

# Лабораторная работа № 6

---

Юрченко Артём Алексеевич

2023, Москва

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux<sup>1</sup>. Проверить работу SELinux на практике совместно с веб-сервером Apache.

1. Настроить и запустить сервер Apache.
2. Исследовать влияние параметров сервера на его работу.

Войдем в систему с полученными учётными данными и убедимся, что SELinux работает в режиме enforcing политики targeted.

```
[root@info-sec temau]# getenforce
Enforcing
[root@info-sec temau]# sestatus
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
Policy MLS status:             enabled
Policy deny_unknown status:    allowed
Memory protection checking:    actual (secure)
Max kernel policy version:     33
[root@info-sec temau]#
```

**Рис. 1:** Конфигурация SELinux

Обратимся с помощью браузера к веб-серверу, запущенному на нашем компьютере, и убедимся, что последний работает.

```
[temau@info-sec ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[temau@info-sec ~]$ 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; preset: disabled)
   Active: active (running) since Sat 2023-10-14 14:53:17 MSK; 7s ago
     Docs: man:httpd.service(8)
   Main PID: 42011 (httpd)
   Status: "Started, listening on: port 80"
     Tasks: 213 (limit: 44971)
    Memory: 35.5M
       CPU: 38ms
    CGroup: /system.slice/httpd.service
           └─42011 /usr/sbin/httpd -DFOREGROUND
             └─42018 /usr/sbin/httpd -DFOREGROUND
               └─42019 /usr/sbin/httpd -DFOREGROUND
                 └─42020 /usr/sbin/httpd -DFOREGROUND
                   └─42021 /usr/sbin/httpd -DFOREGROUND

окт 14 14:53:17 info-sec systemd[1]: Starting The Apache HTTP Server...
окт 14 14:53:17 info-sec httpd[42011]: Server configured, listening on: port 80
окт 14 14:53:17 info-sec systemd[1]: Started The Apache HTTP Server.
lines 1-19/19 (END)
```

Рис. 2: Обращение к веб-серверу

Найдем веб-сервер Apache в списке процессов, определим его контекст безопасности.

```
temau@info-sec ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 42011 0.0 0.1 20116 11376 ?
Ss 14:53 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42018 0.0 0.1 21600 7272 ?
S 14:53 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42019 0.0 0.2 2324556 15020 ?
Sl 14:53 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42020 0.0 0.2 2521228 17072 ?
Sl 14:53 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42021 0.0 0.2 2324556 15020 ?
Sl 14:53 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 temau 42510 0.0 0.0 22182
1 2336 pts/0 S+ 14:54 0:00 grep --color=auto httpd
temau@info-sec ~]$
```

Рис. 3: Контекст безопасности веб-сервера Apache

Посмотрим текущее состояние переключателей SELinux для Apache.

```

httpd_can_network_connect_cobbler      off
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_homedirs                  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_gpg                          off
httpd_use_nfs                          off
httpd_use_openscryptoki                 off
httpd_use_osticket                     off
httpd_use_sasl                         off
httpd_verify_dns                       off
[temau@info-sec ~]$

```

Посмотрим статистику по политике с помощью команды seinfo.

```
[temau@info-sec ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow
Classes:                 135
Sensitivities:           1
Types:                   5100
Users:                   8
Booleans:                353
Allow:                   65008
Auditallow:              170
Type_trans:              265344
Type_member:             35
Role_allow:              38
Constraints:             70
MLS Constrain:           72
Permissives:             2
Defaults:                7
Allowxperm:              0
Auditallowxperm:         0
Ibendportcon:            0
Initial SIDs:            27
Genfscon:                109
Netifcon:                0
Permissions:             457
Categories:             1024
Attributes:              258
Roles:                   14
Cond. Expr.:            384
Neverallow:              0
Dontaudit:               8572
Type_change:             87
Range_trans:             6164
Role_trans:              420
Validatetrans:           0
MLS Val. Tran:           0
Polcap:                  6
Typebounds:              0
Neverallowxperm:         0
Dontauditxperm:          0
Ibpkeycon:               0
Fs_use:                  35
Portcon:                 660
Nodecon:                 0
```

Рис. 5: Статистика по политике

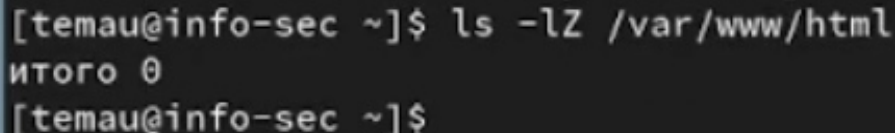


Определим тип файлов и поддиректорий, находящихся в директории /var/www.

```
[temau@info-sec ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая
16 23:21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 мая
16 23:21 html
```

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

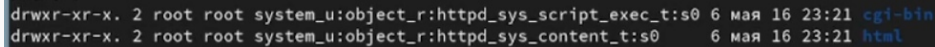
Определим тип файлов, находящихся в директории /var/www/html.



```
[temau@info-sec ~]$ ls -lZ /var/www/html
итого 0
[temau@info-sec ~]$
```

**Рис. 7:** Тип файлов, находящихся в директории /var/www/html

Определим круг пользователей, которым разрешено создание файлов в директории `/var/www/html`.



```
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 16 23:21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 мая 16 23:21 html
```

**Рис. 8:** Круг пользователей, которым разрешено создание файлов в директории `/var/www/html`

Создадим от имени суперпользователя html-файл /var/www/html/test.html.

A terminal window with a dark background. The prompt is [root@info-sec temaui]#. The command touch /var/www/html/test.html is entered. The prompt is repeated on the next line with a cursor after the hash.

```
[root@info-sec temaui]# touch /var/www/html/test.html
[root@info-sec temaui]#
```

**Рис. 9:** Создание файла /var/www/html/test.html

Заполним его следующим содержимым:

```
<html>
```

```
<body>test</body>
```

```
</html>
```

Проверим контекст созданного нами файла.

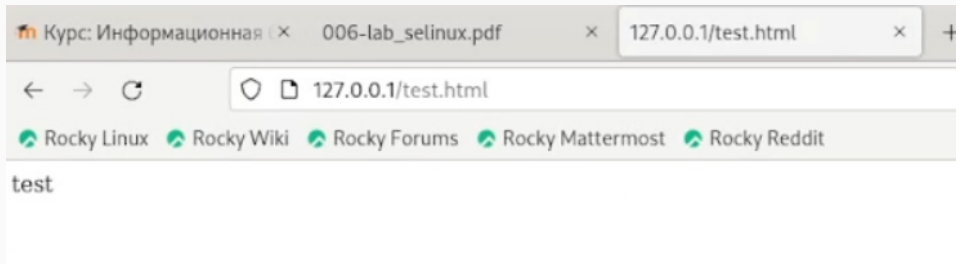


```
[root@info-sec temaui]# ls -lZ /var/www/html
итого 0
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 0 окт 14 14:56 test.html
[root@info-sec temaui]#
```

**Рис. 10:** Работа с параметрами readfile

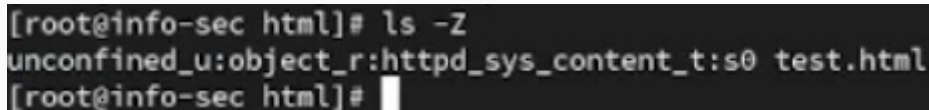
Как видим по умолчанию присваивается контекст  
unconfined\_u:object\_r:httpd\_sys\_content\_t:s0

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



**Рис. 11:** Файл `test.html` в браузере

Изучим справку `man httpd_selinux` и выясним, какие контексты файлов определены для `httpd`. Сопоставим их с типом файла `test.html`.



```
[root@info-sec html]# ls -Z
unconfined_u:object_r:httpd_sys_content_t:s0 test.html
[root@info-sec html]#
```

**Рис. 12:** Вызов справки и тип файла `test.html`

Изменим контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t`.

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

**Рис. 13:** Изменение контекста



Попробуем ещё раз получить доступ к файлу через веб-сервер.

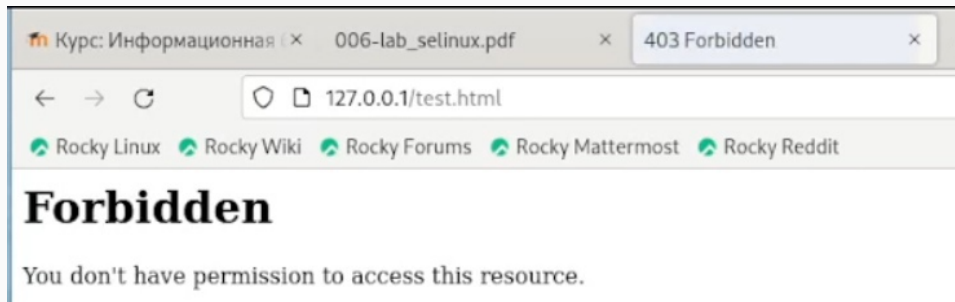


Рис. 14: Файл test.html в браузере после изменения контекста

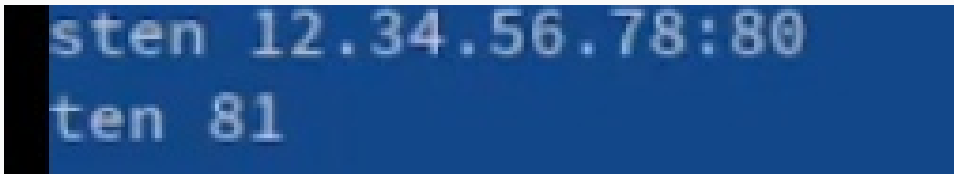
Просмотрим log-файлы веб-сервера Apache и системный лог-файл.

```
[root@info-sec html]# ls -l
итого 4
-rw-r--r--. 1 root root 33 окт 14 14:59 test.html
[root@info-sec html]# tail /var/log/messages
```

**Рис. 15:** Содержимое логов

Как видим, нам не удалось получить доступ к файлу как раз из-за измененного контекста.

Попробуем запустить веб-сервер Apache на прослушивание TCP-порта 81.

A terminal window with a dark blue background and white text. The text shows the configuration of the Listen directive in the httpd.conf file, changing the port from 80 to 81.

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

**Рис. 16:** Изменение содержимого файла `/etc/httpd/httpd.conf`

Выполним перезапуск веб-сервера. Сбоя не произошло.

```
[root@info-sec 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; preset: disabled)
   Active: active (running) since Sat 2023-10-14 15:05:22 MSK; 2min 15s ago
     Docs: man:httpd.service(8)
  Main PID: 43696 (httpd)
    Status: "Total requests: 3; Idle/Busy workers 100/0; Requests/sec: 0.0233; Bytes served/s: 0.0000"
    Tasks: 213 (limit: 44971)
   Memory: 35.4M
      CPU: 92ms
  CGroup: /system.slice/httpd.service
          └─43696 /usr/sbin/httpd -DFOREGROUND
            └─43697 /usr/sbin/httpd -DFOREGROUND
              └─43698 /usr/sbin/httpd -DFOREGROUND
                └─43699 /usr/sbin/httpd -DFOREGROUND
                  └─43701 /usr/sbin/httpd -DFOREGROUND

OCT 14 15:05:22 info-sec systemd[1]: Starting The Apache HTTP Server...
OCT 14 15:05:22 info-sec systemd[1]: Started The Apache HTTP Server.
OCT 14 15:05:22 info-sec httpd[43696]: Server configured, listening on: port 81
```

Рис. 17: Перезапуск веб-сервера

## Проанализируем лог-файлы.

```
[root@user conf]# tail /var/log/messages
Oct 12 14:43:54 user systemd[1]: Started Fingerprint Authentication Daemon.
Oct 12 14:43:58 user NetworkManager[927]: <info> [1697111038.6420] agent-manager: agent[ef6fe3c18efc9fb5,:1.71/org.gnome.Shell.NetworkAgent/1000]: agent registered
Oct 12 14:44:24 user systemd[1]: fprintd.service: Deactivated successfully.
Oct 12 14:44:52 user systemd[1]: Stopping The Apache HTTP Server...
Oct 12 14:44:53 user systemd[1]: httpd.service: Deactivated successfully.
Oct 12 14:44:53 user systemd[1]: Stopped The Apache HTTP Server.
Oct 12 14:44:53 user systemd[1]: httpd.service: Consumed 12.225s CPU time.
Oct 12 14:44:58 user systemd[1]: Starting The Apache HTTP Server...
Oct 12 14:44:58 user systemd[1]: Started The Apache HTTP Server.
Oct 12 14:44:58 user httpd[42774]: Server configured, listening on: port 81
```

**Рис. 18:** Лог-файл `tail -nl /var/log/messages`

Выполним команду `semanage port -a -t http_port_t -p tcp 81`. После этого проверим список портов командой `semanage port -l | grep http_port_t`. Убедимся, что порт 81 есть в списке.

```
[root@info-sec conf]# 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@info-sec conf]# 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
[root@info-sec conf]#
```

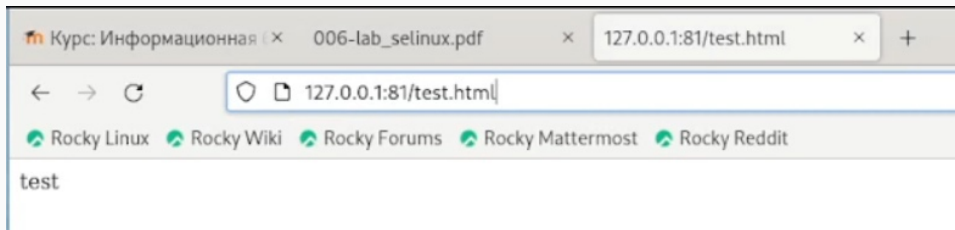
**Рис. 19:** Попытка добавления порта 81 в список и вывод списка допустимых портов

Попробуем запустить веб-сервер Apache ещё раз.

```
[root@info-sec conf]# 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
[root@info-sec 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; preset: disabled)
   Active: active (running) since Sat 2023-10-14 15:05:22 MSK; 2min 15s ago
     Docs: man:httpd.service(8)
  Main PID: 43696 (httpd)
    Status: "Total requests: 3; Idle/Busy workers 100/0; Requests/sec: 0.0233; Bytes served/s"
     Tasks: 213 (limit: 44971)
    Memory: 35.4M
       CPU: 92ms
    CGroup: /system.slice/httpd.service
            └─43696 /usr/sbin/httpd -DFOREGROUND
              └─43697 /usr/sbin/httpd -DFOREGROUND
                └─43698 /usr/sbin/httpd -DFOREGROUND
                  └─43699 /usr/sbin/httpd -DFOREGROUND
                    └─43701 /usr/sbin/httpd -DFOREGROUND

окт 14 15:05:22 info-sec systemd[1]: Starting The Apache HTTP Server...
окт 14 15:05:22 info-sec systemd[1]: Started The Apache HTTP Server.
окт 14 15:05:22 info-sec httpd[43696]: Server configured, listening on: port 81
lines 1-19/19 (END)
```

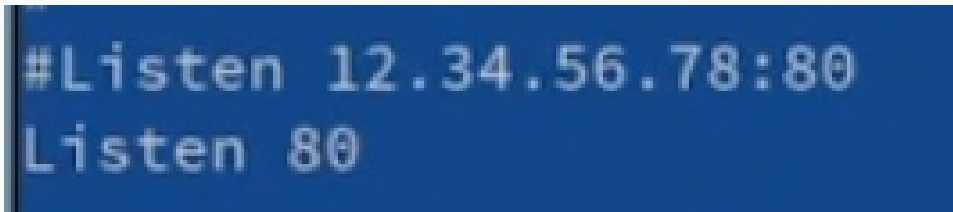
Вернем контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`. Попробуем получить доступ к файлу через веб-сервер.



**Рис. 21:** Файл `test.html` в браузере после возвращения контекста



Исправим обратно конфигурационный файл apache, вернув Listen 80.

A screenshot of a text editor showing two lines of configuration code. The first line is commented out with a hash symbol, and the second line is active.

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

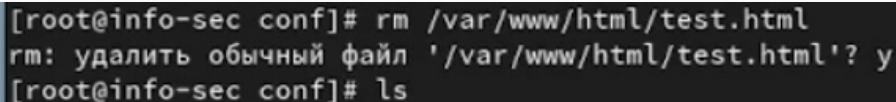
**Рис. 22:** Параметр Listen после возвращения значения

Попробуем удалить привязку http\_port\_t к 81. Удаление невозможно.

```
[root@info-sec conf]# semanage port -d -t http_port_t -p tcp 81  
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален  
[root@info-sec conf]#
```

**Рис. 23:** Попытка удаления привязки к порту 81

Удалим файл /var/www/html/test.html.

A terminal window with a dark background and light gray text. The prompt is [root@info-sec conf]#. The first command is rm /var/www/html/test.html. The second line shows the confirmation prompt rm: удалить обычный файл '/var/www/html/test.html'? y. The third line shows the prompt [root@info-sec conf]# followed by the command ls.

```
[root@info-sec conf]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@info-sec conf]# ls
```

**Рис. 24:** Удаление файла /var/www/html/test.html

В рамках данной лабораторной работы были развиты навыки администрирования ОС Linux. Получено первое практическое знакомство с технологией SELinux<sup>1</sup>. Проверена работа SELinux на практике совместно с веб-сервером Apache.