

Nội dung và hướng dẫn bài thực hành

Mục đích

Phân tích gói tin FTP để hiểu rõ cấu trúc và cơ chế hoạt động của giao thức.

Sử dụng công cụ Tshark để khai thác thông tin từ file PCAP như username, chế độ truyền file, và thời gian truyền dữ liệu.

Yêu cầu đối với sinh viên

Nắm vững các khái niệm cơ bản về giao thức FTP.

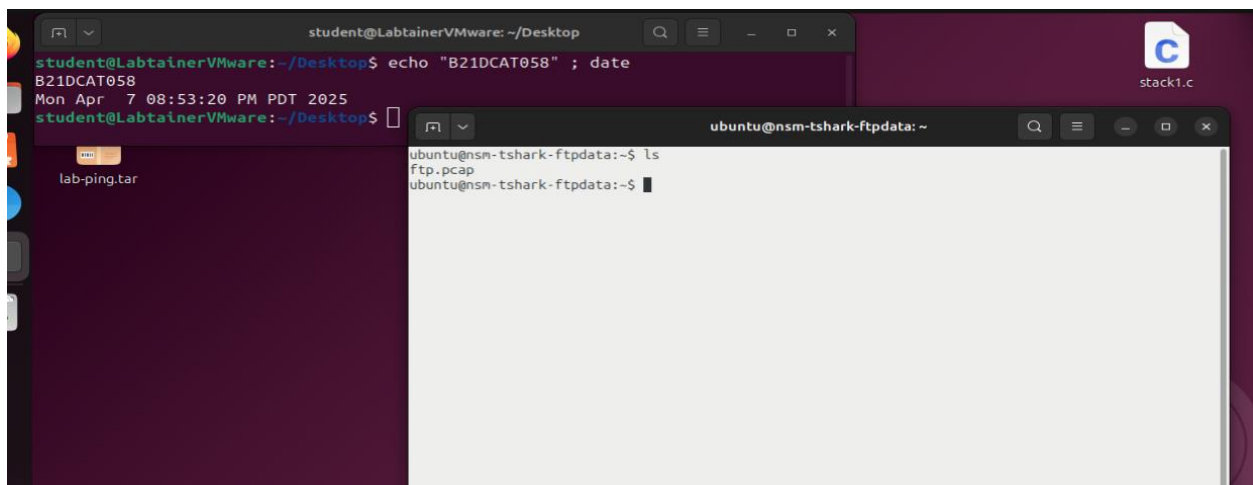
Biết cách sử dụng hệ điều hành Ubuntu và công cụ Tshark.

Nội dung thực hành

Khởi động bài lab:

Vào terminal, gõ:

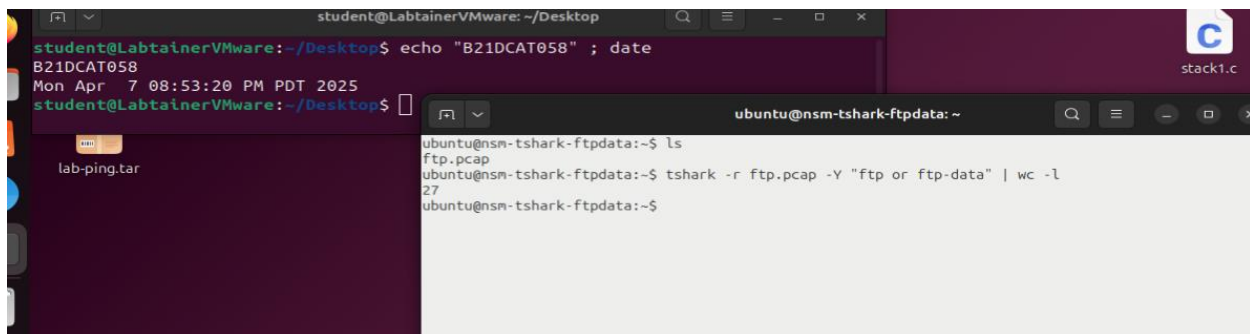
startlab nsm-tshark-ftpdata



(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, đại diện cho máy chủ: *nsm-tshark-ftpdata*. Bài lab đã tạo sẵn 1 file *ftp.pcap* có chứa dữ liệu cần phân tích. Trên terminal thực hiện lệnh đọc ra file *ftp.pcap*, sau đó lọc lấy các gói tin FTP-Control và FTP-Data, sử dụng thêm điều kiện ràng buộc "*| wc -l*" để đếm tổng số gói tin FTP có trong file. ví dụ:

tshark -r ftp.pcap -Y "ftp or ftp-data" | wc -l



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

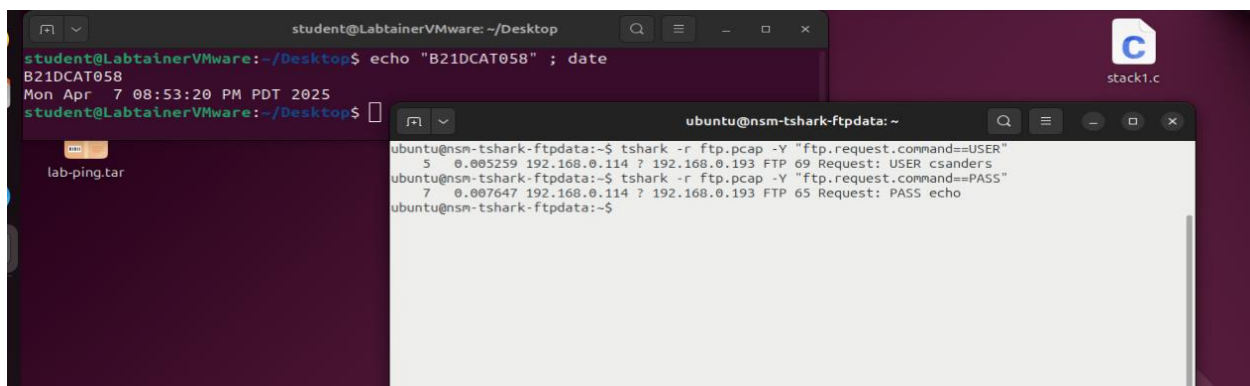
lab-ping.tar

ubuntu@nsm-tshark-ftpdata: ~
ubuntu@nsm-tshark-ftpdata:~$ ls
ftp.pcap
ubuntu@nsm-tshark-ftpdata:~$ tshark -r ftp.pcap -Y "ftp or ftp-data" | wc -l
27
ubuntu@nsm-tshark-ftpdata:~$
```

Sau đó, tìm kiếm tên đăng nhập (username) mà client sử dụng để kết nối tới server. Trong giao thức FTP, khi client gửi lệnh USER, nó sẽ truyền tên đăng nhập tới server. Server sẽ xác minh tên này trước khi yêu cầu mật khẩu qua lệnh PASS. Sử dụng lệnh “ftp.request.command==USER” để lọc gói tin chứa tên đăng nhập của client, ví dụ:

tshark -r ftp.pcap -Y "ftp.request.command==USER "

Cũng có thể lọc gói tin chứa mật khẩu của client nếu thay lệnh “USER” bằng “PASS”



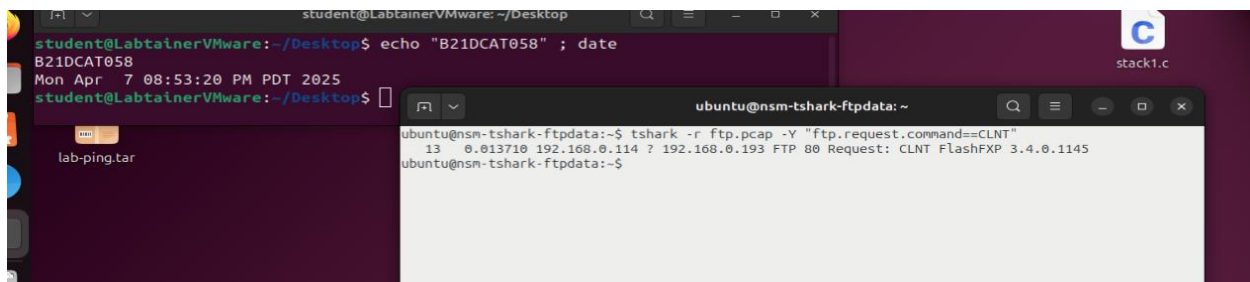
```
student@LabtainerVMware:~/Desktop
student@LabtainerVMware:~/Desktop$ echo "B21DCAT058" ; date
B21DCAT058
Mon Apr 7 08:53:20 PM PDT 2025
student@LabtainerVMware:~/Desktop$

lab-ping.tar

ubuntu@nsm-tshark-ftpdata: ~
ubuntu@nsm-tshark-ftpdata:~$ tshark -r ftp.pcap -Y "ftp.request.command==USER"
5 0.005259 192.168.0.114 ? 192.168.0.193 FTP 69 Request: USER csanders
ubuntu@nsm-tshark-ftpdata:~$ tshark -r ftp.pcap -Y "ftp.request.command==PASS"
7 0.007647 192.168.0.114 ? 192.168.0.193 FTP 65 Request: PASS echo
ubuntu@nsm-tshark-ftpdata:~$
```

Tiếp đến, xác định phần mềm FTP và phiên bản được sử dụng bởi client. Giao thức FTP có thể sử dụng lệnh “CLNT” để client thông báo tên phần mềm và phiên bản đang sử dụng. Thông tin này giúp server hiểu rõ đặc điểm của client, hỗ trợ xử lý tương thích khi cần. Sử dụng lệnh “ftp.request.command==CLNT” để lọc các gói tin chứa thông tin về phiên bản phần mềm FTP, ví dụ:

tshark -r ftp.pcap -Y "ftp.request.command==CLNT "



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

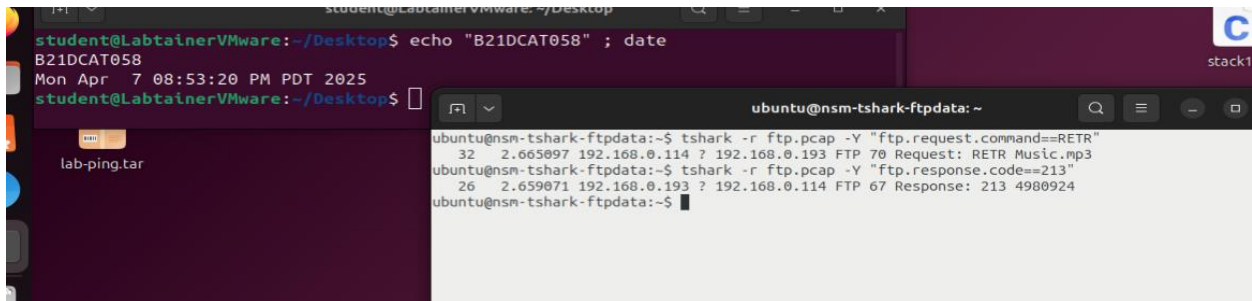
lab-ping.tar

ubuntu@nsm-tshark-ftpdata: ~
ubuntu@nsm-tshark-ftpdata:~$ tshark -r ftp.pcap -Y "ftp.request.command==CLNT"
13 0.013710 192.168.0.114 ? 192.168.0.193 FTP 80 Request: CLNT FlashFXP 3.4.0.1145
ubuntu@nsm-tshark-ftpdata:~$
```

Tiếp đến, ta tìm hiểu lệnh RETR: được client gửi đến server để yêu cầu tải xuống một tệp tin. Mã phản hồi 213: được server gửi tới để thông báo kích thước của tệp tin trong byte. Hai thông tin này kết hợp lại giúp xác định tên và kích thước file được truyền tải, sử dụng lệnh "RETR" và "213" để lọc các gói tin này, ví dụ:

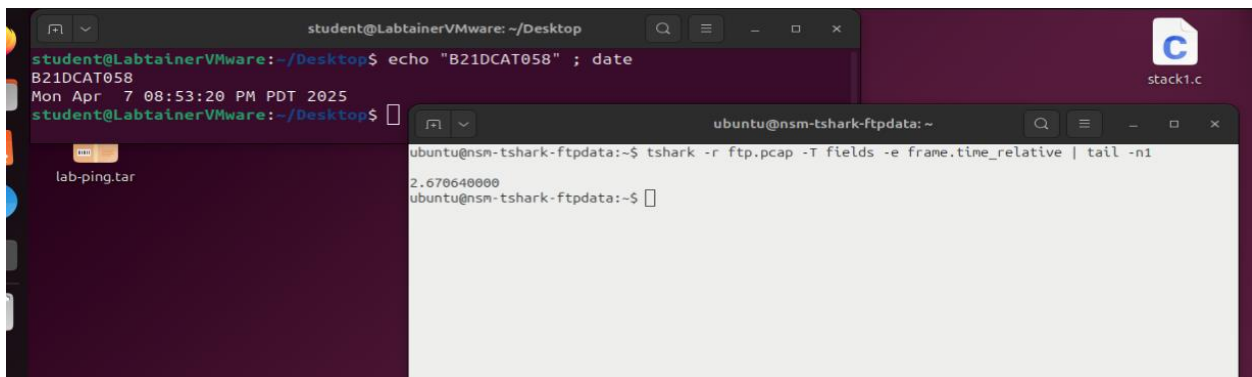
```
tshark -r ftp.pcap -Y "ftp.request.command==RETR"
```

```
tshark -r ftp.pcap -Y ftp.response.code==213
```



Tiếp theo cùng xác định tổng thời gian của phiên làm việc từ khi bắt đầu đến khi kết thúc. Thời gian phiên FTP bao gồm tất cả các bước như thiết lập kết nối, truyền dữ liệu, và kết thúc kết nối. Dữ liệu này giúp đánh giá hiệu suất của phiên truyền tải, sử dụng lệnh "-e frame.time_relative" kèm điều kiện "| tail -n1" để in ra kết quả, ví dụ:

```
tshark -r ftp.pcap -T fields -e frame.time_relative | tail -n1
```



Các gói tin FTP-DATA chứa dữ liệu thực tế được truyền giữa client và server. Kích thước trung bình của gói tin giúp đánh giá hiệu quả sử dụng băng thông trong phiên FTP. Để tính kích thước trung bình của các gói tin thuộc kênh dữ liệu FTP-DATA, sử dụng lệnh "-e frame.len", ví dụ:

```
tshark -r ftp.pcap -Y "ftp-data" -T fields -e frame.len
```

The screenshot shows a terminal window with two panes. The left pane is titled 'student@LabtainerVMware: ~/Desktop' and contains the following text:
student@LabtainerVMware:~/Desktop\$ echo "B21DCAT058" ; date
B21DCAT058
Mon Apr 7 08:53:20 PM PDT 2025
student@LabtainerVMware:~/Desktop\$
Below this text is a file icon labeled 'lab-ping.tar'. The right pane is titled 'ubuntu@nsm-tshark-ftpdata: ~' and contains the command:
ubuntu@nsm-tshark-ftpdata:~\$ tshark -r ftp.pcap -Y "ftp-data" -T fields -e frame.len
The output of the command is:
1506
1506
1506
1506
ubuntu@nsm-tshark-ftpdata:~\$

The screenshot shows a terminal window with two panes. The left pane is identical to the one in the previous image. The right pane is titled 'ubuntu@nsm-tshark-ftpdata: ~' and contains the following commands and output:
ubuntu@nsm-tshark-ftpdata:~\$ tshark -r ftp.pcap -Y "ftp-data" -T fields -e frame.len > ftp_data_len.txt
ubuntu@nsm-tshark-ftpdata:~\$ awk '{ total += \$1; count++ } END { print total/count }' ftp_data_len.txt
1506
ubuntu@nsm-tshark-ftpdata:~\$

Cuối cùng, xác định chế độ truyền file được sử dụng trong phiên FTP, giao thức FTP hỗ trợ hai chế độ truyền tệp chính: ASCII và Binary. Chế độ truyền tệp được thiết lập qua lệnh “TYPE”, sử dụng lệnh này để lọc gói tin có chứa chế độ truyền file, ví dụ:

tshark -r ftp.pcap -Y "ftp.request.command==TYPE"

The screenshot shows a terminal window with two panes. The left pane is identical to the previous images. The right pane is titled 'ubuntu@nsm-tshark-ftpdata: ~' and contains the command:
ubuntu@nsm-tshark-ftpdata:~\$ tshark -r ftp.pcap -Y "ftp.request.command==TYPE"
The output of the command is:
23 2.652615 192.168.0.114 ? 192.168.0.193 FTP 62 Request: TYPE I
ubuntu@nsm-tshark-ftpdata:~\$

Kết thúc bài lab:

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

```
stoplab nsm-tshark-ftpdata
```

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-tshark-ftpdata
```

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

```
student@LabtainerVMware: ~/labtainer/labtainer-student
student@LabtainerVMware:~/labtainer/labtainer-student$ what is automatically assessed for this lab:
ftp_packet_cnt: How many FTP control and FTP data packets in the pcap file?
ftp_user: What username does the client use to log in?
ftp_version: What FTP software and version is the client using?
ftp_packet_size: What is the size of the requested file to be downloaded?
ftp_trf_time: What is the total duration of the file transfer session?
ftp_packet_len: What is the average size of each FTP-DATA packet?
ftp_trf_mode: What file transfer mode is being used (ASCII or Binary)?

student@LabtainerVMware:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/nsm-tshark-ftpdata
Successfully copied 49.2kB to nsm-tshark-ftpdata-igrader:/home/instructor/b21dc058.nsm-tshark-ftpdata.lab
Successfully copied 2.56kB to /home/student/labtainer_xfer/nsm-tshark-ftpdata
Labname nsm-tshark-ftpdata

Student | ftp_packet_cnt | ftp_user | ftp_version | ftp_packet_size | ftp_trf_time | ftp_packet_len | ftp_trf_mode |
-----|-----|-----|-----|-----|-----|-----|-----|
b21dc058 | Y | Y | Y | Y | Y | Y | Y |

what is automatically assessed for this lab:
ftp_packet_cnt: How many FTP control and FTP data packets in the pcap file?
ftp_user: What username does the client use to log in?
ftp_version: What FTP software and version is the client using?
ftp_packet_size: What is the size of the requested file to be downloaded?
ftp_trf_time: What is the total duration of the file transfer session?
ftp_packet_len: What is the average size of each FTP-DATA packet?
ftp_trf_mode: What file transfer mode is being used (ASCII or Binary)?

student@LabtainerVMware:~/labtainer/labtainer-student$ stoplab
Results stored in directory: /home/student/labtainer_xfer/nsm-tshark-ftpdata
student@LabtainerVMware:~/labtainer/labtainer-student$
```