

# **Отчет по лабораторной работе №6**

**Мандатное разграничение прав в Linux**

Дмитрий Сергеевич Шестаков

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>3</b>	<b>Выводы</b>	<b>12</b>
	<b>Список литературы</b>	<b>13</b>

## Список иллюстраций

2.1	Запуск веб-сервера . . . . .	6
2.2	Определение контекста . . . . .	6
2.3	Текущее состояние переключателей . . . . .	7
2.4	Статистика по политике . . . . .	8
2.5	Тип файлов /var/www . . . . .	8
2.6	Тип файлов /var/www/html . . . . .	8
2.7	Обращение к файлу через веб-сервер . . . . .	9
2.8	Изменение контекста файла . . . . .	9
2.9	Системный лог-файл . . . . .	10
2.10	Прослушивание порта 81 . . . . .	10
2.11	Анализ лог-файлов . . . . .	11
2.12	Анализ лог-файлов . . . . .	11
2.13	Команды по привязке TCP-порта . . . . .	11

## **Список таблиц**

# 1 Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux<sup>1</sup>. Проверить работу SELinx на практике совместно с веб-сервером Apache. [1]

## 2 Выполнение лабораторной работы

1. Вошли в систему и убедились, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.
2. С помощью команды `service httpd status` убедились, что веб-сервер работает (рис. 2.1).

```
root@Rocky ~]# service httpd start
Redirecting to /bin/systemctl start httpd.service
root@Rocky ~]# 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: disabled)
   Active: active (running) since Sat 2023-10-14 08:43:01 EDT; 5s ago
     Docs: man:httpd.service(8)
   Main PID: 50469 (httpd)
    Status: "Started, listening on: port 80"
     Tasks: 213 (limit: 4493)
    Memory: 17.7M
       CPU: 68ms
    CGroup: /system.slice/httpd.service
           └─50469 /usr/sbin/httpd -DFOREGROUND
             └─50470 /usr/sbin/httpd -DFOREGROUND
               └─50471 /usr/sbin/httpd -DFOREGROUND
                 └─50472 /usr/sbin/httpd -DFOREGROUND
                   └─50473 /usr/sbin/httpd -DFOREGROUND

окт 14 08:43:01 Rocky systemd[1]: Starting The Apache HTTP Server...
окт 14 08:43:01 Rocky httpd[50469]: Server configured, listening on: port 80
окт 14 08:43:01 Rocky systemd[1]: Started The Apache HTTP Server.
```

Рис. 2.1: Запуск веб-сервера

3. Нашли веб-сервер Apache в списке процессов и определили ее контекст: `unconfined_t` (рис. 2.2).

```
root@Rocky ~]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      50469  0.0  1.4 20172 11426 ?        Ss   08:43   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  50470  0.0  0.9 21508 7320 ?        S    08:43   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  50471  0.0  1.3 1669204 10892 ?      Sl   08:43   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  50472  0.0  1.1 1538068 8836 ?        Sl   08:43   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  50473  0.0  1.1 1538068 8844 ?        Sl   08:43   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 50694  0.0  0.2 221688 2336 pts/1 S+  08:43   0:00 grep --color=auto httpd
root@Rocky ~]#
```

Рис. 2.2: Определение контекста

4. Посмотрели текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -b | grep httpd`(рис. 2.3)

```
httpd_enable_cgi                on
httpd_enable_ftp_server         off
httpd_enable_homedirs           off
httpd_execmem                    off
httpd_graceful_shutdown         off
httpd_manage_ipa                off
httpd_mod_auth_ntlm_winbind     off
httpd_mod_auth_pam              off
httpd_read_user_content         off
httpd_run_ipa                   off
httpd_run_preupgrade            off
httpd_run_stickshift            off
httpd_serve_cobbler_files       off
httpd_setrlimit                 off
httpd_ssi_exec                  off
httpd_sys_script_anon_write     off
httpd_tmp_exec                  off
httpd_tty_comm                  off
httpd_unified                   off
httpd_use_cifs                  off
httpd_use_fusefs                off
httpd_use_gpg                   off
httpd_use_nfs                   off
httpd_use_opencryptoki          off
httpd_use_openstack             off
httpd_use_sasl                  off
httpd_verify_dns                off
```

Рис. 2.3: Текущее состояние переключателей

5. Посмотрели статистику по политике, также определили множество пользователей, ролей, типов.(рис. 2.4)

```

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:             5100    Attributes:           258
Users:             8      Roles:               14
Booleans:          353    Cond. Expr.:         384
Allow:             65009   Neverallow:          0
Auditallow:        170    Dontaudit:           8572
Type_trans:        265337  Type_change:          87
Type_member:        35     Range_trans:         6164
Role allow:         38     Role_trans:          420
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:              660
Netifcon:           0      Nodecon:              0

```

Рис. 2.4: Статистика по политике

6. Определили тип файлов и поддиректорий, находящихся в директории /var/www (рис. 2.5)

```

[root@Rocky ~]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 16 16:21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 мая 16 16:21 html
[root@Rocky ~]# ls -lZ /var/www/html
итого 0

```

Рис. 2.5: Тип файлов /var/www

7. Определили тип файлов в директории /var/www/html. (рис. 2.6)

```

[root@Rocky ~]# ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 окт 14 08:48 test.html

```

Рис. 2.6: Тип файлов /var/www/html

8. Создайте от имени суперпользователя html-файл var/www/html/test.html следующего содержания:



<html>

<body>test</body>

</html>

9. Проверили контекст созданного файла (рис. 2.8)
10. Обратились к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html` (рис. 2.7)

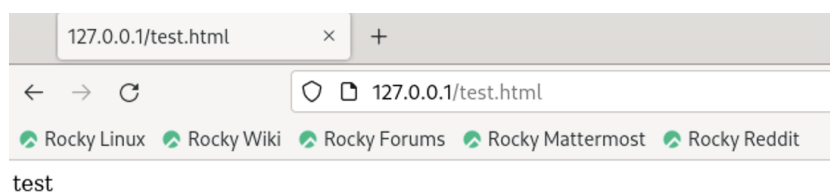


Рис. 2.7: Обращение к файлу через веб-сервер

11. Изучили справку `man httpd_selinux`. Узнали, что существуют следующие контексты файлов: `unconfined_u`, `object_r`, `system_r`, `secadm_r`, `httpd_sys_content_r`.
12. Изменили контекст файла `/var/www/html/test.html` на `samba_share_t`. (рис. 2.8)



Рис. 2.8: Изменение контекста файла

13. Попробовали еще раз получить доступ к файлу через веб-сервер. Не получили сообщение об ошибке.

14. Посмотрели системный лог-файл(рис. 2.9)

[illegible]

Рис. 2.9: Системный лог-файл

15. Запустили веб-сервер Apache на прослушивание TCP-порта 81.(рис. 2.10)

16. Выполнили перезапуск веб-сервера. Сбой не произошёл. (рис. 2.10)

```
[root@Rocky ~]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@Rocky ~]# 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: disabled)
   Active: active (running) since Sat 2023-10-14 09:00:48 EDT; 11s ago
     Docs: man:httpd.service(8)
    Main PID: 52884 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
      Tasks: 213 (limit: 4493)
     Memory: 15.2M
        CPU: 68ms
    CGroup: /system.slice/httpd.service
            └─52884 /usr/sbin/httpd -DFOREGROUND
              └─52885 /usr/sbin/httpd -DFOREGROUND
                └─52886 /usr/sbin/httpd -DFOREGROUND
                  └─52887 /usr/sbin/httpd -DFOREGROUND
                    └─52888 /usr/sbin/httpd -DFOREGROUND

OKT 14 09:00:48 Rocky systemd[1]: Starting The Apache HTTP Server...
OKT 14 09:00:48 Rocky httpd[52884]: Server configured, listening on: port 81
OKT 14 09:00:48 Rocky systemd[1]: Started The Apache HTTP Server.
[root@Rocky ~]#
```

Рис. 2.10: Прослушивание порта 81

17. Проанализировали лог-файлы, и выяснили, что запись появилась только в `/var/log/messages`. (рис. 2.11)

```

ct 14 08:58:30 localhost systemd[1]: Starting The Apache HTTP Server...
ct 14 08:58:30 localhost httpd[52640]: Server configured, listening on: port 80
ct 14 08:58:30 localhost systemd[1]: Started The Apache HTTP Server.
ct 14 09:00:00 localhost NetworkManager[927]: <info> [1697288400.2254] dhcp4 (enp8s5): state changed new lease, address=10.211.55.11
ct 14 09:00:36 localhost systemd[1]: Stopping The Apache HTTP Server...
ct 14 09:00:37 localhost systemd[1]: httpd.service: Deactivated successfully.
ct 14 09:00:37 localhost systemd[1]: Stopped The Apache HTTP Server.
ct 14 09:00:48 localhost systemd[1]: Starting The Apache HTTP Server...
ct 14 09:00:48 localhost httpd[52884]: Server configured, listening on: port 81
ct 14 09:00:48 localhost systemd[1]: Started The Apache HTTP Server.

```

Рис. 2.11: Анализ лог-файлов

```

tail: невозможно открыть '/var/log/http/error_log' для чтения: Нет такого файла или каталога
[root@Rocky ~]# tail /var/log/http/access_log
tail: невозможно открыть '/var/log/http/access_log' для чтения: Нет такого файла или каталога
[root@Rocky ~]# tail /var/log/audit/audit.log
type=SYSCALL msg=audit(1697288234.107:754): arch=c000003e syscall=9 success=yes exit=139823652769792 a0=0 a1=21 a2=1 a3=1 items=0 ppid=5
8469 pid=58473 auid=4294967295 uid=48 gid=48 euid=48 suid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 comm="httpd" exe
="/usr/sbin/httpd" subj=system_u:system_r:httpd_t:s0 key=(null)ARCH=x86_64 SYSCALL=mmap AUID="unset" UID="apache" GID="apache" EUID="ap
ache" SUID="apache" FSUID="apache" EGID="apache" SGID="apache" FSGID="apache"
type=PROCTITLE msg=audit(1697288234.107:754): proctitle=2F573722F7362096E2F6874747064002D44464F524547524F554E44
type=SERVICE_START msg=audit(1697288235.096:755): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=s
etroubleshootd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_START msg=audit(1697288235.683:756): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=s
dbus-1.1-org.fedoraproject.SetroubleshootPrivileged0? comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=su
ccess'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1697288247.758:757): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=s
bus-1.1-org.fedoraproject.SetroubleshootPrivileged0? comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=suc
cess'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1697288247.884:758): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=s
etroubleshootd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1697288304.448:759): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=h
ttpd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_START msg=audit(1697288310.240:760): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=
httpd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1697288437.546:761): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=h
ttpd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_START msg=audit(1697288448.441:762): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=
httpd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"

```

Рис. 2.12: Анализ лог-файлов

18. Выполнили команду `bash semanage port -a -t http_port_t -p tcp 81.`  
(рис. 2.13)

```

[root@Rocky ~]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@Rocky ~]# 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. 2.13: Команды по привязке TCP-порта

19. Перезапустили веб-сервер, также не сбой не произошел. Вернули контекст файлу `/var/www/html/test.html`.
20. Исправили обратно конфигурационный файл `Apache`.

## 3 Выводы

Развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux<sup>1</sup>. Проверили работу SELinx на практике совместно с веб-сервером Apache.

## Список литературы

1. Кулябов Д.С., Королькова А. В., Геворкян М. Н. Лабораторная работа No 6. Мандатное разграничение прав в Linux [Электронный ресурс]. URL: [https://esystem.rudn.ru/pluginfile.php/2090210/mod\\_resource/content/2/006-lab\\_selinux.pdf](https://esystem.rudn.ru/pluginfile.php/2090210/mod_resource/content/2/006-lab_selinux.pdf).