

Лабораторная работа № 6

Сулицкий Богдан Романович

2023, Москва

Целью данной лабораторной работы является развитие навыков администрирования ОС Linux и получение первого практического знакомства с технологией SELinux

```

root@localhost user# getenforce
Enforcing
[root@localhost user#] 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
[root@localhost user#] 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
[root@localhost user#] systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/systemd-httpd.service; vendor preset: disabled)
   Active: active (running) since Sun 2023-10-14 10:43:12 MSK; 14min ago

```

Рис. 1: Getenforce, sestatus и service status

[illegible]

Рис. 2: Apache в списке процессов и состояния переключателей

```
[root@localhost user]# 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
```

Рис. 3: Статистика по политике

```
[root@localhost user]# 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
[root@localhost user]# ls -lZ /var/www/html
[root@localhost user]# █
```

Рис. 4: Проверка данных /var/www/ и /var/www/html

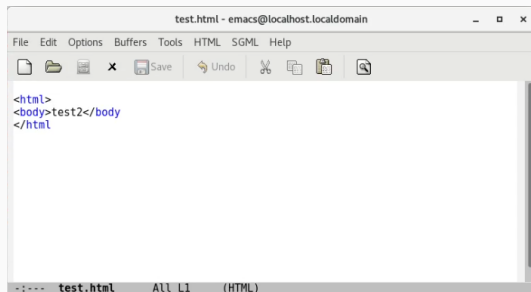


Рис. 5: Содержимое файла test.html

```
[root@localhost user]# ls -lZ /var/www/html/test.html  
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
```

Рис. 6: Проверка контекста файла



Рис. 7: Отображение файла в браузере 1

```
No manual entry for httpd_selinux
[root@localhost user]# chcon -t samba_share_t /var/www/html/test.html
chcon: failed to change context of '/var/www/html/test.html' to 'unconfined_u:object_r:samba_share_t:s0': Invalid argument
[root@localhost user]# chcon -t samba_share_t /var/www/html/test.html
[root@localhost user]# ls -lZ /var/www/html/test.html
-rw-r--r-- . root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

Рис. 8: Изменение контекста файла test.html 1

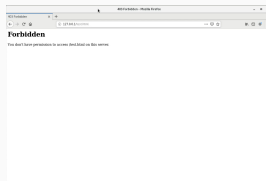


Рис. 9: Отображение файла в браузере 2

Ход работы

[illegible]

Рис. 10: Просмотр информации о файле test.html и вывод log-файлов

```
#Listen 12.34.56.78:80
Listen 81
```

Рис. 11: Изменения порта 1


```
[root@localhost user]# systemctl restart httpd
[root@localhost user]# tail -n1 /var/log/messages
Oct 14 19:22:14 localhost systemd: Started The Apache HTTP Server.
```

Рис. 12: Перезапуск веб-сервера 1

```
[root@localhost user]# tail /var/log/httpd/access_log
127.0.0.1 - [14/Oct/2023:19:34:43 +0000] "GET /test.html HTTP/1.1" 403 211 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:88.0) Gecko/20200818 Firefox/98.0"
127.0.0.1 - [14/Oct/2023:19:34:43 +0000] "GET /favicon.ico HTTP/1.1" 404 289 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:88.0) Gecko/20200818 Firefox/98.0"
127.0.0.1 - [14/Oct/2023:19:36:03 +0000] "GET /test.html HTTP/1.1" 200 31 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:88.0) Gecko/20200818 Firefox/98.0"
127.0.0.1 - [14/Oct/2023:19:36:25 +0000] "GET /test3.html HTTP/1.1" 200 32 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:88.0) Gecko/20200818 Firefox/98.0"
127.0.0.1 - [14/Oct/2023:19:43:18 +0000] "GET /favicon.ico HTTP/1.1" 404 289 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:88.0) Gecko/20200818 Firefox/98.0"
127.0.0.1 - [14/Oct/2023:19:43:18 +0000] "GET /test.html HTTP/1.1" 403 211 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:88.0) Gecko/20200818 Firefox/98.0"
127.0.0.1 - [14/Oct/2023:19:46:18 +0000] "GET /test.html HTTP/1.1" 200 31 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:88.0) Gecko/20200818 Firefox/98.0"
127.0.0.1 - [14/Oct/2023:19:49:18 +0000] "GET /test.html HTTP/1.1" 200 31 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:88.0) Gecko/20200818 Firefox/98.0"
127.0.0.1 - [14/Oct/2023:19:53:34 +0000] "GET /test.html HTTP/1.1" 403 211 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:88.0) Gecko/20200818 Firefox/98.0"
[root@localhost user]# tail /var/log/httpd/error_log
[Sat Oct 14 19:49:26.964083 2023] [mpm_prefork:critical] [pid 13051] AH00183: Apache/2.4.8 (CentOS) configured -- resuming normal operations
[Sat Oct 14 19:49:26.964083 2023] [core:notice] [pid 13051] AH00956: Command Line: '/usr/sbin/httpd -D FOREGROUND'
[Sat Oct 14 19:53:34.405238 2023] [core:error] [pid 13058] (2)Operation not permitted: [client 127.0.0.1:40108] AH00855: access to /test.html denied (file system path '/var/www/html/test.html') because search permission was missing on a component of the path
[Sat Oct 14 19:58:12.387504 2023] [mpm_prefork:critical] [pid 13051] AH00180: caught SIGABRT, shutting down gracefully
[Sat Oct 14 19:58:12.457149 2023] [core:notice] [pid 13250] SLLinux policy enabled, httpd running as context system_u:system_r:httpd_t:s0
[Sat Oct 14 19:58:12.458639 2023] [warn:notice] [pid 13250] AH01212: httpd: Module not found: /usr/lib64/modules/
AH00550: httpd: Could not reliably determine the server's fully qualified domain name, using localhost.localdomain. Set the 'ServerName' directive globally to suppress this message
[Sat Oct 14 19:58:12.460149 2023] [warn:notice] [pid 13250] AH01212: httpd: Module not found: /usr/lib64/modules/
[Sat Oct 14 19:58:12.889139 2023] [mpm_prefork:critical] [pid 13251] AH00183: Apache/2.4.8 (CentOS) configured -- resuming normal operations
[Sat Oct 14 19:58:12.889149 2023] [core:notice] [pid 13250] AH00956: Command Line: '/usr/sbin/httpd -D FOREGROUND'
```

Рис. 13: Access_log и error_log

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

Рис. 14: Привязка порта и проверка списка портов

```
[root@localhost user]# systemctl restart httpd
[root@localhost user]# tail -n1 /var/log/messages
Oct 14 19:22:14 localhost systemd: Started The Apache HTTP Server.
```

Рис. 15: Перезапуск веб-сервера 2

```
[root@localhost user]# chcon -t httpd_sys_content_t /var/www/html/test.html  
[root@localhost user]# ls -lZ /var/www/html/test.html  
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
```

Рис. 16: Изменение контекста файла test.html 2



Рис. 17: Отображение файла в браузере 3

```
#Listen 12.34.56.78:80
Listen 80
```

Рис. 18: Изменения порта 2

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

Рис. 19: Удаление привязки порта и удаление файла test.html

В ходе проделанной лабораторной работы я развил свои навыки администрирования ОС Linux и получил первое практическое знакомство с технологией SELinux