Bài Lab: Phát hiện tin trong ảnh được giấu bằng phương pháp hoán vị giả ngẫu nhiên

1. Mục đích

- Mục tiêu của bài lab này là giúp sinh viên làm quen với việc phát hiện tin trong ảnh được giấu bằng phương pháp hoán vị giả ngẫu nhiên thông qua các kỹ thuật Forensic liên quan đến ảnh và luyện tập lại việc tách tin ra khỏi ảnh. Sau khi hoàn thành bài lab, sinh viên sẽ hiểu sâu hơn về cách giấu một số thông tin liên quan vào ảnh ngoài việc giấu thông điệp vào ma trận điểm ảnh và thuần thục hơn về việc tách tin trong ảnh được giấu bằng phương pháp hoán vị giả ngẫu nhiên.

2. Yêu cầu đối với sinh viên

- Sinh viên đã thực hiện bài lab stego-image-basic-code-hvgnn1 và stego-image-basic-code-hvgnn2.

- Sinh viên nắm được kiến thức về ngôn ngữ Python, câu lệnh scp và hệ điều hành Linux.

- Sinh viên nắm được một số câu lệnh trong lĩnh vực Forensic liên quan đến ảnh của trò chơi CTF.

- Sinh viên nắm được những kiến thức cơ bản về giấu và tách tin trong ảnh và phương pháp hoán vị giả ngẫu nhiên, bộ sinh số giả ngẫu nhiên (PRNG), thuật toán Blum-Blum-Shub.

3. Tải file bài lab và file hướng dẫn thực hành

- Tải thư mục chứa file bài lab và file hướng dẫn thực hành về bằng câu lệnh sau:

git clone https://github.com/vuducmanh2003/stego-image-detect-tool-hvgnn

- Chuyển đường dẫn đến thư mục:

cd ~/labtainer/labtainer-student

- Giải nén và chuyển file bài lab vào thư mục /home/trunk/labs bằng câu lệnh sau:

imodule file:///home/student/<đường dẫn chứa thư mục vừa tải về>/stego-image-detect-tool-hvgnn/imodule.tar

- Giả sử thư mục Downloads chứa thư mục vừa tải về:

imodule file:///home/student/Downloads/stego-image-detect-tool-hvgnn/imodule.tar

4. Nội dung thực hành

- Trong terminal của Labainer, chạy lệnh sau để khởi động bài lab:

labtainer stego-image-detect-tool-hvgnn

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

- Bài lab có 3 terminal là *alice*, *bob* và *remote*. Sau khi khởi động bài lab thành công, có 2 terminal *alice* và *bob* hiện ra. Hãy xem các file có trong đường dẫn hiện tại bằng câu lệnh *ls*. Trên terminal *alice* có 1 file .png. Trên terminal *bob* có 1 file .txt.

- Hãy xem IP 2 terminal *alice* và *bob* bằng câu lệnh *ifconfig*.

- Trong bài lab này, sinh viên sẽ thực hiện phát hiện những điểm kỳ lạ trong ảnh đã giấu thông điệp mà Alice gửi cho Bob, giải mã thông điệp và truy cập đến terminal *remote* và đọc file có trên đó. Sau đây là những nhiệm vụ của bài lab:

4.1. Nhiệm vụ 1: Alice chuyển file ảnh chứa thông điệp đã giấu sang cho Bob

- Trong phương pháp hoán vị giả ngẫu nhiên, người gửi giấu thông điệp vào ảnh và gửi ảnh đã giấu thông điệp qua kênh truyền cho người nhận. Người gửi và người nhận phải thống nhất với nhau về thuật toán sinh số giả ngẫu nhiên để có thể thực hiện giấu và tách tin được.

- Thông điệp trong bài lab này là mật khẩu của terminal *remote.* Alice đã giấu thông điệp vào ma trận điểm ảnh, giấu số lượng vị trí của các bit thông điệp trong chuỗi nhị phân từ ma trận điểm ảnh và thuật toán sinh số giả ngẫu nhiên vào ảnh trước truyền cho Bob.

- Alice thực hiện chuyển file ảnh chứa thông điệp đã giấu sang cho Bob:

scp stegano_image.png ubuntu@<IP bob>:/home/ubuntu/

(Nhập "yes" và mật khẩu của terminal *bob* là ubuntu).

- Trên terminal *bob* kiểm tra các file đã nhận được bằng câu lệnh *ls*.

4.2. Nhiệm vụ 2: Bob phát hiện Alice đã giấu thông điệp vào ảnh bằng phương pháp hoán vị giả ngẫu nhiên

- Sinh viên hãy dùng những câu lệnh như *file*, *strings*, *exiftool*, *binwalk* để phát hiện ra những điểm kỳ lạ trong ảnh mà Alice gửi. Sau đó hãy ghi những điểm kỳ lạ phát hiện được vào file strange.txt.

- Sau đó, sinh viên hãy giải mã điểm kỳ lạ trong ảnh mà Alice gửi bằng câu lệnh *binwalk* cùng tham số của lệnh đó (gợi ý: sinh viên sẽ phải tìm ra 1 file mà trong file đó chứa

thuật toán sinh số giả ngẫu nhiên). Sau khi tìm được file đó hãy đọc nội dung trong file bằng câu lệnh *abiword*.

4.3. Nhiệm vụ 3: Bob tách thông điệp ra khỏi ảnh mà Alice gửi

- Sinh viên hãy hoàn thành phần còn thiếu trong file vừa tìm được và chuyển nội dung đó vào file blum_blum_shub.py và chạy file đó để in ra danh sách các vị trí của các bit thông điệp trong chuỗi nhị phân từ ma trận điểm ảnh và số lượng vị trí.

- Sinh viên hãy viết đoạn mã python trong file extract_message.py và chạy file đó để tách thông điệp dạng nhị phân ra khỏi ảnh mà Alice gửi với đầu vào là ảnh được giấu thông điệp cùng với danh sách các vị trí vừa in ra được và đầu ra là thông điệp ở dạng nhị phân và văn bản. Thông điệp ở dạng văn bản chính là mật khẩu của terminal *remote*.

4.4. Nhiệm vụ 4: Bob truy cập đến terminal remote và đọc file có trên đó

- Sau khi có được mật khẩu của terminal root, sinh viên hãy truy cập vào terminal *remote* từ terminal *bob*:

ssh 172.30.0.10

(Nhập "yes" và mật khẩu của terminal *remote* là thông điệp tách được từ ảnh mà Alice gửi).

- Sau đó hãy đọc file có trên đó.

5. Kiểm tra và kết thúc bài lab

- Trong quá trình làm bài, sinh viên thực hiện kiểm tra kết quả bài lab bằng câu lệnh:

checkwork

- Sau khi hoàn thành bài lab, sinh viên thực hiện kết thúc bài lab bằng câu lệnh:

stoplap

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

labtainer -r stego-image-detect-tool-hvgnn