

# Знакомство с SELinux

---

Ласурия Данил

15 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.

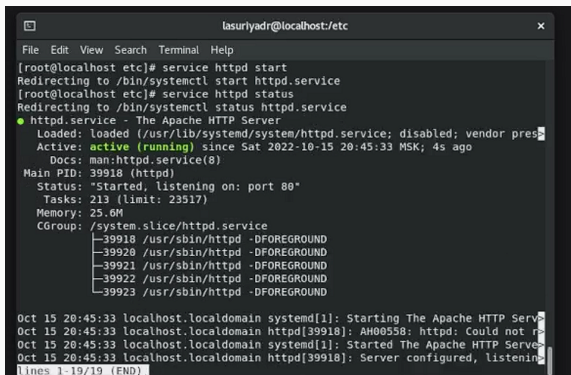
## Цель лабораторной работы

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



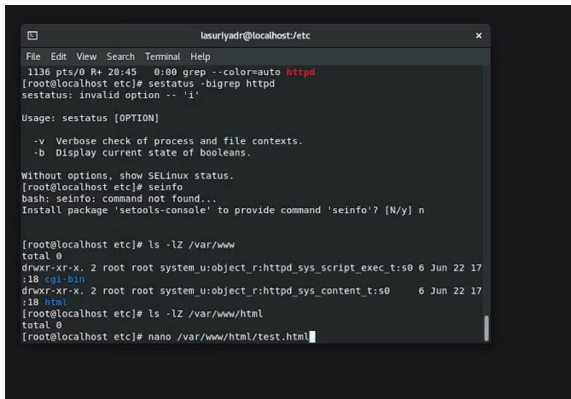
```
lasuriyadi@localhost:/etc
File Edit View Search Terminal Help

[root@localhost etc]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@localhost etc]# 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: enabled)
   Active: active (running) since Sat 2022-10-15 20:45:33 MSK; 4s ago
     Docs: man:httpd.service(8)
   Main PID: 39918 (httpd)
    Status: "Started, listening on: port 80"
     Tasks: 213 (limit: 23517)
    Memory: 25.6M
    CGroup: /system.slice/httpd.service
            └─39918 /usr/sbin/httpd -DFOREGROUND
              └─39920 /usr/sbin/httpd -DFOREGROUND
                └─39921 /usr/sbin/httpd -DFOREGROUND
                  └─39922 /usr/sbin/httpd -DFOREGROUND
                    └─39923 /usr/sbin/httpd -DFOREGROUND

Oct 15 20:45:33 localhost.localdomain systemd[1]: Starting The Apache HTTP Server: httpd.
Oct 15 20:45:33 localhost.localdomain httpd[39918]: AH00558: httpd: Could not r
Oct 15 20:45:33 localhost.localdomain systemd[1]: Started The Apache HTTP Server: httpd.
Oct 15 20:45:33 localhost.localdomain httpd[39918]: Server configured, listening
lines 1-19/19 (END)
```

Figure 1: запуск http

# Создание HTML-файла



```
lasurlyadr@localhost:/etc
File Edit View Search Terminal Help
1136 pts/0 R+ 20:45 0:00 grep --color=auto httpd
[root@localhost etc]# sestatus -bigrep httpd
sestatus: invalid option -- 'i'

Usage: sestatus [OPTION]

  -v Verbose check of process and file contexts.
  -b Display current state of booleans.

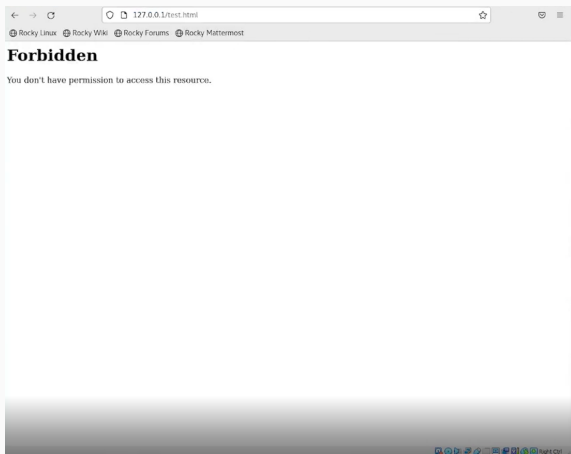
Without options, show SELinux status.
[root@localhost etc]# seinfo
bash: seinfo: command not found...
Install package 'setools-console' to provide command 'seinfo'? [N/y] n

[root@localhost etc]# ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Jun 22 17
:18 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Jun 22 17
:18 html
[root@localhost etc]# ls -lZ /var/www/html
total 0
[root@localhost etc]# nano /var/www/html/test.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 без-опасности

```
[root@localhost etc]# 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@localhost etc]# 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
```

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.