

Лабораторная работа №6

Мандантное разграничение прав в Linux

Шестаков Д. С.

14 октября 2023

Российский университет дружбы народов, Москва, Россия

Информация

- Шестаков Дмитрий Сергеевич
- студент группы НКНбд-01-20
- Российский университет дружбы народов
- dmshestakov@icloud.com

Вводная часть

- Мандатное разграничение прав
- ОС Linux
- Bash

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

- ОС Linux
- Bash

1. Вошли в систему и убедились, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.
2. С помощью команды `service httpd status` убедились, что веб-сервер работает

```
root@rocky:~# service httpd start
Redirecting to /bin/systemctl start httpd.service
root@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; preset: disabled)
   Active: active (running) since Sat 2023-10-14 08:43:01 EDT; 5s ago
     Docs: man:httpd.service(8)
   Main PID: 50469 (httpd)
    Status: "Started, listening on: port 80"
     Tasks: 213 (limit: 4493)
    Memory: 17.7M
       CPU: 68ms
   CGroup: /system.slice/httpd.service
           └─50469 /usr/sbin/httpd -DFOREGROUND
             └─50470 /usr/sbin/httpd -DFOREGROUND
               └─50471 /usr/sbin/httpd -DFOREGROUND
                 └─50472 /usr/sbin/httpd -DFOREGROUND
                   └─50473 /usr/sbin/httpd -DFOREGROUND

окт 14 08:43:01 Rocky systemd[1]: Starting The Apache HTTP Server...
окт 14 08:43:01 Rocky httpd[50469]: Server configured, listening on: port 80
окт 14 08:43:01 Rocky systemd[1]: Started The Apache HTTP Server.
```

Рис. 1: Запуск веб-сервера

Нашли веб-сервер Apache в списке процессов и определили ее контекст: `unconfined_t`

```
[root@Rocky ~]# ps aux | grep httpd
system_u:system_r:httpd_t:s0 root      58469  0.0  1.4 20172 11436 ?        Ss   08:43  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  58470  0.0  0.0 21508 7320 ?        Ss   08:43  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  58471  0.0  1.3 1669204 10892 ?      Sl   08:43  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  58472  0.0  1.1 1538068 8836 ?        Sl   08:43  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  58473  0.0  1.1 1538068 8844 ?        Sl   08:43  0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root  58694  0.0  0.2 221680 2336 pts/1  S+  08:43  0:00 grep --color=auto httpd
[root@Rocky ~]#
```

Рис. 2: Определение контекста

Посмотрели текущее состояние преключателей SELinux для Apache с помощью команды

```
sestatus -b | grep httpd
```

```
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
httpd_use_nfs             off
httpd_use_openscryptoki    off
httpd_use_openstack       off
httpd_use_sasl            off
httpd_verify_dns          off
```

Посмотрели статистику по политике, также определили 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:                  135      Permissions:              457
Sensitivities:            1        Categories:              1024
Types:                    5100     Attributes:               258
Users:                    8         Roles:                   14
Booleans:                 353      Cond. Expr.:             384
Allow:                    65009    Neverallow:              0
Auditallow:              170      Dontaudit:               8572
Type_trans:              265337   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
```

Рис. 4: Статистика по политике

Определили тип файлов и поддиректорий, находящихся в директории `/var/www`

```
[root@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 16 16:21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 мая 16 16:21 html
[root@Rocky ~]# ls -lZ /var/www/html
итого 0
```

Рис. 5: Тип файлов `/var/www`

Определили тип файлов в директории `/var/www/html`

```
[root@Rocky ~]# ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 окт 14 08:48 test.html
```

Рис. 6: Тип файлов `/var/www/html`

Создайте от имени суперпользователя html-файл `var/www/html/test.html` следующего содержания:

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

- Проверили контекст созданного файла
- Обратились к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`.

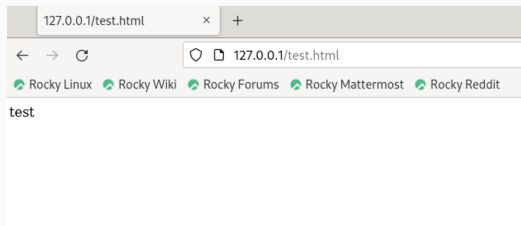


Рис. 7: Обращение к файлу через веб-сервер

- Изучили справку `man httpd_selinux`. Узнали, что существуют следующие контексты файлов: `unconfined_u`, `object_r`, `system_r`, `secadm_r`, `httpd_sys_content_r`.
- Изменили контекст файла `/var/www/html/test.html` на `samba_share_t`.

```
[root@Rocky ~]# chcon -t samba_share_t /var/www/html/test.html
[root@Rocky ~]# ls -Z /var/www/html/test.html
ls: невозможно получить доступ к '/var/www/html/test.html': Нет такого файла или каталога
[root@Rocky ~]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@Rocky ~]#
```

Рис. 8: Изменение контекста файла

- Запустили веб-сервер Apache на прослушивание TCP-порта 81.
- Выполнили перезапуск веб-сервера. Сбой не произошёл.

```
[root@Rocky ~]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@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; preset: disabled)
   Active: active (running) since Sat 2023-10-14 09:00:48 EDT; 11s ago
     Docs: man:httpd.service(8)
   Main PID: 52884 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
     Tasks: 213 (limit: 4493)
    Memory: 15.2M
       CPU: 68ms
    CGroup: /system.slice/httpd.service
            └─52884 /usr/sbin/httpd -DFOREGROUND
              └─52885 /usr/sbin/httpd -DFOREGROUND
                └─52886 /usr/sbin/httpd -DFOREGROUND
                  └─52887 /usr/sbin/httpd -DFOREGROUND
                    └─52888 /usr/sbin/httpd -DFOREGROUND

окт 14 09:00:48 Rocky systemd[1]: Starting The Apache HTTP Server...
окт 14 09:00:48 Rocky httpd[52884]: Server configured, listening on: port 81
окт 14 09:00:48 Rocky systemd[1]: Started The Apache HTTP Server.
[root@Rocky ~]#
```

Рис. 10: Прослушивание порта 81

Проанализировали лог-файлы, и выяснили, что запись появилась только в `/var/log/messages`.

```
Oct 14 08:58:38 localhost systemd[1]: Starting The Apache HTTP Server...
Oct 14 08:58:38 localhost httpd[52640]: Server configured, listening on: port 80
Oct 14 08:58:38 localhost systemd[1]: Started The Apache HTTP Server.
Oct 14 09:00:00 localhost NetworkManager[927]: <info> [1697288400.2254] dhcp4 (enp0s5): state changed new lease, address=10.211.55.11
Oct 14 09:00:36 localhost systemd[1]: Stopping The Apache HTTP Server...
Oct 14 09:00:37 localhost systemd[1]: httpd.service: Deactivated successfully.
Oct 14 09:00:37 localhost systemd[1]: Stopped The Apache HTTP Server.
Oct 14 09:00:48 localhost systemd[1]: Starting The Apache HTTP Server...
Oct 14 09:00:48 localhost httpd[52884]: Server configured, listening on: port 81
Oct 14 09:00:48 localhost systemd[1]: Started The Apache HTTP Server.
```

Рис. 11: Анализ лог-файлов

Выполнили команду `bash semanage port -a -t http_port_t -p tcp 81`.

```
[root@Rocky ~]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@Rocky ~]# 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
```

Рис. 12: Команды по привязке TCP-порта

- Перезапустили веб-сервер, также не сбой не произошел. Вернули контекст файлу `/var/www/html/test.html`.
- Исправили обратно конфигурационный файл Apache.

Изучили механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получили практические навыки работы в консоли с дополнительными атрибутами. Рассмотрели работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.