### **РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

### **Факультет физико-математических и естественных наук**

### **Кафедра прикладной информатики и теории вероятностей**

### **Отчет по лабораторной работе № 6**

### *Дисциплина: Информационная безопасность*

Студент: Логинов Сергей Андреевич

Группа: НФИбд-01-18

**МОСКВА 2021г**

### Цель работы

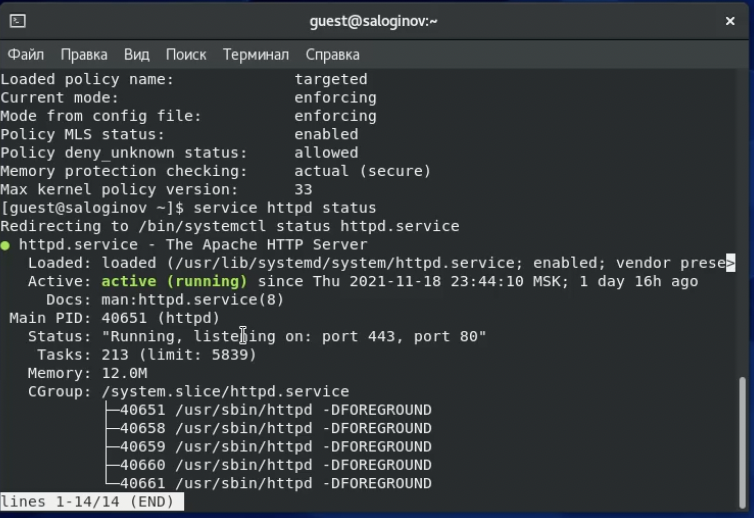
Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux.

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

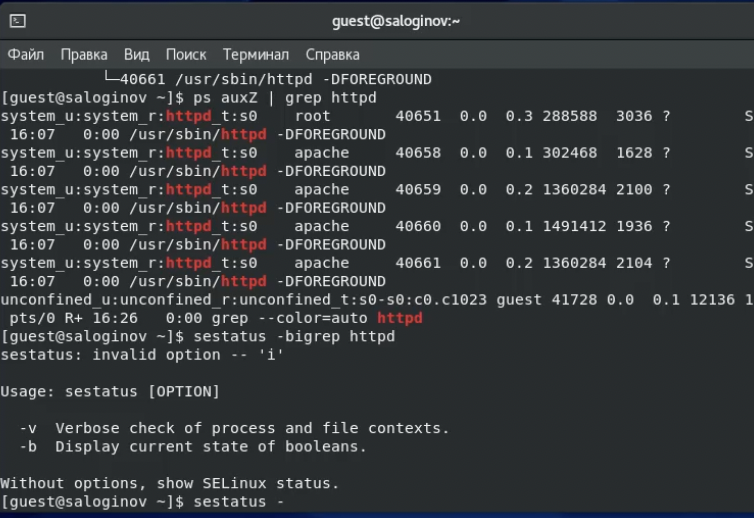
### Ход работы

Были выполнены подготовительные процедуры и установлены необходимые пакеты.

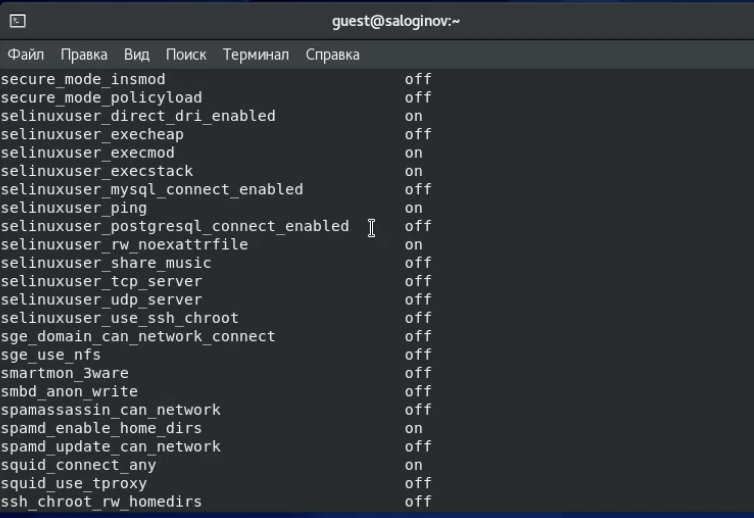
1. Убедились, что SELinux работает в режиме enforcing политики targeted
2. С помощью веб-браузера обратились к локальному веб-серверу и убедились. что он работает

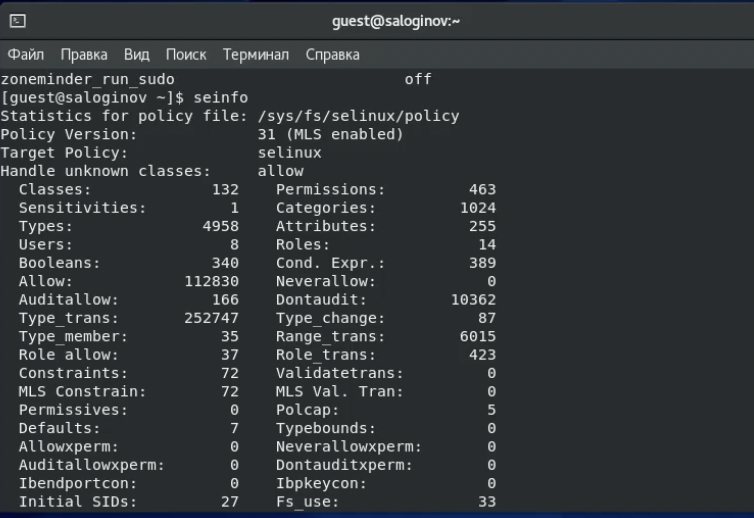
* 

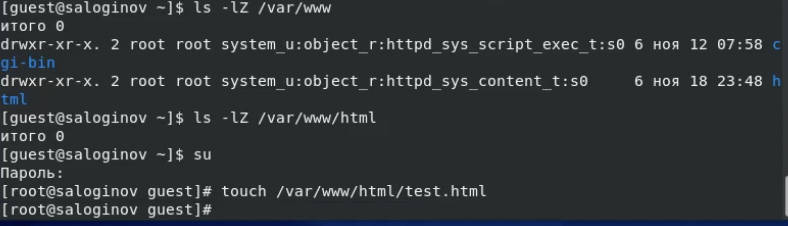
1. Нашли веб-сервер Apache в списке процессов, контекст безопасности:   
   system\_u:system\_r:httpd\_t:s0

* 

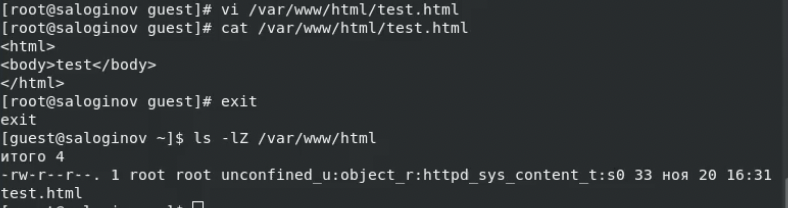
1. Проверили текущее состояние переключателей SELinux для Apache

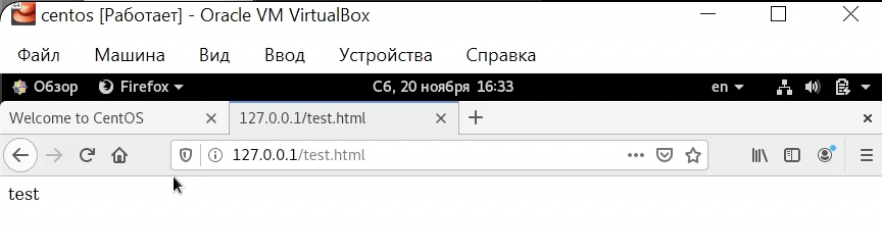
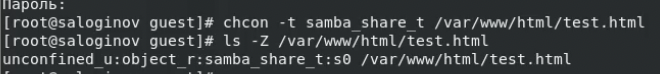
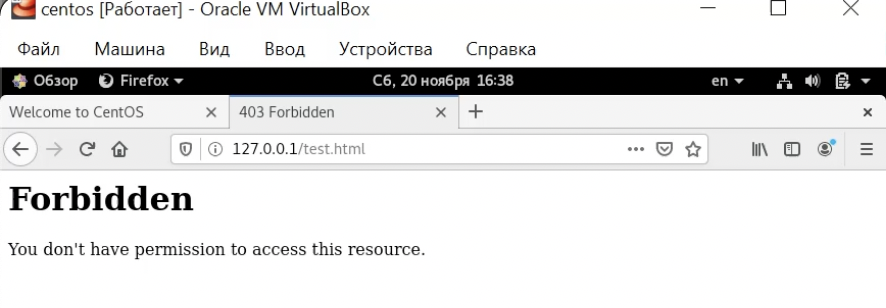
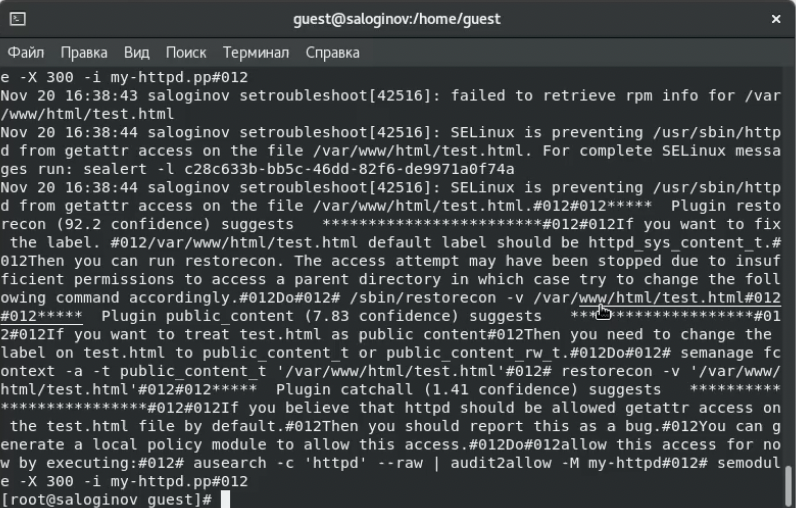
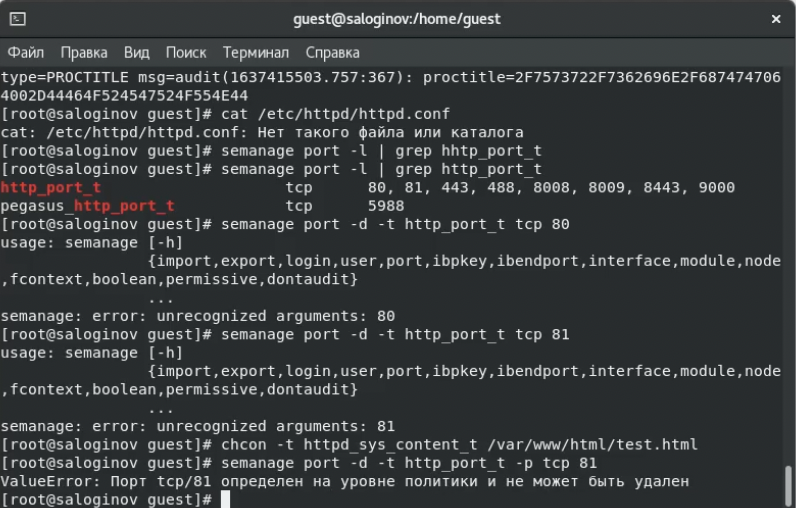
 Действительно, большая часть переключателей находится в положении off

1. Посмотрели статистику по политике. Множество пользователей: 8, ролей: 14, типов: 4958  
   
2. Определили тип файлов и поддиректорий, находящихся в директории /var/www
3. В директории /var/www/html отсутсвтуют какие-либо файлы
4. В данной директории файлы создавать может только владелец
5. От имени суперпользователя создали html-файл следующего содержания:

* <html>  
  <body>test</body>  
  </html>
* 

1. Проверили контекст созданного файла:

* unconfined\_u:object\_r:httpd\_sys\_content\_t:s0
* 

1. Обратились к файлу через веб-сервер  
   
2. Изучили справку SELinux
3. Изменили контекст файла с httpd\_sys\_content\_t на samba\_share\_t  
   
4. Снова попробовали обратиться к файлу через веб-сервер, получили отказ  
   
5. Несмотря на то, что права доступа дают возможность читать файл любому пользователю, обратиться к нему через браузер не получилось, поскольку на файл был установлен другой контекст. Тип samba\_share\_t не позволяет процессу httpd получить доступ к файлу при обращении через браузер  
   Логи:  
   
6. При попытке запустить веб-сервер на прослушивание TCP-порта 81 было выявлено, что 81 порт уже присутствует в списке стандартных портов, которые невозможно удалить. Следовательно, пункты 16-20 не выполнены
7. Вернули контекст нашему файлу и через браузер получили доступ к нему
8. Файл отсутствует
9. Невозможно удалить  
   
10. Удалили файл test.html

### Вывод

В ходе лабораторной работы были получены первые практические навыки работы с SELinux