

Лабораторная работа № 6. Мандатное разграничение прав в Linux

Радикорский Павел Михайлович НФИбд-03-18

15.11.2021

RUDN University, Moscow, Russian Federation

Цели и задачи

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

Выполнение

Процесс выполнения

Вошли в систему с полученными учётными данными и убедились, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`. Обратились с помощью консоли к веб-серверу, запущенному на вашем компьютере, запустили сервер

```
[root@10 httpd]# getenforce
Enforcing
[root@10 httpd]# 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
[root@10 httpd]# 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: enabled)
   Active: inactive (dead)
     Docs: man:httpd.service(8)

lines 1-4/4 (END)
```

Рис. 1: `getenforce`, `sestatus`, `httpd status`

Процесс выполнения

Нашли веб-сервер Apache в списке процессов, определили его контекст безопасности — `unconfined_u`, `unconfined_r`, `unconfined_t`

```
[radix.localdomain@10 ~]$ ps auxZ | grep httpd
system u:system r:httpd t:s0 root 3951 0.0 0.2 280184 11376 ?
Ss 12:39 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 3958 0.0 0.2 294064 8444 ?
S 12:39 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 3959 0.1 0.3 1810616 12140 ?
Sl 12:39 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 3961 0.1 0.5 1941744 20252 ?
Sl 12:39 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 3963 0.0 0.3 1810616 12140 ?
Sl 12:39 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 radix.l+ 4191 0.0 0.2 303
256 8320 pts/1 S+ 12:40 0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 radix.l+ 4258 0.0 0.0 221
928 1128 pts/0 S+ 12:40 0:00 grep --color=auto httpd
```

Рис. 2: контекст безопасности

Процесс выполнения

Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -b httpd`

```
virt_use_usb          on
virt_use_xserver      off
webadm_manage_user_files off
webadm_read_user_files off
wine_mmap_zero_ignore off
xdm_bind_vnc_tcp_port  off
xdm_exec_bootloader   off
xdm_sysadm_login       off
xdm_write_home         off
xen_use_nfs            off
xend_run_blkmap        on
xend_run_gemu          on
xgquest_connect_network on
xgquest_exec_content   on
xgquest_mount_media    on
xgquest_use_bluetooth  on
xserver_clients_write_xshm off
xserver_execmem        off
xserver_object_manager off
zabbix_can_network     off
zabbix_run_sudo        off
zarafe_setrlimit       off
zebra_write_config     off
zoneminder_anon_write  off
zoneminder_run_sudo    off
```

Рис. 3: `sestatus -b httpd`

Процесс выполнения

Посмотрели статистику по политике с помощью команды `seinfo`, также определили множество пользователей, ролей, ТИПОВ

```
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          31 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:                132  Permissions:             463
Sensitivities:          1    Categories:             1024
Types:                  4934  Attributes:              252
Users:                  8     Roles:                   14
Booleans:               337   Cond. Expr.:            383
Allow:                  110939 Neverallow:               0
Auditallow:             163   Dontaudit:              10255
Type_trans:             244537 Type_change:              87
Type_member:            35    Range_trans:            6015
Role_allow:             37    Role_trans:              422
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:                 640
Netifcon:               0     Nodecon:                  0
```

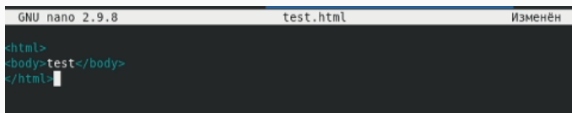
Рис. 4: статистика

Определили тип файлов и поддиректорий, находящихся в директории /var/www

```
[radix.localdomain@10 ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 окт 13 02
:38 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 окт 13 02
:38 html
[radix.localdomain@10 ~]$ cd /var/www/html
[radix.localdomain@10 html]$ cd ..
[radix.localdomain@10 www]$ ls -l
итого 0
drwxr-xr-x. 2 root root 6 окт 13 02:38 cgi-bin
drwxr-xr-x. 2 root root 6 окт 13 02:38 html
```

Рис. 5: типы файлов и поддиректорий

Создали от имени суперпользователя html-файл /var/www/html/test.html следующего содержания

A screenshot of a terminal window showing the GNU nano 2.9.8 text editor. The editor is editing a file named test.html, which is marked as 'Изменён' (Modified). The content of the file is a simple HTML document with a body containing the word 'test'.

```
GNU nano 2.9.8 test.html Изменён
<html>
<body>test</body>
</html>
```

Рис. 6: test.html

Проверили контекст созданного вами файла. По умолчанию присваивается `httpd_sys_content_t`

```
[root@10 html]# ls -Z test.html  
unconfined u:object r:httpd_sys_content t:s0 test.html
```

Рис. 7: контекст

Обратились к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедились, что файл был успешно отображён

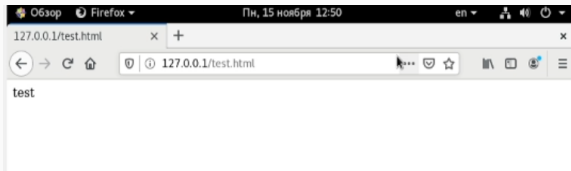


Рис. 8: 127.0.0.1

Проверили контекст файла, сопоставили их с контекстом файлов httpd

```
[root@10 html]# ls -Z test.html  
unconfined u:object r:httpd sys:content t:s0 test.html
```

Рис. 9: контекст

Изменили контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t`, попробовали получить доступ к файлу, получили ошибку

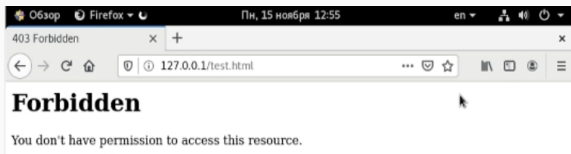


Рис. 10: 127.0.0.1

Процесс выполнения

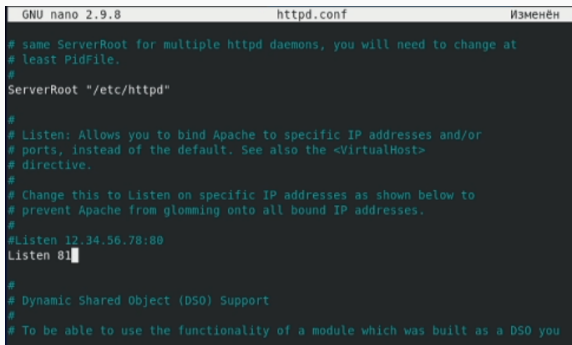
Просмотрели log-файлы веб-сервера Apache. Также просмотрели системный лог-файл: tail /var/log/messages

```
Nov 15 12:55:51 10 setroubleshoot[5547]: failed to retrieve rpm info for /var/www/html/test.html
Nov 15 12:55:51 10 setroubleshoot[5547]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l f549c877-4e64-4bbd-bdbc-94dbd6d251c4
Nov 15 12:55:51 10 setroubleshoot[5547]: 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_sys_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions 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 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 getattr access on the test.html file by default.#012Then you should report this as a bug.#012You can generate 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 -X 300 -i my-httpd.pp#012
```

Рис. 11: messages

Процесс выполнения

Попробовали запустить веб-сервер Apache на прослушивание TCP-порта 81. Для этого в файле `/etc/httpd/httpd.conf` нашли строчку `Listen 80` и заменили её на `Listen 81`



```
GNU nano 2.9.8      httpd.conf      Изменён

# 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 specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#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
```

Рис. 12: http.conf

Выполнили перезапуск сервера Apache, сбоя не произошло

```
[root@10 conf]# sudo systemctl restart httpd.service  
[root@10 conf]#
```

Рис. 13: перезапуск

Выполнили команду `semanage port -a -t http_port_t -p tcp 81`, после этого проверили список портов командой `semanage port -l | grep http_port_t`, убедились, что порт 81 появился в списке.

```
[root@i0 conf]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@i0 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
```

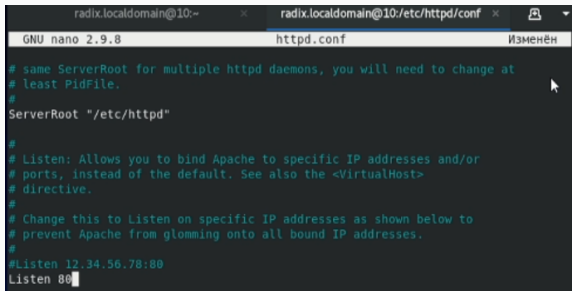
Рис. 14: порт 81

Вернули контекст `httpd_sys_content_t` к файлу
`/var/www/html/test.html`: `chcon -t httpd_sys_content_t`
`/var/www/html/test.html`, получили доступ к файлу

```
[root@10 ~]# chcon -t httpd_sys_content_t /var/www/html/test.html  
[root@10 ~]#
```

Рис. 15: КОНТЕКСТ

Вернули обратно порт 80 в файле конфигурации



The screenshot shows a terminal window with two tabs. The active tab is titled 'radix.localdomain@10:/etc/httpd/conf' and shows the 'httpd.conf' file being edited with 'GNU nano 2.9.8'. The file content includes comments about ServerRoot, Listen, and VirtualHost directives. The current line being edited is 'Listen 80', with the cursor at the end of the line. The status bar at the bottom right of the editor indicates 'Изменён' (Changed).

```
radix.localdomain@10:~  
radix.localdomain@10:/etc/httpd/conf  
GNU nano 2.9.8 httpd.conf Изменён  
  
# 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 specific IP addresses as shown below to  
# prevent Apache from glomming onto all bound IP addresses.  
#  
#Listen 12.34.56.78:80  
Listen 80
```

Рис. 16: httpd.conf

Удалили привязку http_port_t к 81 порту: semanage port -d -t http_port_t -p tcp 81, удалили файл test.html

```
[root@10 conf]# semanage port -d -t http_port_t -p tcp 81
```

Рис. 17: удаление привязки

Выводы

В результате выполнения работы я развил навыки администрирования ОС Linux, получил первое практическое знакомство с технологией SELinux