Bài thực hành: Phát hiện giấu tin trong văn bản bằng công cụ stegcloak sử dụng ký tự vô hình

1. Mục đích

- Giúp sinh viên hiểu được cách thức giấu tin mật trong văn bản bằng ký tự vô hình (zero-width).
- Thực hành sử dụng công cụ stegcloak để giấu và trích xuất thông tin bí mật.

2. Yêu cầu đối với sinh viên

- Sinh viên có kiến thức cơ bản về hệ điều hành Linux
- Có khả năng lập trình bash script bằng Python

3. Nội dung thực hành
   - Tải bài lab: Sinh viên tải bải lab từ link github sau:

     https://github.com/Mbr-clown-lord/stego-zero-width-detect

   - Khởi động bài lab:

     labtainer -r stego-zero-width-detect

     (chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)

   - Cài đặt công cụ Stegcloak:

     sudo npm install -g stegcloak
   - Kiểm tra việc cài đặt công cụ Stegcloak:

     which stegcloak

     Sử dụng lệnh sau để xem các sử dụng công cụ Stegcloak để giấu và tách tin:

     - Hide

       stegcloak hide -h
     - Reveal

       stegcloak reveal -h

3.1. Nhiệm vụ 1: Tìm file giấu tin

Trong thư mục người dùng ubuntu có chưa 2 file trong đó có một file đã được dùng đề giấu tin. Sinh viên có thể xem nội dung 2 file bằng lệnh cat:

cat file1.txt

cat file2.txt

Quan sát nội dung 2 file sẽ thấy chúng đều giống nhau, tuy nhiên khi dùng lệnh diff để kiểm tra sẽ thấy được sự khác nhau giữa 2 file.

diff file1.txt file2.txt

Đề tìm ra có giấu tin bằng kỹ thuật sử dụng ký tự vô hình, sinh viên sử dụng xxd để hiện thị nội dung của 2 file dưới dạng giá trị hex

xxd file1.txt

xxd file2.txt

Xem kết quả trả về và cho biết file nào là file giấu tin. Dùng lệnh echo ra tên file đó

echo filename.txt

3.2. Nhiệm vụ 2: Trích xuất thông điệp được giấu

Thông điệp được giấu trong file tìm được ở nhiệm vụ 1 có dạng flag{this_is_flag}. Sinh viên cần tìm ra được thông điệp và lưu kết quả vào file flag.txt

Sinh viên sử dụng công cụ stegcloak để trích xuất ra thông điệp được giấu.

stegcloak reveal -f filename.txt

Lúc này, sinh viên sẽ được yêu cầu nhập mật khẩu để trích xuất thông tin(rõ ràng file đã được giấu sử dụng mật khẩu để bảo vệ)

Để tìm ra mật khẩu để trích xuất thông điệp, sinh viên có thể sử dụng brute force bằng cách viết một script Python và xây dựng một wordlist mật khẩu có khả năng là mật khẩu được sử dụng để giấu tin.

Sinh viên cần tìm ra mật khẩu dùng để giấu tin và lưu kết quả vào file pass.txt

- Kết thúc bài lab:
  o Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:
  stoplab stego-zero-width-detect
  o 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:

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

labtainer -r stego-zero-width-detect