

Мандатное разграничение прав в Linux

Назарьева Алена НФИбд-03-18

2021, 24 november

inst{1}RUDN University, Moscow, Russian Federation

Цель работы

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

Выполнение лабораторной работы

Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`. Обратилась с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедилась, что последний работает (рис. -fig. 1)

```
[ainazarieva@ainazarieva ~]$ getenforce
Enforcing
[ainazarieva@ainazarieva ~]$ 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
[ainazarieva@ainazarieva ~]$ 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 preset: disabled)
   Active: active (running) since Бр 2021-11-23 14:15:07 MSK; 10min ago
     Docs: man:httpd(8)
           man:apachectl(8)
```

Figure 1: пункты 1-2

Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности. Как мы видим, этот процесс запущен на домене `httpd_t`. Посмотрела текущее состояние переключателей SELinux для Apache (рис. -fig. 2)

```

[ainazarieva@ainazarieva ~]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0      3403 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      3494 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      3495 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      3496 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      3497 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      3498 ?        00:00:00 httpd
[ainazarieva@ainazarieva ~]$ sestatus -bigrep httpd

```

Figure 2: пункты 3-4

Посмотрела статистику по политике с помощью команды `seinfo`, также определила множество пользователей:8, ролей:14, типов:4793. (рис. -fig. 3)

```
[root@ainazarieva ainazarieva]# 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 3: пункт 5

Определила тип файлов и поддиректорий, находящихся в директории `httpd_sys_script_exec_t` `httpd_sys_content_t`
Определила тип файлов, находящихся в директории `/var/www/html` (рис. -fig. 4)

```
[root@ainazarieva ainazarieva]# 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@ainazarieva ainazarieva]# ls -lZ /var/www/html
```

Figure 4: пункты 6-7

Определила круг пользователей, которым разрешено создание файлов в директории `/var/www/html:rwxr-xr-x`. Создала от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) `html`-файл `/var/www/html/test.html`. Проверила контекст созданного файла. Контекст, присваиваемый по умолчанию вновь созданным файлам в директории `/var/www/html`: `unconfined_u:object_r:httpd_sys_content_t:s0` (рис. -fig. ??)

```
[ainazarieva@ainazarieva ~]$ ls -l /var/www
итого 0
drwxr-xr-x. 2 root root 6 ноя 10 17:27 cgi-bin
drwxr-xr-x. 2 root root 6 ноя 10 17:27 html
[ainazarieva@ainazarieva ~]$ su
Пароль:
[root@ainazarieva ainazarieva]# touch /var/www/html/test.html
[root@ainazarieva ainazarieva]# echo "<html>
> <body>test</body>
> </html>" ^C
[root@ainazarieva ainazarieva]# echo "<html>
> <body>test</body>
> </html>" > /var/www/html/test.html
[root@ainazarieva ainazarieva]# sudo ls -lZ /var/www/html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
[root@ainazarieva ainazarieva]# sudo ls -lZ /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.h
tml
```

Изучила справку `man httpd_selinux` и выяснила, какие контексты файлов определены для `httpd:httpd_sys_content_t;httpd_sys_script_exec_t;httpd_sys_script_ro_t;httpd_sys_script_rw_t`. Они совпадают с типом файла `test.html`. Проверила контекст файла можно командой `ls -lZ /var/www/html/test.html`. Изменила контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на любой другой, к которому процесс `httpd` не должен иметь доступа, например, на `samba_share_t`: `chcon -t samba_share_t /var/www/html/test.html`. После этого проверила, что контекст поменялся. (рис. -fig. 6)

```
[root@ainazarieva ainazarieva]# chcon -t samba_share_t /var/www/html/test.html
[root@ainazarieva ainazarieva]# ls -lZ /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@ainazarieva ainazarieva]#
```

Figure 6: пункты 12-13

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 (рис. -fig. 7)



Figure 7: пункт 14

Проанализировала ситуацию. Доступ разрешен только между элементами с одинаковым типом, именно поэтому веб-сервер Apache может без проблем читать файл `/var/www/html/test.html`, который имеет тип `httpd_sys_content_t`. В то же самое время, так как Apache запущен на домене `httpd_t` и не имеет заполненных полей `userid:username`, он не может получить доступ к файлу `home/username/test.html` с другим типом, хотя этот файл доступен для чтения процессам, для которых не определена целевая политика. Просмотрела log-файлы веб-сервера Apache. Также просмотрела системный лог-файл: В системе оказались запущенные процессы `setroubleshootd` и `audtd`, мы также смогли увидеть ошибки, аналогичные указанным выше, в файле `/var/log/audit/audit.log`. (рис. -fig. 8)

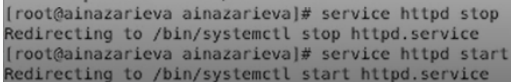
```
[root@ainazarieva ainazarieva]# ls -l /var/www/html/test.html  
-rw-r--r--. 1 root root 33 ноя 23 14:50 /var/www/html/test.html
```

Попробовала запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf нашла строчку Listen 80 и заменила её на Listen 81. (рис. -fig. 9)

```
[root@ainazarieva ainazarieva]# sed -i 's/Listen 80/Listen 81/g' /etc/httpd/conf/httpd.conf
[root@ainazarieva ainazarieva]# █
```

Figure 9: пункт 16

Выполнила перезапуск веб-сервера Apache. Сбой не произошел (рис. -fig. 10)



```
[root@ainazarieva ainazarieva]# service httpd stop
Redirecting to /bin/systemctl stop httpd.service
[root@ainazarieva ainazarieva]# service httpd start
Redirecting to /bin/systemctl start httpd.service
```

Figure 10: пункт 17

Проанализировала лог-файлы. Просмотрите файлы /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log и выяснила, что записи появились только в /var/log/audit/audit.log (рис. -fig. 11)

```
[root@ainazarieva ainazarieva]# tail /var/log/messages
Nov 23 15:24:29 ainazarieva systemd: Stopped The Apache HTTP Server.
Nov 23 15:24:33 ainazarieva systemd: Starting The Apache HTTP Server.
Nov 23 15:24:42 ainazarieva kernel: hrtimer: interrupt took 3582617 n
Nov 23 15:24:49 ainazarieva httpd: AH00558: httpd: Could not reliably
ver's fully qualified domain name, using ainazarieva.localdomain. Set
directive globally to suppress this message
Nov 23 15:24:49 ainazarieva systemd: Started The Apache HTTP Server.
Nov 23 15:26:03 ainazarieva systemd: Stopping The Apache HTTP Server.
Nov 23 15:26:04 ainazarieva systemd: Stopped The Apache HTTP Server.
Nov 23 15:26:04 ainazarieva systemd: Starting The Apache HTTP Server.
Nov 23 15:26:04 ainazarieva httpd: AH00558: httpd: Could not reliably
ver's fully qualified domain name, using ainazarieva.localdomain. Set
directive globally to suppress this message
Nov 23 15:26:04 ainazarieva systemd: Started The Apache HTTP Server.
[root@ainazarieva ainazarieva]# tail /var/log/http/error_log
tail: невозможно открыть «/var/log/http/error_log» для чтения: Нет та
алога
[root@ainazarieva ainazarieva]# tail /var/log/http/access_log
tail: невозможно открыть «/var/log/http/access_log» для чтения: Нет т
алога
```

Figure 11: пункт 18-1

(рис. -fig. 12)

```
[root@ainazarieva ainazarieva]# tail /var/log/audit/audit.log
type=LOGIN msg=audit(1637670001.584:501): pid=6134 uid=0 subj=system_
:s0-s0:c0.c1023 old-auid=4294967295 auid=0 tty=(none) old-ses=4294967
type=USER_START msg=audit(1637670001.767:502): pid=6134 uid=0 auid=0
_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session open grantors=
eyinit,pam_limits,pam_systemd acct="root" exe="/usr/sbin/crond" hostn
al=cron res=success'
type=CRED_REFR msg=audit(1637670001.767:503): pid=6134 uid=0 auid=0 s
u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_er
="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=suc
type=CRED_DISP msg=audit(1637670001.928:504): pid=6134 uid=0 auid=0 s
u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_er
="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=suc
```

Figure 12: пункт 18-2

Выполнила команду `semanage port -a -t http_port_t -p tcp 81`
После этого проверила список портов командой `semanage port -l | grep http_port_t` Убедилась, что порт 81 появился в списке. Попробовала запустить веб-сервер Apache ещё раз. Вернула контекст `httpd_sys_content_t` к файлу `/var/www/html/ test.html`. (рис. -fig. 13)

```
[root@ainazarieva ainazarieva]# semanage port -a -t http_port_t -p tcp 81
usage: semanage [-h]
                {import,export,login,user,port,ibpkey,ibendport,interface,module,node,f
context,boolean,permissive,dontaudit}
...
semanage: error: unrecognized arguments: -p 81
[root@ainazarieva ainazarieva]# 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@ainazarieva ainazarieva]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@ainazarieva ainazarieva]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@ainazarieva ainazarieva]#
```

Figure 13: пункт 19-21-1

После этого попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. Увидела содержимое файла — слово «test». (рис. -fig. 14)

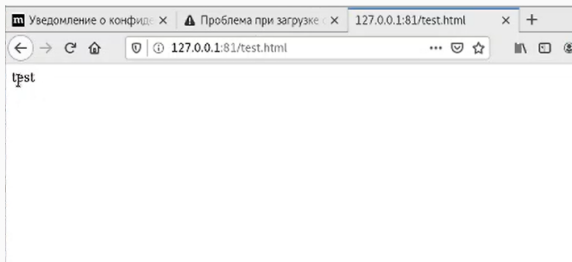


Figure 14: пункт 19-21-2

Исправила обратно конфигурационный файл apache, вернув Listen 80. Попробовала удалить привязку http_port_t к 81 порту. Порт 81 нельзя удалить, т.к. он определен на уровне политики Удалила файл /var/www/html/test.html (рис. -fig. 15)

```
[root@ainazarieva ainazarieva]# sed -i 's/Listen 81/Listen 80/g' /etc/httpd/conf/httpd.conf
[root@ainazarieva ainazarieva]# semanage port -d -t http_port_t -p tcp 81
^[[A^[[AValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@ainazarieva ainazarieva]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@ainazarieva ainazarieva]# 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@ainazarieva ainazarieva]# rm /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»?
[root@ainazarieva ainazarieva]# ls /var/www/html
1.html test.html
[root@ainazarieva ainazarieva]# rm /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»? y
```

Figure 15: пункты 22-24

Выводы

В результате выполнения работы я Развила навыки администрирования ОС Linux, Получида первое практическое знакомство с технологией SELinux1, Проверила работу SELinx на практике совместно с веб-сервером Apache.