

Знакомство с SELinux

Завен Карапетян

29 сентября, 2024, 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

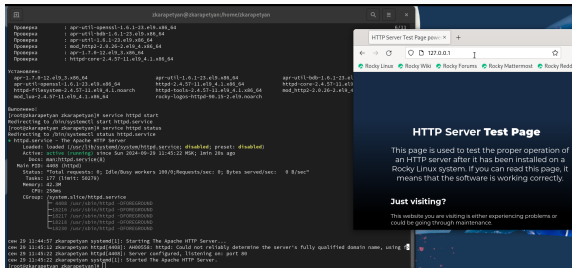
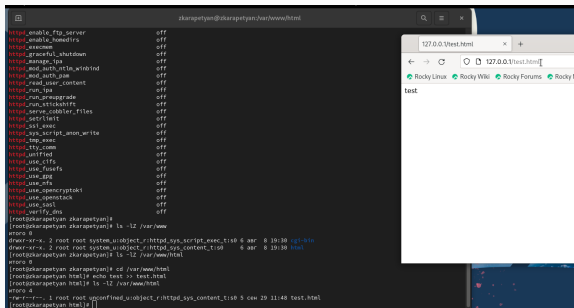


Figure 1: запуск http

Создание HTML-файла



The screenshot shows a terminal window on the left and a web browser on the right. The terminal window is titled 'zkarapetyan@zkarapetyan:/var/www/html' and displays a list of system services that are disabled, including ftp, httpd, and various network and security services. The user then runs the command 'echo test >> test.html' to create a file named 'test.html' in the current directory. The terminal output shows the command being executed successfully. The web browser on the right is titled '127.0.0.1/test.html' and displays the content of the file, which is the word 'test'.

```
zkarapetyan@zkarapetyan:/var/www/html
http_enable_ftp_server off
http_enable_homedirs off
http_execmem off
http_graceful_shutdown off
http_manage_ipa off
http_mod_auth_ntlm_winbind off
http_mod_auth_pam off
http_read_user_content off
http_run_ipa off
http_run_preupgrade off
http_run_atsckshift off
http_serve_cobbler_files off
http_get_tlmnt off
http_ssl_exec off
http_sys_script_anon_write off
http_top_exec off
http_ttycom off
http_unified off
http_use_cifs off
http_use_fusefs off
http_use_gpg off
http_use_nfs off
http_use_openssh off
http_use_openssl off
http_use_sasl off
http_verify_dns off
[roott@zkarapetyan zkarapetyan]#
[roott@zkarapetyan zkarapetyan]# ls -l2 /var/www
drwxr-xr-x 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 4K 8 10:30 cgi-bin
drwxr-xr-x 2 root root system_u:object_r:httpd_sys_content_t:s0 4K 8 10:30 html
[roott@zkarapetyan zkarapetyan]# ls -l2 /var/www/html
drwxr-xr-x 2 root root system_u:object_r:httpd_sys_content_t:s0 4K 8 10:30 test.html
[roott@zkarapetyan zkarapetyan]# cd /var/www/html
[roott@zkarapetyan html]# echo test >> test.html
[roott@zkarapetyan html]# ls -l2 /var/www/html
-rw-r--r-- 1 root root system_u:object_r:httpd_sys_content_t:s0 5 20 11:48 test.html
[roott@zkarapetyan html]#
```

Figure 2: создание html-файла и доступ по http

Изменение контекста безопасности

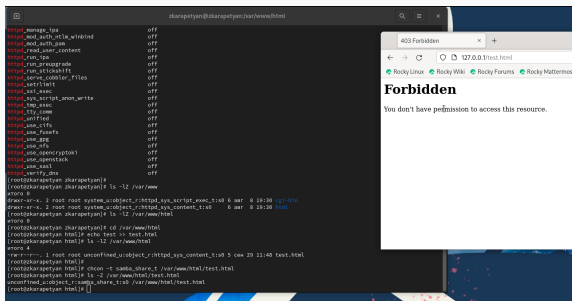


Figure 3: ошибка доступа после изменения контекста

Переключение порта и восстановление контекста безопасности

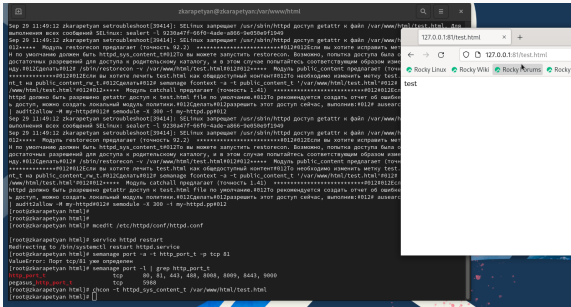


Figure 4: доступ по http на 81 порт

Выводы

Результаты выполнения лабораторной работы

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