Лабораторная работа №6

Мандантное разграничение прав в Linux

Шестаков Д. С.

14 октября 2023

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

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

Вводная часть

Объект и предмет исследования

- Мандатное разграничение прав
- ОС Linux
- Bash

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.

Материалы и методы

- ОС Linux
- Bash

Ход работы

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

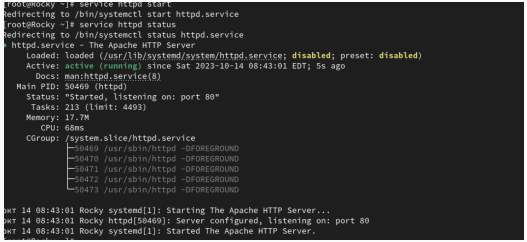


Рис. 1: Запуск веб-сервера

Ход работы

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

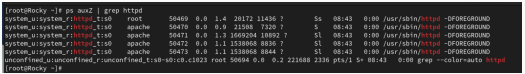
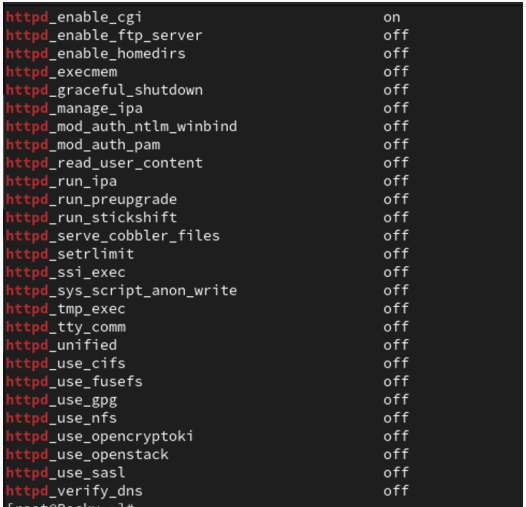


Рис. 2: Определение контекста

Ход работы

Посмотрели текущее состояние преключателей SELinux для Apache с помощью команды

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



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

Ход работы

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

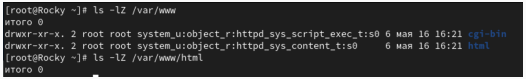


Рис. 5: Тип файлов /var/www

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

Рис. 6: Тип файлов /var/www/html

Ход работы

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

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

Ход работы

- Проверили контекст созданного файла
- Обратились к файлу через веб-сервер, введя в браузере адрес `http://127.0.01/test.html`.

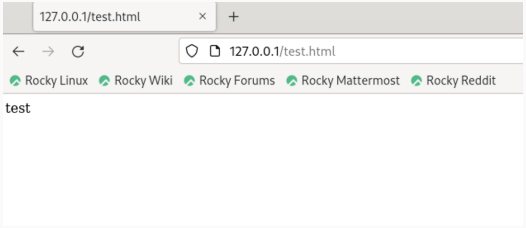


Рис. 7: Обращение к файлу через веб-сервер

Ход работы

- 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.

Рис. 8: Изменение контекста файла

Ход работы

- Попробовали еще раз получить доступ к файлу через веб-сервер. Не получили сообщнеие об ошибке.
- Посмотрели системный лог-файл

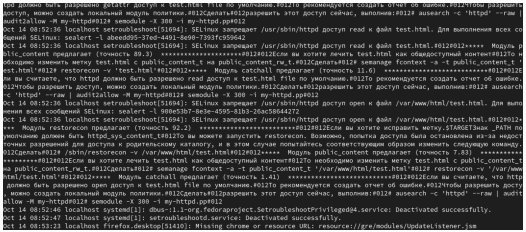


Рис. 9: Системный лог-файл

Ход работы

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

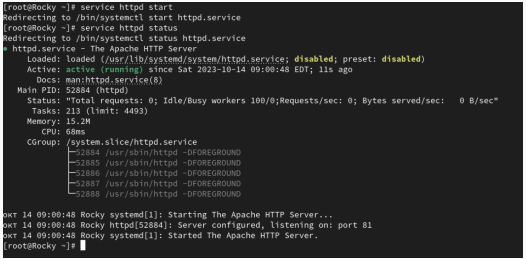


Рис. 10: Прослушивание порта 81

Ход работы

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

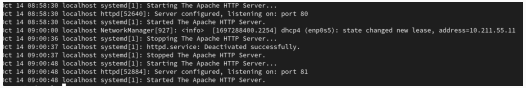


Рис. 11: Анализ лог-файлов

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

Рис. 12: Команды по привязке TCP-порта

Ход работы

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

Вывод

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.