BỘ GIÁO DỤC VÀ ĐÀO TẠO
ĐẠI HỌC ĐÀ NẴNG

NGUYỄN ĐĂNG BẢO PHÚC

XÂY DỰNG HỆ THỐNG HỖ TRỢ GIÁM SÁT VÀ BẢO VỆ MẠNG MÁY TÍNH

Chuyên ngành : **KHOA HỌC MÁY TÍNH**
Mã số : **60.48.01**

TÓM TẮT LUẬN VĂN THẠC SĨ KỸ THUẬT

Đà Nẵng - Năm 2012

Công trình được hoàn thành tại

ĐẠI HỌC ĐÀ NẴNG

Người hướng dẫn khoa học: **TS. NGUYỄN TẤN KHÔI**

Phản biện 1: **PGS.TS. PHAN HUY KHÁNH**

Phản biện 2: **TS. TRƯƠNG CÔNG TUẤN**

Luận văn được bảo vệ tại Hội đồng chấm Luận văn tốt nghiệp thạc sĩ kỹ thuật họp tại Đại học Đà Nẵng vào ngày 03 tháng 03 năm 2012

Có thể tìm hiểu luận văn tại:

- Trung tâm Thông tin - Học liệu, Đại học Đà Nẵng
- Trung tâm Học liệu, Đại học Đà Nẵng

MỞ ĐẦU

1. Lý do chọn đề tài:

Internet ra đời đã mang lại rất nhiều lợi ích cho con người, bên cạnh ưu điểm mang đến cho xã hội sự phát triển vượt bậc, thông tin được cập nhật và phổ biến rộng rãi, xóa đi khoảng cách về địa lý, v.v . Nhưng tồn tại song song đó là các nguy cơ, yếu điểm của internet, một trong những yếu điểm đó là vấn đề an toàn và bảo mật trên Internet. Sự mở rộng về mặt địa lý cũng như các ứng dụng trên mạng Internet chính là sự mở rộng cửa hơn đối với kẻ tấn công mạng. Hơn nữa, các thủ đoạn tấn công mạng ngày càng tinh vi. Bài toán an ninh, an toàn mạng và tấn công mạng luôn đi song hành. Khi có kiểu tấn công mới thì giải pháp an ninh, an toàn cần phải được nâng cấp, cải tiến ngay tức thời để chống lại cuộc tấn công này. Có thể nói rằng, cuộc đua giữa an ninh, an toàn mạng và kẻ tấn công là cuộc chiến đầy phức tạp và không có hồi kết.

Không chỉ trên thế giới mà ngày nay tại Việt Nam, các cuộc tấn công của các hacker[1] nhằm vào các website, máy chủ của các doanh nghiệp ngày càng tăng. Từ các website giáo dục, các tổ chức tài chính, các tổ chức chính phủ cho đến các website cá nhân của các công ty, xí nghiệp và cả những máy chủ của các tập đoàn lớn trong nước hàng ngày đều có những cuộc thăm dò và tấn công. Mọi tài nguyên của các tổ chức, cá nhân khi tham gia vào Internet đều có nhiều nguy cơ tiềm ẩn khả năng mất ATTT. Tài nguyên thông tin

[1] Hacker: kẻ tấn công vào hệ thống mạng nhằm mục đích phá hoại

mang tính bí mật và quyết định cho sự thành công của một doanh nghiệp. Vấn đề cấp thiết là đảm bảo ATTT cho tài nguyên thông tin của các doanh nghiệp khi tham gia vào môi trường Internet.

Hiện nay, các chương trình bảo mật, phòng chống virus, giám sát bảo vệ hệ thống đều có giá thành cao và được phát triển ở nước ngoài. Ngoài ra, các chương trình giám sát hầu hết được tích hợp trên các thiết bị phần cứng nên việc khai thác chức năng, hoặc người dùng tự phát triển mở rộng thêm chức năng của các chương trình này nhằm phục vụ cho công việc quản trị mạng bị hạn chế.

Vì thế, nhu cầu có được một hệ thống hỗ trợ giám sát và bảo vệ hệ thống mạng trực quan nhằm giúp cho công việc quản trị mạng được tập trung và đạt hiệu quả cao là rất cần thiết. Đó là lý do mà tôi chọn nghiên cứu và thực hiện đề tài:

"Xây dựng hệ thống hỗ trợ giám sát và bảo vệ mạng máy tính" dưới sự hướng dẫn của TS. Nguyễn Tấn Khôi.

2. Mục tiêu và nhiệm vụ nghiên cứu:

Mục tiêu mà đề tài hướng đến là nghiên cứu và áp dụng chương trình hỗ trợ phát hiện xâm nhập mạng mã nguồn mở Snort và các công cụ mã nguồn mở được phát triển hỗ trợ cho hệ thống này trên giao diện trực quan để bảo vệ hệ thống mạng máy tính.

Tìm hiểu, phân tích cấu trúc của hệ thống phát hiện xâm nhập đề ra giải pháp hợp lý trong việc xây dựng và triển khai hệ thống.

Nghiên cứu giải thuật lan truyền ngược ứng dụng trên mạng nơ ron truyền thẳng nhiều lớp để ứng dụng trong hệ thống phát hiện xâm nhập.

Áp dụng cơ sở lý thuyết nền tảng để xây dựng và triển khai hệ thống.

3. Đối tượng và phạm vi nghiên cứu:

Từ yêu cầu của đề tài, ta xác định được đối tượng và phạm vi nghiên cứu của đề tài cụ thể như sau:

Đối tượng nghiên cứu:

- Các kỹ thuật và phương pháp giám sát trên hệ thống mạng;
- Các kỹ thuật xâm nhập trái phép vào mạng máy tính;
- Cơ sở, kiến trúc hệ thống phát hiện xâm nhập;
- Mạng nơ ron và thuật toán lan truyền ngược;
- Hệ thống phát hiện xâm nhập Snort.

Phạm vi nghiên cứu:

- Phạm vi nghiên cứu nằm trong lĩnh vực lập trình hệ thống và kỹ thuật giám sát mạng
- Khả năng phát hiện xâm nhập của hệ thống phát hiện xâm nhập mã nguồn mở Snort.

4. Phương pháp nghiên cứu:

- Thu thập và phân tích các tài liệu và thông tin liên quan đến đề tài:
- Phân tích hệ thống phát hiện xâm nhập;
- Triển khai xây dựng chương trình ứng dụng;
- Kiểm tra, thử nghiệm và đánh giá kết quả.

5. Kết quả đạt được:

Đề xuất được giải pháp, xây dựng và đánh giá thành công hệ thống hỗ trợ giám sát và bảo vệ mạng máy tính.

6. Ý nghĩa khoa học và thực tiễn:

Về mặt khoa học:

Đề tài sẽ đưa ra cái nhìn tổng quát về hệ thống hỗ trợ giám sát mạng máy tính và các giải pháp giám sát và bảo vệ hệ thống máy tính. Đồng thời, đưa ra một phương thức ứng dụng mạng nơ ron và thuật toán lan truyền ngược trong hệ thống phát hiện xâm nhập.

Về mặt thực tiễn:

Đề tài sẽ ứng dụng các công cụ mã nguồn mở, các công cụ, ngôn ngữ lập trình phục vụ cho đảm bảo hệ thống để xây dựng hệ thống hỗ trợ giám sát và bảo vệ mạng máy tính.

Kết quả của đề tài cung cấp thêm giải pháp an toàn thông tin cho các tổ chức và doanh nghiệp.

Cung cấp một hệ thống hỗ trợ cho các nhà quản trị mạng

khai thác và phục vụ công việc của cơ quan.

7. Bố cục luận văn:

Sau phần mở đầu, giới thiệu ..., nội dung chính của luận văn đi vào tìm hiểu các phương pháp tấn công mạng, tổng quát về hệ thống phát hiện xâm nhập, giới thiệu về mạng nơ ron và nghiên cứu ứng dụng để phát hiện xâm nhập mạng. Luận văn gồm 4 chương như sau:

Chương 1: Tổng quan về an toàn thông tin: Cho ta cái nhìn tổng quát về các phương pháp tấn công mạng và đưa ra các con số thống kê về tình hình an ninh mạng trên thế giới cũng như tại Việt Nam.

Chương 2: Tổng quan về hệ thống phát hiện xâm nhập: Chương này chủ yếu đi sâu vào tìm hiểu về hệ thống phát hiện xâm nhập, đi sâu vào hệ thống phát hiện xâm nhập IDS Snort với các thành phần, cũng như cấu tạo của các luật trong Snort.

Chương 3: Mạng nơ ron: Chương này mô tả tổng quát, mô hình hóa về mạng nơ ron và thuật toán lan truyền ngược áp dụng trên mạng nơ ron truyền thẳng nhiều lớp.

Chương 4: Hệ thống IDS ứng dụng mạng nơ ron: Đưa ra các mô hình hệ thống, cài đặt giải thuật lan truyền ngược ứng dụng mạng nơ ron tìm hiểu ở chương 3 vào hệ thống phát hiện xâm nhập nhằm giảm bớt cảnh báo thừa.

Cuối cùng là phần đánh giá, kết luận và hướng phát triển của đề tài.

CHƯƠNG 1: AN TOÀN THÔNG TIN MẠNG

1. 1. An toàn thông tin và tính thiết yếu của nó

An toàn thông tin bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin đối với nguy cơ tự nhiên hoặc do con người gây ra. Việc bảo vệ thông tin, tài sản và con người trong hệ thống thông tin nhằm bảo đảm cho các hệ thống thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy. An toàn thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng.

An toàn thông tin được thể hiện qua các tính chất cơ bản sau:

a) Tính tin cậy (confidentiality): đảm bảo thông tin chỉ được truy cập bởi những truy cập cho phép.

b) Tính toàn vẹn (integrity): bảo vệ tính chính xác, đầy đủ của thông tin cũng như các phương pháp xử lý;

c) Tính sẵn sàng (availability): đảm bảo những người dùng hợp pháp mới được truy cập các thông tin và tài sản liên quan khi có yêu cầu.

d) Tính không thể từ chối (Non-repudiation): Thông tin được cam kết về mặt pháp luật của người cung cấp.

1. 2. Các phương pháp tấn công mạng

1. 2. 1. Tấn công trực tiếp

1. 2. 2. Nghe trộm

1. 2. 3. Giả mạo địa chỉ

1. 2. 4. Vô hiệu các chức năng của hệ thống

1. 2. 5. Lỗi của hệ thống

1. 2. 6. Tấn công vào yếu tố con người

1. 3. Các giai đoạn của cuộc tấn công mạng

1. 3. 1. Xác định đối tượng tấn công

1. 3. 2. Thăm dò

1. 3. 2. 1. Thăm dò thông tin công cộng

1. 3. 2. 2. Thăm dò điện tử

1. 3. 2. 3. Những công cụ thăm dò

1. 3. 3. Tấn công

1. 4. Hiện trạng an toàn thông tin hiện nay

Theo thống kê của công ty an toàn mạng BKAV, tình hình virus và an ninh mạng tháng 7 năm 2011 tại Việt Nam như sau:

+ Đã có ít nhất 88 website của các cơ quan, doanh nghiệp tại Việt Nam bị hacker xâm nhập, trong đó có 9 trường hợp gây ra bởi hacker trong nước, 79 trường hợp do hacker nước ngoài.

+ Trong tháng 7 đã có 3.068 dòng virus máy tính mới xuất hiện tại Việt Nam. Các virus này đã lây nhiễm trên 5.627.000 lượt máy tính. Virus lây nhiều nhất trong tháng qua là W32.Sality.PE đã lây nhiễm trên 415.000 lượt máy tính.

CHƯƠNG 2: HỆ THỐNG IDS[2] SNORT HỖ TRỢ PHÁT HIỆN XÂM NHẬP

2. 1. Hệ thống phát hiện xâm nhập

Phát hiện xâm nhập là tiến trình theo dõi các sự kiện xảy ra trên một hệ thống máy tính hay hệ thống mạng, phân tích chúng để tìm ra các dấu hiệu xâm nhập bất hợp pháp.

Mục đích của hệ thống IDS là nhằm cảnh báo cho các nhân viên quản trị hệ thống khi phát hiện ra xâm nhập. Trong thực tế, những hệ thống báo trộm sẽ phát ra tín hiệu dựa trên sự chuyển động của đầu dò, một cửa sổ bị vỡ, hoặc một cánh cửa bị mở, tương tự như vậy các hệ thống IDS cũng có hai dạng cơ chế khởi phát[3]:

- Phát hiện dựa trên dấu hiệu.

- Phát hiện dựa trên sự bất thường.

2. 1. 1. Phát hiện dựa trên dấu hiệu

Phát hiện dựa trên dấu hiệu đòi hỏi cần phải có các file dấu hiệu để nhận dạng những hành động xâm nhập. Những file dấu hiệu sử dụng trong phương pháp phát hiện này thì tương tự như những file dấu hiệu trong những phần mềm diệt virus.

2. 1. 1. 1. Ưu điểm của phát hiện dựa trên dấu hiệu

2. 1. 1. 2. Những hạn chế của phát hiện dựa trên dấu hiệu:

2. 1. 2. Phát hiện dựa trên sự bất thường

---

[2] IDS viết tắt của Instrusion detection system là hệ thống phát hiện xâm nhập.

[3] Tiếng anh là : triggering mechanism

Phát hiện dựa trên sự bất thường là quá trình phân tích những hoạt động của mạng máy tính và lưu lượng mạng nhằm tìm kiếm sự bất thường.

2. 1. 2. 1. Những ưu điểm của phát hiện dựa trên sự bất thường

2. 1. 2. 2. Những hạn chế của phương pháp phát hiện dựa trên sự bất thường

2. 1. 3. Tổng quan về hệ thống IDS

2. 1. 3. 1. Giới thiệu IDS

2. 1. 3. 2. Chức năng của IDS

Hệ thống IDS có 3 chức năng quan trọng là

- Giám sát: lưu lượng mạng và các hoạt động khả nghi;

- Cảnh báo: báo cáo về tình trạng mạng cho hệ thống và nhà quản trị;

- Bảo vệ: Dùng những thiết lập mặc định và sự cấu hình từ nhà quản trị mà có những hành động thiết thực chống lại kẻ tấn công và phá hoại.

2. 1. 3. 3. Lợi ích của hệ thống IDS

2. 1. 4. Phân loại hệ thống phát hiện xâm nhập

2. 1. 4. 1. NIDS (Network based IDS)

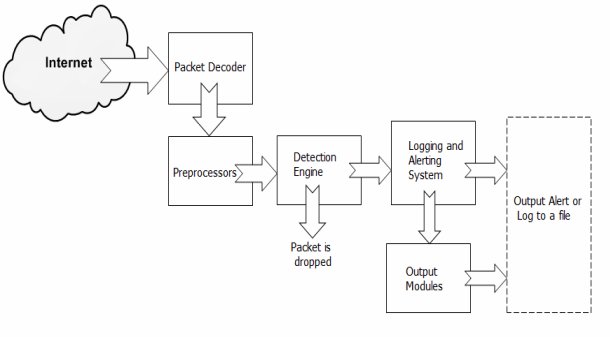
2. 1. 4. 2. HIDS (Host Based IDS)

2. 1. 4. 3. DIDS (Distributed Intrusion Dectection System)

2. 2. Hệ thống IDS Snort

Snort là một hệ thống phát hiện xâm nhập mạng (NIDS) mã nguồn mở miễn phí. Mặc dù tất cả các phương pháp phát hiện xâm nhập vẫn còn mới nhưng Snort được đánh giá là hệ thống tốt nhất hiện nay.

2. 2. 1. Các thành phần của Snort



Hình 2. 1: Các thành phần của Snort

2. 2. 1. 1. Packet Decoder

2. 2. 1. 2. Preprocessor

2. 2. 1. 3. Dectection Engine

2. 2. 1. 4. Logging và Alerting System

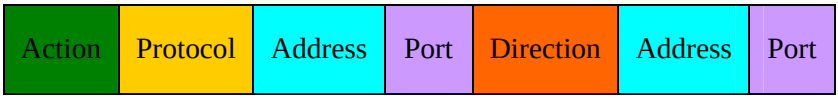
2. 2. 1. 5. Output Modules

2. 3. 1. Tập luật trong Snort

Hình 2. 2: Cấu trúc chung của một luật

2. 3. 2. 1. Rule Header

Cấu trúc chung của rule header như sau:



Hình 2. 3: Cấu trúc chung của rule header

2. 3. 2. 2. Rule Options

Rule option sau rule header và được đặt trong cặp dấu ngoặc đơn. Có thể một option hay nhiều option truyền vào cùng dấu. Nếu có nhiều option thì mỗi option phân cách nhau bởi dấu “;” Hành động trong rule header chỉ được gọi khi tất cả những tiêu chuẩn trong option là đúng. Thường thì một option có 2 phần: một từ khóa và một đối số. Những đối số truyền vào từ từ khóa bằng một dấu “:”. Chẳng hạn như: `msg: "Bi quet cong";`

2. 3. 2. Cài đặt Snort

2. 3. 2. 1. Chuẩn bị

2. 3. 2. 2. Cài đặt và cấu hình

CHƯƠNG 3: MẠNG NƠ RON

3. 1. Giới thiệu

Bộ não con người chứa khoảng 10 tỷ tế báo thần kinh (nơ ron). Trung bình, mỗi nơ ron nối với các nơ ron khác qua 10.000 khớp nối thần kinh (synapses). (Con số thực tế có thể khác phụ thuộc vào số nơ ron của từng cá thể). Mạng lưới các nơ ron thần kinh của não bộ hình thành một hệ thống xử lí song song.

- Não có thể học (tự tổ chức lại chính nó) từ kinh nghiệm.
- Điều này có nghĩa là có thể phục hồi một phần từ các thương tổn nếu các đơn vị khỏe mạnh khác có thể học qua các hàm mà trước đây được thực hiện bởi các đơn vị thương tổn.
- Não thực hiện các tính toán song song cực kì hiệu quả. Ví dụ, một nhận thức hình ảnh phức tạp xuất hiện ít hơn 100ms,
- Não hỗ trợ cho sự thông minh và khả năng tự nhận thức của chúng ta (Không một ai biết điều này xảy ra như thế nào)

3. 1. 1. Mạng nơ ron trong bộ não

3. 1. 2. Nơ ron và Synapses (khớp nối)

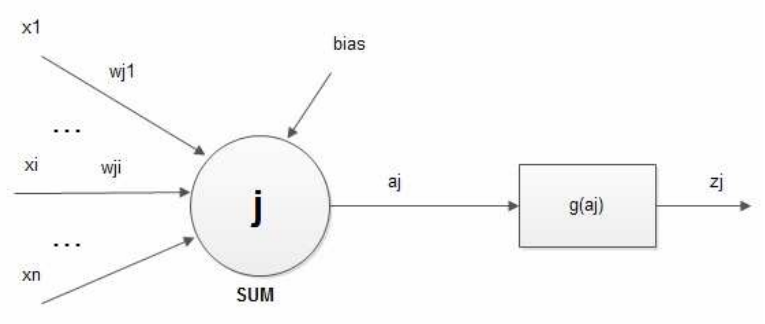
3. 1. 3. Mô hình nơ ron nhân tạo

3. 1. 3. 1. Nơ ron nhân tạo đơn giản

Phần tử tính toán cơ bản trong các mô hình nơ ron thường được gọi là một nút hay một đơn vị xử lí. Hàm f của tổng trọng lượng đầu vào của nó:

$$y_i = f(\sum_j w_{ij} y_j)$$

Đầu ra của nó, lần lượt, có thể phục vụ như là đầu vào cho các đơn vị khác



Hình 3. 5: Một nơ ron nhân tạo đơn giản

3. 1. 3. 2. Phân loại đơn vị xử lí

3. 2. Hàm xử lí

3. 2. 1. Hàm kết hợp

3. 2. 2. Hàm kích hoạt (hàm truyền)

Các hàm kích hoạt hay được sử dụng là:

- Hàm bước $y = \begin{cases} 1 & khi \quad x \geq 0 \\ 0 & khi \quad x < 0 \end{cases}$
- Hàm giới hạn chặt

$$y = \text{sgn}(x) = \begin{cases} 1 & khi \quad x \geq 0 \\ -1 & khi \quad x < 0 \end{cases}$$

- Hàm bậc thang

$$y = \text{sgn}(x) = \begin{cases} 1 & khi \quad x > 1 \\ x & khi \quad 0 \le x \le 1 \\ 0 & khi \quad x < 0 \end{cases}$$

- Hàm ngưỡng đơn cực

$$y = \frac{1}{1+e^{-\lambda x}} \quad \text{với } \lambda > 0$$

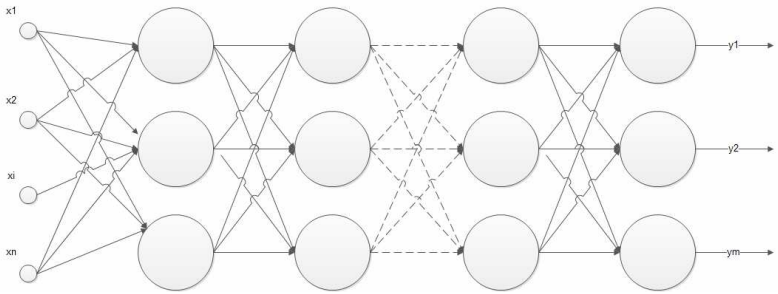
- Hàm ngưỡng hai cực

$$y = \frac{2}{1+e^{-\lambda x}} - 1 \qquad \text{với } \lambda > 0$$

3. 3. Phân loại mạng nơ ron

3. 3. 1. Mạng nơron một lớp

3. 3. 2. Mạng nơron truyền thẳng nhiều lớp



Hình 3. 7: Mạng truyền thẳng nhiều lớp

3. 3. 3. Mạng nơron phản hồi

3. 3. 4. Mạng nơron hồi quy

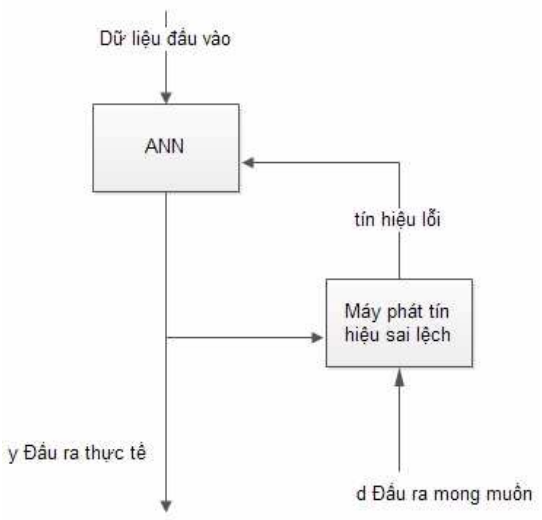
3. 3. 5. Mạng Hopfield

3. 3. 6. Mạng BAM

3. 4. Các luật học

3. 4. 1. Học có giám sát

.



Hình 3. 14: Học có giám sát

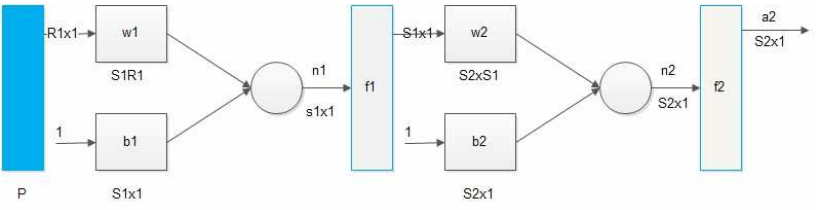
3. 4. 2. Học củng cố

3. 4. 3. Học không có giám sát

3. 5. Hàm mục tiêu

3. 6. Mạng truyền thẳng và thuật toán lan truyền ngược

3. 6. 1. Mạng truyền thẳng:



Hình 3. 17: Sơ đồ các lớp mạng nơ ron truyền thẳng nhiều lớp

Xét trường hợp mạng có hai lớp như hình vẽ, công thức tính toán cho đầu ra như sau: $a^2 = f^2(W^2(f^1(W^1P + b^1))+ b^2)$

3. 6. 2. Thuật toán lan truyền ngược (BP – Back Propagation)

3. 6. 2. 1. Mô tả thuật toán

Ta sẽ sử dụng dạng tổng quát của mạng nơron truyền thẳng nhiều lớp như trong hình 26. Khi đó, đầu ra của một lớp trở thành đầu vào của lớp kế tiếp. Phương trình thể hiện hoạt động này như sau:

$$\mathbf{a}^{m+1} = \mathbf{f}^{m+1}(\mathbf{W}^{m+1}\mathbf{a}^{m} + \mathbf{b}^{m+1}) \text{ với } m = 0, 1, ..., M - 1,$$

Trong đó M là số lớp trong mạng. Các nơron trong lớp thứ nhất nhận các tín hiệu từ bên ngoài:

$$\mathbf{a}^{0} = \mathbf{p}$$

chính là điểm bắt đầu của phương trình phía trên. Đầu ra của lớp cuối cùng được xem là đầu ra của mạng

$$\mathbf{a} = \mathbf{a}^{M}$$

3. 6. 2. 2. Thuật toán BP

Đầu vào: các cặp huấn luyện $\{x^{(k)}, d^{(k)} \mid k=1,2,...,p\}$, ở đó giá trị đầu vào của phần tử cuối cùng bằng -1, tức là $x_{m+1}^{(k)} = -1$.

Bước 0 (Đặt giá trị ban đầu)

Bước 1 (Vòng lặp huấn luyện)

Bước 2 (Lan truyền thẳng)

Bước 3 (Đo lường sai số đầu ra)

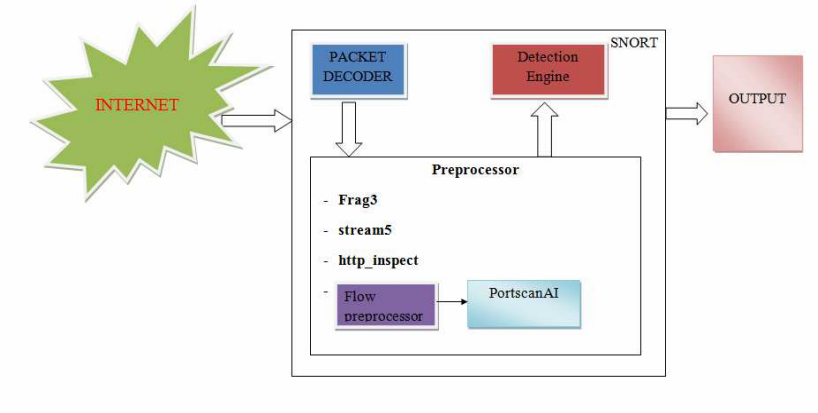
Bước 4 (Lan truyền ngược sai số)

Bước 5 (Sau mỗi vòng lặp)

Bước 6 (Kiểm tra tổng sai số)

3. 6. 2. 3. Biến thể của thuật toán lan truyền ngược

CHƯƠNG 4: HỆ THỐNG IDS ỨNG DỤNG MẠNG NƠ RON



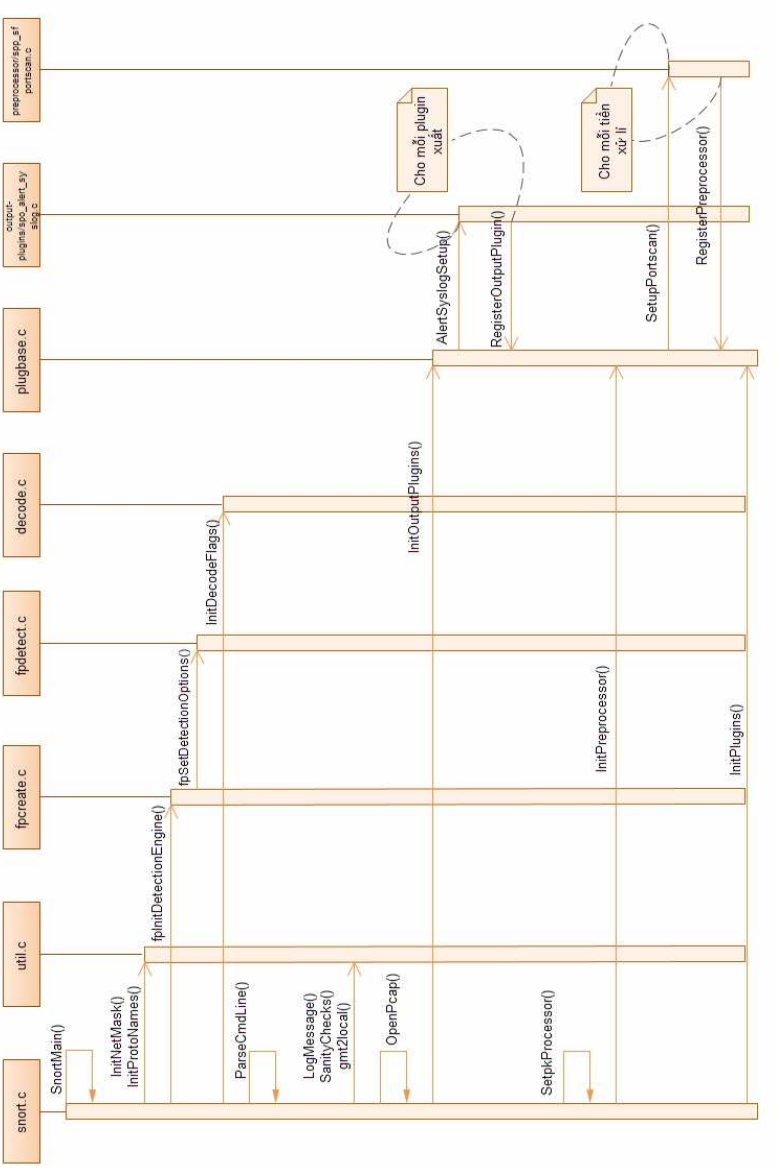
Hình 4. 1: Mô hình hệ thống tích hợp SnortAI

4. 1. Phân tích thiết kế hệ thống phát hiện xâm nhập

4. 1. 1. Sơ đồ hoạt động của hệ thống:

4. 1. 2. Sơ đồ tuần tự của hệ thống:

4. 1. 3. Sơ đồ tuần tự khởi tạo IDS:



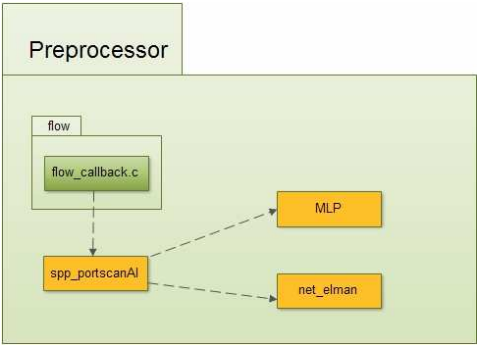
Hình 4. 3: Sơ đồ tuần tự khởi tạo IDS

4. 1. 4. Sơ đồ tuần tự cho phân tích cú pháp luật

4. 1. 5. Sơ đồ tuần tự cho khởi tạo máy dò tìm nhanh gói tin (fast packet detection engine)

4. 1. 6. Sơ đồ tuần tự khi một packet đến

4. 1. 7. Sơ đồ gói cho tiền xử lí AI



Hình 4. 16: Sơ đồ gói AI

4. 2. Thiết kế và xây dựng mạng nơ ron

4. 2. 1. Khối thu thập, phân tích dữ liệu

Như vậy, những dữ liệu thô thu thập được bao gồm:

```
unsigned hits_as_src;
unsigned hits_as_dst;
unsigned ack_rst_resp;
unsigned rst_resp;
ABS_TIME last_rcv_time
ABS_TIME last_snd_time;
AVG_TIME av_rcv_time;
AVG_TIME av_snd_time;
```

4. 2. 2. Khối Tiền xử lí

4. 2. 3. Xây dựng mạng nơ ron

Qua quá trình nghiên cứu, thử sai, ta xây dựng mô hình mạng bao gồm 3 lớp. Lớp đầu vào gồm 7 neuron tương ứng với 7 dữ liệu đầu vào trên, 1 lớp ẩn gồm 4 neuron, lớp đầu ra gồm 2 neuron.

Hàm kích hoạt (hàm chuyển): Sử dụng hàm sigmoid, hàm này đặc biệt thuận lợi khi ta sử dụng thuật toán huấn luyện lan truyền ngược, đồng thời phù hợp với chương trình xây dựng có đầu ra mong muốn rơi vào khoảng [0,1]. Công thức hàm sigmoid:

$$G(x) = \frac{1}{1+e^{-\alpha x}}$$

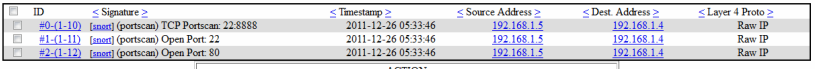
Thử nghiệm với giá trị $\alpha = 5$ là phù hợp nhất.

4. 2. 4. Huấn luyện mạng

4. 2. 5. Cài đặt thuật toán BP:

4. 3. Kết quả thực hiện

4. 3. 1. TCP SYN[4]:



ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(1-10)	[snort] (portscan) TCP Portscan: 22:8888	2011-12-26 05:33:46	192.168.1.5	192.168.1.4	Raw IP
#1-(1-11)	[snort] (portscan) Open Port: 22	2011-12-26 05:33:46	192.168.1.5	192.168.1.4	Raw IP
#2-(1-12)	[snort] (portscan) Open Port: 80	2011-12-26 05:33:46	192.168.1.5	192.168.1.4	Raw IP

Hình 4. 20: TCP SYN trên máy portscan

nmap –sS –P0 192.168.1.6

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(1-4)	(PortscanAI) Generic portscan, Certainty = 98%	2011-12-26 08:17:26	192.168.1.2:139	192.168.1.3:50325	TCP
#1-(1-3)	(PortscanAI) Generic portscan, Certainty = 95%	2011-12-26 08:14:42	192.168.1.6:80	192.168.1.2:7875	TCP
#2-(1-1)	(PortscanAI) Generic portscan, Certainty = 98%	2011-12-26 08:14:39	192.168.1.5:50970	192.168.1.6:445	TCP
#3-(1-2)	(PortscanAI) Generic portscan, Certainty = 99%	2011-12-26 08:14:39	192.168.1.6:1062	192.168.1.5:50970	TCP

Hình 4. 21: TCP SYN trên PortscanAI

4. 3. 2. Decoy scan[5]:

[4] SYN là một gói tin TCP có flag là “SYN”. Đây là gói tin đầu tiên được tạo ra phía máy con đến một dịch vụ dùng giao thức TCP của máy chủ.

[5] Decoy scan là kỹ thuật quét cổng ẩn địa chỉ IP thực sự của máy quét

KẾT LUẬN

Ngày nay, trí tuệ nhân tạo được xem là một lĩnh vực có bước đột phá trong ngành khoa học máy tính. Mạng nơ ron nhân tạo là các mô hình toán học được xây dựng dựa trên sự hoạt động của nơ ron sinh học, nó có thể tự thích ứng với sự thay đổi của thông tin bên ngoài. Đó là ưu điểm nổi bật của mạng nơ ron so với các mô hình khác.

Luận văn đã đi sâu vào nghiên cứu các vấn đề của mạng nơ ron nhân tạo, giải thuật lan truyền ngược, mô hình xử lí gói tin của hệ thống phát hiện xâm nhập dựa trên dấu hiệu. Bên cạnh đó, luận văn cũng đã trình bày đầy đủ về cấu trúc của một luật trong hệ thống hỗ trợ phát hiện xâm nhập mạng và ứng dụng các kiến thức đã nghiên cứu xây dựng chương trình hỗ trợ giám sát mạng máy tính.

Thông qua việc tìm hiểu mạng nơ ron truyền thẳng nhiều lớp, về quá trình tính toán đầu vào cho mạng nơ ron, các mô hình và kiến trúc của mạng, từ đó, xây dựng mô hình hệ thống phát hiện xâm nhập mạng. Vấn đề của các hệ thống phát hiện xâm nhập hiện nay là khả năng cảnh báo sớm các nguy cơ cho người quản trị. Mục tiêu nhằm khắc phục những vấn đề tồn tại trong các hệ thống hiện nay, vẫn còn cảnh báo dư thừa và hay mắc lỗi khi cảnh bảo. Áp dụng mạng nơ ron truyền thẳng và thuật toán lan truyền ngược với các tập huấn luyện tốt, đầy đủ thông tin và các tham số lựa chọn cẩn thận và đúng đắn thì kết quả cho thấy độ chính xác của cảnh báo cao.

Hệ thống hỗ trợ phát hiện xâm nhập mạng kết hợp với mạng nơ ron qua quá trình thử nghiệm thực tế với các công cụ hỗ trợ kiểm tra hệ thống mạng đã cho thấy ưu điểm của khả năng phát hiện lỗi,

hỗ trợ các nhà quản trị mạng trong lĩnh vực an toàn thông tin.

Tuy nhiên vấn đề tồn tại của mạng nơ ron là cấu trúc của mạng nơ ron ảnh hưởng rất nhiều đến khả năng của hệ thống. Nếu mạng có nhiều lớp thì khả năng hội tụ của mạng sẽ rất chậm. Nên để có được một mạng tốt thì phải trải qua thực nghiệm nhiều với các tham số khác nhau để có thể xây dựng được mô hình phù hợp.

Hướng phát triển tiếp theo của đề tài là nghiên cứu, cải tiến thử nghiệm các thuật toán tối ưu khác để nâng cao khả năng của hệ thống phát hiện xâm nhập IDS dựa trên Snort. Đồng thời sẽ xây dựng và phát triển các công cụ hiển thị kết quả quá trình thu thập thông tin chi tiết hơn, trực quan hơn. Đồng thời, hỗ trợ gởi cảnh báo cho người dùng qua tin nhắn SMS hay email giúp chúng ta có thể quản lí hệ thống mọi lúc mọi nơi.

An toàn thông tin là một lĩnh vực rộng, đòi hỏi nhiều kiến thức chuyên sâu và kinh nghiệm thực tiễn. Mặc dù đã cố gắng để hoàn thiện luân văn, nhưng chắc chắn luận văn này vẫn còn những thiếu sót, rất mong nhận được các ý kiến đóng góp nhằm hoàn thiện hơn nữa và triển khai thực tế kết quả nghiên cứu của luận văn.`