

Отчёт по лабораторной работе №6 по предмету Информационная безопасность

Мандатное разграничение прав в Linux

Саттарова Вита Викторовна

Содержание

1	Цели и задачи работы	5
2	Объект и предмет исследования	6
3	Условные обозначения и термины	7
4	Задание	8
5	Теоретическое введение	11
5.1	Организация и описание лабораторного стенда	11
5.2	Подготовка лабораторного стенда и методические рекомендации	11
6	Техническое оснащение и выбранные методы проведения работы	13
7	Выполнение лабораторной работы и полученные результаты	14
8	Анализ результатов	33
9	Заключение и выводы	34
10	Список литературы	35

Список иллюстраций

7.1	Лабораторная работа 6	15
7.2	Задание 1	16
7.3	Задание 2	17
7.4	Задание 3	18
7.5	Задание 4	19
7.6	Задание 5	20
7.7	Задание 6	21
7.8	Задания 7-8	22
7.9	Задание 9	23
7.10	Задание 10	23
7.11	Задание 11	23
7.12	Задания 12-13	24
7.13	Задание 14	25
7.14	Задание 15	26
7.15	Задание 16	27
7.16	Задание 17	28
7.17	Задание 18	29
7.18	Задание 19	30
7.19	Задание 20	30
7.20	Задания 21-24	32

Список таблиц

1 Цели и задачи работы

Цели:

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

Задачи:

- Выполнить все пункты, указанные в методических рекомендациях к лабораторной работе.
- Ответить на вопросы, заданные в методических рекомендациях к лабораторной работе.
- Выполняя задания, познакомиться с технологией SELinux.
- Выполняя задания, поработать с SELinux с веб-сервером Apache.
- Написать отчёт, проанализировав результаты, полученные в ходе выполнения лабораторной работы.

2 Объект и предмет исследования

Объект исследования: использование SELinux и веб-сервером Apache для обеспечения безопасности.

Предмет исследования: администрирование, SELinux, веб-сервер Apache.

3 Условные обозначения и термины

Условные обозначения

- ОС - операционная система

Термины

- контекст безопасности

4 Задание

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.
2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: `service httpd status` или `/etc/rc.d/init.d/httpd status` Если не работает, запустите его так же, но с параметром `start`.
3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду `ps auxZ | grep httpd` или `ps -eZ | grep httpd`
4. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -b | grep httpd` Обратите внимание, что многие из них находятся в положении «off».
5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов.
6. Определите тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www`
7. Определите тип файлов, находящихся в директории `/var/www/html`: `ls -lZ /var/www/html`

8. Определите круг пользователей, которым разрешено создание файлов в директории `/var/www/html`.
9. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл `/var/www/html/test.html` следующего содержания:

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

10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории `/var/www/html`.
11. Обратитесь к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедитесь, что файл был успешно отображён.
12. Изучите справку `man httpd_selinux` и выясните, какие контексты файлов определены для `httpd`. Сопоставьте их с типом файла `test.html`. Проверить контекст файла можно командой `ls -Z. ls -Z /var/www/html/test.html`
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`: `chcon -t samba_share_t /var/www/html/test.html ls -Z /var/www/html/test.html` После этого проверьте, что контекст поменялся.
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.
15. Проанализируйте 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 просмотрите системный лог-файл: `tail /var/log/messages`.

16. Попробуйте 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`.
 17. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему?
 18. Проанализируйте лог-файлы: `tail -nl /var/log/messages`. 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.
 19. Выполните команду `semanage port -a -t http_port_t -p tcp 81` После этого проверьте список портов командой `semanage port -l | grep http_port_t` Убедитесь, что порт 81 появился в списке.
 20. Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему он сейчас запустился, а в предыдущем случае не смог?
 21. Верните 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 попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. Вы должны увидеть содержимое файла — слово «test».
 22. Исправьте обратно конфигурационный файл apache, вернув `Listen 80`.
 23. Удалите привязку `http_port_t` к 81 порту: `semanage port -d -t http_port_t -p tcp 81` и проверьте, что порт 81 удалён.
 24. Удалите файл `/var/www/html/test.html`: `rm /var/www/html/test.html`
- Более подробно о работе см. в [1].

5 Теоретическое введение

5.1 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.

5.2 Подготовка лабораторного стенда и методические рекомендации

1. 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.
2. При необходимости администратор должен разбираться в работе SELinux

и уметь как исправить конфигурационный файл `/etc/selinux/config`, так и проверить используемый режим и политику.

3. Необходимо, чтобы был установлен веб-сервер Apache. При установке системы в конфигурации «рабочая станция» указанный пакет не ставится.
4. 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.
5. 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`.
6. Обратите внимание, что данные правила не являются «точными» и рекомендуются на все случаи жизни, они лишь позволяют правильно организовать работу стенда.
7. В работе специально не делается акцент, каким браузером (или какой консольной программой) будет производиться подключение к вебсерверу. По желанию могут использоваться разные программы, такие как консольные `links`, `lynx`, `wget` и графические `konqueror`, `opera`, `firefox` или др.

Более подробно о работе см. в [1].

6 Техническое оснащение и выбранные методы проведения работы

Техническое оснащение

- Ноутбук
- RockyLinux
- Интернет

Методы проведения работы

- Изучение методической информации
- Выполнение заданий в соответствии с указаниями
- Анализ результатов
- Ответы на вопросы, заданные в задании
- Обобщение проведённой деятельности

7 Выполнение лабораторной работы и полученные результаты

1. Скачала и ознакомилась с методическими указаниями к лабораторной работе (рис. 7.1).

Лабораторная работа № 6. Мандатное разграничение прав в Linux

6.1. Цели работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux¹.

Проверить работу SELinux на практике совместно с веб-сервером Apache.

6.2. Организация и описание лабораторного стенда

Для проведения указанной лабораторной работы на одно рабочее место требуется компьютер с установленной операционной системой Linux, поддерживающей технологию SELinux.

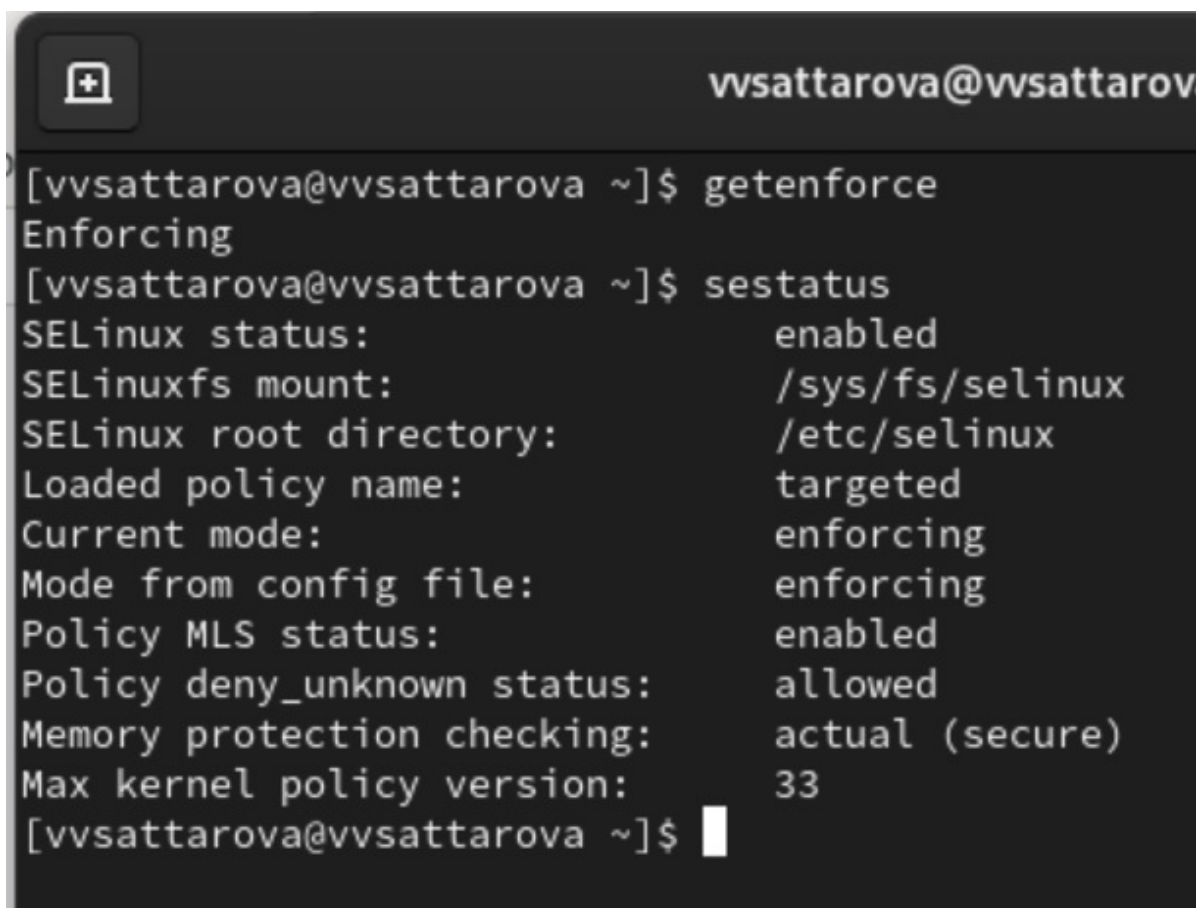
Предполагается использовать стандартный дистрибутив Linux CentOS с включённой политикой SELinux targeted и режимом enforcing. Для выполнения заданий требуется наличие учётной записи администратора (root) и учётной записи обычного пользователя. Постоянно работать от учётной записи root неправильно с точки зрения безопасности.

6.3. Подготовка лабораторного стенда и методические

Рис. 7.1: Лабораторная работа 6

2. Выполнила следующие задания:

- Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus` (рис. 7.2).

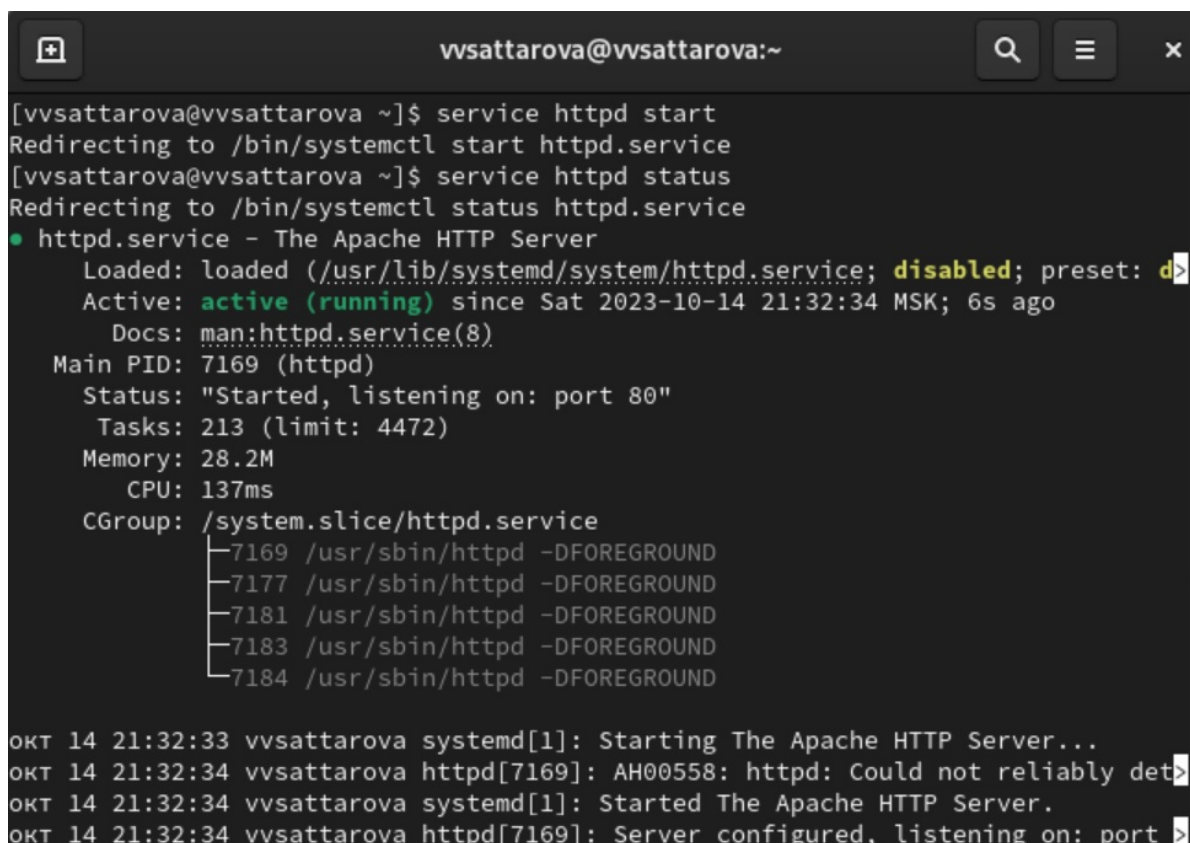
A terminal window with a dark background. The title bar shows a window icon and the text 'vvsattarova@vvsattarova'. The terminal content shows the execution of 'getenforce' and 'sestatus' commands. The output of 'sestatus' lists various SELinux parameters and their values.

```
[vvsattarova@vvsattarova ~]$ getenforce
Enforcing
[vvsattarova@vvsattarova ~]$ 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
[vvsattarova@vvsattarova ~]$
```

Рис. 7.2: Заданит 1

3. Выполнила следующие задания:

- Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: `service httpd status` или `/etc/rc.d/init.d/httpd status` Если не работает, запустите его так же, но с параметром `start` (рис. 7.3).

A terminal window titled 'vvsattarova@vvsattarova:~' with search, menu, and close icons in the title bar. The terminal shows the following commands and output:

```
[vvsattarova@vvsattarova ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[vvsattarova@vvsattarova ~]$ 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; preset: d>
   Active: active (running) since Sat 2023-10-14 21:32:34 MSK; 6s ago
     Docs: man:httpd.service(8)
  Main PID: 7169 (httpd)
    Status: "Started, listening on: port 80"
     Tasks: 213 (limit: 4472)
    Memory: 28.2M
       CPU: 137ms
    CGroup: /system.slice/httpd.service
            └─7169 /usr/sbin/httpd -DFOREGROUND
               └─7177 /usr/sbin/httpd -DFOREGROUND
                  └─7181 /usr/sbin/httpd -DFOREGROUND
                     └─7183 /usr/sbin/httpd -DFOREGROUND
                        └─7184 /usr/sbin/httpd -DFOREGROUND

окт 14 21:32:33 vvsattarova systemd[1]: Starting The Apache HTTP Server...
окт 14 21:32:34 vvsattarova httpd[7169]: AH00558: httpd: Could not reliably det>
окт 14 21:32:34 vvsattarova systemd[1]: Started The Apache HTTP Server.
окт 14 21:32:34 vvsattarova httpd[7169]: Server configured, listening on: port >
```

Рис. 7.3: Заданит 2

4. Выполнила следующие задания:

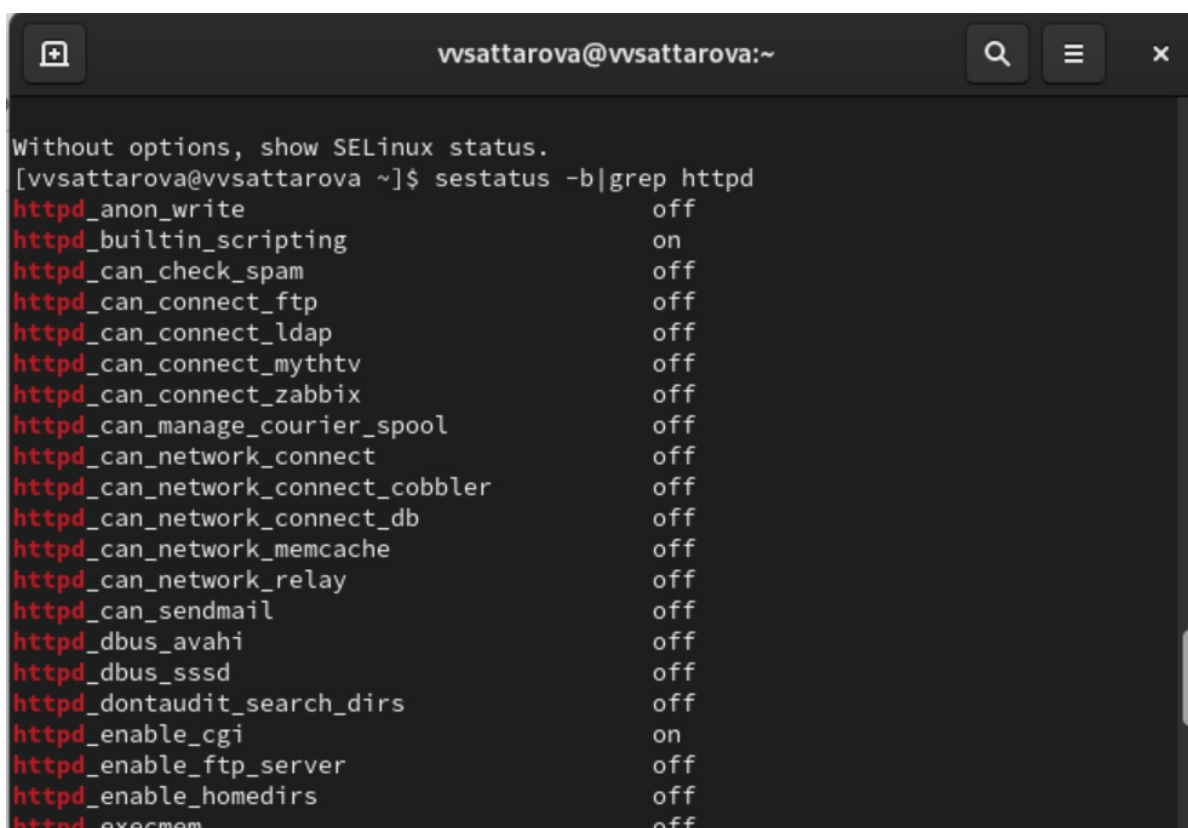
- Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду `ps auxZ | grep httpd` или `ps -eZ | grep httpd` (рис. 7.4).

```
vvsattarova@vvsattarova:~  
-7169 /usr/sbin/httpd -DFOREGROUND  
-7177 /usr/sbin/httpd -DFOREGROUND  
-7181 /usr/sbin/httpd -DFOREGROUND  
-7183 /usr/sbin/httpd -DFOREGROUND  
-7184 /usr/sbin/httpd -DFOREGROUND  
окт 14 21:32:33 vvsattarova systemd[1]: Starting The Apache HTTP Server...  
окт 14 21:32:34 vvsattarova httpd[7169]: AH00558: httpd: Could not reliably det  
окт 14 21:32:34 vvsattarova systemd[1]: Started The Apache HTTP Server.  
окт 14 21:32:34 vvsattarova httpd[7169]: Server configured, listening on: port >  
[vvsattarova@vvsattarova ~]$ ps auxZ | grep httpd  
system_u:system_r:httpd_t:s0 root 7169 0.1 1.4 20328 11240 ?  
Ss 21:32 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 7177 0.0 0.9 21664 7296 ?  
S 21:32 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 7181 0.0 1.4 1079476 11000 ?  
Sl 21:32 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 7183 0.0 1.6 1210612 13048 ?  
Sl 21:32 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 7184 0.0 1.4 1079476 11004 ?  
Sl 21:32 0:00 /usr/sbin/httpd -DFOREGROUND  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 vvsatta+ 7430 0.0 0.3 221  
688 2368 pts/0 S+ 21:34 0:00 grep --color=auto httpd  
[vvsattarova@vvsattarova ~]$
```

Рис. 7.4: Задание 3

5. Выполнила следующие задания:

- Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -b | grep httpd` Обратите внимание, что многие из них находятся в положении «off» (рис. 7.5).

A terminal window with a dark background and light text. The title bar shows the user 'wsattarova@wsattarova:~'. The terminal content shows a command prompt followed by the command 'sestatus -b|grep httpd'. The output is a list of SELinux booleans for the httpd process, each followed by its status (on or off).

```
Without options, show SELinux status.  
[wsattarova@wsattarova ~]$ sestatus -b|grep httpd  
httpd_anon_write off  
httpd_builtin_scripting on  
httpd_can_check_spam off  
httpd_can_connect_ftp off  
httpd_can_connect_ldap off  
httpd_can_connect_mythtv off  
httpd_can_connect_zabbix off  
httpd_can_manage_courier_spool off  
httpd_can_network_connect off  
httpd_can_network_connect_cobbler off  
httpd_can_network_connect_db off  
httpd_can_network_memcache off  
httpd_can_network_relay off  
httpd_can_sendmail off  
httpd_dbus_avahi off  
httpd_dbus_sssd off  
httpd_dontaudit_search_dirs off  
httpd_enable_cgi on  
httpd_enable_ftp_server off  
httpd_enable_homedirs off  
httpd_execmem off
```

Рис. 7.5: Задание 4

6. Выполнила следующие задания:

- Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов (рис. 7.6).

```

[~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:      135      Permissions:      457
Sensitivities: 1      Categories:      1024
Types:        5100    Attributes:       258
Users:        8       Roles:           14
Booleans:     353     Cond. Expr.:     384
Allow:        65009   Neverallow:      0
Auditallow:   170     Dontaudit:       8572
Type_trans:   265337  Type_change:     87
Type_member:  35      Range_trans:     6164
Role allow:   38      Role_trans:      420
Constraints:  70      Validatetrans:   0
MLS Constrai: 72     MLS Val. Tran:   0
Permissives:  2      Polcap:          6
Defaults:     7      Typebounds:      0
Allowxperm:   0      Neverallowxperm: 0
Auditallowxperm: 0    Dontauditxperm:  0
Ibendportcon: 0      Ibpkeycon:       0
Initial SIDs: 27     Fs_use:          35

```

Рис. 7.6: Задание 5

7. Выполнила следующие задания:

- Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды `ls -lZ /var/www` (рис. 7.7).

```
vwsattarova@vwsattarova:~  
Allow: 65009 Neverallow: 0  
Auditallow: 170 Dontaudit: 8572  
Type_trans: 265337 Type_change: 87  
Type_member: 35 Range_trans: 6164  
Role_allow: 38 Role_trans: 420  
Constraints: 70 Validatetrans: 0  
MLS Constrain: 72 MLS Val. Tran: 0  
Permissives: 2 Polcap: 6  
Defaults: 7 Typebounds: 0  
Allowxperm: 0 Neverallowxperm: 0  
Auditallowxperm: 0 Dontauditxperm: 0  
Ibendportcon: 0 Ibkeycon: 0  
Initial SIDs: 27 Fs_use: 35  
Genfscon: 109 Portcon: 660  
Netifcon: 0 Nodecon: 0  
[vwsattarova@vwsattarova ~]$ s -lZ /var/www  
bash: s: command not found...  
[vwsattarova@vwsattarova ~]$ ls -lZ /var/www  
итого 0  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 16 23  
:21 cgi-bin  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 окт 14 21  
:25 html  
[vwsattarova@vwsattarova ~]$
```

Рис. 7.7: Задание 6

8. Выполнила следующие задания:

- Определите тип файлов, находящихся в директории /var/www/html: `ls -lZ /var/www/html`
- Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html (рис. 7.8).

```
vsattarova@vsattarova:~  
Type_trans:      265337  Type_change:      87  
Type_member:      35    Range_trans:      6164  
Role_allow:       38    Role_trans:       420  
Constraints:      70    Validatetrans:    0  
MLS Constrain:    72    MLS Val. Tran:    0  
Permissives:      2    Polcap:           6  
Defaults:         7    Typebounds:       0  
Allowxperm:       0    Neverallowxperm:  0  
Auditallowxperm:  0    Dontauditxperm:   0  
Ibendportcon:     0    Ibkeycon:         0  
Initial SIDs:     27    Fs_use:           35  
Genfscon:         109   Portcon:          660  
Netifcon:         0    Nodecon:          0  
[vsattarova@vsattarova ~]$ s -lZ /var/www  
bash: s: command not found...  
[vsattarova@vsattarova ~]$ ls -lZ /var/www  
итого 0  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 16 23  
:21 cgi-bin  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 окт 14 21  
:25 html  
[vsattarova@vsattarova ~]$ ls -lZ /var/www/html  
итого 0  
[vsattarova@vsattarova ~]$
```

Рис. 7.8: Задания 7-8

9. Выполнила следующие задания:

- Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания:

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

(рис. 7.9).

```
[vvsattarova@vvsattarova ~]$ cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[vvsattarova@vvsattarova ~]$
```

Рис. 7.9: Задание 9

10. Выполнила следующие задания:

- Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html. (рис. 7.10).

```
[vvsattarova@vvsattarova ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[vvsattarova@vvsattarova ~]$
```

Рис. 7.10: Задание 10

11. Выполнила следующие задания:

- Обратитесь к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Убедитесь, что файл был успешно отображён (рис. 7.11).

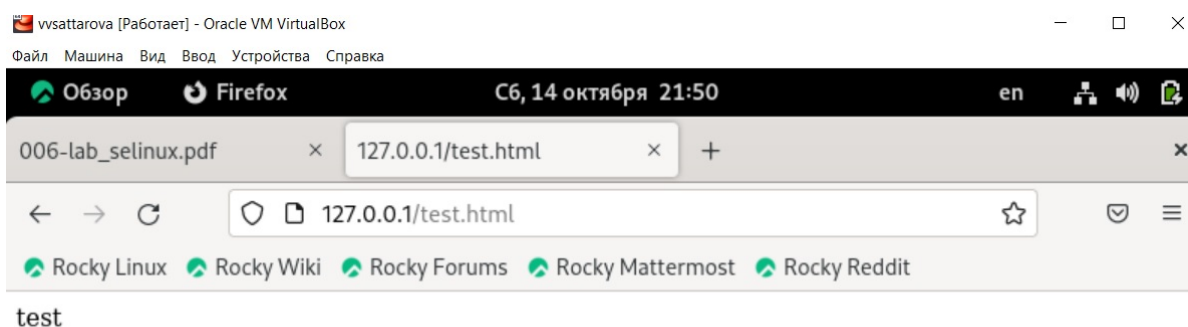
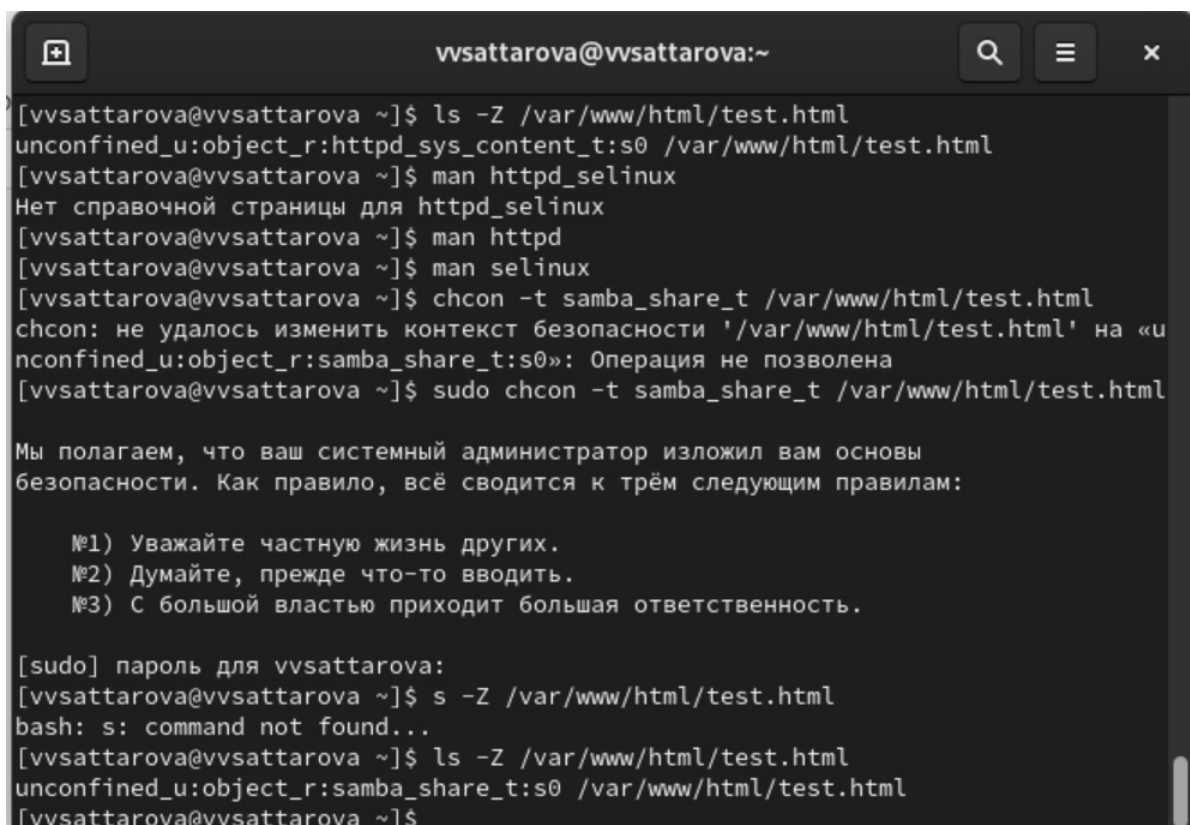


Рис. 7.11: Задание 11

12. Выполнила следующие задания:

- Изучите справку `man httpd_selinux` и выясните, какие контексты файлов определены для `httpd`. Сопоставьте их с типом файла `test.html`. Проверить контекст файла можно командой `ls -Z. ls -Z /var/www/html/test.html`
- 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`: `chcon -t samba_share_t /var/www/html/test.html` `ls -Z /var/www/html/test.html` После этого проверьте, что контекст поменялся (рис. 7.12).



```
vvsattarova@vvsattarova:~  
[vvsattarova@vvsattarova ~]$ ls -Z /var/www/html/test.html  
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html  
[vvsattarova@vvsattarova ~]$ man httpd_selinux  
Нет справочной страницы для httpd_selinux  
[vvsattarova@vvsattarova ~]$ man httpd  
[vvsattarova@vvsattarova ~]$ man selinux  
[vvsattarova@vvsattarova ~]$ chcon -t samba_share_t /var/www/html/test.html  
chcon: не удалось изменить контекст безопасности '/var/www/html/test.html' на «unconfined_u:object_r:samba_share_t:s0»: Операция не позволена  
[vvsattarova@vvsattarova ~]$ sudo chcon -t samba_share_t /var/www/html/test.html  
  
Мы полагаем, что ваш системный администратор изложил вам основы безопасности. Как правило, всё сводится к трём следующим правилам:  
  
№1) Уважайте частную жизнь других.  
№2) Думайте, прежде что-то вводить.  
№3) С большой властью приходит большая ответственность.  
  
[sudo] пароль для vvsattarova:  
[vvsattarova@vvsattarova ~]$ s -Z /var/www/html/test.html  
bash: s: command not found...  
[vvsattarova@vvsattarova ~]$ ls -Z /var/www/html/test.html  
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html  
[vvsattarova@vvsattarova ~]$
```

Рис. 7.12: Задания 12-13

13. Выполнила следующие задания:

- 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 (рис. 7.13).

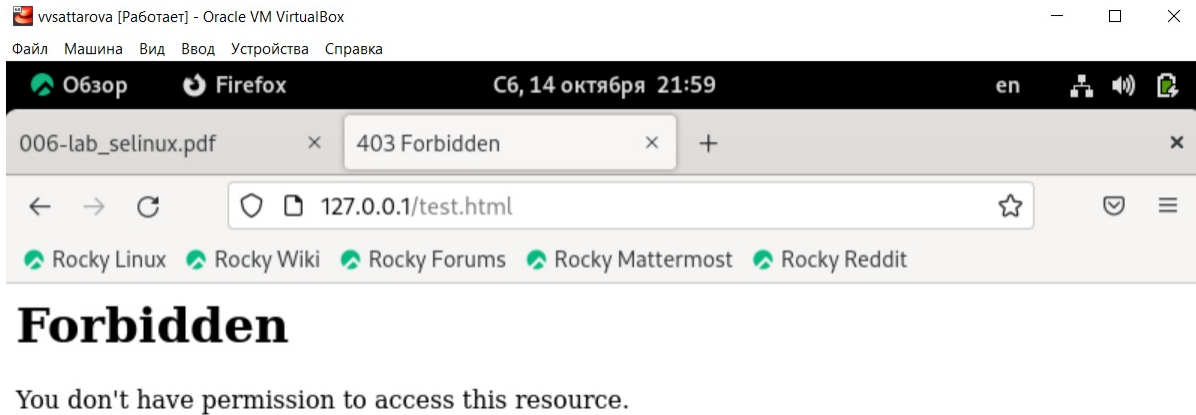
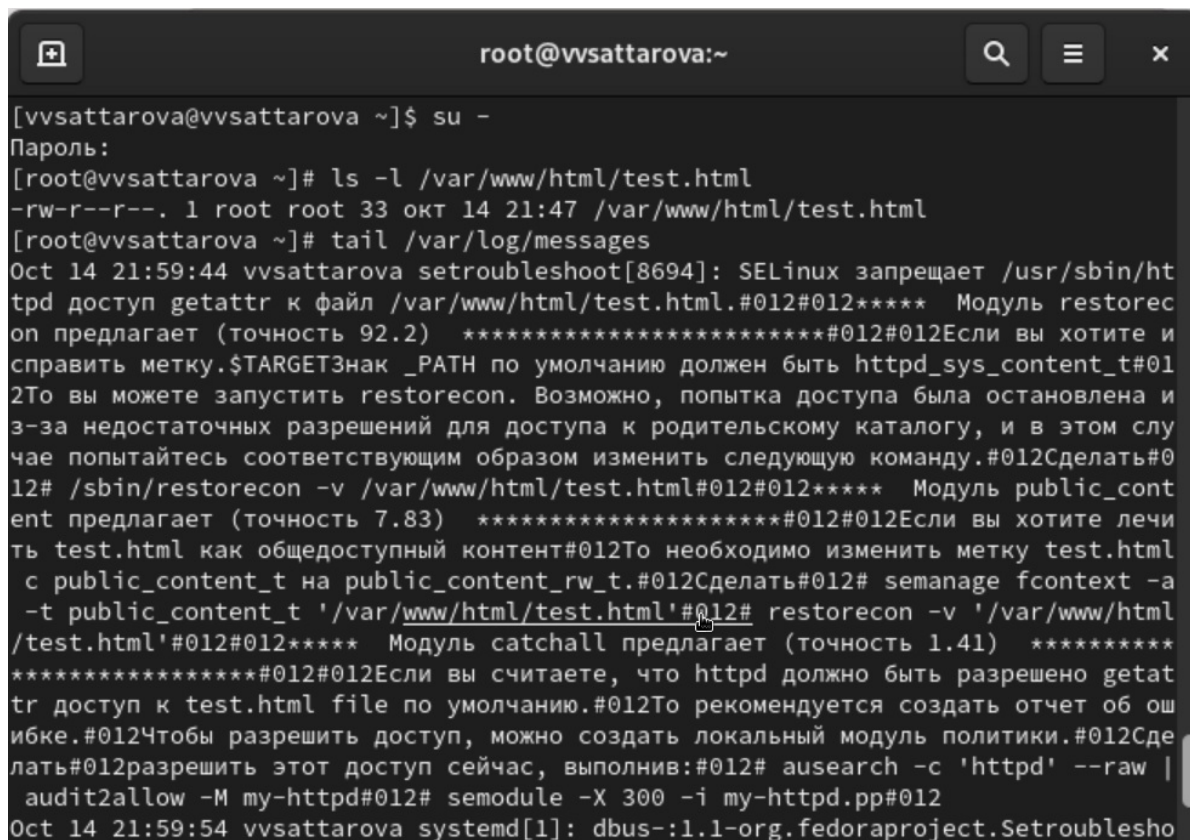


Рис. 7.13: Задание 14

14. Выполнила следующие задания:

- Проанализируйте 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 просмотрите системный лог-файл: `tail /var/log/messages` (рис. 7.14).



```
root@vvsattarova:~  
[vvsattarova@vvsattarova ~]$ su -  
Пароль:  
[root@vvsattarova ~]# ls -l /var/www/html/test.html  
-rw-r--r--. 1 root root 33 окт 14 21:47 /var/www/html/test.html  
[root@vvsattarova ~]# tail /var/log/messages  
Oct 14 21:59:44 vvsattarova setroubleshoot[8694]: SELinux запрещает /usr/sbin/ht  
tpd доступ getattr к файл /var/www/html/test.html.#012#012***** Модуль restorec  
on предлагает (точность 92.2) *****#012#012Если вы хотите и  
справить метку.$TARGETЗнак _PATH по умолчанию должен быть httpd_sys_content_t#01  
2То вы можете запустить restorecon. Возможно, попытка доступа была остановлена и  
з-за недостаточных разрешений для доступа к родительскому каталогу, и в этом слу  
чае попытайтесь соответствующим образом изменить следующую команду.#012Сделать#0  
12# /sbin/restorecon -v /var/www/html/test.html#012#012***** Модуль public_cont  
ent предлагает (точность 7.83) *****#012#012Если вы хотите лечи  
ть test.html как общедоступный контент#012То необходимо изменить метку test.html  
с public_content_t на public_content_rw_t.#012Сделать#012# semanage fcontext -a  
-t public_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html  
/test.html'#012#012***** Модуль catchall предлагает (точность 1.41) *****  
*****#012#012Если вы считаете, что httpd должно быть разрешено getat  
tr доступ к test.html file по умолчанию.#012То рекомендуется создать отчет об ош  
ибке.#012Чтобы разрешить доступ, можно создать локальный модуль политики.#012Сде  
лать#012разрешить этот доступ сейчас, выполнив:#012# ausearch -с 'httpd' --raw |  
audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012  
Oct 14 21:59:54 vvsattarova systemd[1]: dbus-:1.1-org.fedoraproject.Setroublesho
```

Рис. 7.14: Задание 15

15. Выполнила следующие задания:

- Попробуйте 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. 7.15).

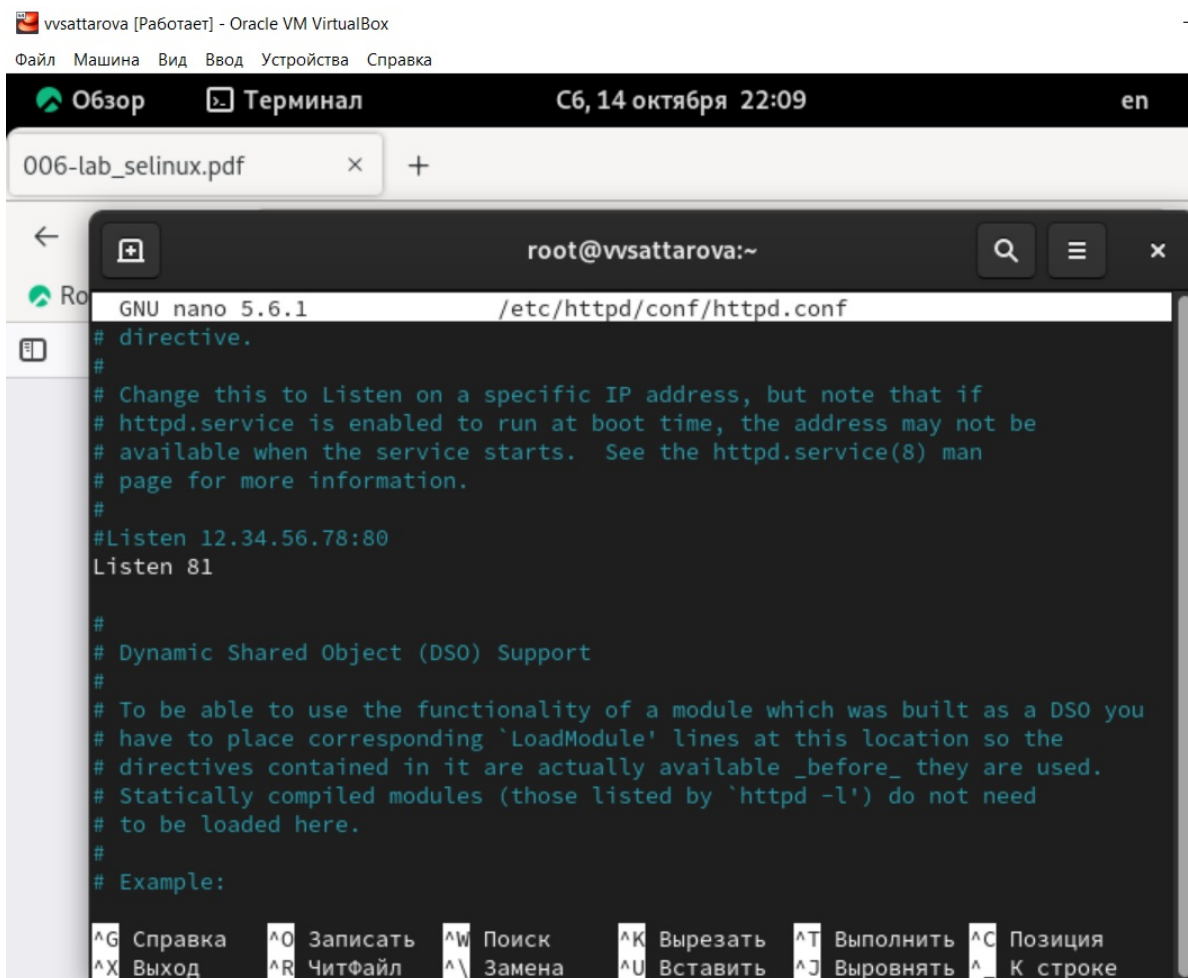


Рис. 7.15: Задание 16

16. Выполнила следующие задания:

- Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему? (рис. 7.16).

```
root@wsattarova:~  
[root@vvsattarova ~]# nano /etc/httpd/conf/httpd.conf  
[root@vvsattarova ~]# service httpd restart  
Redirecting to /bin/systemctl restart httpd.service  
[root@vvsattarova ~]# 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; preset: disabled)  
   Active: active (running) since Sat 2023-10-14 22:10:56 MSK; 13s ago  
     Docs: man:httpd.service(8)  
  Main PID: 8969 (httpd)  
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0; CPU usage: 0%"  
    Tasks: 213 (limit: 4472)  
   Memory: 23.9M  
      CPU: 113ms  
   CGroup: /system.slice/httpd.service  
           └─8969 /usr/sbin/httpd -DFOREGROUND  
             └─8970 /usr/sbin/httpd -DFOREGROUND  
               └─8971 /usr/sbin/httpd -DFOREGROUND  
                 └─8972 /usr/sbin/httpd -DFOREGROUND  
                   └─8973 /usr/sbin/httpd -DFOREGROUND  
  
окт 14 22:10:56 vvsattarova systemd[1]: Starting The Apache HTTP Server...  
окт 14 22:10:56 vvsattarova httpd[8969]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, setting 'ServerName' to localhost.  
окт 14 22:10:56 vvsattarova systemd[1]: Started The Apache HTTP Server.  
окт 14 22:10:56 vvsattarova httpd[8969]: Server configured, listening on: port 80  
[root@vvsattarova ~]#
```

Рис. 7.16: Задание 17

17. Выполнила следующие задания:

- Проанализируйте лог-файлы: `tail -nl /var/log/messages`. 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 (рис. 7.17).

```
root@wsattarova:~  
[root@vvsattarova ~]# tail /var/log/messages  
Oct 14 22:10:56 vvsattarova httpd[8969]: AH00558: httpd: Could not reliably deter  
ine the server's fully qualified domain name, using fe80::a00:27ff:fe4f:53ba%enp0  
3. Set the 'ServerName' directive globally to suppress this message  
Oct 14 22:10:56 vvsattarova systemd[1]: Started The Apache HTTP Server.  
Oct 14 22:10:56 vvsattarova httpd[8969]: Server configured, listening on: port 81  
[root@vvsattarova ~]# tail /var/log/httpd/error_log  
[Sat Oct 14 22:10:56.601610 2023] [lbmethod_heartbeat:notice] [pid 8969:tid 8969]  
AH02282: No slotmem from mod_heartbeat  
[Sat Oct 14 22:10:56.611024 2023] [mpm_event:notice] [pid 8969:tid 8969] AH00489:  
Apache/2.4.53 (Rocky Linux) configured -- resuming normal operations  
[Sat Oct 14 22:10:56.611081 2023] [core:notice] [pid 8969:tid 8969] AH00094: Comm  
nd line: '/usr/sbin/httpd -D FOREGROUND'  
[root@vvsattarova ~]# tail /var/log/httpd/access_log  
127.0.0.1 - - [14/Oct/2023:22:10:08 +0300] "GET /test.html HTTP/1.1" 403 199 "-"  
Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"  
127.0.0.1 - - [14/Oct/2023:22:10:12 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "h  
tp://127.0.0.1/test.html" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201001  
1 Firefox/102.0"  
[root@vvsattarova ~]# tail /var/log/audit/audit.log  
type=SERVICE_START msg=audit(1697311217.761:202): pid=1 uid=0 auid=4294967295 ses  
4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dnf-makecache comm="systemd  
exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root  
" AUID="unset"  
type=SERVICE_STOP msg=audit(1697311217.762:203): pid=1 uid=0 auid=4294967295 ses=  
294967295 subj=system_u:system_r:init_t:s0 msg='unit=dnf-makecache comm="systemd"  
exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root  
AUID="unset"
```

Рис. 7.17: Задание 18

18. Выполнила следующие задания:

- Выполните команду `semanage port -a -t http_port_t -p tcp 81` После этого про
верьте список портов командой `semanage port -l | grep http_port_t` Убедитесь,
что порт 81 появился в списке (рис. 7.18).


```

[root@vvsattarova ~]# semanage port -a -t http_port_t -p tcp 81
usage: semanage [-h]
                {import,export,login,user,port,ibpkey,ibendport,interface,module,n
ode,fcontext,boolean,permissive,dontaudit}
                ...
semanage: error: unrecognized arguments: -p 81
[root@vvsattarova ~]# 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@vvsattarova ~]#

```

Рис. 7.18: Задание 19

19. Выполнила следующие задания:

- Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему он сейчас запустился, а в предыдущем случае не смог? (рис. 7.19).

```

root@vwsattarova:~
pegasus_http_port_t          tcp      5988
[root@vvsattarova ~]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@vvsattarova ~]# 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; preset: disabled)
   Active: active (running) since Sat 2023-10-14 22:31:58 MSK; 5s ago
     Docs: man:httpd.service(8)
  Main PID: 9274 (httpd)
    Status: "Started, listening on: port 81"
    Tasks: 213 (limit: 4472)
   Memory: 23.8M
      CPU: 118ms
   CGroup: /system.slice/httpd.service
           └─9274 /usr/sbin/httpd -DFOREGROUND
             └─9275 /usr/sbin/httpd -DFOREGROUND
               └─9276 /usr/sbin/httpd -DFOREGROUND
                 └─9277 /usr/sbin/httpd -DFOREGROUND
                   └─9278 /usr/sbin/httpd -DFOREGROUND

окт 14 22:31:58 vvsattarova systemd[1]: Starting The Apache HTTP Server...
окт 14 22:31:58 vvsattarova httpd[9274]: AH00558: httpd: Could not reliably deter
окт 14 22:31:58 vvsattarova systemd[1]: Started The Apache HTTP Server.
окт 14 22:31:58 vvsattarova httpd[9274]: Server configured, listening on: port 81
lines 1-20/20 (END)

```

Рис. 7.19: Задание 20

20. Выполните следующие задания:

- Верните 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 попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. Вы должны увидеть содержимое файла — слово «test».
- Исправьте обратно конфигурационный файл `apache`, вернув `Listen 80`.
- Удалите привязку `http_port_t` к 81 порту: `semanage port -d -t http_port_t -p tcp 81` и проверьте, что порт 81 удалён.
- Удалите файл `/var/www/html/test.html`: `rm /var/www/html/test.html` (рис. 7.20).

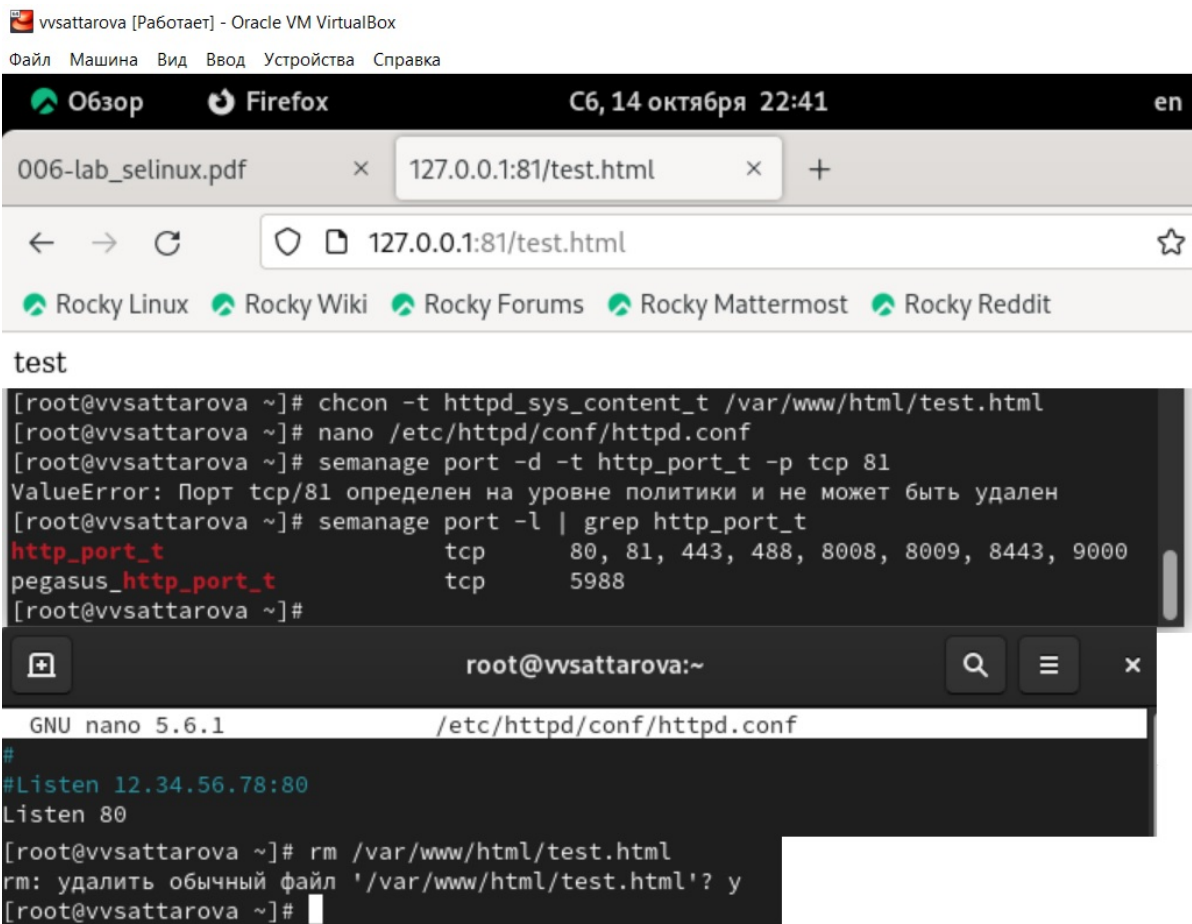


Рис. 7.20: Задания 21-24

8 Анализ результатов

Таким образом, были выполнены задания по изучению администрирования, SELinux, веб-сервера Apache.

9 Заключение и выводы

Таким образом, в ходе выполнения лабораторной работы было сделано следующее:

- Развиты навыки администрирования ОС Linux.
- Получено первое практическое знакомство с технологией SELinux.
- Проверена работа SELinux на практике совместно с веб-сервером Apache.
- Написан отчёт к лабораторной работе.

10 Список литературы

[1]

1. Информационная безопасность [Электронный ресурс]. Российский университет дружбы народов, 2023. URL: https://esystem.rudn.ru/pluginfile.php/2090282/mod_resource/content/2/006-lab_selinux.pdf.