

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

Презентация

ПО ЛАБОРАТОРНОЙ РАБОТЕ № 6

дисциплина: Информационная безопасность

Студент: Пиняева Анна Андреевна

Группа: НФИбд-02-20

МОСКВА

2023

Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux¹. Проверить работу SELinux на практике совместно с веб-сервером Apache.

Ход работы

- Вошли в систему с полученными учётными данными и убедились, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus. (рис. 1).

Рис. 1 Конфигурации SELinux:

```
[user@user ~]$ getenforce  
Enforcing  
[user@user ~]$ 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. Обратились с помощью браузера к веб-серверу, запущенному на компьютере, и убедились, что последний работает (рис. 2).

Рис. 2 Обращение к веб-серверу:

```
[user@user ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[user@user ~]$ 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: d>
  Active: active (running) since Sat 2023-10-14 13:01:59 MSK; 7s ago
    Docs: man:httpd.service(8)
   Main PID: 6578 (httpd)
     Status: "Started, listening on: port 80"
      Tasks: 213 (limit: 10917)
     Memory: 23.4M
        CPU: 99ms
      CGroup: /system.slice/httpd.service
              └─6578 /usr/sbin/httpd -DFOREGROUND
                  ├─6585 /usr/sbin/httpd -DFOREGROUND
                  ├─6591 /usr/sbin/httpd -DFOREGROUND
                  ├─6592 /usr/sbin/httpd -DFOREGROUND
                  └─6593 /usr/sbin/httpd -DFOREGROUND

Oct 14 13:01:59 user.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 14 13:01:59 user.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 14 13:01:59 user.localdomain httpd[6578]: Server configured, listening on: >
lines 1-19/19 (END)
```

3. Нашли веб-сервер Apache в списке процессов, определили его контекст безопасности (рис. 3).

Рис. 3 Контекст безопасности:

```
[user@user ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0      root      6578  0.0  0.6  20328 11592 ?        Ss
13:01  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache    6585  0.0  0.4  21664  7468 ?        S
13:01  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache    6591  0.0  0.7 1210612 13148 ?        Sl
13:01  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache    6592  0.0  0.6 1079476 11100 ?        Sl
13:01  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache    6593  0.0  0.6 1079476 11100 ?        Sl
13:01  0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 user  6850 0.0  0.1 221664 2236 p
ts/0 S+ 13:04  0:00 grep --color=auto httpd
[user@user ~]$
```

N/Solid

4. Посмотрели текущее состояние переключателей SELinux для Apache (рис. 4).

Рис. 4 Состояние переключателей SELinux:

```
[user@user ~]$ 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_avahi           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_ina            off
```

5. Посмотрели статистику по политике (рис. 5).

Рис. 5 Статистика по политике:

```
[user@user ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes: allow
Classes:                 135   Permissions:      457
Sensitivities:          1      Categories:     1024
Types:                   5100   Attributes:       258
Users:                   8      Roles:            14
Booleans:                353   Cond. Expr.:    384
Allow:                  65008  Neverallow:      0
Auditallow:              170   Dontaudit:      8572
Type_trans:              265344 Type_change:     87
Type_member:              35   Range_trans:    6164
Role allow:               38   Role_trans:     420
Constraints:             70   Validatetrans:  0
MLS Constrain:           72   MLS Val. Tran:  0
Permissives:              2   Polcap:          6
Defaults:                 7   Typebounds:     0
Allowxperm:                0   Neverallowxperm: 0
Auditallowxperm:           0   Dontauditxperm: 0
Ibendportcon:              0   Ibpkeycon:      0
Initial SIDs:              27   Fs_use:         35
Genfscon:                  109  Portcon:        660
Netifcon:                   0   Nodecon:        0
```

N/Solid

6. Определили тип файлов и поддиректорий, находящихся в директории /var/www (рис. 6).

Рис. 6 Директория /var/www:

```
[user@user ~]$ 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 23:21 cg
i-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 May 16 23:21 ht
ml
```

N|Solid

7. Определили тип файлов, находящихся в директории /var/www/html (рис. 7).

Рис. 7 Директория /var/www/html:

```
[user@user ~]$ ls -lZ /var/www/html
total 0
```

N|Solid

8. Создали от имени суперпользователя html-файл /var/www/html/test.html (рис. 8).

Рис. 8 Файл /var/www/html/test.html:



The screenshot shows a text editor window titled '*test.html [Read-Only]' located at '/var/www/html'. The window has 'Open' and 'Save' buttons. The text area contains three lines of HTML code:

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

N/Solid

9. Проверили контекст созданного файла (рис. 9).

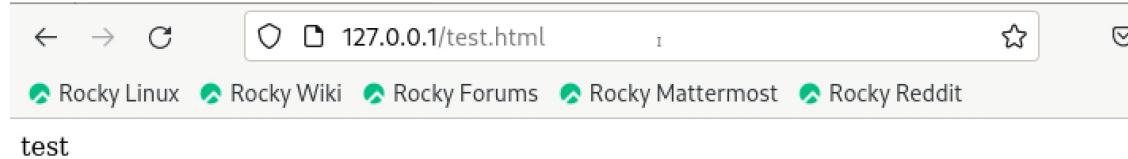
Рис. 9 Контекст файла:

```
[root@user user]# ls -LZ /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@user user]#
```

N/Solid

10. Обратились к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html> (рис. 10).

Rис. 10 Запуск в браузере:



N|Solid

11. Изучили справку man httpd_selinux (рис. 11).

Rис. 11 Справка man httpd_selinux:

```
12 root@user:/home/user
→ selinux(8)          SELinux Command Line documentation      selinux(8)

NAME
selinux - NSA Security-Enhanced Linux (SELinux)

DESCRIPTION
NSA Security-Enhanced Linux (SELinux) is an implementation of a flexible
mandatory access control architecture in the Linux operating system. The
SELinux architecture provides general support for the enforcement of many
kinds of mandatory access control policies, including those based on the
concepts of Type Enforcement®, Role-Based Access Control, and Multi-Level
Security. Background information and technical documentation about SELinux
can be found at https://github.com/SELinuxProject.

The /etc/selinux/config configuration file controls whether SELinux is en-
abled or disabled, and if enabled, whether SELinux operates in permissive
mode or enforcing mode. The SELINUX variable may be set to any one of dis-
abled, permissive, or enforcing to select one of these options. The dis-
abled disables most of the SELinux kernel and application code, leaving the
system running without any SELinux protection. The permissive option en-
ables the SELinux code, but causes it to operate in a mode where accesses
that would be denied by policy are permitted but audited. The enforcing op-
tion enables the SELinux code and causes it to enforce access denials as
well as auditing them. permissive mode may yield a different set of denials
than enforcing mode, both because enforcing mode will prevent an operation
Manual page selinux(8) line 1 (press h for help or q to quit)
```

N/Solid

12. Измените контекст файла /var/www/html/test.html с httpd_sys_content_t на другой (рис. 12).

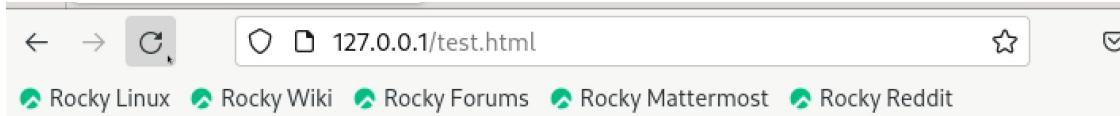
Рис. 12 Изменение контекста:

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

N/Solid

13. Попробовали ещё раз получить доступ к файлу через веб-сервер (рис. 13).

Рис. 13 Запуск в браузере:



Forbidden

You don't have permission to access this resource.

N/Solid

14. Просмотрели log-файлы веб-сервера Apache и системный лог-файл (рис. 14).

Рис. 14 Лог-файлы:

```
[root@user user]# ls -l /var/www/html/test.html
-rwxrwxrwx. 1 root root 33 Oct 14 13:18 /var/www/html/test.html
[root@user user]# tail /var/log/messages
Oct 14 13:25:31 user setroubleshoot[7927]: failed to retrieve rpm info for path '/var/www/html/test.html':
Oct 14 13:25:31 user systemd[1]: Created slice Slice /system/dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged.
Oct 14 13:25:31 user systemd[1]: Started dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service.
Oct 14 13:25:33 user setroubleshoot[7927]: SELinux is preventing /usr/sbin/httpd from
getattr access on the file /var/www/html/test.html. For complete SELinux messages run:
sealert -l e4e26d4c-1773-4bb2-bc3a-03c06clf37df
Oct 14 13:25:33 user setroubleshoot[7927]: SELinux is preventing /usr/sbin/httpd from
getattr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (9
2.2 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 yo
u can run restorecon. The access attempt may have been stopped due to insufficient per
missions to access a parent directory in which case try to change the following comman
d accordingly.#012Do#012# /sbin/restorecon -v '/var/www/html/test.html'#012#012***** Pl
ugin public_content (7.83 confidence) suggests *****#012#012If you wa
nt to treat test.html as public content#012Then you need to change the label on test.h
tml to public_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t pub
lic_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#0
12#012***** Plugin catchall (1.41 confidence) suggests *****#0
12#012If you believe that httpd should be allowed getattr access on the test.html file
```

N/Solid

15. Попробовали запустить веб-сервер Apache на прослушивание TCP-порта 81. Для этого в файле /etc/httpd/httpd.conf нашли строчку Listen 80 и заменили её на Listen 81.

16. Выполнили перезапуск веб-сервера Apache (рис. 15).

Рис. 15 Перезапуск сервера:

```
[root@user user]# service httpd stop
Redirecting to /bin/systemctl stop httpd.service
[root@user user]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@user user]# 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 2023-10-14 13:31:11 MSK; 29s ago
     Docs: man:httpd.service(8)
 Main PID: 8070 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served: 0; Tasks: 213 (limit: 10917)
   Memory: 23.2M
      CPU: 134ms
    CGroup: /system.slice/httpd.service
            ├─8070 /usr/sbin/httpd -DFOREGROUND
            ├─8071 /usr/sbin/httpd -DFOREGROUND
            ├─8072 /usr/sbin/httpd -DFOREGROUND
            ├─8073 /usr/sbin/httpd -DFOREGROUND
            └─8074 /usr/sbin/httpd -DFOREGROUND

Oct 14 13:31:10 user.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 14 13:31:11 user.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 14 13:31:11 user.localdomain httpd[8070]: Server configured, listening on: port 81
1 lines 1-19/19 (FWD) ]
```

N/Solid

17. Проанализировали лог-файлы (рис. 16).

Рис. 16 Лог-файлы:

```
[root@user user]# tail /var/log/messages
Oct 14 13:29:32 user systemd[1]: dnf-makecache.service: Deactivated successfully.
Oct 14 13:29:32 user systemd[1]: Finished dnf makecache.
Oct 14 13:29:34 user journal[7250]: Running on LOW Battery, pausing
Oct 14 13:31:03 user systemd[1]: Stopping The Apache HTTP Server...
Oct 14 13:31:04 user systemd[1]: httpd.service: Deactivated successfully.
Oct 14 13:31:04 user systemd[1]: Stopped The Apache HTTP Server.
Oct 14 13:31:04 user systemd[1]: httpd.service: Consumed 2.058s CPU time.
Oct 14 13:31:10 user systemd[1]: Starting The Apache HTTP Server...
Oct 14 13:31:11 user systemd[1]: Started The Apache HTTP Server.
Oct 14 13:31:11 user httpd[8070]: Server configured, listening on: port 81
[root@user user]#
```

N/Solid

18. Выполнили команду `semanage port -a -t http_port_t -p tcp 81`. После этого проверили список портов командой `semanage port -l | grep http_port_t` (рис. 17).

Рис. 17 Команды:

```
[root@user user]# semanage port -a -t httpd_port_t tcp 81
usage: semanage [-h]
                 {import,export,login,user,port,ibpkey,ibendport,interface,module,node,
fcontext,boolean,permissive,dontaudit}
...
semanage: error: unrecognized arguments: 81
[root@user user]# 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
[root@user user]#
```

N/Solid

19. Запустили веб-сервер Apache ещё раз (рис. 18).

Рис. 18 Запуск веб-сервера:

```
[root@user user]# service httpd stop
Redirecting to /bin/systemctl stop httpd.service
[root@user user]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@user user]# 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 2023-10-14 13:31:11 MSK; 29s ago
     Docs: man:httpd.service(8)
     Main PID: 8070 (httpd)
        Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served: 0"
           Tasks: 213 (limit: 10917)
      Memory: 23.2M
         CPU: 134ms
      CGroup: /system.slice/httpd.service
              ├─8070 /usr/sbin/httpd -DFOREGROUND
              ├─8071 /usr/sbin/httpd -DFOREGROUND
              ├─8072 /usr/sbin/httpd -DFOREGROUND
              ├─8073 /usr/sbin/httpd -DFOREGROUND
              ├─8074 /usr/sbin/httpd -DFOREGROUND

Oct 14 13:31:10 user.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 14 13:31:11 user.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 14 13:31:11 user.localdomain httpd[8070]: Server configured, listening on: port 81
Lines 1-19/19 (Fwd)
```

N/Solid

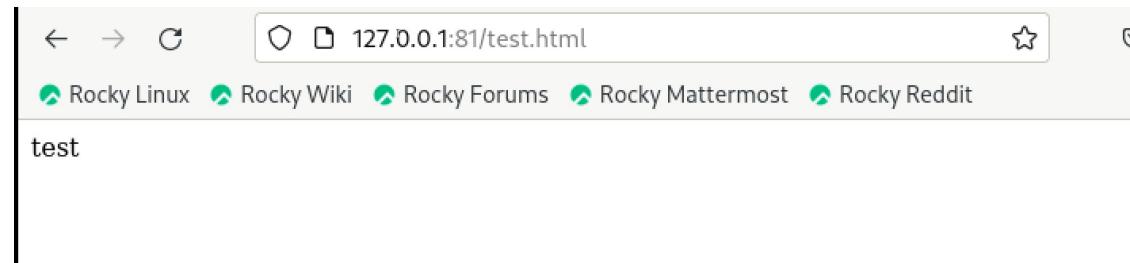
20. Вернули контекст httpd_sys_content_t к файлу /var/www/html/test.html (рис. 19). После этого попробовали получить доступ к файлу через веб-сервер (рис. 20)

Рис. 19 Возвращение контекста:

```
[root@user user]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@user user]# semanage port -d -t httpd_port_t tcp 81
usage: semanage [-h]
                 {import,export,login,user,port,ibpkey,ibendport,interface,module,node,
fcontext,boolean,permissive,dontaudit}
...
semanage: error: unrecognized arguments: 81
[root@user user]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@user user]#
```

N|Solid

Рис. 20 Запуск в браузере:



N|Solid

21. Исправили обратно конфигурационный файл apache, вернув Listen80, удалили привязку http_port_t к 81 порту, удалили файл (рис. 21).

Rис. 21 Команды:

```
[root@user user]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@user user]# semanage port -d -t httpd_port_t tcp 81
usage: semanage [-h]
                 {import,export,login,user,port,ibpkey,ibendport,interface,module,node,
fcontext,boolean,permissive,dontaudit}
...
semanage: error: unrecognized arguments: 81
[root@user user]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@user user]#
```

N/Solid

Выводы