BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG

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

MỘT SỐ DẠNG TẤN CÔNG HỆ THỐNG THÔNG TIN

Ngành: Công Nghệ Thông Tin

Sinh viên thực hiện:…Nguyễn Mạnh Đức……

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

Mã số sinh viên:…121340…….

HẢI PHÒNG - 2012

LỜI CẢM ƠN

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

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

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

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

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

CÁC KÝ HIỆU VIẾT TẮT

ARP	Address Resolution Protocol	Giao thức phân giải địa chỉ
DoS	Denied of Service	Tấn công từ chối dịch vụ
DDoS	Distributed Denied of Service	Tấn công từ chối dịch vụ phân tán
VPN	Virtual Private Network	Mạng riêng ảo
IPSec	Internet Protocol Security	Giao thức Internet bảo mật
SSL	Secure Sockets Layer	Lớp socket bảo mật
TLS	Transport Layer Security	Lớp vận chuyển bảo mật
AD Domain	Active Directory Domain	Miền thư mục chủ

MỤC LỤC

Chương 1. TỔNG QUAN VỀ AN TOÀN THÔNG TIN

1.1. TÌM HIỂU AN TOÀN THÔNG TIN

1.1.1. Tại sao cần đảm bảo an toàn thông tin

Sự ra đời của internet là một thay đổi lớn trong cách tiếp nhận,trao đổi thông tin của con người. Thương mại điện tử (E-commerce) : giao thông buôn bán điện tử, e-banking:ngân hang điện tử.

Nhưng từ đó cũng nảy sinh ra nhiều vấn đề.Thông tin có thể bị đánh cắp, làm sai lệch, tráo đổi…. gây ra không ít tác hại. Điều này ảnh hưởng lớn tới các công ty, tập đoàn, an ninh quốc gia

Trong bối cảnh đó vấn đề an toàn thông tin (ATTT) được đặt ra ngay trong thực tiễn và từng bước lý luận

Cùng với sự phát triển mạnh mẽ của công nghệ thông tin (CNTT), ATTT đã trở thành một môn khoa học thực thụ.

1.1.2. Khái niệm về an toàn thông tin

1.1.2.1.Khái niệm

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

1.1.2.2.Đặc điểm của hệ thống không an toàn

Hệ thống có một trong những địa điểm sau là không an toàn

- Các thông tin dữ liệu trong hệ thống bị người không được quyền truy cập tìm cách lấy và sử dụng (thông tin bị rò rỉ)

- Các thông tin trong hệ thống bị thay thế hoặc sửa đổi làm sai lệch nội dụng (thông tin bị xáo trộn)

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

1.2. VẤN ĐỀ AN TOÀN THÔNG TIN

Khi nhu cầu trao đổi thông tin ngày càng lớn, sự phát triển của ngành công nghệ thông tin để nâng cao chất lượng và lưu lượng thông tin thì các quan niệm ý tưởng và biện pháp bảo vệ an toàn thông tin cũng được đổi mới. Bảo vệ thông tin là một vấn đề lớn, có lien quan đến nhiều lĩnh vực.

1.2.1. Phương pháp bảo vệ thông tin

Các phương pháp bảo vệ thông tin có thể gộp vào 3 nhóm sau:

- Bảo vệ thông tin bằng các phương pháp hành chính

- Bảo vệ thông tin bằng các phương pháp kỹ thuật (phần cứng)

- Bảo vệ thông tin bằng câc phương pháp thuật toán (phần mềm)

Ba nhóm trên có thể kết hợp với nhau hoặc triển khai độc lập.Hiện nay môi trường bảo vệ phức tạp nhất và cũng dễ bị tấn công nhất là môi trường mạng và truyền tin. Biện pháp hiệu quả nhất và kinh tế nhất hiện nay là biện pháp thuật toán.

1.2.2. Nội dung an toàn thông tin

1.2.2.1. Mục tiêu của an toàn thông tin

An toàn thông tin đảm bảo các yêu cầu sau:

1/. Bảo đảm bí mật (Bảo mật)

Bảo đảm thông tin không được tiết lộ cho người không có thẩm quyền

2/. Bảo đảm toàn vẹn

Ngăn chặn hay hạn chế việc bổ sung, loại bỏ, hay sửa đổi thông tin mà không được phép

3/. Bảo đảm xác thực (chứng thực)

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

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

4/. Bảo đảm sẵn sàng

Thông tin luôn sẵn sàng cho người dùng hợp pháp

1.2.2.2. An toàn thông tin

1/. Nội dung chính

*** An toàn máy tính**

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

Là khoa học về đảm bảo ATTT trong máy tính

***An toàn truyền tin**

Là sự bảo vệ thông tin trên đường truyền tin , từ hệ thống này qua hệ thống khác.

Là khoa học về sự đảm bảo thông tin trên đường truyền tin

2/. Hệ quả từ nội dung chính

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

An toàn dữ liệu

An toàn CSDL

An toàn hệ điều hành

An toàn mạng máy tính

1.2.2.3. Hành vi vi phạm thông tin

Để đảm bảo ATTT trên đường truyền hoặc thông tin có định, cần phải lường trước hoặc dự đoán trước được các khả năng không an toàn, các khả năng xâm phạm, các sự cố có thể xảy ra trong quá trình truyền tin. Xác định các chính xác các nguy cơ thì càng quyết định được tốt các giải pháp để giảm thiểu thiệt hại.

Các hành vi đó bao gồm:

Vi phạm thụ động:

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

Vi phạm chủ động:

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

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

1.2.3. Các chiến lược bảo vệ hệ thống thông tin

1.2.3.1. Giới hạn quyền hạn tối thiểu

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

1.2.3.2. Bảo vệ theo chiều sâu

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

1.2.3.3. Nút thắt

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

1.2.3.4. Điểm yếu nhất

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

***Điểm yếu từ mô hình:**

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

***Xác định các dịch vụ có nguy cơ:**

FTP, SMTP, POP3, WWW…..

***Điểm yếu trong yếu tố con người:**

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

1.2.3.5. Tính đa dạng bảo vệ

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

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

1.2.4.1. Chính sách

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

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

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

1.2.4.2. Các giải pháp

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

1.2.4.3. Công nghệ

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

1.2.4.4. Con người

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

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

1.2.5. Nội dung ứng dụng về an toàn thông tin

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

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

- Phục vụ các hoạt động hành chính : Chính quyền “điện tử”, chứng minh thư điện tử, giấy phép điện tử, gửi công văn, quyết định … từ xa trên mạng máy tính công khai.

- Phục vụ các hoạt động kinh tế: thương mại điện tử,…

Quảng bá thương hiệu , bán hàng trực tuyến.

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

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

- Phục vụ các hoạt động giáo dục, đào tạo: Gửi đề thi, bài thi qua mạng máy tính công khai, đào tạo từ xa (E-learning),…

- Bảo vệ thông tin số hóa: thông tin trên bộ nhớ hay trên đường truyền

1.3. KHÁI NIỆM "LỖ HỔNG"

"Lỗ hổng" là các điểm yếu có thể tạo ra sự ngưng trệ các dịch vụ trên hệ thống thông tin, hay nguy hiểm hơn nó cũng là "cửa" vào, ra của hệ thống của hacker. Lỗ hổng có thể tồn tại trong các dịch vụ mạng, các hệ điều hành, các phần mềm ứng dụng, Mức độ nguy hiểm của các lỗ hổng này được giới công nghệ chia làm 3 loại.

1.4. LỖ HỔNG CHIA THEO MỨC ĐỘ NGUY HIỂM

1.4.1. Lỗ hổng loại C

Lỗ hổng loại C có thể chỉ gây ra thiệt hại ở mức trung bình, làm gián đoạn hệ thống, ngưng trệ các dịch vụ.

Ví dụ: tấn công DOS làm ngưng trệ dịch vụ,…

1.4.2. Lỗ hổng loại B

Lỗ hổng loại B cho phép hacker có thể xâm nhập vào hệ thống mà không yêu cầu kiểm tra tính hợp lệ. Loại lỗ hổng này thường xảy ra trong các ứng dụng của hệ thống. Dẫn tới mất mát hoặc để lộ thông tin được bảo vệ

1.4.3. Lỗ hổng loại A

Đây là loại lỗ hổng có mức nguy hiểm cao nhất. Loại lỗ hổng này cho phép hacker một khi đã xâm nhập vào hệ thống, có quyền hạn nhất định, cùng chia sẻ tài nguyên với người dùng chính thống mà còn có thể nâng cao chiếm quyền điều khiển hệ thống.

Những lỗ hổng này có thể có nhiều khả năng xuất phát từ lỗ hổng trong CSDL, lỗ hổng trong cấu hình hệ thống, cấu hình trong các chính sách bảo mật…..

1.5. LỖ HỔNG THEO CHỨC NĂNG , NHIỆM VỤ

1.5.1. Lỗ hổng trong thuật toán

1/. Lỗi tràn vùng đệm:

Là cơ hội để phương thức tấn công sâu (Worm) trên mạng internet phát triển. Vùng đệm lưu chuỗi kí tự nhập vào theo quy định là 512 byte. Điều đáng tiếc là nó lại quên không kiểm tra dữ liệu vào có thực sự nhỏ hơn hoặc bằng 512 byte hay không? Kết quả là hiện tượng tràn dữ liệu xảy ra khi dữ liệu đầu vào lớn 512 byte.

Phần dữ liệu dư thừa kích hoạt một kịch bản khác (script). Script này thực hiện lọc tới một host khác.Kết quả dẫn đến hình thành sâu trên mạng.

2/. Chương trình quét (Scanner)

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

3/. Cơ chế hoạt động của Scanner

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

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

- Yêu cầu về thiết bị và hệ thống : Một chương trình Scanner có thể hoạt động được nếu môi trường đó hỗ trợ TCP/IP.

- Hệ thống phải kết nối vào mạng internet.

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

4/. Ảnh hưởng của chương trình Scanner đến việc bảo mật mạng

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

5/. Công nghệ Java trong bảo vệ thông tin

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

Cho phép các tấn công DOS: với các applet (ứng dụng kí sinh) có lỗi dẫn đến tình trạng chiếm nhiều tài nguyên hệ thống như sử dụng CPU, ổ đĩa,…..

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

6/. Một số lỗ hổng javascipts:

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

Điều đó được thể hiện ở các lỗ hổng sau:

- Có thể sử dụng javascripts để đọc nội dung các file trên máy trạm khi dùng IE

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

1.5.2. Lỗ hổng trong ứng dụng:

1/. Tập tin (file) host.equiv

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

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

2/. Thư mục var/mail

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

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

3/. Chức năng proxy (Ủy nhiệm) của FTPd

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

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

1.5.3. Lỗ hổng trong giao thức

1/. Vấn đề cần nghiên cứu

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

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

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

Cách 1 : Là xây dựng mới các giao thức mạng không còn lỗ hổng, có thể không tương thích với các chuẩn hiện có.

Cách 2 : Cải tiến gia thức cũ để “bịt ” các “lỗ hổng”, nhưng vẫn tương thức với các chuẩn hiện của Internet.

2/. Giao thức phân giải địa chỉ ARP

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

3/. Nguy cơ an ninh của ARP

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

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

Minh họa tình huống trên :

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

Giao thức như sau:

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

Tuy vậy có thể phát sinh tình huống:

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

1.5.4. Một số ví dụ “Lỗ hổng” cụ thể

1.5.4.1. Lỗ hổng trong hệ điều hành

1/. Hệ thống cấu hình không an toàn

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

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

2/. Lỗ hổng mật khẩu cơ bản

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

1.5.4.2. Lỗ hổng trong phần mềm ứng dụng

1/. Chủ quan (lỗi do người viết phần mềm)

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

2/. Khách quan (từ người sử dụng)

Người dùng vô ý để cho người khác sử dụng máy tính của mình, để lộ mật khẩu.

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

1.5.4.3. Lỗ hổng trong hệ thống mạng

1/. Nghe lén đường truyền, dò, đoán

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

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

2/. Thiết kế yếu kém

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

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

3/. Lỗi phát sinh do thiết bị

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

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

4/. Các lỗi chưa biết (Zero-Day)

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

Ví dụ : Khai thác lỗ hỏng Zero - Day từ trình duyệt Safari

Một lỗ hổng an ninh bảo mật thuộc hàng nghiêm trọng trong trình duyệt Safari của Apple.Các phiên bản cũ hơn đều bị ảnh hưởng.

Nếu người dùng vô tình đăng nhập vào các trang web có chứa các công cụ độc hại để khai thác lỗ hổng dành cho Windows của Safari, ngay lập tức các đoạn mã độc sẽ tự động tải về hệ thống với số lượng vô cùng lớn, sẽ khiến cho trình duyệt hoạt động ì ạch, treo…Người sử dụng Safari nên tránh truy cập vào các đường dẫn bất thường để giảm thiểu rủi ro.

1.5.4.4. Lỗ hổng trong Cơ sở dữ liệu (Database)

1/. Khái niệm cơ sở dữ liệu

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

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

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

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

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

Ví dụ trong phần mềm quản lí dữ liệu SQL server

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

Chương 2. MỘT SỐ DẠNG TẤN CÔNG VÀO HỆ THÔNG TIN

2.1. TẤN CÔNG HỆ THỐNG THÔNG TIN

2.1.1. Đối tượng tấn công

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

Một số đối tượng tấn công mạng:

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

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

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

2.1.2. Một số hình thức tấn công thông tin

Có thể tấn công theo các hình thức sau:

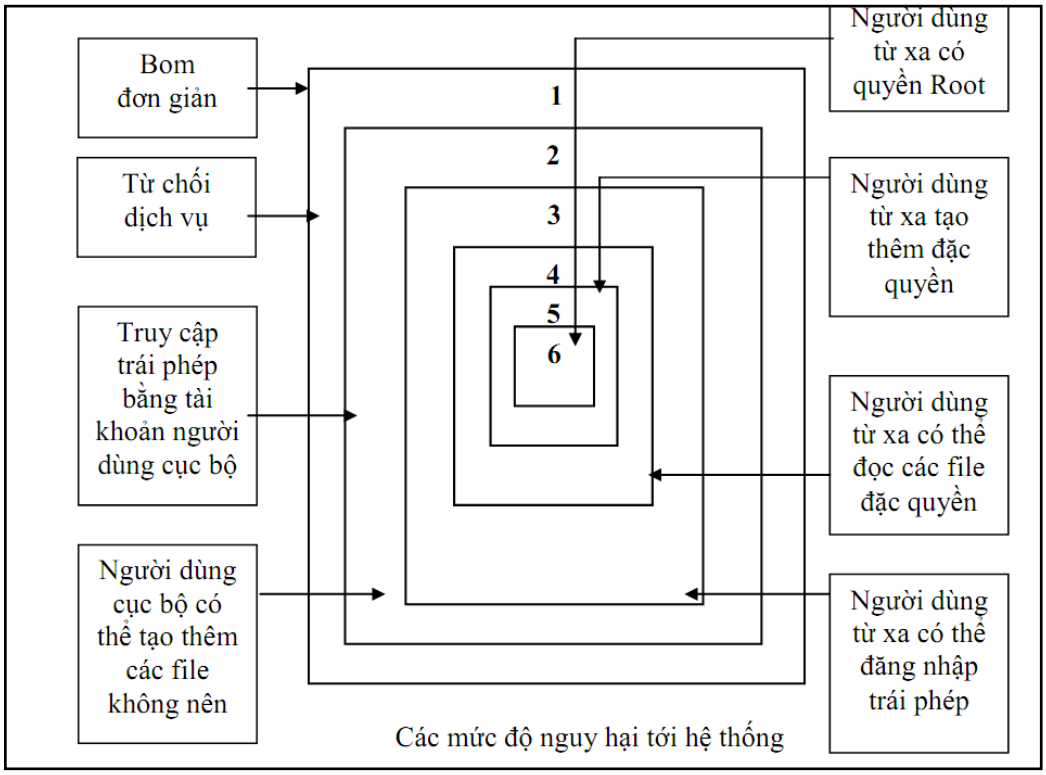
- Dựa vào những lỗ hổng bảo mật trên mạng: những lỗ hổng này có thể là các điểm yếu của dịch vụ mà hệ thống cung cấp. Ví dụ kẻ tấn công lợi dụng các điểm yếu trong các dịch vụ mail, ftp, web… để xâm nhập và phá hoại.

- Sử dụng các công cụ để phá hoại: ví dụ sử dụng các chương trình phá khóa mật khẩu để truy nhập bất hợp pháp vào một số chương trình.

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

2.1.3. Các mức độ nguy hiểm đến hệ thống thông tin

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



Hình 2.1Các mức độ nguy hiểm đến hệ thống thông tin

Mức 1: Tấn công vào một số dịch vụ mạng: Web, Email dẫn đến các nguy cơ lộ các thông tin về cấu hình mạng. Các hình thức tấn công ở mức này có thể dùng DoS hoặc Spam mail.

Mức 2: Kẻ phá hoại dùng tài khoản của người dùng hợp pháp để chiếm đoạt tài nguyên hệ thống (dựa vào các phương thức tấn công như bẻ khóa, đánh cắp mật khẩu…). Kẻ phá hoại có thể thay đổi quyền truy nhập thông qua các lỗ hổng bảo mật đọc các thông tin trong tập tin liên quan đến hệ thống như "/etc/passwd" (Linux) và SAM file (Windows).

Mức 3 đến mức 5: Kẻ phá hoại không sử dụng quyền của người dùng thông thường, mà có thêm một số quyền cao hơn với hệ thống như quyền kích hoạt một số dịch vụ, xem xét các thông tin khác trên hệ thống.

Mức 6: Kẻ tấn công chiếm được quyền Root hoặc Administrator trên hệ thống.

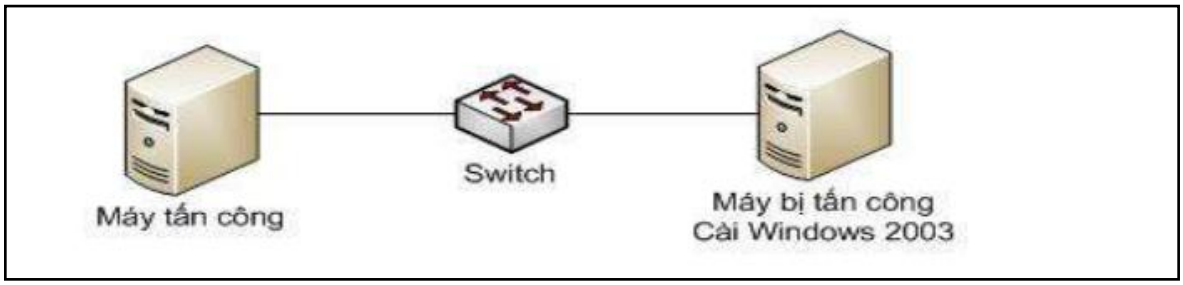
2.2. MỘT SỐ VÍ DỤ TẤN CÔNG VÀO LỖ HỔNG THIẾU AN TOÀN

2.2.1. Tấn công hệ điều hành

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

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

2.2.1.1 .Tấn công password của người dùng tài khoản Windows



Hình 2.2: Tấn công password

1/. Trên máy cục bộ

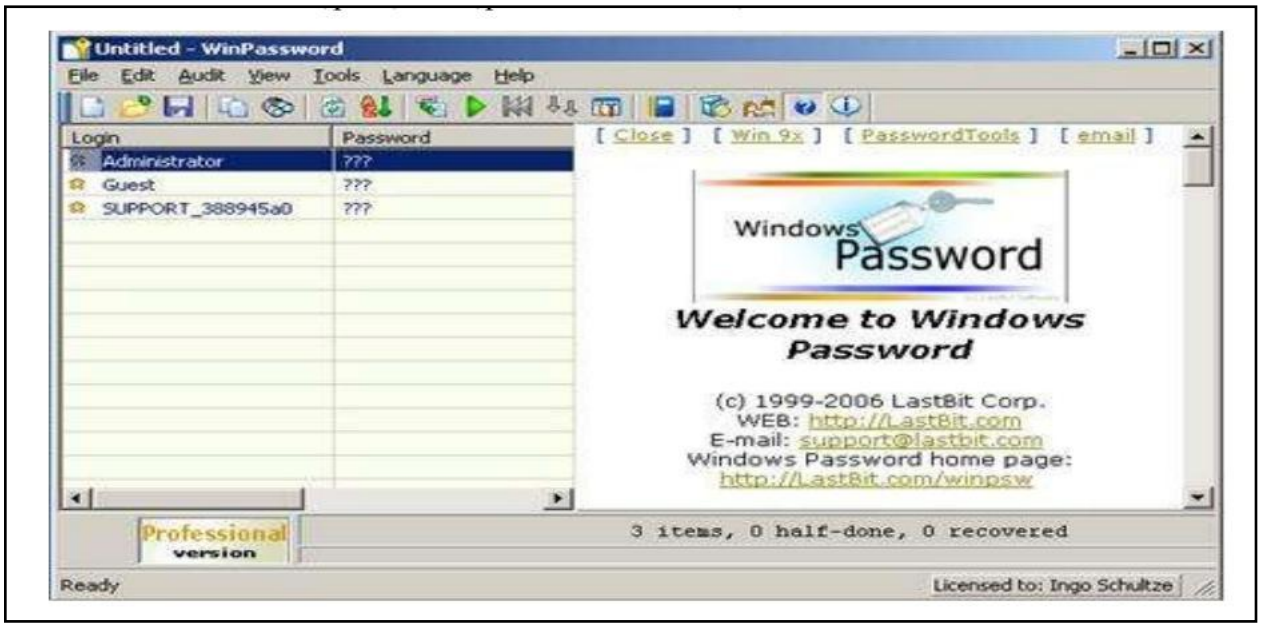
- Giả sử chúng ta không biết mật khẩu của một máy tính trong hệ thống, nhưng nhờ người đó gõ mật khẩu của họ và cho ta mượn máy tính dùng tạm.Và giờ là làm thế nào để biết được mật khẩu trên máy ta đang đăng nhập.

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

Giả sử sử dụng WinPasswordPro.

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

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



Hình 2.3: Giao diện WinPassword

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

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

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

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

Sau khi Import từ file PWDUMP ta được

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

+ Bắt ép thô bạo (brute force).

+ Từ điển (Dictionary).

+ Bảng thông minh (Smart table).

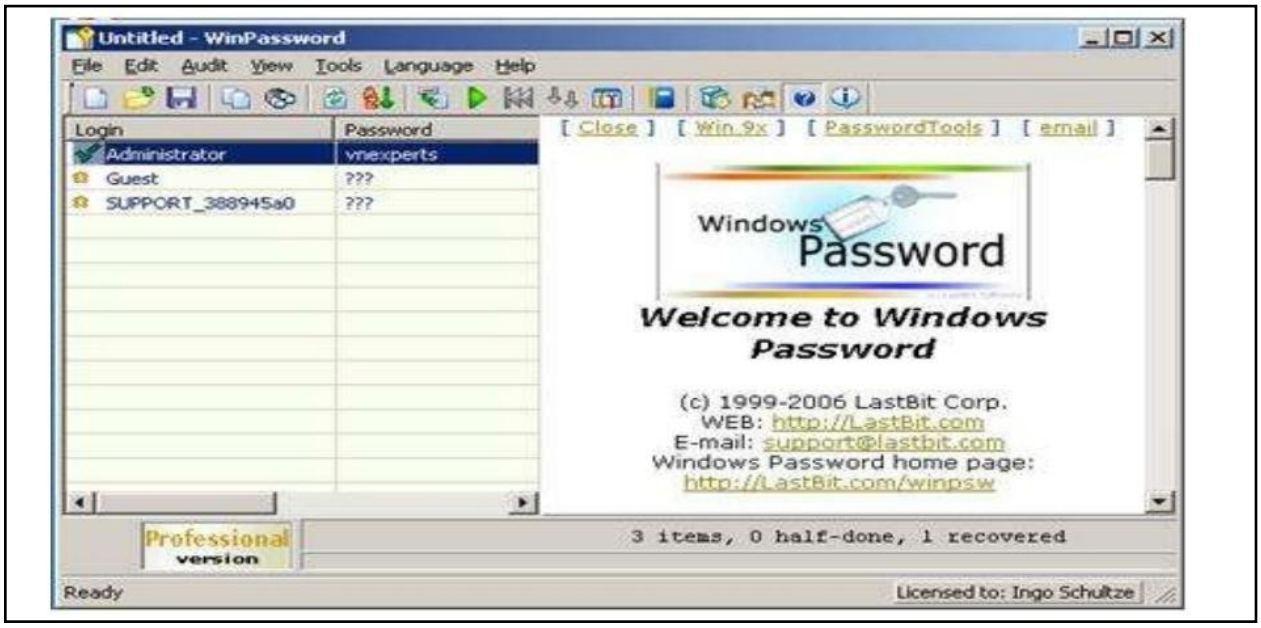
Chọn phương thức tấn công bắt ép thô bạo:

Đợi khoảng 15 phút (password không đặt ký tự đặc biệt, không số, không

hoa và 9 ký tự)

- Kết thúc quá trình ta đã giải mã được tệp mật khẩu đã được mã hoá với:

Tên người dùng là administrator và mật khẩu vnexperts:



Hình 2.4: Kết quả giải mã

2/. Tấn công máy tính từ xa

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

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

- Ở đây sử dụng PasswordDump Version 6.1.6.

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

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

2.2.1.2. Tấn công hệ thống Windows qua lỗ hổng thiếu an toàn

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

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

Bật chương trình Retina Network Security Scanner.

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

Để phát hiện ra lỗ hổng bảo mật sử dụng Tab Audit. Nhấn Start - Chọn Scan Template là chế độ Complete Scan.Đợi một lát thu được kết quả là lỗ hổng bảo mật. Đọc các thông tin về lỗ hổng tìm được để tìm cách tấn công.

Đây là phần mềm có bản quyền.

2/. Sử dụng Metasploit để khai thác

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

2.2.1.3. Ví dụ khác

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

Trong thông báo đưa ra, symantec cho biết đang ghi nhận được các dấu hiệu khai thác lỗ hổng giao diện thiết bị đồ họa (GDI). Microsoft xếp hai lỗ hổng này vào mức "nghiêm trọng", có thể ảnh hưởng tới các phiên bản Windows, kể cả hai phiên bản hệ điều mới nhất Windows Vista SP1 và Server 2008. Tin tặc có thể khai thác lỗ hổng bằng cách kích hoạt một tệp hình ảnh WMF (Windows Metafile) hoặc EMF (Enhanced Meta file) được chế tạo đặc biệt. Tin tặc sẽ nhanh chóng thành công với mã khai thác lỗ hổng bởi chỉ cần một động tác xem ảnh đơn giản trên mạng hoặc trong e-mail, cũng khiến cho hệ thống có thể bị tấn công.

2.2.2. Tấn công trên mạng

2.2.2.1. Tấn công từ chối dịch vụ

Tấn công từ chối dịch vụ (DoS -Denial of Service) là một loại hình tấn công hệ thống mạng nhằm ngăn cản những người dùng hợp lệ được sử dụng một dịch vụ nào đó. Các cuộc tấn công có thể được thực hiện nhằm vào bất kì một thiết bị mạng nào bao gồm tấn công vào các thiết bị định tuyến, web, E-mail, hệ thống DNS,… Tấn công DoS phá huỷ dịch vụ mạng bằng cách làm tràn ngập số lượng kết nối, quá tải server hoặc chương trình chạy trên server, tiêu tốn tài nguyên của server, hoặc ngăn chặn người dùng hợp lệ truy nhập tới các dịch vụ mạng.

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

Có năm kiểu tấn công cơ bản sau:

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

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

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

Nhận diện dấu hiệu của một vụ tấn cống từ chối dịch vụ:

- Mạng thực thi chậm khác thường (mở file hay truy cập website)
- Không thể dùng một website cụ thể
- Không thể truy cập bất kỳ website nào
- Tăng lượng thư rác nhận được (như một trận “bomb mail”)

2.2.2.2. Tấn công giả mạo hệ thống tên miền trên Internet

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

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

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

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

2.2.3. Tấn công cơ sở dữ liệu

Ví dụ: SQL Injection attack

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

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

này, người ta có thể dùng 2 trang, một trang HTML để hiển thị form nhập liệu và một trang ASP dùng để xử lí thông tin nhập từ phía người dùng.

Ví dụ:

Login.htm

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

ExecLogin.asp

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

Đoạn mã trong trang ExecLogin.asp dường như không chứa bất cứ một lỗ hổng về an toàn nào. Người dùng không thể đăng nhập mà không có tên đăng nhập và mật khẩu hợp lệ. Tuy nhiên đoạn mã này không an toàn và là tiền đề cho một SQL Injection attack. Đặc biệt, sơ hở nằm ở chỗ dữ liệu nhập vào từ người dùng được dùng

để xây dựng trực tiếp câu lệnh truy vấn SQL. Điều này cho phép những kẻ tấn công có thể điều khiển câu truy vấn sẽ được thực hiện.

Ví dụ, nếu người dùng nhập chuỗi sau vào trong cả 2 ô nhập liệu tên người dùng/mật khẩu của trang Login.htm: " or "=" . Lúc này, câu truy vấn sẽ được gọi thực hiện là:

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

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

Các tác hại của SQL Injection attack:

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

2.3. CÁC PHƯƠNG PHÁP PHÒNG TRÁNH TẤN CÔNG BẰNG XỬ LÝ LỖ HỔNG

2.3.1. Bảo vệ an toàn thông tin

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

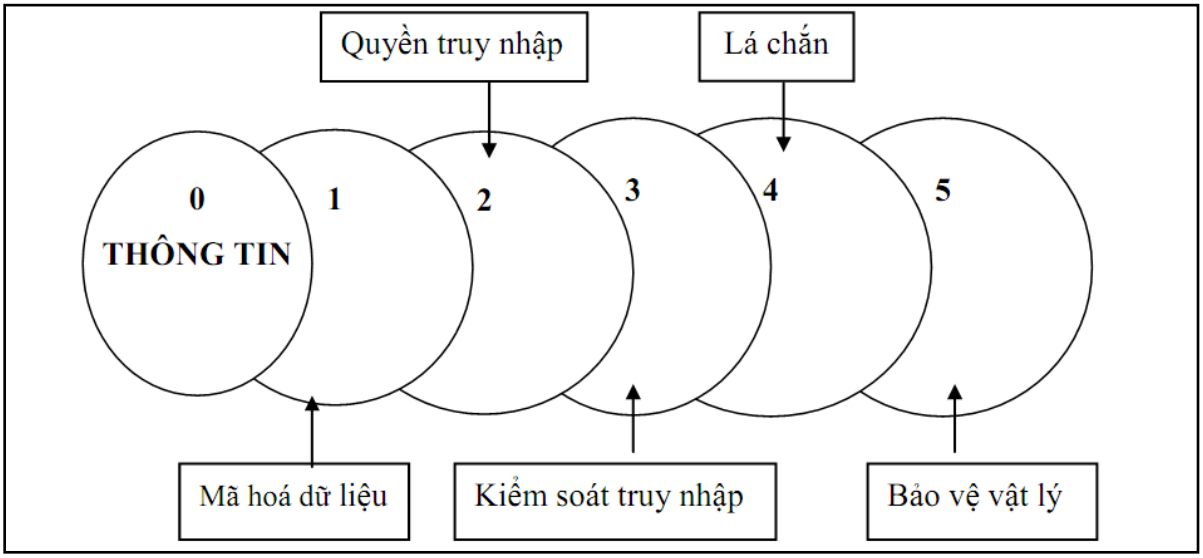
2.3.1.1. Các lớp bảo vệ thông tin

Trong thời đại phát triển của công nghệ thông tin, mạng máy tính quyết định toàn bộ hoạt động của cá nhân, cơ quan, tổ chức, hay các công ty, xí nghiệp.

Vi vậy, việc bảo đảm cho hệ thống máy tính hoạt động một cách an toàn, không xảy ra sự cố là công việc cấp thiết hàng đầu. Công tác quản trị mạng máy tính phải được thực hiện một cách khoa học.

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

Thông thường gồm các mức bảo vệ sau:



Hình 2.5: Các lớp bảo vệ thông tin

1/. Mã hóa dữ liệu

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

2/. Quyền truy nhập

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

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

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

3/. Kiểm soát truy nhập (Đăng ký tên/mật khẩu)

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

Thực ra đây cũng là kiểm soát truy nhập, nhưng không phải truy nhập ở mức thông tin mà ở mức hệ thống. Người quản trị mạng có trách nhiệm quản lý, kiểm soát mọi hoạt động của mạng và xác định quyền truy nhập của những người dùng khác theo thời gian và không gian (nghĩa là người dùng chỉ được truy nhập trong một khoảng thời gian nào đó). Theo lý thuyết nếu mọi người đều giữ kín được mật khẩu và tên đăng ký của mình thì sẽ không xảy ra các truy nhập trái phép. Nhưng điều đó khó đảm bảo trong thực tế vì nhiều nguyên nhân khác nhau dẫn đến làm giảm hiệu quả của lớp bảo vệ này. Có thể khắc phục bằng cách người quản trị mạng chịu trách nhiệm đặt mật khẩu hoặc thay đổi mật khẩu theo thời gian hay theo chu kỳ nhất định.

4/. Lá chắn

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

5/. Bảo vệ vật lý

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

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

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

6/. Các công cụ bảo vệ thông tin

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

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

Tường lửa:

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

7/. Phần mềm quản trị người dùng và kiểm soát mạng

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

8/. Phần mềm chống virus, mã độc , gián điệp (spyware)

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

9/. Giám sát hành vi

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

10/. Dùng phiên bản trình duyệt mới

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

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

11/. Phần mềm mã hóa dữ liệu

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

2.3.2. Phòng tránh tấn công hệ điều hành

2.3.2.1. Phòng tránh tấn công hệ điều hành

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

1/. Thường xuyên cập nhật thông tin về các lỗi bảo mật liên quan đến HĐH mình đang sử dụng trên Website của Microsoft và các diễn đàn bảo mật khác. Không chỉ cần sử dụng các bản cập nhật của Windows mà cần phải chú ý tới các bản cập nhật của Unix/ Linux và Mac khi chúng được phát hành. Trong hầu hết trường hợp, những phiên bản hệ điều hành mới luôn an toàn hơn so với các phiên bản trước đó dù đã được vá hoàn toàn. Ví dụ, Windows 7 và Windows Vista tích hợp cơ chế bảo mật như UAC(User Account Control : điều khiển tài khoản người dùng), chế độ bảo mật cho IE, công cụ mã hóa ổ đĩa BitLocker,…. Mà WinXP không có. Phiên bản Mac OS X mới nhất tích hợp công cụ phát hiện malware. Phiên bản mới nhất của OpenSUSE hỗ trợ công nghệ modul nền tảng tin cậy (TPM – Trusted Platform Module). Trong nhiều trường hợp quá trình nâng cấp lên phiên bản mới của bất kỳ hệ điều hành nào cũng giúp tăng cường bảo mật.

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

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

4/. Thiết lập danh sách những dải địa chỉ IP có nguy cơ cao truy cập vào (có thể tìm thông tin về những dải địa chỉ này từ một số trang web uy tín.)

5/. Thiết lập một tường lửa mềm, hoặc sử dụng một phần mềm tường lửa miễn phí hay thương mại; thiết lập thời gian cho phép truy nhập vào máy chủ, những ứng dụng cho phép chạy, những người dùng được phép truy cập từ xa (Remote) , …

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

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

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

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

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

10/. Chú ý đến an toàn vật lý.

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

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

2.3.2.2. Một số ví dụ cụ thể

1/. Phòng tránh tấn công mật khẩu của tài khoản người dùng

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

2/. Phòng tránh tấn công hệ thống Windows qua lỗ hổng bảo mật

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

2.3.2.3. Xây dựng hệ thống tường lửa

1/. Khái niệm tường lửa

Hình 2.6: Khái niệm tường lửa

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

Phạm vi hẹp hơn. Trong mạng nội bộ người ta sử dụng tường lửa để ngăn cách giữa các miền an toàn với nhau.

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

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

2/. Chức năng của tường lửa

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

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

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

3/. Phân loại tường lửa

Về mặt vật lý :

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

Về mặt chức năng :

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

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

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

4/. Nguyên tắc hoạt động của tường lửa

Nguyên tắc chung : trước khi xây dựng một tường lửa phải nghiên cứu rất kỹ lưỡng và phải nắm rất rõ mạng đó. Điều này cần thiết phải được tổ chức tốt bao gồm nhiều công đoạn khác nhau , có thể kết nối với nhau. Việc kết nối này có thể là tự động hoặc nhờ sự tác động của con người. Đối với một số mạng (IPS – các nhà cung cấp dịch vụ internet) thì việc sử dụng tường lửa là hoàn toàn không cần thiết vì sẽ mất khách hàng nếu áp dụng một loạt các chính sách cứng nhắc. Một số vấn đề nữa là khi sư dụng các dịch vụ như ftp , telnet … thì nó cũng tạo ra một số vấn đề truy nhập dịch vụ.

Lọc gói : Kiểu tường lửa chung nhất là kiểu tường lửa dựa trên mô hình mạng OSI. Tường lửa mức mạng thường hoạt động theo nguyên tắc router, nghĩa là tạo ra các luật cho phép ai , cái gì được truy nhập mạng dựa trên mức mạng, Mô hình này dựa trên hoạt động gói tin packet filtering. Nó kiểm tra các gói tin trên router từ mạng ngoài. Ở kiểu hoạt động này các gói tin đều được kiểm tra địa chỉ nguồn nơi chúng xuất phát . Thông qua địa chỉ IP nguồn dược xác định thì nó kiểm tra với các luật đã được đặt trên router.

Tường lửa mức ủy quyền ứng dụng : Kiểu tường lửa này hoạt động khác với kiểu tường lửa trước, nó dựa trên phần mềm . Khi một kết nối từ người nào đó đến mạng sử dụng kiểu tường lửa này thì kết nối đó sẽ bị chặn lại. Sau đó tường lửa sẽ kiểm tra các trường có tổng quan của gói tin yêu cầu kết nối. Nếu việc kiểm tra thành công , tức là các trường thông tin đáp ứng được các luật đã đặt ra trên tường lửa, nó sẽ tạo một cái cầu kết nối giữa 2 nút với nhau. Ưu điểm của tường lửa loại này là không có chức năng chuyển tiếp giữa các gói tin IP, hơn nữa ta có thể điều khiển một cách chi tiết hơn các kết nối trong qua tường lửa. Đồng thời nó còn đưa ra nhiều công cụ cho phép ghi lại các quá trình kết nối cũng như các gói tin chuyển qua tường lửa đều được kiểm tra kỹ lưỡng với các luật trên tường lửa và rồi nếu như được chấp nhận sẽ chuyển tới nút đích. Sự chuyển tiếp các gói tin IP xảy ra khi một máy chủ nhận được rồi chuyển chúng vào mạng trong. Điều này tạo ra lỗ hổng cho những kẻ phá hoại xâm nhập vào mạng trong. Nhược điểm của tường lửa hoạt động trên ứng dụng là phải tạo cho mỗi dịch vụ trên mạng một trình ứng dụng ủy quyền trên tường lửa.

5/. Các bước xây dựng tường lửa

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

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

Xây dựng kiến trúc mạng và giao thức cần thiết: bước đầu tiên là cần phải hiểu toàn bộ mạng, công việc này không chỉ đơn giản là xem lại các máy, các giấy tờ văn bản, … Nó phải được thảo luận với các phòng với nhau. Công việc đầu tiên là xác định cái nào bị cấm, cái nào không bị cấm, cũng như phải liệt kê tất cả các giao thức cần thiết sử dụng trên mạng. Đây là công việc khá phức tạp.

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

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

2.3.3. Phòng tránh tấn công phần mềm ứng dụng

2.3.3.1. Chủ quan (Lỗi do người viết phần mềm)

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

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

2.3.3.2. Khách quan (Lỗi do người)

Quản lý bằng tên, mật khẩu riêng.

Đảm bảo thông tin người dùng luôn được giữ bí mật

Học cách tự bảo vệ chính mình, thiết lập hệ thống bảo mật toàn diện, nhiều lớp.

Thường xuyên cập nhật các bản vá lỗi mới nhất từ các nhà sản xuất. Cập nhật các cảnh báo được đề phòng trước.

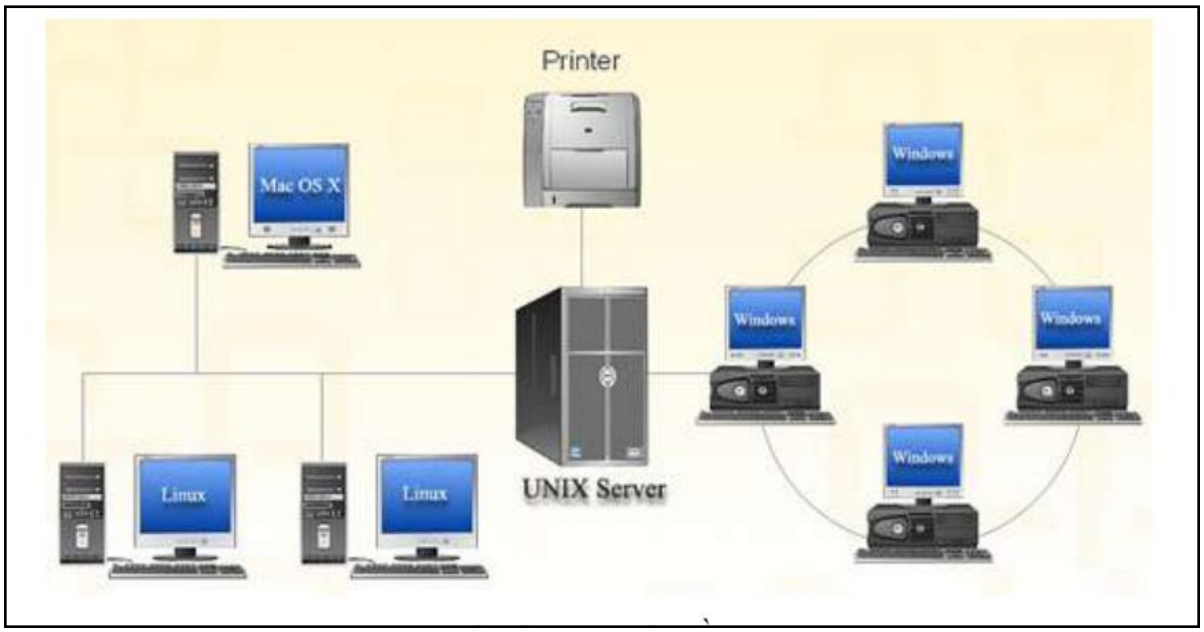
Khai thác tối ưu các tính năng bảo mật của chính những phần mềm này.

2.3.4. Phòng tránh tấn công mạng

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

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

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



Hình 2.7: Mạng đa nền tảng

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

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

Cần phải thường xuyên thống kê thành phần mạng vì:

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

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

Cập nhật và nâng cấp:

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

Thông thường nhắc đến Windows, người ta thường coi đây là hệ thống "yếu nhất" và các hệ thống khác là "an toàn". Tuy nhiên không hẳn như vậy, chỉ là do windows được nhiều người sử dụng nên đây là món mồi hấp dẫn nhất đối với tin tặc.Ví dụ : trong năm 2009 một lỗ hổng trong nhân Linux được phát hiện, trong toàn bộ các phiên bản của Linux cho phép tin tặc có thể kiểm soát toàn bộ hệ thống. Cũng năm 2009 Apple đã phải phát hành bản vá, có tổng cộng 67 lỗ hổng bảo mật có trong hđh MAC OS X và ứng dụng trình duyệt safari, chưa kể một lỗ hổng nguy hiểm trong java bị bỏ xót.

Ví dụ cụ thể phòng tránh tấn công dịch vụ DoS và DDoS

Hậu quả của các cuộc tấn công từ chối dịch vụ gây ra không chỉ tốn nhiều tiền bạc mà còn tốn nhiều công sức, thời gian để hệ thống hồi phục. Vì vậy nên sử dụng những biện pháp sau để phòng chống DoS và DDoS

Phòng ngừa các điểm yếu ứng dụng

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

Phòng ngừa việc tuyển mộ zombies

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

Ngăn ngừa kênh phát động tấn công sử dụng công cụ

Có rất nhiều công cụ tự động tấn công, chủ yếu là tấn công phân tán DDoS TFN, tấn công dựa trên nguyên lý UDP , SYN.. Các công cụ này có đặc điểm là cần phải có các kênh phát dộng để zombie thực hiện tấn công tới mục tiêu cụ thể. Hệ thống cần có sự giám sát ngăn ngừa các kênh phát động đó.

Ngăn chặn tấn công trên băng thông

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

Ngăn chặn tấn công qua SYN

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

Phát hiện và ngăn chặn tấn công "tới hạn" số kết nối

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

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

Phát hiện và ngăn chặn tấn công tới hạn tốc độ thiết lập kết nối

Một trong những điểm mà các server thường bị lợi dụng là khả năng các bộ đệm giới hạn dành cho tốc độ thiết lập kết nối. Ở đây việc áp dụng bộ lọc để giới hạn số lượng kết nối trung bình rất quan trọng. Một bộ lọc sẽ xác định ngưỡng tốc độ kết nối cho từng đối tượng mạng. Thông thường việc này sẽ được xác định bằng số lượng kết nối trong một thời gian nhất định để cho phép sự dao động trong lưu lượng

2.3.5 Mạng riêng ảo VPN

Hình 2.8: Mô hình VPN

2.3.5.1. Khái niệm mạng riêng ảo

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

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

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

Tính bảo mật, riêng tư : người ngoài cuộc khó có thể hiểu được liên lạc đó.

Tính toàn vẹn : người ngoài cuộc khó có thể thay đổi được liên lạc đó.

Tính xác thực : người ngoài cuộc khó có thể tham gia vào liên lạc đó.

2.3.5.2 Các thành phần của mạng riêng ảo

1/. Định đường hầm

Định đường hầm là một cơ chế dùng để đóng gói 1 giao thức vào trong 1 giao thức khác.

Trên internet, định đường hầm giúp cho những giao thức như IPX , GoogleTalk được đóng gói trong IP.

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

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

2/. Bảo mật

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

3/. Thỏa thuận về chất lượng dịch vụ

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

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

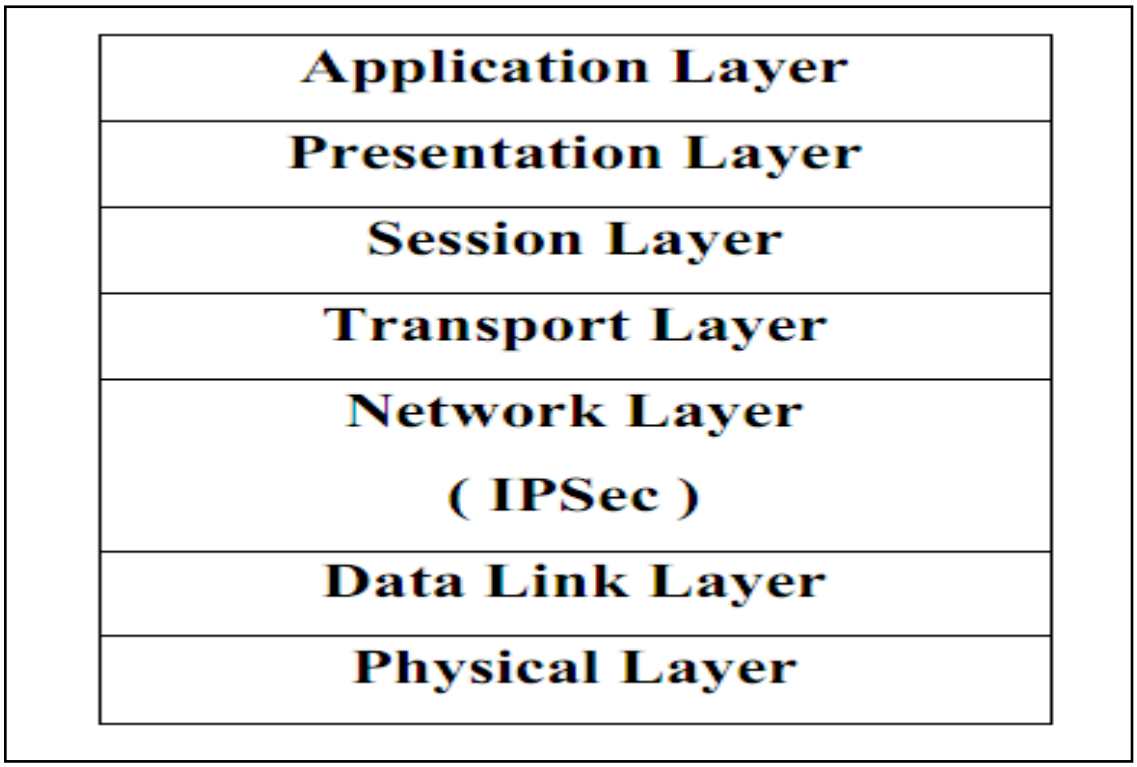
2.3.6. Tổng quan về công nghệ IPSec

2.3.6.1. Khái niệm IPSec

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

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

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



Hình 2.9: Mô hình OSI

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

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

2.3.6.2. IPSec và mục đích sử dụng

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

1/. Cài đặt IPSec

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

2/. Mục đích của IPSec

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

3/. Những thuận lợi khi sử dụng IPSec

Thuận lợi chính khi sử dụng IPSec là cung cấp được giải pháp mã hóa cho tất cả các giao thức hoạt động ở tầng 3 – tầng mạng trong mô hình OSI và kể các giao thức lớp cao hơn.

4/. Khả năng cung cấp bảo mật của IPSec

Chứng thực 2 chiều trước và trong suốt quá trình giao tiếp. IPSec quy định cho cả 2 bên tham giao tiếp phải xác định chính mình trong suốt quá trình giao tiếp.

Tạo sự tin cậy qua việc mã hóa, và xác nhận số các gói. IPSec có 2 chế độ là Encapsulating Security PayLoad (ESP), cung cấp cơ chế mã hóa dùng nhiều thuật toán khác nhau và sự thẩm định quyền của người lãnh đạo (AH – Authentication Header) xác nhận các thông tin chuyển giao nhưng không mã hóa.

Tích hợp các gói tin chuyển giao và sẽ loại ngay bất kỳ thông tin nào bị chỉnh sửa. Cả 2 loại ESP và AH đều kiểm tra tính tích hợp của các thông tin chuyển giao. Nếu một gói tin đã bị chỉnh sửa thì các xác nhận số sẽ không trùng khớp, kết quả gói tin sẽ bị loại. ESP cũng mã hóa đía chỉ nguồn , cũng như địa chỉ đích như là một phần của việc mã hóa thông tin chuyển giao.

Chống lại các cuộc tấn công làm chạy lại, thông tin chuyển giao qua mạng sẽ bị kẻ tấn công chặn lại , chỉnh sửa , và được gửi đi sau đó đến đúng địa chỉ người nhận, người nhận không hề hay biết mà vẫn tin rằng đó là thông tin hợp pháp. IPSec dùn kỹ thuật đánh số liên tiếp cho các gói tin của mình (Sequence Number) , nhằm làm cho kẻ tấn công không thể sử dụng lại các dữ liệu đã chặn được , với ý đồ bất hợp pháp. Dùng kỹ thuật đánh số liên tiếp còn giúp bảo vệ chống việc chặn và đánh cắp dữ liệu, sau đó dùng những dữ liệu để truy cập hợp pháp vào một ngày nào đó.

Ví dụ sử dụng IPSec

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

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

IPSec làm việc thế nào?

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

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

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

Liên kết bảo mật mang tính chất thương lượng. Nếu máy A yêu cầu xác thực thông qua chứng nhận và máy B yêu cầu dùng giao thức Kerberos thì IKE (Internet Key Exchange) sẽ có trách nhiệm thương lượng để tạo liên kết bảo mật , thiết lập liên kết giữa 2 máy tính.

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

Chính sách bảo mật IPSec

IPSec bao gồm một hay nhiều luật xác định cách thức hoạt động của IPSec. Các nhà quản trị có thể cài đặt IPSec thông qua một chính sách. Mỗi chính sách có thể chứa 1 hoặc nhiều luật , nhưng chỉ có thể xác định 1 chính sách hoạt động tại máy tính tại một thời điểm bất kỳ. Các nhà quản trị phải kết hợp tất cả các luật mong muốn vào một chính sách đơn giản . Mỗi luật bao gồm:

- Bộ lọc (Filter) : bộ lọc báo cho chính sách những thông tin lưu chuyển nào sẽ áp dụng với hành động lọc. Ví dụ : người quản trị có thể tạo một đầu lọc chỉ xác định các lưu thông dạng HTTP hoặc FTP.
- Hành động lọc : báo cho chính sách phải đưa ra hành động gì nếu thông tin lưu chuyển trùng với định dạng đã xác định tại filter . Ví dụ : thông báo cho IPSec chặn tất cả các những giao tiếp FTP , nhưng với những giao tiếp HTTP thì dữ liệu sẽ được mã hóa. Hành động lọc cũng có thể xác định những thuật toán mã hóa và hàm băm mà chính sách nên sử dụng.
- Authentication method : IPSec cung cấp 3 phương thức xác thực

Các chứng chỉ (thông thường các máy tính triển khai dùng IPSec nhận các chứng chỉ từ một tổ chức cấp chứng chỉ CA) , Kerberos (giao thức chứng thực phổ biến trong AD) Preshared Key (khóa ngầm hiểu , một phương pháp xác thực đơn giản). Mỗi một luật của chính sách IPSec có thể bao gồm nhiều phương thức xác thực vừa nêu.

Những chính sách IPSec mặc định

Kể từ windows 200 trở đi IPSec đã cấu hình sẵn 2 chính sách , tạo sự thuận tiện khi triển khai IPSec .

Máy trạm

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

Luật này cho phép máy tính phản hồi đến các yêu cầu IPSec ESP từ các máy tính được tin cậy trong AD Domain. ESP là một chế độ IPSec cung cấp độ tin cậy cho việc xác thực , tích hợp và chống sự tấn công lặp lại.

Máy chủ (Server) (Request security – yêu cầu bảo mật)

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

Máy chủ bảo mật – Sercure Server (Require Sercurity – quy định bảo mật)

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

Thương lượng một liên kết bảo mật

Cả 2 máy tính tiến hành thương lượng bảo mật cần phải có những chính sách bổ sung. Nếu 2 máy tính có thể thương lượng thành công, IPSec có thể sử dụng. Nếu thương lượng không thành công do bất đồng về chính sách, 2 máy tính có thể không tiếp tục giao tiếp hoặc chấp nhận giao tiếp không an toàn. Ví dụ về cách thức hoạt động của các chính sách giữa 2 máy tính giữa A và B:

- Máy tính A yêu cầu ESP cho các giao tiếp HTTP , máy tính B yêu cầu AH cho HTTP, như vậy 2 máy tính sẽ không thể thương lượng một liên kết bảo mật.

- Giao thức xác thực Kerberos là phương thức xác thực mặc định , được các máy tính trong cùng AD Forest sử dụng , nếu 1 trong 1 máy tính không cùng AD forest thì không thể thương lượng được phương thức bảo mật. Tương tự, khi máy tính A dùng Kerberos, máy tính B dùng Certificates làm phương thức xác thực lưu lượng IP, thương lượng cũng sẽ không được thiết lập.

2.3.6.3.Ưu điểm và hạn chế của IPSec

Ưu điểm của IPSec

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

- IPSec là một giải pháp tổng thể. Nó có thể bảo vệ bất kỳ giao thức nào chạy trên IP và bất kỳ môi trường nào mà IP chạy trên nó. Đồng thời còn bảo vệ được nhiều giao thức ứng dụng chạy trên nhiều môi trường phức tạp.

- IPSec cung cấp một số dịch vụ bảo mật ở mức nền, không gây ảnh hưởng đến người dùng.

- IPSec là cơ chế chung để bảo mật IP. Nó không cung cấp chức năng bảo mật thư nhưng có thể mã hóa thư. Nên nó đảm bảo kẻ tấn công không thể hiểu được thư dù đánh cắp hay đọc trộm.

- IPSec có thể cung cấp cùng một cơ chế bảo mật cho bất kỳ cái gì truyền qua IP.

- Người dùng sử dụng IPSec không phải làm bất kỳ một thao tác nào. Thậm chí họ có thể không cần biết sự tồn tại của nó. Mọi việc thiết lập , cài đặt đều do người quản trị làm.

Hạn chế của IPSec

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

- IPSec không an toàn nếu sử dụng hệ thống không an toàn. Nếu hệ thống không an toàn thì việc sử dụng IPSec cũng không an toàn như sử dụng nó với 1 hệ thống bình thường.

- IPSec không bảo mật ở dạng End to End. Nó không đảm bảo tính bảo mật giữa những người sử dụng cuối, bất kỳ người sử dụng nào với quyền thích hợp trên 1 máy tính bất kỳ, lưu trữ gói tin nhận được đều có thể biết được nội dung của nó.

- IPSec xác thực máy , không xác thực người dùng.

- IPSec không ngăn chặn kiểu tấn công DoS.

- IPSec không ngăn chặn được các phân tích truyền thông mạng. Là việc cố gắng tìm tri thức từ các gói tin mà không quan tâm đến nội dung của nó. Các phân tích dựa trên những gì đã nhìn thấy được ở các Header không được mã hóa của các gói tin đã mã hóa , địa chỉ cổng, máy nguồn , đích , độ dài gói tin.

2.3.7. Phòng tránh tấn công CSDL

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

2.3.7.1. Giải pháp phòng tránh tấn công CSDL

Lựa chọn phần cứng , nơi lưu trữ đảm bảo an toàn cho dữ liệu.

Lựa chọn phần mềm phù hợp để lưu trữ dữ liệu.

Có giải pháp dự phòng khi có sự cố xảy ra (Ví dụ : bao giờ cũng phải có 1 server backup,..)

Luôn cập nhật các bản vá lỗi , thông tin về nguy cơ bị tấn công để có biện pháp phòng tránh trước.

Giới hạn quyền trong CSDL đối với cả nhà quản trị và người dùng. Chỉ cấp quyền đủ để áp dụng nhu cầu của mỗi đối tượng. Quyền càng bị hạn chế , thiệt hại càng ít.

Cần phải sử dụng những công cụ mã hóa mạnh kết hợp với những giải pháp khác về bảo vệ an ninh hệ thống mạng , chống virus xâm nhập.

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

Giải pháp này tiến hành mã hóa CSDL như sau:

-Mã hóa bản thân CSDL sử dụng các khóa

-Mã hóa khóa

-Mã hóa quan hệ giữa khóa và CSDL.

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

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

2.3.7.2. Ví dụ phòng tránh tấn công lỗ hổng SQL injection attack

Để phòng tránh các nguy cơ có thể xảy ra, nên bảo vệ các câu truy vấn SQL bằng cách kiểm soát chặt chẽ tất cả các dữ liệu nhập vào từ đối tượng Request.

Trong trường hợp dữ liệu nhập vào là chuỗi , lỗi xuất phát từ việc có dấu nháy đơn trong dữ liệu. Để tránh điều này , thay thế các dấu nháy đơn bằng hàm Replace:

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

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

p_lngID = CLng(Request("ID"))

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

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

Chương 3. THỬ NGHIỆM CHƯƠNG TRÌNH

3.1. TẤN CÔNG SQL INJECTION

3.1.1. Bản chất

Cơ chế tấn công SQL Injection là cách thức tận dụng hoặc khai thác triệt để những khuyết điểm, thiếu sót về mặt công nghệ được sử dụng để xây dựng website , và thông thường hacker sẽ kết hợp với những lỗ hổng trong quy trình bảo mật cơ sở dữ liệu. Nếu thành công trong việc xâm nhập này, hacker hoàn toàn có thể mạo danh tài khoản chính thức của người sử dụng, truy cập vào cơ sở dữ liệu và lấy cắp thông tin cá nhân. Không giống như cách làm của DDOS, SQLI hoàn toàn có thể ngăn chặn được nếu người quản trị nhận thức được tầm quan trọng của việc bảo mật cơ sở dữ liệu.

3.1.2 Yêu cầu hệ thống

Yêu cầu phần cứng:

-128 MB RAM

-320 MB free fixed disk

-Tất cả hệ thống 32 bit (hệ thống 64 bit cũng làm việc tốt)

Yêu cầu phần mềm:

-Apache 2.2.14

-MySQL 5.2.41

-PHP 5.3.1

-Chạy Windows 200, XP (Server 2003), Vista (Server 2008), 7

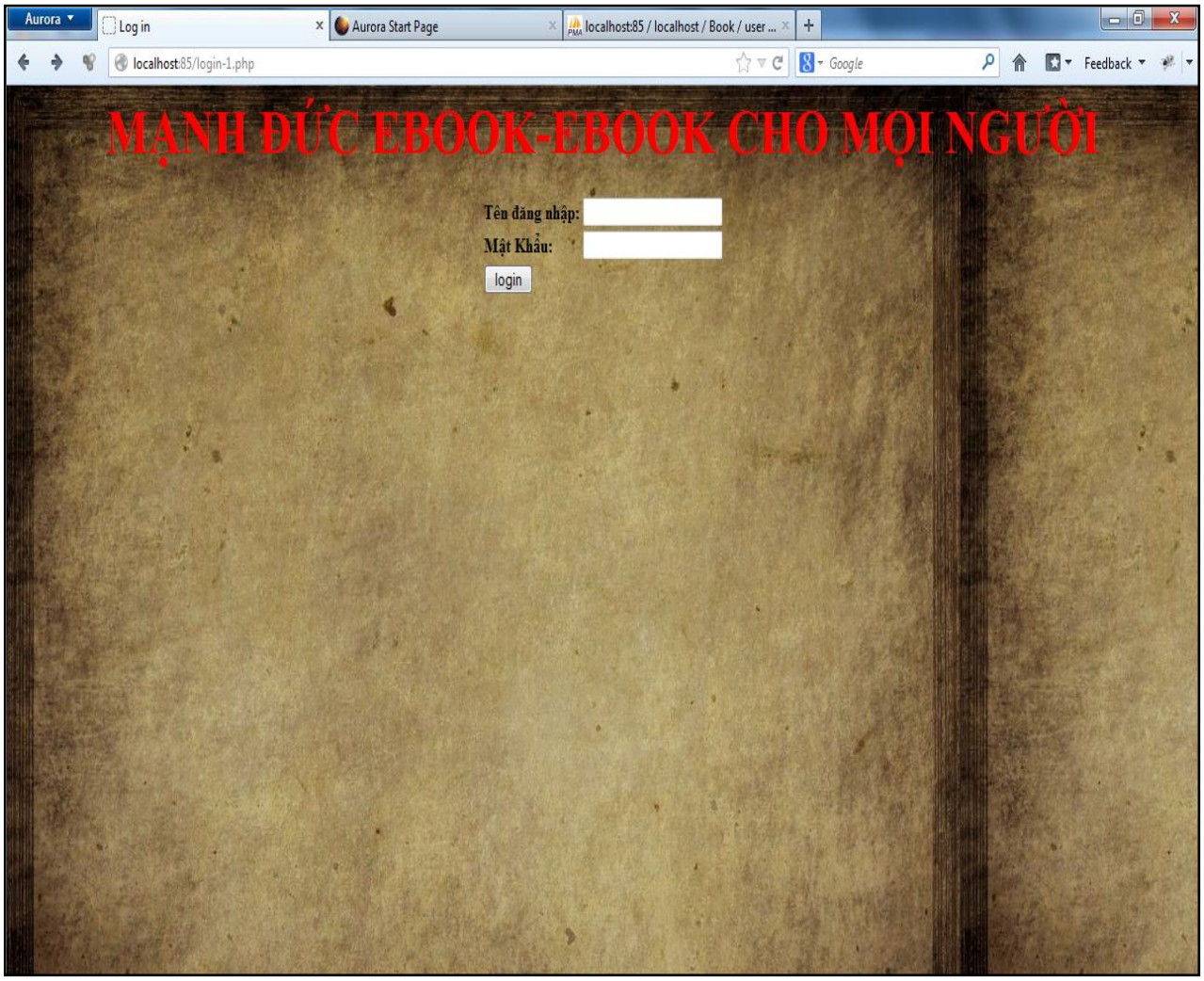
3.1.3. Quá trình thực hiện

Trong quá trình đăng nhập trực tuyến, người dùng buộc phải nhập username và mật khẩu vào form đăng nhập. Khi đó để xử lý quá trình nhập vào nhằm kiểm tra dữ liệu người sử dụng nhập vào có trong CSDL hay không. Người ta thường sử dụng chuỗi câu lệnh SQL sau:

sql= select nickname from user where nickname= 'name' and password= 'pass'

Nếu name và pass được nhập vào trùng khớp với dữ liệu đã có trên bảng user của CSDL, tức là đã xác thực chính xác có người dùng này.

Ví dụ : trang login-1.php được dùng để nhập dữ liệu vào form



Hình 3.1: Giao diện đăng nhập

Mã nguồn trang login-1.php :

<html>

<head><title>Log in</title></head>

<body background="bg-img1.jpg">

<blink>MẠNH ĐỨC EBOOK-EBOOK CHO MỌI NGƯỜI</blink>

```
<br>
<center><table border="0"><form action="login-2.php" method="get">
<tr><td><b>Tên đăng nhập:</b></td><td><input type= "text" name="nickname"></td></tr>
<tr><td><b>Mật Khẩu:</b></td><td><input type ="password" name="password"></td></tr>
<tr><td><input type="submit" value="login"></td></tr>
</form></table></center>
</body></html>
```

Trang login-2.php được dùng để kiểm tra tính xác thực của thông tin nhập vào.

Mã nguồn trang login-2.php:

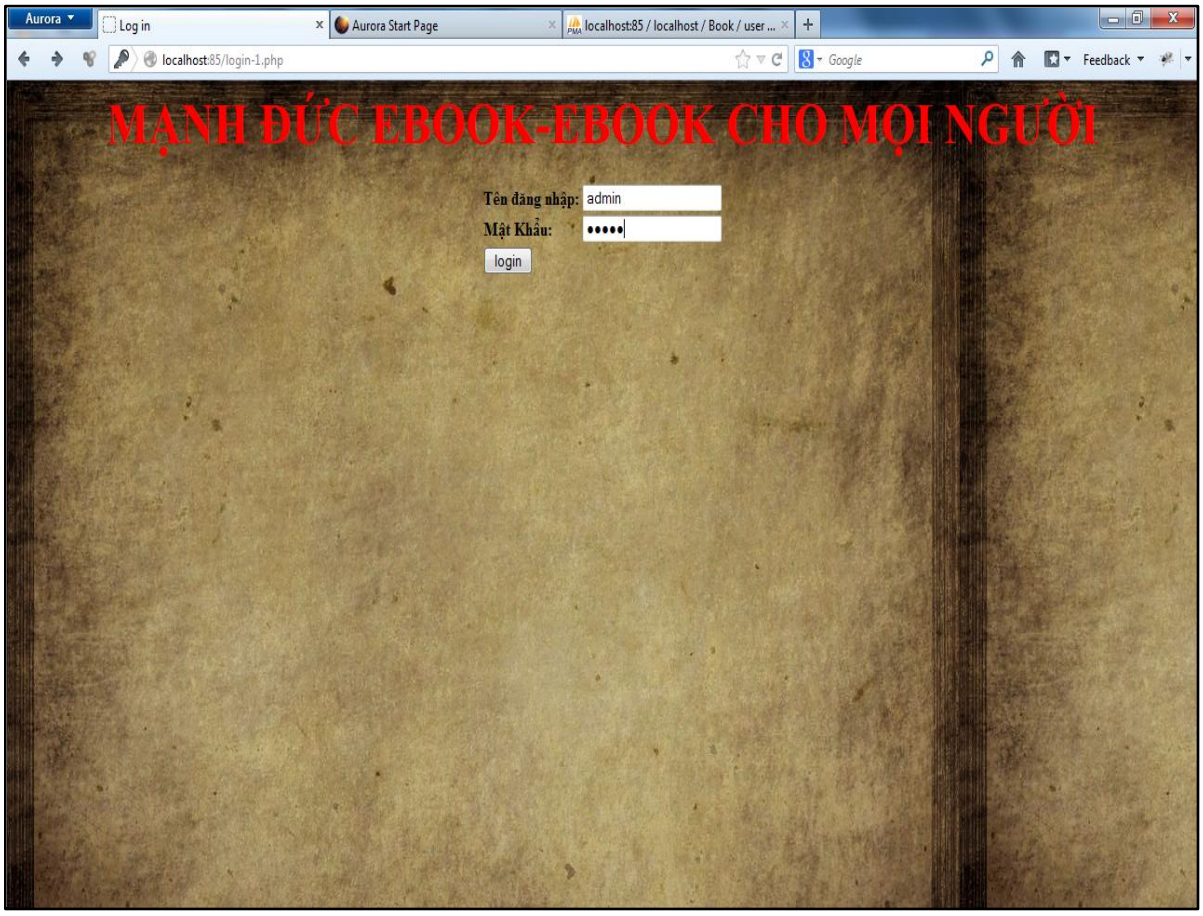
```
<?php
 require("kn.php");
$name=$_GET["nickname"];
$pass=$_GET["password"];
$sql="select nickname from user where nickname='".$name."'"."and password='".$pass."'";
$kq= mysql_query($sql,$sqlcnn);
$row=mysql_fetch_array($kq);
$rows=mysql_affected_rows();
 if($rows!=0)
 {

        echo "Chào mừng bạn  ".$row['nickname'];?>
        <meta http-equiv="refresh" content="60 URL=index-x.php"/>
         <?php mysql_close($sqlcnn);
 }
        else
{
```

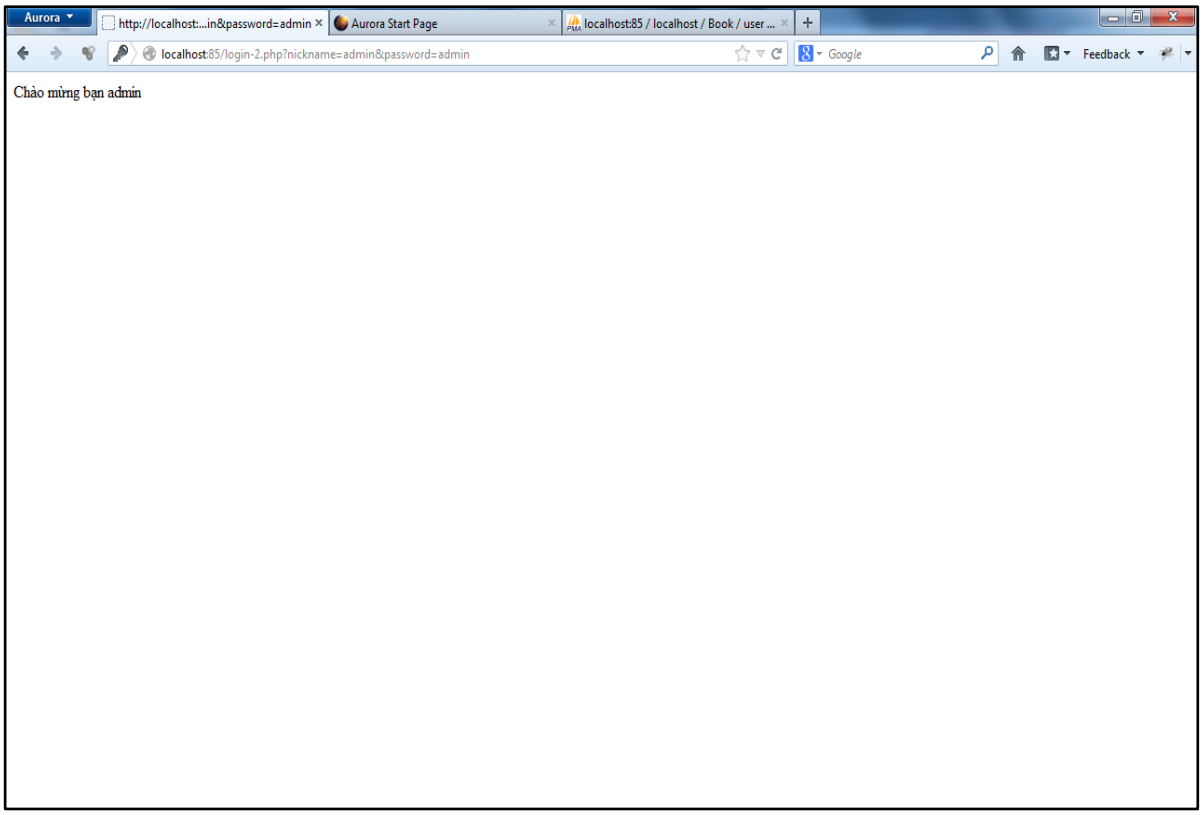
```
        echo "Mời quay lại trang trước";?>
        <meta http-equiv="refresh" content="3 URL=login-1.php"/>
<?php }

  ?>
```

Trong bảng user của CSDL Book, ta đã có một user với nickname là admin, password là admin thì việc xác thực là đúng :



Hình 3.2: Đăng nhập với tài khoản admin



Hình 3.3: Đăng nhập với tài khoản admin thành công

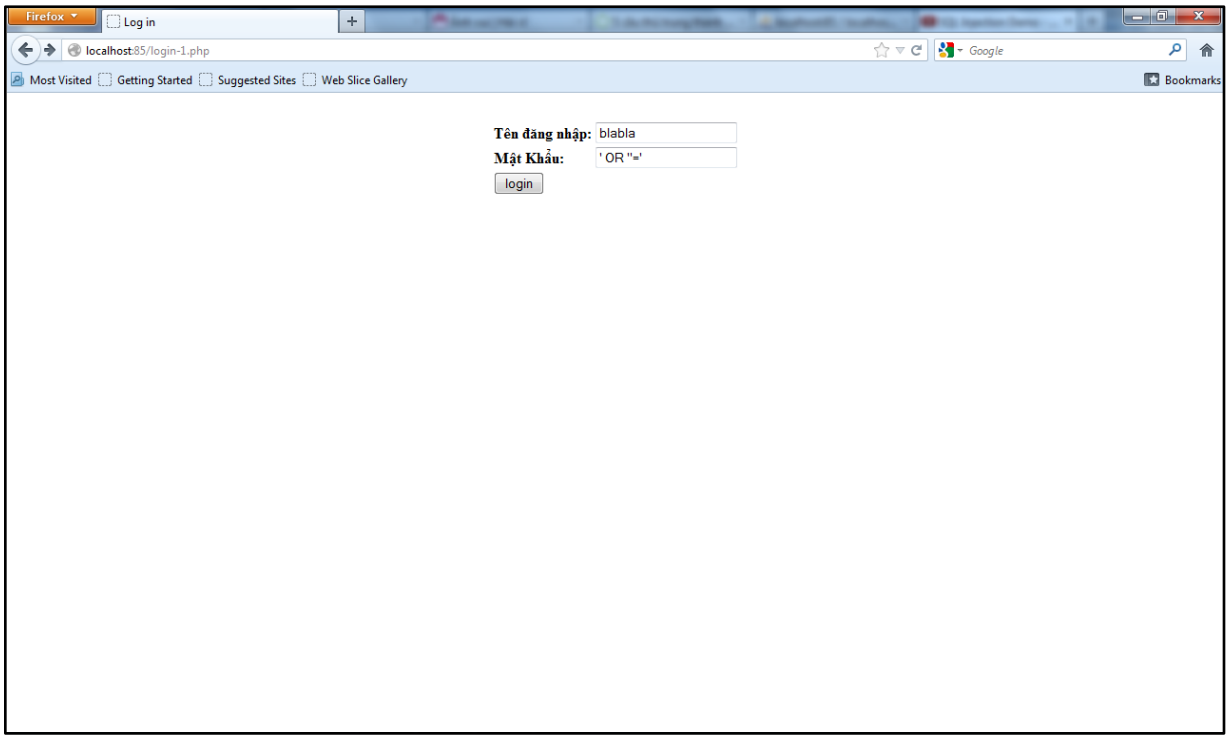
Lúc ấy chuỗi câu lệnh SQL đúng sẽ là :

sql= select * from user where nickname= 'admin' and password= 'admin'

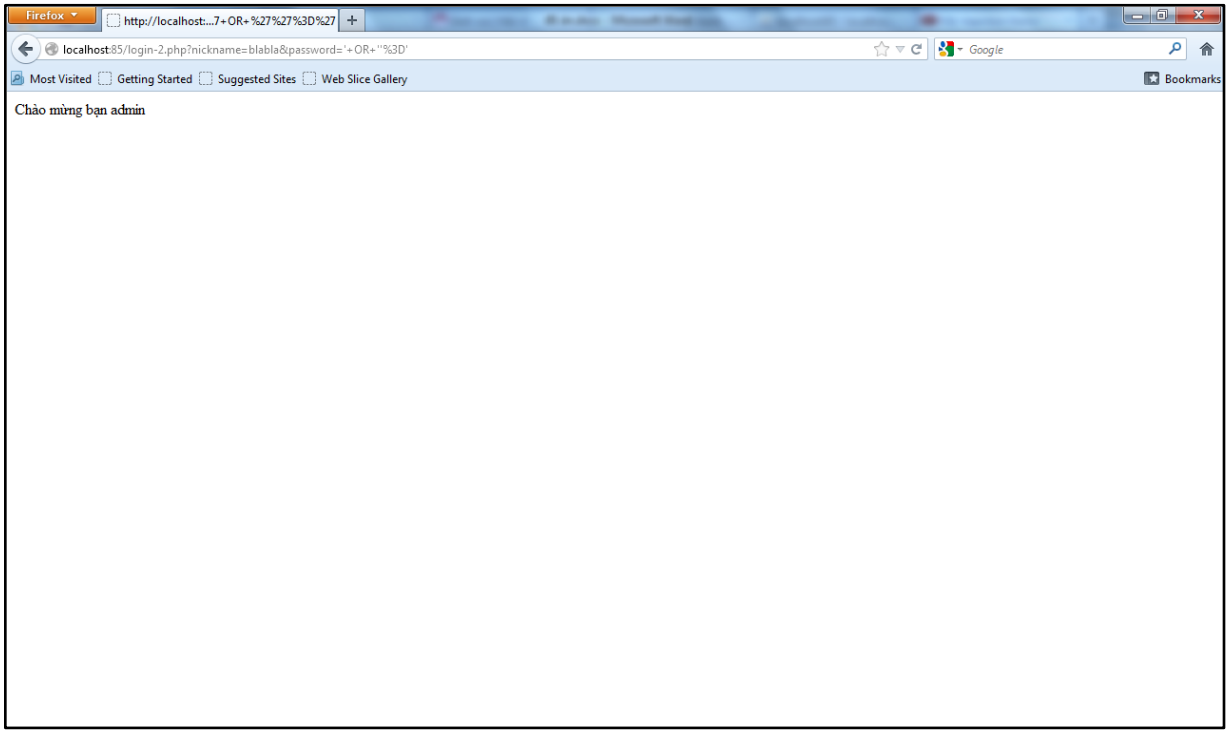
Chuỗi này khi được chạy sẽ trả về giá trị nickname = admin.

Thế nhưng khi ta nhập vào chuỗi sau trong phần password, giá trị vẫn trả về đúng , và ta vẫn có thể đăng nhập thành công mà thực sự không có username nào như thế cả.

Ví dụ : nhập chuỗi **' OR ''='**

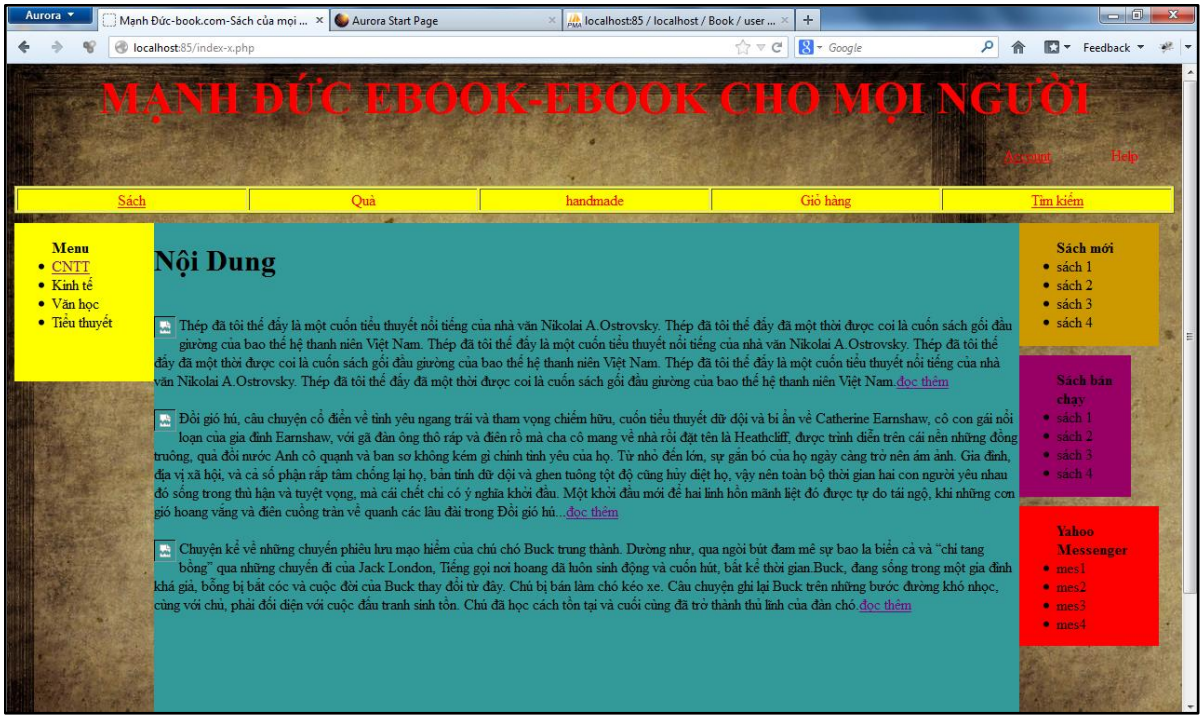


Hình 3.4: Đăng nhập sử dụng SQL Injection



Hình 3.5: Đăng nhập thành công

Đăng nhập bằng chuỗi này vẫn trả về kết quả đúng , ta vẫn có thể tiếp tục duyệt trang tiếp theo:



Hình 3.6: Trang sau khi đăng nhập thành công

Có được điều này là do lúc đăng nhập chuỗi **' OR ''='** , câu lệnh SQL lúc này là:

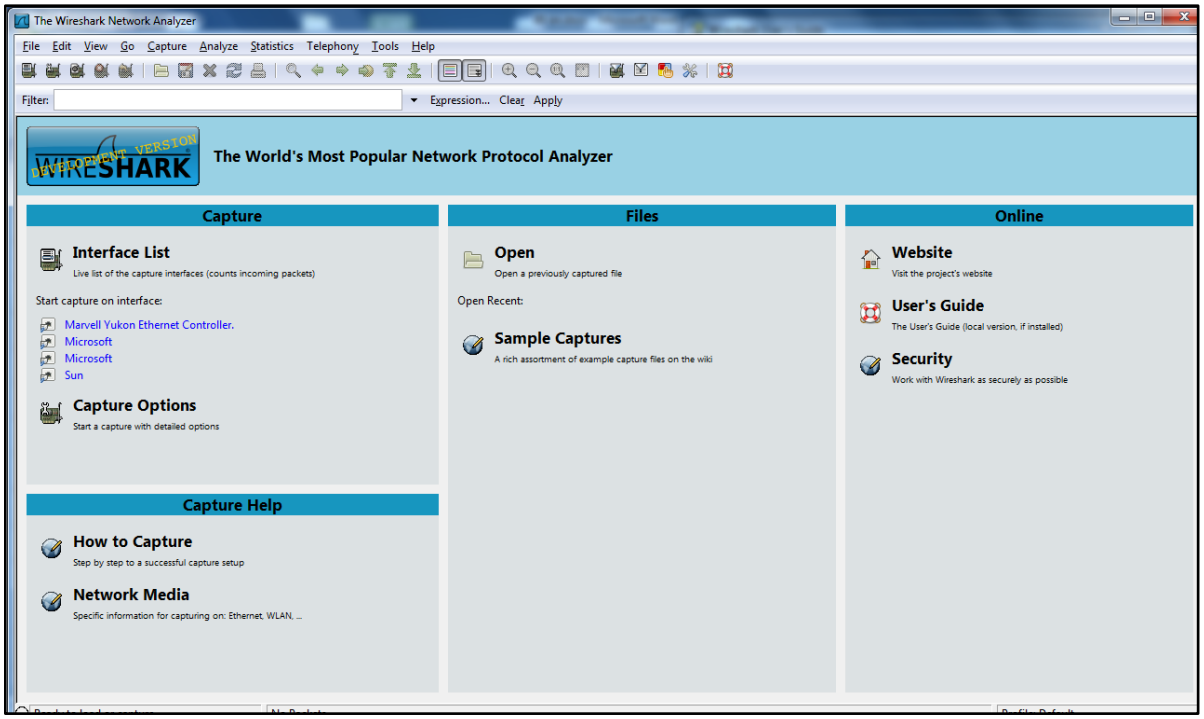
sql= select nickname from user where nickname= 'blabla' and password='' OR ''=''

Câu lệnh sql luôn trả về giá trị đúng, tức là trả về toàn bộ hàng của bảng. Như vậy là không cần nhớ password hay username, ta vẫn có thể truy nhập được vào trang khác nhờ lỗ hổng trong câu lệnh SQL hay cách khác là SQL Injection.

3.2. SỬ DỤNG PHẦN MỀM NGHE LÉN (SNIFFING) WIRESHARK

3.2.1 Phần mềm WireShark

WireShark là một phần mềm phân tích các gói tin trên mạng. Phần mềm này sẽ cố gắng bắt các gói tin trên mạng và phân tích nó chi tiết nhất có thể (Nguồn: Wireshark User's Guide)



Hình 3.7: Giao diện WireShark

3.2.2 Yêu cầu hệ thống

Yêu cầu phần cứng:

- Bộ vi xử lý 32-bit, 64-bit
- 128 MB RAM
- 75 MB còn trống trong ổ đĩa
-Cạc mạng hỗ trợ : Ethernet, WLAN.

Yêu cầu phần mềm:

- Window 2000, XP, Server 2003, Vista, Server 2008

3.2.3. Hướng dẫn sử dụng WireShark

Chọn Capture -> Interface -> chọn interface mà bạn muốn theo dõi hoặc chọn interface hiển thị ngay trên Interface List.

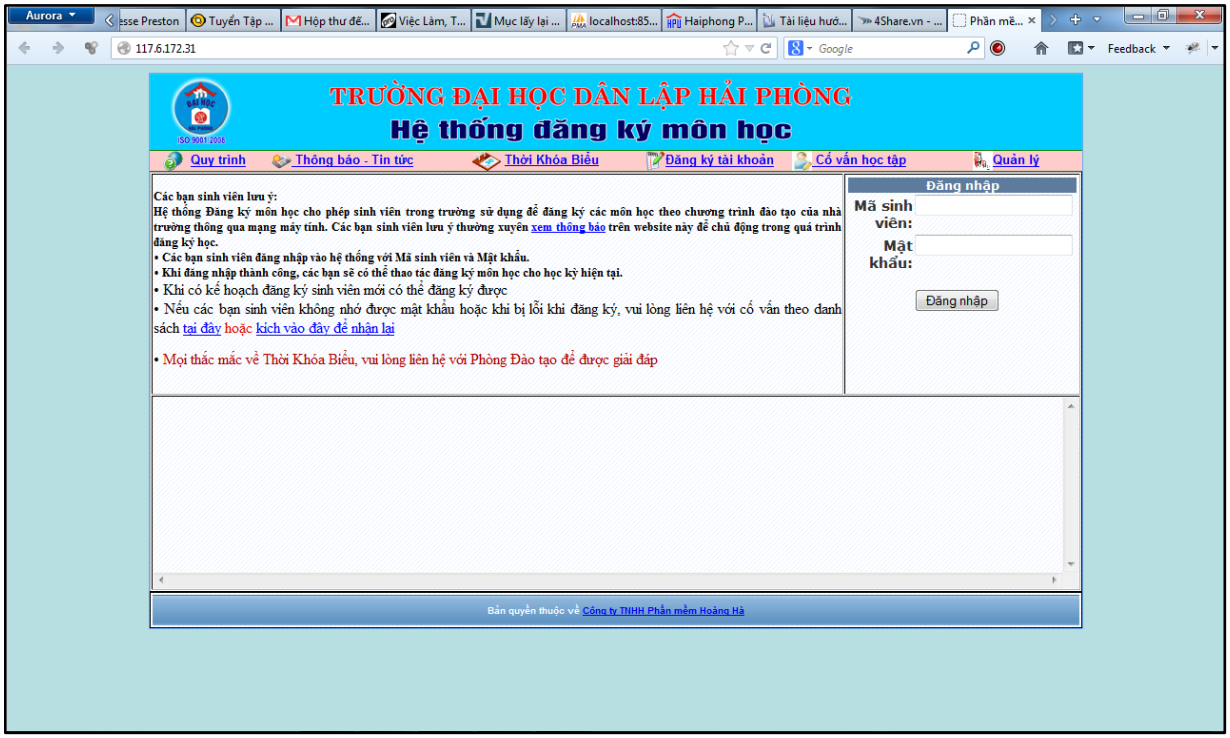
Capture Option : tùy chọn trên Capture, bạn có thể tùy chọn loại giao thức, cổng bao nhiêu để wireshark bắt trên mạng.

Chú ý quan trọng là thanh lọc (Filter) , cho phép ta có thể lọc gói tin lại theo giao thức (TCP, HTTP, UDP), các cổng,…

3.2.4 Ví dụ sử dụng WireShark

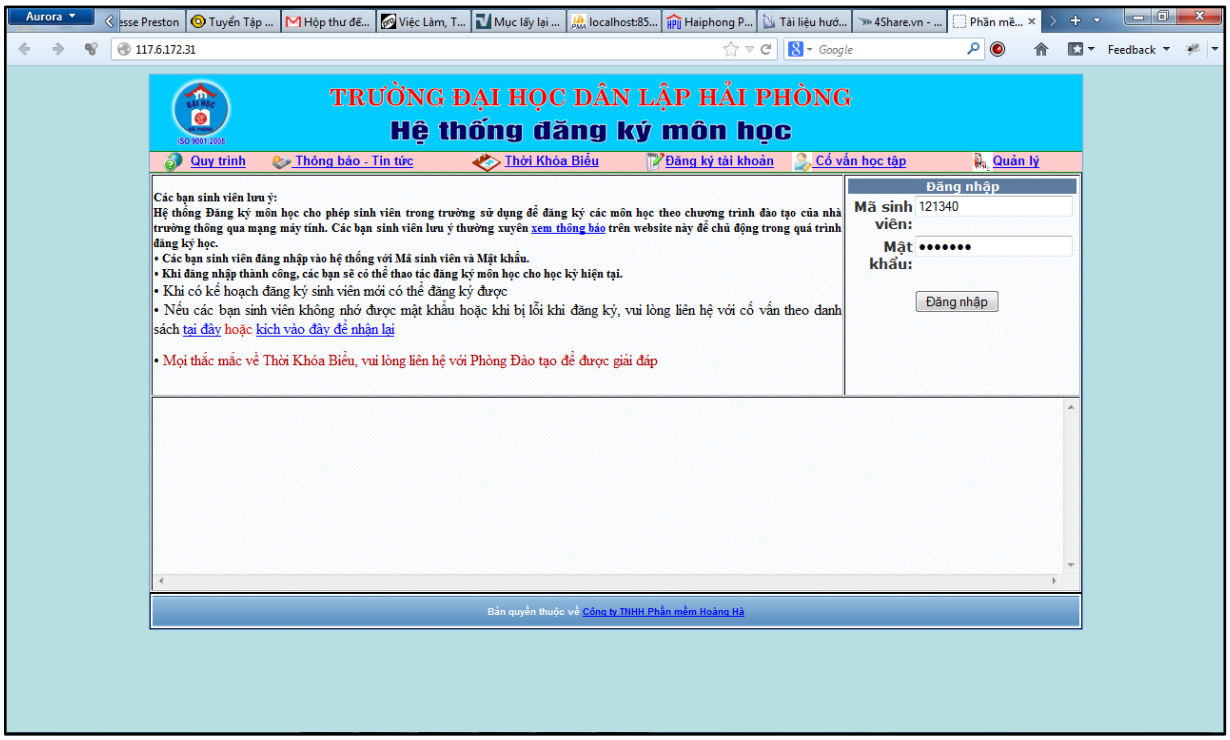
Mục tiêu: dk2.hpu.edu.vn (117.6.172.31)

Mục đích : biết được ID và mật khẩu của người dùng đăng nhập vào địa chỉ 117.6.172.31.

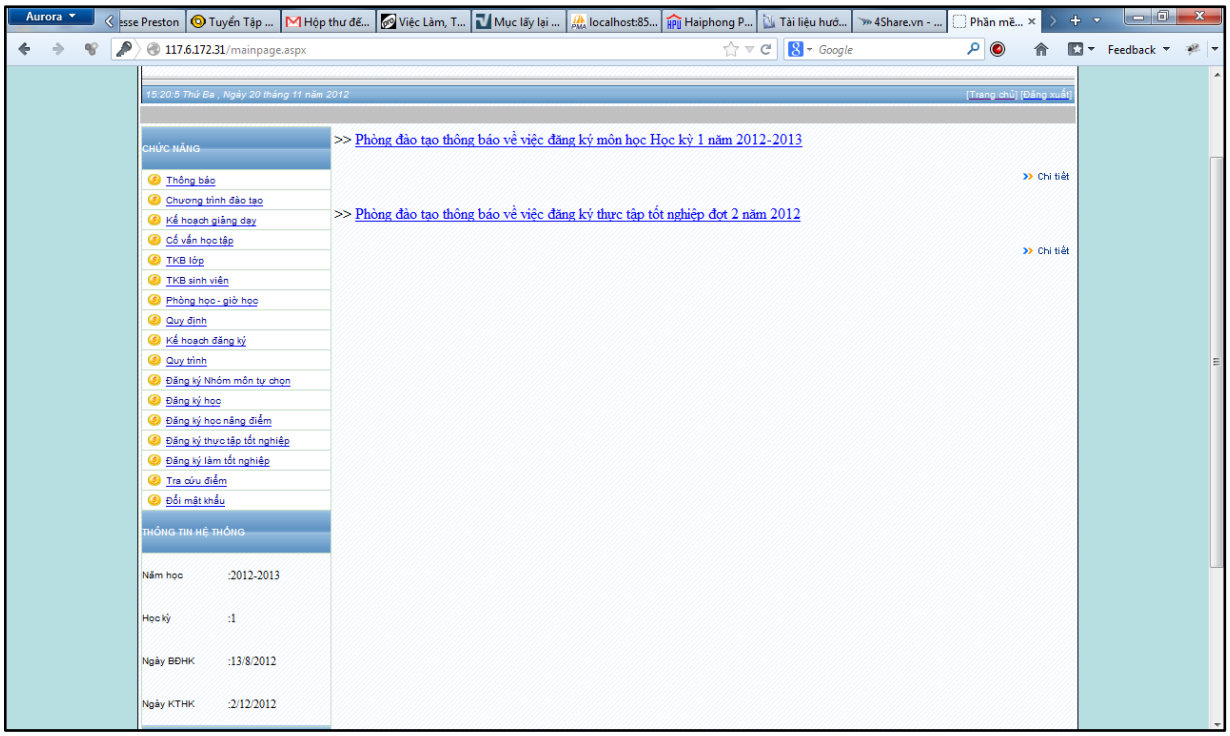


Hình 3.8: Giao diện đăng nhập

Tài khoản được đăng nhập : ID 121340

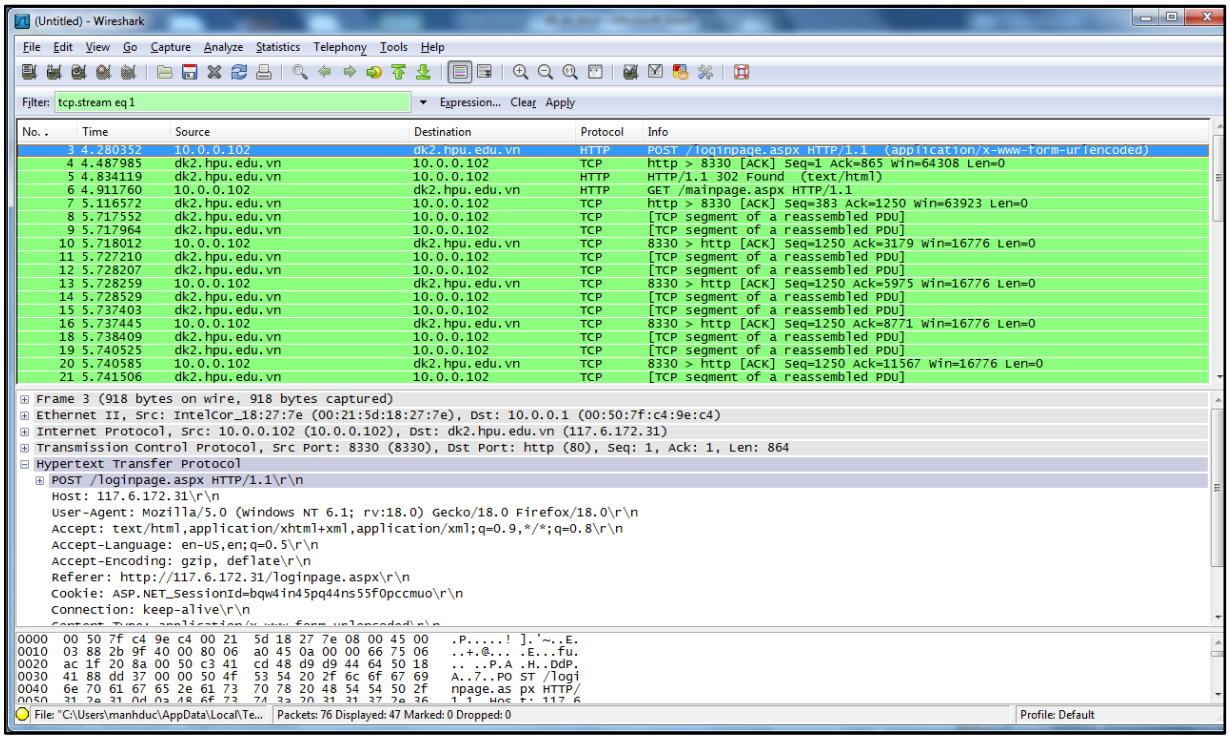


Hình 3.9: Đăng nhập với tài khoản 121340

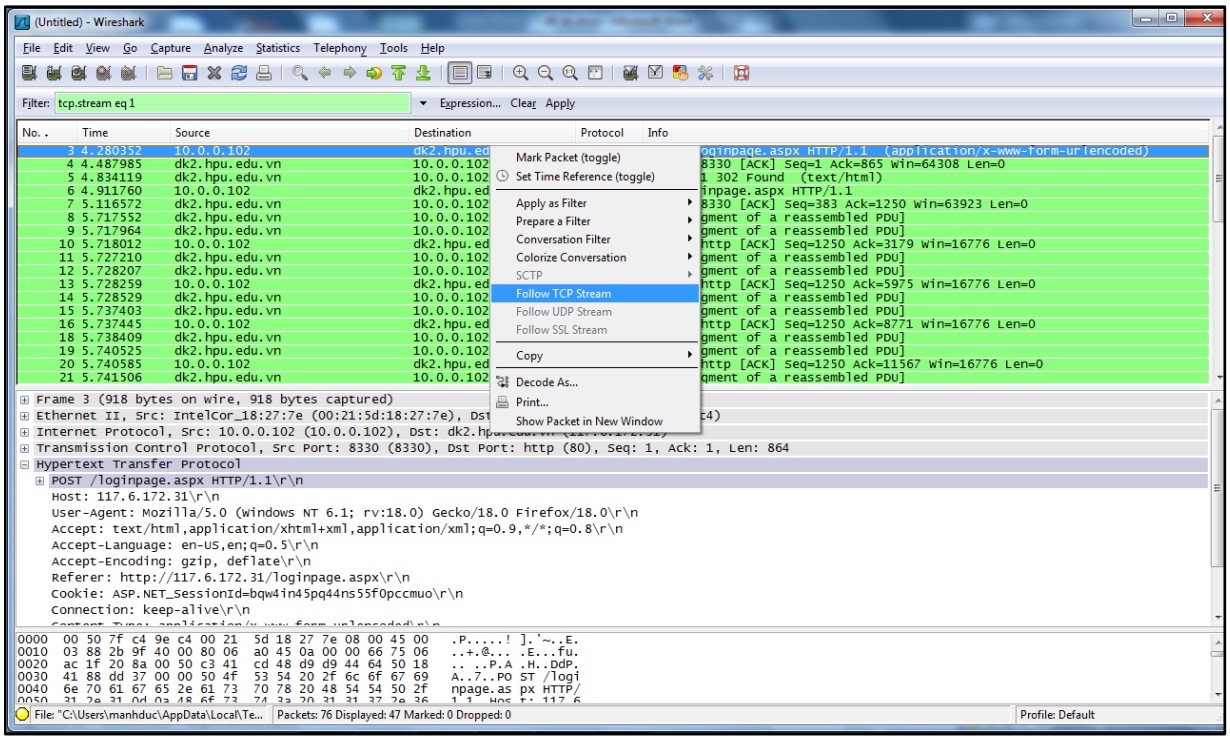


Hình 3.10: Đăng nhập thành công

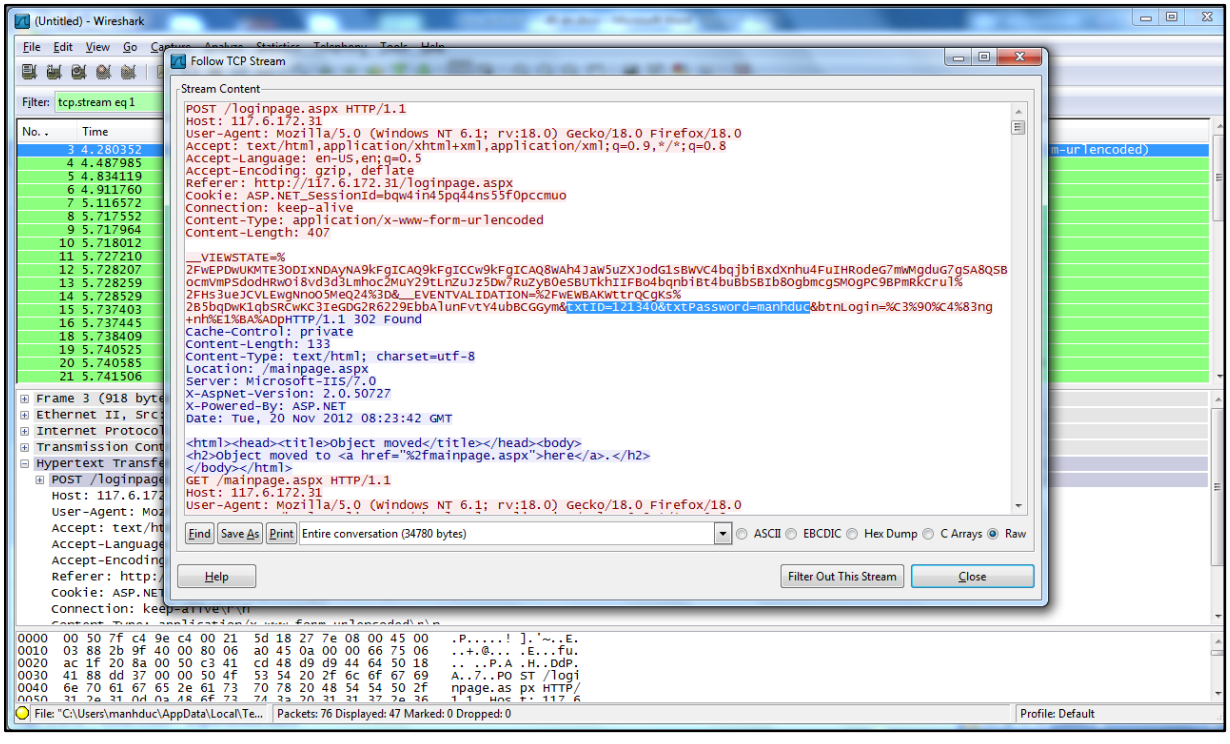
Trên giao diện thể hiện các gói tin của WireShark ta chú ý gói sau:



Hình 3.11



Hình 3.12



Hình 3.13

Như vậy, ta đã biết được mật khẩu của tài khoản 121340 là manhduc.

3.3 CHƯƠNG TRÌNH KIỂM SOÁT ĐĂNG NHẬP CỦA NGƯỜI DÙNG TRÊN WEB

3.3.1 Yêu cầu hệ thống

Yêu cầu phần cứng:

-128 MB RAM

-320 MB free fixed disk

-Chạy Windows 200, XP (Server 2003), Vista (Server 2008), 7

-Tất cả hệ thống 32 bit (hệ thống 64 bit cũng làm việc tốt)

Yêu cầu phần mềm:

-Apache 2.2.14

-MySQL 5.2.41

-PHP 5.3.1

3.3.2 Kỹ thuật Brute Force

Về cơ bản Brute Force (kỹ thuật cưỡng chế, thô bạo) là một thuật toán vét cạn, cho phép đoán mật khẩu của người dùng bằng cách nhập từng chuỗi kí tự trong một bộ từ điển sẵn có theo từng loại thuật toán Brute Force. Dưới đây là một thuật toán Brute Force đơn giản:

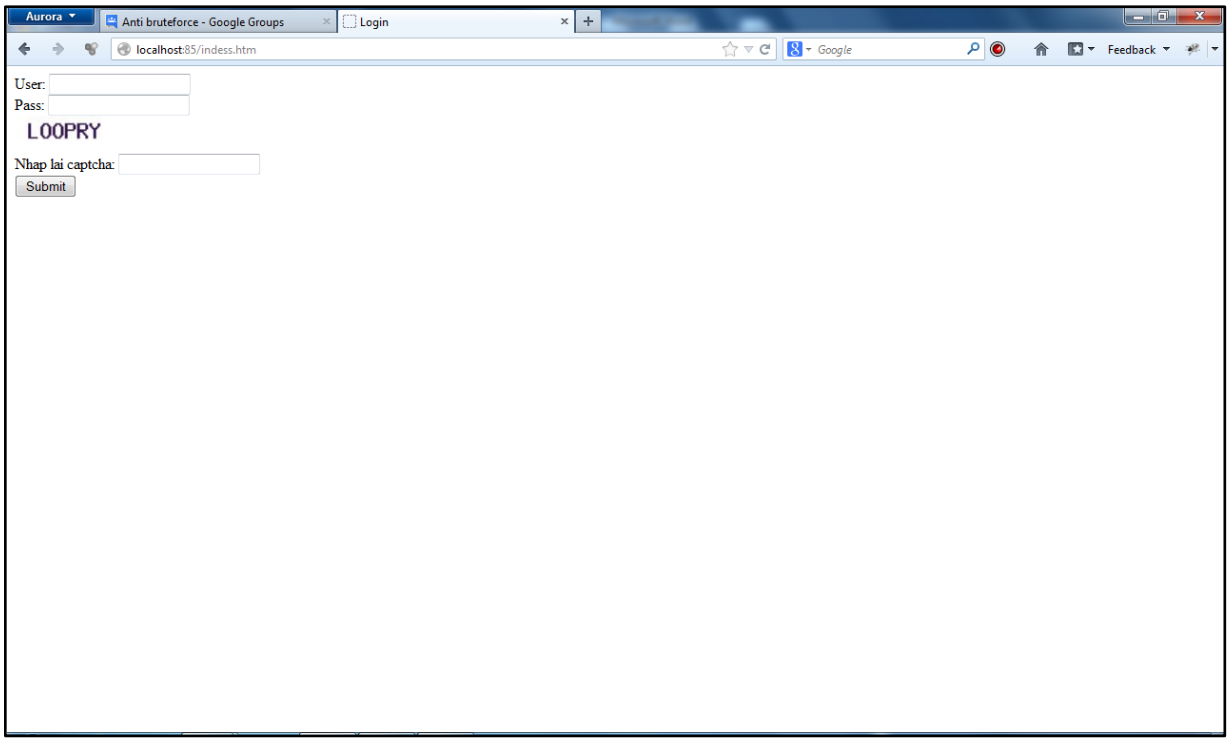
```
        char *Brute_Force(char *source, char *substr, int *k)
{
int i = 0, j = 0, m, n;
n = strlen(source) - 1;
m = strlen(substr) - 1;
do{
if (source == substr[j])
{
i++;
j++;
}
else
{
i = i - j + 2;
j = 0;
}
} while (j <= m && i <= n);
if (j > m)
{
*k = i - m - 1;
return source + i - m - 1;
}
else
return NULL;
}
```

3.3.3 Các kỹ thuật chống Brute Force

Có nhiều kỹ thuật chống Brute Force như sử dụng captcha, mã hóa MD5 đủ khó, các thuật toán kiểm tra đăng nhập người dùng,….

Mỗi kỹ thuật đều có điểm mạnh và điểm yếu riêng. Ở đây tôi xin giới thiệu kỹ thuật chống Brute Force bằng cách sử dụng Captcha.

Điều quan trọng trong sử dụng captcha chống Brute Force là luôn luôn phải kiểm tra xác thực captcha trước khi kiểm tra tài khoản hay mật khẩu, mục đích của nó là nhằm tránh những vụ brute force bằng script.



Hình 3.14: Trang login chứa captch

Các hàm chính của chương trình:

1/. Hàm tạo kí tự captcha:

```
function randomId($len = 16){
   $id = '';
   for($i = 0; $i < $len; $i++){
      $char = rand(65, 90);
      $id .= chr($char);
   }
   return $id;
}
```

2/. Tạo ảnh captcha cho chuỗi kí tự

```
$width=70;
$height=25;
$font=6;
$string = randomId(6);
// ghi nho ki tu duoc ta ra bang session
$_SESSION['captcha'] = $string;
$fontwidth = ImageFontWidth($font) * strlen($string);
$fontheight = ImageFontHeight($font);
$im = @imagecreate ($width,$height);
$background_color = imagecolorallocate ($im, 255, 255, 255);
$text_color = imagecolorallocate ($im, rand(0,100), rand(0,100), rand(0,100));
// Random color Text
imagestring ($im, $font, rand(3, $width-$fontwidth-3), rand(2,$height-
$fontheight-3),  $string, $text_color);
header ("Content-type: image/jpeg");
imagejpeg ($im,'',90);
```

KẾT LUẬN

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

1/. Tìm hiểu và nghiên cứu lý thuyết

-Tìm hiểu về an toàn thông tin

-Tìm hiểu các dạng tấn công hệ thống thông tin

-Tìm hiểu một số phương pháp phòng chống

2/. Thử nghiệm chương trình

-Trình bày một số kỹ thuật tấn công thông dụng

-Một kỹ thuật phòng chống đánh cắp mật khẩu

Hải Phòng, ngày 19 tháng 11 năm 2012

Sinh viên thực hiện

NGUYỄN MẠNH ĐỨC

TÀI LIỆU THAM KHẢO

1.Giáo trình An toàn và bảo mật thông tin, Tác giả PGS.TS Trịnh Nhật Tiến

2.Luận văn tốt nghiệp, Trần Thị Thủy, Giáo viên hướng dẫn PGS.TS Trịnh Nhật Tiến

3.Luận văn tốt nghiệp, Ngô Hồng Trang, Giáo viên hướng dẫn PGS.TS Trịnh Nhật Tiến

Tài liệu tham khảo qua các trang web:

www.hvaonline.net

……