BÀI THỰC HÀNH SỐ 1 – CHƯƠNG 1

Họ tên sinh viên: .....
Nhóm: .....MSSV:.....

I. Mục tiêu

- Hiểu biết về cấu hình TCP/IP trên hệ điều hành Microsoft Windows
- Hiểu biết một số lệnh liên quan về mạng.
- Hiểu biết về phần mềm Wireshark.

II. Các bước thực hiện

1. Hiểu biết về cấu hình TCP/IP trên hệ điều hành Microsoft Windows

a. Xem thông tin TCP/IP

- Sử dụng lệnh ipconfig để xem thông tin cấu hình TCP/IP
- Thông thường có hai Adapter (Network Interface Card và giao tiếp PPP)
- Cho biết các thông tin trên Network Interface Card:

IP Address: ..... Subnet Mask:.....
Default Gateway:..... DNS Server: .....

b. Cấp phát động hoặc cấu hình tĩnh thông tin TCP/IP

- Start -> Settings -> Control Panel -> Network Connections -> Local Area Connection -> Properties -> Internet Protocol (TCP/IP) -> Properties
- Nếu muốn cấu hình tĩnh thì sử dụng các thông tin ở mục 3 để cấu hình.

2. Tìm hiểu một số lệnh liên quan về mạng

*a. Lệnh **ipconfig** (**ifconfig** trên Linux/UNIX)*

- Người quản trị sử dụng lệnh này để xem thông tin TCP/IP trên các giao tiếp mạng, và tất nhiên cũng có thể dùng để cấu hình TCP/IP cho các giao tiếp mạng.
- Cho biết cú pháp của lệnh trên. Cho biết kết quả

.....
.....

*b. Lệnh **netstat***

- Người quản trị sử dụng lệnh này để xem xét toàn diện thông tin về hệ thống cục bộ và bộ giao thức TCP/IP.
- Cho biết kết quả của lệnh netstat –a

.....
.....

*c. Lệnh **tracert** (traceroute trên Linux/UNIX)*

- Người quản trị sử dụng lệnh này để dò tìm đường đi đến một hệ thống khác, mục đích xác định được lỗi xảy ra khi không thực hiện được kết nối.
- Cho biết kết quả của lệnh tracert www.google.com

.....
.....

*d. Lệnh **route***

- Người quản trị sử dụng lệnh này để xem, thêm hay loại bỏ các đường đi trong bảng đường đi của mỗi máy tính.
- Cho biết kết quả của lệnh route PRINT

.....
.....

*e. Lệnh **ping***

- Người quản trị sử dụng lệnh này để hỏi một hệ thống khác để chắc chắn rằng kết nối vẫn còn hoạt động.
- Cho biết kết quả của lệnh ping www.yahoo.com

.....

.....

*f. Công cụ **nslookup***

- Người quản trị sử dụng công cụ này để kiểm tra hoạt động của hệ thống hỏi đáp tên (Domain Name System).
- Cho biết địa chỉ IP của www.vnn.vn (thực hiện nslookup www.vnn.vn):

.....

.....

- Cho biết địa chỉ IP của Mail eXchange domain hotmail.com (thực hiện `nslookup -type=MX hotmail.com`)

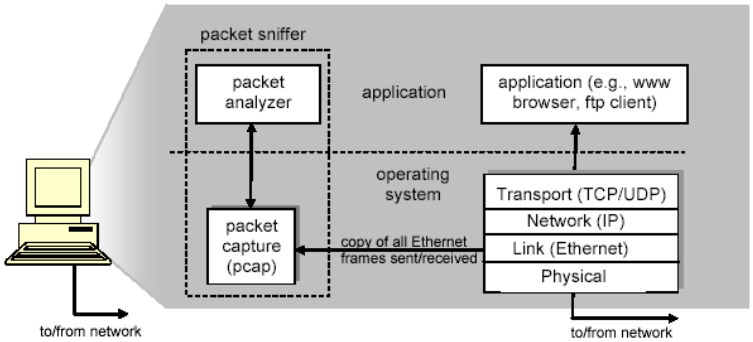
*g. **SSH** (Secure Shell) Client*

- Người quản trị sử dụng công cụ để kết nối vào một hệ thống và làm việc từ xa. Thay thế cho telnet, ftp, rcp, rsh, ...

3. Hiểu biết về Wireshark

a. Packet Sniffer

Công cụ cơ bản cho việc quan sát các thông điệp trao đổi giữa các thực thể hoạt động. Chúng nắm bắt các thông điệp vào ra trên máy tính của bạn, lưu trữ và hiển thị các thành phần của các trường khác nhau của giao thức trong các thông điệp trên.

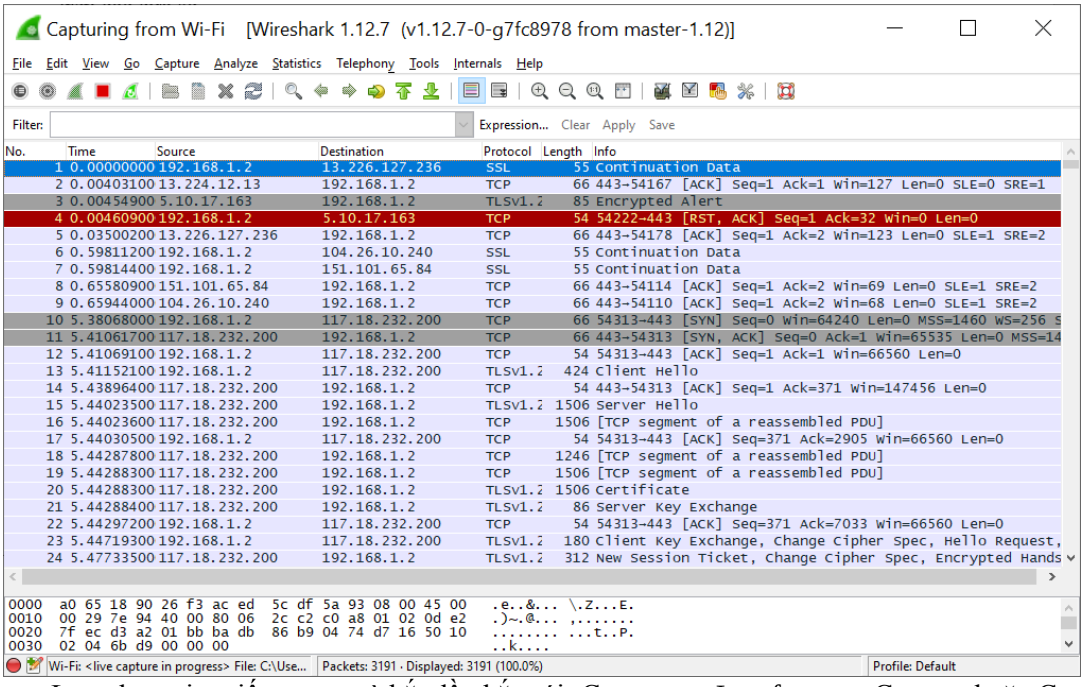


b. Wireshark

Một packet analyzer miễn phí chạy trên nhiều hệ điều hành (Windows, Unix, Mac) kết hợp thư viện pcap. Các thông tin liên quan:
https://www.wireshark.org/download.html

c. Sử dụng Wireshark

Khi chạy chương trình Wireshark giao diện đồ họa sẽ xuất hiện, và chưa có thông tin gì hiển thị trên các cửa sổ.



- Lựa chọn giao tiếp mạng và bắt đầu bắt gói: Capture -> Interfaces -> Capture hoặc Capture -> Start, dừng lại và hiển thị thông tin.

d. Ví dụ

- Khởi động một trình duyệt.
- Khởi động Wireshark.
- Start quá trình bắt gói.
- Nhập URL sau vào trình duyệt: http://www.hcmute.edu.vn/, trang web sẽ được hiển thị.
- Dừng lại tiến trình bắt gói trên Wireshark. Các thông điệp HTTP trao đổi với Web Server (hoặc Proxy Server) chắc chắn xuất hiện đâu đó trong danh sách các thông điệp bắt được. Cho biết hình ảnh của Wireshark sau khi dừng lại tiến trình bắt gói
- Gõ "http" vào nơi khai báo filter, nhấn Apply để chỉ xem các thông điệp liên quan đến HTTP. Cho biết hình ảnh của Wireshark sau khi filter.
- Chọn thông điệp đầu tiên để xem xét. Đây phải là thông điệp HTTP GET mà máy tính bạn đã gởi đến Web Server www.hcmute.edu.vn (hoặc Proxy Server). Khi chọn thông điệp này thì Wireshark frame header, IP datagram header, TCP segment header, HTTP message heder cũng được hiển thị trong cửa sổ packet header.
  Cho biết thông tin của các header (Wireshark frame header, IP datagram header, TCP segment header, HTTP message heder).
- Thoát khỏi Wireshark.

.

--HẾT--