ISSN 2354-0575

NGHIÊN CỨU, XÂY DỰNG MÔ HÌNH GIÁM SÁT HOẠT ĐỘNG VÀ AN TOÀN HỆ THỐNG MẠNG CHO CÁC TRƯỜNG ĐẠI HỌC SỬ DỤNG NGUỒN MỞ

Nguyễn Thị Thanh Tú[1], **Nguyễn Huy Hùng**[1], **Nguyễn Minh Quý**[2]
1 Trường Đại học Bách khoa Hà Nội
2 Trường Đại học Sư phạm Kỹ thuật Hưng Yên

Ngày nhận: 26/1/2016
Ngày xét duyệt: 10/3/2016

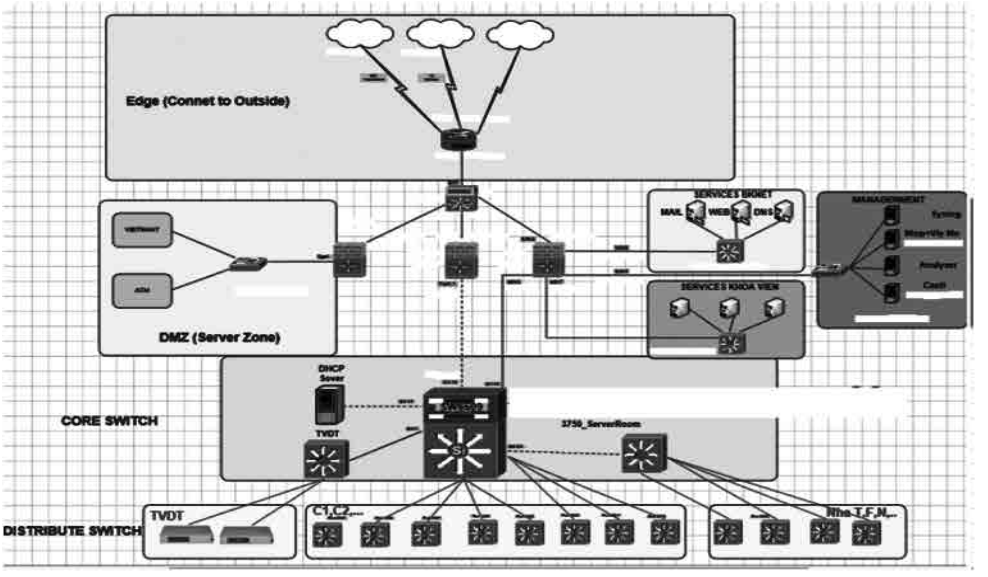
Tóm tắt:

Khoảng 5 năm trở lại đây, các mạng máy tính của các Trường Đại học ở Việt Nam trong đó có mạng Bách khoa Network đã có những bước phát triển mạnh mẽ về quy mô và đóng vai trò ngày càng quan trọng trong hoạt động trao đổi thông tin, hoạt động nghiên cứu tại các trường đại học. Tuy nhiên, do đặc thù kinh tế và lịch sử, các mạng máy tính Campus thường không đồng bộ, các thiết bị được bổ sung dần dần với nhiều chủng loại đến từ các hãng khác nhau. Điều này dẫn đến hiệu năng hoạt động của mạng bị hạn chế, việc vận hành, kiểm soát hệ thống gặp nhiều khó khăn do sự không đồng bộ giữa các thiết bị. Hiện nay, chưa có những nghiên cứu, đánh giá và giải pháp để tối ưu hóa hiệu năng sử dụng của hệ thống phù hợp với đặc thù của các mạng này. Từ đó, chúng tôi nghiên cứu đề xuất và xây dựng giải pháp tối ưu hóa hoạt động của các mạng này để có thể áp dụng cho hệ thống mạng của các trường Đại học.

Từ khóa: *CactiEZ, Bảo mật, IDS, SNMP, Rsyslog.*

1. Đặt vấn đề

Hiện nay, Đại học Bách khoa Hà Nội (Trường ĐHBK HN) có cơ sở vật chất với khu khuôn viên bao gồm các phòng ban và giảng đường, cộng thêm các cơ sở nghiên cứu nằm rải rác xung quanh khu vực Lê Thanh Nghị, Tạ Quang Bửu. Số lượng cán bộ công nhân viên và sinh viên rất lớn với chừng hơn 2000 cán bộ và hàng chục nghìn sinh viên. Để từng bước đáp ứng nhu cầu sử dụng mạng ngày một tăng cao của cán bộ nhân viên và sinh viên, hệ thống mạng Bách khoa Network - BKNET đã được triển khai và mở rộng qua nhiều năm với hàng trăm thiết bị mạng như Router, Switch, Server... với nhiều chủng loại khác nhau, cùng hàng nghìn nút mạng tỏa đi khắp mọi ngóc ngách trong khuân viên rộng lớn. Hệ thống này hàng ngày đang phải chịu tải hàng nghìn lượt truy cập Internet tại trường, và cũng thường xuyên phải hứng chịu các cuộc tấn công mạng với xu hướng ngày một gia tăng. Bên cạnh đó, thời gian vừa qua, trong bối cảnh tranh chấp, xung đột lãnh thổ, văn hóa, tôn giáo. Trên môi trường mạng, Việt Nam là một trong những nước chịu ảnh hưởng của những cuộc tấn công mạng có tổ chức và quy mô lớn.



Hình 1. *Mô hình mạng của trường đại học*

Các cuộc tấn công vào các hệ thống thông tin của cơ quan tổ chức nhà nước nhằm đạt được những mục đích chính trị, gây mất uy tín của của cơ quan tổ chức, gây gián đoạn trong công tác quản lý điều hành. Đặc biệt các cuộc tấn công có dấu hiệu diễn ra trong phạm vi và quy mô lớn trong các dịp nghỉ lễ của Việt Nam như: trong khoảng thời gian từ 28/8 - 04/9/2014, nhằm vào kỳ nghỉ Lễ Quốc khánh, nhiều trang thông tin điện tử của Việt Nam bị nhóm tin tặc Trung Quốc tấn công. Theo con số thống kê của Bộ Thông tin & Truyền thông, có khoảng 300 websites Việt Nam bị tấn công trong khoảng thời gian này, trong số đó có cả các website của cơ quan nhà nước (tên miền .gov.vn), của các tổ chức xã hội và của các tổ chức, doanh nghiệp khác.

Số lượng các máy tính ở Việt Nam là thành viên của mạng máy tính ma (Botnet) ngày càng lớn. Các máy tính này thường bị điều khiển để gửi thư rác, tin nhắn rác, tấn công từ tối dịch vụ phân tán (DDoS) quy mô lớn. Một số số liệu đáng chú ý về an toàn an ninh thông tin tại Việt Nam qua báo cáo ATTT của các công ty an toàn thông tin uy tín thế giới trong năm 2013-2014 như sau (Theo báo cáo của Arbor từ tháng 11 năm 2014 đến tháng 10 năm 2014): (1) Tổng số cuộc tấn công DDoS phải hứng chịu là 861. (2) Băng thông tối đa của lưu lượng tấn công là 43,93Gbps, tốc độ tối đa là 6,985M/s. (3) Quý 2 năm 2014, Việt Nam hứng chịu cuộc tấn công có băng thông lớn nhất là 43,93Gbps sử dụng hình thức tấn công TCP SYN Flood tới dịch vụ Web trong khoảng thời gian 19 phút, 14 giây. (4) Quý 3 năm 2014, Việt Nam hứng chịu cuộc tấn công có băng thông lớn nhất là 13Gbps bằng cách lợi dụng điểm yếu bảo mật của giao thức, dịch vụ NTP để tấn công tới dịch vụ Web trong khoảng thời gian 23 phút, 44 giây.

Từ hiện trạng trên cùng với hệ thống mạng ngày càng được mở rộng nhanh chóng nhưng thiếu tính đồng bộ thống nhất về thiết bị và công nghệ, đã tạo ra rào cản cho việc triển khai các hệ thống quản lý và giám sát mạng với số lượng lớn thiết bị. Từ đó dẫn đến việc phải nghiên cứu, xây dựng mô hình giám ats hoạt động và an toàn hệ thống mạng cho các Trường đại học sử dụng nguồn mở với các nhiệm vụ như sau:

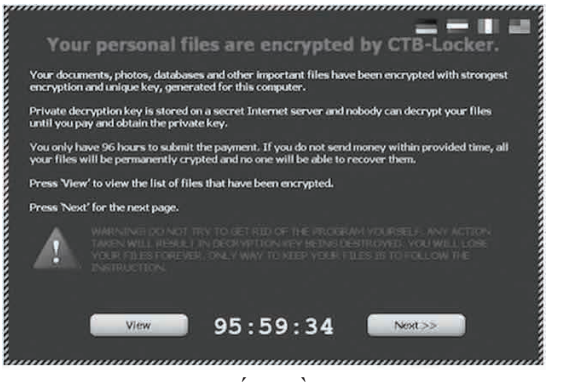
Giám sát mạng giúp người quản trị kịp thời phát hiện ra các trục trặc, sự cố từ đó nhanh chóng xử lý khắc phục.

Giám sát và hỗ trợ phân tích tính toán phân chia tải để tăng hiệu năng sử dụng tài nguyên và băng thông trên toàn bộ hệ thống, tránh được hiện tượng thắt cổ chai cục bộ, đảm bảo cho hệ thống hoạt động được thông suốt với hiệu năng cao nhất [1, 2].

Giám sát và phát hiện thâm nhập giúp người quản trị phát hiện ra các thâm nhập trái phép nhằm phá hoại hệ thống máy tính hay đánh cắp thông tin. Từ đó cung cấp các chức năng thiết yếu giúp người quản trị có thể cô lập hay vô hiệu hóa các cuộc thâm nhập trái phép hay tấn công phá hoại, giúp đảm bảo an toàn cho hoạt động trao đổi thông tin trong toàn hệ thống [3, 4]. Theo khảo sát thực tế tại Trường ĐHBK HN, một số vấn đề mà hệ thống mạng BKNET gặp phải là:

- Hệ thống mạng thường xuyên bị gián đoạn cục bộ do sự hỏng hóc của các thiết bị mạng hay tắc nghẽn đường truyền nhưng không được phát hiện kịp thời và khắc phục hiện quả. Có những hiện tượng như hỏng hóc chỉ được biết đến khi được báo cáo từ các đơn vị bị ảnh hưởng bởi sự cố báo lên, từ đó điều cử nhân viên đi điều tra thăm dò. Các tắc nghẽn cục bộ thường không được giám sát và đánh giá theo thời gian thực để có điều chỉnh chia tải kịp thời, vì thế sự cố này xảy ra khá thường xuyên khi có sự gia tăng đột biến lượng người dùng hay lượng thông tin trao đổi trên một nút mạng, hay do virus mạng tấn công. Hiện nay, cách khắc phục sự cố này mang tính thủ công chậm chạp, nó chỉ được thực hiện sau khi có phản ảnh từ các đơn vị, sau đó các kỹ thuật viên bằng chuyên môn nghiệp vụ của mình sẽ cố gắng điều tra và đánh giá tình hình, để từ đó cùng bàn thảo và đưa ra giải pháp khắc phục. Quá trình này thường mất rất nhiều thời gian và gây trở ngại lớn cho công tác thông tin liên lạc của một số đơn vị trong phạm vị ảnh hưởng của sự cố.

- Hệ thống server dịch vụ bị chiếm quyền điều khiển, từ đó những kẻ tấn công lợi dụng tên miền của Trường để đi tấn công các server khác, làm cho hệ thống tên miền của trường bị liệt vào blacklist. Tạo nên một số tình trạng xấu như hệ thống mail của trường khi gửi mail đến các hệ thống mail khác có thể bị chặn lại hoặc bị đẩy vào hòm thư rác, làm gián đoạn việc trao đổi thông tin liên lạc. Những hiện tượng như trên sẽ gây ảnh hưởng lớn, *đôi khi là khá nghiêm trọng*, đến các hoạt động quản lý điều hành trong trường và hoạt động trao đổi thông tin chuyên môn của giảng viên và các nhà nghiên cứu của trường với các đối tác bên ngoài.



Hình 2. *Virus tống tiền (Ransomware)*

- Server website của các Khoa, viện bị chiếm quyền điều khiển từ đó kẻ tấn công sẽ phát tán virus dựa trên các truy cập đến server đó. Các nguồn lây từ virus có thể chiếm đoạt thông tin của người dùng, lợi dụng các máy tính bị nhiễm virus đi tấn công các server khác trên hệ thống mạng Internet. Các virus đó cũng có khả năng mã hóa các file tài liệu trên máy tính của người dùng (word, excel …).

Có thể thấy những vấn đề trên không phải của riêng mạng BKNET mà nó là phổ biến cho các mạng campus của các trường đại học lớn và có lịch sử phát triển hệ thống mạng qua nhiều giai đoạn lịch sử mà thiếu tính đồng bộ về trang thiết bị công nghệ. Điểm yếu của các hệ thống mạng dạng này là khó khăn trong quản lý giám sát vì thiếu tính đồng bộ để có thể triển khai các hệ thống thiết bị giám sát chuyên dụng của các hãng một cách hiệu quả. Bởi các thiết bị này chỉ thật sự phát huy hiệu quả khi được triển khai trên một hệ thống thiết bị đồng bộ do chính hãng này sản xuất, mặt khác giá thành các thiết bị này cũng là một vấn đề đối với ngân sách.

Từ thực tiễn đó đã đặt ra vấn đề cần nghiên cứu phát triển một hệ thống quản lý giám sát cho hệ thống mạng BKNET nói riêng hay mạng campus nói chung. Đảm bảo hệ thống được giám sát chặt chẽ theo thời gian thực, phát hiện và phòng ngừa ngăn chặn sự tấn công mạng, có khả năng dự báo hay phát hiện tắc nghẽn mạng và trợ giúp quản lý phân chia tải hợp lý để nâng cao hiệu năng sử dụng băng thông. Đồng thời, phát hiện các gián đoạn trên hệ thống mạng và đưa ra các chuẩn đoán hợp lý giúp các kỹ thuật viên có thể nhanh chóng khắc phục, đáp ứng nhu cầu thông tin liên lạc an toán nhanh chóng và thông suốt trên toàn hệ thống.

Hiện nay, chưa có một hệ thống phần mền quản lý và giám sát mạng nào toàn diện, đáp ứng đầy đủ những yêu cầu nói trên. Chúng hoặc chỉ có chức năng giám sát mà thiếu chức năng quản lý phân chia tài nguyên, phân chia cân bằng tải. Về chức năng giám sát thì cũng mạnh yếu trên từng khía cạnh chứ không đáp ứng được đầy đủ các yêu cầu để triển khai giám sát và ngăn chặn một cách phù hợp và hiệu quả trên hệ thống mạng campus ở Việt Nam. Từ thực trạng này, dẫn đến nhu cầu cấp thiết cần xây dựng và tích hợp một hệ thống giám sát mạng toàn diện phù hợp với mạng các trường đại học ở Việt Nam, cũng như mạng của BKNET.

2. Đề xuất và xây dựng giải pháp cho hệ thống mạng BKNET

Qua quá trình nghiên cứu, chúng tôi nhận thấy một hệ thống quản lý giám sát cho mạng campus với đặc thù riêng ở Việt nam phải được hình thành trên cơ sở tích hợp 2 thành phần hạt nhân: (1) Hệ thống giám sát, phân tích, cảnh báo tấn công mạng. Và (2) Hệ thống giám sát, quản lý băng thông mạng.

2.1. Hệ thống giám sát, phân tích, cảnh báo tấn công mạng

Khi các sự kiện nào đó xảy ra trên mạng, các thiết bị mạng đã có các cơ chế để thông báo cho quản trị viên với những thông báo chi tiết về hệ thống. Các thông điệp này có thể là không quan trọng hoặc quan trọng. Quản trị viên có nhiều sự lựa chọn để lưu trữ, diễn tả, hiển thị các thông báo, và được cảnh báo về những thông báo rằng có thể có ảnh hưởng lớn nhất về hạ tầng mạng. Phương pháp phổ biến nhất để truy cập các thông báo của hệ thống thiết bị cung cấp mạng là sử dụng một giao thức gọi là syslog.

Syslog là một thuật ngữ dùng để mô tả một tiêu chuẩn. Nó cũng được sử dụng để mô tả các giao thức được phát triển cho tiêu chuẩn đó. Giao thức syslog được phát triển cho các hệ thống UNIX trong những năm 1980, nhưng lần đầu tiên được ghi nhận như RFC 3164 bởi IETF trong năm 2001. Syslog sử dụng cổng UDP 514 để gửi tin nhắn thông báo sự kiện qua mạng IP cho người thu gom thông báo, như minh họa trong hình [5, 6].

Nhiều thiết bị mạng hỗ trợ syslog, bao gồm: routers, switches, application servers, firewalls, và các thiết bị mạng khác. Giao thức syslog cho phép các thiết bị mạng để gửi tin nhắn hệ thống của họ trên mạng đến các máy chủ syslog. Có thể xây dựng một (OOB) mạng đặc biệt out-of-band cho mục đích này. Có những gói phần mềm máy chủ syslog khác nhau cho Windows và UNIX. Nhiều trong số đó là phần mềm miễn phí [7, 8].

Dịch vụ ghi syslog cung cấp ba chức năng chính: (1) Khả năng thu thập thông tin đăng nhập để theo dõi và xử lý sự cố. (2) Khả năng chọn các loại thông tin đăng nhập mà bị ghi lại. (3) Khả năng xác định những điểm đến của thông điệp syslog bị ghi lại.Từ đó hệ thống chúng tôi muốn triển khai tại Trường ĐHBK là ***"Thiết lập hệ thống Log Server sử dụng Rsyslog và LogAnalyzer trên mã nguồn mở Linux 6.4/6.5"***.

Hệ thống này dựa trên thuật ngữ SIEM (Security Information and Event Management) hay còn gọi là hệ thống bảo mật thông tin và quản lý sự kiện là thuật ngữ của dịch vụ và sản phẩm phần mềm kết hợp của quản lý thông tin bảo mật (SIM) và quản lý sự kiện bảo mật (SEM). Công nghệ SIEM cung cấp phân tích thời gian thực tạo các cảnh báo về bảo mật bằng phần cứng mạng và các ứng dụng. Trong đó hệ thống Log Analyzer là hệ thống SEM sẽ thu thập log từ các thiết bị máy chủ linux, window dựa vào đó để phân tích và đưa ra các cảnh báo cho người quản trị mạng để kịp thời khắc phục sự cố và sửa các lỗi về bảo mật nhằm nâng cao tính an toàn, ổn định của hệ thống mạng.

2.2. Hệ thống giám sát, quản lý băng thông mạng

Hiện nay, Cacti và Nagios Core là hai giải pháp mã nguồn mở hoàn toàn miễn phí với nhiều chức năng mạnh mẽ cho phép quản lý băng thông kết nối, tình trạng hoạt động của các thiết bị, trạng thái của dịch vụ trong hệ thống mạng. Nhiều tính năng trên Nagios Core và Cacti còn được đánh giá cao hơn các sản phẩm thương mại.

Tuy vậy, trong cả hai phần mềm đều có những nhược điểm riêng của mình nhưng khi kết hợp cả hai lại sẽ tạo thành một giải pháp mã nguồn mở gần như hoàn chỉnh. Chính vì vậy các nhà phát triển trên thế giới đã nghiên cứu và ra đời CactiEZ, giải pháp mã nguồn mở kết hợp cả hai phần mềm Cacti và Nagios Core tạo nên sự hoàn chỉnh cho hệ thống quản lý và giám sát mạng [10]. Các hệ thống phát hiện thâm nhập hiện nay hoạt động độc lập với hệ thống giám sát mạng trong khi hai hệ thống này có sự bổ sung cho nhau, là các thành phần chính trong quản trị mạng. Việc xây dựng hệ thống phát hiện thâm nhập phù hợp với mạng Campus quy mô lớn và tích hợp với hệ thống giám sát mạng là nhu cầu đang ngày một lớn.

CactiEZ được phát triển và sản xuất bởi Jimmy Conner, một nhà phát triển đam mê với Cacti và Plugins của nó. CactiEZ khởi đầu là một dự án tạo một phần mềm đơn giản để triển khai máy chủ Cacti, Nagios một cách nhanh chóng nhất và dễ dàng cài đặt. CactiEZ hoàn thành tự động hóa với cấu hình tối thiểu cần thiết là mục tiêu chính của dự án. Kể từ đó nó đã phát triển về phạm vi và cách sử dụng, và đã được sử dụng bởi nhiều công ty có quy mô lớn và cả quy mô nhỏ để triển khai các máy chủ Cacti [9]. CactiEZ là sự kết hợp của hai hệ thống mã nguồn mở tốt nhất là Cacti và Nagios. Phát huy tất cả các ưu điểm và bù trừ những nhược điểm cho nhau tạo ra một hệ thống quản lý mạng hoàn hảo.

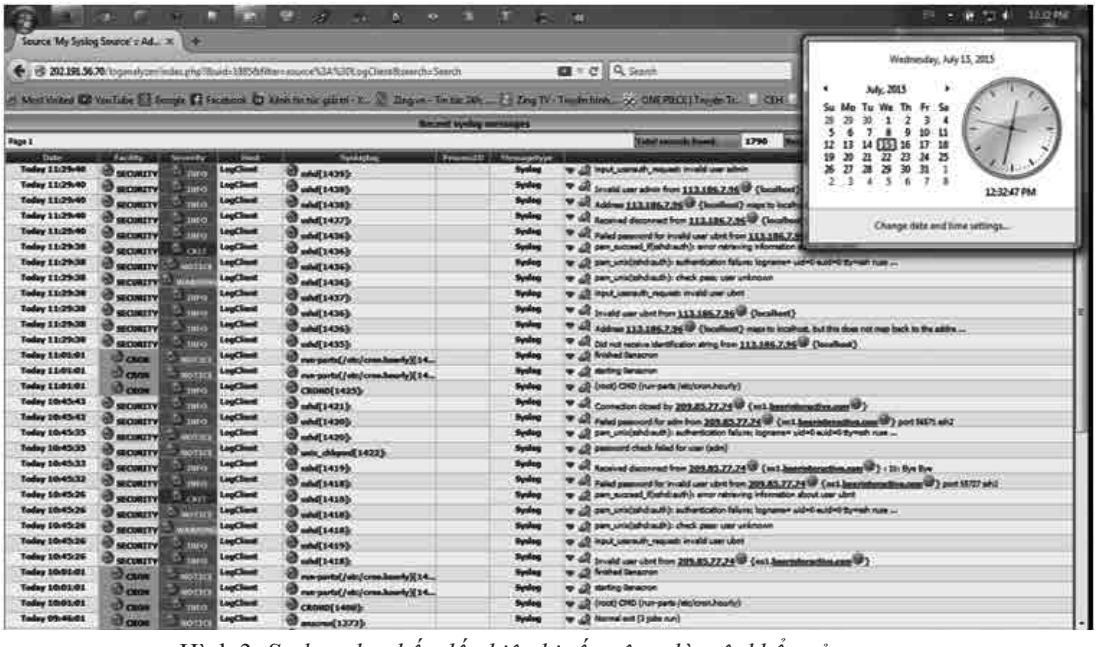
- Lên kế hoạch và cấu hình thiết bị: (1) Xây dựng hệ thống giám sát mạng cho mạng với quy mô đến tất cả port trên thiết bị. (2) Xây dựng hệ thống giám sát hiệu năng của mạng cho phép đo lường các tham số hiệu năng như băng thông, CPU, độ sẵn sàng của các thiết bị... (3) Xây dựng, phát triển hệ thống tương tác, cảnh báo sự cố kịp thời cho người quản trị mạng thông qua các con đường như email, SMS.

- Áp dụng thử nghiệm trên một vùng mạng nhỏ, đánh giá. Sau đó, áp dụng vào môi trường mạng BKNET, thu thập và so sánh các kết quả: (1) Ban đầu tiến hành thử nghiệm ngay trên vùng mạng của Trung tâm Mạng Thông tin. (2) Sau đó cài đặt trên tất cả các thiết bị có thể sử dụng các giao thức quản lý như SNMP cho Router/Switch, NRPE cho Linux/Unix, NSClient++ cho Windows. (3) Vẽ sơ đồ băng thông tổng thể toàn trường ĐHBK Hà Nội.

- Đánh giá chung về hiệu quả với môi trường thực tế, từ đó đưa ra phương hướng phát triển trong tương lai: (1) Hiệu quả của hệ thống sẽ được đánh giá thông qua các số liệu thống kê và so sánh với một số hệ thống điển hình khác. (2) Nghiên cứu, xây dựng hệ thống tính toán mức độ sử dụng tài nguyên mạng của từng người dùng, từng nhóm người dùng trong mạng. (3) Nghiên cứu, xây dựng hệ thống phát hiện các thâm nhập trái phép.

3. Kết quả đạt được

3.1. Chức năng phân tích, giám sát, cảnh báo tấn công mạng

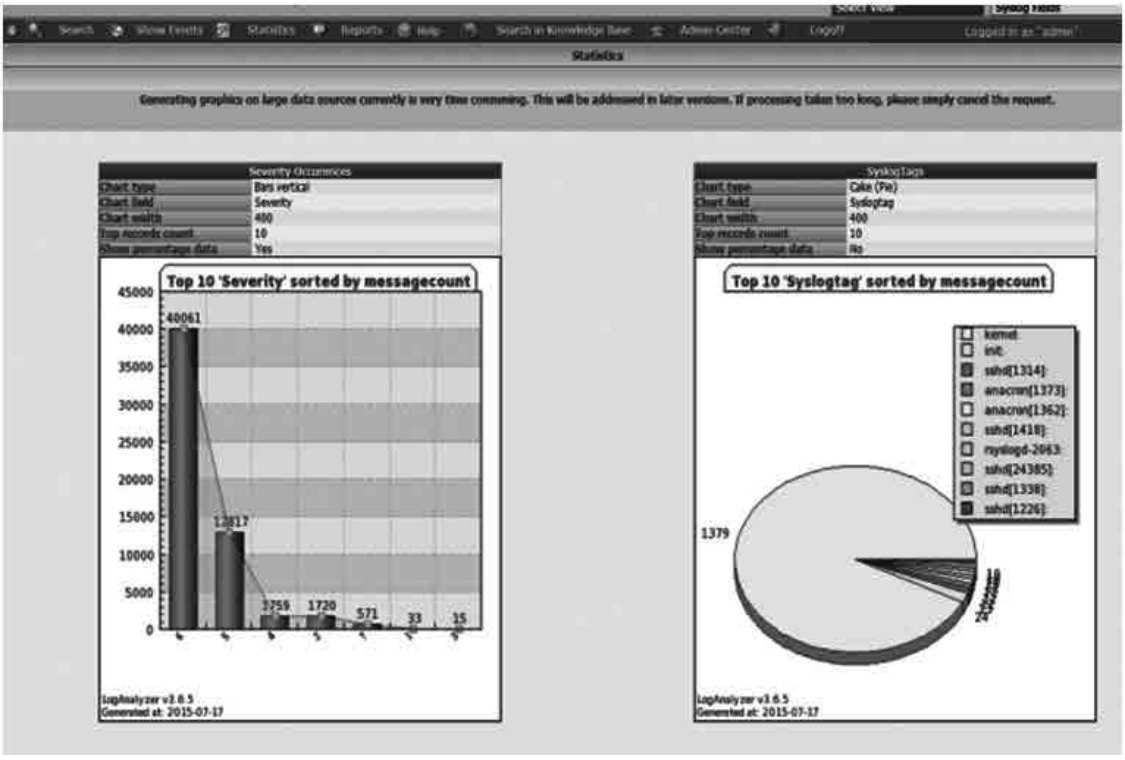


Hình 3. *Syslog cho thấy dấu hiệu bị tấn công dò mật khẩu của server*

Những kết quả đạt được trong quá trình thực nghiệm từ hệ thống máy chủ của trường đại học Bách khoa là rất khả quan. Hệ thống log đã có thể ghi lại những sự kiện xảy ra trên server một cách hiệu quả như ngày giờ đăng nhập vào server, các lỗi của hệ thống, các tiến trình cơ bản xảy ra trên server, và đưa ra các thông báo cảnh bảo về hệ thống rất hiệu quả.

Qua quá trình thực hiện thu thập log của các máy chủ linux đã thu thập được các kết quả rất tốt dựa vào hệ thống phân tích đã cho ta thấy được những kiểu tấn công vào máy chủ tại mạng BKNET như là brute force là kiểu tấn công thử password của các máy chủ để chiếm quyền điều khiển.

Sau khi phát hiện các dấu hiệu thì Log server sẽ đưa ra cảnh bảo bằng cách đưa ra các thống kê dựa trên biểu đồ khá chi tiết như Hình 4 dưới đây.



Hình 4. *Các report của hệ thống giám sát, cảnh báo tấn công mạng*

Từ những dữ liệu thu thập được đã giảm thiểu tối đa được các vấn đề về bảo mật được nêu ra ở phần trước. Giúp hệ thống được an toàn và vận hành ổn định hơn.

3.2. Chức năng giám sát, quản lý băng thông mạng

Hệ thống có khả năng thiết lập SMS, Email để gửi cảnh báo đến người quản trị thông qua tin nhắn trên thiết bị di động hoặc hòm thư. Hệ thống có chức năng tập hợp log, đưa ra thống kê theo ngày, tuần, tháng việc sử dụng băng thông của từng Port trong hệ thống. Hệ thống chia báo cáo log các port có sự thay đổi theo từng giờ mỗi ngày.

Hệ thống với chức năng giám sát việc giao tiếp của các địa chỉ IP nội bộ với các IP bên ngoài, đưa ra thống kê về mức độ thường xuyên sử dụng để kết nối tới đâu. Từ đó người quản trị có thể biết được việc sử dụng hệ thống mạng có đúng mục đích hay không của người dùng để có thể đưa ra các cảnh báo hay ngăn chặn.

4. Kết luận

Nhóm đã nghiên cứu, triển khai thành công hệ thống quản lý và giám sát mạng campus, trên cơ sở xây dựng và tích hợp một số hệ thống mã nguồn mở, tại Trường Đại học Bách Khoa Hà Nội. Hệ thống đã và đang được sử dụng để quản lý và giám sát các thiết bị Router, Switch, Server của Trường, đồng thời theo dõi để phát hiện kịp thời các thiết bị treo, hỏng trong phòng máy chủ. Từ đó, giúp đảm bảo các công đoạn xử lý, khắc phục sự cố được sớm nhất, để không gián đoạn các tới công việc nghiên cứu, giảng dạy và học tập của các đơn vị trong toàn trường. Mặt khác, việc thống kê sử dụng băng thông của các đơn vị trong trường giúp cho người quản trị phát hiện băng thông vượt quá cho phép hoặc không ổn định. Từ đó, kết hợp với các hệ thống quản trị mạng phát hiện ra các máy bị nhiễm mã gửi gói tin làm ảnh hưởng đến việc truy cập mạng để có thể ngăn chặn và cô lập, đảm bảo an toàn và thông tin thông suốt trên toàn hệ thống.

Tài liệu tham khảo

[1]. D Anderson, T Frivold, and A Valdes, *Next-generation Intrusion-Detection Expert System (NIDES)*, Technical Report SRI-CSL-95-07, Computer Science Laboratory, SRI International, Menlo Park, CA 94025-3493, USA, May 1995.
[2]. Stefan Axelsson, Ulf Lindqvist, Ulf Gustafson, and Erland Jonsson, *An Approach to UNIX Security Logging*, In Proceedings of the 21st National Information Systems Security Conference, pages 62–75, Crystal City, Arlington, VA, USA, 5–8 October 1998. NIST - National Institute of Standards and Technology/National Computer Security Center.
[3]. Stefan Axelsson, *The Base-rate Fallacy and Its Implications for the Difficulty of Intrusion Detection*, In 6th ACM Conference on Computer and Communications Security, pages 1–7, Kent Ridge Digital Labs, Singapore, 1–4 November 1999.
[4]. Herve Debar, Monique Becker, and Didier Siboni, *A Neural Network Component for An Intrusion Detection System*, In Proceedings of the 1992 IEEE Computer Sociecty Symposium on Research in Security and Privacy, pages 240–250, Oakland, CA, USA, May 1992. IEEE, IEEE Computer Society Press, Los Alamitos, CA, USA.
[5]. *The syslog-ng Open Source Edition 3.5 Administrator Guide*, Copyright © 1996-2014 BalaBit S.a.r.l. (file:///C:/Users/Administrator/Downloads/syslog-ng-ose-v3.5-guide-admin.pdf).
[6]. Extracting Useful Information from Log Messages
file:///C:/Users/Administrator/Downloads/BSD_12_2011%20%20BalaBit_single_article.pdf)
[7]. *Nagios Core Administration Cookbook*, Tom Ryder.
[8]. *Learning Nagios 4*, Wojciech Kocjan.
[9]. *The Cacti Manual*, Ian Berry, Tony Roman, Larry Adams, J.P.Pasnak, Jimmy Conner, Reinhard Scheck, Andreas Braun.
[10]. *Cacti 0.8 Beginner's Guide*, Thomas Urban.

RESEARCHING, BUILDING NETWORK ACTIVITIES AND SECURITY MONITORING SYSTEM FOR UNIVERSITIES BASE ON OPEN SOURCE

Abstract:

About 5 years recently, computer networks of universities in Vietnam, where in Bach khoa Network has developed strongly in scale and plays a more and more important role in such activities as exchanging information, doing research in universities. However, due to the features of economics and history, campus networks are usually inconsistent, i.e. the equipment is added up gradually with many types from different companies. As a result, the performance of the networks has been limited; their operations, controlling the systems have met many difficulties because of the inconsistency of the equipment. Currently, there have not been any researches, evaluation, and solutions to optimize the using performance of the systems which are suitable with the characteristics of these networks. Thence, we did a proposal research and built solutions applicable for campus networks.

Keywords: *CactiEZ, Security, IDS, SNMP, Rsyslog.*