

Лабораторная работа №6

Мандатное разграничение прав в Linux

Пономарева Лилия Михайловна

Содержание

| | |
|--------------------------------|----|
| Цель работы | 4 |
| Теоретическое введение | 5 |
| Выполнение лабораторной работы | 7 |
| Выводы | 20 |
| Список литературы | 21 |

Список иллюстраций

| | | |
|----|---|----|
| 1 | Режим SELinux | 7 |
| 2 | Проверка работы веб-сервера | 8 |
| 3 | Список процессов | 8 |
| 4 | Состояние переключателей SELinux | 9 |
| 5 | Статистика SELinux | 10 |
| 6 | Тип поддиректорий в директории /var/www | 11 |
| 7 | Директория /var/www/html | 11 |
| 8 | Право на создание файлов | 11 |
| 9 | HTML-файл /var/www/html/test.html | 11 |
| 10 | Контекст файла | 12 |
| 11 | Отображение файла test.html | 12 |
| 12 | Справка man httpd_selinux | 13 |
| 13 | Изменение контекста файла | 13 |
| 14 | Доступ через веб-сервер | 14 |
| 15 | log-файл | 14 |
| 16 | Системный log-файл | 15 |
| 17 | Включение прослушивания 81 порта | 15 |
| 18 | Лог-файл /var/log/messages | 16 |
| 19 | Лог-файл /var/log/http/error_log | 16 |
| 20 | Лог-файл /var/log/http/access_log | 16 |
| 21 | Лог-файл /var/log/audit/audit.log | 17 |
| 22 | Список портов | 17 |
| 23 | Перезапуск Apache | 17 |
| 24 | Контекст файла | 18 |
| 25 | Доступ по другому порту | 18 |
| 26 | Конфигурационный файл Apache | 18 |
| 27 | Удаление порта из списка | 19 |
| 28 | Удаление файла | 19 |

Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux¹. Проверить работу SELinux на практике совместно с веб-сервером Apache. [1]

Теоретическое введение

Security Enhanced Linux, или SELinux – это усовершенствованный механизм контроля доступа, встроенный в большинство современных дистрибутивов Linux.

SELinux реализует так называемый MAC (Mandatory Access Control). Это разграничение контроля внедряется поверх того, что уже есть в каждом дистрибутиве Linux, DAC (Discretionary Access Control).

По сути, в традиционной модели избирательного управления доступом (DAC), хорошо реализованы только два уровня доступа — пользователь и суперпользователь. Нет простого метода, который позволил бы устанавливать для каждого пользователя необходимый минимум привилегий.

Основные термины, используемые в SELinux:

Домен — список действий, которые может выполнять процесс. Обычно в качестве домена определяется минимально-возможный набор действий, при помощи которых процесс способен функционировать. Таким образом, если процесс дискредитирован, злоумышленнику не удастся нанести большого вреда.

Роль — список доменов, которые могут быть применены. Если какого-то домена нет в списке доменов какой-то роли, то действия из этого домена не могут быть применены.

Тип — набор действий, которые допустимы по отношению к объекту. Тип отличается от домена тем, что он может применяться к пайпам, каталогам и файлам, в то время как домен применяется к процессам.

Контекст безопасности — все атрибуты SELinux — роли, типы и домены.

Система SELinux может работать в любом из трех доступных режимов: -

Enforcing - Permissive - Disabled

В режиме *enforcing* SELinux применяет свою политику в системе Linux и следит за тем, чтобы все попытки несанкционированного доступа со стороны пользователей и процессов были запрещены. Отказы в доступе регистрируются в соответствующих логах.

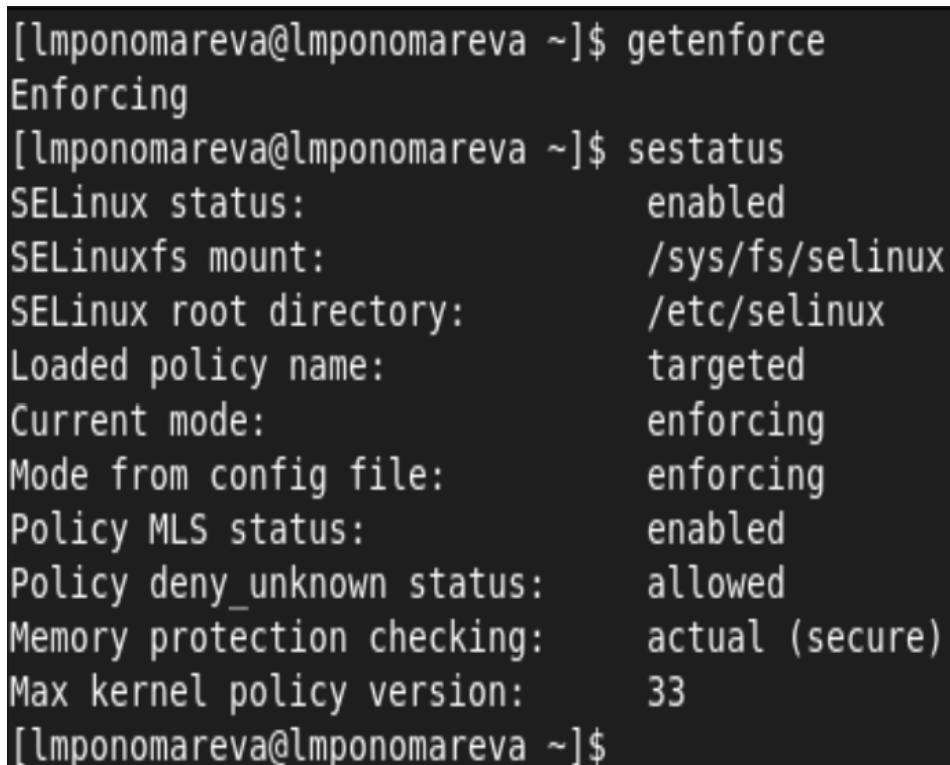
Режим *permissive* – это такое полуоткрытое состояние: в этом режиме SELinux не применяет свою политику, поэтому не блокирует доступ. Однако любое нарушение политики будет зарегистрировано в логах.

Режим *disabled* – система отключена.

SELinux по-умолчанию работает в режиме Enforcing, когда любые действия, кроме разрешенных, автоматически блокируются, каждая программа, пользователь или сервис обладают только теми привилегиями, которые необходимы им для функционирования, но не более того. Это довольно жесткая политика, которая обладает как плюсами — наибольший уровень информационной безопасности, так и минусами — конфигурирование системы в таком режиме сопряжено с большими трудозатратами системных администраторов, к тому же, велик риск того, что пользователи столкнутся с ограничением доступа, если захотят использовать систему хоть сколько-нибудь нетривиальным образом.

Выполнение лабораторной работы

1. Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`. (рис. 1)



```
[lmponomareva@lmponomareva ~]$ getenforce
Enforcing
[lmponomareva@lmponomareva ~]$ 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
[lmponomareva@lmponomareva ~]$
```

Рис. 1: Режим SELinux

2. Запустила веб-сервер. Обратилась с помощью браузера к веб-серверу, запущенному на компьютере, и убедилась, что последний работает: service

httpd status. (рис. 2).

```
[lmponomareva@lmponomareva ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[lmponomareva@lmponomareva ~]$ 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 09:54:43 MSK; 3s ago
     Docs: man:httpd.service(8)
    Main PID: 39855 (httpd)
      Status: "Started, listening on: port 80"
```

Рис. 2: Проверка работы веб-сервера

3. Нашла веб-сервер Apache в списке процессов. (рис. 3).

```
[lmponomareva@lmponomareva ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 39855 0.2 0.5 20064 11596 ?
Ss 09:54 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 39863 0.0 0.3 21516 7284 ?
S 09:54 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 39864 0.0 0.9 1210352 19156 ?
Sl 09:54 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 39867 0.0 0.8 1079216 17108 ?
Sl 09:54 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 39872 0.0 0.8 1079216 17108 ?
Sl 09:54 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 lmponom+ 40111 0.0 0.1 22
1668 2340 pts/1 S+ 09:55 0:00 grep --color=auto httpd
```

Рис. 3: Список процессов

Контекст безопасности: system_u:system_r:httpd_t:s0

4. Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -b | grep httpd`. (рис. 4).


```
[lmponomareva@lmponomareva ~]$ sestatus -b | grep httpd
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
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
httpd_graceful_shutdown off
httpd_manage_ipa off
```

Рис. 4: Состояние переключателей SELinux

Многие из них находятся в положении «off»

5. Посмотрела статистику по политике с помощью команды seinfo. (рис. 5).

```

[lmponomareva@lmponomareva ~]$ 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      Ibpkeycon:              0
Initial SIDs:            27      Fs_use:                 33
Genfscon:                106     Portcon:                651
Netifcon:                0       Nodecon:                0

```

Рис. 5: Статистика SELinux

Множество пользователей - 8

Ролей - 14 Типов - 5002

6. Определила тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды `ls -lZ /var/www` (рис. 6).

```
[lmponomareva@lmponomareva ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 15:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 May 16 15:10 html
```

Рис. 6: Тип поддиректорий в директории /var/www

7. Определила тип файлов, находящихся в директории /var/www/html: `ls -lZ /var/www/html` (рис. 7).

```
[lmponomareva@lmponomareva ~]$ ls -lZ /var/www/html
total 0
```

Рис. 7: Директория /var/www/html

8. Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html. (рис. 8).

```
[lmponomareva@lmponomareva ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 15:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 May 16 15:10 html
```

Рис. 8: Право на создание файлов

Создавать файлы в директории может только её владелец.

9. Создала от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания: (рис. 9).

```
GNU nano 5.6.1 /var/www/html/test.html
<html>
<body> test </body>
</html>
```

Рис. 9: HTML-файл /var/www/html/test.html

10. Проверила контекст созданного файла. (рис. 10).

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

Рис. 10: Контекст файла

Контекст безопасности (по умолчанию для новых файлов в директории):
unconfined_u:object_r:httpd_sys_content_t:s0

11. Обратилась к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>.
(рис. 11).

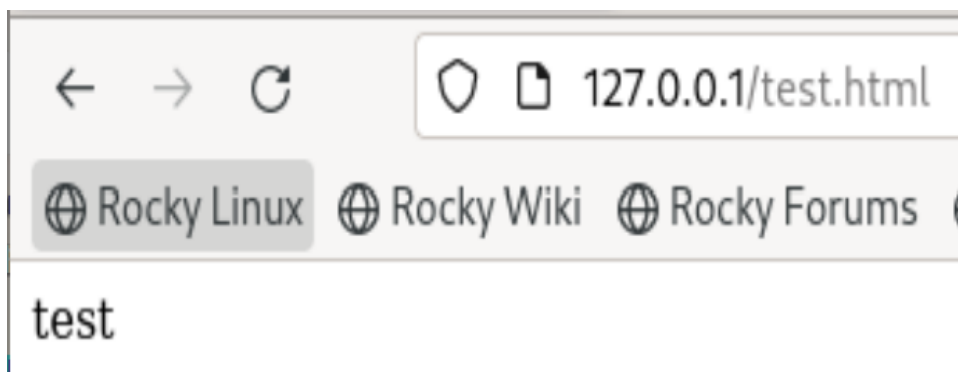


Рис. 11: Отображение файла test.html

12. Изучила справку `man httpd_selinux` (рис. 12).

```

httpd_sys_rw_content_t
/etc/glpi(/.*)?
/etc/horde(/.*)?
/etc/drupal.*
/etc/z-push(/.*)?
/var/lib/svn(/.*)?
/var/www/svn(/.*)?
/etc/owncloud(/.*)?
/var/www/html(/.*)?/uploads(/.*)?
/var/www/html(/.*)?/wp-content(/.*)?
/var/www/html(/.*)?/sites/default/files(/.*)?
/var/www/html(/.*)?/sites/default/settings.php
/etc/mock/koji(/.*)?
/var/lib/drupal.*
/etc/zabbix/web(/.*)?
/var/log/z-push(/.*)?
/var/spool/gosa(/.*)?
/var/lib/moodle(/.*)?
/etc/WebCalendar(/.*)?
/usr/share/joomla(/.*)?
/var/lib/dokuwiki(/.*)?
/var/lib/owncloud(/.*)?
/var/spool/viewvc(/.*)?
/var/lib/pootle/po(/.*)?
/var/www/moodledata(/.*)?
/srv/gallery2/smarty(/.*)?
/var/www/moodle/data(/.*)?
/var/www/gallery/albums(/.*)?
/var/www/html/owncloud/data(/.*)?
/usr/share/wordpress-mu/wp-content(/.*)?
/usr/share/wordpress/wp-content/uploads(/.*)?
/usr/share/wordpress/wp-content/upgrade(/.*)?
/var/www/html/configuration.php

```

Рис. 12: Справка man httpd_selinux

13. Изменила контекст файла /var/www/html/test.html с httpd_sys_content_t на тот, к которому процесс httpd не имеет доступ (samba_share_t) (рис. 13).

```

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

```

Рис. 13: Изменение контекста файла

14. Попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. (рис. 14).

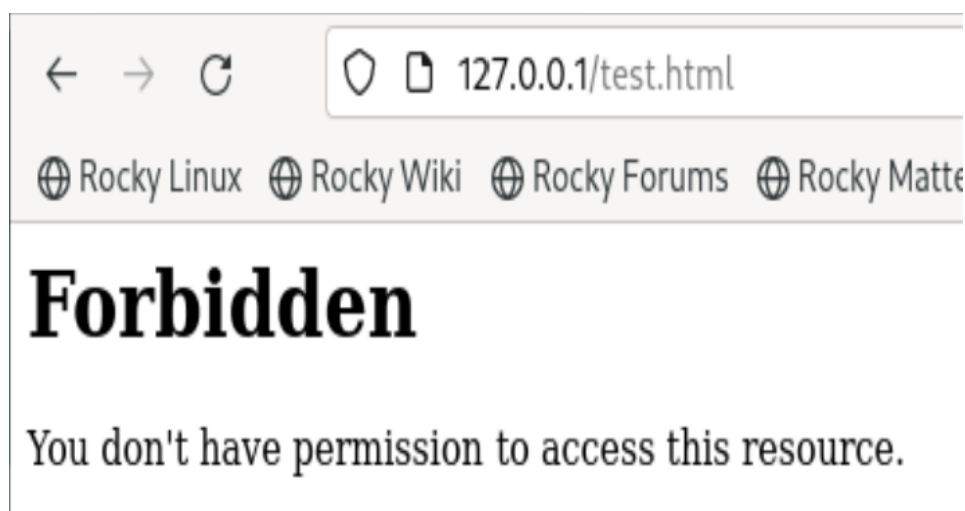


Рис. 14: Доступ через веб-сервер

Файл не отображен, так как к заданному типу контекста httpd не имеет доступа.

15. Просмотрела log-файлы веб-сервера Apache. (рис. 15)

```
[root@lmponomareva lmponomareva]# tail /var/log/audit/audit.log
type=AVC msg=audit(1665822914.169:322): avc: denied { getattr } for pid=39872 comm="httpd" path="/var/www/html/test.html" dev="dm-0" ino=101177494 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:system_u:object_class_t:s0 tclass=file permissive=0
type=SYSCALL msg=audit(1665822914.169:322): arch=c000003e syscall=262 success=no exit=-13 a0=ffffff9c a1=7f3b54004ff0 a2=7f3b6883f830 a3=0 items=0 ppid=39855 pid=39872 auid=4294967295 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 comm="httpd" exe="/usr/sbin/httpd" subj=system_u:system_r:httpd_t:s0 key=(null)ARCH=x86_64 SYSCALL=newfstatat AUID="unset" UID="apache" GID="apache" EUID="apache" FSUID="apache" FSUID="apache" EGID="apache" SGID="apache" FSGID="apache"
type=PROCTITLE msg=audit(1665822914.169:322): proctitle=2F7573722F7362696E2F6874747064002D44464F524547524F554E44
type=AVC msg=audit(1665822914.169:323): avc: denied { getattr } for pid=39872 comm="httpd" path="/var/www/html/test.html" dev="dm-0" ino=101177494 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:system_u:object_class_t:s0 tclass=file permissive=0
type=SYSCALL msg=audit(1665822914.169:323): arch=c000003e syscall=262 success=no exit=-13 a0=ffffff9c a1=7f3b54007140 a2=7f3b6883f830 a3=100 items=0 ppid=39855 pid=39872 auid=4294967295 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 comm="httpd" exe="/usr/sbin/httpd" subj=system_u:system_r:httpd_t:s0 key=(null)ARCH=x86_64 SYSCALL=newfstatat AUID="unset" UID="apache" GID="apache" EUID="apache" FSUID="apache" FSUID="apache" EGID="apache" SGID="apache" FSGID="apache"
type=PROCTITLE msg=audit(1665822914.169:323): proctitle=2F7573722F7362696E2F6874747064002D44464F524547524F554E44
```

Рис. 15: log-файл

Посмотрела системный лог-файл (рис. 16).

```

Oct 15 11:35:21 lmponomareva setroubleshoot[42230]: SELinux is preventing /usr/sbin/httpd from getattr access
on the 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_sy
s_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient perm
issions to access a parent directory in which case try to change the following command accordingly.#012Do#012#
/sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confidence) suggests
*****#012#012If you want to treat test.html as public content#012Then you need to change the la
bel on test.html to public_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_content
_t '/var/www/html/test.html' #012# restorecon -v '/var/www/html/test.html' #012#012***** Plugin catchall (1.41
confidence) suggests *****#012#012If you believe that httpd should be allowed getattr a
ccess on the test.html file by default.#012Then you should report this as a bug.#012You can generate a local p
olicy module to allow this access.#012Do#012allow this access for now by executing:#012# ausearch -c 'httpd' -
-raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012

```

Рис. 16: Системный log-файл

Можем видеть как отображаются ошибки.

16. Попробовала запустить веб-сервер Apache на прослушивание TCP-порта 81 (рис. 17).

```

GNU nano 5.6.1 /etc/httpd/conf/httpd.conf
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# 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

```

Рис. 17: Включение прослушивания 81 порта

17. Выполнила перезапуск веб-сервера Apache и посмотрела лог-файлы (рис. 18-рис. 21).

```
[root@lmponomareva lmponomareva]# tail -l /var/log/messages
Oct 15 11:41:38 lmponomareva gnome-shell[1681]: Window manager warning: Wl appears to be one of the offending windows with a timestamp of 9476651. Working around...
Oct 15 11:42:14 lmponomareva gnome-shell[1681]: Window manager warning: last_user_time (9512828) is greater than comparison timestamp (9512827). This most likely represents a buggy client sending inaccurate timestamps in messages such as _NET_ACTIVE_WINDOW. Trying to work around...
Oct 15 11:42:14 lmponomareva gnome-shell[1681]: Window manager warning: Wl appears to be one of the offending windows with a timestamp of 9512828. Working around...
Oct 15 11:42:17 lmponomareva systemd[1]: Stopping The Apache HTTP Server...
Oct 15 11:42:18 lmponomareva systemd[1]: httpd.service: Deactivated successfully.
Oct 15 11:42:18 lmponomareva systemd[1]: Stopped The Apache HTTP Server.
Oct 15 11:42:18 lmponomareva systemd[1]: httpd.service: Consumed 4.414s CPU time.
Oct 15 11:42:18 lmponomareva systemd[1]: Starting The Apache HTTP Server...
Oct 15 11:42:18 lmponomareva systemd[1]: Started The Apache HTTP Server.
Oct 15 11:42:18 lmponomareva httpd[42363]: Server configured, listening on: port 81
[root@lmponomareva lmponomareva]#
```

Рис. 18: Лог-файл /var/log/messages

```
[root@lmponomareva lmponomareva]# tail -l /var/log/httpd/error_log
[Sat Oct 15 09:54:43.919307 2022] [lbmethod_heartbeat:notice] [pid 39855:tid 39855] AH02282: No slotmem from mod_heartbeat
[Sat Oct 15 09:54:43.977871 2022] [mpm_event:notice] [pid 39855:tid 39855] AH00489: Apache/2.4.51 (Rocky Linux) configured -- resuming normal operations
[Sat Oct 15 09:54:43.977917 2022] [core:notice] [pid 39855:tid 39855] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[Sat Oct 15 11:35:14.170179 2022] [core:error] [pid 39872:tid 40033] (13)Permission denied: [client 127.0.0.1:49236] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Sat Oct 15 11:42:17.584868 2022] [mpm_event:notice] [pid 39855:tid 39855] AH00492: caught SIGWINCH, shutting down gracefully
[Sat Oct 15 11:42:18.825169 2022] [core:notice] [pid 42363:tid 42363] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Sat Oct 15 11:42:18.827985 2022] [suexec:notice] [pid 42363:tid 42363] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Sat Oct 15 11:42:18.852152 2022] [lbmethod_heartbeat:notice] [pid 42363:tid 42363] AH02282: No slotmem from mod_heartbeat
[Sat Oct 15 11:42:18.880599 2022] [mpm_event:notice] [pid 42363:tid 42363] AH00489: Apache/2.4.51 (Rocky Linux) configured -- resuming normal operations
[Sat Oct 15 11:42:18.880639 2022] [core:notice] [pid 42363:tid 42363] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
```

Рис. 19: Лог-файл /var/log/http/error_log

```
[root@lmponomareva lmponomareva]# tail -l /var/log/httpd/access_log
127.0.0.1 - - [15/Oct/2022:11:08:42 +0300] "GET /test.html HTTP/1.1" 200 35 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
127.0.0.1 - - [15/Oct/2022:11:08:43 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/test.html" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
127.0.0.1 - - [15/Oct/2022:11:35:14 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
127.0.0.1 - - [15/Oct/2022:11:35:15 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/test.html" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
[root@lmponomareva lmponomareva]#
```

Рис. 20: Лог-файл /var/log/http/access_log


```

type=SERVICE_STOP msg=audit(1665822931.382:326): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:syst
em_r:init t:s0 msg='unit=dbus-:1.10-org.fedoraproject.SetroubleshootPrivileged@0 comm="systemd" exe="/usr/lib/
systemd/systemd" hostname=? addr=? terminal=? res=failed'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1665822931.597:327): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:syst
em_r:init t:s0 msg='unit=dbus-:1.10-org.fedoraproject.Setroubleshootd@0 comm="systemd" exe="/usr/lib/systemd/s
ystemd" hostname=? addr=? terminal=? res=failed'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1665823338.681:328): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:syst
em_r:init t:s0 msg='unit=httpd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res
=success'UID="root" AUID="unset"
type=SERVICE_START msg=audit(1665823338.853:329): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:sys
tem_r:init t:s0 msg='unit=httpd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res
=success'UID="root" AUID="unset"

```

Рис. 21: Лог-файл /var/log/audit/audit.log

18. Добавила порт 81 в список портов. (рис. 22).

```

[root@lmponomareva lmponomareva]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@lmponomareva lmponomareva]# 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

```

Рис. 22: Список портов

19. Запустила веб-сервер Apache ещё раз. (рис. 23).

```

GNU nano 5.6.1 /etc/httpd/conf/httpd.conf
#
# 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 80

```

Рис. 23: Перезапуск Apache

20. Вернула контекст httpd_sys_content__t к файлу /var/www/html/ test.html: (рис. 24).

```
[root@lmponomareva lmponomareva]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@lmponomareva lmponomareva]#
```

Рис. 24: Контекст файла

Попробовала получить доступ к файлу через веб-сервер по 81 порту (рис. 25).

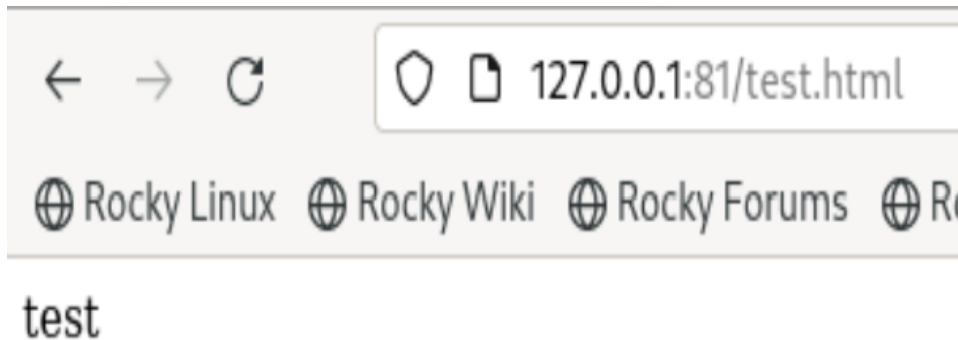


Рис. 25: Доступ по другому порту

21. Исправила обратно конфигурационный файл apache (рис. 26).

```
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf
#
# 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 80
```

Рис. 26: Конфигурационный файл Apache

22. Попробовала удалить привязку http_port_t к 81 порту (рис. 27).

```
[root@lmponomareva lmponomareva]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@lmponomareva lmponomareva]#
```

Рис. 27: Удаление порта из списка

23. Удалила файл /var/www/html/test.html (рис. 28).

```
[root@lmponomareva lmponomareva]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@lmponomareva lmponomareva]#
```

Рис. 28: Удаление файла

Выводы

Получили практическое знакомство с технологией SELinux¹. Проверили работу SELinx на практике совместно с веб-сервером Apache.

Список литературы

1. Основы безопасности информационных систем : Учеб. пособие для студентов вузов, обучающихся по специальностям “Компьютер. безопасность” и “Комплекс. обеспечение информ. безопасности автоматизир. систем” / Д.А. Зегжда, А.М. Ивашко. - М. : Горячая линия - Телеком, 2000. - 449, [2] с. : ил., табл.; 21 см.; ISBN 5-93517-018-3.