

# Лабораторная работа №6

Основы информационной безопасности

Серёгина Ирина Андреевна

# Содержание

|   |                                |    |
|---|--------------------------------|----|
| 1 | Цель работы                    | 3  |
| 2 | Задание                        | 4  |
| 3 | Теоретическое введение         | 5  |
| 4 | Выполнение лабораторной работы | 7  |
| 5 | Выводы                         | 14 |
|   | Список литературы              | 15 |

# 1 Цель работы

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

## 2 Задание

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

### 3 Теоретическое введение

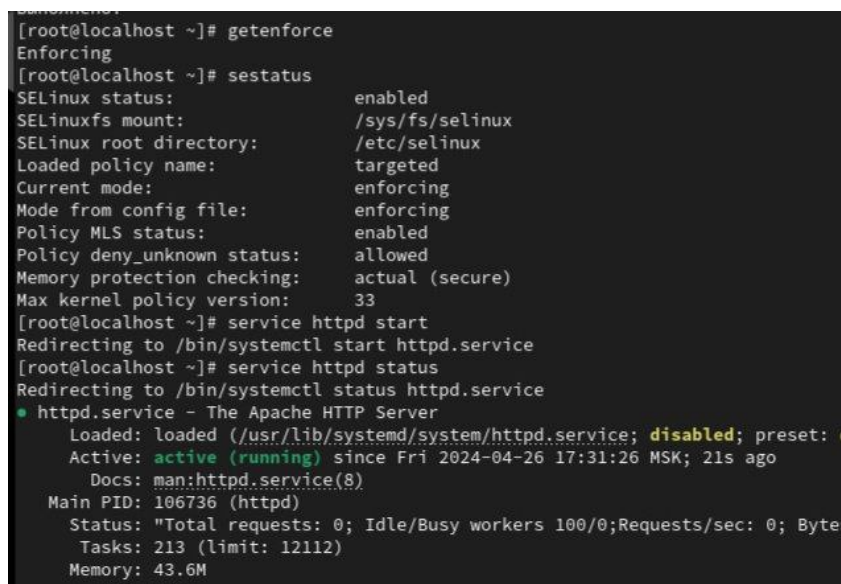
1. При подготовке стенда обратите внимание, что необходимая для работы и указанная выше политика `targeted` и режим `enforcing` используются в данном дистрибутиве по умолчанию, т.е. каких-то специальных настроек не требуется. При этом следует убедиться, что политика и режим включены, особенно когда работа будет проводиться повторно и велика вероятность изменений при предыдущем использовании системы.
2. При необходимости администратор должен разбираться в работе SELinux и уметь как исправить конфигурационный файл `/etc/selinux/config`, так и проверить используемый режим и политику.
3. Необходимо, чтобы был установлен веб-сервер Apache. При установке системы в конфигурации «рабочая станция» указанный пакет не ставится.
4. В конфигурационном файле `/etc/httpd/httpd.conf` необходимо задать параметр `ServerName: ServerName test.ru` чтобы при запуске веб-сервера не выдавались лишние сообщения об ошибках, не относящихся к лабораторной работе.
5. Также необходимо проследить, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола `tcp`. Отключить фильтр можно командами `iptables -F` `iptables -P INPUT ACCEPT` `iptables -P OUTPUT ACCEPT` либо добавить разрешающие правила: `iptables -I INPUT -p tcp -dport 80 -j ACCEPT` `iptables -I INPUT -p tcp`

```
-dport 81 -j ACCEPT iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT iptables -I  
OUTPUT -p tcp --sport 81 -j ACCEPT
```

6. Обратите внимание, что данные правила не являются «точными» и рекомендуемыми на все случаи жизни, они лишь позволяют правильно организовать работу стенда.
7. В работе специально не делается акцент, каким браузером (или какой консольной программой) будет производиться подключение к вебсерверу. По желанию могут использоваться разные программы, такие как консольные `links`, `lynx`, `wget` и графические `konqueror`, `opera`, `firefox` или др.

## 4 Выполнение лабораторной работы

1. 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. [4.1]).



```
[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; Bytes served: 0"
   Tasks: 213 (limit: 12112)
   Memory: 43.6M
```

Рис. 4.1: подготовка к работе

2. Запустила и проверила работу веб-сервера (рис. [4.2]).

```
[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 CEST; 1min 1s 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
```

Рис. 4.2: запуск работы Apache

3. Узнала контекст безопасности (рис. [4.3]).

```
[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. 4.3: проверка контекста безопасности

4. Уточнила текущее состояние переключателей SELinux для Apache (рис. [4.4]).



```
[root@localhost ~]# sestatus -b | grep httpd
httpd_anon_write           off
httpd_builtin_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. 4.4: состояние переключателей

5. С помощью seinfo узнала статистику по политике (рис. [4.5]).

```
[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 Constrain:          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
```

Рис. 4.5: статистика по политике

6. Определила тип файлов и поддиректорий директории /var/www. При определении типа файлов директории /var/www/html ничего не отображается (рис. [4.6]).

```
[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. 4.6: www

7. Создаю файл test.html, заполняю его (рис. [4.7]).

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

Рис. 4.7: test.html

8. Проверяю контекст файла (рис. [4.8]).

```
[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. 4.8: контекст

9. Обращаюсь к файлу через веб-сервер, его содержимое успешно отображается (рис. [4.9]).

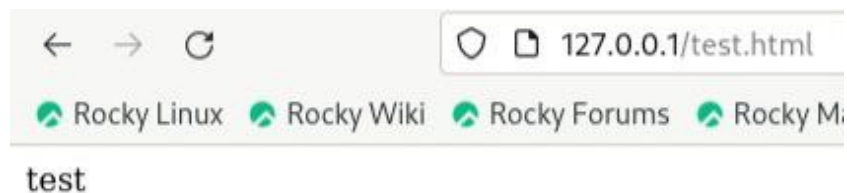


Рис. 4.9: веб-страница файла

10. Изменяю контекст файла (рис. [4.10]).

```
[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. 4.10: изменение контекста

11. После изменения контекста доступ к файлу через веб-сервер был невозможен (рис. [4.11]).

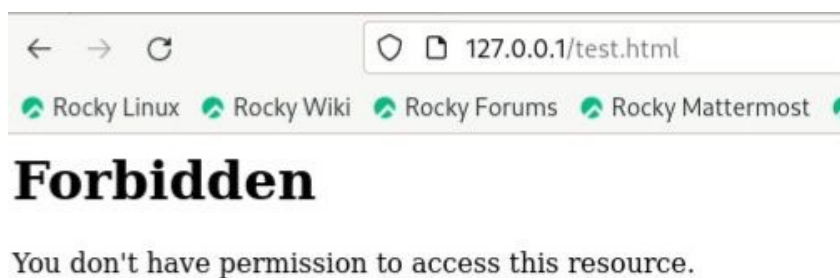


Рис. 4.11: ошибка доступа

12. В файле меняю строку Listen 80 на Listen 81, чтобы запустить веб-сервер на прослушивание TCP-порта 81 (рис. [4.12]).

```
# 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. 4.12: изменения в файле

13. Настраиваю порт (рис. [4.13]).



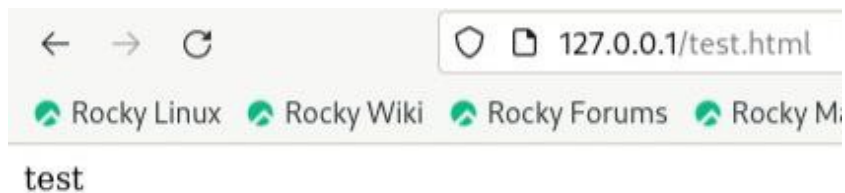


Рис. 4.15: веб-страница

16. Убираю изменения из конфигурационного файла, пытаюсь привязку к 81 порту, но появляется ошибка. Удаляю ранее созданный файл (рис. [4.16]).

```
[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. 4.16: удаление файла

## 5 Выводы

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

## Список литературы