

Знакомство с SELinux

Боровиков Даниил Александрович

27 апреля, 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.

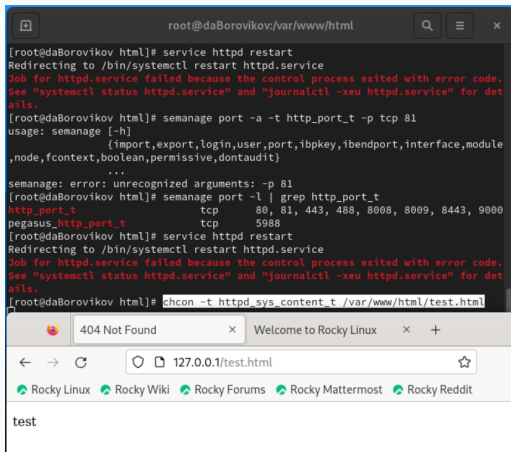
Apache – это свободное программное обеспечение для размещения веб-сервера. Он хорошо показывает себя в работе с масштабными проектами, поэтому заслуженно считается одним из самых популярных веб-серверов. Кроме того, Apache очень гибок в плане настройки, что даёт возможность реализовать все особенности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



The screenshot shows a terminal window with the following commands and output:

```
root@daBorovikov:var/www/html
[root@daBorovikov html]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
Job for httpd.service failed because the control process exited with error code.
See "systemctl status httpd.service" and "journalctl -xeu httpd.service" for details.
[root@daBorovikov html]# semanage port -a -t http_port_t -p tcp 81
usage: semanage [-h]
               {import,export,login,user,port,ibpkey,ibendport,interface,module,
               ,node,fcontext,boolean,permissive,dontaudit}
               ...
semanage: error: unrecognized arguments: -p 81
[root@daBorovikov html]# semanage port -l | grep http_port_t
http_port_t      tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t tcp      5988
[root@daBorovikov html]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
Job for httpd.service failed because the control process exited with error code.
See "systemctl status httpd.service" and "journalctl -xeu httpd.service" for details.
[root@daBorovikov html]# chcon -t http_sys_content_t /var/www/html/test.html
```

Below the terminal window, a web browser is open. The address bar shows "127.0.0.1/test.html". The page content displays "test". The browser's tab bar shows "404 Not Found" and "Welcome to Rocky Linux". The browser's bookmark bar includes links to "Rocky Linux", "Rocky Wiki", "Rocky Forums", "Rocky Mattermost", and "Rocky Reddit".

Figure 1: запуск http

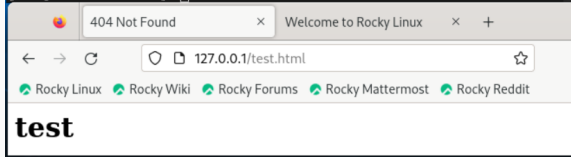
Создание HTML-файла

```
root@daBorovikov:~  
httpd_dbus_sssd off  
httpd_dontaudit_search_dirs off  
httpd_enable_cgi on  
httpd_enable_ftp_server off  
httpd_enable_homedirs off  
httpd_execmem off  
httpd_graceful_shutdown off  
httpd_manage_ipa off  
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_stickshift off  
httpd_serve_cobbler_files off  
httpd_setrlimit off  
httpd_ssi_exec off  
httpd_sys_script_anon_write off  
httpd_tmp_exec off  
httpd_tty_comm off  
httpd_unified off  
httpd_use_cifs off  
httpd_use_fusefs off  
httpd_use_gpg off  
httpd_use_nfs off  
httpd_use_opencryptoki off  
httpd_use_openstack off  
httpd_use_sasl off  
httpd_verify_dns off  
[root@daBorovikov ~]#
```

Figure 2: создание html-файла и доступ по http

Изменение контекста безопасности

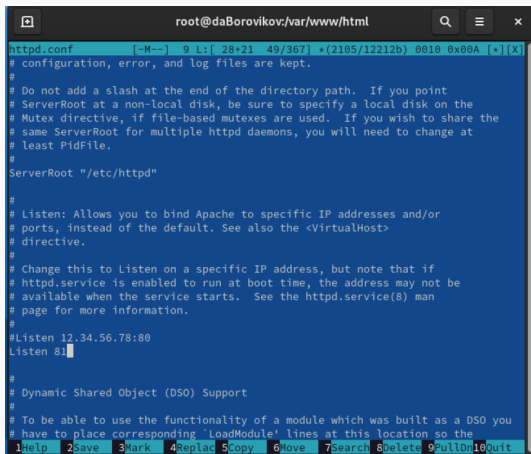
```
[root@daBorovikov ~]# ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Oct 28 12
:35 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Oct 28 12
:35 html
[root@daBorovikov ~]# ls -lZ /var/www/html/
total 0
[root@daBorovikov ~]# cd /var/www/html/
[root@daBorovikov html]# echo "test" > test.html
[root@daBorovikov html]#
```



The screenshot shows a web browser window with two tabs: '404 Not Found' and 'Welcome to Rocky Linux'. The address bar contains '127.0.0.1/test.html'. Below the address bar, there are links to 'Rocky Linux', 'Rocky Wiki', 'Rocky Forums', 'Rocky Mattermost', and 'Rocky Reddit'. The main content area of the browser displays the word 'test' in a large, bold, black font.

Figure 3: ошибка доступа после изменения контекста

Переключение порта и восстановление контекста без-опасности



```
root@daBorovikov:/var/www/html
httpd.conf [-M--] 9 L:[ 28+21 49/367] *(2105/12212b) 0010 0x00A [*][X]
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path. If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used. If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
ServerRoot "/etc/httpd"
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts. See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
Listen 81
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn10Quit
```

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.