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

BÙI THỊ HƯƠNG THƠM

NGHIÊN CỨU XÂY DỰNG CÔNG CỤ HỖ TRỢ PHÂN TÍCH GÓI TIN TRONG ĐIỀU TRA MẠNG

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Thái Nguyên, năm 2015

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

BÙI THỊ HƯƠNG THƠM

NGHIÊN CỨU XÂY DỰNG CÔNG CỤ HỖ TRỢ PHÂN TÍCH GÓI TIN TRONG ĐIỀU TRA MẠNG

Chuyên ngành : Khoa học máy tính
Mã số chuyên ngành: 60 48 01 01

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

NGƯỜI HƯỚNG DẪN KHOA HỌC
TS. TRẦN ĐỨC SỰ

Thái Nguyên, tháng 8 năm 2015

LỜI CAM ĐOAN

Tôi là: **Bùi Thị Hương Thơm**

Lớp: CK12I

Khoá học: 2014 - 2015

Chuyên ngành: Khoa học máy tính

Mã số chuyên ngành: 60 48 0101

Cơ sở đào tạo: Trường Đại học Công nghệ thông tin và Truyền thông Thái Nguyên.

Giáo viên hướng dẫn: **TS. Trần Đức Sự**

Tôi xin cam đoan luận văn "**Nghiên cứu xây dựng công cụ hỗ trợ phân tích gói tin trong điều tra mạng**" này là công trình nghiên cứu của riêng tôi. Các số liệu sử dụng trong luận văn là trung thực. Các kết quả nghiên cứu được trình bày trong luận văn chưa từng được công bố tại bất kỳ công trình nào khác.

Thái Nguyên, ngày 15 tháng 07 năm 2015

HỌC VIÊN

Bùi Thị Hương Thơm

LỜI CẢM ƠN

Để hoàn thành chương trình cao học và viết luận văn này, tôi đã nhận được sự hướng dẫn, giúp đỡ và chỉ bảo nhiệt tình của quý thầy cô trường Đại học Công nghệ thông tin và Truyền thông. Đặc biệt là những thầy cô ở Viện công nghệ thông tin Hà Nội đã tận tình dạy bảo cho tôi trong suốt thời gian học tập tại trường.

Tôi xin gửi lời cảm ơn sâu sắc đến TS. Trần Đức Sự đã dành nhiều thời gian và tâm huyết hướng dẫn tôi hoàn thành luận văn này.

Mặc dù tôi đã cố gắng hoàn thiện luận văn bằng tất cả năng lực của mình, song không thể tránh khỏi những thiếu sót, rất mong nhận được sự đóng góp quý báu của quý thầy cô và các bạn.

Tôi xin chân thành cảm ơn!

MỤC LỤC

DANH MỤC CÁC TỪ VIẾT TẮT

STT	Tên viết tắt	Tên tiếng Anh
1	ARP	Address resolution protocol
2	CPU	Central Processing Unit
3	DHCP	Dynamic Host Configuration Protocol
4	DNS	Domain Name System
5	DoS	Denial of Service
6	HTTP	Hypertext Transfer Protocol
7	ICMP	Internet control message protocol
8	IDS	Intrusion Detection System
9	IP	Internet Protocol
10	TCP	Tranmission Control Protocol
11	RARP	Reserve address resolution protocol
12	OSI	Open Systems Interconnection Reference Model
13	UDP	User Datagram Protocol
14	URL	Uniform Resource Locator

DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ

MỞ ĐẦU

Sự phát triển mạnh mẽ của Công nghệ thông tin nói chung và mạng Internet nói riêng đã tạo điều kiện thuận lợi cho việc cung cấp đa dạng các dịch vụ hữu ích đến với con người. Trong vài năm gần đây, nó không ngừng phát triển để phù hợp với một cộng đồng rộng lớn hơn nhiều, đem lại rất nhiều dịch vụ với các lợi ích thương mại, kinh tế, xã hội... Tuy nhiên, nó cũng trở thành môi trường cho các cuộc chiến tranh không gian số, nơi mà các cuộc tấn công của nhiều loại hình khác nhau (liên quan tài chính, tư tưởng, hành vi trả đũa...) đang được phát động. Các giao dịch thương mại điện tử được thực hiện trực tuyến là mối quan tâm chính của tội phạm mạng. Những hacker ăn cắp tài khoản của người dùng để thực hiện ý đồ xấu như mua bán trực tuyến, thỏa hiệp với một website hay máy chủ, phát động tấn công lên các hệ thống khác. Chính vì thế, hệ thống máy tính cần phải được bảo vệ khỏi các cuộc tấn công và phản ứng một cách thích hợp để tạo ra những xử lý nhằm giảm thiểu thiệt hại do tội phạm gây ra. Quá trình xử lý sự cố, phục hồi chứng cứ và truy tìm dấu vết tội phạm liên quan đến ngành khoa học điều tra số (digital forensics).

Phân tích điều tra mạng(Network Forensics) là một nhánh của ngành khoa học điều tra số đề cập đến việc chặn bắt, ghi âm và phân tích lưu lượng mạng cho mục đích điều tra và ứng phó sự cố. Có rất nhiều kỹ thuật cũng như công cụ hỗ trợ trong việc chặn bắt các dữ liệu lan truyền trên mạng để một cuộc tấn công hay một ý đồ xấu có thể bị điều tra, ngăn chặn.

Công cụ hỗ trợ phân tích gói tin trong điều tra mạng là một vấn đề rất quan trọng và luôn cấp thiết. Để cho quá trình điều tra mạng được nhanh và chính xác thì một chương trình hỗ trợ cần phải được xây dựng một cách chính xác cung cấp nhiều thông tin cần thiết cho người điều tra.