

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

LUU THỊ THANH HƯƠNG

# MỘT SỐ KỸ THUẬT LỌC GÓI TIN TRONG IP

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Thái Nguyên - 2015

## LỜI CAM ĐOAN

Những kết quả nghiên cứu được trình bày trong luận văn là hoàn toàn trung thực, không vi phạm bất cứ điều gì trong luật sở hữu trí tuệ và pháp luật Việt Nam. Nếu sai, tôi hoàn toàn chịu trách nhiệm trước pháp luật.

*Thái nguyên, ngày 20 tháng 5 năm 2015*

**Tác giả luận văn**

***Lưu Thị Thanh Hương***

## LỜI CẢM ƠN

Trước hết tôi xin gửi lời cảm ơn sâu sắc đến thầy hướng dẫn khoa học PGS.TS Nguyễn Văn Tam về những chỉ dẫn khoa học, định hướng nghiên cứu và tận tình hướng dẫn tôi trong suốt quá trình làm luận văn.

Tôi xin cảm ơn các các Thầy trong viện Công Nghệ Thông Tin, các Thầy, Cô giáo trong trường Đại học Công Nghệ Thông Tin và Truyền Thông - Đại học Thái Nguyên đã cung cấp cho tôi những kiến thức vô cùng quý báu và cần thiết trong suốt thời gian học tập tại trường để tôi có thể thực hiện và hoàn thành tốt đề án chuyên ngành này.

Tôi xin chân cảm ơn lãnh đạo, bạn đồng nghiệp trường THPT Đồng Hỷ đã tạo điều kiện giúp đỡ tôi trong công việc để tôi yên tâm theo học.

Cuối cùng, tôi xin cảm ơn gia đình và bạn bè, những người đã luôn ủng hộ và động viên tôi, giúp tôi yên tâm và có tâm lý thuận lợi nhất để tôi nghiên cứu luận văn này. Tuy nhiên do giới hạn về mặt thời gian và kiến thức nên đề án chắc chắn sẽ không tránh khỏi những sai sót ngoài ý muốn. Tôi rất mong nhận được sự thông cảm và đóng góp ý kiến của các thầy cô và các bạn.

Học viên

Lưu Thị Thanh Hương

## MỤC LỤC

LỜI CAM ĐOAN .....	i
LỜI CẢM ƠN .....	iii
MỤC LỤC .....	iv
BẢNG KÝ HIỆU CÁC TỪ VIẾT TẮT .....	vi
DANH MỤC CÁC HÌNH VẼ .....	viii
DANH MỤC BẢNG .....	x
MỞ ĐẦU .....	1
Chương 1.....	3
TỔNG QUAN VỀ AN TOÀN VÀ BẢO MẬT TRONG MẠNG IP.....	3
1.1. Các khái niệm cơ bản.....	3
1.1.1. An toàn và bảo mật là gì? [11] .....	3
1.1.2. Các nguy cơ gây mất an toàn [11].....	4
1.2. Các kiểu tấn công mạng IP [2] .....	4
1.2.1. Các kỹ thuật bắt thông tin.....	4
1.2.2. Tấn công xâm nhập mạng .....	6
1.2.3. Tấn công từ chối dịch vụ DoS, DdoS [6].....	7
1.3. Các biện pháp bảo vệ an toàn mạng .....	10
1.3.1. An toàn trung chuyển (Transit Security).....	10
1.3.1.1. Các mạng riêng ảo (VPN - Virtual Private Network) [11].....	10
1.3.1.2. Giải pháp mật mã thông tin (Cryptography) [2] .....	11
1.3.2. Giải pháp kiểm soát lưu lượng (Traffic Regulation) .....	17
1.3.2.1. Giải pháp phát hiện và phòng tránh xâm nhập [3].....	17
1.3.2.2. Giải pháp kỹ thuật bức tường lửa (Firewall technology) [5].....	19
Chương 2.....	27

KỸ THUẬT LỌC GÓI TIN .....	27
2.1. Kỹ thuật lọc gói tin .....	27
2.2. Kỹ thuật lọc gói tin tĩnh .....	30
2.2.1. Giải thuật lọc gói tĩnh [4].....	30
2.2.2. Lọc gói dựa trên tiêu đề TCP/UDP.....	33
2.2.3. Lọc gói dựa trên tiêu đề của gói tin IP.....	37
2.2.4. Mặc định từ chối so với mặc định cho phép .....	40
2.3. Kỹ thuật lọc gói tin động .....	40
2.3.1. Giải thuật lọc gói tin động [4].....	41
2.3.2. Theo dõi trạng thái .....	43
2.3.3. Lưu giữ và kiểm tra trạng thái .....	46
2.3.4. Theo dõi số trình tự của TCP.....	46
2.3.5. Kiểm tra giao thức.....	47
2.4. Sự khác nhau giữa kỹ thuật lọc gói tin tĩnh và kỹ thuật lọc gói tin động.....	48
<b>Chương 3</b> .....	49
<b>XÂY DỰNG THỬ NGHIỆM BỨC TƯỜNG LỬA</b> .....	49
3.1. Phân tích bài toán.....	49
3.1.1. Xây dựng chính sách lọc gói tin tĩnh.....	50
3.1.2. Xây dựng chính sách lọc gói tin động.....	51
3.2. Phân tích lựa chọn công cụ .....	51
* Hoạt động xử lý gói tin IP.....	53
3.3. Kết quả thử nghiệm thực thi chương trình.....	56
KẾT LUẬN.....	66
TÀI LIỆU THAM KHẢO .....	67
PHỤ LỤC .....	68

## BẢNG KÝ HIỆU CÁC TỪ VIẾT TẮT

ACK	Acknowledgement
AH	Authentication Header. Header xác thực được thêm vào sau header của gói tin IP
AES	Advanced Encryption Standard. Thuật toán mã hóa khối
DA	Destination Address. Địa chỉ IP đích
DES	Data Encryption Standard. Thuật toán mã hoá với 64 bit dữ liệu và 56 bit khoá.
DNS	Domain Name System. Hệ thống tên miền
DoS	Denial of Service. Tấn công từ chối dịch vụ
DDoS	Distributed Denial of Service. Tấn công từ chối dịch vụ phân tán
DNAT	Destination NAT
ESP	Encapsulated Security Payload. Phương thức đóng gói bảo vệ dữ liệu
ICMP	Internet Control Message Protocol. Sử dụng trong giao thức IP để truyền các thông tin điều khiển và lỗi mạng
IP	Internet Protocol (IPV4). Giao thức truyền trên mạng Internet
IDS	Intrusion Detect System. Hệ thống phát hiện xâm nhập
IOS	Intrusion
IPX	Internetwork packet Exchange. Giao thức mạng
LAN	Local area network. Mạng cục bộ
MAC	Media Access Control. Điều khiển truy cập
NAT	Network Address Translation. Phương thức chuyển đổi địa chỉ.
RSA	Rivest Shamir Adleman. RSA là một phương thức mã hoá công khai
SA	Security Association. Địa chỉ IP nguồn
SYN	Synchronous.
SNMP	Simple Network Management Protocol. Tập hợp giao thức
SMTP	Simple Mail Transfer Protocol. Giao thức truyền tải thư tín
UDP	User Datagram Protocol

OSI	Open Systems Interconnection. Mô hình tham chiếu kết nối hệ thống mở
TCP	Transmission Control Protocol. Giao thức điều khiển truyền vận
VPN	Virtual Private Network. Mạng riêng của một tổ chức nhưng sử dụng đường truyền công cộng.

## DANH MỤC CÁC HÌNH VẼ

Tên hình	Trang
<b>Chương 1</b>	
<b>Hình 1.1.</b> Kỹ thuật bắt gói tin thụ động	5
<b>Hình 1.2.</b> Kỹ thuật Sniffers chủ động	5
<b>Hình 1.3.</b> Kỹ thuật tấn công kiểu Smurf	7
<b>Hình 1.4.</b> Kỹ thuật tấn công kiểu SYN flood	8
<b>Hình 1.5.</b> Kỹ thuật tấn công DDoS	9
<b>Hình 1.6.</b> Kỹ thuật tấn công DDoS, các loại tấn công DDoS	9
<b>Hình 1.7.</b> Mạng riêng ảo	10
<b>Hình 1.8.</b> Sơ đồ thuật toán mã hóa	12
<b>Hình 1.9.</b> Vị trí của DES trên mạng	16
<b>Hình 1.10.</b> Bức tường Lửa	18
<b>Hình 1.11.</b> Firewall lọc gói	19
<b>Hình 1.12.</b> Tường lửa ứng dụng	21
<b>Hình 1.13.</b> tường lửa nhiều tầng	22
<b>Hình 1.14.</b> Kiến trúc máy chủ trung gian	23
<b>Hình 1.15.</b> Kiến trúc máy chủ sàng lọc	23
<b>Hình 1.16.</b> Kiến trúc mạng con sàng lọc	24
<b>Hình 1.17.</b> Mô hình sử dụng nhiều Bastion Host	24
<b>Hình 1.18.</b> Kiến trúc ghép chung Router trong và Router ngoài	25
<b>Hình 1.19.</b> Kiến trúc ghép chung Bastion Host và Router ngoài	25
<b>Chương 2</b>	
<b>Hình 2.1.</b> Các luồng gói tin trên bức tường lửa lọc gói	27
<b>Hình 2.2.</b> Lưu đồ thuật toán lọc gói tin tĩnh	29
<b>Hình 2.3a.</b> Tiêu đề mạng tin TCP	30
<b>Hình 2.3b.</b> Tiêu đề mạng tin UDP	31
<b>Hình 2.4.</b> Các cổng trong giao thức TCP	33
<b>Hình 2.5.</b> Quá trình bắt tay ba bước của giao thức TCP	33



<b>Hình 2.6.</b> Tiêu đề của gói tin IP	34
<b>Hình 2.7.</b> Lưu đồ thuật toán lọc gói tin động	38
<b>Hình 2.8.</b> Thông điệp ICMP trong gói tin IP	41
<b>Chương 3</b>	
<b>Hình 3.1.</b> Sơ đồ kết nối mạng trong trường học	47
<b>Hình 3.2.</b> Netfilter và TPTable trong nhân Linux	49
<b>Hình 3.3a, b.</b> Các chính sách luật lọc gói tin tĩnh	52
<b>Hình 3.4.</b> Các luật lọc gói tin tĩnh được cài đặt	53
<b>Hình 3.5a, b.</b> Các chính sách luật lọc gói tin động	54, 55
<b>Hình 3.6.</b> Các luật lọc gói tin động được cài đặt	55
<b>Hình 3.7.</b> Các luật trong firewall được active và bắt đầu thực thi trên HT	56
<b>Hình 3.8.</b> Giao diện chương trình trên Quickly	58
<b>Hình 3.9.</b> Cấm truy cập Internet	60
<b>Hình 3.10.</b> Cho phép truy cập Internet	60
<b>Hình 3.11.</b> Luật chưa được active	61
<b>Hình 3.12.</b> Luật được active	61

**DANH MỤC BẢNG**

<b>Tên bảng</b>	<b>Trang</b>
<b>Bảng 2.1.</b> Bảng dịch vụ và tương ứng với số cổng	32
<b>Bảng 3.2.</b> Miêu tả các target mà IPtables thường dùng	51