

Знакомство с SELinux

Владислав Ракинцев

28 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.

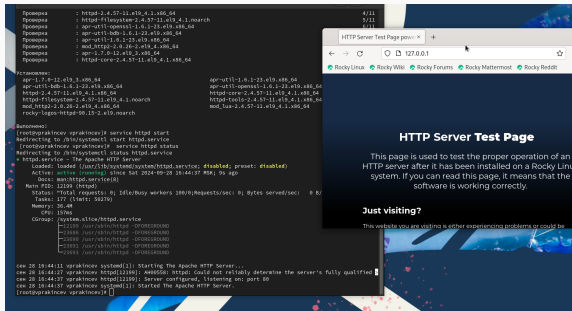
Apache – это свободное программное обеспечение для размещения веб-сервера. Он хорошо показывает себя в работе с масштабными проектами, поэтому заслуженно считается одним из самых популярных веб-серверов. Кроме того, Apache очень гибок в плане настройки, что даёт возможность реализовать все особенности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



```
Процесса : httpd-2.4.57-11.el9_4.1.x86_64
Процесса : httpd-fsfilesystem-2.4.57-11.el9_4.1.march
Процесса : apr-util-openssl-1.6.1-23.el9.x86_64
Процесса : apr-util-ssl-1.6.1-23.el9.x86_64
Процесса : apr-util-1.6.1-23.el9.x86_64
Процесса : mod_ssl-2.4.57-11.el9_4.1.x86_64
Процесса : apr-1.7.5-12.el9_3.x86_64
Процесса : httpd-core-2.4.57-11.el9_4.1.x86_64

#transaction:
apr-1.7.5-12.el9_3.x86_64
apr-util-1.6.1-23.el9.x86_64
httpd-2.4.57-11.el9_4.1.x86_64
httpd-fsfilesystem-2.4.57-11.el9_4.1.march
mod_httpd-2.0.26-2.el9_4.x86_64
rocky-logos-httpd-90.15-2.el9.noarch

#systemd:
[root@prakhincov vprakhincov]# service httpd start
Redirecting to systemctl start httpd.service
[root@prakhincov vprakhincov]# systemctl status httpd.service
Redirecting to systemctl status httpd.service
# httpd.service - The Apache HTTP Server
* Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
* Active: active (running) since Sat 2024-09-29 18:44:37 MSK; 9s ago
* Docs: man:httpd.service(8)
* Main PID: 12193 (httpd)
* Status: 'Total: 0 requests; 0 idle/busy workers 100/0/requests/sec: 0; Bytes served/sec: 0 B/s'
* Tasks: 177 (limit: 50276)
* Memory: 36.4M
* CPU: 139ms
* Group: /system.slice/httpd.service
└─12193 /usr/sbin/httpd --DFOREGROUND
└─12194 /usr/sbin/httpd --DFOREGROUND
└─12195 /usr/sbin/httpd --DFOREGROUND
└─12196 /usr/sbin/httpd --DFOREGROUND
└─12197 /usr/sbin/httpd --DFOREGROUND

csw 20 18:44:11 vprakhincov systemd[1]: Starting The Apache HTTP Server...
csw 20 18:44:17 vprakhincov httpd[12193]: AH00558: httpd: could not reliably determine the server's fully qualified
csw 20 18:44:37 vprakhincov httpd[12193]: Server configured, listening on port 80
csw 20 18:44:37 vprakhincov systemd[1]: Started The Apache HTTP Server.
[root@prakhincov vprakhincov]#
```

HTTP Server Test Page

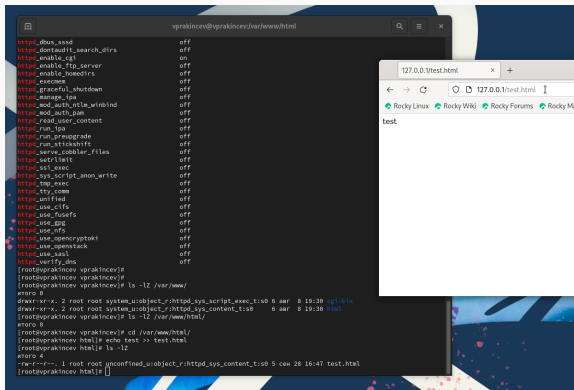
This page is used to test the proper operation of an HTTP server after it has been installed on a Rocky Linux system. If you can read this page, it means that the software is working correctly.

Just visiting?

This website you are visiting is either experiencing problems or could be

Figure 1: запуск http

Создание HTML-файла



The image shows a terminal window and a web browser. The terminal window displays the configuration of the httpd service, followed by commands to create a directory, create an HTML file, and start the service. The web browser shows the content of the created HTML file, which is the word "test".

```
xprakincev@vprakincev:/var/www/html
httpd_dbus_snd off
httpd_dontaudit_search_dirs off
httpd_enable_cgi on
httpd_enable_ftp_server off
httpd_enable_homedirs off
httpd_execroot 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_atctashift off
httpd_serve_cobbler_files off
httpd_setrlimit off
httpd_ssl_exec off
httpd_sys_script_anon_write 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_openssl off
httpd_use_openssl off
httpd_use_sasl off
httpd_verify_dns off
[root@vprakincev vprakincev]#
[root@vprakincev vprakincev]# ls -l /var/www/
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 aur 8 19:38 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 aur 8 19:38 html
[root@vprakincev vprakincev]# ls -l /var/www/html/
total 0
[root@vprakincev vprakincev]# cd /var/www/html/
[root@vprakincev html]# echo test >> test.html
[root@vprakincev html]# ls -l
total 4
-rw-r--r-- 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 5 cew 28 16:47 test.html
[root@vprakincev html]#
```

127.0.0.1/test.html x +
test

Figure 2: создание html-файла и доступ по http

Изменение контекста безопасности

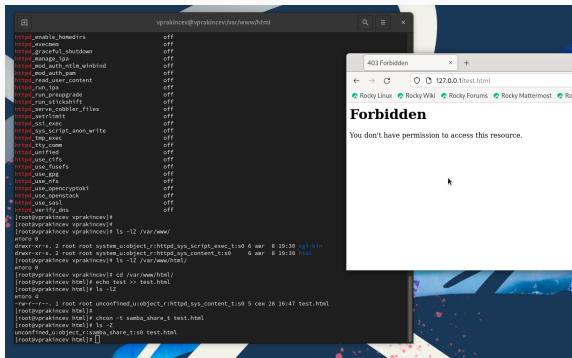


Figure 3: ошибка доступа после изменения контекста

Переключение порта и восстановление контекста без-опасности

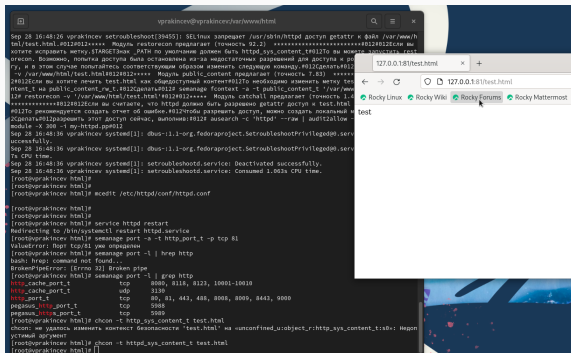


Figure 4: доступ по http на 81 порт

Выводы

Результаты выполнения лабораторной работы

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