

Лабораторная работа №6

Мандатное разграничение прав в Linux

Калинина Кристина Сергеевна

Содержание

Цель работы	5
Теоретические сведения	6
Выполнение лабораторной работы	7
Выводы	15
Список литературы	16

List of Figures

0.1	Проверка SELinux	7
0.2	Проверка Apache	8
0.3	переключатели SELinux для Apache	8
0.4	Статистика по политике	9
0.5	Множество пользователей, ролей и типов	10
0.6	Просмотр информации	11
0.7	Создание html-файл	11
0.8	Контекст html-файла, заданный по умолчанию	11
0.9	Успешное чтение файла через веб-сервер	11
0.10	Изменение контекста html-файла	12
0.11	Ошибка доступа к файлу	12
0.12	Просмотр прав файла и системного лог-файла	12
0.13	Смена TSP-порта	13
0.14	Перезапуск Apache	13
0.15	Просмотр списка портов	13
0.16	Смена контекста файла	13
0.17	Просмотр файла через 81 порт	14
0.18	Восстановление файла	14
0.19	Попытка удаления привязки http_port_t к 81 порту и удаление файла	14

List of Tables

Цель работы

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

Теоретические сведения

Чтобы преодолеть ограничения и расширить механизмы безопасности, предоставляемые стандартными разрешениями `ugo / rwx` и списками контроля доступа, Агентство национальной безопасности США (NSA) разработало гибкий метод мандатного контроля доступа (MAC), известный как SELinux (сокращение от Security Enhanced Linux) для того, чтобы, между прочим, ограничивать способность процессов получать доступ или выполнять другие операции над системными объектами (такими как файлы, каталоги, сетевые порты и т. д.) с наименьшими возможными правами, при этом допуская возможность последующих модификаций этой модели. [1]

Security Enhanced Linux может работать двумя различными способами:

- Enforcing: SELinux запрещает доступ на основе правил политики SELinux, набора руководящих принципов, которые управляют механизмом безопасности.
- Permissive: SELinux не запрещает доступ, но в журнале регистрируются отказы для действий, которые были бы запрещены при запуске в принудительном режиме. [1]

Выполнение лабораторной работы

1. Вошла в систему с полученными учётными данными, провела подготовку к работе и убедилась, что SELinux работает в режиме enforcing политики targeted (fig. 0.1).

```
[root@kskalinina conf]# 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
Max kernel policy version:     31
[root@kskalinina conf]# getenforce
Enforcing
```

Figure 0.1: Проверка SELinux

2. Убедилась, что веб-сервис работает, а также посмотрела список процессов (fig. 0.2).

```
[root@kskalinina conf]# 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 preset: disabled)
   Active: active (running) since Co 2021-11-27 13:46:48 MSK; 1h 48min ago
     Docs: man:httd(8)
           man:apachectl(8)
   Main PID: 21007 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic: 0 B/sec"
    Tasks: 6
   CGroup: /system.slice/httpd.service
           └─21007 /usr/sbin/httpd -DFOREGROUND
             └─21011 /usr/sbin/httpd -DFOREGROUND
               └─21012 /usr/sbin/httpd -DFOREGROUND
                 └─21013 /usr/sbin/httpd -DFOREGROUND
                   └─21014 /usr/sbin/httpd -DFOREGROUND
                     └─21015 /usr/sbin/httpd -DFOREGROUND

ноя 27 13:46:47 kskalinina.localdomain systemd[1]: Starting The Apache HTTP Server...
ноя 27 13:46:48 kskalinina.localdomain httpd[21007]: AH00558: httpd: Could not reliably determine the server's fully qu...ssage
ноя 27 13:46:48 kskalinina.localdomain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[root@kskalinina conf]# ps -eZ | grep httpd
system_u:system_r:httpd_t:s0 21007 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 21011 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 21012 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 21013 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 21014 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 21015 ? 00:00:00 httpd
```

Figure 0.2: Проверка Apache

- Посмотрела текущее состояние переключателей SELinux для Apache, многие из них находятся в положении «off» (fig. 0.3).

```
[root@kskalinina conf]# sestatus -b | 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_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 on
httpd_manage_ipa off
httpd_mod_auth_ntlm_winbind off
httpd_mod_auth_pam off
httpd_read_user_content off
httpd_run_ipa off
httpd_run_preupgrade off
httpd_run_stickshift off
httpd_serve_cobbler_files off
```

Figure 0.3: переключатели SELinux для Apache

4. Посмотрела статистику по политике с помощью команды `seinfo`, также определила множество пользователей, ролей, типов (fig. 0.4, fig. 0.5).

```
[root@kskalinina conf]# seinfo

Statistics for policy file: /sys/fs/selinux/policy
Policy Version & Type: v.31 (binary, mls)

Classes:          130      Permissions:       272
Sensitivities:    1        Categories:       1024
Types:           4793     Attributes:        253
Users:            8        Roles:             14
Booleans:        316     Cond. Expr.:      362
Allow:          107834    Neverallow:        0
Auditallow:      158     Dontaudit:         10022
Type_trans:     18153    Type_change:        74
Type_member:     35      Role_allow:         37
Role_trans:     414     Range_trans:       5899
Constraints:     143     Validatetrans:      0
Initial SIDs:    27      Fs_use:             32
Genfscon:        103     Portcon:            614
Netifcon:         0      Nodecon:             0
Permissives:     0       Polcap:              5
```

Figure 0.4: Статистика по политике

```

[root@kskalinina conf]# seinfo -u

Users: 8
  sysadm_u
  system_u
  xguest_u
  root
  guest_u
  staff_u
  user_u
  unconfined_u
[root@kskalinina conf]# seinfo -r

Roles: 14
  auditadm_r
  dbadm_r
  guest_r
  staff_r
  user_r
  logadm_r
  object_r
  secadm_r
  sysadm_r
  system_r
  webadm_r
  xguest_r
  nx_server_r
  unconfined_r
[root@kskalinina conf]# seinfo -t

Types: 4793
  bluetooth_conf_t
  cmirrord_exec_t
  colord_exec_t
  container_auth_t
  foghorn_exec_t
  jacorb_port_t
  pki_ra_exec_t

```

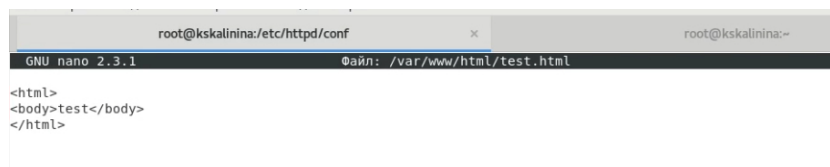
Figure 0.5: Множество пользователей, ролей и типов

5. Просмотрела файлы и поддиректории, находящиеся в директориях “/var/www” и “/var/www/html”. Увидела, что суперпользователь имеет разрешение на создание файлов в директории “/var/www/html” (fig. 0.6).

```
[root@kskalinina conf]# ls -lZ /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[root@kskalinina conf]# ls -lZ /var/www/html
```

Figure 0.6: Просмотр информации

6. Создала от имени суперпользователя html-файл (fig. 0.7).



```
root@kskalinina:/etc/httpd/conf
GNU nano 2.3.1 Файл: /var/www/html/test.html

<html>
<body>test</body>
</html>
```

Figure 0.7: Создание html-файл

7. Проверила контекст созданного файла (fig. 0.8).

```
[root@kskalinina conf]# nano /var/www/html/test.html
[root@kskalinina conf]# ls -lZ /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
```

Figure 0.8: Контекст html-файла, заданный по умолчанию

8. Обратилась к файлу через веб-сервер, убедилась, что файл был успешно отображён (fig. 0.9).

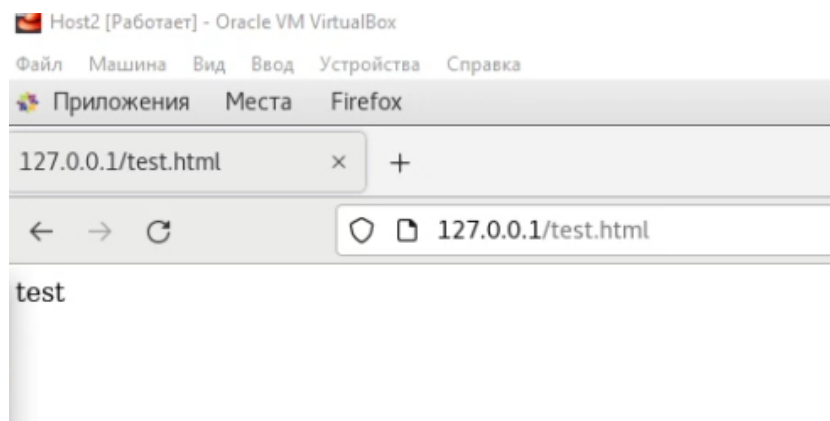


Figure 0.9: Успешное чтение файла через веб-сервер

9. Изменила контекст файла с `httpd_sys_content_t` на `samba_share_t` и проверила это (fig. 0.10).

```
[root@kskalinina conf]# ls -lZ /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@kskalinina conf]# chcon -t samba_share_t /var/www/html/test.html
[root@kskalinina conf]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

Figure 0.10: Изменение контекста html-файла

10. Попробовала ещё раз получить доступ к файлу через веб-сервер и получила сообщение об ошибке (fig. 0.11).

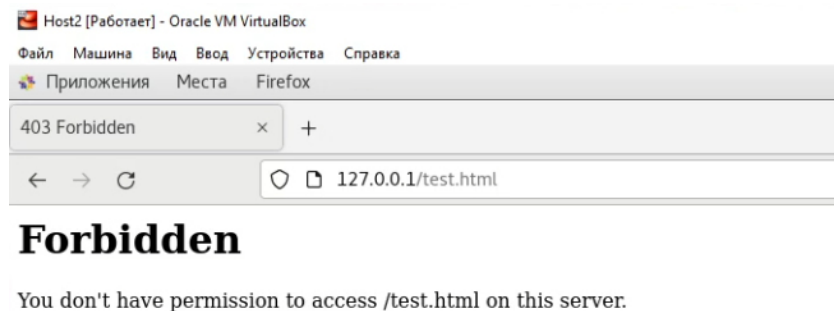


Figure 0.11: Ошибка доступа к файлу

11. Несмотря на то, что все пользователи могут читать файл, но новый контекст не дает домену доступ к файлу, потому и возникает сообщение об ошибке и невозможность посмотреть файл (fig. 0.12).

```
[root@kskalinina conf]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 34 Nov 27 15:42 /var/www/html/test.html
[root@kskalinina conf]# tail /var/log/messages
Nov 27 15:46:15 kskalinina setroubleshoot: SELinux is preventing httpd from getatrr access on the file /var/www/html/test.html. For
r complete SELinux messages run: sealert -l 04185fa9-a41d-4888-a653-cbe4c050ce8d
Nov 27 15:46:15 kskalinina python: SELinux is preventing httpd from getatrr 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_sys_content_t.#012Then you can run restorecon. The access attempt may have been stopped d
ue to insufficient permissions to access a parent directory in which case try to change the following command accordingly.#012Do#0
12# /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 label 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 getatrr access on the test.html file by default.#012Then you should report this as a bug.#012You can gener
ate a local policy module to allow this access.#012Do#012allow this access for now by executing:#012# ausearch -c 'httpd' --raw |
audit2allow -M my-httpd#012# semodule -i my-httpd.pp#012
Nov 27 15:46:27 kskalinina dbus[714]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
Nov 27 15:46:27 kskalinina dbus[714]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
Nov 27 15:46:27 kskalinina setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Nov 27 15:46:27 kskalinina setroubleshoot: SELinux is preventing httpd from getatrr access on the file /var/www/html/test.html. Fo
r complete SELinux messages run: sealert -l 04185fa9-a41d-4888-a653-cbe4c050ce8d
Nov 27 15:46:27 kskalinina python: SELinux is preventing httpd from getatrr 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_sys_content_t.#012Then you can run restorecon. The access attempt may have been stopped d
ue to insufficient permissions to access a parent directory in which case try to change the following command accordingly.#012Do#0
12# /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 label 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 getatrr access on the test.html file by default.#012Then you should report this as a bug.#012You can gener
ate a local policy module to allow this access.#012Do#012allow this access for now by executing:#012# ausearch -c 'httpd' --raw |
audit2allow -M my-httpd#012# semodule -i my-httpd.pp#012
Nov 27 15:50:01 kskalinina systemd: Created slice User Slice of root.
Nov 27 15:50:01 kskalinina systemd: Started Session 18 of user root.
Nov 27 15:50:02 kskalinina systemd: Removed slice User Slice of root.
```

Figure 0.12: Просмотр прав файла и системного лог-файла

12. Попробовала запустить веб-сервер Apache на прослушивание TCP-порта 81 (fig. 0.13).

```

root@kskalinina:/etc/httpd/conf
GNU nano 2.3.1 Файл: /etc/httpd/conf/httpd.conf

#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
# 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.

```

Figure 0.13: Смена TCP-порта

13. Выполнила перезапуск веб-сервера Apache, всё прошло успешно, т.к. 81 порт по умолчанию был в списке портов (fig. 0.14, fig. 0.15).

```

[root@kskalinina conf]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@kskalinina conf]# 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 preset: disabled)
   Active: active (running) since C6 2021-11-27 15:53:18 MSK; 9s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 27629 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=0/SUCCESS)
 Main PID: 27635 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic: 0 B/sec"
    Tasks: 6
   CGroup: /system.slice/httpd.service
           └─27635 /usr/sbin/httpd -DFOREGROUND
             └─27636 /usr/sbin/httpd -DFOREGROUND
               └─27637 /usr/sbin/httpd -DFOREGROUND
                 └─27638 /usr/sbin/httpd -DFOREGROUND
                   └─27639 /usr/sbin/httpd -DFOREGROUND
                     └─27640 /usr/sbin/httpd -DFOREGROUND

ноя 27 15:53:18 kskalinina.localdomain systemd[1]: Stopped The Apache HTTP Server.
ноя 27 15:53:18 kskalinina.localdomain systemd[1]: Starting The Apache HTTP Server...
ноя 27 15:53:18 kskalinina.localdomain systemd[1]: Started The Apache HTTP Server.

```

Figure 0.14: Перезапуск Apache

```

Nov 27 15:50:01 kskalinina systemd: Created slice User Slice of root.
Nov 27 15:50:01 kskalinina systemd: Started Session 18 of user root.
Nov 27 15:50:02 kskalinina systemd: Removed slice User Slice of root.
Nov 27 15:53:17 kskalinina systemd: Stopping The Apache HTTP Server...
Nov 27 15:53:18 kskalinina systemd: Stopped The Apache HTTP Server.
Nov 27 15:53:18 kskalinina systemd: Starting The Apache HTTP Server...
Nov 27 15:53:18 kskalinina systemd: Started The Apache HTTP Server.
[root@kskalinina 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

```

Figure 0.15: Просмотр списка портов

14. Вернула контекст httpd_sys_content__t файлу и попробовала получить доступ к файлу через 81 порт (fig. 0.16, fig. 0.17).

```

[root@kskalinina conf]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@kskalinina conf]# ls -Z /var/www/html/test.html
-rw-r--r-- root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html

```

Figure 0.16: Смена контекста файла

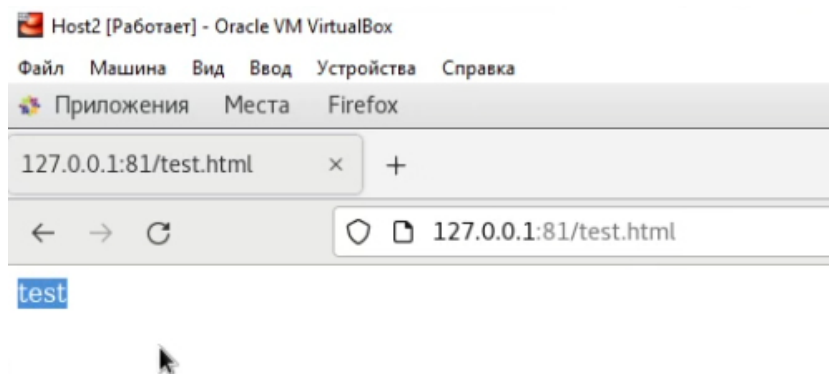


Figure 0.17: Просмотр файла через 81 порт

15. Исправила обратно конфигурационный файл apache (fig. 0.18).

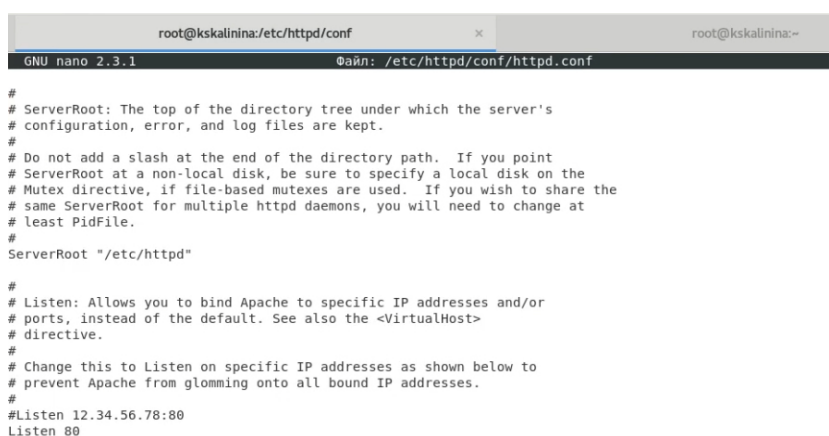


Figure 0.18: Восстановление файла

16. Попыталась удалить привязку `http_port_t` к 81 порту и удалила созданный файл (fig. 0.19).

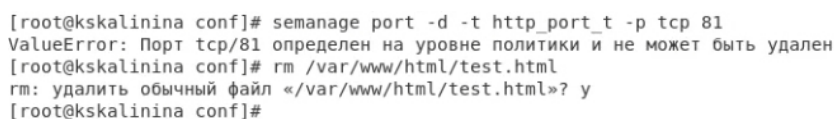


Figure 0.19: Попытка удаления привязки `http_port_t` к 81 порту и удаление файла

Выводы

Таким образом я успешно познакомилась с технологией SELinux и проверила работу SELinux на практике совместно с веб-сервером Apache.

Список литературы

1. Реализация мандатного контроля доступа. // itsecforu.ru 2019. URL:
<https://itsecforu.ru/2019/07/25/%F0%9F%9B%A1%EF%B8%8F-%D1%80%D0%B5%D0%B0%D0%BC%D0%B0%D0%BD%D0%B4%D0%B0%D1%82%D0%BD%D0%BE%D0%B3%D0%BE-%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8F-%D0%B4/> (дата обращения 27.11.2021).
2. Д. С. Кулябов, А. В. Королькова, М. Н. Геворкян. Информационная безопасность компьютерных сетей: лабораторные работы. // Факультет физико-математических и естественных наук. М.: РУДН, 2015. 64 с..