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***)

   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			
	1		0,5
	2	Mỗi câu a,b,c,d là 0,5	2
	3		2
	4		0.5
2		Xây dựng DHCP server, cấp phát IP thành công	1
		Bắt và lọc gói tin DHCP đúng	0,5
	1,2,3,4	Mỗi câu 0,75	3
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:

Chuẩn bị:

- Khởi động chương trình wireshark.
- Tiến hành bắt gói tin trên card mạng có kết nối internet
- Sử dụng trình duyệt web, truy cập trang web http://info.cern.ch/
- Sau khi trình duyệt web đã hiển thị nội dung trang web trên, dừng quá trình bắt gói tin, lưu lại file bắt gói tin dưới tên MSSV1_MSSV2_MSSV3_bai01.pcapng

Yêu cầu:

Dựa trên các gói tin bắt được trả lời các câu hỏi sau:

1. Sử dụng chức năng Statistic của Wireshark và cho biết số gói tin bắt được tương ứng các giao thức sau: TCP, UDP, ICMP, HTTP, DNS
2. Thực hiện lọc gói tin bằng lệnh **dns.a** và cho biết:
    a. IP của DNS server
    b. Port dịch vụ được sử dụng tại DNS server và DNS client
    c. Giao thức được dùng tại tầng transport của gói tin DNS
    d. Thông tin IPv4 và IPv6 của host info.cert.ch
3. Thực hiện lọc gói tin bằng lệnh **http**:

Cho biết nội dung phần header của gói tin http response từ máy chủ info.cert.ch, giải thích ý nghĩa từng trường thông tin trong header

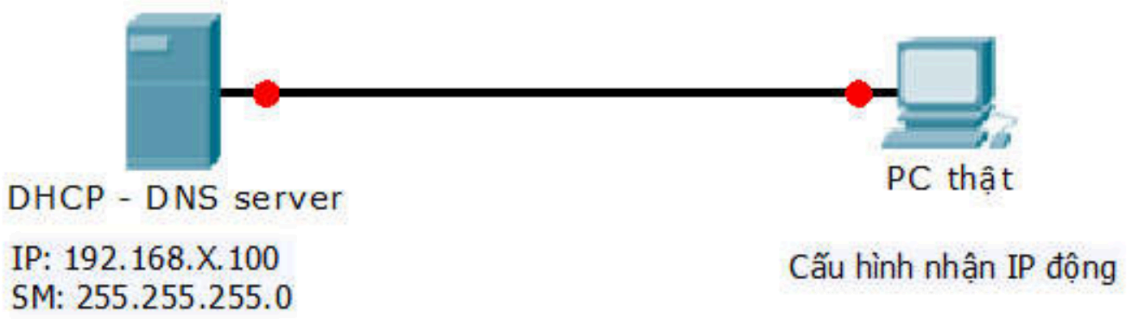
4. Sau đó click chọn một gói tin http sử dụng chức năng Follow -> TCP stream:

Vẽ quá trình trao đổi các gói tin TCP 3-way handshake giữa client và máy chủ info.cert.ch (ghi chú rõ IP của máy chủ, client, sequence number, acknowledgement number của từng gói tin, trong wireshark có chức năng vẽ tự động)

Bài 02: DHCP

Chuẩn bị:

- Thiết lập card mạng ảo là Host Only
- Thực hiện cài đặt dịch vụ DHCP theo mô hình:



- ☐ Khoảng địa chỉ IP sẽ cấp (Address Pool): 192.168.X.10 – 192.168.X.90
- ☐ Subnet Mask: 255.255.255.0 − Khoảng địa chỉ IP để dành: 192.168.X.10- 192.168.X.20
- ☐ Gateway: 192.168.X.1
- ☐ DNS Server: 192.168.X.100

- Tắt tính năng DHCP của phần mềm VMWare (Trên VMWare Player/Workstation > Chọn menu Edit > Virtual Network Editor > Chọn card mạng VMNet1 > Bỏ chọn "Use local DHCP service to distribute IP addresses to VMs).
- Cấu hình PC thật nhận IP động từ DHCP Server vừa cấu hình
- Thực hiện bắt gói tin trên card mạng VMNet 1 của máy thật
- Thực hiện xin cấp IP mới tại máy thật (bắt đầu bắt gói tin)
- Lưu lại file bắt gói tin dưới tên MSSV1_MSSV2_MSSV3_bai02.pcapng

Yêu cầu: Phân tích các gói tin bắt được và trả lời câu hỏi

1. Liệt kê tên các gói tin DHCP bắt được trong quá trình xin cấp mới địa chỉ IP
2. Dịch vụ DHCP sử dụng port ở server và client là bao nhiêu?
3. Địa chỉ IP mà DHCP server đề nghị cấp cho client được gửi từ gói tin nào?
4. Hãy cho biết sự khác biệt giữa 2 trường thông tin: "***Your IP address***" và "***Client IP Address***" trong gói tin DHCP ACK.

Lưu ý: Biết X là 2 chữ số cuối của mã số sinh viên một bạn bất kì trong nhóm

HẾT