

# Лабораторная работа 6

---

Генералов Даниил, 1032212280

2024 г.

Российский университет дружбы народов, Москва, Россия

## Задание

---

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

## Выполнение

---

```

[dmgeneralov@dmgeneralov ~]$ getenforce
Enforcing
[dmgeneralov@dmgeneralov ~]$ 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
[dmgeneralov@dmgeneralov ~]$ systemctl status httpd
○ httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: 0)
   Active: inactive (dead)
     Docs: man:httpd.service(8)

[dmgeneralov@dmgeneralov ~]$ sudo systemctl enable --now httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[dmgeneralov@dmgeneralov ~]$ ps aux | grep httpd
system_u:system_r:httpd_t:s0 root      3444  0.8  0.8  20204 11364 ?        Ss   20:39   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3445  0.0  0.5  21936  7104 ?        S    20:39   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3446  0.0  2.1 1571248 15048 ?        Sl   20:39   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3447  0.0  0.8 1440112 10748 ?        Sl   20:39   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3448  0.0  0.8 1440112 10876 ?        Sl   20:39   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-c0:c1023 dmgener+ 3629 0.0  0.1 221688 2304 pts/0  S+   20:39   0:00 grep --color=auto httpd
[dmgeneralov@dmgeneralov ~]$
[dmgeneralov@dmgeneralov ~]$ sestatus -b | grep httpd
sestatus: Invalid option -- '-'

Usage: sestatus [OPTION]

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

Without options, show SELinux status.
[dmgeneralov@dmgeneralov ~]$ sestatus --bigrep httpd
sestatus: Invalid option -- '-'

Usage: sestatus [OPTION]

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

Without options, show SELinux status.
[dmgeneralov@dmgeneralov ~]$ sestatus -b | grep httpd
httpd_allow_write          off
httpd_builtin_scripting    on
httpd_can_check_spam       off
httpd_can_connect_ftp      off

```

Рис. 1: SELinux

```

[dmgeneralov@dmgeneralov ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:      33 (MLS enabled)
Target Policy:      selinux
Handle unknown classes: allow
Classes:            135
Sensitivities:      1
Types:              5145
Users:              8
Booleans:           356
Allow:              65504
Auditallow:         176
Type_trans:         271778
Type_member:        37
Role_allow:         40
Constraints:        70
MLS_Constrain:      72
Permissives:        4
Defaults:           7
Allowperms:         0
Auditallowperms:    0
Ibendporkcon:       0
Initial SIDs:       27
Genfscon:           109
Netifcon:           0
Permissions:        1824
Attributes:         259
Roles:              15
Cond. Expr.:        388
Neverallow:         0
Dontaudit:          8682
Type_change:        94
Range_trans:        5931
Role_trans:         417
Validatetrans:      0
MLS_Val. Trans:     0
Polcap:             6
Typebounds:         0
Neverallowperms:    0
Dontauditperms:     0
Ibkeycon:           0
Fs_use:             35
Portcon:            665
Nodecon:            0

[dmgeneralov@dmgeneralov ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 аэр  8 19:30 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0  6 аэр  8 19:30 html

[dmgeneralov@dmgeneralov ~]$ ls -lZ /var/www/html
total 0

[dmgeneralov@dmgeneralov ~]$ ls -alZ /var/www/html
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 аэр  8 19:30 .
drwxr-xr-x. 4 root root system_u:object_r:httpd_sys_content_t:s0 33 окт 12 20:37 ..
[dmgeneralov@dmgeneralov ~]$ cat | sudo tee /var/www/html/test.html
<html>
<html>
<body>test</body>
<body>test</body>
</html>
</html>

[dmgeneralov@dmgeneralov ~]$ ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 окт 12 20:44 test.html

[dmgeneralov@dmgeneralov ~]$

```

Рис. 2: SELinux

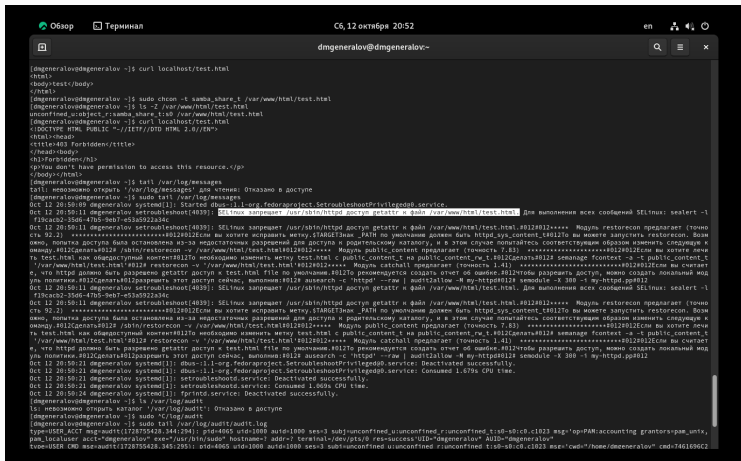
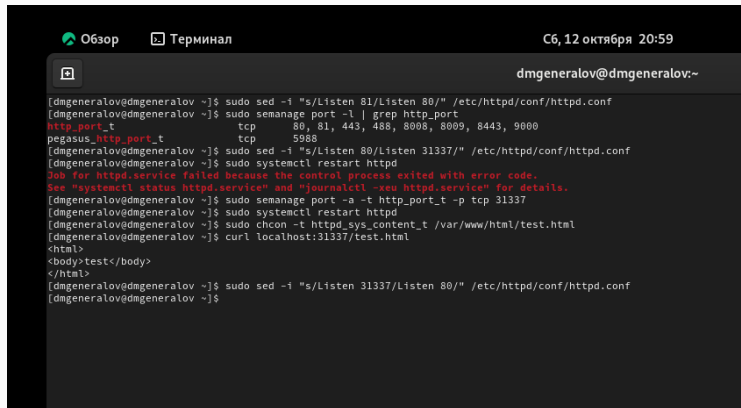


Рис. 3: SELinux



The screenshot shows a terminal window with a dark background. At the top, there are two tabs: 'Обзор' (Overview) and 'Терминал' (Terminal). The date and time 'Сб, 12 октября 20:59' are displayed in the top right corner. The terminal prompt is 'dmgeneralov@dmgeneralov:~'. The user enters several commands to modify SELinux configuration for httpd. The first command is 'sudo sed -i "s/Listen 81/Listen 80/" /etc/httpd/conf/httpd.conf'. The second command is 'sudo semanage port -l | grep http\_port', which outputs a table of ports for http\_port\_t and pegasus\_http\_port\_t. The third command is 'sudo sed -i "s/Listen 80/Listen 31337/" /etc/httpd/conf/httpd.conf'. The fourth command is 'sudo systemctl restart httpd', which fails with an error message. The fifth command is 'sudo semanage port -a -t http\_port\_t -p tcp 31337'. The sixth command is 'sudo systemctl restart httpd'. The seventh command is 'sudo chcon -t httpd\_sys\_content\_t /var/www/html/test.html'. The eighth command is 'curl localhost:31337/test.html', which outputs an HTML document. The final command is 'sudo sed -i "s/Listen 31337/Listen 80/" /etc/httpd/conf/httpd.conf'.

```
dmgeneralov@dmgeneralov:~$ sudo sed -i "s/Listen 81/Listen 80/" /etc/httpd/conf/httpd.conf
dmgeneralov@dmgeneralov:~$ sudo semanage port -l | grep http_port
http_port_t            tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t    tcp      5988
dmgeneralov@dmgeneralov:~$ sudo sed -i "s/Listen 80/Listen 31337/" /etc/httpd/conf/httpd.conf
dmgeneralov@dmgeneralov:~$ sudo systemctl restart httpd
Job for httpd.service failed because the control process exited with error code.
See "systemctl status httpd.service" and "journalctl -xeu httpd.service" for details.
dmgeneralov@dmgeneralov:~$ sudo semanage port -a -t http_port_t -p tcp 31337
dmgeneralov@dmgeneralov:~$ sudo systemctl restart httpd
dmgeneralov@dmgeneralov:~$ sudo chcon -t httpd_sys_content_t /var/www/html/test.html
dmgeneralov@dmgeneralov:~$ curl localhost:31337/test.html
<html>
<body>test</body>
</html>
dmgeneralov@dmgeneralov:~$ sudo sed -i "s/Listen 31337/Listen 80/" /etc/httpd/conf/httpd.conf
dmgeneralov@dmgeneralov:~$
```

Рис. 4: SELinux



## Выводы

---

В этой лабораторной работе мы рассмотрели, как использовать SELinux для ограничения возможностей процессов, на примере Apache.