Tạp chí Khoa học Trường Đại học Cần Thơ
website: sj.ctu.edu.vn

HỆ THỐNG PHÁT HIỆN XÂM NHẬP CHO MẠNG KHÔNG DÂY DỰA TRÊN PHẦN MỀM NGUỒN MỞ

Ngô Bá Hùng[1] và Ngô Trung Hiếu[1]

[1] *Khoa Công nghệ Thông tin & Truyền thông, Trường Đại học Cần Thơ*

Thông tin chung:
Ngày nhận: 23/04/2014
Ngày chấp nhận: 28/08/2014

Title:
Using open source software to build Intrusion Detection System for wireless network

Từ khóa:
Xâm nhập, IDS, mạng không dây, phát hiện xâm nhập, tấn công mạng không dây

Keywords:
Intrusion, IDS, wireless network, intrusion detection system, wireless attack

ABSTRACT

WLAN (Wireless Local Area Network) have become ubiquitous in today's world. With a capability providing "over-the-air" connections, WLAN may be the best choice for accessing Internet anytime and anywhere without heavy investment in infrastructure. In recent times, insecure wireless networks have been exploited to break into companies, banks, and government organizations. The frequency of these attacks has intensified. Therefore, it is very necessary and important to deploy a Wireless Intrusion Detection System (WIDS). Unfortunately, WIDS is usually very expensive, hard to customize and expand. This paper aims at proposing an effective alternative solution to deploy WIDS, which completely bases on open source software and customer-level network devices with low cost. This WIDS solution offers many edge features which are only found in expensive devices. These fearures include inside/outside wireless attack detecting, SMS alerting, and database supporting.

TÓM TẮT

Ngày nay, mạng cục bộ không dây (WLAN - Wireless Local Area Network) đã trở nên vô cùng phổ biến ở khắp nơi trên thế giới. Với đặc tính cung cấp kết nối "qua không khí", mạng WLAN có thể được xem như lựa chọn tốt nhất cho nhu cầu phổ biến Internet mọi lúc mọi nơi mà không cần đầu tư nhiều vào cơ sở hạ tầng ở các nước đang phát triển. Trong thời gian gần đây, những điểm yếu về bảo mật trong mạng WLAN đã liên tục được khai thác nhằm mục đích đột nhập các ngân hàng, công ty và các tổ chức khác… Tần suất diễn ra các cuộc tấn công đã và đang có chiều hướng gia tăng. Do đó, bên cạnh việc triển khai mạng WLAN, việc triển khai một hệ thống phát hiện xâm nhập mạng không dây (WIDS) cũng vô cùng cần thiết. Tuy nhiên, các hệ thống WIDS này thường đắt tiền, khó khăn trong việc tùy biến và mở rộng theo mục đích riêng của nhà triển khai. Bài báo này nhằm đề xuất một giải pháp hiệu quả để triển khai một hệ thống WIDS với giá thành thấp, dựa trên các sản phẩm mã nguồn mở và các thiết bị truy cập không dây thông thường, có khả năng phát hiện và cảnh báo sớm các hình thức tấn công mạng không dây từ bên ngoài và từ bên trong mạng WLAN.

1 GIỚI THIỆU

Nhu cầu truy cập Internet qua mạng không dây không ngừng gia tăng, đặc biệt ở các nước đang phát triển, ví dụ hiện nay tại Việt Nam có chương trình phủ sóng mạng không dây cho các thành phố trực thuộc trung ương và các thành phố du lịch như Hội An, Đà Nẵng, Quảng Ninh… Mạng không dây mang đến những lợi ích to lớn cho người dùng thông qua việc cung cấp khả năng kết nối mọi nơi mọi lúc một cách dễ dàng. Bên cạnh những thuận lợi, mạng không dây cũng chứa đựng nhiều rủi ro tiềm ẩn về bảo mật cho người sử dụng, ví dụ hacker hoàn toàn có thể nghe lén (sniffing) các thông tin quan trọng của người dùng nếu mạng không dây không sử dụng mã hóa, người dùng dễ bị lừa để truy cập vào các điểm truy cập giả mạo để lấy cắp thông tin… Đồng thời, nhà cung cấp dịch vụ mạng không dây hay doanh nghiệp cũng có thể phải hứng chịu các rủi ro như các cuộc tấn công từ chối dịch vụ (De-authentication) để làm tê liệt hoàn toàn khả năng cung cấp kết nối của các điểm truy cập, tấn công gây nhiễu sóng [10]…

Hiện nay, các hãng cung cấp thiết bị mạng nổi tiếng như Cisco, AirDefense, AirTight… đều cung cấp những giải pháp phát hiện xâm nhập mạng không dây (WIDS- Wireless Instrusion Dectection System) của riêng họ. Ví dụ như Cisco có kiến trúc Cisco Unified Wireless Network (CUWN) hỗ trợ tính năng IDS để phát hiện các hình thức tấn công từ bên ngoài mạng WLAN ở tầng 1 và tầng 2 cũng như phát hiện được các hình thức tấn công từ bên trong mạng WLAN (Inside Attack - tức xuất phát từ các client trong mạng WLAN). Tuy nhiên, các giải pháp này đều khó để triển khai tại các nước đang phát triển hay các doanh nghiệp vừa và nhỏ do nhiều yếu tố, trong đó giá thành triển khai cao là nhân tố hàng đầu. Ví dụ giá để triển khai một hệ thống CUWN cơ bản của Cisco khoảng trên 8000 USD, bao gồm 1 Cisco Wireless Controler hỗ trợ cho 12 Access Point với giá 4000 USD [14][18], 2 Access Point giá 1000 USD [6] cho hệ thống chỉ hỗ trợ 5 Access Point, tất cả thiết bị đều phải đặt hàng và nhập khẩu từ các nước phát triển, ngoài ra cần có nhân viên quản trị được đào tạo để cài đặt, cấu hình, quản lý [4]…

Xuất phát từ lý do trên, bài báo này đề xuất một giải pháp khác giúp tiết kiệm về mặt kinh tế nhưng vẫn đảm bảo tính hiệu quả cao để xây dựng hệ thống IDS cho mạng không dây dựa trên kiến trúc phân tán, sử dụng các sản phẩm phần mềm nguồn mở và các thiết bị truy cập mạng không dây thông thường, phổ biến trên thị trường với giá thành rẻ. Hệ thống IDS của bài báo này có thể giám sát và phát hiện được các hình thức tấn công từ bên trong lẫn bên ngoài mạng WLAN, cảnh báo tức thì cho nhà quản trị thông qua tin nhắn SMS (có thể triển khai thêm SNMP, SMTP…), lưu trữ lại các thông tin liên quan đến cuộc tấn công bằng cơ sở dữ liệu tập trung, có khả năng hoạt động như một hệ thống nhật ký trung tâm cho mạng cục bộ không dây (WLAN) cũng như cung cấp khả năng quản trị hệ thống thông qua ứng dụng Web.

Bài báo này gồm 6 phần. Kế tiếp là phần giới thiệu, trong phần sẽ trình bài các nghiên cứu có liên quan đến hệ thống IDS được đề nghị. Phần thứ ba sẽ giới thiệu hướng tiếp cận mới của hệ thống. Chi tiết về hệ thống sẽ được trình bày ở phần thứ tư. Phần thứ năm sẽ trình bày vào thảo luận về kết quả cài đặt, các trường hợp thử nghiệm cũng như kết quả. Cuối cùng là phần kết luận và hướng phát triển của hệ thống đề xuất.

2 CÁC NGHIÊN CỨU LIÊN QUAN

Các hình thức tấn công trong mạng cục bộ không dây WLAN có thể chia ra làm 2 loại: Tấn công từ bên ngoài mạng không dây và tấn công từ bên trong mạng không dây. Tấn công từ bên ngoài mạng không dây là các hình thức tấn công ở tầng 1 và tầng 2 trong mô hình OSI [7]. Phổ biến nhất là 2 kiểu tấn công từ chối dịch vụ (De-authentication Attack) và tấn công nặc danh giả dạng một Access Point (Rogue Access Point Attack) [16]. De-authentication Attack với ý tưởng chính là hacker sẽ gửi những khung De-authentication (thuộc kiểu khung Management trong mạng không dây) nhằm ép client và Access Point thực hiện lại quá trình chứng thực, kết quả là hacker có thể nghe trộm các thông số của quá trình chứng thực giữa client và Access Point để tiến hành dò và lấy các khóa WEP, WPA, hay làm tê liệt hoàn toàn khả năng kết nối giữa các client và Access Point bằng cách gửi quảng bá liên tục những khung De-authentication. Rogue Access Point Attack là hình thức tấn công với ý tưởng chính là hacker sẽ tạo một Access Point giả mạo, trùng SSID với Access Point thật, lừa người dùng kết nối vào, từ đó triển khai các hình thức tấn công nâng cao khác như Men-In-The-Middle, SSL Stripping Attack [8]…

Các hình thức tấn công từ bên trong mạng WLAN là các hình thức tấn công từ tầng 3 của mô hình OSI trở lên. Các cuộc tấn công này xuất phát từ client đã tham gia vào mạng WLAN tương tự như các hình thức tấn công thông thường trong mạng có dây.

Các giải pháp WIDS từ các hãng bảo mật nổi tiếng như Cisco, AirDefense, AirTight… nói chung đều có khả năng giám sát và phát hiện các cuộc tấn công từ bên ngoài lẫn bên trong nói trên, có khả năng lưu trữ các thông tin liên quan đến cuộc tấn công vào cơ sở dữ liệu, gửi cảnh báo qua SNMP, SMTP… Tuy nhiên, các giải pháp này đều khó triển khai tại các nước đang phát triển vì các lý do như đã trình bày trong phần giới thiệu, đồng thời, hầu hết đều thiếu chức năng gửi cảnh báo tức thì cho nhà quản trị thông qua tin nhắn SMS khi có sự kiện xấu xảy ra.

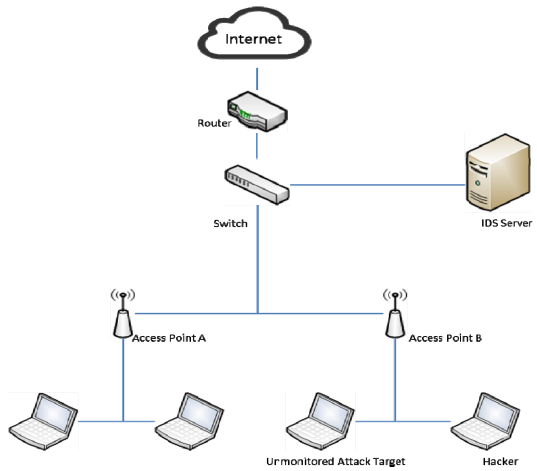
Các dự án IDS miễn phí cho mạng không dây đã từng được khởi động và phát triển như widz hay Snort Wireless đều trở thành dự án "chết" hoặc ngừng cập nhật từ nhiều năm về trước. Hiện nay, giải pháp IDS miễn phí duy nhất cho mạng không dây vẫn còn được duy trì và phát triển là Kismet [12]. Kismet được phát triển bởi Mike Kershaw dưới giấy phép GPL và có thể hoạt động như một WIDS, tuy nhiên, Kismet chỉ có thể phát hiện được các cuộc tấn công từ bên ngoài mạng WLAN dựa vào việc phân tích dữ liệu ở tầng MAC Layer (tầng con thuộc tầng Data-Link) không được mã hóa. Để làm được việc này, Kismet tạo một giao diện mạng ảo (virtual interface) hoạt động ở chế độ monitor dựa trên giao diện mạng không dây của Access Point, sau đó tiến hành bắt các gói tin bằng giao diện mạng ảo này để phân tích. Đối với các khung dữ liệu được mã hóa thì Kismet không thể phân tích để phát hiện ra các dấu hiệu tấn công. Ngoài ra, Snort [11] được biết đến như một giải pháp phát hiện và phòng chống thâm nhập (IDS/IPS – Intrusion Detection and Prevention Systems) nguồn mở mạnh mẽ và được sử dụng rộng rãi trên toàn thế giới để phát hiện các cuộc tấn công từ tầng 3 trở lên. Tuy nhiên, do dữ liệu truyền trong mạng không dây được bảo vệ bởi khóa phiến, khiến cho Snort không thể "đọc-hiểu" được dữ liệu, từ đó không phát hiện được các cuộc tấn công trong nội bộ của một mạng không dây.

Quadrant Information Security cũng đưa ra giải pháp IDS miễn phí cho mạng không dây với ý tưởng chính là cài đặt máy tính trở thành một Access Point, sau đó triển khai Snort và Kismet lên máy tính, từ đó, có thể phát hiện được các cuộc tấn công bên ngoài lẫn bên trong [2]. Tuy nhiên, giải pháp này chỉ mang tính chất "thử nghiệm", không thể triển khai được trong thực tế vì nhiều lý do như kích thước của máy tính to hơn nhiều so với Access Point, không thể đặt máy tính ở những vị trí như treo tường hay ngoài trời, điện năng tiêu thụ của máy tính cao hơn nhiều so với Access Point, tốn kinh phí trang bị phần cứng máy tính…

Jason Murray từng có bài viết về giải pháp IDS cho không dây với ý tưởng chính là cài đặt Kismet trên nền tảng OpenWRT lên Access Point, nhờ vậy, Access Point có thể phát hiện được các cuộc tấn công từ bên ngoài mạng WLAN [9]. Tuy nhiên, giải pháp này chưa thể phát hiện được các cuộc tấn công từ bên trong mạng WLAN, không hỗ trợ lưu trữ thông tin về các cuộc tấn công vào cơ sở dữ liệu, dễ dẫn đến quá tải do việc xử lý gói tin được thực hiện trên Access Point, không tự động gửi cảnh báo.

3 HƯỚNG TIẾP CẬN MỚI

Hình 1 cho thấy phương thức triển khai một hệ thống IDS truyền thống cho mạng không dây. Trong đó, Switch sẽ được cấu hình với kỹ thuật Port Mirroring nhằm chuyển tiếp bảo sao của tất cả gói tin vào/ra của Access Point A hay B về IDS Server để tiến hành phân tích dữ liệu trong các gói tin nhằm phát hiện ra các hành vi xâm nhập và tấn công mạng. Trong kiểu triển khai này, hệ thống IDS có thể kiểm soát một cách hiệu quả toàn bộ lưu thông vào và ra của hệ thống mạng không dây, và xác định được các mối nguy hiểm tiềm ẩn như các hoạt động xâm nhập, virus, worm, hay các hành động nguy hiểm khác… Tuy nhiên, hệ thống IDS hoàn toàn không thể kiểm soát hoạt động trên một mạng WLAN riêng lẻ, tức những lưu thông nội bộ trong WLAN của Access Point A hay B. Kết quả là khi hacker thâm nhập vào hệ thống mạng WLAN, hacker hoàn toàn có thể tấn công bất kỳ client nào trong WLAN (inside attack) mà không bị hệ thống IDS truyền thống phát hiện [1].

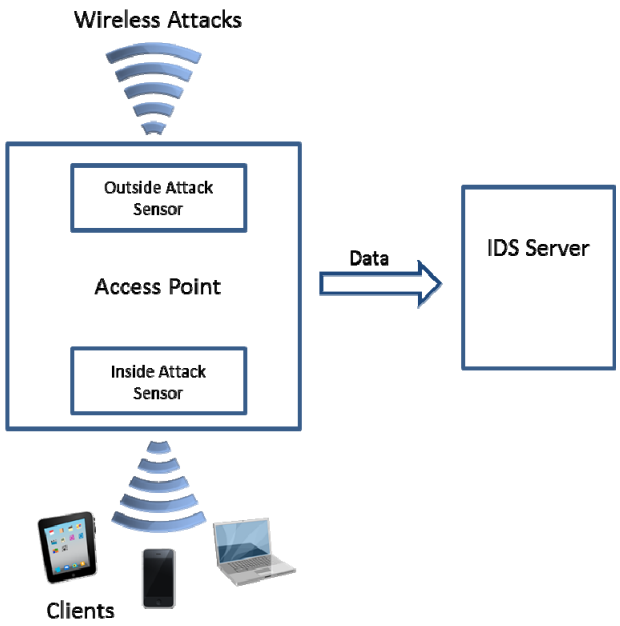


Hình 1: Giải pháp IDS truyền thống cho mạng không dây

Để giám sát và phát hiện được những cuộc tấn công bên ngoài mạng không dây, người ta thường sử dụng một hay nhiều wireless sensor, những thiết bị này có nhiệm vụ bắt tất cả các khung dữ liệu trong phạm vi thu sóng của nó, truyền tất cả các khung này về IDS Server để phân tích xử lý.

Để vượt qua những trở ngại này, hướng tiếp cận được đề xuất ở đây là sử dụng chính các Access Point như những wireless sensor có khả năng nhận và giải mã các gói tin được truyền tải giữa các thiết bị nối kết trong cùng một mạng WLAN mà Access Point đó quản lý và gửi chúng về cho IDS server để phân tích phát hiện các cuộc tấn công xảy ra bên trong mạng WLAN. Đồng thời Access Point cũng được cài đặt để thu thập tất cả các khung dữ liệu bên ngoài nhằm phát hiện cả các cuộc tấn công từ bên ngoài theo kiểu De-authentication Attack hay Rogue Access Point Attack.

Hình 2 cho thấy sơ đồ kiến trúc của hệ thống IDS được đề nghị. Trong giải pháp này, mỗi Access Point sẽ được cài đặt để có thể thu thập 2 loại dữ liệu thông qua 2 sensor ảo (virtual sensor): Outside Attack sensor sẽ thu thập các Frame không mã hóa phục vụ cho phát hiện tấn công ngoài và Inside Attack sensor sẽ thu thập các khung dữ liệu trong WLAN, giải mã chúng để truyền về IDS Server, đây là nơi tiến hành phân tích khung nhận được từ 2 loại sensor, nếu phát hiện có hiện tượng tấn công bên trong hay bên ngoài WIDS server sẽ gửi thông tin này đến Alert system. Hệ thống Alert system sẽ có những hành động đáp trả lại sự kiện này, ví dụ gửi tin nhắn SMS đến số điện thoại đã cài đặt sẵn.



Hình 2: Kiến trúc mới của hệ thống IDS

Với tiêu chí cung cấp một giải pháp WIDS hiệu quả giá thành thấp cho nên chúng tôi chọn giải pháp mã nguồn mở và các access point không đắt tiền để cài đặt thiết kế giải pháp của mình. Chi tiết về việc thiết kế và cài đặt hệ thống IDS được đề nghị sẽ được trình bày ở phần kế tiếp.

4 TỔNG QUAN VỀ HỆ THỐNG IDS ĐƯỢC ĐỀ NGHỊ

Nội dung phần này của bài báo sẽ giới thiệu một cách tổng quan về các thành phần của hệ thống IDS mà bài báo này đề xuất cũng như cách thức hoạt động, tương tác của các thành phần này với nhau.

4.1 Giới thiệu chung về các thành phần chính

Dựa trên các đánh giá từ các cộng đồng mã nguồn mở, chúng tôi chọn các phần mềm mã nguồn mở sau để cài đặt cho giải pháp của mình:

– OpenWRT [15] là một bản phân phối GNU/Linux dành cho các thiết bị nhúng. Thay vì tạo ra một firmware đơn lẻ, tĩnh và không thay đổi, OpenWRT cung cấp một hệ thống tập tin hỗ trợ ghi chép đầy đủ (fully writable filesystem) cùng với hệ thống quản lý gói (package management).

Thông qua việc triển khai OpenWRT lên Access Point, Access Point trở thành một thiết bị vận hành trên nền tảng Linux, nhờ đó dễ dàng cài đặt các phần mềm khác làm nhiệm vụ của Outside Attack Sensor và Inside Attack Sensor.

– Kismet Drone [12] là gói phần mềm được cài đặt lên OpenWRT để làm nhiệm vụ của một Outside Attack sensor, thu thập các khung hỗ trợ cho việc phát hiện các cuộc tấn công từ bên ngoài.

– Kismet Server [12]: Gói phần mềm cài đặt trên IDS server đón nhận và phân tích các frame gửi về từ Kismet Drone nhằm để phát hiện các tấn công ngoài mạng WLAN.

– Daemonlogger [5] là gói phần mềm được cài đặt lên OpenWRT để làm nhiệm vụ của một Inside Attack sensor, thu thập các khung truyền tải giữa các thiết bị đã nối kết vào mạng WLAN của Access Point và chuyển các khung (đã được giải mã) về IDS Server phục vụ cho việc phát hiện các cuộc tấn công bên trong mạng WLAN.

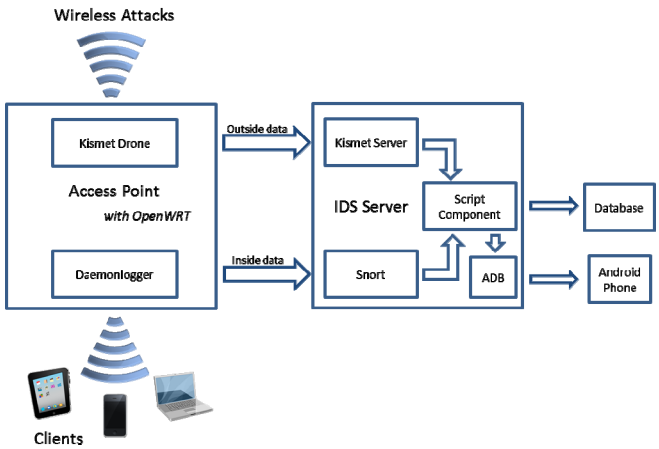
– Snort [11]: Gói phần mềm cài đặt trên IDS server đón nhận và phân tích các frame gửi về từ Daemonlogger nhằm để phát hiện các tấn công bên trong mạng WLAN.

– Script Component: một tập hợp các đoạn mã script nhằm đón nhận các sự kiện từ Kismet Server và Snort xuất ra để tiến hành đưa ra cảnh báo cũng như lưu trữ các thông tin liên quan vào cơ sở dữ liệu.

– ADB (Android Debug Bridge): cầu nối giao tiếp giữa Linux và Android Phone. Alert System sẽ thông qua cầu nối này để tương tác với Android Phone.

– Ngoài ra còn sử dụng một số phần mềm công cụ khác nhằm tăng tốc quá trình xử lý chuyển đổi dữ liệu tăng hiệu quả hoạt động của toàn bộ giải pháp.

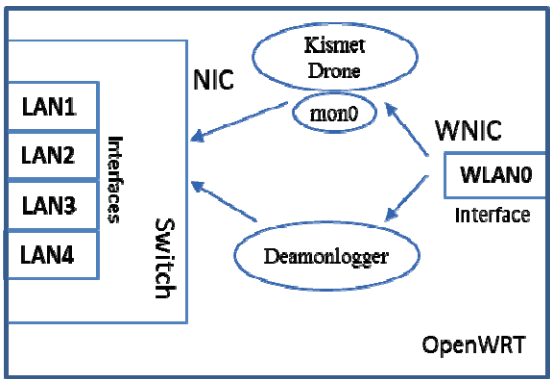
Hình 3 cho thấy vị trí của các phần mềm này trong hệ thống IDS được đề nghị. Các phần tiếp theo sẽ trình bày vai trò và nguyên tắc hoạt động của từng thành phần trong hệ thống.



Hình 3: Vị trí các phần mềm trong hệ thống IDS

4.2 OpenWRT trên Access Point

OpenWRT là một bản phân phối GNU/Linux dành cho các thiết bị nhúng được tùy biến để nạp và chạy như một hệ điều hành cho các Wireless Access Point để cung cấp các nối kết đồng thời cho các thiết bị không dây như máy tính xách tay, điện thoại di động máy tính bảng... Về mặt vật lý, một Access Point được thiết kế như một máy tính với cấu hình khiêm tốn, ví dụ RAM 32 MB, flash size 4MB, bộ vi xử lý 400 MHz và các card giao tiếp mạng. Một Access Point thường có 2 loại card giao tiếp mạng: một hoặc nhiều NIC để giao tiếp với mạng có dây và một WNIC để giao tiếp với mạng không dây. OpenWRT xem các giao tiếp mạng như những giao diện mạng trong một hệ điều hành Linux thông thường. Chẳng hạn, với thiết bị TL-WR941ND của TP-Link, card giao tiếp mạng không dây WNIC sẽ ứng với giao diện mạng wlan0, card giao tiếp mạng có dây NIC sẽ được kết nối với switch để cho ra 4 giao diện mạng lần lượt là lan1, lan2, lan3, lan4 tương ứng với 4 cổng ở mặt sau của thiết bị (như Hình 4).



Hình 4: Kiến trúc TP-Link TL-WR941ND được sử dụng trong hệ thống thực tế

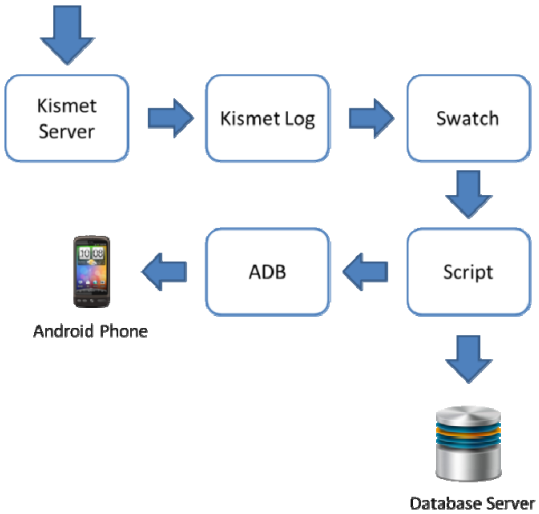
Access Point là điểm kết tập toàn bộ lưu thông của mạng WLAN, do đó, tất cả các gói tin lưu thông trong mạng WLAN đều xuất hiện ở giao diện wlan, như vậy, nhiệm vụ của daemonlogger (đóng vai trò Inside Attack sensor) là lắng nghe trên giao diện wlan này để gửi bản sao của tất cả gói tin trong giao diện này sang một giao diện lan mà từ đó IDS Server có thể nhận được. Do daemonlogger hoạt động ở tầng Application trong mô hình OSI, nên dữ liệu đầu vào (tức những dữ liệu daemonlogger nhận được từ giao diện wlan) là những dữ liệu đã được giải mã ở dạng plain-text bởi chính Access Point. Hơn nữa, giao diện wlan cũng có khả năng thu thập những khung dữ liệu bên ngoài mạng không dây, nhưng do đang hoạt động ở master mode nên nó không thể làm được điều này, giải pháp là Kismet Drone sẽ tạo một giao diện ảo (virtual interface) hoạt động ở monitor mode từ giao diện wlan nhằm thu thập những khung dữ liệu bên ngoài mạng không dây và chuyển tiếp các khung này đến Kismet Server được cài đặt trên IDS Server phục vụ cho việc phát hiện các cuộc tấn công ngoài vào mạng WLAN.

4.3 IDS Server

IDS server thực tế là một máy tính vận hành trên nền tảng Linux, được cài đặt Kismet Server và Snort để phân tích các khung và gói tin do Kismet Drone và Daemonlogger của Access Point gửi đến. Nếu một khung hay gói tin chứa các dấu hiệu hay khớp với các quy tắc đã được thiết đặt trong Kismet Server hay Snort thì IDS Server sẽ đưa ra cảnh báo (xuất nội dung cảnh báo ra màn hình, đồng thời, gửi yêu cầu sang Android Phone) đồng thời ghi nhận nội dung gói tin đó cùng các thông tin liên quan vào một cơ sở dữ liệu nhật ký.

4.3.1 Luồng xử lý dữ liệu của Kismet

Luồng xử lý dữ liệu của Kismet được mô tả như Hình 5.

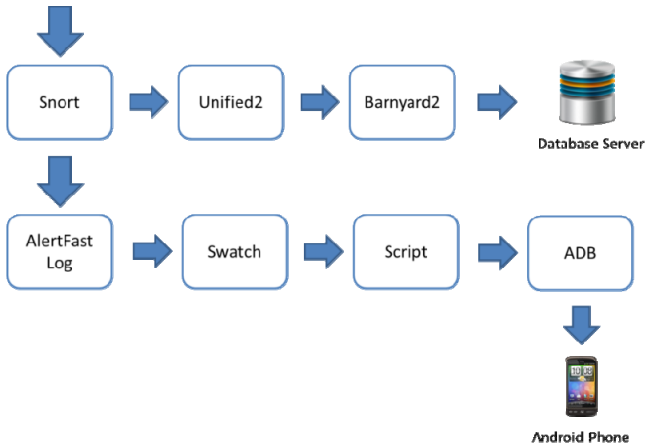


Hình 5: Luồng xử lý dữ liệu của Kismet

Trước hết, Kismet Server nhận dữ liệu từ Kismet Drone (vận hành trên Access Point) gửi đến, xử lý dữ liệu này và xuất cảnh báo ra tập tin Kismet Log (nếu có). Tiện ích Swatch sẽ theo dõi tập tin Kismet Log. Nếu phát hiện có sự thay đổi, Swatch sẽ gọi một đoạn Script đặc biệt, truyền tham số vào đoạn Script này thông qua kỹ thuật ống dẫn pipe. Đoạn Script nhận tham số truyền vào từ Swatch (tham số ở đây là chuỗi cảnh báo mà Kismet đưa ra và lưu vào Kismet Log), tiến hành phân tích chuỗi, trích xuất các thông tin cần thiết, tạo truy vấn để lưu trữ vào cơ sở dữ liệu, đồng thời, thông qua cầu nối ADB (Android Debug Bridge), tạo yêu cầu cho điện thoại Android để gửi tin nhắn đến số điện thoại của nhà quản trị đã được cài đặt trước.

4.3.2 Luồng xử lý dữ liệu của Snort

Luồng xử lý dữ liệu của Snort được mô tả như Hình 6.



Hình 6: Luồng xử lý dữ liệu của Snort

Trước hết, Snort nhận dữ liệu từ Access Point gửi đến, xử lý dữ liệu này, và xuất cảnh báo (nếu có) ra tập tin theo 2 định dạng khác nhau là: Unified2 và AlertFast Log. Một tiến trình độc lập với tên gọi là Barnyard2 sẽ đọc tập tin có định dạng Unified2, phân tích, trích xuất ra các thông tin, và tạo truy vấn để chèn những thông tin cần thiết vào cơ sở dữ liệu. Phần còn lại tương tự như luồng xử lý dữ liệu của Kismet. Swatch sẽ theo dõi tập tin Alert Fast, nếu có thay đổi, sẽ gọi một đoạn Script, truyền tham số thông qua kỹ thuật ống dẫn. Đoạn Script này sẽ tiến hành phân tích chuỗi được truyền vào, thông qua cầu nối ADB, tạo yêu cầu cho điện thoại Android để gửi tin nhắn đến số điện thoại của nhà quản trị đã được cài đặt trước.

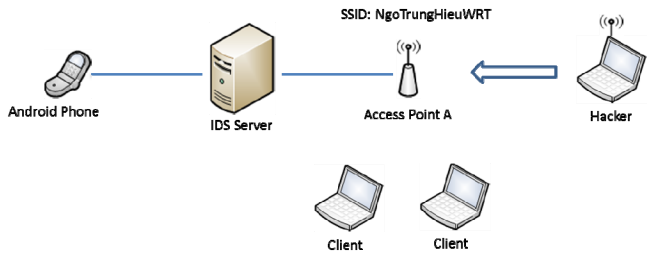
4.4 Hệ thống quản lý sự kiện xâm nhập

Bên cạnh chức năng cảnh báo bằng cách gửi SMS đến số điện thoại đã thiết đặt trước của nhà trị hệ thống, một ứng dụng web cũng được cài đặt để cho phép nhà quản trị xem một cách tổng quát hay chi tiết về các sự kiện xấu xảy ra trong hệ thống mạng không dây của mình đã được lưu lại trong cơ sở dữ liệu bởi Kismet Server và Snort.

5 CÀI ĐẶT, THỬ NGHIỆM, KẾT QUẢ VÀ SO SÁNH

5.1 Cài đặt, thử nghiệm và kết quả

Để kiểm tra khả năng hoạt động và đáp ứng của hệ thống IDS đề nghị, tác giả đã triển khai thử nghiệm trên thiết bị thật. Firmware của Access Point TP-Link TL-WR941ND được thay thế bằng OpenWRT phiên bản Attitude Adjustment 12.09. Sau đó cài đặt thêm vào OpenWRT gói Kismet Drone nằm trong bộ *Kismet-2013-03-R1b* của Kismet và daemonlogger từ *respository* của OpenWRT để Access Point TP-Link TL-WR941ND trở thành một WIDS Access Point của giải pháp đề xuất. IDS Server vận hành trên nền tảng *Ubuntu 13.04*, được cài đặt thêm Kismet Server nằm trong bộ *Kismet-2013-03-R1b*, *Snort 2.9.4.5* và các gói khác như *Apache2*, *PHP5*, *MySQL, android-tools-adb*…từ *respository* của Ubuntu. Điện thoại Android là loại điện thoại Android thông thường, bất kể vận hành dưới quyền root hay user đều tương thích tốt với hệ thống này.



Hình 7: Mô hình kiểm tra tấn công bên ngoài mạng không dây

Mô hình thử nghiệm tấn công bên ngoài được thể hiện như Hình 7. Kết quả khi triển khai tấn công bên ngoài mạng không dây thử nghiệm trình bày cụ thể trong Bảng 1, kết hợp với việc so sánh với giải pháp thương mại CUWN của CISCO.

Bảng 1: Kiểm thử tấn công bên ngoài và so sánh

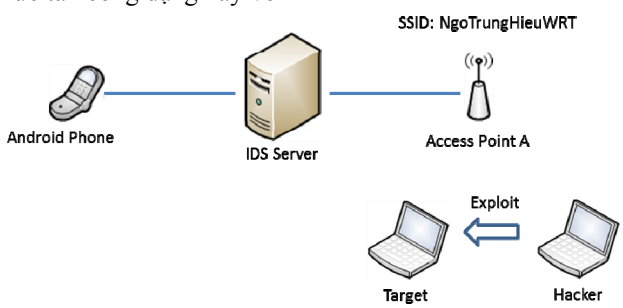
STT	Tên tấn công	IDS của bài báo	CUWN
1	AIRJACKSSID	Phát hiện	Phát hiện
2	APSPOOF	Phát hiện	Phát hiện
3	BSSTIMESTAMP	Phát hiện	Phát hiện
4	CRYPTODROP	Phát hiện	Phát hiện
5	DEAUTHFLOOD	Phát hiện	Phát hiện
6	BCASTDISCON	Phát hiện	Phát hiện
7	DHCPCLIENTID	Phát hiện	Phát hiện
8	DHCPCONFLICT	Phát hiện	Phát hiện
9	DISASSOCTRAFFIC	Phát hiện	Phát hiện
10	DISCONCODEINVALID	Phát hiện	Phát hiện
11	DEAUTHCODEINVALID	Phát hiện	Phát hiện
12	DHCPNAMECHANGE	Phát hiện	Phát hiện
13	DHCPOSCHANGE	Phát hiện	Phát hiện
14	LONGSSID	Phát hiện	Phát hiện
15	LUCENTTEST	Phát hiện	Phát hiện
16	MSFBCOMSSID	Phát hiện	Phát hiện
17	MSFDLINKRATE	Phát hiện	Phát hiện
18	MSFNETGEARBEACON	Phát hiện	Phát hiện
19	NETSTUMBLER	Phát hiện	Phát hiện
20	NULLPROBERESP	Phát hiện	Phát hiện
21	PROBENOJOIN	Phát hiện	Phát hiện

Trong các trường hợp kiểm thử, hệ thống IDS của bài báo này đều phát hiện được và đưa ra cảnh báo ngay lập tức thông qua tin nhắn SMS, lưu thông tin vào cơ sở dữ liệu. Ngoài ra, hệ thống cũng có khả năng phát hiện các hình thức tấn công bên ngoài khác, cụ thể được liệt kê tại Kismet Documentation [11].

Theo đó, với giải pháp nguồn mở miễn phí của bài báo đã có thể hỗ trợ phát hiện được tất cả 21 hình thức tấn công khác nhau từ bên ngoài mạng không dây, ngang với giải pháp thương mại CUWN của CISCO.

Về thực tế, các hình thức tấn công bên trong mạng không dây tương đồng hoặc giống với các hình thức tấn công trong mạng Ethernet thông thường. Do đó, các hình thức tấn công dạng này vô cùng đa dạng và phong phú, nên không thể kiểm thử để bao quát tất cả. Chúng tôi chỉ đưa ra một kết quả thực nghiệm để chứng minh được rằng: với hệ thống IDS của bài báo, có thể ứng dụng được Snort cũng như rules của nó nhằm kiểm tra các gói tin (bất kể hình thức mã hóa) để phát hiện các cuộc tấn công từ bên trong mạng không dây.

Mô hình thử nghiệm tấn công bên trong mạng không dây được thể hiện như Hình 8. Theo đó, vì một lý do nào đó, hacker đã thâm nhập được vào mạng WLAN. Đầu tiên, hacker sẽ tiến hành quét mạng để thu thập thông tin về các host đang hoạt động cũng như các dịch vụ đang vận hành trên host đó. Sau đó, hacker sẽ tiến hành exploit để chiếm quyền điều khiển máy tính target đang vận hành dịch vụ Samba.



Hình 8: Mô hình kiểm tra tấn công bên trong mạng không dây

Tương tự, trong cả 2 bước quét mạng và exploit, hệ thống IDS của bài báo cũng đều phát hiện được và đưa ra cảnh báo ngay lập tức khi sự kiện thâm nhập vừa xảy ra (tức ngay khi hacker vừa quét mạng và ngay khi hacker vừa exploit) thông qua tin nhắn SMS, lưu thông tin vào cơ sở dữ liệu. Việc phát hiện dựa trên những rule được định nghĩa trong Snort.

5.2 So sánh với các kết quả khác và nhận xét

Giải pháp IDS của bài báo sẽ được so sánh về mặt chức năng cùng với các giải pháp nguồn mở tương tự khác và giải pháp thương mại CUWN của CISCO theo Bảng 2:

Bảng 2: Kiểm thử tấn công bên ngoài và so sánh

Tên chức năng	IDS được đề nghị	CUWN	Quadrant Information Security	Jason Murray
Phát hiện tấn công từ bên ngoài	Có, dựa trên Kismet	Có, tương tự Kismet	Có, dựa trên Kismet	Có, dựa trên Kismet
Phát hiện tấn công từ bên trong	Có, dựa trên Snort	Có	Có, dựa trên Snort	Không
Hỗ trợ rules để nhận diện thêm tấn công từ bên trong	Có, Snort rules	Có	Có, Snort rules	Không
Hỗ trợ cảnh báo tức thì bằng tin nhắn SMS	Có	Không	Không	Không
Hỗ trợ quản lý sự kiện với cơ sở dữ liệu	Có, hỗ trợ cả Snort lẫn Kismet	Có	Chỉ hỗ trợ Snort, Kismet không hỗ trợ sẵn	Không
Chặn đứng gói tin xấu (IPS)	Không	Có	Không	Không
Khả năng mở rộng	Có, không ràng buộc bởi phần cứng	Không, ràng buộc phần cứng CISCO	Có, không ràng buộc bởi phần cứng	Có, không ràng buộc bởi phần cứng
Giá thành triển khai	Rất thấp	Rất cao	Rất thấp	Rất thấp

Qua Bảng 2 có thể thấy, giải pháp IDS của bài báo mang nhiều ưu điểm vượt trội so với các giải pháp nguồn mở khác, cụ thể là về khả năng phát hiện được các hình thức tấn công từ bên ngoài lẫn bên trong, cảnh báo tức thì bằng SMS cho một hay nhiều nhà quản trị ngay khi phát hiện tấn công; hỗ trợ quản lý các sự kiện xấu từ tấn công bên ngoài (Kismet) lẫn bên trong (Snort) bằng cơ sở dữ liệu thông qua ứng dụng Web, các giải pháp nguồn mở như Quadrant Information Security chỉ quản lý các sự kiện xấu từ tấn công bên trong bằng cách dùng ứng dụng Web có sẵn của Snort, không hỗ trợ cho Kismet (do Kismet không lưu trữ vào cơ sở dữ liệu cũng như không có ứng dụng Web đi kèm).

Khả năng mở rộng của những giải pháp sử dụng phần mềm mã nguồn mở là vô cùng cao, ví dụ như từ việc hỗ trợ gửi cảnh báo tức thời thông qua tin nhắn SMS, hoàn toàn có thể dễ dàng tích hợp thêm việc gửi cảnh báo qua SMTP, SNMP… Một điều quan trọng khác là những giải pháp này không bị phụ thuộc vào phần cứng, có thể sử dụng kết hợp các thiết bị từ các nhà sản xuất phần cứng khác nhau. Trong khi đó, các giải pháp nguồn đóng thương mại như CUWN dường như không cung cấp cho người dùng những thuận lợi này.

Chức năng chặn đúng gói tin xấu (IPS) của CUWN vẫn hoạt động dựa trên rules, điều này đồng nghĩa với việc chức năng IPS không thể chặn đứng một cuộc tấn công mới (tức cuộc tấn công chưa được định nghĩa trong rules). Mặc dù, giải pháp của bài báo vẫn chưa cài đặt được chức năng chặn đứng gói tin xấu (IPS) như ở giải pháp CUWN của CISCO, nhưng với những tính năng cũng như hiệu quả mà giải pháp này IDS nguồn mở miễn phí của bài báo này mang lại, đây thật sự là một giải pháp tiềm năng cho phần lớn các quốc gia đang phát triển.

6 KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Qua các phần đã trình bày bên trên, bài báo đã đưa ra được một giải pháp thay thế hiệu quả và tiết kiệm trong việc triển khai hệ thống IDS cho mạng không dây. Giải pháp này khắc phục được những nhược điểm của hệ thống WIDS truyền thống như đã đề cập ở phần 3, cung cấp những tính năng nổi bật như lưu trữ sự kiện vào cơ sở dữ liệu, khả năng quản lý sự kiện, cảnh báo tức thì bằng SMS… chỉ

có ở những hệ thống WIDS đắt tiền. Chi phí triển khai của giải pháp vô cùng rẻ do hoàn toàn sử dụng những thiết bị mạng thông thường và các sản phẩm phần mềm mã nguồn mở. Hệ thống này có thể được triển khai một cách rộng rãi tại nhiều nơi như cơ quan, tổ chức, công ty… với quy mô nhỏ, vừa, hay thậm chí quy mô lớn cần tiết kiệm chi phí trong việc triển khai một hệ thống bảo mật cho mạng không dây nhưng vẫn đảm bảo tính bảo mật và hiệu quả.

Bên cạnh đó, hệ thống này vẫn còn tồn tại những khuyết điểm nhất định: khả năng phát hiện tấn công bên ngoài hoàn toàn phụ thuộc vào khả năng phát hiện của Kismet Server, không hỗ trợ viết rule để nhận dạng các cuộc tấn công mới; khả năng phát hiện các cuộc tấn công bên trong đòi hỏi phải định nghĩa trước về các cuộc tấn công này thông qua rule của Snort; dữ liệu gửi từ Access Point về IDS Server mang tính dư thừa do Kismet Drone sẽ gửi những Frame có mã hóa về IDS Server.

Do đây là giải pháp cho một hệ thống phát hiện xâm nhập nên chỉ dừng lại ở việc đưa ra cảnh báo cũng như cung cấp các thông tin liên quan về cuộc xâm nhập, hoàn toàn không có khả năng ngăn chặn cuộc xâm nhập xảy ra hay hạn chế những hậu quả xấu mà nó gây ra. Access Point vận hành trên nền tảng Linux nhờ vào OpenWRT, nên việc ứng dụng iptables để Access Point tiến hành chặn (drop or reject) các gói tin xấu hay chặn địa chỉ gửi gói tin xấu một cách tự động bằng chính iptables hoặc MAC Filter, từ đó chặn được các cuộc tấn công từ bên trong cũng là hướng nghiên cứu tiềm năng.

TÀI LIỆU THAM KHẢO

1. ARUBA networks, 2013. Integrating Wired IDS with Wi-Fi Using Open-Source IDS to Complement a Wireless IDS/IPS Deployment.
2. Champ Clark III, 2014. Building Wireless IDS system using open source, http://sagan.quadrantsec.com/papers/wireless-ids/, assessed on 02/06/2014.
3. Cisco, 2014. Cisco Licensing and Ordering Guide, http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd804b4646.html, assessed on 02/06/2014.
4. Cisco, 2014. Cisco Unified Wireless Network, http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/secwlandg20/ch4_2_SPMb.html, assessed on 02/06/2014.
5. Dice Holdings, 2014. SourceForge: Daemonlogger, http://sourceforge.net/projects/daemonlogger/, accessed on 19/5/2014.
6. Geminicomputersinc, 2014. CSC-AIRLAP1261NAK9, http://www.geminicomputersinc.com/csc-airlap1261nak9.html, accessed on 19/5/2014.
7. Grant Wilson, 2001. OSI Defense in Depth to Increase Application Security, http://www.giac.org/paper/gsec/2868/osi-defense-in-depth-increase-application-security/10484, assessed on 02/06/2014.
8. Hossein Bidgoli, 2006. The Handbook of Information Security. John Wiley & Sons, Inc.
9. Jason Murray, 2014. An Inexpensive Wireless IDS using Kismet and OpenWRT, http://www.sans.org/reading_room/whitepapers/detection/inexpensive-wireless-ids-kismet-openwrt_33103, assessed on 02/06/2014.
10. John Bellardo and Stefan Savage, 2003. 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. Department of Computer Science and Engineering, University of California at San Diego.
11. Martin Roesch, Chris Green, 2014. SNORT Users Manual, http://manual.snort.org/, assessed on 02/06/2014.
12. Mike Kershaw, 2014. Kismet Documentation, http://www.kismetwireless.net/documentation.shtml, assessed on 02/06/2014.
13. Nathan Einwechter, 2010. An Introduction To Distributed Intrusion Detection Systems, http://www.symantec.com/connect/articles/introduction-distributed-intrusion-detection-systems, assessed on 02/06/2014.
14. Network Hardware Australia. 2014, Cisco Wireless Control System, http://www.networkhardware.net.au/cisco-wcsapbase50-p-15452.html?utm_term=CISCO+WCS+APBASE+50&utm_campaign=Network+Products&utm_medium=cpc&utm_source=myshopping, accessed on 19/5/2014.

15. OpenWrt, 2014. OpenWrt: Wireless Freedom, https://openwrt.org/, accessed on 19/5/2014.
16. Prabhaker Mateti, 2005. Hacking Techniques in Wireless Networks, http://cecs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm, assessed on 02/06/2014
17. Rafeeq Ur Rehman, 2003. Intrusion Detection Systems with Snort: Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID.
18. Router-switch Ltd, 2014. AIR-WLC4402-12-K9, http://www.router-switch.com/air-wlc4402-12-k9-p-4378.html, accessed on 17/3/2014.