**BÀI TẬP 1 LÝ THUYẾT**

**THỰC HÀNH AN TOÀN BẢO MẬT MẠNG MÁY TÍNH**

**Lab 1: Làm quen với Wireshark**

**Họ tên: Phạm Hồ Bình An**

**Lớp: 10DH\_CNPM2**

**Mã số sinh viên: 1050080127**

1. **Task 1:**

Kể tên các loại thiết bị liên quan đến Mạng mà bạn biết hoặc đang sử dụng (kèm ảnh minh họa).

Moderm, Router Wifi,…

 

Những vấn đề gì có thể xảy ra nếu không có kết nối Internet trong 5 phút ?

Mục tiêu về kiến thức sau khi hoàn thành môn học Nhập môn Mạng máy tính của bạn là gì?

1. **Task 2:**
   1. **Giới thiệu**

Giới thiệu và làm quen với Wireshark

Wireshark là phần mềm bắt gói tin (packet sniffer) rất phổ biến và miễn phí chạy

trên Windows, Linux, MacOS, hỗ trợ bắt gói tin và quan sát nội dung của các thông

điệp được trao đổi bởi các giao thức tại các tầng mạng khác nhau.

Ngoài ra, Wireshark còn phục vụ cho việc điều tra các chứng cứ số (forensic) liên

quan đến các vụ án về mạng máy tính.

* 1. **Thử nghiệm bắt gói tin với Wireshark**

B1: Khởi động trình duyệt web bất kỳ như Google Chrome, Firefox, Edge,...

và phần mềm Wireshark (phiên bản mới nhất)

Ảnh có chứa văn bản, ảnh chụp màn hình, Phần mềm đa phương tiện, phần mềm

Nội dung do AI tạo ra có thể không chính xác.

B2: Tại phần Capture, chọn interface đang hoạt động chính trên máy để bắt

đầu bắt gói tin.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Nội dung do AI tạo ra có thể không chính xác.

B3: Sau đó, cửa sổ sẽ xuất hiện và hiển thị kết quả bắt gói tin tại

interface đã chọn.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Nội dung do AI tạo ra có thể không chính xác.

B4: Mở trình duyệt web và chỉ truy cập vào website có địa chỉ như sau

<http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, màn hình

Nội dung do AI tạo ra có thể không chính xác.

B5: Sau khi trình duyệt đã hiển thị trang INTRO-wireshark-file1.html (chỉ là

một dòng chào mừng đơn giản), dừng bắt gói tin tại Wireshark.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Nội dung do AI tạo ra có thể không chính xác.

B6: Gõ “http” vào packet-display filter sau đó chọn Apply để Wireshark chỉ

hiển thị các thông điệp HTTP trong packet-listing window.

Ảnh có chứa đồ điện tử, văn bản, ảnh chụp màn hình, phần mềm

Nội dung do AI tạo ra có thể không chính xác.

B7: Tìm 2 thông điệp HTTP GET được gửi từ máy tính đến

gaia.cs.umass.edu server (tìm trong packet-listing window đoạn chứa GET theo

sau bởi gaia.cs.umass.edu) và HTTP 200 OK được trả về từ server đến máy tính

hiện tại. Sau khi chọn thông điệp HTTP GET, các thông tin về Ethernet frame,

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

Nội dung do AI tạo ra có thể không chính xác.

B8: Lưu lại tập tin Wireshark đã bắt được thành file .pcapng có tên dạng

MSSV-Bai1.pcapng. Ví dụ: 18521006-Bai1.pcapng.

Ảnh có chứa văn bản, phần mềm, ảnh chụp màn hình, Phần mềm đa phương tiện

Nội dung do AI tạo ra có thể không chính xác.

B9:

Chọn biểu tượng Start capturing packets để bắt đầu quá trình bắt gói tin

mới.

B10: Chọn 1 website mà sinh viên thường hay truy cập, ví dụ uit.edu.vn,

tinhte.vn,... và tiến hành bắt gói tin trên website đó

Lặp lại các bước 4-5-6-7 với một website khác có chứa nhiều thông tin hơn mà

sinh viên thường truy cập. Ví dụ: tuoitre.vn, uit.edu.vn,...

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Website

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

Nội dung do AI tạo ra có thể không chính xác.

Lưu lại tập tin sau khi bắt được ở website thứ 2 thành file pcapng có tên

dạng MSSV-Bai2.pcapng

Ảnh có chứa văn bản, phần mềm, ảnh chụp màn hình, Phần mềm đa phương tiện

Nội dung do AI tạo ra có thể không chính xác.

* 1. Phân tích kết quả bắt gói tin từ Wireshark

1. Tổng thời gian bắt gói tin trong từng trang web đã thử nghiệm và tổng số gói

tin bắt được là bao nhiêu?

9086 Gói tin trong khoảng 1 phút.

2. Liệt kê ít nhất 5 giao thức khác nhau xuất hiện trong cột giao thức (Protocol)

khi không áp dụng bộ lọc “http” khi truy cập 2 website. Tìm hiểu trên Internet

và mô tả ngắn gọn chức năng chính của các giao thức đó.

STUN

TCP

UDP

**Stun** là giao thức mạng cho phép máy khách (client) tìm thấy địa chỉ công khai, NAT mà nó đang đứng sau, cổng phía internet được NAT gắn liền cổng nội bộ nào đó. Thông tin này được dùng để thiết lập giao tiếp **UDP** giữa 2 Host nằm sau NAT Router. **Stun** là giao thức giữa server và client.

**TCP** (Transmission Control Protocol - "Giao thức điều khiển truyền vận") là một trong các giao thức cốt lõi của bộ giao thức **TCP/IP.** Sử dụng TCP, các ứng dụng trên các máy chủ được nối mạng có thể tạo các "kết nối" với nhau, mà qua đó chúng có thể trao đổi dữ liệu hoặc các gói tin.

3. Mất bao lâu từ khi gói tin HTTP GET đầu tiên được gửi cho đến khi HTTP 200

OK đầu tiên được nhận đối với mỗi website đã thử nghiệm. (mặc định, giá trị

của cột thời gian (Time) trong packet-listing window là khoảng thời gian tính

bằng giây kể từ khi chương trình Wireshark bắt đầu bắt gói tin).

0.278890S

4. Nội dung hiển thị trên trang web gaia.cs.umass.edu

“Congratulations! You've downloaded the first Wireshark lab file!”

có nằm trong các gói tin HTTP bắt được hay không? Nếu có, hãy tìm và xác

định vị trí của nội dung này trong các gói tin bắt được.

…..

5. Địa chỉ IP của gaia.cs.umass.edu và website đã chọn ở bước 10 là gì? Địa chỉ IP

của máy tính đang sử dụng là gì?

Wed: 128.119.245.12

Máy: 192.168.0.106

6. Qua ví dụ bắt gói tin trên và kết quả bắt gói tin từ Wireshark, hãy mô tả ngắn

gọn diễn biến xảy ra khi bắt đầu truy cập vào một đường dẫn đến một trang

web cho đến lúc xem được các nội dung trên trang web đó.