

# Лабораторная работы №6

Павлова В.Ю.

# Цель работы

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

# Ход работы

Войдите в систему и убедитесь, что SELinux находится в режиме enforcing с помощью команды `getenforce` (рис. [fig:001])

```
[vypavlova@localhost ~]$ getenforce
Enforcing
[vypavlova@localhost ~]$ 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
```

ными и  
ng политики  
(рис. [-

команды

# Ход работы

Об  
заг  
по

```
[vypavlova@localhost ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[vypavlova@localhost ~]$ 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: d
   Active: active (running) since Sat 2024-10-12 12:38:11 MSK; 3s ago
     Docs: man:httpd.service(8)
  Main PID: 23211 (httpd)
    Status: "Started, listening on: port 80"
     Tasks: 177 (limit: 24672)
    Memory: 34.3M
       CPU: 183ms
    CGroup: /system.slice/httpd.service
```

обращение к веб-серверу

# Ход работы

Найд  
его к

ите

```
[1] ~$ systemctl status httpd
[vypavlova@localhost ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 23211 0.2 0.2 20152 11432 ?
Ss 12:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 23264 0.0 0.1 22032 7484 ?
S 12:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 23266 0.1 0.3 2161100 15196 ?
Sl 12:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 23268 0.1 0.3 2357772 15412 ?
Sl 12:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 23273 0.1 0.4 2161100 17196 ?
Sl 12:38 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 vypavlo+ 24358 0.0 0.2 23
6780 9216 pts/0 T 12:38 0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 vypavlo+ 34262 0.0 0.0 22
1688 2432 pts/0 S+ 12:38 0:00 grep --color=auto httpd
[vypavlova@localhost ~]$
```

контекст безопасности

# Ход работы

Посмотрите теги SELinux для Apache(рис. [-@

```
[vypavlova@localhost ~]$ getsebool -a | 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_sss --> off
```

состояние переключателей1

# Ход работы

Посмотрите статистику  
seinfo (рис. [-@

о команды

```
[vypavlova@localhost ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:          135      Permissions:       457
Sensitivities:    1        Categories:       1024
Types:            5145     Attributes:        259
Users:            8        Roles:            15
Booleans:         356     Cond. Expr.:      388
Allow:            65500    Neverallow:        0
Auditallow:       176     Dontaudit:         8682
Type_trans:       271770   Type_change:       94
Type_member:      37       Range_trans:       5931
Role allow:       40       Role_trans:        417
Constraints:      70       Validatetrans:     0
MLS Constrains:  72       MLS Val. Tran:     0
Permissives:      4        Polcap:            6
Defaults:         7        Typebounds:        0
```

seinfo

# Ход работы

Определите тип файлов и поддиректорий, находящихся в директории /var/www (рис. [-@fig:006])

```
[vypavlova@localhost ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 авг 8 19
:30 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 авг 8 19
:30 html
[vypavlova@localhost ~]$
```

ls -lZ



# Ход работы

Определите тип файлов, находящихся в директории /var/www/html (рис. [-@fig:008])

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

ls -lZ

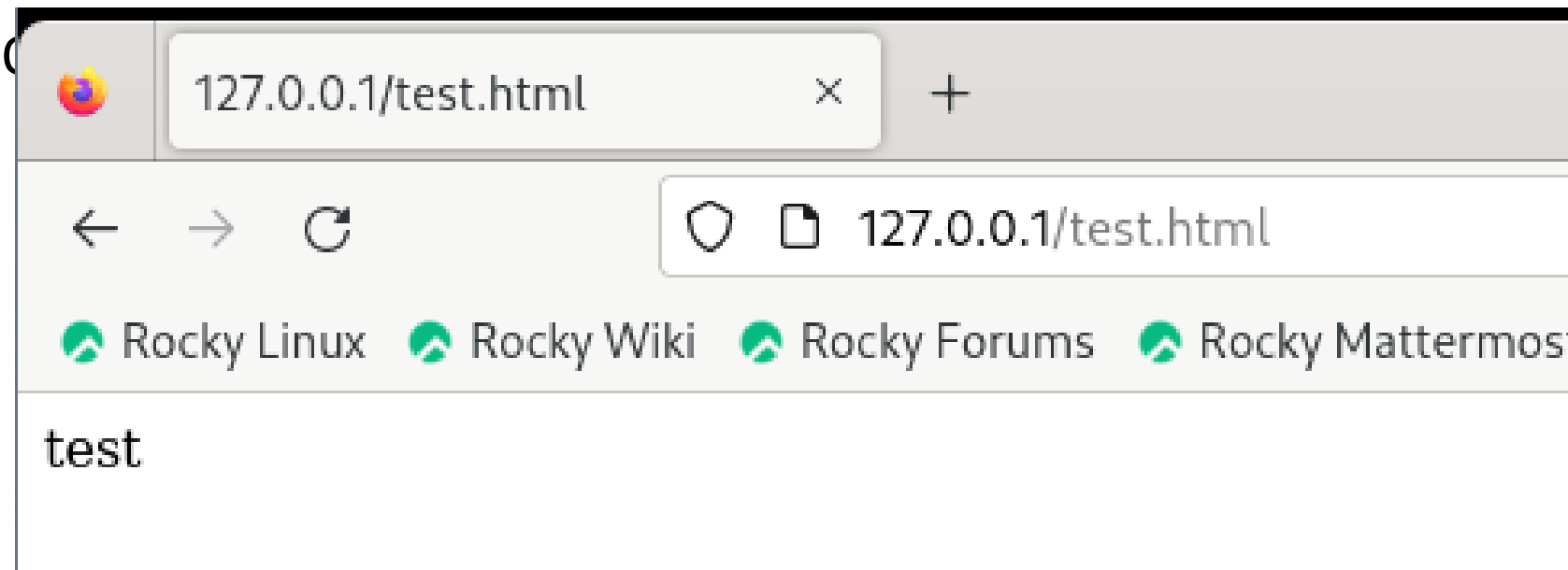
# Ход работы

Создайте от имени суперпользователя (так как в

```
[root@localhost html]# cat test.html  
<html>  
<body>test</body>  
</html>
```

test.html

# Ход работы



браузер

# Ход работы

Выясните, какие контексты файлов определены для httpd (рис. [-@fig:010])

```
[vypavlova@localhost ~]$ ls -Z /var/www/html/test.html  
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
```

ls -Z

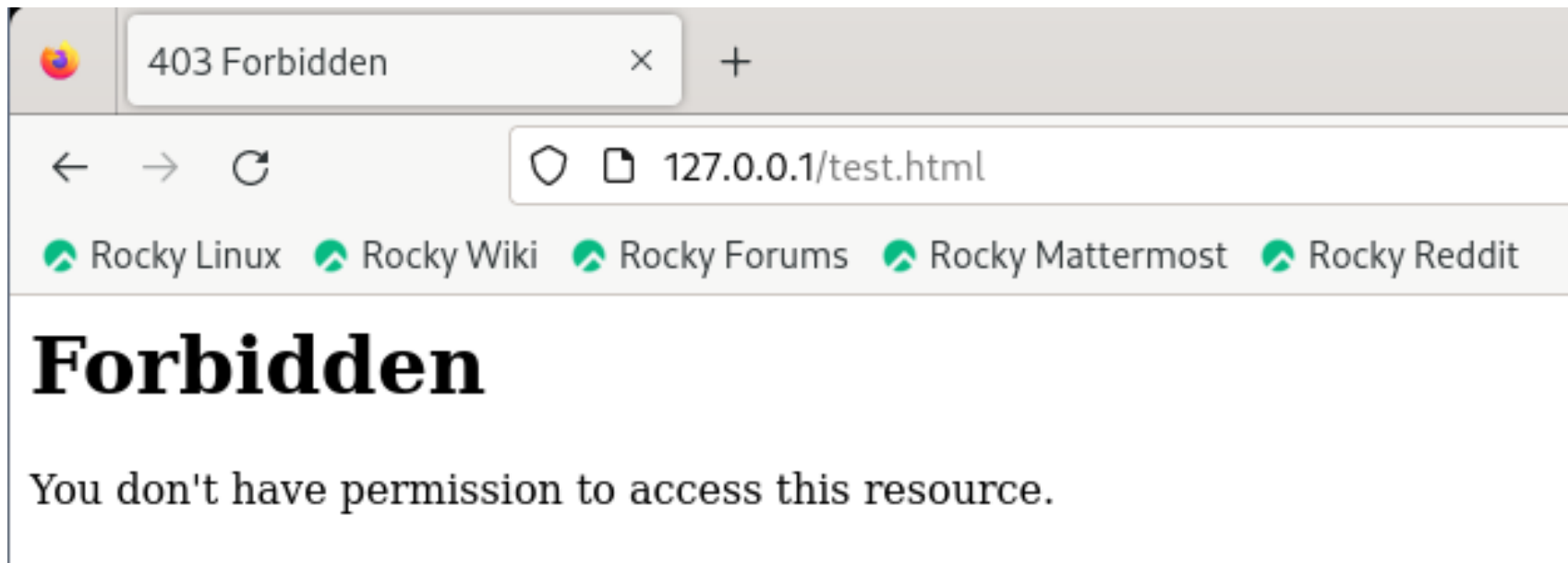
# Ход работы

Измените контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на любой другой, к которому процесс

```
[vypavlova@localhost ~]$ sudo chcon -t samba_share_t /var/www/html/test.html  
[sudo] пароль для vypavlova:  
[vypavlova@localhost ~]$ ls -Z /var/www/html/test.html  
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

chcon

# Ход работы



браузер

# Ход работы

Проанализируйте ситуацию (рис. 1.13).

```
[vypavlova@localhost ~]$ ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 окт 12 12:50 /var/www/html/test.html
[vypavlova@localhost ~]$ tail /var/log/messages
tail: невозможно открыть '/var/log/messages' для чтения: Отказано в доступе
[vypavlova@localhost ~]$ sudo tail /var/log/messages
Oct 12 12:55:31 localhost setroubleshoot[43521]: SELinux запрещает /usr/sbin/httpd
доступ getattr к файл /var/www/html/test.html.#012#012***** Модуль restorecon
предлагает (точность 92.2) *****#012#012Если вы хотите исправить метку.$TARGETЗнак _PATH по умолчанию должен быть httpd_sys_content_t#012
То вы можете запустить restorecon. Возможно, попытка доступа была остановлена из
```

tail

# Ход работы

Попробуйте запустить веб-сервер Apache на прослушивание

```
GNU nano 5.6.1 httpd.conf
Listen 81

#
# Dynamic Shared Object (DSO) Support
#
```

httpd.conf



# Ход работы

Выполните перезапуск веб-сервера Apache. (рис. [-@fig:015])

```
[vypavlova@localhost ~]$ service httpd restart  
Redirecting to /bin/systemctl restart httpd.service
```

restart

# Ход работы

Проанализируйте лог-файлы (рис. [-@fig:016])

```
tail: неверное количество строк: «1»  
[vypavlova@localhost ~]$ sudo tail -n1 /var/log/messages  
Oct 12 12:59:44 localhost systemd[1]: fprintd.service: Deactivated successfully.
```

logs

# Ход работы

Выполните команду `semanage port -a -t http_port_t -p tcp 81`

```
[vypavlova@localhost ~]$ sudo semanage port -a -t http_port_t -p tcp 81
Port tcp/81 already defined, modifying instead
[vypavlova@localhost ~]$ semanage port -l | grep http_port_t
ValueError: Политика SELinux не задана, или нет доступа к хранилищу.
[vypavlova@localhost ~]$ sudo semanage port -l | grep http_port_t
http_port_t                tcp                81, 80, 81, 443, 488, 8008, 8009, 8443
9000
pegasus_http_port_t        tcp                5988
```

команда

# Ход работы

```
pegasus_http_port_t      tcp      5988
[vypavlova@localhost ~]$ service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[vypavlova@localhost ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; vendor preset: enabled)
   Active: active (running) since Sat 2024-10-12 13:01:01 MSK; 1min 45s ago
     Docs: man:httpd.service(8)
   Main PID: 42958 (httpd)
```

restart

# Ход работы

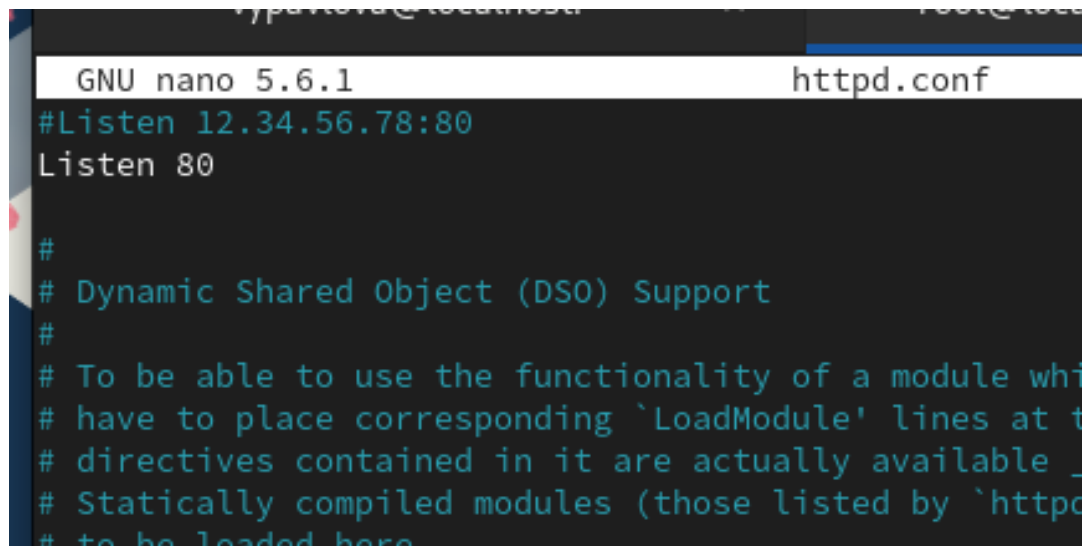
Верните контекст `httpd_sys_content_t` к файлу `/var/www/html/ test.html`: (рис. [-@fig:019])

```
[vypavlova@localhost ~]$ sudo chcon -t httpd_sys_content_t /var/www/html/test.html
```

chcon

## Ход работы

Исправьте обратно конфигурационный файл apache, вернув Listen 80. (рис. [-@fig:020])



```
GNU nano 5.6.1 httpd.conf
#Listen 12.34.56.78:80
Listen 80

#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a
# shared module (DSO) you have to place corresponding 'LoadModule' lines at
# this location so the functions can be found at runtime. Note that the
# module paths must be the same as in the 'LoadModule' lines at the top
# of the 'httpd.conf' file (i.e. relative to the 'httpd.conf' file).
#
# Statically compiled modules (those listed by 'httpd -l') do not
# need to be loaded here.
```

# Ход работы

Удалите файл /var/www/html/test.html (рис. [-@fig:021])

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

rm

# Вывод

В ходе выполнения данной лабораторной 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.