

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ПРЕЗЕНТАЦИЯ ПО ЛАБОРАТОРНОЙ РАБОТЕ №6

дисциплина: Информационная безопасность

Преподаватель: Кулябов Дмитрий Сергеевич

Студент: Серенко Данил Сергеевич

Группа: НФИбд-01-19

МОСКВА 2022 г.

---

## Цель работы

Целью данной лабораторной работы является развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux<sup>1</sup>. Проверить работу SELinx на практике совместно с веб-сервером Apache.

---

## Выполнение лабораторной работы

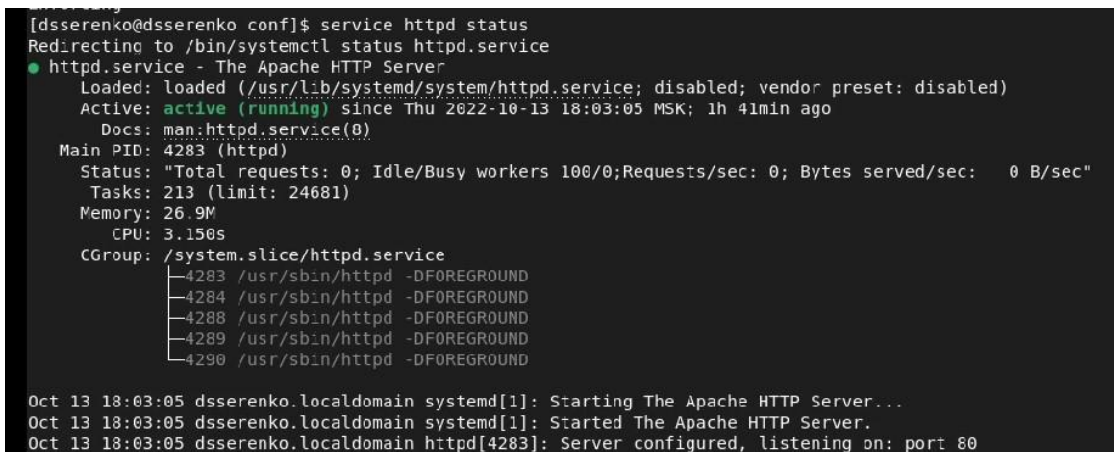
1. Входим в систему с полученными учётными данными. Проверили, что SELinux работает в режиме enforcing политики targeted с помощью команд **getenforce** и **sestatus**.



```
lp' for more information.
rce
s
s
SELinux is mounted: /sys/fs/selinux
SELinux root directory: /etc/selinux
Loaded policy name: targeted
Current mode: enforcing
Mode from config file: enforcing
Policy MLS status: enabled
Policy deny_unknown status: allowed
Memory protection checking: actual (secure)
Max kernel policy version: 33
[dsserenko@dsserenko conf]$ ls
httpd.conf magic
[dsserenko@dsserenko conf]$ getenforce
Enforcing
[dsserenko@dsserenko conf]$ getenforce
Enforcing
```

Выполнение команд *getenforce* и *sestatus*

2. Запустили веб-сервер и обратились к нему с помощью команды: `service httpd status`

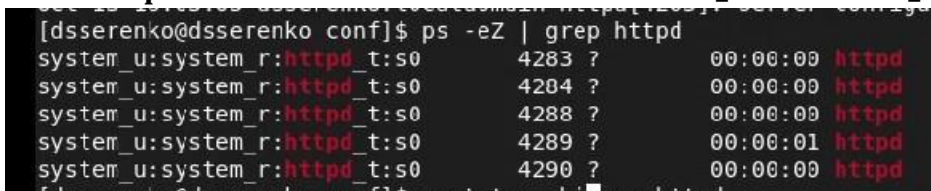


```
[dsserenko@dsserenko conf]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Thu 2022-10-13 18:03:05 MSK; 1h 41min ago
     Docs: man:httpd.service(8)
  Main PID: 4283 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
    Tasks: 213 (limit: 24681)
  Memory: 26.9M
    CPU: 3.150s
   CGroup: /system.slice/httpd.service
           └─4283 /usr/sbin/httpd -DFOREGROUND
             └─4284 /usr/sbin/httpd -DFOREGROUND
               └─4288 /usr/sbin/httpd -DFOREGROUND
                 └─4289 /usr/sbin/httpd -DFOREGROUND
                   └─4290 /usr/sbin/httpd -DFOREGROUND

Oct 13 18:03:05 dsserenko.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 13 18:03:05 dsserenko.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 13 18:03:05 dsserenko.localdomain httpd[4283]: Server configured, listening on: port 80
```

Выполнение команды *status*

3. Найшли веб-сервер Apache в списке процессов с помощью команды `ps auxZ | grep httpd`. Контекст безопасности - `unconfined_u:unconfined_r:unconfined_t`.



```
[dsserenko@dsserenko conf]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0      4283 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      4284 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      4288 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      4289 ?        00:00:01 httpd
system_u:system_r:httpd_t:s0      4290 ?        00:00:00 httpd
```

Выполнение команды *ps auxZ | grep httpd*

4. Посмотрели текущее состояние переключателей SELinux для Apache с помощью команды .

```

httpd_can_network_connect_db off
httpd_can_network_memcache off
httpd_can_network_relay off
httpd_can_sendmail off
httpd_dbus_avahi off
httpd_dbus_sssd off
httpd_dontaudit_search_dirs off
httpd_enable_cgi on
httpd_enable_ftp_server off
httpd_enable_honedirs off
httpd_execmem 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_stickshift off
httpd_serve_cobbler_files off
httpd_setrlimit off
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_qpq off
httpd_use_nfs off
httpd_use_openscryptoki off
httpd_use_openstack off
httpd_use_sasl off
httpd_verify_dns off

```

Выполнение команды `sestatus -ez`

- Определили тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www`.

```

[dsserenko@dsserenko conf]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 15:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 May 16 15:10 html
[dsserenko@dsserenko conf]$

```

6. Создали

от имени суперпользователя html-файл `/var/www/html/test.html` следующего содержания:

```

/var/www/html/test.html
<html>
<body>test</body>
</html>

```

Содержимое файла `test.html`

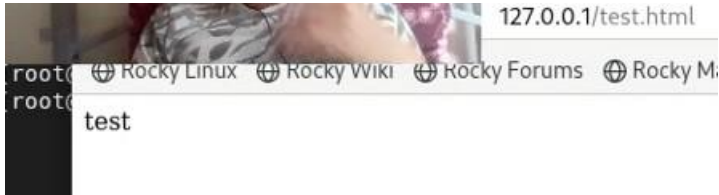
- Проверили контекст созданного файла - `httpd_sys_content_t`.

```
[dsserenko@dsserenko conf]$ ls -lZ /var/www/html/  
total 4  
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Oct 13 19:49 test.html
```

*Контекст файла test.html*

---

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



*Обращение к файлу test.html через веб-сервер*

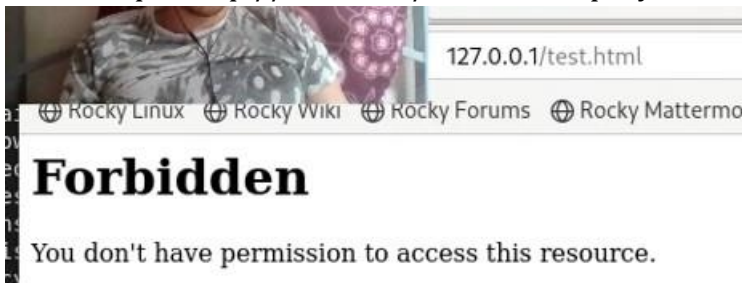
9. Изменили контекст файла И проверили, что контекст поменялся.

```
[dsserenko@dsserenko conf]$ ls -lZ /var/www/html/  
total 4  
-rw-r--r--. 1 root root unconfined_u:object_r:samba_share_t:s0 33 Oct 13 19:49 test.html  
[dsserenko@dsserenko conf]$
```

*Изменение контекста файла /var/www/html/test.html*

---

10. Пробуем ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. В результате получили ошибку.



*Обращение к файлу test.html через веб-сервер после изменения контекста*

11. Попробуем запустить веб-сервер Apache на прослушивание TCP-порта 81. Для этого в файле `/etc/httpd/httpd.conf` находим строчку `Listen 80` и заменяем её на `Listen 81`.

```
#  
#Listen 12.34.56.78:80  
Listen 81
```

*Запуск веб-сервера Apache на прослушивание TCP-порта 81*

---

12. Выполним перезапуск веб-сервера Apache. Произошёл сбой? Нет.  
13. Выполним команду `semanage port -a -t http_port_t -p tcp 81`. Вылетает `ValueError` в связи с тем, что порт уже определен. После этого проверим список портов

командой **semanage port -l | grep http\_port\_t** и убедились, что порт 81 появился в списке.

```
[dsserenko@dsserenko conf]$ sudo semanage port -l | grep 81
http_port_t tcp 1782, 2207, 2208, 8290, 8292, 9100, 9101, 9102, 9220, 9221, 9222, 9280, 9281, 9282, 9290, 9291, 50000, 50002
http_cache_port_t tcp 8080, 8118, 8123, 10001-10010
http_port_t tcp 80, 81, 443, 488, 8008, 8009, 8443, 9000
intermapper_port_t tcp 8181
prosody_port_t tcp 5280-5281
pulp_port_t tcp 24116, 24117
puppet_port_t tcp 8140
radacct_port_t tcp 1646, 1813
radacct_port_t udp 1646, 1813
radius_port_t tcp 1645, 1812, 18120-18121
radius_port_t udp 1645, 1812, 18120-18121
rkt_port_t tcp 18112
statsd_port_t udp 8125
transproxy_port_t tcp 8081
varnishd_port_t tcp 6081-6082
zookeeper_client_port_t tcp 2181
```

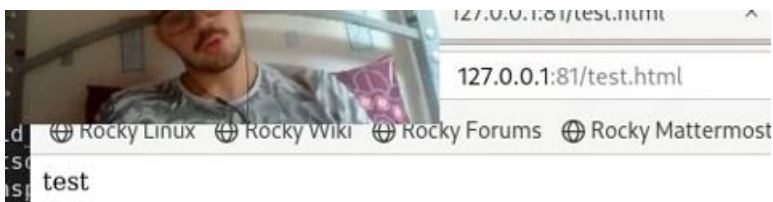
*Проверка установления 81 порта tcp*

- 
14. Вернули контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`: **chcon -t httpd\_sys\_content\_t /var/www/html/test.html**

```
[dsserenko@dsserenko conf]$ sudo chcon -t httpd_sys_content_t /var/www/html/test.html
[dsserenko@dsserenko conf]$
```

*Возвращение контекста `httpd_sys_content_t` к файлу `test.html`*

После этого пробуем получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. В результате увидели содержимое файла — слово «test».



*Обращение к файлу `test.html` через веб-сервер*

- 
15. Исправим обратно конфигурационный файл `apache`, вернув `Listen 80`.

```
#
#Listen 12.34.56.78:80
Listen 80
```

*Исправление конфигурационного файла `apache`*

16. Удалим привязку `http_port_t` к 81 порту: **semanage port -d -t http\_port\_t -p tcp 81** и проверим, что порт 81 удалён. Данная команда не была выполнена.

```
[dsserenko@dsserenko conf]$ sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
```

*Удаление привязки `http_port_t` к 81 порту*

17. Удалим файл `/var/www/html/test.html`: **rm /var/www/html/test.html**.

```
[dsserenko@dsserenko conf]$ sudo rm /var/www/html/test.html
[dsserenko@dsserenko conf]$ ls /var/www/html/
[dsserenko@dsserenko conf]$ ls
httpd.conf  magic
```

*Удаление файла test.html*

---

## Вывод

В ходе выполнения лабораторной работы мы развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux<sup>1</sup>. Проверили работу SELinx на практике совместно с веб-сервером Apache.

---