

Знакомство с SELinux

Хамди Мохаммад

10 апреля, 2025, 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

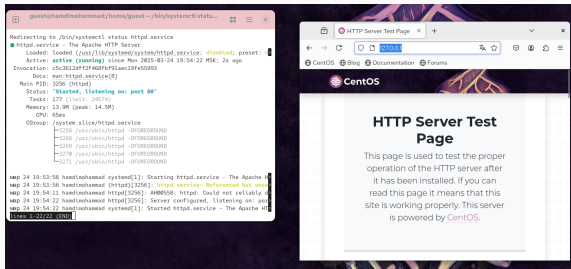


Рис. 1: запуск http

Создание HTML-файла

```
root@hamdimohammad: /home/guest ~#  
root@hamdimohammad:/home/guest# ls -lZ /var/www  
итого 0  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 янв 27 03  
:00 cgi-bin  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 янв 27 03  
:00 html  
root@hamdimohammad:/home/guest# ls -lZ /var/www/html  
итого 0  
root@hamdimohammad:/home/guest# cd /var/www/html  
root@hamdimohammad:/var/www/html# echo test >> test.html  
root@hamdimohammad:/var/www/html# ls -lZ /var/www/html  
итого 4  
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 5 мар 24 19  
:55 test.html  
root@hamdimohammad:/var/www/html#
```

Рис. 2: создание html-файла и доступ по http

Изменение контекста безопасности

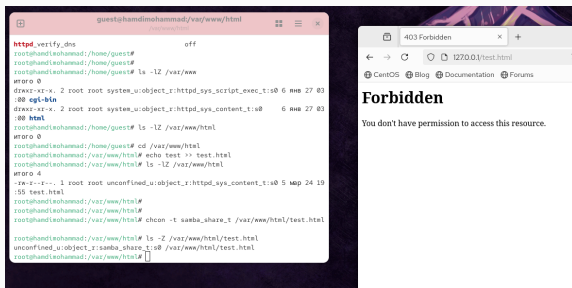


Рис. 3: ошибка доступа после изменения контекста

Переключение порта и восстановление контекста безопасности

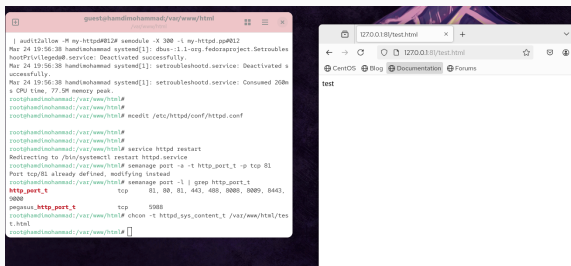


Рис. 4: доступ по http на 81 порт

Выводы

Результаты выполнения лабораторной работы

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