



# Лабораторная работа №6



# Цель лабораторной работы

Развитие навыков администрирования ОС Linux, первое практическое знакомство с технологией SELinux, а также проверка работы SELinux на практике совместно с веб-сервером Apache.

# Проверка работы SELinux и веб-сервера

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

```
[sofa@sofa ~]$ 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
```

```
[sofa@sofa ~]$ 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 Sat 2022-10-15 19:25:52 MSK; 37s ago  
     Docs: man:httpd(8)  
          man:apachectl(8)  
  Main PID: 3533 (httpd)  
    Status: "Total requests: 0; Current requests/sec: 0; Current traffic:  0 B/sec"  
     Tasks: 6  
   CGroup: /system.slice/httpd.service  
           └─3533 /usr/sbin/httpd -DFOREGROUND  
             └─3536 /usr/sbin/httpd -DFOREGROUND  
               └─3537 /usr/sbin/httpd -DFOREGROUND  
                 └─3538 /usr/sbin/httpd -DFOREGROUND  
                   └─3539 /usr/sbin/httpd -DFOREGROUND  
                     └─3540 /usr/sbin/httpd -DFOREGROUND  
  
Oct 15 19:25:51 sofa.localdomain systemd[1]: Starting The Apache HTTP Server...  
Oct 15 19:25:51 sofa.localdomain httpd[3533]: AH00558: httpd: Could not reliably d...ge  
Oct 15 19:25:52 sofa.localdomain systemd[1]: Started The Apache HTTP Server.  
Hint: Some lines were ellipsized, use -l to show in full.
```

# Веб-сервер Apache

```
[sofa@sofa ~]$ ps auxZ | grep httpd
```

system_u:system_r:ht	tpd	t:s0	root	3533	0.0	0.5	230440	5216	?	Ss	19:
25	0:00	/usr/sbin/ht	tpd -DFOREGROUND								
system_u:system_r:ht	tpd	t:s0	apache	3536	0.0	0.3	232524	3160	?	S	19:
25	0:00	/usr/sbin/ht	tpd -DFOREGROUND								
system_u:system_r:ht	tpd	t:s0	apache	3537	0.0	0.3	232524	3160	?	S	19:
25	0:00	/usr/sbin/ht	tpd -DFOREGROUND								
system_u:system_r:ht	tpd	t:s0	apache	3538	0.0	0.3	232524	3160	?	S	19:
25	0:00	/usr/sbin/ht	tpd -DFOREGROUND								
system_u:system_r:ht	tpd	t:s0	apache	3539	0.0	0.3	232524	3160	?	S	19:
25	0:00	/usr/sbin/ht	tpd -DFOREGROUND								
system_u:system_r:ht	tpd	t:s0	apache	3540	0.0	0.3	232524	3160	?	S	19:
25	0:00	/usr/sbin/ht	tpd -DFOREGROUND								
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023	sofa	3596	0.0	0.0	112808	968	pts				
/0 R+ 19:27	0:00	grep --color=auto	ht	tpd							

# Состояние переключателей SELinux

```
[sofa@sofa ~]$ 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
httpd_mod_auth_pam off
```

# Команда seinfo

```
[sofa@sofa ~]$ 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

# Тип файлов и поддиректорий

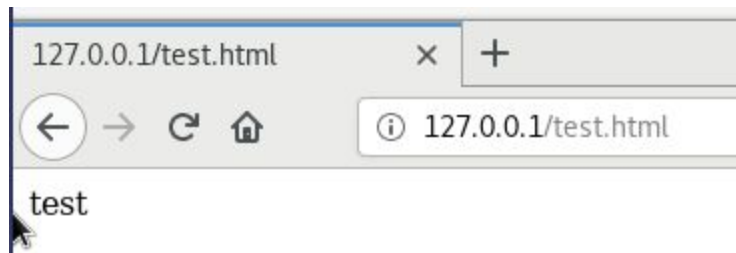
```
[sofa@sofa ~]$ ls -lZ /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[sofa@sofa ~]$ ls -lZ /var/www/html
```

# Создание html-файла /var/www/html/test.html

```
[root@sofa sofa]# touch /var/www/html/test.html  
[root@sofa sofa]# echo "test" >> /var/www/html/test.html  
[root@sofa sofa]# cat /var/www/html/test.html  
test
```



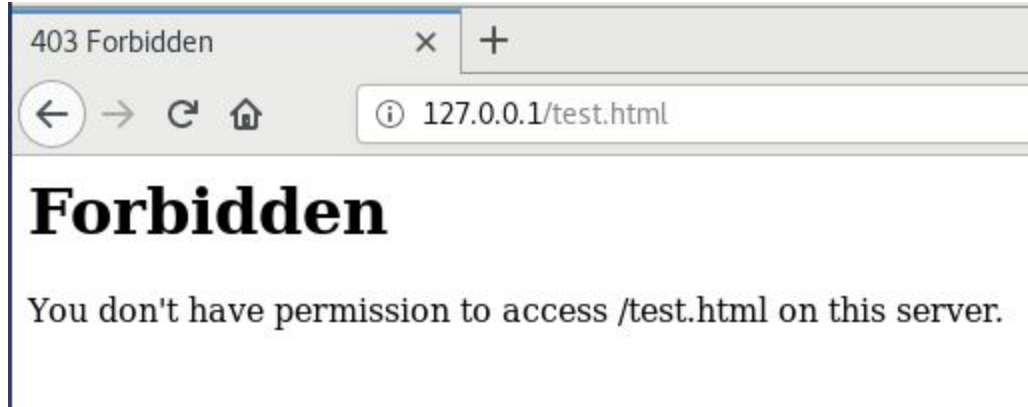
# Обращение к файлу test.html



# Контекст файла test.html

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

# Повторное обращение к файлу test.html



# log-файлы веб-сервера Apache и системный log-файл

```
[root@sofa sofa]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 5 Oct 15 19:37 /var/www/html/test.html
[root@sofa sofa]# tail /var/log/messages
Oct 15 19:44:35 sofa setroubleshoot: SELinux is preventing httpd from getattr access on
the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 24034c
99-eaee-4a6e-8d92-5c7fdc5d262f
Oct 15 19:44:35 sofa python: SELinux is preventing httpd from getattr access on the fil
e /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.h
tml default label should be httpd_sys_content_t.#012Then you can run restorecon. The ac
cess attempt may have been stopped due to insufficient permissions to access a parent d
irectory 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 confi
dence) 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 shou
ld be allowed getattr access on the test.html file by default.#012Then you should repor
t 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
```

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

```
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 81
```

# Просмотр log-файлов

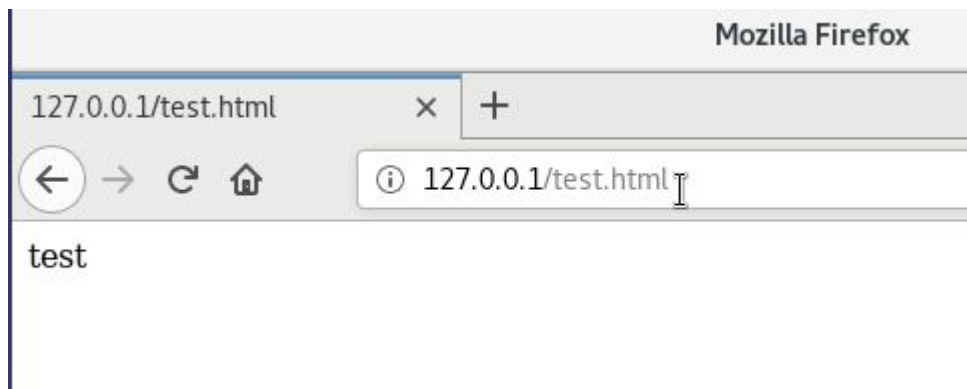
```
[root@sofa sofa]# systemctl start httpd
[root@sofa sofa]# tail -nl /var/log/messages
tail: l: invalid number of lines
[root@sofa sofa]# tail /var/log/messages
Oct 15 20:00:29 sofa setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Oct 15 20:00:29 sofa setroubleshoot: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 24034c99-eaee-4a6e-8d92-5c7fdc5d262f
Oct 15 20:00:29 sofa 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
```

# Вывод списка портов

```
[root@sofa sofa]# 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@sofa sofa]#
```

# Возвращение контекста

```
[root@sofa sofa]# systemctl start httpd
[root@sofa sofa]# chcon -t httpd_sys_content_t /var/www/html/test.html
chcon: failed to change context of '/var/www/html/test.html' to 'unconfined_u:object_r:
httpd_sys_content_t:s0': Invalid argument
[root@sofa sofa]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@sofa sofa]# █
```





# Удаление html файла

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

# Вывод

В результате проделанной лабораторной работы были развиты навыки администрирования ОС Linux, получено первое практическое знакомство с технологией SELinux, а также была проверена работа SELinux на практике совместно с веб-сервером Apache.