BÁO CÁO THỰC HÀNH

**Môn học: Nhập môn mạng máy tính**

**Buổi báo cáo: Lab 01**

**Tên chủ đề: Làm quen với Wireshark**

*GVHD: Phan Trung Phát*

*Ngày thực hiện: 22/09/2022*

*Ngày nộp báo cáo: 05/10/2022*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: IT005.N11.KHTN.1

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Trương Thanh Minh | 21520064 | 21520064@gm.uit.edu.vn |

1. **ĐÁNH GIÁ KHÁC:**

|  |  |
| --- | --- |
| **Nội dung** | **Kết quả** |
| Tổng thời gian thực hiện bài thực hành trung bình | 2 tuần |
| Link Video thực hiện  *(nếu có)* |  |
| Ý kiến *(nếu có)*  + Khó khăn  + Đề xuất … |  |
| Điểm tự đánh giá | 9.5 |

**Phần bên dưới của báo cáo này là báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

---

1. Mở đầu về mạng máy tính

Mục tiêu và kiến thức sau khi hoàn thành môn học Nhập môn Mạng máy tính:

* Nắm được kiến thức tổng quan về mạng.
* Biết được kiến thức cơ bản về các tầng mạng, các giao thức mạng.
* Vận dụng kiến thức đã học để biết được cách thực hiện một số cuộc tấn công và tránh khỏi các cuộc tấn công mạng.

1. Làm quen với Wireshark và thửu nghiệm bắt gói tin trong mạng
2. Tổng thời gian bắt gói tin trong từng trang web thử nghiệm và tổng số gói tin bắt được

* Ở website thứ nhất ([gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html](http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html)):

A picture containing text

Description automatically generated

Hình : Bắt gói tin ở trang web đầu tiên

* Đầu tiên, ta lọc các gói tin vừa bắt được với địa chỉ IP của web (128.119.245.12)

Thời gian thử nghiệm: t = 1.423210 – 0.227256 = 1.195954(s).

* Số gói tin bắt được là 16 (gói tin).
* Ở website thứ hai ([Cổng thông tin đào tạo | Trường Đại Học Công Nghệ Thông Tin (uit.edu.vn)](https://daa.uit.edu.vn/)):

A picture containing table

Description automatically generated

Hình : Những gói tin đầu tin bắt được ở web thứ hai

Table

Description automatically generated

Hình 3: Những gói tin cuối cùng ở web thứ 2

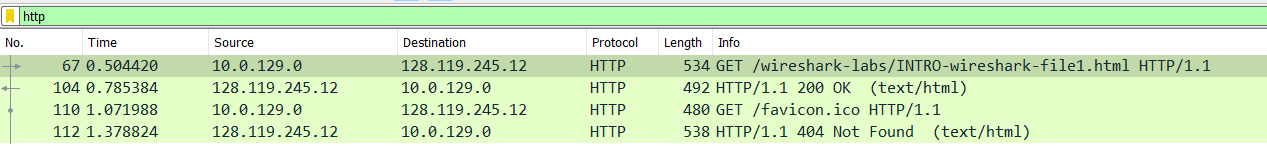
* Tương tự ở website thứ nhất, ở bước đầu tiên, ta cũng lọc lại các gói tin bắt được bằng IP của website đó (45.122.249.78)

Thời gian thử nghiệm là: t = 4.105474 – 1.700630 = 2.404844 (s).

* Số gói tin bắt được là 80 (gói tin).

1. 5 giao thức khác nhau xuất hiện trong cột giao thức (Protocol)
   * TCP (Transmission Control Protocol): Giao thức này có nhiệm vụ chia nhỏ dữ liệu ra thành các gói để truyền dữ liệu đi. Thiết lập các kết nối giữa các máy tính đảm bảo việc truyền dữ liệu thành công.
   * HTTP (HyperText Transfer Protocol): Cho phép trao đổi thông tin (chủ yếu ở dạng siêu văn bản) qua Internet.
   * ARP (Address Resolution Protocol): Là giao thức mạng được dùng để tìm ra địa chỉ phần cứng (địa chỉ MAC) của thiết bị từ một địa chỉ IP nguồn. Nó được sử dụng khi một thiết bị giao tiếp với các thiết bị khác dựa trên nền tảng local network.
   * SSDP (Simple Service Discovey Protocol): Là một giao thức được dùng để phát hiện dịch vụ mạng mà không cần tới sự trợ giúp của cấu hình dựa vào máy chủ như Dynamic Host Configuration Protocol (DHCP) và Domain Name System (DNS) và cấu hình mạng host tĩnh.
   * DNS (Domain Name System): Là hệ thống phân giải tên miền. Nó cho phép thiết lập tương ứng giữa địa chỉ IP và tên miền trên Internet. Nhờ giao thức này nên có thể chuyển đổi tên miền thành địa chỉ IP.
2. Mất bao lâu từ khi gói tin HTTP GET đầu tiên được gửi cho đến khi HTTP 200 OK đầu tiên được nhận đối với mỗi website.

* **Ở website thứ nhất:**



Hình : Các gói tin bắt được ở trang web thứ nhất sau khi dùng bộ lọc HTTP

Đầu tiên, ta dùng filter để lọc ra những lệnh có Protocol là HTTP. Khi lọc ra, thì ta thấy có 4 gói tin có có Protocol là HTTP.

Ta thấy rằng, gói tin HTTP GET đầu tiên được gửi vào lúc t1 = 0.504420.

Và gói tin HTTP 200 OK đầu tiên được nhận vào lúc t2 = 0.785384.

* Thời gian từ khi gói tin HTTP GET đầu tiên đến HTTP 200 OK là t = t2 – t1 = 0.785384 - 0.504420 = 0.280964 (s).

***? Vì sao gói tin trả về HTTP -200 OK chỉ xuất hiện khi bắt gói tin ở lần truy cập đầu tiên trên trình duyệt.***

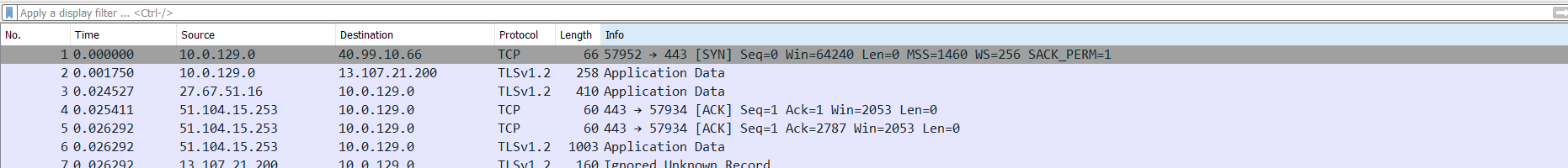
Ta thấy rằng, ở lần đầu tiên, gói tin trả về HTTP -200 OK chỉ xuất hiện khi bắt gói tin ở lần truy cập đầu tiên trên trình duyệt, còn những lần sau, nó trả về cho ta là HTTP -304 NOT MODIFIED.

Về lỗi HTTP 304, nó cho ta biết sự cố giao tiếp giữa trình duyệt của người dùng và máy chủ. Thông báo này cho trình duyệt biết rằng các tài nguyên được lưu trong bộ nhớ cache của trình duyệt đã không được sửa đổi kể từ lần truyền trước đó. Vì vậy, không cần phải truyền lại tài nguyên được yêu cầu cho máy khách một lần nữa. Do đó, trình duyệt hiển thị phiên bản được lưu trong bộ nhớ cahe của trang web.

Còn HTTP 200, nó cho ta biết là yêu cầu ta gửi lên đã được thành công.

Tóm lại, HTTP 200 chỉ xuất hiện ở lần đầu tiên mà request của ta gửi lên thành công. Tuy nhiên, sau đó, các tài nguyên được lưu trong bộ nhớ cache của trình duyệt đã không đổi kể từ lần trước đó (lần mà request của ta gửi lên trình duyệt thành công). Do đó, trình duyệt báo cho ta sự cố giao tiếp giữa trình duyệt của người dùng và máy chủ. Vì thế, nó gửi về cho ta HTTP 304 NOT MODIFIED.

* **Ở website thứ hai:**

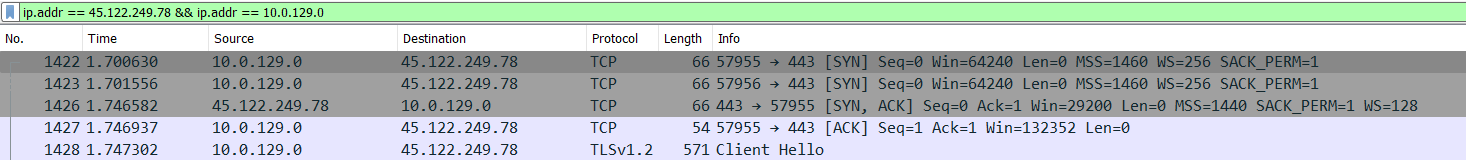
****

Hình : Những gói tin đầu tiên ta bắt được ở website thứ 2

Vì đây là trang web sử dụng giao thức https, do đó, ta không thể sử dụng bộ lọc http như ở trên. Thế nên ta phải sử dụng quy trình bắt tay 3 bước (3 way – handshake). Quy trình đó được mô tả như sau:

* **Bước 1 (SYN):** Trong bước đầu tiên, client thiết lập kết nối với máy chủ. Nó gửi một phân đoạn với SYN và thông báo cho máy chủ về việc client sẽ bắt đầu giao tiếp và với số thứ tự của nó. Client sẽ gửi một message yêu cầu kết nối với Server.
* **Bước 2 (SYN + ACK):** Trong bước này, máy chủ trả lời yêu cầu của client với bộ tín hiệu SYN-ACK (nếu đồng ý kết nối). Trong đó, ACK biểu thị phản hồi của phân đoạn được nhận và SYN biểu thị số thứ tự mà nó có thể bắt đầu với phân đoạn.
* **Bước 3 (ACK):** Ở bước cuối cùng, Client nhận phản hồi của máy chủ và thông báo tới máy chủ bằng một đoạn tin nhắn với ACK và thông báo với máy chủ là đã nhận được phản hồi. Sau đó, cả 2 thiết lập một kết nối đáng tin cậy mà chúng sẽ bắt đầu truyền dữ liệu.

Đầu tiên, ta dùng filter lọc bằng địa chỉ IP của website đó, và IP của máy mình. Cụ thể:

****

Hình : Những gói tin đầu tiên bắt được ở website thứ hai

* ip.addr == 45.122.249.78: Chính là địa chỉ IP của website ta đang bắt gói tin.
* ip.addr == 10.0.129.0: Là địa chỉ IP của máy tính của em đang sử dụng lúc thực hiện bắt gói tin.

Từ hình trên, ta thấy:

* Gói tin [SYN] đầu tiên mà máy ta (Client) gửi yêu cầu tới máy chủ là gói tin No. 1422 ở thời điểm t1 = 1.700630.
* Gói tin [SYN, ACK] đầu tiên bắt được mà máy chủ phản hồi tới máy ta (Client) là gói tin No. 1426 tại thời điểm t2 = 1.746582.
* Gói tin [ACK] sau đó mà máy ta phản hồi lại cho máy chủ là đã nhận được thông báo là gói tin No. 1427 ở thời điểm t3 = 1.746937.

Tuy nhiên, để tính thời gian mà từ lúc Client gửi yêu cầu đầu tiên đến lúc máy chủ phản hồi thì ta chỉ cần sử dụng t1 và t2 để thực hiện tính toán.

* Thời gian từ khi gói tin được gửi đi đầu tiên đến gói tin phản hồi đầu tiên là t = t2 – t1 = 1.746582 – 1.700630 = 0.045952 (s).

1. Nội dung hiển thị trên trang web gaia.cs.umass.edu có nằm trong gói tin HTTP bắt được hay không? Nếu có, hãy tìm và xác định vị trí của nội dung này trong các gói tin bắt được.

Graphical user interface, text, application

Description automatically generated

Hình : Chi tiết của gói tin 200 OK

Trong các gói tin HTTP ta bắt được ở trang web đầu tiên, ta mở gói tin mà nó là HTTP 200 OK. Trong đó, ta thấy rằng nó có xuất hiện nội dung như sau: “Congratulations! You’re downloaded the first Wireshark lab file!”

1. Địa chỉ IP của gaia.cs.umass.edu và website đã chọn ở bước 10 là gì? Địa chỉ IP của máy tính đang sử dụng là gì?

* Địa chỉ IP của gaia.cs.umass.edu:

Từ ảnh trên, ta thấy rằng, địa chỉ IP của trang trên là: 128.119.245.12



Hình : Địa chỉ IP của trang web đầu tiên

* Địa chỉ IP của trang web daa.uit.edu.vn:

Để tìm địa chỉ của một trang web, ta sử dụng câu lệnh sau:

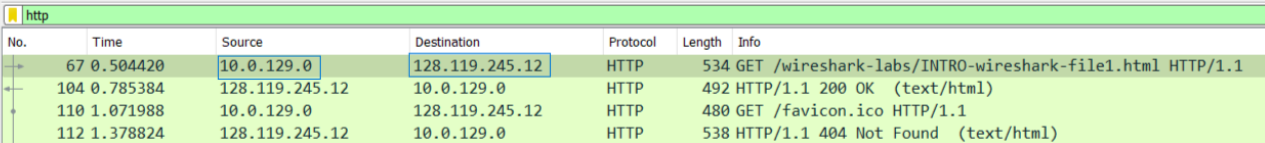
Text

Description automatically generated

Hình : Cách tìm địa chỉ IP của trang web thứ hai

Sau khi gọi câu lệnh đó, ta dễ dàng biết được địa chỉ IP của trang daa.uit.edu.vn là 45.122.249.78

* Địa chỉ IP của máy tính đang sử dụng:



Hình : Hình ảnh các gói tin bắt được ở web thứ 1 sau khi dùng bộ lọc http

Đây là các gói tin sau khi ta sử dụng bộ lọc http, ta thấy rằng, ở ở trên cùng, là gói mà ta gửi request từ máy ta lên server. Do đó, địa chỉ của máy ta lúc này là Source, hay nói cách khác, địa chỉ IP của máy tính ta đang dùng là 10.0.129.0.

1. Qua ví dụ bắt gói tin trên và kết quả bắt gói tin từ Wireshark, hãy mô tả ngắn gọn diễn biến xảy ra khi bắt đầu truy cập vào một đường dẫn đến một trang web cho đến lúc xem được các nội dung trên trang web đó.

* Khi truy cập vào một trang web, trình duyệt sẽ gọi tới máy chủ DNS để biên dịch URL của trang web thành địa chỉ IP (mỗi trang web sẽ có một địa chỉ IP riêng biệt). Khi tìm thấy địa chỉ IP, địa chỉ IP đó sẽ được trả về cho trình duyệt.
* Sau đó, trình duyệt sẽ sử dụng địa chỉ IP vừa được trả về để yêu cầu HTTP gọi tới Server lưu trữ trang web đó.
* Nếu Server chấp nhận thì sẽ gửi lại thông báo “200 OK” (đối với trang web thứ nhất ở trên). Sau đó, trình duyệt sẽ truy xuất mã HTML của trang web được yêu cầu.
* Khi trình duyệt nhận được mã HTML đó từ Server thì nó sẽ hiển thị ra cửa sổ của trình duyệt một trang web hoàn chỉnh.
* Khi đóng trình duyệt thì quá trình kết nối với Server sẽ kết thúc.

\*\*\* Mở rộng: Theo bạn, địa chỉ IP dùng để làm gì và có cách nào khác để xem địa chỉ IP của máy tính và của một website khác hay không? Hãy thực hiện ví dụ minh họa.

* Địa chỉ IP được dùng làm gì và cách xem địa chỉ IP của máy tính và của một website khác?
  + Địa chỉ IP được dùng để giúp các thiết bị mạng Internet phân biệt và nhận ra nhau, từ đó có thể giao tiếp với nhau. Các thiết bị trên mạng có các địa chỉ IP khác nhau.
  + Để xem địa chỉ IP của máy tính, ta thực hiện như sau:
    - Đầu tiên, ta nhấn Window + R, sau đó gõ lệnh cmd

Graphical user interface

Description automatically generated

Hình : Giao diện sau khi nhấn Window + R

* + - Sau đó, chạy lệnh ipconfig



Hình : Lệnh gọi để tìm IP trên máy tính

* + - Sau khi chạy xong lệnh trên, nó sẽ cho ta nhiều địa chỉ IP khác nhau, do đó, ta phải để ý thật kĩ lưỡng để không xem nhầm địa chỉ IP:

A picture containing background pattern

Description automatically generated

Hình : IP của máy tính

Từ hình trên, ta có thể biết được địa chỉ IP của máy tính ta là 10.0.129.0.

* + Để xem địa chỉ IP của một website khác, ta thực hiện như sau:
    - Đầu tiên, ta cũng mở Command Prompt như ở trên.
    - Sau đó, trong cmd, ta gõ lệnh ping + tên website mà ta muốn tìm kiếm.
    - Ví dụ ta muốn tìm địa chỉ IP của website daa.uit.edu.vn, ta thực hiện như sau:

Text

Description automatically generated

Hình : Lệnh tìm địa chỉ IP của một trang web

Qua ảnh trên, ta có thể dễ dàng biết được rằng, địa chỉ IP của website daa.uit.edu.vn là 45.122.249.78.