

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ПРЕЗЕНТАЦИЯ ПО ЛАБОРАТОРНОЙ РАБОТЕ №6

дисциплина: Информационная безопасность

Преподаватель: Кулябов Дмитрий Сергеевич

Студент: Попова Юлия Дмитриевна

Группа: НФИбд-01-19

МОСКВА 2022 г.

Цель работы

Целью данной лабораторной работы является развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux¹. Проверить работу SELinux 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**.

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

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

3. Найшли веб-сервер Apache в списке процессов с помощью команды **ps auxZ | grep httpd**.

Контекст безопасности - `unconfined_u:unconfined_r:unconfined_t`.

```
root@kondashnikova:~# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 39619 0.0 0.5 20248 11704 ? Ss 17:09
0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 39620 0.0 0.3 21572 7444 ? S 17:09
0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 39624 0.0 0.5 1079376 11100 ? Sl 17:09
0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 39625 0.0 0.6 1210512 13148 ? Sl 17:09
0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 39626 0.0 0.5 1079376 11100 ? Sl 17:09
0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 40041 0.0 0.1 221692 2292 pts/0 S
+ 17:30 0:00 grep --color=auto httpd
```

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

```
root@kondashnikova:~# sestatus -b | grep httpd
httpd_anon_write off
httpd_builtin_scripting on
httpd_can_check_spam off
httpd_can_connect_ftp off
httpd_can_connect_ldap off
httpd_can_connect_mythtv off
httpd_can_connect_zabbix off
httpd_can_manage_courier_spool off
httpd_can_network_connect off
httpd_can_network_connect_cobbler off
httpd_can_network_connect_db off
httpd_can_network_memcache off
httpd_can_network_relay off
httpd_can_sendmail off
httpd_dbus_avaahi off
httpd_dbus_sssd off
httpd_dontaudit_search_dirs off
httpd_enable_cgi on
httpd_enable_ftp_server off
httpd_enable_homedirs off
httpd_execmem off
httpd_graceful_shutdown off
httpd_manage_ipa off
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
```

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


```
итоги 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0
```

6. Создали от имени суперпользователя

html-файл `/var/www/html/test.html` следующего содержания:

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

7. Проверили контекст созданного файла - `httpd_sys_content_t`.

 Контекст файла `test.html`

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



test

9. Изменили контекст файла И проверили, что контекст поменялся.

10. 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.



Forbidden

You don't have permission to access this resource

11. 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`.

```
#Listen 12.34.56.78:80
Listen 81
```

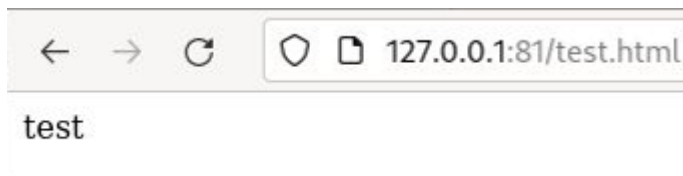
12. Выполним перезапуск веб-сервера Apache. Произошёл сбой? Нет.

13. 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.

```
http_port_t      tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus http_port_t tcp      5988
```

14. Вернули 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 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».



-
15. Исправим обратно конфигурационный файл `apache`, вернув `Listen 80`.

```
#Listen 12.34.56.78:80
Listen 80
```

16. 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.

```
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
```

17. Удалим файл `/var/www/html/test.html`: **`rm /var/www/html/test.html`**.

```
rm: удалить обычный файл '/var/www/html/test.html'? y
```

Вывод

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