

Лабораторная работа №6

Мандатное разграничение прав в Linux

Щепелева М. Е. группа НФИ-01-19

Содержание

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.

Подготовка лабораторного стенда и методические рекомендации

1. Установили веб-сервер Apache.
2. В конфигурационном файле /etc/httpd/httpd.conf задали параметр ServerName.
3. Отключаем пакетный фильтр.

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**. (@fig:004)

```
SELinux root directory: /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
[shepeleva@shepeleva conf]$ ls
httpd.conf magic
[shepeleva@shepeleva conf]$ getenforce
Enforcing
[shepeleva@shepeleva conf]$ getenforce
Enforcing
```

Выполнение команд getenforce и sestatus

2. Запустили веб-сервер и обратились к нему с помощью команды (@fig:005):
service httpd status

```
[shepeleva@shepeleva conf]$ 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 Thu 2022-10-13 18:03:05 MSK; 1h 41min ago
     Docs: man:httpd.service(8)
  Main PID: 4283 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec: 0 B/sec"
    Tasks: 213 (limit: 24681)
   Memory: 26.9M
      CPU: 3.156s
   CGroup: /system.slice/httpd.service
           └─4283 /usr/sbin/httpd -DFOREGROUND
             └─4284 /usr/sbin/httpd -DFOREGROUND
               └─4288 /usr/sbin/httpd -DFOREGROUND
                 └─4289 /usr/sbin/httpd -DFOREGROUND
                   └─4290 /usr/sbin/httpd -DFOREGROUND

Oct 13 18:03:05 shepeleva.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 13 18:03:05 shepeleva.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 13 18:03:05 shepeleva.localdomain httpd[4283]: Server configured, listening on: port 80
```

Выполнение команды service httpd status

3. Нашли веб-сервер Apache в списке процессов. Контекст безопасности - `unconfined_u:unconfined_r:unconfined_t`. (@fig:006)

```
[shepeleva@shepeleva conf]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0      4283 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      4284 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      4288 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      4289 ?        00:00:01 httpd
system_u:system_r:httpd_t:s0      4290 ?        00:00:00 httpd
```

Выполнение команды ps auxZ | grep httpd

4. Посмотрели текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -b | grep httpd`. (@fig:007)

```

httpd_can_network_connect_db off
httpd_can_network_memcache off
httpd_can_network_relay off
httpd_can_sendmail off
httpd_dbus_avahi off
httpd_dbus_sssd off
httpd_dontaudit_search_dirs off
httpd_enable_cgi on
httpd_enable_ftp_server off
httpd_enable_honedirs 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_opq off
httpd_use_nfs off
httpd_use_opencryptoki off
httpd_use_openstack off
httpd_use_sasl off
httpd_verify_dns off

```

Выполнение команды `sestatus -b | grep httpd`

5. Посмотрели статистику по политике с помощью команды **seinfo**. Определили, что множество пользователей = 8; ролей = 14; типов = 5002. (@fig:008)

```

setools-console-4.4.0-4.el9.x86_64      Policy analysis command
Proceed with changes? [N/y] y

* 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:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow
Classes:                 133      Permissions:             454
Sensitivities:           1        Categories:             1024
Types:                   5002     Attributes:              254
Users:                   8        Roles:                   14
Booleans:                347     Cond. Expr.:            381
Allow:                   63996    Neverallow:              0
Auditallow:              168     Dontaudit:              8417
Type_trans:              258486   Type_change:             87
Type_member:              35     Range_trans:            5960
Role_allow:              30      Role_trans:              420
Constraints:              72     Validatetrans:           0
MLS Constrains:          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:                  33
Genfscon:                 106     Portcon:                 651
Netifcon:                 0       Nodecon:                 0

```

Статистика по политике

6. Определили тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды **ls -lZ /var/www**. (@fig:009)

```

[shepeleva@shepeleva conf]$ 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
[shepeleva@shepeleva conf]$

```

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. (@fig:010)

```

[shepeleva@shepeleva conf]$ ls -lZ /var/www/html/
total 0
[shepeleva@shepeleva conf]$

```

Выполнение команды ls -lZ /var/www/html

8. Определим круг пользователей, которым разрешено создание файлов в директории /var/www/html - только uesr. (@fig:011)

```
[shepeleva@shepeleva conf]$ 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
[shepeleva@shepeleva conf]$
```

Выполнение команды `ls -lZ /var/www`

9. Создали от имени суперпользователя html-файл `/var/www/html/test.html` следующего содержания: (@fig:012)

```
/var/www/html/test.html
<html>
<body>test</body>
</html>
```

Содержимое файла `test.html`

10. Проверили контекст созданного файла - `httpd_sys_content_t`. (@fig:013)

```
[shepeleva@shepeleva conf]$ ls -lZ /var/www/html/
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Oct 13 19:49 test.html
```

Контекст файла `test.html`

11. Обратились к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html` и убедились, что файл был успешно отображён. (@fig:014)



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`. (@fig:015)

```
[shepeleva@shepeleva conf]$ ls -lZ /var/www/html/
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Oct 13 19:49 test.html
```

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 -lZ /var/www/html/test.html` И проверили, что контекст поменялся. (@fig:016)

```
[shepeleva@shepeleva conf]$ ls -lZ /var/www/html/
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:samba_share_t:s0 33 Oct 13 19:49 test.html
[shepeleva@shepeleva conf]$
```

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. (@fig:017)

Forbidden

You don't have permission to access this resource.

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 log-файл: `tail /var/log/messages` В системе оказались запущенны процессы **setroubleshootd** и **auditd**. (@fig:018)

```
[shepeleva@shepeleva conf]$ sudo tail /var/log/messages
(sudo) password for shepeleva:
Oct 13 19:56:18 shepeleva setroubleshoot[6016]: failed to retrieve rpm info for /var/www/html/test.html
Oct 13 19:56:18 shepeleva setroubleshoot[6016]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l Bafae8C6-2c7a-482a-b4a
c-3f3c35d59aa
Oct 13 19:56:18 shepeleva setroubleshoot[6016]: 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 ins
ufficient permissions to access a parent directory in which case try to change the following command accordingly.#012Dm012# /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.#012Dm012# semanage
fc context -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 belie
ve 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.#012Dm012# allow this acces
s for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd.#012# semodule -X 300 -i my-httpd.pp#012
Oct 13 19:56:28 shepeleva systemd[1]: dbus-1.10-org.fedoraproject.SetroubleshootPrivilege@00.service: Main process exited, code=killed, status=14/ALRM
Oct 13 19:56:28 shepeleva systemd[1]: dbus-1.10-org.fedoraproject.SetroubleshootPrivilege@00.service: Failed with result 'signal'.
Oct 13 19:56:28 shepeleva systemd[1]: dbus-1.10-org.fedoraproject.SetroubleshootPrivilege@00.service: Consumed 1.056s CPU time.
Oct 13 19:56:28 shepeleva systemd[1]: dbus-1.10-org.fedoraproject.Setroubleshoot@00.service: Main process exited, code=killed, status=14/ALRM
Oct 13 19:56:28 shepeleva systemd[1]: dbus-1.10-org.fedoraproject.Setroubleshoot@00.service: Failed with result 'signal'.
Oct 13 19:57:13 shepeleva systemd[1]: Starting Fingerprint Authentication Daemon...
Oct 13 19:57:13 shepeleva systemd[1]: Started Fingerprint Authentication Daemon.
[shepeleva@shepeleva conf]$
```

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`. (@fig:019)

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

Запуск веб-сервера Apache на прослушивание TCP-порта 81

17. Выполним перезапуск веб-сервера Apache. Произошёл сбой? Нет.
18. Проанализируем log-файлы: `tail -nl /var/log/messages` Просмотрим файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log`. (@fig:020)

```
[shepeleva@shepeleva conf]$ tail /var/log/messages
Oct 13 20:03:09 shepeleva setroubleshoot[6442]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l Bafae8C6-2c7a-482a-b4a
c-3f3c35d59aa
Oct 13 20:03:09 shepeleva setroubleshoot[6442]: 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 ins
ufficient permissions to access a parent directory in which case try to change the following command accordingly.#012Dm012# /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.#012Dm012# semanage
fc context -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 belie
ve 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.#012Dm012# allow this acces
s for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd.#012# semodule -X 300 -i my-httpd.pp#012
Oct 13 20:03:10 shepeleva setroubleshoot[6442]: failed to retrieve rpm info for /var/www/html/test.html
Oct 13 20:03:10 shepeleva setroubleshoot[6442]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l Bafae8C6-2c7a-482a-b4a
c-3f3c35d59aa
Oct 13 20:03:10 shepeleva setroubleshoot[6442]: 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 ins
ufficient permissions to access a parent directory in which case try to change the following command accordingly.#012Dm012# /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.#012Dm012# semanage
fc context -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 belie
ve 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.#012Dm012# allow this acces
s for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd.#012# semodule -X 300 -i my-httpd.pp#012
Oct 13 20:03:20 shepeleva systemd[1]: dbus-1.10-org.fedoraproject.SetroubleshootPrivilege@01.service: Main process exited, code=killed, status=14/ALRM
Oct 13 20:03:20 shepeleva systemd[1]: dbus-1.10-org.fedoraproject.SetroubleshootPrivilege@01.service: Failed with result 'signal'.
Oct 13 20:03:20 shepeleva systemd[1]: dbus-1.10-org.fedoraproject.SetroubleshootPrivilege@01.service: Consumed 1.028s CPU time.
Oct 13 20:03:20 shepeleva systemd[1]: dbus-1.10-org.fedoraproject.Setroubleshoot@01.service: Main process exited, code=killed, status=14/ALRM
Oct 13 20:03:20 shepeleva systemd[1]: dbus-1.10-org.fedoraproject.Setroubleshoot@01.service: Failed with result 'signal'.
[shepeleva@shepeleva conf]$ less /var/log/http/error_log
```

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. (@fig:021)

```
[shepeleva@shepeleva conf]$ sudo semanage port -l | grep 81
httpd_port_t      tcp      1782, 2207, 2208, 8290, 8292, 9100, 9101, 9102, 9220, 9221, 9222, 9280, 9281, 9282, 9290, 9291, 50000, 50002
http_cache_port_t tcp      8080, 8118, 8123, 10001-10010
http_port_t       tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
intermapper_port_t tcp      8181
prosody_port_t    tcp      5280-5281
pulp_port_t       tcp      24816, 24817
puppet_port_t     tcp      8140
radacct_port_t    tcp      1646, 1813
radacct_port_t    udp      1646, 1813
radius_port_t     tcp      1645, 1812, 18120-18121
radius_port_t     udp      1645, 1812, 18120-18121
rkt_port_t        tcp      18112
statsd_port_t     udp      8125
transproxy_port_t tcp      8081
varnishd_port_t   tcp      6081-6082
zookeeper_client_port_t tcp      2181
```

Проверка установления 81 порта tcp

20. Попробуем запустить веб-сервер Apache ещё раз. (@fig:022)

```
[shepeleva@shepeleva conf]$ sudo systemctl restart httpd
[shepeleva@shepeleva conf]$
```

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** (@fig:023)

```
[shepeleva@shepeleva conf]$ sudo chcon -t httpd_sys_content_t /var/www/html/test.html
[shepeleva@shepeleva conf]$
```

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». (@fig:024)



Обращение к файлу test.html через веб-сервер

22. Исправим обратно конфигурационный файл apache, вернув Listen 80. (@fig:025)

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

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. (@fig:026)

```
[shepeleva@shepeleva conf]$ 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**. (@fig:027)

```
[shepeleva@shepeleva conf]$ sudo rm /var/www/html/test.html
[shepeleva@shepeleva conf]$ ls /var/www/html/
[shepeleva@shepeleva conf]$ ls
httpd.conf  magic
```

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 SELinux 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/sozдание-saytov/osnovnye-komandy-linux>)