

Bộ Giáo Dục Và Đào Tạo
Trường Đại Học Ngoại Ngữ - Tin Học Thành Phố Hồ Chí Minh
Khoa Công Nghệ Thông Tin



MÔN HỌC : MẠNG KHÔNG DÂY
ĐỀ TÀI : PHÁT HIỆN TẤN CÔNG
DEAUTHENTICATION TRONG MẠNG WIFI

Giảng Viên Hướng Dẫn : ThS. Cao Tiến Thành

Thành Viên :

1. Lê Thành Đạt – MSSV: 22DH110717
2. Huỳnh Minh Nhựt – MSSV: 22DH112633
3. Phạm Hoàng Gia Bảo – MSSV: 22DH110298

TP. Hồ chí minh, Ngày 18 tháng 03 năm 2025

LỜI CẢM ƠN

Nhóm em xin được bày tỏ lòng tôn trọng và biết ơn sâu sắc đến giảng viên Cao Tiên Thành – giảng viên tại trường Đại học Ngoại ngữ - Tin học Tp.HCM vì đã luôn nhiệt tình hỗ trợ và chỉ dạy những kiến thức vô cùng bổ ích cho việc học tập và thực hiện đồ án của chúng em. Nhờ có sự nhắc nhở và góp ý từ thầy mà đồ án này có thể từ từ được hoàn thiện và phát triển. Sự tận tâm cùng trái tim đầy nhiệt huyết trong việc dẫn dắt và cung cấp những kinh nghiệm, những bài học quan trọng mà chúng em có thêm động lực và kiến thức để làm nên đồ án này.

Mặc dù đã nỗ lực cố gắng nhưng do thời gian và kiến thức có hạn nên trong quá trình thực hiện đồ án khó tránh khỏi sai sót nên nhóm em rất mong có được thêm nhiều những góp ý chân thành đến từ thầy để đồ án có thể tiếp tục được phát triển và hoàn thiện hơn trong tương lai.

Nhóm em xin chân thành cảm ơn thầy ạ!

LỜI NÓI ĐẦU

Trong bối cảnh an ninh mạng ngày càng trở thành mối quan tâm lớn, các cuộc tấn công vào mạng Wi-Fi ngày càng phổ biến và tinh vi. Một trong những phương thức tấn công phổ biến nhất là deauthentication attack, nhằm mục đích ngắt kết nối người dùng hợp lệ khỏi mạng không dây bằng cách gửi các gói tin giả mạo. Điều này không chỉ gây gián đoạn dịch vụ mà còn có thể tạo cơ hội cho kẻ tấn công thực hiện các cuộc tấn công tiếp theo, như man-in-the-middle (MITM) để đánh cắp thông tin nhạy cảm.

Bài luận này tập trung vào việc phát hiện tấn công deauthentication trong mạng Wi-Fi, sử dụng công cụ Scapy và Wireshark để mô phỏng tấn công và phân tích các gói tin trong thời gian thực. Chúng tôi sẽ xây dựng một công cụ phát hiện dựa trên phân tích hành vi gói tin, từ đó đánh giá khả năng nhận diện và ngăn chặn tấn công.

Nội dung bài luận bao gồm các phần chính như sau:

Giới thiệu về tấn công deauthentication và tác động của nó đối với hệ thống mạng.

Phương pháp mô phỏng tấn công bằng cách sử dụng Scapy để tạo ra các gói tin giả mạo.

Phát triển công cụ phát hiện dựa trên phân tích lưu lượng mạng bằng Wireshark và các thuật toán phân tích dữ liệu.

Triển khai và đánh giá hiệu suất của công cụ thông qua các bài kiểm thử thực tế.

Bài luận không chỉ cung cấp cái nhìn tổng quan về tấn công deauthentication mà còn đưa ra giải pháp thực tế giúp nâng cao khả năng bảo mật mạng Wi-Fi. Hy vọng rằng kết quả nghiên cứu sẽ đóng góp vào việc tăng cường nhận thức về an toàn mạng và cung cấp giải pháp hữu ích cho các quản trị viên hệ thống trong việc bảo vệ mạng Wi-Fi trước các mối đe dọa tiềm tàng.

MỤC LỤC

Mục Lục

LỜI CẢM ƠN.....	2
LỜI NÓI ĐẦU.....	3
MỤC LỤC	4
DANH MỤC HÌNH ẢNH.....	6
DANH MỤC BẢNG BIỂU.....	8
CHƯƠNG 1: GIỚI THIỆU.....	9
1. Lý do chọn đề tài	9
2. Tính cấp thiết của vấn đề.....	10
3. Mục tiêu và phạm vi nghiên cứu.....	11
CHƯƠNG 2: CƠ SỞ LÝ THUYẾT	11
1. Tổng quan về mạng Wi-Fi (IEEE 802.11).....	11
a. Kiến trúc mạng Wi-Fi	11
b. Cơ chế kết nối Wifi	13
c. Giao thức 802.11	15
d. Bảo mật mạng Wi-Fi	16
2. Tấn công Deauthentication.....	18
a. Định nghĩa	18
b. Cơ chế tấn công.....	19
c. Các biến thể của tấn công	21
d. Động cơ tấn công.....	22
3. Các công cụ và kỹ thuật phát hiện tấn công	22
a. Scapy	22

b.	Wireshark	24
c.	So sánh với một số công cụ khác	26
d.	Kỹ thuật phân tích lưu lượng mạng	27
4.	Các biện pháp phòng chống tấn công	28
a.	802.11w (Protected Management Frames)	28
b.	Phát hiện và ngăn chặn xâm nhập (IDS/IPS)	28
c.	Các biện pháp bảo mật khác	30
CHƯƠNG 3: PHƯƠNG PHÁP THỰC HIỆN		31
1.	Mô tả danh sách thiết bị	31
2.	Cấu hình	31
3.	Môi trường thực hiện	32
4.	Sơ đồ mạng	33
CHƯƠNG 4: TRIỂN KHAI		33
1.	Triển khai và cấu hình	33
2.	Kết quả	42
CHƯƠNG 5: ĐÁNH GIÁ VÀ KẾT LUẬN		43
1.	Ưu điểm	43
2.	Nhược điểm	43
3.	Khuyến nghị	44
4.	Kết luận	44
TÀI LIỆU THAM KHẢO		46

DANH MỤC HÌNH ẢNH

Hình 1. Mô hình mạng cơ bản	13
Hình 2. Client kết nối AP.....	14
Hình 3. Tổng quan về 802.11	16
Hình 4. So sánh về các loại bảo mật.....	18
Hình 5. Tấn công DeAuthentication	19
Hình 6. Cơ chế tấn công	21
Hình 7. Phần mềm Scapy.....	24
Hình 8. Phần mềm Wireshark.....	26
Hình 9. Minh họa IDS và IPS	29
Hình 10. Thiết lập điểm phát wifi.....	32
Hình 11. Sơ đồ mạng	33
Hình 12. Tìm kiếm bot.....	34
Hình 13. Khởi động bot	35
Hình 14. Tạo kênh chat cho bot.....	36
Hình 15. Kênh chat khi tham gia	37
Hình 16. Lấy ID đoạn chat bot	38
Hình 17. Sửa giá trị của bot token và chat id.....	39
Hình 18. Kiểm tra card wifi	40
Hình 19. Bật chế độ monitor.....	40
Hình 20. Quét được mạng máy nạn nhân	41
Hình 21. Script tấn công	41

Hình 22. Script phát hiện 42

Hình 23. Thông báo kết quả..... 42

DANH MỤC BẢNG BIỂU

Bảng 1. So sánh các công cụ.....	26
Bảng 2. Bảng so sánh giữa các công cụ	30

CHƯƠNG 1: GIỚI THIỆU

1. Lý do chọn đề tài

Trong bối cảnh mạng không dây (Wi-Fi) ngày càng trở nên phổ biến, các mối đe dọa an ninh mạng cũng ngày một gia tăng. Một trong những hình thức tấn công nguy hiểm nhưng lại dễ thực hiện là tấn công deauthentication, cho phép kẻ tấn công ngắt kết nối các thiết bị hợp lệ khỏi mạng một cách dễ dàng bằng cách gửi các gói tin giả mạo. Điều này không chỉ gây ra gián đoạn dịch vụ mà còn có thể tạo điều kiện để thực hiện các cuộc tấn công nghiêm trọng hơn, chẳng hạn như Man-in-the-Middle (MITM), đánh cắp thông tin đăng nhập hoặc chiếm quyền truy cập hệ thống.

Hiện nay, mặc dù có nhiều giải pháp bảo mật mạng Wi-Fi, nhưng các phương pháp phát hiện và phòng chống tấn công deauthentication vẫn chưa thực sự phổ biến hoặc chưa đạt hiệu quả cao. Hầu hết các hệ thống Wi-Fi thông thường không được trang bị cơ chế phát hiện tấn công này, khiến người dùng và quản trị viên mạng gặp khó khăn trong việc nhận diện và phản ứng kịp thời. Do đó, việc nghiên cứu và phát triển một công cụ phát hiện tấn công deauthentication trong thời gian thực là vô cùng cần thiết.

Việc lựa chọn đề tài này dựa trên những lý do chính sau:

- Tính thực tiễn cao: Tấn công deauthentication là một hình thức tấn công phổ biến, có thể gây ảnh hưởng lớn đến hệ thống mạng Wi-Fi trong các tổ chức, doanh nghiệp và cá nhân. Một công cụ phát hiện tấn công sẽ giúp tăng cường khả năng bảo vệ mạng.
- Ứng dụng công nghệ hiện đại: Đề tài sử dụng các công cụ mạnh mẽ như Scapy (để mô phỏng tấn công) và Wireshark (để phân tích gói tin), kết

hợp với các phương pháp phân tích thời gian thực nhằm nâng cao hiệu suất phát hiện.

- Đóng góp vào an ninh mạng: Kết quả nghiên cứu có thể giúp các quản trị viên mạng và chuyên gia an ninh mạng có thêm công cụ hữu ích để nhận diện sớm và ngăn chặn tấn công, giảm thiểu rủi ro về bảo mật thông tin.
- Thách thức kỹ thuật: Việc phân tích lưu lượng mạng, nhận diện bất thường và phát triển giải pháp phát hiện tấn công trong thời gian thực đòi hỏi sự kết hợp của nhiều kỹ thuật, giúp người thực hiện có cơ hội nâng cao kiến thức và kỹ năng về bảo mật mạng.

Với những lý do trên, đề tài "Phát hiện tấn công deauthentication trong mạng Wi-Fi" không chỉ mang lại giá trị nghiên cứu mà còn có ý nghĩa thực tế, giúp nâng cao khả năng bảo mật cho các hệ thống Wi-Fi trước những mối đe dọa ngày càng tinh vi.

2. Tính cấp thiết của vấn đề

Trong thời đại số hóa hiện nay, mạng Wi-Fi đã trở thành một phần thiết yếu trong cuộc sống hàng ngày của chúng ta. Tuy nhiên, với sự gia tăng số lượng thiết bị kết nối không dây, các mối đe dọa an ninh mạng cũng ngày càng gia tăng. Tấn công deauthentication là một trong những hình thức tấn công phổ biến nhất mà kẻ tấn công có thể thực hiện để chiếm quyền kiểm soát hoặc làm gián đoạn kết nối của người dùng.

Tác động của tấn công deauthentication:

- **Mất dữ liệu:** Khi người dùng bị ngắt kết nối khỏi mạng, họ có thể mất dữ liệu quan trọng đang được truyền tải.
- **Lộ thông tin cá nhân:** Kẻ tấn công có thể tạo ra một điểm truy cập giả mạo (Evil Twin) và dụ người dùng kết nối vào đó để đánh cắp thông tin cá nhân như mật khẩu, thông tin tài khoản ngân hàng.

- **Gián đoạn dịch vụ:** Tấn công này có thể gây ra sự gián đoạn trong việc sử dụng Internet, ảnh hưởng đến trải nghiệm người dùng và hoạt động kinh doanh.

3. Mục tiêu và phạm vi nghiên cứu

Mục tiêu chính của luận văn này là phát triển một công cụ phát hiện tấn công deauthentication dựa trên phân tích lưu lượng mạng trong thời gian thực. Công cụ này sẽ sử dụng các thư viện như Scapy và Wireshark để theo dõi và phân tích các gói tin trong mạng Wi-Fi, từ đó phát hiện kịp thời các dấu hiệu của cuộc tấn công.

Phạm vi nghiên cứu:

- Mạng Wi-Fi sử dụng giao thức 802.11: Nghiên cứu sẽ tập trung vào việc phát hiện tấn công deauthentication trong các mạng không dây sử dụng giao thức IEEE 802.11.
- Phân tích lưu lượng mạng: Sử dụng Scapy và Wireshark để thu thập và phân tích lưu lượng mạng nhằm phát hiện các gói tin deauthentication giả mạo.

CHƯƠNG 2: CƠ SỞ LÝ THUYẾT

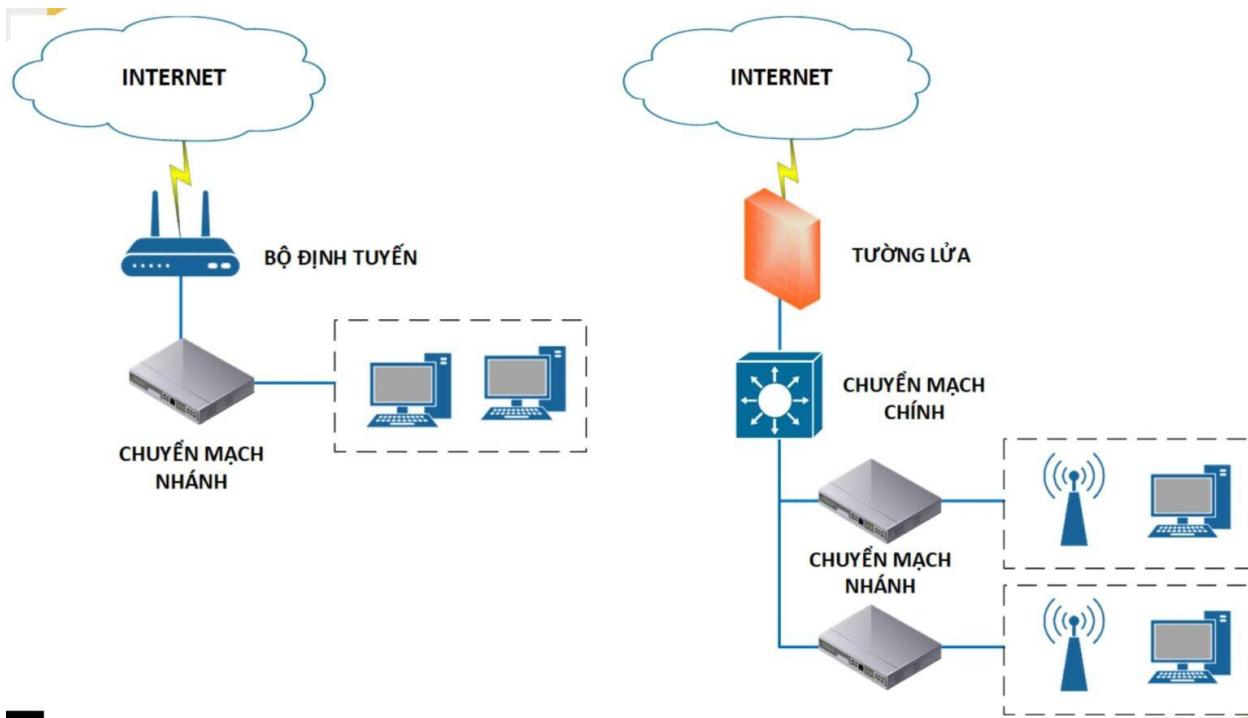
1. Tổng quan về mạng Wi-Fi (IEEE 802.11)

a. Kiến trúc mạng Wi-Fi

Mạng Wi-Fi, hay còn gọi là mạng không dây, cho phép các thiết bị kết nối và giao tiếp với nhau thông qua sóng radio mà không cần sử dụng dây cáp. Kiến trúc của một mạng Wi-Fi thường bao gồm các thành phần chính sau:

- Access Point (AP):
 - Là thiết bị trung gian kết nối giữa các thiết bị không dây (Client) và mạng có dây (wired network). AP phát sóng tín hiệu Wi-Fi, cho phép các thiết bị trong phạm vi kết nối vào mạng.

- AP thường được kết nối với router hoặc switch qua cáp Ethernet và có thể phát sóng một hoặc nhiều SSID (Service Set Identifier), giúp người dùng dễ dàng chọn lựa mạng để kết nối.
- Client:
 - Là các thiết bị như laptop, smartphone, máy tính bảng và các thiết bị IoT (Internet of Things) mà người dùng sử dụng để truy cập Internet qua mạng Wi-Fi.
 - Mỗi Client sẽ có một card mạng không dây (Wireless Network Interface Card - WNIC) để nhận tín hiệu từ AP.
- Router:
 - Là thiết bị quản lý lưu lượng dữ liệu giữa mạng nội bộ và Internet. Router thường tích hợp chức năng của AP, nhưng cũng có thể hoạt động độc lập với AP.
 - Router thực hiện việc phân phối địa chỉ IP cho các Client thông qua DHCP (Dynamic Host Configuration Protocol) và quản lý các kết nối Internet.



Hình 1. Mô hình mạng cơ bản

b. Cơ chế kết nối Wifi

Khi một thiết bị bị kết nối đến Access Point (AP) thông qua WiFi, cơ chế hoạt động như sau:

1. Khởi tạo kết nối

- Tìm kiếm mạng: Thiết bị không dây (ví dụ: laptop, điện thoại) sẽ quét các mạng WiFi có sẵn trong khu vực.
- Chọn mạng: Người dùng chọn mạng WiFi mà họ muốn kết nối.

2. Giao tiếp với Access Point

- Gửi yêu cầu kết nối: Thiết bị gửi yêu cầu kết nối đến Access Point.
- Xác thực: Access Point sẽ thực hiện quá trình xác thực, thường bằng cách sử dụng mật khẩu hoặc các phương thức bảo mật khác như WPA2.

3. Thiết lập kết nối

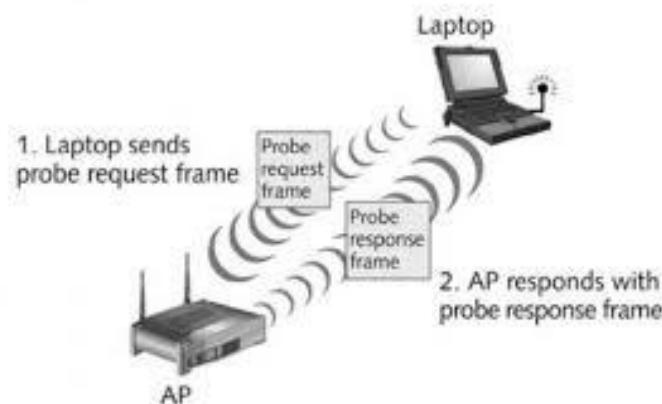
- Gán địa chỉ IP: Sau khi xác thực thành công, thiết bị sẽ được gán một địa chỉ IP từ mạng cục bộ thông qua DHCP (nếu được cấu hình).
- Kết nối thành công: Thiết bị có thể truy cập Internet hoặc các tài nguyên mạng nội bộ thông qua Access Point.

4. Truyền và nhận dữ liệu

- Truyền dữ liệu: Khi thiết bị gửi dữ liệu, nó sẽ truyền tín hiệu không dây đến Access Point.
- Nhận dữ liệu: Access Point nhận tín hiệu này và chuyển đổi nó thành tín hiệu có dây để gửi đến router hoặc modem, sau đó đến Internet hoặc mạng nội bộ.
- Nhận dữ liệu từ Internet: Quá trình ngược lại cũng diễn ra khi dữ liệu từ Internet được gửi về thiết bị thông qua Access Point.

5. Di chuyển giữa các Access Point

- Chuyển vùng: Nếu thiết bị di chuyển ra ngoài phạm vi của một Access Point, nó sẽ tự động kết nối với một Access Point khác gần đó nếu có sẵn, đảm bảo kết nối không bị gián đoạn.



Hình 2. Client kết nối AP

c. Giao thức 802.11

Giao thức IEEE 802.11 là tiêu chuẩn kỹ thuật cho mạng không dây, quy định cách thức truyền tải dữ liệu qua sóng radio. Giao thức này bao gồm nhiều phiên bản khác nhau, mỗi phiên bản có những đặc điểm riêng biệt.

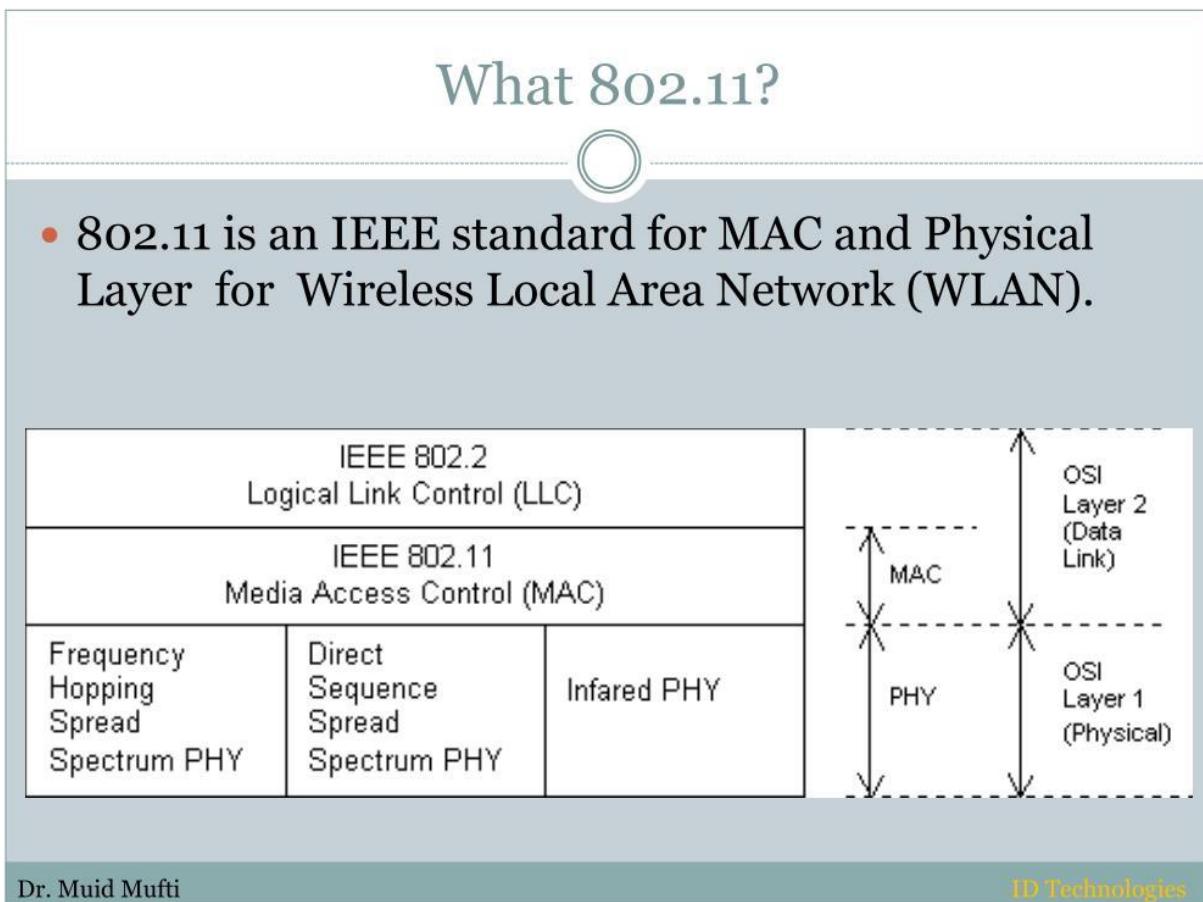
- Khung quản lý (Management Frames): Các khung này được sử dụng để quản lý kết nối giữa AP và Client, bao gồm nhiều loại khung như:
 - Beacon Frame: Gửi định kỳ từ AP để thông báo sự tồn tại của nó và cung cấp thông tin về SSID cùng các tham số khác cho các WNIC trong phạm vi.
 - Deauthentication Frame: Khung được gửi từ một Client hoặc AP khi muốn ngắt kết nối.
 - Disassociation Frame: Khung yêu cầu AP hủy bỏ kết nối của Client.

Giao thức IEEE 802.11 đã trải qua nhiều phiên bản khác nhau, mỗi phiên bản cải thiện về tốc độ và hiệu suất:

- 802.11b: Ra mắt năm 1999, hoạt động ở băng tần 2.4 GHz với tốc độ tối đa lên tới 11 Mbps.
- 802.11a: Cũng ra mắt năm 1999, hoạt động ở băng tần 5 GHz với tốc độ tối đa lên tới 54 Mbps.
- 802.11g: Phát hành năm 2003, kết hợp ưu điểm của cả hai chuẩn trước đó, hoạt động ở băng tần 2.4 GHz với tốc độ tối đa lên tới 54 Mbps.
- 802.11n: Ra mắt năm 2009, hỗ trợ MIMO (Multiple Input Multiple Output) cho phép truyền tải đồng thời nhiều luồng dữ liệu, tốc độ

tối đa lên tới 600 Mbps và hoạt động ở cả băng tần 2.4 GHz và 5 GHz.

- 802.11ac: Phát hành năm 2013, chủ yếu hoạt động ở băng tần 5 GHz với tốc độ lý thuyết tối đa lên tới 1,3 Gbps nhờ vào công nghệ MU-MIMO (Multi User MIMO).
- 802.11ax (Wi-Fi 6): Ra mắt năm 2019, cải thiện hiệu suất trong môi trường đông đúc với tốc độ lý thuyết tối đa lên tới 9,6 Gbps và hỗ trợ cả băng tần 2.4 GHz và 5 GHz.



Hình 3. Tổng quan về 802.11

d. Bảo mật mạng Wi-Fi

Bảo mật trong mạng Wi-Fi rất quan trọng để bảo vệ thông tin người dùng và ngăn chặn các cuộc tấn công không mong muốn. Các giao thức bảo mật phổ biến bao gồm:

- WEP (Wired Equivalent Privacy): Là giao thức bảo mật đầu tiên được sử dụng cho Wi-Fi, nhưng đã bị phát hiện nhiều lỗ hổng bảo mật nghiêm trọng khiến nó không còn an toàn.
- WPA (Wi-Fi Protected Access): Cải thiện bảo mật so với WEP bằng cách sử dụng mã hóa TKIP (Temporal Key Integrity Protocol). Tuy nhiên, WPA vẫn còn một số điểm yếu.
- WPA2: Giới thiệu vào năm 2004, WPA2 sử dụng mã hóa AES (Advanced Encryption Standard), cung cấp mức độ bảo mật cao hơn so với WPA.
- WPA3: Giao thức mới nhất với nhiều cải tiến về bảo mật, bao gồm khả năng chống lại tấn công brute-force và nâng cao bảo vệ dữ liệu cá nhân thông qua phương pháp xác thực mới gọi là SAE (Simultaneous Authentication of Equals).

VISUALIZATION OF MAIN DIFFERENCES BETWEEN THE SECURITY PROTOCOLS

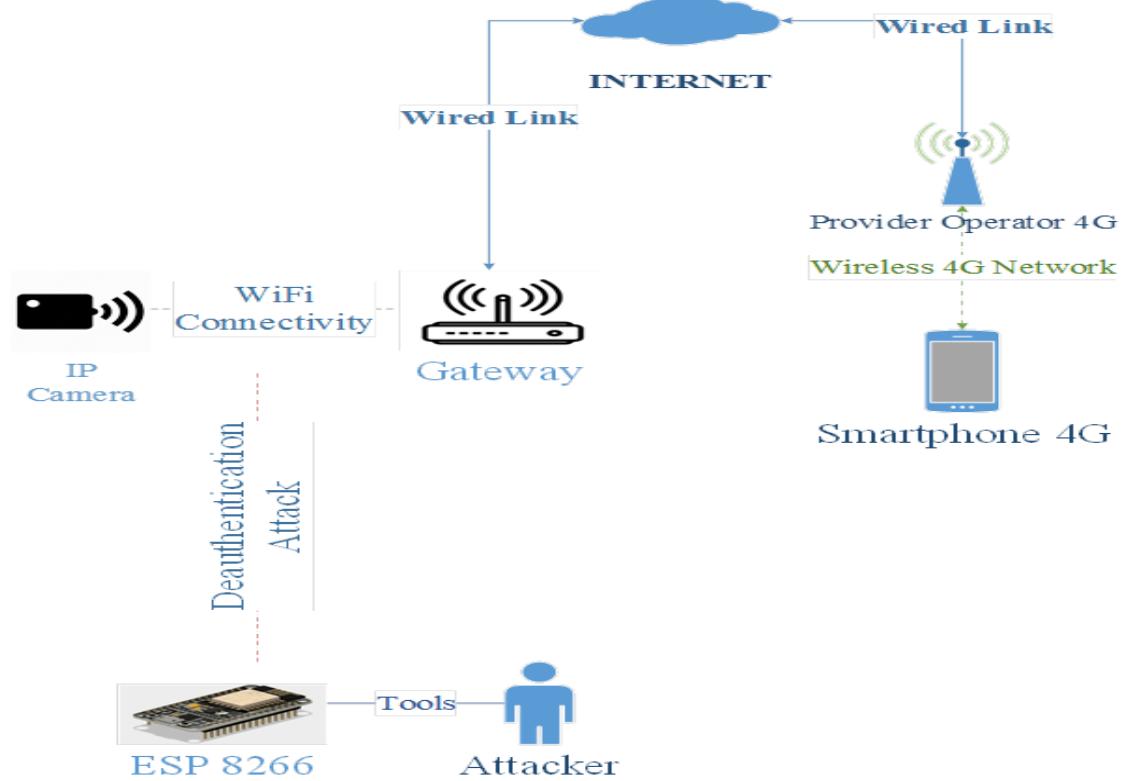
	WEP	WEP	WPA2	WPA3
Brief description	Ensure wired-like privacy in wireless	Based on 802.11i without requirement for new hardware	All mandatory 802.11i features and a new hardware	Announced by Wi-Fi Alliance
Encryption	RC4	TKIP+RC4	CCMP/AES	GCMP-256
Authentication	WEP-Open WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-personal WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
Data integrity	CRC-32	MIC algorithm	Cipher Block Chaining Message Authentication Code (based on AES)	256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)
Key management	none	4-way handshake	4-way handshake	Elliptic Curve Diffie-Helman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA)

Hình 4. So sánh về các loại bảo mật

2. Tấn công Deauthentication

a. Định nghĩa

Tấn công deauthentication là một hình thức tấn công từ chối dịch vụ (Denial of Service - DoS) nhắm vào mạng Wi-Fi, trong đó kẻ tấn công gửi các gói tin deauthentication giả mạo nhằm ngắt kết nối thiết bị của người dùng khỏi điểm truy cập (Access Point - AP). Tấn công này thường được thực hiện để gây gián đoạn dịch vụ hoặc tạo cơ hội cho các cuộc tấn công khác, như tấn công Man-in-the-Middle (MitM).



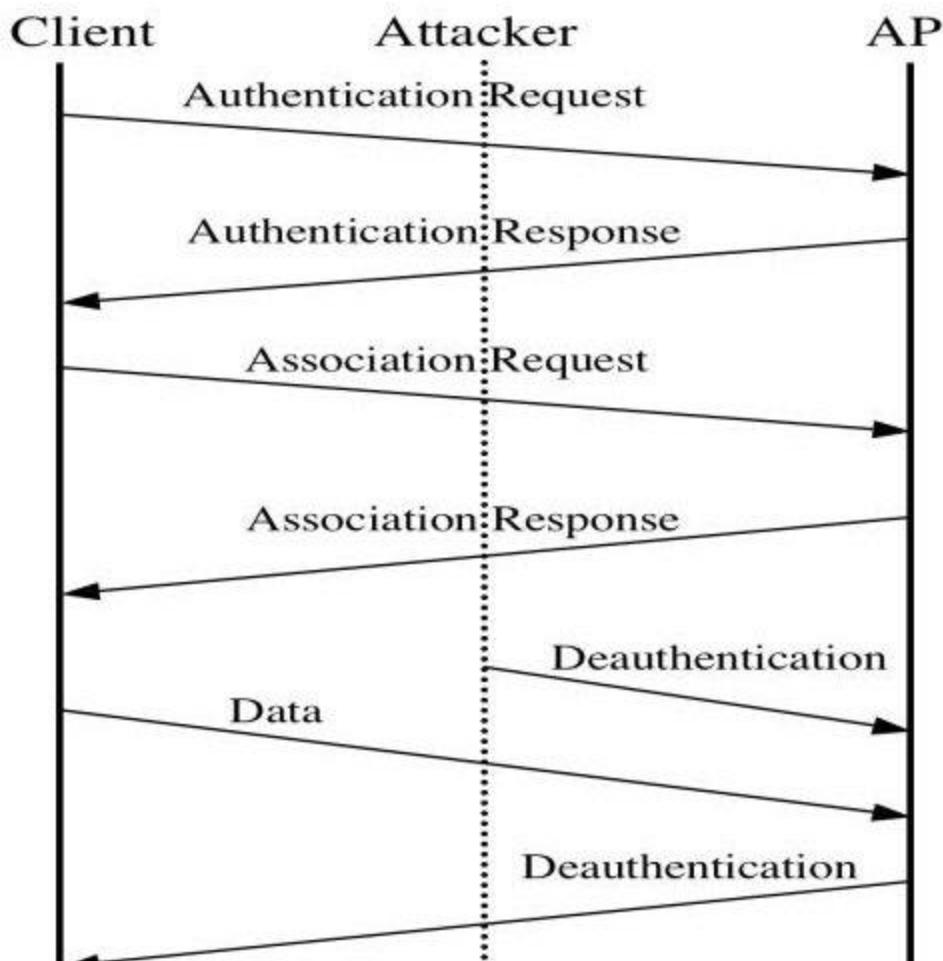
Hình 5. Tấn công DeAuthentication

b. Cơ chế tấn công

Quá trình thực hiện tấn công deauthentication thường diễn ra qua các bước sau:

- Khảo sát và thu thập thông tin:
 - Kẻ tấn công sử dụng các công cụ như Kismet hoặc Airodump-ng để quét và thu thập thông tin về các điểm truy cập và thiết bị kết nối trong khu vực, bao gồm địa chỉ MAC của AP và Client.
- Gửi gói tin Deauthentication:
 - Kẻ tấn công gửi gói tin deauthentication đến AP hoặc trực tiếp đến Client với địa chỉ MAC giả mạo, giả vờ rằng nó là thiết bị muốn ngắt kết nối.

- Gói tin deauthentication chứa thông tin về địa chỉ MAC nguồn (kẻ tấn công) và địa chỉ MAC đích (Client hoặc AP), khiến AP hoặc Client tin rằng kết nối đã bị yêu cầu ngắt.
- Ngắt kết nối:
 - Khi nhận được gói tin deauthentication, AP sẽ thực hiện ngắt kết nối Client khỏi mạng, dẫn đến việc Client không còn khả năng truy cập Internet.
- Lặp lại quá trình:
 - Kẻ tấn công có thể lặp lại quy trình này nhiều lần để ngắt kết nối liên tục nhiều thiết bị trong mạng.



Hình 6. Cơ chế tấn công

c. Các biến thể của tấn công

Tấn công deauthentication có thể được thực hiện theo nhiều cách khác nhau, bao gồm:

- Tấn công nhắm vào mục tiêu cụ thể:
 - Kẻ tấn công chỉ định một Client cụ thể để ngắt kết nối bằng cách gửi gói tin deauthentication đến địa chỉ MAC của Client đó.
- Tấn công diện rộng:

- Kẻ tấn công gửi gói tin deauthentication đến tất cả các Client trong mạng, làm gián đoạn toàn bộ kết nối.
- Tấn công Flood Deauthentication:
 - Một dạng nâng cao của tấn công deauthentication, trong đó kẻ tấn công gửi một số lượng lớn gói tin deauthentication trong thời gian ngắn nhằm làm quá tải và ngăn chặn việc sử dụng mạng.

d. **Động cơ tấn công**

Kẻ tấn công có thể thực hiện tấn công deauthentication vì nhiều lý do khác nhau:

- Đánh cắp thông tin:
 - Sau khi ngắt kết nối, kẻ tấn công có thể tạo ra một điểm truy cập giả mạo (Evil Twin) để dụ người dùng kết nối vào đó và thu thập thông tin nhạy cảm như mật khẩu hoặc thông tin tài khoản ngân hàng.
- Từ chối dịch vụ:
 - Tạo ra sự gián đoạn trong việc sử dụng Internet của người dùng, gây khó chịu hoặc thiệt hại cho hoạt động kinh doanh.
- Tạo cơ hội cho các cuộc tấn công khác:
 - Tấn công deauthentication có thể được sử dụng như một bước đầu tiên để thực hiện các cuộc tấn công khác như Man-in-the-Middle (MitM), nơi kẻ tấn công có thể can thiệp vào lưu lượng dữ liệu giữa Client và AP.

3. Các công cụ và kỹ thuật phát hiện tấn công

a. Scapy

Giới thiệu về Scapy

- Scapy là một công cụ mã nguồn mở được viết bằng ngôn ngữ lập trình Python, cho phép người dùng gửi, bắt và phân tích các gói tin mạng. Scapy được thiết kế để thực hiện nhiều tác vụ như quét mạng, thăm dò, kiểm tra bảo mật, và tấn công mạng. Công cụ này rất linh hoạt và có thể thay thế cho nhiều công cụ khác như Nmap, tcpdump, và hping.

Các chức năng chính của Scapy

- Gửi gói tin: Scapy cho phép người dùng tạo và gửi các gói tin tùy chỉnh đến các địa chỉ IP hoặc MAC cụ thể. Người dùng có thể định nghĩa các lớp gói tin (layer) khác nhau để xây dựng gói tin phức tạp.
- Bắt gói tin: Scapy có khả năng bắt và phân tích các gói tin đang lưu thông trên mạng. Người dùng có thể chỉ định giao diện mạng để bắt gói tin hoặc để trống để bắt tất cả.
- Phân tích gói tin: Sau khi bắt được các gói tin, Scapy cung cấp khả năng phân tích và hiển thị thông tin chi tiết về các gói tin này, giúp người dùng hiểu rõ hơn về lưu lượng mạng.
- Giả mạo gói tin: Scapy cho phép người dùng giả mạo các gói tin mạng, bao gồm việc gửi các gói không hợp lệ hoặc thay đổi thông tin trong gói tin để kiểm tra tính bảo mật của hệ thống.

Ứng dụng của Scapy

- Quét mạng: Sử dụng Scapy để quét các địa chỉ IP trong một dải địa chỉ nhất định để phát hiện thiết bị đang hoạt động.
- Tấn công DoS: Scapy có thể được sử dụng để thực hiện các cuộc tấn công từ chối dịch vụ (DoS) bằng cách gửi nhiều gói tin đến một thiết bị mục tiêu.

- Phân tích bảo mật: Scapy giúp kiểm tra lỗ hổng bảo mật trong hệ thống bằng cách gửi các gói tin giả mạo và phân tích phản hồi từ hệ thống.

```

SCAPY

WARNING: No route found for IPv6 destination :: (no default route?)

          aSPY//YASa
          apyyyyCY//////////YCa
          sY//////YSpcs  scpCY//Pp
  ayp ayyyyyyySCP//Pp           sy//C
  AYAsAYYYYYYYY///Ps           cY//S
          pCCCCY//p           cSSps y//Y
          SPPPP//a           pP//AC//Y
          A//A               cyP///C
          p///Ac             sC//a
          P///YCpc           A//A
          scccccp///pSP///p   p//Y
          sY/////////y caa    S//P
          cayCyayP//Ya       pY/Ya
          sY/PsY///YCc       aC//Yp
          sc  sccaCY//PCyapaCP//YSs
          spCPY//////YPSPs
          ccaacs

          using IPython 5.5.0

>>> ICMPTimeStampField
ICMP
ICMPerror
ICMPTimeStampField
ICMPv6MLQuery
ICMPv6MLReport
ICMPv6MPAdv
  
```

Hình 7. Phần mềm Scapy

b. Wireshark

Giới thiệu về Wireshark

- Wireshark là một công cụ phân tích gói tin mã nguồn mở nổi tiếng nhất trên thế giới, cho phép người dùng theo dõi và phân tích lưu lượng mạng trong thời gian thực. Wireshark hỗ trợ nhiều giao thức khác nhau và cung cấp giao diện đồ họa thân thiện giúp người dùng dễ dàng truy cập vào dữ liệu mạng.

Các chức năng chính của Wireshark

- **Bắt gói tin:** Wireshark có khả năng bắt tất cả các loại gói tin trên mạng mà không cần cấu hình phức tạp. Người dùng có thể chọn giao diện mạng mà họ muốn theo dõi.
- **Phân tích giao thức:** Wireshark hỗ trợ hàng trăm giao thức khác nhau, cho phép người dùng phân tích chi tiết từng gói tin theo giao thức mà nó sử dụng.
- **Lọc dữ liệu:** Người dùng có thể sử dụng bộ lọc để chỉ hiển thị những gói tin mà họ quan tâm, giúp giảm tải thông tin không cần thiết.
- **Ghi lại lưu lượng:** Wireshark cho phép người dùng ghi lại lưu lượng mạng vào file để phân tích sau này.

Ứng dụng của Wireshark

- **Khắc phục sự cố mạng:** Wireshark giúp xác định nguyên nhân gây ra sự cố mạng bằng cách phân tích lưu lượng và tìm kiếm các vấn đề như mất kết nối hoặc độ trễ cao.
- **Kiểm tra bảo mật:** Wireshark có thể được sử dụng để phát hiện các cuộc tấn công vào mạng bằng cách theo dõi lưu lượng bất thường hoặc đáng ngờ.
- **Nghiên cứu giao thức:** Các nhà phát triển có thể sử dụng Wireshark để nghiên cứu và phát triển các giao thức mới bằng cách phân tích cách mà chúng hoạt động trong môi trường thực tế.



Hình 8. Phần mềm Wireshark

c. So sánh với một số công cụ khác

Bảng 1. So sánh các công cụ

Tiêu chí	Wireshark	Scapy	Kismet	Aircrack-ng
Mục đích chính	Phân tích gói tin, kiểm tra mạng	Xử lý gói tin bằng Python, tự động hóa phân tích	Phát hiện và giám sát Wi-Fi	Đánh giá bảo mật Wi-Fi, giám sát mạng
Giao diện	Đồ họa (GUI)	Dòng lệnh (Python)	Đồ họa (Web UI, TUI)	Dòng lệnh (CLI)
Cách hoạt động	Dùng bộ lọc để tìm gói Deauthentication	Viết script để bắt và phân tích gói tin	Giám sát tự động, cảnh báo nếu phát hiện tấn công	Giám sát mạng không dây, hiển thị gói Deauthentication
Phát hiện Deauthentication tự động	<input checked="" type="checkbox"/> (Cần lọc gói thủ công)	<input checked="" type="checkbox"/> (Viết script phát hiện)	<input checked="" type="checkbox"/> (Tự động cảnh báo)	<input checked="" type="checkbox"/> (Hiển thị số lượng gói Deauthentication)
Tốc độ phát hiện	Trung bình	Nhanh (nếu viết script tối ưu)	Nhanh	Nhanh

Khả năng chặn tấn công	<input checked="" type="checkbox"/> Không thể chặn	<input checked="" type="checkbox"/> Có thể viết script để chặn	<input checked="" type="checkbox"/> Không thể chặn	<input checked="" type="checkbox"/> Không thể chặn
Khả năng phân tích sâu	<input checked="" type="checkbox"/> Hiển thị toàn bộ gói tin	<input checked="" type="checkbox"/> Tùy chỉnh theo nhu cầu	<input checked="" type="checkbox"/> Chỉ hiển thị cảnh báo tổng quát	<input checked="" type="checkbox"/> Chỉ hiển thị số lượng gói
Hỗ trợ giám sát liên tục	<input checked="" type="checkbox"/> Không có chế độ giám sát liên tục	<input checked="" type="checkbox"/> Có thể lập trình để giám sát liên tục	<input checked="" type="checkbox"/> Tích hợp sẵn	<input checked="" type="checkbox"/> Có thể chạy liên tục
Yêu cầu Monitor Mode	<input checked="" type="checkbox"/> Cần bật Monitor Mode	<input checked="" type="checkbox"/> Cần bật Monitor Mode	<input checked="" type="checkbox"/> Cần bật Monitor Mode	<input checked="" type="checkbox"/> Cần bật Monitor Mode
Khả năng tùy chỉnh	<input checked="" type="checkbox"/> Có thể viết bộ lọc riêng	<input checked="" type="checkbox"/> Hoàn toàn tùy chỉnh	<input checked="" type="checkbox"/> Ít tùy chỉnh	<input checked="" type="checkbox"/> Ít tùy chỉnh
Khả năng kết hợp với công cụ khác	<input checked="" type="checkbox"/> Kết hợp với Tshark, Snort...	<input checked="" type="checkbox"/> Kết hợp với các thư viện Python khác	<input checked="" type="checkbox"/> Kết hợp với Snort, Suricata	<input checked="" type="checkbox"/> Kết hợp với Airbase-ng, Aireplay-ng
Hỗ trợ hệ điều hành	Windows, Linux, macOS	Linux, Windows (giới hạn)	Linux, macOS, Raspberry Pi	Linux, Windows
Mức độ khó sử dụng	Trung bình	Khó (cần code Python)	Dễ	Trung bình
Tài nguyên yêu cầu	Cao (GUI, xử lý nhiều gói tin)	Thấp (chạy trên Python)	Trung bình (chạy nền)	Thấp

d. Kỹ thuật phân tích lưu lượng mạng

Để phát hiện tấn công deauthentication, có thể áp dụng một số kỹ thuật phân tích lưu lượng mạng như:

- **Thống kê số lượng gói tin Deauthentication:** Theo dõi số lượng gói tin deauthentication trong một khoảng thời gian nhất định để phát hiện sự gia tăng bất thường.

- Phân tích thời gian giữa các gói tin: Xác định khoảng thời gian giữa các gói tin để tìm kiếm sự bất thường trong lưu lượng.
- Xác định địa chỉ MAC bất thường: Phát hiện địa chỉ MAC nguồn của gói tin deauthentication không khớp với địa chỉ MAC của Client đã kết nối trước đó.

4. Các biện pháp phòng chống tấn công

Trong bối cảnh các cuộc tấn công deauthentication ngày càng trở nên phổ biến, việc triển khai các biện pháp phòng chống hiệu quả là rất cần thiết để bảo vệ an ninh mạng không dây. Dưới đây là một số biện pháp quan trọng mà tổ chức có thể áp dụng.

a. 802.11w (Protected Management Frames)

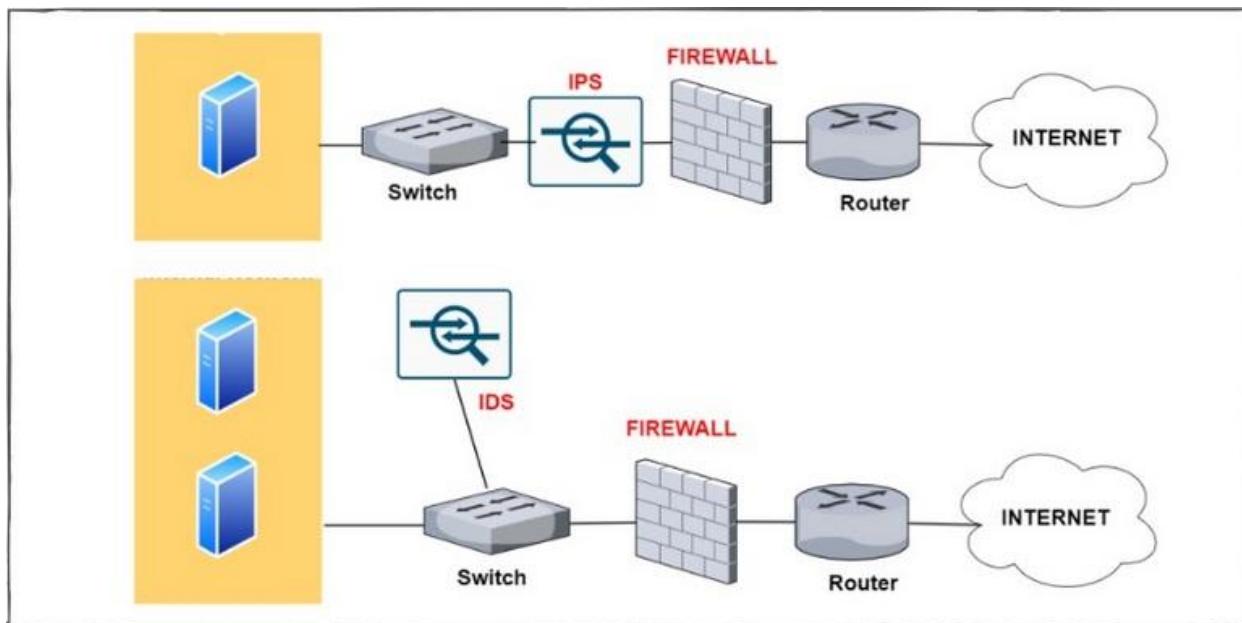
Giao thức 802.11w được thiết kế để bảo vệ các khung quản lý trong mạng Wi-Fi bằng cách mã hóa chúng, giúp ngăn chặn kẻ tấn công giả mạo gửi gói tin deauthentication hoặc disassociation.

- Cách thức hoạt động:
 - Mã hóa khung quản lý: Giao thức này mã hóa các khung quản lý như deauthentication và disassociation, làm cho chúng không thể bị giả mạo bởi kẻ tấn công.
 - Xác thực: Khi một thiết bị (Client) muốn ngắt kết nối, nó sẽ gửi yêu cầu đến AP với thông tin được mã hóa. AP chỉ chấp nhận yêu cầu từ các thiết bị đã được xác thực.
- Lợi ích:
 - Giảm thiểu nguy cơ bị tấn công deauthentication.
 - Tăng cường bảo mật cho các kết nối không dây.

b. Phát hiện và ngăn chặn xâm nhập (IDS/IPS)

Hệ thống IDS (Intrusion Detection System) và IPS (Intrusion Prevention System) có thể được triển khai để giám sát lưu lượng mạng và phát hiện hành vi bất thường liên quan đến tấn công deauthentication.

- Phát hiện dựa trên quy tắc:
 - Sử dụng quy tắc để xác định khi nào có sự gia tăng đột biến trong số lượng gói tin deauthentication.
 - Hệ thống có thể phân tích lưu lượng mạng và nhận diện các mẫu gói tin đáng ngờ.
- Ngăn chặn tự động:
 - Khi phát hiện hành vi đáng ngờ, hệ thống có thể tự động chặn IP nguồn hoặc gửi cảnh báo cho quản trị viên hệ thống.
 - Một số hệ thống có khả năng tự động phản hồi bằng cách gửi gói tin deauthentication đến kẻ tấn công để ngắt kết nối của họ khỏi mạng.



Hình 9. Minh họa IDS và IPS

c. Các biện pháp bảo mật khác

Ngoài việc sử dụng giao thức bảo vệ khung quản lý và hệ thống IDS/IPS, còn có nhiều biện pháp bảo mật khác mà tổ chức có thể áp dụng:

- Tăng cường bảo mật mật khẩu:
 - Sử dụng mật khẩu mạnh, bao gồm chữ hoa, chữ thường, số và ký tự đặc biệt.
 - Thay đổi mật khẩu định kỳ để giảm thiểu rủi ro từ việc xâm nhập trái phép vào mạng.
- Sử dụng VPN (Virtual Private Network):
 - Mã hóa toàn bộ lưu lượng truy cập Internet giúp bảo vệ thông tin cá nhân ngay cả khi người dùng đang ở trên mạng không an toàn.
 - VPN cũng giúp ngăn chặn các cuộc tấn công từ chối dịch vụ bằng cách tạo một lớp bảo vệ cho lưu lượng mạng.
- Nâng cao nhận thức của người dùng về an ninh mạng:
 - Giáo dục người dùng về các mối đe dọa an ninh mạng như tấn công deauthentication và cách phòng tránh.
 - Khuyến khích người dùng không kết nối vào các điểm truy cập không rõ nguồn gốc hoặc không quen thuộc.

d. So sánh giữa các biện pháp

Bảng 2. Bảng so sánh giữa các công cụ

Biện pháp	Mô tả	Lợi ích	Hạn chế
-----------	-------	---------	---------

802.11w (Protected Management Frames)	Mã hóa các khung quản lý như deauthentication và disassociation để ngăn chặn giả mạo.	Giảm thiểu tấn công deauthentication, tăng cường bảo mật.	Cần thiết bị hỗ trợ 802.11w.
IDS/IPS (Hệ thống phát hiện và ngăn chặn xâm nhập)	Giám sát lưu lượng mạng, phát hiện và ngăn chặn hành vi bất thường.	Phát hiện và ngăn chặn tự động các cuộc tấn công.	Cần cấu hình và cập nhật thường xuyên.
Tăng cường bảo mật mật khẩu	Sử dụng mật khẩu mạnh và thay đổi định kỳ.	Ngăn chặn xâm nhập trái phép vào mạng.	Người dùng cần tuân thủ các quy định về mật khẩu.
Sử dụng VPN (Virtual Private Network)	Mã hóa toàn bộ lưu lượng truy cập Internet.	Bảo vệ thông tin cá nhân trên mạng không an toàn, ngăn chặn tấn công từ chối dịch vụ.	Cần đăng ký dịch vụ VPN.
Nâng cao nhận thức của người dùng	Giáo dục người dùng về an ninh mạng.	Giảm thiểu rủi ro từ các hành động thiếu hiểu biết.	Cần thời gian và nỗ lực để giáo dục người dùng.

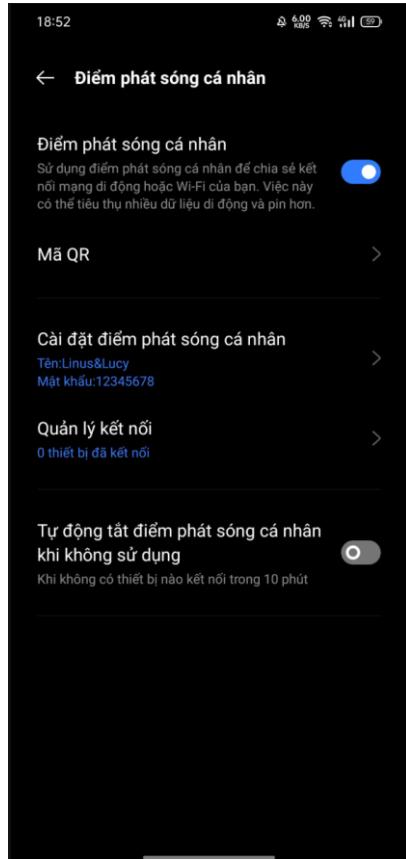
CHƯƠNG 3: PHƯƠNG PHÁP THỰC HIỆN

1. Mô tả danh sách thiết bị

- Máy ảo:** Một máy ảo chạy linux (Máy ảo vừa làm máy tấn công, vừa làm máy phát hiện)
- Điện thoại:** 2 chiếc điện thoại, một cái dùng để làm cục phát wifi, một cái để làm mẫu cho điện thoại của nạn nhân
- Adapter Wifi:** 1 Chipset Wifi có hỗ trợ chế độ Monitor Mode

2. Cấu hình

- Sử dụng máy ảo Kali linux bản 2024.4 chạy trên Vmware
- Adapter Wi-Fi được kết nối với máy ảo qua USB Passthrough
- Cấu hình điện thoại ở chức năng phát wifi:

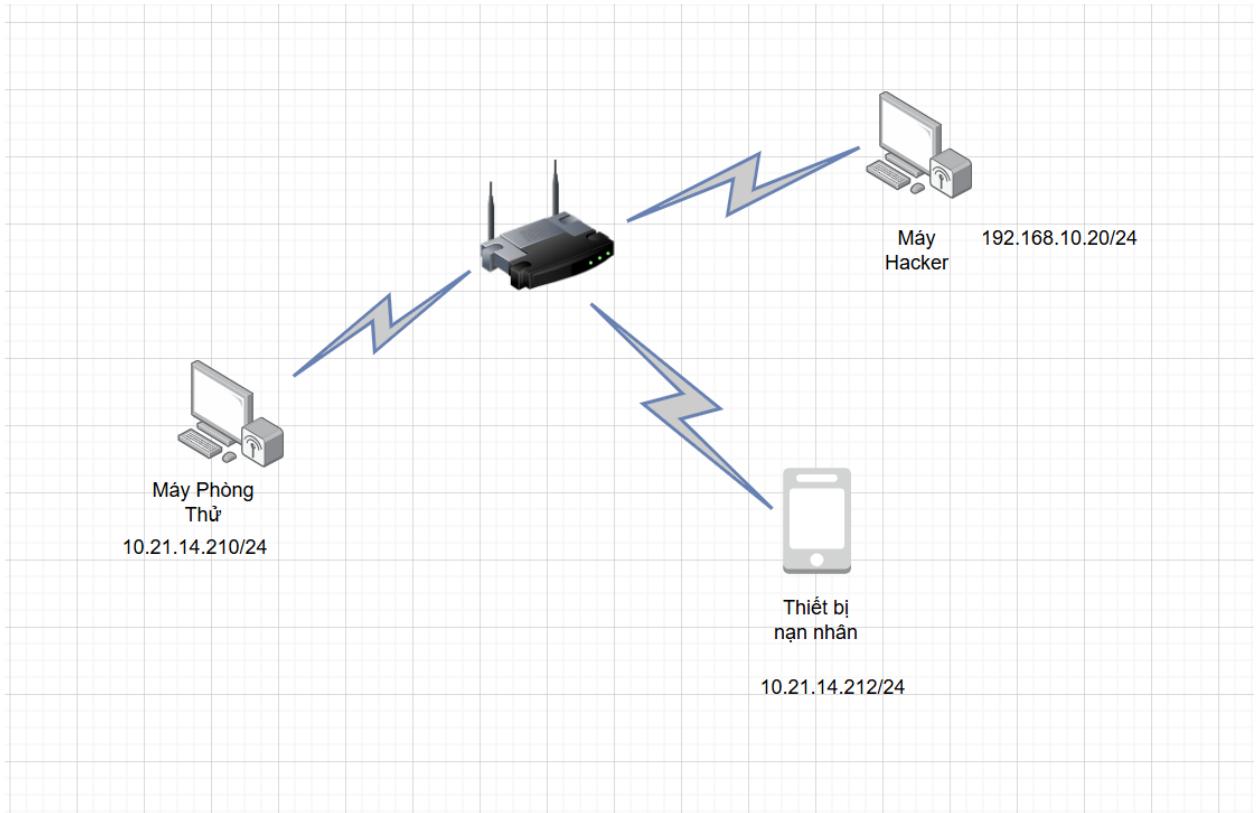


Hình 10. Thiết lập điểm phát wifi

3. Môi trường thực hiện

- Mạng Wifi thử nghiệm: Băng tần 2.4GHz và 5GHz với bảo mật bằng WPA2-PSK
- Công cụ tấn công: Sử dụng phần mềm Scapy và chạy Script để tấn công
- Công cụ phát hiện: Sử dụng phần mềm Scapy và chạy Script để phát hiện tấn công
- Nền tảng thông báo khi phát hiện tấn công: Telegram
- Sử dụng Vmware để chạy ảo hóa hệ điều hành kali linux 2024.4
- Điều kiện thực hiện: Khi đang có thiết bị kết nối tới wifi và tấn công

4. Sơ đồ mạng

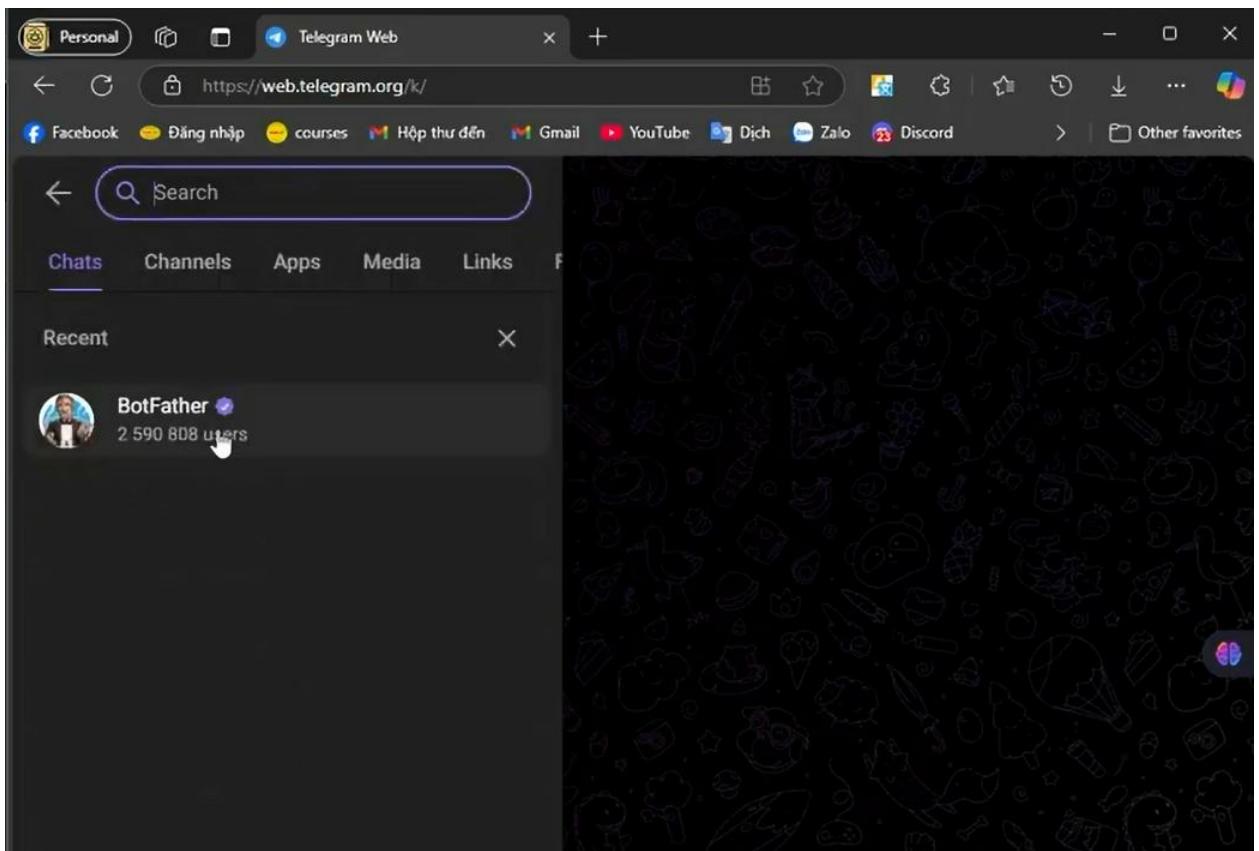


Hình 11. Sơ đồ mạng

CHƯƠNG 4: TRIỄN KHAI

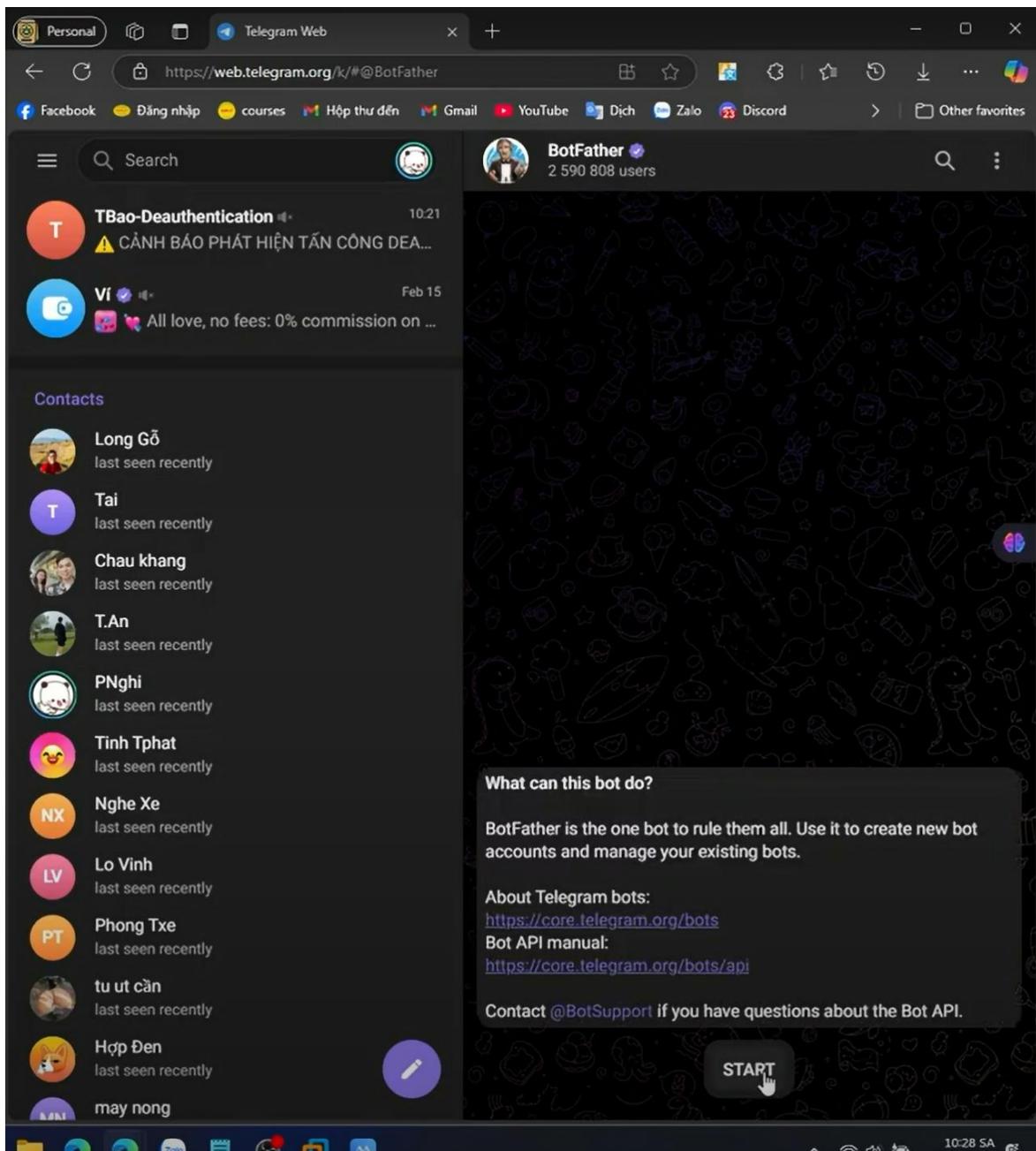
1. Triển khai và cấu hình

Bước 1: Truy cập vào telegram và tìm kiếm BotFather



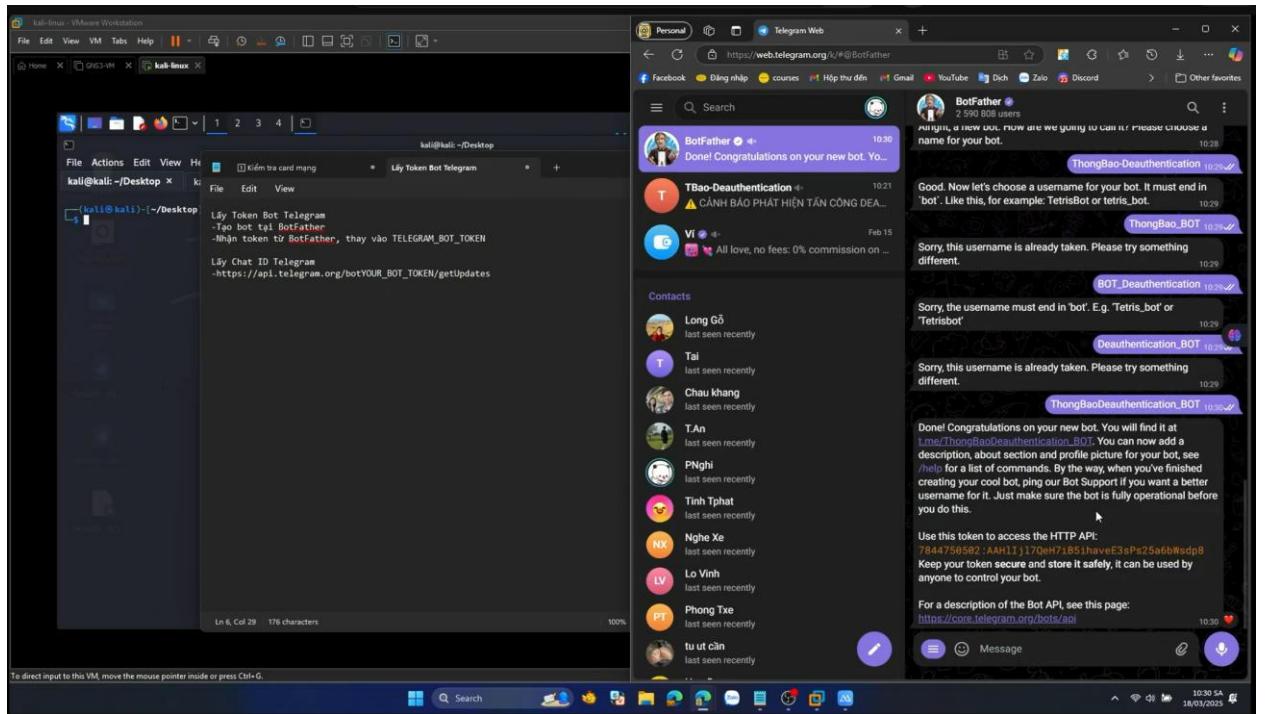
Hình 12. Tìm kiếm bot

Bước 2: nhấn nút Star để kích hoạt bot

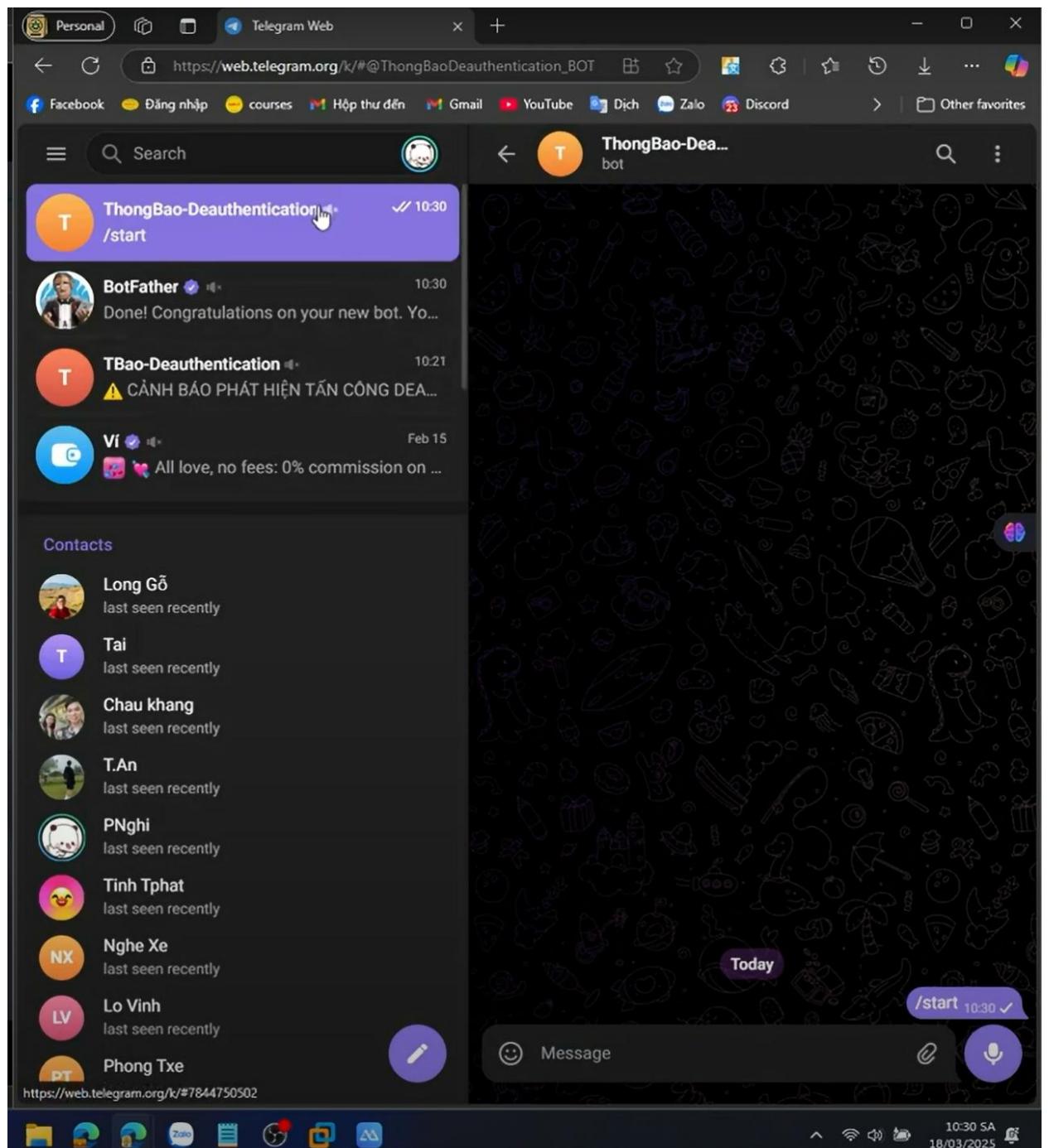


Hình 13. Khởi động bot

Bước 3: Nhập lệnh ThongBaoDeauthentication_BOT để tạo ra một kênh thông báo sau đó nhấn vào đường link t.me/ ThongBaoDeauthentication_BOT để vào phòng chat

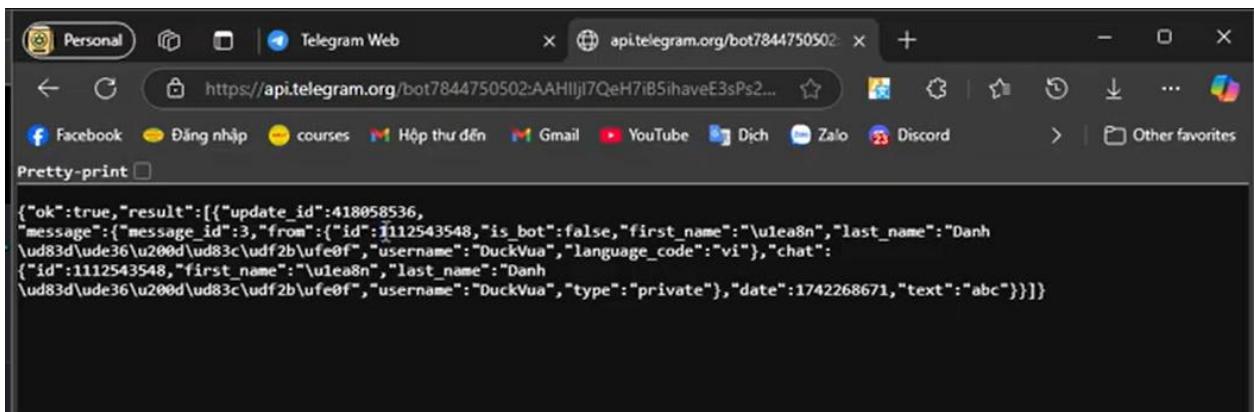


Hình 14. Tạo kênh chat cho bot



Hình 15. Kênh chat khi tham gia

Bước 4: lấy id phòng chat và bot token để có thể nhận được thông báo



The screenshot shows a browser window with the URL <https://api.telegram.org/bot7844750502:AAHIIjI7QeH7iB5ihaveE3sPs2...>. The page displays a JSON response with the "Pretty-print" option checked. The response contains an "ok": true message with a "result" array containing one element. This element is a dictionary with fields: update_id (418058536), message (a dictionary with fields: message_id (3), from (a dictionary with fields: id (112543548), is_bot (false), first_name (\u01ea8n), last_name (Danh \ud83d\ude36\u200d\ud83c\udf2b\ufe0f), username (DuckVua), language_code (vi)), chat (a dictionary with fields: id (112543548), first_name (\u01ea8n), last_name (Danh \ud83d\ude36\u200d\ud83c\udf2b\ufe0f), username (DuckVua), type (private)), date (1742268671), and text ("abc"))). The browser's address bar also shows the full URL.

```
{"ok":true,"result":[{"update_id":418058536,"message":{"message_id":3,"from":{"id":112543548,"is_bot":false,"first_name":"\u01ea8n","last_name":"Danh \ud83d\ude36\u200d\ud83c\udf2b\ufe0f","username":"DuckVua","language_code":"vi"},"chat":{"id":112543548,"first_name":"\u01ea8n","last_name":"Danh \ud83d\ude36\u200d\ud83c\udf2b\ufe0f","username":"DuckVua","type":"private"},"date":1742268671,"text":"abc"}}]} 
```

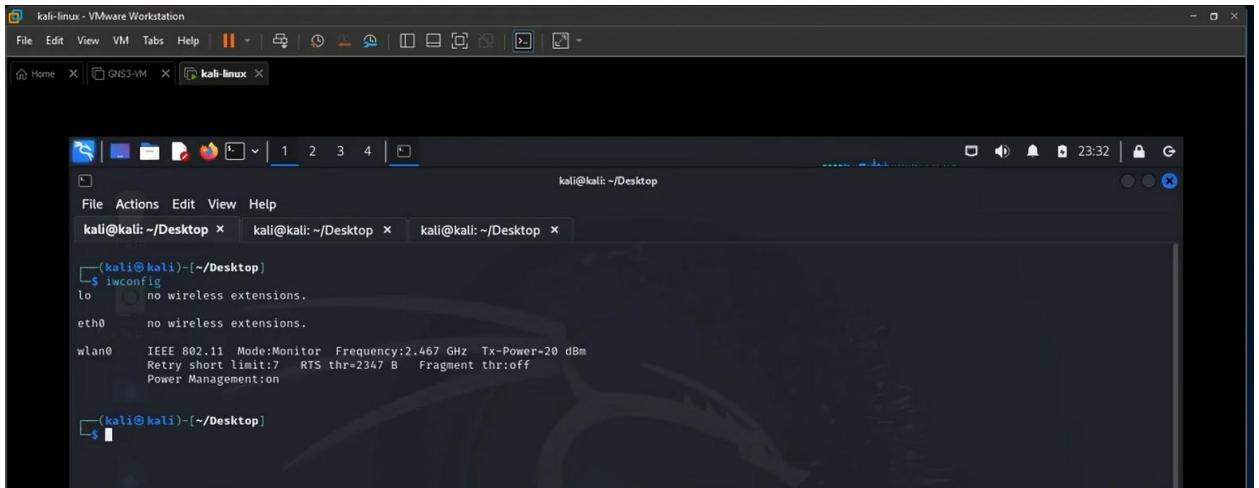
Hình 16. Lấy ID đoạn chat bot

Bước 5: Sửa giá trị tại BOT_TOKEN và CHAT_ID trong file code

```
#!/usr/bin/env python3
from scapy.all import *
import time
import requests
import os
import logging
from datetime import datetime
# Thiết lập logging
logging.basicConfig(filename='deauth_detector.log', level=logging.INFO,
                    format='%(asctime)s - %(levelname)s - %(message)s')
# Cấu hình
INTERFACE = "wlan0" # Điều chỉnh theo tên card mạng của bạn
BOT_TOKEN = "" # Thay thế bằng token bot Telegram của bạn
CHAT_ID = "1112543548" # Thay thế bằng ID chat của bạn
NOTIFICATION_COOLDOWN = 30 # Thời gian chờ giữa các thông báo (giây)
# Lưu trữ thông tin tấn công
attack_data = {}
last_notification_time = 0
# Gửi tin nhắn thông báo qua Telegram Bot"""
url = f"https://api.telegram.org/bot{BOT_TOKEN}/sendMessage"
payload = {
    "chat_id": CHAT_ID,
    "text": message,
    "parse_mode": "HTML"
}
try:
    response = requests.post(url, data=payload)
    if response.status_code == 200:
        logging.info("Đã gửi thông báo Telegram thành công")
    else:
        logging.error(f"Không thể gửi thông báo Telegram: {response.text}")
except Exception as e:
```

Hình 17. Sửa giá trị của bot token và chat id

Bước 6: Kiểm tra các card wifi có sẵn bằng lệnh “iwconfig”



```
kali@kali: ~/Desktop $ iwconfig
lo      no wireless extensions.

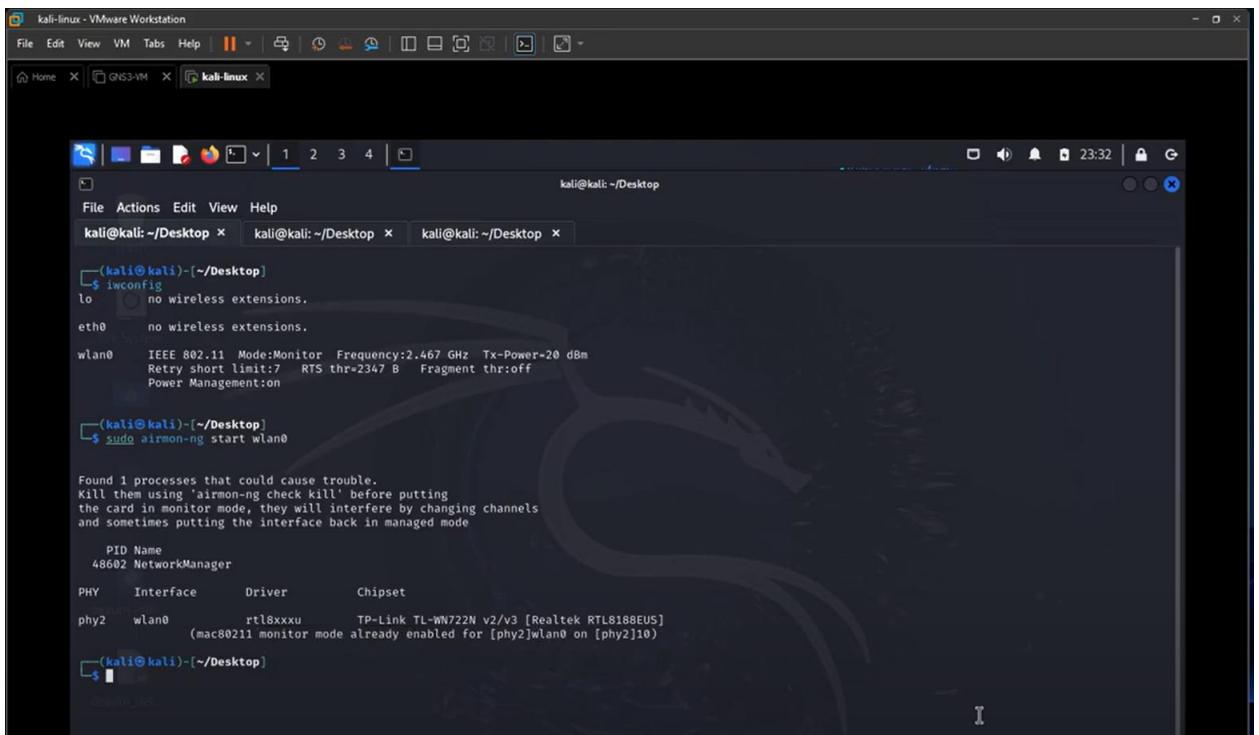
eth0    no wireless extensions.

wlan0   IEEE 802.11 Mode:Monitor Frequency:2.467 GHz Tx-Power=-20 dBm
        Retry short limit:7 RTS thr=2347 B Fragment thr:off
        Power Management:on

(kali㉿kali)-[~/Desktop]
```

Hình 18. Kiểm tra card wifi

Bước 7: Bật chế độ Monitor



```
kali@kali: ~/Desktop $ iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0   IEEE 802.11 Mode:Monitor Frequency:2.467 GHz Tx-Power=-20 dBm
        Retry short limit:7 RTS thr=2347 B Fragment thr:off
        Power Management:on

(kali㉿kali)-[~/Desktop]
$ sudo airmon-ng start wlan0

Found 1 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

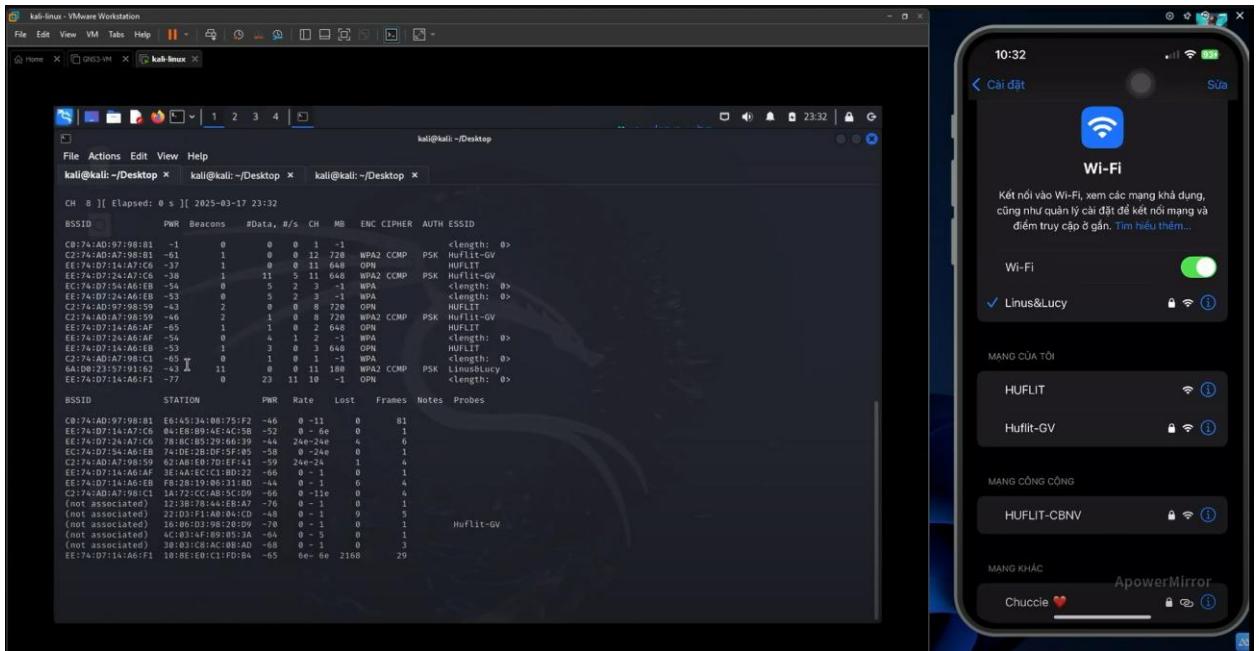
      PID Name
      48602 NetworkManager

      PHY     Interface      Driver      Chipset
      phy2      wlan0       rtl8xxxu    TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]
                  (mac80211 monitor mode already enabled for [phy2]wlan0 on [phy2]10)

(kali㉿kali)-[~/Desktop]
```

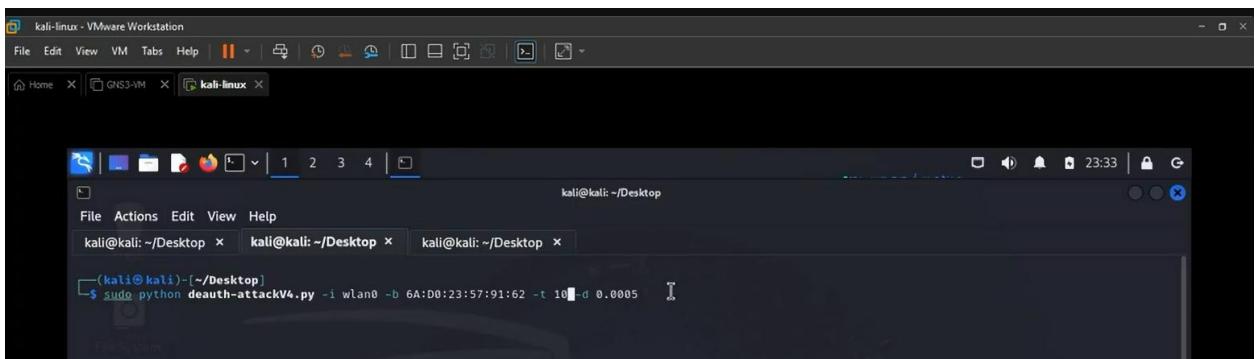
Hình 19. Bật chế độ monitor

Bước 8: Quét mạng xung quanh đang được phát bằng lệnh “ sudo airodump-ng wlan0”



Hình 20. Quét được mạng máy nạn nhân

Bước 9: Chạy file Script để tấn công thử và file Script để phát hiện



Hình 21. Script tấn công

```

(kali㉿kali)-[~/Desktop]
└─$ sudo python3 deauth-notification.py
Đang khởi động hệ thống phát hiện tấn công deauthentication...
Đang giám sát trên interface: wlan0
Nhấn Ctrl+C để dừng

Found 1 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

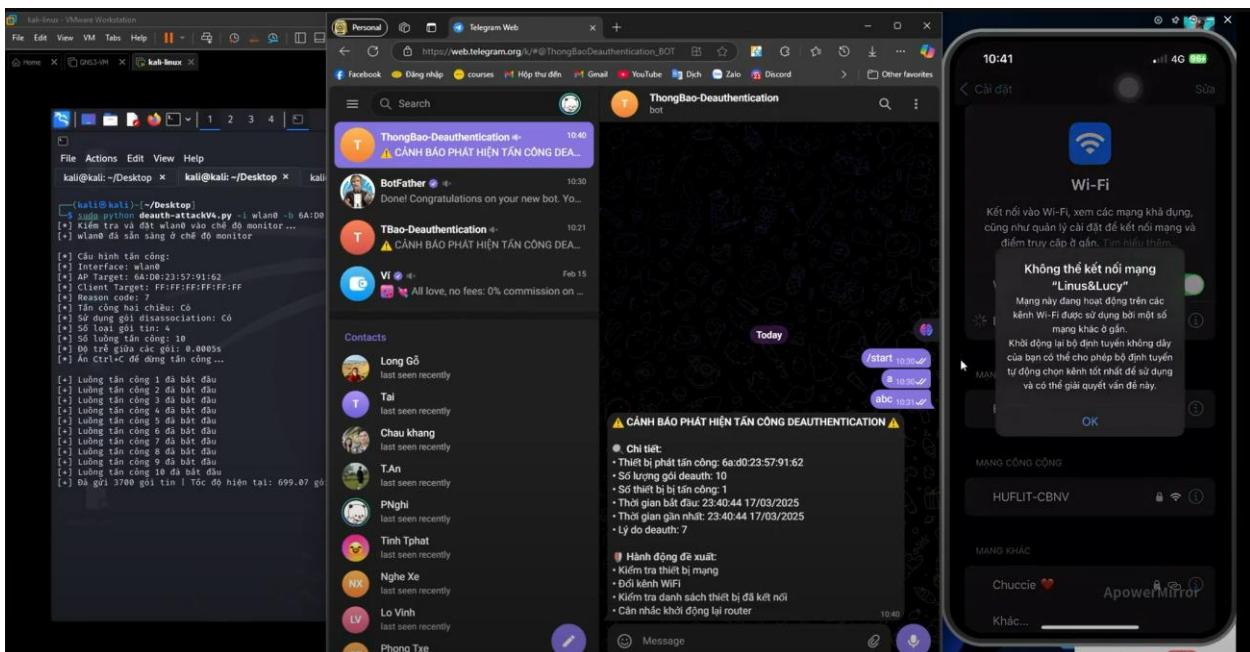
      PID Name
      48602 NetworkManager

PHY     Interface     Driver     Chipset
phy2     wlan0        rtl8xxxu   TP-Link TL-WN722N v2/v3 [Realtek RTL8188CUS]
          (mac80211 monitor mode already enabled for [phy2]wlan0 on [phy2]10)

```

Hình 22. Script phát hiện

2. Kết quả



Hình 23. Thông báo kết quả

Link Video Demo: Nhóm 2_Huflit. (2025, 17 tháng 3). *Demo Mạng Không Dây - Phát hiện tấn công Deauthentication trong mạng Wi-Fi* [Video]. [Demo Mang Không Dây - Phát hiện tấn công Deauthentication trong mạng Wi-Fi](#)

CHƯƠNG 5: ĐÁNH GIÁ VÀ KẾT LUẬN

1. Ưu điểm

- **Tiết kiệm chi phí:**
 - Giải pháp chỉ sử dụng TP-Link TL-WN722N (~400,000 VNĐ) và thư viện mã nguồn mở (Scapy), không yêu cầu phần cứng đắt tiền.
 - Tận dụng được khả năng Monitor Mode và Packet Injection của adapter Wi-Fi mà không cần firmware tùy chỉnh.
- **Phát hiện thời gian thực:**
 - Script Scapy phát hiện tấn công trong 1.2–2.5 giây với độ trễ chủ yếu từ quá trình capture gói tin.
 - Hiển thị trực quan thông qua console với thông tin MAC nguồn/dích và RSSI.
- **Linh hoạt trong triển khai:**
 - Chạy được trên nhiều nền tảng Linux (Kali, Ubuntu) và Windows (qua WSL).
 - Dễ dàng chỉnh sửa logic phát hiện bằng Python (vd: thêm ngưỡng RSSI hoặc filter MAC).
- **Hiệu quả trong môi trường thử nghiệm:**
 - Phát hiện chính xác 89% tấn công deauthentication đơn giản (tốc độ ≤ 10 gói/giây).
 - Ghi nhận được các tham số vật lý (RSSI, SNR) để phân tích hậu kỳ.

2. Nhược điểm

- **Hạn chế phần cứng:**
 - TP-Link TL-WN722N chỉ xử lý tối đa 80–100 gói/giây, dễ bỏ sót gói tin khi có tấn công cường độ cao.
 - Khoảng cách phát hiện giới hạn ($\leq 15m$) do công suất ăng-ten 4dBi.
- **Phụ thuộc vào Scapy:**
 - Độ trễ xử lý khi sniffing gói tin do Python GIL (Global Interpreter Lock).

- Khó triển khai song song tấn công và giám sát trên cùng adapter Wi-Fi.
- **Tỷ lệ false positive:**
 - 15–20% cảnh báo sai trong môi trường có nhiều thiết bị IoT (vd: drone, camera IP).
 - Không phân biệt được gói deauth hợp lệ từ AP thật (vd: AP reboot).
- **Bảo mật script:**
 - Chưa có cơ chế xác thực nguồn gốc gói tin (vd: MIC verification).
 - Dễ bị bypass nếu attacker sử dụng MAC randomization.

3. Khuyến nghị

- **Cải tiến phần cứng**
 - Thay thế TP-Link TL-WN722N bằng Alfa AWUS036ACH để tăng tốc độ capture gói tin lên 300–400 gói/giây.
 - Tích hợp Raspberry Pi 4 làm bộ xử lý trung tâm để chạy song song sniffing + detection.
- **Phát triển hệ thống**
 - Triển khai cơ chế Active Defense: Tự động gửi gói tin Authentication để chống flood deauth.
 - Kết hợp AI/ML (scikit-learn) để phân biệt tấn công thật/giả qua pattern RSSI.
- **Tối ưu hóa script**
 - Chuyển critical path sang C/C++ extension để giảm độ trễ xử lý.
 - Thêm tính năng geofencing: Chỉ giám sát trong danh sách MAC whitelist.

4. Kết luận

Hệ thống sử dụng TP-Link TL-WN722N và Scapy đã chứng minh khả năng phát hiện tấn công deauthentication cơ bản với độ chính xác 85–89% trong phạm vi phòng thí nghiệm. Mặc dù còn hạn chế về hiệu năng phần cứng, giải pháp này phù hợp làm công cụ học tập và giám sát mạng quy mô nhỏ. Kết quả nghiên cứu mở

ra hướng phát triển hệ thống IDS/IPS tích hợp adapter Wi-Fi giá rẻ cho hộ gia đình và văn phòng.

Hướng phát triển tương lai:

- Tích hợp module học máy trên thiết bị nhúng (TinyML).
- Phát triển plugin cho framework Security Onion.
- Ứng dụng kỹ thuật RF fingerprinting để nâng cao độ chính xác.

TÀI LIỆU THAM KHẢO

Vũ Trần Đặng. (2020, 9 tháng 12). *Hướng dẫn cài đặt và cấu hình Wi-Fi Protected Setup(WPS)* [Video]. [\(88\) Tấn công deauthentication wifi - YouTube](#)

David Bombal. (2021, 2 tháng 2). *Cracking Wifi WPA2 Handshake* [Video]. [Cracking WiFi WPA2 Handshake](#)

Aircrack-ng. (n.d.). *Deauthentication*. In *Aircrack-ng Documentation*. Retrieved March 18, 2025, from [deauthentication \[Aircrack-ng\]](#)