Лабораторная работа №6

Мандатное разграничение прав в Linux

Парфенова Е. Е.

12 октября 2024

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Парфенова Елизавета Евгеньвена
- студент
- Российский университет дружбы народов
- 1032216437@pfur.ru
- https://github.com/parfenovaee

Вводная часть

Актуальность

Важность понимания работы технологии SELinux для эффективной работы с ОС Linux и обеспечения директориям и файлам должной безопасности

Цели и задачи

Цель: Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux

Задача: Проверить работу SELinx на практике совместно с веб-сервером Apache.

Теоретическое введение

Теоретичсекое введение(1)

SELinux — это система принудительного контроля доступа, реализованная на уровне ядра, которая применяется только в том случае, если проверка классической системой прав Unix будет успешно пройдена.

Теоретичсекое введение(2)

Основные термины, использующиеся в SELinux:

- *Домен* — список действий, которые может выполнять процесс.
- *Роль* — список доменов, которые могут быть применены.
- *Тип* — набор действий, которые допустимы по отношения к объекту.
- *Контекст безопасности* — все атрибуты SELinux — роли, типы и домены.

Теоретичсекое введение(3)

SELinux имеет три основных режим работы, при этом по умолчанию установлен режим Enforcing. Режимы работы SELinux:

1. Enforcing
2. Permissive
3. Disabled

Выполнение лабораторной работы

Подготовка лабораторного стенда

```
[root@eeparfenova ~]# nano /etc/httpd/httpd.conf
[root@eeparfenova ~]# nano /etc/httpd/conf/httpd.conf
[root@eeparfenova ~]# iptables -F
[root@eeparfenova ~]# iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT
Bad argument `iptables'
Try `iptables -h' or 'iptables --help' for more information.
[root@eeparfenova ~]# iptables -P INPUT ACCEPT
[root@eeparfenova ~]# iptables -P OUTPUT ACCEPT
[root@eeparfenova ~]#
```

Рис. 1: Подготовка лабораторного стенда

Просмотр редима и политики SELinux

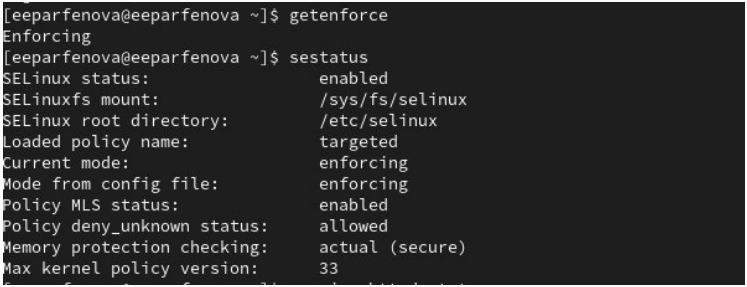

Рис. 2: Просмотр режима и политики SELinux

Запуск и проверка работы сервера Apache

```
[eeparfenova@eeparfenova ~]$ su -
Password:
[root@eeparfenova ~]# 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: inactive (dead)
       Docs: man:httpd.service(8)
[root@eeparfenova ~]# sudo systemctl restart httpd
[root@eeparfenova ~]# sudo systemctl start httpd
[root@eeparfenova ~]# sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
     Active: active (running) since Wed 2024-10-09 17:56:00 MSK; 24s ago
       Docs: man:httpd.service(8)
   Main PID: 42967 (httpd)
     Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec:   0 B/sec"
      Tasks: 177 (limit: 12207)
     Memory: 24.0M
        CPU: 125ms
     CGroup: /system.slice/httpd.service
             ├─42967 /usr/sbin/httpd -DFOREGROUND
             ├─42968 /usr/sbin/httpd -DFOREGROUND
             ├─42969 /usr/sbin/httpd -DFOREGROUND
             ├─42970 /usr/sbin/httpd -DFOREGROUND
             └─42971 /usr/sbin/httpd -DFOREGROUND

Oct 09 17:56:00 eeparfenova.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 09 17:56:00 eeparfenova.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 09 17:56:00 eeparfenova.localdomain httpd[42967]: Server configured, listening on: port 80
[root@eeparfenova ~]#
```

Рис. 3: Запуск и проверка работы сервера Apache

Контекст безопасности сервера Apache: system_u:system_r:httpd_t:s0

```
[root@eeparfenova ~]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root       42967  0.0  0.5  20152 11544 ?        Ss   17:55   0:00 /usr/sbin/http
d -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     42968  0.0  0.3  22032  7484 ?        S    17:56   0:00 /usr/sbin/http
d -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     42969  0.0  0.6 1112588 13600 ?       Sl   17:56   0:00 /usr/sbin/http
d -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     42970  0.0  0.6 981452 13412 ?        Sl   17:56   0:00 /usr/sbin/http
d -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     42971  0.0  0.5 981452 11284 ?        Sl   17:56   0:00 /usr/sbin/http
d -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 43203 0.0  0.1 221664 2304 pts/0 S+ 17:57   0:00 grep
--color=auto httpd
[root@eeparfenova ~]# ps -eZ | grep httpd
system_u:system_r:httpd_t:s0      42967 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      42968 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      42969 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      42970 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      42971 ?        00:00:00 httpd
[root@eeparfenova ~]#
```

Рис. 4: Контекст безопасности сервера Apache

Переключатели SELinux для Apache

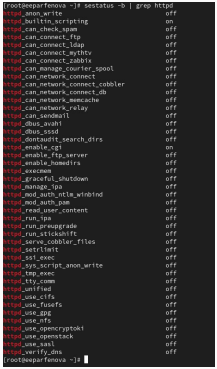

Рис. 5: Текущее состояние переключателей SELinux для Apache

Статистика по политике

```
[root@eeparfenova ~]# 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:              5145    Attributes:          259
  Users:                 8    Roles:                15
  Booleans:            356    Cond. Expr.:         388
  Allow:             65500    Neverallow:            0
  Auditallow:          176    Dontaudit:          8682
  Type_trans:       271770    Type_change:          94
  Type_member:          37    Range_trans:        5931
  Role allow:           40    Role_trans:          417
  Constraints:          70    Validatetrans:         0
  MLS Constrain:        72    MLS Val. Tran:         0
  Permissives:           4    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
```

Рис. 6: Статистика по политике

Множество пользователей, ролей, типов

- Users - 8
- Roles - 15
- Types - 5145

```
[root@eeparfenova ~]# seinfo -u

Users: 8
   guest_u
   root
   staff_u
   sysadm_u
   system_u
   unconfined_u
   user_u
   xguest_u
[root@eeparfenova ~]# seinfo -r

Roles: 15
   auditadm_r
   container_user_r
   dbadm_r
   guest_r
   logadm_r
   nx_server_r
   object_r
   secadm_r
   staff_r
   sysadm_r
   system_r
   unconfined_r
   user_r
   webadm_r
   xguest_r
[root@eeparfenova ~]# seinfo -t

Types: 5145
   NetworkManager_dispatcher_chronyc_script_t
   NetworkManager_dispatcher_chronyc_t
   NetworkManager_dispatcher_cloud_script_t
   NetworkManager_dispatcher_cloud_t
   NetworkManager_dispatcher_console_script_t
   NetworkManager_dispatcher_console_t
   NetworkManager_dispatcher_console_var_run_t
   NetworkManager_dispatcher_custom_t
   NetworkManager_dispatcher_ddclient_script_t
   NetworkManager_dispatcher_ddclient_t
   NetworkManager_dispatcher_dhclient_script_t
   NetworkManager_dispatcher_dhclient_t
   NetworkManager_dispatcher_dnssec_script_t
   NetworkManager_dispatcher_dnssec_t
```

Рис. 7: Множество пользователей, ролей, типов

Файлы и поддиректори в /var/www

```
[root@eeparfenova ~]# ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Aug  8 19:30 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0     6 Aug  8 19:30 html
[root@eeparfenova ~]# ls -lZ /var/www/html
total 0
[root@eeparfenova ~]#
```

Рис. 8: Файлы и поддиректори в /var/www

Файл test.html

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

Рис. 9: Создание файла test.html и его контекст

Файл test.html

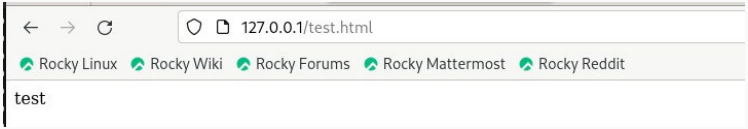

Рис. 10: Отображение файла через веб-сервер

Файл test.html

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

Рис. 11: Изменение контекста файла

Файл test.html

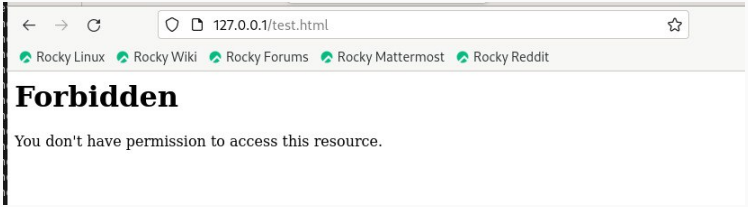

Рис. 12: Сообщение об ошибке после изменения контекста файла

Лог-файлы

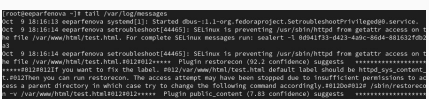

Рис. 13: Файл /var/log/messages*

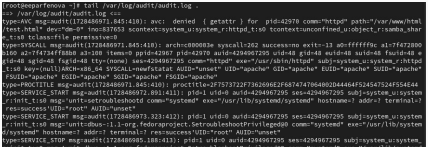

Рис. 14: Файл /var/log/audit/audit.log

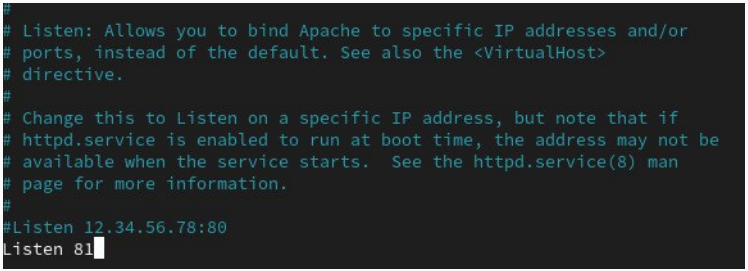

Рис. 15: Замена порта в config файле

Сбой сервера при запуске с 81 порта

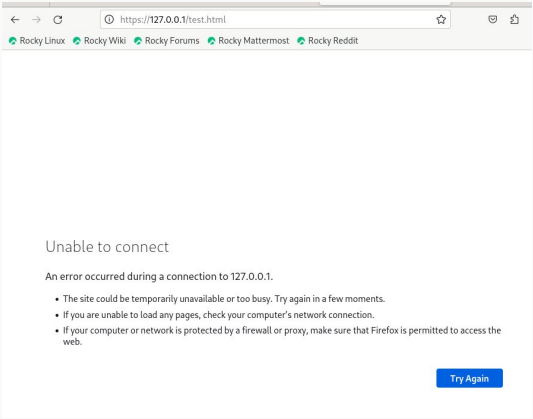

Рис. 16: Сбой сервера при запуске с 81 порта

Вывод: Появилась новая запись в лог-файла ошибок о невозможности загрузки, и не появилось новой записи в лог-файле доступа.

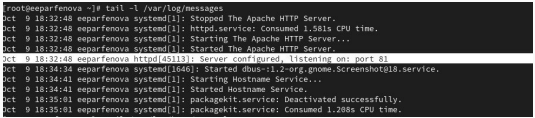

Рис. 17: Файл /var/log/messages

Добавление порта

Вывод: Страницы недоступна из-за неправильного контекста

```
[root@eeparfenova ~]# 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@eeparfenova ~]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@eeparfenova ~]# semanage port -a -t http_port_t -p tcp 81
Port tcp/81 already defined, modifying instead
[root@eeparfenova ~]# semanage port -l | grep http_port_t
http_port_t                    tcp      81, 80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t            tcp      5988
[root@eeparfenova ~]#
```

Рис. 18: Добавление 81 порта

Изменение контекста и открытие страницы

Рис. 19: Изменение контекста обратно

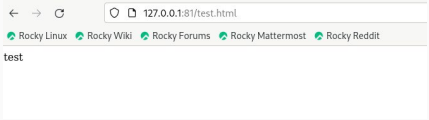

Рис. 20: Содержимое файла по новому адресу

Возвращение всех изменений

Рис. 21: Возвращение всех изменений

Вывод

Выводы

Мы развили навыки администрирования ОС Linux и получили первое практическое знакомство с технологией SELinux. Для этого мы проверили работу SELinx на практике совместно с веб-сервером Apache.