**Labtainer 4: Phát hiện giấu tin qua cơ chế phát lại (Retranmission Stenography) sử dụng công cụ**

1. **Mục đích**

* Bài thực hành này giúp sinh viên nắm bắt được công cụ, cách cấu hình gói tin và cơ chế phát lại, đồng thời biết cách sử dụng công cụ để phát hiện giấu tin.
  + Hiểu được cơ chế giấu tin (qua PDUs và qua mã hóa)

1. **Nội dung lý thuyết**

* Tìm hiểu về công cụ scapy, cách sử dụng công cụ scapy để tiến hành cấu hình gói tin
* Tìm hiểu về cấu trúc của gói tin IP, TCP.
* Làm các bài Labtainer 1, 2, 3

1. **Các bước thực hiện**
   1. **Khởi động bài lab**
      1. **Các bước cần thực hiện**

* Bước 1: Tại **Terminal** của **labtainer** gõ lệnh

`labtainer -r stego-net-rsteg-detect-tool`

* 1. **Tiến hành sử dụng công cụ để lắng nghe và phân giải gói tin với cách giấu tin dùng PDUs**
* Bước 1: Tại **Terminal** của máy ‘**attacker’** gõ lệnh `**start\_detect.sh**`, sau đó nhập vào lần lượt các thông tin
  + Enter target IP: nhập IP của máy client
  + Enter your IP: nhập IP của attacker
* Bước 2: Tại **Terminal** của máy ‘**client’** chạy lệnh để bắt đầu gửi đi các gói tin, bằng lệnh:

`client\_sender.sh`

* + Enter source IP:
  + Enter destination IP:
* Bước 3: Quan sát kết quả công cụ quét được, sẽ có thông được được ẩn dấu trong đó, sau đó hãy chạy tệp chấm kết quả bằng lệnh:

`check\_result.py`

* + Result: Nhập chuỗi thông điệp mà các bạn quan sát được
* **Lưu ý**: Với nhiệm vụ này các thông điệp nằm rải rác qua các gói tin, vậy nên hãy phân tích các kết quả và ghép lại. Cú pháp thông điệp, các từ có nghĩa viết liền, giữa các từ sẽ có khoảng trắng:
  + Ví dụ: “**Kill me**”, đừng viết thành “K i l l m e” hay “Killme”, như vậy tệp chấm sẽ không cho kết quả đúng. Lưu ý cả chữ hoa, chữ thường cho đúng.
  1. **Tiến hành sử dụng công cụ để lắng nghe và phân giải gói tin với cách giấu tin dùng PDUs**
* Bước 1: Tại **Terminal** của **Attacker**, nhấn tổ hợp “**Ctrl + C**” để thoát khỏi công cụ. Sau đó chạy lại công cụ
* Bước 2: Tại **Terminal** của **Client**, chạy tệp để gửi gói tin với kiểu mã hóa bằng lệnh:

`client\_sender\_encrypt.sh`

* + Enter source IP:
  + Enter destination IP
* Bước 3: Tương tự như 3.2 tiến hành phân tích và chạy tệp để kiểm tra kết quả
* **Lưu ý**: Nhiệm vụ này thông điệp sẽ chỉ nằm ở 1 gói duy nhất, vậy nên cần phân tích chi tiết 1 gói để tìm thấy đủ chuỗi trong thông điệp, và nhiệm vụ này sẽ có nhiều hơn 1 thông điệp.
  1. **Kết thúc bài lab**

1. Gõ lệnh **`stoplab**` để kết thúc bài lab