

Лабораторная работа №6

Павлова Варвара Юрьевна

Содержание

Цель работы	1
Ход работы.....	1
Вывод.....	6

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

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

команды

2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает(рис. [-@fig:002])

```

[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: disabled)
   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

3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности(рис. [-@fig:003])

```

[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

```

контекст безопасности

4. Посмотрите текущее состояние переключателей SELinux для Apache(рис. [-@fig:004])

```

[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_avalahi --> off
httpd_dbus_sssd --> off

```

состояние переключателей1

5. Посмотрите статистику по политике с помощью команды seinfo (рис. [-@fig:005])

```
[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 Constrain:          72       MLS Val. Tran:        0
Permissives:            4        Polcap:              6
Defaults:                7       Typebounds:          0
```

seinfo

6. 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 апр  8 19
:30 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 апр  8 19
:30 html
[vypavlova@localhost ~]$
```

ls -lZ

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

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

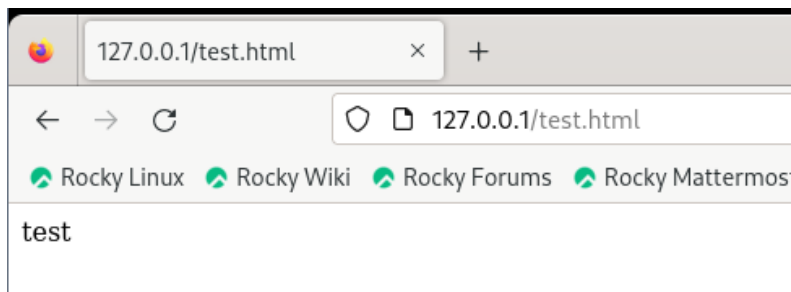
ls -lZ

8. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html (рис. [-@fig:008])

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

test.html

9. Обратитесь к файлу через веб-сервер (рис. [-@fig:009])



браузер

10. 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
```

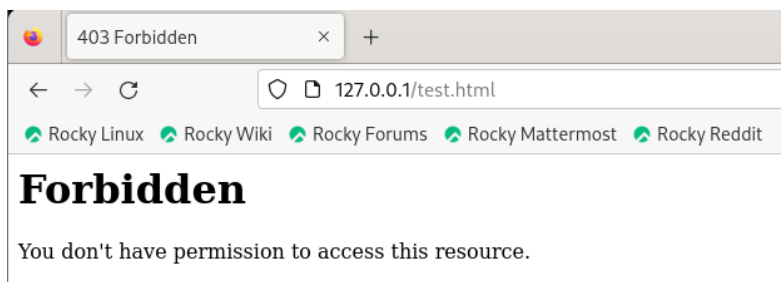
ls -Z

11. 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 (рис. [-@fig:011])

```
[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

12. Попробуйте ещё раз получить доступ к файлу через веб-сервер (рис. [-@fig:012])



браузер

13. Проанализируйте ситуацию (рис. [-@fig:013])

```
[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 restoreco
n предлагает (точность 92.2) *****#012#012Если вы хотите ис
править метку.$TARGETзнак _PATH по умолчанию должен быть httpd_sys_content_t#012
То вы можете запустить restorecon. Возможно, попытка доступа была остановлена из
```

tail

14. Попробуйте запустить веб-сервер Apache на прослушивание TCP-порта 81 (рис. [-@fig:014])

```
GNU nano 5.6.1 httpd.conf
Listen 81

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

httpd.conf

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

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

restart

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

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

logs

17. Выполните команду `semanage port -a -t http_port_t -p tcp 81` (рис. [-@fig:017])

```
[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

18. Попробуйте запустить веб-сервер Apache ещё раз (рис. [-@fig:018])

```
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/systemd/systemd.servi
   Active: active (running) since Sat 2024-10-12 13:0
   Docs: man:httpd.service(8)
   Main PID: 42958 (httpd)
```

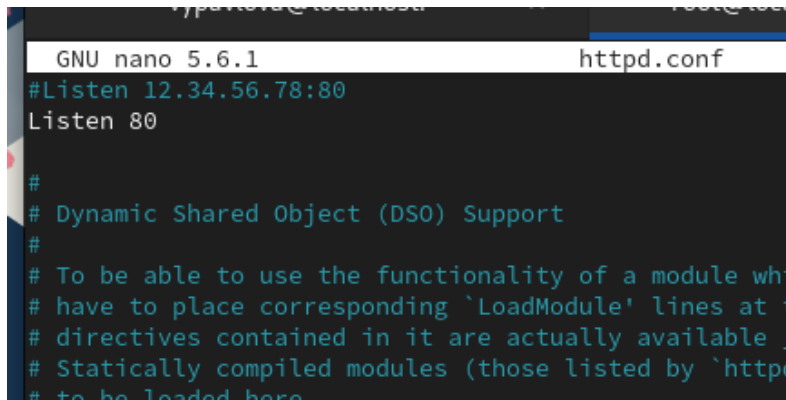
restart

19. 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

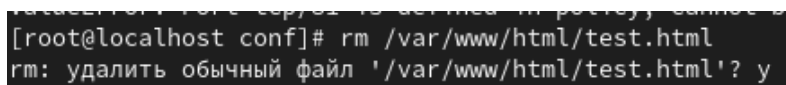
20. Исправьте обратно конфигурационный файл apache, вернув Listen 80. (рис. [-@fig:020])



```
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, you have to place corresponding 'LoadModule' lines at
# this location so the 'mod_...' lines can deal with it. Just uncomment
# the 'LoadModule' lines and you're good to go.
#
# Static compiled modules (those listed by 'httpd -l') do not need this
# to be loaded here.
```

21. 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.