

Отчёт по лабораторной работе №6

дисциплина: Информационная безопасность

Морозова Ульяна

Содержание

1	Цель работы	4
2	Подготовка к лабораторной работе	5
3	Выполнение лабораторной работы	7
4	Выводы	18

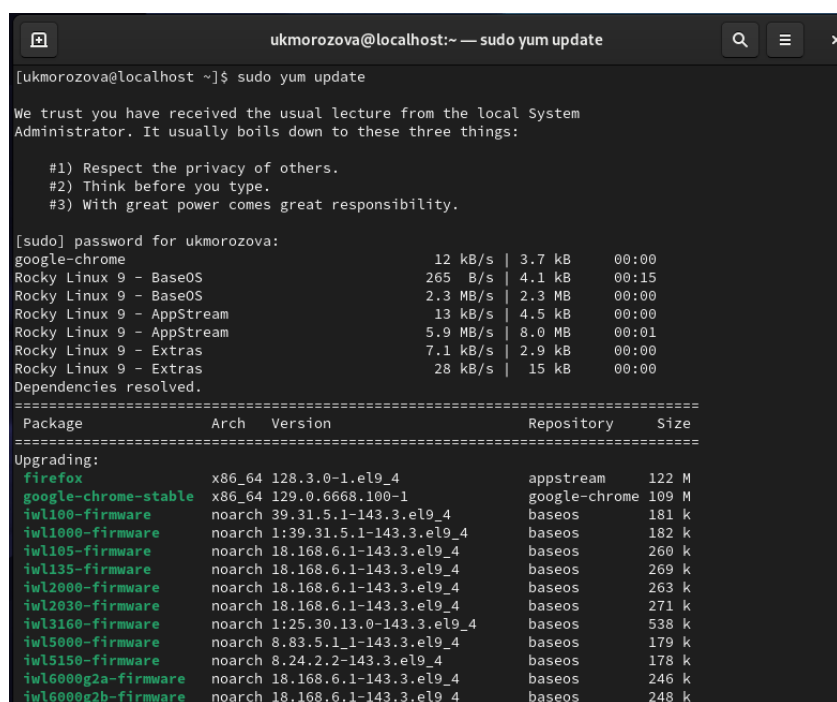
Список иллюстраций

2.1	Установка обновлений	5
2.2	Скачивание Apache	6
3.1	getenforce и sestatus	7
3.2	httpd	8
3.3	веб-сервер Apache	8
3.4	переключатели SELinux	9
3.5	seinfo	10
3.6	/var/www	10
3.7	/var/www/html	10
3.8	Создание файла	11
3.9	test.html	11
3.10	контекст test.html	11
3.11	test.html	11
3.12	Изменение контекста	12
3.13	Ошибка	12
3.14	log-файлы веб-сервера Apache	13
3.15	Listen 81	14
3.16	лог-файлы	14
3.17	error_log	15
3.18	semanage port	15
3.19	веб-сервер Apache	16
3.20	Listen 80	16
3.21	порт 81	16
3.22	Удаление файла	17

1 Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux¹. Проверить работу SELinx на практике совместно с веб-сервером Apache.

2 Подготовка к лабораторной работе



```
[ukmorozova@localhost ~]$ sudo yum update

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

 #1) Respect the privacy of others.
 #2) Think before you type.
 #3) With great power comes great responsibility.

[sudo] password for ukmorozova:
google-chrome                12 kB/s | 3.7 kB      00:00
Rocky Linux 9 - BaseOS       265 B/s | 4.1 kB      00:15
Rocky Linux 9 - BaseOS       2.3 MB/s | 2.3 MB      00:00
Rocky Linux 9 - AppStream     13 kB/s | 4.5 kB      00:00
Rocky Linux 9 - AppStream     5.9 MB/s | 8.0 MB      00:01
Rocky Linux 9 - Extras        7.1 kB/s | 2.9 kB      00:00
Rocky Linux 9 - Extras        28 kB/s | 15 kB      00:00
Dependencies resolved.
=====
Package                        Arch      Version              Repository            Size
=====
Upgrading:
firefox                        x86_64    128.3.0-1.el9_4      appstream              122 M
google-chrome-stable           x86_64    129.0.6668.100-1     google-chrome          109 M
iwl100-firmware                noarch    39.31.5.1-143.3.el9_4 baseos                 181 k
iwl1000-firmware               noarch    1:39.31.5.1-143.3.el9_4 baseos                 182 k
iwl105-firmware                noarch    18.168.6.1-143.3.el9_4 baseos                 260 k
iwl135-firmware                noarch    18.168.6.1-143.3.el9_4 baseos                 269 k
iwl2000-firmware                noarch    18.168.6.1-143.3.el9_4 baseos                 263 k
iwl2030-firmware                noarch    18.168.6.1-143.3.el9_4 baseos                 271 k
iwl13160-firmware              noarch    1:25.30.13.0-143.3.el9_4 baseos                 538 k
iwl5000-firmware                noarch    8.83.5.1-1-143.3.el9_4 baseos                 179 k
iwl5150-firmware                noarch    8.24.2.2-143.3.el9_4 baseos                 178 k
iwl6000g2a-firmware            noarch    18.168.6.1-143.3.el9_4 baseos                 246 k
iwl6000g2b-firmware            noarch    18.168.6.1-143.3.el9_4 baseos                 248 k
```

Рис. 2.1: Установка обновлений

```
[ukmorofova@localhost ~]$ sudo yum -y install httpd
[sudo] password for ukmorofova:
google-chrome                                     6.7 kB/s | 1.3 kB    00:00
Dependencies resolved.
=====
Package                Architecture      Version              Repository          Size
=====
Installing:
httpd                  x86_64            2.4.57-11.el9_4.1    appstream            44 k
Installing dependencies:
apr                    x86_64            1.7.0-12.el9_3       appstream            122 k
apr-util               x86_64            1.6.1-23.el9         appstream            94 k
apr-util-bdb           x86_64            1.6.1-23.el9         appstream            12 k
httpd-core              x86_64            2.4.57-11.el9_4.1    appstream            1.4 M
httpd-filesystem        noarch            2.4.57-11.el9_4.1    appstream            11 k
httpd-tools             x86_64            2.4.57-11.el9_4.1    appstream            79 k
rocky-logos-httpd       noarch            90.15-2.el9          appstream            24 k
Installing weak dependencies:
apr-util-openssl        x86_64            1.6.1-23.el9         appstream            14 k
mod_http2               x86_64            2.0.26-2.el9_4       appstream            162 k
mod_lua                 x86_64            2.4.57-11.el9_4.1    appstream            58 k
Transaction Summary
=====
Install 11 Packages

Total download size: 2.0 M
Installed size: 6.0 M
Downloading Packages:
(1/11): mod_lua-2.4.57-11.el9_4.1.x86_64.rpm          444 kB/s | 58 kB    00:00
(2/11): httpd-tools-2.4.57-11.el9_4.1.x86_64.rpm      444 kB/s | 79 kB    00:00
(3/11): httpd-2.4.57-11.el9_4.1.x86_64.rpm           881 kB/s | 44 kB    00:00
```

Рис. 2.2: Скачивание Apache

3 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` (рис. 3.1).

```
[ukmorofova@localhost ~]$ getenforce
Enforcing
[ukmorofova@localhost ~]$ sestatus
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:      /etc/selinux
Loaded policy name:            targeted
Current mode:                  enforcing
Mode from config file:        enforcing
Policy MLS status:             enabled
Policy deny_unknown status:    allowed
Memory protection checking:    actual (secure)
Max kernel policy version:     33
```

Рис. 3.1: `getenforce` и `sestatus`

2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает:

```
service httpd status
```

Если не работает, запустите его так же, но с параметром `start` (рис. 3.2).

```
[ukmorofova@localhost ~]$ sudo systemctl start httpd
[ukmorofova@localhost ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
   Active: active (running) since Thu 2024-10-10 17:58:32 MSK; 6s ago
     Docs: man:httpd.service(8)
   Main PID: 29253 (httpd)
    Status: "Started, listening on: port 80"
     Tasks: 177 (limit: 23036)
    Memory: 22.0M
       CPU: 101ms
   CGroup: /system.slice/httpd.service
           └─29253 /usr/sbin/httpd -DFOREGROUND
             └─29254 /usr/sbin/httpd -DFOREGROUND
               └─29255 /usr/sbin/httpd -DFOREGROUND
                 └─29256 /usr/sbin/httpd -DFOREGROUND
                   └─29257 /usr/sbin/httpd -DFOREGROUND

Oct 10 17:58:32 localhost.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 10 17:58:32 localhost.localdomain httpd[29253]: AH00558: httpd: Could not reliably determine
Oct 10 17:58:32 localhost.localdomain httpd[29253]: Server configured, listening on: port 80
Oct 10 17:58:32 localhost.localdomain systemd[1]: Started The Apache HTTP Server.
lines 1-20/20 (END)
```

Рис. 3.2: httpd

3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт (рис. 3.3). Например, можно использовать команду

```
ps auxZ | grep httpd
```

```
[ukmorofova@localhost ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 29253 0.0 0.3 20152 11316 ? Ss 17:58 0:0
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 29254 0.0 0.1 22032 7364 ? S 17:58 0:0
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 29255 0.0 0.3 1440204 11256 ? Sl 17:58 0:0
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 29256 0.0 0.3 1571340 13504 ? Sl 17:58 0:0
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 29257 0.0 0.2 1440204 11188 ? Sl 17:58 0:0
0 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 ukmorofo+ 29437 0.0 0.2 236780 9128 pts/0 S
+ 17:58 0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 ukmorofo+ 29497 0.0 0.0 221796 2432 pts/1 S
+ 18:03 0:00 grep --color=auto httpd
[ukmorofova@localhost ~]$
```

Рис. 3.3: веб-сервер Apache

4. Посмотрите текущее состояние переключателей SELinux для Apache помощью команды

```
sestatus -bigrep httpd
```

Обратите внимание, что многие из них находятся в положении «off» (рис. 3.4).


```
[ukmorofova@localhost ~]$ sestatus -b httpd
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:       /etc/selinux
Loaded policy name:            targeted
Current mode:                  enforcing
Mode from config file:         enforcing
Policy MLS status:             enabled
Policy deny_unknown status:    allowed
Memory protection checking:    actual (secure)
Max kernel policy version:    33

Policy booleans:
abrt_anon_write                off
abrt_handle_event              off
abrt_upload_watch_anon_write   on
antivirus_can_scan_system      off
antivirus_use_jit              off
auditadm_exec_content          on
authlogin_nsswitch_use_ldap    off
authlogin_radius               off
authlogin_yubikey              off
awstats_purge_apache_log_files off
boinc_execmem                  on
cdrecord_read_content          off
cluster_can_network_connect    off
cluster_manage_all_files       off
cluster_use_execmem            off
cobbler_anon_write             off
cobbler_can_network_connect    off
cobbler use cifs               off
```

Рис. 3.4: переключатели SELinux

5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов (рис. 3.5).

```
[ukmorofova@localhost ~]$ 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:                   5145     Attributes:           259
Users:                   8         Roles:                 15
Booleans:                356     Cond. Expr.:         388
Allow:                   65504    Neverallow:           0
Auditallow:              176     Dontaudit:            8682
Type_trans:              271770  Type_change:          94
Type_member:              37      Range_trans:          5931
Role_allow:              40       Role_trans:           417
Constraints:              70      Validatetrans:         0
MLS Constrain:           72      MLS Val. Tran:         0
Permissives:              4       Polcap:                6
Defaults:                 7       Typebounds:            0
Allowxperm:               0       Neverallowxperm:       0
Auditallowxperm:          0       Dontauditxperm:        0
Ibendportcon:             0       Ibpkeycon:             0
Initial SIDs:             27      Fs_use:                35
Genfscon:                 109     Portcon:               665
Netifcon:                  0       Nodecon:               0
[ukmorofova@localhost ~]$
```

Рис. 3.5: seinfo

- Определите тип файлов и поддиректорий (рис. 3.6), находящихся в директории /var/www, с помощью команды

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

```
[ukmorofova@localhost ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Aug 8 19:30 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Aug 8 19:30 html
```

Рис. 3.6: /var/www

- Определите тип файлов (рис. 3.7), находящихся в директории /var/www/html:

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

```
[ukmorofova@localhost ~]$ ls -lZ /var/www/html
total 0
```

Рис. 3.7: /var/www/html

- Создайте от имени суперпользователя html-файл /var/www/html/test.html следующего содержания (рис. 3.8 - рис. 3.9):

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

```
[ukmorofova@localhost ~]$ sudo touch /var/www/html/test.html
[sudo] password for ukmorofova:
[ukmorofova@localhost ~]$ sudo gedit /var/www/html/test.html
```

Рис. 3.8: Создание файла

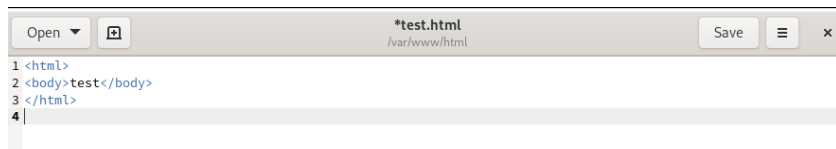


Рис. 3.9: test.html

9. Проверьте контекст созданного вами файла (рис. 3.10). Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html.

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

[ukmorofova@localhost ~]$ ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 Oct 10 18:09 test.html
```

Рис. 3.10: контекст test.html

10. Обратитесь к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html> (рис. 3.11). Убедитесь, что файл был успешно отображён.

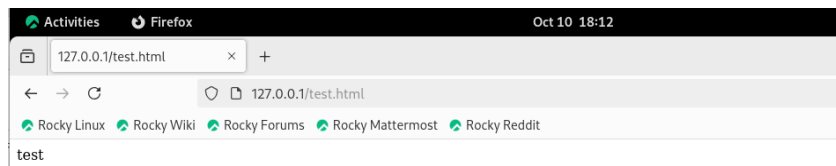


Рис. 3.11: test.html

11. Проверьте контекст файла командой

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

Измените контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на любой другой (рис. 3.12), 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
```



```
[ukmorofova@localhost ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[ukmorofova@localhost ~]$ chcon -t samba_share_t /var/www/html/test.html
chcon: failed to change context of '/var/www/html/test.html' to 'unconfined_u:object_r:samba_share_t:s0': Operation not permitted
[ukmorofova@localhost ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[ukmorofova@localhost ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[ukmorofova@localhost ~]$
```

Рис. 3.12: Изменение контекста

12. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html` (рис. 3.13). Вы должны получить сообщение об ошибке: `Forbidden You don't have permission to access /test.html on this server.`

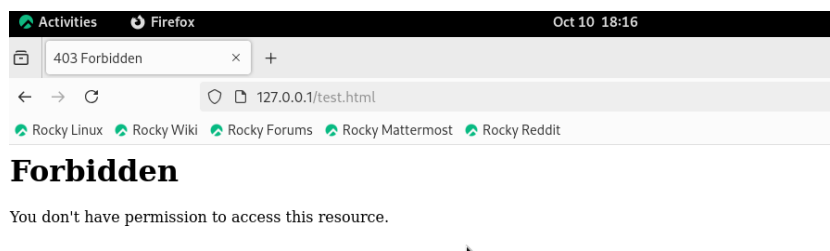


Рис. 3.13: Ошибка

13. 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 (рис. 3.14). Также просмотрите системный лог-файл:

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

```
[ukmorofova@localhost ~]$ ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 34 Oct 10 18:09 /var/www/html/test.html
[ukmorofova@localhost ~]$ sudo tail /var/www/html/test.html
<html>
<body>test</body>
</html>

[ukmorofova@localhost ~]$ sudo tail /var/log/messages
Oct 10 18:16:20 localhost setroubleshoot[30495]: failed to retrieve rpm info for path '/var/www/html/test.html':
Oct 10 18:16:20 localhost systemd[1]: Created slice Slice /system/dbus-1.1-org.fedoraproject.SetroubleshootPrivileged.
Oct 10 18:16:20 localhost systemd[1]: Started dbus-1.1-org.fedoraproject.SetroubleshootPrivileged.service.
Oct 10 18:16:23 localhost setroubleshoot[30495]: SELinux is preventing /usr/sbin/httpd from getting access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 04d5c87a-8095-4188-97d3-369f0ad06bf7
Oct 10 18:16:23 localhost setroubleshoot[30495]: SELinux is preventing /usr/sbin/httpd from getting 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 htt
```

Рис. 3.14: log-файлы веб-сервера Apache

14. 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. 3.15).

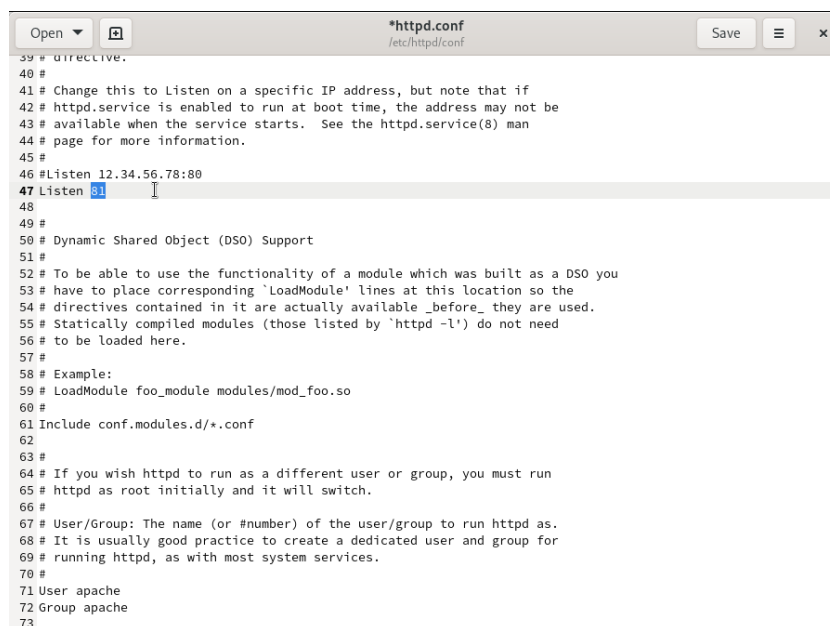


Рис. 3.15: Listen 81

15. Проанализируйте лог-файлы (рис. 3.16):

```
tail -n1 /var/log/messages
```

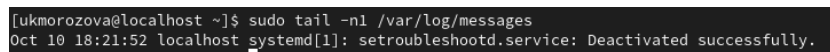


Рис. 3.16: лог-файлы

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. 3.17).

```
[ukmorofova@localhost ~]$ sudo tail /var/log/messages
Oct 10 18:16:20 localhost setroubleshoot[30495]: failed to retrieve rpm info for path '/var/www/html/test.html':
Oct 10 18:16:20 localhost systemd[1]: Created slice Slice /system/dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged.
Oct 10 18:16:20 localhost systemd[1]: Started dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service.
Oct 10 18:16:23 localhost setroubleshoot[30495]: SELinux is preventing /usr/sbin/httpd from getting access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 04d5c87a-8095-4188-97d3-369f0ad06bf7
Oct 10 18:16:23 localhost setroubleshoot[30495]: SELinux is preventing /usr/sbin/httpd from getting 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 to get 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 -q 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct 10 18:16:23 localhost setroubleshoot[30495]: SELinux is preventing /usr/sbin/httpd from getting access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 04d5c87a-8095-4188-97d3-369f0ad06bf7
Oct 10 18:16:23 localhost setroubleshoot[30495]: SELinux is preventing /usr/sbin/httpd from getting 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/
```

Рис. 3.17: error_log

16. 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 (рис. 3.18).

```
[ukmorofova@localhost ~]$ sudo semanage port -a -t http_port_t -p tcp 81
Port tcp/81 already defined, modifying instead
[ukmorofova@localhost ~]$ semanage port -l | grep http_port_t
ValueError: SELinux policy is not managed or store cannot be accessed.
[ukmorofova@localhost ~]$ sudo 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
```

Рис. 3.18: semanage port

17. 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» (рис. 3.19).

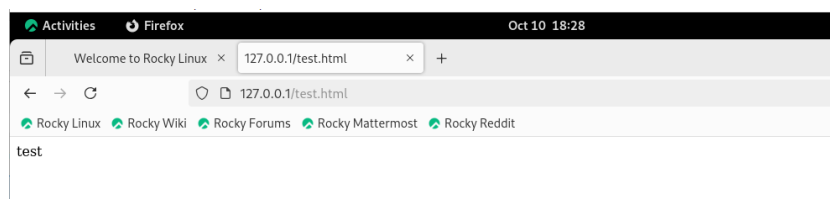


Рис. 3.19: веб-сервер Apache

18. Исправьте обратно конфигурационный файл apache, вернув Listen 80 (рис. 3.20).

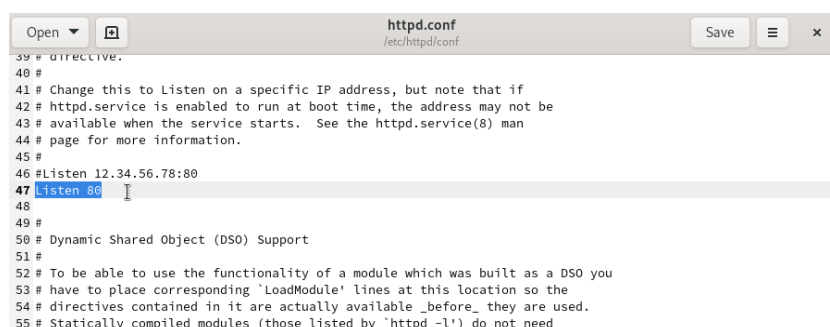


Рис. 3.20: Listen 80

19. Удалите привязку `http_port_t` к 81 порту:

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

и проверьте, что порт 81 удалён (рис. 3.21).

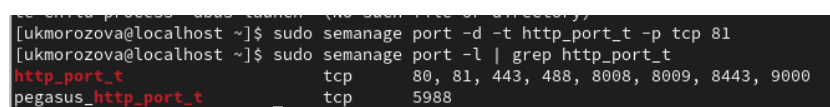
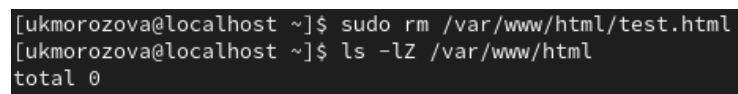


Рис. 3.21: порт 81

24. Удалите файл `/var/www/html/test.html` (рис. 3.22):


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

A terminal window with a dark background. The prompt is [ukmorofova@localhost ~]. The first command is sudo rm /var/www/html/test.html. The second command is ls -lZ /var/www/html. The output is total 0.

```
[ukmorofova@localhost ~]$ sudo rm /var/www/html/test.html
[ukmorofova@localhost ~]$ ls -lZ /var/www/html
total 0
```

Рис. 3.22: Удаление файла

4 Выводы

Развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux¹. Проверили работу SELinx на практике совместно с веб-сервером Apache.