**Labtainer 3: 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, bao gồm:
  + Sử dụng **scapy** để cấu hình và giấu gói tin
  + Sử dụng **wireshark** để bắt và phân tích gói tin mạng

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.

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-basic-tool`

* Bước 2: Tại **Terminal** của máy ‘**server’** gõ lệnh `**server\_receiver.sh**`, sau đó nhập vào lần lượt các thông tin
  + IP của máy server (máy nhận gói tin)
  + IP của máy client ( máy gửi gói tin đến)
  + Vị trí thông điệp mà hai bên thỏa thuận khi nhận được gói tin chứa thông điệp server sẽ trích xuất từ vị trí này
  1. **Tiến hành chạy công cụ để thiết lập kết nối**
* Bước 1: Tại **Terminal** của máy ‘**client’** tiến hành chạy công cụ để bắt tay 3 bước và tiến hành kết nối bằng cách gõ lệnh:

`sudo python3 client\_sender.py -s <IP của client> -d <IP của server> -ha`

* Quá trình kết nối sẽ thành công nếu như bên phía server có thông báo: “**Hand-shake process success**”
  1. Tiến hành chạy công cụ để phát tín hiệu rsteg
* Bước 1: Tại **Terminal** của máy ‘**client’** tiến hành chạy công cụ để phát tín hiệu rsteg, bằng cách gõ lệnh

`sudo python3 client\_sender.py -s <IP của client> -d <IP của server> -rs`

* Quá trình gửi gói tin phát tín hiệu sẽ thành công nếu như bên phía server có thông báo: “**Found RSTEG Signal**”
  1. Tiến hành chạy công cụ để gửi thông điệp giấu trong gói tin
* Bước 1: Tại **Terminal** của máy ‘**client’** tiến hành chạy công cụ để gửi thông điệp bằng lệnh:

`sudo python3 client\_sender.py -s <IP của client> -d <IP của server> -st <thông điệp> -p <vị trí mà sinh viên quy định với server>`

* Bước 2: Dựa vào bước 1 để gửi đi thông điệp “**I <3 PtIT**”
* Quá trình gửi thông điệp sẽ thành công nếu phía server có thông báo: “**Extracted Message: I <3 PtIT**”
  1. **Kết thúc bài lab**
* Gõ lệnh **`stoplab**` để kết thúc bài lab