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

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

   - Khởi động bài lab:

     labtainer -r stego-zero-width

     (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

3.1. Nhiệm vụ 1: Giấu và trích xuất tin mật cơ bản(không dùng mật khẩu)

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

Sinh viên thử chạy một lệnh giấu một thông điệp vào một chuỗi văn bản bất kỳ với cú pháp câu lệnh như sau:

stegcloak hide [options] [serret] [cover]

Ví dụ:

stegcloak hide -n “pass123” “This is cover text”

Sau khi chạy lệnh trên, thông điệp secret sẽ được giấu vào trong chuỗi cover bằng cách sử dụng các ký tự vô hình sau đó được lưu vào clipboad. Tạo tệp bằng nano và lưu chuỗi corver đã giấu tin từ clipboard vào sau đó dùng lệnh cat đọc file để xem chuỗi cover sau khi đã giấu tin.

Để lấy thông điệp đã giấu trong chuỗi cover, sinh vieenh sử dụng lệnh sau:

stegcloak reveal -cp

3.2. Nhiệm vụ 2: Giấu và trình xuất tin từ tệp văn bản(không dùng mật khẩu)

Trong thư mục người dùng ubuntu có lưu 2 file secret.txt(file chứa thông điệp cần giấu) và cover.txt(file chứa văn bản dùng đề giấu) là. Sinh viên có thể xem nội dung của 2 file bằng lệnh cat:

cat secret.txt

cat cover.txt

Sử dụng lệnh sau để thực hiện giấu thông điệp trong file secret.txt vào nội dung văn bản trong file cover.txt.

stegcloak -n -fs secret.txt -fc cover.txt -o output.txt

Lệnh này sẽ thực hiện đọc nội dung file secret.txt sau đó thực hiện giấu chúng vào nội dung văn bản trong file cover.txt và lưu kết quả vào file output.txt. Dùng lệnh cat để xem nộp dung file chứa văn bản đã giấu tin:

cat output.txt

Để trích thông tin giấu trong file output.txt, sử dụng lệnh sau:

stegcloak reveal -f output.txt

3.3. Nhiệm vụ 3: Bảo vệ nội dung với Integrity check(không dùng mật khẩu)

Để đảm bảo tính toàn vẹn của văn bản giấu tin, sử dụng tùy chọn –integrity/-i khi chạy lệnh giấu tin:

stegcloak hide -n *-i -fs secret.txt -fc cover.txt -o output.txt*

Sử dụng nano để chỉnh sửa nội dung file output.txt sau đó chạy lệnh tách tin và xem kết quả:

stegcloak reveal -f output.txt

3.4. Nhiệm vụ 4: Giấu và trích xuất tin có sử dụng mật khẩu

Để tăng tính bảo mật cho thông điệp giấu, mặc định stegcloak có hỗ trợ thêm chức năng sử dụng mật khẩu khi giấu và tách tin. Để sử dụng, chạy lệnh sau:

stegcloak hide *-fs secret.txt -fc cover.txt -o output.txt*

Khi chạy lệnh trên, stegcloak sẽ yêu cầu nhập mật khẩu, sinh viên nhập một mật khẩu bất kỳ.

Để tách thông điệp đã giấu, sử dụng lệnh sau:

stegcloak reveal -f output.txt

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

  stoplab stego-zero-width

  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