

Отчет по лабораторной работе 6

Savchenkov Dmitriy Andreevich¹

27 November, 2021 Moscow, Russian Federation

¹RUDN University, Moscow, Russian Federation

Цель выполнения лабораторной
работы

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

Результаты выполнения лабораторной работы

Подготовка лабораторного стенда

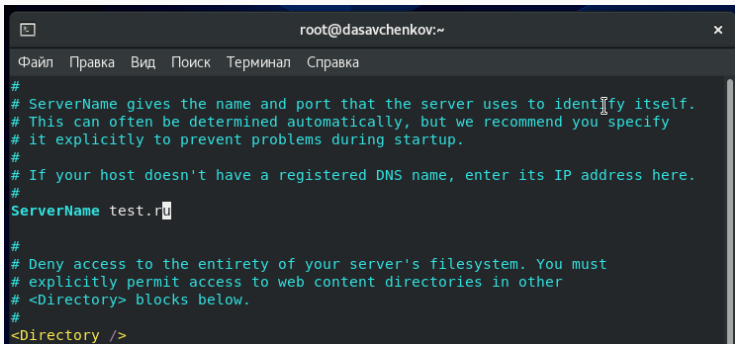
```

#Анализ:
apr-1.6.3-12.el8.x86_64
apr-util-1.6.1-6.el8.x86_64
apr-util-bdb-1.6.1-6.el8.x86_64
apr-util-openssl-1.6.1-6.el8.x86_64
centos-logos-httpd-85.8.2.el8.noarch
mod_2.4.37-42.mod_ssl.el8.5.0+1022=b541f3b1.x86_64
mod_ssl-2.4.37-42.mod_ssl.el8.5.0+1022=b541f3b1.x86_64
httpd-tools-2.4.37.3.module.el8.5.0+1022=b541f3b1.x86_64
mod_php-2.15.7.3.module.el8.4.0+778+c970deab.x86_64

```

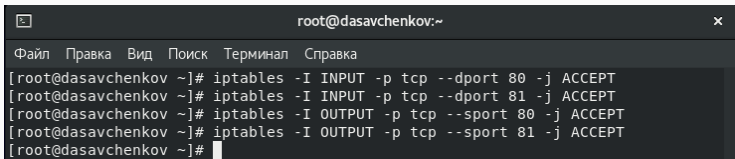
Figure 1: 1

Изменение конфигурационного файла



```
root@dasavchenkov:~
Файл  Правка  Вид  Поиск  Терминал  Справка
#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
ServerName test.ru
#
# Deny access to the entirety of your server's filesystem. You must
# explicitly permit access to web content directories in other
# <Directory> blocks below.
#
<Directory />
```

Figure 2: 2

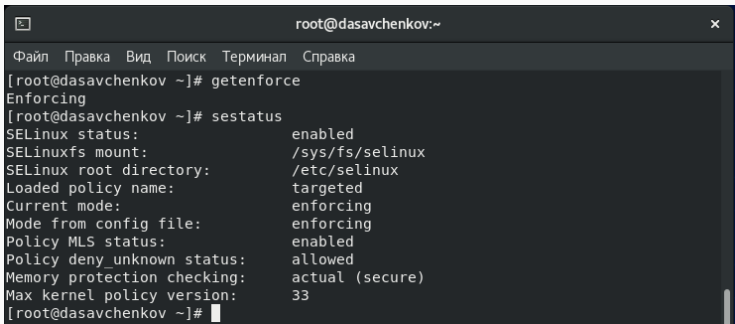
A terminal window titled 'root@dasavchenkov:~' with a menu bar containing 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The terminal displays four iptables commands being executed in sequence, each followed by a prompt character '#'. The commands are: 'iptables -I INPUT -p tcp --dport 80 -j ACCEPT', 'iptables -I INPUT -p tcp --dport 81 -j ACCEPT', 'iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT', and 'iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT'. The cursor is positioned at the end of the last command.

```
root@dasavchenkov:~  
Файл Правка Вид Поиск Терминал Справка  
[root@dasavchenkov ~]# iptables -I INPUT -p tcp --dport 80 -j ACCEPT  
[root@dasavchenkov ~]# iptables -I INPUT -p tcp --dport 81 -j ACCEPT  
[root@dasavchenkov ~]# iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT  
[root@dasavchenkov ~]# iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT  
[root@dasavchenkov ~]#
```

Figure 3: 3

Выполнение лабораторной работы

Проверка режима и политики SELinux



```
root@dasavchenkov:~  
Файл Правка Вид Поиск Терминал Справка  
[root@dasavchenkov ~]# getenforce  
Enforcing  
[root@dasavchenkov ~]# 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  
[root@dasavchenkov ~]#
```

Figure 4: 4

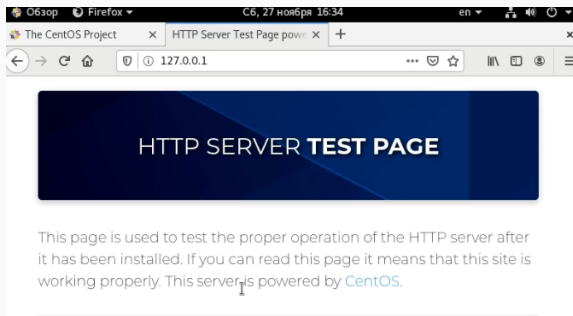


Figure 5: 5

Просмотр состояний переключателей SELinux

```
[root@dasavchenkov ~]# 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_avahi                 off
```

Figure 6: 6

Статистика по политике с помощью команды *seinfo*

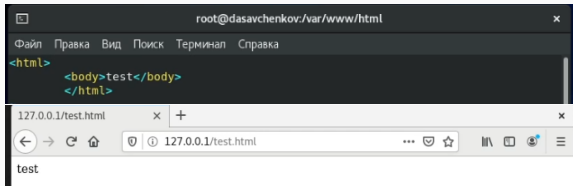
```
Target Policy:          selinux
Handle unknown classes: allow

Classes:                132   Permissions:           463
Sensitivities:          1     Categories:           1024
Types:                  4959   Attributes:           255
Users:                  8     Roles:                14
Booleans:               340   Cond. Expr.:         389
Allow:                  112885 Neverallow:            0
Auditallow:             166   Dontaudit:           10362
Type_trans:             253398 Type_change:           87
Type_member:            35    Range_trans:          6015
Role_allow:             38    Role_trans:           423
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:                33
Genfscon:               106    Portcon:               640
Netifcon:               0     Nodecon:               0
```

```
[root@dasavchenkov ~]#
```


Figure 7: 7

Создание файла *html* и проверка в браузере



Изменение контекста файла и проверка в браузере

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

A screenshot of a web browser window. The title bar says "403 Forbidden". The address bar shows "127.0.0.1/test.html". The main content area displays the word "Forbidden" in a large, bold, black font. Below it, in a smaller font, it says "You don't have permission to access this resource." A mouse cursor is visible over the text.

Forbidden

You don't have permission to access this resource.

Замена порта

```
root@dasavchenkov:var/www/html
Файл Правка Вид Поиск Терминал Справка
#
# 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
```

```
root@dasavchenkov:var/www/html
Файл Правка Вид Поиск Терминал Справка
[root@dasavchenkov html]# semanage port -a -t http_port -p tcp 81
ValueError: Недопустимый тип: http_port. Необходимо указать тип порта.
[root@dasavchenkov html]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@dasavchenkov html]# 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@dasavchenkov html]#
```

```
root@dasavchenkov:var/www/html
Файл Правка Вид Поиск Терминал Справка
[root@dasavchenkov html]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@dasavchenkov html]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@dasavchenkov html]#
```

127.0.0.1/test.html x +

test

Завершение

```
root@dasavchenkov:var/www/html
Файл Правка Вид Поиск Терминал Справка
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 specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80
```

```
[root@dasavchenkov html]# semanage port -d -t http_port_t -p tcp 81
```

```
root@dasavchenkov:var/www/html
Файл Правка Вид Поиск Терминал Справка
[root@dasavchenkov html]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@dasavchenkov html]# ls
[root@dasavchenkov html]#
```

Выводы по лабораторной работе

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

Спасибо за внимание!