РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ПРЕЗЕНТАЦИЯ ПО ЛАБОРАТОРНОЙ РАБОТЕ №6

дисциплина: Информационная безопасность

Преподователь: Кулябов Дмитрий Сергеевич

Студент: Поляков Арсений Андреевич

Группа: НФИбд-01-19

МОСКВА
2022 г.

Цель работы

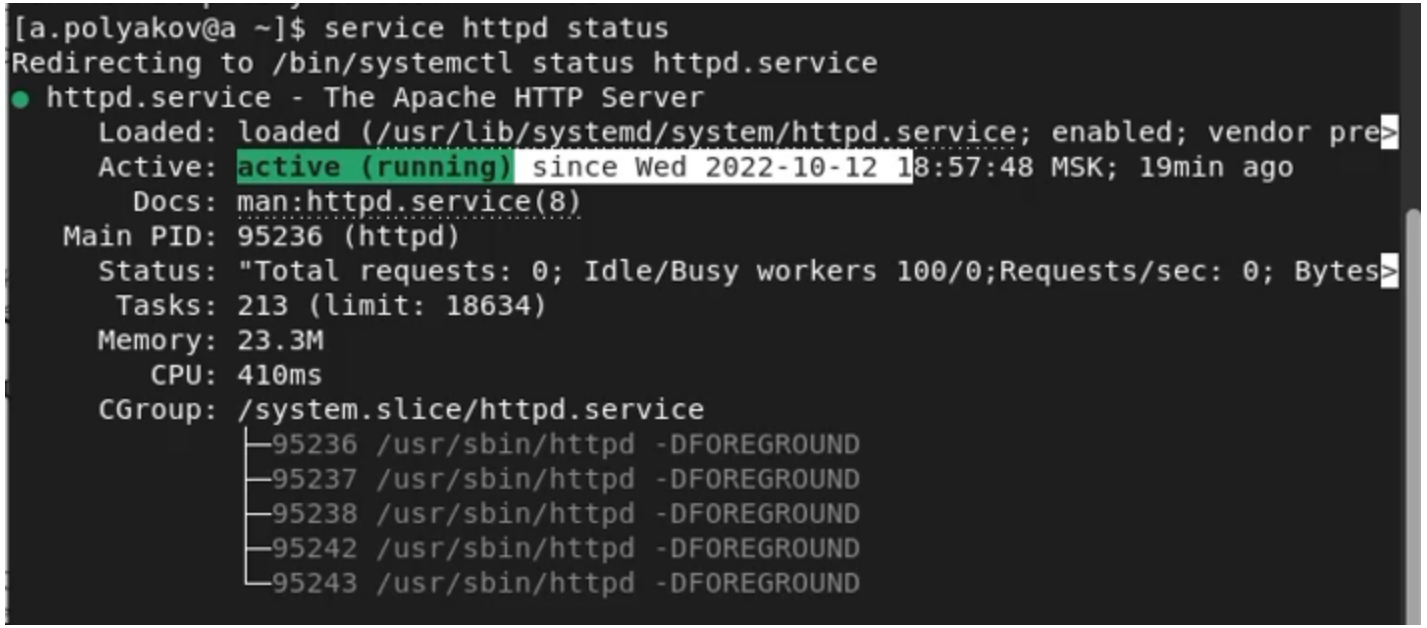
Целью данной лабораторной работы является развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinx на практике совместно с веб-сервером Apache.

Выполнение лабораторной работы

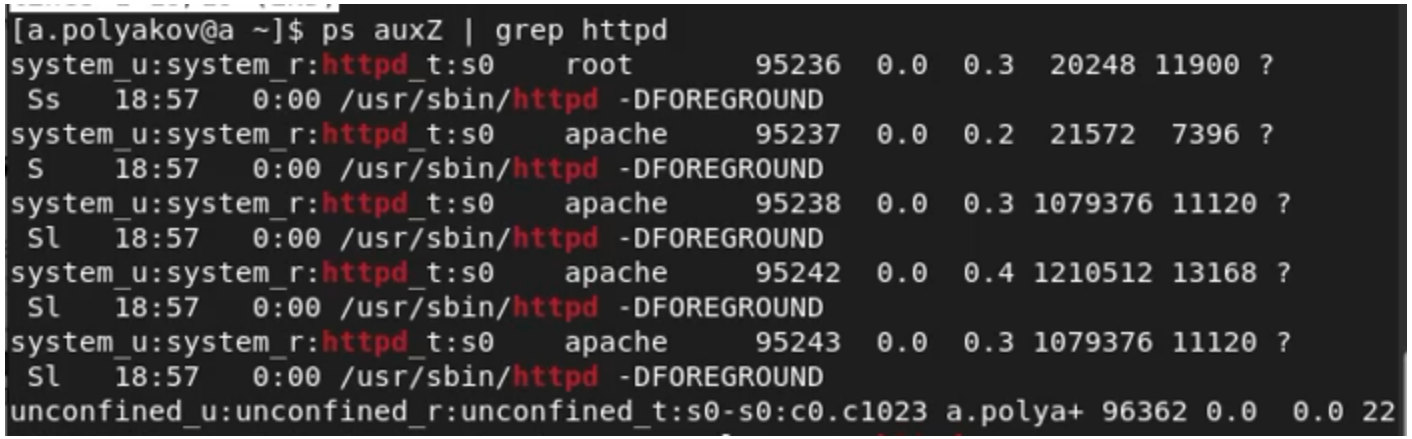
1. Входим в систему с полученными учётными данными. Проверили, что SELinux работает в режиме enforcing политики targeted с помощью команд **getenforce** и **sestatus**.

```
[a.polyakov@a ~]$ getenforce
Enforcing
[a.polyakov@a ~]$ sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
```

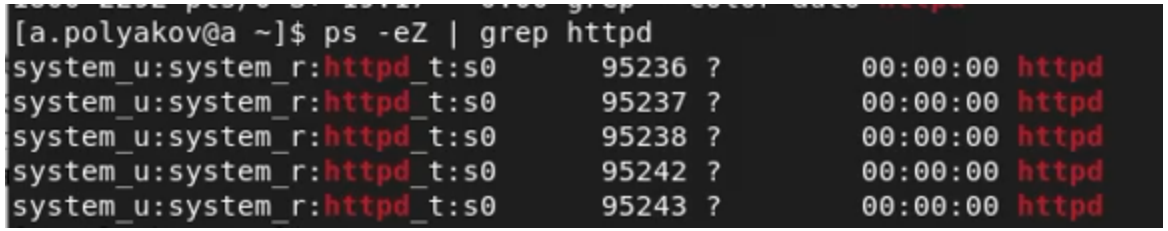
2. Запустили веб-сервер и обратились к нему с помощью команды: service httpd status



3. Найшли веб-сервер Apache в списке процессов с помощью команды **ps auxZ | grep httpd**. Контекст безопасности - unconfined_u:unconfined_r:unconfined_t.



4. Посмотрели текущее состояние переключателей SELinux для Apache с помощью команды .



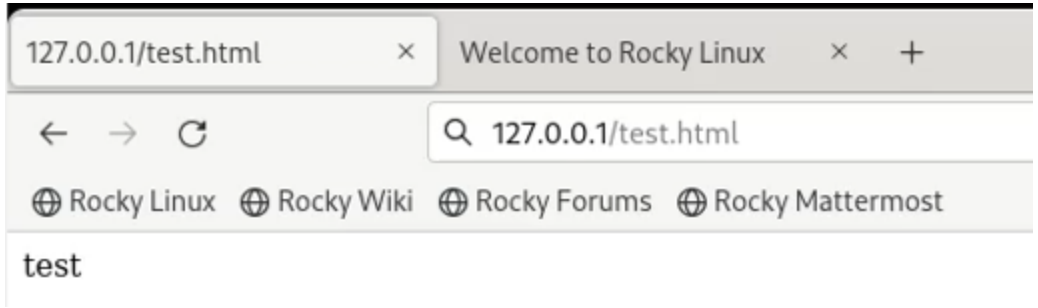
5. Определили тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды **ls -lZ /var/www**.

```
[a.polyakov@a ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 15:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0     6 May 16 15:10 html
```

6. Создали от имени суперпользователя html-файл /var/www/html/test.html следующего содержания:

7. Проверили контекст созданного файла - httpd_sys_content_t.

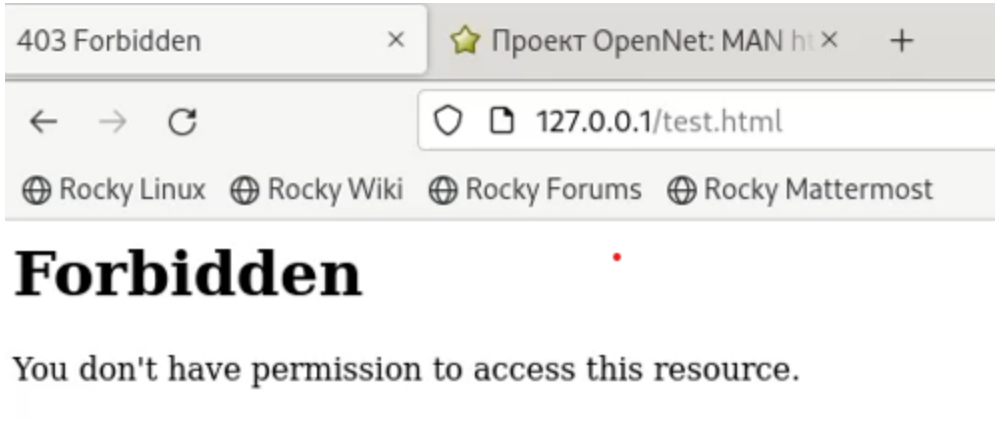
8. Обратитились к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html и убедились, что файл был успешно отображён.



9. Изменили контекст файла И проверили, что контекст поменялся.

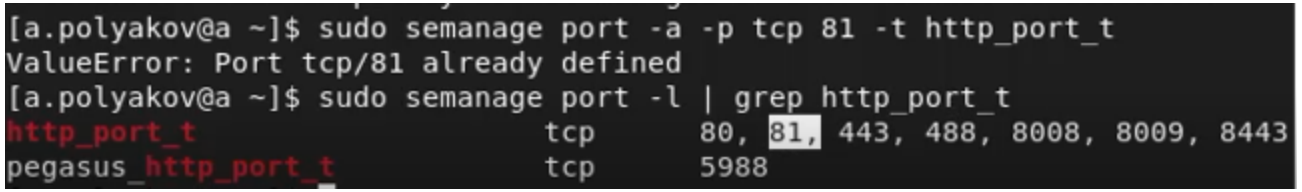
```
[a.polyakov@a ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[a.polyakov@a ~]$ ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:samba_share_t:s0 33 Oct 12 19:27 test.html
```

10. Пробуем ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. В результате получили ошибку.



11. Попробуем запустить веб-сервер Apache на прослушивание TCP-порта 81. Для этого в файле /etc/httpd/httpd.conf находим строчку Listen 80 и заменяем её на Listen 81.

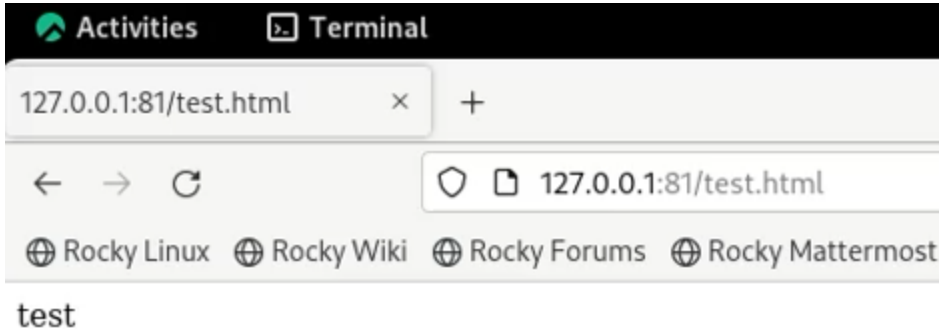
12. Выполним перезапуск веб-сервера Apache. Произошёл сбой? Нет.
13. Выполним команду **semanage port -a -t http_port_t -p tcp 81**. Вылетает ValueError в связи с тем, что порт уже определен. После этого проверим список портов командой **semanage port -l | grep http_port_t** и убедились, что порт 81 появился в списке.



14. Вернули контекст httpd_sys_content__t к файлу /var/www/html/test.html: **chcon -t httpd_sys_content_t /var/www/html/test.html**

```
[a.polyakov@a ~]$ sudo chcon -t httpd_sys_content_t /var/www/html/test.htm
```

После этого пробуем получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. В результате увидели содержимое файла — слово «test».



15. Исправим обратно конфигурационный файл apache, вернув Listen 80.

```
46 #Listen 12.34.56.78:80
47 Listen 80
48
```

16. Удалим привязку http_port_t к 81 порту: **semanage port -d -t http_port_t -p tcp 81** и проверим, что порт 81 удалён. Данная команда не была выполнена.

```
[a.polyakov@a ~]$ sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
```

17. Удалим файл /var/www/html/test.html: **rm /var/www/html/test.html**.

```
[a.polyakov@a ~]$ sudo rm /var/www/html/test.html
[a.polyakov@a ~]$ ls /var/www/html
[a.polyakov@a ~]$ ls -l /var/www/html
total 0
```

Вывод

В ходе выполнения лабораторной работы мы развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux1. Проверили работу SELinx на практике совместно с веб-сервером Apache.