Лабораторная работа №6

Мандатное разграничение прав в Linux

Федорина Эрнест Васильевич

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Федорина Эрнест Васильевич
- студент
- Российский университет дружбы народов
- 1032216454@pfur.ru
- https://evfedorina.github.io/ru/

Цель работы

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

Apache HTTP-сервер (в иронической трактовке является искажённым сокращением от англ. a patchy server; среди русских пользователей общепринято переводное апа́ч) — свободный веб-сервер.

Выполнение лабораторной работы

Для начала организуем рабочий стренд, - установим apache, проверим используемый режим и политику, а также отключим некоторые пакетные фильтры (рис. (fig:001?))

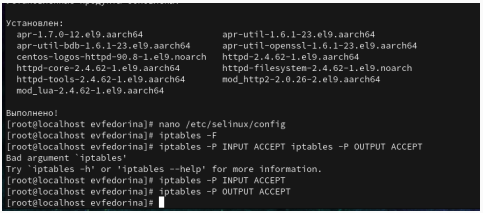

Рис. 1: начало работы с selinux

Старт работы веб-сервера

Увидели, что веб-сервер не работает (рис. (fig:002?)), включили его (рис. (fig:003?)) и посмотрели контекст безопасности (рис. (fig:004?))

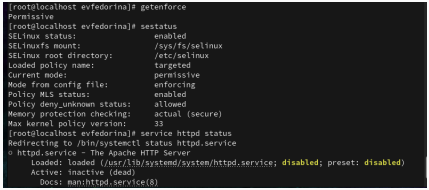

Рис. 2: статус enforce и работы веб-сервера

Старт работы веб-сервера

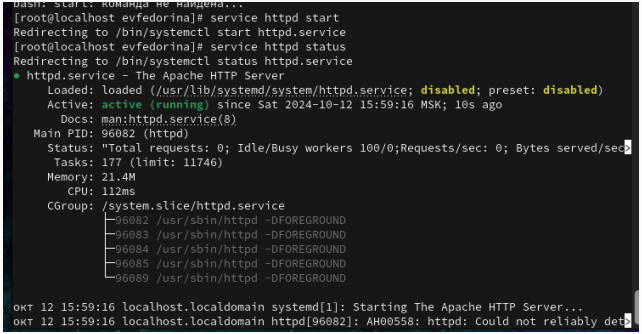

Рис. 3: активный веб-сервер

Старт работы веб-сервера

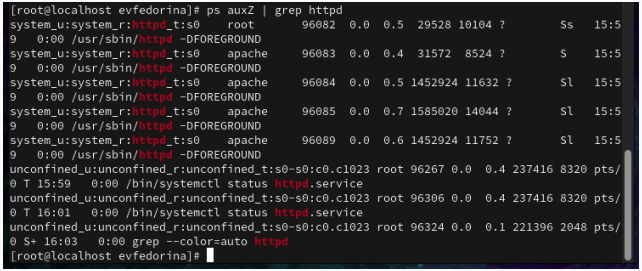

Рис. 4: контекст безопасности

Просмотр состояния переключателей

Потом посмотрели состояние переключателей (рис. (fig:005?))

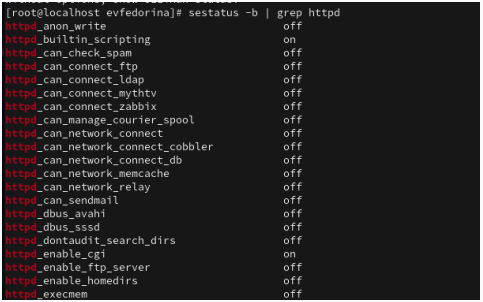

Рис. 5: состояние переключателей SELinux

Статистика по политике

Далее посмотрим статистику по политике (рис. (fig:006?))

```
[root@localhost evfedorina]# 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:              5169    Attributes:          259
  Users:                 8    Roles:                15
  Booleans:            358    Cond. Expr.:         390
  Allow:             65633    Neverallow:            0
  Auditallow:          176    Dontaudit:          8703
  Type_trans:       271851    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:           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
[root@localhost evfedorina]#
```

Рис. 6: статистика по политике

Старт работы веб-сервера

У нас 8 пользователей, 5169 типов и 15 ролей.

Начало работы с файлом test.html

Определим тип файлов в директории /var/www/html, создадим там файл test.html и проверим его контекст (рис. (fig:007?))

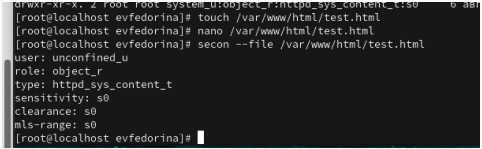

Рис. 7: работа с директорией html

Обратимся к файлу через веб-сервер и увидим там текст, написанный нами ранее в файле test.html, доступ есть (рис. (fig:008?))

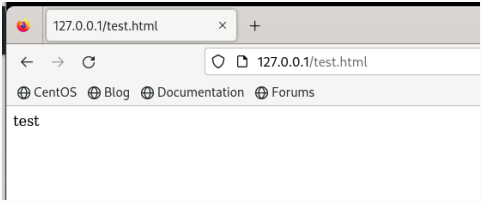

Рис. 8: открытие test.html через веб-сервер

Работа с контекстами

Изучив справку httpd_selinux мы выяснили нужные контексты, сопоставили их с контекстами нашего файла, рассмотреои полученный контекст детально, а потом изменили контекст файла, чтобы процесс httpd не имел доступа к файлу (рис. (**fig:009?**))

Рис. 9: просмотр и изменение контекста файла

Просмотр log-файлов

Смотрим log-файлы веб-сервера и системные логи (рис. (fig:010?))

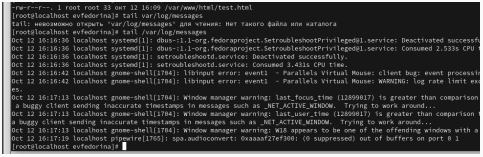

Рис. 10: просмотр log-файлов

Просмотр log-файлов и изменение параметра listen

В httpd.conf изменили параметр listen с 80 на 81, потом перезапустили веб-сервер, произошёл сбой.

Далее мы опять посмотрели log-файлы (рис. (**fig:011?**))

Просмотр log-файлов и изменение параметра listen

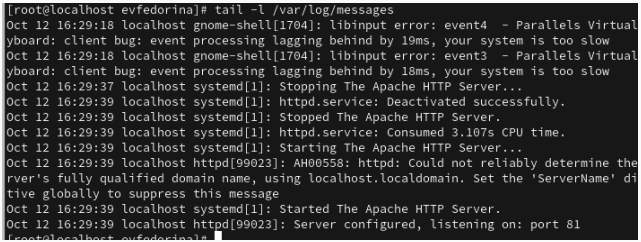

Рис. 11: просмотр новых log-файлов

Использование команды semanage port и просмотр log-файлов

Выполнили команду semanage port, проверили список портов и увидели там 81, а затем снова запустили веб-сервер Apache, успешно (рис. (fig:012?))

Рис. 12: просмотр новых log-файлов

Завершение лабораторной работы

В конце лабораторной работы убрали все изменения в файлах, удалили test.html и удалили привязку httpd_port_t к 81 порту

Выводы

Выводы

Развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux. Проверили работу SELinx на практике совместно с веб-сервером Apache.

Список литературы:

Список литературы:

1. Apache[Электронный ресурс] - https://ru.wikipedia.org/wiki/Apache