http://vietdown.org

Sưu Tầm Thủ Thuật

PII

Thiết Kế: Nguyễn Anh Tú

NÓI THÊM VỀ CÁC TRÌNH DUYỆT WEB (BROWSER)

Nhân đọc bài Duyệt Web mê ly với Opera 7.5x ở LBVMVT 61,tôi đã sử dụng phần mềm này lâu rồi,nay xin mạn phép đóng góp một vài ý kiến với đọc giả:

- Không phải chỉ IE mới có nhiều "tử huyệt" ,mà vì IE là trình duyệt phổ biến nhất Thế Giới, . Cho nên là mục tiêu của nhiều Hacker. Điều đó cũng giống như Mỹ hay xảy ra tai nạn máy bay vì họ có số lượng máy bay chiếm 1/5 thế giới.Opera & Netscape cũng có nhiều khuyết điểm nhưng vì không phổ biến nên không lôi cuốn các Hacker.

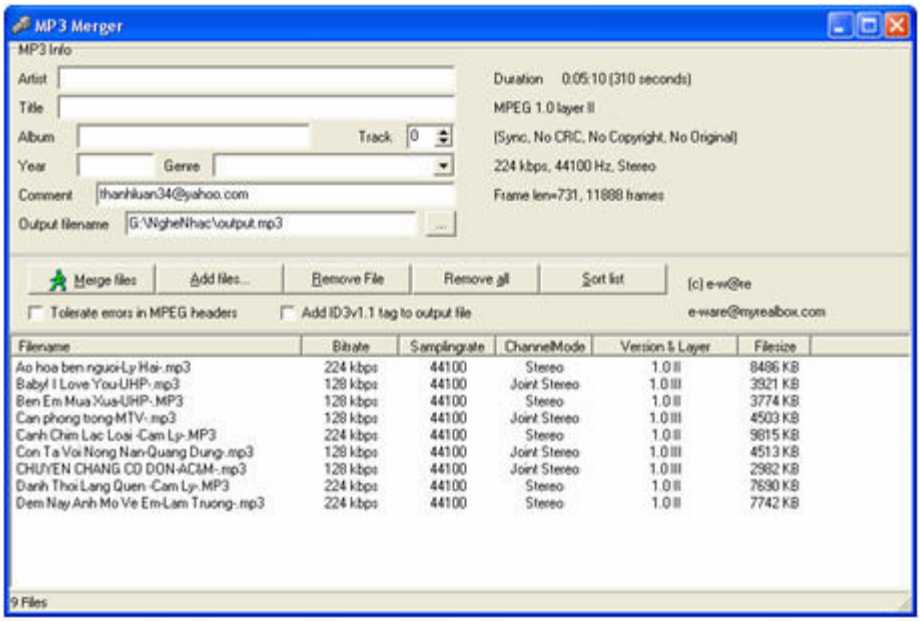
- Mặt khác cũng chính vì IE rất phổ biến,cho nên các Hacker thường xâm nhập vào các trang Web phổ biến (như PCWorld.com…) để chèn vào các đoạn mã lập trình nhằm làm cho server của trang Web đó sẽ trở nên chậm chạp khi người truy cập dùng IE để viếng thăm trang Web đó.Mục đích của việc phá hoại đó thật đơn giản: hoặc chỉ vì muốn chọc ghẹo Bill Gates ,hoặc là làm như vậy bọn Hacker sẽ bán được các phần mềm (mà chúng gọi là Plug-ins cho IE).Cơ chế hoạt động của những phần mềm này thật đơn giản:xóa bỏ các đoạn mã mà chúng đã chèn vào các trang Web,như vậy tự động trang Web đó sẽ không còn chậm chạp nữa.

- Với các trang Web chuyên nghiệp, được thiết kế để xem với rất nhiều trình duyệt,cho nên khi chúng ta truy cập những trang Web đó với trình duyệt không phổ biến lắm (như ở VN là Opera & Netscape) thì vẫn xem được bình thường.Nhưng với những trang Web nghiệp dư,phi thương mại của những bạn ít am hiểu về lập trình mạng & thiết kế Web,thì các trình duyệt không phổ biến hầu như không mở được đúng với định dạng & kích thước ban đầu (font, table…)

Như vậy với những gì đã nói ở trên,tốt nhất là chúng ta sử dụng song song hai trình duyệt: một trình duyệt phổ biến (IE) & một trình duyệt khác (ở đây tốt nhất là Opera…).Khi xem một trang Web nào đó,nếu trình duyệt này chậm chạp hoặc lộn xộn,chúng ta hãy thử duyệt trang đó với trình duyệt còn lại.

NOI FILE MP3 VOI MP3 MERGER

Có bao giờ bạn muốn nối tất cả các file Mp3 trong máy bạn thành một file duy nhất và có thể nghe tất cả các bài hát bạn yêu thích xuyên suốt từ đầu đến cuối thì phần mềm Mp3merge là một giải pháp hòan tòan thích hợp. Ưu điểm của phần mềm này là cực kì nhỏ gọn không cần bất kỳ thủ tục cài đặt nào mà chỉ cần chạy trực tiếp trên một file duy nhất và đặc biệt là hòan tòan được miễn phí. Sau khi chạy chương trình giao diện của Mp3merge sẽ như hình bên



Khi cần nối các file Mp3 nào với nhau bạn nhấn vào nút Add files để nối các file này lại thành một file Mp3 duy nhất, sau khi đã chọn xong nó sẽ hiện được tất cả các bài thông qua menu list ở bên dưới, bài nào bạn cảm thấy không thích hợp thì bạn chọn bài đó và bấm nút Remove files hoặc bấm nút Remove All để bỏ chọn hết tất các bài. Trên mục Mp3 Info là các mục lên quan đến thông tin bài hát, bạn có thể chỉnh sửa tùy ý trong các mục này. Trong mục Output filename là đường dẫn lưu lại và tên bài hát sẽ được nối lại. Sau khi đã hòan tất các bước bạn bấm nút Merge files để nối các bài hát lại là xong. Bạn có thể tải chương trình này tại địa chỉ : http://www.download.com/ dung lượng 428 Kb hòan tòan miễn phí.

NHỮNG CÁCH ĐƠN GIẢN TĂNG TỐC INTERNET

Gần đây có rất nhiều ý kiến về tốc độ download thế nào là nhanh thế nào là chậm. Qua kinh nghiệm của mình tôi xin trình bày một số thủ thuật để có thể tăng tối đa tốc độ tải file và duyệt web. Hy vọng các bạn có thể áp dụng và giảm cước phí truy cập cái Internet "giá trên trời" này.

Trước hết phải nói rằng, tốc độ tải file và kết nối phụ thuộc vào rất nhiều yếu tố "thiên thời, địa lợi, nhân hòa" như: bạn thuộc mạng nào, đường dây điện thoại có tốt không, có nhiều người đang ở trên mạng không và thậm chí thời tiết thế nào... nên việc cho rằng tải file với tốc độ bao nhiêu là nhanh, bao nhiêu là chậm chỉ có ý nghĩa tương đối. Tuy nhiên chúng ta vẫn có thể can thiệp vào một số vấn đề như các thông số của Windows và nhờ các trình tăng tốc trợ giúp.

1) Các thủ thuật tối ưu hóa hệ thống: Đây là các thủ thuật để vượt qua các thông số mặc định (nhưng không phải là tối ưu cho Internet) của Windows.

- Tối ưu thông số MaxMTU (Max Transnission Unit): đây là một việc thuộc dạng "must-do". Theo mặc định của Windows thông số này là 1500, thông số tối ưu là 576. Để xác lập thông số này, và các thông số khác như NDI cache, IPMTU, RcvWindow,TTL (Time To Live)... tốt nhất bạn nên dùng các trình tiện ích như NetMaster (có thể download tại http://www.magellass.com/) vì nó động tới cái gọi là Registry rất rắc rối của anh WINDOZE.
- Tối ưu tốc độ Modem và Dial-Up Networking:

+Vào Start menu/Run gõ sysedit và chọn cửa sổ WIN.INI. Tìm mục [Port] và sửa gía trị cổng modem như sau: COMx:=921600,n,8,1,p , x = số cổng modem (vd: modem gắn ở cổng COM2) 921600 = tốc độ tối đa (bps) , n = non-parity , 8 = 8 data bits , 1 = 1 stop bit , p = hardware flow control

+ Vào Control Panel/Modem, nhấn vào nút Properties, chọn "Maximum speed" là 115200. Tiếp theo vào tab Connection nhấn nút Advanced và bỏ chọn (uncheck) "Use error control" và "Required to connect". Nhấn OK để lưu các thông số.

+ Để tăng tốc độ quay số, ở tab Connection/Advanced nói trên, bạn có thể thêm dòng S11=40 vào "Extra Settings". Số 40 là chỉ thời gian giữa hai số quay tính bằng mili-giây.

+ Vào Dial-Up Networking, nhấp chuột phải vào quay số kết nối, chọn Properties. Nhấp vào tab "Server Type", bỏ chọn NetBEUI và IPX/SPX (nhưng phải chọn TCP/IP). Tiếp theo vào Control Panel/Network, chọn Dial-Up Adapter và nhấn vào nút Properties. Tại tab "Bindings" bạn bỏ hết các giao thức ngoại trừ TCP/IP.

Với tất cả các xác lập này, hệ thống của bạn đã sẵn sàng để kết nối và tải file với tốc độ nhanh nhất. Nhưng... nếu bạn muốn tăng tốc download lên thêm 300% và tăng tốc duyệt web lên từ 50 - 70% nữa thì bạn nên sử dụng các tiện ích mà tôi xin giới thiệu và đánh giá trong phần sau.

2) Các nhà vô địch trong download: Download Accelerator 4.0 và Mass Downloader 1.2

-Đây là hai tiện ích tăng tốc không thể thiếu cho việc tải file nó có thể tăng tốc độ tải file nhanh hn từ 200 - 300% so với cách thông thường nhờ cùng một lúc nó tải nhiều phần của tập tin với các thuật toán thông minh. Ngoài ra nó còn hỗ trợ resume trong mọi trường hợp (kể cả khi FTP site không hỗ trợ resume).

- Mass Dowloader luôn đạt điểm cao nhất về tốc độ tải file (tính bằng kbps) nhưng không có nghĩa là nó luôn hoàn thành việc tải file nhanh nhất. Theo thử nghiệm của bản thân tôi trong tất cả các trường hợp (cùng tốc độ kết nối, cùng tập tin) Mass Downloader chưa bao giờ vượt được Download Accelerator mà thường chậm hn từ 5 - 20%. Sau đây là các so sánh ưu nhược điểm của hai trình tăng tốc này:
- Download Accelerator 4.0 (tải về tại http://download7.speedbit.com/dap4.exe): Trình tăng tốc này tải về một lúc 4 phần của file và ghép nối lại thành file chính khi tải xong.

*Ưu:

+ Là trình tải file nhanh nhất (được thế giới công nhận đấy).
+ Hỗ trợ Resume trong mọi trường hợp (bản 4.0)
+ Tích hợp hoàn toàn với IE và Netscape Navigator (nhấp vào tên file để download)
+ Tự động dò tìm các mirror site và tải về từ site có tốc độ nhanh nhất.
+ Có tiện tích tìm file theo tên, MP3, games...

+ Có thể lập lịch trình tải file (bản 4.0).
+ Miễn phí hoàn toàn

*Khuyết:

+ Kém trực quan hơn Mass Downloader.
+ Khi tải file, mỗi file tải về cần một cửa sổ theo dõi riêng.
+ Bạn phải xem các quảng cáo "miễn phí" (vì đây là trình miễn phí mà).

Mass Downloader 1.2 (tải về tại http://www.tlnet.com.vn/weblh/): Trình tăng tốc này luôn tìm cách đạt được tốc độ tải file cao nhất và sử dụng một lúc đến 10 dòng dữ liệu để tải file về.

*Ưu:

+ Rất trực quan với các thông số về thời gian, tốc độ và các biểu đồ theo dõi tốc độ tải file...
+ Hỗ trợ Resume trong mọi trường hợp.
+ Tích hợp vời IE và NN (nhấn phím ALT+Click vào tên file để tải về).
+ Lập lịch tải file về.
+ Tất cả tích hợp trong một cửa sổ duy nhất.

*Khuyết:

+ Kém về tốc độ tải về so với Download Accelerator.
+ Thiếu một số tính năng so với DA.

-Lời khuyên của tôi là bạn có thể cài cả hai trình này vào máy mà không ảnh hưởng chi đến nhau. Nếu muốn dùng DA bạn nhấp thẳng vào tên file, còn nếu bạn thích dùng MD thì giữ phím ALT trong khi nhấp.

3) Trình tăng tốc duyệt Web bằng NetSonic Pro 2.5 :

-Nguyên tắc tăng tốc của NetSonic khá đơn giản và hiệu quả là duyệt đón đầu tức là trong lúc chúng ta đang xem các trang Web thì nó tải về các kết nối tới trang Web này để hiện ra tức thì khi chúng ta cần tời. Nó lưu các trang Web thường lui tới để hiển thị nhanh những phần cố định và sẽ refresh những phần khác biệt sau đó. Nó còn tối ưu được hai thông số hệ thống quan trọng nhất là MaxMTU và Receive Window Size.

-Bản NetSonic miễn phí có tại http://www.web3000.com/ , nhưng thiếu nhiều tính năng quan trọng như tải về trước hình đồ họa... tốt nhất bạn nên tìm bản NetSonic Pro 2.5 (có rất nhiều tại các site download trên Internet)

NHỮNG CÁCH BẢO VỆ HOSTING VÀ SERVER

I. .htaaccess:

1. Các trang báo lỗi:

Trong quá trình làm việc với client, nếu có lỗi xảy ra (vi dụ như không tìm thấy file) thì Apache sẽ báo lỗi bằng một trang có sẵn hiển thị mã số của lỗi đó, rất không đẹp và khó hiểu. Với .haccess thì bạn có thể tự tạo các trang báo lỗi hay hơn. Để làm được điều này thì trong file .htaccess bạn thêm dòng sau:
ErrorDocument errornumber /file.html
Trong đó errornumber là mã số của lỗi phát sinh, sau đây là những lỗi hay gặp:
401 - Authorization Required (cần password để truy nhập)
400 - Bad request (request bị sai)
403 - Forbidden (không được vào)
500 - Internal Server Error (lỗi server)
404 - Wrong page (lỗi trang, không tìm thấy...)
còn file.html là trang web mà ban muốn hiện thị khi lỗi phát sinh. Ví dụ: ErrorDocument 404 /notfound.html
hoặc: ErrorDocument 500 /errorpages/500.html

2. Không cho hiện danh sách file trong thư mục:

Trong trường hợp bạn không muốn cho người khác thấy được danh sách file trong thu mục không có file index, thêm lệnh sau vào .htaccess: Options -Indexes

3. Chỉ định các IP được/không được truy cập vào trang web:

Thêm lệnh sau: deny from 203.239.110.2 để cấm ip 203.239.110.2 hoặc allow from 203.239.110.20 để cho phép ip 203.239.110.20. Nếu bạn chỉ viết ip dưới dạng 203.239.110 thì sẽ cấm/cho phép tất cả ip trong giải từ 203.239.110.1 đến 203.239.110.254. Còn: deny from all : sẽ cấm tất cả mọi truy cập đến các trang web trong thư mục, tuy nhiên các file trong đó vẫn có thể được sử dụng từ bên ngoài thông qua các dang require hay include.

4. Thay thế trang index:

Dùng dòng lệnh sau: DirectoryIndex index.php index.php3 messagebrd.pl index.html index.htm . Với dòng lệnh này thì tất cả các file được liệt kê sẽ được tìm theo thứ tự khi có yêu cầu tới thư mục hiện hành, trang nào được tìm thấy đầu tiên sẽ thành trang index của thư mục.

5. Redirection:

Có thể redirect truy cập từ xa một cách đơn giản bằng lệnh sau: Redirect /location/from/root/file.ext http://www.othersite.com/new/file/location.xyz hoặc Redirect /olddirectory http://www.newsite.com/newdirectory

6. Bảo vệ thư mục bằng password :

-Trong file .htaccess có thể viết thêm:

```
+AuthUserFile /mnt/web/guide/somewhere/somepath/.htpasswd
AuthGroupFile /dev/null
AuthName Somewhere.com's Secret Section
AuthType Basic

<Limit GET POST>
require valid-user
</Limit>
```

+Trong đó quan trọng nhất là file .htpassword, có dạng như sau:

```
username:v3l0KWx6v8mQM
bob:x4DtaLTqsElC2
```

với phần trước là tên user, phần sau là password đã được mã hoá bằng DES (có thể dùng john để giải mã).
Bạn có thể tạo ra file .htpasswd này bằng một công cụ có sẵn trong *nix là trình htpasswd, vi dụ:

```
root@vnofear$htpasswd -c .htpasswd username
Adding password for username.
```

New password:
password
Re-type new password:
password

Khi truy cập vào thư mục được bảo vệ bởi .htpasswd, browser sẽ hiện ra một cửa sổ yêu cầu bạn nhập username và password.
*Lưu ý trước khi sử dụng .htaccess bạn nhớ kiểm tra xem host server có hỗ trợ .htaccess hay không.
Chú ý: các bạn có thể soạn file .htaccess bằng notepad

II. Bảo vệ ứng dụng Web ASP:

Điều này tưởng chừng như đơn giản nhưng chẳng đơn giản chút nào cả! Nếu như bạn nghĩ: ối giời! Web lỗi thì ăn nhằm gì đến pass host chứ! Thì bạn đã…trật rồi đấy! Nếu như tôi biết ứng dụng web của bạn bị lỗi gì và chèn vào đó một số mã nguy hiểm hay backdoor chẳng hạn thì mọi chuyện sẽ thay đổi!

1. An toàn trước khả năng bị tấn công CSS (Cross-Site Scripting)

Kiểu tấn công CSS điển hình nhất xảy ra khi tin tặc cố tình chèn một đoạn văn bản có chứa script độc hại vào các form nhập dữ liệu. Nội dung nhập vào có thể chứa các thẻ <OBJECT> hoặc <SCRIPT> cùng các đoạn mã hết sức nguy hiểm. Trình duyệt, khi truy nhập site, cho rằng các srcipt này do máy chủ gửi tới, hoàn toàn vô hại nên sẽ chạy nó ở cấp độ bảo mật bình thường, gây ra hậu quả tai hại cho máy tính của người sử dụng .

Để bảo vệ khỏi bị tấn công theo kiểu CSS, cần chú ý ít nhất những điểm sau:

- Cập nhật thường xuyên các bản sửa lỗi bảo mật mới nhất của IIS và Windows.
- Lọc các ký tự đặc biệt do người sử dụng nhập vào như < > " ' % ( ) & + -
- Lọc để loại bỏ các ký tự đặc biệt, kết xuất trên cơ sở thông tin nhập vào của người sử dụng. Xem kỹ các dữ liệu từ:

- Request.Form Collection
- Request.QueryString Conllection
- Request Object
- Database
- Cookie
- Các biến Session và Application

Để có thể lọc được, cần xác định cụ thể lược đồ mã hoá ký tự trên các trang Web, trong thẻ META, ở phần header. Ví dụ:

```
<head> <META http-equiv="Content-Type" Content="text/html; charset=ISO-8859-1">
</head>
```

2. Ứng dụng có thể không cần sử dụng các cookie thường trực

Cookie thường trực là những tệp, được các ứng dụng Web gửi tới máy tính người sử dụng và vẫn tồn tại trên ổ cứng của máy tính ngay cả khi họ không còn duyệt site. Chúng lưu một số thông tin về người sử dụng để các ứng dụng Web tuỳ biến nội dung cho phù hợp với từng đối tượng người sử dụng hoặc cho phép họ bỏ qua giai đoạn đăng ký đăng nhập. Các cookie không thường trực được lưu trong bộ nhớ máy tính của người sử dụng và chỉ tồn tại trong thời gian người sử dụng duyệt site. IIS dựa vào các cookie không thường trực để xác định một phiên ASP. Không có nó, IIS không thể duy trì bất kỳ các thông tin về phiên làm việc, chẳng hạn như các biến phiên.

Nếu site của bạn sử dụng cookie thường trực, không nên yêu cầu IIS lưu trữ chúng trong tệp log của IIS. Nếu tệp log lưu lại tất cả các thông tin đăng nhập của người sử dụng thì rất có nhiều khả năng, do một thoả hiệp nào đó, những thông tin này có thể được tiết lộ ra ngoài.

3. Sử dụng SSL cho tất cả các trang nhạy cảm được chuyển trên mạng Internet

SSL mã hoá nội dung của các thông điệp TCP/IP để nó không bị nhòm ngó trên đường truyền. SSL, hoặc một giải pháp mã hoá khác VPN chẳng hạn, rất cần thiết khi gửi các thông tin nhạy cảm (như số thẻ tín dụng) qua mạng. Cơ hội thâm nhập đường truyền và lấy cắp các thông tin bí mật là thấp song không phải không thể có.Người sử dụng sẽ không đặt niềm tin vào site của bạn nếu các thông tin nhạy cảm không được mã hoá.

Tuy nhiên, mặt trái của SSL là làm chậm lại hiệu năng thực hiện của ứng dụng. Mức sử dụng tài nguyên hệ thống CPU đòi hỏi trong tiến trình mã hoá và giải mã cho một trang SSL có thể cao hơn từ 10 đến 100% so với các trang không được bình thường. Nếu máy chủ của bạn có lưu lượng các trang SSL cao, bạn có thể phải cân nhắc tới việc sử dụng thêm một bộ tăng tốc SSL phần cứng.

4. Yêu cầu người sử dụng đăng nhập mỗi khi sử dụng ứng dụng

Nguyên tắc này áp dụng cho các ứng dụng có yêu cầu thủ tục đăng nhập. Điều này có nghĩa là việc đăng nhập tự động dựa trên cookie là không được phép. Mặc dù người sử dụng có thể thấy phiền hà nhưng nếu cho họ đăng nhập tự động dựa trên cookie sẽ có rất nhiều nguy hiểm (và như ta đã thấy ở phần trước, sử dụng các cookie thường trực không phải lúc nào cũng phù hợp).

Một biện pháp tiếp theo cần thiết để bảo vệ mật khẩu là huỷ tính năng Autocomplete của IE trên các trường mật khẩu. Điều này có thể thực hiện bằng cách thêm thuộc tính AUTOCMPLET ="OFF" cho thẻ <FORM> hoặc <INPUT>. Ví dụ:

```
<input type="password" name="pwd" size=16 maxlength=16 AUTOCOMPLETE="OFF">
```

5. Log out người sử dụng ra khỏi hệ thống ngay khi họ rời site

-Giả sử một người sử dụng đang xem một trang web trên site của bạn, sau đó họ truy cập một site mới nhưng cuối cùng lại quyết định quay trở lại trang của bạn bằng cách ấn phím BACK. Trong trường hợp này, ứng dụng phải yêu cầu người sử dụng đăng nhập lại một lần nữa. Phát hiện những tình huống tương tự như tình huống vừa rồi của người sử dụng phải dựa hoàn toàn vào các script chạy ở phía trình duyệt mà không thể dựa vào server vì nó không biết người sử dụng đã ở những đâu. Cách giải quyết đầy đủ nhất cho vấn đề này là sử dụng một giải pháp bảo mật Proxy Server như của Netegrity SiteMinder (http://www.netegrity.com).Giải pháp Proxy Server sẽ giám sát mọi yêu cầu Web từ trình duyệt và ghi lại mọi địa chỉ trình duyệt đã truy nhập để ứng dụng có thể kiểm tra.

-Một cách thức không đầy đủ trong việc kiểm tra các giới hạn site có thể thực hiện bằng cách thiết lập Request.ServerVariables("HTTP_REFERER"). Nếu người sử dụng có gắng truy nhập bất kỳ trang nào khác với trang đăng nhập, từ một URL của một site khác, thì họ sẽ bị từ chối. Tuy nhiên, phương pháp này không thể ngăn
ngừa một người sử dụng rời bỏ site của bạn để tới một site khác nhưng sau đó lại quay trở lại site của bạn và tiếp tục phiên làm của họ.

6.Cắt kết nối khi người sử dụng không tương tác với site trong một khoảng thời gian nhất định

-Có hai giải pháp cho vấn đề này, một giải pháp ở phía máy chủ và một giải pháp sử dụng script ở phía trình duyệt. Trong giải pháp thứ nhất, chúng ta sử dụng IIS Manager và đặt giới hạn phiên ASP là một khoảng thời gian mong muốn nào đó (giá trị mặc định là 20 phút). Trong ứng dụng, lưu trữ thông tin truy nhập vào một biến phiên làm việc và kiểm tra nó trên mọi trang người sử dụng duyệt qua. Nếu thông tin truy nhập không thuộc về một biến phiên, người sử dụng đã bị cắt kết nối với site và ứng dụng cần định hướng họ sang trang truy nhập hệ thống. Hơn nữa, mặc dù chưa phải có thể tin cậy tuyệt đối, bạn cũng có thể viết mã để xử lý cắt kết nối người sử dụng trong sự kiện Session_OnEnd ở tệp Global.asa.

-Giải pháp phía client sử dụng chút ít JavaScript. Chèn thêm đoạn mã sau vào đầu của mọi trang Web kết xuất bởi ứng dụng:

```
<script Language="JavaScript">
window.setTimeout("window.navigate('Logout.asp')", 900000); </script>
```

'Logout.ASP' là trang để cắt kết nối người sử dụng với ứng dụng. 9000000 là khoảng thời tối đa tính bằng mily giây người sử dụng vẫn duy trì phiên làm việc của họ trong trường hợp không có tương tác nào với site.

7. Ứng dụng không cho phép login đồng thời

Yêu cầu này có nghĩa là tại một thời điểm, người sử dụng không thể truy nhập ứng dụng với 2 phiên làm việc khác nhau. Đây cũng là nguyên tắc áp dụng cho phần lớn các ứng dụng client/server và máy trạm khác.

Trong môi trường IIS/ASP, việc đáp ứng yêu cầu này không có gì khó khăn. 2 sự kiện Session_OnStart và Session_OnEnd trong Global.asa có thể sử dụng để kiểm tra phiên truy nhập hiện thời của người sử dụng. Bạn cũng có thể áp dụng một giải pháp của cơ sở dữ liệu để huỷ một phiên làm việc đang tồn tại khi một phiên làm việc mới được bắt đầu.

8. Mã nguồn ứng dụng không chứa chú thích của người phát triển

Bất cứ cấp bảo mật nào cũng có thể thất bại. Trong những trường hợp khi đã truy nhập được vào các tệp mã nguồn của Website thì những chú thích của người phát triển sẽ là những trợ giúp đắc lực cho tin tặc, nguy hiểm nhất là trong trường hợp mã nguồn có chứa những "viên ngọc" như tên và mật khẩu dùng trong quá trình chạy thừ ứng dụng. Yêu cầu này chỉ áp dụng cho những tệp script, chẳng hạn như các trang ASP, không áp dụng cho các đoạn mã trong các đối tượng COM đã được biên dịch.

Trước đây, những điểm yếu về bảo mật chưa được khắc phục của IIS làm cho các script ASP trên một số site rất dễ bị đọc trộm. Nhiều tin tặc biết rằng học có thể đọc các script này bằng cách thêm chuỗi "::$DATE" vào cuối yêu cầu truy xuất trang. Để tránh các rủi ro có thể xảy ra, cần loại bỏ mọi chú thích trên trang ASP, HTML hoặc mã JavaScript. Bạn có thể thực hiện bằng tay nhưng cách nhanh nhất là viết một chương trình để loại bỏ các chú thích từ các loại tệp khác
nhau.

9. Không lưu trữ thông tin kết nối cơ sở dữ liệu trong global.asa

Thông tin kết nối cơ sở dữ liệu gồm tên server , tên cơ sở dữ liệu, thông tin truy nhập SQL Server. Vì là một tệp văn bản, những thông tin trong global.asa có thể bị lộ và rơi vào tay những đối tượng sử dụng không đúng mục đích. Những thông tin này nên được lưu trữ ở những nơi khác. Hai cách phổ biến là lưu trữ nó trong một tệp hoặc trong một Register.

Lưu trữ thông tin kết nối cơ sở dữ liệu trong một tệp và sau đó có thể đọc được bằng File System Object hoặc XML Parser là cách an toàn hơn lưu trong global.asa. Một giải pháp lưu thông tin trên tệp khác là sử dụng tệp UDL vì nó cho phép lưu tất cả các chi tiết về kết nối. Chuỗi kết nối ADO sẽ trở thành "FILE Name =C:\ Path_That_IUSR_<machinename>_Can_Get_To\MyDataLink.UDL" trong đó tài khoản dịch vụ IIS, IUSR_<machinename>phải có quyền truy nhập để đọc được tệp này.

Lưu các thông tin kết nối dưới hình thức được mã hoá trong registry là cách an toàn nhất. Điều này yêu cầu ứng dụng phải viết các thông tin mã hoá vào trong registry và các thành phần COM phải thu về và giải mã nó ở thời gian chạy.

Đối với IS 5, nếu sử dụng thành phần COM+, còn có một lựa chọn registry khác. COM+ cho phép mỗi thành phần có Constructor được thiết lập trong Component Services Manager. Vì không mã hoá thông tin, cách này cho phép người quản trị site kiểm soát việc truy nhập cơ sở dữ liệu và thay đổi nó vào bất cứ lúc nào.

10. Các tệp audit log của cơ sở dữ liệu nên ghi nhận tất cả các thay đổi đối với dữ liệu

Các tệp audit log của cơ sở dữ liệu cung cấp các thông tin quá khứ về những thay đổi đối với dữ liệu trong các bảng. Một cách thông thường là tạo các trigger của cơ sở dữ liệu để ghi lại tất cả các thao tác Insert, Update và Delete. Tuy nhiên, ghi nhận tất cả thay đổi đối với mọi bản ghi có thể làm tăng kích cỡ cơ sở dữ liệu của bạn lên nhiều lần. Để giảm khối lượng dữ liệu lưu, cần phải cân nhắc kỹ những thay đổi dữ liệu ở các bảng nào cần được ghi nhận. Mặc dù có thể tạo các bảng và viết trigger bằng tay, nhưng để giảm nhẹ khối lượng công việc, chúng ta có thể sử dụng giải pháp tự động. Một số sản phẩm và script miễn phí tại địa chỉ http://www.sqldevpro.com/articles/MagicAuditingCode.htm có thể giúp bạn thực hiện điều này.

11. Sử dụng các thủ tục lưu sẵn (stored procedure) để truy nhập cơ sở dữ liệu

- Giới hạn việc truy nhập cơ sở dữ liệu, chỉ cho phép thực hiện thông qua các thủ tục lưu sẵn có nhiều ưu điểm về bảo mật và hiệu năng thực hiện. Cách tiếp cận này nên được tính đến ngay từ khi bắt đầu phát triển ứng dụng để việc triển khai về sau được dễ dàng hơn.
- Sử dụng thủ tục lưu sẵn an toàn hơn sử dụng ADO Recoredset hoặc các lệnh SQL bởi vì qua nó cho phép chỉ có người sở hữu cơ sở dữ liệu, dbo, mới có quyền quyền truy nhập tới bảng của tất cả những người sử dụng khác. Người sử dụng có quyền thi hành trên các thủ tục lưu sẵn nhưng không có quyền đọc hoặc sửa đổi dữ liệu trong các bảng một cách trực tiếp. Chỉ có dbo và người quản trị mới được phép sử dụng Query Analyzer hoặc Crystal Reports để làm việc với dữ liệu. Vì vậy, yêu cầu này có nghĩa là nếu Crystal Reports hoặc các công cụ tương tự khác được sử dụng trên Website, việc thu nhận dữ liệu phải được triển khai qua các thủ tục lưu sẵn.
- Với cách tiếp cận này, chúng ta cần tạo 4 thủ tục cho mỗi bảng cho các lệnh Select, Insert, Update and Delete. Bạn cũng có thể tạo một lớp bao (wrapper class) đóng vai trò là giao diện của thủ tục trong tầng truy nhập cơ sở dữ liệu của ứng dụng.

Dưới đây là thí dụ về thủ tục chèn dữ liệu vào bảng Authors trong cơ sở dữ liệu của một nhà xuất bản:

```
CREATE PROCEDURE dp_authors_ins @au_id varchar(11), @au_lname varchar(40),
@au_fname varchar(20), @phone char(12) = NULL OUTPUT , @address varchar(40) =
NULL , @city varchar(20) = NULL , @state char(2) = NULL , @zip char(5) = NULL ,
@contract bit AS IF @phone IS Null SET @phone = ('UNKNOWN')

INSERT INTO authors WITH (ROWLOCK) ( au_id, au_lname, au_fname, phone, address,
city, state, zip, contract) VALUES (@au_id, @au_lname, @au_fname, @phone,
@address, @city, @state, @zip, @contract)

SELECT @phone = phone FROM authors WHERE au_id = @au_id

GO
```

Đọc và thay đổi dữ liệu có hơi khác với cách tiếp cận thủ tục lưu sẵn. Thay vì làm việc với các recorset ADO hoặc tạo các câu lệnh SQL để thi hành trên server, tất cả việc truy nhập cơ sở dữ liệu đều thông qua đối tượng điều khiển ADO. Các đối tượng điều khiển ADO sẽ thi hành thủ tục lưu sẵn này.

III. Những điều cần biết khi chọn host:

Duy trì Web server có thể là một việc rất tốn kém về tiền bạc và thời gian. Thế nhưng với khoản phí hàng tháng, một nhà cung cấp host sẽ đảm bảo mọi vấn đề kỹ thuật, giúp cho công ty bạn có thể chú tâm vào việc phát triển nội dung. Trang Internet ngày nay kỳ này xin đăng 21 điều bạn cần biết khi chọn host.

1. Hãy nghĩ đến ngày mai cũng như ngày hôm nay

Khi site của bạn trở nên phức tạp hơn, nó có thể cần thực hiện script ở trên server, hỗ trợ cơ sở dữ liệu, thương mại điện tử hay cung cấp đủ băng thông để truyền âm thanh và hình ảnh. Bạn sẽ không tìm thấy những hỗ trợ đó trên các site host miễn phí. Điều quan trọng là bạn phải đánh giá một cách thực tế những nhu cầu của site của bạn không chỉ ở hiện tại mà cả trong tương lai.

2. Hãy để tâm đến các vấn đề bảo mật

Một host cung cấp hàng rào bảo vệ giúp phòng tránh mọi sự tấn công và các hành vi tin tặc khác diễn ra hàng ngày làm ngừng hoạt động nhắm vào server của bạn. Thực sự bạn có muốn ngày nào cũng mất thời gian để xem lại những lần truy cập server, cập nhật phần mềm vŕ phục hồi những thiệt hại do các tuyến phòng thủ của bạn thường xuyên bị chọc thủng?

3. Quyết định loại host nào là tốt nhất cho bạn

Mức thứ nhất của host sẽ đặt site của bạn cùng nhiều site khác lên một máy chủ trong một domain ảo có thể định vị site bạn trẹn máy đó . Đây chính là kiểu nuôi chung (shared hosting). Khi nội dung nhiều lên hay khi chuyển trang Web từ dạng tĩnh sang trang tương tác, bạn nên chuyển site của mình sang máy có nhiều nguồn

tài nguyên hơn và có ít site dùng chung nguồn tài nguyên đó hơn . Bước tiếp theo là một máy dành riêng cho site của bạn. Nhà cung cấp host sẽ sở hữu, duy trì và sao lưu máy chủ đồng thời cung cấp tất cả các hạng mục về bảo mật vật lý cho site, lưu điện và các vấn đề khác về điều hành trung tâm dữ liệu.

Mức cao nhất của host là sắp đặt các máy chủ ở cùng một chỗ. Trong trường hợp này bạn sở hữu toàn bộ phần cứng của mình nhưng về mặt vật lý nó được đặt lại chỗ của bên host để tận dụng được ưu thế của nhà cung cấp: Bạn có thể chọn dải băng tần mí bạn cần và nhà cung cấp sẽ cho bạn một đường kết nối riêng vào Internet. Đây là một tuỳ chọn hết sức hấp dẫn nhưng với phần lớn các nhà cung cấp, điều này có nghĩa là bạn phải tự thực hiện các khoản mục về bảo an và tường lửa của riêng bạn; bạn sẽ không được sự bảo vệ từ tường lửa của bên cung cấp hosting. Trừ khi bạn là chuyên gia về các vấn đề bảo an, còn không thì bạn sẽ muốn ký kết hợp đồng với bên cung cấp host hay một nhà tư vấn về bảo an để có được sự bảo vệ thích hợp cho site và máy chủ của bạn.

4. Nhu cầu dịch vụ nhanh chóng và hiệu năng

Việc site của ban có đạt được thành công và danh tiếng hay không phụ thuộc vào cấp độ host. Một site phục vụ chậm do các server bị quá tải sẽ không thu hút được người xem. Một site khó duy trì sẽ không thể đáp ứng hết nhu cầu hoặc khiến bạn phải làm việc vất vả hơn để làm mọi thứ mà bạn cần làm. Chẳng hạn, có thể bạn muốn lập một hộp e-mail đặc biệt dành để quảng cáo hay tranh luận. Một vài mục nhập nhanh vào một trang HTML hay một bảng của các tài khoản thư hợp thức có thể là tất cả những gì bạn cần, nhưng nếu như bạn phải đợi cho bộ phận kỹ thuật của bên cung cấp host làm việc đó thì bạn có thể để tuột mất cơ hội của mình.

5. Các ứng dụng của bạn phải phù hợp với mức của nhà cung cấp host

Một số ứng dụng và một số kiểu site là rất khó thực hiện với host. Nếu một dịch vụ được xây dựng với một vùng đĩa lớn và một số máy chạy nhanh thì nó có thể đủ phục vụ rất nhiều trang tĩnh. Nhưng nếu một site đặt ra những đòi hỏi lớn đối với CPU thẻ nó sẽ chạy chậm hơn trong môi trường đó, ví tồi tệ hơn sẽ làm giảm tốc độ của các site khác. Các diễn đàn thảo luận đòi hỏi đặc biệt khắt khe đối với các máy chủ hosting, bởi vẽ chúng cần bộ nhớ dung tích lớn, khả năng truy cập nhanh vào cơ sở dữ liệu tranh luận. Nếu bạn dự định cho một diễn đàn lớn, sôi động thì hãy tìm nhà cung cấp biết cách thực hiện chúng.

Site mà bạn mong muốn có thể còn đặt ra những đòi hỏi đặc biệt đối với máy chủ hosting. Luồng dữ liệu âm thanh với hình ảnh yêu cầu kết nối nhanh tới mạng trục, hệ thống đĩa lưu trữ tốn kém và các server mạnh có phần mềm phù hợp. Kinh nghiệm cung cấp host đa phương tiện cũng cần thiết, vì vậy bạn nên tìm một bên cung cấp host có kinh nghiệm, họ sẽ tạo các công cụ thuận tiện cho bạn.

6. Chọn hệ điều hành.

Hãy để các ứng dụng dẫn dắt bạn; hãy chạy chúng trên hệ điều hành mà theo bạn là hiệu quả nhất. Một nhà cung cấp host cung cấp cả Microsoft Windows và Unix sẽ đưa ra những lời khuyên khách quan. Đừng cho rằng cần có Windows NT để chạy site của bạn với những phần mở rộng Frontpage. Đã có ít nhất một nhà cung cấp host, Eas Street Online Services (www.easystreet.com), gặt hái được thành công lớn trong việc viết lại những phần mở rộng để chạy tốt hơn trẹn Unix so với trên Windows NT.

7. Đọc kỹ các giấy tờ

Chúng tôi đã dành rất nhiều thời gian để đảm bảo rằng mình hiểu những điều khoản và điều kiện của mỗi nhà cung cấp dịch vụ mà chúng tôi ký kết. Bạn cũng nên làm như vậy. Nên có một luật sư xem xét các điều khoản. Đừng bao giờ cho rằng một điều khoản trong bản hợp đồng sẽ không được thực thi hay như thế nào đó không áp dụng đối với bạn. Nó có áp dụng đấy. Phải đặc biệt quan tâm đến việc sở hữu bản quyền, trả lời các khiếu nại về site của bạn, thời hạn của hợp đồng cung cấp dịch vụ, thông báo về việc gia hạn hay chấm dứt hợp đồng, những phụ phí và luật hiện hành.

8. Biết cách xử lý các khiếu nại

Vấn đề khiếu nại rất quan trọng. Nếu ai đó phàn nàn rằng Site bạn gửi đi bom thư hay chứa tranh ảnh khiêu dâm (bất kể tính hiệu lực của lời khiếu nại), nhiều nhà cung cấp dịch vụ sẽ khước từ bạn. Hãy tìm xem chỗ dựa của bạn là gì? Nếu trong bản hợp đồng có những điều khoản không thể chấp nhận được và nhà cung

cấp dịch vụ không muốn thay đổi chúng, hãy tìm nhà cung cấp khác. Nhớ rằng hợp đồng được lập ra là để bảo vệ cả hai bên và đảm bảo lợi ích của bạn được nêu ra đầy đủ.

9. Kiểm tra các tham chiếu

Trước khi bạn gửi gắm site quý giá của mình cho một nhà cung cấp host, hãy hỏi tên các nhà làm Web hiện đang điều hrnh các site như site của bạn. Gọi điện hay gửi E-mail cho họ, nhưng bằng mọi cách phải nhận được sự phản hồi. Hãy lướt qua các site của họ. Ghi lại những khoảng thời gian đáp ứng vào giờ cao điểm hay giờ rỗi . Phải đảm bảo rằng là có thể chấp nhận được dịch vụ của họ.

10. Hãy tò mò một chút

Sử dụng những công cụ dựa trên Web để biết bạn đang giao dịch với ai? Tra cơ sở dữ liệu Whois (http://www.whois.net/ , www.pavietnam.com/index.php?parm=whois) để tìm xem ai sở hữu site đó. Ghi lại địa chỉ giao dịch. Chạy ứng dụng Traceroute (có sẵn trên phần lớn các site được tải xuống) để xem đường dẫn đến các máy đã liệt kê trong tìm kiếm Whois. Nếu Traceroute tìm thấy site đó thông qua server của LSP khác trong cùng một domain thì có thể bạn đang giao dịch với người bán lại chứ không phải là một nhà cung cấp host thực sự. Chẳng hạn CIHost, một nhà cung cấp host có năng lực tự quảng cáo, dường nư đang cung cấp dịch vụ truy cập mạng cho Propagation.net trong khi dùng dịch vụ của tập đoàn khổng lồ BBN Planet.

Khi sử dụng cơ sở dữ liệu Whois, hãy xem xét kỹ máy trên cái dưới cùng một bậc. Nhập những tên mà bạn tìm thấy vào công cụ tìm kiếm Deja.com. Chúng tôi thấy rằng mạng Propagation.net được kết nối với những site có bom thư và CIHost đã đưa ra những lời chỉ trích trên nhóm tin alt.www.webmaster . Hãy so sánh việc này với công cụ truy nguyên Verio.net.

11 . Bỏ qua những hiệp hội chuyên nghiệp

Và cũng nên bỏ qua phần lớn ý kiến của các site xếp hạng. Bởi vì thành viên của Hội cung cấp host (Web Hosting Guild) bao gồm các công ty có danh tiếng nhưng có một số trong đó nói chung không được giới Webmaster đánh giá cao. Các site xếp hạng thường tổng hợp các lần trước đây được xếp hạng ưu bởi các webmaster là những người sau đó rời bỏ host thường vì những lý do tiêu cực.

12. Hãy đọc những gì mà webmaster nói

Hãy xem nhóm tin alt.www.webmaster , vww.hostinvestigater.com , www.scriptkeeper.com/cgi-bin/ultimate.cgi và http://www.hostcompare.com/ . Điều đó có thể mất một thời gian để "tiêu hoá" tất cả mọi ý kiến và đề xuất nhưng kết quả thu được cũng xứng đáng.

13. Biết rõ thính giả của bạn

Càng biết rõ thính giả tiềm năng của bạn, bạn càng có khả năng ước tính chuẩn xác các chi phí và lập ra một biểu giá thích hợp. Nếu bạn đã làm chủ một site hãy nghiên cứu các tệp truy cập và các công cụ phân tích lưu thông của bạn để biết cần bao nhiêu băng tần và bao nhiêu tài nguyên Server, từ đó lựa chọn một cách tương ứng khi bạn chuyển sang nhà cung cấp host. Nếu bạn lần đầu điều hành một Website hãy sử dụng khoảng thời gian thử nghiệm để làm như vậy rồi đưa ra những sửa đổi cần thiết trong bản kế hoạch của mình trước khi thời hạn lấy lại tiền kết thúc.

14. Chọn một kế hoạch phù hợp với bạn

Những tính toán chi phí không kỹ lưỡng có thể đặt ra những gánh nặng tài chính không thể lường trước lên site của bạn. Một số nhà cung cấp host hướng kế hoạch của mình về phía nhiều site nhỏ, trong khi số khác hướng tới ít site có dung tích lớn hơn. Phí hàng tháng tương ứng với số lượng byte giới hạn, và khoản phụ trội có thể sẽ rất ấn tượng. Một chút thành công đôi khi là kẻ thù nguy hiểm nhất đối với các site nhỏ, bởi vẻ thu nhập của các site chuyên quảng cáo thường tăng không tương ứng, trừ khi các nhà quảng cáo trên site bạn trả chí phí theo số lượng lần truy cập ngược lại, việc tăng nhiều số lần truy cập tới site thương mại điện tử có thể đồng nghĩa với nhiều đơn đặt hàng hơn hoặc thu hút được sự quan tâm lớn đến sản phẩm mới. Một trong hai trường hợp trẹn doanh thu cũng sẽ tăng tương ứng.

15. Thận trọng trước khi cam kết

Giá chào thường tính theo hàng tháng, còn hoá đơn thanh toán thực tế lại mang tới những khoản phụ trội lớn hơn. Nhưng để nhận ra được điều này thường phải có sự liên lạc giữa các chủ thể, không phải chỉ bằng việc vào xem site đó. Chúng tôi cho rằng sẽ hợp lý khi bắt đầu bằng một dịch vụ ngắn hạn có lẽ là 90 ngày để chắc chắn rằng mọi việc diễn ra như bạn đã định. Khi bạn thấy hŕi lòng, hãy gia hạn để có giảm giá.

16. Hãy xem hoá đơn

Chúng tôi đăng ký 30 ngày dùng thử 9NetAve và lập tức bị lập hoá đơn cho một năm dịch vụ. Khi chúng tôi khiếu nại, công ty đã đề nghị xin cắt giảm thời hạn tính phí xuống còn 6 tháng, sau đó là 3 tháng. Đáp lại,

chúng tôi đòi lấy lại tiền. Phải mất thêm một cú điện thoại nữa mới nhận được tiền và chúng tôi đã quyết định không tham khảo nhà cung cấp host đó nữa.

17. Lập chiến lược rút lui

Cho dù các dự định có hoàn hảo đi chăng nữa thẻ mối quan hệ đôi khi vẫn trục trặc. Hoặc bạn có ý định rời bỏ nhà cung cấp host của mình với vô số lý do. Có một số người rất đúng mức mà chúng tôi biết đã trở thành những khách hàng khủng khiếp đối với nhà cung cấp host của họ, và một số nhà cung cấp host đắt hàng cũng đã trở chứng thành những phòng khủng bố khách hàng của họ.

18. Lưu trữ tất cả mọi thứ

Dĩ nhiên các trang HTML của bạn đang được lưu trữ vẽ bạn tạo ra chúng trên máy của mình và tải chúng lên site của nhà cung cấp host. Hãy nghĩ đến tất cả các file khác hiện đặt trẹn Server của bạn: những bản ghi truy cập người sử dụng, cơ sở dữ liệu sản phẩm, đơn đặt híng của khách, CSDL tranh luận, script của Servel; phần mềm thương mại như thương mại điện từ ví các gói diễn đírn thảo luận, phần mềm phân tích lưu thông, và tất cả những thứ mà bạn tải lên site của nhà cung cấp host hay dịch vụ này tải xuống cho bạn.

19. Giảm nhẹ sự chuyển đổi site của bạn

Nếu bạn nhận thấy rằng site bạn phát triển nhanh hơn cả nhà cung cấp host, thì họ cũng nhận thấy điều đó và sẽ làm việc với nhà cung cấp host mới để chuyển site của bạn với sự phiền nhiễu và hỏng hóc tối thiểu. Đa số sự chia tay là tốt đẹp. Nhưng khi không phải vậy, thẻ hãy chuẩn bị sẵn bản sao của tất cả những thứ mà bạn có thể nghĩ đến.

20. Sở hữu một tên miền của riêng bạn

Thậm chí ngay cả khi bạn không có ý định từ bỏ nhà cung cấp host của mình thì bạn cũng phải chắc chắn rằng mình có một tên miền riêng. Nếu nhà cung cấp host đã đăng ký tẹn miền cho bạn, hãy tra Whois để biết chắc rằng bạn hay người trong công ty bạn là người đăng ký và liên lạc hành chính cho site của bạn. Nếu nhà cung cấp host được niệm yết là đầu mối kỹ thuật và quản lý thì nó sẽ sở hữu tên miền chứ không phải là bạn và bạn có thể sẽ phải bỏ tiền để mua tên đó. Hãy làm như vậy từ khi nhà cung cấp host không có điều gì giận bạn, nếu không tên miền của bạn có thể sẽ bị giữ để đòi tiền chuộc.

21 . Hãy giúp các vị khách tìm trang chủ mới của bạn

Có lẽ lý do lớn nhất để rời khỏi nhí cung cấp host theo các điều kiện rộng rãi là sao cho site cũ của bạn chỉ tới site mới trong một khoảng thời gian nào đó. Người sử dụng hay khách hàng của bạn có thể sẽ đánh dấu địa chỉ theo tên chứ không phải địa chỉ IP của site hay các trang mà họ sử dụng. Nhưng có thể phải mất vài ngày, thậm chí một tuần để địa chỉ IP mới được truyền bá suốt các Server tên miền của Internet. Và nếu vì một lý do nào đó người sử dụng được hướng tới địa chỉ IP cũ thẻ nên có những chỉ dẫn tới site mới và hướng dẫn cách cập nhật các book- mark. Đừng quên gửi e-mail cho khách hàng và đưa thông tin lên trang của bạn để báo cho họ về sự thay đổi có thể xảy ra.

Dịch vụ cung cấp host vẫn còn là một ngành kinh doanh mới mẻ, một ngành kinh doanh đang tiếp tục tái tạo ra chính nó. Bạn sẽ phải chuẩn bị cho sự thay đổi liên tục, sự cải thiện lớn hơn và biến đổi đột phá có tính cơ hội về dịch vụ, hiệu quả giá cả hay hiệu năng. Đừng có dao động mà hãy tiếp tục đánh giá dịch vụ bạn đang có ví những gì bạn đang phải bỏ tiền để mua.

22. Hãy lưu trữ các thông tin bí mật của bạn trong host free

Bạn đừng quá tin tưởng rằng server hay host mình mua luôn luôn bảo mật cao hơn các host free. Đó là một ý nghĩ sai lầm! Hầu hết các hosting ở VN bị các hacker "qua mặt" một các dễ dàng bằng nhiều các và cách thường dùng là hack local. Khi bạn giữ các thông tin bí mật của mình trong host riêng thì tình trạng bị hack cao hơn là khi bạn giữ các thông tin bí mật ở host free. Vì các host free luôn luôn bảo mật tốt và không có hacker nào đủ siêng năng để hack hết toàn bộ các user và hắn cũng chẳng biết được user nào của mình. Khi chọn host free thì hãy chọn các host ở nước ngoài vì khi ấy host ở nước ngoài bảo mật cao hơn nhiều so với host ở VN. Chẳng hạn host ở t35 hầu như chưa bị hack dù là một host free còn host của www.dangquang.com đã từng bị hack local ở khu vực host free!

23. Hãy cẩn thận với cả những người quen

Bạn đừng quá tin tưởng với những người quen mà giao pass host hay bất cứ thông tin gì về nó. Chẳng hạn HVA từng bị một moderator của VHF chơi "lén" bằng cách cài keylog vào máy của admin HVA khi anh chàng HVA mời người bạn VHF về nhà chơi.

24. Hãy lưu ý đến các chương trình upload

Đừng nên upload những thông tin quan trọng lên host chính của mình ở DV, vì ở DV bạn có thể "được" chương trình upload lưu lại mật khẩu v.v... hay ai đó dùng chương trình tìm lại mật khẩu thì sao? Nếu muốn upload ngoài DV thì nên sau khi up xong hãy Uninstall chương trình upload đó.

IV. Loại bỏ các ký tự đặc biệt:

Loại bỏ các kí tự đặc biệt như ../, |, &, ... là điều làm đau đầu những người mới bắt đầu vào nghề viết ứng dụng web nhằm ngăn chặn tấn công phê chuẩn đầu vào của hacker. Trong Perl, =~s chưa chắc đã lọc được hết các kí tự này bởi bạn có thể bị hacker chưa khâm. Một ví dụ khá điển hình là trường hợp của fileseek.cgi đã được thông báo trên bugtraq trước đây. Fileseek.cgi cố gắng lọc bỏ tất cả các kí tự '../' nhưng nó sẽ thất bại nếu hacker dùng '....//'. Fileseek.cgi làm việc như một cái máy, nó loại bỏ '../' trong '....//', kết quả trả về là '../' và hacker sẽ ung dung làm thêm vài cái '....//' để leo lên thư mục root '....//....//....//....//....//' sau đó cat file /etc/passwd.

Một cách đơn giản để loại bỏ các kí tự đặc biệt là bạn chỉ chấp nhận các kí tự thường, không cần quan tâm đến các kí tự đặc biệt.

```
#!/usr/local/bin/perl
$_ = $user_data = $ENV{'QUERY_STRING'}; # nhận dữ liệu từ phía người dùng
print "$user_data\n";
$OK_CHARS='-a-zA-Z0-9_.@'; # tập kí tự được cho phép

s/[^$OK_CHARS]/_/go; # gỡ bỏ các kí tự không nằm trong tập kí tự trên
$user_data = $_;
print "$user_data\n";
exit(0)
```

Rất đơn giản như vô cùng hiệu quả, chúng ta không cần phải quan tâm đến các kí tự ../, |, ...

* Bạn tham khảo thêm Perl CGI problems (phrack 55/9 - http://www.phrack.org/) để biết rõ về các lỗi liên quan đến các script viết bằng Perl/CGI.

V. Bảo vệ file và thư mục:

Việc bảo mật tuyệt đối một thư mục hoặc một tệp là một nhu cầu bức thiết của nhiều người dùng máy tính, đặc biệt với những người dùng chung một máy tính. Mặc dù trong hệ điều hành DOS, trong hệ điều hành Windows và đặc biệt là trong hệ điều hành mạng đã có những thủ tục cài đặt mật khẩu, cài đặt thuộc tính ẩn (H), thuộc tính chỉ đọc (R) vv... Nhưng đó chỉ là những bảo mật cục bộ và mức bảo mật không cao. Các thư mục hoặc các tệp bảo mật được ở chỗ này nhưng không bảo mật được ở chỗ khác. Có các thư mục và tệp được Windows bảo vệ chống xoá nhưng lại xoá được dễ dàng trong DOS...
Vậy có cách nào bảo mật được thư mục một cách tuyệt đối không ? Có. Bạn phải tự làm lấy vì chưa có một chương trình nào giúp bạn làm điều này. Phương án để bảo mật tuyệt đối một thư mục mà chúng tôi đã lựa chọn và dùng rất có hiệu quả là đánh lạc hướng địa chỉ lưu trú của thư mục trên đĩa, làm cô lập các cluster mà thư mục đã chiếm giữ, do đó không thể can thiệp được vào thư mục này bằng bất kì cách nào. Vậy làm thế nào để đánh lạc hướng địa chỉ lưu trú thật của thư mục ?.

Để làm được điều này bạn cần biết rằng FAT là một bảng định vị file (File Allocation Table). Bảng này gồm nhiều phần tử. Đĩa có bao nhiêu cluster thì FAT cũng có bấy nhiêu phần tử (Cluster là một liên cung gồm nhiều sector nhóm lại). Phần tử thứ n của FAT tương ứng với cluster thứ n trên đĩa. Một file chiếm bao nhiêu cluster trên đĩa thì đề mục FAT của nó cũng có bấy nhiêu phần tử. Phần tử FAT này chứa số thứ tự của một phần tử FAT khác. Phần tử chứa FF FF là mã kết thúc file <EOF>. Như vậy một đề mục FAT của một File sẽ chứa số thứ tự của các cluster mà file chiếm giữ. Đề mục FAT của một thư mục chỉ có một phần tử chứa mã <EOF>. Số thứ tự của phần tử này ứng với số thứ tự của cluster chứa đề mục của các thư mục con và của các

tệp có trong thư mục đó. Mỗi phần tử FAT chiếm 2 bytes với FAT 16 bit và chiếm 4 bytes với FAT 32 bit.

Mỗi đề mục của thư mục hoặc của tệp trong bảng thư mục gốc (Root Directory) đều chiếm 32 bytes, phân thành 8 trường như sau: Trường 1 chứa 8 byte tên chính, trường 2 chứa 3 byte phần tên mở rộng, trường 3 là 1 byte thuộc tính, trường 4 chiếm 10 byte (DOS không dùng và dành riêng cho Windows), trường 5 chiếm 2 byte về ngày tháng tạo lập, trường 6 chiếm 2 byte về giờ phút giây tạo lập, trường 7 gọi là trường Cluster chiếm 2 byte chứa số thứ tự của phần tử FAT đầu tiên của mỗi đề mục FAT, trường 8 chiếm 4 byte về dung lượng.

Khi truy cập một thư mục hay một tệp, trước tiên máy đọc 8 trường nói trên trong bảng thư mục, sau đó nhờ đọc được thông tin ở trường cluster mà máy chuyển đến đọc cluster đầu tiên của tệp đồng thời chuyển đến đọc phần tử FAT đầu tiên của đề mục FAT rồi đọc tiếp các phần tử FAT khác trong đề mục để biết số thứ tự của các cluster tiếp theo và truy cập tiếp các cluster này cho đến khi gặp mã FF FF đó là mã kết thúc file <EOF> trong đề mục FAT thì dừng.

Như vậy muốn bảo mật thư mục hoặc tệp nào đó ta phải thay đổi nội dung của trường thứ 7 trong đề mục ROOT để nó không trỏ vào địa chỉ thật của thư mục hoặc của tệp mà trỏ vào một phần tử rỗng nằm ở cuối của FAT (khi đĩa chưa đầy thì phần tử này bao giờ cũng rỗng, tương ứng với cluster rỗng trên đĩa). Đồng thời để trình SCANDISK không phát hiện ra sự thất lạc cluster ta cần phải ghi vào phần tử FAT cuối cùng này giá trị thật của cluster mà thư mục chiếm giữ.

Các thao tác cần thiết để bảo mật thư mục như sau :

1 - Tạo một thư mục BAOMAT ở thư mục gốc và chép tất cả các tệp cần bảo mật vào đó.

2 - Đọc số thứ tự của phần tử FAT cuối cùng (cũng là số thứ tự của cluster có nghĩa cuối cùng của đĩa):

Chạy chương trình Diskedit trong thư mục NC sau đó gõ ALT+C để làm hiện ra cửa sổ Select Cluster Range. Giả sử trong cửa sổ này bạn nhận được thông tin Valid Cluster numbers are 2 through 33,196. điều này có nghĩa là số thứ tự của Cluster có nghiã cuối cùng của đĩa là 33.196, đó cũng là số thứ tự của phần tử có nghĩa cuối cùng của FAT. Đọc xong thì gõ ESC .

3 - Tìm đề mục của thư mục cần bảo mật trong bảng Root Directory để ghi giá trị vừa đọc được ở bước 2 vào trường Cluster của đề mục ấy như sau:

Chạy Diskedit và gõ ALT+R, dịch con trỏ lên thư mục gốc và ấn Enter để mở bảng thư mục gốc. Rà bảng thư mục từ trên xuống và dừng lại ở đề mục cần bảo mật. Dịch chuyển con trỏ tới cột Cluster của đề mục này, ghi lại giá trị cũ vào giấy và nhập vào đó giá trị mới (với ví dụ trên là 33196). Nhập xong thì dịch con trỏ xuống dưới rồi gõ CTRL+W, chọn nút Write trong cửa sổ Write changes để ghi vào đĩa.

4 - Ghi giá trị cũ đã ghi nhớ trên giấy vào phần tử cuối của FAT bằng cách chạy chương trình Diskedit, gõ ALT+S làm hiện lên cửa sổ Select Sector Range, với mục Sector Usage bạn sẽ nhìn thấy vùng FAT 1 và vùng FAT 2 chiếm từ sector nào đến sector nào. Chẳng hạn bạn được thông tin sau: 1-130 1st FAT area, 131-260 2nd FAT area, có nghĩa là phần tử cuối cùng của FAT 1 nằm ở sector 130 và của FAT 2 là sector 260. Bạn hãy gõ vào hộp Starting Sector:[...] số thứ tự của Sector cuối cùng của FAT 1 (với ví dụ trên là 130) và ấn Enter để mở cửa sổ Disk Editor, dịch chuyển con trỏ đến cluster cuối cùng có nghiã của FAT 1 (vừa dịch con trỏ vừa quan sát chỉ thị số cluster ở thanh trạng thái và dừng lại ở cluster có nghĩa cuối cùng với ví dụ trên là 33196). Nhập vào đó giá trị đã ghi nhớ trên giấy ở bước 3 . Cuối cùng gõ Ctrl+W, đánh dấu vào mục Synchronize FATs và chọn Write để ghi vào 2 FAT của đĩa.

Chú ý:

* Khi cần truy cập thư mục này bạn chỉ cần nạp lại giá trị cũ cho trường Cluster của đề mục Root mà không cần xoá bỏ giá trị đã ghi ở cuối FAT.

* Vì hệ điều hành Windows có chế độ bảo vệ vùng đĩa hệ thống nên muốn thực hiện các thao tác trên bạn phải khởi động máy ở hệ điều hành DOS.

* Cần bỏ chế độ bảo mật này trước khi thực hiện chống phân mảnh (Defrag).

VI. An toàn hệ thống:

Bước 1: Thành lập bộ phận chuyên trách về vấn đề bảo mật

Bất kỳ kế hoạch bảo mật nào cũng cần sự hỗ trợ trên nhiều phương diện khác nhau, nếu nó muốn thành công. Một trong những phương thức tốt nhất để có thể được sự hỗ trợ là nên thiết lập một bộ phận chuyên trách về vấn đề bảo mật. Bộ phận này sẽ chịu trách nhiệm trước công ty về các công việc bảo mật.

Mục đích trước tiên của bộ phận này là gây dựng uy tín với khách hàng. Hoạt động của bộ phận này sẽ khiến cho khách hàng cảm thấy yên tâm hơn khi làm việc hoặc sử dụng các dịch vụ của công ty. Bộ phận này có trách nhiệm thường xuyên cung cấp các lưu ý, cảnh báo liên quan đến an toàn bảo mật thông tin nhằm tránh các rủi ro đáng tiếc cho khách hàng và công ty.
Bộ phận này còn có trách nhiệm tìm hiểu, đưa ra giải pháp, cơ chế bảo mật cho toàn công ty. Sẽ là hiệu quả và xác thực hơn khi công việc này được thực hiện bởi chính đội ngũ trong công ty thay vì đi thuê một công ty bảo mật khác thực hiện.

Cuối cùng, một bộ phận chuyên trách về vấn đề bảo mật có thể thay đổi cách làm, cách thực hiện công việc kinh doanh của công ty để tăng tính bảo mật trong khi cũng cải tiến được sức sản xuất, chất lượng, hiệu quả và tạo ra sức cạnh tranh của công ty. Ví dụ, chúng ta hãy nói đến VPN (Virtual Private Network), đây là một công nghệ cho phép các nhân viên đảm bảo an toàn khi đọc email, làm việc với các tài liệu tại nhà, hay chia sẻ công việc giữa hai nhân viên hay hai phòng ban.

Bước 2: Thu thập thông tin

Trước khi đưa ra các thông báo mô tả thực hiện bảo mật, bạn phải lường được mọi tình huống sẽ xảy ra, không chỉ bao gồm toàn bộ các thiết bị và hệ thống đi kèm trong việc thực hiện bảo mật mà còn phải kế đến cả các tiền trình xử lý, các cảnh bảo bảo mật, sự thẩm định hay các thông tin cần được bảo vệ. Điều này rất quan trọng khi cung cấp một cái nhìn bao quát về hệ thống bảo mật của công ty. Sự chuẩn bị này cũng nên tham chiếu tới các chính sách bảo mật cũng như các hướng dẫn thực hiện của công ty trong vấn đề an toàn bảo mật. Phải lường trước được những gì xảy ra trong từng bước tiến hành của các dự án.

Để kiểm tra mức độ yếu kém của hệ thống, hãy bắt đầu với những vấn đề có thể dẫn tới độ rủi ro cao nhất trong hệ thống mạng của bạn, như Internet. Hãy sử dụng cơ chế bảo mật bên ngoài từ sản phẩm của một hãng có danh tiếng, có thể cung cấp thông tin cần thiết để ước lượng mức bảo mật hiện tại của công ty bạn khi bị tấn công từ Internet. Sự thẩm định này không chỉ bao gồm việc kiểm tra các lỗ hổng, mà còn gồm cả các phân tích từ người sử dụng, hệ thống được kết nối bằng VPN, mạng và các phân tích về thông tin công cộng sẵn có.

Một trong những cân nhắc mang tính quan trọng là thẩm định từ bên ngoài vào. Đây chính là điểm mấu chốt trong việc đánh giá hệ thống mạng. Điển hình, một công ty sử dụng cơ chế bảo mật bên ngoài, cung cấp các dịch vụ email, Web theo cơ chế đó, thì họ nhận ra rằng, không phải toàn bộ các tấn công đều đến từ Internet. Việc cung cấp lớp bảo mật theo account, mạng bảo vệ bản thân họ từ chính những người sử dụng

VPN và các đồng nghiệp, và tạo ra các mạng riêng rẽ từ các cổng truy cập đầu cuối là toàn bộ các ưu thế của cơ chế này.

Cơ chế bảo mật bên trong cũng giúp việc quản lý bảo mật công ty được tốt hơn. Bằng cách kiểm tra toàn bộ công việc kinh doanh, các cơ chế chính sách, các quá trình xử lý, xác thực dữ liệu tương phản với những gì được mô tả, hay sự tương thích với những chuẩn đã tồn tại được thẩm định. Cơ chế bảo mật bên trong cung cấp thông tin một cách chi tiết tương tự như việc khảo sát kỹ lưỡng phạm vi ở mức sâu hơn, thậm chí bao gồm cả việc phá mã mật khẩu và các công cụ phân tích hệ thống để kiểm tra tính tương thích về chính sách trong tương lai.

Bước 3: Thẩm định tính rủi ro của hệ thống

Khi thẩm định tính rủi ro của hệ thống, hãy sử dụng công thức sau:

Tính rủi ro = Giá trị thông tin * Mức độ của lỗ hổng * Khả năng mất thông tin

Tính rủi ro bằng với giá trị thông tin trong câu hỏi (bao gồm giá trị đồng tiền, giá trị thời gian máy bị lỗi do lỗi bảo mật, giá trị mất mát khách hàng – tương đối), thời gian của quy mô lỗ hổng (tổng cộng/từng phần của tổn thất dữ liệu, thời gian hệ thống ngừng hoạt động, sự nguy hiểm khi dữ liệu hỏng), thời gian về khả năng xuất hiện mất thông tin.
Để lấy được các kết quả từ bước đầu (các giá trị, báo cáo về cơ chế bảo mật ngoài, và chính sách bảo mật), và tập trung vào 3 trong số các mặt thường được đề cập. Sau đó, bắt đầu với một số câu hỏi khung sau:
*Cơ chế bảo mật đã tồn tại của công ty có được đề ra rõ ràng và cung cấp đủ biện pháp bảo mật chưa?
*Kết quả từ cơ chế bảo mật bên ngoài có hợp lệ so với chính sách bảo mật của công ty?
*Có mục nào cần sửa lại trong cơ chế bảo mật mà không được chỉ rõ trong chính sách?
*Hệ thống bảo mật sẽ mất tác dụng trong tính rủi ro cao nhất nào?
*Giá trị, thông tin gì mang tính rủi ro cao nhất?
Các câu trả lời cung cấp cái nhìn toàn diện cho việc phân tích về toàn bộ chính sách bảo mật của công ty. Có lẽ, thông tin quan trọng được lấy trong quá trình kết hợp các giá trị thẩm định và tính rủi ro tương ứng. Theo giá trị thông tin, bạn có thể tìm thấy các giải pháp mô tả được toàn bộ các yêu cầu, bạn có thể tạo ra một danh sách quan tâm về lỗ hổng bảo mật.

Bước 4: Xây dựng giải pháp

Trên thực tế không tồn tại giải pháp an toàn, bảo mật thông tin dang Plug and Play cho các tổ chức đặc biệt khi phải đảm bảo các luật thương mại đã tồn tại và phải tương thích với các ứng dụng, dữ liệu sẵn có. Không có một tài liệu nào có thể lượng hết được mọi lỗ hổng trong hệ thống và cũng không có nhà sản xuất nào có thể cung cấp đủ các công cụ cần thiết. Cách tốt nhất vẫn là sử dụng kết hợp các giải pháp, sản phẩm nhằm tạo ra cơ chế bảo mật đa năng.

Firewall

Xem xét và lựa chọn một sản phẩm firewall hợp lý và đưa và hoạt động phù hợp với chính sách của công ty là một trong những việc đầu tiên trong quá trình bảo mật hệ thống. Firewall có thể là giải pháp phần cứng hoặc phần mềm hoặc kết hợp cả hai. Nhiệm vụ của firewall là ngăn chặn các tấn công trực tiếp vào các thông tin quan trọng của hệ thống, kiểm soát các thông tin ra vào hệ thống. Việc lựa chọn firewall thích hợp cho một hệ thống không phải là dễ dàng. Các firewall đều phụ thuộc trên một môi trường, cấu hình mạng, ứng dụng cụ thể. Khi xem xét lựa chọn một firewall, cần tập trung tìm hiểu tập các chức năng của firewall, tính năng lọc địa chỉ, gói tin, ...

Hệ thống kiểm tra xâm nhập mạng (IDS)

Một firewall được gọi là tốt chỉ khi nó có thể lọc và tạo khả năng kiểm soát các gói tin khi đi qua nó. Và đây cũng chính là nơi mà hệ thống IDS nhập cuộc. Nếu bạn xem firewall như một con đập ngăn nước, thì thì bạn có thể ví IDS như một hệ thống điều khiển luồng nước trên các hệ thống xả nước khác nhau. Một IDS, không liên quan tới các công việc điều khiển hướng đi của các gói tin, mà nó chỉ có nhiệm vụ phân tích các

gói tin mà firewall cho phép đi qua, tìm kiếm các chữ kí tấn công đã biết (các chữ kí tấn công chính là các đoạn mã được biết mang tính nguy hiểm cho hệ thống) mà không thể kiểm tra hay ngăn chặn bởi firewall. IDS tương ứng với việc bảo vệ đằng sau của firewall, cung cấp việc chứng thực thông tin cần thiết để đảm bảo chắc chắn cho firewall hoạt động hiệu quả.

Hệ thống kiểm tra xâm phạm dựa theo vùng (H-IDS)

Sự lựa chọn, thực hiện và sử dụng một hệ thống kiểm tra sự xâm phạm trên máy chủ dựa trên nhiều hệ điều hành và môi trường ứng dụng chỉ định. Một hàm chức năng đầy đủ của H-IDS có thể cung cấp các thông báo đều đặn theo thời gian của bất kỳ sự thay đổi nào tới máy chủ từ tác động bên trong hay bên ngoài. Nó là một trong những cách tốt nhất để giảm thiểu sự tổn thương của hệ thống. Việc tìm kiếm hệ thống mà hỗ trợ hầu hết các hệ điều hành sử dụng trong tổ chức của bạn nên được xem như một trong những quyết định chính cho mỗi H-IDS.

Hệ thống kiểm tra xâm phạm dựa theo ứng dụng (App-IDS)

Số lượng App-IDS xuất hiện trên thị trường ngày càng nhiều. Các công cụ này thực hiện việc phân tích các thông điệp từ một ứng dụng cụ thể hay thông tin qua proxy tới ứng dụng đó. Trong lúc chúng có mục đích cụ thể, chúng có thể cung cấp mức bảo mật tăng lên theo từng mảng ứng dụng cụ thể. Khi được kết hợp với một H-IDS, chúng đảm bảo rằng sự xâm nhập tới một máy chủ sẽ giảm thiểu. Một App-IDS nên được xem như một chức năng hỗ trợ bảo mật trong suốt, mặc dù không đúng trong một số trường hợp.

Phần mềm Anti-Virus (AV)

Phần mềm AV nên được cài trên toàn bộ máy trạm (workstation), máy chủ (server), hệ thống hỗ trợ dịch vụ số, và hầu hết những nơi chứa dữ liệu quan trọng vào ra. Hai vấn đề quan trọng nhất để xem xét khi đặt yêu cầu một nhà sản xuất AV quản lý nhiều máy chủ và máy trạm trên toàn bộ phạm vi của công ty là khả năng nhà cung cấp đó có đối phó được các đe doạ từ virus mới hay không. (nguyên nhân: không bao giờ cho rằng phầm mềm đang chạy, luôn kiểm tả phiên bản của virus và các file cập nhật cho virus mới).

Mạng riêng ảo (VPN)

Việc sử dụng VPN để cung cấp cho các nhân viên hay các cộng sự truy cập tới các tài nguyên của công ty từ nhà hay nơi làm việc khác với mức bảo mật cao, hiệu quả nhất trong quá trình truyền thông, và làm tăng hiệu quả sản xuất của nhân viên. Tuy nhiên, không có điều gì không đi kèm sự rủi ro. Bất kỳ tại thời điểm nào khi một VPN được thiết lập, bạn phải mở rộng phạm vi kiểm soát bảo mật của công ty tới toàn bộ các nút được kết nối với VPN.

Để đảm bảo mức bảo mật cho hệ thống này, người sử dụng phải thực hiện đầy đủ các chính sách bảo mật của công ty. Điều này có thể thực hiện được qua việc sử dụng các hướng dẫn của nhà sản xuất về dịch vụ VPN như hạn chế các ứng dụng có thể chạy ở nhà, cổng mạng có thể mở, loại bỏ khả năng chia kênh dữ liệu, thiết lập hệ thống bảo vệ virus khi chạy hệ thống từ xa, tất cả công việc này giúp giảm thiểu tính rủi ro. Điều này rất quan trọng đối với các công ty phải đối mặt với những đe doạ trong việc kiện cáo, mạng của họ hay hệ thống được sử dụng để tấn công các công ty khác.

Sinh trắc học trong bảo mật

Sinh trắc học đã được biết đến từ một số năm trước đây, nhưng cho đến nay vẫn có rất nhiều khó khăn cho việc nhân rộng để áp dụng cho các hệ thống bảo mật thương mại. Dấu tay, tròng mắt, giọng nói, ..., cung cấp bảo mật mức cao trên các mật khẩu thông thường hay chứng thực hai nhân tố, nhưng cho đến hiện tại, chúng cũng vẫn được coi như phương thức tốt nhất để truy cập vào hệ thống.

Các thế hệ thẻ thông minh

Các công ty gần đây sử dụng đã sử dụng thẻ thông minh như một phương thức bảo mật hữu hiệu. Windows 2000 cung cấp cơ chế hỗ trợ thẻ thông minh như một phương tiện chính trong việc chứng thực quyền đăng nhập hệ thống. Nói chung, sự kết hợp đa công nghệ (như tròng mắt, thẻ thông minh, dấu tay) đang dần hoàn thiện và mở ra một thời đại mới cho việc chứng thực quyền truy cập trong hệ thống bảo mật.

Kiểm tra máy chủ

Sự kiểm tra đều đặn mức bảo mật được cung cấp bởi các máy chủ phụ thuộc chủ yếu vào sự quản lý. Mọi máy chủ ở trong một công ty nên được kiểm tra từ Internet để phát hiện lỗ hổng bảo mật. Thêm nữa, việc kiểm tra từ bên trong và quá trình thẩm định máy chủ về căn bản là cần thiết để giảm thiểu tính rủi ro của hệ thống, như khi firewall bị lỗi hay một máy chủ, hệ thống nào đó bị trục trặc.
Hầu hết các hệ điều hành đều chạy trong tình trạng thấp hơn với mức bảo mật tối thiểu và có rất nhiều lỗ hổng bảo mật. Trước khi một máy chủ khi đưa vào sản xuất, sẽ có một quá trình kiểm tra theo một số bước nhất định. Toàn bộ các bản sửa lỗi phải được cài đặt trên máy chủ, và bất cứ dịch vụ không cần thiết nào phải được loại bỏ. Điều này làm tránh độ rủi ro xuống mức thấp nhất cho hệ thống.
Việc tiếp theo là kiểm tra các log file từ các máy chủ và các ứng dụng. Chúng sẽ cung cấp cho ta một số thông tin tốt nhất về hệ thống, các tấn công bảo mật. Trong rất nhiều trường hợp, đó chính là một trong những cách để xác nhận quy mô của một tấn công vào máy chủ.

Kiểm soát ứng dụng

Vấn đề an toàn bảo mật trong mã nguồn của các ứng dụng hầu hết không được quan tâm. Điều này không được thể hiện trên các sản phẩm như liệu nó có được mua, được download miễn phí hay được phát triển từ một mã nguồn nào đó. Để giúp đỡ giảm thiểu sự rủi ro bảo mật trong các ứng dụng, thẩm định lại giá trị của ứng dụng trong công ty, như công việc phát triển bên trong của các ứng dụng, Điều này cũng có thể bao gồm các đánh giá của các thực thể bên ngoài như đồng nghiệp hay các khách hàng.

Việc điều khiển cấu hình bảo mật các ứng dụng có thể làm tăng mức bảo mật. Hầu hết các ứng dụng được cấu hình tại mức tối thiểu của tính năng bảo mật, nhưng qua các công cụ cấu hình, mức bảo mật của hệ thống có thể được tăng lên. Lượng thông tin kiểm soát được cung cấp bởi ứng dụng cũng có thể được cấu hình. Nơi mà các ứng dụng cung cấp thông tin về quy mô bảo mật, thời gian kiểm soát và sự phân tích thông tin này sẽ là chìa khoá để kiểm tra các vấn đề bảo mật thông tin.

Các hệ điều hành

Sự lựa chọn hệ điều hành và ứng dụng là quá trình đòi hỏi phải có sự cân nhắc kỹ càng. Chọn cái gì giữa hệ điều hành Microsoft hay UNIX, trong rất nhiều trường hợp, điều thường do ấn tượng cá nhân ề sản phẩm. Khi lựa chọn một hệ điều hành, thông tin về nhà sản xuất không quan trọng bằng những gì nhà sản xuất đó làm được trong thực tế, về khả năng bảo trì hay dễ dàng thực hiện với các tài liệu đi kèm. Bất kỳ một hệ điều hành nào từ 2 năm trước đây đều không thể đảm bảo theo những chuẩn ngày nay, và việc giữ các máy chủ, ứng dụng của bạn được cập nhật thường xuyên sẽ đảm bảo giảm thiểu khả năng rủi ro của hệ thống.

Khi lựa chọn một hệ điều hành, hãy tìm hiểu không chỉ các tiêu chuẩn thông thường như (quản trị, hiệu năng, tính chứng thực), mà còn phải xem xét khả năng áp dụng được của hệ điều hành với hệ thống hiện tại. Một hệ điều hành có thể cung cấp cơ chế bảo mật tốt hơn khi nó tương thích với các ứng dụng chạy bên

trong nó như DNS hay WebServer, trong khi các hệ điều hành khác có thể có nhiều chức năng tốt hơn như một hệ thống application, database hay email server.

Bước 5: Thực hiện và giáo dục

Ban đầu, sự hỗ trợ cần thiết sẽ được đúc rút lại và lên kế hoạch hoàn chỉnh cho dự án bảo mật. Đây chính là bước đi quan trọng mang tính chiến lược của mỗi công ty về vấn đề bảo mật. Các chi tiết kỹ thuật của bất kỳ sự mô tả nào cũng sẽ thay đổi theo môi trường, công nghệ, và các kỹ năng liên quan, ngoài ra có một phần không nằm trong việc thực thi bảo mật nhưng chúng ta không được coi nhẹ, đó chính là sự giáo dục. Để đảm bảo sự thành công bảo mật ngay từ lúc đầu, người sử dụng phải có được sự giáo dục cần thiết về chính sách, gồm có:

- Kỹ năng về các hệ thống bảo mật mới, các thủ tục mới.
- Hiểu biết về các chính sách mới về tài sản, dữ liệu quan trọng của công ty.
- Hiểu các thủ tục bắt buộc mới, chính sách bảo mật công ty.

Nói tóm lại, không chỉ đòi hỏi người sử dụng có các kỹ năng cơ bản, mà đòi hỏi học phải biết như tại sao và cái gì họ đang làm là cần thiết với chính sách của công ty.

Bước 6: Tiếp tục kiểm tra, phân tích và thực hiện

Hầu hết những gì mong đợi của một hệ thống bảo mật bất kỳ là chạy ổn định, điều khiển được hệ thống và nắm bắt được các luồng dữ liệu của hệ thống. Quá trình phân tích, tổng hợp các thông tin, sự kiện từ firewall, IDS's, VPN, router, server, và các ứng dụng là cách duy nhất để kiểm tra hiệu quả của một hệ thống bảo mật, và cũng là cách duy nhất để kiểm tra hầu hết sự vi phạm về chính sách cũng như các lỗi thông thường mắc phải với hệ thống.

Các gợi ý bảo mật cho hệ thống và mạng

Theo luận điểm này, chúng tôi tập trung chủ yếu và các bước mang tính hệ thống để cung cấp một hệ thống bảo mật. Từ đây, chúng tôi sẽ chỉ ra một vài bước đi cụ thể để cải thiện hệ thống bảo mật, dựa trên kết quả của việc sử dụng các phương thức bảo mật bên ngoài và bảo mật bên trong của hệ thống. Chúng tôi cũng giới hạn phạm vi của các gợi ý này theo các vấn đề chung nhất mà chúng tôi đã gặp phải, để cung cấp, mô tả vấn đề một cách chính xác hơn cũng như các thách thức mà mạng công ty phải đối mặt ngày nay. Để mang tính chuyên nghiệp hơn về IT, các gợi ý này được chia thành các phần như sau:

Đặc điểm của bảo mật

*Tạo bộ phận chuyên trách bảo mật để xem xét toàn bộ các vấn đề liên quan tới bảo mật
*Thực hiện các thông báo bảo mật tới người sử dụng để đảm bảo mọi người hiểu và thực hiện theo các yêu cầu cũng như sự cần thiết của việc thực hiện các yêu cầu đó.
*Tạo, cập nhật, và theo dõi toàn bộ chính sách bảo mật của công ty.

Windows NT/IIS

* Hầu hết 95% các vấn đề bảo mật của NT/IIS, chúng ta có thể giải quyết theo các bản sửa lỗi. Đảm bảo chắc chắn toàn bộ các máy chủ NT và IIS được sửa lỗi với phiên bản mới nhất.
*Xoá (đừng cài đặt) toàn bộ các script từ Internet.

Cisco Routers

*Loại bỏ các tính năng như finger, telnet, và các dịch vụ, cổng khác trên thiết bị định tuyến (router).
*Bỏ các gói tin tài nguyên IP dẫn đường trong router.
*Chạy Unicast RPF để ngăn chặn người sử dụng của bạn sử dụng việc giả mạo IP.

*Sử dụng router của bạn như một firewall phía trước và thực hiện các ACL tương tự theo các luật trong firewall của bạn.

Quy định chung về cầu hình firewall

*Cấu hình của firewall nên có các luật nghiêm ngặt. Chỉ rõ các luật đối với từng loại truy nhập cả bên ngoài lẫn bên trong.

*Giảm thiểu các truy nhập từ xa tới firewall.

*Cung cấp hệ thống kiểm soát tập luật của firewall.

*Kiểm tra lại các luật.

Cisco PIX Firewalls

*Không cho phép truy cập qua telnet

*Sử dụng AAA cho việc truy cập, điều khiển hệ thống console

Kiểm soát Firewall-1

*Loại bỏ các luật mặc định cho phép mã hoá và quản lý của firewall, thay thế các luật không rõ ràng bằng các luật phân biệt rạch ròi trong công việc thực thi của bạn.

*Không sử dụng mặc định luật "allow DNS traffic" - chấp nhận luật này chỉ cho các máy chủ cung cấp DNS cho bên ngoài.

DNS bên trong

Bất kỳ máy chủ nào cung cấp DNS bên trong và các dịch vụ mang tính chất nội bộ phải không được cung cấp DNS bên ngoài.

Kiểm tra với nhà cung cấp DNS của bạn để cấu hình bảo vệ từ thuộc tính "*cache poisoning*"

VII. Quản trị mạng NT:

Ngày nay, hầu hết các server của VN đều dùng HĐH WindowsNT của Microsoft vì vậy, bài viết này chủ yếu để chia sẻ kinh nghiệm quản trị mạng WindowsNT của tôi cho một số nhà quản lý server ở VN.

Phần I - Giới thiệu Hệ điều hành Windows NT Server.

Windows NT Advanced Server là hệ điều hành độc lập với các nền tảng phần cứng (hardware platform), có thể chạy trên các bộ vi xử lý Intel x86, DEC Alpha, PowerPC có thể chạy trên cấu hình đa vi xử lý đối xứng, cân bằng công việc của các CPUs. Windows NT là hệ điều hành 32 bits thực sự với khả năng thực hiện đa nhiệm ưu tiên (preemptive multitasking). Hệ điều hành thực hiện phân chia thời gian thực hiện tiến trình cho từng ứng dụng một cách thích hợp. Windows NT Advanced Server bao gồm các khả năng đặc trưng mạng hoàn thiện.

I. Kiến trúc mạng

Tìm hiểu về mô hình tham chiếu OSI

Năm 1978, Tổ Chức Chuẩn Hóa Thế Giới OSI (International Organization for Standardization) đã phát triển một mô hình cho công nghệ mạng máy tính được gọi là Mô Hình Tham Chiếu Kết Nối Các Hệ Thống Mở (Open System Interconnection Reference Model) được gọi tắt là Mô Hình Tham Chiếu OSI. Mô hình này mô tả luồng dữ liệu trong một mạng, từ các kết nối vật lý của mạng cho tới các ứng dụng dùng cho người dùng cuối. Mô Hình Tham Chiếu OSI bao gồm 7 tầng, như thể hiện trong hình dưới đây. Tầng thấp nhất, Tầng Vật Lý (Physical Layer), là nơi các bit dữ liệu được truyền tới đường dây cáp (cable) vật lý. ở trên cùng là Tầng ứng Dụng (Application Layer), là nơi các ứng dụng được thể hiện cho người dùng.

Tầng Vật Lý (Physical Layer) có trách nhiệm chuyển các bit từ một máy tính tới một tính khác, và nó quyết định việc truyền

một luồng bit trên một phương tiện vật lý. Tầng này định nghĩa cách gắn cáp vào một bảng mạch điều hợp mạng (network adapter card) và kỹ thuật truyền dùng để gửi dữ liệu qua cáp đó. Nó định nghĩa việc đồng bộ và kiểm tra các bit.

Tầng Liên Kết Dữ Liệu (Data Link Layer) đóng gói thô cho các bit từ tầng vật lý thành các frame (khung). Một frame là một gói tin logic, có cấu trúc trong đó có chứa dữ liệu. Tầng Liên Kết Dữ Liệu có trách nhiệm truyền các frame giữa các máy tính, mà không có lỗi. Sau khi Tầng Liên Kết Dữ Liệu gửi đi một frame, nó đợi một xác nhận (acknowledgement) từ máy tính nhận frame đó. Các frame không được xác nhận sẽ được gửi lại.

Tầng Mạng (Network Layer) đánh địa chỉ các thông điệp và chuyển đổi các địa chỉ và các tên logic thành các địa chỉ vật lý. Nó cũng xác định con đường trong mạng từ máy tính nguồn tới máy tính đích, và quản lý các vấn đề giao thông, như chuyển mạch, chọn đường, và kiểm soát sự tắc nghẽn của các gói dữ liệu.

Tầng Giao Vận (Transport Layer) quan tâm tới việc phát hiện lỗi và phục hồi lỗi, đảm bảo phân phát các thông điệp một các tin cậy. Nó cũng tái đóng gói các thông điệp khi cần thiết bằng cách chia các thông điệp dài thành các gói tin nhỏ để truyền đi, và ở nơi nhận nó sẽ xây dựng lại từ các gói tin nhỏ thành thông điệp ban đầu. Tầng Giao Vận cũng gửi một xác nhận về việc nhận của nó.

Tầng Phiên (Session Layer) cho phép hai ứng dụng trên 2 máy tính khác nhau thiết lập, dùng, và kết thúc một phiên làm việc (session). Tầng này thiết lập sự kiểm soát hội thoại giữa hai máy tính trong một phiên làm việc, qui định phía nào sẽ truyền, khi nào và trong bao lâu.
Tầng Trình Diễn (Presentation Layer) chuyển đổi dữ liệu từ Tầng ứng Dụng theo một khuôn dạng trung gian. Tầng này cũng quản lý các yêu cầu bảo mật bằng cách cung cấp các dịch vụ như mã hóa dữ liệu, và nén dữ liệu sao cho cần ít bit hơn để truyền trên mạng.

Tầng ứng Dụng (Application Layer) là mức mà ở đó các ứng dụng của người dùng cuối có thể truy nhập vào các dịch vụ của mạng.

Khi hai máy tính truyền thông với nhau trên một mạng, phần mềm ở mỗi tầng trên một máy tính giả sử rằng nó đang truyền thông với cùng một tầng trên máy tính kia. Ví dụ, Tầng Giao Vận của một máy tính truyền thông với Tầng Giao Vận trên máy tính kia. Tầng Giao Vận trên máy tính thứ nhất không cần để ý tới truyền thông thực sự truyền qua các tầng thấp hơn của máy tính thứ nhất, truyền qua phương tiện vật lý, và sau đó đi lên tới các tầng thấp hơn của máy tính thứ hai.
Mô Hình Tham Chiếu OSI là một ý tưởng về công nghệ mạng, và một số ít hệ thống tuân thủ theo nó, nhưng mô hình này được dùng để thảo luận và so sánh các mạng với nhau.

II. Network Card Driver và Protocol làm gì?

Một network adapter card, tức bảng mạch điều hợp mạng, (đôi khi gọi là network interface card hay vắn tắt là NIC) là một bảng mạch phần cứng được cài đặt trong máy tính của bạn để cho phép máy tính hoạt động được trên mạng. Network adapter card cung cấp một (hoặc nhiều) cổng để cho cáp mạng được nối vào về mặt vật lý, và về mặt vật lý bảng mạch đó sẽ truyền dữ liệu từ máy tính tới cáp mạng và theo chiều ngược lại.
Mỗi máy tính trong mạng cần phải có một trình điều khiển (driver) cho network adapter card, đó là một chương trình phần mềm kiểm soát bảng mạch mạng. Mỗi trình điều khiển của network adapter card được cấu hình cụ thể để chạy với một kiểu bảng mạch mạng (network card) nhất định.
Cùng với các bảng mạch mạng và trình điều khiển bảng mạch mạng, một máy tính mạng cũng cần phải có một trình điều khiển giao thức (protocol driver) mà đôi khi gọi là một giao thức giao vận hay chỉ vắn tắt là giao thức. Trình điều khiển giao thức thực hiện công việc giữa phần mềm mạng ở mức trên (giống như trạm làm việc và máy chủ) và network adapter card. Giao thức đóng gói dữ liệu cần gửi đi trên mạng theo cách mà máy tính ở nơi nhận có thể hiểu được.
Qui trình kết hợp một trình điều khiển giao thức với network adapter card tương ứng, và thiết lập một kênh truyền thông giữa hai thứ đó gọi là kết gắn (binding).
Để hai máy tính truyền thông với nhau trên một mạng, chúng phải dùng cùng một giao thức. Đôi khi một máy tính được cấu hình để dùng nhiều giao thức. Trong trường hợp này, hai máy tính chỉ cần một giao thức chung là có thể truyền thông với nhau.
Trong một số mạng, mỗi trình điều khiển network adapter card và giao thức của máy tính là một phần mềm

riêng. Trong một số mạng khác thì chỉ một phần mềm gọi là monolithic protocol stack thực hiện các chức năng của cả trình điều khiển network adapter card và giao thức.

III. Kiến trúc mở

Windows NT Advanced Server sử dụng hai chuẩn là NDIS (Network Driver Interface Specification) và TDI (Transport Driver Interface). NDIS là chuẩn cung cấp cho việc nói chuyện giữa card mạng (network card) và các giao thức (protocol) mạng được dùng. NDIS cho phép sử dụng nhiều giao thức mạng trên cùng một card mạng. Mặc định Windows NT Advanced Server được cung cấp sử dụng bốn giao thức đó là NetBEUI (NetBIOS Extended User Interface), TCP/IP, Microsoft NWLINK, và Data Link Control. TDI cung cấp khả năng nói chuyện giữa các giao thức mạng với các phần mềm mạng mức trên (như Server và Redirector).

IV. Ưu điểm của NDIS

Như trên đã nói NDIS cung cấp sự liên lạc giữa các giao thức mạng với card mạng. Bất cứ trạm làm việc nào (sử dụng hệ điều hành Windows NT Workstation) đều có thể các trình điều khiển điều khiển card mạng được cung cấp nội tại trong Windows NT Advanced Server. Trong trường hợp phải sử dụng một loại card mạng khác, tức là phải cần trình điều khiển cho card mạng không có sẵn trong Windows NT, NDIS vẫn có thể sử dụng đa giao thức mạng trên card mạng này.

Khi máy tính sử dụng đa giao thức mạng, các gói tin dữ liệu sẽ được chuyển đi thông qua giao thức mạng thứ nhất (giao thức này được gọi là primary protocol), nếu không được máy tính sẽ sử dụng tiếp giao thức thứ hai và cứ thế tiếp tục.
Trên mỗi máy tính được cài đặt Windows NT, mỗi một giao thức mạng được đặt sử dụng trên một card mạng cần phải được đặt một giá trị gọi là LAN adapter number trên card mạng đó.

V. Tìm hiểu về TDI

TDI là giao diện giữa tầng phiên (Session) và tầng giao vận (Transport). TDI được xây dựng với mục đích cho phép tầng giao vận có thể làm việc với các chương trình thuộc tầng trên (ví dụ như Server và Redirector) sử dụng chung một giao diện. Khi Server và Redirector tạo một lời gọi tới tầng giao vận, nó sẽ sử dụng giao diện TDI để thực hiện lời gọi này và do vậy nó không cần biết cụ thể giao thức tầng giao vận sẽ được sử dụng.
Windows NT sử dụng TDI nhằm mục đích đảm bảo rằng các hệ thống sử dụng các giao thức khác nhau, thậm chí cả các Server và Redirector được viết bởi các hãng khác nhau (Third parties) có thể làm việc được với Windows NT.

Sử dụng TDI đã làm cho Windows NT khắc phục nhược điểm của sản phẩm LAN manager 2.x đó là trong khi Windows NT không hạn chế số lượng các trạm làm việc nối vào Server thì LAN manager 2.x lại hạn chế ở con số 254 trạm làm việc.
Có một trường hợp ngoại lệ, cho dù TDI là chuẩn giao diện giữa tầng giao vận và các tầng mức trên song riêng đối với NetBIOS các trình điều khiển và các DLLs được sử dụng để thực hiện nhiệm vụ này.

VI. Cách thức làm việc của các giao thức

1. NetBEUI:

NetBEUI lần đầu tiên được đề cập tới vào năm 1985, đây là một giao thức mạng gọn nhẹ, nhanh. Khi được bắt đầu phát triển từ năm 1985, NetBEUI cho phép phân đoạn các mạng nhóm tác nghiệp từ 20 đến 200 máy tính, cho phép kết nối giữa các segment LAN với segment LAN khác hoặc với mainframe.

NetBEUI tối ưu hoá khả năng xử lý khi được sử dụng trên mạng LAN. Trên LAN, đây là giao thức mạng có cho phép lưu thông các gói tin nhanh nhất. Phiên bản NetBEUI được sử dụng cho Windows NT là NetBEUI 3.0 và có một số điểm khác với các phiên bản trước đó.
Loại trừ hạn chế 254 phiên làm việc của một Server trên một card mạng. Hoàn thiện khả năng seft-tuning. Khả năng xử lý trên đường truyền tốt hơn. NetBEUI trong Windows NT là giao thức NetBIOS Frame (NBF) format.

Nó sử dụng NetBIOS làm cách thức nói chuyện với các tầng mức trên.
Hạn chế của NetBEUI là không có khả năng chọn đường và thực hiện kém hiệu quả trong môi trường mạng WAN. Do vậy thông thường để cài đặt mạng thường sử dụng phương pháp cài cả NetBEUI và TCP/IP để đáp ứng các chức năng thích hợp.

2. TCP/IP :

TCP/IP (Transmission Control Protocol/Internet Protocol) được phát triển từ cuối những năm 1970, đó là kết quả của Defense Advanced Research Projects Agency (DARPA) nghiên cứu dự kết nối giữa các mạng với nhau. Ưu điểm của giao thức TCP/IP là cung cấp khả năng kết nối giữa các mạng với hệ điều hành và phần cứng khác nhau. TCP/IP tương thích với môi trường Internet, môi trường kết nối mạng của các trường đại học, các tổ chức, chính phủ, quân đội với nhau với nhau.
Với Windows NT có thể sử dụng hệ quản trị mạng SNMP để theo dõi sự hoạt động của máy tính sử dụng giao thức TCP/IP. Microsoft thực hiện giao thức TCP/IP bằng cách sử dụng STREAMS - tương thích với môi trường giao diện, Windows NT sử dụng STREAMS như là một giao diện giữa tầng TDI và tầng thấp hơn. Nhược điểm của TCP/IP là khả năng xử lý chậm hơn so với NetBEUI trong môi trường mạng LAN

3. NWLink

Microsoft NWLink là chuẩn NDIS tương thích với giao thức IPX/ SPX trong môi trường mạng Novell Netware. Tương tự TCP/IP, NWLink cũng sử dụng môi trường giao diện STREAMS.
NWLink cho phép một Server Windows NT có thể "nhìn thấy" một Server Netware. Song để sử dụng các tài nguyên được chia sẻ trên Server Netware này nhất thiết vẫn phải chạy chương trình Netware Client.

4. Data Link Control

Data Link Control không bao giờ được đặt là primary protocol. Data Link Protocol được sử dụng nhằm các mục đích sau :

Cài đặt máy tính sử dụng Windows NT cho phép truy cập đến IBM@ mainframes.
Cài đặt máy in nối trực tiếp vào mạng, thay vì được nối vào cổng song song hay nối tiếp tại một print server nào đó. Data Link Control cho phép các chương trình truy cập trực tiếp tới tầng Data Link trong mô hình tham chiếu OSI.

VII. Sử dụng RPC (Remote Procedure Call)

Windows NT cung cấp khả năng sử dụng RPC để thực thi các ứng dụng phân tán. Microsoft RPC bao gồm các thư viện và các dịch vụ cho phép các ứng dụng phân tán hoạt động được trong môi trường Windows NT. Các ứng dụng phân tán chính bao gồm nhiều tiến trình thực thi với nhiệm vụ xác định nào đó. Các tiến trình này có thể chạy trên một hay nhiều máy tính.
Microsoft RPC sử dụng name service provider để định vị Servers trên mạng. Microsoft RPC name service provider phải đi liền với Microsoft RPC name service interface (NIS). NIS bao bao gồm các hàm API cho phép truy cập nhiều thực thể trong cùng một name service database (name service database chứa các thực thể, nhóm các thực thể, lịch sử các thực thể trên Server).
Khi cài đặt Windows NT, Microsoft Locator tự động được chọn như là name service provider. Nó là name service provider tối ưu nhất trên môi trường mạng Windows NT.

VIII. Sử dụng Remote Access Service (RAS)

RAS cho phép remote User làm việc như là khi họ kết nối trực tiếp vào mạng. RAS là sự kết nối trong suốt với Microsoft Client và các ứng dụng trên mạng.
Windows NT RAS Server phiên bản 3.5 trở lên cung cấp giao thức PPP cho phép bất cứ PPP client nào đều có thể sử dụng TCP/IP, NetBEUI, IPX truy cập. Ngoài ra Windows NT client có thể sử dụng giao thức SLIP để thực

hiện Remote Access Servers. Giao thức Microsoft RAS cho phép bất cứ Microsoft RAS client nào đều có thể truy cập sử dụng Dial-in.
Để truy cập vào WAN, Clients có thể sử dụng dial-in sử dụng chuẩn đường điện thoại thông qua một modem hoặc một modem pool. Nhanh nhất là sử dụng ISDN, ngoài ra có thể sử dụng X.25 hay RS-232 null modem. Microsoft RAS cho phép tối đa 256 clients dial-in.
Đối với mạng LAN, giao thức IP cho phép truy cập tới mạng TCP/IP (như mạng Internet). Giao thức IPX cho phép truy cập tới các Servers Novell Netware.
Windows NT Server Multi-Protocol Routing
Windows NT Server, kết hợp với Windows NT Server Multi-Protocol Routing, cho phép nối giữa các mạng cục bộ, giữa mạng cục bộ với mạng diện rộng mà không cần phải có một Router riêng biệt. Windows NT Server sử dụng cả hai RIP cho IP và RIP cho IPX.
Windows NT Server Multi-Protocol được cài đặt bằng cách chạy chương trình UPDATE.EXE từ đĩa hay CDROM. Chương trình này sẽ copy các tệp tin cần thiết để cài đặt.
Khả năng của Windows NT Server MPR
Sử dụng một RAS server để route giữa một client truy cập từ xa và một mạng LAN
Dưới đây là các yêu cầu cần thiết khi sử dụng Windows NT RAS như một dial-up rouuter giữa mạng LAN và Internet hoặc với TCP/IP enterprise.
1. Windows NT computer cần một card mạng và một modem tốc độ cao.
2. Sử dụng PPP nối vào Internet hoặc mạng TCP/IP enterprise.
3. Đặt đúng địa chỉ và subnet.
4. Cài đặt đúng Registry và Default Gateway để máy tính này thực hiện đồng như là một Router và là một Client của mạng LAN.

IX. Route giữa các LANs với nhau

Windows NT Server có thể được tăng cường bằng cách cài đặt khả năng routing giữa các mạng cục bộ với nhau và chức năng BOOTP/DHCP Relay Agent. Để cài đặt Route giữa các LANs với nhau thì Windows NT computer phải có tối thiểu 2 card mạng.

X. Route WAN

Không thể route giữa các mạng WAN thông qua chuyển mạch gói (switched circuits) hoặc đường điện thoại (dial-up lines). Khả năng route này chỉ thực hiện được khi có WAN card (ví dụ T1 hay Frame-Relay).

XI. RIP routing cho IPX

RIP routing cho IPX cung cấp chức năng địa chỉ hoá cho phép các gói tin được gửi đi đến một đích định trước. Phiên bản này hiện nay chưa có bất kỳ một khả năng lọc nào cho việc chuyển tiếp các gói tin, bởi vậy tất cả các thực thể trong bảng RIP và SAP chọn đường cần phải được truyền bá. Trên mạng có phạm vi rộng vấn đề giải thông cho việc chuyển tiếp các gói tin cần phải được quan tâm. Internal routing không cho phép thực hiện thông qua đường điện thoại.

XII. RIP routing cho IP

Windows NT Server cung cấp RIP cho chức năng quản trị động bảng chọn đường giao thức IP (dynamic routing tables). Phiên bản RIP cho IP cũng không hoạt động được thông qua đường kết nối dial-up. RIP cho IP lặp lại các thông tin broadcast nên sử dụng UDP/IP thay thế cho TCP/IP.

XIII. Bảo vệ và quản trị hệ thống

Windows NT xây dựng hệ thống bảo vệ bên trong hệ điều hành. Tự thân điều khiển truy cập cho phép người sử dụng phân quyền tới từng tệp tin riêng lẻ, tự do điều khiển trên cơ sở các chức năng cơ bản của hệ thống.
Với khả năng cho phép cài đặt các domains và trust relationships, cho phép tập trung hoá việc quản trị Users và bảo vệ thông tin tại một địa điểm. Với khả năng này hệ thống mạng sẽ dễ dàng quản trị và vận hành.

XIV. Phương thức bảo vệ trên mạng

Cơ sở của sự bảo vệ và quản trị tập trung trong môi trường Windows NT Advanced Server là domain. Một domain là một nhóm các Servers cài đặt hệ điều hành Windows NT Advanced Server chứa cùng một tập hợp các User accounts. Do vậy thông tin về một User mới chỉ cần nhập tại một Server bất kỳ nhưng đều cho phép các Servers khác trong domain nhận ra.
Trust Relationship nối các domains với nhau, cho phép pass-through authentication. Điều này có nghĩa là người sử dụng chỉ cần có account trong một domain có thể truy cập tới các thực thể trên toàn mạng.

1. Domains : Đơn vị quản trị cơ bản

Việc nhóm các máy tính vào các domains đem lại hai cái lợi chính cho người quản trị mạng và người sử dụng. Cái quan trọng nhất đó là tất cả các Servers trong một domain được xem như là một đơn vị quản trị đơn chia sẻ khả năng bảo vệ và thông tin về người sử dụng. Mỗi một domain có một cơ sở dữ liệu (database) lưu trữ thông tin về User account. Mỗi một Server trong domain lưu trữ một bản copy database. Do đó Windows NT Advanced Server tiết kiệm cho người quản trị mạng cũng như người sử dụng thời gian và đem lại các kết quả thích đáng. Cái lợi thứ hai đó chính là sử thuận tiện cho người sử dụng.

2. Trust Relationship : nối giữa các domains

Bằng cách thiết lập Trust Relationship nối giữa các domains trên mạng với nhau cho phép các User accounts và global group được sử dụng trên nhiều domains thay vì chỉ trên một domain. Khả năng này làm cho công việc của người quản trị mạng trở nên dễ dàng hơn, họ chỉ cần tạo account cho người sử dụng trên một domain song vẫn có thể truy cập tới các máy tính của các domains khác chứ không riêng gì các máy tính trong cùng một domain.
Việc thiết lập Trust Relationship có thể theo một chiều hoặc hai chiều. Trust Relationship hai chiều là một cặp của Trust Relationship một chiều, ở đó mỗi domain tin tưởng vào domain khác.

3. Hoạt động của domain

Yêu cầu tối thiểu cho một domain là phải có domain controller và lưu trữ bản copy chính (master copy) của User và group database. Tất cả các thông tin thay đổi trong database này phải được thực hiện trên domain controller, tức là bất cứ sự thay đổi User database trên một Server nào trong domain sẽ được tự động cập nhật lại trong domain controller. Domain account database được sao lưu trên tất cả các Server cài đặt Windows NT Advaced Server. Cứ 5 phút một lần các Servers lại gửi query lên domain controller hỏi xem có sự thay đổi gì không. Nếu có sự thay đổi, domain cntroller gửi thông tin bị thay đổi (chỉ có thông tin bị thay đổi mới được gửi) tới các Servers trong domain. Để đảm bảo hệ thống hoạt động liên tục, cách tốt nhất là tạo thêm backup domain controller cho domain controller chính.

4. Các kiểu domain

Có bốn kiểu domains được đưa ra để tổ chức hệ thống mạng đó là single domain, master domain, multiple master domain, complete trust domain.

Single domain
Nếu như hệ thống mạng không có quá nhiều User do đó không cần phải chia nhỏ việc tổ chức bằng các sử dụng kiểu domain đơn giản nhất đó là simple domain. Mạng máy tính khi đó chỉ có một domain duy nhất và không cần đặt Trust Relationship. Mô hình này không phức tạp rất phù hợp đối với mạng có quy mô nhỏ.
Master domain
Trong trường hợp phải phân chia mạng thành các domains cho những mục đích khác nhau song quy mô của mạng lại đủ nhỏ thì lựa chọn tốt nhất là sử dụng master domain. Mô hình này cho phép quản lý tập trung nhiều domains. Trong mạng sử dụng master domain cần có một master domain trong đó tạo tất cả Users và global groups. Tất cả các domains khác trên mạng phải "trust" vào master domain này và như vậy có thể sử dụng Users và global groups được tạo ra như trên đã nói. Có thể hiểu rằng master domain là một accounts domain, với mục đích chính là quản lý các User accounts của mạng, các domain còn lại được xem như là các domain tài nguyên tức là không lưu trữ các User accounts mà đơn giản chỉ cung cấp các tài nguyên.
Multiple master domain
Đối với một quy mô lớn hơn, rộng hơn kiểu master domain không thể đáp ứng được khi đó có thể cách tốt nhất là sử dụng Multiple Master Domain. Mô hình này bao gồm một số (đủ nhỏ) các master domains, mọi User accounts được tạo ra trên một master domain trong số các master domains trên mạng. Các domain khác không

phải là master domain (gọi là các department domain) sẽ là các domain tài nguyên. Mỗi một master domain cần phải "trust" vào tất cả các master domains khác. Mọi department domain khi đã "trust" vào một master domain sẽ "trusts" tất cả các master domains khác. Nhược điểm chính của mô hình này là đòi hỏi nhiều sự quản lý Trust Relationship.

Complete trust domain

Trong trường hợp yêu cầu phải quản lý các domains phân tán trên các departments thì mô hình Complete Trust Domain là rất phù hợp. Với Complete trust domain, mỗi một domain "trust" vào domain khác, tức là mỗi một domain có một Users và global groups riêng của mình nhưng các Users và global groups này vẫn có thể được sử dụng trên các domain khác trong mạng. Như vậy giả sử có n domains trên mạng sẽ có n*(n-1) Trust Relationship.

XV. Quản trị môi trường người sử dụng

Trong hệ điều hành mạng Windows NT Advanced Server có nhiều cách để quản lý môi trường người sử dụng. Phương pháp được sử dụng nhiều nhất để quản lý môi trường người sử dụng đó là thông qua các User profiles. Một profile là một tệp phục vụ như một bản chụp nhanh của môi trường làm việc hiện thời của người sử dụng (User desktop environment). Với các profiles có thể hạn chế khả năng của người sử dụng, thay đổi các tham số được đặt tại trạm làm việc riêng của họ. Phương pháp thứ hai để quản lý đó là sử dụng lập các logon scripts cho các Users. Nếu mỗi một User có một logon script thì có nghĩa là script sẽ được chạy bất cứ khi nào User này logon vào hệ thống tại bất cứ trạm làm việc nào trên mạng. Script có thể là một tệp tin dạng lô (batch file) chứa đựng các câu lệnh của hệ điều hành hoặc các chương trình chạy. Cách khác có thể cung cấp cho mỗi người sử dụng một thư mục riêng (home directory) trên Server hay tại Workstation. Một home directory của một User là một vùng lưu trữ riêng của người sử dụng này và họ có toàn quyền trên đó. Ngoài ra có thể đặt các biến môi trường cho mỗi trạm làm việc. Các biến môi trường này xác định sự tìm kiếm đường dẫn của trạm làm việc, thư mục, các tệp tạm thời hay các thông tin tương tự khác.

XVI. Quản lý hệ thống tệp trên mạng

Một vấn đề quan trọng khi sử dụng các Servers trên mạng là sự chia sẻ các tệp tin và các thư mục. Hệ điều hành Windows NT Advanced Server cung cấp khả năng xử lý cao, an toàn và bảo mật cho các tệp tin được chia sẻ nhất là khi sử dụng cấu trúc hệ thống tệp NTFS (Windows NT File System). Phân quyền truy cập các tệp tin và thư mục trên ổ đĩa NTFS đảm bảo rằng chỉ có những người sử dụng thích hợp mới có khả năng truy cập theo quyền hạn được phân ở các mức khác nhau. Với Windows NT Advanced Server các tệp tin và các thư mục trên ổ đĩa NTFS chịu sự kiểm tra kỹ càng. Một khái niệm khác được nhắc tới ở đây đó là file ownership, mỗi một tệp tin và thư mục đều có một người chủ có thể điều khiển nó tất cả các người khác muốn truy cập đều phải được sự cho phép của người chủ này. Windows NT Advanced Server cung cấp chức năng sao lưu thư mục. Với dịch vụ Replicator, có thể duy trì bản sao của hệ thống tệp hiện thời phục vụ khi có sự cố xảy ra đối với hệ thống tệp chính.

XVII. An toàn dữ liệu

1` **Fault tolerance**

Fault tolerance là khả năng đảm bảo cho hệ thống tiếp tục thực hiện chức năng của mình khi một phần gặp sự cố. Thông thường khái niệm Fault tolerance được nhắc tới nhằm mô tả hệ thống đĩa lưu trữ (disk subsystems) song nhìn một cách tổng thể nó còn được ứng dụng cho các phần, thực thể khác của hệ thống. Một cách đầy đủ hệ thống Fault tolerance bao gồm disk subsystems, nguồn cung cấp và hệ thống các bộ điều khiển đĩa dư thừa (redundant disk controllers).

2. Tìm hiểu về RAID

Hệ thống Fault tolerance ổ đĩa được chuẩn hoá bao gồm sáu mức từ 0 đến 5 được biết đến như là Redundant Arrays of Inexpensive Disks (RAID). Mỗi một mức là sự kết hợp của khả năng xử lý, an toàn và giá thành.

Mức 0

Thông thường được biết đến là disk striping và sử dụng hệ thống tệp tin gọi là stripe set. Dữ liệu được chia thành các khối và được trải khắp trên các đĩa cố định (fixed disk) theo một thứ tự định trước.

Mức 1

Được biết đến là disk mirroring sử dụng hệ thống tệp tin gọi là mirror set. Tất cả dữ liệu được ghi trên đĩa thứ nhất đều được ghi lại giống hệt trên đĩa thứ hai. Do vậy chỉ sử dụng được 50 phần trăm dung lượng lưu trữ. Khi một đĩa gặp sự cố, dữ liệu sẽ được lấy từ đĩa còn lại.

Mức 2

Phương pháp sử dụng thêm mã error-correcting. RAID mức 2 chia các tệp tin thành các bytes trải khắp trên nhiều đĩa. Phương pháp error-correcting yêu cầu tất cả các các đĩa đều phải lưu thông tin error-correcting.

Mức 3

Tương tự như mức 2, nhưng chỉ yêu cầu một đĩa để lưu trữ dữ liệu parity (thông tin error-correcting).

Mức 4

Xử lý dữ liệu với kích cỡ của các khối (blocks) và các đoạn (segments) lớn hơn so với mức 2 và mức 3. Nó lưu trữ thông tin error-correcting trên một đĩa tách rời dữ liệu của người sử dụng.

Mức 5

Được biết đến với cái tên striping and parity. Đây là loại thông dụng. RAID 5 tương tự như RAID 4 nhưng thông tin parity được ghi không phải chỉ trên một đĩa mà là trên tất cả các đĩa. Điều đó có nghĩa là có hai loại thông tin trên một đĩa.

3. Quản lý UPS (Uninterrupt Power Supplies)

Có hai cách thức sử dụng UPS là online và standby.

Online : Sử dụng online UPS kết nối trung gian giữa máy tính và nguồn điện, khi đó UPS trở thành đơn vị cung cấp nguồn chính.

Standby : UPS được sử dụng nối giữa máy tính và nguồn cung cấp, song UPS được sử dụng ở trạng thái chờ đợi sẵn sàng hoạt động bất cứ khi nào có sự cố về nguồn.

Windows NT Advanced Server sử dụng UPS service để theo dõi trạng thái của UPS cung cấp các thông tin đầy đủ của UPS cho người quản trị mạng.

XVIII. Hệ sao lưu dữ liệu

Windows NT Advanced Server cung cấp tiện ích tape backup, cho phép sao lưu dữ liệu tập trung tất cả các ổ đĩa của các máy tính trên mạng chạy trên các hệ điều hành khác nhau từ Microsoft LAN Manager 2.x, Windows NT Workstation, Windows for Workgroup đến các máy chủ được cài đặt Windows NT Advanced Server khác.

XIX. Clustering

1. So sánh với Fault Tolerant

Ưu điểm của Cluster so với Fault Tolerant là ở chỗ trong khi Fault Tolerant xây dựng khả năng làm việc với mức độ cao của thiết bị chính thì thiết bị backup lại ở trạng thái chờ (idle) chỉ bắt đầu hoạt động khi thiết bị chính gặp lỗi. Đối với Cluster không như vậy, trong khi hệ thống chính vẫn thực hiện với mức độ cao thì hệ thống backup cũng thực hiện song song đồng thời kết hợp với hệ thống chính cùng chia sẻ tài nguyên Cluster. Windows NT Cluster là một giải pháp phần mềm phù hợp với giá mà người sử dụng phải trả để có được một hệ thống có khả năng thay đổi dễ dàng mềm dẻo đồng thời đảm bảo được sự ổn định an toàn của hệ thống.

2. Giới thiệu kỹ thuật

Các ứng dụng Cluster được xây dựng theo mô hình Client/Server, luồng công việc được chia thành các đơn vị nhỏ được thực hiện trên các máy khác nhau.
Windows NT Cluster được thiết kế tương thích với các chuẩn được xây dựng từ trước trong Windows NT, các tiện ích quản trị mạng không cần phải có sự thay đổi nào khi hoạt động trên hệ thống Windows NT.

3. Mô hình phần cứng

NT Cluster được thiết kế theo chuẩn công nghiệp các vi xử lý có thể là Intel hoặc RISC, các kỹ thuật mạng cục bộ thông dụng, các giao thức giao vận như IPX/SPX, TCP?IP, xây dựng theo phương pháp Module hoá dễ dàng mở rộng phát triển. Windows NT Cluster được xây dựng điều khiển tập trung nhằm cung cấp kỹ thuật cluster mang lại nhiều tiện lợi nhất. Mục đích của việc thiết kế này là nhằm đưa ra một sản phẩm bao hàm tất cả các khía cạnh xu hướng phát triển của phần cứng bao gồm các vi xử lý, kết nối giữa các hệ thống lưu trữ. Tất cả các vi xử lý trong hệ Cluster đều phải chạy hệ điều hành Windows NT, hiện tại hệ Cluster chỉ support cho hệ thống trong đó các máy chủ phải có dòng vi xử lý giống nhau. Trong tương lai việc hoà trộn các loại máy chủ trong cùng một hệ thống là một mục tiêu quan trọng. Có hai kiểu kết nối trong Windows NT Cluster là kết nối Processor-to-Processor và kết nối Processor-to-Storage.
Với kết nối Processor-to-Processor, Windows NT sử dụng phương thức giao vận nội tại trong hệ điều hành để thực hiện việc liên lạc như giao thức TCP/IP, IPX/SPX. Các giao thức này hoạt động được trên các chuẩn mạng như Ethernet, FDDI, ATM, Token Ring ..v..v..

4. Mô hình phần mềm

Windows NT Cluster được xây dựng theo mô hình Client/Server phân rã về mặt chức năng các ứng dụng hoặc giải pháp giữa các hệ thống. Windows NT Cluster đòi hỏi một client User interface phải khởi tạo một phép xử lý hoặc một dịch vụ được cung cấp bởi một hay nhiều máy chủ trong hệ thống. Với Windows NT Cluster, kiểu Partitioned data được thiết kế trong đó luồng công việc thực hiện chung được chia nhỏ thành các segments, mỗi segment sẽ được điều khiển cục bộ tại một nhân tố tạo thành hệ cluster. Kiểu Shared data lại hoạt động theo nguyên tắc khác. Luồng công việc vẫn nguyên khối không bị chia nhỏ mà hoạt động trên toàn bộ hệ thống với việc lập biểu điều khiển thực hiện phân tán. Windows NT Cluster ngoài ra còn cung cấp các APIs cho phép xây dựng các ứng dụng trên hệ cluster trong cả hai chế độ của Windows NT là User mode và kernel mode. Windows NT là giải pháp server-oriented, client không cần biết tới có bao nhiêu nhân tố tạo thành hệ cluster. Client sẽ làm việc với server cung cấp cho nó cách thức tốt nhất xử lý tài nguyên trên mạng. Sử dụng kiểu partitioned data sẽ đảm bảo việc cân bằng công việc giữa các server tốt nhất.

5. Quản trị hệ thống Cluster

Cluster hoạt động kết hợp với một trình quản trị chung và với security domain. Các khả năng này đều tồn tại trong các sản phẩm khác nhau của bộ Windows NT. Trình quản trị account và security chung được cung cấp bởi Windows NT Server Domain. Việc quản trị các phần mềm hoạt động phân tán được thực hiện qua Systems Management Server. Hệ quản trị Windows NT Cluster sẽ tập hợp các khả năng lại tạo thành bộ công cụ cho phép quan trị cluster như một hệ thống đơn lẻ. Hệ quản trị Cluster được thiết kế với giao diện đồ hoạ, quản lý tập trung tài nguyên và các dịch vụ trong hệ thống cluster.

6. Mô hình truy cập dữ liệu

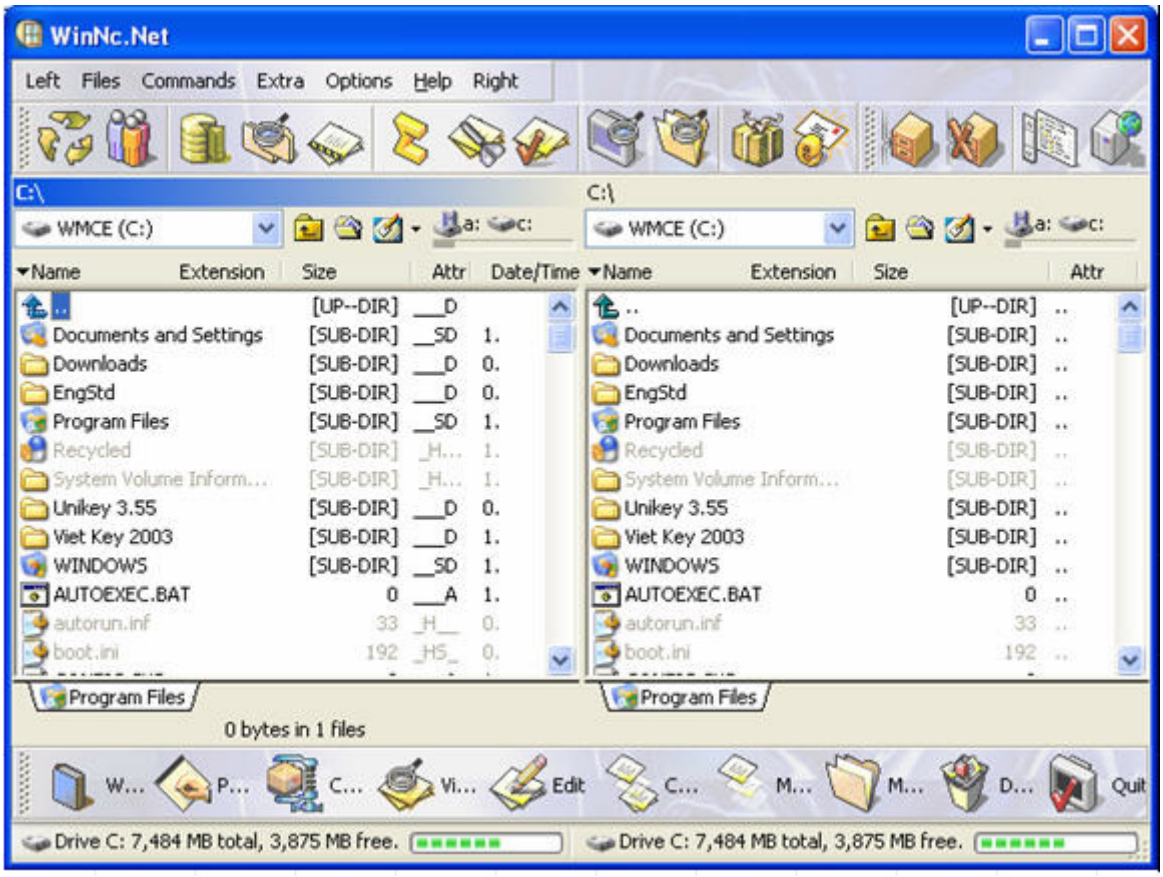
Như trên đã trình bày Windows NT Cluster đưa ra hai phương thức truy cập dữ liệu là Partitioned data và Shared data. Trong đó mô hình phân chia mọi thứ phù hợp với hệ thống xử lý đối xứng, luồng công việc được đồng bộ xử lý trên toàn hệ thống. Mô hình Partitioned data được thực hiện trên hệ thống không đối xứng, luồng công việc được chia thành các đơn vị công việc riêng rẽ được thực hiện trên các phần khác nhau.

NHÀ QUẢN LÝ ĐẠI TÀI
WINNC.NET 4.0

Đã là dân vi tính thì hầu hết tất cả mọi người đều từng sử dụng qua chương trình Norton Commander (NC) xa xưa của Symantec ! Chương trình rất hữu ích để quản lý file nhưng đáng tiếc là chỉ hoạt động trong Dos và không cập nhật . Trong khi đó Windows Explorer lại không đáp ứng hết nhu cầu . Về sau có các chương trình quản lý file mang dáng dấp của " cố nhân" lại bổ sung thêm một số tiện ích khác như : Total Commander , EF Commander , XP Manager , ... Nhưng theo quan điểm của tôi thì tất cả không bằng chương trình WinNC.Net 4.0 . Với WinNC.Net 4.0 bạn sẽ có tất cả những gì liên quan đến việc quản lý file !

Những người đã từng sử dụng Norton Commander khi dùng WinNC thì hoàn toàn không phải tốn thời gian tập làm quen . Tất cả những phím tắt trong WinNC đều giống như NC . Ngoài những chức năng cơ bản của một chương trình quản lý file như : copy , paste , biên tập (edit) , xem dung lượng , ... mà còn có các điểm nổi bật sau : \

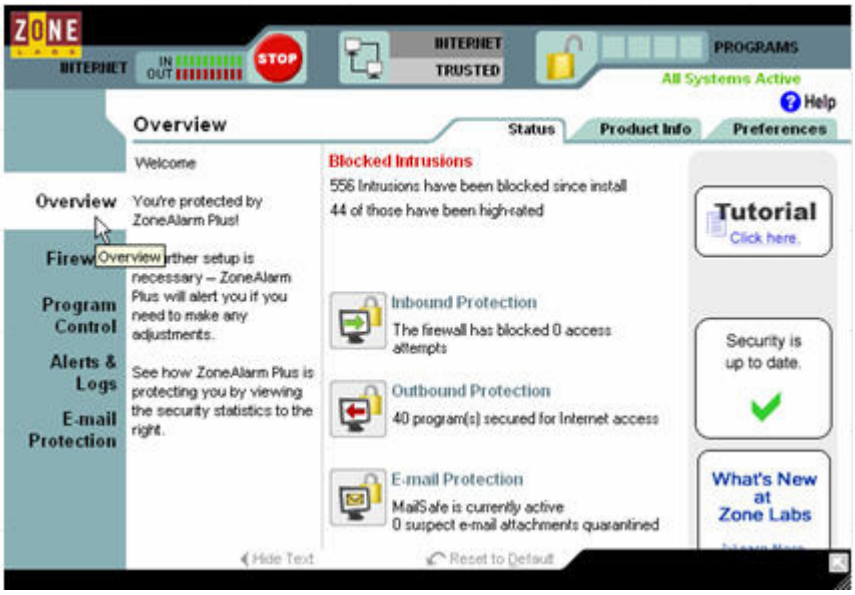
-Mã hóa file hoặc thư mục (nhấn Shift + F5)
-Giải mã file hoặc thư mục (nhấn Shift + F6)
-Dễ dàng thay đổi thuộc tính của file (nhấn F11)
-So sánh sự khác nhau giữa hai thực mục (chọn Commands --> Compare Directories)
-Thông tin " tất tần tật " về hệ thống như : CPU , Mainboard , ... (nhấn Ctrl + S)
-Khả năng tìm file được mở rộng so với Find của Windows Explorer (nhấn Ctrl + F)
-Nén và giải nén file với 11 định dạng như : zip , rar , ace , ... (nhấn F12)
-Cắt và nối file (nhấn Ctrl + F12)
-Tạo file tự bung (chọn Commands --> Create Self Extractor)
-Sữa chữa file zip (Chọn Commands --> Fix Corrupted Zip File)
-Nén nhạc từ Wav --> MP3 (chọn Extra --> Compress wav to mp3)
-Trích nhạc từ CD (Extra --> Extract CD to mp3)
-Cung cấp trình nghe nhạc và khả tạo tạo list MP3
-Và một trình upload/download FTP (chọn Right --> FTP)



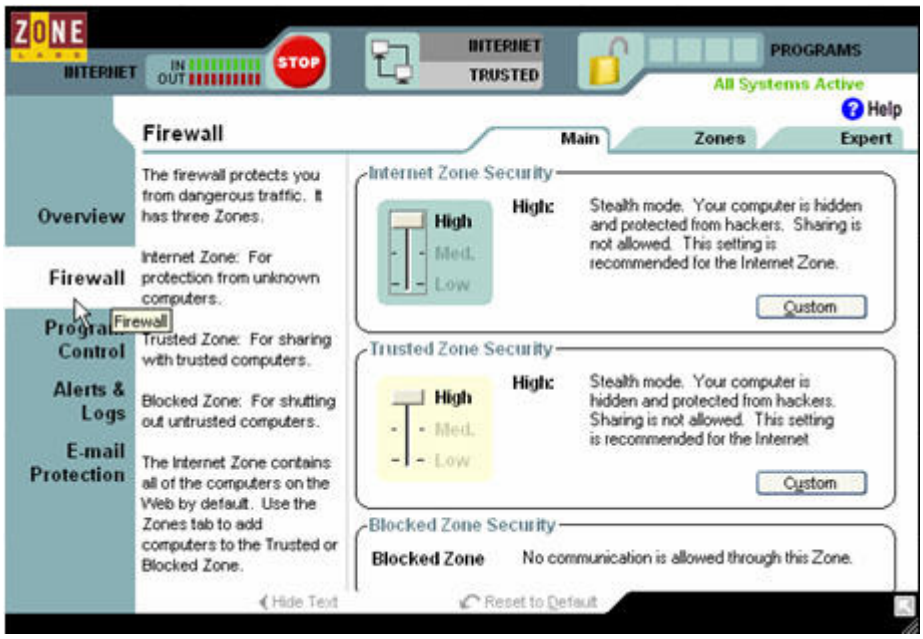
Với các chức năng đó bạn sẽ tiết kiệm được khá nhiều bộ nhớ , không gian và ... tiền bạc cho việc mua thêm các phần mềm phục vụ cho từng mục đích như : nén , mã hoá , trích xuất nhạc , FTP , ... Hãy lưu ý rằng phiên bản WinNC 3000 có dung lượng rất lớn và khi chạy chiếm nhiều bộ nhớ lại khá chậm . WinNc.Net đã khắc phục được các nhược điểm của phiên bản cũ.

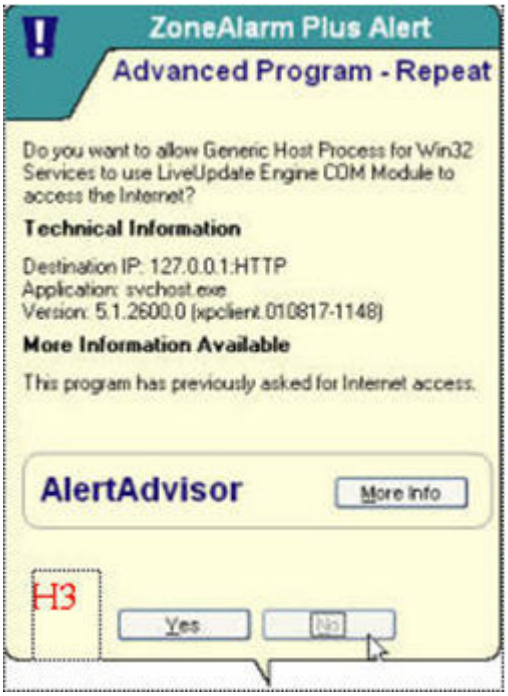
NGĂN CHẶN CÁC MỐI NGUY HIỂM VỚI ZONEALARM

Mình biết các bạn lo ngại gì khi kết nối vào Internet, các mối nguy hiểm khôn lường đang rình rập (virus,spyware,...) . Với phần mềm ZoneAlarm Plus thì nỗi lo đó sẽ vơi đi !



Chương trình sẽ ngăn chặn mối nguy hiểm từ bên ngoài cũng như bên trong máy, khi khởi động máy thì ZoneAlarm sẽ tự động Startup lúc đó thì chương trình đã bắt đầu giám sát mọi hoạt động của máy, khi ZoneAlarm hoạt động thì sẽ có biểu tượng , nếu thấy có nguy hiểm thì chương trình sẽ hiện bảng thông báo (H3). Tuy vậy cũng có đôi khi một chương trình bất kỳ nào đó khởi động thì ZoneAlarm cũng sẽ hỏi "Bạn có muốn file *.exe khởi động không ?", tất nhiên là bạn sẽ chọn Yes nếu nó đúng với tên chương trình mà bạn cần chạy, ngược lại trong rất nhiều trường hợp không biết tên thì đừng nên cho chương trình đó chạy (có thể đó là virus). Ngoài ra bạn có thể dùng cách này để ngăn chặn virus Blaster (khi ZoneAlarm hỏi có muốn file Blaster.exe chạy không, tất nhiên bạn sẽ chọn NO thì yên chuyện). Một khả năng đặc biệt khác của chương trình này là khả năng tạo tường lửa (firewall) đểbảo vệ máy khi lướt net . Bạn nên chọn ở mức cao nhất để có thể yêm tâm hơn . (H2)

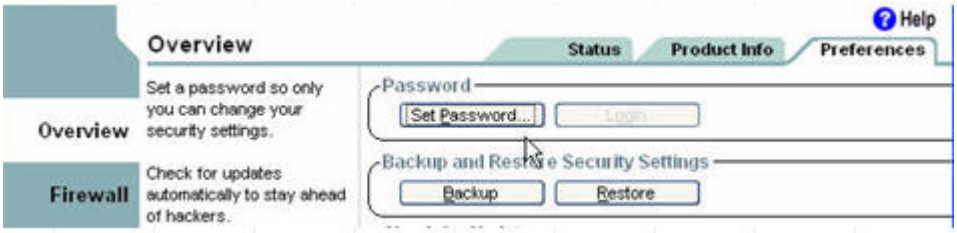




Để không ai có thể điều chỉnh chương trình này thì bạn có thể cài đặt Password, rất đơn giản chỉ cần chọn Tab "Overview" và chọn thẻ "Preferences" nhấn ô "Set Password" và nhập mật khẩu vào ! (H4)

Ngoài ra, nếu bạn không muốn ai vào Internet mà không được sự đồng ý của bạn thì chỉ cần nhấn vào hình ổ khóa màu vàng ở góc trên bên phải  , hoặc nhấn chuột phải vào biểu tượng của chương trình và chọn "Engage Internet Lock" (Nếu ai đó muốn tắt chế độ này thì phải biết Password để mở chương trình , vậy là an toàn rồi nhé !).

Không chỉ ngừng lại ở đó, bạn có thể thiết lập phạm vi báo động ở phần "Alerts & Logs" , và bạn có thể bảo vệ thư điện tử khỏi virus khi vào phần "E-mail Protection". Chúc các bạn thành công với phần mềm này !



Có lẽ bạn sẽ thấy rất phiền khi lần đầu tiên chương trình chạy vì thấy gì nó cũng hỏi ! Nhưng bạn đừng lo, hãy đánh dấu vào ô "Don't show this message again" và chọn YES hoặc NO thì chương trình sẽ nhớ lại và lần sau sẽ không hỏi nữa.

Download : http://www.zonelabs.com
Version : 4.5.594.000
License key : dgfhr - begac - n4xrp - bwp2kd - ipi1g0

MỘT SỐ WEB SITE HỌC NGOẠI NGỮ TRỰC TUYẾN

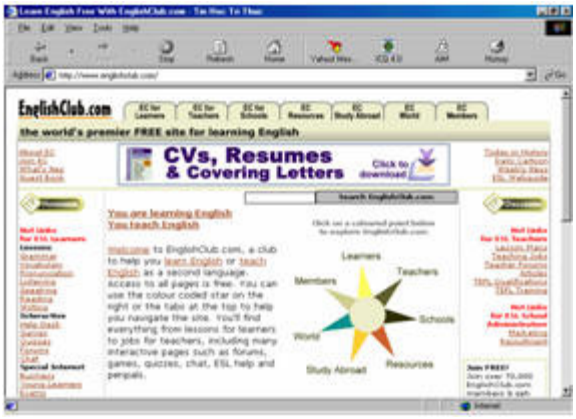
1. http://www.englsih-nz.ac.nz/english

Trang web cung cấp cho các bạn rất nhiều link và các bài học ngoại ngữ trực tuyến trên trang web, đặc biệt có các phần hướng dẫn chi tiết về bài học và các hình ảnh minh họa theo kèm.

2. http://www.learnenglish.org.uk/

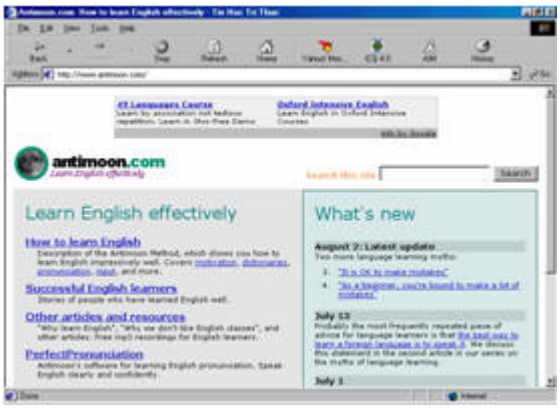
Một trang web học anh văn trực tuyến rất thú vị mà các bạn không nên bỏ qua, một trang học ngoại ngữ cho tất cả mọi lứa tuổi từ các bài học trực tuyến đơn giản phù hợp với lứa tuổi nhỏ cho đến các bài học nâng cao cho những ai mong muốn luyện thi để có một trình độ cao hơn, ngòai ra trang web còn cung cấp các giáo trình anh ngữ cho các thầy cô và những bài hát anh văn vừa chơi vừa học.

3. http://www.englishclub.com/



Trang web dành cho những ai yêu thích ngoại ngữ, trong đây bạn sẽ tìm thấy rất nhiều cấu trúc văn phạm chặt chẽ và có thể trao đổi kiến thức của mình với mọi người thông qua một diễn đàn khá hấp dẫn ở đây.

4. http://www.antimoon.com/
Trang web liệt kê cho các bạn những bài học, những bí quyết đơn giản nhưng hiệu quả để làm cách nào làm cho các bạn học ngoại ngữ một cách đạt hiệu quả cao nhằm nâng cao khả năng trau dồi ngoại ngữ của mình



5. http://www.free-translator.com/
Hiện nay trên Internet có rất nhiều trang web phục vụ cho việc học ngoại ngữ cho các bạn, nhưng nếu các bạn đang cần tìm một trang web học ngoại ngữ trực tuyến cấp tốc với rất nhiều thứ tiếng thông dụng hiện nay trên thế giới thì nên vào trang web http://www.free-translator.com và bắt đầu các bài ngoại ngữ cấp tốc của mình được rồi, ngòai ra trang web còn cung cấp cho các bạn các cung cụ phiên dịch qua lại các thứ tiếng cực mạnh thông dụng hiện nay như: Anh, Pháp, Đức, Tây Ban Nha,…… Thậm chí còn có thể giúp cho các dịch luôn cả một trang web về một thứ tiếng do bạn chỉ định.

MỘT SỐ THỦ THUẬT NHỎ TRONG VIỆC SỬ DỤNG MÁY TÍNH

1> Quản lý giờ giấc mở computer của con cái trong windows 98

Đa số các bậc phụ huynh khi đi làm tất bật suốt ngày mà lại ghét con cái mở máy chơi game ở nhà khi mình đi vắng. Vì vậy, cách này tôi viết ra cốt để cho những phụ huynh nào có ý nghĩ như vậy.

Ta vào Start --> Settings --> Control Panel --> xuất hiện cữa sổ Control Panel --> Find Fast --> ta vào menu Index --> Show Indexer Log.

Bây giờ tất cả những giờ giấc mở máy của mình và cả con cái đã hiện ra hết rồi đấy, chỉ còn thiếu đó là: cây roi để tra khảo xem giờ đó nó mở máy để làm gì thôi!

2> Thủ thuật về Microsoft Office

Cách đánh pass cho MS-Word:

Nếu như chúng ta, ai có những bài viết riêng tư hay những dòng nhật ký đời mình thì không thể nào cho người khác xem được! Vì thế "lão" Bill Gates cũng cho chúng ta một số phương pháp chống xem tài liệu nếu không có pass, vì thế, với tài năng bé nhỏ của mình tôi cũng xin "share" cùng các bạn:

Cách 1: Vào menu Tools --> Chọn Options... --> Chọn thẻ Save --> Khung password to open ta đánh pass của mình vào --> Khung password to modify ta đánh password y chang như trong khung password to open --> OK

Cách 2: Vào menu File --> Save --> Hiện hộp thoại --> Trên các thanh công cụ gần phần Save in chọn Tools -->General Options... --> Xuất hiện hộp thoại --> Cũng giống như trong cách 1 khung password to open ta đánh pass để mở và khung password to modify ta đánh password giống như trong khung password to open -->OK -->Save (nhớ chọn thư mục cần lưu và đặt lại tên file)

Vậy là xong, nhưng tốt nhất sau khi lưu xong các bạn nên ẩn "nhật ký" của mình đi nếu không sẽ bị người khác xem đấy!

Cách đánh pass cho MS-Excel:

Công ty của chúng ta, ai cũng có những tài liệu bí mật, riêng tư không muốn cho công ty khác "chỏ mũi" vào thì cũng nên đánh pass cho phần Excel vốn là phần tính toán thu chi nhiều nhất:

Vào menu File --> Save... --> Hiện hộp thoại --> Trên các thanh công cụ gần phần Save in chọn Tools --> General Options... --> Xuất hiện hộp thoại --> Khung password to open ta đánh pass để mở và khung

password to modify ta đánh password giống như trong khung password to open --> OK --> Save (nhớ chọn thư mục cần lưu và đặt lại tên file)

Vậy là xong, nhưng tốt nhất sau khi lưu xong các bạn nên ẩn "tài liệu mật" của công ty đi nếu không bị mất sẽ bị ông chủ dần xương đó!

Cách đánh pass cho MS-Access:

Mỗi công ty lớn, công ty nào cũng phải dùng những CSDL nói chung là sử dụng MS-Access và cũng có những tài liệu mật tránh bị người khác ăn cắp, vì thế nếu muốn làm cho Access có pass thì phải làm như sau:

Khi vào Access --> Chọn menu File --> Open hay vào biểu tượng Open trên thanh Standard --> Chọn CSDL cần có pass --> Sát bên biểu tượng Open chọn mũi tên xuống vào chọn Open Exclusive --> Xuất hiện CSDL --> Menu Tools -->security -->set Database Password --> Khung password gõ vào pass mình cần, khung verify gõ lại y chang pass khung password --> Ok

Cũng giống như các phần trên, bạn cũng nên ẩn CSDL của mình đi, nhưng mà nếu là dân đã lâu năm thì việc xoá cũng không khó khăn gì !

3> Cách xem mã nguồn trang Web mà không cần vào trang Web đó.

Chẳng hạn tôi muốn xem mã nguồn của Website LBVMT mà không cần vào website thì sao? (Vì một số lý do: vào website thì phải chờ cho web download những hình ảnh về…) Ta mở IE (Internet Explorer) và gõ: view-source:http://www.lbvmvt.com/ và một cửa sổ Notepad sẽ hiện ra cùng với mả nguồn của trang Web. Thật thú vị và không tốn thời gian chờ lâu nữa! Các bạn hãy "vọc" thử đi nhé!

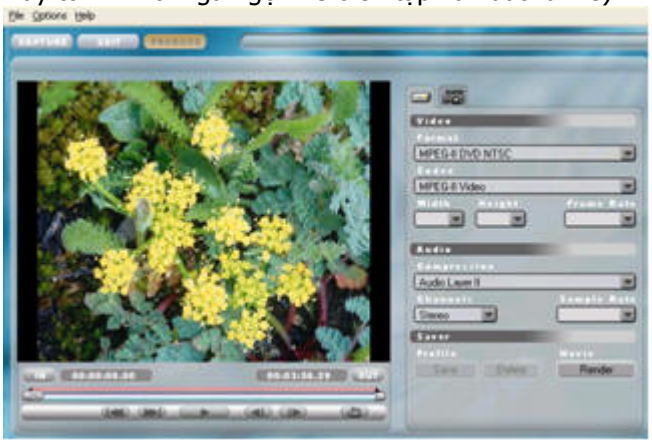
Học tiếng Anh bằng ENGLISH FOR HIGH SCHOOL không cần đĩa

Đầu tiên bạn install EfHSch ,tiếp theo bạn copy toàn bộ các file và các folder của đĩa EfHCh vào một thư mục trong ổ cứng (ở đây tôi sẽ copy vào E:\Efhsch).Như vậy là đã xong một công đoạn,bây giờ bạn vào Start >Program >English for High School>English for High School, rồi nhấn chuột phải và chọn Properties,tiếp đó trong ô Start in,bạn đánh đường dẫn vào thư mục bạn đã copy EfHSch (ở đây là E:\Efhsch).

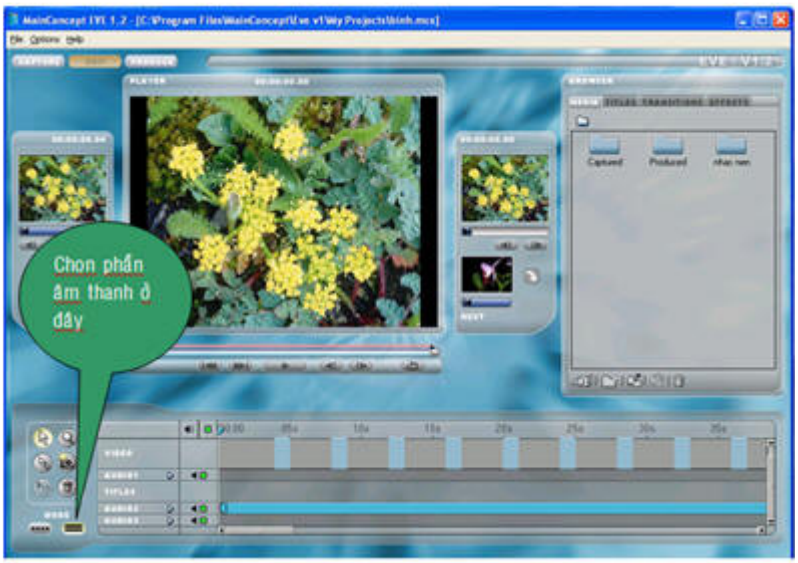
MAINCONCEPT EVE CÔNG CỤ BIÊN TẬP VIDEO VÀ HÌNH ẢNH CHẤT LƯỢNG CAO DÀNH CHO NGƯỜI KHÔNG CHUYÊN

Bên cạnh rất nhiều các phần mềm dùng để biên tập các clip hình ảnh cũng như Video như: Proshow Gold, Pinnacle Studio, …còn có một công cụ đơn giản, gọn gàng hơn nhưng hiệu ứng thì không thua kém bao nhiêu kể cả về hiệu ứng đó là Mainconcept EVE. Chương trình cài đặt của nó vào khoảng 26Mb nhưng cũng bao gồm rất nhiều các hiệu ứng và kỹ xảo, chương trình này đòi hỏi cấu hình máy tối thiểu là từ P3 1.2Ghz và RAM tối thiểu 256Mb kèm theo Card màn hình tối thiểu là 32Mb trở lên (nếu bạn muốn biên tập cả Video thì cầu hình đòi hỏi tối thiểu từ P4 2.0Ghz, RAM 512Mb, Card màn hình 64Mb trở lên mới chạy tốt không bị treo máy). Sau khi cài đặt xong bạn chạy chương trình sẽ được giao diện:

Ở phía dưới thanh menu là 3 thẻ lệnh: Capture, Edit và Produce với 3 chức năng chính: quay phim lại, biên tập và xuất ra file (trong bài viết này tôi xin nói ngắn gọn về biên tập và xuất ra file)



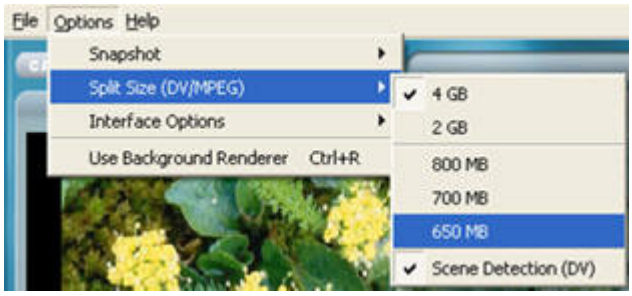
Trong của sổ ngoài cùng phía bên trái là cửa sổ dùng để add các hình ảnh hoặc các file video vào để biên tập (bằng cách chọn các file này sau đó kéo xuống các các clip còn trống ở phía dưới), sau đó chọn các thẻ lệnh title (dùng để biên soạn tựa), Transitions (dùng để chèn các hiệu ứng cuộn hình), Effects (dùng để chèn các hiệu ứng Video) trên cửa số này để chèn các hiệu ứng vào giữa các clip.



Để cho sống động thêm bạn cũng có thể thêm một vài bài nhạc làm nhạc nền cho đoạn phim của mình bằng cách bấm chọn 1 file nhạc mp3 nào đó, sau đó rê vào dòng AUDIO2 hoặc AUDIO3

Sau khi chọn các hiệu ứng vào Clip của mình xong và đã chọn nhạc cho đoạn phim của mình, bạn chọn qua thẻ lệnh Produce để xuất ra thành file Video, trong phần này bạn chỉ việc chọn định dạng kiểu Video mà mình muốn xuất ra: AVI, DV-AVI PAL, DV-AVI NTSC, MPEG 1 VCD PAL, …

Nhưng để video xuất ra có hình chất lượng cao bạn nên chọn SVCD hoặc DVD. Cuối cùng bạn chọn nút lệnh Render để xuất file ra đĩa cứng, sau đó dùng một trình ghi đĩa chẳng hạn như Nero, Winoncd, … để ghi ra thành đĩa hình và trình chiếu cho bà con xem được rồi, rất là dễ phải không bạn.

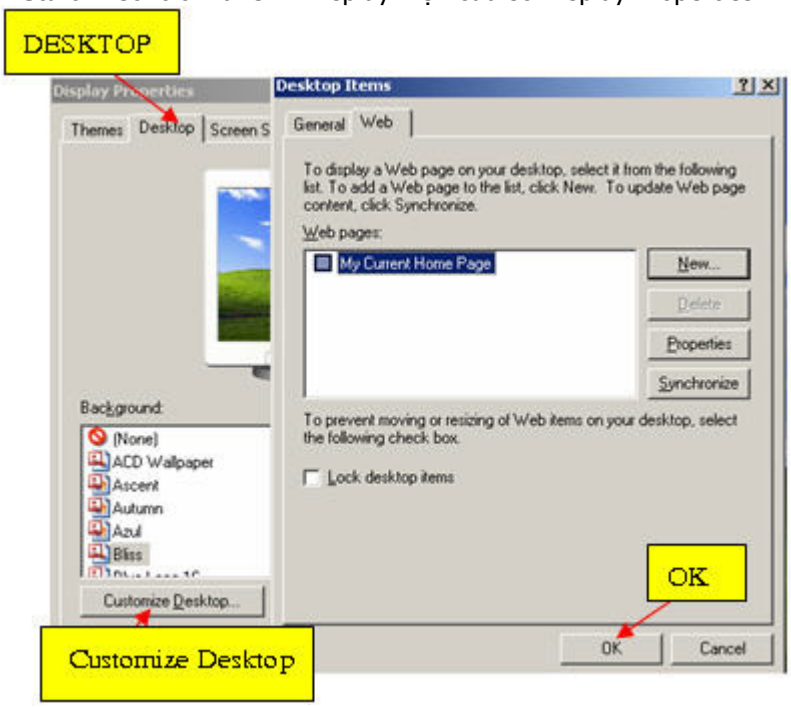


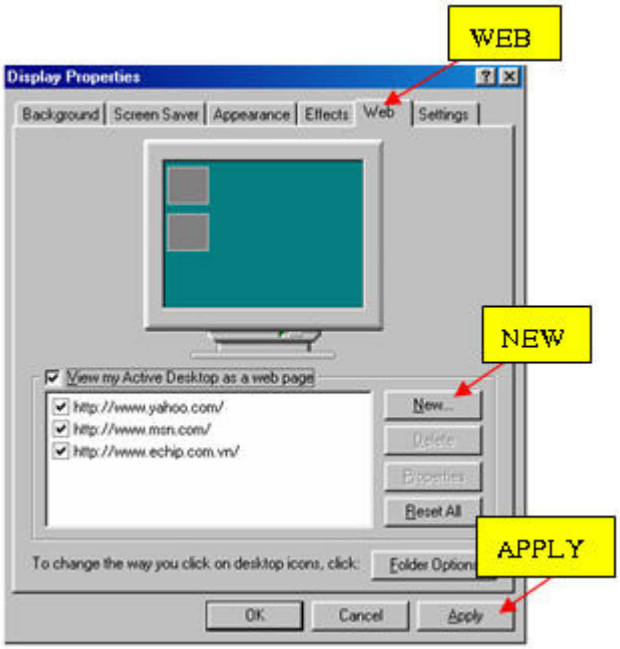
(xin lưu ý với bạn là chương trình này có thể xuất ra file Video dài đến 4Gb, nên nếu ổ cứng của bạn không đủ thì nên vào menu Options chọn split size (DV/MPEG) để lựa chọn cho mình độ dài của đoạn phim là bao nhiêu cho phù hợp)
Chúc bạn làm thành công và tạo ra các sản phẩm made in chính mình

LƯỚT WEB MÀ KHÔNG CẦN TRÌNH DUYỆT WEB

Khi hiệu chỉnh màn hình desktop theo những cách sau đây bạn sẽ tạo ra trên màn hinh desktop những trang mà bạn thường xuyên truy cập:

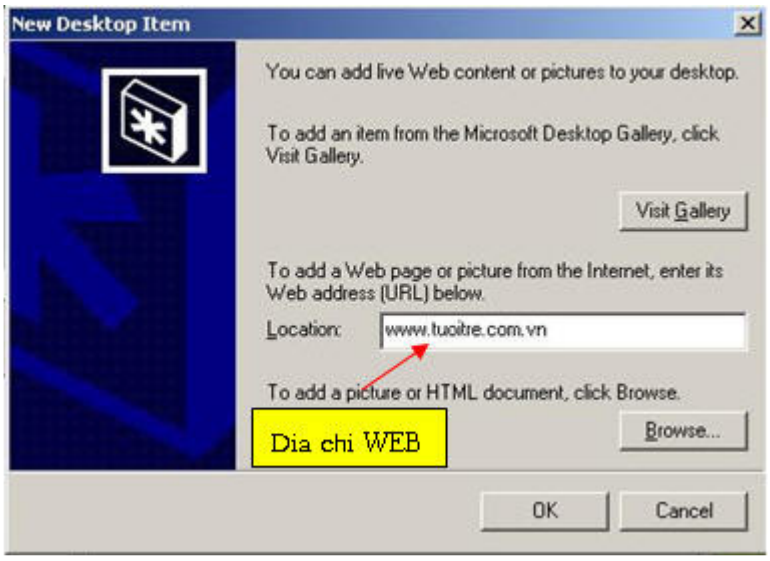
Đầu tiên theo cách sau: Start > Control Panel > Display hiện cửa sổ Display Properties





Bạn chọn thẻ Web (đối với Win 98&2000) còn đối với Win XP bạn chọn thẻ Desktop rồi click nút Customize Desktop ở phía dưới cùng rồi chọn thẻ Web . Sau đó bạn chọn nút New để thêm địa chỉ trang web mới vào ô

Location. Bạn nhớ chọn dấu kiểm vào ô View my Active Desktop as a Web page thì mới có tác dụng(Win98&2000). Để kết thúc nhấn nút Apply và trở về màn hình Desktop. Lúc này bạn sẽ thấy những trang web đó hiện ra.



Nếu bạn không thấy trang web đó trên màn hình Desktop thì bạn hãy nhấp chuột phải trên Desktop sẽ có 1 thanh menu hiện ra và bạn chọn Active Desktop > View As Webpage (Win 98&2000).Chúc bạn thành công.

LOẠI BỎ TÍNH NĂNG AUTO UPDATE CỦA YAHOO MESSENGER

Như các bạn đã biết hiện nay Yahoo Messenger đã có phiên bản 6.0 nhưng sau khi hồ hởi cài đặt xong bạn lại phải thất vọng vì sau khi cài đặt và chạy chương trình bạn cảm thấy việc sử dụng phiên bản 6.0 này rất nặng nề và chậm chạp hơn so với phiên bản 5.6 trước đó vì cấu hình máy bạn không được mạnh lắm, nhưng vấn đề đặt ra ở đây là sau mỗi lần chạy phiên bản 5.6 tính năng Auto Update lại thực thi và làm phiền bạn thì với thủ thuật này sẽ khắc phục được vấn đề đó.
Bạn vào Run gõ dòng lệnh regedit và chạy theo khóa sau:

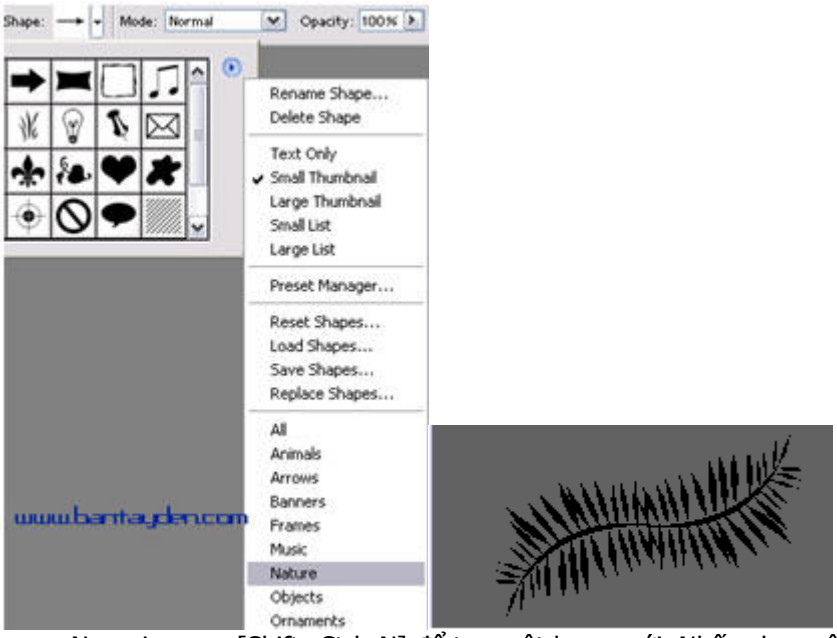
- [HKEY_CURRENT_USER\Software\Yahoo]
  "ClientUpdatePage"="null"

  [HKEY_CURRENT_USER\Software\Yahoo\Pager]
  "LatestSocketServerUrl"="null"

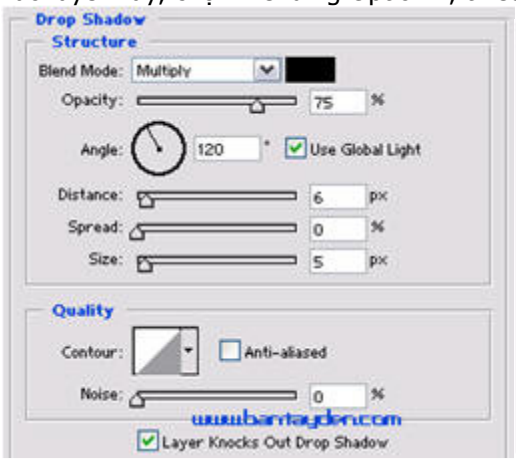
  [HKEY_CURRENT_USER\Software\Yahoo\Pager\Update]
  "LastUpdaterRunTime"=dword: 00000000
  Sau khi thực hiện các bước trên thì bây giờ bạn có thể sử dụng Yahoo một cách dễ dàng và không bị làm phiền nữa.

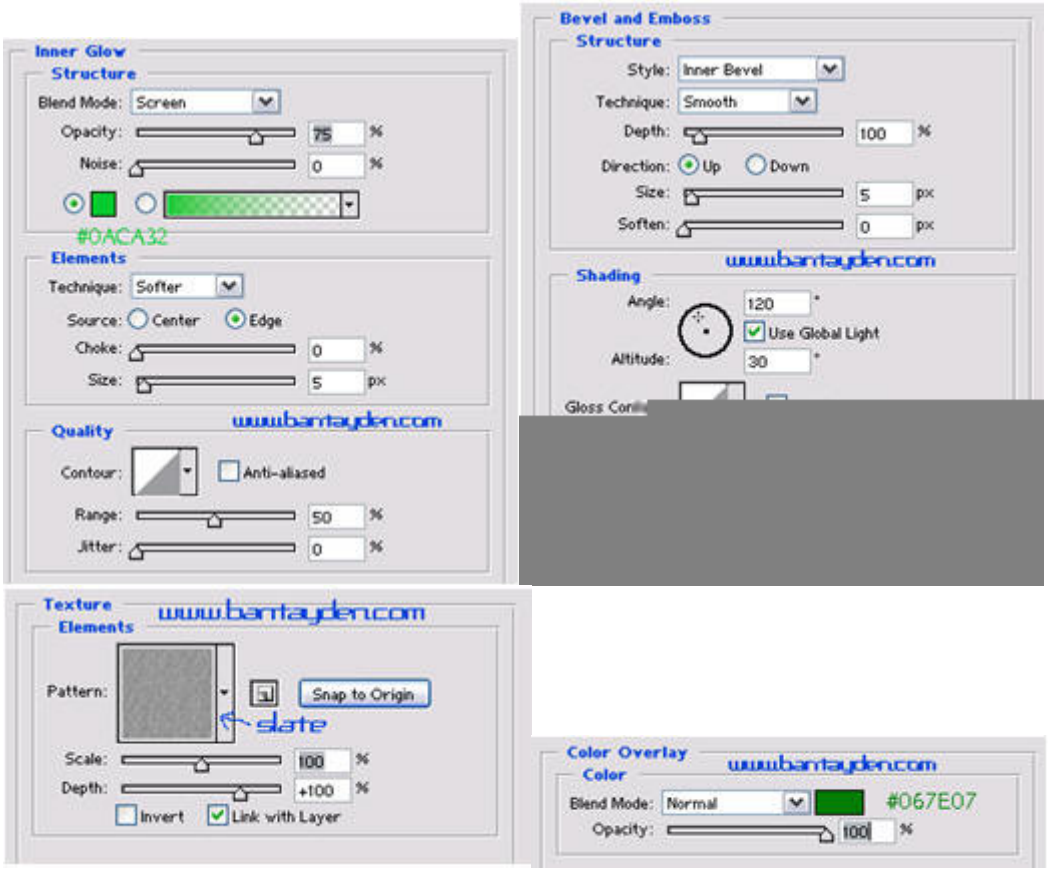
LÀM MỘT CHIẾC LÁ DƯƠNG XỈ VỚI PHOTOSHOP

1. Tạo một file ảnh mới [Ctrl+N], chọn màu nền tuỳ ý bạn, ở đây tôi chọn là #333333. Nhấn D để đưa màu foreground và background về lại thành trắng đen.



2. Vào Layer>New>Layer… [Shift+Ctrl+N] để tạo một layer mới. Nhấn chọn công cụ Custom Sharp Tool [U] nằm trên Toolbar (nó nằm cùng nhóm với Rectangle Tool). Trong phần Sharp, bạn chọn group là Nature, click chọn hình cái lá dương xỉ (Fern). Bạn vẽ một cái lá, to nhỏ tuỳ thích.
3. Nhấp chuột phải vào layer vừa rồi, chọn Duplicate Layer… để nhân đôi layer này lên. Vào Edit>Transform>Rotate 180. Bạn dùng công cụ Move Tool [V] trên thanh Toolbar để dịch chuyển hai chiếc lá sao cho ăn khớp với nhau.
4. Chọn Layer ở trên cùng, vào Layer>Merge Down [Ctrl+E] để ghép hai chiếc lá lại thành một. Nhấp chuột phải vào layer này, chọn Blending Option…, thiết lập các thông số như hình.





Và kết quả cuối cùng đây:

LÀM GÌ KHI CON CHUỘT CỦA BẠN BỊ HƯ ?

Câu trả lời là Hãy đi tìm một con chuột mới . Nhưng nếu trước đó , máy bạn có cài đặt và sử dụng Hot Keyboard Pro thì câu trả lời lại khác , Tạm dùng bàn phím để thay thế trước khi mua một con chuột mới . Phần mềm Hot Keyboard Pro giúp bạn quy định các phím tắt để truy cập các ứng dụng , mở trang web , tắt máy , điều chỉnh Volume …. tất cả đều bằng bàn phím nên chẳng hề đả đỏng gì đến chú chuột cả . Bạn vẫn có thể tiếp tục công việc của mình trước khi có thời gian lượn qua các gian hàng vi tính để sắm cho mình một chú chuột mới về . Hot Keyboard Pro phiên bản mới nhất là 2.5 , được phát hành ngày 11-8-04 , giá 29,95 usd .

Hình 1

Cách sử dụng chương trình này rất đơn giản .

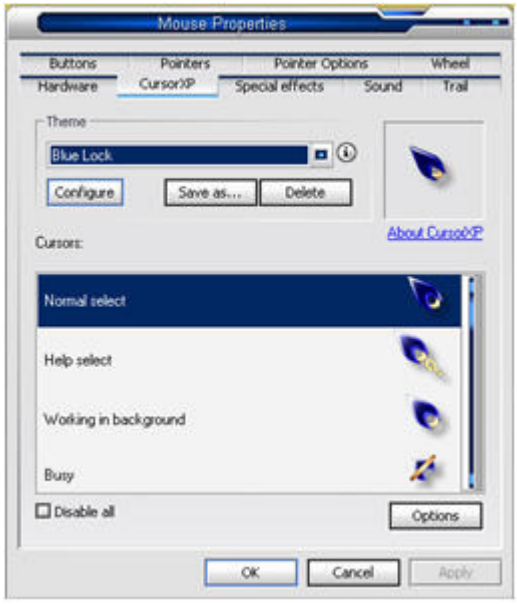
Để quy định một phím tắt mới , bạn chạy chương trình và chọn new macro (hình 1) , cửa số Edit Macro hiện ra , bạn nên đặt tên Macro trong Macro name (để dễ phân biệt với các macro khác ý mà !) . Phần HotKey , hãy quy định tổ hợp phím tắt để chạy macro này . Phần Action Type , hãy nhấn vào nút để xem danh sách thả xuống các loại hành động mà Hot keyboard Pro hỗ trợ (hình 3) :
Open Folder (mở và duyệt thư mục chỉ định bằng phím tắt) ;
Execute the programs (thi hành ứng dụng bằng phím tắt) ;
Launch web browser (truy cập trang web đã chỉ định) ;
Dialup Networking (quay số kết nối Internet) ;
Window manipulations (Thu nhỏ , phóng to … các cửa sổ , ứng dụng đang thi hành) ;
Shutdown Windows (Tắt , khởi động … Windows) ;

Paste Text (Dán đoạn văn bản soạn trước bằng phím tắt) ;
AutoReplace Text (tự động thay thế văn bản) ,
Reminder (bật ghi chú , nhắc nhở bằng phím tắt) ,
Control Winamp (quản lý chương trình Winamp),
Sound Volume Control (Điều chỉnh âm lượng của máy)…..

LÀM ĐẸP CON CHUỘT VỚI CURSORXP PLUS 1.3

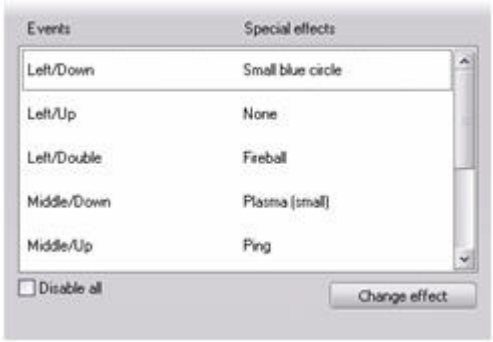
Nếu như bạn là một người rất kỳ công trong việc trang điểm cho máy tính của mình với những phần mềm như StyleXP, Windowblinds, DestopCyler hay BeeIcons thì chắc hẳn bạn phải phải cảm thấy thiếu trong khi giao diện, icon, wallpaper có thể thay đổi liên tục thì con trỏ chuột của bạn "vũ như cẩn" mặc dù có thể thay đổi được theo các hình dạng cho trước. Giờ đây với phần mềm CursorXP Plus 1.3 của hãng Stardock bạn có thể hoàn toàn yên tâm về vấn đề này.

Khi cài đặt thành công thì khi chọn Cursor trong Control Panel sẽ có thêm phần CursorXP và Special Effects .



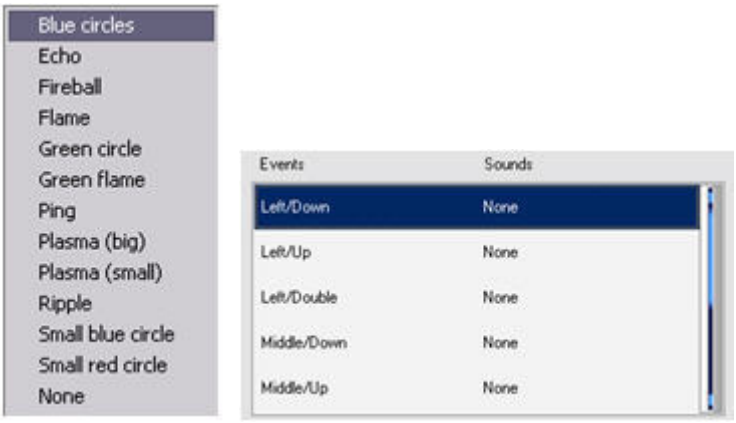
Tại phần CursorXP bạn có thể chọn cho mình hình dạng một con trỏ chuột thật ưng ý trong ô Scheme.

Nhưng chỉ với tiện ích đơn giản đó thì bạn chỉ cần tải CursorXPFree130 cũng tại địa chỉ http://www.stardock.com/ và những theme về con trỏ chuột mà bạn thật ưng ý về là được. Sự khác biệt giữa hai phần mềm tính phí và free này là ở phần hiệu ứng đặc biệt Special effects.



Tại đây bạn có thể chọn cho mình hiệu ứng khi bấm phải chuột, trái chuột, nhấn đúp chuột như những vòng

nhỏ màu đỏ, xanh, những đốm lửa bằng cách nhấn phải chuột vào phần tương ứng và chọn một trong những hiệu ứng từ menu. (Hình 4) và chọn Apply để xác nhận sự lựa chọn và Sound



Với lựa chọn tương tự bạn có thể lựa chọn cho mình âm thanh mà mình ưa thích ở bảng. Bây giờ bạn có thể thoải mái tận hưởng cảm giác mà CursorXP Plus mang lại. Bản Plus bắt buộc phải trả tiền mới được download nhưng bạn có thể nhò Google để tải được ở nơi khác.

LÀM ĐẸP CHO WINDOWS XP VỚI STYLE XP

Có lúc nào bạn nghĩ sao con computer của mình nó không được xì tin lắm nhỉ , nhan sắc thì cũng thường thôi , mình phải làm đẹp cho nó thôi . Các bạn chắc đã nghe đến nhiều chương trình làm đẹp cho win xp . Hôm nay tôi xin giới thiệu cùng các bạn phần mềm Style XP thay đổi tất tần tật những gì có liên quan đến giao diện hay icon … của win xp chỉ bằng cách click và click .

Các bạn có thể tìm thấy Style XP trên các đĩa phần mềm trên thị trường.

Sau khi cài đặt bạn sẽ thấy các mục :

-Option : Bạn có thể cho hay không Style XP khởi động ở mục Enable Style XP, đổi giao diện ở Style XP background ,chay luc khởi động run at startup …

-Themes : Bạn có thể chọn rất nhiều theme ở mục themes có hình minh họa kế bên để bạn xem thử, bạn có thể xem thêm về Background hay sound ở mục Themes parts . Ở mục Themes tools bạn co thể tạo ,mở Display Properties , đổi tên Themes , hay là quay trở về WinXP mặc định, ở mục Preview bạn có thể chọn ,thêm hay là xóa themes đã chọn. Để thêm : Bạn chọn add a new theme (nếu đã có trên máy) hay download (nếu máy có kết nối internet), bạn chỉ đưởng dẫn đến file và chọn open . Sau khi thay đổi hợp lý bạn có thể chọn bằng cách nhấn Apply Theme.

-Visual style: Bạn có thể thay đổi cho hợp ý mình hơn với visual themes , color schemes , font size : thường , lớn hay là rất lớn , mở display properties. Bạn có thể chọn ,thêm mới , hay là xóa đi những gì bạn đã chọn … tương tự như chọn theme.

-Background : Bạn có thể xem hình nền của từng themes, thay đổi vị trí : trung tâm , title hay cả màn hình , chọn màu ở background color , mở display properties. Cuối cùng bạn sẽ chọn , không chọn , thêm , xóa những gì bạn đã chọn , tương tự như chọn theme.

-Logons : Bạn có thể thay đổi cho phù hợp màn hình logons với logons settings , virus free , logon tools và chọn , thêm , xóa những gì bạn đã thay đổi tương tự như mục theme.

-Icons : Bạn có thể sử dụng những icon mặc định hay icons mới (XP- I candy) . Bạn có thể thay đổi kích thước của icons (16x16 , 32x32 , 48x48 , 64x64) .Bạn có thể xem các icons ở khung Preview , chọn , thêm hay xóa những gì bạn đã chọn như ở mục theme.

-Boot screens : bạn có thể thay đổi màn hình khởi động , và thêm vào những hình khởi động mới để thêm phong phú .

-Transparency : bạn có thể làm trong suốt các khung như taskbar , start panel , start menus hay tất cả . Bên dưới là các mức độ làm trong suốt , từ chậm đến nhanh .

-Rotate : Bạn có thể lập một bảng những theme , visual style , background , logon để chúng có thể thay đổi tự động . Tuỳ mức bạn chọn : không bao giờ, lúc khởi động , hàng ngày , hàng tuần mà nó sẽ thay đổi giúp bạn . Thêm vào rotation list bằng nut include , bout ra bằng nút exclude , di chuyển lên trên hay xuống dưới bằng nút move up , move down.

chúc các bạn thật vui và hài lòng với nhan sắc mới của người bạn mình .

LÀM ẨN CHƯƠNG TRÌNH VỚI HIDE WINDOW NOW

Bạn đang viết một bức thư hoặc đang làm một số việc riêng tư trên máy tính mà phải rời đi đâu đó trong một vài phút thì chắc hẳn bạn phải lo lắng không biết lúc đó có ai động vào máy tính của mình không. Nếu bạn sử dụng Screen Saver có kèm password hoặc một số phần mềm khóa màn hình thì chắc hẳn sẽ gây tính tò mò cho những người xung quanh. Lúc này Hide Window Now có lẽ sẽ giúp được cho bạn.

Sau khi khởi động, chương trình sẽ có giao diện như hình:

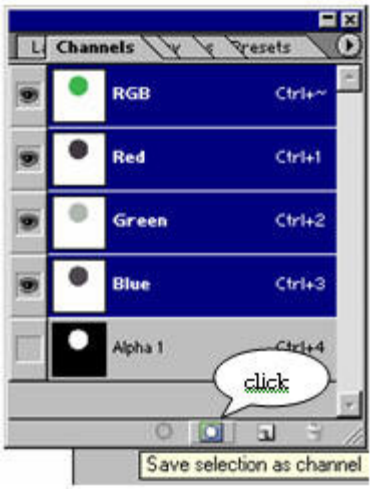
Lúc này bạn chỉ việc chọn những chương trình mà mình không muốn dấu để đánh lừa mắt mọi người trong bảng liệt kê những chương trình mà bạn đang sử dụng bằng cách đánh dấu tích vào ô vuông rồi nhấn nút Hide. Tại thẻ Setting:

Mouse HotKey: cách làm ẩn chương trình bằng các nút của chuột.
Keyboard HotKey: làm ẩn chương trình bằng các phím nóng.
Start with Windows: khởi động chương trình cùng Windows.
Minimize after startup: thu nhỏ sau khi khởi động.
Muting all sounds when hiding windows: tắt tất cả âm thanh sau khi sử dụng chương trình để đề phòng người khác biết được bạn đang làm gì như nghe nhạc hoặc chơi game.
Hide Trayicon when hiding windows: ẩn đi biểu tượng ở thanh taskbar để mọi người không biết bạn đang sử dụng chương trình này.
Password protect hidden windows: đặt password để lỡ có người biết và muốn bật chương trình này lên.

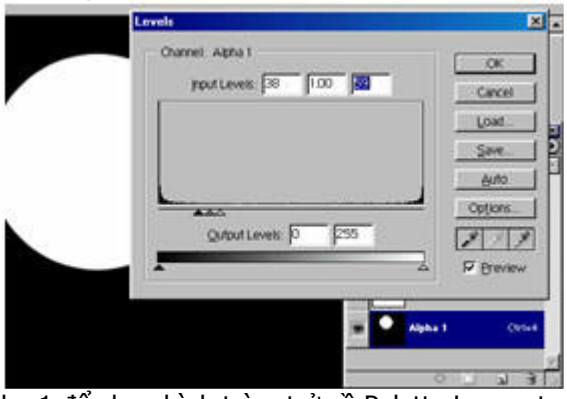
Bạn có thể tải bản dùng thử Hide Window Now với dung lượng 537KB tại địa chỉ http://www.anloer.com/ hoặc mua với giá $15. Mong bạn cảm thấy hài lòng khi sử dụng chương trình này.

KỸ THUẬT KHỬ RĂNG CƯA TRONG PHOTOSHOP

Ơ đây tôi vẽ hình tròn không bị khử răng cưa để minh họa
1. Tạo một tập tin mới kích thước 500 x 300 nền trắng
2. Chọn công cụ Elliptical Marquee Tool(M) bỏ chọn Anti-aliased, nhấn giữ Shift vẽ một hình tròn rồi fill bằng màu xanh 
3. Không bỏ chọn, vào Palette Channels tạo một kênh Alpha 1 như hình



4. Nhấp chọn kênh Alpha 1 và nhấn Ctrl + D để bỏ chọn, vào Filter > Blur > Gaussian Blur chọn Radius là 4.0
5. Vẫn ở kênh Alpha 1, vào Imgae > Adjustment > Levels và điều chỉnh như hình



6. Giữ Ctrl và nhấp vào kênh Alpha 1 để chọn hình tròn, trở về Palette Layers tạo một layer mới rồi fill nó bằng màu xanh như trên
7. Nhấn Z để chọn công cụ Zoom, nhấp phải lên hình chọn Actual Pixels sau đó bạn kéo hình tròn mới ra để so sánh với hình ban đầu bạn sẽ thấy sự khác biệt