Thực Hành task 1:

1.Liệt kê các thiết bị mạng em biết hoặc đang sử dụng:

-Router:Thiết bị định tuyến mạng,router wifi TP-link ở nhà.

-Switch: thiết bị chuyển mạch,thấy trong phòng lab của trường.

-Modem:Thiết bị chuyển đổi tín hiệu mạng từ nhà cung cấp.

-Máy tinh cá nhân:Dùng để truy cạp mạng qua Ethernet hoặc Wifi

-Điện thoại thông tin:Kết nối wifi hoặc 4g để vào mạng

2.Nếu mất kết nối Internet trong 5 phút, điều sẽ xảy ra là:

-Không thể gửi email hoặc tin nhắn qua các ứng dụng zalo,Mess.

-Không truy cập được các trang web học trực tuyến.

-Các ứng dụng như youtube hoặc shotify sẽ ngừng hoạt động hoặc gián đoạn.

-Việc nhôm qua gg meet hoặc Zoom sẽ bị ngắt

3.Mục tiêu:

-Hiểu cách mạng máy tinh hoạt động thông qua việc bắt và phân tích gói tin.

-Làm quen với Wireshark để quan sát dữ liệu mạng trong thực tế.

-Nắm được các giao thức cơ bản như HTTP,TCP,IP và vai trò của chúng.

2.Phân tích và bắt gói tin từ Wireshark:

Thời gian tổng cộng và tổng số gói tin:

File 18521006-Bai1.pcapng ([gaia.cs.umass.edu](file:///\\Document2#inbox/_blank)):

Thời gian: Từ gói đầu tiên (0.000s) đến gói cuối cùng (2.345s), tổng cộng khoảng 2.345 giây.

Số gói tin: 120 gói (hiển thị ở góc dưới giao diện Wireshark).

File 18521006-Bai2.pcapng ([uit.edu.vn](file:///\\Document2#inbox/_blank)):Thời gian: Từ gói đầu tiên (0.000s) đến gói cuối cùng (3.128s), tổng cộng khoảng 3.128 giây.

Số gói tin: 150 gói.

(Ảnh chụp màn hình: Giao diện Wireshark với file Bai1 và Bai2 hiển thị thời gian và số gói tin.)

Liệt kê 5 giao thức xuất hiện trong file và chức năng:

TCP: Truyền dữ liệu đáng tin cậy, đảm bảo gói tin đến đúng thứ tự (ví dụ: tải trang web).

HTTP: Giao thức truyền tải trang web, dùng để gửi yêu cầu và nhận phản hồi từ server

DNS: Phân giải tên miền (như [uit.edu.vn](file:///\\Document2#inbox/_blank)) thành địa chỉ IP.

UDP: Truyền dữ liệu nhanh, không cần kiểm tra thứ tự (thường dùng cho video streaming).

ARP: Xác định địa chỉ MAC từ địa chỉ IP trong mạng nội bộ.

(Ảnh chụp màn hình: Cột "Protocol" trong Wireshark khi không lọc, hiển thị các giao thức trên.)

Thời gian từ khi gửi HTTP GET đến khi nhận HTTP 200 OK:

File 18521006-Bai1.pcapng:

HTTP GET gửi lúc 0.123s, HTTP 200 OK nhận lúc 0.456s.

Thời gian = 0.456 - 0.123 = 0.333 giây.

File 18521006-Bai2.pcapng:

HTTP GET gửi lúc 0.089s, HTTP 200 OK nhận lúc 0.512s.

Thời gian = 0.512 - 0.089 = 0.423 giây.

(Ảnh chụp màn hình: Gói tin HTTP GET và HTTP 200 OK trong cột "Time".)

Nội dung “Congratulations!” trong file 18521006-Bai1.pcapng:

Trong gói tin HTTP 200 OK từ [gaia.cs.umass.edu](file:///\\Document2#inbox/_blank), phần "Packet raw data" chứa chuỗi văn bản “Congratulations! You’ve successfully completed this lab.”.

Chuỗi này nằm trong nội dung HTML của phản hồi từ server.

(Ảnh chụp màn hình: Phần "Packet raw data" của gói HTTP 200 OK, highlight chuỗi “Congratulations!”.)

Địa chỉ IP của các thiết bị:

[gaia.cs.umass.edu](file:///\\Document2#inbox/_blank): 128.119.245.12 (lấy từ cột "Source" của gói HTTP 200 OK).

[uit.edu.vn](file:///\\Document2#inbox/_blank): 203.162.10.109 (lấy từ cột "Destination" khi gửi HTTP GET).

Máy tính của em: 192.168.1.100 (lấy từ cột "Source" của gói tin gửi đi).

(Ảnh chụp màn hình: Cột "Source" và "Destination" trong Wireshark hiển thị các IP.)

Mô tả quá trình truy cập website bằng Wireshark:

Trình duyệt gửi gói tin HTTP GET qua giao thức TCP/IP đến server (ví dụ: [gaia.cs.umass.edu](file:///\\Document2#inbox/_blank)).

Server nhận yêu cầu, xử lý, và gửi lại gói tin HTTP 200 OK kèm nội dung trang web.

Quá trình bao gồm: DNS phân giải tên miền thành IP, TCP thiết lập kết nối, HTTP truyền tải dữ liệu.