BÁO CÁO THỰC HÀNH

Môn học: Nhập môn mạng máy tính

Buổi báo cáo: Lab 06

Tên chủ đề: Tên bài thực hành

GVHD: Phan Trung Phát

Ngày thực hiện: 13/12/2022

Ngày nộp báo cáo: 14/12/2022

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: IT005.N11.KHTN.1

STT	Họ và tên	MSSV	Email
1	Trương Thanh Minh	21520064	21520064@gm.uit.edu.vn
2	Huỳnh Phạm Đức Lâm	21521050	21521050@gm.uit.edu.vn

2. ĐÁNH GIÁ KHÁC:

Nội dung	Kết quả
Tổng thời gian thực hiện bài thực hành trung bình	2 ngày
Link Video thực hiện *(nếu có)*	21520064_21521050_WifiCracking.mp4 - Google Drive
Ý kiến *(nếu có)* + Khó khăn + Đề xuất …	
Điểm tự đánh giá	9.5

Phần bên dưới của báo cáo này là báo cáo chi tiết của nhóm thực hiện.

BÁO CÁO CHI TIẾT

1) Phân chia công việc trong nhóm

	Trương Thanh Minh	Huỳnh Phạm Đức Lâm
Lên ý tưởng kịch bản	x	
Quay màn hình dò pass wifi		x
Viết report	x	x

2) Kịch bản của nhóm thực hiện trước khi bắt gói tin:

Là sinh viên IT, mà IT nổi tiếng là khô khan, nhạt nhẽo, vì vậy đến bây giờ LM vẫn chưa kiếm được người để cùng nhau sưởi ấm vào đêm đông Noel lạnh lẽo này. Tuy rất muốn kiếm được người yêu nhưng deadline trên trường lại dí ngập đầu LM, vì vậy cậu chẳng thể chuyên tâm đi kiếm gấu. Vì thế, LM đã quyết định ra quán Café vừa để chạy deadline môn IT005 vừa để kiếm gấu.

Khi tới quán Café để làm Lab6 môn IT005, khi đang thử dò tìm mật khẩu Wifi của quán Café (nội dung Lab6) thì LM đã vô tình được một cô em xinh xẻo, dễ thương chú ý đến. Thế là cô bé ấy đến xin FB của LM để tiện nhắn tin làm quen (có lẽ vì cô bé ấy ngại vì mình là con gái nên hong dám làm quen trực tiếp =)))).

Sau khi về nhà, LM nhận được tin nhắn làm quen của cô bé đấy. Sau khi nhắn tin làm quen một hồi, LM biết được rằng, cô em đấy chung trường và cũng học môn IT005, nhưng vẫn chưa học Lab6. Tuy nhiên, cô em đấy nói thêm rằng, thầy có dặn cô bạn đấy là ở buổi Lab6 kế tiếp tới, thầy sẽ cho lớp cô chơi 1 trò chơi: thầy cho cả lớp 1 mật mã Wifi và cả lớp có nhiệm vụ phải tìm ra mật khẩu Wifi đó (có thể kiếm 1 bạn làm chung cho trò chơi thêm vui, vì phần thưởng là 1 cặp vé xem phim cho ai tìm ra đầu tiên) thông qua các gợi ý của thầy, vì lớp khá đông, nên các gợi ý của thầy sẽ được thầy nhắn qua nhóm lớp. Và đến giờ cô vẫn chưa tìm được teammate cho mình, và cuối cùng, giờ cô đã tìm thấy LM. Thế nên cô đã rủ LM cùng tham gia trò chơi này. Vì

nếu thắng trò chơi này, LM không chỉ có 1 mùa Noel ấm áp mà còn được bonus thêm buổi hẹn hò đầu tiên cùng cô bé ấy ở rạp chiếu phim.

- **Trong kịch bản này**:
  - **Trương Thanh Minh**: vào vai thầy giáo ra gợi ý.
  - **Huỳnh Phạm Đức Lâm**: vào vai anh bạn LM chưa có gấu.
  - Wifi thầy giáo đưa có tên là: ***TimDuocPassSeCoGau***
  - Mật khẩu wifi: tetquymao11122023
  - Gợi ý đầu tiên như sau:
    - Mật khẩu có 17 kí tự (chỉ gồm số và chữ cái in thường).

3) Chi tiết các bước tìm ra mật khẩu

LM sẽ tìm mật khẩu wifi theo phương pháp Brute-force sử dụng bộ công cụ **aircrack-ng** trong **Kali Linux** theo các bước sau:

- **Bước 1**: Mở Terminal để thực hiện các câu lệnh (tương tự Command Prompt trong Windows).
- **Bước 2**: Kiểm tra tên card Wireless đang sử dụng bằng lệnh **iwconfig** (thường là card wlan0), nếu card wireless chưa được bật thì có thể bật bằng lệnh **ifconfig wlan0 up.**
- **Bước 3**: Chuyển card mạng Wifi sang chế độ monitor (chế độ theo dõi toàn bộ các tín hiệu trong mạng) bàng airmon-ng. Chuyển card mạng wlan0 sang chế độ monitor bằng công cụ **airmon** với lệnh **airmon-ng start wlan0.**
- **Bước 4**: Sử dụng **airodump** để theo dõi hoạt động của các mạng wifi hiện tại qua card wlan0mon: **airodump-ng wlan0mon.**
- **Bước 5:** Xác định mạng Wifi mục tiêu (***TimDuocPassSeCoGau)*** và sử dụng airodump để bắt gói tin và chỉ theo dõi duy nhất mạng mục tiêu đó:

  airodump-ng -c [channel] **-w** [tập tin] **–bssid** [BSSID của mạng] **wlan0mon.**
- **Bước 6:** Thu thập gói tin bắt tay WPA handshake (bắt tay 4 bước) trong quá trình đăng nhập để dựa vào đó dò tìm mật khẩu. (Thầy đã đăng nhập vào wifi đó trước đó rồi).
- **Bước 7:** Khi nhận được gói tin WPA handshake của mạng mục tiêu tương ứng, ta dừng quá trình bắt gói tin và tiến hành dò tim mật khẩu dựa vào file .cap đã bắt được.

Thực hiện lệnh với cú pháp sau:

crunch [min] [max] [danh sách các ký tự có trong chuỗi] -**t** [mẫu định dạng mật khẩu] | **aircrack -ng** -**w**- [tập tin đã capture.cap] –**bssid** [địa chỉ MAC của mục tiêu].

- Chỉ với gợi ý là mật khẩu gồm 17 kí tự, qua 10 phút cả lớp chưa dò cả, vì quá mông lung. Do đó, thầy đã thả ra gợi ý tiếp theo: trong 17 kí tự, 9 kí tự đầu là chữ, còn lại là số.
- Nhận được gợi ý này, LM đoán rằng 9 kí tự đó sẽ là một chuỗi kí tự nào đó liên quan đến thầy, do đó, LM đã mạnh dạn đoán rằng, đó là chuỗi "**ptpmmtuit**". Vì vậy, LM đã nhanh tay dò thử thông qua cú pháp:

  crunch 17 17 0123456789 -t ptpmmtuit%%%%%%%% | aircrack-ng -w- sniff-01.cap --bssid F4:28:53:D3:CE:68

  Tuy nhiên, LM đã coi nhẹ sự nham hiểm của thầy khi thử với mật khẩu đó, thế nên cuối cùng sau ~10' dò tìm cũng không ra kết quả. Và cả lớp cũng thế.
- Vì vậy thầy quyết định cho ra gợi ý tiếp theo, chuỗi ký tự liên quan đến một trong các ngày lễ trong năm.

  LM khi nghe xong kiểu "Ú Òa, ez, sắp có ghệ rồi kaka.". Và LM đã nhanh trí đoán ra rằng, chuỗi kí tự này là "**noelvuive**" vì sắp Noel rồi.

  crunch 17 17 0123456789 -t noelvuive%%%%%%%% | aircrack-ng -w- sniff-01.cap --bssid F4:28:53:D3:CE:68

  Thật đáng buồn cho LM, ~10' câu trả lời trên vẫn sai, và cả lớp cũng chẳng ai tìm thấy (vì ai cũng nghĩ là Noel). Thế là cả lớp lại năn nỉ thầy cho thêm gợi ý nữa.
- Gợi ý cuối cùng của thầy như sau: trong chuỗi kí tự có tên một con vật. Với ông hoàng tử vi, anh hùng bàn phím, LM đã nhanh tay dò tìm với chuỗi kí tự "**tetquymao**".

  crunch 17 17 0123456789 -t* tetquymao*%%%%%%%% | aircrack-ng -w- sniff-01.cap.cap --bssid F4:28:53:D3:CE:68

  Sau bao nhiêu cố gắng, cuối cùng LM đã đoán trúng Wifi cần tìm là tetquymao11122023 và may mắn là LM là người đoán ra sớm nhất nên đã giành được quà tặng là 2 vé xem phim của thầy.

  LM rất vui vì cuối cùng đã có gấu. Tuy nhiên điều đáng buồn là cô bé ấy đã lừa LM tham gia trò chơi để lấy vé đi chơi với gấu của cô bé đó. Và LM cuối

cùng vẫn là kẻ codon giữa mùa Noel lạnh lẽo. Tuy là kẻ chiến thắng trên đường trường nhưng LM vẫn là kẻ thua cuộc trên trường tình. Chia buồn với LM.

4) Link drive clip

21520064_21521050_WifiCracking.mp4 - Google Drive

HẾT