

Защита лабораторной работы №6.

Мандатноограничение прав в Linux

Бармина Ольга Константиновна

2022 Sep 22th

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@localhost okbarmina]# getenforce
Enforcing
[root@localhost okbarmina]# 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
[root@localhost okbarmina]#
```

Figure 1: рис 1. вход в систему

Результат выполнения лабораторной работы

```
[root@localhost okbarmina]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor pre>
   Active: active (running) since Tue 2022-09-27 11:17:26 MSK; 4s ago
     Docs: man:httpd.service(8)
  Main PID: 3576 (httpd)
    Status: "Started, listening on: port 80"
     Tasks: 213 (limit: 12215)
    Memory: 26.9M
       CPU: 86ms
    CGroup: /system.slice/httpd.service
            └─3576 /usr/sbin/httpd -DFOREGROUND
              └─3577 /usr/sbin/httpd -DFOREGROUND
                └─3581 /usr/sbin/httpd -DFOREGROUND
                  └─3582 /usr/sbin/httpd -DFOREGROUND
                    └─3583 /usr/sbin/httpd -DFOREGROUND
```

Figure 2: рис 2. обращение к серверу

Результат выполнения лабораторной работы

```
[root@localhost okbarmina]# 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:            5002     Attributes:           254
Users:            8        Roles:                14
Booleans:         347     Cond. Expr.:         381
Allow:            63996    Neverallow:          0
Auditallow:       168     Dontaudit:            8417
Type_trans:       258486  Type_change:          87
Type_member:      35      Range_trans:          5960
Role_allow:       38      Role_trans:           420
Constraints:      72      Validatetrans:        0
MLS Constrains:  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
Netifcon:         0       Nodecon:              0
```



```
1 <html>
2 <body>
3     test
4 </body>
5 </html>
6
```

Figure 4: рис 4. html файл

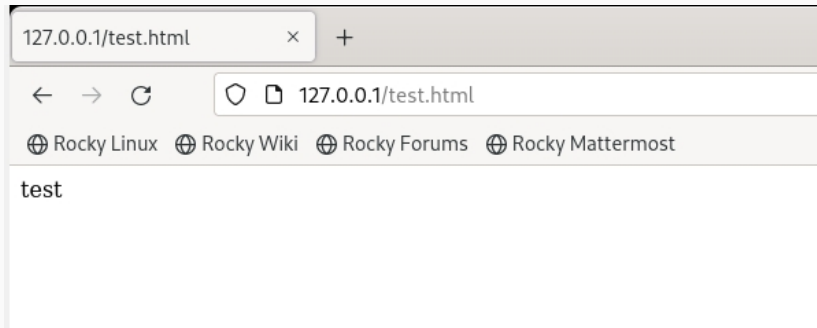


Figure 5: рис 5. отображение в браузере


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

Figure 6: рис 6. изменение контекста

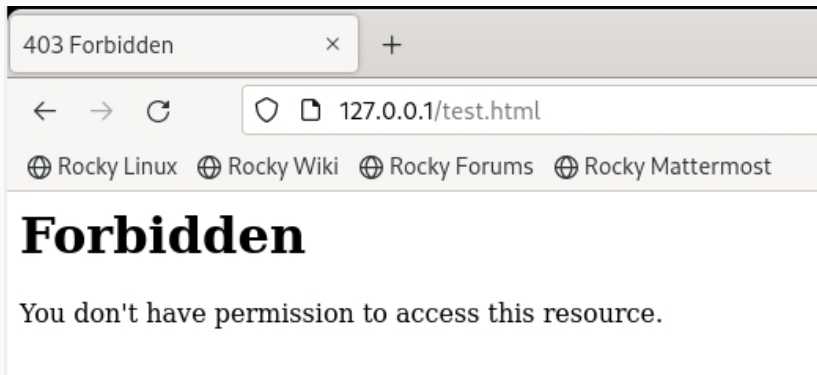
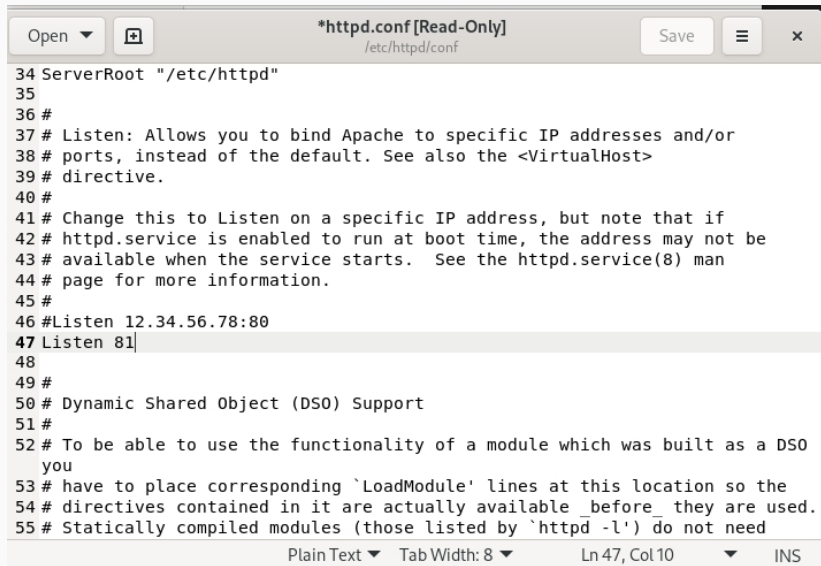


Figure 7: рис 7. отказ в доступе

Результат выполнения лабораторной работы



The image shows a text editor window titled `*httpd.conf [Read-Only]` with the file path `/etc/httpd/conf`. The editor contains the following configuration lines:

```
34 ServerRoot "/etc/httpd"
35
36 #
37 # Listen: Allows you to bind Apache to specific IP addresses and/or
38 # ports, instead of the default. See also the <VirtualHost>
39 # directive.
40 #
41 # Change this to Listen on a specific IP address, but note that if
42 # httpd.service is enabled to run at boot time, the address 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 #
50 # Dynamic Shared Object (DSO) Support
51 #
52 # To be able to use the functionality of a module which was built as a DSO
53 # you
54 # have to place corresponding 'LoadModule' lines at this location so the
55 # directives contained in it are actually available _before_ they are used.
56 # Statically compiled modules (those listed by 'httpd -l') do not need
```

The status bar at the bottom indicates: Plain Text ▼ Tab Width: 8 ▼ Ln 47, Col 10 ▼ INS

Figure 8: рис 8. изменение порта

```
[root@localhost okbarmina]# semanage port -a -t http_port_t -p tcp 81
bash: semanage: command not found.
[root@localhost okbarmina]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@localhost okbarmina]# 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
```

Figure 9: рис 9. подключение порта

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

Figure 10: рис 10. возвращение параметров

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.