ĐẠI HỌC THÁI NGUYÊN

TR- ỜNG 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

TR- ỜNG 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

MỤC LỤC

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 hằng 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.