

ĐẠI HỌC THÁI NGUYÊN
TR- ỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

NGUYỄN THANH TÙNG

**KIỂM SOÁT AN NINH MẠNG MÁY TÍNH
VÀ ỨNG DỤNG**

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

NGUYỄN THANH TÙNG

**KIỂM SOÁT AN NINH MẠNG MÁY TÍNH
VÀ ỨNG DỤNG**

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Chuyên ngành: KHOA HỌC MÁY TÍNH

Mã số: 60.48.01

Người hướng dẫn khoa học: PGS.TS. TRỊNH NHẬT TIẾN

Thái Nguyên, 2014

LỜI CẢM ƠN

Lời đầu tiên tôi xin bày tỏ lòng biết ơn chân thành tới PGS.TS Trịnh Nhật Tiến đã tận tình hướng dẫn, giúp đỡ để tôi có thể hoàn thành đề tài nghiên cứu này.

Tôi gửi lời cảm ơn tới các thầy, cô giáo Trường Đại học Công nghệ Thông tin và Truyền thông - Đại học Thái Nguyên đã truyền đạt cho tôi những kiến thức chuyên đề, là cơ sở để tôi tiếp cận các kiến thức khoa học cơ bản và kiến thức chuyên ngành công nghệ thông tin. Tôi xin bày tỏ lòng biết ơn đối với các thầy cô giáo Phòng Quản lý đào tạo sau đại học đã tạo điều kiện để tôi có được thời gian học tập và nghiên cứu tốt nhất.

Tôi cũng đặc biệt muốn cảm ơn Sở Thông tin và Truyền thông và các sở, ban, ngành của tỉnh Tuyên Quang đã tạo điều kiện thuận lợi, giúp đỡ tôi trong quá trình tìm hiểu, nghiên cứu thực tế tại địa phương; cảm ơn sự giúp đỡ của gia đình, bạn bè và các đồng nghiệp trong thời gian qua.

Mặc dù đã cố gắng rất nhiều, song do điều kiện về thời gian và kinh nghiệm thực tế còn nhiều hạn chế nên không tránh khỏi thiếu sót. Vì vậy, tôi rất mong nhận được ý kiến góp ý của các thầy cô cũng như bạn bè, đồng nghiệp.

Tôi xin chân thành cảm ơn!

Thái Nguyên, tháng 7 năm 2014

Nguyễn Thanh Tùng

LỜI CAM ĐOAN

Tôi là Nguyễn Thanh Tùng, học viên lớp cao học khoá 2012-2014 ngành CNTT, chuyên ngành Khoa học máy tính. Tôi xin cam đoan luận văn "Kiểm soát an ninh mạng máy tính và ứng dụng" là do tôi nghiên cứu, tìm hiểu dưới sự hướng dẫn của PGS.TS.Trịnh Nhật Tiến. Tôi xin chịu trách nhiệm về lời cam đoan này.

Thái Nguyên, tháng 7 năm 2014

Tác giả

Nguyễn Thanh Tùng

Lớp Cao học KHMT 2012-2014

MỤC LỤC

LỜI CẢM ƠN	i
LỜI CAM ĐOAN	iv
MỤC LỤC.....	v
DANH MỤC HÌNH VẼ.....	vii
MỞ ĐẦU.....	1
<i>Chương 1. VẤN ĐỀ AN NINH MẠNG MÁY TÍNH.....</i>	<i>3</i>
1.1. TỔNG QUAN VỀ HẠ TẦNG MẠNG MÁY TÍNH.....	3
1.1.1. Khái niệm mạng máy tính	3
1.1.2. Các thiết bị kết nối mạng.....	4
1.1.3. Các hình thức kết nối mạng.....	4
1.1.4. Phân loại mạng máy tính	6
1.2. CÁC HIỂM HOẠ TRÊN MẠNG MÁY TÍNH	10
1.2.1. Xem trộm thông tin	11
1.2.2. Mạo danh.....	11
1.2.3. Vi phạm Tính bí mật thông tin	11
1.2.4. Vi phạm Tính toàn vẹn thông tin	12
1.2.5. Sự can thiệp của Tin tặc (Hacker).....	12
1.2.6. Vi phạm Tính toàn vẹn mã.....	12
1.2.7. Tấn công “Từ chối dịch vụ”	12
1.3. NGUYÊN NHÂN CỦA CÁC HIỂM HOẠ TRÊN MẠNG MÁY TÍNH	13
1.3.1. Do Dùng chung tài nguyên mạng MT.....	13
1.3.2. Do Sự phức tạp của hệ thống mạng MT	13
1.3.3. Do Ngoại vi không giới hạn của mạng MT.....	13
1.3.4. Do có Nhiều điểm tấn công.....	13
1.4. MỘT SỐ VẤN ĐỀ BẢO VỆ HỆ THỐNG VÀ MẠNG.....	13
1.4.1. Các vấn đề chung về bảo vệ hệ thống và mạng	13
1.4.2. Một số khái niệm và lịch sử bảo vệ hệ thống.....	14
1.4.3. Các loại lỗ hổng bảo vệ và phương thức tấn công mạng chủ yếu.....	15
1.5. KẾT LUẬN CHƯƠNG.....	18
<i>Chương 2. KIỂM SOÁT AN NINH MẠNG MÁY TÍNH.....</i>	<i>19</i>
2.1. KIỂM SOÁT TRUY NHẬP MẠNG MÁY TÍNH	19
2.1.1. Hiểm họa về an toàn đối với hệ thống máy tính	19
2.1.2. Phương thức thực hiện các cuộc tấn công.....	20
2.1.3. Các hình thức ngăn chặn và kiểm soát lỗi vào ra thông tin	21

2.1.4. Sử dụng mật khẩu một cách an toàn.....	25
2.2. KIỂM SOÁT VÀ XỬ LÝ CÁC “LỖ HỔNG” THIẾU AN NINH TRONG MẠNG MÁY TÍNH.....	28
2.2.1. Khái niệm “lỗ hổng” trong ATTT	28
2.2.2. Phân loại lỗ hổng theo mức nguy hiểm.....	28
2.2.3. “Lỗ hổng” trong hệ thống mạng.....	28
2.2.4. Xử lý các lỗ hổng thiếu an ninh bằng các phương pháp bảo vệ.....	29
2.3. KIỂM SOÁT VÀ PHÒNG CHỐNG CÁC DẠNG "TẤN CÔNG" VÀO MẠNG MÁY TÍNH.....	32
2.3.1. Tấn công trên mạng.....	32
2.3.2. Phòng chống các dạng tấn công vào mạng máy tính	33
2.4. MỘT SỐ CÔNG CỤ BẢO VỆ MẠNG MÁY TÍNH	36
2.4.1. Tường lửa	36
2.4.2. Mạng riêng ảo.....	38
2.5. KẾT LUẬN CHƯƠNG.....	43
<i>Chương 3. ỨNG DỤNG MÃ NGUỒN MỞ CẤU HÌNH CÁC GÓI LỌC TIN</i>	<i>44</i>
3.1. BÀI TOÁN THỰC TẾ	44
3.1.1. Khảo sát nhu cầu	44
3.1.2. Mô hình	44
3.1.3. Giải pháp	45
3.2. CÀI ĐẶT CẤU HÌNH CÁC GÓI LỌC TIN	45
3.2.1. Firewall Iptable trên Redhat.....	45
3.2.2. Cấu hình Iptable	51
3.2.3. Ứng dụng Iptables làm IP Masquerading.....	54
3.2.4. Ứng dụng IPTABLES làm NAT	62
KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN	73
TÀI LIỆU THAM KHẢO.....	74

DANH MỤC CÁC CHỮ VIẾT TẮT

Viết tắt	Tiếng Anh	Tiếng Việt
ATTT		An toàn thông tin
DHCP	Dynamic Host Configuration Protocol	Giao thức cấu hình động máy chủ
DNS	Domain Name System	Hệ thống tên miền
FTP	File Transfer Protocol	Giao thức truyền tập tin
GAN	Global Area Network	Mạng toàn cầu
GUI	Graphical User Interface	Giao diện người dùng đồ họa
HĐH		Hệ điều hành
HTTP	Hypertext Transfer Protocol	Giao thức truyền tải siêu văn bản
HTTPS	Hypertext Transfer Protocol Secure	Là một sự kết hợp giữa giao thức HTTP và giao thức bảo mật SSL hay TLS.
IP	Internet Protocol	Giao thức Internet
LAN	Local Area Network	Mạng nội bộ
MAN	Metropolitan Area Network	Mạng đô thị
MT		Máy tính
OSI	Open Systems Interconnection Reference Model	Mô hình tham chiếu kết nối các hệ thống mở
TCP	Transmission Control Protocol	Giao thức Điều Khiển Truyền Thông
WAN	Wide Area Network	Mạng diện rộng

DANH MỤC HÌNH VẼ

Số hiệu hình vẽ	Tên hình vẽ
Hình 1.1	Kết nối hình sao
Hình 1.2	Kết nối dạng đường thẳng
Hình 1.3	Kết nối dạng đường tròn
Hình 1.4	Kết nối vệ tinh
Hình 1.5	Xem trộm thông tin
Hình 1.6	Mạo danh
Hình 1.7	Sửa nội dung thông tin
Hình 2.1	Hacker
Hình 2.2	Mật khẩu là cách thức bảo vệ cơ bản nhất
Hình 2.3	Sử dụng và cất giữ mật khẩu một cách an toàn
Hình 2.4	Mô hình mạng đa nền tảng
Hình 2.5	Tường lửa cứng
Hình 2.6	Tường lửa mềm
Hình 2.7	Mạng riêng ảo
Hình 2.8	Truy nhập từ xa
Hình 2.9	Đặc trưng của máy khách VPN
Hình 3.1	Mô hình tường lửa bảo vệ mạng
Hình 3.2	Đường đi của packet
Hình 3.3	Mô hình kết nối máy Linux và Anybox
Hình 3.4	Mô hình kết nối máy Linux với mạng nội bộ và Internet

MỞ ĐẦU

1. Lý do chọn đề tài

Hiện nay các cơ quan, tổ chức đều có hệ thống mạng máy tính riêng kết nối với mạng Internet và ứng dụng nhiều tiện ích CNTT trong công tác chuyên môn, nghiệp vụ. Việc làm này đã góp phần tích cực trong quản lý, điều hành, kết nối, quảng bá và là chìa khoá thành công cho sự phát triển chung của họ. Trong các hệ thống mạng máy tính đó có chứa rất nhiều các dữ liệu, các thông tin quan trọng liên quan đến hoạt động của các cơ quan, tổ chức. Điều này hấp dẫn, thu hút các kẻ tấn công. Công nghệ về máy tính và mạng máy tính liên tục phát triển và thay đổi, các phần mềm mới liên tục ra đời mang đến cho con người nhiều tiện ích hơn, lưu trữ được nhiều dữ liệu hơn, tính toán tốt hơn, sao chép và truyền dữ liệu giữa các máy tính nhanh chóng thuận tiện hơn,...Nhưng bên cạnh đó, hệ thống mạng vẫn còn tồn tại nhiều lỗ hổng, các nguy cơ về mất an toàn thông tin. Các vụ xâm nhập mạng lấy cắp thông tin nhạy cảm cũng như phá hủy thông tin diễn ra ngày càng nhiều, thủ đoạn của kẻ phá hoại ngày càng tinh vi.

Vấn đề an ninh mạng máy tính đã được biết đến khá nhiều trên thế giới và hiện nay cũng đã có rất nhiều phương pháp kiểm soát an ninh mạng máy tính. Tuy nhiên, ở địa phương hiện nay, vấn đề an ninh mạng máy tính vẫn chưa được nhận thức một cách đầy đủ. Từ đó tôi lựa chọn đề tài "Kiểm soát an ninh mạng máy tính và ứng dụng" là cơ sở nghiên cứu chính của luận văn này.

2. Đối tượng và phạm vi nghiên cứu

Đối tượng nghiên cứu:

Nghiên cứu các phương pháp kiểm soát an ninh mạng máy tính (Kiểm soát truy nhập mạng máy tính; kiểm soát và xử lý các "lỗ hổng" thiếu an ninh trong mạng máy tính; kiểm soát và phòng chống các dạng "tấn công" vào mạng máy tính).

Phạm vi nghiên cứu:

Nghiên cứu về tường lửa và mạng riêng ảo. Ứng dụng tường lửa mã nguồn mở cài đặt thử nghiệm chương trình.

3. Những nội dung nghiên cứu chính

Chương 1. Vấn đề an ninh mạng máy tính

Nội dung chương này nêu tổng quan về mạng máy tính, các hiểm họa trên mạng máy tính và nguyên nhân của các hiểm họa.

Chương 2. Kiểm soát an ninh mạng máy tính

Nội dung chương này trình bày các phương pháp kiểm soát an ninh mạng máy tính.

Chương 3. Ứng dụng mã nguồn mở để cấu hình các gói lọc tin

Giới thiệu về mô hình mạng máy tính tại địa phương và ứng dụng tường lửa nguồn mở để kiểm soát an ninh mạng.