

Презентация к лабораторной работе №6

Мандатное разграничение прав в Linux

Ким И. В. НФИбд-01-21

Российский университет дружбы народов, Москва, Россия

Цели и задачи

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

Установил httpd на CentOS

```
[root@localhost ilya]# yum install httpd
Обновление репозитория службы управления подписками.
Невозможно прочитать идентификатор клиента.

This system is not registered with an entitlement server. You can use "rhc" or "subscription-manager" to register.

Последняя проверка окончания срока действия метаданных: 0:00:20 назад, Сб 12 окт 2024 17:20:05.
Зависимости разрешены.
=====
Пакет                Архитектура  Версия          Репозиторий      Размер
=====
Установка:
  httpd              x86_64       2.4.62-1.el9    appstream         47 k
Установка зависимостей:
  apr                x86_64       1.7.0-12.el9    appstream        123 k
  apr-util           x86_64       1.6.1-23.el9    appstream         95 k
  apr-util-bdb       x86_64       1.6.1-23.el9    appstream         13 k
  centos-logos-httpd noarch       90.8-1.el9      appstream         1.5 M
  httpd-core         x86_64       2.4.62-1.el9    appstream        1.5 M
  httpd-filesystem   noarch       2.4.62-1.el9    appstream         13 k
  httpd-tools        x86_64       2.4.62-1.el9    appstream         82 k
Установка слабых зависимостей:
  apr-util-openssl   x86_64       1.6.1-23.el9    appstream         15 k
  mod_http2          x86_64       2.0.26-2.el9    appstream        163 k
  mod_lua            x86_64       2.4.62-1.el9    appstream         59 k

Результат транзакции
=====
```

В конфигурационном файле httpd.conf задал параметр ServerName

```
[root@localhost ilya]# echo "ServerName test.ru" > /etc/httpd/httpd.conf
```

Добавил разрешающие правила

```
[root@localhost ilya]# iptables -I INPUT -p tcp --dport 80 -j ACCEPT  
[root@localhost ilya]# iptables -I INPUT -p tcp --dport 81 -j ACCEPT  
[root@localhost ilya]# iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT  
[root@localhost ilya]# iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT
```

```
[root@localhost ilya]# getenforce
Enforcing
[root@localhost ilya]# 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
```


Запустил сервер apache (рис. [-@fig:005])

```
[root@localhost ilya]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@localhost ilya]# 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; preset: d>
   Active: active (running) since Sat 2024-10-12 17:34:32 MSK; 7s ago
     Docs: man:httpd.service(8)
  Main PID: 3876 (httpd)
    Status: "Started, listening on: port 80"
     Tasks: 177 (limit: 10962)
    Memory: 22.1M
       CPU: 27ms
    CGroup: /system.slice/httpd.service
            └─3876 /usr/sbin/httpd -DFOREGROUND
              └─3877 /usr/sbin/httpd -DFOREGROUND
                └─3878 /usr/sbin/httpd -DFOREGROUND
                  └─3879 /usr/sbin/httpd -DFOREGROUND
                    └─3880 /usr/sbin/httpd -DFOREGROUND

окт 12 17:34:32 localhost.localdomain systemd[1]: Starting The Apache HTTP Serv>
окт 12 17:34:32 localhost.localdomain httpd[3876]: AH00558: httpd: Could not re>
окт 12 17:34:32 localhost.localdomain httpd[3876]: Server configured, listening>
окт 12 17:34:32 localhost.localdomain systemd[1]: Started The Apache HTTP Serve>
```

Определил контекст безопасности Apache

```
[root@localhost ilya]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 3876 0.0 0.6 21104 11300 ? Ss 17:34 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3877 0.0 0.3 22980 7144 ? S 17:34 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3878 0.0 0.6 1441156 11116 ? Sl 17:34 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3879 0.0 0.7 1572292 13240 ? Sl 17:34 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3880 0.0 0.6 1441156 11120 ? Sl 17:34 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 4071 0.0 0.1 221688 2304 pts/0 S+ 17:36 0:00 grep --color=auto httpd
[root@localhost ilya]# ps -eZ | grep httpd
system_u:system_r:httpd_t:s0 3876 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 3877 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 3878 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 3879 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 3880 ? 00:00:00 httpd
```

Посмотрел текущее состояние переключателей SELinux для Apache

```
[root@localhost ilya]# 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_manage_courier_spool 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_avahi 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 off
httpd_manage_ima off
```

Установил пакет “settools-console”

```
[root@localhost ilya]# seinfo
bash: seinfo: команда не найдена...
Установить пакет «settools-console», предоставляющий команду «seinfo»? [N/y] y

* Ожидание в очереди...
* Загрузка списка пакетов....
Следующие пакеты должны быть установлены:
settools-console-4.4.4-1.el9.x86_64    Policy analysis command-line tools for SELinux
Продолжить с этими изменениями? [N/y] y
```

Посмотрел статистику по политике

```
[root@localhost ilya]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:          135      Permissions:          457
Sensitivities:    1        Categories:          1024
Types:            5169     Attributes:           259
Users:            8        Roles:                15
Booleans:         358     Cond. Expr.:         390
Allow:            65633    Neverallow:           0
Auditallow:       176     Dontaudit:            8703
Type_trans:       271851   Type_change:          94
Type_member:      37       Range_trans:          5931
Role allow:       40       Role_trans:           417
Constraints:      70       Validatetrans:        0
MLS Constrains:  72       MLS Val. Tran:        0
Permissives:      2        Polcap:               6
Defaults:         7        Typebounds:           0
Allowxperm:       0        Neverallowxperm:      0
Auditallowxperm:  0        Dontauditxperm:       0
Ibendportcon:     0        Ibpkeycon:            0
Initial SIDs:     27       Fs_use:               35
Genfscon:         109     Portcon:              665
Netifcon:         0        Nodcon:               0
```

Посмотрел тип файлов и поддиректорий

```
[root@localhost ilya]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 авг 12 16:20 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 авг 12 16:20 html
[root@localhost ilya]# ls -lZ /var/www/html
итого 0
```

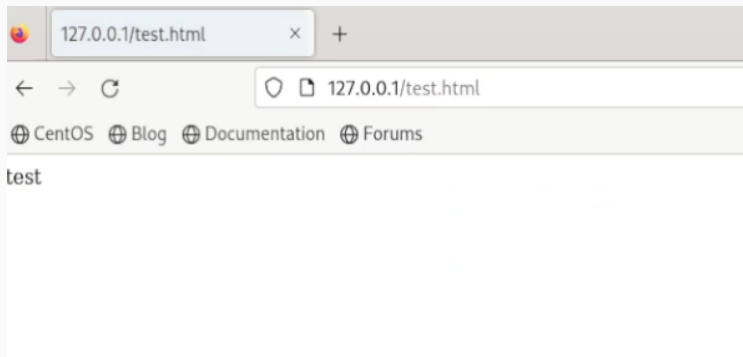
Создал html файл от имени суперпользователя

```
[root@localhost ilya]# touch /var/www/html/test.html
[root@localhost ilya]# vim /var/www/html/test.html
[root@localhost ilya]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>
```

Проверил контекст созданного файла

```
[root@localhost ilya]# ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 окт 12 17:48 test.html
[root@localhost ilya]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
```

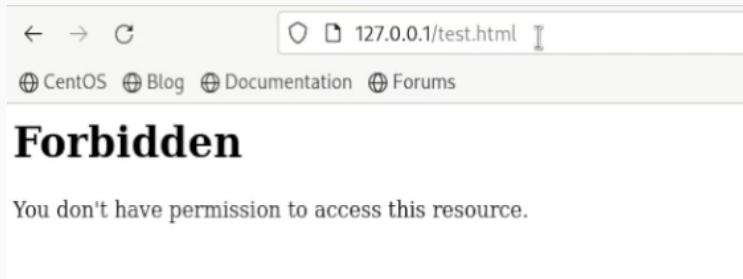

Открыл в браузере наш файл



Изменил контекст файла test.html

```
[root@localhost ilya]# chcon -t samba_share_t /var/www/html/test.html
[root@localhost ilya]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@localhost ilya]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 окт 12 17:48 /var/www/html/test.html
```

Попробовал открыть в браузере наш файл, получил ошибку



В файле httpd.conf изменил Listen с 80 на 81

```
ilya@localhost:/home/ilya — vim /etc/httpd/conf/httpd.conf

ServerRoot: The top of the directory tree under which the server's
configuration, error, and log files are kept.

Do not add a slash at the end of the directory path.  If you point
ServerRoot at a non-local disk, be sure to specify a local disk on the
Mutex directive, if file-based mutexes are used.  If you wish to share the
same ServerRoot for multiple httpd daemons, you will need to change at
least PidFile.

ServerRoot "/etc/httpd"

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 a specific IP address, but note that if
httpd.service is enabled to run at boot time, the address may not be
available when the service starts. See the httpd.service(8) man
page for more information.

Listen 12.34.56.78:80
listen 81
```

Сделал перезапуск Apache, произошел сбой

```
[root@localhost ilya]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
Job for httpd.service failed because the control process exited with error code.
See "systemctl status httpd.service" and "journalctl -xeu httpd.service" for details.
```

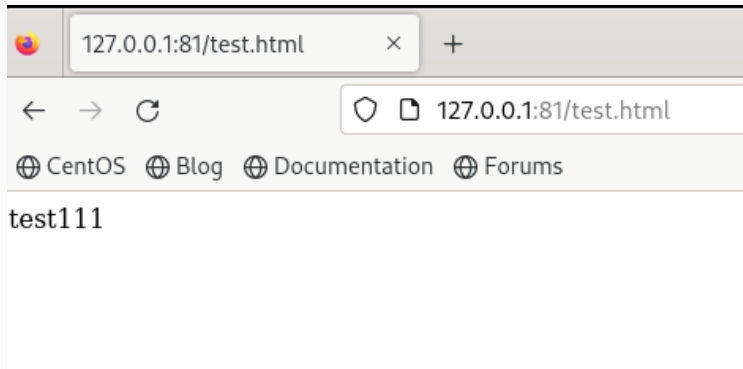
Добавил 81 порт в список

```
[root@localhost ilya]# semanage port -a -t http_port_t -p tcp 81
Port tcp/81 already defined, modifying instead
[root@localhost ilya]# semanage port -l | grep http_port_t
http_port_t          tcp      81, 80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t  tcp      5988
```

Добавил 81 порт в список, также изменил test.html

```
[root@localhost ilya]# semanage port -a -t http_port_t -p tcp 81
Port tcp/81 already defined, modifying instead
[root@localhost ilya]# semanage port -l | grep http_port_t
http_port_t          tcp      81, 80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t  tcp      5988
```

Открыл файл в браузере



Вернул контекст файлу test.html

```
[root@localhost ilya]# chcon -t httpd_sys_content_t /var/www/html/test.html
```

Вернул Listen 80 в файл html.config

```
#  
#Listen 12.34.56.78:80  
Listen 80  
  
#
```

Удалил привязку к 81 порту

```
[root@localhost ilya]# semanage port -d -t http_port_t -p tcp 81
[root@localhost ilya]# semanage port -l | grep http_port_t
http_port_t          tcp      80, 80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t  tcp      5988
```

Удалил файл test.html

```
[root@localhost ilya]# rm /var/www/html/test.html  
rm: удалить обычный файл '/var/www/html/test.html'? y
```

Выводы

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinux на практике совместно с веб-сервером Apache.