ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH

----ꕥ🕮ꕥ----

MẠNG MÁY TÍNH TN (CO3094)

BÀI TẬP LAB 3B

WIRESHARK UDP

LỚP: L09

GVHD: Bùi Xuân Giang

Sinh viên thực hiện

Nguyễn Tấn Tài : 2212990

Thành phố Hồ Chí Minh, tháng 9 năm 2024

Trong bài lab này, chúng ta sẽ xem qua giao thức truyền tải UDP. Như chúng ta đã thấy trong Chương 3 của sách giáo khoa, UDP là một giao thức đơn giản, không cầu kỳ. Bạn có thể muốn đọc lại mục 3.3 trong sách trước khi làm bài lab này. Bởi vì UDP đơn giản và dễ hiểu, chúng ta sẽ có thể hoàn thành nhanh chóng trong bài lab này. Nếu bạn có hẹn trong vòng 30 phút tới, bạn cũng không cần lo lắng, vì bạn sẽ hoàn thành bài lab này với nhiều thời gian rảnh.

Ở giai đoạn này, bạn nên đã là một chuyên gia Wireshark. Vì vậy, chúng tôi sẽ không liệt kê rõ các bước như trong các bài lab trước. Đặc biệt, chúng tôi sẽ không cung cấp ảnh minh họa cho tất cả các bước.

Nhiệm vụ

Bắt đầu bắt gói tin trong Wireshark và sau đó thực hiện hành động nào đó để máy chủ của bạn gửi và nhận một số gói UDP. Rất có thể chỉ cần làm không gì khác (ngoài việc bắt các gói tin qua Wireshark) mà một số gói UDP do người khác gửi sẽ xuất hiện trong bản ghi của bạn. Đặc biệt, giao thức Quản lý Mạng Đơn giản (SNMP – xem phần 5.7 trong sách giáo khoa) gửi các thông điệp SNMP bên trong UDP, vì vậy có thể bạn sẽ tìm thấy một số thông điệp SNMP (và do đó các gói UDP) trong bản ghi của bạn.

Sau khi bắt gói tin, hãy đặt bộ lọc gói tin của bạn để Wireshark chỉ hiển thị các gói UDP được gửi và nhận tại máy chủ của bạn. Chọn một trong các gói UDP này và kiểm tra các trường UDP trong cửa sổ chi tiết. Nếu bạn không thể tìm thấy gói UDP hoặc không thể chạy Wireshark trên kết nối mạng trực tiếp, bạn có thể tải về bản ghi gói chứa một số gói UDP.

Bất cứ khi nào có thể, khi trả lời câu hỏi dưới đây, bạn nên nộp kèm một bản in của gói tin (hoặc các gói tin) trong bản ghi mà bạn đã sử dụng để trả lời câu hỏi. Chú thích trên bản in để giải thích câu trả lời của bạn. Để in một gói tin, sử dụng File -> Print, chọn Selected packet only, chọn Packet summary line, và chọn lượng thông tin tối thiểu của chi tiết gói tin mà bạn cần để trả lời câu hỏi.

1. **Chọn một gói UDP từ bản ghi của bạn. Từ gói này, xác định có bao nhiêu trường trong tiêu đề UDP. (Bạn không nên tra cứu trong sách giáo khoa! Trả lời các câu hỏi này trực tiếp từ những gì bạn quan sát được trong bản ghi gói tin.) Liệt kê các trường này.**

udp

No.	Time	Source	Destination	Protocol	Lengtl	Info
1	12:39:52.896793	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
2	12:39:52.913753	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
11	12:39:55.913764	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
12	12:39:55.930920	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
13	12:39:58.930512	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
14	12:39:58.947601	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
15	12:40:01.947256	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
16	12:40:01.964285	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
17	12:40:04.964007	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
18	12:40:04.981940	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
19	12:40:05.217358	192.168.1.100	192.168.1.255	NBNS	92	Name query NB NOHO<20>
20	12:40:05.217393	192.168.1.102	192.168.1.100	NBNS	104	Name query response NB 192.168.1.102
56	12:40:07.981721	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
57	12:40:07.999107	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
58	12:40:10.753003	192.168.1.102	192.168.1.255	NBNS	92	Name query NB WORKGROUP<1b>
59	12:40:10.999449	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
60	12:40:11.016762	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
69	12:40:11.502246	192.168.1.102	192.168.1.255	NBNS	92	Name query NB WORKGROUP<1b>
71	12:40:12.252279	192.168.1.102	192.168.1.255	NBNS	92	Name query NB WORKGROUP<1b>
72	12:40:14.017174	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
73	12:40:14.034659	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0

```
No.     Time                Source                Destination           Protocol Length Info
      1 12:39:52.896793     192.168.1.102         192.168.1.104         SNMP     92     get-request
1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: HewlettPacka_61:eb:ed (00:30:c1:61:eb:ed)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.104
User Datagram Protocol, Src Port: 4334, Dst Port: 161
    Source Port: 4334
    Destination Port: 161
    Length: 58
    Checksum: 0x65f8 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Stream Packet Number: 1]
    [Timestamps]
        [Time since first frame: 0.000000000 seconds]
        [Time since previous frame: 0.000000000 seconds]
    UDP payload (50 bytes)
Simple Network Management Protocol
[Community ID: 1:RCQochaFG8OuYkHBXO2m41aaQoo=]
```

Các trường tiêu đề UDP là:

- Source Port (Cổng nguồn): 4334
- Destination Port (Cổng đích): 161
- Length (Chiều dài): 58 bytes (đây là chiều dài toàn bộ datagram UDP, bao gồm cả phần tiêu đề và dữ liệu)
- Checksum (Mã kiểm tra): 0x65f8 (chưa được xác minh – unverified)

2. **Bằng cách tham khảo thông tin hiển thị trong cửa sổ nội dung gói tin của Wireshark cho gói tin này, xác định chiều dài (tính bằng byte) của từng trường trong tiêu đề UDP.**

Dựa trên cấu trúc tiêu chuẩn của tiêu đề UDP:

- Source Port: 2 bytes
- Destination Port: 2 bytes
- Length: 2 bytes
- Checksum: 2 bytes

Tổng chiều dài của tiêu đề UDP là 8 bytes.

3. **Giá trị trong trường Length (Chiều dài) là chiều dài của cái gì? (Bạn có thể tham khảo văn bản trong sách để trả lời câu hỏi này). Xác minh câu trả lời của bạn bằng gói UDP đã bắt được.**

Trường Length trong tiêu đề UDP đại diện cho tổng chiều dài của toàn bộ datagram UDP, bao gồm cả:

- Phần tiêu đề UDP (8 byte)
- Và phần dữ liệu (payload): 50 byte.

Vì vậy, trường Length trong tiêu đề UDP luôn là tổng chiều dài của toàn bộ gói tin UDP, bao gồm cả tiêu đề và dữ liệu.

4. **Số byte tối đa có thể bao gồm trong một gói dữ liệu UDP là bao nhiêu? (Gợi ý: câu trả lời cho câu hỏi này có thể được xác định bằng câu trả lời cho câu hỏi 2 ở trên).**

Trường Length trong tiêu đề UDP có độ dài 2 byte, nghĩa là giá trị tối đa của trường này có thể lên đến 65535 (vì 2 byte có thể biểu diễn giá trị từ 0 đến $2^{16} - 1$).

Tuy nhiên, trường Length này bao gồm cả:

- Phần tiêu đề UDP (cố định là 8 byte).
- Phần dữ liệu (payload).

Vì vậy, số byte tối đa có thể chứa trong phần dữ liệu của gói UDP sẽ được tính bằng cách trừ đi độ dài của tiêu đề UDP (8 byte) từ tổng chiều dài tối đa (65535 byte):

Số byte tối đa trong dữ liệu = 65535 − 8= **65527 bytes**

5. **Số cổng nguồn lớn nhất có thể là bao nhiêu? (Gợi ý: xem gợi ý trong câu 4).**

Trường Source Port (Cổng nguồn) trong tiêu đề UDP có độ dài 2 byte. Vì 2 byte có thể biểu diễn các giá trị từ 0 đến $2^{16} - 1$, số cổng nguồn lớn nhất có thể là:

Số cổng nguồn lớn nhất: $2^{16} - 1$ = **65535**

6. **Số giao thức của UDP là gì? Hãy đưa ra câu trả lời của bạn dưới dạng số thập lục phân và thập phân. Để trả lời câu hỏi này, bạn cần xem trường Protocol trong datagram IP chứa đoạn UDP này (xem Hình 4.13 trong sách giáo khoa, và phần thảo luận về các trường tiêu đề IP).**

Số giao thức (Protocol Number) của UDP được xác định trong tiêu đề IP, tại trường Protocol của tiêu đề IP (chỉ ra giao thức lớp trên mà IP đang sử dụng). Trong trường hợp của UDP, giá trị này là:

- Số thập phân: 17
- Số thập lục phân: 0x11

Cách xác định

- Trong Wireshark, khi bạn chọn một gói tin UDP, mở rộng phần Internet Protocol Version 4 (hoặc IPv6 nếu bạn đang sử dụng IPv6).
- Tìm trường Protocol trong phần tiêu đề IP.
- Trường này sẽ hiển thị giá trị của giao thức UDP, là 17 (thập phân) hoặc 0x11 (thập lục phân).

7. **Kiểm tra một cặp gói UDP trong đó máy chủ của bạn gửi gói UDP đầu tiên và gói UDP thứ hai là phản hồi cho gói UDP đầu tiên này. (Gợi ý: đối với một gói thứ hai được gửi để phản hồi một gói đầu tiên, người gửi của gói đầu tiên nên là đích đến của gói thứ hai). Mô tả mối quan hệ giữa số cổng trong hai gói tin này.**

```
No.     Time               Source                Destination           Protocol Length Info
      1 12:39:52.896793    192.168.1.102         192.168.1.104         SNMP     92     get-request
1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: HewlettPacka_61:eb:ed (00:30:c1:61:eb:ed)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.104
User Datagram Protocol, Src Port: 4334, Dst Port: 161
    Source Port: 4334
    Destination Port: 161
    Length: 58
    Checksum: 0x65f8 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Stream Packet Number: 1]
    [Timestamps]
        [Time since first frame: 0.000000000 seconds]
        [Time since previous frame: 0.000000000 seconds]
    UDP payload (50 bytes)
Simple Network Management Protocol
[Community ID: 1:RCQochaFG8OuYkHBXO2m41aaQoo=]
```


```
No.     Time               Source                Destination           Protocol Length Info
      1 12:39:52.896793    192.168.1.102         192.168.1.104         SNMP     92     get-request
1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: HewlettPacka_61:eb:ed (00:30:c1:61:eb:ed)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.104
User Datagram Protocol, Src Port: 4334, Dst Port: 161
    Source Port: 4334
    Destination Port: 161
    Length: 58
    Checksum: 0x65f8 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Stream Packet Number: 1]
    [Timestamps]
        [Time since first frame: 0.000000000 seconds]
        [Time since previous frame: 0.000000000 seconds]
    UDP payload (50 bytes)
Simple Network Management Protocol
[Community ID: 1:RCQochaFG8OuYkHBXO2m41aaQoo=]
```


Gói tin 1: UDP yêu cầu (get-request)

- Source: 192.168.1.102 (máy khách)
- Destination: 192.168.1.104 (máy chủ)
- Source Port: 4334 (Cổng nguồn)
- Destination Port: 161 (Cổng đích - dành cho giao thức SNMP)

Gói tin 2: UDP phản hồi (get-response)

- Source: 192.168.1.104 (máy chủ)
- Destination: 192.168.1.102 (máy khách)
- Source Port: 161 (Cổng nguồn - cổng SNMP trên máy chủ)

- Length: 58 bytes

- Destination Port: 4334 (Cổng đích - cổng nguồn từ gói tin yêu cầu của máy khách)
- Length: 59 bytes

Mối quan hệ giữa số cổng

- Trong gói yêu cầu (gói đầu tiên):
  - Cổng nguồn là 4334 (máy khách).
  - Cổng đích là 161 (máy chủ - cổng SNMP).
- Trong gói phản hồi (gói thứ hai):
  - Cổng nguồn là 161 (máy chủ - cổng SNMP).
  - Cổng đích là 4334 (máy khách - cổng nguồn từ gói yêu cầu ban đầu).

Kết luận

- Cổng nguồn của gói yêu cầu (4334) trở thành cổng đích của gói phản hồi.
- Cổng đích của gói yêu cầu (161) trở thành cổng nguồn của gói phản hồi.
- Điều này cho thấy cách hai gói tin UDP liên kết với nhau, với cổng nguồn và cổng đích được hoán đổi để phản hồi lại đúng máy khách đã gửi yêu cầu ban đầu.