

# Отчет по лабораторной работе №6

Мандатное разграничение прав в Linux

Евсеева Дарья Олеговна

15 октября, 2022

# Содержание

|                                                  |    |
|--------------------------------------------------|----|
| Цель работы                                      | 4  |
| Задание                                          | 5  |
| Теоретическое введение                           | 6  |
| Выполнение лабораторной работы                   | 7  |
| Работа с SELinux и веб-сервером Apache . . . . . | 7  |
| Выводы                                           | 19 |
| Список литературы                                | 20 |

# Список иллюстраций

|    |                                                         |    |
|----|---------------------------------------------------------|----|
| 1  | Проверка режима работы SELinux . . . . .                | 7  |
| 2  | Проверка работы веб-сервера . . . . .                   | 8  |
| 3  | Определение контекста . . . . .                         | 8  |
| 4  | Просмотр состояния переключателей . . . . .             | 8  |
| 5  | Просмотр статистики по политике . . . . .               | 9  |
| 6  | Просмотр содержимого директории /var/www . . . . .      | 9  |
| 7  | Просмотр содержимого директории /var/www/html . . . . . | 9  |
| 8  | Создание html-файла . . . . .                           | 10 |
| 9  | Содержимое файла . . . . .                              | 10 |
| 10 | Определение контекста файла . . . . .                   | 10 |
| 11 | Обращение к файлу через веб-сервер . . . . .            | 11 |
| 12 | Просмотр справки httpd_selinux . . . . .                | 11 |
| 13 | Соответствующий файлу контекст . . . . .                | 11 |
| 14 | Изменение контекста . . . . .                           | 12 |
| 15 | Попытка получения доступа к файлу . . . . .             | 12 |
| 16 | Проверка прав доступа . . . . .                         | 12 |
| 17 | Просмотр лог-файлов (1) . . . . .                       | 13 |
| 18 | Просмотр лог-файлов (2) . . . . .                       | 13 |
| 19 | Просмотр лог-файлов (3) . . . . .                       | 13 |
| 20 | Просмотр системного лог-файла . . . . .                 | 14 |
| 21 | Открытие файла /etc/httpd/conf/httpd.conf . . . . .     | 14 |
| 22 | Внесение изменений в файл . . . . .                     | 14 |
| 23 | Перезапуск веб-сервера Apache . . . . .                 | 14 |
| 24 | Просмотр системного лог-файла . . . . .                 | 15 |
| 25 | Просмотр лог-файлов (1) . . . . .                       | 15 |
| 26 | Просмотр лог-файлов (2) . . . . .                       | 15 |
| 27 | Просмотр лог-файлов (3) . . . . .                       | 16 |
| 28 | Выполнение привязки и просмотр списка портов . . . . .  | 16 |
| 29 | Перезапуск веб-сервера Apache . . . . .                 | 16 |
| 30 | Возвращение изначального контекста . . . . .            | 17 |
| 31 | Получение доступа к файлу через веб-сервер . . . . .    | 17 |
| 32 | Исправление конфигурационного файла . . . . .           | 18 |
| 33 | Удаление привязки к порту . . . . .                     | 18 |
| 34 | Удаление html-файла . . . . .                           | 18 |

## Цель работы

Целью данной работы является развитие навыков администрирования ОС Linux, ознакомление с технологией SELinux, а также проверка работы SELinux на практике совместно с веб-сервером Apache.

# Задание

Провести работу с SELinux и веб-сервером Apache.

# Теоретическое введение

Мандатное управление доступом (Mandatory Access Control, MAC) - это система разграничения доступа на основе уровня доступа субъекта и защитной метки объекта. Смысл состоит в том, что субъект может получить доступ к тем объектам, у которых метка безопасности имеет тот же уровень или ниже, что и у объекта.

Субъект - это пользователь, вернее процесс, который он инициализирует. Объект - это файл, программа, база данных и любой из ее объектов, даже сетевой пакет. Также предусмотрена иерархическая структура уровней доступа. Всем субъектам и объектам назначаются так называемые метки - значение уровня доступа у субъекта и значение уровня конфиденциальности для объекта.

Каждый раз, когда субъект запрашивает объект происходит проверка соответствия меток и принимается решение о разрешении или запрете доступа. Так как структура уровней доступа иерархическая, то субъект имеет доступ к объектам соответствующего уровня конфиденциальности, а также ко всем другим уровням, находящимся по иерархии ниже. Проверка уровня доступа это вертикальная безопасность, но в MAC предусмотрена и горизонтальная. В дополнение к уровням безопасности, существуют категории. Благодаря им можно разграничивать доступ среди субъектов с одинаковым уровнем доступа.

# Выполнение лабораторной работы

Выполнять работу будем в операционной системе, установленной при выполнении первой лабораторной работы.

## Работа с SELinux и веб-сервером Apache

Для начала войдем в систему и убедимся, что SELinux работает в режиме enforcing политики targeted.

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

Рис. 1: Проверка режима работы SELinux

Далее, обратимся с помощью браузера к веб-серверу и убедимся, что последний работает.

```
[root@doevseeva doevseeva]# 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 Sat 2022-10-15 12:41:35 MSK; 1h 41min ago
     Docs: man:httpd.service(8)
   Main PID: 4062 (httpd)
      Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes
      Tasks: 213 (limit: 12212)
     Memory: 26.8M
        CPU: 5.620s
       CGroup: /system.slice/httpd.service
           ├─4062 /usr/sbin/httpd -DFOREGROUND
           ├─4063 /usr/sbin/httpd -DFOREGROUND
           ├─4067 /usr/sbin/httpd -DFOREGROUND
           ├─4068 /usr/sbin/httpd -DFOREGROUND
           └─4069 /usr/sbin/httpd -DFOREGROUND

Oct 15 12:41:35 doevseeva.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 15 12:41:35 doevseeva.localdomain systemd[1]: Started The Apache HTTP Server...
Oct 15 12:41:35 doevseeva.localdomain httpd[4062]: Server configured, listening...
[root@doevseeva doevseeva]#
```

Рис. 2: Проверка работы веб-сервера

Найдем веб-сервер Apache в списке процессов и определим его контекст безопасности.

```
[root@doevseeva doevseeva]# ps -eZ | grep httpd
system_u:system_r:httpd_t:s0    4062 ?          00:00:00 httpd
system_u:system_r:httpd_t:s0    4063 ?          00:00:00 httpd
system_u:system_r:httpd_t:s0    4067 ?          00:00:01 httpd
system_u:system_r:httpd_t:s0    4068 ?          00:00:01 httpd
system_u:system_r:httpd_t:s0    4069 ?          00:00:01 httpd
[root@doevseeva doevseeva]#
```

Рис. 3: Определение контекста

Как мы видим, контекст веб-сервера Apache – system\_u:system\_r:httpd\_t:s0.  
Посмотрим текущее состояние переключателей SELinux для Apache.

```
[root@doevseeva doevseeva]# 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
```

Рис. 4: Просмотр состояния переключателей

Мы видим, что многие выключатели находятся в положении ‘off’.

Посмотрим статистику по политике с помощью команды seinfo и определим множество пользователей, ролей и типов.

```
[root@doevseeva doevseeva]# 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
```

Рис. 5: Просмотр статистики по политике

Здесь мы видим, что множество пользователей состоит из 4 пользователей, во множестве ролей находится 14 ролей, а во множестве типов — 5002 типа.

Далее посмотрим на содержимое директории /var/www.

```
[root@doevseeva doevseeva]# 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@doevseeva doevseeva]#
```

Рис. 6: Просмотр содержимого директории /var/www

Мы видим, что в директории находятся две поддиректории.

Также определим содержимое директории /var/www/html.

```
[root@doevseeva doevseeva]# ls -lZ /var/www/html/
total 0
[root@doevseeva doevseeva]#
```

Рис. 7: Просмотр содержимого директории /var/www/html

Мы видим, что в данной директории нет файлов или поддиректорий.

Чтобы определить круг пользователей, который разрешено создание файлов в директории /var/www/html, посмотрим на вывод команды на рис.6. Как мы видим,

создание файлов в данной директории разрешено только для пользователя, который является владельцем директории.

Создадим от имени суперпользователя html-файл /var/www/html/test.html.

```
[root@doevseeva doevseeva]# touch /var/www/html/test.html  
[root@doevseeva doevseeva]# vi /var/www/html/test.html
```

Рис. 8: Создание html-файла

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

Рис. 9: Содержимое файла

Далее проверим контекст созданного файла.

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

Рис. 10: Определение контекста файла

Мы видим, что контекст, присваиваемый по умолчанию файлам, созданным в данной директории — это `unconfined_u:object_r:httpd_system_content_t:s0`.

Обратимся к файлу через веб-сервер.

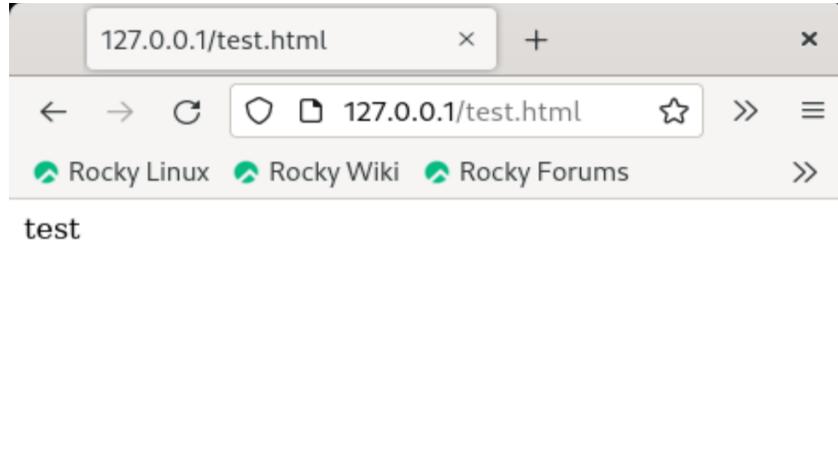


Рис. 11: Обращение к файлу через веб-сервер

Как мы видим, файл успешно отображается.

Изучим справку man httpd\_selinux и найдем в ней контекст, соответствующий созданному файлу.

```
[root@doevseeva doevseeva]# man httpd_selinux  
[root@doevseeva doevseeva]#
```

Рис. 12: Просмотр справки httpd\_selinux

```
httpd_sys_content_t  
- Set files with the httpd_sys_content_t type, if you want to treat the  
files as httpd sys content.  
Paths:  
/srv/([^\/*/]?)?www(.*?), /var/www(.*?), /etc/htdig(.*?),  
/srv/gallery2(.*?), /var/lib/trac(.*?), /var/lib/htdig(.*?),  
/var/www/icons(.*?), /usr/share/glpi(.*?), /usr/share/ht-  
dig(.*?), /usr/share/drupal.*, /usr/share/z-push(.*?),  
/var/www/svn/conf(.*?), /usr/share/icecast(.*?),  
/var/lib/cacti/rra(.*?), /usr/share/ntop/html(.*?),  
/usr/share/nginx/html(.*?), /usr/share/doc/ghc/html(.*?),  
/usr/share/openca/htdocs(.*?), /usr/share/selinux-pol-  
icy[^/*/]*/html(.*?)?
```

Рис. 13: Соответствующий файлу контекст

Изменим контекст файла на такой, к которому процесс httpd не должен иметь доступа, и проверим успешность изменения контекста.

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

Рис. 14: Изменение контекста

Еще раз попробуем получить доступ к файлу через веб-сервер, а также проверим права доступа к файлу.

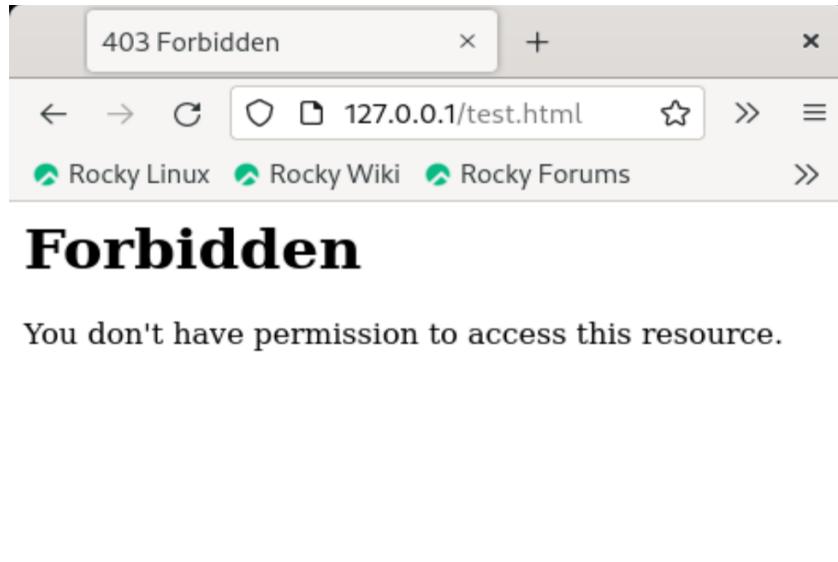


Рис. 15: Попытка получения доступа к файлу

```
[root@doevseeva doevseeva]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 34 Oct 15 14:30 /var/www/html/test.html
[root@doevseeva doevseeva]#
[root@doevseeva doevseeva]#
```

Рис. 16: Проверка прав доступа

Мы видим, что на этот раз в доступе было отказано, и файл не был отображен. Несмотря на то, что доступ на чтение файла является открытым, файл не отображается из-за того, что ранее мы поменяли его контекст на такой, к которому нет доступа у процесса httpd.

Просмотрим лог-файлы веб-сервера Apache, а также системный лог-файл.

```
[root@doevseeva doevseeva]# tail -n 5 /var/log/httpd/error_log
[Sat Oct 15 12:41:35.946597 2022] [suexec:notice] [pid 4062:tid 4062] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Sat Oct 15 12:41:35.958939 2022] [lbmethod_heartbeat:notice] [pid 4062:tid 4062] AH02282: No slotmem from mod_heartbeat
[Sat Oct 15 12:41:35.969710 2022] [mpm_event:notice] [pid 4062:tid 4062] AH00489: Apache/2.4.51 (Rocky Linux) configured -- resuming normal operations
[Sat Oct 15 12:41:35.969741 2022] [core:notice] [pid 4062:tid 4062] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[Sat Oct 15 14:37:53.409216 2022] [core:error] [pid 4069:tid 4260] (13)Permission denied: [client 127.0.0.1:48036] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[root@doevseeva doevseeva]#
```

Рис. 17: Просмотр лог-файлов (1)

```
[root@doevseeva doevseeva]# tail -n 5 /var/log/httpd/access_log
127.0.0.1 - - [15/Oct/2022:14:34:55 +0300] "GET /test.html HTTP/1.1" 200 34 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
127.0.0.1 - - [15/Oct/2022:14:34:56 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "
http://127.0.0.1/test.html" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201
0101 Firefox/102.0"
127.0.0.1 - - [15/Oct/2022:14:37:53 +0300] "GET /test.html HTTP/1.1" 403 199 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
[root@doevseeva doevseeva]#
```

Рис. 18: Просмотр лог-файлов (2)

```
[root@doevseeva doevseeva]# tail -n 5 /var/log/audit/audit.log
type=PROCTITLE msg=audit(1665833873.406:252): proctitle=2F7573722F7362696E2F6874
747064002D044464F524547524F554E44
type=SERVICE_START msg=audit(1665833873.454:253): pid=1 uid=0 auid=4294967295 se
s=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dbus-:1.10-org.fedoraproj
ect.Setroubleshootd@0 comm="systemd" exe="/usr/lib/systemd/systemd" hostname=?'
addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_START msg=audit(1665833877.520:254): pid=1 uid=0 auid=4294967295 se
s=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dbus-:1.10-org.fedoraproj
ect.SetroubleshootPrivileged@0 comm="systemd" exe="/usr/lib/systemd/systemd" ho
stname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1665833895.843:255): pid=1 uid=0 auid=4294967295 ses
=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dbus-:1.10-org.fedoraproj
ect.SetroubleshootPrivileged@0 comm="systemd" exe="/usr/lib/systemd/systemd" hos
tname=? addr=? terminal=? res=failed'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1665833895.924:256): pid=1 uid=0 auid=4294967295 ses
=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dbus-:1.10-org.fedoraproj
ect.Setroubleshootd@0 comm="systemd" exe="/usr/lib/systemd/systemd" hostname=?'
addr=? terminal=? res=failed'UID="root" AUID="unset"
[root@doevseeva doevseeva]#
```

Рис. 19: Просмотр лог-файлов (3)

```
[root@doevseeva doevseeva]# tail -n 5 /var/log/messages
Oct 15 14:38:15 doevseeva systemd[1]: dbus-:1.10-org.fedoraproject.Setroublesho
td@0.service: Main process exited, code=killed, status=14/ALRM
Oct 15 14:38:15 doevseeva systemd[1]: dbus-:1.10-org.fedoraproject.Setroublesho
td@0.service: Failed with result 'signal'.
Oct 15 14:38:15 doevseeva systemd[1]: dbus-:1.10-org.fedoraproject.Setroublesho
td@0.service: Consumed 1.853s CPU time.
Oct 15 14:41:22 doevseeva gnome-shell[1594]: Window manager warning: last_user_t
ime (8227526) is greater than comparison timestamp (8227495). This most likely
represents a buggy client sending inaccurate timestamps in messages such as _NET
_ACTIVE_WINDOW. Trying to work around...
Oct 15 14:41:22 doevseeva gnome-shell[1594]: Window manager warning: W1 appears
to be one of the offending windows with a timestamp of 8227526. Working around.
..
[root@doevseeva doevseeva]#
[root@doevseeva doevseeva]#
```

Рис. 20: Просмотр системного лог-файла

Теперь попробуем запустить веб-сервер Apache на прослушивание TCP-порта 81, для чего внесем изменения в файл /etc/httpd/conf/httpd.conf.

```
[root@doevseeva doevseeva]# vi /etc/httpd/conf/httpd.conf
[root@doevseeva doevseeva]#
[root@doevseeva doevseeva]#
```

Рис. 21: Открытие файла /etc/httpd/conf/httpd.conf

```
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts. See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
Listen 81

#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
-- INSERT --          47,10      9%
```

Рис. 22: Внесение изменений в файл

Выполним перезапуск веб-сервера Apache.

```
[root@doevseeva doevseeva]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
```

Рис. 23: Перезапуск веб-сервера Apache

Далее просмотрим лог-файлы.

```
[root@doevseeva doevseeva]# tail -n 5 /var/log/messages
Oct 15 14:49:53 doevseeva gnome-shell[1594]: Window manager warning: W1 appears
to be one of the offending windows with a timestamp of 8738930. Working around.
...
Oct 15 14:51:07 doevseeva gnome-shell[1594]: Window manager warning: last_user_t
ime (8813261) is greater than comparison timestamp (8813248). This most likely
represents a buggy client sending inaccurate timestamps in messages such as _NET
_ACTIVE_WINDOW. Trying to work around...
Oct 15 14:51:07 doevseeva gnome-shell[1594]: Window manager warning: W1 appears
to be one of the offending windows with a timestamp of 8813261. Working around.
...
Oct 15 14:51:20 doevseeva gnome-shell[1594]: Window manager warning: last_user_t
ime (8825866) is greater than comparison timestamp (8825858). This most likely
represents a buggy client sending inaccurate timestamps in messages such as _NET
_ACTIVE_WINDOW. Trying to work around...
Oct 15 14:51:20 doevseeva gnome-shell[1594]: Window manager warning: W1 appears
to be one of the offending windows with a timestamp of 8825866. Working around.
...
[root@doevseeva doevseeva]#
```

Рис. 24: Просмотр системного лог-файла

```
[root@doevseeva doevseeva]#
[root@doevseeva doevseeva]# tail -n 5 /var/log/httpd/error_log
[Sat Oct 15 14:48:28.448243 2022] [core:notice] [pid 8593:tid 8593] SELinux poli
cy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Sat Oct 15 14:48:28.452531 2022] [suexec:notice] [pid 8593:tid 8593] AH01232: s
uEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Sat Oct 15 14:48:28.487958 2022] [lbmethod_heartbeat:notice] [pid 8593:tid 8593
] AH02282: No slotmem from mod_heartbeatmonitor
[Sat Oct 15 14:48:28.556027 2022] [mpm_event:notice] [pid 8593:tid 8593] AH00489
: Apache/2.4.51 (Rocky Linux) configured -- resuming normal operations
[Sat Oct 15 14:48:28.556082 2022] [core:notice] [pid 8593:tid 8593] AH00094: Com
mand line: '/usr/sbin/httpd -D FOREGROUND'
[root@doevseeva doevseeva]#
```

Рис. 25: Просмотр лог-файлов (1)

```
[root@doevseeva doevseeva]# tail -n 5 /var/log/httpd/access_log
127.0.0.1 - - [15/Oct/2022:14:34:56 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "
http://127.0.0.1/test.html" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201
00101 Firefox/102.0"
127.0.0.1 - - [15/Oct/2022:14:37:53 +0300] "GET /test.html HTTP/1.1" 403 199 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
127.0.0.1 - - [15/Oct/2022:14:46:26 +0300] "GET /test.html HTTP/1.1" 403 199 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
127.0.0.1 - - [15/Oct/2022:14:46:33 +0300] "GET /test.html HTTP/1.1" 403 199 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
127.0.0.1 - - [15/Oct/2022:14:47:21 +0300] "GET /test.html HTTP/1.1" 403 199 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
[root@doevseeva doevseeva]#
```

Рис. 26: Просмотр лог-файлов (2)

```
[root@doevseeva doevseeva]# tail -n 5 /var/log/audit/audit.log
type=SERVICE_START msg=audit(1665834444.166:268): pid=1 uid=0 auid=4294967295 se
s=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dbus-1.10-org.fedoraproj
ect.SertroubleshootPrivileged@2 comm="systemd" exe="/usr/lib/systemd/systemd" ho
stname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1665834456.705:269): pid=1 uid=0 auid=4294967295 ses
=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dbus-1.10-org.fedoraproj
ect.SertroubleshootPrivileged@2 comm="systemd" exe="/usr/lib/systemd/systemd" hos
tname=? addr=? terminal=? res=failed'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1665834456.773:270): pid=1 uid=0 auid=4294967295 ses
=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dbus-1.10-org.fedoraproj
ect.Sertroubleshootd@2 comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? a
ddr=? terminal=? res=failed'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1665834508.313:271): 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" A
UID="unset"
type=SERVICE_START msg=audit(1665834508.484:272): pid=1 uid=0 auid=4294967295 se
s=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"
[root@doevseeva doevseeva]#
```

Рис. 27: Просмотр лог-файлов (3)

Мы можем заметить, что в каждом из лог-файлов появились записи.

Выполним команду semanage port и проверим список портов.

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

Рис. 28: Выполнение привязки и просмотр списка портов

Мы видим, что в нашей системе порт 81 изначально находился в списке.

Еще раз попробуем перезапустить веб-сервер Apache.

```
Redirecting to /bin/systemctl restart httpd.service
[root@doevseeva doevseeva]#
[root@doevseeva doevseeva]# 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 Sat 2022-10-15 15:02:30 MSK; 38s ago
     Docs: man:httpd.service(8)
   Main PID: 9058 (httpd)
      Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes
      Tasks: 213 (limit: 12212)
     Memory: 32.7M
        CPU: 289ms
      CGroup: /system.slice/httpd.service
              └─9058 /usr/sbin/httpd -DFOREGROUND
                  ├─9059 /usr/sbin/httpd -DFOREGROUND
                  ├─9063 /usr/sbin/httpd -DFOREGROUND
                  ├─9064 /usr/sbin/httpd -DFOREGROUND
                  └─9066 /usr/sbin/httpd -DFOREGROUND

Oct 15 15:02:30 doevseeva.localdomain systemd[1]: Starting The Apache HTTP Server>
Oct 15 15:02:30 doevseeva.localdomain systemd[1]: Started The Apache HTTP Server>
Oct 15 15:02:30 doevseeva.localdomain httpd[9058]: Server configured, listening on >
[root@doevseeva doevseeva]#
```

Рис. 29: Перезапуск веб-сервера Apache

Вернем изначальный контекст созданному файлу, и попробуем получить к нему доступ через веб-сервер.

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

Рис. 30: Возвращение изначального контекста

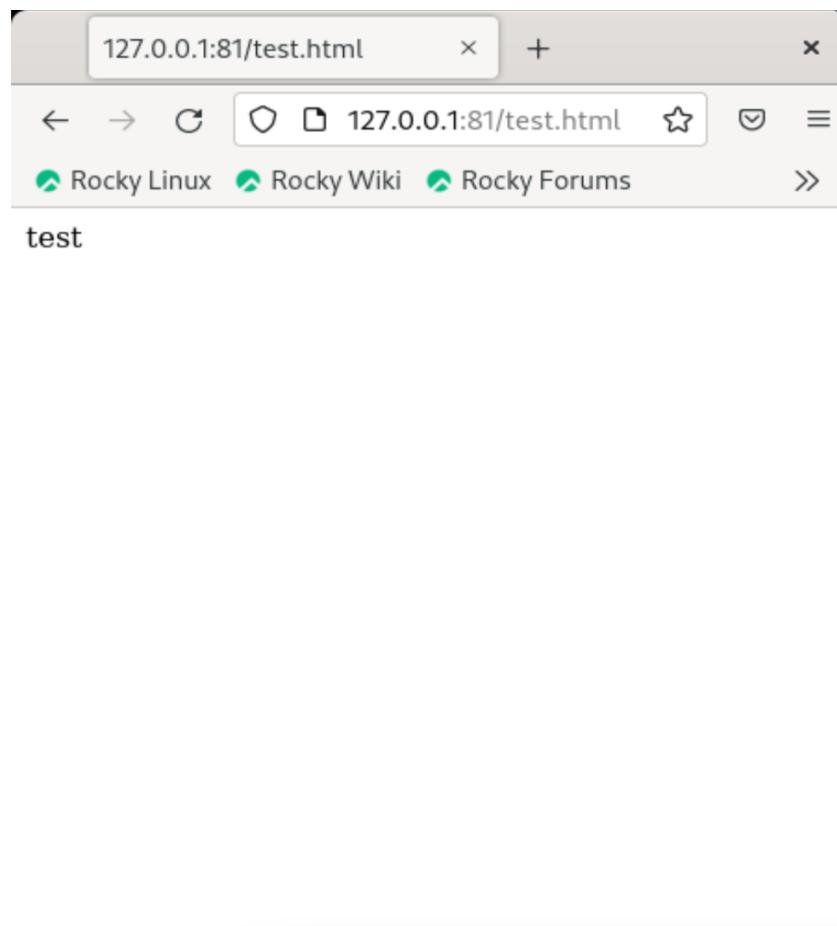


Рис. 31: Получение доступа к файлу через веб-сервер

Мы видим, что содержимое файла успешно отобразилось.

Исправим конфигурационный файл Apache, вернув 'Listen 80'.

```
#  
# Change this to Listen on a specific IP address, but note that if  
# httpd.service is enabled to run at boot time, the address may not be  
# available when the service starts. See the httpd.service(8) man  
# page for more information.  
#  
#Listen 12.34.56.78:80  
Listen 80  
  
#  
# Dynamic Shared Object (DSO) Support  
#  
# To be able to use the functionality of a module which was built as a DSO you  
# have to place corresponding 'LoadModule' lines at this location so the  
# directives contained in it are actually available _before_ they are used.  
# Statically compiled modules (those listed by 'httpd -l') do not need  
# to be loaded here.  
#  
# Example:  
# LoadModule foo_module modules/mod_foo.so  
:wq
```

Рис. 32: Исправление конфигурационного файла

Удалим привязку к 81 порту.

```
[root@doevseeva doevseeva]# semanage port -d -t http_port_t -p tcp 81  
ValueError: Port tcp/81 is defined in policy, cannot be deleted
```

Рис. 33: Удаление привязки к порту

Как мы видим, в нашей системе мы не можем удалить привязку к данному порту.

Удалим созданный html-файл.

```
[root@doevseeva doevseeva]# rm /var/www/html/test.html  
rm: remove regular file '/var/www/html/test.html'? y  
[root@doevseeva doevseeva]#
```

Рис. 34: Удаление html-файла

## Выводы

В результате проделанной работы мы развили навыки администрирования ОС Linux, ознакомились с технологией SELinux, а также проверили работу SELinux на практике совместно с веб-сервером Apache.

## Список литературы

- Методические материалы к лабораторной работе, представленные на сайте “ТУИС РУДН” <https://esystem.rudn.ru/>