# Bài thực hành: Giấu tin trong trường định danh IPv4 bằng covert_tcp

## 1. Khái quát chung

### 1.1. Tổng quan

Bài lab này giúp sinh viên tìm hiểu một kỹ thuật giấu tin trong mạng dựa trên trường Identification (ID) của gói tin IPv4 bằng công cụ **covert_tcp**. Đây là một tool mã nguồn mở được phát triển để thực hiện giấu tin nhằm mục đích học tập, nghiên cứu.

### 1.2. Nguyên lý giấu tin

- Trường IP ID (Identification) trong header IPv4 có độ dài 16 bit, thường được sử dụng để nhận diện và tái lắp ráp các gói tin bị phân mảnh.
- Trong kỹ thuật giấu tin này, **covert_tcp** mã hóa từng byte của thông điệp cần giấu trực tiếp vào giá trị IP ID của gói tin TCP trước khi gửi đi.
- Mỗi byte của file được gán vào IP ID, và một gói tin đặc biệt với IP ID = 0 được gửi để báo hiệu kết thúc.

### 1.3. Mục tiêu của bài lab

- Hiểu được cách giấu tin trong header gói tin IPv4 bằng cách sử dụng trường Identification với công cụ **covert_tcp**.
- Thực hành gửi và nhận file bí mật giữa hai máy tính trong môi trường Labtainers.
- Kiểm tra và xác nhận quá trình truyền dữ liệu giấu tin thông qua file nhận được.

### 1.4. Yêu cầu đối với sinh viên

- Sinh viên đã có kiến thức về giấu tin trong mạng, hiểu về cấu trúc gói tin IP và trường ID của tiêu đề IP.
- Có kiến thức cơ bản về hệ điều hành Linux.

## 2. Chuẩn bị môi trường thực hành

Mở terminal, trong thư mục labtainer-student, bắt đầu bài thực hành bằng lệnh:

*labtainer -r stego-tool-identification_ipv4*

*(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)*

Kiểm tra các bài tập phải làm trong bài thực hành

*Checkwork*

## 3. Nội dung thực hành

### 3.1. Chuẩn bị môi trường

Trên terminal của máy sender sinh viên thực hiện lệnh biên dịch:

*gcc -o covert_tcp covert_tcp.c*

Thực hiện tạo thông điệp bí mật chứa trong file *message.txt*. Ví dụ:

*echo "this is secret" > message.txt*

hoặc có thể thể dụng **nano, vim** để mở trình soạn thảo văn bản rồi nhập thông điệp bí mật vào đó.

### 3.2. Chạy chương trình giấu tin và gửi gói tin.

Trên terminal máy **receiver**, chạy lệnh sau để bắt đầu lắng nghe gói tin:

*sudo ./covert_tcp -source 172.20.0.2 -source_port 7777 -file received.txt -server -ipid*

Trên terminal máy **sender**, chạy lệnh sau để gửi file *message.txt*:

*sudo ./covert_tcp -dest 172.20.0.3 -source 172.20.0.2 -dest_port 7777 -source_port 1234 -file message.txt -ipid*

- ***Lưu ý***: Chạy phía **receiver** trước, sau đó mới chạy bên **sender** để đảm bảo **receiver** sẵn sàng nhận dữ liệu tránh mất mát giữ liệu.

Kết quả mong đợi: **Receiver** sẽ hiển thị các dòng Receiving Data: tương ứng với mỗi byte. Nhấn **Ctrl + C** để thoát.

### 3.3. Giải mã và xác nhận thông điệp bí mật

Sau khi bên phía **sender** gửi xong, kiểm tra file *received.txt* trên máy **receiver**:

*cat received.txt*

- Kết quả mong đợi: Nội dung file *received.txt* phải giống với *message.txt*.

## 4. Kết thúc bài lab

- **Kết thúc bài lab:**
    - Kiểm tra checkwork:

      *checkwork*

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

      *stoplab*

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

      *labtainer -r stego-tool-identification_ipv4*