**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 môi trường không hoàn toàn thuận lợi.

**Yêu cầu đối với sinh viên**

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

**Nội dung thực hành**

Khởi động bài lab:

Vào terminal, gõ:

*Labtainer nsec\_wifi\_crack\_2 -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 thông tin hữu ích trong file capture-1.cap**

Sử dụng câu lệnh để mở file capture-1.cap

*aircrack-ng <tên tập.cap>*

Nhận thấy thông tin bị trong file capture-1.cap bị thiếu

Do đó nếu áp dụng câu lệnh *sudo aircrack-ng -w /path/to/wordlist.txt -b <BSSID> <tên tệp.cap>* tương tự như bài **nsec\_wifi\_crack1,**hệ thống sẽ báo không thể crack được wifi.

* **Task 2:** **Xác định thông tin hữu ích trong file capture-2.cap**

Tương tự với file capture-1.cap, file capture-2.cap cũng chứa thông tin hữu ích để crack mật khẩu tuy nhiên cũng không đủ, nhiệm vụ của ta là sẽ phải kết hợp thông tin của 2 file để crack mật khẩu.

* **Task 3: Chạy công cụ để phát hiện mật khẩu**

Sau khi mở 2 file, ta cần xác định các thông tin như đã nói ở đầu bài để có thể crack mật khẩu wifi. Ta sẽ sử dụng câu lệnh

*aircrack-ng --help*

để tìm hiểu thêm về các các tham số của công cụ, từ đó điểu chỉnh lệnh để có thể bổ sung thêm thông tin vào câu lệnh sau

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

Với tệp đã chứa handshake mà ta có thể xác định được thông qua việc xác định thông tin hữu ích của các file.

* **Task 4: Cracked**

Sau khi thành công crack được mật khẩu wifi, task 4 sẽ được hoàn thành.

**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.