

Лабораторная №6

Основы информационной безопасности

Жибицкая Е.Д.

Российский университет дружбы народов, Москва, Россия

Цель

- Развитие навыков администрирования ОС Linux. Знакомство с технологией SELinux1 и проверка работы SELinx на практике совместно с веб-сервером Apache

Ход работы

```
edzhibitskaya@edzhibitskaya ~]$ sudo dnf install httpd -y
[sudo] password for edzhibitskaya:
Last metadata expiration check: 0:10:00 ago on Tue 11 Mar 2025 08:40:33 PM MSK.
Dependencies resolved.
=====
Package           Arch      Version      Repository    Size
=====
Installing:
httpd             x86_64    2.4.62-1.el9_5.2  appstream    45 k
Installing dependencies:
apr               x86_64    1.7.0-12.el9_3  appstream    122 k
apr-util          x86_64    1.6.1-23.el9    appstream    94 k
apr-util-devel    x86_64    1.6.1-23.el9    appstream    12 k
=====
```

Рис. 1: Установка Apache

Сначала проведем подготовительные действия: для работы необходим Apache - установим его, также уберем пакетный фильтр.

```
edzhibitskaya@edzhibitskaya ~]$ getenforce
enforcing
edzhibitskaya@edzhibitskaya ~]$ 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
edzhibitskaya@edzhibitskaya ~]$ 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: disabled)
   Active: active (running) since Tue 2025-03-11 20:54:02 MSK; 6min ago
     Docs: man:httpd.service(8)
   Main PID: 7222 (httpd)
   CGroup: /systemd/system/httpd.service
```

Рис. 2: Статус Selinux

```
[edzhbitskaya@edzhbitskaya ~]$ ps auxZ | grep httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 edzhibi+ 47491 0.0 0.5 23
7756 9300 pts/1 T 20:51 0:00 /bin/systemctl status httpd.service
system_u:system_r:httpd_t:s0 root 73298 0.0 0.6 21236 11492 ?
Ss 20:54 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 73299 0.0 0.4 22968 7652 ?
S 20:54 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 73303 0.0 0.6 982392 11368 ?
Sl 20:54 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 73304 0.0 0.9 1113528 17732 ?
Sl 20:54 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 73305 0.0 0.6 982392 11368 ?
Sl 20:54 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 edzhibi+ 73493 0.0 0.5 23
7756 9428 pts/1 T 20:54 0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 edzhibi+ 73641 0.0 0.5 23
7756 9556 pts/0 T 21:00 0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 edzhibi+ 73692 0.0 0.1 22
1796 2560 pts/0 S+ 21:02 0:00 grep --color=auto httpd
[edzhbitskaya@edzhbitskaya ~]$
```

Рис. 3: Контекст безопасности

```
[edzhbitskaya@edzhbitskaya ~]$ 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
```

Рис. 4: Состояние переключателей для Apache

Посмотрим статистику по политике с помощью команды `seinfo`, также определим множество пользователей, ролей, типов.

```
[edzhibitskaya@edzhibitskaya ~]$  
[edzhibitskaya@edzhibitskaya ~]$ 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 Constrain:           72       MLS Val. Tran:        0  
Permissives:             1        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        Nodecon:              0  
[edzhibitskaya@edzhibitskaya ~]$
```


Определение типа файлов в каталоге, создание нового

```
[edzhibitskaya@edzhibitskaya ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Jan 22 03
:25 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Jan 22 03
:25 html
[edzhibitskaya@edzhibitskaya ~]$ ls -lZ /var/www/html
total 0
[edzhibitskaya@edzhibitskaya ~]$
```

Рис. 6: Типы файлов

```
[edzhibitskaya@edzhibitskaya ~]$ su -
Password:
[root@edzhibitskaya ~]# touch /var/www/html/test.html
[root@edzhibitskaya ~]# nano /var/www/html/test.html
[root@edzhibitskaya ~]#
```

Рис. 7: Создание файла



```
root@edzhibitskaya:~  
GNU nano 5.6.1 /var/www/html/test.html  
<html>  
<body>test</body>  
</html>
```

Рис. 8: Test.html

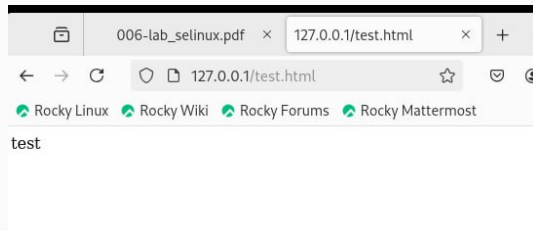
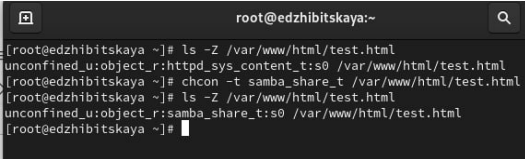


Рис. 9: Проверка сервера

Далее проверим контекст файла командой `ls -Z` и изучим его подробно. Изменим его на `samba_share_t` и убедимся, что это произошло.

A terminal window titled 'root@edzhbitskaya:~' with a search icon in the top right. It displays the following commands and output:

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

Рис. 10: Контекст файла

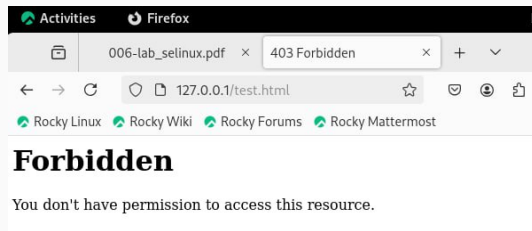
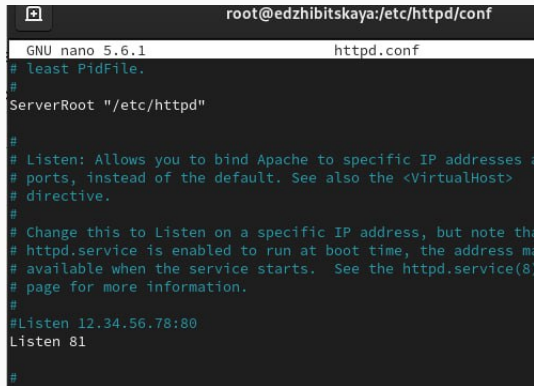


Рис. 11: Доступ к серверу

```
[root@edzhibitskaya ~]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 Mar 11 21:13 /var/www/html/test.html
[root@edzhibitskaya ~]# tail /var/log/messages
Mar 11 21:18:34 edzhibitskaya systemd[1]: Created slice Slice /system/dbus-:1.1-
org.fedoraproject.SetroubleShootPrivileged.
Mar 11 21:18:34 edzhibitskaya systemd[1]: Started dbus-:1.1-org.fedoraproject.Se
troubleShootPrivileged@0.service.
Mar 11 21:18:37 edzhibitskaya setroubleShoot[74392]: SELinux is preventing /usr/
sbin/httpd from getattr access on the file /var/www/html/test.html. For complete
SELinux messages run: sealert -l 6a5b5ffd-8a25-4573-adfd-d94e011a3f27
Mar 11 21:18:37 edzhibitskaya setroubleShoot[74392]: SELinux is preventing /usr/
sbin/httpd from getattr access on the file /var/www/html/test.html.#012#012*****
Plugin restorecon (92.2 confidence) suggests *****#012#01
25f.....
```

Рис. 12: Системный лог-файл

Просмотрим log-файлы веб-сервера Apache. Также посмотрим системный лог-файл. Если в системе окажутся запущенными процессы setroubleShootd и audtd, то сможем увидеть ошибки, аналогичные указанным выше, в файле /var/log/audit/audit.log



```
root@edzhbitskaya:/etc/httpd/conf
GNU nano 5.6.1 httpd.conf
# least PidFile.
#
ServerRoot "/etc/httpd"
#
# Listen: Allows you to bind Apache to specific IP addresses and
# ports, instead of the default. See also the <VirtualHost>
# 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 81
#
```

Попробуем запустить веб-сервер Apache на прослушивание TCP-порта 81. Для этого в файле `/etc/httpd/httpd.conf` строчку `Listen 80` заменим на `Listen 81`.

Рис. 13: Порт 81

```
root@edzhibitskaya:~  
[root@edzhibitskaya ~]# service httpd restart  
Redirecting to /bin/systemctl restart httpd.service  
[root@edzhibitskaya ~]# tail -n1 /var/log/messages  
Mar 11 21:30:35 edzhibitskaya httpd[74853]: Server configured, listening on: port 81  
[root@edzhibitskaya ~]# tail -n1 /var/log/httpd/error_log  
[Tue Mar 11 21:30:35.287985 2025] [core:notice] [pid 74853:tid 74853] AH00094: Core command line: '/usr/sbin/httpd -D FOREGROUND'  
[root@edzhibitskaya ~]# tail -n1 /var/log/httpd/access_log  
127.0.0.1 - - [11/Mar/2025:21:27:43 +0300] "GET /test.html HTTP/1.1" 403 199 "-"  
"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"  
[root@edzhibitskaya ~]# tail -n1 /var/log/audit/audit.log  
type=SERVICE_START msg=audit(1741717835.264:332): pid=1 uid=0 auid=4294967295 se  
s=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=httpd comm="systemd" exe  
="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root"  
AUID="unset"  
[root@edzhibitskaya ~]#
```

Рис. 14: Перезапуск и анализ файлов

```
[root@edzhibitskaya ~]# 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@edzhibitskaya ~]#
```

Рис. 15: Системный лог-файл

Вернем контекст `httpd_sys_content__t` к файлу `/var/www/html/ test.html` и попробуем получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`

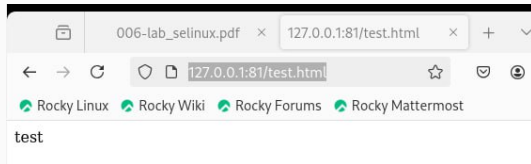


Рис. 16: Повторный запуск сервера


```
# change this to listen on a specific IP address; see note above
# httpd.service is enabled to run at boot time, the address may not
# available when the service starts. See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
Listen 80

#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as
# have to place corresponding 'LoadModule' lines at this location so
```

Рис. 17: Возвращение порта 80

```
pegasus_http_port_t tcp 5988
[root@edzhibitskaya conf]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@edzhibitskaya conf]#
```

Рис. 18: Удаление файла

Выводы

- В ходе работы было произведено знакомство с Apache и Selinux, получены навыки по работе с ними и взаимодействию с веб-сервером