

Отчет по лабораторной работе №6

Мандатное разграничение прав в Linux

Каримов Зуфар НПИ-01-18

Содержание

1 Цель работы	3
2 Последовательность выполнения работы	4
3 Выводы	17

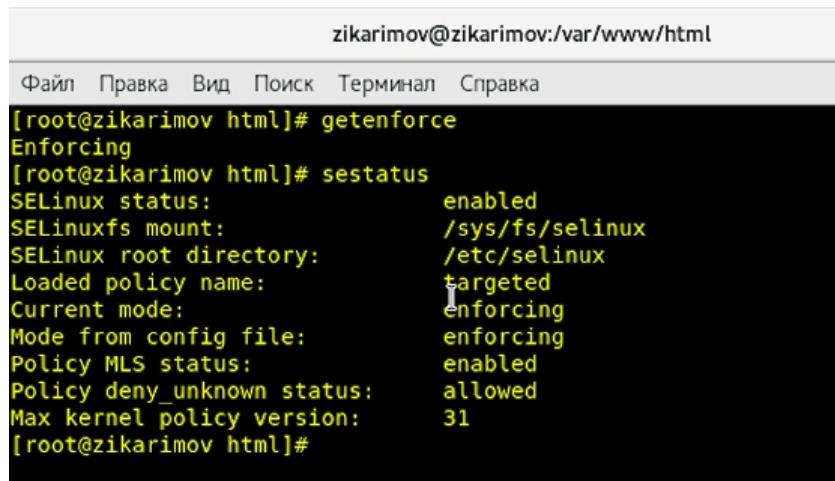
1 Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux.

Проверить работу SELinux на практике совместно с веб-сервером Apache.

2 Последовательность выполнения работы

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus (рис. 2.1)



The screenshot shows a terminal window with the title bar "zikarimov@zikarimov:/var/www/html". The menu bar includes "Файл", "Правка", "Вид", "Поиск", "Терминал", and "Справка". The terminal content displays the output of SELinux commands:

```
[root@zikarimov html]# getenforce
Enforcing
[root@zikarimov html]# 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@zikarimov html]#
```

Figure 2.1: SELinux

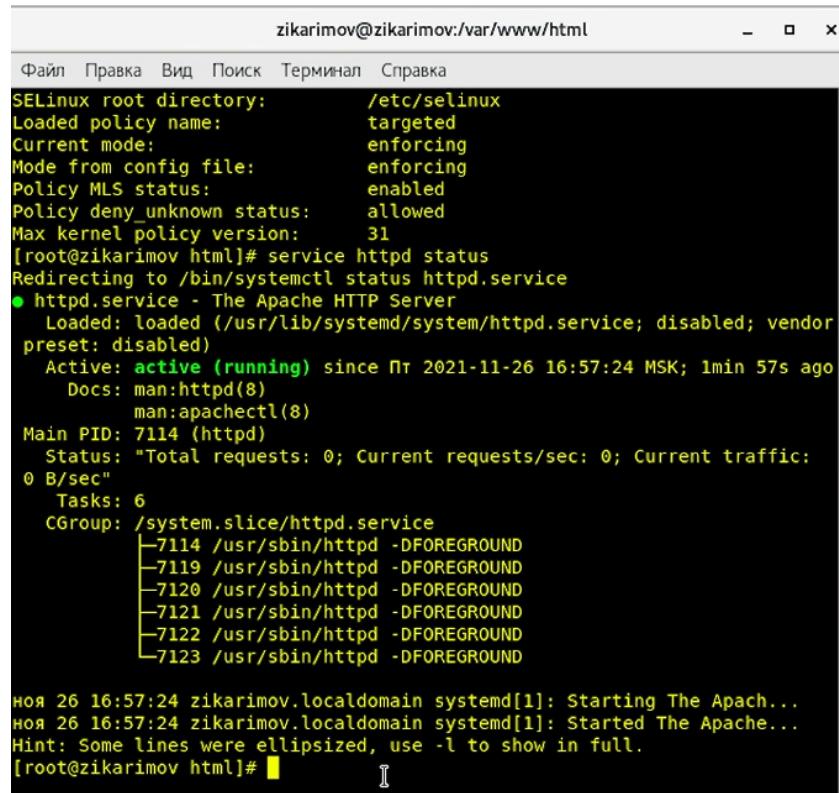
2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает:

service httpd status

или

/etc/rc.d/init.d/httpd status

Если не работает, запустите его так же, но с параметром start. (рис. 2.2)



```
zikarimov@zikarimov:/var/www/html
Файл Правка Вид Поиск Терминал Справка
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@zikarimov html]# 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 16:57:24 MSK; 1min 57s ago
       Docs: man:httpd(8)
              man:apachectl(8)
   Main PID: 7114 (httpd)
      Status: "Total requests: 0; Current requests/sec: 0; Current traffic:
0 B/sec"
      Tasks: 6
     CGroup: /system.slice/httpd.service
             ├─7114 /usr/sbin/httpd -DFOREGROUND
             ├─7119 /usr/sbin/httpd -DFOREGROUND
             ├─7120 /usr/sbin/httpd -DFOREGROUND
             ├─7121 /usr/sbin/httpd -DFOREGROUND
             ├─7122 /usr/sbin/httpd -DFOREGROUND
             └─7123 /usr/sbin/httpd -DFOREGROUND

ноя 26 16:57:24 zikarimov.localdomain systemd[1]: Starting The Apache...
ноя 26 16:57:24 zikarimov.localdomain systemd[1]: Started The Apache...
Hint: Some lines were ellipsized, use -l to show in full.
[root@zikarimov html]#
```

Figure 2.2: Apache HTTP Server

3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду

ps auxZ | grep httpd

ИЛИ

ps -eZ | grep httpd (рис. 2.3)

```
zikarimov@zikarimov:~\nФайл Правка Вид Поиск Терминал Справка\n[root@zikarimov ~]# ps auxZ | grep httpd\nsystem_u:system_r:htpd_t:s0    root      7114  0.0  0.2 224084  5016 ?\n    Ss 16:57 0:00 /usr/sbin/httpd -DFOREGROUND\nsystem_u:system_r:htpd_t:s0    apache    7119  0.0  0.1 226168  3092 ?\n    Ss 16:57 0:00 /usr/sbin/httpd -DFOREGROUND\nsystem_u:system_r:htpd_t:s0    apache    7120  0.0  0.1 226168  3092 ?\n    Ss 16:57 0:00 /usr/sbin/httpd -DFOREGROUND\nsystem_u:system_r:htpd_t:s0    apache    7121  0.0  0.1 226168  3092 ?\n    Ss 16:57 0:00 /usr/sbin/httpd -DFOREGROUND\nsystem_u:system_r:htpd_t:s0    apache    7122  0.0  0.1 226168  3092 ?\n    Ss 16:57 0:00 /usr/sbin/httpd -DFOREGROUND\nsystem_u:system_r:htpd_t:s0    apache    7123  0.0  0.1 226168  3092 ?\n    Ss 16:57 0:00 /usr/sbin/httpd -DFOREGROUND\nunconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 7273 0.0  0.0 1\n12832 976 pts/0 S+ 16:59 0:00 grep --color=auto httpd\n[root@zikarimov ~]#\n
```

Figure 2.3: Apache в списке процессов

4. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды

`sestatus -b | grep httpd`

Обратите внимание, что многие из них находятся в положении «off». (рис. 2.4)

```
zikarimov@zikarimov:~\nФайл Правка Вид Поиск Терминал Справка\n[root@zikarimov ~]# sestatus -b | grep httpd\nhttpd_anon_write                      off\nhttpd_builtin_scripting                 on\nhttpd_can_check_spam                   off\nhttpd_can_connect_ftp                  off\nhttpd_can_connect_ldap                 off\nhttpd_can_connect_mythtv               off\nhttpd_can_connect_zabbix              off\nhttpd_can_network_connect             off\nhttpd_can_network_connect_cobbler     off\nhttpd_can_network_connect_db          off\nhttpd_can_network_memcache            off\nhttpd_can_network_relay                off\nhttpd_can_sendmail                   off\nhttpd_dbus_avahi                     off\nhttpd_dbus_sssd                      off\nhttpd_dontaudit_search_dirs           off\nhttpd_enable_cgi                      on\nhttpd_enable_ftp_server                off\nhttpd_enable_homedirs                 off\nhttpd_execmem                         off\nhttpd_graceful_shutdown               on\nhttpd_manage_ipa                      off\nhttpd_mod_auth_ntlm_winbind          off\nhttpd_mod_auth_pam                   off\nhttpd_read_user_content              off\nhttpd_run_ipa                        off\nhttpd_run_preupgrade                 off\nhttpd_run_stickshift                 off\nhttpd_serve_cobbler_files            off\nhttpd_setrlimit                      off\nhttpd_ssi_exer                       off\n
```

Figure 2.4: Текущее состояние переключателей SELinux для Apache

5. Посмотрите статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов. (рис. 2.5)

```
zikarimov@zikarimov:~  
Файл Правка Вид Поиск Терминал Справка  
[root@zikarimov ~]# 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@zikarimov ~]#
```

Figure 2.5: Статистику по политике

Множество типов: 4793. Множество пользователей: 8. Множество ролей: 14.

6. Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды (рис. 2.6)

ls -lZ /var/www

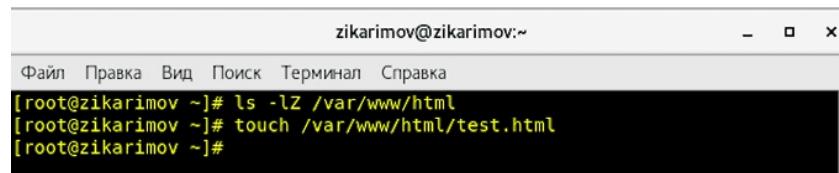
```
zikarimov@zikarimov:~  
Файл Правка Вид Поиск Терминал Справка  
[root@zikarimov ~]# ls -lZ /var/www  
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin  
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html  
[root@zikarimov ~]#
```

Figure 2.6: Определение типов файлов и поддиректорий

7. Определите тип файлов, находящихся в директории /var/www/html:

ls -lZ /var/www/html (рис. 2.7)

8. Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html.

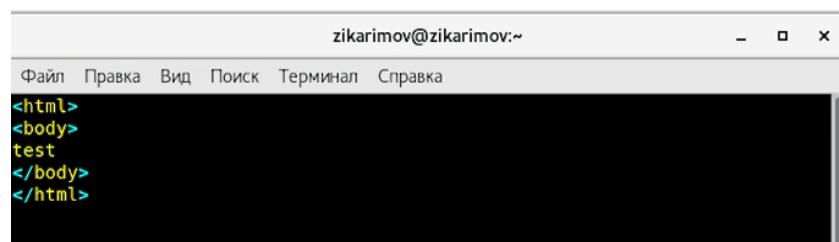


```
zikarimov@zikarimov:~  
Файл Правка Вид Поиск Терминал Справка  
[root@zikarimov ~]# ls -lZ /var/www/html  
[root@zikarimov ~]# touch /var/www/html/test.html  
[root@zikarimov ~]#
```

Figure 2.7: Определение типов файлов и поддиректорий

9. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания: (рис. 2.8)

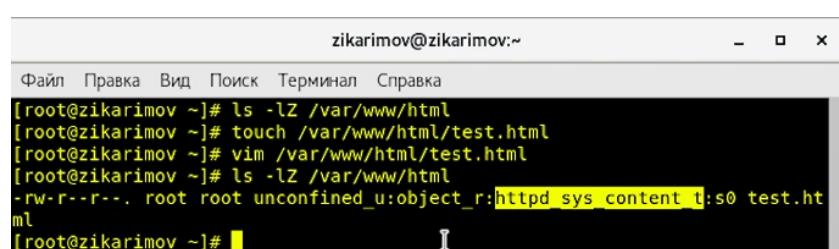
test



```
zikarimov@zikarimov:~  
Файл Правка Вид Поиск Терминал Справка  
<html>  
<body>  
test  
</body>  
</html>
```

Figure 2.8: Файл test.html

10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html (рис. 2.9)



```
zikarimov@zikarimov:~  
Файл Правка Вид Поиск Терминал Справка  
[root@zikarimov ~]# ls -lZ /var/www/html  
[root@zikarimov ~]# touch /var/www/html/test.html  
[root@zikarimov ~]# vim /var/www/html/test.html  
[root@zikarimov ~]# ls -lZ /var/www/html  
-rw-r--r-- root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html  
[root@zikarimov ~]#
```

Figure 2.9: Контекст файла

11. Обратитесь к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>.

Убедитесь, что файл был успешно отображён. (рис. 2.10)

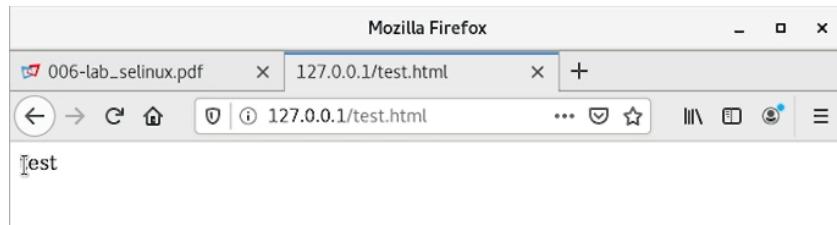


Figure 2.10: Обращение к файлу через браузер

12. Изучите справку man httpd_selinux и выясните, какие контексты файлов определены для httpd. Сопоставьте их с типом файла test.html. Проверить контекст файла можно командой ls -Z.

```
ls -Z /var/www/html/test.html
```

Рассмотрим полученный контекст детально. Обратите внимание, что так как по умолчанию пользователи CentOS являются свободными от типа (unconfined в переводе с англ. означает свободный), созданному нами файлу test.html был сопоставлен SELinux, пользователь unconfined_u. Это первая часть контекста. Далее политика ролевого разделения доступа RBAC используется процессами, но не файлами, поэтому роли не имеют никакого значения для файлов. Роль object_r используется по умолчанию для файлов на «постоянных» носителях и на сетевых файловых системах. (В директории /proc файлы, относящиеся к процессам, могут иметь роль system_r. Если активна политика MLS, то могут использоваться и другие роли, например, secadm_r. Данного случая мы рассматривать не будем, как и предназначение :s0).

Тип httpd_sys_content_t позволяет процессу httpd получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер.

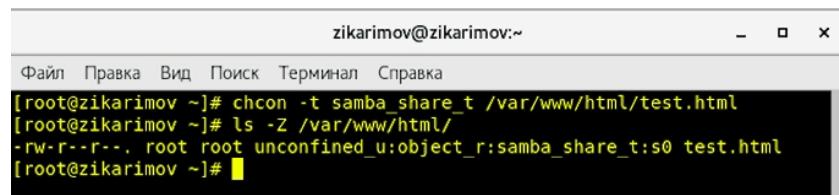
13. Измените контекст файла /var/www/html/test.html с httpd_sys_content_t на

любой другой, к которому процесс httpd не должен иметь доступа, например, на samba_share_t: (рис. 2.11)

```
chcon -t samba_share_t /var/www/html/test.html
```

```
ls -Z /var/www/html/test.html
```

После этого проверьте, что контекст поменялся



A screenshot of a terminal window titled "zikarimov@zikarimov:~". The window contains the following text:

```
зикаримов@зикаримов:~ - □ ×
Файл Правка Вид Поиск Терминал Справка
[root@zikarimov ~]# chcon -t samba_share_t /var/www/html/test.html
[root@zikarimov ~]# ls -Z /var/www/html/
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 test.html
[root@zikarimov ~]# █
```

Figure 2.11: Изменение контекста файла

14. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Вы должны получить сообщение об ошибке: (рис. 2.12)

Forbidden

You don't have permission to access /test.html on this server.

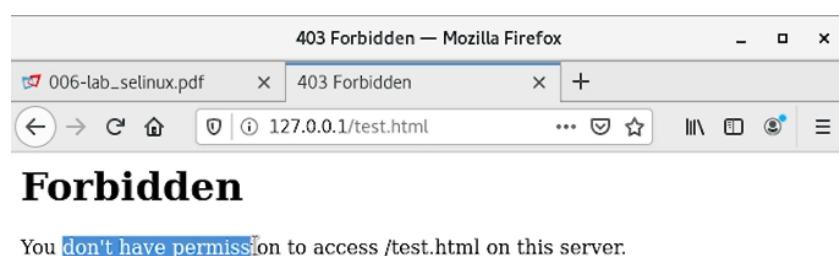


Figure 2.12: Обращение к файлу через браузер

15. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? (рис. 2.13) (рис. 2.14)

```
ls -l /var/www/html/test.html
```

Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл:

```
tail /var/log/messages
```

Если в системе окажутся запущенными процессы `setroubleshootd` и `audtd`, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле `/var/log/audit/audit.log`. Проверьте это утверждение самостоятельно.

```
zikarimov@zikarimov:~ - □ ×
Файл Правка Вид Поиск Терминал Справка
[root@zikarimov ~]# chcon -t samba_share_t /var/www/html/test.html
[root@zikarimov ~]# ls -Z /var/www/html/
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 test.html
[root@zikarimov ~]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 37 ноя 26 17:02 /var/www/html/test.html
[root@zikarimov ~]# █
```

Figure 2.13: Права доступа

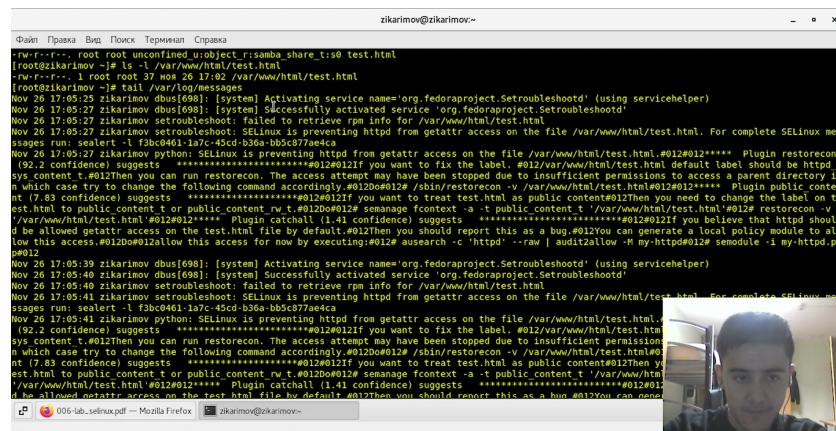


Figure 2.14: log-файлы веб-сервера Apache

16. Попробуйте запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf найдите строчку Listen 80 и замените её на Listen 81. (рис. 2.15)

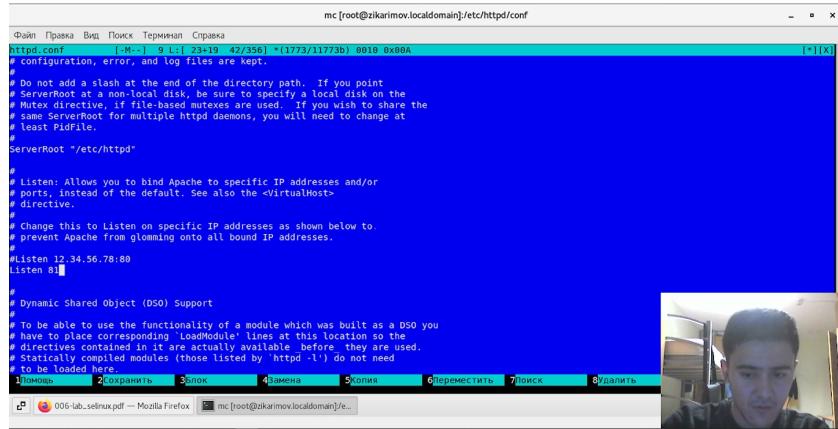


Figure 2.15: TCP-порт 81

17. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему? (рис. 2.16)

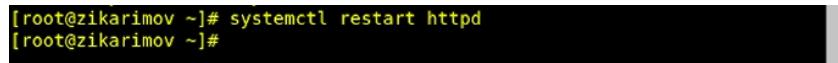


Figure 2.16: Перезапуск веб-сервера Apache

Никакого сбоя не произошло.

18. Проанализируйте лог-файлы: (рис. 2.17)

```
zikarimov@zikarimov:~ - x
Файл Правка Вид Поиск Терминал Справка
Nov 26 17:05:41 zikarimov python: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html.#012#012***** Plugin 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 been stopped due to insufficient permissions to access a parent directory in which case try to change the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin publ ic_content (7.83 confidence) suggests *****#012#012If you want to treat test.html as public content#012Then you need to change the label on test.html to public_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012# re storecon -v '/var/www/html/test.html'#012#012***** Plugin catchall (1.41 confidence) suggests *****#012#012If you believe that httpd should be allowed getattr access on the test.html file by default .#012Then you should report this as a bug.#012You can generate a local policy module to allow this access.#012Do#012allow this access for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -i my-httpd.pp#012
Nov 26 17:07:58 zikarimov dbus[698]: [system] Activating service name='org .freedesktop.problems' (using servicehelper)
Nov 26 17:07:59 zikarimov dbus[698]: [system] Successfully activated service 'org.freedesktop.problems'
Nov 26 17:09:39 zikarimov systemd: Stopping The Apache HTTP Server...
Nov 26 17:09:40 zikarimov systemd: Stopped The Apache HTTP Server.
Nov 26 17:09:40 zikarimov systemd: Starting The Apache HTTP Server...
Nov 26 17:09:40 zikarimov systemd: Started The Apache HTTP Server.
Nov 26 17:10:01 zikarimov systemd: Created slice User Slice of root.
Nov 26 17:10:01 zikarimov systemd: Started Session 14 of user root.
Nov 26 17:10:01 zikarimov systemd: Removed slice User Slice of root.
[root@zikarimov ~]# █
```

Figure 2.17: log-файлы веб-сервера Apache

19. Выполните команду

```
semanage port -a -t http_port_t -p tcp 81
```

После этого проверьте список портов командой

```
semanage port -l | grep http_port_t
```

Убедитесь, что порт 81 появился в списке. (рис. 2.18)

```
zikarimov@zikarimov:~ - □ ×
Файл Правка Вид Поиск Терминал Справка
[root@zikarimov ~]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@zikarimov ~]# 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@zikarimov ~]# █
```

Figure 2.18: Проверка порта

20. Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему он

сейчас запустился, а в предыдущем случае не смог? (рис. 2.19)

```
[root@zikarimov ~]# systemctl restart httpd
[root@zikarimov ~]#
```

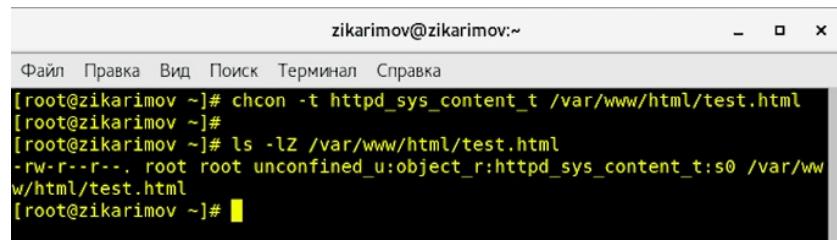
Figure 2.19: Презапуск веб-сервера Apache

21. Верните контекст httpd_sys_content_t к файлу /var/www/html/test.html: (рис. 2.20)

```
chcon -t httpd_sys_content_t /var/www/html/test.html
```

После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html.

Вы должны увидеть содержимое файла — слово «test». (рис. 2.21)



The screenshot shows a terminal window titled 'zikarimov@zikarimov:~'. The menu bar includes 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The terminal history shows:

```
[root@zikarimov ~]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@zikarimov ~]#
[root@zikarimov ~]# ls -lZ /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@zikarimov ~]#
```

Figure 2.20: Изменение контекста

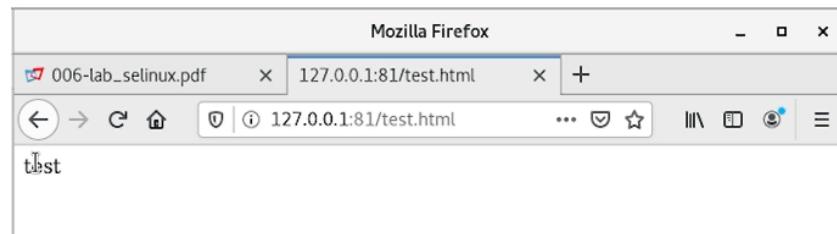


Figure 2.21: Обращение к файлу через браузер

22. Исправьте обратно конфигурационный файл apache, вернув Listen 80. (рис. 2.22)

```
mc [root@zikarimov.localdomain]:/etc/httpd/conf
Файл Правка Вид Поиск Терминал Справка
httpd.conf      [---] 9 L:[ 29+13 42/356] *(1773/11773b) 0010 [*][X]
# 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 specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#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 a DSO
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used
# Statically compiled modules (those listed by 'httpd -l') do not need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
Include conf.modules.d/*.conf
```

Figure 2.22: TCP-порт 80

23. Удалите привязку http_port_t к 81 порту:

semanage port -d -t http_port_t -p tcp 81

и проверьте, что порт 81 удалён. (рис. 2.23) (рис. 2.24)

```
zkarimov@zkarimov:~
Файл Правка Вид Поиск Терминал Справка
[root@zkarimov ~]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@zkarimov ~]#
```

Figure 2.23: Удаление TCP-порта 81

```
[root@zkarimov ~]# 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@zkarimov ~]#
```

Figure 2.24: Удаление TCP-порта 81

24. Удалите файл /var/www/html/test.html:

rm /var/www/html/test.html (рис. 2.25)

```
[root@zikarimov ~]# rm /var/www/html/test.html
rm: удалять обычный файл «/var/www/html/test.html»? y
[root@zikarimov ~]# ls -lz /var/www/
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[root@zikarimov ~]# ls -lz /var/www/html/
[root@zikarimov ~]#
```

Figure 2.25: Удаление файла

3 Выводы

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux.

Проверил работу SELinux на практике совместно с веб-сервером Apache.