**Nội dung và hướng dẫn bài thực hành**

**Mục đích**

Giúp sinh viên được thực hiện các thao tác trong việc crack mật khẩu sử dụng aircrack-ng một cách đơn giản với điều kiện thuận lợi.

**Yêu cầu đối với sinh viên**

Có kiến thức cơ bản về mạng wifi và aircrack-ng.

**Nội dung thực hành**

imodule https://github.com/ParadoxParadise/labattt-2025/raw/refs/heads/main/nsec-wifi-crack/imodule.tar

Khởi động bài lab:

Vào terminal, gõ:

*Labtainer nsec\_wifi\_crack -r*

*(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.

* **Task 1: Xác định các thông tin cần sử dụng để crack mật khẩu:**

Để crack mật khẩu WPA2 của một mạng Wi-Fi (chẳng hạn như sử dụng Aircrack-ng), ta cần thu thập một số thông tin và dữ liệu sau:

**Tệp danh sách từ điển (wordlist):**

Aircrack-ng sử dụng từ điển để thử các mật khẩu. Bạn có thể tạo một từ điển của riêng mình hoặc sử dụng từ điển có sẵn như list.txt

Càng có nhiều mật khẩu trong từ điển, khả năng tìm ra mật khẩu chính xác càng cao.

**Tệp handshake (đã được cung cấp trong bài lab này)**

Đây là dữ liệu được ghi lại trong quá trình một thiết bị kết nối vào mạng Wi-Fi. Tệp này sẽ chứa thông tin cần thiết để crack mật khẩu.

Bạn có thể thu thập handshake này bằng cách sử dụng các công cụ như airodump-ng trong Aircrack-ng để giám sát mạng Wi-Fi và bắt tay khi một thiết bị kết nối.

**Thông tin về mạng Wi-Fi:**

SSID: Tên của mạng Wi-Fi (mạng mà bạn đang cố gắng crack mật khẩu).

BSSID: Địa chỉ MAC của điểm truy cập (AP) Wi-Fi.

Giao thức mã hóa: WPA2 (WPA2-PSK) là loại mã hóa phổ biến mà bạn đang muốn crack.

Sử dụng câu lệnh sau để xem thông tin của tệp cap đã được cung cấp

aircrack-ng <tên tệp.cap>

**Công cụ để crack:**

Aircrack-ng: Một bộ công cụ giúp bạn sử dụng handshake và từ điển để tìm ra mật khẩu.

* **Task 2:** **Đối chiếu địa chỉ MAC**

Với các thông tin đã năm được bên trên, ta có thể chạy công cụ aircrack để crack mật khẩu wifi

*sudo aircrack-ng -w /path/to/wordlist.txt -b <BSSID> <tên tệp.cap>*

Sau khi đợi công cụ thực hiện việc crack mật khẩu thành công, password sẽ được hiển thị cho người dùng

Nếu trong file *list.txt*chứa password của wifi việc crack sẽ thành công

**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.