

Защита лабораторной работы №6. Мандатное разграничение прав в Linux

Асеинова Елизавета

2022 Oct 4th

RUDN University, Moscow, Russian Federation

Результат выполнения лабораторной работы №6

Цель выполнения лабораторной работы

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

```
[root@evaseinova evaseinova]# getenforce
Enforcing
[root@evaseinova evaseinova]# 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
```

Figure 1: Вход в систему

Результат выполнения лабораторной работы

```
[root@evaseinova evaseinova]# 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: enabled)
   Active: active (running) since Wed 2022-10-05 18:44:09 MSK; 1min 45s ago
     Docs: man:httpd.service(8)
  Main PID: 2565 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0;Requests served 0"
    Tasks: 213 (limit: 12202)
   Memory: 25.1M
      CPU: 221ms
   CGroup: /system.slice/httpd.service
           └─2565 /usr/sbin/httpd -DFOREGROUND
             └─2573 /usr/sbin/httpd -DFOREGROUND
               └─2578 /usr/sbin/httpd -DFOREGROUND
                 └─2579 /usr/sbin/httpd -DFOREGROUND
                   └─2581 /usr/sbin/httpd -DFOREGROUND
```

Figure 2: Обращение к серверу

Результат выполнения лабораторной работы

```
[root@evaseinova evaseinova]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:          133      Permissions:          454
Sensitivities:    1       Categories:          1024
Types:            4995    Attributes:           254
Users:            8       Roles:               14
Booleans:         347    Cond. Expr.:         382
Allow:            63727   Neverallow:           0
Auditallow:       163    Dontaudit:            8391
Type_trans:       251060  Type_change:           87
Type_member:      35     Range_trans:          5958
Role allow:       38     Role_trans:           418
Constraints:      72     Validatetrans:        0
MLS Constrain:    72     MLS Val. Tran:        0
Permissives:      0      Polcap:               5
Defaults:         7      Typebounds:           0
Allowxperm:       0      Neverallowxperm:      0
Auditallowxperm:  0      Dontauditxperm:       0
Ibendportcon:     0      Ibpkeycon:            0
Initial SIDs:     27     Fs_use:               33
Genfscon:         106    Portcon:              651
```

Figure 3: Статистика

```
[root@evaseinova evaseinova]# cat /var/www/html/test.html  
<html>  
<body>test</body>  
</html>
```

Figure 4: Html файл

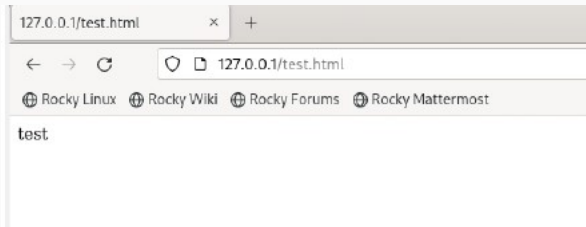


Figure 5: Отображение в браузере


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

Figure 6: Изменение контекста

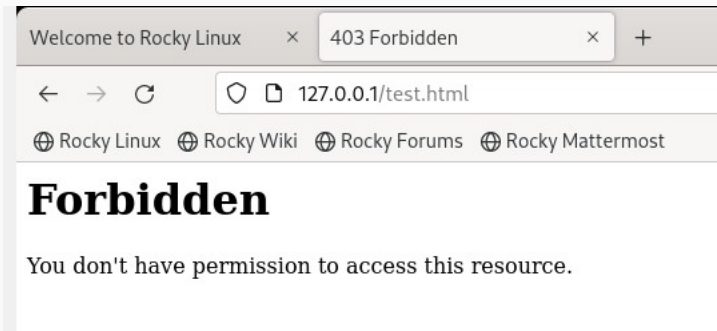


Figure 7: Отказ в доступе

```
42 # httpd.service is enabled to run at boot time, the a
    may not be
43 # available when the service starts.  See the
    httpd.service(8) man
44 # page for more information.
45 #
46 #Listen 12.34.56.78:80
47 Listen 81
48
49 #
```

Figure 8: Изменение порта

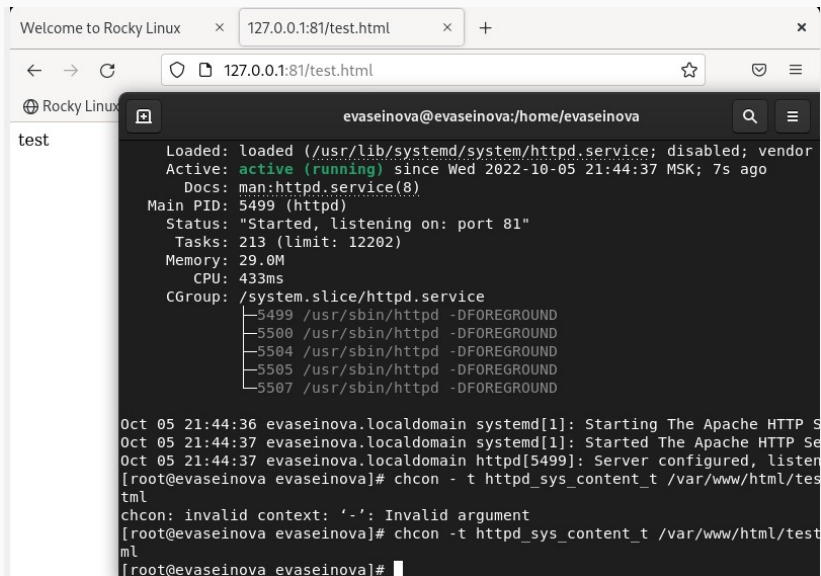
Результат выполнения лабораторной работы

```
[root@evaseinova evaseinova]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined

[root@evaseinova evaseinova]#
[root@evaseinova evaseinova]# 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@evaseinova evaseinova]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@evaseinova evaseinova]# 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 pr>
   Active: active (running) since Wed 2022-10-05 21:44:37 MSK; 7s ago
     Docs: man:httd.service(8)
```

Figure 9: Подключение порта

Результат выполнения лабораторной работы



The screenshot shows a terminal window with the prompt `evaseinova@evaseinova:/home/evaseinova`. The terminal output displays the status of the `httpd.service` and the execution of the `chcon` command.

```
Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor
Active: active (running) since Wed 2022-10-05 21:44:37 MSK; 7s ago
   Docs: man:httpd.service(8)
Main PID: 5499 (httpd)
Status: "Started, listening on: port 81"
Tasks: 213 (limit: 12202)
Memory: 29.0M
CPU: 433ms
CGroup: /system.slice/httpd.service
├─5499 /usr/sbin/httpd -DFOREGROUND
├─5500 /usr/sbin/httpd -DFOREGROUND
├─5504 /usr/sbin/httpd -DFOREGROUND
├─5505 /usr/sbin/httpd -DFOREGROUND
└─5507 /usr/sbin/httpd -DFOREGROUND

Oct 05 21:44:36 evaseinova.localdomain systemd[1]: Starting The Apache HTTP S
Oct 05 21:44:37 evaseinova.localdomain systemd[1]: Started The Apache HTTP Se
Oct 05 21:44:37 evaseinova.localdomain httpd[5499]: Server configured, listen
[root@evaseinova evaseinova]# chcon - t httpd_sys_content_t /var/www/html/tes
tml
chcon: invalid context: '-': Invalid argument
[root@evaseinova evaseinova]# chcon -t httpd_sys_content_t /var/www/html/test
ml
[root@evaseinova evaseinova]#
```

В ходе работы мы развили навыки администрирования ОС Linux, получили первое практическое знакомство с технологией SELinux¹, проверили работу SELinux на практике совместно с веб-сервером Apache.