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

DƯƠNG THANH TUẤN

MỘT SỐ KỸ THUẬT VÀ XÂY DỰNG MÔ HÌNH PHÒNG THỦ MẠNG

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN - NĂM 2014

LỜI CAM ĐOAN

Luận văn tốt nghiệp là sản phẩm tổng hợp toàn bộ các kiến thức mà sinh viên đã học được trong suốt thời gian học tập tại trường đại học. Ý thức được điều đó, với tinh thần nghiêm túc, tự giác cùng sự lao động miệt mài của bản than và sự hướng dẫn tận tình của thầy giáo TS. Hồ Văn Canh em đã hoàn thành xong luận văn tốt nghiệp cao học của mình.

Em xin cam đoan: Nội dung luận văn của em không sao chép nội dung cơ bản từ các luận văn khác và sản phẩm của luận văn là của chính bản thân em nghiên cứu xây dựng lên. Mọi thông tin sai lệch em xin hoàn toàn chịu trách nhiệm trước hội đồng bảo vệ.

Học viên

Dương Thanh Tuấn

LỜI CẢM ƠN

Qua thời gian học tập và rèn luyện tại Trường Công nghệ thông tin – Đại học Thái Nguyên, đến nay chúng em đã kết thúc khóa học 2 năm và hoàn thành luận án tốt nghiệp. Để có được kết quả này em xin chân thành cảm ơn:

- Ban chủ nhiệm khoa Công nghệ thông tin cùng các thầy, cô giáo trong khoa đã giảng dạy, quan tâm và tạo điều kiện thuận lợi để chúng em học tập và rèn luyện trong suốt thời gian theo học tại trường.
- Thầy giáo - TS. Hồ Văn Canh đã tận tình hướng dẫn, giúp đỡ em trong quá trình học tập và đặc biệt là trong suốt thời gian làm luận văn tốt nghiệp. Thầy luôn quan tâm và rất nhiệt tình hướng dẫn em từ việc tìm tài liệu cho đến việc định hướng lựa chọn giải pháp để triển khai luận văn. Thầy cũng luôn nhắc nhở, động viên em mỗi khi gặp khó khăn, nhờ vậy mà em đã hoàn thành tốt luận văn tốt nghiệp của mình đúng thời hạn.
- Em cũng xin gửi lời cảm ơn tới gia đình, tập thể lớp Cao học CK11G, ban quan hệ quốc tế, trung tâm hợp tác quốc tế (ICC) – Đại học Thái Nguyên đã động viên, giúp đỡ, tạo điều kiện cho em được giao lưu, học hỏi với các thầy giáo, sinh viên trên quốc tế trong thời gian học tập tại Thái Nguyên.

MỤC LỤC

DANH MỤC KÝ HIỆU, CHỮ VIẾT TẮT

Viết tắt	Ý nghĩa
OSI	Open System Interconnection
AH	Giao thức xác thực AH-Authentication Header
ESP	Giao thức đóng gói (xác thực + bảo mật) ESP - Encapsulating Security Payload
CA	Cấp giấy xác nhận - Certification Authority
MD5	Phương thức mã hóa MD5
IDS	Hệ thống phát hiện xâm nhập - Intrustion Detection System
NIDS	Network Base IDS
IP	Địa chỉ IP
TCP	Giao thức điều khiển truyền vận - Transmission Control Protocol
Anonymous	Kẻ nặc danh, tin tặc
SPI	Chỉ số tham số bảo mật - Security Parameter Index
CVP	Thời hạn hiệu lực của chứng chỉ -Certificate Validity Period
Mesh CA Model	Mô hình CA dạng lưới

DANH MỤC CÁC HÌNH VẼ

LỜI MỞ ĐẦU

Cùng với sự phát triển của công nghệ thông tin, công nghệ mạng máy tính và sự phát triển của mạng internet ngày càng phát triển đa dạng và phong phú. Các dịch vụ trên mạng đã thâm nhập vào hầu hết các lĩnh vực trong đời sống xã hội. Các thông tin trên internet cũng đa dạng về nội dung và hình thức, trong đó có rất nhiều thông tin cần được bảo mật cao hơn bởi tính kinh tế, tính chính xác và tính tin cậy của nó.

Bên cạnh đó, cách hình thức phá hoại mạng cũng trở nên tinh vi và phức tạp hơn. Do đó đối với hệ thống, nhiệm vụ bảo mật được đặt ra cho người quản trị mạng là hết sức quan trọng và cần thiết. Xuất phát từ những thực tế đó, chúng ta sẽ tìm hiểu về các cách tấn công phổ biến nhất hiện nay và các cách phòng thủ các loại tấn công này, đặc biệt là phòng thủ trong website.

Được sự giúp đỡ của thầy giáo TS. Hồ Văn Canh cùng với nhu cầu thực tế về tấn công, phòng thủ mạng, em thực hiện luận văn tốt nghiệp với những mặt mình đã đạt được: Hiểu được và nắm vững các cách phòng thủ, tấn công mạng cơ sở nhất, mong muốn góp một phần nhỏ vào việc nghiên cứu và tìm hiểu về các vấn đề an ninh mạng giúp cho việc học tập và nghiên cứu.

Tuy nhiên, trong thời gian có hạn và khả năng tìm hiểu của em còn nhiều hạn chế nên trong luận văn này không thể trách được thiếu sót. Kính mong các thầy cô, cùng các bạn sinh viên trong khoa đóng góp ý kiến để luận văn của em không những được hoàn thiện hơn trong đợt bảo vệ tốt nghiệp này. Em mong, với sự đóng góp nhiệt tình của các thầy, cô giáo cùng với các bạn sinh viên sẽ giúp em hoàn thiện và phát triển luận văn tốt nghiệp của em thành sản phẩm thương mại có tính ứng dụng thực tế mang lợi ích đến người dùng đồng thời cũng là một tài liệu quí giá để cho các bạn sinh viên khóa sau lấy để tham khảo và phát triển tiếp những phần còn chưa đạt được.

Em xin chân thành cảm ơn!

Thái Nguyên, ngày 29 tháng 09 năm 2014

Học viên: **Dương Thanh Tuấn**

CHƯƠNG 1: TỔNG QUAN VỀ AN NINH MẠNG

1.1. Tình hình an ninh mạng trong nước và quốc tế

1.1.1. Tình hình an ninh mạng tại Việt Nam

Khi CNTT ngày càng phát triển, Internet ngày càng được sử dụng rộng rãi và đa dạng, thì vấn đề an ninh mạng càng trở nên phức tạp và nóng bỏng. Đặc biệt là trong những năm gần đây.

Dưới đây là tình hình an ninh mạng tại Việt Nam một vài năm trở lại đây:

Số liệu chung:

	Máy tính bị nhiễm virus (Triệu lượt)	Dòng virus mới	Số Website Việt Nam bị hacker tấn công	Cảnh báo lỗ hổng
Năm 2007	33,6	6752	342	140
Năm 2008	59,4	33137	461	104
Năm 2009	64,7	50128	1037	
Năm 2010	58,6	57835	> 1000	
Năm 2011	64,2	38961	2245	

Qua bảng số liệu chung chúng ta thấy: Số lượt máy tính bị nhiễm virus không ngừng tăng lên qua các năm. Mỗi năm đều có một số lượng lớn dòng virus mới xuất hiện. Số lượng website bị tấn công cũng không ngừng tăng lên với sô lượng lớn. Điều này cho thấy rõ sự nóng bỏng của an ninh mạng Việt Nam

- **Các website và hệ thống Server liên tục bị tấn công**

Hiệp hội an toàn thông tin Việt Nam cho biết: "Việt Nam là 1 trong 5 nước có nguy cơ mất an toàn thông tin cao nhất".

Hiện số thuê bao Internet chiếm gần 32% dân số Việt Nam. Đa số các doanh nghiệp và các tổ chức có hệ thống mạng và website giới thiệu, quảng

bá thương hiệu, với gần 200.000 tên miền .vn, và hàng triệu tên miền thương mại. Có rất nhiều doanh nghiệp đã ứng dụng thanh toán trực tuyến vào công việc kinh doanh và giao dịch.

Thế nhưng, mạng Internet Việt Nam còn rất nhiều tiềm ẩn, nguy cơ về an ninh an toàn thông tin. Năm 2010 được đánh giá là năm thực sự nóng bỏng của an ninh an toàn thông tin trên thế giới chung và an ninh mạng Việt Nam nói riêng. Hàng loạt website lớn bị tấn công với mức độ phức tạp ngày càng gia tăng. Ở nước ta, theo đánh giá của một số chuyên gia về an ninh mạng, các tên miền .vn đang đứng hàng thứ 3 trong bảng xếp hạng các tên miền có nguy cơ bị tấn công. Cách đây chưa lâu, cuộc tấn công quy mô lớn, liên tục và kéo dài đã phá hủy hầu như gần hết cơ sở dữ liệu đã lưu trữ 10 năm của báo Vietnamnet.

Các cuộc tấn công trên mạng chủ yếu có mục tiêu vụ lợi, có tổ chức và mang tính quốc tế đang nở rộ với quy mô lớn. Thủ phạm các cuộc tấn công nhằm vào các website có trình độ cao, hình thức tấn công tinh vi, chuyên nghiệp và rất khó chống đỡ. Mục tiêu của hacker không chỉ là các tổ chức, doanh nghiệp tài chính, ngân hàng mà là tất cả hệ thống. Các cuộc tấn công trên là một lời cảnh báo về an toàn thông tin đối với các báo điện tử và những website quan trọng của Việt Nam.

Năm 2011, đã có 38.961 dòng virus xuất hiện mới, lây lan nhiều nhất là virus W32.Sality.PE. Virus này đã lây nhiễm trên 4.2 triệu lượt máy tính. Cũng trong 2011, đã có 2,245 website của các cơ quan, doanh nghiệp tại Việt Nam bị tấn công, tính trung bình mỗi tháng có 187 website bị tấn công.

Năm 2011 là năm của các cuộc tấn công mạng, liên tiếp xảy ra các cuộc tấn công với các hình thức khác nhau vào hệ thống của các tổ chức, doanh nghiệp tại Việt Nam. Có những cuộc tấn công xâm nhập trái phép phá hoại cơ sở dữ liệu hoặc deface các website. Cũng có những cuộc tấn công