

Лабораторная работа №6: Мандатное разграничение прав в Linux

дисциплина: Информационная безопасность

Голова Варвара Алексеевна

2021, 25 November

Цель работы

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

Выполнение работы

Убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.

```
[vgoiova@vagoiova ~]$ getenforce
Enforcing
[vgoiova@vagoiova ~]$ 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
```

Figure 1: SELinux

Обратилась с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедилась, что последний работает, предварительно запустив его.

```
[vagalova@vagalova ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[vagalova@vagalova ~]$ 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: active (running) since Thu 2021-11-25 16:37:47 MSK; 3s ago
     Docs: man:httpd.service(8)
  Main PID: 3045 (httpd)
    Status: "Started, listening on: port 80"
    Tasks: 213 (limit: 5840)
   Memory: 24.2M
    CGroup: /system.slice/httpd.service
            └─3045 /usr/sbin/httpd -DFOREGROUND
              └─3057 /usr/sbin/httpd -DFOREGROUND
                └─3058 /usr/sbin/httpd -DFOREGROUND
                  └─3059 /usr/sbin/httpd -DFOREGROUND
                    └─3060 /usr/sbin/httpd -DFOREGROUND

ноя 25 16:37:47 vagalova.localdomain systemd[1]: Starting The Apache HTTP Server:
ноя 25 16:37:47 vagalova.localdomain systemd[1]: Started The Apache HTTP Server:
ноя 25 16:37:47 vagalova.localdomain httpd[3045]: Server configured, listening
lines 1-18/18 (END)
```

Figure 2: Веб-сервер

Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности и занесла эту информацию в отчёт.

```
[vgolova@vagolova ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0      root          3045   0.1  1.1 282900 11712 ?
Ss   16:37   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache        3057   0.0  0.8 296780  8516 ?
S    16:37   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache        3058   0.0  1.0 1354568 10220 ?
Sl   16:37   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache        3059   0.0  1.0 1485596 10220 ?
Sl   16:37   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache        3060   0.0  1.0 1354568 10220 ?
Sl   16:37   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 vgolova 3348 0.0  0.1 1213
G 1196 pts/0 R+  16:38   0:00 grep --color=auto httpd
```

Figure 3: Apache

Текущее состояние переключателей

Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd`. Обратила внимание, что многие из них находятся в положении «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_blktp               on
xend_run_qemu                 on
xguest_connect_network       on
xguest_exec_content          on
xguest_mount_media           on
xguest_use_bluetooth         on
xserver_clients_write_xshm   off
xserver_execrem              off
xserver_object_manager       off
zabbix_can_network           off
zabbix_run_sudo              off
zarafa_setrlimit             off
zebra_write_config           off
zoneminder_anon_write        off
zoneminder_run_sudo          off
lvgolova@vagoLova ~]$
```

Figure 4: Многие находятся в положении “off”

Посмотрела статистику по политике с помощью команды `seinfo`.

```
Policy Version:      31 (MLS enabled)
Target Policy:       selinux
Handle unknown classes: allow
Classes:             132
Sensitivities:       1
Types:               4959
Users:               8
Booleans:            340
Allow:               112885
Auditallow:          166
Type_trans:          253398
Type_member:         35
Role_allow:          38
Constraints:         72
MLS Constrain:       72
Permissives:         0
Defaults:            7
Allowxperm:          0
Auditallowxperm:     0
Ibendportcon:        0
Initial SIDs:        27
Genfscon:            106
Netifcon:            0
Permissions:         463
Categories:          1024
Attributes:          255
Roles:               14
Cond. Expr.:         389
Neverallow:          0
Dontaudit:           10362
Type_change:         87
Range_trans:         6015
Role_trans:          423
Validatetrans:       0
MLS Val. Tran:       0
Polcap:              5
Typebounds:          0
Neverallowxperm:     0
Dontauditxperm:      0
Ibpkeycon:           0
Fs_use:              33
Portcon:             540
Nodecon:             0
```

Figure 5: Статистика

Определила тип файлов и поддиректорий, находящихся в директории /var/www.

```
[vagalova@vagalova ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0  6 ноя 12 0
7:58 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      23 ноя 25 1
1:36 html
```

Figure 6: Директория

Создала от имени суперпользователя html-файл
/var/www/html/test.html.

A screenshot of a terminal window with a dark background. It displays three lines of HTML code in a light green monospaced font: the first line is <html>, the second line is <body>test</body>, and the third line is </html>. The code is left-aligned.

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

Figure 7: Содержимое файла

Проверила контекст созданного мной файла.

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

Figure 8: Контекст

Отображение в браузере

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

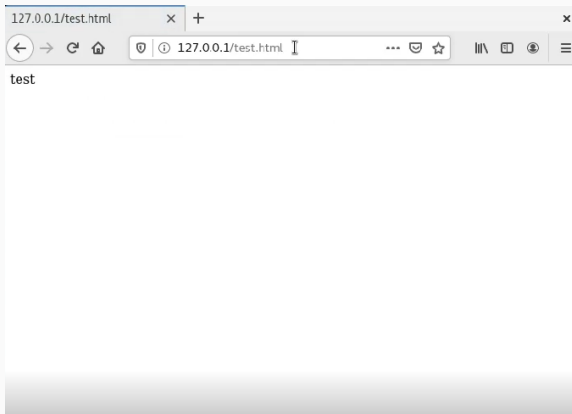


Figure 9: Отображение

Изменила контекст файла /var/www/html/test.html с httpd_sys_content_t на samba_share_t.

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

Figure 10: Контекст

Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Получила сообщение об ошибке.

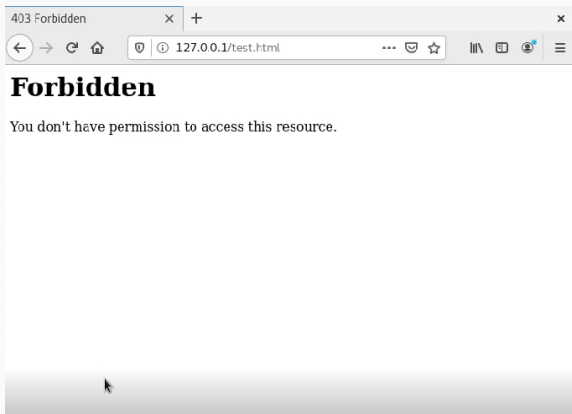


Figure 11: Сообщение об ошибке

Просмотрела log-файлы веб-сервера Apache. Также просмотрела системный лог-файл.

Log-файлы

Попробовала запустить веб-сервер Apache на прослушивание ТСР-порта 81. Для этого в файле /etc/httpd/httpd.conf нашла строчку Listen 80 и заменила её на Listen 81.

```
# 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
# 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:
# LoadModule foo_module modules/mod_foo.so
#
Include conf.modules.d/*.conf
```

Figure 12: ТСР-порт

Отображение в браузере

Вернула контекст `httpd_sys_content_t` к файлу `/var/www/html/ test.html`. После этого попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`.

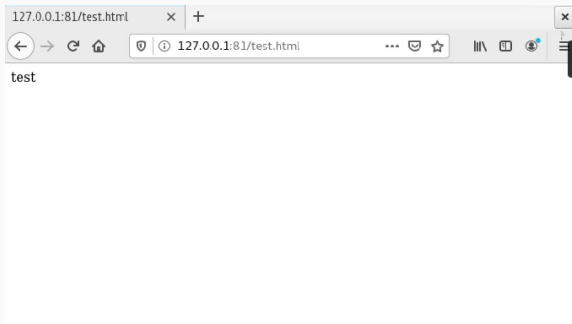


Figure 13: Отображение в браузере

Исправила обратно конфигурационный файл apache, вернув Listen 80. Удалила привязку http_port_t к 81 порту и проверила, что порт 81 удалён. Затем удалила файл /var/www/html/test.html.

```
# 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
#
# 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:
# LoadModule foo_module modules/mod_foo.so
#
Include conf.modules.d/*.conf
```

Figure 14: TCP-порт

Выводы

Я развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux. Проверила работу SELinux на практике совместно с веб-сервером Apache.