

Отчёт по лабораторной работе № 6

Информационная безопасность

Кинсиклунон Доря Флора

Содержание

0.1	Цель работы	4
0.2	Теоретическое введение	4
0.3	Выполнение лабораторной работы	5
0.4	Выводы	14
1	Список литературы	15

Список иллюстраций

1	Рис. 3.1: Проверка режима enforcing политики targeted	5
2	Рис. 3.2: 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	8
7	Рис. 6.7: Создание файла /var/www/html/test.html	9
8	Рис. 6.8: Обращение к файлу через веб-сервер	9
9	Рис. 6.9: Изменение контекста	10
10	Рис. 6.10: Обращение к файлу через веб-сервер	10
11	Рис. 6.11: Просмотр log-файла	11
12	Рис. 6.12: Установка веб-сервера Apache на прослушивание TCP- порта 81	11
13	Рис. 6.13: Перезапуск веб-сервера и анализ лог-файлов	11
14	Рис. 6.14: Содержание файла var/log/audit/audit.log	12
15	Рис. 6.15: Проверка установки порта 81	12
16	Рис. 6.16: Возвращение исходного контекста файлу	13
17	Рис. 6.17: Обращение к файлу через веб-сервер	13
18	Рис. 6.18: Возвращение Listen 80 и попытка удалить порт 81 . . .	13
19	Рис. 6.19: Удаление файла test.html	14

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

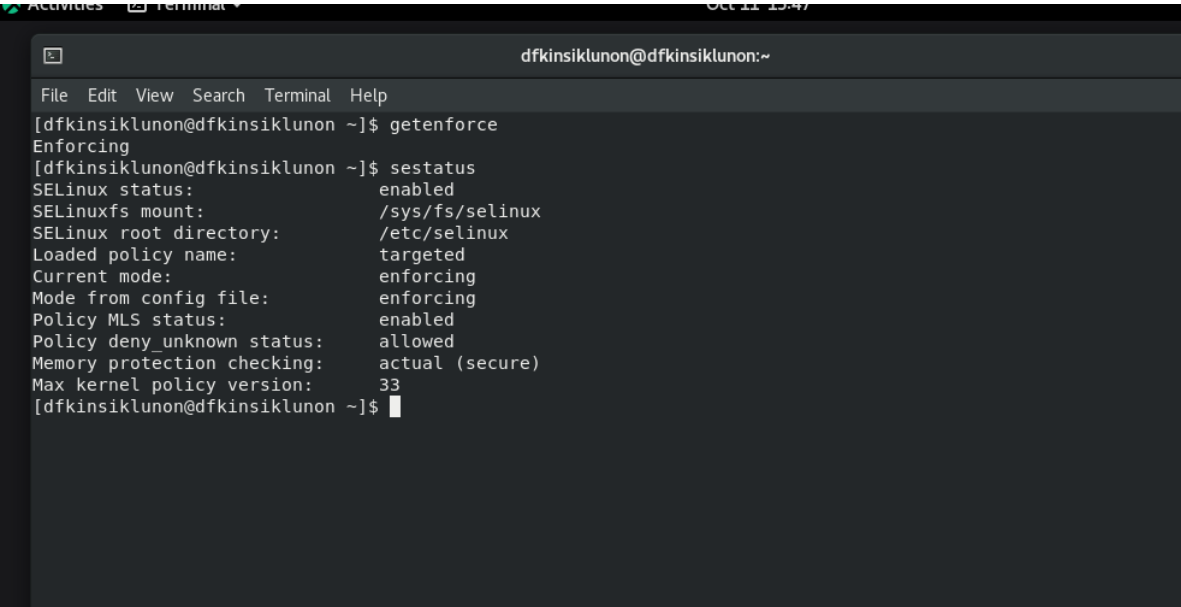
SELinux (Security-Enhanced Linux) обеспечивает усиление защиты путем внесения изменений как на уровне ядра, так и на уровне пространства пользователя, что превращает ее в действительно «непробиваемую» операционную систему. Впервые эта система появилась в четвертой версии CentOS, а в 5 и 6 версии реализация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



```
dfkinsiklunon@dfkinsiklunon:~$ getenforce
Enforcing
dfkinsiklunon@dfkinsiklunon:~$ 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
dfkinsiklunon@dfkinsiklunon:~$
```

Рис. 1: Рис. 3.1: Проверка режима enforcing политики targeted

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

```
dfkinsiklunon@dfkinsiklunon:~  
File Edit View Search Terminal Help  
[dfkinsiklunon@dfkinsiklunon ~]$ sudo systemctl start httpd  
[dfkinsiklunon@dfkinsiklunon ~]$ 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; vendor preset: disabled)  
   Active: active (running) since Wed 2023-10-11 15:51:54 MSK; 1min 25s ago  
     Docs: man:httpd.service(8)  
  Main PID: 37619 (httpd)  
    Status: "Running, listening on: port 80"  
    Tasks: 213 (limit: 12246)  
   Memory: 20.5M  
    CGroup: /system.slice/httpd.service  
            └─37619 /usr/sbin/httpd -DFOREGROUND  
              └─37626 /usr/sbin/httpd -DFOREGROUND  
                └─37627 /usr/sbin/httpd -DFOREGROUND  
                  └─37628 /usr/sbin/httpd -DFOREGROUND  
                    └─37629 /usr/sbin/httpd -DFOREGROUND  
  
Oct 11 15:51:53 dfkinsiklunon.localdomain systemd[1]: Starting The Apache HTTP Server...  
Oct 11 15:51:54 dfkinsiklunon.localdomain systemd[1]: Started The Apache HTTP Server.  
Oct 11 15:51:54 dfkinsiklunon.localdomain httpd[37619]: Server configured, listening on: port 80  
[dfkinsiklunon@dfkinsiklunon ~]$
```

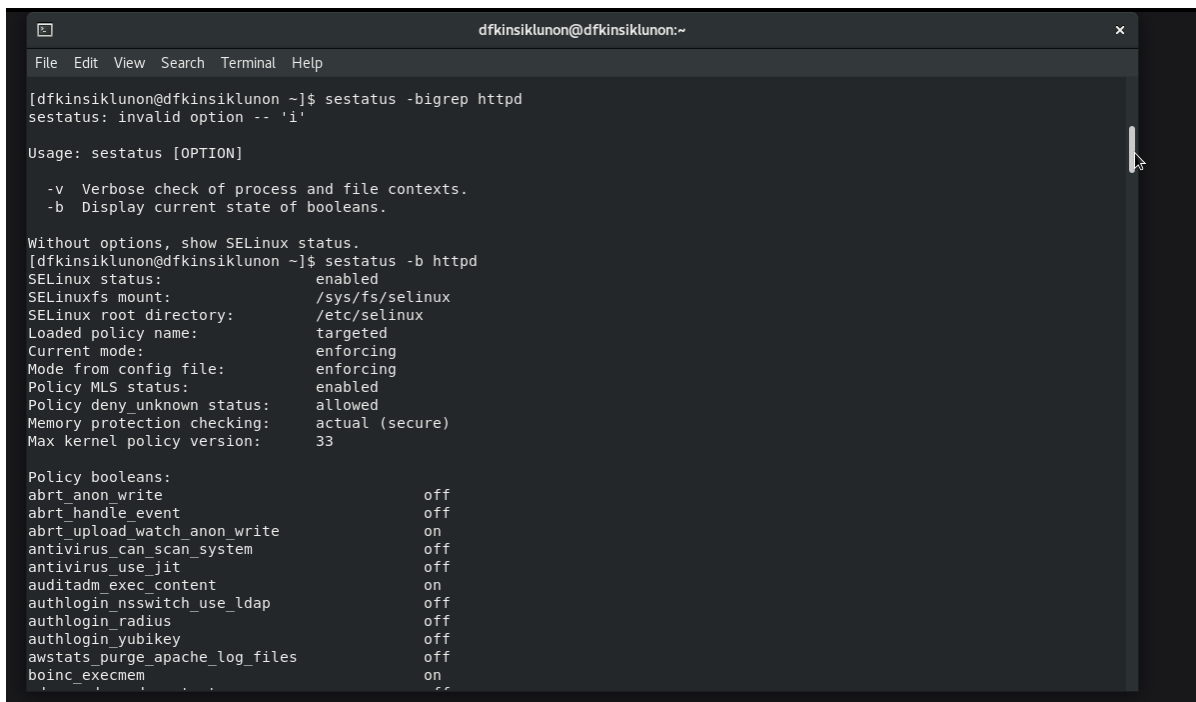
Рис. 2: Рис. 3.2: Проверка работы веб-сервера

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

```
dfkinsiklunon@dfkinsiklunon:~  
File Edit View Search Terminal Help  
[dfkinsiklunon@dfkinsiklunon ~]$ ps auxZ | grep httpd  
system_u:system_r:httpd_t:s0 root 37619 0.0 0.5 282968 12088 ? Ss 15:51 0:00 /usr/sbin/httpd -DFOREG  
ROUND  
system_u:system_r:httpd_t:s0 apache 37626 0.0 0.4 296852 8764 ? S 15:51 0:00 /usr/sbin/httpd -DFOREG  
ROUND  
system_u:system_r:httpd_t:s0 apache 37627 0.0 0.5 1354640 10384 ? Sl 15:51 0:00 /usr/sbin/httpd -DFOREG  
ROUND  
system_u:system_r:httpd_t:s0 apache 37628 0.0 0.6 1485768 12432 ? Sl 15:51 0:00 /usr/sbin/httpd -DFOREG  
ROUND  
system_u:system_r:httpd_t:s0 apache 37629 0.0 0.5 1354640 10384 ? Sl 15:51 0:00 /usr/sbin/httpd -DFOREG  
ROUND  
unconfined_u:unconfined_r:unconfined_t:s0-c0:c1023 dfkinsi+ 37937 0.0 0.0 221936 1096 pts/0 R+ 15:54 0:00 grep --col  
or=auto httpd  
[dfkinsiklunon@dfkinsiklunon ~]$
```

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).

A terminal window titled 'dfkinsiklunon@dfkinsiklunon:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the command 'sestatus -bigrep httpd' and its output. The output indicates an invalid option and provides usage information. It then shows the command 'sestatus -b httpd' and its output, which lists SELinux status and various policy booleans.

```
dfkinsiklunon@dfkinsiklunon ~]$ 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.
dfkinsiklunon@dfkinsiklunon ~]$ 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
```

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).

```
Oct 11 15:58
dfkinsiklunon@dfkinsiklunon:~
File Edit View Search Terminal Help

* 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: 31 (MLS enabled)
Target Policy: selinux
Handle unknown classes: allow
Classes: 132 Permissions: 464
Sensitivities: 1 Categories: 1024
Types: 4982 Attributes: 255
Users: 8 Roles: 14
Booleans: 339 Cond. Expr.: 387
Allow: 112932 Neverallow: 0
Auditallow: 166 Dontaudit: 10378
Type_trans: 252848 Type_change: 87
Type_member: 35 Range_trans: 5782
Role_allow: 38 Role_trans: 421
Constraints: 72 Validatetrans: 0
MLS Constrain: 72 MLS Val. Tran: 0
Permissives: 0 Polcap: 5
Defaults: 7 Typebounds: 0
Allowxperm: 0 Neverallowxperm: 0
Auditallowxperm: 0 Dontauditxperm: 0
Ibendportcon: 0 Ibpkeycon: 0
Initial SIDs: 27 Fs_use: 34
Genfscon: 107 Portcon: 646
Netifcon: 0 Nodecon: 0

[dfkinsiklunon@dfkinsiklunon ~]$
```

Рис. 5: Рис. 6.5: Статистика по политике

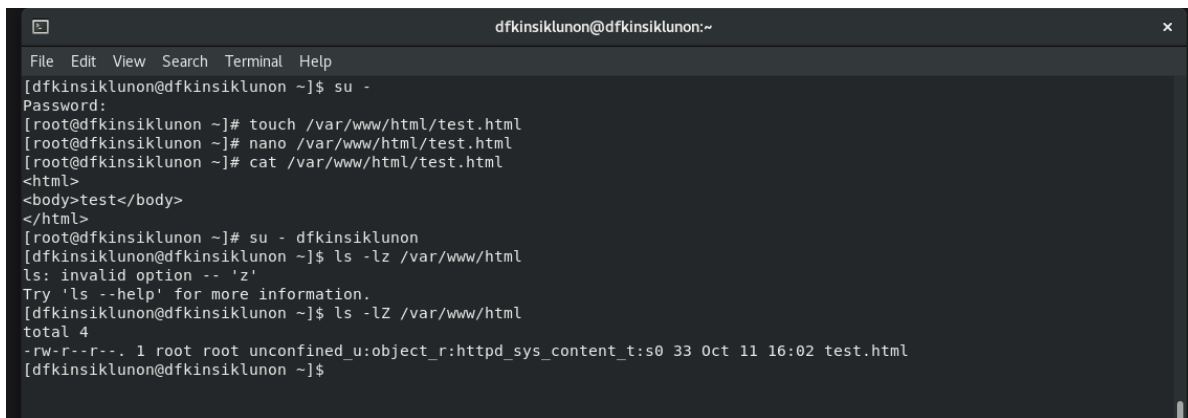
С помощью команды “ls -lZ /var/www” посмотрела файлы и поддиректории, находящиеся в директории /var/www. Используя команду “ls -lZ /var/www/html”, определила, что в данной директории файлов нет. Только владелец/суперпользователь может создавать файлы в директории /var/www/html (рис. 6.6).

```
Oct 11 15:59
dfkinsiklunon@dfkinsiklunon:~
File Edit View Search Terminal Help

[dfkinsiklunon@dfkinsiklunon ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Sep 23 02:22 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Sep 23 02:22 html
[dfkinsiklunon@dfkinsiklunon ~]$ ls -lZ /var/www/html
total 0
[dfkinsiklunon@dfkinsiklunon ~]$
```

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

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



```
dfkinsiklunon@dfkinsiklunon:~  
File Edit View Search Terminal Help  
[dfkinsiklunon@dfkinsiklunon ~]$ su -  
Password:  
[root@dfkinsiklunon ~]# touch /var/www/html/test.html  
[root@dfkinsiklunon ~]# nano /var/www/html/test.html  
[root@dfkinsiklunon ~]# cat /var/www/html/test.html  
<html>  
<body>test</body>  
</html>  
[root@dfkinsiklunon ~]# su - dfkinsiklunon  
[dfkinsiklunon@dfkinsiklunon ~]$ ls -lz /var/www/html  
ls: invalid option -- 'z'  
Try 'ls --help' for more information.  
[dfkinsiklunon@dfkinsiklunon ~]$ ls -lZ /var/www/html  
total 4  
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Oct 11 16:02 test.html  
[dfkinsiklunon@dfkinsiklunon ~]$
```

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).

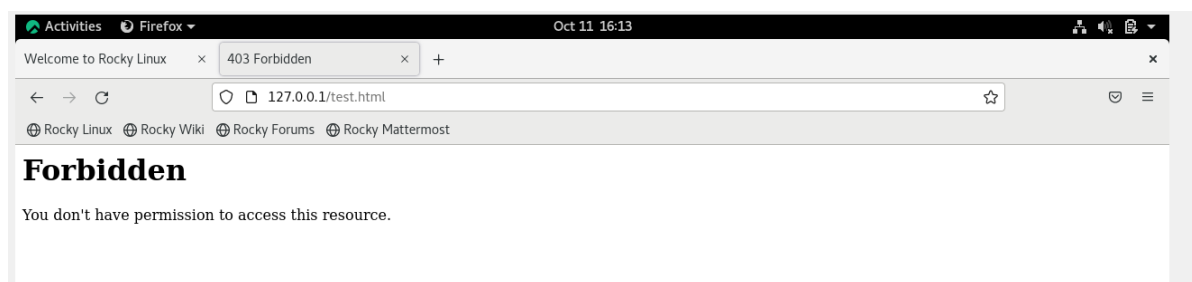


Рис. 10: Рис. 6.10: Обращение к файлу через веб-сервер

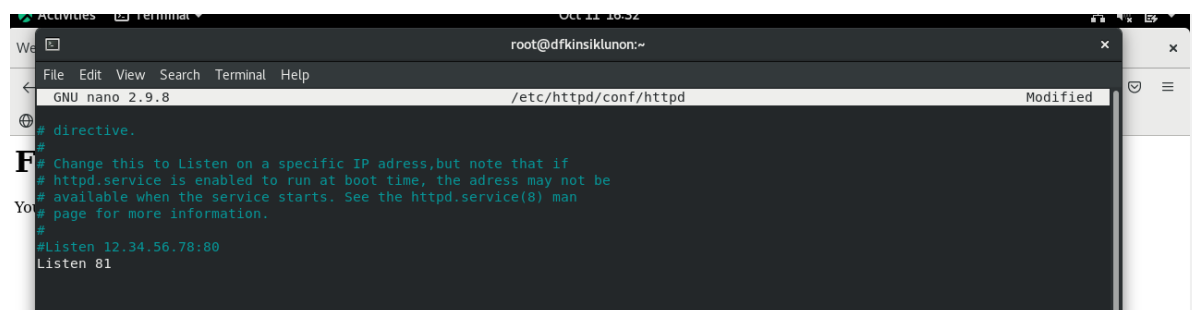
Командой “ls -l /var/www/html/test.html” убедилась, что читать данный файл может любой пользователь. Просмотрела системный лог-файл веб-сервера Apache командой “sudo tail /var/log/messages”, отображающий ошибки (рис. 6.11).



```
dfkinsiklunon@dfkinsiklunon:~  
File Edit View Search Terminal Help  
[dfkinsiklunon@dfkinsiklunon ~]$ ls -l /var/www/html/test.html  
-rw-r--r-- 1 root root 33 Oct 11 16:02 /var/www/html/test.html  
[dfkinsiklunon@dfkinsiklunon ~]$ tail /var/log/messages  
tail: cannot open '/var/log/messages' for reading: Permission denied  
[dfkinsiklunon@dfkinsiklunon ~]$ sudo tail /var/log/messages  
[sudo] password for dfkinsiklunon:  
Oct 11 16:13:24 dfkinsiklunon setroubleshot[39501]: failed to retrieve rpm info for /var/www/html/test.html  
Oct 11 16:13:24 dfkinsiklunon dbus-daemon[875]: [system] Activating service name='org.fedoraproject.SetroubleshotPrivileged' requested by ':1.532' (uid=991 pid=39501 comm="/usr/libexec/platform-python -Es /usr/sbin/setroub" label="system_u:system_r:setroubleshootd_t:s0-s0:c0.c1023") (using servicehelper)  
Oct 11 16:13:25 dfkinsiklunon dbus-daemon[875]: [system] Successfully activated service 'org.fedoraproject.SetroubleshotPrivileged'  
Oct 11 16:13:26 dfkinsiklunon setroubleshot[39501]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l d9369bad-0075-4880-81f8-8c37725e9c6f  
Oct 11 16:13:26 dfkinsiklunon setroubleshot[39501]: SELinux is preventing /usr/sbin/httpd from getattr 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 getattr 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 -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012  
Oct 11 16:14:43 dfkinsiklunon dbus-daemon[875]: [system] Activating via systemd: service name='net.reactivated.Fprint' unit='fprintd.service' requested by ':1.536' (uid=0 pid=40186 comm="sudo tail /var/log/messages " label="unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023")  
Oct 11 16:14:43 dfkinsiklunon systemd[1]: Starting Fingerprint Authentication Daemon...  
Oct 11 16:14:43 dfkinsiklunon dbus-daemon[875]: [system] Successfully activated service 'net.reactivated.Fprint'  
Oct 11 16:14:43 dfkinsiklunon systemd[1]: Started Fingerprint Authentication Daemon.  
Oct 11 16:15:13 dfkinsiklunon systemd[1]: fprintd.service: Succeeded.  
[dfkinsiklunon@dfkinsiklunon ~]$
```

Рис. 11: 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@dfkinsiklunon:~  
File Edit View Search Terminal Help  
GNU nano 2.9.8 /etc/httpd/conf/httpd Modified  
# 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
```

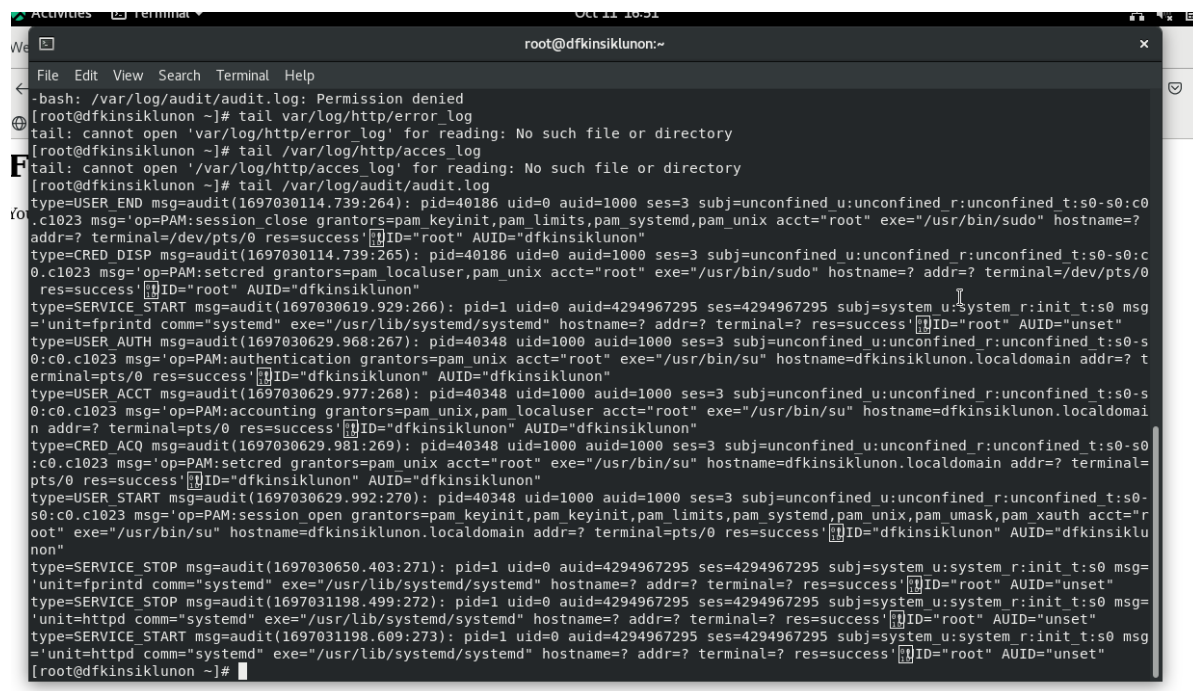
Рис. 12: Рис. 6.12: Установка веб-сервера Apache на прослушивание TCP-порта 81

Перезапускаем веб-сервер Apache и анализирует лог-файлы командой “tail -n1 /var/log/messages” (рис. 6.13).

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

Рис. 13: Рис. 6.13: Перезапуск веб-сервера и анализ лог-файлов

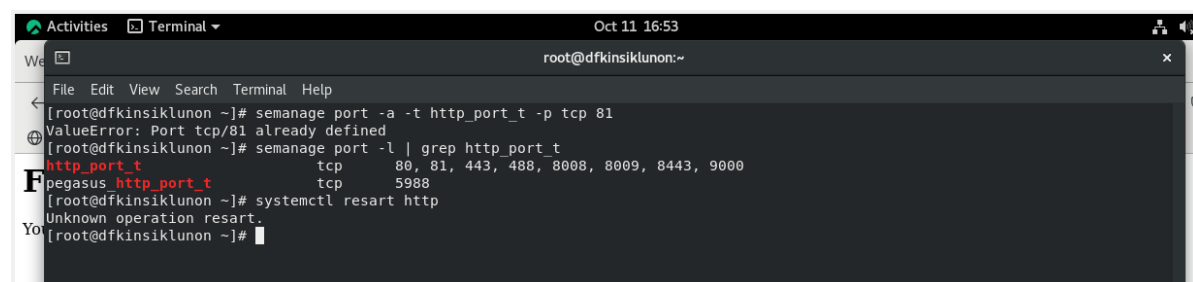
Просмотрела файлы “var/log/http/error_log”, “/var/log/http/access_log” и “/var/log/audit/audit.log” и выяснила, что запись появилась в последнем файле (рис. 6.14).



```
root@dfkinsiklunon:~# tail -n 20 /var/log/audit/audit.log
type=USER_END msg=audit(1697030114.739:264): pid=40186 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' ID="root" AUID="dfkinsiklunon"
type=CRED_DISP msg=audit(1697030114.739:265): pid=40186 uid=0 auid=1000 ses=3 subj=unconfined u:unconfined r:unconfined t:s0-s0:c
0.c1023 msg='op=PAM:setcred grantors=pam_localuser,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0
res=success' ID="root" AUID="dfkinsiklunon"
type=SERVICE_START msg=audit(1697030619.929:266): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system u:system r:init t:s0 msg=
'unit=fprintd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' ID="root" AUID="unset"
type=USER_AUTH msg=audit(1697030629.968:267): pid=40348 uid=1000 auid=1000 ses=3 subj=unconfined u:unconfined r:unconfined t:s0-s
0:c0.c1023 msg='op=PAM:authentication grantors=pam_unix acct="root" exe="/usr/bin/su" hostname=dfkinsiklunon.localdomain addr=? t
erminal=pts/0 res=success' ID="dfkinsiklunon" AUID="dfkinsiklunon"
type=USER_ACCT msg=audit(1697030629.977:268): pid=40348 uid=1000 auid=1000 ses=3 subj=unconfined u:unconfined r:unconfined t:s0-s
0:c0.c1023 msg='op=PAM:accounting grantors=pam_unix,pam_localuser acct="root" exe="/usr/bin/su" hostname=dfkinsiklunon.localdomai
n addr=? terminal=pts/0 res=success' ID="dfkinsiklunon" AUID="dfkinsiklunon"
type=CRED_ACQ msg=audit(1697030629.981:269): pid=40348 uid=1000 auid=1000 ses=3 subj=unconfined u:unconfined r:unconfined t:s0-s0
:c0.c1023 msg='op=PAM:setcred grantors=pam_unix acct="root" exe="/usr/bin/su" hostname=dfkinsiklunon.localdomain addr=? terminal=
pts/0 res=success' ID="dfkinsiklunon" AUID="dfkinsiklunon"
type=USER_START msg=audit(1697030629.992:270): pid=40348 uid=1000 auid=1000 ses=3 subj=unconfined u:unconfined r:unconfined t:s0-
s0:c0.c1023 msg='op=PAM:session_open grantors=pam_keyinit,pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_umask,pam_xauth acct="r
oot" exe="/usr/bin/su" hostname=dfkinsiklunon.localdomain addr=? terminal=pts/0 res=success' ID="dfkinsiklunon" AUID="dfkinsiklu
non"
type=SERVICE_STOP msg=audit(1697030650.403:271): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system u:system r:init t:s0 msg=
'unit=fprintd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' ID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1697031198.499:272): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system u:system r:init t:s0 msg=
'unit=htpdd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' ID="root" AUID="unset"
type=SERVICE_START msg=audit(1697031198.609:273): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system u:system r:init t:s0 msg=
'unit=htpdd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' ID="root" AUID="unset"
[root@dfkinsiklunon ~]#
```

Рис. 14: Рис. 6.14: Содержание файла var/log/audit/audit.log

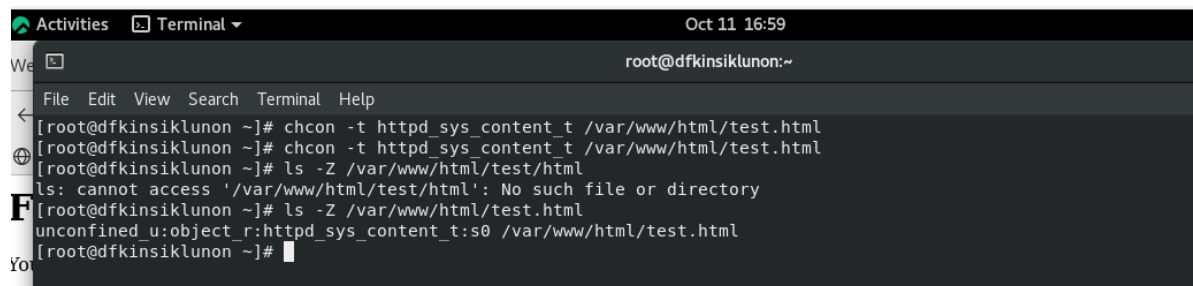
Выполнила команду “semanage port -a -t http_port_t -p tcp 81” и убедилась, что порт TCP-81 установлен. Проверила список портов командой “semanage port -l | grep http_port_t”, убедилась, что порт 81 есть в списке и запускаем веб-сервер Apache снова (рис. 6.15).



```
root@dfkinsiklunon:~# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@dfkinsiklunon ~]# 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@dfkinsiklunon ~]# systemctl resart http
Unknown operation resart.
[root@dfkinsiklunon ~]#
```

Рис. 15: 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, введя адрес “http://127.0.0.1:81/test.html”, в результате чего увидела содержимое файла - слово “test” (рис. 6.17).



```
Oct 11 16:59
root@dfkinsiklunon:~
File Edit View Search Terminal Help
[root@dfkinsiklunon ~]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@dfkinsiklunon ~]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@dfkinsiklunon ~]# ls -Z /var/www/html/test/html
ls: cannot access '/var/www/html/test/html': No such file or directory
[root@dfkinsiklunon ~]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@dfkinsiklunon ~]#
```

Рис. 16: Рис. 6.16: Возвращение исходного контекста файлу

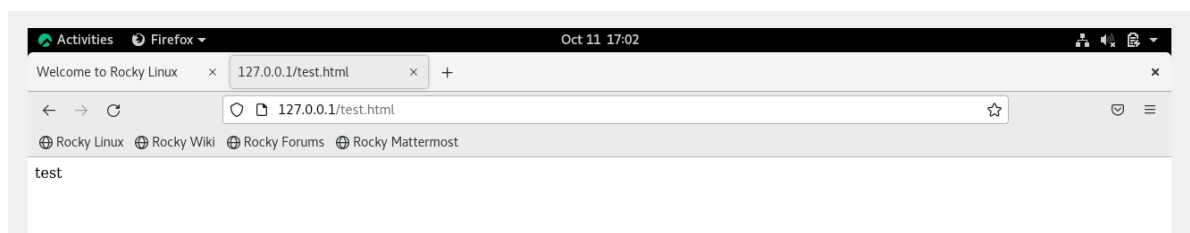


Рис. 17: Рис. 6.17: Обращение к файлу через веб-сервер

Исправила 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).

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

Рис. 18: 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. 3.19).

Рис. 6.19: Удаление файла test.html

Рис. 19: 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.

1 Список литературы

1. SELinux – описание и особенности работы с системой [Электронный ресурс]. URL: <https://habr.com/ru/company/kingservers/blog/209644/>.
2. Что такое Apache и зачем он нужен? [Электронный ресурс]. URL: <https://2domains.ru/support/vps-i-servery/shto-takoye-apache>.