

Отчет по лабораторной работе №6

Мандатное разграничение прав в Linux

Галацан Николай, НПИбд-01-22

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы [1]	5
3	Выводы	11
	Список литературы	12

Список иллюстраций

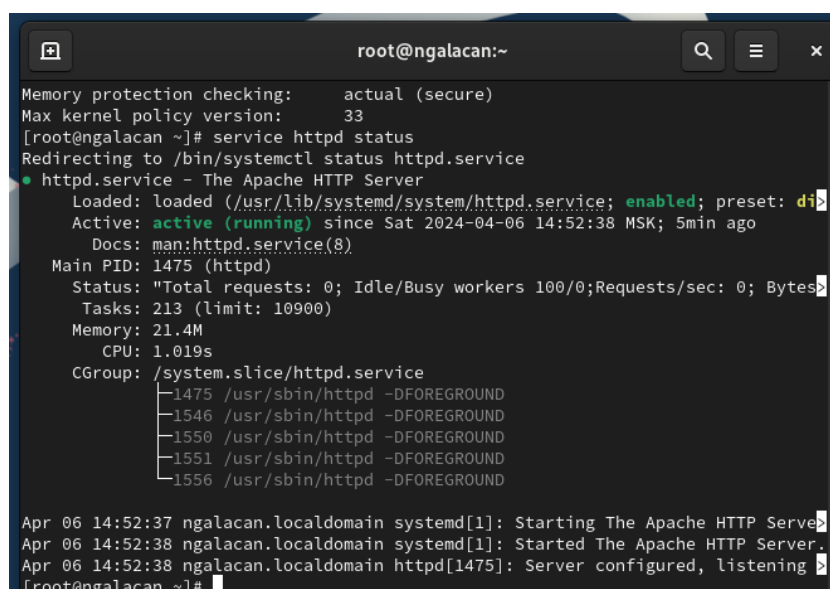
2.1	Режим работы SELinux, статус httpd	5
2.2	Контекст безопасности веб-сервера Apache, состояние переключателей SELinux	6
2.3	Статистика по политике	6
2.4	Просмотр файлов, создание test.html и просмотр контекста	7
2.5	Запуск файла в браузере	7
2.6	Изменение контекста файла и попытка просмотра	8
2.7	Просмотр лог-файла	8
2.8	Изменение порта в конфигурационном файле	9
2.9	Сбой веб-сервера	9
2.10	Просмотр лог-файла	9
2.11	Добавление порта 81 и проверка. Перезапуск веб-сервера. Возвращение контекста	10
2.12	Завершение выполнения работы	10

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. [1]

2 Выполнение лабораторной работы [1]

Убеждаюсь, что SELinux работает в режиме enforcing политики targeted. Также убеждаюсь, что веб-сервер запущен и работает (рис. 2.1).



```
root@ngalacan:~  
Memory protection checking:    actual (secure)  
Max kernel policy version:    33  
[root@ngalacan ~]# 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; preset: disabled)  
   Active: active (running) since Sat 2024-04-06 14:52:38 MSK; 5min ago  
     Docs: man:httpd.service(8)  
  Main PID: 1475 (httpd)  
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0; CPU usage 0.0%"  
    Tasks: 213 (limit: 10900)  
   Memory: 21.4M  
      CPU: 1.019s  
    CGroup: /system.slice/httpd.service  
            └─1475 /usr/sbin/httpd -DFOREGROUND  
              └─1546 /usr/sbin/httpd -DFOREGROUND  
                └─1550 /usr/sbin/httpd -DFOREGROUND  
                  └─1551 /usr/sbin/httpd -DFOREGROUND  
                    └─1556 /usr/sbin/httpd -DFOREGROUND  
  
Apr 06 14:52:37 ngalacan.localdomain systemd[1]: Starting The Apache HTTP Server:  
Apr 06 14:52:38 ngalacan.localdomain systemd[1]: Started The Apache HTTP Server.  
Apr 06 14:52:38 ngalacan.localdomain httpd[1475]: Server configured, listening on: 0.0.0.0:80  
[root@ngalacan ~]#
```

Рис. 2.1: Режим работы SELinux, статус httpd

Определяю контекст безопасности веб-сервера Apache. Просматриваю текущее состояние переключателей SELinux (рис. 2.2).

```
root@ngalacan:~  
[root@ngalacan ~]# ps auxZ | grep httpd  
system_u:system_r:httpd_t:s0 root 1475 0.0 0.2 20340 4568 ?  
Ss 14:52 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 1546 0.0 0.1 21676 3324 ?  
S 14:52 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 1550 0.0 0.1 1538248 3336 ?  
Sl 14:52 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 1551 0.0 0.1 1669384 3128 ?  
Sl 14:52 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 1556 0.0 0.1 1538248 3304 ?  
Sl 14:52 0:00 /usr/sbin/httpd -DFOREGROUND  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 4409 0.0 0.1 221796  
2272 pts/0 S+ 14:59 0:00 grep --color=auto httpd  
[root@ngalacan ~]# sestatus -bigrep httpd  
sestatus: invalid option -- 'i'  
  
Usage: sestatus [OPTION]  
  
-v Verbose check of process and file contexts.  
-b Display current state of booleans.  
  
Without options, show SELinux status.  
[root@ngalacan ~]# sestatus -b httpd  
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
```

Рис. 2.2: Контекст безопасности веб-сервера Apache, состояние переключателей SELinux

Просматриваю статистику по политике с помощью команды seinfo (рис. 2.3).

```
[root@ngalacan ~]# 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 Constrains: 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  
Initial SIDs: 27 Fs_use: 35  
Genfscon: 109 Portcon: 665  
Netifcon: 0 Nodecon: 0  
[root@ngalacan ~]#
```

Рис. 2.3: Статистика по политике

Определяю тип файлов и поддиректорий, находящихся в директории /var/www, /var/www/html, создаю файл test.html следующего содержания:

```
<html>
<body>test</body>
</html>
```

и проверяю контекст созданного файла (рис. 2.4).

```
[root@ngalacan ~]# ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Oct 28 12
:35 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Oct 28 12
:35 html
[root@ngalacan ~]# ls -lZ /var/www/html
total 0
[root@ngalacan ~]# mcedit /var/www/html/test.html
[root@ngalacan ~]# ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 32 Apr 6 1
5:09 test.html
[root@ngalacan ~]#
```

Рис. 2.4: Просмотр файлов, создание test.html и просмотр контекста

Обращаюсь к файлу через веб-сервер и вижу простую веб-страницу (рис. 2.5).

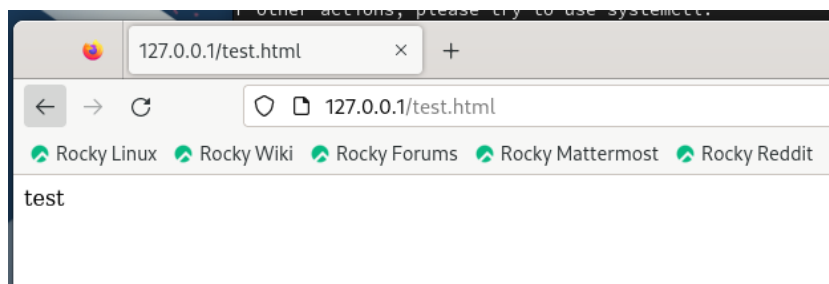


Рис. 2.5: Запуск файла в браузере

Просматриваю справку по `httpd` и `selinux`. Проверяю контекст файла. Тип `httpd_sys_content_t` позволяет процессу `httpd` получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер. Меняю контекст файла и проверяю. Пробую еще раз открыть файл в браузере, но файл не отображается по той причине, что `httpd` не имеет доступа к измененному контексту файла (рис. 2.6).

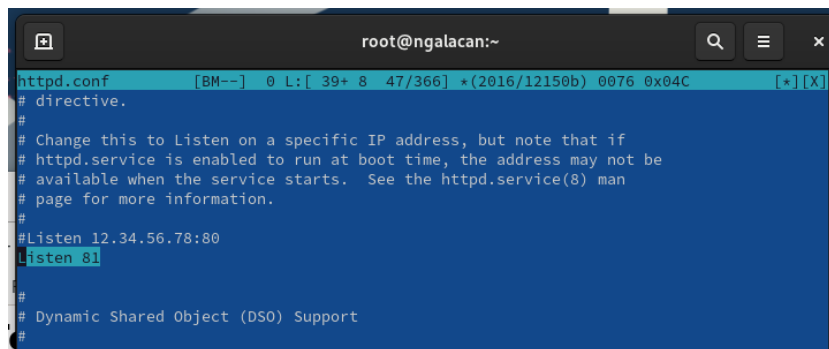


Рис. 2.8: Изменение порта в конфигурационном файле

Перезагружаю веб-сервер и наблюдаю сбой (рис. 2.9).

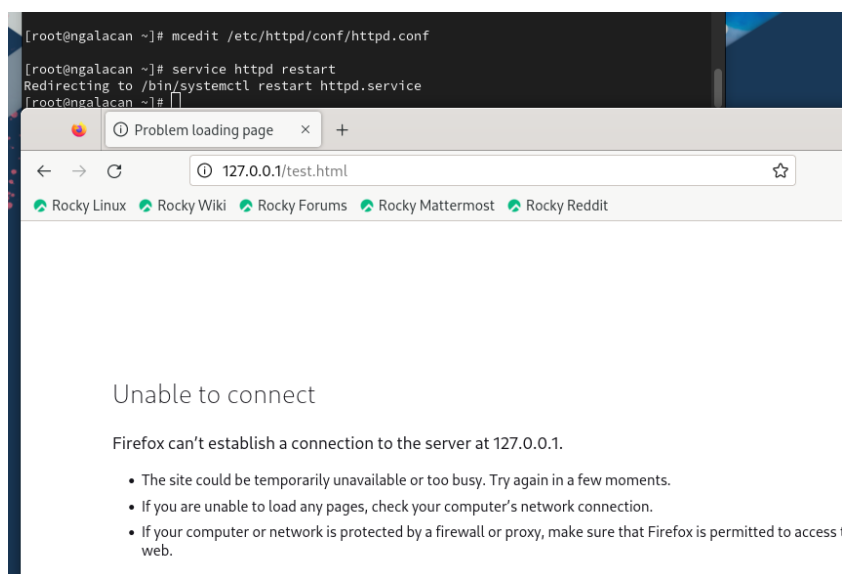


Рис. 2.9: Сбой веб-сервера

Анализирую лог-файлы (рис. 2.10).

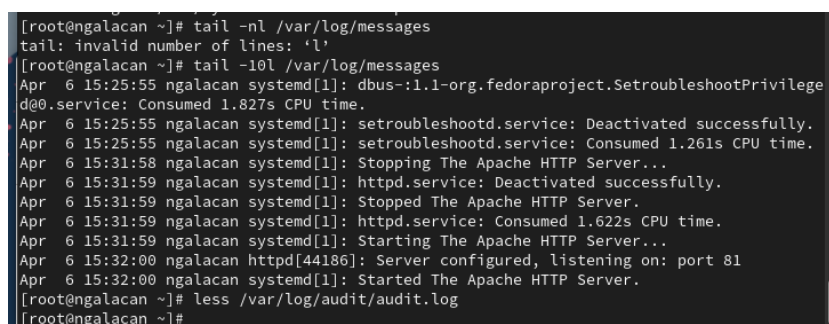
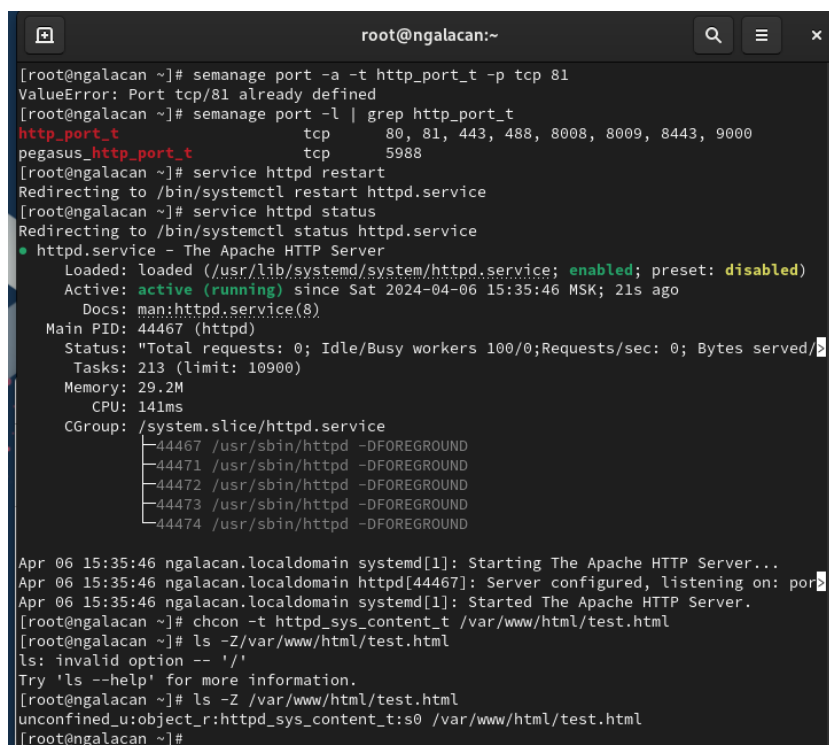


Рис. 2.10: Просмотр лог-файла

Выполняю команду `semanage port -a -t http_port_t -p tcp 81` и проверяю список портов командой `semanage port -l | grep http_port_t` и вижу, что порт 81 появился в списке. Перезагружаю веб-сервер. Возвращаю контекст для `test.html`, к которому `httpd` имеет доступ (рис. 2.11).

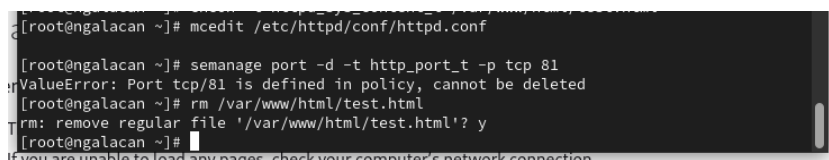


```
root@ngalacan:~  
[root@ngalacan ~]# semanage port -a -t http_port_t -p tcp 81  
ValueError: Port tcp/81 already defined  
[root@ngalacan ~]# semanage port -l | grep http_port_t  
http_port_t      tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000  
pegasus_http_port_t tcp      5988  
[root@ngalacan ~]# service httpd restart  
Redirecting to /bin/systemctl restart httpd.service  
[root@ngalacan ~]# 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; preset: disabled)  
   Active: active (running) since Sat 2024-04-06 15:35:46 MSK; 21s ago  
     Docs: man:httpd.service(8)  
  Main PID: 44467 (httpd)  
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served: 0"  
    Tasks: 213 (limit: 10900)  
   Memory: 29.2M  
      CPU: 141ms  
   CGroup: /system.slice/httpd.service  
           └─44467 /usr/sbin/httpd -DFOREGROUND  
             └─44471 /usr/sbin/httpd -DFOREGROUND  
               └─44472 /usr/sbin/httpd -DFOREGROUND  
                 └─44473 /usr/sbin/httpd -DFOREGROUND  
                   └─44474 /usr/sbin/httpd -DFOREGROUND  
  
Apr 06 15:35:46 ngalacan.localdomain systemd[1]: Starting The Apache HTTP Server...  
Apr 06 15:35:46 ngalacan.localdomain httpd[44467]: Server configured, listening on: port  
Apr 06 15:35:46 ngalacan.localdomain systemd[1]: Started The Apache HTTP Server.  
[root@ngalacan ~]# chcon -t httpd_sys_content_t /var/www/html/test.html  
[root@ngalacan ~]# ls -Z /var/www/html/test.html  
ls: invalid option -- '/'  
Try 'ls --help' for more information.  
[root@ngalacan ~]# ls -Z /var/www/html/test.html  
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html  
[root@ngalacan ~]#
```

Рис. 2.11: Добавление порта 81 и проверка. Перезапуск веб-сервера. Возвращение контекста

После этого тестовая страница вновь открывается в браузере.

Исправляю конфигурационный файл обратно, изменив порт на 80. Удаляю привязку `http_port_t` к 81 порту. Удаляю файл `/var/www/html/test.html` (рис. 2.12).



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

Рис. 2.12: Завершение выполнения работы

3 Выводы

Я развил навыки администрирования ОС Linux, познакомился с технологией SELinux. Проверена работа SELinux на практике совместно с веб-сервером Apache.

Список литературы

1. Кулябов Д.С., Королькова А.В., Геворкян М.Н. Информационная безопасность компьютерных сетей. Лабораторные работы, учебное пособие. Москва: РУДН, 2015. 64 с.