BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP. HCM

KHOA CÔNG NGHỆ THÔNG TIN

****

BÁO CÁO MÔN HỌC

WIRELESS NETWORK INSTRUSION DETECTION SYSTEM

Môn học: An toàn mạng không dây và di động

MÃ SỐ LỚP HỌC PHẦN: WISE432380_05

GVHD: ThS. Đinh Công Đoan

NHÓM THỰC HIỆN: 12

HỌC KỲ: I

NĂM HỌC: 2025 - 2026

TP. HCM, tháng 12 năm 2025

SINH VIÊN THỰC HIỆN ĐỀ TÀI

Họ và tên	MSSV
Dương Đình Ngọc Khang	23162036
Đỗ Đoàn Duy Hoàng	23162025
Cao Đăng Huy	23162028

LỜI CẢM ƠN

Kính gửi thầy Đinh Công Đoan,

Chúng em xin gửi lời cảm ơn chân thành đến thầy đã tận tình hướng dẫn và hỗ trợ nhóm em trong suốt quá trình thực hiện đồ án cuối kỳ. Những kiến thức quý báu và sự tận tâm của thầy đã giúp chúng em vượt qua những khó khăn và hoàn thiện đồ án của mình.

Không chỉ vậy, sự động viên và khích lệ từ thầy đã giúp chúng em tự tin hơn, sẵn sàng đối mặt với thử thách và phát triển bản thân. Chúng em rất trân trọng những góp ý, chỉ bảo của thầy, điều đó không chỉ giúp nhóm em phát triển kỹ năng chuyên môn mà còn nâng cao khả năng tư duy sáng tạo. Chúng em hy vọng sẽ có nhiều cơ hội học hỏi từ thầy hơn nữa trong tương lai.

Một lần nữa, chúng em xin chân thành cảm ơn thầy!

Trân trọng.

MỤC LỤC

PHẦN MỞ ĐẦU

1.1. Lý do chọn đề tài

Trong kỷ nguyên chuyển đổi số, mạng không dây theo chuẩn IEEE 802.11 đã trở thành hạ tầng kết nối không thể thiếu tại các cơ quan, doanh nghiệp và hộ gia đình. Tuy nhiên, do đặc tính sử dụng môi trường truyền dẫn là sóng vô tuyến, mạng không dây chứa đựng nhiều rủi ro bảo mật nghiêm trọng hơn so với mạng có dây truyền thống. Kẻ tấn công có thể dễ dàng nghe lén, chèn gói tin hoặc giả mạo trạm phát sóng mà không cần tiếp cận vật lý vào hạ tầng mạng.

Các kỹ thuật tấn công như Từ chối dịch vụ, giả mạo điểm truy cập hay thu thập thông tin ngày càng trở nên tinh vi và dễ thực hiện với các công cụ mã nguồn mở. Trong khi đó, các giải pháp giám sát an ninh mạng truyền thống (IDS/IPS) thường tập trung vào lớp mạng và bỏ qua các mối đe dọa tại lớp liên kết dữ liệu của sóng vô tuyến.

Xuất phát từ thực tế đó, việc nghiên cứu và triển khai một hệ thống phát hiện xâm nhập mạng không dây (Wireless Intrusion Detection System - WIDS) là vô cùng cấp thiết. Đề tài **"Nghiên cứu và xây dựng hệ thống phát hiện xâm nhập mạng không dây sử dụng Kismet"** được lựa chọn nhằm mục đích tìm hiểu sâu về các nguy cơ an ninh mạng Wifi, đồng thời xây dựng một giải pháp giám sát chi phí thấp nhưng hiệu quả, giúp phát hiện sớm các dấu hiệu tấn công để có biện pháp ngăn chặn kịp thời.

1.2. Đối tượng nghiên cứu

Để giải quyết vấn đề nêu trên, đề tài tập trung vào các đối tượng nghiên cứu chính sau:

1. **Giao thức mạng không dây:** Cấu trúc khung tin của chuẩn IEEE 802.11, đặc biệt là các khung quản lý thường bị lợi dụng để tấn công.
2. **Các kỹ thuật tấn công WLAN:** Cơ chế hoạt động của các hình thức tấn công phổ biến như: Do thám, Tấn công ngắt kết nối, và Giả mạo điểm truy cập.
3. **Hệ thống phòng thủ:** Công cụ phát hiện xâm nhập mạng không dây Kismet và các luật cảnh báo tương ứng.

1.3. Phương pháp nghiên cứu

Đề tài sử dụng kết hợp hai phương pháp nghiên cứu chính:

- **Phương pháp nghiên cứu lý thuyết:** Thu thập và phân tích tài liệu về chuẩn IEEE 802.11 và các chuẩn bảo mật (WPA2, WPA3). Nghiên cứu cơ chế hoạt động của

các công cụ tấn công và công cụ phòng thủ. Phân tích các dấu hiệu nhận biết của từng loại tấn công.

- **Phương pháp nghiên cứu thực nghiệm:** Xây dựng mô hình phòng lab gồm: Máy tấn công, Máy phòng thủ, Router Wifi mục tiêu và Thiết bị người dùng. Thực hiện mô phỏng các kịch bản tấn công thực tế. Cấu hình hệ thống WIDS để giám sát, bắt gói tin và đưa ra cảnh báo. Phân tích nhật ký và cảnh báo để đánh giá độ chính xác của hệ thống.

1.4. Nội dung nghiên cứu

Nội dung của đồ án được triển khai qua các nhiệm vụ cụ thể:

1. Tổng quan về an ninh mạng không dây và các lỗ hổng của giao thức 802.11.
2. Phân tích chi tiết kỹ thuật của các cuộc tấn công: Reconnaissance, DoS, và Impersonation.
3. Cài đặt và cấu hình hệ thống WIDS sử dụng Kismet trên nền tảng Linux.
4. Xây dựng các tập luật để phát hiện các hành vi bất thường.
5. Thực nghiệm tấn công kiểm thử và đánh giá kết quả phát hiện của hệ thống thông qua các chỉ số cảnh báo.

1.5. Phạm vi nghiên cứu

Do giới hạn về thời gian và thiết bị phần cứng, đề tài tập trung vào phạm vi sau:

- **Môi trường mạng:** Mạng WLAN chuẩn 802.11n/ac hoạt động ở dải tần 2.4GHz.
- **Công cụ:** Sử dụng bộ công cụ mã nguồn mở (Kali Linux, Kismet, Aircrack-ng) trên phần cứng máy tính thông dụng.
- **Giới hạn chức năng:** Hệ thống tập trung vào chức năng phát hiện và cảnh báo, chưa bao gồm chức năng tự động ngăn chặn hoặc phản công.
- **Kịch bản thử nghiệm:** Tập trung vào 3 nhóm tấn công chính có mức độ rủi ro cao: Do thám chủ động, từ chối dịch vụ và giả mạo Access Point.

1.6. Các tài liệu có liên quan

Hiện nay, lĩnh vực phát hiện xâm nhập mạng không dây đã có nhiều công trình nghiên cứu trong và ngoài nước:

- Trên thế giới, các nghiên cứu thường tập trung vào việc tích hợp WIDS vào các thiết bị phần cứng chuyên dụng (Cisco, Aruba) hoặc sử dụng AI/Machine Learning để phát hiện bất thường trong lưu lượng.
- Các dự án mã nguồn mở như Snort hay Suricata rất mạnh về IDS truyền thống (lớp mạng), nhưng hạn chế khả năng giám sát lớp vật lý của Wifi (Layer 1/Layer 2).
- Đề tài này kế thừa các nghiên cứu về kỹ thuật phân tích gói tin 802.11, nhưng tập trung vào việc tối ưu hóa cấu hình công cụ Kismet – một công cụ chuyên dụng cho Wifi – để xây dựng một giải pháp WIDS chi phí thấp, phù hợp cho nhu cầu giám sát của cá nhân hoặc doanh nghiệp nhỏ, đồng thời làm rõ quy trình từ tấn công đến phát hiện một cách trực quan.

PHẦN NỘI DUNG

CHƯƠNG 1: CƠ SỞ LÝ THUYẾT

1.1. Tổng quan về IEEE 802.11

IEEE 802.11 là tập hợp các chuẩn kỹ thuật cho hệ thống mạng cục bộ không dây (WLAN), hoạt động chủ yếu ở các dải tần 2.4GHz, 5GHz và 6GHz. Hiểu rõ kiến trúc và cơ chế hoạt động của 802.11 là nền tảng cốt lõi để xây dựng hệ thống phát hiện xâm nhập.

1.1.1. Kiến trúc mạng WLAN

Mạng WLAN thường được triển khai theo hai mô hình chính:

- **Mô hình cơ sở:** Đây là mô hình phổ biến nhất. Mô hình bao gồm các trạm thu phát gốc đóng vai trò trung tâm điều phối, kết nối các thiết bị khách vào mạng có dây. Tập hợp một AP và các STA kết nối với nó được gọi là Tập dịch vụ cơ sở (Basic Service Set - BSS).
- **Mô hình mạng ngang hàng:** Các thiết bị kết nối trực tiếp với nhau không thông qua Access Point. Tập hợp này được gọi là Tập dịch vụ cơ sở độc lập (IBSS).

1.1.2. Cấu trúc khung tin (802.11 Frames)

Khác với mạng có dây Ethernet (802.3), chuẩn 802.11 bổ sung nhiều loại khung tin để quản lý môi trường truyền dẫn vô tuyến phức tạp. Hệ thống WIDS tập trung phân tích các loại khung tin sau để phát hiện tấn công:

Management Frames (Khung quản lý): Chịu trách nhiệm thiết lập và duy trì kết nối. Đây là mục tiêu chính của các cuộc tấn công DoS và giả mạo.

Beacon Frame: Được AP gửi định kỳ để quảng bá sự hiện diện của mạng (chứa SSID, thông tin kênh, mã hóa).

Probe Request/Response: Được thiết bị khách gửi để chủ động tìm kiếm mạng Wifi.

Authentication/Deauthentication: Dùng để yêu cầu xác thực hoặc hủy bỏ xác thực.

Association/Disassociation: Dùng để thiết lập hoặc ngắt kết nối vào mạng.

Control Frames (Khung điều khiển): Hỗ trợ việc truyền dữ liệu tin cậy (ví dụ: RTS/CTS để tránh xung đột, ACK để xác nhận nhận tin).

Data Frames (Khung dữ liệu): Chứa dữ liệu thực tế của người dùng (gói tin IP).

1.1.3. Quy trình kết nối và xác thực

Để truy cập mạng, một thiết bị phải trải qua các bước: Quét -> Xác thực -> Liên kết.

Trong đó, quy trình bắt tay 4 bước là quan trọng nhất trong mạng bảo mật (WPA/WPA2). Quá trình này giúp AP và Client thỏa thuận khóa phiên để mã hóa dữ liệu mà không cần gửi trực tiếp mật khẩu qua không gian truyền dẫn. Các cuộc tấn công như KRACK hoặc Dictionary Attack thường nhắm vào việc bắt giữ gói tin bắt tay này.

1.1.4. Các chuẩn bảo mật mạng không dây

WEP (Wired Equivalent Privacy): Chuẩn bảo mật đời đầu, sử dụng thuật toán RC4. Hiện đã bị phá vỡ hoàn toàn và không còn được khuyến nghị sử dụng.

WPA/WPA2 (Wi-Fi Protected Access):

- WPA2 sử dụng mã hóa AES-CCMP mạnh mẽ hơn. Đây là chuẩn phổ biến nhất hiện nay.
- Tuy nhiên, WPA2 vẫn tồn tại lỗ hổng đối với các cuộc tấn công từ chối dịch vụ (do khung quản lý không được mã hóa) và tấn công từ điển nếu mật khẩu yếu.

WPA3: Chuẩn mới nhất, sử dụng giao thức SAE (Simultaneous Authentication of Equals) để chống lại tấn công từ điển, tăng cường bảo mật cho các mạng mở.

1.2. Các kỹ thuật tấn công mạng không dây

1.2.1. Kỹ thuật Do thám

Trước khi tấn công, hacker cần thu thập thông tin về mục tiêu (BSSID, Kênh, Mã hóa, Số lượng Client).

Quét thụ động: Hacker chuyển card mạng sang chế độ giám sát (Monitor Mode) để nghe lén các gói tin Beacon mà không phát tín hiệu. Kỹ thuật này rất khó bị phát hiện.

Quét chủ động: Hacker gửi các gói *Probe Request* đến địa chỉ Broadcast hoặc một SSID cụ thể. AP sẽ phản hồi bằng *Probe Response*. Kỹ thuật này giúp hacker tìm ra các mạng ẩn nhưng dễ bị WIDS phát hiện.

1.2.2. Tấn công Từ chối dịch vụ (Denial of Service - DoS)

Mục tiêu là làm gián đoạn kết nối của người dùng hợp pháp.

Cơ chế Deauthentication Flood: Trong chuẩn 802.11 truyền thống, khung *Deauthentication* (hủy xác thực) không được mã hóa. Hacker giả mạo địa chỉ MAC của AP, gửi liên tục các gói tin Deauth tới Client.

Tác động: Client bị ngắt kết nối ngay lập tức và cố gắng kết nối lại liên tục, gây tê liệt đường truyền. WIDS phát hiện dựa trên sự gia tăng đột biến của loại khung tin này.

1.2.3. Tấn công Giả mạo (Impersonation & Rogue AP)

Đây là kỹ thuật nguy hiểm nhằm đánh cắp thông tin người dùng thông qua tấn công "Người đứng giữa" (Man-in-the-Middle).

Evil Twin: Hacker dựng một AP giả mạo có cùng tên và thường là cùng địa chỉ MAC với AP thật, phát sóng ở cường độ mạnh hơn để lừa thiết bị nạn nhân kết nối.

Hạ cấp bảo mật: Vì hacker không biết mật khẩu Wifi thật, AP giả mạo thường được cấu hình ở chế độ Open. Người dùng hoặc thiết bị tự động kết nối vào do nhầm lẫn, dẫn đến toàn bộ lưu lượng truy cập đi qua máy hacker.

Phát hiện: WIDS phát hiện dựa trên sự xuất hiện của SSID quen thuộc nhưng có thông số lạ (khác MAC, khác kênh, hoặc mất mã hóa).

1.3. Hệ thống phát hiện xâm nhập

1.3.1. Tổng quan về IDS và WIDS

IDS (Intrusion Detection System): Là hệ thống giám sát lưu lượng mạng nhằm phát hiện các hành vi bất thường hoặc vi phạm chính sách bảo mật.

WIDS (Wireless IDS): Là IDS chuyên dụng cho môi trường không dây. Khác với IDS truyền thống chỉ giám sát lớp mạng (Layer 3), WIDS phải giám sát lớp liên kết dữ liệu (Layer 2) và lớp vật lý (Layer 1) trong không gian sóng vô tuyến để phát hiện các cuộc tấn công đặc thù như Rogue AP hay Deauth Flood.

1.3.2. Các phương pháp phát hiện xâm nhập

Phát hiện dựa trên chữ ký: Hệ thống so sánh các gói tin thu được với cơ sở dữ liệu các mẫu tấn công đã biết. Phương pháp này có độ chính xác cao với các tấn công đã biết nhưng kém hiệu quả với các tấn công mới.

Phát hiện dựa trên bất thường: Hệ thống xây dựng một hồ sơ "bình thường" của mạng (ví dụ: danh sách MAC tin cậy, lưu lượng trung bình). Bất kỳ hành vi nào sai lệch khỏi hồ sơ này (ví dụ: lưu lượng Deauth tăng vọt, xuất hiện MAC lạ phát cùng SSID) đều bị coi là xâm nhập.

1.3.3. Giới thiệu công cụ Kismet

Kismet là công cụ phát hiện mạng không dây, sniffer và WIDS mã nguồn mở phổ biến nhất hiện nay trên nền tảng Linux.

- Kiến trúc: Kismet hoạt động theo mô hình Server/Client, cho phép thu thập dữ liệu từ nhiều nguồn cảm biến khác nhau.
- Chế độ Monitor Mode: Kismet yêu cầu card mạng hoạt động ở chế độ Monitor, cho phép bắt toàn bộ các gói tin 802.11 trong không gian, kể cả các gói tin không gửi đến máy của mình.
- Khả năng phát hiện: Kismet có khả năng giải mã các khung tin quản lý, phát hiện các mạng ẩn, và tích hợp sẵn các luật phát hiện tấn công như: *Fingerprinting* (nhận diện thiết bị), *Spoofing detection* (phát hiện giả mạo), và *DoS detection*. Đây là công cụ chính được sử dụng trong phần thực nghiệm của đề tài.

CHƯƠNG 2: THỰC NGHIỆM VÀ THIẾT KẾ HỆ THỐNG WIDS

2.1. Mô hình hệ thống thử nghiệm

Để đánh giá hiệu quả của giải pháp WIDS dựa trên Kismet, hệ thống thử nghiệm được thiết kế theo mô hình giám sát thụ động (Passive Monitoring) nhằm đảm bảo tính ẩn danh và không gây ảnh hưởng đến hiệu năng mạng hiện có.

2.1.1. Kiến trúc phần cứng và Vai trò

Hệ thống bao gồm 03 thành phần vật lý chính tương tác qua môi trường sóng vô tuyến (RF):

Đầu tiên là Thiết bị Giám sát (Sensor), đóng vai trò của đội phòng thủ (Blue Team). Thành phần này sử dụng máy tính cài đặt hệ điều hành Kali Linux, kết hợp với card mạng không dây (USB Wi-Fi Adapter) hỗ trợ chế độ Monitor Mode và Packet Injection. Nhiệm vụ chính của Sensor là hoạt động như một cảm biến thụ động, thu thập toàn bộ các gói tin chuẩn 802.11 trong vùng phủ sóng, sau đó giải mã tiêu đề để phục vụ quá trình phân tích.

Thành phần thứ hai là Thiết bị Tấn công (Attacker), đại diện cho đội tấn công (Red Team). Thiết bị này sử dụng bộ công cụ kiểm thử Aircrack-ng suite (bao gồm airbase-ng, aireplay-ng) để giả lập các kỹ thuật tấn công thực tế như DoS hay Evil Twin.

Cuối cùng là Thiết bị Nạn nhân (Victim), bao gồm các thiết bị di động hoặc máy tính xách tay thông thường. Đây là đối tượng người dùng cuối kết nối vào mạng, phục vụ cho việc kiểm chứng khả năng phát hiện của WIDS khi người dùng bị tấn công.

2.1.2. Sơ đồ luồng dữ liệu

Luồng dữ liệu của hệ thống WIDS được vận hành qua bốn giai đoạn tuần tự. Quá trình bắt đầu bằng bước Thu thập (Capture), tại đó card mạng chuyển sang chế độ giám sát để bắt các khung tin (Frames) lớp 2 trong không gian. Kế đến là giai đoạn Tiền xử lý (Preprocessing), Kismet Engine sẽ phân loại các gói tin (Management, Control, Data) và trích xuất các thông tin định danh quan trọng như địa chỉ MAC, SSID và Timestamp.

Dữ liệu sau khi trích xuất sẽ được đưa vào Bộ máy phát hiện (Detection Engine) để so sánh thời gian thực với các quy tắc (Rules) đã định nghĩa. Cuối cùng, khi phát hiện vi phạm, hệ thống thực hiện bước Cảnh báo (Alerting) bằng cách hiển thị thông báo trên giao diện Web UI và ghi log sự kiện phục vụ điều tra số.

2.1.3. Cấu hình tham số vận hành cho Sensor (Kismet)

Để chuyển hóa các thiết kế mô hình thành hệ thống thực tế, phần mềm Kismet trên thiết bị giám sát được thiết lập với các tham số kỹ thuật cụ thể trong tệp cấu hình chính kismet.conf.

Đầu tiên, tham số quan trọng nhất là định nghĩa nguồn thu thập dữ liệu (Capture Source). Hệ thống được cấu hình để trỏ trực tiếp vào giao diện card mạng không dây với cú pháp source=wlan0:type=linuxwifi. Cấu hình này ép buộc Kismet tự động chuyển card mạng sang chế độ Monitor Mode ngay khi khởi động, đảm bảo khả năng bắt trọn vẹn các gói tin quản lý (Management Frames) mà không cần thao tác thủ công phức tạp.

Tiếp theo, để phục vụ cho việc giám sát trực quan, module giao diện Web (Web UI) được kích hoạt trên cổng mặc định 2501. Điều này cho phép quản trị viên truy cập Dashboard thông qua trình duyệt để theo dõi thời gian thực các cảnh báo và thiết bị trong vùng phủ sóng. Đồng thời, cơ chế định danh thiết bị tin cậy (Whitelisting) cũng được thiết lập thông qua giao diện này, cho phép gán nhãn "Known" cho các Access Point hợp pháp, làm cơ sở tham chiếu cho quy tắc phát hiện giả mạo.

Cuối cùng, cơ chế ghi nhật ký (Logging) được tối ưu hóa để phục vụ công tác điều tra số sau sự cố. Hệ thống được cấu hình để lưu trữ dữ liệu dưới định dạng .kismet (chứa metadata và cảnh báo) và .pcapng (chứa gói tin thô). Việc lưu trữ song song này đảm bảo rằng khi một cảnh báo được kích hoạt, quản trị viên có thể truy xuất lại toàn bộ gói tin gốc để phân tích sâu hơn bằng các công cụ như Wireshark.

2.2. Xây dựng kịch bản phát hiện (Detection Ruleset)

Hệ thống được cấu hình tập trung vào ba nhóm nguy cơ chính: Tấn công từ chối dịch vụ, Giả mạo hạ tầng và Các dấu hiệu bất thường về mã hóa. Các luật (Rules) dưới đây được định nghĩa chi tiết trong file cấu hình *kismet_alerts.conf*.

2.2.1. Rule phát hiện Tấn công Từ chối Dịch vụ (DoS Detection)

Tấn công DoS nhằm mục đích ngắt kết nối người dùng khỏi AP thật, gây gián đoạn dịch vụ hoặc ép buộc người dùng kết nối lại để thu thập bắt tay (Handshake).

Rule 1: DEAUTHFLOOD (Deauthentication Flood)

- Cấu hình: *alert=DEAUTHFLOOD,10/min,1/sec*
- Cơ chế: Hệ thống giám sát tần suất xuất hiện của gói tin Deauthentication (Mã quản lý: 0x0C). Nếu số lượng gói tin vượt quá ngưỡng (Threshold) quy định (ví dụ: 10 gói/phút), cảnh báo sẽ được kích hoạt.
- Mục tiêu: Phát hiện các cuộc tấn công nhắm vào một hoặc một nhóm nạn nhân cụ thể nhằm ngắt kết nối họ khỏi mạng.

Rule 2: BCASTDISCON (Broadcast Disassociation)

- Cấu hình: *alert=BCASTDISCON,10/min,1/sec*
- Cơ chế: Phát hiện các gói tin Disassociation (Mã quản lý: 0x0A) được gửi tới địa chỉ quảng bá (Broadcast Address: FF:FF:FF:FF:FF:FF).
- Mục tiêu: Phát hiện hành vi tấn công diện rộng. Khác với Deauth Flood nhắm vào mục tiêu cụ thể, Broadcast Disconnect là dấu hiệu kẻ tấn công muốn "làm sạch" toàn bộ mạng (Network Clearing) để chuẩn bị cho việc dựng AP giả mạo.

2.2.2. Rule phát hiện Giả mạo (Evil Twin Detection)

Đây là chức năng cốt lõi để bảo vệ người dùng khỏi việc kết nối nhầm vào trạm phát sóng của kẻ tấn công.

Rule: APSPOOF (Access Point Spoofing)

- Cấu hình: *alert=APSPOOF,10/min,1/sec*
- Cơ chế: Dựa trên kỹ thuật Whitelisting (Danh sách tin cậy). Hệ thống lưu trữ cặp giá trị hợp lệ [SSID: Tên_Mạng_Thật | BSSID: MAC_Router_Thật]. Khi hệ thống phát hiện một gói tin Beacon mang Tên_Mạng_Thật nhưng xuất phát từ một địa chỉ MAC_Lạ, quy tắc Spoofing sẽ được kích hoạt.

- Ý nghĩa: Xác định chính xác sự tồn tại của một thiết bị giả mạo (Rogue AP) đang hoạt động song song hoặc đè lên mạng thật.

2.2.3. Rule phát hiện Dấu hiệu Bất thường & Xâm nhập

Các công cụ tấn công giả lập AP (như airbase-ng) thường không tuân thủ hoàn toàn chuẩn 802.11 hoặc có các lỗi cài đặt đặc trưng. WIDS tận dụng các lỗi này để nhận diện mối đe dọa.

Rule 1: NONCEREUSE (Nonce Reuse)

- Cấu hình: *alert=NONCEREUSE,5/min,1/sec*
- Cơ chế: Phát hiện việc tái sử dụng giá trị Nonce (Number used once - số ngẫu nhiên dùng một lần) trong quá trình bắt tay mã hóa.
- Phân tích kỹ thuật: Các Router thương mại hoạt động ổn định hiếm khi mắc lỗi này. Ngược lại, các AP giả lập bằng phần mềm (Soft AP) của Hacker thường gặp lỗi trong việc sinh số ngẫu nhiên.
- Ý nghĩa: Đây là dấu hiệu kỹ thuật (Technical Fingerprint) giúp phân biệt AP giả mạo với Router thật ngay cả khi Hacker đã giả mạo MAC và tên mạng.

Rule 2: NOCLIENTMFP (No Management Frame Protection)

- Cấu hình: *alert=NOCLIENTMFP,10/min,1/sec*
- Cơ chế: Cảnh báo khi có thiết bị người dùng (Client) kết nối vào AP mà không kích hoạt chuẩn bảo vệ khung quản lý (Management Frame Protection - 802.11w).
- Ý nghĩa: Trong kịch bản tấn công, AP giả mạo thường hạ cấp cấu hình bảo mật để dễ dàng kiểm soát nạn nhân. Việc Client kết nối thiếu MFP cho thấy kết nối đó kém an toàn và dễ bị tổn thương trước các cuộc tấn công tiếp diễn (như bị ngắt kết nối giả mạo). Đây là chỉ báo cho thấy nạn nhân có thể đã kết nối nhầm vào mạng lưới của kẻ tấn công.

2.3. Thiết kế kịch bản thử nghiệm

Dựa trên các nguy cơ và bộ luật đã xây dựng, hệ thống WIDS sẽ được kiểm thử qua 03 kịch bản tấn công thực tế nhằm đánh giá độ chính xác và khả năng phản hồi.

Kịch bản 1: Tấn công gây nhiễu và ngắt kết nối (DoS) Kịch bản này giả lập việc kẻ tấn công sử dụng công cụ aireplay-ng để gửi hàng loạt gói tin Deauthentication. Mục

tiêu là kiểm chứng xem hệ thống có kích hoạt quy tắc DEAUTHFLOOD và BCASTDISCON khi lưu lượng tấn công vượt ngưỡng quy định hay không.

Kịch bản 2: Triển khai trạm phát sóng giả mạo (Evil Twin) Kịch bản này sử dụng công cụ giả lập để tạo ra một Access Point (AP) có tên (SSID) trùng khớp với mạng thật. Mục tiêu là kiểm tra khả năng của quy tắc APSPOOF trong việc phân biệt thiết bị thật và giả dựa trên địa chỉ MAC (BSSID) và danh sách tin cậy (Whitelist).

Kịch bản 3: Khai thác kết nối người dùng Kịch bản cuối cùng cho phép thiết bị nạn nhân kết nối vào AP giả mạo. Mục tiêu là kiểm chứng khả năng phân tích sâu của WIDS thông qua các quy tắc NONCEREUSE (phát hiện lỗi mã hóa của công cụ tấn công) và NOCLIENTMFP (phát hiện thiết bị kết nối thiếu an toàn).

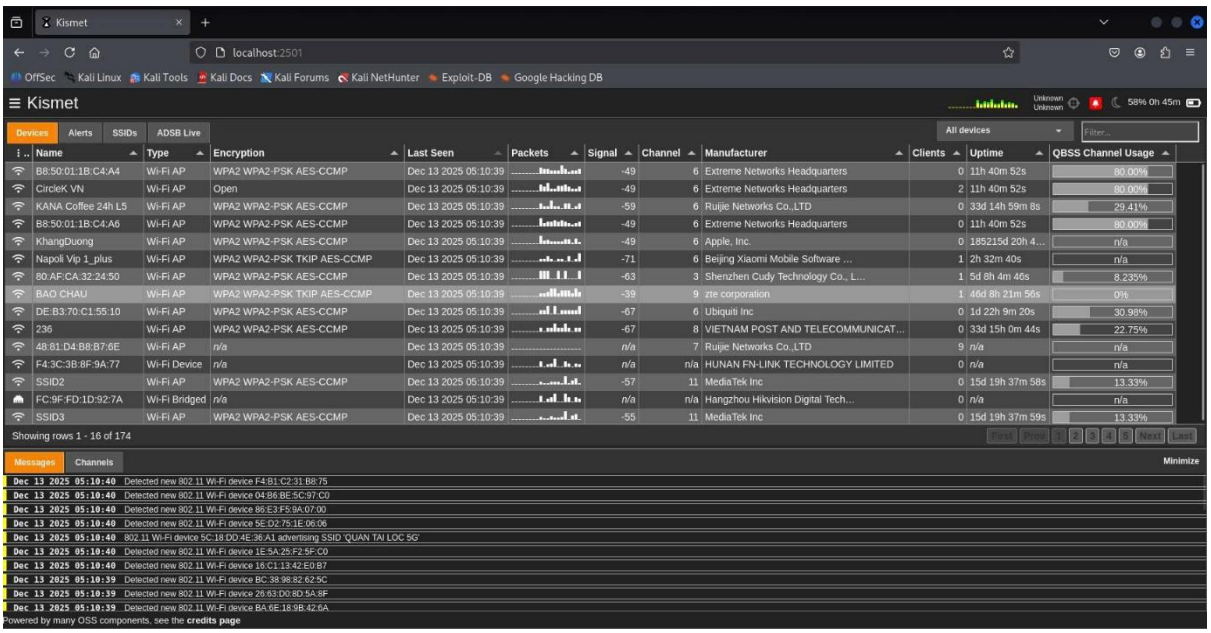
CHƯƠNG 3: THỰC NGHIỆM VÀ ĐÁNH GIÁ KẾT QUẢ

3.1. Thiết lập môi trường và Quy trình thực nghiệm

Để kiểm chứng tính chính xác của các quy tắc phát hiện đã xây dựng, quá trình thực nghiệm được tiến hành trong môi trường mạng không dây cô lập (Isolated WLAN). Việc này nhằm đảm bảo an toàn thông tin và tránh gây nhiễu sóng ảnh hưởng đến các hệ thống mạng lân cận.

Môi trường thực nghiệm được cấu thành từ ba thành phần chính: Máy trạm giám sát (Sensor) chạy Kali Linux với card mạng Monitor Mode, Máy tấn công (Attacker) sử dụng bộ công cụ Aircrack-ng, và Thiết bị nạn nhân (Victim) là điện thoại thông minh.

Trước khi tiến hành các kịch bản tấn công, hệ thống giám sát được khởi động để thiết lập trạng thái ban đầu. Hình 3.1 dưới đây hiển thị giao diện Dashboard chính của Kismet, cho thấy hệ thống đang hoạt động ổn định, bắt đầu thu thập dữ liệu và phân loại các thiết bị trong vùng phủ sóng theo thời gian thực mà chưa ghi nhận dấu hiệu bất thường nào.

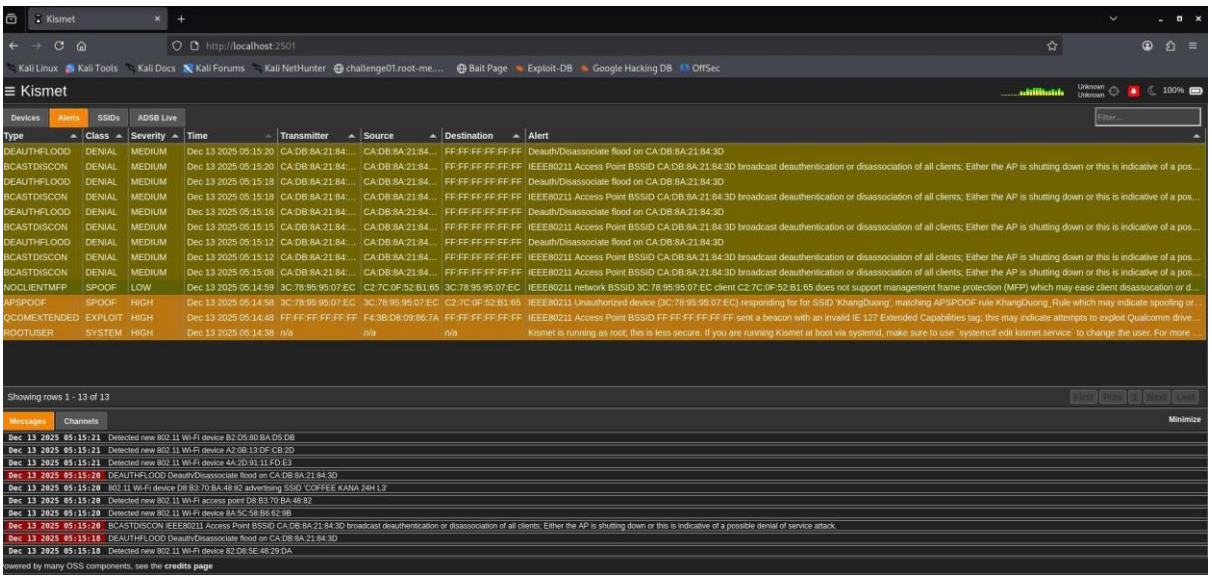


Hình 1: Giao diện kismet khi khởi động

3.2. Kịch bản 1: Phát hiện Tấn công Từ chối Dịch vụ (DoS)

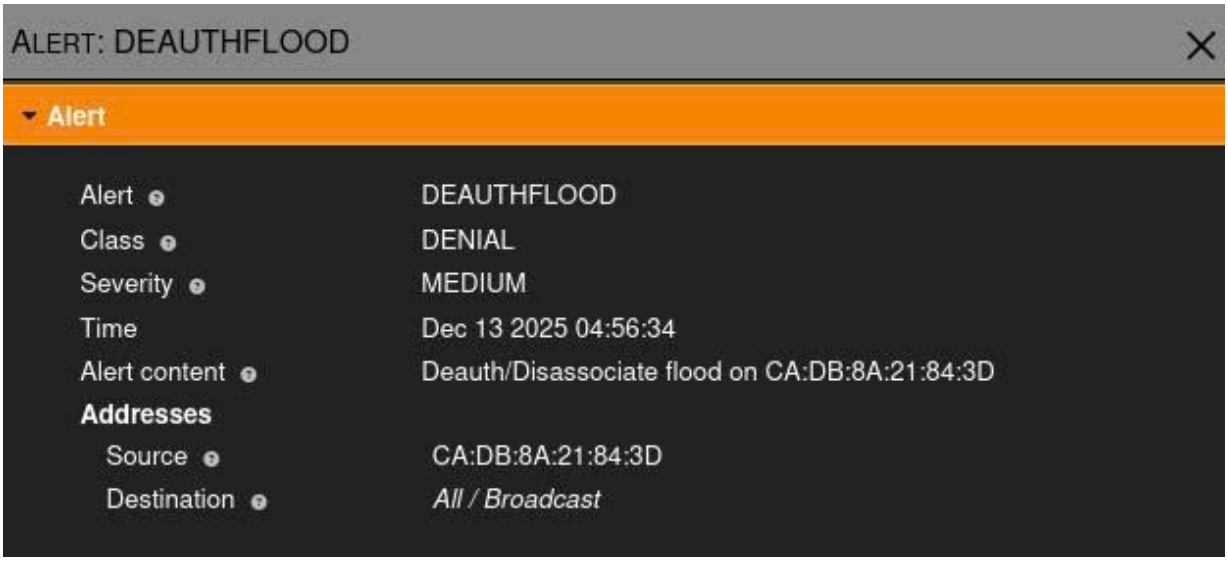
Giai đoạn đầu tiên của cuộc tấn công tập trung vào việc làm gián đoạn dịch vụ, ép buộc thiết bị nạn nhân ngắt kết nối khỏi trạm phát sóng (AP) hợp pháp. Kẻ tấn công sử dụng công cụ aireplay-ng để bơm liên tục các khung tin quản lý vào mạng mục tiêu nhằm gây nghẽn đường truyền.

Ngay khi cuộc tấn công bắt đầu, hệ thống WIDS lập tức phản ứng với các bất thường trong không gian sóng. Tại giao diện quản lý cảnh báo (Tab Alerts), hệ thống ghi nhận một lượng lớn các sự kiện xảy ra dồn dập. Như quan sát thấy trong Hình 3.2, danh sách cảnh báo bị lấp đầy bởi các thông báo thuộc nhóm "DENIAL" với tần suất dày đặc, cho thấy mạng đang chịu một đợt tấn công cường độ cao.



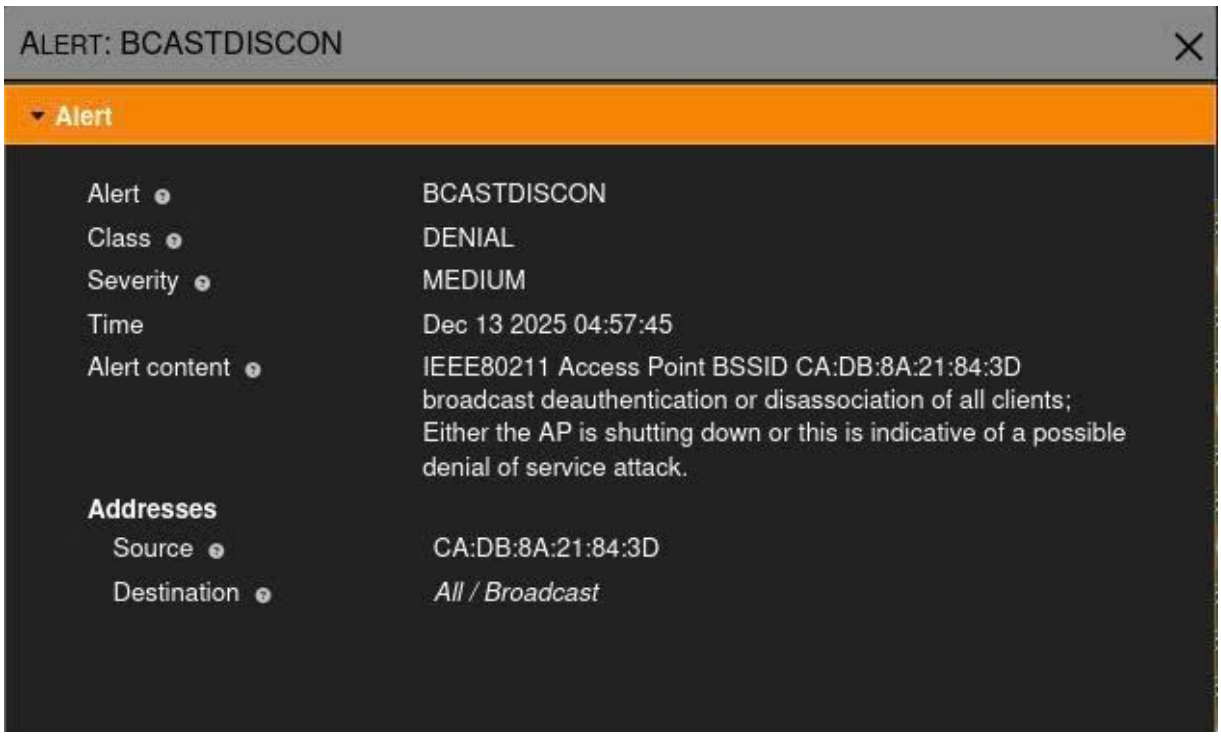
Hình 3.2: Giao diện tab Alerts hiển thị hàng loạt cảnh báo tấn công từ chối dịch vụ (DoS) xảy ra liên tiếp.

Đi sâu vào phân tích chi tiết từng cảnh báo, hệ thống đã kích hoạt thành công quy tắc Deauthentication Flood (DEAUTHFLOOD). Hình 3.3 hiển thị chi tiết nội dung cảnh báo này, trong đó hệ thống xác định được nguồn phát tấn công đang gửi lượng lớn gói tin ngắt kết nối (Deauth) vượt quá ngưỡng an toàn cho phép. Điều này khẳng định đây là hành vi phá hoại có chủ đích chứ không phải hiện tượng rớt mạng ngẫu nhiên.



Hình 3.3: Chi tiết cảnh báo tấn công Deauthentication Flood (DEAUTHFLOOD).

Song song với đó, hệ thống cũng phát hiện cảnh báo Broadcast Disconnect (BCASTDISCON). Hình 3.4 bên dưới cho thấy chi tiết cảnh báo này, trong đó kẻ tấn công gửi các gói tin ngắt kết nối đến địa chỉ đích là All/Broadcast thay vì một thiết bị cụ thể. Đây là dấu hiệu đặc trưng của hành vi tấn công diện rộng nhằm "làm sạch" toàn bộ các thiết bị trong vùng phủ sóng, tạo điều kiện thuận lợi cho việc triển khai trạm phát sóng giả mạo sau đó.



Hình 3.4: Cảnh báo Broadcast Disconnect (BCASTDISCON) cho thấy hành vi ngắt kết nối diện rộng.

3.3. Kịch bản 2: Phát hiện Tấn công Giả mạo (Evil Twin)

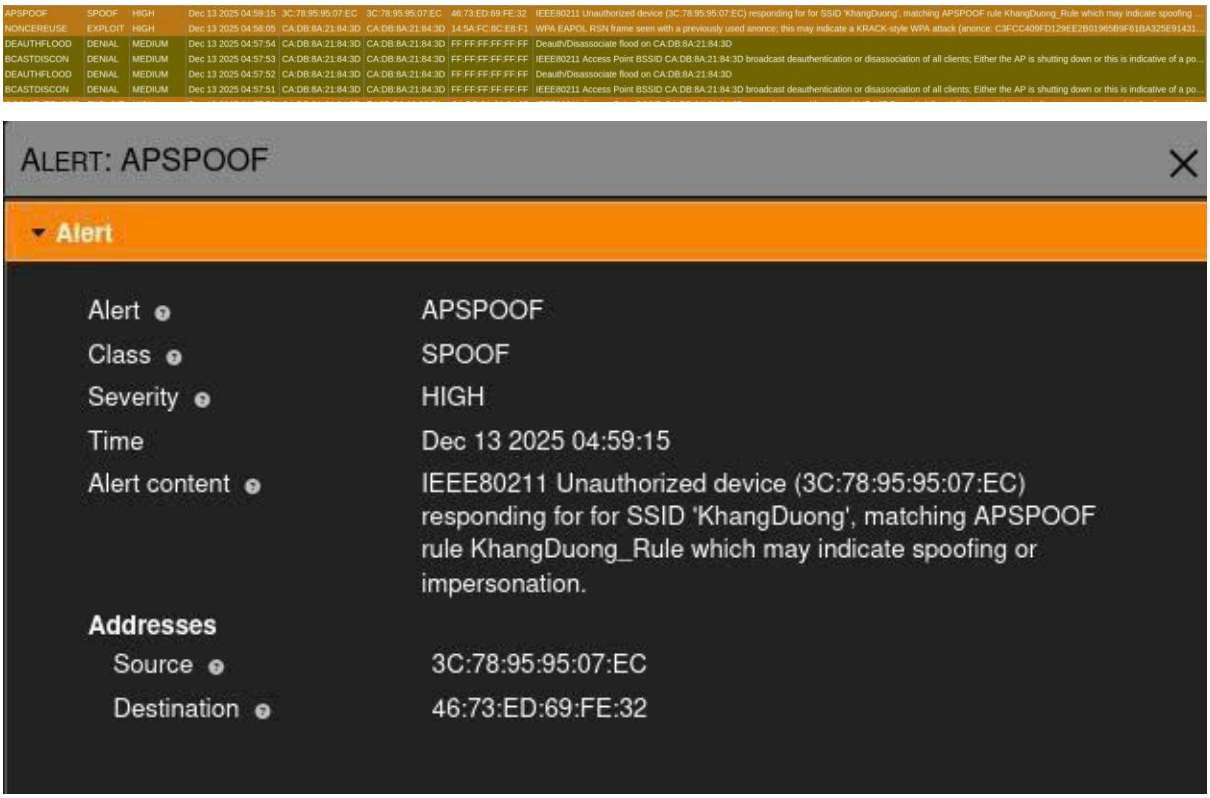
Sau khi thành công trong việc làm gián đoạn kết nối mạng thật, kẻ tấn công kích hoạt một trạm phát sóng giả (Rogue AP) với thông tin định danh (SSID) trùng khớp hoàn toàn với mạng mục tiêu là "KhangDuong" nhằm đánh lừa người dùng.

Tại giai đoạn này, cơ chế so khớp dựa trên danh sách tin cậy (Whitelist) của WIDS phát huy tác dụng tối đa. Hình 3.5 cung cấp bằng chứng trực quan rõ ràng nhất về cuộc tấn công này. Phần trên của hình ảnh cho thấy sự xuất hiện đồng thời của hai mạng cùng tên "KhangDuong": một mạng hợp pháp sử dụng mã hóa WPA2 và một mạng giả mạo không có mật khẩu (Open). Ngay lập tức, hệ thống kích hoạt cảnh báo Access Point Spoofing (APSPOOF) do phát hiện thiết bị lạ phát sóng SSID đã được bảo vệ.

Hình 3.5: Hệ thống phát hiện mạng "KhangDuong" giả mạo và kích hoạt cảnh báo APSPOOF.

Việc phát hiện này dựa trên định danh phần cứng (BSSID) thay vì chỉ dựa vào tên mạng, giúp loại bỏ khả năng bị đánh lừa bởi các kỹ thuật giả mạo SSID thông thường, cung cấp bằng chứng xác thực về sự tồn tại của thiết bị bất hợp pháp. Hình 3.6 dưới đây hiển thị

chi tiết nội dung cảnh báo giả mạo với mức độ nghiêm trọng cao (High).



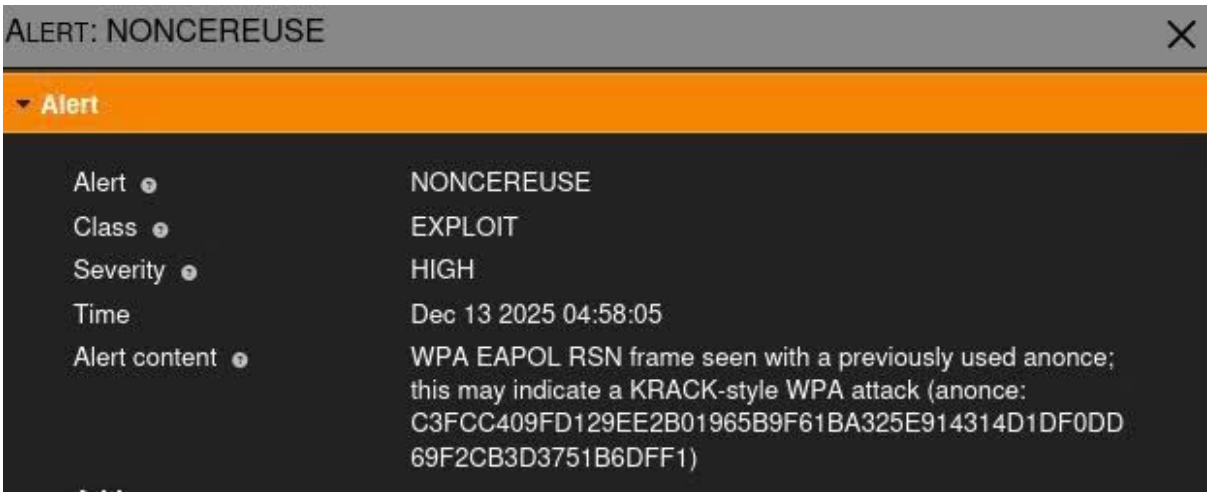
Hình 3.6: Chi tiết cảnh báo Access Point Spoofing xác định thiết bị giả mạo.

3.4. Kịch bản 3: Phân tích Dấu hiệu Bất thường và Xâm nhập

Trong giai đoạn cuối cùng, khi thiết bị nạn nhân kết nối nhầm vào trạm phát sóng giả mạo, hệ thống WIDS thực hiện phân tích sâu (Deep Inspection) vào các đặc điểm kỹ thuật của kết nối để xác định mức độ nguy hiểm.

Đầu tiên, hệ thống đưa ra cảnh báo kỹ thuật Nonce Reuse (NONCEREUSE) với mức độ nghiêm trọng cao, được phân loại là hành vi khai thác (Exploit). Hình 3.7 cho thấy chi tiết cảnh báo này, chỉ ra việc tái sử dụng giá trị Nonce trong quá trình trao đổi khóa. Đây là một "dấu vân tay số" quan trọng, vì các AP giả lập bằng phần mềm của hacker thường gặp lỗi sinh số ngẫu nhiên này, trong khi các Router thương mại chuẩn mực thì

không.



Hình 3.7: Cảnh báo Nonce Reuse (NONCEREUSE) - dấu hiệu kỹ thuật đặc trưng của công cụ tấn công.

Bên cạnh đó, hệ thống cũng ghi nhận cảnh báo No Management Frame Protection (NOCLIENTMFP) khi một thiết bị khách (Client) kết nối vào mạng giả mạo. Hình 3.8 hiển thị cảnh báo cho thấy Client kết nối mà không có tính năng bảo vệ khung quản lý. Điều này xác nhận rằng nạn nhân đã rơi vào một môi trường kết nối lỏng lẻo, thiếu an toàn do kẻ tấn công hạ cấp cấu hình bảo mật để dễ dàng kiểm soát.

Hình 3.8: Cảnh báo thiết bị nạn nhân kết nối không có bảo vệ khung quản lý (NOCLIENTMFP).

3.5. Đánh giá tổng quan kết quả thực nghiệm

Tổng hợp kết quả từ các thực nghiệm trên cho thấy hệ thống WIDS hoạt động hiệu quả và ổn định. Hệ thống đã phát hiện thành công trọn vẹn chuỗi tấn công: từ việc nhận diện hành vi gây nhiễu (DoS) qua các cảnh báo tràn ngập, đến việc chỉ điểm chính xác thiết bị giả mạo (Evil Twin) và cuối cùng là phân tích sâu các dấu hiệu kỹ thuật khi nạn nhân bị xâm nhập. Thời gian phản hồi của các cảnh báo là gần như tức thời (Real-time), cung cấp thông tin giá trị và kịp thời cho công tác giám sát an ninh mạng không dây.

PHẦN KẾT LUẬN

1. Kết luận chung

Sau quá trình nghiên cứu và thực nghiệm, đồ án **"Wireless Network Intrusion Detection System"** đã hoàn thành các mục tiêu đề ra ban đầu, bao gồm việc hệ thống hóa cơ sở lý thuyết về bảo mật mạng không dây và triển khai thành công một giải pháp giám sát thực tế với chi phí thấp.

Về mặt lý thuyết, đồ án đã làm rõ các nguy cơ an ninh đặc thù trong chuẩn IEEE 802.11, đặc biệt là các lỗ hổng trong khung quản lý (Management Frames) chưa được mã hóa. Về mặt thực tiễn, hệ thống WIDS được xây dựng trên nền tảng mã nguồn mở Kismet đã chứng minh được hiệu quả trong môi trường thử nghiệm. Hệ thống hoạt động ổn định ở chế độ giám sát thụ động (Passive Monitoring), đảm bảo tính ẩn danh và không gây ảnh hưởng đến hiệu năng của mạng hiện hành.

Kết quả thực nghiệm khẳng định hệ thống có khả năng phát hiện chính xác và tức thời (Real-time) ba nhóm tấn công nguy hiểm nhất hiện nay. Cụ thể, các quy tắc DEAUTHFLOOD và BCASTDISCON đã phát hiện thành công hành vi tấn công từ chối dịch vụ. Quy tắc APSPOOF hoạt động hiệu quả trong việc nhận diện trạm phát sóng giả mạo (Evil Twin) dựa trên danh sách tin cậy. Đặc biệt, khả năng phân tích sâu gói tin thông qua quy tắc NONCEREUSE và NOCLIENTMFP đã giúp hệ thống phát hiện được các dấu hiệu bất thường về mặt kỹ thuật mà các giải pháp giám sát thông thường dễ bỏ qua.

2. Những hạn chế của đề tài

Bên cạnh những kết quả đạt được, đồ án vẫn còn tồn tại một số hạn chế nhất định do giới hạn về thời gian nghiên cứu và thiết bị phần cứng:

Thứ nhất là hạn chế về phạm vi giám sát do sử dụng đơn nhất một card mạng (Single Sensor). Khi card mạng thực hiện cơ chế nhảy kênh (Channel Hopping) để quét toàn bộ dải tần, hệ thống có thể bỏ lỡ các gói tin tấn công xuất hiện ở các kênh khác trong khoảnh khắc đó. Điều này tạo ra các điểm mù nhất định trong quá trình giám sát liên tục.

Thứ hai, hệ thống hiện tại mới chỉ dừng lại ở mức độ phát hiện và cảnh báo (Detection), chưa tích hợp cơ chế ngăn chặn chủ động (Prevention - IPS). Khi phát hiện tấn công, quản trị viên vẫn cần can thiệp thủ công để xử lý sự cố, điều này có thể tạo ra độ trễ trong việc phản ứng với các mối đe dọa tốc độ cao.

3. Hướng phát triển trong tương lai

Để khắc phục các hạn chế trên và nâng cao tính ứng dụng thực tế của hệ thống, các hướng phát triển tiếp theo được đề xuất bao gồm:

Một là, mở rộng mô hình sang kiến trúc đa cảm biến (Distributed WIDS). Việc bố trí nhiều Drone/Sensor vệ tinh tại các vị trí khác nhau sẽ giúp phủ sóng toàn bộ không gian vật lý, đồng thời khắc phục triệt để vấn đề bỏ sót gói tin do nhảy kênh. Các Sensor này sẽ gửi dữ liệu về một máy chủ trung tâm để tổng hợp và phân tích.

Hai là, tích hợp khả năng phản ứng tự động (IPS). Nghiên cứu phát triển các module có khả năng tự động gửi gói tin ngắt kết nối (Deauth) tới thiết bị của kẻ tấn công hoặc tự động cô lập Client nạn nhân khi phát hiện dấu hiệu thỏa hiệp, giúp giảm thiểu thiệt hại ngay lập tức mà không cần sự can thiệp của con người.

Ba là, tích hợp với các hệ thống quản lý sự kiện và thông tin bảo mật (SIEM) như ELK Stack hoặc Splunk. Việc này sẽ giúp trực quan hóa dữ liệu tấn công trên các biểu đồ Dashboard chuyên nghiệp, hỗ trợ tốt hơn cho công tác phân tích xu hướng và điều tra số (Forensics) dài hạn.

TÀI LIỆU THAM KHẢO

[1] IEEE, "IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11-2020*, pp. 1-4379, Feb. 2021.

[2] M. S. Gast, *802.11 Wireless Networks: The Definitive Guide*, 2nd ed. Sebastopol, CA: O'Reilly Media, 2005, pp. 30-65.

[3] J. Edney and W. A. Arbaugh, *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*. Boston, MA: Addison-Wesley, 2004, pp. 85-112.

[4] Kismet Wireless, "Kismet Wireless Intrusion Detection System Documentation," *kismetwireless.net*, accessed Dec. 15, 2025. [Online]. Available: https://www.kismetwireless.net/docs/readme/intro/kismet/

[5] Aircrack-ng, "Aircrack-ng: WiFi security auditing tools suite," *aircrack-ng.org*, accessed Dec. 15, 2025. [Online]. Available: https://www.aircrack-ng.org/