

Лабораторная работа №6. Мандатное разграничение прав в Linux

Евдокимов Иван Андреевич. НФИбд-01-20

13 октября, 2023, Москва, Россия

Российский Университет Дружбы Народов

Цель лабораторной работы

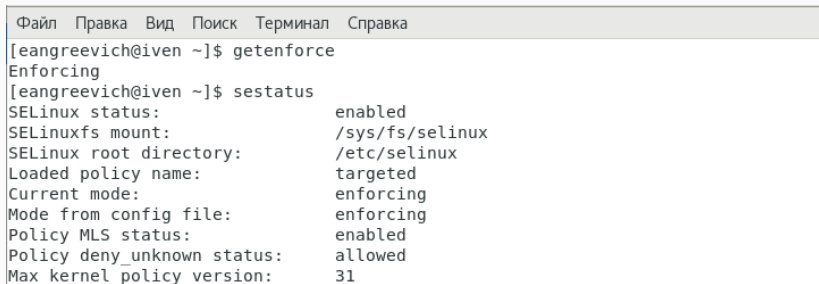
Цель лабораторной работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux на практике совместно с веб-сервером Apache.

Процесс выполнения лабораторной работы

Процесс выполнения лабораторной работы

1. Вошёл в систему с полученными учётными данными и убедился, что SELinux работает в режиме enforcing политики targeted. Обратился с помощью браузера к веб-серверу, запущенному на компьютере, и убедился, что последний работает (рис. 1).



The screenshot shows a terminal window with a menu bar at the top containing 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The terminal text shows the user 'eangreevich@iven' in the home directory. They run the command 'getenforce', which returns 'Enforcing'. Then they run 'sestatus', which displays the following status:

```
[eangreevich@iven ~]$ getenforce
Enforcing
[eangreevich@iven ~]$ 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
Max kernel policy version:     31
```

Рис. 1: Рис. 1

2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: `service httpd status`, запустил его так же, но с параметром `start`. (рис. 2).

```
[eangreevich@iven ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[eangreevich@iven ~]$ 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 prese
t: disabled)
   Active: active (running) since C6 2023-10-14 17:48:10 MSK; 10s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Main PID: 7879 (httpd)
    Status: "Total requests: 0; Current requests/sec: 0; Current traffic:   0 B/s
ec"
    Tasks: 6
   CGroup: /system.slice/httpd.service
           └─7879 /usr/sbin/httpd -DFOREGROUND
             └─7884 /usr/sbin/httpd -DFOREGROUND
               └─7885 /usr/sbin/httpd -DFOREGROUND
                 └─7886 /usr/sbin/httpd -DFOREGROUND
                   └─7887 /usr/sbin/httpd -DFOREGROUND
                     └─7888 /usr/sbin/httpd -DFOREGROUND

окт 14 17:48:10 iven.localdomain systemd[1]: Starting The Apache HTTP Ser....
окт 14 17:48:10 iven.localdomain httpd[7879]: AH00558: httpd: Could not r...e
окт 14 17:48:10 iven.localdomain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
```

3. Нашёл веб-сервер Apache в списке процессов, определил его контекст безопасности, используя команду `auxZ | grep httpd` (рис. 3).

```
[eangreevich@iven ~]$ ps auxZ | grep httpd
system_u:system_r:httd_t:s0 root 7879 0.0 0.1 230444 5216 ? S
s 17:48 0:00 /usr/sbin/httd -DFOREGROUND
system_u:system_r:httd_t:s0 apache 7884 0.0 0.0 232528 3160 ? S
17:48 0:00 /usr/sbin/httd -DFOREGROUND
system_u:system_r:httd_t:s0 apache 7885 0.0 0.0 232528 3160 ? S
17:48 0:00 /usr/sbin/httd -DFOREGROUND
system_u:system_r:httd_t:s0 apache 7886 0.0 0.0 232528 3160 ? S
17:48 0:00 /usr/sbin/httd -DFOREGROUND
system_u:system_r:httd_t:s0 apache 7887 0.0 0.0 232528 3160 ? S
17:48 0:00 /usr/sbin/httd -DFOREGROUND
system_u:system_r:httd_t:s0 apache 7888 0.0 0.0 232528 3160 ? S
17:48 0:00 /usr/sbin/httd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 eangree+ 7973 0.0 0.0 112
832 968 pts/0 S+ 17:50 0:00 grep --color=auto httd
[eangreevich@iven ~]$
```

Рис. 3: Рис. 3

4. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -b | grep httpd` (рис. 4)

```
[eangreevich@iven ~]$ 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_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 on
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
```


5. Посмотрел статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов. (рис. 5).

```
[eangreevich@iven ~]$ seinfo

Statistics for policy file: /sys/fs/selinux/policy
Policy Version & Type: v.31 (binary, mls)

Classes:          130      Permissions:      272
Sensitivities:    1       Categories:      1024
Types:            4793     Attributes:      253
Users:            8       Roles:           14
Booleans:         316     Cond. Expr.:    362
Allow:            107834   Neverallow:      0
Auditallow:       158     Dontaudit:       10022
Type_trans:       18153   Type_change:     74
Type_member:      35      Role_allow:      37
Role_trans:       414     Range_trans:     5899
Constraints:      143     Validatetrans:   0
Initial SIDs:     27      Fs_use:          32
Genfscon:         103     Portcon:         614
Netifcon:         0       Nodecon:         0
Permissives:      0       Polcap:          5

[eangreevich@iven ~]$
```

Рис. 5: Рис. 5

6. Определил тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www` (рис. 6).

```
[eangreevich@iven ~]$ ls -lZ /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[eangreevich@iven ~]$ █
```

Рис. 6: Рис. 6

7. Определил тип файлов, находящихся в директории /var/www/html: `ls -lZ /var/www/html` (рис. 7).



```
[eangreevich@iven ~]$ ls -lZ /var/www/html
```

Рис. 7: Рис. 7

8. Определил круг пользователей, которым разрешено создание файлов в директории /var/www/html. (рис. 8).

```
[eangreevich@iven ~]$ ls -l /var/www/html  
итого 0
```

Рис. 8: Рис. 8

9. Создал от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html (рис. 9).

```
[eangreevich@iven ~]$ su
Пароль:
[root@iven eangreevich]# touch /var/www/html/test.html
[root@iven eangreevich]# vim /var/www/html/test.html
[root@iven eangreevich]# █
```

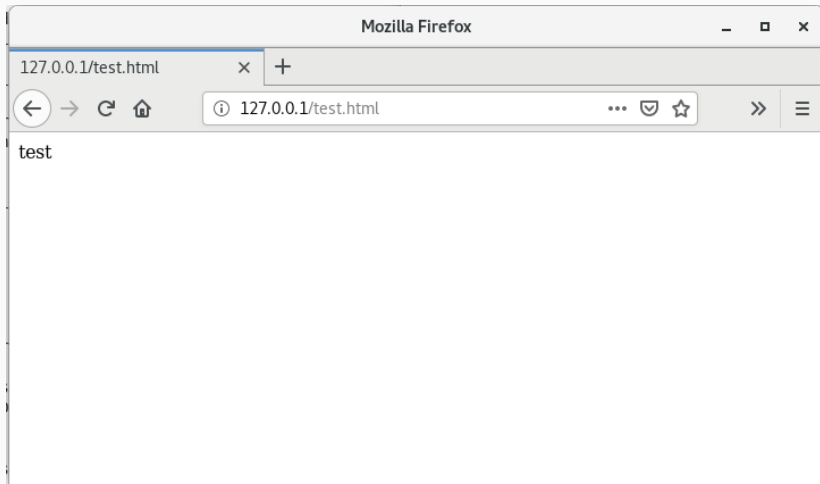
Рис. 9: Рис. 9

10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html. (рис. 10).

```
[root@iven eangreevich]# ls -lZ /var/www/html/test.html  
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html  
/test.html
```

Рис. 10: Рис. 10

11. Обратился к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедился, что файл был успешно отображён. (рис. 11).



12. Изучил справку `man httpd_selinux` и выясните, какие контексты файлов определены для `httpd`. Сопоставил их с типом файла `test.html`. Проверить контекст файла можно командой `ls -Z`. `ls -Z /var/www/html/test.html` (рис. 12).

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

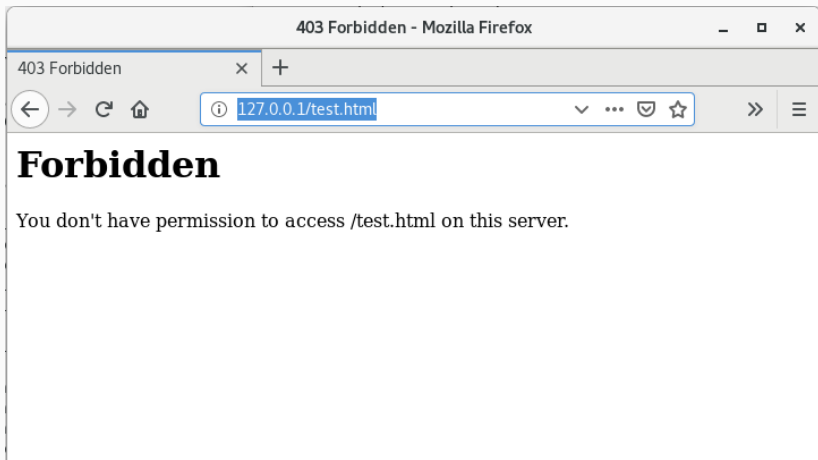
Рис. 12: Рис. 12

13. Изменил контекст файла /var/www/html/test.html
httpd_sys_content_t на любой другой, к которому
процесс httpd не должен иметь доступа, например, на
samba_share_t: chcon -t samba_share_t
/var/www/html/test.html ls -Z /var/www/html/test.html
После этого проверил, что контекст поменялся.(рис. 13).

```
[root@iven eangreevich]# chcon -t samba_share_t /var/www/html/test.html
[root@iven eangreevich]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.
html
[root@iven eangreevich]# █
```

Рис. 13: Рис. 13

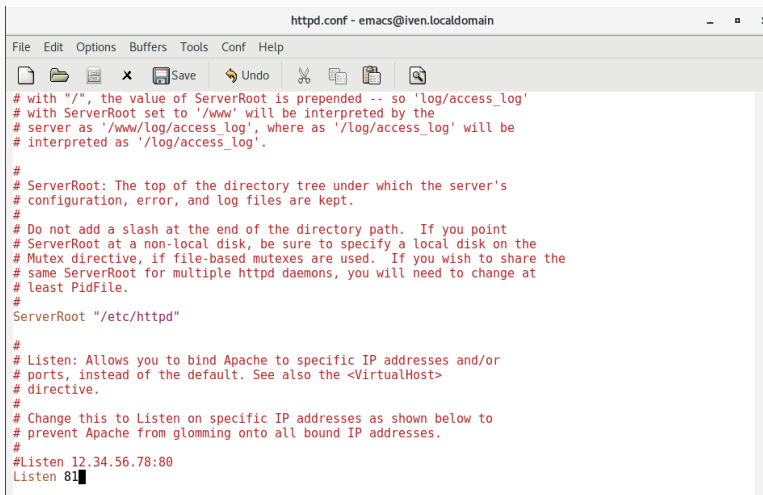
14. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Вы должны получить сообщение об ошибке: `Forbidden You don't have permission to access /test.html on this server.` (рис. 14).



15. Проанализировал ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? ls -l /var/www/html/test.html Просмотрите log-файлы веб-сервера Apache. Также просмотрел системный лог-файл: tail /var/log/messages (рис. 15).

```
[root@iven eangreevich]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 34 окт 14 18:15 /var/www/html/test.html
[root@iven eangreevich]# tail /var/log/messages
Oct 14 18:27:34 iven dbus[716]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
Oct 14 18:27:34 iven dbus[716]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
Oct 14 18:27:34 iven setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Oct 14 18:27:34 iven setroubleshoot: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 10d33aa6-c06b-4157-b383-dd59f6918588
Oct 14 18:27:34 iven python: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (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.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions to access a parent directory in which case try to change the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confidence) suggests *****#012#012If you want to treat test.html as public content#012Then you need to change the label on test.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.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# semodule -i my-httpd.pp#012
Oct 14 18:27:46 iven dbus[716]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
Oct 14 18:27:46 iven dbus[716]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
Oct 14 18:27:46 iven setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Oct 14 18:27:46 iven setroubleshoot: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 10d33aa6-c06b-4157-b383-dd59f6918588
Oct 14 18:27:46 iven python: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (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.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions to access a parent directory in which case try to change the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confidence) suggests *****#012#012If you want to treat test.html as public content#012Then you need to change the label on test.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.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# semodule -i my-httpd.pp#012
```

16. Попробовал запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf найдите строчку Listen 80 и замените её на Listen 81. (рис. 16).



```
# with "/", the value of ServerRoot is prepended -- so 'log/access_log'
# with ServerRoot set to '/www' will be interpreted by the
# server as '/www/log/access_log', where as '/log/access_log' will be
# interpreted as '/log/access_log'.

#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path. If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used. If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
ServerRoot "/etc/httpd"

#
# 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
```

17. Выполните перезапуск веб-сервера Apache. Произошёл сбой (рис. 17).

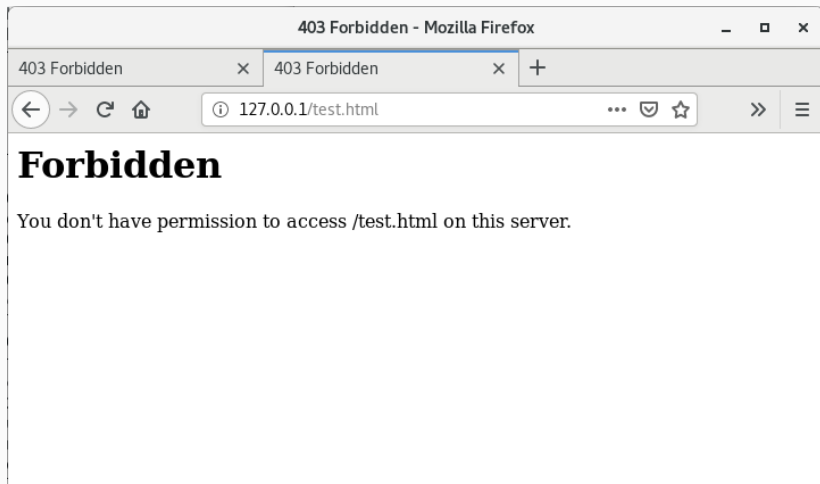


Рис. 17: Рис. 17

18. Проанализировал лог-файлы: tail -nl /var/log/messages Просмотрел файлы /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log и выяснил, в каких файлах появились записи (рис. 18).

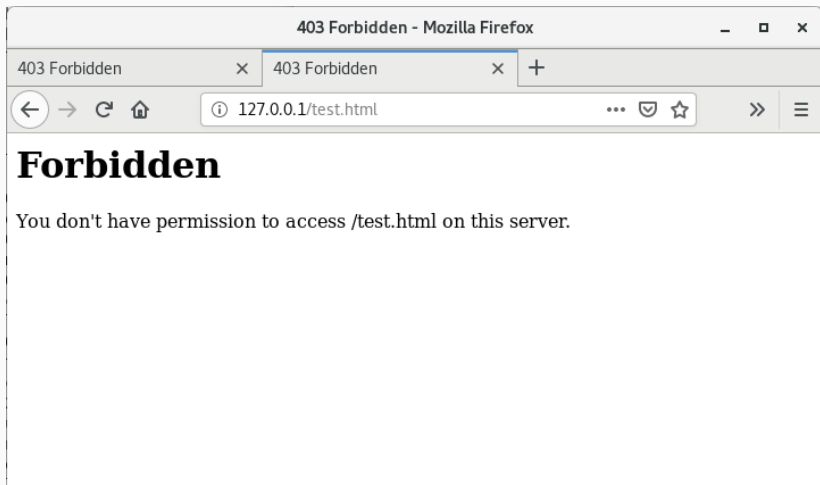
```
[root@iven eangreevich]# tail -nl /var/log/messages
Oct 14 18:39:57 iven dbus[716]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
Oct 14 18:39:57 iven setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Oct 14 18:39:57 iven setroubleshoot: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 10d33aa6-c06b-4157-b383-dd59f6918588
Oct 14 18:39:57 iven python: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (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.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions to access a parent directory in which case try to change the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confidence) suggests *****#012#012If you want to treat test.html as public content#012Then you need to change the label on test.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.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.pp#012
Oct 14 18:40:01 iven systemd: Created slice User Slice of root.
Oct 14 18:40:01 iven systemd: Started Session 50 of user root.
Oct 14 18:40:01 iven systemd: Removed slice User Slice of root.
Oct 14 18:40:01 iven setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Oct 14 18:40:01 iven setroubleshoot: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 10d33aa6-c06b-4157-b383-dd59f6918588
Oct 14 18:40:01 iven python: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (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.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions to access a parent directory in which case try to change the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confidence) suggests *****#012#012If you want to treat test.html as public content#012Then you need to change
```

19. Выполнил команду `semanage port -a -t http_port_t -p tcp 81` После этого проверил список портов командой `semanage port -l | grep http_port_t` Убедился, что порт 81 появился в списке(рис. 19).

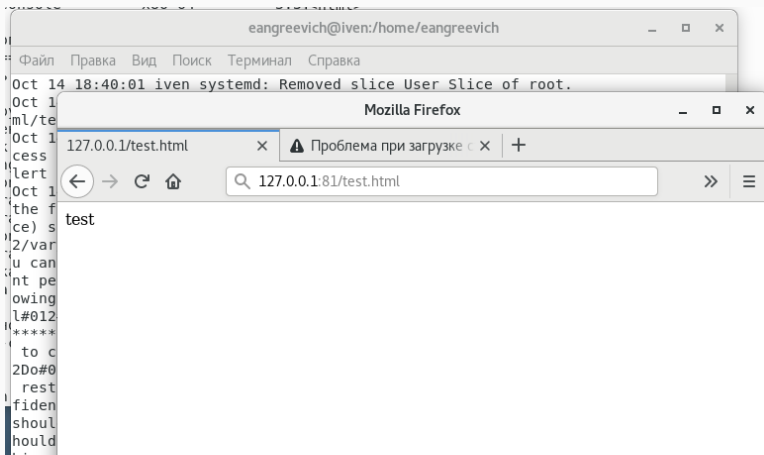
```
[root@iven eangreevich]# semanage port -a -t http_port -p tcp81
port option is needed for add
[root@iven eangreevich]# semanage port -l | grep https_port_t
pegasus_https_port_t      tcp      5989
[root@iven eangreevich]#
```

Рис. 19: Рис. 19

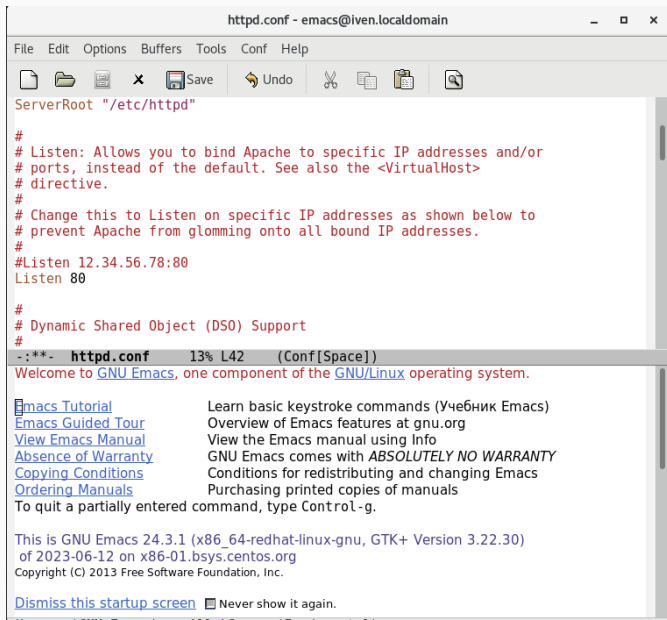
20. Пробую запустить веб-сервер Apache ещё раз (рис. 20).



21. Вернул контекст `httpd_sys_content_t` к файлу `/var/www/html/ test.html`: `chcon -t httpd_sys_content_t /var/www/html/test.html` После этого попробовал получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. Увидеть содержимое файла — слово «test»(рис. 21).



22. . Исправил обратно конфигурационный файл apache, вернув Listen 80 (рис. 22).



```
httpd.conf - emacs@iven.localdomain
File Edit Options Buffers Tools Conf Help
ServerRoot "/etc/httpd"
#
# 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
#
# Dynamic Shared Object (DSO) Support
#
-:***- httpd.conf 13% L42 (Conf[Space])
Welcome to GNU Emacs, one component of the GNU/Linux operating system.
Emacs Tutorial Learn basic keystroke commands (Учебник Emacs)
Emacs Guided Tour Overview of Emacs features at gnu.org
View Emacs Manual View the Emacs manual using Info
Absence of Warranty GNU Emacs comes with ABSOLUTELY NO WARRANTY
Copying Conditions Conditions for redistributing and changing Emacs
Ordering Manuals Purchasing printed copies of manuals
To quit a partially entered command, type Control-g.
This is GNU Emacs 24.3.1 (x86_64-redhat-linux-gnu, GTK+ Version 3.22.30)
of 2023-06-12 on x86-01.bsys.centos.org
Copyright (C) 2013 Free Software Foundation, Inc.
Dismiss this startup screen ☐ Never show it again.
```

23. Удалил привязку http_port_t к 81 порту: semanage port -d -t http_port_t -p tcp 81 и проверил, что порт 81 удалён, затем удалил файл /var/www/html/test.html: rm /var/www/html/test.html

```
[root@iven eangreevich]# semanage port -d -t http_port_t -p tcp81
port option is needed for delete
[root@iven eangreevich]# rm /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»? y
[root@iven eangreevich]#
```


Выводы:

Выводы:

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinux на практике совместно с веб-сервером Apache.