

**ĐẠI HỌC THÁI NGUYÊN**  
**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

**VŨ DUY TUÂN**

**NGHIÊN CỨU XÂY DỰNG**  
**MODULE GIÁM SÁT AN NINH MẠNG DỰA TRÊN**  
**MÃ NGUỒN MỞ SNORT**

**LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH**  
**THÁI NGUYÊN - NĂM 2014**

**ĐẠI HỌC THÁI NGUYÊN**  
**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

**VŨ DUY TUÂN**

**NGHIÊN CỨU XÂY DỰNG**  
**MODULE GIÁM SÁT AN NINH MẠNG DỰA TRÊN**  
**MÃ NGUỒN MỞ SNORT**

**LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH**

**Chuyên ngành: KHOA HỌC MÁY TÍNH**

**Mã số: 60.48.01**

**Người hướng dẫn khoa học: TS. TRẦN ĐỨC SỰ**

**Thái Nguyên, 2014**

## LỜI CẢM ƠN

Sau hơn 8 tháng nỗ lực tìm hiểu, nghiên cứu và thực hiện luận văn Cao học với nội dung “*Nghiên cứu xây dựng Module giám sát an ninh mạng dựa trên mã nguồn mở Snort*” đã cơ bản hoàn thành. Ngoài sự nỗ lực của bản thân, tôi còn nhận được rất nhiều sự quan tâm, giúp đỡ của các thầy cô trường ĐH Công nghệ thông tin và Truyền thông, Viện Công nghệ thông tin, Học viện Kỹ thuật mật mã, gia đình và bạn bè. Những sự động viên giúp đỡ này đã giúp tôi vượt qua được những khó khăn để hoàn thành tốt Luận văn của mình.

Trước hết em xin gửi lời cảm ơn chân thành đến các thầy cô trường ĐH Công nghệ thông tin và Truyền thông – ĐH Thái Nguyên, các thầy cô là các giáo sư, tiến sỹ công tác tại Viện Công nghệ thông tin đã truyền đạt cho em những kiến thức quý báu trong suốt thời gian học thạc sỹ tại trường. Đặc biệt, em xin gửi lời cảm ơn sâu sắc tới thầy **TS. Trần Đức Sự** Giám đốc Trung tâm Công nghệ thông tin & Giám sát an ninh mạng – Ban cơ yếu chính phủ đã tận tình hướng dẫn và chỉ bảo em trong suốt thời gian làm luận văn. Bên cạnh đó em cũng xin gửi lời cảm ơn tới các thầy, các anh chị trong khoa An toàn thông tin – Học viện Kỹ thuật mật mã, đã nhiệt tình giải đáp những thắc mắc, tạo điều kiện cho em có được các tài liệu hữu ích, cũng như được tham gia thực nghiệm Module trên mô hình thử nghiệm tại trường.

Cuối cùng, xin cảm ơn gia đình, bạn bè đã luôn động viên, giúp đỡ trong suốt thời gian học tập và hoàn thành Luận văn.

Do thời gian, kiến thức và các trang thiết bị còn hạn chế, chưa thực nghiệm được nhiều kết quả đạt được chỉ mang tính chất thử nghiệm. Em rất mong nhận được sự góp ý từ phía thầy cô, bạn bè để bản luận văn của em được hoàn thiện hơn.

*Thái Nguyên, tháng 09 năm 2014*

Học viên

**VŨ DUY TUÂN**

## **LỜI CAM ĐOAN**

Để hoàn thành luận văn đúng thời gian quy định và đáp ứng được mục tiêu đặt ra, bản thân em đã luôn cố gắng nghiên cứu, học tập và làm việc. Trong quá trình làm luận văn em có tham khảo một số tài liệu (đã được nêu trong phần “TÀI LIỆU THAM KHẢO” và không sao chép nội dung từ bất kỳ bản luận văn nào khác. Toàn bộ luận văn là do bản thân nghiên cứu, xây dựng nên dưới sự định hướng, hướng dẫn của thầy hướng dẫn.

Em xin cam đoan những lời trên là đúng, mọi thông tin sai lệch em xin hoàn toàn chịu trách nhiệm trước thầy giáo hướng dẫn và nhà trường.

*Thái Nguyên, tháng 9 năm 2014*

Học viên

**VŨ DUY TUÂN**

## DANH MỤC CÁC TỪ VIẾT TẮT

IETF	:	Internet Engineering Task Force
RFC	:	Request for Comments
IDS	:	Intrusion Detection System
ARP	:	Address Resolution Protocol
GSANM	:	Giám sát an ninh mạng
CSDL	:	Cơ sở dữ liệu
OSSIM	:	Open Source Security Information Management
NIDS	:	Network-based IDS
HIDS	:	Host based IDS
CPU		Central Processing Unit

## DANH MỤC CÁC HÌNH VẼ

Hình 1.1: Mô hình triển khai hệ thống NIDS .....	10
Hình 1.2: Mô hình hệ thống HIDS .....	12
Hình 1.3 – Mô hình mạng phổ biến của các đơn vị vừa và nhỏ .....	13
Hình 2.1: Mis-match trong khi đang so sánh tại vị trí j .....	17
Hình 2.2: Good-suffix shift, trường hợp u lại xuất hiện trong P .....	17
Hình 2.3: Good-suffix shift, trường hợp chỉ suffix của u xuất hiện trong P.....	17
Hình 2.4: Dịch để ký tự b ăn khớp với văn bản.....	18
Hình 2.5: Dịch khi b không xuất hiện trong P .....	18
Hình 2.6: Đồ thị hàm goto với các từ khóa đầu vào.....	21
Hình 2.7: Hàm failure .....	22
Hình 2.8: Hàm output .....	24
Hình 2.9: Ví dụ hàm goto .....	25
Bảng 2.10: Ví dụ hàm failure.....	25
Bảng 2.11: Ví dụ hàm output.....	25
Hình 3.1: Mô hình Module giám sát an ninh mạng.....	35
Hình 3.2: Các cơ sở dữ liệu của Module giám sát an ninh mạng .....	42
Hình 3.3: Giao diện quản lý các sự kiện của Module giám sát an ninh mạng.....	59
Hình 3.4: Giao diện quản trị người dùng của Module giám sát an ninh mạng.....	59
Hình 3.5: Mô hình thử nghiệm Module giám sát an ninh mạng.....	60
Hình 3.6: Attacker sử dụng chương trình DoSHTTP để tấn công vào WebServer .....	62
Hình 3.7: Kiểm tra hoạt động của CPU trên WebServer.....	62
Hình 3.8: Theo dõi gói tin đi vào WebServer sử dụng Wireshark .....	65
Hình 3.9: Xây dựng luật Snort phát hiện tấn công DoS qua giao diện Web .....	66
Hình 3.10: Màn hình cảnh báo tấn công từ chối dịch vụ của Module giám sát an ninh mạng.....	67
Hình 3.11: Sử dụng phần mềm Nmap dò quét các cổng trên máy WebServer .....	68
Hình 3.12: Màn hình cảnh báo tấn công dò quét của Module giám sát an ninh mạng..	68
Hình 3.13: Chức năng lưu trữ file giám sát của Module giám sát an ninh mạng .....	69
Hình 3.14: Phân tích file Pcap sử dụng phần mềm Wireshark .....	69

## MỤC LỤC

LỜI NÓI ĐẦU .....	1
1. Lý do chọn đề tài .....	1
2. Mục tiêu và nhiệm vụ nghiên cứu: .....	1
3. Đối tượng và phạm vi nghiên cứu .....	2
4. Hướng nghiên cứu của đề tài .....	2
5. Bố cục của đề tài.....	2
Chương 1 – TỔNG QUAN VỀ GIÁM SÁT AN NINH MẠNG.....	3
1.1. Khái niệm .....	3
1.1.1. Giới thiệu chung .....	3
1.1.2. Một số khái niệm liên quan .....	3
1.1.2.1. Thu thập dữ liệu.....	3
1.1.2.2. Phân tích dữ liệu .....	3
1.1.2.3. Phát hiện và phản ứng .....	4
1.2. Giám sát mạng .....	4
1.2.1. Khái niệm .....	4
1.2.2. Cách thức hoạt động và mục đích ứng dụng .....	5
1.3. Hệ thống phát hiện xâm nhập .....	6
1.3.1. Giới thiệu chung .....	6
1.3.2. Nguyên lý hoạt động .....	7
1.3.2.1. Giám sát mạng (monotoring).....	7
1.3.2.2. Phân tích lưu thông (Analyzing) .....	7
1.3.2.3. Liên lạc .....	8
1.3.2.4. Cảnh báo (Alert) .....	8
1.3.2.5. Phản ứng (Response).....	8
1.4. Phân loại một số kiểu giám sát .....	9
1.4.1. Giám sát toàn bộ mạng (NIDS).....	9
1.4.2. Giám sát máy tính đơn lẻ (HIDS).....	11
1.5. Mô hình mạng thực tế.....	13

Chương 2 – KỸ THUẬT XÂY DỰNG HỆ THỐNG GIÁM SÁT AN NINH	
MẠNG .....	15
2.1. Kỹ thuật phát hiện dựa trên dấu hiệu thông qua đối sánh mẫu .....	15
2.1.1. Giới thiệu bài toán đối sánh mẫu .....	15
2.1.2. Phát biểu bài toán .....	16
2.1.3. Thuật toán Boyer-Moore .....	16
2.1.4. Thuật toán Aho-Corasick .....	18
2.1.4.1. Định nghĩa .....	18
2.1.4.2. Xây dựng máy đối sánh mẫu hữu hạn trạng thái từ tập các mẫu phù hợp với từ khóa. ....	19
2.1.4.3. Sử dụng máy hữu hạn trạng thái để xác định vị trí các mẫu trong văn bản. ....	24
2.1.4.4. Độ phức tạp thuật toán.....	27
2.1.5. So sánh giữa các thuật toán .....	27
2.2. Kỹ thuật phát hiện dựa trên sự bất thường .....	28
2.2.1. Định nghĩa .....	28
2.2.2. Dữ liệu phát hiện bất thường .....	29
2.2.3. Kỹ thuật .....	31
2.2.4. Phương pháp .....	32
Kết chương: .....	34
Chương 3 - XÂY DỰNG MODULE GIÁM SÁT AN NINH MẠNG DỰA	
TRÊN PHẦN MỀM SNORT .....	35
3.1. Mô hình Module giám sát an ninh mạng .....	35
3.1.1. Mô hình tổng quan.....	35
3.1.2. Mô hình chi tiết.....	36
3.1.2.1. Máy trình sát.....	36
3.1.2.2. Máy thu thập.....	41
3.1.2.3. Cơ sở dữ liệu.....	41
3.1.2.4. Phân tích .....	43
3.1.2.5. Website .....	46



3.2. Triển khai xây dựng Module giám sát an ninh mạng .....	46
3.2.1. Lựa chọn phần mềm .....	46
3.2.1.1. Giới thiệu về Snort .....	46
3.2.1.2. Các thành phần của Snort .....	46
3.2.1.3. Các chế độ hoạt động của Snort .....	49
3.2.1.4. Các tùy chọn trong việc sử dụng Snort .....	53
3.2.1.5. Ưu điểm, hạn chế của Snort .....	55
3.2.2. Phân tích yêu cầu chức năng của Module .....	55
3.2.3. Phân tích thiết kế .....	56
3.2.4. Tích hợp tính năng quản lý luật Snort vào Module giám sát an ninh mạng .....	57
3.2.5. Xây dựng thành phần quản trị tập trung .....	58
3.3. Vận hành và thử nghiệm.....	59
3.3.1. Mô hình thử nghiệm .....	59
3.3.2. Tấn công từ chối dịch vụ .....	61
3.3.3. Tấn công thăm dò .....	67
3.3.4. Đánh giá kết quả.....	69
KẾT LUẬN .....	71
TÀI LIỆU THAM KHẢO .....	73

# LỜI NÓI ĐẦU

## 1. Lý do chọn đề tài

Ngày nay với sự phát triển mạnh mẽ của khoa học kỹ thuật nói chung và công nghệ thông tin nói riêng, việc ứng dụng công nghệ thông tin, Internet ngày càng trở lên phổ biến trong đời sống hàng ngày cũng như trong hầu hết các lĩnh vực. Việc trao đổi, quản lý, khai thác thông tin trên Internet đã trở thành xu hướng tất yếu của xã hội hiện đại. Song song với sự phát triển đó là hàng loạt các nguy cơ về mất an toàn thông tin. Vấn đề đảm bảo an toàn thông tin luôn được các cơ quan, tổ chức đặt lên hàng đầu. Tuy nhiên hàng năm các vụ tấn công mạng vẫn liên tục gia tăng mà chưa có biện pháp khắc phục triệt để.

Cách tốt nhất để có thể đảm bảo cho hệ thống mạng an toàn đó là chủ động phát hiện các tấn công và đưa ra những phản ứng thích hợp. Để làm được như vậy cần phải có một hệ thống có khả năng giám sát toàn bộ các hành động đi ra cũng như đi vào bên trong hệ thống mạng cần bảo vệ, có một vấn đề là các công cụ bảo vệ hệ thống được triển khai ở nước ta hầu hết đều mua của nước ngoài với giá thành rất cao đây là một khó khăn lớn đối với các đơn vị vừa và nhỏ. Mặt khác vì là sản phẩm thương mại nên công nghệ và kỹ thuật của các hệ thống đó luôn luôn được giữ kín vì thế mỗi khi phát sinh các dạng tấn công mới, các nhà quản trị trong nước không thể tự phát triển mở rộng được.

Từ đó phát sinh nhu cầu cần có một hệ thống hỗ trợ giám sát và bảo vệ hệ thống mạng một cách hiệu quả, các nhà quản trị có thể chủ động mở rộng hay phát triển cho phù hợp với các cuộc tấn công mạng kiểu mới. Đó là lý do mà tôi chọn đề tài “ *Nghiên cứu xây dựng Module giám sát an ninh mạng dựa trên mã nguồn mở Snort*” dưới sự hướng dẫn của TS Trần Đức Sự.

## 2. Mục tiêu và nhiệm vụ nghiên cứu:

Mục tiêu mà đề tài là tìm hiểu, nghiên cứu hệ thống phát hiện xâm nhập, phân tích và đưa ra giải pháp hợp lý.