

Защита лабораторной работы №6 Мандатное разграничение прав в Linux

Исаханян Эдуард Тигранович

2022 Sep 21th

RUDN University, Moscow, Russian Federation

Защита лабораторной работы №6

Цель

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

Подготовка лабораторного стенда

Параметр ServerName

```
ServerAdmin root@localhost

#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
ServerName test.ru
```

Figure 1: Параметр ServerName

```
Try 'iptables -h' or 'iptables --help' for more information.  
[root@edikisakhayan conf]# iptables -P INPUT ACCEPT  
[root@edikisakhayan conf]# iptables -F  
[root@edikisakhayan conf]# iptables -P OUTPUT ACCEPT
```

Figure 2: Отключение фильтра

```
[root@edikisakhayan conf]# iptables -I INPUT -p tcp --dport 80 -j ACCEPT
[root@edikisakhayan conf]# iptables -I INPUT -p tcp --dport 81 -j ACCEPT
[root@edikisakhayan conf]# iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT
[root@edikisakhayan conf]# iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT
```

Figure 3: Отключение фильтра

Выполнение лабораторной работы

```
[root@edikisakhayan conf]# getenforce
Enforcing
[root@edikisakhayan 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
```

Figure 4: Проверка режима и политики

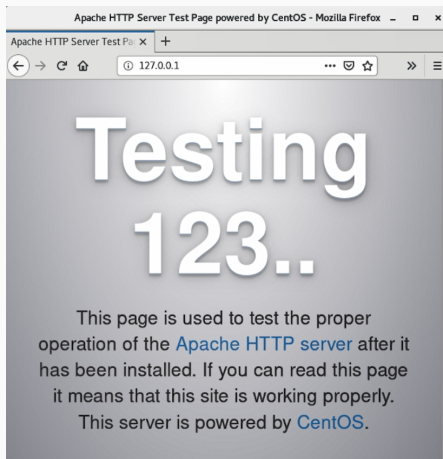


Figure 5: Проверка через браузер

Проверка через браузер

```
[root@edikisakhayan 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 prese
   t: disabled)
   Active: active (running) since Br 2022-09-20 18:38:28 MSK; 1s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Main PID: 6361 (httpd)
    Status: "Processing requests..."
     Tasks: 6
   CGroup: /system.slice/httpd.service
           └─6361 /usr/sbin/httpd -DFOREGROUND
             └─6371 /usr/sbin/httpd -DFOREGROUND
               └─6372 /usr/sbin/httpd -DFOREGROUND
                 └─6373 /usr/sbin/httpd -DFOREGROUND
                   └─6374 /usr/sbin/httpd -DFOREGROUND
                     └─6375 /usr/sbin/httpd -DFOREGROUND

сен 20 18:38:28 edikisakhayan.localdomain systemd[1]: Starting The Apache ...
сен 20 18:38:28 edikisakhayan.localdomain systemd[1]: Started The Apache H...
Hint: Some lines were ellipsized, use -l to show in full.
```

Figure 6: Проверка статуса

```
[root@edikisakhayan conf]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 6361 0.1 0.4 224084 5012 ? S
s 18:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 6371 0.0 0.3 226168 3096 ? S
18:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 6372 0.0 0.3 226304 3828 ? S
18:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 6373 0.0 0.3 226304 3832 ? S
18:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 6374 0.0 0.3 226168 3096 ? S
18:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 6375 0.0 0.3 226168 3096 ? S
18:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 6427 0.0 0.3 226168 3096 ? S
18:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 6442 0.0 0.3 226168 3096 ? S
18:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 6443 0.0 0.3 226168 3096 ? S
18:38 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 6445 0.0 0.0 112832
972 pts/1 R+ 18:39 0:00 grep --color=auto httpd
```

Figure 7: веб-сервер Apache

Просмотр переключателей SELinux для Apache

```
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
httpd_setrlimit off
httpd_ssi_exec off
httpd_sys_script_anon_write off
httpd_tmp_exec off
httpd_tty_comm off
httpd_unified off
httpd_use_cifs off
httpd_use_fusefs off
httpd_use_gpg off
httpd_use_nfs off
httpd_use_openstack off
httpd_use_sasl off
httpd_verify_dns off
[root@edkibizhava ~]#
```

Figure 8: Просмотр переключателей SELinux для Apache

```
[root@edikisakhayan 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 9: Статистика

Определение типов файлов и круг пользователей

```
[root@edikisakhayan 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@edikisakhayan conf]# ls -lZ /var/www/html/
[root@edikisakhayan conf]# ls -l /var/www/html/
итого 0
[root@edikisakhayan conf]# ls -l /var/www/
итого 0
drwxr-xr-x. 2 root root 6 map 24 17:58 cgi-bin
drwxr-xr-x. 2 root root 6 map 24 17:58 html
```

Figure 10: Определение типов файлов и круг пользователей


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

Figure 11: Создание файла

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

Figure 12: Проверка

Получение доступа к файлу через браузер

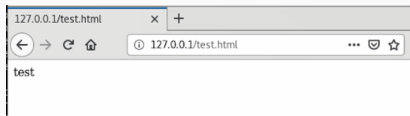


Figure 13: Получение доступа к файлу через браузер

```
[root@edikisakhayan html]# ls -Z test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
[root@edikisakhayan html]# chcon -t samba_share_t /var/www/html/test.html
[root@edikisakhayan html]# 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 14: Изменение контекста, проверка



Figure 15: Получение доступа к файлу через браузер

```
'org.fedoraproject.Setroubleshoot'
```

Sep 20 18:45:43 edikisakhayan setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html

Sep 20 18:45:43 edikisakhayan setroubleshoot: SELinux is preventing httpd from gettingattr access on the file /var/www/html/test.html. For complete SELinux messages run: `sealert -l 499f4863-d847-4b0a-9f13-7c8229dc801f`

Sep 20 18:45:43 edikisakhayan python: SELinux is preventing httpd from gettingattr 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 -i my-httpd.pp#012

Figure 16: Анализ ситуации

Изменение порта 80 на 81

```
#  
# 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  
#
```

Figure 17: Изменение порта 80 на 81

```
[root@edikisakhayan html]# tail -n1 /var/log/messages  
Sep 20 18:47:09 edikisakhayan dbus[733]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
```

Figure 18: Анализ и просмотр лог-файлов


```
[root@edikisakhayan htal]# semanage port -a -t http_port_t -p tcp 81
ValueError: Поп tcp/81 yxe onpegenem
[root@edikisakhayan htal]# 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@edikisakhayan htal]# 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 19: Выполнение и проверка

```
root@edikisakhayan htmlj# chcon -t httpd_sys_content_t /var/www/html/test.html  
root@edikisakhayan htmlj#
```

Figure 20: Возвращение контекста

Получение доступа к файлу через браузер

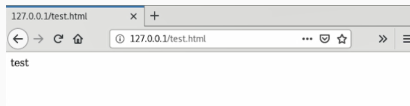


Figure 21: Получение доступа к файлу через браузер

```
#  
# 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  
  
#  
# Dynamic Shared Object (DSO) Support  
#
```

Figure 22: Исправленный файл apache

Удаление привязки к 81 порту и удаление файла

```
[root@edikisakhayan html]# semanage port -d -t http_port_t -p tcp 81
ValueError: порт tcp/81 определен на уровне политики и не может быть удален
[root@edikisakhayan html]# rm /var/www/html/test.html
rm: удалить обычный файл ~/var/www/html/test.html? y
[root@edikisakhayan html]#
```

Figure 23: Удаление привязки к 81 порту и удаление файла

Вывод

В ходе работы, мы развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux. Проверили работу SELinux на практике совместно с веб-сервером Apache.