MÔ HÌNH HỆ THỐNG GIÁM SÁT MẠNG TÍCH HỢP DỰA VÀO PHẦN MỀM NGUỒN MỞ

Nguyễn Đình Thúc[1], Huỳnh Nguyên Chính[2]

[1]Trường Đại học Khoa Học Tự Nhiên, Đại học Quốc gia Tp. Hồ Chí Minh.
[2]Trường Đại học Sư Phạm Kỹ Thuật Tp. Hồ Chí Minh

ndthuc@hcmuns.edu.vn, chinhhn@fit.hcmute.edu.vn

Tóm tắt. Mạng máy tính đang ngày càng phát triển mạnh và có vai trò quan trọng cho mỗi cá nhân, tổ chức, doanh nghiệp. Đi đôi với sự phát triển này thì bảo mật mạng đang là một nhu cầu cấp thiết nhằm bảo vệ hệ thống mạng bên trong, chống lại những tấn công xâm nhập và thực hiện các trao đổi thông tin, giao dịch qua mạng được an toàn.

Trong bài viết này, tác giả tập trung nghiên cứu giải pháp giám sát hệ thống mạng tích hợp bao gồm các thành phần: hệ thống phát hiện và phòng chống xâm nhập mạng, hệ thống giám sát lưu lượng, hệ thống giám sát thiết bị và dịch vụ. Cụ thể, tác giả cài đặt minh họa giải pháp trên với sự kết hợp của các phần mềm nguồn mở Snort, Fwsnort, Cacti, Nagios. Tạo ra một hệ thống giám sát mạng, có khả năng: phát hiện những xâm nhập, phòng chống tấn công mạng, giám sát tình trạng hoạt động của các thiết bị quan trọng trong hệ thống (Server, Router, switch,...) và các dịch vụ chạy trên nó. Đồng thời cài đặt hệ thống báo động đa dạng, tiện dụng và linh động hỗ trợ cho người quản trị mạng giám sát hệ thống một cách hiệu quả hơn thông qua nhiều hình thức như Web, Email, âm thanh và SMS.

Từ khóa: Hệ thống giám sát mạng, hệ thống phát hiện và phòng chống xâm nhập mạng, hệ thống giám sát lưu lượng, hệ thống giám sát thiết bị và dịch vụ, hệ thống báo động.

INTEGRATED NETWORK MONITORING MODEL BASED ON OPEN SOURCE SOFTWARE

Abstract. Computer networks are increasingly powerful and played an important role for individuals, organizations and businesses. Together with this development, the network security is a critical need with the purpose of protecting the inside network, preventing attacks and making the exchange of information through the computer network system is secured.

In this paper, the author focused on researching solutions surveillance network includes integrated components: intrusion detection systems and intrusion prevention systems, traffic monitoring systems, hosts and services monitoring systems. Specifically, the author illustrates the solution with the combination of open source softwares: Snort, Fwsnort, Cacti, and Nagios. Implementing a network monitoring system with capable of: intrusion detection and prevention of attacks, monitoring the operation of network devices such as servers, routers, switches... and services running on it. Simultaneously install an alert system diversity, convenience and flexibility to support network administrators to monitor the system more effectively through various forms such as Web, Email, Audio, and SMS.

Keywords: network monitoring system, network intrusion detection and intrusion prevention system, traffic monitoring systtem, hosts and services monitoring system, alert system.

MÔ HÌNH HỆ THỐNG GIÁM SÁT MẠNG TÍCH HỢP DỰA VÀO PHẦN MỀM NGUỒN MỞ

Nguyễn Đình Thúc
Khoa CNTT, Trường Đại học Khoa Học Tự Nhiên
Đại học Quốc gia Tp. Hồ Chí Minh
ndthuc@hcmuns.edu.vn

Huỳnh Nguyên Chính
Bộ môn Mạng Máy Tính, Khoa CNTT
Trường Đại học Sư Phạm Kỹ Thuật Tp. Hồ Chí Minh
chinhhn@fit.hcmute.edu.vn

Tóm tắt -- Mạng máy tính đang ngày càng phát triển mạnh và có vai trò quan trọng cho mỗi cá nhân, tổ chức, doanh nghiệp. Đi đôi với sự phát triển này thì bảo mật mạng đang là một nhu cầu cấp thiết nhằm bảo vệ hệ thống mạng bên trong, chống lại những tấn công xâm nhập và thực hiện các trao đổi thông tin, giao dịch qua mạng được an toàn.

Trong bài viết này, tác giả tập trung nghiên cứu giải pháp giám sát hệ thống mạng tích hợp bao gồm các thành phần: hệ thống phát hiện và phòng chống xâm nhập mạng, hệ thống giám sát lưu lượng, hệ thống giám sát thiết bị và dịch vụ. Cụ thể, tác giả cài đặt minh họa giải pháp trên với sự kết hợp của các phần mềm nguồn mở Snort, Fwsnort, Cacti, Nagios. Tạo ra một hệ thống giám sát mạng, có khả năng: phát hiện những xâm nhập, phòng chống tấn công mạng, giám sát tình trạng hoạt động của các thiết bị quan trọng trong hệ thống (Server, Router, switch,...) và các dịch vụ chạy trên nó. Đồng thời cài đặt hệ thống báo động đa dạng, tiện dụng và linh động hỗ trợ cho người quản trị mạng giám sát hệ thống một cách hiệu quả hơn thông qua nhiều hình thức như Web, Email, âm thanh và SMS.

Từ khóa -- Hệ thống giám sát mạng, hệ thống phát hiện và phòng chống xâm nhập mạng, hệ thống giám sát lưu lượng, hệ thống giám sát thiết bị và dịch vụ, hệ thống báo động.

I. GIỚI THIỆU

A. Phân loại các lỗ hổng bảo mật

Hiểu được những điểm yếu trong bảo mật là một vấn đề hết sức quan trọng để tiến hành những chính sách bảo mật có hiệu quả.

Những điểm yếu trong bảo mật mạng gồm có những điểm yếu: về mặt kỹ thuật, về mặt cấu hình và các chính sách bảo mật.

- *Điểm yếu về mặt kỹ thuật*: điểm yếu trong kỹ thuật gồm có điểm yếu trong các giao thức, trong Hệ điều hành và các thiết bị phần cứng như Server, Switch, Router,...
- *Điểm yếu trong cấu hình hệ thống*: đây là lỗi do nhà quản trị tạo ra. Lỗi này do các thiếu sót trong việc cấu hình hệ thống như: không bảo mật tài khoản khách hàng, sử dụng các cấu hình mặc định trên thiết bị...
- *Điểm yếu trong chính sách bảo mật*: chính sách bảo mật diễn tả việc làm thế nào và ở đâu chính sách bảo mật được thực hiện. Đây là điều kiện quan trọng giúp việc bảo mật có hiệu quả tốt nhất.

B. Các công cụ phát hiện lỗ hổng mạng

Những kẻ phá hoại sẽ lợi dụng những lỗ hổng bảo mật để xâm nhập vào hệ thống. Như vậy, việc dò tìm những điểm yếu trong hệ thống để có những biện pháp khắc phục nhằm hạn chế các nguy hại cho hệ thống là cần thiết.

Các thông tin từ nhà sản xuất phần cứng, phần mềm, các bản vá lỗi nên được cập nhật thường xuyên cũng là một giải pháp để bảo vệ cho hệ thống của mình.

Hơn nữa, hiện nay có rất nhiều công cụ giúp người quản trị mạng dò tìm những lỗ hổng bảo mật trong hệ thống mạng của mình. Điển hình một số công cụ được sử dụng phổ biến là: Nmap, Metasploit, Nessus, Nikto, Paros Proxy, WebScarab, WebInspect, Whisker, Wikto, Acunetix Web Vulnerability Scanner, Watchfire AppScan, N-Stealth,...

C. Các kiểu tấn công mạng

Có rất nhiều dạng tấn công mạng được biết đến hiện nay. Có thể phân loại dựa vào những tiêu chí sau:

Nếu dựa vào hành động của cuộc tấn công có thể phân tấn công ra làm hai loại là: tấn công chủ động và tấn công bị động:

- *Tấn công chủ động*: kẻ tấn công thay đổi hoạt động của hệ thống và hoạt động của mạng khi tấn công và làm ảnh hưởng đến tính toàn vẹn, sẵn sàng và xác thực của dữ liệu.
- *Tấn công bị động*: kẻ tấn công cố gắng thu thập thông tin từ hoạt động của hệ thống và hoạt động của mạng làm phá vỡ tính bí mật của dữ liệu.

Nếu dựa vào nguồn gốc của cuộc tấn công thì có thể phân loại tấn công làm hai loại: tấn công từ bên trong và tấn công từ bên ngoài:

- *Tấn công từ bên trong*: là những tấn công xuất phát từ bên trong hệ thống mạng. Kẻ tấn công là những người trong hệ thống

mạng nội bộ muốn truy cập, lấy thông tin nhiều hơn quyền cho phép.

- *Tấn công từ bên ngoài*: là những tấn công xuất phát từ bên ngoài Internet hay các kết nối truy cập từ xa.

Mặc dù có nhiều kiểu tấn công mạng nhưng để thực hiện một cuộc tấn công xâm nhập, kẻ tấn công thường thực hiện qua 5 bước như sau:

- Bước 1: **Khảo sát, thu thập thông tin**: kẻ tấn công thu thập thông tin về nơi tấn công như phát hiện các máy chủ, địa chỉ IP, các dịch vụ mạng, ...
- Bước 2: **Dò tìm**: kẻ tấn công sử dụng các thông tin thu thập được từ bước 1 để tìm kiếm thêm thông tin về lỗ hổng, điểm yếu của hệ thống mạng. Các công cụ thường được sử dụng cho quá trình này là các công cụ quét cổng, quét IP, dò tìm lỗ hổng, ...
- Bước 3: **Xâm nhập**: các lỗ hổng được tìm thấy trong bước 2 được kẻ tấn công sử dụng, khai thác để xâm nhập vào hệ thống. Ở bước này, kẻ tấn công có thể dùng các kỹ thuật như: tràn bộ đệm, từ chối dịch vụ (DoS), ...
- Bước 4: **Duy trì xâm nhập**: một khi kẻ tấn công đã xâm nhập được vào hệ thống, bước tiếp theo là làm sao để duy trì các xâm nhập này nhằm khai thác và xâm nhập tiếp trong tương lai. Một vài kỹ thuật như backboors, trojans... được sử dụng ở bước này. Một khi kẻ tấn công đã làm chủ hệ thống, chúng có thể gây ra những nguy hại cho hệ thống hoặc đánh cắp thông tin. Ngoài ra, chúng có thể sử dụng hệ thống này để tấn công vào các hệ thống khác như loại tấn công DDoS.
- Bước 5: **Che đậy, xóa dấu vết**: một khi kẻ tấn công đã xâm nhập và cố gắng duy trì xâm nhập. Bước tiếp theo là chúng phải làm sao xóa hết dấu vết để không còn chứng cứ pháp lí xâm nhập. Kẻ tấn công phải xóa các tập tin log, xóa các cảnh báo từ hệ thống phát hiện xâm nhập.

Ở bước **"Dò tìm"** và **"Xâm nhập"**, kẻ tấn công thường làm lưu lượng kết nối mạng thay đổi khác với lúc mạng bình thường rất nhiều. Đồng thời tài nguyên của hệ thống máy chủ bị ảnh hưởng đáng kể. Những dấu hiệu này rất có ích cho người quản trị mạng trong việc phân tích và đánh giá tình hình hoạt động của hệ thống mạng.

Hầu hết các cuộc tấn công đều tiến hành tuần tự 5 bước trên. Làm sao để nhận biết hệ thống mạng đang bị tấn công, xâm nhập ngay từ hai bước đầu tiên là hết sức quan trọng. Ở tại bước 3 là **"Xâm nhập"**, bước này không dễ dàng đối với kẻ tấn công. Do vậy, khi không thể xâm nhập được vào hệ thống để phá hoại có nhiều khả năng kẻ tấn công sẽ sử dụng tấn công từ chối dịch vụ (DoS hay DDoS) để ngăn cản không cho người dùng hợp lệ truy xuất tài nguyên hệ thống.

D. Hệ thống phát hiện và phòng chống xâm nhập

Phát hiện xâm nhập là một tập hợp các kỹ thuật và phương pháp dùng để dò tìm những hoạt động đáng nghi ngờ trên mạng. Một hệ thống phát hiện xâm nhập được định nghĩa là một tập hợp các công cụ, phương thức và tài nguyên giúp người quản trị xác định, đánh giá và báo cáo hoạt động không được phép trên mạng.

Phát hiện xâm nhập được xem là một tiến trình được quyết định khi một người đang cố gắng để xâm nhập hệ thống mạng trái phép. Hệ thống phát hiện xâm nhập sẽ kiểm tra tất cả các gói tin đi qua hệ thống và quyết định gói tin đó có vấn đề khả nghi hay không. Hệ thống phát hiện xâm nhập được trang bị hàng triệu tình huống để nhận dạng tấn công và được cập nhật thường xuyên. Chúng thực sự quan trọng và là lựa chọn hàng đầu để phòng thủ trong việc phát hiện và phòng chống xâm nhập mạng trong các hệ thống mạng hiện nay.

Việc nghiên cứu xây dựng hệ thống phát hiện và phòng chống xâm nhập đang được phát triển mạnh và còn phát triển mạnh mẽ trong thời gian tới. Các sản phẩm thương mại trên thị trường có chi phí rất lớn, vượt quá khả năng đầu tư của nhiều doanh nghiệp. Bên cạnh đó, các nghiên cứu về mã nguồn mở cũng đã được đầu tư nghiên cứu và triển khai. Có nhiều đề tài nghiên cứu liên quan đến IDS/IPS bằng mã nguồn mở chủ yếu tập trung vào Snort. Các nghiên cứu này chưa được áp dụng rộng rãi, còn tồn tại nhiều hạn chế như: do chương trình mã nguồn mở nên hầu hết không có giao diện thân thiện; thành phần báo động không được tích hợp sẵn, hoặc nếu có cũng chỉ qua giao diện console, hoặc qua giao diện Web chưa tạo được sự linh động và tiện dụng cho người quản trị mạng. Hầu hết các phần mềm mang tính đơn lẻ trong khi nhu cầu tích hợp nhiều tính năng giám sát khác để nâng cao hiệu quả sử dụng chưa được chú trọng và phát triển[1],[3],[4].

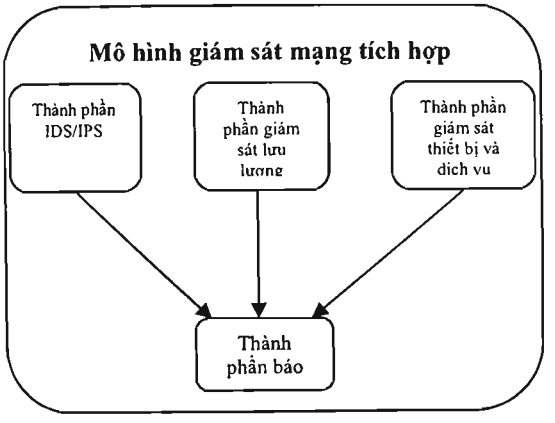
Hơn nữa, các dấu hiệu của các kiểu tấn công ngày một tinh vi phức tạp đòi hỏi hệ thống phát hiện và phòng chống xâm nhập phải được thường xuyên cập nhật những dấu hiệu mới. Người quản trị mạng còn có thể dựa vào những phân tích khác như những dấu hiệu bất thường về lưu lượng ra vào hệ thống, hoạt động của CPU, RAM... để có những phản ứng kịp thời. Bên cạnh đó, hệ thống báo động cũng cần triển khai mang tính chất đa dạng nhiều hình thức, linh động, tiện dụng thực sự hỗ trợ thiết thực cho người quản trị mạng.

Như vậy, một hệ thống giám sát hiệu quả cần thiết phải thiết lập tích hợp giữa các chức năng: phát hiện và phòng chống xâm nhập, giám sát lưu lượng, giám sát thiết bị và dịch vụ mạng, giám sát tài nguyên trên các thiết bị.

II. HỆ THỐNG GIÁM SÁT MẠNG

Nhu cầu về việc giám sát hệ thống mạng máy tính ngày càng cao. Bên cạnh việc theo dõi mạng để phát hiện truy cập trái phép, phòng chống xâm nhập còn là việc giám sát lưu lượng mạng, giám sát các thiết bị và dịch vụ mạng, giám sát nguồn tài nguyên trên hệ thống. Bên cạnh đó, hệ thống báo động phải được cài đặt linh hoạt và đa dạng.

Trong hệ thống giám sát mạng với những tính năng kể trên, tác giả đề xuất mô hình giám sát mạng tích hợp với các thành phần: thành phần phát hiện và phòng chống xâm nhập (IDS/IPS), thành phần giám sát lưu lượng, thành phần giám sát thiết bị và dịch vụ mạng và thành phần báo động. Các thành phần này được mô tả trong hình sau:



Hình 1. Mô hình giám sát mạng tích hợp

A. Thành phần phát hiện và phòng chống xâm nhập mạng

Hệ thống phát hiện xâm nhập (IDS) dùng để lắng nghe, dò tìm các gói tin qua hệ thống mạng để phát hiện những dấu hiệu bất thường trong mạng. Thông thường những dấu hiệu bất thường là những dấu hiệu của những cuộc tấn công xâm nhập mạng. IDS sẽ phát những tín hiệu cảnh báo tới người quản trị mạng.

Hệ thống phòng chống xâm nhập (IPS) là một phần mềm hoặc một thiết bị chuyên dụng có khả năng phát hiện xâm nhập và có thể ngăn chặn các nguy cơ mạng bị tấn công.

Hệ thống phòng chống xâm nhập là một kỹ thuật an ninh mới, kết hợp các ưu điểm của kỹ thuật tường lửa với hệ thống phát hiện xâm nhập có khả năng phát hiện sự xâm nhập và tự động ngăn chặn các cuộc tấn công đó. Hệ thống IDS/IPS thường được đặt ở phần biên mạng để bảo vệ tất cả các thiết bị trong mạng

Có hai phương pháp được dùng trong việc phân tích các sự kiện để phát hiện các vụ tấn công: phát hiện dựa trên các dấu hiệu và phát hiện sự bất thường.

- *Phát hiện dựa trên dấu hiệu*: Phương pháp này nhận dạng các sự kiện hoặc tập hợp các sự kiện phù hợp với một mẫu các sự kiện đã được định nghĩa là tấn công.
- *Phát hiện sự bất thường*: công cụ này thiết lập một hiện trạng các hoạt động bình thường và sau đó duy trì một hiện trạng hiện hành cho một hệ thống. Khi hai yếu tố này xuất hiện sự khác biệt, nghĩa là đã có sự xâm nhập.

Quá trình phát hiện có thể được mô tả bởi ba yếu tố cơ bản nền tảng sau:

- *Thu thập thông tin:* kiểm tra tất cả các gói tin trên mạng.
- *Phân tích:* phân tích tất cả các gói tin đã thu thập để cho biết hành động nào là tấn công.
- *Cảnh báo:* hành động cảnh báo cho sự tấn công được phân tích ở trên.

B. Thành phần giám sát lưu lượng

Một hệ thống IDS/IPS có thể phát hiện và phòng chống các cuộc tấn công xâm nhập mạng dựa vào các dấu hiệu tấn công được lưu trữ và cập nhập thường xuyên. Tuy nhiên cũng không tránh khỏi những trường hợp có những dạng tấn công mới mà những dấu hiệu chưa được biết tới.

Hệ thống giám sát lưu lượng hỗ trợ cho người quản trị mạng giám sát lưu lượng trao đổi giữa các thiết bị mạng. Nó hoạt động thời gian thực và thể hiện lưu lượng của các giao tiếp mạng (các giao tiếp của Router, Switch, Server,..), hoạt động của CPU, RAM một cách trực quan thông qua những đồ thị,... Điều này giúp người quản trị mạng có những phân tích tình trạng hoạt động của các thiết bị mạng trong hệ thống.

Ngoài ra, người quản trị có thể thiết lập những ngưỡng cảnh báo để kết hợp với hệ thống báo động để giúp người quản trị nhanh chóng có được những thông tin về những cuộc tấn công hay phát hiện những bất thường trong hệ thống. Những bất thường ở đây như là lưu lượng trên một giao tiếp mạng hoạt động bất thường hay CPU hoạt động quá tải (đặt ngưỡng cảnh báo), ...

C. Thành phần giám sát thiết bị và dịch vụ

Hệ thống giám sát thiết bị và dịch vụ có chức năng theo dõi trạng thái hoạt động của các thiết bị và các dịch vụ trong hệ thống mạng. Ngoài ra, nó còn có thể giám sát các tài nguyên trên các thiết bị như là dung lượng trống của các ổ cứng trên Server, kiểm tra trạng thái hoạt động của các cổng trên các Switch trung tâm...

Mọi hoạt động bất thường như có thiết bị ngưng làm việc hay dịch vụ mạng ngưng hoạt động, hay dung lượng ổ cứng trên các server còn quá ít (thiết lập ngưỡng theo dõi) sẽ được gửi cảnh báo tới người quản trị mạng.

D. Thành phần báo động

Hệ thống báo động là một trong những thành phần quan trọng trong hệ thống giám sát mạng. Hệ

thống báo động giúp người quản trị mạng nắm bắt được trạng thái hoạt động của hệ thống mạng. Đây cũng là một yêu cầu lớn đặt ra cho hệ thống giám sát mạng.

Trong bài viết này, tác giả đề xuất triển khai hệ thống báo động đa dạng qua nhiều hình thức: qua giao diện Web, E-mail, âm thanh và SMS.

Hệ thống báo động kết hợp với hệ thống dò tìm xâm nhập, hệ thống giám sát thiết bị và dịch vụ phát ra những tín hiệu cảnh báo đến người quản trị khi hệ thống có sự cố xâm nhập hay sự cố bất thường khác... Những thông tin từ thiết bị phát hiện xâm nhập hay hệ thống phát hiện những dấu hiệu bất thường được chuyển tới hệ thống báo động để phát cảnh báo tới người quản trị.

III. CÁC CÔNG CỤ NGUỒN MỞ HỖ TRỢ TRONG VIỆC GIÁM SÁT MẠNG

Có rất nhiều công cụ cho phép người quản trị mạng dò tìm những lỗ hổng trong hệ thống mạng đã nêu ở phần trên... Những công cụ này rất cần thiết để kiểm tra những lỗ hổng bảo mật trong hệ thống mạng.

Ở cấp độ cao hơn là tiến hành xây dựng một giải pháp toàn diện có tính khả thi cao nhằm giúp nhanh chóng cho các nhà quản trị mạng phát hiện ra những cuộc tấn công xâm nhập mạng, những sự cố trong quá trình hoạt động của hệ thống như một dịch vụ mạng ngưng hoạt động hay một thiết bị mạng (Router, Switch, Server) ngưng hoạt động, hay theo dõi luồng lưu lượng qua các kết nối, hoạt động của CPU, RAM, ...trong các thiết bị cần giám sát

Trong bài viết này này, tác giả đề xuất xây dựng một hệ thống giám sát mạng có tính trực quan, hệ thống báo động hoạt động đa dạng, nhanh chóng và tiện lợi, giúp người quản trị mạng nắm bắt hoạt động của hệ thống kịp thời, mọi lúc, mọi nơi, ... Mô hình kết hợp mà tác giả đề xuất là kết hợp của các phần mềm nguồn mở: Snort, Fwsnort, Cacti, Nagios và hệ thống báo động qua SMS Gnokii. Như một minh họa cho mô hình giám sát kết hợp IDS/IPS, giám sát lưu lượng, giám sát thiết bị, dịch vụ và thành phần cảnh báo.

Phần tiếp theo sẽ trình bày một số đặc điểm của Snort, Fwsnort, Cacti và Nagios trong việc giám sát những dấu hiện bất thường trong hệ thống mạng.

A. *Snort*

Snort là một phần mềm phát hiện xâm nhập mã nguồn mở hoạt động dựa trên các dấu hiệu cho phép giám sát, phát hiện những dấu hiện tấn công mạng [1] [2]. Snort được nhiều tổ chức phát triển và biến thành sản phẩm thương mại như Sourcefire, Astaro, ...

Các luật trên Snort có tính mở, cho phép người quản trị mạng tạo ra các luật mới.

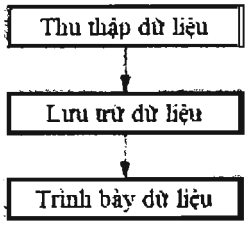
Hệ thống báo động trong mô hình thực nghiệm được cài đặt qua giao diện console, Web, Email và SMS

B. *Fwsnort*

Fwsnort hay cũng được gọi là *Firewall Snort* là phần mềm nguồn mở có chức năng chuyển các luật trong Snort thành các luật trong Iptables. Sự kết hợp này giúp cho những xâm nhập được Snort phát hiện sẽ được ngăn chặn bởi Iptables tạo thành hệ thống phát hiện và phòng chống xâm nhập [8].

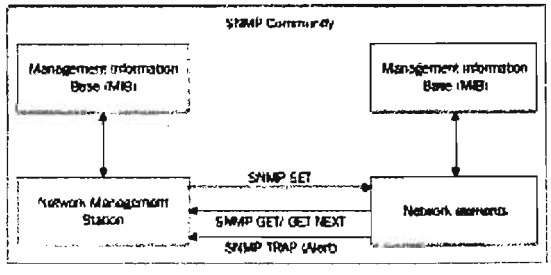
C. *Cacti*

Cacti là một phần mềm nguồn mở hàng đầu về việc giám sát các lưu lượng mạng. Cacti trong hệ thống đề xuất được dùng để giám sát lưu lượng qua các Switch trung tâm, Router và các Server trong hệ thống mạng.



Hình 2. Sơ đồ hoạt động của Cacti

Cacti thể hiện lưu lượng qua các đồ thị trực quan. Điều này giúp cho người quản trị theo dõi được sự bất thường trong hệ thống. Những bất thường này có thể là những dấu hiệu của tấn công xâm nhập hoặc sự quá tải của một số thiết bị mạng trong hệ thống. Cacti sử dụng giao thức SNMP để thu thập thông tin từ các thiết bị, lưu trữ thông tin và vẽ hình trên các đồ thị.[3]



Hình 3. Sơ đồ trao đổi thông tin SNMP giữa Cacti và một thiết bị [3]

Để tạo ra những đồ thị, Cacti cần thu thập dữ liệu từ các thiết bị giám sát thông qua giao thức SNMP [3][7]. Trong hệ thống mạng lớn với nhiều thiết bị cần giám sát thì dữ liệu thu thập nên được quản lý dựa vào cơ sở dữ liệu. Trong mô hình thực nghiệm của luận văn này, dữ liệu thu thập được từ SNMP được lưu trữ vào cơ sở dữ liệu MySQL.

Cacti có khả năng giám sát lưu lượng vào/ra các cổng của thiết bị cần theo dõi; giám sát tình trạng hoạt động của CPU và bộ nhớ. Cacti còn cho phép thể hiện sơ đồ mạng trực quan để theo dõi lưu lượng trao đổi giữa các thiết bị mạng.

Một đặc điểm quan trọng của Cacti là cho phép tích hợp nhiều nhiều phần mềm khác vào nó. Đây là

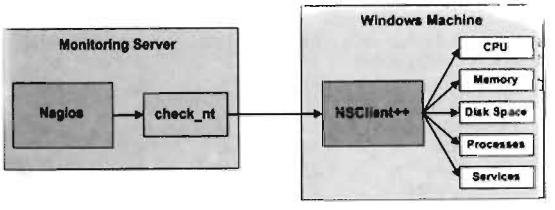
một đặc điểm quan trọng cho việc cài đặt hệ thống giám sát mạng tích hợp.

D. Nagios

Nagios là một phần mềm mã nguồn mở hàng đầu trong việc giám sát hoạt động của các thiết bị và các dịch vụ trong mạng. Nagios hỗ trợ trong việc giám sát hoạt động một số thiết bị trung tâm trong mạng như Server, Switch trung tâm, Router, ... Đồng thời, nó kết hợp với bộ phận phát cảnh báo qua SMS, Audio, Web nhằm phát cảnh báo trong trường hợp một thiết bị ngưng hoạt động hoặc một dịch vụ mạng ngưng hoạt động.

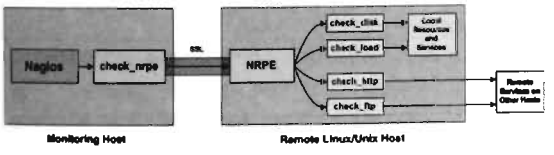
Nagios giám sát các thiết bị mạng thông qua các giao thức ICMP, SNMP, ... để theo dõi trạng thái hoạt động của các thiết bị. Đồng thời Nagios còn cho phép thiết lập cơ chế giám sát hoạt động của các dịch vụ mạng trên các thiết bị. Các dịch vụ phổ biến được giám sát như: HTTP, FTP, SMTP, POP3, DHCP, SSH, IMAP...[4][6]

Để giám sát các host Windows, chúng ta có thể sử dụng trực tiếp thông qua SNMP hoặc sử dụng phần mềm NSClient++ để lấy thêm nhiều thông tin hơn từ máy Windows [9].



Hình 4. Nagios theo dõi các dịch vụ trên Windows qua NSClient [9]

Cũng tương tự như vậy, chúng ta có thể sử dụng SNMP để giám sát các máy Linux qua việc cài đặt gói NRPE để giám sát host và các dịch vụ trên máy Linux [9].



Hình 5. Nagios giám sát các dịch vụ trên máy Unix/Linux qua NRPE[9]

E. Hệ thống báo động

Trong mô hình đề xuất, cài đặt các hình thức báo động qua các hình thức:

- Cảnh báo qua Web: được tích hợp trong khi cài đặt Snort, Cacti và Nagios
- Cảnh báo qua E-mail: sử dụng Sendmail
- Cảnh báo bằng âm thanh: tích hợp file âm thanh vào sự kiện phát cảnh báo.
- Cảnh báo qua SMS: sử dụng phần mềm nguồn mở Gnokii giao tiếp với GSM/GPRS modem.

Hình 6. Các thiết bị sử dụng trong việc cảnh báo SMS

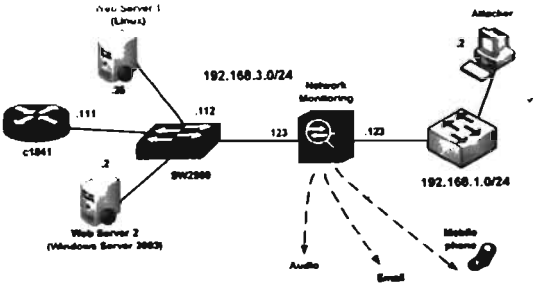
Gnokii là một phần mềm nguồn mở cho phép giao tiếp với thiết bị GSM/GPRS để phục vụ cho việc nhắn tin SMS. Cú pháp sử dụng đơn giản hỗ trợ cho việc nhắn tin qua SMS là:

printf <message> | gnokii --sendsms <telephone>

Cú pháp này được đưa vào chương trình Nagios, Cacti, Snort để hệ thống tự động gửi tin nhắn SMS khi có sự cố xảy ra.

IV. CÀI ĐẶT MÔ HÌNH ĐỀ XUẤT KẾT HỢP SNORT, FWSNORT, CACTI VÀ NAGIOS

A. Mô hình cài đặt



Hình 7. Mô hình mạng thực nghiệm

Trong mô hình thực nghiệm này, máy làm chức năng giám sát chạy hệ điều hành CentOS. Trên đó cài đặt hệ thống giám sát tích hợp và quản lý với một giao diện chung trên Cacti. Các thành phần được tích hợp và giao diện quản lý của Cacti. Hệ thống chia thành bốn khối chức năng chính:

- Bộ phận phát hiện xâm nhập (Snort)
- Bộ phận phòng chống xâm nhập (FwSnort)
- Bộ phận giám sát trạng thái hoạt động của các host và services (Nagios)
- Bộ phận báo động: báo động bằng âm thanh, Web, qua email và SMS (GSM/GPRS modem)

B. Cài đặt các thành phần

Trong phần thực nghiệm này các thành phần được cài đặt riêng sau đó được tích hợp vào trong giao diện của Cacti.

Sau đây là một số đoạn mã nguồn tích hợp Snort, Nagios vào giao diện Cacti.

Các thông số trong tập tin *global.php* nằm trong *(/var/www/cacti/plugin/)*

```
$plugins = array();
$plugins[] = 'update'; //cập nhập các phiên bản mới
$plugins[] = 'settings'; //
$plugins[] = 'manage';
$plugins[] = 'realtime'; //xử lý thời gian thực
$plugins[] = 'npc'; // tích hợp Nagios
$plugins[] = 'base'; // tích hợp giao diện Web cho Snort
$plugins[] = 'weathermap'; // giám sát lưu lượng
```

Định nghĩa việc giám sát thiết bị (host) và dịch vụ (service) trong Nagios

```
define host {
        host_name   winserver     ; đặt tên cho Host
        alias My Favorite Host    ; bí danh
        address 192.168.1.254     ; IP của thiết bị cần giám sát
        check_command check-host-alive      ; Kiểm tra trạng thái host
        max_check_attempts  5  ; số lần kiểm tra trước khi kết luận
        contact_groups  admins  ; group của người quản trị
        notification_interval  30  ; thời gian giữa các lần kiểm tra
(phút)
        notification_period  24x7; thời gian hoạt động của hệ thống
báo
        notification_options  d,u,r ; phát báo động khi host (u: down,
                                    ; u: unreachable, r: recovery)
}
```

```
define service{
        use                     generic-servic
        host_name               winserver
        service_description     HTTP        ; Mô tả dịch vụ cần giám
sát
        check_command           check_http  ; Kiểm tra trạng thái
HTTP
        notifications_enabled   1           ; bật tính năng phát báo
động
}
```

Thiết lập cảnh báo qua SMS khi dịch vụ cần giám sát gặp sự cố:

Xác định email và số điện thoại để gửi cảnh báo trong */usr/local/nagios/etc/object/contacts.cfg*

```
Define contact {
    contact_name        nagiosadmin
    use                 generic-contact
    alias               Nagios Admin
    email               chinhhn@fit.hcmute.edu.vn
    pager               0983929445
```

Định nghĩa cú pháp lệnh báo động trong */usr/local/nagios/etc/object/commands.conf.*

```
#notify-service-by-sms

Define command{
    Command_name      notify-service-by-sms
    Command_line  /usr/bin/printf  "%.120"
"Nagios -- $NOTIFICATIONTYPE$
$HOSTALIAS$/$SERVICEDESC$ is $SERVICESTATE$
($OUTPUT$)" | /usr/local/bin/gnokii -sendsms
$CONTACTPAGER$
    }
```

```
#notify-host-by-sms
Define command{
    Command_name      notify-host-by-sms
    Command_line  /usr/bin/printf  "%.120"
"Nagios -- $NOTIFICATIONTYPE$   $HOSTALIAS$ is
$HOSTSTATE$ ($OUTPUT$)" |
/usr/local/bin/gnokii -sendsms $CONTACTPAGER$

}
```

Thực hiện việc chuyển đổi các luật trong Snort thành các luật trong Iptables.

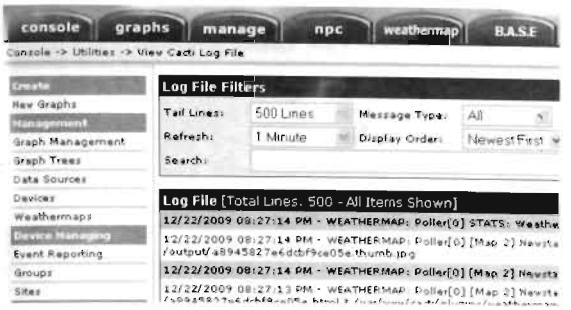
```
[iptables fw]# fwsnort

    Snort Rules File          Success   Fail    Ipt_apply Total
[+] attack-responses.rules    15        2       0         17
[+] backdoor.rules            62        7       1         69
[+] bad-traffic.rules         10        3       0         13
[+] bleeding-all.rules        1075      573     5         1649
[+] exploit.rules             31        43      0         74
[+] web-cgi.rules             256       92      0         348
[+] web-client.rules          7         10      0         17
[+] web-coldfusion.rules      35        0       0         35
[+] web-frontpage.rules       34        1       0         35
[+] web-iis.rules             103       11      0         114
[+] web-misc.rules            265       61      0         326
[+] web-php.rules             78        48      0         126
[+] x11.rules                 2         0       0         2

                              2725      1761    [illegible]   4486
[+] Generated iptables rules for 2725 out of 4486 signatures: 60.74%
[+] Found 91 applicable snort rules to your current iptables policy.
[+] Logfile:          /var/log/fwsnort.log
[+] Iptables script: /etc/fwsnort/fwsnort.sh
```

Cài đặt chế độ lập lịch cho chương trình trong */etc/cron.d*

```
*/1 * * * * cactiuser php /var/www/cacti/poller.php> /dev/null
2>&1
*/1 * * * * /var/snortnotify-v2.1/SnortNotify.pl
```

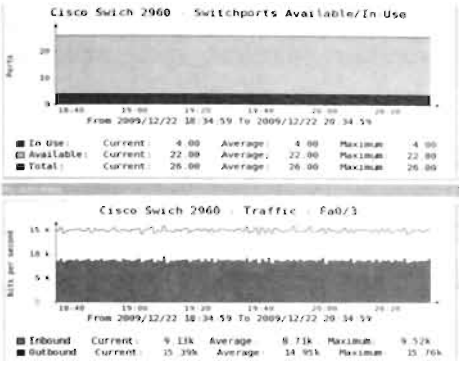
V. KẾT QUẢ THỰC NGHIỆM

Hệ thống giám sát mạng được tích hợp các tính năng giám sát từ Cacti (Console, Manage, Weathermap), Nagios (npc), Snort (BASE).



Hình 8. Các module tích hợp trên nền Cacti

Theo dõi trạng thái hoạt động và lưu lượng của Switch Cisco.



Hình 9. Theo dõi hoạt động của Cisco Switch qua đồ thị

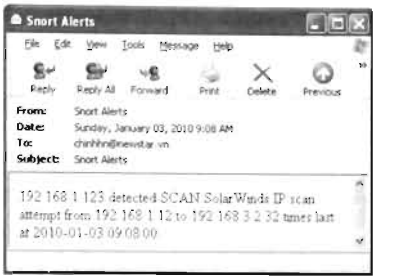
Theo dõi tình trạng hoạt động (up/down) của các thiết bị.

Hình 10. Theo dõi các trạng thái các thiết bị và phát báo động bằng âm thanh

Theo dõi trạng thái các dịch vụ mạng trong từng thiết bị và mức độ sử dụng một số tài nguyên trên thiết bị như RAM, CPU, đĩa cứng, ... thông qua 'npc'

Hình 11. Theo dõi một số dịch vụ trên các thiết bị

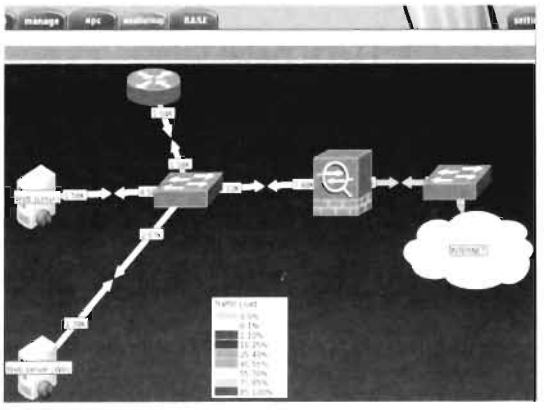
Kiểm tra hoạt động của hệ thống báo động khi dùng phần mềm SolarWinds quét IP đến máy bên trong mạng.



Hình 12. Cảnh báo gửi qua Email khi dùng chương trình SolarWinds scan IP

Hình 13. Cảnh báo gửi qua SMS khi dùng chương trình SolarWinds scan IP

Theo dõi lưu lượng mạng giữa các thiết bị mạng trên đồ thì trực quan dùng thành phần Weathermap.



Hình 14. Theo dõi các lưu lượng mạng giữa các thiết bị

Trong phần thực nghiệm này, tác giả sử dụng bộ luật của Snort trong việc phát hiện tấn công xâm nhập mạng.

Bên cạnh dựa vào dấu hiệu nhận dạng của hệ thống phát hiện và phòng chống xâm nhập, người quản trị mạng còn có thể phân tích lưu lượng mạng trên các thiết bị để phát hiện ra những dấu hiệu bất thường trên hệ thống (có thể là những tấn công xâm nhập mà thành phần IDS/IPS chưa phát hiện ra) và phát cảnh báo qua nhiều hình thức (âm thanh, Web, SMS) đến người quản trị mạng.

Phần thực nghiệm này chỉ là để minh họa cho hoạt động của thành phần phát hiện và phòng chống xâm nhập mạng kết hợp với thành phần phân tích lưu lượng, thành phần giám sát thiết bị và dịch vụ và thành phần cảnh báo tạo nên một hệ thống giám sát mạng tích hợp hỗ trợ cho người quản trị mạng. Trong khi các sản phẩm thương mại có những tính năng chuyên dụng cho từng chức năng riêng biệt như IDS/IPS, giám sát,... thì có thể coi sự kết hợp này là một framework cho một hệ thống giám sát mạng tích hợp.

VI. KẾT LUẬN

Trong bài viết này, tác giả đề xuất mô hình xây dựng một hệ thống giám sát tích hợp với các chức năng: phát hiện và phòng chống xâm nhập, giám sát lưu lượng, thiết bị, dịch vụ, tài nguyên các thiết bị (CPU, dung lượng ổ đĩa, RAM,...). Để minh họa cho mô hình đề xuất này, tác giả đã cài đặt tích hợp kết hợp các công cụ nguồn mở *Snort*, *Fwsnort*, *Cacti*, *Nagios* và *GSM/GPRS modem*.

Bài viết này giới thiệu một giải pháp trong việc giám sát hệ thống mạng không những giúp phát hiện các cuộc tấn công xâm nhập mạng mà còn giúp giám sát hoạt động của hệ thống một cách trực quan, nhanh chóng, tiện lợi. Hệ thống báo động qua Web, E-mail, báo động bằng âm thanh (audio) và SMS tạo nên sự đa dạng, linh hoạt cho phép người quản trị mạng theo dõi hệ thống ở mọi lúc, mọi nơi. Giúp nhanh chóng phát hiện những sự cố để có những giải pháp kịp thời.

TÀI LIỆU THAM KHẢO

[1] D. Andrew R. Baker, Joel Esler "Snort Intrusion Detection and Prevention Toolkit", Syngress, 2007

[2] Rafeeq UR Rehman,"Intrusion Detection With Snort Advanced IDS Techniques using Snort, Apache, MySQL, PHP, and ACID", Prentice Hall PTR, 2003

[3] Dinangkur Kundu, S.M. Ibrahim Lavlu, "Cacti 0.8 Network Monitoring" PACKT Publishing, 2009

[4] Wojciech Kocjan, "Learning Nagios 3.0", PACKT Publishing, 2009

[5] Max Schubert, Derrick Bennett, "Nagios 3 Enterprise Network Monitoring Including Plug-ins and Hardware Devices", Syngress, 2008

[6] David Josephsen,"Building a Monitoring Infrastructure with Nagios", Prentic Hall, 2007

[7] Douglas Mauro, Kevin Schmidt, "Essential SNMP 2nd Edition", Oreilly, 2005

[8] Michael Rash, "Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort", No Starch Press, 2007

[9] Ethan Galstad," NRPE Documentation", Nagios Press, 2007