

Лабораторная работа №6

Основы информационной безопасности

Серёгина Ирина Андреевна

27 апреля 2024

Российский университет дружбы народов, Москва, Россия

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

1. Подготовить рабочую среду.
2. Выполнить лабораторную работу.
3. Записать вывод.

Выполнение лабораторной работы

Для начала я обновила ПО, установила Apache с помощью команд `yum update -y` и `yum install httpd -y`. Затем вошла в систему и проверила, что SELinux работает в режиме enforcing (рис. 1).

```
[root@localhost ~]# getenforce
Enforcing
[root@localhost ~]# 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 ~]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@localhost ~]# 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: enabled)
   Active: active (running) since Fri 2024-04-26 17:31:26 MSK; 21s ago
     Docs: man:httpd.service(8)
   Main PID: 106736 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Byte
   Tasks: 213 (limit: 12112)
```

2.

Запустила и проверила работу веб-сервера (рис. 2).

```
[root@localhost ~]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@localhost ~]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; vendor preset: enabled)
   Active: active (running) since Fri 2024-04-26 17:31:26 MSK; 1min 11s ago
     Docs: man:httpd.service(8)
  Main PID: 106736 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests served 0/0"
    Tasks: 213 (limit: 12112)
   Memory: 43.6M
      CPU: 50ms
   CGroup: /system.slice/httpd.service
           └─106736 /usr/sbin/httpd -DFOREGROUND
              └─106737 /usr/sbin/httpd -DFOREGROUND
                 └─106738 /usr/sbin/httpd -DFOREGROUND
                    └─106739 /usr/sbin/httpd -DFOREGROUND
                       └─106740 /usr/sbin/httpd -DFOREGROUND
```

Узнала контекст безопасности (рис. 3).

```
[root@localhost ~]# ps -auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 106736 0.0 0.5 20128 11300 ?
Ss 17:31 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 106737 0.0 0.3 21612 7232 ?
S 17:31 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 106738 0.0 1.0 2521240 21144 ?
Sl 17:31 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 106739 0.0 0.8 2324568 17048 ?
Sl 17:31 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 106740 0.0 0.8 2324568 17052 ?
Sl 17:31 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 107002 0.0 0.1 2216
```

Рис. 3: проверка контекста безопасности

Уточнила текущее состояние переключателей SELinux для Apache (рис. 4).

```
[root@localhost ~]# sestatus -b | grep httpd
httpd_anon_write off
httpd_built_in_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
```

Рис. 4: состояние переключателей

С помощью seinfo узнала статистику по политике (рис. 5).

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

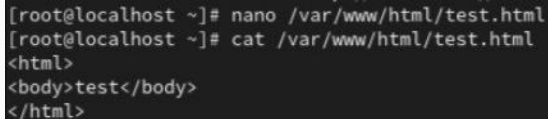
Classes:      135      Permissions:      457
Sensitivities: 1      Categories:      1024
Types:        5135     Attributes:       259
Users:        8        Roles:           15
Booleans:     357      Cond. Expr.:     390
Allow:        65409     Neverallow:      0
Auditallow:   172      Dontaudit:       8647
Type_trans:   267813   Type_change:     94
Type_member:  37        Range_trans:     6164
Role allow:   39        Role_trans:      419
Constraints:  70        Validatetrans:   0
MLS Constrai: 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
```

Определила тип файлов и поддиректорий директории /var/www. При определении типа файлов директории /var/www/html ничего не отображается (рис. 6).

```
[root@localhost ~]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 окт 28 12
:35 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 окт 28 12
:35 html
[root@localhost ~]# ls -lZ /var/www/html
итого 0
```

Рис. 6: www

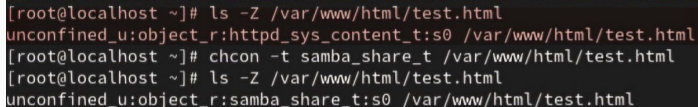
Создаю файл test.html, заполняю его (рис. 7).

A terminal window with a black background and white text. The first line shows the command 'nano /var/www/html/test.html' being executed. The second line shows the command 'cat /var/www/html/test.html' being executed, followed by the output of the file's contents: '<html>', '<body>test</body>', and '</html>'.

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

Рис. 7: test.html

Проверяю контекст файла (рис. 8).



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

Рис. 8: контекст

9.

Обращаюсь к файлу через веб-сервер, его содержимое успешно отображается (рис. 9).

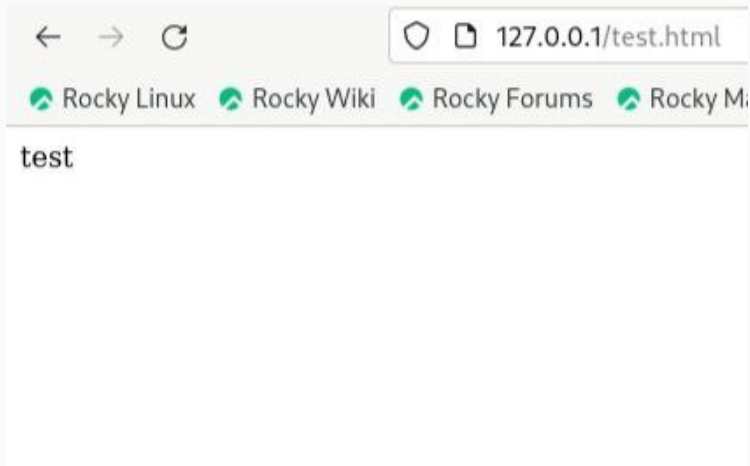
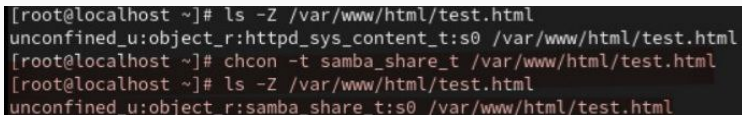


Рис. 9: веб-страница файла

Изменяю контекст файла (рис. 10).

A terminal window with a dark background and light-colored text. It shows a sequence of four commands and their outputs. The first command is 'ls -Z /var/www/html/test.html' which outputs 'unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html'. The second command is 'chcon -t samba_share_t /var/www/html/test.html'. The third command is 'ls -Z /var/www/html/test.html' which outputs 'unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html'. The fourth command is identical to the third and produces the same output.

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

Рис. 10: изменение контекста

После изменения контекста доступ к файлу через веб-сервер был невозможен (рис. 11).

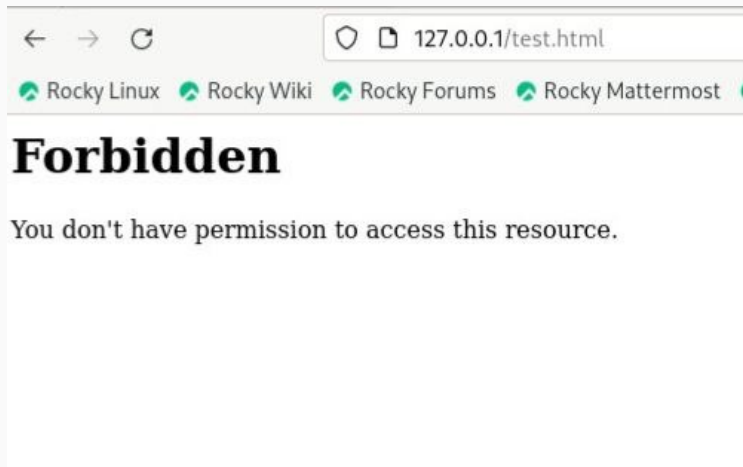


Рис. 11: ошибка доступа

В файле меняю строку Listen 80 на Listen 81, чтобы запустить веб-сервер на прослушивание TCP-порта 81 (рис. 12).

```
# Change this to Listen on a specific IP address, but note that
# httpd.service is enabled to run at boot time, the address may
# available when the service starts.  See the httpd.service(8) m
# page for more information.
#
#Listen 12.34.56.78:80
Listen 81
```

Рис. 12: изменения в файле

Настраиваю порт (рис. 13).

```
[root@localhost ~]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@localhost ~]# semanage port -l | grep http_port_t
http_port_t                tcp      80, 81, 443, 488, 8008, 8080, 5000
```

Рис. 13: настройка порта 81

Однако даже после этого веб-сервер не отображает файл (рис. 14).

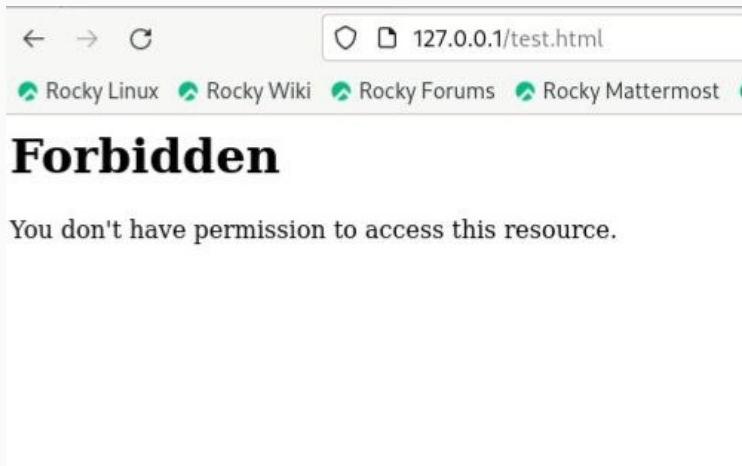


Рис. 14: ошибка

Убираю изменения из конфигурационного файла, пытаюсь привязку к 81 порту, но появляется ошибка. Удаляю ранее созданный файл (рис. 16).

A terminal window with a black background and white text. The prompt is [root@localhost ~]#. The first command is semanage port -d -t http_port_t -p tcp 81, which results in a ValueError: Port tcp/81 is defined in policy, cannot be deleted. The second command is rm /var/www/html/test.html, which results in a message: rm: удалить обычный файл '/var/www/html/test.html'? followed by a cursor.

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

Рис. 16: удаление файла

Я развила навыки администрирования ОС Linux, получила первое практическое знакомство с технологией SELinux. Проверила работу SELinux на практике совместно с веб-сервером Apache.

Спасибо за внимание!