**Họ và tên: Tăng Dũng Cẩm**

**MSSV: 22520141**

**Nhóm thực hiện bài tập cuối kì của em gồm 3 người:**

**Tăng Dũng Cẩm – 22520141**

**Lê Anh Hào – 22520399**

**Phạm Đức Anh - 22520067**

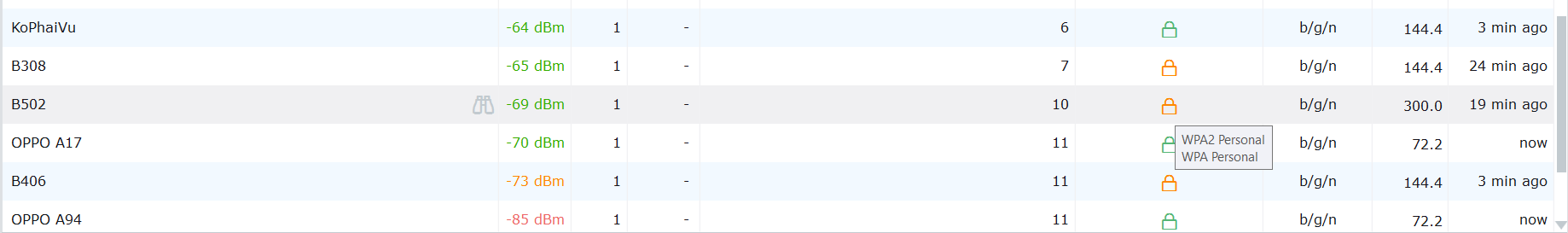
**Bài 1: Cài đặt hai công cụ khám phá mạng không dây. Phân tích các mạng trong phạm vi xung quanh.**

Phần mềm inISSIDer:

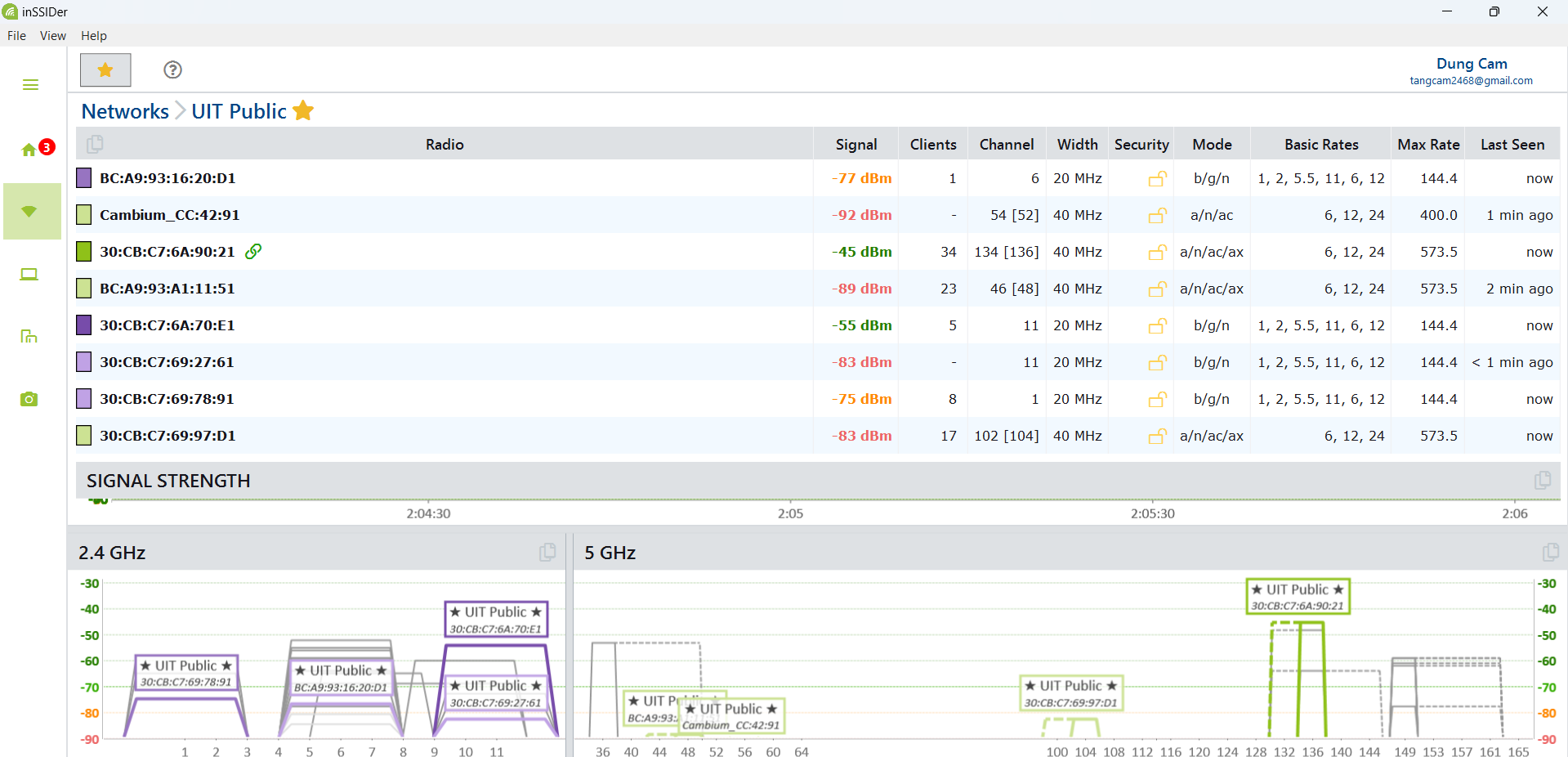
A screenshot of a computer

Description automatically generated

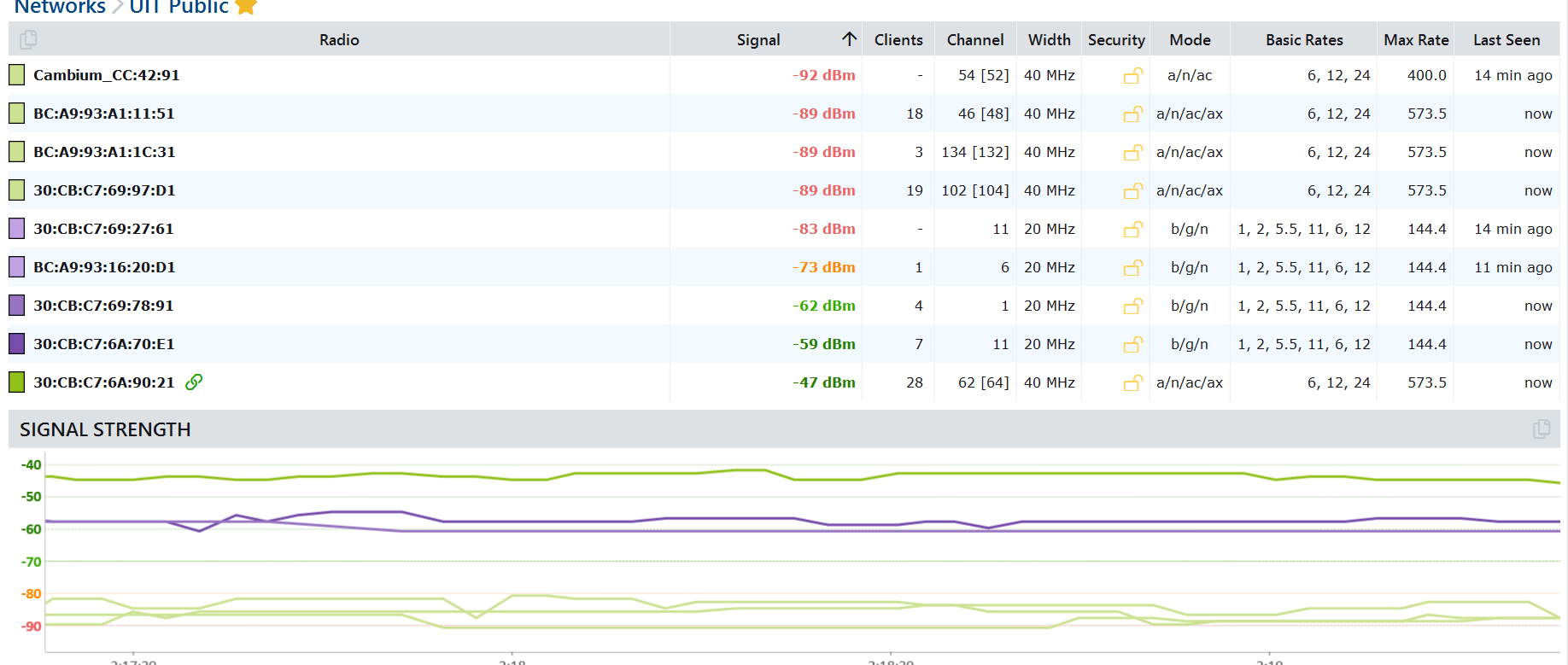
* Hiển thị loại bảo mật của mạng, ở đây có thể thấy B308, B502 và B406 có loại bảo mật là WPA2 Personal và WPA Personal.



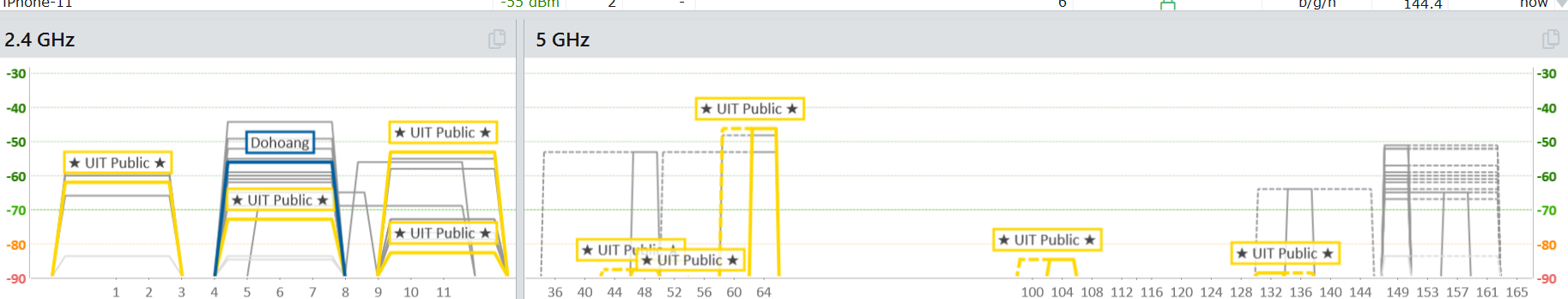
* Hiển thị địa chỉ MAC của các AP của mạng, dưới đây là của mạng UIT. Từng AP sẽ có cường độ tín hiệu khác nhau, có số Client kết nối đến, loại bảo mật và chuẩn wifi mà AP đố hỗ trợ (Mode)



* Ở đây phần mềm cũng hỗ trợ đo và hiển thị cường độ tín hiệu thành biểu đồ của mạng.



* Phần mềm cũng hỗ trợ hiển thị phân loại các mạng xung quanh vào 2 loại bằng tần 2.4 GHz và 5 GHz

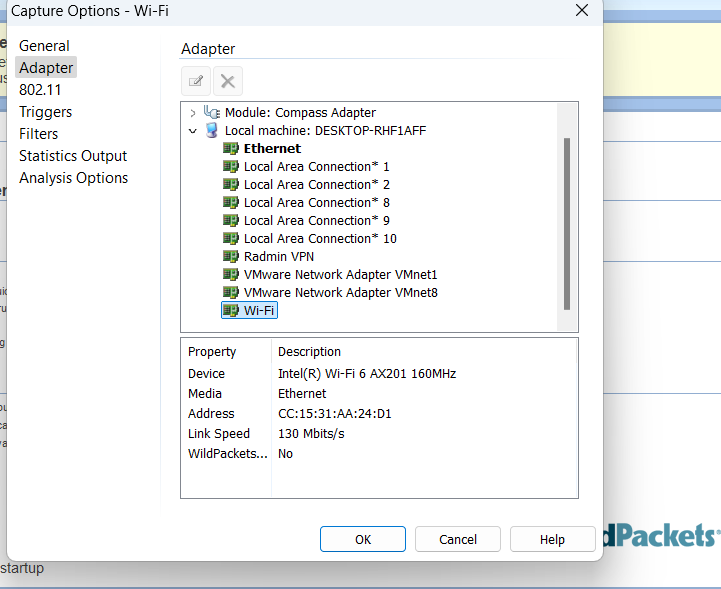


A graph on a white sheet

Description automatically generated

**Bài 2: Cài đặt một công cụ phân tích mạng như Pilot, OmniPeek… nêu cách sử dụng.**

OmniPeek



* Công cụ hiển thị các gói tin đã bắt được sau đó thực hiện phân tích. Ở đây có thể thấy top các người dùng được tổng hợp theo địa chỉ IP, và top các giao thức được sử dụng nhiều nhất.

A screenshot of a computer

Description automatically generated

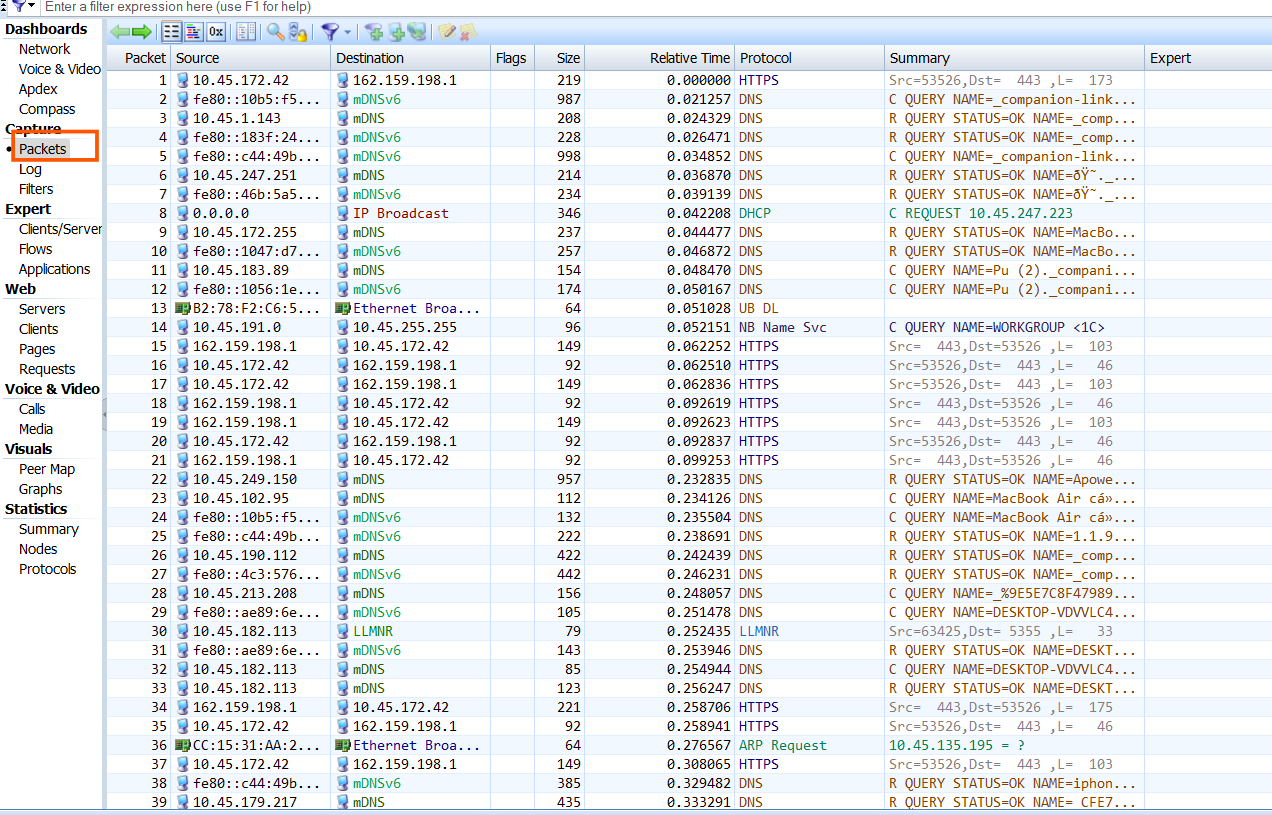
A screenshot of a computer

Description automatically generated

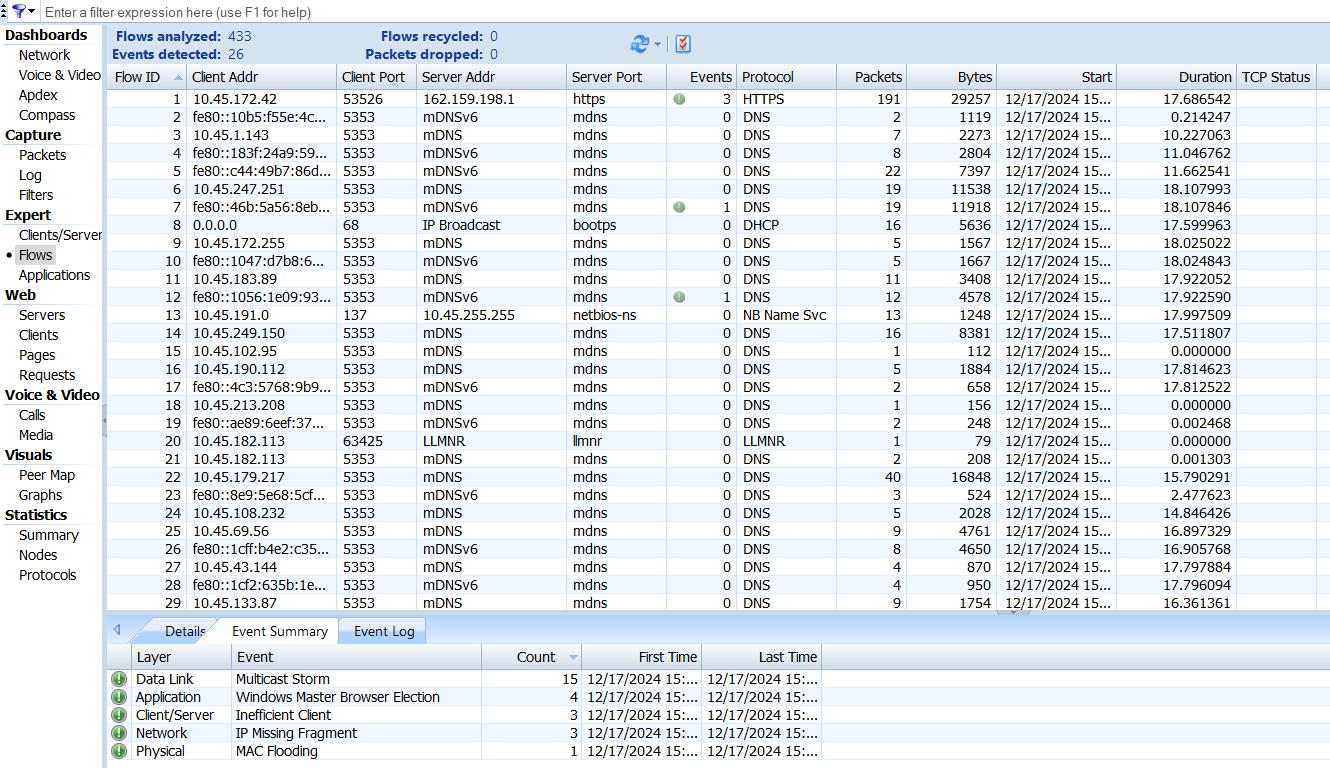
A screenshot of a computer

Description automatically generated

* Chọn loại capture để hiển thị được các gói tin bắt được cùng với các thông tin của gói tin đó:



* Tuỳ chọn Flows trong Expert cung cấp, hiển thị các luồng dữ liệu trong mạng, trong đó có các thông tin như địa chỉ nguồn, địa chỉ đích, giao thức sử dụng, các cổng port nguồn và đích cũng như tốc độ truyền dữ liệu, dung lượng,…



**Bài 3: Cho biết công dụng của các tool trong bộ Aircrack-ng Suite.**

|  |  |
| --- | --- |
| **Tên công cụ** | **Nội dung** |
| Airbase-ng | Thu thập bắt tay WPA/WPA2 và có thể hoạt động như một điểm truy cập ad-hoc. |
| Aircrack-ng | Công cụ bẻ khóa WEP và WPA/WPA2-PSK. |
| Airdecap-ng | Giải mã WEP/WPA/WPA2 và loại bỏ header không dây khỏi các gói tin Wi-Fi. |
| Airdriver-ng | Cung cấp thông tin trạng thái về các driver không dây trên hệ thống của bạn. |
| Airdrop-ng | Chương trình dùng để hủy xác thực có mục tiêu, dựa trên quy tắc xác định. |
| Airplay-ng | Dùng để tạo lưu lượng, giả mạo xác thực, phát lại gói tin và tiêm các yêu cầu ARP. |
| Airgraph-ng | Tạo đồ thị mối quan hệ giữa client và AP từ tệp Airodump-ng. |
| Airodump-ng | Thu thập gói tin thô 802.11 và thu thập IVs WEP. |
| Airolib-ng | Lưu trữ và quản lý danh sách ESSID và mật khẩu để bẻ khóa WPA/WPA2. |
| Airserv-ng | Cho phép nhiều chương trình độc lập sử dụng card Wi-Fi thông qua kết nối TCP client-server. |
| Airmon-ng | Kích hoạt chế độ monitor trên card không dây hoặc chuyển về chế độ quản lý. |
| Airtun-ng | Tiêm các khung WPA TKIP với QoS, phân tích keystream và MIC từ lưu lượng Wi-Fi. |
| Easside-ng | Cho phép bạn giao tiếp với điểm truy cập (AP) được mã hóa WPA mà không cần key. |
| Packetforge-ng | Tạo các gói tin được mã hóa có thể được sử dụng để tiêm dữ liệu. |
| Tkiptun-ng | Tạo một giao diện ảo để giám sát lưu lượng được mã hóa và tiêm các khung tin trong mạng. |
| Wesside-ng | Tự động phát hiện và bẻ khóa WEP một cách nhanh chóng trong vài phút. |

**Bài 4: Trình bày các biện pháp phòng chống tấn công mạng wifi.**

**Cài cấu hình bảo mật Wi-Fi:**

* Thay đổi SSID mặc định sau khi cấu hình WLAN
* Đặt mật khẩu truy cập router và bật tường lửa
* Không nên tắt SSID broadcast
* Tắt truy cập từ xa và quản lý router qua Wi-Fi
* Bật lọc địa chỉ MAC trên access point hoặc router
* Bật mã hóa trên access point và thường xuyên thay đổi mật khẩu

**Cài đặt SSID:**

* Sử dụng SSID cloaking
* Không sử dụng mật khẩu dễ đoán
* Đặt firewall hoặc packet filter
* Hạn chế phạm vi phủ sóng của mạng không dây
* Kiểm tra thiết bị không dây thường xuyên
* Sử dụng mã hóa traffic như IPSEC hoặc WPA3

**Cài đặt xác thực Wifi**

* Sử dụng Wi-Fi Protected Access (WPA) thay vì WEP
* Triển khai WPA2 Enterprise khi có thể
* Vô hiệu hóa mạng khi không cần thiết
* Đặt access point (AP) ở vị trí an toàn
* Cập nhật driver cho tất cả thiết bị
* Sử dụng máy chủ tập trung cho việc xác thực