

Лабораторная работа 6

Юдин Герман Станиславович, НФИбд-01-19

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Вывод	13
4	Список литературы	14

List of Figures

2.1	enforcing	6
2.2	service httpd status	6
2.3	httpd context	7
2.4	sestatus	8
2.5	seinfo	9
2.6	/var/www	9
2.7	test.html	10
2.8	httpd context	10
2.9	working web	10
2.10	samba context	10
2.11	forbidden	11
2.12	81 port already added	11
2.13	web 81 port	12

List of Tables

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ
Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №6

дисциплина: Информационная безопасность

Преподаватель: Кулябов Дмитрий Сергеевич

Студент: Юдин Герман Станиславович

Группа: НФИбд-01-19

МОСКВА

2022 г.

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 Выполнение лабораторной работы

1. Убедился, что SELinux работает в режиме enforcing (Рис fig. 2.1).

```
[gsyudin@gsyudin ~]$ getenforce
Enforcing
```

Figure 2.1: enforcing

2. Проверил, что httpd работает (Рис fig. 2.2).

```
[gsyudin@gsyudin ~]$ 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; vendor preset: disabled)
   Active: active (running) since Tue 2022-10-11 09:37:00 MSK; 16min ago
     Docs: man:httpd.service(8)
  Main PID: 3750 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec:  0 B/sec"
    Tasks: 213 (limit: 50447)
   Memory: 23.1M
      CPU: 788ms
   CGroup: /system.slice/httpd.service
           └─3750 /usr/sbin/httpd -DFOREGROUND
             └─3751 /usr/sbin/httpd -DFOREGROUND
               └─3752 /usr/sbin/httpd -DFOREGROUND
                 └─3753 /usr/sbin/httpd -DFOREGROUND
                   └─3757 /usr/sbin/httpd -DFOREGROUND

Oct 11 09:37:00 gsyudin.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 11 09:37:00 gsyudin.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 11 09:37:00 gsyudin.localdomain httpd[3750]: Server configured, listening on: port 80
```

Figure 2.2: service httpd status

3. Нашел контекст безопасность httpd - это system_u:system_r:httpd_t:s0 (Рис fig. 2.3).

```
[gsyudin@gsyudin ~]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0      3750 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      3751 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      3752 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      3753 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      3757 ?        00:00:00 httpd
```

Figure 2.3: httpd context

4. Посмотрел текущее состояние переключателей SELinux для Apache (Рис fig. 2.4).

```
[gsyudin@gsyudin ~]$ 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
httpd_can_network_connect_db off
httpd_can_network_memcache off
httpd_can_network_relay off
httpd_can_sendmail off
httpd_dbus_avahi off
httpd_dbus_sssd off
httpd_dontaudit_search_dirs off
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
[gsyudin@gsyudin ~]$
```

Figure 2.4: sestatus

5. Посмотрел статистику по политике (Рис fig. 2.5). Количество пользователей - 8, ролей - 14, типов - 5002.

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

Classes:                  133      Permissions:              454
Sensitivities:            1        Categories:              1024
Types:                    5002     Attributes:               254
Users:                    8         Roles:                    14
Booleans:                 347      Cond. Expr.:             381
Allow:                    63996    Neverallow:              0
Auditallow:               168      Dontaudit:               8417
Type_trans:               258486   Type_change:              87
Type_member:              35        Range_trans:             5960
Role_allow:               38        Role_trans:              420
Constraints:              72        Validatetrans:           0
MLS Constrain:            72        MLS Val. Tran:           0
Permissives:              0         Polcap:                  5
Defaults:                 7         Typebounds:              0
Allowxperm:               0         Neverallowxperm:         0
Auditallowxperm:          0         Dontauditxperm:          0
Ibendportcon:             0         Ibpkeycon:               0
Initial SIDs:             27        Fs_use:                  33
Genfscon:                 106       Portcon:                 651
Netifcon:                 0         Nodecon:                 0
```

Figure 2.5: seinfo

6. Тип файлов у /var/www - это директории, который на данный момент пустые (Рис fig. 2.6). Файлов никаких нет. Только root может менять данную директорию .

```
[gsyudin@gsyudin ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 15:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 May 16 15:10 html
```

Figure 2.6: /var/www

7. Создал тестовый файл для вывода на сайте (Рис fig. 2.7).



Figure 2.7: test.html

8. Проверил контекст созданного файла, он оказался unconfined_u:object_r:httpd_sys_content (Рис fig. 2.8).

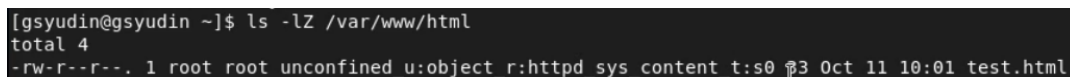


Figure 2.8: httpd context

9. Убедился в корректности работы системы (Рис fig. 2.9).

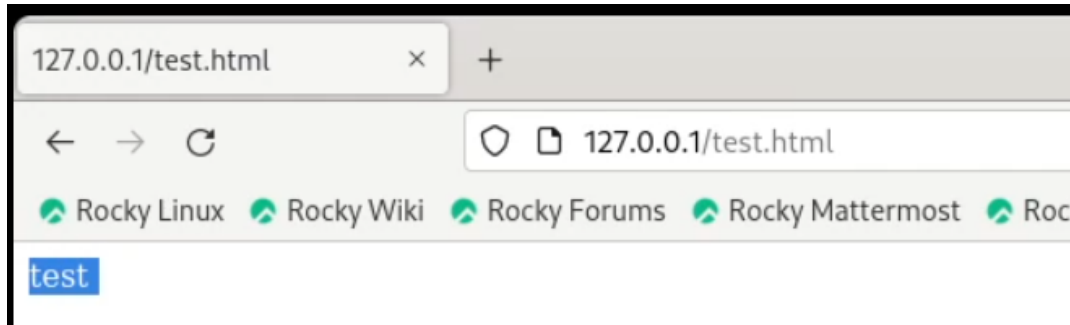


Figure 2.9: working web

10. Сменил контекст безопасности на не связанный с httpd (Рис fig. 2.10).

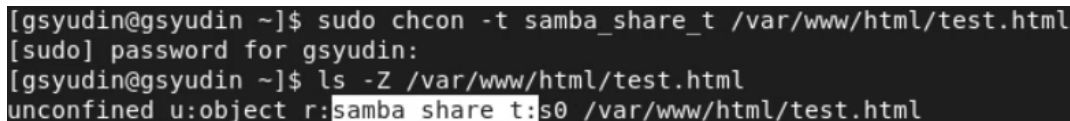


Figure 2.10: samba context

11. После этого возникла ошибка (Рис fig. 2.11).

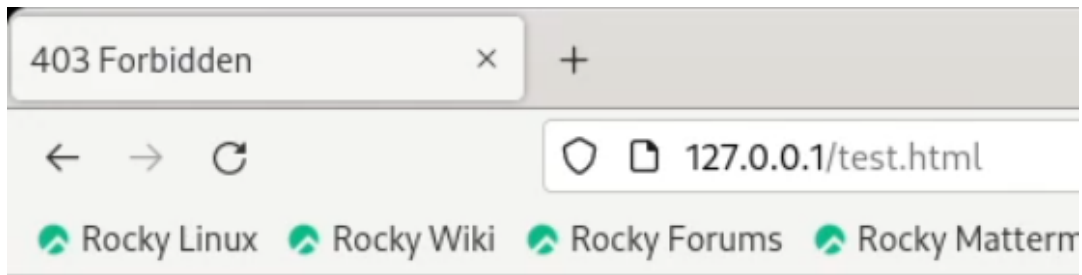


Figure 2.11: forbidden

12. Далее идёт настройка портов, но так как у меня 81 изначально добавлен (Рис fig. 2.12), то я не могу его добавить снова. Поэтому и сайт работает с самого начала (Рис fig. 2.13), когда мы меняет порт на 81. Удалить порт также нельзя.

```
[gsyudin@gsyudin log]$ sudo semanage port -a -p tcp 81 -t http_port_t
ValueError: Port tcp/81 already defined
[gsyudin@gsyudin log]$ sudo semanage port -l | grep 81
http_port_t tcp 1782, 2207, 2208, 8290, 8292, 9100, 9101, 9102, 9220, 9221, 9222, 9280, 9281, 9282, 9290
, 9291, 50000, 50002
http_cache_port_t tcp 8080, 8118, 8123, 10001-10010
http_port_t tcp 80, 81, 443, 488, 8008, 8009, 8443, 9000
intermapper_port_t tcp 8181
prosody_port_t tcp 5280-5281
pulp_port_t tcp 24816, 24817
puppet_port_t tcp 8140
radacct_port_t tcp 1646, 1813
radacct_port_t udp 1646, 1813
radius_port_t tcp 1645, 1812, 18120-18121
radius_port_t udp 1645, 1812, 18120-18121
rkt_port_t tcp 18112
statsd_port_t udp 8125
transproxy_port_t tcp 8081
varnishd_port_t tcp 6081-6082
zookeeper_client_port_t tcp 2181
[gsyudin@gsyudin log]$
```

Figure 2.12: 81 port already added

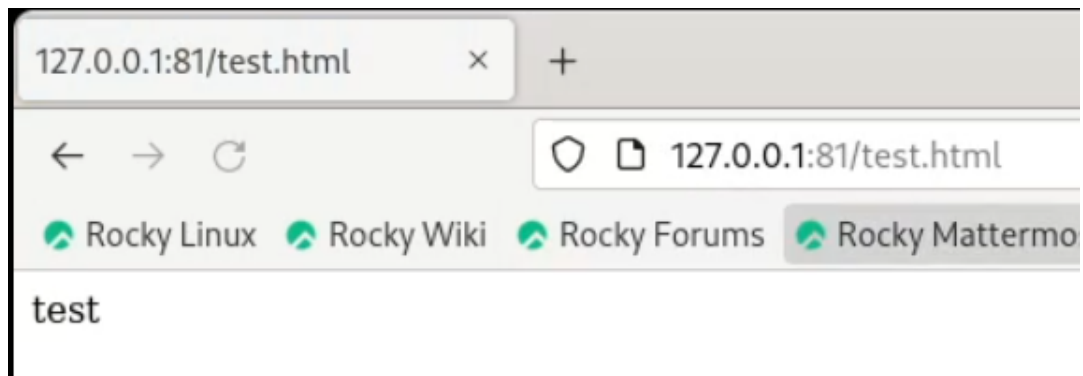


Figure 2.13: web 81 port

3 Вывод

Выполнив данную лабораторную работу, я развил навыки администрирования ОС Linux, получил первое практическое знакомство с технологией SELinux и проверил работу SELinux на практике совместно с веб-сервером Apache.

4 Список литературы

1. Кулябов, Д.С. - Лабораторная работа № 6. Мандатное разграничение прав в Linux https://esystem.rudn.ru/pluginfile.php/1651891/mod_resource/content/2/006-lab_selinux.pdf