

Лабораторная работа 6. Мандатное разграничение прав в Linux.

Поленикова Анна Алексеевна

Москва, 2021

Российский Университет Дружбы Народов

Цель лабораторной работы

Развитие навыков администрирования ОС Linux, первое практическое знакомство с технологией SELinux, а также проверка работы SELinux на практике совместно с веб-сервером Apache.

Проверка работы SELinux и веб-сервера

```
[aapolenikova@aapolenikova ~]$ getenforce
Enforcing
[aapolenikova@aapolenikova ~]$ 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
[aapolenikova@aapolenikova ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor prese
   Active: active (running) since Sat 2021-11-27 16:56:19 MSK; 22min ago
     Docs: man:httpd.service(8)
  Main PID: 34336 (httpd)
    Status: "Running, listening on: port 80"
     Tasks: 213 (limit: 4809)
    Memory: 10.0M
    CGroup: /system.slice/httpd.service
            └─34336 /usr/sbin/httpd -DFOREGROUND
              └─34343 /usr/sbin/httpd -DFOREGROUND
                └─34344 /usr/sbin/httpd -DFOREGROUND
                  └─34345 /usr/sbin/httpd -DFOREGROUND
                    └─34346 /usr/sbin/httpd -DFOREGROUND
lines 1-14/14 (END)
```

Рис. 1: Проверка работы SELinux и веб-сервера

Веб-сервер Apache

```
[aapolenikova@aapolenikova ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 34336 0.0 0.0 282912 708 ?
Ss 16:56 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 34343 0.0 0.0 296796 152 ?
S 16:56 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 34344 0.0 0.0 1354584 780 ?
Sl 16:56 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 34345 0.0 0.0 1354584 760 ?
Sl 16:56 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 34346 0.0 0.0 1485712 760 ?
Sl 16:56 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 aapolen+ 35935 0.0
0.1 221928 1192 pts/0 S+ 17:22 0:00 grep --color=auto httpd
```

Рис. 2: Веб-сервер Apache в списке процессов


```
[aapolenikova@aapolenikova ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          31 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:                132      Permissions:             464
Sensitivities:          1        Categories:             1024
Types:                  4936     Attributes:             252
Users:                  8        Roles:                  14
Booleans:               335     Cond. Expr.:           380
Allow:                  110637   Neverallow:             0
Auditallow:             163     Dontaudit:             10251
Type_trans:            243882   Type_change:            87
Type_member:            35      Range_trans:            5781
Role_allow:             37      Role_trans:             420
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:                 34
Genfscon:               107     Portcon:                642
Netifcon:               0       Nodecon:                0
```

Рис. 4: Статистика

Тип файлов и поддиректорий

```
[aapolenikova@aapolenikova ~]$ 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 07:58
cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 ноя 12 07:58
html
[aapolenikova@aapolenikova ~]$ ls -lZ /var/www/html
итого 0
```

Рис. 5: Тип файлов и поддиректорий в директориях
/var/www и /var/www/html

Создание html-файла /var/www/html/test.html

```
[aapolenikova@aapolenikova ~]$ su
Пароль:
[root@aapolenikova aapolenikova]# touch /var/www/html/test.html
[root@aapolenikova aapolenikova]# echo "test" >> /var/www/html/test.html
```

Рис. 6: Создание html-файла /var/www/html/test.html

Обращение к файлу test.html

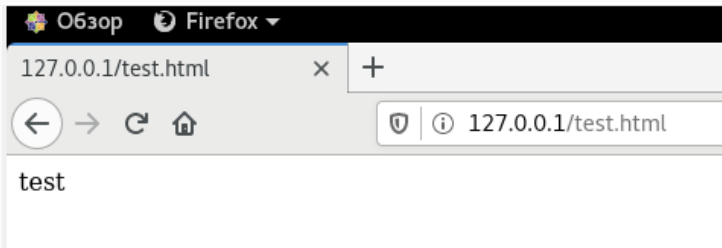


Рис. 7: Обращение к файлу test.html через веб-сервер

Контекст файла test.html

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

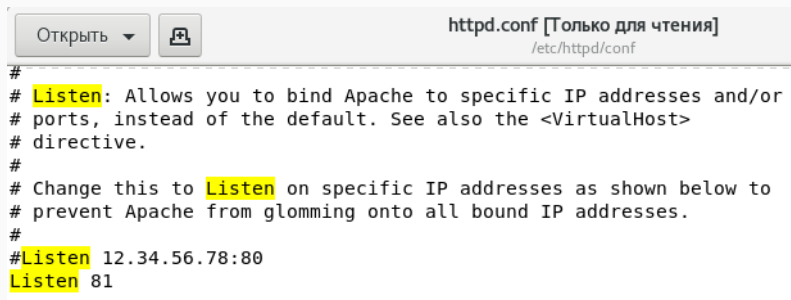
Рис. 8: Контекст файла test.html

log-файлы веб-сервера Apache и системный log-файл

```
[root@aapolenikova aapolenikova]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 5 ноя 27 17:50 /var/www/html/test.html
[root@aapolenikova aapolenikova]# tail /var/log/messages
Nov 27 18:09:05 aapolenikova setroubleshoot[38227]: failed to retrieve rpm info for
/var/www/html/test.html
Nov 27 18:09:06 aapolenikova dbus-daemon[849]: [system] Activating service name='org
.fedoraproject.SetroubleshootPrivileged' requested by ':1.721' (uid=978 pid=38227 co
mm="/usr/libexec/platform-python -Es /usr/sbin/setroub" label="system_u:system_r:set
roubleshootd_t:s0-s0:c0.c1023") (using servicehelper)
Nov 27 18:09:07 aapolenikova dbus-daemon[849]: [system] Successfully activated servi
ce 'org.fedoraproject.SetroubleshootPrivileged'
Nov 27 18:09:10 aapolenikova setroubleshoot[38227]: SELinux is preventing /usr/sbin/
httpd from getattr access on the file /var/www/html/test.html. For complete SELinux
messages run: sealert -l 6b7609af-0046-4693-9d3a-flc6e8747dd8
Nov 27 18:09:10 aapolenikova setroubleshoot[38227]: 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_cont
ent_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/tes
t.html#012#012***** Plugin public_content (7.83 confidence) suggests *****
```

Рис. 9: log-файлы веб-сервера Apache и системный log-файл

Запуск веб-сервера Apache на прослушивание TCP-порта 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
```

Рис. 10: Запуск веб-сервера Apache на прослушивание TCP-порта 81

Вывод списка портов

```
[root@aapolenikova aapolenikova]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@aapolenikova aapolenikova]# 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. 11: Вывод списка портов

Возвращение контекста

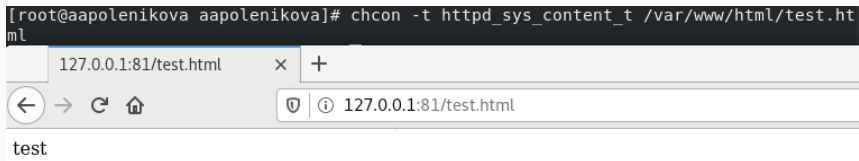


Рис. 12: Возвращение контекста

В результате проделанной лабораторной работы были развиты навыки администрирования ОС Linux, получено первое практическое знакомство с технологией SELinux, а также была проверена работа SELinux на практике совместно с веб-сервером Apache.