

# Цель работы

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

# Задание


Выполнить задания из лабораторной работы и проанализировать полученные результаты.

# Теоретическое введение

Для выполнения данной лабораторной нет специальной теории. Необходимы общие знания в области компьютерных наук.

# Выполнение лабораторной работы

Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.



The screenshot shows a terminal window with a dark background. At the top, there are three tabs: 'Обзор' (Overview) with a green icon, 'Терминал' (Terminal) with a terminal icon, and a timestamp 'Сб, 15 октября 10:42'. Below the tabs is a header bar with a user icon and the text 'vyzhukova@localhost:~'. The terminal content shows the following commands and output:

```
[vyzhukova@user ~]$ getenforce
Enforcing
[vyzhukova@user ~]$ 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
[vyzhukova@user ~]$
```

Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: `service httpd status` или `/etc/rc.d/init.d/httpd status`. Если не работает, запустите его так же, но с параметром `start`.

```

Redirecting to /bin/systemctl start httpd.service
[root@user ~]# 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 pr>
   Active: active (running) since Sat 2022-10-15 11:54:16 MSK; 8s ago
     Docs: man:httpd.service(8)
  Main PID: 108160 (httpd)
    Status: "Started, listening on: port 80"
     Tasks: 213 (limit: 12210)
    Memory: 15.0M
       CPU: 38ms
    CGroup: /system.slice/httpd.service
            └─108160 /usr/sbin/httpd -DFOREGROUND
              └─108161 /usr/sbin/httpd -DFOREGROUND
                └─108162 /usr/sbin/httpd -DFOREGROUND
                  └─108163 /usr/sbin/httpd -DFOREGROUND
                    └─108164 /usr/sbin/httpd -DFOREGROUND

окт 15 11:54:15 user.localhost systemd[1]: Starting The Apache HTTP Server...
окт 15 11:54:16 user.localhost httpd[108160]: AH00558: httpd: Could not reliabl>
окт 15 11:54:16 user.localhost systemd[1]: Started The Apache HTTP Server.
окт 15 11:54:16 user.localhost httpd[108160]: Server configured, listening on: >
lines 1-20/20 (END)

```

Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду `ps auxZ | grep httpd` или `ps -eZ | grep httpd`

```

[root@user ~]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 108160 0.0 0.5 20092 11508 ?
Ss 11:54 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 108161 0.0 0.3 21416 7244 ?
S 11:54 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 108162 0.0 0.4 1079216 8816 ?
Sl 11:54 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 108163 0.0 0.4 1079216 8816 ?
Sl 11:54 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 108164 0.0 0.4 1210352 8816 ?
Sl 11:54 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 108384 0.0 0.1 22169
2 2436 pts/0 S+ 11:55 0:00 grep --color=auto httpd
[root@user ~]#

```

Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd` Обратите внимание, что многие из них находятся в положении «off»

```

[root@user ~]# 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 15
:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 мая 16 15
:10 html
[root@user ~]#

```

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

```
Without options, show SELinux status.
[root@user ~]# 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_manage_courier_spool 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_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
```

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

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

```
[root@user ~]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version: 33 (MLS enabled)
Target Policy: selinux
Handle unknown classes: allow
Classes: 133 Permissions: 454
Sensitivities: 1 Categories: 1024
Types: 5002 Attributes: 254
Users: 8 Roles: 14
Booleans: 347 Cond. Expr.: 381
Allow: 63996 Neverallow: 0
Auditallow: 168 Dontaudit: 8417
Type_trans: 258486 Type_change: 87
Type_member: 35 Range_trans: 5960
Role_allow: 38 Role_trans: 420
Constraints: 72 Validatetrans: 0
MLS Constrain: 72 MLS Val. Tran: 0
Permissives: 0 Polcap: 5
Defaults: 7 Typebounds: 0
Allowxperm: 0 Neverallowxperm: 0
Auditallowxperm: 0 Dontauditxperm: 0
Ibendportcon: 0 Ibkeycon: 0
Initial SIDs: 27 Fs_use: 33
```

Проверьте контекст созданного вами файла.

```

[root@user ~]# 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 15
:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 мая 16 15
:10 html
[root@user ~]#

```

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

```

[root@user ~]# ls -lZ /var/www/html
итого 0

```

Проверить контекст файла можно командой `ls -Z`. `ls -Z /var/www/html/test.html`

```

[root@user ~]# cd /var/www/html
[root@user html]# touch test.html
[root@user html]# nono test.html
bash: nono: command not found...
[root@user html]# vim test.html
[root@user html]# cat test.html
<html>
<body>test</body>
</html>
[root@user html]#

```

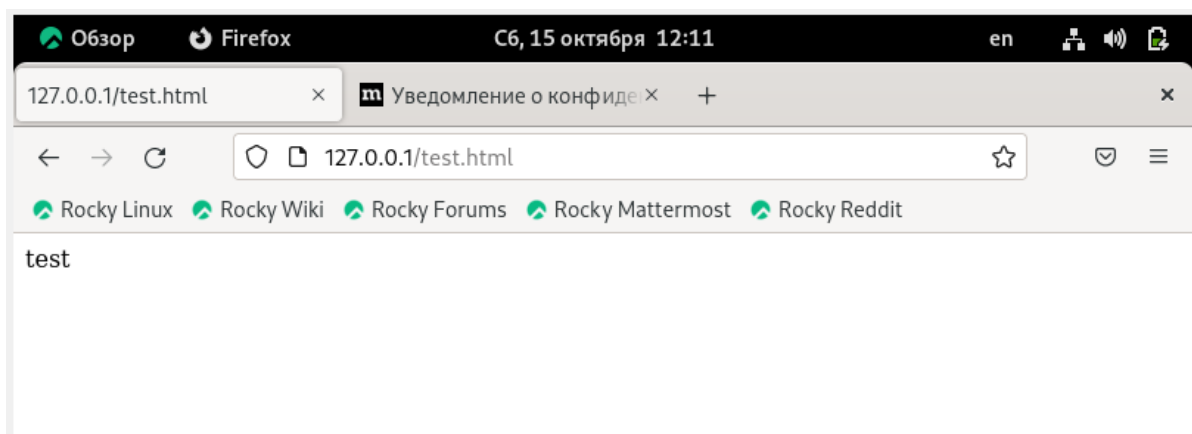
Измените контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на любой другой, к которому процесс `httpd` не должен иметь доступа, например, на `samba_share_t`: `chcon -t samba_share_t /var/www/html/test.html` `ls -Z /var/www/html/test.html`

```

[root@user html]# ps auxZ | grep test.html
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 108689 0.0 0.1 22182
8 2380 pts/0 S+ 12:09 0:00 grep --color=auto test.html
[root@user html]#

```

Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>



Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? `ls -l /var/www/html/test.html` Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный log-файл: `tail /var/log/messages` Если в системе окажутся запущенными процессы `setroubleshootd` и `audtd`, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле `/var/log/audit/audit.log`. Проверьте это утверждение самостоятельно.

```

нет справочной страницы для httpd_selinux
[root@user html]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@user html]#

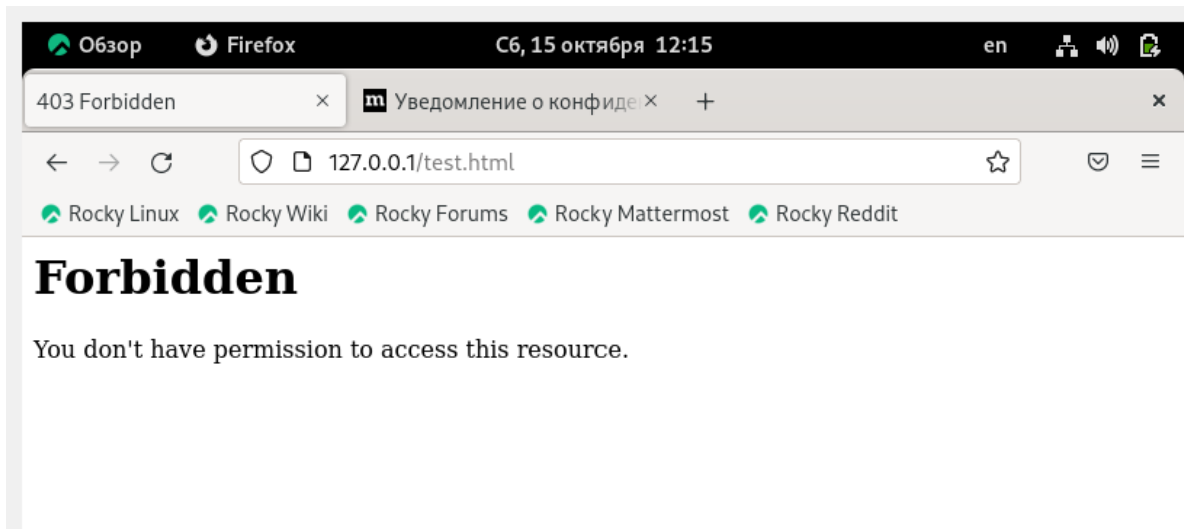
```

```

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

```

Попробуйте 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 найдите строчку Listen 80 и замените её на Listen 81.



```

unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@user html]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 окт 15 12:07 /var/www/html/test.html
[root@user html]# tail /var/log/messages
Oct 15 12:15:46 user systemd[1]: Started dbus-:1.10-org.fedoraproject.Setroubles
hootPrivileged@0.service.
Oct 15 12:15:47 user setroubleshoot[109065]: SELinux запрещает /usr/sbin/httpd д
оступ getattr к файл /var/www/html/test.html. Для выполнения всех сообщений SELi
nux: sealert -l dd1386df-4eaf-4542-ace0-ebb89bbbed0e2
Oct 15 12:15:47 user setroubleshoot[109065]: SELinux запрещает /usr/sbin/httpd д
оступ getattr к файл /var/www/html/test.html.#012#012***** Модуль restorecon пр
едлагает (точность 92.2) *****#012#012Если вы хотите исправ
ить метку.$TARGETЗнак _PATH по умолчанию должен быть httpd_sys_content_t#012То в
ы можете запустить restorecon. Возможно, попытка доступа была остановлена из-за
недостаточных разрешений для доступа к родительскому каталогу, и в этом случае п
опытайтесь соответствующим образом изменить следующую команду.#012Сделать#012# /
sbin/restorecon -v /var/www/html/test.html#012#012***** Модуль public_content п
редлагает (точность 7.83) *****#012#012Если вы хотите лечить te
st.html как общедоступный контент#012То необходимо изменить метку test.html с pu
blic_content_t на public_content_rw_t.#012Сделать#012# semanage fcontext -a -t p
ublic_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test
.html'#012#012***** Модуль catchall предлагает (точность 1.41) *****
*****#012#012Если вы считаете, что httpd должно быть разрешено getattr до

```

Сервер успешно запустился на 81 порту.

Выполните команду `semanage port -a -t http_port_t -p tcp 81` После этого проверьте список портов командой `semanage port -l | grep http_port_t`

```
Forbidden X Уведомление о конфиден X +
root@localhost:/etc/httpd/conf
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts. See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
Listen 81
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
Include conf.modules.d/*.conf
```

Порт определен.

Верните контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`: `chcon -t httpd_sys_content_t /var/www/html/test.html` После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1:81/test.html>. Вы должны увидеть содержимое файла — слово «test».

Удалите файл `/var/www/html/test.html`: `rm /var/www/html/test.html`

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

## Выводы

В ходе данной лабораторной работы я развил навыки администрирования ОС Linux, получил первое практическое знакомство с технологией SELinux, проверил работу SELinux на практике совместно с веб-сервером Apache.

## Список литературы

- [Кулябов Д. С., Королькова А. В., Геворкян М. Н. Лабораторная работа №6](#)