

Лабораторная работа №6

Мандатное разграничение прав в Linux

Румянцева Александра Сергеевна

27 ноября, 2021

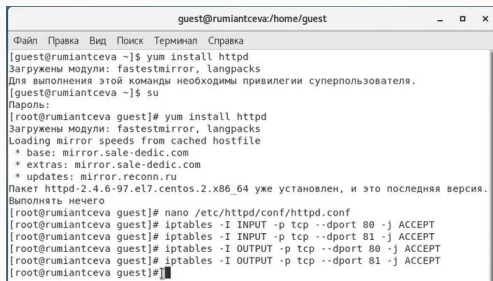
Цель: Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux на практике совместно с веб-сервером Apache.

Задание: Лабораторная работа подразумевает изучение технологий SELinux и веб-сервера Apache опытным путём.

Установила от имени суперпользователя веб-сервер Apache с помощью команды `yum install httpd`. В моём случае оказалось, что он уже установлен.

В конфигурационном файле `/etc/httpd/httpd.conf` задала параметр `ServerName: ServerName test.ru`

С помощью команд сделала так, чтобы пакетный фильтр в своей рабочей конфигурации позволял подключаться к 80-му и 81-му портам протокола tcp, добавив разрешающие правила (рис. 1).



```
guest@rumiantceva:/home/guest
Файл Правка Вид Поиск Терминал Справка
[guest@rumiantceva ~]$ yum install httpd
Загружены модули: fastestmirror, langpacks
Для выполнения этой команды необходимы привилегии суперпользователя.
[guest@rumiantceva ~]$ su
Пароль:
[root@rumiantceva guest]# yum install httpd
Загружены модули: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirror.sale-dedic.com
 * extras: mirror.sale-dedic.com
 * updates: mirror.reconn.ru
Пакет httpd-2.4.6-97.el7.centos.2.x86_64 уже установлен, и это последняя версия.
Выполнять нечего
[root@rumiantceva guest]# nano /etc/httpd/conf/httpd.conf
[root@rumiantceva guest]# iptables -I INPUT -p tcp --dport 80 -j ACCEPT
[root@rumiantceva guest]# iptables -I INPUT -p tcp --dport 81 -j ACCEPT
[root@rumiantceva guest]# iptables -I OUTPUT -p tcp --dport 80 -j ACCEPT
[root@rumiantceva guest]# iptables -I OUTPUT -p tcp --dport 81 -j ACCEPT
[root@rumiantceva guest]#
```

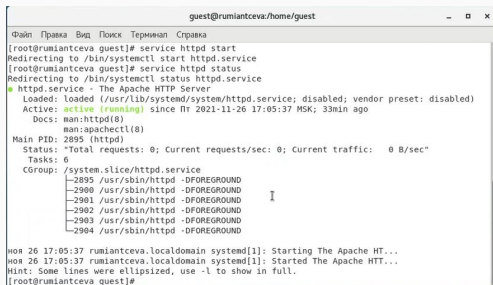
Figure 1: рис.1. Установка веб-сервер Apache. Добавле разрешающих правил.

1. Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus` (рис.2).

```
[root@rumiantceva guest]# getenforce
Enforcing
[root@rumiantceva guest]# 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@rumiantceva guest]#
```

Figure 2: рис.2. Команды `getenforce` и `sestatus`.

Обратилась к веб-серверу, запущенному на нашем компьютере, и убедимся, что последний работает: `service httpd status` (рис. 3).



```
guest@rumiantceva:/home/guest
Файл Правка Вид Поиск Терминал Справка
[root@rumiantceva guest]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@rumiantceva guest]# 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 Пт 2021-11-26 17:05:37 MSK; 33min ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Main PID: 2895 (httpd)
    Status: "Total requests: 0; Current requests/sec: 0; Current traffic:  0 B/sec"
      Tasks: 6
    CGroup: /system.slice/httpd.service
             └─2895 /usr/sbin/httpd -DFOREGROUND
               └─2900 /usr/sbin/httpd -DFOREGROUND
                 └─2901 /usr/sbin/httpd -DFOREGROUND
                   └─2902 /usr/sbin/httpd -DFOREGROUND
                     └─2903 /usr/sbin/httpd -DFOREGROUND
                       └─2904 /usr/sbin/httpd -DFOREGROUND

ноя 26 17:05:37 rumiantceva.localdomain systemd[1]: Starting The Apache HT...
ноя 26 17:05:37 rumiantceva.localdomain systemd[1]: Started The Apache HTT...
Hint: Some lines were ellipsized, use -l to show in full.
[root@rumiantceva guest]#
```

Figure 3: рис.3. `service httpd status`

Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности, используя команду `ps auxZ | grep httpd` (рис. 4).

```
[root@rumiantceva guest]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      2895  0.0  0.4 224084 5012 ?        Ss   17:05   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  2900  0.0  0.3 226168 3088 ?        S    17:05   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  2901  0.0  0.3 226168 3088 ?        S    17:05   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  2902  0.0  0.3 226168 3088 ?        S    17:05   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  2903  0.0  0.3 226168 3088 ?        S    17:05   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  2904  0.0  0.3 226168 3088 ?        S    17:05   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-c1023 root  3617  0.0  0.0 112032 976 pts/0 R+   17:42   0:00 grep --color=auto h
ttpd
[root@rumiantceva guest]#
```

Figure 4: рис.4. Команда `ps auxZ | grep httpd`.

Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -b | grep httpd` (рис. 5).

```
guest@rumiantceva:/home/guest
Файл Правка Вид Поиск Терминал Справка
[root@rumiantceva guest]# sestatus -b | grep httpd
httpd anon_write off
httpd builtIn_scripting on
httpd can_check_spam off
httpd can_connect_ftp off
httpd can_connect_ldap off
httpd can_connect_mythtv off
httpd can_connect_zabbix off
httpd can_network_connect off
httpd can_network_connect_cobbler off
httpd can_network_connect_db off
httpd can_network_memcache off
httpd can_network_relay off
httpd can_sendmail off
httpd dbus_avaahi off
httpd dbus_sssd off
httpd dontaudit_search_dirs off
httpd enable_cgi on
httpd enable_ftp_server off
httpd enable_homedirs off
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
```

Figure 5: рис.5. Команда `sestatus -b | grep httpd`.

Посмотрела статистику по политике с помощью команды `seinfo`, также определила множество пользователей, ролей и типов. (рис. 6)

Замечу, что для выполнения команды пришлось выполнить установку `setools-console`

```
guest@rumiantceva:/home/guest
Файл  Правка  Вид  Поиск  Терминал  Справка
Проверка      : setools-console-3.3.8-4.el7.x86_64

Установлено:
setools-console.x86_64 0:3.3.8-4.el7

Выполнено!
[root@rumiantceva guest]# 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@rumiantceva guest]# █
```

Figure 6: рис.6. Команда `seinfo`.

Из рисунка наглядно видно, что пользователей: 8, ролей: 14, типов: 4793.

Опытным путём определила, что только суперпользователь может создать файл в данной директории (рис. 7). Поэтому создала от имени суперпользователя html-файл `/var/www/html/test.html` с содержанием, которое требовалось в задании:

test

Проверила контекст созданного файла: контекст, присваиваемый по умолчанию вновь созданным файлам в директории `/var/www/html`:
`unconfined_u:object_r:httpd_sys_content_t`

```
[guest@rumiantceva ~]$ touch /var/www/html/file.txt
touch: невозможно выполнить touch для «/var/www/html/file.txt»: Отказано в доступе
[guest@rumiantceva ~]$ su guest2
Пароль:
[guest2@rumiantceva guest]$ touch /var/www/html/file.txt
touch: невозможно выполнить touch для «/var/www/html/file.txt»: Отказано в доступе
[guest2@rumiantceva guest]$ exit
exit
[guest@rumiantceva ~]$ su asrumiantceva
su: user asrumiantceva does not exist
[guest@rumiantceva ~]$ su rumiantceva
Пароль:
[rumiantceva@rumiantceva guest]$ touch /var/www/html/file.txt
touch: невозможно выполнить touch для «/var/www/html/file.txt»: Отказано в доступе
[rumiantceva@rumiantceva guest]$ exit
exit
[guest@rumiantceva ~]$ su
Пароль:
[root@rumiantceva guest]# touch /var/www/html/file.txt
[root@rumiantceva guest]# nano /var/www/html/test.html
[root@rumiantceva guest]# ls -lZ /var/www/html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 file.txt
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
[root@rumiantceva guest]# ls -l /var/www/html
итого 4
-rw-r--r--. 1 root root 0 ноя 26 18:01 file.txt
-rw-r--r--. 1 root root 33 ноя 26 18:03 test.html
[root@rumiantceva guest]#
```

Figure 7: рис.7. Определение пользователей, которым разрешено создание файлов в директории `/var/www/html`. Контекст созданного файла.

Обратилась к файлу через веб-сервер, введя в браузере firefox адрес: `http://127.0.0.1/test.html`. Файл был успешно отображен (рис. 8).

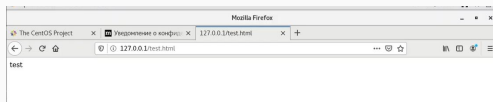


Figure 8: рис.8. `http://127.0.0.1/test.html`.

Изменила контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на другой, к которому процесс `httpd` не имеет доступа (на `samba_share_t`) (рис. 9).

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

Figure 9: рис.9. Работа с контекстом файла `/var/www/html/test.html`.

Попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Но получила сообщение об ошибке (рис. 10).



Figure 10: рис.10. `http://127.0.0.1/test.html` при контексте `samba_share_t`.

Попробовала запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services), заменив в файле /etc/httpd/conf/httpd.conf строчку Listen 80 на Listen 81.

Перезапустила веб-сервер Apache и попробовала обратиться к файлу через веб-сервер, введя в браузере firefox адрес `http://127.0.0.1/test.html` (рис. 11).

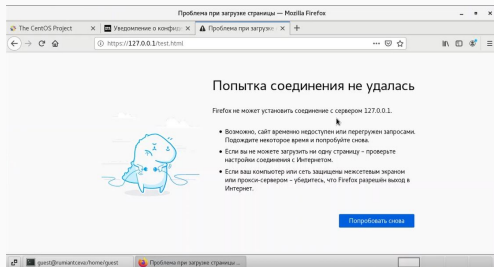


Figure 11: рис.11. `http://127.0.0.1/test.html` при Listen 81.

Выполнила команду `semanage port -a -t http_port_t -p tcp 81` и после этого проверила список портов командой `semanage port -l | grep http_port_t` (рис. 12).

```
[n/cron@~]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@rumiantceva guest]# 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@rumiantceva guest]#
```

Figure 12: рис.12. Порт 81.

Попробовала запустить веб-сервер Apache еще раз. Он успешно запустился. Вернула контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`:
`chcon -t httpd_sys_content_t /var/www/html/test.html`.

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

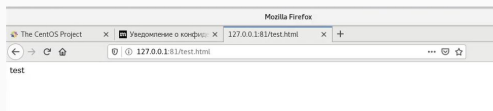


Figure 13: рис.13. `http://127.0.0.1:81/test.html`.

Попробовала удалить привязку `http_port_t` к 81 порту: `semanage port -d -t http_port_t -p tcp 81`. Данную команду выполнить невозможно на моей версии CentOS, так как порт 81 определён на уровне политики.

Удалила файл `/var/www/html/test.html`: `rm /var/www/html/test.html`

```
[root@rumiantceva ~]# semanage port -d -t http_port_t -p tcp 81
[[AValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@rumiantceva ~]# semanage port -l | grep http_port_t
http_port_t      tcp      80, 81, 443, 488, 8080, 8089, 8443, 9080
pegasus http_port_t      tcp      5988
[root@rumiantceva ~]# rm /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»? y
[root@rumiantceva ~]#
```

Figure 14: рис.14. Удаление привязку `http_port_t` к 81 порту и файла `/var/www/html/test.html`.

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