

Лабораторная работа № 6. Мандатное разграничение прав в Linux

Ильин Никита Евгеньевич, НФИбд-01-19

Содержание

1	Цель работы	5
2	Последовательность выполнения работы	6
3	Выводы	16
4	Библиография	17

List of Figures

2.1	проверка	6
2.2	проверка	7
2.3	процессы	7
2.4	процессы	9
2.5	процессы	10
2.6	процессы	11
2.7	процессы	11
2.8	процессы	11
2.9	процессы	12
2.10	процессы	13
2.11	процессы	13
2.12	процессы	14
2.13	процессы	15
2.14	процессы	15

List of Tables

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 Последовательность 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`.

```
[root@Rocky nktllyn]# getenforce
Enforcing
[root@Rocky nktllyn]# 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
```

Figure 2.1: проверка

2. 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.

```
[nkt1lyn@Rocky ~]$ 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 pr>
   Active: inactive (dead)
   Docs: man:httpd.service(8)
```

Figure 2.2: проверка

3. 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
```

```
Redirecting to /bin/systemctl start httpd.service
[nkt1lyn@Rocky ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0  root          3111  0.1  0.3  29184 10032 ?
Ss   17:50   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache      3115  0.0  0.3  30680  8440 ?
S    17:50   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache      3116  0.0  0.4 1551132 11768 ?
Sl   17:50   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache      3117  0.0  0.6 1683228 15856 ?
Sl   17:50   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache      3118  0.0  0.4 1551132 11768 ?
Sl   17:50   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 nkt1lyn 3358 0.0  0.0 2213
96 1944 pts/1 R+ 17:51   0:00 grep --color=auto httpd
```

Figure 2.3: процессы

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

```
sestatus -bigrep httpd
```

Обратите внимание, что многие из них находятся в положении «off».


```

[nkt1lyn@Rocky ~]$ sestatus -b 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.
[nkt1lyn@Rocky ~]$ 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
cdrecord_read_content            off
cluster_can_network_connect     off
cluster_manage_all_files        off
cluster_use_execmem             off
cobbler_anon_write              off
cobbler_can_network_connect     off
cobbler_use_cifs                 off
cobbler_use_nfs                  off
collectd_tcp_network_connect    off
colord_use_nfs                   off
condor_tcp_network_connect      off
conman_can_network              off
conman_use_nfs                   off
container_connect_any           off
container_manage_cgroup         off
container_use_cephfs            off

```

Figure 2.4: процессы

5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов.

```
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:   38        Role_trans:      420
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:          33
Genfscon:     106      Portcon:         651
Netifcon:     0        Nodecon:         0
```

Figure 2.5: процессы

6. Определите тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды

```
ls -lZ /var/www
```

```
[nktilyn@Rocky ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 13 15
:56 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 мая 13 15
:56 html
[nktilyn@Rocky ~]$
```

Figure 2.6: процессы

7. Определите тип файлов, находящихся в директории /var/www/html:

```
ls -lZ /var/www/html
```

```
[nktilyn@Rocky ~]$ ls -lZ /var/www/html
итого 0
```

Figure 2.7: процессы

8. Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html.
9. 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:

```
<html>
<body>test</body>
</html>
```

```
[nktilyn@Rocky ~]$ sudo nano /var/www/html/test.html
[nktilyn@Rocky ~]$ ls -lZ /var/www/html
102138924 unconfined_u:object_r:httpd_sys_content_t:s0 test.html
[nktilyn@Rocky ~]$
```

Figure 2.8: процессы

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

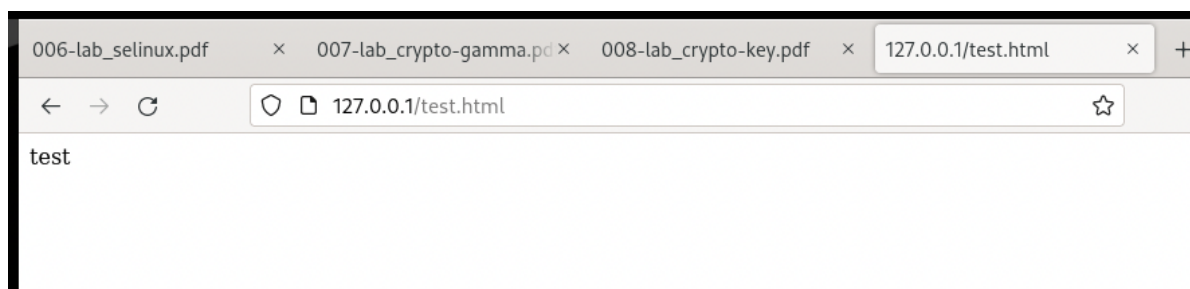


Figure 2.9: процессы

12. 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`. Рассмотрим полученный контекст детально. Обратите внимание, что так как по умолчанию пользователи CentOS являются свободными от типа (`unconfined` в переводе с англ. означает свободный), созданному нами файлу `test.html` был сопоставлен SELinux, пользователь `unconfined_u`. Это первая часть контекста.

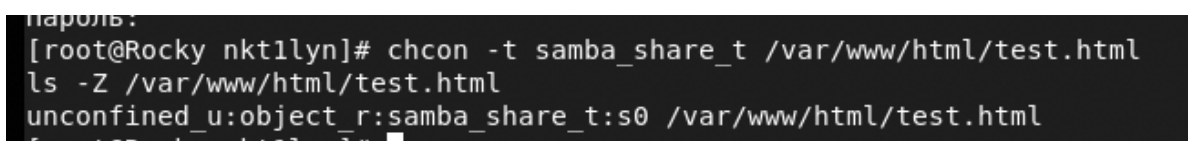
Далее политика ролевого разделения доступа RBAC используется процессами, но не файлами, поэтому роли не имеют никакого значения для файлов. Роль `object_r` используется по умолчанию для файлов на «постоянных» носителях и на сетевых файловых системах. (В директории `/proc` файлы, относящиеся к процессам, могут иметь роль `system_r`. Если активна политика MLS, то могут использоваться и другие роли, например, `secadm_r`. Данный случай мы рассматривать не будем, как и предназначение `:s0`).

Тип `httpd_sys_content_t` позволяет процессу `httpd` получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер.

13. 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.



```
пароль:
[root@Rocky nkt1lyn]# chcon -t samba_share_t /var/www/html/test.html
ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@Rocky nkt1lyn]#
```

Figure 2.10: процессы

14. 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.

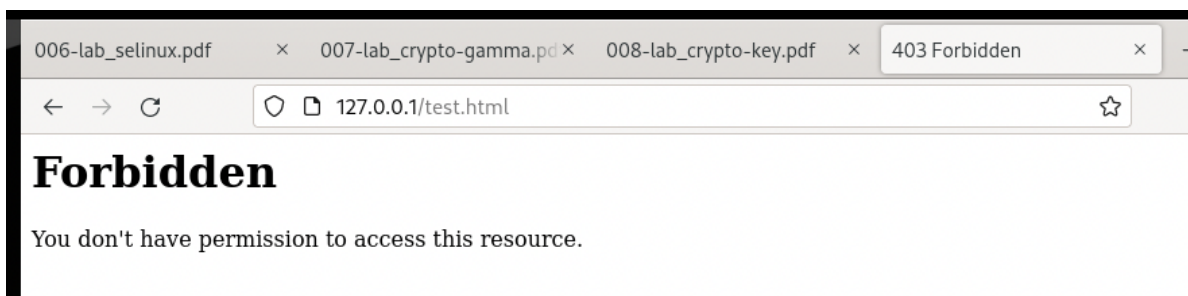


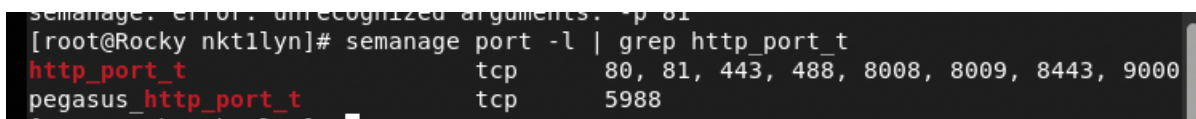
Figure 2.11: процессы

15. 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 `audtd`, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле `/var/log/audit/audit.log`. Проверьте это утверждение самостоятельно.

16. 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`.



```
semanage: error: unrecognized arguments: -p 81
[root@Rocky nktilyn]# 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
```

Figure 2.12: процессы

17. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему?
18. 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.
19. Выполните команду `semanage port -a -t http_port_t -p tcp 81` После этого проверьте список портов командой `semanage port -l | grep http_port_t` Убедитесь, что порт 81 появился в списке.
20. Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему он сейчас запустился, а в предыдущем случае не смог?

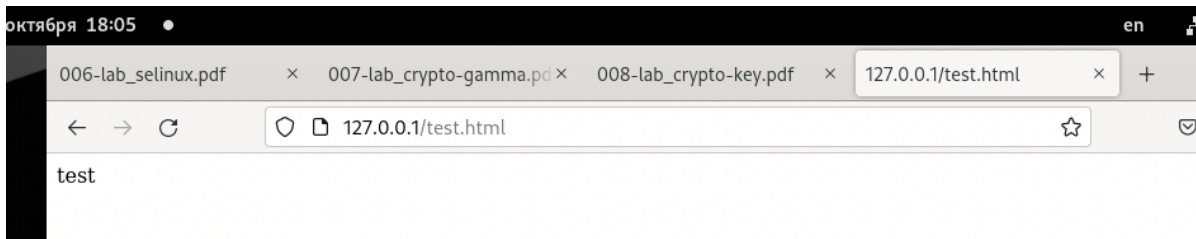


Figure 2.13: процессы

21. 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».

22. Исправьте обратно конфигурационный файл `apache`, вернув `Listen 80`.
23. Удалите привязку `http_port_t` к 81 порту: `semanage port -d -t http_port_t -p tcp 81` и проверьте, что порт 81 удалён.
24. Удалите файл `/var/www/html/test.html`:

```
rm /var/www/html/test.html
```

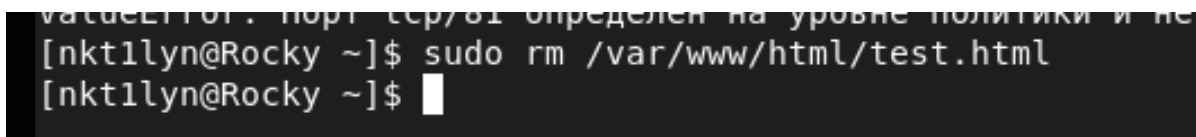


Figure 2.14: процессы

3 Выводы

Развиты навыки администрирования ОС Linux. Получено первое практическое знакомство с технологией SELinux. Проверена работу SELinx на практике совместно с веб-сервером Apache.

4 Библиография

1. Методические материалы курса