

Nội dung và hướng dẫn bài thực hành

Mục đích

Giúp sinh viên nắm vững cách sử dụng Wireshark để thu thập, giám sát và phân tích các gói tin trong mạng

Yêu cầu đối với sinh viên

Có kiến thức cơ bản về hệ điều hành Linux, công cụ wireshark và giao thức TCP

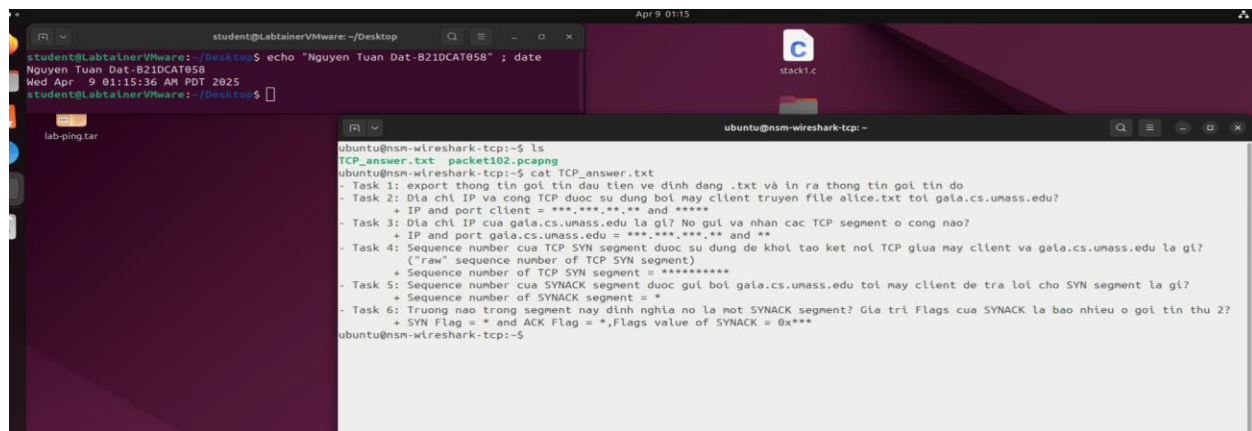
Nội dung thực hành

Khởi động bài lab:

Vào terminal, gõ:

labtainer nsm-wireshark-tcp

(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)



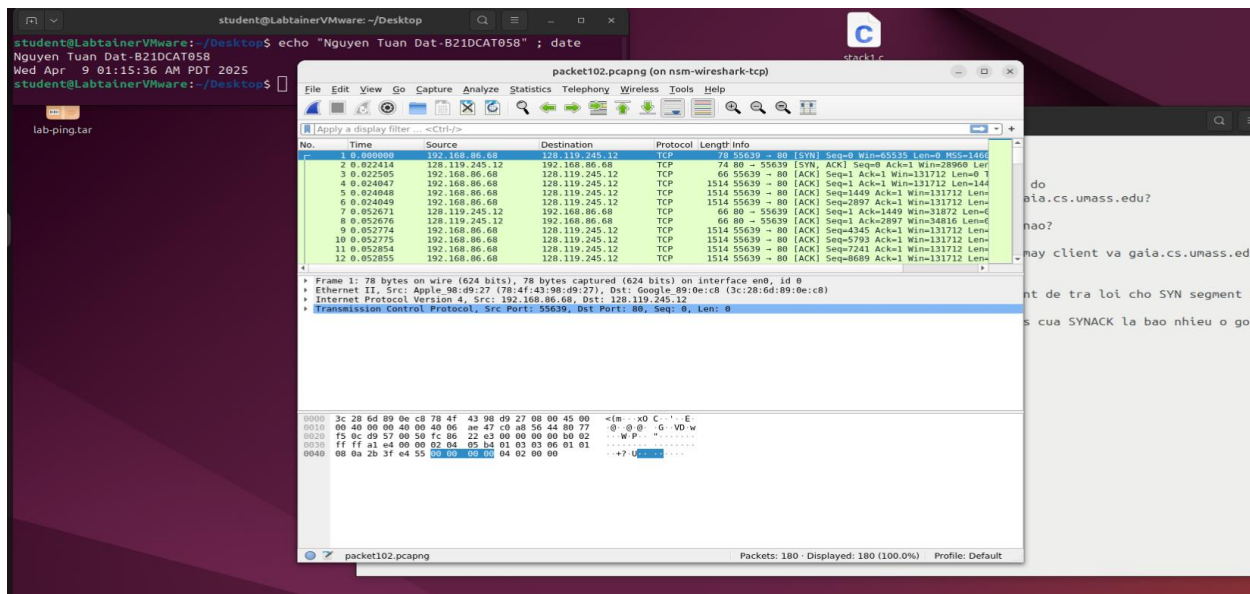
```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware: ~/Desktop$ echo "Nguyen Tuan Dat-B21DCAT058" ; date
Nguyen Tuan Dat-B21DCAT058
Wed Apr  9 01:15:36 AM PDT 2025
student@LabtainerVMware: ~/Desktop$

lab-ping.tar

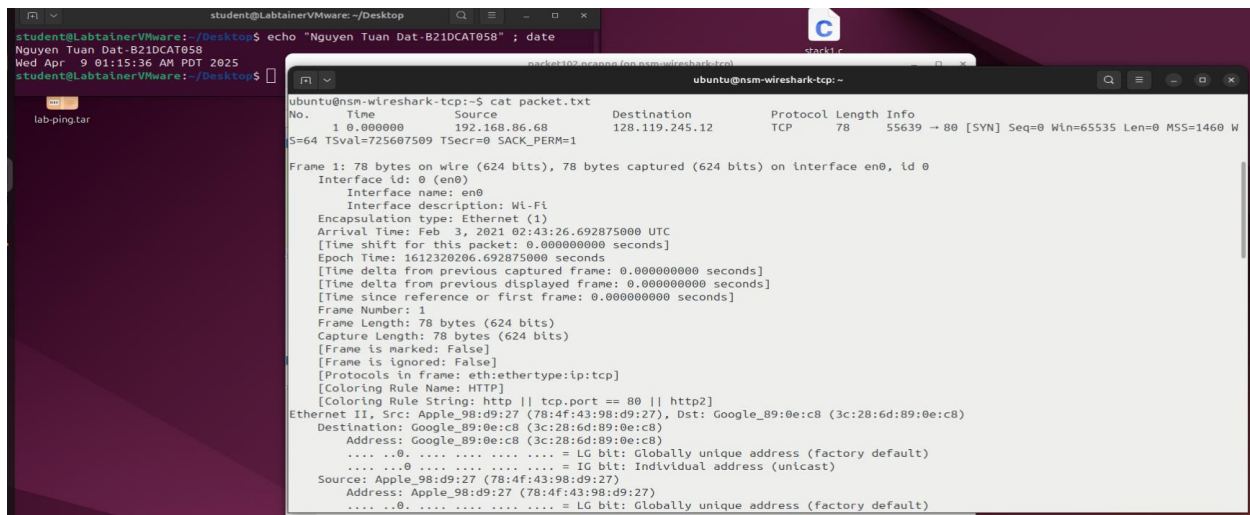
ubuntu@nsm-wireshark-tcp:~$ ls
TCP_answer.txt  packet102.pcapng
ubuntu@nsm-wireshark-tcp:~$ cat TCP_answer.txt
- Task 1: export thông tin gói tin đầu tiên về định dạng .txt và in ra thông tin gói tin đó
- Task 2: Địa chỉ IP và cổng TCP được sử dụng bởi máy client truyền file alice.txt tới gaia.cs.umass.edu?
+ IP and port client = ***,***,**,* and ****
- Task 3: Địa chỉ IP của gaia.cs.umass.edu là gì? Nó gửi và nhận các TCP segment ở cổng nào?
+ IP and port gaia.cs.umass.edu = ***,***,***,** and **
- Task 4: Sequence number của TCP SYN segment được sử dụng để khởi tạo kết nối TCP giữa máy client và gaia.cs.umass.edu là gì?
("raw" sequence number of TCP SYN segment)
+ Sequence number of TCP SYN segment = *****
- Task 5: Sequence number của SYNACK segment được gửi bởi gaia.cs.umass.edu tới máy client để trả lời cho SYN segment là gì?
+ Sequence number of SYNACK segment = *
- Task 6: Trường nào trong segment này định nghĩa nó là một SYNACK segment? Giá trị Flags của SYNACK là bao nhiêu ở gói tin thu 2?
+ SYN Flag = * and ACK Flag = *,Flags value of SYNACK = 0x***
ubuntu@nsm-wireshark-tcp:~$
```

Sau khi khởi động xong một terminal ảo sẽ xuất hiện đại diện cho máy khởi chạy wireshark: nsm-wireshark-tcp và điền kết quả sau khi phân tích các gói tin .Trên terminal khởi chạy wireshark bằng câu lệnh:

Wireshark



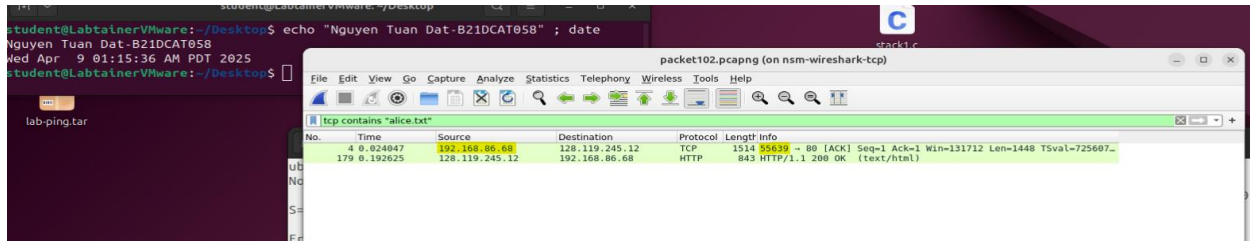
Task 1: export thông tin gói tin đầu tiên về định dạng .txt và in ra thông tin gói tin đó



Task 2: Địa chỉ IP và cổng TCP được sử dụng bởi máy client truyền file alice.txt tới gaia.cs.umass.edu?

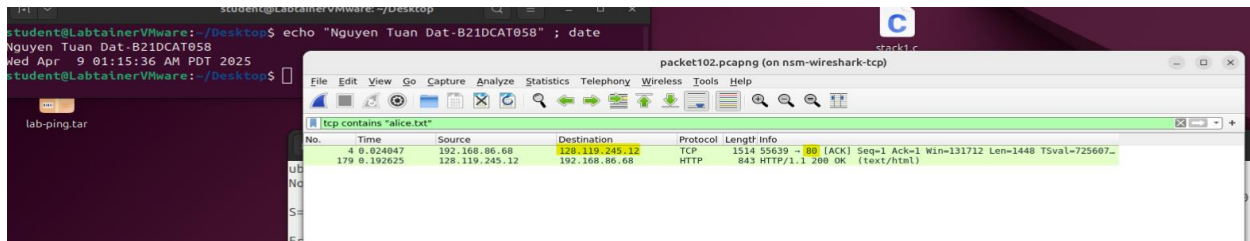
Sử dụng bộ lọc **tcp contains "alice.txt"**

➔ IP and port client = **192.168.86.68** and **55639**



Task 3: Địa chỉ IP của gaia.cs.umass.edu là gì? Nó gửi và nhận các TCP segment ở cổng nào?

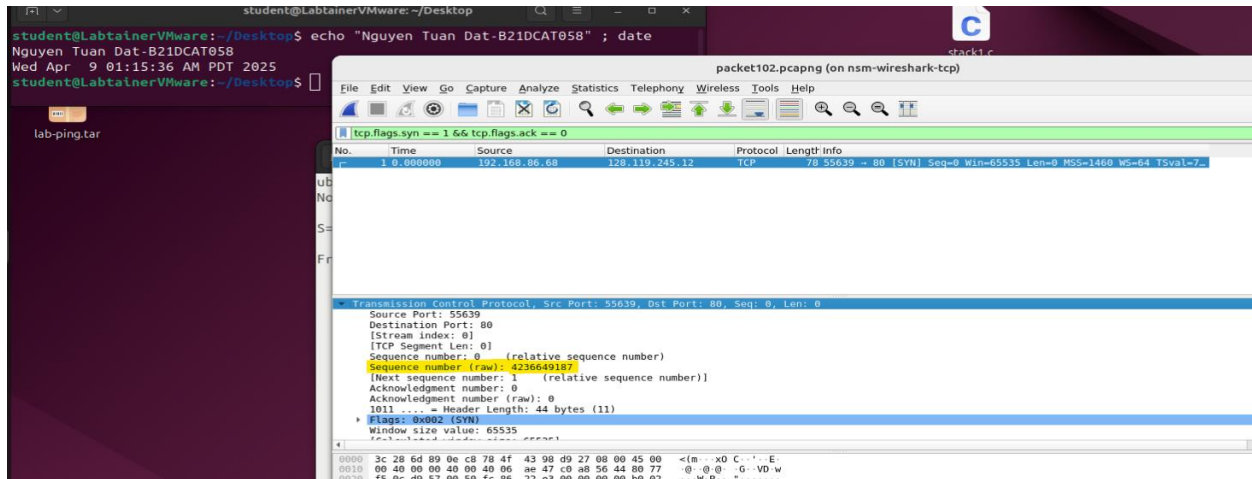
➔ IP and port gaia.cs.umass.edu **192.168.245.12** and **80**



Task 4: Sequence number của TCP SYN segment được sử dụng để khởi tạo kết nối TCP giữa máy client và gaia.cs.umass.edu là gì? ("raw" sequence number of TCP SYN segment)

Sử dụng bộ lọc `tcp.flags.syn == 1 && tcp.flags.ack == 0`

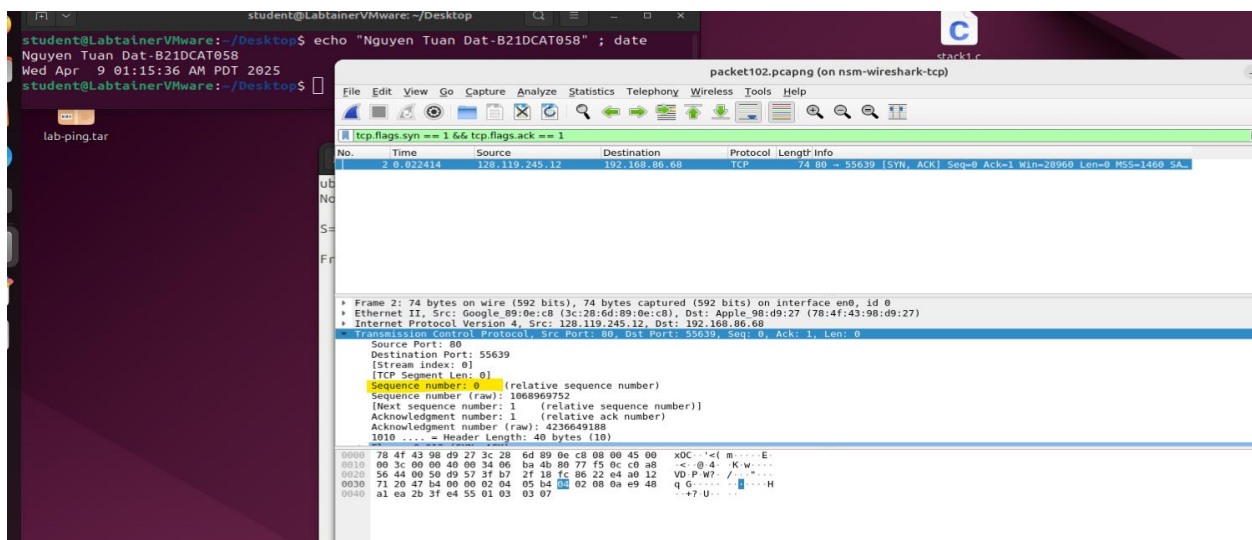
➔ Sequence number of TCP SYN segment = 4236649187



Task 5: Sequence number của SYNACK segment được gửi bởi gaia.cs.umass.edu tới máy client để trả lời cho SYN segment là gì?

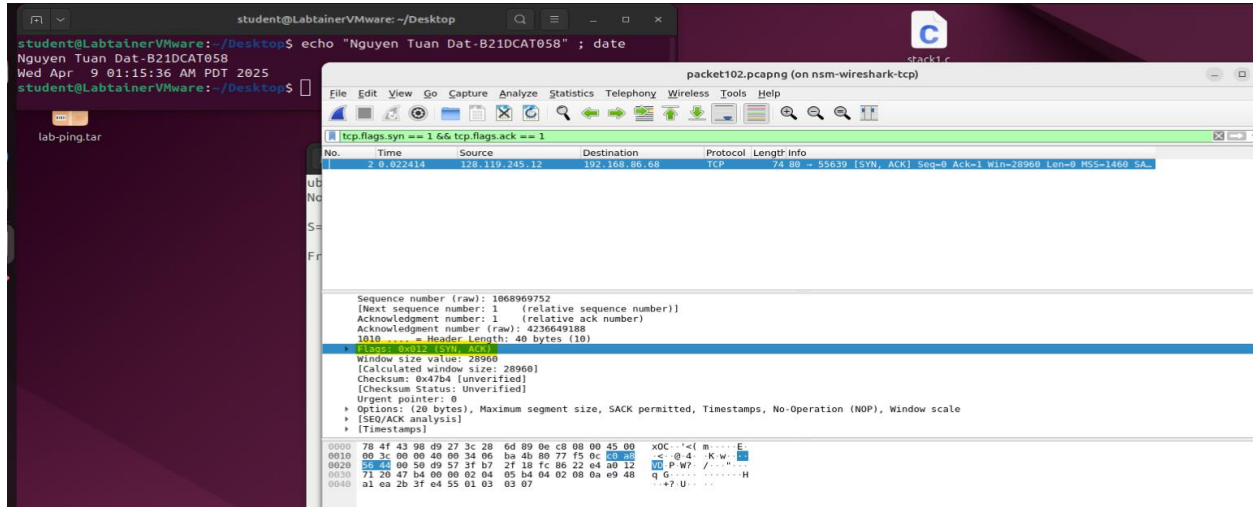
Sử dụng bộ lọc `tcp.flags.syn == 1 && tcp.flags.ack == 1`

➔ Sequence number of SYNACK segment = 0



Task 6: Truong nao trong segment nay dinh nghia no la mot SYNACK segment? Gia tri Flags cua SYNACK la bao nhieu o goi tin thu 2?

➔ SYN Flag = 1 and ACK Flag = 1, Flags value of SYNACK = 0x012



Kết thúc bài lab:

Checkwork

