**ĐẠI HỌC QUỐC GIA TP.HCM**

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN**

**KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG**

Logo, company name

Description automatically generated

**BÁO CÁO ĐỒ ÁN MÔN HỌC**

**MÔN: HỆ THỐNG NHÚNG MẠNG KHÔNG DÂY**

**Tên đề tài: Xây dựng và triển khai kịch bản tấn công crack password wifi**

| Sinh viên thực hiện: | Võ Thị Hưởng – 19520586  Nguyễn Hoàng Phúc – 20520277  Hồ Văn Phước - 22521151 |
| --- | --- |
| Giảng viên hướng dẫn: | Lê Anh Tuấn |
| Lớp: | NT131.O21 |

**Thành phố Hồ Chí Minh, tháng 5 năm 2024**

# LỜI CẢM ƠN

Trước hết, chúng em muốn bày tỏ lòng biết ơn và sự tôn trọng sâu sắc đến thầy Bùi Đức Hoàng - người hướng dẫn của chúng em. Chúng em muốn dành lời cảm ơn chân thành và tri ân đến thầy vì sự tận tâm và nhiệt tình trong việc hỗ trợ chúng em trong quá trình thực hiện đồ án môn học này. Những định hướng, bổ sung và góp ý từ thầy đã làm nền tảng và chỉ dẫn cho chúng em, giúp chúng em đi đúng hướng và đạt được kết quả tốt nhất trong việc phát triển và hoàn thiện đồ án môn học.

Tiếp theo, chúng em muốn gửi lời cảm ơn đặc biệt đến gia đình và người thân. Gia đình luôn là nguồn động lực và niềm tin vững chắc giúp chúng em vượt qua khó khăn và hoàn thành tốt nhiệm vụ này.

Trong quá trình thực hiện nhiệm vụ thực tập và viết báo cáo, chúng em thừa nhận rằng kiến thức của mình còn hạn chế, do đó khó tránh khỏi những sai sót không mong muốn. Chúng em rất mong nhận được sự chỉ bảo và đóng góp ý kiến từ thầy và các bạn để chúng em ngày càng hoàn thiện hơn trong kiến thức. Chúng em mong nhận được ý kiến đóng góp từ thầy và các bạn để chúng em học hỏi thêm kinh nghiệm giúp chúng em trong tương lai.

Cuối cùng, chúng em muốn gửi lời cảm ơn đến các anh, chị và các bạn sinh viên của trường Đại học Công nghệ Thông tin đã hỗ trợ, chia sẻ ý kiến và góp ý cho chúng em trong suốt quá trình thực hiện đồ án. Một lần nữa, chúng em xin chân thành cảm ơn và gửi lời chúc sức khỏe đến thầy Bùi Đức Hoàng. Kính chúc thầy luôn tiến tới và thành công trong sự nghiệp của mình.

Thành phố Hồ Chí Minh, tháng 05 năm 2024

**Võ Thị Hưởng – 19520586**

**Nguyễn Phúc Hoàng – 20520277**

**Hồ Văn Phước – 22521151**

# NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN

# MỤC LỤC

[LỜI CẢM ƠN 1](#_heading=h.gjdgxs)

[NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN 2](#_heading=h.30j0zll)

[MỤC LỤC 3](#_heading=h.1fob9te)

[DANH MỤC HÌNH ẢNH 5](#_heading=h.3znysh7)

[DANH MỤC TỪ VIẾT TẮT 6](#_heading=h.2et92p0)

[PHẦN MỞ ĐẦU 7](#_heading=h.tyjcwt)

[PHẦN NỘI DUNG 8](#_heading=h.3dy6vkm)

[Chương 1: Tổng quan đề tài 8](#_heading=h.1t3h5sf)

[1.1.](#_heading=h.4d34og8) Tên đề tài 8

[1.2.](#_heading=h.2s8eyo1) Mục tiêu đề tài 8

[1.3.](#_heading=h.17dp8vu) Đối tượng và phạm vi 8

[1.4.](#_heading=h.3rdcrjn) Nội dung và phương pháp nghiên cứu 8

[Chương 2: Cơ sở lý thuyết 9](#_heading=h.26in1rg)

[2.1.](#_heading=h.lnxbz9) Chuẩn mạng WEP 9

[a.](#_heading=h.35nkun2) Khái niệm 9

[b.](#_heading=h.1ksv4uv) Kiến trúc tổng quan 9

[c.](#_heading=h.2jxsxqh) Cơ chế mã hóa 10

[d.](#_heading=h.3j2qqm3) Ưu điểm 11

[e.](#_heading=h.1y810tw) Nhược điểm 11

[2.2.](#_heading=h.4i7ojhp) Chuẩn mạng WPA 12

[a.](#_heading=h.2xcytpi) Khái niệm 12

[b.](#_heading=h.1ci93xb) Kiến trúc tổng quan 13

[c.](#_heading=h.2bn6wsx) Cơ chế mã hóa 14

[d.](#_heading=h.3as4poj) Ưu điểm 14

[e.](#_heading=h.1pxezwc) Nhược điểm 15

[2.3.](#_heading=h.49x2ik5) Chuẩn mạng WPA 2 15

[a.](#_heading=h.2p2csry) Khái niệm 15

[b.](#_heading=h.147n2zr) Cơ chế xác thực 15

[c.](#_heading=h.23ckvvd) WPA2-PSK 16

[d.](#_heading=h.1hmsyys) WPA2-Enterprise 19

[e.](#_heading=h.2grqrue) Lỗ hổng của WPA2: 20

[Chương 3: Kịch bản tấn công và demo 20](#_heading=h.3fwokq0)

[3.1.](#_heading=h.1v1yuxt) Cấu hình và cài đặt thiết bị 20

[a.](#_heading=h.4f1mdlm) Các thiết bị sử dụng: 20

[b.](#_heading=h.2u6wntf) Cấu hình hệ thống: 20

[3.2.](#_heading=h.3tbugp1) Thực hiện 21

[a.](#_heading=h.28h4qwu) Bruce force attack password sử giao thức bảo mật WEP mã hóa 64 bits với tool aircrack-ng 21

[b.](#_heading=h.46r0co2) Bruce force attack password sử giao thức bảo mật WEP mã hóa 128 bits với tool wifite. 24

[c.](#_heading=h.206ipza) Distionary attack password sử giao thức bảo mật WPA2-PSK mã hóa AES với tool aircrack-ng. 25

[PHẦN KẾT LUẬN 29](#_heading=h.3cqmetx)

[1.](#_heading=h.1rvwp1q) So sánh chuẩn mã hóa WEP, WPA và WPA2 29

[2.](#_heading=h.4bvk7pj) Kết luận 30

[TÀI LIỆU THAM KHẢO 31](#_heading=h.2r0uhxc)

[Bibliography 31](#_heading=h.1664s55)

# DANH MỤC HÌNH ẢNH

[Hình 2.1: Quá trình xác thực của WEP 10](#_heading=h.44sinio)

[Hình 2.2: Quá trình mã hóa của WEP 11](#_heading=h.z337ya)

[Hình 2.3: Quá trình xác thực của chuẩn mã hóa WPA 13](#_heading=h.3whwml4)

[Hình 2.4: Quá trình mã hóa của WPA 14](#_heading=h.qsh70q)

[Hình 2.5: Kiến trúc tổng quan và quá trình bắt tay 4 bước 16](#_heading=h.3o7alnk)

[Hình 2.6: Quá trình mã hóa của WPA2-PSK 17](#_heading=h.ihv636)

[Hình 2.7: Quá trình mã hóa của WPA2 18](#_heading=h.32hioqz)

[Hình 2.8: Quá trình xác thực ở WPA2-Enterprise 19](#_heading=h.41mghml)

[Hình 2.9: So sánh WEP, WPA và WPA2 20](#_heading=h.vx1227)

[Hình 3.1: Mô hình mạng của kịch bản tấn công 21](#_heading=h.19c6y18)

[Hình 3.2: Kết quả thu thập gói tin 22](#_heading=h.nmf14n)

[Hình 3.3: Kết quả sau khi thực hiện fakeauthen 23](#_heading=h.37m2jsg)

[Hình 3.4: Kết quả thực hiện crack password wifi Wireless\_lab 24](#_heading=h.1mrcu09)

[Hình 3.5: Kết quả quét wifi của lệnh ./wifite-kill 25](#_heading=h.2lwamvv)

[Hình 3.6: Kết quả crack thành công password của wifi Wireless\_lab 25](#_heading=h.3l18frh)

[Hình 3.7: Kết quả scan wifi 26](#_heading=h.4k668n3)

[Hình 3.8: Thông tin thu thập được của TP-Link\_83C8 27](#_heading=h.2zbgiuw)

[Hình 3.9: Kết quả nhận được sau khi thực hiện tấn công Deauth 27](#_heading=h.1egqt2p)

[Hình 3.10: Các gói handshake thu được 28](#_heading=h.3ygebqi)

[Hình 3.11: Kết quả thực hiện tạo list pasword 28](#_heading=h.2dlolyb)

[Hình 3.12: Kết quả sau khi crack thành công password của TP-Link\_83C8 29](#_heading=h.sqyw64)

# DANH MỤC TỪ VIẾT TẮT

| **Từ viết tắt** | **Ý nghĩa** |
| --- | --- |
| WEP | Wired Equivalent Privacy |
| WPA | Wifi Protected Access |
| WPA2 | Wi-Fi Protected Access 2 |
| OSA | Open System Authentication |
| SKA | Shared Key Authentication |
| RC4 | Rivest Cipher 4 |
| IV | Initialization Vector |
| IEEE | Institute of Electrical and Electronics Engineers |
| WPA3 | Wi-Fi Protected Access 3 |
| EAP | Extensible Authentication Protocol |
| PSK | Pre-Shared Key |
| TKIP | Temporal Key Integrity Privacy |
| RADIUS | Remote Authentication Dial-In User Service |
| MIC | Message Integrity Code |
| AAA | Authentication, Authorization, and Accounting |
| SSL | Secure Sockets Layer |
| TLS | Transport Layer Security |
| PEAP | Protected Extensible Authentication Protocol |
| AES | Advanced Encryption Standard |
| KRACK | Key Reinstallation Attack |
| CRC-32 | Cyclic Redundancy Check 32 |

# PHẦN MỞ ĐẦU

Đồ án tập trung nghiên cứu ba chuẩn mã hóa dành cho wifi gồm WEP, WPA và WPA2. Mục tiêu là tìm hiểu, so sánh và đưa ra kết luận chính xác nhất cho việc sử dụng các chuẩn mã hóa để mã hóa trên mạng không dây. Điều này cung cấp hiểu biết về các chuẩn mã hóa và đưa ra giải pháp trong bối cảnh các cuộc tấn công trên môi trường mạng không dây ngày càng tăng cả về số lượng lẫn cách thức. [1] [2] [3]

Thông qua tìm kiếm các khái niệm, đặc điểm về cấu trúc, phương pháp mã hóa của ba chuẩn trên và thực hiện các cuộc tấn công đối với các thiết bị sử dụng các chuẩn mã hóa khác nhau để đánh giá khả năng bảo mật và bảo vệ tính toàn vẹn của dữ liệu được truyền qua mạng không dây của từng chuẩn. Từ đó đưa ra kết luận cho việc sử dụng các biện pháp mã hóa cho mạng không dây.

Nội dung báo cáo gồm 3 phần sau:

* **Phần mở đầu**
* **Phần nội dung**
* **Chương 1:** Tổng quan đề tài
* **Chương 2:** Cơ sở lý thuyết
* **Chương 3:** Kịch bản tấn công và demo
* **Phần kết luận**

# PHẦN NỘI DUNG

## Chương 1: Tổng quan đề tài

### Tên đề tài

Xây dựng và triển khai kịch bản tấn công crack password wifi.

### Mục tiêu đề tài

Mục tiêu của đề tài này là xây dựng và triển khai các kịch bản tấn công crack password wifi đối với các access point sử dụng các chuẩn mã hóa WEP, WPA và WPA2. Điều này giúp so sánh và đánh giá khả năng bảo mật của các chuẩn mã hóa được nếu trên. Đồng thời cung cấp hiểu biết về sự nguy hiểm của các tấn công trên mạng không dây đối với người dùng và dữ liệu được truyền ở đó.

### Đối tượng và phạm vi

* Đối tượng: bao gồm các hệ thống mạng wifi, người quản trị và người dùng trong các hệ thống mạng wifi đó.
* Phạm vi: Các chuẩn mã hóa trong mạng không dây (ở đây là WEP, WPA và WPA2), các kỹ thuật tấn công, đánh giá mức độ an toàn của các chuẩn mã hóa.

### Nội dung và phương pháp nghiên cứu

* Nội dung của đề tài bao gồm:
* Tìm hiểu, nghiên cứu khái niệm, đặc điểm, kiến trúc của các chuẩn mã hóa WEP, WPA và WPA2
* Đánh giá tổng quát về ưu, nhược điểm của từng chuẩn mã hóa
* Xây dựng kịch bản và thực hiện các cuộc tấn công đối với từng chuẩn mã hóa
* Tiến hành so sánh và đánh giá mức độ bảo mật
* Đưa ra kết luận
* Phương pháp nghiên cứu bao gồm tìm kiếm, thu thập các thông tin về các chuẩn mã hóa và các cuộc tấn công, xây dựng kịch bản, thực hiện tấn công, đánh giá hiệu quả bảo mật của từng chuẩn mã hóa và so sánh với nhau.

## Chương 2: Cơ sở lý thuyết

### Chuẩn mạng WEP

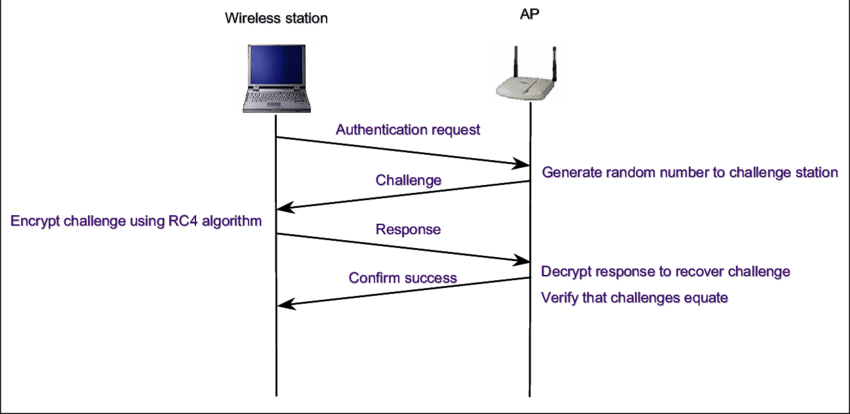
#### Khái niệm

* WEP hay Wired Equivalent Privacy, là một giao thức bảo mật được sử dụng trong mạng không dây (Wi-Fi) để bảo vệ dữ liệu truyền qua mạng, là một phần của tiêu chuẩn IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b.
* Giao thức WEP được giới thiệu vào năm 1997 nhưng gặp phải một số vấn đề về bảo mật. Các cơ quan bắt đầu không khuyến khích sử dụng nó vào đầu những năm 2000, khi các tiêu chuẩn hiệu quả hơn được đưa ra.

#### Kiến trúc tổng quan

WEP xác thực các máy khách khi chúng kết nối lần đầu tiên với điểm truy cập mạng không dây. Nó cho phép xác thực của các máy khách không dây thông qua hai cơ chế sau:

* **OSA** (Open System Authentication): Với OSA, các hệ thống kết nối Wi-Fi có thể truy cập vào bất kỳ điểm truy cập mạng không dây WEP nào, miễn là hệ thống kết nối sử dụng Service Set Identifier - SSID phù hợp với SSID của điểm truy cập.
* **SKA** (Shared Key Authentication): Với SKA, các hệ thống kết nối Wi-Fi sử dụng quá trình bắt tay bốn bước để xác thực

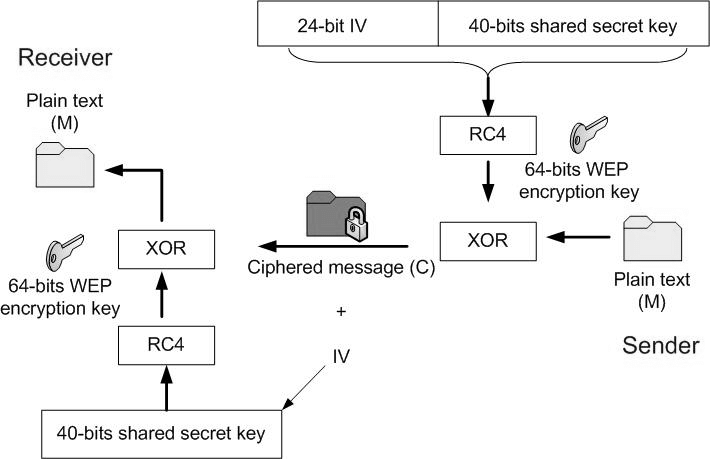


*Hình 2.1: Quá trình xác thực của WEP*

* **Các bước xác thực trong mạng không dây sử dụng chuẩn mã hóa WEP:**
* Thiết bị client cung cấp các thông tin đăng nhập (SSID, mật khẩu,…)
* AP gửi gói tin Authentication Request cho thiết bị client
* Client sẽ gửi một gói Authentication Response bao gồm một khóa được XOR từ IV (được đính kèm trong gói tin trước AP gửi cho client) và mật khẩu của AP
* Nếu khóa đó đúng với mật khẩu và IV được lưu trữ trong AP thì AP sẽ gửi một gói Authentication Confirmation hoặc Authentication Failure nếu ngược lại.
* Sau khi được xác thực, các gói tin được gửi giữa client và AP sẽ được mã hóa bằng khóa

#### Cơ chế mã hóa

* Sử dụng thuật toán mã hóa RC4: WEP sử dụng thuật toán mã hóa RC4 để mã hóa dữ liệu trên mạng không dây. RC4 là một thuật toán mã hóa dòng được sử dụng rộng rãi trong WEP, nhưng nó đã bị phát hiện có nhiều lỗ hổng bảo mật và không an toàn.
* Initialization Vector (IV): Mỗi gói tin dữ liệu được truyền trong mạng WEP được mã hóa bằng một IV. IV là một chuỗi ngẫu nhiên có kích thước nhỏ (thường là 24-bit hoặc 48-bit), được kết hợp với khóa để tạo ra mã hóa.
* Tính toàn vẹn dữ liệu: WEP sử dụng thuật toán kiểm tra CRC-32 để kiểm tra xem dữ liệu truyền đi có được thay đổi hay không khi đến đích. Bên gửi sử dụng kiểm tra CRC-32 để tạo ra một giá trị băm 32-bit từ một chuỗi dữ liệu. Bên nhận sử dụng kiểm tra tương tự khi nhận được dữ liệu. Nếu hai giá trị này khác nhau, bên nhận có thể yêu cầu gửi lại dữ liệu.



*Hình 2.2: Quá trình mã hóa của WEP*

* Quá trình mã hóa trong WEP:
* IV được AP tạo ra bao gồm 24 bit, IV được thêm vào header của gói tin và được thay đổi mỗi khi gói tin mới được gửi đi.
* Khóa mã hóa được tạo ra bằng cách XOR IV và khóa con ngẫu nhiên được chọn từ shared secret key (thường có độ dài 40 bits)
* Sử dụng khóa mã hóa và thuật toán RC4 để mã hóa dữ liệu
* Sau đó gói tin được gửi đi trong mạng không dây
* Bằng IV được đính kém trong header của gói tin và shared secret key được chia sẻ giữa client và AP, bên nhận sẽ giải mã ra dữ liệu

#### Ưu điểm

Mặc dù WEP (Wired Equivalent Privacy) đã bị thay thế bởi các giao thức bảo mật mạng không dây mạnh mẽ hơn như WPA2 và WPA3 do những lỗ hổng bảo mật đã được phát hiện trong WEP, nhưng vẫn có một số ưu điểm:

* Dễ triển khai: WEP đã được tích hợp sẵn trong nhiều thiết bị mạng không dây và dễ dàng cấu hình trên các điểm truy cập và thiết bị kết nối.
* Tính tương thích: WEP được hỗ trợ trên hầu hết các thiết bị mạng không dây từ những thập kỷ trước, làm cho nó có tính tương thích rộng rãi với các thiết bị cũ và mới.

#### Nhược điểm

WEP (Wired Equivalent Privacy) đã bị xem là không an toàn và không nên được sử dụng trong môi trường mạng hiện đại do những nhược điểm sau:

* Mã hóa yếu: WEP sử dụng thuật toán mã hóa RC4, đã được phát hiện nhiều lỗ hổng và không an toàn. Các kẻ tấn công có thể dễ dàng phá vỡ mã hóa WEP và truy cập vào dữ liệu mạng.
* Quản lý khóa không an toàn: WEP yêu cầu tất cả các thiết bị trên mạng chia sẻ cùng một khóa bí mật. Quản lý và phân phối khóa này không an toàn, làm tăng nguy cơ bị tấn công.
* Khả năng tái sử dụng Initialization Vector (IV): IV trong WEP có kích thước nhỏ và có thể tái sử dụng, dẫn đến việc mật khẩu có thể dễ dàng bị crack.
* Xác thực yếu: Cả hai cơ chế xác thực của WEP (Open System Authentication và Shared Key Authentication) đều có nhược điểm. Open System Authentication không yêu cầu bất kỳ xác thực nào, trong khi Shared Key Authentication dễ bị tấn công và không an toàn.
* Khả năng tấn công đơn giản: Có nhiều công cụ và phương pháp tấn công có sẵn để phá vỡ bảo mật của WEP, bao gồm tấn công dựa trên IV và tấn công từ điển.

Tóm lại, WEP đã bị bỏ qua và không được khuyến nghị cho việc sử dụng trong bất kỳ môi trường mạng nào do những nhược điểm bảo mật nghiêm trọng của nó. Thay vào đó, các giao thức bảo mật mạng không dây mạnh mẽ hơn như WPA2 và WPA3 được khuyến nghị để đảm bảo an toàn cho mạng Wi-Fi.

### Chuẩn mạng WPA

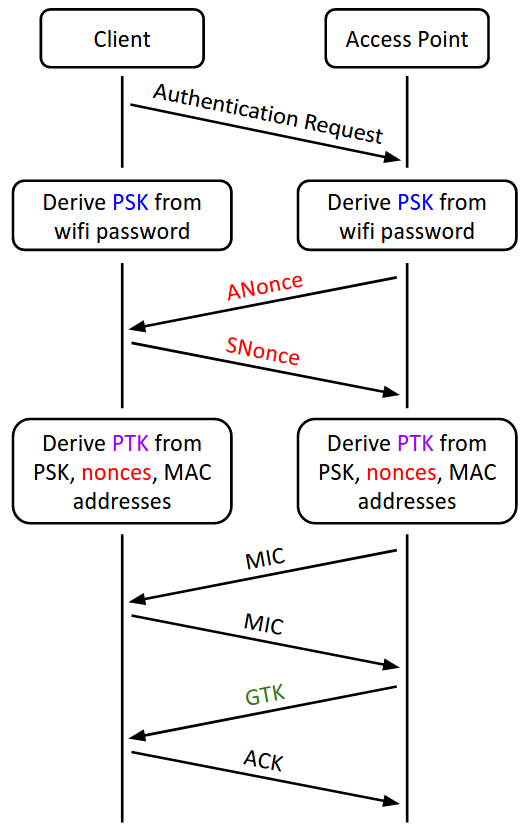
#### Khái niệm

WPA (Wifi Protected Access) là một tiêu chuẩn mã hóa mạng không dây ra mắt vào năm 2003, và được phát triển như một phần của tiêu chuẩn IEEE 802.11i. WPA được phát triển bởi Wifi Alliance nhằm cung cấp phương pháp mã hóa dữ liệu và xác thực tốt hơn so với chuẩn WEP (Wired Equivalent Privacy)

#### Kiến trúc tổng quan

WPA có 2 chế độ: WPA-EAP (WPA Extensible Authentication Protocol) và WPA-PSK (Pre-Shared Key)

* **WPA-EAP (WPA-802.1x):** được thiết kế để sử dụng trong các hệ thống mạng vừa và lớn. Hệ thống bao gồm RADIUS server và các máy client sẽ sử dụng mã định danh riêng để kết nối với mạng. WPA-EAP cho phép quản lý theo user-by-user, từ đó nếu một thiết bị client bị hack, quyền truy cập của thiết bị đó có thể bị thu hồi mà không gây ra bất kỳ ảnh hưởng nào đối với các thiết bị khác.
* **WPA-PSK:** Được thiết kế cho các hệ thống mạng nhỏ hoặc trong phạm vi gia đình, nó sử dụng một mật khẩu công khai cho tất cả người dùng. Hệ thống này rất dễ thiết lập nhưng nếu một thiết bị bị xâm nhập, thì cần phải thay đổi mật khẩu và thiết lập lại kết nối bằng mật khẩu mới trên tất cả các thiết bị client khác.

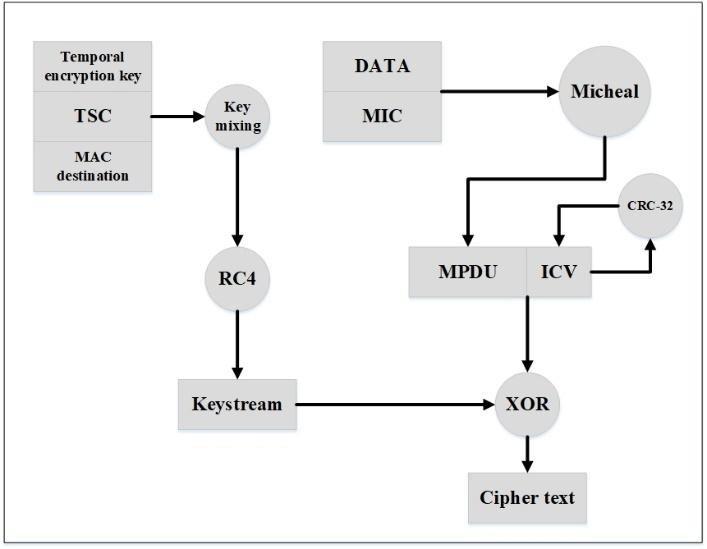


*Hình 2.3: Quá trình xác thực của chuẩn mã hóa WPA*

* **Quá trình xác thực của WPA-PSK:**
* Client gửi Authentication Request đến AP
* AP tạo ra một khóa Session từ PSK, SSID và một số tham số khác. Khóa Session được sử dụng để mã hóa và giải mã dữ liệu truyền qua mạng. Bản gốc khóa Session được lưu trên AP và cũng được gửi cho người dùng.
* Khi nhập mật khẩu vào thiết bị để xác thực, thiết bị sẽ dùng mật khẩu này để tạo Session key chung với AP
* Sử dụng 4-Way Handshake Protocol để xác thực và trao đổi Session key (Temporal Key) giữa AP và thiết bị client. Quá trình này cho phép 2 thiết bị hình thành một bản sao của session key
* AP và client sử dụng bản sao của Session key để mã hóa và giải mã tất cả các gói tin được truyền qua mạng
* **Quá trình xác thực của WPA-EAP:**
* Khi người dùng kết nối với mạng không dây, AP yêu cầu người dùng cung cấp username và password
* Thiết bị client sẽ tìm kiếm và liên lạc với máy chủ xác thực để đăng nhập và lấy chứng chỉ xác thực
* Sau khi nhận được chứng chỉ xác thực, thiết bị client sẽ ký và mã hóa một thông điệp và gửi lại cho AP.
* AP sẽ gửi thông điệp được mã hóa và chứng chỉ đến máy chủ xác thực
* Máy chủ xác thực sẽ xác nhận và gửi lại thông điệp để xác nhận kết nối
* Sau khi quá trình này hoàn thành, AP và client sẽ được cấp một khóa Session để mã hóa và giải mã trong quá trình truyền qua mạng không dây.

#### Cơ chế mã hóa

* WPA sử dụng TKIP (Temporal Key Integrity Privacy) để mã hóa dữ liệu.
* Với mỗi session truyền dữ liệu, WPA tạo ra một khóa duy nhất để mã hóa và giải mã dữ liệu. Khi session thay đổi, TKIP tự động thay đổi khóa mã hóa cho từng packet dữ liệu được truyền đi, điều nay ngăn chặn một số loại tấn công có thể xảy ra với chuẩn WEP.
* Với mỗi packet dữ liệu, WPA cung cấp mã MIC (Message Integrity Code) để đảm bảo tính nguyên vẹn của dữ liệu.



*Hình 2.4: Quá trình mã hóa của WPA*

* **Quá trình mã hóa của WPA:**
* Khi xác thực kết nối hoàn tất, một Temporal Key được tạo ra. Khóa này được sử dụng để tạo ra 2 mã khóa: cho mã hóa dữ liệu (Data Encryption Key) và mã hóa xác thực Micheal
* Khóa mã hóa được sử dụng để mã hóa và giải mã tất cả các gói dữ liệu truyền qua mạng không dây
* ICV được kèm theo mỗi gói tin nhằm đảm bảo tính toàn vẹn của dữ liệu
* Dữ liệu được chia thành các khối có độ dài là 64 bits

#### Ưu điểm

* Giải quyết các lỗ hổng bảo mật của chuẩn WEP nhờ sử dụng TKIP và MIC.
* Sử dụng khóa có độ dài hơn so với WEP (40 bit) khiến cho attacker khó bẻ khóa hơn.
* Tự động tạo khóa mã hóa cho từng packet, khiến attacker khó bẻ khóa mã hơn so với WEP
* WPA được thiết kế để tương thích ngược với các thiết bị Wifi cũ hơn, cho phép kết nối với mạng bằng WPA ngay cả khi các thiết bị đó không hỗ trợ các giao thức WPA2 hay WPA3.
* Hỗ trợ nhiều phương thức xác thực phù hợp với các quy mô từ nhỏ như các hộ gia đình (PSK) đến lớn như quy mô doanh nghiệp hay trường học (EAP)

#### Nhược điểm

* Lỗ hổng trong TKIP.
* WPA sử dụng khóa 128-bit (EAP) hoặc 256-bit (PSK), nhưng với kích thước khóa như thế attacker vẫn có thể tấn công, đặc biệt với mật khẩu yếu được sử dụng trong PSK
* WPA tuy là bản tiên tiến hơn so với WEP, tuy nhiên vẫn dễ gặp phải các lỗ hổng bảo mật, cần có các bản cập nhật và bản vá lỗi. Việc không kịp thời áp dụng các bản vá và cập nhật có thể khiến cho mạng dễ bị khai thác
* Tuy WPA có hỗ trợ sử dụng với các thiết bị Wifi cũ hơn, nhưng đôi khi cũng sẽ phát sinh các sự cố về tương tác. Điều này dẫn đến khó khăn trong việc thiết lập và duy trì bảo mật.

### Chuẩn mạng WPA 2

#### Khái niệm

WPA2 (Wi-Fi Protected Access 2) được công bố chính thức năm 2004, được sử dụng phổ biến đến nay. Nó được xem là một bước tiến lớn hơn so với WPA, nhằm cải thiện tính bảo mật và hiệu suất của mạng wifi. WPA2 được thiết kế để cung cấp một phương tiện mã hóa an toàn hơn cho việc truyền dữ liệu qua mạng không dây.

#### Cơ chế xác thực

WPA2 cung cấp 2 cơ chế xác thực gồm WPA2-PSK và WPA2-Enterprise:

* **WPA2-PSK** (Wi-Fi Protected Access 2 – Pre-Shared Key): là một giao thức bảo mật được sử dụng để bảo mật các mạng không dây, đặc biệt là mạng gia đình và văn phòng nhỏ. WPA2-PSK được giới thiệu là bản nâng cấp lên tiêu chuẩn WPA ban đầu, được chứng minh là có lỗ hổng. A diagram of a process

  Description automatically generated

*Hình 2.5: Kiến trúc tổng quan và quá trình bắt tay 4 bước*

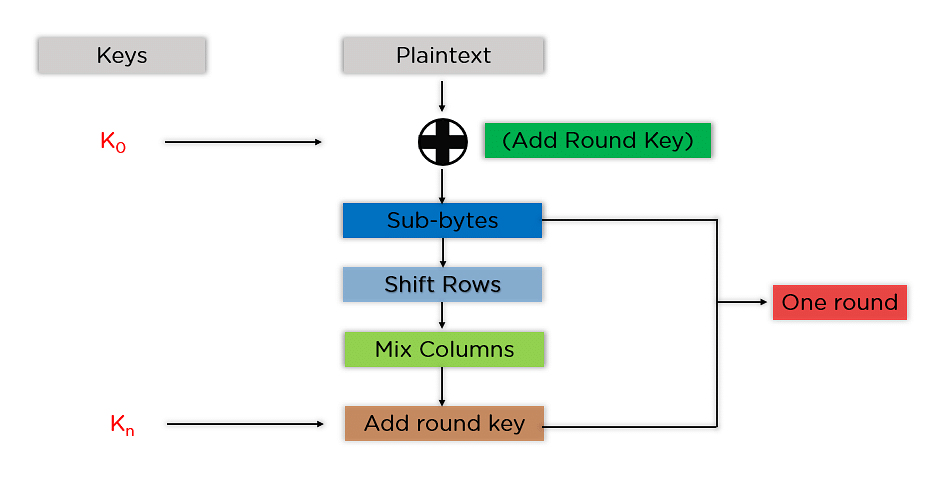
* **WPA2-Enterprise**: Phiên bản WPA2- Enterprise mới nhất phù hợp với 802.11i. Giao thức xác thực cơ bản của nó là 802.1X, cho phép các thiết bị wi-fi được xác thực bằng tên người dùng và mật khẩu hoặc sử dụng chứng chỉ bảo mật. Xác thực 802.1X được triển khai trên máy chủ AAA (thường là RADIUS) cung cấp chức năng quản lý người dùng và xác thực tập trung. EAP là tiêu chuẩn được sử dụng để truyền tin nhắn và xác thực trình xác thực máy khách và máy chủ trước khi gửi. Các tin nhắn này được bảo mật thông qua các giao thức như SSL, TLS và PEAP.

#### WPA2-PSK

WPA2-PSK cung cấp liên lạc an toàn giữa các thiết bị được kết nối với mạng không dây. Nếu không có các biện pháp bảo mật thích hợp, những cá nhân không được ủy quyền có thể truy cập vào mạng và có khả năng đánh cắp thông tin nhạy cảm. WPA2-PSK giúp ngăn chặn điều này bằng cách mã hóa dữ liệu và yêu cầu mật khẩu duy nhất để truy cập.

1. **Mã hóa:**

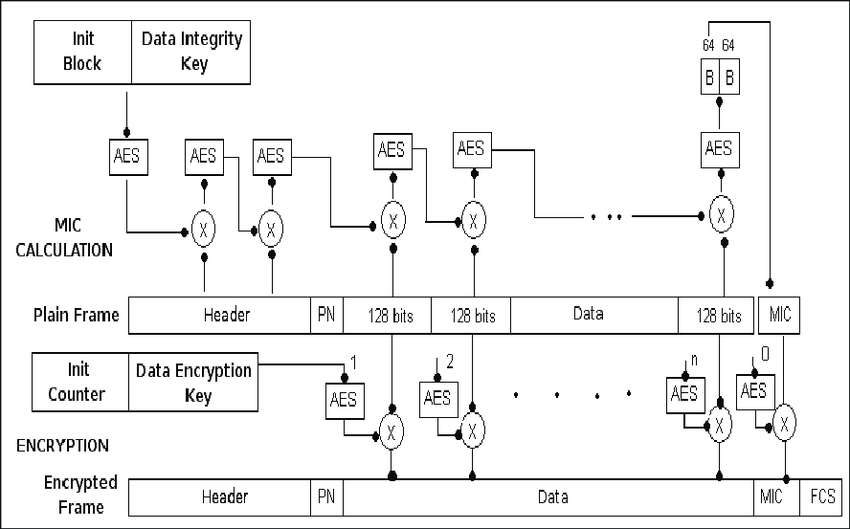
Dùng thuật toán mã hóa mạnh mẽ AES (Advanced Encryption Standard), sử dụng thuật toán mã hóa đối xứng theo khối Rijindael, sử dụng khối mã hóa thường là 128 bit.



*Hình 2.6: Quá trình mã hóa của WPA2-PSK*

Vòng lặp chính của AES thực hiện các hàm sau: SubBytes(), ShiftRows(), MixColumns() và AddRoundKey(). Ba hàm đầu của một vòng AES được thiết kế để ngăn chặn phân tích mã bằng phương thức “mập mờ“ (confusion) và phương thức “khuếch tán“ (diffusion), còn hàm thứ tư mới thực sự được thiết kế để mã hóa dữ liệu. Trong đó “khuếch tán“ có nghĩa là các kiểu mẫu trong bản rõ (Dữ liệu đầu vào của phép mã hóa hoặc dữ liệu đầu ra của phép giải mã) được phân tán trong các bản mã (Dữ liệu đầu ra của phép mã hóa hoặc dữ liệu đầu vào của phép giải mã), “mập mờ“ nghĩa là mối quan hệ giữa bản rõ và bản mã bị che khuất. Một cách đơn giản hơn để xem thứ tự hàm AES là: Trộn từng byte (SubBytes), trộn từng hàng (ShiftRows), trộn từng cột (MixColumns) và mã hóa (AddRoundKey).

Ngay khi người dùng kết nối với bộ định tuyến, họ được yêu cầu cung cấp mật khẩu để xác nhận danh tính của mình. Nếu nhập đúng mật khẩu, người dùng sẽ được kết nối với mạng Wifi.



*Hình 2.7: Quá trình mã hóa của WPA2*

* **Quá trình mã hóa của WPA2:**
* Hai quá trình bao gồm **tính toán MIC** và **mã hóa** được thực hiện song song.
* Tính toán MIC:
* **Bước 1:** Init Block (128 bit) và Data Integrity Key được đưa vào AES ở chế độ CCMP để tạo ra khối 128 bit.
* **Bước 2:** XOR kết quả của bước trước với 128 bit đầu trong payload của khối IEE 802.11 để tạo ra khối 128 bit.
* Kết quả từ bước 2 lại được đưa vào AES-CCMP để tạo ra khối 128 bit
* Bước 3 và bước 4 được thực hiện với các khối payload khác, ngoại trừ field PN được dùng để đánh số frame.
* Từ khối 128 bit cuối cùng, 64 bit được lấy là đặt tên là “R1”, R1 tương ứng với MIC không được mã hóa.
* Mã hóa:
* **Bước 1:** Init counter và Data Encryption Key là input của hàm AES để tạo ra khối 128 bit.
* **Bước 2:** Với khối vừa được tạo ra ở trên, sử dụng XOR với 128 bit payload đầu tiên để tạo ra frame payload đầu tiên.
* Bước 1 và bước 2 được lặp lại với giá trị Init counter tăng dần cho đến khi hoàn thành việc mã hóa toàn bộ payload.
* Counter được tăng lên, và được dùng làm input của hàm AES. Kết quả sau đó được XOR với MIC (R1)
* 64 bit mã hóa quan trọng được lấy và đóng gói cùng với FCS và header của IEEE 802.11

1. **Ưu điểm:**

* Bảo mật tương đối tốt, hơn các công nghệ bảo mật trước đó là WEP và WPA do sử dụng mã hóa AES và khóa PSK.
* Dễ triển khai trong các mạng nhỏ, mạng gia đình.
* Khóa PSK có thể chia sẻ cho tất cả các thiết bị trong mạng giúp quản lí hiệu quả hơn.
* Không tốn nhiều tài nguyên, hiệu quả trong việc cung cấp hiệu suất ổn định và nhanh chóng khi kết nối wifi.

1. **Nhược điểm:**

* Thiếu tính xác thực và quản lí người dùng.
* Khó thay đổi khóa PSK do được chia sẻ với tất cả thiết bị trong mạng , quá trình này có thể gây rắc rối và phải điều chỉnh trên tất cả thiết bị trong mạng.
* Khóa PSK để bị tấn công trong trường hợp mật khẩu yếu, dễ đoán.

#### WPA2-Enterprise

* Thay vì nhập password như WPA2-PSK, người dùng phải nhập User name và Password. Thông tin được lưu ở một server tập trung.

A diagram of a router

Description automatically generated

*Hình 2.8: Quá trình xác thực ở WPA2-Enterprise*

Trong hình có 3 thành phần chính:

* Supplicant/ Client
* Authenticator: thiết bị xác thực quyết định để cho Supplicant truy cập vào mạng hay không.
* Authentication Server: thường dùng RADIUS.
  + 1. **Ưu điểm**
* Quản lí User tập quan
* Kiểm soát AAA để quản lí người dung.
* Quá trình xác thực được mã hóa hoàn toàn vì mã hóa động.
* Được xem là cách xác thực an toàn hơn WPA2-PSK
  + 1. **Nhược điểm**
* Tăng thêm chi phí do có thêm server.
* Cấu hình phức tạp, ảnh hưởng đến trải nghiệm người dùng.
* Không phù hợp cho các mạng nhỏ và mạng cá nhân.

#### Lỗ hổng của WPA2:

Key Reinstallation Attack (KRACK) là một cuộc tấn công trực tiếp vào giao thức WPA2 làm suy yếu quy trình bắt tay 4 bước của WPA2, cho phép tin tặc chặn và thao túng việc tạo khóa mã hóa khóa mới trong quy trình kết nối an toàn.

A table with black text

Description automatically generated

*Hình 2.9: So sánh WEP, WPA và WPA2*

## Chương 3: Kịch bản tấn công và demo

### Cấu hình và cài đặt thiết bị

#### Các thiết bị sử dụng:

* Switch
* Router wifi TL-WR940N
* Usb-wifi: TL-WN722N
* Máy ảo kali
* Các thiết bị kết nối wifi: smart phone, laptop.

#### Cấu hình hệ thống:

* Sử dụng ethernet để kết nối mạng từ switch đến router wifi TL-WR940N
* Cấu hình router wifi TL-WR940N:
  + Cấu hình sử dựng giao thức bảo mật WEP:
    - Định dạng mã ASCII
    - Dạng mã 64 bit và 128 bit
    - Password: 1234a cho 64 bit, và 1234567890uit cho 128 bit
  + Cấu hình sử dựng giao thức bảo mật WPA2:
    - Phiên bản: WPA2-PSK
    - Mã hóa: AES
    - Password: 12345670a
* Attacker sử dụng usb-wifi cho máy kali và sử dụng chế độ monitor.
* Các thiết bị smart phone, laptop đống vai trò client đã kết nối vào vùng mạng qua router wifi.
* Mô hình mạng hệ thống:

A diagram of a computer network

Description automatically generated

*Hình 3.1: Mô hình mạng của kịch bản tấn công*

* Các tool sử dụng: aircarck-ng, wifite, reware.

### Thực hiện

#### Bruce force crack password sử giao thức bảo mật WEP mã hóa 64 bits với tool aircrack-ng

1. **Kịch bản:**

* Đầu tiên thực hiện scan để dò quét các wifi sử dụng giao thức bảo mật WEP, lưu lại các gói tin bắt được vào file .cap.
* Trong trường hợp mạng ít trao đổi data thực hiện tấn công Fakeauthen và tấn công Arp request replay để router wifi liên tục trong đổi data và tạo ra các key IV mới.
* Thu thập tất cả các gói key IV trong file .cap và tiến hành crack password wifi sử dụng giao thức WEP.

1. **Cách thực hiện**

* **Bước 1:** Scan phát hiện wifi xung quanh và thu thập các thông tin các wifi
* Sử dụng lệnh scan: **airodump-ng wlan0** (wlan0: card mạng máy kali đang sử dụng)
* Sau khi scan wifi phát hiện wifi mục tiêu Wireless\_lab sử dụng giao thức bảo mật WEP, với bssid là 50:D4:F7:DB:D2:B7, channel sử dụng là channel 4.
* **Bước 2:** Tiến hành thu thập các gói tin đang trao đổi giữa wifi mục tiêu Wireless\_lab và các client khác trong mạng là lưu vào file arpreplay-01.cap
* Sử dụng lệnh sau để thu thập các gói tin: **airodump-ng --bssid 50:D4:F7:DB:D2:B7 --channel 4 --write arpreplay-01 wlan0**
* --bssid: là bssid(MAC) của wifi mục tiêu
* --chanel: là channel wifi đang sử dụng
* --write: lưu các gói tin vào file .cap
* Wlan0: card mạng mà máy kali đang sử dụng
* Các thông tin thu thập được: địa chỉ MAC của các thiết bị đang kết nối đến wifi Wireless\_lab, “Beacons” số gói beacons, “#Data #/s” là số lượng data/s đang gửi trong mạng.

A screenshot of a computer

Description automatically generated

*Hình 3.2: Kết quả thu thập gói tin*

* **Bước 3:** Thực hiện tấn công fakeauthen mục tiêu để làm cho wifi Wireless\_lab trao đổi dữ liệu nhiều hơn tăng lượng lớn các gói Beacons và gửi nhiều data hơn để quá trình bắt các gói tin chứa key IV điễn ra nhanh hơn.
* Lệnh tấn công: aireplay-ng --fakeauth 0 -a 50:D4:F7:DB:D2:B7 -h C4:6E:1F:11:1C:DE wlan0
* --fakeauth 0: thực hiện tấn công giả mạo xát thực
* -a 50:D4:F7:DB:D2:B7: là tùy chọn để chỉ định địa chỉ MAC của router wifi muốn tấn công.
* -h C4:6E:1F:11:1C:DE: là tùy chọn để chỉ định địa chỉ MAC của thiết bị thực hiện tấn công.
* Wlan0: card mạng máy kali đang sử dụng.
* Tấn công Fakeauthen: attacker sẽ gửi hàng loạt các gói tin giả mạo xát thực yêu cầu xác thực nhưng không cung cấp thông tin xác thực đúng. Khi Router wifi nhận được các gói giả mạo nó sẽ phản hồi lại yêu cầu và gửi kèm theo key IV trong các gói tin (attacker chỉ liên kết trao đổi gói tin với router wifi chứ không phải vào được mạng của wifi).

A computer screen shot of a computer program

Description automatically generated

*Hình 3.3: Kết quả sau khi thực hiện fakeauthen*

* **Bước 4:** Thực hiện tấn công ARP request replay mục tiêu để router wifi liên tục tạo ra các gói tin có chứa key IV mới và gửi đi.
* Lệnh tấn công: aireplay-ng --arpreplay -b 50:D4:F7:DB:D2:B7 -h C4:6E:1F:11:1C:DE wlan0
* --arpreplay: thực hiện tùy chọn tấn công arpreplay.
* -b 50:D4:F7:DB:D2:B7: là tùy chọn để chỉ định địa chỉ MAC của router wifi muốn tấn công.
* -h C4:6E:1F:11:1C:DE: là tùy chọn để chỉ định địa chỉ MAC của thiết bị thực hiện tấn công.
* Wlan0: card mạng máy kali đang sử dụng.
* Tấn công ARP request replay: sau khi attacker đã liên kết thành công với router wifi. Attacker chờ đợi các gói ARP broadcat được gừi từ router wifi, sau đó attacker gửi lại các gói ARP đó làm cho router wifi cập nhật lại bảng arp lưu lại IP và MAC của attacker. Sau đó router wifi gửi các gói có chứa key IV mới liên tục cho attcker trong mõi lần replay ARP.
* **Bước 5:** Thực hiện crack password khi đã thu thập đủ các gói tin chứa key IV
* Lệnh tấn công: aircrack-ng arpreplay-01.cap
* arpreplay-01.cap: là file .cap đã thu thập được ở bước 2 có chứa các key IV.
* Sau khoảng vài phút crack password thành công password wifi Wireless\_lab: 1234a

A screenshot of a computer

Description automatically generated

*Hình 3.4: Kết quả thực hiện crack password wifi Wireless\_lab*

#### Bruce force crack password sử giao thức bảo mật WEP mã hóa 128 bits với tool wifite.

1. **Kịch bản:**

* Sử dụng tool wifite để dò quét wifi có sử dụng giao thức bảo mật WEP, lựa chọn mục tiêu và tiến hành tấn công crack password.
* Với Tool wifite tự động thu thập các gói .cap chứa key IV khi đã đủ gói tự động thực hiện crack password.
* Với Tool Wifite mọi thứ đều được tích hợp tự động, không cần làm từng bước thủ công như tool aircrack-ng.

1. **Cách thực hiện**

* **Bước 1:** sử dụng lệnh: ./Wifite –kill để dò quét wifi và thực hiện tấn công crack password tự động.

A screen shot of a computer

Description automatically generated

*Hình 3.5: Kết quả quét wifi của lệnh ./wifite-kill*

* **Bước 2:** lựa chọn mục tiêu để tiến hành crack password, mục tiêu wifi Wireless\_lab với số thứ tự 12:
* Sau khoảng 10 phút đã crack thành công password wifi Wireless\_lab: 1234567890uit

A computer screen with text and numbers

Description automatically generated

*Hình 3.6: Kết quả crack thành công password của wifi Wireless\_lab*

#### Distionary crack password sử giao thức bảo mật WPA2-PSK mã hóa AES với tool aircrack-ng.

1. **Kịch bản**

* Scan dò quét để phát hiện ra wifi mục tiêu TP-Link\_83C8 và thu thập các gói tin Handshake vào file wpa\_handshake-02.cap.
* Sau đó thực hiện tấn công hủy xát thực giữa router wifi và client kết nối đến wifi đó để bắt các gói handshake.
* Khi đã có đủ các gói tin Handshake hiện crack password wifi với phương pháp distionary attack.

1. **Cách thực hiện**

* **Bước 1:** Scan phát hiện wifi xung quanh và thu thập các thông tin các wifi
* Sử dụng lệnh scan: airodump-ng –band abg wlan0
* Wlan0: card mạng máy kali đang sử dụng.
* --band abg: scan wifi có tần số từ 2.4ghz – 5 ghz.
* Sau khi scan wifi phát hiện wifi mục tiêu TP-Link\_83C8 sử dụng giao thức bảo mật WPA2-PSK, với bssid là 40:ED:00:35:83:C8, channel sử dụng là channel 10.

A screenshot of a computer

Description automatically generated

*Hình 3.7: Kết quả scan wifi*

* **Bước 2:** Tiến hành thu thập các gói tin đang trao đổi giữa wifi mục tiêu TP-Link\_83C8 và các client khác trong mạng là lưu vào file wpa\_handshake-02.cap
* Sử dụng lệnh sau để thu thập các gói tin handshake: airodump-ng --bssid 40:ED:00:35:83:C8--channel 10 --write wpa\_handshake-02 wlan0
* --bssid: là bssid(MAC) của wifi mục tiêu
* --channel: là channel wifi đang sử dụng
* --write: lưu các gói tin vào file .cap
* Wlan0: card mạng mà máy kali đang sử dụng
* Các thông tin thu thập được: “Station” địa chỉ MAC của các thiết bị đang kết nối đến wifi TP-Link\_83C8, “Beacons” số gói beacons, “#Data #/s” là số lượng data/s đang gửi trong mạng.

A screenshot of a computer

Description automatically generated

*Hình 3.8: Thông tin thu thập được của TP-Link\_83C8*

* **Bước 3:** Thực hiện tấn công hủy xát thực giữa router wifi và client kết nối đến wifi đó. Mục tiêu của tấn công làm mất kết nối wifi giữa client và router wifi trong vài giây và bắt các gói Handshake và lưu các gói này vào file wpa\_handshake.cap.
* Lệnh tấn công: aireplay-ng --deauth 4 -a 40:ED:00:35:83:C8 -c 16:66:0D:D1:2A:CD wlan0
* --deauth 4: Tùy chọn tấn công hủy xát thực và gửi 4 gói tin hủy xát thực đến router wifi và cả client.
* -a 40:ED:00:35:83:C8: là tùy chọn để chỉ định địa chỉ MAC của router wifi muốn tấn công.
* -c 16:66:0D:D1:2A:CD: là tùy chọn để chỉ định địa chỉ MAC của client muốn tấn công.
* Wlan0: card mạng máy kali đang sử dụng.
* Tấn công hủy xát thực: attacker giả mạo địa chỉ MAC của router wifi gửi gói tin hủy xát thực đối với client, đồng thời attacker giả mạo cả MAC của client gửi gói tin hủy xát thực đến router wifi. Sau đó client tự động vào mạng và xác thực lại với router wifi, trong quá trình xát thực này sinh ra các gói tin handshake.

A screen shot of a computer

Description automatically generated

*Hình 3.9: Kết quả nhận được sau khi thực hiện tấn công Deauth*

* Các gói handshake đã bắt được:

A screenshot of a computer program

Description automatically generated

*Hình 3.10: Các gói handshake thu được*

* **Bước 4:** tạo list các password theo một mẫu có khả năng là password của wifi với tool crunch (giả sử chúng ta biết thói quen đặt password của victim thông qua các cuộc tấn trước đó như social engineering, phishing, sniffing,.. ta phát hiện thói quen đặt password của victim như sau: có số 1 ở đầu, số 0 và chữ cái a ở cuối).
* Lệnh tạo list password theo mẫu: crunch 9 9 123345679 -o wordlist.txt -t 1@@@@@@0a
* 9 9: độ dài password tối thiểu và tối đa là 9 ký tự
* 123345679: là các ký tự để tạo ra mẫu password (số, chữ hoa, thường,..)
* -o wordlist.txt: lưu vào file wordlist.txt
* -t 1@@@@@@0a: tạo list password theo mẫu có số 1 ở đầu và số 0, chữ a ở cuối, @ tượng trưng cho các ký tự chưa biết.

A screenshot of a computer

Description automatically generated

*Hình 3.11: Kết quả thực hiện tạo list pasword*

* **Bước 5:** Thực hiện crack password với list vừa tạo sử dụng tool aircrack-ng và file wpa\_handshake-02.cap đã bắt được.
* Lệnh crack password: aircrack-ng wpa\_hanshake-02.cap -w wordlist.txt
* wpa\_hanshake-02.cap: file chứa các gói handshake bắt được ở bước 3.
* -w wordlist.txt: sử dụng wordlist.txt chứa các mẫu password vừa tạo.
* Sau khoảng vài phút đã crack thành công password wifi TP-Link\_83C8: 12345670a

A screenshot of a computer

Description automatically generated

*Hình 3.12: Kết quả sau khi crack thành công password của TP-Link\_83C8*

# PHẦN KẾT LUẬN

### So sánh chuẩn mã hóa WEP, WPA và WPA2

* WEP (Wired Equivalent Privacy): là giao thức lâu đời và cũng có hiệu quả bảo mật kém nhất. Giao thức này sử dụng khóa mã hóa có độ dài 64 bits hoặc 128 bits để bảo vệ dữ liệu truyền qua mạng. Tuy nhiên WEP dễ bị tấn công hoặc bẻ khóa bằng nhiều cách khác nhau. Vì vậy giao thức này được khuyến nghị không nên sử dụng trong mã hóa mạng không dây.
* WPA (Wifi Protected Access): là giao thức mã hóa bảo mật hơn so với WEP. Giao thức này sử dụng thuật toán TKIP để mã hóa các dữ liệu truyền qua mạng. WPA còn sử dụng MIC để đảm bảo tính toàn vẹn của dữ liệu đồng thời ngăn chặn các cuộc tấn công cố gắng thay đổi dữ liệu trong quá trình truyền. Tuy nhiên WPA vẫn có thể bị tấn công và còn một số hạn chế
* WPA2 (Wifi Protected Access II): là giao thức bảo mật tốt nhất hiện tại. Giao thức này sử dụng AES để mã hóa dữ liệu được truyền qua mạng. WPA2 còn bao gồm một tính năng là CCMP cung cấp tính năng bảo mật nâng cao và tính toàn vẹn dữ liệu. WPA2 không ngăn chặn tất cả các cuộc tấn công nhưng nó an toàn hơn nhiều so với WEP và WPA.

### Kết luận

Không có biện pháp nào có thể bảo vệ bạn an toàn 100% khỏi các cuộc tấn công mạng không dây. Tuy nhiên, để nâng cao và bảo vệ bản than và dữ liệu của mình một cách tốt nhất thì ngoài việc sử dụng các chuẩn mã hóa mới nhất, an toàn nhất có thể, thì việc triển khai mật khẩu với độ dài và cấu trúc khó đoán hơn, đồng thời kết hợp nhiều biện pháp bảo mật sẽ đem lại kết quả tốt hơn.

# TÀI LIỆU THAM KHẢO

# Bibliography

| [1] | M. Vanhoef, “Key Reinstallation Attacks,” KRACKATTACK, 2017. [Trực tuyến]. Available: https://www.krackattacks.com/. [Đã truy cập 20 4 2024]. |
| --- | --- |
| [2] | SECUREW2, “Simplifying WPA2-Enterprise and 802.1x,” [Trực tuyến]. Available: https://www.securew2.com/solutions/wpa2-enterprise-and-802-1x-simplified. |
| [3] | B. K. Jena, “What Is AES Encryption and How Does It Work?,” 9 February 2023. [Trực tuyến]. Available: https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption. [Đã truy cập 20 4 2024]. |
| [4] | Zenarmor, “Zenarmor,” 24 April 2024. [Trực tuyến]. Available: https://www.zenarmor.com/docs/network-security-tutorials/what-is-wpa. |
| [5] | K. Hanko, “Clario,” 25 November 2022. [Trực tuyến]. Available: https://clario.co/blog/wep-vs-wpa-vs-wpa2/. |
| [6] | A. S. Gillis, “TechTarget,” December 2022. [Trực tuyến]. Available: https://www.techtarget.com/searchmobilecomputing/definition/Wi-Fi-Protected-Access. |
| [7] | P. Loshin, “TechTarget,” August 2021. [Trực tuyến]. Available: https://www.techtarget.com/searchsecurity/definition/Wired-Equivalent-Privacy. |
| [8] | INFORSECTRAIN, “INFORSECTRAIN,” 17 February 2023. [Trực tuyến]. Available: https://www.infosectrain.com/blog/wep-vs-wpa-or-wpa2/. |
| [9] | OKTA, “OKTA,” 26 July 2022. [Trực tuyến]. Available: https://www.okta.com/identity-101/wep/. |