Лабораторная работа №6

Мандатное разграничение прав в Linux

Поляков Арсений Андреевич

Содержание

Цель работы

Целью данной лабораторной работы является развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinx на практике совместно с веб-сервером Apache.

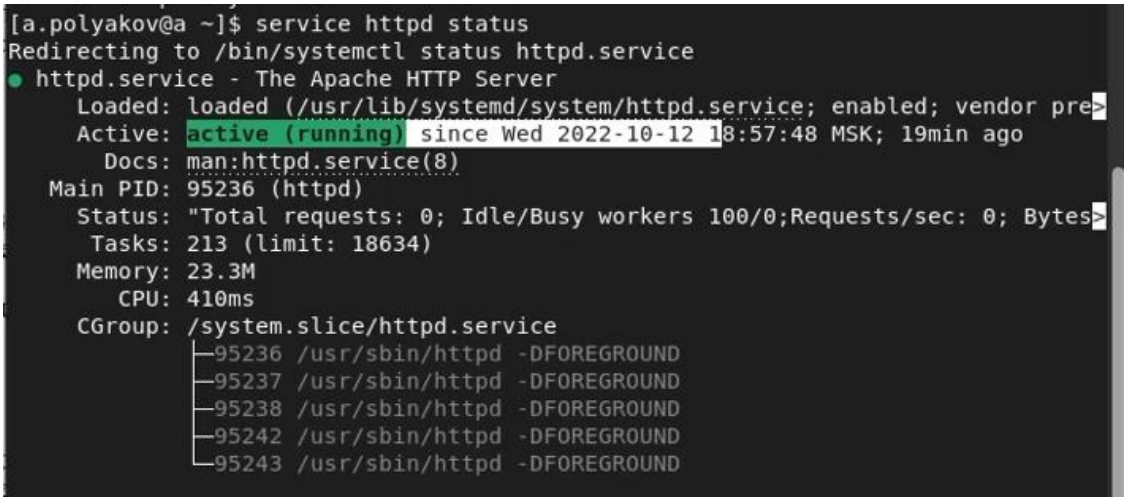
Выполнение лабораторной работы

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

```
[a.polyakov@a ~]$ getenforce
Enforcing
[a.polyakov@a ~]$ 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
```

Выполнение команд getenforce и sestatus

2. Запустили веб-сервер и обратились к нему с помощью команды: service httpd status

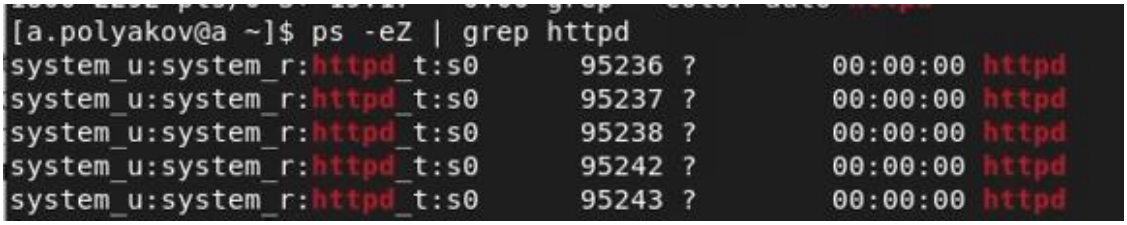


Выполнение команды status

3. Найшли веб-сервер Apache в списке процессов с помощью команды **ps auxZ | grep httpd**. Контекст безопасности - unconfined_u:unconfined_r:unconfined_t.

Выполнение команды ps auxZ | grep httpd

4. Посмотрели текущее состояние переключателей SELinux для Apache с помощью команды .



Выполнение команды sestatus -ez

5. Посмотрели статистику по политике с помощью команды **seinfo**. Определили, что множество пользователей = 8; ролей = 14; типов = 5002.

```
httpd_mod_auth_ntlm_winbind                off
httpd_mod_auth_pam                         off
httpd_read_user_content                    off
httpd_run_ipa                              off
httpd_run_preupgrade                       off
httpd_run_stickshift                       off
httpd_serve_cobbler_files                  off
httpd_setrlimit                            off
httpd_ssi_exec                             off
httpd_sys_script_anon_write                off
httpd_tmp_exec                             off
httpd_tty_comm                             off
httpd_unified                              off
httpd_use_cifs                             off
httpd_use_fusefs                           off
httpd_use_gpg                              off
httpd_use_nfs                              off
httpd_use_opencryptoki                     off
httpd_use_openstack                        off
httpd_use_sasl                             off
httpd_verify_dns                           off
```

Статистика по политике

6. Определили тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды **ls -lZ /var/www**.

```
[a.polyakov@a ~]$ 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 15:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0     6 May 16 15:10 html
```

Выполнение команды ls -lZ /var/www

7. Необходимо было определить тип файлов, находящихся в директории /var/www/html, с помощью команды **ls -lZ /var/www/html**. Но в данной директории файлов не обнаружилось.

```
[a.polyakov@a ~]$ ls -lZ /var/www/html
total 0
```

Выполнение команды ls -lZ /var/www/html

9. Создали от имени суперпользователя html-файл /var/www/html/test.html следующего содержания:

Open

*test.html
/var/www/html

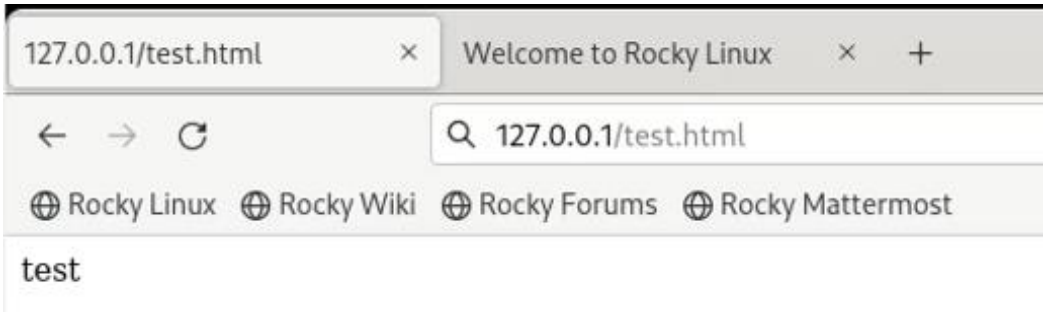
```
1 <html>
2 <body>test</body>
3 </html>
```

Содержимое файла test.html

10. Проверили контекст созданного файла - httpd_sys_content_t.

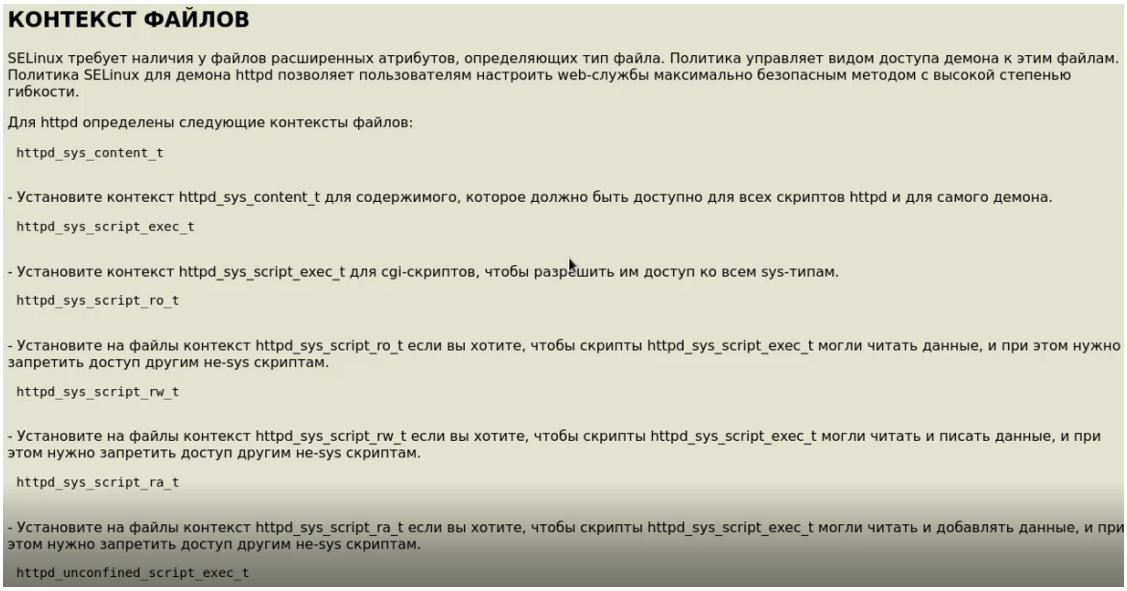
Контекст файла test.html

11. Обратитились к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html и убедились, что файл был успешно отображён.



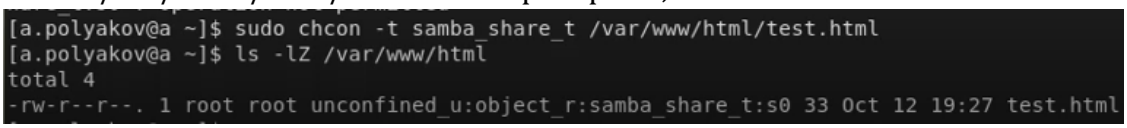
Обращение к файлу test.html через веб-сервер

12. Изучили справку man httpd_selinux. Тип файла test.html - контекст созданного файла - httpd_sys_content_t.



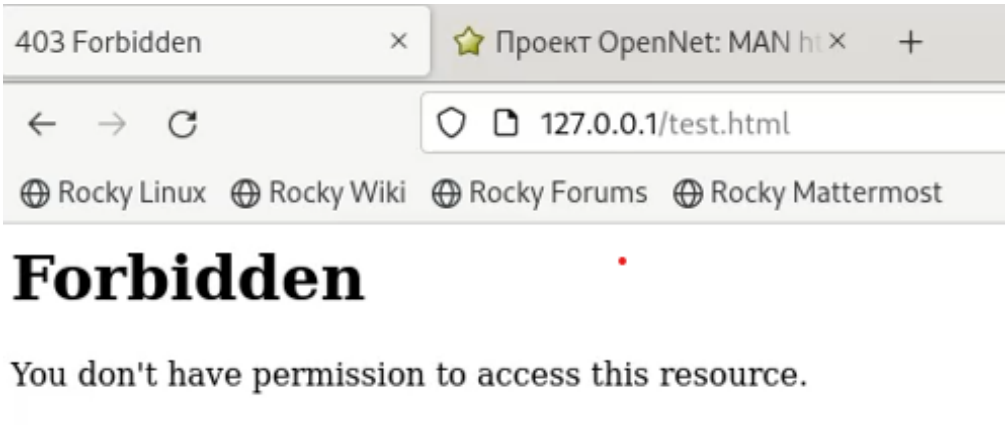
Контекст файла test.html

13. Изменили контекст файла /var/www/html/test.html с httpd_sys_content_t на samba_share_t: chcon -t samba_share_t /var/www/html/test.html ls -Z /var/www/html/test.html И проверили, что контекст поменялся.



Изменение контекста файла /var/www/html/test.html

14. Пробуем ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. В результате получили ошибку.



Обращение к файлу test.html через веб-сервер после изменения контекста

15. Проанализируем ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? ls -l /var/www/html/test.html Просмотрим log-файлы веб-сервера Apache и системный лог-файл: tail /var/log/messages В системе оказались запущенны процессы **setroubleshootd** и **audtd**.

```
[a.polyakov@a ~]$ sudo tail /var/log/messages
Oct 12 19:33:17 a setroubleshoot[97478]: failed to retrieve rpm info for /var/www/html/test.ht
ml
Oct 12 19:33:17 a setroubleshoot[97478]: SELinux is preventing /usr/sbin/httpd from getattr ac
cess on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 2d869f
b5-9db8-4f5a-acdf-2a6546f92eaf
Oct 12 19:33:17 a setroubleshoot[97478]: SELinux is preventing /usr/sbin/httpd from getattr ac
cess on the file /var/www/html/test.html.#012#012*****  Plugin restorecon (92.2 confidence) su
ggests   ********************#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 a
ttempt may have been stopped due to insufficient permissions to access a parent directory in w
hich 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 fconte
```

Вывод команд ls -l /var/www/html/test.html и tail /var/log/messages

16. Попробуем запустить веб-сервер Apache на прослушивание TCP-порта 81. Для этого в файле /etc/httpd/httpd.conf находим строчку Listen 80 и заменяем её на Listen 81.

```
46 #Listen 12.34.56.78:80
47 Listen 81
```

Запуск веб-сервера Apache на прослушивание TCP-порта 81

17. Выполним перезапуск веб-сервера Apache. Произошёл сбой? Нет.
18. Проанализируем лог-файлы: tail -nl /var/log/messages Просмотрим файлы /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log.

```
[a.polyakov@a ~]$ sudo tail /var/log/messages
Oct 12 19:40:18 a systemd[1385]: Started Application launched by gnome-shell.
Oct 12 19:40:20 a rtkit-daemon[739]: Successfully made thread 98319 of process 98203 (/usr/lib64/firefox/firefox) ow
ned by '1000' RT at priority 10.
Oct 12 19:40:25 a firefox.desktop[98203]: Missing chrome or resource URL: resource://gre/modules/UpdateListener.jsm
Oct 12 19:40:25 a firefox.desktop[98203]: Missing chrome or resource URL: resource://gre/modules/UpdateListener.sys.
mjs
Oct 12 19:40:54 a systemd[1]: Stopping The Apache HTTP Server...
Oct 12 19:40:55 a systemd[1]: httpd.service: Deactivated successfully.
Oct 12 19:40:55 a systemd[1]: Stopped The Apache HTTP Server.
Oct 12 19:40:55 a systemd[1]: Starting The Apache HTTP Server...
Oct 12 19:41:06 a systemd[1]: Started The Apache HTTP Server.
Oct 12 19:41:06 a httpd[98501]: Server configured, listening on: port 81
```

Перезапуск веб-сервера Apache

19. Выполним команду **semanage port -a -t http_port_t -p tcp 81**. Вылетает ValueError в связи с тем, что порт уже определен. После этого проверим список портов командой **semanage port -l | grep http_port_t** и убедились, что порт 81 появился в списке.

```
[a.polyakov@a ~]$ sudo semanage port -a -p tcp 81 -t http_port_t
ValueError: Port tcp/81 already defined
[a.polyakov@a ~]$ sudo semanage port -l | grep http_port_t
http_port_t                    tcp      80, 81, 443, 488, 8008, 8009, 8443
pegasus_http_port_t            tcp      5988
```

Проверка установления 81 порта tcp

20. Попробуем запустить веб-сервер Apache ещё раз.

```
[a.polyakov@a ~]$ sudo systemctl restart httpd
```

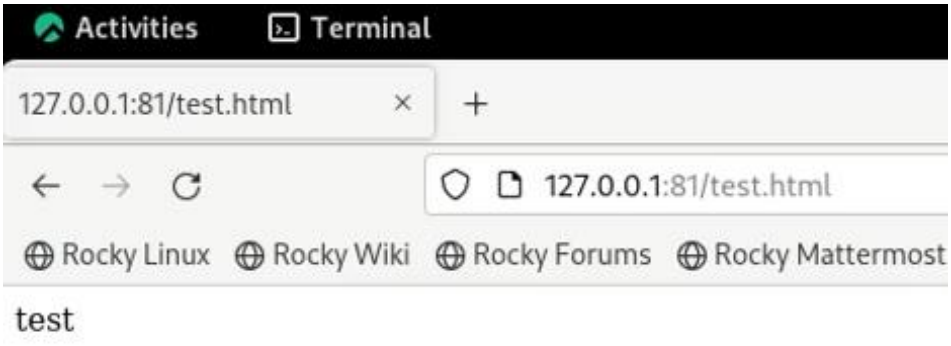
Перезапуск веб-сервера Apache

21. Вернули контекст httpd_sys_content__t к файлу /var/www/html/test.html: **chcon -t httpd_sys_content_t /var/www/html/test.html**

```
[a.polyakov@a ~]$ sudo chcon -t httpd_sys_content_t /var/www/html/test.htm
```

Возвращение контекста httpd_sys_content__t к файлу test.html

После этого пробуем получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. В результате увидели содержимое файла — слово «test».



Обращение к файлу test.html через веб-сервер

22. Исправим обратно конфигурационный файл apache, вернув Listen 80.

```
46 #Listen 12.34.56.78:80
47 Listen 80
48
```

Исправление конфигурационного файла apache

23. Удалим привязку http_port_t к 81 порту: **semanage port -d -t http_port_t -p tcp 81** и проверим, что порт 81 удалён. Данная команда не была выполнена.

```
[a.polyakov@a ~]$ sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
```

Удаление привязки http_port_t к 81 порту

24. Удалим файл /var/www/html/test.html: **rm /var/www/html/test.html**.

```
[a.polyakov@a ~]$ sudo rm /var/www/html/test.html
[a.polyakov@a ~]$ ls /var/www/html
[a.polyakov@a ~]$ ls -l /var/www/html
total 0
```

Удаление файла test.html

Вывод

В ходе выполнения лабораторной работы мы развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux1. Проверили работу SELinx на практике совместно с веб-сервером Apache.

Библиография

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Мандатное разграничение прав в Linux [Текст] / Кулябов Д. С., Королькова А. В., Геворкян М. Н. - Москва: - 5 с. [^1]: Мандатное разграничение прав в Linux.
2. Справочник 70 основных команд Linux: полное описание с примерами (https://eternalhost.net/blog/sozdanie-saytov/osnovnye-komandy-linux)