ĐỒ ÁN THỰC HÀNH 2 – PHÂN TÍCH GÓI TIN

MÔN MẠNG MÁY TÍNH

1. Quy định chung

- Đồ án được làm theo nhóm: mỗi nhóm tối đa **3** sinh viên, tối thiểu **2** sinh viên.

- Các bài làm giống nhau sẽ đều bị điểm **0 toàn bộ phần thực hành** (dù có điểm các bài tập, đồ án thực hành khác).

- Môi trường: Sử dụng công cụ Wireshark

2. Cách thức nộp bài

Nộp bài trực tiếp trên Website môn học, không chấp nhận nộp bài qua email hay hình thức khác.

Tên file: **MSSV1_MSSV2_MSSV3.zip** (Với MSSV1 < MSSV2 < MSSV3)

Ví dụ: Nhóm gồm 3 sinh viên: 2012001, 2012002 và 2012003, tên file nộp: **2012001_2012002_2012003.zip**

Cấu trúc file nộp gồm:

1. **2012001_2012002_2012003.pdf:** chứa báo cáo về bài làm
2. **Packets**: thư mục chứa pcap file (**2012001_2012002_2012003_*bai1.pcapng*, 2012001_2012002_2012003_*bai2.pcapng*, 2012001_2012002_2012003_*bai3.pcapng***)

   Nhóm nào không nộp pcap file thì không được chấm bài đó.

Lưu ý: Cần thực hiện đúng các yêu cầu trên, nếu không, bài làm sẽ không được chấm.

3. Hình thức chấm bài

GV chấm dựa trên bài làm được nộp tại Moodle

4. Tiêu chí đánh giá

Về báo cáo:

- Thông tin của nhóm.
- Đánh giá mức độ hoàn thành từ 0 – 100% (Chú thích rõ những mục làm được,chưa làm được và còn bị lỗi)

- Trả lời các câu hỏi mà đồ án đưa ra
- Chụp hình để minh chứng cho câu trả lời (có tô đậm/ khoanh vùng cụ thể chi tiết minh chứng cho câu trả lời, ảnh có chứa một phần màn hình desktop)
- Bảng phân công công việc và cho biết rõ ràng ai làm việc gì cách rõ ràng. Không ghi chia đều công việc hay cùng làm mọi việc.
- Các nguồn tài liệu tham khảo.

5. Thang điểm chi tiết

Mỗi câu trả lời, nếu có hình ảnh để trả lời, thì bắt buộc phải chèn hình ảnh và highlight nội dung trả lời, đồng thời kèm theo giải thích chi tiết về câu trả lời đó nếu có.

Bài	Câu	Ghi chú	Điểm
1			**3,5đ**
	1		0,25
	2		0,5
	3		1
	4		1
	5		0,75
2			**3đ**
	1		0,75
	2		0,75
	3		0,75
	4		0,75
3			3,5đ
	1		0,5
	2		0,5
	3		0,5
	4		0,75
	5	a,b,c,d,e mỗi câu 0,25	1,25
Báo cáo		Trình bày rõ ràng, nội dung đầy đủ, không có báo cáo, không chấm điểm	[-10, 0.5]
Tổng			**10**

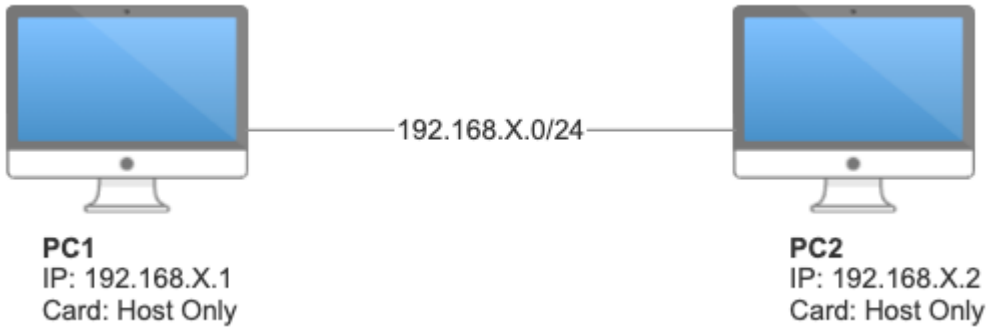
Giới thiệu:

Wireshark là công cụ cho phép giám sát gửi/nhận gói tin trên card mạng. Có 2 modes hoạt động: Open và Capture. Capture mode cho phép người dùng có thể xem trực tiếp các gói tin hiện tại đang ra/vào card mạng, và có thể lưu trữ lại với định dạng pcap file. Open mode cho phép người dùng đọc gói tin pcap file có sẵn.

Nội dung:

Bài 01: SMTP & POP3 (3đ)

Chuẩn bị:
Thiết lập mô hình mạng như hình:
Lưu ý: X là 2 chữ số cuối của mã số sinh viên một bạn bất kì trong nhóm



1. Khởi động chương trình Test mail server được cung cấp trong đồ án 1 trên PC1. Sử dụng port cho dịch vụ SMTP (25) và POP3 (110)
2. Khởi động chương trình Thunderbird trên PC2. Thiết lập các thông số cần thiết để kết nối đến Test mail server tại PC1.
3. Khởi động chương trình bắt gói tin Wireshark tại PC2:
4. Sử dụng Thunderbird để:
    - Đăng nhập một tài khoản email với cú pháp MSSV1@mmt.edu.vn, Password: 123456
    - Soạn và gửi email có file đính kèm đến địa chỉ email MSSV2@mmt.edu.vn
    - Đăng nhập tài khoản email MSSV2@mmt.edu.vn, Password 123456

- Kiểm tra email mới, đọc email và tải file đính kèm
- Dừng quá trình bắt gói tin

5. Lưu các gói tin bắt được dưới dạng file: MSSV1_MSSV2_MSSV3_bai1.pcapng

Yêu cầu:

1. Lọc các gói tin sử dụng giao thức smtp và pop3.
2. Quan sát lưu lượng được ghi lại trong ngăn danh sách gói tin bắt được. Hãy chỉ ra giao thức được sử dụng tại tầng transport của gói tin SMTP và POP3
3. Vẽ quá trình trao đổi gói tin giữa SMTP server và SMTP client.
4. Lọc gói tin theo giao thức sử dụng tại tầng transport của gói tin SMTP. Cho biết ý nghĩa 3 gói tin đầu tiên trong danh sách. Ghi rõ thông tin sequence number, acknowledgement number của những gói tin này.
5. Lọc các gói tin SMTP có nhãn 221. Quan sát chi tiết những gói tin này và cho biết giá trị các trường "Response Code", "Response Parameter". Cho biết ý nghĩa các thông số này.

Bài 02: ARP (3đ)

Chuẩn bị:

- Xóa lịch sử cache có liên quan tên miền gaia.cs.umass.edu của trình duyệt web đang sử dụng
- Mở Wireshark và tiến hành bắt gói tin trên card mạng (có kết nối internet)
- Dùng trình duyệt web truy xuất vào trang: http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html
- Dừng quá trình bắt gói tin

Yêu cầu: Hãy dựa vào những gói tin bắt được để trả lời các câu hỏi sau:

1. Lọc những gói tin dùng giao thức ARP. Quan sát và cho biết gói tin ARP có chứa thông tin source IP và destination IP hay không? Giao thức ARP hoạt động ở tầng nào trong mô hình TCP/IP?
2. Cho biết địa chỉ MAC nguồn và địa chỉ MAC đích trong Ethernet frame của gói tin ARP request, ARP reply (hexadecimal value)
3. Hãy cho biết giá trị trường Type trong Ethernet frame của gói ARP request (hexadecimal value), trường này có ý nghĩa gì?
4. Dựa vào gói tin bắt được, hãy chỉ ra có bao nhiêu trường thông tin trong phần ARP payload. Kể tên các trường thông tin trên, xác định kích thước của từng trường (bytes), giá trị trong từng trường là gì?

Bài 03: Traceroute (3đ)

Nếu bạn dùng Window thì dùng lệnh ***tracert***, nếu bạn dùng Linux/iOS thì bạn dùng lệnh ***traceroute***. Lưu ý kết quả bắt gói tin trên Window và Linux/iOS sẽ khác nhau, vì vậy câu trả lời phụ thuộc bạn dùng OS nào.

Bật wireshark để bắt gói tin lệnh traceroute từ máy của mình (có thể dùng máy ảo) đến www.fit.hcmus.edu.vn (FIT). Trả lời những câu hỏi sau:

1. Chụp hình kết quả bắt gói tin sau khi traceroute hoặc tracert (thấy được những gói tin liên quan)
2. Cho biết chức năng của lệnh traceroute/tracert?
3. Cho biết địa chỉ IP của máy gửi request?
4. Quan sát và chỉ rõ những gói tin dùng xác định địa chỉ IP của FIT từ tên miền trong danh sách các gói tin bắt được. Cho biết các gói tin này dùng giao thức gì tại tầng ứng dụng trong mô hình TCP/IP
5. Sau khi xác định được IP của www.fit.hcmus.edu.vn, máy sẽ bắt đầu gửi gói tin đến FIT
    a. Protocol được sử dụng của những gói tin sau đó là gì?
    b. Có bao nhiêu gói tin được gửi đi (**request**) trước khi nhận được **response đầu tiên trả lời** cho những request? (Hay nói một cách khác là: lệnh trace* sẽ gửi request message đi, và nhận về response. Vậy có bao nhiêu gói tin request đã gửi đi đến khi nhận được gói tin response đầu tiên?)
    c. Cho biết **TTL của gói tin cuối cùng** được gửi trước khi nhận được gói tin **response đầu tiên trả lời** cho những gói tin request?
    d. Bạn có thấy thông tin **port** trong các gói tin gửi đi? Nếu có bạn nhận thấy port nguồn/đích của gói tin có gì đặc biệt? Nếu không thấy thông tin port, hãy giải thích nguyên nhân?
    e. Gói tin **response đầu tiên** là trả lời cho **gói tin request thứ mấy**? (No.)

HẾT