BÁO CÁO THỰC HÀNH

**Môn học: Nhập môn mạng máy tính**

**Buổi báo cáo: Lab 6**

**Tên chủ đề: Scaning WPA/WPA2 password**

*GVHD: Phan Trung Phát*

*Ngày thực hiện: 16/12/2022*

*Ngày nộp báo cáo: 17/12/2022*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: IT005.N11.KHTN.1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| STT | Họ và tên | MSSV | Email | Phân chia công việc |
| 1 | Nguyễn Đình Luân | 21521105 | 21521105@gm.uit.edu.vn | Làm video thực hành |
| 2 | Trần Đức Trí Dũng | 21520748 | 21520748@gm..uit.edu.vn | Làm kịch bản |

1. **ĐÁNH GIÁ KHÁC:**

|  |  |
| --- | --- |
| **Nội dung** | **Kết quả** |
| Tổng thời gian thực hiện bài thực hành trung bình | 2 tiếng |
| Link Video thực hiện  *(nếu có)* | [lab6 - Google Drive](https://drive.google.com/drive/folders/1vPH8YbkmdcLrlAyORhpUHpHQxnXIzS1K?fbclid=IwAR2bWN5QMK2yScHpEdhh8b5AC0huJP8V16obpQyTiUgIDD9tz3pHOTvJSNw) |
| Ý kiến *(nếu có)*  + Khó khăn  + Đề xuất … |  |
| Điểm tự đánh giá | 8 |

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

BÁO CÁO CHI TIẾT

\*Mở rộng thêm về việc scanning password:

Có 2 cách mớm mật khẩu: brute force và dictionary force

Brute Force là gì?

Việc Hack Password WiFi WPA/WPA2 cần sử dụng cách Tấn công Brute Force, đây là một loại tấn công mạng, trong đó bạn có một phần mềm, xoay vòng các ký tự khác nhau, kết hợp để tạo ra một mật khẩu đúng. Phần mềm Brute Force Attack password cracker đơn giản sẽ sử dụng tất cả các kết hợp có thể để tìm ra mật khẩu cho máy tính hoặc máy chủ mạng. Nó rất đơn giản và không sử dụng bất kỳ kỹ thuật thông minh nào.

Vì phương pháp này chủ yếu dựa trên toán học, phải mất ít thời gian hơn để crack mật khẩu, bằng cách sử dụng các ứng dụng brute force thay vì tìm ra chúng theo cách thủ công. Nói phương pháp này dựa trên toán học vì máy tính làm rất tốt các phép toán và thực hiện chúng trong vài giây, nhanh hơn rất nhiều lần so với bộ não con người (mất nhiều thời gian hơn để tạo ra các sự kết hợp).

Dictionary force là gì ?

 Nếu bạn có file từ điển (là một file .txt, trong đó mỗi dòng là một mật khẩu cần check), aircrack-ng sẽ bốc từng cụm từ trong từ điển ra đối chiếu. Nhược điểm là, từ điển của bạn phải đủ phong phú, bởi nếu mật khẩu thật sự ko có trong từ điển, bạn cũng tốn công vô ích. Nhưng cái ưu việt ở chỗ, bạn ko phải tốn thời gian đi kiểm tra những tổ hợp mà bạn tin rằng chả bố con thằng nào đặt thế cho khó nhớ, kiểu “awhjfyqhcedcb”. File từ điển bạn có thể gg search ra rất nhiều trên mạng, tự lập trình để tự sinh file từ điển theo quy tắc ngôn ngữ riêng của bạn.

\*Aircrack-ng là gì?

Aircrack-ng là một bộ công cụ hoàn chỉnh để đánh giá khả năng bảo mật mạng WiFi. Nó tập trung vào các lĩnh vực bảo mật WiFi khác nhau:

Giám sát: Chụp gói và xuất dữ liệu sang tệp văn bản để xử lý thêm bằng các công cụ của bên thứ ba

Tấn công: Phát lại các cuộc tấn công, hủy xác thực, điểm truy cập giả mạo và những thứ khác thông qua chèn gói

Kiểm tra: Kiểm tra thẻ WiFi và khả năng của trình điều khiển (chụp và chèn)

Bẻ khóa: WEP và WPA PSK (WPA 1 và 2) Tất cả các công cụ đều là dòng lệnh cho phép tạo script nặng.  
Rất nhiều GUI đã tận dụng tính năng này.

Nó hoạt động chủ yếu trên Linux nhưng cũng có Windows, macOS, FreeBSD, OpenBSD, NetBSD, cũng như Solaris và thậm chí cả eComStation 2.

\*Crunch là gì?

\*Crunch là một phần mềm cho phép người dùng sử dụng trong việc tạo wordlist hỗ trợ Brute Force dùng để Hack Password WiFi WPA/WPA2. Nó có thể tạo word list từ tất cả các kí tự từ in hoa , viết thường , số và các kí tự đặc biệt.