

Презентация лабораторной работы №6

Мандатное разграничение прав в Linux

Тасыбаева Н.С.

14 октября 2023

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux¹. Проверить работу SELinux на практике совместно с веб-сервером Apache.

```
Installed:
  apr-1.7.0-11.el9.x86_64
  apr-util-1.6.1-20.el9_2.1.x86_64
  apr-util-bdb-1.6.1-20.el9_2.1.x86_64
  apr-util-openssl-1.6.1-20.el9_2.1.x86_64
  httpd-2.4.53-11.el9_2.5.x86_64
  httpd-core-2.4.53-11.el9_2.5.x86_64
  httpd-filesystem-2.4.53-11.el9_2.5.noarch
  httpd-tools-2.4.53-11.el9_2.5.x86_64
  mod_http2-1.15.19-4.el9_2.4.x86_64
  mod_lua-2.4.53-11.el9_2.5.x86_64
  rocky-logos-httpd-90.14-1.el9.noarch

Complete!
[nstasihbaeva@nstasihbaeva ~]$ cat etc/httpd/httpd.conf
```

Рис. 1: Запуск сервера

```
# ServerName gives the name and port that the server uses to identify itself.  
# This can often be determined automatically, but we recommend you specify  
# it explicitly to prevent problems during startup.  
#  
# If your host doesn't have a registered DNS name, enter its IP address here.  
#  
ServerName test.ru
```

Рис. 2: Параметр ServerName

```
[nstashbaeva@nstashbaeva ~]$ 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: inactive (dead)
   Docs: man:httpd.service(8)
[nstashbaeva@nstashbaeva ~]$ getenforce
Enforcing
[nstashbaeva@nstashbaeva ~]$ 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
[nstashbaeva@nstashbaeva ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[nstashbaeva@nstashbaeva ~]$ 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 Sat 2023-10-14 15:37:49 MSK; 13s ago
   Docs: man:httpd.service(8)
  Main PID: 42349 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec: 0 B/sec"
    Tasks: 213 (limit: 12224)
   Memory: 23.3M
     CPU: 447ms
    CGroup: /system.slice/httpd.service
            └─42349 /usr/sbin/httpd -DFOREGROUND
              └─42357 /usr/sbin/httpd -DFOREGROUND
                └─42361 /usr/sbin/httpd -DFOREGROUND
                  └─42362 /usr/sbin/httpd -DFOREGROUND
                    └─42365 /usr/sbin/httpd -DFOREGROUND

Oct 14 15:37:48 nstashbaeva.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 14 15:37:49 nstashbaeva.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 14 15:37:49 nstashbaeva.localdomain httpd[42349]: Server configured, listening on: port 80
```

```
Oct 14 15:37:49 nstasihbaeva.localdomain httpd[42349]: Server configured, listening on: port 80
[nstasihbaeva@nstasihbaeva ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 42349 0.1 0.5 20116 11328 ? Ss 15:37 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42357 0.0 0.3 21600 7244 ? S 15:37 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42361 0.0 0.6 1210508 12880 ? Sl 15:37 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42362 0.5 0.5 1079372 10832 ? Sl 15:37 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42365 0.0 0.5 1079372 10832 ? Sl 15:37 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 nstasih+ 42622 0.0 0.1 221664 2184 pts/0 S+ 15:38 0:00 grep --color=auto httpd
[nstasihbaeva@nstasihbaeva ~]$ sestatus -bigrep httpd
sestatus: invalid option -- 'i'

Usage: sestatus [OPTION]

  -v Verbose check of process and file contexts.
  -b Display current state of booleans.

Without options, show SELinux status.
[nstasihbaeva@nstasihbaeva ~]$ 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_sss 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
```

```
* Installing packages...
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:                  5100     Attributes:              258
Users:                  8         Roles:                  14
Booleans:               353      Cond. Expr.:            384
Allow:                  65000     Neverallow:              0
Auditallow:             170      Dontaudit:              8572
Type_trans:             265341    Type_change:             87
Type_member:            35        Range_trans:            6164
Role allow:             38        Role_trans:              420
Constraints:            70        Validatetrans:           0
MLS Constrains:         72        MLS Val. Tran:           0
Permissives:            2         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:                 660
Netifcon:               0         Nodecon:                 0
```

```
[nstasihbaeva@nstasihbaeva ~]$
```



```
[nstashbaeva@nstashbaeva ~]$ 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 23:21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 May 16 23:21 html
[nstashbaeva@nstashbaeva ~]$ ls -lZ /var/www/html
total 0
[nstashbaeva@nstashbaeva ~]$ cd /var/www
[nstashbaeva@nstashbaeva www]$ cd html
[nstashbaeva@nstashbaeva html]$ ls -lZ
total 0
[nstashbaeva@nstashbaeva html]$ ls -l
total 0
[nstashbaeva@nstashbaeva html]$ cd ../
[nstashbaeva@nstashbaeva www]$ ls -l
total 0
drwxr-xr-x. 2 root root 6 May 16 23:21 cgi-bin
drwxr-xr-x. 2 root root 6 May 16 23:21 html
[nstashbaeva@nstashbaeva www]$ sudo -i
[sudo] password for nstashbaeva:
[root@nstashbaeva ~]# cd /var/www/html
[root@nstashbaeva html]# touch test.html
[root@nstashbaeva html]# vi test.html
[root@nstashbaeva html]# cat test.html
<html>
<body>test</body>
</html>

[root@nstashbaeva html]# ls -l
total 4
-rw-r--r--. 1 root root 34 Oct 14 15:49 test.html
[root@nstashbaeva html]# ls -lZ
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 Oct 14 15:49 test.html
[root@nstashbaeva html]#
```

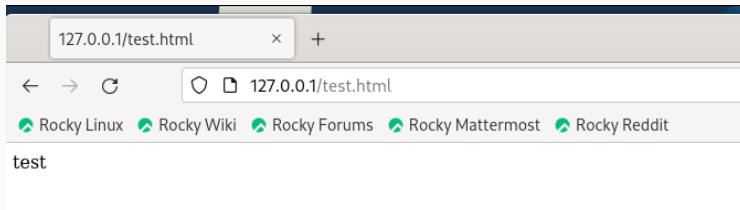


Рис. 7: Запуск в браузере

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

Рис. 8: Изменение контекста безопасности

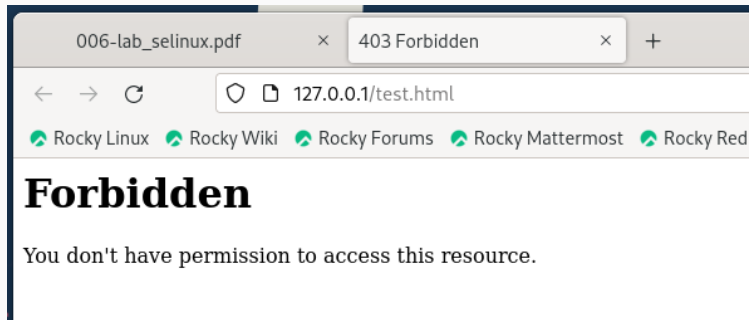


Рис. 9: Запуск в браузере с ошибкой

```

[root@nstasishbaeva ~]# ls -l /var/www/html/test.html
-rw-r--r-- 1 root root 34 Oct 14 15:49 /var/www/html/test.html
[root@nstasishbaeva ~]# tail /var/log/messages
Oct 14 16:18:28 nstasishbaeva gnome-shell[2656]: libinput error: client bug: timer event3 debounce: scheduled expiry is in the past (-507ms), your system is too slow
Oct 14 16:18:31 nstasishbaeva gnome-shell[2656]: libinput error: client bug: timer event3 debounce: scheduled expiry is in the past (-2490ms), your system is too slow
Oct 14 16:18:32 nstasishbaeva gnome-shell[2656]: libinput error: client bug: timer event3 debounce: scheduled expiry is in the past (-4271ms), your system is too slow
Oct 14 16:18:32 nstasishbaeva gnome-shell[2656]: libinput error: client bug: timer event3 debounce: scheduled expiry is in the past (-4272ms), your system is too slow
Oct 14 16:18:32 nstasishbaeva gnome-shell[2656]: libinput error: client bug: timer event3 debounce: scheduled expiry is in the past (-3217ms), your system is too slow
Oct 14 16:18:32 nstasishbaeva gnome-shell[2656]: libinput error: client bug: timer event3 debounce: scheduled expiry is in the past (-3284ms), your system is too slow
Oct 14 16:18:32 nstasishbaeva gnome-shell[2656]: libinput error: client bug: timer event3 debounce: scheduled expiry is in the past (-2905ms), your system is too slow
Oct 14 16:18:32 nstasishbaeva gnome-shell[2656]: libinput error: client bug: timer event3 debounce: scheduled expiry is in the past (-2806ms), your system is too slow
Oct 14 16:18:32 nstasishbaeva gnome-shell[2656]: libinput error: client bug: timer event3 debounce short: scheduled expiry is in the past (-2813ms), your system is too slow
Oct 14 16:18:32 nstasishbaeva gnome-shell[2656]: libinput error: client bug: timer event3 debounce: scheduled expiry is in the past (-2366ms), your system is too slow
[root@nstasishbaeva ~]# cd /etc/httpd/conf/
[root@nstasishbaeva conf]# vi httpd.conf
[root@nstasishbaeva conf]# cat httpd.conf
#
# This is the main Apache HTTP server configuration file. It contains the
# configuration directives that give the server its instructions.
# See <URL:http://httpd.apache.org/docs/2.4/> for detailed information.
# In particular, see
# http://httpd.apache.org/docs/2.4/configuring.html

```

Рис. 10: Лог файлы

```
[root@ntasishbaeva ~]# cd httpd
[root@ntasishbaeva httpd]# ls
access_log  error_log
[root@ntasishbaeva httpd]# cat error_log
[Sat Oct 14 15:17:48.948619 2023] [core:notice] [pid 42349:tid 42349] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Sat Oct 14 15:17:48.951897 2023] [suexec:notice] [pid 42349:tid 42349] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Sat Oct 14 15:17:49.034060 2023] [lbmethod_heartbeat:notice] [pid 42349:tid 42349] AH02282: No slotses from mod_heartbeat
[Sat Oct 14 15:17:49.088706 2023] [mpm_event:notice] [pid 42349:tid 42349] AH00489: Apache/2.4.53 (Rocky Linux) configured -- resuming normal operations
[Sat Oct 14 15:17:49.088804 2023] [core:notice] [pid 42349:tid 42349] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[Sat Oct 14 16:17:43.680467 2023] [core:error] [pid 42365:tid 42356] (13)Permission denied: [client 127.0.0.1:57702] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because
# on a component of the path
[Sat Oct 14 16:19:44.125544 2023] [mpm_event:notice] [pid 42349:tid 42349] AH00492: caught SIGWINCH, shutting down gracefully
[Sat Oct 14 16:19:45.323614 2023] [core:notice] [pid 43872:tid 43872] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Sat Oct 14 16:19:45.325249 2023] [suexec:notice] [pid 43872:tid 43872] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Sat Oct 14 16:19:45.343083 2023] [lbmethod_heartbeat:notice] [pid 43872:tid 43872] AH02282: No slotses from mod_heartbeat
[Sat Oct 14 16:19:45.357795 2023] [mpm_event:notice] [pid 43872:tid 43872] AH00489: Apache/2.4.53 (Rocky Linux) configured -- resuming normal operations
[Sat Oct 14 16:19:45.357835 2023] [core:notice] [pid 43872:tid 43872] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[root@ntasishbaeva httpd]# cat access_log
127.0.0.1 - - [14/Oct/2023:16:10:06 +0300] "GET /test.html HTTP/1.1" 200 34 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
127.0.0.1 - - [14/Oct/2023:16:10:37 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/test.html" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
127.0.0.1 - - [14/Oct/2023:16:17:43 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
[root@ntasishbaeva httpd]# semanage port -a -t http_port_t -p tcp 81
usage: semanage -f -s
      [-import,export,login,user,port,fbkey,fbendport,interface,module,node,fcontext,boolean,permissive,dontaudit]
      ...
semanage: error: unrecognized arguments: -p 81
[root@ntasishbaeva httpd]# semanage port -l | grep http_port_t
http_port_t
tcp      80, 81, 441, 488, 8088, 8089, 8443, 9080
pagasus_http_port_t
tcp      5988
[root@ntasishbaeva httpd]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@ntasishbaeva httpd]# 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 Sat 2023-10-14 16:16:17 MSK; 11s ago
     Docs: man:httpd.service(8)
   Main PID: 42416 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec:  0 B/sec"
```

Рис. 11: Настройки

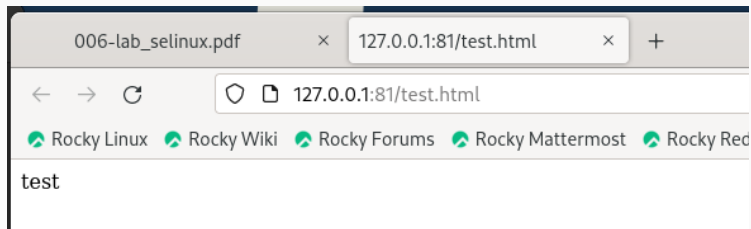


Рис. 12: Запуск в браузере

```
Oct 14 16:36:17 nstasihbaeva.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 14 16:36:17 nstasihbaeva.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 14 16:36:17 nstasihbaeva.localdomain httpd[44186]: Server configured, listening on: port 81
[root@nstasihbaeva httpd]# cd
[root@nstasihbaeva ~]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@nstasihbaeva ~]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@nstasihbaeva ~]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 34 Oct 14 15:49 /var/www/html/test.html
[root@nstasihbaeva ~]# cd /etc/httpd/conf/
[root@nstasihbaeva conf]# vi httpd.conf
[root@nstasihbaeva conf]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@nstasihbaeva conf]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@nstasihbaeva conf]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@nstasihbaeva conf]# 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@nstasihbaeva conf]# cd
[root@nstasihbaeva ~]# cd /var/www/html
[root@nstasihbaeva html]# rm test.html
rm: remove regular file 'test.html'? y
[root@nstasihbaeva html]# ls
[root@nstasihbaeva html]#
```

Рис. 13: Открытие файла

Выводы по проделанной работе

Я изучила механизмы изменения идентификаторов, применения SetUID- и Sticky-битов, получила практические навыки работы в консоли с дополнительными атрибутами. Рассмотрела работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.