Journal of educational equipment: Applied research, Volume 2, Issue 323 (September 2024)
ISSN 1859 - 0810

Xây dựng hệ thống phát hiện xâm nhập và giám sát mạng nội bộ

Kiều Đức Hồng*

**ThS ,Trường đại học Tài nguyên và Môi trường Hà Nội*
Received: 16/09/2024; Accepted: 26/09/2024; Published: 5/10/2024

Abstract: *This paper presents an approach in order to build an intrusion detection and monitor system for a local network area (LAN). This system is designed to monitor network and system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. When an attack is detected, it can drop the offending packets and bring the message to network administrator.*

Keywords: *System monitoring and administration, network intrusion*

1. Đặt vấn đề

Trong một hệ thống mạng, các máy chủ thường là mục tiêu chính trong các cuộc tấn công, truy cập trái phép. Một hệ thống mạng phải được bảo vệ theo nhiều tầng để tăng cường khả năng bảo vệ hệ thống [1,2,3]. Hiện nay, các chương trình bảo mật, phòng chống virus bảo vệ hệ thống (BKIS, Kaspersky Anti-Virus, BitDefender Antivirus, ...) đều có giá thành cao và chủ yếu được phát triển ở nước ngoài. Ngoài ra, các chương trình firewall bảo vệ mạng hiện nay hầu hết được tích hợp trong các thiết bị phần cứng của mạng. Bên cạnh đó, các chương trình được phát triển riêng lẻ với các tính năng tương đối độc lập với nhau cho nên việc khai thác các chức năng của các chương trình này nhằm phục vụ công việc giám sát và quản trị hệ thống bị hạn chế.

Xuất phát từ nhu cầu thực tiễn trên, chúng tôi tìm hiểu xây dựng một chương trình tích hợp nhiều chức năng hỗ trợ giám sát hệ thống mạng và phát hiện các xâm nhập trái phép có nhằm giúp cho công việc quản trị mạng được tập trung và đạt hiệu quả cao. Báo cáo này trình bày những vấn đề chủ yếu liên quan đến hệ thống này.

2. Nội dung nghiên cứu

2.1. Các phương thức xâm nhập mạng và cách phòng chống

2.1.1. Các kĩ thuật cơ bản xâm nhập một hệ thống mạng

Một số hình thức cơ bản tấn công xâm nhập mạng phổ biến như [1]: FootPrinting, Scanning, Enumeration, Gaining Access, Escalating Privileges, Pilfering, Covering Tracks, Denial of Service (DoS). Ngoài ra còn có một số hình thức tấn công khác như: tấn công không qua chứng thực (Deauthentication attack), tấn công truyền lại (Replay Attack), tấn công dựa trên sự cảm nhận sóng mang lớp vật lý, giả mạo địa chỉ MAC, ...

2.1.2. Tấn công từ chối dịch vụ và phòng chống

Tấn công từ chối dịch vụ (DoS) là các cuộc tấn công trên hệ thống mạng nhằm ngăn cản những truy xuất tới một dịch vụ bằng cách làm tràn ngập số lượng kết nối, quá tải server hoặc chương trình chạy trên server, tiêu tốn tài nguyên của server, hoặc ngăn chặn người dùng hợp lệ truy nhập tới dịch vụ mạng. Có 3 phương pháp tấn công DoS chủ yếu: Smurf hay Fraggle, SYN Flood và DNS attack [1,3,4].

Các biện pháp cơ bản phòng ngừa tấn công DoS như sau:

- Phòng ngừa các điểm yếu của ứng dụng (Application Vulnerabilities).
- Phòng ngừa việc khai thác sử dụng các zombie.
- Ngăn ngừa sử dụng công cụ tạo các kênh phát động tấn công.
- Ngăn chặn tấn công trên băng thông.
- Ngăn chặn tấn công qua SYN.
- Phát hiện và ngăn chặn tấn công tới hạn số kết nối.

Mục tiêu của việc phát hiện xâm nhập là xác định các hoạt động trái phép, dùng sai, lạm dụng đối với hệ thống máy tính gây ra bởi cả người dùng trong hệ thống lẫn người xâm nhập ngoài hệ thống. Đây là một công việc đầy khó khăn do ảnh hưởng của sự tăng trưởng nhanh chóng các kết nối mạng, môi trường máy tính không đồng nhất, nhiều giao thức truyền thông, ... Việc phát hiện xâm nhập được xây dựng chủ yếu dựa trên sự khác biệt ứng xử của kẻ xâm nhập so với người dùng hợp lệ.

2.2. Thiết kế xây dựng chương trình

Hệ thống chương trình được phân tích, thiết kế bao gồm nhiều mục tiêu như giám sát lưu thông gói tin IP,

theo dõi các tiến trình hệ thống đang hoạt động, các user đăng nhập trên hệ thống, phát hiện và cảnh báo các nguy cơ tấn công hay xâm nhập vào hệ thống trên máy chủ từ đó có thể tác động lên chương trình để bảo vệ thông tin mạng. Ngoài ra, chương trình còn có các công cụ và tiện ích mạng giúp cho người quản trị có thể thao tác quản lý tập trung. Với mục tiêu như vậy, hệ thống có những chức năng chính sau:

- Giám sát gói tin ra/vào trên hệ thống,
- Lọc gói tin từ nguồn đến đích dựa theo danh sách từ khóa cho trước để phát hiện thông tin không hợp pháp.
- Kiểm soát và phòng chống các cuộc tấn công DoS, DDoS, các hành vi tạo ra backdoor vào hệ điều hành của server.
- Kiểm tra các tiến trình, số hiệu tiến trình, cổng dịch vụ đang hoạt động trên Server để tìm ra các dịch vụ không hợp pháp.
- Quản lý các user hệ thống.
- Thông báo email cảnh báo cho các người sử dụng liên quan.

2.2.1.Chức năng lọc gói tin

Chức năng lọc gói tin (Packet Filtering) là cho phép phân tích các gói tin lưu thông trên máy chủ (máy nằm giữa mạng nội bộ và mạng công cộng) thành các thông tin trực quan hơn: IP đích, IP nguồn, Port đích, Port nguồn, giao thức… Trên cơ sở này, chúng ta có thể kiểm soát được các kết nối, nguy cơ tấn công hay xâm nhập vào trong mạng của chúng ta thông qua các tham số lọc gói tin. Các tham số lọc gói tin sẽ giúp chúng ta tính toán được những con số cụ thể từ đó đưa ra cảnh báo về nguy cơ bị tấn công DoS.

Chức năng lọc gói tin bao gồm 2 môđun chính:

Mô đun Packet: Cho phép định nghĩa cho gói tin, bao gồm các trường trong cấu trúc gói tin IP [4] như VER, IHL, Type of Service, Total Leng, Identification, … Gói tin chính là các luồng bit dữ liệu, mô đun Packet sẽ phân tích các luồng dữ liệu bit này thành các trường tương ứng. Từ đó ta sẽ truy cập và xử lý đến các trường dữ liệu một cách dễ dàng.

b. Mô đun PacketMonitor: Class định nghĩa cơ chế lấy dữ liệu các gói tin đi qua các giao diện.

2.2.2. Chức năng cảnh báo khả năng bị tấn công DDoS

Tấn công từ chối dịch vụ DDoS DDOS (Distributed Denial of Service attack) là hành động gây quá tải hệ thống hoặc băng thông của một máy tính, thường là các máy chủ Web, làm cho tài nguyên của một máy tính không thể sử dụng. Dựa vào các tham số lọc tói tin (giao thức, địa chỉ, tần số gửi,...), ta có thể đưa ra các qui tắc để cảnh báo máy có bị tấn công giúp cho người quản trị mạng có những biện pháp đối phó kịp thời.

Giải thuật cảnh báo tấn công DDoS như sau:

1. Tính toán các tham số lọc gói tin.
2. Kiểm tra các tham số lọc gói tin.
3. Nếu các tham số vượt ngưỡng cho phép thì thực hiện cảnh báo tấn công DDoS.
4. Ngược lại thông báo tình trạng hoạt động bình thường của hệ thống.

Các tham số lọc gói tin bao gồm: tổng số gói tin TCP, UDP, ICMP đến máy chủ, lưu lượng TCP, UDP, ICMP đến máy trong 1 phút.

2.2.3. Chức năng giám sát dịch vụ mạng (Services Monitor)

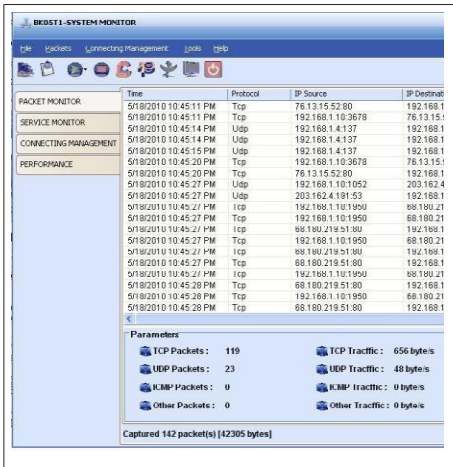
Services Monitor có chức năng quản lý các dịch vụ chạy trên Server, cho phép

người quản trị giám sát, tắt / mở các dịch vụ đang chạy trên hệ thống.Qua đó cho phép nhận dạng những tiến trình hoạt động bất hợp pháp.

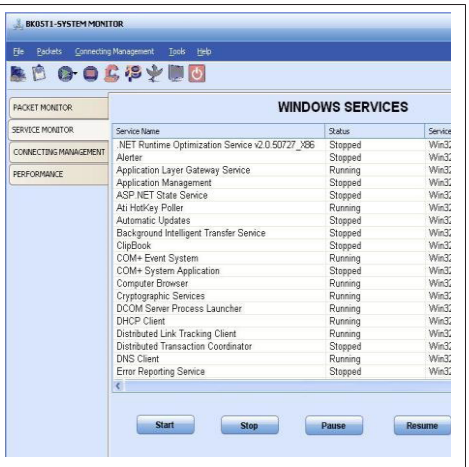
2.2.4. Giám sát hiệu suất mạng

Việc giám sát hiệu suất mạng thông qua việc đo lưu lượng gói tin vào/ra mạng và thể hiện kết quả ở dạng biểu đồ phản ánh trực quan.

Một số giao diện minh họa các kết quả thực hiện chương trình như sau:



Hình 2.1. Chức năng lọc gói tin.



Hình 2.2. Chức năng quản lý các dịch vụ.

Xem tiếp trang 345

rằng mặc dù quản lý tốt có thể mang lại lợi ích, nhưng hiện tại chưa được thực hiện đầy đủ, dẫn đến sự hạn chế trong khả năng tiếp cận dịch vụ của bệnh nhân.

Những nhóm như hộ nghèo, cận nghèo, và người có trình độ học vấn – giáo dục thấp thường gặp khó khăn trong việc tiếp cận thông tin và dịch vụ y tế. Báo cáo cho thấy rằng các nhóm này có khả năng tiếp cận dịch vụ cao hơn nhờ các chương trình hỗ trợ tài chính, đặc biệt là nhóm hộ cận nghèo (Exp(B) = 15, 241) . Điều này chỉ ra rằng hoạt động cung cấp thông tin, giáo dục kiến thức trong lĩnh vực y tế và hỗ trợ tài chính cho các nhóm này là cần thiết để giúp họ vượt qua các rào cản về tài chính và tiếp cận dịch vụ y tế một cách hiệu quả hơn. Một trong những yếu tố chính ảnh hưởng đến khả năng tiếp cận dịch vụ là khả năng tài chính của bệnh nhân. Các nhóm yếu thế không chỉ gặp khó khăn trong việc chi trả cho dịch vụ y tế mà còn thiếu các kiến thức và phương tiện để tiếp cận thông tin về các chương trình hỗ trợ tài chính và bảo hiểm y tế.

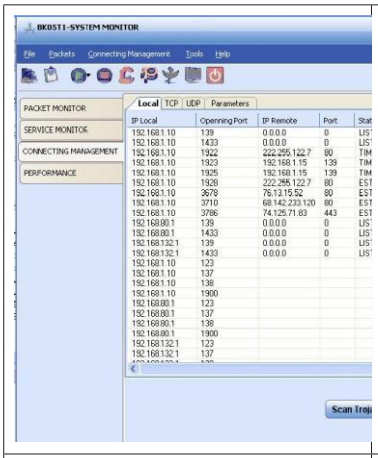
Tóm lại, việc tăng cường hỗ trợ tiếp cận thông tin, truyền thông và giáo dục về dịch vụ y tế nói chung và dịch vụ CTXH trong bệnh viện nói riêng dành cho các nhóm yếu thế không chỉ giúp họ tiếp cận dễ dàng hơn với dịch vụ y tế và thông tin, mà còn góp phần giảm bớt sự bất bình đẳng trong hệ thống y tế. Việc đầu tư vào các chương trình hỗ trợ tài chính và mở rộng các dịch vụ y tế sẽ mang lại lợi ích lâu dài cho cả người bệnh và hệ thống y tế, giúp nâng cao chất lượng dịch vụ y tế toàn diện.

Tài liệu tham khảo

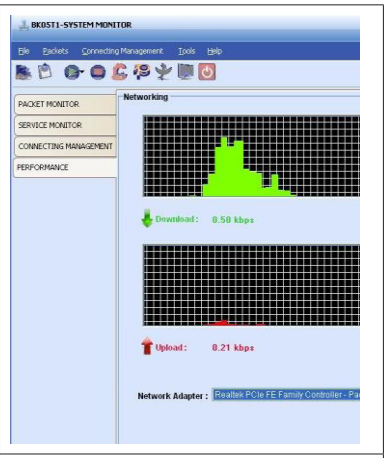
1. Quyết định số 712/QĐ-BYT về Ban hành Kế hoạch phát triển CTXH trong ngành y tế giai đoạn 2021-2030

2. Hà Thị Thư (chủ nhiệm đề tài), Viện Hàn Lâm Khoa học xã hội Việt Nam, Dịch vụ CTXH cho người bệnh trong bệnh viện ở Hà Nội, Đề tài Khoa học cấp Bộ năm 2023-2024.

Xây dựng hệ thống phát hiện... *(tiếp theo trang 323)*



Hình 2.3. Quản lý các kết nối hệ thống.



Hình 2.4. Giám sát lưu lượng mạng.

3. Kết luận

Thông thường phải sử dụng nhiều kỹ thuật bảo mật đi kèm với các mạng để bảo đảm tính an toàn cho mạng. Giám sát an ninh mạng nói chung, các hoạt động vào ra của gói tin và kết nối nói riêng đóng một khâu then chốt trong chiến lược bảo mật của một hệ thống mạng máy tính. Cùng với các thành phần bảo vệ mạng, máy chủ khác, chương trình phát hiện xâm nhập và bảo vệ mạng cung cấp các chức năng quản lý tập trung, hỗ trợ cho các quản trị mạng khả năng giám sát gói tin, quản lý các kết nối dịch vụ, cảnh báo các tiềm năng tấn công DoS, Trojan, chương trình được xây dựng dựa trên công nghệ lập trình mạng của .NET Framework, là môi trường tích hợp trong các phiên bản Windows hiện nay. Trong tương lai, chương trình sẽ được phát triển theo hướng đưa ra các phương án phát hiện Trojan tối ưu, đa dạng hóa các cảnh báo tấn công DoS, thiết lập các thông số tối ưu hiệu suất mạng dựa trên tình hình thực tiễn, ...

Tài liệu tham khảo

1. Kaufman, C., Perlman, R., Speciner, M.. *Network security. Private communication in a public worls*, Prentice Hall, 2022.

2. Stallings, W., Cryptography and Network Security. Principles and Practice, 3rd edition, Prentice Hall, 2012.

3. S.Bellovin and W.Chesvick. *Internet Security and Firewalls*, Second Edition, Addison-Wesley, Reading, 2018.

4. Tanenbaum, A.S., *Computer Networks*, 4th edition, Prentice Hall, 2003.

5. Bach, E., Shallit, J., *Algorithmic Number Theory*, Vol. I: Efficient Algorithms, 2nd printing, MIT Press, 2017.

6. http://www.codeproject.com