

Знакомство с SELinux

Шаян Фаисал НФИбд-02-19

14 октября, 2022, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

SELinux или Security Enhanced Linux — это улучшенный механизм управления доступом, разработанный Агентством национальной безопасности США (АНБ США) для предотвращения злонамеренных вторжений. Он реализует принудительную (или мандатную) модель управления доступом (англ. Mandatory Access Control, MAC) поверх существующей дискреционной (или избирательной) модели (англ. Discretionary Access Control, DAC), то есть разрешений на чтение, запись, выполнение.

Apache – это свободное программное обеспечение для размещения веб-сервера. Он хорошо показывает себя в работе с масштабными проектами, поэтому заслуженно считается одним из самых популярных веб-серверов. Кроме того, Apache очень гибок в плане настройки, что даёт возможность реализовать все особенности размещаемого веб-ресурса.

Цель лабораторной работы

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

Выполнение лабораторной работы

Запуск HTTP-сервера

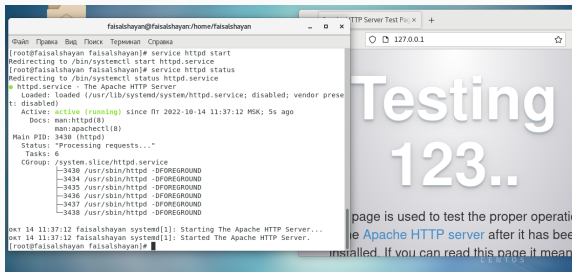


Figure 1: запуск http

Создание HTML-файла

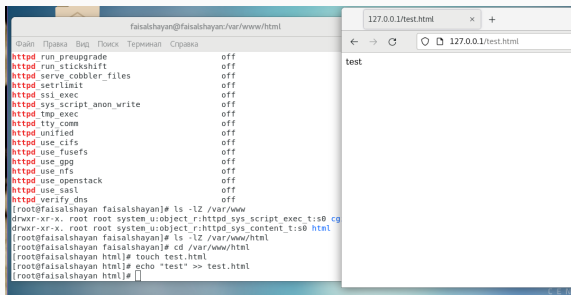


Figure 2: создание html-файла и доступ по http

Изменение контекста безопасности

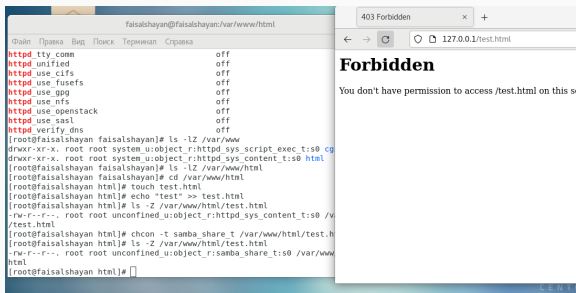
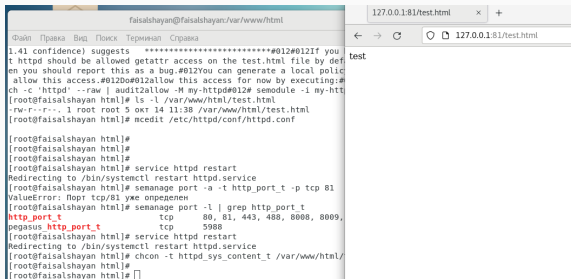


Figure 3: ошибка доступа после изменения контекста

Переключение порта и восстановление контекста безопасности



The image shows a terminal window on the left and a web browser on the right. The terminal window is titled 'faisalshayan@faisalshayan:/var/www/html' and shows the following commands and output:

```
faisalshayan@faisalshayan:/var/www/html
1.41 confidence) suggests *****#012#012If you
t httpd should be allowed getattr access on the test.html file by def
en you should report this as a bug.#012You can generate a local polic
allow this access.#012Do#012allow this access for now by executing:#
ch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -i my-htt
[root@faisalshayan html]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 50K 14 11:38 /var/www/html/test.html
[root@faisalshayan html]# ncedit /etc/httpd/conf/httpd.conf

[root@faisalshayan html]#
[root@faisalshayan html]#
[root@faisalshayan html]#
[root@faisalshayan html]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@faisalshayan html]# semanage port -a -t http_port_t -p tcp 81
ValueError: Nopr tcp/81 yxe onpedenen
[root@faisalshayan html]# semanage port -l | grep http_port_t
http_port_t tcp 80, 81, 443, 488, 8008, 8009,
pegasus http_port_t tcp 5988
[root@faisalshayan html]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@faisalshayan html]# chcon -t httpd_sys_content_t /var/www/html/
[root@faisalshayan html]#
```

The web browser on the right shows the address bar with the URL '127.0.0.1:81/test.html' and the page content 'test'.

Figure 4: доступ по http на 81 порт

Выводы

Результаты выполнения лабораторной работы

В процессе выполнения лабораторной работы мною были получены базовые навыки работы с технологией seLinux.