ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG

TRƯƠNG HỒNG TIỆP

NGHIÊN CỨU CƠ CHẾ THÂM NHẬP HỆ THỐNG MÁY TÍNH THÔNG QUA LỖ HỔNG BẢO MẬT VÀ ỨNG DỤNG TRONG CÔNG TÁC BẢO ĐẢM AN NINH MẠNG

LỜI CAM ĐOAN

Tôi xin cam đoan bản luận văn *"Nghiên cứu cơ chế thâm nhập hệ thống máy tính thông qua lỗ hổng bảo mật và ứng dụng trong công tác đảm bảo an ninh mạng"* là công trình nghiên cứu của tôi dưới sự hướng dẫn khoa học của TS. Nguyễn Ngọc Cương, tham khảo các nguồn tài liệu đã được chỉ rõ trong trích dẫn và danh mục tài liệu tham khảo. Các nội dung công bố và kết quả trình bày trong luận văn này là trung thực và chưa từng được ai công bố trong bất cứ công trình nào.

Thái Nguyên, tháng 11 năm 2012

Trương Hồng Tiệp

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ VÀ BẢNG BIỂU

MỞ ĐẦU

Trong những năm gần đây, việc xâm nhập, tấn công mạng của hacker và tội phạm mạng nhằm vào các hệ thống máy tính ở Việt Nam và trên thế giới có xu hướng ngày càng gia tăng, gây nhiều hậu quả nghiêm trọng về kinh tế và chính trị.

Các cuộc tấn công vào các hệ thống máy tính có thể được tiến hành bằng nhiều kỹ thuật khác nhau. Trong đó, đặc biệt có các cuộc tấn công thông qua khai thác lỗ hổng bảo mật của hệ thống và ứng dụng. Do một số ứng dụng hiện nay thường sử dụng các mã nguồn mở nên có nhiều lỗi sẽ gây ra các lỗ hổng, dẫn đến các hệ thống sử dụng các phần mềm này có thể bị tấn công.

Chính vì vậy, việc tìm kiếm, phát hiện các lỗ hổng trên hệ thống máy tính để hiểu được cơ chế và kỹ thuật xâm nhập chúng là cần thiết trong phòng chống sự tấn công của hacker vào hệ thống.

Đây là lý do để chúng tôi lựa chọn đề tài: "***Nghiên cứu cơ chế thâm nhập hệ thống máy tính thông qua lỗ hổng bảo mật và ứng dụng trong công tác đảm bảo an ninh mạng***".

1. Mục tiêu của đề tài

Tìm hiểu các lỗ hổng bảo mật của hệ thống và ứng dụng, bản chất quá trình thâm nhập tấn công của hacker vào hệ thống máy tính thông qua khai thác lỗ hổng bảo mật và đưa ra phương pháp phòng tránh đảm bảo an ninh máy tính và mạng máy tính.

2. Nội dung nghiên cứu

Nghiên cứu, tìm hiểu một số lỗ hổng bảo mật phổ biến trên hệ thống máy tính như: lỗ hổng bảo mật ứng dụng Web, Internet Explorer, Window Microsoft,..

Nghiên cứu các phương pháp thâm nhập hệ thống máy tính trên cơ sở khai thác các lỗ hổng bảo mật như: Buffer Overflow (tràn bộ đệm), tấn công từ chối dịch vụ, tấn công Injection,...

Viết chương trình thử nghiệm tấn công bằng kết hợp phương pháp gây tràn bộ đệm và cài đặt vào máy cần tấn công thông qua lỗ hổng bảo mật.

Nghiên cứu các phương pháp, công cụ để dò tìm, phát hiện lỗ hổng bảo mật thông qua các công cụ bảo mật như: Retina, Backtrack,...

Đề xuất một số phương pháp kiểm tra và phát hiện sự xâm nhập.

3. Phương pháp nghiên cứu

Phương pháp tổng hợp: thu thập tài liệu, đối chiếu, so sánh, phân tích, liệt kê, đối sánh, trực quan, thực nghiệm,...

Phương pháp chuyên gia: tìm hiểu các hệ thống máy tính, xây dựng hệ thống hoàn chỉnh, các phần mềm phát hiện lỗ hổng bảo mật, thâm nhập hệ thống.

Nghiên cứu ngôn ngữ lập trình để viết chương trình gây tràn bộ đệm.

Phương pháp thực nghiệm: sử dụng mạng máy tính để thực hành xâm nhập thông qua lỗ hổng bảo mật.

4. Cấu trúc luận văn

Chương 1: TỔNG QUAN VỀ BẢO MẬT HỆ THỐNG MÁY TÍNH

1.1. An toàn bảo mật thông tin

1.1.1. Khái niệm an toàn bảo mật thông tin

Ngày nay, với sự phát triển bùng nổ của công nghệ thông tin, hầu hết các thông tin của tổ chức, doanh nghiệp như chiến lược kinh doanh, các thông tin về khách hàng,... điều được lưu trữ trên hệ thống máy tính. Cùng với sự phát triển của các cơ quan, tổ chức, doanh nghiệp là những đòi hỏi ngày càng cao của môi trường làm việc nhanh chóng, hiệu quả nên thông tin cần được chia sẻ cho nhiều đối tượng khác nhau thông qua môi trường Intranet hay Internet. Việc mất mát, rò rỉ thông tin có thể ảnh hưởng nghiêm trọng đến tài chính, danh tiếng,... của các cơ quan, tổ chức.

Các phương thức tấn công thông qua mạng ngày càng tinh vi, phức tạp có thể dẫn đến mất mát thông tin, thậm chí có thể làm sụp đổ hoàn toàn hệ thống thông tin của tổ chức. Vì vậy an toàn bảo mật thông tin là nhiệm vụ rất nặng nề và khó đoán trước được.

An toàn bảo mật (an ninh) thông tin là cách bảo vệ, đảm bảo cho tất cả các thành phần của hệ thống máy tính bao gồm dữ liệu, thiết bị, cơ sở hạ tầng mạng, và đảm bảo mọi tài nguyên được sử dụng tương ứng với một chính sách hoạt động được ấn định và với chỉ người có thẩm quyền tương ứng.

An toàn bảo mật thông tin gồm 3 hướng chính sau:

- Đảm bảo an toàn thông tin tại máy chủ
- Bảo đảm an toàn thông tin phía máy trạm
- Bảo đảm an toàn thông tin trên đường truyền

An toàn bảo mật thông tin bao gồm:

- Xác định chính sách các khả năng, nguy cơ xâm phạm hệ thống máy tính, các sự cố rủi ro đối với thiết bị, dữ liệu trên hệ thống để có giải pháp phù hợp đảm bảo an toàn cho hệ thống.

- Đánh giá nguy cơ tấn công của hacker tác động đến hệ thống, sự phát tán virus.. An toàn bảo mật hệ thống thông tin là một trong những vấn dề cực kỳ quan trọng trong các hoạt đọng, giao dịch điện tử và trong việc khai thác, sử dụng tài nguyên của hệ thống.

- Xác định chính xác cấp độ an toàn, đánh giá nguy cơ, các lỗ hổng khiến hệ thống có thể bị xâm phạm thông qua cách tiếp cận có cấu trúc. Xác định những nguy cơ ăn cắp, phá hoại máy tính, thiết bị, nguy cơ virus, bọ gián điệp,.. nguy cơ xóa, phá hoại CSDL, ăn cắp mật khẩu,... nguy cơ đối với sự hoạt động của hệ thống như nghẽn mạng, nhiễu điện tử... Khi đánh giá được hết những nguy cơ ảnh hưởng tới an ninh mạng thì mới có thể có được những biện pháp tốt nhất để đảm bảo an toàn cho hệ thống.

- Sử dụng hiệu quả các công cụ bảo mật (như Firewall...) và những biện pháp, chính sách cụ thể chặt chẽ.

1.1.2. Hệ thống và tài sản của hệ thống máy tính

Hệ thống là một tập hợp các máy tính gồm các thành phần phần cứng, phần mềm và dữ liệu làm việc được tích lũy qua thời gian.

Tài sản của hệ thống bao gồm:

- Phần cứng
- Phần mềm
- Dữ liệu
- Các truyền thông giữa các máy tính của hệ thống
- Môi trường làm việc
- Con người

1.1.3. Đặc trưng kỹ thuật của an toàn bảo mật

- *Xác thực (Authentification*): Kiểm tra tính xác thực của một thực thể giao tiếp trên mạng. Một thực thể có thể là một người sử dụng, một chương trình máy tính, hoặc một thiết bị phần cứng. Các hoạt động kiểm tra tính xác thực được đánh giá là quan trọng nhất trong các hoạt động của một phương thức bảo mật. Một hệ thống thông thường phải thực hiện kiểm tra tính xác thực của các phương thức bảo mật dựa vào 3 mô hình chính sau:

+ Đối tượng cần kiểm tra phải cung cấp những thông tin trước, ví dụ như password, hoặc mã số thông tin cá nhân PIN (Personal Infomation Number).

+ Kiểm tra dựa vào mô hình những thông tin đã có, đối tượng kiểm tra cần phải thể hiện những thông tin mà chúng sở hữu, ví dụ như Private Key, hoặc số thẻ tín dụng.