

Презентация

Ощепков Дмитрий Владимирович НКАбд-02-22

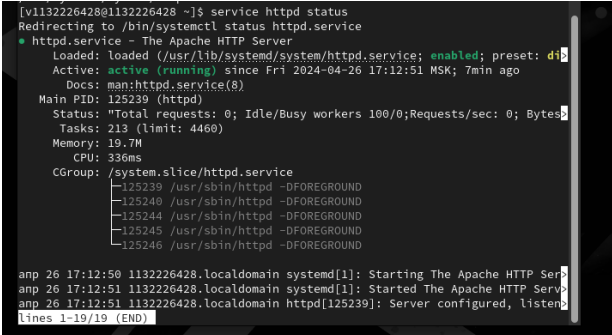
Дисциплина: Основы информационной безопасности

Лабораторная работа №6

Цель работы: развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux на практике совместно с веб-сервером Apache.

Обратился с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает:

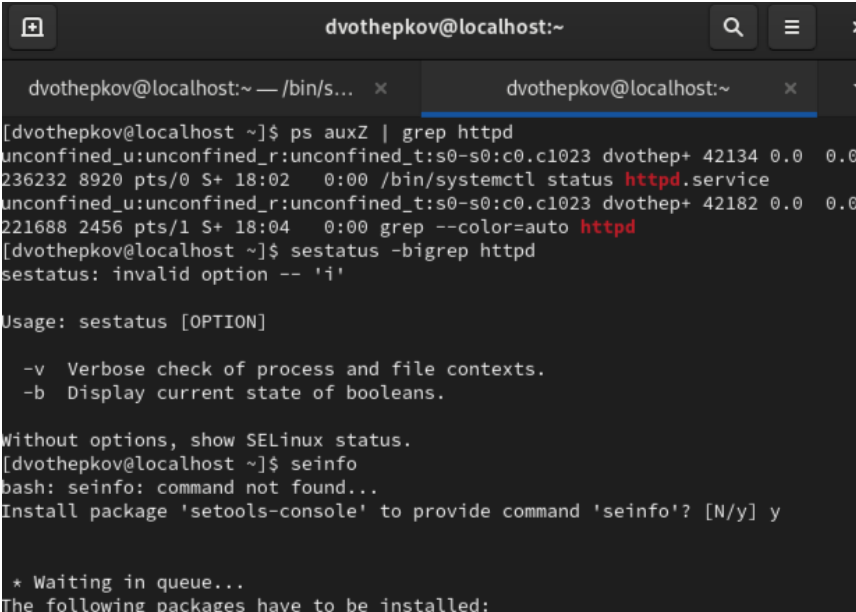
```
[dvothepkov@localhost ~]$ service httpd status
```



```
Redirecting to /bin/systemctl status httpd.service
• httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Active: active (running) since Fri 2024-04-26 17:12:51 MSK; 7min ago
     Docs: man:httpd.service(8)
   Main PID: 125239 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served: 0; CPU usage: 0.0%; Uptime: 7min 12s"
   Tasks: 213 (limit: 4460)
   Memory: 19.7M
     CPU: 336ms
   CGroup: /system.slice/httpd.service
           └─125239 /usr/sbin/httpd -DFOREGROUND
             └─125240 /usr/sbin/httpd -DFOREGROUND
               └─125244 /usr/sbin/httpd -DFOREGROUND
                 └─125245 /usr/sbin/httpd -DFOREGROUND
                   └─125246 /usr/sbin/httpd -DFOREGROUND

anp 26 17:12:50 1132226428.localdomain systemd[1]: Starting The Apache HTTP Server: httpd.service.
anp 26 17:12:51 1132226428.localdomain systemd[1]: Started The Apache HTTP Server: httpd.service.
anp 26 17:12:51 1132226428.localdomain httpd[125239]: Server configured, listening on: 127.0.0.1:80
lines 1-19/19 (END)
```

Найшел веб-сервер Apache в списке процессов, определил его контекст безопасности и занес эту информацию в отчёт.



```
dvothepkov@localhost:~
```

```
[dvothepkov@localhost ~]$ ps auxZ | grep httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 dvothep+ 42134 0.0 0.0
236232 8920 pts/0 S+ 18:02 0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 dvothep+ 42182 0.0 0.0
221688 2456 pts/1 S+ 18:04 0:00 grep --color=auto httpd
[dvothepkov@localhost ~]$ sestatus -bigrep httpd
sestatus: invalid option -- 'i'

Usage: sestatus [OPTION]

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

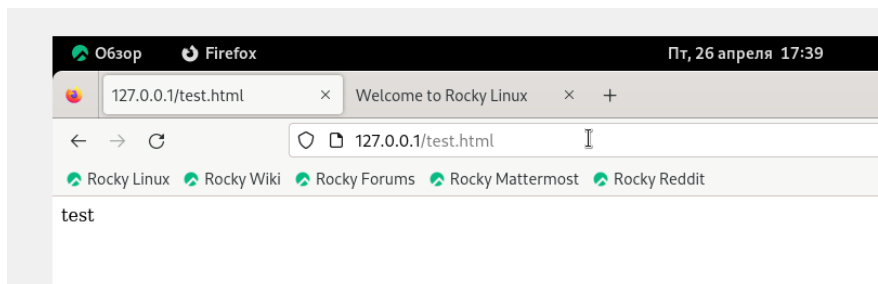
Without options, show SELinux status.
[dvothepkov@localhost ~]$ seinfo
bash: seinfo: command not found...
Install package 'setools-console' to provide command 'seinfo'? [N/y] y

* Waiting in queue...
The following packages have to be installed:
```

Создал от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл `/var/www/html/test.html` следующего содержания:

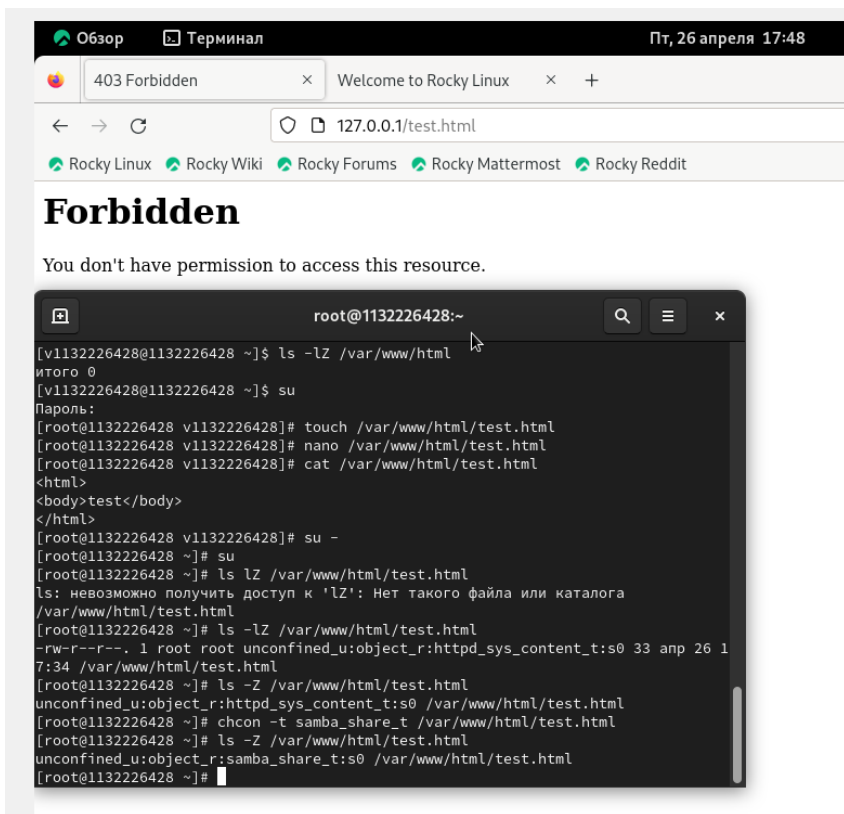
```
[root@1132226428 v1132226428]# touch /var/www/html/test.html
[root@1132226428 v1132226428]# nano /var/www/html/test.html
[root@1132226428 v1132226428]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[root@1132226428 v1132226428]#
```

Обратился к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедитесь, что файл был успешно отображён

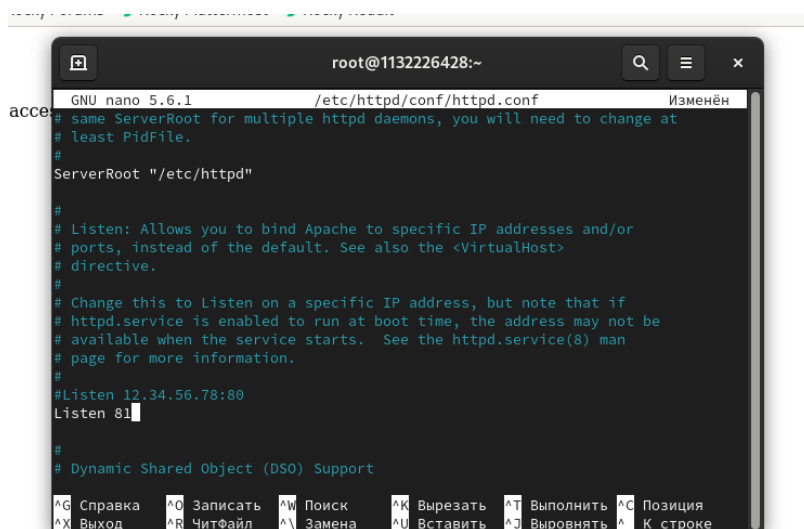


Изменил контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на любой другой, к которому процесс `httpd` не должен иметь доступа, например, на `samba_share_t`: `chcon -t samba_share_t /var/www/html/test.html ls -Z /var/www/html/test.html`

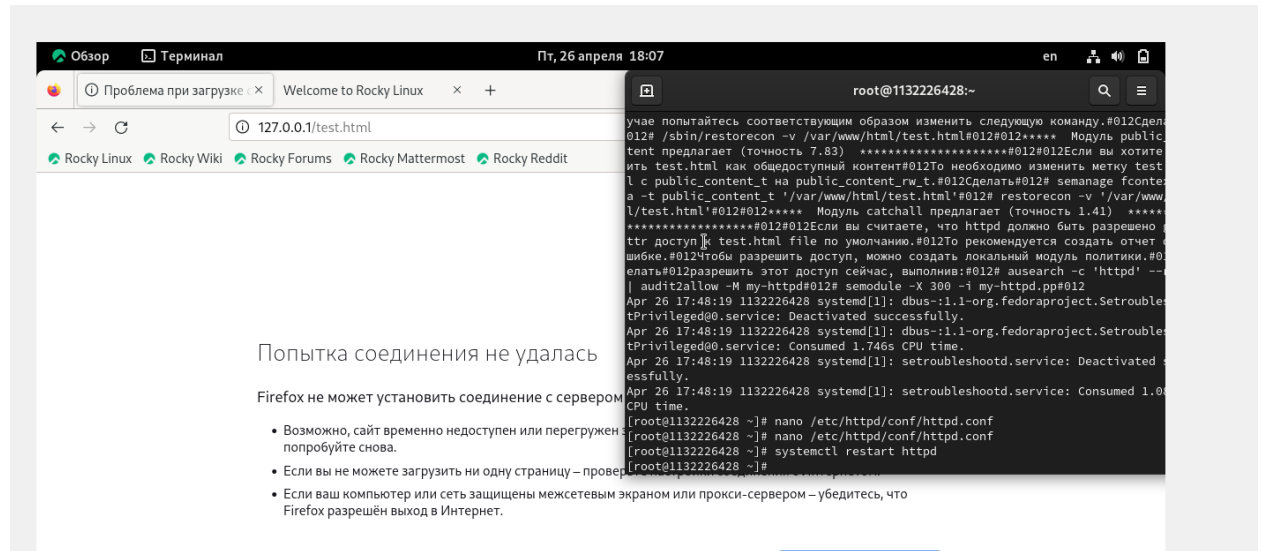
После этого проверил, что контекст поменялся. Попробовал ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`.



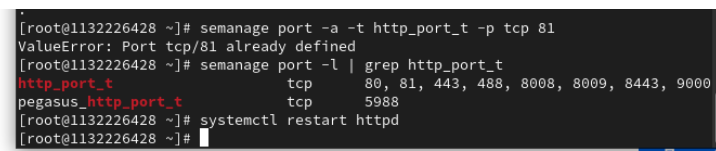
Попробовал запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf нашел строчку Listen 80 и заменил её на Listen 81.

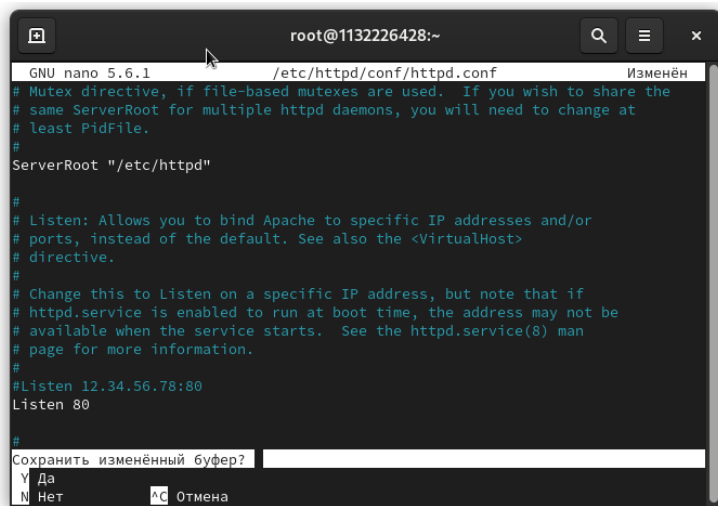
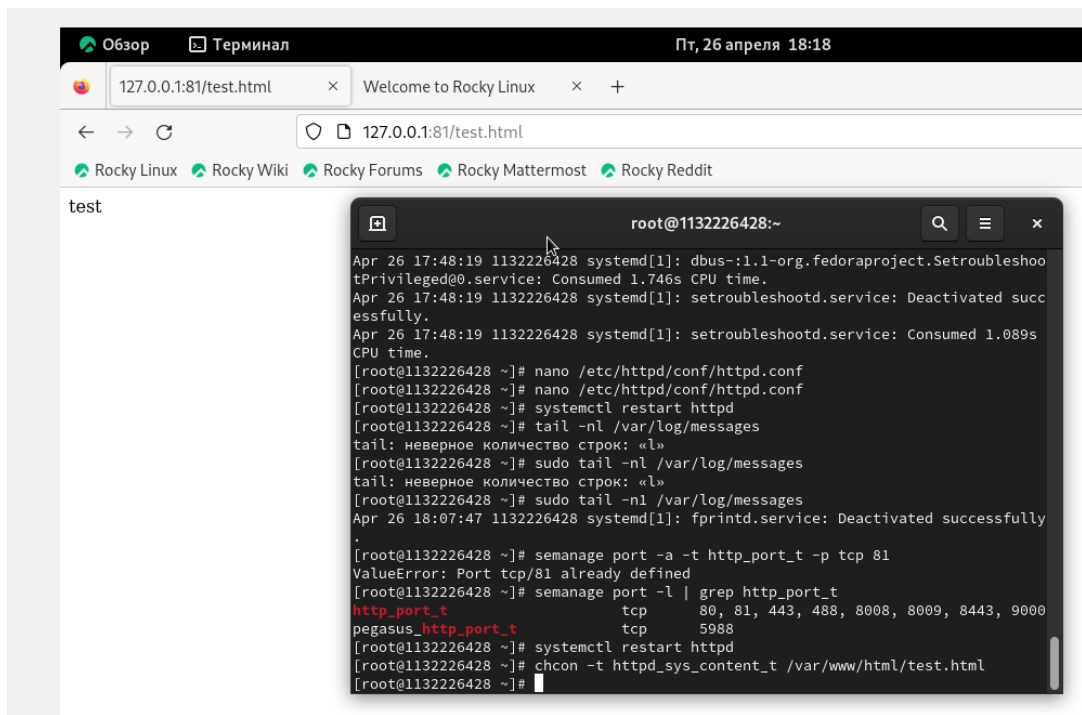


Выполнил перезапуск веб-сервера Apache



Выполнил следующую команду





Удалил привязку http_port_t к 81 порту

```
[root@1132226428 ~]# nano /etc/httpd/conf/httpd.conf  
[root@1132226428 ~]# semanage port -d -t http_port_t -p tcp 81
```

Вывод: развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinux на практике совместно с веб-сервером Apache.