

Отчёт по лабораторной работе №6

Дисциплина: Информационная безопасность

Выполнил: Танрибергенов Эльдар

Содержание

1	Цель работы	5
2	Задания	6
3	Указания к работе	7
4	Выполнение работы	10
5	Выводы	23

Список иллюстраций

3.1	Статус SELinux	8
3.2	Установка веб-сервера Apache	8
3.3	Установка параметра в конф. файле веб-сервера Apache	8
3.4	Отключение пакетного фильтра и разрешение подключения к портам 80 и 81 портам протокола tcp	9
4.1	Проверка того, что SELinux работает в режиме enforcing политики targeted	10
4.2	Проверка статуса веб-сервера	10
4.3	Запуск веб-сервера	11
4.4	Процесс веб-сервера Apache в списке процессов	11
4.5	Просмотр состояния переключателей SELinux для Apache	12
4.6	Статистика по политике	12
4.7	Просмотр типов файлов и поддиректорий	13
4.8	Просмотр типов файлов, находящихся в директории /var/www/html	13
4.9	Просмотр атрибутов директории для определения круга пользователей, которым разрешено создание файлов в директории	13
4.10	Содержимое HTML-файла test-etanribergenov	13
4.11	Проверка контекста безопасности созданного файла	14
4.12	Обращение к файлу через веб-сервер в браузере	14
4.13	Информация о контекстах безопасности SELinux файлов определённых для httpd	15
4.14	Сопоставление типа файла с типами, описанными в справке	15
4.15	Изменение контекста SELinux для файла	16
4.16	Попытка получения доступа к файлу через веб-сервер в браузере	16
4.17	Сообщения в системном лог-файле	17
4.18	Сообщения в лог-файле процесса audtd	17
4.19	Изменение порта прослушивания веб-сервера Apache	18
4.20	Выполнение перезапуска веб-сервера	18
4.21	Просмотр системного лог-файла	18
4.22	Просмотр лог-файла access_log	19
4.23	Просмотр лог-файла error_log	19
4.24	Добавление tcp-порта 81 в список портов SELinux для веб-сервера	20
4.25	Просмотр списка портов SELinux для веб-сервера	20
4.26	Перезапуск веб-сервера Apache	20
4.27	Возвращение контекста SELinux к файлу	20
4.28	Получение доступа к файлу через веб-сервер в браузере	21

4.29 Изменение конф. файла веб-сервера Apache	21
4.30 Удаление привязки http_port_t к 81 порту и проверка выполнения действий	21
4.31 Удаление файла	22

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 Задания

- Выполнить указания к работе
- Проверить работу *SELinux* на практике совместно с веб-сервером *Apache*

3 Указания к работе

Организация и описание лабораторного стенда. Для проведения указанной лабораторной работы на одно рабочее место требуется компьютер с установленной операционной системой *Linux*, поддерживающей технологию *SELinux*. Предполагается использовать стандартный дистрибутив *Linux CentOS* с включённой политикой *SELinux targeted* и режимом *enforcing*. Для выполнения заданий требуется наличие учётной записи администратора (*root*) и учётной записи обычного пользователя. Постоянно работать от учётной записи *root* неправильно с точки зрения безопасности. Подготовка лабораторного стенда и методические рекомендации. При подготовке стенда обратите внимание, что необходимая для работы и указанная выше политика *targeted* и режим *enforcing* используются в данном дистрибутиве по умолчанию, т.е. каких-то специальных настроек не требуется. При этом следует убедиться, что политика и режим включены, особенно когда работа будет проводиться повторно и велика вероятность изменений при предыдущем использовании системы. При необходимости администратор должен разбираться в работе *SELinux* и уметь как исправить конфигурационный файл */etc/selinux/config*, так и проверить используемый режим и политику. Необходимо, чтобы был установлен веб-сервер *Apache*.

```
etanribergenov@etanribergenov:~  
File Edit View Search Terminal Help  
[etanribergenov@etanribergenov ~]$ 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  
[etanribergenov@etanribergenov ~]$  
[etanribergenov@etanribergenov ~]$
```

Рис. 3.1: Статус SELinux

```
etanribergenov@etanribergenov:~  
File Edit View Search Terminal Help  
[etanribergenov@etanribergenov ~]$ sudo yum install -y httpd  
[sudo] password for etanribergenov:  
Last metadata expiration check: 1:02:49 ago on Sat 16 Nov 2024 09:27:23 AM +05.  
Dependencies resolved.  
=====
```

Package	Architecture	Version
	Repository	Size
Installing:		
httpd	x86_64	2.4.37-65.module+el8.10.0+

```
=====
```

Рис. 3.2: Установка веб-сервера Apache

В конфигурационном файле */etc/httpd/conf/httpd.conf* необходимо задать параметр *ServerName*:

`ServerName test.ru`

```
Open [icon] httpd.conf  
/etc/httpd/conf  
#  
# ServerName gives the name and port that the server uses to identify itself.  
# This can often be determined automatically, but we recommend you specify  
# it explicitly to prevent problems during startup.  
#  
# If your host doesn't have a registered DNS name, enter its IP address here.  
#  
#ServerName www.example.com:80  
ServerName test-etanribergenov.ru
```

Рис. 3.3: Установка параметра в конф. файле веб-сервера Apache

чтобы при запуске веб-сервера не выдавались лишние сообщения об ошибках, не относящихся к лабораторной работе. Также необходимо проследить, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp. Отключить фильтр можно командами

```
iptables -F
```

```
iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT
```

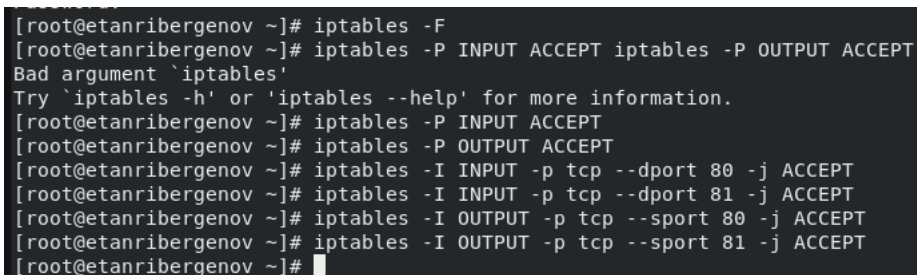
либо добавить разрешающие правила:

```
iptables -I INPUT -p tcp --dport 80 -j ACCEPT
```

```
iptables -I INPUT -p tcp --dport 81 -j ACCEPT
```

```
iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT
```

```
iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT
```



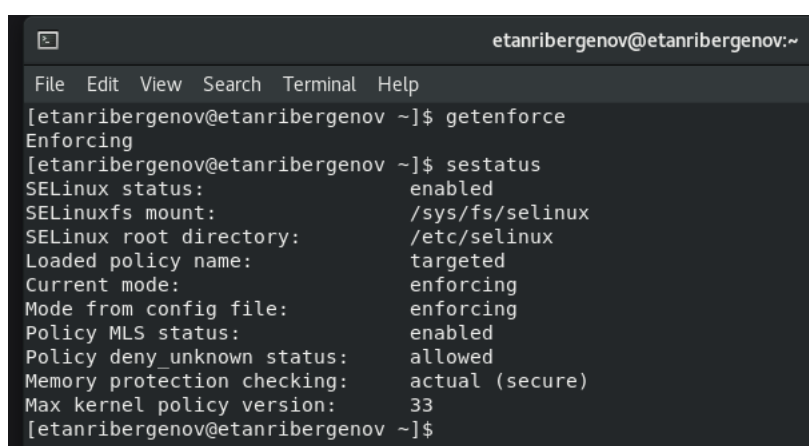
```
[root@etanribergenov ~]# iptables -F
[root@etanribergenov ~]# iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT
Bad argument `iptables'
Try `iptables -h' or `iptables --help' for more information.
[root@etanribergenov ~]# iptables -P INPUT ACCEPT
[root@etanribergenov ~]# iptables -P OUTPUT ACCEPT
[root@etanribergenov ~]# iptables -I INPUT -p tcp --dport 80 -j ACCEPT
[root@etanribergenov ~]# iptables -I INPUT -p tcp --dport 81 -j ACCEPT
[root@etanribergenov ~]# iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT
[root@etanribergenov ~]# iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT
[root@etanribergenov ~]#
```

Рис. 3.4: Отключение пакетного фильтра и разрешение подключения к портам 80 и 81 портам протокола tcp

Обратите внимание, что данные правила не являются «точными» и рекомендуемыми на все случаи жизни, они лишь позволяют правильно организовать работу стенда. В работе специально не делается акцент, каким браузером (или какой консольной программой) будет производиться подключение к веб-серверу. По желанию могут использоваться разные программы, такие как консольные *links*, *lynx*, *wget* и графические *konqueror*, *opera*, *firefox* или др.

4 Выполнение работы

1. Вошёл в систему с полученными учётными данными и убедился, что *SELinux* работает в режиме *enforcing* политики *targeted* с помощью команд ***getenforce*** и ***sestatus***.

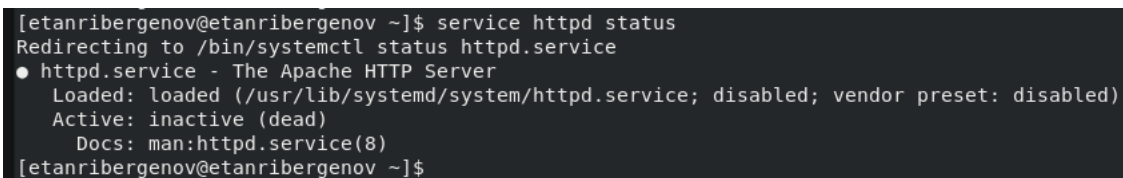
A terminal window titled 'etanribergenov@etanribergenov:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The user enters 'getenforce' and 'sestatus' commands. The output shows SELinux is enabled, in enforcing mode, with the targeted policy loaded.

```
etanribergenov@etanribergenov:~$ getenforce
Enforcing
etanribergenov@etanribergenov:~$ 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
etanribergenov@etanribergenov:~$
```

Рис. 4.1: Проверка того, что SeLinux работает в режиме enforcing политики targeted

2. Обратился с помощью браузера к веб-серверу, запущенному на компьютере - неуспешно. Проверил статус веб-сервера - он не включен.

`service httpd status`

A terminal window showing the output of the 'service httpd status' command. It indicates that the httpd.service is loaded but inactive (dead).

```
[etanribergenov@etanribergenov ~]$ 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: inactive (dead)
     Docs: man:httpd.service(8)
[eetanribergenov@etanribergenov ~]$
```

Рис. 4.2: Проверка статуса веб-сервера

Запустил его.

```
service httpd start
```

```
[etanribergenov@etanribergenov ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[eetanribergenov@etanribergenov ~]$ 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 Sat 2024-11-16 12:40:10 +05; 5s ago
     Docs: man:httpd.service(8)
  Main PID: 3520 (httpd)
    Status: "Started, listening on: port 80"
    Tasks: 213 (limit: 37634)
   Memory: 49.8M
    CGroup: /system.slice/httpd.service
            └─3520 /usr/sbin/httpd -DFOREGROUND
              └─3536 /usr/sbin/httpd -DFOREGROUND
                └─3537 /usr/sbin/httpd -DFOREGROUND
                  └─3538 /usr/sbin/httpd -DFOREGROUND
                    └─3539 /usr/sbin/httpd -DFOREGROUND

Nov 16 12:40:09 etanribergenov.localdomain systemd[1]: Starting The Apache HTTP Server...
Nov 16 12:40:10 etanribergenov.localdomain systemd[1]: Started The Apache HTTP Server.
Nov 16 12:40:10 etanribergenov.localdomain httpd[3520]: Server configured, listening on: port 80
[eetanribergenov@etanribergenov ~]$
```

Рис. 4.3: Запуск веб-сервера

3. Нашёл веб-сервер *Apache* в списке процессов, определил его контекст безопасности - *httpd_t*.

```
ps auxZ | grep httpd
```

```
[etanribergenov@etanribergenov ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root      3520  0.0  0.1 258204 10612 ?        Ss   12:40   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3536  0.0  0.1 262908  8284 ?        S    12:40   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3537  0.0  0.2 2697036 18048 ?        Sl   12:40   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3538  0.0  0.3 2500360 20116 ?        Sl   12:40   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3539  0.0  0.3 2500360 20092 ?        Sl   12:40   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 etanrib+ 3804  0.0  0.0 222012 1104 pts/0  S+   12:41   0:00 grep --color=auto httpd
[eetanribergenov@etanribergenov ~]$
```

Рис. 4.4: Процесс веб-сервера Apache в списке процессов

4. Посмотрел текущее состояние переключателей *SELinux* для *Apache* с помощью команды

```
sestatus -b httpd
```

```
etanribergenov@etanribergenov:~  
File Edit View Search Terminal Help  
[etanribergenov@etanribergenov ~]$ 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
```

Рис. 4.5: Просмотр состояния переключателей SELinux для Apache

Многие из них находятся в положении «off».

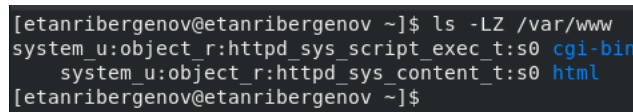
5. Посмотрел статистику по политике с помощью команды *seinfo*, также определил множество пользователей, ролей, типов.

```
[etanribergenov@etanribergenov ~]$ 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: 5015 Attributes: 258  
Users: 8 Roles: 15  
Booleans: 349 Cond. Expr.: 399  
Allow: 116272 Neverallow: 0  
Auditallow: 172 Dontaudit: 10529  
Type_trans: 262670 Type_change: 94  
Type_member: 37 Range_trans: 5989  
Role_allow: 40 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: 649  
Netifcon: 0 Nodecon: 0  
[etanribergenov@etanribergenov ~]$
```

Рис. 4.6: Статистика по политике

6. Определил тип файлов и поддиректорий, находящихся в директории */var/www*, с помощью команды

```
ls -lZ /var/www
```

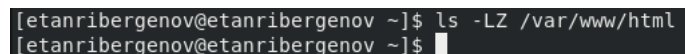


```
[etanribergenov@etanribergenov ~]$ ls -lZ /var/www
system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
system_u:object_r:httpd_sys_content_t:s0 html
[etanribergenov@etanribergenov ~]$
```

Рис. 4.7: Просмотр типов файлов и поддиректорий

7. Определил тип файлов, находящихся в директории */var/www/html*:

```
ls -lZ /var/www/html
```

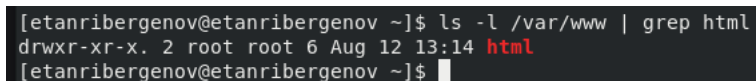


```
[etanribergenov@etanribergenov ~]$ ls -lZ /var/www/html
[etanribergenov@etanribergenov ~]$
```

Рис. 4.8: Просмотр типов файлов, находящихся в директории */var/www/html*

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

```
ls -l var/www | grep html
```



```
[etanribergenov@etanribergenov ~]$ ls -l /var/www | grep html
drwxr-xr-x. 2 root root 6 Aug 12 13:14 html
[etanribergenov@etanribergenov ~]$
```

Рис. 4.9: Просмотр атрибутов директории для определения круга пользователей, которым разрешено создание файлов в директории

Только у суперпользователя есть разрешение на запись в директорию.

9. Создал от имени суперпользователя html-файл */var/www/html/test-etanribergenov.html* следующего содержания:

```
<html>
```

```
<body>test</body>
```

```
</html>
```

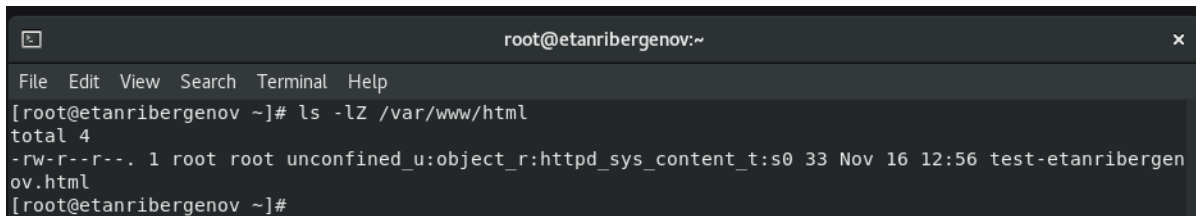


```
test-etanribergenov.html
/var/www/html

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

Рис. 4.10: Содержимое HTML-файла *test-etanribergenov*

10. Проверил контекст созданного файла.



```
root@etanribergenov:~  
File Edit View Search Terminal Help  
[root@etanribergenov ~]# ls -lZ /var/www/html  
total 4  
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Nov 16 12:56 test-etanribergenov.html  
[root@etanribergenov ~]#
```

Рис. 4.11: Проверка контекста безопасности созданного файла

Контекст, присваиваемый по умолчанию вновь созданным файлам в директории `/var/www/html` - `httpd_sys_content_t`.

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

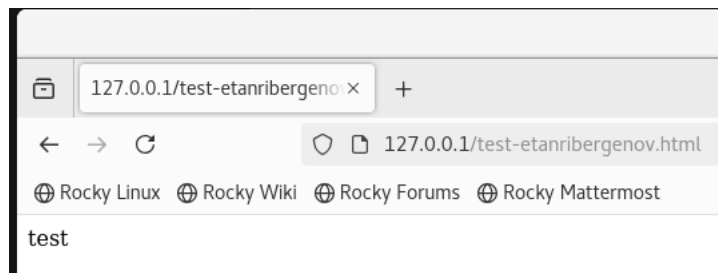


Рис. 4.12: Обращение к файлу через веб-сервер в браузере

12. Изучил справку `man httpd_selinux` и выяснил, какие контексты файлов определены для `httpd`.

```
root@etanribergenov:~  
File Edit View Search Terminal Help  
  
The following file types are defined for httpd:  
  
httpd_cache_t  
  
- Set files with the httpd_cache_t type, if you want to store the files under the /var/cache directory.  
  
Paths:  
/var/cache/rt(3|4)(.*)?, /var/cache/ssl.*.sem, /var/cache/mod_.*, /var/cache/php-.*,  
/var/cache/httpd(.*)?, /var/cache/mason(.*)?, /var/cache/mod_ssl(.*)?,  
/var/cache/lighttpd(.*)?, /var/cache/mediawiki(.*)?, /var/cache/mod_proxy(.*)?,  
/var/cache/mod_gnutls(.*)?, /var/cache/php-mmcache(.*)?, /var/cache/php-eaccelera-  
tor(.*)?  
  
httpd_config_t  
  
- Set files with the httpd_config_t type, if you want to treat the files as httpd configura-  
tion data, usually stored under the /etc directory.  
  
Paths:  
/etc/httpd(.*)?, /etc/nginx(.*)?, /etc/apache(2)?(.*)?, /etc/ Cherokee(.*)?,  
/etc/lighttpd(.*)?, /etc/apache-ssl(2)?(.*)?, /var/lib/openshift/.httpd.d(.*)?,  
/etc/opt/rh/rh-nginx18/nginx(.*)?, /var/lib/stickshift/.httpd.d(.*)?, /etc/vhosts,  
/etc/thttpd.conf
```

Рис. 4.13: Информация о контекстах безопасности SELinux файлов определённых для httpd

Сопоставил их с типом файла *test-etanribergenov.html*. Да, тип контекста этого файла есть в справке.

```
ls -Z /var/www/html/test-etanribergenov.html
```

```
[root@etanribergenov ~]#  
[root@etanribergenov ~]# ls -Z /var/www/html/test-etanribergenov.html  
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test-etanribergenov.html  
[root@etanribergenov ~]#  
[root@etanribergenov ~]# man httpd_selinux  
[root@etanribergenov ~]# man httpd_selinux | grep -i "httpd_sys_content"  
httpd_sys_content_t  
- Set files with the httpd_sys_content_t type, if you want to treat the files as httpd sys  
[root@etanribergenov ~]#
```

Рис. 4.14: Сопоставление типа файла с типами, описанными в справке

Рассмотрим полученный контекст детально. Так как по умолчанию пользователи CentOS являются свободными от типа (*unconfined* в переводе с англ. означает свободный), созданному файлу *test-etanribergenov.html* был сопоставлен *SELinux*, пользователь *unconfined_u*. Это первая часть контекста. Далее политика ролевого разделения доступа RBAC используется процессами, но не файлами, поэтому роли не имеют никакого значения для файлов. Роль *object_r* используется по умол-

чанию для файлов на «постоянных» носителях и на сетевых файловых системах. Если активна политика MLS, то могут использоваться и другие роли, например, `secadm_r`. Данный случай мы рассматривать не будем, как и предназначение `:s0`. Тип `httpd_sys_content_t` позволяет процессу `httpd` получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер.

13. Изменил контекст файла `/var/www/html/test-etanribergenov.html` с `httpd_sys_content_t` на `samba_share_t`, к которому процесс `httpd` не имеет доступа. После этого проверил, что контекст поменялся.

```
chcon -t samba_share_t /var/www/html/test-etanribergenov.html
ls -Z /var/www/html/test-etanribergenov.html
```

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

Рис. 4.15: Изменение контекста SELinux для файла

14. Попробовал ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test-etanribergenov.html`. Получил сообщение об ошибке:

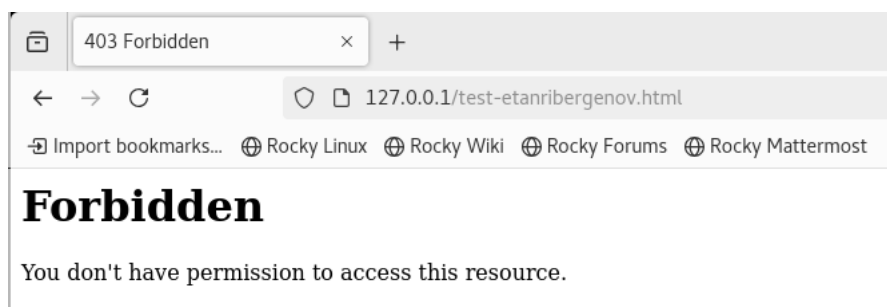


Рис. 4.16: Попытка получения доступа к файлу через веб-сервер в браузере

15. Файл не был отображён, несмотря на то, что права доступа позволяют читать этот файл любому пользователю, потому что контекст безопасности изменился и `httpd` больше не имеет доступа к файлу.

Просмотрел системный лог-файл:

```
tail /var/log/messages
```

```
[root@etanribergenov ~]# tail /var/log/messages
Nov 16 13:40:50 etanribergenov dbus-daemon[816]: [system] Successfully activated
service 'org.fedoraproject.Setroubleshootd'
Nov 16 13:40:50 etanribergenov systemd[1]: Started SETroubleshoot daemon for pro
cessing new SELinux denial logs.
Nov 16 13:40:52 etanribergenov setroubleshoot[7002]: failed to retrieve rpm info
for /var/www/html/test-etanribergenov.html
Nov 16 13:40:52 etanribergenov dbus-daemon[816]: [system] Activating service nam
e='org.fedoraproject.SetroubleshootPrivileged' requested by ':1.532' (uid=984 pi
d=7002 comm="/usr/libexec/platform-python -Es /usr/sbin/setroub" label="system_u
:system_r:setroubleshootd_t:s0") (using servicehelper)
Nov 16 13:40:52 etanribergenov dbus-daemon[816]: [system] Successfully activated
service 'org.fedoraproject.SetroubleshootPrivileged'
Nov 16 13:40:53 etanribergenov setroubleshoot[7002]: SELinux is preventing /usr/
sbin/httpd from getattr access on the file /var/www/html/test-etanribergenov.htm
l. For complete SELinux messages run: sealert -l d1273dfd-9d5e-4131-a4df-fceb556
fe925
Nov 16 13:40:53 etanribergenov setroubleshoot[7002]: SELinux is preventing /usr/
sbin/httpd from getattr access on the file /var/www/html/test-etanribergenov.htm
l.#012#012***** Plugin restorecon (92.2 confidence) suggests *****
*****#012#012If you want to fix the label. #012/var/www/html/test-etanriberge
nov.html default label should be httpd_sys_content_t.#012Then you can run restor
econ. The access attempt may have been stopped due to insufficient permissions t
```

Рис. 4.17: Сообщения в системном лог-файле

Если в системе окажутся запущенными процессы *setroubleshootd* и *auditd*, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле */var/log/audit/audit.log*.

```
[root@etanribergenov ~]# cat /var/log/audit/audit.log | grep setroubleshootd
type=SERVICE_START msg=audit(1731746115.462:222): pid=1 uid=0 auid=4294967295 se
s=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=setroubleshootd comm="sy
stemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1731746130.344:223): pid=1 uid=0 auid=4294967295 ses
=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=setroubleshootd comm="sys
temd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
ID="root" AUID="unset"
```

Рис. 4.18: Сообщения в лог-файле процесса auditd

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* нашёл строчку ***Listen 80*** и заменил её на ***Listen 81***.

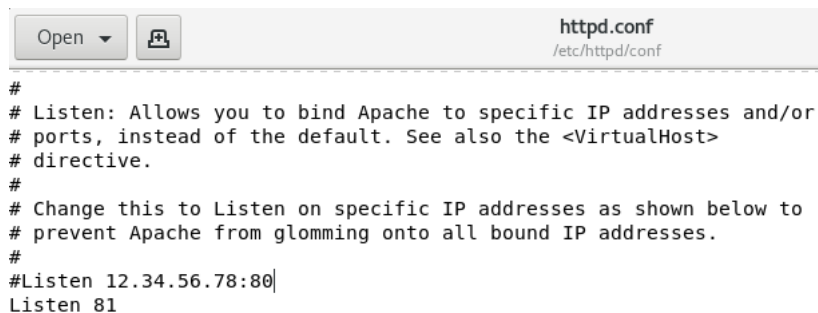


Рис. 4.19: Изменение порта прослушивания веб-сервера Apache

17. Выполнил перезапуск веб-сервера *Apache*. Сбой не произошёл. Это потому, что в разделе подготовки лабораторного стенда были приведены команды, разрешающие веб-серверу *Apache* прослушивать *tcp* порт 81.

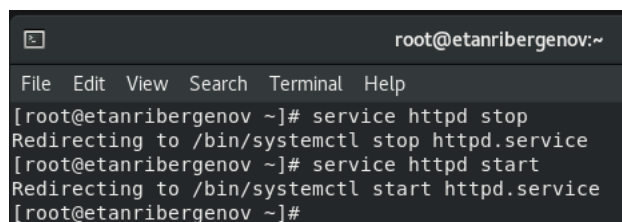


Рис. 4.20: Выполнение перезапуска веб-сервера

18. Проанализируйте лог-файлы:

```
tail -nl /var/log/messages
```

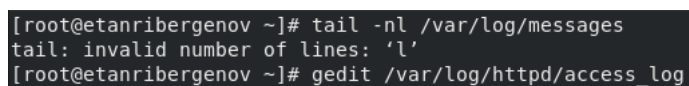


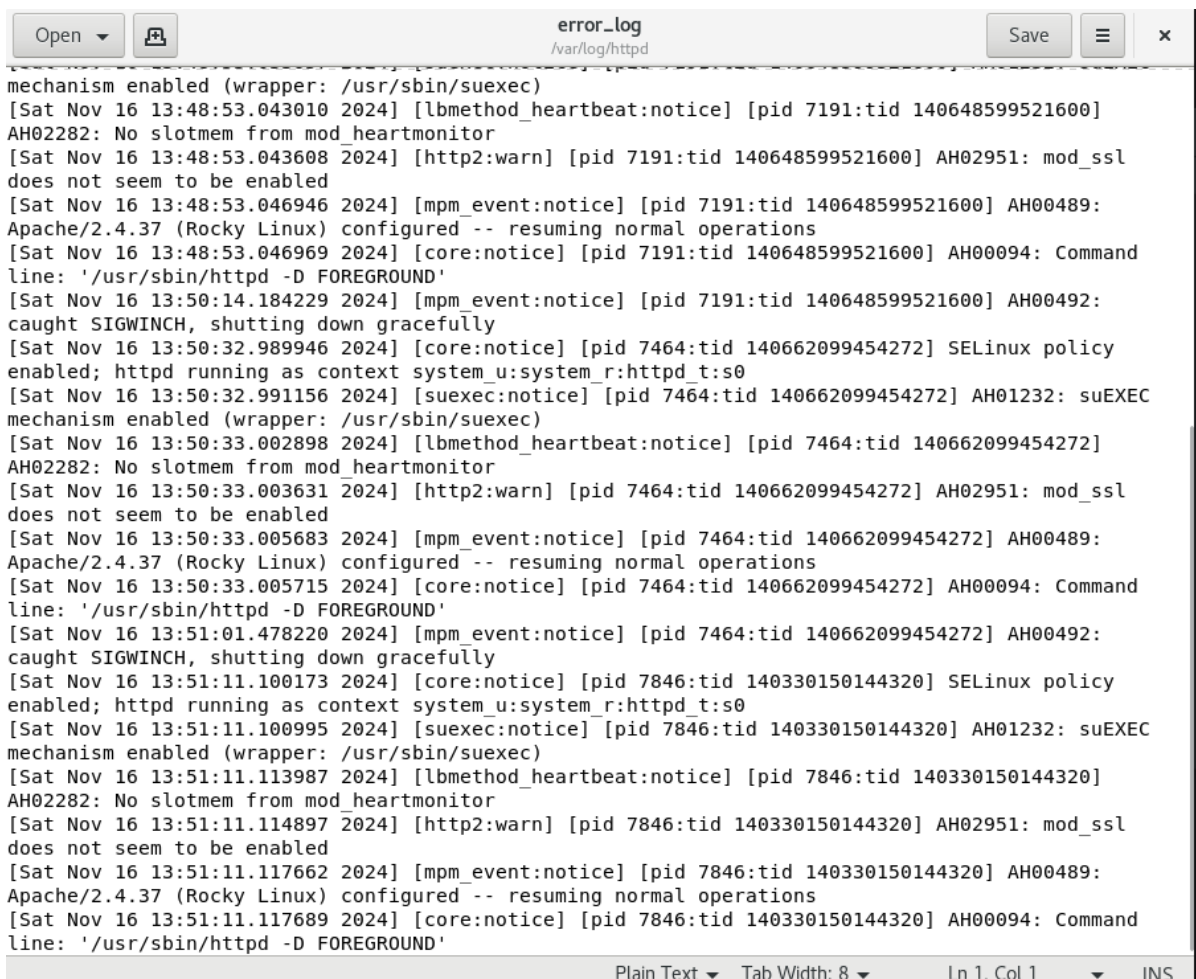
Рис. 4.21: Просмотр системного лог-файла

Просмотрите файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log` и выясните, в каких файлах появились записи.



```
Open  access_log  Save  x
/var/log/httpd
127.0.0.1 - - [16/Nov/2024:13:11:35 +0500] "GET /test-etanribergenov.html HTTP/1.1" 200 33 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
127.0.0.1 - - [16/Nov/2024:13:11:35 +0500] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/
test-etanribergenov.html" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
127.0.0.1 - - [16/Nov/2024:13:35:14 +0500] "GET /test-etanribergenov.html HTTP/1.1" 403 199 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
127.0.0.1 - - [16/Nov/2024:13:35:14 +0500] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/
test-etanribergenov.html" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
127.0.0.1 - - [16/Nov/2024:13:40:46 +0500] "GET /test-etanribergenov.html HTTP/1.1" 403 199 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
```

Рис. 4.22: Просмотр лог-файла access_log



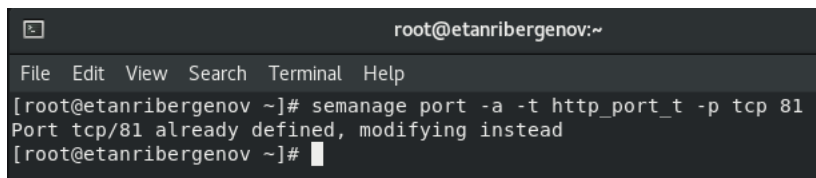
```
Open  error_log  Save  x
/var/log/httpd
mechanism enabled (wrapper: /usr/sbin/suexec)
[Sat Nov 16 13:48:53.043010 2024] [lbmethod_heartbeat:notice] [pid 7191:tid 140648599521600]
AH02282: No slotmem from mod_heartbeat
[Sat Nov 16 13:48:53.043608 2024] [http2:warn] [pid 7191:tid 140648599521600] AH02951: mod_ssl
does not seem to be enabled
[Sat Nov 16 13:48:53.046946 2024] [mpm_event:notice] [pid 7191:tid 140648599521600] AH00489:
Apache/2.4.37 (Rocky Linux) configured -- resuming normal operations
[Sat Nov 16 13:48:53.046969 2024] [core:notice] [pid 7191:tid 140648599521600] AH00094: Command
line: '/usr/sbin/httpd -D FOREGROUND'
[Sat Nov 16 13:50:14.184229 2024] [mpm_event:notice] [pid 7191:tid 140648599521600] AH00492:
caught SIGWINCH, shutting down gracefully
[Sat Nov 16 13:50:32.989946 2024] [core:notice] [pid 7464:tid 140662099454272] SELinux policy
enabled; httpd running as context system_u:system_r:httpd_t:s0
[Sat Nov 16 13:50:32.991156 2024] [suexec:notice] [pid 7464:tid 140662099454272] AH01232: suEXEC
mechanism enabled (wrapper: /usr/sbin/suexec)
[Sat Nov 16 13:50:33.002898 2024] [lbmethod_heartbeat:notice] [pid 7464:tid 140662099454272]
AH02282: No slotmem from mod_heartbeat
[Sat Nov 16 13:50:33.003631 2024] [http2:warn] [pid 7464:tid 140662099454272] AH02951: mod_ssl
does not seem to be enabled
[Sat Nov 16 13:50:33.005683 2024] [mpm_event:notice] [pid 7464:tid 140662099454272] AH00489:
Apache/2.4.37 (Rocky Linux) configured -- resuming normal operations
[Sat Nov 16 13:50:33.005715 2024] [core:notice] [pid 7464:tid 140662099454272] AH00094: Command
line: '/usr/sbin/httpd -D FOREGROUND'
[Sat Nov 16 13:51:01.478220 2024] [mpm_event:notice] [pid 7464:tid 140662099454272] AH00492:
caught SIGWINCH, shutting down gracefully
[Sat Nov 16 13:51:11.100173 2024] [core:notice] [pid 7846:tid 140330150144320] SELinux policy
enabled; httpd running as context system_u:system_r:httpd_t:s0
[Sat Nov 16 13:51:11.100995 2024] [suexec:notice] [pid 7846:tid 140330150144320] AH01232: suEXEC
mechanism enabled (wrapper: /usr/sbin/suexec)
[Sat Nov 16 13:51:11.113987 2024] [lbmethod_heartbeat:notice] [pid 7846:tid 140330150144320]
AH02282: No slotmem from mod_heartbeat
[Sat Nov 16 13:51:11.114897 2024] [http2:warn] [pid 7846:tid 140330150144320] AH02951: mod_ssl
does not seem to be enabled
[Sat Nov 16 13:51:11.117662 2024] [mpm_event:notice] [pid 7846:tid 140330150144320] AH00489:
Apache/2.4.37 (Rocky Linux) configured -- resuming normal operations
[Sat Nov 16 13:51:11.117689 2024] [core:notice] [pid 7846:tid 140330150144320] AH00094: Command
line: '/usr/sbin/httpd -D FOREGROUND'
```

Рис. 4.23: Просмотр лог-файла error_log

Сообщений об ошибке нет.

19. Выполнил команду

```
semanage port -a -t http_port_t -p tcp 81
```

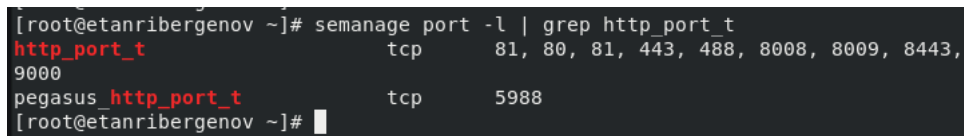


```
root@etanribergenov:~  
File Edit View Search Terminal Help  
[root@etanribergenov ~]# semanage port -a -t http_port_t -p tcp 81  
Port tcp/81 already defined, modifying instead  
[root@etanribergenov ~]#
```

Рис. 4.24: Добавление tcp-порта 81 в список портов SELinux для веб-сервера

После этого проверил список портов командой

```
semanage port -l | grep http_port_t
```

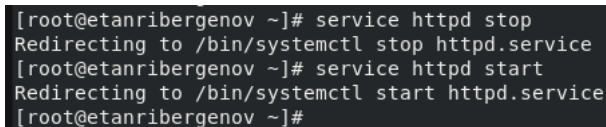


```
[root@etanribergenov ~]# semanage port -l | grep http_port_t  
http_port_t tcp 81, 80, 81, 443, 488, 8008, 8009, 8443, 9000  
pegasus http_port_t tcp 5988  
[root@etanribergenov ~]#
```

Рис. 4.25: Просмотр списка портов SELinux для веб-сервера

Убедился, что порт 81 появился в списке.

20. Попробовал запустить веб-сервер *Apache* ещё раз. Он вновь запустился без проблем, как и в прошлый раз.

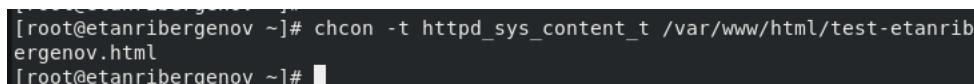


```
[root@etanribergenov ~]# service httpd stop  
Redirecting to /bin/systemctl stop httpd.service  
[root@etanribergenov ~]# service httpd start  
Redirecting to /bin/systemctl start httpd.service  
[root@etanribergenov ~]#
```

Рис. 4.26: Перезапуск веб-сервера Apache

21. Вернул контекст `*httpd_sys_content__t*` к файлу `/var/www/html/test-etanribergenov.html`:

```
chcon -t httpd_sys_content_t /var/www/html/test-etanribergenov.html
```



```
[root@etanribergenov ~]# chcon -t httpd_sys_content_t /var/www/html/test-etanribergenov.html  
[root@etanribergenov ~]#
```

Рис. 4.27: Возвращение контекста SELinux к файлу

После этого попробовал получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test-etanribergenov.html`. Увидел содержимое файла — слово «test».

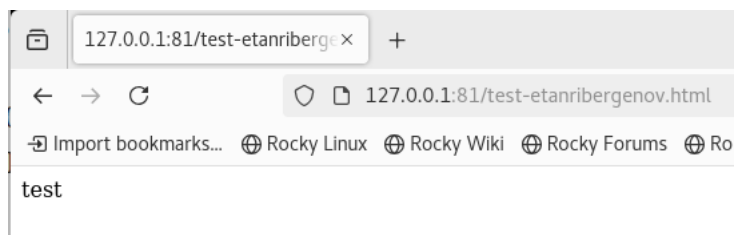


Рис. 4.28: Получение доступа к файлу через веб-сервер в браузере

22. Исправил обратно конфигурационный файл *apache*, вернув ***Listen 80***.

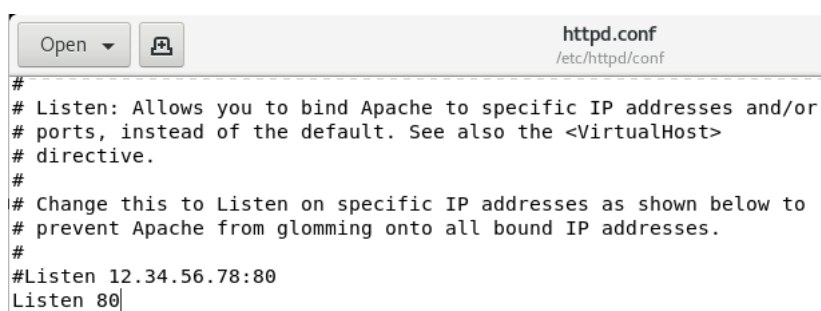


Рис. 4.29: Изменение конф. файла веб-сервера Apache

23. Удалил привязку *http_port_t* к 81 порту и проверил, что порт 81 удалён.

```
semanage port -d -t http_port_t -p tcp 81
```

```
semanage port -l | grep http_port_t
```

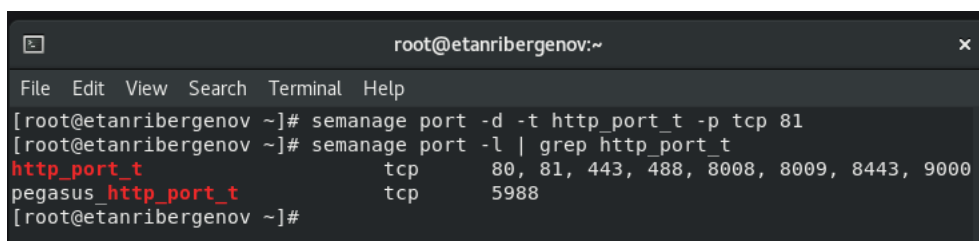


Рис. 4.30: Удаление привязки `http_port_t` к 81 порту и проверка выполнения действия

24. Удалил файл */var/www/html/test-etanribergenov.html*

```
rm /var/www/html/test-etanribergenov.html
```

A terminal window with a dark background. The prompt is [root@etanribergenov ~]#. The command rm /var/www/html/test-etanribergenov.html is entered. The output is rm: remove regular file '/var/www/html/test-etanribergenov.html'? y. The prompt returns to [root@etanribergenov ~]#.

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

Рис. 4.31: Удаление файла

5 Выводы

В результате выполнения работы я развил навыки администрирования ОС *Linux*. Получил первое практическое знакомство с технологией *SELinux*. Проверил работу *SELinux* на практике совместно с веб-сервером *Apache*.