BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG

----- ~ ------ ~ ------ ~ -----

ISO 9001:2008

# ĐỒ ÁN TỐT NGHIỆP

NGÀNH CÔNG NGHỆ THÔNG TIN

*Đề tài*: Một số dạng "tấn công" hệ thống thông tin và phòng tránh bằng xử lý các "lỗ hổng" thiếu an ninh


Giáo viên hướng dẫn : PGS.TS. Trịnh Nhật Tiến

Sinh viên thực hiện : Trần Thị Thủy

Mã số sinh viên : 101276


HẢI PHÒNG – 2010

# LỜI CẢM ƠN

-------- o0o-------

Trước hết, em xin được bày tỏ lòng biết ơn sâu sắc tới thầy hướng dẫn **PGS.TS. Trịnh Nhật Tiến,** trường Đại học Công nghệ, Đại học QG Hà Nội. Trong quá trình nghiên cứu đề tài, thầy đã tận tình giúp đỡ, cung cấp đầy đủ các tài liệu và giải đáp những thắc mắc của em liên quan đến đề tài.Tạo điều kiện tốt nhất để em thực hiện và hoàn thành đồ án tốt nghiệp của mình.

Em xin được gửi lời cảm ơn tới Ban lãnh đạo trường Đại học Dân Lập Hải phòng, những người đã tạo điều kiện thuận lợi về cơ sở vật chất, trang thiết bị,... tốt nhất, tạo điều kiện cho chúng em có môi trường học tập tốt và có điều kiện tiếp thu những công nghệ, khoa học kỹ thuật mới.

Em xin chân thành cảm ơn các thầy cô giáo trường Đại học Dân Lập Hải Phòng nói chung, các thầy cô giáo trong khoa Công nghệ thông tin, trường Đại học Dân Lập Hải Phòng. Những người thầy, người cô đã tận tình giảng dạy và truyền đạt cho em những kiến thức, kinh nghiệm quý báu trong suốt quá trình học tập, rèn luyện tại trường Đại học Dân Lập Hải Phòng.

Cuối cùng, em xin được gửi lời cảm ơn tới gia đình, bạn bè đã động viên, giúp đỡ, tạo mọi điều kiện thuận lợi cho em trong thời gian nghiên cứu và hoàn thành đồ án tốt nghiệp của mình.

Hải Phòng, ngày .... tháng 07 năm 2009

Sinh viên

Trần Thị Thuỷ

# NHIỆM VỤ ĐỀ TÀI

Nội dung và các yêu cầu cần giải quyết trong nhiệm vụ đề tài tốt nghiệp

**1/. Tên đề tài**

Một số dạng "tấn công" hệ thống thông tin và phòng chống bằng xử lý các "lỗ hổng" thiếu an ninh.

**2/. Nhiệm vụ đề tài**

Các yêu cầu cần giải quyết

* Tìm hiểu và nghiên cứu lý thuyết:

+ Tìm hiểu một số loại "lỗ hổng" thiếu an ninh trong hệ thống thông tin (thông qua mạng máy tính, hệ điều hành, cơ sở dữ liệu,...).

+ Tìm hiểu một số dạng "tấn công" hệ thống thông tin thông qua "lỗ hổng".

+ Nghiên cứu phương pháp phòng tránh "tấn công" bằng xử lý các "lỗ hổng".

* Thử nghiệm chương trình:

Chỉ ra một ví dụ cụ thể để phòng tránh "lỗ hổng".

Trong đó thử nghiệm chương trình ký số để xác thực, xử lý "lỗ hổng".

# BẢNG KÝ HIỆU CÁC TỪ VIẾT TẮT

| STT | Từ viết tắt | Từ đầy đủ | Nghĩa tiếngViệt (nếu có) |
|---|---|---|---|
| 1 | ATTT | An toàn thông tin | |
| 2 | SSL | Secure Sockets Layer | Giao thức web |
| 3 | FTP | File Transfer Protocol | Giao thức truyền tệp tin |
| 4 | DoS | Denial of Service | Từ chối dịch vụ |
| 5 | TCP | Transmission Control Protocol | Giao thức điều khiển đường truyền |
| 6 | IP | Internet Protocol | Giao thức Internet |
| 7 | UDP | User DataGram Protocol | Giao thức gói dữ liệu người dùng |
| 8 | IE | Internet Explorer | Trình duyện mạng liên kết |
| 9 | CPU | Central Processing Unit | Đơn vị xử lý trung tâm |
| 10 | URL | Address To An Internet or Intranet Site | Địa chỉ tới một trạm Internet hay mạng nội bộ |
| 11 | IETF | Internet Engineering Task Force | Tổ chức quốc tế Internet |
| 12 | ARP | Address Resolution Protocol | Giao thức phân giải địa chỉ |
| 13 | MAC | | Địa chỉ cứng máy tính |
| 14 | IPSec | Internet Protocol Security | Bảo mật giao thức mạng |
| 15 | L2F | Layer 2 Forwarding | |
| 16 | L2TP | Layer 2 Tunneling Protocol | |
| 17 | UAC | User Account Control | Điều khiển tài khoản người dùng |
| 18 | TPM | Trusted Platform Module | |
| 19 | HĐH | Hệ Điều Hành | |
| 20 | SQL | Structured Query Language | Ngôn ngữ truy vấn có cấu trúc |

# MỤC LỤC

# *Chương 1*. TỔNG QUAN VỀ AN TOÀN THÔNG TIN

## 1.1. VẤN ĐỀ AN TOÀN THÔNG TIN

### 1.1.1. Tại sao cần bảo đảm an toàn thông tin ?

Sự xuất hiện Internet và mạng máy tính giúp cho việc trao đổi thông tin trở lên nhanh gọn, dề dàng: E-business (Electronic business:Giao dịch điện tử) cho phép thực hiện các giao dịch buôn bán trên mạng, hay E-mail (Thư điện tử) cho phép nhận hay gửi thư ngay trên máy tính của mình, …

Tuy nhiên, một số vấn đề mới lại phát sinh. Thông tin quan trọng nằm ở kho dữ liệu hay đang trên đường truyền có thể bị trộm cắp, bị làm sai lệch, bị giả mạo. Điều này có thể ảnh hưởng lớn tới các công ty, các cơ quan, tổ chức hay cả một quốc gia. Như: Bí mật kinh doanh, tình hình tài chính, tin tức an ninh quốc gia, …

Để giải quyết tình hình trên, vấn đề đảm bảo ***An toàn thông tin (ATTT)*** đã được đặt ra trong lý luận cũng như trong thực tiễn.

Sự phát triển mạnh mẽ của Công nghệ thông tin (CNTT), ATTT đã trở thành một khoa học thực thụ.

### 1.1.2. Khái niệm về an toàn thông tin

❖ ***Khái niệm***

An toàn thông tin (ATTT) nghĩa là thông tin được bảo vệ, các hệ thống và những dịch vụ có khả năng chống lại những tai hoạ, lỗi và sự tác động không mong đợi, các thay đổi tác động đến độ an toàn của hệ thống là nhỏ nhất.

❖ ***Đặc điểm hệ thống không an toàn***

Hệ thống có một trong các đặc điểm sau là không an toàn:

- Các thông tin dữ liệu trong hệ thống bị người không được quyền truy nhập tìm cách lấy và sử dụng (thông tin bị rò rỉ).
- Các thông tin trong hệ thống bị thay thế hoặc sửa đổi làm sai lệch nội dung (thông tin bị xáo trộn).

Thông tin chỉ có giá trị cao khi đảm bảo tính chính xác và kịp thời. Quản lý an toàn và sự rủi ro được gắn chặt với quản lý chất lượng. Khi đánh giá độ ATTT cần phải dựa trên phân tích rủi ro, tăng sự an toàn bằng cách giảm tối thiểu rủi ro. Đánh giá cần hài hoà với đặc tính, cấu trúc hệ thống, quá trình kiểm tra chất lượng và các yêu cầu ATTT.

## 1.2. NỘI DUNG CỦA AN TOÀN THÔNG TIN

Khi nhu cầu trao đổi thông tin ngày càng lớn và đa dạng, các tiến bộ về điện tử - viễn thông và công nghệ thông tin không ngừng được phát triển ứng dụng để nâng cao chất lượng và lưu lượng truyền tin thì các quan niệm ý tưởng và biện pháp bảo vệ thông tin cũng được đổi mới. Bảo vệ thông tin là một chủ đề rộng, có liên quan đến nhiều lĩnh vực và trong thực tế có rất nhiều phương pháp bảo vệ thông tin.

### 1.2.1. Phương pháp bảo vệ thông tin

Các phương pháp bảo vệ thông tin có thể được quy tụ vào ba nhóm sau:

- Bảo vệ thông tin bằng các biện pháp hành chính.
- Bảo vệ thông tin bằng các biện pháp kỹ thuật (phần cứng).
- Bảo vệ thông tin bằng các biện pháp thuật toán (phần mềm).

Ba nhóm trên có thể được ứng dụng riêng rẽ hoặc phối kết hợp. Môi trường khó bảo vệ thông tin nhất và cũng là môi trường đối phương dễ xâm nhập nhất đó là môi trường mạng và truyền tin. Biện pháp hiệu quả nhất và kinh tế nhất hiện nay trên mạng truyền tin là biện pháp thuật toán (phần mềm).

### 1.2.2. Nội dung an toàn thông tin

#### *1.2.1.1. Mục tiêu của an toàn thông tin*

Hiện nay các biện pháp tấn công hệ thống thông tin càng ngày càng tinh vi, sự đe doạ tới độ ATTT có thể đến từ nhiều nơi theo nhiều cách, chúng ta nên đưa ra các chính sách và phương pháp đề phòng cần thiết. ATTT là bảo vệ các thông tin và tài nguyên theo các yêu cầu sau:

**** Bảo đảm bí mật (Bảo mật)*:**

Thông tin không bị lộ đối với người không được phép.

**** Bảo đảm toàn vẹn (bảo toàn)*:**

Ngăn chặn hay hạn chế việc bổ sung, loại bỏ và sửa dữ liệu không được phép.

**** Bảo đảm xác thực (chứng thực)*:**

Xác thực đối tác (bài toán nhận dạng): Xác thực đúng thực thể cần kết nối, giao dịch.

Xác thực thông tin trao đổi: Xác thực đúng thực thể có trách nhiệm về nội dung thông tin (Xác thực nguồn gốc thông tin)

**** Bảo đảm sẵn sàng:*** Thông tin luôn sẵn sàng cho người dùng hợp pháp.

### *1.2.2.2. Nội dung an toàn thông tin*

**1/. Nội dung chính**

Để bảo vệ thông tin bên trong máy tính hay đang trên đường truyền tin, phải nghiên cứu về an toàn máy tính và an toàn truyền tin.

**** An toàn máy tính (Computer Security)***

Là sự bảo vệ thông tin cố định trong máy tính (Static Informations).

Là khoa học về bảo đảm ATTT trong máy tính.

**** An toàn truyền tin (Communication Security)***

Là sự bảo vệ thông tin trên đường truyền tin (Dynamic Informations), thông tin đang được truyền từ hệ thống này sang hệ thống khác.

Là khoa học về bảo đảm an toàn thông tin trên đường truyền tin.

**2/. Hệ quả từ nội dung chính**

Để bảo vệ thông tin trên máy tính hay trên đường truyền tin, cần nghiên cứu:

* An toàn dữ liệu (Data Security).
* An toàn cơ sở dữ liệu (CSDL) (Data base security).
* An toàn hệ điều hành (Operation system security).
* An toàn mạng máy tính (Netword security).

### *1.2.2.3. Hành vi vi phạm thông tin*

Để đảm bảo ATTT trên đường truyền có hiệu quả, trước tiên phải lường trước hoặc dự đoán trước các khả năng không an toàn, khả năng xâm phạm, các sự cố rủi ro có thể xảy ra đối với thông tin được lưu trữ và trao đổi trên đường truyền tin cũng như trên mạng máy tính. Xác định càng chính xác các nguy cơ trên thì càng quyết định được tốt các giải pháp để giảm thiểu các thiệt hại.

Có hai loại hành vi xâm phạm thông tin đó là: Vi phạm chủ động và vi phạm thụ động.

- **Vi phạm thụ động:**

Chỉ nhằm mục đích cuối cùng là nắm bắt được thông tin (đánh cắp thông tin). Việc làm đó có khi không biết được nội dung cụ thể nhưng có thể dò ra được người gửi, người nhận nhờ thông tin điều khiển giao thức chứa trong phần đầu các gói tin. Kẻ xâm nhập có thể kiểm tra được số lượng, độ dài và tần số trao đổi. Vì vậy, vi phạm thụ động không làm sai lệch hoặc hủy hoại nội dung thông tin được trao đổi. Vi phạm thụ động thường khó phát hiện nhưng có thể có những biện pháp ngăn chặn hiệu quả.

- **Vi phạm chủ động:**

Là dạng vi phạm có thể làm thay đổi nội dung, xóa bỏ, làm trễ, sắp xếp lại thứ tự hoặc làm lặp lại gói tin tại thời điểm đó hoặc sau đó một thời gian. Vi phạm chủ động có thể thêm vào một số thông tin ngoại lai để làm sai lệch nội dung thông tin trao đổi. Vi phạm chủ động dễ phát hiện nhưng để ngăn chặn hậu quả thì khó khăn hơn nhiều.

Một thực tế là không có một biện pháp bảo vệ thông tin nào là an toàn tuyệt đối. Một hệ thống dù được bảo vệ chắc chắn đến đâu cũng không thể đảm bảo là an toàn tuyệt đối.

### 1.2.3. Các chiến lược bảo vệ hệ thống thông tin

#### 1.2.3.*1. Giới hạn quyền hạn tối thiểu (Last Privilege)*

Đây là chiến lược cơ bản nhất. Theo nguyên tắc này, bất kỳ một đối tượng nào (người quản trị mạng, người sử dụng,…) cũng chỉ có những quyền hạn nhất định (đủ dùng cho công việc của mình) đối với tài nguyên hệ thống. Khi thâm nhập vào hệ thống đối tượng đó chỉ được sử dụng một số tài nguyên nhất định.

#### 1.2.3.*2. Bảo vệ theo chiều sâu (Defence In Depth)*

Nguyên tắc này nhắc nhở: Không nên dựa vào một cơ chế an toàn nào dù cho chúng rất mạnh, mà nên tạo nhiều cơ chế an toàn để tương hỗ lẫn nhau. Cụ thể là tạo lập nhiều lớp bảo vệ khác nhau cho hệ thống.

#### 1.2.3.*3. Nút thắt (Choke Point)*

Tạo ra một "cửa khẩu" hẹp, và chỉ cho phép thông tin đi vào hệ thống của mình bằng con đường duy nhất chính là "cửa khẩu" này, sau đó phải tổ chức một cơ cấu kiểm soát và điều khiển thông tin đi qua cửa này.

#### 1.2.3.*4. Điểm yếu nhất (Weakest Point)*

Kẻ phá hoại thường tìm những chỗ yếu nhất của hệ thống để tấn công, do đó ta cần phải gia cố các yếu điểm của hệ thống.

**- Điểm yếu từ mô hình:**

Là các nguy cơ tiềm ẩn của hệ thống do thiết kế, thông thường, trên mô hình cái gì quan trọng nhất (nếu bị tấn công có thể làm ảnh hưởng nghiêm trọng đến cả hệ thống) cũng là điểm yếu nhất, do đây là mục tiêu chính của kẻ tấn công.

Ví dụ: Một hệ thống mạng máy tính có 1 máy chủ và 10 máy trạm thì máy chủ là điểm yếu nhất, do nó chứa dữ liệu quan trọng nhất của hệ thống.

**- Xác định các dịch vụ có nguy cơ:**

Ví dụ: Trong các dịch vụ FTP (File transfer protocol: Giao thức truyền tệp tin ), E-mail (thư điện tử), WWW (World Wide Web) thì www chưa nguy cơ cao nhất; Do nó chứa thông tin tài khoản điện tử, mọi thông tin gần như đều được trao đổi trên Web, …

**- Điểm yếu trong yếu tố con người:**

Là các yếu kém trong quy định, năng lực, nhận thức của con người (nhà quản lý, quản trị viên, lập trình viên, người dùng).

#### 1.2.3.*5. Tính đa dạng bảo vệ*

Cần phải sử dụng nhiều biện pháp bảo vệ khác nhau cho hệ thống khác nhau, nếu không có kẻ tấn công vào được một hệ thống thì chúng cũng dễ dàng tấn công vào các hệ thống khác.

### 1.2.4. Một số giải pháp chung bảo đảm an toàn thông tin

#### 1.2.4.*1. Chính sách*

- Chính sách bảo mật: là tập hợp các quy tắc áp dụng cho mọi đối tượng có tham gia quản lý và sử dụng các tài nguyên và dịch vụ mạng.

- Mục tiêu của chính sách bảo mật giúp người dùng biết được trách nhiệm của mình trong việc bảo vệ các tài nguyên thông tin trên mạng, đồng thời giúp nhà quản trị thiết lập các biện pháp bảo đảm hữu hiệu trong quá trình trang bị, cấu hình kiểm soát hoạt động của hệ thống và mạng.

- Một chính sách bảo mật được coi là hoàn hảo nếu nó gồm các văn bản pháp quy, kèm theo các công cụ bảo mật hữu hiệu và nhanh chóng giúp người quản trị phát hiện, ngăn chặn các truy nhập trái phép.

#### 1.2.4.*2. Giải pháp*

Là tập hợp các biện pháp nhằm đảm bảo an toàn thông tin.

Ví dụ: Một số các giải pháp để khắc phục lỗ hổng là: Xây dựng chính sách xây dựng hệ thống Firewalls, Giao thức SSL,...

#### 1.2.4.*3. Công nghệ*

Là quy trình kỹ thuật để thực hiện giải pháp bảo đảm an toàn thông tin. Nâng cấp phần cứng, giảm thiểu các điểm yếu do phần cứng yếu kém. Cập nhật các phiên bản phần mềm mới đã được xử lý phần nào các điểm yếu của phiên bản trước đó của nó.

#### 1.2.4.*4. Con người*

Để bảo đảm an toàn cho hệ thống cơ sở hạ tầng công nghệ thông tin cần phải chú trọng đến vấn đề con người, chính sách và quy trình bảo vệ. Con người và quy trình là yếu tố đóng vai trò cực kỳ quan trọng trong việc bảo vệ thông tin.

Cần phải có sự cân đối giữa yếu tố con người, chính sách, quy trình và công nghệ trong việc quản lý bảo vệ nhằm giảm thiểu các nguy cơ nảy sinh trong môi trường kinh doanh số một cách hiệu quả nhất.

### 1.2.5. Nội dung ứng dụng về an toàn thông tin

- Phục vụ an ninh quốc phòng: Thám mã, lọc tin, bắt trộm,...

- Phục vụ các hoạt động xã hội: Bầu cử, bỏ phiếu từ xa, thăm dò từ xa,...

- Phục vụ các hoạt động hành chính: Chính quyền "điện tử" chứng minh thư điện tử, giấy phép điện tử,....

Gửi công văn, quyết định,... từ xa trên mạng máy tính công khai.

- Phục vụ các hoạt động kinh tế: Thương mại điện tử,..

Quảng bá thương hiệu, bán hàng trực tuyến,...

Thoả thuận hợp đồng, đấu giá, thanh toán trên mạng máy tính công khai.

Thẻ tín dụng điện tử, thẻ rút tiền điện tử, ví tiền điện tử, tiền điện tử, Sec điện tử,...

- Phục vụ các hoạt động giáo dục, đào tạo:

Gửi đề thi, bài thi qua mạng máy tínhcông khai, đào tạo từ xa (E-learning),...

- Bảo vệ bản quyền thông tin số hoá: Thông tin trong bộ nhớ hay trên đường truyền.

# *Chương 2.* "LỖ HỔNG" TRONG HỆ THỐNG THÔNG TIN

## 2.1. CÁC LOẠI "LỖ HỔNG" TRONG HỆ THỐNG THÔNG TIN

### 2.1.1. Khái niệm "lỗ hổng" trong ATTT

Lỗ hổng ATTT trên một hệ thống là các điểm yếu có thể tạo ra sự ngưng trệ của dịch vụ, thêm quyền đối với người sử dụng hoặc cho phép các truy nhập không hợp pháp vào hệ thống. Các lỗ hổng cũng có thể nằm ngay trong các dịch vụ cung cấp như: Sendmail, web, ftp,…. Ngoài ra các lỗ hổng còn tồn tại ngay trong hệ thống điều hành như WindowsNT, Windows95, UNIX, hoặc trong các ứng dụng mà người dùng thường xuyên sử dụng như Word processing, các hệ database…

### 2.1.2. Phân loại lỗ hổng

#### *2.1.2.1. Phân loại lỗ hổng theo mức nguy hiểm*

Có nhiều tổ chức khác nhau tiến hành phân loại các lỗ hổng. Theo cách phân loại của bộ quốc phòng Mỹ, các lỗ hổng bảo mật trên một hệ thống được chia như sau:

- *Lỗ hổng mức A (Mức rất nguy hiểm)*

Lỗ hổng loại này cho phép người ngoài có thể truy nhập vào hệ thống bất hợp pháp. Lỗ hổng loại này rất nguy hiểm, có thể phá hủy toàn bộ hệ thống.

- *Lỗ hổng mức B (Mức nguy hiểm)*

Lỗ hổng mức B cho phép người dùng có thêm quyền trên hệ thống mà không cần kiểm tra tính hợp lệ. Lỗ hổng loại này thường có trong các ứng dụng của hệ thống, có thể dẫn đến mất hoặc lộ thông tin yêu cầu bảo vệ.

- *Lỗ hổng mức C (Mức trung bình)*

Lỗ hổng loại này cho phép thực hiện tấn công theo DoS (Denial of Service - Từ chối dịch vụ)

Mức độ nguy hiểm trung bình, chỉ ảnh hưởng tới chất lượng dịch vụ, có thể làm ngưng chệ, gián đoạn hệ thống. Không làm phá hỏng dữ liệu hay đạt được quyền truy nhập hợp pháp.

**1/. Các lỗ hổng mức A (Mức rất nguy hiểm)**

Lỗ hổng loại A có mức độ rất nguy hiểm, đe dọa tính toàn vẹn và bảo mật của hệ thống. Các lỗ hổng loại này thường xuất hiện ở những hệ thống quản trị yếu kém hoặc không kiểm soát được cấu hình mạng.

Những lỗ hổng loại này thường hết sức nguy hiểm vì nó tồn tại sẵn có trong phần mềm sử dụng. Người quản trị nếu không hiểu sâu về dịch vụ và phần mềm sử dụng có thể bỏ qua những điểm yếu này.

Đối với hệ thống cũ, thường xuyên phải kiểm tra thông báo của các nhóm tin về bảo mật trên mạng để phát hiện những lỗ hổng loại này.

**2/. Các lỗ hổng mức B (Mức nguy hiểm)**

Lỗ hổng loại B có mức độ nguy hiểm hơn lỗ hổng loại C, cho phép người dùng nội bộ có thể chiếm được quyền cao hơn hoặc truy nhập bất hợp pháp.

Những lỗ hổng loại này thường xuất hiện trong các dịch vụ trên hệ thống.

Một số lỗ hổng loại B thường xuất hiện trong các ứng dụng, ví dụ như: Sendmail,…

Một loạt các vấn đề khác về quyền sử dụng chương trình trên Unix cũng thường gây nên các lỗ hổng mức B.

Các lỗ hổng loại B khác:

- Một dạng khác của lỗ hổng loại B xảy ra đối với chương trình có mã nguồn viết bằng C. Chương trình viết bằng C thường dùng một vùng đệm, là một vùng trong bộ nhớ sử dụng để lưu trữ dữ liệu trước khi xử lý.

- Người lập trình thường sử dụng vùng đệm trong bộ nhớ trước khi gán một khoảng không gian bộ nhớ cho từng khối dữ liệu.

- Việc kiểm soát chặt chẽ cấu hình hệ thống và các chương trình sẽ hạn chế được các lỗ hổng loại B.

**3/. Các lỗ hổng mức C (Mức trung bình)**

Các lỗ hổng này cho phép thực hiện các cuộc tấn công theo DoS.

DoS là hình thức tấn công sử dụng các giao thức ở tầng Internet trong bộ giao thức TCP/IP để làm hệ thống ngưng chệ dẫn đến tình trạng từ chối người dùng hợp pháp truy nhập hay sử dụng hệ thống.

Một số lượng lớn các gói tin được gửi tới server trong khoảng thời gian liên tục làm cho hệ thống trở nên quá tải, kết quả là máy chủ (server) đáp ứng chậm hoặc không thể đáp ứng các cầu yêu cầu từ máy khách (client) gửi tới.

Các dịch vụ có chứa lỗ hổng cho phép thực hiện các cuộc tấn công DoS có thể được nâng cấp hoặc sửa chữa bằng các phiên bản mới hơn của các nhà cung cấp dịch vụ.

Hiện nay chưa có một giải pháp toàn diện nào để khắc phục các lỗ hổng loại này vì bản thân việc thiết kế giao thức ở tầng Internet (IP) nói riêng và bộ giao thức TCP/IP đã chứa đựng những nguy cơ tiềm tàng của lỗ hổng này.

Ví dụ bị tấn công kiểu DoS là một số website lớn như: www.ebay.com, www.yahoo.com,...

Tuy nhiên, mức độ nguy hiểm của các lỗ hổng loại này được xếp loại C, ít nguy hiểm vì chúng chỉ làm gián đoạn cung cấp dịch vụ của hệ thống trong một thời gian mà không làm nguy hại tới dữ liệu và những kẻ tấn công cũng không đạt được quyền truy nhập bất hợp pháp vào hệ thống.

### *2.1.2.2. Phân loại lỗ hổng theo chức năng nhiệm vụ*

**1/. Lỗ hổng trong thuật toán**

*a) Lỗi tràn vùng đệm (Deamon finger)*

Lỗ hổng lỗi tràn vùng đệm (deamon finger) là cơ hội để phương thức tấn công sâu (Worm) trên Internet phát triển.

Đó là lỗi tràn vùng đệm trong các tiến trình finger (lỗi khi lập trình). Vùng đệm để lưu chuỗi ký tự nhập được giới hạn là 512 bytes. Tuy nhiên chương trình không thực hiện kiểm tra dữ liệu đầu vào khi lớn hơn 512 bytes trước khi nó được thi hành. Kết quả là xảy ra hiện tượng tràn dữ liệu ở vùng đệm khi dữ liệu lớn hơn 512 bytes.

Phần dữ liệu dư thừa chứa những đoạn mã để kích hoạt một bản thảo (script) khác hoạt động. Script này tiếp tục thực hiện lọc tới một máy (host) khác. Dẫn đến là hình thành một mắt xích các "sâu" trên mạng Internet.

*b) Chương trình quét (Scanner)*

- Khái niệm Scanner:

Scanner là một chương trình tự động rà soát và phát hiện những điểm yếu về bảo mật trên một trạm cục bộ hoặc trên một trạm ở xa. Với chức năng này, một kẻ phá hoại sử dụng chương trình Scanner có thể phát hiện ra những lỗ hổng về bảo mật trên một server ở xa.

- Cơ chế hoạt động của các chương trình Scanner:

Các chương trình scanner thường có một cơ chế chung là rà soát và phát hiện những cổng TCP/UDP được sử dụng trên một hệ thống cần tấn công, từ đó phát hiện những dịch vụ sử dụng trên hệ thống đó. Sau đó các chương trình Scanner ghi lại những đáp ứng trên hệ thống ở xa tương ứng với các dịch vụ mà nó phát hiện ra. Dựa vào những thông tin này, kẻ tấn công có thể tìm ra điểm yếu trên hệ thống.

Những yếu tố để chương trình quét có thể hoạt động là:

- Yêu cầu về thiết bị và hệ thống: Một chương trình scanner có thể hoạt động được nếu môi trường đó có hỗ trợ TCP/IP.
- Hệ thống đó phải kết nối vào mạng Internet.

Để xây dựng một chương trình Scanner, kẻ phá hoại cần có kiến thức sâu về TCP/IP, những kiến thức về lập trình C và một số ngôn ngữ lập trình cấu trúc. Ngoài ra người lập trình (hoặc là người sử dụng) cần có hiểu biết về phương thức hoạt động của các ứng dụng Client/Server.

- Ảnh hưởng của chương trình Scanner đến bảo mật trên mạng:

Chương trình Scanner có vai trò quan trọng trong hệ thống bảo mật. Vì chúng có khả năng phát hiện ra những điểm yếu kém trên hệ thống mạng. Đối với người quản trị mạng những thông tin này hết sức hữu ích và cần thiết, đối với những kẻ phá hoại những thông tin này sẽ hết sức nguy hiểm.

*c) Công nghệ Java trong bảo mật dịch vụ Web*

Ngôn ngữ lập trình Java được Sun Microsystems xây dựng và phát triển. Hiện nay, có rất nhiều trang web động phát triển dựa trên ngôn ngữ Java. Hai trình duyệt web phổ biến hiện nay (IE và Netcape Comunication) đều hỗ trợ Java. Một trong số điểm mạnh của Java là hỗ trợ bảo mật rất cao. Tuy nhiên vẫn có một số lỗ hổng được phát hiện đó là:

- Đối với các trình duyệt Netscape phiên bản 2.0 và 2.1 có một số lỗ hổng cho phép chạy các Java applet có chức năng xóa file trên hệ thống.

- Cho phép các tấn công DoS: Với các applet (ứng dụng ký sinh) có lỗi dẫn đến tình trạng chiếm nhiều tài nguyên hệ thống như sử dụng CPU, ổ đĩa,…

- Một số các applet cho phép tạo các kết nối tới các địa chỉ tuỳ ý mà người dùng không kiểm soát được. Một số trang web cố tình đưa ra các applet có những đoạn mã nguồn cho phép các máy khách sau khi tải các applet về máy trạm thực hiện kết nối tới một host bất kỳ nào khác trên mạng.

*d) Một số lỗ hổng của Javascripts*

Javascripts là một ngôn ngữ kịch bản, làm việc ở phía web client, được phát triển bởi Netscape. Hiện nay, việc sử dụng Javascripts hết sức phổ biến, trong hầu hết các trang web đều có các đoạn mã Javascripts. Không giống như các lỗ hổng bảo mật của Java, các lỗ hổng bảo mật của Javascripts thường liên quan đến các thông tin cá nhân người dùng.

Điều đó thể hiện qua một số lỗ hổng của Javascripts như sau:

- Trong các Web browser Netscape 4.5 có khả năng chạy các javascripts đọc thuộc tính các file trên máy trạm, sau đó gửi chúng đến các máy khác trên mạng Internet.

- Có thể sử dụng các Javascripts để đọc nội dung các file trên máy trạm khi dùng IE 4.0 – 4.01.

- Các bản Netscape Comunicator đến 4.35 cho phép chạy các đoạn mã Javascripts đọc nội dung các địa chỉ URL trong cache.

- Một lỗ hổng khác trong bản Netscape Comunicator 4.04 là dùng các đoạn mã Javascripts đọc thông tin các tham số cài đặt hệ thống (ví dụ địa chỉ email, mật khẩu người dùng...).

- Khả năng giám sát các phiên làm việc người dùng: Có thể sử dụng các đoạn mã Javascripts để đọc các thông tin về trang web người dùng đã truy nhập trong một phiên làm việc, rồi chuyển những thông tin đó tới địa chỉ email, vì Javascripts có thể mở các cửa sổ dưới dạng không nhìn thấy, nên người dùng không nhận biết được các đoạn chương trình Javascripts đang thực thi trên hệ thống của mình.

**2/. Lỗ hổng trong ứng dụng**

*a) Tệp tin (file) host.equiv*

Nếu người dùng được xác định trong file host.equiv cùng với địa chỉ máy của người đó, thì họ được phép truy nhập từ xa vào hệ thống đã khai báo. Tuy nhiên có một lỗ hổng khi thực hiện chức năng này đó là nó cho phép người truy nhập từ xa có quyền của bất cứ người nào trên hệ thống.

Ví dụ: Nếu trên máy A có một file/etc/host.equiv có định danh của B là Mai, thì Mai trên B có thể truy nhập vào hệ thống A và có quyền của bất cứ người nào khác trên A. Đây là lỗi của thủ tục ruserok() trong thư viện khi lập trình.

*b) Thư mục /var /mail*

Nếu thư mục /var /mail được thiết lập với quyền được ghi (Writeable) đối với mọi người trên hệ thống, thì bất cứ ai cũng có thể tạo tệp tin trong thư mục này. Sau đó tạo một tệp tin liên kết với tên là tên của một người đã có trên hệ thống, kết nối tới một tệp tin trên hệ thống, thì các thư tới người người dùng có tên trùng với tên tệp liên kết sẽ được gán trong tệp mà nó kết nối tới.

*Ví dụ:* Một người dùng tạo liên kết từ "…/var /mail /root" tới "…/etc /passwd", sau đó gửi mail bằng tên một người mới tới root thì tên người dùng mới này sẽ được gán thêm vào trong tệp "…/etc /passwd". Do vậy thư mục "…/var /mail" không bao giờ được thiết lập với quyền có quyền viết (writeable).

*c) Chức năng Proxy (uỷ nhiệm) của FTPd*

Chức năng uỷ nhiệm của FTPd cho phép người dùng có thể truyền tệp tin từ một FTPD này tới một FTPD server khác. Sử dụng chức năng này có thể bỏ qua các xác thực địa chỉ IP.

Nguyên nhân là người dùng có thể yêu cầu một file trên FTP server gửi một tệp tin tới bất kỳ địa chỉ IP nào. Nên người dùng có thể yêu cầu FTP server đó gửi một tệp tin gồm các lệnh PORT và PASV tới các server đang nghe trên các cổng TCP trên bất kỳ một host nào. Kết quả là một trong các host đó có FTP server chạy và tin cậy người dùng đó, bỏ qua xác thực địa chỉ IP.

### 3/. Lỗ hổng trong giao thức

*a) Vấn đề cần nghiên cứu*

Trên mạng Internet, đa số các nguy cơ an ninh xuất hiện do phần mềm có lỗi, không thực hiện theo đúng chuẩn TCP/IP. Nhưng cũng có một số điểm yếu nằm ở mức giao thức, tức là hệ thống bị tổn thương khi các phần mềm vẫn chạy đúng theo các chuẩn do Internet Engineering Task Force đề ra. Ví dụ là giao thức ARP, nó có lỗ hổng an ninh.

Trong khi IETF chưa ban hành giao thức mới có khả năng loại bỏ điểm yếu trên, thì các nhà cung cấp riêng lẻ đua nhau đưa ra các cách riêng của mình để hạn chế các nguy cơ an ninh. Điều này tạo ra tình trạng hỗn loạn. Vốn các chuẩn được đặt ra để các thiết bị có thể liên lạc với nhau dễ dàng, thì nay các hãng sản xuất khác nhau đang sa vào con đường tự ý thay đổi chuẩn để giải quyết các vấn đề trước mắt.

Nếu để hiện tượng này kéo dài, sự tương thích của Internet sẽ dần đổ vỡ.Có 2 cách giải quyết chính:

- Cách 1: Là xây dựng mới giao thức mạng "không còn lỗ hổng", có thể không tương thích với các chuẩn hiện có.
- Cách 2: Cải tiến giao thức cũ để "bịt" các "lỗ hổng", nhưng vẫn tương thích với các chuẩn hiện có của Internet.

*b) Giao thức phân giải địa chỉ ARP*

Giao thức phân giải địa chỉ ARP (ARP – Address Resolution Protocol) là giao thức đơn giản. Dùng ARP để phân giải từ địa chỉ tầng mạng thành địa chỉ tầng liên kết dữ liệu. Trong thực tế, người ta thường dùng để chuyển đổi từ địa chỉ IP sang địa chỉ Ethernet.

*Nguy cơ an ninh của ARP*

ARP không cung cấp cơ chế để các thiết bị phân biệt các gói tin giả mạo, vì thế kỹ thuật ARP Spoofing - Lừa gạt (hay ARP Poisoning - Đầu độc) cho phép kẻ tấn công lừa nạn nhân gửi các gói tin IP đến một nơi mà kẻ tấn công chọn trước, thường là đến chính vị trí mà kẻ tấn công đang chờ đợi.

Khi các gói tin đến, kẻ tấn công toàn quyền xử lý, từ đọc lén đến thay đổi nội dung của dữ liệu, hoặc đơn giản hơn là vứt bỏ gói tin, làm cho mạng không hoạt động.

Minh họa tình huống trên:

Trên thực tế, khi nút mạng A nào đó cần kết nối với nút mạng B, thì nó phải biết rõ địa chỉ vật lý của nút mạng B. Để làm việc này đã có giao thức phân giải địa chỉ ARP, nó thực hiện một ánh xạ giữa địa chỉ logic (địa chỉ mạng IP) và địa chỉ vật lý (địa chỉ phần cứng MAC) bên trong các đoạn mạng.

Giao thức như sau:

Máy A gửi yêu cầu kết nối có chưa địa chỉ IP của máy cần tìm, tới tất cả các máy trong mạng cục bộ, chỉ có một máy B nhận ra địa chỉ IP của mình, nó gửi địa chỉ MAC của nó cho máy A.

Tuy vậy có thể phát sinh tình huống:

Khi máy A gửi yêu cầu kết nối có chứa địa chỉ IP của máy cần tìm, máy B có địa chỉ IP như vậy nhưng bị lỗi. Nhân cơ hội này, máy C nào đó giả mạo máy B, gửi địa chỉ MAC của nó cho máy A. Một kết nối giữa A và C được hình thành, nhưng A vẫn đinh ninh rằng mình đang kết nối với B. Vì vậy, có thể dẫn đến làm lộ thông tin.

## 2.2. MỘT SỐ VÍ DỤ "LỖ HỔNG" CỤ THỂ

### 2.2.1. "Lỗ hổng" trong hệ điều hành

#### *2.2.1.1. Hệ thống có cấu hình không an toàn*

Cấu hình không an toàn là một lỗ hổng bảo mật của hệ thống. Các lỗ hổng này được tạo ra do các ứng dụng có các thiết lập không an toàn hoặc người quản trị hệ thống định cấu hình không an toàn. Chẳng hạn như cấu hình máy chủ web cho phép ai cũng có quyền duyệt qua hệ thống thư mục. Việc thiết lập như trên có thể làm lộ các thông tin nhạy cảm như mã nguồn, mật khẩu hay các thông tin của khách hàng.

Nếu quản trị hệ thống cấu hình hệ thống không an toàn sẽ rất nguy hiểm vì nếu người tấn công duyệt qua được các tệp mật khẩu thì họ có thể tải về và giải mã ra, khi đó họ có thể làm được nhiều thứ trên hệ thống.

#### *2.2.1.2. Lỗ hổng mật khẩu cơ bản (Password-base)*

Thông thường, hệ thống khi mới cấu hình có tên người dùng và mật khẩu mặc định. Sau khi cấu hình hệ thống một số admin vẫn không đổi lại các thiết lập mặc định này. Đây là lỗ hổng giúp kẻ tấn công có thể thâm nhập vào hệ thống bằng con đường hợp pháp. Khi đã đăng nhập vào, hacker có thể tạo thêm user, cài backboor cho lần viếng thăm sau.

### 2.2.2. "Lỗ hổng" trong phần mềm ứng dụng

#### *2.2.2.1. Chủ quan (lỗi do người viết phần mềm)*

Do người lập trình, người thiết kế, quản lý của chính phần mềm có thể vì lý do, mục đích nào đó tiết lộ bí mật. Điều này là vô cùng nguy hại do hacker nắm được thiết kế của phần mềm sẽ dễ dàng tấn công hệ thống.

#### *2.2.2.2. Khách quan (từ người sử dụng)*

Người dùng vô ý đã để máy tính cho người khác dùng, để lộ mật khẩu…

Ví dụ: Khi người dùng đang dùng máy mà có việc đi ra ngoài không tắt máy, đóng ứng dụng. Kẻ tấn công có thể lợi dụng sơ hở này tấn công vào hệ thống.

### 2.2.3. “Lỗ hổng” trong hệ thống mạng

#### *2.2.3.1. Nghe lén đường truyền, dò, đoán*

Các hệ thống truyền đạt thông tin qua mạng không chắc chắn, lợi dụng điều này, hacker có thể truy cập vào các đường dẫn đến dữ liệu (data paths) để nghe trộm hoặc đọc trộm luồng dữ liệu truyền qua.

Hacker nghe trộm sự truyền đạt thông tin, dữ liệu sẽ chuyển đến chương trình nghe trộm (sniffing) hoặc “sự rình mò” (snooping). Nó sẽ thu thập những thông tin quý giá về hệ thống như một gói (packet) chứa mật mẩu (password) và tên người dùng (user name) của một ai đó. Các chương trình nghe trộm còn được gọi là các sniffing. Các sniffing này có nhiệm vụ lắng nghe các cổng của một hệ thống mà hacker muốn nghe trộm. Nó sẽ thu thập dữ liệu trên các cổng này và chuyển về cho hacker.

#### *2.2.3.2. Thiết kế kém, yếu*

Là việc có nhiều hơn một con đường dẫn vào hệ thống (bị mở cổng hậu),…

Khi thiết kế một mạng (Lan, WAN,…), người thiết kế không xác định được hết các cổng vào hệ thống. Khi quản trị, người quản trị chỉ biết đến cổng chính vào hệ thống, xây dựng các bảo vệ hệ thống. Kẻ tấn công sẽ rất khó tấn công vào bằng những cổng này. Nhưng nếu kẻ tấn công tìm ra “con đường” khác xâm nhập vào hệ thống thì sẽ mất an toàn do những đường này không được người quản trị biết đến và bảo vệ.

#### *2.2.3.3. Lỗi phát sinh do thiết bị*

Các lỗi treo thiết bị, tràn bộ đệm, nghẽn mạng, không có khả năng cung cấp dịch vụ…

Một lỗ hổng vật lý của máy tính sẽ hoàn toàn bị khai thác ngay cả khi phương pháp nhận dạng phức tạp nhất, phương pháp mã hóa bảo mật nhất. Một chương trình theo dõi các thao tác trên bàn phím (key logger), cả phần mềm lẫn phần cứng được cài đặt, khóa PGP - Pretty Good Privacy (tiện ích mã hóa và chữ ký điện tử) bí mật của bạn sẽ bị lộ, do đó mọi dữ liệu mã hóa và tài khoản bị tổn hại. Bất chấp mật khẩu dài và bảo mật đến đâu thì lỗ hổng bảo mật vật lý là một trong những trường hợp nguy hiểm nhất.

#### *2.2.3.4. Các lỗi chưa biết (Zero Day)*

Là các lỗ hổng mà tại thời điểm hiện tại chưa bộc lộ ra (chưa được biết đến). Đây là lỗ hổng rất nguy hiểm do ngay cả người lập trình, nhà quản lý, người dùng đều chưa biết đến mà phòng tránh trước.

Ví dụ: Khai thác lỗ hổng Zero-day trong trình duyệt Safari

Một lỗ hổng an ninh bảo mật thuộc hàng nghiêm trọng trong trình duyệt Safari của Apple. Phiên bản hiện tại (4.0.5) và những bản cũ hơn đều bị ảnh hưởng.

Nếu người dùng vô tình đăng nhập vào trang web có chứa các công cụ độc hại để khai thác lỗ hổng dành cho Windows của Safari, ngay lập tức các đoạn mã độc sẽ tự động tải về hệ thống với số lượng vô cùng lớn, sẽ khiến cho trình duyệt hoạt động ì ạch, treo (not responding)... Người sử dụng Safari nên tránh truy cập vào các đường dẫn bất thường để giảm thiểu rủi ro.

### 2.2.4. Lỗ hổng cơ sở dữ liệu (database)

**1/. Cơ sở dữ liệu (CSDL)**

CSDL hiểu theo kỹ thuật, là một tập hợp thông tin có cấu trúc. Nhưng trong công nghệ thông tin CSDL được hiểu rõ hơn dưới dạng một tập hợp liên kết các dữ liệu, thường đủ lớn để lưu trên một thiết bị lưu trữ như đĩa hay băng. Dữ liệu này được duy trì dưới dạng một tập hợp các tập tin trong hệ điều hành hay được lưu trữ trong các hệ quản trị cơ sở dữ liệu.

Cơ sở dữ liệu là nơi lưu giữ các thông tin, giá trị quan trọng của cơ quan, tổ chức, cá nhân,… Nên CSDL là miếng mồi hấp dẫn đối với kẻ tấn công. Khi CSDL nhiều và được quản lý tập trung. Khả năng rủi ro mất dữ liệu rất cao. Các nguyên nhân chính là mất điện đột ngột hoặc hỏng thiết bị lưu trữ, lỗi trực tiếp trong phần mềm lưu trữ (tiềm ẩn các lỗ hổng bảo mật),…

**2/. Các nguy cơ đối với an toàn dữ liệu**

- Mất dữ liệu do hư hỏng vật lý:
    + Các sự cố do hư hỏng các thiết bị lưu trữ
    + Mạng bị hư hỏng do thiên tai, hoả hoạn
    + Hư hỏng do sự cố nguồn điện
- Mất dữ liệu do hư hỏng hệ thống điều hành.
- Dữ liệu bị sửa đổi một cách bất hợp pháp thậm chí bị đánh cắp

Hacker có thể dùng những công cụ hack có sẵn trên mạng hoặc các Trojan để đột kích vào hệ thống. lấy cắp mật khẩu Admin để có quyền tuyệt đối sửa đổi, làm hỏng dữ liệu quan trọng.

**3/. Ví dụ lỗ hổng trong phần mềm quản lý dữ liệu SQL Server**

SQL Server 7.0 và 2000 đã tồn tại các lỗi tràn bộ đệm. Điểm yếu này cho phép kẻ tấn công thực hiện các đoạn mã nguy hiểm trên hệ thống của nạn nhân bằng cách khai thác lỗi tràn bộ đệm. Lỗi này liên quan tới các quy trình lưu trữ mở rộng (extended stored procedure) do Microsoft thiết kế sẵn, mà được sử dụng để giúp SQL Server thực hiện các thao tác thông thường. Một số quy trình lưu trữ mở rộng được cài đặt bởi SQL Server 7.0 và 2000 tồn tại các lỗi tràn bộ bộ đệm có thể cho phép tin tặc khai thác bằng cách gọi một trong những chức năng bị ảnh hưởng trong cơ sở dữ liệu (database) hoặc tạo yêu cầu truy vấn được thiết kế đặc biệt. Qua đó, tin tặc có thể làm lỗi máy chủ hoặc chạy các đoạn mã nguy hiểm.

Lỗi tràn bộ đệm cũng được phát hiện trong động cơ Microsoft Jet DataBase dùng để xử lý các file Access.

"Lỗ hổng" này được đánh giá là lỗi có mức tác hại trung bình.

# *Chương 3.* MỘT SỐ DẠNG "TẤN CÔNG" HỆ THỐNG THÔNG TIN THÔNG QUA "LỖ HỔNG"

## 3.1. "TẤN CÔNG" HỆ THỐNG THÔNG TIN

### 3.1.1. Đối tượng tấn công

Đối tượng tấn công mạng (Intruder): Là cá nhân hoặc tổ chức sử dụng các công cụ phá hoại như phần mềm hoặc phần cứng để dò tìm các điểm yếu, lỗ hổng bảo mật trên hệ thống, thực hiện các hoạt động xâm nhập và chiếm đoạt tài nguyên trái phép.

Một số đối tượng tấn công mạng:

- *Hacker*: Là kẻ xâm nhập vào mạng trái phép bằng cách sử dụng các công cụ phá mật khẩu hoặc khai thác các điểm yếu của thành phần truy nhập trên hệ thống.

- *Masquerader (Kẻ giả mạo)*: Là kẻ giả mạo thông tin trên mạng. Một số hình thức giả mạo như giả mạo địa chỉ IP, tên miền, định danh người dùng.

- *Eavesdropper (Người nghe trộm)*: Là kẻ nghe trộm thông tin trên mạng, sử dụng các công cụ nghe nén (sniffer), sau đó dùng các công cụ phân tích và gỡ rối để lấy các thông tin có giá trị.

### 3.1.2. Một số hình thức tấn công thông tin

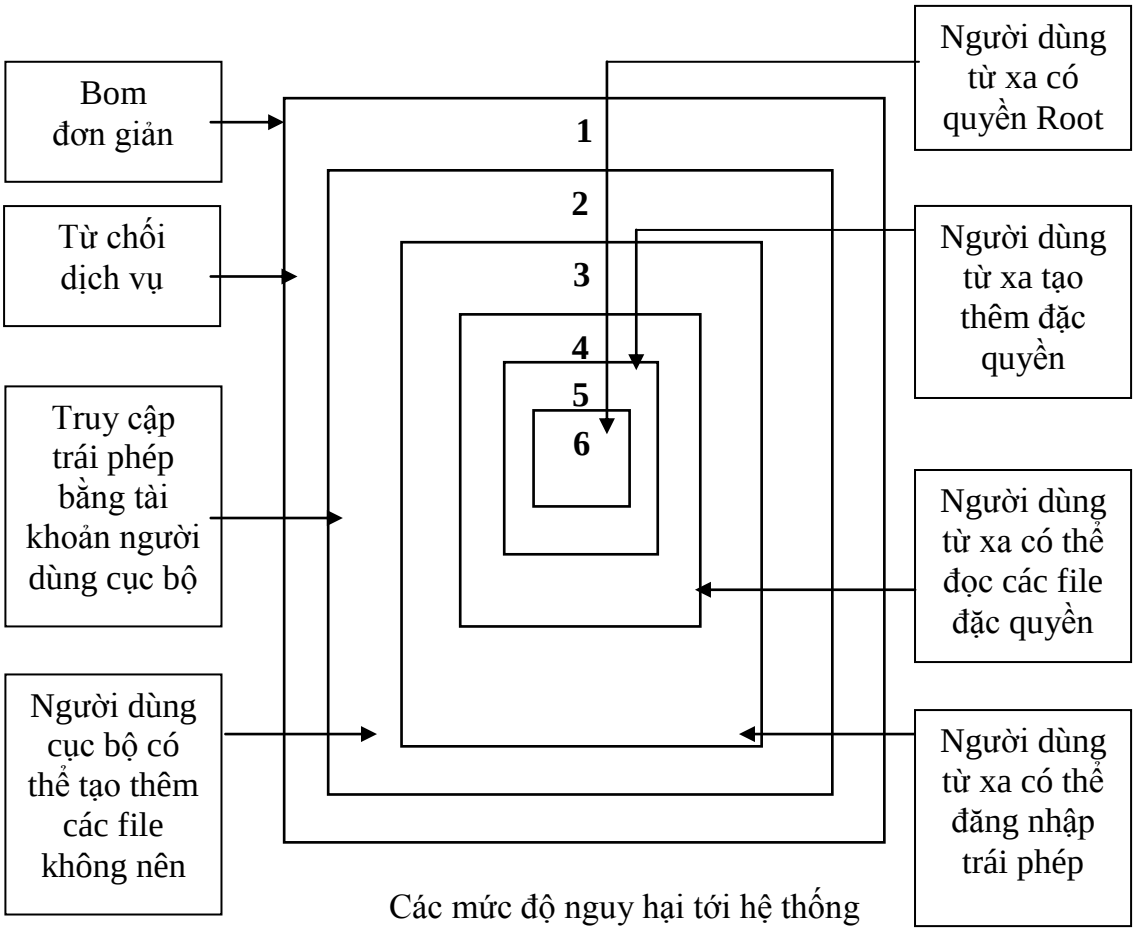
Có thể tấn công theo các hình thức sau:

- Dựa vào những lỗ hổng bảo mật trên mạng: những lỗ hổng này có thể là các điểm yếu của dịch vụ mà hệ thống cung cấp. Ví dụ kẻ tấn công lợi dụng các điểm yếu trong các dịch vụ mail, ftp, web… để xâm nhập và phá hoại.
- Sử dụng các công cụ để phá hoại: ví dụ sử dụng các chương trình phá khóa mật khẩu để truy nhập bất hợp pháp vào một số chương trình.

Ngoài ra, kẻ tấn công mạng cũng có thể kết hợp 2 hình thức trên để đạt mục đích.

### 3.1.3. Các mức độ nguy hại đến hệ thống thông tin

Các mức độ nguy hại tới hệ thống tương ứng với các hình thức tấn công khác nhau:




Các mức độ nguy hại tới hệ thống

- Mức 1: Tấn công vào một số dịch vụ mạng: Web, Email dẫn đến các nguy cơ lộ các thông tin về cấu hình mạng. Các hình thức tấn công ở mức này có thể dùng DoS hoặc Spam mail.
- Mức 2: Kẻ phá hoại dùng tài khoản của người dùng hợp pháp để chiếm đoạt tài nguyên hệ thống (dựa vào các phương thức tấn công như bẻ khóa, đánh cắp mật khẩu…). Kẻ phá hoại có thể thay đổi quyền truy nhập thông qua các lỗ hổng bảo mật đọc các thông tin trong tập tin liên quan đến hệ thống như "/etc/passwd" (Linux) và SAM file (Windows).
- Mức 3 đến mức 5: Kẻ phá hoại không sử dụng quyền của người dùng thông thường, mà có thêm một số quyền cao hơn với hệ thống như quyền kích hoạt một số dịch vụ, xem xét các thông tin khác trên hệ thống.
- Mức 6: Kẻ tấn công chiếm được quyền Root hoặc Admintrator trên hệ thống.

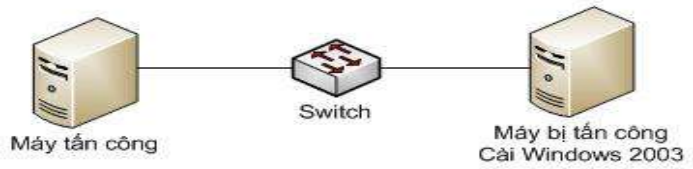
## 3.2. MỘT SỐ VÍ DỤ "TẤN CÔNG" VÀO "LỖ HỔNG" BẢO MẬT

### 3.2.1. Tấn công hệ điều hành

Hệ điều hành là mục tiêu tấn công phá hoạt vô vùng lớn. Đây là nhưng phần mềm phổ biến và lớn trong thế giới máy tính, đồng thời cũng tiềm ẩn nhiều "lỗ hổng bảo mật". Khai thác điểm yếu để tấn công vào hệ điều hành mang lại nhiều lợi ích lớn lao cho Hacker.

Dưới đây, tôi xin trình bày một vài ví dụ tấn công hệ điều hành:

#### *3.2.1.1. Tấn công Password của tài khoản người dùng trong Windows*




**1/. Trên máy cục bộ (Local)**

- Giả sử chúng ta không biết mật khẩu của một máy tính trong hệ thống, nhưng nhờ người đó gõ mật khẩu của họ và cho ta mượn máy tính dùng tạm. Và giờ là làm thế nào để biết được mật khẩu trên máy ta đang đăng nhập.

- Rất nhiều phần mềm có thể xuất khẩu (exports) đoạn mã hoá của mật khẩu ra thành một tệp điển hình là PasswordDump, WinPasswordPro.

Giả sử sử dụng WinPasswordPro.

- Bật chương trình WinPasswordPro lên Import Password từ máy cục bộ.

- Sau khi nhập mật từ tệp SAM vào sẽ được:


Sau đó ta xuất danh sách người dùng và mật khẩu đã được mã hoá ra một tệp "*.txt" và gửi vào mail, sau đó tại máy của mình chúng ta cũng dùng phần mềm này để giải mã ngược lại.

Mở file TXT đã xuất ra ta có dữ liệu mật khẩu đã được mã hoá.

Sau khi lấy được dữ liệu người dùng - mật khẩu đã mã hoá ta gỡ bỏ chương trình này trên máy nạn nhân để khỏi lộ, rồi gửi tệp đó vào mail để về máy của ta giải mã, đây là công đoạn tốn thời gian. Đối với mật khẩu dài 10 ký tự mất khoảng 1 tiếng.

- Bật chương trình WinPasswordPro trên máy của chúng ta chọn File, xuất tệp tin PWDUMP rồi chọn đường dẫn tới tệp tin mật khẩu được mã hoá.

Sau khi Import từ file PWDUMP ta được

Nhấn vào Start ta sẽ có 3 phương thức tấn công mật khẩu

+ Bắt ép thô bạo (brute force).

+ Từ điển (Dictionary).

+ Bảng thông minh (Smart table).

Chọn phương thức tấn công bắt ép thô bạo:

Đợi khoảng 15 phút (password không đặt ký tự đặc biệt, không số, không hoa và 9 ký tự)

- Kết thúc quá trình ta đã giải mã được tệp mật khẩu đã được mã hoá với: Tên người dùng là administrator và mật khẩu vnexperts


**2/. Tấn công máy tính từ xa**

- Khi chúng ta được ngồi trên máy nạn nhân để xuất mật khẩu (được mã hoá) là đơn giản, nhưng thực tế sẽ rất ít khi thực hiện được phương thức này.

- Dùng Password Dump, chúng ta sẽ lấy được dữ liệu đã được mã hoá từ một máy từ xa.

- Ở đây sử dụng PasswordDump Version 6.1.6.

Lấy dữ liệu mã hoá tên người dùng và mật khẩu từ máy tính 192.168.1.156 dùng PWDump và đẩy dữ liệu đó ra file: vnehack.txt tại ổ C\:, dùng lệnh Type xem dữ liệu của file đó.

Sau khi có dữ liệu, ta lại sử dụng WinPasswordPro để giải mã. Và sau khi ta có tài khoản người dùng là quản trị viên và mật khẩu của nó, thì việc làm gì là tuỳ thuộc vào chúng ta.

### *3.2.1.2. Tấn công hệ thống Windows qua lỗ hổng bảo mật*

- Đầu tiên chúng ta phải tìm những lỗ hổng bảo mật.
- Khai thác lỗ hổng đã tìm được.

**1/. Dùng Retina Network Security Scanner 5.1 để tìm lỗ hổng trên hệ thống**

Bật chương trình Retina Network Security Scanner.

Tìm kiếm trong hệ thống mạng những máy nào đang Online vào phần Discover.

Để phát hiện ra lỗ hổng bảo mật sử dụng Tab Audit.

Nhấn Start - Chọn Scan Template là chế độ Complete Scan.

Đợi một lát thu được kết quả là lỗ hổng bảo mật. Đọc các thông tin về lỗ hổng tìm được để tìm cách tấn công.

Đây là phần mềm có bản quyền.

**2/. Sử dụng Metasploit để khai thác**

Những lỗ hổng vừa được Retina phát hiện, chúng ta sẽ sử dụng Metasploit để khai thác chúng.

### *3.2.1.3. Ví dụ khác*

Tin tặc tấn công hai lỗ hổng "nghiêm trọng" của Windows. Phiên bản hệ điều hành duy nhất không bị ảnh hưởng là Windows XP SP3.

Trong thông báo đưa ra, symantec cho biết đang ghi nhận được các dấu hiệu khai thác lỗ hổng giao diện thiết bị đồ họa (GDI). Microsoft xếp hai lỗ hổng này vào mức "nghiêm trọng", có thể ảnh hưởng tới các phiên bản Windows, kể cả hai phiên bản hệ điều mới nhất Windows Vista SP1 và Server 2008. Tin tặc có thể khai thác lỗ hổng bằng cách kích hoạt một tệp hình ảnh WMF (Windows Metafile) hoặc EMF (Enhanced Meta file) được chế tạo đặc biệt.

Tin tặc sẽ nhanh chóng thành công với mã khai thác lỗ hổng bởi chỉ cần một động tác xem ảnh đơn giản trên mạng hoặc trong e-mail, cũng khiến cho hệ thống có thể bị tấn công.

### 3.2.2. Tấn công trên mạng

#### *3.2.2.1. Tấn công từ chối dịch vụ*

* Tấn công từ chối dịch vụ (DoS -Denial of Service) là một loại hình tấn công hệ thống mạng nhằm ngăn cản những người dùng hợp lệ được sử dụng một dịch vụ nào đó. Các cuộc tấn công có thể được thực hiện nhằm vào bất kì một thiết bị mạng nào bao gồm tấn công vào các thiết bị định tuyến, web, E-mail, hệ thống DNS,…

Tấn công DoS phá huỷ dịch vụ mạng bằng cách làm tràn ngập số lượng kết nối, quá tải server hoặc chương trình chạy trên server, tiêu tốn tài nguyên của server, hoặc ngăn chặn người dùng hợp lệ truy nhập tới các dịch vụ mạng.

Tấn công từ chối dịch vụ có thể được thực hiện theo một số cách nhất định.

Có năm kiểu tấn công cơ bản sau:

- Nhằm tiêu tốn tài nguyên tính toán như băng thông, dung lượng đĩa cứng hoặc thời gian xử lý.
- Phá vỡ các thông tin cấu hình như thông tin định tuyến.
- Phá vỡ các trạng thái thông tin như việc tự động xác lập lại (reset) các phiên TCP.
- Phá vỡ các thành phần vật lý của mạng máy tính.
- Làm tắc nghẽn thông tin liên lạc có chủ đích giữa các người dùng và nạn nhân dẫn đến việc liên lạc giữa hai bên không được thông suốt.

* Tấn công từ chối dịch vụ phân tán (DDoS - Distributed Denial of Service) là mối đe doạ hàng đầu đến các hệ thống công nghệ thông tin trên thế giới. Về mặt kỹ thuật, gần như chỉ có thể hy vọng tin tặc sử dụng những công cụ đã biết và có hiểu biết kém cỏi về các giao thức để có thể nhận biết và loại trừ các con đường dễ bị tấn công.

Với hạ tầng mạng cùng với thương mại điện tử vừa chớm hình thành, DDoS là một mối nguy hại rất lớn cho Internet Việt Nam.

* Nhận diện dấu hiệu của một vụ tấn cống từ chối dịch vụ
  - Mạng thực thi chậm khác thường (mở file hay truy cập Website).
  - Không thể dùng một Website cụ thể.
  - Không thể truy cập bất kỳ website nào .
  - Tăng lượng thư rác nhận được (như một trận "boom mail").

#### *3.2.2.2. Tấn công giả mạo hệ thống tên miền trên Internet*

Tấn công giả mạo hệ thống tên miền trên Internet (Man-in-the-Middle*)*

Mỗi truy vấn DNS (Domain Name System) được gửi qua mạng đều có chứa một số nhận dạng duy nhất, mục đích của số nhận dạng này là để phân biệt các truy vấn và đáp trả chúng. Điều này có nghĩa rằng nếu một máy tính đang tấn công, chúng ta có thể chặn một truy vấn DNS nào đó được gửi đi từ một thiết bị cụ thể, thì tất cả những gì chúng ta cần thực hiện là tạo một gói giả mạo có chứa số nhận dạng đó để gói dữ liệu được chấp nhận bởi mục tiêu.

Chúng ta sẽ hoàn tất quá trình bằng cách thực hiện hai bước với một công cụ đơn giản. Đầu tiên, chúng ta cần giả mạo ARP cache thiết bị mục tiêu để định tuyến lại lưu lượng của nó qua host đang tấn công của mình, từ đó có thể chặn yêu cầu DNS và gửi đi gói dữ liệu giả mạo. Mục đích của kịch bản này là lừa người dùng trong mạng truy cập vào website độc, thay vì website mà họ đang cố gắng truy cập.

Việc tạo ra một kiểu tấn công mới là mục đích của các hacker. Trên mạng Internet hiện nay, có thể sẽ xuất hiện những kiểu tấn công mới được khai sinh từ những hacker thích mày mò và sáng tạo.

### 3.2.3. Tấn công cơ sở dữ liệu

Ví dụ: SQL Injection attack

Là đoạn mã tiềm ẩn lỗ hổng nghiêm trọng, nó cho phép những kẻ tấn công thi hành các câu lệnh truy vấn SQL bất hợp pháp bằng cách lợi dụng lỗ hổng trong việc kiểm tra dữ liệu nhập trong các ứng dụng Web. Hậu quả của nó rất tai hại vì nó cho phép những kẻ tấn công thực hiện thao tác xoá, hiệu chỉnh,… do có toàn quyền trên cơ sở dữ liệu của ứng dụng. Lỗi này thường xảy ra trên các ứng dụng web có dữ liệu được quản lí bằng các hệ quản trị CSDL như SQL Server, Oracle, DB2, Sysbase.

Xét một ví dụ điển hình của SQL Injection attack, thông thường để cho phép người dùng truy cập vào các trang web được bảo mật, hệ thống thường xây dựng trang đăng nhập để yêu cầu người dùng nhập thông tin về tên đăng nhập và mật khẩu. Sau khi người dùng nhập thông tin vào, hệ thống sẽ kiểm tra tên đăng nhập và mật khẩu có hợp lệ hay không để quyết định cho phép hay từ chối thực hiện tiếp. Trong trường hợp này, người ta có thể dùng 2 trang, một trang HTML để hiển thị form nhập liệu và một trang ASP dùng để xử lí thông tin nhập từ phía người dùng.

Ví dụ:

**Login.htm**

```
<form action="ExecLogin.asp" method="post">
 Username:  <input type="text" name="txtUsername"><br>
 Password:  <input type="password" name="txtPassword"><br>
 <input type="submit">
</form>
```

**ExecLogin.asp**

```
<%
 Dim p_strUsername, p_strPassword, objRS, strSQL
  p_strUsername = Request.Form("txtUsername")
 p_strPassword = Request.Form("txtPassword")
  strSQL = "SELECT * FROM tblUsers " & _
        "WHERE Username='" & p_strUsername & _
        "' and Password='" & p_strPassword & "'"
  Set objRS = Server.CreateObject("ADODB.Recordset")
 objRS.Open strSQL, "DSN=..."
  If (objRS.EOF) Then
   Response.Write "Invalid login."
 Else
   Response.Write "You are logged in as " & objRS("Username")   End If
  Set objRS = Nothing
%>
```

Đoạn mã trong trang ExecLogin.asp dường như không chứa bất cứ một lỗ hổng về an toàn nào. Người dùng không thể đăng nhập mà không có tên đăng nhập và mật khẩu hợp lệ. Tuy nhiên, đoạn mã này không an toàn và là tiền đề cho một SQL injection attack. Đặc biệt, sơ hở nằm ở chỗ dữ liệu nhập vào từ người dùng được dùng để xây dựng trực tiếp câu lệnh truy vấn SQL. Điều này cho phép những kẻ tấn công có thể điều khiển câu truy vấn sẽ được thực hiện.

Ví dụ, nếu người dùng nhập chuỗi sau vào trong cả 2 ô nhập liệu tên người dùng/ mật khẩu của trang Login.htm:

‘ or ‘’ = ‘ . Lúc này, câu truy vấn sẽ được gọi thực hiện là:

SELECT * FROM tblUsers WHERE Username='' or ''='' and Password = '' or ''=''

Câu truy vấn này là hợp lệ và sẽ trả về tất cả các bản ghi của tblUsers và đoạn mã tiếp theo xử lí người dùng đăng nhập bất hợp pháp này như là người dùng đăng nhập hợp lệ.

**Các tác hại của SQL Injection attack:**

Tác hại từ SQL Injection attack tùy thuộc vào môi trường và cách cấu hình hệ thống. Nếu ứng dụng sử dụng quyền dbo (quyền của người sở hữu CSDL - owner) khi thao tác dữ liệu, nó có thể xóa toàn bộ các bảng dữ liệu, tạo các bảng dữ liệu mới, … Nếu ứng dụng sử dụng quyền quản trị hệ thống, nó có thể điều khiển toàn bộ hệ quản trị CSDL và với quyền hạn rộng lớn như vậy nó có thể tạo ra các tài khoản người dùng bất hợp pháp để điều khiển hệ thống.

# *Chương 4.* CÁC PHƯƠNG PHÁP PHÒNG TRÁNH "TẤN CÔNG" BẰNG XỬ LÝ "LỖ HỔNG"

## 4.1. BẢO VỆ AN TOÀN THÔNG TIN

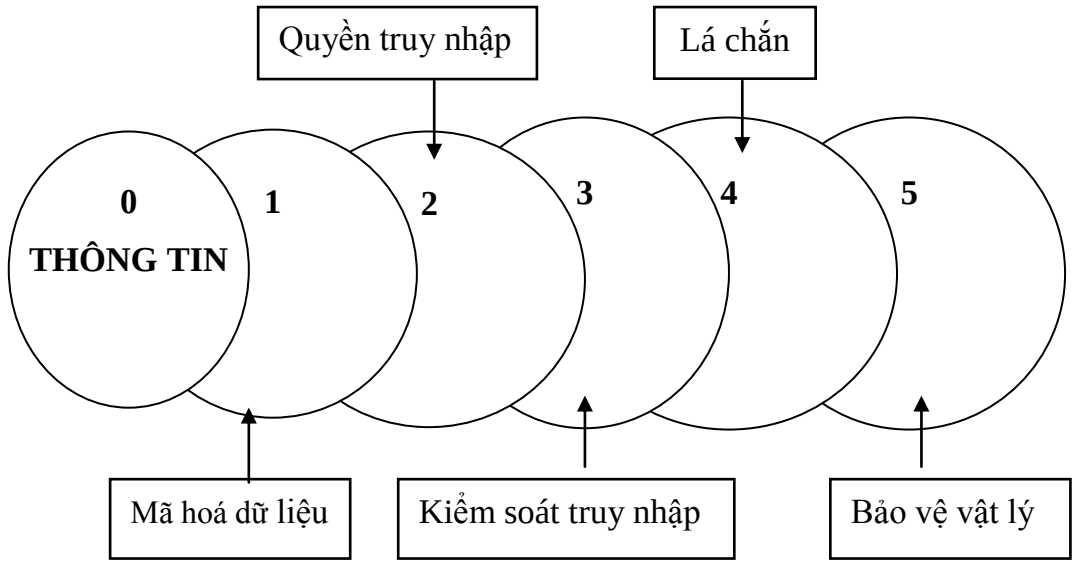
Khoa học máy tính ra đời, cùng với sự phát triển về phần cứng là sự phát triển hùng hậu của ngành phần mềm, mạng, cơ sở dữ liệu... Chính vì vậy việc tấn công và phòng tránh tấn công là một vấn đề luôn rất quan trọng.

### 4.1.1. Các lớp bảo vệ thông tin

Trong thời đại phát triển của công nghệ thông tin, mạng máy tính quyết định toàn bộ hoạt động của cá nhân, cơ quan, tổ chức, hay các công ty, xí nghiệp. Vì vậy, việc bảo đảm cho hệ thống máy tính hoạt động một cách an toàn, không xảy ra sự cố là công việc cấp thiết hàng đầu. Công tác quản trị mạng máy tính phải được thực hiện một cách khoa học.

Vì không thể có một giải pháp an toàn tuyệt đối nên người ta thường phải sử dụng đồng thời nhiều mức bảo vệ khác nhau, tạo thành nhiều lớp "rào chắn" đối với các hoạt động xâm phạm. Việc bảo vệ thông tin chủ yếu là bảo vệ thông tin cất giữ trong máy tính, đặc biệt là các máy chủ trên mạng.

Thông thường bao gồm các mức bảo vệ sau:




Mô tả các lớp rào chắn thông dụng hiện nay

#### *4.1.1.1. Mã hoá dữ liệu*

Để bảo mật thông tin trên máy tính hay trên đường truyền người ta sử dụng các phương pháp mã hoá (Encryption). Dữ liệu bị biến đổi từ dạng "hiểu được" sang dạng "không hiểu được" theo một thuật toán nào đó và sẽ được biến đổi ngược lại ở trạm nhận (giải mã). Đây là lớp bảo vệ thông tin rất quan trọng.

#### *4.1.1.2. Quyền truy nhập*

Là việc phân quyền truy nhập tài nguyên thông tin và quyền hạn trên tài nguyên đó.

Xây dựng cơ chế quản lý truy nhập nhằm kiểm soát, bảo vệ các tài nguyên thông tin, càng kiểm soát được chi tiết càng tốt.

Trong một hệ thống quyền cao nhất nên do ít nhất 2 người nắm giữ đề phòng mất mát về con người. Nếu chỉ do 1 người nắm giữ, không may xảy ra vấn đề với người đó (bệnh tật, tai nạn,…) sẽ dẫn đến làm ngưng trệ hoạt động của hệ thống; gây hậu quả nghiêm trọng. Đối với các hệ thống lớn như: Ngân hàng, an ninh quốc gia,… thì phải 3 người quản lý.

#### *4.1.1.3.Kiểm soát truy nhập (Đăng ký tên /mật khẩu)*

Hạn chế theo tài khoản truy nhập (gồm đăng ký tên và mật khẩu). Đây là phương pháp bảo vệ phổ biến nhất vì nó đơn giản, ít tốn kém và cũng rất hiệu quả. Mỗi người dùng muốn truy nhập vào hệ thống để sử dụng tài nguyên đều phải có đăng ký tên và mật khẩu.

Thực ra đây cũng là kiểm soát truy nhập, nhưng không phải truy nhập ở mức thông tin mà ở mức hệ thống. Người quản trị mạng có trách nhiệm quản lý, kiểm soát mọi hoạt động của mạng và xác định quyền truy nhập của những người dùng khác theo thời gian và không gian (nghĩa là người dùng chỉ được truy nhập trong một khoảng thời gian nào đó tại một vị trí nhất định nào đó).

Theo lý thuyết nếu mọi người đều giữ kín được mật khẩu và tên đăng ký của mình thì sẽ không xảy ra các truy nhập trái phép. Nhưng điều đó khó đảm bảo trong thực tế vì nhiều nguyên nhân khác nhau dẫn đến làm giảm hiệu quả của lớp bảo vệ này. Có thể khắc phục bằng cách người quản mạng chịu trách nhiệm đặt mật khẩu hoặc thay đổi mật khẩu theo thời gian hay chu kỳ nhất định.

#### *4.1.1.4. Lá chắn*

Cài đặt các lá chắn nhằm ngăn chặn các thâm nhập trái phép và cho phép lọc bỏ các gói tin không mong muốn gửi đi, hoặc thâm nhập vì lý do nào đó để bảo vệ một máy tính hoặc cả mạng nội bộ (intranet). Ví dụ: Tường lửa

#### *4.1.1.5. Bảo vệ vật lý*

Bảo vệ vật lý nhằm ngăn chặn các truy nhập bất hợp pháp vào hệ thống.

Thường dùng các biện pháp truyền thống như ngăn cấm người không có nhiệm vụ vào phòng máy, dùng hệ thống khóa trên máy tính, cài đặt các hệ thống báo động khi có truy nhập trái phép.

* Ngoài 5 lớp bảo vệ trên, tuỳ mức độ lớn nhỏ của hệ thống cần bảo vệ mà còn có thể xây dựng thêm các lớp bảo vệ thông tin khác như: Sao lưu dự phòng (trước khi mã hoá), bảo vệ bằng sự đa dạng hệ thống (Ví dụ: Các máy tính trong 1 hệ thống thì có thể khác hãng xản xuất, khác cấu hình, khác hệ điều hành, khác hình thức bảo vệ,…), sử dụng các ứng dụng có thể hoạt động trên các môi trường khác nhau,…

### 4.1.2. Các công cụ bảo vệ thông tin

Mỗi khi chúng ta kết nối mạng, nghĩa là là chúng ta đang đặt máy tính và các thông tin lưu trong máy tính của mình đối diện với các mối nguy hiểm rình rập trên mạng, 99% các cuộc tấn công đến từ web.

Cách tốt nhất là bảo vệ máy tính qua các lớp bảo mật. Nếu một vùng bảo vệ chỉ đạt hiệu quả 75%, các lớp bảo vệ khác sẽ lấp nốt các lỗ hổng còn lại. Các lớp bảo vệ này gồm có:

#### 4.1.2.*1. Tường lửa*

Tường lửa bảo vệ máy tính khỏi những kẻ tấn công. Có nhiều lựa chọn tường lửa: Tường lửa phần cứng, phần mềm, tường lửa trong các định tuyến không dây.

#### 4.1.2.*2. Phần mềm quản trị người dùng và kiểm soát mạng*

Một máy tính bị tấn công có thể làm phá hủy cả hệ thống máy tính hay mạng, do đó để đảm bảo an toàn hơn nên kiểm soát các website nhân viên truy nhập thông qua các chính sách quản lý trên máy chủ.

#### 4.1.2.*3. Phần mềm chống virus, mã độc và  gián điệp (spyware)*

Các phần mềm này bảo vệ máy tính khỏi virus, trojans, sâu, rootkit và những cuộc tấn công. Ngày nay, các chương trình này thường được đóng gói lại. Bởi vì có hàng nghìn biến thể mã độc xuất hiện hàng ngày nên rất khó để các công ty phần mềm có thể theo kịp. Vì vậy, nhiều người dùng cảm thấy an toàn hơn khi cài nhiều chương trình bảo mật, nếu chương trình này bỏ qua một mã độc nào đó, có thể chương trình khác sẽ phát hiện được.

#### 4.1.2.*4. Giám sát hành vi*

Giám sát hành vi là để phát hiện ra những hành vi khả nghi của mã độc. Ví dụ, một chương trình mới tự cài đặt vào máy tính có thể là mã độc có chức năng ghi lại hoạt động của bàn phím.

#### 4.1.2.*5. Dùng phiên bản trình duyệt mới*

Thường xuyên cập nhật thông tin, tìm hiểu các phiên bản mới. Nếu thấy phù hợp thì nên chuyển sang dùng các phiên bản mới. Các phiên bản mới thường là phát triển từ phiên bản cũ nên tránh được một số lỗi phiên bản cũ đã gặp phải…

Ví dụ: Internet Explorer 8 (IE8) có thể không hoàn hảo, nhưng nó còn an toàn hơn nhiều IE6, phiên bản trình duyệt lỗi thời này của Microsoft hiện vẫn còn rất nhiều người sử dụng.

#### 4.1.2.*6. Phần mềm mã hóa dữ liệu*

Nên lưu dữ liệu an toàn bằng cách mã hóa chúng. Xây dựng hệ thống dự phòng trực tuyến. Điều này giúp chúng ta có thể lấy lại dữ liệu trong trường hợp máy tính bị ăn cắp hay hỏng.

## 4.2. PHÒNG TRÁNH TẤN CÔNG HỆ ĐIỀU HÀNH

### 4.2.1. Phòng tránh tấn công hệ điều hành

Đối với việc phòng tránh tấn công hệ điều hành (HĐH) cần chú ý 12 điểm sau:

1/. Thường xuyên cập nhật thông tin về các lỗi bảo mật liên quan đến HĐH mình đang sử dụng trên Website của Microsoft và các diễn đàn bảo mật khác.

Không chỉ cần sử dụng các bản cập nhật của Windows mà cần phải chú ý tới các bản cập nhật của Unix/ Linux và Mac khi chúng được phát hành.

Trong hầu hết trường hợp, những phiên bản hệ điều hành mới luôn an toàn hơn so với các phiên bản trước đó dù đã được vá hoàn toàn. Ví dụ, Windows 7 và Windows Vista tích hợp một số cơ chế bảo mật như UAC (User Account Control: Điều khiển tài khoản người dùng), chế độ bảo mật cho IE (Internet Explorer: Trình duyện mạng liên kết), công cụ mã hóa ổ đĩa Bitlocker,… mà Windows XP không có. Phiên bản Mac OS X mới nhất tích hợp công cụ phát hiện malware. Phiên bản mới nhất của OpenSUSE hỗ trợ công nghệ modul nền tảng tin cậy (TPM - Trusted Platform Module). Trong nhiều trường hợp, quá trình nâng cấp lên phiên bản mới của bất kì hệ điều hành nào cũng giúp tăng cường bảo mật.

2/. Hạn chế tối đa quyền truy cập trực tiếp vào máy chủ, không cài đặt những phần mềm không cần thiết lên những máy chủ dịch vụ, không cho phép người sử dụng dùng máy chủ để làm những công việc không liên quan đến quản trị,...

3/. Hạn chế tối đa mở các cổng (port), không cần thiết thì nên đóng chúng lại.

4/. Thiết lập danh sách những dải địa chỉ IP có nguy cơ cao truy cập vào (có thể tìm thông tin về những dải này trên một số trang web uy tín như: http://www.countryipblocks.net/,...).

5/.Thiết lập một tường lửa (firewall) mềm (có thể dùng chính tường lửa của Windows (điển hình Windows 2008 rất mạnh phần này), hoặc sử dụng một tường lửa miễn phí hay thương mại; thiết lập thời gian cho phép truy cập vào máy chủ, những ứng dụng cho phép chạy, những người dùng được phép truy cập từ xa (Remote),...

6/. Phải có tối thiểu một phần mềm diệt virus được cài đặt, hoạt động trên máy.

7/.Thiết lập nhật ký và thường xuyên theo dõi nhật ký hệ thống. Cài đặt, thiết lập trình xem sự kiện (Control Panel -> Administrative Tools; Chọn Event Viewer).

Ngoài ra còn phải thường xuyên giám sát năng lực máy chủ (server) thông qua hiệu suất máy màn hình - Performance Monitor (Control Panel -> Administrative Tools; Chọn Performance Monitor).

8/. Luôn có phương án sao lưu (backup) hệ thống và dữ liệu (chủ yếu là việc đặt lịch sao lưu). Thiết lập sao lưu tự động hệ thống và sao lưu hoạt động thư mục (Backup Active Directory). Ngoài ra, có thể đặt lịch Ghost máy tính.

9/. Thiết lập các chính sách nội bộ nếu máy tính hoạt động theo mô hình Workgroup (Chủ yếu dựa vào GPO - Group Policy Object - Đối tượng chính sách nhóm), Thiết lập trong Start->run->gpedit.msc.

10/. Chú ý đến an toàn vật lý (xem thêm: "*4.1.1.5. Bả*o vệ vật lý"**).**

11/. Duy trì sự đa dạng của hệ thống (Hệ thống phải được duy trì ở đa dạng một số HĐH, đề phòng khi một HĐH cụ thể nào đó bị lỗi thì không phải tất cả các dịch vụ hay máy chủ cũng bị lỗi).

12/. Yếu tố con người: Phần này nói đến người làm công tác quản trị mạng phải thường xuyên tự học tập nâng cao trình độ, làm việc phải có quy trình tác nghiệp, phải có nhật ký làm việc để những người cùng làm biết được những thay đổi,…

### 4.2.2. Một số ví dụ cụ thể

#### *4.2.2.1. Phòng tránh tấn công mật khẩu (password) của tài khoản người dùng*

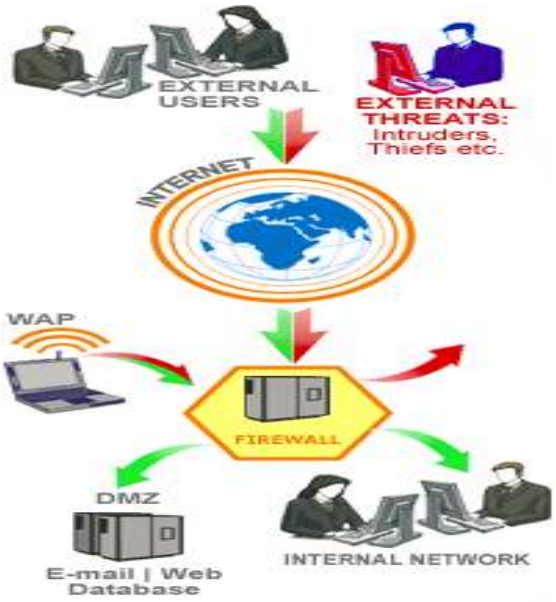
- Đề phòng những người truy cập trái phép vào máy tính của mình.
- Đặt mật khẩu dài trên 14 ký tự và có đầy đủ các ký tự: Đặc biệt, hoa, số, thường.
- Bật tường lửa bảo vệ (Enable Firewall) để chống PasswordDUMP.
- Cài đặt và cập nhật các bản vá lỗi mới nhất từ nhà sản xuất.
- Cài đặt tối thiểu một chương trình diệt Virus mạnh.

#### *4.2.2.2. Phòng tránh tấn công hệ thống Windows qua lỗ hổng bảo mật*

- Luôn cập nhật (update) các bản vá lỗi mới nhất từ nhà sản xuất.
- Bật tường lửa (Enable Firewall), chỉ mở cổng cần thiết cho các ứng dụng.
- Có thiết bị IDS (Intrusion Detection Systems) phát hiện xâm nhập.
- Có tường lửa (Firewall) chống quét các dịch vụ đang chạy.

### *4.2.3.* Xây dựng hệ thống tường lửa (Firewalls)

#### *4.2.3.1. Khái niệm tường lửa*




Tường lửa trong công nghệ mạng thông tin được hiểu là một hệ thống gồm phần cứng, phần mềm, hay hỗn hợp phần cứng - phần mềm, có tác dụng như một tấm ngăn cách giữa các tài nguyên thông tin của mạng nội bộ với thế giới internet bên ngoài.

Phạm vi hẹp hơn, như trong mạng nội bộ, người ta cũng bố trí tường lửa để ngăn cách các miền an toàn khác nhau (Security domain).

Thuật ngữ tường lửa có nguồn gốc trong kỹ thuật xây dựng để ngăn chặn, hạn chế hỏa hoạn. Trong công nghệ thông tin, tường lửa là kỹ thuật được tích hợp vào hệ thống mạng để chống lại sự truy cập trái phép. Kỹ thuật nhằm bảo vệ thông tin nội bộ, mặt khác hạn chế sự xâm nhập của thông tin trái phép vào hệ thống.

Kỹ thuật này phục vụ cho an toàn hệ thống máy tính là chính, nhưng cũng hỗ trợ bảo đảm an toàn truyền tin. Ví dụ chống trộm cắp, sửa đổi thông tin trước khi đến tay người nhận.

#### *4.2.3.2. Chức năng của tường lửa*

Hoạt động hệ thống tường lửa đảm bảo các chức năng sau:

- Hạn chế truy nhập tại một điểm kiểm tra.
- Ngăn chặn các truy nhập từ ngoài vào trong hệ thống.
- Hạn chế các truy nhập ra ngoài.

Xây dựng tường lửa là một biện pháp khá hữu hiệu, nó cho phép bảo vệ và kiểm soát hầu hết các dịch vụ. Do đó, nó được áp dụng phổ biến nhất trong các biện pháp bảo vệ mạng.

#### *4.2.3.3. Phân loại tường lửa*

**1/. Về mặt vật lý, tường lửa gồm có**

- Một hay nhiều máy chủ kết nối với bộ định tuyến (Router) hoặc có chức năng định tuyến.
- Các phần mềm quản lý an ninh trên hệ thống máy chủ, ví dụ hệ quản trị xác thực (athetication), hệ cấp quyền (authorization), hệ kế toán (accounting), …

**2/. Về mặt chức năng, tường lửa có các thành phần**

- Tường lửa loại lọc gói (Packet filter firewall)

Là hệ thống tường lửa cho phép chuyển thông tin giữa hệ thống trong và ngoài mạng có kiểm soát. Nó có nhiệm vụ kiểm tra tất cả các luồng dữ liệu vào ra giữa mạng tin cậy và Internet. Nó kiểm tra địa chỉ nguồn và đích, các cổng để từ chối hoặc cho phép các gói tin đi vào khi thỏa mãn các quy tắc được lập trình trước.

- Tường lửa kiểm soát trạng thái (Stateful inspection firewall)

Có nhiệm vụ kiểm tra từng cổng riêng biệt của các máy trạm, được thực hiện thông qua "bảng trạng thái", không mở nhiều cổng cho các lưu thông đi vào. Vì vậy, tránh được các rủi ro xâm nhập vào hệ thống từ những người dùng trái phép.

- Tường lửa uỷ quyền mức ứng dụng (Application proxy firewall)

Là hệ thống tường lửa thực hiện các kết nối thay cho các kết nối trực tiếp từ máy khách yêu cầu. Có khả năng ghi lại các thông tin nhật ký do nó kiểm tra toàn bộ các gói tin trên mạng chứ không phải là địa chỉ mạng và các cổng. Đồng thời, cho phép người quản trị áp dụng phương pháp xác thực người dùng trực tiếp tránh được việc giả mạo.

### *4.2.3.4. Nguyên tắc hoạt động của tường lửa*

**1/. Nguyên tắc chung**

Trước khi xây dựng một tường lửa phải nghiên cứu rất kỹ lưỡng và phải hiểu rất rõ mạng đó. Điều này cần thiết phải được tổ chức tốt bao gồm nhiều công đoạn khác nhau, có thể được kết nối với nhau. Việc kết nối này có thể là tự động hoặc nhờ sự tác động của con người. Đối với một số mạng (nhất là với các ISPs - Internet service provider – nhà cung cấp dịch vụ mạng liên kết) thì việc sử dụng tường lửa hoàn toàn không cần nhất thiết vì sẽ mất khách hàng nếu như áp dụng một loạt các chính sách ngăn chặn cứng nhắc.

Một vấn đề khác nữa khi sử dụng tường lửa là đối với các dịch vụ như ftp, telnet, http,… thì nó cũng tạo ra một số vấn đề về truy nhập dịch vụ.

**2/. Lọc gói (Packet Filtering)**

Kiểu tường lửa chung nhất là kiểu dựa trên mức mạng của mô hình OSL, tường lửa mức mạng thường hoạt động theo nguyên tắc router, có nghĩa là tạo ra các luật cho phép ai hay cái gì được truy nhập mạng dựa trên mức mạng. Mô hình này hoạt động dựa trên gói tin packet filtering.

Nó kiểm tra các gói tin trên router (bộ định tuyến) từ mạng ngoài. Ở kiểu hoạt động này các gói tin đều được kiểm tra địa chỉ nguồn nơi chúng xuất phát. Thông qua địa chỉ IP nguồn được xác định thì nó được kiểm tra với các luật đã được đặt ra trên router.

Các gói tin hoạt động trong một lớp mạng (tương tự như một router) thường cho phép tốc độ xử lý nhanh bởi nó chỉ kiểm tra địa chỉ IP nguồn mà không có một lệnh thực sự nào trên router, nó không cần một khoảng thời gian nào để kiểm tra là địa chỉ sai hay bị cấm, nhưng điều này bị trả giá bởi tính tin cậy của nó. Kiểu tường lửa này sử dụng địa chỉ IP làm chỉ thị, điều này tạo ra một lỗ hổng là nếu gói tin mang địa chỉ nguồn là địa chỉ giả thì như vậy nó sẽ có được một số mức truy nhập vào mạng trong của chúng ta.

**3/. Tường lửa uỷ quyền mức ứng dụng (Application proxy firewall)**

Kiểu tường lửa này hoạt động khác với kiểu tường lửa trước, nó dựa trên phần mềm. Khi một kết nối từ người nào đó đến mạng sử dụng tưởng lửa kiểu này thì kết nối đó sẽ bị chặn lại, sau đó tường lửa sẽ kiểm tra các trường có tổng quan của gói tin yêu cầu kết nối. Nếu việc kiểm tra thành công, có nghĩa là các trường thông tin đáp ứng được các luật đã đặt ra trên tường lửa, nó sẽ tạo một cái cầu kết nối giữa hai nút (node) với nhau.

Ưu điểm của kiểu tường lửa loại này là không có chức năng chuyển tiếp các gói tin IP, hơn nữa ta có thể điều khiển một cách chi tiết hơn các kết nối trong qua tường lửa. Đồng thời nó còn đưa ra nhiều công cụ cho phép ghi lại các quá trình kết nối cũng như các gói tin chuyển qua tường lửa đều được kiểm tra kỹ lưỡng với các luật trên tường lửa, và rồi nếu như được chấp nhận sẽ được chuyển tiếp tới nút (điểm) đích.

Sự chuyển tiếp các gói tin IP xảy ra khi một máy chủ nhận được một yêu cầu từ mạng ngoài, rồi chuyển chúng vào mạng trong. Điều này tạo ra một lỗ hổng cho những kẻ phá hoại xâm nhập từ mạng ngoài vào mạng trong.

Nhược điểm của tường lửa hoạt động dựa trên ứng dụng là phải tạo cho mỗi dịch vụ trên mạng một trình ứng dụng uỷ quyền (proxy) trên tường lửa.

***4.2.3.5. Các bước xây dựng tường lửa***

Xây dựng một hệ thống tường lửa không phải là đơn giản, yêu cầu người quản trị hê thống phải có kinh nghiệm quản trị hệ thống và hiểu biết cơ chế hoạt động các dịch vụ ngoài ra người cài đặt tường lửa cần kiểm tra từng bước sau:

- Xác định kiến trúc mạng và giao thức cần thiết.
- Xây dựng các chính sách an toàn.
- Sử dụng những công cụ này một cách hiệu quả.
- Kiểm tra thử nghiệm hệ thống.

**1/. Xác định kiến trúc mạng và giao thức cần thiết**

Bước đầu tiên là cần phải hiểu toàn bộ mạng, công việc này không chỉ đơn giản là xem lại các máy, các giấy tờ văn bản…. Nó phải được thảo luận với các phòng khác nhau.

Công việc đầu tiên là xác định cái nào bị cấm và cái nào không bị cấm, cũng như phải liệt kê tất cả các giao thức cần thiết được sử dụng trên mạng.

Đây là công việc khá phức tạp, ví dụ như chúng ta sẽ không cho các mạng tung ra những email không mong muốn mang nội dung xấu hay những thông tin không phục vụ cho việc kinh doanh của mình, là một điều rất khó.

**2/. Xây dựng các chính sách về bảo mật**

Cần thiết lập một chính sách cụ thể về bảo mật, từ đó xác định các "luật" áp dụng trên tường lửa:

- Các "luật" trên tường lửa bị mâu thuẫn với nhau.
- Các "luật" quá chặt, hạn chế dịch vụ cung cấp và người sử dụng.
- Các "luật" quá lỏng, mất các chức năng của tường lửa.

## 4.3. PHÒNG TRÁNH TẤN CÔNG PHẦN MỀM ỨNG DỤNG

### 4.3.1. Chủ quan (lỗi do người viết phần mềm)

Đây là lỗi chủ quan từ phía quản lý, người viết phần mềm; Vì vậy phòng tránh tấn công vào điểm này:

- Lựa chọn nhà quản lý, người viết phần mềm tin cậy.
- Chia nhỏ công việc như vậy sẽ tránh để một người thao túng toàn bộ.
- Có mô hình thiết kế, tài liệu kèm theo đầy đủ giúp người sau có thể nắm bắt hệ thống giúp nâng cấp, bảo trì, kiểm soát, quản trị hệ thống toàn diện.

### 4.3.2. Khách quan (từ người sử dụng)

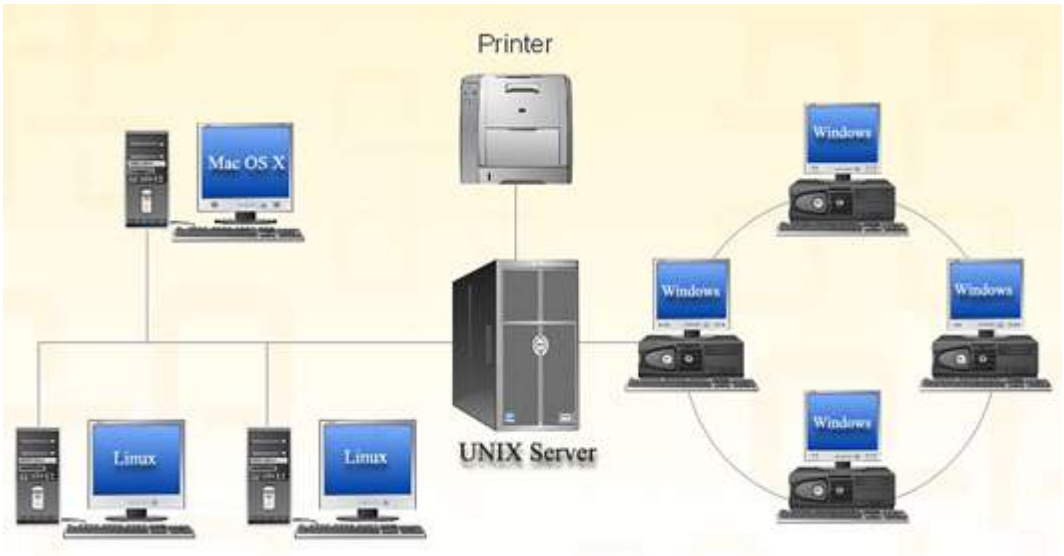
- Quản lý bằng tên, mật khẩu riêng.
- Đảm bảo thông tin người dùng luôn được giữ bí mật.
- Học cách tự bảo vệ chính mình, thiết lập hệ thống bảo mật toàn diện, nhiều lớp.
- Thường xuyên cập nhật các bản vá lỗi mới nhất từ nhà sản xuất. Cập nhật các cảnh báo để đề phòng trước.
- Khai thác tối ưu các tính năng bảo mật của chính những phần mềm sử dụng.

## 4.4. PHÒNG TRÁNH TẤN CÔNG MẠNG

Hiện nay, hệ thống mạng ngày càng chứa nhiều loại máy tính khác nhau (bao gồm nhiều loại phần cứng, phần mềm và hệ điều hành) - gọi là mạng đa nền tảng.

Những hệ thống mạng thuần ngày càng ít xuất hiện, nhiều công ty đã sử dụng miền Windows cho các máy chủ Web UNIX, được truy cập bởi các máy trạm sử dụng hệ điều hành Windows, Linux và Mac.

Chúng ta luôn cần tải mail, tài nguyên hay truy cập vào các tài nguyên khác trên mạng. Trong những trường hợp đó chúng ta sẽ gặp nhiều khó khăn trong việc bảo vệ mạng.




Mô hình mạng đa nền tảng

Phần lớn những quản trị viên được đào tạo để quản trị một kiểu hệ thống cụ thể (Windows, UNIX, Mainframe,…). Trong khi đó bảo mật là một lĩnh vực nhạy cảm, không chỉ cần những quản trị viên có thể cấu hình và quản lý nhiều kiểu hệ thống khác nhau trên mạng, mà còn cần những người được đào tạo bảo mật nhiều loại hệ điều hành (HĐH) khác nhau. Họ cần có những hiểu biết cơ bản về bảo mật và được các nhà cung cấp (HĐH, chương trình ứng dụng,…) đào tạo. Có như vậy mới khai thác hết được cơ chế bảo mật tích hợp của HĐH.

Kết quả bảo mật phụ thuộc một phần vào thói quen, kinh nghiệm của từng người. Nếu một quản trị viên phải ghi nhớ nhiều thao tác và phương pháp khác nhau với từng loại thiết bị, luôn tồn tại những rủi ro nhất định dẫn đến hệ thống mạng sẽ xuất hiện điểm yếu. Đó là lí do tại sao hệ thống mạng hỗn hợp cần phải được quản trị bởi nhiều nhân viên chuyên trách cho mỗi loại hệ thống khác nhau.

Cần phải thường xuyên thống kê thành phần mạng vì:

Nếu một hệ thống mạng không được lên kế hoạch thiết kế cụ thể (thường chỉ là những hệ thống tự phát), khi có nhu cầu sử dụng dẫn đến việc mua và triển khai các máy tính mới không tuân theo một trật tự nào. Nguyên tắc đầu tiên cần tuân thủ để bảo mật mạng là phải biết được chúng ta có những gì, do đó tiến trình kiểm kê phần mềm và phần cứng mạng không thể bỏ qua.

Bản thống kê phải bao gồm mọi phần cứng và mọi phần mềm vận hành trên mạng, cho dù một số thiết bị nào đó không thường xuyên kết nối tới mạng.

Cập nhật và/ hoặc nâng cấp:

Cho dù sử dụng hệ thống nào hay nền tảng nào thì cũng không có gì đảm bảo rằng hệ thống đó là bất khả xâm phạm. Vì vậy cần phải thường xuyên cập nhật các lỗi, các phiên bản mới,…

Thông thường khi nhắc đến Windows, người ta thường coi đây là hệ thống "yếu nhất" và những hệ thống khác là "an toàn". Tuy nhiên không hẳn như vậy, chỉ là do hệ điều hành Windows được nhiều người dùng sử dụng nên đây là "miếng mồi" hấp dẫn nhất với tin tặc. Ví dụ: Linux, năm 2009 một lỗ hổng trong nhân được phát hiện trên hầu hết các phiên bản Linux cho phép tin tặc kiểm soát hoàn toàn hệ thống. Cũng trong năm 2009, Apple đã phải phát hành một bản vá, vá tổng cộng 67 lỗ hổng bảo mật trong Mac OS X và ứng dụng trình duyệt Safari, chưa kể một lỗ hổng nguy hiểm trong Java bị bỏ xót.

**Ví dụ cụ thể phòng tránh tấn công từ chối dịch vụ DoS & DDoS**

Hậu quả mà DoS gây ra không chỉ tiêu tốn nhiều tiền bạc, và công sức mà còn mất rất nhiều thời gian để khắc phục. Vì vậy, nên sử dụng các biện pháp sau để phòng chống DoS & DDoS:

**1/. Phòng ngừa các điểm yếu của ứng dụng (Application Vulnerabilities)**

Các điểm yếu trong tầng ứng dụng có thể bị khai thác gây lỗi tràn bộ đệm dẫn đến dịch vụ bị chấm đứt. Lỗi chủ yếu được tìm thấy trên các ứng dụng mạng nội bộ của Windows, trên các chương trình webserver, DNS, hay SQL database. Cập nhật bản vá (patching) là một trong những yêu cầu quan trọng cho việc phòng ngừa. Ngoài ra, hệ thống cần đặc biệt xem xét những yêu cầu trao đổi nội dung giữa client và server, nhằm tránh cho server chịu tấn công qua các thành phần gián tiếp (ví dụ SQL injection).

**2/. Phòng ngừa việc tuyển mộ zombie**

Zombie là các đối tượng được lợi dụng trở thành thành phần phát sinh tấn công. Một số trường hợp điển hình như thông qua rootkit, hay các thành phần hoạt động đính kèm trong mail, hoặc trang web, ví dụ như sử dụng các file jpeg khai thác lỗi của phần mềm xử lý ảnh hay thông qua việc lây lan worm (Netsky, MyDoom, Sophos). Để phòng chống, hệ thống mạng cần có những công cụ theo dõi và lọc bỏ nội dung (content filtering) nhằm ngăn ngừa việc tuyển mộ zombie của hacker.

**3/. Ngăn ngừa kênh phát động tấn công sử dụng công cụ**

Có rất nhiều các công cụ tự động tấn công DoS, chủ yếu là tấn công phân tán DDoS như TFN, TFN2000 (Tribe Flood Network) tấn công dựa trên nguyên lý như UDP, SYN,… . Các công cụ này có đặc điểm cần phải có các kênh phát động để zombie thực hiện tấn công tới một đích cụ thể. Hệ thống cần phải có sự giám sát và ngăn ngừa các kênh phát động đó.

**4/. Ngăn chặn tấn công trên băng thông**

Khi một cuộc tấn công DDoS được phát động, nó thường được phát hiện dựa trên sự thay đổi đáng kể trong thành phần của lưu lượng hệ thống mạng. Ví dụ một hệ thống mạng điển hình có thể có 80% TCP và 20% UDP và ICMP. Thống kê này nếu có thay đổi rõ rệt có thể là dấu hiệu của một cuộc tấn công. Việc phân tán lưu lượng gây ra bởi các virus máy tính (Worm) gây tác hại lên router, firewall, hoặc cơ sở hạ tầng mạng. Hệ thống cần có những công cụ giám sát và điều phối băng thông nhằm giảm thiểu tác hại của tấn công dạng này.

**5/. Ngăn chặn tấn công qua SYN**

SYN flood là một trong những tấn công cổ nhất còn tồn tại được đến hiện tại, Tuy nhiên, tác hại của nó không hề giảm. Điểm căn bản để phòng ngừa việc tấn công này là khả năng kiểm soát được số lượng yêu cầu SYN-ACK tới hệ thống mạng.

**6/. Phát hiện và ngăn chặn tấn công "tới hạn" số kết nối**

Bản thân các server có một số lượng "tới hạn" đáp ứng các kết nối tới nó. Ngay bản thân firewall (đặc biệt với các firewall có tính năng Kiểm tra trạng thái - Stateful inspection), các kết nối luôn được gắn liền với bảng trạng thái có giới hạn dung lượng. Đa phần các cuộc tấn công đều sinh số lượng kết nối ảo thông qua việc giả mạo.

Để phòng ngừa tấn công dạng này, hệ thống cần phân tích và chống được sự giả mạo (spoofing). Giới hạn số lượng kết nối từ một nguồn cụ thể tới server.

**7/. Phát hiện và ngăn chặn tấn công tới hạn tốc độ thiết lập kết nối**

Một trong những điểm các server thường bị lợi dụng là khả năng các bộ đệm giới hạn giành cho tốc độ thiết lập kết nối, dẫn đến quá tải khi phải chịu sự thay đổi đột ngột về số lượng sinh kết nối. Ở đây việc áp dụng bộ lọc để giới hạn số lượng kết nối trung bình rất quan trọng. Một bộ lọc sẽ xác định ngưỡng tốc độ kết nối cho từng đối tượng mạng. Thông thường, việc này được xách định bằng số lượng kết nối trong thời gian nhất định để cho phép sự dao động trong lưu lượng.

### 4.4.1. Mạng riêng ảo VPN (Virtual Private Network)


#### *4.4.1.1. Khái niệm mạng riêng ảo*

Mạng riêng ảo không phải là giao thức, cũng không phải là phần mềm máy tính. Đó là một chuẩn công nghệ cung cấp sự liên lạc an toàn giữa 2 thực thể bằng cách mã hóa các giao dịch trên mạng công khai (không an toàn, ví dụ như internet).

Mạng riêng ảo VPN (Virtual Private Network) được thiết kế cho những tổ chức có xu hướng tăng cường thông tin từ xa vì địa bàn hoạt động rộng (trên toàn quốc hay toàn cầu). Tài nguyên ở trung tâm có thể kết nối từ nhiều nguồn nên tiết kiệm được chi phí và thời gian. Về cơ bản, mạng riêng ảo VPN là một mạng riêng sử dụng hệ thống mạng công cộng (thường là Internet) để kết nối các địa điểm hoặc người sử dụng từ xa với một mạng LAN (Local Area Network) ở trụ sở trung tâm. Thay vì  việc sử dụng các kết nối phức tạp như đường dây thuê bao số, VPN tạo ra các "liên kết ảo" được truyền qua Internet giữa mạng riêng của một tổ chức với địa điểm hoặc người sử dụng ở xa thông suốt và bảo mật.

Qua mạng công khai, một thông điệp được chuyển qua một số máy tính, router, switch, vv… trên đường truyền tin thông điệp có thể bị chặn lại, bị sửa đổi hoặc bị đánh cắp. Mục đích của mạng riêng ảo là đảm bảo các yêu cầu sau:

- Tính bí mật, riêng tư: Người ngoài cuộc khó có thể hiểu được liên lạc đó.
- Tính toàn vẹn: Người ngoài cuộc khó có thể thay đổi được liên lạc đó.
- Tính xác thực: Người ngoài cuộc khó có thể tham gia vào liên lạc đó.

#### *4.4.1.2. Các thành phần của mạng riêng ảo*

**1/. Định đường hầm**

Định đường hầm là một cơ chế dùng để đóng gói một giao thức vào trong một giao thức khác.

Trên internet "định đường hầm" cho phép những giao thức như IPX (Internetwork Packet Exchange), talk,... được mã hóa, sau đó đóng gói trong IP.

Trong VPN, "định đường hầm" che giấu giao thức lớp mạng nguyên thủy bằng cách mã hóa gói dữ liệu này vào trong một vỏ bọc IP. Đó là một gói IP được truyền an toàn qua mạng internet. Khi nhận được gói IP trên, người nhận tiến hành gỡ bỏ vỏ bọc bên ngoài, giải mã dữ liệu trong gói này và phân phối nó đến thiết bị truy cập thích hợp.

Đường hầm cũng là một đặc tính ảo trong VPN. Các công nghệ đường hầm được dùng phổ biến hiện nay cho truy cập VPN gồm có: Giao thức định đường hầm điểm, L2F (Layer 2 Forwarding), L2TP (Layer 2 Tunneling Protocol), hoặc IP (Internet Protocol)…

**2/. Bảo mật**

Bảo mật bằng mã hóa đó là việc chuyển dữ liệu có thể hiểu được vào trong một định dạng "khó" thể hiểu được.

**3/. Thỏa thuận về chất lượng dịch vụ (QoS – service quality)**

Thỏa thuận về chất lượng dịch vụ thường định ra giới hạn cho phép về độ trễ trung bình của gói tin trong mạng. Ngoài ra, các thỏa thuận này được phát triển thông qua các dịch vụ với nhà cung cấp.

Mạng riêng ảo là sự kết hợp của định đường hầm, bảo mật và thỏa thuận QoS.

### 4.4.2. Tổng quan về công nghệ IPSEC

#### *4.4.2.1. Khái niệm IPSec*

Bảo mật giao thức mạng (IPSec - Internet Protocol Security), cho phép truyền dữ liệu an toàn ở lớp mạng. Và nó là sự lựa chọn cho các kết nối yêu cầu băng thông rộng, hiệu suất cao, dữ liệu lớn, kết nối liên tục và cố định. Đây là công nghệ mới đã và đang được ứng dụng rộng rãi trong thực tế.

Giao thức IPSec bao gồm một hệ thống các giao thức để bảo mật quá trình truyền thông tin trên nền tảng IP (Internet Protocol: Giao thức mạng liên kết). Nó bao gồm quá trình xác thực và /hoặc mã hóa (Authenticating and /or Encrypting) cho mỗi gói tin IP (IP parket) trong quá trình truyền thông tin. Việc xác thực đảm bảo các gói tin được gửi đi từ người gửi đích thực và không bị thay đổi trên đường đi. Việc mã hóa chống lại ý định đọc trộm nội dung của các gói tin. IPSec có thể bảo vệ bất kỳ một thủ tục nào dựa trên IP và bất kỳ một môi trường nào được sử dụng dưới tầng IP.

IPSec có quan hệ với một số bộ giao thức (AH, ESP, FIP - 140 - 1, và một số chuẩn khác) được phát triển bởi IETF (Internet Engineering Task Force). Mục đích của việc phát triển IPSec là cung cấp một cơ cấu bảo mật ở tầng 3 (Network Layer) của mô hình OSI. Các giao thức bảo mật khác như SSL, TLS, SSH đều hoạt động từ tầng 4 – tầng chuyển tải (Transport layer) trở lên. Điều này tạo ra tính mềm dẻo cho IPSec, nó có thể hoạt động từ tầng 4 với UDP (User datagram protocol), TCP (Transmission control protocol), và hầu hết các giao thức sử dụng ở tầng này.

| **Application Layer** |
|---|
| **Presentation Layer** |
| **Session Layer** |
| **Transport Layer** |
| **Network Layer**<br>**( IPSec )** |
| **Data Link Layer** |
| **Physical Layer** |

Với IPSec, tất cả các ứng dụng đang chạy ở tầng ứng dụng của mô hình OSI đều độc lập trên tầng 3 khi định tuyến dữ liệu từ nguồn đến đích. Bởi vì IPSec được tích hợp chặt chẽ với IP nên những ứng dụng có thể dùng các dịch vụ kế thừa tính năng bảo mật mà không cần phải có sự thay đổi lớn lao nào.

Các dịch vụ IPSec cho phép xây dựng các đường ngầm an toàn thông qua các mạng chưa được tin cậy. Bất kỳ một thông tin gì khi đi qua mạng chưa được tin cậy sẽ được mã hóa bởi công nghệ IPSec gateway, được giải mã bởi một IPSec Gateway ở đầu kia của đường truyền. Kết quả, thu được một mạng riêng ảo VPN - là một mạng được bảo mật hoàn toàn mặc dù nó bao gồm nhiều máy tại nhiều điểm được nối với nhau qua Internet.

#### *4.4.2.2. IPSec và mục đích sử dụng*

Với các quản trị viên, việc hiểu IPSec sẽ giúp chúng ta bảo vệ thông tin lưu chuyển trên mạng an toàn hơn, và cấu hình IPSec có thể tạo ra quy trình xác thực an toàn trong giao tiếp mạng ở mức tối đa.

**1/. Cài đặt IPSec**

IPSec là một chuẩn an toàn trong giao tiếp thông tin giữa các hệ thống, giữa các mạng. Với IPSec việc kiểm tra, xác thực, và mã hóa dữ liệu là những chức năng chính. Tất cả những việc này được tiến hành tại cấp độ gói IP.

**2/. Mục đích của IPSec**

Được dùng để bảo mật dữ liệu cho các chuyển giao thông tin qua mạng. Người quản trị có thể xác lập một hoặc nhiều chuỗi các luật, gọi là chính sách IPSEC, các luật này chứa các đầu lọc, có trách nhiệm xác định những loại thông tin lưu chuyển nào yêu cầu được mã hóa (Encryption), xác nhận (chữa ký số - digital signing), hoặc cả hai. Sau đó, mỗi gói tin được máy tính gửi đi, được xem xét có hay không gặp các điều kiện của chính sách. Nếu gặp những điều kiện này, thì các gói tin có thể được mã hóa, được xác nhận số, theo những quy định từ các chính sách. Quy trình này hoàn toàn vô hình với người dùng và ứng dụng kích hoạt truyền thông tin trên mạng. Do IPSec được chứa bên trong mỗi gói IP chuẩn, cho nên có thể dùng IPSec qua mạng, mà không yêu cầu những cấu hình đặc biệt trên thiết bị hoặc giữa 2 máy tính.

**3/. Những thuận lợi khi sử dụng IPSec**

Thuận lợi chính khi dùng IPSec là cung cấp được giải pháp mã hóa cho tất cả các giao thức hoạt động tại tầng 3 – tầng mạng trong mô hình OSI (Network layer of OSI model) và kể cả các giao thức lớp cao hơn.

**4/. Khả năng cung cấp bảo mật của IPSec**

- Chứng thực 2 chiều trước và trong suốt quá trình giao tiếp. IPSec quy định cho cả 2 bên tham gia giao tiếp phải xác định chính mình trong suốt quy trình giao tiếp.
- Tạo sự tin cậy qua việc mã hóa, và xác nhận số các gói. IPSEC có 2 chế độ là Encapsulating Security Payload (ESP), cung cấp cơ chế mã hóa dùng nhiều thuật toán khác nhau và sự thẩm định quyền của người lãnh đạo (AH - Authentication Header) xác nhận các thông tin chuyển giao, nhưng không mã hóa.
- Tích hợp các thông tin chuyển giao và sẽ loại ngay bất kì thông tin nào bị chỉnh sửa. Cả hai loại ESP và AH đều kiểm tra tính tích hợp của các thông tin chuyển giao. Nếu một gói tin đã chỉnh sửa, thì các xác nhận số sẽ không trùng khớp, kết quả gói tin sẽ bị loại. ESP cũng mã hóa địa chỉ nguồn và địa chỉ đích như một phần của việc mã hóa thông tin chuyển giao.
- Chống lại các cuộc tấn công làm chạy lại (replay), thông tin chuyển giao qua mạng sẽ bị kẻ tấn công chặn, chỉnh sữa, và được gửi đi sau đó đến đúng địa chỉ người nhận, người nhận không hề hay biết và vẫn tin rằng đấy là thông tin hợp pháp. IPSec dùng kĩ thuật đánh số liên tiếp cho các gói dữ liệu của mình (Sequence numbers), nhằm làm cho kẻ tấn công không thể sử dụng lại các dữ liệu đã chặn được, với ý đồ bất hợp pháp. Dùng kĩ thuật đánh số liên tiếp còn giúp bảo vệ chống việc chặn và đánh cắp dữ liệu, sau đó dùng những thông tin lấy được để truy cập hợp pháp vào một ngày nào đó.

**Ví dụ sử dụng IPSec:**

Việc mất mát các thông tin khi chuyển giao qua mạng, có thể gây thiệt hại cho hoạt động của tổ chức, điều này cảnh báo các tổ chức cần trang bị và xây dựng những hệ thống mạng bảo mật chặt chẽ những thông tin quan trọng như dữ liệu về sản phẩm, báo cáo tài chính, kế hoạch tiếp thị. Trong trường hợp này các tổ chức có thể sử dụng IPSec đảm bảo tính chất riêng tư và an toàn của truyền thông mạng (Intranet – mạng nội bộ, Extranet – mạng nội bộ mở rộng) bao gồm giao tiếp giữa trạm công tác với máy chủ (server), máy chủ với máy chủ.

Ví dụ: Có thể tạo chính sách IPSec cho các máy tính kết nối với Server (nắm giữ những dữ liệu quan trọng của tổ chức: Tình hình tài chính, danh sách nhân sự, chiến lược phát triển của tổ chức). Chính sách IPSecsẽ bảo vệ dữ liệu của tổ chức chống lại các cuộc tấn công từ bên ngoài, và đảm bảo tính tích hợp thông tin, cũng như an toàn cho máy khách.

***IPSec làm việc thế nào?***

Có thể cấu hình IPSec thông qua chính sách cục bộ, hoặc triển khai trên diện rộng thì dùng nhóm chính sách thư mục hiện hành (Active directory group policy).

a/. Giả sử chúng ta có 2 máy tính: Máy tính A và máy tính B, chính sách IPSec đã được cấu hình trên 2 máy này. Sau khi được cấu hình, IPSecsẽ báo cho bộ phận điều khiển IPSec cách làm thế nào để vận hành và xác định các liên kết bảo mật giữa 2 máy tính khi kết nối được thiết lập.

Các liên kết bảo mật ảnh hưởng đến những giao thức mã hóa sẽ được sử dụng cho những loại thông tin giao tiếp nào và những phương thức xác thực nào sẽ được đem ra thương lượng.

b/. Liên kết bảo mật mang tính chất thương lượng. Nếu máy A yêu cầu xác thực thông qua chứng nhận và máy B yêu cầu dùng giao thức kerberos (kiểm tra định danh người dùng và các thiết bị trong môi trường mạng client/server), thì IKE (Internet Key Exchange) sẽ có trách nhiệm thương lượng để tạo liên kết bảo mật, thiết lập liên kết bảo mật giữa 2 máy tính.

c/. Nếu như liên kết bảo mật được thiết lập giữa 2 máy tính, bộ phận điều khiển IPSEC sẽ quan sát tất cả các đường IP (IP traffic), so sánh các con đường đã được định nghĩa trong các bộ lọc, nếu có hướng đi tiếp các đường này sẽ được mã hóa hoặc xác nhận số.

***Chính sách bảo mật IPSec:***

IPSEC bao gồm một hoặc nhiều luật xác định cách thức hoạt động IPSEC. Các nhà quản trị có thể có thể cài đặt IPSEC thông qua một chính sách. Mỗi chính sách có thể chứa một hoặc nhiều luật, nhưng chỉ có thể xác định một chính sách hoạt động tại máy tính tại một thời điểm bất kì. Các nhà quản trị phải kết hợp tất cả những luật mong muốn vào một chính sách đơn giản. Mỗi luật bao gồm:

- Bộ lọc (Filter): bộ lọc báo cho chính sách những thông tin lưu chuyển nào sẽ áp dụng với hành động lọc (Filter action).

Ví dụ: người quản trị có thể tạo một đầu lọc chỉ xác định các lưu thông dạng HTTP hoặc FTP.

- Hành động lọc (Filter Action): Báo cho Policy phải đưa ra hành động gì nếu thông tin lưu chuyển trùng với định dạng đã xác định tại Filter. Ví dụ: Thông báo cho IPSEC chặn tất cả những giao tiếp FTP, nhưng với những giao tiếp HTTP thì dữ liệu sẽ được mã hóa. Filter action cũng có thể xác định những thuật toán mã hóa và hashing ( hàm băm) mà chính sách nên sử dụng.

- Authentication method: IPSEC cung cấp 3 phương thức xác thực:

Các chứng chỉ (thông thường các máy tính triển khai dùng IPSEC nhận các chứng chỉ từ một tổ chức cấp chứng chỉ (Certificate Authority – CA server)), Kerberos (Giao thức chứng thực phổ biến trong Active directory Domain), Preshared Key (khóa ngầm hiểu, một phương thức xác thực đơn giản). Mỗi một luật của chính sách IPSEC có thể bao gồm nhiều phương thức xác thực vừa nêu.

***Những chính sách IPSec mặc định***

Kể từ Windows 2000 trở đi IPSEC đã cấu hình sẵn 3 chính sách, tạo sự thuận tiện khi triển khai IPSEC.

* Máy trạm (Client)

Chính sách thụ động, chỉ phản hồi sử dụng IPSEC nếu đối tác có yêu cầu, thường được làm cho có thể (Enable) trên các trạm làm việc (Workstation). Chính sách mặc định này chỉ có một luật được gọi là luật đáp ứng mặc định (Default respond rule).

Luật này cho phép máy tính phản hồi đến các yêu cầu IPSEC ESP từ các máy tính được tin cậy trong miền thư mục hành động (Active directory domain). ESP là một chế độ IPSEC cung cấp độ tin cậy cho việc xác thực, tích hợp, và chống sự tấn công lặp lại (Replay attack).

* Máy chủ - Server (Request Security – yêu cầu bảo mật):

Máy tính hoạt động với chính sách này luôn chủ động dùng IPSEC trong giao tiếp, tuy nhiên nếu đối tác không dùng IPSEC, vẫn có thể cho phép giao tiếp không bảo mật. Chính sách này được dùng cho cả máy chủ và trạm làm việc.

* Máy chủ bảo mật - Secure Server (require security – quy định bảo mật):

Bắt buộc dùng IPSEC cho giao tiếp mạng. Có thể dùng chính sách này cho cả máy chủ và trạm làm việc. Nếu chính sách được xác lập, không cho phép giao tiếp không bảo mật.

***Thương lượng một liên kết bảo mật (A security sociation)***

Cả hai máy tính tiến hành thương lượng bảo mật cần phải có những chính sách bổ sung. Nếu 2 máy có thể thương lượng thành công, IPSEC sẽ được sử dụng. Nếu thương lượng không thành công do bất đồng về chính sách, 2 máy có thể không tiếp tục giao tiếp hoặc chấp nhận giao tiếp không an toàn.

Ví dụ về cách thức hoạt động của các chính sách giữa 2 máy tính A và B:

- Máy A yêu cầu ESP cho các giao tiếp HTTP, máy B yêu cầu AH cho HTTP, như vậy 2 máy sẽ không thể thương lượng một liên kết bảo mật.
- Giao thức xác thực Kerberos là phương thức xác thực mặc định, được các máy trong cùng hoạt động cây thư mục (Active directory forest) sử dụng, nếu một trong 2 máy không cùng AD Forest, thì không thể thương lượng được phương thức bảo mật. Tương tự, khi máy A dùng Kerberos, máy B dùng Certificates (chứng chỉ) làm phương thức xác thực lưu lượng IP, thương lượng cũng sẽ không được thiết lập.

***4.4.2.3. Ưu điểm và hạn chế của IPSec***

**1/. Ưu điểm của IPSec**

IPSec là cách tổng quan nhất để cung cấp các dịch vụ bảo mật trên mạng Internet, nó có 1 số đặc điểm sau:

- IPSec là một giải pháp tổng thể. Nó có thể bảo vệ bất kỳ giao thức nào chạy trên IP và bất kỳ môi trường nào mà IP chạy trên nó. Đồng thời còn bảo vệ được nhiều giao thức ứng dụng chạy trên nhiều môi trường phức tạp.
- IPSec có thể cung cấp một số dịch vụ bảo mật ở mức nền, không gây ảnh hưởng đến người dùng.
- IPSec là cơ chế chung để bảo mật IP. Nó không cung cấp chức năng bảo mật thư nhưng có thể mã hóa thư, nên nó đảm bảo kẻ tấn công không thể "hiểu" được thư dù có đánh cắp hay đọc trộm.
- IPSec có thể cung cấp cùng một cơ chế bảo mật cho bất kỳ cái gì được truyền qua IP.
- Người dùng sử dụng IPSec không phải làm bất kỳ một thao tác nào. Thậm chí họ có thể không cần biết là có sự tồn tại của nó. Mọi việc thiết lập và cài đặt đều do người quản trị làm.

**2./ Hạn chế của IPSec**

Bên cạnh những ưu điểm trên IPSec còn có những hạn chế mà nó không làm được:

- IPSec không an toàn nếu sử dụng ở hệ thống không an toàn. Nếu hệ thống không an toàn (hệ thống có máy bị phá hoại) thì việc sử dụng IPSec cũng không đảm bảo an toàn như sử dụng nó với 1 hệ thống bình thường.
- IPSec không bảo mật ở dạng End to End. Nó không đảm bảo tính bảo mật giữa những người sử dụng cuối, bất kỳ người sử dụng nào với quyền thích hợp trên một máy bất kỳ, lưu trữ gói tin nhận được đều có thể biết được nội dung của nó.
- IPSec xác thực máy, không xác thực người dùng.
- IPSec không ngăn chặn được kiểu tấn công từ chối dịch vụ.
- IPSec không chặn được các phân tích truyền thông mạng, là việc cố gắng tìm tri thưc từ các gói tin mà không quan tâm đến nội dung của nó. Các phân tích dựa trên những gì nhìn thấy được ở các Header chưa được mã hóa của các gói tin đã mã hóa, địa chỉ máy cổng nguồn hoặc đích, độ dài gói tin,…

## 4.5. PHÒNG TRÁNH TẤN CÔNG CƠ SỞ DỮ LIỆU

CSDL là một đối tượng hàng đầu cần phải được bảo vệ. Trong thời đại bùng nổ thông tin như hiện nay, CSDL luôn là đối tượng nhòm ngó của các đối thủ cạnh tranh, các đối tượng tấn công,... Các cá nhân, công ty, tổ chức, quốc gia luôn coi trọng việc bảo mật CSDL.

### 4.5.1. Giải pháp phòng tránh tấn công cơ sở dữ liệu

- Lựa chọn phần cứng, nơi lưu trữ đảm bảo an toàn cho dữ liệu.
- Lựa chọn phần mềm phù hợp để lưu trữ dữ liệu.
- Có giải pháp dự phòng khi có sự cố xảy ra (Ví dụ: Đối với server lưu trữ dữ liệu, cần tách biệt với Server cung cấp dịch vụ, và có Server lưu trữ dự phòng khi Server chính xảy ra lỗi sẽ có Server thay thế ngay,…).
- Luôn cập nhật các bản vá lỗi, thông tin về nguy cơ bị tấn công để có biện pháp phòng tránh trước.
- Giới hạn quyền trong cơ sở dữ liệu đối với cả nhà quản trị và người dùng. Chỉ cấp quyền đủ để áp dụng nhu cầu của mỗi đối tượng. Quyền càng bị hạn chế, thiệt hại càng ít.
- Cần phải sử dụng những công cụ mã hoá mạnh kết hợp với những giải pháp khác về bảo vệ an ninh hệ thống mạng, chống virus xâm nhập.

Dữ liệu bị mất, bị lộ là do không có một giải pháp mã hoá nào triệt để. Ta có thể tham khảo giải pháp Tricrytion (giải pháp bảo vệ dữ liệu 3 lớp của hãng ERUCES).

Giải pháp này sẽ tiến hành mã hoá CSDL như sau:

+ Mã hoá bản thân CSDL sử dụng các Khoá
+ Mã hoá Khoá
+ Mã hoá quan hệ giữa khoá và CSDL

Hệ thống cần có những server riêng cho từng thành phần CSDL, Khoá và mối liên kết.

Đây là một giải pháp mang tính triệt để cao, có thể được tích hợp vào nhiều hệ thống khác nhau và được sự hỗ trợ của nhiều hãng phần mềm hàng đầu như Microsoft, Sun,…

### 4.5.2. Ví dụ phòng tránh tấn công lỗ hổng SQL Injection attack

Để phòng tránh các nguy cơ có thể xảy ra, nên bảo vệ các câu truy vấn SQL bằng cách kiểm soát chặt chẽ tất cả các dữ liệu nhập vào nhận được từ đối tượng Request (Request, Request.QueryString, Request.Form, Request.Cookies, và Request.ServerVariables).

- Trong trường hợp dữ liệu nhập vào là chuỗi, như trong ví dụ phần **3.2.3. Tấn công cơ sở dữ liệu**, lỗi xuất phát từ việc có dấu nháy đơn trong dữ liệu. Để tránh điều này, thay thế các dấu nháy đơn bằng hàm Replace để thay thế bằng 2 dấu nháy đơn:

```
p_strUsername = Replace (Request.Form ("txtUsername"), "'", "''")
p_strPassword = Replace (Request.Form ("txtPassword"), "'", "''")
```

- Trong trường hợp dữ liệu nhập vào là số, lỗi xuất phát từ việc thay thế một giá trị được tiên đoán là dữ liệu số bằng chuỗi chứa câu lệnh SQL bất hợp pháp. Để tránh điều này, đơn giản ta kiểm tra dữ liệu có đúng kiểu hay không:

```
p_lngID = CLng(Request("ID"))
```

Như vậy, nếu người dùng truyền vào một chuỗi, hàm này sẽ trả về lỗi ngay lập tức.

Ngoài ra để tránh các nguy cơ từ SQL Injection attack, nên chú ý loại bỏ bất kì thông tin kĩ thuật nào chứa trong thông điệp chuyển xuống cho người dùng khi ứng dụng có lỗi. Các thông báo lỗi thông thường tiết lộ các chi tiết kĩ thuật có thể cho phép kẻ tấn công biết được điểm yếu của hệ thống. Cuối cùng, để giới hạn mức độ của SQL Injection attack, nên kiểm soát chặt chẽ và giới hạn quyền xử lí dữ liệu đến tài khoản người dùng mà ứng dụng web đang sử dụng. Các ứng dụng thông thường nên tránh dùng đến các quyền như dbo hay "sa" (quyền quản trị hệ thống).

# *Chương 5.* THỬ NGHIỆM CHƯƠNG TRÌNH

## 5.1. VÍ DỤ PHÒNG TRÁNH TẤN CÔNG MẠNG

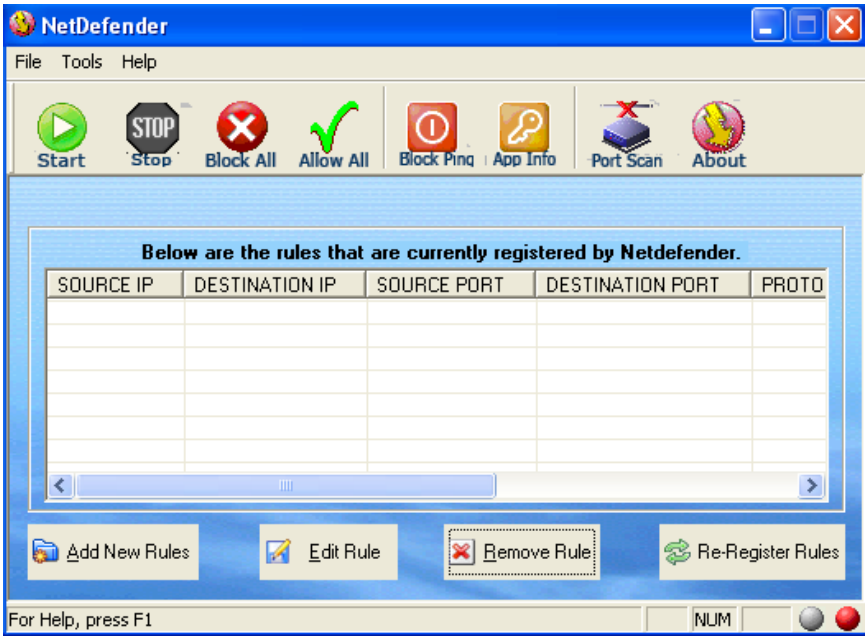
*** Mô tả:** Ví dụ phòng tránh tấn công máy tính cá nhân qua mạng sử dụng chương trình NetDefrnder, bằng cách lập luật cho phép (allow) hoặc ngăn chặn (deny) các cổng (port) hoặc giao thức TCP hoặc UDP.

*** Yêu cầu hệ thống:**

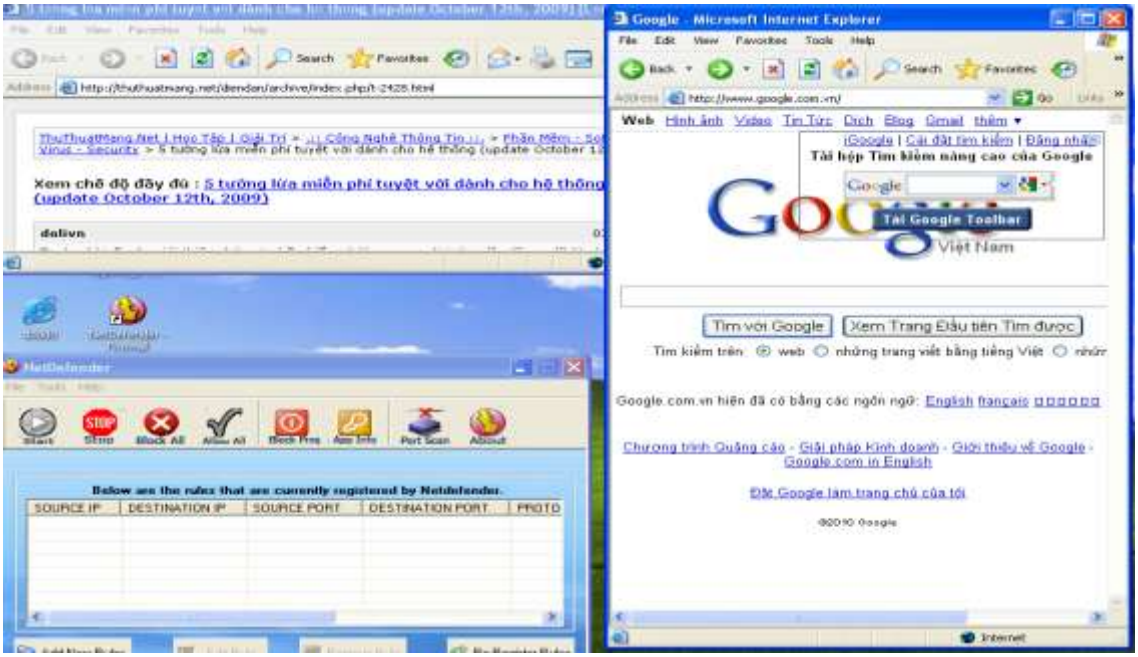
- Chương trình chạy trên HĐH WindowXP - SP2.
- Cần bổ sung thêm thư viện: mfc71.dll, msvcr71.dll, mfc71u.dll, msvcp71.dll.
- Chương trình viết bằng Visual studio solution.

*** Giao diện chụp lại khi chạy kiểm thử chương trình:**

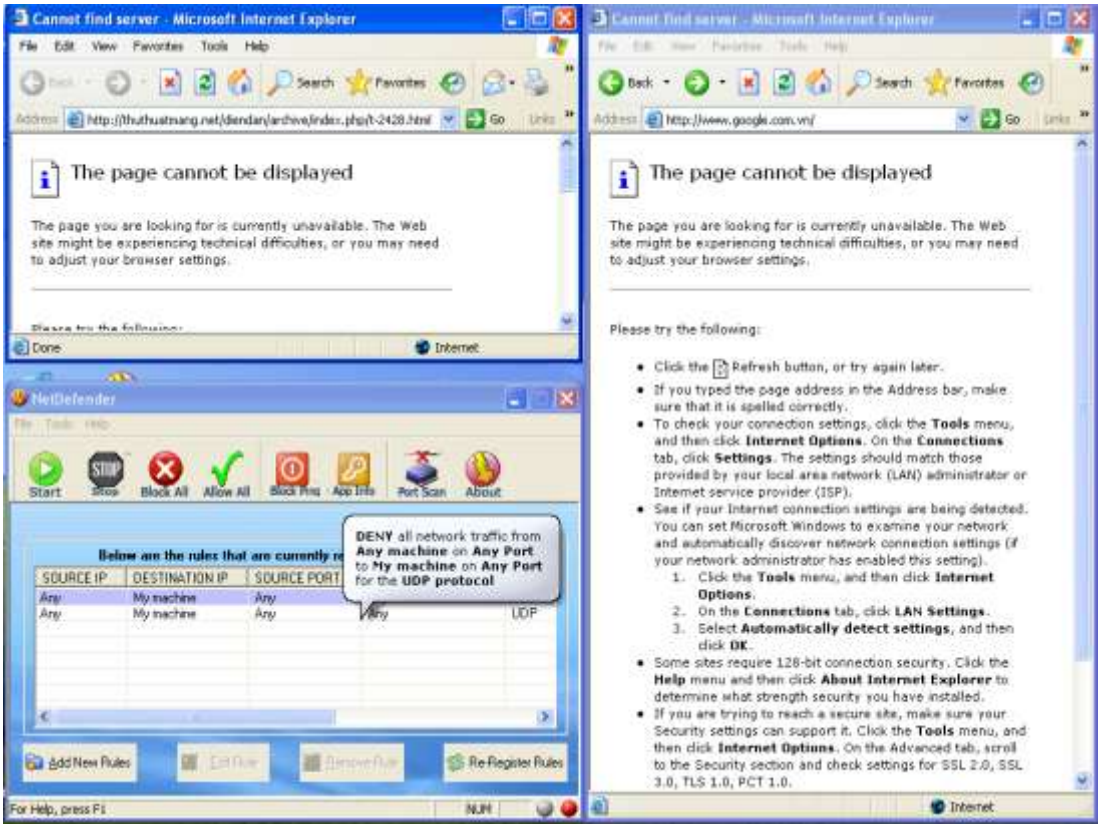
### 5.1.1. Giao diện chính



### 5.1.2. Hình ảnh khi chưa lập luật




### 5.1.3. Kết quả chạy chương trình khi lập luật cấm tất cả các cổng và giao thức



## 5.2. VIẾT CHƯƠNG TRÌNH "VÁ LỖ HỔNG" TRONG ARP

### 5.2.1. Giao thức phân giải địa chỉ ARP

#### *5.2.1.1. Khái niệm*

Giao thức phân giải địa chỉ ARP (ARP – Address Resolution Protocol), phân giải từ địa chỉ tầng mạng thành địa chỉ tầng liên kết dữ liệu. Thường dùng để chuyển đổi từ địa chỉ IP sang địa chỉ Ethernet.

#### *5.2.1.2. Nguy cơ an ninh của ARP*

ARP không cung cấp cơ chế để các thiết bị phân biệt các gói tin giả mạo, vì thế kỹ thuật ARP Spoofing - lừa gạt (hay ARP Poisoning - đầu độc) cho phép kẻ tấn công lừa nạn nhân gửi các gói tin IP đến một nơi mà kẻ tấn công chọn trước. Khi các gói tin đến, kẻ tấn công toàn quyền xử lý, từ đọc lén đến thay đổi nội dung của dữ liệu, hoặc đơn giản là vứt bỏ gói tin.

#### *5.2.1.3. Minh họa chi tiết tình huống xảy ra*

Khi nút mạng A nào đó cần kết nối với nút mạng B thì nó phải biết rõ địa chỉ vật lý của nút mạng B. Để làm việc này đã có giao thức phân giải địa chỉ ARP, nó thực hiện một ánh xạ giữa địa chỉ logic (địa chỉ mạng IP) và địa chỉ vật lý (địa chỉ phần cứng MAC) bên trong các đoạn mạng.

Quá trình: Máy A gửi yêu cầu kết nối có chứa địa chỉ IP của máy cần tìm tới tất cả các máy trong mạng cục bộ, chỉ có một máy B nhận ra địa chỉ IP của mình, B sẽ gửi địa chỉ MAC của nó cho máy A.

Tuy vậy có thể phát sinh tình huống: Khi máy A gửi yêu cầu kết nối có chứa địa chỉ IP của máy cần tìm, máy B có địa chỉ IP như vậy nhưng đang bị lỗi (vắng mặt, hỏng hóc,... ) không thể trả lời. Nhân cơ hội này, máy C nào đó giả mạo máy B, gửi địa chỉ MAC của nó cho máy A.. Một kết nối giữa A và C được hình thành, nhưng A vẫn đinh ninh rằng mình đang kết nối với B. Điều này rất nguy hiểm. Vì có thể A sẽ làm lộ thông tin quan trọng mà A muốn trao đổi với B.

### 5.2.2. Giải pháp

Sau khi A có địa chỉ vật lý máy cần liên kết (B), A phải chứng thực xem đối phương có đúng là người cần liên lạc không, A có thể kiểm tra bằng một trong các cách sau:

- Kiểm tra chữ ký.
- Kiểm tra vân tay.
- Kiểm tra giọng nói.

### 5.2.3. Thực nghiệm thực hiện giao thức ARP an toàn

Thực hiện giao thức ARP một cách an toàn (Chọn giải pháp kiểm tra chữ ký), thực hiện theo các bước sau:

1/. Người muốn kết nối (A) tới 1 nút mạng nào đó thông báo địa chỉ IP (Địa chỉ quảng bá) của nút mạng mà A cần kết nối trên mạng (B).

2/. Nếu B có địa chỉ IP như vậy thì gửi địa chỉ cứng (Địa chỉ MAC - Medium Access Control) của mình cho A.

3/. A kiểm tra chữ ký của người cung cấp địa chỉ cứng, bằng cách kiểm tra chữ ký của người đó.

4/. Sau khi kiểm tra (bằng khoá công khai của B), nếu chữ ký đúng là của B thì tiến hành kết nối, nếu sai thì dừng kết nối.

### 5.2.4. Xây dựng chương trình ký và kiểm tra chữ ký (RSA)

A gửi cho B (đối tượng cần liên kết) một văn bản yêu cầu B ký vào văn bản. Sau đó, A tiến hành kiểm tra chữ ký với khóa công khai của B. Nếu đúng thì tiếp tục trao đổi, sai thì dừng trao đổi.

#### *5.2.3.1. Sơ đồ ký RSA*

Sơ đồ chữ ký RSA được cho bởi bộ 5: (P,A,K,S,V).

Trong đó:

P là một tập hữu hạn các văn bản có thể có.A là một tập chữ ký có thể có.

$P = A = Z_n$ với n là tích của 2 số nguyên lớn p và q ($n = p * q$).

K là tập các cặp khoá $K = (K_1, K_2)$.

$K_1 = a$ là khoá bí mật dành cho việc ký.

$K_2 = (n , b)$ là khoá công khai dùng cho việc kiểm thử chữ ký.

Với $a , b \in Z_n$ và thoả mãn : $a * b \equiv 1 (\mathrm{mod} \varnothing (n))$.

S là tập hữu hạn các hàm ký, trong S có một thuật toán ký:

$Sig_{k1}: P \rightarrow A$ với $Sig_{k1}( x ) = x^a \bmod n$.

V là tập hữu hạn các hàm kiểm thử, trong V có một thuật toán kiểm thử:

$Ver_{k2} : P \times A$ với $ver_{k2}( x , y ) = \{đúng, sai\}$

$Ver_{k2} ( x, y ) = \{đúng\} \Leftrightarrow x \equiv y^b ( \mathrm{mod}\ n)$. ($x \in P, \forall y \in A$)

Rút gọn: $\forall x \in P$ và mọi chữ ký $y \in A$, ta có:

$Ver_{k2} (x, y) = \{đúng\} \Leftrightarrow y = Sig_{k1} ( x )$.

**1/. Tạo khoá**

Chọn 2 số nguyên tố lớn p và q.

Tính: $n = p * q$

Tính: $\varnothing (n) = (p – 1) * (q – 1)$

Chọn b sao cho: $\gcd(b, \varnothing (n))=1$

Tính a sao cho: $a * b = 1 (\mathrm{mod} \varnothing (n))$

Khi đó ta được cặp khóa K ($K_1, K_2$) với:

$K_1 = (a)$ là khoá bí mật dành cho việc ký.

$K_2 = (n, b)$ là khoá công khai dùng cho việc kiểm thử chữ ký.

**2/. Ký số**

Ký trên bản rõ x.

Chữ kí là y: $y = Sig_{k1}(x) = x^{a} \pmod n$, a là khoá bí mật.

**3/. Kiểm thử chữ ký**

Sau khi nhận $(x, y, K_2)$.

Trong đó: x là bản rõ, y là chữ ký và khoá công khai $K_2$ (n, b).

Tiến hành kiểm tra bằng hàm kiểm thử: $Ver_{k2}(x, y) = \{đúng, sai\}$

$Ver_{k2}(x, y) = \{đúng\} \Leftrightarrow x \equiv y^{b} \pmod n$. $(x \in P, \forall y \in A)$

Ngược lại là sai.

***5.2.3.2. Ví dụ***

**1/. Tạo khoá**

Chọn p = 3, q = 7.

n = p * q = 21

$\varnothing(n) = (p - 1) * (q - 1) = 12$

Chọn b =5 thoả mãn: $gcd(b, \varnothing(n)) = gcd(5, 12) = 1$

a = 5 thoả mãn: $a * b = 1 \pmod{\varnothing(n)} \Leftrightarrow 5 * 5 = 25$; $25 \bmod 12 = 1$

Khi đó ta được cặp khóa K $(K_1, K_2)$ là:

$K_1$ = (5) là khoá bí mật để ký.

$K_2$ = (21, 5) là khoá công khai dùng để kiểm thử chữ ký.

**2/. Ký số**

Ký trên bản rõ x = 12

Chữ kí là y = 3: $y = Sig_5(12) = 12^5 \pmod{21}$, (a = 5 là khoá bí mật).

**3/. Kiểm thử chữ ký**

Khoá công khai $K_2$ (21, 5).

- Tiến hành kiểm tra bằng hàm kiểm thử: $Ver_{(21, 5)}(12, 3) = \{đúng, sai\}$ ?

  Xét: $3^5 = 243$; $243 \pmod{21} = 12 = x$

  $\Rightarrow Ver_{(21, 5)}(12, 3) = \{Đúng\}$

- Giả sử kiểm tra với khoá công khai (21, 2)

  Ta có: $3^2 = 9$; $9 \pmod{21} = 9 \neq 12$

  $\Rightarrow Ver_{(21, 2)}(12, 3) = \{Sai\}$

### *5.2.3.3. Chương trình ký và kiểm tra chữ ký (RSA)*

**1/ Yêu cầu cấu hình của hệ thống**

* Phần cứng (cấu hình tối thiểu):

Bộ nhớ ổ cứng: 20 GB

Bộ nhớ ram: 128 MB

Tốc độ máy tối thiểu: 1 GHz

* Phần mềm:

Hệ điều hành:Linux, Window,…

Ngôn ngữ lập trình: Turbo C 3.0

**2/. Các hàm chính trong chương trình**

**a) Hàm main**

```
  void main()
{
  clrscr();
  textbackground (010111);
  int Chon;
  long p,q,a,b;
  long n,fi;
  long x,y;

 while(1)
 {
 clrscr();
 cout<<"                                  ";
 cout<<endl<<"  --------- Chu ky RSA -----------";
 cout<<endl<<"                                  ";
 cout<<endl<<"            [1] Ky                ";
 cout<<endl<<"                                  ";
 cout<<endl<<"            [2] Kiem tra chu ky   ";
 cout<<endl<<"                                  ";
 cout<<endl<<"            [0] Thoat             ";
 cout<<endl<<"                                  ";
 cout<<endl<<"Chon: ";cin>>Chon;
```

```
switch(Chon)
 {
 case 1:
  while(1)
  {
   cout<<"Nhap so nguyen to p = ";cin>>p;
   if(!SoNguyenTo(p)) cout<<"p khong phai la so nguyen to. Moi nhap
lai!"<<endl;
   else break;
  }

  while(1)
  {
    cout<<"Nhap so nguyen to q = ";cin>>q;
    if(!SoNguyenTo(q)) cout<<"q khong phai la so nguyen to. Moi nhap
lai!"<<endl;
    else break;
  }

  n = p * q;
  fi = (p-1) * (q-1);

  while(1)
  {
    cout<<"Nhap so ngau nhien b = ";cin>>b;
    if(gcd(b,fi) !=1) cout<<"b khong thoa man: gcd(b,fi) = 1. Moi nhap
lai"<<endl;
    else break;
  }

  a = SoNghichDao(b,fi);

  cout<<endl<<"Khoa bi mat de ky K' = ("<<a<<")";
  cout<<endl<<"Khoa cong khai de kiem thu: K\" = ("<<n<<","<<b<<")";

  while(1)
  {
   cout<<endl<<"Nhap ban ma X = ";cin>>x;
   if(x<1 || x>=n-1) cout<<"X khong thoa man: 1 < x < n-1";
   else break;
  }

  y = Sig(x,a,n);
  cout<<"Chu ky RSA cua ban ma X: "<<y;
  getch();
  break;
```

```
case 2:
    cout<<"Nhap ban ma X = ";cin>>x;
    cout<<"Nhap chu ky tuong ung: ";cin>>y;
    cout<<"Nhap khoa cong khai: "<<endl;
    cout<<"n = ";cin>>n;
    cout<<"b = ";cin>>b;
    if(Ver(x,b,n,y)) cout<<"Chu ky dung";
    else cout<<"Chu ky sai!";
    getch();
    break;
  case 0:return;
  }
 }
}
```

**b) Hàm ký**

```
long Sig(long x,long a,long n)
{
 long t;
 t = x;
 for(long i=1;i<=a-1;i++)
   t=(t*x)%n;
 return t;
}
```

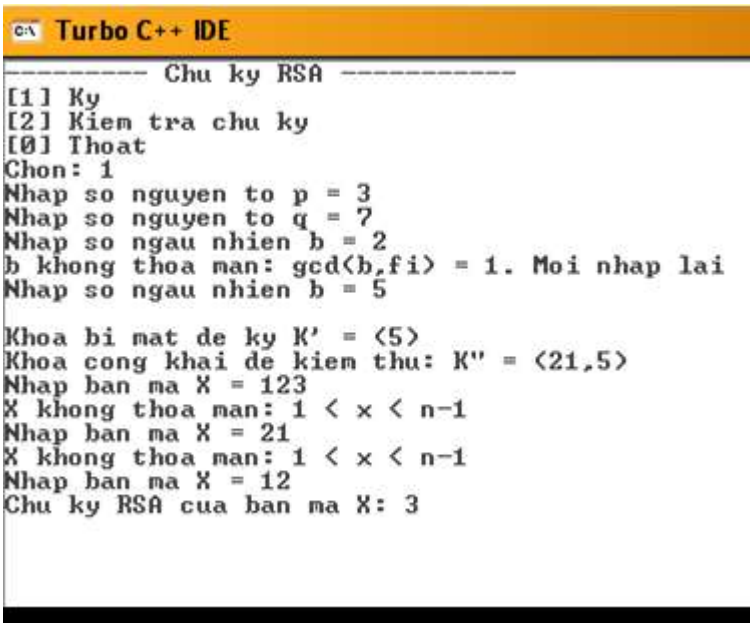
**c) Hàm kiểm thử**

```
int Ver(long x,long b,long n,long y)
{
  long Y;
  Y = Sig(y,b,n);
  if (Y==x) return 1;
  else return 0;
}
```

### 3/. Giao diện chương trình

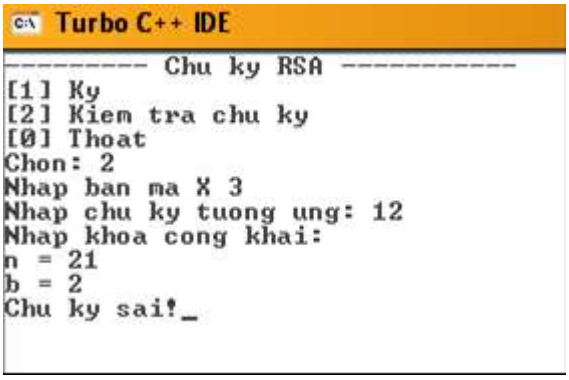
### Giao diện chính:

**Giao diện ký số RSA:**

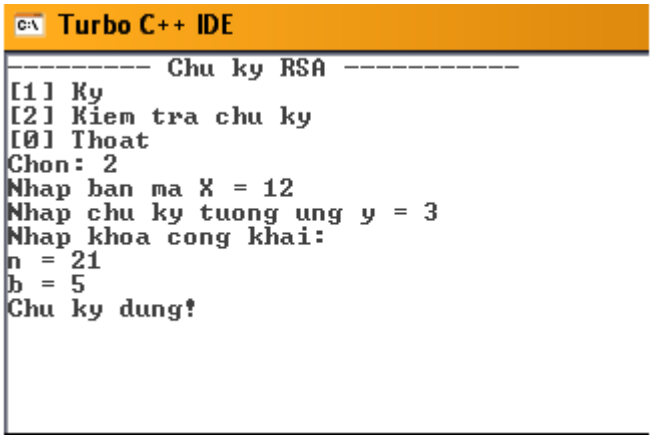



**Giao diện kiểm thử chữ ký**

***Kiểm thử sai:***




***Kiểm thử đúng:***



# KẾT LUẬN

----o0o----

Trong quá trình thực hiện đề tài, với sự tận tình hướng dẫn, giúp đỡ của thầy hướng dẫn **PGS.TS. Trịnh Nhật Tiến,** kết hợp với kiến thức thu được trong quá trình học tập tại trường. Sau quá trình tìm hiểu, nghiên cứu các vấn đề liên quan đến đề tài: "Tìm hiểu một số dạng tấn công hệ thống thông tin và phòng chống bằng xử lý các lỗ hổng thiếu an ninh" đúng thời hạn, em đã thu được các kết quả sau:

**1/. Tìm hiểu và nghiên cứu lý thuyết**

- Tìm hiểu một số loại "lỗ hổng" thiếu an ninh trong hệ thống thông tin (thông qua mạng máy tính, hệ điều hành, cơ sở dữ liệu,...).
- Tìm hiểu một số dạng "tấn công" hệ thống thông tin thông qua "lỗ hổng".
- Nghiên cứu phương pháp phòng tránh "tấn công" bằng xử lý các "lỗ hổng".

**2/. Thử nghiệm chương trình**

Chỉ ra một ví dụ cụ thể để phòng tránh "lỗ hổng".

Trong đó thử nghiệm chương trình ký số để xác thực, xử lý "lỗ hổng".

**Hải phòng, tháng 7/2010**

. Sinh viên thực hiện

TRẦN THỊ THỦY

# TÀI LIỆU THAM KHẢO


1. Giáo trình An toàn và bảo mật thông tin, Tác giả PGS.TS Trịnh Nhật Tiến
2. Luận văn tốt nghiệp, Đoàn Thị Hà, Giáo viên hướng dẫn PGS.TS Trịnh Nhật Tiến
3. Luận văn tốt nghiệp, Vũ Thị Tố Uyên, Giáo viên hướng dẫn TS Hồ Văn Canh.
4. Bảo mật trên mạng bí quyết và giải pháp, tổng hợp biên dịch VN - GUIDE, nhà xuất bản thống kê.
5. Tham khảo tài liệu tại các trang Web

   http://www.quantrimang.com.vn

   www.technet.com.vn/

   http://vi.wikipedia.org/

   http://tuonglua.net/

   http://netdefender.codeplex.com/releases/view/6988

   …….