**ĐỒ ÁN WIRESHARK  
BẮT VÀ PHÂN TÍCH GÓI TIN**

**QUY ĐỊNH:**

* Đồ án làm cá nhân
* **X** là 2 chữ số cuối của MSSV. Ví dụ MSSV là 1812123 thì **X**=23
* Các bài làm giống nhau bất kể vì lý do gì đều bị 0 điểm phần thực hành.
* **Bài nộp MSSV.rar/zip gồm:**
* 1**.** File **MSSV.docx/pdf** trả lời các câu hỏi và bắt buộc phải có hình chụp chứng minh (cần đóng khung, chú thích các thông tin quan trọng của hình chụp) ứng với từng câu trả lời. Khi chụp hình phải chụp đầy đủ và có 1 phần Desktop Background.
* 2. File gói tin Wireshark **ICMP\_MSSV.pcapng, HTTP\_MSSV.pcapng và FTP\_MSSV.pcapng**
* Lưu ý: Sinh viên chỉ trình bày phần phân tích gói tin, không trình bày phần cấu hình các dịch vụ vào báo cáo.

**ĐỀ BÀI**

**Bài 1: ICMP**

1. Thiết lập card mạng máy ảo là Host-Only.
2. Cấu hình IP để máy thật và máy ảo có thể ping nhau:
   1. Card VMnet 1 trên máy thật:

* IP: 192.168.X.2
* Subnet mask: 255.255.255.0
  1. Máy ảo: 192.168.X.1
* IP: 192.168.X.1
* Subnet mask: 255.255.255.0

1. Bắt gói tin ICMP giữa máy thật và máy ảo (lưu file với tên **ICMP\_MSSV.pcapng)**, trả lời các câu hỏi:
   1. Mục đích của việc ping?
   2. Có bao nhiêu các gói tin trong quá trình ping? (Giả sử các máy dùng để test là Windows)
   3. Địa chỉ MAC nguồn? MAC đích?
   4. Địa chỉ IP nguồn? IP đích?
   5. Nội dung phần Data của gói tin ICMP?

**Bài 2: HTTP**

1. Thực hiện các bước sau:
2. Start Wireshark
3. Mở trình duyệt (Chrome, Firefox…)
4. Clear Cache của trình duyệt
5. Truy cập: gaia.cs.umass.edu
6. Bấm vào 1 link bất kỳ trong web.
7. Truy cập lần 1: gaia.cs.umass.edu/ethereal-labs/lab2-1.html
8. Truy cập lần 2: gaia.cs.umass.edu/ethereal-labs/lab2-1.html
9. Truy cập: gaia.cs.umass.edu/ethereal-labs/lab2-3.html
10. Stop Wireshark
11. Lưu file với tên **HTTP\_MSSV.pcapng**
12. Phân tích gói tin vừa bắt được và trả lời các câu hỏi sau:
13. Trình duyệt của bạn sử dụng HTTP phiên bản 1.0 hay 1.1? Phiên bản của HTTP được server chạy/hỗ trợ là bao nhiêu?
14. Ngôn ngữ mà trình duyệt web mong muốn chấp nhận từ server là gì?
15. Địa chỉ IP của máy client và máy gaia.cs.umass.edu server là gì?
16. Mã trả về từ server cho trình duyệt là gì và ý nghĩa của nó là gì?
17. Thời điểm file HTML mà bạn đang nhận được chỉnh sửa lần cuối ở server khi nào?
18. Có bao nhiêu byte trong nội dung được trả về cho trình duyệt?
19. Kiểm tra nội dung của yêu cầu HTTP GET đầu tiên từ trình duyệt tới server. Bạn có tìm thấy 1 dòng “IF-MODIFIED-SINCE” trong HTTP GET?
20. Kiểm tra các nội dung phản hồi của server. Server có trả về nội dung của file một cách rõ ràng không (tức có trả về đúng nội dung mà trình duyệt yêu cầu ban đầu hay trả về nội dung nào đó khác)?
21. Tiếp theo kiểm tra các nội dung của yêu cầu HTTP GET thứ hai từ trình duyệt của bạn tới server. Bạn có tìm thấy dòng “IF-MODIFIED-SINCE” trong HTTP GET? Nếu có thì đó là thông tin gì sau “IF-MODIFIED-SINCE:” header? Cho biết ý nghĩa của nó?
22. Cho biết mã trả về từ server cho HTTP GET request thứ hai? Server có trả về rõ ràng nội dung của các file (tức có trả về đúng file đó không hay trả về nội dung gì khác)? Giải thích tại sao lại như vậy?

**Bài 3: FTP**

1. Thiết lập card mạng máy ảo là Host-Only.
2. Cấu hình IP để máy thật và máy ảo có thể ping nhau:
3. Card VMnet 1 trên máy thật:
   * IP: 192.168.X.2
   * Subnet mask: 255.255.255.0
4. Máy ảo: 192.168.X.1
   * IP: 192.168.X.1
   * Subnet mask: 255.255.255.0
5. Cài đặt và cấu hình FTP Server trên máy ảo, FTP Client trên máy thật.

FTP Server: <https://filezilla-project.org/download.php?type=server>

FTP Client: <https://filezilla-project.org/download.php?type=client>

1. Thực hiện các bước sau:
2. Start Wireshark ở máy thật
3. FTP Client kết nối đến FTP Server với user/password là **họ tên/MSSV** (Sinh viên cấu hình ở câu 3 ở trên)
4. FTP Client download 1 file bất kỳ từ FTP Server.
5. FTP Client upload 1 file bất kỳ lên FTP Server
6. FTP Client xóa 1 file bất kỳ trên FTP Server
7. Stop Wireshark
8. Lưu file với tên **FTP\_MSSV.pcapng**
9. Phân tích các gói tin và trả lời các câu hỏi:
10. Có bao nhiêu FTP command đã bắt được? Giải thích ý nghĩa từng command?
11. IP nguồn, IP đích của các gói tin FTP kể trên?
12. MAC nguồn, MAC đích của các gói tin FTP kể trên?
13. FTP sử dụng port ở server và client là bao nhiêu?
14. FTP đang sử dụng mode passive hay active?
15. Có lấy được thông tin user và password khi phân tích các gói tin FTP không?