

Отчёта по лабораторной работе № 6

Информационная безопасность

Адоле Фейт Эне

Содержание

0.1	Цель работы	4
0.2	Теоретическое введение	4
0.3	Выполнение лабораторной работы	5
0.4	Выводы	15

Список иллюстраций

1	Рис. 6.1: Проверка режима enforcing политики targeted	5
2	Рис. 6.2: Проверка работы веб-сервера	6
3	Рис. 6.3: Контекст безопасности веб-сервера Apache	6
4	Рис. 6.4: Текущее состояние переключателей SELinux	7
5	Рис. 6.5: Статистика по политике	8
6	Рис. 6.6: : Просмотр файлов и поддиректорий в директории /var/www	9
7	Рис. 6.7: Создание файла /var/www/html/test.html	9
8	Рис. 6.8: Обращение к файлу через веб-сервер	10
9	Рис. 6.9: Изменение контекста	10
10	Рис. 6.11: Просмотр log-файла	11
11	Рис. 6.12: Установка веб-сервера Apache на прослушивание TCP- порта 81	12
12	Рис. 6.13: Перезапуск веб-сервера и анализ лог-файлов	12
13	Рис. 6.14: : Содержание файла var/log/audit/audit.log	13
14	Рис. 6.15: Проверка установки порта 81	13
15	Рис. 6.16: Возвращение исходного контекста файлу	14
16	Рис. 6.17: Обращение к файлу через веб-сервер	14
17	Рис. 6.18: Возвращение Listen 80 и попытка удалить порт 81 . . .	15
18	Рис. 6.19: Удаление файла test.html	15

Список таблиц

0.1 Цель работы

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

0.2 Теоретическое введение

SELinux (Security-Enhanced Linux) обеспечивает усиление защиты путем внесения изменений как на уровне ядра, так и на уровне пространства пользователя, что превращает ее в действительно «непробиваемую» операционную систему. Впервые эта система появилась в четвертой версии CentOS, а в 5 и 6 версии реализация была существенно дополнена и улучшена. SELinux имеет три основных режим работы:

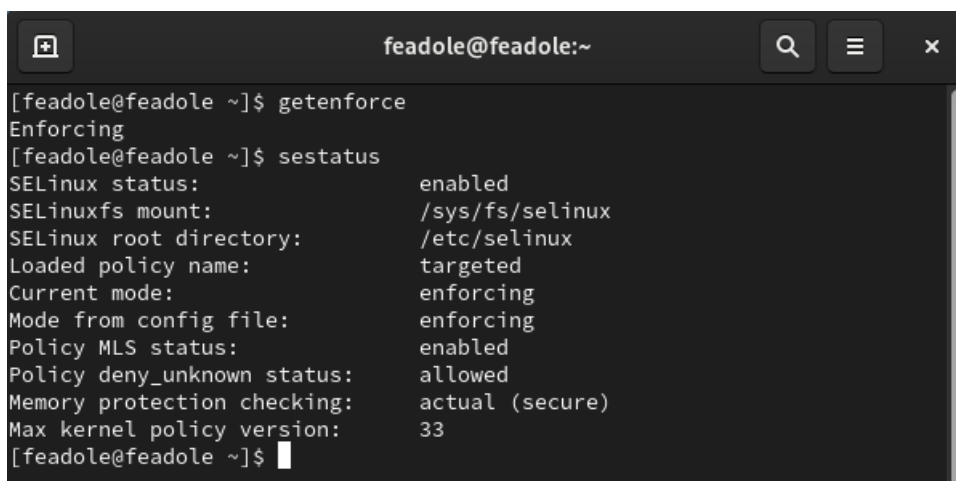
- Enforcing: Режим по-умолчанию. При выборе этого режима все действия, которые каким-то образом нарушают текущую политику безопасности, будут блокироваться, а попытка нарушения будет зафиксирована в журнале.
- Permissive: В случае использования этого режима, информация о всех действиях, которые нарушают текущую политику безопасности, будут зафиксированы в журнале, но сами действия не будут заблокированы.
- Disabled: Полное отключение системы принудительного контроля доступа. Политика SELinux определяет доступ пользователей к ролям, доступ ролей к доменам и доступ доменов к типам. Контекст безопасности — все атрибуты SELinux — роли, типы и домены. Более подробно см. в [1]. Apache — это свободное программное обеспечение, с помощью которого можно создать веб-сервер. Данный продукт возник как доработанная

версия другого HTTP-клиента от национального центра суперкомпьютерных приложений (NCSA).

Для чего нужен Apache сервер: • чтобы открывать динамические PHP-страницы, • для распределения поступающей на сервер нагрузки, • для обеспечения отказоустойчивости сервера, • чтобы потренироваться в настройке сервера и запуске PHP-скриптов. Apache является кроссплатформенным ПО и поддерживает такие операционные системы, как Linux, BSD, MacOS, Microsoft, BeOS и другие. Более подробно см. в [2].

0.3 Выполнение лабораторной работы

Вошла в систему под своей учетной записью и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд “getenforce” и “sestatus” (рис. 6.1).

A screenshot of a terminal window with a dark background. The window title is "feadole@feadole:~". The terminal shows the following commands and output:

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

Рис. 1: Рис. 6.1: Проверка режима enforcing политики targeted

брatилась с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедилась, что последний работает с помощью команды “service httpd status” (рис. 6.2).

```
feadole@feadole:~$ 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 Wed 2023-10-11 15:40:28 MSK; 7min ago
     Docs: man:httpd.service(8)
  Main PID: 13305 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
    Tasks: 213 (limit: 12223)
   Memory: 21.5M
      CPU: 303ms
   CGroup: /system.slice/httpd.service
           └─13305 /usr/sbin/httpd -DFOREGROUND
             └─13518 /usr/sbin/httpd -DFOREGROUND
               └─13522 /usr/sbin/httpd -DFOREGROUND
                 └─13523 /usr/sbin/httpd -DFOREGROUND
                   └─13528 /usr/sbin/httpd -DFOREGROUND

Oct 11 15:40:28 feadole.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 11 15:40:28 feadole.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 11 15:40:28 feadole.localdomain httpd[13305]: Server configured, listening on: port 80
[feadole@feadole ~]$
```

Рис. 2: Рис. 6.2: Проверка работы веб-сервера

С помощью команды “ps auxZ | grep httpd” определила контекст безопасности веб-сервера Apache - httpd_t (рис. 6.3).

```
feadole@feadole:~$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 13305 0.0 0.5 20328 11572 ? Ss 15:40 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 13518 0.0 0.3 21664 7416 ? S 15:40 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 13522 0.0 0.5 1079476 11084 ? Sl 15:40 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 13523 0.0 0.6 1210612 13132 ? Sl 15:40 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 13528 0.0 0.4 1079476 9040 ? Sl 15:40 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 feadole 40116 0.0 0.1 221664 2240 pts/0 S+ 15:49 0:00 grep --color=auto httpd
[feadole@feadole ~]$
```

Рис. 3: Рис. 6.3: Контекст безопасности веб-сервера Apache

Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды “sestatus -bigrep httpd”, многие из переключателей находятся в положении “off” (рис. 6.4).

```
feadole@feadole:~  
[feadole@feadole ~]$ sestatus -bigrep httpd  
sestatus: invalid option -- 'i'  
  
Usage: sestatus [OPTION]  
  
-v Verbose check of process and file contexts.  
-b Display current state of booleans.  
  
Without options, show SELinux status.  
[feadole@feadole ~]$ 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
```

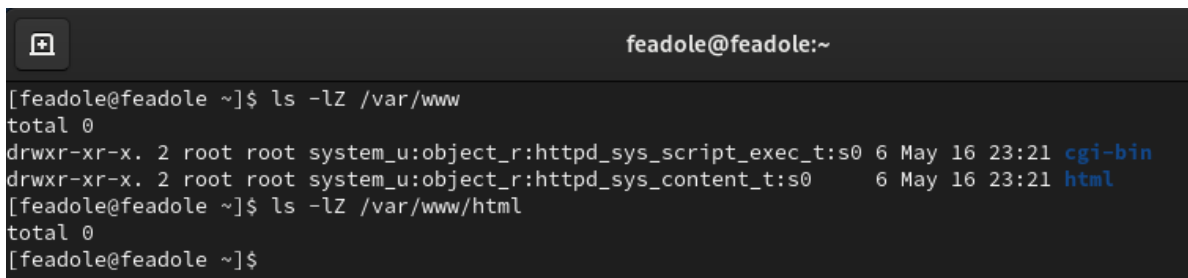
Рис. 4: Рис. 6.4: Текущее состояние переключателей SELinux

Посмотрела статистику по политике с помощью команды “seinfo”. Множество пользователей - 8, ролей - 14, типов 4995 (рис. 6.5).

```
feadole@feadole:~  
[feadole@feadole ~]$ seinfo  
bash: seinfo: command not found...  
Install package 'setools-console' to provide command 'seinfo'? [N/y] y  
  
* Waiting in queue...  
The following packages have to be installed:  
setools-console-4.4.1-1.el9.x86_64 Policy analysis command-line tools for SELinux  
Proceed with changes? [N/y] y  
  
* Waiting in queue...  
* Waiting for authentication...  
* Waiting in queue...  
* Downloading packages...  
* Requesting data...  
* Testing changes...  
* Installing packages...  
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: 65000 Neverallow: 0  
Auditallow: 170 Dontaudit: 8572  
Type_trans: 265341 Type_change: 87  
Type_member: 35 Range_trans: 6164  
Role_allow: 38 Role_trans: 420  
Constraints: 70 Validatetrans: 0  
MLS Constrains: 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  
Genfscon: 109 Portcon: 660
```

Рис. 5: Рис. 6.5: Статистика по политике

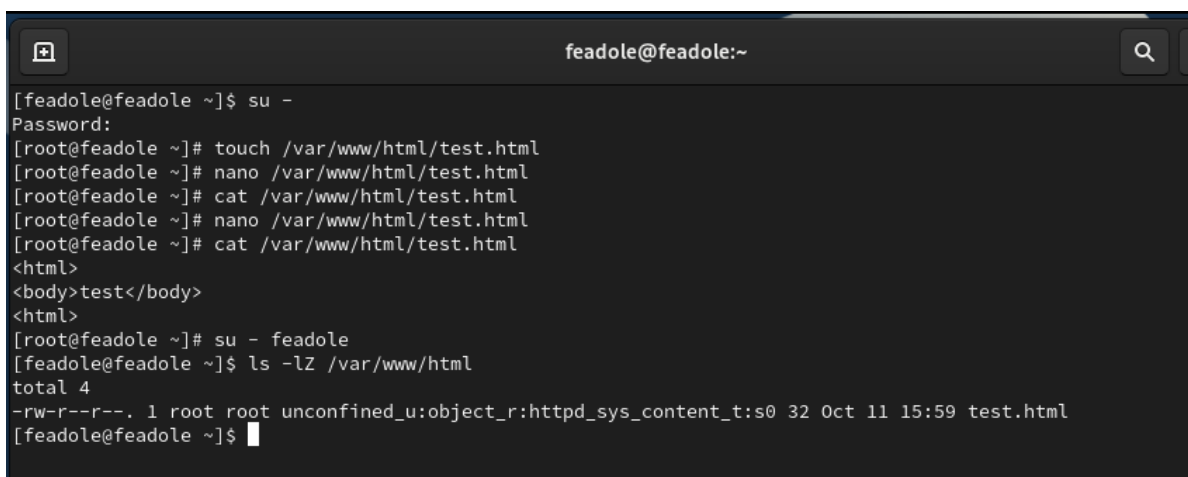
С помощью команды “ls -lZ /var/www” посмотрела файлы и поддиректории, находящиеся в директории /var/www. Используя команду “ls -lZ /var/www/html”, определила, что в данной директории файлов нет. Только владелец/суперпользователь может создавать файлы в директории /var/www/html (рис. 6.6).

A terminal window titled 'feadole@feadole:~' with a dark background. It shows the execution of two 'ls -lZ' commands. The first command lists the contents of '/var/www', showing two directories: 'cgi-bin' and 'html', both with permissions 'drwxr-xr-x', owned by 'root:root', and having SELinux contexts 'system_u:object_r:httpd_sys_script_exec_t:s0' and 'system_u:object_r:httpd_sys_content_t:s0' respectively. The second command lists the contents of '/var/www/html', which is currently empty.

```
[feadole@feadole ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 23:21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 May 16 23:21 html
[feadole@feadole ~]$ ls -lZ /var/www/html
total 0
[feadole@feadole ~]$
```

Рис. 6: Рис. 6.6: : Просмотр файлов и поддиректорий в директории /var/www

От имени суперпользователя создала html-файл /var/www/html/test.html. Кон-текст созданного файла - httpd_sys_content_t (рис. 6.7).

A terminal window titled 'feadole@feadole:~' with a dark background. It shows a sequence of commands to create and edit a file. First, 'su -' is used to become root. Then, 'touch /var/www/html/test.html' creates the file. 'nano /var/www/html/test.html' is used to create the file, and 'cat /var/www/html/test.html' shows its content: '<html><body>test</body></html>'. Finally, 'su - feadole' switches back to the feadole user. A final 'ls -lZ /var/www/html' command shows the newly created file 'test.html' with permissions '-rw-r--r--', owned by 'root:root', and having SELinux context 'httpd_sys_content_t:s0'.

```
[feadole@feadole ~]$ su -
Password:
[root@feadole ~]# touch /var/www/html/test.html
[root@feadole ~]# nano /var/www/html/test.html
[root@feadole ~]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[root@feadole ~]# su - feadole
[feadole@feadole ~]$ ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 32 Oct 11 15:59 test.html
[feadole@feadole ~]$
```

Рис. 7: Рис. 6.7: Создание файла /var/www/html/test.html

Обратилась к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Файл был успешно отображен (рис. 6.8).

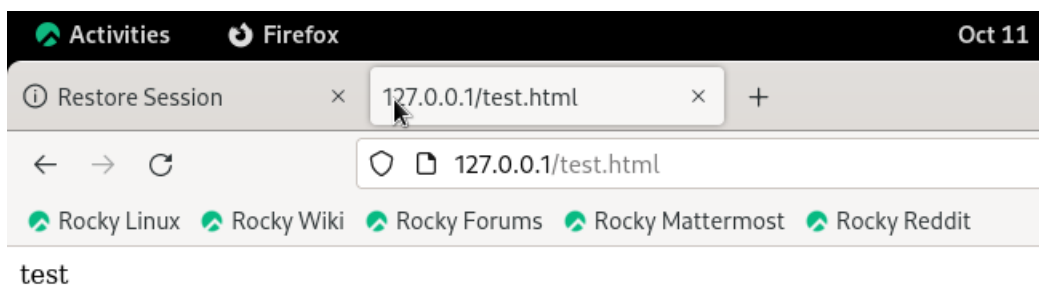


Рис. 8: Рис. 6.8: Обращение к файлу через веб-сервер

Изучив справку `man httpd_selinux`, выяснила, что для `httpd` определены следующие контексты файлов: `httpd_sys_content_t`, `httpd_sys_script_exec_t`, `httpd_sys_script_ro_t`, `httpd_sys_script_rw_t`, `httpd_sys_script_ra_t`, `httpd_unconfined_script_exec_t`. Контекст моего файла - `httpd_sys_content_t` (в таком случае содержимое должно быть доступно для всех скриптов `httpd` и для самого демона). Изменила контекст файла на `samba_share_t` командой “`sudo chcon -t samba_share_t /var/www/html/test.html`” и проверила, что контекст поменялся (рис. 6.9).

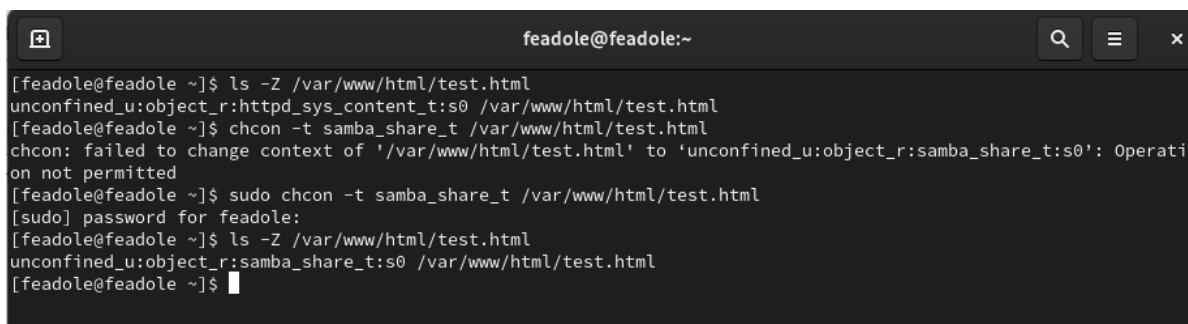
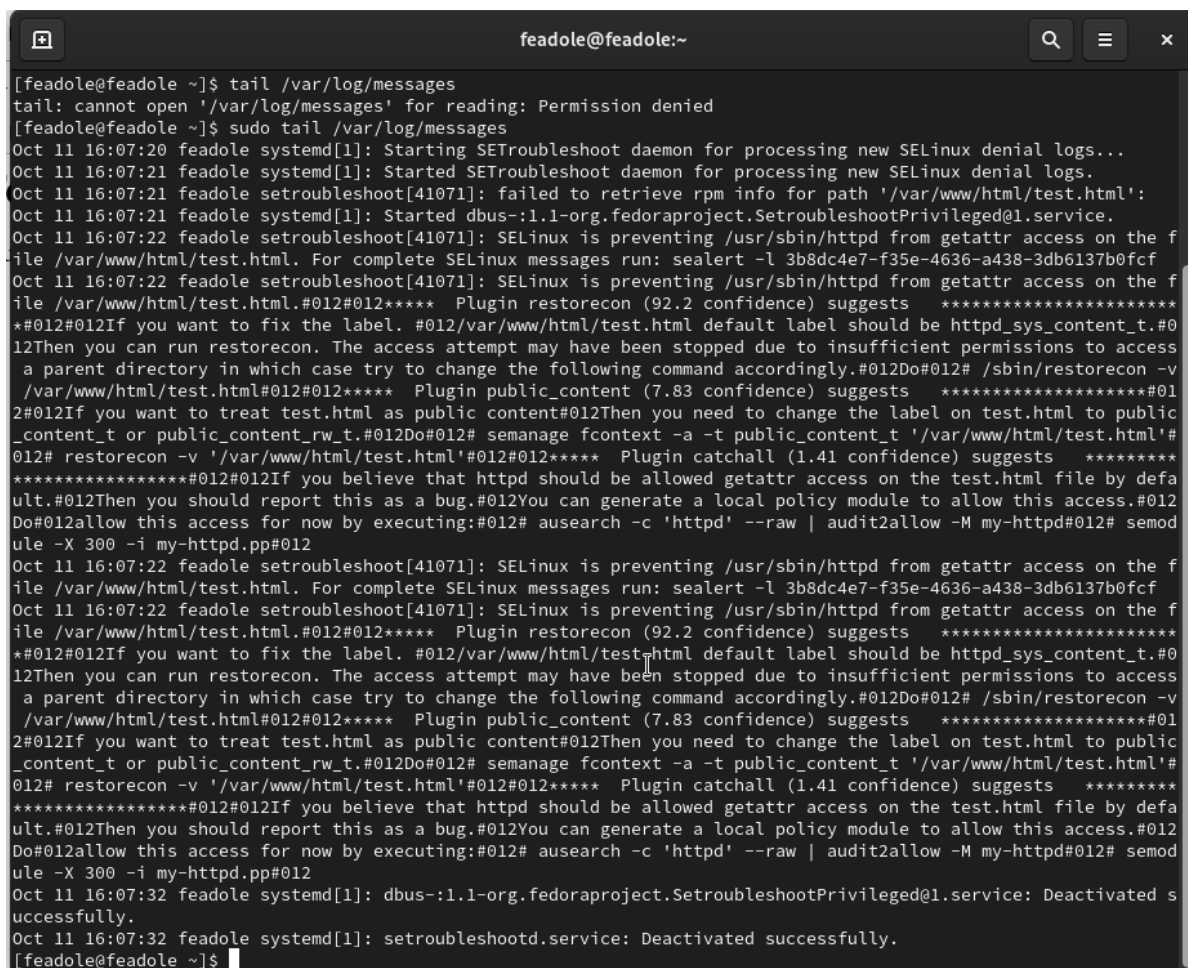


Рис. 9: Рис. 6.9: Изменение контекста

Попробовала еще раз получить доступ к файлу через веб-сервер, введя в браузере адрес “`http://127.0.0.1/test.html`” и получила сообщение об ошибке (т.к. к установленному ранее контексту процесс `httpd` не имеет доступа) (рис. 6.10).

Рис. 6.10: Обращение к файлу через веб-сервер

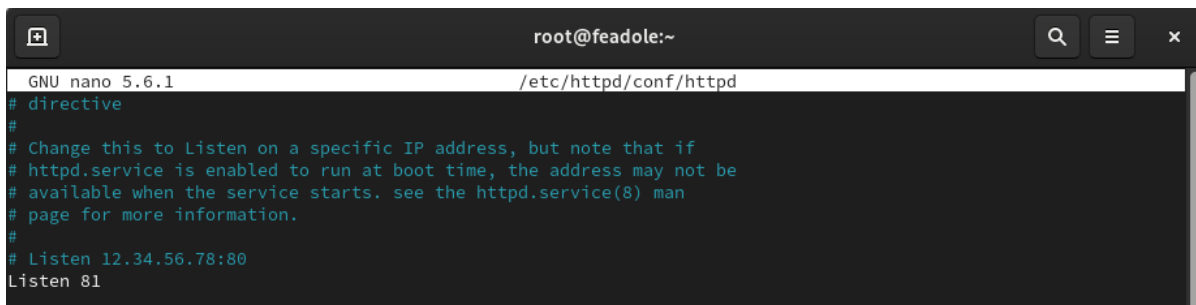
Командой “ls -l /var/www/html/test.html” убедилась, что читать данный файл может любой пользователь. Просмотрела системный лог-файл веб-сервера Apache командой “sudo tail /var/log/messages”, отображающий ошибки (рис. 6.11).



```
feadole@feadole:~$ tail /var/log/messages
tail: cannot open '/var/log/messages' for reading: Permission denied
feadole@feadole:~$ sudo tail /var/log/messages
Oct 11 16:07:20 feadole systemd[1]: Starting SETroubleshoot daemon for processing new SELinux denial logs...
Oct 11 16:07:21 feadole systemd[1]: Started SETroubleshoot daemon for processing new SELinux denial logs.
Oct 11 16:07:21 feadole setroubleshoot[41071]: failed to retrieve rpm info for path '/var/www/html/test.html':
Oct 11 16:07:21 feadole systemd[1]: Started dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@1.service.
Oct 11 16:07:22 feadole setroubleshoot[41071]: SELinux is preventing /usr/sbin/httpd from getattr access on the f
ile /var/www/html/test.html. For complete SELinux messages run: sealert -l 3b8dc4e7-f35e-4636-a438-3db6137b0fcf
Oct 11 16:07:22 feadole setroubleshoot[41071]: SELinux is preventing /usr/sbin/httpd from getattr access on the f
ile /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.#0
12Then 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 *****#01
2#012If you want to treat test.html as public content#012Then you need to change the label on test.html to public
_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#
012# restorecon -v '/var/www/html/test.html'#012#012***** Plugin catchall (1.41 confidence) suggests *****
*****#012#012If you believe that httpd should be allowed getattr access on the test.html file by defa
ult.#012Then you should report this as a bug.#012You can generate a local policy module to allow this access.#012
Do#012allow this access for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semod
ule -X 300 -i my-httpd.pp#012
Oct 11 16:07:22 feadole setroubleshoot[41071]: SELinux is preventing /usr/sbin/httpd from getattr access on the f
ile /var/www/html/test.html. For complete SELinux messages run: sealert -l 3b8dc4e7-f35e-4636-a438-3db6137b0fcf
Oct 11 16:07:22 feadole setroubleshoot[41071]: SELinux is preventing /usr/sbin/httpd from getattr access on the f
ile /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.#0
12Then 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 *****#01
2#012If you want to treat test.html as public content#012Then you need to change the label on test.html to public
_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#
012# restorecon -v '/var/www/html/test.html'#012#012***** Plugin catchall (1.41 confidence) suggests *****
*****#012#012If you believe that httpd should be allowed getattr access on the test.html file by defa
ult.#012Then you should report this as a bug.#012You can generate a local policy module to allow this access.#012
Do#012allow this access for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semod
ule -X 300 -i my-httpd.pp#012
Oct 11 16:07:32 feadole systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@1.service: Deactivated s
uccessfully.
Oct 11 16:07:32 feadole systemd[1]: setroubleshoold.service: Deactivated successfully.
feadole@feadole:~$
```

Рис. 10: Рис. 6.11: Просмотр log-файла

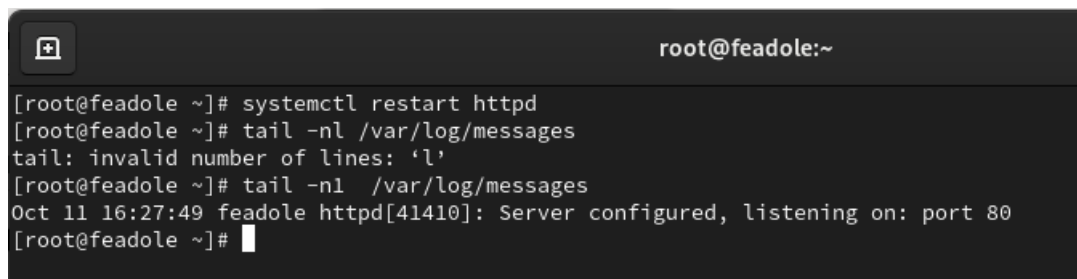
В файле /etc/httpd/conf/httpd.conf заменила строчку “Listen 80” на “Listen 81”, чтобы установить веб-сервер Apache на прослушивание TCP-порта 81 (рис. 6.12).



```
root@feadole:~  
GNU nano 5.6.1 /etc/httpd/conf/httpd  
# 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
```

Рис. 11: Рис. 6.12: Установка веб-сервера Apache на прослушивание TCP-порта 81

Перезапускаем веб-сервер Apache и анализирует лог-файлы командой “tail -nl /var/log/messages” (рис. 6.13).



```
root@feadole:~  
[root@feadole ~]# systemctl restart httpd  
[root@feadole ~]# tail -nl /var/log/messages  
tail: invalid number of lines: 'l'  
[root@feadole ~]# tail -nl /var/log/messages  
Oct 11 16:27:49 feadole httpd[41410]: Server configured, listening on: port 80  
[root@feadole ~]#
```

Рис. 12: Рис. 6.13: Перезапуск веб-сервера и анализ лог-файлов

Просмотрела файлы “var/log/http/error_log”, “/var/log/http/access_log” и “/var/log/audit/audit.log” и выяснила, что запись появилась в последнем файле (рис. 6.14).

```

[root@feadole ~]# tail /var/log/audit/audit.log
type=CRED_REFR msg=audit(1697031614.693:297): pid=41734 uid=0 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="root" AUID="feadole"
type=USER_START msg=audit(1697031614.696:298): pid=41734 uid=0 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session_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="root" AUID="feadole"
type=USER_END msg=audit(1697031614.698:299): pid=41734 uid=0 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="root" AUID="feadole"
type=CRED_DISP msg=audit(1697031614.698:300): pid=41734 uid=0 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="root" AUID="feadole"
type=USER_ACCT msg=audit(1697031990.480:301): pid=41791 uid=0 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:accounting grantors=pam_unix,pam_localuser acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="root" AUID="feadole"
type=USER_CMD msg=audit(1697031990.480:302): pid=41791 uid=0 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='cwd="/root" cmd=7461696C202F7661722F6C6F672F687474702F6572726F725F6C6F67 exe="/usr/bin/sudo" terminal=pts/0 res=success'UID="root" AUID="feadole"
type=CRED_REFR msg=audit(1697031990.490:303): pid=41791 uid=0 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="root" AUID="feadole"
type=USER_START msg=audit(1697031990.490:304): pid=41791 uid=0 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session_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="root" AUID="feadole"
type=USER_END msg=audit(1697031990.496:305): pid=41791 uid=0 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="root" AUID="feadole"
type=CRED_DISP msg=audit(1697031990.496:306): pid=41791 uid=0 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="root" AUID="feadole"
[root@feadole ~]#

```

Рис. 13: Рис. 6.14: Содержание файла var/log/audit/audit.log

Выполнила команду “semanage port -a -t http_port_t -p tcp 81” и убедилась, что порт TCP-81 установлен. Проверила список портов командой “semanage port -l | grep http_port_t”, убедилась, что порт 81 есть в списке и запускаем веб-сервер Apache снова (рис. 6.15).

```

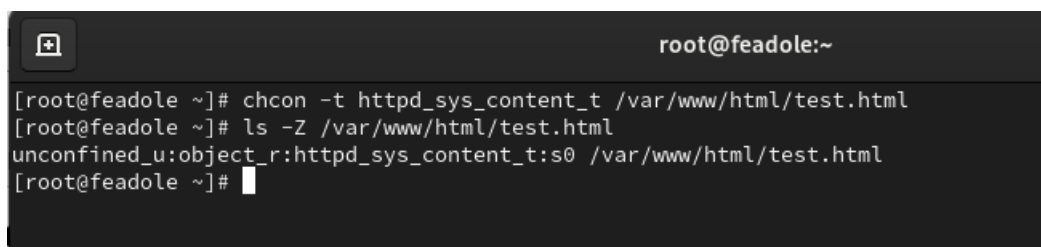
root@feadole:~
[root@feadole ~]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@feadole ~]# semanage port -l | grep http_port_t
http_port_t          tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t  tcp      5988
[root@feadole ~]# systemctl restart httpd
Failed to restart http.service: Unit http.service not found.
[root@feadole ~]# systemctl restart httpd
[root@feadole ~]#

```

Рис. 14: Рис. 6.15: Проверка установки порта 81

Вернула контекст “httpd_sys_content_t” файлу “/var/www/html/test.html”

командой “chcon -t httpd_sys_content_t /var/www/html/test.html” (рис. 6.16) и после этого попробовала получить доступ к файлу через веб-сервер, введ “http://127.0.0.1:81/test.html”, в результате чего увидела содержимое файла - слово “test” (рис. 6.17).



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

Рис. 15: Рис. 6.16: Возвращение исходного контекста файлу

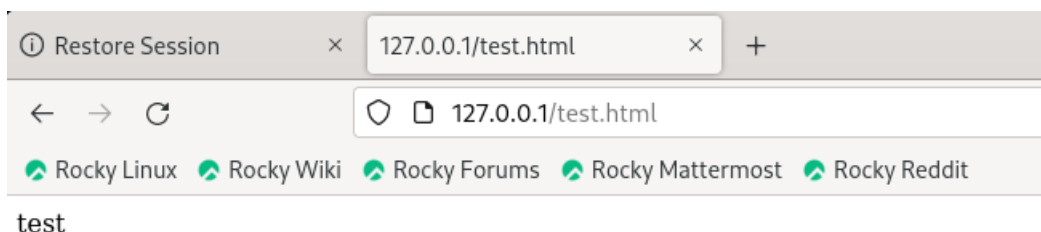
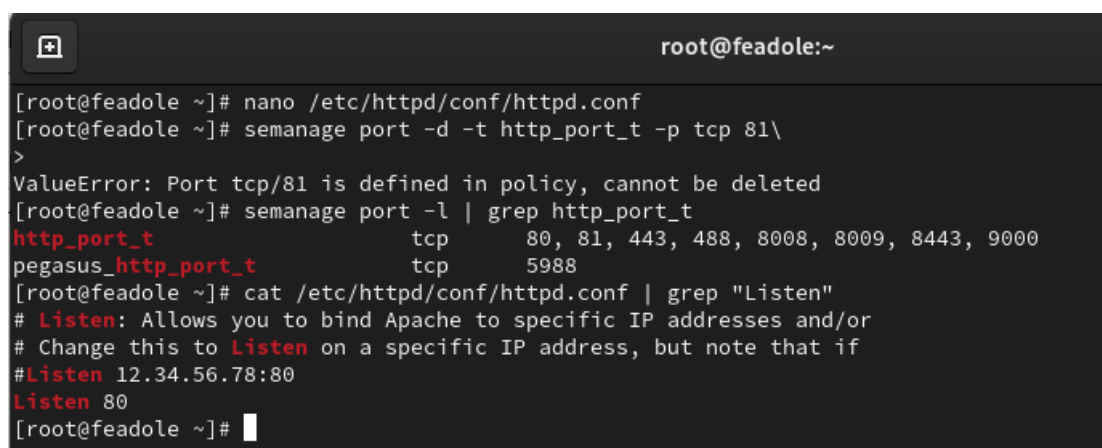


Рис. 16: Рис. 6.17: Обращение к файлу через веб-сервер

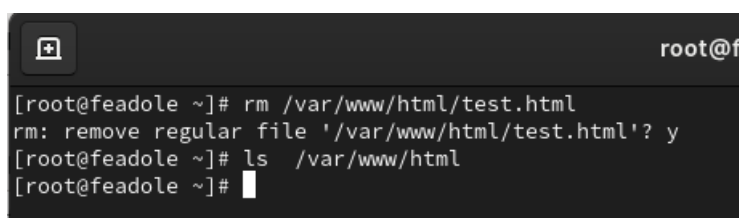
справила обратно конфигурационный файл apache, вернув “Listen 80”. Попыталась удалить привязку http_port к 81 порту командой “semanage port -d -t http_port_t -p tcp 81”, но этот порт определен на уровне политики, поэтому его нельзя удалить (рис. 6.18).



```
root@feadole:~  
[root@feadole ~]# nano /etc/httpd/conf/httpd.conf  
[root@feadole ~]# semanage port -d -t http_port_t -p tcp 81\  
>  
ValueError: Port tcp/81 is defined in policy, cannot be deleted  
[root@feadole ~]# 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@feadole ~]# cat /etc/httpd/conf/httpd.conf | grep "Listen"  
# Listen: Allows you to bind Apache to specific IP addresses and/or  
# Change this to Listen on a specific IP address, but note that if  
#Listen 12.34.56.78:80  
Listen 80  
[root@feadole ~]#
```

Рис. 17: Рис. 6.18: Возвращение Listen 80 и попытка удалить порт 81

Удалила файл “/var/www/html/test.html” командой “rm /var/www/html/test.html” (рис. 6.19).



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

Рис. 18: Рис. 6.19: Удаление файла test.html

0.4 Выводы

В ходе выполнения данной лабораторной работы я развила навыки администрирования ОС Linux, получила первое практическое знакомство с технологией SELinux и проверила работу SELinux на практике совместно с веб-сервером Apache.