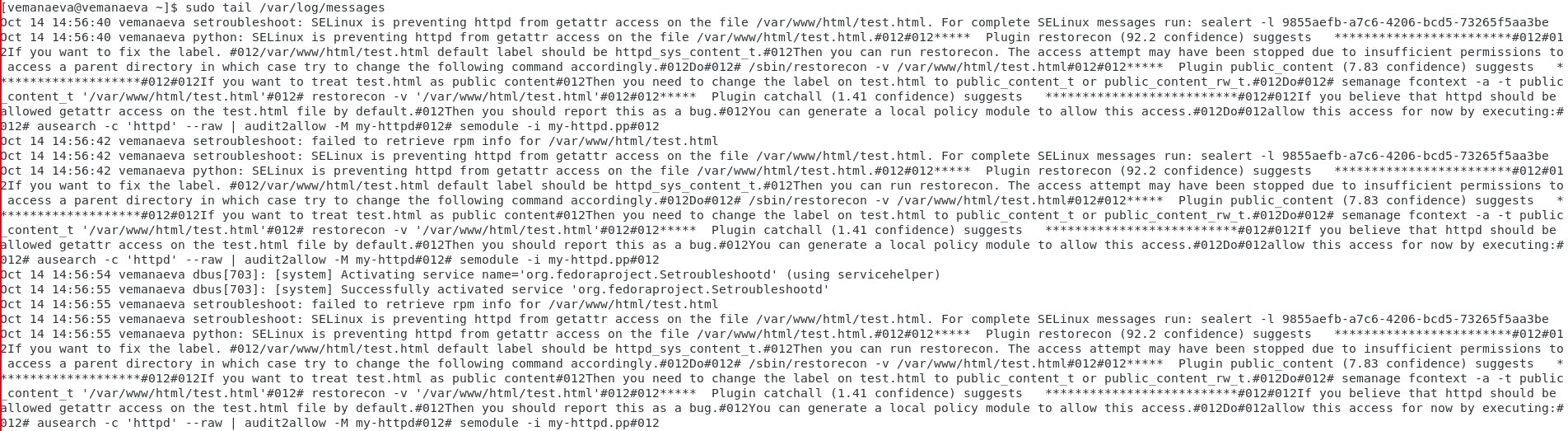
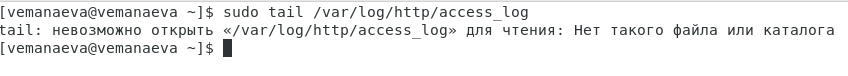
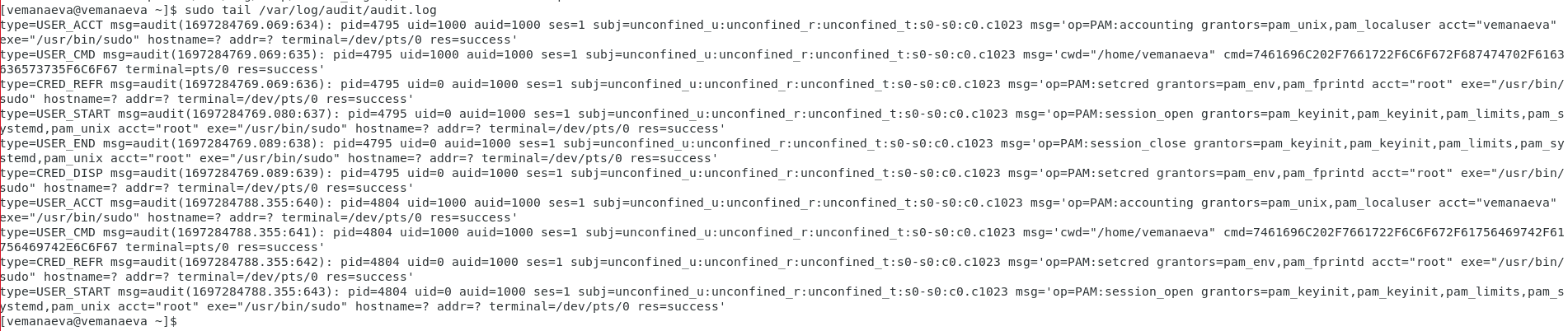
sudo systemctl start httpd

Перезапуск веб-сервера

Перезапуск веб-сервера

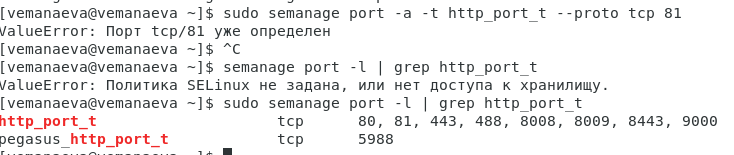
1. Проанализируем лог-файлы /var/log/messages. Также просмотрим файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log и выясним, в каких файлах появились записи (??)

tail /var/log/messages  
tail /var/log/http/error\_log  
tail /var/log/http/access\_log  
tail /var/log/audit/audit.log

1. Выполним команду semanage port -a -t http\_port\_t -р tcp 81. После этого проверим список портов. Убедимся, что порт 81 появился в списке. (??)

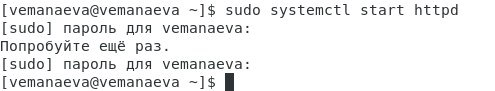
sudo semanage port -a -t http\_port\_t --proto tcp 81  
semanage port -l | grep http\_port\_t



Список портов

1. Пробуем запустить веб-сервер Apache ещё раз. И он работает. (??)

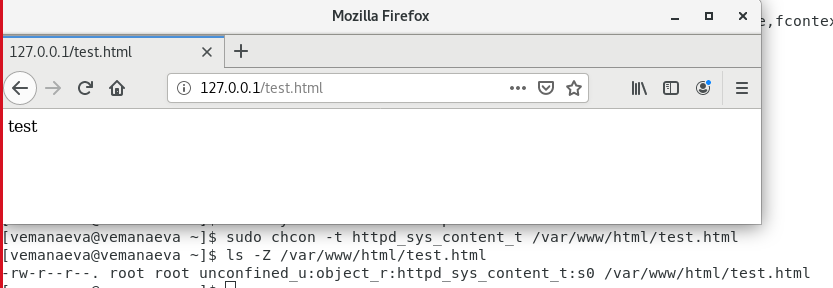
sudo systemctl start httpd



Веб-сервер работает

1. Вернём контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/test.html. После этого попробуем получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. (??)

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



http://127.0.0.1:81/test.html

1. Исправим обратно конфигурационный файл apache, вернув Listen 80. (??)

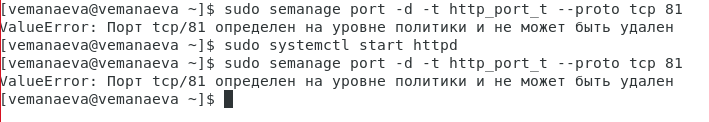
nano /etc/httpd/httpd.conf



Исправляем конфигурационный файл

1. Удалим привязку http\_port\_t к 81 порту и проверим, что порт 81 удалён.(??)

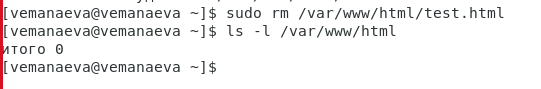
semanage port -d -t http\_port\_t -p tcp 81



Удаляем привязку

1. Удалим файл /var/www/html/test.html командой (??)

rm /var/www/html/test.html



Удаляем файл

# 5 Выводы по проделанной работе

## 5.1 Вывод

В результате выполнения работы мы развили навыки администрирования ОС Linux, получили первое практическое знакомство с технологией SELinux и проверили работу SELinx на практике совместно с веб-сервером Apache.

Были записаны скринкасты выполнения и защиты лабораторной работы.

Ссылки на скринкасты:

* [Выполнение, Youtube](https://youtu.be/glRNW5eHxy4)
* [Выполнение, Rutube](https://rutube.ru/video/2ad492d2a864812e943cd7cc99cba76b/)
* [Защита презентации, Youtube](https://youtu.be/hAC2qCEJLxE)
* [Защита презентации, Rutube](https://rutube.ru/video/23a39ff1f64eee6a60e286136a3e8d00/)

# 6 Список литературы

1. Лабораторная работа № 6 [Электронный ресурс]. Российский Университет Дружбы Народов имени Патрису Лумумбы, 2023. URL: <https://esystem.rudn.ru/mod/resource/view.php?id=1031379>.