

Отчет по лабораторной работе №6

Мандатное разграничение прав в Linux

Бармина Ольга Константиновна

2022 Sep 22th

Содержание

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

Список таблиц

Список иллюстраций

2.1. рис 1. вход в систему	6
2.2. рис 2. обращение к серверу	7
2.3. рис 3. состояние переключателей	7
2.4. рис 4. статистика	8
2.5. рис 5. тип файлов	8
2.6. рис 6. html файл	9
2.7. рис 7. контекст	9
2.8. рис 8. отображение в браузере	9
2.9. рис 9. изменение контекста	9
2.10. рис 10. отказ в доступе	10
2.11. рис 11. лог-файлы	10
2.12. рис 12. изменение порта	11
2.13. рис 13. лог файлы	11
2.14. рис 14. подключение порта	12
2.15. рис 15. возвращение параметров	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@localhost okbarmina]# getenforce
Enforcing
[root@localhost okbarmina]# 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 okbarmina]#
```

Рис. 2.1.: рис 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@localhost okbarmina]# 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 pre>
   Active: active (running) since Tue 2022-09-27 11:17:26 MSK; 4s ago
     Docs: man:httpd.service(8)
  Main PID: 3576 (httpd)
    Status: "Started, listening on: port 80"
     Tasks: 213 (limit: 12215)
    Memory: 26.9M
       CPU: 86ms
    CGroup: /system.slice/httpd.service
            └─3576 /usr/sbin/httpd -DFOREGROUND
              └─3577 /usr/sbin/httpd -DFOREGROUND
                └─3581 /usr/sbin/httpd -DFOREGROUND
                  └─3582 /usr/sbin/httpd -DFOREGROUND
                    └─3583 /usr/sbin/httpd -DFOREGROUND
```

Рис. 2.2.: рис 2. обращение к серверу

```
[root@localhost okbarmina]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 3576 0.0 0.5 20064 11536 ?
Ss 11:17 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3577 0.0 0.3 21516 7216 ?
S 11:17 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3581 0.0 0.5 1079216 10864 ?
Sl 11:17 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3582 0.0 0.6 1210352 12912 ?
Sl 11:17 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3583 0.0 0.5 1079216 10864 ?
Sl 11:17 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 3819 0.0 0.1 221668
2316 pts/0 S+ 11:19 0:00 grep --color=auto httpd
```

Рис. 2.3.: рис 3. состояние переключателей

3. Посмотрела статистику по политике, также определила множество пользо-
вателей, ролей, типов.

```

[root@localhost okbarmina]# 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

```

Рис. 2.4.: рис 4. 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@localhost okbarmina]# 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
[root@localhost okbarmina]# ls -lZ /var/www/html
total 0

```

Рис. 2.5.: рис 5. 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.

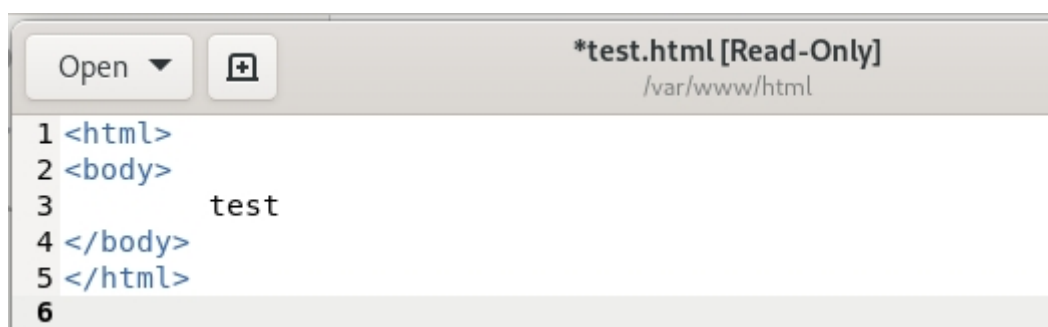


Рис. 2.6.: рис 6. html файл

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

Рис. 2.7.: рис 7. контекст

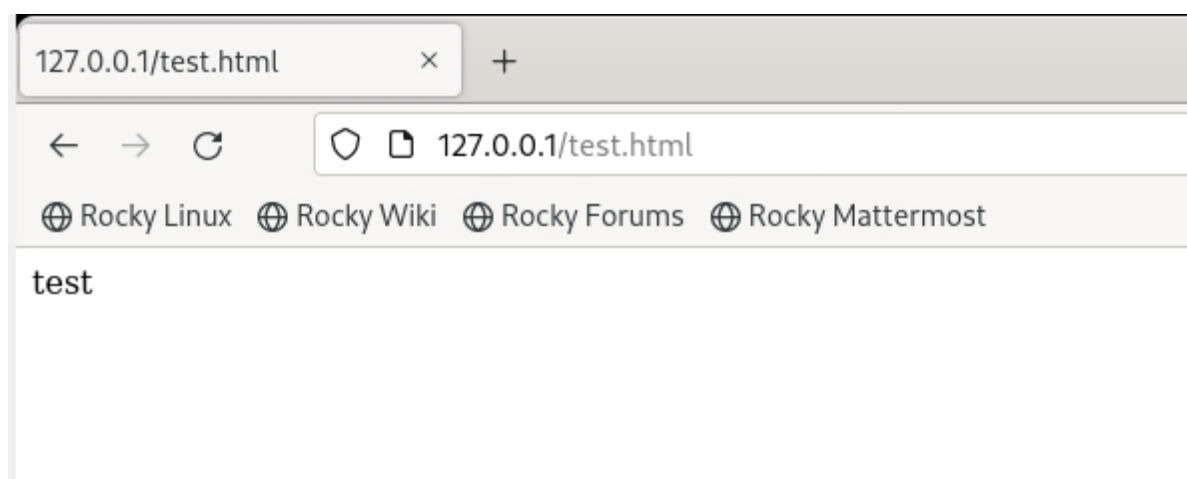


Рис. 2.8.: рис 8. отображение в браузере

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

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

Рис. 2.9.: рис 9. изменение контекста

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

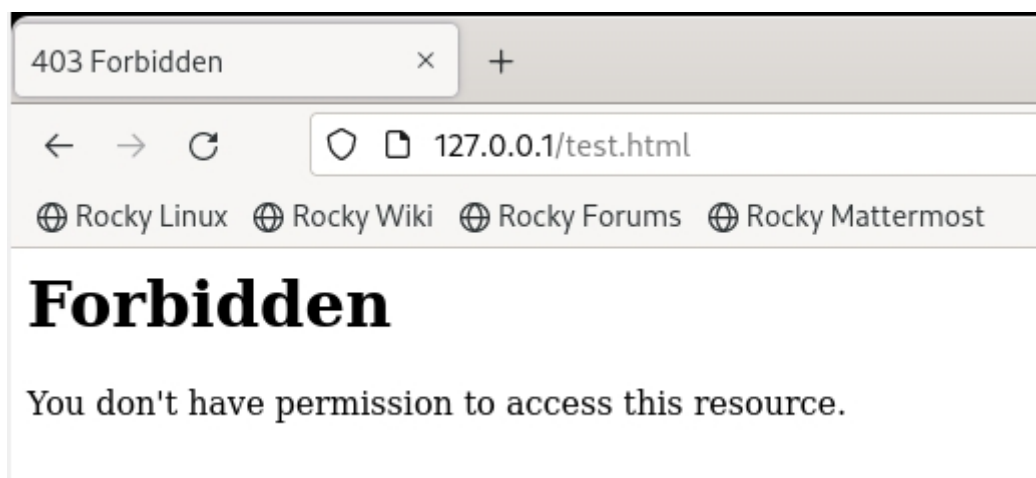


Рис. 2.10.: рис 10. отказ в доступе

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

```
[root@localhost okbarmina]# tail /var/log/messages
Sep 27 11:33:36 localhost setroubleshoot[4702]: SELinux is preventing /usr/sbin/httpd
from getattr access on the file /var/www/html/test.html. For complete SELinux messages
run: sealert -l 7723672c-f35a-4c73-8a0c-2882b8e6709c
Sep 27 11:33:36 localhost setroubleshoot[4702]: SELinux is preventing /usr/sbin/httpd
from getattr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon
on (92.2 confidence) suggests *****#012#012If you want to fix the
label. #012/var/www/html/test.html default label should be httpd_sys_content_t.#012Th
en you can run restorecon. The access attempt may have been stopped due to insufficien
t permissions to access a parent directory in which case try to change the following c
ommand accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012****
* Plugin public_content (7.83 confidence) suggests *****#012#012If y
ou want to treat test.html as public content#012Then you need to change the label on t
est.html to public_content_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.ht
ml'#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# semodule -X 300 -i my-ht
tpd.pp#012
```

Рис. 2.11.: рис 11. лог-файлы

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

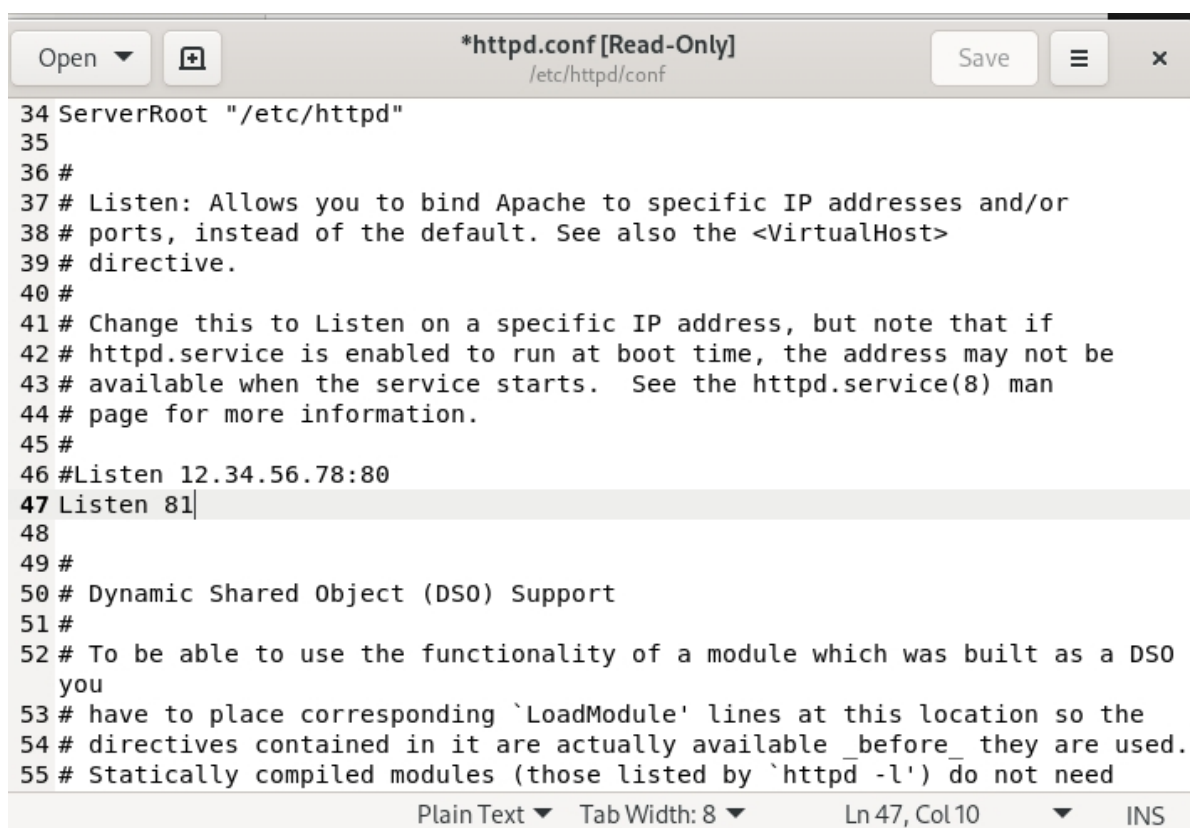


Рис. 2.12.: рис 12. изменение порта

10. Просмотрела log-файлы веб-сервера Apache.

```

[root@localhost okbarmina]# tail /var/log/http/error_log
tail: cannot open '/var/log/http/error_log' for reading: No such file or directory
[root@localhost okbarmina]# tail /var/log/http/access_log
tail: cannot open '/var/log/http/access_log' for reading: No such file or directory
[root@localhost okbarmina]# tail /var/log/audit/audit.log
type=AVC msg=audit(1664267877.485:245): avc: denied { getattr } for pid=3582 comm="
httpd" path="/var/www/html/test.html" dev="dm-0" ino=101151653 scontext=system_u:syste
m_r:httpd_t:s0 tcontext=unconfined_u:object_r:samba_share_t:s0 tclass=file permissive=
0
type=SYSCALL msg=audit(1664267877.485:245): arch=c000003e syscall=262 success=no exit=
-13 a0=ffffff9c a1=7fafd0043a30 a2=7fafca7f3330 a3=0 items=0 ppid=3576 pid=3582 auid=4
294967295 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) s
es=4294967295 comm="httpd" exe="/usr/sbin/httpd" subj=system_u:system_r:httpd_t:s0 key
=(null)ARCH=x86_64 SYSCALL=newfstatat AUID="unset" UID="apache" GID="apache" EUID="apa
che" SUID="apache" FSUID="apache" EGID="apache" SGID="apache" FSGID="apache"
type=PROCTITLE msg=audit(1664267877.485:245): proctitle=2F7573722F7362696E2F6874747064
002D44464F524547524F554E44
type=AVC msg=audit(1664267877.486:246): avc: denied { getattr } for pid=3582 comm="
httpd" path="/var/www/html/test.html" dev="dm-0" ino=101151653 scontext=system_u:syste
m_r:httpd_t:s0 tcontext=unconfined_u:object_r:samba_share_t:s0 tclass=file permissive=
0

```

Рис. 2.13.: рис 13. лог файлы

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

```
[root@localhost okbarmina]# semanage port -a -t http_port_t -p tcp 81
bash: semanage: command not found.
[root@localhost okbarmina]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@localhost okbarmina]# 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. 2.14.: рис 14. подключение порта

12. Вернула контекст `httpd_sys_content_t` к файлу `/var/www/html/ test.html`. Исправила обратно конфигурационный файл `apache`, удалила привязку `http_port_t` к 81 порту, удалила файл `/var/www/html/test.html`.

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

Рис. 2.15.: рис 15. возвращение параметров

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