

Отчёт по лабораторной работе

Лабораторная работа №_06 / Мандатное разграничение прав в Linux

Габриэль Тьерри

Содержание

| | |
|--------------------------------|----|
| Цель работы | 5 |
| Выполнение лабораторной работы | 6 |
| Выводы | 14 |

Список таблиц

Список иллюстраций

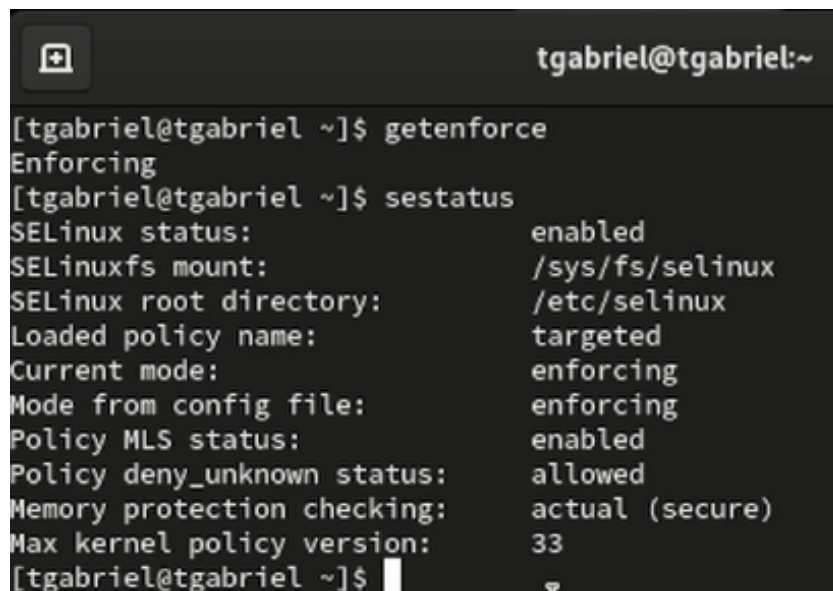
| | | |
|----|---------------------------|----|
| 1 | изображение 001 | 6 |
| 2 | изображение 002 | 7 |
| 3 | изображение 003 | 7 |
| 4 | изображение 004 | 8 |
| 5 | изображение 005 | 8 |
| 6 | изображение 006 | 9 |
| 7 | изображение 007 | 9 |
| 8 | изображение 008 | 10 |
| 9 | изображение 009 | 10 |
| 10 | изображение 010 | 11 |
| 11 | изображение 011 | 11 |
| 12 | изображение 012 | 12 |
| 13 | изображение 013 | 12 |
| 14 | изображение 014 | 13 |
| 15 | изображение 015 | 13 |
| 16 | изображение 016 | 13 |

Цель работы

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

Выполнение лабораторной 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`.

A terminal window with a dark background. The title bar shows a window icon and the text 'tgabriel@tgabriel:~'. The terminal content shows the user running 'getenforce' which returns 'Enforcing', and then 'sestatus' which returns a detailed status report. The status report indicates SELinux is enabled, the mount point is /sys/fs/selinux, the root directory is /etc/selinux, the loaded policy is targeted, and the current mode is enforcing.

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

Рис. 1: изображение 001

2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: `service httpd status`

```
[tgabriel@tgabriel ~]$ 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 2023-10-14 19:10:22 MSK; 6min ago
     Docs: man:httpd.service(8)
  Main PID: 3017 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0"
    Tasks: 213 (limit: 12146)
   Memory: 33.3M
      CPU: 583ms
   CGroup: /system.slice/httpd.service
           └─3017 /usr/sbin/httpd -DFOREGROUND
             └─3018 /usr/sbin/httpd -DFOREGROUND
               └─3022 /usr/sbin/httpd -DFOREGROUND
                 └─3023 /usr/sbin/httpd -DFOREGROUND
                   └─3025 /usr/sbin/httpd -DFOREGROUND

Oct 14 19:10:22 tgabriel.localdomain systemd[1]: Starting The Apache HTTP Server:
Oct 14 19:10:22 tgabriel.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 14 19:10:22 tgabriel.localdomain httpd[3017]: Server configured, listening on:
[tgabriel@tgabriel ~]$
```

Рис. 2: изображение 002

3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду `ps auxZ | grep httpd` или `ps -eZ | grep httpd`

```
[tgabriel@tgabriel ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      3017   0.0  0.5 20328 11660 ?
Ss  19:10   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3018   0.0  0.3 21664 7540 ?
S   19:10   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3022   0.0  0.8 1210612 17220 ?
Sl  19:10   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3023   0.0  0.6 1079476 13132 ?
Sl  19:10   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3025   0.0  0.7 1079476 15176 ?
Sl  19:10   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 tgabriel 3373 0.0  0.1 221
664 2236 pts/0 S+ 19:17   0:00 grep --color=auto httpd
[tgabriel@tgabriel ~]$
```

Рис. 3: изображение 003

4. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd` Обратите внимание, что многие из них находятся в положении «off».

```
[tgabriel@tgabriel ~]$ sestatus -b httpd
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

Policy booleans:
abrt_anon_write               off
abrt_handle_event             off
abrt_upload_watch_anon_write  on
antivirus_can_scan_system     off
antivirus_use_jit             off
auditadm_exec_content         on
authlogin_nsswitch_use_ldap    off
authlogin_radius              off
authlogin_yubikey             off
```

Рис. 4: изображение 004

5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов.
6. Определите тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www`
7. Определите тип файлов, находящихся в директории `/var/www/html`: `ls -lZ /var/www/html`
8. Определите круг пользователей, которым разрешено создание файлов в директории `/var/www/html`.

```
[tgabriel@tgabriel ~]$ 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 23
:21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 May 16 23
:21 html
[tgabriel@tgabriel ~]$ ls -lZ /var/www/html
total 0
```

Рис. 5: изображение 005

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

test

```
[tgabriel@tgabriel ~]$ su
Password:
[root@tgabriel tgabriel]# touch /var/www/html/test.html
[root@tgabriel tgabriel]# vim /var/www/html/test.html
[root@tgabriel tgabriel]# cat /var www/html/test.html
cat: /var: Is a directory
cat: www/html/test.html: No such file or directory
[root@tgabriel tgabriel]# cat /var/www/html/test.html
<html>
    <body>test</body>
</html>
```

Рис. 6: изображение 006

10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории `/var/www/html`.
11. Обратитесь к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедитесь, что файл был успешно отображён.

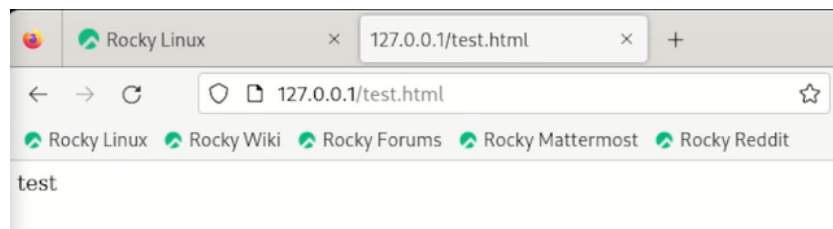


Рис. 7: изображение 007

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. ls -Z /var/www/html/test.html`
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: `chcon -t samba_share_t /var/www/html/test.html` `ls -Z /var/www/html/test.html` После этого проверьте, что контекст поменялся.

```
[root@tgabriel tgabriel]# man httpd_selinux
No manual entry for httpd_selinux
[root@tgabriel tgabriel]# ls -z /var/www/html/test.html
ls: invalid option -- 'z'
Try 'ls --help' for more information.
[root@tgabriel tgabriel]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@tgabriel tgabriel]# chcon -t samba_share_t /var/www/html/test.html
[root@tgabriel tgabriel]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@tgabriel tgabriel]#
```

Рис. 8: изображение 008

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: `Forbidden You don't have permission to access /test.html on this server.`

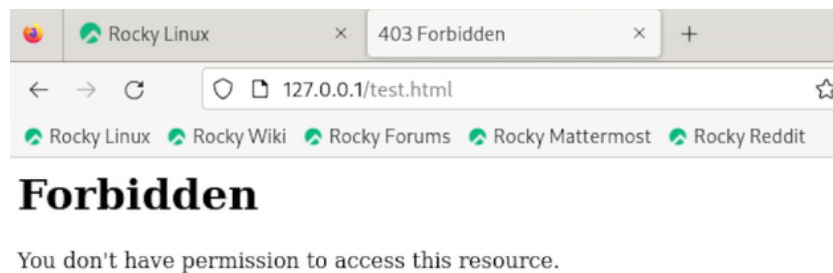


Рис. 9: изображение 009

15. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? `ls -l /var/www/html/test.html` Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный log-файл: `tail /var/log/messages` Если в системе окажутся запущенными процессы `setroubleshootd` и `audtd`, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле `/var/log/audit/audit.log`. Проверьте это утверждение самостоятельно.

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`.

```
[root@tgabriel tgabriel]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 34 Oct 14 19:27 /var/www/html/test.html
[root@tgabriel tgabriel]# tail /var/log/messages
Oct 14 19:54:13 tgabriel gnome-shell[1689]: libinput error: event5 - VirtualBox
mouse integration: client bug: event processing lagging behind by 21ms, your sy
stem is too slow
Oct 14 19:54:16 tgabriel systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootP
rivileged@0.service: Deactivated successfully.
Oct 14 19:54:16 tgabriel systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootP
rivileged@0.service: Consumed 4.746s CPU time.
Oct 14 19:54:16 tgabriel systemd[1]: setroubleshootd.service: Deactivated succes
sfully.
Oct 14 19:54:16 tgabriel systemd[1]: setroubleshootd.service: Consumed 4.391s CP
U time.
Oct 14 19:54:32 tgabriel systemd[1]: Starting dnf makecache...
Oct 14 19:54:37 tgabriel dnf[4362]: Metadata cache refreshed recently.
Oct 14 19:54:37 tgabriel systemd[1]: dnf-makecache.service: Deactivated successf
ully.
Oct 14 19:54:38 tgabriel systemd[1]: Finished dnf makecache.
Oct 14 19:54:38 tgabriel systemd[1]: dnf-makecache.service: Consumed 2.127s CPU
time.
[root@tgabriel tgabriel]# vim /etc/httpd/http.conf
[root@tgabriel tgabriel]# vim /etc/http.conf
[root@tgabriel tgabriel]# vim /etc/httpd/conf/httpd.conf
```

Рис. 10: изображение 010

```
tgabriel@tgabriel:/home/tgabriel — vim /etc/httpd/conf/httpd....
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
ServerRoot "/etc/httpd"

#
# 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

#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
#
```

Рис. 11: изображение 011

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

18. Проанализируйте лог-файлы: `tail -n1 /var/log/messages` Просмотрите файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log` и выясните, в каких файлах появились записи.

```
[root@tgabriel tgabriel]# tail -n1 /var/log/httpd/error_log
[Sat Oct 14 19:53:41.914934 2023] [core:error] [pid 4217:tid 4272] (13)Permissio
n denied: [client 127.0.0.1:56766] AH00035: access to /test.html denied (filesys
tem path '/var/www/html/test.html') because search permissions are missing on a
component of the path
[root@tgabriel tgabriel]# tail -n1 /var/log/httpd/access_log
127.0.0.1 - - [14/Oct/2023:19:53:41 +0300] "GET /test.html HTTP/1.1" 403 199 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
[root@tgabriel tgabriel]# tail -n1 /var/log/audit/audit.log
type=SERVICE_STOP msg=audit(1697302478.008:238): pid=1 uid=0 auid=4294967295 ses
=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dnf-makecache comm="syste
md" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID=
"root" AUID="unset"
```

Рис. 12: изображение 012

19. Выполните команду `semanage port -a -t http_port_t -p tcp 81` После этого про-
верьте список портов командой `semanage port -l | grep http_port_t` Убедитесь,
что порт 81 появился в списке.

```
[root@tgabriel tgabriel]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@tgabriel tgabriel]# semanage port -l | grep http_port_t
semanage port: error: one of the arguments -a/--add -d/--delete -m/--modify -l/-
-list -E/--extract -D/--deleteall is required
[root@tgabriel tgabriel]# 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@tgabriel tgabriel]#
```

Рис. 13: изображение 013

20. Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему он
сейчас запустился, а в предыдущем случае не смог?
21. Верните контекст `httpd_sys_content__t` к файлу `/var/www/html/test.html`:
`chcon -t httpd_sys_content_t /var/www/html/test.html` После этого попро-
буйте 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».

```
[root@tgabriel tgabriel]# systemctl restart httpd
[root@tgabriel tgabriel]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@tgabriel tgabriel]#
```

Рис. 14: изображение 014

22. Исправьте обратно конфигурационный файл apache, вернув Listen 80.

```
#
# 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 80

#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
# to be loaded here.
#
# Example:
-- INSERT --
```

Рис. 15: изображение 015

23. Удалите привязку http_port_t к 81 порту: semanage port -d -t http_port_t -p tcp 81 и проверьте, что порт 81 удалён.
24. Удалите файл /var/www/html/test.html: rm /var/www/html/test.html

```
[root@tgabriel tgabriel]# vim /etc/httpd/conf/httpd.conf
[root@tgabriel tgabriel]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@tgabriel tgabriel]# 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@tgabriel tgabriel]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@tgabriel tgabriel]#
```

Рис. 16: изображение 016

Выводы

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