

# **Отчёт по лабораторной работе №06**

**Дисциплина: Основы информационной безопасности**

**Бансимба Клодели Дьегра НПИбд-02-22**

# Содержание

1	6.1 Цель работы	4
2	6.2 Порядок выполнения работы	5
3	Выводы	14

## Список иллюстраций

2.1	запуск http . . . . .	6
2.2	переключатели SELinux для http . . . . .	7
2.3	переключатели SELinux для http . . . . .	8
2.4	создание html-файла и доступ по http . . . . .	9
2.5	создание html-файла и доступ по http . . . . .	9
2.6	создание html-файла и доступ по http . . . . .	9
2.7	Изменение контекст файла . . . . .	10
2.8	ошибка доступа после изменения контекста . . . . .	10
2.9	лог ошибок . . . . .	11
2.10	переключение порта . . . . .	12
2.11	доступ по http на 81 порт . . . . .	12

## **1 6.1 Цель работы**

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

## 2 6.2 Порядок выполнения работы

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: `service httpd status` или `/etc/rc.d/init.d/httpd status`. Если не работает, запустите его так же, но с параметром `start`.

```
claudeybansimba@claudey:~ — /bin/systemctl status httpd.service
[claudeybansimba@claudey ~]$ getenforce
Enforcing
[claudeybansimba@claudey ~]$ 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
[claudeybansimba@claudey ~]$
[claudeybansimba@claudey ~]$ 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: inactive (dead)
     Docs: man:httpd.service(8)

[1]+  Stopped                  service httpd status
[claudeybansimba@claudey ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service

[claudeybansimba@claudey ~]$
[claudeybansimba@claudey ~]$ 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 Sat 2024-04-27 17:23:49 MSK; 4s ago
     Docs: man:httpd.service(8)
  Main PID: 34920 (httpd)
    Status: "Started, listening on: port 80"
    Tasks: 213 (limit: 23033)
   Memory: 35.5M
      CPU: 136ms
   CGroup: /system.slice/httpd.service
           └─34920 /usr/sbin/httpd -DFOREGROUND
           └─34928 /usr/sbin/httpd -DFOREGROUND
           └─34929 /usr/sbin/httpd -DFOREGROUND
```

Рис. 2.1: запуск http

2. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду `ps auxZ | grep httpd` или `ps -eZ | grep httpd`. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd`. Обратите внимание, что многие из них находятся в положении «off».

```

[3]+ Stopped service httpd status
[claudelybansimba@claudely ~]$ ps auxZ | grep httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 claudel+ 34874 0.0 0.2 23622
0 8760 pts/1 T 17:23 0:00 /bin/systemctl status httpd.service
system_u:system_r:httpd_t:s0 root 34920 0.0 0.3 20332 11604 ? Ss
17:23 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 34928 0.0 0.1 21668 7432 ? S
17:23 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 34929 0.0 0.4 2455800 15220 ? Sl
17:23 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 34930 0.0 0.4 2259128 17264 ? Sl
17:23 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 34931 0.0 0.4 2259128 15224 ? Sl
17:23 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 claudel+ 35168 0.0 0.2 23622
0 8992 pts/1 T 17:23 0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 claudel+ 35222 0.0 0.2 23622
0 8972 pts/1 T 17:26 0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 claudel+ 35242 0.0 0.0 22166
4 2296 pts/1 S+ 17:27 0:00 grep --color=auto httpd
[claudelybansimba@claudely ~]$
[claudelybansimba@claudely ~]$
[claudelybansimba@claudely ~]$ 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.
[claudelybansimba@claudely ~]$

```

Рис. 2.2: переключатели SELinux для http

3. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов. Определите тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www`. В поддиректориях могут располагаться системные скрипты и контент для http.

```

[claudelybansimba@claudely ~]$
[claudelybansimba@claudely ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow
Classes:                  135
Sensitivities:            1
Types:                    5100
Users:                     8
Booleans:                 353
Allow:                    65009
Auditallow:               170
Type_trans:               265337
Type_member:              35
Role_allow:               38
Constraints:              70
MLS Constrain:            72
Permissives:              2
Defaults:                 7
Allowxperm:               0
Auditallowxperm:          0
Ibendportcon:             0
Initial SIDs:             27
Genfscon:                 109
Netifcon:                 0
Permissions:              457
Categories:               1024
Attributes:               258
Roles:                    14
Cond. Expr.:              384
Neverallow:               0
Dontaudit:                8572
Type_change:              87
Range_trans:              6164
Role_trans:               420
Validatetrans:            0
MLS Val. Tran:            0
Polcap:                   6
Typebounds:               0
Neverallowxperm:          0
Dontauditxperm:           0
Ibpkeycon:                0
Fs_use:                   35
Portcon:                  660
Nodecon:                  0
[claudelybansimba@claudely ~]$
[claudelybansimba@claudely ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Oct 28 12:35
  cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 Oct 28 12:35
  html
[claudelybansimba@claudely ~]$
[claudelybansimba@claudely ~]$

```

Рис. 2.3: переключатели SELinux для http

4. Определите тип файлов, находящихся в директории /var/www/html: `ls -lZ /var/www/html`. В директории изначально нет файлов. Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html. Создавать файлы может только root. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания: Test



```

[claudeybansimba@cloudely ~]$
[claudeybansimba@cloudely ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Oct 28 12:35
  cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 Oct 28 12:35
  html
[claudeybansimba@cloudely ~]$
[claudeybansimba@cloudely ~]$ ls -lZ /var/www/html
total 0
[claudeybansimba@cloudely ~]$
[claudeybansimba@cloudely ~]$
[claudeybansimba@cloudely ~]$
[claudeybansimba@cloudely ~]$
[claudeybansimba@cloudely ~]$ sudo touch /var/www/html/test.html
[sudo] password for claudeybansimba:
[claudeybansimba@cloudely ~]$ sudo vi /var/www/html/test.html
[claudeybansimba@cloudely ~]$

```

Рис. 2.4: создание html-файла и доступ по http

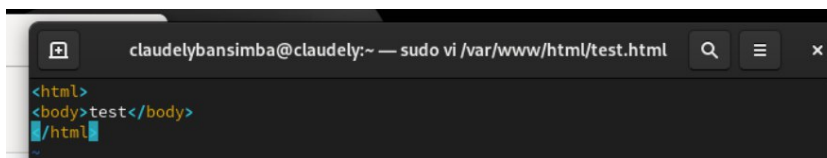


Рис. 2.5: создание html-файла и доступ по http

5. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html. Обратитесь к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедитесь, что файл был успешно отображён.

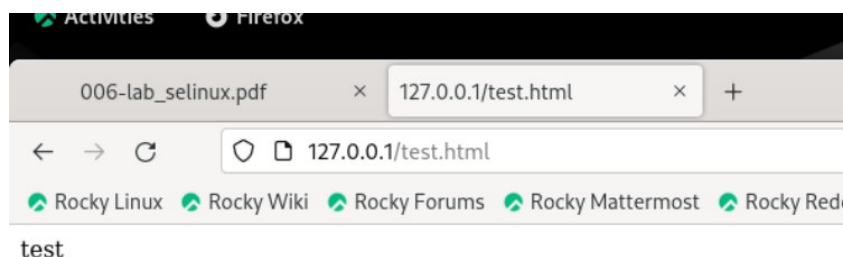


Рис. 2.6: создание html-файла и доступ по http

6. Изучите справку `man httpd_selinux` и выясните, какие контексты файлов определены для `httpd`. Сопоставьте их с типом файла `test.html`. Проверить контекст файла можно командой `ls -Z`. `ls -Z /var/www/html/test.html`.

Основным контекстом является `httpd_sys_content_t`, его мы и увидели в выводе команды. Измените 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` После этого проверьте, что контекст поменялся.

```
[claudeybansimba@cloudely ~]$
[claudeybansimba@cloudely ~]$ ls -lZ /var/www/html
total 0
[claudeybansimba@cloudely ~]$
[claudeybansimba@cloudely ~]$
[claudeybansimba@cloudely ~]$
[claudeybansimba@cloudely ~]$
[claudeybansimba@cloudely ~]$ sudo touch /var/www/html/test.html
[sudo] password for claudeybansimba:
[claudeybansimba@cloudely ~]$ sudo vi /var/www/html/test.html
[claudeybansimba@cloudely ~]$
[claudeybansimba@cloudely ~]$
[claudeybansimba@cloudely ~]$ ps auxZ | grep test.html
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 claudeyl+ 35741 0.0 0.0 22179
6 2276 pts/1 S+ 17:40 0:00 grep --color=auto test.html
[claudeybansimba@cloudely ~]$
[claudeybansimba@cloudely ~]$ ls -lZ /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[claudeybansimba@cloudely ~]$
```

Рис. 2.7: Изменение контекст файла

7. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Вы должны получить сообщение об ошибке: `Forbidden You don't have permission to access /test.html on this server`. При изменении контекста файл стал считаться чужим для `http` и программа не может его прочитать.

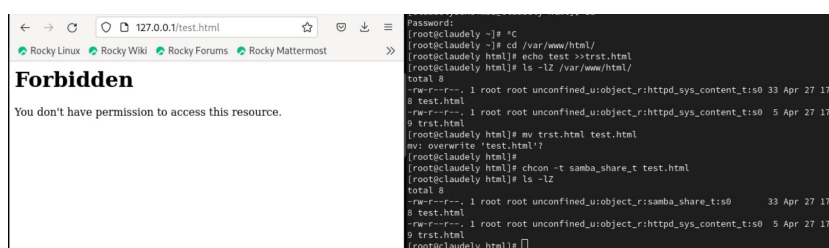


Рис. 2.8: ошибка доступа после изменения контекста

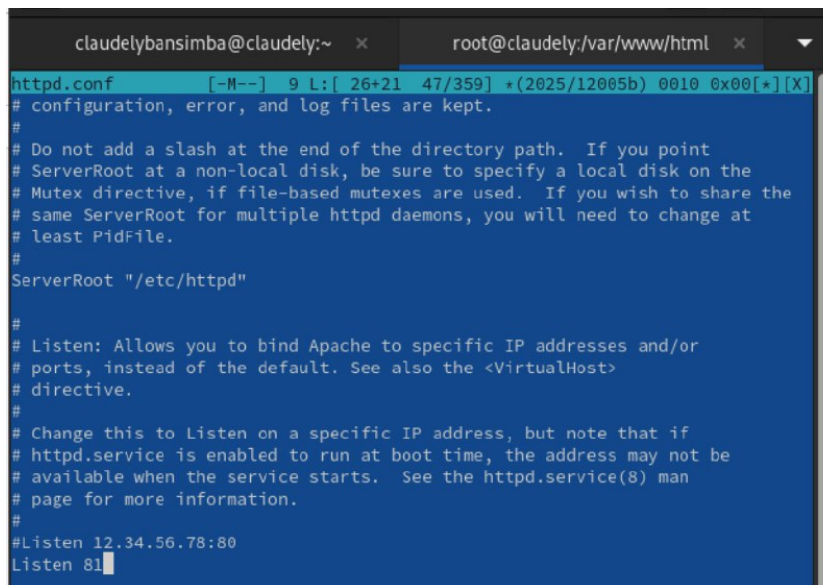
8. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? `ls -l`

/var/www/html/test.html Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: tail /var/log/messages Если в системе окажутся запущенными процессы setroubleshootd и auditd, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле /var/log/audit/audit.log. Проверьте это утверждение самостоятельно.

```
[root@cloudely html]#
[root@cloudely html]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 Apr 27 17:38 /var/www/html/test.html
[root@cloudely html]# tail /var/log/messages
Apr 27 18:02:41 cloudely setroubleshoot[36283]: failed to retrieve rpm info for path
'/var/www/html/test.html':
Apr 27 18:02:41 cloudely systemd[1]: Started dbus-:1.1-org.fedoraproject.Setroubles
hootPrivileged@1.service.
Apr 27 18:02:43 cloudely setroubleshoot[36283]: SELinux is preventing /usr/sbin/http
d from getattr access on the file /var/www/html/test.html. For complete SELinux me
ssages run: sealert -l e12cc3f6-c303-4244-blec-739240c6e247
Apr 27 18:02:43 cloudely setroubleshoot[36283]: SELinux is preventing /usr/sbin/http
d from getattr access on the file /var/www/html/test.html.#012#012***** Plugin re
storecon (92.2 confidence) suggests *****#012#012If you want t
o fix the label. #012/var/www/html/test.html default label should be httpd_sys_cont
ent_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 chan
ge 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 ne
ed to change the label on test.html to public_content_t or public_content_rw_t.#012
Do#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012# res
torecon -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.#012D
o#012allow this access for now by executing:#012# ausearch -c 'httpd' --raw | audit
2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Apr 27 18:02:43 cloudely setroubleshoot[36283]: SELinux is preventing /usr/sbin/http
d from getattr access on the file /var/www/html/test.html. For complete SELinux me
ssages run: sealert -l e12cc3f6-c303-4244-blec-739240c6e247
Apr 27 18:02:43 cloudely setroubleshoot[36283]: SELinux is preventing /usr/sbin/http
d from getattr access on the file /var/www/html/test.html.#012#012***** Plugin re
storecon (92.2 confidence) suggests *****#012#012If you want t
o fix the label. #012/var/www/html/test.html default label should be httpd_sys_cont
ent_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 chan
ge 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 ne
ed to change the label on test.html to public_content_t or public_content_rw_t.#012
Do#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012# res
torecon -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.#012D
o#012allow this access for now by executing:#012# ausearch -c 'httpd' --raw | audit
2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
```

Рис. 2.9: лог ошибок

9. Попробуйте запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf найдите строчку Listen 80 и замените её на Listen 81.



```
claudelybansimba@claudely:~ x root@claudely:/var/www/html x
httpd.conf [-M--] 9 L: 26+21 47/359 *(2025/12005b) 0010 0x00[*][X]
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path. If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used. If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# 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
```

Рис. 2.10: переключение порта

10. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему? Сбой не происходит, порт 81 уже вписан в разрешенные
11. Проанализируйте лог-файлы: `tail -nl /var/log/messages` Просмотрите файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log` и выясните, в каких файлах появились записи. . Верните контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`: `chcon -t httpd_sys_content_t /var/www/html/test.html` После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. Вы должны увидеть содержимое файла — слово «test».

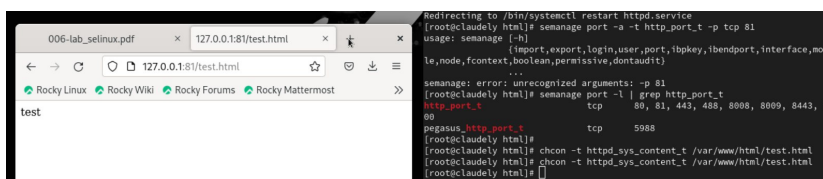


Рис. 2.11: доступ по http на 81 порт

12. Исправьте обратно конфигурационный файл apache, вернув Listen 80.

13. Удалите привязку `http_port_t` к 81 порту: `semanage port -d -t http_port_t -p tcp 81` и проверьте, что порт 81 удалён.
14. Удалите файл `/var/www/html/test.html`: `rm /var/www/html/test.html`

## **3 Выводы**

В процессе выполнения лабораторной работы мною были получены базовые навыки работы с технологией seLinux.