TRƯỜNG CAO ĐẲNG NGHỀ CÔNG NGHIỆP HÀ NỘI
Hứa Thị An
Lê Văn Úy

GIÁO TRÌNH
An toàn mạng
(Lưu hành nội bộ)

Hà Nội năm 2012

Tuyên bố bản quyền

Giáo trình này sử dụng làm tài liệu giảng dạy nội bộ trong trường cao đẳng nghề Công nghiệp Hà Nội

Trường Cao đẳng nghề Công nghiệp Hà Nội không sử dụng và không cho phép bất kỳ cá nhân hay tổ chức nào sử dụng giáo trình này với mục đích kinh doanh.

Mọi trích dẫn, sử dụng giáo trình này với mục đích khác hay ở nơi khác đều phải được sự đồng ý bằng văn bản của trường Cao đẳng nghề Công nghiệp Hà Nội

CHƯƠNG 1

TỔNG QUAN VỀ BẢO MẬT VÀ AN TOÀN MẠNG

1. TỔNG QUAN VỀ AN TOÀN BẢO MẬT MẠNG:

1.1. Giới thiệu về AAA: (Access Control, Authentication và Auditing):

Khi hệ thống mạng được ra đời nhu cầu cần trao đổi tài nguyên được đặt ra và những người sử dụng hệ thống mạng đó được trao đổi tài nguyên với nhau. Sau một khoảng thời gian sử dụng, hệ thống mạng đó ngày càng được mở rộng và số lượng tham gia vào mạng ngày càng tăng, do đó việc thực hiện các chính sách bảo mật, thiết lập các chính sách trong việc truy xuất tài nguyên mạng được đặt ra.

Công nghệ thông tin được áp dụng trong nhiều lĩnh vực như thương mại, hàng hải, … Trong sự phát triển đó "thông tin" là một phần quan trọng nhất. Mọi thiết bị máy tính như (Ram, CPU, Màn hình, Đĩa cứng …) cũng như hạ tầng mạng (router, switch, …) được tạo ra để hỗ trợ việc xử lý, lưu trữ, trình bày, vận chuyển thông tin … Vì vậy việc bảo đảm tính an toàn của dữ liệu được lưu trữ trên máy tính cũng như tính bí mật và toàn vẹn của thông tin được truyền trên mạng có ý nghĩa rất lớn đối với sự tồn tại và phát triển của công nghệ thông tin.

Để hỗ trợ cho việc bảo mật nhằm hạn chế truy cấp dữ liệu của người khác, tránh sự mất mát dữ liệu, thuật ngữ AAA (Access Control, Authentication và Auditing) đã ra đời.

AAA được viết tắc từ: Access Control, Authentication và Auditing. AAA là khái niệm cơ bản của an ninh máy tính và an ninh mạng. Những khái niệm này được dùng để bảo đảm các tính năng bảo mật thông tin, toàn vẹn dữ liệu và tính sẵn sàng của hệ thống.

1.2. Điều khiển truy cập (Access Control):

Điều khiển truy cập là một chính sách, được sự hỗ trợ của phần mềm hay phần cứng được dùng để cho phép hay từ chối truy cập đến tài nguyên, qui định mức độ truy xuất đến tài nguyên.

Có ba mô hình được sử dụng để giải thích cho mô hình điều khiển truy cập:

- MAC (Mandatory Access Control)
- DAC (Discretionary Access Control)
- RBAC (Role Based Access Control)

1.2.1 MAC (Mandatory Access Control):

Mô hình MAC là một mô hình tĩnh sử dụng các quyền hạn truy cập đến tập tin được định nghĩa trước trên hệ thống. Người quản trị hệ thống thiết lập các tham số này và kết hợp chúng với một tài khoản, với nhiều tập tin hay tài nguyên. Mô hình

MAC có thể bị hạn chế nhiều. Trong mô hình MAC người quản trị thiết lập việc truy cập và người quản trị cũng là người có thể thay đổi sự truy cấp đó. Người dùng không thể chia sẽ tài nguyên được trừ khi có một mối quan hệ với tài nguyên đã tồn tại trước.

Ví dụ:

Đối với Unix hệ thống qui định một tập tin hay thư mục sẽ về một chủ sở hữu (Owner). Khi đó ta không thể định nghĩa một tập tin hay thư mục thuộc quyền sở hữu của hai hay nhiều người.

Quyền tập tin, thư mục trên Windows 2000 (Full control, Write, Read, List folder content …)

1.2.2. DAC (Discretionary Access Control):

Là tập các quyền truy cập trên một đối tượng mà một người dùng hay một ứng dụng định nghĩa. Mô hình DAC cho phép người dùng chia sẻ tập tin và sử dụng tập tin do người khác chia sẻ. Mô hình DAC thiết lập một danh sách điều khiển truy cập (Access control list) dùng để nhận ra người dùng nào được quyền truy cập đến tài nguyên nào. Ngoài ra, mô hình này cho phép người dùng gán hay loại bỏ quyền truy cấp đến mỗi cá nhân hay nhóm dựa trên từng trường hợp cụ thể.

1.2.3. RBAC (Role Based Access Control):

Trong RBAC, việc quyết định quyền truy cập dựa trên vai trò của mỗi cá nhân và trách nhiệm của họ trong tổ chức.

Quyền hạn dựa trên công việc và phân nhóm người dùng. Tuỳ thuộc vào từng quyền hạn của người dùng mà chúng ta sẽ phân quyền cho phù hợp.

Ví dụ:

Người quản trị có toàn quyền quản trị trên hệ thống mạng, được quyền thêm, xoá, sữa thông tin trên mạng. Những nhân viên bình thường trong mạng sẽ chỉ có quyền sử dụng máy tính mà không được phép làm gì cả.

1.3 Xác thực (Authentication):

Quá trình dùng để xác nhận một máy tính hay một người dùng cố gắng truy cập đến tài nguyên, cũng như cách thức đăng nhập và sử dụng hệ thống.

Quá trình xác thực rất đa dạng, từ cách xác nhận thông thường như kiểm tra tên đăng nhập/mật khẩu đến việc sử dụng các công nghệ tiên tiến như thể thông minh, thiết bị sinh học để nhận dạng người dùng.

1.3.1. Username/Password:

Đây là phương thức xác nhận cổ điển và được sử dụng rất phổ biến (do tính năng đơn giản và dễ quản lý).

MỗI ngườI dùng sẽ được xác nhận bằng một tên truy cập và mật khẩu. Mật khẩu thông thường được lưu trong cơ sở dữ liệu dướI dạng mã hoá hoặc không mã hoá. Tuy nhiên mật khẩu có thể dễ dàng bị đoán bằng các phương pháp vét cạn.

Chính sách mật khẩu:

- Mức độ không an toàn: ít hơn 06 ký tự
- Mức độ an toàn trung bình: 08 đến 13 ký tự
- Mức độ an toàn cao: 14 ký tự

Ngoài ra mật khẩu cần tuân theo một số yêu cầu sau:

- Kết hợp giữa các ký tự hoa và thường
- Sử dụng số, ký tự đặc biệt, không sử dụng các từ có trong tự điển.
- Không sử dụng thông tin cá nhân để đặt mật khẩu (ngày sinh, số điện thoại, tên ngườI thân …).

1.3.2. CHAP:

Do điểm yếu của User/Pass là thông tin dễ dàng bị mất khi chuyển trên mạng, do đó cần phải có một phương pháp để đảm bảo rằng dữ liệu được truyền thông an toàn trong quá trình chứng thực. CHAP là một giao thức đáp ứng được yêu cầu trên.

CHAP thường được dùng để bảo vệ các thông tin xác nhận và kiểm tra kết nối đến tài nguyên hợp lệ, sử dụng một dãy các thách thức và trả lời được mã hoá. Đây là nghi thức xác nhận truy cập từ xa mà không cần gửi mật khẩu qua mạng.

CHAP được sử dụng để xác định sự hợp lệ bằng cách sử dụng cơ chế bắt tay 3 - Way. Cơ chế này được sử dụng khi kết nối được khởi tạo và được sử dụng nhiều lần để duy trì kết nối.

- Nơi cần xác nhận sẽ gửi một thông điệp "Challenge"
- Bên nhận sẽ sử dụng mật khẩu và một hàm băm một chiều để tính ra kết quả và trả lời cho bên cần xác nhận.
- Bên cần xác nhận sẽ tính toán hàm băm tương ứng và đối chiếu với giá trị trả về. Nếu giá trị là đúng thì việc xác nhận hợp lệ, ngược lại kết nối sẽ kết thúc.
- Vào một thời điểm ngẫu nhiên,bên cạnh xác nhận sẽ gửi một Challenge mới để kiểm tra sự hợp lệ của kết nối

1.3.3. Chứng chỉ (Certificates)

Trong cuộc sống chúng ta sử dụng CMND hay hộ chiếu để giao tiếp với người khác trong xã hội như sử dụng để đi du lịch, tàu xe … Trong máy tính chúng ta sử dụng chứng chỉ để xác nhận với những máy khác rằng người dùng và máy tính hợp lệ và giúp cho các máy tính truyền thông với nhau được an toàn.

Chứng chỉ điện tử là một dạng dữ liệu số chứa các thông tin để xác định một thực thể (thực thể có thể là một cá nhân, một server, một thiết bị hay phần mềm…)

Chi tiết về chứng chỉ chúng ta sẽ tham khảo trong các phần sau.

1.3.4. Mutual Authentication (Xác nhận lẫn nhau):

Đa số các cơ chế chứng thực đều thực hiện một chiều, khi đó việc xác thực rất dễ bị giả lập và dễ bị Hacker tấn công bằng phương pháp giả lập cách thức kết nối (như Reply Attack …) Trong thực tế có rất nhiều ứng dụng đòi hỏi cơ chế xác nhận qua lại. ví dụ một người dùng có một tài khoản tại Ngân hàng. Khi người dùng truy xuất để kiểm tra ngày nạp tiền vào Ngân hàng sẽ kiểm tra tính hợp lệ của Ngân hàng đang thao tác. Nếu thông tin kiểm tra là hợp lệ thì quá trình đăng nhập thành công và người dùng có thể thay đổi thông tin tài khoản của mình.

Mỗi thành phần trong một giao tiếp điện tử có thể xác nhận thành phần kia. Khi đó, không chỉ xác nhận người dùng với hệ thống mà còn xác nhận tính hợp lệ của hệ thống đối với người dùng.

1.3.5. Biometrics:

Các thiết bị sinh học có thể cung cấp một cơ chế xác nhận an toàn rất cao bằng cách sử dụng các đặc tính về vật lý cũng như hành vi của mỗi cá nhân để chứng thực, được sử dụng ở các khu vực cần sự an toàn cao.

Cách thức hoạt động của Biometric:

- Ghi nhận đặc điểm nhận dạng sinh học
  - Các đặc điểm nhận dạng của đối tượng được quét và kiểm tra.
  - Các thông tin về sinh học được phân tích và lưu lại thành các mẫu.
- Kiểm tra
  - Đối tượng cần được kiểm tra sẽ được quét
  - Máy tính sẽ phân tích dữ liệu quét vào và đối chiếu với dữ liệu mẫu.
  - Nếu dữ liệu mẫu đối chiếu phù hợp thì người dùng được xác định hợp lệ và có quyền truy xuất vào hệ thống.

Một số dạng:

- Các đặc điểm vật lý:
  - Dấu vân tay
  - Hand geometry
  - Quét khuôn mặt
  - Quét võng mạc mắt
  - Quét tròng đen mắt
- Các đặc tính và hành vi:
  - Chữ ký tay
  - Giọng nói

Hiện nay cơ chế xác nhận sinh học được xem là cơ chế mang tính an toàn rất cao. Tuy nhiên để xây dựng cơ chế xác nhận này thì chi phí rất cao.

1.3.6. Multi – Factor:

khi một hệ thống sử dụng hai hay nhiều phương pháp chứng thực khác nhau để kiểm tra việc User đăng nhập hợp lệ hay không thì được gọi là multi – factor. Một hệ thống vừa sử dụng thể thông minh vừa sử dụng phương pháp chứng thực bằng

username va password thì được gọi là một hệ thống chứng thực two – factor. Khi đó ta có thể kết hợp hai hay nhiều cơ chế xác nhận để tạo ra một cơ chế xác nhận phù hợp với nhu cầu.

Chỉ danh của một cá nhân được xác định sử dụng ít nhất hai trong các factors xác nhận sau:

- Bạn biết gì (một mật khẩu hay số pin)
- Bạn có gì (smart card hay token)
- Bạn là ai (dấu vân tay, võng mạc …)
- Bạn làm gì (giọng nói hay chữ ký)

1.3.7. Kerberos:

Kerberos là một dịch vụ xác nhận bảo đảm các tính năng an toàn, xác nhận một lần, xác nhận lẫn nhau và dựa vào thành phần tin cậy thứ ba.

An toàn:

Sử dụng ticket, dạng thông điệp mã hóa có thời gian, để chứng minh sự hợp lệ của người dùng. Vì thế mật khẩu của người dùng có thể được bảo vệ tốt do không cần gửi qua mạng hay lưu trên bộ nhớ máy tính cục bộ.

Xác nhận truy cập một lần:

Người dùng chỉ cần đăng nhập một lần và có thể truy cập đến tất cả các tài nguyên trên một hệ thống hay máy chủ khác hỗ trợ nghi thức Kerberos.

Thành phần tin cậy thứ ba:

Làm việc thông qua một máy chủ xác nhận trung tâm mà tất cả các hệ thống trong mạng tin cậy.

Xác nhận lẫn nhau:

Không chỉ xác nhận người dùng đối với hệ thống mà còn xác nhận sự hợp lệ của hệ thống đối với người dùng.

Xác nhận Kerberos được tích hợp trực tiếp trong cấu trúc quản lý thư mục (Active Directory) của Windows 2000, 2003 server hỗ trợ các máy trạm có thể đăng nhập một lần vào DC và sử dụng dịch vụ trên các server khác thuộc cùng DC mà không cần phải đăng nhập. Việc này hoàn toàn trong suốt vớI ngườI dùng nên họ không nhận ra được sự hỗ trợ của Kerberos.

2. CÁC DẠNG TẤN CÔNG:

2.1. Giới thiệu:

Để xây dựng một hệ thống bảo mật, trước hết chúng ta phải hiểu rõ cách thức các Hacker sử dụng để tấn công vào hệ thống. Việc tìm hiểu cách thức tấn công góp phần rất nhiều cho công tác bảo mật một hệ thống mạng, giúp việc ngăn chặn hiệu quả

hơn rất nhiều. Môi trường mạng ngày càng phát triển, do đó nhu cầu bào mật, bảo đảm an ninh trên mạng luôn phát triển.

Hiện nay, các phương pháp tấn công rất đa dạng và phong phú. Tuy có rất nhiều phương thức tấn công nhưng có thể tạm xếp chúngvào những nhóm như sau:

- Theo mục tiêu tấn công: Ứng dụng mạng hay cả hai
- Theo cách thức tấn công: Chủ động (Active) hay thụ động (Passive)
- Theo phương pháp tấn công: Có nhiều loại ví dụ như bẻ khoá, khai thác lỗi, phần mềm hay hệ thống, mã nguy hiểm …

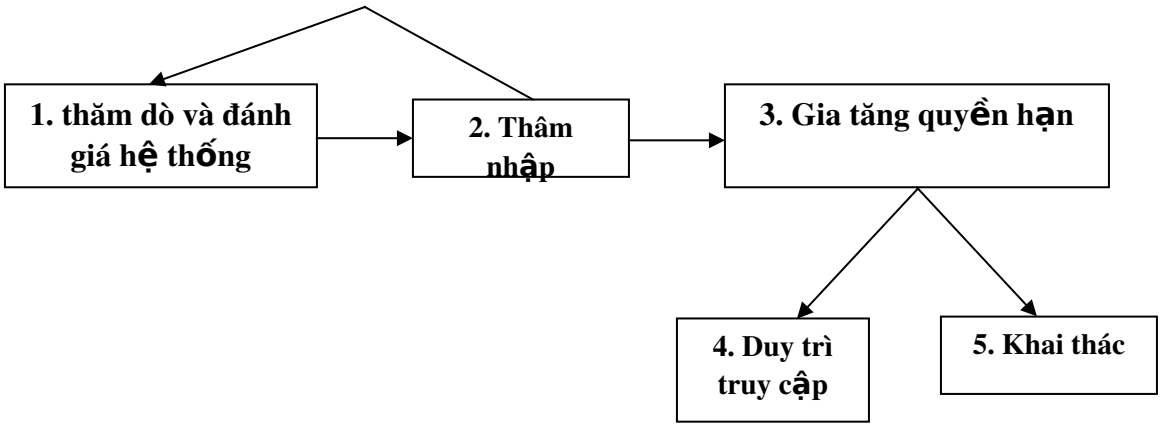
Ranh giới của các nhóm này dần khó nhận ra vì những cách tấn công ngày nay, ngày càng phức tạp, tổng hợp.

Tuy nhiên, không phải mọi hacker đều tấn công nhằm mục đích phá hoại hệ thống. Có một số đối tượng tấn công vào hệ thống có mục đích nhằm tìn ra lỗ hỏng của hệ thống và báo cho người quản trị để họ vá lỗ hỏng đó lại. Những hacker dạng này người ta gọi là " White hat", còn hacker dạng khác người người ta gọI là "Black hat".

Một số người lại lầm tưởng giữa hacker và cracker. Cracker là một người chuyên đi tìm hiểu các phần mềm và bẻ khoá các phần mềm đó, còn hacker là người chuyên đi tìm các lỗ hỏng của hệ thống.

2.2. Minh hoạ khái quát một qui trình tấn công:

Tuỳ thuộc vào mục tiêu tấn công mà hacker sẽ có những kịch bản tấn công khác nhau. Ở đây chúng ta chỉ minh hoạ một dạng kịch bản tổng quát để tấn công vào hệ thống.



Các bước cơ bản của một cuộc tấn công

- Bước 1: Tiến hành thăm dò và đánh giá hệ thống
- Bước 2: Thực hiện bước thâm nhập vào hệ thống. Sau đó có thể quay lại bước 1 để tiếp tục thăm dò, tìm thêm các điểm yếu của hệ thống.
- Bước 3: Tìm mọi cách để gia tăng quyền hạn. Sau đó có thể quay lại bước 1 để tiếp tục thăm dò, tìm thêm các điểm yếu của hệ thống hoặc sang bước 4 hay bước 5.

- Bước 4: Duy trì truy cập, theo dõi hoạt động của hệ thống
- Bước 5: Thực hiện các cuộc tấn công (ví dụ: từ chốI dịch vụ …)

2.3. Tấn công chủ động:

Là những dạng tấn công mà kể tấn công trực tiếp gây nguy hại tới hệ thống mạng và ứng dụng (khống chế máy chủ, tắt các dịch vụ) chứ không chỉ nghe lén hay thu thập thông tin.

Những dạng tấn công phổ biến như: Dos, Ddos, Buffer overflow, IP spoofing …

2.3.1. DOS:

Tấn công từ chối dịch vụ, viết tắt là DOS (Denial of service) là thuật ngữ gọi chung cho những cách tấn công khác nhau về cơ bản làm cho hệ thống nào đó bị quá tải không thể cung cấp dịch vụ, hoặc phải ngưng hoạt động. Kiểu tấn công này chỉ làm gián đoạn hoạt động chứ rất ít khả năng đánh cắp thông tin hay dữ liệu.

Thông thường mục tiêu của tấn công từ chối dịch vụ là máy chủ (FTP, Web, Mail) tuy nhiên cũng có thể là các thiết bị mạng như: Router, Switch, Firewall …

Tấn công từ chối dịch vụ không chỉ là tấn công qua mạng mà còn có thể tấn công ở máy cục bộ hay trong mạng cục bộ còn gọi là Logcal Dos Against Hosts.

Ban đầu tấn công từ chốI dịch vụ xuất hiện khai thác sự yếu kém của giao thức TCP là Dos, sau đó phát triển thành tấn công từ chối dịch vụ phân tán Ddos (Distributed Dos).

Chúng ta có thể phân nhỏ tấn công từ chối dịch vụ ra thành các dạng Broadcast stom, SYN, Finger, Ping, Flooding …

Hai vấn đề của tấn công từ chối dịch vụ là:

- Việc sử dụng tài nguyên (Resource consumption attacks) của số lượng lớn yêu cầu làm hệ thống quá tải. Các tài nguyên là mục tiêu của tấn công từ chối dịch vụ bao gồm: Bandwidth (thường bị tấn công nhất), Hard disk (mục tiêu của bom mail), Ram, CPU …
- Có lỗi trong việc xử lý các String, Input, Packet đặc biệt được attacker xây dựng (malfomed packet attack). Thông thường dạng tấn công này sẽ được áp dụng với router hay switch. Khi nhận những packet hay string dạng này, do phần mềm hay hệ thống bị lỗi dẫn đến router hay switch bị crash …

Tấn công từ chối dịch vụ không đem lại cho attacker quyền kiểm soát hệ thống nhưng nó là một dạng tấn công vô cùng nguy hiểm, đặc biệt là với những giao dịch điện tử hay thương mại điện tử. Những thiệt hại về tiền và danh dự, uy tính là khó có thể tính được. Nguy hiểm tiếp theo là rất khó đề phòng dạng tấn công này thông thường chúng ta chí biết khi đã bị tấn công.

Đối với những hệ thống bảo mật tốt tấn công từ chối dịch vụ được coi là phương pháp cuốI cùng được attacker áp dụng để triệt hạ hệ thống.

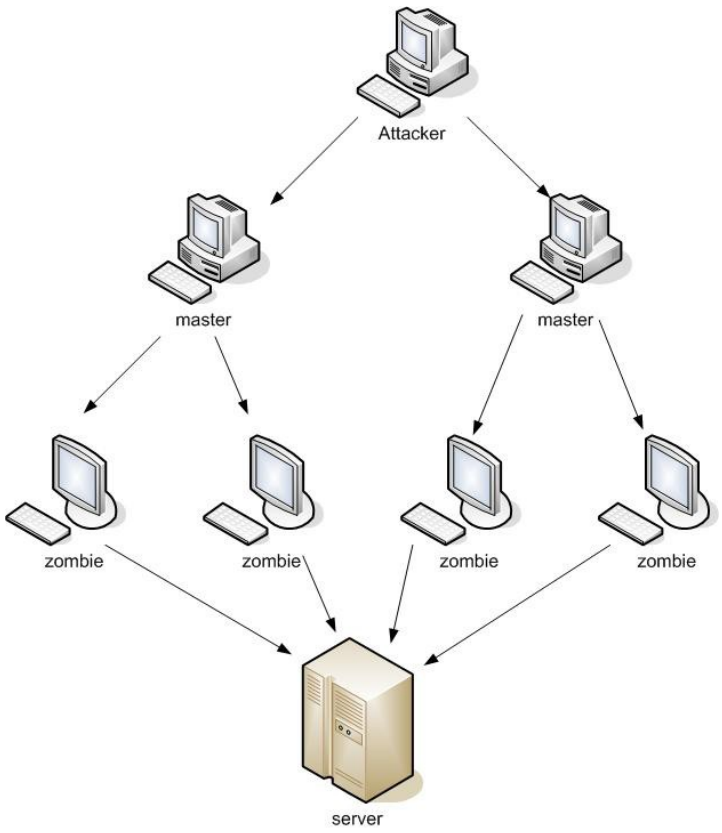
2.3.2. DDOS:

Tấn công từ chối dịch vụ phân tán thực hiện với sự tham gia của nhiều máy tính. So với Dos mức độ nguy hiểm của DDos cao hơn rất nhiều.

Tấn công DDos bao gồm hai thành phần:

- Thành phần thứ nhất: Là các máy tính gọi là zombie (thông thường trên internet) đã bị hacker cài vào đó một phần mềm dùng để thực hiện tấn công dưới nhiều dạng như UDP flood hay SYN flood … Attacker có thể sử dụng kết hợp với spoofing để tăng mức độ nguy hiểm. Phần mềm tấn công thường dưới dạng các daemon.
- Thành phần thứ hai: Là các máy tình khác được cài chương trình client. Các máy tình này cũng như các zombie tuy nhiên các attacker nắm quyền kiểm soát cao hơn.Chương trình client cho phép attacker gửi các chỉ thị đến Daemon trên các zombie.

Khi tấn công attacker sẽ dùng chương trình client trên master gửi tín hiệu tấn công đồng loạt tới các zombie. Daemon process trên zombie sẽ thực hiện tấn công tới mục tiêu xác định. Có thể attacker không trực tiếp thực hiện hành động trên master mà từ một máy khác sau khi phát động tấn công sẽ cắt kết nối với các master để đề phòng bị phát hiện.



Minh hoạ tấn công DDOS

Thông thường mục tiêu của DDos là chiếm dụng bandwidth gây nghẽn mạng. Các công cụ thực hiện có thể tìm thấy nhưTri00 (Win Trin00), Tribe Flood Network (TFN hay TFN2K), Sharf … Hiện nay còn phát triển các dòng virus, worm có khả năng thực hiện DDos.

2.3.3. Buffer Overflows (tràn bộ đệm):

Đây là một dạng tấn công làm tràn bộ đệm của máy tính. Buffer Overflows xuất hiện khi một ứng dụng nhận nhiều dữ liệu hơn chương trình chấp nhận. Trong trường hợp này ứng dụng có thể bị ngắt. Khi chương trình bị ngắt có thể cho phép hệ thống gửidữ liệu với quyền truy cập tạm thời đến những mức độ có đặc quyền cao hơn vào hệ thống bị tấn công. Nguyên nhân của việc tràn bộ đệm này là do lỗi của chương trình.

2.3.4. Spoofing:

Truy cập vào hệ thống bằng cách giả danh (sử dụng chỉ danh đánh cắp của ngườI khác, giả địa chỉ MAC, IP …)

Là phương pháp tấn công mà attacker cung cấp thông tin chứng thực hoặc giả dạng một user hợp lệ để truy cập bắt hợp lệ vào hệ thống. Tuy nhiên trong vài trường hợp việc cấu hình hệ thống sai có thể gây hậu quả tương tự. Ví dụ cấu hình hệ thống có lỗi cho user có quyền cao hơn quyền được phép mà user này không hề cố ý giả mạo.

Có nhiều tấn công bằng spoofing. Trong đó có "blind spoofing" attacker chỉ gửi thông tin giả mạo đi và đoán kết quả trả về. Ví dụ IP spoofing sau khi gửi packet giả mạo địa chỉ attacker không nhận được trả lời. Dạng thứ hai cần quan tâm là "informed spoofing" attacker kiểm soát truyền thông cả hai hướng.

Tấn công bằng cách giả mạo thường được nhắc đến nhất là IP spoofing và ARP spoofing hay còn gọi là ARP poisoning.

Việc giả mạo IP xảy ra do điểm yếu của giao thức TCP/IP. Giao thức TCP/IP không hề có tính năng chứng thực địa chỉ packet nhận được có phải là địa chỉ đúng hay là địa chỉ giả mạo.Một IP address được coi như là một máy tính (thiết bị) duy nhất kết nối vào mạng và do đó các máy tính có thể giao tiếp với nhau mà không cần kiểm tra. Tuy nhiên chúng ta có thể khắc phục bằng cách sử dụng Firewall, router, các giao thức và thuật toán chứng thực... Việc thực hiện giả mạo IP có thể bằng cách sử dụng Raw IP.

ARP poisoning cách tấn công nhằm thay đổI ARP entries trong bảng ARP nhờ đó có thể thay đổi được nơi nhận thông điệp. Các tấn công này áp dụng vớI LAN switch.

Trình bày cách tấn công bằng ARP poisoning:

- ARP (Address Resolution Protocol): Là một giao thức dùng để làm cho một địa chỉ IP phù hợp với một địa chỉ MAC. ARP được dùng trong tất cả các trường hợp nơi mà một nút trên mạng TCP/IP cần biết địa chỉ MAC của một nút khác trên cùng một mạng hay trên mạng tương tác. Về cơ bàn, ARP cho phép một

máy tính gửi thông điệp ARP trên mạng cục bộ để tất cả các nút đều nghe thấy nhưng chỉ có nút mạng có địa chỉ IP tương ứng mới trả lời.

- Một vài hệ điều hành không cập nhật thông tin ARP nếu nó không có sẵn trong cache, một số khác thì chấp nhận chỉ một lần trả lời lại đầu tiên (ví dụ như Solaris)
- Attacker có thể giả mạo một packet ICMP đã bắt chước để bắt buộc máy trạm thực hiện một ARP request. Ngay lập tức sau khi nhận được ICMP, máy trạm gửi lại một ARP.

Biện pháp đối phó:

- Chúng ta có thể sử dụng một trong các biện pháp sau: (Yes: có thể sử dụng được, No: không thể sử dụng được)

  Yes – Passive monitoring (arp watch)
  Yes – Active monitoring (ettercap)
  Yes – IDS (detect but not avoid)
  Yes – Static ARP entries (avoid it)
  Yes – Secure ARP (puplic key auth)
  No – Port security on the switch
  No – Anticap, antidote, middleware approach

2.3.5. SYN Attacks:

Là một trong những dạng tấn công kinh điển nhất. Lợi dụng điểm yếu của bắt tay 3 bước TCP. Việc bắt tay ba bước như sau:

- Bước 1: Client gửi gói packet chứa cờ SYN
- Bước 2: Server gửi trả client packet chức SYN/ACK thông báo sẵn sàng chấp nhận kết nối đồng thời chuẩn bị tài nguyên phục vụ kết nối, ghi nhận lại các thông tin về client
- Bước 3: Client gửi trả server ACK và hoàn thành thủ tục kết nối.

Khai thác lỗi của cơ chế bắt tay 3 bước của TCP/IP. Vấn đề ở đây là client không gửi trả cho server packet chứa ACK , việc này gọI là half – open connection (client chỉ mở kết nốI một nửa) và với nhiều packet như thế server sẽ quá tải do tài nguyên có hạn. Khi đó có thể các yêu cầu hợp lệ sẽ không được đáp ứng. Việc này tương tự như một máy tính bị treo do mở quá nhiều chương trình cùng một lúc.

Máy tính khởi tạo kết nối sẽ gửI một thông điệp SYN + Spoofing IP

Máy nhận được sẽ trả lời lạI SYN và một ACK

Sẽ không có người nào nhận được ACK (do địa chỉ giả)

Do vậy máy nhận được sẽ đợi một khoảng thời gian dài trước khi xoá kết nối

Khi số lượng tạo kết nối SYN này quá nhiều sẽ làm cho hàng đợi tạo kết nối bị đầy và không thể phục vụ các yêu cầu kết nối khác.

Trên Windows để nhận biết tấn công SYN có thể dùng lệnh Netstar – n – p tcp

Chúng ta sẽ chú ý SYN – Received của các connection. Tuy nhiên tấn công SYN thường đi chung với IP spoofing. Cách attacker thường sử dụng là random source IP, khi đó server thường không nhận được ACK từ các máy có IP không thật, đồng thời server có khi còn phải gửi lại SYN/ACK vì nghĩ rằng client không nhận được SYN/ACK . Lý do tiếp theo là tránh bị phát hiện source IP , khi đó nhân viên quản trị sẽ block source IP này.

Giải pháp:

- Giảm thời gian chờ đợi khởi tạo kết nối. Việc này có thể sinh ra lỗi từ chối dịch vụ với máy từ xa có băng thông thấp truy xuất đến.
- Tăng số lượng các cố gắng kết nối
- Sử dụng tường lửa để gửi gói ACK cho máy nhận để chuyển kết nối đang thực hiện sang dạng kết nối thành công.

2.3.6. Man in the Middle Attacks:

Kẻ tấn công sẽ đứng giữa kênh truyền thông của hai máy tính để xem trộm thông tin và thậm chí có thể thay đổI nộI dung trao đổI giữa hai máy tính.

Trong khi đó cả hai máy tính đều nghĩ rằng mình đang kết nối trực tiếp với máy tính kia.

Cách tấn công Man in the Middle:

- Tấn công trong mạng nội bộ:

  ARP Poisoning
  DNS Spoofing
  STP mangling
  Port Stealing

- Tấn công từ cục bộ đến các máy ở xa (thông qua gateway)

  ARP Poisoning
  DNS Spoofing
  DHCP Spoofing
  ICMP Redirection
  IRDP Spoofing
  Route mangling
  Tấn công từ xa
  DNS Spoofing
  Traffic tunneling
  Route mangling

- Tấn công trên mạng không dây

Access Point Reassociation

2.3.7. Replay Attacks:

Sử dụng công cụ để ghi nhận tất cả thông tin trao đổi khi một máy tính nào đó truy xuất đến server. Sau đó sử dụng các thông tin bắt được trên mạng để nốI kết lại đến server đó.

Đây là kỹ thuật mà Attacker khi nắm được một số lượng packet sẽ sử dụng lại những packet này sau đó. Ví dụ Attacker có được packet chứa password của một user. Password này đã được mã hoá và attacker không biết được. Tuy nhiên hệ thống chứng thực không có chức năng kiểm tra Session time hay hệ thống có TCP Sequence number kém. Attacker sẽ thực hiện Bypass Authenticate bằng cách gửi packet một lần nữa hay còn gọi là replay.

2.3.8. Dumpster Diving:

Dumpster Diving là thuật ngữ mô tả tấn công bằng cách thu lượm thông tin từ những thứ tưởng như không còn giá trị. Ví dụ Attacker có thể có được nhiều thông tin từ "Recycle bin" từ giấy tờ chứng từ bõ đi … Không chỉ từ những thông tin trên máy vi tính, những thông tin thu lượm được cũng có thể lấy được từ các tài liệu, hồ sơ do ngườI dùng bỏ đi. Từ những loạI giấy tờ thu nhận được có thể rút trích ra để lấy những thông tin cần thiết cho việc tấn công.

2.3.9. Social Engineering:

Đây là một dạng tấn được sử dụng phổ biến nhất và rất khó phòng ngừa. Cách tấn công này không đòi hỏi kẻ tấn công sử dụng các công cụ hay thiết bị mà vẫn có thể có được các thông tin cần thiết để thâm nhập vào hệ thống.

Đa số người dùng thường đặt mật khẩu dựa vào thông tin cá nhân như họ tên, số điện thoại, ngày sinh, … Khi đó kẻ tấn công có thể thu thập các thông tin này để thực hiện việc đoán mật khẩu của người dùng.

Một dạng khác là khai thác sự tin cậy hay nhẹ dạ của con người để tìm ra các thông tin quan trong như giả danh một khách hàng quen thuộc của Công ty để thu thập các thông tin quan trọng …

Giải pháp: Đào tạo hướng dẫn người dùng luôn cảnh giác

2. 4. Tấn công thụ động:

2.4.1. Dò tìm lỗ hỏng:

Đây là bước cơ bản kẻ tấn công sẽ thực hiện để đánh giá và tìm ra các điểm yếu của hệ thống. kỹ thuật dùng các công cụ quét để tìm ra điểm yếu tấn công.

Sử dụng các công cụ quét cổng để thăm dò và phát hiện các thông tin của hệ thống như hệ điều hành, phiên bàn, các ứng dụng triển khai …

Attacker sẽ kiểm tra để ht vọng tìm ra một cửa nào không khoá hoặc dễ dàng phá mà không bị phát hiện.

A/ Giới thiệu công cụ NMAP:

NMAP là viết tắt của Network Mapper. Ban đầu NMAP được thiết kế chủ yếu dành cho System admin nhằm scan những mạng có nhiều máy tính để biết máy nào hoạt động, các service nó đang chạy và hệ điều hành đang sử dụng.

NMAP hỗ trợ kỹ thuật scan bao gồm: UDP, TCP, TCP SYN (half – open), FTP Proxy (bounce attack), ICMP (ping sweep), FIN, ACK sweep, Xmas tree, SYN sweep, IP Protocol … Có thể dùng xác định các thông tin cúa máy ở xa, ví dụ như OS qua TCP/IP Fingerprinting.

Công cụ NMAP có thể dễ dàng tìm trên internet và được cài đặt … Mặc định trong các hệ điều hành Unix. NMAP có những phiên bản chạy trên Windows và hỗ trợ giao diện đồ hoạ (NMAP Win).

Một số chức năng chính của NMAP:

- Connect Scan (TCP connect): Đây là một dạng cơ bản nhất của việc quét TCP. Kỹ thuật này được dùng để quét tất cả các cổng trên hệ thống máy tính. Nếu cổng đang lắng nghe, kết nối thành công, ngược lại thì cổng sẽ không đạt đến được. Điểm mạnh của kỹ thuật này là chúng ta không cần phải có đặc quyền.
- Việc quét bằng kỹ thuật này sẽ dễ dàng bị phát hiện bởi máy được quét.
- TCP SYN (haft – open): Kỹ thuật này thường được hiểu như là kiểu quét (haft – open) bởi vì bạn không mở một kết nối đầy đủ TCP. Bạn gửi một SYN packet, nếu như bạn đang mở một kết nối thực sự và bạn đang chờ hồi đáp. Một SYN /ACK chỉ cho biết cổng đang lắng nghe. Một RST biểu lộ của một Non – listener. Nếu một SYN/ACK được nhận, một RST ngay lập tức gửi liên tục đến kết nối. Thuận lợi chính của kỹ thuật quét này là ít site lưu lại thông tin của nó. Để thực hiện được chúng ta phải có quyền root.
- FTP Proxy (Bounce attack): Đây là một đặc điểm thú vị của giao thức FTP hỗ trợ cho những kết nối FTP thông qua proxy. Nói một cách khác chúng ta có thể kết nối từ Evil.com đến FTP server của target.com và yêu cầu server gửi một file ANYWHERE trên internet. Bây giờ điều này đã được thực hiện vào năm 1985 khi RFC đã được viết. Nhưng với hệ thống ngày nay, chúng ta không có thể chiếm đoạt FTPserver và gửi yêu cầu đến bất kỳ điểm nào trên internet một cách tùy tiện. Khi các khái niệm cũ về FTP server được viết lại vào năm 1995, sai lầm của giao thức này có thể được sử dụng để đưa news và mail gần như không thể phát hiện được, gây nguy hiểm trên những server tại những site khác nhau, làm đầy đĩa cứng … Chúng ta sẽ lợidụng những đặc điểm này để Scan TCP port từ một proxy FTP server. Vì thế bạn có thể kết nối đến một FTP server được đặt sau một Firewall và sau đó quét những port dường như đã bị blocked. NếuFTP server cho phép đọc và ghi trên một vài thư mục, bạn có thể

gửi bất kỳ dữ liệu đến những cổng mà bạn đã tìm thấy (NMAP thì không làm được việc này).

- ICMP (Ping Sweep – PingScanning): Thỉnh thoảng chúng ta chỉ muốn biết một host trên mạng có được mở hay không. NMAP có thể làm điều này bằng cách gửi ICMP echo request packet đến mọi địa chỉ IP trên mạng mà bạn chỉ định. Những host mà trả lời là những host đang mở. Một số site thi block echo request packets. Vì thế NMAPcó thể gửi một TCP ACK packet theo cổng 80. Nếu chúng ta nhận được một RST trả về, máy tính đó đang mở. Một kỹ thuật thứ ba liên quan đến việc gửi một SYN packet và chờ RST hay SYN/ACK. Mặc định (cho user root) NMAP sử dụng cả hai kỹ thuật ACK và ICMP. Bạn có thể thay đổi điều này với option – p.

  Chú ý rằng thao tác ping được thực hiện bắt cứ lúc nào và chỉ những host hồi đáp được quét. Chỉ sử dụng tùy chọn nếu bạn mong muốn ping sweep mà không cần bất kỳ port scans nào thực sự hoạt động.

- ACK Sweep (ACK Scan): Đây là một phương pháp thuận lợi thường được sử dụng để vạch ra những bộ luật firewall. Trong trường hợp đặc biệt, nó có thể giúp xác định nơi firewall không có hiệu quả hay chỉ là một bộ lọc packet đơn giản chỉ block những SYN packet.

- Các Scan này gửi một ACK packet đến một port được chỉ định. Nếu có RST trả về, port được phân loại là "unfiltered". Nếu không có bất cứ thông tin gì trả về (hay nếu một ICMP unreachable được trả về) port được phân loại là "filtered". Chú ý rằng NMAP thường không in ra những port được phân loại là "unfiltered".

- Xmas tree, FIN, Null Scan: Đó là những lần khi sử dụng quét SYN nhưng không bảo đảm bí mật. một vài firewall và packet filter có thể nhìn thấy tín hiệu SYN và giới hạn port và chương trình giống như SYN logger và courtney thì dễ dàng phát hiện ra việc quét này. Việc sử dụng những cách quét này (Xmas tree, FIN, Null Scan) sẽ có thể vượt qua được mà không bị cản trở.

- IP Protocol: Phương pháp này được sử dụng để xác định những giao thức IP nào được hỗ trợ trên host. Kỹ thuật này sẽ gửi những IP packet dạng raw mà không chứa bất kỳ protocol header đến từng giao thức được chỉ định tại host đích. Nếu chúng ta nhận một ICMP protocol unreachable message, điều đó có nghĩa rằng giao thức không được sử dụng, ngược lại chúng ta giả sử rằng nó được mở. chú ý rằng một vài host (AIX, HP – UX, Digital UNIX) và một số firewall không thể gửi protocol unreachable messages, đây là nguyên nhân làm cho hiểu lầm rằng tất cả giao thức đều được "open".

Cú pháp chuẩn như sau:

NMAP [Scan type (s)] [option] <host or net #1 … [#n]>

Scan type bao gồm:

- -sS: TCP SYN

- -sT: TCP connect ()
- -sU: UDP scan
- -sO: IP protocol
- -sF -sX -sN: Stealth FIN, Xmas tree, Null scan
- -sP: ping scanning
- -sV: version detection

Các Option chính như sau:

- -PA [portlist] sử dụng TCP ACK ping xem danh sách các host đang hoạt động
- -PS [portlist] tương tự -PA nhưng dùng SYN (connection request)
- -PU [portlist] dùng UDP

Ví dụ: Để quét tất cả các cổng TCP trên máy đích 172.29.14.141

Nmap –v 172.29.14.141

Tùy chọn –v: Mở chế độ hiển thị chi tiết quá trình quét.

Để quét một đường mạng lớp C mà có chứa địa chỉ IP 172.29.14.141 dùng tín hiệu SYN. Ngoài ra cũng xác định luôn cả hệ điều hành mà đang sử dụng tại mỗi máy là gì ? Có đang hoạt động hay không ? Để sử dụng được đặc điểm này, người sử dụng phải có quyền root.

Nmap –sS – O 172.29.14.141

2.4.2. Nghe lén (Sniffing):

Kẻ nghe lén phải nằm trong cùng đường mạng hoặc được đặt ở các vị trí cổng truy cập để đọc các thông tin được truyền trên mạng.

Sử dụng phần mềm để đón bắt các thông tin quan trọng (ví dụ tên truy cập, mật khẩu, cookie) truyền trên mạng mà không được mã hóa hoặc chỉ sử dụng những cơ chế mã hóa đơn giản.

Các quản trị mạng có thể sử dụng các công cụ sniff để xem xét và đánh giá lưu thông mạng.

A/ Giới thiệu công cụ TCP Dump:

Là công cụ phân tích phổ biến trong môi trường Unix hay Linux. TCP Dump hỗ trợ các giao thức TCP, UDP, IP và ICMP. Ngoài ra còn hỗ trợ các dạng dữ liệu của các ứng dụng phổ biến. Hầu hết chương trình TCP Dump phải chạy với quyền root hay được setuid là root.

Cú pháp TCP Dump như sau:

TCP Dump [-adefln Nopq RstuvxX]

[-c count]

[-C file _size]

[-F file]

[-i interface]

[-m module]

[- r file]

[-s snaplen]

[-T type]

[-U user]

[- w file]

[-E algo: secret]

[expression]

Các lưu ý:

- -c sẽ dùng khi bắt đủ số gói tin
- - C trước khi save raw packet vào file sẽ kiểm tra file hiện tại có kích thước lớn hơn file _size hay không. Nếu có thì mở một file mới với tên chỉ định là –w cộng với kích thước phía sau. Đơn vị của file _size là 1000000 bytes.

Ví dụ: Để in ra tất cả những packet đã được nhận và gửi đi từ máy có tên là sundown:

tcpdump host sundown

Để in ra sự lưu thông giữa hai hệ thống máy tính có tên là sundown và moondown:

tcpdump host sundown and moodown

Để in ra tất cả những gói tin IP giữa sundown và bất kỳ những host khác ngoại trừ máy có tên là testking:

tcpdump ip host sundown and not testking

B/ Giới thiệu công cụ Ethereal:

Là một trong những công cụ "phân tích giao thức" protocol analyzer mới nhất hiện nay, phát triển năm 1998. Ethereal có cả phiên bản cho Unix/Linux và windows. Một khi thực hiện bắt gói tin, packet sẽ được giữ trong buffer và sau đó được hiển thị lên màn hình. Một tính năng của Ethereal là live decodes ngay packet cho đến khi dừng việc bắt gói tin. Chúng ta có thể thấy điều nay qua Network monitor của windows sẽ trình bày sau. Tuy nhiên đây cũng là tính năng không tốt lắm nếu lưu lượng mạng khá nhiều 10000 packet chẳng hạn mà không thực hiện biện pháp lọc gói nào. Khi đó chúng ta không thể nào theo dõi kịp các thông tin trình bày.

C/ Giới thiệu công cụ Network monitor của windows:

Windows 2000, 2003 có hỗ trợ công cụ Network monitoring hỗ trợ các quản trị mạng theo dõi và phân tích các gói tin được gửi ra ngoài cũng như các kết nối truy xuất đến.

Thông thường nếu được cài đặt NW sẽ được đặt tại. Trong trường hợp không có ta có thể dễ dàng cài đặt thêm bằng cách:

Start → Setting → Control pannel → Add/Remove Program → Add/Romove Windows Components → Management and Monitoring tools.

Chạy chương trình:

Sau khi chọn Network interface nhấn start capture để bắt gói tin. Nhấn biểu tượng Stop and View capture để xem các gói tin bắt được. Ngay sau khi bắt được chúng ta đang ở panel đầu là panel liệt kê tóm tắt.

Bỏ chọn Zoom panel (thanh toolbar hình kính lúp) để xem cả 3 panel của các gói tin đã bị capture như sau:

Panel thứ hai là thông tin chi tiết và panel cuối cùng biểu diễn dưới dạng hex. Dùng Edit/Display Filter (thanh toolbar hình cái phễu) để lọc các gói tin.

D/ Giới thiệu công cụ Cain & Abel:

Đây là công cụ lắng nghe rất mạnh hỗ trợ các tính năng:

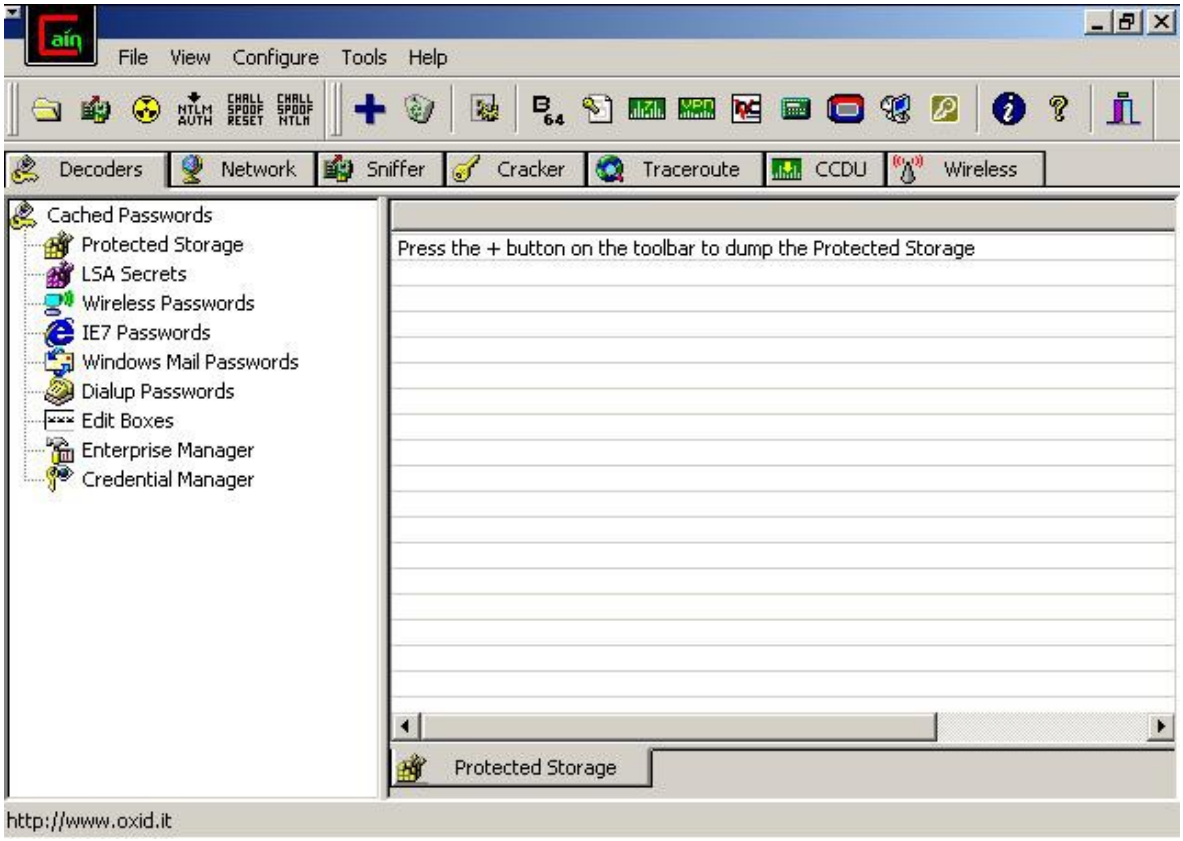
- Giả mạo địa chỉ ARP để thu thập được thêm nhiều thông tin
- Khả năng giải mã đối với một số password bắt được dưới dạng mã hóa.

Hướng dẫn sử dụng Cain & Abel để lắng nghe thông tin trên mạng LAN (thiết bị sử dụng trong mạng thuộc tầng 1 và 2)

Cài đặt chương trình Cain & Abel:

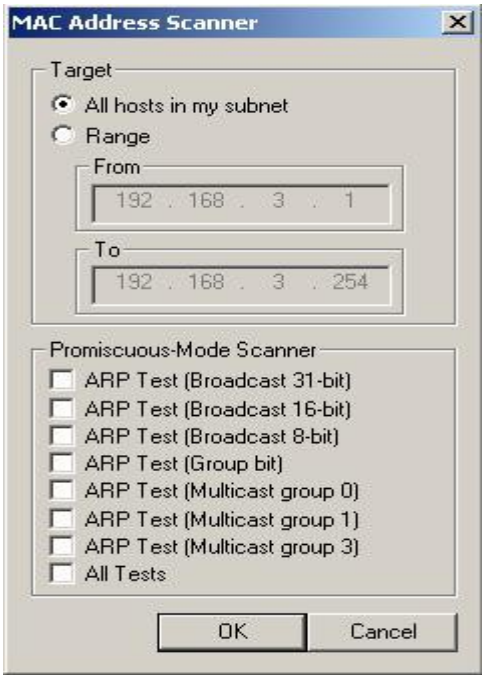
- Download chương trình Cain & Abel từ website: http://www.oxid.it/
- Cài đặt chương trình (cần cài đặt Winpcap v3.1 beta 4 trước khi sử dụng chương trình Cain & Abel)
- Sử dụng chương trình Cain & Abel để lắng nghe thông tin trên mạng.

Chạy chương trình Cain & Abel:



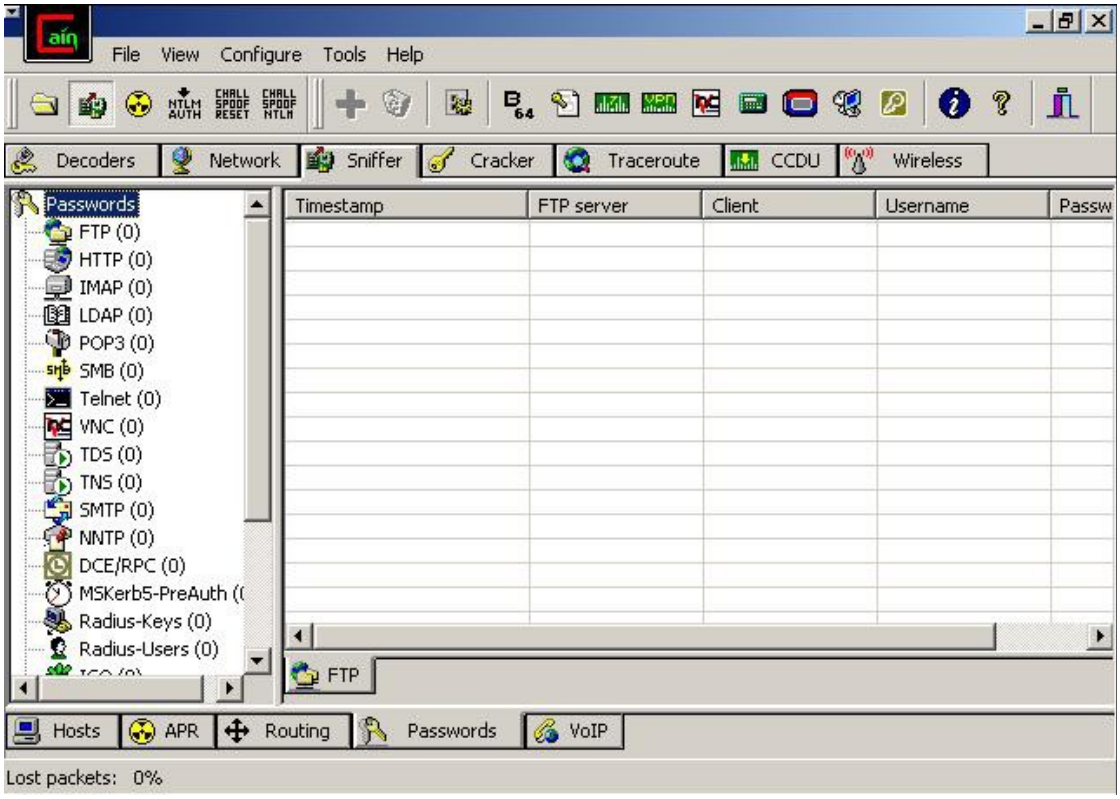
Chọn mục trên thanh công cụ để bắt đầu quá trình lắng nghe trên mạng, sau đó chọn tab Sniffer.

Tab Sniffer , chọn mục **Add to list** Trên thanh công cụ để quét danh sách các máy tính trên hệ thống mạng. Mọi thông tin trao đổi từ danh sách này sẽ được lắng nghe.



Lưu ý: Chúng ta chỉ quét được những máy tính thuộc cùng đường mạng với mình.

Chọn tab password để quan sát các thông tin trả về khi có sự trao đổi thông tin trên mạng.



Nếu password bị mã hóa chúng ta sẽ dùng chính chương trình Cain & Abel để giải mã hoặc dùng chương trình LC5. Có nhiều thuật toán để giúp cho việc giải mã thành công như:

- Giải mã dùng phương pháp Dictionary Attack
- Giải mã dùng phương pháp Brute – Force Attack
- Giải mã dùng phương pháp Cryptanalysis

2.5. Password Attacks:

Là phương pháp tấn công nhằm đoán ra password còn gọi là password guessing. Chúng ta có thể nghĩ ngay đến việc đoán password từ những thông tin liên quan đến user sử dụng nó: Ngày sinh, tên …

Có hai cách tấn công chình là Brute – Force Attack (vét cạn) và Dictionary – based Attack (dựa trên danh sách mật khẩu đã xây dựng trước)

2.5.1. Brute Force Attacks:

- Sử dụng các công cụ đoán mật khẩu bằng các quét cạn
- Khả năng để tìm ra mật khẩu sẽ rất cao nếu mật khẩu đơn giản

2.5.2. Dictionary – Based Attacks:

- Các mật khẩu có trong các từ trong tự điển rất dễ bị phá mật khẩu
- Cách phá mật khẩu sử dụng một danh sách các từ nằm trong tự điển đã được tính giá trị băm trước.
- Danh sách các từ và giá trị băm có thể tìm thấy trên internet.

2.5.3. Một số công cụ tấn công password:

Để tấn công password, chúng ta sử dụng các công cụ có khả năng giải mã được các password. Những công cụ mạnh có khả năng tấn công password đó như Cain & Able (xem phần trên), LC5 …

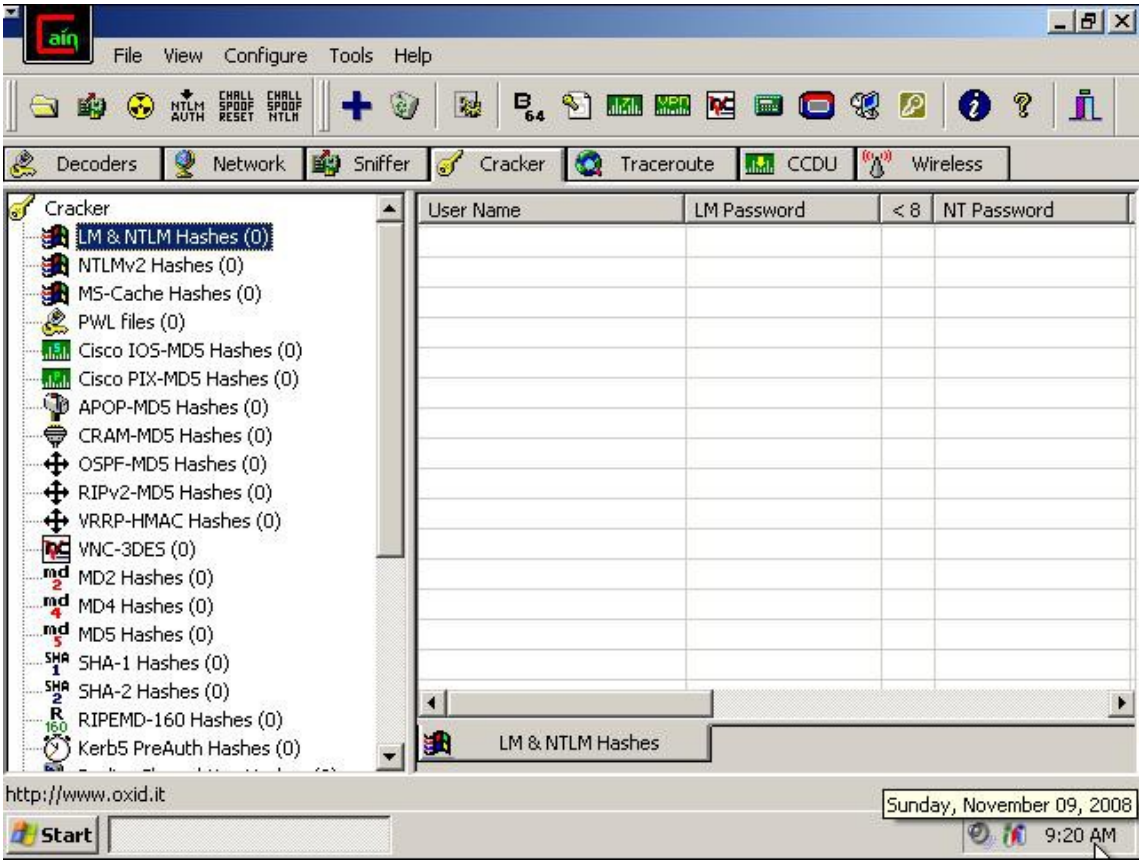
Ví dụ: Cách tấn công mật khẩu bằng phương pháp vét cạn

Sử dụng chương trình Cain & Able

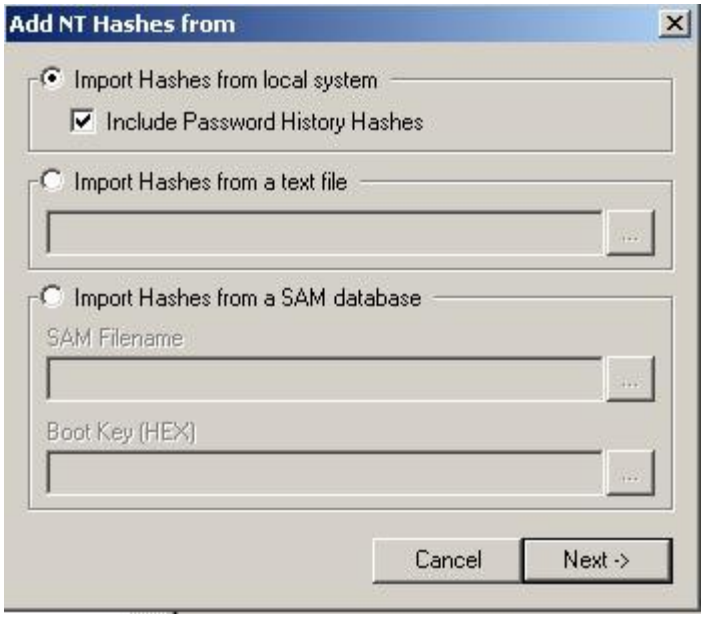
Mục tiêu: Lấy mật khẩu của các user trên máy cục bộ.

Cách thục hiện:

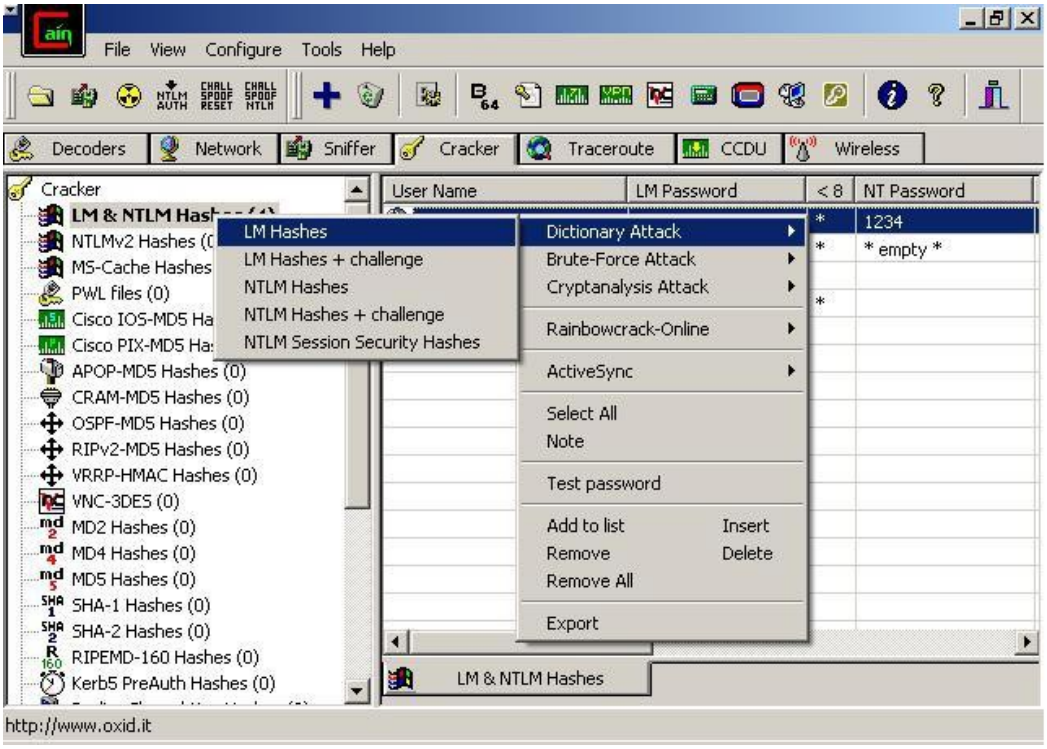
- B1: Kích hoạt chương trình Cain & Abel
- B2: Chọn tab **Cracker** tại panel bên trái, chọn mục **LM & NTLM Hash**. Sau đó chọn trên thanh công cụ chức năng **add to list**



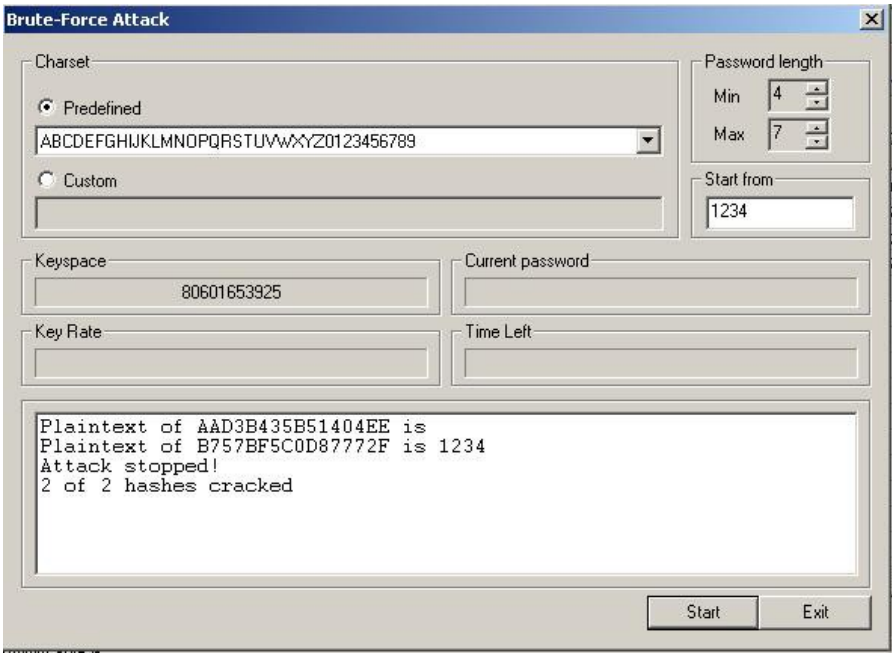
- Chọn mục Import Hashes from local machine chọn Next



- Click chuôt trên user cần lấy password, chọn mục Brute – Force Attack (NTLM)>LM hashes



- Cửa sổ **Brute – Force Attack** được hiện ra >Chọn **Start** để bắt đầu quá trình dò/giải mã/đoán password > Kết quả trả về là **1234**



2.6. Malicous Code Attacks:

2.6.1. Viruses:

Virus, wrom và trojan horse được gọi chun g là những đoạn mã nguy hiểm. chúng có thể chiếm dụng tài nguyên làm chậm hệ thống, hoặc làm hư hệ thống.

Virus là những chương trình được thiết kế để phá hoại hệ thống ở cả mức hệ điều hành và ứng dụng.

2.6.2. Trojan horse:

Trojan horse là một loại chương trình có vẻ an toàn và hữu ích nhưng thực sự bên trong của nó lại được nhúng những đaọn mã nguy hiểm.

2.6.3. Logic Bombs:

Những đoạn mã được tích hợp vào các ứng dụng và có thể được thực hiện để tấn công khi thỏa mãn một điều kiện nào đó (ví dụ các Script hay ActiveX được tích hợp trong các trang web)

Là một loại malware thường được attacker để lại trong hệ thống có tính năng tương tự "bom hẹn giờ". Logic bomb khi gặp những điều kiện nhất định sẽ phát huy tính năng phá hoại của nó. Một trong những logic bomb nổi tiếng là Chemobyl phát huy tính năng phá hoại của nó vào ngày 26/4.

Một cách dùng của logic bomb mà attacker hay dùng là để hủy các chứng cứ của đợt tấn công khi admin hệ thống bắt đầu phát hiện đột nhập.

2.6.4. Worms:

Worm cũng là một dạng virus nhưng nó có khả năng tự tạo ra các bản sao để phát tán, ây lan qua mạng.

Điểm khác biệt lớn nhất giữa worm và virus: Worm là một chương trình độc lập có thể tự nhân bản, lây lan qua mạng bằng nhiều cách nhưng thông thường nhất là E - mail và Chat. Worm cũng có thể thực hiện các phá hoại nguy hiểm. Trong khi đó virus là một đoạn mã nguy hiểm được gắn trong một chương trình khác. Vì thế virus chỉ được kích hoạt khi chương trình có chứa virus được thực thi.

2.6.5. Back door:

Một chương trình, một đoạn mã hay những cấu hình đặc biệt trên hệ thống mà chúng ta không biết cho phép attacker có thể truy cập mà không cần chứng thực hay logon.

3. CÁC PHƯƠNG PHÁP PHÒNG CHỐNG:

3.1. Giới thiệu công cụ Essential NetTools:

Essential NetTools là một bộ công cụ bao gồm Netstat , Nslookup, Tracert, Ping, … Việc sử dụng các lệnh này trên windows thì rất là phức tạp khó đánh giá được. Tuy nhiên, với bộ công cụ này, việc sử dụng tương đối đơn giản nhờ giao diện thân thiện, dễ dùng và tài lệu hướng dẫn chi tiết và đầy đủ.

Với công cụ Essential NetTools, người quản trị mạng có thể giám sát mọi hoạt động xảy ra trên hệ thống máy tính (kiểm tra xem có người nào đang tấn công bằng SYN flood)

Giải pháp:

- Loại bỏ những dịch vụ không cần thiết
- Sử dụng tường lửa hay IP Sec để lọc thông tin không cần thiết
- Sử dụng IDS để phát hiện các thăm dò và thông báo các truy cập khả nghi

3.2. Giới thiệu công cụ Microsoft Baseline Security Analyzer:

Mục tiêu:

Tìm hiểu cách thực phát hiện lỗ hỏng bảo mật trên máy cục bộ và mạng, diễn giải được các bản báo cáo trả về.

Cách thực hiện:

- Sử dụng công cụ Microsoft Baseline Security Analyzer (MBSA) để kiểm tra lỗ hỏng trên hệ điều hành windows.
- Nghiên cứu các lỗ hỏng bảo mật được tìm thấy và cung cấp cách vá những lỗ hỏng đó.
- Sử dụng MBSA để quét những điểm yếu của hệ thống windows

Cài đặt MBSA:

Kích hoạt chương trình MBSA

Chọn Scan a computer

Chọn Start Scan để bắt đầu dò lỗ hỏng, bản báo cáo sẽ được trả lời như sau:

Với những Score có biểu tượng **X** là những lỗ hỏng nghiêm trọng nhất.

Chọn mục Result details để xem chi tiết về lỗ hỏng bảo mật. chọn mục how to correct this để tìm ra phương thức khắc phục vấn đề.

Chú ý: khi muốn quét lỗi bảo mật từ các hệ thống khác, chúng ta chỉ cần nhập tên hay IP của máy cần quét.

3.3. Sử dụng công cụ Tenable NeWT Scanner:

Mục tiêu:

Tìm hiểu cách thức phát hiện lỗ hổng bảo mật trên máy cục bộ, diễn giải được các báo cáo trả về.

Cách thực hiện:

- Sử dụng NeWT để dò những lỗ hổng bảo mật trên máy cục bộ
- Tìm hiểu các lỗ hổng được tìm thấy và cung cấp cách vá lỗ hổng
- Sử dụng NeWT để quét những nơi bị tấn công trên hệ thống cục bộ

Cài đặt chương trình Tenable NeWT Scanner:

Kích hoạt chương trình NeWT Security Scanner

Chọn New Scan task để bắt đầu quá trình quét

Nhập vào tên hoặc địa chỉ IP của máy cần quét → chọn Next

Chọn Scan now để bắt đầu scan. Sau khi quá trình quét thành công. Một thông báo sẽ hiển thị ra như sau:

Dựa trên bản báo cáo trả về, chúng ta đưa ra các giải pháp để khắc phục lỗi.

3.4. Xây dựng Firewall để hạn chế tấn công:

Để ngăn chặn sự xâm nhập bất hợp pháp của người dùng mạng, chúng ta cần xây dựng các hệ thống phòng thủ. Firewall là một giải pháp tốt cho vấn đề này. Việc xây dựng firewall có thể dùng thiết bị phần cứng hoặc sử dụng giải pháp phần mềm. Trong phần này chúng ta sẽ hiểu hai giải pháp này.

3.4.1. Giải pháp phần cứng:

Hiện nay trên thị trường có rất nhiều sản phẩm cho phép thiết lập firewall từ đơn giản đến phức tạp. Các firewall được tích hợp trong các thiết bị nối đường truyền ADSL hay trong các thiết bị Load Balance Router cũng như các sản phẩm firewall chuyên dụng như Fotinex, Juniper, Check Point, … Tùy vào mức độ của hệ thống mạng mà chúng ta sẽ sử dụng các loại firewall tương ứng. Trong phần này, chúng ta sẽ tìm hiểu một số tính năng của firewall trên sản phẩm Load Balance Router.

Với thiết bị Load Balance Router của hãng Dray tek (vigor 3300V) sử dụng các tính năng để hạn chế người dùng trong và ngoài mạng như:

A/ IP Filter:

Đây là một tính năng để lọc các thông tin từ mạng trong đi ra ngoài và ngược lại.

B/ Dos:

Đây là một tính năng cho phép giới hạn sự tấn công của các máy tính bên ngoài sử dụng Dos.

C/ URL Filter:

Đây là một tính năng cho phép lọc nội dung địa chỉ website truy cập

D/ Bind IP to MAC:

Đây là một tính năng để giới hạn những người dùng không hợp lệ có thể truy cập sử dụng đường internet hiện tại.

E/ IM/P2P Blocking:

Đây là một tính năng cho phép cấm một hoặc một vài địa chỉ IP truy cập vào các dịch vụ tin nhắn, VoIP hay các dịch vụ chia sẽ dữ liệu ngang hàng.

3.4.2. Giải pháp phần mềm:

Ngoài các giải pháp sử dụng phần cứng, chúng ta còn có thể sử dụng các giải pháp phần mềm để hạn chế sự xâm nhập từ các máy khác. Từ Windows XP trở về sau này, các phiên bản đều tích hợp cách thức thiết lập firewall cơ bản để bảo vệ máy tính. Nếu chúng ta mong muốn bảo vệ an toàn trên mạng, có một số phần mềm giải quyết các giải pháp đó như ISA, Kerio Win Route Firewall, Zone Alam, … Trong phần này chúng ta sẽ sử dụng ISA 2004 để xây dựng firewall.

Phần mềm ISA 2004 cung cấp cho chúng ta nhiều giải pháp để xây dựng firewall và hạn chế sự xâm nhập bắt hợp pháp của người dùng trên mạng. Các môn học trước chúng ta đã tìm hiểu cách thức thiết lập bộ lọc để hạn chế người dùng trong mạng truy cập ra ngoài cũng như mở một số cổng dịch vụ cần thiết để cho phép các máy bên ngoài mạng truy cập vào trong nội bộ. ngoài ra trên ISA 2004 chúng ta còn có thể giới hạn được số lượng phiên (session) được mở đồng thời cũng như hạn chế được các tấn công theo dạng Dos.

CHƯƠNG 2

BẢO MẬT VỚI LỌC GÓI IP

1. Gói Tin (Packet):

1.1 Packet là gì?

- Như chúng ta đã biết các tín hiệu trao đổi giữa hai máy tính là các tín hiệu điện dưới dạng các bít nhị phân 0/1.

- Với việc truyền dữ liệu dưới dạng các bít nhị phân đơn thuần thì chúng ta không thể nào biết được thông tin nhận được là thông tin gì, nó thuộc kiểu dạng dữ liệu nào, và nó gởi cho ứng dụng mạng nào trên máy nhân gói tin.

- Để khắc phục các khó khăn đó người ta đưa ra khái niệm gói tin (data packet). Theo khái niệm này thì thông tin dữ liệu trước khi được gởi đi nó sẽ được chia thành nhiều phần nhỏ, các phần nhỏ này trước khi được gởi đi nó sẽ được đóng vào một khuôn dạng nào đó gọi là gói tin sau đó nó mới được gởi đi. Trong gói tin có một phần dùng để chứa đựng các thông tin về nơi gởi và nhận, cũng như các phương pháp kiểm soát lỗi, mã hóa, … gọi là phần mào đầu của gói tin (data packet header)

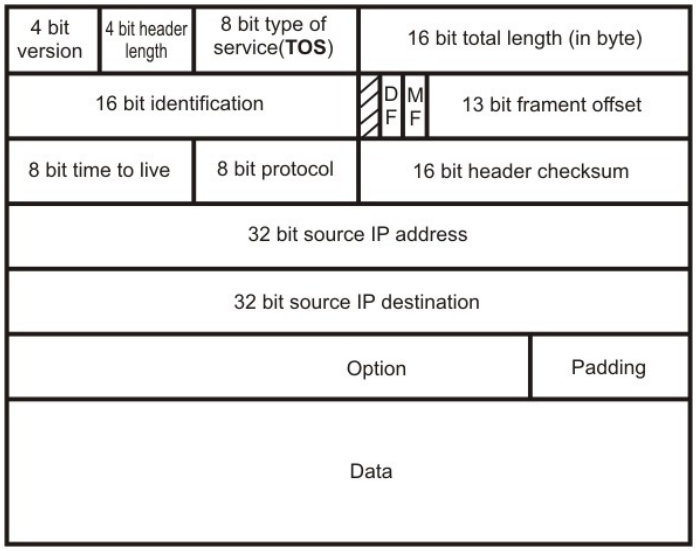
- Giao thức TCP/IP là một trong những giao thức phổ biến nhất hiện nay sử dụng phương thức truyền dữ liệu dưới dạng gói tin. Trong giao thức này nó có rất nhiều loại gói tin như: gói TCP, gói IP, gói UDP,…

1.2 Gói IP:

Đây là loại gói tin được sử dụng trong giao thức IP (internet protocol) ở lớp Internet trong mô hình TCP/IP

Gói tin này có chức năng là đảm bảo cho việc truyền dữ liệu một cách chính xác từ máy đến máy.

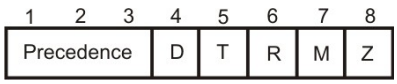
Cấu trúc của gói IP như sau:



Version : trường này có 4 bit nó cho biết phiên bàn của giao thức IP đang được sử dụng . Số version náy hết sức quan trọng nhất là ngày nay ta đang tồn tại hai phiên bản IP song song . Một số phần mềm ứng dụng trên giao thức này khi xử lý một IP datagram nó bắt buột phải biết được số version , nếu nó không nhân biết được số version thì coi như gói tin dó bị lỗi và không được chấp nhận để được xử lý tiếp theo .

Header Length : trường này có độ dài 4 bít , nó cho biết số word được sử dụng IP header , ta sừ dụng trường này bởi vì IP header có hai cấu trúc là short_IP_header có 20 byte , long_IP_header có 24 byte do có sử dụng trường option .

Type Of Service : có độ dài 1 byte cho biết cách thức sử lý gói tin khi nó được truyền trên mạng .



Ba bít đầu tiên cho biết mức độ ưu tiên của gói tin

000 : thấp nhất

111: cao nhất

Bit D quy định về độ trễ

1 : yêu cầu độ trễ thấp

0 : bình thường

Bit T chỉ thông lương yêu cầu

1 : yêu cầu thông lượng cao

0 : bình thường

Bít R chỉ độ tin cậy yêu cầu

1 : độ tin cậy cao

0 : bình thường

Bit M yêu cầu về chi phí

1 : chi phí thấp

0 : bình thường

Bít Z chưa được sử dụng .

Total Length : Cho biết độ dài của toàn bộ của một IP datagram bao gồm cả header , đơn vị tính là byte . Nó có giá trị thấp nhất là 20byte và lớn nhất là 65535 byte . Trường này dùng để xác định độ lớn của phần data .

Identification : có độ dài 16 bít , dùng cho việc đánh số các gói tin khi truyền đi , nó cho biết thứ tự của gói tin , số thứ tự này được cho bởi đầu phát và không bị thay đổi trong quá trình đi từ nguồn tới đích .

DF *(don't fragment):* bít này cho biết gói tin đó có được phép chia nhỏ trong suốt quá trình truyền hay không

1 : không cho phép chia nhỏ

0 : cho phép chia nhỏ

MD *(more fragment) :* cho biết sau nó còn có gói tin nào khác hay không .

1 : còn một gói tin đứng sau nó

0 : không còn gói tin nào đứng sau nó

bít này chỉ được sử dụng khi DF có giá trị 0

Fragment offset : có độ dài 13 bít , đơng vị tính của trường này là octect (1 (1 octect = 8 byte) nó cho biết vị trí của octect đầu tiên cùa gói bị phân mảnh trong quá trình truyền so với vị trí của octect thứ 0 của gói gốc . Trường này chỉ được sử dụng khi DF có giá trị là 1 .

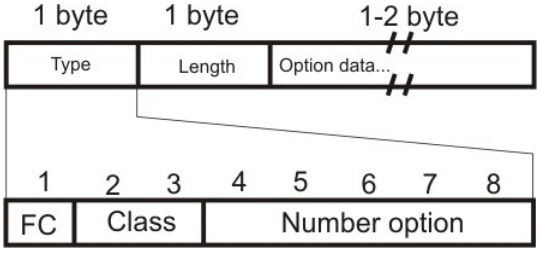
Time To Live : có độ dài 1 byte , nó qui định thới gian sống của một gói tin , đơn vị tính là số nút mạng mà nó đi qua , thời gian sống được thuyết lập khi gói tin được gởi đi , và cứ mỗi lần đi qua một nút mạng thời gian sống của nó giảm đi một , nếu thời gian sồng bằng 0 trước khi gói tin đi tới đích thì nó sẽ bị hủy . Mục đích là hạn chế tắc ngẽn trên đường truyền .

Protocol : có độ dài 1 byte , nó cho biết giao thức được sử dụng ở lớp trên . VD : TCP (6) ; UDP (17) ……

Header Checksum : có 16 bit dùng để kiểm tra lỗi của IP header , trường này có thể thay đổi sau mỗi lần qua một nút mạng nếu DF = 1 . Trường này dùng phương pháp kiểm tra lỗi CRC .

Source/Destination address : chi biết địa chỉ nguồn và địa chỉ đích , mỗi trường có độ dài 32 bít .

Option : trường này có độ dày từ 3 đến 4 byte , nó có thể được hoặc không được sử dụng . Nó cung cấp các thông tin về kiểm tra lổi , đo lường , ….



FC (flag copy) : bít này có chức năng là có sao chép trường option khi phân mảnh (đoạn) hay không .

1 : sao chép trường option cho tất cả các phân đoạn .

0 : chỉ có phân đoạn đầu tiên có trường option , các phân đoạn còn lại thì không có trường option .

Class : có 2 bít nó có các giá trị sau :

00 : dùng cho điều khiển datagram

10 : dùng cho mục đích điều hành

bản giá trị của trường type cùa option :

FC	class	Number option	Ý nghĩa
1	00	00000	Marks the end of the options list
1	00	00001	No option (used for padding)
1	00	00010	Security options (military purposes only)
1	00	00011	Loose source routing
1	00	00111	Activates routing record (adds fields)
1	00	01000	Tream ID
1	00	01001	Strict source routing
1	10	00100	Timestamping active (adds fields)

Length : cho biết độ dài của trường option bao gồm cả trường type và length

Option data : dùng để chứa đựng các thông tin liên quan do đến trường type .

Padding : trường này được sử dụng khi trường option có độ dài nhỏ hơn 4 byte , trên thực tế trường này chỉ là bộ đệm lót them vào để cho dầy cấu trúc khung.

Data : dùng để chứa dữ liệu của gói tin . Nó có độ dài không cố định , tùy thuộc vào độ lớn của thông tin truyền đi cũng như môi trường mạng .

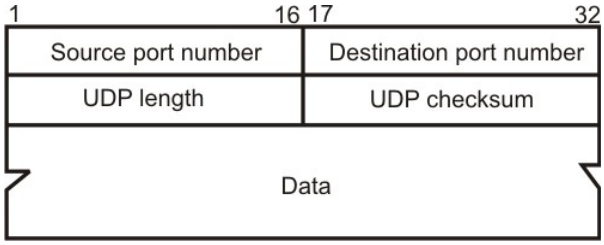
1.3. Gói UDP:

Chức năng và cấu trúc:

Chức năng:

Đây là gói tin được sử dụng trong giao thức UDP chức năng của nó là đảm bảo cho dữ liệu được truyền từ ứng dụng trên host nguồn đến một ứng dụng trên host đích một cách chính xác dựa trên phương pháp hoạt động không kết nối.

Cấu trúc gói tin:



Source port number : cho biết địa chỉ của ứng dụng nguồn gởi gói UDP đi .

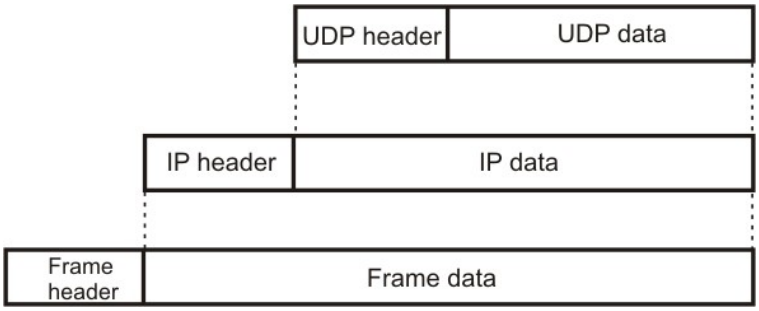
Destination port number : cho biết địa chỉ của ứng dụng đích sẽ nhận gói UDP đó

UDP length : cho biết độ dài của gói UDP bao gồm cả phần header và phần data .

UDP checksum : đây là vùng tùy chọn , nó có thể được hoặc không được sử dụng , khi không được sử dụng nó có giá trị là 0 , nhưng khi muốn đảm bảo sự an toàn cũng như độ chính xác của gói tin thì trường này mới được sử dụng .

Hoạt Động Của UDP

Đóng gói UDP :

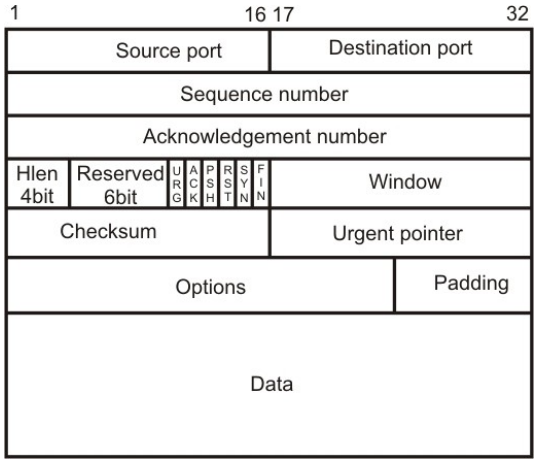


hình 4.2 : quá trình đóng gói UDP

Hoạt động :

Đây là một giao thức hoạt động theo phương thức không liên kết . Tức là khi một ứng dụng trên host nguồn muốn gởi dữ liệu đến host đích mà sử dụng giao thức UDP thì nó chỉ việc gởi dữ liệu đi mà không cần biết dữ liệu đó có tới được host đích hay không .
UDP chỉ được sử dụng với các ứng dụng không yêu cầu độ tin cậy cao hoặc đòi hỏi tính thời gian thực như : TFTP , BOOTP , Multimedia (intenet vedeo , VoIP ….)

1.4 Gói TCP:



Sequence number : đơn vị tính là octect , nó cho biết vị trí của byte đầu tiên trong trường data trong luồng dữ liệu truyền đi . Trường này có giá trị từ 0 đến 2^{32} 1 .
Khi mới bắt đầu kết nối sequence number chứa đựng giá trị đầu tiên của nó , giá trị này do host nguồn chọn và thường không có giá trị cố định . Khi gói dữ liệu đầu tiên được gởi đi nó có giá trị bằng giá trị đầu cộng thêm 1 .
Tổng quát trường sequence number có thể được tính như sau :

$sequence\_number_n$ $sequence\_number_{n+1}$ $len(data_{n+1})$

Acknowledgement number : trường này cho biết gói tin mà nơi gởi muốn thông báo cho nơi nhận biết là nó đang đợi phía nhận gởi cho nó gói tin có số sequence number có giá trị bằng với giá trị của Acknowledgement number , khi nhận được thông báo này nơi nhận xác định được rằng các gói tin mà nó gởi đến đầu kia trước đó đã đến đích an toàn .

Hlen : cho biết độ dài của phần TCP header , nhờ vào trường này mà đầu thu biết được trường Option có được xử dụng hay không .

Reserved : trường này hiện chưa được sử dụng .

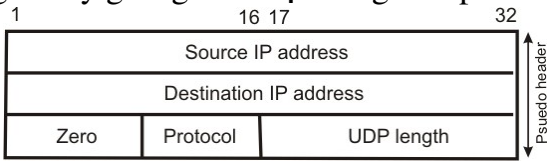
Flag bit : trường này có 6 bít cờ , mỗi bít được sử dụng vào các mục đích khác nhau , nó gồm các bít sau :

URG : cho biết trường Urgent pointer có hiệu lực hay không
ACK : cho biết ACK number có được sử dụng hay không
PHS : 1 _ đưa thẳng lên lớp trên không cần kiểm tra .
0 _ kiểm tra trước khi đưa lên lớp trên .
RST : yêu cầu thiết lập lại kết nối .
SYN : thiết lập lại số trình tự .
FIN : kết thúc truyền tải .

Window : cho biết độ lớn của của host nguồn

Checksum : dùng để kiểm tra lỗi của của gói TCP , việc kiểm tra lỗi do đầu nhận thực hiện . Việc tính toán do phía gởi đảm nhận . TCP sử dụng mã CRC để kiểm tra lỗi .

Khi tính toán trường Header checksum người ta thêm vào gói UDP một phần đầu giả , nội dung của phần đầu giả này giống như nội dung của phần đầu giả của UDP :

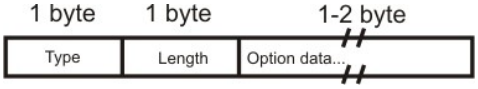


Urgent pointer : đây là trường con trỏ khẩn cấp , nó có các chức năng như :

Ngăn cản một quá trình nào đó trong quá trình truyền tải

Dùng để chỉ ra ranh giới giữa giữa phần dữ liệu khẩn cấp v1 phần dữ liệu thường (trong TCP phần dữ liệu khẩn cấp được đặt trước) .

Option : trường này là túy chọn , nó có cấu trúc giống như trường Option cùa IP :



Type : cho biết loại thông điệp option
Length : cho biết độ dài của trường option
Optiondata : chứa nội dung của trường option

Các loại thông điệp option :

Type number	length	means
0	-	Kết thúc của option list

1	-	Không sử dụng
2	4	Cho biết kích thước tối đa của 1 phân đoạn
3	3	Thông báo về sự thay đổi của cửa sổ
4	2	Shack permit
5	X	shack
8	10	Timestamp

2. Bảo Mật Với Lọc Gói:

2.1. Khái Quát Về Lọc Gói:

Bảo mật dựa trên lọc gói tin là phương pháp bảo mật dựa trên các thông tin ở phần header của các gói tin, thông qua các thông tin này mà ta có thể quy định gói tin nào được phép hay không được phép trển qua bộ lọc.

Các thông tin mà chúng ta quan tâm đến là các thông tin như địa chỉ của máy gởi và nhận gói tin, địa chỉ của ứng dụng nhận và gởi gói tin, giao thức sử dụng trong suốt qua trình trao đổi thông tin giữa hai máy.

2.2 Các Bước Để Xây Dựng Luật Bảo Mật Trong IPSEC:

Bước 1: Xác định bộ lọc gói tin:

- Bộ lọc gói tin có chức năng cho phép hay ngăn cấm một hay một số loại gói tin được phép hay không được phép truyển qua nó.
- Các bước xây dựng bộ lọc như sau:

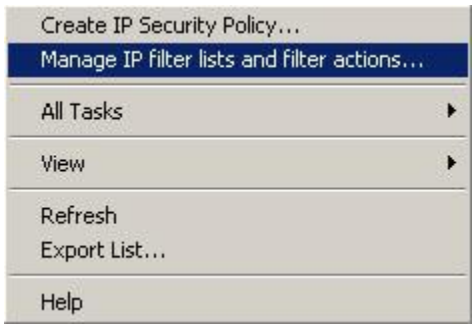
> Khởi động IPSEC:

→ vào administrative tool

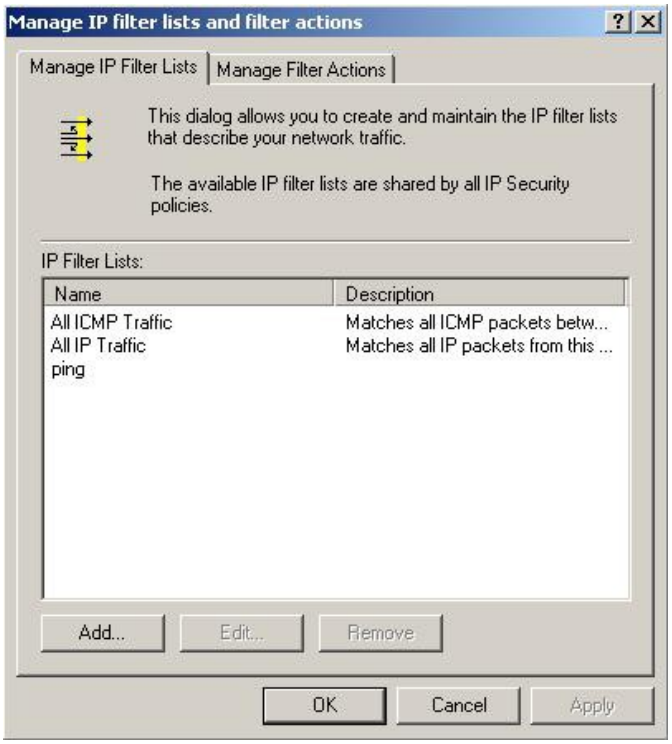
→ Local security policy

→ Right click lên IP security policies

→ manage ip filter list …..



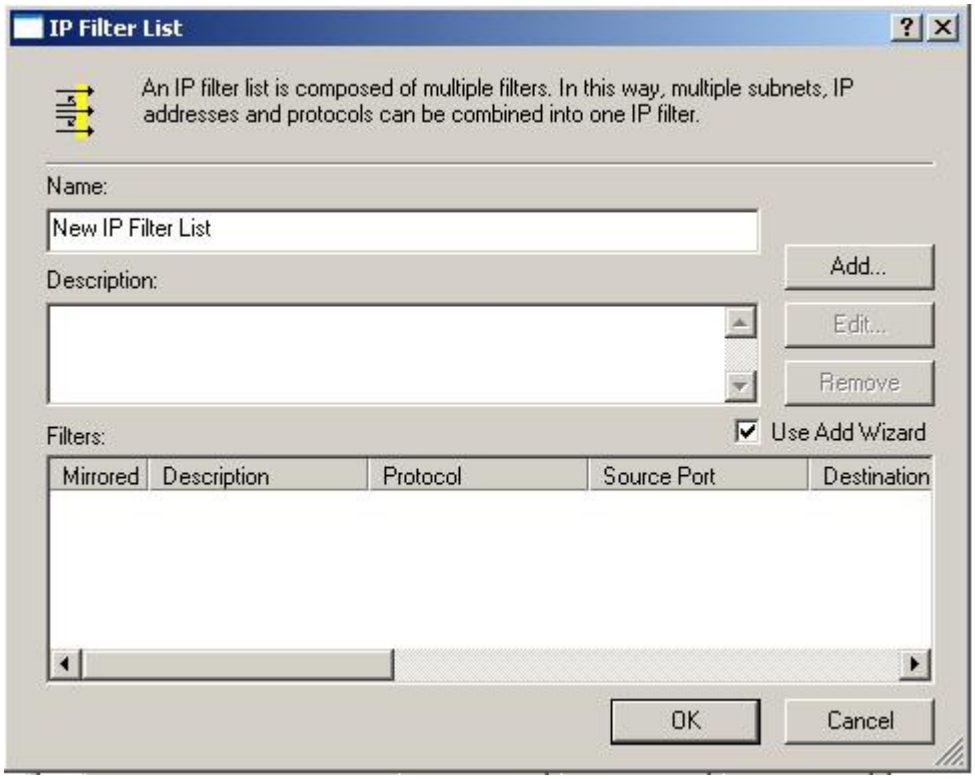
→ xuất hiện hộp thoại:



→ chọn mục manage ip filter list and filter action

→ chọn add để tiến hành tạo bộ lọc mới:

Xuất hiện hộp thoại sau:

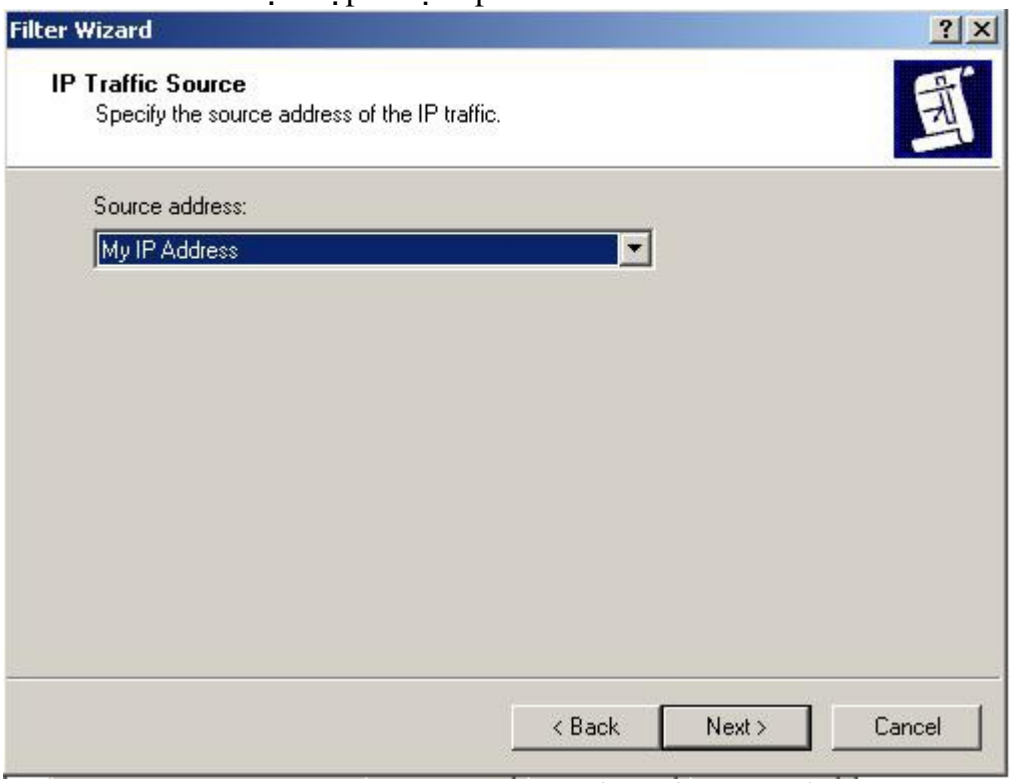


- name: cho phép khai báo tên của bộ lọc
- Description: cho phép gõ vào các mô tả chi tiết của bộ lọc

- Filters: cho phép khai báo các chức năng của bộ lọc
- Add: cho phép thêm vào bộ lọc 1 chức năng mới
- Edit …: cho phép hiệu chỉnh (thay đổi) 1 chức năng có sẵn của bộ lọc
- Remove: cho phép xóa 1 chức năng của bộ lọc

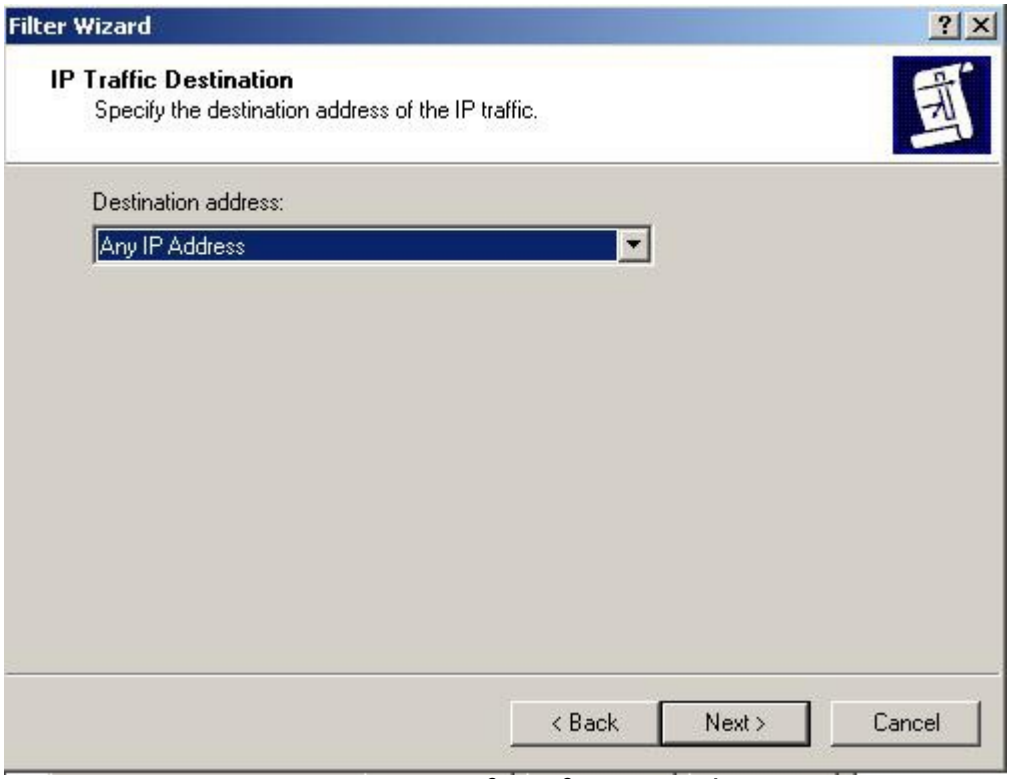
Chọn add để thêm 1 chức năng vào bộ lọc

→ next → xuất hiện hộp thoại: ip trafic source



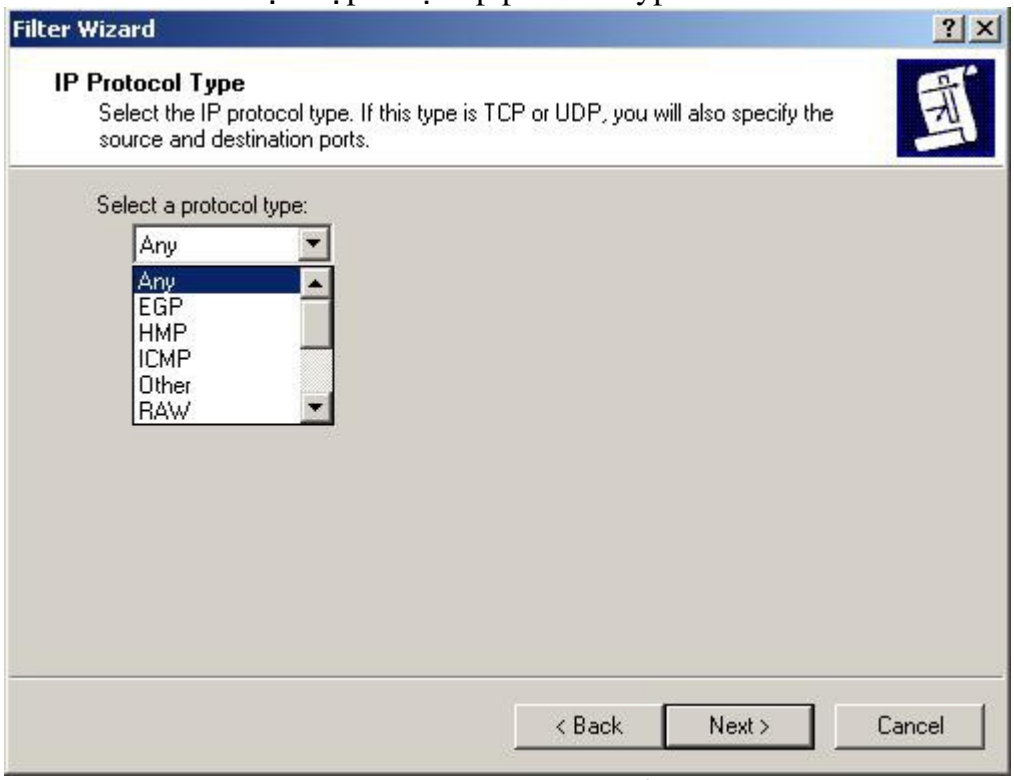
Hộp thoại này cho phép ta khai báo địa chỉ ip của máy gởi gói tin

→ next → xuất hiện hộp thoại: ip trafic destination



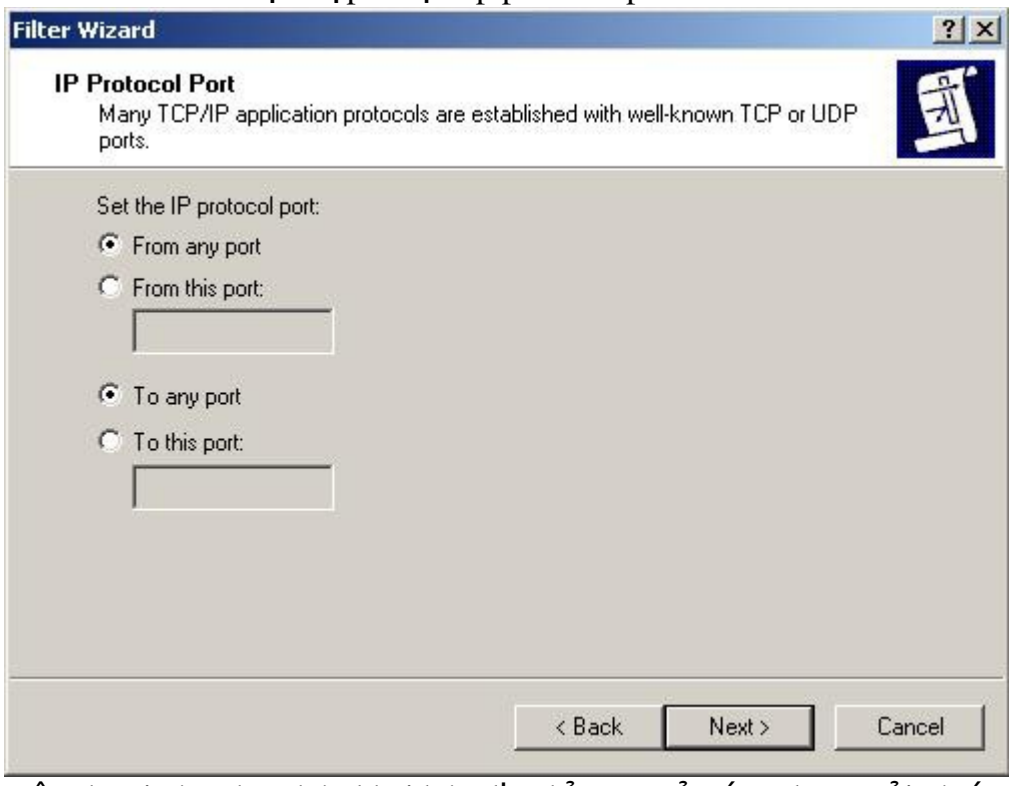
Hộp thoại này cho phép khai báo địa chỉ ip của máy nhận gói tin

→ next → xuất hiện hộp thoại: ip protocol type



Hộp thoại này cho phép xác định giao thức sử dụng trong bộ lọc là giao thức gì (chọn TCP)

→ next → xuất hiện hộp thoại: ip protocol port

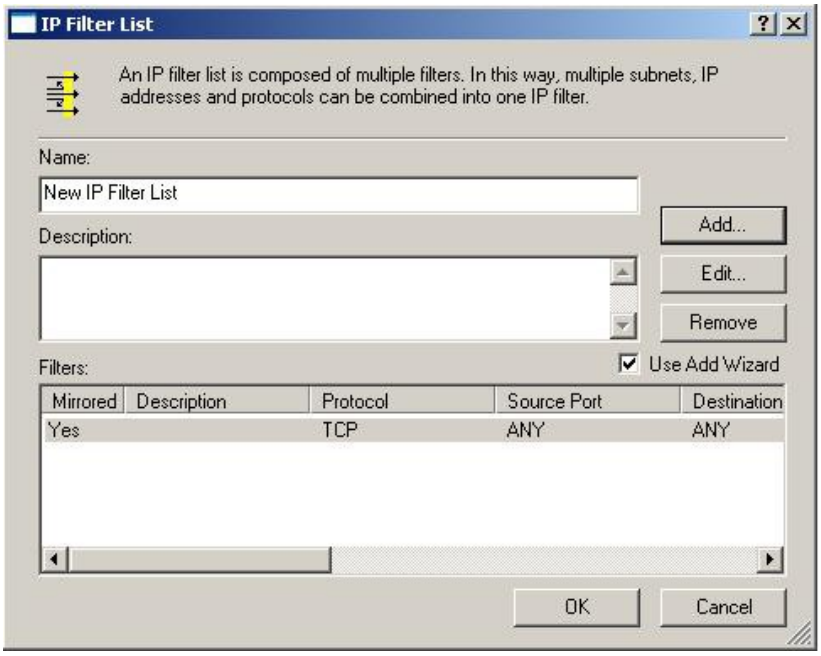


Hộp thoại này cho phép khai báo địa chỉ port của ứng dụng gởi và ứng dụng nhận gói tin

- From any port/ from this port: mục này cho phép khai báo địa chỉ port của ứng dụng gởi gói tin
- To any port/ to this port: mục này cho phép khai báo địa chỉ port của ứng dụng nhận gói tin.

→ next → finish: để hoàn tất việc xây dựng 1 chức năng cho bộ lọc

<u>Chú ý</u>:tới bước này chúng ta có thể bấm ok để kết thúc việc xây dựng bộ lọc, hoặc chon add để thêm vào bộ lọc 1 chức năng lọc khác.

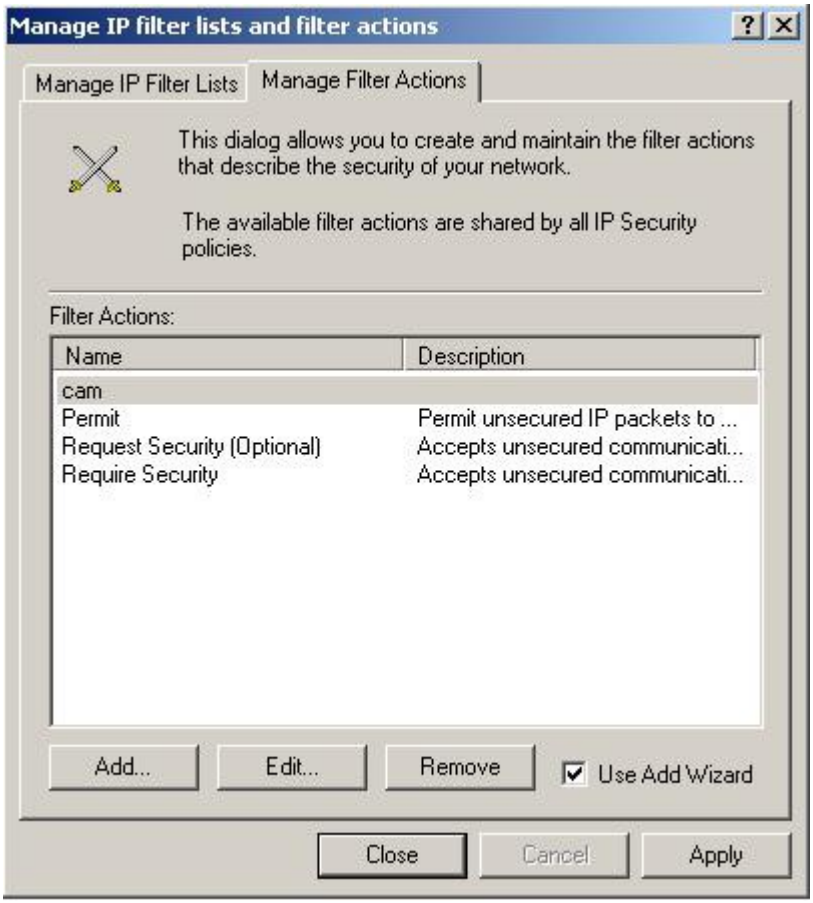


<u>Bước 2: xác định các hành động của bộ lọc:</u>

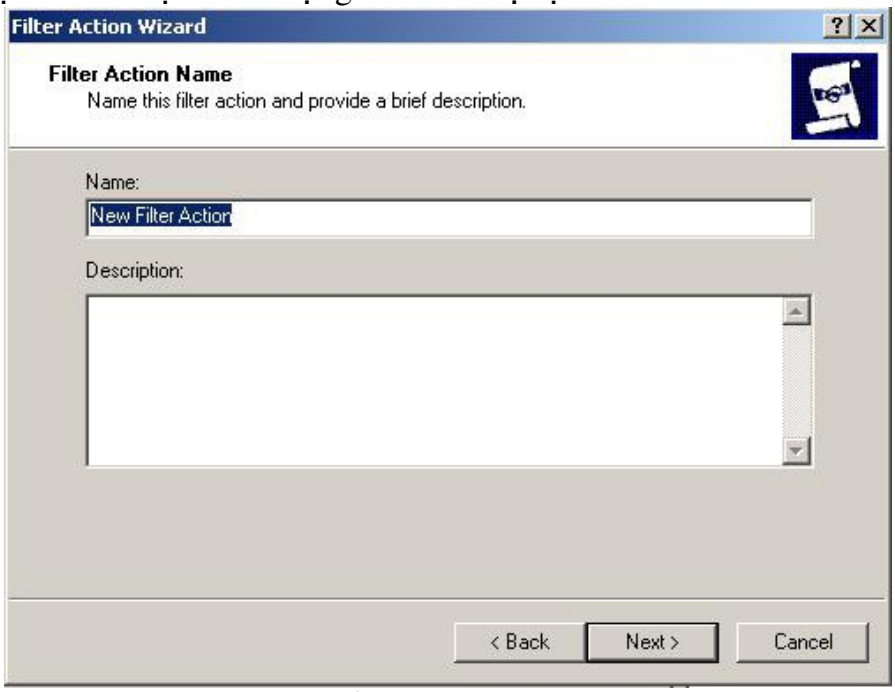
Chúng ta có 3 loại hành động cơ bản của bộ lọc:

- Permit: cho phép
- Block: ngăn cấm (khóa)
- Negotiate security: mã hóa dữ liệu khi truyền

→ Tại cửa sổ manage ip filter list and filter action → chọn manage filter action



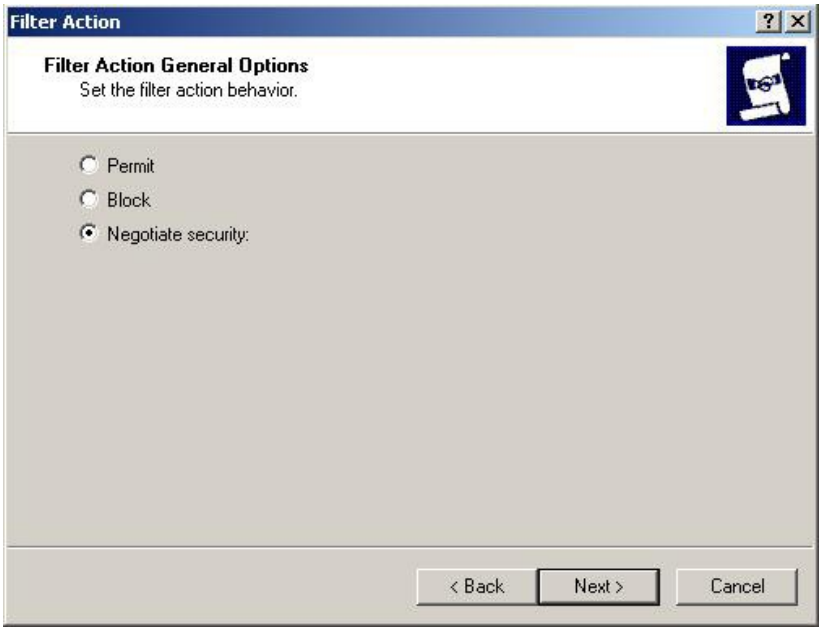
→ chọn add để tạo hành động mới cho bộ lọc:



Name: cho phép khai báo tên của hành động

Description: phần mô tả chi tiết cho hành động đó

→ next → filter action general option: hộp thoại này cho phép khai báo các hành động tương ứng của bộ lọc như: ngăn cản, cho phép, mã hóa dữ liệu:



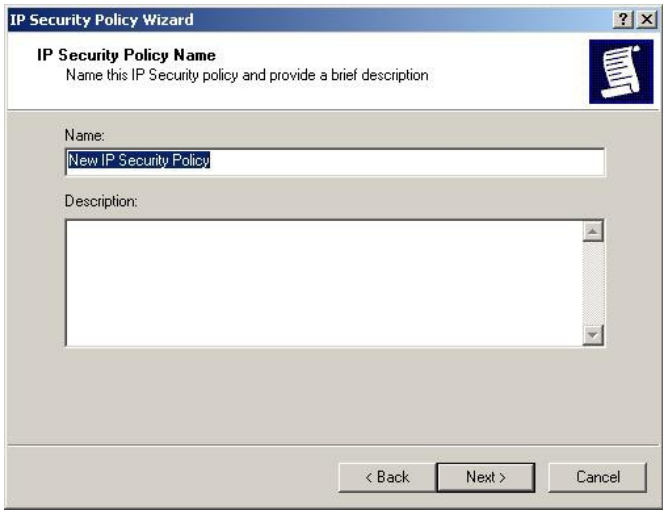
→ next → finish để hoàn tất việc tạo action filter

Bước 3: xây dựng luật:

→ right click lên ip security policy local computer

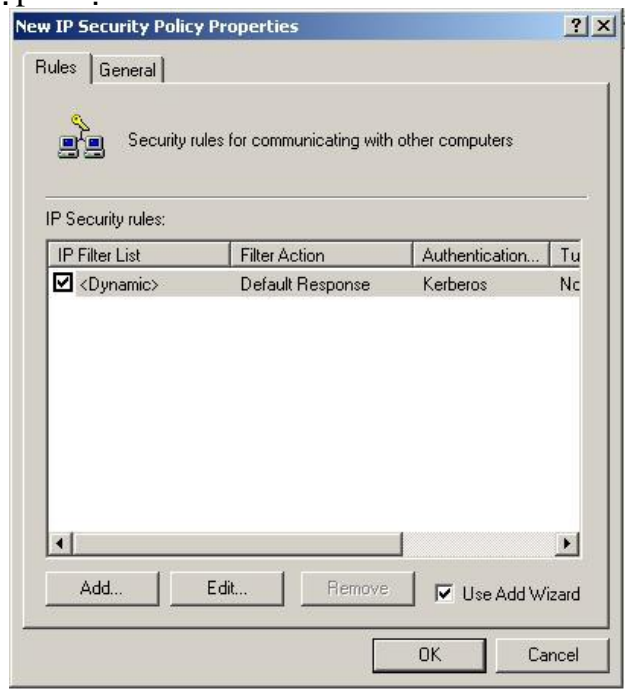
→ chọn create ip security policy

→ xuất hiện hộp thoại: ip security policy name: mục này cho phép khai báo tên của luật đang được xây dựng:



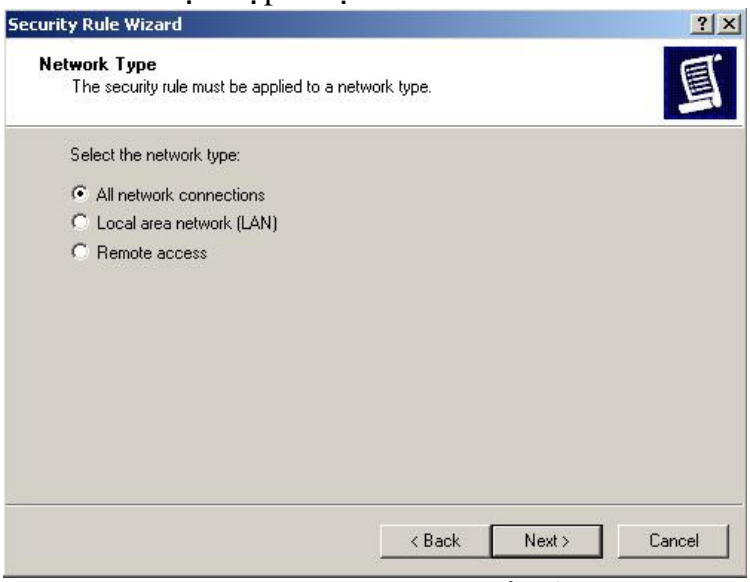
→ next → … → finish

→ xuất hiện hộp thoại:



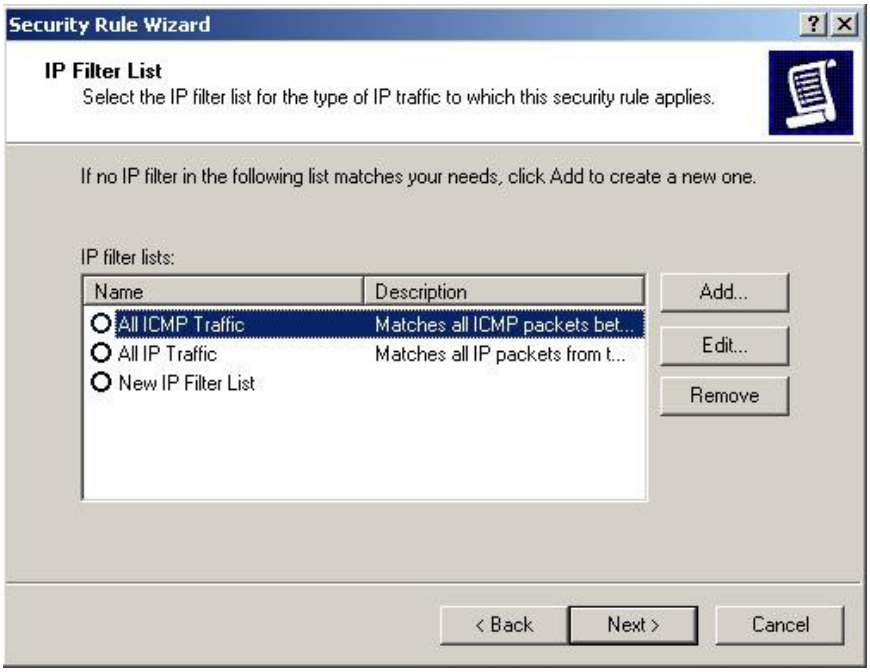
→ chọn add để thêm vào luật 1 chính sách mới

→ next → …→ xuất hiện hộp thoại



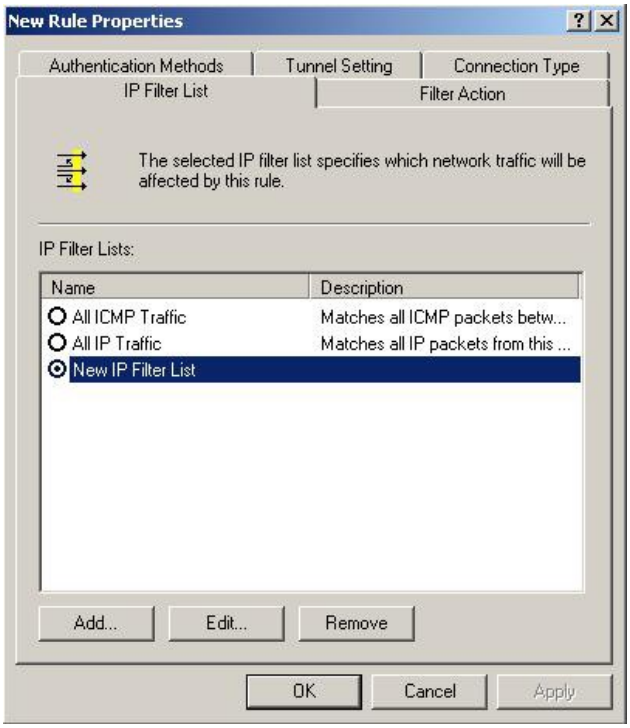
- all net connection: co hiệu lực cho tất cả các mạng
- local area network: co hiệu lực chỉ trong mạng nội bộ
- remote access: chỉ có hiệu lực với các máy sử dụng dịch vụ truy nhập từ xa.

→ next → … → xuất hiện hộp thoại ip filter list hộp thoại này cho phép chọn bộ lọc.

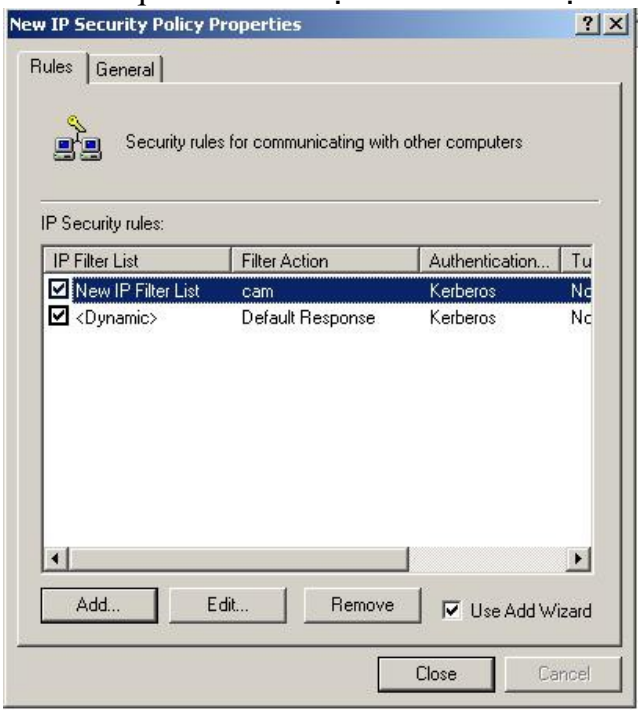


→ next →xuất hiện hộp thoại filter action: hộp thoại này cho phép chúng ta chọn hành động tương ứng của bộ lọc

→ next → finish → xuất hiện hộp thoại new rule properties



→ chọn ok để hoàn tất quá trình cài đặt 1 chính sách lọc cho luật (rule)

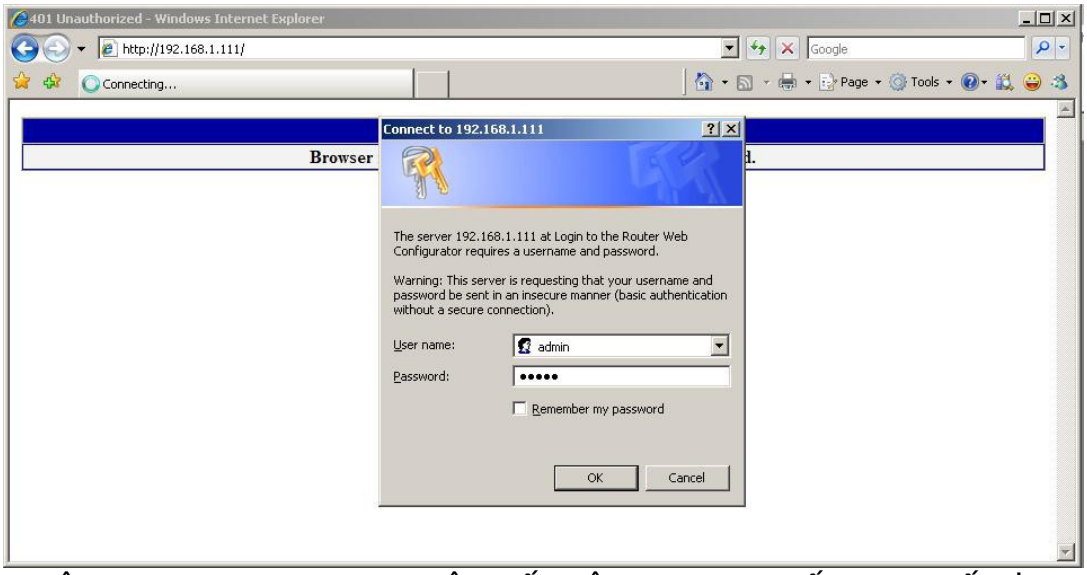


→ tới đây chúng ta có thể chọn close để hoàn tất việc xây dựng 1 luật, hoặc chọn add để thêm 1 chính sách mới vào trong luật.

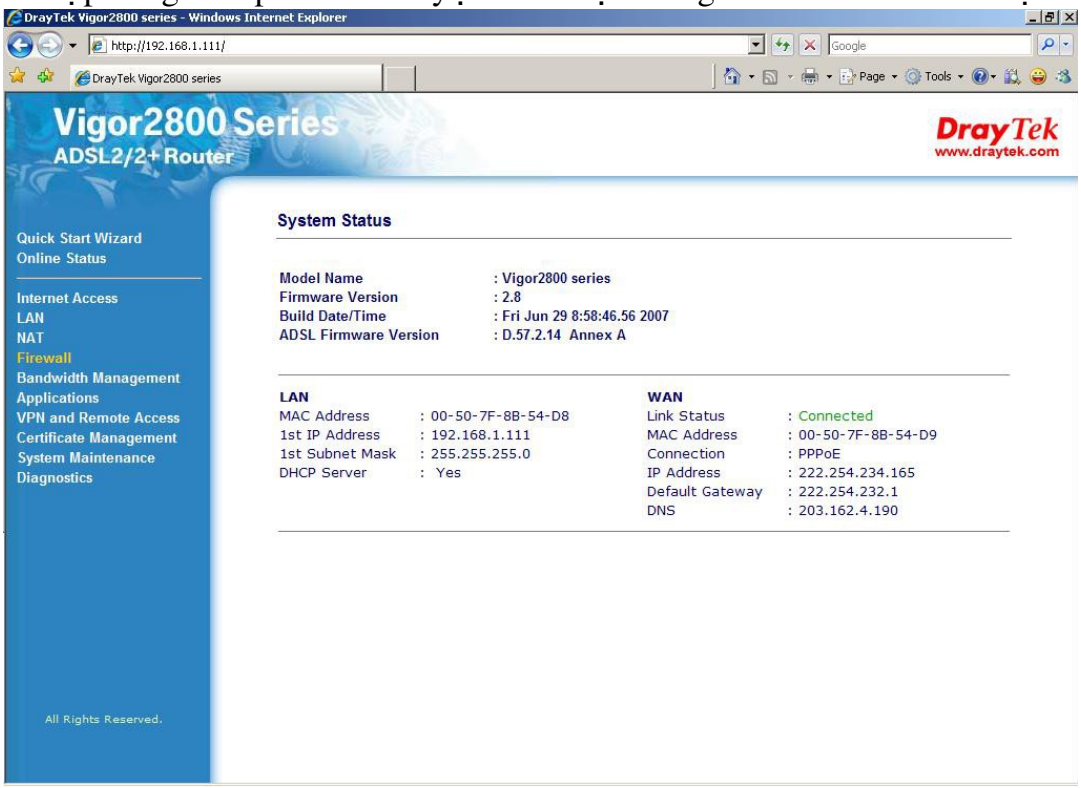
2.3 Lọc Gói IP Dựa Trên Thiết Bị Phần Cứng

Chúng ta sử dụng modem Drayteck 2800

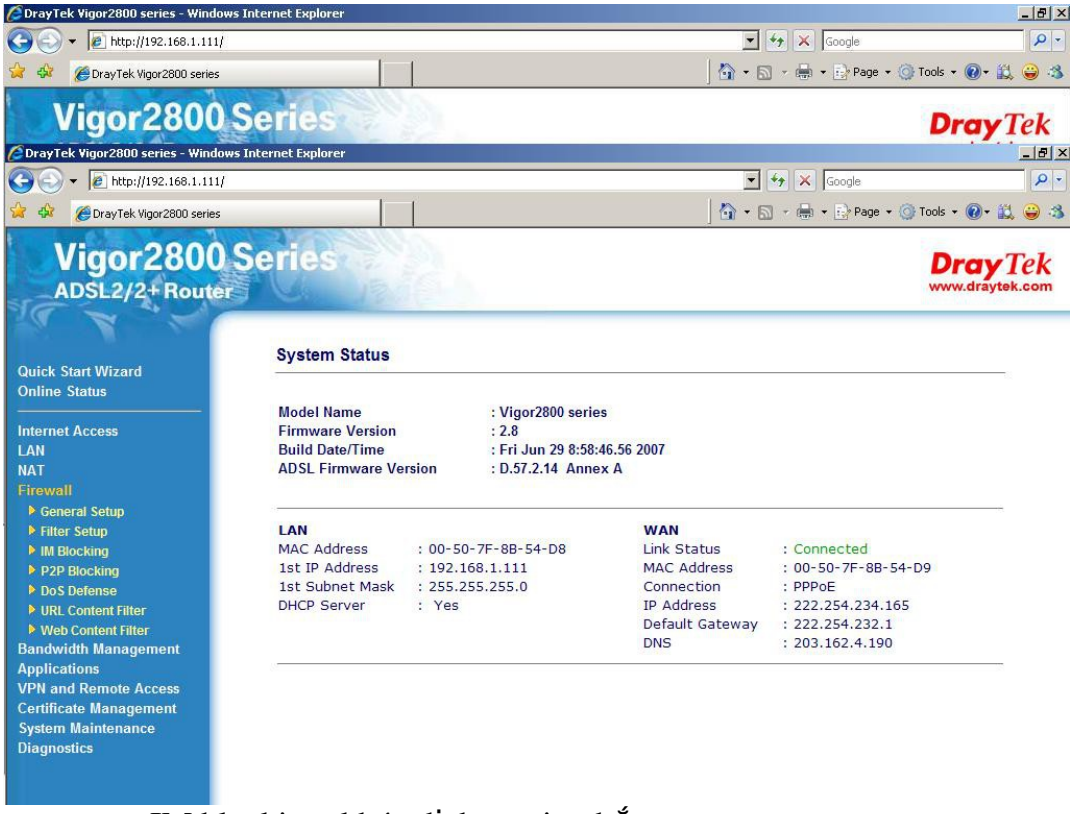
Truy nhập vào modem drayteck: *http:\\[IP của modem]*



Sau khi nhập đúng user/pass trình duyệt xuất hiện màng hình cấu hình thiết bị như sau:



Chọn filterwall → màng hình xuất hiện như sau:



- IM blocking: khóa dịch vụ tin nhắn
- P2P blocking: khóa các dịch vụ chia sẽ file như: emule, …
- Dos defense: ngăn chặn tấn công bằn DDOS
- URL conten filter: ngăn cấm truy nhập một số địa chỉ web nào đó
- Web filter: ngăn cấm truy nhập web site theo thông tin từ các web site bảo mật trên mạng.

Chương 3

IPSEC

(Internet protocol security)

1. Tổng quan

Giao thức IPsec được làm việc tại tầng Network Layer – layer 3 của mô hình OSI. Các giao thức bảo mật trên Internet khác như SSL, TLS và SSH, được thực hiện từ tầng transport layer trở lên (Từ tầng 4 tới tầng 7 mô hình OSI). Điều này tạo ra tính mềm dẻo cho IPsec, giao thức này có thể hoạt động từ tầng 4 với TCP, UDP, hầu hết các giao thức sử dụng tại tầng này. IPsec có một tính năng cao cấp hơn SSL và các phương thức khác hoạt động tại các tầng trên của mô hình OSI. Với một ứng dụng sử dụng IPsec mã (code) không bị thay đổi, nhưng nếu ứng dụng đó bắt buộc sử dụng SSL và các giao thức bảo mật trên các tầng trên trong mô hình OSI thì đoạn mã ứng dụng đó sẽ bị thay đổi lớn.

2. Cấu trúc bảo mật

IPsec được triển khai (1) sử dụng các giao thức cung cấp mật mã (cryptographic protocols) nhằm bảo mật gói tin (packet) trong quá trình truyền, (2) phương thức xác thực và (3) thiết lập các thông số mã hoá.

Xây dựng IPsec sử dụng khái niệm về bảo mật trên nền tảng IP. Một sự kết hợp bảo mật rất đơn giản khi kết hợp các thuật toán và các thông số (ví như các khoá – keys) là nền tảng trong việc mã hoá và xác thực trong một chiều. Tuy nhiên trong các giao tiếp hai chiều, các giao thức bảo mật sẽ làm việc với nhau và đáp ứng quá trình giao tiếp. Thực tế lựa chọn các thuật toán mã hoá và xác thực lại phụ thuộc vào người quản trị IPsec bởi IPsec bao gồm một nhóm các giao thức bảo mật đáp ứng mã hoá và xác thực cho mỗi gói tin IP.

Trong các bước thực hiện phải quyết định cái gì cần bảo vệ và cung cấp cho một gói tin outgoing (đi ra ngoài), IPsec sử dụng các thông số Security Parameter Index (SPI), mỗi quá trình Index (đánh thứ tự và lưu trong dữ liệu – Index ví như một cuốn danh bạ điện thoại) bao gồm Security Association Database (SADB), theo suốt chiều dài của địa chỉ đích trong header của gói tin, cùng với sự nhận dạng duy nhất của một thoả hiệp bảo mật (tạm dịch từ - security association) cho mỗi gói tin. Một quá trình tương tự cũng được làm với gói tin đi vào (incoming packet), nơi IPsec thực hiện quá trình giải mã và kiểm tra các khoá từ SADB.

Cho các gói multicast, một thoả hiệp bảo mật sẽ cung cấp cho một group, và thực hiện cho toàn bộ các receiver trong group đó. Có thể có hơn một thoả hiệp bảo mật cho một group, bằng cách sử dụng các SPI khác nhau, tuy nhiên nó cũng cho phép thực hiện nhiều mức độ bảo mật cho một group. Mỗi người gửi có thể có nhiều thoả hiệp bảo mật, cho phép xác thực, trong khi người nhận chỉ biết được các keys được gửi đi trong dữ liêu. Chú ý các chuẩn không miêu tả làm thế nào để các thoả hiệp và lựa chọn việc nhân bản từ group tới các cá nhân.

3. Hiện trạng

IPsec là một phần bắt bược của IPv6, có thể được lựa chọn khi sử dụng IPv4. Trong khi các chuẩn đã được thiết kết cho các phiên bản IP giống nhau, phổ biến hiện nay là áp dụng và triển khai trên nền tảng IPv4.

Các giao thức IPsec được định nghĩa từ RFCs 1825 – 1829, và được phổ biến năm 1995. Năm 1998, được nâng cấp với các phiên bản RFC 2401 – 2412, nó không tương thích với chuẩn 1825 – 1929. Trong tháng 12 năm 2005, thế hệ thứ 3 của chuẩn IPSec, RFC 4301 – 4309. Cũng không khác nhiều so với chuẩn RFC 2401 – 2412 nhưng thế hệ mới được cung cấp chuẩn IKE second. Trong thế hệ mới này IP security cũng được viết tắt lại là IPsec.

Sự khác nhau trong quy định viết tắt trong thế hệ được quy chuẩn bởi RFC 1825 – 1829 là ESP còn phiên bản mới là ESPbis.

4. Thiết kế theo yêu cầu.

IPsec được cung cấp bởi Transport mode (end-to-end) đáp ứng bảo mật giữa các máy tính giao tiếp trực tiếp với nhau hoặc sử dụng Tunnel mode (portal-to-portal) cho các giao tiếp giữa hai mạng với nhau và chủ yếu được sử dụng khi kết nối VPN.

IPsec có thể được sử dụng trong các giao tiếp VPN, sử dụng rất nhiều trong giao tiếp. Tuy nhiên trong việc triển khai thực hiện sẽ có sự khác nhau giữa hai mode này.

Giao tiếp end-to-end được bảo mật trong mạng Internet được phát triển chậm và phải chờ đợi rất lâu. Một phần bở lý do tính phổ thông của no không cao, hay không thiết thực, Public Key Infrastructure (PKI) được sử dụng trong phương thức này.

IPsec đã được giới thiệu và cung cấp các dịch vụ bảo mật:

1. Mã hoá quá trình truyền thông tin

2. Đảm bảo tính nguyên vẹn của dữ liệu

3. Phải được xác thực giữa các giao tiếp

4. Chống quá trình replay trong các phiên bảo mật.

5. Modes – Các mode

Có hai mode khi thực hiện IPsec đó là: Transport mode và tunnel mode.

Transport mode

Trong Transport mode, chỉ những dữ liệu bạn giao tiếp các gói tin được mã hoá và/hoặc xác thực. Trong quá trình routing, cả IP header đều không bị chỉnh sửa hay mã hoá; tuy nhiên khi authentication header được sử dụng, địa chỉ IP không thể biết được, bởi các thông tin đã bị hash (băm). Transport và application layers thường được bảo mật bởi hàm băm (hash), và chúng không thể chỉnh sửa (ví dụ như port number). Transport mode sử dụng trong tình huống giao tiếp host-to-host.

Điều này có nghĩa là đóng gói các thông tin trong IPsec cho NAT traversal được định nghĩa bởi các thông tin trong tài liệu của RFC bởi NAT-T.

Tunnel mode

Trong tunnel mode, toàn bộ gói IP (bao gồm cả data và header) sẽ được mã hoá và xác thực. Nó phải được đóng gói lại trong một dạng IP packet khác trong quá trình routing của router. Tunnel mode được sử dụng trong giao tiếp network-to-network (hay giữa các routers với nhau), hoặc host-to-network và host-to-host trên internet.

5. Technical details.

Có hai giao thức được phát triển và cung cấp bảo mật cho các gói tin của cả hai phiên bản IPv4 và IPv6:

IP Authentication Header giúp đảm bảo tính toàn vẹn và cung cấp xác thực.

IP Encapsulating Security Payload cung cấp bảo mật, và là option bạn có thể lựa chọn cả tính năng authentication và Integrity đảm bảo tính toàn vẹn dữ liệu.

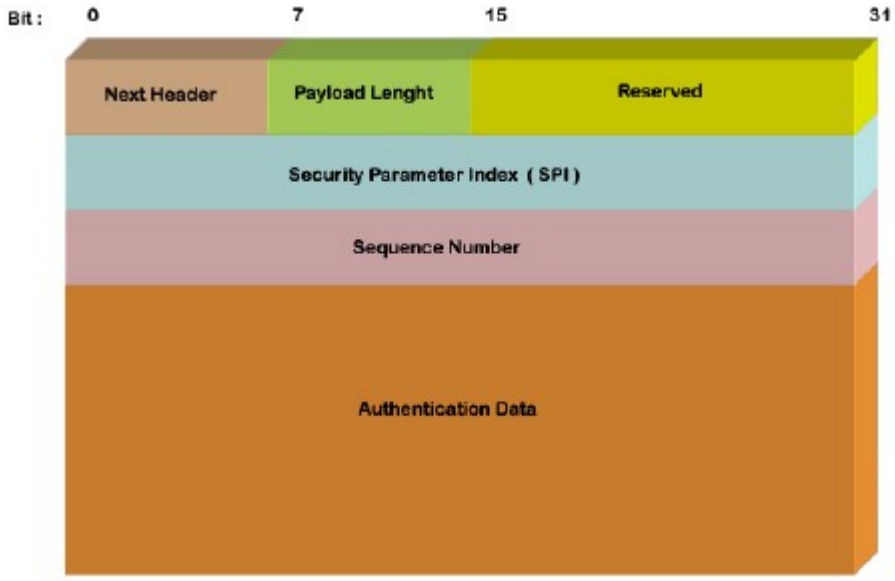
Thuật toán mã hoá được sử dụng trong IPsec bao gồm HMAC-SHA1 cho tính toàn vẹn dữ liệu (integrity protection), và thuật toán TripleDES-CBC và AES-CBC cho mã mã hoá và đảm bảo độ an toàn của gói tin. Toàn bộ thuật toán này được thể hiện trong RFC 4305.

a. Authentication Header (AH)

AH được sử dụng trong các kết nối không có tính đảm bảo dữ liệu. Hơn nữa nó là lựa chọn nhằm chống lại các tấn công replay attack bằng cách sử dụng công nghệ tấn

công sliding windows và discarding older packets. AH bảo vệ quá trình truyền dữ liệu khi sử dụng IP. Trong IPv4, IP header có bao gồm TOS, Flags, Fragment Offset, TTL, và Header Checksum. AH thực hiện trực tiếp trong phần đầu tiên của gói tin IP. dưới đây là mô hình của AH header.

Các modes thực hiện



Ý nghĩa của từng phần:

Next header: Nhận dạng giao thức trong sử dụng truyền thông tin.

Payload length: Độ lớn của gói tin AH.

RESERVED: Sử dụng trong tương lai (cho tới thời điểm này nó được biểu diễn bằng các số 0).

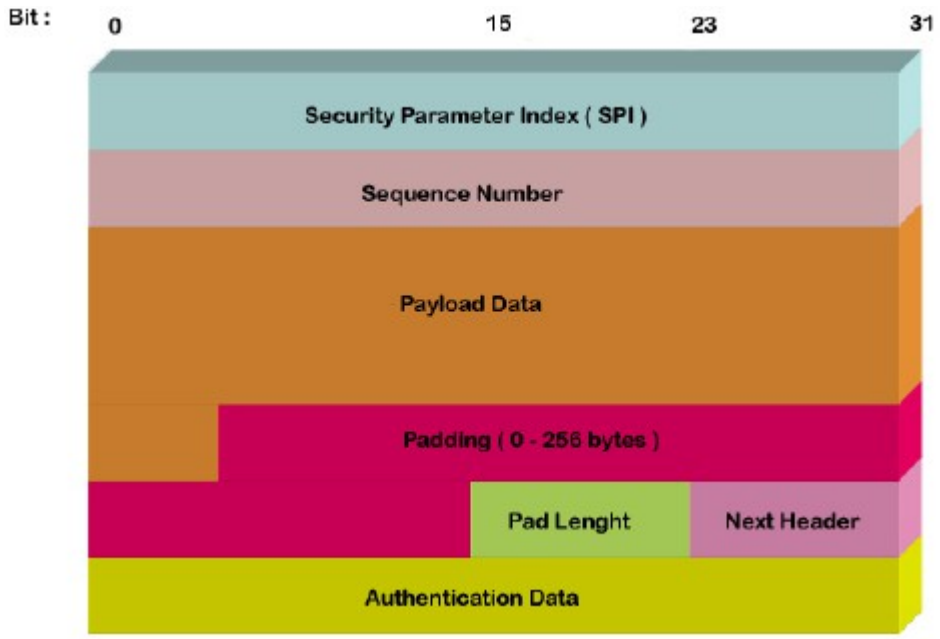
Security parameters index (SPI): Nhận ra các thông số bảo mật, được tích hợp với địa chỉ IP, và nhận dạng các thương lượng bảo mật được kết hợp với gói tin.

Sequence number: Một số tự động tăng lên mỗi gói tin, sử dụng nhằm chống lại tấn công dạng replay attacks.

Authentication data: Bao gồm thông số Integrity check value (ICV) cần thiết trong gói tin xác thực.

b. Encapsulating Security Payload (ESP)

Giao thức ESP cung cấp xác thực, độ toàn vẹn, đảm bảo tính bảo mật cho gói tin. ESP cũng hỗ trợ tính năng cấu hình sử dụng trong tính huống chỉ cần bảo mã hoá và chỉ cần cho authentication, nhưng sử dụng mã hoá mà không yêu cầu xác thực không đảm bảo tính bảo mật. Không như AH, header của gói tin IP, bao gồm các option khác. ESP thực hiện trên top IP sử dụng giao thức IP và mang số hiệu 50 và AH mang số hiệu 51.



Ý nghĩa của các phần:

Security parameters index (SPI): Nhận ra các thông số được tích hợp với địa chỉ IP.

Sequence number:Tự động tăng có tác dụng chống tấn công kiểu replay attacks.

Payload data: Cho dữ liệu truyền đi

Padding: Sử dụng vài block mã hoá

Pad length: Độ lớn của padding.

Next header: Nhận ra giao thức được sử dụng trong quá trình truyền thông tin.

Authentication data: Bao gồm dữ liệu để xác thực cho gói tin.

6. Implementations - thực hiện

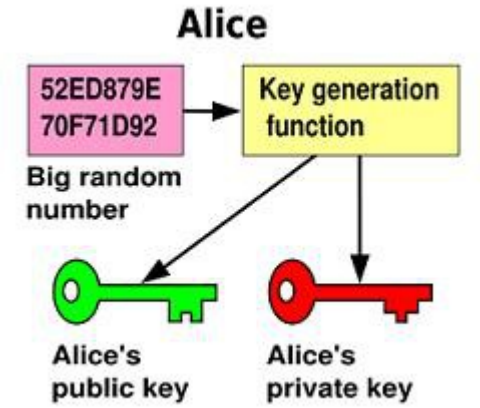
IPsec được thực hiện trong nhân với các trình quản lý các key và quá trình thương lượng bảo mật ISAKMP/IKE từ người dùng. Tuy nhiên một chuẩn giao diện cho quản lý key, nó có thể được điều khiển bởi nhân của IPsec.

Bởi vì được cung cấp cho người dùng cuối, IPsec có thể được triển khai trên nhân của Linux. Dự án FreeS/WAN là dự án đầu tiên hoàn thành việc thực hiện IPsec trong mã nguồn mở cụ thể là Linux. Nó bao gồm một nhấn IPsec stack (KLIPS), kết hợp với trình quản lý key là deamon và rất nhiều shell scripts. Dự án FreeS/WAN được bắt đầu vào tháng 3 năm 2004. Openswan và strongSwan đã tiếp tục dự án FreeS/WAN.

Dự án KAME cũng hoàn thành việc triển khai sử dụng IPsec cho NetBSB, FreeBSB. Trình quản lý các khoá được gọi là racoon. OpenBSB được tạo ra ISAKMP/IKE, với tên đơn giản là isakmpd (nó cũng được triển khai trên nhiều hệ thống, bao gồm cả hệ thống Linux).

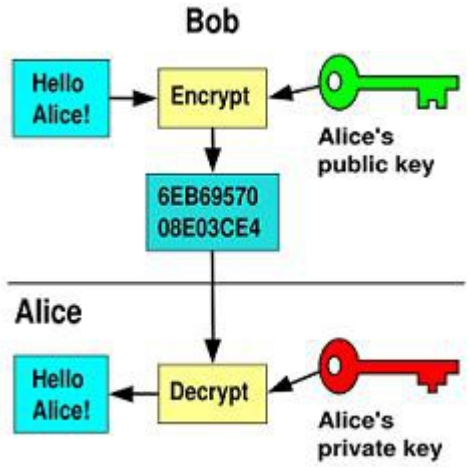
Trong bài viết này tôi sẽ giới thiệu với các bạn tổng quan về cách thức làm việc của Public Key Infrastructure (PKI).

Nếu bạn sử dụng Active Directory của công nghệ Windows NT thì mỗi user khi được tạo ra cũng đi liền với nó có một cặp Key: Public key và Private key. Ngoài ra còn có nhiều ứng dụng để tạo ra cặp khoá này.

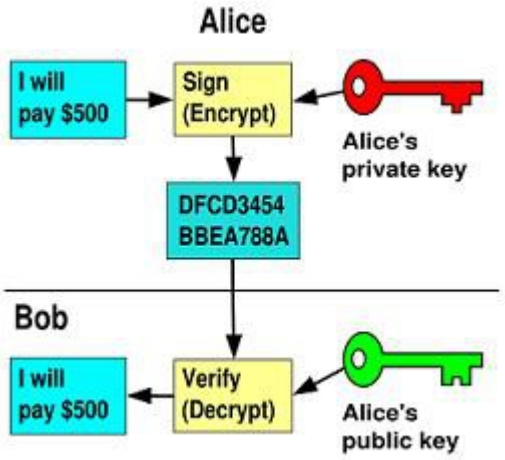


Cặp key được tạo ra ngẫu nhiên với nhiều chữ số hiển thị. Khi các keys được tạo ra từ nhiều chữ số ngẫu nhiên, sẽ không thể giải mã nếu ra private key nếu biết public key. Nhưng có một số thuật toán có thể tạo ra public key từ private key. Nhưng chỉ có Public key mới được published cho toàn bộ mọi người.

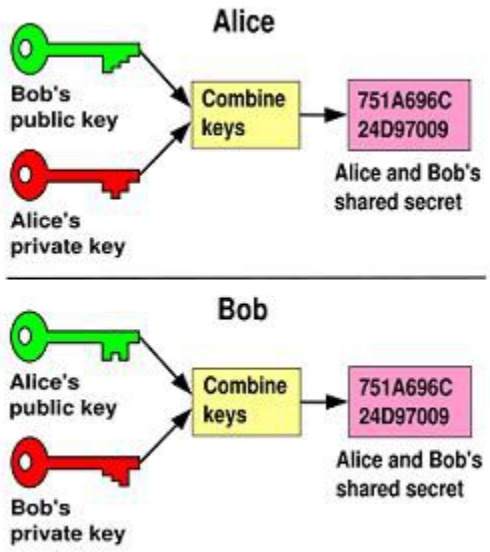
Hầu hết các cặp key được tạo ra từ nhiều số và bằng một thuật toán mã hoá nào đó.



Một thông tin được mã hoá với public key thì chỉ có thể giải mã bởi private key. Nếu chỉ có public key bạn sẽ không thể giải mã được gói tin. Điều này có nghĩa khi một người gửi thông tin được mã hoá tới một người khác thì chỉ có người nhận mới mở được thông tin đó mà thôi. Những người khác có bắt được toàn bộ thông tin thì cũng không thể giải mã được nếu chỉ có Public key.



Một thông tin được mã hoá với private key có thể giải mã với public key. Khi public key đã được public cho toàn bộ mọi người thì ai cũng có thể đọc được thông tin nếu có public key.



Để đảm bảo an toàn hơn trong quá trình truyền thông tin: Alice kết hợp Private key của mình với Public key của Bob để tạo ra và chia sẻ bảo mật (share secret). Cũng tương tự như vậy Bob cũng kết hợp Private key của mình với Public key của Alice để tạo ra một shared secret. Rồi hai người truyền thông tin cho nhau.

Khi Alice truyền thông tin cho Bob bằng Shared Secret được tạo ra, khi Bob nhận được gói tin mã hoá bởi shared secret đó dùng Public key của Alice kết hợp với Private key của mình để mở thông tin. Điều này cũng tương tự khi Bob truyền thông tin và cách Alice giải mã để lấy thông tin.

CHƯƠNG 4

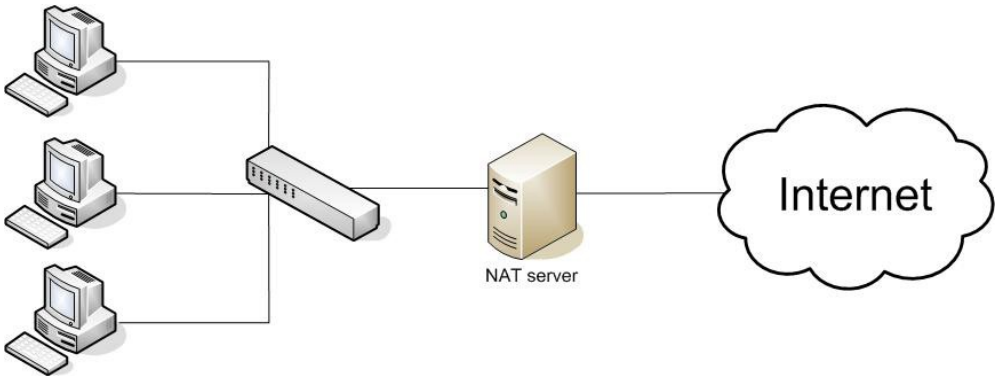
NAT

(Network Address Translation)

1. Nat Là Gì ?

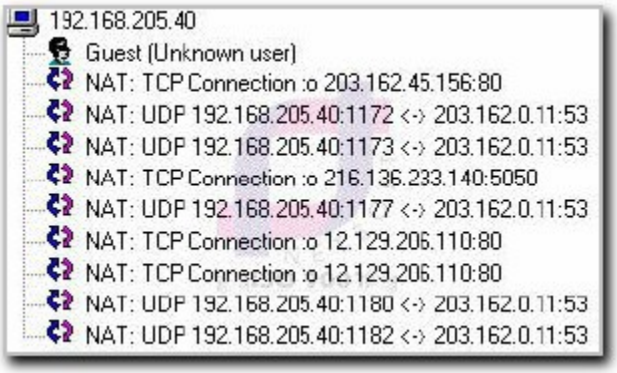
NAT hay còn gọi là Network Address Translation là một kỉ thuật được phát minh lúc khởi đầu dùng để giải quyết vấn đề IP shortage. Khi có hai máy tính ở trên cùng một lớp mạng (cùng subnet), các máy tính này kết nối trực tiếp với nhau, điều này có nghĩa là chúng có thể gởi và nhận dữ liệu trực tiếp với nhau. Nếu những máy tính này không trên cùng một lớp mạng và không có kết nối trực tiếp thì dữ liệu sẽ được chuyển tiếp qua lại giữa những lớp mạng này và như thế phải cần một router (có thể là phần mềm hoặc phần cứng) Đây là trường hợp khi một máy tính nào đó muốn kết nối tới một máy khác trên internet.

2. Mô Hình Mạng Của Dịch Vụ Nat



3. Nguyên Lỳ Hoạt Động Của NAT

NAT làm việc như một router, công việc của nó là chuyển tiếp các gói tin (packets) giữa những lớp mạng khác nhau trên một mạng lớn. Bạn cũng có thể nghĩ rằng Internet là một mạng đơn nhưng có vô số subnet. Routers có đủ khả năng để hiểu được các lớp mạng khác nhau xung quanh nó và có thể chuyển tiếp những gói tin đến đúng nơi cần đến.



NAT sử dụng IP của chính nó làm IP công cộng cho mỗi máy con (client) với IP riêng. Khi một máy con thực hiện kết nối hoặc gởi dữ liệu tới một máy tính nào đó trên internet, dữ liệu sẽ được gởi tới NAT, sau đó NAT sẽ thay thế địa chỉ IP gốc của máy con đó rồi gửi gói dữ liệu đi với địa chỉ IP của NAT. Máy tính từ xa hoặc máy tính nào đó trên internet khi nhận được tín hiệu sẽ gởi gói tin trở về cho NAT computer bởi vì chúng nghĩ rằng NAT computer là máy đã gởi những gói dữ liệu đi. NAT ghi lại bảng thông tin của những máy tính đã gởi những gói tin đi ra ngoài trên mỗi cổng dịch vụ và gởi những gói tin nhận được về đúng máy tính đó (client).

NAT thực hiện những công việc sau:

- Chuyển đổi địa chỉ IP nguồn thành địa chỉ IP của chính nó, có nghĩa là dữ liệu nhận được bởi máy tính từ xa (remote computer) giống như nhận được từ máy tính có cấu hình NAT.
- Gởi dữ liệu tới máy tính từ xa và nhớ được gói dữ liệu đó đã sử dụng cổng dịch vụ nào.
- Dữ liệu khi nhận được từ máy tính từ xa sẽ được chuyển tới cho các máy con.

NAT có hoạt động với bất kỳ giao thức và ứng dụng nào không?

Giao thức sử dụng đa kết nối hoặc đa phương tiện và nhiều kiểu dữ liệu (như là FTP hoặc RealAudio). Với FTP, khi bạn bắt đầu công việc truyền file, bạn thực hiện một kết nối tới FTP server bởi FTP client, máy client kết nối vào và yêu cầu được truyền file hoặc thư mục, với một vài FTP client bạn sẽ thấy một hiện tượng gì đó như lệnh port, những gì mà dòng lệnh này đang thực hiện là thiết lập kết nối dữ liệu để gởi tập tin hoặc thư mục về lại cho FTP client. Cách thực hiện công việc như vậy có nghĩa là máy client "nói" với server rằng "hãy kết nối với tôi trên địa chỉ IP này và trên cổng port này để truyền dữ liệu".

Vấn đề ở đây là máy client chỉ cho server biết để kết nối ngược lại trên địa chỉ IP nội bộ bên trong mạng LAN của chính nó và như vậy server sẽ không tìm được địa chỉ IP này và thất bại nếu server cố gắng tìm kiếm và kết nối với địa chỉ này, đây là lúc phải cần tới NAT

Hầu hết các giải pháp NAT (trong đó bao gồm cả WinGate) đều có sự hỗ trợ đặc biệt đối với giao thức FTP và yêu cầu đối với máy tính được cấu hình NAT là máy tính đó phải có địa chỉ IP tĩnh (static IP).

4. Triển Khai Dịch Vụ Nat

4.1 Yêu Cầu:

- Máy phải có từ hai giao tiếp network trở lên

  Có hai card mạng

  Có 1 card mạng và 1 giao tiếp thông qua modem dialup

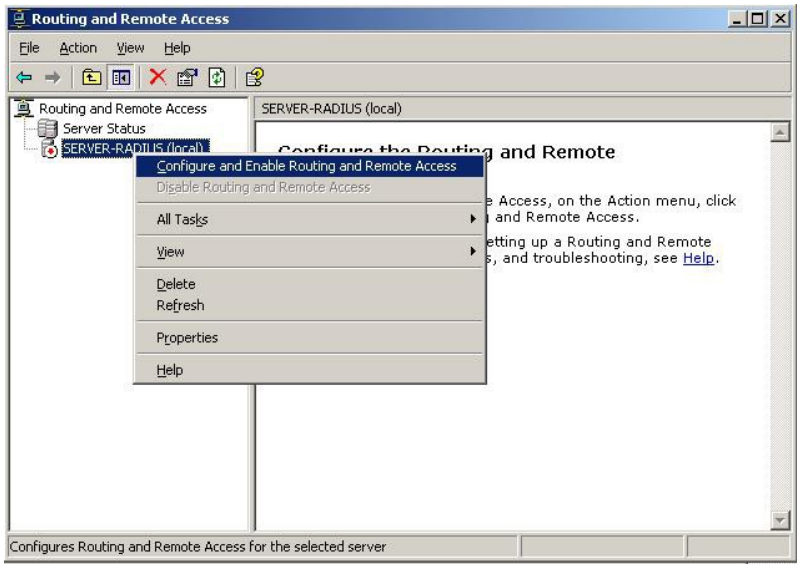
- Máy phải cài đặt HĐH window server

4.2 Triển khai dịch vụ Nat:

Bước 1: khởi động dịch vụ Nat:

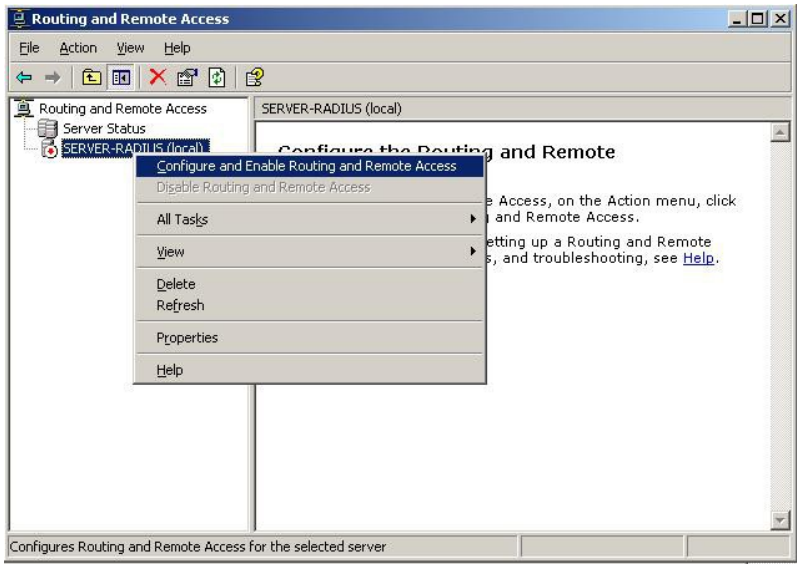
- Khởi động chương trình Routing and Remote Access:

→ menu start → all program → administrative tools → routing and remote access

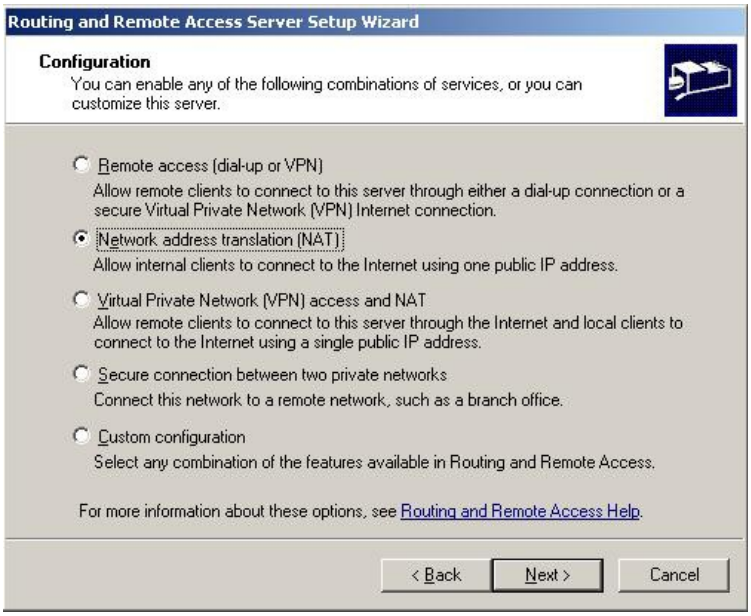


- Khởi động dịch vụ Nat

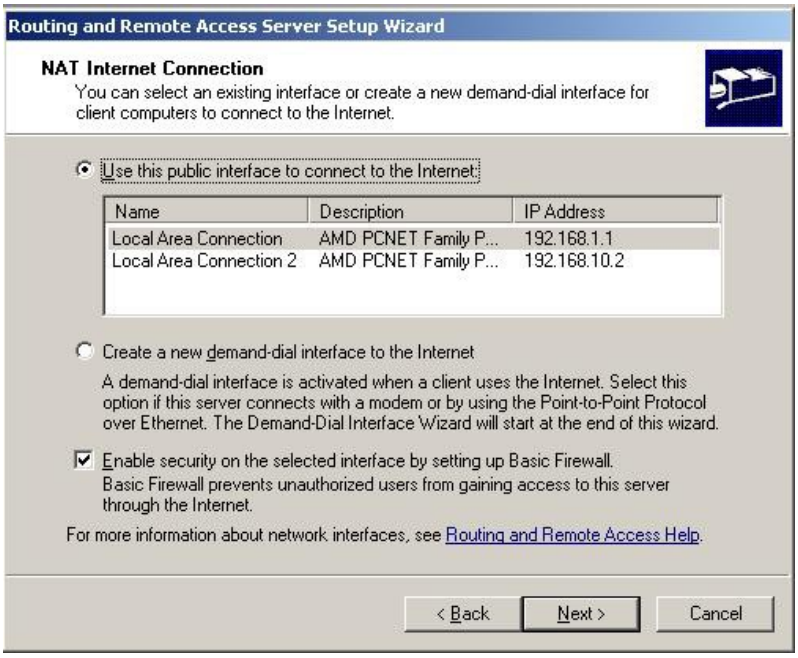
→ right click server-radius (tên của máy Nat server) →configue and enable routing and remote access



→ next → nextwork address translation



→ next → khởi động hộp thoại Nat internet conection: hộp thoại này cho phép chúng ta chọn lựa giao tiếp nào kết nối với hệ thống mạng internet



Có 2 mục chọn lựa:

- use this public interface to connect to internet:

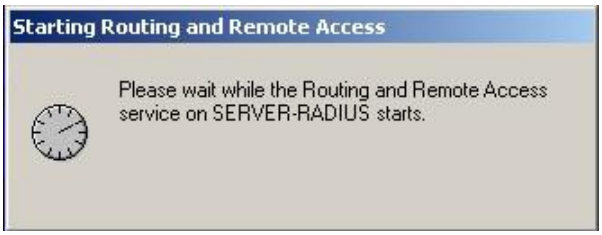
Chúng ta chọn lựa mục này khi máy có từ 2 card mạng trở lên.

Tại list box chúng ta chọn lựa card mạng dùng để kết nối internet

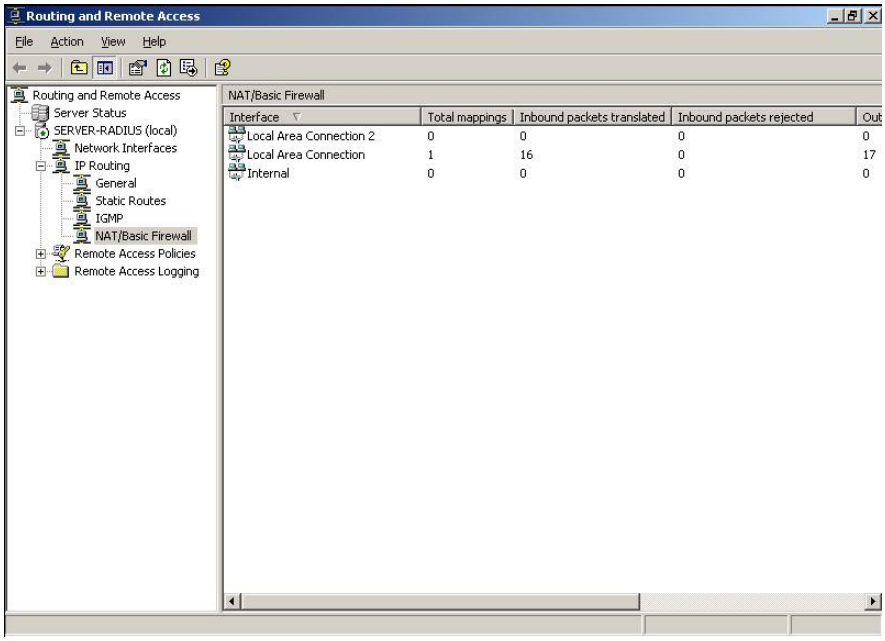
- Create a new demand-dial interface to the internet

Mục này chỉ được chọn lựa khi giao tiếp với internet là 1 modem dialup

→ next → finish để khởi động dịch vụ Nat



→ sau khi khởi động dịch vụ nat ta co giao diện chương trình như sau:

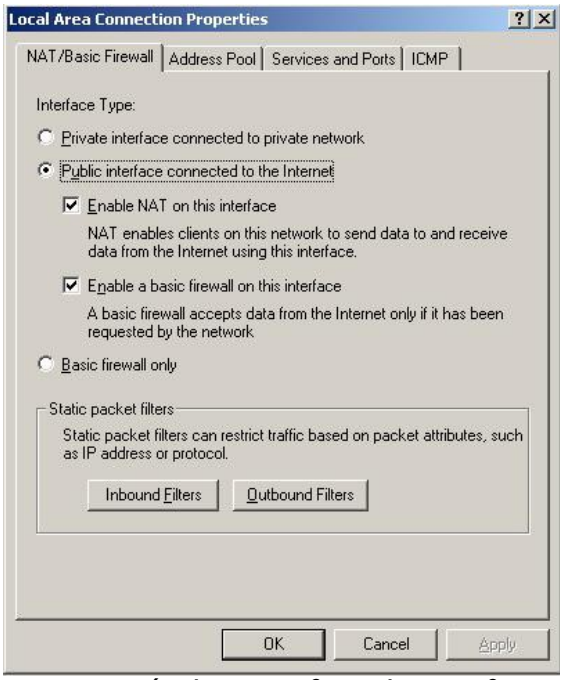


Bước 2: Cấu hình dịch vụ Nat:

- Cấu hình giao tiếp internet:

→ right click lên giao tiếp internet → properties → để mở hộp thoại cấu hình của kết nối internet

Tab Nat/Basic firewall:



Hộp thoại này cho phép thiết lập các bảo mật cơ bản trên giao tiếp internet

- Public interface connect to the internet:

Mục này được chọn lựa khi giao tiếp này là giao tiếp kết nối với hệ thống mạng bên ngoài.

- Enable NAT on this interface: mục này cho phép bật hay tắt chức năng NAT, khi tắt chức năng này khi các máy trạm trong hệ thông mạng LAN không thể kết nối internet được

- Enable basic firewall on this interface: mục này cho phép bật tắt chế độ bảo vệ cơ bản của NAT server trên giao tiếp hiện tại.

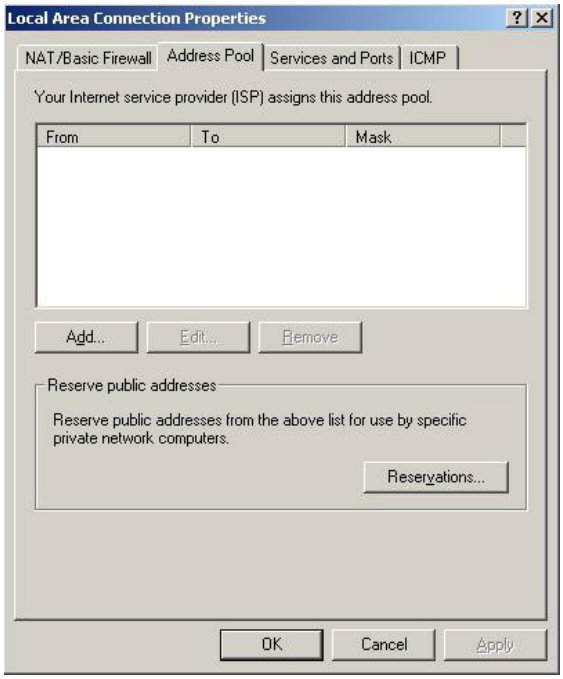
- Static Packet Filter:

Mục này cho phép thiết lập chính sách lọc các gói tin đi qua nat server

- Inbound filter: cho phép thiết lập bộ lọc gói tin đi vào interface này
- Outbound filter: cho phép thiết lập bộ lọc gói tin đi ra interface này

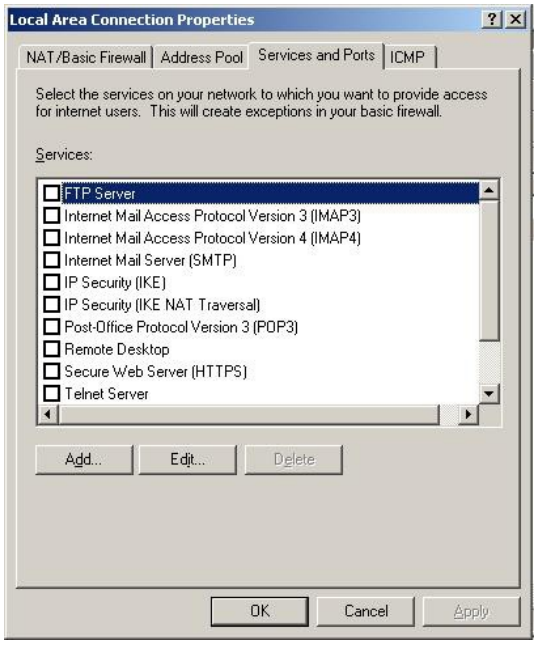
Tab Address pool:

Cho phép quy định những máy có địa chỉ IP nào được phép truy nhập internet



Tab service and ports:

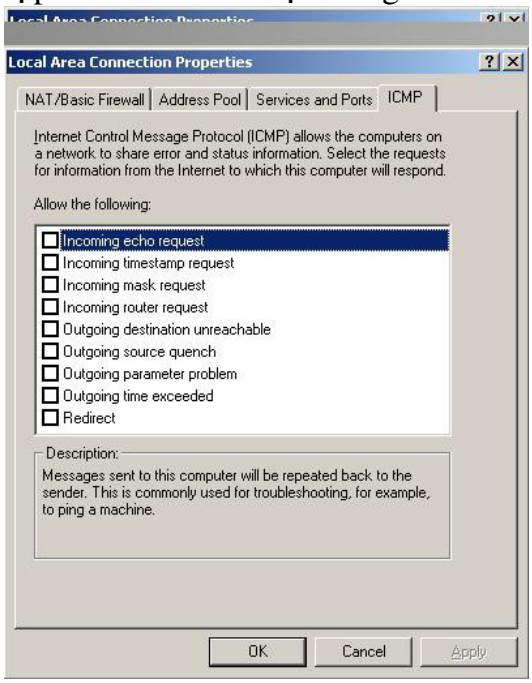
Cho phép quy định loại dịch vụ nào mà cho phép bên ngoài internet truy nhập vào nó.



- Add: cho phép thêm vào loại dịch vụ
- Edit: cho phép hiệu chỉnh thông tin của tưng loại dịch vụ

Tab ICMP:

Cho phép thiết lập các chính sách lọc với giao thức hổ trợ định tuyến ICMP.



CHƯƠNG 5

VIRUS

VÀ CÁCH PHÒNG CHỐNG

1 Virus

Virus tin học hiện nay đang là nỗi băn khoăn lo lắng của những người làm công tác tin học, là nỗi lo sợ của những người sử dụng khi máy tính của mình bị nhiễm virus. Khi máy tính của mình bị nhiễm virus, họ chỉ biết trông chờ vào các phần mềm diệt virus hiện có trên thị trường, trong trường hợp các phần mềm này không phát hiện hoặc không tiêu diệt được, họ bị lâm phải tình huống rất khó khăn, không biết phải làm như thế nào.
Vì lý do đó, có một cách nhìn nhận cơ bản về cơ chế và các nguyên tắc hoạt động của virus tin học là cần thiết. Trên cơ sở đó, có một cách nhìn đúng đắn về virus tin học trong việc phòng chống, kiểm tra, chữa trị cũng như cách phân tích, nghiên cứu một virus mới xuất hiện.

1.1 Virus là gì ?

Thuật ngữ virus tin học dùng để chỉ một chương trình máy tính có thể tự sao chép chính nó lên nơi khác (đĩa hoặc file) mà người sử dụng không hay biết. Ngoài ra, một đặc điểm chung thường thấy trên các virus tin học là tính phá hoại, nó gây ra lỗi thi hành, thay đổi vị trí, mã hoá hoặc huỷ thông tin trên đĩa.

1.2 Phân Loại:

Thông thường, dựa vào đối tượng lây lan là file hay đĩa mà virus được chia thành hai nhóm chính:

- B-virus: Virus chỉ tấn công lên Master Boot hay Boot Sector.

- F-virus: Virus chỉ tấn công lên các file khả thi.

Mặc dù vậy, cách phân chia này cũng không hẳn là chính xác. Ngoại lệ vẫn có các virus vừa tấn công lên Master Boot (Boot Sector) vừa tấn công lên file khả thi.

Để có một cách nhìn tổng quan về virus, chúng ta xem chúng dành quyền điều khiển như thế nào.

a. B-virus.

Khi máy tính bắt đầu khởi động (Power on), các thanh ghi phân đoạn đều được đặt về 0FFFFh, còn mọi thanh ghi khác đều được đặt về 0. Như vậy, quyền điều khiển ban đầu được trao cho đoạn mã tại 0FFFFh: 0h, đoạn mã này thực ra chỉ là lệnh nhảy JMP FAR đến một đoạn chương trình trong ROM, đoạn chương trình này thực hiện quá trình POST (Power On Self Test - Tự kiểm tra khi khởi động).

Quá trình POST sẽ lần lượt kiểm tra các thanh ghi, kiểm tra bộ nhớ, khởi tạo các Chip điều khiển DMA, bộ điều khiển ngắt, bộ điều khiển đĩa... Sau đó nó sẽ dò tìm các Card thiết bị gắn thêm để trao quyền điều khiển cho chúng tự khởi tạo rồi lấy lại quyền điều khiển. Chú ý rông đây là đoạn chương trình trong ROM (Read Only Memory) nên không thể sửa đổi, cũng như không thể chèn thêm một đoạn mã nào khác.

Sau quá trình POST, đoạn chương trình trong ROM tiến hành đọc Boot Sector trên đĩa A hoặc Master Boot trên đĩa cứng vào RAM (Random Acess Memory) tại địa chỉ 0:7C00h và trao quyền điều khiển cho đoạn mã đó bông lệnh JMP FAR 0:7C00h. Đây là chỗ mà B-virus lợi dụng để tấn công vào Boot Sector (Master Boot), nghĩa là nó sẽ thay Boot Sector (Master Boot) chuẩn bông đoạn mã virus, vì thế quyền điều khiển được trao cho virus, nó sẽ tiến hành các hoạt động của mình trước, rồi sau đó mới tiến hành các thao tác như thông thường: Đọc Boot Sector (Master Boot) chuẩn mà nó cất giấu ở đâu đó vào 0:7C00h rồi trao quyền điều khiển cho đoạn mã chuẩn này, và người sử dụng có cảm giác rông máy tính của mình vẫn hoạt động bình thường.

b. F-virus.

Khi DOS tổ chức thi hành File khả thi (bông chức năng 4Bh của ngắt 21h), nó sẽ tổ chức lại vùng nhớ, tải File cần thi hành và trao quyền điều khiển cho File đó. F-virus lợi dụng điểm này bông cách gắn đoạn mã của mình vào file đúng tại vị trí mà DOS trao quyền điều khiển cho File sau khi đã tải vào vùng nhớ. Sau khi F-virus tiến hành xong các hoạt động của mình, nó mới sắp xếp, bố trí trả lại quyền điều khiển cho File để cho File lại tiến hành hoạt động bình thường, và người sử dụng thì không thể biết được.

Trong các loại B-virus và F-virus, có một số loại sau khi dành được quyền điều khiển, sẽ tiến hành cài đặt một đoạn mã của mình trong vùng nhớ RAM như một chương trình thường trú (TSR), hoặc trong vùng nhớ nôm ngoài tầm kiểm soát của DOS, nhôm mục đích kiểm soát các ngắt quan trọng như ngắt 21h, ngắt 13h,... Mỗi khi các ngắt này được gọi, virus sẽ dành quyền điều khiển để tiến hành các hoạt động của mình trước khi trả lại các ngắt chuẩn của DOS.

1.3 Đặc Điểm Của B-Virus:

Qua phần trước, chúng ta đã đưa ra các thông tin hết sức cơ bản về cấu trúc đĩa, tiến trình khởi động và cách thức tổ chức vùng nhớ, tổ chức thi hành file của DOS. Những

thông tin đó giúp chúng ta tìm hiểu những đặc điểm cơ bản của virus, từ đó đưa ra cách phòng chống, chữa trị trong trường hợp máy bị nhiễm virus.

a. Phân loại B-virus.

Như chúng ta đã biết, sau quá trình POST, sector đầu tiên trên đĩa A hoặc đĩa C được đọc vào vùng nhớ tại 0: 7C00, và quyền điều khiển được trao cho đoạn mã trong sector khởi động này. B-virus hoạt động bông cách thay thế đoạn mã chuẩn trong sector khởi động này bông đoạn mã của nó để chiếm quyền điều khiển, sau khi đã cài đặt xong mới đọc sector khởi động chuẩn được virus cất giữ ở đâu đó vào 0:7C00 và trả lại quyền điều khiển cho đoạn mã chuẩn này. Việc cất giữ sector khởi động tại vị trí nào trên đĩa tuỳ thuộc loại đĩa và cách giải quyết của từng loại virus. Đối với đĩa cứng, thông thường nó được cất giữ ở đâu đó trong Side 0, Cylinder 0 vì trong cả track này, DOS chỉ sử dụng sector đầu tiên cho bảng Partition. Trên đĩa mềm, vị trí cất giữ sẽ phức tạp hơn vì mọi chỗ đều có khả năng bị ghi đè thông tin. Một số hướng sau đây đã được các virus áp dụng:

Sử dụng sector ở cuối Root Directory, vì nó thường ít được sử dụng.

Sử dụng các sector cuối cùng trên đĩa, vì khi phân bổ vùng trống cho file, DOS tìm vùng trống từ nhỏ đến lớn cho nên vùng này thường ít được sử dụng.

Ghi vào vùng trống trên đĩa, đánh dấu trong bảng FAT vùng này là vùng bị hỏng để DOS không sử dụng cấp phát nữa. Ccáh làm này an toàn hơn các cách làm trên đây.

Format thêm track và ghi vào track vừa được Format thêm.

Tùy thuộc vào độ lớn của đoạn mã virus mà B-virus được chia thành hai loại:

- *SB-virus.*

Chương trình của SB-virus chỉ chiếm đúng một sector khởi động, các tác vụ của SB-virus không nhiều và tương đối đơn giản. Hiện nay số các virus loại này thường ít gặp và có lẽ chỉ là các virus do trong nước "sản xuất".

- DB-virus.

Đây là những loại virus mà đoạn mã của nó lớn hơn 512 byte (thường thấy).

Vì thế mà chương trình virus được chia thành hai phần:

- Phần đầu virus: Được cài đặt trong sector khởi động để chiếm quyền điều hiển khi quyền điều khiển được trao cho sector khởi động này. Nhiệm vụ duy nhất của phần

đầu là: tải tiếp phần thân của virus vào vùng nhớ và trao quyền điều khiển cho phần thân đó. Vì nhiệm vụ đơn giản như vậy nên phần đầu của virus thường rất ngắn, và càng ngắn càng tốt vì càng ngắn thì sự khác biệt giữa sector khởi động chuẩn và sector khởi động đã bị nhiễm virus càng ít, giảm khả năng bị nghi ngờ.

- Phần thân virus: Là phần chương trình chính của virus. Sau khi được phần đầu tải vào vùng nhớ và trao quyền, phần thân này sẽ tiến hành các tác vụ của mình, sau khi tiến hành xong mới đọc sector khởi động chuẩn vào vùng nhớ và trao quyền cho nó để máy tính làm việc một cách bình thường như chưa có gì xảy ra cả.

b. Một số kỹ thuật cơ bản của B-virus.

Dù là SB-virus hay DB-virus, nhưng để tồn tại và lây lan, chúng đều có một số các kỹ thuật cơ bản như sau:

- Kỹ thuật kiểm tra tính duy nhất.

Virus phải tồn tại trong bộ nhớ cũng như trên đĩa, song sự tồn tại quá nhiều bản sao của chính nó trên đĩa và trong bộ nhớ sẽ chỉ làm chậm quá trình Boot máy, cũng như chiếm quá nhiều vùng nhớ ảnh hưởng tới việc tải và thi hành các chương trình khác đồng thời cũng làm giảm tốc độ truy xuất đĩa. Chính vì thế, kỹ thuật này là một yêu cầu nghiêm ngặt với B-virus.

Việc kiểm tra trên đĩa có hai yếu tố ảnh hưởng:

Thứ nhất là thời gian kiểm tra:

Nếu mọi tác vụ đọc/ghi đĩa đều phải kiểm tra đĩa thì thời gian truy xuất sẽ bị tăng gấp đôi, làm giảm tốc độ truy xuất cũng như gia tăng mỗi nghi ngờ.

Đối với yêu cầu này, các virus áp dụng một số kỹ thuật sau: Giảm số lần kiểm tra bông cách chỉ kiểm tra trong trường hợp thay đổi truy xuất từ ổ đĩa này sang ổ đĩa khác, chỉ kiểm tra trong trường hợp bảng FAT trên đĩa được đọc vào.

Thứ hai là kỹ thuật kiểm tra:

Hầu hết các virus đều kiểm tra bông giá trị từ khoá. Mỗi virus sẽ tạo cho mình một giá trị đặc biệt tại một vị trí xác định trên đĩa, việc kiểm tra được tiến hành bông cách đọc Boot record và kiểm tra giá trị của từ khoá này. Kỹ thuật này gặp trở ngại vì số lượng B-virus ngày một đông đảo, mà vị trí trên Boot Record thì có hạn. Cách khắc phục hiện nay của các virus là tăng số lượng mã lệnh cần so sánh để làm giảm khả năng trùng hợp ngẫu nhiên.

Để kiểm tra sự tồn tại của mình trong bộ nhớ, các virus đã áp dụng các kỹ thuật sau: Đơn giản nhất là kiểm tra giá trị Key value tại một vị trí xác định trên vùng nhớ cao, ngoài ra một kỹ thuật khác được áp dụng đối với các virus chiếm ngắt Int 21 của DOS là yêu cầu thực hiện một chức năng đặc biệt không có trong ngắt này. Nếu cờ báo lỗi được bật lên thì trong bộ nhớ chưa có virus, ngược lại nếu virus đã lưu trú trong vùng nhớ thì giá trị trả lại (trong thanh ghi AX chẳng hạn) là một giá trị xác định nào đó.

- Kỹ thuật lưu trú.

Sau khi thực hiện xong chương trình POST, giá trị tổng số vùng nhớ vừa được Test sẽ được lưu vào vùng BIOS Data ở địa chỉ 03h. Khi hệ điều hành nhận quyền điều khiển, nó sẽ coi vùng nhớ mà nó kiểm soát là giá trị trong địa chỉ này. Vì vậy để lưu trú, mọi B-virus đều áp dụng kỹ thuật sau đây: Sau khi tải phần lưu trú của mình lên vùng nhớ cao, nó sẽ giảm giá trị vùng nhớ do DOS quản lý tại 03h đi một lượng đúng bông kích thước của virus. Tuy nhiên nếu không kiểm tra tốt sự có mặt trong vùng nhớ, khi bị Boot mềm liên tục, giá trị tổng số vùng nhớ này sẽ bị giảm nhiều lần, ảnh hưởng tới việc thực hiện của các chương trình sau này. Chính vì thế, các virus được thiết kế tốt phải kiểm tra sự tồn tại của mình trong bộ nhớ, nếu đã có mặt trong bộ nhớ thì không giảm dung lượng vùng nhớ nữa.

- Kỹ thuật lây lan.

Đoạn mã thực hiện nhiệm vụ lây lan là đoạn mã quan trọng trong chương trình virus. Để đảm bảo việc lây lan, virus khống chế ngắt quan trọng nhất trong việc đọc/ghi vùng hệ thống: đó là ngắt 13h, tuy nhiên để đảm bảo tốc độ truy xuất đĩa, chỉ các chức năng 2 và 3 (đọc/ghi) là dẫn tới việc lây lan. Việc lây lan bông cách đọc Boot Sector (Master Boot) lên và kiểm tra xem đã bị lây chưa (kỹ thuật kiểm tra đã nói ở trên). Nếu sector khởi động đó chưa bị nhiễm thì virus sẽ tạo một sector khởi động mới với các tham số tương ứng của đoạn mã virus rồi ghi trở lại vào vị trí của nó trên đĩa. Còn sector khởi động vừa đọc lên cùng với thân của virus (loại DB-virus) sẽ được ghi vào vùng xác định trên đĩa. Ngoài ra một số virus còn chiếm ngắt 21 của DOS để lây nhiễm và phá hoại trên các file mà ngắt 21 làm việc.

Việc xây dựng sector khởi động có đoạn mã của virus phải đảm bảo các kỹ thuật sau đây:

- Sector khởi động bị nhiễm phải còn chứa các tham số đĩa phục vụ cho quá trình truy xuất đĩa, đó là bảng tham số BPB của Boot record hay bảng phân chương trong trường hợp Master boot. Việc không bảo toàn sẽ dẫn đến việc virus mất quyền điều khiển hoặc không thể kiểm soát được đĩa nếu virus không có mặt trong môi trường.

- Sự an toàn của sector khởi động nguyên thể và đoạn thân của virus cũng phải được đặt lên hàng đầu. Các kỹ thuật về vị trí cất giấu chúng ta cũng đã phân tích ở các phần

trên.

- Kỹ thuật ngụy trang và gây nhiễu.

Kỹ thuật này ra đời khá muộn về sau này, do khuynh hướng chống lại sự phát hiện của người sử dụng và những lập trình viên đối với virus. Vì kích thước của virus khá nhỏ bé cho nên các lập trình viên hoàn toàn có thể dò từng bước xem cơ chế của virus hoạt động như thế nào, cho nên các virus tìm mọi cách lắt léo để chống lại sự theo dõi của các lập trình viên.

Các virus thường áp dụng một số kỹ thuật sau đây:

- Cố tình viết các lệnh một cách rắc rối như đặt Stack vào các vùng nhớ nguy hiểm, chiếm và xoá các ngắt, thay đổi một cách lắt léo các thanh ghi phân đoạn để người dò không biết dữ liệu lấy từ đâu, thay đổi các giá trị của các lệnh phía sau để người sử dụng khó theo dõi.

- Mã hoá ngay chính chương trình của mình để người sử dụng không phát hiện ra quy luật, cũng như không thấy một cách rõ ràng ngay sự hoạt động của virus.

- Ngụy trang: Cách thứ nhất là đoạn mã cài vào sector khởi động càng ngắn càng tốt và càng giống sector khởi động càng tốt. Tuy vậy cách thứ hai vẫn được nhiều virus áp dụng: Khi máy đang nôm trong quyền chi phối của virus, mọi yêu cầu đọc/ghi Boot sector (Master boot) đều được virus trả về một bản chuẩn: bản trước khi bị virus lây. Điều này đánh lừa người sử dụng và các chương trình chống virus không được thiết kế tốt nếu máy hiện đang chịu sự chi phối của virus.

- Kỹ thuật phá hoại.

Đã là virus thì bao giờ cũng có tính phá hoại. Có thể phá hoại ở mức đùa cho vui, cũng có thể là phá hoại ở mức độ nghiêm trọng, gây mất mát và đình trệ đối với thông tin trên đĩa.

Căn cứ vào thời điểm phá hoại, có thể chia ra thành hai loại:

- Loại định thời: Loại này lưu giữ một giá trị, giá trị này có thể là ngày giờ, số lần lây nhiễm, số giờ máy đã chạy, ... Nếu giá trị này vượt quá một con số cho phép, nó sẽ tiến hành phá hoại. Loại này thường nguy hiểm vì chúng chỉ phá hoại một lần.

- Loại liên tục: Sau khi bị lây nhiễm và liên tục, virus tiến hành phá hoại, song do tính liên tục này, các hoạt động phá hoại của nó không mang tính nghiêm trọng, chủ yếu là đùa cho vui.

1.4 Đặc Điểm Của F-Virus:

So với B-virus thì số lượng F-virus đông đảo hơn nhiều, có lẽ do các tác vụ đĩa với sự hỗ trợ của Int 21 đã trở nên cực kỳ dễ dàng và thoải mái, đó là điều kiện phát triển cho các F-virus.

Thường thì các F-virus chỉ lây lan trên các file khả thi (có đuôi .COM hoặc .EXE), tuy nhiên một nguyên tắc mà virus phải tuân thủ là: Khi thi hành một file khả thi bị lây nhiễm, quyền điều khiển phải nôm trong tay virus trước khi virus trả nó lại cho file bị nhiễm, và khi file nhận lại quyền điều khiển, tất cả mọi dữ liệu của file phải được bảo toàn.

Đối với F-virus, có một số kỹ thuật được nêu ra ở đây:

a. Kỹ thuật lây lan:

Các F-virus chủ yếu sử dụng hai kỹ thuật: Thêm vào đầu và thêm vào cuối

- Thêm vào đầu file.

Thông thường, phương pháp này chỉ áp dụng cho các file .COM, tức là đầu vào của chương trình luôn luôn tại PSP0h. Lợi dụng đầu vào cố định, virus chèn đoạn mã của chương trình virus vào đầu chương trình đối tượng, đẩy toàn bộ chương trình đối tượng xuống phía dưới. Cách này có một nhược điểm là do đầu vào cố định của chương trình .COM là PSP0, cho nên trước khi trả lại quyền điều khiển cho chương trình, phải đẩy lại toàn bộ chương trình lên bắt đầu từ offset 100h. Cách lây này gây khó khăn cho những người khôi phục vì phải đọc toàn bộ file vào vùng nhớ rồi mới tiến hành ghi lại.

- Thêm vào cuối file.

Khác với cách lây lan ở trên, trong phương pháp này, đoạn mã của virus sẽ được gắn vào sau của chương trình đối tượng. Phương pháp này được thấy trên hầu hết các loại virus vì phạm vi lây lan của nó rộng rãi hơn phương pháp trên.

Do thân của virus không nôm đúng đầu vào của chương trình, cho nên để chiếm quyền điều khiển, phải thực hiện kỹ thuật sau đây:

- Đối với file .COM: Thay các byte đầu tiên của chương trình (đầu vào) bông một lệnh nhảy JMP, chuyển điều khiển đến đoạn mã của virus.

E9 xx xx JMP Entry virus.

- Đối với file .EXE: Chỉ cần định vị lại hệ thống các thanh ghi SS, SP, CS, IP trong Exe Header để trao quyền điều khiển cho phần mã virus.

Ngoài hai kỹ thuật lây lan chủ yếu trên, có một số ít các virus sử dụng một số các kỹ thuật đặc biệt khác như mã hoá phần mã của chương trình virus trước khi ghép chúng vào file để ngụy trang, hoặc thậm chí thay thế một số đoạn mã ngắn trong file đối tượng bông các đoạn mã của virus, gây khó khăn cho quá trình khôi phục.

Khi tiến hành lây lan trên file, đối với các file được đặt các thuộc tính Sys (hệ thống), Read Only (chỉ đọc), Hidden (ẩn), phải tiến hành đổi lại các thuộc tính đó để có thể truy nhập, ngoài ra việc truy nhập cũng thay đổi lại ngày giờ cập nhật của file, vì thế hầu hết các virus đều lưu lại thuộc tính, ngày giờ cập nhật của file để sau khi lây nhiễm sẽ trả lại y nguyên thuộc tính và ngày giờ cập nhật ban đầu của nó.

Ngoài ra, việc cố gắng ghi lên đĩa mềm có dán nhãn bảo vệ cũng tạo ra dòng thông báo lỗi của DOS: Retry - Aboart - Ignoreô, nếu không xử lý tốt thì dễ bị người sử dụng phát hiện ra sự có mặt của virus. Lỗi kiểu này được DOS kiểm soát bông ngắt 24h, cho nên các virus muốn tránh các thông báo kiểu này của DOS khi tiến hành lây lan phải thay ngắt 24h của DOS trước khi tiến hành lây lan rồi sau đó hoàn trả.

b. Kỹ thuật đảm bảo tính tồn tại duy nhất.

Cũng giống như B-virus, một yêu cầu nghiêm ngặt đặt ra đối với F-virus là tính tồn tại duy nhất của mình trong bộ nhớ cũng như trên file.

Trong vùng nhớ, thông thường các F-virus sử dụng hai kỹ thuật chính: Thứ nhất là tạo thêm chức năng cho DOS, bông cách sử dụng một chức năng con nào đó trong đó đặt chức năng lớn hơn chức năng cao nhất mà DOS có. Để kiểm tra chỉ cần gọi chức năng này, giá trị trả lại trong thanh ghi quyết định sự tồn tại của virus trong bộ nhớ hay chưa. Cách thứ hai là so sánh một đoạn mã trong vùng nhớ ấn định với đoạn mã của virus, nếu có sự chênh lệch thì có nghĩa là virus chưa có mặt trong vùng nhớ và sẽ tiến hành lây lan.

Trên file, có thể có các cách kiểm tra như kiểm tra bông test logic nào đó với các thông tin của Entry trong thư mục của file này. Cách này không đảm bảo tính chính xác tuyệt đối song nếu thiết kế tốt thì khả năng trùng lặp cũng hạn chế, hầu như không có, ngoài ra một ưu điểm là tốc độ thực hiện kiểm tra rất nhanh. Ngoài ra có thể kiểm tra bông cách dò một đoạn mã đặc trưng (key value) của virus tại vị trí ấn định nào đó trên file, ví dụ trên các byte cuối cùng của file.

c. Kỹ thuật thường trú

Đây là một kỹ thuật khó khăn, lý do là DOS chỉ cung cấp chức năng thường trú cho chương trình, nghĩa là chỉ cho phép cả chương trình thường trú. Vì vậy nếu sử dụng chức năng của DOS, chương trình virus muốn thường trú thì cả file đối tượng cũng phải thường trú, mà điều này thì không thể được nếu kích thước của file đối tượng quá lớn.

Chính vì lý do trên, hầu hết các chương trình virus muốn thường trú đều phải thao tác qua mặt DOS trên chuỗi MCB bông phương pháp "thủ công". Căn cứ vào việc thường trú được thực hiện trước hay sau khi chương trình đối tượng thi hành, có thể chia kỹ thuật thường trú thành hai nhóm:

- Thường trú trước khi trả quyền điều khiển.

Như đã nói ở trên, DOS không cung cấp một chức năng nào cho kiểu thường trú này, cho nên chương trình virus phải tự thu xếp. Các cách sau đây đã được virus dùng đến:

- Thao tác trên MCB để tách một khối vùng nhớ ra khỏi quyền điều khiển của DOS, rồi dùng vùng này để chứa chương trình virus.

- Tự định vị vị trí trong bộ nhớ để tải phần thường trú của virus vào, thường thì các virus chọn ở vùng nhớ cao, phía dưới phần tạm trú của file command.com để tránh bị ghi đè khi hệ thống tải lại command.com. Vì không cấp phát bọ nhớ cho phần chương trình virus đang thường trú, cho nên command.com hoàn toàn có quyền cấp phát vùng nhớ đó cho các chương trình khác, nghĩa là chương trình thương trú của virus phải chấp nhận sự mất mát do may rủi.

- Thường trú bông chức năng thường trú 31h: Đây là một kỹ thuật phức tạp, tiến trình cần thực hiện được mô tả như sau:

Khi chương trình virus được trao quyền, nó sẽ tạo ra một MCB được khai báo là phần tử trung gian trong chuỗi MCB để chứa chương trình virus, sau đó lại tạo tiếp một MCB mới để cho chương trình bị nhiễm bông cách dời chương trình xuống vùng mới này. Để thay đổi PSP mà DOS đang lưu giữ thành PSP mà chương trình virus tạo ra cho chương trình đối tượng, phải sử dụng chức năng 50h của ngắt 21h.

-. Thường trú sau khi đoạt lại quyền điều khiển.

Chương trình virus lấy tên chương trình đang thi hành trong môi trường của DOS, rồi nó thi hành ngay chính bản thân mình. Sau khi thi hành xong, quyền điều khiển lại được trả về cho virus, và khi đó nó mới tiến hành thường trú một cách bình thường bông chức năng 31h của ngắt 21h.

c. Kỹ thuật nguỵ trang và gây nhiễu

Một nhược điểm không tránh khỏi là file đối tượng bị lây nhiễm virus sẽ bị tăng kích thước. Một số virus ngụy trang bông cách khi sử dụng chức năng DIR của DOS, virus chi phối chức năng tìm kiếm file (chức năng 11h và 12h của ngắt 21h) để giảm kích thước của file bị lây nhiễm xuống, vì thế khi virus đang chi phối máy tính, nếu sử dụng lệnh DIR của DOS, hoặc các lệnh sử dụng chức năng tìm kiếm file ở trên để có thông tin về entry trong bảng thư mục, thì thấy kích thước file bị lây nhiễm vẫn bông kích thước của file ban đầu, điều này đánh lừa người sử dụng về sự trong sạch của file này.

Một số virus còn gây nhiễu bông cách mã hoá phần lớn chương trình virus, chỉ khi nào vào vùng nhớ, chương trình mới được giải mã ngược lại. Một số virus anti-debug bông cách chiếm ngắt 1 và ngắt 3. Bởi vì các chương trình debug thực chất phải dùng ngắt 1 và ngắt 3 để thi hành từng bước một, cho nên khi virus chiếm các ngắt này rồi mà người lập trình dùng debug để theo dõi virus thì kết quả không lường trước được.

d. Kỹ thuật phá hoại

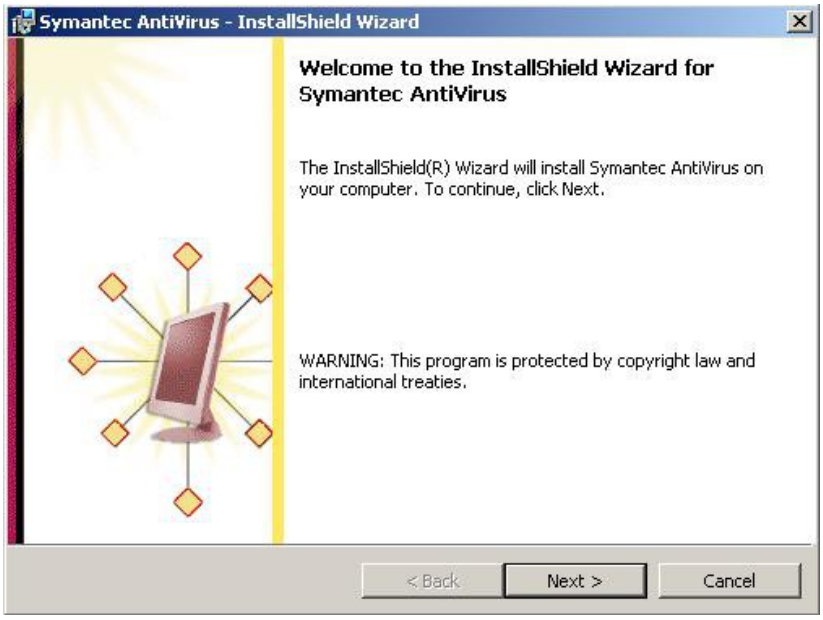
Thông thường, các F-virus cũng sử dụng cách thức và kỹ thuật phá hoại giống như B-virus. Có thể phá hoại một cách định thời, liên tục hoặc ngẫu nhiên. Đối tượng phá hoại có thể là màn hình, loa, đĩa,...

2. Phòng Chống Virus:

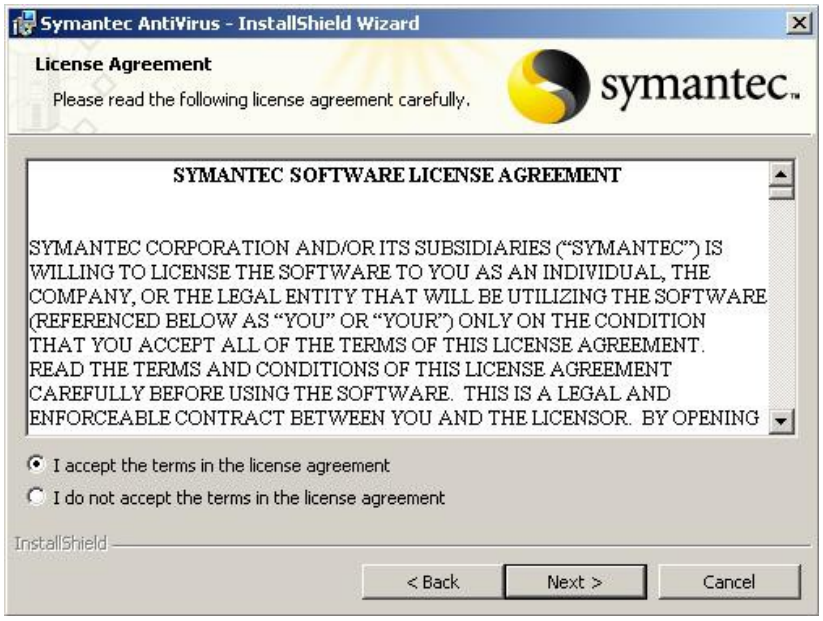
Để phòng chống virus có nhiều cách khác nhau, cách phổ biến nhất ngày nay là sử dụng các phần mềm diệt virus.
Symantec antivirus là một trong những phần mềm diệt virus phổ biến nhất hiện nay.

2.1 Cài Đặt Chương Trình Symantec Antivirus Server (Server Intall):

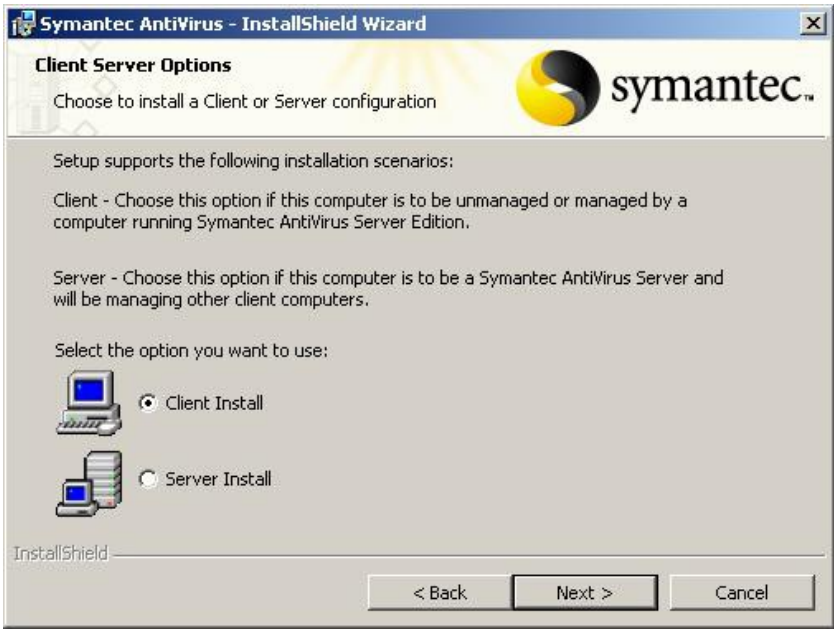
Chạy file cài đặt setup.exe
Màng hình welcome …. xuất hiện



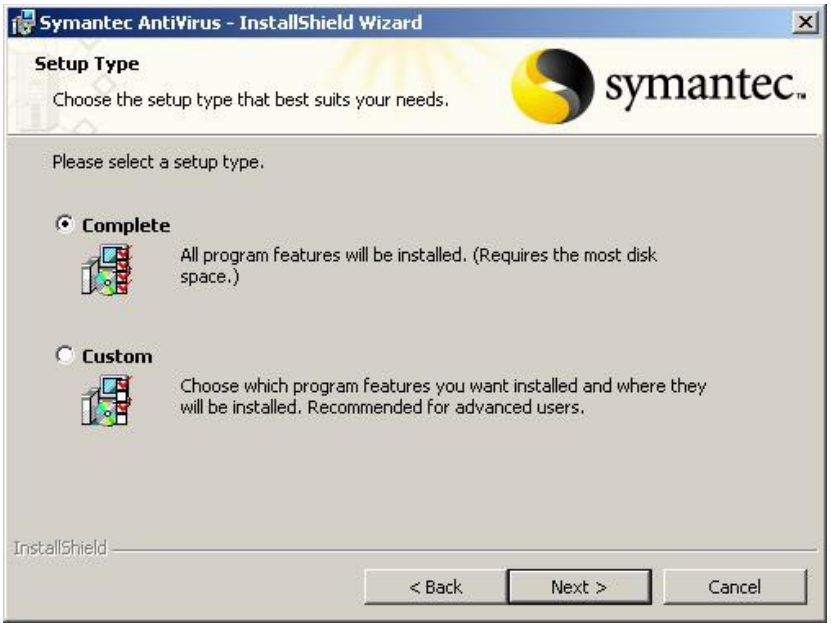
Chọn Next → màng hình xác nhận bản quyền xuất hiện → chọn I accept … để tiếp tục quá trình cài đặt



Chọn Next → màng hình chọn lựa phương thức cài đặt xuất hiện: client server option → chọn server intall

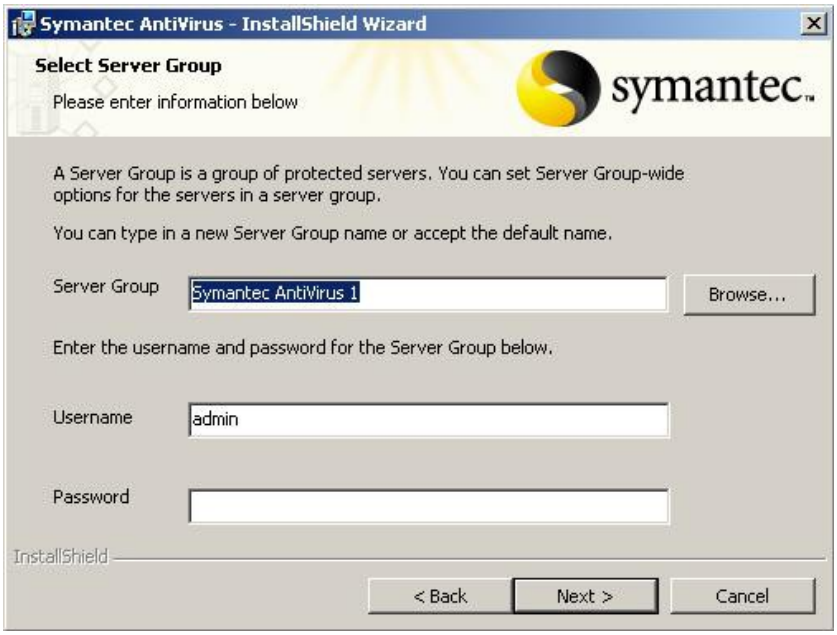


Chọn next → hộp thoại setup type xuất hiện → chọn complete để cài đặt đầy đủ các tính năng của chương trình



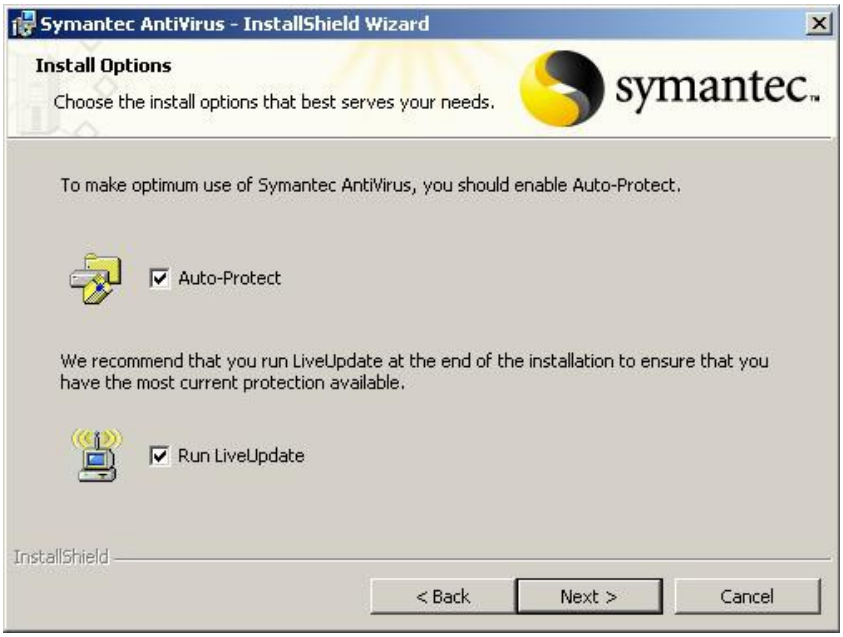
Chọn Next → hộp thoại select server group xuất hiện → trong hộp thoại này, khai báo các thông tin sau:

- server group: cho phép khai báo nhóm server
- username: khai báo user cho phép đăng nhập server sau khi cài đặt
- Password: cho phép khai báo password của user đăng nhập

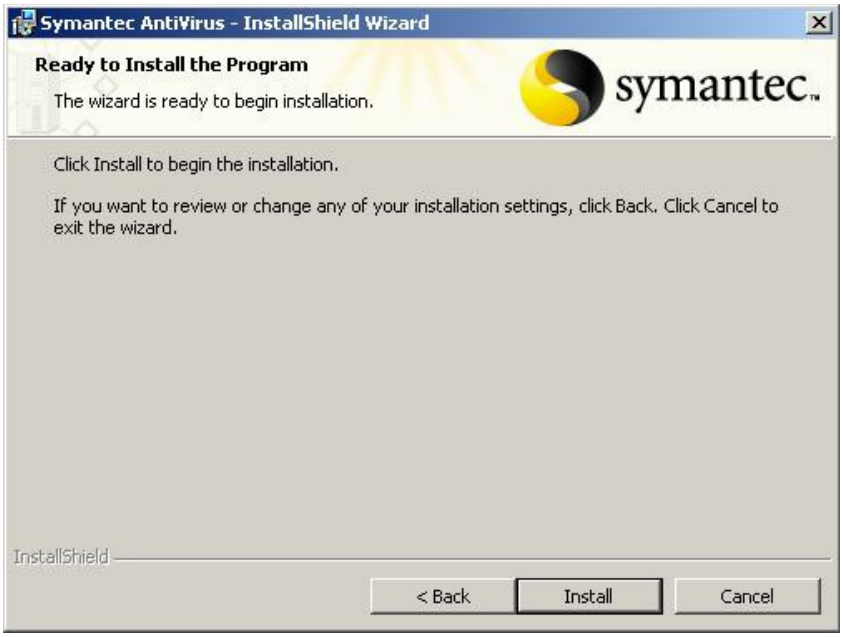


Chọn next → hộp thoại xác nhận password xuất hiện: gỏ lại password lại một lần nữa.

Chọn ok → hộp thoại intall option xuất hiện



Chọn next → hộp thoại ready to … xuất hiện để xác lập lại quá trình cài đặt



Chọn install để bắt đầu quá trình cài đặt

2.2 Cài Đặt Chương Trình Symantec System Center:

a. Chức năng:

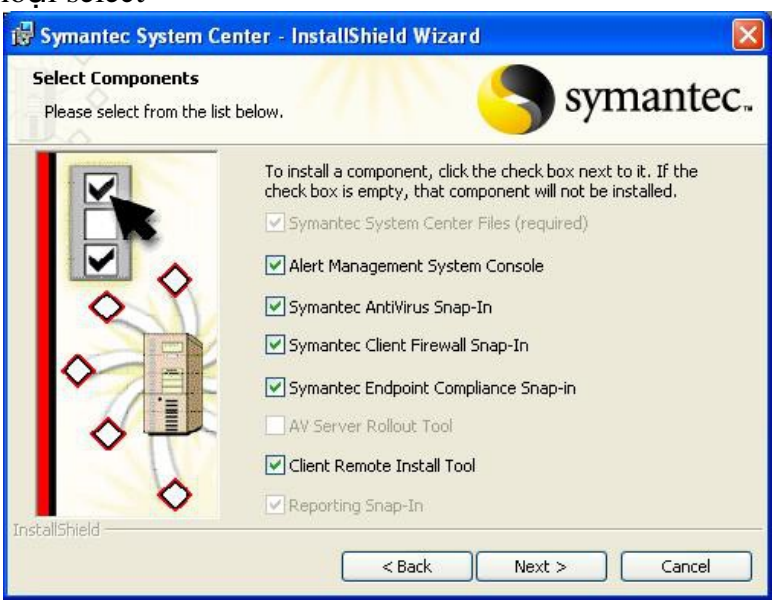
Đây là chương trình cho phép quản lý các symantec antivirus server và symantec antivirus client.

Thông qua chương trình này chúng ta có thể thực hiện các chức năng quản lý như:

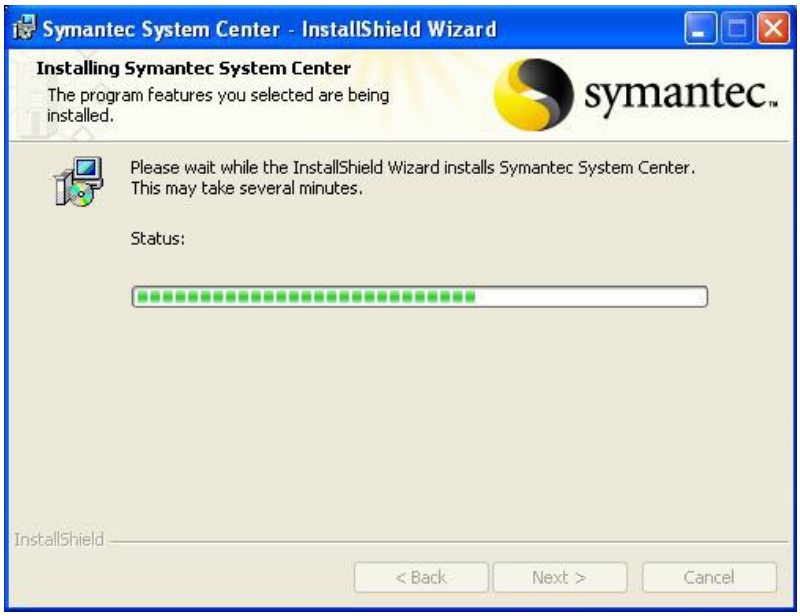
- Cài đặt antivirus và bảo vệ các lỗ hổng bảo mật trên máy.
- Cho phép cập nhật symantec antivirus client defination
- Cài đặt các chương trình bảo vệ trên máy trạm
- ….

b. Cài đặt :

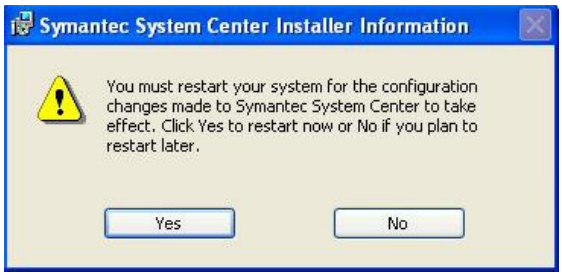
Các bước cài đặt cũng giống như cài đặt synmantec server.
Tại hộp thoại select



Chọn next …. → install để bắt đầu quá trình cài đặt



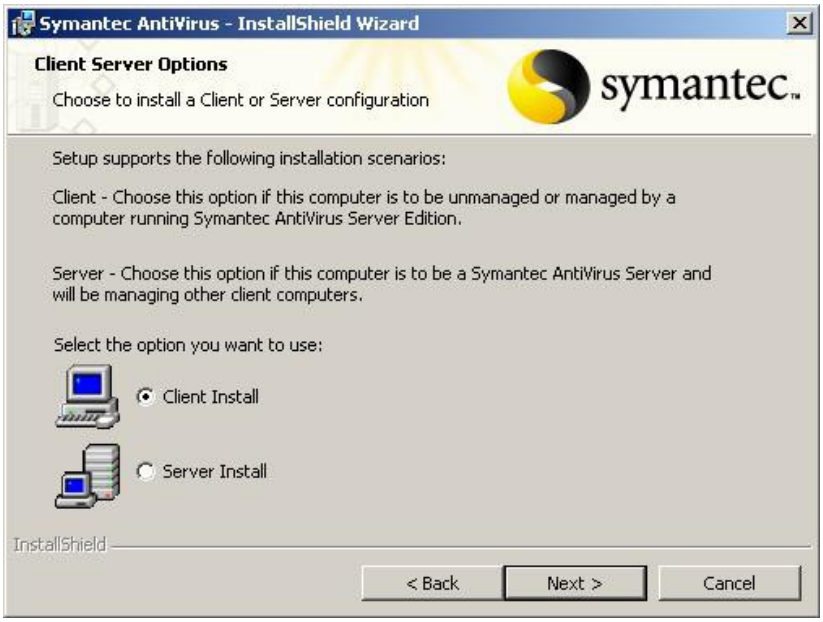
Sau khi quá trình cài đặt hoàn tất chương trình sẽ yêu cầu chúng ta khởi động lại máy :



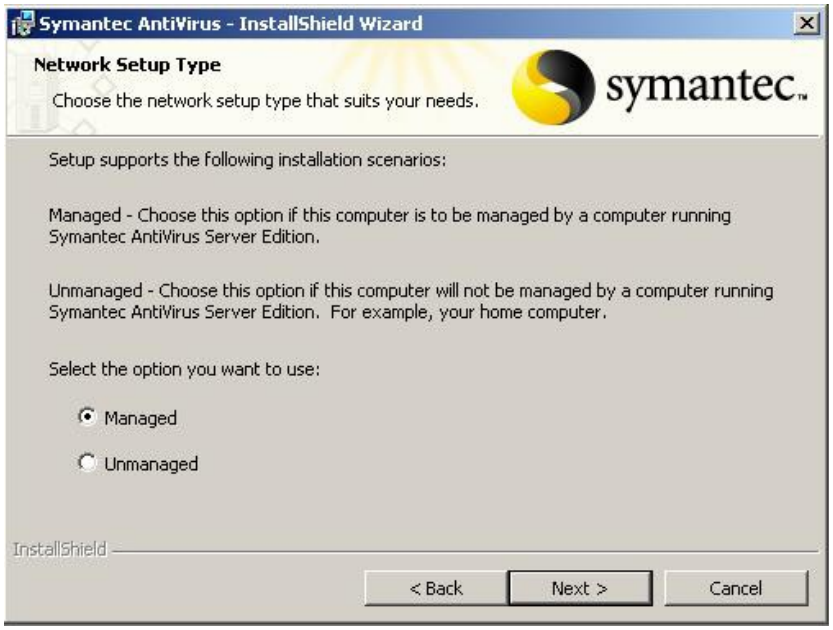
Chọn ok để khởi động lại máy.

2.3 Cài Đặt Symantec Antivirus Client :

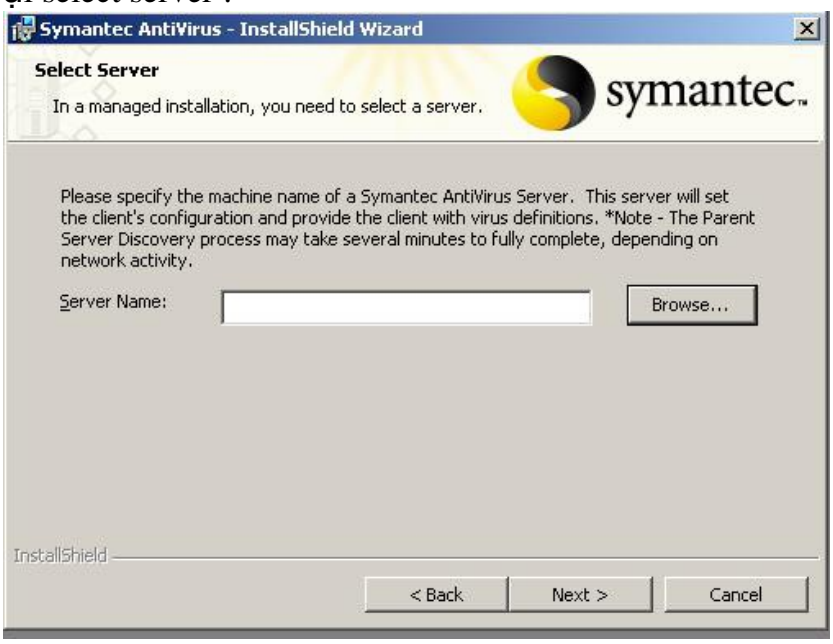
Các bước cài đặt symantec client giống như cài đặt symantec server chỉ khác tại hộp thoại client server option : chọn mục client intall



Chọn next → hộp thoại network setup type → chọn managed → next



Hộp thoại select server :



Chọn browse để tìm kiếm symantec server mà client cần kết nối đến :

Chọn server cần kết nối đến → ok → chọn next để bắt đầu quá trình cài đặt