

HƯỚNG DẪN LAB: Labtainer -r steghide-extract-lab

1. Mục đích

Bài lab này hướng dẫn sinh viên cách sử dụng công cụ Steghide để giấu tin trong ảnh, một kỹ thuật phổ biến trong Steganography (giấu tin mật). Qua bài lab, sinh viên sẽ:

- Hiểu khái niệm cơ bản về Steganography.
- Sinh viên sẽ học cách giải mã thông tin đã giấu trong ảnh bằng công cụ Steghide.
- Sinh viên sẽ làm quen với các bước kiểm tra và trích xuất dữ liệu bị giấu.

2. Yêu cầu đối với sinh viên

Trước khi thực hiện bài lab này, sinh viên cần:

- Có kiến thức cơ bản về dòng lệnh Linux.
- Hiểu khái niệm về Steganography và ứng dụng của nó.
- Biết cách sử dụng Labtainer để chạy môi trường thực hành.

3. Nội dung lý thuyết

3.1. Giới thiệu về Steganography

Steganography là kỹ thuật giấu thông tin trong các file đa phương tiện (ảnh, âm thanh, video, v.v.) sao cho sự tồn tại của thông tin bí mật không bị phát hiện. So với mã hóa, steganography giúp ẩn dữ liệu mà không gây nghi ngờ.

3.2. Công cụ Steghide

Steghide là một công cụ mã nguồn mở dùng để giấu và trích xuất dữ liệu từ các file ảnh hoặc âm thanh. Nó hỗ trợ nén và mã hóa dữ liệu trước khi nhúng vào file chứa.

4. Nội dung thực hành

4.1. Khởi động Lab

1. Chạy Labtainer và mở bài lab steghide_lab:

```
labtainer steghide-extract-lab
```

4.2. Thực hiện giấu tin trong ảnh

1. Kiểm tra thông tin file ảnh

```
Steghide info input.jpg(pass = 123456)
```

2. Thực hiện giải mã thông tin

`steghide extract -sf input.jpg`

- `-sf` (Source File): Tùy chọn này dùng để chỉ ra tệp tin nguồn, tức là tệp ảnh (hoặc âm thanh) chứa thông tin đã được giấu bên trong.
- Hệ thống sẽ yêu cầu nhập mật khẩu bảo vệ(123456)

3. Kiểm tra thông tin được trích xuất

`cat secret.txt`

4. Thay đổi mật khẩu ảnh chứa tin bằng cách ghi đè

`steghide embed -cf input.jpg -ef secret.txt`

Kết thúc bài lab

- Kiểm tra checkwork

`checkwork`

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

`Stoplabs`

- Khởi động lại bài lab :

`Labtainer -r steghide-extract-lab`