

# Лабораторная работа №6

Титаренко Анастасия Дмитриевна

## Содержание

Цель работы .....	1
Выполнение лабораторной работы .....	1
Вывод.....	10
Список литературы .....	10

## Цель работы

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

## Выполнение лабораторной работы

1. Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.

```
[adtitarenko@adtitarenko ~]$ getenforce
Enforcing
[adtitarenko@adtitarenko ~]$ 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
[adtitarenko@adtitarenko ~]$
```

*Проверка, что SELinux работает в режиме enforcing политики targeted*

2. Обратилась с помощью браузера к веб-серверу, запущенному на компьютере, и убедилась, что последний работает: `service httpd status` или `/etc/rc.d/init.d/httpd status`

```
[adtitarenko@adtitarenko ~]$ 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 Чт 2022-10-13 22:43:10 MSK; 3s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Main PID: 9545 (httpd)
    Status: "Processing requests..."
     Tasks: 6
    CGroup: /system.slice/httpd.service
            └─9545 /usr/sbin/httpd -DFOREGROUND
              └─9549 /usr/sbin/httpd -DFOREGROUND
                └─9550 /usr/sbin/httpd -DFOREGROUND
                  └─9551 /usr/sbin/httpd -DFOREGROUND
                    └─9552 /usr/sbin/httpd -DFOREGROUND
                      └─9553 /usr/sbin/httpd -DFOREGROUND

окт 13 22:43:08 adtitarenko systemd[1]: Starting The Apache HTTP Server...
окт 13 22:43:09 adtitarenko httpd[9545]: AH00558: httpd: Could not reliably det...ge
окт 13 22:43:10 adtitarenko systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[adtitarenko@adtitarenko ~]$
```

*Проверка, что веб-сервис запущен*

3. Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности. Используя команду: `ps auxZ | grep httpd`

```
[adtitarenko@adtitarenko ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 9545 0.0 0.2 230440 5244 ? Ss 22:43:10 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 9549 0.0 0.1 232524 3160 ? S 22:43:10 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 9550 0.0 0.1 232524 3160 ? S 22:43:10 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 9551 0.0 0.1 232524 3160 ? S 22:43:10 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 9552 0.0 0.1 232524 3160 ? S 22:43:10 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 9553 0.0 0.1 232524 3160 ? S 22:43:10 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-c0.c1023 adtitara+ 9594 0.0 0.0 112832 968 pts/0 S+ 22:44 0:00 grep --color=auto httpd
[adtitarenko@adtitarenko ~]$
```

*Нахождение веб-сервер Apache в списке процессов*

4. Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды: `sestatus -bigrep httpd`. Обратила внимание, что многие из них находятся в положении «off»

```
[adtitarenko@adtitarenko ~]$ 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
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          on
httpd_manage_ipa                 off
httpd_mod_auth_ntlm_winbind      off
```

*Текущее состояние переключателей SELinux для Apache*

- Посмотрела статистику по политике с помощью команды `seinfo`, также определила множество пользователей, ролей, типов.

```
[adtitarenko@adtitarenko ~]$ 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

[adtitarenko@adtitarenko ~]$
```

*Статистика по политике с помощью команды `seinfo`*

- Определила тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды: `ls -lZ /var/www`

```
[adtitarenko@adtitarenko ~]$ 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
[adtitarenko@adtitarenko ~]$
[adtitarenko@adtitarenko ~]$
[adtitarenko@adtitarenko ~]$
```

*Типы файлов и поддиректорий, находящихся в директории `/var/www`*

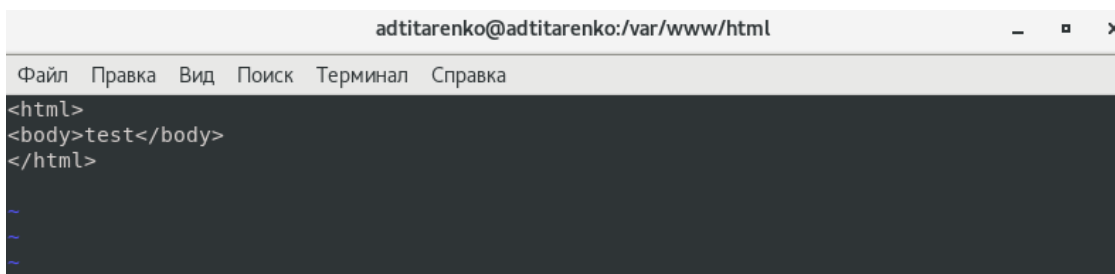
7. Определила тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html

```
[adtitarenko@adtitarenko ~]$  
[adtitarenko@adtitarenko ~]$ ls -lZ /var/www/html  
[adtitarenko@adtitarenko ~]$  
[adtitarenko@adtitarenko ~]$
```

*Типы файлов, находящихся в директории /var/www/html*

8. Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html.
9. Создала от имени суперпользователя html-файл /var/www/html/test.html следующего содержания:

test



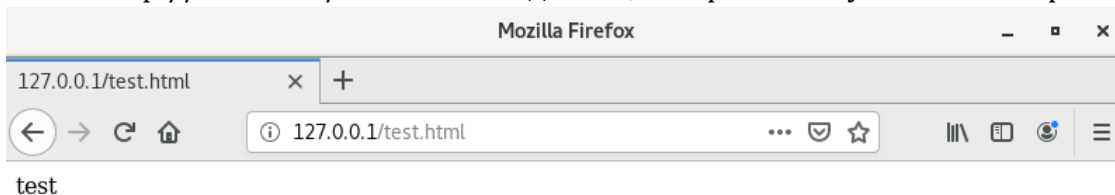
*Создание html-файла test.html*

10. Проверила контекст созданного файла.

```
[root@adtitarenko html]# cat test.html  
<html>  
<body>test</body>  
</html>  
  
[root@adtitarenko html]# ls -lZ  
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html  
[root@adtitarenko html]#
```

*Контекст созданного файла*

11. Обратилась к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедилась, что файл был успешно отображён.



*Обращение к файлу через веб-сервер*

12. Изучила справку man httpd\_selinux и выяснила, какие контексты файлов определены для httpd.

```
HTTPD(8)                                httpd                                HTTPD(8)

NAME
    httpd - Apache Hypertext Transfer Protocol Server

SYNOPSIS
    httpd [ -d serverroot ] [ -f config ] [ -C directive ] [ -c directive ] [ -D
    parameter ] [ -e level ] [ -E file ] [ -k start|restart|graceful|stop|grace-
    ful-stop ] [ -R directory ] [ -h ] [ -l ] [ -L ] [ -S ] [ -t ] [ -v ] [ -V ]
    [ -X ] [ -M ] [ -T ]

    On Windows systems, the following additional arguments are available:

    httpd [ -k install|config|uninstall ] [ -n name ] [ -w ]

SUMMARY
    httpd is the Apache HyperText Transfer Protocol (HTTP) server program. It is
    designed to be run as a standalone daemon process. When used like this it
    will create a pool of child processes or threads to handle requests.

    In general, httpd should not be invoked directly, but rather should be
    invoked via apachectl on Unix-based systems or as a service on Windows NT,
    2000 and XP and as a console application on Windows 9x and ME.

Manual page httpd(8) line 1/121 25% (press h for help or q to quit)
```

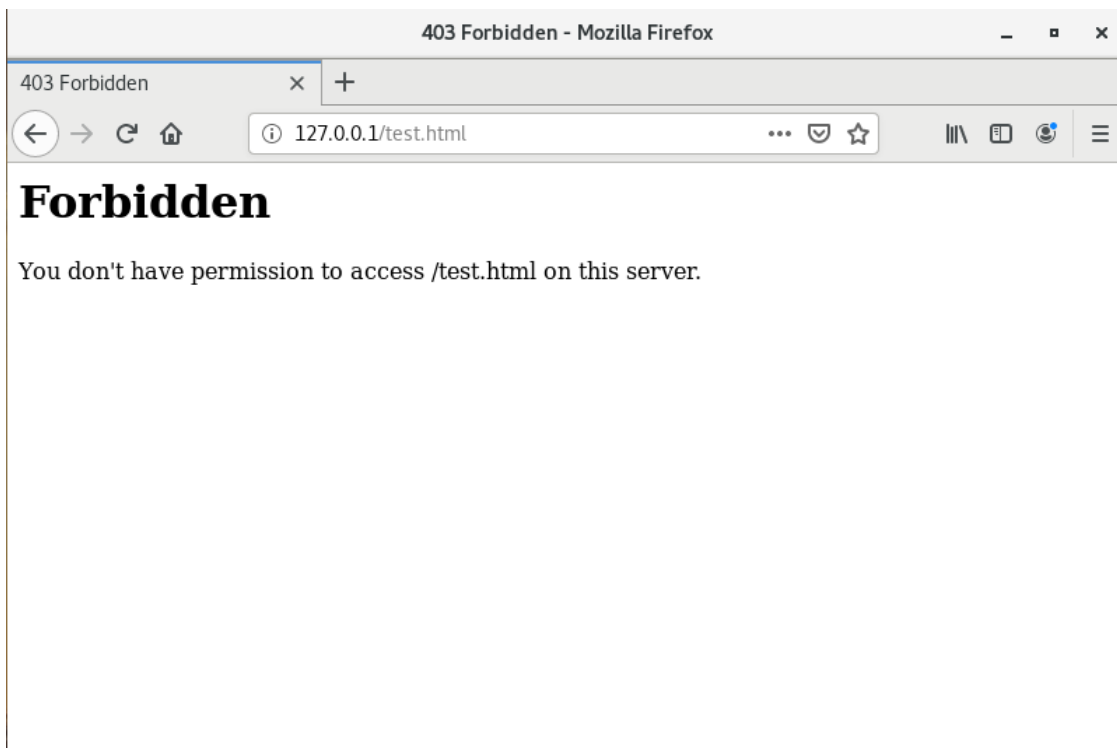
#### *Справка man httpd*

13. Изменила 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: chcon -t samba\_share\_t /var/www/html/test.html ls -Z /var/www/html/test.html После этого проверила, что контекст поменялся.

```
[root@adtitarenko html]# chcon -t samba_share_t /var/www/html/test.html
[root@adtitarenko html]# ls -lZ /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@adtitarenko html]#
[root@adtitarenko html]#
[root@adtitarenko html]#
```

#### *Изменение контекста файла /var/www/html/test.html*

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



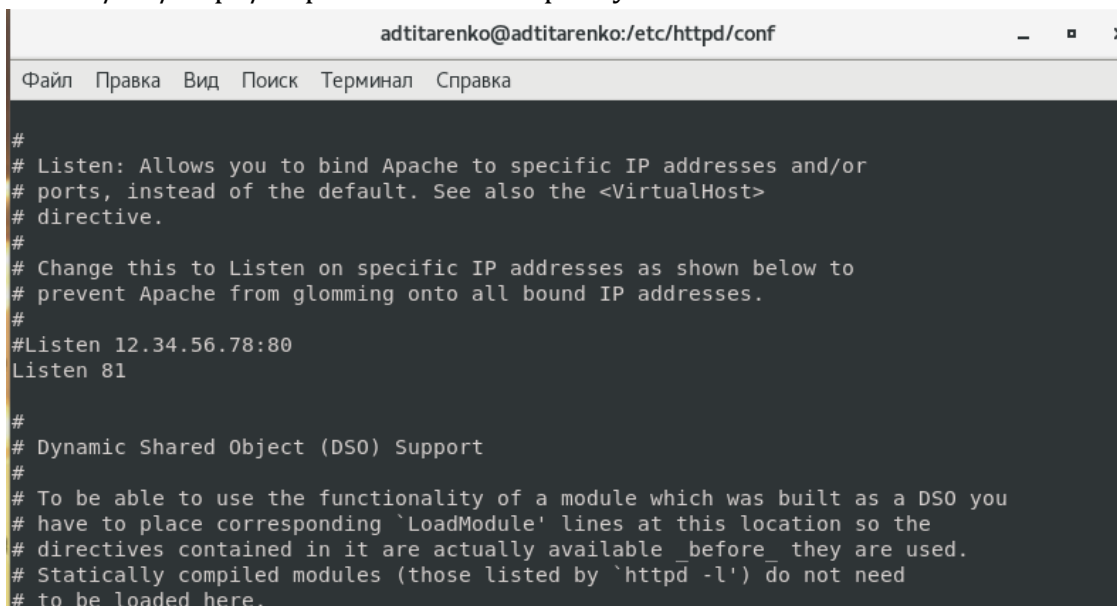
*Доступ к файлу через веб-сервер*

15. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? `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.

```
[root@adtitarenko html]# tail /var/log/messages
Oct 13 23:13:27 adtitarenko dbus[693]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
Oct 13 23:13:28 adtitarenko dbus[693]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
Oct 13 23:13:28 adtitarenko setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Oct 13 23:13:28 adtitarenko setroubleshoot: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l e2b583dc-d028-49af-b78b-916d0fbb1a68
Oct 13 23:13:28 adtitarenko 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 public_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# restorecon -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
```

### log-файлы веб-сервера Apache

16. Попробовала 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 нашла строчку Listen 80 и заменила её на Listen 81.



```
adtitarenko@adtitarenko:/etc/httpd/conf
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
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# 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.
```

### Запуск веб-сервер Apache на прослушивание TCP-порта 81

17. Выполнила перезапуск веб-сервера Apache. Произошёл сбой.

```
[root@adtitarenko conf]#
[root@adtitarenko conf]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@adtitarenko conf]#
[root@adtitarenko conf]#
```

### Перезапуск веб-сервера Apache



18. Проанализировала лог-файлы: `tail -nl /var/log/messages`. Просмотрела файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log` и выяснила, в каких файлах появились записи.

```
[root@adtitarenko conf]# tail -l /var/log/messages
Oct 13 23:30:04 adtitarenko systemd: Stopping The Apache HTTP Server...
Oct 13 23:30:05 adtitarenko systemd: Stopped The Apache HTTP Server.
Oct 13 23:30:05 adtitarenko systemd: Starting The Apache HTTP Server...
Oct 13 23:30:05 adtitarenko httpd: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using fe80::875a:3be7:b015:2e13. Set the 'ServerName' directive globally to suppress this message
Oct 13 23:30:05 adtitarenko systemd: Started The Apache HTTP Server.
Oct 13 23:33:00 adtitarenko systemd: Stopping The Apache HTTP Server...
Oct 13 23:33:01 adtitarenko systemd: Stopped The Apache HTTP Server.
Oct 13 23:33:01 adtitarenko systemd: Starting The Apache HTTP Server...
Oct 13 23:33:02 adtitarenko httpd: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using fe80::875a:3be7:b015:2e13. Set the 'ServerName' directive globally to suppress this message
Oct 13 23:33:02 adtitarenko systemd: Started The Apache HTTP Server.
[root@adtitarenko conf]#
```

Лог-файлы: `tail -nl /var/log/messages`

```
[root@adtitarenko httpd]# cat /var/log/httpd/error_log
[Thu Oct 13 22:43:09.231570 2022] [core:notice] [pid 9545] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Thu Oct 13 22:43:09.233168 2022] [suexec:notice] [pid 9545] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using fe80::875a:3be7:b015:2e13. Set the 'ServerName' directive globally to suppress this message
[Thu Oct 13 22:43:10.059966 2022] [lbmethod_heartbeat:notice] [pid 9545] AH02282: No slotm from mod_heartbeat
[Thu Oct 13 22:43:10.062822 2022] [mpm_prefork:notice] [pid 9545] AH00163: Apache/2.4.6 (CentOS) configured -- resuming normal operations
[Thu Oct 13 22:43:10.062933 2022] [core:notice] [pid 9545] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[Thu Oct 13 23:13:24.559257 2022] [core:error] [pid 9549] (13)Permission denied: [client 127.0.0.1:45998] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Thu Oct 13 23:30:04.164664 2022] [mpm_prefork:notice] [pid 9545] AH00170: caught SIGWINCH, shutting down gracefully
[Thu Oct 13 23:30:05.590829 2022] [core:notice] [pid 11368] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Thu Oct 13 23:30:05.591871 2022] [suexec:notice] [pid 11368] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using fe80::875a:3be7:b015:2e13. Set the 'ServerName' directive globally to suppress this message
```

Файл `/var/log/http/error_log`

```
[root@adtitarenko httpd]# cat /var/log/httpd/audit_log
cat: /var/log/httpd/audit_log: Нет такого файла или каталога
[root@adtitarenko httpd]#
[root@adtitarenko httpd]# cat /var/log/httpd/access_log
127.0.0.1 - - [13/Oct/2022:23:06:41 +0300] "GET /test.html HTTP/1.1" 200 34 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
127.0.0.1 - - [13/Oct/2022:23:06:41 +0300] "GET /favicon.ico HTTP/1.1" 404 209 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
127.0.0.1 - - [13/Oct/2022:23:13:24 +0300] "GET /test.html HTTP/1.1" 403 211 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
[root@adtitarenko httpd]#
```

Файлы `/var/log/http/access_log` и `/var/log/audit/audit.log`

19. Выполнила команду: `semanage port -a -t http_port_t -p tcp 81`. После этого проверила список портов командой: `semanage port -l | grep http_port_t`. Убедилась, что порт 81 появился в списке.



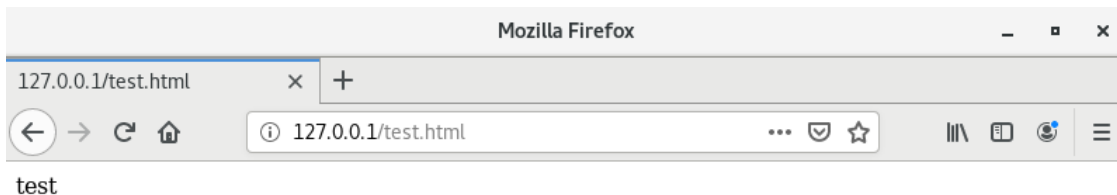
```
[root@adtitarenko httpd]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@adtitarenko httpd]#
[root@adtitarenko httpd]# semanage port -l | grep http_port_t
http_port_t          tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus http_port_t  tcp      5988
[root@adtitarenko httpd]#
```

### Список портов

20. Попробовала запустить веб-сервер Apache ещё раз.
21. Вернула контекст httpd\_sys\_content\_t к файлу /var/www/html/test.html: `chcon -t httpd_sys_content_t /var/www/html/test.html`. После этого попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`.

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

### Возвращение контекста httpd\_sys\_content\_t к файлу /var/www/html/test.html



### Доступ к файлу через веб-сервер

22. Исправила обратно конфигурационный файл apache, вернув `Listen 80`.

```
# 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 you
# 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.
```

### Исправление конфигурационного файла apache (Listen 80)

23. Удалила привязку http\_port\_t к 81 порту: `semanage port -d -t http_port_t -p tcp 81`. Проверила, что порт 81 удалён.

```
[root@adtitarenko httpd]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@adtitarenko httpd]# 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@adtitarenko httpd]#
[root@adtitarenko httpd]#
```

*Удаление привязки http\_port\_t к 81 порту*

24. Удалила файл /var/www/html/test.html: `rm /var/www/html/test.html`

```
[root@adtitarenko httpd]# rm /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»? y
[root@adtitarenko httpd]# cd /var/www/html/
[root@adtitarenko html]# ls
[root@adtitarenko html]#
```

*Удаление файла /var/www/html/test.html*

## Вывод

Развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux. Проверила работу SELinux на практике совместно с веб-сервером Apache.

## Список литературы

1. Лабораторная работа № 6. Мандатное разграничение прав в Linux