Nội dung và hướng dẫn bài thực hành

Mục đích

Giúp sinh viên làm quen với công cụ Tshark để phân tích và xử lý các gói tin mạng.

Yêu cầu đối với sinh viên

Có kiến thức cơ bản về hệ điều hành Linux, công cụ Tshark.

Nội dung thực hành

Khởi động bài lab:

Vào terminal, gõ:

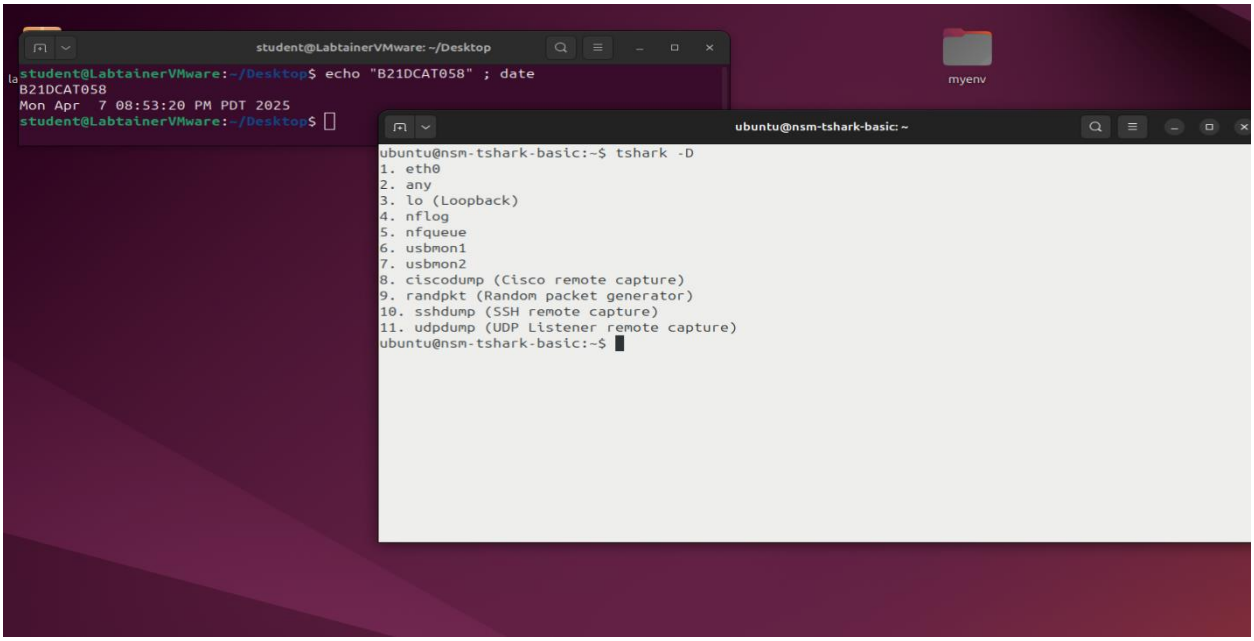
labtainer -r nsm-tshark-basic

(chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)

Sau khi khởi động xong terminal ảo sẽ xuất hiện.

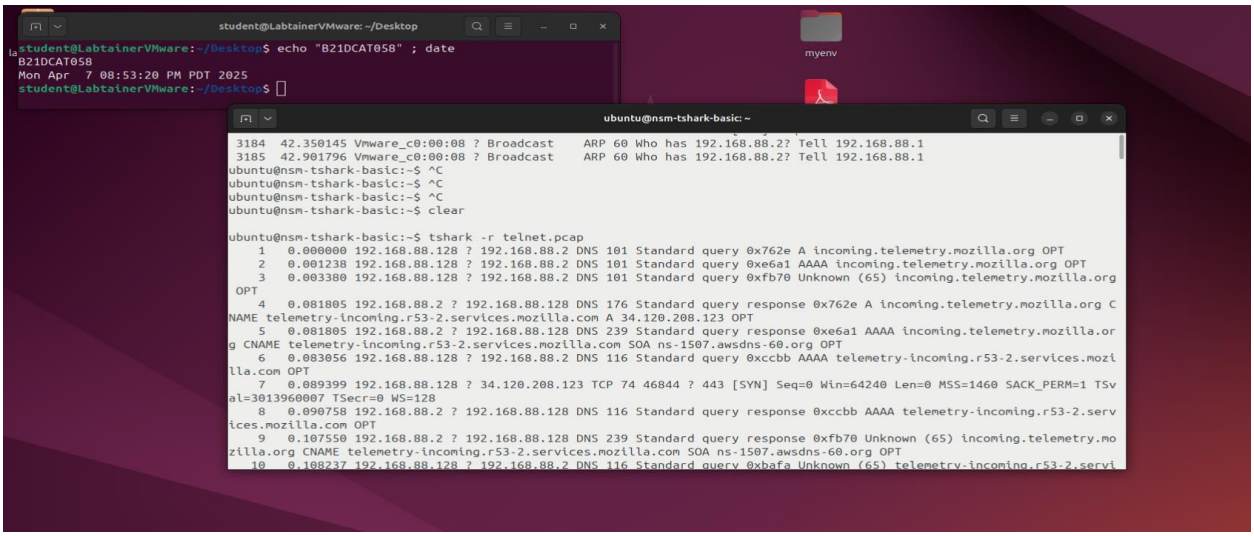
Sinh viên thực hiện liệt kê các giao diện mạng khả dụng:

tshark -D



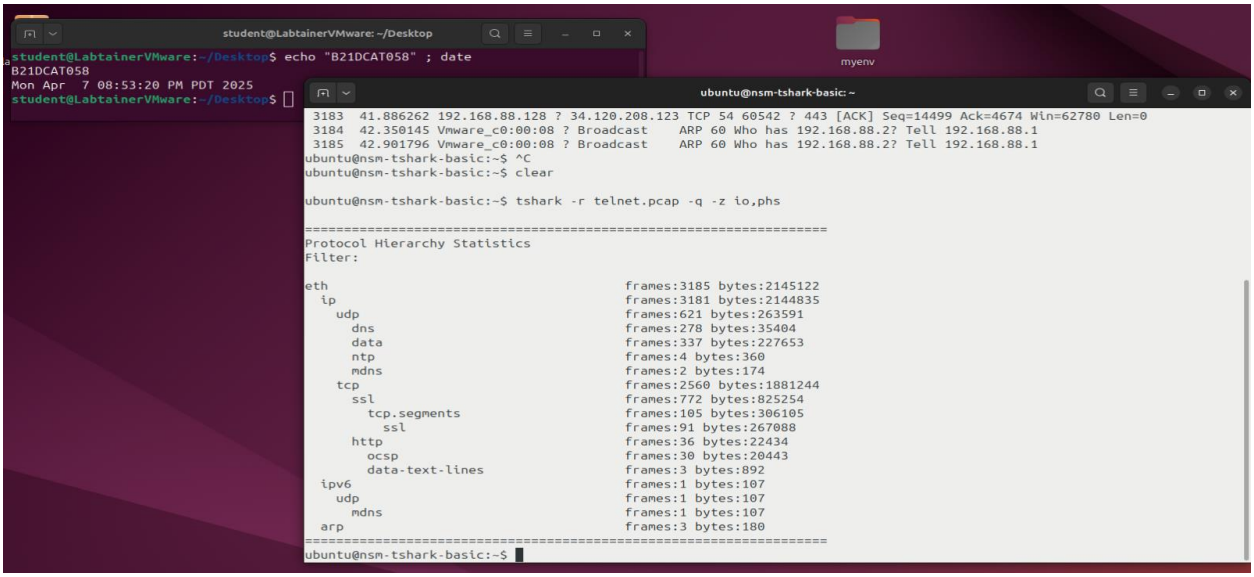
Sinh viên đọc các gói tin trong file pcap

tshark -r telnet.pcap



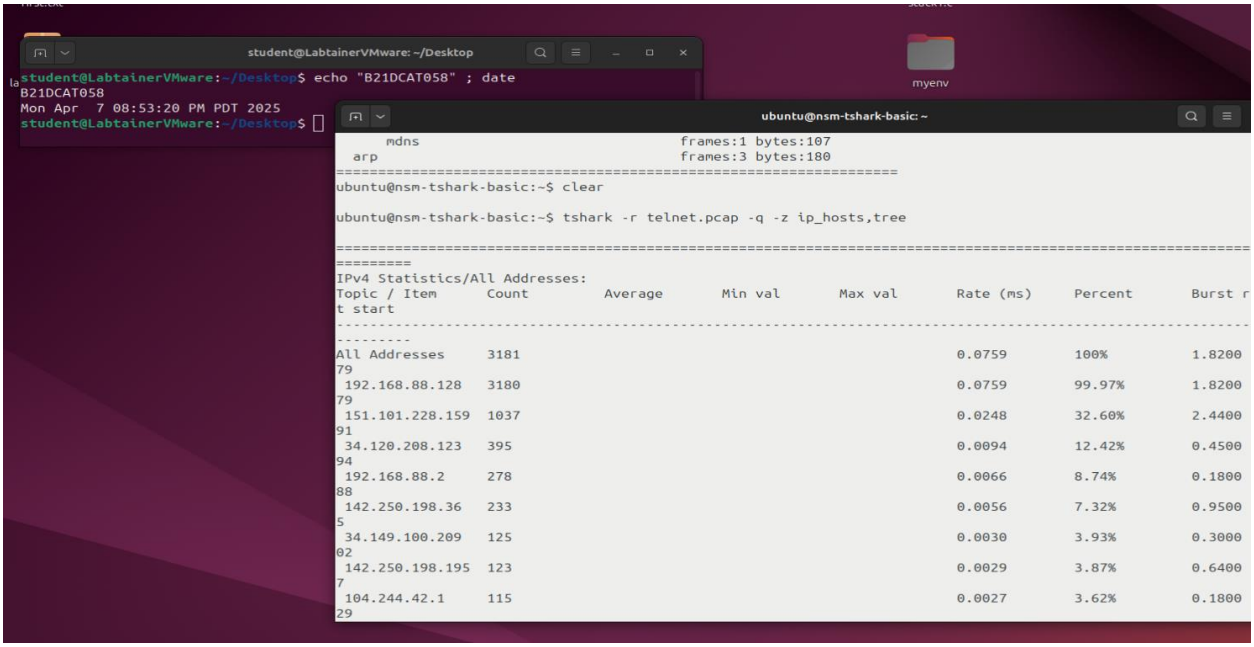
Sinh viên thống kê các giao thức trong file pcap:

tshark -r telnet.pcap -q -z io,phs



Sinh viên thống kê các địa chỉ IP trong file pcap dưới dạng cây:

tshark -r telnet.pcap -q -z ip_hosts,tree



Kết thúc bài lab:

Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

stoplab nsm-tshark-basic

Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.

Khởi động lại bài lab:

Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

labtainer -r nsm-tshark-basic