ĐỒ ÁN THỰC HÀNH

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

- **Các bài làm giống nhau 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 làm đề 1, tên file nộp: **2012001_2012002_2012003.zip**

Cấu trúc file nộp gồm thư mục MSSV1_MSSV2_MSSV3 chứa:

1. **MSSV1_MSSV2_MSSV3_Report.pdf:** chứa báo cáo về bài làm
2. **Packets**: thư mục chứa pcap file

   MSSV1_MSSV2_MSSV3_*bai2.pcapng*

   MSSV1_MSSV2_MSSV3_ *bai3.pcapng*

   MSSV1_MSSV2_MSSV3_*bai4.pcapng*

   Nhóm nào không nộp pcap file bài 2, bài 3 và bài 4 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

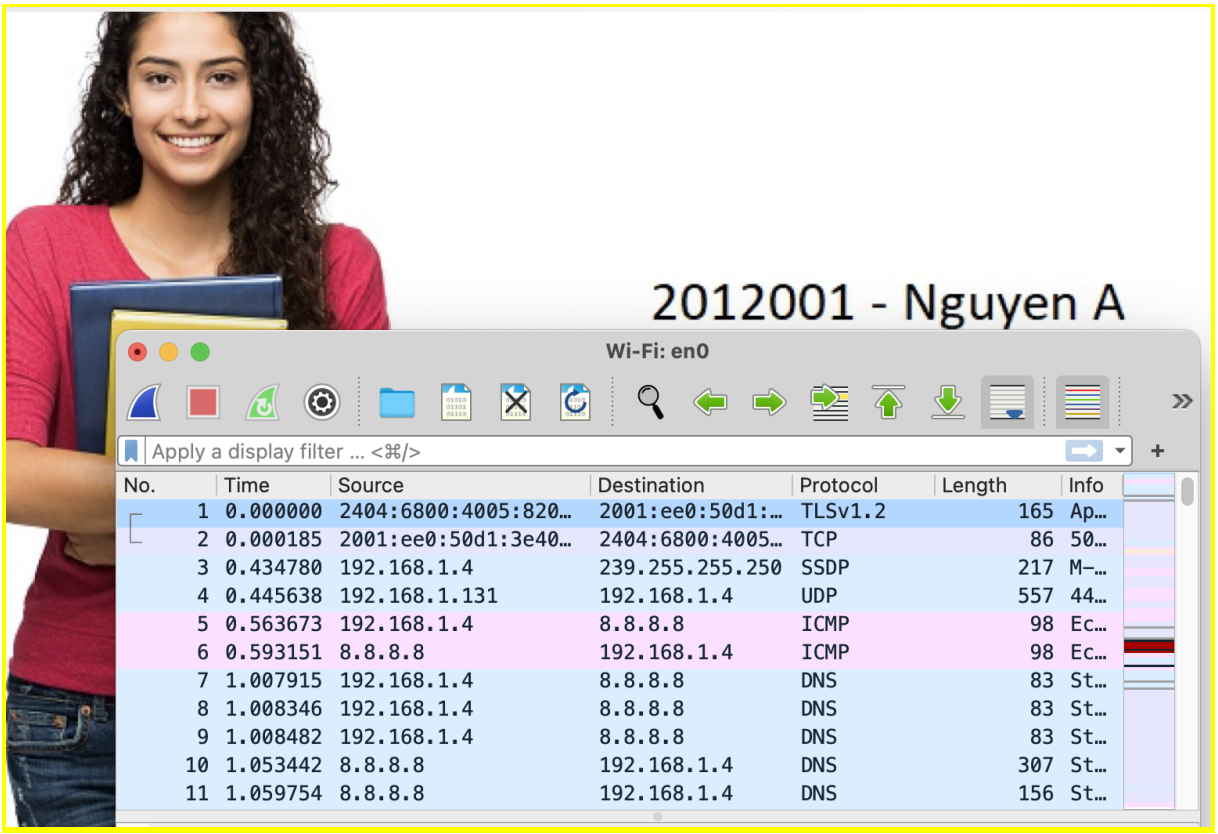
GV chấm dựa trên bài làm được nộp tại Moodle

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

- Sử dụng màn hình nền chứa MSSV - Họ tên - ảnh của sinh viên làm bài
- Chụp hình để minh chứng cho câu trả lời (có tô đậm/ khoanh vùng cụ thể) có chứa một phần desktop như hình minh họa



- Bảng phân công công việc và cho biết rõ ràng ai làm việc gì 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 (2.0)			
	1,2,3a,3b	Mỗi câu 0.375	**1.5**
	3c		**0.5**
2 (2.5)	1		**0.5**
	2		**0.5**
	3		**0.5**
	4,6	Mỗi câu 0.25	**0.5**
	5		**0.5**
3 (2.5)			
	1		**0.5**
	2a,b,c,d	**0,25x4**	**1.0**
	3		**0.5**
	4		**0.5**
4 (3.0)			
	1		**0.5**
	2, 3, 4, 5a, 5b,	**0.3125x8**	**2.5**

	5c, 5d, 5e		
		Tổng	**10đ**
Sai tên/định dạng file			**-2đ**
Sai MSSV			**-2đ**
Báo cáo		Đầy đủ nội dung và trình bày theo quy định Không có báo cáo: 0 điểm đồ án	

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: Ping (2đ)

Mở ping.pcapng file, nội dung của file pcap là thông tin các gói tin gửi từ một máy sang một máy khác bằng lệnh ping. Trả lời các câu hỏi sau:

1. Cho biết địa chỉ IP của host ping và host được ping?
   Host ping: 192.168.0.105
   Host được ping: 192.168.1.1
2. Cho biết port được sử dụng là bao nhiêu? Nếu không có port thì giải thích tại sao?
   Không có port, vì ICMP nằm ở tầng Network
3. Với gói tin ICMP request:

a. Cho biết kích thước (bytes) của từng phần trong diagram. (Chú ý: Kích thước tổng của gói tin là 98 bytes)

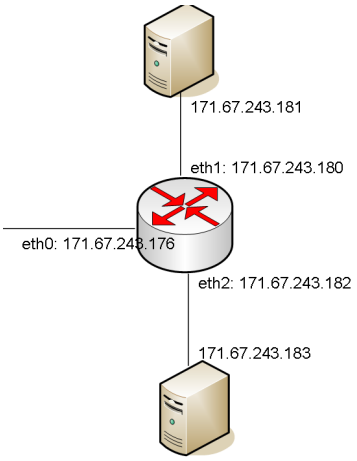
48	16(64-48)	20	14
ICMP data	ICMP header	IP header	Ethernet header

b. Cho biết có bao nhiêu gói tin ARP? Giải thích tại sao lại có các gói tin ARP này, nêu ý nghĩa của các gói tin đó.

Có 2 gói tin ARP (ARP request, và ARP reply), để biết được thông tin MAC

c. Dựa trên nội dung gói pcap, hãy vẽ sơ đồ logic của đường mạng. Ví dụ:

192.168.0.0/24 ---------- (192.168.0.1)Router(...) ---------- 192.168.1.0/24



Bài 2: UDP (2.5đ)

- Mở Wireshark và tiến hành bắt gói tin trên card mạng (có kết nối internet)
- Mở dòng lệnh và thực hiện lệnh sau:

```
nslookup www.fit.hcmus.edu.vn
```

- Tạm dừng quá trình bắt gói tin
- Thực hiện lọc gói tin bằng dòng lệnh như hình

Hãy trả lời các câu hỏi sau:

1. Câu lệnh “nslookup” trên có ý nghĩa gì?, trong phần trả lời trên màn hình dòng lệnh có dòng "Non-authoritative answer" có ý nghĩa gì?

2. Hãy cho biết có bao nhiêu trường thông tin trong phần header của gói tin UDP? Kể tên các trường thông tin trên, xác định kích thước của từng trường (bytes) - có hình minh chứng bằng gói tin bắt được
3. Hãy cho biết giá trị trong trường Length là bao nhiêu? đơn vị là gì? và trường này đang nói đến kích thước gì?
4. Protocol number của UDP là gì? (trả lời giá trị dạng hexadecimal và decimal)
5. Lượng dữ liệu tối đa có thể đưa vào UDP payload là bao nhiêu bytes? (ghi công thức tính rõ ràng để ra được kết quả)
6. Hãy cho biết mối quan hệ giữa port number trong những gói tin lọc được

Bài 03: HTTP (2.5đ)

- Tải file theo link sau: http://gaia.cs.umass.edu/wireshark-labs/alice.txt
- Dùng trình duyệt web truy cập trang: http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html
- Mở Wireshark và tiến hành bắt gói tin trên card mạng (có kết nối internet)
- Thực hiện chọn đường dẫn đến file alice.txt vừa download, chọn Upload alice.txt file trên trình duyệt
- Dừng quá trình bắt gói tin và lọc ra những gói tin gửi đi hoặc gửi đến máy chủ gaia.cs.umass.edu

Hãy trả lời các câu hỏi sau:

1. Hãy cho biết địa chỉ IP của máy chủ gaia.cs.umass.edu. Port dịch vụ được máy chủ sử dụng để gửi và nhận các gói tin TCP segment là bao nhiêu?
2. Tìm 7 TCP segments tiếp theo, tính từ TCP segment của HTTP POST đầu tiên ở câu 2
    a. Cho biết No. của 7 TCP segments đó
    b. Cho biết sequence number của 7 TCP segments đó
    c. Cho biết No. của ACK báo nhận của 7 TCP segments đó
    d. Lượng data gửi trong mỗi TCP segment đó
3. Cho biết throughput (bytes transferred per unit time) cho kết nối upload file này, vui lòng cho biết cách tính
4. Vẽ quá trình trao đổi gói tin từ lúc khởi tạo đến lúc đóng kết nối TCP (có ghi rõ SEQ number, ACK number của từng segment), dùng chức năng Flow Graph trong Wireshark nhưng yêu cầu chỉ vẽ giữa máy bạn và web server, không có những traffic ngoài luồng trong hình vẽ

Bài 04: Traceroute (3đ)

Nếu bạn dùng Windows thì dùng lệnh ***tracert***, nếu bạn dùng Unix/Linux/macOS thì bạn dùng lệnh ***traceroute***. Lưu ý kết quả bắt gói tin trên Windows và Unix/Linux/macos 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 traceroute/tracert dùng để làm gì?
3. Cho biết địa chỉ IP của máy gửi request?
4. Cho biết cách máy tính xác định được địa chỉ IP của FIT
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 **phản hồi đầu tiên** cho những request?
    c. Cho biết **TTL của gói tin cuối cùng** được gửi trước khi nhận được gói tin **phản hồi đầu tiên** 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 **phản hồi đầu tiên** là trả lời cho **gói tin request thứ mấy**? (No.)

HẾT