

Знакомство с SELinux

Суннатилло Махмудов

7 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 НТТР-сервера

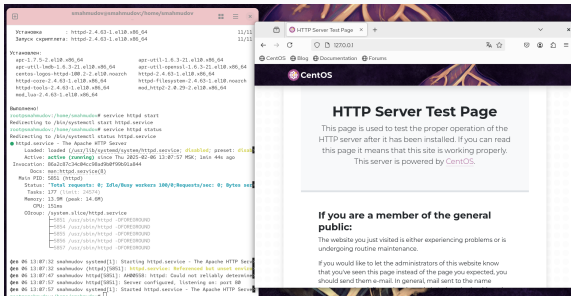
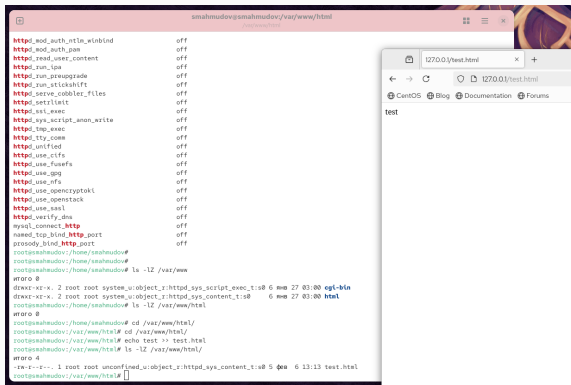


Рис. 1: запуск http

Создание HTML-файла



The image shows a terminal window on the left and a web browser on the right. The terminal window displays the output of the `ls -lZ /var/www` command, showing the permissions and ownership of files in the `/var/www` directory. The files listed are `cgi-bin` and `html`. The terminal also shows the command `echo test > test.html` being executed, which creates a file named `test.html` in the `/var/www/html` directory. The web browser on the right shows the URL `127.0.0.1/test.html` and the content of the file, which is the word `test`.

```
smahudov@smahudov: /var/www/html
/var/www/html
httpd_mod_auth_ntlm_winbind off
httpd_mod_auth_pam off
httpd_read_user_content off
httpd_run_ipa off
httpd_run_preupgrade off
httpd_run_stickshifft off
httpd_serve_cobbler_files off
httpd_setrlimit off
httpd_ssl_exec off
httpd_sys_script_anon_write off
httpd_tmp_exec off
httpd_tty_coma off
httpd_unified off
httpd_use_cifs off
httpd_use_fusefs off
httpd_use_gpg off
httpd_use_nfs off
httpd_use_openssl off
httpd_use_openssl off
httpd_use_openssl off
httpd_verify_dns off
mysql_connect_http off
named_top_bind_http_port off
prosody_bind_http_port off
root@smahudov: /home/smahudov#
root@smahudov: /home/smahudov#
root@smahudov: /home/smahudov# ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Мб 27 03:00 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Мб 27 03:00 html
root@smahudov: /home/smahudov# ls -lZ /var/www/html
total 0
-rw-r--r-- 1 root root system_u:object_r:httpd_sys_content_t:s0 5 Кб 6 13:13 test.html
root@smahudov: /var/www/html#
```

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

Изменение контекста безопасности

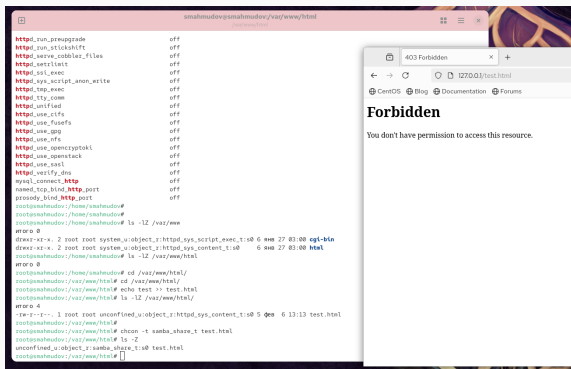
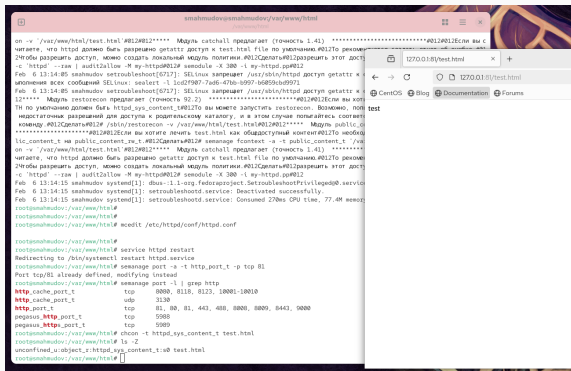


Рис. 3: ошибка доступа после изменения контекста

Переключение порта и восстановление контекста безопасности



```
on -v "/var/www/html/test.html #012#012"**** Модуль catchall предлагает (точность 1.41) *****#012#012Если вы с
читаете, что httpd должно быть разрешено получать доступ к test.html, file по умолчанию #012#012 реком
ndует разрешить доступ, можно создать локальный модуль политики.#012#012Сделайте#012#012разрешить этот досту
-c 'httpd' --raw | audit2allow -M my-httpd#012#012 semodule -X 300 -l my-httpd.pp#012
Feb 6 13:14:05 smahmudov setroubleshoot[6717]: SELinux запрещает /usr/sbin/httpd доступ getattr к
исполнению всех сообщений SELinux: sealert -l loc@1907-7a66-470a-b697-16859a9d9071
Feb 6 13:14:05 smahmudov setroubleshoot[6717]: SELinux запрещает /usr/sbin/httpd доступ getattr к
12**** Модуль restorecon предлагает (точность 92.2) *****#012#012Если вы хот
ли по умолчанию должен быть httpd_sys_content_t.#012#012То вы можете запустить restorecon. Возможно, по
недостаточная разрешенная для доступа к родительскому каталогу, и в этом случае попытайтесь команд
команду.#012#012Сделайте#012#012/var/www/html/test.html#012#012**** Модуль public_o
*****#012#012Если вы хотите лечить test.html как общедоступный контент.#012#012То необо
lic_content_t на public_content_rw_t.#012#012Сделайте#012#012 semanage fcontext -a -t public_content_t '/var
on -v "/var/www/html/test.html #012#012"**** Модуль catchall предлагает (точность 1.41) *****
читаете, что httpd должно быть разрешено получать доступ к test.html, file по умолчанию.#012#012То реком
ndует разрешить доступ, можно создать локальный модуль политики.#012#012Сделайте#012#012разрешить этот досту
-c 'httpd' --raw | audit2allow -M my-httpd#012#012 semodule -X 300 -l my-httpd.pp#012
Feb 6 13:14:15 smahmudov systemd[1]: dbus-1.12.org.fedoraproject.SetroubleshootPrivileged@0.service
Feb 6 13:14:15 smahmudov systemd[1]: setroubleshoot.service: Deactivated successfully.
Feb 6 13:14:15 smahmudov systemd[1]: setroubleshoot.service: Consumed 270ms CPU time, 77.4M memory.
root@smahmudov:/var/www/html#
root@smahmudov:/var/www/html#
root@smahmudov:/var/www/html# nccedit /etc/httpd/conf/httpd.conf
root@smahmudov:/var/www/html#
root@smahmudov:/var/www/html# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
root@smahmudov:/var/www/html# semanage port -a -t httpd_t -p tcp 81
Port tcp/81 already defined, modifying instead
root@smahmudov:/var/www/html# semanage port -l | grep http
http_cache_port_t          tcp      8080, 8118, 8123, 10001-10010
http_cache_port_t          udp      3130
http_port_t                tcp      81, 80, 82, 443, 488, 8080, 8089, 8443, 9000
pegasus_http_port_t        tcp      5988
pegasus_https_port_t       tcp      5989
root@smahmudov:/var/www/html# chcon -t httpd_sys_content_t test.html
root@smahmudov:/var/www/html# ls -l
unconfined_u:object_r:httpd_sys_content_t:0 test.html
root@smahmudov:/var/www/html#
```

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.