

Лабораторная работа №6.

Мандатное разграничение прав в Linux.

Ишанова А.И. группа НФИ-02-19

Содержание

1	Цель работы	4
2	Теоретическое введение	5
3	Выполнение лабораторной работы	6
3.1	Подготовка лабораторного стенда	6
3.2	Основная часть	7
4	Вывод	15
5	Библиография	16

List of Figures

3.1	Установка httpd	6
3.2	Задача параметра ServerName	6
3.3	Отключение фильтров	6
3.4	Режим работы SELinux	7
3.5	Проверка работы сервера	7
3.6	Запуск сервера	7
3.7	Определение контекста безопасности	8
3.8	Текущее состояние переключателей SELinux для Apache	9
3.9	Статистика по политике	10
3.10	Тип файлов и поддиректорий в /var/www	10
3.11	Тип файлов и поддиректорий в /var/www/html	10
3.12	Создание test.html	11
3.13	Обращение к файлу через браузер	11
3.14	Смена контекста test.html	11
3.15	Обращение к файлу через браузер после смены контекста	11
3.16	Просмотр системного лог-файла	12
3.17	Изменение прослушивания TCP-порта	12
3.18	Перезапуск Apache	12
3.19	Добавление порта 81	12
3.20	Перезапуск Apache, возвращение изначального контекста test.html	13
3.21	Обращение к файлу через браузер после возвращения контекста	13
3.22	Возвращение порта 80 в httpd.conf	13
3.23	Работа команды удаления порта 81 и удаление test.html	14

1 Цель работы

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

2 Теоретическое введение

SELinux (англ. Security-Enhanced Linux — Linux с улучшенной безопасностью) — реализация системы принудительного контроля доступа, которая может работать параллельно с классической избирательной системой контроля доступа. [2]

Apache HTTP-сервер — свободный веб-сервер. Apache является кроссплатформенным ПО, поддерживает операционные системы Linux, BSD, macOS, Microsoft Windows, Novell NetWare, BeOS.

Основными достоинствами Apache считаются надёжность и гибкость конфигурации. Он позволяет подключать внешние модули для предоставления данных, использовать СУБД для аутентификации пользователей, модифицировать сообщения об ошибках и т. д. Поддерживает IPv4. [3]

3 Выполнение лабораторной работы

3.1 Подготовка лабораторного стенда

1. Установили httpd. (fig. 3.1)

```
[aiishanova@aiishanova ~]$ su root
Password:
[root@aiishanova aiishanova]# yum install httpd
Rocky Linux 9 - BaseOS                7.5 kB/s | 3.6 kB      00:00
Rocky Linux 9 - BaseOS                1.6 MB/s | 1.7 MB      00:01
Rocky Linux 9 - AppStream             7.5 kB/s | 3.6 kB      00:00
Rocky Linux 9 - AppStream             3.4 MB/s | 6.0 MB      00:01
Rocky Linux 9 - Extras                6.7 kB/s | 2.9 kB      00:00
Dependencies resolved.
=====
Package                               Arch      Version           Repository        Size
=====
Installing:
httpd                                   x86_64     2.4.51-7.el9_0    appstream         1.4 M
```

Figure 3.1: Установка httpd

2. В конфигурационном файле /etc/httpd/httpd.conf необходимо задали параметр ServerName. (fig. 3.2)

```
root@aiishanova aiishanova]# cd /etc/httpd
root@aiishanova httpd]# echo "ServerName test.ru" >> httpd.conf
```

Figure 3.2: Задача параметра ServerName

3. Отключили фильтры. (fig. 3.3)

```
[root@aiishanova httpd]# iptables -F
[root@aiishanova httpd]# iptables -P INPUT ACCEPT
[root@aiishanova httpd]# iptables -P OUTPUT ACCEPT
```

Figure 3.3: Отключение фильтров

3.2 Основная часть

1. Убедились, что SELinux работает в режиме enforcing политики targeted.
(fig. 3.4)

```
[root@aiishanova httpd]# getenforce
Enforcing
[root@aiishanova httpd]# 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
```

Figure 3.4: Режим работы SELinux

2. Увидели, что сервер не работает и запустили его. (fig. 3.5, fig. 3.6)

```
Max kernel policy version: 33
[root@aiishanova httpd]# cd ~
[root@aiishanova ~]# 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 pr
  Active: inactive (dead)
  Docs: man:httpd.service(8)
...skipping...
○ httpd.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor pr
  Active: inactive (dead)
  Docs: man:httpd.service(8)
~
```

Figure 3.5: Проверка работы сервера

```
[root@aiishanova ~]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@aiishanova ~]# 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 pr
  Active: active (running) since Sat 2022-10-15 17:37:11 MSK; 3s ago
```

Figure 3.6: Запуск сервера

3. Определили контекст безопасности Apache - unconfined_u:unconfined_r:unconfined_t.
(fig. 3.7)

```
[root@aiishanova ~]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 39411 0.0 0.5 20248 11628 ?
Ss 17:37 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 39412 0.0 0.3 21572 7400 ?
S 17:37 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 39417 0.0 0.6 1210512 13044 ?
Sl 17:37 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 39418 0.0 0.5 1079376 11040 ?
Sl 17:37 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 39419 0.0 0.5 1079376 11040 ?
Sl 17:37 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 39648 0.0 0.1 221668
2268 pts/0 S+ 17:38 0:00 grep --color=auto httpd
```

Figure 3.7: Определение контекста безопасности

4. Посмотрели текущее состояние переключателей SELinux для Apache.
(fig. 3.8)


```

[root@aiishanova ~]# 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_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
httpd_serve_cobbler_files off
httpd_setrlimit off
httpd_ssi_exec off
httpd_sys_script_anon_write off
httpd_tmp_exec off
httpd_tty_comm off
httpd_unified off
httpd_use_cifs off
httpd_use_fusefs off
httpd_use_gpg off
httpd_use_nfs off

```

Figure 3.8: Текущее состояние переключателей SELinux для Apache

5. осмотрели статистику по политике с помощью команды seinfo. (fig. 3.9)

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

Classes:          133      Permissions:        454
Sensitivities:    1        Categories:         1024
Types:            4995     Attributes:         254
Users:            8        Roles:              14
Booleans:         347     Cond. Expr.:       382
Allow:            63727    Neverallow:         0
Auditallow:       163     Dontaudit:          8391
Type_trans:       251060   Type_change:        87
Type_member:      35      Range_trans:        5958
Role_allow:       38      Role_trans:         418
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:             651
Netifcon:         0      Nodecon:             0
```

Figure 3.9: Статистика по политике

6. Определили тип файлов и поддиректорий, находящихся в директории /var/www. (fig. 3.10)

```
[root@aiishanova ~]# ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 15
:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 May 16 15
:10 html
```

Figure 3.10: Тип файлов и поддиректорий в /var/www

7. Определили тип файлов и поддиректорий, находящихся в директории /var/www/html. (fig. 3.11)

```
[root@aiishanova ~]# ls -lZ /var/www/html
total 0
```

Figure 3.11: Тип файлов и поддиректорий в /var/www/html

8. Создали файл test.html и проверили его контекст. (fig. 3.12)

```
[root@aiishanova ~]# touch /var/www/html/test.html
[root@aiishanova ~]# echo '<html>' >> /var/www/html/test.html
[root@aiishanova ~]# echo '<body> test </body>' >> /var/www/html/test.html
[root@aiishanova ~]# echo '</html>' >> /var/www/html/test.html
[root@aiishanova ~]# ls -lZ /var/www/html/test.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 35 Oct 15 17:50 /var/www/html/test.html
[root@aiishanova ~]#
```

Figure 3.12: Создание test.html

9. Обратились к файлу через веб-сервер. (fig. 3.13)

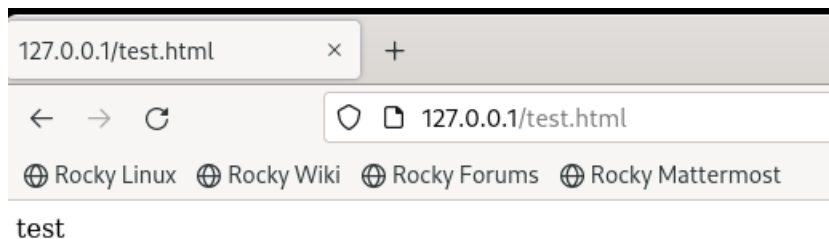


Figure 3.13: Обращение к файлу через браузер

10. Изменили контекст файла и проверили что он поменялся. (fig. 3.14)

```
[root@aiishanova ~]# chcon -t samba_share_t /var/www/html/test.html
[root@aiishanova ~]# ls -lZ /var/www/html/test.html
-rw-r--r--. 1 root root unconfined_u:object_r:samba_share_t:s0 35 Oct 15 17:50 /var/www/html/test.html
```

Figure 3.14: Смена контекста test.html

11. Попробовали получить доступ к файлу через браузер. (fig. 3.15)

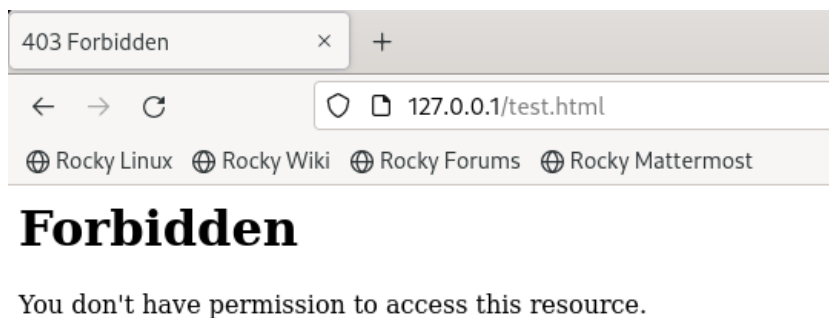


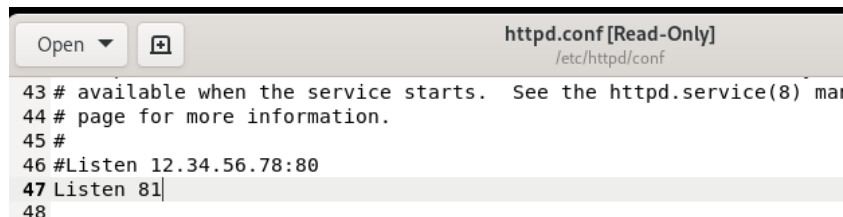
Figure 3.15: Обращение к файлу через браузер после смены контекста

12. Просмотрели системный лог-файл. Увидели, что проблема в смененном контексте. (fig. 3.16)

```
var/www/html/test.html
[root@aiishanova ~]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 35 Oct 15 17:50 /var/www/html/test.html
[root@aiishanova ~]# tail /var/log/messages
Oct 15 18:01:18 aiishanova systemd[1]: Started dbus-1.9-org.fedoraproject.Setrou
bleshootPrivileged@0.service.
Oct 15 18:01:19 aiishanova setroubleshoot[40697]: SELinux is preventing /usr/sbi
n/httpd from getattr access on the file /var/www/html/test.html. For complete SE
Linux messages run: sealert -l e451f71d-aaaa-49a2-9401-5e083dfa23fe
Oct 15 18:01:19 aiishanova setroubleshoot[40697]: SELinux is preventing /usr/sbi
n/httpd from getattr access on the file /var/www/html/test.html.#012#012***** P
ugin 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_content_t.#012Then you can run restorecon. The access attempt may have
```

Figure 3.16: Просмотр системного лог-файла

13. Поменяли прослушивание TCP-порта на 81. (fig. 3.17)



```
Open [icon] httpd.conf [Read-Only]
/etc/httpd/conf
43 # available when the service starts. See the httpd.service(8) man
44 # page for more information.
45 #
46 #Listen 12.34.56.78:80
47 Listen 81
48
```

Figure 3.17: Изменение прослушивания TCP-порта

14. Перезапустили Apache, не получили ошибки. (fig. 3.18)

```
[root@aiishanova ~]# systemctl restart httpd
[root@aiishanova ~]# tail -n1 /var/log/messages
Oct 15 18:16:08 aiishanova httpd[41122]: Server configured, listening on: port 8
1
[root@aiishanova ~]#
```

Figure 3.18: Перезапуск Apache

15. Добавили порт 81 и проверили, что он появился в списке. (fig. 3.19)

```
[root@aiishanova ~]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@aiishanova ~]# 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@aiishanova ~]#
```

Figure 3.19: Добавление порта 81

16. Перезапустили Apache, вернули изначальный контекст test.html. (fig. 3.20)

```
[root@aiishanova ~]# systemctl restart httpd
[root@aiishanova ~]# chcon -t httpd_sys_content_t /var/www/html/test.html
```

Figure 3.20: Перезапуск Apache, возвращение изначального контекста test.html

17. Обратились к файлу через веб-сервер. (fig. 3.21)

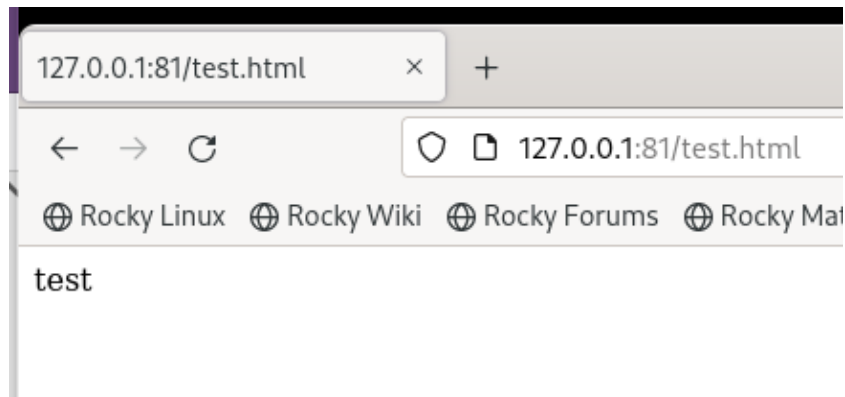


Figure 3.21: Обращение к файлу через браузер после возвращения контекста

18. Вернули порт 80. (fig. 3.22)

```
aiishanova@aiishanova:/home/aiishanova — nano /etc/httpd/conf/httpd.conf
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf
# directive.
#
# Change this to Listen on a specific IP address, but note that
# httpd.service is enabled to run at boot time, the address must
# be available when the service starts. See the httpd.service(8)
# page for more information.
#
#Listen 12.34.56.78:80
Listen 80
```

Figure 3.22: Возвращение порта 80 в httpd.conf

19. Ввели команду для удаления порта 81 из списка. Удалили файл test.html. (fig. 3.23)

```
[root@aiishanova ~]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@aiishanova ~]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@aiishanova ~]#
```

Figure 3.23: Работа команды удаления порта 81 и удаление test.html

4 Вывод

В ходе выполнения лабораторной работы были развиты навыки администрирования ОС Linux и проверена работа SELinux на практике совместно с веб-сервером Apache.

5 Библиография

1. Методические материалы курса.
2. Wikipedia: SELinux (URL: <https://ru.wikipedia.org/wiki/SELinux>)
3. Wikipedia: Apache HTTP Server (URL: https://ru.wikipedia.org/wiki/Apache_HTTP_Server)