

Знакомство с SELinux

Баранова Анастасия Павловна

30 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

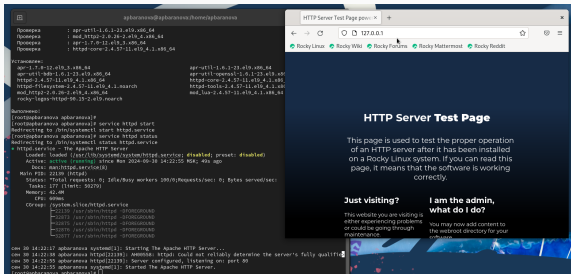
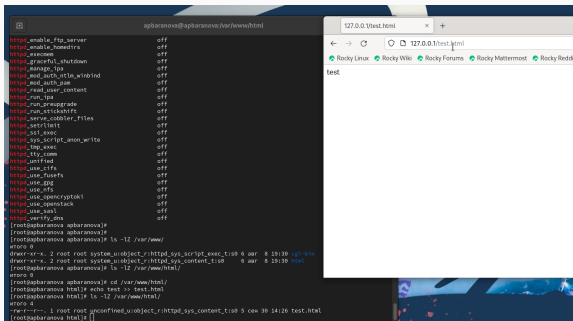


Figure 1: запуск http

Создание HTML-файла



The screenshot shows a terminal window on the left and a web browser on the right. The terminal window is titled 'apbaranova@apbaranova:~/var/www/html' and displays a list of services and their status, followed by commands to create and access an HTML file. The web browser window is titled '127.0.0.1/test.html' and shows the content 'test!'. The terminal output is as follows:

```
apbaranova@apbaranova:~/var/www/html
httpd_enable_ftp_server    off
httpd_enable_homedirs     off
httpd_execmem              off
httpd_grooveful_shutdown  off
httpd_manage_ipa           off
httpd_mod_auth_ntlm_wirbnd off
httpd_mod_auth_pam         off
httpd_read_user_content   off
httpd_run_ipa              off
httpd_run_apupgrade        off
httpd_run_atskshiffo       off
httpd_serve_cobalier_files off
httpd_setrlimit            off
httpd_ssl_exec             off
httpd_sys_script_anon_write off
httpd_ttp_exec             off
httpd_tty_comm             off
httpd_unified              off
httpd_use_cifs             off
httpd_use_fusefs           off
httpd_use_gpg              off
httpd_use_ftp              off
httpd_use_openssl           off
httpd_use_openssl          off
httpd_use_sasl             off
httpd_userid_ana           off
[root@apbaranova apbaranova]#
[root@apbaranova apbaranova]# ls -l /var/www/
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:0 0 aar 8 19:38 opt-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:0 0 aar 8 19:38 html
[root@apbaranova apbaranova]# ls -l /var/www/html/
total 0
[root@apbaranova apbaranova]# cd /var/www/html/
[root@apbaranova html]# echo test > test.html
[root@apbaranova html]# ls -l /var/www/html/
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:0 5 cex 30 14:26 test.html
[root@apbaranova html]#
```

Figure 2: создание html-файла и доступ по http

Изменение контекста безопасности

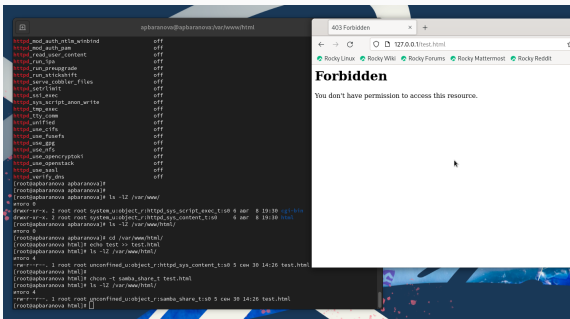


Figure 3: ошибка доступа после изменения контекста

Переключение порта и восстановление контекста безопасности

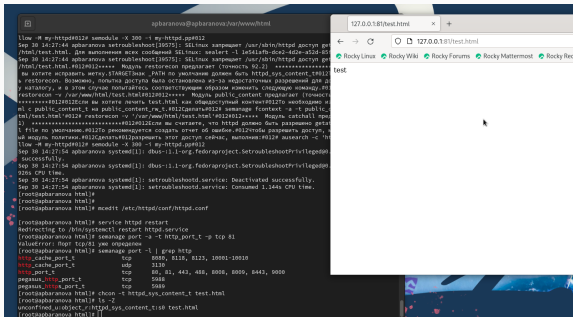


Figure 4: доступ по http на 81 порт

Выводы

Результаты выполнения лабораторной работы

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