

Отчет по лабораторной работе №6

Мандатное разграничение прав в Linux

Асеинова Елизавета

2022 Oct 4th

Содержание

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

Список таблиц

Список иллюстраций

2.1. Вход в систему	6
2.2. Обращение к серверу	7
2.3. Apache в списке процессов	7
2.4. Переключатели	7
2.5. Статистика	8
2.6. Тип файлов	8
2.7. Html файл	9
2.8. Контекст	9
2.9. Отображение в браузере	9
2.10. Изменение контекста	9
2.11. Отказ в доступе	9
2.12. Лог-файлы	10
2.13. Изменение порта	10
2.14. Лог файлы	11
2.15. Подключение порта	11
2.16. Возвращение параметров	12
2.17. Удаление файла	12

1. Цель работы

Целью данной работы является развитие навыка администрирования ОС Linux, получение первого практического знакомства с технологией SELinux¹, проверка работы SELinx на практике совместно с веб-сервером Apache.[1]

2. Выполнение лабораторной работы

1. Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted.

```
[root@evaseinova evaseinova]# getenforce
Enforcing
[root@evaseinova evaseinova]# 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
```

Рис. 2.1.: Вход в систему

2. Обратилась с помощью браузера к веб-серверу, и убедилась, что он работает. Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности. Посмотрела текущее состояние переключателей SELinux для Apache.

```
[root@evaseinova evaseinova]# 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; vendor preset: enabled)
   Active: active (running) since Wed 2022-10-05 18:44:09 MSK; 1min ago
     Docs: man:httpd.service(8)
    Main PID: 2565 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests served 0/0"
     Tasks: 213 (limit: 12202)
    Memory: 25.1M
       CPU: 221ms
    CGroup: /system.slice/httpd.service
            └─2565 /usr/sbin/httpd -DFOREGROUND
              └─2573 /usr/sbin/httpd -DFOREGROUND
                └─2578 /usr/sbin/httpd -DFOREGROUND
                  └─2579 /usr/sbin/httpd -DFOREGROUND
                    └─2581 /usr/sbin/httpd -DFOREGROUND
```

Рис. 2.2.: Обращение к серверу

```
[root@evaseinova evaseinova]# ps auxZ | grep httpd
system u:system r:httpd t:s0 root 2565 0.0 0.5 20248 11512 ?
Ss 18:44 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 2573 0.0 0.3 21572 7316 ?
S 18:44 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 2578 0.0 0.5 1210512 10992 ?
Sl 18:44 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 2579 0.0 0.5 1079376 10992 ?
Sl 18:44 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 2581 0.0 0.5 1079376 10992 ?
Sl 18:44 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023 root 2953 0.0 0.1 2216
2376 pts/0 S+ 18:51 0:00 grep --color=auto httpd
```

Рис. 2.3.: Апахе в списке процессов

```
[root@evaseinova evaseinova]# 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_sss off
httpd_dontaudit_search_dirs off
httpd_enable_cgi on
httpd_enable_ftp_server off
httpd_enable_homedirs off
httpd_execmem off
```

Рис. 2.4.: Переключатели

3. Посмотрела статистику по политике, также определила множество пользователей - 8, ролей - 14, типов - 4995.

```
[root@evaseinova evaseinova]# 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:            4995     Attributes:            254
Users:            8        Roles:                 14
Booleans:         347     Cond. Expr.:          382
Allow:            63727    Neverallow:            0
Auditallow:       163     Dontaudit:             8391
Type_trans:       251060   Type_change:           87
Type_member:       35     Range_trans:           5958
Role_allow:        38     Role_trans:            418
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
```

Рис. 2.5.: Статистика

4. Определила тип файлов и поддиректорий, находящихся в директории /var/www. Определила тип файлов, находящихся в директории /var/www/html. Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html.

```
[root@evaseinova evaseinova]# ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0
:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0
:10 html
[root@evaseinova evaseinova]# ls -lZ /var/www/html
total 0
```

Рис. 2.6.: Тип файлов

5. Создала от имени суперпользователя html-файл. Проверила контекст созданного файла. Обратилась к файлу через веб-сервер. Убедилась, что файл был успешно отображён.


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

Рис. 2.7.: Html файл

```
[root@evaseinova evaseinova]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
```

Рис. 2.8.: Контекст

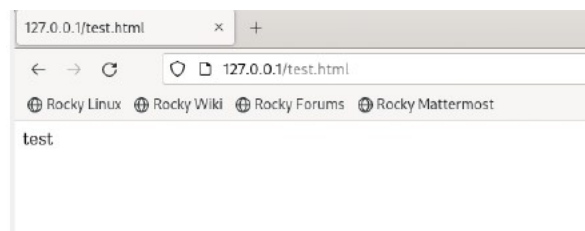


Рис. 2.9.: Отображение в браузере

6. Изменила контекст файла /var/www/html/test.html на samba_share_t.

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

Рис. 2.10.: Изменение контекста

7. Попробовала ещё раз получить доступ к файлу через веб-сервер.

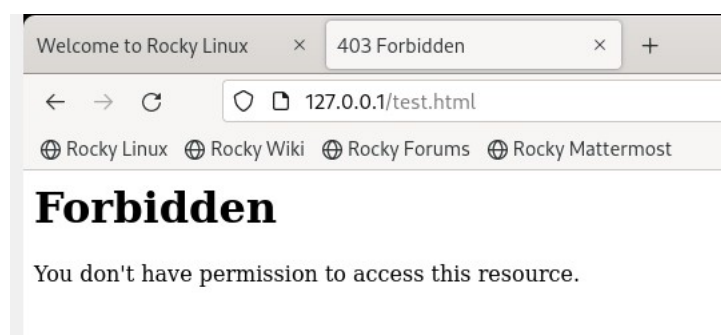


Рис. 2.11.: Отказ в доступе

8. Просмотрела log-файлы веб-сервера Apache и системный лог-файл.

```
[root@evaseinova evaseinova]# tail /var/log/messages
Oct  5 19:24:50 evaseinova setroubleshoot[4006]: SELinux is preventing /usr/sbin
/httd from getattr access on the file /var/www/html/test.html.#012#012***** Pl
ugin restorecon (92.2 confidence) suggests *****#012#012If
you want to fix the label. #012/var/www/html/test.html default label should be h
ttpd_sys_content_t.#012Then you can run restorecon. The access attempt may have
been stopped due to insufficient permissions to access a parent directory in whi
ch case try to change the following command accordingly.#012Do#012# /sbin/restor
econ -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confid
ence) suggests *****#012#012If you want to treat test.html as p
ublic content#012Then you need to change the label on test.html to public_conten
t_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_content_t
'/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012**
*** Plugin catchall (1.41 confidence) suggests *****#012
#012If you believe that httpd should be allowed getattr access on the test.html
file by default.#012Then you should report this as a bug.#012You can generate a
local policy module to allow this access.#012Do#012allow this access for now by
executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodul
e -X 300 -i my-httpd.pp#012
Oct  5 19:24:50 evaseinova setroubleshoot[4006]: failed to retrieve rpm info for
/var/www/html/test.html
Oct  5 19:24:50 evaseinova setroubleshoot[4006]: SELinux is preventing /usr/sbin
/httd from getattr access on the file /var/www/html/test.html. For complete SEL
```

Рис. 2.12.: Лог-файлы

9. Попробовала запустить веб-сервер Apache на прослушивание TCP-порта 81. Выполнила перезапуск веб-сервера Apache.

```
42 # httpd.service is enabled to run at boot time, the s
may not be
43 # available when the service starts. See the
httpd.service(8) man
44 # page for more information.
45 #
46 #Listen 12.34.56.78:80
47 Listen 81
48
49 #
```

Рис. 2.13.: Изменение порта

10. Просмотрела log-файлы веб-сервера Apache.

```
[root@evaseinova evaseinova]# tail /var/log/http/error_log
tail: cannot open '/var/log/http/error_log' for reading: No such file or directory
[root@evaseinova evaseinova]# tail /var/log/httpd/error_log
[Wed Oct 05 18:44:09.022395 2022] [lbmethod_heartbeat:notice] [pid 2565:tid 2565] AH02282: No slotmem from mod_heartbeat
[Wed Oct 05 18:44:09.037429 2022] [mpm_event:notice] [pid 2565:tid 2565] AH00489: Apache/2.4.51 (Rocky Linux) configured -- resuming normal operations
[Wed Oct 05 18:44:09.037452 2022] [core:notice] [pid 2565:tid 2565] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[Wed Oct 05 19:24:43.083592 2022] [core:error] [pid 2579:tid 2770] (13)Permission denied: [client 127.0.0.1:47564] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Wed Oct 05 21:39:25.405352 2022] [mpm_event:notice] [pid 2565:tid 2565] AH00492: caught SIGWINCH, shutting down gracefully
[Wed Oct 05 21:39:26.558674 2022] [core:notice] [pid 5178:tid 5178] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Wed Oct 05 21:39:26.560746 2022] [suexec:notice] [pid 5178:tid 5178] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Wed Oct 05 21:39:26.607127 2022] [lbmethod_heartbeat:notice] [pid 5178:tid 5178]
```

Рис. 2.14.: Лог файлы

11. Выполнила команду `semanage port -a -t http_port_t -p tcp 81`. Попробовала запустить веб-сервер Apache ещё раз.

```
[root@evaseinova evaseinova]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined

[root@evaseinova evaseinova]#
[root@evaseinova evaseinova]# 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@evaseinova evaseinova]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@evaseinova evaseinova]# 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; vendor preset: enabled)
   Active: active (running) since Wed 2022-10-05 21:44:37 MSK; 7s ago
     Docs: man:httpd.service(8)
```

Рис. 2.15.: Подключение порта

12. Вернула контекст `httpd_sys_content_t` к файлу `/var/www/html/ test.html` и открыла его в браузере.

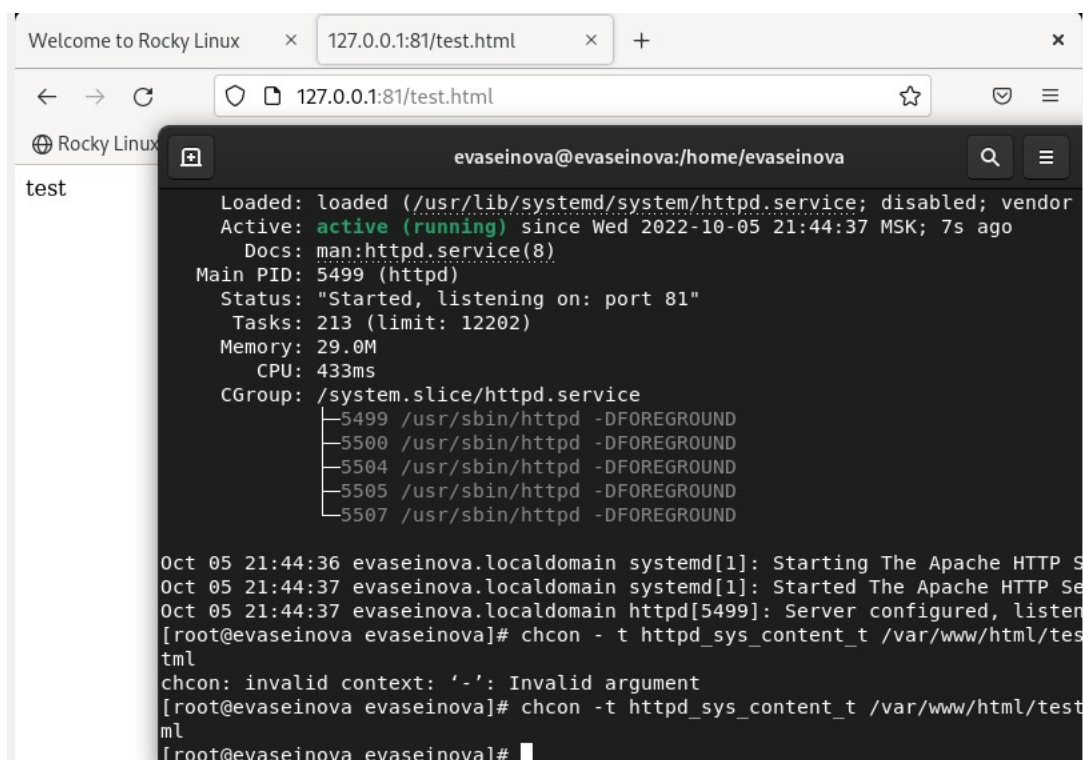


Рис. 2.16.: Возвращение параметров

- Исправила обратно конфигурационный файл apache, удалила привязку http_port_t к 81 порту, удалила файл /var/www/html/test.html.

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

Рис. 2.17.: Удаление файла

3. Выводы

В ходе работы мы развили навыки администрирования ОС Linux, получили первое практическое знакомство с технологией SELinux¹, проверили работу SELinx на практике совместно с веб-сервером Apache.

4. Список литературы

1. Методические материалы курса