ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

BÁO CÁO ĐỒ ÁN

An toàn mạng không dây

ĐỒ ÁN MÔN HỌC

Nghiên cứu và Xây dựng thử nghiệm hệ thống WIDS

Giảng viên hướng dẫn: Lê Đức Thịnh

Nhóm 07

Nguyễn Lê Thảo Ngọc - 21521191

Hồ Công Long - 21522297

TP. HỒ CHÍ MINH, 2024

LỜI CẢM ƠN

Lời đầu tiên, nhóm chúng em xin trân trọng cảm ơn giảng viên Lê Đức Thịnh đã giúp chúng em hiểu rõ hơn về cơ sở lý thuyết nhằm hoàn thành được đồ án này.

Mặc dù đã có những đầu tư nhất định trong quá trình làm bài song cũng khó có thể tránh khỏi những sai sót, em kính mong nhận được ý kiến đóng góp của quý thầy/cô để đồ án của chúng em được hoàn thiện hơn nữa.

Nhóm em xin chân thành cảm ơn!

Mục lục

DANH MỤC HÌNH ẢNH

Chương 1. GIỚI THIỆU VỀ ĐỀ TÀI

1. Tổng quan đề tài

Ngày nay với sự phát triển mạnh mẽ của công nghệ, mạng Wifi (đặc biệt là chuẩn 802.11) đã và đang trở thành thành phần không thể thiếu trong cuộc sống hàng ngày của con người. Bởi từ chiếc điện thoại (thứ mà ai cũng mang theo bên người), laptop cho tới các thiết bị dân dụng như tủ lạnh, máy giặt, máy điều hoà,… hay các thiết bị IoT đều cần sử dụng mạng và kết nối tới Internet. Sự ứng dụng rộng rãi này khiến mạng Wifi trở thành đối tượng hấp dẫn bị nhiều kẻ xấu nhắm tới nhằm khai thác thông tin và dữ liệu người dùng một cách trái phép, do đó chúng cần phải thực hiện các biện bảo vệ thích hợp như là sử dụng hệ thống WIDS hoặc WIPS nhằm kịp thời phát hiện và ngăn chặn cuộc tấn công mạng không dây. Trong đề tài này, chúng ta sẽ chỉ làm việc với mạng không dây sử dụng giao thức mã hoá WPA2 để tái hiện lại các cuộc tấn công đơn giản và biểu diễn khả năng phát hiện cuộc tấn công của hệ thống WIDS mà nhóm triển khai.

2. Lý do chọn đề tài

Hiện nay mạng Wifi được sử dụng rất rộng rãi, do đó vấn đề bảo mật trong mạng này ngày càng được quan tâm dẫn tới rất nhiều giao thức mã hoá đã được ra đời như WEP, WPA, WPA2, WPA3. Tuy nhiên theo thời gian, giao thức nào cũng xuất hiện các lỗ hổng và dần bị thay thế bởi giao thức khác tốt hơn, cụ thể là bây giờ WPA2 là giao thức được dùng phổ biến nhất (thay thế hoàn toàn WEP và WPA), WPA3 thì bảo mật tốt hơn WPA2 nhưng chưa được ứng dụng rộng rải bằng. Do đó nhóm chọn đề tài Nghiên cứu và Xây dựng thử nghiệm hệ thống WIDS nhằm cung cấp cái nhìn rõ hơn về cách mạng không dây bị tấn công dù sử dụng giao thức mã hoá WPA2 và cũng như cách 1 hệ thống WIDS phát hiện một số tấn công.

3. Tóm tắt đề tài

Hệ thống WIDS trong đề tài sẽ được xây dựng theo kiến trúc Overlay với 1 sensor và 1 WIDS server chạy trên máy ảo Kali linux. WIDS mà nhóm triển khai là dạng phần mềm cài trên máy ảo nên nó sẽ sử dụng các công cụ có sẵn như Tshark, Aircrack-NG để phân tích các gói tin mà sensor bắt được. Sau đó WIDS sẽ thực hiện phân tích và xuất thông báo nếu phát hiện dấu hiệu nguy hiểm tiềm ẩn thông qua kỹ thuật phát hiện tấn công Signature Analysis (Signature-based).

WIDS này sẽ có các chức năng như:

+ Phát hiện beacon attack, deauthentication attack, authentication attack

+ Phát hiện một số tấn công diễn ra trong mạng không dây mã hoá WPA2: evil twins,

+ Phát hiện một số tấn công diễn ra trong mạng không dây mã hoá WPA:

+ Phát hiện một số tấn công diễn ra trong mạng không dây mã hoá WEP:

+Xuất ra thông báo khi phát hiện nguy hiểm tiềm ẩn

Chương 2. CƠ SỞ LÝ THUYẾT

I. Wireless Networking

1. Khái niệm

Mạng không dây cho phép các thiết bị sử dụng tài nguyên máy tính mà không cần được kết nối vật lý với mạng. Các thiết bị không dây chỉ cần ở trong một khoảng cách nhất định (phạm vi phủ sóng mạng) của cơ sở hạ tầng mạng không dây là có thể kết nối tới Internet.

Mạng cục bộ không dây (WLAN) là một nhóm các nút mạng không dây nằm trong một khu vực địa lý giới hạn, có khả năng trao đổi dữ liệu thông qua truyền thông vô tuyến. Mạng WLAN thường được sử dụng bởi các thiết bị trong phạm vi khá hạn chế, chẳng hạn như tòa nhà văn phòng hoặc khuôn viên công ty và được triển khai như dạng mở rộng của mạng (LAN) để nâng cao tính di động cho người dùng.

2. Các thành phần trong mạng không dây

Các host không dây:

+Các thiết bị điện tử kết nối tới mạng mà không cần có kết nối vật lý

+Dùng để chạy các ứng dụng

+ Có thể di động hoặc cố định (Không dây không có nghĩa là luôn luôn di động)

Ví dụ: Laptop, smartphone, thiết bị

IoT, …

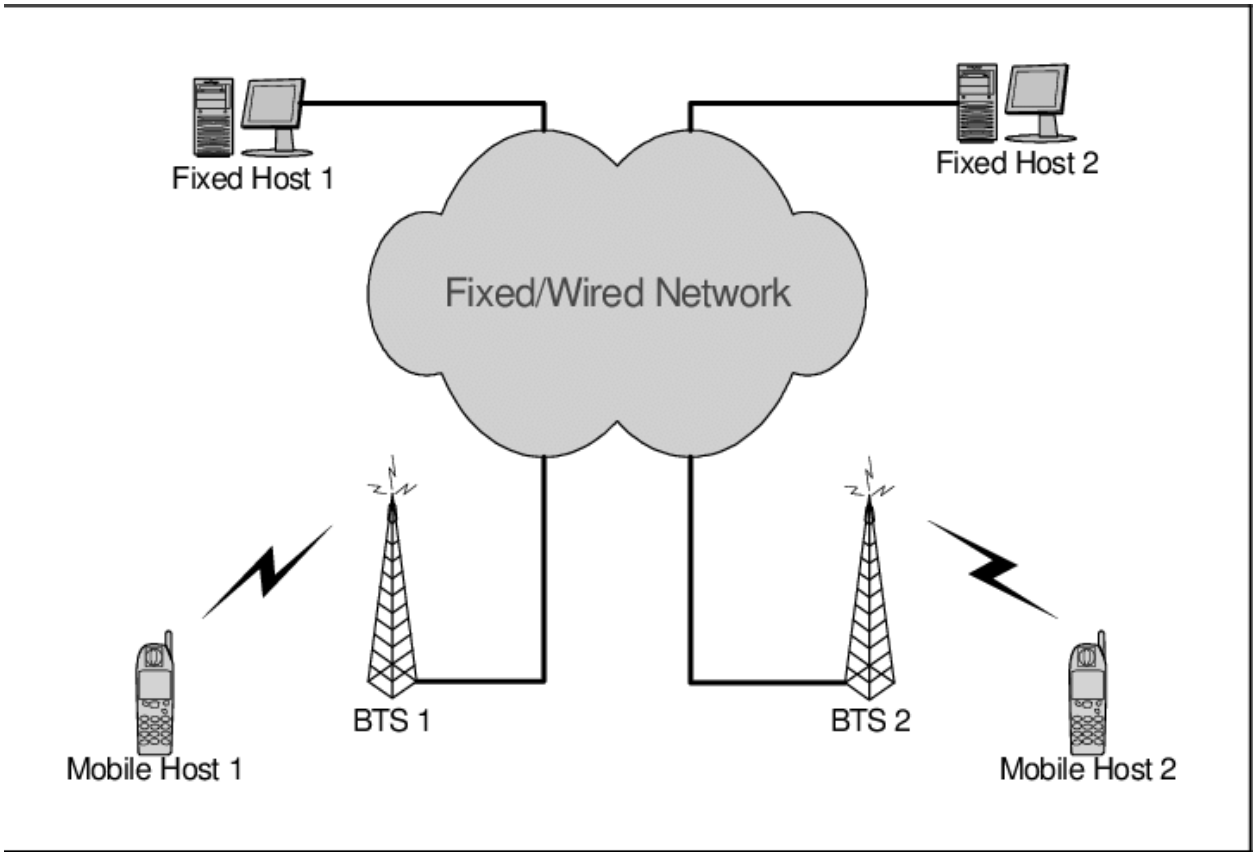
Hình 2. 1 Các thiết bị kết nối không dây

Base station:

Thường được kết nối vào mạng có dây

+ relay – chịu trách nhiệm cho việc gửi các gói giữa mạng có dây và các host không dây trong “vùng” của nó

Ví dụ cell towers, 802.11 access points, base transceiver station (BTS)



Hình 2. 2 Mô tả quá trình Relay của BTS

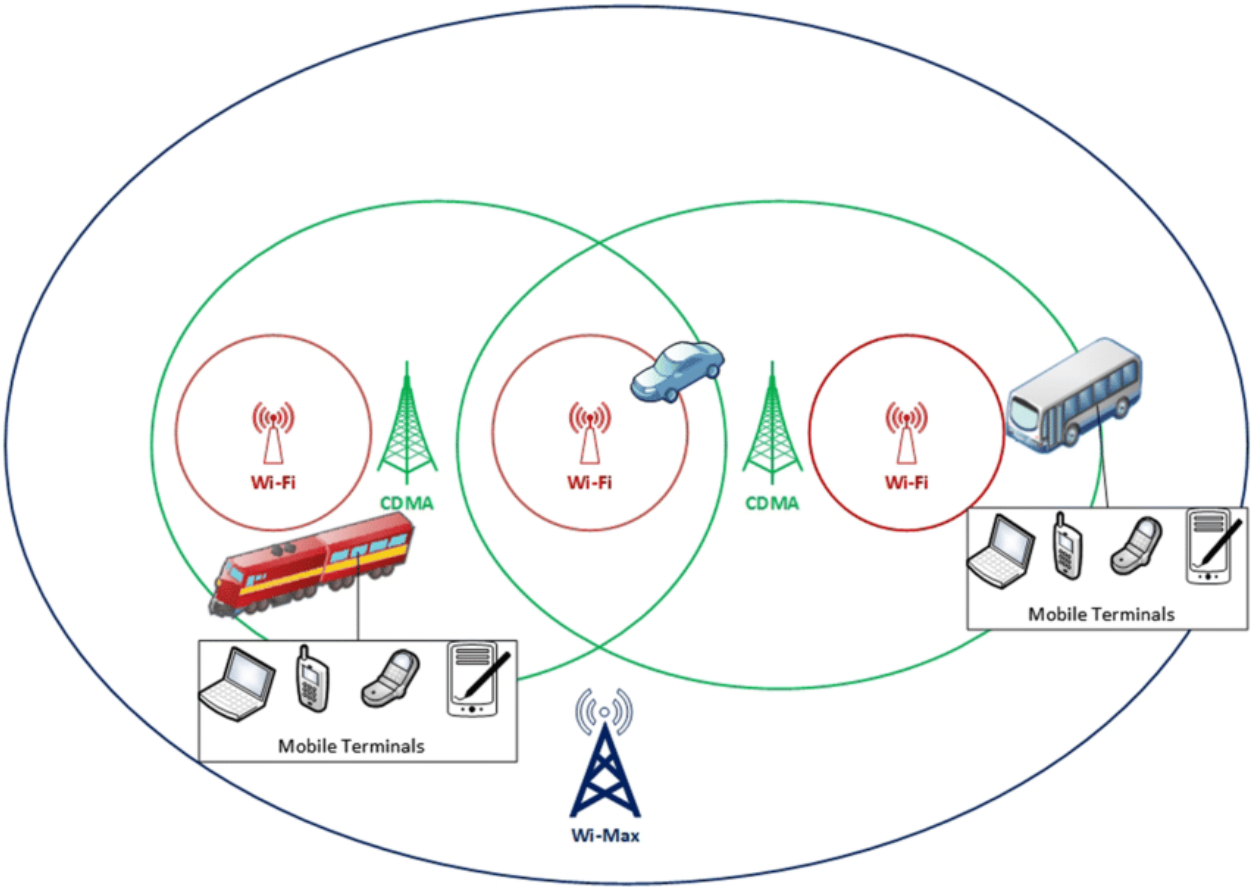
Môi trường kết nối không dây

+ Thường được sử dụng để kết nối các mobile tới base station

+ Cũng được sử dụng như là đường kết nối xương sống (backbone link)

+ Giao thức đa truy cập

+ Tốc độ dữ liệu và khoảng cách truyền khác nhau



Hình 2. 3 Môi trường mạng không dây

3. Nguy cơ bảo mật trong mạng không dây

- Các lỗ hỏng trong mạng dây đều có thể tồn tại trong mạng không dây như tấn công DdoS, Eavesdropping, sniffing and spoofing,…
- Môi trường truyền dẫn khác nhau dẫn đến một số nguy cơ riêng biệt.

Mạng không dây cung cấp nhiều thuận lợi cho kẻ tấn công hơn khi muốn tiếp cận hệ thống của nạn nhân.

Kẻ tấn công có thể đứng ở ngoài phạm vi của tổ chức của nạn nhân để thực hiện tấn công qua mạng không dây.

- Thiết bị đầu cuối trong mạng không dây có nhiều đặc điểm dễ gây ra các nguy cơ bảo mật.

Năng lực xử lý yếu

Nguồn năng lượng hạn chế

Thường đặt tại các vị trí có tính “Physical security” yếu

- Cung cấp các dịch vụ mới, cần có các kỹ thuật đánh giá bảo mật mới.

Hầu hết các giao thức giao tiếp hiện nay không đủ bảo mật. Các chuẩn bảo mật WEP, WPA2, WPA đều có thể bị bypass.

II. Wireless IDS

1. Giới thiệu

Trong WLAN với môi trường truyền dẫn là không khí, các thiết bị có hỗ trợ chuẩn 802.11 trong phạm vi phủ sóng đều có thể truy cập vào mạng. Việc này tiềm ẩn nhiều rủi ro bảo mật, cũng như dễ khiến ta trở thành nạn nhân trong cuộc tấn công mạng. Do đó nhiều công ty, tổ chức đã triển khai WIDS/WIPS để phát hiện các cuộc tấn công trong mạng không dây 802.11.

Wireless IDS là hệ thống phần mềm hoặc phần cứng tự động ứng dụng trong mạng không dây nhằm thực hiện quy trình phát hiện xâm nhập. Đây là quy trình theo dõi các sự kiện diễn ra trong một hệ thống máy tính hoặc mạng máy tính và phân tích lưu lượng mạng để nhận biết các dấu hiệu của sự bất thường. Nó bao gồm việc *giám sát tần số sóng*(RF_Radio frequency), *phát hiện nhiễu*,….

WIDS thường tập trung theo dõi 24/7 phổ sóng vô tuyến (radio spectrum) trên mạng WLAN chuẩn 802.11(vì phần lớn các doanh nghiệp đều triển khai mạng theo chuẩn này) để phát hiện, định vị các thiết bị không dây nằm trong vùng phủ sóng của WLAN.

**** Sự khác biệt giữa WIDPS và IDPS truyền thống***

Nhìn chung, WIDPS có khá nhiều điểm tương đồng với IDPS truyền thống, tuy nhiên chỉ WIDPS mới hoạt động ở tầng Physical (mô hình OSI) và ứng dụng cho môi trường mạng không dây.

Thay vì bắt tất cả gói tin trong mạng mà nó giám sát thì WIDPS làm việc bằng cách “sampling traffic” tức là bắt gói tin không liên tục. Việc này là do có tới 2 băng tần để giám sát (2.4 GHz và 5GHz) và mỗi băng tần lại có thể hỗ trợ nhiều channel. Do đó 1 sensor không thể nào giám sát tất cả lưu lượng mạng trên cùng 1 băng tần một cách liên tục như IDPS truyền thống được vì mỗi sensor chỉ có khả năng giám sát 1 channel tại 1 thời điểm.

(Khi sensor đã sẵn sàng để theo dõi một channel khác, nó sẽ tắt radio của nó rồi chuyển sang channel khác, sau đó mới bật radio lên lại để thực hiện giám sát)

Ngoài ra, phạm vi hoạt động của WIDPS bị hạn chế bởi các cơ sở vật chất. Vì làm việc với sóng vô tuyến nên với khả năng giao tiếp giữa sensor với WIDPS server có thể bị cản trở hoặc gián đoạn bởi vật chất như tường (bê tông, gạch, đá) , vật liệu bằng kim loại có tính hấp thụ điện cao, các thiết bị sử dụng chung tần số wifi như lò vi sóng,…

	Đặc điểm chính	**Ưu điểm**	**Nhược điểm**
WIDPS	+ Dùng trong môi trường wireless network + Giám sát môi trường mạng không dây, phát hiện, ngăn chặn các cuộc tấn công có thể xảy ra và có khả năng phát hiện được rouge access point +Thường có nhiều sensor +Phạm vi hoạt động lớn	+ Dễ mở rộng phạm vi giám sát + Giám sát được cả tầng physical +Đáp ứng được tính di động	+ Phạm vi hoạt động của sensor bị giới hạn bởi cơ sở vật chất + Có hiện tượng nhiễu nếu môi trường truyền dẫn không tốt + Không bắt được tất cả gói tin trong mạng mà nó giám sát
IDPS truyền thống	+Dùng trong môi trường wire network + Giám sát môi trường mạng có dây, phát hiện, ngăn chặn các cuộc tấn công có thể xảy ra +Phạm vi hoạt động có giới hạn	+Có tính bảo mật cao hơn +Hiệu suất hoạt động không bị ảnh hưởng bởi ngoại cảnh (ví dụ như không có hiện tượng nhiễu tín hiệu như bên WIDPS, phạm vi hoạt động của sensor cũng không bị giới hạn bởi cơ sở vật chất xnug quanh,…)	+ Kiến trúc phức tạp tuỳ theo yêu cầu sử dụng + Tốn chi phí cho dây liên kết các thiết bị

		+Có thể bắt được tất cả gói tin trong mạng mà nó giám sát	

**** Yêu cầu cần có khi triển khai hệ thống IDPS***

+ Xác định rõ các mục tiêu và chính sách bảo mật muốn thực hiện

+ Chọn và triển khai đúng loại IDPS phù hợp với kiến trúc xây dựng dựa trên các yếu tố như: lưu lượng truy cập, cấu trúc mạng, security zone,….

+ Biết tuỳ chỉnh và thiết lập cài đặt cũng như các quy tắc tương ứng với hệ thống triển khai và mục tiêu đề ra

2. Thành phần hệ thống

Hệ thống WIDS gồm 2 thành phần chính WIDS server và các sensor

2.1 Sensor

2.1.1 Tổng quan

Sensor khá giống với access point nhưng có nhiều chức năng hơn như giám sát tần số sóng(RF_Radio frequency), phát hiện nhiễu,… Thu thập thông tin gồm địa chỉ MAC (Media Access Control), SSID, các đặc tính được thiết lập ở các trạm, tốc độ truyền, kênh hiện tại, trạng thái mã hóa, …..

Sensor sử dụng sóng vô tuyến 802.11 để thu thập thông tin giúp phân tích và bảo vệ lưu lượng mạng WLAN. Nó có thể là 1 thiết bị phần cứng hoặc phần mềm, điều quan trọng là vị trí đặt nó phải được quyết định theo chiến lược sao cho sensor có khả năng lắng nghe và nắm bắt tất cả các thông tin liên lạc chuẩn 802.11.

Hình 2. 4 Thiết bị cảm biến của WIDS/WIPS

2.1.2 Vị trí đặt sensor

Vì các sensor đóng vai trò như tai và mắt của WIDS nên chúng ta cần phải đặt chúng ở vị trí lắng nghe và bắt được nhiều dữ liệu nhất có thể trong môi trường mạng không dây, hoặc dùng càng nhiều sensor càng tốt. Tuy nhiên thực tế, khi triển khai hệ thống WIDS vì nhiều vấn đề liên quan như kinh phí, phạm vi triển khai, mục đích dùng WIDS,… mà các doanh nghiệp thường cân nhắc kỹ để quyết định vị trí lắp đặt sensor. Một số yếu tố thường được quan tâm khi chọn vị trí lắp đặt sensor:

+**Physical security:** vì sensor thường đặt ở các vị trí mở (trần hành lang, phòng họp, khuôn viên trường,…) thay vì đặt trong nơi khép kín (tủ thiết bị) nhằm tăng phạm vi hoạt động nên chúng thường dễ bị tác động bởi các yếu tố vật lý. Do đó chúng ta nên có biện pháp tăng khả năng an toàn cho sensor như dùng sensor có tính năng chống giả mạo, lắp đặt ở nơi công cộng nhưng ở vị trí khó bị phát hiện hoặc trong tầm nhìn của camera an ninh.

+Sensor range: Phạm vi hoạt động của sensor phụ thuộc vào nhiều yếu tố như cơ sở vật chất xung quanh (tường, cửa, vách ngăn,…), môi trường truyền dẫn,…. Do đó chúng nên được triển khai sao cho phạm vi của chúng giao nhau ít nhất 20%.

+ Wired Network Connections: Vì một số loại sensor cần có kết nối với mạng có dây nên việc lắp đặt quá xa mạng có dây cũng là vấn đề cần quan tâm.

+Cost: Lý tưởng nhất là một tổ chức có thể triển khai các sensor khắp cơ sở của mình để thực hiện giám sát toàn bộ mạng không dây. Tuy nhiên, số lượng cảm biến cần thiết để làm được điều đó có thể khá lớn, đặc biệt là trong môi trường mở và quá rộng. Do đó các tổ chức thường so sánh tác hại của các mối đe doạ tiềm ẩn có thể xảy ra cùng

với các chi phí phải chi trả khác, từ đó họ sẽ xây dựng và phát triển giải pháp nhằm tạo ra sự an toàn trong mạng WLAN với các rủi ro ở mức độ chấp nhận được.

+ AP and Wireless Switch Locations: Với kiến trúc Intergrated, các sensor sẽ vừa là AP vừa là sensor thực hiện thu thập thông tin cho WIDS, do đó vị trí switch và AP khác (nếu có) trong WLAN sẽ rất quan trọng . Bởi nếu đặt sensor quá xa chúng thì sẽ ảnh hưởng tới lưu lượng mạng (như dễ mất kết nối, gây chậm trễ quá trình truyền gửi gói tin).

2.2 WIDS/WIPSServer

2.2.1 Tổng quan

WIDS/WIPS server đóng vai trò như trung tâm giám sát, thu thập và phân tích dữ liệu mà các sensor thu thập được nhằm phát hiện mối đe doạ. Nó thường là thiết bị độc lập hoặc phần mềm chạy trên máy ảo.

Ngoài ra WIDS/WIPS server cũng được tích hợp trong WLAN controller. Khả năng giám sát của WIDS/WIPS server cũng có thể được tận dụng, hợp nhất với network management server (NMS) như giải pháp giúp giám sát toàn diện mạng WLAN.

2.2.2 Khả năng phân tích dữ liệu

Một server thường có khả năng dùng kết hợp nhiều loại phân tích dữ liệu khác nhau để đưa ra cảnh báo kịp thời ngay khi phát hiện sự bất thường như:

+ Dùng signature analysis, behavior analysis, protocol analysis và RF spectrum analysis để phát hiện các rủi ro, mối đe doạ tiềm ẩn

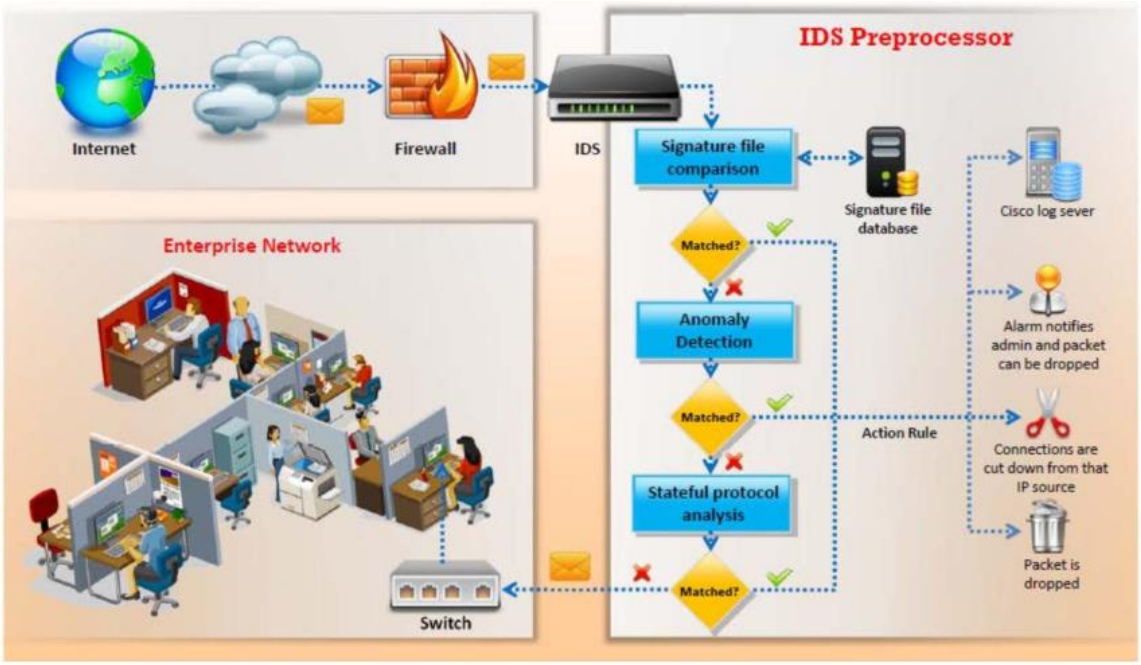
+Dùng Protocol analysis để khai thác thông tin tầng MAC ở khung 802.11 trong packet

+ RF spectrum analysis dùng để giám sát trạng thái Radio Frequency như cường độ tín hiệu và tỷ lệ tín hiệu trên tạp âm (SNR).

+ Performance analysis có thể được sử dụng để đánh giá số liệu thống kê về tình trạng của mạng WLAN, chẳng hạn như dung lượng và độ phủ sóng.

3. Mô hình hoạt động

Về cơ bản, phần lớn các thành phần của IDS và WIDS (ngoại trừ sensor thì đều có chức năng, hoạt động tương tự nhau



Hình 2. 5 Quy trình hoạt động

Khi có gói tin từ bên ngoài vào mạng WLAN, trước tiên gói tin này sẽ đi qua firewall rồi mới tới IDS, việc đặt firewall trước IDS để nó lọc bớt các gói tin, nhằm giảm tải số lượng gói tin cần phân tích cho IDS cũng như bảo vệ IDS khỏi bị tấn công. Tại IDS server, gói tin sẽ được phân tích bằng các kỹ thuật như Signature Analysis, Behavioral Analysis, Protocol Analysis,….Kết quả sau khi phân tích sẽ được ghi vào các bản record và nếu phát hiện mối nguy hiểm hay sự kiện vi phạm rule được thiết lập thì IDS sẽ xuất ra thông báo tới người dùng cuối. Tuy nhiên vì đây chỉ là hệ thống IDS nên nó sẽ không ngăn cản gói tin tới mạng nội bộ dù cho có thể nguy hiểm.

4. Phân loại

Dựa trên Nguồn dữ liệu

• Network-based: theo dõi các đặc điểm của một host riêng lẻ và các sự kiện xảy ra trong host đó để phát hiện hoạt động bất thường.

• Host-based:) theo dõi lưu lượng mạng cho một phần của mạng (network segment) hoặc các thiết bị, phân tích các hoạt động mạng và các giao thức, ứng dụng để xác định các hành vi bất thường

• Hybrid (lai): Sự kết hợp giữa mô hình Host-based và Network-based

Dựa trên kiến trúc triển khai thường có 2 loại chính:

- Overlay
- Integrated

Dựa trên Các kỹ thuật phát hiện tấn công

- Signature Analysis (Signature-based)
- Behavioral Analysis (Anomaly-based)
- Protocol Analysis
- Spectrum Analysis
- Forensic Analysis
- Performance Analysis

4.1 Kiến trúc triển khai

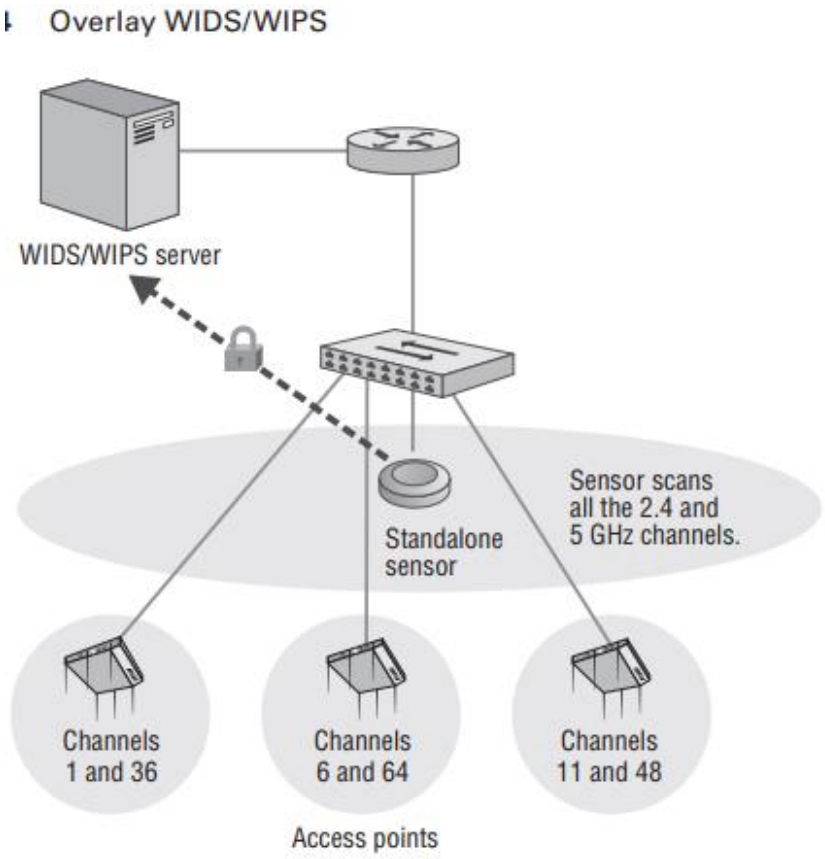
4.1.1 Overlay

Trong kiến trúc overlay, hệ thống WIDS/WIPS sẽ gồm 1 WIDS/WIPS server và nhiều sensor chuyên biệt (standalone sensor) dùng riêng cho hệ thống này.

Các sensor chuyên biệt này sử dụng sóng vô tuyến chuyên dụng do đó nó chỉ hoạt động như cảm biến của WIDS/WIPS server chứ không được sử dụng làm access point trong mạng WLAN. Ngoài ra các sensor này còn cần có cáp riêng để chạy và giao tiếp với WIDS/WIPS server thông qua mạng IP.

Thông thường, các standalone sensor có thể sử dụng một đài phát thanh băng tần kép 802.11 để giám sát cả băng tần ISM 2,4 GHz và băng tần UNII 5 GHz, chúng cũng có thể có 2 radio: 1 radio dàng riêng cho giám sát channel 2,4 GHz và 1 radio giám sát channel 5GHz.

Việc triển khai WIDS/WIPS với kiến trúc Overlay thường có nhiều tính năng và khả năng giám sát rộng hơn kiến trúc thông thường nhưng tốn nhiều chi phí hơn. Bởi kiến trúc này sẽ làm tăng chi phí phần cứng và triển khai nhưng cung cấp nhiều chức năng và bảo mật hơn các kiến trúc truyền thống. Ngoài ra một ưu điểm lớn khác của mô hình overlay là nếu WLAN ngừng hoạt động, WIDS/WIPS vẫn tiếp tục thực hiện giám sát do WIDS/WIPS độc lập với cơ sở hạ tầng WLAN.



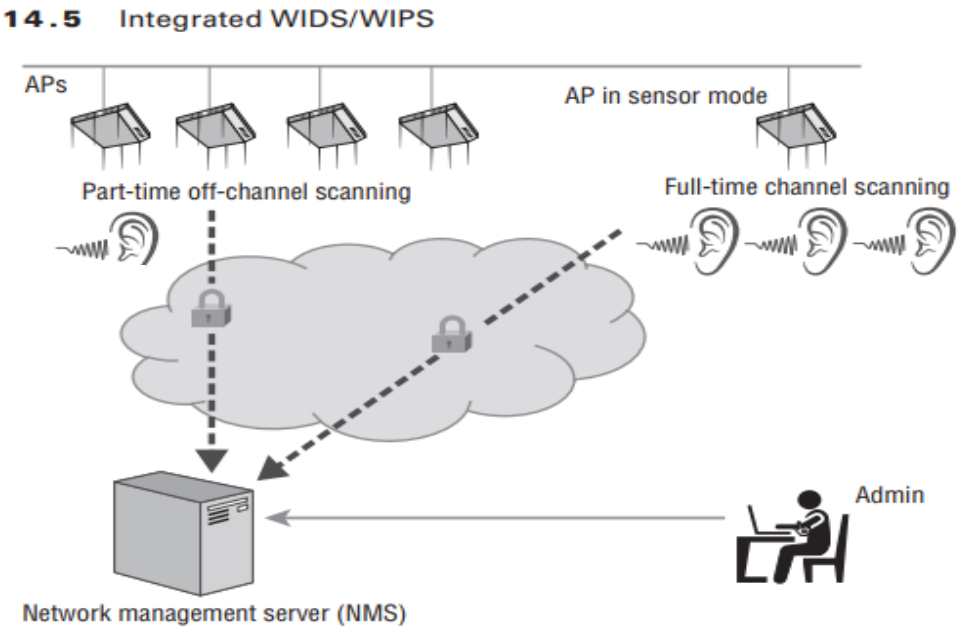
Hình 2. 6 Kiến trúc Overlay

4.1.2 Intergrated

Trong kiến trúc Intergrated, WIDS/WIPS có khả năng vừa giám sát mạng một cách bảo mật vừa cung cấp quyền truy cập mạng cho client trong WLAN. Để thực hiện việc này, các access point được yêu cầu có chức năng như một sensor của WIDS/WIPS server trong khi vừa phải thực hiện các chức năng vốn có của access point như cung cấp quyền truy cập mạng cho các client, cung cấp kết nối chuẩn 802.11,…

Ngoài ra với kiến trúc này, việc triển khai WIDS/WIPS server phụ thuộc vào kiến trúc ban đầu của WLAN. Cụ thể là:

Kiến trúc WLAN tập trung	Kiến trúc WLAN phân tán
WIDS/WIPS server sẽ được tích hợp vào contro.Các AP dựa trên bộ điều khiển (có chức năng như cảm biến), được quản lý và giám sát tập trung từ bộ điều khiển WLAN.	Máy chủ quản lý mạng NMS - (Network management server) sẽ kết hợp với máy chủ WIDS. Các AP phân tán (có chức năng như cảm biến), được quản lý và giám sát tập trung từ NMS (dựa trên đám mây hoặc tại chỗ)



Hình 2. 7 Kiến trúc Intergrated

4.2 Các kỹ thuật phát hiện tấn công

4.2.1 Signature Analysis (Signature-based)

Signature là một mẫu tương ứng với một nguy cơ tấn công (cơ sở dữ liệu về *các tấn công đã biết trước*)

Signature Analysis (hay còn gọi knowledgebased) là một quá trình so sánh các signature với các sự kiện quan sát được để xác định các sự cố có thể có.

Ví dụ:

+ Một kết nối telnet với username là root là dấu hiệu vi phạm chính sách

bảo mật của 1 tổ chức.
+ Một email với tiêu đề “Free pictures!” và có tên file đính kèm freepics.exe là đặc điểm của một malware đã biết.

Một số signature về các cuộc tấn công phổ biến như man-in-the-middle attacks, DoS attacks, flood attacks

Hình 2. 8 Signature của một số cuộc tấn công

Trong WIDS, các signature là các mẫu tương ứng với cuộc tấn công nhằm vào Layer 1 và Layer 2. Dữ liệu về các signature cũng sẽ được các nhà cung cấp WIDS cập nhập tự động ngay khi có signature mới được phát hiện. Ngoài ra hệ thống WIDS cũng cho phép người quản trị WLAN tự tạo signature phù hợp hơn với tấn công có thể xảy ra trong mạng WLAN của họ.

Ưu điểm:

Độ chính xác cao khi phát hiện các tấn công đã biết, tỉ lệ cảnh báo sai thấp.

Nhược điểm:

Không thể phát hiện các hành vi bất thường chưa biết trước hoặc các biến đổi nhỏ trong những tấn công đã biết.

Yêu cầu phải cập nhật liên tục cơ sở dữ liệu signature

Việc triển khai và cập nhật signature khó và tốn thời gian.

4.2.2 Behavioral Analysis

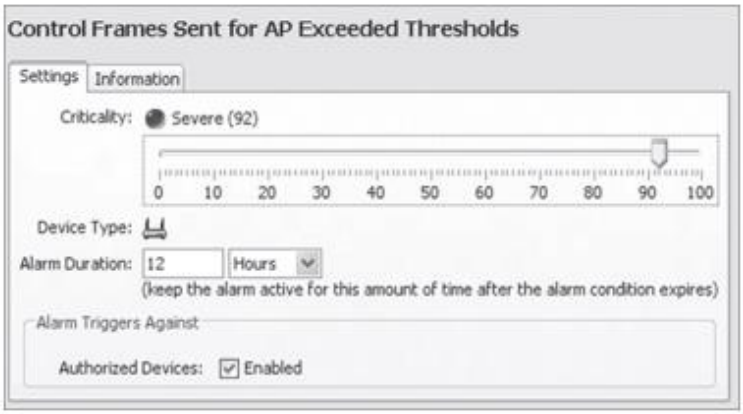
Behavioral Analysis (hoặc profile-based) hoạt động dựa trên việc:

• Tạo ra một profile cơ sở đại diện cho các hành vi bình thường/dự kiến trong mạng.

• Dựa trên đó, bất kỳ hoạt động mạng đang xem xét nào có sai khác so với profile này đều bị xem là bất thường.

○ Profiles đại diện cho hoạt động mạng bình thường hầu hết được tạo ra thông qua phân tích lịch sử lưu lượng mạng (qua các hàm thống kê, máy học, clustering, fuzzy logic, heuristics…)

• Ví dụ: Hoạt động web thường chiếm khoảng 13% băng thông mạng tại cổng Internet trong giờ hành chính của 1 doanh nghiệp.



Hình 2. 9 Behavior thresholds

Ưu điểm:

Phát hiện được cả các hành vi bất thường đã biết và chưa biết, không cần phải có hiểu biết trước.

Phát hiện được các tấn công mới (về sau có thể sử dụng trên các

signature-based IDS).

Nhược điểm:

Tỷ lệ false positives cao (phát hiện nhầm hành vi bình thường là tấn công).

Ít hiệu quả quả trong các môi trường mạng động, thay đổi nhiều.

Yêu cầu thời gian và tài nguyên để xây dựng được profile đại diện cho mạng.

4.2.3 Protocol Analysis

Sử dụng phân tích giao thức để phân tích thông tin lớp MAC trong khung 802.11. Nó cũng có thể được sử dụng để phân tích thông tin Lớp 3–7 của khung dữ liệu 802.11 nhưng với điều kiện dữ liệu không được mã hóa

Các thông tin có thể phân tích được từ data frame:

+ Layer 2 MAC header, frame body, a trailer, which is a 32-bit CRC known as the *frame check sequence (FCS)*

+ MAC Service Data Unit (MSDU),

Các cuộc tấn công có thể được phát hiện tại lớp 2 bằng cách đọc header và trailer của tất cả các frame bắt được bằng bộ phân tích giao thức phân tán

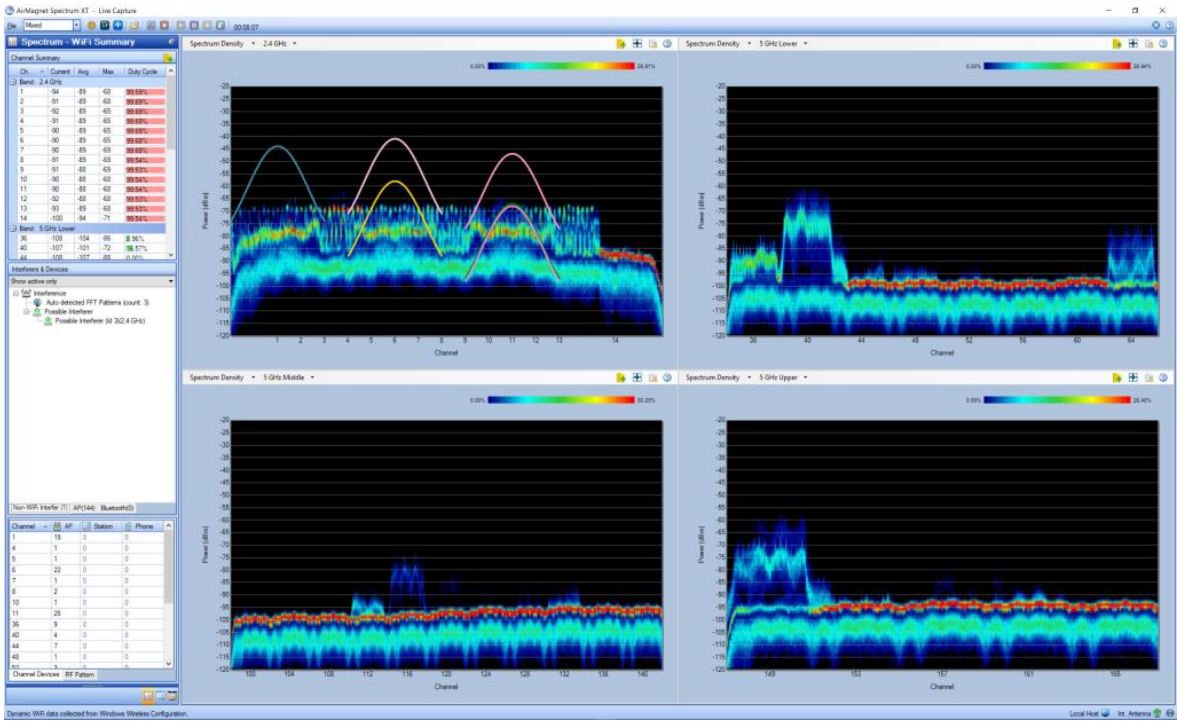
4.2.4 Spectrum Analysis

Là quá trình giám sát và phân tích tần số của môi trường không dây để phát hiện các hoạt động không mong muốn hoặc đe dọa bảo mật. Quá trình này bao gồm:

- *Giám Sát Tần Số*
- *Phát Hiện Tín Hiệu Nhiễu*
- *Phân Tích Mô Hình Tần Số*
- *Xác Định Các Mối Đe Dọa*
- *Cảnh Báo và Phản Ứng*

Các radio bên trong sensor sẽ giám sát băng tần ISM 2.4GHz và UNII 5GHz. Nhưng vì các radio này chỉ sử dụng trải phổ tuần tự trực tiếp (DSSS) và ghép kênh phân chia tần số trực giao OFDM nên sẽ không phát hiện được dữ liệu dược truyền ở băng tần khác với công nghệ khác.

Sử dụng phân tích chữ ký RF để xác định và phân loại các tác nhân RF gây nhiễu chẳng hạn như Bluetooth, lò vi sóng, máy ảnh không dây, thiết bị gây nhiễu, v.v.



Hình 2. 10 WLAN spectrum analyzer

4.2.5 Forensic Analysis

Các giải pháp WIDS cho doanh nghiệp có thể cung cấp phân tích điều tra cho phép quản trị viên truy xuất lại hành động của bất kỳ thiết bị WLAN nào đến từng phút

Với Forensic Analysis, việc điều tra một sự kiện chỉ mất vài phút thay vì hàng giờ. Quản trị viên có thể tua và xem lại các bản ghi từng phút về kết nối và liên lạc trong mạng WLAN. Ngoài ra quản trị viên cũng có thể dự trữ hàng trăm điểm dữ liệu của mỗi thiết bị và mỗi kết nối thuộc mạng WLAN đang giám sát. Việc lưu trữ này cho phép một tổ chức xem lại lịch sử dữ liệu hàng tháng trên bất kỳ thiết bị nào được uỷ quyền. Lịch sử dữ liệu sẽ gồm hoạt động của channel, đặc điểm signal, hoạt động thiết bị và luồng lưu lượng cũng như các cuộc tấn công đã phát hiện.

4.2.6 Performance Analysis

Performance Analysis được sử dụng để xác định performance baseline, đây là baseline được dùng để thiết lập các tiêu chuẩn hoặc mức độ hiệu suất dự kiến và nó cũng liên

Hình 2. 11 Forensic analysis

quan tới việc xác định mạng WLAN hoạt động như thế nào về mặt hiệu suất.

Việc ngưỡng hiệu suất giảm hoặc tăng quá mức là một cảnh báo cho mối nguy tiềm tàng hoặc là lúc doanh nghiệp nên có các nâng cấp cho cơ sở hạ tầng của mình.

Giám sát hiệu suất cho phép quản trị viên xử lý các sự cố mạng tiềm ẩn trước khi người dùng nhận thấy bất kỳ vấn đề nào về hiệu suất. Ngoài ra giám sát hiệu suất cũng hỗ trợ trong việc lập kế hoạch cho bất kỳ sự mở rộng cần thiết nào trong mạng WLAN. Ví dụ như khi thêm người dùng hoặc thêm thiết bị trong WLAN, nếu quản trị viên biết rõ chức năng của mạng WLAN, biết số lượng AP và station hiện có, cũng như các ứng dụng đang chạy trên chúng thì quản trị viên có thể dự đoán chính xác hơn các tình huống sẽ xảy ra dựa trên việc giám sát hiệu suất trước đây.

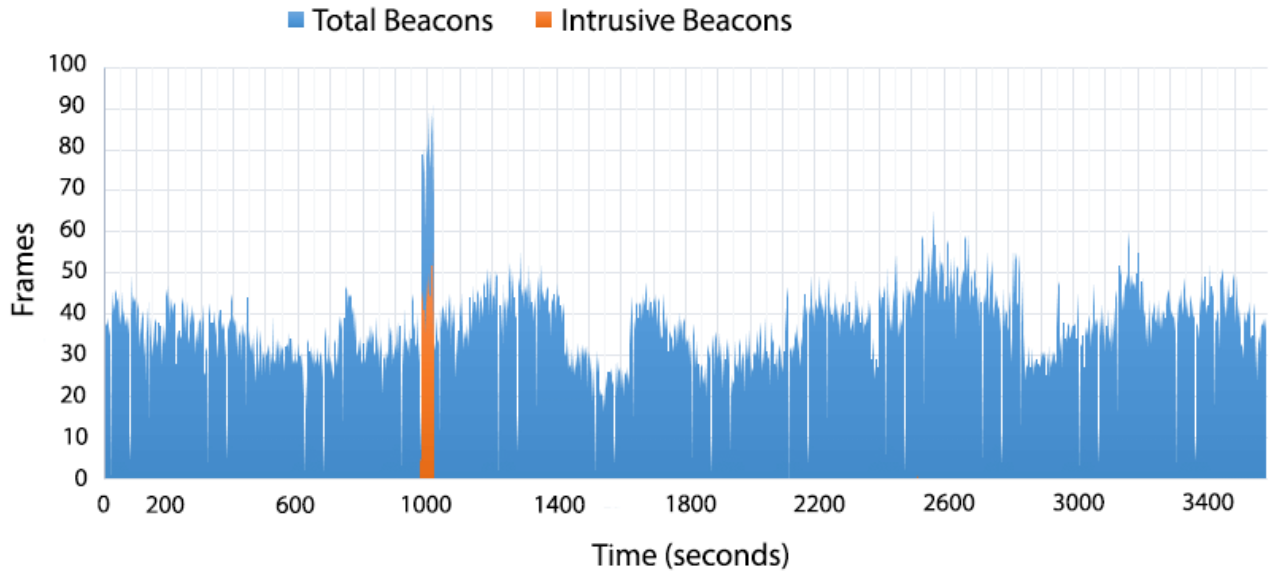
Chương 3: MỘT SỐ CUỘC TẤN CÔNG TRONG MẠNG WLAN

1. Beacon flood attack

Beacon flooding WIFI Attack là kiểu tấn công Spam mạng WIFI ảo. Khiến cho người dùng gặp khó khăn trong việc kết nối và sử dụng mạng WIFI.

1.1 Tổng quan

Khác với kiểu tấn công Crack mật khẩu WIFI bằng Aircrack-ng, kỹ thuật này sẽ đưa người dùng lạc vào mê hồn trận của WIFI. Nếu quan sát tổng thể toàn bộ hệ thống mạng WIFI, số lượng Frame Beacon được phát ra trong một khoảng thời gian ở thời điểm không bị tấn công sẽ rất đều và ổn định. Khi Beacon Flooding diễn ra số lượng Frame Beacon sẽ tăng vọt, bao gồm cả các tín Beacon giả mạo (Intrusive Beacons)



Hình 3. 1 Thống kê lượng Frame Beacon

Kỹ thuật này cần thực hiện theo 2 bước, đây cũng là cách thức hoạt động của kỹ thuật tấn công này.

Bước 1: Tạo SSID ảo

Trong mỗi gói tin beacon, SSID (tên mạng) có thể được đặt là duy nhất hoặc sao chép tên của các mạng xung quanh. Điều này tạo ra nhiều mạng WiFi "ảo" trong danh sách tìm kiếm của các thiết bị đang tìm kiếm mạng để kết nối.

Bước 2: Gửi Gói Tin Beacon Giả Mạo

Kẻ tấn công sử dụng card WIFI để gửi hàng loạt gói tin beacon giả mạo. Mỗi gói tin beacon này giả mạo một điểm truy cập (AP) không tồn tại hoặc sao chép thông tin của một AP đã có.

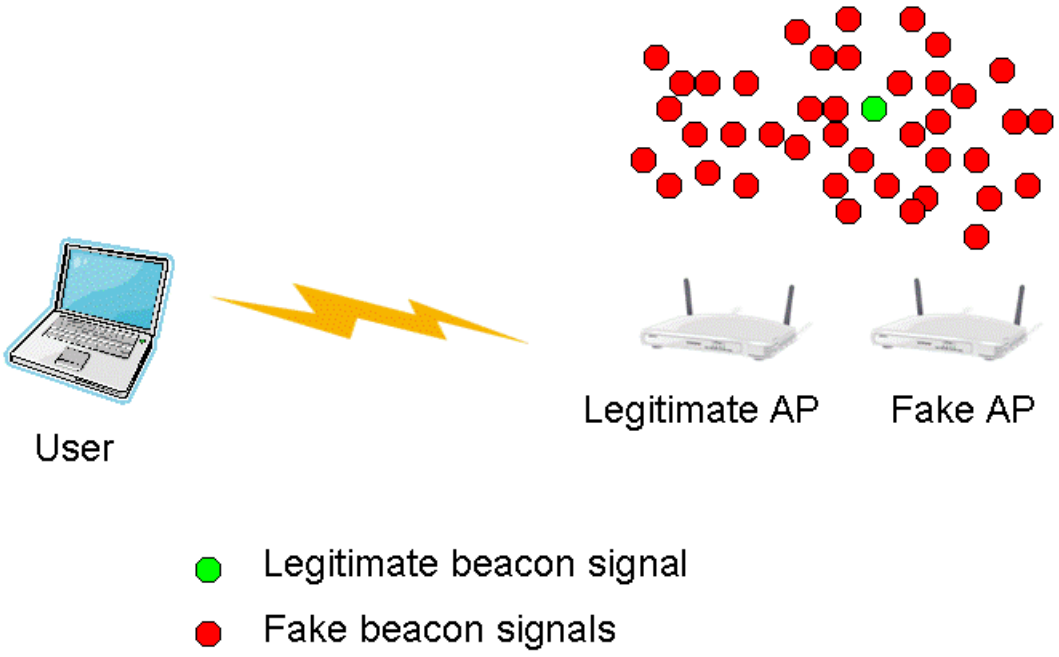
1.2 Mục đích của Beacon Flood

+ Gây Nhiễu và Làm Rối

Việc gửi số lượng lớn các gói tin beacon có thể làm rối loạn không gian sóng WIFI, khiến các thiết bị trong khu vực khó có thể xác định và kết nối với một điểm truy cập thực sự. Điều này gây khó khăn cho người dùng trong việc tìm kiếm và kết nối với mạng WiFi ban đầu

+ Làm Chậm và Làm Quá Tải Hệ Thống

Các AP thực sự có thể bị ảnh hưởng bởi tín hiệu nhiễu, dẫn đến giảm hiệu suất và độ ổn định của mạng. Trong một số trường hợp, điều này cũng có thể khiến AP bị quá tải và cần phải khởi động lại.



Hình 3. 2 Beacon Flood

2. Evil Twins attack

Rogue Access Points là mạng WIFI giả mạo (clone) có các thông số giống hệt một WIFI mục tiêu. Rogue Access Points do Hacker tạo ra để lừa người dùng kết nối vào, sau đó thực hiện đánh cắp mật khẩu hoặc các thông tin cá nhân khác.

2.1 Tổng quan

Khi một thiết bị đã từng kết nối vào mạng WiFi trước đây, nó sẽ lưu thông tin của mạng đó, bao gồm tên SSID (Service Set Identifier) và mật khẩu. Lần sau khi thiết bị này phát hiện ra một mạng có cùng SSID, nó có khả năng sẽ tự động kết nối lại với mạng đó, dựa trên một số tiêu chí như cường độ tín hiệu và chất lượng kết nối.

Nếu có nhiều điểm truy cập trùng tên mạng SSID, thiết bị sẽ thường kết nối với Access Point nào có công suất phát mạnh nhất, điểm phát sóng nào gần với họ nhất. Điều này là do thiết bị sẽ tìm kiếm tín hiệu tốt nhất để đảm bảo kết nối ổn định và hiệu suất cao nhất có thể.

Tuy nhiên, điều này cũng là một rủi ro bảo mật. Hacker sẽ tạo một Rogue AP với cùng SSID như mạng WIFI hiện tại. Có thể họ sẽ sử dụng một thiết bị phát sóng để tạo ra cường độ tín hiệu mạnh hơn, hoặc Hacker sẽ đứng gần bạn.

Nếu người dùng kết nối với Rogue AP và tin rằng đó là AP thật mà không hay biết sự thật là kẻ tấn công đang chặn tất cả lưu lượng giữa người dùng và máy chủ, đồng thời đánh cắp dữ liệu cá nhân mà không để lại dấu vết gì thì hậu quả của việc này đó là thông tin người dùng sẽ bị đánh cắp nhằm phục vụ hành vi trộm cắp danh tính hoặc tổn thất tài chính.

Dễ hình dung hơn, Evil Twin là một sự gian lận, trong đó kẻ tấn công thiết lập mạng WiFi giả trông giống như một điểm truy cập hợp pháp để đánh lừa nạn nhân truy cập. Nạn nhân không hay biết gì mà đăng nhập vào những tài khoản cá nhân, những thứ này sẽ được gửi thẳng đến kẻ tấn công và khi sở hữu chúng kẻ tấn công có thể thay nạn nhân thực hiện các hành vi tiếp theo như thực hiện một giao dịch ngân hàng chẳng hạn.

2.2 Mục tiêu tấn công

+ Đánh lừa nạn nhân truy cập Rogue AP

+ Đánh cắp dữ liệu hoặc thiết lập phần mềm độc hại. Người dùng cuối là mục tiêu chính cho hình thức tấn công này.

3. Authentication DoS

Authentication DoS Attack là một trong những kỹ thuật WIFI DoS Attack làm cho các thiết bị phát sóng WIFI không đủ tài nguyên phục vụ người dùng, có thể dẫn tới việc treo thiết bị.

3.1 Tổng quan

Authentication DoS Attack là kỹ thuật giả mạo rất nhiều Client muốn thực hiện xác thực với Access Point. Khiến các bộ phát WIFI tiêu tốn tài nguyên.

Mỗi một thiết bị muốn kết nối vào mạng, nó sẽ làm việc với Access Point (cục phát WIFI) để thực hiện kiểm tra, tính toán. Mỗi lần xác thực như này sẽ tiêu tốn một tài nguyên bộ nhớ, CPU nhất định của Access Point.

Không giống như máy tính hay các máy chủ, Access Point ở các hộ gia đình hoặc doanh nghiệp nhỏthường sở hữu các cấu hình yếu, số lượng RAM và CPU giới hạn. Đấy cũng là lý do một số doanh nghiệp, gia đình nếu có lượng người dùng quá lớn, Access Point sẽ bị nóng và chậm chạp đi.

Lợi dụng điểm yếu về cấu hình, các Hacker sẽ thực hiện giả mạo đang có rất rất nhiều Client đang muốn xác thực với Access Point.

3.2 Mục tiêu tấn công

+ Làm cho thiết bị AP thật bị treo hoặc khởi động lại.

+ Làm ngập lụt không gian sóng với các tín hiệu SSID giả, khiến người dùng không thể tìm thấy hoặc kết nối với mạng WiFi hợp pháp.

Chương 4.KIẾN TRÚC HỆ THỐNG WIDS XÂY DỰNG

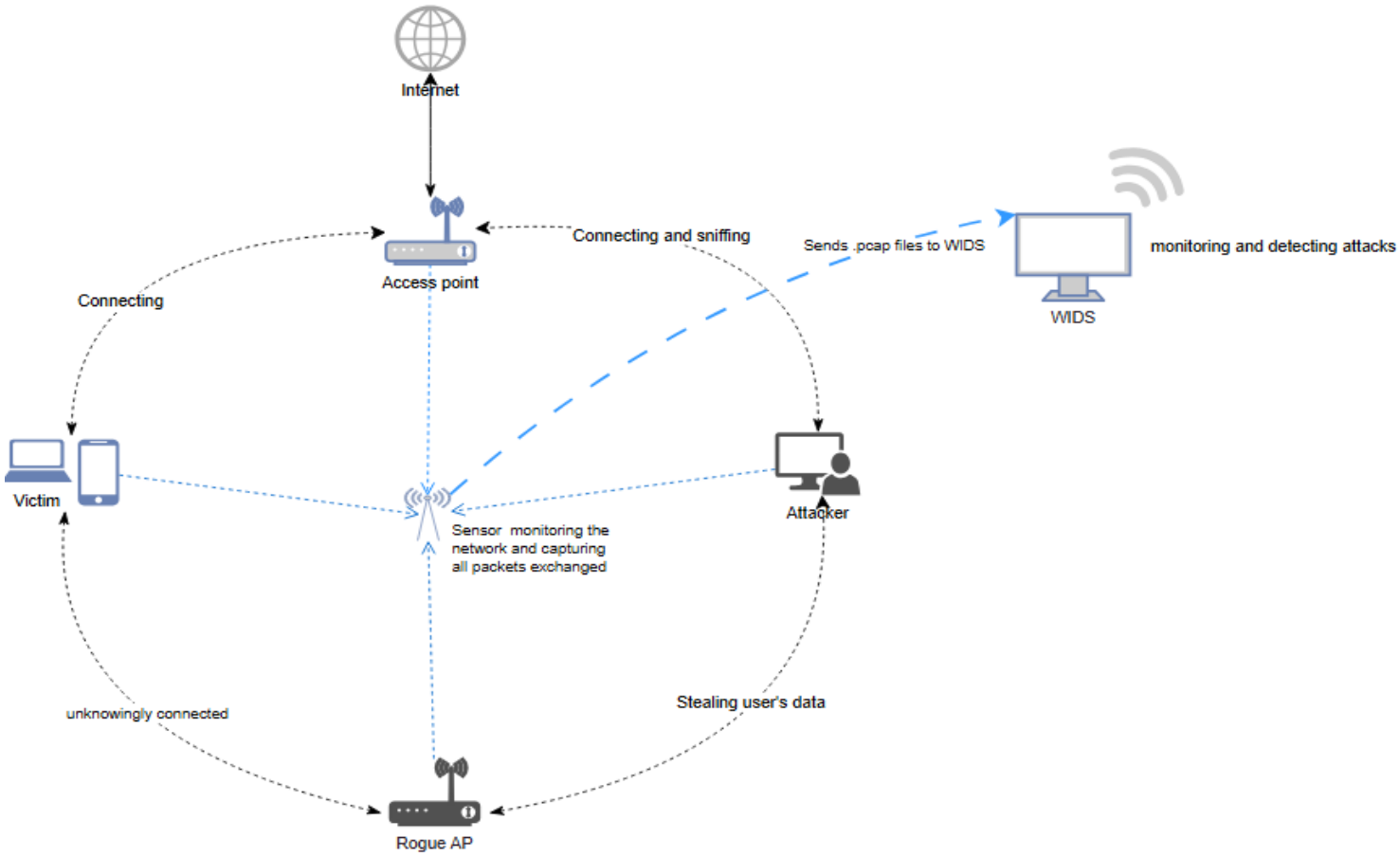
1. Giới thiệu về WIDS được triển khai

Nhóm sử dụng phần mềm WIDS mã nguồn mở tại (1) để triển khai hệ thống WIDS và thực hiện một số chỉnh sửa để chạy trên Python3 và môi trường Kali Linux

Hệ thống WIDS này sẽ sniff các lưu lượng truy cập trong môi trường mạng không dây để phát hiện các tín hiệu đáng ngờ như các gói tấn công WEP/WPA/WPS. Cụ thể hệ thống WIDS sẽ hoạt động như sau:

- Phát hiện các gói tin deauthentication được gửi hàng loạt đến Client hoặc Access point với số lượng không hợp lý => cho thấy có thể xảy ra cuộc tấn công WPA trong quá trình handshake.
- Phát hiện nhiều gói tin được gửi liên tục đến Access point bằng địa chỉ MAC broadcast => cho thấy khả năng bị tấn công WEP
- Phát hiện lưu lượng giao tiếp không hợp lý giữa Client và AP (có sử dụng xác thực EAP) trong môi trường không dây => cho thấy khả năng bị tấn công bruteforce WPS bằng Reaver / WPSCrack
- Phát hiện sự thay đổi AP mà Client kết nối tới => có khả năng Client kết nối với Rogue AP mà không biết gì, ví dụ như tấn công evil twins.

2. Mô hình triển khai



Hình 4. 1 Mô hình triển khai

3. Môi trường thực nghiệm

Các thiết bị gồm có:

+ 1 Access point để truy cập Internet

+ 1 Rogue AP để giả mạo AP thật

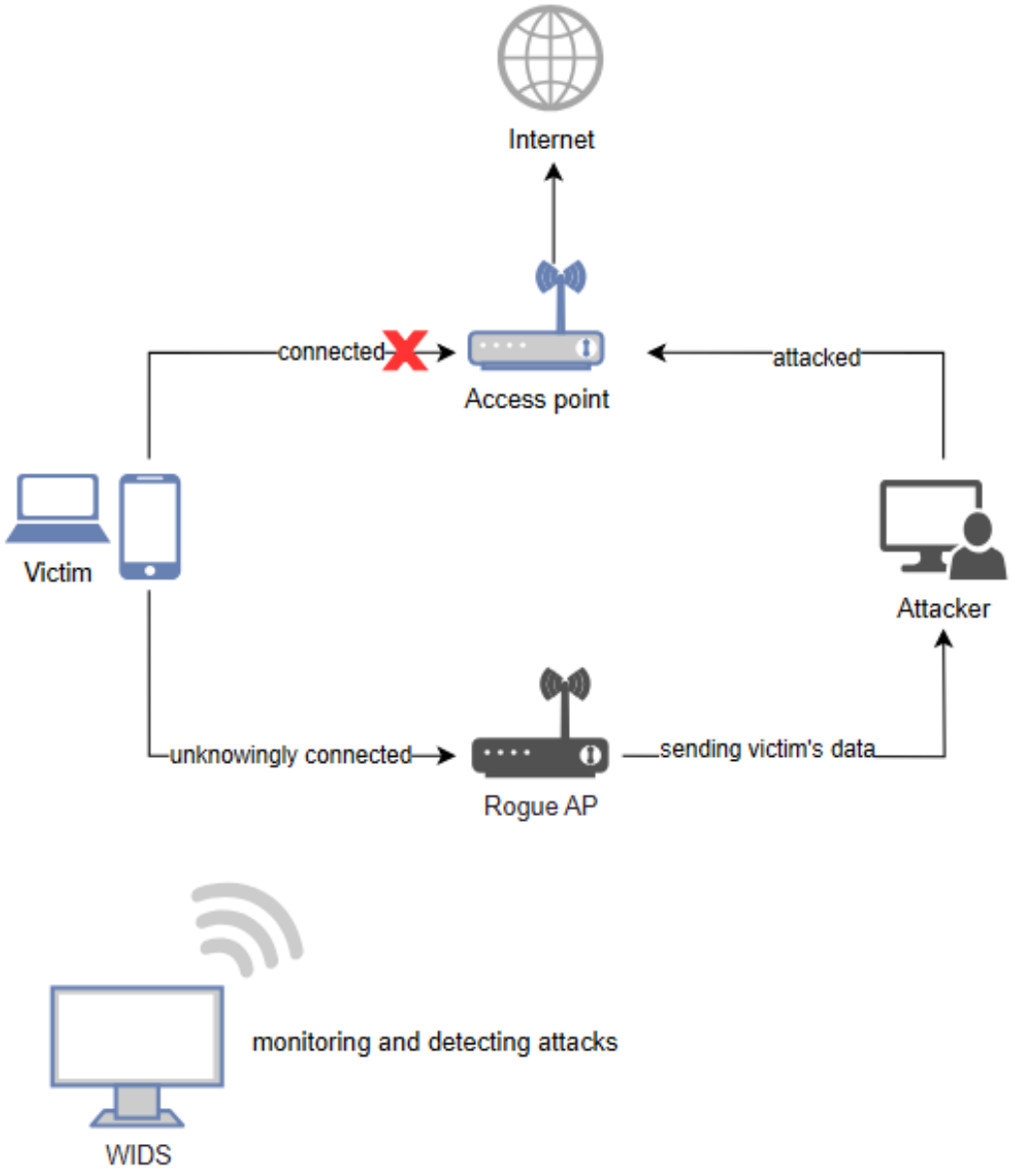
+ 1 máy Kali linux đóng vai trò WIDS giám sát các lưu lượng truy cập trong môi trường mạng không dây

+ 1 máy ảo đóng vai trò attacker để thực hiện tấn công

+1 thiết bị có kết nối wifi dùng làm sensor

Chương 5. KỊCH BẢN TRIỂN KHAI

1. Evil Twins attack



Hình 5. 1 Evil Twins attack

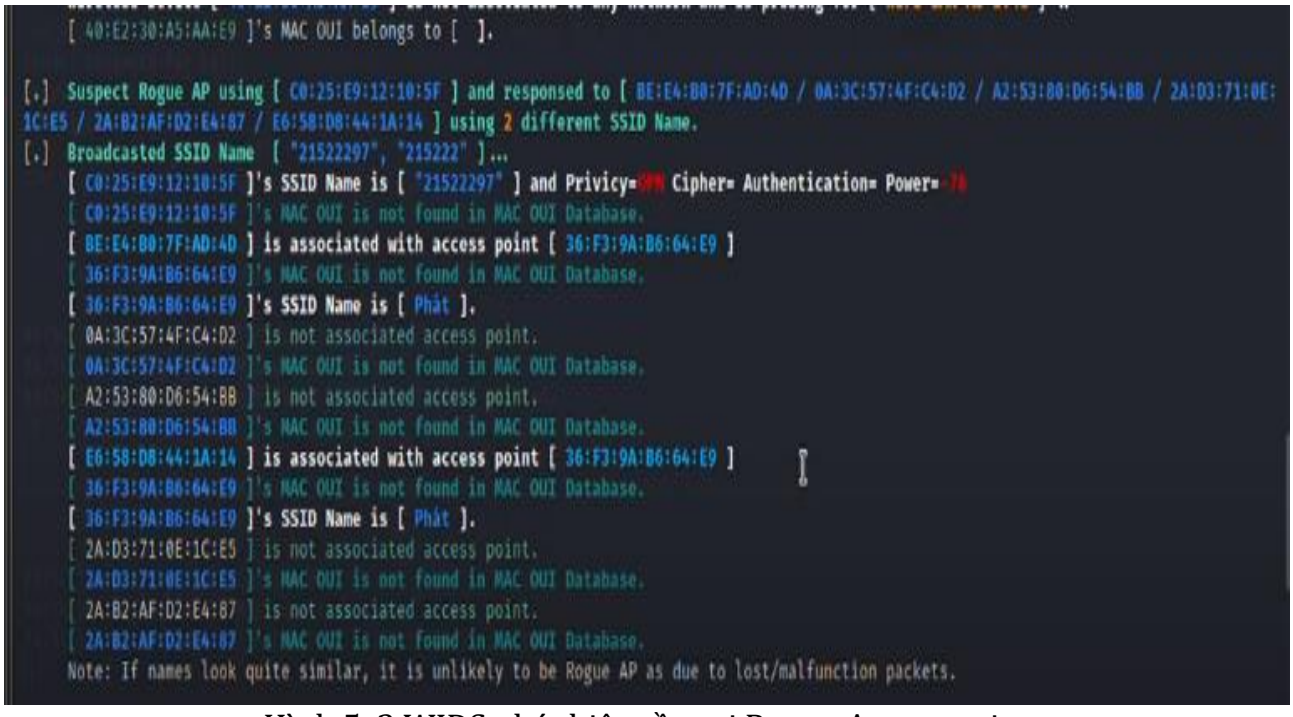
Sau khi tạo 1 AP giả mạo, attacker sẽ tấn công AP thật để ngắt kết nối giữa Client với AP. Tiếp đến chờ hoặc chủ động khiến Client kết nối tới Rogue AP. Cuối cùng là thu thập thông tin cũa nạn nhân thông qua Rogue AP.

+WIDS sẽ phân biệt Rogue AP và Real AP bằng cách xác định xem có 1 BSSID nào đó sở hữu 2 SSID hay không và đưa ra cảnh báo.

+Tại máy Attacker thực hiện tạo access point giả:

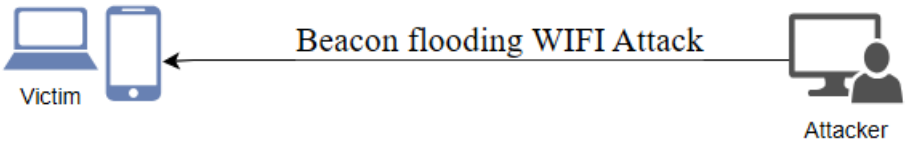
Hình 5. 2 Tạo Fake Access point

+Sau 1 khoảng thời gian, máy WIDS xuất ra thông báo việc phát hiện thấy Rogue access point:



Hình 5. 3 WIDS phát hiện tồn tại Rogue Access point

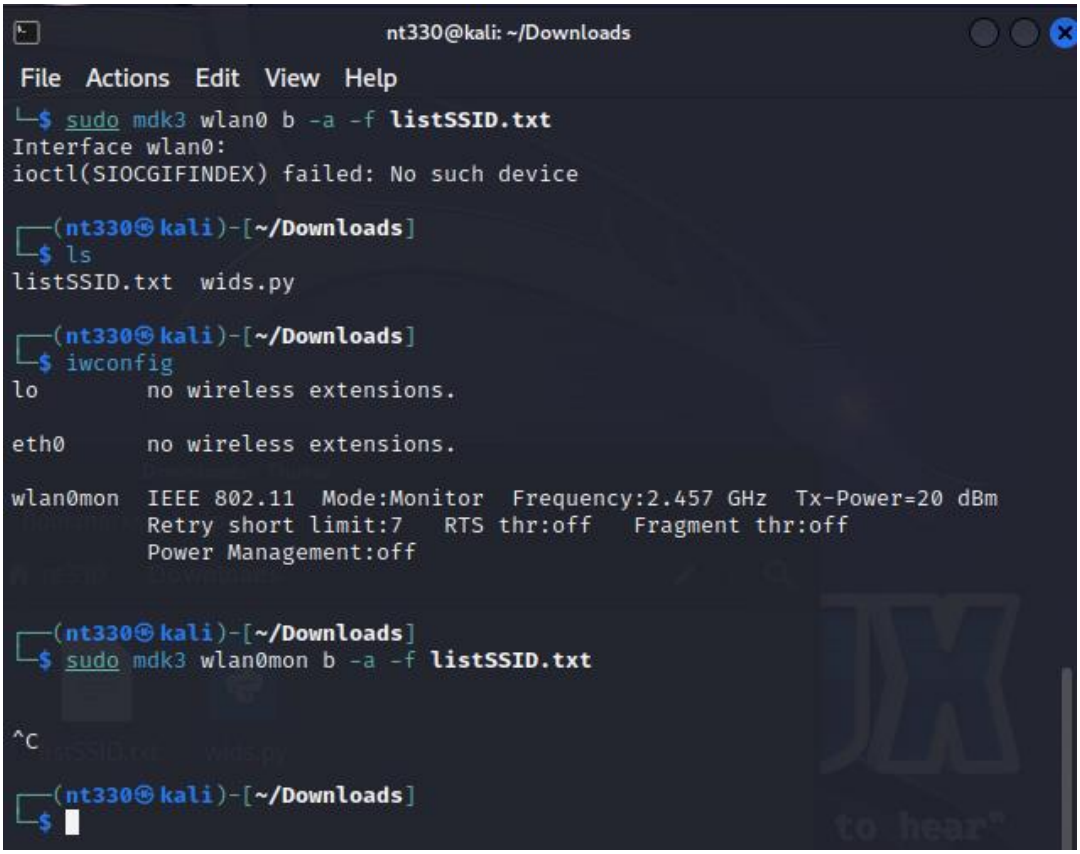
2. Beacon flood attack



Hình 5. 4 Beacon Flood attack

Sử dụng mkd3 để khởi tạo cuộc tấn công Beacon flooding WIFI Attack. Sau đó attaker sẽ gửi hàng loạt gói tin Beacon ra môi trường mạng không dây

- Máy attacker thực hiện tạo ra hàng loạt gói Beacon giả rồi phát tán lên môi trường mạng wifi

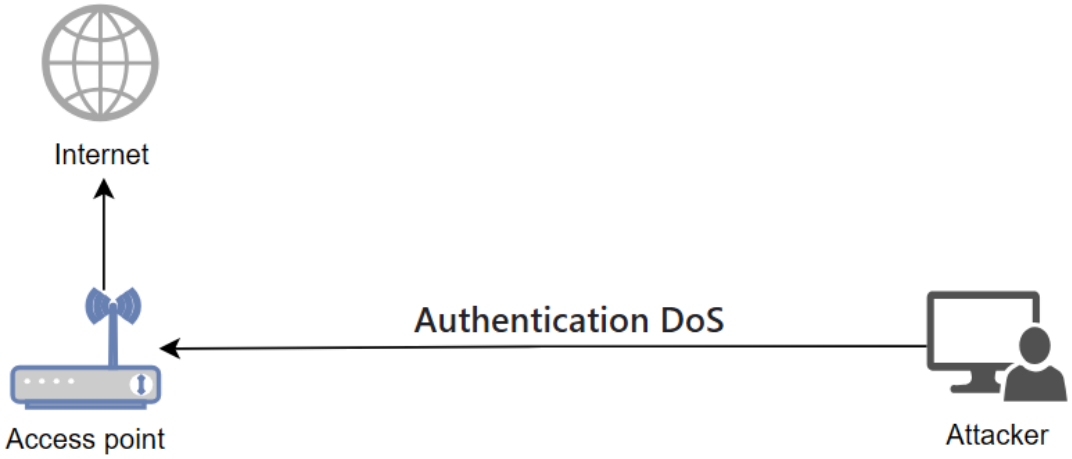


Hình 5. 5 Thực hiện tấn công Beacon Flood

- Máy WIDS phát hiện được rất nhiều ESSID giống nhau nhưng không có hoạt động cũng như không có client nào

Hình 5. 6 WIDS phát hiện Beacon Flood

3 Authentication DoS



Hình 5. 7 Authentication DoS attack

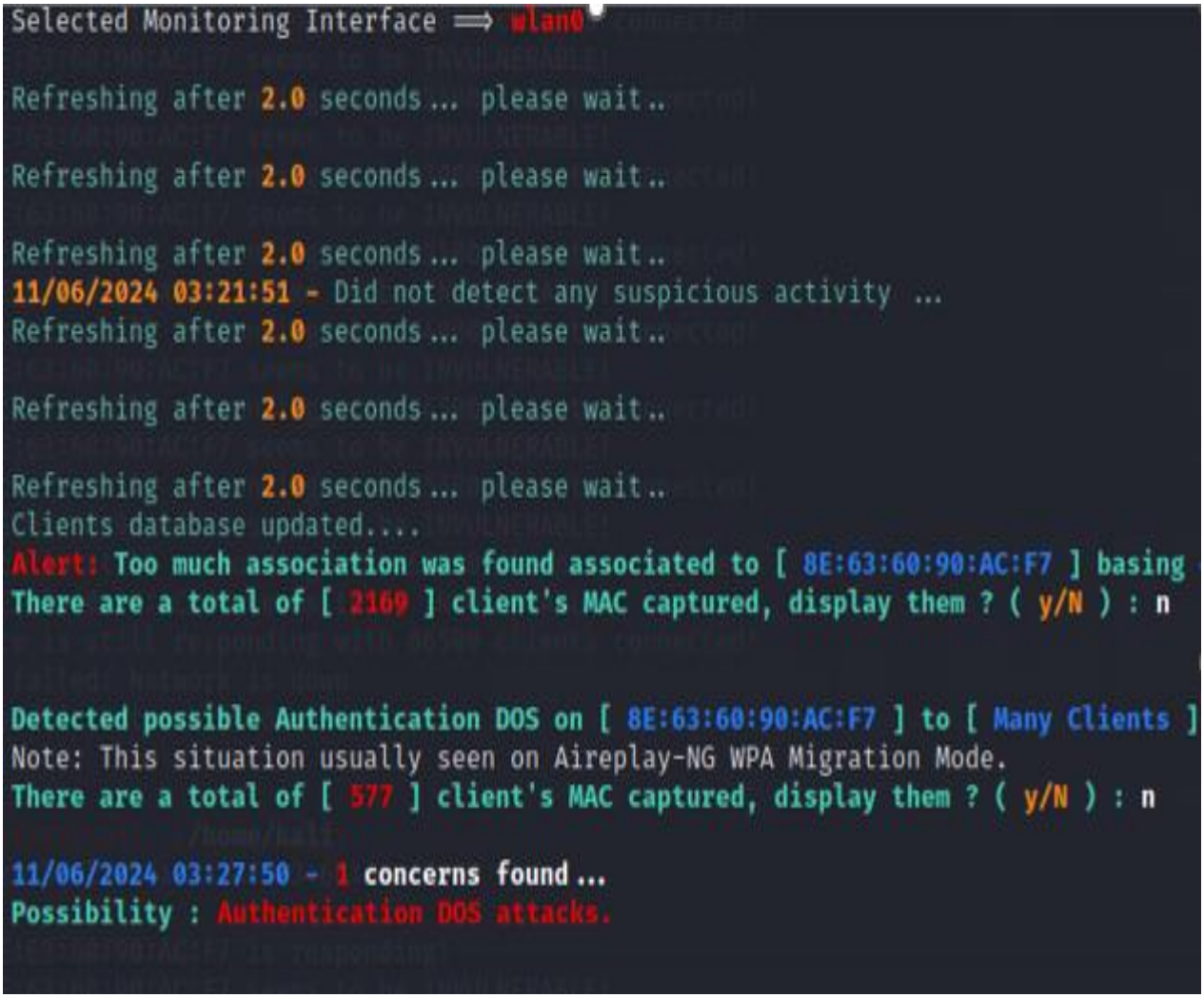
Sử dụng công cụ mdk3 để thực hiện Authentication DoS Attack. Sau đó attacker sẽ gửi một lượng lớn gói tin authentication đến AP

+Máy attacker thực hiện tấn công Authentication DoS

```
┌──(root㉿kali)-[/home/kali]
└─# mdk3 wlan0 a -a 8E:63:60:90:AC:F7  -m
AP 8E:63:60:90:AC:F7 is responding!
AP 8E:63:60:90:AC:F7 seems to be INVULNERABLE!
Device is still responding with   500 clients connected!
AP 8E:63:60:90:AC:F7 seems to be INVULNERABLE!
Device is still responding with  1000 clients connected!
AP 8E:63:60:90:AC:F7 seems to be INVULNERABLE!
Device is still responding with  1500 clients connected!
```

Hình 5. 8 Thực hiện tấn công Authentication DoS

+Máy WIDS phát hiện và đưa ra cảnh báo về Authentication DoS



Hình 5. 9 WIDS phát hiện Authentication DoS

Chương 6: KẾT LUẬN

Trong đồ án này, chúng em đã nghiên cứu và phát triển một hệ thống phát hiện xâm nhập không dây (WIDS) nhằm tăng cường bảo mật cho mạng không dây. Mục tiêu chính của đồ án là xây dựng một hệ thống có khả năng phát hiện các cuộc tấn công phổ biến trong mạng không dây và đưa ra các cảnh báo kịp thời.

Kết quả thực nghiệm cho hệ thống WIDS của chúng em có thể phát hiện hiệu quả các loại tấn công như tấn công giả mạo (spoofing), tấn công từ chối dịch vụ (DoS),… Hệ thống sử dụng các phương pháp phát hiện dựa trên chữ ký và quy tắc để phân tích và nhận diện các hoạt động bất thường trong mạng.

Trong tương lai chúng em hi vọng sẽ có thể cải thiện được hiệu suất hoạt động của công cụ WIDS bằng cách tối ưu hóa các quy tắc phát hiện và mở rộng khả năng phát hiện đối với các loại tấn công mới. Ngoài ra, chúng em cũng muốn tích hợp WIDS với các hệ thống bảo mật khác để tạo ra một giải pháp bảo mật toàn diện hơn cho mạng không dây.

THAM KHẢO

1. CWSP Certified Wireless Security Professional Study Guide: Exam CWSP-205

2. Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (idps). NIST special publication, 800(2007), 94.

3. https://github.com/SYWorks/wireless-ids

4. https://www.aircrack-ng.org/doku.php?id=aireplay-ng

5. https://en.kali.tools/?p=34 (mdk3 instruction)

6. https://forum.vnpro.org/forum/công-nghệ-mạng/wireless-mobility/28588-thiết-kế-hệ-thống-phát-hiện-xâm-nhập-widspro?view=stream