Отчет по лабораторной работе № 6. Мандатное разграничение прав в Linux

дисциплина: Информационная безопасность

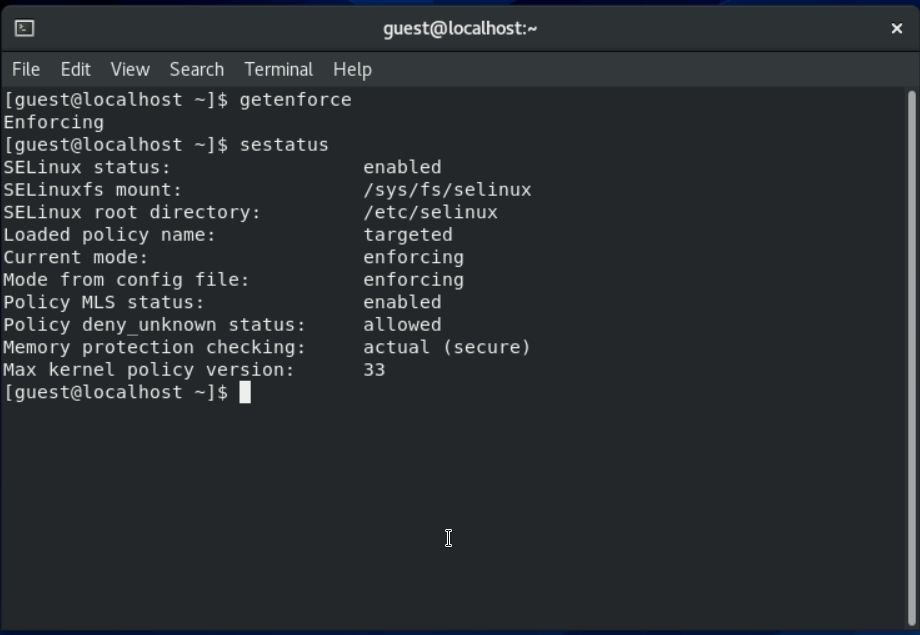
Смирнова Мария Александровна

# Цель работы

Развитие навыков администрирования ОС Linux. Практическое освоение технологии SELinux. Проверка работы SELinux совместно с веб-сервером Apache.

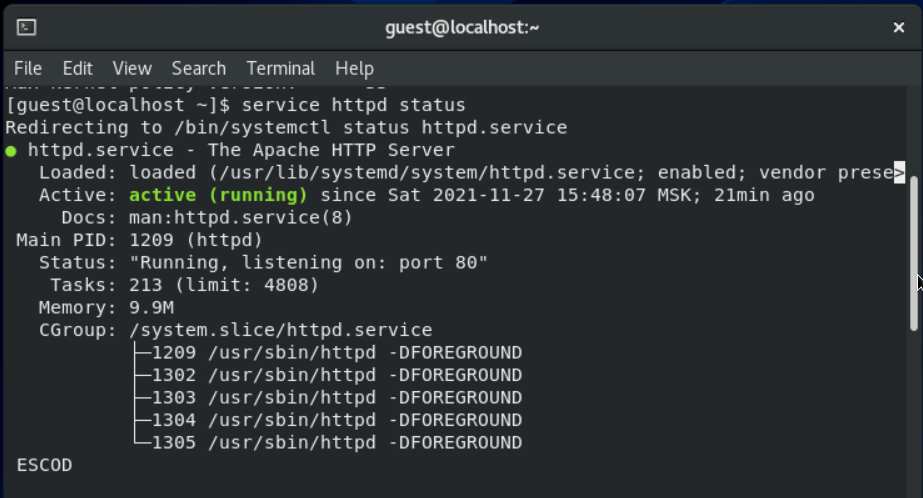
# Выполнение лабораторной работы

1. От имени пользователя guest войдем в систему. Проверим, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus (рис. -@fig:001).



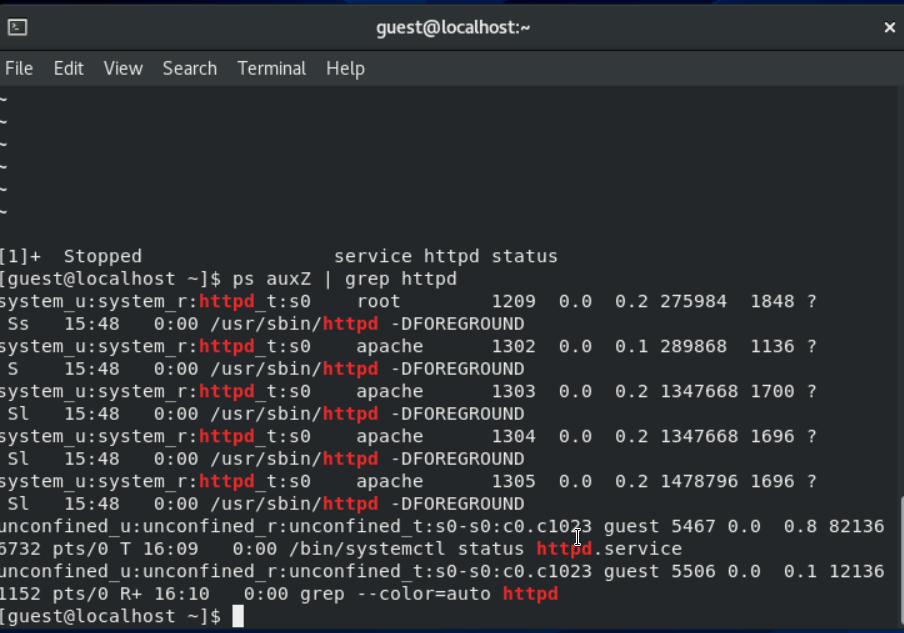
Проверка SELinux

1. Обратимся к веб-серверу, запущенному на нашем устройстве и проверим, что он работает (рис. -@fig:002).



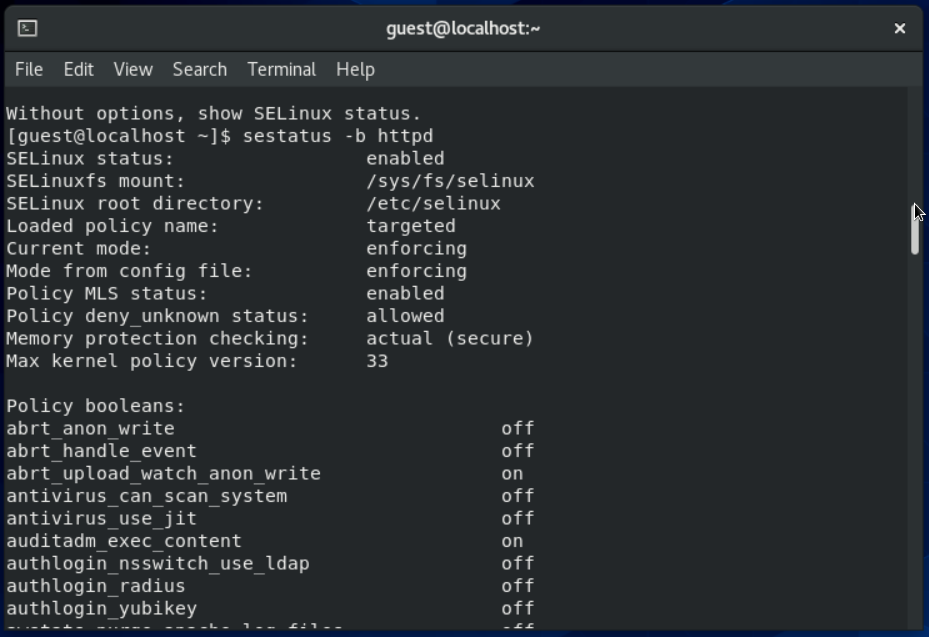
Httpd status

1. Посмотрим командой ps auxZ | grep httpd список процессов и найдем в нем Apache. Посмотрим на его контекст безопасности: httpd (рис. -@fig:003).



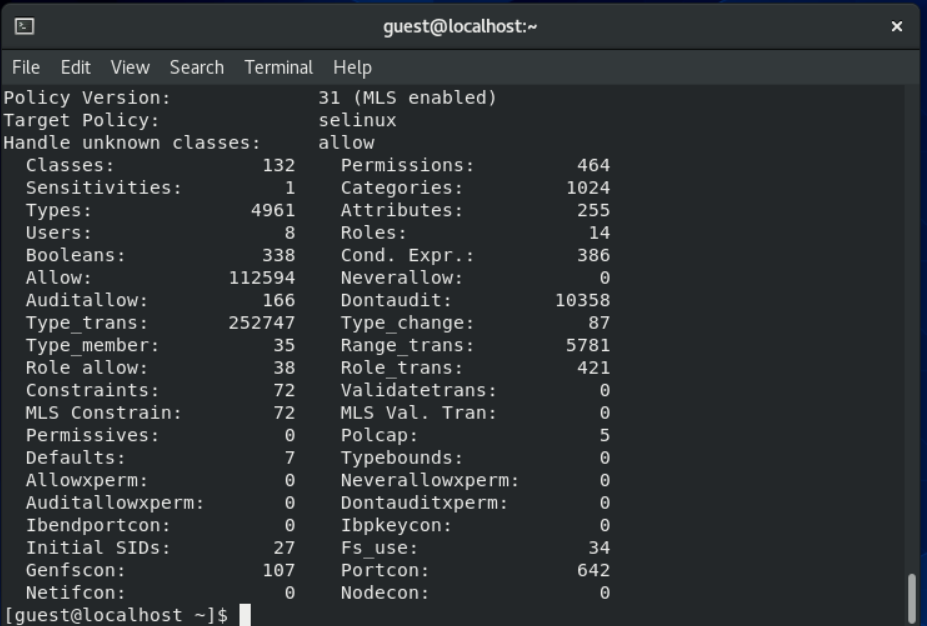
Контекст безопасности Apache

1. Посмотрим на текущее состояние переключателей, большинство из них находятся в положении off (рис. -@fig:004).



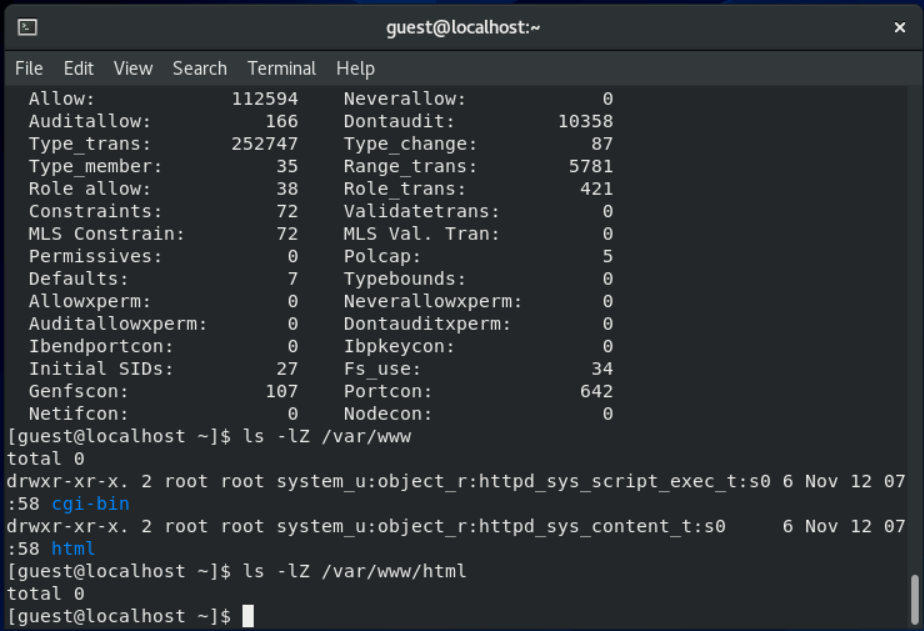
Переключатели

1. Посмотрим статистику по политике с помощью команды seinfo. У нас есть 8 пользователей, 38 ролей и 35 типов (рис. -@fig:005).



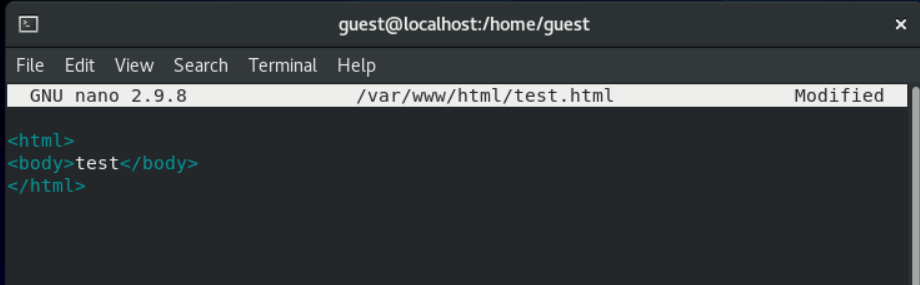
Seinfo

1. Определим тип файлов в директории /var/www и /var/www/html. Круг пользователей, которым разрешено создание файлов в последней директории - root (рис. -@fig:006)



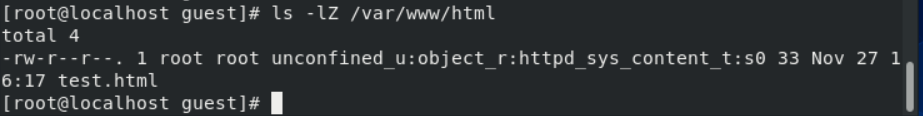
Директория /var/www/html

1. Создадим от имени суперпользователя html-файл с содержанием из задания (рис. -@fig:007)



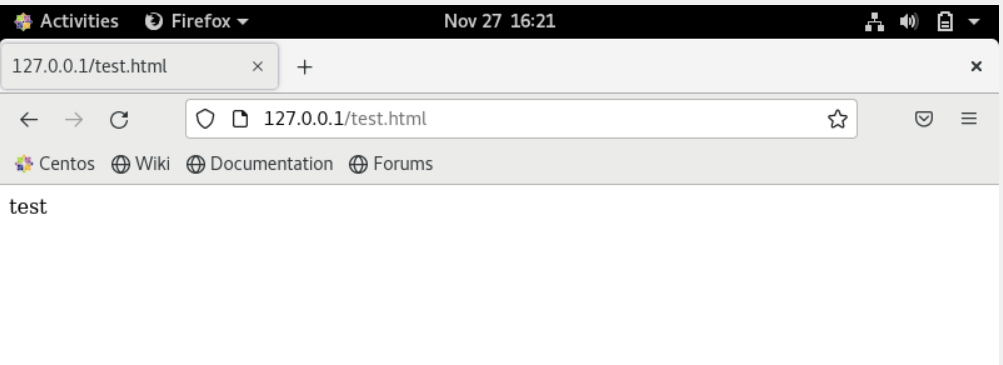
test.html

1. Проверим контекст созданного файла - httpd\_sys\_content\_t. Это контекст по умолчанию (рис. -@fig:008)



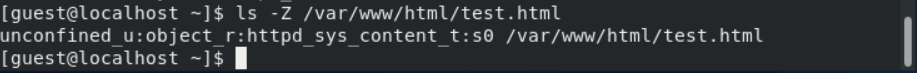
Контекст test.html

1. Обратимся к созданному файлу через веб-сервер, введя в браузере http://127.0.0.1/test.html. Увидим, что файл успешно отображен (рис. -@fig:009).



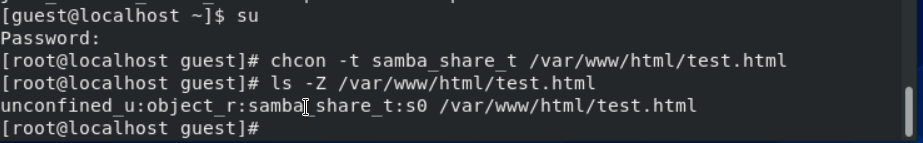
http://127.0.0.1/test.html

1. Выясним, какие контексты файлов определены для httpd и сопоставим их с контекстом нашего файла test (рис. -@fig:010)



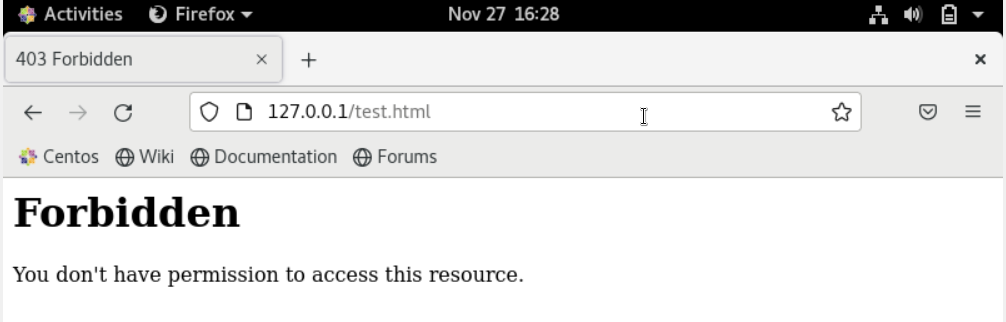
Контексты файлов httpd

1. Изменим контекст файла с httpd\_sys\_content\_t на samba\_share\_t (рис. -@fig:011)



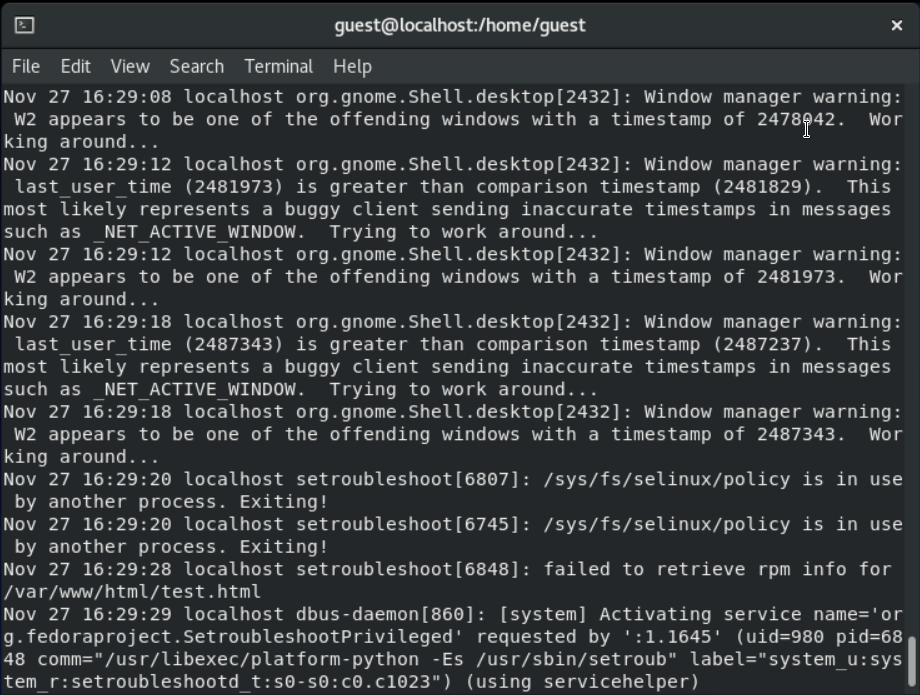
Изменение контекста test

1. Попробуем еще раз получить доступ к файлу через браузер. Получим сообщение об ошибке. Файл не был отображен из-за неправильного контекста (который мы поменяли) (рис. -@fig:012)



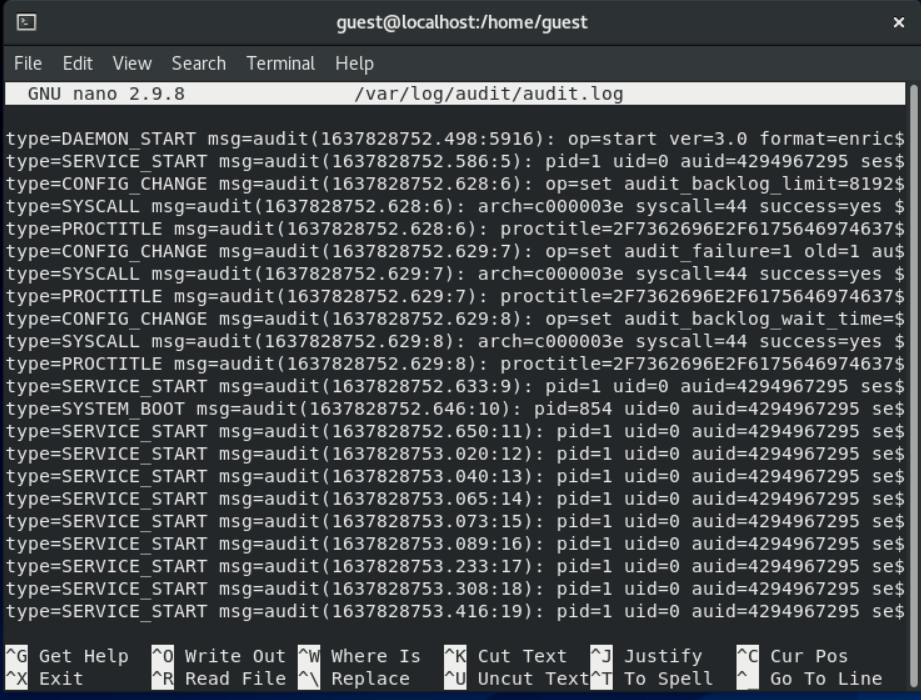
Сообщение об ошибке

1. Посмотрим log-файлы веб-сервера Apache и системный log-файл (рис. -@fig:013)



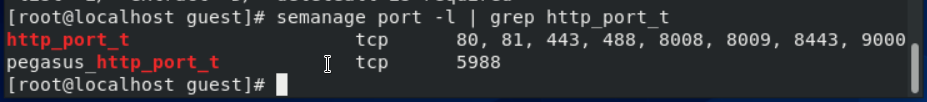
log-файл

1. Увидим ошибки, аналогичные указанным в файле audit.log (рис. -@fig:014)



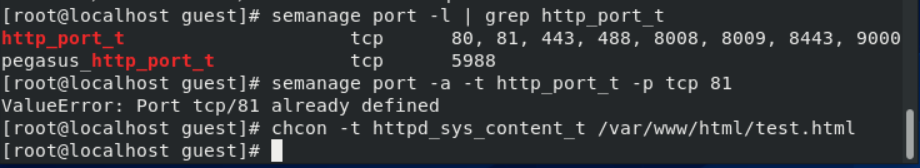
audit.log

1. В моем случае tcp port 81 уже есть по умолчанию в списке портов (рис. -@fig:015)



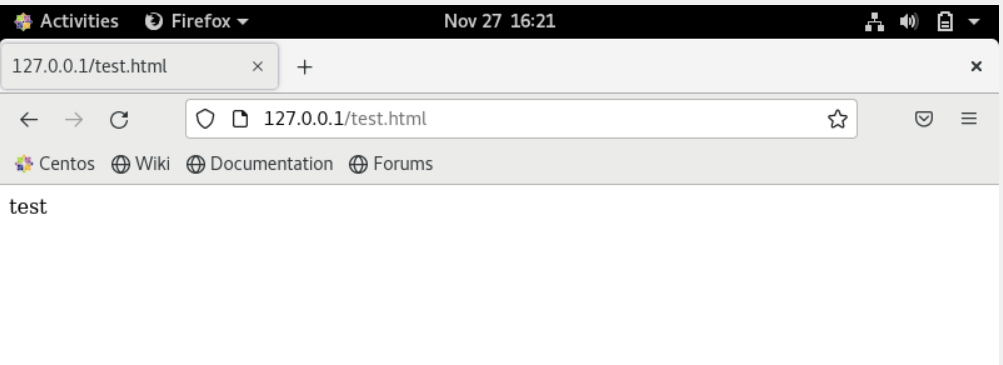
Порт 81

1. Мы также не можем его удалить. Заменим контекст обратно на корректный (рис. -@fig:016)



Контекст файла test

1. Наш файл через браузер снова открывается корректно. Удалим файл test.html (рис. -@fig:016)



Контекст файла test

# Выводы

В процессе выполнения лабораторной работы мы развили навыков администрирования ОС Linux, а также освоили технологии SELinux. Мы проверили работу SELinux совместно с веб-сервером Apache.