Лабораторная работа №6

Мандатное разграничение прав в Linux

Дугаева Светлана Анатольевна

Содержание

Список иллюстраций

1 Цель работы

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

2 Подготовка лабораторного стенда

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. Выполнила здание параметра с помощью команды echo “ServerName test.ru” » /etc/httpd/httpd.conf

Также необходимо проследить, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp. Отключила фильтр можно командами iptables -F iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT

3 Выполнение лабораторной работы

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

Действия из подготовки лабораторного стенда и пункта 1 выполнения лабораторной работы представленны на (рис. -@fig:001):

```
[dugaevas@localhost ~]$ su
Пароль:
[root@localhost dugaevas]# echo "ServerName test.ru" >> /etc/httpd/httpd.conf
[root@localhost dugaevas]# cat /etc/httpd/httpd.conf
ServerName test.ru
[root@localhost dugaevas]# iptables -F
[root@localhost dugaevas]# iptables -P INPUT ACCEPT
[root@localhost dugaevas]# iptables -P OUTPUT ACCEPT
[root@localhost dugaevas]# EXIT
bash: EXIT: команда не найдена...
[root@localhost dugaevas]# exit
exit
[dugaevas@localhost ~]$ getrnforce
bash: getrnforce: команда не найдена...
[dugaevas@localhost ~]$ getenforce
Enforcing
[dugaevas@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
[dugaevas@localhost ~]$
```

Рис. 3.1: П. 1 выполения ЛР и подготовка

2. Обратилась с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедилась, что последний работает: service httpd status
3. Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности: пользователь system_u, политика ролевого разделения system_r, тип https_t, уровень доступа s0.

Действия пунктов 2-3 предствленны на (рис. -@fig:002):

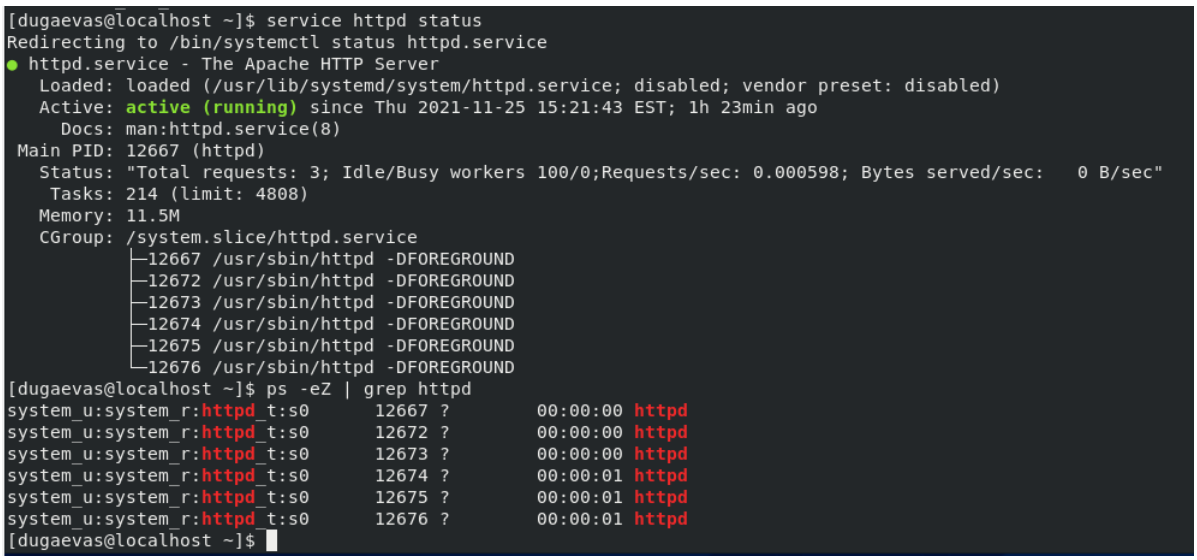

Рис. 3.2: Статус веб-сервера и политика безопасности

4. Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды sestatus -b httpd Многие из них находятся в положении «off». (рис. -@fig:003):

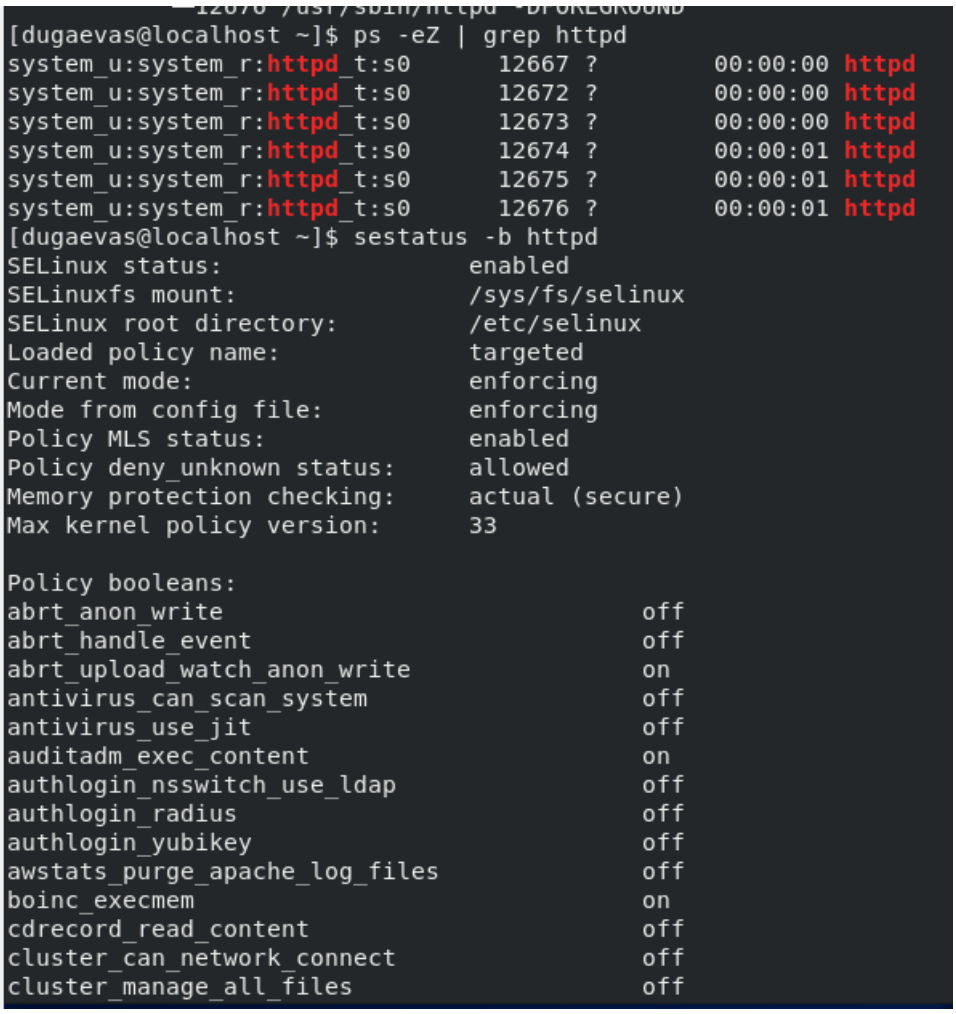

Рис. 3.3: Состояние переключателей

5. Посмотрела статистику по политике с помощью команды seinfo
6. Определила тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www:
7. пределю тип файлов, находящихся в директории /var/www/html с помощью команды ls -lZ /var/www/html.
8. Определю круг пользователей, которым разрешено создание файлов в директории /var/www/html. Создавать файлы можно только суперпользователю, который является владельцем.

Действия пунктов 5-8 представленны на (рис. -@fig:004):

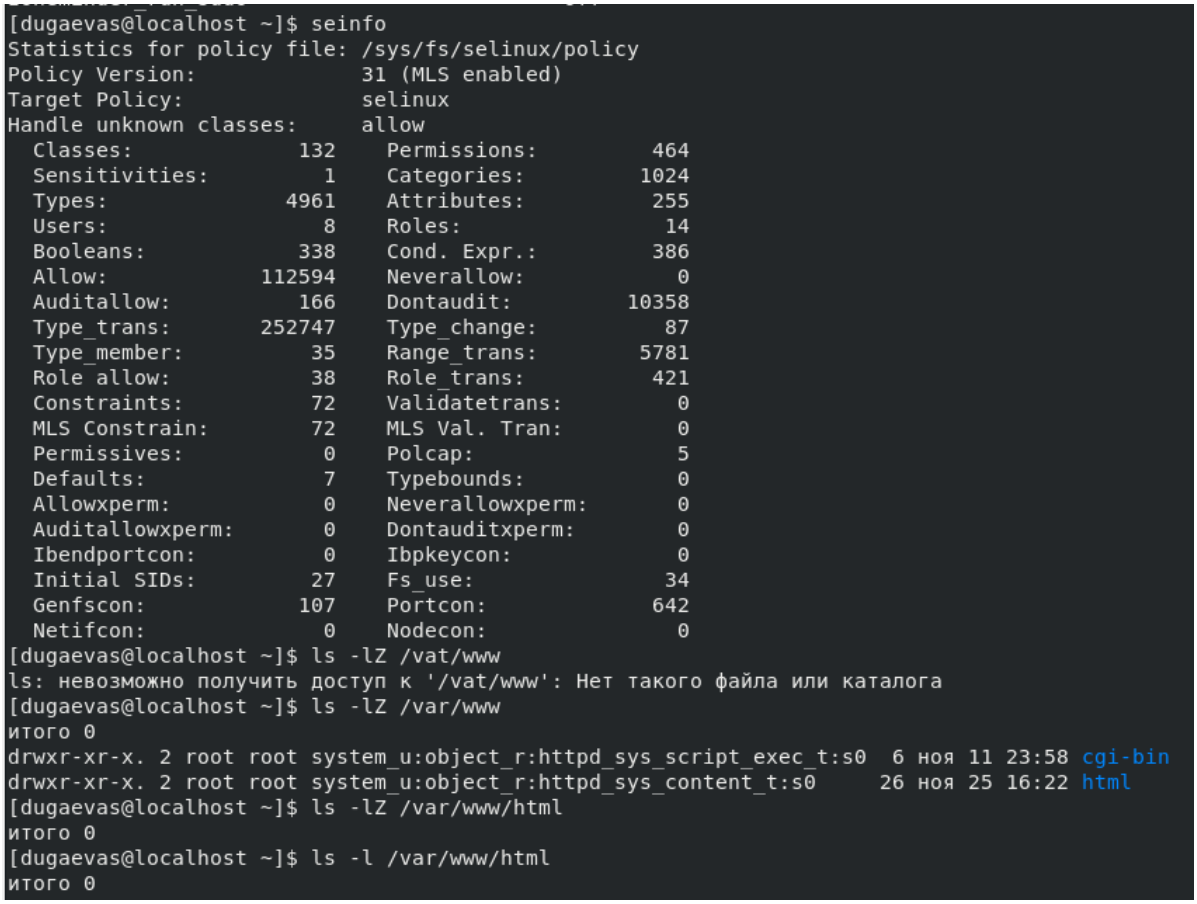

Рис. 3.4: Пункты 5-8

9. Создам от имени суперпользователя html-файл /var/www/html/test.html следующего содержания:
   test
10. Проверю контекст созданного мной файла. По умолчанию вновь созданным файлам в директории /var/www/html присваивается контекст unconfined_u:object_r:httpd_sys_conent_t:s0

Действия пунктов 9-10 представленны на (рис. -@fig:005):

```
[root@localhost dugaevas]# nano /var/www/html/test.html
[root@localhost dugaevas]# cat /var/www/html/test.html
<html>
        <body>test</body>
</html>
[root@localhost dugaevas]# ls -lZ /var/www/html/test.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 ноя 25 17:11 /var/www/html/test.html
[root@localhost dugaevas]#
```

Рис. 3.5: Пункты 9-10

11. Обратилась к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Файл был успешно отображён (рис. -@fig:006):

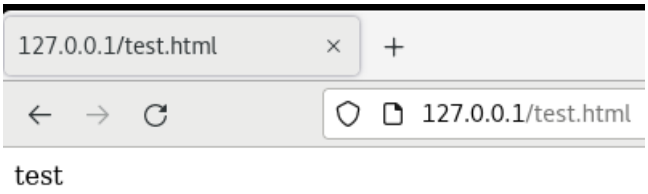

Рис. 3.6: Обращение к файлу через веб-сервер

12. Изучила справку man httpd_selinux (рис. -@fig:007):

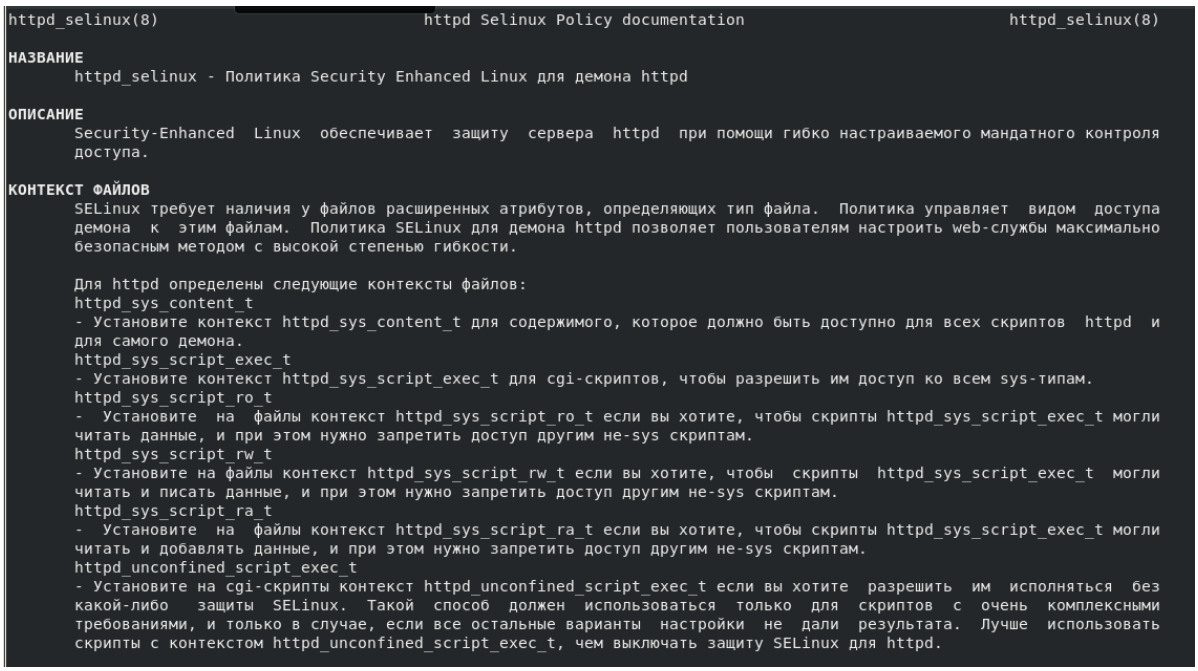

Рис. 3.7: Справка о контекстах

Контекст созданного мной файла: unconfined_u : object_r : httpd_sys_content_t : s0, Тип httpd_sys_content_t позволяет получить доступ к файлу, если мы обращаемся к нему через браузер.

13. Изменила контекст файла /var/www/html/test.html с httpd_sys_content_t на samba_share_t: (рис. -@fig:008):

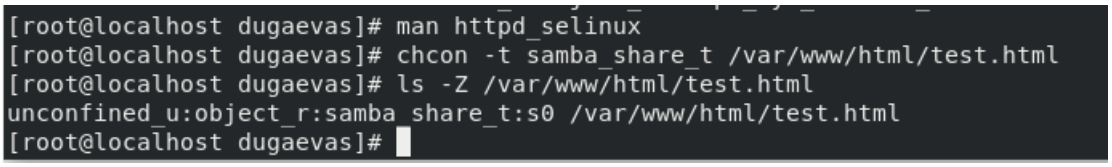

Рис. 3.8: Изменение контекста

14. Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html (рис. -@fig:009):

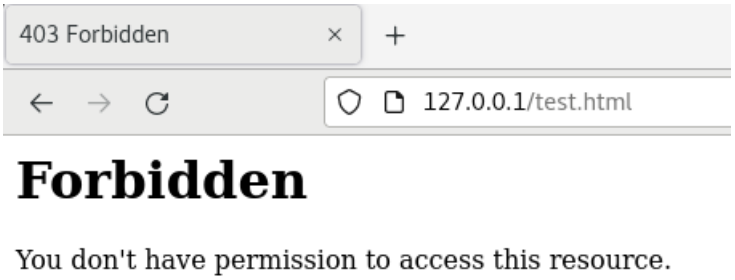

Рис. 3.9: Доступ к файлу через веб-браузер

15. Файл не был отображен из-за того, что несмотря на возможность у любого пользователя просматривать файл, политика SELinux не задает правило, которое разрешало бы доступ, и операция сразу блокируется. Посмотрю log-файлы веб-сервера Apache и системный log файл (рис. -@fig:010):

```
[root@localhost dugaevas]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@localhost dugaevas]# tail /var/log/httpd/error_log
[Thu Nov 25 15:21:43.710154 2021] [core:notice] [pid 12667:tid 139813255399744] SELinux policy enabled; httpd running as conte
xt system_u:system_r:httpd_t:s0
[Thu Nov 25 15:21:43.713794 2021] [suexec:notice] [pid 12667:tid 139813255399744] 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 'S
erverName' directive globally to suppress this message
[Thu Nov 25 15:21:43.752873 2021] [lbmethod_heartbeat:notice] [pid 12667:tid 139813255399744] AH02282: No slotmem from mod_hea
rtmonitor
[Thu Nov 25 15:21:43.757124 2021] [mpm_event:notice] [pid 12667:tid 139813255399744] AH00489: Apache/2.4.37 (centos) OpenSSL/1
.1.1k mod_fcgid/2.3.9 configured -- resuming normal operations
[Thu Nov 25 15:21:43.757151 2021] [core:notice] [pid 12667:tid 139813255399744] AH00094: Command line: '/usr/sbin/httpd -D FOR
EGROUND'
[Thu Nov 25 15:53:49.312643 2021] [core:error] [pid 12676:tid 139812409382656] (13)Permission denied: [client 127.0.0.1:34864]
 AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing on a
component of the path
[Thu Nov 25 17:25:46.987092 2021] [core:error] [pid 12675:tid 139812367419136] (13)Permission denied: [client 127.0.0.1:34962]
 AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing on a
component of the path
[root@localhost dugaevas]# tail /var/log/messages
Nov 25 17:33:39 localhost org.gnome.Shell.desktop[7757]: libinput error: client bug: timer event4 debounce short: scheduled ex
piry is in the past (-254ms), your system is too slow
Nov 25 17:33:43 localhost gnome-keyring-daemon[7675]: couldn't initialize slot with master password: The password or PIN is in
correct
Nov 25 17:33:43 localhost journal[7757]: Could not delete runtime/persistent state file: Произошла ошибка при удалении файла /
run/user/1000/gnome-shell/runtime-state-LE.:0/screenShield.locked: Нет такого файла или каталога
Nov 25 17:33:44 localhost NetworkManager[1207]: <info>  [1637879624.3113] agent-manager: agent[0486686103f9013c,:1.240/org.gno
me.Shell.NetworkAgent/1000]: agent registered
Nov 25 17:34:09 localhost systemd[1]: fprintd.service: Succeeded.
Nov 25 17:36:24 localhost org.gnome.Shell.desktop[7757]: libinput error: event4  - VirtualBox USB Tablet: client bug: event pr
ocessing lagging behind by 12ms, your system is too slow
Nov 25 17:36:27 localhost org.gnome.Shell.desktop[7757]: libinput error: event4  - VirtualBox USB Tablet: client bug: event pr
ocessing lagging behind by 21ms, your system is too slow
Nov 25 17:36:31 localhost org.gnome.Shell.desktop[7757]: libinput error: event4  - VirtualBox USB Tablet: client bug: event pr
ocessing lagging behind by 24ms, your system is too slow
Nov 25 17:36:32 localhost org.gnome.Shell.desktop[7757]: libinput error: event4  - VirtualBox USB Tablet: client bug: event pr
ocessing lagging behind by 20ms, your system is too slow
Nov 25 17:36:32 localhost org.gnome.Shell.desktop[7757]: libinput error: event4  - VirtualBox USB Tablet: WARNING: log rate li
mit exceeded (5 msgs per 60min). Discarding future messages.
```

Рис. 3.10: log-файлы веб-сервера Apache и системный log файл

В системном log файле указано, что моя система слишком медленная, поэтому посмотрю ошибки в файле /var/log/audit/audit.log (рис. -@fig:011):

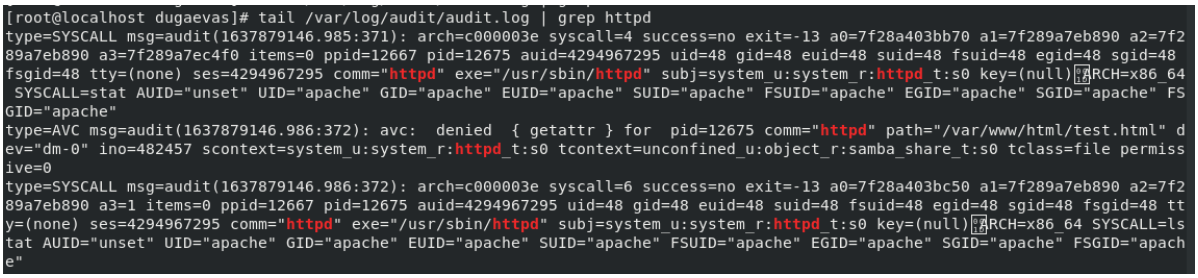

Рис. 3.11: ошибки в файле audit.log

Сравнить ошибки не получилось из-за ошибки в чтении системного лог файла.

16. Попробовала запустить веб-сервер Apache на прослушивание TCP-порта 81. Для этого в файле /etc/httpd/httpd.conf найду строчку Listen 80 и заменю 80 на 81 (рис. -@fig:012):

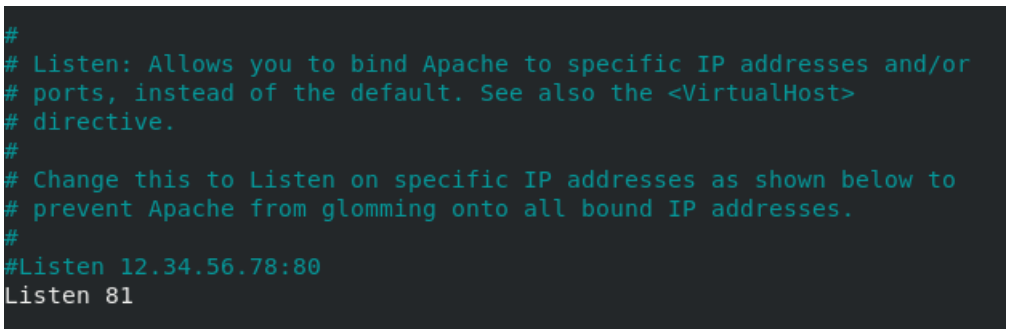

Рис. 3.12: Смена порта

17. Выполнила перезапуск веб-сервера Apache. У меня сбоев не произошло. Возможно, это связано с тем, что данный порт зарезервирован и определен. Заменила 81 на 82. (рис. -@fig:013):

```
[root@localhost dugaevas]# nano /etc/httpd/httpd.conf
[root@localhost dugaevas]# nano /etc/httpd/conf/httpd.conf
[root@localhost dugaevas]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@localhost dugaevas]# nano /etc/httpd/conf/httpd.conf
[root@localhost dugaevas]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
Job for httpd.service failed because the control process exited with error code.
See "systemctl status httpd.service" and "journalctl -xe" for details.
[root@localhost dugaevas]#
```

Рис. 3.13: Перезапуск веб-сервера

Сбой произошел из-за того, что порт 82 не определен.

18. Проанализировала log файлы /var/log/messages (рис. -@fig:014):

```
[root@localhost dugaevas]# tail /var/log/messages
Nov 25 18:11:24 localhost org.gnome.Shell.desktop[7757]: libinput error: client bug: timer event4 debounce: scheduled expiry i
s in the past (-1ms), your system is too slow
Nov 25 18:11:24 localhost org.gnome.Shell.desktop[7757]: libinput error: client bug: timer event4 debounce short: scheduled ex
piry is in the past (-17ms), your system is too slow
Nov 25 18:11:56 localhost org.gnome.Shell.desktop[7757]: libinput error: event2  - AT Translated Set 2 keyboard: client bug: e
vent processing lagging behind by 12ms, your system is too slow
Nov 25 18:11:56 localhost dbus-daemon[1018]: [system] Activating via systemd: service name='net.reactivated.Fprint' unit='fpri
ntd.service' requested by ':1.918' (uid=0 pid=54673 comm="su " label="unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023")
Nov 25 18:11:56 localhost systemd[1]: Starting Fingerprint Authentication Daemon...
Nov 25 18:11:56 localhost dbus-daemon[1018]: [system] Successfully activated service 'net.reactivated.Fprint'
Nov 25 18:11:56 localhost systemd[1]: Started Fingerprint Authentication Daemon.
Nov 25 18:11:59 localhost su[54673]: (to root) dugaevas on pts/0
Nov 25 18:12:21 localhost cupsd[1235]: REQUEST localhost - - "POST / HTTP/1.1" 200 187 Renew-Subscription successful-ok
Nov 25 18:12:27 localhost systemd[1]: fprintd.service: Succeeded.
```

Рис. 3.14: log файлы /var/log/messages

Снова ошибка, но я поискала информацию и определила, что подключение оборвалось, поскольку нет доступных сокетов и не получилось подключиться к адресу 0.0.0.82.

Просмотрела файл /var/log/http/error_log: (рис. -@fig:015):

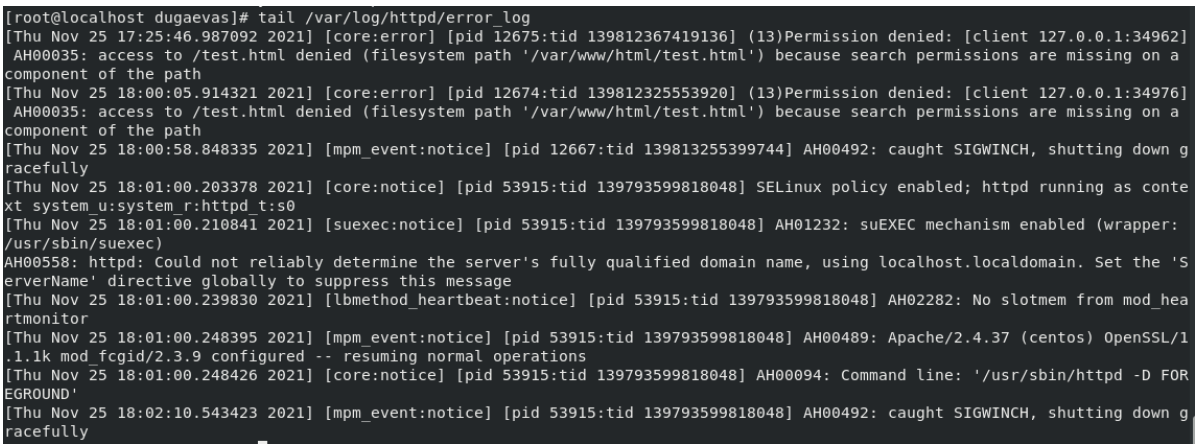

Рис. 3.15: Файл error_log

Просмотрю файл /var/log/audit/audit.log: (рис. -@fig:016):

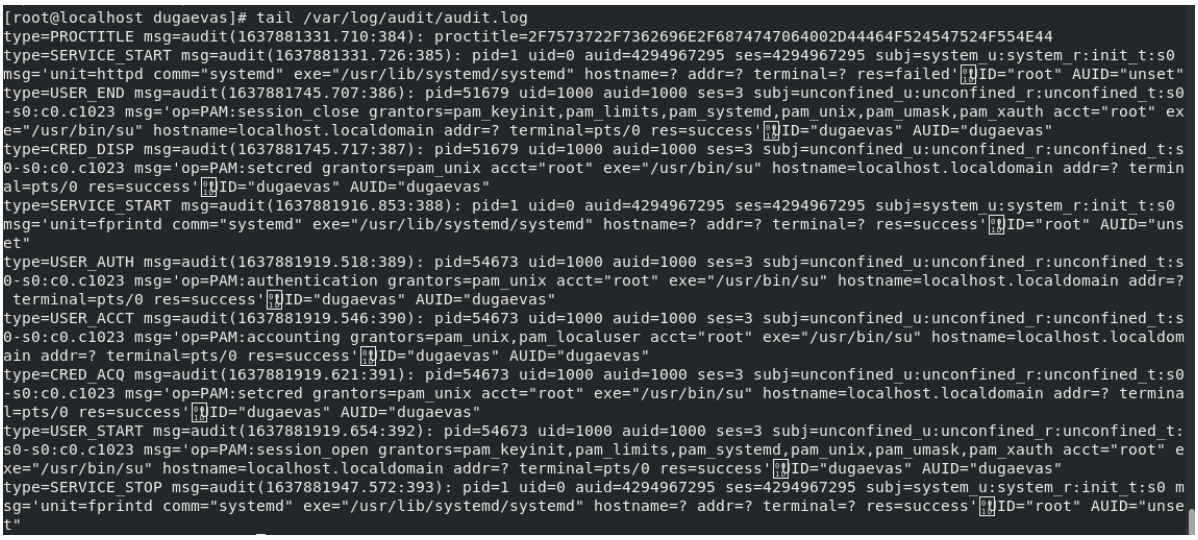

Рис. 3.16: Файл audit.log

Новых сообщений не появилось.

19. Выполнила команду semanage port -a -t http_port_t -p tcp 82: После этого проверила список портов командой semanage port -l | grep http_port_t:

20. Попробовала запустить веб-сервер Apache ещё раз. В этот раз запустить сервер получилось, поскольку на предыдущем шаге мы привязали новый порт.
21. Вернула контекст httpd_sys_content__t к файлу /var/www/html/ test.html:

Действия пунктов 19-21 представленны на (рис. -@fig:017):

```
[root@localhost dugaevas]# semanage port -a -t http_port_t -p tcp 82
[root@localhost dugaevas]# semanage port -l | grep http_port_t
http_port_t                    tcp      82, 80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t            tcp      5988
[root@localhost dugaevas]# servise httpd restart
bash: servise: команда не найдена...
Аналогичная команда: 'service'
[root@localhost dugaevas]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@localhost dugaevas]# chcon -t httpd_sys_content_t /var/www/html/test.html
```

Рис. 3.17: Пункты 19-21

Попробовала получить доступ к файлу /var/www/html/ test.html через браузер (рис. -@fig:018):

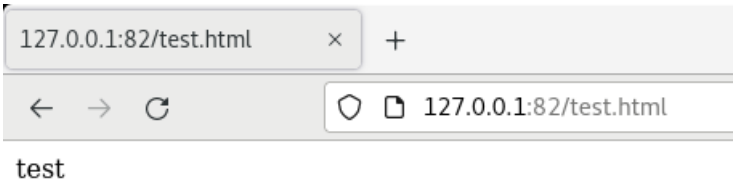

Рис. 3.18: Доступ к файлу через веб-браузер

22. Исправила обратно конфигурационный файл apache, вернув Listen 80 (рис. -@fig:019):

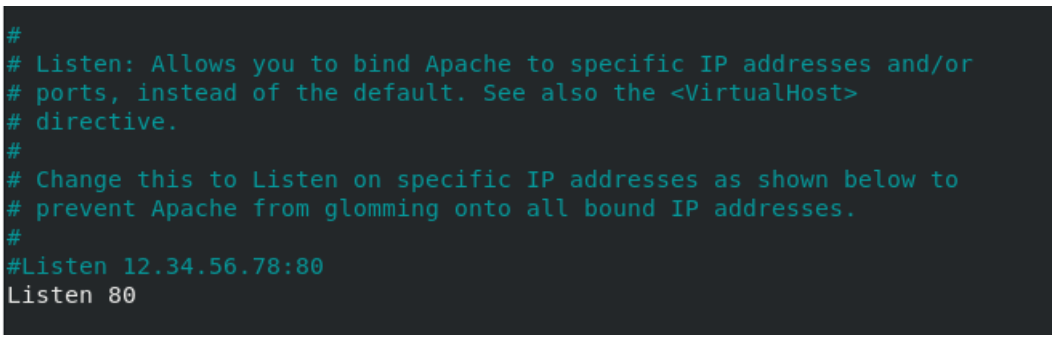

Рис. 3.19: Вернула конфиг. файл в первоначальное состояние

23. Удалила привязку http_port_t к 82 порту
24. Удалила файл /var/www/html/test.html

Действия пунктов 23-24 представленны на (рис. -@fig:020):

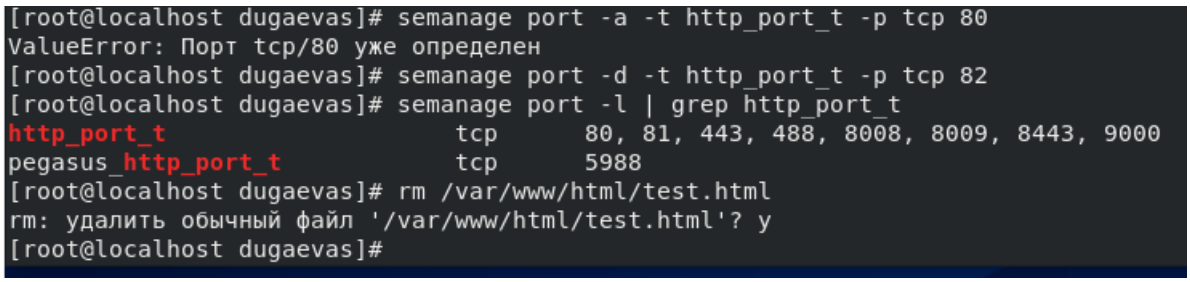

Рис. 3.20: Пункты 23-24

4 Выводы

Развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux. Проверила работу SELinx на практике совместно с веб-сервером Apache.