

# Отчет по лабораторной работе 6

Дисциплина: Информационная безопасность

---

Дяченко Злата Константиновна, НФИбд-03-18

Данная лабораторная работа выполнялась мной для приобретения практических навыков администрирования ОС Linux и знакомства с работой SELinux.

## Цель выполнения лабораторной работы

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

# Задачи выполнения лабораторной работы

Войти в систему и убедиться, что SELinux работает в режиме enforcing политики targeted. Обратиться с помощью браузера к веб-серверу и запустить его. Найти веб-сервер Apache в списке процессов, определить его контекст безопасности (рис. 1)

```
[zkdyachenko@zkdyachenko ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 4381 0.0 0.4 224084 5008 ? Ss 13:18 0:00 /usr/sbin/httpd
-DFOREGROUND
system_u:system_r:httpd_t:s0 apache 4386 0.0 0.3 226168 3092 ? S 13:18 0:00 /usr/sbin/httpd
-DFOREGROUND
system_u:system_r:httpd_t:s0 apache 4387 0.0 0.3 226168 3092 ? S 13:18 0:00 /usr/sbin/httpd
-DFOREGROUND
system_u:system_r:httpd_t:s0 apache 4388 0.0 0.3 226168 3092 ? S 13:18 0:00 /usr/sbin/httpd
-DFOREGROUND
system_u:system_r:httpd_t:s0 apache 4389 0.0 0.3 226168 3092 ? S 13:18 0:00 /usr/sbin/httpd
-DFOREGROUND
system_u:system_r:httpd_t:s0 apache 4390 0.0 0.3 226168 3092 ? S 13:18 0:00 /usr/sbin/httpd
-DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 zkdyach+ 4509 0.0 0.0 112832 968 pts/0 S+ 13:22 0:00 gre
p --color=auto httpd
```

Figure 1: Список процессов

# Задачи выполнения лабораторной работы

Посмотреть текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd` (рис. 2).

```
izkdyachenko@zkdyaachenko ~]$ sestatus -b | grep httpd
httpd_anon_write off
httpd_builtin_scripting on
httpd_can_check_spam off
httpd_can_connect_ftp off
httpd_can_connect_ldap off
httpd_can_connect_mythtv off
httpd_can_connect_zabbix off
httpd_can_network_connect off
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_avaahi 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 on
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_openstack off
httpd_use_sasl off
httpd_verify_dns off
izkdyachenko@zkdyaachenko ~$
```

**Figure 2:** Состояния переключателей SELinux для Apache

# Задачи выполнения лабораторной работы

Посмотреть статистику по политике с помощью команды `seinfo` (рис. 3).

```
[zkdyachenko@zkdyachenko ~]$ seinfo

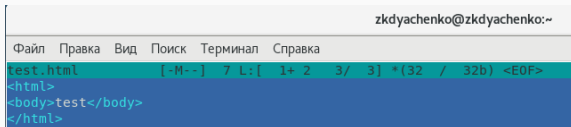
Statistics for policy file: /sys/fs/selinux/policy
Policy Version & Type: v.31 (binary, mls)

Classes:          130      Permissions:        272
Sensitivities:    1        Categories:        1024
Types:            4793     Attributes:         253
Users:            8        Roles:              14
Booleans:         316     Cond. Expr.:       362
Allow:            107834   Neverallow:         0
Auditallow:       158     Dontaudit:          10022
Type_trans:       18153   Type_change:        74
Type_member:      35      Role_allow:         37
Role_trans:       414     Range_trans:        5899
Constraints:      143     Validatetrans:      0
Initial SIDs:     27      Fs_use:             32
Genfscon:         103     Portcon:            614
Netifcon:         0       Nodecon:            0
Permissives:      0       Polcap:             5
```

**Figure 3:** `seinfo`

# Задачи выполнения лабораторной работы

Создать от имени суперпользователя html-файл /var/www/html/test.html (рис. 4).



```
zkdyachenko@zkdyachenko:~
Файл  Правка  Вид  Поиск  Терминал  Справка
test.html  [-M- -]  7 L: [ 1+ 2 3/ 3] *(32 / 32b) <EOF>
<html>
<body>test</body>
</html>
```

**Figure 4:** Содержание файла test.html

Проверить контекст созданного файла (рис. 5).

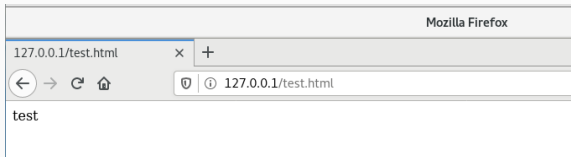
```
[zkdyachenko@zkdyachenko ~]$ ls -lZ /var/www/html  
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
```

**Figure 5:** Контекст файла



# Задачи выполнения лабораторной работы

Обратиться к файлу через веб-сервер (рис. 6).



**Figure 6:** Отображение файла

Изменить контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t`, к которому процесс `httpd` не имеет доступа. Проверить, что контекст поменялся (рис. 7).

```
[zkdyachenko@zkdyachenko ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[sudo] пароль для zkdyachenko:
[zkdyachenko@zkdyachenko ~]$ ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[zkdyachenko@zkdyachenko ~]$ █
```

**Figure 7:** Изменение контекста файла

# Задачи выполнения лабораторной работы

Попробовать ещё раз получить доступ к файлу через веб-сервер (рис. 8).

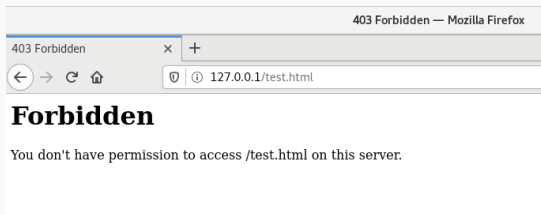


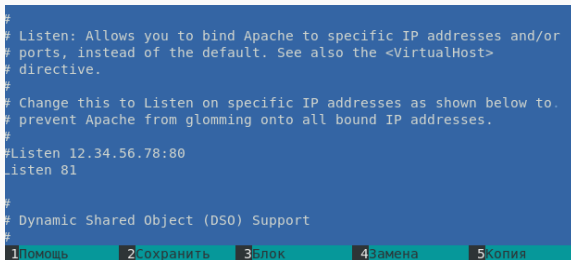
Figure 8: Ошибка

Просмотреть лог-файл `tail /var/log/messages` и  
`/var/log/audit/audit.log`

# Задачи выполнения лабораторной работы

Попробовать запустить веб-сервер Apache на прослушивание TCP-порта 81 (рис. 9).

```
#  
# Listen: Allows you to bind Apache to specific IP addresses and/or  
# ports, instead of the default. See also the <VirtualHost>  
# directive.  
#  
# Change this to Listen on specific IP addresses as shown below to  
# prevent Apache from glomming onto all bound IP addresses.  
#  
#Listen 12.34.56.78:80  
Listen 81  
#  
# Dynamic Shared Object (DSO) Support  
#
```

The image shows a screenshot of a text editor window displaying an Apache configuration file. The text is white on a dark blue background. At the bottom of the window, there is a toolbar with five buttons: '1 Помощь' (Help), '2 Сохранить' (Save), '3 Блок' (Block), '4 Замена' (Replace), and '5 Копия' (Copy). The buttons are numbered 1 through 5, corresponding to the steps in the figure caption.

1 Помощь	2 Сохранить	3 Блок	4 Замена	5 Копия
----------	-------------	--------	----------	---------

**Figure 9:** Замена строчки в файле

Выполнить перезапуск веб-сервера Apache (рис. 10).

```
[zkdyachenko@zkdyachenko ~]$ sudo mcedit /etc/httpd/conf/httpd.conf  
[zkdyachenko@zkdyachenko ~]$ sudo service httpd restart  
Redirecting to /bin/systemctl restart httpd.service  
[zkdyachenko@zkdyachenko ~]$ █
```

**Figure 10:** Перезапуск веб-сервера Apache

Выполнить команду `semanage port -a -t http_port_t -p tcp 81`, после этого проверить список портов (рис. 11).

```
[zkdyachenko@zkdyachenko ~]$ sudo semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[zkdyachenko@zkdyachenko ~]$ sudo 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
[zkdyachenko@zkdyachenko ~]$
```

**Figure 11:** Список портов

Попробовать запустить веб-сервер Apache ещё раз (рис. 12).

```
[zkdyachenko@zkdyachenko ~]$ sudo 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
[zkdyachenko@zkdyachenko ~]$ sudo service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[zkdyachenko@zkdyachenko ~]$ 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 Cp 2021-11-24 14:55:26 MSK; 17s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 12664 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=0/SUCCESS)
 Main PID: 12672 (httpd)
    Status: "Total requests: 0; Current requests/sec: 0; Current traffic:  0 B/sec"
      Tasks: 6
   CGroup: /system.slice/httpd.service
           └─12672 /usr/sbin/httpd -DFOREGROUND
             └─12673 /usr/sbin/httpd -DFOREGROUND
               └─12674 /usr/sbin/httpd -DFOREGROUND
                 └─12675 /usr/sbin/httpd -DFOREGROUND
                   └─12676 /usr/sbin/httpd -DFOREGROUND
                     └─12677 /usr/sbin/httpd -DFOREGROUND

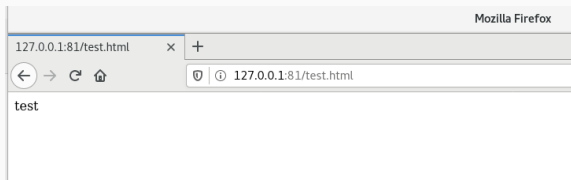
ноя 24 14:55:26 zkdyachenko.localdomain systemd[1]: Stopped The Apache HTTP Server.
ноя 24 14:55:26 zkdyachenko.localdomain systemd[1]: Starting The Apache HTTP Server...
ноя 24 14:55:26 zkdyachenko.localdomain systemd[1]: Started The Apache HTTP Server.
```

**Figure 12:** Перезапуск веб-сервера Apache



# Задачи выполнения лабораторной работы

Вернуть контекст `httpd_sys_content_t` к файлу `/var/www/html/ test.html`. Попробовать получить доступ к файлу через веб-сервер (рис. 13).



**Figure 13:** Получение доступа к файлу через веб-браузер

Исправить обратно конфигурационный файл apache, вернув Listen 80 (рис. 14).

```
#  
# Listen: Allows you to bind Apache to specific IP addresses and/or  
# ports, instead of the default. See also the <VirtualHost>  
# directive.  
#  
# Change this to Listen on specific IP addresses as shown below to  
# prevent Apache from glomming onto all bound IP addresses.  
#  
#Listen 12.34.56.78:80  
Listen 80
```

**Figure 14:** Исправление файла

Попытаться удалить привязку `http_port_t` к 81 порту. Удалить файл `/var/www/html/test.html` (рис. 15).

```
[zkdyachenko@zkdyachenko ~]$ sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[zkdyachenko@zkdyachenko ~]$ sudo rm /var/www/html/test.html
[zkdyachenko@zkdyachenko ~]$ sudo ls /var/www/html
[zkdyachenko@zkdyachenko ~]$
```

**Figure 15:** Попытка удалить привязку `http_port_t` к 81 порту и удаление файла

В результате выполнения работы я развила навыки администрирования ОС Linux, получила первое практическое знакомство с технологией SELinux. Также я проверила работу SELinux на практике совместно с веб-сервером Apache.