

Лабораторная работа № 6

Мандатное разграничение прав в Linux

Юрченко Артём Алексеевич

Содержание

0.1	Цели	3
0.2	Задачи	4
0.3	Ход работы	4
0.4	Ход работы	4
0.5	Ход работы	5
0.6	Ход работы	5
0.7	Ход работы	6
0.8	Ход работы	6
0.9	Ход работы	7
0.10	Ход работы	7
0.11	Ход работы	7
0.12	Ход работы	8
0.13	Ход работы	8
0.14	Ход работы	9
0.15	Ход работы	9
0.16	Ход работы	10
0.17	Ход работы	10
0.18	Ход работы	10
0.19	Ход работы	11
0.20	Ход работы	11
0.21	Ход работы	12
0.22	Ход работы	12
0.23	Ход работы	13
0.24	Ход работы	13
0.25	Ход работы	13
0.26	Ход работы	14
0.27	Результаты	14

Список иллюстраций

0.1	Конфигурация SELinux	4
0.2	Обращение к веб-серверу	5
0.3	Контекст безопасности веб-сервера Apache	5
0.4	Текущее состояние переключателей SELinux для Apache	6
0.5	Статистика по политике	6
0.6	Тип файлов и поддиректорий, находящихся в директории /var/www	7
0.7	Тип файлов, находящихся в директории /var/www/html	7
0.8	Круг пользователей, которым разрешено создание файлов в дирек-	
	тории /var/www/html	7
0.9	Создание файла /var/www/html/test.html	8
0.10	Работа с параметрами readfile	8
0.11	Файл test.html в браузере	9
0.12	Вызов справки и тип файла test.html	9
0.13	Изменение контекста	9
0.14	Файл test.html в браузере после изменения контекста	10
0.15	Содержимое логов	10
0.16	Изменение содержимого файла /etc/httpd/httpd.conf	11
0.17	Перезапуск веб-сервера	11
0.18	Лог-файл tail -nl /var/log/messages	11
0.19	Попытка добавления порта 81 в список и вывод списка допустимых	
	портов	12
0.20	Повторный запуск веб-сервера	12
0.21	Файл test.html в браузере после возвращения контекста	13
0.22	Параметр Listen после возвращения значения	13
0.23	Попытка удаления привязки к порту 81	13
0.24	Удаление файла /var/www/html/test.html	14

0.1 Цели

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

0.2 Задачи

1. Настроить и запустить сервер Apache.
2. Исследовать влияние параметров сервера на его работу.

0.3 Ход работы

Войдем в систему с полученными учётными данными и убедимся, что SELinux работает в режиме enforcing политики targeted.

```
[root@info-sec temau]# getenforce
Enforcing
[root@info-sec temau]# 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
[root@info-sec temau]#
```

Рис. 0.1: Конфигурация SELinux

0.4 Ход работы

Обратимся с помощью браузера к веб-серверу, запущенному на нашем компьютере, и убедимся, что последний работает.

```

[temau@info-sec ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[temau@info-sec ~]$ 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 14:53:17 MSK; 7s ago
     Docs: man:httpd.service(8)
  Main PID: 42011 (httpd)
    Status: "Started, listening on: port 80"
   Tasks: 213 (limit: 44971)
  Memory: 35.5M
    CPU: 38ms
   CGroup: /system.slice/httpd.service
           └─42011 /usr/sbin/httpd -DFOREGROUND
             42018 /usr/sbin/httpd -DFOREGROUND
             42019 /usr/sbin/httpd -DFOREGROUND
             42020 /usr/sbin/httpd -DFOREGROUND
             42021 /usr/sbin/httpd -DFOREGROUND

окт 14 14:53:17 info-sec systemd[1]: Starting The Apache HTTP Server...
окт 14 14:53:17 info-sec httpd[42011]: Server configured, listening on: port 80
окт 14 14:53:17 info-sec systemd[1]: Started The Apache HTTP Server.
lines 1-19/19 (END)

```

Рис. 0.2: Обращение к веб-серверу

0.5 Ход работы

Найдем веб-сервер Apache в списке процессов, определим его контекст безопасности.

```

[temau@info-sec ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 42011 0.0 0.1 20116 11376 ?
Ss 14:53 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42018 0.0 0.1 21600 7272 ?
S 14:53 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42019 0.0 0.2 2324556 15020 ?
Sl 14:53 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42020 0.0 0.2 2521228 17072 ?
Sl 14:53 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42021 0.0 0.2 2324556 15020 ?
Sl 14:53 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 temau 42510 0.0 0.0 22182
2336 pts/0 S+ 14:54 0:00 grep --color=auto httpd
[temau@info-sec ~]$

```

Рис. 0.3: Контекст безопасности веб-сервера Apache

0.6 Ход работы

Посмотрим текущее состояние переключателей SELinux для Apache.

```

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_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_setlimit                          off
httpd_ssl_exec                          off
httpd_sys_script_anon_write             off
httpd_ttp_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_opensslcryptoki               off
httpd_use_openssl                       off
httpd_use_sasl                           off
httpd_verify_dns                        off
[teama@info-sec ~]$

```

Рис. 0.4: Текущее состояние переключателей SELinux для Apache

0.7 Ход работы

Посмотрим статистику по политике с помощью команды `seinfo`.

```
[tmeaux@info-sec ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version: 33 (MLS enabled)
Target Policy: selinux

Handle unknown classes: allow

Classes: 135
Sensitivities: 1 Categories: 457
Types: 5190 Attributes: 258
Users: 8 Roles: 14
Booleans: 353 Cond. Expr.: 384
Allow: 6508 Neverallow: 70
Audit allow: 170 Dontaudit: 832
Type_trans: 265344 Type_Erange: 87
Type_member: 35 Range_trans: 6164
Role allow: 38 Role_trans: 420
Constraints: 70 Validatetrans: 0
MLS Constrains: 72 MLS Val. Tran: 0
Permissive: 2 Polcap: 0
Defaults: 7 Typebounds: 0
Allowxperm: 0 Neverallowxperm: 0
Auditallowxperm: 0 Dontauditxperm: 0
Ibendpoint: 0 Ipkeycon: 0
Initial SDOs: 27 F_keycon: 35
Genfscon: 199 Portcon: 668
Netifcon: 0 Nodetcon: 0

[tmeaux@info-sec ~]$
```

Рис. 0.5: Статистика по политике

0.8 Ход работы

Определим тип файлов и поддиректорий, находящихся в директории /var/www.

```
[temau@info-sec ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая
16 23:21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 мая
16 23:21 html
```

Рис. 0.6: Тип файлов и поддиректорий, находящихся в директории /var/www

0.9 Ход работы

Определим тип файлов, находящихся в директории /var/www/html.

```
[temau@info-sec ~]$ ls -lZ /var/www/html
итого 0
[temau@info-sec ~]$
```

Рис. 0.7: Тип файлов, находящихся в директории /var/www/html

0.10 Ход работы

Определим круг пользователей, которым разрешено создание файлов в директории /var/www/html.

```
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 16 23:21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 мая 16 23:21 html
```

Рис. 0.8: Круг пользователей, которым разрешено создание файлов в директории /var/www/html

0.11 Ход работы

Создадим от имени суперпользователя html-файл /var/www/html/test.html.

```
[root@info-sec temaui]# touch /var/www/html/test.html
[root@info-sec temaui]#
```

Рис. 0.9: Создание файла /var/www/html/test.html

Заполним его следующим содержимым:

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

0.12 Ход работы

Проверим контекст созданного нами файла.

```
[root@info-sec temaui]# ls -lZ /var/www/html
итого 0
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 0 окт 14 14:56 test.html
[root@info-sec temaui]#
```

Рис. 0.10: Работа с параметрами readfile

Как видим по умолчанию присваивается контекст `unconfined_u:object_r:httpd_sys_content_t:s0`

0.13 Ход работы

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

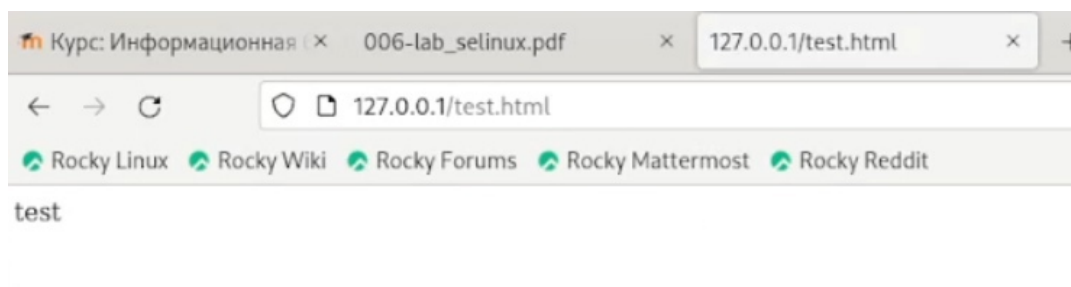


Рис. 0.11: Файл test.html в браузере

0.14 Ход работы

Изучим справку `man httpd_selinux` и выясним, какие контексты файлов определены для `httpd`. Сопоставим их с типом файла `test.html`.

```
[root@info-sec html]# ls -Z
unconfined_u:object_r:httpd_sys_content_t:s0 test.html
[root@info-sec html]#
```

Рис. 0.12: Вызов справки и тип файла test.html

0.15 Ход работы

Изменим контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t`.

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

Рис. 0.13: Изменение контекста

0.16 Ход работы

Попробуем ещё раз получить доступ к файлу через веб-сервер.

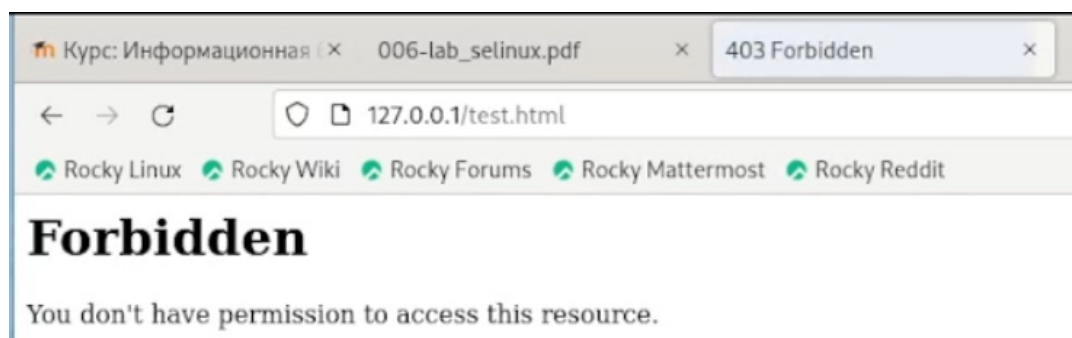


Рис. 0.14: Файл test.html в браузере после изменения контекста

0.17 Ход работы

Посмотрим log-файлы веб-сервера Apache и системный лог-файл.

```
[root@info-sec html]# ls -l
итого 4
-rw-r--r--. 1 root root 33 окт 14 14:59 test.html
[root@info-sec html]# tail /var/log/messages
```

Рис. 0.15: Содержимое логов

Как видим, нам не удалось получить доступ к файлу как раз из-за измененного контекста.

0.18 Ход работы

Попробуем запустить веб-сервер Apache на прослушивание TCP-порта 81.

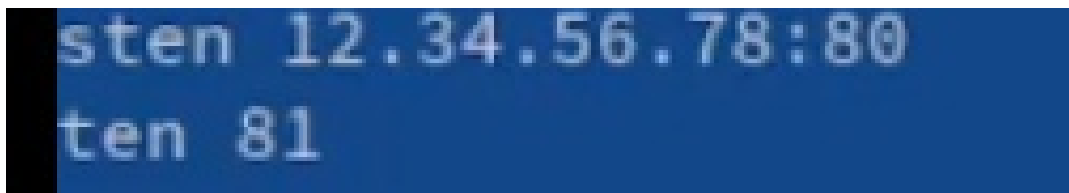


Рис. 0.16: Изменение содержимого файла /etc/httpd/httpd.conf

0.19 Ход работы

Выполним перезапуск веб-сервера. Сбоя не произошло.

```
[root@info-sec 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; preset: disabled)
   Active: active (running) since Sat 2023-10-14 15:05:22 MSK; 2min 15s ago
     Docs: man:httpd.service(8)
   Main PID: 43696 (httpd)
   Status: "Total requests: 3; Idle/Busy workers 100/0; Requests/sec: 0.0233; Bytes served/s: 0"
   Tasks: 213 (limit: 44971)
  Memory: 35.4M
    CPU: 92ms
   CGroup: /system.slice/httpd.service
           └─43696 /usr/sbin/httpd -DFOREGROUND
             └─43697 /usr/sbin/httpd -DFOREGROUND
               └─43698 /usr/sbin/httpd -DFOREGROUND
                 └─43699 /usr/sbin/httpd -DFOREGROUND
                   └─43701 /usr/sbin/httpd -DFOREGROUND

окт 14 15:05:22 info-sec systemd[1]: Starting The Apache HTTP Server...
окт 14 15:05:22 info-sec systemd[1]: Started The Apache HTTP Server.
окт 14 15:05:22 info-sec httpd[43696]: Server configured, listening on: port 81
```

Рис. 0.17: Перезапуск веб-сервера

0.20 Ход работы

Проанализируем лог-файлы.

```
[root@user conf]# tail -nl /var/log/messages
Oct 12 14:43:54 user systemd[1]: Started Fingerprint Authentication Daemon.
Oct 12 14:43:58 user NetworkManager[927]: <info> [1697111038.6420] agent-manager: agent[ef6fe3c18efc9fb5,;1.71/org.gnome.Shell.NetworkAgent/1000]: agent registered
Oct 12 14:44:24 user systemd[1]: fprintd.service: Deactivated successfully.
Oct 12 14:44:52 user systemd[1]: Stopping The Apache HTTP Server...
Oct 12 14:44:53 user systemd[1]: httpd.service: Deactivated successfully.
Oct 12 14:44:53 user systemd[1]: Stopped The Apache HTTP Server.
Oct 12 14:44:53 user systemd[1]: httpd.service: Consumed 12.225s CPU time.
Oct 12 14:44:58 user systemd[1]: Starting The Apache HTTP Server...
Oct 12 14:44:58 user systemd[1]: Started The Apache HTTP Server.
Oct 12 14:44:58 user httpd[42774]: Server configured, listening on: port 81
```

Рис. 0.18: Лог-файл tail -nl /var/log/messages

0.21 Ход работы

Выполним команду `semanage port -a -t http_port_t -p tcp 81`. После этого проверим список портов командой `semanage port -l | grep http_port_t`. Убедимся, что порт 81 есть в списке.

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

Рис. 0.19: Попытка добавления порта 81 в список и вывод списка допустимых портов

0.22 Ход работы

Попробуем запустить веб-сервер Apache ещё раз.

```
[root@info-sec conf]# 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@info-sec 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; preset: disabled)
   Active: active (running) since Sat 2023-10-14 15:05:22 MSK; 2min 15s ago
     Docs: man:httpd.service(8)
  Main PID: 43696 (httpd)
    Status: "Total requests: 3; Idle/Busy workers 100/0; Requests/sec: 0.0233; Bytes served/s"
    Tasks: 213 (limit: 44971)
   Memory: 35.4M
      CPU: 92ms
    CGroup: /system.slice/httpd.service
            └─43696 /usr/sbin/httpd -DFOREGROUND
              └─43697 /usr/sbin/httpd -DFOREGROUND
                └─43698 /usr/sbin/httpd -DFOREGROUND
                  └─43699 /usr/sbin/httpd -DFOREGROUND
                    └─43701 /usr/sbin/httpd -DFOREGROUND

окт 14 15:05:22 info-sec systemd[1]: Starting The Apache HTTP Server...
окт 14 15:05:22 info-sec systemd[1]: Started The Apache HTTP Server.
окт 14 15:05:22 info-sec httpd[43696]: Server configured, listening on: port 81
lines 1-19/19 (END)
```

Рис. 0.20: Повторный запуск веб-сервера

0.23 Ход работы

Вернем контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`. Попробуем получить доступ к файлу через веб-сервер.

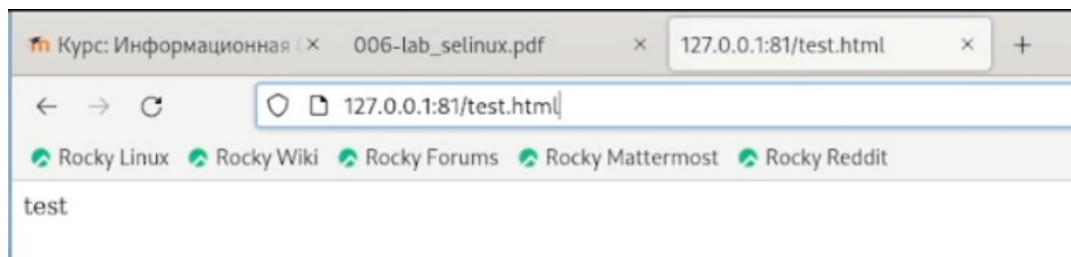


Рис. 0.21: Файл `test.html` в браузере после возвращения контекста

0.24 Ход работы

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

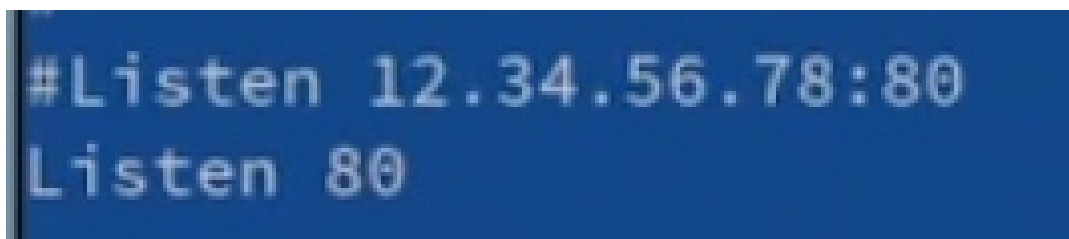


Рис. 0.22: Параметр `Listen` после возвращения значения

0.25 Ход работы

Попробуем удалить привязку `http_port_t` к 81. Удаление невозможно.

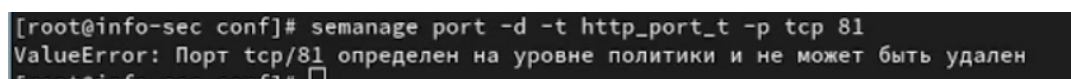
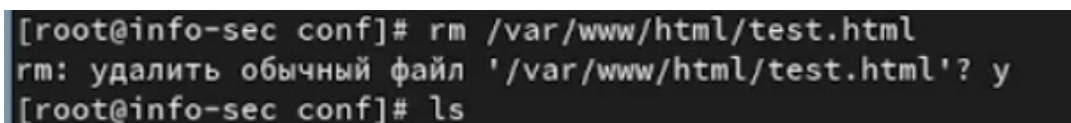


Рис. 0.23: Попытка удаления привязки к порту 81

0.26 Ход работы

Удалим файл /var/www/html/test.html.

A terminal window with a dark background and light-colored text. The prompt is [root@info-sec conf]#. The first command is rm /var/www/html/test.html. The second line shows the output: rm: удалить обычный файл '/var/www/html/test.html'? y. The third line shows the prompt again followed by the command ls.

```
[root@info-sec conf]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@info-sec conf]# ls
```

Рис. 0.24: Удаление файла /var/www/html/test.html

0.27 Результаты

В рамках данной лабораторной работы были развиты навыки администрирования ОС Linux. Получено первое практическое знакомство с технологией SELinux1. Проверена работа SELinux на практике совместно с веб-сервером Apache.