

# Презентация к лабораторной работе 6

## Основы информационной безопасности

---

Хрусталев Влад Николаевич

Российский университет дружбы народов им. Патриса Лумумбы, Москва, Россия

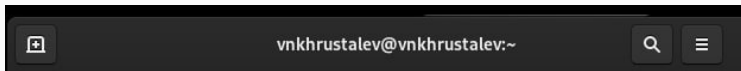
Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux на практике совместно с веб-сервером Apache.

# Сделаем подготовительные операции перед работой

```
[vnkhrustalev@vnkhrustalev ~]$ 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 Sat 2024-04-27 19:46:36 MSK; 15min ago
  Docs: man:httpd.service(8)
  Main PID: 1304 (httpd)
  Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec: 0;CPU usage: 0%"
  Tasks: 213 (limit: 24609)
  Memory: 33.9M
  CPU: 1.180s
  CGroup: /system.slice/httpd.service
          └─1304 /usr/sbin/httpd -DFOREGROUND
             └─1324 /usr/sbin/httpd -DFOREGROUND
                └─1325 /usr/sbin/httpd -DFOREGROUND
                   └─1326 /usr/sbin/httpd -DFOREGROUND
                      └─1327 /usr/sbin/httpd -DFOREGROUND

anp 27 19:46:34 vnkhrustalev.localdomain systemd[1]: Starting The Apache HTTP Server: httpd
anp 27 19:46:36 vnkhrustalev.localdomain systemd[1]: Started The Apache HTTP Server: httpd
anp 27 19:46:36 vnkhrustalev.localdomain httpd[1304]: Server configured, listening on ports 80 and 443
```

Рис. 1: Проверка статуса SeLinux



## Определение контекста безопасности и попытка проверки наличия команды StInfo. +sestatus команды не существует.

```
[vnkhrustalev@vnkhrustalev ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 1304 0.0 0.2 20328 11588 ?
Ss 19:46 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 1324 0.0 0.1 21664 7332 ?
S 19:46 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 1325 0.0 0.3 1669372 15132 ?
Sl 19:46 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 1326 0.0 0.3 1538236 15132 ?
Sl 19:46 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 1327 0.0 0.2 1538236 11044 ?
Sl 19:46 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 vnkhrus+ 3314 0.0 0.0 221
320 2340 pts/0 S+ 20:02 0:00 grep --color=auto httpd
[vnkhrustalev@vnkhrustalev ~]$
```

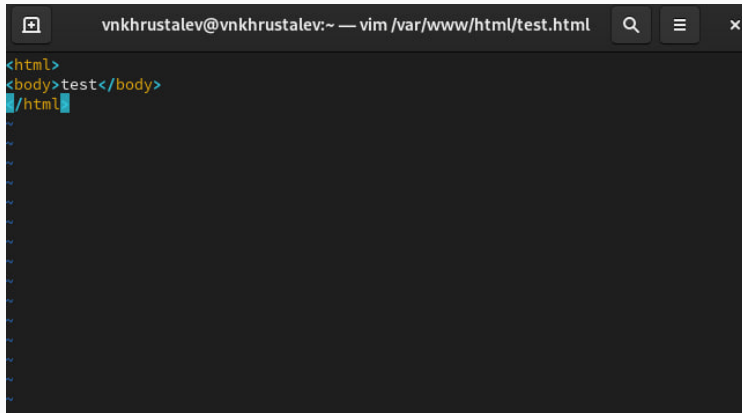
Рис. 3: Просмотр контекста безопасности httpd

```
[vnkhrustalev@vnkhrustalev ~]$ sestatus -b httpd
SELinux status: enabled
SELinuxfs mount: /sys/fs/selinux
SELinux root directory: /etc/selinux
Loaded policy name: targeted
Current mode: enforcing
Mode from config file: enforcing
```

# Определение типов файлов в директориях Apache (файлов сервера)

```
[vnkhrustalev@vnkhrustalev ~]$ ls -lZ /var/www/html  
итого 0  
[vnkhrustalev@vnkhrustalev ~]$
```

**Рис. 6:** Тип файлов и поддиректорий, находящихся в директории /var/www

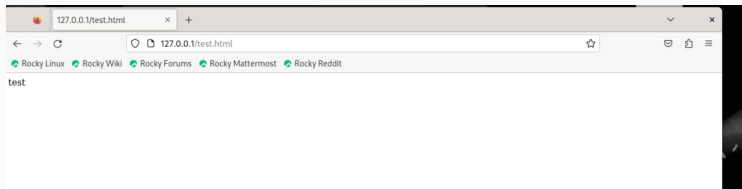


The screenshot shows a vim editor window with the title bar "vnkhrustalev@vnkhrustalev:~ — vim /var/www/html/test.html". The editor content displays an HTML document structure: `<html>` on the first line, `<body>test</body>` on the second line, and `/html` on the third line. The cursor is positioned at the end of the third line. The left margin of the editor shows a series of blue wavy lines, indicating the fold state of the document.

# Создание html файла, проверка его контекста и визуальный просмотр

```
vnkhrustalev@vnkhrustalev ~]$ sudo vim /var/www/html/test.html
vnkhrustalev@vnkhrustalev ~]$ ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 апр 27 2
0:07 test.html
vnkhrustalev@vnkhrustalev ~]$
```

**Рис. 8:** Создание html-файл /var/www/html/test.html



**Рис. 9:** Контекст созданного файла

```
[vnkhrustalev@vnkhrustalev ~]$ man httpd_selinux
Нет справочной страницы для httpd_selinux
```

## Просмотр инфо о команде `httpd_selinux` – она отсутствует

```
[root@vnkhurstalev vnkhurstalev]# chcon -t samba_share_t /var/www/html/test.html
[root@vnkhurstalev vnkhurstalev]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@vnkhurstalev vnkhurstalev]#
```

**Рис. 11:** `man httpd_selinux`

Изменение контекста html файла на любой другой и попытка просмотра. У нас нет доступа. Так же проверим логи.

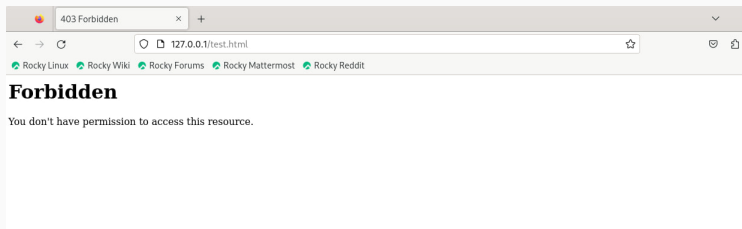
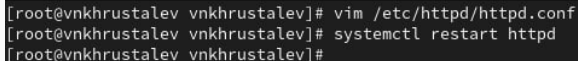


Рис. 12: Измените контекст файла /var/www/html/test.html

```
[root@vnkhurstalev vnkhurstalev]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 апр 27 20:07 /var/www/html/test.html
[root@vnkhurstalev vnkhurstalev]# tail /var/log/messages
Apr 27 20:11:21 vnkhurstalev systemd[1]: Created slice Slice /system/dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged.
Apr 27 20:11:21 vnkhurstalev systemd[1]: Started dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service.
Apr 27 20:11:26 vnkhurstalev setroubleshoot[3920]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/www/html/test.html. Для выполнения всех сообщений SELinux: sealert -l 048ee060-23a3-4270-8f0f-12037443e804
Apr 27 20:11:26 vnkhurstalev setroubleshoot[3920]: SELinux запрещает /usr/sbin/h
```

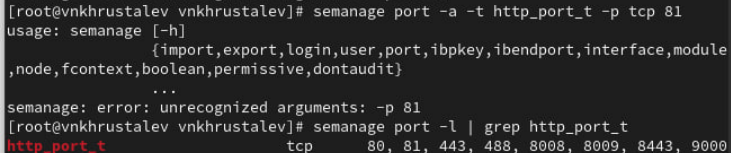


Проведём доп изменения. Изменим прослушиваемый порт сервера на 81 и перезапустим веб-сервер. Ошибок у нас нет, так как я ранее пользовался тут Apache и порт 81 прописал в разрешённые. Поэтому команда добавления в разрешённые тут была излишняя



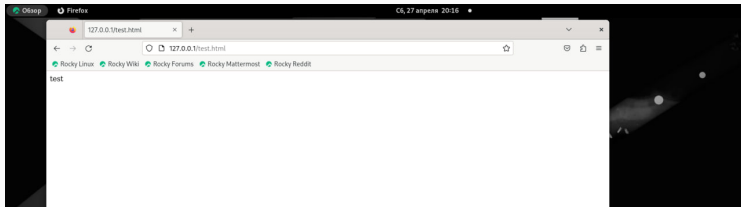
```
[root@vnkhrustalev vnkhrustalev]# vim /etc/httpd/httpd.conf
[root@vnkhrustalev vnkhrustalev]# systemctl restart httpd
[root@vnkhrustalev vnkhrustalev]#
```

**Рис. 15:** Изменение прослушиваемого порта Apache на 81



```
[root@vnkhrustalev vnkhrustalev]# 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@vnkhrustalev vnkhrustalev]# semanage port -l | grep http_port_t
http_port_t      tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
```

**Вернём всё обратно. Проверим что всё отображается. И попытаемся отключить порт 81, но не выйдет так как он уже используется и прописан в другом месте**



**Рис. 18:** Возврат стандарт контекста



## Выводы

---

На данной лабораторной работе мы развили навыки администрирования ОС Linux, получили первое практическое знакомство с технологией SELinux.