Labtainer 1: Giấu tin qua cơ chế truyền lại (Retransmission Stegna), sử dụng phương pháp thủ công

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

2. 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.
- Tìm hiểu về cách tính toán các dữ liệu bên trong gói tin như dữ liệu(payload), thứ tự (sequence), tín hiệu nhận (acknowledge), v.v

3. Các bước thực hiện

3.1. Khởi động bài lab

3.1.1. Các bước cần thực hiện

- Bước 1: Tại Terminal của labtainer gõ lệnh **`labtainer -r manual-rsteg`**.
- Bước 2: Tại Terminal của máy **'server'** gõ lệnh **`start_server.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)

3.1.2. Kết quả cần đạt

- Server hiển thị '**Start to listen packet from client...**'.

3.2. Gửi cờ SYN để thiết lập bước đầu quá trình bắt tay Hand-Shake

3.2.1. Các bước thực hiện

- Bước 1: Tại máy '**client'** gõ lệnh **`sudo scapy`** để khởi động trình chỉnh sửa gói tin
- Bước 2: Dựa vào kiến thức đã tìm hiểu thiết lập một gói tin đơn giản, cú pháp sẽ có dạng như sau
    - `(tên biên 1) = IP()`
    - `(tên biến 2) = TCP()`
    - `(tên gói tin) = (tên biến 1) / (tên biến 2)
- Ví dụ:
    - My_ip = IP()
    - My_tcp = TCP()
    - My_packet = My_ip / My_tcp
- Bước 3: Dựa vào kiến thức đã tìm hiểu thiết lập cờ (flags) **SYN** cho gói tin để tiến hành bước đầu cho quá trình Hand-shake. Sau đó gõ lệnh **`send(tên gói tin)`**.

3.2.2. Kết quả cần đạt

- Server sẽ hiển thị '**First step hand-shake success'** nếu quá trình bắt tay bước đầu thành công

3.3. Gửi cờ ACK để hoàn thành quá trình Hand-shake

3.3.1. Các bước thực hiện

- Bước 1: Sau khi đã hoàn thành bước đầu quá trình Hand-shake, thiết lập cờ (flags) **ACK** cho gói tin.
- Bước 2: Dựa vào kiến thức đã tìm hiểu cần tính toán lại trường thứ tự **(seq)** cho gói tin sao cho phù hợp.
- Bước 3: Chạy lệnh **`send(tên gói tin)`** để gửi gói tin.

3.3.2. Kết quả cần đạt

- Server sẽ hiển thị '**Hand-shake process success'** nếu quá trình Hand-shake thành công
- **Lưu ý**: Nếu một trong các bước 1 và 2 bị sai sẽ phải quay lại bước 3.2 để thực hiện lại, và số lần sinh viên tính toán sai trường seq phải < 3, nếu sai quá 2 lần sẽ phải làm lại cả bài lab.

3.4. Cấu hình và tiền xử lí phần dữ liệu cho gói tin

3.4.1. Các bước thực hiện

- Bước 1: Sử dụng '**scapy**' để cấu hình thêm phần dữ liệu cho gói tin. Cú pháp sẽ có dạng như sau:
  - `(tên biên 1) = IP()`
  - `(tên biến 2) = TCP()`
  - `(tên biến 3) = Raw(load='Phần dữ liệu')
  - `(tên gói tin) = (tên biến 1) / (tên biến 2) / (tên biến 3)
- Bước 2: Gõ lệnh **`send (tên gói tin)`** để tiến hành gửi gói tin đi và quan sát kết quả trả về phía bên Server.
- Bước 3: Tại Terminal thứ 2 của client gõ '**wireshark'** để khởi động trình bắt gói tin. Trong phần lọc của gói tin sử dụng cú pháp để lọc như sau **`ip.addr == (IP của máy client) && tcp.flags.rst != 0`**
- Bước 4: Cấu hình lại phần định dạng của dữ liệu theo cú pháp **`(tên gói tin).load=b'\x00\x00\x00\x00\x00(phần dữ liệu)`**, sau đó gửi gói tin. Đồng thời quan sát trên wireshark phần thông tin của gói tin vừa rồi. Nếu như để ý sinh viên sẽ thấy ký tự **'\x00'** sẽ tương đương với ký tự '**.**', điều mà sẽ giúp ẩn giấu đi phần ký tự sau này.

3.4.2. Kết quả cần đạt

- Server sẽ hiển thị '**Payload: (phần dữ liệu mà sinh viên đã cấu hình)**'
- **Lưu ý**: Dựa vào kiến thức đã học sinh viên cần tính toán trường '**seq'** của gói tin, đặc biệt là khi gói tin có thêm phần dữ liệu.
- **Mẹo**: Với '**wireshark'**, hãy tìm đến phần hiển thị thông tin chi tiết và để ý đến 2 giá trị '**sequence raw'** và '**acknowledge raw'**.

3.5. Thực hành quá trình giấu tin

3.5.1. Các bước thực hiện

- Bước 1: Dựa vào kiến thức đã tìm hiểu, hãy cấu hình gói tin và bật cờ (flags) của gói tin IP, với tín hiệu cho việc giấu gói tin là cờ **Don't Fragment** được bật
- Bước 2: Cấu hình lại phần định dạng dữ liệu theo cú pháp
- **`(tên gói).load=b"\x00\x00\x00(ký tự cần giấu)\x00\x00\x00(\x00 có thể dài tùy theo sinh viên)(phần dữ liệu)"`,** sau đó gửi gói tin
- Bước 3: Cấu hình lại gói tin và bật cờ (flags) về tín hiệu 0. Sau đó gửi gói tin. Kết thúc quá trình giấu và quan sát kết quả bên server

3.5.2. Kết quả cần đạt

- Server sẽ hiển thị '**Extracted Mess: (phần ký tự mà sinh viên đã giấu**)'
- **Lưu ý**: Ký tự cần giấu phải nằm ở ký tự thứ tư của phần dữ liệu.

3.6. Thực hiện giấu tin với thông điệp cần giấu là `Hi!`

3.6.1. Các bước thực hiện

- Sinh viên dựa vào phần 3.5 để thực hiện.

3.6.2. Kết quả cần đạt

- Server sẽ hiển thị '**Extracted Mess: Hi!**'

3.7. Kết thúc quá trình kết nối với Server

3.7.1. Các bước thực hiện

- Bước 1: Hoàn thành đầy đủ các bước từ 3.1 đến 3.6
- Bước 2: Dựa vào kiến thức đã tìm hiểu, hãy cấu hình gói tin và bật cờ (flags) **FIN** của tói tin TCP. Và sau đó gửi gói tin

3.7.2. Kết quả cần đạt

- Server sẽ hiện thị `**Your connection is canceled, seê ju later <._.>**`

3.8. Kết thúc bài lab

- Gõ lệnh `**stoplab**` để kết thúc bài lab