

Nội dung và hướng dẫn bài thực hành

Mục đích

Giúp sinh viên nắm vững các khái niệm cơ bản mà còn nâng cao khả năng nhận diện các nguy cơ bảo mật tiềm ẩn trong hệ thống mạng, từ đó biết cách phòng chống và bảo vệ hệ thống một cách hiệu quả.

Yêu cầu đối với sinh viên

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

Nội dung thực hành

Khởi động bài lab:

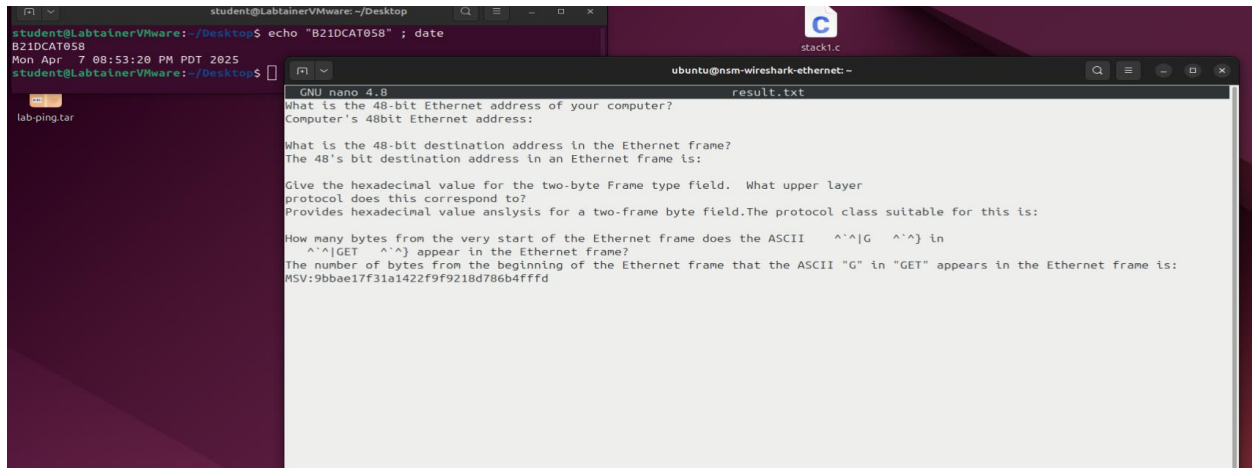
Vào terminal, gõ:

```
labtainer -r nsm-wireshark-ethernet
```

(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 một terminal ảo sẽ xuất hiện. Trên terminal thực hiện mở file result.txt để điền kết quả:

```
sudo nano result.txt
```

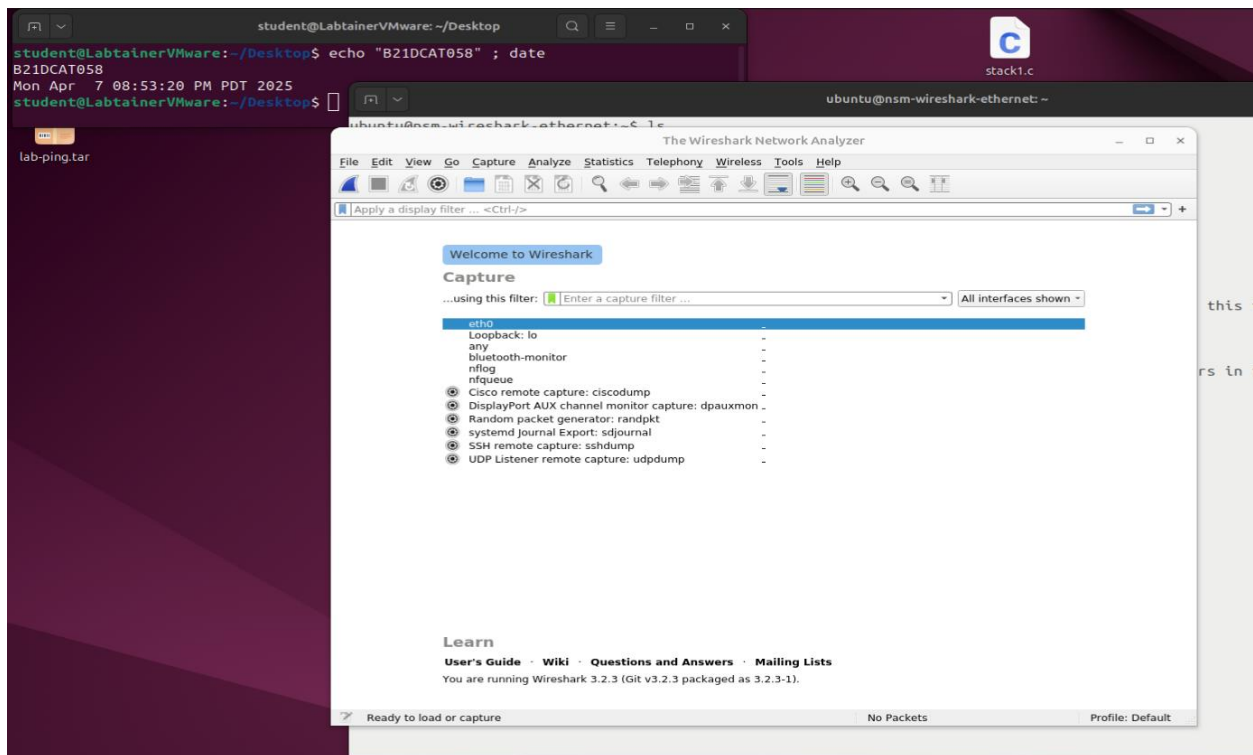


Bài lab đã tạo sẵn 1 file ethernet.pcap chứa nội dung các gói tin đã chụp. Chúng ta sẽ thực hiện mở file này bằng wireshark và thực hiện phân tích và trả lời câu hỏi trong file result.txt

Từ file ethernet.pcap ta sẽ tìm được các gói tin phù hợp với câu hỏi

Câu trả lời sẽ phải điền vào file *result.txt*.

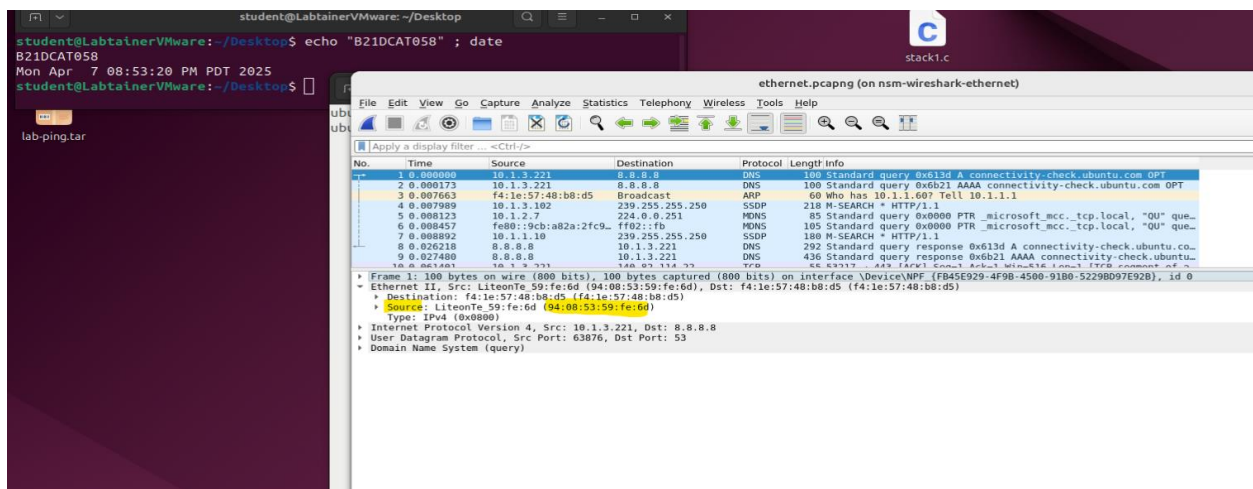
Thực hiện chạy lệnh “wireshark & ” để mở wireshark và phân tích gói tin:



Task 1: Địa chỉ MAC 48-bit của máy

➔ Computer's 48bit Ethernet address:94:08:53:59:fe:6d

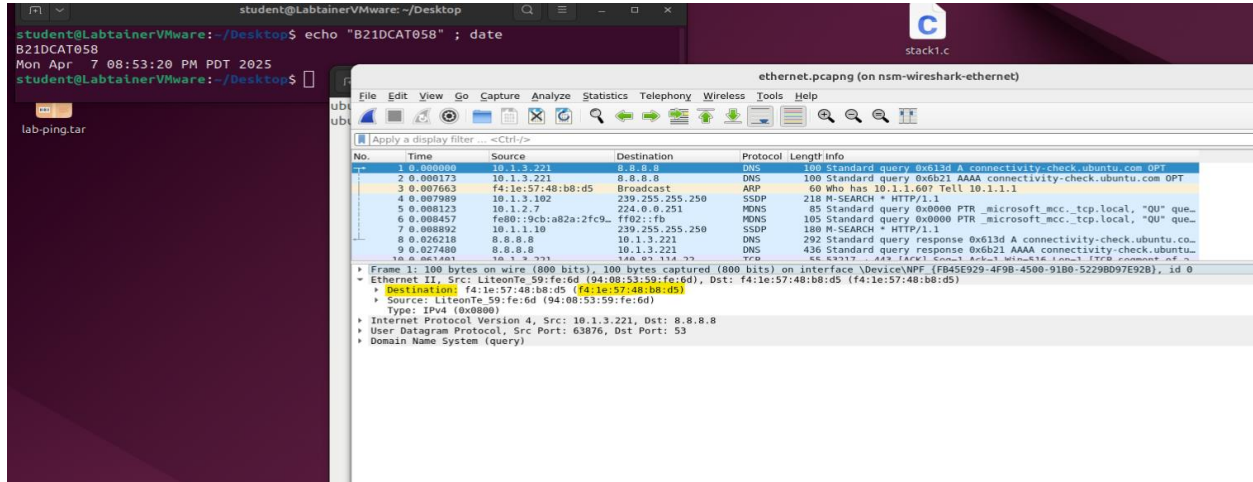
Trường **Source** trong phần Ethernet là địa chỉ MAC



Task 2: Địa chỉ MAC đích trong khung Ethernet

➔ The 48's bit destination address in an Ethernet frame is: **f4:1e:57:48:b8:d5**

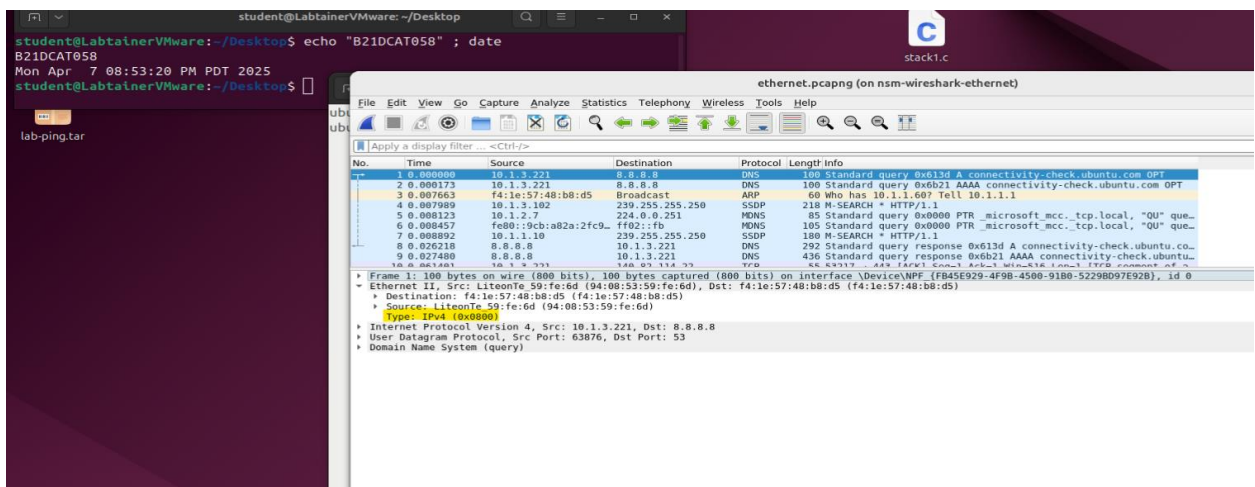
Trường **Destination** trong phần Ethernet chính là địa chỉ đích



Task 3: Giá trị Hex 2 byte của Frame Type + giao thức ứng với nó

➔ Provides hexadecimal value analysis for a two-frame byte field. The protocol class suitable for this is: **0x0800**

Trong phần **Ethernet II**, xem mục **Type**



Task 4: Vị trí byte chứa ASCII “G” trong “GET”

➔ The number of bytes from the beginning of the Ethernet frame that the ASCII "G" in "GET" appears in the Ethernet frame is:54

Chọn gói HTTP chứa phương thức “GET”, vào khung Packet Bytes → bên phải có chuỗi ASCII, tìm chữ G trong “GET” → Di chuột lên, phía dưới sẽ hiển thị byte offset

The image shows a terminal window on the left and a Wireshark packet capture window on the right. The terminal window displays the command `echo "B21DCAT058" ; date` and the output `Mon Apr 7 08:53:20 PM PDT 2025`. The Wireshark window shows a packet capture of an HTTP GET request. The packet list on the left shows a packet of type HTTP. The packet details pane on the right shows the request method as GET. The packet bytes pane at the bottom shows the raw data of the packet, with the ASCII string "GET" highlighted. The byte offset for the 'G' is 54.

Kết thúc bài lab:

The image shows a terminal window with the following commands and output:

```
student@LabtainerVMware:~/Desktop$ echo "B21DCAT058" ; date
B21DCAT058
Mon Apr 7 08:53:20 PM PDT 2025
student@LabtainerVMware:~/Desktop$

ubuntu@nsm-wireshark-ethernet:~$ cat result.txt
What is the 48-bit Ethernet address of your computer?
Computer's 48bit Ethernet address:94:08:53:59:fe:6d

What is the 48-bit destination address in the Ethernet frame?
The 48's bit destination address is:f4:1e:57:48:b8:d5

Give the hexadecimal value for the two-byte Frame type field. What upper layer
protocol does this correspond to?
Provides hexadecimal value anlystis for a two-frame byte field.The protocol class suitable for this is:0x0800

How many bytes from the very start of the Ethernet frame does the ASCII "G" in
"GET" appear in the Ethernet frame?
The number of bytes from the beginning of the Ethernet frame that the ASCII "G" in "GET" appears in the Ethernet frame is:54
MSV:9bbae17f31a1422f9f9218d786b4fffd
ubuntu@nsm-wireshark-ethernet:~$
```

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

`stoplab nsm-wireshark-ethernet`

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:

startlab -r nsm-wireshark-ethernet

```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo "B21DCAT058" ; date
B21DCAT058
Mon Apr 7 08:53:20 PM PDT 2025
student@LabtainerVMware:~/Desktop$
```

lab-ping.tar

```
student@LabtainerVMware: ~/labtainer/labtainer-student
student@LabtainerVMware: ~/labtainer/labtainer-student
6b5a151afeb1: Pull complete
Digest: sha256:468955d5b8b83dd293358c388b231d2a6cd94418c4242d231d6f45e125f21f2d
Status: Downloaded newer image for trangninh/nsm-wireshark-ethernet.nsm-wireshark-ethernet.student:latest

Please enter your e-mail address: [b21dcat058]
Started 1 containers, 1 completed initialization. Done.

The lab manual for this lab is at:
  file:///home/student/labtainer/trunk/labs/nsm-wireshark-ethernet/docs/nsm-wireshark-ethernet.pdf
Right click on the above link to open the lab manual.

Press <enter> to start the lab

student@LabtainerVMware: ~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/nsm-wireshark-ethernet
Successfully copied 167kB to nsm-wireshark-ethernet-lgrader:/home/instructor/b21dcat058.nsm-wireshark-ethernet.lab
Successfully copied 2.05kB to /home/student/labtainer_xfer/nsm-wireshark-ethernet
Labname nsm-wireshark-ethernet

Student | personalization | address | hex_value | byte_number |
=====|=====|=====|=====|=====|
b21dcat058 | Y | Y | Y | Y |
What is automatically assessed for this lab:

personalization: used wireshark to extract the proper packet
```