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:

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

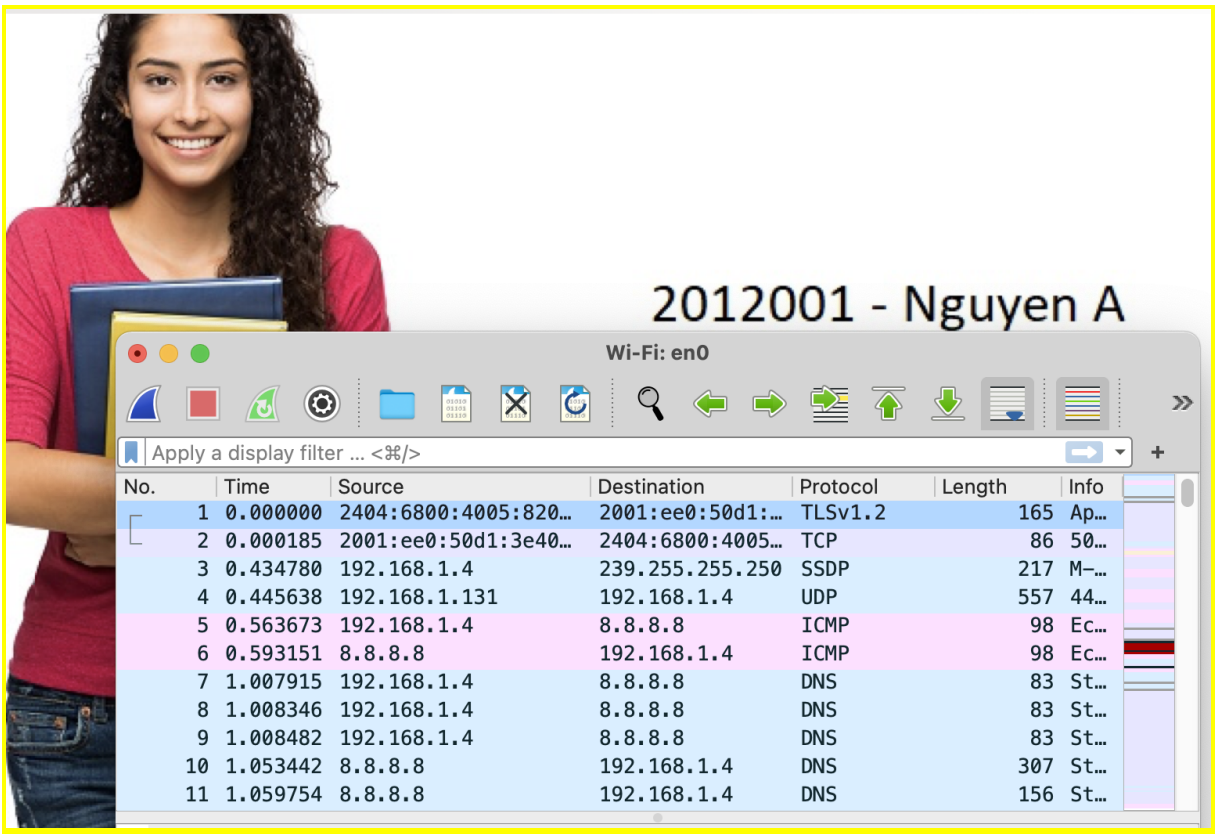
GV chấm dựa trên bài làm được nộp tại Moodle

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			
	1,2,3	Mỗi câu 0.5	**1.5**
	4		**1**
2	1		**0.25**
	2		**0.75**
	3		**0.5**
	4,5	Mỗi câu 0.25	**0.5**
	6		**0.5**
3			
	1		**0.5**
	2		**0.25**
	3		**1.25đ**
	4		**0.5**
4			
	1,2,3,4,5	Mỗi câu 0.5	**2.5**
		Tổng	**10đ**
Sai tên/định			**-2đ**

dạng file			
Sai MSSV			**-2đ**
Báo cáo		Đầy đủ nội dung và trình bày theo quy định	

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 1: ARP (2.5đ)

- Xóa lịch sử cache 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

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

1. ARP là giao thức gì? Lọc những gói tin dùng giao thức ARP
2. Cho biết địa chỉ nguồn và địa chỉ đích trong Ethenet 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 (hexadicimal value), trường này có ý nghĩa gì?
4. Hãy cho biết 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? - có hình minh chứng bằng gói tin bắt được

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 trên 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?
6. Hãy cho biết mối quan hệ giữa port number trong những gói tin lọc được

Bài 3: TCP (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

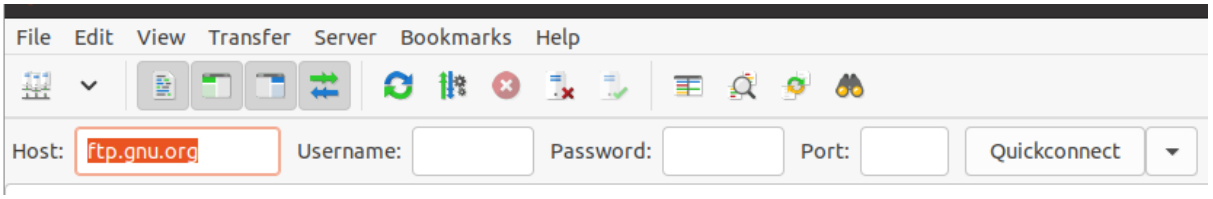
Hãy trả lời các câu hỏi sau:

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. Kích thước của 3 gói tin TCP đầu tiên bắt được là bao nhiêu?
3. 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)

4. Hãy cho biết cách máy chủ gaia.cs.umass.edu xác định ACK number trong TCP SYNACK segment?

Bài 4: FTP(2.5đ)

Cài phần phềm FTP client (như FileZilla) và kết nối vào host sau: ftp.gnu.org



Dùng wireshark để bắt gói tin trao đổi giữa máy của bạn và ftp.gnu.org.

Nhấn Quickconnect để tiến hành kết nối

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

1. Chụp hình kết quả sau khi kết nối đến server ftp.gnu.org
2. Cho biết Username sử dụng để login vào server là gì
3. Cho biết port client và server dùng để truyền lệnh (command port)
4. Để hiển thị được danh sách folder và file trên server, thì phải dùng kênh truyền data. Cho biết mode sử dụng là gì (Active Mode-PORT, Passive Mode-PASV hay Extended Passive Mode-EPSV). Ý nghĩa của mode data đang được dùng là gì?
5. Cho biết port client và server sử dụng để truyền - nhận danh sách folder và file

HẾT