Информационная безопасность

Лабораторная работа №6

Мандатное разграничение прав в Linux

Выполнила: Халфина Айсылу Зуфаровна

Группа: НПМбд-02-19

14.10.2022

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

Проверим включен ли режим **enforcing** и политика **targeted**. Проверим что вебсервер работает с помощию команды **service httpd status**.

```
[root@akhalfina akhalfina]# getenforce
Enforcing
[root@akhalfina akhalfina]# setstatus
bash: setstatus: command not found...
[root@akhalfina akhalfina]# 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@akhalfina akhalfina]# 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 Fri 2022-10-14 20:21:37 MSK; 38min ago
     Docs: man:httpd(8)
           man:apachectl(8)
 Main PID: 3195 (httpd)
   Status: "Total requests: 10; Current requests/sec: 0; Current traffic:   0 B/sec"
    Tasks: 9
   CGroup: /system.slice/httpd.service
           ├─3195 /usr/sbin/httpd -DFOREGROUND
           ├─3200 /usr/sbin/httpd -DFOREGROUND
           ├─3201 /usr/sbin/httpd -DFOREGROUND
           ├─3202 /usr/sbin/httpd -DFOREGROUND
           ├─3203 /usr/sbin/httpd -DFOREGROUND
           ├─3204 /usr/sbin/httpd -DFOREGROUND
           ├─4764 /usr/sbin/httpd -DFOREGROUND
           ├─4780 /usr/sbin/httpd -DFOREGROUND
           └─4781 /usr/sbin/httpd -DFOREGROUND

Oct 14 20:21:37 akhalfina.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 14 20:21:37 akhalfina.localdomain httpd[3195]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name...message
Oct 14 20:21:37 akhalfina.localdomain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[root@akhalfina akhalfina]#
```

Определим контекст безопасности процесса **Apache**.

```
[root@akhalfina akhalfina]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root      3195  0.0  0.2 230440  5208 ?        Ss   20:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3200  0.0  0.1 232524  3156 ?        S    20:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3201  0.0  0.1 232660  3880 ?        S    20:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3202  0.0  0.1 232660  3900 ?        S    20:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3203  0.0  0.1 232660  3900 ?        S    20:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3204  0.0  0.1 232524  3156 ?        S    20:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    4764  0.0  0.1 232524  3156 ?        S    20:54   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    4780  0.0  0.1 232524  3156 ?        S    20:54   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    4781  0.0  0.1 232524  3156 ?        S    20:54   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 4923 0.0  0.0 112812 984 pts/0 R+ 21:00   0:00 grep --color=auto httpd
[root@akhalfina akhalfina]# ps -eZ | grep httpd
system_u:system_r:httpd_t:s0     3195 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0     3200 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0     3201 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0     3202 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0     3203 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0     3204 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0     4764 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0     4780 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0     4781 ?        00:00:00 httpd
```

Просмотрим статистику по политике с помощью **seinfo**.

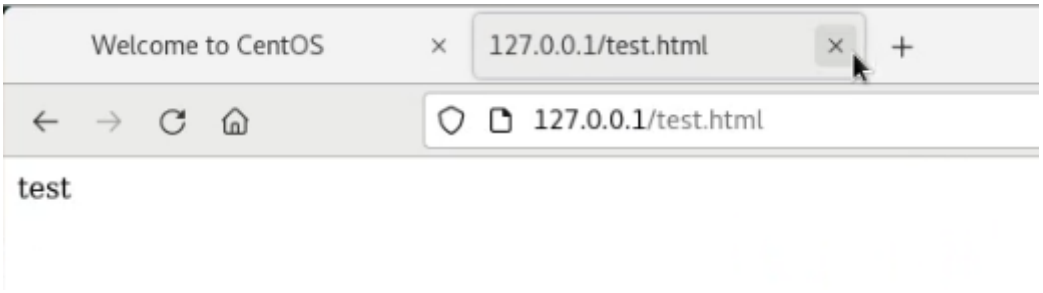
```
Without options, show SELinux status.
[root@akhalfina akhalfina]# sestatus httpd
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      31
[root@akhalfina akhalfina]# seinfo
bash: seinfo: command not found...
[root@akhalfina akhalfina]# 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

[root@akhalfina akhalfina]#
```

Создадим файл **test.html** и проверим что он открывается в браузере.



Проверим контекст файла. Сменим его на **samba_share_t**

```
[root@akhalfina akhalfina]# 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
[root@akhalfina akhalfina]# chcon -t samba_share_t /var/www/html/test.html
[root@akhalfina akhalfina]# 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
[root@akhalfina akhalfina]#
```

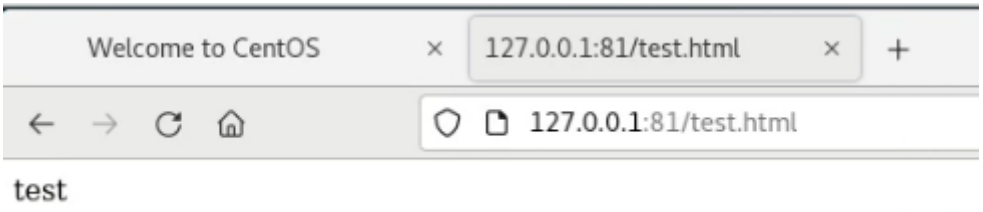
Попробуем открыть снова открыть файл. Видим сообщение, что доступ запрещён. Просмотрим ошибку в логах.

```
[root@akhalfina akhalfina]# tail /var/log/messages
Oct 14 21:19:02 akhalfina dbus[647]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
Oct 14 21:19:03 akhalfina dbus[647]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
Oct 14 21:19:03 akhalfina setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Oct 14 21:19:03 akhalfina setroubleshoot: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html. For complete SELinu
x messages run: sealert -l 3731723d-91a6-4bcb-a0aa-53b32b40f5ff
Oct 14 21:19:03 akhalfina python: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html.#012#012*****  Plugin restor
econ (92.2 confidence) suggests   ************************#012#012If you want to fix the label. #012/var/www/html/test.html default label should b
e 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*****  Plu
gin public_content (7.83 confidence) suggests   *******************#012#012If you want to treat test.html as public content#012Then you need to c
hange 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.h
tml'#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 gene
rate 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
Oct 14 21:19:15 akhalfina dbus[647]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
Oct 14 21:19:15 akhalfina dbus[647]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
Oct 14 21:19:15 akhalfina setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Oct 14 21:19:15 akhalfina setroubleshoot: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html. For complete SELinu
x messages run: sealert -l 3731723d-91a6-4bcb-a0aa-53b32b40f5ff
Oct 14 21:19:15 akhalfina python: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html.#012#012*****  Plugin restor
econ (92.2 confidence) suggests   ************************#012#012If you want to fix the label. #012/var/www/html/test.html default label should b
e 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*****  Plu
gin public_content (7.83 confidence) suggests   *******************#012#012If you want to treat test.html as public content#012Then you need to c
hange 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.h
tml'#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 gene
rate 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
```

Переключим **Apache** на прослушивание порта **81**. Просмотрим список портов командой **semanage port -l | grep http_port_t**

```
[root@akhalfina akhalfina]# 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
```

Попробуем теперь открыть файл с указанием порта **81**.



Выводы

Мы получили первое практическое знакомство с технологией SELinux1. Проверили работу SELinx на практике совместно с веб-сервером Apache.