Labtainer 2: Phát hiện giấu tin trong cơ chế truyền lại

Mục lục

[**1.** **Mục đích** 2](#_Toc197542859)

[**2.** **Nội dung lý thuyết** 2](#_Toc197542860)

[**3.** **Các bước thực hiện** 2](#_Toc197542861)

[**3.1.** **Khởi động bài lab** 2](#_Toc197542862)

[**3.2.** **Tìm kiếm gói tin phát tín hiệu (RSTEG\_SIGNAL) cơ bản** 2](#_Toc197542863)

[**3.3.** **Tìm kiếm gói tin chứa thông điệp (STEG\_MESS) cơ bản** 3](#_Toc197542864)

[**3.4.** **Tìm ra thông điệp cơ bản** 3](#_Toc197542865)

[**3.5.** **Tìm kiếm gói tin phát tín hiệu(RSTEG\_SIGNAL) có dùng hàm băm** 4](#_Toc197542866)

[**3.6.** **Tìm kiếm gói chứa thông điệp(STEG\_MESS) có sử dụng hàm băm:** 5](#_Toc197542867)

[**3.7.** **Tìm thông điệp có sử dụng mã hóa** 5](#_Toc197542868)

[**3.8.** **Kết thúc bài lab** 5](#_Toc197542869)

1. **Mục đích**

* Bài thực hành giúp sinh viên nắm được các thức phát hiện việc giấu tin qua cơ chế truyền lại, sử dụng các công cụ để phân tích như Wireshark

1. **Nội dung lý thuyết**

* Tìm hiểu về gửi đi tín hiệu giấu tin sử dụng hàm băm
* Tìm hiểu cấu trúc, cách tính toán trường của gói tin IP(IP packet), phân đoạn TCP(TCP Segment).

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

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

`labtainer stego-net-rsteg-detect-code`

* 1. **Tìm kiếm gói tin phát tín hiệu (RSTEG\_SIGNAL) cơ bản**
* Bước 1: Tại **Terminal** của máy **server** khởi chạy hệ thống để lắng nghe các lưu lượng từ máy client bằng lệnh:

`server\_receiver.sh`

* + Sau đó dựa theo hướng dẫn để gõ vào địa chỉ IP của máy nguồn và máy đích.
* Bước 2: Tải **Terminal** của máy **client** khởi động **wireshark** nhằm lắng nghe gói tin, bằng lệnh

`wireshark`

* Bước 3: Bài lab đã được cài đặt lệnh để gửi hàng loạt các gói yêu cầu đến máy server, bao gồm cả gói tin tín hiệu và gói tin chứa thông điệp, tại **Terminal** của máy **client** chạy tệp lệnh đó bằng cách gõ:

`client\_sender.sh`

* Bước 4: Nhiệm vụ của sinh viên là thông qua **wireshark** phân tích nhằm tìm ra gói tin phát tín hiệu, gói tin chứa thông điệp và tìm ra thông điệp.
* Bước 5: Khi tìm được gói tin phát tín hiệu, để kiểm tra gói tin sinh viên đã tìm là đúng, gõ lệnh:

`check\_result.sh`

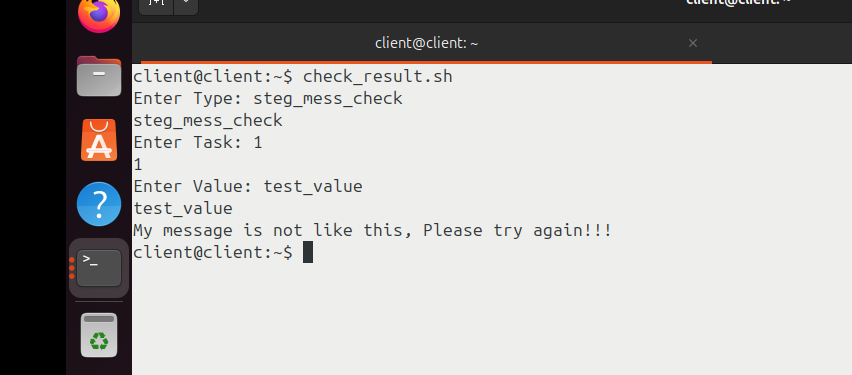
* Bước 6: Sau khi chạy lệnh cần nhập vào các giá trị tương ứng sau:
  + Type: Nhập “**rsteg\_signal\_seq\_check**”
  + Task: Nhập “**1**”
  + Value: Nhập **<sequence của gói tin mà sinh viên cho là chứa tín hiệu thông báo>**
* Ví dụ về cách dùng xin xem qua Hình 1
* Gói tin mà sinh viên tìm sẽ đúng là gói phát tín hiệu khi kết quả trả về chứa chuỗi “**correct rsteg\_signal packet**”.
* **Lưu ý**: Khi nhập giá trị thì nhập giá trị trong đoạn dấu ngoặc kép, đừng nhập tất cả
* Gói tin chứa tín hiệu là gói tin mà báo hiệu cho bên nhận biết bên gửi chuẩn bị gửi gói tin có chứa thông điệp. Các sinh viên cần lưu ý để phân biệt với gói tin chứa thông điệp, gói tin chứa thông điệp sẽ được gửi sau khi đã gửi gói chứa tín hiệu. Trong phần **checkwork** sẽ chấm theo thứ tự các bạn hoàn thành nhiệm vụ, nếu hoàn thành nhiệm vụ tìm gói chứa thông điệp trước sẽ không hợp lệ, phải hoàn thành theo thứ tự.
* **Mẹo**: Hãy chú ý đến phần **payload** của các gói tin.
  1. **Tìm kiếm gói tin chứa thông điệp (STEG\_MESS) cơ bản**
* Bước 1: Sử dụng **wireshark** để phân tích tìm ra gói tin chứa thông điệp
* **Lưu ý**: Gói tin chứa thông điệp ứng với 1 gói tin phát tín hiệu sẽ có 4 gói, và các thông điệp sẽ nằm rải rác trong gói tin chứa thông điệp. Sinh viên cần nắm rõ cách tính **sequence** nhằm tìm ra đủ 4 gói và ghép các ký tự để tạo thành thông điệp bí mật.
* Bước 2: Sau khi tìm được gói tin chứa thông điệp, cần chạy tệp như 3.2 để kiểm tra kết quả

`check\_result.sh`

* + Type: Nhập “**steg\_mess\_seq\_check**”
  + Task: Nhập “**1**”
  + Value: Nhập **<seq mà sinh viên nghĩ là của gói tin chứa thông điệp>**
* Gói tin mà sinh viên tìm sẽ đúng là gói chứa thông điệp khi kết quả trả về chứa chuỗi “**correct steg\_mess packet**”.
* **Lưu ý**: với giá trị **Value**, 1 gói phát tín hiệu tương ứng 4 gói chứa thông điệp, thì khi sinh viên nhập giá trị **Value** cần nhập seq của 1 trong 3 gói cuối, bỏ qua 1 gói đầu vì gói đầu sẽ có seq trùng với gói phát tín hiệu bởi gói phát tín hiệu sẽ cố ý kích hoạt cơ chế phát lại.
  1. **Tìm ra thông điệp cơ bản**
* Dựa vào việc phân tích gói chứa thông điệp tại 3.3, tìm ra đủ 4 gói chứa thông điệp
* Bước 2: Chạy tệp để kiểm tra kết quả

`check\_result.sh`

* + Type: Nhập “**steg\_mess\_check**”
  + Task: Nhập “**1**”
  + Value: **<chuỗi thông điệp>**
* Chuỗi thông điệp sẽ đúng khi kết quả trả về chứa chuỗi “**my message seems leaked**”
* Ví dụ về cách dùng tệp:



1. – Ví dụ về cách dùng lệnh để kiểm tra
   1. **Tìm kiếm gói tin phát tín hiệu(RSTEG\_SIGNAL) có dùng hàm băm**

* Bước 1: Tại **Terminal** của máy **server** khởi chạy hệ thống để lắng nghe các lưu lượng từ máy client bằng lệnh:

`**server\_receiver\_encrypt.sh`**

* + Sau đó dựa theo hướng dẫn để gõ vào địa chỉ IP của máy nguồn và máy đích.
* Bước 3: Bài lab đã được cài đặt tệp tin để gửi hàng loạt các gói yêu cầu đến máy **server**, bao gồm cả gói tin tín hiệu và gói tin chứa thông điệp, tại **Terminal** của máy **client** chạy tệp lệnh đó bằng cách gõ:

`client\_sender\_encrypt.sh`

* Bước 4: Nhiệm vụ của bạn là thông qua **wireshark** phân tích nhằm tìm ra gói tin phát tín hiệu, gói tin chứa thông điệp và tìm ra thông điệp.
* Bước 5: Khi tìm được gói tin phát tín hiệu, để kiểm tra gói tin sinh viên đã tìm đúng hay chưa, gõ lệnh:

`check\_result.sh`

* Bước 6: Sau khi chạy lệnh cần nhập vào các giá trị tương ứng sau:
  + Type: Nhập “**rsteg\_signal\_seq\_check**”
  + Task: Nhập “**2**”
  + Value: Nhập **<sequence của gói tin mà sinh viên cho là chứa tín hiệu thông báo>**
* **Lưu ý**: Để phát hiện được gói nào phát tín hiệu cần dựa vào công thức sau:

`mã\_băm = SHA256(<sequence của gói phát tín hiệu> + <checksum của gói phát tín hiệu> + 0`

* + Với ‘**+**’ chính là phép nối liền
* Để giúp quá trình tìm kiếm dễ hơn, hãy chú ý tìm điểm khác biệt giữa gói tín phát tín hiệu và gói tin bị lost thông thường.
* Trong trường hợp không thể phát hiện điểm bất thường sinh viên cần tính toán lại giá trị mã băm và so sánh mã băm sinh viên tính được với mã băm trong phần payload của gói tin bắt được để biết gói nào là gói phát tín hiệu. Cách này có một điểm lưu ý là giá trị **checksum** gửi đi và **checksum** mà bắt được bằng **wireshark** là không giống nhau. Để hiểu hơn về lí do hãy xem xét đoạn dưới đây:
  + Để A gửi gói tin tín hiệu cho B, A tính **mã\_băm** theo như công thức ở trên với **check\_sum** là “**123**”
  + A chèn giá trị băm vào payload -> **check\_sum** thay đổi thành “**abc**” do gói tin đã có sự thay đổi.
  + B bắt gói tin và thấy **check\_sum** = “**abc**”
  + Nếu B tính mã\_băm với **check\_sum** bắt được thì **`mã\_băm(B tính) != mã\_băm(A tính)`** vì **check\_sum** do A dùng luôn khác với **check\_sum** do B dùng để tạo mã băm.
* Gói tin mà sinh viên tìm sẽ đúng là gói phát tín hiệu khi kết quả trả về chứa chuỗi “**correct rsteg\_signal packet**”.
  1. **Tìm kiếm gói chứa thông điệp(STEG\_MESS) có sử dụng hàm băm:**
* Bước 1: Phân tích gói tin. Cách cài đặt với nhiệm vụ này cũng tương tự như **3.3**. Mỗi gói tin phát tín hiệu đều chứa 4 gói chứa thông điệp.
* Bước 2: Để kiểm tra tiến hành chạy tệp kiểm tra

`check\_result.sh`

* + Type: Nhập “**steg\_mess\_seq\_check**”
  + Task: Nhập “**2**”
  + Value: Nhập **<seq của gói tin chứa thông điệp>**
* **Lưu ý**: Tương tự như phần cơ bản, hãy chỉ nhập sequence của 1 trong 3 gói tin sau.
  1. **Tìm thông điệp có sử dụng mã hóa**
* Bước 1: Dựa vào phân tích hãy tìm ra 4 gói tin chứa thông điệp
* Bước 2: Chạy lệnh để kiểm tra

`check\_result.sh`

* + Type: Nhập “**steg\_mess\_check**”
  + Task: Nhập “**2**”
  + Value: Nhập **<chuỗi thông điệp**
  1. **Kết thúc bài lab**
* Tại Terminal của labtainer, hõ lệnh **`stoplab**` để kết thúc bài lab