UBND TỈNH LÂM ĐỒNG

TRƯỜNG CAO ĐẲNG ĐÀ LẠT

GIÁO TRÌNH

MÔ ĐUN: AN TOÀN VÀ BẢO MẬT THÔNG TIN

NGÀNH/NGHỀ: CÔNG NGHỆ THÔNG TIN (ỨNG DỤNG PHẦN MỀM)

TRÌNH ĐỘ: CAO ĐẲNG

Ban hành kèm theo Quyết định số: /QĐ-... ngày…….tháng….năm ..... …… ..... của……

LƯU HÀNH NỘI BỘ

Đà Lạt, năm 2017.

TUYÊN BỐ BẢN QUYỀN

LỜI GIỚI THIỆU

Giáo trình An toàn và bảo mật thông tin là giáo trình thuộc trình độ Cao đẳng Nghề Công nghệ thông tin(ứng dụng phần mềm)

Giáo trình gồm 05 bài cụ thể như sau:

Bài 1: Các khái niệm cơ bản về an toàn thông tin

Bài 2: Những điểm yếu và phương pháp tấn công vào hệ thống

Bài 3: Hạ tầng cơ sở an toàn thông tin

Bài 4: Mật mã công khai mô hình ứng dụng

Bài 5: Các chính sách và quy trình thực thi an toàn thông tin trên hệ thống

Lâm đồng, ngày 7 tháng 7 năm 2017

Tham gia biên soạn

Chủ biên: Phan Ngọc Bảo

MỤC LỤC

GIÁO TRÌNH MÔ ĐUN

Tên mô đun: AN TOÀN VÀ BẢO MẬT THÔNG TIN

Mã mô đun: MĐ 22

Vị trí, tính chất, ý nghĩa và vai trò của mô đun:

- Vị trí: Mô đun An toàn và bảo mật thông tin là mô đun thuộc nhóm các môn học/mô đun chuyên môn nghề, thuộc trình độ Cao đẳng Nghề Công nghệ thông tin(ứng dụng phần mềm).

- Tính chất: Mô đun được học sau các mô đun chuyên môn nghề: Hệ điều hành Windows Server, Thiết kế và quản trị website.

- Ý nghĩa và vai trò của môn học/mô đun: Mô đun này cung cấp cho người học những kiến thức về an toàn và bảo mật thông tin.

Mục tiêu của mô đun:

- Về kiến thức:

+ Trình bày các khái niệm cơ bản về an toàn thông tin và mật mã;

+ Trình bày quy trình thực thi an toàn thông tin trong hệ thống;

+ Trình bày về chứng thực điện tử và một số giải pháp bảo mật khác;

+ Vận dụng được các phương pháp mã hóa đối xứng và cơ sở hạ tầng khóa công khai;

- Về kỹ năng:

+ Thực hiện được các quy trình thực thi an toàn thông tin hệ thống;

+ Cấu hình hệ thống đảm bảo an toàn dữ liệu, chống tấn công thâm nhập trái phép;

+ Thiết kế được hạ tầng cơ sở an toàn thông tin cho hệ thống;

+ Xây dựng được mô hình bảo mật, toàn vẹn dữ liệu trên hệ thống khóa công khai

+ Phục hồi sự cố trong hệ thống;

+ Quản trị và phân quyền trên hệ thống;

- Về năng lực tự chủ và trách nhiệm:

- Có khả năng tự nghiên cứu, tự học, tham khảo tài liệu liên quan đến môn học để vận dụng vào hoạt động hoc tập.

- Vận dụng được các kiến thức tự nghiên cứu, học tập và kiến thức, kỹ năng đã được học để hoàn thiện các kỹ năng liên quan đến môn học một cách khoa học, đúng quy định.

Nội dung của mô đun:

Bài 1: Các khái niệm cơ bản về an toàn thông tin

Mã bài: MD22-1

Giới thiệu: Bài 1 cung cấp các khái niệm cơ bản về an toàn thông tin

Mục tiêu:

- Trình bày những khái niệm cơ bản về an toàn thông tin, vai trò của chúng;
- Trình bày một số dịch vụ và phương thức hay sử dụng trên hệ thống thông tin;
- Trình bày các phương thức truy cập hệ thống;
- Xác định được rủi ro và các mối đe dọa trên hệ thống; Có được tính chủ động, khoa học, cẩn thận, tỉ mỉ, chính xác.

Nội dung chính:

1. Thế nào là an toàn thông tin

1.1. Định nghĩa

An toàn thông tin là các hoạt động bảo vệ tài sản thông tin và là một lĩnh vực rộng lớn. Nó bao gồm cả những sản phẩm và những quy trình nhằm ngăn chặn truy cập trái phép, hiệu chỉnh, xóa thông tin,...

An toàn thông tin liên quan đến hai khía cạnh đó là an toàn về mặt vật lý và an toàn về mặt kỹ thuật.

- Mục tiêu cơ bản của an toàn thông tin

+ Đảm bảo tính bảo mật

+ Đảm bảo tính toàn vẹn

+ Đảm bảo tính xác thực

+ Đảm bảo tính sẵn sàng

1.2. Vai trò của an toàn thông tin: Yếu tố con người , công nghệ

* Bảo vệ tài nguyên của hệ thống

Các hệ thống máy tính lưu giữ rất nhiều thông tin và tài nguyên cần được bảo vệ. Trong một tổ chức, những thông tin và tài nguyên này có thể là dữ liệu kế toán, thông tin nguồn nhân lực, thông tin quản lý, bán hàng, nghiên cứu, sáng chế, phân phối, thông tin về tổ chức và thông tin về các hệ thống nghiên cứu. Đối với rất

nhiều tổ chức, toàn bộ dữ liệu quan trọng của họ thường được lưu trong một cơ sở dữ liệu và được quản lý và sử dụng bởi các chương trình phần mềm.

Các tấn công vào hệ thống có thể xuất phát từ những đối thủ của tổ chức hoặc cá nhân do đó, các phương pháp để bảo đảm an toàn cho những thông tin này có thể rất phức tạp và nhạy cảm. Các tấn công có thể xuất phát từ nhiều nguồn khác nhau, cả từ bên trong và bên ngoài tổ chức. Hậu quả mà những tấn công thành công để lại sẽ rất nghiêm trọng.

* Bảo đảm tính riêng tư

Các hệ thống máy tính lưu giữ rất nhiều thông tin cá nhân cần được giữ bí mật. Những thông tin này bao gồm: Số thẻ bảo hiểm xã hội, số thẻ ngân hàng, số thẻ tín dụng, thông tin về gia đình,…

Tính riêng tư là yêu cầu rất quan trọng mà các ngân hàng, các công ty tín dụng, các công ty đầu tư và các hãng khác cần phải đảm bảo để gửi đi các tài liệu thông tin chi tiết về cách họ sử dụng và chia sẻ thông tin về khách hàng. Các hãng này có những quy định bắt buộc để bảo đảm những thông tin cá nhân được bí mật và bắt buộc phải thực hiện những quy định đó để bảo đảm tính riêng tư. Hậu quả nghiêm trọng sẽ xảy ra nếu một kẻ giả mạo truy nhập được những thông tin cá nhân.

Nói chung là có rất nhiều thủ thuật, từ việc trực tiếp sử dụng kỹ thuật hoặc không cần đế kỹ thuật như Social Engineering là cách thức không cần nhiều đến kỹ thuật, hoặc là khống chế người thân của ai đó để có được thông tin mình cần (nghe có vẻ bạo lực quá) hoặc là cài key-logger cho nó nhẹ nhàng và liên quan tới kỹ thuật một tí. Đó chính là lý do mà việc kiểm soát truy cập ra đời và kiểm soát cũng đi liền với giám sát (bao gồm cả Monitoring và Recording, tức là cả Prevention lẫn Detection).

1.3. Các chính sách về an toàn thông tin

Chính sách bảo mật

2. Kiểm sóat truy cập

2.1. Khái niệm

Access Control hay kiểm soát truy cập, được chia thành 2 thành phần là Access và Control. Access được biết đến như việc truy cập các tài nguyên của một chủ thể (Subject) tới một đối tượng (Object), Control được biết đến là hành động cho phép hoặc không cho phép truy cập, cũng như các phương thức áp dụng cho Access Control. Một chủ thể (Subject) có thể là Users, Program, Service…và đối tượng (Object) có thể là File, Database, hay một Service nào đó; việc xác định chủ thể để cấp cho quyền hạn truy cập vào đối tượng là công việc chủ yếu của Access

Control. Áp dụng Access Control vào trong cuộc sống rất nhiều, và cũng có rất nhiều mô hình dựng nên cho Access Control này. Xem xét một số ví dụ về Access Control, khóa cửa là một cách thức áp dụng Access Control vì chỉ có người có chìa khóa (Subject) mới có thể mở khóa và sử dụng phòng (Object). Ở ví dụ này, người là chủ thể, khóa và chìa khóa là phương thức áp dụng, còn phòng là đối tượng.

Việc xác định chủ thể (Subject) thường được biết đến với cái tên là Identify, có nhiều cách để định danh, nhận diện, giữa các chương trình với nhau có thể sử dụng các PID (Process ID), cũng có thể dựa trên Username, hoặc một Biometric như giọng nói, vân tay … Việc này không khó, và dĩ nhiên để đảm bảo chính xác là người đó thì cần phải kiểm chứng thông qua một vài điều bí mật mà chỉ có người đó mới biết, chẳng hạn như Password, PIN, Token, hoặc là Biometric (Fingerprint), và lần này sẽ dùng những thông tin đó cùng với thuật toán, cách thức xử lý để đối chiếu thông tin và 'thẩm định' có đúng người đó hay không. Quá trình này được gọi là Authentication, tức là chứng thực; chứng thực có thể chỉ sử dụng một lần hoặc nhiều lần tùy thuộc chính sách và cũng có thể có nhiều phương pháp, cách thức khác nhau.

2.2. Các phương thức truy cập hệ thống

Tấn công trực tiếp

Kỹ thuật đánh lừa

Kỹ thuật tấn công vào tường ẩn

2.3. MAC/DAC/RBAC

MAC (tiếng Anh: Media Access Control hay Medium Access Control có nghĩa là "điều khiển truy nhập môi trường") là tầng con giao thức truyền dữ liệu - một phần của tầng liên kết dữ liệu trong mô hình 7 tầng OSI. Nó cung cấp các cơ chế đánh địa chỉ và điều khiển truy nhập kênh (channel access), các cơ chế này cho phép các trạm cuối (terminal) hoặc các nút mạng liên lạc với nhau trong một mạng, điển hình là mạng LAN hoặc MAN. Giao thức MAC không cần thiết trong liên lạc điểm-tới-điểm song công (full-duplex).

Tầng con MAC hoạt động với vai trò một giao diện giữa tầng con điều khiển liên kết lôgic LLC và tầng vật lý của mạng.

Tầng MAC cung cấp một cơ chế đánh địa chỉ được gọi là địa chỉ vật lý hoặc địa chỉ MAC. Đây là một con số được cấp một cách phân biệt cho từng bo mạch mạng, cho phép chuyển giao các gói dữ liệu tới đích trong một mạng con, nghĩa là một mạng vật lý không có các thiết bị định tuyến, ví dụ một mạng Ethernet.

MAC - Media access control thường được dùng như là một từ đồng nghĩa với giao thức đa truy nhập (multiple access protocol), do tầng con MAC cung cấp giao thức và các cơ chế điều khiển cần thiết cho một phương pháp truy nhập kênh nhất định (channel access method). Việc này cho phép nhiều trạm kết nối tới cùng một môi trường vật lý dùng chung môi trường đó. Ví dụ về các môi trường vật lý dùng chung là bus network, ring network, hub network, mạng không dây và các liên kết điểm-tới-điểm bán song công (half-duplex).

Các ví dụ về các giao thức đa truy nhập kiểu gói tin (packet mode) dành cho các mạng nối dây đa chặng (multi-drop):

CSMA/CD (dùng trong Ethernet và IEEE 802.3),

Token ring (IEEE 802.4)

Token bus (IEEE 802.5)

Token passing (dùng trong FDDI).

3. Xác thực

3.1. Kerberos

Kerberos là một giao thức mật mã dùng để xác thực trong các mạng máy tính hoạt động trên những đường truyền không an toàn. Giao thức Kerberos có khả năng chống lại việc nghe lén hay gửi lại các gói tin cũ và đảm bảo tính toàn vẹn của dữ liệu. Mục tiêu khi thiết kế giao thức này là nhằm vào mô hình máy chủ-máy khách (*client-server*) và đảm bảo nhận thực cho cả hai chiều.

Giao thức được xây dựng dựa trên mật mã hóa khóa đối xứng và cần đến một bên thứ ba mà cả hai phía tham gia giao dịch tin tưởng.

3.2. CHAP

Chap là giao thức Three way

Bước 1: Các ISP lúc nào cũng tung ra các gói challenge(thách thức) broadcast

Bước 2: Khi model nhận được gói challenge nó sẽ trả lời lại(response). Password được hash rồi mới gửi. Chuỗi hash bao gồm: Username/password và hostname. Nên username của bên này là hostname của bên kìa và ngược lại

Bước 3: ISP sẽ kiểm tra xác thực nếu đúng thì accept sai thì reject

- CHAP chủ động thuộc về ISP

3.3. Chứng nhận

Trong an ninh máy tính (*computer security*), xác thực là một quy trình nhằm cố gắng xác minh nhận dạng số (*digital identity*) của phần truyền gửi thông tin

(*sender*) trong giao thông liên lạc chẳng hạn như một yêu cầu đăng nhập. Phần gửi cần phải xác thực có thể là một người dùng sử dụng một máy tính, bản thân một máy tính hoặc một chương trình ứng dụng máy tính (*computer program*). Ngược lại Sự tin cậy mù quáng (*blind credential*) hoàn toàn không thiết lập sự đòi hỏi nhận dạng, song chỉ thiết lập quyền hoặc địa vị hẹp hòi của người dùng hoặc của chương trình ứng dụng mà thôi.

3.4. Username/Password

Tài khoản người dùng username

Mật khẩu người dùng password

3.5. Tokens

Phương pháp truy nhập có điều khiển dùng kỹ thuật "chuyển thẻ bài" để cấp phát quyền truy nhập đường truyền. Thẻ bài (Token) là một đơn vị dữ liệu đặc biệt, có kích thước và có chứa các thông tin điều khiển trong các khuôn dạng

Nguyên lý: Để cấp phát quyền truy nhập đường truyền cho các trạm đang có nhu cầu truyền dữ liệu,một thẻ bài được lưu chuyển trên một vòng logic thiết lập bởi các trạm đó. Khi một trạm nhận được thẻ bài thì nó có quyền sử dụng đường truyền trong một thời gian định trước.

Trong thời gian đó nó có thể truyền một hoặc nhiều đơn vị dữ liệu. Khi đã hết dữ liệu hay hết thời đoạn cho phép, trạm phải chuyển thẻ bài đến trạm tiếp theo trong vòng logic.

Như vậy công việc phải làm đầu tiên là thiết lập vòng logic (hay còn gọi là vòng ảo) bao gồm các trạm đang có nhu cầu truyền dữ liệu được xác định vị trí theo một chuỗi thứ tự mà trạm cuối cùng của chuỗi sẽ tiếp liền sau bởi trạm đầu tiên. Mỗi trạm được biết địa chỉ của các trạm kề trước và sau nó.

Thứ tự của các trạm trên vòng logic có thể độc lập với thứ tự vật lý. Các trạm không hoặc chưa có nhu cầu truyền dữ liệu thì không được đưa vào vòng logic và chúng chỉ có thể tiếp nhận dữ liệu.

3.6. Multi-Factor (Đa thành phần)

Là phương pháp xác thực người dùng không chỉ dựa vào một mà là nhiều yếu tố

liên quan tới người dùng, bao gồm: những thứ người dùng biết (knowledge factor),

những thứ người dùng sở hữu (possession factor) và những thứ thuộc về bản thân

người dùng (inherence factor)

Thực ra thì xác thực đa yếu tố không hề xa lạ, ví dụ đơn giản nhất là khi ta rút tiền ở ATM. Ta phải có hai yếu tố để đăng nhập vào ATM: thẻ ATM cầm trên tay (thứ mà ta sở hữu) và mật khẩu của thẻ (thứ mà ta biết). Các loại yếu tố chính bao gồm:

Yếu tố này là phổ biến nhất, bao gồm các loại như:

- Mật khẩu
- PIN: Personal Identification Number, một xâu gồm các ký tự số được sử dụng như trong thẻ ATM
- Pattern: giống như khi đăng nhập trên các thiết bị di động Android và iOS

NHỮNG THỨ NGƯỜI DÙNG SỞ HỮU (POSSESSION FACTOR)

Bao gồm một số loại như:

- One-time password (OTP): mật khẩu dùng một lần, chỉ có hiệu lực tại session hiện tại. Ví dụ như các thiết bị sau:

Thiết bị OTP của RSA, khi giao dịch người dùng sẽ nhập mã số hiện tại có trên thiết bị. Mã số sẽ thay đổi liên tục theo thời gian

Đơn giản hơn như là thẻ ma trận xác thực của ACB, khi giao dịch người dùng sẽ nhập mã số tại một số ô mà hệ thống yêu cầu

SMS OTP của VTC Pay, khi giao dịch mã số sẽ được gửi về điện thoại của khách hàng

Ngoài ra cũng có các OTP software có thể cài đặt trực tiếp lên PC hoặc smartphone giúp giảm bớt chi phí sử dụng.

- Chứng thư số: là một dạng định danh điện tử của một cá thể nào đó, được một tổ chức tin cậy cấp và đi kèm với nó là cặp public/private key duy nhất (đọc thêm về mã hóa bất đối xứng, chữ ký điện tử ở đây). Khác với chứng thư (certificate) và public key được public, private key của người dùng thường được chứa trong một thiết bị đặc biệt, có thể là usb token hoặc smartcard có chứa chip xử lý. Private key không được extract ra khỏi thiết bị này mà thiết bị chỉ cung cấp ra ngoài các API để thực hiện ký/mã hóa dữ liệu. Dữ liệu khi ký hoặc mã hóa sẽ được thực hiện ngay trong thiết bị này. Quá trình xác thực sử dụng chứng thư số diễn ra như sau:
    - Thông tin đăng nhập bao gồm username/password được người dùng nhập vào
    - Người dùng sử dụng private key của mình để ký lên thông tin đăng nhập này
    - Thông tin đăng nhập kèm theo chữ ký được gửi lên server. Server sử dụng public key của người dùng để kiểm tra tính hợp lệ của chữ ký, nếu chữ ký hợp lệ mới tiếp tục kiểm tra password được nhập vào
- Định danh của thiết bị di động: Ngày nay, với sự phổ biến của các thiết bị di động như smartphone và tablet, chúng cũng được tích hợp thêm chức năng là một yếu tố để xác thực. Một tài khoản người dùng sẽ được liên kết với một hoặc nhiều thiết bị. Dựa vào các thông tin của thiết bị như số IMEI, vị trí, khoảng cách với người đang đăng nhập, mật khẩu của thiết bị… sẽ quyết định xem người dùng có thể đăng nhập được vào hệ thống hay không. Việc tích hợp này rất tiện lợi khi người dùng không phải mang theo các token làm "móc chìa khóa".

Những thứ thuộc về người dùng (inherence factor)

Yếu tố này bao gồm những thứ thuộc về sinh trắc học, là các đặc điểm sinh học của mỗi cá nhân dấu vân tay, giọng nói, khuôn mặt hay mống mắt.

Đây được coi là công cụ xác thực hữu hiệu nhất, trong đó phổ biến nhất vẫn là nhận dạng vân tay bởi đặc tính ổn định và độc nhất của nó và cho đến nay, nhận dạng dấu vân tay vẫn được xem là một trong những phương pháp sinh trắc tin cậy nhất. Trên thế giới đã nhiều nơi sử dụng dấu vân tay trong các giao dịch tài chính hay quản lý hộ chiếu, còn ở Việt Nam mới chỉ áp dụng trong chấm công, điểm danh…Với đặc điểm là chi phí cao và khó sử dụng nên tuy mạnh nhưng công nghệ xác thực này vẫn chưa thực sự phổ biến.

Đối với một hệ thống, việc áp dụng hình thức xác thực nào, một hay nhiều yếu tố phụ thuộc khá nhiều vào khả năng tích hợp, chi phí, nhận thức về an toàn thông tin, hiểu biết về công nghệ của người dùng và vào cả tầm quan trọng của hệ thống đó. Xác thực đa yếu tố không phải là hoàn hảo, tuy nhiên nó cũng đảm bảo an toàn hơn nhiều so với phương pháp xác thực truyền thống dựa trên một yếu tố là mật khẩu/số PIN.

3.7. Mutual Authentication (Chứng thực tương hỗ)

Ngày càng có nhiều trang web đang sử dụng two-factor (2 yếu tố) hoặc multi-factor authentication (đa yếu tố chứng thực) để tăng cường khả năng bảo mật. Google muốn có số điện thoại di động của tôi để xác nhận danh tính trước khi tôi có thể đăng nhập vào Gmail. Và đó là một ý tưởng tốt. Bạn có thấy những câu chuyện về hack thường được nhấn mạnh trên các trang tin tức? Bảo mật (hoặc thiếu bảo mật) là một vấn đề thực sự quan trọng và trong khi bạn có thể không đủ khả năng để ngăn chặn những vi phạm bảo mật lớn như đã xảy ra tại The Home Depot gần đây, bạn vẫn có thể làm một điều gì đó để bảo vệ thông tin và trang web của mình.

3.8. Biometrics (Sinh trắc học)

Sinh trắc học hay **Công nghệ sinh trắc học** (tiếng Anh: Biometric) là công nghệ sử dụng những thuộc tính vật lý, đặc điểm sinh học riêng của mỗi cá nhân như vân tay, mống mắt, khuôn mặt... để nhận diện. Đây được coi là công cụ xác thực nhân thân hữu hiệu nhất mà người ta sử dụng phổ biến vẫn là nhận dạng vân tay bởi đặc tính ổn định và độc nhất của nó và cho đến nay, nhận dạng dấu vân tay vẫn được xem là một trong những phương pháp sinh trắc tin cậy nhất.

Mỗi người có một đặc điểm sinh học duy nhất. Dữ liệu sinh trắc học của từng cá nhân với đặc điểm khuôn mặt, ảnh chụp võng mạc, giọng nói sẽ được kết hợp với nhau bằng phần mềm để tạo ra mật khẩu dành cho những giao dịch điện tử, phương thức đó là "công nghệ sinh trắc đa nhân tố" Sự phát triển của công nghệ đã thay đổi từ việc lăn tay trên mực và lưu trữ trên giấy sang quét trên máy và lưu trữ kỹ thuật số.

4. Những dịch vụ và phương thức không thiết yếu
4.1. Các giao thức xoá bỏ những hệ thống
4.2. Chương trình không cần thiết.
IP Helper

Chức năng: Cung cấp kết nối đường hầm bằng cách sử dụng công nghệ chuyển tiếp IPv6 (6to4, ISATAP, Port Proxy, Teredo) và IP-HTTPS. Nếu service này dừng lại, máy tính sẽ không có các tiện ích kết nối nâng cao mà các công nghệ này cung cấp.

Tại sao có thể vô hiệu hóa: Nhiều tổ chức vẫn chưa bắt đầu thử nghiệm IPv6, chưa kể đến việc triển khai. Như đã nói, service IP Helper được đẩy mạnh trong quá trình chuyển đổi IPv4-IPv6.

Offline Files

Chức năng: Offline Files duy trì các hoạt động trong bộ nhớ cache Offline Files, đáp ứng cho các sự kiện đăng nhập và đăng xuất của người dùng, cài đặt bên trong API chung, và báo cáo các sự kiện đáng quan tâm trong các hoạt động Offline Files và những thay đổi trong trạng thái bộ nhớ cache.

Tại sao có thể vô hiệu hóa: Nếu công ty của bạn không sử dụng tính năng Offline Files trong cả Windows server và client, service này có thể được vô hiệu hóa một cách an toàn. Còn nếu bạn đang đồng bộ các tập tin trên mạng, bạn không nên vô hiệu hóa service này.

Network Access Protection Agent

Chức năng: NAP thu thập và quản lý thông tin an toàn cho các máy khách trên mạng. Thông tin được thu thập bởi NAP được sử dụng để đảm bảo rằng các máy khách có các phần mềm và thiết lập đã yêu cầu.

Nếu một máy khách không phù hợp với chính sách an toàn, nó có thể phải chấp nhận quyền truy cập mạng hạn chế cho đến khi cấu hình được cập nhật. Tùy thuộc vào việc đặt cấu hình, máy khách có thể được tự động cập nhật để người dùng nhanh chóng lấy lại quyền truy cập mạng đầy đủ mà không cần phải tự cập nhật máy tính của họ.

Tại sao có thể vô hiệu hóa: Nếu bạn không đang khắc phục lỗi hệ thống, hoặc nếu

bạn đang sửa lỗi với một công cụ của bên thứ ba mà không tận dụng NAP client, service này có thể được vô hiệu hóa.

Parental Controls

Chức năng: Service này còn sơ khai cho chức năng Windows Parental Control tồn tại trong Vista. Nó được cung cấp chỉ cho khả năng tương thích ngược.

Tại sao có thể vô hiệu hóa: Các mạng doanh nghiệp hiếm khi sử dụng chức năng Parental Control. Hơn nữa, đây lại là một service kế thừa từ Windows Vista.

Smart Card

Chức năng: Việc quản lý truy cập thẻ thông minh được thực hiện bởi service này. Nếu service này ngừng hoạt động, máy tính sẽ không thể đọc thẻ thông minh. Nếu service này bị vô hiệu hóa, rõ ràng là bất kỳ service nào phụ thuộc vào nó sẽ không thể hoạt động.

Tại sao có thể vô hiệu hóa: Nếu công ty của bạn không sử dụng thẻ thông minh cho các mục đích xác thực, bạn có thể vô hiệu hóa một cách an toàn service này.

Smart Card Removal Policy

Chức năng: Cho phép cấu hình hệ thống để khóa máy tính để bàn sau khi rút thẻ thông minh.

Tại sao có thể vô hiệu hóa: Nếu công ty không sử dụng thẻ thông minh cho các mục đích xác thực, bạn có thể vô hiệu hóa an toàn.

Windows Media Center Receiver Service

Chức năng: Service Windows Media Center dùng cho bắt sóng truyền hình và các kênh FM.

Tại sao có thể vô hiệu hóa: Trong hầu hết các môi trường doanh nghiệp, tiếp sóng truyền hình và FM trên máy tính bàn không được coi là một “chiến lược kinh doanh quan trọng" cần hỗ trợ, và nó thường không được chấp nhận. Bạn có thể vô hiệu hóa service này để tiết kiệm một số tài nguyên.

Windows Media Center Scheduler Service

Chức năng: Bắt đầu và kết thúc ghi âm các chương trình truyền hình trong Windows Media Center.

Tại sao có thể vô hiệu hóa: Cũng như Reciever service, không cần thiết phải ghi lại các chương trình truyền hình trong một môi trường doanh nghiệp.

Windows Media Player Network Sharing Service

Chức năng: Chia sẻ thư viện Windows Media Player tới những người dùng khác trên mạng và thiết bị đa phương tiện sử dụng Universal Plug and Play.

Tại sao có thể vô hiệu hóa: Trong mạng công ty, Windows Media Player không gần như không có ích gì, có lẽ chỉ trong mạng gia đình. Vô hiệu hóa service này sẽ không ảnh hưởng đến hoạt động kinh doanh.

Fax

Chức năng: Cho phép bạn gửi và nhận fax, tận dụng tài nguyên có sẵn trên máy tính hoặc trên mạng.

Tại sao có thể vô hiệu hóa:Nếu tổ chức không sử dụng service fax trong mạng lưới, vô hiệu hóa service này sẽ không ảnh hưởng đến hoạt động kinh doanh.

Home Group Listener

Chức năng: Tạo thay đổi máy tính nội bộ kết hợp với cấu hình và duy trì cho máy tính tham gia Home Group. Nếu service này dừng lại hay bị vô hiệu hóa, máy tính của bạn sẽ không hoạt động chuẩn xác trong một Home Group và Home Group của bạn cũng có thể không hoạt động chính xác.

Tại sao có thể vô hiệu hóa: Hầu hết các tổ chức kinh doanh ngoại trừ một số tổ chức nhỏ hơn-không thể sử dụng Home Group để chia sẻ tài nguyên trên mạng lưới. Hầu như an toàn khi vô hiệu hóa service này trong hệ thống mạng lưới kinh doanh.

Home Group Provider

Chức năng: Thực hiện các nhiệm vụ mạng liên quan đến cấu hình và duy trì các nhóm Home Group. Nếu service này bị dừng lại hay vô hiệu hóa, máy tính của bạn sẽ không thể phát hiện các Home Group khác và Home Group của bạn có thể không hoạt động chính xác. Chúng tôi cũng đề nghị bạn giữ lại service này.

Tại sao có thể vô hiệu hóa: Như đã nói ở trên, chỉ những tổ chức rất nhỏ có khả năng sử dụng các nhóm Home Group để chia sẻ tài nguyên trên mạng, do đó, nó gần như luôn luôn an toàn để vô hiệu hóa service này trong hệ thống.

Tablet PC Input Service

Chức năng: Kích hoạt các chức năng pen and ink trong máy tính bảng.

Tại sao có thể vô hiệu hóa: phần lớn các máy tính được triển khai cho người sử dụng không có phần cứng có thể tận dụng khả năng giống như máy tính bảng. Service này chỉ sử dụng các tài nguyên hệ thống mà không hề có lợi ích

5. Các topo mạng an toàn

5.1. Các vùng an toàn

Topology của mạng là cấu trúc hình học không gian mà thực chất là cách bố trí phần tử của mạng cũng nh cách nối giữa chúng với nhau. Thông thờng mạng có 3 dạng cấu trúc là: Mạng dạng hình sao (Star Topology), mạng dạng vòng (Ring Topology) và mạng dạng tuyến (Linear Bus Topology). Ngoài 3 dạng cấu hình kể trên còn có một số dạng khác biến tớng từ 3 dạng này nh mạng dạng cây, mạng dạng hình sao – vòng, mạng hỗn hợp,v.v….

5.1.1 Mạng dạng hình sao (Star topology)

Mạng dạng hình sao bao gồm một trung tâm và các nút thông tin. Các nút thông tin là các trạm đầu cuối, các máy tính và các thiết bị khác của mạng. Trung tâm của mạng điều phối mọi hoạt động trong mạng với các chức năng cơ bản là:

o Xác định cặp địa chỉ gửi và nhận được phép chiếm tuyến thông tin và liên lạc với nhau.

o Cho phép theo dõi và xử lý sai trong quá trình trao đổi thông tin.

o Thông báo các trạng thái của mạng…

– Ưu điểm:

o Mạng dạng hình sao cho tốc độ nhanh nhất

o Khi cable mạng bị đứt thì thưởng chí làm mất kết nối của một máy, còn những máy khác vẫn hoạt động bình thường.

o Khi có lỗi xảy ra , ta dễ dàng kiểm tra và sửa chữa

o Mạng có thể được mở rộng tuỳ theo nhu cầu sử dụng của người dùng

– Nhược điểm:

o Khả năng mở rộng mạng đều phụ thuộc vào khả năng của trung tâm. Khi trung tâm gặp sự cố thì toàn mạng đều ngưng hoạt động.

o Mạng yêu cầu nối độc lập riêng rẽ từng thiết bị ở các nút thông tin đến trung tâm. Khoảng cách từ máy đến trung tâm rất hạn chế (100 m).

o Chi phí dây mạng và thiết bị trung gian tốn kém nhiều

Nhìn chung, mạng dạng hình sao cho phép nối các máy tính vào một bộ tập trung (HUB) bằng cáp xoắn, giải pháp này cho phép nối trực tiếp máy tính với HUB không cần thông qua trục BUS, tránh được các yếu tố gây ngng trệ mạng. Gần đây, cùng với sự phát triển switching hub, mô hình này ngày càng trở nên phổ biến và chiếm đa số các mạng mới lắp.

5.1.2. Mạng dạng vòng (Ring Topology)

Mạng dạng này, bố trí theo dạng xoay vòng, đường dây cáp được thiết kế làm thành một vòng khép kín, tín hiệu chạy quanh theo một chiều nào đó. Các nút truyền tín hiệu cho nhau mỗi thời điểm chỉ đợc một nút mà thôi. Dữ liệu truyền đi phải có kèm theo địa chỉ cụ thể của mỗi trạm tiếp nhận.

– Ưu điểm:

o Mạng dạng vòng có thuận lợi là có thể nới rộng ra xa, tổng đường dây cần thiết ít hơn nên tiết kiệm được dây cable, tốc độ nhanh hơn kiểu BUS

– Nhược điểm:

o Nhược điểm của mạng này là tốc độ vẫn bị chậm

o Khi trên đường cable có sự cố thì toàn bộ mạng sẽ ngưng hoạt động

o Khi có sự cố rất khó kiểm tra phát hiện lỗi

Do mạng này có nhiều nhược điểm nên trong thực tế ít được sử dụng

5.1.3. Mạng dạng tuyến (BUS topology)

Theo cách bố trí hành lang các đường như hình vẽ thì máy chủ (host) cũng như tất cả các máy tính khác (workstation) hoặc các nút (node) đều được nối về với nhau trên một trục đường dây cáp chính để chuyển ti n tín hiệu.

Tất cả các nút đều sử dụng chung đường dây cáp chính này. Phía hai đầu dây cáp được bịt bởi một thiết bị gọi là terminator. Các tín hiệu và gói dữ liệu (packet) khi di chuyển lên hoặc xuống trong dây cáp đều mang theo địa chỉ của nơi đến.

– Ưu điểm:

o Loại hình mạng này dùng dây cáp ít nhất, dễ lắp đặt nên tiết kiệm được chi phí lắp đặt

– Nhược điểm:

o Tuy vậy cũng có những bất lợi đó là sẽ có sự ùn tắc giao thông khi di chuyển dữ liệu với lưu lượng lớn

o Khi có sự hỏng hóc ở đoạn nào đó thì rất khó phát hiện, một sự ngừng trên đường dây để sửa chữa sẽ ngừng toàn bộ hệ thống.

* Một số dạng khác:

– Mạng dạng lưới – Mesh topology:

o Cấu hình mạng dạng này kết hợp các mạng hình sao lại với nhau bằng cách kết nối các HUB hay Switch Lợi điểm của cấu hình mạng dạng này là có thể mở rộng đợc khong cách cũng nh độ lớn của mạng hình sao.

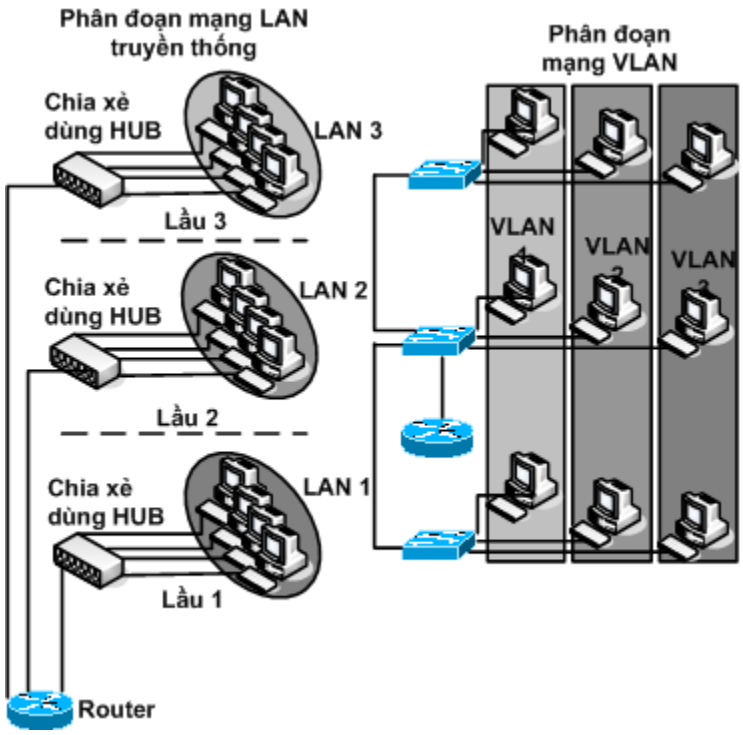
– Mạng có cấu trúc cây – Hierachical topology

o Mạng dạng này tươnng tự như mạng hình sao mở rộng nhưng thay vì liên kết các switch/hub lại với nhau thì hệ thống kết nối với một máy tính làm nhiệm vụ kiểm tra lưu thông trên mạng.

5.2. VLANs

Một chức năng lớn của công nghệ chuyển mạch Ethernet đó là VLAN. Công nghệ VLAN được sử dụng để nhóm các máy trạm và máy chủ vào trong một nhóm logic. Các thiết bị trong một VLAN được hạn chế truyền thông cùng với các thiết bị trong VLAN cho nên hoạt động mạng chuyển mạch giống như một số lượng của các LAN riêng lẻ không kết nối. Các doanh nghiệp thường sử dụng VLAN như một cách chắc chắn rằng các nhóm người dùng riêng biệt được nhóm một cách logic. Với mạng LAN thông thường các nhóm làm việc và các phòng ban (Tiếp thị

kinh doanh, Kế toán…) nằm trong một mạng vật lý, nhưng với VLAN thì được nằm trong một mạng logic.



Ví dụ: Trong một toà nhà nhiều tầng của một công ty. Các công ty con thành viên nằm trên một tầng riêng biệt. Các công ty đều có các bộ phận giống nhau như: tiếp thị, kế toán…Những người của bộ phận Tiếp thị thì nằm trong VLAN Tiếp thị nhưng họ vẫn làm việc với bộ phận Kế toán nằm trong VLAN Tiếp thị.

Trong môi trường Ethernet LAN, tập hợp các thiết bị cùng nhận một broadcast bởi bất kỳ một thiết bị còn lại được gọi là một broadcast domain. Trên các switch không hỗ trợ VLAN, switch sẽ đẩy tất cả các broadcast ra tất cả các cổng, ngoại trừ cổng mà nó nhận frame. Kết quả là, tất cả các interface trên loại switch này là cùng broadcast domain. Nếu switch này kết nối đến các switch và các hub khác, các cổng trên switch này cũng sẽ trong cùng broadcast domain. Mỗi một cổng trên switch có thể chia cho một VLAN. Những cổng được chia sẽ cho cùng một VLAN thì chia sẽ broadcast. Cổng nào không thuộc cùng VLAN thì sẽ không chia sẽ broadcast. Những cải tiến của VLAN là làm giảm bớt broadcast và sự lãng phí băng thông.

Một VLAN đơn giản là một tập hợp của các cổng của switch nằm trong cùng broadcast domain. Các cổng có thể được nhóm vào các VLAN khác nhau trên từng switch và trên nhiều switch. Bằng cách tạo ra nhiều VLAN, các switch sẽ tạo ra nhiều broadcast domains. Khi đó, khi có một broadcast được gửi bởi một thiết bị nằm trong một VLAN sẽ được chuyển đến những thiết bị khác trong cùng VLAN,

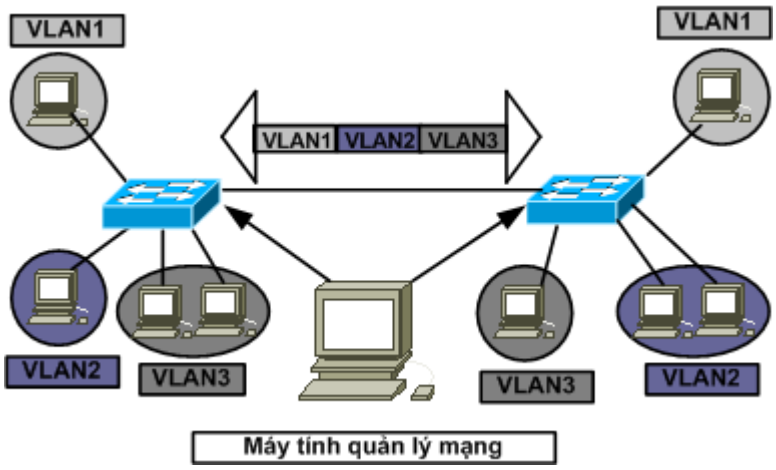
tuy nhiên broadcast sẽ không được forward đến các thiết bị trong VLAN khác. Có 2 phương thức để tạo lập VLAN là VLAN tĩnh (Static VLAN) và VLAN động (Dynamic VLAN).

Static VLAN

Phương thức này được ám chỉ như là port-base membership. Việc gán các cổng switch vào một VLAN là đã tạo một static VLAN. Giống như một thiết bị được kết nối vào mạng, nó tự động thừa nhận VLAN của cổng đó. Nếu user thay đổi các cổng và cần truy cập vào cùng một VLAN, thì người quản trị mạng cần phải khai báo cổng tới VLAN cho kết nối tới.

Dynamic VLAN

VLAN được tạo thông qua việc sử dụng các phần mềm như Ciscowork 2000. Với một VMPS (VLAN Management Policy Server) có thể đăng ký các cổng cuả switch vào các VLAN một cách tự động dựa trên địa chỉ MAC nguồn của thiết bị được nối vào cổng. Dynamic VLAN hiện thời tính đến thành viên của nó dựa trên địa chỉ MAC của thiết bị. Như mộ thiết bị trong mạng, nó truy vấn một cơ sở dữ liệu trên VMPS của các VLAN thành viên.



Trên cổng của switch được gán cho một VLAN cụ thể thì độc lập với người dùng hoặc hệ thống gắn với cổng đó. Khi người dùng gắn với cùng một phân đoạn mạng dùng chung, tất cả các người dùng đó cùng chia sẽ băng thông của phân đoạn mạng. Mỗi một người dùng được gắn vào môi trường chia sẽ, thì sẽ có ít băng thông sẵn có cho mỗi người dùng, bởi vì tất cả các người dùng đầu nằm trên một miền xung đột. Nếu chia sẽ trở nên quá lớn, xung đột có thể sảy ra quá mức và các trình ứng dụng có thể bị mất chất lượng.

Mỗi một cổng trên switch giống như một cổng của bridge và switch đơn giản là một bridge nhiều cổng.

End-to-End VLAN (VLAN đầu cuối)

Các End-to-end VLAN cho phép các thiết bị trong một nhóm sử dụng chung tài nguyên. Bao gồm các thông số như máy chủ lưu trữ, nhóm dự án và các phòng ban. Mục đích của các End-to-end VLAN là duy trì 80% thông lượng trên VLAN hiện thời. Một End-to-end VLAN có các đặc điểm sau:

Các người dùng được nhóm vào các VLAN độc lập về vị trí vật lý nhưng lại phụ thuộc vào nhóm chức năng hoặc nhóm đặc thù công việc.

Tất cả các người dùng trong một VLAN nên có cùng kiểu truyền dữ liệu 80/20 (80% băng thông cho VLAN hiên thời/ 20% băng thông cho các truy cập từ xa).

Như một người dùng di chuyển trong một khuôn viên mạng, VLAN dành cho người dùng đó không nên thay đổi.

Mỗi VLAN có những bảo mật riêng cho từng thành viên.

Như vậy, trong End-to-end VLAN, các người dùng sẽ được nhóm vào thành những nhóm dựa theo chức năng, theo nhóm dự án hoặc theo cách mà những người dùng đó sử dụng tài nguyên mạng.

Local VLAN (VLAN cục bộ)

Nhiều hệ thống mạng mà cần có sự di chuyển tới những nơi tập trung tài nguyên, End-to-end VLAn trở nên khó duy trì. Những người dùng yêu cầu sử dụng nhiều nguồn tài nguyên khác nhau, nhiều trong số đó không còn ở trong VLAN của chúng nữa. Bởi sự thay đổi về địa điểm và cách sử dụng tài nguyên. Các VLAN được tạo ra xung quanh các giới hạn địa lý hơn là giới hạn thông thường. Vị trí địa lý có thể rộng như toàn bộ một toà nhà, hoặc cũng có thể nhỏ như một switch trong một WiringCloset.

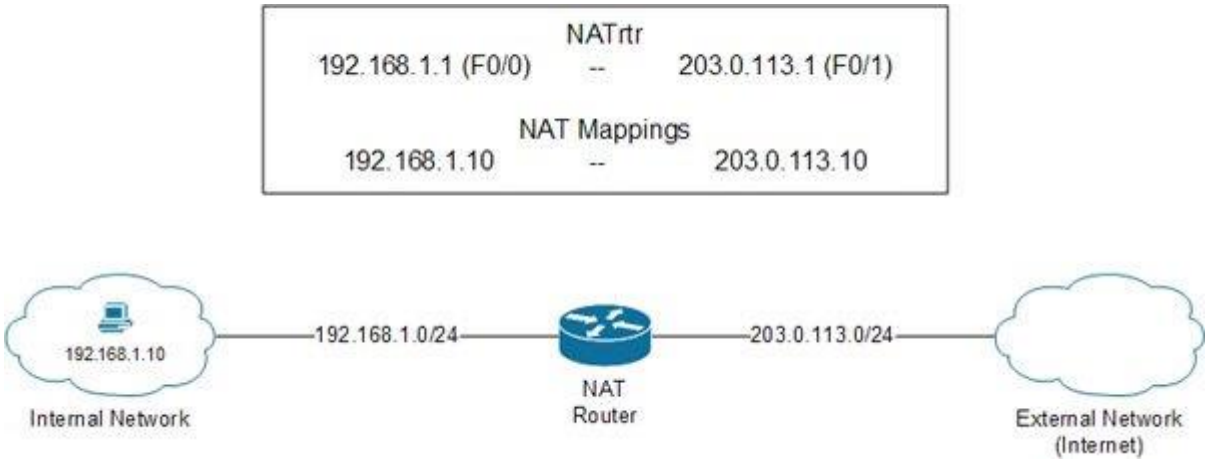
5.3. NAT

Hầu hết những người sở hữu một kết nối Internet hiện đại ngày nay đều phải sử dụng đến kỹ thuật NAT (Network Address Translation). NAT đã là một phần không thể thiếu khi triển khai mạng IP diện rộng do không gian địa chỉ IPv4 đã bắt đầu co hẹp. Về cơ bản, NAT cho phép một (hay nhiều) địa chỉ IP nội miền được ánh xạ với một (hay nhiều) địa chỉ IP ngoại miền. Điều này cho phép sử dụng dải địa chỉ IP riêng theo chuẩn RFC 1918 trên các mạng nội bộ trong khi chỉ sử dụng một hoặc một số ít các địa chỉ IP công cộng.

Bài viết sẽ trình bày những khái niệm cơ bản về NAT, các loại NAT và cách thức hoạt động của công nghệ này.

NAT

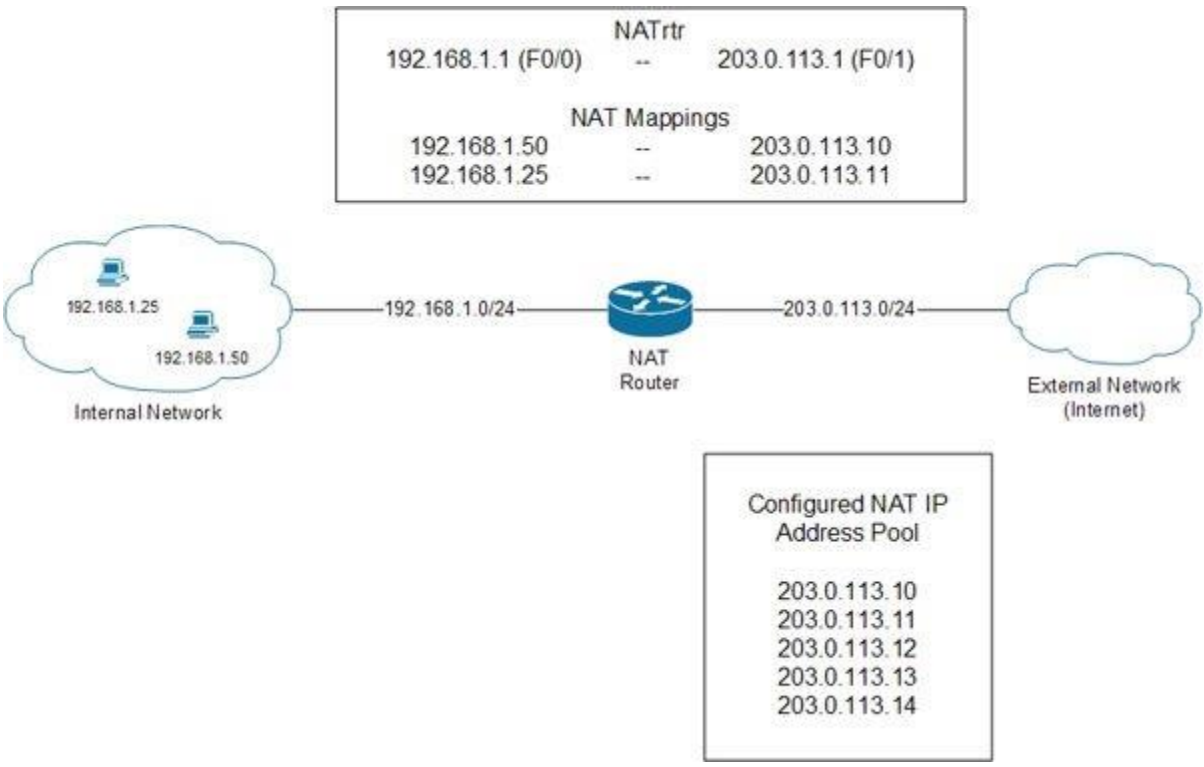
Có ba loại NAT khác nhau gồm có: NAT động, NAT tĩnh và NAT vượt tải (NAT overloaded). Với NAT tĩnh, một địa chỉ IP nội miền chỉ định sẽ được ánh xạ sang một địa chỉ IP chỉ định khác ngoài miền, như hình dưới đây.



Trong hình trên, một PC trong mạng nội bộ cần truyền thông tới một máy khác thuộc mạng ngoài, trong trường hợp này là Internet. Nhưng địa chỉ thuộc RFC 1918 không có khả năng định tuyến trên mạng Internet công cộng do vậy không được sử dụng làm địa chỉ nguồn hay đích.

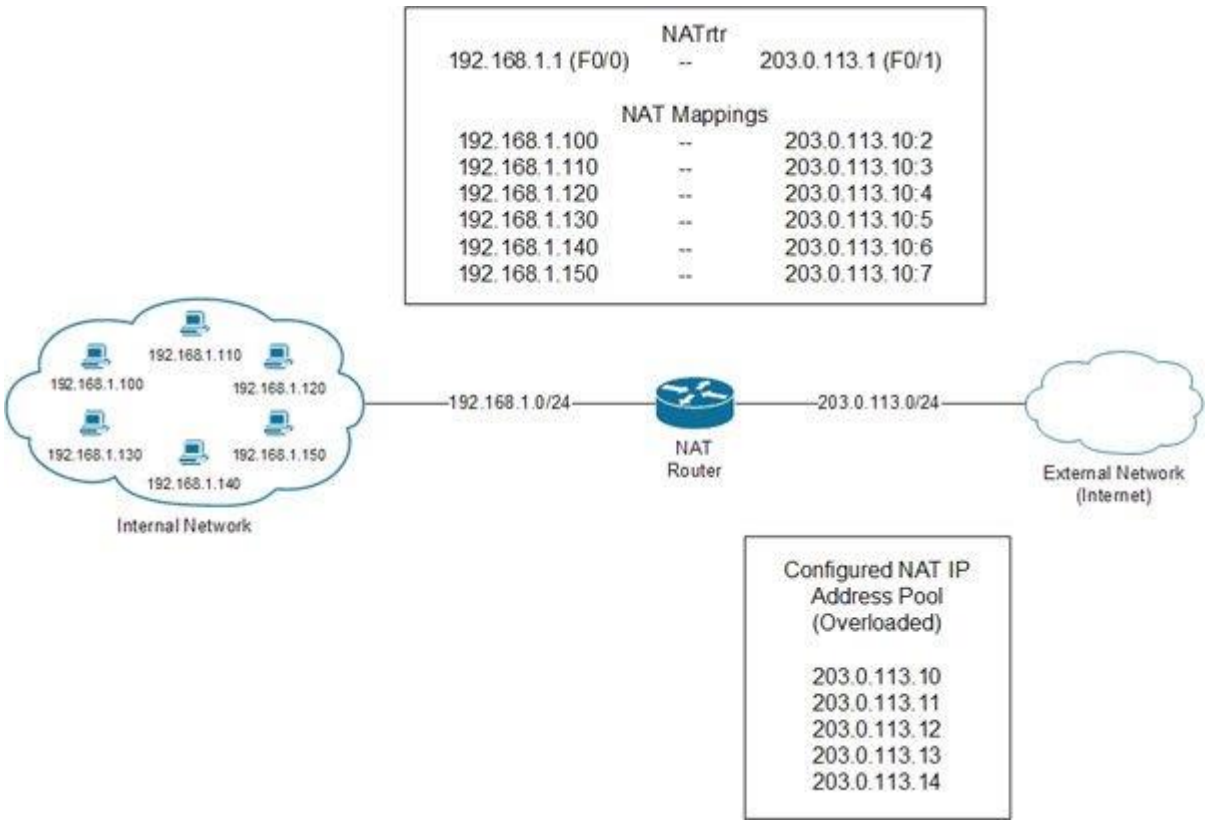
Để xử lý vấn đề này, NAT có thể được cấu hình tĩnh để nối địa chỉ nội bộ 192.168.1.10 với địa chỉ ngoài 203.0.113.10. Như vậy, với mạng ngoài, lưu lượng đến sẽ là từ địa chỉ 203.0.113.10 thay vì 192.168.1.10. Trong tình huống này, NAT sẽ coi địa chỉ IP 192.168.1.10 là địa chỉ cục bộ bên trong và địa chỉ được ánh xạ 203.0.113.10 là địa chỉ chung bên trong.

Với NAT động, Địa chỉ IP nội bộ sẽ tự động được khớp với một bộ các địa chỉ IP ngoài. Quá trình ánh xạ vẫn là giữa 1 địa chỉ nội bộ với một địa chỉ ngoài nhưng được diễn ra tự động.



Ở hình trên, hai PC trong mạng nội bộ cần truyền thông tới máy ở mạng ngoài, trong trường hợp này là Internet. NAT được cấu hình động để ánh xạ các địa chỉ nội bộ là 192.168.1.25 và 192.168.1.50 với những địa chỉ IP trong tập hợp địa chỉ đã cấu hình NAT. Trong hình, máy có địa chỉ 192.168.1.50 đã được ánh xạ đến địa chỉ 203.0.113.10 và máy có địa chỉ 192.168.1.25 được ánh xạ tới địa chỉ 203.0.113.11. Điều này có nghĩa là máy có địa chỉ 192.168.1.50 sẽ được khởi tạo lưu lượng ngoài trước.

Với NAT vượt tải (còn gọi là biên dịch địa chỉ cổng PAT), ánh xạ một một như NAT động và NAT tĩnh không được sử dụng. Thay vì một địa chỉ ngoài chỉ được gán cho 1 địa chỉ IP nội bộ thì giờ đây nó có thể được gán cho tất cả các máy nội bộ dựa trên số cổng (port number). Chỉ khi số lượng cổng khả dụng sử dụng bởi địa chỉ IP ngoài bị cạn kiệt thì một địa chỉ IP ngoài thứ hai mới được dùng đến với phương pháp tương tự.



Ở hình trên, có sáu máy khác nhau đang truy cập tới các máy thuộc mạng ngoài. NAT vượt tải được cấu hình với tập hợp địa chỉ trong dải 203.0.113.10 đến 203.0.113.14. Giả sử rằng lưu lượng qua NAT router một cách tuần tự thì mỗi loại lưu lượng sẽ được ánh xạ với một địa chỉ IP ngoài (trong trường hợp này là địa chỉ IP đầu tiên tron dải-203.0.113.10) và số cổng chỉ định.

Với mỗi ví dụ, NAT router được cấu hình sử dụng cùng địa chỉ IP là 192.168.1.1 trên giao diện Fast Ethernet 0/0 được đánh dấu là giao diện NAT nội và 203.0.113.1 trên giao diện FastEthernet 0/1, được đánh dấu là giao diện NAT ngoài.

5.4. Tunneling

Cơ sở hạ tầng mạng Internet hoạt động trên nền IPv4, hoạt động khá ổn định và

quy mô hết sức rộng lớn. Tận dụng khả năng này, các nhà thiết kế IPv6 đã đưa ra giải pháp thực hiện cơ chế Tunneling như sau: Automatic Tunneling và Configured Tunneling.

Sau đây là một số đặc điểm của các loại Tunneling và một số khái niệm liên

quan đến các kỹ thuật Tunneling:

- IPv4-only Node : Là một Host hay Router hoạt động trên nền IPv4, những

Host hoặc Router này không hiểu IPv6, các Host này chiếm phần lớn các thiết bị trên mạng Internet hiện nay. Các Node này còn được gọi là Node thuần IPv4.

- IPv6/IPv4 Node : Là các Node có khả năng thực hiện trên nền IPv4 hoặc IPv6. Đây chính là các Dual-stack Node.

- IPv6-only Node: là những Node chỉ có khả năng hoạt động trên nền IPv6,

không có khả năng hoạt động trên nền IPv4. Các Node này được gọi là Node thuần IPv6.

- IPv6 Node: Bao gồm những Node sau: Node thuần IPv6, Dual-stack Node

IPv6/IPv4.

- IPv4 Node: Bao gồm những Node sau: Node thuần IPv4, Dual-stack Node

IPv6/IPv4.

- IPv4-compatible IPv6 address: Là một địa chỉ IPv6, được gán cho các Node

đôi IPv6/IPv4 (định dạng địa chỉ này đã mô tả ở phần trên). Dạng địa chỉ này được sử dụng trong cơ chế Tunnel IPv6 trên nền IPv4 sẽ được mô tả

dưới đây.

- IPv6-only address: Là những địa chỉ IPv6 còn lại.

- IPv6-over-IPv4 Tunneling: Kỹ thuật này thực hiện việc đóng gói các

Datagram theo cấu trúc IPv6 vào phần dữ liệu của Datagram IPv4 để có thể mang gói tin IPv6 qua mạng IPv4. Ta gọi cơ chế này là Tunnel IPv6 trên nền IPv4.Có hai phương thức Tunnel như đã nói đến ở trên: Automatic Tunneling và

Configured Tunneling được định nghĩa như sau:

- Automatic Tunneling: Theo phương thức này, địa chỉ cuối cùng trong Tunnel

là địa chỉ IPv4-compatible IPv4.

- Configured Tunneling: Theo phương thức này, địa chỉ cuối cùng trong Tunnel được xác định nhờ thông tin cấu hình tại các nút thực hiện đóng, mở gói IPv6 thành gói IPV4 và ngược lại.

Cơ chế Tunneling được mô tả như sau: Các Node IPv6/IPv4 sẽ thực hiện đóng

gói các Datagram IPv6 vào thành phần dữ liệu trong Datagram IPv4 (phần tải của gói tin IPv4 truyền trên hạ tầng mạng là gói tin IPv6) và do đó, gói tin này có thể truyền qua trên nền IPv4.

Các kết nối có thể áp dụng cơ chế Tunneling là:

- Router-to-Router: Các Router IPv6/IPv4 kết nối với nhau bởi cơ sở hạ tầng mạng IPv4, do đó, có thể thực hiện chuyển các Datagram theo định dạng IPv6 trên nền IPv4. Trong trường hợp này, Tunnel trãi rộng từ điểm bắt đầu tới điểm kết thúc của đoạn mạng IPv4.
- Host-to Router: Một Dual-stack Host IPv6/IPv4 có thể thực hiện Tunnel IPv6 trên nền IPv4 để chuyển các gói tin tới các Router trung gian cũng được cấu hình là các Node đôi IPv6/IPv4. Trong trường hợp này, Tunnel trãi rộng trong phạm vi từ Host tới Router đó.
- Host-to-Host: Hai Host IPv6/IPv4 có thể truyền các Datagram theo định dạng IPv6 trên nền IPv4. Trong trường hợp này, cơ chế Tunnel trãi rộng từ điểm đầu đến điểm cuối.
- Router-to-Host: IPv6/IPv4 Router có thể dùng Tunnel kết nối với IPv6/IPv4 Host thông qua hạ tầng mạng IPv4.

Trong hai phương pháp đầu: Router-to-Router và Host-to Router, gói tin IPv6 được Tunneled vào Router và điểm cuối của đường hầm này là một Router, Router này có nhiệm vụ mở gói "IPv4" vừa ra khỏi đường hầm để tách ra gói IPv6 ban đầu, sau đó chuyển gói IPv6 vừa tách tới đích, địa chỉ IPv6 trong gói tin được đưa qua Tunnel không liên quan (không hỗ trợ) đến địa chỉ điểm cuối của Tunnel. Do đó, các thông tin này phải được cấu hình cố định trên Router hay Node thực hiện đóng gói.

Theo cơ chế xác định địa chỉ đầu cuối như vậy, điểm cuối của Tunnel phải được khai báo trước. Trường hợp này gọi là Configured Tunneling . Hai phương pháp còn lại, Host-to-Host và Router-to-Host gói IPv6/IPv4 được Tunneled từ Host hoặc Router đến đích là một Host. Trong trường hợp này địa chỉ đầu cuối của Tunnel và địa chỉ Host đích phải giống nhau. Nếu địa chỉ IPv6 dùng cho Node đầu cuối là IPv4-compatible IPv6, địa chỉ cuối của Tunnel có thể tự động tạo ra từ địa chỉ IPv6 đó. Vì vậy không cần khai báo các thông số cho Tunneling. Kỹ thuật này gọi là Automatic Tunneling.

Hai kỹ thuật Automatic Tunneling và Configured Tunneling có điểm khác nhau

cơ bản nhất chính là việc quyết định địa chỉ cuối của quá trình Tunneling, còn lại về cơ bản, hai cơ chế này giống nhau. Cụ thể như sau:

- Điểm khởi tạo Tunnel (điểm đóng gói tin) tạo một Header IPv4 đóng gói và

truyền gói tin vừa đóng gói.

- Node kết thúc của quá trình Tunnel (điểm mở gói tin) nhận được gói tin đóng gói, tách bỏ phần Header IPv4, sửa đổi một số trường của Header IPv6 và xử lý phần dữ liệu này như một gói tin IPv6.

- Node đóng gói cần duy trì các thông tin về trạng thái của mỗi quá trình Tunneling. Ví dụ tham số MTU để xử lý các gói tin IPv6 bắt đầu thực hiện

Tunneling. Vì số lượng các quá trình Tunneling có thể tăng lên một số lượng

khá lớn, trong khi đó các thông tin này thường lặp lại và do đó, có thể sử dụng kỹ thuật cache và được loại bỏ khi cần thiết.

6. Xác định rủi ro

6.1. Xác định tài nguyên

• Cấu hình không chuẩn và việc thiếu các bản vá lỗi làm tăng các mối nguy hiểm.

Các máy tính (MT) ở nhà do thiếu sự giám sát của các chuyên gia CNTT nên thường có cấu hình không phù hợp trong việc chia sẻ file hay in ấn, gây nên những nguy cơ như lộ thông tin quan trọng đối với bạn cùng phòng, vợ con. Những người làm việc từ xa thường không sử dụng hệ điều hành và các ứng dụng không được cập nhật mới nhất, ngay cả các PM diệt virus cũng không được cập nhật. Vì vậy các MT ở nhà thường dễ bị nhiễm virus và các chương trình phá hoại hơn các MT ở trong công ty. Việc phát hiện, làm sạch các MT này thường mất nhiều thời gian hơn. Do đó, MT của những người làm việc từ xa là một nguyên nhân tiềm tàng gây mất an toàn cho cả hệ thống mạng khi truy cập từ xa vào hệ thống.

• Mạng không dây (Wireless) không an toàn với cấu hình mặc định.

Một mối nguy hiểm đối với môi trường MT tại nhà chính là Wireless. Ngày nay, nhiều MT ở nhà được nối bằng mạng Wireless. Đa số các thiết bị Wireless thường được cấu hình mặc định và tính năng kiểm soát WEP (phương thức để mã hóa và xác thực trong kết nối Wireless) ở chế độ tắt, những người dùng thông thường thường quên hoặc không biết cách bật tính năng này lên. Chính vì vậy những người dùng khác có thể sử dụng như là một phương tiện để xâm nhập vào hệ thống bên trong, truy cập vào mục chia sẻ file. Nguy hiểm hơn nữa là những kẻ tấn công

giỏi vẫn có thể dễ dàng vượt qua rào cản WEP.

• Nguy cơ bị tấn công MT ở nhà.

Với các kết nối băng thông rộng, các kẻ tấn công có thể tiết kiệm thời gian để xâm nhập vào máy người dùng ở nhà. Trừ khi có các sản phẩm như tường lửa cá nhân được triển khai hợp lý, còn không thì các hoạt động dò đường, tìm cách xâm nhập của hacker sẽ không bị phát hiện trong thời gian dài. Những hacker này có thể khai thác các cổng được mở trên MT để ăn cắp tài nguyên hoặc phá hoại các hệ thống không được bảo vệ kết nối khác.

Ngoài ra, không thể không kể đến mối nguy hại từ những PM phá hoại (các loại virus, sâu MT) làm chậm hệ thống của người dùng, phá hoại file và các ứng dụng, làm tiêu tốn băng thông. Các loại sâu MT thường cài đặt một cửa hậu trên MT bị lây nhiễm để sau này những kẻ gửi thư rác thông qua đó gửi các email quảng cáo hoặc ăn trộm thông tin. Nguy hại hơn phải kể đến các PM gián điệp thường được đính kèm trong các PM chia sẻ, các bức ảnh hay file nhạc. Nếu không có các giải pháp bảo mật (BM) thích hợp, những kẻ tấn công có thể dùng loại PM này để truy cập đến các tài nguyên trong hệ thống thông qua các mạng riêng ảo (VPN) không được bảo vệ.

6.2. Đánh giá rủi ro

Để hạn chế các rủi ro khi làm việc từ xa, có thể áp dụng công nghệ mã hóa đường truyền (tạo đường hầm) theo chuẩn IPSec hoặc SSL (Secure Sockets Layer) từ người dùng tới tài nguyên của DN/tổ chức. Mỗi một chuẩn mã hóa có ưu nhược điểm khác nhau, chuẩn mã hóa IPSec độ ổn định cao, hỗ trợ các ứng dụng tốt nhưng đòi hỏi phải cài đặt và cấu hình rất phức tạp cho các máy trạm này trước khi kết nối. Trong khi đó mạng riêng ảo sử dụng công nghệ mã hóa SSL (gọi tắt là SSLVPN) cho phép kết nối từ bất cứ đâu có kết nối mạng và một trình duyệt web thông dụng, mà không cần cấu hình trên máy trạm khi kết nối tới tài nguyên của DN/tổ chức.

Hiện nay trên thị trường Aventail là một trong những hãng được đánh giá có giải pháp SSL VPN dễ dàng triển khai và tối ưu về công nghệ. Các công nghệ nổi bật của Aventail là:

• Bảo vệ tài nguyên hệ thống

Aventail được xây dựng như một cổng truy cập các tài nguyên, nó hạn chế tối đa các truy cập trực tiếp vào hệ thống, che giấu toàn bộ mô hình mạng (Topology) đối

với mạng bên ngoài, qua đó các hacker từ xa không có khả năng truy cập trực tiếp vào các tài nguyên, cũng như không có khả năng tấn công từ chối dịch vụ vào các tài nguyên của hệ thống. Aventail cũng hạn chế tối đa việc lợi dụng đường truyền để phát tán thư rác, các mã độc hại vào trong hệ thống mạng cũng như lợi dụng các tài nguyên này để tấn công các hệ thống khác.

• Xác thực mạnh các người dùng từ xa

Nhằm đảm bảo chỉ có người dùng hợp pháp mới có khả năng kết nối tới các tài nguyên của hệ thống, ngoài phương thức xác thực của mình, Aventail hỗ trợ các phương thức xác thực người dùng khác như SecurID, Certificate, Radius, AD... và các phương thức xác thực mạnh khác có khả năng tạo thành hệ thống xác thực qua N yếu tố, tùy thuộc vào lựa chọn của khách hàng, sẽ giúp cho khách hàng đảm bảo đúng người có quyền mới có thể khai thác tài nguyên của hệ thống.

• Mã hóa dữ liệu trên đường truyền với công nghệ SSL VPN

Công nghệ SSL VPN với các thuật toán mã hóa mạnh của Aventail cung cấp một phương thức kết nối mà các người dùng từ xa không cần cài đặt chương trình đặc biệt nào khi kết nối đến tài nguyên của tổ chức/DN. Điểm đặc biệt trong công nghệ SSL VPN của Aventail so với một số sản phẩm SSL VPN cùng loại là Aventail hỗ trợ mọi ứng dụng, tài nguyên trên giao thức chuẩn TCP.

• Chính sách điều khiển truy cập tới các tài nguyên

Aventail cho phép áp dụng các chính sách khác nhau đối với từng tài nguyên, đối với từng người dùng, thậm chí cho phép áp dụng chính sách theo cả độ an toàn của thiết bị/MT mà người dùng từ xa sử dụng để truy cập đến tài nguyên.

• Kiểm soát an ninh đối với thiết bị/MT của người dùng từ xa

Một trong những rủi ro đối với phương thức làm việc từ xa là các MT của người dùng không được đảm bảo an toàn. Giải pháp bảo vệ máy trạm (End Point Control) của Aventail có khả năng thiết lập chính sách an toàn cho các máy trạm bằng cách tích hợp chặt chẽ với tường lửa cá nhân và PM chống virus, đảm bảo chỉ những thiết bị người dùng cuối đã được bảo vệ đúng đắn mới được phép kết nối đến tài nguyên của hệ thống.

Riêng đối với các máy PDA và MT công cộng ở quán Café Internet, Aventail giới

hạn quyền truy cập đối với một số tài nguyên. Ví dụ, khi người dùng từ xa truy cập đến tài nguyên từ MT công cộng(không đảm bảo an toàn) sẽ chỉ được truy cập email, một số ứng dụng Web và không cho phép truy cập file hoặc dữ liệu nhạy cảm của DN. Ngoài ra, giải pháp của Aventail cung cấp nhiều tính năng BM cao hơn, ví dụ các máy từ xa sẽ được quét dọn để xóa các dữ liệu nhạy cảm đã tạo ra trong quá trình kết nối hoặc dữ liệu tải về sẽ được đưa vào một "kho mã hóa" tạm thời và chúng sẽ bị xóa khi phiên làm việc kết thúc.

6.3. Xác định mối đe dọa

Những tấn công trên web tiếp tục phát triển vì các hacker nhắm tới mục tiêu là thông tin về người dùng cuối; nền kinh tế ngầm tiếp tục trở thành mối đe doạ lớn…

Đây là những kết luận của Symantec trong bản báo cáo về các mối đe dọa bảo mật mạng (ISTR) thứ 14 của hãng, khẳng định rằng các hoạt động tấn công mạng trên thế giới tiếp tục phát triển ở mức kỷ lục trong năm 2008, chủ yếu nhắm tới những thông tin quan trọng từ máy tính của người dùng.

Theo bản báo cáo, Symantec đã tạo ra hơn 1,6 triệu mẫu chữ ký về các loại mã độc mới trong năm 2008, tương đương với hơn 60% tổng số mẫu chữ ký mà Symantec đã từng tạo ra từ trước đến nay - một phản ứng đối với sự tăng trưởng mạnh về số lượng cũng như sự phong phú, đa dạng của những mối đe doạ nguy hại mới.

Bản báo cáo cũng cho thấy duyệt web vẫn là một trong những nguyên nhân chủ đạo gây ra những phát tán và lây nhiễm virus trên mạng trong năm 2008. Hacker ngày nay tận dụng ngày càng nhiều những công cụ sinh mã độc hại khác nhau để phát triển và phát tán những mối đe doạ của chúng.

Nền kinh tế ngầm ngày càng hoạt động phức tạp

Dựa trên số liệu của Bản báo cáo về nền kinh tế ngầm mới nhất, Symantec cho biết có một nền kinh tế ngầm với cơ cấu tổ chức tinh vi chuyên buôn bán những thông tin quan trọng bị đánh cắp, đặc biệt là thông tin về thẻ tín dụng và thông tin về tài khoản ngân hàng.

Nền kinh tế ngầm này đang bùng nổ, một điều minh chứng là trong khi giá thành sản phẩm ở những thị trường hợp pháp đang suy giảm thì giá thành sản phẩm ở thế giới ngầm vẫn không đổi từ năm 2007 đến cuối năm 2008.

Báo cáo cũng cho thấy những kẻ viết mã độc luôn thay đổi để chống lại những nỗ lực ngăn chặn các hành vi của chúng. Chẳng hạn như, việc đánh sập 2 hệ thống hosting mạng ma (botnet) đặt tại Mỹ đã góp phần làm giảm đáng kể các hoạt động botnet chủ động kể từ tháng 9 đến tháng 11 năm 2008; tuy nhiên, những kẻ vận hành botnet đã tìm ra những địa chỉ Web hosting thay thế và sự lây nhiễm botnet lại nở rộ, trở lại ngưỡng trước khi bị đánh sập một cách nhanh chóng.

Ứng dụng web, nguồn gốc của lỗ hổng bảo mật

Theo Symantec, những nền tảng ứng dụng Web lại thường là những nguồn gốc của những lỗ hổng bảo mật, trong giai đoạn đánh giá của báo cáo.

Những sản phẩm phần mềm được xây dựng sẵn này được thiết kế nhằm giúp đơn giản hoá việc triển khai những Website mới và được sử dụng rộng rãi trên Internet. Nhiều trong số những nền tảng này không có chức năng bảo mật, và một hệ quả tất yếu là chúng tiềm ẩn rất nhiều lỗ hổng và trở nên rất dễ bị xâm hại bởi các tấn công mạng.

Trong số những lỗ hổng bảo mật được xác định trong năm 2008, có đến 63% là các ứng dụng web bị lây nhiễm, tăng so với con số 59% của năm 2007. Trong số 12.885 lỗ hổng về mã lệnh liên kết chéo của báo cáo năm 2008 thì chỉ có 3% (394 lỗ hổng) đã được khắc phục tại thời điểm báo cáo này được viết ra.

Báo cáo cũng chỉ ra rằng những tấn công trên Web phát sinh từ nhiều quốc gia trên thế giới mà trong đó Mỹ dẫn đầu (38%), sau đó là Trung Quốc (13%) và Ucraina (12%). Sáu trong số 10 quốc gia dẫn đầu về tấn công trên web là các nước trong khu vực Châu Âu, Trung Đông và Châu Phi, những quốc gia này có tỷ lệ tấn công trên web chiếm tới 45% so với con số toàn cầu, nhiều hơn các khu vực khác.

Lừa đảo qua mạng và nạn thư rác tiếp tục gia tăng

Báo cáo cho hay nạn lừa đảo qua mạng tiếp tục phát triển. Trong năm 2008, 55.389 máy chủ đặt website lừa đảo, tăng 66% so với con số 33.428 của năm 2007. Những vụ lừa đảo liên quan đến các dịch vụ tài chính chiếm tới 76% các vụ lừa đảo năm 2008, tăng mạnh so với con số 52% năm 2007.

Symantec cũng cho biết, số lượng thư rác trong thời gian trở lại đây lại tiếp tục tăng mạnh. Trong năm vừa qua, Symantec đã theo dõi sự tăng trưởng của thư rác là

192% trên toàn mạng Internet, con số này tăng từ 119.6 tỷ tin nhắn (năm 2007) lên tới 349.6 tỷ trong năm 2008. Năm 2008, các mạng botnet thực hiện việc phát tán tới khoảng 90% tất cả thư rác.

6.4. Các điểm yếu

Một số kỹ thuật kiểm tra điểm yếu về An toàn thông tin

Bài báo giới thiệu một số kỹ thuật kiểm tra, đánh giá các lỗ hổng về an toàn **thông tin trong các hệ thống CNTT của tổ chức. Đây là những công đoạn cần thiết để có thể phát hiện những đểm yếu và điều chỉnh các biện pháp khắc phục kịp thời để đảm bảo hệ thống hoạt động an toàn.**

6.4.1. Quét mạng

Phương pháp quét mạng liên quan đến việc quét các cổng (port) trên hệ thống mạng để xác định các thiết bị có lỗ hổng, dễ bị tin tặc lợi dụng tấn công vào hệ thống mạng hoặc các dịch vụ chạy trên các thiết bị đó. Ví dụ như: dịch vụ truyền file (FTP), dịch vụ truyền siêu văn bản (HTTP) và đặc biệt là các ứng dụng chạy một dịch vụ xác định như WU-FTPD, Internet Information Server (IIS), Apache chạy dịch vụ HTTP,.… Kết quả của phương pháp quét này là một danh sách toàn diện các máy tính đang hoạt động, các dịch vụ và các thiết bị khác trong hệ thống. Phương pháp quét các cổng (ví dụ công cụ nmap) sẽ xác định các máy tính đang hoạt động trên vùng địa chỉ quét. Sau đó, trên mỗi một máy tính, chương trình sẽ kiểm tra các cổng mở thuộc các giao thức TCP hoặc UDP để xác định các dịch vụ chạy trên thiết bị.

Nội dung cơ bản của phương pháp quét là xác định các máy tính hoạt động và các cổng mở của nó. Để thực hiện tốt mục tiêu của phương pháp này, nên quét mạng theo các tiêu chí sau: Kiểm tra quyền kết nối của các máy tính trong mạng; Xác định các lỗ hổng của dịch vụ; Kiểm tra sự sai lệch của tất cả các dịch vụ so với chính sách bảo mật; Chuẩn bị cho việc kiểm tra sự xâm nhập mạng; Hỗ trợ cấu hình cho hệ thống phát hiện xâm nhập; Thu thập bằng chứng về các sự xâm nhập....

Kết quả của quá trình quét mạng phải được lưu giữ lại để làm căn cứ khắc phục sự cố. Sau khi quét mạng cần làm một số việc: Ngắt và điều tra các kết nối không được phép; Vô hiệu hóa hoặc gỡ bỏ các dịch vụ không cần thiết hoặc có nhiều lỗ hổng bảo mật; Hạn chế quyền truy cập vào các dịch vụ có nhiều điểm yếu; Cấu hình firewall để hạn chế quyền truy cập từ bên ngoài các dịch vụ có lỗ hổng.

6.4.2. Quét lỗ hổng bảo mật

Phương pháp quét lỗ hổng bảo mật thực chất là việc quét các cổng ở mức độ cao

hơn. Ngoài việc xác định các máy tính hoạt động và các cổng mở, nó còn cung cấp thêm các thông tin về lỗ hổng của các máy tính đó. Phương pháp này cung cấp cho hệ thống và người quản trị mạng một công cụ để phát hiện các lỗ hổng trước khi kẻ tấn công có thể tiếp cận đến nó, bao gồm các khả năng sau: Xác định các máy tính hoạt động trên mạng; Xác định các dịch vụ (cổng) đang hoạt động trên mạng và các điểm yếu của chúng nếu có; Xác định các ứng dụng và đọc "biểu ngữ" được trả lời từ các ứng dụng; Xác định hệ điều hành; Xác định các lỗ hổng thông qua việc tìm hiểu hệ điều hành và các ứng dụng chạy trên nó; Xác định các thiết lập cấu hình sai; Kiểm tra việc tuân thủ sử dụng ứng dụng hoặc chính sách bảo mật; Thiết lập nền tảng cho việc kiểm tra sự xâm nhập.

Kết quả của quá trình quét lỗ hổng bảo mật phải được lưu giữ lại và làm căn cứ để tiến hành khắc phục các lỗ hổng nếu có. Một số biện pháp cần phải làm ngay sau khi quét lỗ hổng là: Nâng cấp hoặc vá lỗi hệ thống để giảm thiểu các nguy cơ từ lỗ hổng; Triển khai các biện pháp giảm nhẹ nguy cơ nếu như hệ thống chưa được vá lỗi; Cấu hình và nâng cấp thường xuyên chương trình quản lý; Giám sát và cảnh báo về lỗ hổng, thay đổi cấu hình hệ thống để giảm thiểu nguy cơ; Thay đổi các chính sách bảo mật, kiến trúc hệ thống hoặc các tài liệu khác để đảm bảo hoạt động ổn định cho hệ thống.

6.4.3. Phá mật khẩu

Chương trình phá mật khẩu được sử dụng để xác định các mật khẩu yếu. Mật khẩu được lưu trữ và truyền đi dưới dạng mã hóa "băm". Khi người dùng đăng nhập vào hệ thống, hệ thống sẽ tạo ra dãy mã hóa băm từ mật khẩu đăng nhập và so sánh với dãy mã hóa băm đã được lưu. Nếu chúng trùng nhau tức là người dùng đã được xác thực.

Trong suốt quá trình thâm nhập hoặc tấn công, việc phá mật khẩu đòi hỏi phải lấy được dãy mã hóa băm của mật khẩu. Việc chặn bắt này xảy ra khi dãy mã hóa của mật khẩu truyền đi trên mạng hoặc được lấy từ hệ thống mục tiêu. Khi đã lấy được dãy băm của mật khẩu, chương trình sẽ nhanh chóng tạo ra các dãy băm cho đến khi trùng với dãy băm của mật khẩu đã nhận được. Phương pháp nhanh nhất của cách này là sử dụng bộ từ điển tấn công gồm rất nhiều từ phổ biến trên thế giới. Phương pháp mạnh nhất để phá mật khẩu là chương trình "tấn công tổng lực", tức là chương trình sẽ tấn công tất cả các mật khẩu có thể có.

Sau đây là một số phương pháp có thể sử dụng để giảm thiểu khả năng phá mật khẩu của kẻ tấn công:

- Thay đổi chính sách để giảm tỉ lệ mật khẩu bị phá hoặc thay thế phương pháp xác thực (ví dụ sử dụng token key).
- Phổ biến với người sử dụng về những tác hại của mật khẩu yếu. Nếu người dùng vẫn sử dụng mật khẩu yếu thì người quản trị nên áp dụng các biện pháp bổ sung để đảm bảo.

6.4.4. Kiểm tra file log

Các file log trên hệ thống bao gồm firewall log, IDS log, server log hoặc bất kỳ một file nào ghi lại quá trình kiểm tra dữ liệu trên hệ thống. Việc kiểm tra các file log và phân tích chúng sẽ cho biết các hoạt động đang diễn ra trên hệ thống, để có

thể so sánh với mục đích và nội dung của chính sách bảo mật. Vì thế, việc kiểm tra này sẽ xác định hệ thống có vận hành theo đúng chính sách bảo mật hay không. Ví dụ, khi ta đặt một hệ thống phát hiện xâm nhập (IDS) đằng sau tường lửa thì file log của nó sẽ được sử dụng để kiểm tra các yêu cầu dịch vụ và các giao dịch được tường lửa cấp phép. Nếu như trên file log của IDS này ghi lại các hoạt động không được phép, điều đó chứng tỏ tường lửa đã bị vượt qua và hệ thống mạng đã mất an toàn.
Nên định kỳ cho việc kiểm tra file log, trừ những trường hợp yêu cầu kiểm tra do việc nâng cấp hệ thống. Nếu hệ thống không được cấu hình theo đúng chính sách bảo mật thì có thể thực hiện những việc sau: Gỡ bỏ các dịch vụ có lỗ hổng nếu chúng không cần thiết; Cấu hình lại hệ thống; Thay đổi chính sách bảo mật của tường lửa để hạn chế quyền truy cập vào các hệ thống hoặc dịch vụ có lỗ hổng.

6.4.5. Kiểm tra sự toàn vẹn
Kiểm tra sự toàn vẹn của một file là tạo và lưu trữ một biến phát hiện lỗi checksum cho mọi file được bảo vệ và thiết lập một cơ sở dữ liệu của biến checksum đó. Phương pháp này cung cấp một công cụ cho quản trị hệ thống nhận ra sự thay đổi của các file, đặc biệt là sự thay đổi trái phép. Các biến checksum lưu trữ nên được tính toán lại thường xuyên để so sánh với giá trị hiện tại được lưu trữ, sau đó xác định có sự thay đổi file hay không. Chức năng kiểm tra sự toàn vẹn của file thường được tích hợp vào trong hệ thống phát hiện xâm nhập trên máy chủ thương mại. Phương pháp kiểm tra sự toàn vẹn là một công cụ hữu ích mà không đòi hỏi sự can thiệp của con người ở mức độ cao, nhưng nó cần phải thực hiện một cách thận trọng để đảm bảo tính hiệu quả.
Một số công cụ kiểm tra sự toàn vẹn của dữ liệu như Aide, LANGuard, Tripwire,....

6.4.6. Phát hiện virus
Mọi hệ thống mạng đều có nguy cơ nhiễm virus, trojan, sâu nếu như chúng kết nối với mạng Internet hoặc sử dụng USB, phần mềm miễn phí.
Có hai dạng chương trình diệt virus chính là chương trình được cài đặt trên hạ tầng mạng và chương trình cài đặt trên máy người sử dụng. Mỗi loại có những ưu điểm và nhược điểm riêng, nhưng với những hệ thống yêu cầu bảo mật cao thì nên sử dụng cả hai loại chương trình diệt virus đó.

6.4.7. Kiểm tra mạng không dây
Giao thức mạng không dây phổ biến nhất là 802.11b có nhiều lỗi nghiêm trọng khi sử dụng công cụ mã hóa WEP, bởi vì ở chế độ mặc định nó được cấu hình không an toàn.
Mỗi một hệ thống mạng không dây nên được kiểm tra định kỳ để tìm ra các kết nối trái phép hoặc các cấu hình yếu, đồng thời cũng phải kiểm tra các tín hiệu của mạng không dây lân cận. Một số phần mềm kiểm tra sự an toàn của hệ thống mạng không dây như Aerosol, AirSnort, Kismet, Sniffer Wireless,....
6.4.8. Thâm nhập thử nghiệm
Đây là việc kiểm tra an toàn của hệ thống bằng cách phá vỡ các tính năng an toàn

của chúng dựa trên các hiểu biết về thiết kế và hoạt động của hệ thống. Mục đích là để xác định các phương pháp tiếp cận hệ thống thông qua các công cụ và kỹ thuật cơ bản của kẻ tấn công. Việc thâm nhập phải được tiến hành sau khi khảo sát hệ thống một cách cẩn thận, thông báo cho toàn hệ thống và lập kế hoạch thâm nhập đầy đủ.
Việc thử nghiệm thâm nhập chính là tạo ra một mô phỏng cuộc tấn công vào hệ thống, nên có thể bị pháp luật hoặc chính sách bảo mật ngăn cấm. Do đó, trước khi thực hiện phải được sự cho phép và chỉ nên thực hiện như sau: Thực hiện trên một địa chỉ hoặc một dải địa chỉ cụ thể; Không thực hiện trên một số máy tính bị ngăn cấm; Dùng một số các kỹ thuật thâm nhập cho phép; Xác định rõ thời gian thực hiện việc thâm nhập; Xác định khoảng thời gian hữu hạn cho việc thâm nhập; Xác định rõ địa chỉ IP từ máy sẽ thực hiện thâm nhập để người quản trị có thể phân biệt cuộc tấn công thử nghiệm với các cuộc tấn công thực sự khác; Xử lý các thông tin được thu thập bởi đội thử nghiệm thâm nhập.

Như vậy, việc kiểm tra an toàn của hệ thống thông tin chính là hoạt động tìm kiếm các lỗ hổng bảo mật sau đó khắc phục các điểm yếu đó. Thông thường, nhiều phương pháp kiểm tra sẽ được kết hợp cùng lúc để đánh giá một cách toàn diện về tình trạng bảo đảm an toàn của mạng. Ví dụ, để kiểm tra sự thâm nhập mạng thì kết hợp việc quét mạng và quét lỗ hổng để xác định các máy tính dễ bị tấn công và các dịch vụ có thể là mục tiêu của sự tấn công sau này. Một số phương pháp quét lỗ hổng bảo mật lại cần đi kèm với phương pháp phá mật khẩu và không một phương pháp nào có thể cung cấp một bức tranh toàn diện về mạng và tình trạng bảo mật của chúng.

Bài 2: Những điểm yếu và phương pháp tấn công vào hệ thống

Mã bài: MD22-2

Giới thiệu: Bài 2 trình bày những điểm yếu và phương pháp tấn công vào hệ thống

Mục tiêu:

- Trình bày các kiểu tấn công vào hệ thống thường gặp;
- Trình bày các loại mã độc hại tác động đến hệ thống;
- Kiểm tra truy cập vào hệ thống;
- Nghiêm túc, khoa học, chính xác, cẩn thận.

Nội dung chính:

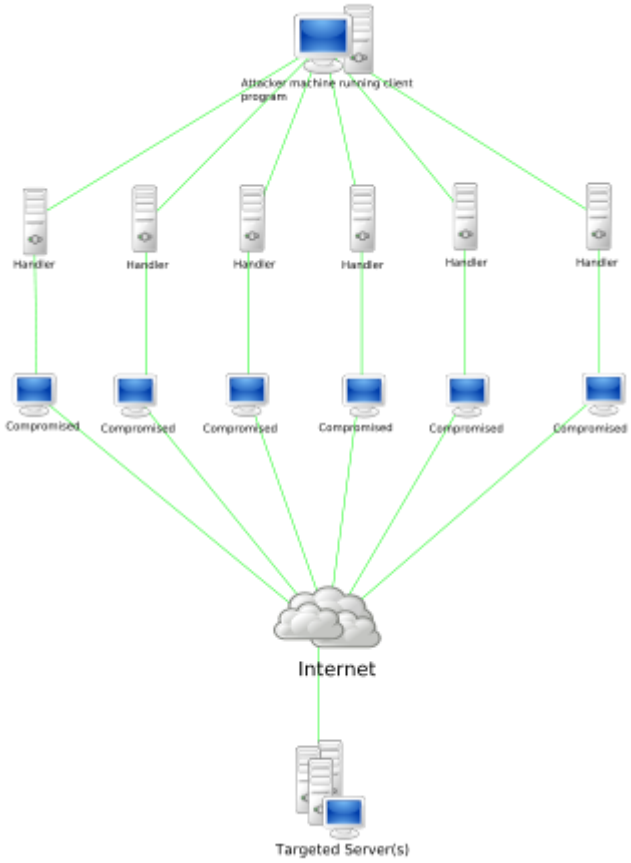
1. Các kiểu tấn công

1.1. DOS/DDOS – từ chối dịch vụ

Một **cuộc tấn công từ chối dịch vụ** (**tấn công DoS** - viết tắt của **Denial of Service**) hay **tấn công từ chối dịch vụ phân tán** (**tấn công DDoS** - viết tắt của **Distributed Denial of Service**) là một nỗ lực làm cho những người dùng không thể sử dụng tài nguyên của một máy tính. Mặc dù phương tiện để tiến hành, động cơ, mục tiêu của tấn công từ chối dịch vụ có thể khác nhau, nhưng nói chung nó gồm có sự phối hợp, sự cố gắng ác ý của một người hay nhiều người để một trang, hay hệ thống mạng không thể sử dụng, làm gián đoạn, hoặc làm cho hệ thống đó chậm đi một cách đáng kể với người dùng bình thường, bằng cách làm quá tải tài nguyên của hệ thống. Thủ phạm tấn công từ chối dịch vụ thường nhắm vào các trang mạng hay server tiêu biểu như ngân hàng, cổng thanh toán thẻ tín dụng và thậm chí DNS root servers.

Một phương thức tấn công phổ biến kéo theo sự bão hoà máy mục tiêu với các yêu cầu liên lạc bên ngoài, đến mức nó không thể đáp ứng giao thông hợp pháp, hoặc đáp ứng quá chậm. Trong điều kiện chung, các cuộc tấn công DoS được bổ sung bởi ép máy mục tiêu khởi động lại hoặc tiêu thụ hết tài nguyên của nó đến mức nó không cung cấp dịch vụ, hoặc làm tắc nghẽn liên lạc giữa người sử dụng và nạn nhân.

Tấn công từ chối dịch vụ là sự vi phạm chính sách sử dụng internet của IAB (Internet Architecture Board) và những người tấn công hiển nhiên vi phạm luật dân sự.



1.2. Back Door – cửa sau

Sau đây là 12 backdoor được đánh giá là "xảo quyệt" nhất trong lịch sử máy tính. Những loại mã độc "cửa hậu này khiến nhiều chuyên gia giỏi nhất cũng khó biết được chúng làm gì trên máy tính của nạn nhân và ai là kẻ điều khiển.

Trước hết, bạn cần biết backdoor là gì? Đây là khái niệm để chỉ một loại Trojan, sau khi được cài đặt vào máy nạn nhân sẽ tự mở ra một cổng dịch vụ cho phép kẻ tấn công (hacker) có thể kết nối từ xa tới máy nạn nhân, từ đó nó sẽ nhận và thực

hiện lệnh mà kẻ tấn công đưa ra.
Thông thường, việc xác định những phần mềm đang sử dụng có được an toàn hay không vốn rất khó khăn, thì để tìm và phát hiện ra các Trojan "cửa hậu" lại là vấn đề nan giải gấp bội. Việc phát hiện ra những backdoor vừa nguy hiểm với phương thức hoạt động rất tinh tế như các loại sau đây cũng không phải là vấn đề đơn giản.

12. Back Orifice

Được xem là loại backdoor đầu tiên trong lịch sử, Back Orifice đã khiến cho thế giới phải có một cái nhìn mới, rộng lớn hơn về những mối nguy hiểm của backdoor. Được tạo ra vào năm 1998 bởi một nhóm có tên Cult of the Dead Cow (Tín đồ của Bò chết) gồm những hacker khét tiếng. Back Orifice giúp những tin tặc này có thể kiểm soát và điều khiển từ xa qua mạng với cổng xâm nhập là 31337, hoạt động trên Microsoft BackOffice Server – tiền thân của Windows Small Business Server.

Back Orifice sau đó được đưa ra để chứng minh cho những lo ngại về vấn đề bảo mật trên Windows 98. Hệ điều hành này bị các hacker khai thác nhiều trong tính năng ẩn người dùng để phát tán mã độc.

Cũng từ khi backdoor Back Orifice ra đời, khái niệm Trojan được ra đời để chỉ những chương trình máy tính hoạt động bí mật nhằm phá hoại, gây tổn hại máy tính.

11.DSLBackdoor

Cuối năm 2013, một số bộ định tuyến sử dụng phần cứng của Sercomm như Linksys, Netgear, Cisco và Diamond bị phát hiện ra có một backdoor bí mật của nhà sản xuất đang gia tăng tại cổng 32764. Backdoor này cho phép kẻ tấn công gửi các lệnh đến những bộ định tuyến theo cổng TCP 32764 từ một dòng lệnh shell mà không cần bất cứ sự xác thực nào của quản trị mạng. Eloi Vanderbeken, một Reverse-Engneer (người chuyên dịch ngược phần mềm) người Pháp đã phát hiện

ra backdoor này và nhận thấy rằng mặc dù lỗ hổng này đã được vá trong phiên bản Firmware mới nhất, tuy nhiên Sercomm đã cài thêm một backdoor tương tự bằng một cách khác.

Một bản vá sau đó được tung ra vào tháng 4/2014 để khắc phục vấn đề này. Tuy vậy, đây cũng chỉ là một thao tác nhằm ẩn truy cập vào cổng 32764 và phải đợi có một gói cập nhật đặc biệt mới tìm ra cách trị được backdoor TCP 32764. Hiện vẫn chưa có một bản vá chính thức hoàn chỉnh nào cho backdoor mới được phát hiện này.

10.Backdoor mã hoá toàn bộ ổ đĩa dữ liệu

Đây là một đại diện cho một loại "không phải backdoor, nhưng là một tính năng" (not a backdoor, but a feature). PGP Whole Disk Encryption này hiện đã thuộc về hãng bảo mật Symantec. Công cụ này giúp tạo ra một mật khẩu vào các tiến trình lúc khởi động cho ổ đĩa được mã hoá. Mặc định mật khẩu sẽ không còn hiệu lực ngay trong lần đầu sử dụng. Lần đầu tiên về loại backdoor này được tìm thấy vào năm 2007, khi đó những sản phẩm mã hoá toàn ổ đĩa lưu trữ của PGP cũng có chức năng tương tự. Tuy vậy, không có bất cứ tài liệu nào được công bố là tiện ích này có một "tính năng" đáng sợ như vậy.

9. Backdoor ẩn trong các plug-in lậu của WordPress

WordPress hiện là một trong những blog nổi tiếng với những chức năng và hệ thống quản trị nội dung mạnh mẽ. Những trong hồ sơ về bảo mật của blog này thì có nhiều sự cố ngoài mong đợi của người sử dụng. Trong đó đáng sợ nhất là hacker đã lợi dụng những sơ hở trong việc quản lý các tiện ích cài thêm cho blog để thêm backdoor vào trang WordPress. Tuy nhiên, hành vi này không phải ai cũng phát hiện ra, kể cả những chuyên gia về WordPress.

8. Backdoor trong các plug-in của Joomla

Không chỉ có WordPress chịu ảnh hưởng của cách thức tấn công qua hệ thống quản trị nội dung (CMS – Content Management System) mà cả Joomla – một tiện ích CMS mã nguồn mở cũng là nạn nhân. Hệ thống quản trị nội dung Joomla được viết bằng ngôn ngữ PHP và kết nối tới cơ sở dữ liệu MySQL được tin tặc lợi dụng những sơ hở trong cách quản lý và cài đặt các tiện ích để tấn công (nhất là các plug-in miễn phí).

Các cuộc tấn công nhờ backdoor mở đường này thường là bước đệm để tội phạm mạng tấn công vào trang web và đánh sập nó. Việc này khiến cho cả những người làm web "tay mơ" lẫn các lập trình viên chuyên nghiệp làm việc với mã nguồn Joomla phải đắn đo và cẩn thận hơn nhiều trước khi cài thêm một plug-in cho trang web của mình.

7. Backdoor ProFTPD

ProFTPD, một chuẩn FTP Server mở được sử dụng rộng rãi đã từng là mục tiêu của các cuộc tấn công với backdoor. Quay trở lại năm 2010, những kẻ tấn công đã truy cập vào bộ mã nguồn của máy chủ hosting (không gian trên máy chủ có cài dịch vụ Internet như ftp, www… để chứa nội dung trang web hay dữ liệu). Sau đó, chúng thêm những đoạn mã để giúp cho kẻ tấn công truy cập vào tận gốc của máy chủ FTP bằng cách gửi lệnh HELP ACIDBITCHEZ. Mục tiêu cuối cùng là tin tặc sẽ sử dụng phương thức khai thác zero-day trong ProFTPD của mình để đột nhập vào các trang web và phát tán nhiều loại mã độc hại.

6. "Cửa hậu" Borland Interbase

Từ năm 1994 đến 2001, phiên bản Borland (sau này là Inprise) Interbase phiên bản từ phiên bản 4.0 đến 6.0 chứa một mã "cửa hậu" cực độc hại (hard-coded backdoor). Điều đáng nói là mã này được thêm vào bởi các kỹ sư của Borland.

Backdoor này có thể truy cập qua kết nối mạng với cổng 3050, một khi người dùng đăng nhập với công cụ này thì hacker có thể toàn quyền truy cập các cơ sở dữ liệu của Interbase.
Có một chi tiết thú vị là thông tin đăng nhập để mở cửa cho backdoor rất độc đáo với username là politically (chính trị) và mật khẩu là correct (chính xác).

InterBase
Cross-platform embedded database

5. Backdoor có trên cả Linux

Vào năm 2003, một kẻ nặc danh đã có gắng chèn một backdoor rất xảo quyệt vào mã nguồn của nhân Linux. Mã này được viết ra với vẻ ngoài không có bất cứ dấu hiệu nào của một backdoor, từ đó kẻ đột nhập vào máy chủ có thể thêm vào mã nguồn nhân của hệ điều hành.

Hai dòng mã thực tế đã bị thay đổi, nếu lướt qua thì không dễ gì phát hiện ra. Về lý thuyết, sự thay đổi này có thể giúp kẻ tấn công có được quyền quản trị trên máy. May mắn là backdoor này đã kịp thời bị phát hiện bởi một tiện ích kiểm soát mã độc.

4. Mã cửa sau tcpdump

Một năm trước khi kẻ nặc danh cố gắng đưa backdoor vào nhân Linux thì cũng có một tin tặc khác tìm cách đưa backdoor vào tiện ích tcpdump trên Linux (và cả Unix).

```
13:08:05.737768 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1221 > dsl-usw-cust
.nop,timestamp 1247771 114849487> (DF)
13:08:07.467571 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-1
<nop,nop,timestamp 114849637 1247771> (DF)
13:08:07.707634 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-1
<nop,nop,timestamp 114849637 1247771> (DF)
13:08:07.707922 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1221 > dsl-usw-cust
.nop,timestamp 1247968 114849637> (DF)
13:08:08.057841 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1045 > ns.de.ibm.ne
13:08:08.747598 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-1
<nop,nop,timestamp 114849813 1247968> (DF)
13:08:08.847870 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-1
<nop,nop,timestamp 114849813 1247968> (DF)
13:08:08.848063 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1221 > dsl-usw-cust
.nop,timestamp 1248082 114849813> (DF)
13:08:08.907566 ppp0 < ns.de.ibm.net.domain > slip139-92-26-177.ist.tr.ibm.
TR fingerless.or (199)
13:08:09.151742 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1221 > dsl-usw-cust
.nop,timestamp 1248112 114849813> (DF)
13:08:10.137603 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-1
p,nop,timestamp 114849967 1248112> (DF)
13:09:01.984210 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1222 > dsl-usw-cust
mss 1460,sackOK,timestamp 1253395 0,nop,wscale 0> (DF)
13:09:03.097569 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-1
7286 win 32120 <mss 1460,sackOK,timestamp 114855252 1253395,nop,wscale 0> (
13:09:03.098197 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1222 > dsl-usw-cust
```

Backdoor này có cơ chế hoạt động rõ ràng và dễ phát hiện hơn so với "cửa hậu" tấn công nhân Linux sau này. Mã độc này sẽ bổ sung một cơ chế ra lệnh và kiểm soát (command and control) để tiện ích tcpdump có thể hoạt động trên cổng 1963. Tương tự như backdoor tấn công Linux, âm mưu này cũng nhanh chóng bị phát hiện và tiêu diệt tận gốc ngay sau đó.

3. Backdoor phần cứng TAO của NSA

Tiết lộ gần đây cho biết, nhóm Tailored Access Operations (TAO – Điệp vụ Truy cập Hoàn hảo) của NSA (Cơ quan An ninh Quốc gia Mỹ) có thể can thiệp vào các đơn hàng thiết bị điện tử và cài đặt các phần cứng, phần mềm theo dõi trước khi các thiết bị này đến tay người mua. Các phần cứng được giao đến các nước khác sẽ bị thêm các backdoor vào firmware để phục vụ cho việc nghe trộm. Bên cạnh các thiết bị mạng, NSA cũng tạo ra những phần mềm giám sát được cài trong firmware của nhiều dòng máy tính, thậm chí cả những thiết bị ngoại vi – linh kiện như ổ cứng lưu trữ. Nếu người dùng thực hiện

Cụ thể, theo một tờ báo của Đức, NSA có thể cài phần mềm, linh kiện gián điệp lên đủ loại thiết bị từ thiết bị mạng của Huawei cho tới Cisco, các hãng ổ cứng tên tuổi như Seagate, Western Digital… Một vài linh kiện theo dõi cho phép NSA theo dõi "vĩnh viễn" nạn nhân, bởi chúng được thiết kế để tiếp tục hoạt động ngay cả khi người dùng format ổ cứng hoặc cập nhật firmware.

2. Windows _NSAKEY backdoor

Theo phát biểu của NSA, vào năm 1999, các nhà nghiên cứu đã phát hiện ra một biến có tên _NSAKEY đi kèm với một khoá công khai (public key) 1.024-bit trong phiên bản Windows NT 4 Service Pack 5. Nhiều nhận định cho rằng Microsoft đã bí mật cũng cấp cho NSA backdoor này để truy cập những dữ liệu đã được mã hoá trên Windows. Tuy nhiên, Microsoft đã phủ nhận cáo buộc này và khẳng định không có chuyện cấu kết với NSA để đặt backdoor. Nhưng vẫn có nhiều chuyên gia nghi ngờ có điều không rõ ràng trong chuyện này.

1. Dual Elliptic Curve backdoor

Lại liên quan đến NSA, theo tiết lộ của Reuters, NSA đã trả cho RSA 10 triệu USD để công ty này thiết kế hệ thống mặc định trong phần mềm bảo mật được sử dụng rộng rãi trên Internet và trong các chương trình an ninh máy tính. Hệ thống này có tên Dual Elliptic Curve - là bộ tạo số ngẫu nhiên dựa trên đường cong elip nhưng nó được kín đáo tạo một số lỗi hay "cửa hậu" cho phép NSA giải mã.

Về lý thuyết, các thông điệp sẽ được mã hoá với chuẩn Dual_EC_DRBG (Dual Elliptic Curve Deterministic Random Bit Generator) – một tiêu chuẩn đã được phê chuẩn bởi NIST. Sau khi Edward Snowden làm rò rỉ bản ghi nhớ nội bộ NSA đã đưa việc này ra ánh sáng.

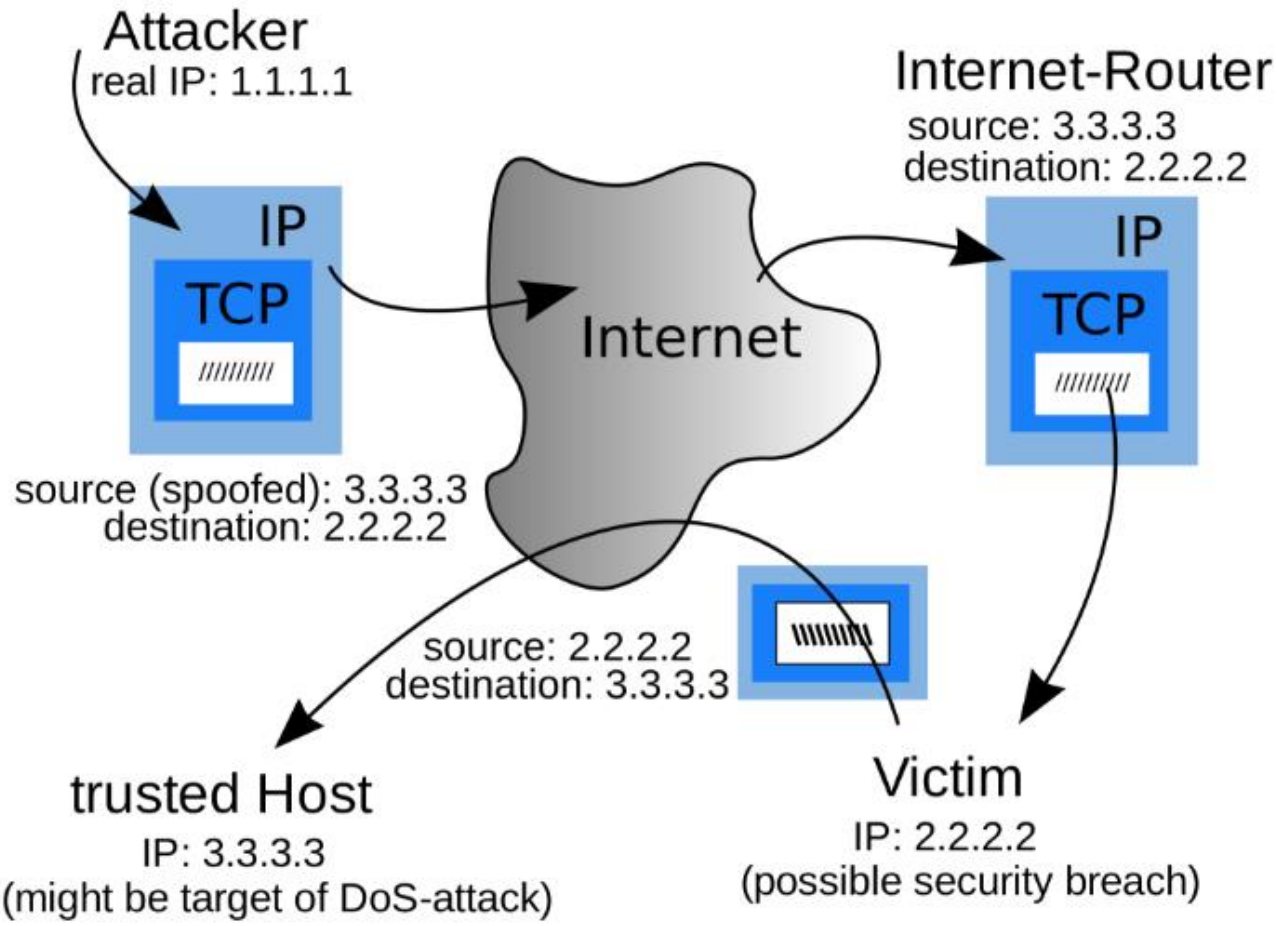
Sau khi "cửa sau" của Dual Elliptic Curve bị phát giác, RSA đã nhanh chóng lên tiếng khuyến cáo khách hàng ngưng sử dụng hệ thống này. Tuy nhiên, câu chuyện về 10 triệu USD mà NSA hối lộ cho RSA đã gây bất ngờ cho các chuyên gia an ninh máy tính trên thế giới. Bởi vì, RSA là công ty bảo mật lâu đời của Mỹ có danh tiếng bảo vệ quyền riêng tư cho người dân và từng chống lại nỗ lực của NSA vào thập niên 90 nhằm thuyết phục Chính phủ Mỹ cho phép sử dụng con chip Clipper để cài vào các điện thoại và máy tính giúp cho các cơ quan chính quyền dễ giải mã tín hiệu khi được luật pháp cho phép.

1.3. Spoofing – giả mạo

Khi một máy tính ở bên ngoài hệ thống mạng của bạn "giả vờ" là một máy tính đáng tin cậy trong hệ thống, hành động này của kẻ tấn công được gọi là IP Spoofing.

Để truy cập vào hệ thống mạng của bạn, máy tính bên ngoài phải "giành" được một địa chỉ IP tin cậy trên hệ thống mạng. Vì vậy kẻ tấn công phải sử dụng một địa chỉ IP nằm trong phạm vi hệ thống mạng của bạn. Hoặc cách khác là kẻ tấn công có thể sử dụng một địa chỉ IP bên ngoài nhưng đáng tin cậy trên hệ thống mạng của bạn.

Các địa chỉ IP có thể được hệ thống tin tưởng là bởi vì các địa chỉ này có các đặc quyền đặc biệt trên các nguồn tài nguyên quan trọng trên hệ thống mạng.



Một số cách tấn công khác nhau của IP Spoofing?

- Tấn công dữ liệu hoặc thiết lập các lệnh tồn tại trên dòng dữ liệu đang được chuyển đổi giữa một client và ứng dụng Server (máy chủ).

- Tấn công dữ liệu hoặc các lệnh trong kết nối mạng ngang hàng (peer-to-peer).

Tuy nhiên kẻ tấn công cũng phải thay đổi bảng định tuyến (routing table) trên hệ thống mạng. Việc thay đổi bảng định tuyến (routing table) trên hệ thống mạng cho phép kẻ tấn công có được thông tin liên lạc 2 chiều . Với mục đích này, kẻ tấn công "nhắm" vào tất cả bảng định tuyến (routing table) thành địa chỉ IP giả mạo.

Một khi bảng định tuyến (routing table) đã thay đổi, những kẻ tấn công bắt đầu nhận tất cả các dữ liệu được chuyển từ hệ thống mạng đến địa chỉ IP giả mạo. Thậm chí những kẻ giả mạo này có thể phản hồi lại các gói dữ liệu giống như một người dùng tin cậy.

1.4. Man in the Middle

Một trong những tấn công mạng thường thấy nhất được sử dụng để chống lại những cá nhân và các tổ chức lớn chính là các tấn công MITM (Man in the Middle). Có thể hiểu nôm na về kiểu tấn công này thì nó như một kẻ nghe trộm. MITM hoạt động bằng cách thiết lập các kết nối đến máy tính nạn nhân và relay các message giữa chúng. Trong trường hợp bị tấn công, nạn nhân cứ tin tưởng là họ đang truyền thông một cách trực tiếp với nạn nhân kia, trong khi đó sự thực thì

các luồng truyền thông lại bị thông qua host của kẻ tấn công. Và kết quả là các host này không chỉ có thể thông dịch dữ liệu nhạy cảm mà nó còn có thể gửi xen vào cũng như thay đổi luồng dữ liệu để kiểm soát sâu hơn những nạn nhân của nó.

Trong loạt bài này, chúng tôi sẽ giải thích một số hình thức tấn công MITM hay được sử dụng nhất, chẳng hạn như tấn công giả mạo ARP Cache, DNS Spoofing, chiếm quyền điều khiển (hijacking) HTTP session,.. Như những gì bạn thấy trong thế giới thực, hầu hết các máy tính nạn nhân đều là các máy tính Windows. Với lý do đó, loạt bài này chúng tôi sẽ tập trung toàn bộ vào những khai thác MITM trên các máy tính đang chạy hệ điều hành Windows. Có thể tấn công sẽ được thực hiện từ các máy tính Windows. Tuy nhiên trong một số trường hợp, khi không có công cụ nào cho các tấn công hiện diện, chúng tôi sẽ sử dụng Backtrack Linux 4, có thể download dưới dạng một live-CD hoặc một máy ảo tại đây.

1.5. Replay

1.6. TCP/IP Hijacking

DNS Hijacking là một loại tấn công độc hại mà nó xóa bỏ các thiết lập TCP/IP của máy tính tới điểm mà nó ở một máy chủ DNS giả mạo, do đó làm mất hiệu lực của các thiết lập DNS mặc định. Khi kẻ tấn công chiếm quyền kiểm soát của một máy tính để thay đổi các thiết lập DNS, dẫn tới chiếc máy tính này sẽ được đặt tới điểm của một DNS server giả mạo, quá trình này được gọi là DNS hijacking.

Như chúng ta đã biết, DNS có nhiệm vụ dịch một tên miền mà bạn có thể dễ nhớ hơn so với việc phải nhớ một địa chỉ IP, ví dụ google.com sẽ có địa chỉ IP tương ứng là 74.125.235.46.

1.7. Social Engineering

Social engineering là phương pháp phi kỹ thuật đột nhập vào hệ thống hoặc mạng công ty. Đó **là** quá trình đánh lừa người dùng của hệ thống, hoặc thuyết phục họ cung cấp thông tin có thể giúp chúng ta đánh bại bộ phận an ninh.

1.8. Password Guessing – Đoán mật khẩu

Kỹ thuật tấn công và phòng thủ trên không gian mạng - Kỹ thuật tấn công - System Hacking

Kỹ thuật bẽ khóa mật khẩu được sử dụng để khôi phục/xác định mật khẩu của một hệ thống máy tính Kẻ tấn công sử dụng kỹ thuật bẽ khóa mật khẩu để dành quyền truy cập trái phép vào hệ thống nguy cơ về bảo mật Phần lớn các trường hợp bẽ khóa mật khẩu thành công là do các mật khẩu dễ đoán và mật khẩu yếu

2. Malicious Code – Các mã độc hại

2.1. Viruses

Trong khoa học máy tính, **virus máy tính** (thường được người sử dụng gọi tắt là virus hay **vi-rút**) là những đoạn mã chương trình được thiết kế để thực hiện tối thiểu là hai việc:

- Tự xen vào hoạt động hiện hành của máy tính một cách hợp lệ, để thực hiện tự nhân bản và những công việc theo chủ ý của người lập trình. Sau khi kết thúc thực thi mã virus thì điều khiển được trả cho trình đang thực thi mà máy không bị "treo", trừ trường hợp virus cố ý treo máy.
- Tự sao chép chính nó, tức tự nhân bản, một cách hợp lệ lây nhiễm vào những tập tin (file) hay các vùng xác định (boot, FAT sector) ở các thiết bị lưu trữ như đĩa cứng, đĩa mềm, thiết bị nhớ flash (phổ biến là USB),... thậm chí cả EPROM chính của máy.

Trước đây, virus thường được viết bởi một số người am hiểu về lập trình muốn chứng tỏ khả năng của mình nên thường virus có các hành động như: cho một chương trình không hoạt động đúng, xóa dữ liệu, làm hỏng ổ cứng,... hoặc gây ra những trò đùa khó chịu.

Những virus mới được viết trong thời gian gần đây không còn thực hiện các trò đùa hay sự phá hoại đối máy tính của nạn nhân bị lây nhiễm nữa, mà đa phần hướng đến việc lấy cắp các thông tin cá nhân nhạy cảm (các mã số thẻ tín dụng) mở cửa sau cho tin tặc đột nhập chiếm quyền điều khiển hoặc các hành động khác nhằm có lợi cho người phát tán virus.

Chiếm trên 90% số virus đã được phát hiện là nhắm vào hệ thống sử dụng hệ điều hành họ Windows chỉ đơn giản bởi hệ điều hành này được sử dụng nhiều nhất trên thế giới. Do tính thông dụng của Windows nên các tin tặc thường tập trung hướng vào chúng nhiều hơn là các hệ điều hành khác. Cũng có quan điểm cho rằng Windows có tính bảo mật không tốt bằng các hệ điều hành khác (như Linux) nên có nhiều virus hơn, tuy nhiên nếu các hệ điều hành khác cũng thông dụng như Windows hoặc thị phần các hệ điều hành ngang bằng nhau thì cũng lượng virus xuất hiện có lẽ cũng tương đương nhau.

2.2. Trojan Horses

Trojan Horses là những chương trình cải trang bản thân mình như các chương trình vô hại và có lợi nhưng thay vào đó sẽ có một mục đích ẩn mà bạn không thể biết được ví dụ các kiểu Trojan có thể thực hiện là :

- Xóa tập tin và dữ liệu của bạn một cách bạn không hay biết
- Khóa máy tính của bạn
- Cài đăt backdoor để truy cập máy tính của bạn từ xa

- Thực hiện các lệnh trên máy tính của bạn
- Mã hóa dữ liệu của bạn và viết 1 thông điệp tống tiền bạn để nhận được chương trình giải mã dữ liệu trên
- Tự động tải và cài đặt phần mêm độc hại vào máy tính bạn
- Đăng nhập tổ hợp phím và thực hiện trên máy tính bạn
- Ăn cấp mật khẩu mà bạn nhập vào trang web nhất định
- Tự khởi động máy tính của bạn
- Tắt chương trình bảo vệ máy tính của bạn (firewall,antivirus)
- Chụp ảnh màn hình theo dõi những gì đang hoạt động trên máy tính của bạn
- Tự động điều khiển webcam trên máy tính bạn để chụp hình bạn
- Tạo ra vài âm thanh khó chịu trên máy tính bạn
- Hiển thị vài hình ảnh không đẹp trên máy tính bạn
- In tài liệu trên máy in của bạn

2.3. Logic Bombs

Phần mềm độc hại giấu mình - Bom lô gíc Bom lôgic (logic bom) Mã máy tính ở trạng thái "ngủ đông" Được kích hoạt bởi một sự kiện lôgic xác định Sau đó thực hiện các hành vi phá hoại Rất khó phát hiện cho tới khi được kích hoạt Đôi khi, bom lôgíc được các hãng phần mềm hợp pháp sử dụng để đảm bảo việc chi trả cho phần mềm của họ. Nếu việc chi trả không được thực hiện đúng hạn, bom lôgíc sẽ được kích hoạt và ngăn chặn không cho dùng phần mềm nữa.

Trong một số trường hợp, bom lôgíc thậm chí còn xóa bỏ phần mềm, các file về khách hàng, cùng bảng chi trả kèm theo. Bom lôgic (logic bom) Mã máy tính ở trạng thái "ngủ đông" Được kích hoạt bởi một sự kiện lôgic xác định Sau đó thực hiện các hành vi phá hoại Rất khó phát hiện cho tới khi được kích hoạt Đôi khi, bom lôgíc được các hãng phần mềm hợp pháp sử dụng để đảm bảo việc chi trả cho phần mềm của họ.

Nếu việc chi trả không được thực hiện đúng hạn, bom lôgíc sẽ được kích hoạt và ngăn chặn không cho dùng phần mềm nữa. Trong một số trường hợp, bom lôgíc thậm chí còn xóa bỏ phần mềm, các file về khách hàng, cùng bảng chi trả kèm theo

2.4. Auditing – Logging, system scanning

Scanning là một bước tiếp theo trong tiến trình tấn công hệ thống. Giai đoạn này giúp ta xác định được nhiều thông tin của hệ thống cần tấn công.

Các loại scanning gồm: Port Scanning, Network Scanning, Vulnerability scanning

3. Social Engineering

Social engineering là phương pháp phi kỹ thuật đột nhập vào hệ thống hoặc mạng công ty. Đó là quá trình đánh lừa người dùng của hệ thống, hoặc thuyết phục họ cung cấp thông tin có thể giúp chúng ta đánh bại bộ phận an ninh. Social engineering là rất quan trọng để tìm hiểu, bởi vì hacker có thể lợi dụng tấn công

vào yếu tố con người và phá vỡ hệ thống kỹ thuật an ninh hiện tại. Phương pháp này có thể sử dụng để thu thập thông tin trước hoặc trong cuộc tấn công.

Social engineering sử dụng *sự ảnh hưởng và sự thuyết phục* để đánh lừa người dùng nhằm khai thác các thông tin có lợi cho cuộc tấn công hoặc thuyết phục nạn nhân thực hiện một hành động nào đó. **Social engineer** (người thực hiện công việc tấn công bằng phương pháp social engineering) thường sử dụng **điện thoại hoặc internet** để dụ dỗ người dùng tiết lộ thông tin nhạy cảm hoặc để có được họ có thể làm một chuyện gì đó để chống lại các chính sách an ninh của tổ chức. Bằng phương pháp này, Social engineer tiến hành khai thác các thói quen tự nhiên của người dùng, hơn là tìm các lỗ hổng bảo mật của hệ thống. Điều này có nghĩa là người dùng với kiến thức bảo mật kém cõi sẽ là cơ hội cho kỹ thuật tấn công này hành động.

Các công ty với các phương pháp xác thực, các firewalls, các mạng riêng ảo VPN, các phần mềm giám sát mạng vẫn có rất nhiều khả năng bị tấn công. Một nhân viên có thể vô tình để lộ thông tin key trong email hoặc trả lời điện thoại của một người mà họ không quen biết hoặc thậm chí nói về đề án của họ với đồng nghiệp hàng giờ liền ở quán rượu.

Thông thường, mọi người không nhận thấy sai sót của họ trong việc bảo mật, mặc dù họ không cố ý. Những kẻ tấn công đặc biệt rất thích phát triển kĩ năng về **Social Engineering** và có thể thành thạo đến mức những nạn nhân của không hề biết rằng họ đang bị lừa. Mặc dù có nhiều chính sách bảo mật trong công ty, nhưng họ vẫn có thể bị hại do tin tặc lợi dụng lòng tốt và sự giúp đỡ của mọi người.

Những kẻ tấn công luôn tìm những cách mới để lấy được thông tin. Họ chắc chắn là họ nắm rõ vành đai bảo vệ và những người trực thuộc – nhân viên bảo vệ, nhân viên tiếp tân và những nhân viên ở bộ phận hỗ trợ – để lợi dụng sơ hở của họ. Thường thì mọi người dựa vào vẻ bề ngoài để phán đoán. Ví dụ, khi nhìn thấy một người mặc đồng phục màu nâu và mang theo nhiều hộp cơm, mọi người sẽ mở cửa vì họ nghĩ đây là người giao hàng. Hay khi bạn nhặt được một chiếc USB bạn có thể rất vô tư cắm nó ngay vào máy tính để xem nó là của ai và chứa thông tin gì. Nhưng đó có thể chính là nguồn phát tán virus và mã độc đến bạn, tổ chức và người thân của bạn.

Một số công ty liệt kê danh sách nhân viên trong công ty kèm theo số điện thoại, email trên Website của công ty. Ngoài ra, các công ty còn thêm danh sách các nhân viên chuyên nghiệp đã được đào tạo trong cơ sở dữ liệu Oracle hay UNIX servers. Đây là một số ít thông tin giúp cho attacker biết được loại hệ thống mà họ đang định xâm nhập.

4. Auditing – Logging, system scanning

Audit account logon event: ghi nhận các sự kiện liên quan đến quá trình chứng thực. Trên domain: account logon events được tạo ra khi user được chứng thực trên AD. Trên local: account logon events được tạo ra khi user được chứng thực trên máy cục bộ. 2 trạng thái: Successes hoặc Failures.Audit account management: ghi

nhận sự thay đổi thông tin(Tạo/xóa/modify/password/…) của user/group. Audit Directory service Access: ghi nhận người dùng truy cập vào objects. Audit logon event: ghi nhận kết quả quá trình logon hay logoff của user.

Bài 3: Hạ tầng cơ sở an toàn thông tin
Mã bài: MD22-3

Giới thiệu: Bài 3 trình bày về hạ tầng cơ sở an toàn thông tin

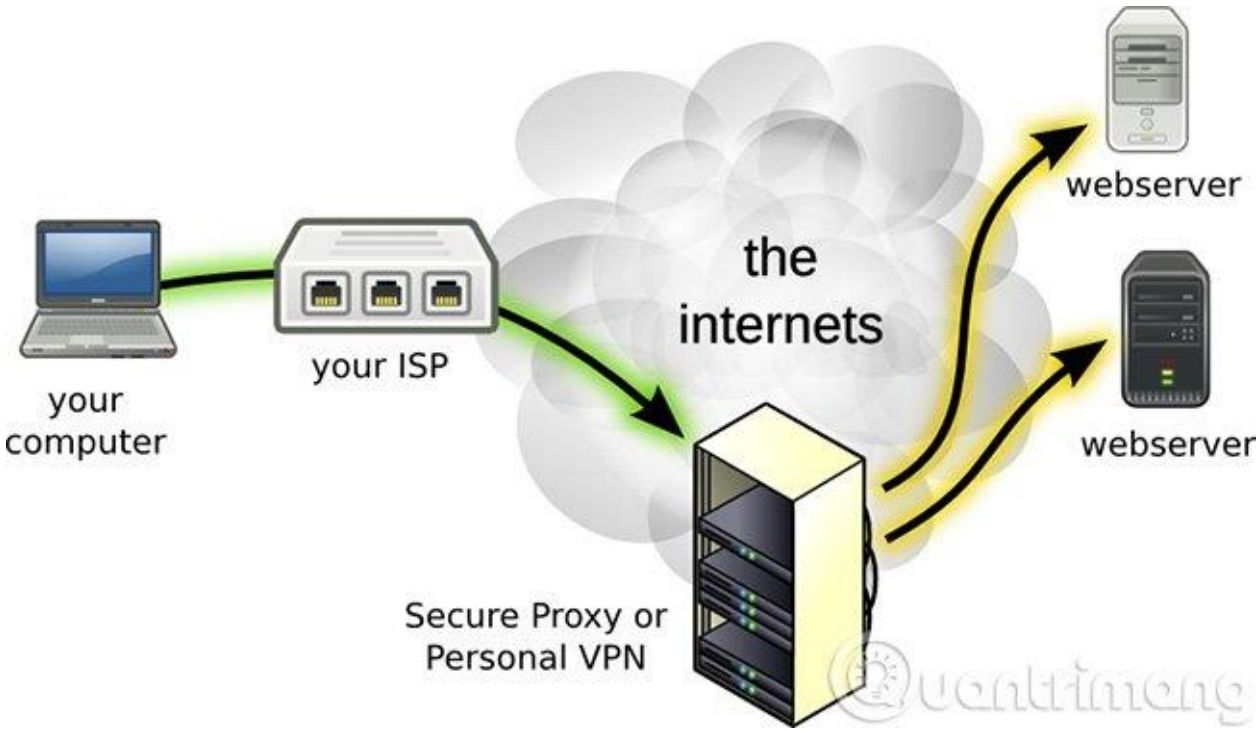
Mục tiêu:

- Trình bày về hạ tầng cơ sở trong hệ thống;
- Trình bày các thiết bị, phương tiện được sử dụng trong hệ thống và các phương thức để truy cập đến hệ thống;
- Phân biệt và sử dụng được các phương tiện, công cụ dùng trong hệ thống;
- Cấu hình được các phương thức để truy cập vào hệ thống;
- Cẩn thận, chính xác, khoa học.

Nội dung chính:

1. Truy cập từ xa
1.1. 802.1x
1.2. VPN

VPN là mạng riêng ảo, Virtual Private Network, là một công nghệ mạng giúp tạo kết nối mạng an toàn khi tham gia vào mạng công cộng như Internet hoặc mạng riêng do một nhà cung cấp dịch vụ sở hữu. Các tập đoàn lớn, các cơ sở giáo dục và cơ quan chính phủ sử dụng công nghệ VPN để cho phép người dùng từ xa kết nối an toàn đến mạng riêng của cơ quan mình



1 hệ thống VPN có thể kết nối được nhiều site khác nhau, dựa trên khu vực, diện tích địa lý... tượng tự như chuẩn **Wide Area Network (WAN)**. Bên cạnh đó, VPN còn được dùng để "khuếch tán", mở rộng các mô hình Intranet nhằm truyền tải thông tin, dữ liệu tốt hơn. Ví dụ, các trường học vẫn phải dùng VPN để nối giữa các khuôn viên của trường (hoặc giữa các chi nhánh với trụ sở chính) lại với nhau.
Nếu muốn kết nối vào hệ thống VPN, thì mỗi 1 tài khoản đều phải được xác thực (phải có **Username** và **Password**). Những thông tin xác thực tài khoản này được dùng để cấp quyền truy cập thông qua 1 dữ liệu - **Personal Identification Number (PIN)**, các mã PIN này thường chỉ có tác dụng trong 1 khoảng thời gian nhất định (30s hoặc 1 phút).

Khi kết nối máy tính hoặc một thiết bị khác chẳng hạn như điện thoại, máy tính bảng với một VPN, máy tính hoạt động giống như nó nằm trên cùng mạng nội bộ với VPN. Tất cả traffic trên mạng được gửi qua kết nối an toàn đến VPN. Nhờ đó, bạn có thể truy cập an toàn đến các tài nguyên mạng nội bộ ngay cả khi đang ở rất xa.

Bạn cũng có thể sử dụng Internet giống như đang ở vị trí của của VPN, điều này mang lại một số lợi ích khi sử dụng WiFi public hoặc truy cập trang web bị chặn, giới hạn địa lý.

Khi duyệt web với VPN, máy tính sẽ liên hệ với trang web thông qua kết nối VPN được mã hóa. Mọi yêu cầu, thông tin, dữ liệu trao đổi giữa bạn và website sẽ được truyền đi trong một kết nối an toàn. Nếu sử dụng VPN tại Hoa Kỳ để truy cập vào Netflix, Netflix sẽ thấy kết nối của bạn đến từ Hoa Kỳ.

Dù nghe có vẻ khá đơn giản, nhưng trên thực tế VPN lại được ứng dụng để làm rất nhiều thứ:

- **Truy cập vào mạng doanh nghiệp khi ở xa:** VPN thường được sử dụng bởi những người kinh doanh để truy cập vào mạng lưới kinh doanh của họ, bao gồm tất cả tài nguyên trên mạng cục bộ, trong khi đang đi trên đường, đi du lịch,... Các nguồn lực trong mạng nội bộ không cần phải tiếp xúc trực tiếp với Internet, nhờ đó làm tăng tính bảo mật.
- **Truy cập mạng gia đình, dù không ở nhà:** Bạn có thể thiết lập VPN riêng để truy cập khi không ở nhà. Thao tác này sẽ cho phép truy cập Windows từ xa thông qua Internet, sử dụng tập tin được chia sẻ trong mạng nội bộ, chơi game trên máy tính qua Internet giống như đang ở trong cùng mạng LAN.
- **Duyệt web ẩn danh:** Nếu đang sử dụng WiFi công cộng, duyệt web trên những trang web không phải https, thì tính an toàn của dữ liệu trao đổi trong mạng sẽ dễ bị lộ. Nếu muốn ẩn hoạt động duyệt web của mình để dữ liệu được bảo mật hơn thì bạn nên kết nối VPN. Mọi thông tin truyền qua mạng lúc này sẽ được mã hóa.
- **Truy cập đến những website bị chặn giới hạn địa lý,** bỏ qua kiểm duyệt Internet, vượt tường lửa,...
- **Tải tập tin:** Tải BitTorrent trên VPN sẽ giúp tăng tốc độ tải file. Điều này cũng có ích với các traffic mà ISP của bạn có thể gây trở ngại.

Các giao thức thường dùng trong VPN:

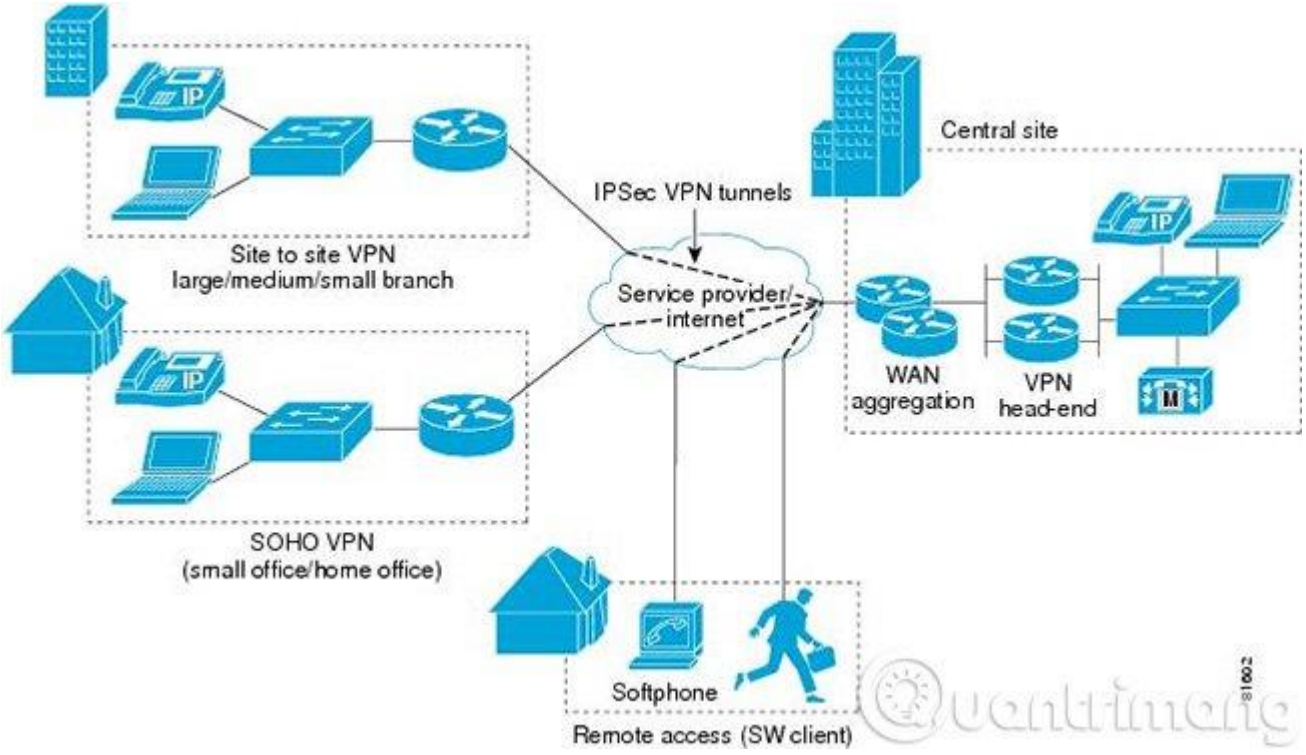
Để bảo mật các dữ liệu trong hệ thống VPN, có 1 vài giao thức - **Protocol** phổ biến được áp dụng trong mô hình này. Bao gồm:

IP security (IPSec):
Được dùng để bảo mật các giao tiếp, các luồng dữ liệu trong môi trường **Internet** (môi trường bên ngoài VPN). Đây là điểm mấu chốt, lượng traffic qua IPSec được dùng chủ yếu bởi các **Transport mode**, hoặc các **tunnel** (hay gọi là hầm - khái niệm này hay dùng trong Proxy, SOCKS) để **MÃ HÓA** dữ liệu trong VPN.

- Proxy là gì?
- SOCKS là gì?

Sự khác biệt giữa các mode này là:

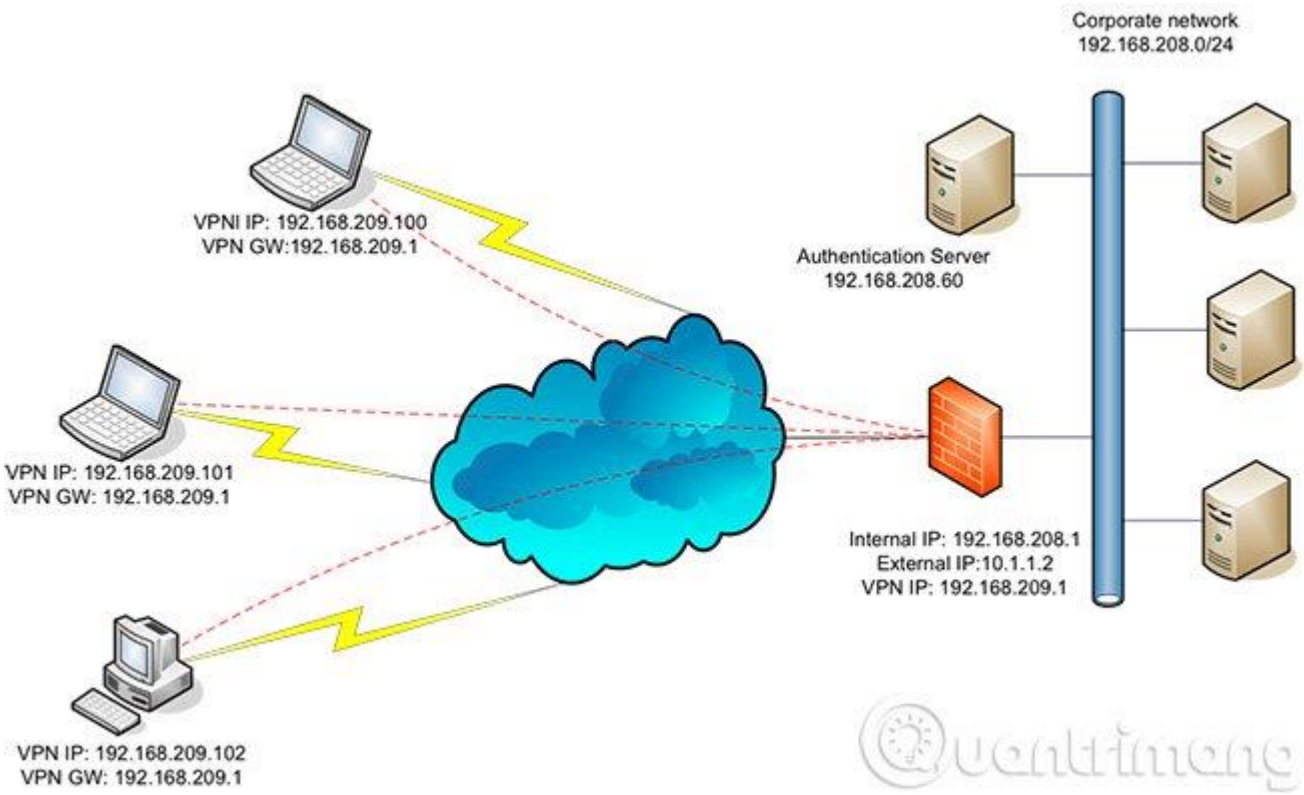
- **Transport mode** chỉ có nhiệm vụ mã hóa dữ liệu bên trong các gói (data package - hoặc còn biết dưới từ payload). Trong khi các **Tunnel** mã hóa toàn bộ các data package đó.



Do vậy, IPSec thường được coi là **Security Overlay**, bởi vì IPSec dùng các lớp bảo mật so với các Protocol khác.

Secure Sockets Layer (SSL) và Transport Layer Security (TLS):

Có 1 phần tương tự như IPSec, 2 giao thức trên cũng dùng mật khẩu để đảm bảo an toàn giữa các kết nối trong môi trường Internet.

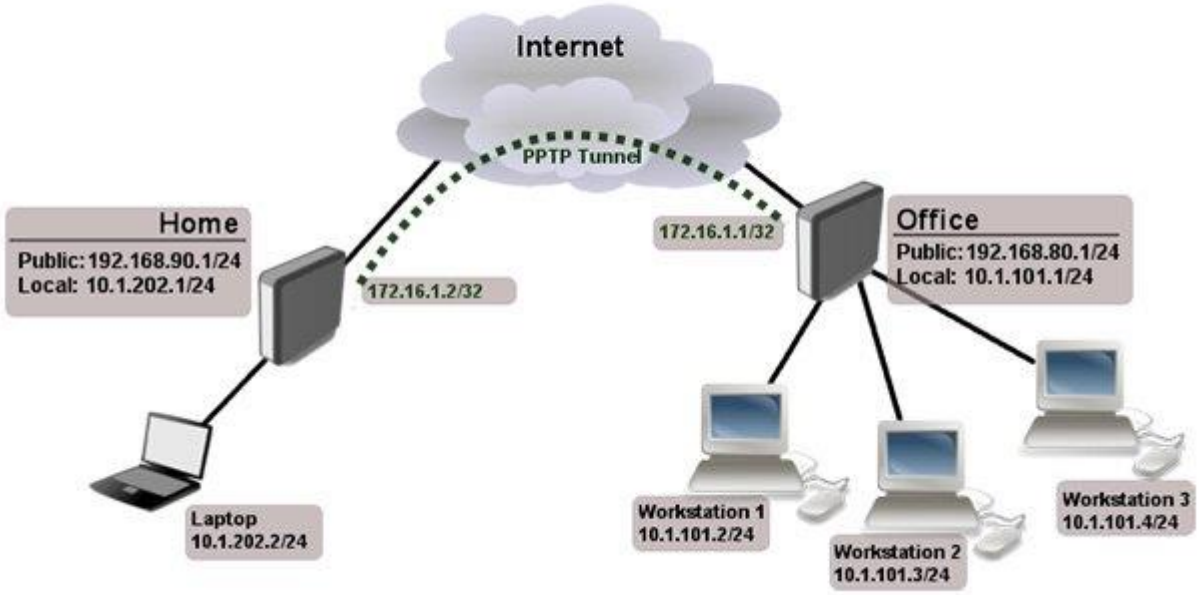


Mô hình SSL VPN

Bên cạnh đó, 2 giao thức trên còn sử dụng chế độ **Handshake** - có liên quan đến quá trình xác thực tài khoản giữa client và server. Để 1 kết nối được coi là thành công, quá trình xác thực này sẽ dùng đến các **Certificate** - chính là các khóa xác thực tài khoản được lưu trữ trên cả server và client.

Point-To-Point Tunneling Protocol (PPTP):

Là giao thức được dùng để truyền dữ liệu qua các hầm - Tunnel giữa 2 tầng traffic trong Internet. L2TP cũng thường được dùng song song với IPSec (đóng vai trò là **Security Layer** - đã đề cập đến ở phía trên) để đảm bảo quá trình truyền dữ liệu của L2TP qua môi trường Internet được thông suốt. Không giống như PPTP, VPN sẽ "kế thừa" toàn bộ lớp L2TP/IPSec có các key xác thực tài khoản được chia sẻ hoặc là các **Certificate**.



Ưu điểm, nhược điểm của VPN:

Lý thuyết là như vậy, còn khi áp dụng vào thực tế thì VPN sẽ có những ưu, nhược điểm như thế nào. Mời các bạn tiếp tục thảo luận với Quản Trị Mạng.

Để xây dựng 1 hệ thống mạng riêng, mạng cá nhân ảo thì dùng VPN là 1 giải pháp không hề tốn kém. Chúng ta có thể tưởng tượng thế này, môi trường Internet là cầu nối, giao tiếp chính để truyền tải dữ liệu, xét về mặt chi phí thì nó hoàn toàn hợp lý so với việc trả tiền để thiết lập 1 đường kết nối riêng với giá thành cao. Bên cạnh đó, việc phải sử dụng hệ thống phần mềm và phần cứng nhằm hỗ trợ cho quá trình xác thực tài khoản cũng không phải là rẻ. Việc so sánh sự tiện lợi mà VPN mang lại cùng với chi phí bỏ ra để bạn tự thiết lập 1 hệ thống như ý muốn, rõ ràng VPN chiếm ưu thế hơn hẳn.

Nhưng bên cạnh đó, có nhược điểm rất dễ nhận thấy như:

VPN không có khả năng quản lý **Quality of Service (QoS)** qua môi trường Internet, do vậy các gói dữ liệu - Data package vẫn có nguy cơ bị thất lạc, rủi ro. Khả năng quản lý của các đơn vị cung cấp VPN là có hạn, không ai có thể ngờ trước được những gì có thể xảy ra với khách hàng của họ, hay nói ngắn gọn là bị hack đó.

1.3. RADIUS

RADIUS là một giao thức dùng để chứng thực người dùng từ xa (remote access). Thông tin dùng để chứng thực được lưu tập trung ở **RADIUS server**.

1.4. TACACS / +

TACACS + là giao thức cung cấp điều khiển truy cập cho các bộ định tuyến,mạng truy cập vào máy chủ và các thiết bị máy tính khác nối mạng thông qua mộthoặc

tập trung nhiều máy chủ. TACACS + cung cấp riêng biệt chứng thực, uỷquyền và các dịch vụ kế toán.TACACS cho phép một khách hàng chấp nhận một tên người dùng và mật khẩuvà gửi một truy vấn đến một máy chủ xác thực TACACS, đôi khi được gọi là mộtTACACS daemon hoặc đơn giản chỉ TACACSD.

Máy chủ đó,được dùng để chạychương trình trên host. Các máy chủ sẽ xác định xem liệu chấp nhận hoặc từ chốiyêu cầu và gửi một phản ứng trở lại. Các TIP sau đó sẽ cho phép truy cập haykhông, dựa trên phản ứng đó . Trong này cách, quá trình ra quyết định là "mở cửa"và các thuật toán và dữ liệu sử dụng để đưa ra quyết định là dưới sự kiểm soát hoàntoàn của bất cứ ai chạy TACACS daemon.

Các phần mở rộng cho giao thức cungcấp cho nhiều loại yêu cầu chứng thực và các loại mã nhiều phản ứng hơn là trong bản gốc đặc điểm kỹ thuật.Có ba phiên bản của TACACS và phiên bản thứ ba được gọi là TACACS +, màkhông tương thích với các phiên bản trước.TACACS + là một phương pháp trao đổi thông tin giữa một thiết bị cung cấp truycập mạng người sử dụng (các "TACACS + client") và một thiết bị có chứa thông tinxác thực cho những người người sử dụng (các "TACACS + server").

TACACS +được dựa trên mô hình AAA: xác thực, uỷ quyền và kế toán.Các TACACS dựa trên môi trường truy cập từ xa có ba thành phần chính: ClientAccess, Network Access Server, và TACACS Server +.

Các Client Access có thể là một người quay số vào một mạng lưới cung cấp dịch vụkết nối với các trang web khác nhau trên internet (traditional User role). Ngoài ra,các Client Access có thể là một thiết bị; nó có thể là một bộ định tuyến router ISDNhoặc quay số theo yêu cầu để có thể kết nối nhiều người dùng tại một văn phòngnhỏ / home office

1.5. L2TP / PPTP

Các kỹ thuật mã hóa VPN được phát triển và chứng nhận bởi **National Institute of Standards and Technology,** tuy nhiên với vụ Edward Snowden tiết lộ về các bị mật mà NSA đang cố gắng bẽ khóa công nghệ này là một thông tin gây sốc. Điều này đặt dấu chấm hỏi liệu “các công nghệ VPN này có thực sự bảo mật”? Và để trả lời cầu hỏi này, chúng tối nhận thấy đây là thời điểm để viết về chủ đề này.

Chúng ta sẽ băt đầu bằng cách mổ sẻ những điểm khác biệt giữa các giao thức VPN protocols trước khi đi vào nội dung chính liên quan tới kỹ thuật mã hóa và phân tích việc NSA cố gắng bẻ khóa các công nghệ mã hóa này sẽ tác động tới người dùng như thế nào.

	PPTP	L2TP	OpenVPN	SSTP	IKEv2
Pros	• Fast. • Client built-in to almost all platforms. • Easy to set up. •	• Typically considered secure. • Available on all modern devices and operating systems. • Easy to set up. •	• Has the ability to bypass most firewalls. • Highly configurable. • Since it is open source, it can be easily be vetted for backdoors. • It is compatible a variety of encryption algorithms. • Highly secure.	• Has the ability to bypass most firewalls. • The level of security depends on the cipher, but it is usually secure. • Entirely integrated into Windows operating system. • Microsoft support.	• Extremely secure – supports a variety of ciphers such as 3DES, AES, AES 256. • Comes with support for Blackberry devices. • It's stable, especially when reconnecting after losing a connection or switching networks. • It's easy to set up, at least from the user's end. • Relatively faster than L2TP, PPTP and SSTP.
Cons	• It's compromised by the NSA. • Not completely secure.	• Slower than OpenVPN. • May be compromised by the NSA. • Can be problematic if used with restrictive firewalls. • It's likely that the NSA has deliberately weakened the protocol. •	• Can be a little tricky to set up. • It requires third-party software. • Support for desktop is great, but on mobile devices, it needs improvement.	• Since it's a proprietary standard owned by the Microsoft Corporation, it cannot be vetted for backdoors. • Only works on Windows-only platforms	• Supported on limited platforms. • The UDP port 500 used is easy to block as compared to SSL based solutions, like SSTP or OpenVPN. • Not an open source implementation • At the server-end, implementing IKEv2 is tricky, which can cause a few potential issues.

PPTP

Được phát triển bởi nhóm thành viên được ủng hộ bởi Microsoft Corporation, Point-to-Point Tunneling (PPTP) tạo hệ thống riêng ảo dựa trên kết nói quay số (dial-up) còn gọi là VPN . Và kể từ khi nó xuất hiện PPTP được sử dụng rộng rãi như là một chuẩn protocol VPNs . cũng là VPN protocol đầu tiê được hỗ trợ bởi Windows, PPTP hoạt động dựa vào các chuẩn xác thực như MS_CHAP v2 là chuẩn phổ biến nhất hiện nay.

Ưu điểm của PTTP là khả năng thiết lập dễ dàng và không tốn nhiều tài nguyên hệ thống. Và đây là lý do mà nhiều doanh nghiệp lựa chọn VPN này như là giải pháp.

Mặc dù sử dụng chuẩn mã hóa 128-bit, nhưng PPTP chỉ có vài lỗ hỏng nhỏ trong đó đáng lưu ý là khả năng giải mã MS-CHAP v2 Authentication là lỗi nghiêm trọng nhất. Vì vậy, PPTP có thể bị bẻ khóa trong vòn 2 đây. Mặc dù lổ hổng đã được khắc phục bởi Microsoft nhưng người khổng lồ công nghệ này cũng khuyến nghị người dùng sử dụng các giao thức thay thế như SSTP hoặc L2TP.

Do khả năng bảo mật chưa cao nên không quá bất ngờ khi giải mã các gói dữ liệu PPTP là công việc hằng ngày tai NSA. tuy vậy, rủi ro đáng ngại hơn còn nằm ở chỗ là khả năng có thể giải mã hàng loạt các dữ liệu cũ hơn được mã hóa bởi PPTP khi nhiều chuyên gia khuyến nghị đây là giao thức bảo mật.

Ưu điêm

- Nhanh.
- Phần mềm máy trạm trên nhiều hệ điều hành.

- Thiết lập cấu hình dễ.

Cons

- Đã bị bẻ khóa bởi NSA.
- Không hoàn toàn bảo mật.

L2TP và L2TP/IPsec

Layer 2 Tunnel Protocol không giống các VPN protocol khác khi nó không mã hóa các dữ liệu đi qua nó mà phải nhờ vào một bộ protocol có tên là IPsec để mã hóa dữ liệu trước khi gửi. Tất cả thiết bị tương thích và hệ điều hành đều được cài đặt sẵn chuẩn L2TP/IPsec. Quá trình thiết lập cũng dễ như PPTP nhưng giao thức này lại sử dụng cổng UDP port 500, nên dễ dàng bị tường lửa NAT firewall chặn lại. Dó đó, bạn sẽ cần chuyên tiếp cổng trong trường hợp này.

Không có những lổ hổng lớn đi kèm với mã hóa IPsec encryption. Tuy vậy, Edward Snowden ám chỉ khả năng NSA cũng đã bẻ khóa được trong khi John Gilmore thành viên sáng lập và chuyên gia an ninh của Electric Frontier Foundation cho rằng NSA đang chủ đích làm yếu đi giao thức này. Ngoài ra, do LT29/IPsec đóng gói tới 2 lần dữ liệu nên được đánh gia là không hiệu quả bằng SSL và kéo theo tốc độ chậm hơn so với các VPN protocols khác.

Ưu điểm

- Được đánh giá là bảo mật.
- Cài đặt sẵn trên tất cả OS và thiết bị gần đây.
- Thiết lập dễ dàng.

Nhược điểm

- Chậm hơn so với OpenVPN.
- Có thể bị mở khóa bởi NSA.
- Có thể có vấn đề nếu được sử dụng với các tường lừa.
- Khả năng NSA đã cố tình làm suy yếu giao thức.

OpenVPN

OpenVPN là một dạng VPN mã nguồn mở khá mới hiện nay sử dụng giao thức SSLv3/TLSv1 và OpenSSL library kết hợp với các công nghệ khác. protocol này có độ tùy chỉnh cao và chạy tốt nhất trên cổng UDP port nhưng vẫn có thể cấu hình để chạy trên các cổng khác.

Một ưu điểm nổi bật của giao thức này là nó sử dụng OpenSSL library hỗ trợ nhiều thuật toán mã hóa như 3DES, AES, Camellia, Blowfish, CAST-128 và nhiều nữa trong đó Blowfish , ES là sử dụng rộng rãi bởi các nhà cung cấp VPN. OpenVPN sử dụng chuẩn mã hóa 128-bit Blowfish được đánh giá là bảo mật nhưng vẫn có một số điểm yếu

Khi nói về các thuật toán mã hóa, AES là mới nhất và được xem là tiêu chuẩn "vàng" do được biết đến như là không có điểm yếu nào. Do đó, giao thức này được chính p hủ và các cơ quan chính phủ Mỹ sử dụng để bảo vệ các dữ liệu mật. Nó cũng có thể xử lý file dung lượng lớn tốt hơn Blowfish nhờ vào khả năng hỗ trợ gói 128-bit so với 64-bit của Blowfish. Tuy vậy, cả hai đều là các thuật toán mã hóa được công nhận NIST và được biết là không có nhiều lổ hỏng. Tuy nhiên, vẫn có một số vấn đề mà không được công khai nhiều mà chúng tôi sẽ đề cập dưới đây.

Đầu tiên, tốc độ của OpenVPN phụ thuộc vào thuật toán mã hóa mà nó sử dụng nhưng thông thường nhanh hơn IPsec. Mặc dù OpenVPN được mặc định trong nhiều dịch vụ VPN nhưng lại không được hỗ trợ ở bất kỳ hệ điều hành nào. Một số phần mềm thứ 3 hỗ trợ cho cả Android và iOS.

Về thiết lập, thật không dễ để so sánh OpenVPN với L2TP/IPsec và PPTP, khi mà có khá nhiều dạng phần mềm OpenVPN đang được sử dụng hiện nay. Ngoài việc tải xuống, cài đặt mà thao tác cấu hình cũng cần thiết.

Tuy vậy, nếu nhận xét ở bức tranh tổng thể và với thông tin từ Edward Snowden cung cấp có vẻ như OpenVPN vẫn chưa bị giải mã hay làm yếu được bởi NSA. Khả năng miễn nhiễm trước các cuộc tấn công của NSA chủ yếu là nhờ vào các khóa tạm thời được hoán đổi. Tuy vậy, không ai lường được khả năng của NSA đến đâu nhưng với số liệu và chứng cứ cho thấy OpenVPN khi kết hợp với mật mã mạnh là VPN protocol tduy nhất bảo mật hoàn toàn.

Ưu điểm

- Khả năng vượt hầu hết các firewalls.
- Tùy chỉnh cao.
- Do là phần mềm mã nguồn mở nên có thể được dùng để phòng hờ.

- Tương thích với nhiều thuật toán mã hóa.
- Bảo mật cao.

Nhược điểm

- Thiết lập khó hơn.
- Cần thêm phần mềm thứ 3.
- Phiên bản desktop thì đáng khen nhưng trên di động cần cải thiện thêm.

SSTP

Được trình làng bởi Microsoft Corporation trong phiên bản Windows Vista Service Package 1, SSTP (secure socket tunneling) giờ còn xuất hiện trên SEIL, Linux và RouterOS nhưng chủ yếu vẫn dành cho phiên bản Windows. Sử dụng SSL v3 nên tính năng khá tương tự với OpenVPN như khả năng giảm thiệu trình trạng NAT firewall. SSTP là một VPN protocol khá ổn định và dễ dùng đặc biệt là ở hệ điều hành Windows.

Tuy nhiên, được sở hữu bởi Microsoft và gã khổng lồ này có lịch sử "bắt tay" với NSA nên độ bảo mật vẫn chưa cao.

Ưu điểm

- Khả năng vượt hầu hết firewalls.
- Mức độ bảo mật phụ thuộc vào thuật toán mã hóa nhưng nhìn chung là bảo mật cao.
- Tích hợp hoàn toàn trong Window.
- Hỗ trợ bởi Microsoft.

Nhược điểm

- Do được sở hữu bởi Microsoft Corporation nên không thể sử dụng như phương án dự phòng.
- Chỉ hỗ trợ hệ điều hành Windows

IKEv2

IKEv2 là viế t tắc của cụm từ tiếng anh-Internet Key Exchange Version 2 một giao thức dựa theo công nghệ đường hầm IPsec, được phát triển bởi Cisco và Microsoft. Giao thức này hiện xuất hiện trên Windows 7 trở đi cũng như Linux và các nền tảng khác bao gồm cả Blackberry.

Giao thức này còn có tên khác là VPN Connect theo cách gọi của Microsoft Corporation. Nó có tác dụng tạo lại kết nối VPN một cách tự động khi kết nối bị ngắt tạm th ời. enefit the most from Trên di động, IKEv2 có cái tên khác là Mobility and Multi-homing protocol là một chuẩn hóa giúp thay đổi mạng một cách dễ dàng. Ngoài ra, nó cũng khá hữu dụng với thiết bị Blackberry vì nó là số ít giao thức hỗ trợ c ho nền tảng này. Mặc dù hỗ trợ ít hệ điều hành hơn nếu so với IPsec nhưng IKEv2 lại không thua kém về tính ổn định, bảo mật và hiệu suất.

Ưu điểm

- Cực kỳ bảo mật-Hỗ trợ nhiều mật mã như 3DES, AES, AES 256.
- Hỗ trợ thiết bị Blackberry.
- Ổn định đặc biệt khi gặp phải trình trạng rớt mạng hoặc chuyển mạng.
- Thiết lập dễ dàng ít nhất là cho người dùng cuối.
- Nhanh hơn so với L2TP, PPTP and SSTP.

Nhược điểm

- Không hỗ trợ nhiều hệ điều hành
- Cổng UDP 500 dễ bị chặn nếu so với các giải pháp SSL như SSTP hay OpenVPN.
- Không phải là giải pháp mã nguồn mở
- Ở tại máy chủ việc thiết lập IKEv2 khá rắc rối có thể kéo theo một số vấn đề tiềm ẩn.

Issues

Để hiểu về mã hóa, bạn phải nắm rõ một số khái niệm quan trọng mà chúng tôi sẽ đề cập dưới đây.

Độ dài khóa mã hóa

Cách thô nhất để xác định mất bao lâu để bẻ khóa được một mật mã là dựa vào độ dài của nó tức là số lượng số 0 và 1. Dựa trên hình thức này, các kiểu dò khóa thô (còn gọi là dò ép bức) là kiểu tấn công thô nhất hoạt động bằng cách thử tất cả các cách ghép có thể cho tới khi thành công. Hầu hết các nhà cung cấp VPN đều sử dụng khóa 128-bits và 256-bits. Các cấp độ cao được sử dụng để xác thực dữ liệu và handshaking, nhưng điều đó có nghĩa là mã hóa 256- bit thì tốt hơn so với 128-bit?

Để cho cầu trả lời chính xác hãy đặt các con số lên bàn cân:

- Để bẽ khóa được mã 128-bit, máy tính cần tới 3.4×10(38) bước tính toán.
- Để bẽ khóa được mã 256-bit, máy tính cần tới 2(128) thời gian so với thời lượng cần cho mã 128-bit.
- Tấn công kiểu ép bứt mã 256-bit cần tới 3.31 x 10(65) bước tính toán tương đương tổng số nguyên tử phóng xạ toàn vũ trụ.
- Lấy minh họa, máy tính Fujitsu K, siêu máy tính nhanh nhất thế giới 2011 có tốc độ Rmax lên tới 10.51 petaflops thì cũng phải mất tới hơn 1 tỷ năm để bẻ khóa mã 128-bit AES bằng hình thức tấn công ép bức.
- NUDT Tianhe-2, siêu máy tính mạnh nhất thế giới 2013 trên thế giới có tốc độ lên tới 33.86 petaflops, gấp 3 lần chiếc Fujitsu K, và nó cũng mất 1/3 của tỷ năm để bẻ khóa 128-bit AES key.

Trước khi sự kiện Edward Snowden thì thế giới vẫn tin rằng mã hóa 128-bit là không thể bẻ khóa bằng hình thức áp bức (by force) được và nó sẽ vẫn như vậy trong trăm năm tới. Tuy vậy, với những tài lực mà NSA có trong tay , không tí các chuyên gia và quản trị mạng đã nâng cấp độ dài khóa mã hóa. Điều cần lưu ý là chính phủ Mỹ hiện đang dùng mã hóa 256-bit để bảo vệ các dữ liệu nhạy cảm (mã hóa 128-bit dùng cho các nhu cầu mã hóa hằng ngày). Với phương thức nào được dùng đi nữa như AES, cũng nảy sinh ra một số vấn đề.

Mật mã

Mật mã thực chất là các thuật toán đại số được sử dụng trong mã hóa nhằm tăng sức mạnh khi các thuật toán thông thường khá yếu và dễ bị khai thác bởi hacker. Có thể nói, Blowfish và AES là hai mật mã thông dụng được sử dụng ở các phần mềm VPN hiện nay. Ngoài ra, RSA được dùng để má hóa và giải mã các mật mã trong khi SHA-1 và SHA-2 được dùng để xác thực dữ liệu dưới dạng dấu #.

tuy nhiên, AES được cho là mật mã bảo mật nhất cho VPN ngay cả chính phủ Mỹ cũng sử dụng phương thức này. Tuy nhiên, cũng có lý do cho thấy lòng tin vào phương thức này đã không đặt đúng chỗ.

NIST

SHA-1, SHA-2, RSA và AES tất cả đều được phát triển và chứng nhận bởi Hiệp hội kỹ thuật và tiêu chuẩn quốc gia Mỹ (tên tiếng Anh là **United States National Institute of Standards and Technology** (NIST)) là một định chế hoạt động mật thiết với NSA để phát triển các mật mã. Giờ chúng ta đều biết các nổ lực làm yếu hoặc bẻ kh óa ngầm các mật mã của NSA, điều này kéo theo câu hỏi về sự minh bạch của thuật toán NIST.

Mặc dù NIST luôn phủ nhận các cáo buộc hành vi sai trái(ví dụ như cố ý làm yếu các tiêu chuẩn mã hóa), họ cũng tăng lòng tin người dùng bằng cách mời gọi sự tham gia của công chung trong các lượt ra mắt các tiêu chuẩn mật mã mới của họ. Trong khi đó, NSA đã từng bị cáo buộc bởi thời báo New York Times khi cố ý be khóa các tiêu chuẩn mã hóa của NIST' bằng các làm gián đoạn các cuộc thử nghiệm đại trà hoặc cài các phần mềm gián điệp không thể phát hiện để làm yếu đi thuật toán. .

Vào 17/12/2013, sự bất tin nhiệm càng cao hơn khi RSA Security khuyến nghị người dùng ngưng sử dụng các thuật toán mã hóa cụ thể khi chúng có thể có lổ hỏng được cố ý tạo ra bởi NSA.

Ngoài ra, các tiêu chuẩn mã hóa thiết kế bởi NIST, Dual EC DRBG đều đã không còn bảo mật trong nhiều năm rồi. Bằng chứng là Đại học kỹ thuật Hà Lan cũng đã lưu ý điều này năm 2006. tuy vậy, việc đi theo các tiêu chuẩn NIST vẫn cứ tiếp diễn khi mà cần phải đáp ứng các tiêu chuẩn của NIST đê có thể giành các hợp đồng của chính phủ Mỹ.

Do sự quá thông dụng của tiêu chuẩn NIST trên toàn cầu và ở nhiều lĩnh vực liên quan tới tính riêng tư như VPN khiến vấn đề khá nang giải. Nhiều chuyên gia trong ngành cũng chưa có giải pháp để không phụ thuộc vào NIST. Công ty duy nhất tìm hướng đi riêng là là **Silent Circle**, cũng đành đóng dịch vụ Silent Mail của họ thay vị chấp nhận bị thâu tóm bởi NSA, và chính thức rút lui khỏi tiêu chuẩn NIST vào tháng 11/ 2013.

Thông qua bài viết này cũng cảm ơn sự đóng góp của BestVPN, và LiquidVPN đã bắt đầu thử nghiệm các mật mã không liên quan tới NIST. Tuy nhiên, đây củng là VPN duy nhất đang chọn hướng đi riêng này mà chúng tôi biết. Do đó, tính tới thời điểm hiện tại việc sử dụng chuẩn mã hóa 256-bit AES vẫn được xem là tối ưu nhất

Các cuộc tấn công NSA bẻ khóa RSA

Một trong các tiết lộ gần đây của Edward Snowden liên quan tới chương trình tên là 'Cheesy Name' được phát triển để dò ra các key mã hóa hay 'certificates' mà có khả năng dễ dàng bẻ khóa bởi siêu máy tính tại GCHQ. Điều này cho thấy các chứng chỉ này (gọi là certificate) thường được bảo vệ bởi mã hóa 1024-bit yếu hơn là mọi người nghĩ và có thể dễ dàng giải mã nhanh hơn nhờ vào GHCQ và NSA. Một khi đã được giải mã thành công thì các trao đổi quá khứ và tương lai sẽ bị xâm pham nhờ vào các key vĩnh viễn dùng để giải mã.

Kết quả là, rất nhiều dạng mã hóa dựa vào các key và certificate lâu năm được cho là đã bị bẽ khóa bao gồm cả TLS và SSL. Điều này đánh động tới giao thức HTTPS. Tuy nhiên, vẫn có tin vui là OpenVPN lại nằm vùng nguy hiểm do sử dụng các key tạm thời. Lý do là mỗi trao đổi lại yêu cầu một key mới nên không yêu cầu certificate.

Nếu hacker lấy được key riêng của certificate, việc giải mã chúng không phải là chuyện đơn giản. Với kiểu tấn công MitM, hacker có thể xác định các kết nối OpenVPN connection nhưng cần xác định riêng kết nối và cả key riêng cũng cần phải được bẽ khóa. Kể từ khi thông tin GHCQ và NSA có thể bẻ khóa mã hóa 1024-bits một số nhà cung cấp VPN đã nâng cấp lên 2048- bits thậm chí là 4096-bits.

Perfect Forward Secrecy

Vẫn còn tin vui là giải pháp cho vấn đề kể trên vẫn có thâm chí cho cả c kết nối TLS và SSL khi trang web thực hiện hệ thống perfect forward secrecy system (PFS) cho phép chỉ mỗi key mã hóa (encryption key) được tạo ra cho mỗi session. Tuy vậy, chỉ có một cái tên thực hiện thành công điều này hiện nay là Google.

Trước khi kết thúc bài viết này, có một điều mà các bạn nên làm theo là nghe theo lời của Edward Snowden, là mã hóa vẫn còn được việc và các hệ thống mã hóa cần phải được áp dụng để tăng cường tính bảo mật. Do đó, bạn học được gì từ bài viết này? Đơn gian thôi! OpenVPN là protocol bảo mật nhất hiện có và các nhà cung cấp VPN vẫn luôn cải tiến các biện pháp phòng vệ bảo mật của họ. Thật tuyệt vời hơn nữa nói các nhà cung cấp này cũng từ bỏ tiêu chuẩn NIST nhưng có 1 điều mà chúng tôi vẫn còn nhắc bạn nhớ.

- PPTP là giao thức kém bảo mật nhất. Không những bị bẻ khóa bởi NSA mà Microsoft cũng đã bỏ giao thức này. Đó là lý do mà chúng tôi khuyên người dùng không dùng tới PPTP mặc dù khả năng tương thích với nhiều hệ điều hành. Hơn nữa, các ưu điểm này vẫn được hỗ trợ ở giao thức bảo mật hơn như L2TP/IPsec.

- Với các mục đích sử dụng không quan trọng , L2TP/IPsec là giải pháp phù hợp mặc dù đã bị làm yếu và có thể bẻ khóa bởi NSA. Với khả năng thiết lập VPN nhanh mà không cần tới phần mềm thứ 3, L2TP/IPsec vẫn nên được cân nhắc đặc biệt là ở các thiết bị di động thiếu vắng hỗ trợ chuẩn OpenVPN.

- Sẽ cần tới các phần mềm thứ e để cài đặc được ở các hệ điều hành , OpenVPN không thể tranh cãi là VPN tốt nhất phù hợp với mọi nhu cầu. Nhanh, bảo mật, đáng tin cậy mặc dù thiết lập sẽ mất chút thời gian hơn nhưng đây là phần mềm có tính bảo mật và bảo vệ sự riêng tư tố nhất cho người dùn mà chúng tôi nhận thấy.

- IKEv2 cũng là giao thức có tốc độ nhanh và bảo mật nếu dùng kèm với các giải pháp mã nguồn mở đặc biệt là tính năng tự động kết nối lại khi kết nối bị ngắt ở các thiết bị di động. Ngoài ra, nó cũng là một trong số ít giao thức VPN hỗ trợ thiết bị Blackberry.

- SSTP có những tính năng khá tương đồng với OpenVPN tuy nhiên chỉ hỗ trợ mỗi Windows. Do đó, khả năng tương thích với Windows ở giao thức này là khá lớn so với các giao thức VPN còn lại. Tuy nhiên, đây cũng là giới hạn mà nhiều nhà cung cấp VPN không hỗ trợ nhiều giao thức này. Ngoài ra, với lịch sự liên quan mật thiết với NSA của Microsoft, SSTP là một giao thức không còn đáng tín cậy đối với chúng tôi.

Tóm lại, hãy dùng OpenVPN mỗi khi có thể, trên thiết bị di động có thêm lựa chọn là IKEv2, về tốc độ hãy chọn L2TP trong khi OpenVPN đang tiếp cận tốt các thiết bị di động, chúng tôi khuyến nghị giao thức này trên cả.

1.6. SSH

SSH (tiếng Anh: ***Secure Shell***) là một giao thức mạng dùng để thiết lập kết nối mạng một cách bảo mật. SSH hoạt động ở lớp trên trong mô hình phân lớp TCP/IP. Các công cụ SSH (như là OpenSSH,...) cung cấp cho người dùng cách thức để thiết lập kết nối mạng được mã hoá để tạo một kênh kết nối riêng tư. Hơn nữa tính năng tunneling của các công cụ này cho phép chuyển tải các giao vận theo các giao thức khác. Do vậy có thể thấy khi xây dựng một hệ thống mạng dựa trên SSH, chúng ta sẽ có một hệ thống mạng riêng ảo VPN đơn giản.

SSH là gì?

SSH là một chương trình tương tác giữa máy chủ và máy khách có sử dụng cơ chế mã hoá đủ mạnh nhằm ngăn chặn các hiện tượng nghe trộm, đánh cắp thông tin trên đường truyền. Các chương trình trước đây: telnet, rlogin không sử dụng phương pháp mã hoá. Vì thế bất cứ ai cũng có thể nghe trộm thậm chí đọc được toàn bộ nội dung của phiên làm việc bằng cách sử dụng một số công cụ đơn giản. Sử dụng SSH là biện pháp hữu hiệu bảo mật dữ liệu trên đường truyền từ hệ thống này đến hệ thống khác.

Cách thức làm việc của SSH

SSH làm việc thông qua 3 bước đơn giản:

- Định danh host - xác định định danh của hệ thống tham gia phiên làm việc SSH.
- Mã hoá - thiết lập kênh làm việc mã hoá.
- Chứng thực - xác thực người sử dụng có quyền đăng nhập hệ thống.

Định danh host

Việc định danh host được thực hiện qua việc trao đổi khoá. Mỗi máy tính có hỗ trợ kiểu truyền thông SSH có một khoá định danh duy nhất. Khoá này gồm hai thành phần: khoá riêng và khoá công cộng. Khoá công cộng được sử dụng khi cần trao đổi giữa các máy chủ với nhau trong phiên làm việc SSH, dữ liệu sẽ được mã hoá bằng khoá công khai và chỉ có thể giải mã bằng khoá riêng. Khi có sự thay đổi về cấu hình trên máy chủ: thay đổi chương trình SSH, thay đổi cơ bản trong hệ điều hành, khoá định danh cũng sẽ thay đổi. Khi đó mọi người sử dụng SSH để đăng nhập vào máy chủ này đều được cảnh báo về sự thay đổi này. Khi hai hệ thống bắt đầu một phiên làm việc SSH, máy chủ sẽ gửi khoá công cộng của nó cho máy khách. Máy khách sinh ra một khoá phiên ngẫu nhiên và mã hoá khoá này bằng khoá công cộng của máy chủ, sau đó gửi lại cho máy chủ. Máy chủ sẽ giải mã khoá phiên này bằng khoá riêng của mình và nhận được khoá phiên. Khoá phiên này sẽ là khoá sử dụng để trao đổi dữ liệu giữa hai máy. Quá trình này được xem như các bước nhận diện máy chủ và máy khách.

Mã hoá

Sau khi hoàn tất việc thiết lập phiên làm việc bảo mật (trao đổi khoá, định danh), quá trình trao đổi dữ liệu diễn ra thông qua một bước trung gian đó là mã hoá/giải mã. Điều đó có nghĩa là dữ liệu gửi/nhận trên đường truyền đều được mã hoá và giải mã theo cơ chế đã thoả thuận trước giữa máy chủ và máy khách. Việc lựa chọn cơ chế mã hoá thường do máy khách quyết định. Các cơ chế mã hoá thường được chọn bao gồm: 3DES, IDEA, và Blowfish. Khi cơ chế mã hoá được lựa chọn, máy chủ và máy khách trao đổi khoá mã hoá cho nhau. Việc trao đổi này cũng được bảo mật dựa trên đinh danh bí mật của các máy. Kẻ tấn công khó có thể nghe trộm thông tin trao đổi trên đường truyền vì không biết được khoá mã hoá. Các thuật toán mã hoá khác nhau và các ưu, nhược điểm của từng loại:

- 3DES (cũng được biết như Triple-DES) -- phương pháp mã hoá mặc định cho SSH.
- IDEA—Nhanh hơn 3DES, nhưng chậm hơn Arcfour và Blowfish.
- Arcfour—Nhanh, nhưng các vấn đề bảo mật đã được phát hiện.
- Blowfish—Nhanh và bảo mật, nhưng các phương pháp mã hoá đang được cải tiến.

Chứng thực

Việc chứng thực là bước cuối cùng trong ba bước, và là bước đa dạng nhất. Tại thời điểm này, kênh trao đổi bản thân nó đã được bảo mật. Mỗi định danh và truy nhập của người sử dụng có thể được cung cấp theo rất nhiều cách khác nhau. Chẳng hạn, kiểu chứng thực rhosts có thể được sử dụng, nhưng không phải là mặc định; nó đơn giản chỉ kiểm tra định danh của máy khách được liệt kê trong file rhost (theo DNS và địa chỉ IP). Việc chứng thực mật khẩu là một cách rất thông dụng để định danh người sử dụng, nhưng ngoài ra cũng có các cách khác: chứng thực RSA, sử dụng ssh-keygen và ssh-agent để chứng thực các cặp khoá.

1.7. IPSEC

Trong hệ thống Windows Server 2003 không hỗ trợ một công cụ riêng cấu hình IPSec, do đó để triển khai IPSec chúng ta dùng các công cụ thiết lập chính sách dành cho máy cục bộ hoặc dùng cho miền. Để mở công cụ cấu hình IPSec bạn nhấp chuột vào Start => Run rồi gõ secpol.msc hoặc nhấp chuột vào Start =>Programs =>Administrative Tools =>Local Security Policy, trong công cụ đó bạn chọn IP Security Policies on Local Machine.

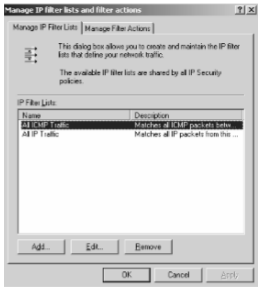
Tóm lại, các điều mà bạn cần nhớ khi triển khai IPSec: - B ạn triển khai IPSec trên Windows Server 2003 thông qua các chính sách, trên một máy tính bất kỳ nào đó vào tại một thời điểm thì chỉ có một chính sách IPSec được hoạt động. - M ỗi chính sách IPSec gồm một hoặc nhiều qui tắc (rule) và một phương pháp chứng thực nào đó. Mặc dù các qui tắc permit và block không dùng đến chứng thực nhưng Windows vẫn đòi bạn chỉ định phương pháp chứng thực. - IPSec cho phép bạn chứng thực thông qua Active Directory, các chứng chỉ PKI hoặc một khóa được chia sẻ trước. - M ỗi qui tắc (rule) gồm một hay nhiều bộ lọc (filter) và một hay nhiều tác động bảo mật (action). - Có bốn tác động mà qui tắc có thể dùng là: block, encrypt, sign và permit.

Các chính sách IPSec tạo sẵn. Trong khung cửa sổ chính của công cụ cấu hình IPSec, bên phải chúng ta thấy xuất hiện ba chính sách được tạo sẵn tên là: Client, Server và Secure. Cả ba chính sách này đều ở trạng thái chưa áp dụng (assigned). Nhưng chú ý ngay cùng một thời điểm thì chỉ có thể có một chính sách được áp dụng và hoạt động, có nghĩa là khi bạn áp dụng một chính sách mới thì chính sách đang hoạt động hiện tại sẽ trở về trạng thái không hoạt động. Sau đây chúng ta sẽ khảo sát chi tiết ba chính sách tạo sẵn này. - Client (Respond Only): chính sách qui định máy tính của bạn không chủ động dùng IPSec trừ khi nhận được yêu cầu dùng IPSec từ máy đối tác. Chính sách này cho phép bạn có thể kết nối được cả với các máy tính dùng IPSec hoặc không dùng IPSec. - Server (Request Security): chính sách này qui định máy server của bạn chủ động cố gắng khởi tạo IPSec mỗi khi thiết lập kết nối với các máy tính khác, nhưng nếu máy client không thể dùng IPSec thì Server vẫn chấp nhận kết nối không dùng IPSec. - Secure Server

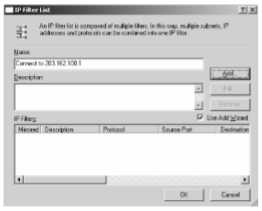
(Require Security): chính sách này qui định không cho phép bất kỳ cuộc trao đổi dữ liệu nào với Server hiện tại mà không dùng IPSec.

Ví dụ tạo chính sách IPSec đảm bảo một kết nối được mã hóa.

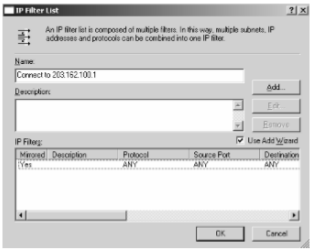
Trong phần này chúng ta bắt tay vào thiết lập một chính sách IPSec nhằm đảm bảo một kết nối được mã hóa giữa hai máy tính. Chúng ta có hai máy tính, máy A có địa chỉ 203.162.100.1 và máy B có địa chỉ 203.162.100.2. Chúng ta sẽ thiết lập chính sách IPSec trên mỗi máy thêm hai qui tắc (rule), trừ hai qui tắc của hệ thống gồm: một qui tắc áp dụng cho dữ liệu truyền vào máy và một qui tắc áp dụng cho dữ liệu truyền ra khỏi máy. Ví dụ qui tắc đầu tiên trên máy A bao gồm: - B ộ lọc (filter): kích hoạt qui tắc này khi có dữ liệu truyền đến địa chỉ 203.162.100.1, qua bất kỳ cổng nào. - Tác động bảo mật (action): mã hóa dữ liệu đó. - Chứng thực: chìa khóa chia sẻ trước là chuỗi “quantri”. Qui tắc thứ hai áp dụng cho máy A cũng tương tự nhưng bộ lọc có nội dung ngược lại là “dữ liệu truyền đi từ địa chỉ 203.162.100.1”. Chú ý: cách dễ nhất để tạo ra một qui tắc là trước tiên bạn phải qui định các bộ lọc và tác động bảo mật, rồi sau đó mới tạo ra qui tắc từ các bộ lọc và tác động bảo mật này. Các bước để thực hiện một chính sách IPSec theo yêu cầu như trên: Trong công cụ Domain Controller Security Policy, bạn nhấp phải chuột trên mục IP Security Policies on Active Directory, rồi chọn Manage IP filter lists and filter actions.



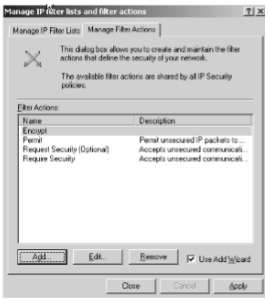
Hộp thoại xuất hiện, bạn nhấp chuột vào nút add để thêm một bộ lọc mới. Bạn nhập tên cho bộ lọc này, trong ví dụ này chúng ta đặt tên là “Connect to 203.162.100.1”. Bạn nhấp chuột tiếp vào nút Add để hệ thống hướng dẫn bạn khai báo các thông tin cho bộ lọc.



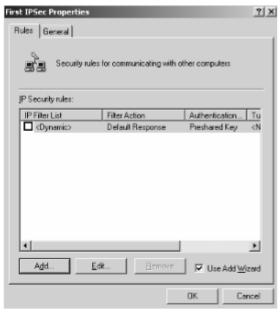
Bạn theo hướng dẫn của hệ thống để khai báo các thông tin, chú ý nên đánh dấu vào mục Mirrored để qui tắc này có ý nghĩa hai chiều bạn không phải tốn công để tạo ra hai qui tắc. Mục Source address chọn My IP Address, mục Destination address chọn A specific IP Address và nhập địa chỉ "203.162.100.1" vào, mục IP Protocol Type bạn để mặc định. Cuối cùng bạn chọn Finish để hoàn thành phần khai báo, bạn nhấp chuột tiếp vào nút OK để trở lại hộp thoại đầu tiên.



Tiếp theo bạn chuyển sang Tab Manage Filter Actions để tạo ra các tác động bảo mật. Bạn nhấp chuột vào nút Add hệ thống sẽ hướng dẫn bạn khai báo các thông tin về tác động. Trước tiên bạn đặt tên cho tác động này, ví dụ như là Encrypt.Tiếp tục trong mục Filter Action bạn chọn Negotiate security, trong mục IP Traffic Security bạn chọn Integrity and encryption. Đến đây bạn đã hoàn thành việc tạo một tác động bảo mật.

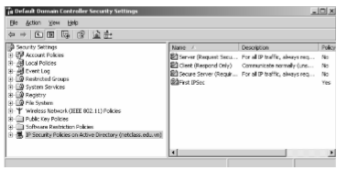


Công việc tiếp theo là bạn một chính sách IPSec trong đó có chứa một qui tắc kết hợp giữa bộ lọc và tác động vừa tạo ở phía trên. Trong công cụ Domain Controller Security Policy, bạn nhấp phải chuột trên mục IP Security Policies on Active Directory, rồi chọn Create IP Security Policy, theo hướng dẫn bạn nhập tên của chính vào, ví dụ là First IPSec, tiếp theo bạn phải bỏ đánh dấu trong mục Active the default response rule. Các giá trị còn lại bạn để mặc định vì qui tắc Dynamic này chúng ta không dùng và sẽ tạo ra một qui tắc mới.



Trong hộp thoại chính sách IPSec, bạn nhấp chuột vào nút Add để tạo ra qui tắc mới. Hệ thống sẽ hướng dẫn bạn từng bước thực hiện, đến mục chọn bộ lọc bạn chọn bộ lọc vừa tạo phía trên tên "Connect to 203.162.100.1", mục chọn tác động bạn chọn tác động vừa tạo tên Encypt. Đến mục chọn phương pháp chứng thực bạn chọn mục Use this string to protect the key exchange và nhập chuỗi làm khóa để mã hóa dữ liệu vào, trong ví dụ này là "quantri".

Đến bước này thì công việc thiết lập chính sách IPSec theo yêu cầu trên của bạn đã hoàn thành, trong khung của sổ chính của công cụ Domain Controller Security Policy, bạn nhấp phải chuột lên chính sách First IPSec và chọn Assign để chính sách này được hoạt động trên hệ thống Server.



1.8. Tính dễ bị tổn thương

2. Email

Thư điện tử, hay **email** (từ chữ *electronic mail*), đôi khi được dịch không chính xác là *điện thư*, là một hệ thống chuyển nhận thư từ qua các mạng máy tính.

Email là một phương tiện thông tin rất nhanh. Một mẫu thông tin (thư từ) có thể được gửi đi ở dạng mã hoá hay dạng thông thường và được chuyển qua các mạng máy tính đặc biệt là mạng Internet. Nó có thể chuyển mẫu thông tin từ một máy nguồn tới một hay rất nhiều máy nhận trong cùng lúc.

Ngày nay, email chẳng những có thể truyền gửi được chữ, nó còn có thể truyền được các dạng thông tin khác như hình ảnh, âm thanh, phim, và đặc biệt các phần mềm thư điện tử kiểu mới còn có thể hiển thị các email dạng sống động tương thích với kiểu tệp HTML.

Phần mềm thư điện tử (*email software*) là loại phần mềm nhằm hỗ trợ cho người dùng việc chuyển và nhận các mẫu thông tin (thường là dạng chữ). Thông tin có thể đưa vào phần mềm thư điện tử bằng cách thông dụng nhất là gõ chữ bàn phím hay cách phương cách khác ít dùng hơn như là dùng máy quét hình (*scanner*), dùng máy ghi hình số (*digital camera*) đặc biệt là các Web cam. Phần mềm thư điện tử giúp đỡ cho việc tiến hành soạn thảo, gửi, nhận, đọc, in, xoá hay lưu giữ các (điện) thư. Có hai trường hợp phân biệt phần mềm thư điện tử là

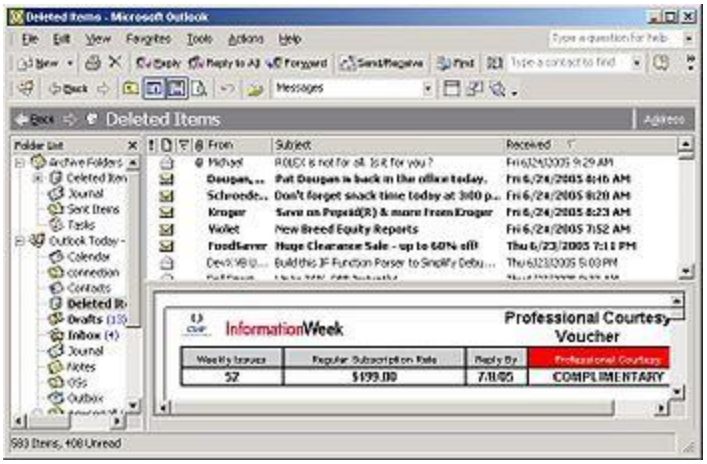
- Loại phần mềm thư điện tử được cài đặt trên từng máy tính của người dùng gọi là **email client**, hay **phần mềm thư điện tử (cho) máy khách**. Các ví dụ loại phần mềm này bao gồm: Microsoft Outlook, Microsoft Outlook Express, Netscape Comunicator, hay Eudora. Phần mềm thư điện tử này còn có tên là **MUA** (từ chữ *mail user agent*) tức là **Tác nhân sử dụng thư**. Một cách gọi tên thông dụng khác của email client là **ứng dụng thư điện tử** (*email application*) nếu không bị nhầm lẫn

- Ngược lại, loại phần mềm thư điện tử không cần phải cài đặt mà nó được cung ứng bởi các máy chủ (*web server*) trên Internet gọi là **WebMail**, hay **Phần mềm thư điện tử qua Web**. Để dùng được các phần mềm loại này thường các máy tính nối vào phải có một máy truy cập tương thích với sự cung ứng của WebMail. Ví dụ loại này là mail.Yahoo.com, hay hotmail.com.

Nơi cung ứng phần mềm cũng như phương tiện chuyển thư điện tử gọi là **nhà cung ứng dịch vụ thư điện tử** (*email sevice provider*).

Máy tính làm việc cung ứng các dịch vụ thư điện tử là **MTA** (từ chữ *mail transfer agent*) hay là **đại lý chuyển thư**. Vì đây là máy chủ nên khi không bị nhầm lẫn với các loại máy chủ khác thì người ta cũng gọi MTA là **máy chủ** hay rõ hơn là máy chủ thư điện tử.

Các dịch vu thư điện tử có thể được cung ứng miễn phí hay có lệ phí tuỳ theo nhu cầu và mục đích của người dùng. Ngày nay, email thường được cung cấp kèm với các phương tiện Internet khi người tiêu dùng ký hợp đồng với các dịch vụ Internet một cách miễn phí.



3. WEB

3.1. SSL/TLS

SSL viết tắt của Secure Socket Layer là một **giao thức** (protocol) cho phép bạn truyền đạt thông tin một cách bảo mật và an toàn qua mạng. Việc kết nối giữa một Web browser tới bất kỳ điểm nào trên mạng Internet đi qua rất nhiều các hệ thống độc lập mà không có bất kỳ sự bảo vệ nào với các thông tin trên đường truyền.

TLS (tiếng Anh: Transport Layer Security: "Bảo mật tầng truyền tải"), cùng với SSL (Secure Sockets Layer: "Tầng ổ bảo mật") dẫn trước, là các giao thức mật mã nhằm mục đích bảo mật sự vận chuyển trên Internet.

3.2. HTTP / S

HTTPS, viết tắt của Hypertext Transfer Protocol Secure, là một giao thức kết hợp giữa giao thức HTTP và giao thức bảo mật SSL hay TLS cho phép trao đổi thông tin một cách bảo mật trên Internet.

3.3. Tính dễ bị tổn thương

3.4. Tính dễ bị tổn thương

4. File Transfer

4.1. S / FTP

sFTP (viết tắt của từ Secure File Transfer Protocol, hoặc SSH File Transfer Protocol) là một **giao thức** mạng giúp bạn có thể upload hoặc download dữ liệu trên máy chủ

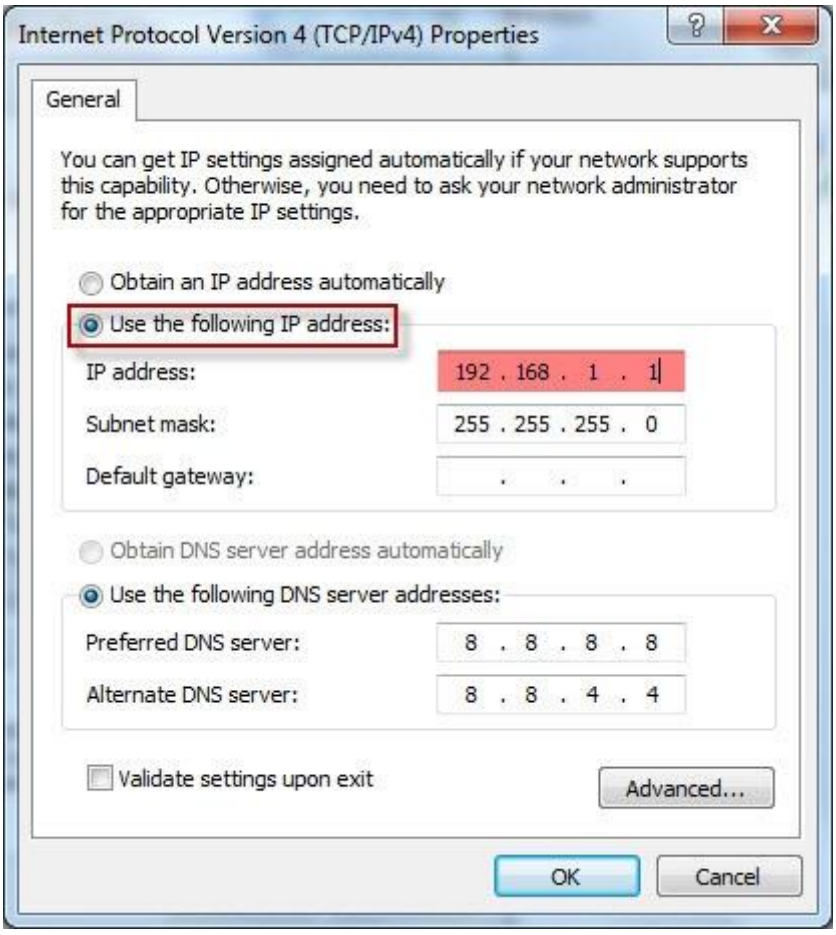
4.2. Blind FTP / Giấu tên

Giao thức giấu tên FTP

4.3. Chia sẻ File

Trong Windows 7, bạn có thể dễ dàng thực hiện chia sẻ một thư mục hay ổ đĩa bất kỳ, bằng cách nhấn chuột phải vào nó, chọn Properties > chọn thẻ Sharing > nhấn vào Advanced Sharing. Có thể chọn nhanh hơn bằng cách nhấn chuột phải, rồi chọn trong mục Share with…

Trên cửa sổ hiện ra, đánh dấu chọn vào Share this folder để chia sẻ.
Tuy nhiên, mặc định việc chia sẻ chỉ cho phép người khác đọc dữ liệu chứ không thể xóa hay thêm dữ liệu vào máy tính của bạn. Bạn có thể cấp thêm những quyền đã được giới hạn này cho người khác bằng cách nhấn vào Permisssion, đánh dấu vào Full Control.
Khuyến cáo: Chỉ nên thực hiện việc mở rộng quyền truy cập này khi bạn là người thao tác trên máy tính kia nhằm tự quản lý dữ liệu của mình. Sau khi không cần dùng nữa thì nên tắt ngay để tránh mất hay lộ dữ liệu.
Tính năng chia sẻ trên Windows 7 cho phép được bảo mật cao hơn với cơ chế 128-bit. Mặc định thì Windows đã thiết đặt chế độ này. Tuy nhiên, nếu tùy chọn đã bị thay đổi bởi ai đó, vào Start > chọn Control Panel > mở Network and Sharing Center. Sau đó, chọn thẻ Change advanced sharing setttings và tùy chọn ở mục File sharing connections.



Rất nhiều trường hợp người dùng không thể truy cập dữ liệu của nhau, dù đã thực hiện chia sẻ đầy đủ quyền. Hiện tượng là sẽ gặp thông báo nhập Username vàPassword truy cập. Nguyên nhân đơn giản là do máy chứa dữ liệu cần truy cập có tạo mật khẩu đăng nhập cho tài khoản quản trị đang dùng. Vì vậy, nếu gặp thông báo như hiện tượng trên thì bạn hãy nhập tên tài khoản và mật khẩu của tài khoản đang mở trên máy chứa dữ liệu. Còn một cách khác là chọn Turn off password protected sharing ở mục Password protected sharing.

Trường hợp hai hay nhiều máy kết nối ngang hàng với nhau thông qua thiết bị trung gian là modem để kết nối Internet nhưng đường truyền bị hỏng, và bạn muốn các máy tính thấy nhau trong mạng LAN, thì cần phải thiết lập IP tĩnh như sau. Bạn vào Network Connection Center như đã hướng dẫn ở trên, chọn Change adapter settings, nhấn chuột phải vào biểu tượng Local Area Connection, chọnProperties.

Trong danh sách this connection users the following items, nhấn đôi chuột vàoInternet Protocol Version 4 (TCP/IPv4), chọn thẻ General. Sau đó, đánh dấu chọn vào Use the following IP address, nhập vào ô IP address một chuỗi các số liên tiếp trong 4 khoảng trống lần lượt là 192.168.1.x (x là con số theo thứ tự các máy đang kết nối trong mạng LAN, mỗi máy sẽ sử dụng một giá trị khác nhau, nhưng nên liên tiếp cho dễ nhớ). Ô Subnet mask sẽ tự động được điền giá chuỗi225.225.225.0 , bạn cứ để mặc định như vậy. Ví dụ: với mạng LAN 3 máy thì 3 chuỗi IP là 192.168.1.1; 192.168.1.2; 192.168.1.3.

4.4. Tính dễ bị tổn thương

4.5. Packet Sniffing

Packet Sniffer hay Protocol Analyzer **là** những công cụ được sử dụng để chuẩn đoán và phát hiện lỗi hệ thống mạng và các vấn đề liên quan. Các Hacker sử dụng **Packet Sniffer** với mục đích nghe trộm trên những dữ liệu chưa được mã hóa và xem những thông tin được trao đổi giữa 2 bên

5. Thiết bị

5.1. Firewall

Tường lửa (**Firewall**) **là** một bức rào chắn giữa mạng nội bộ (local network) với một mạng khác (chẳng hạn như Internet), điều khiển lưu lượng ra vào giữa hai mạng này. ... Do đó, việc thiết lập tường lửa **là** hết sức quan trọng, đặc biệt **là** đối với những máy tính thường xuyên kết nối internet.

5.2. Router

Router, hay thiết bị định tuyến hoặc bộ định tuyến, **là** một thiết bị mạng máy tính dùng để chuyển các gói dữ liệu qua một liên mạng và đến các đầu cuối, thông qua một tiến trình được gọi **là** định tuyến. Định tuyến xảy ra ở tầng 3 tầng mạng của mô hình OSI 7 tầng.

Là thiết bị trung gian dùng để nối kết mạng nội bộ bên trong và mạng bên ngoài. Nó có chức năng kiểm soát tất cả các luồng dữ liệu đi ra và vào mạng nhằm ngăn chặn hacker tấn công. Gateway cũng hỗ trợ chuyển đổi giữa các giao thức khác nhau, các chuẩn dữ liệu khác nhau (ví dụ IP/IPX). Proxy giống như một firewall (bức tường lửa), nâng cao khả năng bảo mật giữa mạng nội bộ bên trong và mạng bên ngoài. Proxy cho phép thiết lập các danh sách được phép truy cập vào mạng

nội bộ bên trong, cũng như danh sách các ứng dụng mà mạng nội bộ bên trong có thể truy cập ra mạng bên ngoài. Ngoài ra Proxy còn là máy đại điện cho các máy trạm bên trong mạng nội bộ truy cập ra Internet, đây là chức năng quan trọng nhất của Proxy.

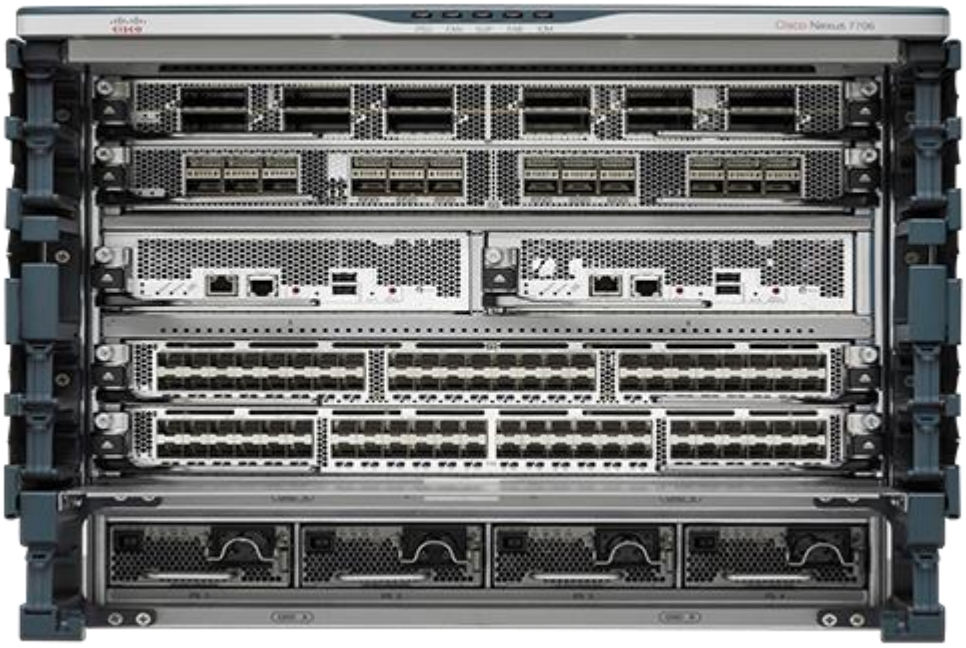
5.3. Switch

Switch (tiếng Anh), hay còn gọi là **thiết bị chuyển mạch**, là một thiết bị dùng để kết nối các đoạn mạng với nhau theo mô hình mạng hình sao (*star*). Theo mô hình này, switch đóng vai trò là thiết bị trung tâm, tất cả các máy tính đều được nối về đây.

- Làm việc như một Bridge nhiều cổng. Khác với HUB nhận tín hiệu từ một cổng rồi chuyển tiếp tới tất cả các cổng còn lại, switch nhận tín hiệu vật lý, chuyển đổi thành dữ liệu, từ một cổng, kiểm tra địa chỉ đích rồi gửi tới một cổng tương ứng.

Hỗ trợ công nghệ Full Duplex dùng để mở rộng băng thông của đường truyền mà không có repeater hoặc Hub nào dùng được

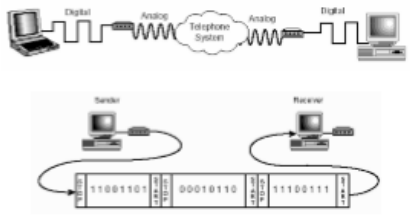
Trong mô hình tham chiếu OSI, switch hoạt động ở tầng liên kết dữ liệu, ngoài ra có một số loại switch cao cấp hoạt động ở tầng mạng.



5.4. Modem không dây

Là thiết bị dùng để nối hai máy tính hay hai thiết bị ở xa thông qua mạng điện thoại. Modem thường có hai loại: internal (là loại được gắn bên trong máy tính giao tiếp qua khe cắm ISA hoặc PCI), external (là loại thiết bị đặt bên ngoài CPU và giao tiếp với CPU thông qua cổng COM theo chuẩn RS-232). Cả hai loại trên đều có cổng giao tiếp RJ11 để nối với dây điện thoại. Chức năng của Modem là

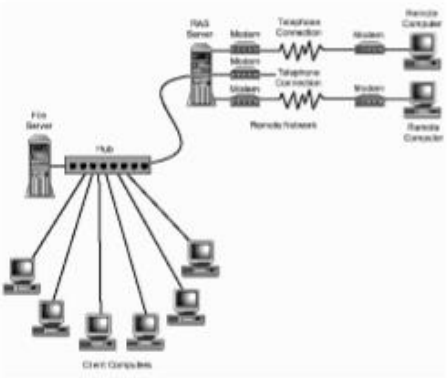
chuyển đổi tín hiệu số (digital) thành tín hiệu tương tự (analog) để truyền dữ liệu trên dây điện thoại. Tại đầu nhận, Modem chuyển dữ liệu ngược lại từ dạng tín hiệu tương tự sang tín hiệu số để truyền vào máy tính. Thiết bị này giá tương đối thấp nhưng mang lại hiệu quả rất lớn. Nó giúp nối các mạng LAN ở xa với nhau thành các mạng WAN, giúp người dùng có thể hòa vào mạng nội bộ của công ty một cách dễ dàng dù người đó ở nơi nào



Hình 4.24 – Mô hình truyền dữ liệu thông qua **Modem**.

5.5. RAS

Remote Access Services (RAS): là một dịch vụ mềm trên một máy tính hoặc là một dịch vụ trên thiết bị phần cứng. Nó cho phép dùng Modem để nối kết hai mạng LAN với nhau hoặc một máy tính vào mạng nội bộ.



Hình 4.25 – Sử dụng **RAS** để liên lạc.

5.6. Telecomm / PBX

PBX là tên viết tắt của cụm từ tiếng Anh Private Branch Exchange (Tổng đài Nhánh Riêng), **là** một mạng điện thoại riêng được sử dụng trong phạm vi một công ty. Những người sử dụng hệ thống điện thoại **PBX** dùng chung một số đường điện thoại ngoài để thực hiện các cuộc gọi ra bên ngoài.

5.7. VPN

VPN (virtual private network) **là** công nghệ xây dựng hệ thống mạng riêng ảo nhằm đáp ứng nhu cầu chia sẻ thông tin, truy cập từ xa và tiết kiệm chi phí. ...**VPN** cho phép các máy tính truyền thông với nhau thông qua một môi trường chia sẻ như mạng Internet nhưng vẫn đảm bảo được tính riêng tư và bảo mật dữ liệu.

5.8. IDS

IDS (Hệ thống phát hiện xâm phạm) **là** một hệ thống phòng chống, nhằm phát hiện các hành động tấn công vào một mạng. Mục đích của nó **là** phát hiện và ngăn ngừa các hành động phá hoại đối với vấn đề bảo mật hệ thống, hoặc những hành động trong tiến trình tấn công như sưu tập, quét các cổng

5.9. Chẩn đoán / Theo dõi mạng

Khởi động lại thiết bị

Một trong những cách đơn giản và dễ dàng nhất để khắc phục vấn đề trên mọi thiết bị công nghệ từ máy tính để bàn, máy tính bảng cho đến smartphone đó chính là khởi động lại thiết bị. Trong nhiều trường hợp, thao tác này có thể khắc phục được nhiều lỗi hệ thống của thiết bị vốn đang bị treo, không hồi đáp hay bị quá tải. Ngoài việc thử khởi động lại máy tính, bạn cũng nên khởi động lại modem và router trong mạng. Lưu ý là bạn nên đợi ít nhất vài phút trước khi mở trở lại để modem và router có thể xóa hẳn bộ nhớ cache.

Sau khi khởi động lại máy tính cũng như các thiết bị trong hệ thống mạng, bạn có thể thử truy cập vào Internet bằng chính thiết bị đó. Nếu vẫn không được, hãy thử bằng máy tính khác hoặc một thiết bị di động sẵn có nào đó. Nếu vẫn không được thì giờ đây bạn có thể khoanh vùng lỗi xuất hiện từ các thiết bị mạng hay từ đường truyền của nhà cung cấp mạng ISP.

Trong trường hợp máy tính hoặc thiết bị di động khác có thể truy cập mạng thì vấn đề nằm ở chiếc máy tính của bạn. Nếu rơi vào trường hợp đó, bạn nên thử tải về các phần mềm diệt virus để kiểm tra xem máy có bị dính mã độc nào hay không, hoặc có thể dùng một trình duyệt khác để mở trang web.

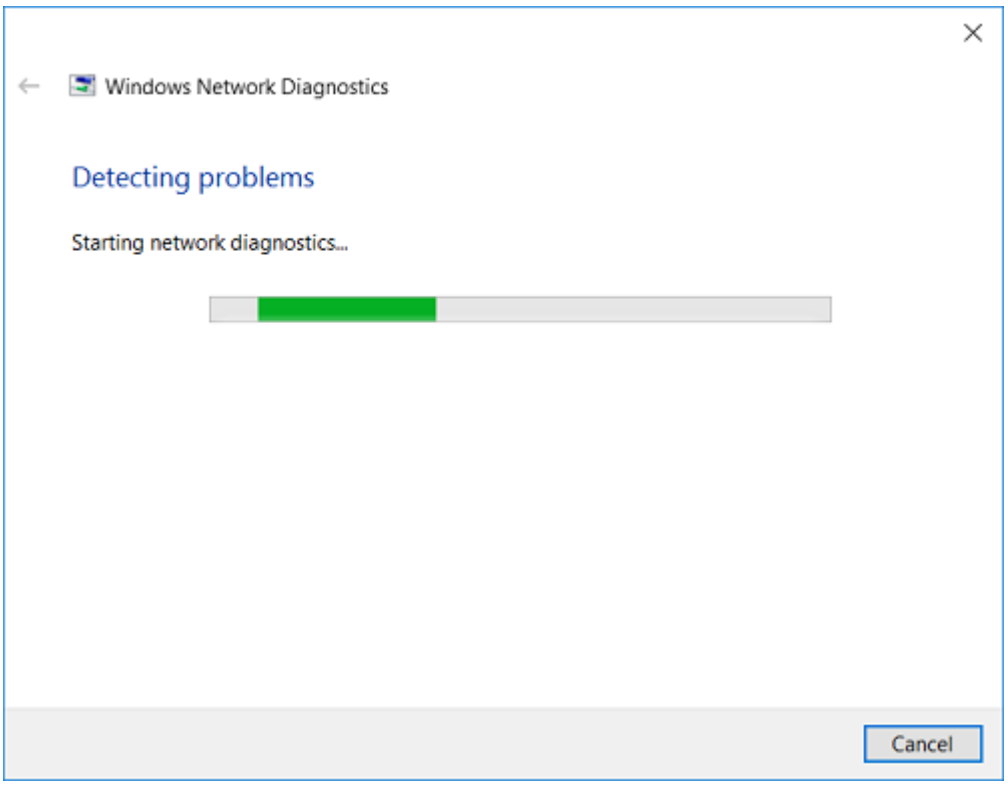
Kiểm tra kết nối

Khi đã khởi động lại máy tính và các thiết bị trong hệ thống mạng mà vẫn không khắc phục được lỗi. Điều tiếp theo bạn cần làm là kiểm tra lại kết nối vật lý giữa thiết bị và nơi phát tín hiệu mạng. Trường hợp bạn đang sử dụng cáp Ethernet để kết nối máy tính với router, hãy kiểm tra để đảm bảo rằng nó đang được gắn chắc chắn và không bị ai đó tháo ra. Nếu laptop của bạn có tích hợp công tắc chuyển đổi vật lý để bật/tắt chế độ kết nối không dây Wi-Fi thì hãy chắc rằng nó không bị chuyển sang chế độ OFF.

Một khi đã kiểm tra kết nối, hãy xem qua tình trạng của các thiết bị mạng. Bạn cần kiểm tra xem đèn tín hiệu trên router và modem có nhấp nháy màu xanh như bình thường không? Nếu không thấy thì có thể thiết bị này đã bị hỏng. Hoặc nếu thấy đèn tín hiệu chuyển sang màu đỏ hay đèn tín hiệu nguồn điện sáng nhưng không có kết nối, rất có thể đường truyền từ nhà mạng ISP của bạn có vấn đề.

Chạy trình Network Troubleshooter

Ngoài hai cách kể trên thì bạn cũng có thể kiểm tra lỗi hệ thống mạng bằng cách sử dụng công cụ gỡ rối (Troubleshooter) được tích hợp sẵn trên hệ điều hành Windows. Công cụ này sẽ tự động tìm và sửa chữa nhiều vấn đề liên quan đến hệ thống, ổ đĩa hay kết nối mạng. Để khởi chạy trình gỡ rối này, bạn hãy nhấn chuột phải vào biểu tượng Network trong khay hệ thống của Windows rồi chọn Troubleshooter Problems.



Khi trình gỡ rối này chạy xong, có thể xuất hiện nhiều trường hợp như: tìm thấy và khắc phục được vấn đề, tìm thấy vấn đề nhưng không giải quyết được hay không tìm thấy bất cứ vấn đề nào.

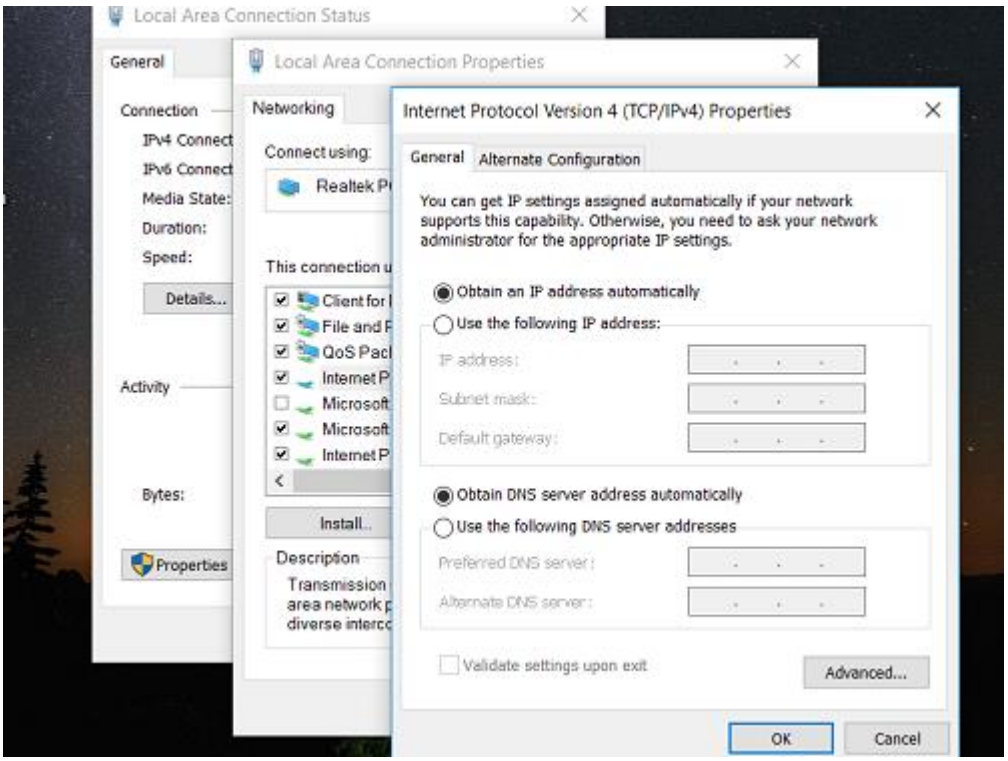
Nếu trình Troubleshoot phát hiện được vấn đề và có thể sửa lỗi, hãy thử kết nối lại ngay sau đó. Nếu bạn nhận được thông báo lỗi với thông báo tên cụ thể nhưng Windows không thể sửa chữa được thì có thể lưu lại và tìm cách khắc phục được bổ biến trên các diễn dàn và trang công nghệ uy tín.

Kiểm tra địa chỉ IP hợp lệ

Nếu đã thử các cách trên mà vẫn không vào được mạng, có thể xác định rằng vấn đề không phải là tạm thời và nó có liên quan đến phần cứng. Do Windows không thể khắc phục vấn đề này, chúng ta phải tự xác định nguyên nhân và tìm cách giải quyết.

Một trong những nguyên nhân thường gặp nhất khi rơi vào tình huống này đó chính là địa chỉ IP chưa chính xác. Do đó, bạn cần kiểm tra xem máy tính của mình đã được gán IP hợp lệ từ modem hay router hay chưa.

Để kiểm tra điều đó, bạn hãy gõ cụm từ Network and Sharing Centrer vào Start Menu để mở quản lý kết nối mạng. Ở bên phải, bạn sẽ thấy mục Connectios và nhấn vào liên kết có tên của kết nối mạng có dây hoặc Wi-Fi. Trong cửa sổ trạng thái của kết nối đã chọn, hãy nhấn vào nút Properties trong phần Activity và tiếp theo nhấn đúp vào Internet Protocol Version 4 (TCP/IP v4).



Hãy đảm bảo rằng các tùy chọn "Obtain an IP address automatically" và "Obtain DNS server address automatically" đang được đánh dấu. Khi đó, hệ thống sẽ tự động được gán IP từ modem hoặc router một cách chính xác. Bạn có thể lặp lại các bước tương tự với địa chỉ IPv6 ở phần Internet Protocol Version 6 (TCP/IP v6).

Sau khi đã thực hiện các bước thiết lập trên, bạn nên kiểm tra thêm lần nữa để chắc chắn rằng máy tính đang được router cấp một địa chỉ IP hợp lệ. Để làm điều này, bạn hãy mở giao diện dòng lệnh Windows và gõ cmd vào Start Menu. Tiếp đó, bạn gõ lệnh ipconfig và tìm thông tin bên dưới phần Ethernet adapter (đối với kết nối có dây) hoặc Wireless LAN Adapter (đối với kết nối không dây).

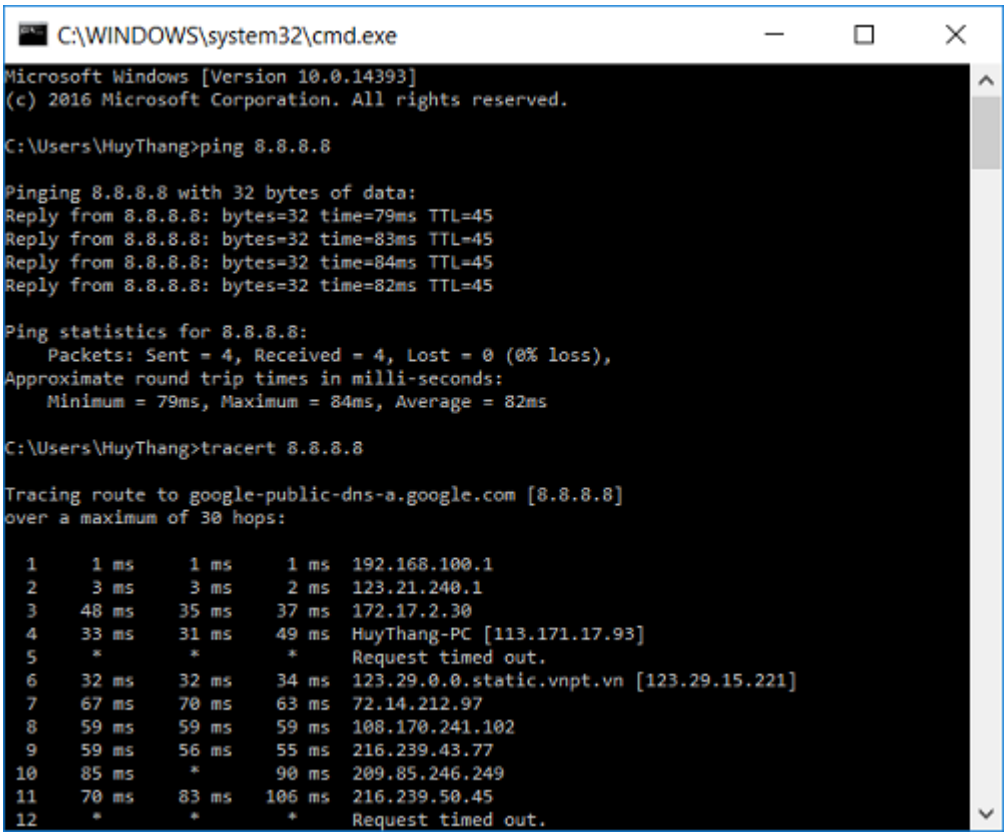
Nếu địa chỉ IPv4 có dạng 169.x.x.x có nghĩa là máy tính của bạn chưa được router cấp IP mà chỉ nhận được địa chỉ IP cục bộ của hệ điều hành. Hãy thử gõ lần lượt hai lệnh dưới đây trong giao diện cmd để giải quyết vấn đề: ipconfig/release và ipconfig/renew. Sau đó, nếu máy tính vẫn có địa chỉ IP dạng 169.x.x.x kho gõ các lệnh trên, hãy thử gắn dây mạng kết nối máy tính truwcjt iếp vào modem và xem có mạng Internet vào được không. Nếu vào được tức là router của bạn có vấn đề.

Chạy lệnh Ping và Tracet

Nếu địa chỉ IP bắt đầu bằng chuỗi số khác dạng 169.x.x.x khi chạy lệnh ipconfig theo hướng dẫn trên, điều đó có nghĩa là máy tính của bạn đã nhận được IP hợp lệ từ router và vấn đề có thể xảy ra giữa router và mạng Internet.

Để xác định lỗi này, bạn hãy thử gõ lệnh ping 8.8.8.8 đến các máy chủ DNS của Google để kiểm tra xem máy tính có thể kết nối được mạng hay không. Thao tác trên sẽ gửi 4 gói tin đến Google. Nếu thất bại, bạn sẽ nhận được thông báo gói tin gặp vấn đề trong khi gửi. Để biết thêm chi tiết, hãy gõ lệnh tracert 8.8.8.8 nhằm

theo dõi đường đi của từng gói tin này giữa máy tính của bạn đến máy chủ DNS của Google.



Mục đích của việc thực hiện các lệnh này này là giúp bạn theo dõi đường đi nước bước của các gói trên mà xem vấn đề nằm ở chỗ nào, trong mạng cục bộ hay ngoài mạng Internet.

Liên hệ nhà mạng ISP

Nếu đã hoàn thành tất cả các bước trên, kiểm tra các thiết bị đang hoạt động tốt, máy tính được gán địa chỉ IP hợp lệ từ bộ đính tuyết và xác định được vấn đề đang xuary ra bên ngoài mạng Internet, lựa chọn tốt nhất tiếp theo mà bạn nên làm là liên hệ ngay với nhà cung cấp mạng IPS để thông báo vấn đề.

5.10. Máy trạm

Máy trạm Workstation (còn gọi **là máy trạm**, **máy**tính **trạm**, **máy** tính workstation,...) **là** một **máy** tính dành cho cá nhân hay doanh nghiệp sử dụng có cấu hình mạnh hơn, chạy nhanh hơn được thiết kế dành để chạy các ứng dụng kỹ thuật hoặc khoa học và có nhiều khả năng hơn một **máy** tính cá nhân thông thường có thể kết nối với ...

5.11. Server

Server (máy chủ) **là** một hệ thống (phần mềm và phần cứng máy tính phù hợp) đáp ứng yêu cầu trên một mạng máy tính để cung cấp, hoặc hỗ trợ cung cấp một dịch vụ mạng. Các **server** có thể chạy trên một máy tính chuyên dụng, mà cũng

thường được gọi **là** "máy chủ", hoặc nhiều máy tính nối mạng có khả năng máy chủ lưu trữ

5.12. Thiết bị di động

- ổ cứng di động trong mạng

6. Phương tiện truyền thông

6.1. Coax

Là kiểu cáp đầu tiên được dùng trong các LAN, cấu tạo của cáp đồng trục gồm: - Dây dẫn trung tâm: dây đồng hoặc dây đồng bện. - M ột lớp cách điện giữa dây dẫn phía ngoài và dây dẫn phía trong. - Dây dẫn ngoài: bao quanh dây dẫn trung tâm dưới dạng dây đồng bện hoặc lá. Dây này có tác dụng bảo vệ dây dẫn trung tâm khỏi nhiễu điện từ và được nối đất để thoát nhiễu. - Ngoài cùng là một lớp vỏ plastic bảo vệ cáp.

Ưu điểm của cáp đồng trục: là rẻ tiền, nhẹ, mềm và dễ kéo dây. Cáp mỏng (thin cable/thinnet): có đường kính khoảng 6mm, thuộc họ RG-58, chiều dài đường chạy tối đa là 185 m. - Cáp RC-58, trở kháng 50 ohm dùng với Ethernet mỏng. - Cáp RC-59, trở kháng 75 ohm dùng cho truyền hình cáp. - Cáp RC-62, trở kháng 93 ohm dùng cho ARCnet.

6.2. UTP / STP

Cáp xoắn đôi có vỏ bọc chống nhiễu STP (Shielded Twisted- Pair). - G ồm nhiều cặp xoắn được phủ bên ngoài một lớp vỏ làm bằng dây đồng bện. Lớp vỏ này có tác dụng chống EMI từ ngoài và chống phát xạ nhiễu bên trong. Lớp vỏ bọc chống nhiễu này được nối đất để thoát nhiễu. Cáp xoắn đôi có bọc ít bị tác động bởi nhiễu điện và truyền tín hiệu xa hơn cáp xoắn đôi trần. - Chi phí: đắt tiền hơn Thinnet và UTP nhưng lại rẻ tiền hơn Thicknet và cáp quang. - T ốc độ: tốc độ lý thuyết 500Mbps, thực tế khoảng 155Mbps, với đường chạy 100m; tốc độ phổ biến 16Mbps (Token Ring). - Độ suy dần: tín hiệu yếu dần nếu cáp càng dài, thông thường chiều dài cáp nên ngắn hơn 100m. - Đầu nối: STP sử dụng đầu nối DIN (DB –9).

Cáp xoắn đôi không có vỏ bọc chống nhiễu UTP (Unshielded Twisted- Pair). Gồm nhiều cặp xoắn như cáp STP nhưng không có lớp vỏ đồng chống nhiễu. Cáp xoắn đôi trần sử dụng chuẩn 10BaseT hoặc 100BaseT. Do giá thành rẻ nên đã nhanh chóng trở thành loại cáp mạng cục bộ được ưu chuộng nhất. Độ dài tối đa của một đoạn cáp là 100 mét. Do không có vỏ bọc chống nhiễu nên cáp UTP dễ bị nhiễu khi đặt gần các thiết bị và cáp khác do đó thông thường dùng để đi dây trong nhà. Đầu nối dùng đầu RJ-45.

Cáp UTP có năm loại: - Loại 1: truyền âm thanh, tốc độ < 4Mbps. - Loại 2: cáp này gồm bốn dây xoắn đôi, tốc độ 4Mbps. - Loại 3: truyền dữ liệu với tốc độ lên đến 10 Mbps. Cáp này gồm bốn dây xoắn đôi với ba mắt xoắn trên mỗi foot (foot là đơn vị đo chiều dài, 1 foot = 0.3048 mét). - Loại 4: truyền dữ liệu, bốn cặp xoắn đôi, tốc độ đạt được 16 Mbps. - Loại 5: truyền dữ liệu, bốn cặp xoắn đôi, tốc độ 100Mbps. Cáp xoắn có vỏ bọc ScTP-FTP (Screened Twisted-pair). FTP là loại cáp lai tạo giữa cáp UTP và STP, nó hỗ trợ chiều dài tối đa 100m.

6.3. Fiber

Cáp quang có cấu tạo gồm dây dẫn trung tâm là sợi thủy tinh hoặc plastic đã được tinh chế nhằm cho phép truyền đi tối đa các tín hiệu ánh sáng. Sợi quang được tráng một lớp nhằm phản chiếu các tín hiệu. Cáp quang chỉ truyền sóng ánh sáng (không truyền tín hiệu điện) với băng thông rất cao nên không gặp các sự cố về nhiễu hay bị nghe trộm. Cáp dùng nguồn sáng laser, diode phát xạ ánh sáng. Cáp rất bền và độ suy giảm tín hiệu rất thấp nên đoạn cáp có thể dài đến vài km. Băng thông cho phép đến 2Gbps. Nhưng cáp quang có khuyết điểm là giá thành cao và khó lắp đặt. Các loại cáp quang: - Loại lõi 8.3 micron, lớp lót 125 micron, chế độ đơn. - Loại lõi 62.5 micron, lớp lót 125 micron, đa chế độ. - Loại lõi 50 micron, lớp lót 125 micron, đa chế độ. - Loại lõi 100 micron, lớp lót 140 micron, đa chế độ.

6.4. Phương tiện truyền thông có thể dời đi được

6.4.1 Băng từ

Cassette (còn được gọi **Compact Cassette** hoặc *phiên âm* **cát-xét**) là một thiết bị dùng để lưu trữ dữ liệu là tín hiệu hình ảnh hay âm thanh. Tại Việt Nam, khi nói đến Cassette, thường được nghĩ đến **băng nhạc Cassette**, xa hơn chút là nghĩ đến **máy Cassette**, và sau này là **băng Video Cassette**. Ra đời từ thập niên 60, phổ biến rộng từ cuối thập niên 70, trong gần 40 năm, Cassette đóng một vai trò quan trọng trong việc ghi âm và truyền bá âm nhạc, ra đời sau băng cối (ở Việt Nam còn gọi là *băng Akai*) và đĩa nhựa và chất lượng âm thanh không bằng nhưng Cassette được ứng dụng nhiều trong công nghệ thu-phát âm thanh và đạt được mức phổ biến cao hơn vì tiện lợi, nhỏ gọn và giá thành rẻ. Từ những năm 90, cùng với việc phát triển kỹ thuật số và sự ra đời những kỹ thuật ghi âm, ghi hình tân kỳ hơn, như dùng đĩa CD, DVD, do đó Cassette đã không còn được ưa chuộng nữa và dần dần chìm vào quên lãng.

6.4.2. CD-R

Đĩa CD (tiếng Anh: **Compact Disc**) là một trong các loại đĩa quang, chúng thường chế tạo bằng chất dẻo, đường kính 4,75 inch, dùng phương pháp ghi quang học để lưu trữ khoảng 80 phút âm thanh hoặc 700 MB dữ liệu máy tính đã được mã hóa theo kỹ thuật số.

6.4.3. Ổ cứng

Ổ đĩa cứng, hay còn gọi là **ổ cứng** (tiếng Anh: ***H**ard **D**isk **D**rive*, viết tắt: **HDD**) là thiết bị dùng để lưu trữ dữ liệu trên bề mặt các tấm đĩa hình tròn phủ vật liệu từ tính.

Ổ đĩa cứng là loại bộ nhớ "không thay đổi" (*non-volatile*), có nghĩa là chúng không bị mất dữ liệu khi ngừng cung cấp nguồn điện cho chúng.

Ổ đĩa cứng là một thiết bị rất quan trọng trong hệ thống bởi chúng chứa dữ liệu thành quả của một quá trình làm việc của những người sử dụng máy tính. Những sự hư hỏng của các thiết bị khác trong hệ thống máy tính có thể sửa chữa hoặc thay thế được, nhưng dữ liệu bị mất do yếu tố hư hỏng phần cứng của ổ đĩa cứng thường rất khó lấy lại được.

Ổ đĩa cứng là một khối duy nhất, các đĩa cứng được lắp ráp cố định trong ổ ngay từ khi sản xuất nên không thể thay thế được các "đĩa cứng" như với cách hiểu như đối với ổ đĩa mềm hoặc ổ đĩa quang.

6.4.4. Đĩa

Đĩa CD (tiếng Anh: **Compact Disc**) là một trong các loại đĩa quang, chúng thường chế tạo bằng chất dẻo, đường kính 4,75 inch, dùng phương pháp ghi quang học để lưu trữ khoảng 80 phút âm thanh hoặc 700 MB dữ liệu máy tính đã được mã hóa theo kỹ thuật số.

6.4.5. Flash Card

Flashcard hoặc **Flash Card** là loại thẻ mang thông tin (từ, số hoặc cả hai), được sử dụng cho việc học bài trên lớp hoặc trong nghiên cứu cá nhân. người dùng sẽ viết một câu hỏi ở mặt trước thẻ và một câu trả lời ở trang sau. Người ta thường dùng flashcard học từ vựng tiếng Anh rất hiệu quả. Ngoài ra có thể dùng flashcard để học ngày tháng năm lịch sử, công thức hoặc bất kỳ vấn đề gì có thể được học thông qua định dạng một câu hỏi và câu trả lời. Flashcard được sử dụng rộng rãi như một cách rèn luyện để hỗ trợ ghi nhớ bằng cách lặp đi lặp lại cách nhau

6.4.6. SmartCard

Thẻ thông minh, **thẻ gắn chip**, hay **thẻ tích hợp vi mạch** (**integrated circuit card -ICC**) là loại thẻ bỏ túi thường có kích thước của thẻ tín dụng, bên trong chứa một mạch tích hợp có khả năng lưu trữ và xử lý thông tin. Nó có thể đóng vai trò như thẻ căn cước, thực hiện việc xác thực thông tin, lưu trữ dữ liệu hay dùng trong các ứng dụng thẻ. Có hai loại thẻ thông minh chính. Các thẻ nhớ (*Memory card*) chỉ chứa các thành phần bộ nhớ bất biến(*non-volatile memory*), và có thể có một số chức năng bảo mật cụ thể. Thẻ vi xử lý chứa bộ nhớ khả biến(*volatile memory*) và các thành phần vi xử lý. Thẻ làm bằng nhựa, thường là PVC, đôi khi ABS. Thẻ có thể chứa một ảnh 3 chiều (*hologram*) để tránh các vụ lừa đảo.

Bài 4: Mật mã công khai mô hình ứng dụng

Mã bài: MD22-4

Giới thiệu: Bài 4 trình bày mật mã công khai mô hình ứng dụng.

Mục tiêu:

- Trình bày các giải thuật về mật mã;
- Trình bày mô hình khóa công khai trong hệ thống;
- Thiết kế được cơ sở hạ tầng khóa công khai;
- Chính xác, cẩn thận, tỉ mỉ, khoa học.

Nội dung chính:

1. Attacks

1.1. Weak Keys

Hacker có thể xâm nhập hệ thống dùng các kỹ thuật brute-force attacks, trojan horce, IP spoofing và packet sniffer.

Thường một cuộc tấn công brute-force attack được thực hiện dùng 1 chu trình chạy xuyên qua mạng và cố gắng xen vào chia sẻ môi trường. Khi hacker giành được quyền access đến một nguồn tài nguyên, hacker cùng với user cùng chia sẻ quyền lợi. Nếu như có đủ tài nguyên thì hacker sẽ tạo ra một của sổ kín cho lần access sau.

Hacker có thể làm thay đổi bảng định tuyến trong mạng. Điều đó sẽ làm chắc chắn rằng tất cả các gói tin sẽ được gởi đến hacker trước khi được gởi đến đích cuối cùng.

Trong một vài trường hợp, hacker có thể giám sát tất cả các traffic, thật sự trở thành một man in the middle.

Ta có thể hạn chế password attack bằng những cách sau:

Không cho phép user dùng cùng password trên các hệ thống.

Làm mất hiệu lực account sau một vài lần login không thành công. Bước kiểm tra này giúp ngăn chặn việc rà soát password nhiều lần.

Không dùng passwords dạng clear text: dùng kỹ thuật OTP hoặc mã hoá password như đã trình bày phần trên.

Dùng “strong” passwords: Dạng password này dùng ít nhất 8 ký tự, chứa các uppercase letters, lowercase letters, những con số và những ký tự đặc biệt.

1.2. Mathematical

Phương pháp tấn công toán học

1.3. Birthday

Tấn công Ngày sinh là một loại tấn công mật mã dựa trên sự khai thác vấn đề Ngày sinh(Birthday problem)- một hiện tượng xác suất tạo ra nghịch lý đối với cảm giác của con người, do vậy còn được gọi là "Nghịch lý Ngày sinh"(Birthday paradox).

Bài này phân tích và chứng minh hiện tượng nghịch lý trên cùng với mối liên hệ ứng dụng mật mã trong tấn công/phòng vệ tấn công. Cuối bài là một chương trình với mã nguồn thực thi, kèm theo các giải thích cần thiết. Kiến thức trong bài phần lớn là những kiến thức phổ thông cho nên các bạn sẽ hiểu được dễ dàng, chỉ cần tốt nghiệp phổ thông trung học(bằng thật, học thật). Bạn sẽ gặp thuận lợi đối với một vài chi tiết khác nếu bạn có trình độ tin học căn bản. Về phần chương trình thì bạn cần biết sơ qua về ngôn ngữ C++, bạn sẽ làm việc với hệ Unix/Linux nếu muốn thực hành chương trình. Còn lại khái niệm nào chưa được thông tin đầy đủ, chúng sẽ thuộc về chủ đề trọng tâm trong các bài sau.

Bài này cũng là cơ sở cho các khái niệm có thể gặp trong các bài sau có liên quan đến các vấn đề bí mật thông tin, các thuật toán mật mã, thuật toán mật mã không an toàn, tấn công tiền ảnh, tấn công tiền ảnh thứ hai, tấn công xung đột mạnh, chiến lược tìm kiếm, kỹ thuật mật mã khóa công khai, thực hành mã hóa và giải mã thông tin, thực hành ký kỹ thuật số, thực hành xác minh chữ ký kỹ thuật số, thực hành xác minh chứng chỉ thẩm định an ninh mạng**.**

Nếu bạn đang ở trong một nhóm người ngẫu nhiên trong một căn phòng với số người lớn hơn con số 23, bạn có thể cá cược với ai đó rằng có ít nhất một cặp hai người nào đó có trùng ngày sinh, và phần thắng sẽ nghiêng về bạn. Một năm không kể năm nhuận là có 365 ngày vì thế có 365 ngày sinh khác nhau, một con số lớn hơn nhiều so với 23 làm cho chúng ta có cảm giác đây là điều nghịch lý. Nhưng lý thuyết xác suất thống kê đã chỉ ra rằng với 23 người ngẫu nhiên thì xác suất có ít nhất hai người có trùng ngày sinh là 50%.

Gọi xác suất cần tính là P(A). Chúng ta giải bài toán ngược lại, tìm xác suất P(A') để 23 người ngẫu nhiên có ngày sinh hoàn toàn khác nhau.

Vì mỗi một người đều có thể có ngày sinh là một ngày trong 365 ngày của năm nên số khả năng về tình trạng ngày sinh của 23 người sẽ là chỉnh hợp lặp chập 23 của 365 phần tử

$$n^k = 365^{23}$$

Số khả năng thuận lợi là số bộ 23 ngày sinh mà không có cặp hai ngày sinh nào trùng nhau, đây chính là chỉnh hợp(không lặp) chập 23 của 365 phần tử

$$P(n,k) = \frac{n!}{(n-k)!} = \frac{365!}{(365-23)!}$$

Vậy xác suất P(A'), từ đó xác suất P(A) sẽ bằng

$$P(A') = \frac{P(n,k)}{n^k} = \frac{n!}{n^k(n-k)!} = \frac{365!}{365^{23}(365-23)!} \approx 0.4927\,(49.27\,\%)$$

$$P(A) = 1 - P(A') \approx 1 - 0.4927 = 0.5073\,(50.73\,\%)$$

Công thức tổng quát cho n người, xác suất p(n) để có ít nhất hai người trong n người ngẫu nhiên trùng ngày sinh sẽ là

$$p(n) = 1 - \frac{365!}{365^n(365-n)!}$$ **(*)**

Để thử kết quả, bạn dùng một tiện ích tính toán. 365! là một số rất lớn, có đến 778 chữ số 0, một chương trình tính toán bình thường không tính được. Bạn chạy chương trình kcalc, vào menu Settings, chọn chế độ khoa học(Science Mode)

2. Các thuật giải (Algorithms)

2.1. Cơ sở toán học

Các cấu trúc điều khiển, Các phép biến đổi từ số nguyên sang nhị phân, ngược lại.

Các thuật toán sắp xếp, tìm kiếm. Biểu diễn mảng, chuỗi.

Lệnh if:

Cú pháp: if (điều kiện) Phát_biểu1 ;
Biểu thức điều kiện được tính toán (trả trị 0: sai; 1: đúng)
Hoặc: if (biểu thức) Phát_biểu1;
else Phát_biểu2;

```
<!--
#include<stdio.h>
int Max3(int a, int b, int c)
{
        int max=a;
        if(max < b)
            max=b;
        if(max < c)
        max=c;
```

```
	return max;
}

void main()
{
	int kq = Max3(4,8,2);
	printf("max la: %d", kq);
}
-->
```

Lệnh switch

– Cú pháp :switch (biểu thức).
{
case N1 : lệnh 1; break;
case N2 : lệnh 2; break;
…..
[default : lệnh;]
}

switch case hay còn gọi là cấu trúc chọn. nếu biểu thức thỏa case 1 thì sẽ thực hiện khối lệnh 1 đồng thời sẽ thoát khỏi switch bằng lệnh break, nếu không thỏa thì cứ xuống dưới kiểm tra tiếp tục.

Ví dụ: Viết chương trình cho người dùng nhập 1,2 hoặc 3 và xuất thông báo tác vụ mà họ đã nhập.

```
<!--
#include<stdio.h>
void main()
{
    int Choice;
    printf("Ban go vao tac vu: 1, 2 hoac 3: \t");
```

```
    scanf("%d",&Choice);
    switch (Choice)
    {
        case 1 :
                    printf("Ban vua chon 1");
                    break;
        case 2 :
              printf("Ban vua chon 2");
              break;
        case 3 :
                  printf("Ban vua chon 2");
                  break;
             default:
                    printf("Ban da khong chon 1, 2 hoac 3");
                  break;
     }
}
-->
```

Kết luận:
Vậy là chúng ta đã hình dung được cấu trúc điều khiển, đây là các câu lệnh quan trọng mà C hoặc bất kỳ ngôn ngữ lập trình nào cũng trang bị. Nó được sử dụng rất nhiều trong lập trình.
Bài tập đề nghị:
.Tính điểm TB của 3 môn Toán, Lý, Hóa và xếp loại học lực:

- ĐTB<5: Yếu
- 5<=DTB<7: TB
- 7<=DTB<8: Khá
- 8<=DTB<9: Giỏi
- ĐTB>9: Xuất sắc

2.2. Hashing

Hàm băm (tiếng Anh: *hash function*) là giải thuật nhằm sinh ra các **giá trị băm** tương ứng với mỗi **khối dữ liệu** (có thể là một chuỗi ký tự, một đối tượng trong lập trình hướng đối tượng, v.v...). **Giá trị băm** đóng vai gần như một **khóa** để phân biệt các **khối dữ liệu**, tuy nhiên, người ta chấp **hiện tượng trùng khóa** hay còn gọi là đụng độ và cố gắng cải thiện giải thuật để giảm thiểu sự đụng độ đó. Hàm băm thường được dùng trong bảng băm nhằm giảm **chi phí tính toán** khi tìm một **khối dữ liệu** trong một tập hợp (nhờ việc so sánh các **giá trị băm** nhanh hơn việc so sánh những *khối dữ liệu* có kích thước lớn).

Vì tính thông dụng của bảng băm, ngày nay, đa số ngôn ngữ lập trình đều cung cấp thư viện ứng dụng bảng băm, thường gọi là thư viện collection trong đó có các vấn đề như: tập hợp (collection), danh sách (list), bảng(table), ánh xạ (mapping), từ điển (dictionary)). Thông thường, các lập trình viên chỉ cần viết hàm băm cho các đối tượng nhằm tích hợp với thư viện bảng băm đã được xây dựng sẵn.

Một hàm băm tốt phải thỏa mãn các điều kiện sau:

- Tính toán nhanh.
- Các khoá được phân bố đều trong bảng.
- Ít xảy ra đụng độ.
- Xử lý được các loại khóa có kiểu dữ liệu khác nhau.

2.3. Symmetric: RSA , Diffe-Hellman

Trong mật mã học, các **thuật toán khóa đối xứng** (*tiếng Anh: symmetric-key algorithms*) là một lớp các thuật toán mật mã hóa trong đó các khóa dùng cho việc mật mã hóa và giải mã có quan hệ rõ ràng với nhau (có thể dễ dàng tìm được một khóa nếu biết khóa kia). Mã khóa loại này không công khai.

Khóa dùng để mã hóa có liên hệ một cách rõ ràng với khóa dùng để giải mã có nghĩa chúng có thể hoàn toàn giống nhau, hoặc chỉ khác nhau nhờ một biến đổi đơn giản giữa hai khóa. Trên thực tế, các khóa này đại diện cho một bí mật được phân hưởng bởi hai bên hoặc nhiều hơn và được sử dụng để giữ gìn sự bí mật trong kênh truyền thông tin.

Nhiều thuật ngữ khác dành cho việc mã hóa dùng chìa khóa đối xứng bao gồm các phương pháp mã hóa **đơn khóa** (*single-key*), phương pháp mã hóa **một khóa** (*one-key*) và phương pháp mã hóa **khóa cá nhân** (*private-key*). Cách sử dụng thuật ngữ sau cùng đôi khi gây xung đột với thuật ngữ *khóa cá nhân* (*private-key*) dùng trong mật mã hóa khóa công khai (*public key cryptography*).

2.4. Asymmetric: DES , 3DES

Các hệ mật mã cổ điển đoợc giới thiệu trong choơng trojớc đều thuộc loại mật mã dòng (stream cipher), trong đó phép biển đổi mật mã thực hiện trên từng ký tự độc lập. Tuy nhiên ngày nay đoợc oịa chuộng sử dụng hơn là một kiểu mật mã khác – mật mã khối (block cipher) -- trong đó từng khối nhiều ký tự đoợc mã hóa cùng

một lúc. Trong mật mã khối, các tham số quan trọng là kích thoịớc (độ dài khối) và kích thoịớc khóa. Các khái niệm này đoịợc minh họa qua ví dụ sau đây.

key	000	001	010	011	100	101	110	111
0	001	111	110	000	100	010	101	011
1	001	110	111	100	011	010	000	101
2	001	000	100	101	110	111	010	011
3	100	101	110	111	000	001	010	011
4	101	110	100	010	011	001	011	111

Theo bảng này, dữ liệu plaintext 010100110111 sẽ được mã hóa thành:

010 100 110 111 => 111 011 000 101 theo key=1

010 100 110 111 => 100 011 011 111 theo key=4

Ở đây số loịợng khóa là 5, do 2^2 < 5 < 2^3 nên cần 3 bit để biểu diễn và loịu giữ khóa, tức là kich thoịớc khóa là 3. Đồng thời kích thoịớc khối cũng là 3.

Cũng qua ví dụ đơn giản này (chỉ có tính chất minh họa), ta thấy rằng nếu các tham số kích thoịớc khối và khóa qua nhỏ thì mật mã rất dễ bị phá bằng các tấn công thông qua phân tích thống kê. Chẳng hạn trong ví dụ trên, nếu kẻ thù nhận đoịợc một khối mã ciphertext 001 thì nó có thể dễ dàng suy ra plaintext toịơng ứng chỉ có thể là 000 hoặc 101 (nhờ thống kê trên bảng biến đổi mã). Vì vây, các điều kiện cần cho mật mã khối an toàn là: • Kích thoịớc khối phải đủ lớn để chống lại các loại tấn công phá hoại bằng phoịơng pháp thống kê. Tuy nhiên cần loịu ý rằng kích thoịớc khối lớn sẽ làm thời gian trễ lớn. • Không gian khóa phải đủ lớn (tức là chiều dài khóa phải đủ lớn) để chống lại tìm kiếm vét cạn.Tuy nhiên mặt khác, khóa cần phải đủ ngắn để việc làm khóa, phân phối và loịu trữ đoịợc hiệu quả. Về các nguyên lý thiết kế mật mã khối, ngoịời ta đã ghi nhận 2 nguyên tắc cơ sở sau để có bảo mật cao, đó là việc tạo ra confusion (tính hỗn loạn, rắc rối) và diffusion (tính khuếch tán). Confusion. (Hỗn loạn, rắc rối) Sự phụ thuộc của bản mã đối với bản rõ phải thực phức tạp để gây rắc rối, cảm giác hỗn loạn đối với kẻ thù có ý định phân tích tìm qui luật để phá mã. Quan hệ hàm số của mã-tin là phi tuyến (non-linear). Diffusion. (Khuếch tán) Làm khuếch tán những mẫu văn bản mang đặc tính thống kê (gây ra do doị thừa của ngôn ngữ) lẫn vào toàn bộ văn bản. Nhờ đó tạo ra khó khăn cho kẻ thù trong việc dò phá mã trên cơ sở thống kê các mẫu lặp lại cao. Sự thay đổi của một bit trong một khối bản rõ phải dẫn tới sự thay đối hoàn toàn trong khối mã tạo ra. Một cách đơn giản nhất, confusion có thể đoịợc thực hiện bằng phép thay thế (substitution) trong khi diffusion đoịợc tạo ra bằng

các phép chuyển đổi chỗ (transposition/permutation) hay hoán vị. Toàn bộ sơ đồ biến đổi mật mã sẽ là một lợới các biến đổi thay thế-hoán vị (substitution-permutation network).

Ví du 2.2: Phép hoán vị cột: Để mã hóa "computer security",

ta viết lại thành nhiều hàng 5 cột

c o m p u

t e r s e

c u r i t

y.

Mã tạo ra bằng cách viết lại theo cột: C T C Y O E U M R R P S I U E T Bên cạnh các nguyên tắc tạo tính bảo mật nói trên, việc thiết kế mật mã khối cũng đề cao các nguyên tắc cài đặt hiệu quả.: Cài đặt cho phần mềm cần đảm bảo tính mềm dẻo và giá thành thấp. Cài đặt cho phần cứng cần đảm bảo tốc độ cao và tính kinh tế. Để đáp ứng tốt các nguyên lý thiết kế đã nêu trên, các thuật toán mật mã khối thợờng đợợc tổ chức nhợ một cấu trúc nhiều vòng lặp

3. Sử dụng mật mã

3.1. Bảo mật

Bí mật: Chỉ có người nhận đã xác thực có thể lấy ra được nội dung của thông tin chứa đựng trong dạng đã mật mã hóa của nó. Nói khác đi, nó không thể cho phép thu lượm được bất kỳ thông tin đáng kể nào về nội dung của thông điệp.

3.2. Toàn vẹn dữ liệu

Người nhận cần có khả năng xác định được thông tin có bị thay đổi trong quá trình truyền thông hay không.

3.3. Xác thực

Người nhận cần có khả năng xác định người gửi và kiểm tra xem người gửi đó có thực sự gửi thông tin đi hay không.

3.4. Tính không chối từ

Người gửi không thể từ chối việc mình đã gửi thông tin đi.

3.5. Kiểm sóat truy cập

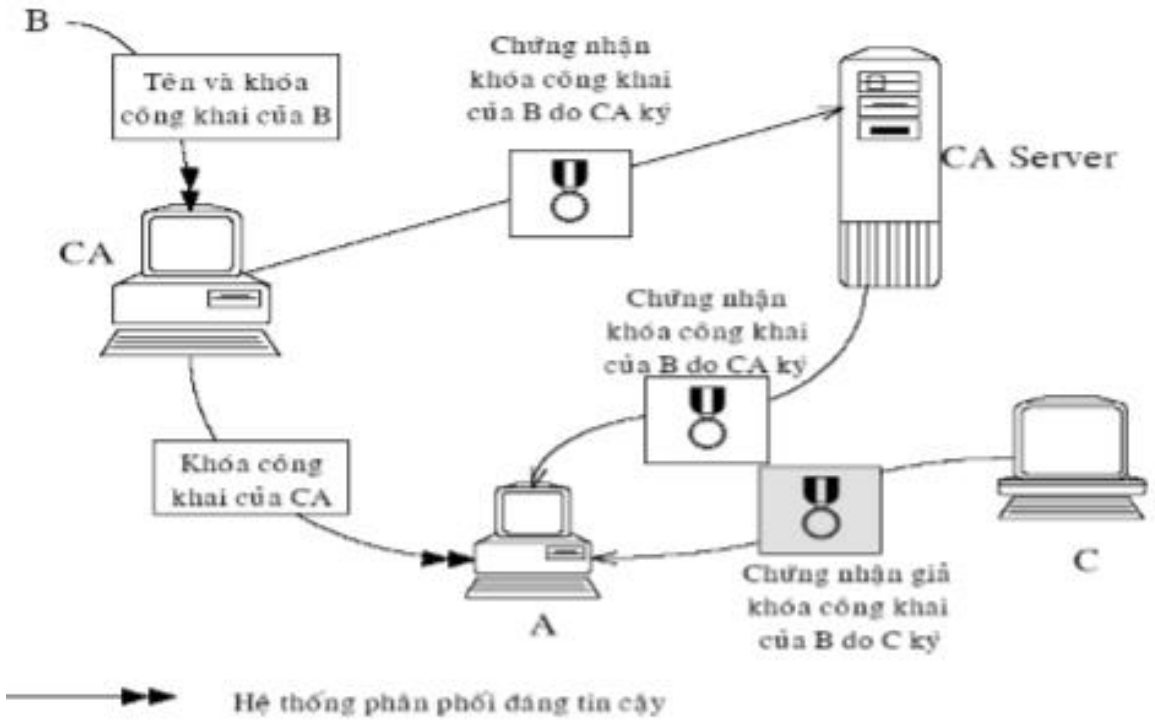
Nếu như Xác thực (authentication) là pha đảm bảo an toàn đầu tiên mà hệ thống

cần kiểm soát khi ngợời sử dụng mới đăng nhập, nhằm đảm sự chính danh, thì điều khiển truy nhập (AC: access control) là pha thứ hai quyết định xem ngợời dùng có thể làm gì và nhợ thế nào trong ngôi nhà hệ thống này. Trong giáo trình

“Security Engineering”, tác giả Ross Anderson có viết “Its function is to control which principals (persons, processes, machines, …) have access to which resources in the system -- which files they can read, which programs they can execute, and how they share data with other principals, and so on”. Có thể hình dung hệ thống có một kho tập hợp các tài nguyên (files, tiến trình, cổng thiết bị …) mà NSD (thông qua tiến trình thực hiện) có thể được cho phép truy nhập đến một mức độ nào đó (từ không đoợc phép đến toàn quyền), và cũng có thể chia sẻ những quyền truy nhập mà mình có này với các NSD khác. Một cơ chế điều khiển truy nhập cụ thể (AC mechanism) sẽ quyết định toàn bộ câu chuyện cho phép và chia sẻ quyền sử dụng tài nguyên này.

Ý nghĩa mang tính nền móng của AC cho thấy tầm quan trọng và sự phổ biến rộng rãi của nó. Dễ nhìn thấy AC có mặt ở hầu khắp các ứng dụng liên quan đến doanh nghiệp, các hệ cơ sở dữ liệu, và đoƚơng nhiên là các hệ điều hành và trình điều khiển thiết bị phần cứng. Đoƚơng nhiên khái niệm về AC đã ra đời từ rất sớm khi mà một cỗ máy tính toán không phải đoợc chế tạo cho chỉ một NSD mà là một tập hợp ngoời, chia sẻ sử dụng, với các nhiệm vụ (và kéo theo nó là pham vi sử dụng tài nguyên) khác nhau mà có thể rất phong phú. Vậy mô hình đầu tiên về AC đã đoợc hình thành như thế nào và từ bao giờ? Mô hình đầu tiên đoợc biết đến về AC là một mô hình rất cơ bản, mô hình ma trận điều khiển truy nhập (access control matrix), được đưa ra để nghiên cứu cơ chế bảo vệ hệ thống (Protection), tức là thuộc về những nghiên cứu đầu tiên trong lĩnh vực anh toàn thông tin. Mô hình bảo vệ này đoợc đoƚa ra bởi Lampson (1971), sau đó được làm mịn hơn bởi Graham và Denning (1972) và đoợc nâng cao thành một mô hình khái quát về bảo vệ hệ điều hành (“Protection in Operating Systems”, 1976). Ở đây các tác giả khái quát khái niệm hệ thống nhoƚ một máy trạng thái, trong đó tình trạng an toàn (được bảo vệ của hệ thống) đoợc gọi là trạng thái bảo vệ (protection state). Trạng thái bảo vệ này có thể mô tả bằng các thuộc tính chế độ cài đặt của hệ thống có liên quan đến bảo vệ. Sự hoạt động không ngừng của hệ thống sẽ gây nên sự chuyển dịch của trạng thái bảo vệ. Chẳng hạn như sự thay đổi quyền toƚơng tác của một NSD với hệ thống, dù chỉ là thêm vào hay bớt đi khả năng sử dụng đối với một tệp dữ liệu.

4. Mô hình PKI (Cơ sở hạ tầng khoá công khai)



4.1. Chứng nhận (Certificates)

PKIs dựa vào một thiết bị mật mã để bảo đảm các khoá công khai được quản lý an toàn. Các thiết bị này không hoạt động cùng lúc được thực hiện ở các hàm mảng rộng có liên quan đến việc quản lý phân phối khoá, bao gồm các thành phần sau:
-chứng thực và đăng ký mật mã đầu cuối
-kiểm tra tính toàn vẹn của khoá công khai
-chứng thực yêu cầu trong quá trình bảo quản các khoá công khai
-bí mật cấp phát khoá công cộng
-huỷ bỏ khoá công khai khi nó không có đủ giá trị độ dài
-duy trì việc thu hồi các thông tin về khoá công cộng (CRL) và phân bổ thông tin (thông qua CRL cấp phát hoặc đáp ứng đến Online Certificate Status Protocol [OCSP] messages).
-đảm bảo an toàn về độ lớn của khoá.

·**Public Keys Certificates :**

Mục tiêu của việc trao đổi khoá bất đối xứng là phát một cách an toàn khoá công khai từ người gửi (mã hoá) đến người nhận (giải mã). PKI hỗ trợ tạo điều kiện cho việc trao đổi khoá an toàn để đảm bảo xác thực các bên trao đổi với nhau.
Public key Certificate được phát bởi Certificate Authority(CA). Để CA phát public key certificate cho đáp ứng mật mã đầu cuối thì đầu cuối đầu tiên phải đăng ký với CA. Quá trình đăng ký gồm: sự đăng ký, sự kích hoạt, và sự chứng nhận của mật mã đầu cuối với PKI (CAs và RAs). Quá trình đăng ký như sau:

- Mật mã đầu cuối đăng ký với CA hoặc RA. Trong quá trình đăng ký, mật mã đầu cuối đưa ra cách nhận biết đến CA. CA sẽ xác thực đầu cuối, phát public key đến đầu cuối .
- Các đầu cuối bắt đầu khởi tạo phase bằng cách tạo ra một public/private keypair và public key của keypair được chuyển đến CA.

- CA viết mật hiệu lên public key certificate cùng với private key để tạo một public key certificate cho mật mã đầu cuối.

Lúc này các mật mã đầu cuối có thể yêu cầu public key certificate từ mật mã đầu cuối khác. Chúng có thể sử dụng CAs public key để giải mã public key certificate để thu được khoá thích hợp·**Registration Authorities:**

Trong nhiều trường hợp, CA sẽ cung cấp tất cả các dịch vụ cần thiết của PKI để quản lý các public key bên trong mạng. Tuy nhiên có nhiều trường hợp CA có thể uỷ nhiệm làm công việc của RA. một số chức năng mà CA có thể uỷ nhiệm thay thế cho RA như:

kiểm tra mật mã đầu cuối thử đã đăng ký public key với CA để có private key mà được dùng để kết hợp với public key.

- Phát public/private keypairs được dùng để khởi tạo phase của quá trình đăng ký.
- xác nhận các thông số của public key.
- phát gián tiếp các certificate Revocation List (CRL).

·**Certificate Authorities :**

CA dùng để cấp phát chứng nhận, xác thực PKI clients, và khi cần thiết thu hồi lại chứng nhận.

CA đại diện cho nguồn tin cậy chính của PKI. Vì CA là yếu tố duy nhất trong PKI mà có thể phát Public Key Certificates đến các mật mã đầu cuối.

CA cũng luôn đáp ứng cho việc duy trì CRL và phục vụ các loại như: CRL Issuer.

PKI không phải chỉ có 1 CA mà PKI có thể thiết lập nhiều CAs.

CAs giúp thiết lập cho việc nhận dạng của các thực thể giao tiếp với nhau được đúng đắn. CAs không chỉ chứng cho PKI client mà còn cho những CAs khác bằng cách cấp phát những chứng nhận số đến chúng. Những CAs đã chứng nhận lần lượt có thể chứng nhận cho những CAs khác cho đến khi mỗi thực thể có thể uỷ nhiệm cho những thực thể khác có liên quan trong quá trình giao dịch.

a.Mục tiêu và các chức năng của PKI

PKI cho phép những người tham gia xác thực lẫn nhau và sử dụng các thông tin từ các chứng thực khoá công khai để mật mã hoá và giải mã thông tin trong quá trình trao đổi.

PKI cho phép các giao dịch điện tử được diễn ra đảm bảo tính bí mật, toàn vẹ và xác thực lẫn nhau mà không cần trao đổi các thông tin bảo mật từ trước.

Mục tiêu chính của PKI là cung cấp khoá công khai và xác định mối liên hệ giữa khoá và định dạng người dùng. Nhờ vậy, người dùng có thể sử dụng trong một số ứng dụng như :

-Mã hoá Email hoặc xác thực người gửi Email

-Mã hoá hoặc chứng thực văn bản

-Xác thực người dùng ứng dụng

-Các giao thức truyền thông an toàn : trao đổi bằng khoá bất đối xứng, mã hoá bằng khoá đối xứng.

PKI bao gồm các thành phần sau đây:

-Phát sinh một cặp khoá riêng và khoá chung cho PKI client

-Tạo và xác nhận chữ ký điện tử

-cấp phát chứng nhậo người dùng

-Đánh dấu những khoá đã cấp phát và bảo trì quá trình sử dụng của mỗi khoá
-Hủy bỏ những đăng ký sai và hết hạn
-Xác nhận PKI client

c)Mục đích của PKI

PKI được sử dụng với các mục đích :
-Mã hoá: giữ bí mật thông tin và chỉ có người có khoá bí mật mới giải mã được.
-Tạo chữ ký số : cho phép kiểm tra một văn bản có phải đã được tạo với một khoá bí mật nào đó hay không.
-Thoả thuận khoá: cho phép thiết lập khoá dùng để trao đổi thông tin bảo mật giữa 2 bên.

4.2. Revocation – Thu hồi chứng nhận

4.3. Trust Models – Các mô hình uỷ quyền

Kiểm tra

Bài 5: Các chính sách và quy trình thực thi an toàn thông tin trên hệ thống

Mã bài: MD22-5

Giới thiệu: Bài 5 trình bày các chính sách và quy trình thực thi an toàn thông tin trên hệ thống.

Mục tiêu:

- Sao lưu và phục hồi được nếu hệ thống gặp sự cố;
- Quản trị và phân quyền người dùng;
- Chính xác, cẩn thận, khoa học, sáng tạo, linh hoạt.

Nội dung chính:

1. Phục hồi sau sự cố

1.1. Backups

"Back-up dữ liệu" có nghĩa là bạn **sao chép các dữ liệu trong máy tính** (hoặc **tablet, smartphone**) của bạn và lưu trữ nó ở một nơi khác, phòng khi máy tính của bạn gặp vấn đề như hỏng ổ cứng, bị nhiễm **virus** nặng, bị mất máy. Bạn sẽ không lo bị mất dữ liệu trên máy nữa vì bạn có thể **backup dữ liệu** của mình về từ nơi lưu trữ dự bị. Cách nhanh nhất để **back-up dữ liệu** là sử dụng các ổ đĩa rời, ổ cứng di động, **USB** hay thậm chí là đĩa **DVD, VCD.** Tuy nhiên đây là cách làm truyền thống đã trở nên lỗi thời, vì nguy cơ mất dữ liệu do các nguyên nhân vật lý cũng có thể xảy ra với chính các thiết bị lưu trữ di động này, đó là chưa kể đến chi phí mua sắm cũng không hề rẻ và dung lượng lưu trữ .**Dữ liệu là** tài sản quý giá đối với mỗi cá nhân và mỗi doanh nghiệp. Nếu bạn không muốn một hôm đẹp trời nào đó toàn bộ dữ liệu của mình lưu trên máy tính cá nhân, máy tính bảng hay thậm chí điện thoại di động bốc hơi mất vì máy bị hỏng hay mất trộm thì bạn cần phải **back-up dữ liệu.**

1.2. Secure Recovery

Bảo mật tính phục hồi dữ liệu

1.3. Kế hoạch hục hồi sau sự cố (Disaster Recovery Plan)

Một kế hoạch phục hồi sau thảm họa (Disaster Recovery Plan - DRP) là một quá trình được văn bản hóa hoặc tập hợp các quy trình để phục hồi và bảo vệ hạ tầng công nghệ thông tin (IT) khi xảy ra thảm họa.

Thảm họa có thể là tự nhiên (natural), môi trường (environmental), hoặc do con người (man-made).

Các tổ chức không phải lúc nào cũng tránh được thảm họa, nhưng với một kế hoạch kỹ lưỡng thì sẽ giảm thiểu được ảnh hưởng của thảm họa. Mục đích của kế hoạch phục hồi sau thảm họa là giảm thiểu thời gian gián đoạn của hệ thống và mất mát dữ liệu.

Thực tế, một kế hoạch DRP hiệu quả không chỉ giúp giải quyết việc bảo vệ và phục hồi công nghệ, mà còn cần có những yếu tố cần thiết như con người, quy trình và thủ tục để tạo nên thành công thực sự. Nó còn cho phép người dùng cuối quản lý nguy cơ doanh nghiệp, phản ứng với các rủi ro đình trệ hệ thống, và hoàn tất các giao dịch kinh doanh mới, trong khi vẫn bảo vệ được các giao dịch truyền thống có vai trò tối quan trọng với doanh nghiệp.

Trong DRP, cần phải đưa ra các bước chi tiết để khôi phục các hệ thống IT về trạng thái bình thường để có thể hỗ trợ hoạt động sau một thảm họa. Trước khi xây dựng kế hoạch khôi phục chi tiết, cần phải thực hiện đánh giá rủi ro (Risk Assessment - RA) và/hoặc phân tích tác động (Business Impact Analysis - BIA) để xác định các dịch vụ IT hỗ trợ các hoạt động quan trọng của tổ chức; sau đó xây dựng các thời gian khôi phục và điểm khôi phục. Sau đó cần tiến hành xây dựng kế hoạch chung phục hồi thảm họa (Disaster Recovery Strategies), sau đó là các kế hoạch chi tiết thực hiện (Disaster Recovory Plan).

2. Tính liên tục trong kinh doanh (Business Continuity)

2.1. Các tiện ích

Công nghệ quang và công nghệ lưu trữ cho phép bảo đảm tính liên tục trong kinh doanh và khắc phục thảm họa.

2.2. High Availability/Fault Tolerance

Sự khác nhau cơ bản giữa Fault Tolerance và High Availability là: Fault tolerance không gây ra sự gián đoạn cho hệ thống nhưng chi phí sẽ cao hơn nhiều, còn High Availablility giảm thiểu tới mức tối đa sự gián đoạn của hệ thống

Fault Tolerance dựa vào các phần cứng đặc biệt để xác định các lỗi phần cứng và ngay lập tức thay thế bằng các thành phần dự trữ. Điều này có vẻ khá sướng và đã vì hệ thống luôn chạy mượt mà không ngừng nghỉ nhưng thực tế thì phải trả giá khá cao cho cả phần cứng và hiệu năng bởi vì các phần cứng dự trữ chả làm gì cả mà chỉ chờ mấy thằng chính bị hư là nhảy vào thay thế mà thôi. Ngoài ra, khi có sự cố thì hiệu năng có thể sẽ giảm xuống nếu như các thành phần thay thế có tốc độ xử lý không bằng thành phần bị hư hại.

Trong khi đó, High Availability không tiến hành thay thế các thành phần phần cứng bị lỗi. High Avalibility sử dụng tập hợp các hệ thống chia sẻ tài nguyên nhằm giảm thiểu tới mức tối đa thời gian hệ thống không hoạt động bằng cách nhanh chóng phục hồi các dịch vụ thiết yếu trong khoảng thời gian chưa tới 1 phút. Do vậy, với High Availability, người dùng sẽ có thể chịu đựng một vài khoảng thời gian "downtime" ngắn của hệ thống.

High Availibility thường được sử dụng nhiều hơn bởi vì chi phí thấp hơn nhiều so với Fault Tolerance và các công ty, tập đoàn có thể chấp nhận được khoảng thời gian "downtime" của hệ thống. Các công ty Dịch vụ thường đưa ra con số ước lượng khoảng thời gian mà dịch vụ của các công ty đó sẵn sàng bằng "nines of availabillity" như Amazone là three nines of availibility (99.9% uptime) – tức là downtime khoảng 43.2 phút/tháng. Còn Hadoop sử dụng Fault Tolerance như một giải pháp đảm bảo dữ liệu trên HDFS. Ngoài ra RAID cũng là một cách thể hiện của Fault Tolerance khi dữ liệu được lưu trữ và back-up trên nhiều đĩa cứng khác nhau.

2.3. Backups

3. Chính sách và các quy trình (Policy and Procedures)

3.1. Chính sách an toàn thông tin (Security Policy)

Chỉ thị và hướng dẫn về an toàn thông tin.

3.2. Chính sách phản ứng trước sự cố (Incident Response Policy)

4. Quản trị phân quyền (Privilege Management)

4.1. Quản trị vai trò người dùng / nhóm (User/Group Role Management)

User và Group là những thành phần cơ bản để quản lý máy tính và tài nguyên trên máy tính. Tùy vào mức độ được cấp quyền mà người dùng có quyền truy xuất vào những tài nguyên nào trên máy tính, hoặc trong hệ thống mang. Ở bài này chúng ta tìm hiểu vế cách tạo và quản lý user trên máy cục bộ (local host).

Đây là hệ thống quản lý người dùng (User) và nhóm người dùng (Group) của Windows. Bạn có thể tìm thấy trình quản lý này trên các phiên bản Workstation: Windows XP pro, Windows Vista & Windows 7 professional , Ultimate, Windows server (chưa dựng Domain).

Trong trường hợp Windows server chưa lên Domain thì chúng hoạt quản lý user và Group như Windows workstation. Khi đã nâng cấp lên Domain thì Local user and group không hoat động nữa, thay vào đó lá Active Directory User and Computer .

4.2. Đăng nhập đơn (Single Sign-on)

Với hệ thống có nhiều website và application thì việc sử dụng Single Sign On (SSO) là khá cần thiết nhằm đem lại nhiều thuận tiện cho người dùng và tăng tính năng bảo mật.SSO chỉ được triển khai sau khi đã xây dựng được hệ thống xác thực và phân quyền. SSO có nhiệm vụ cung cấp cho người dùng quyền truy cập nhiều

tài nguyên Web, Applications trong phạm vi cho phép chỉ với một lần đăng nhập (xác thực). Nói thêm về Phân quyền (Access Control), có 2 Rules chính:

- Authentication: Là quá trình để định danh một người dùng có hợp lệ hay không. (Thường thể hiện qua một form đăng nhập)
- Authorization: Là quá trình kiểm chứng một người dùng đã được xác thực có đủ quyền truy cập vào tài nguyên (mà người dùng) yêu cầu hay không. Tài nguyên yêu cầu có thể phụ thuộc vào Policy domain (cấp quyền theo domain) hoặc một policy đặc biệt nào đó (ví dụ cấp quyền theo cấp).

SSO có thể được sử dụng dưới các dạng:

1. Single Domain: Khi xác thực thành công vào domain.com, người dùng đồng thời được xác thực vào các sub-domain.domain.com tồn tại.
2. Multi Domain: Khi xác thực thành công vào facebook.com, người dùng đồng thời được xác thực vào example.com
3. Applications vs Third-Party Products: ví dụ SSO giữa Oracle Access Manager và IBM WebSphere Application Server

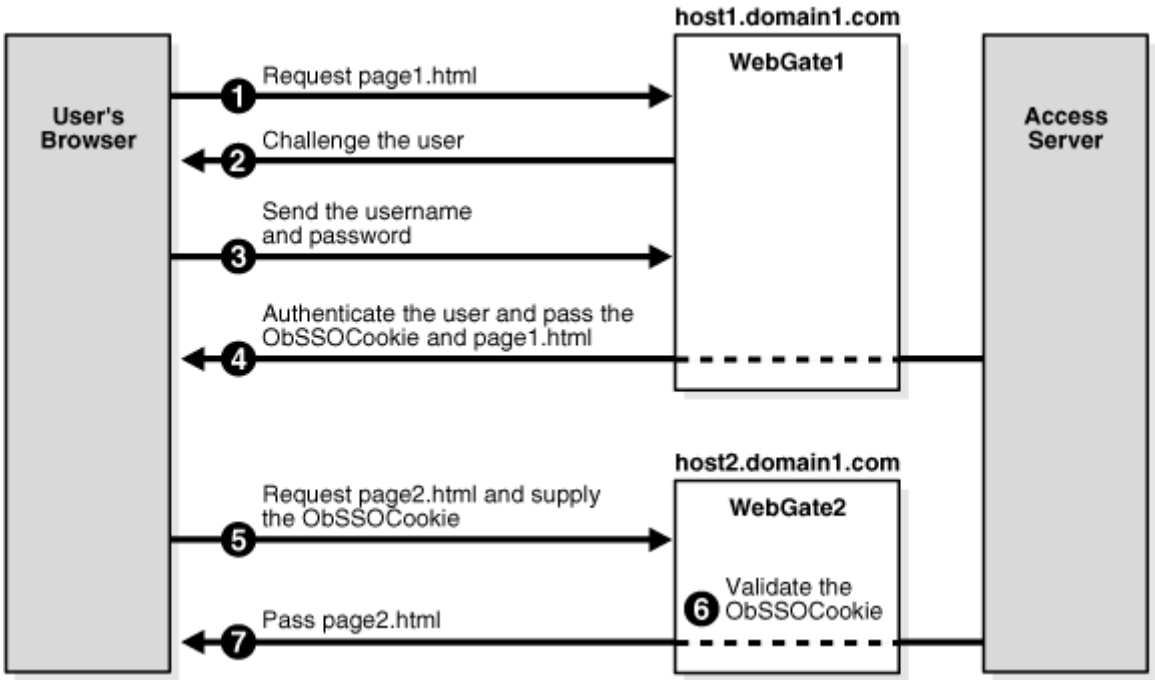
Ở 2 dạng đầu tiên, SSO thường sử dụng Cookie để nhận diện, webserver (hay webgate) gửi cookie đã được mã hóa cho browser đã xác thực thành công, cookie này sẽ là chìa khóa sử dụng cho các xác thực tới các tài nguyên khác hoặc cho các xác thực có cùng cấp.

Phần Cookie được mã hóa có thể bao gồm các thông tin: session, distinguished name của người dùng đã xác thực thành công, IP của client đã yêu cầu, thời điểm khởi tạo cookie, thời điểm sửa đổi cookie.. các thành phần không mã hóa của cookie có thể bao gồm: thời gian expired, domain hoạt động, SSL/ Httponly…

Thuật toán mã hóa được recommend hiện nay là AES, bên cạnh là các thuật toán kém bền vững hơn nhưng thông dụng như MD5-salt, RC4, RC6 vẫn được sử dụng phổ biến trong các mã hóa cookie/ session.

- **Single Domain SSO**

Cookie Path được cấu hình để dùng chung cho mọi subdomain: **.domain.com** (bao gồm dấu . ở đầu)



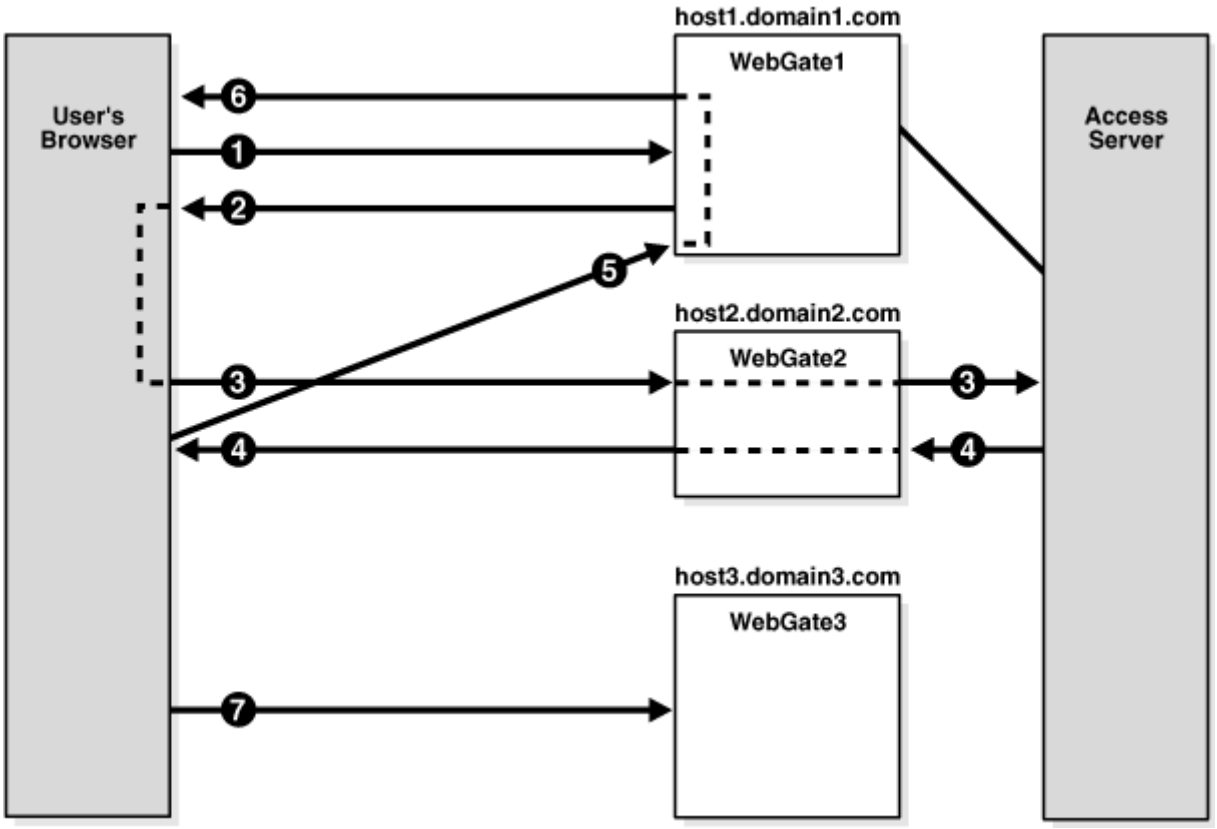
Mô hình của **Oracle® Access Manager**

- **Multi Domain SSO**

Multi Domain SSO cho phép người dùng truy cập vào nhiều domains/hosts sau 1 lần đăng nhập. Một ứng dụng xác thực chính sẽ cung cấp các cookie hợp lệ cho mỗi domain.Chẳng hạn người dùng truy cập vào gmail.com, khi đó toàn bộ services của Google, như Google.com, Picasa, Blogspot… đều nhận diện tính xác thực cho người dùng đó.

Tuy nhiên cookie không thể được thiết đặt cho across domains do Policy bảo mật của hầu hết browser, do đó một domain chính sẽ được chọn để xác thực ở mọi quy trình, gọi chung là master domain. Với mỗi domain khác mà người dùng thực hiện quá trình xác thực, mỗi webgate của hệ thống đó sẽ redirect tới master domain.

Master domain sẽ hoạt động như quy trình của Single Domain SSO, nó chính là *proxy* để truyền tải cookie hợp lệ về cho mỗi domain có yêu cầu xác thực.



Mô hình của **Oracle® Access Manager**

Hoạt động

1. Ta thiết đặt master domain, login-service.domain.com.
2. Mỗi một domain nằm trong group SSO đều có script login riêng.
3. Mọi hệ thống trên mỗi domain đều sử dụng chung Session Database.
4. Khi mỗi Client yêu cầu người dùng xác thực, Webgate của nó sẽ redirects tới master domain có chứa login service. Nếu người dùng chưa đăng nhập, master domain sẽ triệu gọi script login của client để thực hiện việc login vào master domain. Khi người dùng đã xác thực, một session sẽ được tạo trong database và master domain sẽ cung cấp session id cho client yêu cầu để có thể tạo cookie theo session đó.

Notes:

- Các thuật toán mã hóa session. session id phải được dùng chung (RFC 4122)
- Master service chỉ xử lý & redirect tới những domain nằm trong whilelist
- Các domain có thể ở nhiều dạng khác nhau, login.domain.com, domain.com/service, client.abc.com…

Logout

Đây là quá trình quan trọng vì mỗi quá trình logout ở một client chỉ có hiệu lực với cookie của client đó, cần thiết đặt một timeout phù hợp cho cookie hay thiết đặt cơ chế clear cookie ở mọi domain liên quan (chậm chạp), có thể xóa luôn session ở database nhưng lưu ý session có thể tạo lại bởi tính năng Ghi nhớ đăng nhập.

4.3. Quản trị tập trung và phân tán (Centralized vs. Decentralized)

Một hệ thống lớn, tức là gồm rất nhiều bộ phận và có tầm bao phủ rộng, thường thì rất khó điều khiển, quản lý hoặc kiểm soát (sẽ gọi chung là "vận hành"). Nên khi xem xét hệ thống lớn, mô hình tổ chức vận hành như thế nào thường là vấn đề nền tảng được giải quyết đầu tiên, từ đó xác định hướng thiết kế toàn hệ thống.

Hai loại mô hình cơ bản là mô hình centralized mang tính chất tập trung mọi thứ về một trung tâm để ra các quyết định vận hành, và mô hình decentralized mang ý tưởng chia phần việc ra và phân về cho những bộ phận nhỏ xử lý, ra quyết định ở cấp bộ phận.

Để mọi người đỡ phải tự thắc mắc, tớ nói luôn là việc xem xét các loại mô hình vận hành sẽ nhằm giúp thiết kế hệ thống lớn mà chúng ta đang là thành viên của nó, OlympiaVN. Lựa chọn mô hình phát triển nào cho OlympiaVN, điều đó sẽ ảnh hưởng đến chiến lược xây dựng cộng đồng, cẩm nang phát triển OlympiaVN sẽ xoay quanh tinh thần của mô hình đó.

Chọn cho mình mô hình như thế nào thì cần đắn đo nhiều, trước tiên tớ giới thiệu 2 loại mô hình centralized và decentralized, để sau này dùng chúng mà tạo ra mô hình cho riêng mình.

Thử lấy ví dụ để minh họa về các mô hình centralized và decentralized:

+ Một nhóm bạn cùng giải một bài tập lớn. Nếu nhóm này có một người rất giỏi và làm hầu hết công việc cho cả nhóm, thì đó là kiểu centralized. Còn chia ra mỗi người làm một phần thì là decentralized.

+ Một tập đoàn đa quốc gia, nếu tất cả số liệu về tài chính được đưa về tổng hành dinh để xử lý, thì việc quản lý tài chính đó là theo centralized (trong khi các hoạt động khác vẫn có thể do các chi nhánh tự thực hiện). Nếu mỗi chi nhánh tự kiểm soát tài chính của mình và chỉ báo cáo kết quả kinh doanh cho tổng hành dinh, thì đó là decentralized.

+ Nhà nước đầu tư cho giáo dục để xây tất cả các trường học bằng ngân sách nhà nước, thì đó là kiểu đầu tư centralized. Còn "xã hội hóa giáo dục" để nhiều tổ chức khác cùng đầu tư thì là một hình thức decentralized.

+ Dữ liệu trên mạng Internet đặt ở các servers trải khắp thế giới, đó là mô hình decentralized. Nếu Google gom tất cả dữ liệu về trung tâm lưu trữ của nó, thì là Google đang tạo một bản copy kiểu centralized cho Internet.

Cái lợi của mô hình centralized là:

- Không có sự chồng chéo, mỗi quyết định / thông tin / dữ liệu đều là duy nhất, tránh rắc rối khi có nhiều dị bản.

- Hoạt động xuyên suốt, ít trở ngại.

- Truy cập thông tin nhanh và chính xác, do chỉ cần kết nối với trung tâm là được.

Khiếm khuyết của mô hình centralized:

* Tuy vậy, mô hình centralized gặp khuyết điểm là tốn kém rất nhiều để có thể xây dựng được cả hệ thống lớn, lại có những hệ thống lớn không thể đạt được mô hình centralized vì các bộ phận của nó không tuân theo một trung tâm đầu não nào. Ngoài ra, khi trung tâm đầu não gặp vấn đề thì toàn bộ hệ thống bị tê liệt.

Ưu điểm của mô hình decentralized là:

- Đầu tư cho từng bộ phận là nhỏ, có thể vừa vận hành vừa đầu tư thêm dần.

- Các bộ phận chỉ có ảnh hưởng nhau một cách hạn chế, nếu một bộ phận gặp vấn đề thì chỉ ảnh hưởng một cụm xung quanh nó, còn các nơi khác vẫn có thể tiếp tục hoạt động.

- Xử lý công việc đơn giản, không đòi hỏi nhiều năng lực (trình độ đầu óc, cơ sở hạ tầng).

Hạn chế của mô hình decentralized:

* Khuyết điểm của mô hình decentralized là các vấn đề mà mô hình centralized có ưu điểm như liệt kê ở trên. Quan trọng nhất là mô hình decentralized tiềm tàng các mâu thuẫn nội bộ, có khi thông tin từ các bộ phận không khớp nhau, hoặc nhiều bộ phận cùng làm một việc và bị thừa, trùng lặp.

4.4. Kiểm tra (Auditing (Privilege, Usage, Escalation))

Thông thường khi thâm nhập vào một hệ thống (Từ Windows 7 trở lên) bạn chỉ có quyền là 1 user Nhưng, một số tác vụ đặc biệt yêu cầu quyền Administrator vì vậy các bạn phải thực hiện kĩ thuật leo thang đặc quyền

4.5. MAC/DAC/RBAC

Điều khiển truy cập trên cơ sở vai trò (RBAC) khác với hình thức MAC và DAC truyền thống. MAC và DAC trước đây là hai mô hình duy nhất được phổ biến trong điều khiển truy cập. Nếu một hệ thống không dùng MAC thì người ta chỉ có thể cho rằng hệ thống đó dùng DAC, hoặc ngược lại, mà thôi. Song cuộc nghiên cứu trong những năm 1990 đã chứng minh rằng RBAC không phải là MAC hoặc DAC.

Trong nội bộ một tổ chức, các vai trò (*roles*) được kiến tạo để đảm nhận các chức năng công việc khác nhau. Mỗi vai trò được gắn liền với một số quyền hạn cho phép nó thao tác một số hoạt động cụ thể ('permissions'). Các thành viên trong lực lượng cán bộ công nhân viên (hoặc những người dùng trong hệ thống) được phân phối một vai trò riêng, và thông qua việc phân phối vai trò này mà họ tiếp thu được một số những quyền hạn cho phép họ thi hành những chức năng cụ thể trong hệ thống.

Vì người dùng không được cấp phép một cách trực tiếp, song chỉ tiếp thu được những quyền hạn thông qua vai trò của họ (hoặc các vai trò), việc quản lý quyền hạn của người dùng trở thành một việc đơn giản, và người ta chỉ cần chỉ định những vai trò thích hợp cho người dùng mà thôi. Việc chỉ định vai trò này đơn giản hóa những công việc thông thường như việc cho thêm một người dùng vào trong hệ thống, hay đổi ban công tác (*department*) của người dùng.

RBAC khác với các danh sách điều khiển truy cập (*access control list - ACL*) được dùng trong hệ thống điều khiển truy cập tùy quyền, ở chỗ, nó chỉ định các quyền hạn tới từng hoạt động cụ thể với ý nghĩa trong cơ quan tổ chức, thay vì tới các đối tượng dữ liệu hạ tầng. Lấy ví dụ, một danh sách điều khiển truy cập có thể được dùng để cho phép hoặc từ chối quyền truy cập viết một tập tin hệ thống (*system file*), song nó không nói cho ta biết phương cách cụ thể để thay đổi tập tin đó. Trong một hệ thống dùng RBAC, một thao tác có thể là việc một chương trình ứng dụng tài chính kiến tạo một giao dịch trong 'tài khoản tín dụng' (*credit account transaction*), hay là việc một chương trình ứng dụng y học khởi thủy một bản ghi 'thử nghiệm nồng độ đường trong máu' (*blood sugar level test*). Việc chỉ định quyền hạn cho phép thi hành một thao tác nhất định là một việc làm đầy ý nghĩa, vì các thao tác đã được phân định tinh tế[1] và mỗi cá nhân thao tác có một ý nghĩa riêng trong chương trình ứng dụng.

5. Kiểm tra

CÂU HỎI ÔN TẬP

Câu 1: Học sinh/ sinh viên hãy trình bày các khái niệm cơ bản về an toàn thông tin và mật mã?

Câu 2: Học sinh/ sinh viên hãy trình bày quy trình thực thi an toàn thông tin trong hệ thống?

Câu 3: Học sinh/ sinh viên hãy trình bày về chứng thực điện tử và một số giải pháp bảo mật khác?

Câu 4: Học sinh/ sinh viên hãy vận dụng các phương pháp mã hóa đối xứng và cơ sở hạ tầng khóa công khai?

TÀI LIỆU THAM KHẢO

[1] Andrew S. Tanenbaum (2003), *Computer Networks*, Prentice Hall, New Jersey, Fourth Edition.

[2] Man Young Rhee, Wilay (2003), *Internet Security - Cryptographic Principles, Algorithms and Protocols*.

[3] William Stallings (1999), *Network Security Essentials: Applications and Standards*, Prentice Hall, New Jersey.

[4] William Stallings (2000), *Network Security* Essentials.

[5] Wasim.E. Rajput (2000),*Commerce Systems-Architecture & Application*.

[6] Douglas R. Stinson, *Cryptography Theory and Practice*, University of Nebraska- Lincoln;

[7] Thái Hồng Nhị, Phạm Minh Việt (2004), *An toàn thông tin*, Nhà xuất bản Khoa học & Kỹ thuật.

[8] Nguyễn Ngọc Tuấn (2005), *Công nghệ bảo mật World Wide Web*, Nhà xuất bản thống kê.

[9] Nguyễn Tiến, Đặng Xuân Hưởng, Nguyễn Văn Hoài, Bảo mật mạng (2000), Nhà Xuất bản Thông kê.