

# **Лабораторная работа №6**

**Мандатное разграничение прав в Linux**

Дугаева Светлана Анатольевна

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Подготовка лабораторного стенда</b>	<b>5</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>4</b>	<b>Выводы</b>	<b>18</b>

## Список иллюстраций

3.1	П. 1 выполнения ЛР и подготовка . . . . .	6
3.2	Статус веб-сервера и политика безопасности . . . . .	7
3.3	Состояние переключателей . . . . .	8
3.4	Пункты 5-8 . . . . .	9
3.5	Пункты 9-10 . . . . .	10
3.6	Обращение к файлу через веб-сервер . . . . .	10
3.7	Справка о контекстах . . . . .	11
3.8	Изменение контекста . . . . .	11
3.9	Доступ к файлу через веб-браузер . . . . .	12
3.10	log-файлы веб-сервера Apache и системный log файл . . . . .	12
3.11	ошибки в файле audit.log . . . . .	13
3.12	Смена порта . . . . .	13
3.13	Перезапуск веб-сервера . . . . .	14
3.14	log файлы /var/log/messages . . . . .	14
3.15	Файл error_log . . . . .	15
3.16	Файл audit.log . . . . .	15
3.17	Пункты 19-21 . . . . .	16
3.18	Доступ к файлу через веб-браузер . . . . .	16
3.19	Вернула конфиг. файл в первоначальное состояние . . . . .	17
3.20	Пункты 23-24 . . . . .	17

# 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 Подготовка лабораторного стенда

В конфигурационном файле `/etc/httpd/httpd.conf` необходимо задать параметр `ServerName: ServerName test.ru` чтобы при запуске веб-сервера не выдавались лишние сообщения об ошибках, не относящихся к лабораторной работе. Выполнила задание параметра с помощью команды `echo "ServerName test.ru" > /etc/httpd/httpd.conf`

Также необходимо проследить, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp. Отключила фильтр можно командами `iptables -F iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT`

### 3 Выполнение лабораторной работы

1. Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`

Действия из подготовки лабораторного стенда и пункта 1 выполнения лабораторной работы представлены на (рис. -@fig:001):

```
[dugaevs@localhost ~]$ su
Пароль:
[root@localhost dugaevs]# echo "ServerName test.ru" >> /etc/httpd/httpd.conf
[root@localhost dugaevs]# cat /etc/httpd/httpd.conf
ServerName test.ru
[root@localhost dugaevs]# iptables -F
[root@localhost dugaevs]# iptables -P INPUT ACCEPT
[root@localhost dugaevs]# iptables -P OUTPUT ACCEPT
[root@localhost dugaevs]# EXIT
bash: EXIT: команда не найдена...
[root@localhost dugaevs]# exit
exit
[dugaevs@localhost ~]$ getenforce
bash: getenforce: команда не найдена...
[dugaevs@localhost ~]$ getenforce
Enforcing
[dugaevs@localhost ~]$ 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
[dugaevs@localhost ~]$
```

Рис. 3.1: П. 1 выполнения ЛР и подготовка

2. Обратилась с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедилась, что последний работает: `service httpd status`
3. Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности: пользователь `system_u`, политика ролевого разделения `system_r`, тип `https_t`, уровень доступа `s0`.

Действия пунктов 2-3 предствленны на (рис. -@fig:002):

```
[dugaevas@localhost ~]$ 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: disabled)
   Active: active (running) since Thu 2021-11-25 15:21:43 EST; 1h 23min ago
     Docs: man:httpd.service(8)
  Main PID: 12667 (httpd)
    Status: "Total requests: 3; Idle/Busy workers 100/0;Requests/sec: 0.000598; Bytes served/sec: 0 B/sec"
    Tasks: 214 (limit: 4808)
   Memory: 11.5M
    CGroup: /system.slice/httpd.service
            └─12667 /usr/sbin/httpd -DFOREGROUND
              └─12672 /usr/sbin/httpd -DFOREGROUND
                └─12673 /usr/sbin/httpd -DFOREGROUND
                  └─12674 /usr/sbin/httpd -DFOREGROUND
                    └─12675 /usr/sbin/httpd -DFOREGROUND
                      └─12676 /usr/sbin/httpd -DFOREGROUND
[dugaevas@localhost ~]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0      12667 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      12672 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      12673 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      12674 ?        00:00:01 httpd
system_u:system_r:httpd_t:s0      12675 ?        00:00:01 httpd
system_u:system_r:httpd_t:s0      12676 ?        00:00:01 httpd
[dugaevas@localhost ~]$
```

Рис. 3.2: Статус веб-сервера и политика безопасности

4. Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -b httpd` Многие из них находятся в положении «off». (рис. -@fig:003):

```
12676 /usr/sbin/httpd -brokeokomb
[dugaevas@localhost ~]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0      12667 ?          00:00:00 httpd
system_u:system_r:httpd_t:s0      12672 ?          00:00:00 httpd
system_u:system_r:httpd_t:s0      12673 ?          00:00:00 httpd
system_u:system_r:httpd_t:s0      12674 ?          00:00:01 httpd
system_u:system_r:httpd_t:s0      12675 ?          00:00:01 httpd
system_u:system_r:httpd_t:s0      12676 ?          00:00:01 httpd
[dugaevas@localhost ~]$ sestatus -b httpd
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

Policy booleans:
abrt_anon_write                  off
abrt_handle_event                off
abrt_upload_watch_anon_write     on
antivirus_can_scan_system        off
antivirus_use_jit                off
auditadm_exec_content            on
authlogin_nsswitch_use_ldap      off
authlogin_radius                 off
authlogin_yubikey                off
awstats_purge_apache_log_files  off
boinc_execmem                    on
cdrecord_read_content             off
cluster_can_network_connect      off
cluster_manage_all_files         off
```

Рис. 3.3: Состояние переключателей

5. Посмотрела статистику по политике с помощью команды `seinfo`
6. Определила тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www`:
7. пределю тип файлов, находящихся в директории `/var/www/html` с помощью команды `ls -lZ /var/www/html`.
8. Определяю круг пользователей, которым разрешено создание файлов в директории `/var/www/html`. Создавать файлы можно только суперпользователю, который является владельцем.

Действия пунктов 5-8 представленные на (рис. -@fig:004):



```

[dugaevs@localhost ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          31 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow
Classes:                 132      Permissions:          464
Sensitivities:           1        Categories:           1024
Types:                   4961     Attributes:           255
Users:                   8         Roles:                14
Booleans:                338     Cond. Expr.:         386
Allow:                   112594   Neverallow:           0
Auditallow:              166     Dontaudit:            10358
Type_trans:              252747   Type_change:          87
Type_member:              35      Range_trans:          5781
Role_allow:               38      Role_trans:           421
Constraints:              72      Validatetrans:        0
MLS Constrains:          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:               34
Genfscon:                 107     Portcon:              642
Netifcon:                 0       Nodecon:              0
[dugaevs@localhost ~]$ ls -lZ /vat/www
ls: невозможно получить доступ к '/vat/www': Нет такого файла или каталога
[dugaevs@localhost ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0  6 ноя 11 23:58 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      26 ноя 25 16:22 html
[dugaevs@localhost ~]$ ls -lZ /var/www/html
итого 0
[dugaevs@localhost ~]$ ls -l /var/www/html
итого 0

```

Рис. 3.4: Пункты 5-8

9. Создам от имени суперпользователя html-файл /var/www/html/test.html следующего содержания:  
test
10. Проверю контекст созданного мной файла. По умолчанию вновь созданным файлам в директории /var/www/html присваивается контекст unconfined\_u:object\_r:httpd\_sys\_content\_t:s0

Действия пунктов 9-10 представлены на (рис. -@fig:005):

```
[root@localhost dugaevs]# nano /var/www/html/test.html
[root@localhost dugaevs]# cat /var/www/html/test.html
<html>
    <body>test</body>
</html>
[root@localhost dugaevs]# ls -lZ /var/www/html/test.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 ноя 25 17:11 /var/www/html/test.html
[root@localhost dugaevs]#
```

Рис. 3.5: Пункты 9-10

11. Обратилась к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>.  
Файл был успешно отображён (рис. -@fig:006):

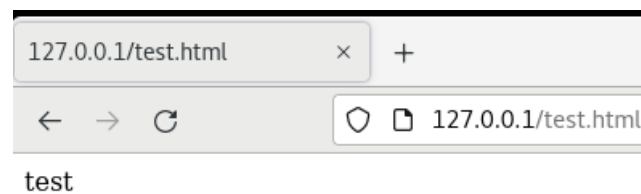


Рис. 3.6: Обращение к файлу через веб-сервер

12. Изучила справку `man httpd_selinux` (рис. -@fig:007):

```
httpd_selinux(8)                                httpd Selinux Policy documentation                                httpd_selinux(8)

НАЗВАНИЕ
  httpd_selinux - Политика Security Enhanced Linux для демона httpd

ОПИСАНИЕ
  Security-Enhanced Linux обеспечивает защиту сервера httpd при помощи гибко настраиваемого мандатного контроля
  доступа.

КОНТЕКСТ ФАЙЛОВ
  SELinux требует наличия у файлов расширенных атрибутов, определяющих тип файла. Политика управляет видом доступа
  демона к этим файлам. Политика SELinux для демона httpd позволяет пользователям настроить web-службы максимально
  безопасным методом с высокой степенью гибкости.

  Для httpd определены следующие контексты файлов:
  httpd_sys_content_t
  - Установите контекст httpd_sys_content_t для содержимого, которое должно быть доступно для всех скриптов httpd и
  для самого демона.
  httpd_sys_script_exec_t
  - Установите контекст httpd_sys_script_exec_t для cgi-скриптов, чтобы разрешить им доступ ко всем sys-типам.
  httpd_sys_script_ro_t
  - Установите на файлы контекст httpd_sys_script_ro_t если вы хотите, чтобы скрипты httpd_sys_script_exec_t могли
  читать данные, и при этом нужно запретить доступ другим не-sys скриптам.
  httpd_sys_script_rw_t
  - Установите на файлы контекст httpd_sys_script_rw_t если вы хотите, чтобы скрипты httpd_sys_script_exec_t могли
  читать и писать данные, и при этом нужно запретить доступ другим не-sys скриптам.
  httpd_sys_script_ra_t
  - Установите на файлы контекст httpd_sys_script_ra_t если вы хотите, чтобы скрипты httpd_sys_script_exec_t могли
  читать и добавлять данные, и при этом нужно запретить доступ другим не-sys скриптам.
  httpd_unconfined_script_exec_t
  - Установите на cgi-скрипты контекст httpd_unconfined_script_exec_t если вы хотите разрешить им исполняться без
  какой-либо защиты SELinux. Такой способ должен использоваться только для скриптов с очень комплексными
  требованиями, и только в случае, если все остальные варианты настройки не дали результата. Лучше использовать
  скрипты с контекстом httpd_unconfined_script_exec_t, чем выключать защиту SELinux для httpd.
```

Рис. 3.7: Справка о контекстах

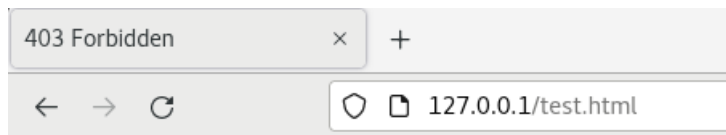
Контекст созданного мной файла: `unconfined_u : object_r : httpd_sys_content_t : s0`, Тип `httpd_sys_content_t` позволяет получить доступ к файлу, если мы обращаемся к нему через браузер.

13. Изменила контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t`: (рис. -@fig:008):

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

Рис. 3.8: Изменение контекста

14. Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html` (рис. -@fig:009):



## Forbidden

You don't have permission to access this resource.

Рис. 3.9: Доступ к файлу через веб-браузер

15. Файл не был отображен из-за того, что несмотря на возможность у любого пользователя просматривать файл, политика SELinux не задает правило, которое разрешало бы доступ, и операция сразу блокируется. Посмотрю log-файлы веб-сервера Apache и системный log файл (рис. -@fig:010):

```
[root@localhost dugaevs]# ls -Z /var/www/html/test.html
unconfined u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@localhost dugaevs]# tail /var/log/httpd/error_log
[Thu Nov 25 15:21:43.710154 2021] [core:notice] [pid 12667:tid 139813255399744] SELinux policy enabled; httpd running as conte
xt system_u:system_r:httpd_t:s0
[Thu Nov 25 15:21:43.713794 2021] [suexec:notice] [pid 12667:tid 139813255399744] AH01232: suEXEC mechanism enabled (wrapper:
/usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using localhost.localdomain. Set the 'S
erverName' directive globally to suppress this message
[Thu Nov 25 15:21:43.752873 2021] [lbmethod_heartbeat:notice] [pid 12667:tid 139813255399744] AH02282: No slotmem from mod_hea
rtmonitor
[Thu Nov 25 15:21:43.757124 2021] [mpm_event:notice] [pid 12667:tid 139813255399744] AH00489: Apache/2.4.37 (centos) OpenSSL/1
.1.1k mod_fcgid/2.3.9 configured -- resuming normal operations
[Thu Nov 25 15:21:43.757151 2021] [core:notice] [pid 12667:tid 139813255399744] AH00094: Command line: '/usr/sbin/httpd -D FOR
EGROUND'
[Thu Nov 25 15:53:49.312643 2021] [core:error] [pid 12676:tid 139812409382656] (13)Permission denied: [client 127.0.0.1:34864]
AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing on a
component of the path
[Thu Nov 25 17:25:46.987092 2021] [core:error] [pid 12675:tid 139812367419136] (13)Permission denied: [client 127.0.0.1:34962]
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@localhost dugaevs]# tail /var/log/messages
Nov 25 17:33:39 localhost org.gnome.Shell.desktop[7757]: libinput error: client bug: timer event4 debounce short: scheduled ex
piry is in the past (~254ms), your system is too slow
Nov 25 17:33:43 localhost gnome-keyring-daemon[7675]: couldn't initialize slot with master password: The password or PIN is in
correct
Nov 25 17:33:43 localhost journal[7757]: Could not delete runtime/persistent state file: Произошла ошибка при удалении файла /
run/user/1000/gnome-shell/runtime-state-LE.:0/screenShield.locked: Нет такого файла или каталога
Nov 25 17:33:44 localhost NetworkManager[1207]: <info> [1637879624.3113] agent-manager: agent[0486686103f9013c,:1.240/org.gno
me.Shell.NetworkAgent/1000]: agent registered
Nov 25 17:34:09 localhost systemd[1]: fprintd.service: Succeeded.
Nov 25 17:36:24 localhost org.gnome.Shell.desktop[7757]: libinput error: event4 - VirtualBox USB Tablet: client bug: event pr
ocessing lagging behind by 12ms, your system is too slow
Nov 25 17:36:27 localhost org.gnome.Shell.desktop[7757]: libinput error: event4 - VirtualBox USB Tablet: client bug: event pr
ocessing lagging behind by 21ms, your system is too slow
Nov 25 17:36:31 localhost org.gnome.Shell.desktop[7757]: libinput error: event4 - VirtualBox USB Tablet: client bug: event pr
ocessing lagging behind by 24ms, your system is too slow
Nov 25 17:36:32 localhost org.gnome.Shell.desktop[7757]: libinput error: event4 - VirtualBox USB Tablet: client bug: event pr
ocessing lagging behind by 20ms, your system is too slow
Nov 25 17:36:32 localhost org.gnome.Shell.desktop[7757]: libinput error: event4 - VirtualBox USB Tablet: WARNING: log rate li
mit exceeded (5 msgs per 60min). Discarding future messages.
```

Рис. 3.10: log-файлы веб-сервера Apache и системный log файл

В системном log файле указано, что моя система слишком медленная, поэтому посмотрю ошибки в файле /var/log/audit/audit.log (рис. -@fig:011):

```
[root@localhost dugaevs]# tail /var/log/audit/audit.log | grep httpd
type=SYSCALL msg=audit(1637879146.985:371): arch=c000003e syscall=4 success=no exit=-13 a0=7f28a403bb70 a1=7f289a7eb890 a2=7f289a7eb890 a3=7f289a7ec4f0 items=0 ppid=12667 pid=12675 auid=4294967295 uid=48 gid=48 euid=48 suid=48 fsuid=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) RCH=x86_64 SYSCALL=stat AUID="unset" UID="apache" GID="apache" EUID="apache" SUID="apache" FSUID="apache" EGID="apache" SGID="apache" FSUID="apache"
type=AVC msg=audit(1637879146.986:372): avc: denied { getattr } for pid=12675 comm="httpd" path="/var/www/html/test.html" dev="dm-0" ino=482457 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:samba_share_t:s0 tclass=file permission=0
type=SYSCALL msg=audit(1637879146.986:372): arch=c000003e syscall=6 success=no exit=-13 a0=7f28a403bc50 a1=7f289a7eb890 a2=7f289a7eb890 a3=1 items=0 ppid=12667 pid=12675 auid=4294967295 uid=48 gid=48 euid=48 suid=48 fsuid=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) RCH=x86_64 SYSCALL=ls stat AUID="unset" UID="apache" GID="apache" EUID="apache" SUID="apache" FSUID="apache" EGID="apache" SGID="apache" FSUID="apache"
```

Рис. 3.11: ошибки в файле audit.log

Сравнить ошибки не получилось из-за ошибки в чтении системного лог файла.

16. Попробовала запустить веб-сервер Apache на прослушивание TCP-порта 81. Для этого в файле /etc/httpd/httpd.conf найду строчку Listen 80 и заменю 80 на 81 (рис. -@fig:012):

```
#
# 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 specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 81
```

Рис. 3.12: Смена порта

17. Выполнила перезапуск веб-сервера Apache. У меня сбоев не произошло. Возможно, это связано с тем, что данный порт зарезервирован и определен. Заменяла 81 на 82. (рис. -@fig:013):

```
[root@localhost dugaevs]# nano /etc/httpd/httpd.conf
[root@localhost dugaevs]# nano /etc/httpd/conf/httpd.conf
[root@localhost dugaevs]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@localhost dugaevs]# nano /etc/httpd/conf/httpd.conf
[root@localhost dugaevs]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
Job for httpd.service failed because the control process exited with error code.
See "systemctl status httpd.service" and "journalctl -xe" for details.
[root@localhost dugaevs]#
```

Рис. 3.13: Перезапуск веб-сервера

Сбой произошел из-за того, что порт 82 не определен.

18. Проанализировала log файлы /var/log/messages (рис. -@fig:014):

```
[root@localhost dugaevs]# tail /var/log/messages
Nov 25 18:11:24 localhost org.gnome.Shell.desktop[7757]: libinput error: client bug: timer event4 debounce: scheduled expiry is in the past (-1ms), your system is too slow
Nov 25 18:11:24 localhost org.gnome.Shell.desktop[7757]: libinput error: client bug: timer event4 debounce short: scheduled expiry is in the past (-17ms), your system is too slow
Nov 25 18:11:56 localhost org.gnome.Shell.desktop[7757]: libinput error: event2 - AT Translated Set 2 keyboard: client bug: event processing lagging behind by 12ms, your system is too slow
Nov 25 18:11:56 localhost dbus-daemon[1018]: [system] Activating via systemd: service name='net.reactivated.Fprint' unit='fprintd.service' requested by ':1.918' (uid=0 pid=54673 comm='su' label='unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023')
Nov 25 18:11:56 localhost systemd[1]: Starting Fingerprint Authentication Daemon...
Nov 25 18:11:56 localhost dbus-daemon[1018]: [system] Successfully activated service 'net.reactivated.Fprint'
Nov 25 18:11:56 localhost systemd[1]: Started Fingerprint Authentication Daemon.
Nov 25 18:11:59 localhost su[54673]: (to root) dugaevs on pts/0
Nov 25 18:12:21 localhost cupsd[1235]: REQUEST localhost - - "POST / HTTP/1.1" 200 187 Renew-Subscription successful-ok
Nov 25 18:12:27 localhost systemd[1]: fprintd.service: Succeeded.
```

Рис. 3.14: log файлы /var/log/messages

Снова ошибка, но я поискала информацию и определила, что подключение оборвалось, поскольку нет доступных сокетов и не получилось подключиться к адресу 0.0.0.82.

Просмотрела файл /var/log/http/error\_log: (рис. -@fig:015):

```
[root@localhost dugaevs]# tail /var/log/httpd/error_log
[Thu Nov 25 17:25:46.987092 2021] [core:error] [pid 12675:tid 139812367419136] (13)Permission denied: [client 127.0.0.1:34962]
AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing on a
component of the path
[Thu Nov 25 18:00:05.914321 2021] [core:error] [pid 12674:tid 139812325553920] (13)Permission denied: [client 127.0.0.1:34976]
AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing on a
component of the path
[Thu Nov 25 18:00:58.848335 2021] [mpm_event:notice] [pid 12667:tid 139813255399744] AH00492: caught SIGWINCH, shutting down g
racefully
[Thu Nov 25 18:01:00.203378 2021] [core:notice] [pid 53915:tid 139793599818048] SELinux policy enabled; httpd running as conte
xt system_u:system_r:httpd_t:s0
[Thu Nov 25 18:01:00.210841 2021] [suexec:notice] [pid 53915:tid 139793599818048] AH01232: suEXEC mechanism enabled (wrapper:
/usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using localhost.localdomain. Set the 'S
erverName' directive globally to suppress this message
[Thu Nov 25 18:01:00.239830 2021] [lbmethod_heartbeat:notice] [pid 53915:tid 139793599818048] AH02282: No slotmem from mod_hea
rtmonitor
[Thu Nov 25 18:01:00.248395 2021] [mpm_event:notice] [pid 53915:tid 139793599818048] AH00489: Apache/2.4.37 (centos) OpenSSL/1
.1.1k mod_fcgid/2.3.9 configured -- resuming normal operations
[Thu Nov 25 18:01:00.248426 2021] [core:notice] [pid 53915:tid 139793599818048] AH00094: Command line: '/usr/sbin/httpd -D FOR
EGROUND'
[Thu Nov 25 18:02:10.543423 2021] [mpm_event:notice] [pid 53915:tid 139793599818048] AH00492: caught SIGWINCH, shutting down g
racefully
```

Рис. 3.15: Файл error\_log

Просмотрю файл /var/log/audit/audit.log: (рис. -@fig:016):

```
[root@localhost dugaevs]# tail /var/log/audit/audit.log
type=PROCTITLE msg=audit(1637881331.710:384): proctitle=2F7573722F7362696E2F6874747064002D44464F524547524F554E44
type=SERVICE_START msg=audit(1637881331.726:385): 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=failed' ID="root" AUID="unset"
type=USER_END msg=audit(1637881745.707:386): pid=51679 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0
-s0:c0.c1023 msg='op=PAM:session close grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_umask,pam_xauth acct="root" exe
="/usr/bin/su" hostname=localhost.localdomain addr=? terminal=pts/0 res=success' ID="dugaevs" AUID="dugaevs"
type=CRED_DISP msg=audit(1637881745.717:387): pid=51679 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0
-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_unix acct="root" exe="/usr/bin/su" hostname=localhost.localdomain addr=? termina
l=pts/0 res=success' ID="dugaevs" AUID="dugaevs"
type=SERVICE_START msg=audit(1637881916.853:388): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init t:s0
msg='unit=fprintd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' ID="root" AUID="uns
et"
type=USER_AUTH msg=audit(1637881919.518:389): pid=54673 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0
-s0:c0.c1023 msg='op=PAM:authentication grantors=pam_unix acct="root" exe="/usr/bin/su" hostname=localhost.localdomain addr=?
terminal=pts/0 res=success' ID="dugaevs" AUID="dugaevs"
type=USER_ACCT msg=audit(1637881919.546:390): pid=54673 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0
-s0:c0.c1023 msg='op=PAM:accounting grantors=pam_unix,pam_localuser acct="root" exe="/usr/bin/su" hostname=localhost.localdom
ain addr=? terminal=pts/0 res=success' ID="dugaevs" AUID="dugaevs"
type=CRED_ACO msg=audit(1637881919.621:391): pid=54673 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0
-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_unix acct="root" exe="/usr/bin/su" hostname=localhost.localdomain addr=? termina
l=pts/0 res=success' ID="dugaevs" AUID="dugaevs"
type=USER_START msg=audit(1637881919.654:392): pid=54673 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0
-s0:c0.c1023 msg='op=PAM:session open grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_umask,pam_xauth acct="root" exe
="/usr/bin/su" hostname=localhost.localdomain addr=? terminal=pts/0 res=success' ID="dugaevs" AUID="dugaevs"
type=SERVICE_STOP msg=audit(1637881947.572:393): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init t:s0 m
sg='unit=fprintd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' ID="root" AUID="unse
t"
```

Рис. 3.16: Файл audit.log

Новых сообщений не появилось.

19. Выполнила команду `semanage port -a -t http_port_t -p tcp 82`: После этого проверила список портов командой `semanage port -l | grep http_port_t`:



20. Попробовала запустить веб-сервер Apache ещё раз. В этот раз запустить сервер получилось, поскольку на предыдущем шаге мы привязали новый порт.
21. Вернула контекст `httpd_sys_content__t` к файлу `/var/www/html/ test.html`:

Действия пунктов 19-21 представлены на (рис. -@fig:017):

```
[root@localhost dugaevas]# semanage port -a -t http_port_t -p tcp 82
[root@localhost dugaevas]# semanage port -l | grep http_port_t
http_port_t          tcp      82, 80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t  tcp      5988
[root@localhost dugaevas]# service httpd restart
bash: service: команда не найдена...
Аналогичная команда: 'systemctl'
[root@localhost dugaevas]# systemctl restart httpd.service
Redirecting to /bin/systemctl restart httpd.service
[root@localhost dugaevas]# chcon -t httpd_sys_content_t /var/www/html/test.html
```

Рис. 3.17: Пункты 19-21

Попробовала получить доступ к файлу `/var/www/html/ test.html` через браузер (рис. -@fig:018):

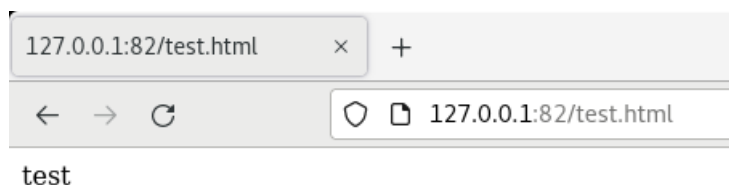


Рис. 3.18: Доступ к файлу через веб-браузер

22. Исправила обратно конфигурационный файл `apache`, вернув `Listen 80` (рис. -@fig:019):



```
#
# 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 specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80
```

Рис. 3.19: Вернула конфиг. файл в первоначальное состояние

23. Удалила привязку http\_port\_t к 82 порту

24. Удалила файл /var/www/html/test.html

Действия пунктов 23-24 представленны на (рис. -@fig:020):

```
[root@localhost dugaevs]# semanage port -a -t http_port_t -p tcp 80
ValueError: Порт tcp/80 уже определен
[root@localhost dugaevs]# semanage port -d -t http_port_t -p tcp 82
[root@localhost dugaevs]# 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@localhost dugaevs]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@localhost dugaevs]#
```

Рис. 3.20: Пункты 23-24

## 4 Выводы

Развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux. Проверила работу SELinx на практике совместно с веб-сервером Apache.