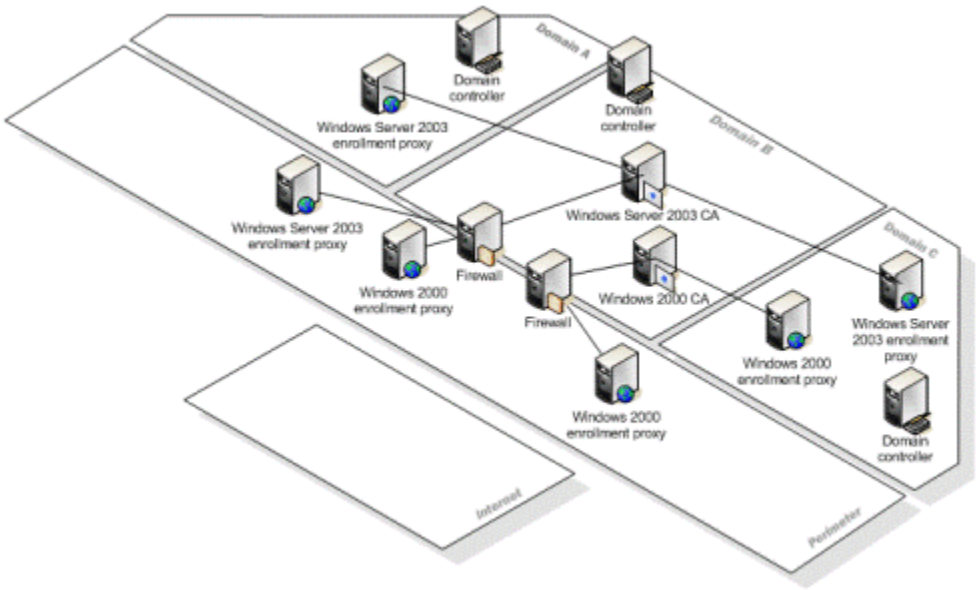
Mạng ngang hàng có thể tăng năng suất sử dụng máy tính bởi nó được thiết kế đơn giản trong việc chia sẻ thông tin và tài nguyên trên mạng của bạn. Tuy nhiên, khả năng của các máy tính người sử dụng truy cập vào máy tính của họ có thể bị đánh cắp thông tin, xóa bỏ dữ liệu hoặc thiếu thận trọng trong việc chia sẻ thông tin. Đó là nguyên nhân tại sao mà bạn cần thêm vào các chính sách, quy định sử dụng máy tính trong công ty, bạn có thể chắc chắn rằng bạn và nhân viên công ty hiểu được các kiến thức cơ bản về bảo mật mạng ngang hàng.

Nội dung các phần:

1. Giới thiệu
2. Bảo mật hệ thống tập tin
3. Bảo mật tài khoản
4. Sử dụng tường lửa
5. Cập nhật các bản vá lỗi bảo mật
6. Kiểm tra tính bảo mật với công cụ phân tích MSBA
7. Các tài liệu tham khảo

Phần 1: Giới thiệu tổng quan

Ở đây chúng tôi muốn cung cấp cho bạn các kiến thức cơ bản bảo mật tốt nhất bao gồm:



- Cập nhật các bản vá lỗi bảo mật của Windows mới nhất

- Sử dụng các phần mềm diệt Virus
- Sử dụng kết nối tường lửa khi truy cập Internet
- Sử dụng mật khẩu an toàn
- Không chia sẻ file hoặc thư mục với các máy chủ trên Internet
- Giới hạn quyền trên các thư mục được chia sẻ

- Hạn chế thấp nhất các thư mục được chia sẻ

- Ngắt các chia sẻ khi không có nhu cầu

Ngày nay với sự gia tăng của các đoạn mã nguy hiểm như các sâu, virus, hacker chúng có thể làm tê liệt, phá hủy dữ liệu, đánh cắp thông tin trên máy của người dùng. Tài liệu này với mục đích đưa ra các giải pháp bảo mật cho các doanh nghiệp vừa và nhỏ khi sử dụng mạng ngang hàng. Trợ giúp các máy tính của bạn sử dụng hệ điều hành Microsoft Windows 2000 Pro được bảo mật hơn trước các mối đe dọa bảo mật nhằm đảm quá trình làm việc được hiệu quả an toàn trên máy tính

Các vấn đề được hướng dẫn trong tài liệu này bao gồm

• Bảo mật hệ thống tập tin

• Bảo mật tài khoản người dùng

• Bảo mật sự truy cập từ mạng

• Kiểm tra phân tích đánh giá mức độ bảo mật với phần mềm Microsoft Baseline

Thêm vào đó các hướng dẫn nâng cao từng bước trong tài liệu này, bạn sẽ cũng tìm thấy các thông tin về các giới thiệu bảo mật hàng đầu

mà Microsoft đang làm cho toàn bộ khách hàng, từ những người dùng gia đình cho đến các doanh nghiệp

Chú ý quan trọng:

Toàn bộ các hướng dẫn từng bước trong tài liệu này được phát triển theo dạng mặc định khi bạn cài đặt hệ điều hành. Nếu bạn có thay đổi thanh Start menu, các bước hướng dẫn có thể sẽ không còn đúng

Yêu cầu cập nhật các bản Service Pack

Tài liệu này sử dụng tốt nhất cho các hệ điều hành Windows 2000 Professional Service Pack 4. Nếu bạn chưa cài đặt hoặc bạn không biết địa chỉ cài đặt bạn có thể truy cập vào địa chỉ Windows Update của trang web Microsoft tại địa chỉ: http://go.microsoft.com/fwlink/?LinkID=22630, và tại đó bạn có thể quét các bản cập nhật trên máy bạn. Nếu Service Pack 4 được hiển thị trên danh sách các bản vá lỗi, bạn hãy cài đặt nó trước

Các yêu cầu quản trị

Bạn phải đăng nhập với tài khoản truy cập cao nhất là Administrator hoặc với tài khoản là thành viên của nhóm quản trị để có thể hoàn thành các hướng dẫn này. Nếu máy tính của bạn kết nối tới Internet, các chính sách thiết lập mạng cũng có thể ngăn cản sự hoàn thành của các hướng dẫn này

Bảo mật hệ thống File

Một hệ thống quản lý tập tin là các phương thức mà các file hoặc thư mục được tổ chức trên máy tính của bạn. Có một số phương pháp bảo vệ hệ thống tập tin từ các truy cập trái phép nhằm mục đích thay đổi hoặc xóa bỏ dữ liệu. Trong mục này tôi muốn giới thiệu với các bạn từng bước để bảo vệ hệ thống tập tin như sau:

• Chuyển đổi hệ thống quản lý tập tin thành NTFS

• Sử dụng các phần mềm diệt Virus

• Bảo vệ các file được chia sẻ

• Bảo vệ các thư mục được chia sẻ

• Ngắt hoặc xoá các account không cần thiết

• Chuyển đổi hệ thống quản lý tập tin thành NTFS

Trong khi cài đặt Windows 2000, các máy tính được cấu hình để sử dụng hệ thống quản lý tập tinFAT32 hoặc NTFS. FAT32 là công nghệ cũ được sử dụng trong các phiên bản Windows trước đây như Windows 98, Me. Hệ thống quản lý tập tin NTFS nhanh hơn và bảo mật hơn FAT32. Giải pháp tối ưu nhất về thực thi và bảo mật hệ điều hành là sử dụng NTFS cho việc quản lý tập tin trong máy tính của bạn.

Kiểm tra hệ thống quản lý tập tin trên máy tính của bạn.

Trước khi chuyển đổi hệ thống quản lý tập tin trên máy tính của bạn, bạn cần phải xác nhận là máy tính của bạn chưa được chuyển đổi thành NTFS. Bạn hãy theo các hướng dẫn sau để kiểm tra. Nếu các bước kiểm tra xác nhận là bạn đang sử dụng NTFS thì bạn không cần chuyển đổi hệ thống quản lý tập tin

• Kiểm tra hệ thống quản lý tập tin hiện tại trên máy tính bạn:

1. Trên màn hình Desktop, bạn kiách đúp chuột phải vào My Computer
2. Kích chuột phải vào ổ cứng mà bạn cần kiểm tra, sau đó chọn Properties
3. Xác nhận đó là hệ thống quản lý tập tin NTFS. Nếu không phải, bạn có thể sử dụng tiện ích chuyển đổi (convert.exe) được hướng dẫn bên dưới để chuyển dổi FAT16 hoặc FAT32 thành NTFS

Kiểm tra toàn bộ các ổ đĩa còn lại trên máy tính của bạn. Trong trường hợp nếu toàn bộ các ổ cứng hiện thời trên máy bạn là FAT32 bạn cũng có thể dễ dàng chuyển đổi thành NTFS theo các hướng dẫn bên dưới

Chuyển đổi hệ thống quản lý tập tin thành NTFS

Để chuyển đổi hệ thống quản lý tập tin thành NTFS, bạn phải chú ý tên của ổ đĩa mà bạn đã đặt và làm theo các bước chỉ dẫn dưới đây

• Chuyển đổi hệ thống quản lý tập tin thành NTFS

1. Từ menu Start bạn kích vào Run gõ câu lệnh cmd sau đó nhấn OK

2. Sau khi cửa sổ MS-Prompt DOS hiện ra bạn gõ câu lệnh sau:
"Convert Tên_Ổ_Đĩa: /fs:ntfs"
Sau đó bạn phải nhập Volume ổ đĩa . Giả sử bạn cần Convert ổ D với tên ổ đĩa là KIEMTRA bạn làm như sau:

Convert D: /fs:ntfs

Sau đó màn hình sẽ nhắc bạn nhập tên ổ đĩa vào và bạn gõ KIEMTRA

3. Tiếp theo bạn nhập tên ổ đĩa và nhấn ENTER

4. Khi việc chuyển đổi hoàn thành, bạn đóng cửa sổ bằng câu lệnh EXIT

CHÚ Ý: Chú ý quan trọng khi bạn đang chạy các chương trình của hệ điều hành thì đương nhiên hệ điều hành sẽ không chuyển đổi ngay cho bạn tại thời điểm đó. Tuy nhiên hệ điều hành sẽ nhắc bạn rằng việc chuyển đổi này sẽ được thực hiện sau khi bạn khởi động lại máy. Và bạn phải gõ Y để đồng ý

Sử dụng các phần mềm diệt Virus

Virus máy tính là các chương trình được cài đặt hoặc lây nhiễm vào máy tính ngoài sự cho phép của bạn. Ngày nay các virus ngày càng nguy hiểm với khả năng tự sao chép và lây nhiễm qua Internet và email trên toàn thế giới với tốc độ rất nhanh trong vài giờ
Phần mềm diệt sẽ giúp bạn bảo vệ máy tính của mình với nhiều loại virus, sâu, trojan và các đoạn mã nguy hiểm. Bằng cách này bạn có thể quét và diệt virus. Tuy nhiên các phần mềm diệt virus chỉ giải quyết được một phần vấn đề .

Nhiều máy tính mới được mua với các phần mềm diệt virus đã được cài đặt sẵn trên máy tính. Tuy nhiên, phần mềm diệt virus này yêu cầu bạn phải đăng ký để có thể cập nhật các Virus mới nhất. Nếu bạn không đăng ký cập nhật, máy tính của bạn sẽ bị nguy hiểm trước các virus mới

Bạn hãy sử dụng email an toàn bằng cách không mở các file đính kèm, không kích vào các liên kết trên trên email (Tốt nhất hãy copy và paste vào trình duyệt để truy cập web). Nếu bạn cài phần mềm diệt virus thì các chương trình này sẽ quét các file có đính kèm

Để biết được các chương trình diệt virus và các nhà cung cấp phần mềm diệt virus tốt nhất với HĐH Windows mời bạn tham khảo tại địa chỉ http://go.microsoft.com/fwlink/?LinkId=22712

Bảo vệ các file được chia sẻ

Trong bài trước tôi đã đưa các khái niệm, chuyển đổi hệ thống tập tin NTFS. Phần này sẽ tiếp tục hướng dẫn bạn cách bảo vệ các tập tin, thư mục được chia sẻ trong mạng LAN. Mạng ngang hàng cho phép bạn tạo các chia sẻ dữ liệu do đó người dùng có thể giới hạn truy cập chỉ đọc hoặc có thể vừa đọc, thay đổi, xóa file. Nếu bạn kết nối với Internet, và không sử dụng tường lửa, bạn hãy nhớ rằng bất kỳ một file nào bạn chia sẻ bạn cũng có thể bị truy cập từ các người dùng khác trên mạng Internet

Theo mặc định, Windows 2000 cho phép toàn quyền điều khiển, thay đổi và đọc với bất kỳ người dùng nào truy cập vào các thư mục được chia sẻ (share). Tuy nhiên bạn hoàn tòan có thể thay đổi bằng cách xóa thuộc tính này trên các thư mục được chia sẻ hoặc thay đổi giới hạn truy cập toàn quyền bằng các truy cập chỉ có đọc. Hoặc bạn có thể thêm các tài khoản truy cập theo đúng người cần chia sẻ. Việc xóa bỏ quyền Everyone trong Windows bạn sẽ được đảm bảo rằng không có ai có thể truy cập vào các thư mục cần bảo vệ trừ khi bạn thêm một người dùng mới vào tài khoản truy cập.

Hoặc bạn muốn bảo vệ các chia sẻ ẩn trước người dùng bạn có thể thêm dấu "$" vào sau các thư mục chia sẻ. Ví dụ bạn muốn chia sẻ một thư mục "**Du lieu**" bạn có thê thêm "**Du lieu$"** vào sau thư mục này khi đó nếu bạn muốn truy cập vào thư mục chia sẻ này thì bạn chỉ việc gõ tên máyà Tên chia sẻ của thư mục+$ ví dụ: Computerdata$ khi đó bạn đã có thể truy cập được vào thư mục ẩn này rồi. Tuy nhiên cách này chưa thực sự an toàn với một người dùng có hiểu biết về máy tính. Họ chỉ việc xem thư mục chia sẻ này bằng cách vào Start, Run, type **cmd** , Gõ câu lệnh **NET SHARE** nó sẽ liệt kê hết các chia sẻ kể cả chia sẻ ẩn. Vậy thì bạn phải làm gì ? Xin mời bạn tiếp tục đến với phần

Bảo vệ các thư mục chia sẻ

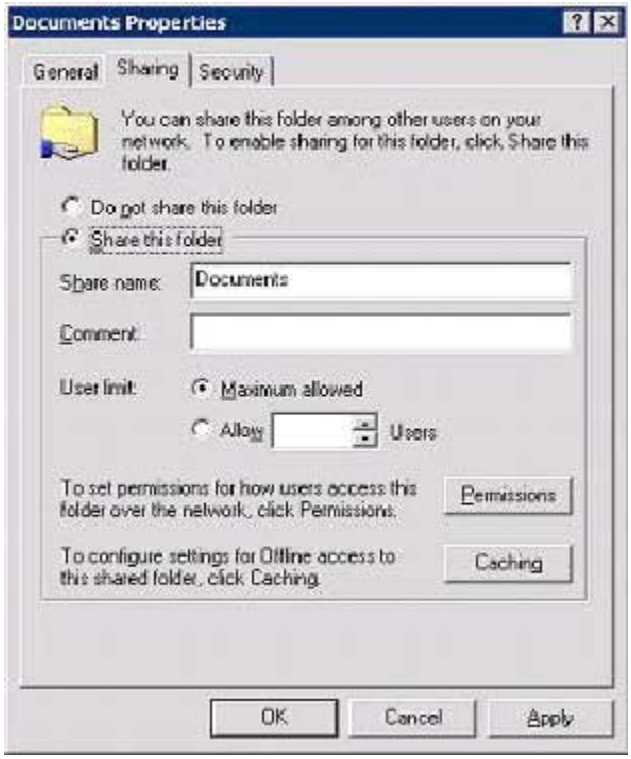
Mạng ngang hàng Windows cho phép bạn chia sẻ các thông tin với máy tính khác trên mạng. Bằng một vài thao tác nhỏ bạn đã có thể chia sẻ được các file và các thư mục. Bằng các thay đổi một vài các thiết lập mặc định, bạn có thể ngăn chặn các truy cập bất hợp pháp tới các file và thưc mục của bạn

Các bước để bảo vệ thư mục chia sẻ

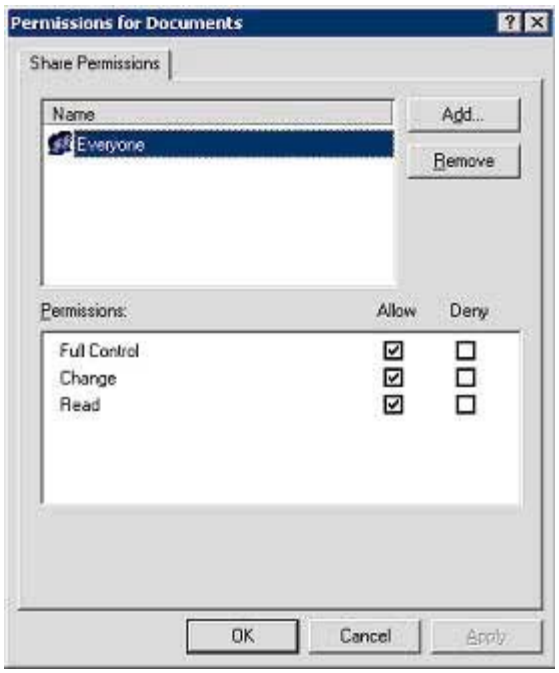
Bước 1: Trên màn hình Desktop, kích đúp vào My Computer, sau đó mở file hoặc thư mục mà bạn muốn bảo vệ

Bước 2: Kích phải chuột vào thư mục bạn muốn bảo về và chọn sharing

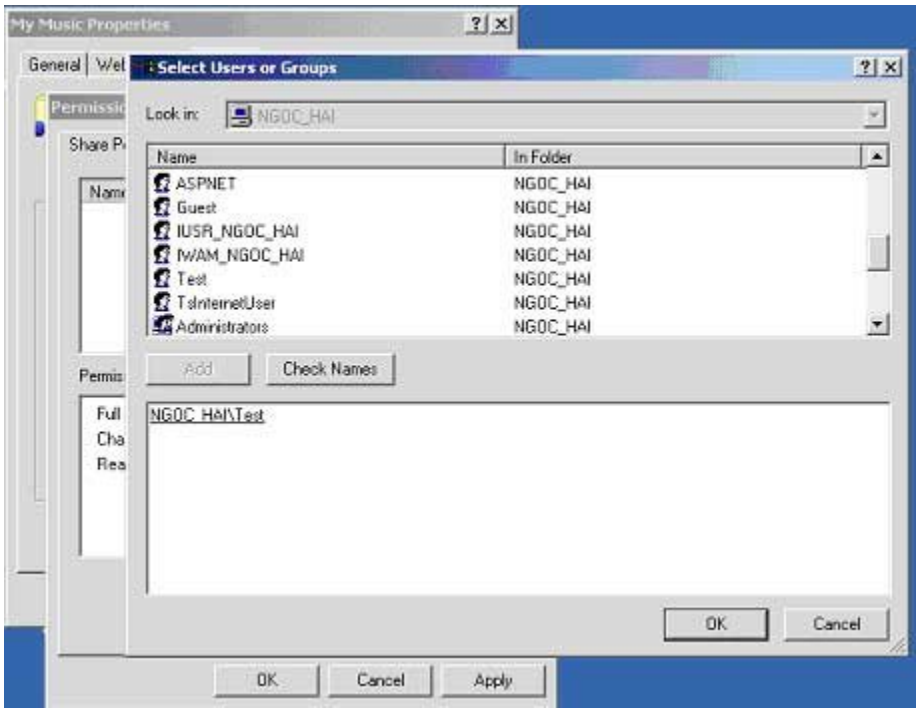
Bước 3: Trên tab Sharing, kích vào Permissions



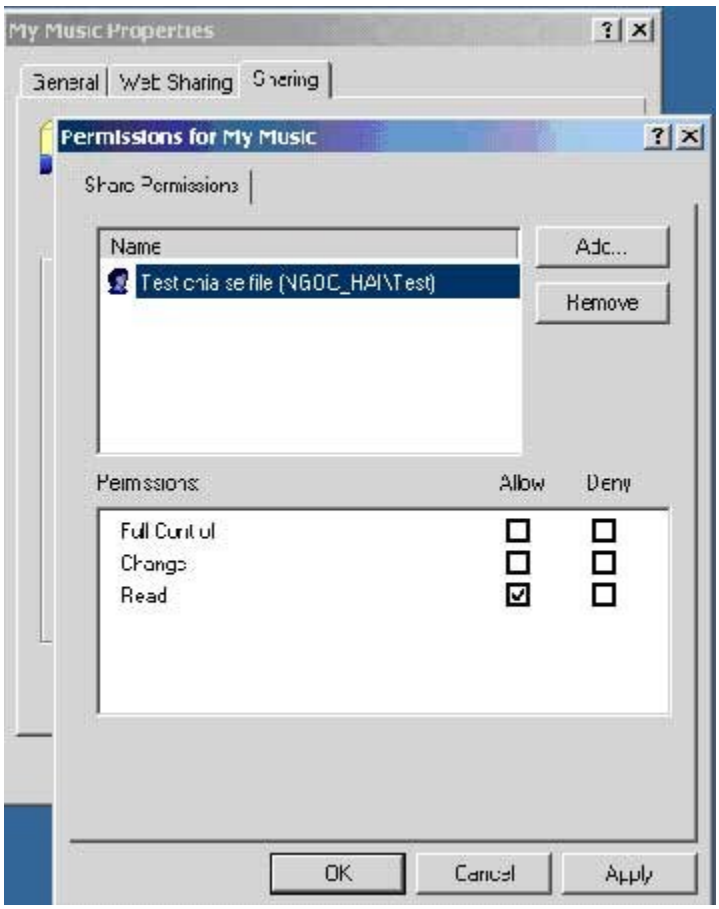
Bước 4: Chọn EveryOne và kích Remove nhằm hạn chế bất kỳ người dùng nào muốn truy cập



Bước 5: Kích vào **Add** sau đó chọn tài khoản truy cập thích hợp mà bạn muốn cho người dùng chia sẻ



Sau đó kích OK



Bạn chú ý nếu thư mục bạn cần chia sẻ mà chỉ cho người dùng Copy thì tốt nhất chỉ đặt quyền truy cập "Read".

Bước 6: Bạn nhấn "Apply"à OK. Công việc chia sẻ bây giờ đã hoàn thành. Bạn có thể yên tâm rằng file của bạn chắc chắn được bảo vệ chỉ có những người được phép truy cập mới có thể truy cập được.

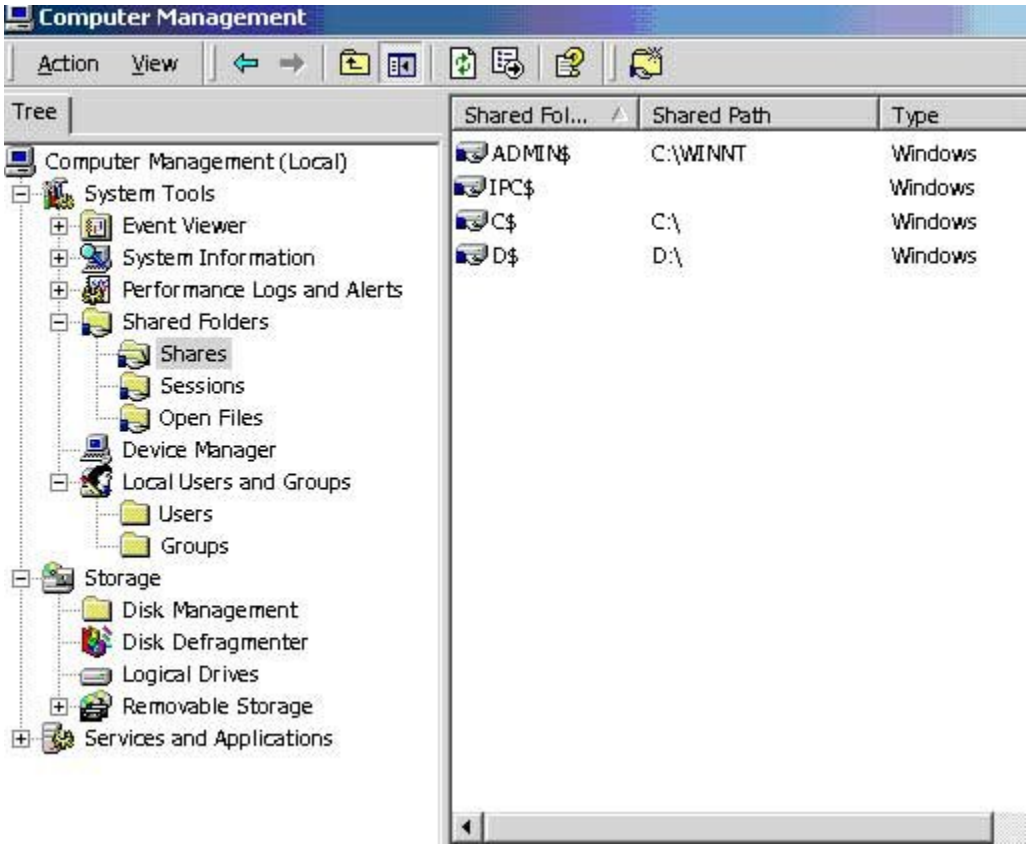
Chú ý:

- Các file hoặc thư mục chia sẻ hoạt động tốt nhất với hệ thống NTFS

- Để thay đổi quyền truy cập, bạn chỉ việc thêm hoặc remove bớt User hoặc thay đổi quyền truy cập thông tin

- Trong các Account và các nhóm người dùng (Groups) nếu bạn đặt Full Control Permissions thì người dùng có thể xóa file, xóa các thư mục con trong thư mục được chia sẻ

Nhân tiện đây tôi muốn cảnh báo với các bạn một điều cực kỳ quan trọng rằng: Theo chế độ mặc định Windows 2000, XP, 2003 đều chia sẻ **tất cả các ổ đĩa cứng** của bạn và các thư mục là: IPC, Admin theo hình thức chia sẻ ẩn (có dấu $) mà ở trên tôi đã nói với bạn (Bạn có thể kiểm tra điều này bằng cách truy cập vào Control Panel à Administrative Tools à Computer management à System Tool à Share Folder.



Các chia sẻ mặc định này mặc dù không truy cập được với tài khỏan khách nhưng nếu bạn vô tình tạo Account truy cập với quyền Administrator cho người sử dụng thì đương nhiên rằng may bạn sẽ bị khai thác hết thông tin. Vậy thì bạn phải làm gì để xóa bỏ các chia sẻ này ? Bạn ngắt các chia sẻ từ Computer Management? Hoàn toàn sai lầm! Vì sau khi khởi động lại máy chúng lại xuất hiện không tin bạn cứ thử mà xem.

Để giải quyết vấn đề này tôi hướng dẫn ban cách xóa các chia sẻ này đơn giản mà cực kỳ hiệu quả. Đầu tiên bạn tạo một File là secure.bat (Từ File trong **My Computer à New à Text document à** bạn đặt tên file là secure.bat. Chú ý rằng nếu phần mở rộng của file không được

hiển thị thì file của bạn vẫn có phần mở rộng là *.txt bạn phải vào **Toolsà Folder Options à View** à Bỏ đánh dấu "**Hide file extentions for known file types**". Tiếp theo bạn kích phải chuột vào file secure.bat vừa tạo chọn Edit và thêm vào các dòng lệnh sau:

net share c$ /delete /y

net share d$ /delete /y

net share IPC$ /delete /y

net share ADMIN$ /delete /y

Sau đó Save lại. Bây giờ bạn thử chạy file này và kiểm tra lại các file share. Kết quả thế nào? Tuyệt vời phải không. Vậy thì bạn hãy copy file này vào mục Startup của Windows để mỗi lần khởi động máy sẽ xóa bỏ các mục chia sẻ mặc định này.

Bảo mật tài khoản người dùng, mật khẩu, thiết lập tường lửa.

Phần này chúng ta tiếp tục học các kỹ năng bao gồm: Vô hiệu hoá tài khoản người dùng không cần thiết, bảo mật các tài khoản, chống truy cập bằng các phần mềm tường lửa, cập nhật các bản vá lỗi hệ điều hành.

Vô hiệu hóa hoặc xóa các tài khoản không cần thiết

Bạn tạo rất nhiều Account nhưng sau một thời gian các Account này không được dùng hoặc có sự thay đổi nhân sự từ phía người dùng hoặc các chương trình cài đặt tự động tạo Account mà bạn không dùng đến. Vậy thì giải pháp tốt nhất là bạn hãy xóa hoặc vô hiệu hóa các Account này nhằm bảo vệ máy tính và thông tin.

Các bước để vô hiệu hóa các tài khỏan người dùng:

1. Từ Start chọn Settings, Control Panel
2. Kích đúp vào **Administrative Tools,** sau đó kích đúp vào **Computer Management**
3. Bạn chọn **Local Users and Groups** và kích vào **Users**
4. Kích phải chuột vào các Account mà bạn cần vô hiệu hóa chọn **Properties**
5. Trên tab **General**, bạn chọn **Account is disabled , Apply, Ok**

Chú ý:

1. Khi tài khoản đã được vô hiệu hóa thì đương nhiên tài khỏan này không thể được sử dụng để đăng nhập và biểu tượng của tài khỏan này sẽ biến thành dấu **X** gạch đỏ

2. Tài khoản **Administrator** không thể vô hiệu hóa được

Xóa tài khoản người dùng:

1. Từ Start chọn Settings , Control Panel

2. Kích đúp vào **Administrative Tools,** sau đó kích đúp vào **Computer Management**

3. Bạn chọn **Local Users and Groups** và kích vào **Users**

4. Kích phải chuột vào các Account mà bạn cần xóa bỏ chọn **Delete**

Chú ý:

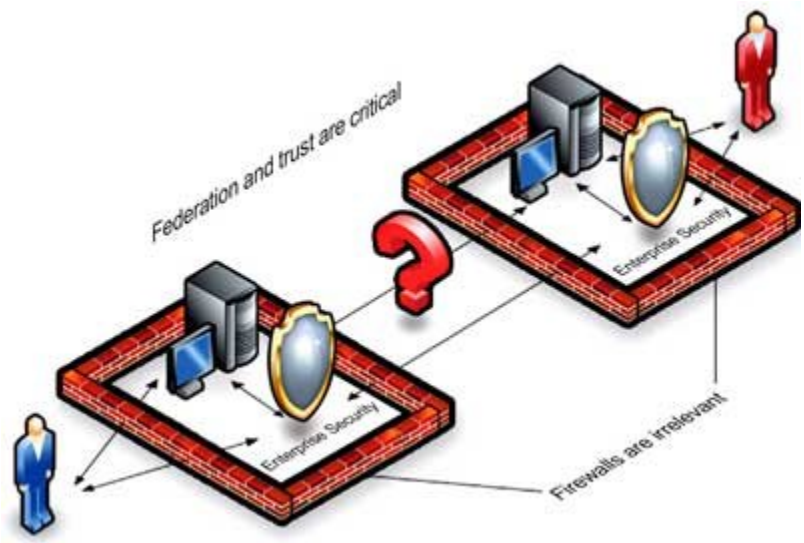
1. Để an toàn bạn hãy vô hiệu hóa các tài khoản trước khi xóa chúng

2. Một tài khoản đã bị xóa sẽ không có khả năng khôi phục

3. Theo mặc định tài khoản **Administrator và Guest** không thể xóa được

Bảo mật các tài khoản người dùng:

Bằng cách sử dụng mật khẩu, vô hiệu hóa hoặc xóa bỏ các tài khoản không cần thiết bạn có thể làm giảm nguy cơ truy cập trái phép vào máy tính của mình



Sử dụng mật khẩu

Một điều cực kỳ quan trọng là phải đặt mật khẩu cho toàn bộ các tài khoản của Windows – với 02 nguyên nhân chủ yếu sau:

Nguyên nhân thứ 1: Nếu bất kỳ một tài khoản nào không đặt mật khẩu thì đương nhiên rằng bất kỳ một người dùng nào cũng có thể truy cập vào máy tính của bạn bằng tài khoản không được đặt mật khẩu

Nguyên nhân thứ 2: Theo mặc định, tất cả các tài khoản không đặt mật khẩu thì người dùng chỉ có thể đăng nhập vào máy tính của bạn trực tiếp khi họ ngồi trên máy bạn mà không thể đăng nhập từ xa hoặc điều khiển máy bạn từ xa. Nhưng sự giới hạn này sẽ không có hiệu lực đối vúoi các tài khoản tên miền hoặc tài khoản Guest. Nếu tài khoản Guest không bị vô hiệu hóa và không đặt mật khẩu, nó sẽ có thể bị sử

dụng để đăng nhập vào bất kỳ một tài nguyên nào trên mạng ngang hàng

Để thiết lập hoặc reset lại mật khẩu tài khoản có sẵn bạn làm như sau:

1. Từ **Start, Settings ,Control panel**

2. Kích phải chuột chọn Set Password . Bạn hãy nhập mật khẩu mới

Sử dụng tường lửa:

Phần mềm tường lửa hoặc phần cứng tường lửa sẽ tạo hàng rào bảo vệ máy tính trước các mối đe dọa tiềm tàng trên Internet. Nếu máy tính bạn sử dụng hệ điều hành Windows 2000 sẽ không có tường lửa được cài đặt trên hệ điều hành (trừ Windows XP, Windows 2003), do đó Microsoft khuyên bạn nên cài đặt tường lửa trước khi truy cập Internet.

Hệ điều hành không có các hướng dẫn sử dụng tường lửa mà bạn phải đọc các tài liệu hướng dẫn từ chính các nhà cung cấp phần mềm hoặc phần cứng

Các phần cứng về tường lửa:

Phần cứng tường lửa là lựa chọn tốt nhất cho hệ điều hành Windows trước khi bạn có ý định sử dụng Windows XP. Một số mạng máy tính như các điểm truy cập không dây và các các bộ định tuyến băng thông rộng được xây dựng sẵn tường lửa. Microsoft Broadband Networking Wireless là một ví dụ cho điểm truy cập không dây được cài đặt sẵn phần cứng tường lửa và các mạng khác trong tương lai.

Phần mềm tường lửa

Một phần mềm tường lửa được xây dựng bởi một vài các đối tác như BlackICE PC Proection, Computer Associates, McAfee Security, Symantec, Tiny Software, và ZoneAlarm.

Để có thể sử dụng các phần mềm hoặc phần cứng Firewall của các công ty này bạn có thể tham khảo tài liệu tại

http://go.microsoft.com/fwlink/?LinkId=22496

http://go.microsoft.com/fwlink/?LinkId=19713.

Cập nhật các bản vá lỗi

Một trong những điều tối quan trọng là "Cập nhật đầy đủ các bản vá lỗi của Windows" trước cơn đại hồng thuỷ: Virus (Blaster,Netsky, Sasser, Lovegate,..), hacker, phần mềm gián điệp. Nếu bạn không tuân thủ quy tắc này máy tính của bạn sẽ bị hạ gục chỉ sau từ 10 phút đến 30 phút. Bạn có tin không? Nếu bạn tin tôi thì hãy tiếp tục đọc và cập nhật Windows còn nếu không tin tốt nhất bạn hãy chuyển sang các bài đọc khác thú vị hơn. Nhưng nếu có điều gì xảy ra với máy tính của bạn thì đừng trách tôi không cảnh báo nhé! Cách tốt nhất giúp bạn tìm hiểu về các bản vá lỗi bảo mật và các bản thông báo bảo mật từ hãng Microsoft được mô tả ở tại

http://go.microsoft.com/fwlink/?LinkId=22339.

Tại đây bạn sẽ đăng ký để có thể cập nhật các thông tin về bảo mật, các bản vá lỗi bảo mật qua email. Thêm nữa nó còn cung cấp cho bạn các kiến thức và công nghệ giúp bạn tự động vá lỗi hệ điều hành

Tự động cập nhật

Windows 2000 SP 4, XP, 2003 cung cấp cho bạn các tính năng tự động kiểm tra và download các bản vá lỗi bảo mật mới nhất từ Microsoft Automatic Update sẽ có thể cấu hình để giúp bạn download tự động các bản vá mà không ảnh hưởng đến công việc bạn đang làm trên máy tính sau đó nó sẽ nhắc nhở bạn cài đặt sau khi download được hoàn thành

Để cấu hình hệ thống cập nhật tự động bạn làm như sau:

1. Từ Menu Start, Settings, Chọn Control Panel sau đó kích vào Automatic Updates

2. Chọn **Keep my computer up to date** để bật tính năng cập nhật tự động

3. Chọn **Automatically download the updates, and install them on the schedule that I specify**.

4. Chọn lịch cập nhật

5. Sau đó kích **OK** và đóng **System Properties**

Chú ý: Ngòai ra, Các bản thông báo bảo mật được phát hành thông qua Security Notification Service. Với hệ thống này sẽ tự động rà soát máy tính của bạn và nhắc nhở bạn download và cài đặt chúng trên máy tính của bạn

Kiểm tra bảo mật với công cụ Microsoft Baseline Security Analyzer

Nằm trong chiến lược bảo mật của Microsoft, phần mềm ***Microsoft Baseline Security Analyzer (MBSA),*** *sẽ báo cáo cho bạn các cấu hình không bảo mật và các bản vá lỗi Windows 2000, XP và Windows Server 2003. Chương trình này bạn có thể sử dụng trên máy bạn hoặc trên một máy điều khiển từ xa. Phần mềm này không thể thiếu cho những nhà quản trị mạng cần phân tích hiện trạng của máy chủ. Kể cả những người dùng bình thường nó cũng đưa ra được lời khuyên và các chỉ dẫn cần thiết về bảo mật*

Các bước cài đặt và sử dụng chương trình MBSA

Để cài đặt MBSA bạn cần phải download phần mềm này (Dung lượng khoảng 1.56 Mb): **Download MBSA**

Sau đó bạn cài đặt bình thường như các phần mềm khác theo từng bước. Quá trình cài đặt được hoàn thiện bạn tiếp tục thực hiện các bước ở phía dưới đây

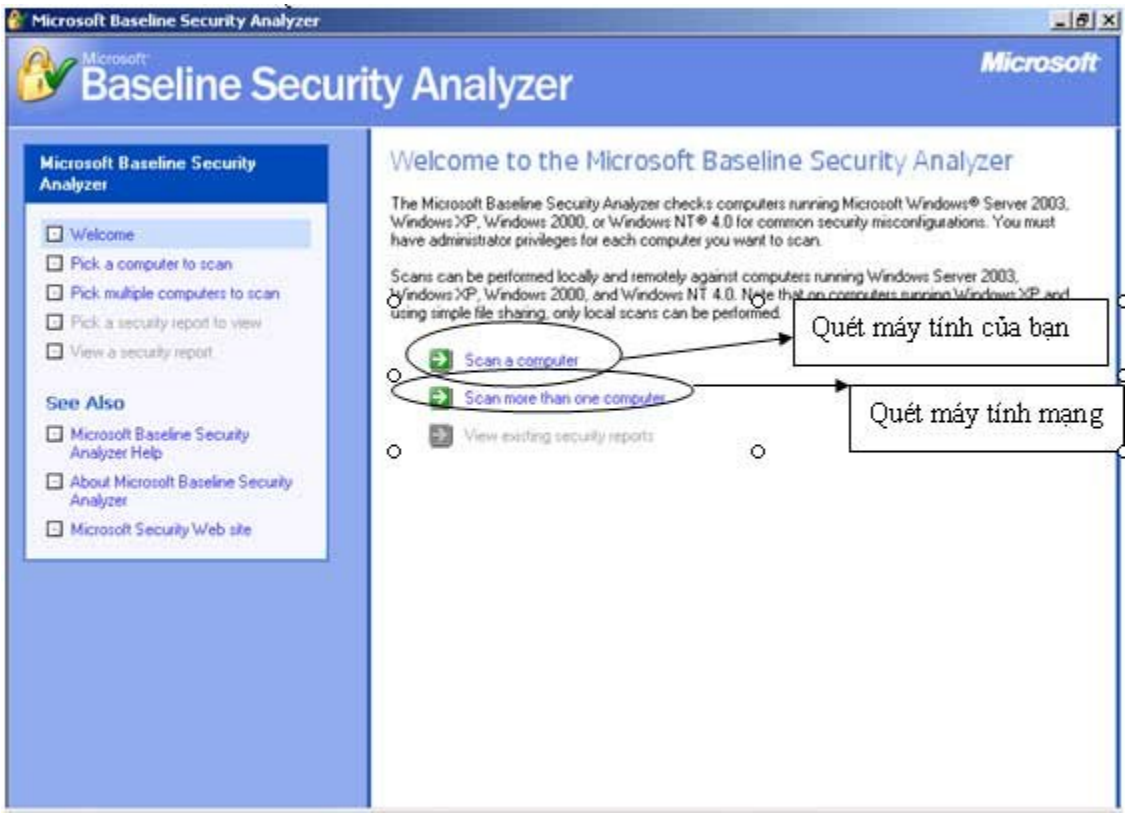
Quét các bản cập nhật và vá lỗi

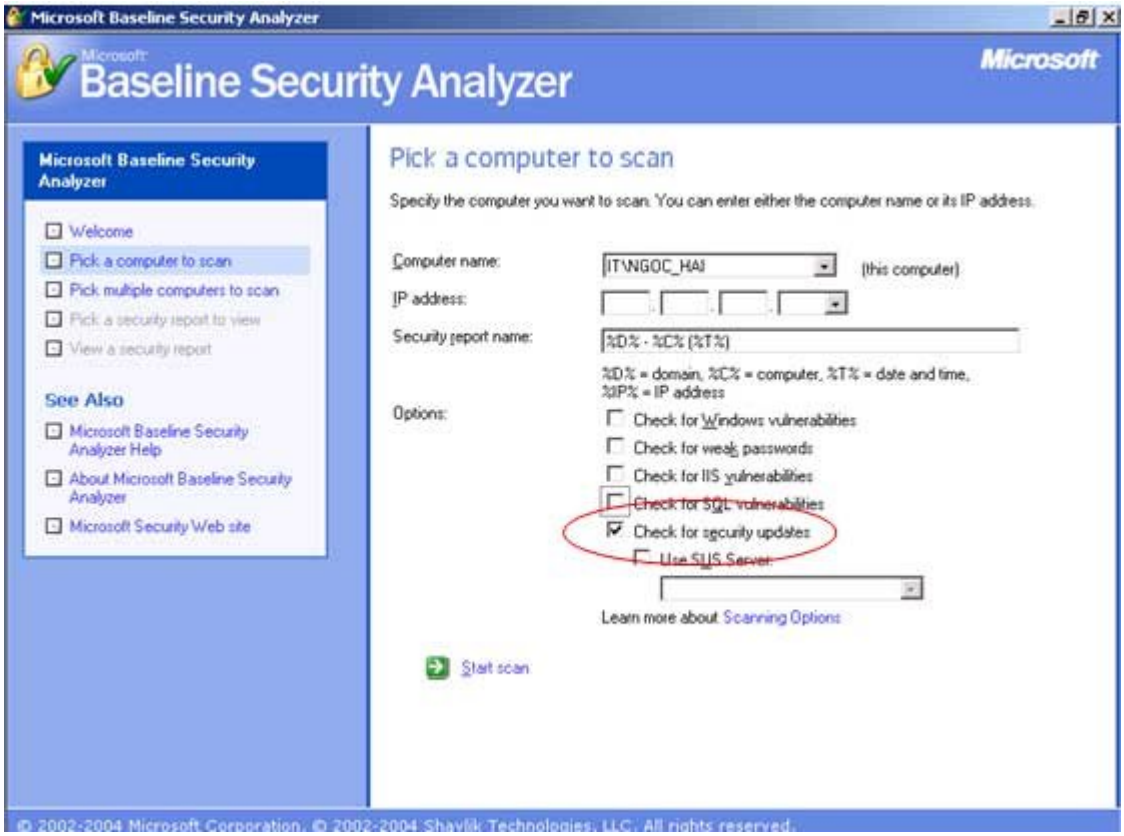
1. Từ Start menu chọn Programs à Microsoft Baseline Security Analyzer

2. Kích vào *Pick a computer to scan*

3. Bỏ các lựa chọn sau:

- ***Check for Windows vulnerabilities***
- ***Check for weak passwords***
- ***Check for IIS vulnerabilities***
- ***Check for SQL vulnerabilities***


Microsoft Baseline Security Analyzer
Microsoft
Baseline Security Analyzer
Microsoft
Microsoft Baseline Security Analyzer
Welcome
Pick a computer to scan
Pick multiple computers to scan
Pick a security report to view
View a security report
See Also
Microsoft Baseline Security Analyzer Help
About Microsoft Baseline Security Analyzer
Microsoft Security Web site
Welcome to the Microsoft Baseline Security Analyzer
The Microsoft Baseline Security Analyzer checks computers running Microsoft Windows® Server 2003, Windows XP, Windows 2000, or Windows NT® 4.0 for common security misconfigurations. You must have administrator privileges for each computer you want to scan.
Scans can be performed locally and remotely against computers running Windows Server 2003, Windows XP, Windows 2000, and Windows NT 4.0. Note that on computers running Windows XP and using simple file sharing, only local scans can be performed.
Scan a computer
Scan more than one computer
View existing security reports
Quét máy tính của bạn
Quét máy tính mạng



Sau đó kích vào **Start Scan**

Quét các cấu hình bảo mật

Để quét các cấu hình bảo mật bạn làm như sau:

1. Loại bỏ lựa chọn **Check for security updates,** và chắc chắn rằng các lựa chọn sau phải được đánh dấu: (Cách làm này ngược với cách làm trên)

    - § Check for Windows vulnerabilities
    - § Check for weak passwords
    - § Check for IIS vulnerabilities
    - § Check for SQL vulnerabilities

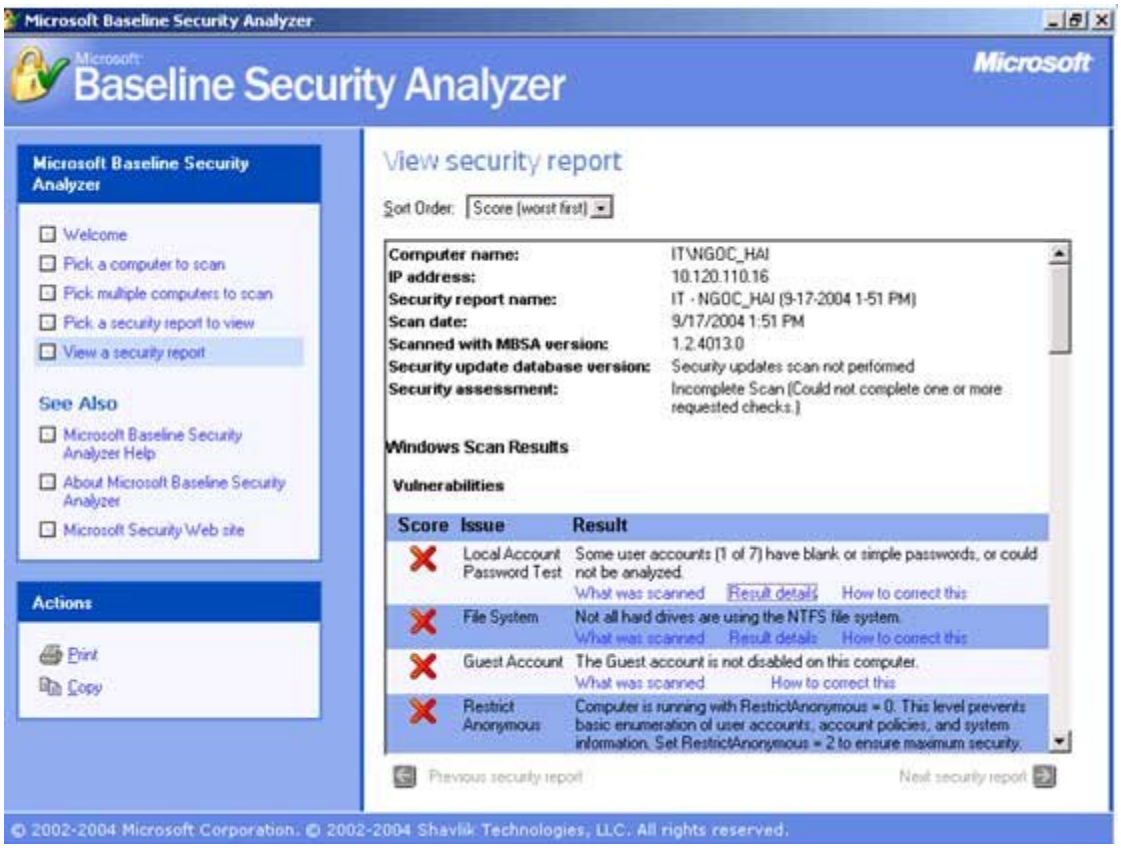
2. Sau đó kích vào **Start Scan**

3. Sau khi quét xong, bảng báo cáo kết quả sẽ xuất hiện giống như khi bạn quét các bản cập nhật của Windows Update. Nó chỉ khác ở chỗ là tại khác đường liên kết trong kết quả được tìm

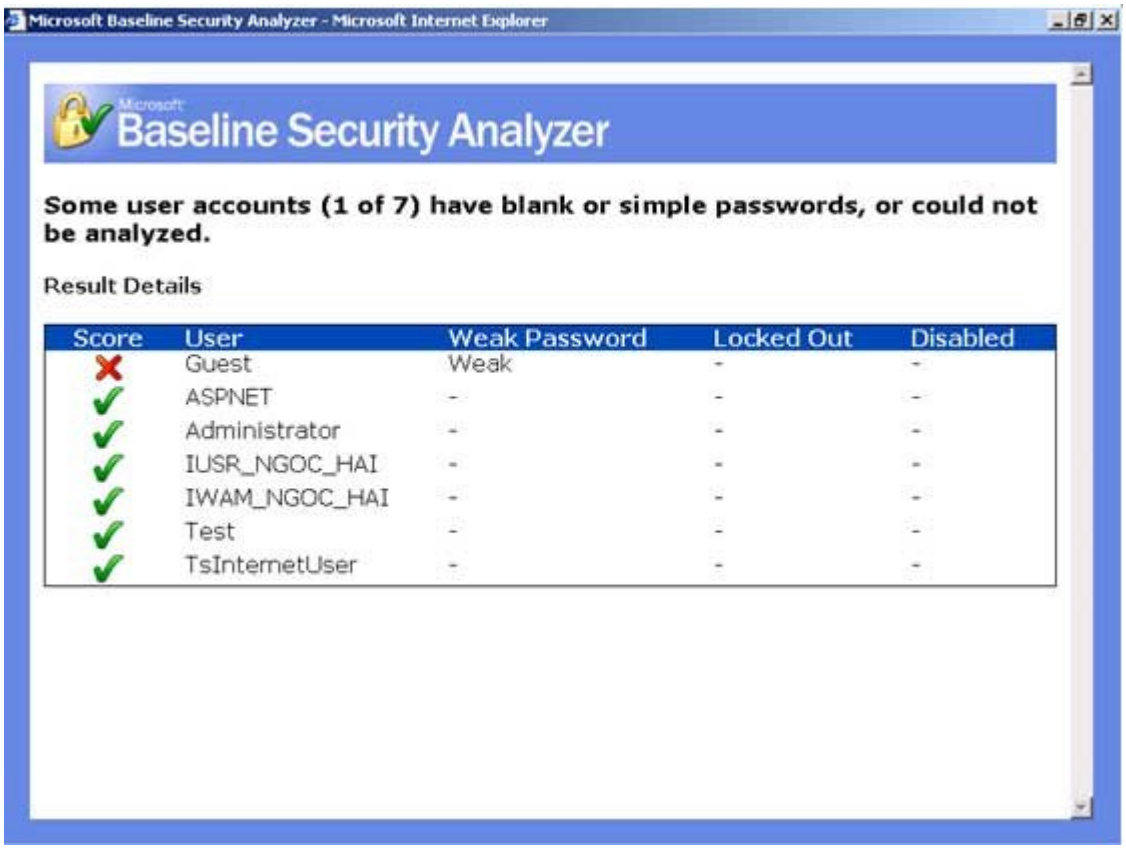
thấy. Khi bạn kích vào liên kết, một trang sẽ xuất hiện với chi tiết các kết quả tìm thấy, các giải pháp được đưa ra

4. Vậy thì bạn phải làm gì và giải pháp như thế nào?Xin vui lòng kích vào liên kết "**How to correct this**" bạn sẽ được liệt kê các nội dung chi tiết, giải pháp, các giải thích và bạn phải làm gì và từng bước giải quyết vấn đề

Ví dụ sau khi kiểm tra máy tính thử nghiệm tôi có kết quả như sau:

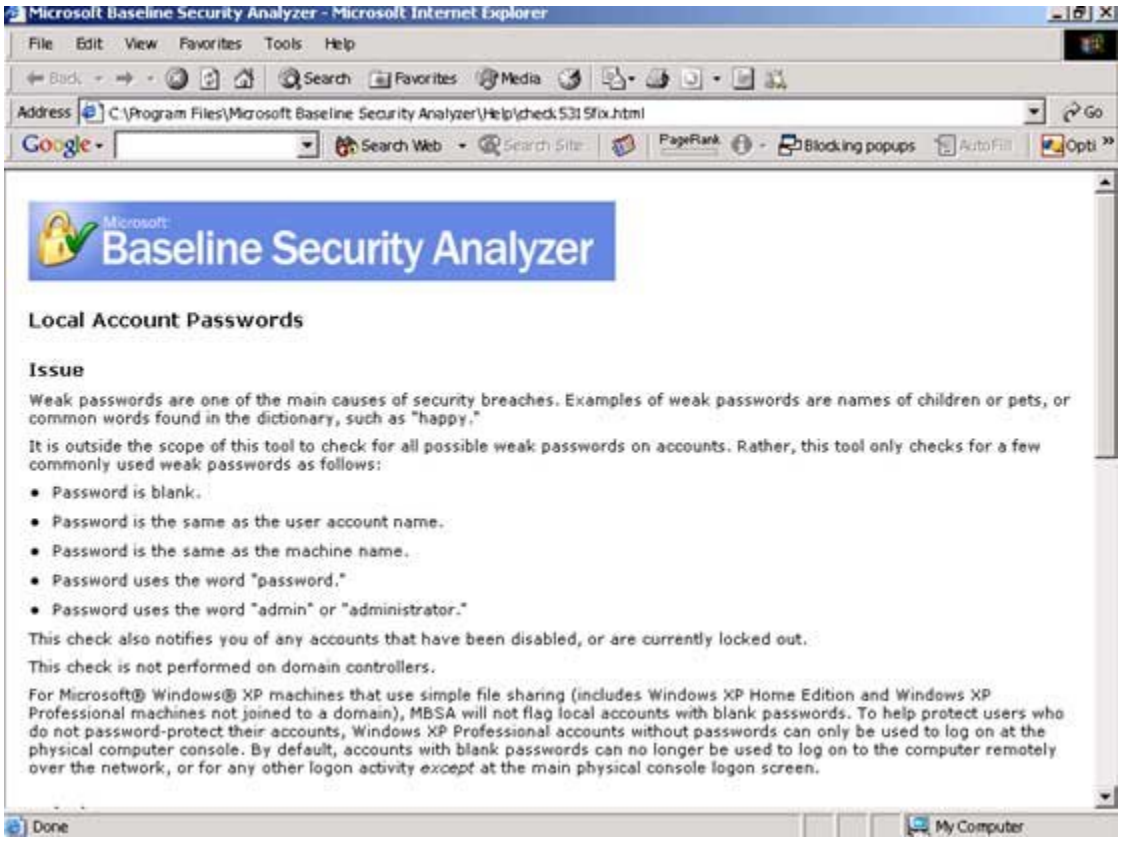


Khi kích vào liên kết "**Result details**" ta sẽ được các bảng mô tả chi tiết sau:



Trong bảng thông báo này ta sẽ thấy tài khỏan khách (Guest) của máy đang được mở và không đặt mật khẩu hoặc là mật khẩu quá ngắn (từ 1 đến 7 ký tự) không an toàn. Rõ ràng là không an toàn rồi (Như ở trên tôi đã phân tích về bảo mật các chia sẻ)

Bạn kích vào "**How to correct this**"



Tại đây công cụ sẽ đưa cho bạn các lời khuyên, các hướng dẫn khắc phục. Phần mềm này rất hữu ích cho tất cả các nhà Quản Trị mạng và nó có thể áp dụng cho máy tính cá nhân của bạn để kiểm tra độ an toàn của máy tính mình. Trên đây chỉ là một số hướng dẫn cơ bản sử dụng phần mềm mong rằng nó sẽ hữu ích đối với bạn đọc. Bài học của chúng ta đến đây kết thúc. Chúc các bạn bảo vệ máy tính an toàn và hiệu quả.