ĐỒ ÁN THỰC HÀNH

PHÂN TÍCH GÓI TIN VỚI WIRESHARK

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 (theo nhóm TH đã đăng ký).

- 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: 2312001, 2312002 và 2312003 làm đề 1, tên file nộp: **2312001_2312002_2312003.zip**

Cấu trúc file nộp gồm:

Thư mục **MSSV1_MSSV2_MSSV3** chứa tập tin, thư mục con:

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

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)
- 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			
	1		**0,25**
	2		**0,5**
	3		**0,5**
	4		**0,5**
	5	a,b,c,d,e mỗi câu 0,25	**1,25**
		Tổng	**3đ**
2			
	1,...,8		**0,5**
		Tổng	**4đ**
3			
	1,2	Bắt được gói tin yêu cầu Xác định IP	**0.5**
	3		**0,5**
	4		**0,5**
	5		**0,5**
	6		**0,75**
		Tổng	**3đ**
Báo cáo		Đầy đủ nội dung yêu cầu, trình bày tốt Không có báo cáo: 0 điểm đồ án 2	

Bài 01: Traceroute (3đ)

- Nếu bạn dùng Windows, sử dụng WSL(Windows Subsystem for Linux) để cài đặt Ubuntu và cài đặt lệnh **traceroute** để dùng (không dùng tracert trên Windows trong bài tập này)

Hướng dẫn dùng WSL

```
$ sudo apt install traceroute
<nhập password để cài đặt gói>
```

- Khởi chạy Wireshark để bắt gói tin
- Thực hiện lệnh ***traceroute*** đến : www.fit.hcmus.edu.vn (FIT).

```
$ traceroute www.fit.hcmus.edu.vn
```

- Sau khi nhận được kết quả của lệnh traceroute, ngừng quá trình bắt gói tin trên Wireshark

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?
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
    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.)

Bài 02: DHCP (4đ)

Chuẩn bị:

1. Khởi chạy terminal/ command promt, gõ lệnh ipconfig /release
2. Khởi chạy wireshark, kiểm tra và bắt gói tin trên card mạng thật của máy tính
3. Khởi chạy terminal/ command promt, gõ lệnh ipconfig /renew
4. Sau khi nhận được cấu hình IP, thực hiện lại bước 1 và 3 một lần nữa
5. Dừng quá trình bắt gói tin

Yêu cầu:

1. Lọc các gói tin theo giao thức DHCP
2. Gói tin DHCP sử dụng giao thức nào tại tầng transport
3. Hãy cho biết địa chỉ tại tầng link của host được cấp IP
4. Cho biết thông tin IP nguồn, Port nguồn và IP đích, Port đích của 4 gói tin (Discover/Offer/Request/ACK) trong đợt xin cấp IP đầu tiên
5. Chỉ ra điểm khác biệt giữa các giá trị trong gói tin DHCP Discover và DHCP Request
6. Cho biết giá trị Transaction-ID của 4 gói tin (Discover/Offer/Request/ACK) trong đợt xin cấp IP đầu tiên, giá trị Transaction-ID của 2 gói tin (Request/ACK) trong đợt xin cấp IP lần hai. Mục đích sử dụng của transaction-ID là gì?
7. Cho biết ý nghĩa trường thông tin lease-time, giá trị của trường này trong gói tin bắt được là bao nhiêu?
8. Trong gói tin DHCP bắt được, hãy chỉ ra trường giá trị cho biết có thông tin DHCP relay agent hay không? Nếu có hãy cho biết IP của DHCP relay agent.

Bài 03: TCP (3đ)

Chuẩn bị:

1. Mở trình duyệt web, truy cập trang http://gaia.cs.umass.edu/wiresharklabs/alice.txt và tải file alice.txt về máy tính

2. Truy cập trang http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html . Chọn đường dẫn đến file alice.txt (chú ý: không chọn upload)
3. Khởi chạy wireshark, bắt đầu bắt gói tin. Quay lại trình duyệt web chọn chức năng "Upload alice.txt". Sau khi upload thành công bạn sẽ nhận được một thông điệp chúc mừng
4. Dừng quá trình bắt gói tin trên wireshark

Yêu cầu:

1. Lọc các gói tin HTTP bắt được trong quá trình upload file alice.txt
2. Xác định IP của gaia.cs.umass.edu (máy chủ HTTP)
3. Lọc các gói tin TCP và cho biết sequence number của TCP SYN segment, gói tin dùng để tạo kết nối giữa client và máy chỉ HTTP. Giá trị nào trong gói tin cho biết đây chính là gói SYN segment
4. Cho biết sequence number của TCP SYNACK segment, gói tin phản hồi gói SYN segment từ máy chủ HTTP đến client. Xác định giá trị trường Acknowledgement trong gói tin SYNACK. Máy chủ HTTP đã xác định giá trị này như thế nào?
5. Xác định sequence number trong gói tin chứa HTTP POST command. Hướng dẫn: kiểm tra phần nội dung của gói tin/cột info để tìm thấy câu lệnh POST.
6. Vẽ quá trình trao đổi gói tin giữa client và máy chủ HTTP khi upload file alice.txt, bắt đầu từ gói tin TCP SYN và kết thúc với gói TCP FIN (Gợi ý: sử dụng chức năng Statistics/Flow Graph của Wireshark)

HẾT