

Знакомство с SELinux

Стаменкович Огнен

11 октября, 2022, 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.

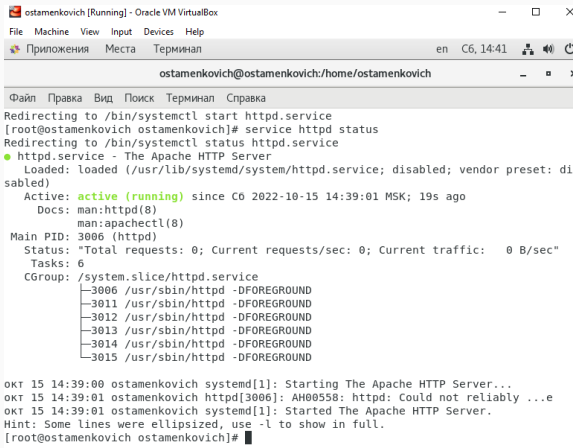
Apache – это свободное программное обеспечение для размещения веб-сервера. Он хорошо показывает себя в работе с масштабными проектами, поэтому заслуженно считается одним из самых популярных веб-серверов. Кроме того, Apache очень гибок в плане настройки, что даёт возможность реализовать все особенности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

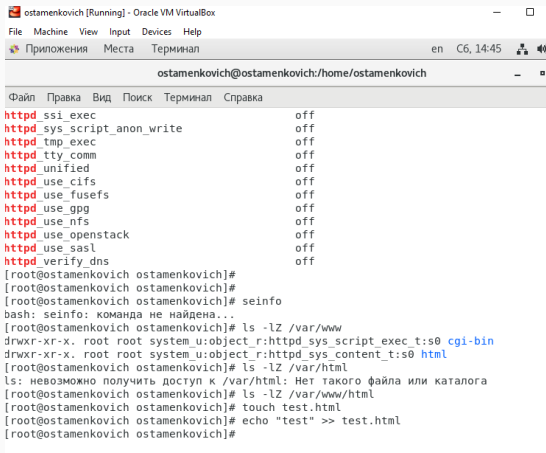


```
ostamenkovich [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Приложения Места Терминал en C6, 14:41
ostamenkovich@ostamenkovich:/home/ostamenkovich
Файл Правка Вид Поиск Терминал Справка
Redirecting to /bin/systemctl start httpd.service
[root@ostamenkovich ostamenkovich]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since C6 2022-10-15 14:39:01 MSK; 19s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Main PID: 3006 (httpd)
    Status: "Total requests: 0; Current requests/sec: 0; Current traffic:  0 B/sec"
     Tasks: 6
    CGroup: /system.slice/httpd.service
            └─3006 /usr/sbin/httpd -DFOREGROUND
              └─3011 /usr/sbin/httpd -DFOREGROUND
                └─3012 /usr/sbin/httpd -DFOREGROUND
                  └─3013 /usr/sbin/httpd -DFOREGROUND
                    └─3014 /usr/sbin/httpd -DFOREGROUND
                      └─3015 /usr/sbin/httpd -DFOREGROUND

окт 15 14:39:00 ostamenkovich systemd[1]: Starting The Apache HTTP Server...
окт 15 14:39:01 ostamenkovich httpd[3006]: AH00558: httpd: Could not reliably ...e
окт 15 14:39:01 ostamenkovich systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[root@ostamenkovich ostamenkovich]#
```

Figure 1: запуск http

Создание HTML-файла



```
ostamenkovich [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Приложения Места Терминал en C6, 14:45
ostamenkovich@ostamenkovich:/home/ostamenkovich

Файл Правка Вид Поиск Терминал Справка

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_openstack off
httpd_use_sasl off
httpd_verify_dns off

[root@ostamenkovich ostamenkovich]#
[root@ostamenkovich ostamenkovich]#
[root@ostamenkovich ostamenkovich]# seinfo
bash: seinfo: команда не найдена...
[root@ostamenkovich ostamenkovich]# ls -lZ /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[root@ostamenkovich ostamenkovich]# ls -lZ /var/html
ls: невозможно получить доступ к /var/html: Нет такого файла или каталога
[root@ostamenkovich ostamenkovich]# ls -lZ /var/www/html
[root@ostamenkovich ostamenkovich]# touch test.html
[root@ostamenkovich ostamenkovich]# echo "test" >> test.html
[root@ostamenkovich ostamenkovich]#
```

Figure 2: создание html-файла и доступ по http

Изменение контекста безопасности

```
[root@ostamenkovich ostamenkovich]# ls -lZ /var/www/html
[root@ostamenkovich ostamenkovich]# cd /var/www/html
[root@ostamenkovich html]# echo "test" >> test.html
[root@ostamenkovich html]#
[root@ostamenkovich html]#
[root@ostamenkovich html]#
[root@ostamenkovich html]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@ostamenkovich html]# chcon -t samba_share_t /var/www/html/test.html
[root@ostamenkovich html]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@ostamenkovich html]#
```

Figure 3: ошибка доступа после изменения контекста

Переключение порта и восстановление контекста без-опасности

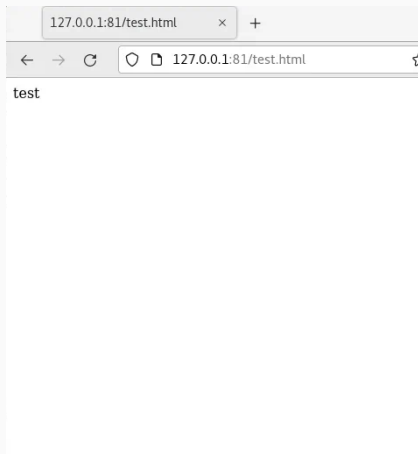


Figure 4: доступ по http на 81 порт

Выводы

Результаты выполнения лабораторной работы

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