

# **Лабораторная работа №6. Мандатное разграничение прав в Linux**

**дисциплина: Информационная безопасность**

Рыбалко Элина Павловна

# Содержание

Цель работы	5
Техническое обеспечение	6
Объект/Предмет исследования	7
Теоретическое введение	8
Выполнение лабораторной работы	9
Вывод	20
Список литературы	21

# Список иллюстраций

1	Проверка SELinux . . . . .	9
2	Проверка веб-сервера . . . . .	10
3	Контекст безопасности . . . . .	10
4	Состояние переключателей . . . . .	11
5	Создание файла . . . . .	12
6	Просмотр файла через браузер . . . . .	12
7	Статистика по политике, типы файлов, просмотр и изменение кон- текста . . . . .	13
8	Попытка просмотра файла через браузер . . . . .	13
9	Просмотр log-файлов . . . . .	14
10	Просмотр log-файлов . . . . .	14
11	Изменение порта . . . . .	15
12	Изменение порта . . . . .	15
13	Перезапуск сервера . . . . .	16
14	Попытка просмотра файла через браузер . . . . .	16
15	Просмотр log-файлов . . . . .	17
16	Просмотр log-файлов . . . . .	17
17	Просмотр log-файлов . . . . .	18
18	Добавление порта, перезапуск сервера и изменение контекста . .	18
19	Просмотр файла через 81 порт . . . . .	19
20	Изменение файла . . . . .	19
21	Удаление привязки и файла . . . . .	19

## **Список таблиц**

## Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux<sup>1</sup>. Проверить работу SELinx на практике совместно с веб-сервером Apache.

# Техническое обеспечение

Лабораторная работа подразумевает наличие на виртуальной машине VirtualBox операционной системы Linux (дистрибутив Rocky или CentOS). Выполнение работы возможно как в дисплейном классе факультета физико-математических и естественных наук РУДН, так и дома. Описание выполнения работы приведено для дисплейного класса со следующими характеристиками: – Intel Core i3-550 3.2 GHz, 4 GB оперативной памяти, 20 GB свободного места на жёстком диске; – ОС Linux Gentoo (<http://www.gentoo.ru/>); – VirtualBox верс. 6.1 или старше; – каталог с образами ОС для работающих в дисплейном классе: [/afs/dk.sci.pfu.edu.ru/common/files/iso/](http://afs.dk.sci.pfu.edu.ru/common/files/iso/).

# **Объект/Предмет исследования**

Операционная система Linux и мандатное разграничение прав.

# Теоретическое введение

В Linux дискреционные механизмы разграничения доступа (DAC, discretionary access control) являются основными и всегда активны. Их использование предполагает, что владельцы объектов правильно распоряжаются правами доступа к находящимся в их владении объектам. [[2]] (#список-литературы).



# Выполнение лабораторной работы

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus` (см. рис. -@fig:001).

```
[eprybalko@eprybalko ~]$ getenforce
Enforcing
[eprybalko@eprybalko ~]$ 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
[eprybalko@eprybalko ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
Unit httpd.service could not be found.
```

Рис. 1: Проверка SELinux

2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает (см. рис. -@fig:002).

```
[eprybalko@eprybalko ~]$ 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: inactive (dead)
     Docs: man:httpd(8)
          man:apachectl(8)
[eprybalko@eprybalko ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[eprybalko@eprybalko ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
Failed to start httpd.service: Access denied
See system logs and 'systemctl status httpd.service' for details.
[eprybalko@eprybalko ~]$ 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 Чт 2022-10-13 15:15:04 MSK; 7s ago
     Docs: man:httpd(8)
          man:apachectl(8)
  Main PID: 3431 (httpd)
    Status: "Processing requests..."
```

Рис. 2: Проверка веб-сервера

3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду (см. рис. -@fig:003).

```
[eprybalko@eprybalko ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 3431 0.2 1.2 314768 12192 ? S
s 15:15 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3439 0.0 0.6 316988 6428 ? S
15:15 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3440 0.0 0.6 316988 6428 ? S
15:15 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3441 0.0 0.6 316988 6428 ? S
15:15 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3442 0.0 0.6 316988 6428 ? S
15:15 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3443 0.0 0.6 316988 6428 ? S
15:15 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 eprybal+ 3528 0.0 0.0 112
832 972 pts/0 S+ 15:16 0:00 grep --color=auto httpd
```

Рис. 3: Контекст безопасности

4. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды (см. рис. -@fig:004).

```
[eprybalko@eprybalko ~]$ sestatus -b grep 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
Max kernel policy version:     31

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
```

Рис. 4: Состояние переключателей

5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов. (см. рис. -@fig:005).
6. Определите тип файлов и поддиректорий, находящихся в директории `/var/www` (см. рис. -@fig:004 и рис. -@fig:005).
7. Определите тип файлов, находящихся в директории `/var/www/html` (см. рис. -@fig:005).
8. Определите круг пользователей, которым разрешено создание файлов в директории `/var/www/html`. (см. рис. -@fig:005).
9. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) `html`-файл (см. рис. -@fig:006).

```
епрыbalko@епрыbalko:/home/епрыbalko
Файл  Правка  Вид  Поиск  Терминал  Справка
<html>
<body>test</body>
</html>
~
~
```

Рис. 5: Создание файла

10. Проверьте контекст созданного вами файла (см. рис. -@fig:005).
11. Обратитесь к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html” (см. рис. -@fig:007).

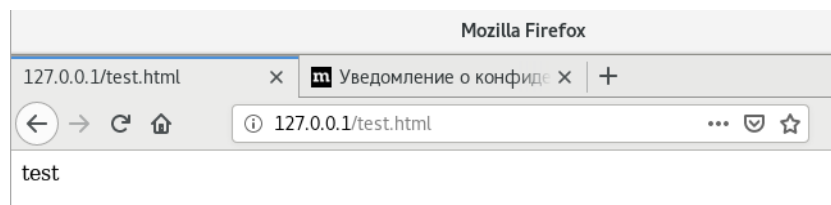


Рис. 6: Просмотр файла через браузер

12. Изучите справку man httpd\_selinux.
13. Измените контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на любой другой, к которому процесс httpd не должен иметь доступа, например, на samba\_share\_t (см. рис. -@fig:005).

```
[eprybalko@eprybalko ~]$ 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

[eprybalko@eprybalko ~]$ 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
[eprybalko@eprybalko ~]$ ls -lZ /var/www/html
[eprybalko@eprybalko ~]$ su
Пароль:
[root@eprybalko eprybalko]# vim /var/www/html/test.html
[root@eprybalko eprybalko]# ls -lZ /var/www/html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
[root@eprybalko eprybalko]# chcon -t samba_share_t /var/www/html/test.html
[root@eprybalko eprybalko]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.
```

Рис. 7: Статистика по политике, типы файлов, просмотр и изменение контекста

14. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html> (см. рис. -@fig:008).

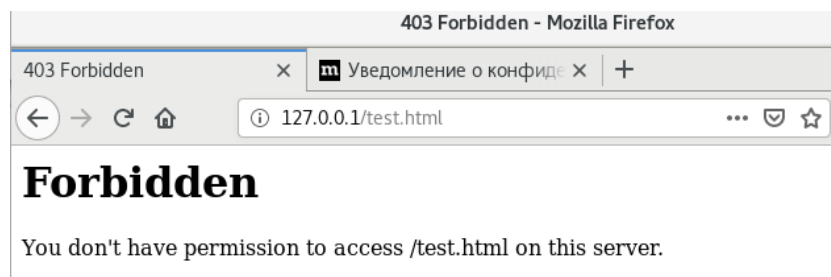


Рис. 8: Попытка просмотра файла через браузер

15. Проанализируйте ситуацию. Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл (см. рис. -@fig:009, -@fig:010).

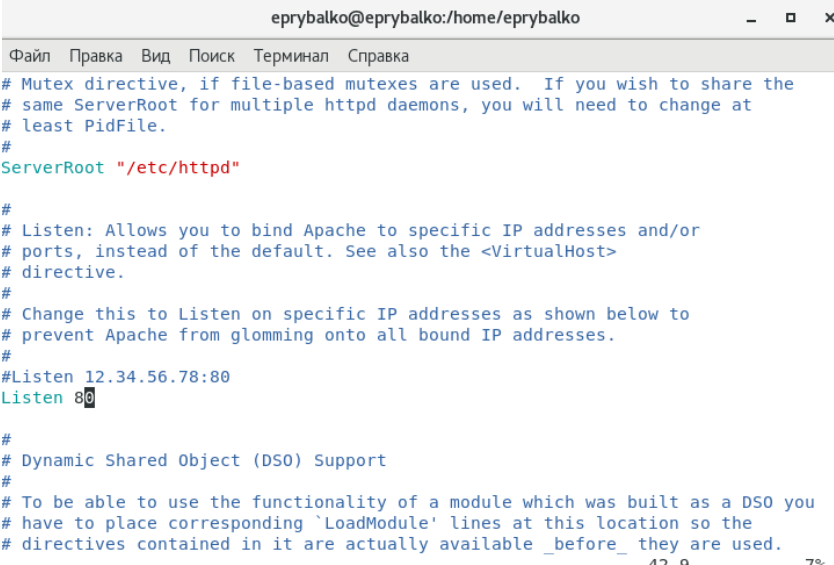
```
[root@eprybalko epryalko]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 34 окт 13 15:26 /var/www/html/test.html
[root@eprybalko epryalko]# tail /var/log/messages
Oct 13 15:36:41 epryalko journal: clutter_actor_iter_next: assertion 'ri->age == ri->root->priv->age' failed
Oct 13 15:37:07 epryalko dbus[674]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
Oct 13 15:37:14 epryalko dbus[674]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
Oct 13 15:37:16 epryalko setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Oct 13 15:37:18 epryalko setroubleshoot: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run:
sealert -l be020a1a-e8a4-4728-9f16-4f198d6b7fed
Oct 13 15:37:18 epryalko python: SELinux is preventing /usr/sbin/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 13 15:37:25 epryalko setroubleshoot: failed to retrieve rpm info for /var/www/html
```

Рис. 9: Просмотр log-файлов

```
[root@eprybalko epryalko]# tail /var/log/audit/audit.log
type=AVC msg=audit(1665664624.563:297): avc: denied { getattr } for pid=3439 comm="httpd" path="/var/www/html/test.html" dev="dm-0" ino=52065274 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(1665664624.563:297): arch=c000003e syscall=6 success=no exit=-13 a0=561b67bee120 a1=7fff436ee670 a2=7fff436ee670 a3=0 items=0 ppid=3431 pid=3439 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)
type=PROCTITLE msg=audit(1665664624.563:297): proctitle=2F7573722F7362696E2F6874747064002D44464F524547524F554E44
type=USER ACCT msg=audit(1665664802.415:298): pid=4989 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:cron_t:s0-s0:c0.c1023 msg='op=PAM:accounting grantors=pam_access,pam_unix,pam_localuser acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=CRED ACQ msg=audit(1665664802.424:299): pid=4989 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:cron_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=LOGIN msg=audit(1665664802.439:300): pid=4989 uid=0 subj=system_u:system_r:cron_t:s0-s0:c0.c1023 old-auid=4294967295 auid=0 tty=(none) old-ses=4294967295 ses=7 res=1
type=USER_START msg=audit(1665664802.731:301): pid=4989 uid=0 auid=0 ses=7 subj=system_u:system_r:cron_t:s0-s0:c0.c1023 msg='op=PAM:session_open grantors=pam_loginuid,pam_keyinit,pam_limits,pam_systemd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=CRED_REFR msg=audit(1665664802.838:302): pid=4989 uid=0 auid=0 ses=7 subj=system_u:system_r:cron_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd a
```

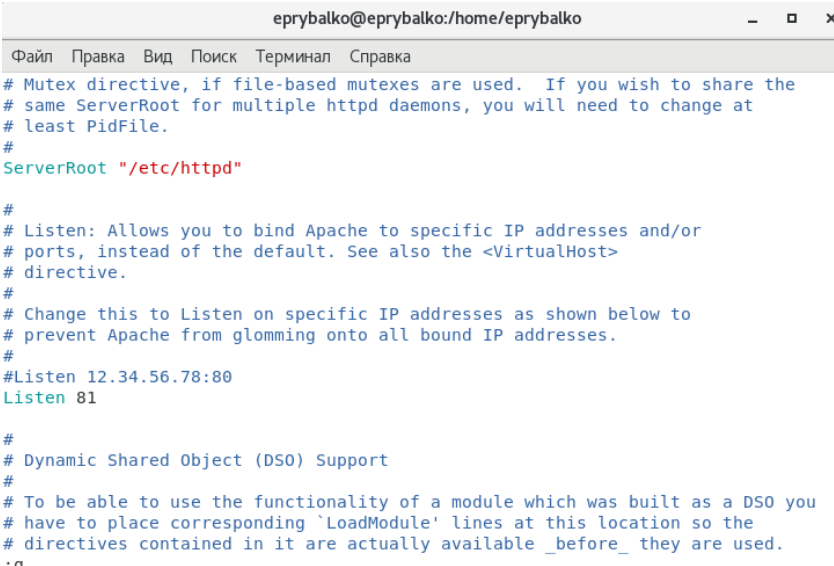
Рис. 10: Просмотр log-файлов

16. Попробуйте запустить веб-сервер Apache на прослушивание TCP-порта 81 (см. рис. -@fig:011 и -@fig:012).



```
eprybalko@eprybalko:/home/eprybalko
Файл Правка Вид Поиск Терминал Справка
# 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 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.
```

Рис. 11: Изменение порта



```
eprybalko@eprybalko:/home/eprybalko
Файл Правка Вид Поиск Терминал Справка
# 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
#
# 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.
```

Рис. 12: Изменение порта

17. Выполните перезапуск веб-сервера Apache. (см. рис. -@fig:013 и -@fig:014).

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

Рис. 13: Перезапуск сервера

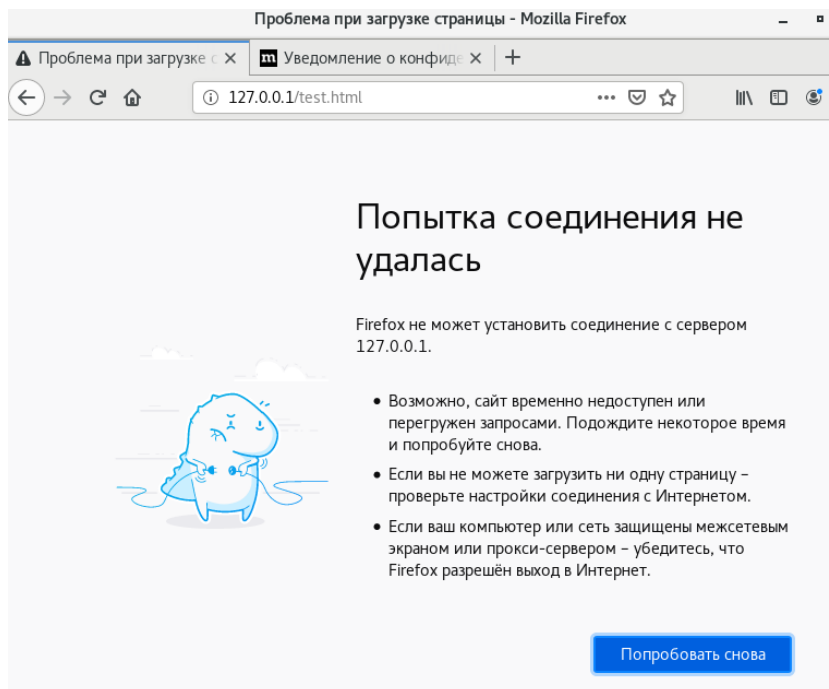


Рис. 14: Попытка просмотра файла через браузер

18. Проанализируйте лог-файлы (см. рис. -@fig:015, -@fig:016 и -@fig:017).



```
[root@eprybalko epryalko]# tail -10l /var/log/messages
Oct 13 15:57:39 epryalko setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Oct 13 15:57:39 epryalko setroubleshoot: SELinux is preventing /usr/sbin/httpd from
getattr access on the file /var/www/html/test.html. For complete SELinux messages run
: sealert -l be020a1a-e8a4-4728-9f16-4f198d6b7fed
Oct 13 15:57:39 epryalko python: SELinux is preventing /usr/sbin/httpd from getattr
access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (92.2 con
fidence) suggests *****#012#012If you want to fix the label. #01
2/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 permis
sions to access a parent directory in which case try to change the following command a
ccordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plug
in public_content (7.83 confidence) suggests *****#012#012If you wan
t to treat test.html as public content#012Then you need to change the label on test.h
tml to public_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t pu
blic_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.p
p#012
Oct 13 15:58:17 epryalko systemd: Stopping The Apache HTTP Server...
Oct 13 15:58:19 epryalko systemd: Stopped The Apache HTTP Server.
Oct 13 15:58:19 epryalko systemd: Starting The Apache HTTP Server...
Oct 13 15:58:19 epryalko httpd: AH00558: httpd: Could not reliably determine the ser
ver's fully qualified domain name, using fe80::63ec:426f:e3b7:640d. Set the 'ServerNa
me' directive globally to suppress this message
Oct 13 15:58:20 epryalko systemd: Started The Apache HTTP Server.
```

Рис. 15: Просмотр log-файлов

```
[root@eprybalko epryalko]# tail -10l /var/log/audit/audit.log
type=CRED_REFR msg=audit(1665666002.705:336): pid=5615 uid=0 auid=0 ses=9 subj=system
_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd a
cct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=CRED_DISP msg=audit(1665666002.762:337): pid=5615 uid=0 auid=0 ses=9 subj=system
_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd a
cct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=USER_END msg=audit(1665666002.768:338): pid=5615 uid=0 auid=0 ses=9 subj=system
_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_close grantors=pam_loginuid,pam
_keyinit,pam_limits,pam_systemd acct="root" exe="/usr/sbin/crond" hostname=? addr=? t
erminal=cron res=success'
type=USER_ACCT msg=audit(1665666001.810:339): pid=5648 uid=0 auid=4294967295 ses=4294
967295 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:accounting grantors=
pam_access,pam_unix,pam_localuser acct="root" exe="/usr/sbin/crond" hostname=? addr=?
terminal=cron res=success'
type=CRED_ACQ msg=audit(1665666001.810:340): pid=5648 uid=0 auid=4294967295 ses=42949
67295 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam
_env,pam_fprintd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res
=success'
type=LOGIN msg=audit(1665666001.814:341): pid=5648 uid=0 subj=system_u:system_r:crond
_t:s0-s0:c0.c1023 old-auid=4294967295 auid=0 tty=(none) old-ses=4294967295 ses=10 res
=1
type=USER_START msg=audit(1665666001.857:342): pid=5648 uid=0 auid=0 ses=10 subj=syst
em_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_open grantors=pam_loginuid,p
am_keyinit,pam_limits,pam_systemd acct="root" exe="/usr/sbin/crond" hostname=? addr=?
terminal=cron res=success'
type=CRED_REFR msg=audit(1665666001.858:343): pid=5648 uid=0 auid=0 ses=10 subj=syste
m_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd
acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=CRED_DISP msg=audit(1665666002.091:344): pid=5648 uid=0 auid=0 ses=10 subj=syste
```

Рис. 16: Просмотр log-файлов

```
[root@eprybalko epryalko]# tail -10l /var/log/httpd/access_log
127.0.0.1 - - [13/Oct/2022:15:33:11 +0300] "GET /test.html HTTP/1.1" 200 34 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
127.0.0.1 - - [13/Oct/2022:15:33:14 +0300] "GET /favicon.ico HTTP/1.1" 404 209 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
127.0.0.1 - - [13/Oct/2022:15:36:12 +0300] "GET /test.html HTTP/1.1" 403 211 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
127.0.0.1 - - [13/Oct/2022:15:36:12 +0300] "GET /favicon.ico HTTP/1.1" 404 209 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
127.0.0.1 - - [13/Oct/2022:15:37:04 +0300] "GET /test.html HTTP/1.1" 403 211 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
127.0.0.1 - - [13/Oct/2022:15:37:04 +0300] "GET /favicon.ico HTTP/1.1" 404 209 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
127.0.0.1 - - [13/Oct/2022:15:57:30 +0300] "GET /test.html HTTP/1.1" 403 211 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
[root@eprybalko epryalko]# tail -10l /var/log/httpd/error_log
[Thu Oct 13 15:36:12.571826 2022] [core:error] [pid 3442] (13)Permission denied: [client 127.0.0.1:59088] 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 Oct 13 15:37:04.565021 2022] [core:error] [pid 3439] (13)Permission denied: [client 127.0.0.1:59092] 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 Oct 13 15:57:30.572314 2022] [core:error] [pid 3443] (13)Permission denied: [client 127.0.0.1:59122] 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 Oct 13 15:58:18.059413 2022] [mpm_prefork:notice] [pid 3431] AH00170: caught SIGWINCH, shutting down gracefully
[Thu Oct 13 15:58:19.780812 2022] [core:notice] [pid 5517] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Thu Oct 13 15:58:19.823757 2022] [suexec:notice] [pid 5517] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
```

Рис. 17: Просмотр log-файлов

19. Выполните команду `semanage port -a -t http_port_t -p tcp 81`. После этого проверьте список портов командой (см. рис. -@fig:018).
20. Попробуйте запустить веб-сервер Apache ещё раз (см. рис. -@fig:018).
21. Верните контекст `httpd_sys_content_t` к файлу `/var/www/html/ test.html`. После этого попробуйте получить доступ к файлу. После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html` (см. рис. -@fig:018 и -@fig:019).

```
[root@eprybalko epryalko]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@eprybalko epryalko]# 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@eprybalko epryalko]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@eprybalko epryalko]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@eprybalko epryalko]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@eprybalko epryalko]# service httpd start
Redirecting to /bin/systemctl start httpd.service
```

Рис. 18: Добавление порта, перезапуск сервера и изменение контекста

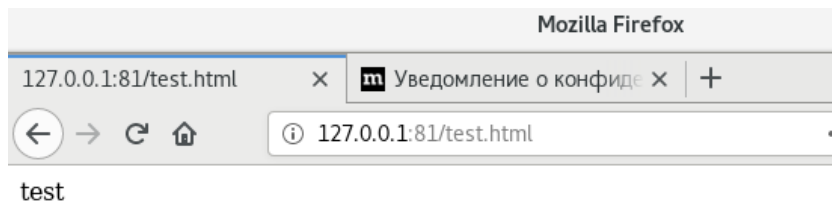


Рис. 19: Просмотр файла через 81 порт

22. Исправьте обратно конфигурационный файл apache, вернув Listen 80 (см. рис. -@fig:020).

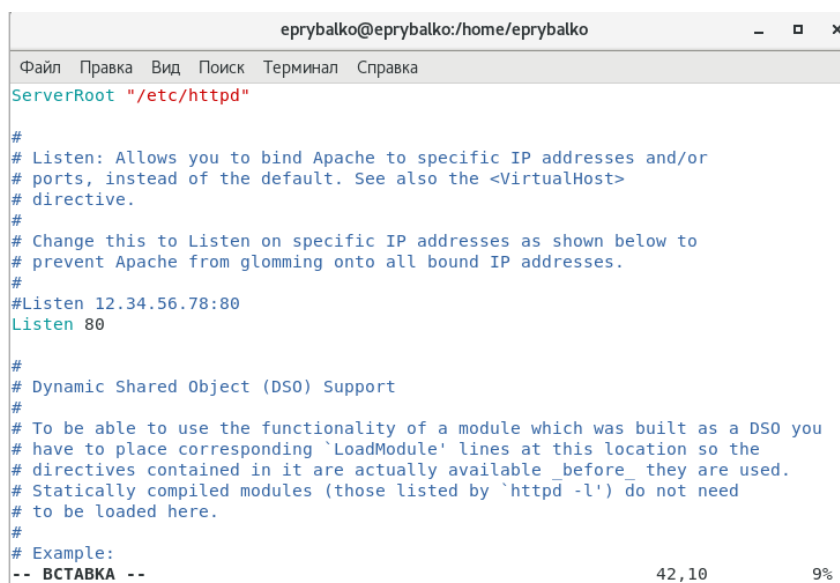


Рис. 20: Изменение файла

23. Удалите привязку http\_port\_t к 81 порту (см. рис. -@fig:021).
24. Удалите файл /var/www/html/test.html (см. рис. -@fig:021).

```
[root@eprybalko eptrybalko]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@eprybalko eptrybalko]# rm /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»? y
```

Рис. 21: Удаление привязки и файла

## **Вывод**

Развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux. Проверили работу SELinx на практике совместно с веб-сервером Apache.

# Список литературы

1. Лабораторная работа №6
2. Мандатное (принудительное) разграничение доступа Linux
3. Руководство по формуле Cmd Markdown
4. Руководство по оформлению Markdown файлов