2

Lab

BÁO CÁO BÀI THỰC HÀNH SỐ 2

Phân tích gói tin HTTP với Wireshark

Sniffing HTTP Traffic with Wireshark

Môn học: Nhập môn Mạng máy tính

|  |  |
| --- | --- |
| Sinh viên thực hiện | Mai Nguyễn Nam Phương (22521164) |
| Thời gian thực hiện | 15/10/2023 – 22/10/2023 |
| Tự chấm điểm | 10/10 |

TRẢ LỜI CÁC CÂU HỎI

Câu 1. Trình duyệt đang sử dụng phiên bản HTTP 1.0 hay 1.1? Phiên bản HTTP server đang sử dụng là bao nhiêu?

**Trả lời**: Trình duyệt đang sử dụng phiên bản HTTP 1.1, phiên bản của HTTP server là 1.1 Ảnh có chứa văn bản, Phông chữ, số, phần mềm

Mô tả được tạo tự động

Câu 2. Địa chỉ IP của máy tính bạn là bao nhiêu? Của web server là bao nhiêu?

**Trả lời**: Địa chỉ IP của máy tính là 172.20.10.2, của web server là 172.20.10.3

Ảnh có chứa văn bản, Phông chữ, số, phần mềm

Mô tả được tạo tự động

Câu 3. Các mã trạng thái (status code) trả về từ server là gì?

Bao gồm các mã 200 OK, 302 Found, 304 Not Modified

Ảnh có chứa văn bản, Phông chữ, số, phần mềm

Mô tả được tạo tự động

Câu 4: Server đã trả về cho trình duyệt tổng cộng bao nhiêu bytes nội dung?

**Trả lời**: Chỉ có 1 gói tin HTTP GET nhờ vào cột info khi ta điền filter

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

Mô tả được tạo tự động

Câu 5. Tìm và xác định gói tin HTTP GET đầu tiên được gửi đến web server gaia.cs.umass.edu?

**Trả lời**: Dựa trên hình ảnh ta thấy được gói HTTP GET đầu tiên là packet số 151, có trường host là gaia.cs.umass.edu và các thông tin liên quan của gói

Ảnh có chứa văn bản, Phông chữ, số, ảnh chụp màn hình

Mô tả được tạo tự động

Câu 6. Xác định gói tin phản hồi cho gói HTTP GET ở trên (Câu 5)?

**Trả lời**: Dựa vào hình ảnh ta thấy được gói tin phản hồi ở câu 5 là gói tin số 169Ảnh có chứa văn bản, Phông chữ, Trang web, phần mềm

Mô tả được tạo tự động

Câu 7. Mất bao lâu từ lúc gửi gói tin HTTP GET (Câu 5) đến khi nhận được gói tin phản hồi (Câu 6)?

**Trả lời**: Dựa trên thông tin của gói tin 169 thì tổng thời gian mất sẽ là 0.246583 giây

Ảnh có chứa văn bản, Phông chữ, phần mềm, Trang web

Mô tả được tạo tự động

Câu 8. Dự đoán địa chỉ IP của gaia.cs.umass.edu là gì? Địa chỉ IP của máy tính đang sử dụng là gì? Tại sao?

**Trả lời**: Dựa trên gợi í ta có thể thấy được câu trả lời, ví dụ như IP của máy tính sẽ là IP yêu cầu (Source) là 192.168.1.11 và IP của địa chỉ sẽ là IP phản hồi (Destination) là 128.119.245.12



Câu 9. Tổng thời gian bắt gói tin và tổng số gói tin bắt được là bao nhiêu?

**Trả lời**: Tương tự như câu 1 ta sẽ có tổng số gói tin bắt được là 435 gói và tổng thời gian là 10.69777 giây

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Mô tả được tạo tự động

Câu 10. Liệt kê ít nhất 3 giao thức khác nhau xuất hiện trong cột giao thức (Protocol). Tìm hiểu trên Internet và mô tả ngắn gọn chức năng chính của các giao thức đó.

**Trả lời**: Có các giao thức là TCP, HTTP, DNS, UDP…

Chức năng của TCP: Thiết lập kết nối (cho phép 2 máy tính thiết lập như 1), đảm bảo tính toàn vẹn (đảm bảo dữ liệu truyền giữa 2 máy không xảy ra các vấn đề), điều khiển luồng (kiểm soát tốc độ truyền dữ liệu giữa 2 máy để đảm bảo an toàn cho máy chủ), xác nhận và tái gửi, kết thúc kết nối

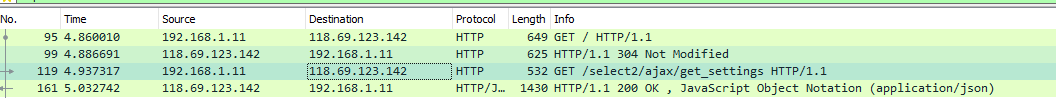
Chức năng của HTTP: Truyền tải dữ liệu (truyền dữ liệu giữa máy tính máy chủ và trình duyệt web), yêu cầu và phản hồi (hoạt động dựa trên mô hình trình duyệt web gửi yêu cầu và máy chủ phản hồi), định dạng văn bản (sử dụng các thông điệp văn bản có định dạng đơn giản và dễ đọc cho việc truyền tải và giao tiếp giữa máy tính máy chủ và trình duyệt), khả năng tương tác (cho phép người dùng tương tác với các trang và thực hiện các hành động trên trang web)

Chức năng của DNS: Chuyển đổi tên miền và địa chỉ IP (giúp máy tính xác định địa chỉ IP tương ứng với một tên miền và ngược lại), phân giải tên miền (hỗ trợ quá trình phân giải tên miền bằng cách truy vấn các máy chủ DNS để tìm địa chỉ IP tương ứng cho một tên miền cụ thể), tạo hệ thống tên miền phân cấp (tổ chức các tên miền vào một cấu trúc phân cấp, giúp quản lý và quản trị tên miền trên Internet một cách hiệu quả)

Chức năng của UDP: Truyền dữ liệu không đáng tin cậy (cho phép gửi và nhận dữ liệu mà không đảm bảo tính toàn vẹn, độ tin cậy hoặc thứ tự. Điều này làm cho UDP nhanh hơn và ít tốn tài nguyên hơn so với giao thức TCP), nhưng cũng có nghĩa rằng dữ liệu có thể bị mất hoặc bị trùng lặp trong quá trình truyền tải.

Câu 11. Tìm cách để xác định địa chỉ IP của trang web đã chọn ở Bước 8. Địa chỉ IP trang web đã chọn là gì ?

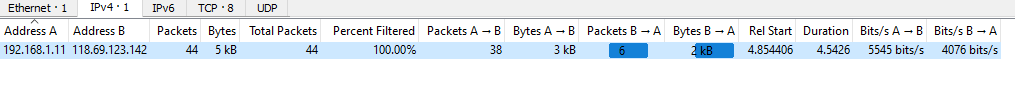
**Trả lời**:



Dựa trên hình ảnh trên ta sẽ thấy địa chỉ IP của trang web đã chọn ở mục Destination của gói 119 hoặc gói 95 là 118.69.123.142

Câu 12. Số lượng gói tin và khối lượng dữ liệu được gửi (trao đổi) giữa Địa chỉ trang web ở trên (Câu 11) và máy tính đang sử dụng ?

**Trả lời**:



Dựa trên cách 2 ta có:

Địa chỉ máy tính: 192.158.1.11 và địa chỉ trang web: 118.69.123.142

Vậy thì số lượng gói tin được trao đổi là 44 gói và khố lượng dữ liệu được gửi là 5 kB