TCP_covert

- Khởi động bài lab:
    - Vào terminal, gõ:

Labtainer -r ptit-covert-tcp

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

Sau khi khởi động xong hai terminal ảo sẽ xuất hiện, mỗi một rerminal sẽ có hai tab, một cái là đại diện cho máy gửi: ***send***, một cái là đại diện cho máy nhận: ***receive.*** Biết rằng 2 máy nằm cùng mạng LAN.

- Trên terminal ***send , receive*** sử dụng lệnh "ifconfig", xác định địa chỉ IP và địa chỉ mạng LAN.

- Thêm vào file message.txt được tạo sẵn chuỗi: "Secret Message!"
  (Lưu ý, không xóa mã băm được tạo sẵn)
- Config máy receive
    - Sử dụng quyền sudo và mở tcpdump để theo dõi

tcpdump -nvvX port 8888 -i lo

    - Mở terminal thứ hai Lưu ý: Trường hợp gặp lỗi về cc lệnh, hãy cài đặt trình biên dịch: sudo apt install gcc
      Biên dịch file Convert_tcp.c

cc -o covert_tcp covert_tcp.c

    - Thiết lập thiết lập trình nghe
        - Source_port using port 9999
        - Dest_port using port 8888
        - Receive.txt cần điền đầy đủ đường dẫn tạo ra file

./covert_tcp -dest <ip máy receive >-source <ip máy send>-source_port <port>-dest_port <port> -server -file /receive.txt

- Config máy send
    - Biên dịch file Convert_tcp.c
    - Mở wireshark

- Thiết lập trình gửi bở tab thứ hai
  - Port cần config ngược lại so với máy receive
  - Message.txt cần điền đường dẫn đến file thực tế

./covert_tcp -dest <ip máy receive>-source <ip máy send>-source_port <>-dest_port <>-file /message.txt

- Trên máy send
  - Trên máy send dừng tcpdump Tcpdump cho thấy không có gói nào bị bắt trong mạng.
  - Sử dụng ls kiểm tra các file đã tạo ra, và cat file để kiểm tra nội dung
- Trên máy receive Mở wireshark
  - Search các gói tin tcp theo dõi kiểm tra giao tiếp giữa 2 máy send và receive. Quan sát để thấy từng ký tự của chuỗi tin nhắn được gửi dưới dạng các gói riêng lẻ
  - Covert_tcp thay đổi tiêu đề của gói TCP và thay thế nó bằng các ký tự của chuỗi từng ký tự một để gửi tin nhắn mà không bị phát hiện.
- Kiểm tra kết quả bằng lệnh :

Checkwork

- Dừng bài lab

Stop lab