

Информационная безопасность

Лабораторная работа №6

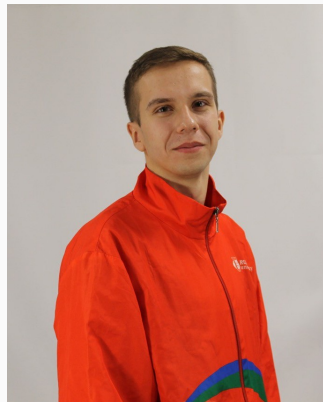
Матюшкин Д. В.

12 октября 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Матюшкин Денис Владимирович
- студент 4-го курса
- группа НПИбд-02-21
- Российский университет дружбы народов
- 1032212279@pfur.ru
- <https://stifell.github.io/ru/>



Цель работы

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

Выполнение лабораторной работы

1. Убедитесь, что SELinux работает в режиме enforcing политики targeted

```
[dvmatyushkin@dvmatyushkin etc]$ getenforce
Enforcing
[dvmatyushkin@dvmatyushkin etc]$ 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
[dvmatyushkin@dvmatyushkin etc]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
• httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Active: active (running) since Sat 2024-10-12 20:44:15 MSK; 50s ago
     Docs: man:httpd.service(8)
  Main PID: 122347 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
     Tasks: 177 (limit: 23033)
    Memory: 24.7M
       CPU: 207ms
    CGroup: /system.slice/httpd.service
            └─122347 /usr/sbin/httpd -DFOREGROUND
              └─122349 /usr/sbin/httpd -DFOREGROUND
                └─122350 /usr/sbin/httpd -DFOREGROUND
                  └─122351 /usr/sbin/httpd -DFOREGROUND
                    └─122352 /usr/sbin/httpd -DFOREGROUND

Oct 12 20:44:10 dvmatyushkin.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 12 20:44:15 dvmatyushkin.localdomain httpd[122347]: Server configured, listening on: port 80
Oct 12 20:44:15 dvmatyushkin.localdomain systemd[1]: Started The Apache HTTP Server.
```

Рис. 1: Проверка работы SELinux

2. Запуск localhost

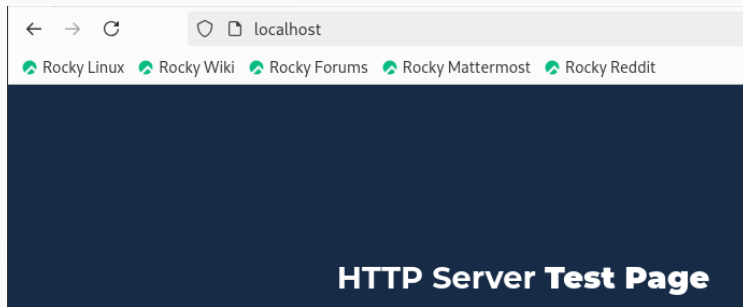


Рис. 2: localhost

3. Определите контекст безопасности Apache

```
[dvmatyushkin@dvmatyushkin etc]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 122347 0.0 0.3 20364 11548 ? Ss 20:44 0:00 /usr/sbin/httpd -D
FOREGROUND
system_u:system_r:httpd_t:s0 apache 122349 0.0 0.1 22096 7144 ? S 20:44 0:00 /usr/sbin/httpd -D
FOREGROUND
system_u:system_r:httpd_t:s0 apache 122350 0.0 0.2 2226704 10816 ? Sl 20:44 0:00 /usr/sbin/httpd -D
FOREGROUND
system_u:system_r:httpd_t:s0 apache 122351 0.0 0.3 2226704 11676 ? Sl 20:44 0:00 /usr/sbin/httpd -D
FOREGROUND
system_u:system_r:httpd_t:s0 apache 122352 0.0 0.4 2423376 15072 ? Sl 20:44 0:00 /usr/sbin/httpd -D
FOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 dvmatyu+ 123087 0.0 0.0 221796 2304 pts/0 S+ 20:47 0:00 grep
--color=auto httpd
[dvmatyushkin@dvmatyushkin etc]$ sestatus -bigrep httpd
```

Рис. 3: Список процессов

4. Посмотрите текущее состояние переключателей SELinux

```
[dvmatyushkin@dvmatyushkin etc]$ sudo getsebool -a | grep httpd
[sudo] password for dvmatyushkin:
httpd_anon_write --> off
httpd_built_in_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
```

Рис. 4: Текущее состояние переключателей

5. Посмотрите статистику по политике

```
[dvmatyushkin@dvmatyushkin etc]$ 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:                  65504    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
Allowxperm:             0        Neverallowxperm:       0
Auditallowxperm:        0        Dontauditxperm:       0
Ibendportcon:           0        Ibpkeycon:             0
Initial SIDs:           27       Fs_use:                35
Genfscon:               109     Portcon:               665
Netifcon:               0        Nodecon:               0
```

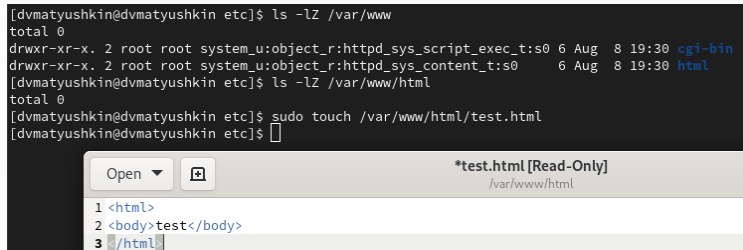
Рис. 5: Статистика по политике

6.1. Выполнение нескольких задач

- Определите тип файлов и поддиректорий `/var/www` и `/var/www/html`
- Определите круг пользователей, которым разрешено создание файлов в директории `/var/www/html`
- Создайте от имени суперпользователя html-файл `/var/www/html/test.html`

6.2. Скриншот

```
[dvmatyushkin@dvmatyushkin etc]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Aug  8 19:30 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 Aug  8 19:30 html
[dvmatyushkin@dvmatyushkin etc]$ ls -lZ /var/www/html
total 0
[dvmatyushkin@dvmatyushkin etc]$ sudo touch /var/www/html/test.html
[dvmatyushkin@dvmatyushkin etc]$
```



The image shows a terminal window with a dark background. The first part shows the execution of 'ls -lZ /var/www' and 'ls -lZ /var/www/html', displaying directory permissions and SELinux contexts. Then, 'sudo touch /var/www/html/test.html' is executed. Below the terminal, a file editor window is open for '*test.html [Read-Only]' located at '/var/www/html'. The editor shows three lines of HTML code: '<html>', '<body>test</body>', and '</html>'. The first line is highlighted in blue, and the third line is highlighted in grey.

Рис. 6: Тип файлов и поддиректорий

7. Проверьте контекст созданного вами файла

```
[dvmatyushkin@dvmatyushkin etc]$ ls -lZ /var/www/html/  
total 4  
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Oct 12 20:53 test.html  
[dvmatyushkin@dvmatyushkin etc]$
```

Рис. 7: Проверка контекста

8. Обратитесь к файлу через веб-сервер

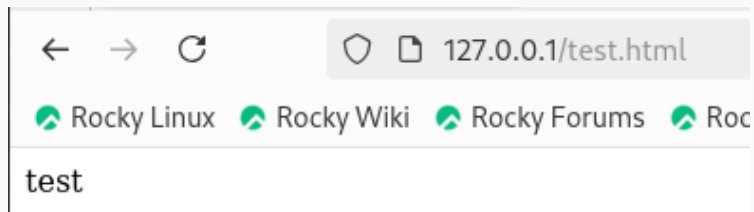


Рис. 8: Проверка

9. Измените контекст файла /var/www/html/test.html

```
[dvmatyushkin@dvmatyushkin etc]$ sudo chcon -t samba_share_t /var/www/html/test.html
[dvmatyushkin@dvmatyushkin etc]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[dvmatyushkin@dvmatyushkin etc]$
```

Рис. 9: Изменение контекста

10. Попробуйте ещё раз получить доступ к файлу через веб-сервер

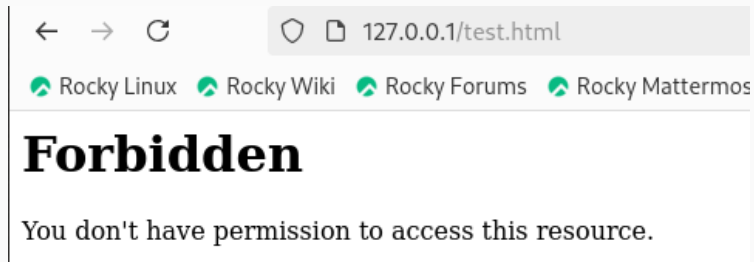


Рис. 10: Проверка

11. Проанализируйте ситуацию

```
[dvmatyushkin@dvmatyushkin etc]$ sudo tail /var/log/messages
Oct 12 20:58:25 dvmatyushkin systemd[1]: Started dbus-:1.1-org.fedoraproject.SetroubleshootPr
Oct 12 20:58:27 dvmatyushkin setroubleshoot[123820]: SELinux is preventing /usr/sbin/httpd from
  file /var/www/html/test.html. For complete SELinux messages run: sealert -l aa48e141-45b9-4f
Oct 12 20:58:27 dvmatyushkin setroubleshoot[123820]: SELinux is preventing /usr/sbin/httpd from
  file /var/www/html/test.html.#012#012***** Plugin restorecon (92.2 confidence) suggests  **
012#012If you want to fix the label. #012/var/www/html/test.html default label should be httpd
  you can run restorecon. The access attempt may have been stopped due to insufficient permis
directory in which case try to change the following command accordingly.#012Do#012# /sbin/rest
```

Рис. 11: Системный лог-файл

12. Попробуйте запустить веб-сервер Apache на прослушивание TCP-порта 81

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

Рис. 12: Смена порта

13. Выполните перезапуск веб-сервера Apache

- Сбоя не произошло, потому что порт 81 уже был в списке портов.

14. Проанализируйте лог-файлы

```
[root@dvmatyushkin conf]# tail /var/log/messages
Oct 12 20:59:47 dvmatyushkin systemd[1]: Started Fingerprint Authentication Daemon.
Oct 12 20:59:48 dvmatyushkin su[123885]: (to root) dvmatyushkin on pts/0
Oct 12 21:00:18 dvmatyushkin systemd[1]: fprintd.service: Deactivated successfully.
Oct 12 21:01:40 dvmatyushkin systemd[1]: Stopping The Apache HTTP Server...
Oct 12 21:01:41 dvmatyushkin systemd[1]: httpd.service: Deactivated successfully.
Oct 12 21:01:41 dvmatyushkin systemd[1]: Stopped The Apache HTTP Server.
Oct 12 21:01:41 dvmatyushkin systemd[1]: httpd.service: Consumed 1.678s CPU time.
Oct 12 21:01:41 dvmatyushkin systemd[1]: Starting The Apache HTTP Server...
Oct 12 21:01:47 dvmatyushkin httpd[124006]: Server configured, listening on: port 81
Oct 12 21:01:47 dvmatyushkin systemd[1]: Started The Apache HTTP Server.
```

Рис. 13: Системный лог-файл

15. Выполните команду добавления порта

```
[root@dvmatyushkin conf]# semanage port -a -t http_port_t -p tcp 81
usage: semanage [-h]
               {import,export,login,user,port,ibpkey,ibendport,interface,module,node,fc
taudit}
               ...
semanage: error: unrecognized arguments: -p 81
[root@dvmatyushkin 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@dvmatyushkin conf]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@dvmatyushkin conf]#
```

Рис. 14: Добавление порта

16. Возвращение настроек

- Верните контекст `httpd_sys_content__t` к файлу `/var/www/html/ test.html`
- Исправьте обратно конфигурационный файл `apache`, вернув `Listen 80`

17. Удалите привязку и созданный ранее файл

```
[root@dvmatyushkin conf]# ls -Z /var/www/html/  
unconfined_u:object_r:httpd_sys_content_t:s0 test.html  
[root@dvmatyushkin conf]# semanage port -d -t http_port_t -p tcp 81  
ValueError: Port tcp/81 is defined in policy, cannot be deleted  
[root@dvmatyushkin conf]# rm /var/www/html/test.html  
rm: remove regular file '/var/www/html/test.html'?  
[root@dvmatyushkin conf]#
```

Рис. 15: Удаление привязки и файла

Выводы

- В ходе данной лабораторной работы мы развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux. Проверили работу SELinux на практике совместно с веб-сервером Apache.