BỘ LAO ĐỘNG - THƯƠNG BINH VÀ XÃ HỘI
TỔNG CỤC DẠY NGHỀ

GIÁO TRÌNH

Môn học: An toàn mạng

NGHỀ QUẢN TRỊ MẠNG MÁY TÍNH

TRÌNH ĐỘ: CAO ĐẲNG NGHỀ

(Ban hành kèm theo Quyết định số:120/QĐ-TCDN ngày 25 tháng 02 năm 2013 của Tổng cục trưởng Tổng cục dạy nghề)



Hà Nôi, năm 2013

TUYÊN BỐ BẢN QUYỀN:

Tài liệu này thuộc loại sách giáo trình nên các nguồn thông tin có thể được phép dùng nguyên bản hoặc trích dùng cho các mục đích về đào tạo và tham khảo.

Mọi mục đích khác mang tính lệch lạc hoặc sử dụng với mục đích kinh doanh thiếu lành mạnh sẽ bị nghiêm cấm.

MÃ TÀI LIỆU: **MH28**

LỜI GIỚI THIỆU

Trong những năm qua, dạy nghề đã có những bước tiến vượt bậc cả về số lượng và chất lượng, nhằm thực hiện nhiệm vụ đào tạo nguồn nhân lực kỹ thuật trực tiếp đáp ứng nhu cầu xã hội. Cùng với sự phát triển của khoa học công nghệ trên thế giới, lĩnh vực Công nghệ thông tin nói chung và ngành Quản trị mạng ở Việt Nam nói riêng đã có những bước phát triển đáng kể.

Chương trình dạy nghề Quản trị mạng đã được xây dựng trên cơ sở phân tích nghề, phần kỹ năng nghề được kết cấu theo các mô đun môn học. Để tạo điều kiện thuận lợi cho các cơ sở dạy nghề trong quá trình thực hiện, việc biên soạn giáo trình theo các mô đun đào tạo nghề là cấp thiết hiện nay.

Môn học 28: An toàn mạng là môn học đào tạo chuyên môn nghề được biên soạn theo hình thức tích hợp lý thuyết và thực hành. Trong quá trình thực hiện, nhóm biên soạn đã tham khảo nhiều tài liệu An toàn mạng trong và ngoài nước, kết hợp với kinh nghiệm trong thực tế.

Mặc dầu có rất nhiều cố gắng, nhưng không tránh khỏi những khiếm khuyết, rất mong nhận được sự đóng góp ý kiến của độc giả để giáo trình được hoàn thiện hơn.

Xin chân thành cảm ơn

Hà Nội, ngày 25 tháng 02 năm 2013

Tham gia biên soạn

1.Chủ biên Nguyễn Đình Liêm

2. Nguyễn Như Thành

3. Trần Nguyễn Quốc Dũng

MỤC LỤC

LỜI GIỚI THIỆU 1
MỤC LỤC 2
CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN VÀ BẢO MẬT THÔNG TIN 6
1. Các khái niệm chung 7
1.1. Đối tượng tấn công mạng (Intruder) 7
1.2. Các lỗ hổng bảo mật 7
2. Nhu cầu bảo vệ thông tin 7
2.1. Nguyên nhân 7
2.2 Bảo vệ dữ liệu 7
2.3. Bảo vệ tài nguyên sử dụng trên mạng 8
2.4. Bảo bệ danh tiếng của cơ quan 8
Bài tập thực hành của học viên 8
CHƯƠNG 2: MÃ HÓA THÔNG TIN 9
1. Cơ bản về mã hoá (Cryptography) 9
1.1. Tại sao cần phải sử dụng mã hoá 9
1.2. Nhu cầu sử dụng kỹ thuật mã hoá 9
1.3. Quá trình mã hoá và giải mã như sau: 11
2. Độ an toàn của thuật toán 11
3. Phân loại các thuật toán mã hoá 12
3.1. Mã hoá cổ điển: 12
3.2. Mã hoá đối xứng: 13
Bài tập thực hành của học viên 17
CHƯƠNG 3: NAT (Network Address Translation) 18
1. Giới thiệu: 18
2. Các kỹ thuật NAT cổ điển: 18
2.1. NAT tĩnh 19
2.2. NAT động 19
3. NAT trong Window server 22
Bài tập thực hành của học viên 23
CHƯƠNG 4: BẢO VỆ MẠNG BẰNG TƯỜNG LỬA 31
1. Các kiểu tấn công 31
1.1. Tấn công trực tiếp 31
1.2. Nghe trộm 31
1.3. Giả mạo địa chỉ 31
1.4. Vô hiệu hoá các chức năng của hệ thống 31
1.5. Lỗi của người quản trị hệ thống 32
1.6. Tấn công vào yếu tố con người 32
2. Các mức bảo vệ an toàn 32
3. Internet Firwall 33
3.1. Định nghĩa 33
3.2. Chức năng chính 33
3.3. Cấu trúc 34

3.4. Các thành phần của Firewall và cơ chế hoạt động..... 34
3.5. Những hạn chế của firewall 37
3.6. Các ví dụ firewall..... 38
Bài tập thực hành của học viên 41
CHƯƠNG 5: DANH SÁCH ĐIỀU KHIỂN TRUY CẬP.....42
Giới thiệu..... 42
1. Định nghĩa danh sách truy cập..... 43
2. Nguyên tắc hoạt động của Danh sách truy cập 44
2.1 Tổng quan về các lệnh trong Danh sách truy cập 46
2.2. Danh sách truy cập chuẩn trong mạng TCP/IP..... 47
Bài tập thực hành của học viên 50
CHƯƠNG 6 : VIRUS VÀ CÁCH PHÒNG CHỐNG.....55
1. Giới thiệu tổng quan về virus tin học..... 55
2. Cách thức lây lan – phân loại..... 56
Bài tập thực hành của học viên 67
TÀI LIỆU THAM KHẢO..... 72

MÔN HỌC : AN TOÀN MẠNG

Mã số của môn học: MH 28

Vị trí, tính chất, ý nghĩa và vai trò của môn học:

- Vị trí: Môn học được bố trí sau khi sinh viên học xong môn, mô đun: Mạng máy tính và Quản trị mạng 1.
- Tính chất: Là môn học chuyên môn nghề.
- Ý nghĩa và vai trò: Đây là môn học cơ sở ngành của ngành quản trị mạng, cung cấp cho sinh viên các kiến thức cơ bản về bảo mật hệ thống mạng để làm nền tản cho việc bảo mật giải quyết các vấn đề cần thiết.

Mục tiêu của môn học:

- Xác định được các thành phần cần bảo mật cho một hệ thống mạng;
- Trình bày được các hình thức tấn công vào hệ thống mạng;
- Mô tả được cách thức mã hoá thông tin;
- Trình bày được quá trình NAT trong hệ thống mạng;
- Xác định được khái niệm về danh sách truy cập;
- Mô tả được nguyên tắc hoạt động của danh sách truy cập;
- Liệt kê được danh sách truy cập trong chuẩn mạng TCP/IP;
- Phân biệt được các loại virus thông dụng và cách phòng chống virus;
- Bố trí làm việc khoa học đảm bảo an toàn cho người và phương tiện học tập.

Nội dung chính của môn học:

Số TT	Tên chương mục	Thời gian			
		Tổng số	Lý thuyết	Thực hành Bài tập	Kiểm tra* (LT hoặcTH)
I	**Tổng quan về an toàn và bảo mật thông tin** Các khái niệm chung Nhu cầu bảo vệ thông tin	**5**	**5**	**0**	
II	**Mã hóa thông tin** Cơ bản về mã hoá (Cryptography) Độ an toàn của thuật toán Phân loại các thuật toán mã hoá	**10**	**5**	**5**	
III	**NAT** Giới thiệu Các kỹ thuật NAT cổ điển NAT trong window server	**10**	**5**	**4**	**1**
IV	**Bảo vệ mạng bằng tường lửa** Các kiểu tấn công	**11**	**5**	**5**	**1**

	Các mức bảo vệ an toàn Internet Firewall				
V	**Danh sách điều khiển truy cập** Khái niệm về danh sách truy cập Nguyên tắc hoạt động của danh sách truy cập	**17**	**7**	**9**	**1**
VI	**Virus và cách phòng chống** Giới thiệu tổng quan về virus Cách thức lây lan và phân loại virus Ngăn chặn sự xâm nhập virus	**7**	**3**	**4**	
	Cộng	**60**	**30**	**27**	**3**

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN VÀ BẢO MẬT THÔNG TIN
Mã chương: **MH 26-01**

Giới thiệu:

Bảo mật là một trong những lĩnh vực mà hiện nay giới công nghệ thông tin khá quan tâm. Một khi Internet ra đời và phát triển, nhu cầu trao đổi thông tin trở nên cần thiết. Mục tiêu của việc nối mạng là làm cho mọi người có thể sử dụng chung tài nguyên từ những vị trí địa lý khác nhau. Cũng chính vì vậy mà các tài nguyên cũng rất dễ dàng bị phân tán, dẫn đến một điều hiển nhiên là chúng sẽ bị xâm phạm, gây mất mát dữ liệu cũng như các thông tin có giá trị. Càng giao thiệp rộng thì càng dễ bị tấn công, đó là một quy luật. Từ đó, vấn đề bảo vệ thông tin cũng đồng thời xuất hiện, bảo mật ra đời.

Tất nhiên, mục tiêu của bảo mật không chỉ nằm gói gọn trong lĩnh vực bảo vệ thông tin mà còn nhiều phạm trù khác như kiểm duyệt web, bảo mật internet, bảo mật http, bảo mật trên các hệ thống thanh toán điện tử và giao dịch trực tuyến….

Mọi nguy cơ trên mạng đều là mối nguy hiểm tiềm tàng. Từ một lổ hổng bảo mật nhỏ của hệ thống, nhưng nếu biết khai thác và lợi dụng với tầng suất cao và kỹ thuật hack điêu luyện thì cũng có thể trở thành tai họa.

Theo thống kê của tổ chức bảo mật nổi tiếng **CERT** (Computer Emegancy Response Team) thì số vụ tấn công ngày càng tăng. Cụ thể năm 1989 có khoản 200 vụ, đến năm 1991 có 400 vụ, đến năm 1994 thì con số này tăng lên đến mức 1330 vụ, và sẽ còn tăng mạnh trong thời gian tới.

Như vậy, số vụ tấn công ngày càng tăng lên với mức độ chóng mặt. Điều này cũng dễ hiểu, vì một thực thể luôn tồn tại hai mặt đối lập nhau. Sự phát triển mạnh mẽ của công nghệ thông tin và kỹ thuật sẽ làm cho nạn tấn công, ăn cắp, phá hoại trên internet bùng phát mạnh mẽ.

Internet là một nơi cực kỳ hỗn loạn. Mọi thông tin mà bạn thực hiện truyền dẫn đều có thể bị xâm phạm, thậm chí là công khai. Bạn có thể hình dung internet là một phòng họp, những gì được trao đổi trong phòng họp đều được người khác nghe thấy. Với internet thì những người này không thấy mặt nhau, và việc nghe thấy thông tin này có thể hợp pháp hoặc là không hợp pháp.

Tóm lại, internet là một nơi mất an toàn. Mà không chỉ là internet các loại mạng khác, như mạng LAN, đến một hệ thống máy tính cũng có thể bị xâm phạm. Thậm chí, mạng điện thoại, mạng di động cũng không nằm ngoài cuộc. Vì thế chúng ta nói rằng, phạm vi của bảo mật rất lớn, nói không còn gói gọn trong một máy tính một cơ quan mà là toàn cầu.

Mục tiêu:

- Trình bày được các hình thức tấn công vào hệ thống mạng;
- Xác định được các thành phần của một hệ thống bảo mật;
- Thực hiện các thao tác an toàn với máy tính.

Nội dung chính:

1. Các khái niệm chung

Mục tiêu:

- Mô tả được các đối tượng tấng công hệ thống mạng ;

- Xác định được các lỗ hổng bảo mật.

1.1. Đối tượng tấn công mạng (Intruder)

Là những cá nhân hoặc các tổ chức sử dụng các kiến thức về mạng và các công cụ phá hoại (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 mạng trái phép.

Một số đối tượng tấn công mạng là:

- **Hacker:** Là những kẻ xâm nhập vào mạng trái phép bằng cách sử dụng các công cụ phá mật khẩu hoặc khai thác các điểm yếu của các thành phần truy nhập trên hệ thống.
- **Masquerader:** Là những 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 ...
- **Eavesdropping:** Là những đối tượng nghe trộm thông tin trên mạng, sử dụng các công cụ sniffer; sau đó dùng các công cụ phân tích và debug để lấy được các thông tin có giá trị. Những đối tượng tấn công mạng có thể nhằm nhiều mục đích khác nhau: như ăn cắp những thông tin có giá trị về kinh tế, phá hoại hệ thống mạng có chủ định, hoặc cũng có thể chỉ là những hành động vô ý thức, thử nghiệm các chương trình không kiểm tra cẩn thận ...

1.2. Các lỗ hổng bảo mật

Các lỗ hổng bảo mật là những điểm yếu kém trên hệ thống hoặc ẩn chứa trong một dịch vụ mà dựa vào đó kẻ tấn công có thể xâm nhập trái phép để thực hiện các hành động phá hoại hoặc chiếm đoạt tài nguyên bất hợp pháp.

Nguyên nhân gây ra những lỗ hổng bảo mật là khác nhau: có thể do lỗi của bản thân hệ thống, hoặc phần mềm cung cấp, hoặc do người quản trị yếu kém không hiểu sâu sắc các dịch vụ cung cấp ...

Mức độ ảnh hưởng của các lỗ hổng là khác nhau. Có những lỗ hổng chỉ ảnh hưởng tới chất lượng dịch vụ cung cấp, có những lỗ hổng ảnh hưởng nghiêm trọng tới toàn bộ hệ thống ...

2. Nhu cầu bảo vệ thông tin

Mục tiêu:

- Trình bày được các nhu cầu cần bảo vệ trên hệ thống mạng

2.1. Nguyên nhân

Tài nguyên đầu tiên mà chúng ta nói đến chính là dữ liệu. Đối với dữ liệu, chúng ta cần quan tâm những yếu tố sau:

2.2 Bảo vệ dữ liệu

Những thông tin lưu trữ trên hệ thống máy tính cần được bảo vệ do các yêu cầu sau:

- Bảo mật: những thông tin có giá trị về kinh tế, quân sự, chính sách vv... cần được bảo vệ và không lộ thông tin ra bên ngoài.

- Tính toàn vẹn: Thông tin không bị mất mát hoặc sửa đổi, đánh tráo.

- Tính kịp thời: Yêu cầu truy nhập thông tin vào đúng thời điểm cần thiết.

Trong các yêu cầu này, thông thường yêu cầu về bảo mật được coi là yêu cầu số 1 đối với thông tin lưu trữ trên mạng. Tuy nhiên, ngay cả khi những thông tin này không được giữ bí mật, thì những yêu cầu về tính toàn vẹn cũng rất quan trọng. Không một cá nhân, một tổ chức nào lãng phí tài nguyên vật chất và thời gian để lưu trữ những thông tin mà không biết về tính đúng đắn của những thông tin đó.

2.3. Bảo vệ tài nguyên sử dụng trên mạng

Trên thực tế, trong các cuộc tấn công trên Internet, kẻ tấn công, sau khi đã làm chủ được hệ thống bên trong, có thể sử dụng các máy này để phục vụ cho mục đích của mình như chạy các chương trình dò mật khẩu người sử dụng, sử dụng các liên kết mạng sẵn có để tiếp tục tấn công các hệ thống khác.

2.4. Bảo bệ danh tiếng của cơ quan

Một phần lớn các cuộc tấn công không được thông báo rộng rãi, và một trong những nguyên nhân là nỗi lo bị mất uy tín của cơ quan, đặc biệt là các công ty lớn và các cơ quan quan trọng trong bộ máy nhà nước. Trong trường hợp người quản trị hệ thống chỉ được biết đến sau khi chính hệ thống của mình được dùng làm bàn đạp để tấn công các hệ thống khác, thì tổn thất về uy tín là rất lớn và có thể để lại hậu quả lâu dài.

Bài tập thực hành của học viên

Câu 1: Trình bày các đối tượng tấng công hệ thống mạng

Câu 2: Đối với dữ liệu, chúng ta cần quan tâm những yếu tố nào?

CHƯƠNG 2: MÃ HÓA THÔNG TIN
Mã chương: MH26-02

Mục tiêu:

- Liệt kê và phân biệt được các kiểu mã hóa dữ liệu;
- Áp dụng được việc mã hóa và giải mã với một số phương pháp cơ bản;
- Mô tả về hạ tầng ứng dụng khóa công khai;
- Thực hiện các thao tác an toàn với máy tính.

1. Cơ bản về mã hoá (Cryptography)

Mục tiêu:

- Trình bày được nhu cầu sử dụng mã hóa;

- Mô tả được quá trình mã hóa và giải mã.

Những điều căn bản về mã hoá

Khi bắt đầu tìm hiểu về mã hoá, chúng ta thường đặt ra những câu hỏi chẳng hạn như là: Tại sao cần phải sử dụng mã hoá ? Tại sao lại có quá nhiều thuật toán mã hoá ?...

1.1. Tại sao cần phải sử dụng mã hoá

Thuật toán Cryptography đề cập tới nghành khoa học nghiên cứu về mã hoá và giải mã thông tin. Cụ thể hơn là nghiên cứu các cách thức chuyển đổi thông tin từ dạng rõ (clear text) sang dạng mờ (cipher text) và ngược lại. Đây là một phương pháp hỗ trợ rất tốt cho trong việc chống lại những truy cập bất hợp pháp tới dữ liệu được truyền đi trên mạng, áp dụng mã hoá sẽ khiến cho nội dung thông tin được truyền đi dưới dạng mờ và không thể đọc được đối với bất kỳ ai cố tình muốn lấy thông tin đó.

1.2. Nhu cầu sử dụng kỹ thuật mã hoá

Không phải ai hay bất kỳ ứng dụng nào cũng phải sử dụng mã hoá. Nhu cầu về sử dụng mã hoá xuất hiện khi các bên tham gia trao đổi thông tin muốn bảo vệ các tài liệu quan trọng hay gửi chúng đi một cách an toàn. Các tài liệu quan trọng có thể là: tài liệu quân sự, tài chính, kinh doanh hoặc đơn giản là một thông tin nào đó mang tính riêng tư.

Như chúng ta đã biết, Internet hình thành và phát triển từ yêu cầu của chính phủ Mỹ nhằm phục vụ cho mục đích quân sự. Khi chúng ta tham gia trao đổi thông tin, thì Internet là môi trường không an toàn, đầy rủi ro và nguy hiểm, không có gì đảm bảo rằng thông tin mà chúng ta truyền đi không bị đọc trộm trên đường truyền. Do đó, mã hoá được áp dụng như một biện pháp nhằm giúp chúng ta tự bảo vệ chính mình cũng như những thông tin mà chúng ta gửi đi. Bên cạnh đó, mã hoá còn có những ứng dụng khác như là bảo đảm tính toàn vẹn của dữ liệu.

Tại sao lại có quá nhiều thuật toán mã hoá

Theo một số tài liệu thì trước đây tính an toàn, bí mật của một thuật toán phụ thuộc vào phương thức làm việc của thuật toán đó. Nếu như tính an toàn của một thuật toán chỉ dựa vào sự bí mật của thuật toán đó thì thuật toán đó là một thuật toán hạn chế (Restricted Algrorithm). Restricted Algrorithm có tầm quan trọng trong lịch sử nhưng không còn phù hợp trong thời đại ngày nay. Giờ đây,

nó không còn được mọi người sử dụng do mặt hạn chế của nó: mỗi khi một user rời khỏi một nhóm thì toàn bộ nhóm đó phải chuyển sang sử dụng thuật toán khác hoặc nếu người đó người trong nhóm đó tiết lộ thông tin về thuật toán hay có kẻ phát hiện ra tính bí mật của thuật toán thì coi như thuật toán đó đã bị phá vỡ, tất cả những user còn lại trong nhóm buộc phải thay đổi lại thuật toán dẫn đến mất thời gian và công sức.

Hệ thống mã hoá hiện nay đã giải quyết vấn đề trên thông qua khoá (Key) là một yếu tố có liên quan nhưng tách rời ra khỏi thuật toán mã hoá. Do các thuật toán hầu như được công khai cho nên tính an toàn của mã hoá giờ đây phụ thuộc vào khoá. Khoá này có thể là bất kì một giá trị chữ hoặc số nào. Phạm vi không gian các giá trị có thể có của khoá được gọi là Keyspace . Hai quá trình mã hoá và giải mã đều dùng đến khoá. Hiện nay, người ta phân loại thuật toán dựa trên số lượng và đặc tính của khoá được sử dụng.

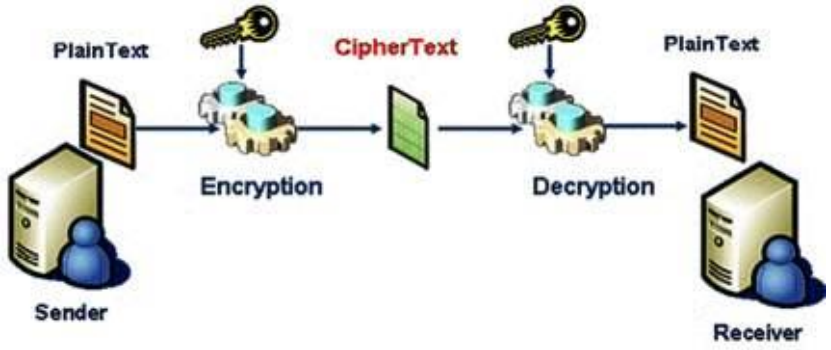
Nói đến mã hoá tức là nói đến việc che dấu thông tin bằng cách sử dụng thuật toán. Che dấu ở đây không phải là làm cho thông tin biến mất mà là cách thức chuyển từ dạng tỏ sang dạng mờ. Một thuật toán là một tập hợp của các câu lệnh mà theo đó chương trình sẽ biết phải làm thế nào để xáo trộn hay phục hồi lại dữ liệu. Chẳng hạn một thuật toán rất đơn giản mã hoá thông điệp cần gửi đi như sau:

Bước 1: Thay thế toàn bộ chữ cái “e” thành số “3”

Bước 2: Thay thế toàn bộ chữ cái “a” thành số “4”

Bước 3: Đảo ngược thông điệp

Trên đây là một ví dụ rất đơn giản mô phỏng cách làm việc của một thuật toán mã hoá. Sau đây là các thuật ngữ cơ bản nhất giúp chúng ta nắm được các khái niệm:



Hinh1: Minh hoạ quá trình mã hóa và giải mã

Sender/Receiver: Người gửi/Người nhận dữ liệu

- Plaintext (Cleartext): Thông tin trước khi được mã hoá. Đây là dữ liệu ban đầu ở dạng rõ
- Ciphertext: Thông tin, dữ liệu đã được mã hoá ở dạng mờ
- Key: Thành phần quan trọng trong việc mã hoá và giải mã
- CryptoGraphic Algorithm: Là các thuật toán được sử dụng trong việc mã hoá hoặc giải mã thông tin
- CryptoSystem: Hệ thống mã hoá bao gồm thuật toán mã hoá, khoá, Plaintext, Ciphertext

Kí hiệu chung: P là thông tin ban đầu, trước khi mã hoá. E() là thuật toán mã hoá. D() là thuật toán giải mã. C là thông tin mã hoá. K là khoá.

1.3. Quá trình mã hoá và giải mã như sau:

- Quá trình mã hoá được mô tả bằng công thức: EK(P)=C
- Quá trình giải mã được mô tả bằng công thức: DK(C)=P

Bên cạnh việc làm thế nào để che dấu nội dung thông tin thì mã hoá phải đảm bảo các mục tiêu sau:

a. Confidentiality (Tính bí mật): Đảm bảo dữ liệu được truyền đi một cách an toàn và không thể bị lộ thông tin nếu như có ai đó cố tình muốn có được nội dung của dữ liệu gốc ban đầu. Chỉ những người được phép mới có khả năng đọc được nội dung thông tin ban đầu.

b. Authentication (Tính xác thực): Giúp cho người nhận dữ liệu xác định được chắc chắn dữ liệu mà họ nhận là dữ liệu gốc ban đầu. Kẻ giả mạo không thể có khả năng để giả dạng một người khác hay nói cách khác không thể mạo danh để gửi dữ liệu. Người nhận có khả năng kiểm tra nguồn gốc thông tin mà họ nhận được.

c. Integrity (Tính toàn vẹn): Giúp cho người nhận dữ liệu kiểm tra được rằng dữ liệu không bị thay đổi trong quá trình truyền đi. Kẻ giả mạo không thể có khả năng thay thế dữ liệu ban đầu băng dữ liệu giả mạo

d. Non-repudation (Tính không thể chối bỏ): Người gửi hay người nhận không thể chối bỏ sau khi đã gửi hoặc nhận thông tin.

2. Độ an toàn của thuật toán

Mục tiêu:

- Trình bày được các thuật toán mã hóa

Nguyên tắc đầu tiên trong mã hoá là "Thuật toán nào cũng có thể bị phá vỡ". Các thuật toán khác nhau cung cấp mức độ an toàn khác nhau, phụ thuộc vào độ phức tạp để phá vỡ chúng. Tại một thời điểm, độ an toàn của một thuật toán phụ thuộc:

- Nếu chi phí hay phí tổn cần thiết để phá vỡ một thuật toán lớn hơn giá trị của thông tin đã mã hóa thuật toán thì thuật toán đó tạm thời được coi là an toàn.
- Nếu thời gian cần thiết dùng để phá vỡ một thuật toán là quá lâu thì thuật toán đó tạm thời được coi là an toàn.
- Nếu lượng dữ liệu cần thiết để phá vỡ một thuật toán quá lơn so với lượng dữ liệu đã được mã hoá thì thuật toán đó tạm thời được coi là an toàn

Từ tạm thời ở đây có nghĩa là độ an toàn của thuật toán đó chỉ đúng trong một thời điểm nhất định nào đó, luôn luôn có khả năng cho phép những người phá mã tìm ra cách để phá vỡ thuật toán. Điều này chỉ phụ thuộc vào thời gian, công sức, lòng đam mê cũng như tính kiên trì bên bỉ. Càng ngày tốc độ xử lý của CPU càng cao, tốc độ tính toán của máy tính ngày càng nhanh, cho nên không ai dám khẳng định chắc chắn một điều rằng thuật toán mà mình xây dựng sẽ an toàn mãi mãi. Trong lĩnh vực mạng máy tính và truyền thông luôn luôn tồn tại hai phe đối lập với nhau những người chuyên đi tấn công, khai thác lỗ hổng của hệ thống và những người chuyên phòng thủ, xây dựng các qui trình bảo vệ hệ thống. Cuộc chiến giữa hai bên chẳng khác gì một cuộc chơi trên bàn cờ, từng

bước đi, nước bước sẽ quyết định số phận của mỗi bên. Trong cuộc chiến này, ai giỏi hơn sẽ dành được phần thắng. Trong thế giới mã hoá cũng vậy, tất cả phụ thuộc vào trình độ và thời gian…sẽ không ai có thể nói trước được điều gì. Đó là điểm thú vị của trò chơi.

3. Phân loại các thuật toán mã hoá

Có rất nhiều các thuật toán mã hoá khác nhau. Từ những thuật toán được công khai để mọi người cùng sử dụng và áp dụng như là một chuẩn chung cho việc mã hoá dữ liệu; đến những thuật toán mã hoá không được công bố. Có thể phân loại các thuật toán mã hoá như sau:

Phân loại theo các phương pháp:

- Mã hoá cổ điển (Classical cryptography)
- Mã hoá đối xứng (Symetric cryptography)
- Mã hoá bất đối xứng(Asymetric cryptography)
- Hàm băm (Hash function)

Phân loại theo số lượng khoá:

- Mã hoá khoá bí mật (Private-key Cryptography)
- Mã hoá khoá công khai (Public-key Cryptography)

3.1. Mã hoá cổ điển:

Xuất hiện trong lịch sử, các phương pháp này không dùng khoá. Thuật toán đơn giản và dễ hiểu. Những từ chính các phương pháp mã hoá này đã giúp chúng ta tiếp cận với các thuật toán mã hoá đối xứng được sử dụng ngày nay. Trong mã hoá cổ điển có 02 phương pháp nổi bật đó là:

- Mã hoá thay thế (Substitution Cipher):

Là phương pháp mà từng kí tự (hay từng nhóm kí tự) trong bản rõ (Plaintext) được thay thế bằng một kí tự (hay một nhóm kí tự) khác để tạo ra bản mờ (Ciphertext). Bên nhận chỉ cần đảo ngược trình tự thay thế trên Ciphertext để có được Plaintext ban đầu.

Các hệ mật mã cổ điển- Hệ mã hóa thay thế(Substitution Cipher)

Chọn một hoán vị p: Z26 → Z26 làm khoá.

VD:

Mã hoá

ep(a)=X

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
d	**l**	**r**	**y**	**v**	**o**	**h**	**e**	**z**	**x**	**w**	**p**	**t**

n	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
S	**F**	**L**	**R**	**C**	**V**	**M**	**U**	**E**	**K**	**J**	**D**	**I**

Giải mã:

dp(A)=d

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
d	**l**	**r**	**y**	**v**	**o**	**h**	**e**	**z**	**x**	**w**	**p**	**t**

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	g	f	j	q	n	m	u	s	k	a	c	i

Bảng rõ "nguyenthanhnhut"
Mã hóa "SOUDHSMGXSGSGUM"

- Mã hoá hoán vị (Transposition Cipher):

Bên cạnh phương pháp mã hoá thay thế thì trong mã hoá cổ điển có một phương pháp khác nữa cũng nổi tiếng không kém, đó chính là mã hoá hoán vị. Nếu như trong phương pháp mã hoá thay thế, các kí tự trong Plaintext được thay thế hoàn toàn bằng các kí tự trong Ciphertext, thì trong phương pháp mã hoá hoán vị, các kí tự trong Plaintext vẫn được giữ nguyên, chúng chỉ được sắp xếp lại vị trí để tạo ra Ciphertext. Tức là các kí tự trong Plaintext hoàn toàn không bị thay đổi bằng kí tự khác.

Mã hoán vị - Permutation Cipher

Chuyển đổi vị trí bản thân các chữ cái trong văn bản gốc từng khối m chữ cái.

Mã hoá:

$e\pi(x1, \ldots, xm) = (x\pi(1), \ldots, x\pi m))$.

Giải mã:

$d\pi(y1, \ldots, ym) = (y\pi'(1), \ldots, y\pi'(m))$.

Trong đó, π: Z26 $\rightarrow$Z26 là một hoán vị, $\pi' := \pi$-1 là nghịch đảo của π.

Hoán vị

x	1	2	3	4	5	6
Π(x)	3	5	1	6	4	2

x	1	2	3	4	5	6
Π^{-1}(x)	3	6	1	5	2	4

"shesellsseashellsbytheseashore".
shesel | lsseas | hellsb | ythese | ashore
EESLSH | SALSES | LSHBLE | HSYEET | HRAEOS
"EESLSHSALSESLSHBLEHSYEETHRAEOS".

3.2. Mã hoá đối xứng:

Ở phần trên, chúng ta đã tìm hiểu về mã hoá cổ điển, trong đó có nói rằng mã hoá cổ điển không dùng khoá. Nhưng trên thực nếu chúng ta phân tích một cách tổng quát, chúng ta sẽ thấy được như sau:

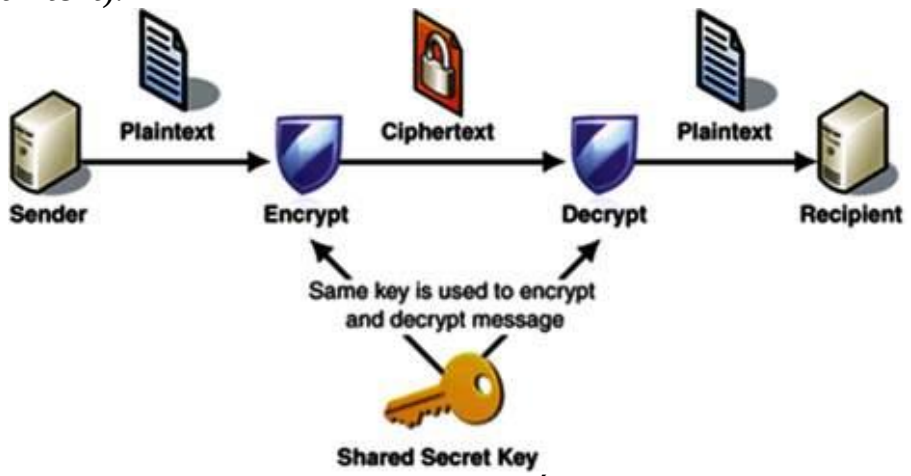
- Mã hoá cổ điển có sử dụng khoá. Bằng chứng là trong phương pháp Ceaser Cipher thì khoá chính là phép dịch ký tự, mà cụ thể là phép dịch 3 ký tự. Trong phương pháp mã hoá hoán vị thì khóa nằm ở số hàng hay số cột mà chúng ta qui định. Khoá này có thể được thay đổi tuỳ theo mục đích mã hoá của chúng ta, nhưng nó phải nằm trong một phạm vi cho phép nào đó.

- Để dùng được mã hoá cổ điển thì bên mã hoá và bên giải mã phải thống nhất với nhau về cơ chế mã hoá cũng như giải mã. Nếu như không có công việc này thì hai bên sẽ không thể làm việc được với nhau.

Mã hoá đối xứng còn có một số tên gọi khác như Secret Key Cryptography (hay Private Key Cryptography), sử dụng cùng một khoá cho cả hai quá trình mã hoá và giải mã.

Quá trình thực hiện như sau:

Trong hệ thống mã hoá đối xứng, trước khi truyền dữ liệu, 2 bên gửi và nhận phải thoả thuận về khoá dùng chung cho quá trình mã hoá và giải mã. Sau đó, bên gửi sẽ mã hoá bản rõ (Plaintext) bằng cách sử dụng khoá bí mật này và gửi thông điệp đã mã hoá cho bên nhận. Bên nhận sau khi nhận được thông điệp đã mã hoá sẽ sử dụng chính khoá bí mật mà hai bên thoả thuận để giải mã và lấy lại bản rõ (Plaintext).



Hình 2: Mã hóa đối xứng

Hình vẽ trên chính là quá trình tiến hành trao đổi thông tin giữa bên gửi và bên nhận thông qua việc sử dụng phương pháp mã hoá đối xứng. Trong quá trình này, thì thành phần quan trọng nhất cần phải được giữ bí mật chính là khoá. Việc trao đổi, thoả thuận về thuật toán được sử dụng trong việc mã hoá có thể tiến hành một cách công khai, nhưng bước thoả thuận về khoá trong việc mã hoá và giải mã phải tiến hành bí mật. Chúng ta có thể thấy rằng thuật toán mã hoá đối xứng sẽ rất có lợi khi được áp dụng trong các cơ quan hay tổ chức đơn lẻ. Nhưng nếu cần phải trao đổi thông tin với một bên thứ ba thì việc đảm bảo tính bí mật của khoá phải được đặt lên hàng đầu.

Mã hoá đối xứng có thể được phân thành 02 loại:

- **Loại thứ nhất** tác động trên bản rõ theo từng nhóm bits. Từng nhóm bits này được gọi với một cái tên khác là khối (Block) và thuật toán được áp dụng gọi là **Block Cipher**. Theo đó, từng khối dữ liệu trong văn bản ban đầu được thay thế bằng một khối dữ liệu khác có cùng độ dài. Đối với các thuật toán ngày nay thì kích thước chung của một Block là 64 bits.
- **Loại thứ hai** tác động lên bản rõ theo từng bit một. Các thuật toán áp dụng được gọi là **Stream Cipher**. Theo đó, dữ liệu của văn bản được mã hoá từng bit một. Các thuật toán mã hoá dòng này có tốc độ nhanh hơn các thuật toán mã hoá khối và nó thường được áp dụng khi lượng dữ liệu cần mã hoá chưa biết trước.

Một số thuật toán nổi tiếng trong mã hoá đối xứng là: DES, Triple DES(3DES), RC4, AES…

+ **DES:** viết tắt của Data Encryption Standard. Với DES, bản rõ (Plaintext) được mã hoá theo từng khối 64 bits và sử dụng một khoá là 64 bits, nhưng thực tế thì chỉ có 56 bits là thực sự được dùng để tạo khoá, 8 bits còn lại dùng để kiểm tra tính chẵn, lẻ. DES là một thuật toán được sử dụng rộng rãi nhất trên thế giới. Hiện tại DES không còn được đánh giá cao do kích thước của khoá quá nhỏ 56 bits, và dễ dàng bị phá vỡ.

+ **Triple DES (3DES):** 3DES cải thiện độ mạnh của DES bằng việc sử dụng một quá trình mã hoá và giải mã sử dụng 3 khoá. Khối 64-bits của bản rõ đầu tiên sẽ được mã hoá sử dụng khoá thứ nhất. Sau đó, dữ liệu bị mã hóa được giải mã bằng việc sử dụng một khoá thứ hai. Cuối cùng, sử dụng khoá thứ ba và kết quả của quá trình mã hoá trên để mã hoá.

C = EK3(DK2(EK1(P)))

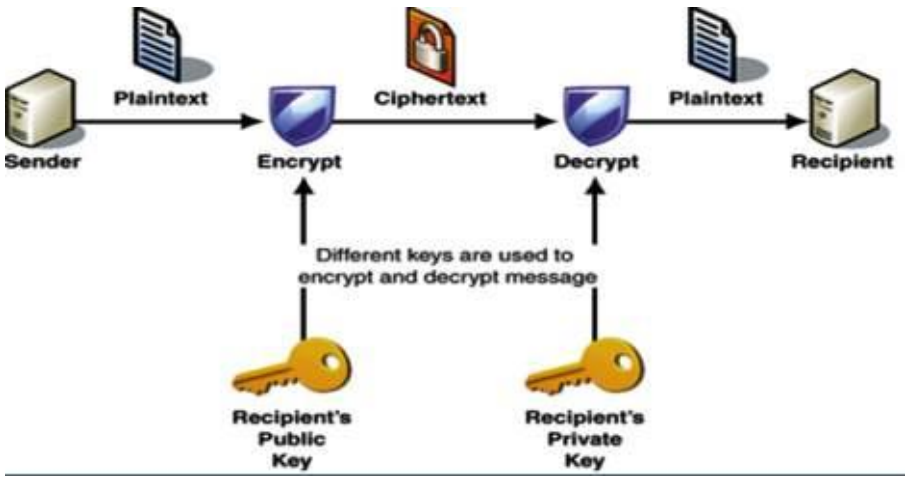
P = DK1(EK2(DK3(C)))

+ **AES**: Viết tắt của Advanced Encryption Standard, được sử dụng để thay thế cho DES. Nó hỗ trợ độ dài của khoá từ 128 bits cho đến 256 bits.

3.3. Mã hoá bất đối xứng:

Hay còn được gọi với một cái tên khác là mã hoá khoá công khai (Public Key Cryptography), nó được thiết kế sao cho khoá sử dụng trong quá trình mã hoá khác biệt với khoá được sử dụng trong quá trình giải mã. Hơn thế nữa, khoá sử dụng trong quá trình giải mã không thể được tính toán hay luận ra được từ khoá được dùng để mã hoá và ngược lại, tức là hai khoá này có quan hệ với nhau về mặt toán học nhưng không thể suy diễn được ra nhau. Thuật toán này được gọi là mã hoá công khai vì khoá dùng cho việc mã hoá được công khai cho tất cả mọi người. Một người bất kỳ có thể dùng khoá này để mã hoá dữ liệu nhưng chỉ duy nhất người mà có khoá giải mã tương ứng mới có thể đọc được dữ liệu mà thôi. Do đó trong thuật toán này có 2 loại khoá: Khoá để mã hoá được gọi là Public Key, khoá để giải mã được gọi là Private Key.

Mã hoá khoá công khai ra đời để giải quyết vấn đề về quản lý và phân phối khoá của các phương pháp mã hoá đối xứng. Hình minh hoạ ở trên cho chúng ta thấy được quá trình truyền tin an toàn dựa vào hệ thống mã hoá khoá công khai. Quá trình truyền và sử dụng mã hoá khoá công khai được thực hiện như sau:



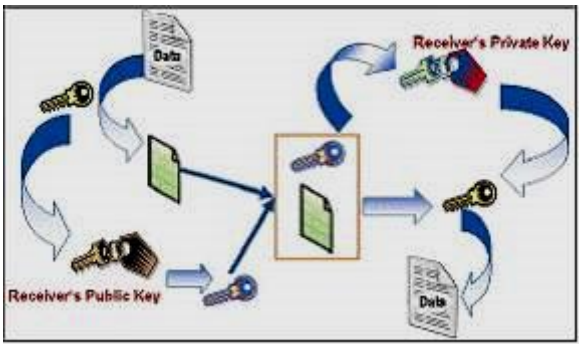
Hình 3: mã hóa bất đối xứng

- Bên gửi yêu cầu cung cấp hoặc tự tìm khoá công khai của bên nhận trên một server chịu trách nhiệm quản lý khoá.
- Sau đó hai bên thống nhất thuật toán dùng để mã hoá dữ liệu, bên gửi sử dụng khoá công khai của bên nhận cùng với thuật toán đã thống nhất để mã hoá thông tin được gửi đi.
- Khi nhận được thông tin đã mã hoá, bên nhận sử dụng khoá bí mật của mình để giải mã và lấy ra thông tin ban đầu.

Vậy là với sự ra đời của Mã hoá công khai thì khoá được quản lý một cách linh hoạt và hiệu quả hơn. Người sử dụng chỉ cần bảo vệ Private key. Tuy nhiên nhược điểm của Mã hoá khoá công khai nằm ở tốc độ thực hiện, nó chậm hơn rất nhiều so với mã hoá đối xứng. Do đó, người ta thường kết hợp hai hệ thống mã hoá khoá đối xứng và công khai lại với nhau và được gọi là Hybrid Cryptosystems. Một số thuật toán mã hoá công khai nổi tiếng: Diffle-Hellman, RSA,…

3.4. Hệ thống mã hoá khoá lai (Hybrid Cryptosystems):

Trên thực tế hệ thống mã hoá khoá công khai chưa thể thay thế hệ thống mã hoá khoá bí mật được, nó ít được sử dụng để mã hoá dữ liệu mà thường dùng để mã hoá khoá. Hệ thống mã hoá khoá lai ra đời là sự kết hợp giữa tốc độ và tính an toàn của hai hệ thống mã hoá ở trên. Dưới đây là mô hình của hệ thống mã hoá lai:



Hình 4: Mã hóa công khai

Nhìn vào mô hình chúng ta có thể hình dung được hoạt động của hệ thống mã hoá này như sau:

- Bên gửi tạo ra một khoá bí mật dùng để mã hoá dữ liệu. Khoá này còn được gọi là Session Key.
- Sau đó, Session Key này lại được mã hoá bằng khoá công khai của bên nhận dữ liệu.
- Tiếp theo dữ liệu mã hoá cùng với Session Key đã mã hoá được gửi đi tới bên nhận.
- Lúc này bên nhận dùng khoá riêng để giải mã Session Key và có được Session Key ban đầu.
- Dùng Session Key sau khi giải mã để giải mã dữ liệu.

Như vậy, hệ thống mã hoá khoá lai đã tận dụng tốt được các điểm mạnh của hai hệ thống mã hoá ở trên đó là: tốc độ và tính an toàn. Điều này sẽ làm hạn chế bớt khả năng giải mã của tin tặc.

*** Một số ứng dụng của mã hoá trong Security**

Một số ứng dụng của mã hoá trong đời sống hằng ngày nói chung và trong lĩnh vực bảo mật nói riêng.

Đó là:

- Securing Email - Bảo mật hệ thông mail
- Authentication System – Hệ thống xác thực
- Secure E-commerce – Bảo mật trong thương mại điện tử
- Virtual Private Network – Mạng riêng ảo
- Wireless Encryption – Mã hóa hệ thống Wireless

Bài tập thực hành của học viên

Câu 1: Tại sao cần phải sử dụng mã hoá thông tin?

Câu 2: Trình bày phương pháp mã hóa cổ điển

Câu 3: Trình bày phương pháp mã hóa dối xứng

Bài 1:

Thực hiện với hệ mã hóa thay thế(Substitution Cipher) mã hóa và giải mã với bảng rõ sau:

“ khoacongnghethongtin”

“sinhviencongnghethongtin”

Bài 2:

Thực hiện với hệ Mã hoá hoán vị (**Permutation Cipher**) mã hóa và giải mã với bảng rõ sau:

“ khoacongnghethongtin”

“sinhviencongnghethongtin”

CHƯƠNG 3: NAT (Network Address Translation)

Mã chương: MH26-03

Mục tiêu:

- Trình bày được quá trình NAT của một hệ thống mạng;
- Trình bày được NAT tĩnh và NAT động;
- Thiết lập cấu hình NAT trên Windows server;
- Thực hiện các thao tác an toàn với hệ thống mạng.

1. Giới thiệu:

Mục tiêu:

- Trình bày được quá trình NAT của một hệ thống mạng;

- Trình bày được NAT tĩnh và NAT động.

Lúc đầu, khi NAT được phát minh ra nó chỉ để giải quyết cho vấn đề thiếu IP. Vào lúc ấy không ai nghĩ rằng NAT có nhiều hữu ích và có lẽ nhiều ứng dụng trong những vấn đề khác của NAT vẫn chưa được tìm thấy.

Trong ngữ cảnh đó nhiều người đã cố gắng tìm hiểu vai trò của NAT và lợi ích của nó trong tương lai. Khi mà IPv6 được hiện thực thì nó không chỉ giải quyết cho vấn đề thiếu IP. Qua nhiều cuộc thử nghiệm họ đã chỉ ra rằng viêc chuyển hoàn toàn qua IPv6 thì không có vấn đề gì và mau lẹ nhưng để giải quyết những vấn đề liên qua giữa IPv6 và IPv4 là khó khăn. Bởi vậy có khả năng IPv4 sẽ là giao thức chủ yếu cho Internet và Intranet … lâu dài hơn những gì họ mong muốn.

Trước khi giải thích vai trò của NAT ngày nay và trong tương lai, những người này muốn chỉ ra sự khác nhau về phạm vi của NAT được sủ dụng vào ngày đó. Sự giải thích sẽ đưa ra một cái nhìn tổng quan và họ không khuyên rằng làm thế nào và nên dùng loại NAT nào. Sau đây chỉ là giới thiệu và phân loại các NAT phần chi tiết sẽ được thảo luận và đề cập trong chương sau khi hiện thực NAT là một layd out.

Phần trình bày được chia làm 2 phần :

- Phần đầu được đặt tên là CLASSIC NAT nó là các kỹ thuật NAT vào những thời kỳ sơ khai (đầu những năm 90) được trình bày chi tiết trong RFC 1931. Ứng dụng của nó chủ yếu giải quyết cho bài toán thiếu IP trên Internet.
- Phần hai trình bày những kỹ thuật NAT được tìm ra gần đây và ứng dụng trong nhiều mục đích khác.

2. Các kỹ thuật NAT cổ điển:

Nói về NAT chúng ta phải biết rằng có 2 cách là tĩnh và động. Trong trường hợp đầu thì sự phân chia IP là rõ ràng còn trường hợp sau thì ngược lại. Với NAT tĩnh thì một IP nguồn luôn được chuyển thành chỉ một IP đích mà thôi trong bất kỳ thời gian nào. Trong khi đó NAT động thì IP này là thay đổi trong các thời gian và trong các kết nối khác nhau.

Trong phần này chúng ta định nghĩa :

m: số IP cần được chuyển đổi (IP nguồn)

n: số IP sẵn có cho việc chuyển đổi (IP NATs hay gọi là IP đích)

2.1. NAT tĩnh

Yêu cầu m, n >= 1; m = n (m, n là số tự nhiên)

Với cơ chế IP tĩnh chúng ta có thể chuyển đổi cùng một số lượng các IP nguồn và đích. Trường hợp đặc biệt là khi cả 2 chỉ chứa duy nhất một IP ví dụ netmask là 255.255.255.255. Cách thức hiện thực NAT tĩnh thì dễ dàng vì toàn bộ cơ chế dịch địa chỉ được thực hiện bởi một công thức đơn giản:

Địa chỉ đích = Địa chỉ mạng mới OR (địa chỉ nguồn AND (NOT netmask))

Không có thông tin về trạng thái kết nối. Nó chỉ cần tìm các IP đích thích hợp là đủ. Các kết nối từ bên ngoài hệ thống vào bên trong hệ thống thì chỉ khác nhau về IP vì thế cơ chế NAT tĩnh thì hầu như hoàn toàn trong suốt.

Ví dụ một rule cho NAT tĩnh:

Dịch toàn bộ IP trong mạng 138.201.148.0 đến mạng có địa chỉ là 94.64.15.0, netmask là 255.255.255.0 cho cả hai mạng.

Dưới đây là mô tả việc dịch từ địa chỉ có IP là 138.201.148.27 đến 94.64.15.27, các cái khác tương tự.

10001010.11001001.10010100.**00011011** (host 138.201.148.0) AND

00000000.00000000.00000000.**11111111** (reverse netmask)

01011110.01000000.00001111 (new net: 94.64.15.0)

01011110.01000000.00001111.**00011011** (địa chỉ mới)

2.2. NAT động

Yêu cầu m >= 1 và m >= n

NAT động được sử dụng khi số IP nguồn không bằng số IP đích. Số host chia sẻ nói chung bị giới hạn bởi số IP đích có sẵn. NAT động phức tạp hơn NAT tĩnh vì thế chúng phải lưu giữ lại thông tin kết nối và thậm chí tìm thông tin của TCP trong packet.

Như đã đề cập ở trên NAT động cũng có thể sử dụng như một NAT tĩnh khi m = n. Một số người dùng nó thay cho NAT tĩnh vì mục đích bảo mật. Những kẻ từ bên ngoài không thể tìm được IP nào kết nối với host chỉ định vì tại thời điểm tiếp theo host này có thể nhận một IP hoàn toàn khác. Trong trường hợp đặc biệt thậm chí có nhiều địa chỉ đích hơn địa chỉ nguồn (m< n) Những kết nối từ bên ngoài thì chỉ có thể khi những host này vẫn còn nắm giữ một IP trong bảng NAT động. Nơi mà NAT router lưu giữ những thông tin về IP bên trong (IP nguồn) được liên kết với NAT-IP(IP đích).

Cho một ví dụ trong một session của FPT non-passive. Nơi mà server cố gắng thiết lập một kênh truyền dữ liệu, vì thế khi server cố gắng gửi một IP packet đến FTP client thì phải có một entry cho client trong bảng NAT. Nó vẫn phải còn liên kết một IP client với cùng một NAT-IPs khi client bắt đầu một kênh truyền control trừ khi FTP session rỗi sau một thời gian timeout. Giao thức FTP có 2 cơ chế là passive và non-passive. Giao thức FTP luôn dùng 2 port

(control và data) . Với cơ chế passive (thụ động) host kết nối sẽ nhận thông tin về data port từ server và ngược lại non-passive thì host kết nối sẽ chỉ định data port yêu cầu server lắng nghe kết nối tới. Tham khảo thêm về FTP protocol trong RFC 959. Bất cứ khi nào nếu một kẻ từ bên ngoài muốn kết nối vào một host chỉ định ở bên trong mạng tại một thời điểm chỉ có 2 trường hợp :

+ Host bên trong không có một entry trong bảng NAT khi đó sẽ nhận được thông tin "host unreachable" hoặc có một entry nhưng NAT-IPs là không biết.

+ Biết được IP của một kết nối bởi vì có một kết nối từ host bên trong ra ngoài mạng. Tuy nhiên đó chỉ là NAT-IPs và không phải là IP thật của host. Và thông tin này sẽ bị mất sau một thời gian timeout của entry này trong bảng NAT router.

Ví dụ về một rule cho NAT động:

Dịch toàn bộ những IP trong class B, địa chỉ mạng 138.201.0.0 đến IP trong class B 178.201.112.0. Mỗi kết nối mới từ bên trong sẽ được liên kết với tập IP của class B khi mà IP đó không được sử dụng.

Vd: xem quá trình NAT trong trường hợp sau:

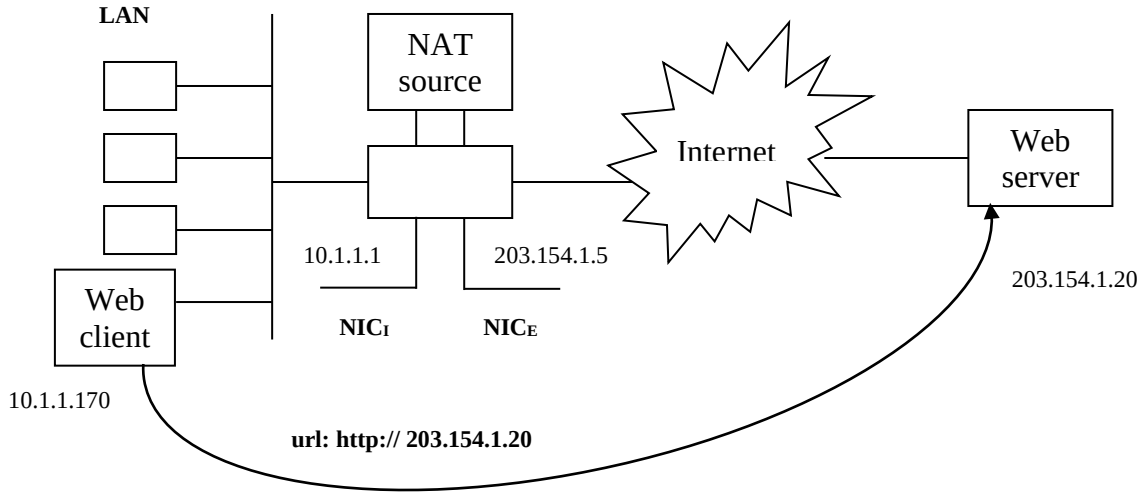
+ Client cục bộ 10.1.1.170/ 1074

+ NAT server IP_I : 10.1.1.1 / $port_I$:80

IP_E : 202.154.1.5 / $Port_E$ 1563

+ Web server : 203 .154.1.20 /80

Minh hoạ:



Hình 5: Mô tả quá trình NAT tĩnh

Quá trình NAT: Khi Client gởi yêu cầu đến webserver, Header sẽ báo tin gói tin bắt đầu tại:

10.1.1.170/1074 và đích gói tin này là cổng 80 trên Webserver có địa chỉ là 203.154.1.20 gói tin này được chặn tại cổng 80 của NAT Server, 10.1.1.1, NAT Server sẽ gắn header của gói tin này trước khi chuyển tiếp nó đến đích

Webserver. Header mới của gói tin cho biết gói tin xuất phát từ 203.154.1.5 / 1563 khi đến đích vẫn không thay đổi.

- Webserver nhận yêu cầu tại cổng 80 của nó và đáp ứng yêu cầu trở lại cho NAT server.

- Header của gói tin cho biết gói tin được gởi lại từ Webserver và đích của nó là cổng 1563 trên 203.154.1.5

+ NAT là một cách để giấu địa chỉ IP của các Server bên trong mạng nội bộ, tiết kiệm địa chỉ IP công cộng, NAT bảo mật sự tấn công trực tiếp từ bên ngoài vào các server dịch vụ bên trong, vì bên ngoài không nhìn thấy địa chỉ IP của các server này. Như vậy NAT là một trong những công cụ bảo mật mạng LAN.

NAT hoạt động trên một route giữa mạng nội bộ bên trong với bên ngoài, nó giúp chuyển đổi các địa chỉ IP. Nó thường được sử dụng cho các mạng có địa chỉ của lớp A,B,C.

- Hoạt động NAT bao gồm các bước sau:

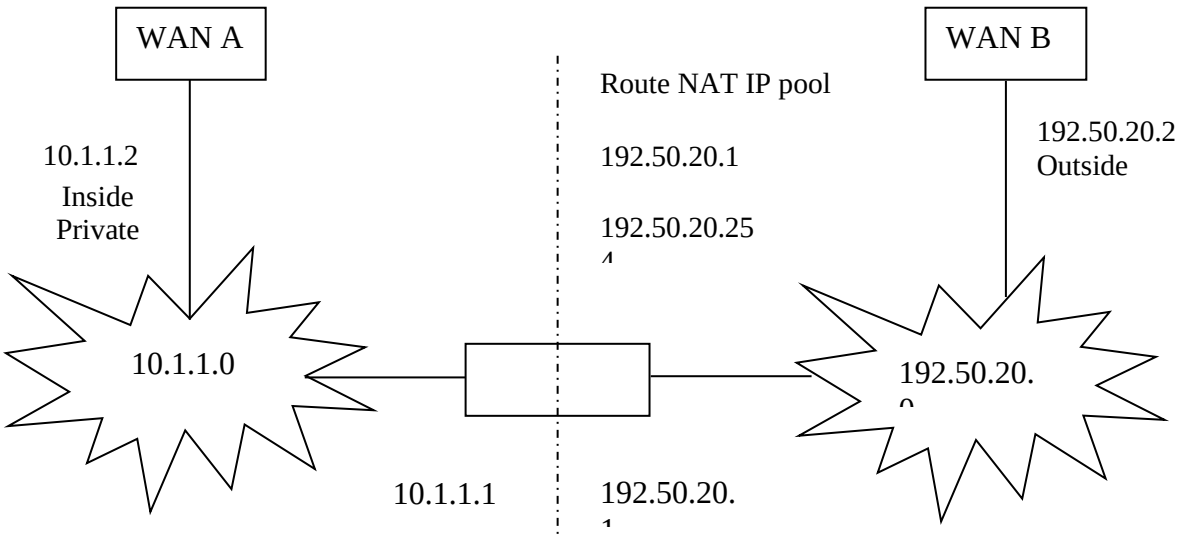
+ Địa chỉ IP trong header IP được thay đổi bằng một địa chỉ mới bên trong hoặc bên ngoài, số hiệu cổng trong header TCP cũng được thay thế thành số hiệu cổng mới.

+ Tổng kiểm tra các gói IP và tính toán lại sao cho dữ liệu được đảm bảo tính toàn vẹn. (Đảm bảo kết quả trả về đúng nơi mà nó yêu cầu)

+ Header TCP/IP checksum cũng phải được tính toán lại sao cho phù hợp với địa chỉ TCP/IP mới cả bên trong và bên ngoài lẫn cổng dịch vụ.

+ Có hai loại NAT: Nat tĩnh và Nat động, tương ứng với hai kỹ thuật cấp phát địa chỉ IP (địa chỉ IP tỉnh và địa chỉ IP động DHCP)

Minh hoạ:



Hình 6: Mô tả quá trình NAT động

Chú Ý:

NAT có thể chuyển đổi địa chỉ theo:

+ Một - Một

+ Nhiều - Một

=> Một địa chỉ bên trong có thể chuyển thành một địa chỉ hợp lệ bên ngoài hoặc ngược lại.

NAT Pool: Cho phép chuyển đổi địa chỉ nội bộ thành một dãy đia chỉ Public.

3. NAT trong Window server.

Mục tiêu:

- Trình bày được khái niệm và các thành phần Nat trong Windows server

- Thiết lập cấu hình NAT trên Windows server

3.1. Win 2003 cung cấp khái niệm NAT

NAT liên quan đến việc kết nối các LAN vào Internet, NAT cho phép các mạng nhỏ kết nối vào Internet như trong trường hợp của IPSec. Do đó chỉ cần một địa chỉ IP công cộng là có thể kết nối một lượng lớn để tuy cập vào Internet.

- NAT server cũng cần địa chỉ của một LAN bên trong, Người sử dụng bên ngoài không thể nhìn thấy địa chỉ của các server bên trong nhờ đó mà bảo vệ được các loại tấn công từ Internet.

- NAT của Win 2003 bao gồm các thành phần sau:

+ TRANSLATION: Là một máy tính chạy Win 2003 có chức năng Nat được, nó đóng vai trò của bộ chuyển đổi địa chỉ IP và số hiệu cổng của LAN bên trong thành các máy chủ bên ngoài Intranet.

+ ADDRESS: Là một máy tính đóng vai trò bộ chuyển đổi địa chỉ mạng nó cung cấp các thông tin địa chỉ IP của các Máy tính + mạng được xem như một DHCP server cung cấp thông tin về địa chỉ IP/ Subnet Mask/ Default Gateway/ DNS Server…

Trong trường hợp này tất cả máy tính bên trong LAN phải được cấu hình DHCP client.

+ Name Resolution: Là một mạng máy tính đóng vai trò NAT server nhưng cũng đồng thời là DNS server. Cho các máy tính khac trong mạng nội bộ, khi Client gởi yêu cầu đến NAT Server, NAT Server chuyển tiếp đến DNS server để đổi tên và chuyển kết quả về trở lại cho NAT và NAT server chuyển kết quả về lại theo yêu cầu.

3. 2. Hoạt động của NAT:

Khi một Client trong mạng cụ bộ gởi yêu cầu đi -> NAT server gởi dữ liệu của nó chứa địa chỉ IP, riêng và địa chỉ cổng trong Header IP NAT Server chuyển địa chỉ IP và địa chỉ cổng này thành địa chỉ công cộng và địa chỉ của nó rồi gởi gói dữ liệu.

Với Header IP mới này đến một host hay một Server trên Internet. Trong trường hợp này NATserver phải giữ lại địa chỉ IP và địa chỉ cổng Client yêu cầu trong mạng cục bộ để có cơ sở chuyển kết quả về cho Client sau này.

Khi nhân được yêu cầu từ host Internet, NATserver sẽ thay Header của gói tin thành Header nguyên thuỷ và gởi lại về cho Client yêu cầu.

3.3. Cài Đặt và cấu hình:

Phân tích bảng luật sau:

Rule	S_Addr	D_Addr	Service	Action	log	NAT
A	Firewall	Any	Any	Permit	Yes	
B	192.168.1.0 255.255.255.0	Firewall	Any	Permit	Na	
C	192.168.1.15	Any	Any	Permit	No	Nat(LAN)
D	Any	Firewall	TCP/80	Permit	Yes	MAP 192.168.1.15
E	Any	Any	Any	Deny	Na	

- Luật A không cho phép các máy trọng mạng nội bộ đi ra ngoài

- Luật B cho phép máy Client trong mạng nội bộ qua Firewall, được sử dụng mọi dịch vụ, không ghi lại File lưu, NAT không có chỉ được tới đích của Firewall

- Luật C cho phép các máy có địa chỉ nguồn như trên đi qua internet với bất kỳ dịch vụ nào, không ghi lại file lưu sử dụng NAT trong LAN.

- Luật D cho phép từ bên ngoài với Firewall sử dụng giao thức TCP với cổng 80 (giao thức http)

- Luật E mặc định

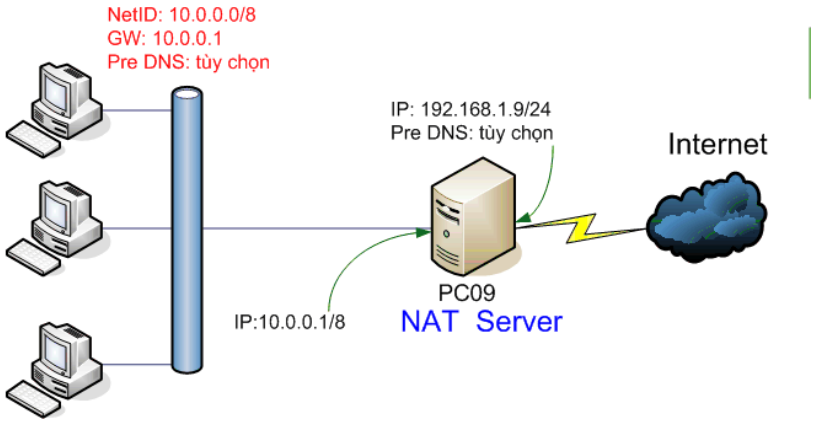
Bài tập thực hành của học viên

Câu 1: So sánh Nat tĩnh và Nat động

Câu 2: Trình bày khái niệm và cơ chế hoạt động Nat trong Window

Bài tập

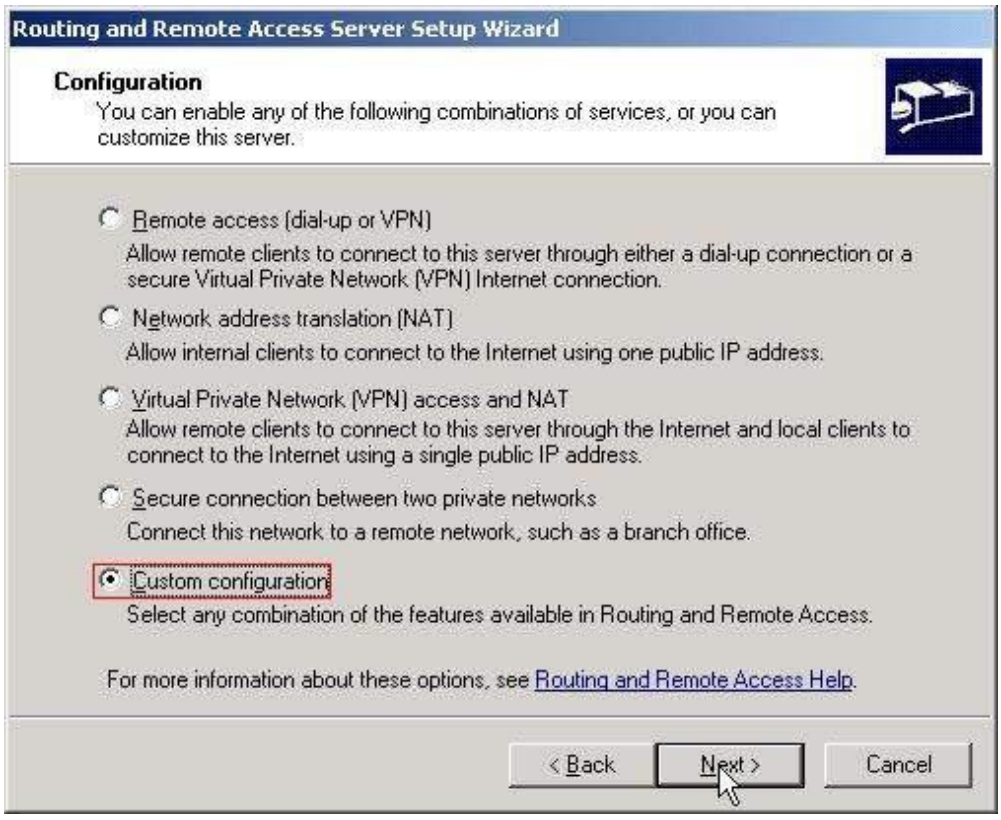
Thực hiện Nat trên nền Windows Server 2003 theo mô hình sau.



I.NAT outbound (NAT ra)

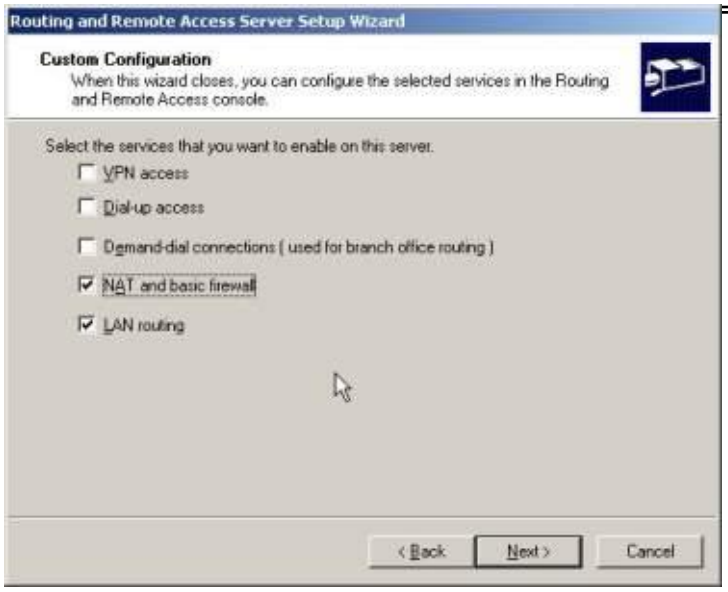
1.Cấu hình máy PC09 làm NAT Server

B1: Mở **Routing and Remote Access** -> Click phải chuột lên **NAT Server (PC09)** chọn **Configure and Enable Routing and Remote Access** -> Trong **Welcome** chọn **Next** -> Trong **Configuration** chọn ô **Custom configuration -> Next**

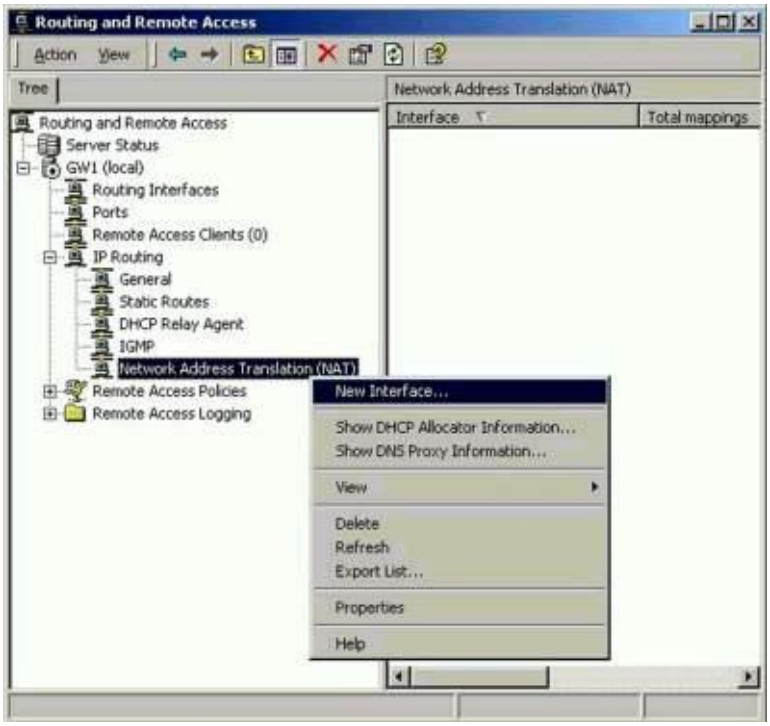


-Trong **Custome Configuration** -> Đánh dấu chọn ô **NAT and basic firewall** và ô **Lan Routing** -> **Next -> Finish**

Note: Khi kết thúc quá trình cấu hình hệ thống yêu cầu restart Service, chọn **Yes**



B2: Trong **Routing and Remote Access**, Click chuột phải lên **NAT/Basic Firewall**, chọn **New Interface** -> trong **New Interface for Network Address Tranlation (NAT)** -> Chọn card **LAN -> OK**



-Trong **Network Address Translation Properties -> LAN Properties ->** Chọn ô **Public interface connected to private network** -> Đánh dấu chọn ô **Enable NAT on this interface -> OK**



<u>B3:</u> Tương tự như **<u>B2</u>** Trong **Routing and Remote Access**, Click chuột phải lên **NAT/Basic Firewall**, chọn **New Interface** -> trong **New Interface for Network Address Tranlation (NAT)** -> Chọn card **LAN -> OK**

-Trong **Network Address Translation Properties** -> **CROSS Properties** -> Chọn ô **Private interface connected to private network -> OK**



<u>B4:</u> Trong **Routing and Remote Access** -> vào **IP Routing** -> Click phải chuột trên **Static Routes** chọn **New Static Route…** -> Trong cửa **Static Route** cấu

hình như sau:

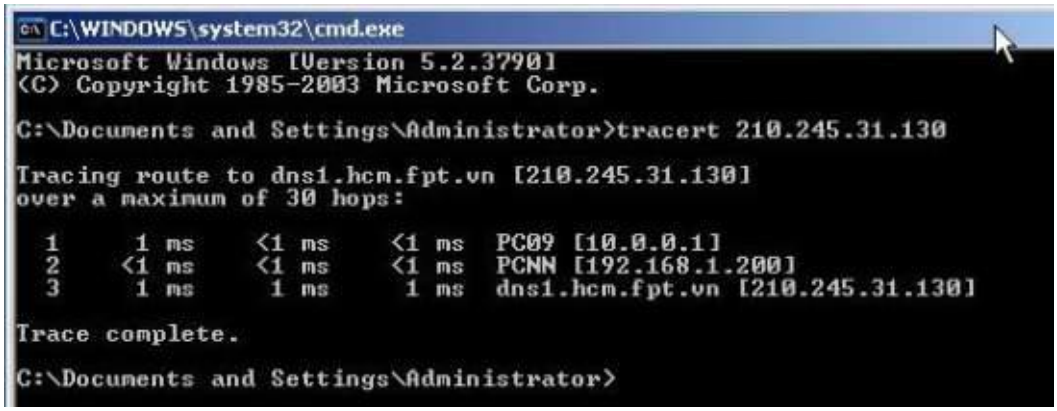
Interface: LAN
Destination: 0.0.0.0
Network mask: 0.0.0.0
Gateway: 192.168.1.200 (gateway ra Internet)
Metric: 1
-> OK
Note: **Gateway** phải cùng **NetID** với địa chỉ IP card **LAN**



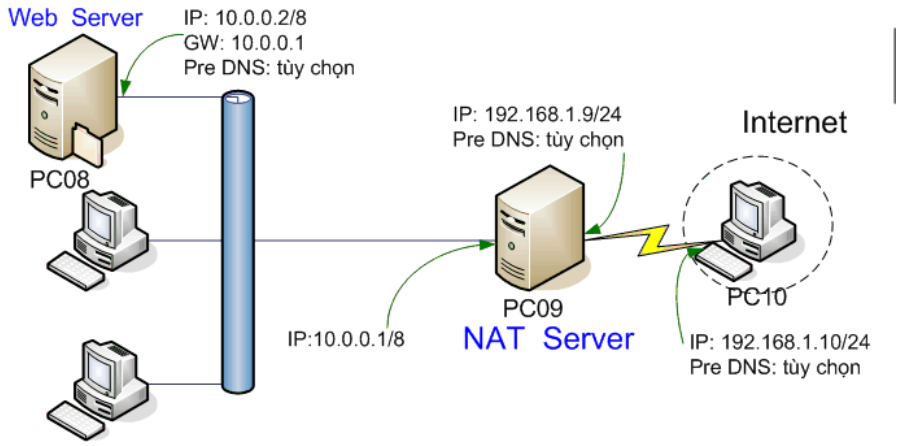
B5: Trong **Routing and Remote Access** -> Click phải chuột lên **PC09** chọn **All Tasks -> Restart**

2.Kiểm tra kết quả

Các máy trong **NetID** 10.0.0.0/8 đều có thể truy cập Internet. Ta có thể dùng lệnh **Tracert (phân tích đường đi của gói dữ liệu)** để kiểm tra



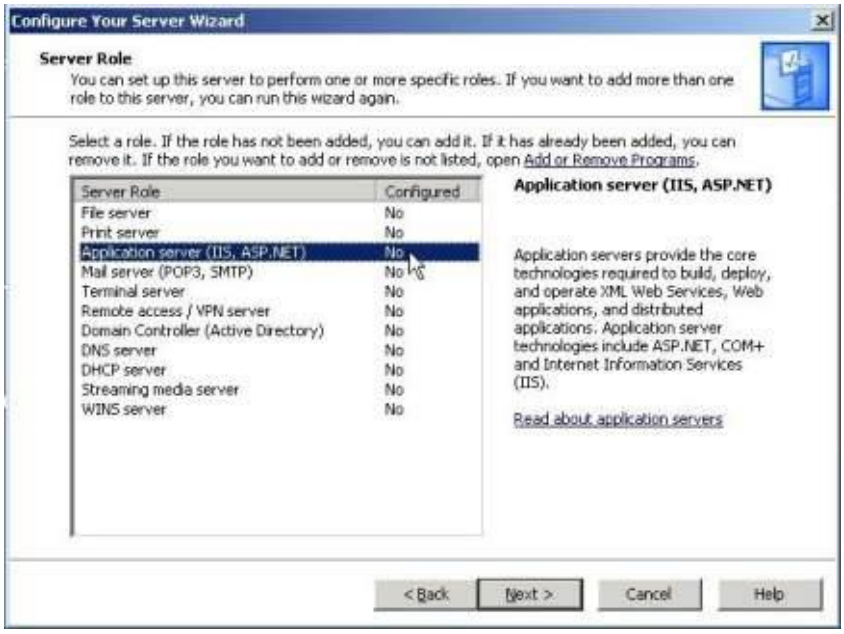
II.NAT Inbound (NAT vào)



1.Cấu hình Web Server trên máy PC08

B1:Start -> Programs -> Administrator Tools -> Configure Your Server Wizard -> Next -> Chọn **Application Server (IIS, ASP.NET)** -> **Next** . Làm theo các hướng dẫn để hoàn thành việc cài đặt.

Note: Trong quá trình cài đặt **IIS**, chỉ đường dẫn vào thư mục I386 trong đĩa CD Windows Server 2003 khi hệ thống yêu cầu



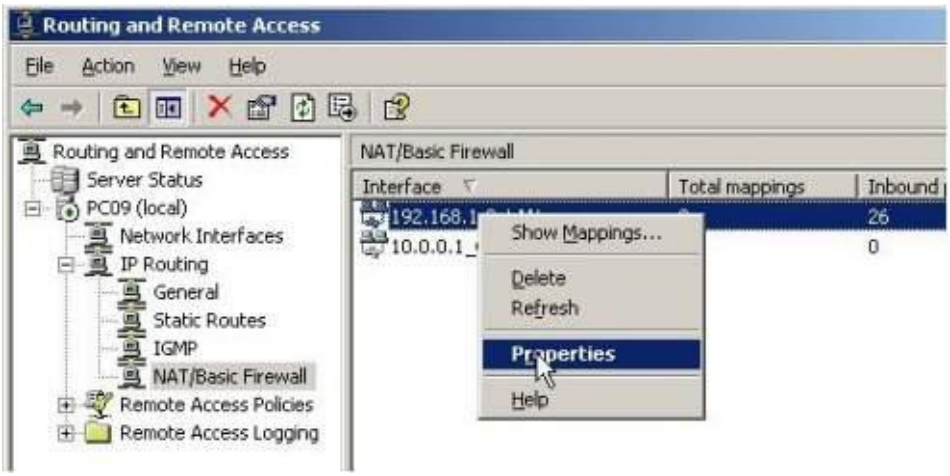
B2:Mở **Windows Explore** -> Vào thư mục **C:\Inetpub\wwwroot** -> Tạo file **index.htm** có nội dung (Vd: Welcome to website)

B3:Mở **Internet Explore** -> Truy cập vào địa chỉ IP hoặc địa chỉ Webserver

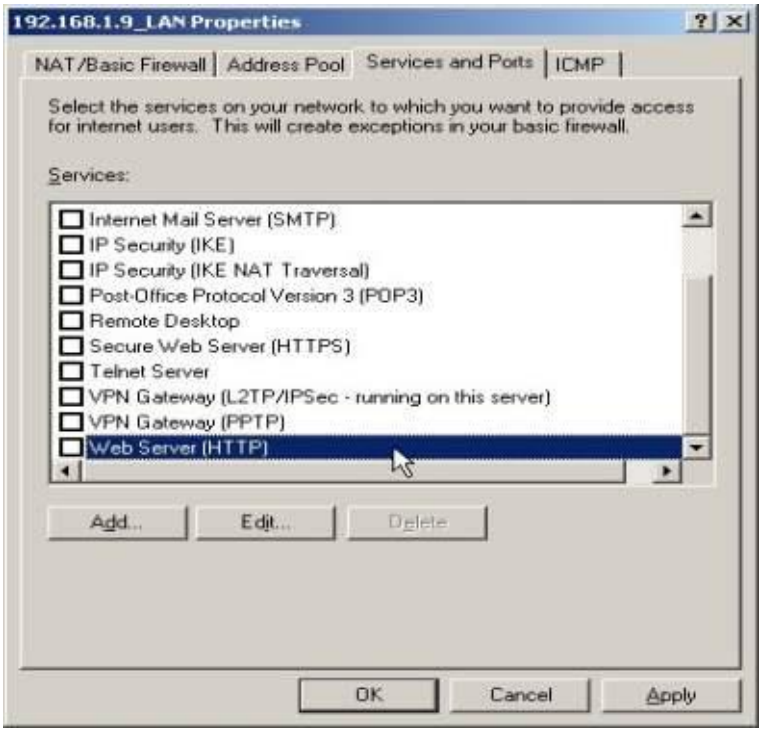
Note: Kiểm tra đã truy cập được vào trang web vừa mới tạo

2.Cấu hình NAT Server trên máy PC09

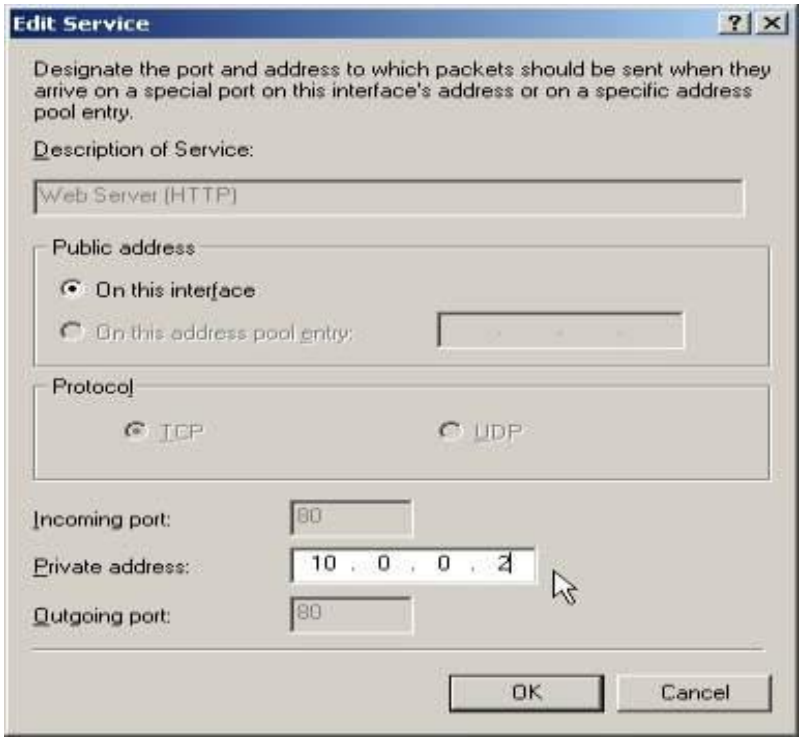
B1:Mở **Routing and Remote Access** -> chọn mục **NAT/Basic Firewall** -> Click chuột phải lên **LAN** chọn **Properties**



-chọn tab **Services and Ports** -> Kéo thanh trượt xuống phía dưới chọn mục **Web Server (HTTP)**



-Trong mục **Edit Service** nhập địa chỉ IP vào ô **Private Address:**

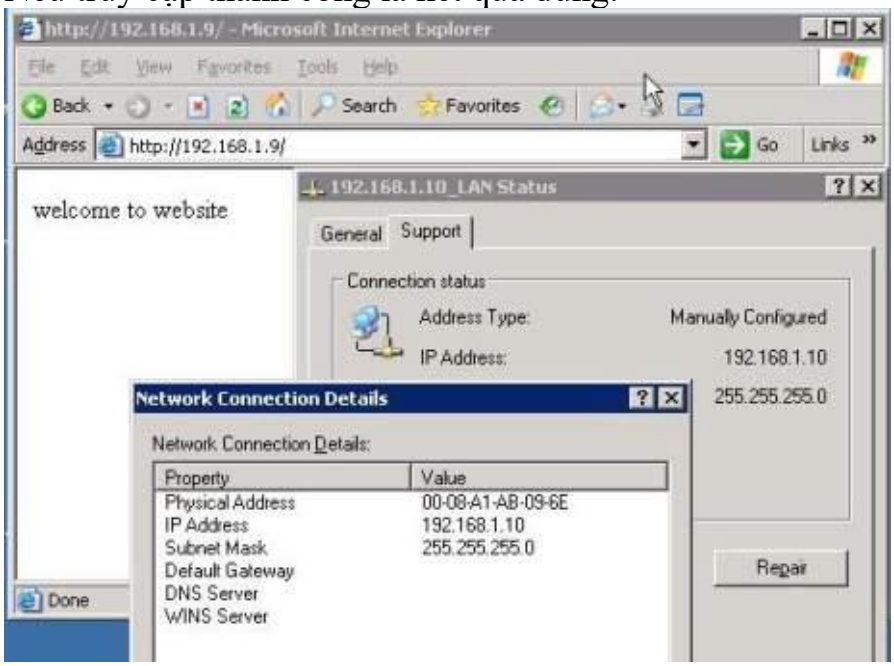


B2: Trong **Routing and Remote Access** -> Click chuột phải lên **PC09** chọn **All Tasks -> Restart**

3. Kiểm tra:

Máy **PC10** mở **Internet Explorer** -> Truy cập vào địa chỉ IP hoặc địa chỉ Webserver

Nếu truy cập thành công là kết quả đúng.



CHƯƠNG 4: BẢO VỆ MẠNG BẰNG TƯỜNG LỬA

Mã chương: MH26-04

Mục tiêu:

- Liệt kê được các tình huống tấn công mạng;
- Mô tả được xây dựng kiến trúc mạng sử dụng tường lửa;
- Cấu hình tường lửa để bảo vệ mạng;
- Thực hiện các thao tác an toàn với máy tính.

1. Các kiểu tấn công

Mục tiêu: Liệt kê được các tình huống tấn công mạng.

1.1. Tấn công trực tiếp

Sử dụng một máy tính để tấn công một máy tính khác với mục đích dò tìm mật mã, tên tài khoản tương ứng, …. Họ có thể sử dụng một số chương trình giải mã để giải mã các file chứa password trên hệ thống máy tính của nạn nhân. Do đó, những mật khẩu ngắn và đơn giản thường rất dễ bị phát hiện.

Ngoài ra, hacker có thể tấn công trực tiếp thông qua các lỗi của chương trình hay hệ điều hành làm cho hệ thống đó tê liệt hoặc hư hỏng. Trong một số trường hợp, hacker đoạt được quyền của người quản trị hệ thống.

1.2. Nghe trộm

Việc nghe trộm thông tin trên mạng có thể đưa lại những thông tin có ích như tên-mật khẩu của người sử dụng, các thông tin mật chuyển qua mạng. Việc nghe trộm thường được tiến hành ngay sau khi kẻ tấn công đã chiếm được quyền truy nhập hệ thống, thông qua các chương trình cho phép đưa vỉ giao tiếp mạng (Network Interface Card-NIC) vào chế độ nhận toàn bộ các thông tin lưu truyền trên mạng. Những thông tin này cũng có thể dễ dàng lấy được trên Internet.

1.3. Giả mạo địa chỉ

Việc giả mạo địa chỉ IP có thể được thực hiện thông qua việc sử dụng khả năng dẫn đường trực tiếp (*source-routing*). Với cách tấn công này, kẻ tấn công gửi các gói tin IP tới mạng bên trong với một địa chỉ IP giả mạo (thông thường là địa chỉ của một mạng hoặc một máy được coi là an toàn đối với mạng bên trong), đồng thời chỉ rõ đường dẫn mà các gói tin IP phải gửi đi.

1.4. Vô hiệu hoá các chức năng của hệ thống

Đây là kểu tấn công nhằm tê liệt hệ thống, không cho nó thực hiện chức năng mà nó thiết kế. Kiểu tấn công này không thể ngăn chặn được, do những phương tiện được tổ chức tấn công cũng chính là các phương tiện để làm việc và truy nhập thông tin trên mạng. Ví dụ sử dụng lệnh *ping* với tốc độ cao nhất có thể, buộc một hệ thống tiêu hao toàn bộ tốc độ tính toán và khả năng của mạng để trả lời các lệnh này, không còn các tài nguyên để thực hiện những công việc có ích khác.

1.5. Lỗi của người quản trị hệ thống

Đây không phải là một kiểu tấn công của những kẻ đột nhập, tuy nhiên lỗi của người quản trị hệ thống thường tạo ra những lỗ hổng cho phép kẻ tấn công sử dụng để truy nhập vào mạng nội bộ.

1.6. Tấn công vào yếu tố con người

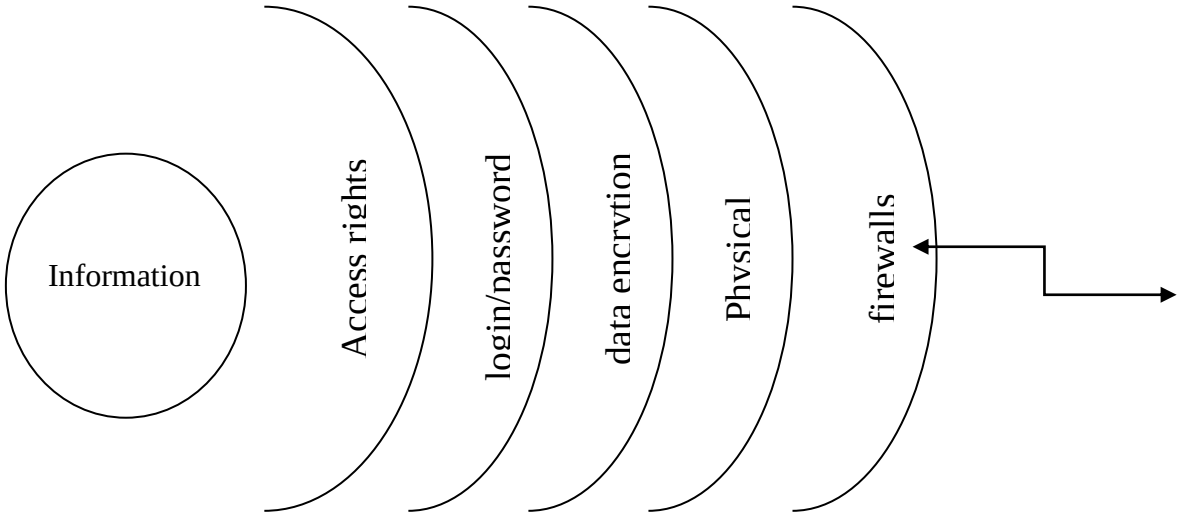
Kẻ tấn công có thể liên lạc với một người quản trị hệ thống, giả làm một người sử dụng để yêu cầu thay đổi mật khẩu, thay đổi quyền truy nhập của mình đối với hệ thống, hoặc thậm chí thay đổi một số cấu hình của hệ thống để thực hiện các phương pháp tấn công khác. Với kiểu tấn công này không một thiết bị nào có thể ngăn chặn một cách hữu hiệu, và chỉ có một cách giáo dục người sử dụng mạng nội bộ về những yêu cầu bảo mật để đề cao cảnh giác với những hiện tượng đáng nghi. Nói chung yếu tố con người là một điểm yếu trong bất kỳ một hệ thống bảo vệ nào, và chỉ có sự giáo dục cộng với tinh thần hợp tác từ phía người sử dụng có thể nâng cao được độ an toàn của hệ thống bảo vệ.

2. Các mức bảo vệ an toàn

Mục tiêu:

- Mô tả được xây dựng kiến trúc mạng sử dụng tường lửa

Vì không 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 trên mạng chủ yếu là bảo vệ thông tin cất giữ trong các máy tính, đặc biệt là trong các server của mạng. Hình sau mô tả các lớp rào chắn thông dụng hiện nay để bảo vệ thông tin tại các trạm của mạng



Hình 7:Các mức độ bảo vệ mạng

Như minh hoạ trong hình trên, các lớp bảo vệ thông tin trên mạng gồm:

- Lớp bảo vệ trong cùng là quyền truy nhập nhằm kiểm soát các tài nguyên (ở đây là thông tin) của mạng và quyền hạn (có thể thực hiện những thao tác gì) trên tài nguyên đó. Hiện nay việc kiểm soát ở mức này được áp dụng sâu nhất đối với tệp

- Lớp bảo vệ tiếp theo là hạn chế theo tài khoản truy nhập gồm đăng ký tên/ và mật khẩu tương ứng. Đây là phương pháp bảo vệ phổ biến nhất vì nó đơn giản, ít tốn kém và cũng rất có hiệu quả. Mỗi người sử dụng muốn truy nhập được vào mạng sử dụng các tài nguyên đều phải có đăng ký tên và mật khẩu. Người quản trị hệ thống có trách nhiệm quản lý, kiểm soát mọi hoạt động của mạng và xác định quyền truy nhập của những người sử dụng khác tuỳ theo thời gian và không gian.
- Lớp thứ ba là sử dụng các phương pháp mã hoá (encryption). Dữ liệu được biến đổi từ dạng "đọc được " sang dạng không "đọc được " theo một thuật toán nào đó. Chúng ta sẽ xem xét các phương thức và các thuật toán mã hoá hiện được sử dụng phổ biến ở phần dưới đây.
- Lớp thứ tư là bảo vệ vật lý (physical protection) nhằm ngăn cản các truy nhập vật lý bất hợp pháp vào hệ thống. Thườngdùng các biện pháp truyền thống Như ngăn cấm người không có nhiệm vụ vào phòng đặt máy, dùng hệ thống khoá trên máy tính, cài đặt các hệ thống báo động khi có truy nhập vào hệ thống ...
- Lớp thứ năm: Cài đặt các hệ thống bức tường lửa (firewall), nhằm ngăn chặn các thâm nhập trái phép và cho phép lọc các gói tin mà ta không muốn gửi đi hoặc nhận vào vì một lý do nào đó.

3. Internet Firwall

Mục tiêu:
- Trình bày được định nghĩa Firewall;
- Mô tả chức năng và cấu trúc của Firewall.

3.1. Định nghĩa

Thuật ngữ Firewall có nguồn gốc từ một kỹ thuật thiết kế trong xây dựng để ngăn chặn, hạn chế hoả hoạn. Trong công nghệ mạng thông tin, Firewall là một kỹ thuật được tích hợp vào hệ thống mạng để chống sự truy cập trái phép nhằm bảo vệ các nguồn thông tin nội bộ cũng như hạn chế sự xâm nhập vào hệ thống của một số thông tin khác không mong muốn. Cũng có thể hiểu rằng Firewall là một cơ chế để bảo vệ mạng tin tưởng (trusted network) khỏi các mạng không tin tưởng (untrusted network).

Internet Firewall là một thiết bị (phần cứng+phần mềm) giữa mạng của một tổ chức, một công ty, hay một quốc gia (Intranet) và Internet. Nó thực hiện vai trò bảo mật các thông tin Intranet từ thế giới Internet bên ngoài.

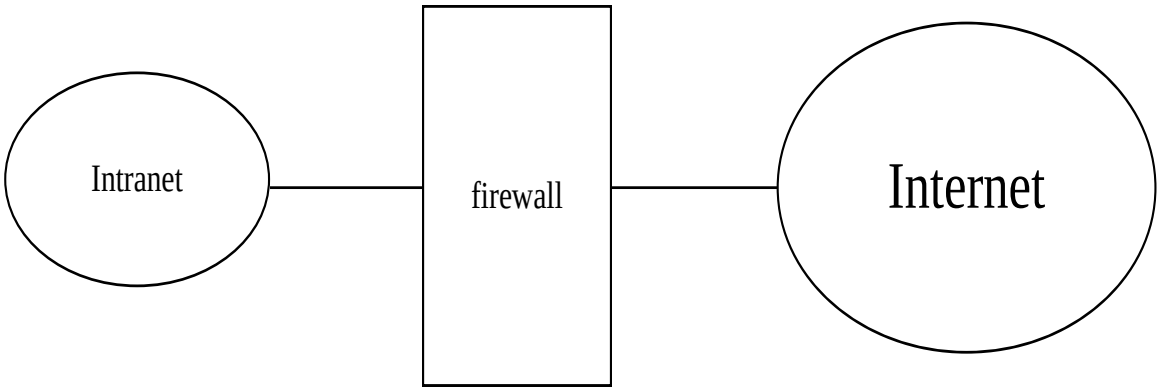
3.2. Chức năng chính

Internet Firewall (từ nay về sau gọi tắt là firewall) là một thành phần đặt giữa Intranet và Internet để kiểm soát tất cả các việc lưu thông và truy cập giữa chúng với nhau bao gồm:

Firewall quyết định những dịch vụ nào từ bên trong được phép truy cập từ bên ngoài, những người nào từ bên ngoài được phép truy cập đến các dịch vụ bên trong, và cả những dịch vụ nào bên ngoài được phép truy cập bởi những người bên trong.

Để firewall làm việc hiệu quả, tất cả trao đổi thông tin từ trong ra ngoài và ngược lại đều phải thực hiện thông qua Firewall.

Chỉ có những trao đổi nào được phép bởi chế độ an ninh của hệ thống mạng nội bộ mới được quyền lưu thông qua Firewall.



Hình 8 :Sơ đồ chức năng hệ thống của firewall

3.3. Cấu trúc

Firewall bao gồm:

Một hoặc nhiều hệ thống máy chủ kết nối với các bộ định tuyến (router) hoặc có chức năng router.

Các phần mềm quản lý an ninh chạy trên hệ thống máy chủ. Thông thường là các hệ quản trị xác thực (Authentication), cấp quyền (Authorization) và kế toán (Accounting).

3.4. Các thành phần của Firewall và cơ chế hoạt động

Một Firewall chuẩn bao gồm một hay nhiều các thành phần sau đây:

Bộ lọc packet (packet-filtering router)

Cổng ứng dụng (application-level gateway hay proxy server)

Cổng mạch (circuite level gateway)

3.4.1.Bộ lọc gói tin (Packet filtering router)

Nguyên lý:

Khi nói đến việc lưu thông dữ liệu giữa các mạng với nhau thông qua Firewall thì điều đó có nghĩa rằng Firewall hoạt động chặt chẽ với giao thức liên mạng TCP/IP. Vì giao thức này làm việc theo thuật toán chia nhỏ các dữ liệu nhận được từ các ứng dụng trên mạng, hay nói chính xác hơn là các dịch vụ chạy trên các giao thức (Telnet, SMTP, DNS, SMNP, NFS...) thành các gói dữ liệu (data packets) rồi gán cho các packet này những địa chỉ để có thể nhận dạng, tái lập lại ở đích cần gửi đến, do đó các loại Firewall cũng liên quan rất nhiều đến các *packet* và những con số địa chỉ của chúng.

Bộ lọc packet cho phép hay từ chối mỗi *packet* mà nó nhận được. Nó kiểm tra toàn bộ đoạn dữ liệu để quyết định xem đoạn dữ liệu đó có thoả mãn một trong số các luật lệ của lọc *packet* hay không. Các luật lệ lọc *packet* này là dựa trên các thông tin ở đầu mỗi *packet* (packet header), dùng để cho phép truyền các packet đó ở trên mạng. Đó là:

Địa chỉ IP nơi xuất phát (IP Source address)

Địa chỉ IP nơi nhận (IP Destination address)

Những thủ tục truyền tin (TCP, UDP, ICMP, IP tunnel)

Cổng TCP/UDP nơi xuất phát (TCP/UDP source port)

Cổng TCP/UDP nơi nhận (TCP/UDP destination port)

Dạng thông báo ICMP (ICMP message type)

giao diện packet đến (incomming interface of packet)

giao diện packet đi (outcomming interface of packet)

Nếu luật lệ lọc packet được thoả mãn thì *packet* được chuyển qua firewall. Nếu không *packet* sẽ bị bỏ đi. Nhờ vậy mà Firewall có thể ngăn cản được các kết nối vào các máy chủ hoặc mạng nào đó được xác định, hoặc khoá việc truy cập vào hệ thống mạng nội bộ từ những địa chỉ không cho phép. Hơn nữa, việc kiểm soát các cổng làm cho Firewall có khả năng chỉ cho phép một số loại kết nối nhất định vào các loại máy chủ nào đó, hoặc chỉ có những dịch vụ nào đó (Telnet, SMTP, FTP...) được phép mới chạy được trên hệ thống mạng cục bộ.

Ưu điểm

Đa số các hệ thống firewall đều sử dụng bộ lọc *packet*. Một trong những ưu điểm của phương pháp dùng bộ lọc packet là chi phí thấp vì cơ chế lọc *packet* đã được bao gồm trong mỗi phần mềm router.

Ngoài ra, bộ lọc *packet* là trong suốt đối với người sử dụng và các ứng dụng, vì vậy nó không yêu cầu sự huấn luyện đặc biệt nào cả.

Hạn chế:

Việc định nghĩa các chế độ lọc *packet* là một việc khá phức tạp, nó đòi hỏi người quản trị mạng cần có hiểu biết chi tiết về các dịch vụ Internet, các dạng *packet header*, và các giá trị cụ thể mà họ có thể nhận trên mỗi trường. Khi đòi hỏi về sự lọc càng lớn, các luật lệ về lọc càng trở nên dài và phức tạp, rất khó để quản lý và điều khiển.

Do làm việc dựa trên *header* của các *packet*, rõ ràng là bộ lọc *packet* không kiểm soát được nội dung thông tin của *packet*. Các *packet* chuyển qua vẫn có thể mang theo những hành động với ý đồ ăn cắp thông tin hay phá hoại của kẻ xấu.

3.4.2. Cổng ứng dụng (application-level gateway)

Nguyên lý

Đây là một loại Firewall được thiết kế để tăng cường chức năng kiểm soát các loại dịch vụ, giao thức được cho phép truy cập vào hệ thống mạng. Cơ chế hoạt động của nó dựa trên cách thức gọi là Proxy service (dịch vụ đại diện). Proxy service là các bộ chương trình đặc biệt cài đặt trên gateway cho từng ứng dụng. Nếu người quản trị mạng không cài đặt chương trình proxy cho một ứng dụng nào đó, dịch vụ tương ứng sẽ không được cung cấp và do đó không thể chuyển thông tin qua firewall. Ngoài ra, proxy code có thể được định

cấu hình để hỗ trợ chỉ một số đặc điểm trong ứng dụng mà người quản trị mạng cho là chấp nhận được trong khi từ chối những đặc điểm khác.

Một cổng ứng dụng thường được coi như là một pháo đài (bastion host), bởi vì nó được thiết kế đặt biệt để chống lại sự tấn công từ bên ngoài. Những biện pháp đảm bảo an ninh của một bastion host là:

Bastion host luôn chạy các version an toàn (secure version) của các phần mềm hệ thống (Operating system). Các version an toàn này được thiết kế chuyên cho mục đích chống lại sự tấn công vào Operating System, cũng như là đảm bảo sự tích hợp firewall.

Chỉ những dịch vụ mà người quản trị mạng cho là cần thiết mới được cài đặt trên bastion host, đơn giản chỉ vì nếu một dịch vụ không được cài đặt, nó không thể bị tấn công. Thông thường, chỉ một số giới hạn các ứng dụng cho các dịch vụ Telnet, DNS, FTP, SMTP và xác thực user là được cài đặt trên bastion host.

Bastion host có thể yêu cầu nhiều mức độ xác thực khác nhau, ví dụ như user password hay smart card.

Mỗi proxy được đặt cấu hình để cho phép truy nhập chỉ một sồ các máy chủ nhất định. Điều này có nghĩa rằng bộ lệnh và đặc điểm thiết lập cho mỗi proxy chỉ đúng với một số máy chủ trên toàn hệ thống.

Mỗi proxy duy trì một quyển nhật ký ghi chép lại toàn bộ chi tiết của giao thông qua nó, mỗi sự kết nối, khoảng thời gian kết nối. Nhật ký này rất có ích trong việc tìm theo dấu vết hay ngăn chặn kẻ phá hoại.

Mỗi proxy đều độc lập với các proxies khác trên bastion host. Điều này cho phép dễ dàng quá trình cài đặt một proxy mới, hay tháo gỡ môt proxy đang có vấn đề.

Ví dụ: Telnet Proxy

Ví dụ một người (gọi là outside client) muốn sử dụng dịch vụ TELNET để kết nối vào hệ thống mạng qua môt bastion host có Telnet proxy. Quá trình xảy ra như sau:

Outside client telnets đến bastion host. Bastion host kiểm tra password, nếu hợp lệ thì outside client được phép vào giao diện của Telnet proxy. Telnet proxy cho phép một tập nhỏ những lệnh của Telnet, và quyết định những máy chủ nội bộ nào outside client được phép truy nhập.

Outside client chỉ ra máy chủ đích và Telnet proxy tạo một kết nối của riêng nó tới máy chủ bên trong, và chuyển các lệnh tới máy chủ dưới sự uỷ quyền của outside client. Outside client thì tin rằng Telnet proxy là máy chủ thật ở bên trong, trong khi máy chủ ở bên trong thì tin rằng Telnet proxy là client thật.

Ưu điểm:

Cho phép người quản trị mạng hoàn toàn điều khiển được từng dịch vụ trên mạng, bởi vì ứng dụng proxy hạn chế bộ lệnh và quyết định những máy chủ nào có thể truy nhập được bởi các dịch vụ.

Cho phép người quản trị mạng hoàn toàn điều khiển được những dịch vụ nào cho phép, bởi vì sự vắng mặt của các proxy cho các dịch vụ tương ứng có nghĩa là các dịch vụ ấy bị khoá.

Cổng ứng dụng cho phép kiểm tra độ xác thực rất tốt, và nó có nhật ký ghi chép lại thông tin về truy nhập hệ thống.

Luật lệ filltering (lọc) cho cổng ứng dụng là dễ dàng cấu hình và kiểm tra hơn so với bộ lọc packet.

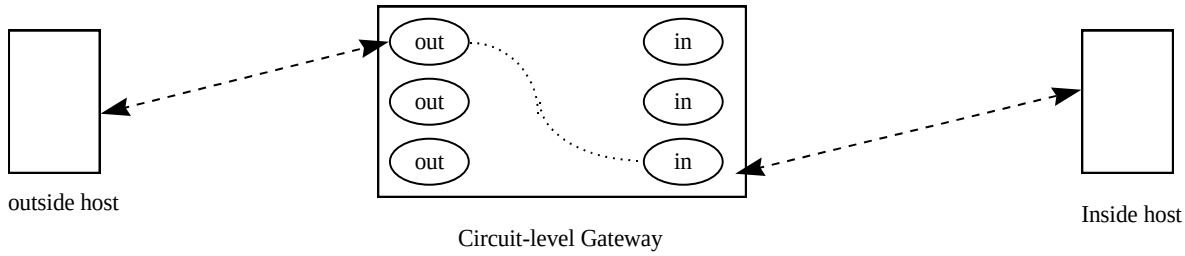
Hạn chế:

Yêu cầu các users biến đổi (modify) thao tác, hoặc modify phần mềm đã cài đặt trên máy client cho truy nhập vào các dịch vụ proxy. Ví dụ, Telnet truy nhập qua cổng ứng dụng đòi hỏi hai bước đê nối với máy chủ chứ không phải là một bước thôi. Tuy nhiên, cũng đã có một số phần mềm client cho phép ứng dụng trên cổng ứng dụng là trong suốt, bằng cách cho phép user chỉ ra máy đích chứ không phải cổng ứng dụng trên lệnh Telnet.

3.4.3. Cổng vòng (circuit-Level Gateway)

Cổng vòng là một chức năng đặc biệt có thể thực hiện đươc bởi một cổng ứng dụng. Cổng vòng đơn giản chỉ chuyển tiếp (relay) các kết nối TCP mà không thực hiện bất kỳ một hành động xử lý hay lọc packet nào.

Một hành động sử dụng nối telnet qua cổng vòng. Cổng vòng đơn giản chuyển tiếp kết nối telnet qua firewall mà không thực hiện một sự kiểm tra, lọc hay điều khiển các thủ tục Telnet nào.Cổng vòng làm việc như một sợi dây,sao chép các byte giữa kết nối bên trong (inside connection) và các kết nối bên ngoài (outside connection). Tuy nhiên, vì sự kết nối này xuất hiện từ hệ thống firewall, nó che dấu thông tin về mạng nội bộ.



Hình 9: Mô tả chức năng của cổng vòng

Cổng vòng thường được sử dụng cho những kết nối ra ngoài, nơi mà các quản trị mạng thật sự tin tưởng những người dùng bên trong. Ưu điểm lớn nhất là một bastion host có thể được cấu hình như là một hỗn hợp cung cấp Cổng ứng dụng cho những kết nối đến, và cổng vòng cho các kết nối đi. Điều này làm cho hệ thống bức tường lửa dễ dàng sử dụng cho những người trong mạng nội bộ muốn trực tiếp truy nhập tới các dịch vụ Internet, trong khi vẫn cung cấp chức năng bức tường lửa để bảo vệ mạng nội bộ từ những sự tấn công bên ngoài.

3.5. Những hạn chế của firewall

Firewall không đủ thông minh như con người để có thể đọc hiểu từng loại thông tin và phân tích nội dung tốt hay xấu của nó. Firewall chỉ có thể ngăn

chặn sự xâm nhập của những nguồn thông tin không mong muốn nhưng phải xác định rõ các thông số địa chỉ.

Firewall không thể ngăn chặn một cuộc tấn công nếu cuộc tấn công này không "đi qua" nó. Một cách cụ thể, firewall không thể chống lại một cuộc tấn công từ một đường dial-up, hoặc sự dò rỉ thông tin do dữ liệu bị sao chép bất hợp pháp lên đĩa mềm.

Firewall cũng không thể chống lại các cuộc tấn công bằng dữ liệu (data-driven attack). Khi có một số chương trình được chuyển theo thư điện tử, vượt qua firewall vào trong mạng được bảo vệ và bắt đầu hoạt động ở đây.

Một ví dụ là các virus máy tính. Firewall không thể làm nhiệm vụ rà quét virus trên các dữ liệu được chuyển qua nó, do tốc độ làm việc, sự xuất hiện liên tục của các virus mới và do có rất nhiều cách để mã hóa dữ liệu, thoát khỏi khả năng kiểm soát của firewall.

3.6. Các ví dụ firewall

3.6.1. Packet-Filtering Router (Bộ trung chuyển có lọc gói)

Hệ thống Internet firewall phổ biến nhất chỉ bao gồm một packet-filtering router đặt giữa mạng nội bộ và Internet . Một packet-filtering router có hai chức năng: chuyển tiếp truyền thông giữa hai mạng và sử dụng các quy luật về lọc gói để cho phép hay từ chối truyền thông. Căn bản, các quy luật lọc đượ định nghĩa sao cho các host trên mạng nội bộ được quyền truy nhập trực tiếp tới Internet, trong khi các host trên Internet chỉ có một số giới hạn các truy nhập vào các máy tính trên mạng nội bộ. Tư tưởng của mô cấu trúc firewall này là tất cả những gì không được chỉ ra rõ ràng là cho phép thì có nghĩa là bị từ chối.

Packet-filtering router

Ưu điểm:

giá thành thấp (vì cấu hình đơn giản)

trong suốt đối với người sử dụng

Hạn chế:

Có tất cả hạn chế của một packet-filtering router, như là dễ bị tấn công vào các bộ lọc mà cấu hình được đặt không hoàn hảo, hoặc là bị tấn công ngầm dưới những dịch vụ đã được phép.

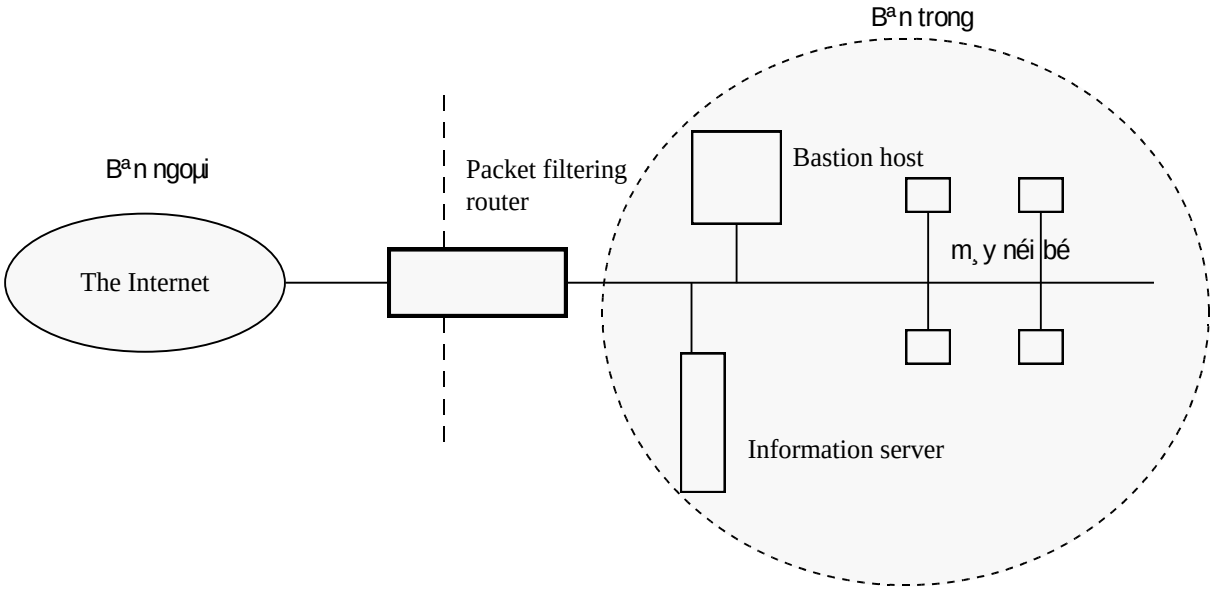
Bởi vì các packet được trao đổi trực tiếp giữa hai mạng thông qua router , nguy cơ bị tấn công quyết định bởi số lượng các host và dịch vụ được phép. Điều đó dẫn đến mỗi một host được phép truy nhập trực tiếp vào Internet cần phải được cung cấp một hệ thống xác thực phức tạp, và thường xuyên kiểm tra bởi người quản trị mạng xem có dấu hiệu của sự tấn công nào không.

Nếu một packet-filtering router do một sự cố nào đó ngừng hoạt động, tất cả hệ thống trên mạng nội bộ có thể bị tấn công.

3.6.2. Screened Host Firewall

Hệ thống này bao gồm một packet-filtering router và một bastion host. Hệ thống này cung cấp độ bảo mật cao hơn hệ thống trên, vì nó thực hiện cả bảo mật ở tầng network(packet-filtering) và ở tầng ứng dụng (application level).

Đồng thời, kẻ tấn công phải phá vỡ cả hai tầng bảo mật để tấn công vào mạng nội bộ.



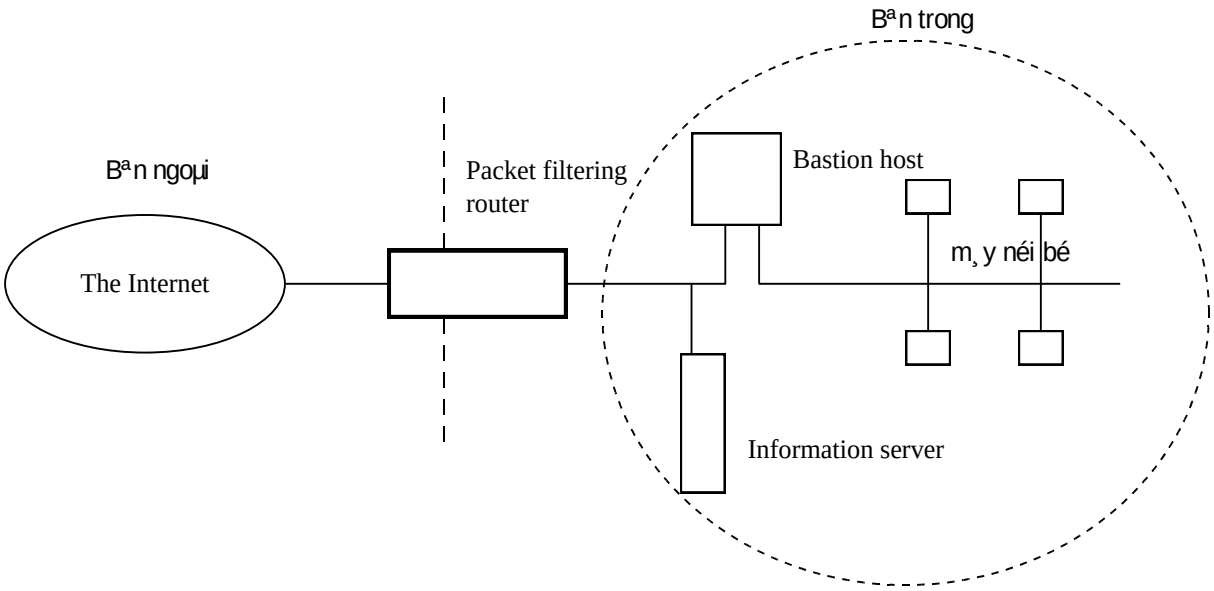
Hình10 : Screened host firewall (Single- Homed Bastion Host)

Trong hệ thống này, bastion host được cấu hình ở trong mạng nội bộ. Qui luật filtering trên packet-filtering router được định nghĩa sao cho tất cả các hệ thống ở bên ngoài chỉ có thể truy nhập bastion host; Việc truyền thông tới tất cả các hệ thống bên trong đều bị

khoá. Bởi vì các hệ thống nội bộ và bastion host ở trên cùng một mạng, chính sách bảo mật của một tổ chức sẽ quyết định xem các hệ thống nội bộ được phép truy nhập trực tiếp vào bastion Internet hay là chúng phải sử dụng dịch vụ proxy trên bastion host. Việc bắt buộc những user nội bộ được thực hiện bằng cách đặt cấu hình bộ lọc của router sao cho chỉ chấp nhận những truyền thông nội bộ xuất phát từ bastion host.

Ưu điểm:

Máy chủ cung cấp các thông tin công cộng qua dịch vụ Web và FTP có thể đặt trên packet-filtering router và bastion. Trong trường hợp yêu cầu độ an toàn cao nhất, bastion host có thể chạy các dịch vụ proxy yêu cầu tất cả các user cả trong và ngoài truy nhập qua bastion host trước khi nối với máy chủ. Trường hợp không yêu cầu độ an toàn cao thì các máy nội bộ có thể nối thẳng với máy chủ.



Hình 11: Screened host firewall (Dual- Homed Bastion Host)

Nếu cần độ bảo mật cao hơn nữa thì có thể dùng hệ thống firewall dual-home (hai chiều) bastion host. Một hệ thống bastion host như vậy có 2 giao diện mạng (network interface), nhưng khi đó khả năng truyền thông trực tiếp giữa hai giao diện đó qua dịch vụ proxy là bị cấm.

Bởi vì bastion host là hệ thống bên trong duy nhất có thể truy nhập được từ Internet, sự tấn công cũng chỉ giới hạn đến bastion host mà thôi. Tuy nhiên, nếu như người dùng truy nhập được vào bastion host thì họ có thể dễ dàng truy nhập toàn bộ mạng nội bộ. Vì vậy cần phải cấm không cho người dùng truy nhập vào bastion host.

3.6.3. Demilitarized Zone (DMZ - khu vực phi quân sự) hay Screened-subnet Firewall

Hệ thống này bao gồm hai packet-filtering router và một bastion host . Hệ thống firewall này có độ an toàn cao nhất vì nó cung cấp cả mức bảo mật : network và application trong khi định nghĩa một mạng "phi quân sự". Mạng DMZ đóng vai trò như một mạng nhỏ, cô lập đặt giữa Internet và mạng nội bộ. Cơ bản, một DMZ được cấu hình sao cho các hệ thống trên Internet và mạng nội bộ chỉ có thể truy nhập được một số giới hạn các hệ thống trên mạng DMZ, và sự truyền trực tiếp qua mạng DMZ là không thể được.

Với những thông tin đến, router ngoài chống lại những sự tấn công chuẩn (như giả mạo địa chỉ IP), và điều khiển truy nhập tới DMZ. Nó cho phép hệ thống bên ngoài truy nhập chỉ bastion host, và có thể cả information server. Router trong cung cấp sự bảo vệ thứ hai bằng cách điều khiển DMZ truy nhập mạng nội bộ chỉ với những truyền thông bắt đầu từ bastion host.

Với những thông tin đi, router trong điều khiển mạng nội bộ truy nhập tới DMZ. Nó chỉ cho phép các hệ thống bên trong truy nhập bastion host và có thể

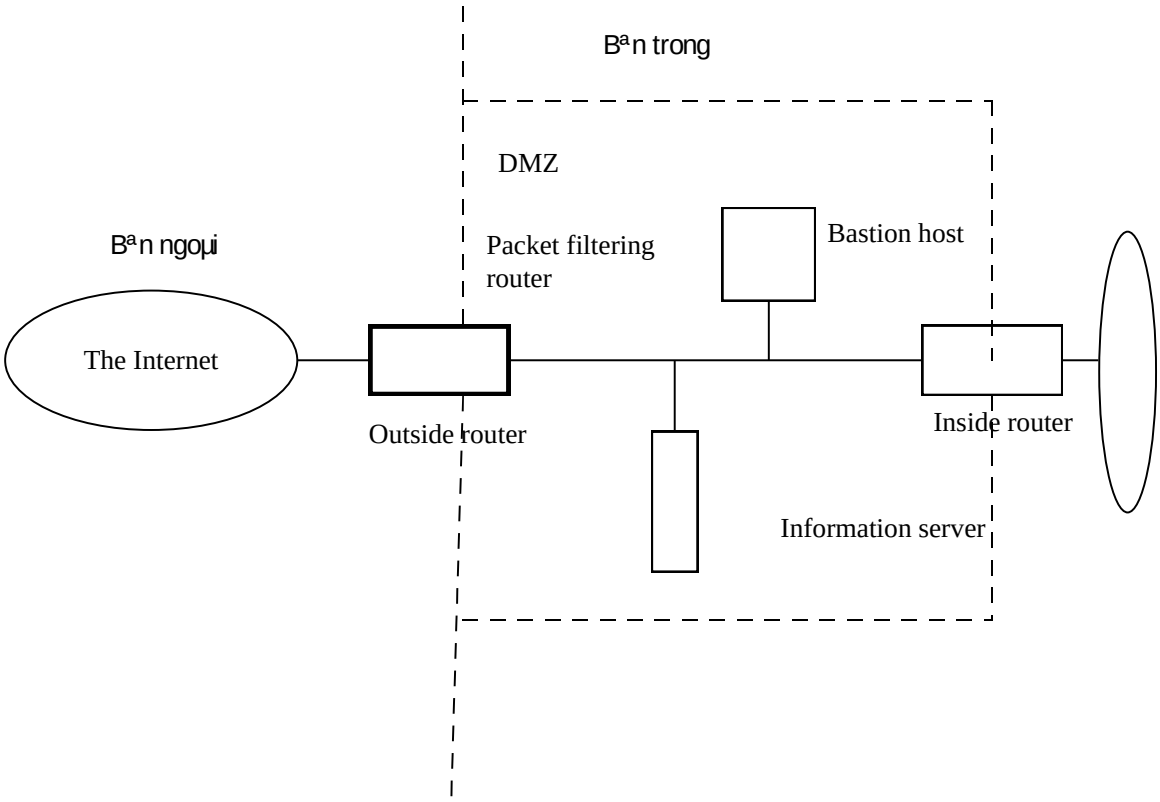
cả information server. Quy luật filtering trên router ngoài yêu cầu sử dụng dịch vụ proxy bằng cách chỉ cho phép thông tin ra bắt nguồn từ bastion host.

Ưu điểm:

Kẻ tấn công cần phá vỡ ba tầng bảo vệ: router ngoài, bastion host và router trong.

Bởi vì router ngoài chỉ quảng bá DMZ network tới Internet, hệ thống mạng nội bộ là không thể nhìn thấy (invisible). Chỉ có một số hệ thống đã được chọn ra trên DMZ là được biết đến bởi Internet qua routing table và DNS information exchange (Domain Name Server).

Bởi vì router trong chỉ quảng bá DMZ network tới mạng nội bộ, các hệ thống trong mạng nội bộ không thể truy nhập trực tiếp vào Internet. Điều nay đảm bảo rằng những user bên trong bắt buộc phải truy nhập Internet qua dịch vụ proxy.



Hình 12:Screened-Subnet Firewall

Bài tập thực hành của học viên

Câu 1: Trình bày các kiểu tấn công mạng

Câu 2: Vẽ và trình bày chức năng và cấu truca cua Firewall

Câu 3: Trình bày Ưu và nhược điểm của Bộ lọc gói tin (Packet filtering router)

Câu 4: Trình bày Ưu và nhược điểm của Cổng ứng dụng (application-level gateway)

CHƯƠNG 5: DANH SÁCH ĐIỀU KHIỂN TRUY CẬP

Mã chương:MH26-05

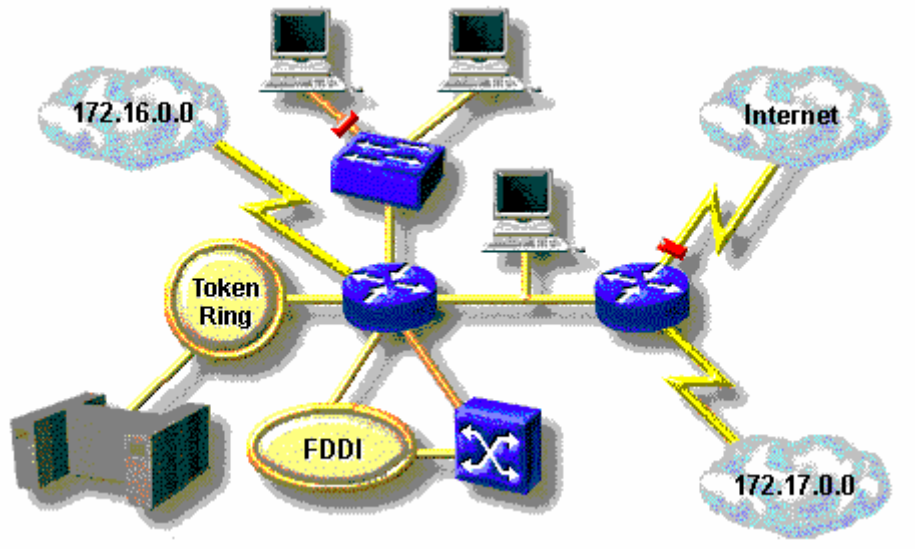
Mục tiêu:

- Trình bày được khái niệm về danh sách truy cập;
- Mô tả được nguyên tắc hoạt động của danh sách truy cập;
- Mô phỏng được danh sách truy cập trong chuẩn mạng TCP/IP;
- Thực hiện các thao tác an toàn với máy tính.

Giới thiệu

Các mạng có sử dụng chọn đường đầu tiên đã nối một tập nhỏ các mạng LAN và các máy tính lại với nhau. Kế tiếp nhà quản trị mạng mở rộng các nối kết của router sang các mạng bên ngoài. Sự gia tăng của việc sử dụng Internet đã mang đến nhiều thách thức đối với việc điều khiển truy cập. Các công nghệ mới hơn như mạng đường trục bằng cáp quang cho đến các dịch vụ băng thông rộng và những bộ hoán chuyển tốc độ cao đã làm gia tăng nhiều hơn các thách thức trong điều khiển truy cập mạng.

Các nhà quản trị đang đối mặt với các vấn đề có tính tiến thoái lưỡng nan như: Làm sao từ chối các nối kết không mong muốn trong khi vẫn cho phép các truy cập hợp lệ ? Mặc dù các công cụ như mật khẩu, các thiết bị phản hồi và các thiết bị an toàn vật lý thì hữu ích, chúng thường thiếu sự diễn giải mềm dẽo và những cơ chế điều khiển mà hầu hết các nhà quản trị mạng mong muốn.



Hình 13: Vấn đề an ninh trong mạng diện rộng

Danh sách truy cập (Access list) hay còn gọi Danh sách điều khiển truy cập (Access Control List) cung cấp một công cụ mạnh cho việc điều khiển mạng. Những danh sách này đưa vào cơ chế mềm dẽo trong việc lọc dòng các gói tin mà chúng đi ra, đi vào các giao diện của các router. Các danh sách này giúp mở rộng việc bảo vệ các tài nguyên mạng mà không làm ảnh hưởng đến

những dòng giao tiếp hợp lệ. Danh sách truy cập phân biệt giao thông của các gói tin ra thành nhiều chủng loại mà chúng được phép hay bị từ chối. Danh sách truy cập có thể được sử dụng để:

- Nhận dạng các gói tin cho việc xếp thứ tự ưu tiên hay sắp xếp trong hàng đợi
- Hạn chế hoặc giảm nội dung của thông tin cập nhật chọn đường.

  Danh sách truy cập cũng xử lý các gói tin cho các tính năng an toàn khác như:
- Cung cấp cơ chế điều khiển truy cập động đối với các gói tin IP dựa vào cơ chế nhận dạng người dùng nâng cao, sử dụng tính năng chìa và ổng khóa.
- Nhận dạng các gói tin cho việc mã hóa
- Nhận dạng các truy cập bằng dịch vụ Telnet được cho phép để cấu hình router.

1. Định nghĩa danh sách truy cập

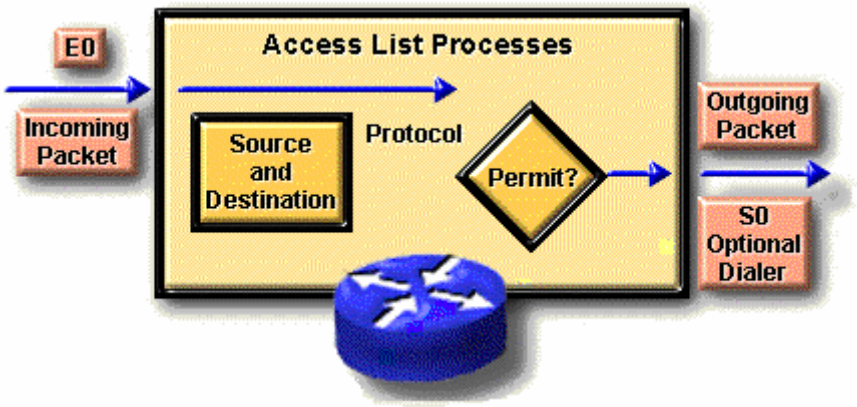
Mục tiêu:

- Trình bày được khái niệm về danh sách truy cập;

Danh sách truy cập là những phát biểu dùng để đặc tả những điều kiện mà một nhà quản trị muốn thiết đặt, nhờ đó router sẽ xử lý các cuộc truyền tải đã được mô tả trong danh sách truy cập theo một cách thức không bình thường. Danh sách truy cập đưa vào những điều khiển cho việc xử lý các gói tin đặc biệt theo một cách thức duy nhất. Có hai loại danh sách truy cập chính là:

- Danh sách truy cập chuẩn (standard access list): Danh sách này sử dụng cho việc kiểm tra địa chỉ gởi của các gói tin được chọn đường. Kết quả cho phép hay từ chối gởi đi cho một bộ giao thức dựa trên địa chỉ mạng/mạng con hay địa chỉ máy.

Ví dụ: Các gói tin đến từ giao diện E0 được kiểm tra về địa chỉ và giao thức. Nếu được phép, các gói tin sẽ được chuyển ra giao diện S0 đã được nhóm trong danh sách truy cập. Nếu các gói tin bị từ chối bởi danh sách truy cập, tất cả các gói tin cùng chủng loại sẽ bị xóa đi.



Hình 14: Ý nghĩa của danh sách truy cập chuẩn

- ❖ Danh sách truy cập mở rộng (Extended access list): Danh sách truy cập mở rộng kiểm tra cho cả địa chỉ gởi và nhận của gói tin. Nó cũng kiểm tra cho các giao thức cụ thể, số hiệu cổng và các tham số khác. Điều này cho phép các nhà quản trị mạng mềm dẻo hơn trong việc mô tả những gì muốn danh sách truy cập kiểm tra. Các gói tin được phép hoặc từ chối gởi đi tùy thuộc vào gói tin đó được xuất phát từ đâu và đi đến đâu.

2. Nguyên tắc hoạt động của Danh sách truy cập

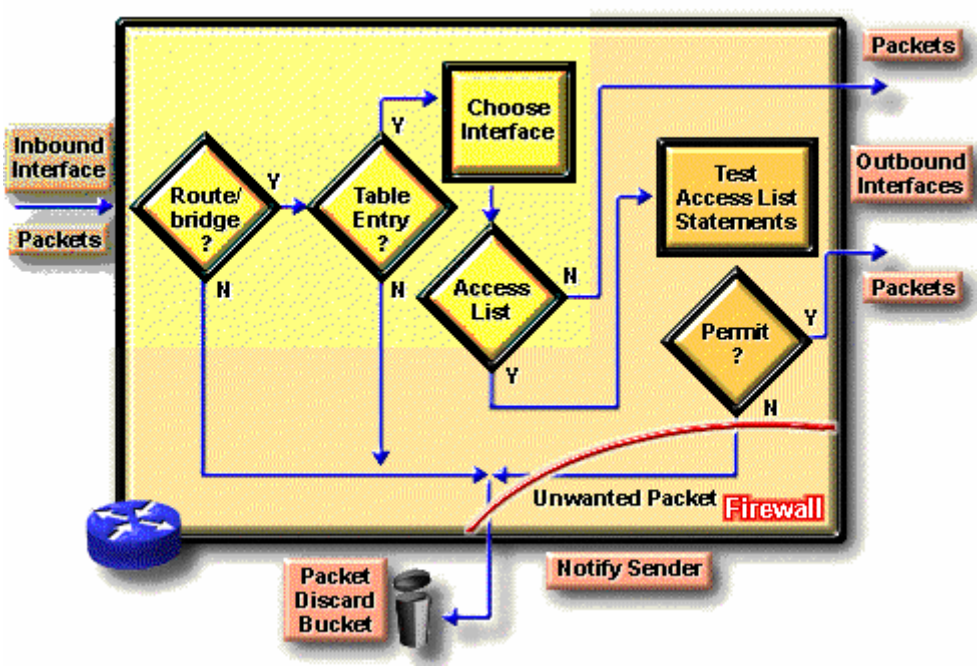
Mục tiêu:

- Mô tả được nguyên tắc hoạt động của danh sách truy cập

- Trình bày được danh sách truy cập chuẩn và danh sách truy cập mở rộng

- Mô tả được các thành phần trong câu lệnh của danh sách truy cập

Danh sách truy cập diễn tả một tập hợp các qui luật cho phép đưa vào các điều khiển các gói tin đi vào một giao diện của router, các gói tin lưu lại tạm thời ở router và các gói tin gởi ra một giao diện của router. Danh sách truy cập không có tác dụng trên các gói tin xuất phát từ router đang xét.



Hình 15: Nguyên tắc hoạt động của danh sách truy cập

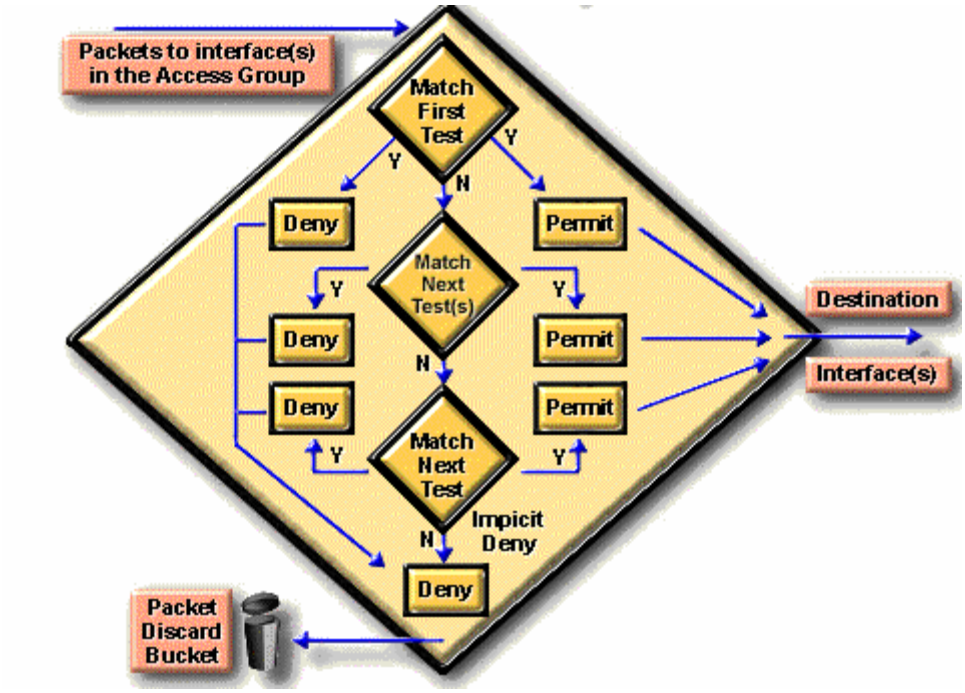
Khởi đầu của tiến trình thì giống nhau không phân biệt có sử dụng danh sách truy cập hay không: Khi một gói tin đi vào một giao diện, router kiểm tra để xác định xem có thể chuyển gói tin này đi hay không. Nếu không được, gói tin sẽ bị xóa đi. Một mục từ trong bảng chọn đường thể hiện cho một đích đến trên mạng cùng với chiều dài đường đi đến đích và giao diện của router hướng về đích đến này.

Kế tiếp router sẽ kiểm tra để xác định xem giao diện hướng đến đích đến có trong một danh sách truy cập không. Nếu không, gói tin sẽ được gởi

ra vùng đệm cho ngõ ra tương ứng, mà không bị một danh sách truy cập nào chi phối.

Giả sử giao diện nhận đã được đặt trong một danh sách truy cập mở rộng. Nhà quản trị mạng đã sử dụng các biểu thức luận lý, chính xác để thiết lập danh sách truy cập này. Trước khi một gói tin có thể được đưa đến giao diện ra, nó phải được kiểm tra bởi một tập các quy tắc được định nghĩa trong danh sách truy cập được gán cho giao diện.

Dựa vào những kiểm tra trên danh sách truy cập mở rộng, một gói tin có thể được phép đối với các danh sách vào (inbound list), có nghĩa là tiếp tục xử lý gói tin sau khi nhận trên một giao diện hay đối với danh sách ra (outbound list), điều này có nghĩa là gởi gói tin đến vùng đệm tương ứng của giao diện ra. Ngược lại, các kết quả kiểm tra có thể từ chối việc cấp phép nghĩa là gói tin sẽ bị hủy đi. Khi hủy gói tin, một vài giao thức trả lại gói tin cho người đã gởi. Điều này báo hiệu cho người gởi biết rằng không thể đi đến đích được.



Hình 16: Nguyên tăc lọc dựa trên danh sách truy cập

Các lệnh trong danh sách truy cập hoạt động một cách tuần tự. Chúng đánh giá các gói tin từ trên xuống. Nếu tiêu đề của một gói tin và một lệnh trong danh sách truy cập khớp với nhau, gói tin sẽ bỏ qua các lệnh còn lại. Nếu một điều kiện được thỏa mãn, gói tin sẽ được cấp phép hay bị từ chối. Chỉ cho phép một danh sách trên một giao thức trên một giao diện.

Trong ví dụ trên, giả sư có sự trùng hợp với bước kiểm tra đầu tiên và gói tin bị từ chối truy cập giao diện hướng đến đích đến. Gói tin sẽ bị bỏ đi và đưa vào một thùng rác. Gói tin không còn đi qua bất kỳ bước kiểm tra nào khác.

Chỉ các gói tin không trùng với bất kỳ điều kiện nào của bước kiểm tra đầu tiên mới được chuyển vào bước kiểm tra thứ hai. Giả sử rằng một tham số khác của gói tin trùng khớp với bước kiểm tra thứ hai, đây là một lệnh cho phép, gói tin được phép chuyển ra giao diện hướng về đích.

Một gói tin khác không trùng với bất cứ điều kiện nào của bước kiểm tra thứ nhất và kiểm tra bước thứ hai, nhưng lại trùng với điều kiện kiểm tra thứ ba với kết quả là được phép.

Chú ý rằng: Để hoàn chỉnh về mặt luận lý, một danh sách truy cập phải có các điều kiện mà nó tạo ra kết quả đúng cho tất cả các gói tin. Một lệnh cài đặt cuối cùng thì bao trùm cho tất cả các gói tin mà các bước kiểm tra trước đó đều không có kết quả đúng. Đây là bước kiểm tra cuối cùng mà nó khớp với tất cả các gói tin. Nó là kết quả từ chối. Điều này sẽ làm cho tất cả các gói tin sẽ bị bỏ đi.

2.1 Tổng quan về các lệnh trong Danh sách truy cập

Trong thực tế, các lệnh trong danh sách truy cập có thể là các chuỗi với nhiều ký tự. Danh sách truy cập có thể phức tạp để nhập vào hay thông dịch. Tuy nhiên chúng ta có thể đơn giản hóa các lệnh cấu hình danh sách truy cập bằng cách đưa chúng về hai loại tổng quát sau:

Loại 1: Bao gồm các lệnh cơ bản để xử lý các vấn đề tổng quát, cú pháp được mô tả như sau:

access-list *access-list- number* *{permit|deny}* *{test conditions}*

o access-list: là từ khóa bắt buộc

o access-list-number: Lệnh tổng thể này dùng để nhận dạng danh sách truy cập, thông thường là một con số. Con số này biểu thị cho loại của danh sách truy cập.

o Thuật ngữ cho phép (permit) hay từ chối (deny) trong các lệnh của danh sách truy cập tổng quát biểu thị cách thức mà các gói tin khớp với điều kiện kiểm tra được xử lý bởi hệ điều hành của router. Cho phép thông thường có nghĩa là gói tin sẽ được phép sử dụng một hay nhiều giao diện mà bạn sẽ mô tả sau.

o *test conditions:* Thuật ngữ cuối cùng này mô tả các điều kiện kiểm tra được dùng bởi các lệnh của danh sách truy cập. Một bước kiểm tra có thể đơn giản như là việc kiểm tra một địa chỉ nguồn. Tuy nhiên thông thường các điều kiện kiểm tra được mở rộng để chứa đựng một vài điều kiện kiểm tra khác. Sử dụng các lệnh trong danh sách truy cập tổng quát với cùng một số nhận dạng để chồng nhiều điều kiện kiểm tra vào trong một chuỗi luận lý hoặc một danh sách kiểm tra.

Loại 2: Xử lý của danh sách truy cập sử dụng một lệnh giao diện. Cú pháp như sau:

{protocol} access-group access-list-number

Với:

Protocol: là giao thức áp dụng danh sách truy cập

Access-group: là từ khóa

Access-list-number: Số hiệu nhận dạng của danh sách truy cập đã được định nghĩa trước

Tất cả các lệnh của danh sách truy cập được nhận dạng bởi một con số tương ứng với một hoặc nhiều giao diện. Bất kỳ các gói tin mà chúng vượt qua được các điều kiện kiểm tra trong danh sách truy cập có thể được gán phép sử dụng bất kỳ một giao diện trong nhóm giao diện được phép.

2.2. Danh sách truy cập chuẩn trong mạng TCP/IP

2.2.1.Kiểm tra các gói tin với danh sách truy cập

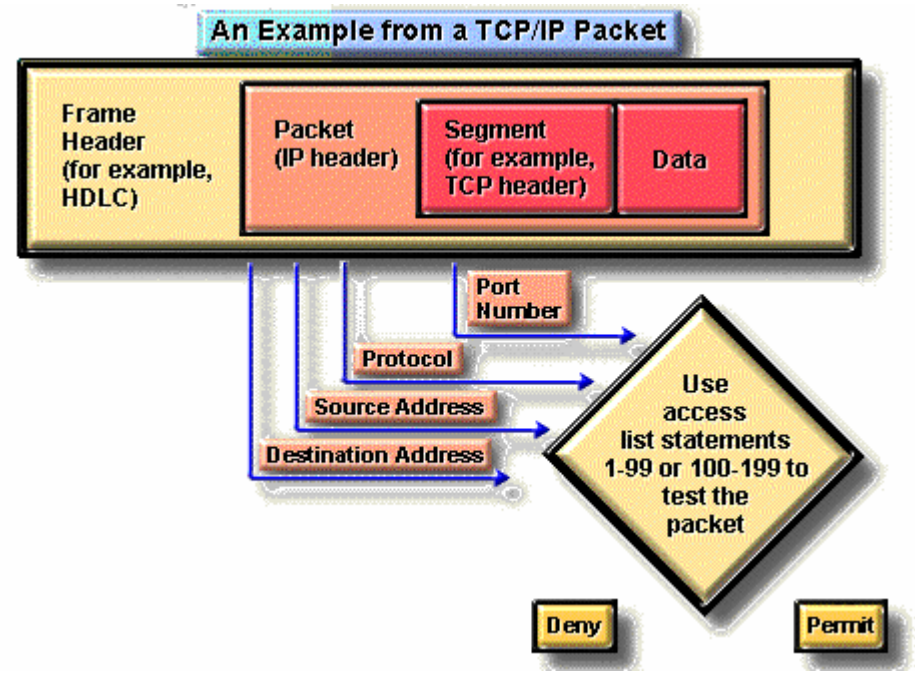
Để lọc các gói tin TCP/IP, danh sách truy cập trong hệ điều hành liên mạng của Cisco kiểm tra gói tin và phần tiêu đề của giao thức tầng trên.

Tiến trình này bao gồm các bước kiểm tra sau trên gói tin:

o Kiểm tra địa chỉ nguồn bằng danh sách truy cập chuẩn. Nhận dạng những danh sách truy cập này bằng các con số có giá trị từ 1 đến 99

o Kiểm tra địa chỉ đích và địa chỉ nguồn hoặc giao thức bằng danh sách truy cập mở rộng . Nhận dạng các danh sách này bằng các con số có giá trị từ 100 đến 199.

o Kiểm tra số hiệu cổng của các giao thức TCP hoặc UDP bằng các điều kiện trong các danh sách truy cập mở rộng. Các danh sách này cũng được nhận dạng bằng các con số có giá trị từ 100 đến 199.



Hinh 17: Ví dụ về danh sách truy cập trong gói tin TCP/IP

Đối với tất cả các danh sách truy cập của giao thức TCP/IP này, sau khi một gói tin được kiểm tra để khớp một lệnh trong danh sách, nó có thể bị từ chối hoặc cấp phép để sử dụng một giao diện trong nhóm các giao diện được truy cập.

Một số lưu ý khi thiết lập danh sách truy cập:

o Nhà quản trị mạng phải hết sức thận trọng khi đặc tả các điều khiển truy cập

và thứ tự các lệnh để thực hiện các điều khiển truy cập này. Chỉ rõ các giao thức được phép trong khi các giao thức TCP/IP còn lại thì bị từ chối.

o Chỉ rõ các giao thức IP cần kiểm tra. Các giao thức IP còn lại thì không cần kiểm tra.

o Sử dụng các ký tự đại diện (wildcard) để mô tả luật chọn lọc địa chỉ IP.

2.2.3. Sử dụng các bit trong mặt nạ ký tự đại diện

- **Wilcard mask:** wilcard mask bit nào trong địa chỉ IP sẽ được bỏ qua khi so sánh với địa chỉ IP khác. <1> trong wildcard mask có nghĩa bỏ qua vị trí bit đó khi so sánh với địa chỉ IP, và <0> xác định vị trí bit phải giống nhau. Với Standard access-list, nếu không thêm wildcard mask trong câu lệnh tạo access-list thì 0.0.0.0 ngầm hiểu là wildcard mask. Với standard access list, nếu không thêm wilcard mark trong câu lệnh tạo access-list thì 0.0.0.0 ngầm hiểu là wildcard mask.

Mặt nạ ký tự đại hiện (Wildcard mask) là một chuỗi 32 bits được dùng để kết hợp với địa chỉ IP để xác định xem bit nào trong địa chỉ IP được bỏ qua khi so sánh với các địa chỉ IP khác. Các mặt nạ ký tự đại diện này được mô tả khi xây dựng các danh sách truy cập. Ý nghĩa của các bits trong mặt nạ các ký tự đại diện được mô tả như sau:

o Một bits có giá trị là 0 trong mặt nạ đại diện có nghĩa là « hãy kiểm tra bit của địa chỉ IP có vị trí tương ứng với bit này »

o Một bits có giá trị là 1 trong mặt nạ đại diện có nghĩa là « đừng kiểm tra bit của địa chỉ IP có vị trí tương ứng với bit này »

Bằng cách thiết lập các mặt nạ ký tự đại diện, một nhà quản trị mạng có thể chọn lựa một hoặc nhiều địa chỉ IP để các kiểm tra cấp phép hoặc từ chối. Xem ví dụ trong hình dưới đây:

128	64	32	16	8	4	2	1	Vị trí các bit trong byte và giá trị địa chỉ của nó
0	0	0	0	0	0	0	0	Mặt nạ kiểm tra tất cả các bit địa chỉ
0	0	1	1	1	1	1	1	Mặt nạ không kiểm tra 6 bits cuối cùng của địa chỉ
0	0	0	0	1	1	1	1	Mặt nạ không kiểm tra 4 bits cuối cùng của địa chỉ
1	1	1	1	1	1	0	0	Mặt nạ kiểm tra 2 bits cuối cùng của địa chỉ
1	1	1	1	1	1	1	1	Mặt nạ không kiểm tra địa chỉ

Ví dụ: Cho một địa chỉ mạng ở lớp B 172.16.0.0. Mạng này được chia thành 256 mạng con bằng cách sử dụng 8 bit ở bytes thứ 3 của địa chỉ để làm số nhận dạng mạng con. Nhà quản trị muốn định kiểm tra các địa chỉ IP của các

mạng con từ 172.16.16.0 đến 172.16.31. Các bước suy luận để đưa ra mặt nạ các ký tự đại diện trong trường hợp này như sau:

o Đầu tiên mặt nạ ký tự đại diện phải kiểm tra hai bytes đầu tiên của địa chỉ (172.16). Như vậy các bits trong hai bytes đầu tiên của mặt nạ ký tự đại diện phải bằng 0. Ta có 0000 0000.0000 0000.-.-

o Do không kiểm tra địa chỉ của các máy tính trong mạng nên các bit của bytes cuối cùng sẽ được bỏ qua. Vì thế các bits của bytes cuối cùng trong mặt nạ ký tự đại diện sẽ là 1. Ta có 0000 0000.0000 0000.-.1111 1111

o Trong byte thứ ba của địa chỉ nơi mạng con được định nghĩa, mặt nạ ký tự đại diện sẽ kiểm tra bit ở vị trí có giá trị thứ 16 của địa chỉ phải được bật (giá trị là 1) và các bits ở phần cao còn lại phải tắt (giá trị là 0). Vì thế các bits tương ứng trong mặt nạ ký tự đại diện phải bằng 0.

o Bốn bits còn lại của bytes thứ 3 không cần kiểm tra để nó có thể tạo nên các giá trị từ 16 đến 31. Vì thế các bits tương ứng trong mặt nạ ký tự đại diện tương ứng sẽ bằng 1.

o Như vậy mặt nạ ký tự đại diện là đầy đủ là: 0000 0000.0000 0000.0000 1111.1111 1111 hay 0.0.15.255

Để đơn giản, một số router, chẳng hạn CISCO, sử dụng một số từ viết tắt để chỉ một số mặt nạ thường sử dụng:

o any: dùng để chỉ mặt nạ cho phép tất cả địa chỉ (255.255.255.255) hoặc cấm
tất cả (0.0.0.0.).

o host: được đặt phía trước một địa chỉ IP của một máy tính để chỉ rằng hãy kiểm tra tất cả các bit của địa chỉ trên. Ví dụ: host 172.16.1.1.

* Cấu hình danh sách truy cập chuẩn cho giao thức IP

Phần này giới thiệu một số lệnh được hỗ trợ trong các router của Cisco.

7.4.3.1 Lệnh access list

Lệnh này dùng để tạo một mục từ trong danh sách bộ lọc chuẩn. Cú pháp như sau:

access-list access-list-No {permit | deny } source {source-mask}

Ý nghĩa của các tham số:

o access-list-No: Là số nhận dạng của danh sách truy cập, có giá trị từ 1 đến 99

o permit | deny: Tùy chọn cho phép hay không cho phép đối với giao thông của khối địa chỉ được mô tả phía sau.

o source: Là một địa chỉ IP

o source-mask: Là mặt nạ ký tự đại diện áp dụng lên khối địa chỉ source

Lệnh ip access-group

Lệnh này dùng để liên kết một danh sách truy cập đã tồn tại vào một giao diện. Cú pháp như sau:

ip access-group *access-list-No {in/out}*

o access-list-no: số nhận dạng của danh sách truy cập được nối kết vào giao diện

o in/out: xác định chiều giao thông muốn áp dụng và vào hay ra.

Bài tập thực hành của học viên

Câu 1: So sánh danh sách truy cập chuẩn (standard access list) và Danh sách truy cập mở rộng (Extended access list)

Câu 2: Trình bày nguyên tắc hoạt động của Danh sách truy cập

Câu 3: Trình bày và mô tả cú pháp trong danh sách truy cập chuẩn và truy cập mở rộng

Bài 1: standard access-list

Mô tả:

– Lab này mô tả lọc gói dữ liệu sử dụng standard access-list thực hiện cấm tất cả dữ liệu từ PC2 và các PC trong mạng 200.200.200.0/24 đến tất cả Pc trong mạng 172.16.0.254/16



Cấu hình:

Router R2:

hostname R2
interface Loopback0
ip address 162.16.0.1 255.255.0.0
interface FastEthernet0/0
ip address 172.16.0.254 255.255.0.0
ip access-group 1 out **<- lọc các gói đi ra khỏi cổng F0/0 của router**
interface Serial0/0
ip address 203.162.0.2 255.255.255.0
clockrate 64000
ip classless
ip route 192.168.0.0 255.255.255.0 203.162.0.1 **<- Cấu hình định tuyến tĩnh cho router**
ip route 200.200.200.0 255.255.255.0 203.162.0.1
access-list 1 deny 192.168.0.2 0.0.0.0 **<- Cấm PC2**

access-list 1 deny 200.200.200.0 0.0.0.255 <- **Cấm tất cả PC trong mạng 200**
access-list 1 permit any <- **phải có lệnh này vì mặc định cuối access-list sẽ là cấm tất cả (deny)**

Router R1:

hostname R1
interface Loopback0
ip address 200.200.200.1 255.255.255.0
interface FastEthernet0/0
ip address 192.168.0.254 255.255.255.0
interface Serial0/0
ip address 203.162.0.1 255.255.255.0
ip route 162.16.0.0 255.255.0.0 203.162.0.2
ip route 172.16.0.0 255.255.0.0 203.162.0.2

Thực hiện:

Hai bước để cấu hình access list trên router:
1. Tạo access list tại global config mode:
Tạo access-list trên R2 cấm PC2 và mạng 200.200.200.0/24.

R2(config)# access-list 1 deny 192.168.0.2 0.0.0.0
R2(config)# access-list 1 deny 200.200.200.0 0.0.0.255
R2(config)# access-list 1 permit any

2. Áp access-list vào cổng
–Áp access-list này vào chiều ra của cổng F0/0 trên R2.
–Khi áp access-list vào một cổng, xem như đang trên router. Vì vậy nếu muốn cấm dữ liệu đi ra khỏi cổng, ta dùng từ khóa out; muốn cấm dữ liệu vào một cổng, ta dùng từ khóa in.
–Vì standard access-list chỉ kiểm tra được địa chỉ nguồn nên phải áp access-list vào cổng gần đích nhất.

R2(config)# cổng f0/0
R2(config-if)# ip access-group 1 out

Kiểm tra:

–Dùng extended ping trên R1, lấy địa chỉ nguồn là 200.200.200.1 hoặc 192.168.0.2 lệnh ping sẽ không thành công.

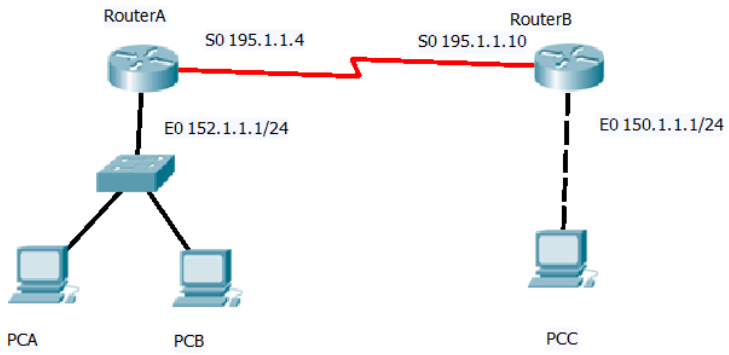
R1#ping 172.16.0.3
Sending 5, 100-byte ICMP Echos to 172.16.0.3, timeout is 2 seconds:
U.U.U <- **không thể tới được (Unreachable)**
Success rate is 0 percent (0/5)
–Lệnh ping không thành công do access-list đã hoạt động trên R2, kiểm tra các gói vào trên R2 bằng lệnh debug ip packet. Lưu ý rằng các gói bị loại bỏ bản tin ICMP host unreachable được gởi ngược trở lại R1:
R2#debug ip packet
IP packet debugging is on

R2#
IP: s=200.200.200.1 (Serial0/0), d=172.16.0.3 (FastEthernet0/0), len 100, access denied
IP: s=203.162.0.2 (local), d=200.200.200.1 (Serial0/0), len 56, sending <- **gởi bản tin ICMP host unreachable**

–Dùng extended ping trên R2 tới PC3, lấy địa chỉ nguồn là 162.16.0.1

R2#ping 172.16.0.3
Sending 5, 100-byte ICMP Echos to 172.16.0.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
–Có thể ping PC3 từ PC1 được do access–list chỉ cấm PC2 vào mạng 172.16.0.0/24
C:\Windows\Desktop>ping 172.16.0.3
Pinging 172.16.0.3 with 32 bytes of data:
Reply from 172.16.0.3: bytes=32 time=18ms TTL=126
Reply from 172.16.0.3: bytes=32 time=18ms TTL=126
Reply from 172.16.0.3: bytes=32 time=18ms TTL=126
Reply from 172.16.0.3: bytes=32 time=18ms TTL=126

Bài 2: LAB EXTENDED ACCESS-LIST



Mô tả:

– Lab này mô tả cách lọc các gói sử dụng extended access-list. Router A cho phép tất cả lưu lưu lượng từ PCC (150.1.1.2) đến PCA (152.1.1.2) và từ chối tất cả các lưu lượng từ PCC (150.1.1.2) tới PCB (152.1.1.3). Extened Access-list được sử dụng vì cần lọc trên cả địa chỉ IP nguồn và đích.
–Router A và RouterB nối bằng đường serial và đặt địa chỉ IP như trên hình. RouterA và RouterB có địa chỉ IP secondary tạo trên cổng Ethernet để làm điểm kiểm tra.

–Access-list được dùng để lọc ngõ vào trên cổng serial của RouterA, cho phép các gói từ PCC 150.1.1.2 tới PCA và không cho phép các gói từ PCC tới PCB.
Cấu hình:

Router A:

hostname RouterA
no ip domain-lookup
interface Ethernet0
ip address 152.1.1.2 255.255.255.0 secondary ← **Địa chỉ IP thứ hai để làm điểm kiểm tra**
ip address 152.1.1.3 255.255.255.0 secondary
ip address 152.1.1.1 255.255.255.0
no keepalive ← **vô hiệu hóa keepalive trên router cho phép cổng ethernet0 vẫn up khi không kết nối ra bên ngoài**
interface Serial0
ip address 195.1.1.4 255.255.255.0
ip access-group 100 in ← **Dùng Access-list 100 cho tất cả lưu lượng vào trên đường serial0**
no ip classless
ip route 150.1.1.0 255.255.255.0 Serial0 ← **dùng định tuyến tĩnh (không dùng định tuyến động)**
ip route 151.1.1.1 255.255.255.255 Serial0
access-list 100 permit ip host 150.1.1.2 host 152.1.1.2 log ← **tổng hợp các bản tin thông tin về các gói thoả điều kiện.**
access-list 100 deny ip host 150.1.1.2 host 152.1.1.3 log ← **Loại tất cả các gói IP từ 150.1.1.2 tới 152.1.1.3; tổng hợp bản tin thông báo về các gói thoả điều kiện.**
(Chú ý: tất cả các gói khác ngầm hiểu là bị loại bỏ; tất cả các access list đều kết thúc bằng câu lệnh loại bỏ tất cả)

Router B:

hostname RouterB
interface Loopback0
ip address 150.1.1.1 255.255.255.255
interface Ethernet0
ip address 150.1.1.2 255.255.255.0 secondary
ip address 150.1.1.1 255.255.255.0
no keepalive
interface Serial0
ip address 195.1.1.10 255.255.255.0
clock rate 64000
no ip classless
ip route 152.1.1.0 255.255.255.0 Serial0

Chú ý:Khi tạo access list tất cả các mục tuần tự theo thứ tự như khi ta đánh vào. Tất cả các câu lệnh thêm vào sau đó sẽ đặt ở vị trí tiếp của access list. Cuối access list luôn có câu lệnh loại bỏ tất cả, do đó một access list phải có ít nhất một lệnh permit. Tốt nhất là soạn thảo access list trước (dùng Notepad chẳng hạn) sau đó cut và paste vào CLI của router.

Kiểm tra:

- Sử dụng ping mở rộng (extended ping) trên RouterB hướng gói tới các địa chỉ IP secondary tạo ra trong cấu hình dùng địa chỉ nguồn khác nhau (cách này dùng thay cho nhiều PC ở trong mạng LAN của RouterA và RouterB).

1. Từ RouterB, ping 152.1.1.3 dùng nguồn là 1501.1.2

–Dùng lệnh debug ip packet trên RouterA, ta thấy các gói bị loại bỏ và bản tin ICMP host unreachable được gởi

IP: s=150.1.1.2 (Serial0), d=152.1.1.3, len 100, access denied

IP: s=195.1.1.4 (local), d=150.1.1.2 (Serial0), len 56, sending ← ICMP host unreachable

–Dùng lệnh show ip access-list trên RouterA. Chú ý các dòng hiển thị chỉ loại access list và số các điều kiện thoả của mỗi mục.

RouterA#show ip access-lists

Extended IP access list 100

permit ip host 150.1.1.2 host 152.1.1.2 log (5 matches)

deny ip host 150.1.1.2 host 152.1.1.3 log (105 matches)

–Tùy chọn log sẽ tổng hợp các bản tin thông báo mọi gói thoả điều kiện. Từ khóa log được đặt ở cuối câu lệnh access-list. Bản tin logging là công cụ tốt để kiểm soát lỗi access list.

SEC-6-IPACCESSLOGDP: list 100 denied icmp 150.1.1.2 -> 152.1.1.3 (0/0). 4 packets

2. Từ RouterB, ping 152.1.1.3 dùng nguồn 150.1.1.2

–Tại RouterA, lệnh debug ip packet hiển thị trên RouterA, ta có thể thấy các gói được cho phép.

IP: s=150.1.1.2 (Serial0), d=152.1.1.2, len 100, rcvd 7

–Dùng lệnh show ip access-list để xem số lượng các gói thoã điều kiện.

RouterA# show ip access-lists

Extended IP access list 100

permit ip host 150.1.1.2 host 152.1.1.2 log (308 matches)

deny ip host 150.1.1.2 host 152.1.1.3 log

CHƯƠNG 6 : VIRUS VÀ CÁCH PHÒNG CHỐNG

Mã chương: MH26-06

Mục tiêu:

- Mô tả được virus máy tính;
- Trình bày được cách thức lây lan của virus máy tính;
- Phân biệt được các loại virus;
- Phòng ngừa được sự xâm nhập của virus;
- Thực hiện các thao tác an toàn với máy tính.

1. Giới thiệu tổng quan về virus tin học

Mục tiêu:

- Mô tả được virus máy tính

Căn cứ vào tính chất của đoạn mã phá hoại, có thể chia thành hai loại: virus và Trojan horse.

- Trojan horse: Thuật ngữ này dựa vào một điển tích cổ, chỉ một đoạn mã được "cắm" vào bên trong một phần mềm, cho phép xuất hiện và ra tay phá hoại một cách bất ngờ như những anh hùng xông ra từ bụng con ngựa thành Troa. Trojan horse là một đoạn mã HOÀN TOÀN KHÔNG CÓ TÍNH CHẤT LÂY LAN, chỉ nằm trong những phần mềm nhất định. Đoạn mã này sẽ phá hoại vào một thời điểm xác định, có thể được tác giả định trước và đối tượng của chúng là thông tin trên đĩa như format lại đĩa, xóa FAT, Root,..Thông thường các phần mềm có chứa Trojan horse được phân phối như là các phiên bản bổ sung hay mới và điều này sẽ trừng phạt những người thích sao chép phần mềm ở những nơi có nguồn gốc không xác định.

- Virus tin học: thuật ngữ này nhằm chỉ một chương trình máy tính có thể tự sao chép chính nó lên những đĩa, file khác mà người sử dụng không hay biết. Thông thường virus cũng mang tính phá hoại, nó sẽ gây ra lỗi thi hành, lệch lạc hay hủy dữ liệu,… bắt đầu lịch sử lây nhiễm của nó trên máy tính lớn vào năm 1970. Sau đó chúng xuất hiện trên máy PC vào năm 1986 và "liên tục phát triển" thành một lực lượng hùng hậu cùng với sự phát triển của họ máy tính cá nhân. Người ta thường thấy chúng thường xuất hiện ở các trường đại học, nơi tập trung các sinh viên giỏi và hiếu động. Dựa vào các phương tiện giao tiếp máy tính (mạng, đĩa...), chúng lan truyền và có mặt khắp nơi trên thế giới với số lượng đông không kể xiết. Có thể nói rằng nơi nào có máy tính, nơi đó có virus tin học.

- Internet Worm: là một bước tiến đáng kể của virus. Worm kết hợp cả sức phá hoại của virus, sự bí mật của Trojan và sự lây lan rất mạnh mà những kẻ viết virus trang bị cho nó. Ví dụ tiêu biểu là worm Mellisa hay Love Letter, với sự lây lan đáng sợ, chúng đã làm tê liệt hàng loạt các hệ thống máy chủ, làm ách tắc đường truyền. Worm thường phát tán bằng cách tìm các địa chỉ trong sổ địa chỉ (Address book) của máy mà nó đang lây nhiễm, ở đó thường là địa chỉ của bạn bè, người thân, khách hàng... của chủ máy. Tiếp đến, nó tự gửi bản sao của nó cho những địa chỉ mà nó tìm thấy. Với cách hoàn toàn tương tự trên những máy nạn nhân, Worm có thể nhanh chóng lây lan trên toàn cầu theo cấp số nhân, điều đó lý giải tại sao chỉ trong vòng vài tiếng đồng hồ mà Mellisa và Love

Letter lại có thể lây lan tới hàng chục triệu máy tính trên toàn cầu. Với sự lây lan nhanh và rộng lớn như vậy, Worm thường được kẻ viết ra chúng cài thêm nhiều tính năng đặc biệt, chẳng hạn như chúng có thể định cùng một ngày giờ và đồng loạt từ các máy nạn nhân tấn công vào một địa chỉ nào đó, làm cho máy chủ có thể bị tê liệt. Ngoài ra, chúng còn có thể cho phép chủ nhân của chúng truy nhập vào máy của nạn nhân và có thể làm đủ mọi thứ như ngồi trên máy đó một cách bất hợp pháp.

Theo thống kê 10 virus nguy hiểm nhất tháng 3/2005, nằm ở vị trí số 1, Zafi.D chiếm 45,1% tỷ lệ lây nhiễm trong tháng 3/2005. Ngôi vị "á quân" thuộc về Netsky.P với tỷ lệ lây nhiễm 21%.

Xuất hiện vào cuối năm 2004, Zafi.D liên tục đứng đầu danh sách các virus nguy hiểm nhất trong tháng theo bình chọn của Sophos. Mới xuất hiện trong xếp hạng tháng 3 là Sober.K- virus lây nhiễm thông qua các tệp tin đính kèm email mang tiêu đề 'You visit illegal websites' hoặc 'Alert! New Sober Worm!'.

Theo chuyên gia bảo mật của Sophos, hơn một nghìn virus và các đoạn mã nguy hiểm đã xuất hiện trong tháng 3. Để phòng ngừa, người sử dụng máy tính nên nắm chắc các hướng dẫn về bảo mật và thường xuyên theo dõi thông tin về cách phòng chống những virus mới.

Zafi.D	45,1%
Netsky.P	21%
Zafi.B	5,9%
Sober.K	5,8%
Netsky.D	4,3%
Netsky.Z	2,7%
Netsky.B	2,3%
MyDoom.O	1,3%
Netsky.C	1,1%
Netsky.Q	1,0%
Loại khác	9,5%

2. Cách thức lây lan – phân loại

Mục tiêu:

- Trình bày được cách thức lây lan của virus máy tính;

- Phân biệt được các loại virus;

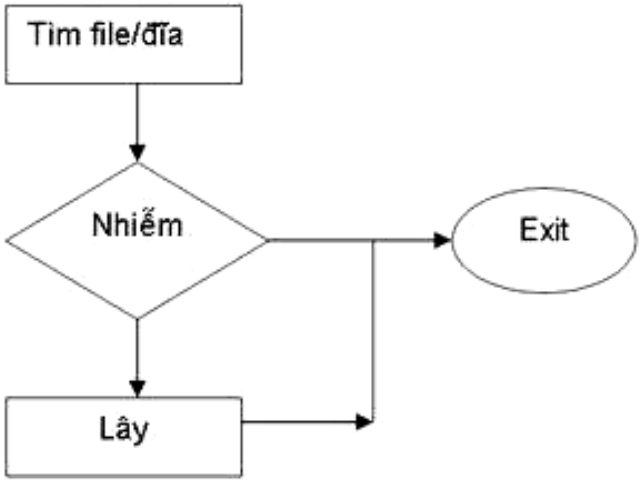
Dựa vào đối tượng lây lan là file hay đĩa, chia virus thành hai nhóm chính:

- B-virus (boot virus): Virus chỉ tấn công trên các Boot sector hay Master boot.

- F-virus (file virus): Virus chỉ tấn công lên các file thi hành được (dạng có thể thi hành bằng chức năng 4Bh của DOS hơn là những file dạng .COM hay .EXE)

Cách phân loại này chỉ mang tính tương đối, vì trên thực tế có những loại virus lưỡng tính vừa lây trên boot record, vừa trên file thi hành.

Dạng tổng quát của một virus có thể biểu diễn bằng sơ đồ sau:



Như đã giới thiệu về định nghĩa virus, đoạn mã này một lúc nào đó phải được trao quyền điều khiển. Như vậy, rõ ràng virus phải khai thác một chỗ hở nào đó mà máy 'tự nguyện' trao quyền điều khiển lại cho nó. Thực tế có hai khe hở, sẽ lần lượt xét dưới đây.

1. B-virus

Lây vào các mẫu tin khởi động bao gồm:

- Master boot của đĩa cứng.

- Boot sector của đĩa cứng và đĩa mềm.

B-virus chỉ có thể được kích hoạt khi ta khởi động máy tính bằng đĩa nhiễm. Lúc này hệ thống chưa được một hệ điều hành (HĐH) nào kiểm soát, do đó B-virus có thể khống chế hệ thống bằng cách chiếm các ngắt của BIOS, chủ yếu là Int 13 (phục vụ đĩa), Int 8 (đồng hồ). Nhờ đặc điểm này mà nó có khả năng lây trên mọi Hệ điều hành. Nếu một B-virus được thiết kế nhằm mục đích phá hoại thì đối tượng chính của chúng là đĩa và các thành phần của đĩa. Để mở rộng tầm hoạt động, một số loại còn có khả năng tấn công lên file khi quá trình khởi động của Hệ điều hành hoàn tất, nhưng đó chỉ là những trường hợp ngoại lệ, có hành vi phá hoại giống như F-virus.

Chúng ta sẽ xem xét từng thành phần chính của đĩa, bao gồm master boot, boot sector, bảng FAT, bảng Thư mục, Vùng dữ liệu...

a. Master boot

Master boot chỉ có mặt trên đĩa cứng, nằm tại sector 1, track 0, side 0. Ngoài đoạn mã tìm HĐH trên đĩa, master boot còn chứa Partition table. Đây là một bảng tham số nằm tại offset 1BEh, ghi nhận cấu trúc vật lý, địa chỉ bắt đầu và kết thúc mỗi partition, partition nào chứa hệ điều hành hoạt động... Các thông tin này rất quan trọng, hệ thống sẽ rối loạn hoặc không thể nhận dạng đĩa cứng nếu chúng bị sai lệch.

Khi ghi vào master boot, virus thường giữ lại Partition table. Do đó để diệt B-virus, ta chỉ cần cập nhật lại master boot. Có thể dùng lệnh FDISK / MBR cho mục đích nói trên.

b. Boot Sector

Giống như master boot, khi ghi vào boot sector, B-virus thường giữ lại bảng tham số đĩa (BPB-BIOS Parameter Block). Bảng này nằm ở offset 0Bh của boot sector, chứa các thông số quan trọng như dấu hiệu nhận dạng loại đĩa, số bảng FAT, số sector dành cho bảng FAT, tổng số sector trên đĩa... Có thể phục hồi boot sector bằng lệnh SYS.COM của DOS. Một số virus phá hỏng BPB khiến cho hệ thống không đọc được đĩa trong môi trường sạch (và lệnh SYS cũng mất tác dụng). Đối với đĩa mềm, việc phục hồi boot sector (bao gồm BPB) khá đơn giản vì chỉ có vài loại đĩa mềm thông dụng (360KB, 720KB, 1.2 MB, 1.44 MB), có thể lấy boot sector bất kỳ của một đĩa mềm cùng loại để khôi phục BPB mà không cần format lại toàn bộ đĩa. Tuy nhiên vấn đề trở nên phức tạp hơn trên đĩa cứng: BPB của đĩa được tạo ra trong quá trình FDISK dựa trên các tùy chọn của người dùng cũng như các tham số phục vụ cho việc phân chia đĩa. Trong một số trường hợp, phần mềm NDD có thể phục hồi BPB cho đĩa cứng, nhưng do trước đó máy phải khởi động từ A (vì BPB của đĩa cứng đã hư, không khởi động được), nên việc quản lý các phần tiếp theo của đĩa sẽ gặp nhiều khó khăn. Tốt nhất nên lưu lại boot sector của đĩa cứng để có thể phục hồi chúng khi cần thiết.

c. Bảng FAT (File Allocation Table)

Được định vị một cách dễ dàng ngay sau boot sector, FAT là một "miếng mồi ngon" cho virus. Đây là bảng ghi nhận trật tự lưu trữ dữ liệu theo đơn vị liên cung (cluster) trên đĩa ở vùng dữ liệu của DOS. Nếu hỏng một trong các mắt xích của FAT, dữ liệu liên quan sẽ không truy nhập được. Vì tính chất quan trọng của nó, FAT luôn được DOS lưu trữ thêm một bảng dự phòng nằm kề bảng chính. Tuy nhiên các virus đủ sức định vị FAT khiến cho tính cẩn thận của DOS trở nên vô nghĩa. Mặt khác, một số DB-virus (Double B-virus) thường chọn các sector cuối của FAT để lưu phần còn lại của progvi. Trong đa số trường hợp, người dùng thường cầu cứu các chương trình chữa đĩa, nhưng những chương trình này chỉ có thể định vị các liên cung thất lạc, phục hồi một phần FAT hỏng... chứ không thể khôi phục lại toàn bộ từ một bảng FAT chỉ chứa toàn "rác". Hơn nữa thông tin trên đĩa luôn biến động, vì vậy không thể tạo một bảng FAT "dự phòng" trên đĩa mềm như đối với master boot và boot sector được. Cách tốt nhất vẫn là sao lưu dự phòng tất cả dữ liệu quan trọng bằng các phương tiện lưu trữ tin cậy.

d. Bảng Thư mục (Root directory)

Ngay sau FAT là bảng Thư mục chứa các tên hiển thị trong lệnh DIR\, bao gồm nhãn đĩa, tên file, tên thư mục. Mỗi tên được tổ chức thành entry có độ dài 32byte, chứa tên entry, phần mở rộng, thuộc tính, ngày giờ, địa chỉ lưu trữ, kích thước (nếu entry đặc tả tên file).

DOS qui định một thư mục sẽ kết thúc bằng một entry bắt đầu với giá trị 0. Vì vậy để vô hiệu từng phần Root, virus chỉ cần đặt byte 0 tại một entry nào đó.

Nếu byte này được đặt ở đầu Root thì cả đĩa sẽ trống rỗng một cách thảm hại! Trường hợp DB_virus chọn các sector cuối của Root để lưu phần còn lại của progvi cũng gây hậu quả giống như trường hợp bảng FAT: nếu vùng này đã được DOS sử dụng, các entry trên đó sẽ bị phá hủy hoàn toàn.

Vì số lượng các entry trên Root có hạn, DOS cho phép ta tạo thêm thư mục con để mở rộng các entry ra vùng dữ liệu. Chính vì thế nội dung của Root thường ít biến động do chỉ chứa các file hệ thống như IO.SYS, MSDOS.SYS, COMMAND.COM, CONFIG .SYS, AUTOEXEC.BAT, các tên thư mục nằm ở gốc... Do đó ta có thể tạo một bản Root dự phòng, với điều kiện sau đó không thay đổi/cập nhật bất cứ một entry nào. Điều này sẽ không cần thiết trên hệ thống có áp dụng các biện pháp sao lưu dữ liệu định kỳ.

e. Vùng dữ liệu

Đây là vùng chứa dữ liệu trên đĩa, chiếm tỷ lệ lớn nhất, nằm ngay sau Root. Ngoại trừ một số ít DB_virus sử dụng vài sector ở vùng này để chứa phần còn lại của progvi (xác suất ghi đè lên file rất thấp), vùng dữ liệu được coi như vùng có độ an toàn cao, tránh được sự "nhòm ngó" của B_virus. Chúng ta sẽ lợi dụng đặc điểm này để bảo vệ dữ liệu khỏi sự tấn công của B_virus (chủ yếu vào FAT và Root, hai thành phần không thể tạo bản sao dự phòng).

Khi thực hiện quá trình phân chia đĩa bằng FDISK, đa số người dùng có thói quen khai báo toàn bộ đĩa cứng chỉ cho một partition duy nhất, cũng chính là đĩa khởi động của hệ thống. Việc sử dụng một ổ đĩa luận lý. Ví dụ ta chia đĩa cứng làm hai ổ luận lý C và D, ổ C (chứa boot sector của hệ điều hành) chỉ dùng để khởi động, các tiện ích, phần mềm có thể cài đặt lại một cách dễ dàng, riêng ổ D dùng chứa dữ liệu quan trọng. Khi FAT, Root của đĩa cứng bị B_virus tấn công, ta chỉ cần cài đặt lại các phần mềm trên C mà không sợ ảnh hưởng đến dữ liệu trên D. Nếu đĩa cứng đủ lớn, ta nên chia chúng theo tỷ lệ 1:1 (hoặc 2:3) để nâng cao hiệu quả sử dụng. Với những đĩa cứng nhỏ, tỷ lệ này không đáp ứng được nhu cầu lưu trữ của các phần mềm lớn, do đó ta chỉ cần khai báo đĩa C với kích thước đủ cho hệ điều hành và các tiện ích cần thiết mà thôi. Lúc này tính kinh tế phải nhường chỗ cho sự an toàn.

Tuy nhiên giải pháp này chỉ mang tính tương đối, vì nếu tồn tại một B_virus có khả năng tự định vị địa chỉ vật lý của partition thứ hai để phá hoại thì vấn đề sẽ không đơn giản chút nào.

2. F-virus

Nếu như các B_virus có khả năng lây nhiễm trên nhiều HĐH và chỉ khai thác các dịch vụ đĩa của ROM BIOS, thì F_virus chỉ lây trên một HĐH nhất định nhưng ngược lại chúng có thể khai thác rất nhiều dịch vụ nhập xuất của HĐH đó. Các F_virus dưới DOS chủ yếu khai thác dịch vụ truy nhập file bằng các hàm của ngắt 21h. Một số ít sử dụng thêm ngắt 13h (hình thức phá hoại giống như B_virus), do đó ta chỉ cần xem xét các trường hợp dùng ngắt 21h của F_virus.

a. Lây vào file thi hành

Đặc điểm chung của F_virus là chúng phải đính progvi vào các tập tin thi hành dạng COM, EXE, DLL, OVL... Khi các tập tin này thi hành, F_virus sẽ khống chế vùng nhớ và lây vào tập thi hành khác. Do đó kích thước của các tập tin nhiễm bao giờ cũng lớn hơn kích thước ban đầu. Đây chính là dấu hiệu đặc trưng cơ bản để nhận dạng sự tồn tại của F_virus trên file thi hành. Để khắc phục nhược điểm này, một số F_virus giải quyết như sau:

- Tìm trên file các buffer đủ lớn để chèn progvi vào. Với cách này, virus chỉ có thể lây trên một số rất ít file. Để mở rộng tầm lây nhiễm, chúng phải tốn thêm giải thuật đính progvi vào file như các virus khác, và kích thước file lại tăng lên!

- Khống chế các hàm tìm, lấy kích thước file của DOS, gây nhiễu bằng cách trả lại kích thước ban đầu. Cách này khá hiệu quả, có thể che dấu sự có mặt của chúng trên file, nhưng hoàn toàn mất tác dụng nếu các tập tin nhiễm được kiểm tra kích thước trên hệ thống sạch (không có mặt virus trong vùng nhớ), hoặc bằng các phần mềm DiskLook như DiskEdit, PCTool...

- Lây trực tiếp vào cấu trúc thư mục của đĩa (đại diện cho loại này là virus Dir2/FAT). Cách này cho lại kích thước ban đầu rất tốt, kể cả trên môi trường sạch. Tuy nhiên ta có thể dùng lệnh COPY để kiểm tra sự có mặt của loại virus này trên thư mục. Hơn nữa, sự ra đời của Windows 95 đã cáo chung cho họ virus Dir2/FAT, vì với mục đích bảo vệ tên file dài hơn 13k

Như vậy việc phát hiện F_virus trên file chỉ phụ thuộc vào việc giám sát thường xuyên kích thước file. Để làm điều này, một số chương trình AntiVirus thường giữ lại kích thước ban đầu làm cơ sở đối chiếu cho các lần duyệt sau. Nhưng liệu kích thước được lưu có thật sự là "ban đầu" hay không? AntiVirus có đủ thông minh để khẳng định tính trong sạch của một tập tin bất kỳ hay không? Dễ dàng nhận thấy rằng các tập tin COM, EXE là đối tượng tấn công đầu tiên của F_virus. Các tập tin này chỉ có giá trị trên một hệ phần mềm nhất định mà người dùng bao giờ cũng lưu lại một bản dự phòng sạch. Vì vậy, nếu có đủ cơ sở để chắc chắn về sự gia tăng kích thước trên các tập tin thi hành thì biện pháp tốt nhất vẫn là khởi động lại máy bằng đĩa hệ thống sạch, sau đó tiến hành chép lại các tập thi hành từ bộ dự phòng.

b. Nhiễm vào vùng nhớ

Khi lây vào các file thi hành, F_virus phải bảo toàn tính logic của chủ thể. Do đó sau khi virus thực hiện xong các tác vụ thường trú, file vẫn chạy một cách bình thường. Việc thường trú của F_virus chỉ làm sụp đổ hệ thống (là điều mà F_virus không mong đợi chút nào) khi chúng gây ra những xung đột về tính nhất quán của vùng nhớ, khai thác vùng nhớ không hợp lệ, làm rối loạn các khối/trình điều khiển thiết bị hiện hành... Các sự cố này thường xảy ra đối với phần mềm đòi hỏi vùng nhớ phải được tổ chức nghiêm ngặt, hoặc trên các HĐH đồ sộ như Windows 95. Thực tế cho thấy khi F_virus nhiễm vào các file DLL (Dynamic Link Library - Thư viện liên kết động) của Windows 95, HĐH này không thể khởi động được. Trong những trường hợp tương tự, chúng ta thường tốn khá nhiều công sức và tiền bạc để cài đặt lại cả bộ Windows 95 mà không đủ kiên nhẫn tìm ra nguyên nhân hỏng hóc ở một vài EXE, DLL nào đó.

Khi thường trú, F_virus luôn chiếm dụng một khối nhớ nhất định và khống chế các tác vụ nhập xuất của HĐH. Có thể dùng các trình quản lý

Có một khám phá thú vị cho việc bảo vệ hệ thống khỏi sự lây nhiễm của F_virus trong vùng nhớ là chạy các ứng dụng DOS (mà bạn không chắc chắn về sự trong sạch của chúng) dưới nền Windows 95. Sau khi ứng dụng kết thúc, HĐH này sẽ giải phóng tất cả các trình thường trú cổ điển (kể cả các F_virus) nếu như chúng được sử dụng trong chương trình. Phương pháp này không cho F_virus thường trú sau Windows 95, nhưng không ngăn cản chúng lây vào các file thi hành khác trong khi ứng dụng còn hoạt động.

c. Phá hoại dữ liệu

Ngoài việc phá hoại đĩa bằng Int 13h như B_virus, F_virus thường dùng những chức năng về file của Int 21h để thay đổi nội dung các tập tin dữ liệu như văn bản, chương trình nguồn, bảng tính, tập tin cơ sở dữ liệu, tập tin nhị phân ... Thông thường virus sẽ ghi "rác" vào file, các dòng thông báo đại loại "File was destroyed by virus..." hoặc xóa hẳn file. Đôi khi đối tượng phá hoại của chúng lại là các phần mềm chống virus đang thịnh hành. Vì file bị ghi đè (overwrite) nên ta không thể phục hồi được dữ liệu về tình trạng ban đầu. Biện pháp tốt nhất có thể làm trong trường hợp này là ngưng ngay các tác vụ truy nhập file, thoát khỏi chương trình hiện hành, và diệt virus đang thường trú trong vùng nhớ.

3. Macro virus

Thuật ngữ "Macro virus" dùng để chỉ các chương trình sử dụng lệnh macro của Microsoft Word hoặc Microsoft Excel. Khác với F_virus truyền thống chuyên bám vào các file thi hành, Macro virus bám vào các tập tin văn bản .DOC và bảng tính .XLS. Khi các tập tin này được Microsoft Word (hoặc Microsoft Excel) mở ra, macro sẽ được kích hoạt, tạm trú vào NORMAL.DOT, rồi lây vào tập DOC, XLS khác. Đây là một hình thức lây mới, tiền thân của chúng là macro Concept. Tuy ban đầu Concept rất "hiền" nhưng do nó không che dấu kỹ thuật lây này nên nhiều hacker khác dễ dàng nắm được giải thuật, hình thành một lực lượng virus "hậu Concept" đông đúc và hung hãn.

Mối nguy hiểm của loại virus này thật không lường. Chúng lợi dụng nhu cầu trao đổi dữ liệu (dưới dạng văn thư, hợp đồng, biên bản, chứng từ...) trong thời đại bùng nổ thông tin để thực hiện hành vi phá hoại. Có trường hợp một văn bản thông báo của công ty X được gửi lên mạng lại chứa macro virus. Dù chỉ là sự vô tình nhưng cũng gây nhiều phiền toái, chứng tỏ tính phổ biến và nguy hại của loại virus "hậu sinh khả úy".

Đặc biệt, một biến thể của macro virus có hình thức phá hoại bằng "bom thư tin học" vừa được phát hiện trong thời gian gần đây. Tên "khủng bố" gửi đến địa chỉ "nạn nhân" một bức thư dưới dạng tập tin .DOC. Người nhận sẽ gọi WinWord để xem, thế là toàn bộ đĩa cứng sẽ bị phá hoại. Hậu quả sau đó đã rõ, mọi dữ liệu trên đĩa cứng đều bị mất.

Tuy cùng sử dụng macro của Microsoft Word để thực hiện hành vi xấu nhưng hình thức phá hoại của loại này khác với virus. Virus chỉ phá hoại dữ liệu của máy tính một cách ngẫu nhiên, tại những địa chỉ không xác định. "Bom thư tin

học" nhằm vào những địa chỉ cụ thể, những cơ sở dữ liệu mà chúng biết chắc là vô giá. Cũng không loại trừ khả năng chúng mạo danh một người nào đó để thực hiện âm mưu với dụng ý "một mũi tên trúng hai mục tiêu". Chúng ta phải tăng cường cảnh giác.

Để phòng chống loại virus macro này, khi sử dụng một tập tin .DOC, .XLS bạn phải chắc chắn rằng chúng không chứa bất kỳ một macro lạ nào (ngoài các macro do chính bạn tạo ra). Ngoại trừ hình thức phá hoại kiểu "bom thư", macro virus thường đếm số lần kích hoạt mới thực hiện phá hoại (để chúng có thời gian lây). Vì vậy khi mở tập tin, bạn hãy chọn menu Tool/Macro (của WinWord) để xem trong văn bản có macro lạ hay không (kể cả các macro không có tên). Nếu có, đừng ngần ngại xóa chúng ngay. Sau đó thoát khỏi WinWord, xóa luôn tập tin NORMAL.DOT. Một số Macro virus có khả năng mã hóa progvi, che dấu menu Tool/Macro của WinWord, hoặc không cho xóa macro..., đó là những dấu hiệu chắc chắn để tin rằng các macro virus đang rình rập xâu xé dữ liệu của bạn. Hãy cô lập ngay tập tin này và gửi chúng đến địa chỉ liên lạc của các AntiVirus mà bạn tin tưởng.

4. Trojan

Trojan là gì?

Trojan là một mã độc hại có khả năng thực hiện những tác vụ bất hợp pháp, thường là độc hại. Bản thân của Trojan là một chương trình bất hợp pháp nhưng lại được che giấu trong một chương trình hợp pháp. Khác nhau lớn nhất giữa Trojan và virus là khả năng nhân bản: Trojan có thể gây thiệt hại cho máy tính, khởi tạo các lỗi hệ thống, thậm chí là gây mất mát dữ liệu... nhưng nó lại không có khả năng nhân bản giống virus. Ngược lại, một khi Trojan có khả năng nhân bản thì nó sẽ được phân loại thành virus.

Trojan được lấy tên từ một câu chuyện thần thoại cũ về những người Hy Lạp trong thời gian chiến tranh. Họ đã tặng cho kẻ thù một con ngựa làm bằng gỗ khổng lồ. Kẻ thù của những người Hy Lạp đã chấp nhận món quà tặng và mang nó vào trong thành. Ngay trong đêm đó, những người lính Hy Lạp đã chui ra khỏi con ngựa và tấn công thành, gây bất ngờ cho kẻ thù và đã chiếm được thành sau đó một thời gian ngắn.

Trojan còn có 1 loại nữa gọi là Trojan 'chiếm quyền kiểu leo thang', thường được sử dụng đối với các administrator (quản trị viên) kém cỏi. Chúng có thể được nhúng vào một ứng dụng hệ thống và khi được quản trị viên kích hoạt, chúng sẽ tạo cho hacker quyền cao hơn trong hệ thống. Những con Trojan này có thể được gửi tới những người dùng có ít quyền và cho họ quyền xâm nhập hệ thống .

Ngoài ra, còn có một số loại Trojan nữa, trong đó bao gồm cả những chương trình tạo ra chỉ để chọc ghẹo, không có hại. Các thông báo của những Trojan này thường là: 'Ổ cứng của bị sẽ bị format', hoặc 'password của bạn đã bị lộ'...

Theo những thống kê không đầy đủ, hiện có gần 2.000 loại Trojan khác nhau. Đây chỉ là 'phần nổi của tảng băng' vì thực chất số lượng các loại Trojan là rất lớn, vì mỗi hacker, lập trình viên hay mỗi nhóm hacker đều viết Trojan cho

riêng mình và những con Trojan này sẽ không được công bố lên mạng cho đến khi nó bị phát hiện. Chính vì số lượng cực kỳ đông đảo, nên Trojan luôn luôn là vấn đề lớn trong bảo mật và an toàn trên mạng.

Người dùng có an toàn trước Trojan bằng phần mềm diệt virus

Có rất nhiều người nghĩ rằng họ có thể an toàn khi có trong tay một chương trình quét virus tốt với bản cập nhật mới nhất, rằng máy tính của họ hoàn toàn 'miễn dịch' trước Trojan. Thật không may, thực tế lại không hoàn toàn đúng như vậy. Mục đích của những viết chương trình diệt virus là phát hiện ra những virus mới chứ không phải là những con Trojan. Và chỉ khi những con Trojan được nhiều người biết đến, các chuyên viên viết phần mềm diệt virus mới bổ sung nó vào chương trình quét virus. Vì thế, một điều hiển nhiên là các phần mềm diệt virus đành 'bó tay' trước những con Trojan chưa từng biết đến.

Cách thức lây nhiễm của Trojan

- Từ Mail: Trojan lây nhiễm theo con đường này thường có tốc độ lây lan rất nhanh. Khi chúng 'chui' vào máy tính của nạn nhân, việc đầu tiên các Trojan này làm là 'gặt hái' địa chỉ mail trong address book rồi phát tán theo các địa chỉ đó.

- Từ ICQ: Nhiều người biết rằng ICQ là kênh truyền thông tin rất tiện lợi, tuy nhiên lại không biết rằng nó là môi trường kém an toàn nhất vì người đối thoại có thể gửi Trojan trong lúc đang nói chuyện với nhau. Điều này hoàn toàn có thể thực hiện nhờ một lỗi (bug) trong ICQ, cho phép gửi file ở dạng .exe nhưng người nhận là thấy chúng có vẻ như là các file ở dạng âm thanh, hình ảnh... Để ngăn ngừa được bug này, trước khi mở file bạn phải luôn kiểm tra kiểu file (tức là phần mở rộng của file để biết nó thuộc loại nào).

- Từ IRC: Cách lây nhiễm cũng tương tự như ICQ.

Mức độ nguy hiểm của Trojan

Khi Trojan lây nhiễm vào máy tính nạn nhân, người dùng hầu như không cảm thấy có điều gì bất thường. Tuy nhiên, sự nguy hiểm lại phụ thuộc vào quyết định của hacker - tác giả của con Trojan đó. Đặc biệt, mức độ nguy hiểm sẽ trầm trọng hơn nếu máy tính nạn nhân là nơi lưu trữ tài liệu mật của các tổ chức, công ty hoặc tập đoàn lớn. Hacker có thể sẽ sao chép và khai thác nguồn tài liệu đó, hoặc cũng có thể sẽ xóa chúng đi.

Phân loại Trojan

Hiện nay có rất nhiều trojan, nhưng có thể phân ra các loại cơ bản sau dựa vào tính chất của chúng:

- Trojan dùng để truy cập từ xa: một khi những con Trojan này nhiễm vào hệ thống, nó sẽ gửi các username (tên đăng nhập), password (mật khẩu), và địa chỉ IP của máy tính đó cho hacker. Từ những tài nguyên này, hacker có thể truy cập vào máy đó đó bằng chính username và password lấy được.

- Trojan gửi mật khẩu: đọc tất cả mật khẩu lưu trong cache và thông tin về máy nạn nhân rồi gửi về cho hacker mỗi khi nạn nhân online.

- Trojan phá hủy sự tai hại của loại Trojan này đúng như cái tên của nó, chúng chỉ có một nhiệm vụ duy nhất là tiêu diệt tất cả file trên máy tính nạn nhân (file

.exe, .dll, .ini ...). Thật 'bất hạnh' cho những máy tính nào bị nhiễm con Trojan này, vì khi đó tất cả các dữ liệu trên máy tính sẽ chẳng còn gì.

- FTP Trojan: loại này sẽ mở cổng 21 trên máy của nạn nhân để mọi người có thể kết nối tới mà không cần mật khẩu và họ sẽ toàn quyền tải bất kỳ dữ liệu nào xuống.

- Keylogger: phần mềm này sẽ ghi lại tất cả các tác vụ bàn phím khi nạn nhân sử dụng máy tính, và gửi chúng cho hacker theo địa chỉ e-mail.

5. Sâu - worm

Mọi sự tập trung hiện nay được hướng vào MSBlaster Worm và SoBig Virus bởi sức lây lan của nó. Trong khi Melissa Virus trở thành hiện tượng toàn cầu vào tháng 3 năm 1999 khi nó buộc Microsoft và hàng loạt công ty khác phải ngắt hệ thống E-mail của họ khỏi mạng cho đến khi Virus này được ngăn chặn thì ILOVEYOU Virus xuất hiện trong năm 2000 cũng có sức tàn phá không kém. Thật không ngờ khi con người nhận ra rằng cả Melissa và ILOVEYOU đều hết sức đơn giản.

Worm là một chương trình máy tính có khả năng tự sao chép từ máy tính này sang máy tính khác. Worm thường lây nhiễm sang các máy tính khác nhau qua mạng máy tính. Qua mạng máy tính, Worm có thể phát triển cực nhanh từ một bản sao. Chẳng hạn chỉ trong chín giờ đồng hồ ngày 19/7/2001, CodeRed Worm đã nhân bản lên tới 250.000 lần. Worm thường khai thác những điểm yếu về bảo mật của các chương trình hoặc hệ điều hành. Slammer Worm đã khai thác lỗ hổng bảo mật của Microsoft SQL Server trong khi nó chỉ là một chương trình cực nhỏ (376Byte).

CodeRed Worm làm cho mạng Internet chậm đáng kể khi tận dụng băng thông mạng để nhân bản. Mỗi bản sao của nó tự dò tìm trong mạng Internet để tìm ra các Server sử dụng hệ điều hành Windows NT hay Windows 2000 chưa được cài các bản Patch sửa lỗi bảo mật. Mỗi khi tìm được một Server chưa được khắc phục lỗ hổng bảo mật, CodeRed Worm tự sinh ra một bản sao của nó và ghi vào Server này. Bảo sao mới của nó lại tự dò tìm trên mạng để lây nhiễm sang các Server khác. Tùy thuộc vào số lượng các Server chưa được khắc phục lỗ hổng bảo mật, Worm có thể tạo ra hàng trăm ngàn bản sao.

CodeRed Worm được thiết kế để thực hiện 3 mục tiêu sau:

- Tự nhân bản trong 20 ngày đầu tiên của mỗi tháng.

- Thay trang Web của Server mà nó nhiễm bằng trang Web có nội dung “Hacked by Chinese”.

- Tấn công liên tục White House Web Server.

Các phiên bản của CodeRed luôn biến đổi liên tục. Sau khi nhiễm vào Server, Worm này sẽ chọn một thời điểm định sẵn và tấn công vào Domain www.whitehouse.gov. Các Server bị nhiễm sẽ đồng loạt gửi khoảng 100 kết nối tới cổng 80 của www.whitehouse.gov (198.137.240.91) khiến chính phủ Mỹ phải thay đổi IP của WebServer và khuyến cáo người sử dụng ngay lập tức phải nâng cấp WindowsNT và 2000 bằng các bản “vá” sửa lỗi.

6. Họ đa hình – polymorphic

Những virus họ này có khả năng tự nhân bản nhưng ngụy trang thành những biến thể khác với mẫu đã biết để tránh bị các chương trình diệt virus phát hiện.

Một chi của họ virus đa hình dùng các thuật toán mã hóa và giải mã khác nhau trên các hệ thống hoặc thậm chí bên trong các tệp khác nhau, làm cho rất khó nhận dạng. Một chi khác lại thay đổi trình tự các lệnh và dùng các lệnh giả để đánh lừa các chương trình diệt virus. Nguy hiểm nhất là mutant thì sử dụng các số ngẫu nhiên để thay đổi mã tấn công và thuật toán giải mã.

7. Họ lừa dọa - hoaxes

Đây không phải là virus mà chỉ là những thông điệp có vẻ như cảnh báo của một người nào đó tốt bụng nhưng nếu có nhiều người nhận nhẹ dạ cả tin lại gửi tiếp chúng đến những người khác thì có thể bùng lên một vụ lây lan đến mức nghẽn mạng và gây ra sự mất lòng tin. Trên thế giới có rất nhiều cơ sở dữ liệu cung cấp mẫu của các dạng thông điệp giả này và cần so sánh chúng với mỗi thông điệp cảnh báo vừa nhận được để khỏi bị lừa và tiếp tay cho tin tặc.

2. NGĂN CHẶN SỰ XÂM NHẬP

Mục tiêu:

- Phòng ngừa được sự xâm nhập của virus

Virus tin học tuy ranh ma và nguy hiểm nhưng có thể bị ngăn chặn và loại trừ một cách dễ dàng. Có một số biện pháp dưới đây

1. Chương trình diệt virus - Anti-virus

Dùng những chương trình chống virus để phát hiện và diệt virus gọi là anti-virus. Thông thường các anti-virus sẽ tự động diệt virus nếu phát hiện. Với một số chương trình chỉ phát hiện mà không diệt được, phải để ý đọc các thông báo của nó.

Để sử dụng anti-virus hiệu quả, nên trang bị cho mình một vài chương trình để sử dụng kèm, cái này sẽ bổ khuyết cho cái kia thì kết quả sẽ tốt hơn. Một điều cần lưu ý là nên chạy anti-virus trong tình trạng bộ nhớ tốt (khởi động máy từ đĩa mềm sạch) thì việc quét virus mới hiệu quả và an toàn, không gây lan tràn virus trên đĩa cứng. Có hai loại anti-virus, ngoại nhập và nội địa.

Các anti-virus ngoại đang được sử dụng phổ biến là SCAN của McAfee, Norton Anti-virus của Symantec, Toolkit, Dr. Solomon... Các anti-virus này đều là những sản phẩm thương mại. Ưu điểm của chúng là số lượng virus được cập nhật rất lớn, tìm-diệt hiệu quả, có đầy đủ các công cụ hỗ trợ tận tình (thậm chí tỉ mỉ đến sốt ruột). Nhược điểm của chúng là cồng kềnh.

Các anti-virus nội thông dụng là D2 và BKAV. Đây là các phần mềm miễn phí. Ngoài ưu điểm miễn phí, các anti-virus nội địa chạy rất nhanh do chúng nhỏ gọn, tìm-diệt khá hiệu quả và "rất nhạy cảm" với các virus nội địa. Nhược điểm của chúng là khả năng nhận biết các virus ngoại kém, ít được trang bị công cụ hỗ trợ và chế độ giao tiếp với người sử dụng, để khắc phục nhược điểm này, các anti-virus nội cố gắng cập nhật virus thường xuyên và phát hành nhanh chóng đến tay người dùng.

Tuy nhiên cũng đừng quá tin tưởng vào các anti-virus. Bởi vì anti-virus chỉ tìm-diệt được các virus mà nó đã cập nhật. Với các virus mới chưa được cập nhật vào thư viện chương trình thì anti-virus hoàn toàn không diệt được. Đây chính là nhược điểm lớn nhất của các chương trình diệt virus. Xu hướng của các anti-virus hiện nay là cố gắng nhận dạng virus mà không cần cập nhật. Symantec đang triển khai hệ chống virus theo cơ chế miễn dịch của IBM, sẽ phát hành trong tương lai. Phần mềm D2 nội địa cũng có những cố gắng nhất định trong việc nhận dạng virus lạ. Các phiên bản D2- Plus version 2xx cũng được trang bị các môđun nhận dạng New macro virus và New-Bvirus, sử dụng cơ chế chẩn đoán thông minh dựa trên cơ sở tri thức của lý thuyết hệ chuyên gia. Đây là các phiên bản thử nghiệm hướng tới hệ chương trình chống virus thông minh của chương trình này. Lúc đó phần mềm sẽ dự báo sự xuất hiện của các loại virus mới. Nhưng dù sao cũng nên tự trang bị thêm một số biện pháp phòng chống virus hữu hiệu như được đề cập sau đây.

2. Đề phòng B-virus

Đừng bao giờ khởi động máy từ đĩa mềm nếu có đĩa cứng, ngoại trừ những trường hợp tối cần thiết như khi đĩa cứng bị trục trặc chẳng hạn. Nếu buộc phải khởi động từ đĩa mềm, hãy chắc rằng đĩa mềm này phải hoàn toàn sạch. Đôi khi việc khởi động từ đĩa mềm lại xảy ra một cách ngẫu nhiên, ví dụ như để quên đĩa mềm trong ổ đĩa A ở phiên làm việc trước. Nếu như trong Boot record của đĩa mềm này có B-virus, và nếu như ở phiên làm việc sau, quên không rút đĩa ra khỏi ổ thì B-virus sẽ "lây nhiễm" vào đĩa cứng. Tuy nhiên có thể diệt bằng cách dùng D2-Plus đã dự trù trước các trường hợp này bằng chức năng chẩn đoán thông minh các New B-virus trên các đĩa mềm. Chỉ cần chạy D2 thường xuyên, chương trình sẽ phân tích Boot record của các đĩa mềm và sẽ dự báo sự có mặt của virus dưới tên gọi PROBABLE B-Virus.

3. Đề phòng F-virus

Nguyên tắc chung là không được chạy các chương trình không rõ nguồn gốc. Hầu hết các chương trình hợp pháp được phát hành từ nhà sản xuất đều được đảm bảo. Vì vậy, khả năng tiềm tàng F-virus trong file COM,EXE chỉ còn xảy ra tại các chương trình trôi nổi (chuyền tay, lấy từ mạng,...).

4. Đề phòng Macro virus

Như trên đã nói, họ virus này lây trên văn bản và bảng tính của Microsoft. Vì vậy, khi nhận một file DOC hay XL? bất kỳ, nhớ kiểm tra chúng trước khi mở ra. Điều phiền toái này có thể giải quyết bằng D2- Plus giống như trường hợp của New B-virus, các New macro virus sẽ được nhận dạng dưới tên PROBABLE Macro. Hơn nữa nếu sử dụng WinWord và Exel của Microsoft Office 97 thì không phải lo lắng gì cả. Chức năng AutoDectect Macro virus của bộ Office này sẽ kích hoạt Warning Box nếu văn bản hoặc bảng tính cần mở có chứa macro (chỉ cần Disable).

5. Cách bảo vệ máy tính trước Trojan

- Sử dụng những chương trình chống virus, trojan mới nhất của những hãng đáng tin cậy.

- Để phát hiện xem máy tính có nhiễm Trojan hay không, bạn vào Start -> Run -> gõ regedit -> HKEY_LOCAL_MACHINE -> SOFTWARE -> Microsoft -> Windows -> CurrentVersion ->Run, và hãy nhìn vào cửa sổ bên phía tay phải. Bảng này sẽ hiển thị các chương trình Windows sẽ nạp khi khởi động, và nếu nhìn thấy những chương trình lạ ngoài những chương trình bạn đã biết, chẳng hạn như: sub7, kuang, barok, … thì hãy mạnh dạn xóa chúng (để xóa triệt để, bạn hãy nhìn vào đường dẫn để tìm tới nơi lưu các file đó), rồi sau đó hãy khởi động lại máy tính.

- Nhấn tổ hợp phím Ctrl+Alt+Del để hiện thị bảng Close Program (Win9x), bảng Task Manager (WinNT, Win2K, và WinXP) để xem có chương trình nào lạ đang chạy không. Thường sẽ có một số loại Trojan sẽ không thể che dấu trước cơ chế này.

- Sử dụng một số chương trình có thể quan sát máy của bạn và lập firewall như lockdown, log monitor, PrcView.

- Không tải tệp từ những nguồn không rõ hay nhận mail của người lạ.

- Trước khi chạy tệp lạ nào, kiểm tra trước

Bài tập thực hành của học viên

Câu 1: Lựa chọn một phần mềm Virus thông dụng để cài đặt trên hệ thống

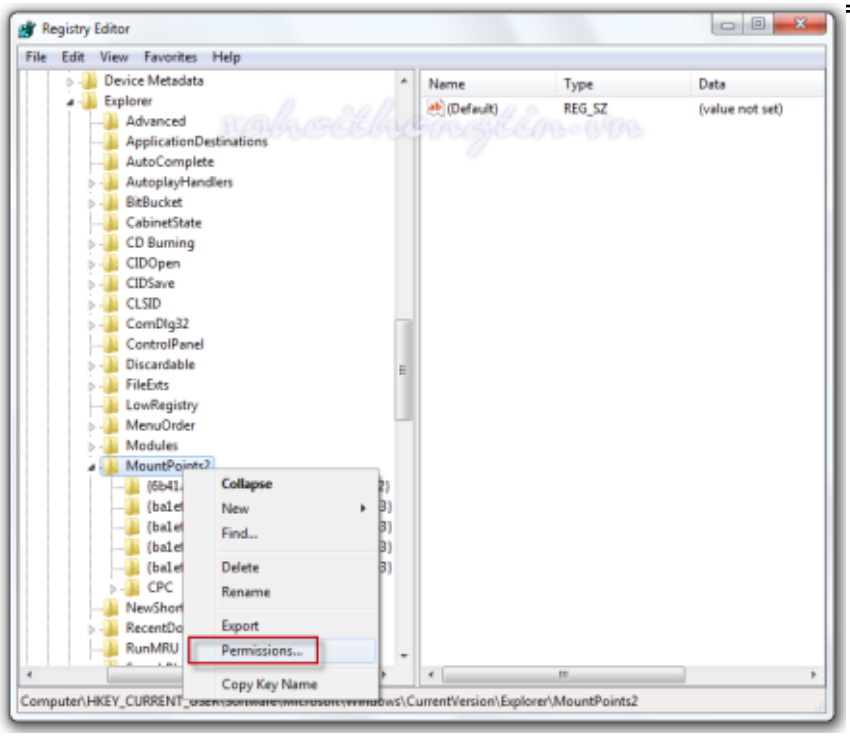
Câu 2: Thực hiện cách ngăn chặn Autorun.inf. Virus.exe xâm nhập máy tính thông qua USB

Hướng dẫn thực hiện

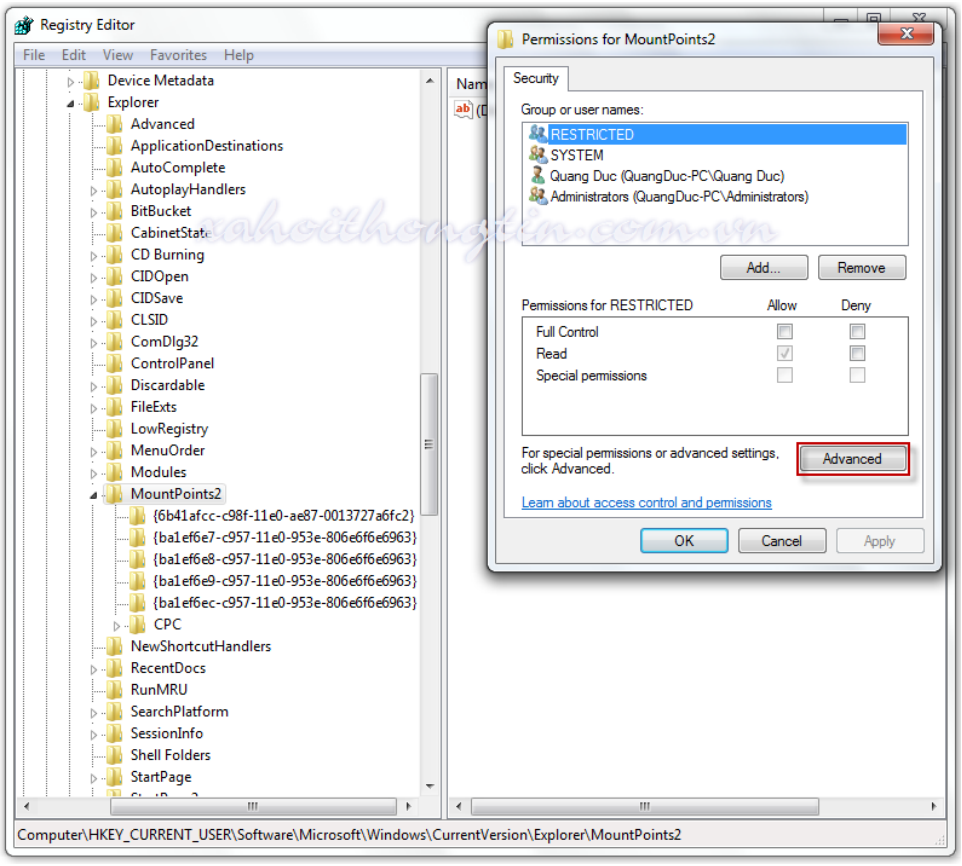
Để thực hiện việc vô hiệu hóa tính năng MountPoints2, bạn thực hiện các bước sau

1. Start > Run hoặc Win + R
2. Nhập Regedit vào ô run > Enter
3. Tại cửa sổ Registry Editor thực hiện tại khóa:

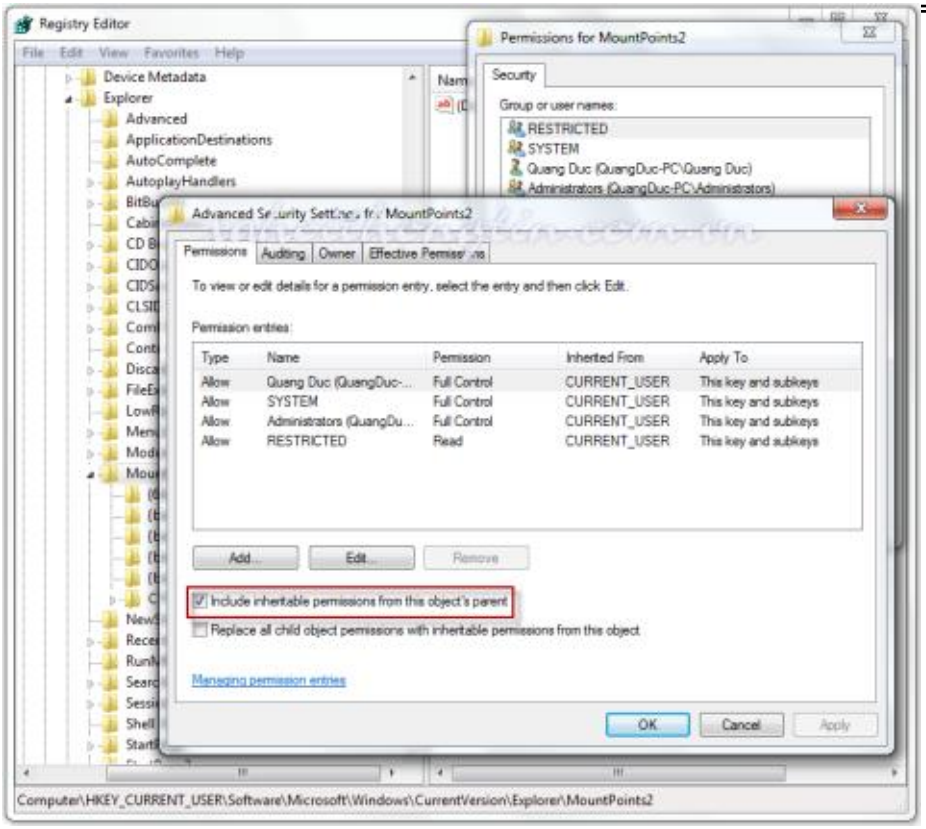
HKEY_CURENT_USER\Software\Microsoft\Windows\Curent Version\Explorer\MountPoints2



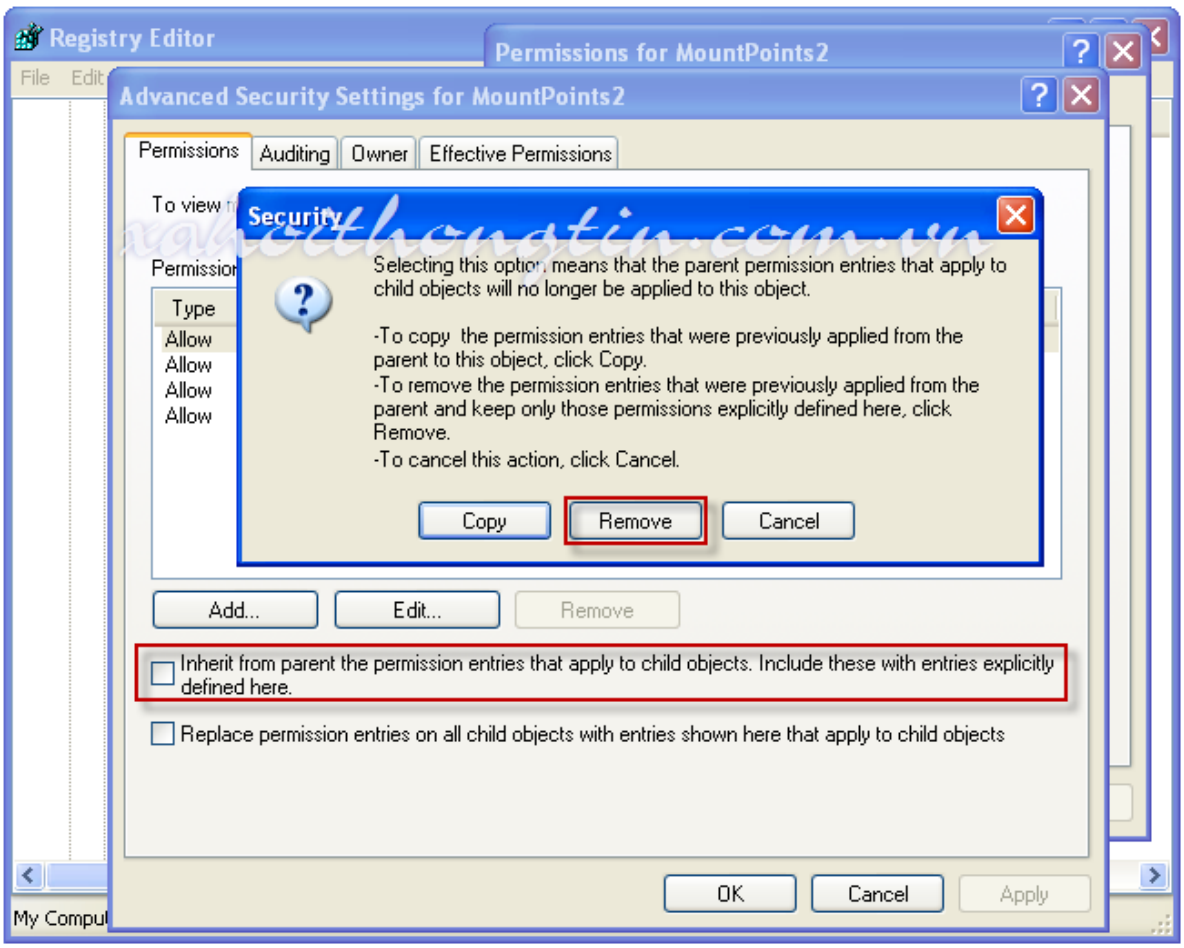
4. Nhấn phải chuột vào MountPoints2 > Permission...



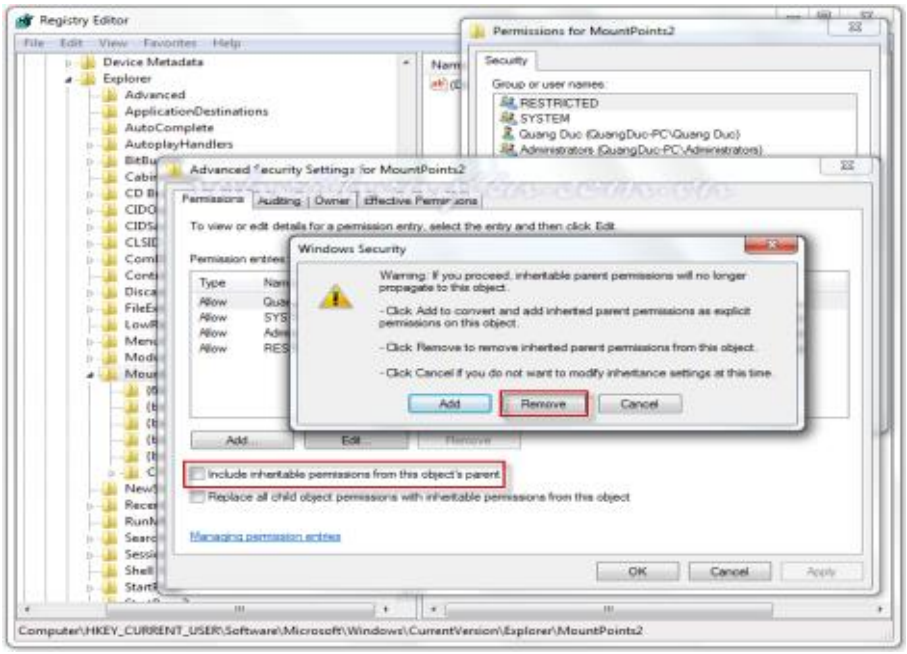
5. Cửa sổ Pemission for MountPoints2 mở ra > Advanced
6. Tại cửa sổ thiết lập Advanced Security Settings for MountPoints2 > Permissions



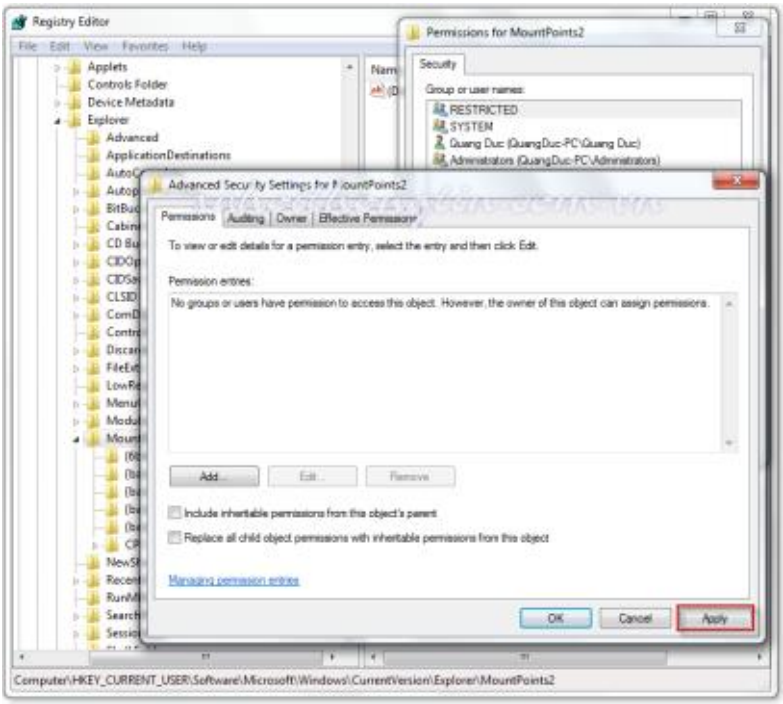
*** Win 7** : Bỏ chọn tính năng **Include inheritable pemssions from this object's parrent** và hiện tại đang có 4 khóa đăng ký hiển thị trong khung Pemission entries.



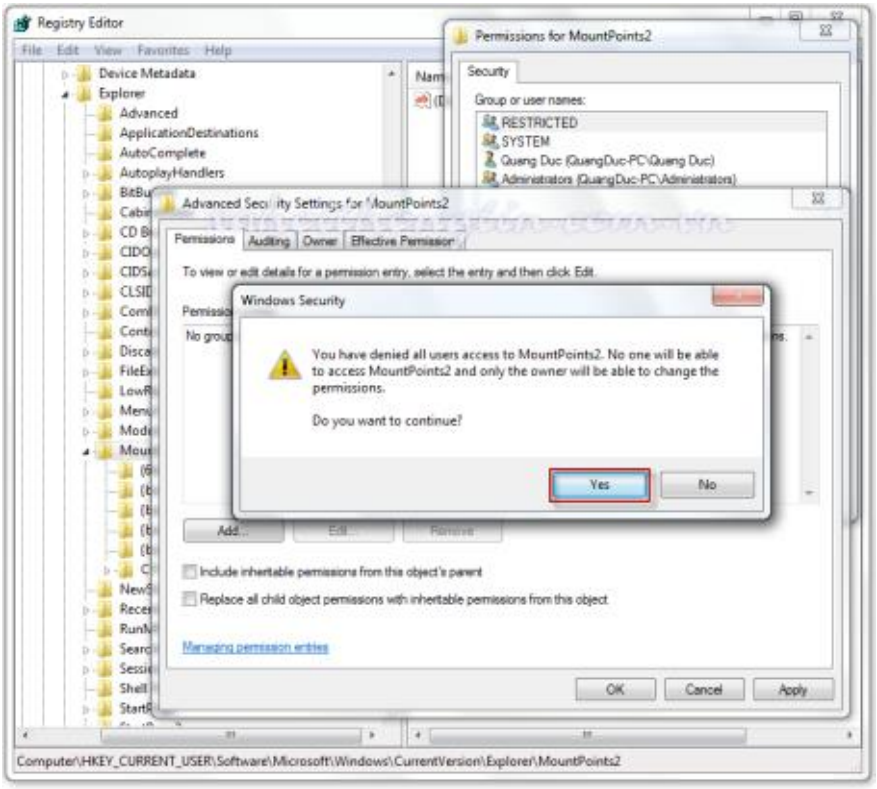
*** Win XP** : Bỏ chọn tính năng **Inherit from parent the pemission entries that apply to child objects. Include these with entries explicitly defined here**.

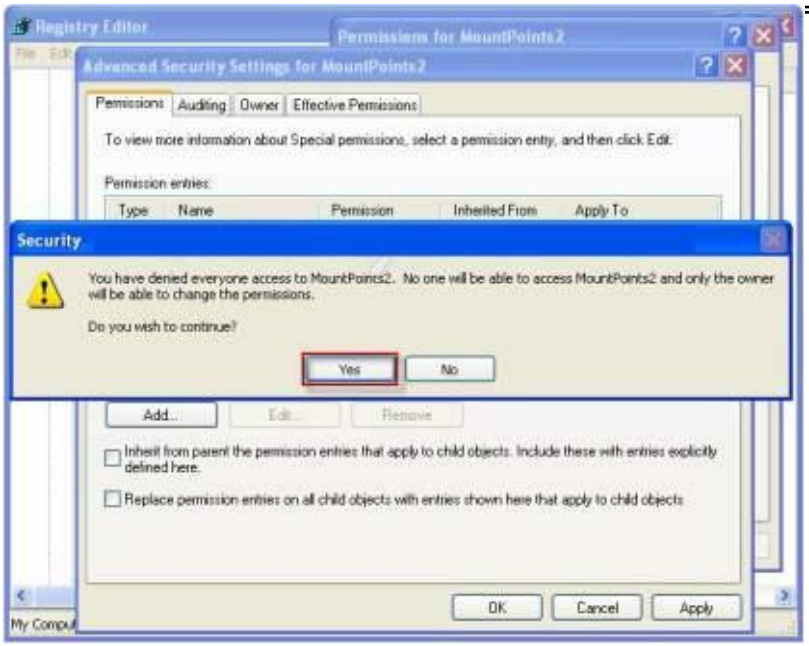


7. Hộp thoại Windows Security xuất hiện > Remove



8. Tại cửa sổ Advanced Security Settings for MountPoints2 > Apply





9. Hộp thoại Windows Security xuất hiện lần nữa với nội dung "Bạn đã từ chối tất cả người dùng truy cập MountPoints2. Không một ai có thể truy cập MountPoints2 và chỉ có bạn có thể thay đổi sự cho phép. Bạn có muốn tiếp tục?" > Yes > OK 2 lần > đóng cửa sổ Registry Editor > khởi động lại hệ thống.

TÀI LIỆU THAM KHẢO

[1]. THs. Ngô Bá Hùng-Ks. Phạm Thế phi *Giáo trình mạng máy tính*, Đại học Cần Thơ, năm 2005

[2]. Đặng Xuân Hà, *An toàn mạng máy tính Computer Networking* năm 2005

[3]. Nguyễn Anh Tuấn, Bài giảng Kỹ thuật an toàn mạng , Trung tâm TH-NN Trí Đức, 2009

[4]. TS. Nguyễn Đại Thọ, *An Toàn Mạng,* Trường Đại học Công nghệ - ĐHQGHN, 2010