Отчёт по лабораторной работе №6

Дисциплина: Информационная безопасность

Андрианова Марина Георгиевна

Содержание

Цель работы

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

Выполнение лабораторной работы

Вошла в систему под своей учетной записью. Убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus (рис. [-@fig:001]).

```
[mgandrianova@localhost ~]$ getenforce
Enforcing
[mgandrianova@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
[mgandrianova@localhost ~]$
```

Проверка режима работы SELinux

Запускаю сервер apache, далее обращаюсь с помощью браузера к веб-серверу, запущенному на компьютере, он работает, что видно из вывода команды `service httpd status` (рис. [-@fig:002]).

```
[mgandrianova@localhost ~]$ sudo systemctl start httpd
[sudo] пароль для mgandrianova:
[mgandrianova@localhost ~]$ sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[mgandrianova@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; enabled; preset: disabled)
     Active: active (running) since Wed 2024-10-09 21:10:51 MSK; 1min 29s ago
       Docs: man:httpd.service(8)
   Main PID: 2860 (httpd)
     Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec:   0 B/sec"
      Tasks: 177 (limit: 10980)
     Memory: 38.2M
        CPU: 727ms
     CGroup: /system.slice/httpd.service
             ├─2860 /usr/sbin/httpd -DFOREGROUND
             ├─2861 /usr/sbin/httpd -DFOREGROUND
             ├─2862 /usr/sbin/httpd -DFOREGROUND
             ├─2863 /usr/sbin/httpd -DFOREGROUND
             └─2868 /usr/sbin/httpd -DFOREGROUND

окт 09 21:10:50 localhost.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 09 21:10:50 localhost.localdomain httpd[2860]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using localhost.loc>
окт 09 21:10:51 localhost.localdomain systemd[1]: Started The Apache HTTP Server.
окт 09 21:10:51 localhost.localdomain httpd[2860]: Server configured, listening on: port 80
lines 1-20/20 (END)
```

Проверка работы Apache

С помощью команды `ps auxZ | grep httpd` нашла веб-сервер Apache в списке процессов. Его контекст безопасности - httpd_t (рис. [-@fig:003]).

```
[mgandrianova@localhost ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root        2860  0.1  0.6  20152 11432 ?        Ss   21:10   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      2861  0.0  0.4  22032  7356 ?        S    21:10   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      2862  0.1  0.9 1112588 17612 ?       Sl   21:10   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      2863  0.0  0.8 981452 15340 ?        Sl   21:10   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      2868  0.1  0.8 981452 15344 ?        Sl   21:10   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 mgandri+ 3132 0.0  0.1 221688 2560 pts/0 S+ 21:14   0:00 grep --color=auto httpd
[mgandrianova@localhost ~]$
```

Контекст безопасности Apache

Просмотрела текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd` (рис. [-@fig:004]).

Состояние переключателей SELinux

Просмотрела статистику по политике с помощью команды `seinfo`. Множество пользователей - 8, ролей - 40, типов - 5145. (рис. [-@fig:005]).

```
[mgandrianova@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
[mgandrianova@localhost ~]$
```

Статистика по политике

Типы поддиректорий, находящихся в директории `/var/www`, нашли с помощью команды `ls -lZ /var/www`, они следующие: владелец - root, права на изменения только у владельца. Файлов в директории нет (рис. [-@fig:006]).

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

Типы поддиректорий

В директории `/var/www/html` нет файлов. (рис. [-@fig:007]).

```
[mgandrianova@localhost ~]$ ls -lZ /var/www/html
итого 0
```

Типы файлов

Создать файл может только суперпользователь, поэтому от его имени создаем файл touch.html со следующим содержанием:

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

(рис. [-@fig:008]).

```
[mgandrianova@localhost ~]$ sudo touch /var/www/html/test.html
[sudo] пароль для mgandrianova:
[mgandrianova@localhost ~]$ sudo nano /var/www/html/test.html
[mgandrianova@localhost ~]$ sudo cat /var/www/html/test.html
<html>
<bosy>test</body>
</html>
```

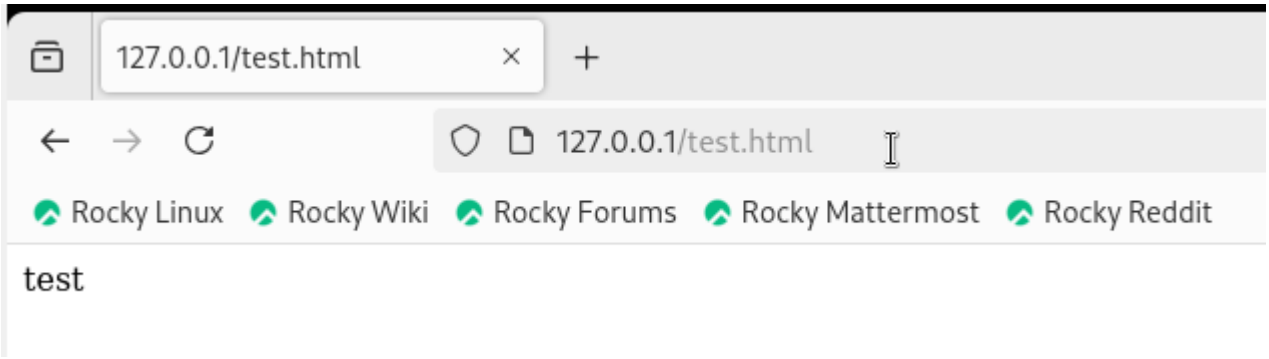
Создание файла

Проверяю контекст созданного файла. По умолчанию это httpd_sys_content_t (рис. [-@fig:009]).

```
[mgandrianova@localhost ~]$ ls -lZ /var/www/html/
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 окт  9 21:22 test.html
```

Контекст файла

Обращаюсь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Файл был успешно отображён (рис. [-@fig:010]).



Отображение файла

Изучила справку man httpd_selinux. Справочной страницы не оказалось (рис. [-@fig:011]). Проверила контекст файла командой ls -Z. Рассмотрим полученный контекст детально. Так как по умолчанию пользователи CentOS являются свободными от типа (unconfined в переводе с англ. означает свободный), созданному нами файлу test.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 умолчанию для файлов на «постоянных» носителях и на сетевых файловых системах. (В директории /proc файлы, относящиеся к процессам, могут иметь роль system_r. 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. (рис. [-@fig:011]).

```
[mgandrianova@localhost ~]$ man httpd_selinux
Нет справочной страницы для httpd_selinux
[mgandrianova@localhost ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
```

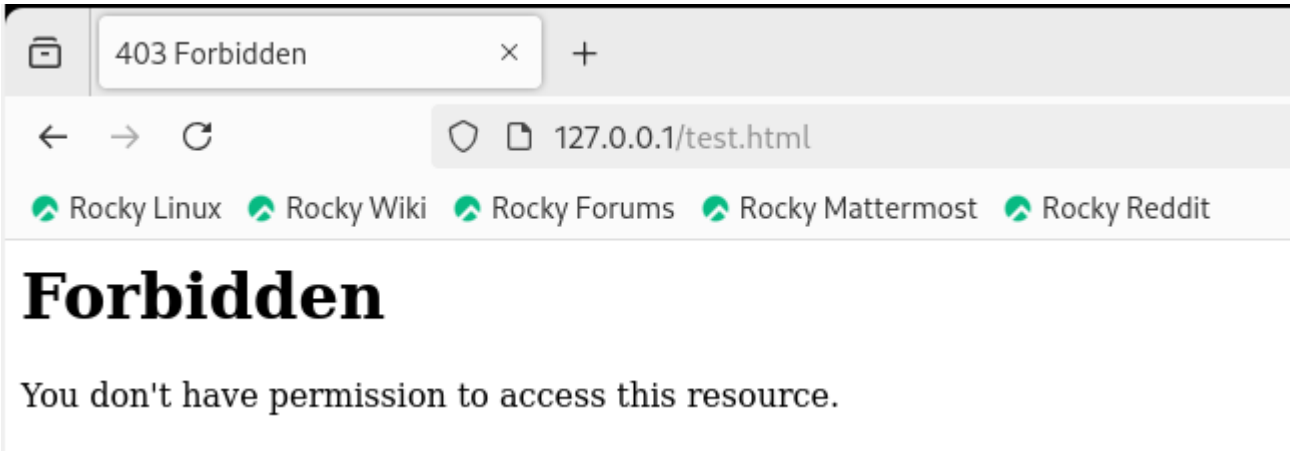
Изучение справки по команде

Изменяю 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` Контекст действительно поменялся (рис. [-@fig:012]).

```
[mgandrianova@localhost ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[sudo] пароль для mgandrianova:
[mgandrianova@localhost ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

Изменение контекста

При попытке отображения файла в браузере получаем сообщение об ошибке (рис. [-@fig:013]).



Отображение файла

Файл не был отображён, хотя права доступа позволяют читать этот файл любому пользователю (рис. [-@fig:014]), потому что установлен контекст, к которому процесс httpd не должен иметь доступа.

```
[mgandrianova@localhost ~]$ ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 окт  9 21:22 /var/www/html/test.html
```

Права доступа

Просматриваю log-файлы веб-сервера Apache (рис. [-@fig:015]) и системный лог-файл: `tail /var/log/messages`(рис. [-@fig:016]).

```
[mgandrianova@localhost ~]$ sudo tail /var/log/audit/audit.log
type=USER_ACCT msg=audit(1728498912.743:221): pid=4059 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:account
ing grantors=pam_unix,pam_localuser acct="mgandrianova" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="mgandrianova" AUID="mgandri
anova"
type=USER_CMD msg=audit(1728498912.743:222): pid=4059 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='cwd="/home/mgan
drianova" cmd=7461696C202F7661722F6C6F672F6D65737361676573 exe="/usr/bin/sudo" terminal=pts/0 res=success'UID="mgandrianova" AUID="mgandrianova"
type=CRED_REFR msg=audit(1728498912.751:223): pid=4059 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred
 grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="mgandrianova" AUID="mgandrianova"
type=USER_START msg=audit(1728498912.779:224): pid=4059 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:sessio
n_open grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="mgandrianov
a" AUID="mgandrianova"
type=USER_END msg=audit(1728498912.812:225): pid=4059 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session_
close grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="mgandrianova
" AUID="mgandrianova"
type=CRED_DISP msg=audit(1728498912.812:226): pid=4059 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred
 grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="mgandrianova" AUID="mgandrianova"
type=USER_ACCT msg=audit(1728498963.047:227): pid=4080 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:account
ing grantors=pam_unix,pam_localuser acct="mgandrianova" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="mgandrianova" AUID="mgandri
anova"
type=USER_CMD msg=audit(1728498963.047:228): pid=4080 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='cwd="/home/mgan
drianova" cmd=7461696C202F7661722F6C6F672F61756469742F61756469742E6C6F67 exe="/usr/bin/sudo" terminal=pts/0 res=success'UID="mgandrianova" AUID="mgandrianova"
type=CRED_REFR msg=audit(1728498963.075:229): pid=4080 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred
 grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="mgandrianova" AUID="mgandrianova"
type=USER_START msg=audit(1728498963.075:230): pid=4080 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:sessio
n_open grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="mgandrianov
a" AUID="mgandrianova"
[mgandrianova@localhost ~]$
```

Попытка прочесть лог-файл

```
[mgandrianova@localhost ~]$ sudo tail /var/log/messages
Oct  9 21:32:24 localhost systemd[1]: Created slice Slice /system/dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged.
Oct  9 21:32:24 localhost systemd[1]: Started dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service.
Oct  9 21:32:30 localhost setroubleshoot[4007]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/www/html/test.html. Для выполнения всех сообщений
 SELinux: sealert -l 5691fab9-3d50-46b5-b3b2-181b9c605c15
Oct  9 21:32:30 localhost setroubleshoot[4007]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/www/html/test.html.#012#012*****  Модуль restorec
on предлагает (точность 92.2)  ************************#012#012Если вы хотите исправить метку.$TARGETЗнак _PATH по умолчанию должен быть httpd_sys_content_t#
012То вы можете запустить restorecon. Возможно, попытка доступа была остановлена из-за недостаточных разрешений для доступа к родительскому каталогу, и в этом
 случае попытайтесь соответствующим образом изменить следующую команду.#012Сделать#012# /sbin/restorecon -v /var/www/html/test.html#012#012*****  Модуль publi
c_content предлагает (точность 7.83)  *********************#012#012Если вы хотите лечить test.html как общедоступный контент#012То необходимо изменить метку t
est.html с public_content_t на public_content_rw_t.#012Сделать#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v '/va
r/www/html/test.html'#012#012*****  Модуль catchall предлагает (точность 1.41)  ***************************#012#012Если вы считаете, что httpd должно быть раз
решено getattr доступ к test.html file по умолчанию.#012То рекомендуется создать отчет об ошибке.#012Чтобы разрешить доступ, можно создать локальный модуль по
литики.#012Сделать#012разрешить этот доступ сейчас, выполнив:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct  9 21:32:30 localhost setroubleshoot[4007]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/www/html/test.html. Для выполнения всех сообщений
 SELinux: sealert -l 5691fab9-3d50-46b5-b3b2-181b9c605c15
Oct  9 21:32:30 localhost setroubleshoot[4007]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/www/html/test.html.#012#012*****  Модуль restorec
on предлагает (точность 92.2)  ************************#012#012Если вы хотите исправить метку.$TARGETЗнак _PATH по умолчанию должен быть httpd_sys_content_t#
012То вы можете запустить restorecon. Возможно, попытка доступа была остановлена из-за недостаточных разрешений для доступа к родительскому каталогу, и в этом
 случае попытайтесь соответствующим образом изменить следующую команду.#012Сделать#012# /sbin/restorecon -v /var/www/html/test.html#012#012*****  Модуль publi
c_content предлагает (точность 7.83)  *********************#012#012Если вы хотите лечить test.html как общедоступный контент#012То необходимо изменить метку t
est.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 '/va
r/www/html/test.html'#012#012*****  Модуль catchall предлагает (точность 1.41)  ***************************#012#012Если вы считаете, что httpd должно быть раз
решено getattr доступ к test.html file по умолчанию.#012То рекомендуется создать отчет об ошибке.#012Чтобы разрешить доступ, можно создать локальный модуль по
литики.#012Сделать#012разрешить этот доступ сейчас, выполнив:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct  9 21:32:40 localhost systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Deactivated successfully.
Oct  9 21:32:40 localhost systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Consumed 2.261s CPU time.
Oct  9 21:32:41 localhost systemd[1]: setroubleshootd.service: Deactivated successfully.
Oct  9 21:32:41 localhost systemd[1]: setroubleshootd.service: Consumed 2.030s CPU time.
```

Попытка прочесть системный лог-файл

Чтобы запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services) открываю файл /etc/httpd/httpd.conf для изменения. (рис. [-@fig:017]).

```
[mgandrianova@localhost ~]$ sudo nano /etc/httpd/conf/httpd.conf
```

Изменение файла

Нахожу строчку Listen 80 и заменяю её на Listen 81. (рис. [-@fig:018]).

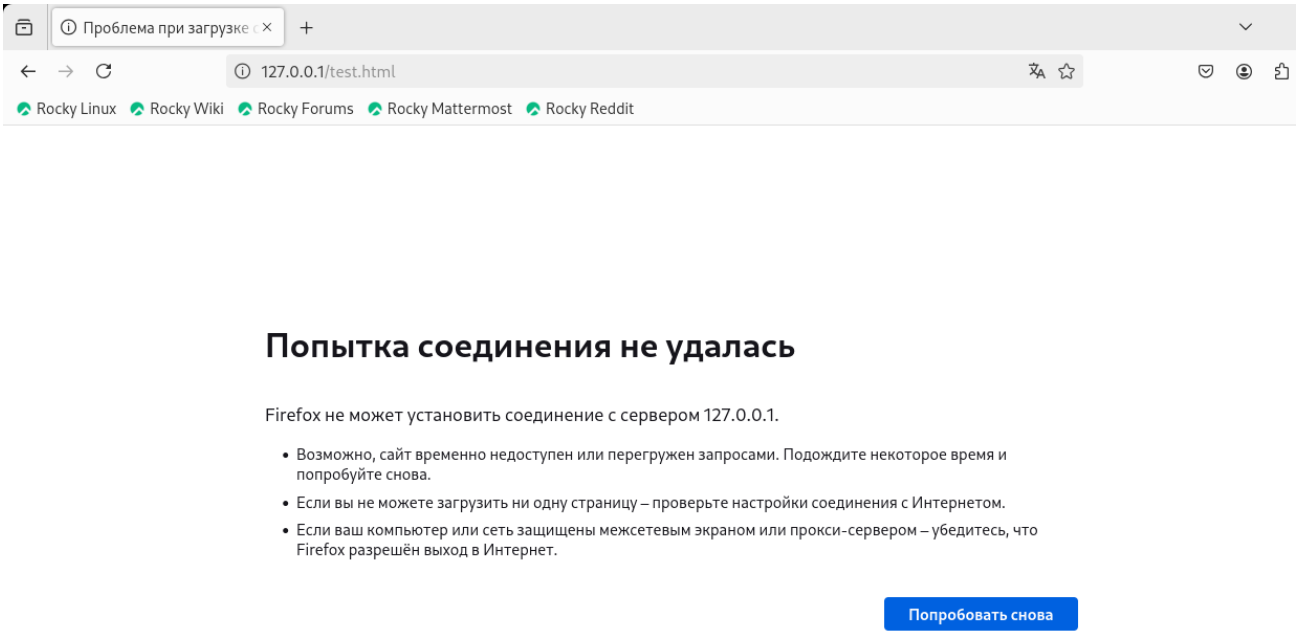
```
  GNU nano 5.6.1                                  /etc/httpd/conf/httpd.conf
# least PidFile.
#
ServerRoot "/etc/httpd"

#
# 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 a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts.  See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
Listen 81

#
# Dynamic Shared Object (DSO) Support
#
```

Изменение порта

Выполняю перезапуск веб-сервера Apache. Произошёл сбой, потому что порт 80 для локальной сети, а 81 нет (рис. [-@fig:019]).



Попытка прослушивания другого порта

Проанализируем лог-файлы: `tail -n1 /var/log/messages` (рис. [-@fig:020]).

```
[mgandrianova@localhost ~]$ sudo tail -n1 /var/log/messages
Oct  9 21:42:56 localhost systemd[1]: setroubleshootd.service: Consumed 1.375s CPU time.
```

Проверка лог-файлов

Просмотрела файлы `/var/log/http/error_log`(рис. [-@fig:021]), `/var/log/http/access_log`(рис. [-@fig:022]) и `/var/log/audit/audit.log`(рис. [-@fig:023]) и выяснила, в каких файлах появились записи. Запись появилась в файле error_log (рис. [-@fig:021]).

```
[mgandrianova@localhost ~]$ sudo cat /var/log/httpd/error_log
[Wed Oct 09 21:10:50.967219 2024] [core:notice] [pid 2860:tid 2860] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Wed Oct 09 21:10:50.974793 2024] [suexec:notice] [pid 2860:tid 2860] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using localhost.localdomain. Set the 'ServerName' directive globally to
 suppress this message
[Wed Oct 09 21:10:51.020701 2024] [lbmethod_heartbeat:notice] [pid 2860:tid 2860] AH02282: No slotmem from mod_heartmonitor
[Wed Oct 09 21:10:51.094759 2024] [mpm_event:notice] [pid 2860:tid 2860] AH00489: Apache/2.4.57 (Rocky Linux) configured -- resuming normal operations
[Wed Oct 09 21:10:51.094808 2024] [core:notice] [pid 2860:tid 2860] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[Wed Oct 09 21:32:17.302191 2024] [core:error] [pid 2868:tid 2965] (13)Permission denied: [client 127.0.0.1:57404] AH00035: access to /test.html denied (files
ystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Wed Oct 09 21:40:10.382464 2024] [core:error] [pid 2868:tid 2987] (13)Permission denied: [client 127.0.0.1:53564] AH00035: access to /test.html denied (files
ystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Wed Oct 09 21:40:51.946583 2024] [core:error] [pid 2868:tid 2984] (13)Permission denied: [client 127.0.0.1:33096] AH00035: access to /test.html denied (files
ystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Wed Oct 09 21:41:12.888745 2024] [core:error] [pid 2868:tid 3016] (13)Permission denied: [client 127.0.0.1:43038] AH00035: access to /test.html denied (files
ystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Wed Oct 09 21:41:14.282998 2024] [core:error] [pid 2868:tid 3012] (13)Permission denied: [client 127.0.0.1:43038] AH00035: access to /test.html denied (files
ystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Wed Oct 09 21:42:33.873245 2024] [core:error] [pid 2868:tid 3018] (13)Permission denied: [client 127.0.0.1:52002] AH00035: access to /test.html denied (files
ystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Wed Oct 09 21:42:45.243468 2024] [core:error] [pid 2868:tid 3013] (13)Permission denied: [client 127.0.0.1:55880] AH00035: access to /test.html denied (files
ystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[mgandrianova@localhost ~]$
```

Проверка лог-файлов

```
[mgandrianova@localhost ~]$ sudo cat /var/log/httpd/access_log
127.0.0.1 - - [09/Oct/2024:21:26:33 +0300] "GET /test.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 - - [09/Oct/2024:21:26:33 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/test.html" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/2
0100101 Firefox/128.0"
127.0.0.1 - - [09/Oct/2024:21:32:17 +0300] "GET /test.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 - - [09/Oct/2024:21:40:10 +0300] "GET /test.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 - - [09/Oct/2024:21:40:51 +0300] "GET /test.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 - - [09/Oct/2024:21:41:12 +0300] "GET /test.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 - - [09/Oct/2024:21:41:14 +0300] "GET /test.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 - - [09/Oct/2024:21:42:33 +0300] "GET /test.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 - - [09/Oct/2024:21:42:45 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
[mgandrianova@localhost ~]$
```

Проверка лог-файлов

```
[mgandrianova@localhost ~]$ sudo cat /var/log/audit/audit.log
type=DAEMON_START msg=audit(1727967546.257:565): op=start ver=3.1.2 format=enriched kernel=5.14.0-427.13.1.el9_4.x86_64 auid=4294967295 pid=674 uid=0 ses=4294
967295 subj=system_u:system_r:auditd_t:s0 res=successAUID="unset" UID="root"
type=SERVICE_START msg=audit(1727967546.335:5): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=systemd-journal-catalog-
update comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=CONFIG_CHANGE msg=audit(1727967546.735:6): op=set audit_backlog_limit=8192 old=64 auid=4294967295 ses=4294967295 subj=system_u:system_r:unconfined_servic
e_t:s0 res=1AUID="unset"
type=SYSCALL msg=audit(1727967546.735:6): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7ffd39b70fa0 a2=3c a3=0 items=0 ppid=679 pid=689 auid=429496729
5 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:unconfined
_service_t:s0 key=(null)ARCH=x86_64 SYSCALL=sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root
"
type=PROCTITLE msg=audit(1727967546.735:6): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C6573
type=CONFIG_CHANGE msg=audit(1727967546.738:7): op=set audit_failure=1 old=1 auid=4294967295 ses=4294967295 subj=system_u:system_r:unconfined_service_t:s0 res
=1AUID="unset"
type=SYSCALL msg=audit(1727967546.738:7): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7ffd39b70fa0 a2=3c a3=0 items=0 ppid=679 pid=689 auid=429496729
5 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:unconfined
_service_t:s0 key=(null)ARCH=x86_64 SYSCALL=sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root
"
type=PROCTITLE msg=audit(1727967546.738:7): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C6573
type=CONFIG_CHANGE msg=audit(1727967546.739:8): op=set audit_backlog_wait_time=60000 old=60000 auid=4294967295 ses=4294967295 subj=system_u:system_r:unconfine
d_service_t:s0 res=1AUID="unset"
type=SYSCALL msg=audit(1727967546.739:8): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7ffd39b70fa0 a2=3c a3=0 items=0 ppid=679 pid=689 auid=429496729
5 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:unconfined
_service_t:s0 key=(null)ARCH=x86_64 SYSCALL=sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root
"
type=PROCTITLE msg=audit(1727967546.739:8): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C6573
type=SERVICE_START msg=audit(1727967546.748:9): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=auditd comm="systemd" ex
e="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
```

Проверка лог-файлов

Выполняю команду `semanage port -a -t http_port_t -p tcp 81` После этого проверяю список портов командой `semanage port -l | grep http_port_t` Порт 81 появился в списке (рис. [-@fig:024]).

```
[mgandrianova@localhost ~]$ sudo semanage port -a -t http_port_t -p tcp 81
Port tcp/81 already defined, modifying instead
[mgandrianova@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
```

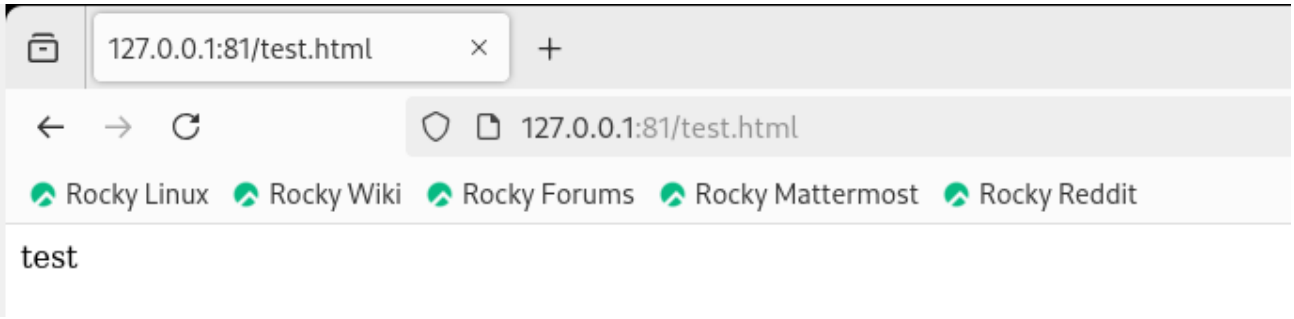
Проверка портов

Перезапускаю сервер Apache (рис. [-@fig:025]).

```
[mgandrianova@localhost ~]$ sudo systemctl restart httpd
[mgandrianova@localhost ~]$ sudo chcon -t httpd_sys_content_t /var/www/html/test.html
[mgandrianova@localhost ~]$ sudo systemctl restart httpd
```

Перезапуск сервера

Теперь он работает, ведь мы внесли порт 81 в список портов `htttpd_port_t` (рис. [-@fig:026]).



Проверка сервера

Возвращаю в файле /etc/httpd/httpd.conf порт 80, вместо 81. Проверяю, что порт 81 удален, это правда (рис. [-@fig:027]).

```
[mgandrianova@localhost ~]$ sudo nano /etc/httpd/conf/httpd.conf
[mgandrianova@localhost ~]$ sudo semanage port -d -t http_port_t -p tcp 81
[mgandrianova@localhost ~]$ sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
```

Проверка порта 81

Далее удаляю файл test.html, проверяю, что он удален (рис. [-@fig:028]).

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

Удаление файла

Выводы

В ходе выполнения данной лабораторной работы были развиты навыки администрирования ОС Linux, получено первое практическое знакомство с технологией SELinux и проверена работа SELinux на практике совместно с веб-сервером Apache.