Лабораторная работа № 6

Мандатное разграничение прав в Linux

Хамдамова А. А.

12 апреля 2024

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Хамдамова Айжана Абдукаримовна
- студент Факультета Физико-математических и естественных наук
- Российский университет дружбы народов
- 1032225989@pfur.ru
- https://github.com/AizhanaKhamdamova/study_2023-2024_infosec

Теоретическое введение

SELinux (Security-Enhanced Linux) обеспечивает усиление защиты путем внесения изменений как на уровне ядра, так и на уровне пространства пользователя, что превращает ее в действительно «непробиваемую» операционную систему. Впервые эта система появилась в четвертой версии CentOS, а в 5 и 6 версии реализация была существенно дополнена и улучшена. SELinux имеет три основных режим работы:

Enforcing: режим по умолчанию. При выборе этого режима все действия, которые каким-то образом нарушают текущую политику безопасности, будут блокироваться, а попытка нарушения будет зафиксирована в журнале.

Permissive: в случае использования этого режима, информация о всех действиях, которые нарушают текущую политику безопасности, будут зафиксированы в журнале, но сами действия не будут заблокированы. Disabled: полное отключение системы принудительного контроля доступа.

Политика SELinux определяет доступ пользователей к ролям, доступ ролей к доменам и доступ доменов к типам. Контекст безопасности — все атрибуты SELinux — роли, типы и домены. Более подробно см. в [1]. Apache — это свободное программное обеспечение, с помощью которого можно создать веб-сервер. Данный продукт возник как доработанная версия другого HTTP-клиента от национального центра суперкомпьютерных приложений (NCSA). Для чего нужен Apache сервер: чтобы открывать динамические PHP-страницы, для распределения поступающей на сервер нагрузки, для обеспечения отказоустойчивости сервера, чтобы потренироваться в настройке сервера и запуске PHP-скриптов.

Apache является кроссплатформенным ПО и поддерживает такие операционные системы, как Linux, BSD, MacOS, Microsoft, BeOS и другие.

Цели и задачи

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

Ход работы

Пример №1

```
[akhamdamova@akhamdamova ~]$ 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: inactive (dead)
       Docs: man:httpd.service(8)
[akhamdamova@akhamdamova ~]$ sudo systemctl start httpd
[akhamdamova@akhamdamova ~]$ sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[akhamdamova@akhamdamova ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
     Active: active (running) since Fri 2024-04-26 12:55:43 MSK; 16s ago
       Docs: man:httpd.service(8)
   Main PID: 41268 (httpd)
     Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec:   0 B/sec"
      Tasks: 213 (limit: 10901)
     Memory: 23.5M
        CPU: 118ms
     CGroup: /system.slice/httpd.service
             ├─41268 /usr/sbin/httpd -DFOREGROUND
             ├─41269 /usr/sbin/httpd -DFOREGROUND
             ├─41270 /usr/sbin/httpd -DFOREGROUND
             ├─41271 /usr/sbin/httpd -DFOREGROUND
             └─41275 /usr/sbin/httpd -DFOREGROUND

Apr 26 12:55:42 akhamdamova.localdomain systemd[1]: Starting The Apache HTTP Server...
Apr 26 12:55:43 akhamdamova.localdomain systemd[1]: Started The Apache HTTP Server.
Apr 26 12:55:43 akhamdamova.localdomain httpd[41268]: Server configured, listening on: port 80
[akhamdamova@akhamdamova ~]$
```

Пример №2

```
[akhamdamova@akhamdamova ~]$ 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
```

Пример №3

```
 * 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:             135    Permissions:         457
  Sensitivities:         1    Categories:         1024
  Types:              5135    Attributes:          259
  Users:                 8    Roles:                15
  Booleans:            357    Cond. Expr.:         390
  Allow:             65409    Neverallow:            0
  Auditallow:          172    Dontaudit:          8647
  Type_trans:       267813    Type_change:          94
  Type_member:          37    Range_trans:        6164
  Role allow:           39    Role_trans:          419
  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:             665
  Netifcon:              0    Nodecon:               0

[akhamdamova@akhamdamova ~]$
```

Пример №4

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

Результаты

Развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux1. Проверила работу SELinx на практике совместно с веб-сервером Apache.