1. Mục đích

Nhằm giúp sinh viên làm quen với wireshark và cách phân tích các gói tin pcap, giúp sinh viên tiếp cận một số bộ lọc thường xuyên sử dụng khi phân tích gói tin.

2. Yêu cầu đối với sinh viên

Có kiến thức cơ bản về Wireshark.

3. Nội dung thực hành

Dùng Wireshark để phân tích file PCAP giúp sinh viên hiểu sâu hơn về các luồng dữ liệu, giao thức mạng, và các sự kiện đang diễn ra trong một mạng lưới. Điều này rất quan trọng trong việc chẩn đoán sự cố mạng, phát hiện xâm nhập, và phân tích hiệu suất của các hệ thống mạng.

Bài thực hành bao gồm 6 task, cung cấp cho sinh viên kiến thức cơ bản theo các task:

- Task 1: Kiến thức về Open SSID
- Task 2: Tìm hiểu về kênh (channels) của 1 SSID
- Task 3: Phân loại giữa các lại địa chỉ nguồn, đích, máy thu, máy phát
- Task 4: Tìm hiểu các cơ chế bảo mật được dùng cho 1 SSID
- Task 5: Tìm hiểu về WPS
- Task 6: Cách xem nơi gói đường đi của gói tin (nơi gửi và nơi nhận)

Thông qua bài thực hành, sinh viên sẽ nắm được cách sử dụng Wireshark trong phân tích dữ liệu mạng thực tế.

Khởi động bài lab:

labtainer -r traffic-analysis

(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 student ảo sẽ xuất hiện. Xem các file có sẵn trong terminal student:

ls -l

Sinh viên cầu tạo một file text để lưu kết quả của mỗi task trên một dòng với cú pháp:

nano ten_file

Task n: <ket_qua>

Sau khi hoàn thành hết các task, sinh viên sẽ biên dịch file code result.c để có thể chạy file kết quả của sinh viên.

Khởi động wireshark:

wireshark

Sau đó sinh viên tìm kiếm kết quả cho các câu hỏi sau:

Task 1: Gói tin đầu tiên có Open SSID (SSID không bảo mật) trong file wireless.pcap. (Khoảng trống giữa tên để kí tự "_")

- Điểm truy cập WiFi phát gói tin các gói tin beacon frame trong môi trường không dây sau một khoảng thời gian cụ thể. Beacon frame là một loại management frame, chứa thông tin về mạng WiFi và hướng dẫn để thiết lập kết nối với nó.

- Trong Wireshark, các frame được biểu diễn theo dạng thập lục phân:

  + Management frame: 0x0

  + Subtype của beacon frame: 0x8

- Lệnh để hiển thị tất cả các biến của beacon frame:

wlan.fc.type == 0x0 && wlan.fc.type_subtype == 0x8

- Bit privacy trong beacon frame được dùng để kiểm tra xem mạng Wifi có được mã hóa hay không. Nếu điểm truy cập WiFi ở chế độ mở (OPEN) và không sử dụng mã hóa hoặc xác thực, bit privacy sẽ có trạng thái unset (== 0).

- Bộ lọc để chỉ hiển thị các mạng mở:

wlan.fixed.capabilities.privacy == 0

Task 2: Tìm kênh hoạt động của 1 SSID wlantest DIR655 trong gói tin wireless.pcap.

- Channels được sử dụng để chia băng tần WiFi thành nhiều phần nhỏ, giúp các thiết bị dùng chung băng tần mà không gây nhiễu lẫn nhau. Nếu access point (điểm truy cập) phát các beacon trên một kênh cụ thể, thì chỉ những thiết bị được cấu hình đúng trên kênh đó mới có thể phát hiện ra điểm truy cập này.

- Vì mọi gói tin không dây đều chứa Radio Information, nên chỉ cần lọc theo SSID để tìm đúng mạng muốn theo dõi:

- Bộ lọc:

wlan.ssid == "wlantest_DIR655"

Task 3: Tổng số gói tin được truyền của địa chỉ MAC "ca:d7:19:4b:66:2d" trong file wireless.pcap.

- Trong mạng không dây, có 4 loại địa chỉ MAC:

+ **wlan.ta (Transmitter Address):** Địa chỉ máy phát.

+ **wlan.ra (Receiver Address):** Địa chỉ máy thu.

+ **wlan.sa (Source Address):** Địa chỉ nguồn phát gói tin, nơi tạo ra gói tin.

+ **wlan.da (Destination Address):** Địa chỉ đích, nơi gói tin cần đến.

-Bộ lọc:

wlan.ta == ca:d7:19:4b:66:2d

Task 4: Tìm cơ chế bảo mật của 1 SSID "DIR-655@506" (OPEN, WPA-PSK, WPA2-PSK) trong file capture.cap

- Trong beacon frame của mạng có SSID "A" có tag RSN Information (Robust Security Network). Điều này cho biết mạng sử dụng cơ chế xác thực PSK (Pre-Shared Key), thường dùng trong các mạng gia đình hoặc văn phòng nhỏ. Tuy nhiên, thông tin này chưa cho biết chính xác mạng sử dụng chuẩn mã hóa nào.

- Để xác định chuẩn mã hóa chính xác, cần kiểm tra Group Cipher Suite và Pairwise Cipher Suite trong beacon frame. Đây là các thông số mã hóa được dùng để bảo vệ dữ liệu truyền qua mạng.

- Bộ lọc:

wlan.ssid == "DIR-655@506"

+ **AES (Advanced Encryption Standard):** cơ chế mã hóa được sử dụng trong WPA2.

+ **TKIP (Temporal Key Integrity Protocol):** cơ chế mã hóa thuộc WPA.

Task 5: Trong file capture.cap, kiểm tra WPS(Wifi Protect Setup) có được bật trên SSID "DIR-655@506" không.

- WPS (Wi-Fi Protected Setup) là tính năng cho phép kết nối nhanh các thiết bị như máy in, ki-ốt, hoặc thiết bị IoT vào mạng WiFi mà không cần nhập mật khẩu. Khi nhấn nút WPS trên router, thiết bị sẽ tự động kết nối với mạng WiFi trong vài giây và bỏ qua bước xác thực mật khẩu thông thường.

- Thông tin về WPS được chứa trong Tag Vendor Specific (221). Trong đó:

+ Type: 0x04 biểu thị hỗ trợ WPS.

+ Type: 0x01 biểu thị hỗ trợ WPA

+ Bất kỳ gói tin nào chứa tham số này đều chỉ ra rằng WPS được hỗ trợ.

- Bộ lọc:

wlan.ssid == "DIR-655@506"

- Một số lưu ý:

+ Khi sử dụng toán tử "==" để lọc SSID trong Wireshark. Nếu tên SSID trong tệp pcap có khoảng trắng thì sẽ không có gói tin nào hiển thị vì toán tử "==" yêu cầu so sánh chính xác.

+ Vì vậy sử dụng toán tử "contains" để lọc các gói tin có SSID chứa khoảng trắng hoặc ký tự thừa.

Task 6: Tìm địa chỉ MAC được trao đổi với địa chỉ MAC "00:1b:11:60:82:f9" trong file capture.cap.

- Giá trị 0x20 đại diện cho gói dữ liệu (Data Packet) trong trường type_subtype của Wi-Fi frame. Nếu trạm đang gửi bất kỳ dữ liệu nào đến điểm truy cập, trạm phải đặt BSSID trong wlan.ra và phải đặt type_subtype frame thành 0x20:

wlan.fc.type_subtype == 0x20 && wlan.ra == 00:1b:11:60:82:f9

Kiểm tra kết quả:

- Thực hiện biên dịch chương trình result.c và chạy:

gcc result.c -o result

./result

- Sau khi chạy chương trình, chương trình sẽ yêu cầu nhập tên file chứa đáp án để kiểm tra kết quả.

Kết thúc bài lab:

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

stoplab

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.

Kiểm tra kết quả:

checkwork