

Информационная безопасность

Лабораторная работа №6

Матюшкин Денис Владимирович (НПИбд-02-21)

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Ход работы	7
4	Выводы	15
	Список литературы	16

Список иллюстраций

3.1	Проверка работы SELinux	7
3.2	localhost	8
3.3	Список процессов	8
3.4	Текущее состояние переключателей	8
3.5	Статистика по политике	9
3.6	Тип файлов и поддиректорий	10
3.7	Проверка контекста	10
3.8	Проверка	10
3.9	Изменение контекста	11
3.10	Проверка	11
3.11	Системный лог-файл	12
3.12	Смена порта	12
3.13	Системный лог-файл	12
3.14	Добавление порта	13
3.15	Удаление привязки и файла	14

Список таблиц

1 Цель работы

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

2 Теоретическое введение

VirtualBox (Oracle VM VirtualBox) — программный продукт виртуализации для операционных систем Windows, Linux, FreeBSD, macOS, Solaris/OpenSolaris, ReactOS, DOS и других [1].

Rocky Linux — дистрибутив Linux, разработанный Rocky Enterprise Software Foundation. Предполагается, что это будет полный бинарно-совместимый выпуск, использующий исходный код операционной системы Red Hat Enterprise Linux (RHEL) [2].

3 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. 3.1).

```
[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. 3.1: Проверка работы SELinux

2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает (рис. 3.2).

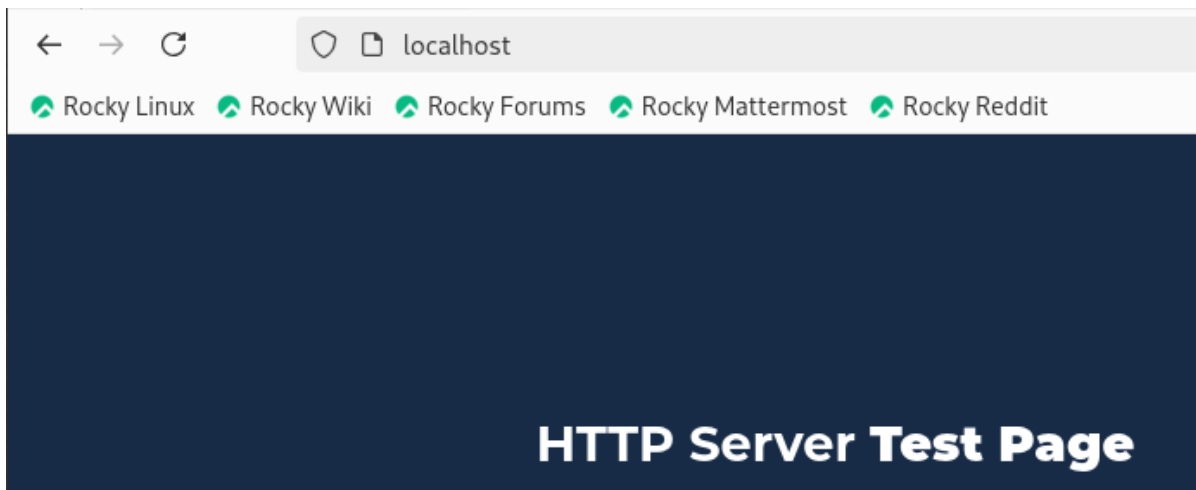


Рис. 3.2: localhost

3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт (рис. 3.3).

```
[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. 3.3: Список процессов

4. Посмотрите текущее состояние переключателей SELinux для Apache (рис. 3.4).

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

Рис. 3.4: Текущее состояние переключателей

5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов (рис. 3.5).

```
[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 Constrains:  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. 3.5: Статистика по политике

6. Определите тип файлов и поддиректорий, находящихся в директории `/var/www` (рис. 3.6).
7. Определите тип файлов, находящихся в директории `/var/www/html` (рис. 3.6).
8. Определите круг пользователей, которым разрешено создание файлов в директории `/var/www/html` (рис. 3.6).
9. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) `html`-файл `/var/www/html/test.html` (рис. 3.6).

```
[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]$
```

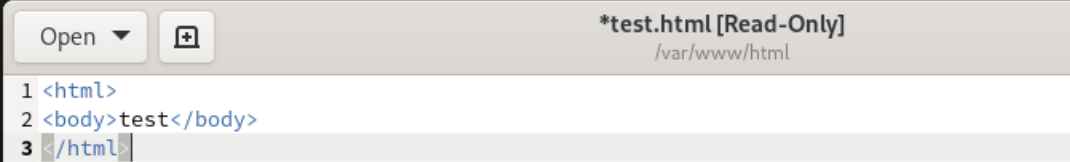


Рис. 3.6: Тип файлов и поддиректорий

10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html (рис. 3.7).

```
[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. 3.7: Проверка контекста

11. Обратитесь к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Убедитесь, что файл был успешно отображён (рис. 3.8).

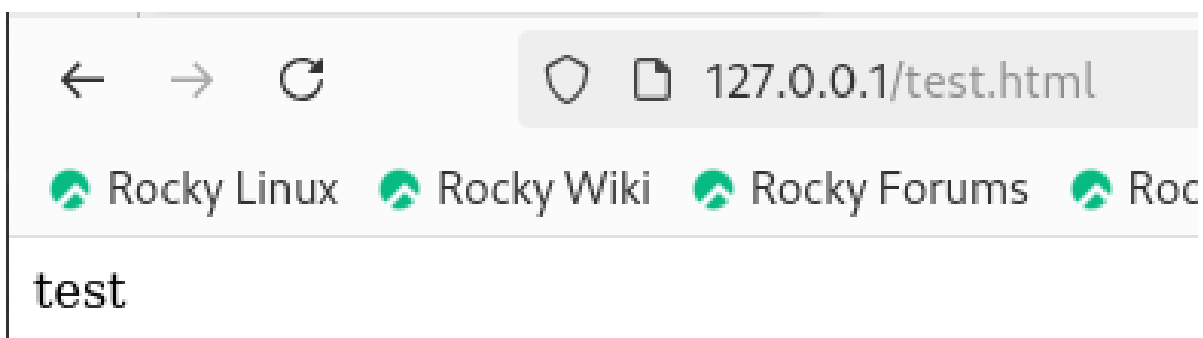


Рис. 3.8: Проверка

12. Изучите справку `man httpd_selinux` и выясните, какие контексты файлов определены для `httpd`. Сопоставьте их с типом файла `test.html`. Проверить контекст файла можно командой `ls -Z`.

13. 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. 3.9).

```
[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. 3.9: Изменение контекста

14. . Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Вы должны получить сообщение об ошибке (рис. 3.10).

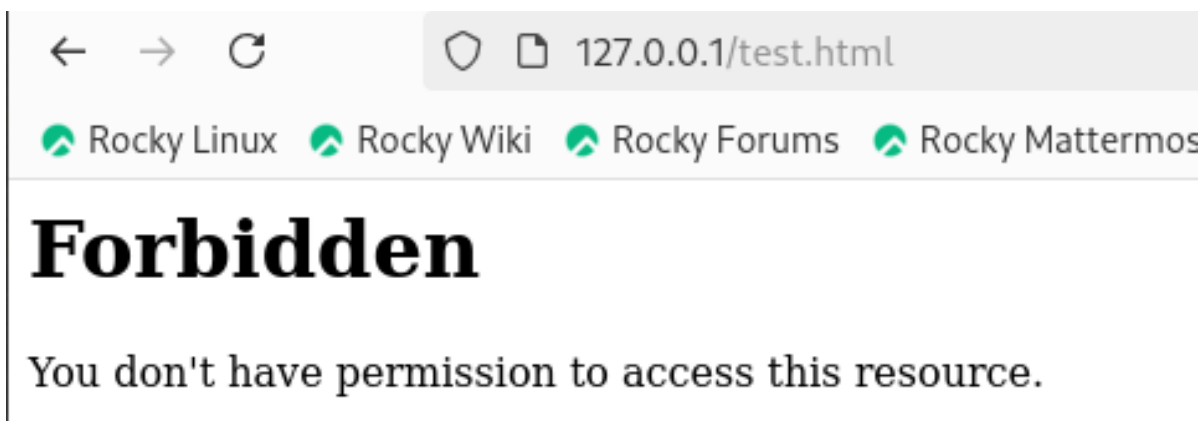


Рис. 3.10: Проверка

15. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: `tail /var/log/messages` (рис. 3.11).

```
[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 aa48e141-45b9-4f1
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. 3.11: Системный лог-файл

16. 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 (рис. 3.12).

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

Рис. 3.12: Смена порта

17. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему?

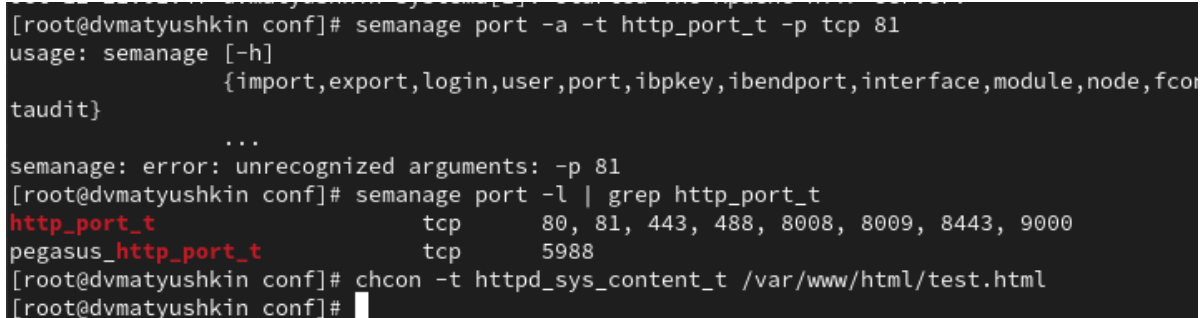
Сбоя не произошло, потому что порт 81 уже был в списке портов.

18. Проанализируйте лог-файлы: tail -nl /var/log/messages (рис. 3.13).

```
[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. 3.13: Системный лог-файл

19. 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`. Убедитесь, что порт 81 появился в списке (рис. 3.14).



```
[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. 3.14: Добавление порта

Порт уже был добавлен.

20. Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему он сейчас запустился, а в предыдущем случае не смог?

И в прошлый раз мог.

21. Верните контекст `httpd_sys_content_t` к файлу `/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».
22. Исправьте обратно конфигурационный файл `apache`, вернув `Listen 80`.
23. Удалите привязку `http_port_t` к 81 порту (рис. 3.15).
24. Удалите файл `/var/www/html/test.html` (рис. 3.15).

```
[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. 3.15: Удаление привязки и файла

4 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.

Список литературы

1. VirtualBox Documentation [Электронный ресурс]. Oracle, 2024. URL: <https://www.virtualbox.org/wiki/Documentation>.
2. Rocky Documentation [Электронный ресурс]. Rocky Enterprise Software Foundation, 2024. URL: <https://docs.rockylinux.org/ru/>.