5 cách đơn giản tăng cường bảo mật trong Windows 7

Bài viết hướng dẫn bạn tận dụng những tính năng bảo mật tích hợp sẵn trong Windows 7 để PC của bạn được an toàn hơn.

Máy tính chạy Windows 7 của bạn đã được bảo vệ tới đâu?

Đừng bao giờ nghĩ rằng chiếc PC chạy Windows của bạn luôn an toàn trước vấn nạn virus. Mặc dù trên máy đã có cài phần mềm phòng chống virus miễn phí uy tín (Avast, Microsoft Security Essentials) hay phải trả tiền cho những thương hiệu mạnh (Symantec Norton, Kaspersky), bạn vẫn nên tận dụng hết lợi thế của những thiết lập bảo mật được tích hợp sẵn trong Windows 7.

Dưới đây là 5 tính năng bảo mật có thiết lập đơn giản trong Windows 7 giúp bạn giữ máy an toàn hơn.

Action Center

Action Center trong Windows 7 cho phép bạn quan sát và thiết lập chế độ bảo mật cũng như bảo trì hệ thống.

Action Center là trung tâm quản trị bảo mật trên PC, nơi liệt kê và cho phép thiết lập tăng cường bảo mật như tường lửa, cũng như kiểm tra thường xuyên tình trạng bảo trì, bao gồm sao lưu và phục hồi dữ liệu, để đảm bảo chắc chắn là máy của bạn luôn "*sạch*".

Action Center có biểu tượng là lá cờ trắng bên phải thanh công cụ của Windows 7, hoặc có thể truy xuất bằng cách nhấp chuột vào: **Control Panel/System and Security/Action Center**.

Tại cửa sổ Action Center, bạn nên chắc chắn rằng Windows Firewall đang được bật (on), phần mềm phòng chống virus đã được cập nhật

bản mới nhất và hệ thống Windows đang được đặt chế độ tự động cập nhật.

Mỗi khi một mục bảo mật nào đó trong diện giám sát có sự thay đổi, ví dụ phần mềm virus đã quá hạn cập nhật, Action Center đưa ra cảnh báo trên thanh tác vụ taskbar. Khi đó, mở Action Center sẽ thấy mục này có màu đỏ, cho thấy vấn đề là nghiêm trọng, và yêu cầu xử lý.

Action Center hữu ích trong việc cảnh báo cho bạn những rắc rối có thể xảy đến, và hãy nhớ, đừng phớt lờ những cảnh báo do Action Center đưa ra.

Windows Defender

Windows Defender là phần mềm phòng chống spyware, được tích hợp sẵn và chạy tự động (nếu được bật lên) trong Windows 7.

Spyware (phần mềm gián điệp) là bất kỳ phần mềm nào không mong muốn hoặc có thể gây hại, đã âm thầm "chui" vào máy của bạn vào một lúc nào đó bạn không hề biết. Nó có thể lây qua đường Internet, mạng nội bộ, hoặc từ các thiết bị lưu trữ đã bị nhiễm như CD/DVD hay USB.

Windows Defender ngăn chặn spyware theo 2 cách:

• Bảo vệ theo thời gian thực. Windows Defender đưa ra cảnh báo khi

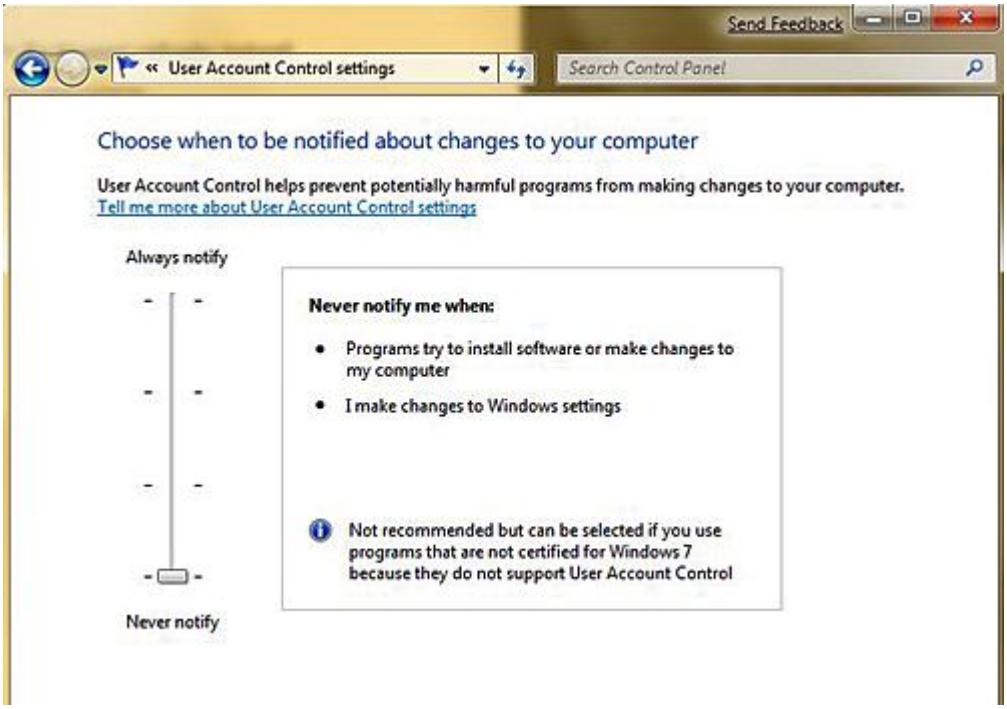
spyware tìm cách tự cài nó vào máy tính hoặc bắt đầu hoạt động. Cảnh báo cũng được đưa ra khi các chương trình tìm cách thay đổi các thiết lập quan trọng trong Windows.

• Tùy chọn quét. Bạn có thể sử dụng Windows Defender để quét phát hiện spyware có thể có trên máy của mình, lên lịch quét thường xuyên, và đặt tùy chọn tự động gỡ bỏ bất cứ thứ gì bị phát hiện là đã nhiễm trong quá trình quét.

Để mở Windows Defender, nhấp chuột vào Start, gõ Defender vào hộp tìm kiếm (search), rồi chọn Windows Defender trong danh sách kết quả hiện lên.

User Account Control

UAC (kiểm soát tài khoản người dùng) là tính năng bảo mật nhắc nhở bạn quyền cài đặt hoặc chạy một chương trình. UAC hỏi nhiều tới mức khiến người dùng Windows Vista khó chịu, nhưng đã được cải tiến trong Windows 7. Tùy chọn không còn đơn giản với on/off mà đã có 4 cấp độ cảnh báo người dùng có thể đặt.



Windows 7 UAC có 4 mức cảnh báo.

Windows 7 UAC thông báo cho bạn biết khi một chương trình tạo sự thay đổi có thể gây hại cho máy hoặc khiến hệ thống dễ bị tấn công.

Nếu bạn có quyền quản trị (đa phần là như vậy), bạn chấp nhận (chọn "Yes") để tiếp tục. Nếu tài khoản Windows bạn đang dùng không phải là quản trị, sẽ cần nhập mật khẩu của một tài khoản quản trị để tiếp tục.

Khi hệ thống yêu cầu bạn quyền để chạy hoặc cài đặt một phần mềm, UAC sẽ bật lên một hộp thoại, nhắc bạn một trong bốn câu sau, tùy theo tình huống:

• Chương trình hay thiết lập là một phần của Windows và cần có

quyền (administrator) mới thực hiện được.

• Chương trình không thuộc Windows và cần có quyền mới thực hiện được.

• Chương trình chưa được nhận biết và cần có quyền mới thực hiện được.

• Chương trình đã bị chặn bởi người quản trị hệ thống vì chưa được nhận biết hoặc không đáng tin cậy.

Để sửa các thiết lập đối với UAC, nhấp chuột vào Start, và chọn Control Panel. Trong hộp tìm kiếm, gõ uac rồi chọn Change User Account Control Settings.

Windows Update

Windows Update nhiều khi có thể gây phiền hà cho bạn. Đó là lúc nó liên tục đề nghị khởi động lại máy sau khi có bản cập nhật quan trọng đã được tự động tải về và cài đặt lên hệ thống. Nhưng, nhờ vậy mà PC của bạn được nâng cấp chế độ bảo mật với những bản vá mới nhất của Windows, trong khi bạn chẳng mất công gì cả.

Bạn có thể thiết lập cho Windows luôn luôn tự động cài các bản cập nhật hay chỉ những bản "quan trọng" mà thôi. Các bản cập nhật quan trọng là những bản vá cho các lỗ hổng bảo mật được xác định là

“nghiêm trọng”. Ngoài ra, còn có các bản cập nhật “khuyến nghị” dành cho những vấn đề ít quan trọng hơn.

Để bật tính năng tự động cập nhật cho Windows Updates, thực hiện các thao tác sau:

• Nhấp chuột vào Start, rồi gõ Update vào trong hộp tìm kiếm, sau đó chọn Windows Update trong danh sách kết quả.

• Trên cửa sổ bên trái, chọn Change Settings.

• Dưới Important Updates (cập nhật quan trọng), bạn có thể chọn nếu muốn các bản cập nhật mới được tự động tải về và cài đặt lên máy, kèm theo là giờ hẹn cập nhật hàng ngày mà bạn cho là thích hợp.

• Dưới Recommended Updates (cập nhật theo khuyến nghị) chọn vào hộp "Give me recommended updates the same way I receive important updates", rồi nhấp chuột vào nút OK.

Windows Firewall

Windows Firewall là tính năng tường lửa trong Windows với hai lựa chọn on/off nhằm giúp ngăn chặn tin tặc và sâu máy tính tìm cách xâm nhập vào máy tính của bạn thông qua mạng nội bộ hay Internet. Tường lửa còn có tác dụng chặn máy tính của bạn, khi đã bị nhiễm, không cho gửi phần mềm độc hại đến các máy tính khác trong mạng.

Trừ khi máy của bạn đã nằm trong vùng an toàn nhờ có một tường lửa ngăn cách, như tường lửa mạng doanh nghiệp chẳng hạn, bạn nên bật tính năng Windows Firewall để bảo vệ máy của mình cũng như an toàn cho mạng nội bộ.

Để bật tính năng Windows Firewall, thực hiện như sau:

• Nhấp chuột vào Start, và chọn Control Panel. Gõ firewall vào hộp tìm kiếm, rồi chọn Windows Firewall.

• Trên cửa sổ bên trái, chọn "Turn Windows Firewall on or off". Nếu bạn được nhắc nhập mật khẩu quản trị (administrator) thì gõ vào mật khẩu của một tài khoản quản trị.

• Chọn bật Windows Firewall dưới mỗi mạng nội bộ mà bạn muốn bảo vệ, rồi chọn OK.

Chú ý: Nếu máy tính của bạn được nối với một mạng doanh nghiệp, các thiết lập của mạng này có thể ngăn bạn bật Windows Firewall.

Theo PCWorld VN

Tăng cường bảo mật cho hệ điều hành Mac

Trên tình hình thực tế hiện nay dựa trên các cuộc khảo sát đối với người sử dụng Mac OS, phần lớn họ đều không có bất cứ phương pháp bảo mật nào, và số ít người dùng có kinh nghiệm mới có thể nhận biết được những sự thay đổi trong hệ thống. Thêm 1 điều cần chú ý rằng rất nhiều người nghĩ hệ điều hành Mac OS không bao giờ bị nhiễm virus hoặc an toàn tuyệt đối. Và tất cả họ đều nhầm, vì hiện nay đã xuất hiện khá nhiều phần mềm bảo mật giả mạo đã xuất hiện và lây lan ngày càng nhanh với quy mô khó có thể kiểm soát được. Trong bài viết dưới đây, chúng tôi sẽ giới thiệu với các bạn một số công cụ hỗ trợ người sử dụng trong quá trình chống lại hiểm họa từ Internet.

Từ trước đến nay, hệ thống bảo mật của Mac OS X vẫn đáp ứng đủ nhu cầu của một số bộ phận người dùng thông thường, nhưng vẫn chưa thực sự hoàn thiện trước trình độ của những kẻ tin tặc hiện nay. Thực chất, hệ điều hành

Snow Leopard đã được tích hợp sẵn một số dịch vụ phát hiện và phòng chống các phần mềm độc hại, nhưng lại chỉ tỏ ra hữu ích khi hệ cơ sở dữ liệu được cập nhật theo định kỳ, tương tự như ứng dụng Sophos. Còn OS X là hệ thống UNIX – với cấu trúc tài khoản người dùng cũng như phân quyền các cấp rất phức tạp, nhưng virus hoặc các chương trình mã độc không cần đến quyền quản trị cao nhất để đánh cắp thông tin cá nhân của bạn.

Gần đây nhất, sự xuất hiện của Mac Defender cũng như một số biến thể đi kèm như **MacSecurity** và **MacProtector**, đã "thu hút" được nhiều sự quan tâm từ người sử dụng cũng như các công ty an ninh mạng. Với thủ đoạn tương tự như với Windows, chúng dẫn dắt người dùng bằng những đoạn thông tin cảnh báo giả mạo, làm cho họ tin rằng hệ thống đang dùng đã bị nhiễm virus... đã có không ít người bị lâm vào tình trạng nguy kịch.

1. Little Snitch:

Thực chất, Little Snitch không phải là ứng dụng diệt virus hoặc malware như chúng ta thường biết đến. Đơn giản đây chỉ là 1 dịch vụ bảo mật hoạt động ở chế độ ngầm, với chức năng tương tự như Firewall. Bất cứ chương trình nào muốn "giao tiếp" với hệ thống hoặc Internet... đều phải "đi qua" Little Snitch. Mỗi khi ứng dụng nào thực hiện 1 yêu cầu kết nối, Little Snitch sẽ hiển thị 1 cửa sổ pop – up yêu cầu người dùng chấp nhận hoặc từ chối hoạt động của chương trình đó, đi kèm với đó là lựa chọn tạm thời hoặc chấp nhận vĩnh viễn, thiết lập quy luật – Rule cố định. Bên cạnh đó,

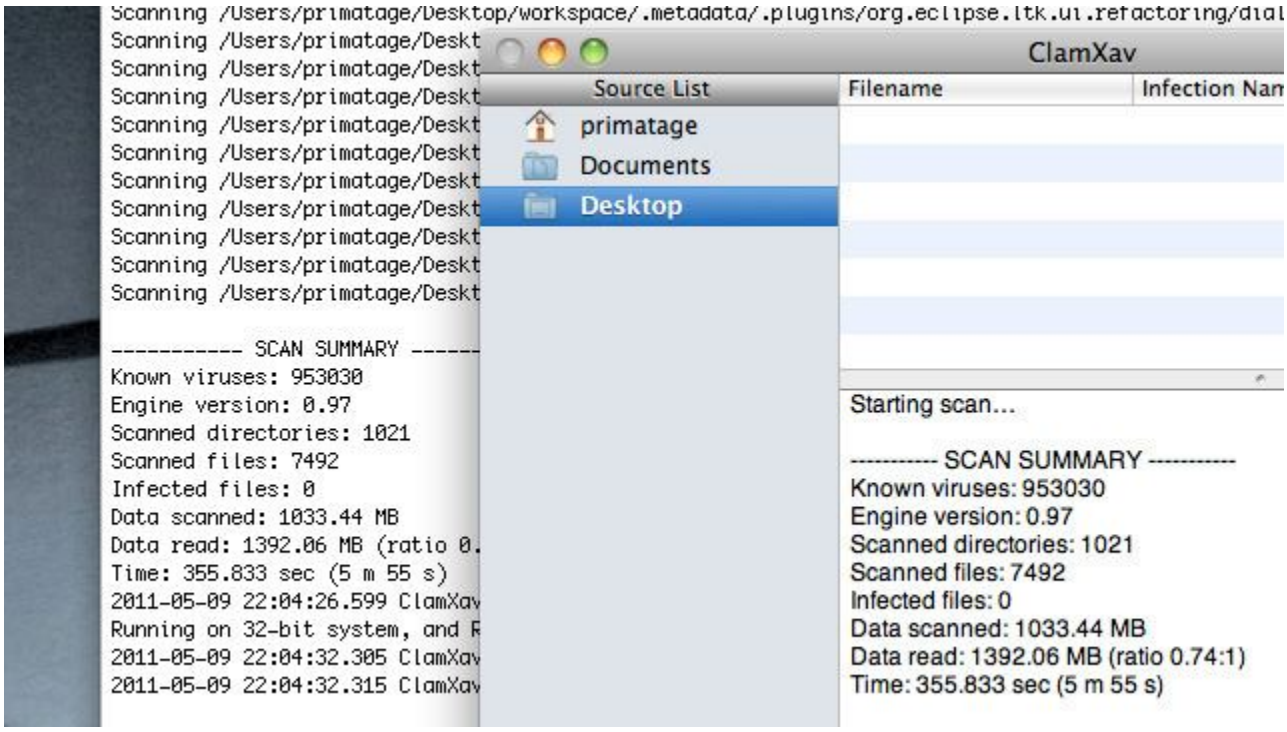
Little Snitch còn có chức năng hiển thị chính xác những hoạt động nào đang diễn ra, các chương trình đang "liên lạc" qua Internet. Chương trình có thời hạn dùng thử, và mức giá 29,99$ bản quyền.

2. Sophos Free Antivirus dành cho Mac:

Như tất cả chúng ta đã biết, Sophos hiện đang là 1 trong những thương hiệu nổi tiếng nhất thế giới trong lĩnh vực phòng chống virus và malware dành cho mô hình công nghiệp. Và phiên bản **Sophos Free Antivirus** miễn phí dành cho hệ điều hành Mac OS là một sự lựa chọn sáng

suốt khi người dùng cảm thấy không yên tâm. Giao diện điều khiển chính của chương trình rất đơn giản và dễ sử dụng, thậm chí bạn còn có thể nâng cấp lên phiên bản trả phí chỉ với 1 thao tác duy nhất – nhấn nút Upgrade, với nhiều tính năng vượt trội khác. Được đi kèm với file gỡ bỏ – Uninstaller, hỗ trợ chế độ quét các phân vùng, ổ đĩa khác trong cùng hệ thống mạng, chương trình có khả năng nhận dạng và tiêu diệt những mối nguy hiểm mới nhất (với điều kiện người dùng luôn phải cập nhật cơ sở dữ liệu), tuy nhiên đối với những loại mã độc hoặc chương trình có khả năng gây hại nhưng chưa được nhận biết, Sophos sẽ hiển thị dưới dạng unknown malware threats. Một điểm mạnh rất đáng chú ý của Sophos là gần như không ảnh hưởng đến tốc độ và hiệu suất làm việc của hệ điều hành, cũng như các chương trình bên trong hệ thống.

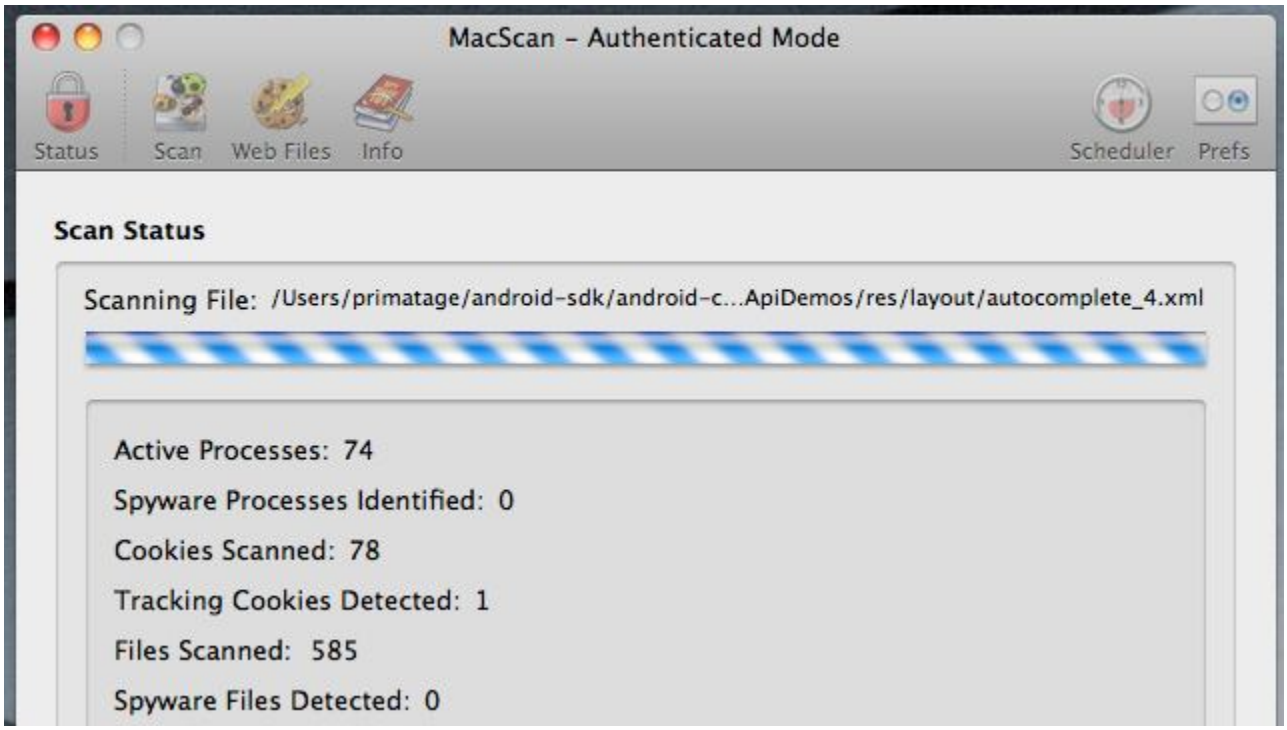
3. ClamXav:



ClamXav – Clam Antivirus dành cho Mac OS X có thể gây đôi chút khó khăn cho những người dùng ít kinh nghiệm, nhưng thực ra lại rất đơn giản và mạnh mẽ trong lĩnh vực bảo mật. Gần như không để lại "dấu vết" nào trong quá trình hoạt động, luôn chạy ở chế độ ngầm – Background, người sử dụng sẽ luôn cảm thấy an tâm khi truy cập bất cứ thư mục hoặc file dữ liệu nào với sự hiện diện của ClamXav. Cơ chế cập nhật cơ sở dữ liệu luôn được cập nhật hàng ngày, và bên cạnh đó, toàn bộ hoạt động của người dùng luôn được kiểm soát trong mức độ

cho phép. Mỗi khi bạn tiến hành quét toàn bộ hệ thống hoặc áp dụng với 1 phân vùng, thư mục nhất định nào đó, chỉ cần ngồi trước màn hình và theo dõi dữ liệu được ghi vào file LOG. ClamXav là ứng dụng mã nguồn mở và tất nhiên, hoàn toàn miễn phí.

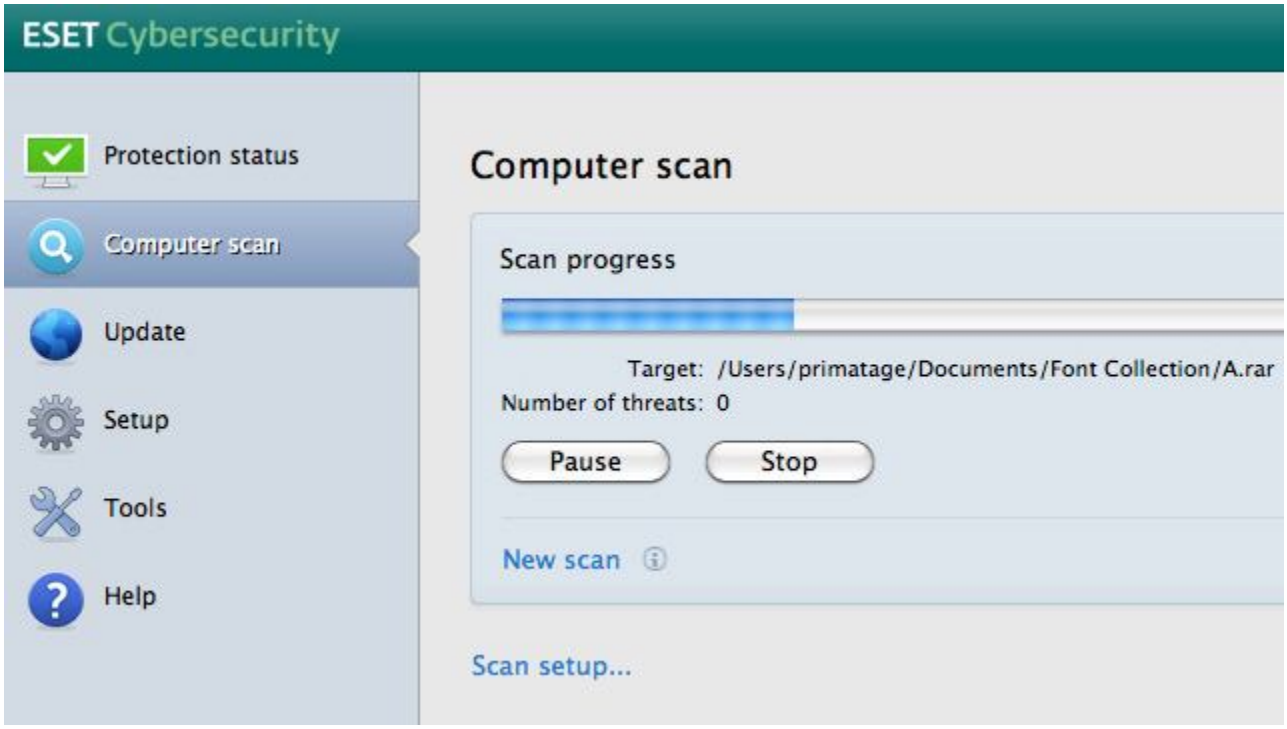
4. MacScan;



Khi sử dụng, chắc hẳn mọi người sẽ ít nhiều ngạc nhiên vì **MacScan** không giống với những chương trình thông thường, thay vì hoạt động ở chế độ **Background**, ứng dụng được chạy trực tiếp bởi tài khoản người dùng, và tắt bỏ khi

kết thúc. Khi hoạt động, chương trình sẽ tự động dò tìm tất cả các thông tin, dấu hiệu có liên quan đến malware, nhưng có đôi chút khác biệt với phần lớn ứng dụng bảo mật khác trong việc xác định cookies. Tính năng này có thể thật sự không quan trọng, nhưng lại gây ra đôi chút phiền phức cho người dùng vì hiển thị nhiều bảng thông báo chô người sử dụng. Mặt khác, nếu các bạn muốn nâng cấp lên phiên bản đầy đủ chức năng (với mức giá 29,99$) thì sẽ gặp khó khăn trong khâu thực hiện, do vậy bản miễn phí vẫn được phần lớn mọi người sử dụng.

5. ESET Cybersecurity dành cho Mac:



Hãng công nghệ ESET, cũng giống như Sophos trong lĩnh vực bảo mật với mô hình công nghiệp. Nếu bạn đang muốn tìm giải pháp an ninh mạng toàn diện dành cho hệ thống Mac của mình thì ESET Cybersecurity là 1 sự lựa chọn không thể tốt hơn. Gần như không ảnh hưởng đến tốc độ và hiệu suất làm việc của máy tính, luôn hoạt động ở chế độ ngầm, giao diện đơn giản, thân thiện và dễ sử dụng... là những điểm đáng chú ý của ESET Cybersecurity. Dựa vào các quá trình thử nghiệm trên thực tế, tỉ lệ phát hiện và tiêu diệt thành công những mối nguy hiểm, ví dụ như virus,

trojan, mã độc, malware... luôn cao hơn so với những sản phẩm cùng loại trên thị trường. Thời hạn dùng thử của chương trình là 30 ngày, nhưng nếu muốn sở hữu toàn bộ tính năng của **ESET Cybersecurity,** các bạn chỉ phải bỏ ra 39,99$ trong vòng 1 năm.

6. Kaspersky Antivirus dành cho Mac:

Phiên bản Antivirus của Kaspersky dành cho hệ điều hành Mac OS khá giống với ESET, đầy đủ chức năng, giao diện dễ sử dụng, hỗ trợ khả năng kiểm tra đường dẫn dành cho một số trình duyệt như Chrome, Safari, và Firefox... Toàn

bộ các mục thiết lập được gói gọn trong phần Preference của chương trình, thời hạn dùng thử tối đa là 30 ngày, còn nếu muốn nâng cấp lên phiên bản đầy đủ, người sử dụng chỉ cần bỏ ra 39,99$ cho 1 năm.

7. Một số ứng dụng khác:

Bên cạnh những chương trình bảo mật chúng tôi đã đề cập ở phía trên của bài viết, các bạn có thể tham khảo thêm 2 lựa chọn khác là iAntiVirus và VirusBarrier Express, cũng được trang bị khá đầy đủ chức năng bảo mật cơ bản, hoàn toàn miễn phí. Nhưng với VirusBarrier Express thì các bạn cần cân nhắc trước khi quyết định, vì ứng dụng này thường có xu hướng yêu cầu người dùng nâng cấp lên phien bản trả phí - VirusBarrier Plus. Hy vọng những thông tin trên có thể giúp mọi người trong việc tự bảo vệ chiếc máy tính của mình trước những hiểm họa ngày càng nhiều trên Internet ngày nay. Chúc các bạn thành công!

T.Anh (theo Life Hacker)

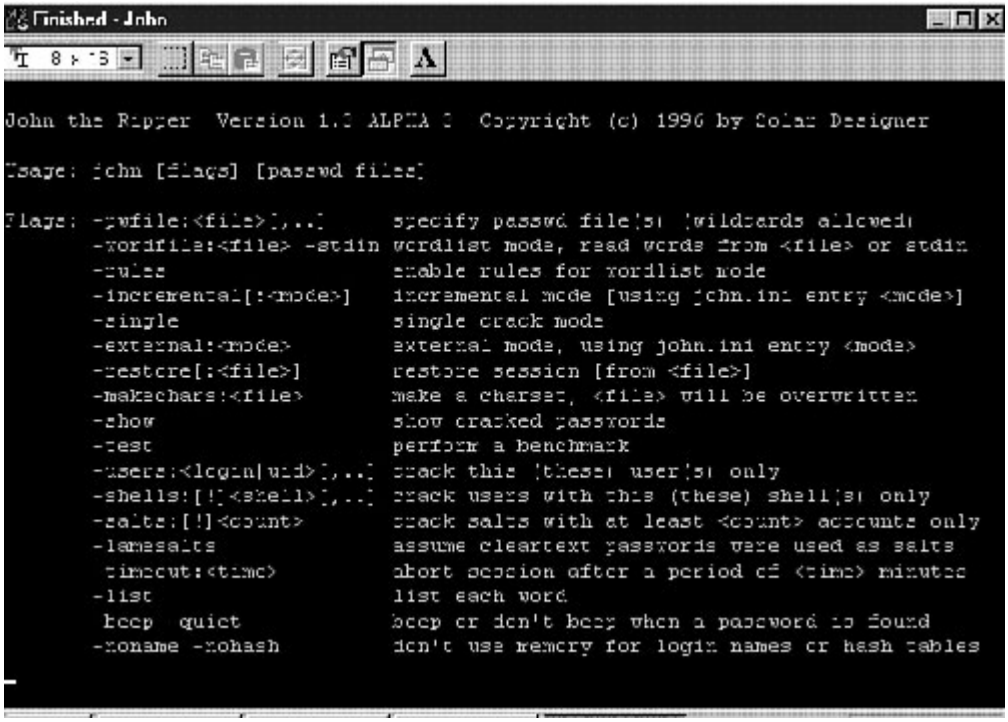
10 công cụ bảo mật và Hacking tốt nhất cho Linux

Nguồn : quantrimang.com

Quản trị mạng - *Linux chính là hệ điều hành máy tính giấc mơ của các hacker. Nó hỗ trợ rất nhiều các công cụ và tiện ích cho việc bẻ khóa các mật khẩu, quét các lỗ hổng mạng và phát hiện những xâm nhập có thể. Chúng tôi đã sưu tập một bộ khoảng 10 công cụ tốt nhất trong việc hacking và bảo mật cho Linux. Tuy nhiên các bạn cần lưu ý rằng các công cụ này không có nghĩa là đều có hại.*

1. John the Ripper

John the Ripper là một công cụ phần mềm bẻ khóa mật khẩu ban đầu được phát triển cho hệ điều hành Unix. Nó là một trong những chương trình testing/breaking mật khẩu phổ biến nhất vì có kết hợp một số bộ cracker mật khẩu trong cùng một gói phần mềm, tự động phát hiện các kiểu mật khẩu và có một bộ cracker có khả năng tùy chỉnh. Công cụ này có thể được chạy cho các định dạng mật khẩu đã được mã hóa chẳng hạn như các kiểu mật khẩu mã hóa vẫn thấy trong một số bản Unix khác (dựa trên DES, MDS hoặc Blowfish), Kerberos AFS và Windows NT/2000/XP/2003 LM hash. Bên cạnh đó còn có các mođul bổ sung mở rộng khả năng gồm có cả các kiểu mật khẩu MD4 và các mật khẩu được lưu trong LDAP, MySQL và các thành phần khác.



2. Nmap

Nmap là một trình quét bảo mật mạng được nhiều người ưa thích. Nó được sử dụng để phát hiện các máy tính và các dịch vụ trên mạng máy tính, sau đó sẽ tạo một “bản đồ” mạng. Cũng giống như các bộ quét cổng đơn giản, Nmap có khả năng phát hiện các dịch vụ thụ động (passive) trên một mạng dù các dịch vụ như vậy không tự khuyếch trương bản thân chúng bằng một giao thức phát hiện dịch vụ. Thêm vào đó, Nmap có thể phát hiện các thông tin chi tiết khác nhau về các máy tính từ xa. Chúng có thể phát hiện ra hệ điều hành, kiểu thiết bị, thời gian và sản phẩm phần mềm chạy dịch vụ, số phiên bản chính xác của sản phẩm đó, sự hiện diện của một số công nghệ tường lửa trên một mạng nội bộ hoặc thậm chí cả hãng sản xuất card mạng từ xa.

Nmap chạy trên Linux, Microsoft Windows, Solaris, và BSD (gồm có Mac OS X), và trên cả AmigaOS. Linux là một nền tảng của nmap phổ biến nhất còn Windows là thứ hai.

3. Nessus

Nessus là một phần mềm quét lỗ hổng khá toàn diện. Mục tiêu của nó là phát hiện các lỗ hổng tiềm ẩn trên các hệ thống được kiểm tra chẳng hạn như:

- Vulnerabilities that allow a remote cracker to control or access sensitive data on a system.

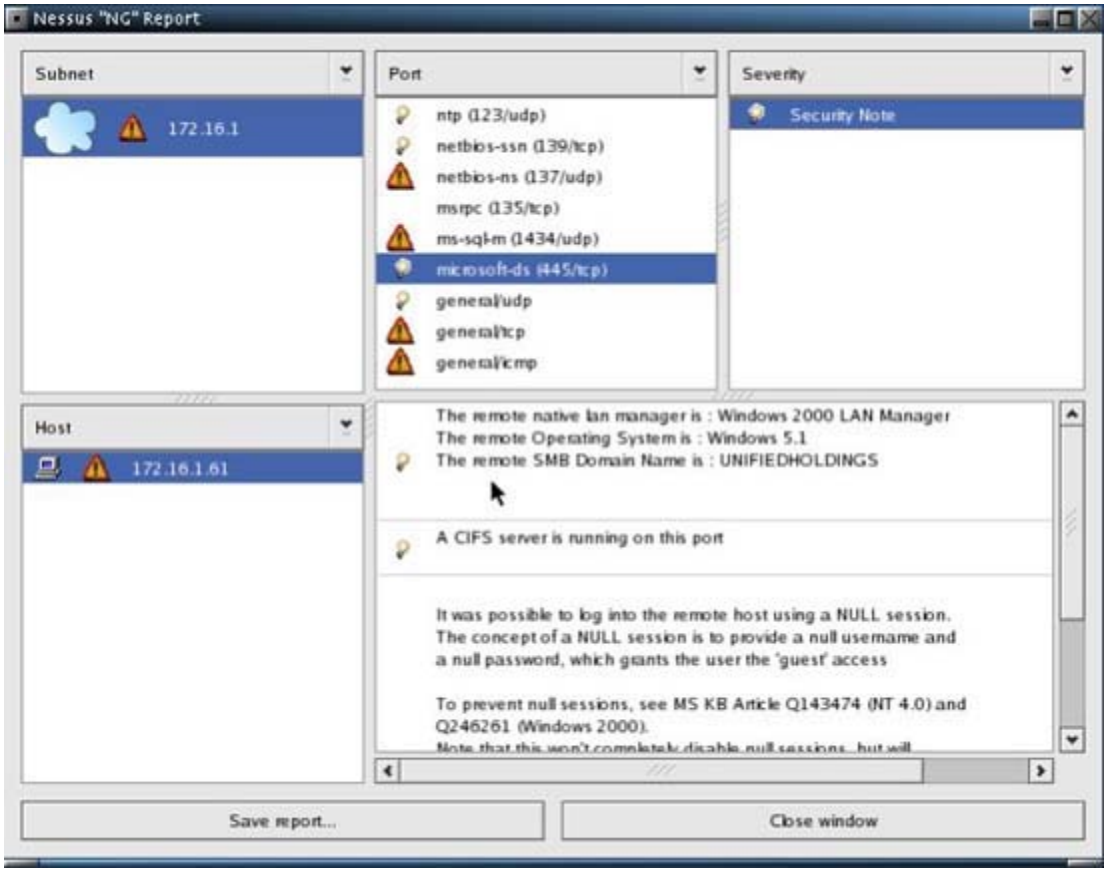
- Các lỗ hổng cho phép cracker từ xa có thể kiểm soát hoặc truy cập các dữ liệu nhạy cảm trên hệ thống.

- Lỗi cấu hình (ví dụ như mở mail relay, mất các bản vá,…)

- Các mật khẩu mặc định, một số mật khẩu chung, các một khẩu blank/absent (trắng hay thiếu) trên một số tài khoản hệ thống. Nessus cũng có thể gọi Hydra (một công cụ bên ngoài) để khởi chạy một tấn công dictionary.

- Từ chối dịch vụ đối với ngăn xếp TCP/IP bằng bằng sử dụng các gói dữ liệu đã bị đọc sai.

Nessus là một trình quét lỗ hổng phổ biến nhất hiện nay trên thế giới, ước lượng có đến 75.000 tổ chức trên toàn thế giới sử dụng. Nó xuất hiện lần đầu tiên trong bảng thống kê các công cụ bảo mật 2000, 2003 và 2006 cúa SecTools.Org.

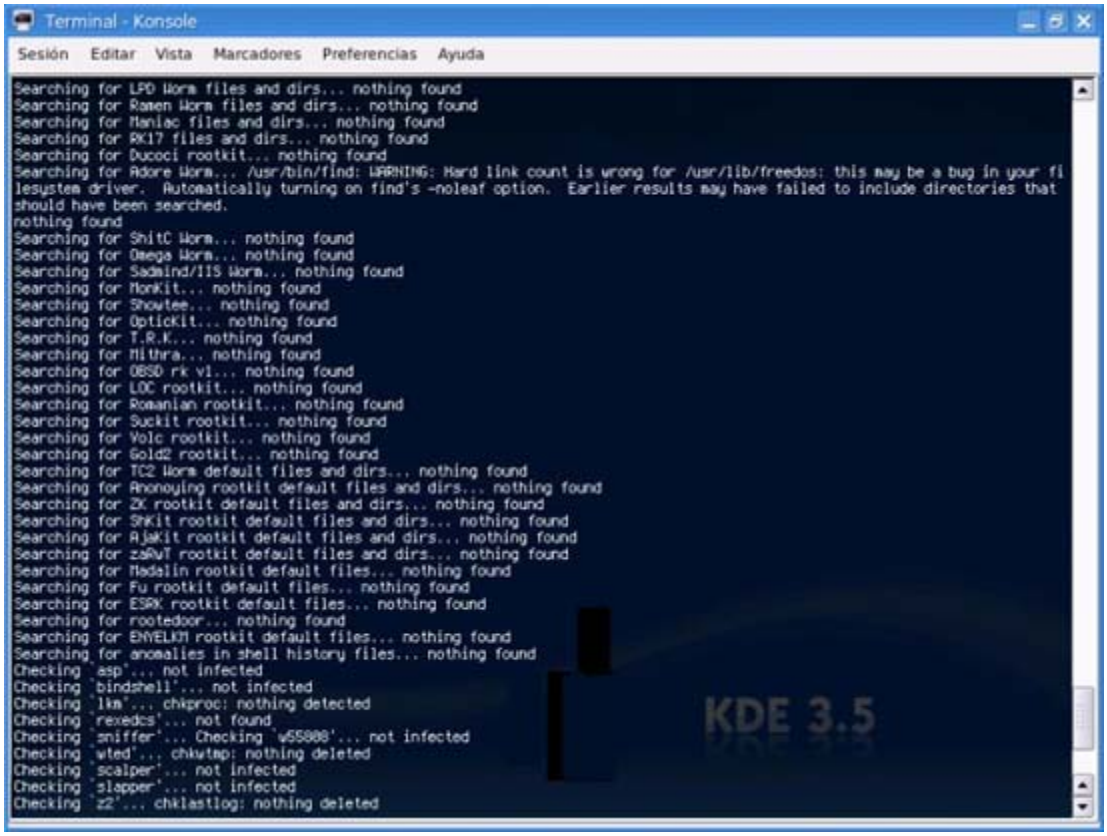


4. chkrootkit

Chkrootkit (Check Rootkit) là một chương trình của Unix nhằm giúp các quản trị viên hệ thống kiểm tra hệ thống của họ về các rootkit. Nó là một kịch bản sử dụng các công cụ UNIX/Linux giống như các chuỗi và các lệnh grep để tìm kiếm các dấu hiệu trong các chương trình hệ thống lõi và so sánh sự mâu thuẫn của /proc filesystem với đầu ra của lệnh ps (process status) nhằm tìm kiếm những vấn đề khác nhau.

Chương trình này có thể được sử dụng từ một “đĩa giải cứu” hoặc có có thể sử dụng một thư mục khác để chạy tất cả các lệnh của riêng nó.

Tuy vậy vẫn có một số hạn chế cố hữu về độ tin cậy của bất cứ chương trình nào muốn phát hiện sự thỏa hiệp (chẳng hạn như các rootkit và các virus máy tính). Các rootkit mới hơn có thể phát hiện và thỏa hiệp các copy của các chương trình chkrootkit hoặc dùng các thủ đoạn khác để vòng tránh sự phát hiện bởi chương trình này.

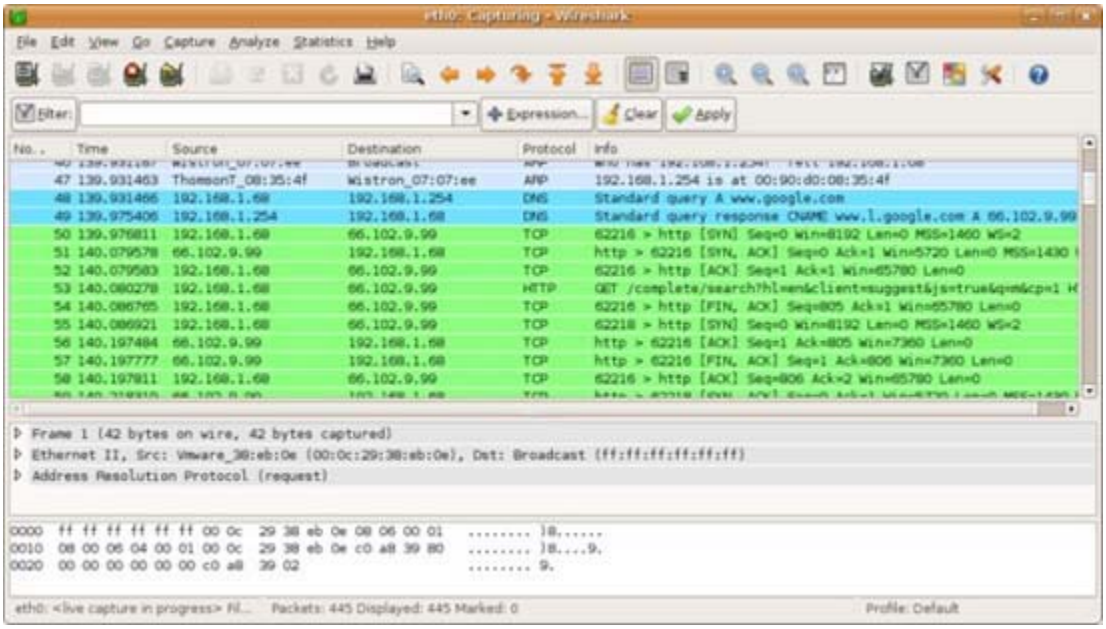


5. Wireshark

Wireshark là môt ứng dụng được sử dụng để khắc phục sự cố mạng, phân tích, phần mềm và phát triển giao thức truyền thông. Vào tháng 6 năm 2006, dự án đã được đổi tên thành Ethereal do một số vấn đề về tên thương mại.

Wireshark cung cấp các chức năng giống như tcpdump, tuy nhiên nó lại có giao diện đồ họa người dùng và nhiều thông tin khác cũng như các tùy chọn. Chương trình này cho phép người dùng có thể quan sát tất cả lưu lượng trên mạng (thường là mạng Ethernet nhưng cũng hỗ trợ các tùy chọn khác).

Wireshark sử dụng cross-platform GTK+ widget toolkit và là cross-platform, chạy trên nhiều hệ điều hành khác nhau chẳng hạn như Linux, Mac OS X và Microsoft Windows. Được phát hành dưới dạng GNU General Public License và đây là một phần mềm miễn phí.



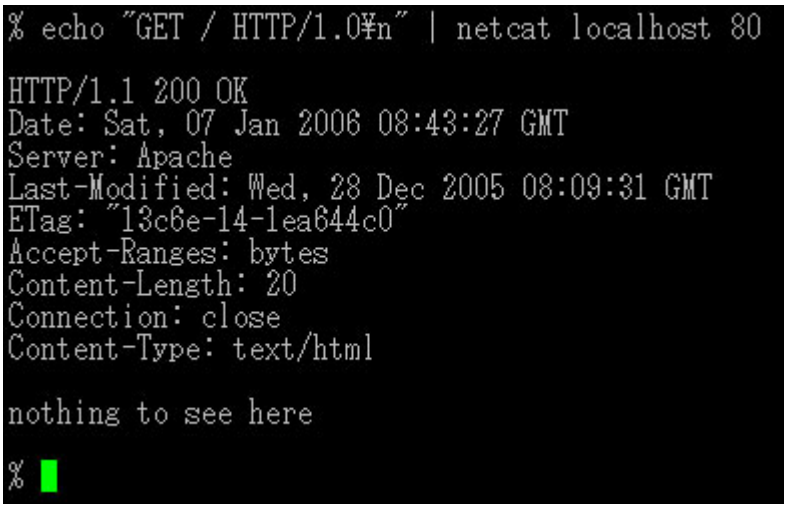
6. Netcat

Netcat là một tiện ích mạng dành để đọc và ghi các kết nối mạng TCP hoặc UDP.

Phần mềm này được bình chọn là công cụ bảo mật mạng hữu dụng thứ hai vào năm 2000 do insecure.org bình chọn. Đứng thứ tư vào năm 2003 và giữ nguyên vị trí đó cho đến cuộc bình chọn năm 2006.

Phiên bản ban đầu của netcat là một chương trình UNIX. Tác giả viết chương trình này đã phát hành phiên bản 1.1 và tháng Ba năm 1996.

Netcat có khả năng tương thích POSIX và những bổ sung đang tồn tại, có thể ghi đè với tính năng GNU netcat.

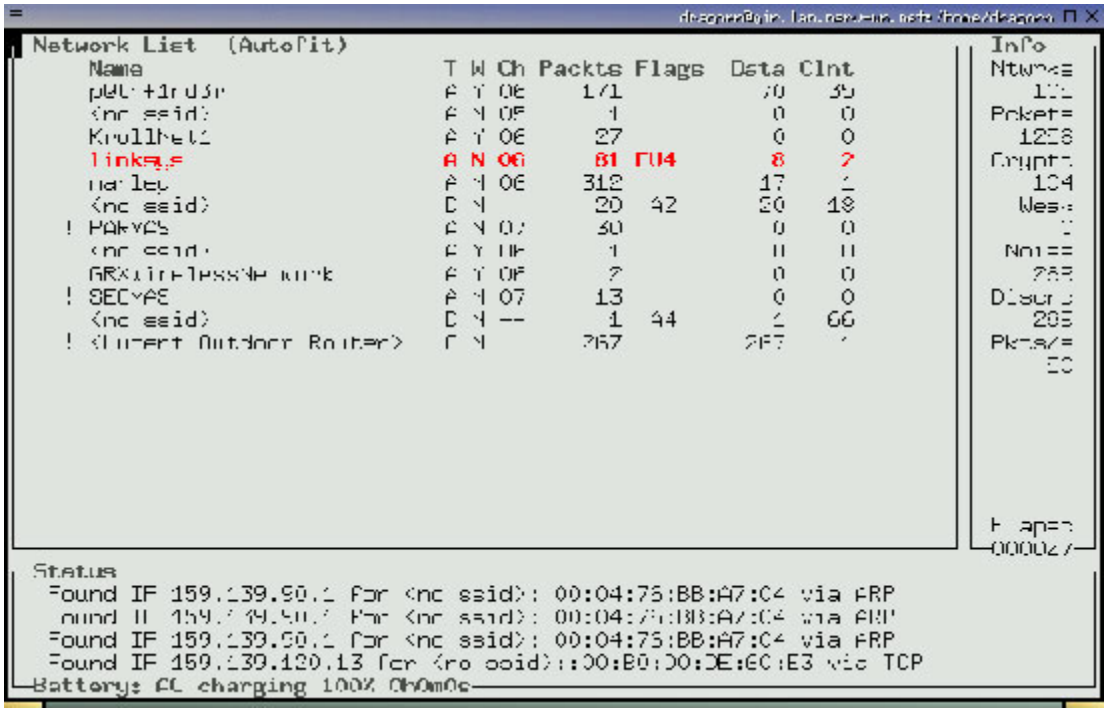


7. Kismet

Kismet là một bộ phát hiện, kiểm tra dữ liệu và hệ thống phát hiện xâm phạm cho các mạng LAN không dây 802.11. Nó làm việc với bất cứ card không dây nào có hỗ trợ chế độ kiểm tra các mưu đồ bất lương, bên cạnh đó còn có thể sử dung để kiểm tra lưu lượng của các chuẩn 802.11a, 802.11b và 802.11g.

Kismet không giống như hầu hết các bộ phát hiện mạng không dây khác ở tính thụ động. Điều này có nghĩa rằng không cần gửi bất kỳ một gói tin có thể ghi nào, nó vẫn có thể phát hiện sự hiện diện của các điểm truy cập không dây, các máy khách không dây và mối liên quan giữa chúng.

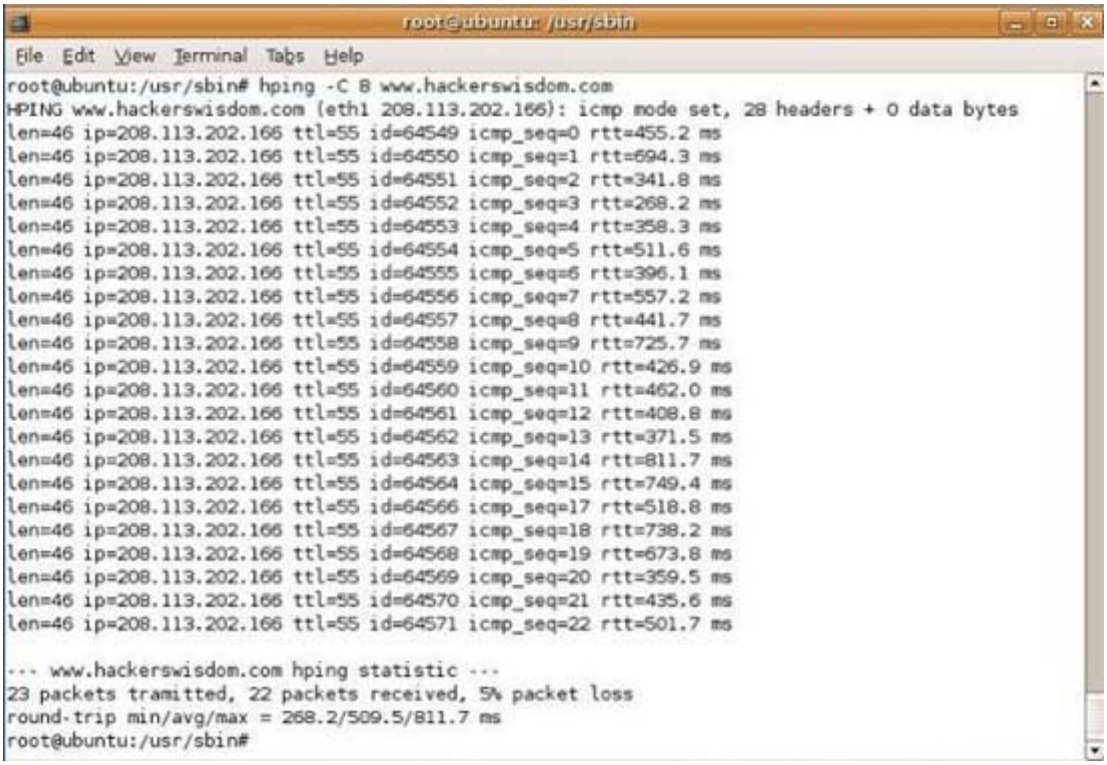
Công cụ này cũng có các tính năng cơ bản của một IDS không dây, chẳng hạn như phát hiện các chương trình kiểm tra ở chế độ tích cực NetStumbler cũng như một số các tấn công mạng không dây khác.



8. Hping

Hping là một bộ tạo và phân tích gói cho giao thức TCP/IP. Đây là một trong những công cụ hữu hiệu cho việc thẩm định bảo mật và kiểm tra các tường lửa và các mạng, nó được sử dụng để khai thác các kỹ thuật quét nhàn rỗi (cũng được dự định bởi chính tác giả viết ra nó) và hiện được bổ sung thêm trong Nmap Security Scanner. Phiên bản mới của hping là hping3 có khả năng tạo kịch bản bằng cách sử dụng ngôn ngữ Tcl và thực thi một cơ chế dựa trên chuỗi, mô tả các gói TCP/IP có thể đọc để các lập trình viên có thể viết các kịch bản để thao tác ở các gói TCP/IP mức thấp và phân tích trong thời gian rất ngắn.

Giống như các công cụ khác được sử dụng cho việc bảo mật máy tính, hping cũng rất hữu dụng cho cả các quản trị viên hệ thống và các cracker (hoặc những người mới viết kịch bản).



9. Snort

Snort là một chương trình mã nguồn mở, miễn phí, nó có khả năng phát hiện sự xâm nhập mạng và ngăn chặn sự xâm nhập này bằng viêc thực hiện ghi các gói và phân tích lưu lượng theo thời gian thực trên các mạng IP.

Snort thực hiện phân tích giao thức, searching/matching nội dung và được sử dụng để khóa (chủ động) hoặc phát hiện (thụ động) các tấn công hay những sự thăm dò chẳng hạn như tràn bộ đệm, việc quét trái phép các cổng, tấn công ứng dụng web, thăm dò SMB và nhiều tính năng khác nữa. Phần mềm này được sử dụng nhiều nhất cho mục đích ngăn chặn sự xâm nhập bằng cách khóa chặn các tấn công khi chúng bị phát hiện. Snort có thể được kết hợp với các phần mềm khác như SnortSnarf, sguil, OSSIM và Basic Analysis and Security Engine (BASE) để cung cấp một trình diễn mang tính trực giác đối với dữ liệu xâm phạm.

```
Snort ran for 0 Days 0 Hours 1 Minutes 8 Seconds
Packet analysis time averages:

Snort Analyzed 524 Packets Per Minute
Snort Analyzed 7 Packets Per Second

Snort received 524 packets
    Analyzed: 521(99.427%)
    Dropped: 0(0.000%)
    Outstanding: 3(0.573%)
===================================
Breakdown by protocol:
    TCP: 354         (67.946%)
    UDP: 18          (3.455%)
   ICMP: 50          (9.597%)
    ARP: 34          (6.526%)
  EAPOL: 0           (0.000%)
   IPv6: 0           (0.000%)
ETHLOOP: 11          (2.111%)
    IPX: 0           (0.000%)
   FRAG: 0           (0.000%)
  OTHER: 54          (10.365%)
DISCARD: 0           (0.000%)
===================================
Action Stats:
ALERTS: 26
LOGGED: 26
PASSED: 0
```

10. tcpdump

Tcpdump là một công cụ gỡ rối các vấn đề về mạng, công cụ này chạy trong tiện ích dòng lệnh. Nó cho phép người dùng thông dịch và hiển thị các gói TCP/IP và các gói khác đang được truyền tải hoặc được nhận trên một mạng mà máy tính đó kết nối với.

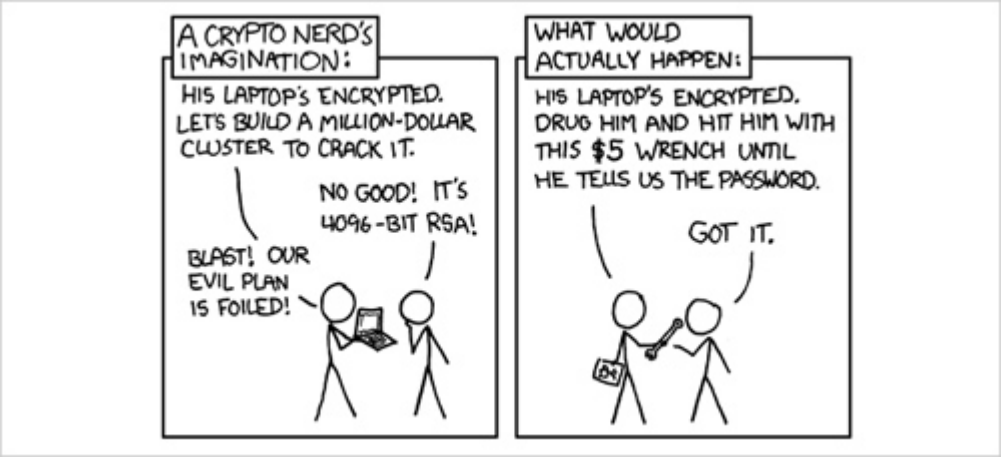
Trong một số hệ điều hành giống như Unix, một người dùng phải có các đặc quyền “superuser” để sử dụng tcpdump vì các cơ chế capture gói dữ liệu trên các hệ thống khác yêu cầu các đặc quyền này. Tuy vậy, tùy chọn –Z có thể được sử dụng để bỏ đi những đặc quyền đối với một người dùng không có đặc quyền cụ thể sau khi việc capture đã được thiết lập. Trong các hệ điều hành giống như Unix, cơ chế capture có thể được cấu hình để cho phép những người dùng không có đặc quyền cũng có thể sử dụng nó; nếu điều đó được thực thi thì các đặc quyền superuser sẽ không cần thiết.

Người dùng có thể tùy chọn sử dụng bộ lọc BPF để hạn chế số lượng gói được quan sát bởi tcpdump; điều này ám chỉ rằng đầu ra sẽ hiệu suất hơn với phân vùng cao lưu lượng.

```
13:08:05.737768 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1221 > dsl-usw-cust-110.inetarena.com.www: . 342:342(0) ack 1449 win 31856 <nop
,nop,timestamp 1247771 114849487> (DF)
13:08:07.467571 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1221: . 1449:2897(1448) ack 342 win 31856
<nop,nop,timestamp 114849637 1247771> (DF)
13:08:07.707634 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1221: . 2897:4345(1448) ack 342 win 31856
<nop,nop,timestamp 114849637 1247771> (DF)
13:08:07.707922 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1221 > dsl-usw-cust-110.inetarena.com.www: . 342:342(0) ack 4345 win 31856 <nop
,nop,timestamp 1247968 114849637> (DF)
13:08:08.057841 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1045 > ns.de.ibm.net.domain: 8929+ PTR? 110.107.102.209.in-addr.arpa. (46)
13:08:08.747598 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1221: P 4345:5793(1448) ack 342 win 31856
<nop,nop,timestamp 114849813 1247968> (DF)
13:08:08.847870 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1221: FP 5793:6297(504) ack 342 win 31856
<nop,nop,timestamp 114849813 1247968> (DF)
13:08:08.848063 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1221 > dsl-usw-cust-110.inetarena.com.www: . 342:342(0) ack 6298 win 31856 <nop
,nop,timestamp 1248082 114849813> (DF)
13:08:08.907566 ppp0 < ns.de.ibm.net.domain > slip139-92-26-177.ist.tr.ibm.net.1045: 8929* 3/1/1 PTR dsl-usw-cust-110.inetarena.com., P
TR fingerless.or (199)
13:08:09.151742 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1221 > dsl-usw-cust-110.inetarena.com.www: F 342:342(0) ack 6298 win 31856 <nop
,nop,timestamp 1248112 114849813> (DF)
13:08:10.137603 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1221: . 6298:6298(0) ack 343 win 31856 <no
p,nop,timestamp 114849967 1248112> (DF)
13:09:01.984210 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1222 > dsl-usw-cust-110.inetarena.com.www: S 920197285:920197285(0) win 32120 <
mss 1460,sackOK,timestamp 1253395 0,nop,wscale 0> (DF)
13:09:03.097569 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1222: S 1222277738:1222277738(0) ack 92019
7286 win 32120 <mss 1460,sackOK,timestamp 114855252 1253395,nop,wscale 0> (DF)
13:09:03.098197 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1222 > dsl-usw-cust-110.inetarena.com.www: . 1:1(0) ack 1 win 32120 <nop,nop,ti
mestamp 1253507 114855252> (DF)
13:09:03.102171 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1222 > dsl-usw-cust-110.inetarena.com.www: P 1:322(321) ack 1 win 32120 <nop,no
p,timestamp 1253507 114855252> (DF)
13:09:04.147613 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1222: . 1:1(0) ack 322 win 31856 <nop,nop,
timestamp 114855369 1253507> (DF)
13:09:04.507608 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1222: . 1:1449(1448) ack 322 win 31856 <no
p,nop,timestamp 114855369 1253507> (DF)
13:09:04.507934 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1222 > dsl-usw-cust-110.inetarena.com.www: . 322:322(0) ack 1449 win 31856 <nop
,nop,timestamp 1253648 114855369> (DF)
13:09:05.627604 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1222: . 1449:2897(1448) ack 322 win 31856
<nop,nop,timestamp 114855491 1253648> (DF)
13:09:05.857649 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1222: . 2897:4345(1448) ack 322 win 31856
<nop,nop,timestamp 114855491 1253648> (DF)
13:09:05.857918 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1222 > dsl-usw-cust-110.inetarena.com.www: . 322:322(0) ack 4345 win 31856 <nop
,nop,timestamp 1253783 114855491> (DF)
13:09:06.907557 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1222: FP 4345:5792(1447) ack 322 win 31856
 <nop,nop,timestamp 114855627 1253783> (DF)
13:09:06.907887 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1222 > dsl-usw-cust-110.inetarena.com.www: . 322:322(0) ack 5793 win 31856 <nop
,nop,timestamp 1253888 114855627> (DF)
13:09:07.401206 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1222 > dsl-usw-cust-110.inetarena.com.www: F 322:322(0) ack 5793 win 31856 <nop
,nop,timestamp 1253937 114855627> (DF)
13:09:08.317623 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1222: . 5793:5793(0) ack 323 win 31856 <no
p,nop,timestamp 114855780 1253937> (DF)
```

Mã hóa dữ liệu ổ cứng để tăng tính bảo mật trên Linux

Dữ liệu cá nhân trong ổ cứng là điều nhạy cảm và yêu cầu độ bảo mật tối đa, tùy vào nhu cầu và mục đích sử dụng trong công việc mà người dùng lựa chọn cách thức bảo vệ cho phù hợp**.** Trong bài viết sau, Quản Trị Mạng sẽ giới thiệu với các bạn cách mã hóa dữ liệu ổ cứng, cụ thể là từng phân vùng, thư mục trong hệ điều hành Linux với TrueCrypt và eCryptfs.

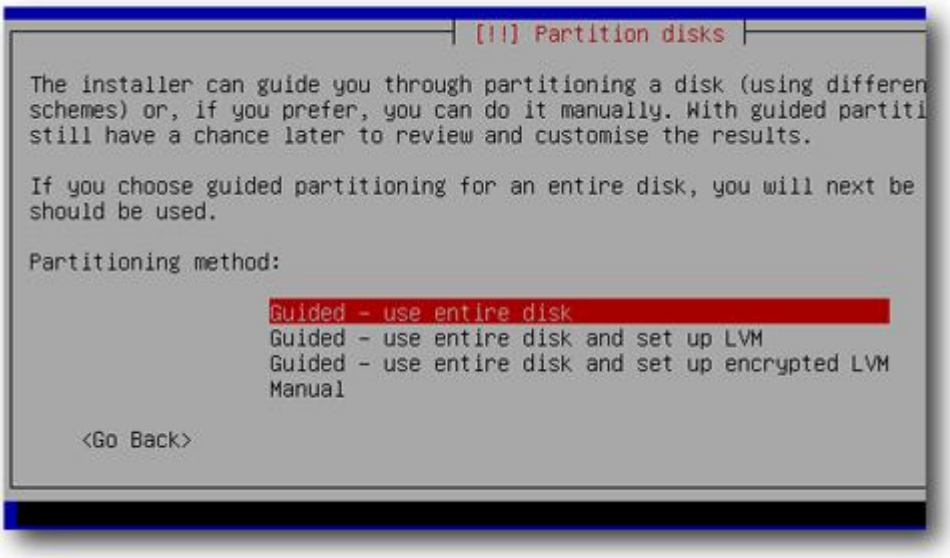


Mã hóa phân vùng ổ cứng

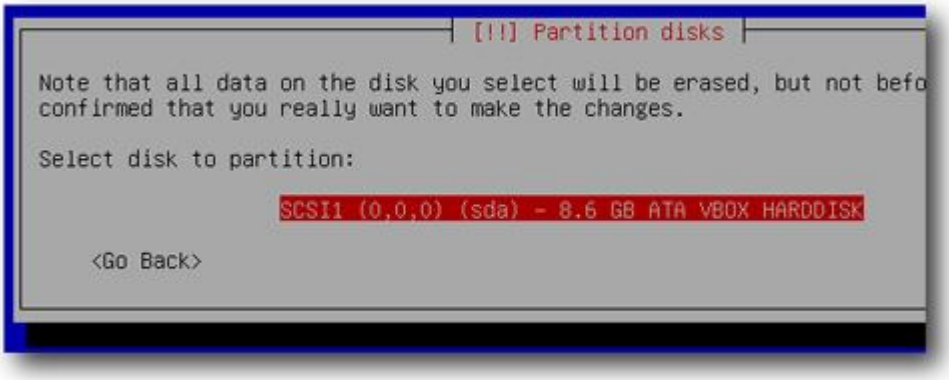
Phiên bản đĩa cài đặt thay thế của Ubuntu cung cấp thêm cho người dùng 1 sự lựa chọn nữa để mã hóa phân vùng cài đặt Ubuntu, do vậy các bạn chỉ cần tải file ISO về máy, ghi ra đĩa CD/DVD hoặc tạo

USB boot và tiến hành cài đặt Ubuntu sau đó.

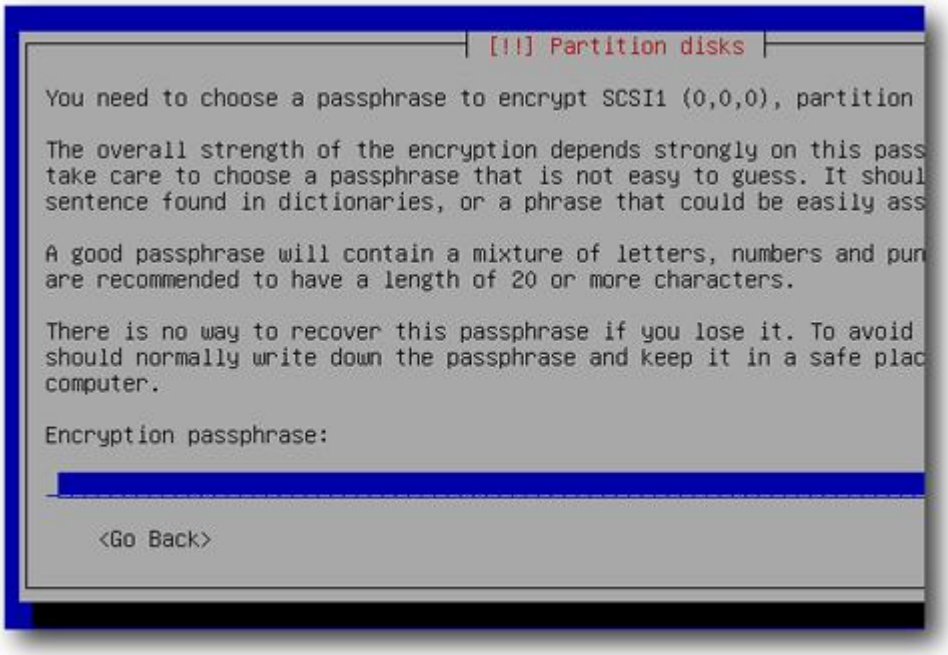
Với quy trình cài đặt khá giống với với Ubuntu nguyên bản, bước đầu người sử dụng sẽ phải chọn ngôn ngữ hiển thị, kiểu bàn phím, hệ thống network, và bước quan trọng nhất đương nhiên là phân vùng cài đặt với lựa chọn *Guided – use entire disk and set up encrypted LVM* để áp dụng trên toàn bộ ổ cứng:



Lưu ý rằng chúng ta cần khai báo hoặc khởi tạo phân vùng Master hoặc không phải là Slave để bắt đầu cài đặt:



Khởi tạo khóa mật khẩu sử dụng để mã hóa ổ cứng khi đăng nhập vào Ubuntu:



Lựa chọn có muốn mã hóa thư mục gốc - home hay không, chỉ trong trường hợp chúng ta thay thế thư mục này bên ngoài phân vùng cài đặt Ubuntu:

Như vậy là chúng ta đã hoàn tất các bước cơ bản, các bạn chỉ cần thực hiện các bước tiếp theo để hoàn tất quá trình này.

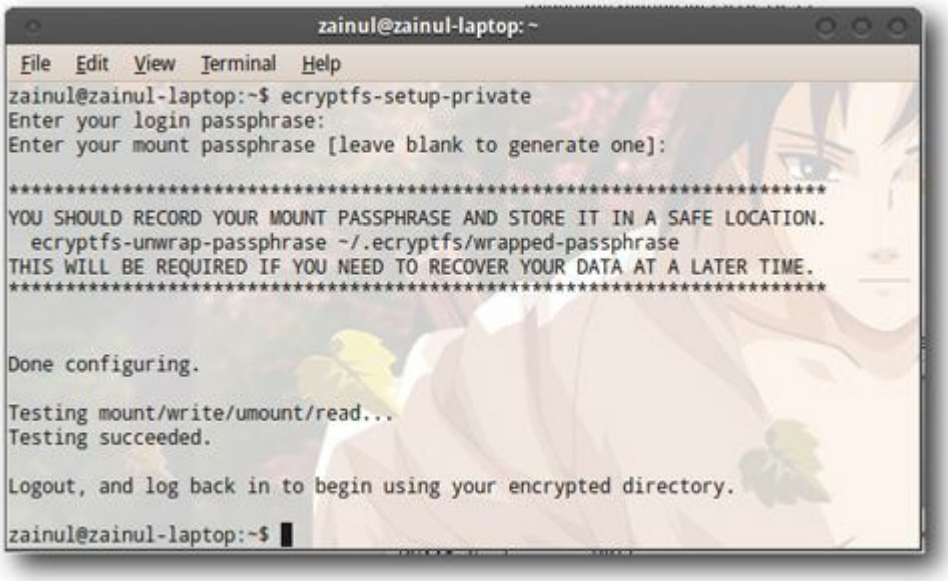
Mã hóa thư mục

eCryptfs là 1 hệ thống mã hóa file dựa trên chuẩn PGP được tạo ra bởi Philip Zimmerman vào năm 1991. Điểm độc đáo của eCryptfs so với các công cụ mã hóa khác, như TrueCrypt, là không cần xác định trước dung lượng phân vùng hoặc ổ cứng chúng ta cần áp dụng. Để cài đặt eCryptfs, các bạn hãy sử dụng lệnh sau:

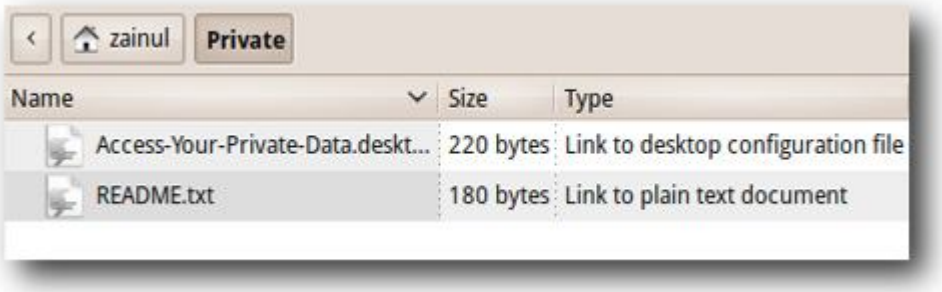
```
sudo aptitude install ecryptfs-utils
```

eCryptfs sẽ tạo ra 1 thư mục private trên ổ cứng nơi chương trình hoạt động và dùng để lưu trữ dữ liệu trong đó:

```
ecryptfs-setup-private
```



Lưu ý rằng quá trình này sẽ ẩn thư mục *~/.Private*. Chúng ta nên lưu trữ các dữ liệu nhạy cảm trong thư mục private này để đảm bảo không ai có thể truy cập và sử dụng, vì ecryptfs sẽ giấu toàn bộ dữ liệu trong thư mục đó:



1 điểm khác là thư mục private này sẽ tự động xuất hiện trong hệ thống khi bạn đăng nhập, đồng thời đây cũng là cơ hội cho người khác sử dụng và truy cập khi bạn không ở bên cạnh máy tính. Chúng

ta có thể áp dụng cách làm sau để khắc phục vấn đề này là ngăn chặn ecryptfs mở khóa các thư mục khi người dùng đăng nhập bằng cách xóa bỏ các file rỗng lưu trữ trong thư mục ~/.ecryptfs/ và “cách ly” thư mục này khi không sử dụng máy tính:

```
ecryptfs-umount-private
```

14 “chiêu” bảo mật PC dùng Vista

Windows Vista là phiên bản có khả năng bảo mật tốt nhất đến thời điểm này của hệ điều hành Windows. Đây là 15 “chiêu” đơn giản để bảo mật cho máy tính dùng hệ điều hành này.

Bật tính năng chống phishing

Theo mặc định, tính năng chống lừa đảo trực tuyến (Phishing Filter) của trình duyệt Internet Explorer trong Windows Vista thường tắt. Để tăng cường bảo mật cho trình duyệt, nên bật tính năng này bằng cách vào **Tools**, **Phishing Filter**, chọn **Turn On Automatic Website Checking**.

Xóa “history” của trình duyệt

Khi bạn lướt web, một số thông tin của trang web được lưu trên ổ cứng. Điều này giúp bạn mở lại các

trang web thường xuyên truy cập nhanh hơn, bởi nó được tải từ ổ cứng thay vì phải tải từ trên web. Tuy nhiên, việc lưu các thông tin này (gọi là lược sử duyệt web – history) trên ổ cứng có thể gây ra nguy cơ bảo mật thông tin cá nhân như hacker có thể biết các trang web bạn hay truy cập.

Để xóa bỏ các thông tin này, vào **Tools**, **Internet Options**, kích vào ô **Delete** trong mục **Browser History** để xóa bỏ history.

Không dùng chung mật khẩu

Không nên dùng một mật khẩu cho các dịch vụ khác nhau. Cố gắng dùng kết hợp ký tự, số và không nên dùng ký tự hay ngày dễ đoán làm mật khẩu, ví dụ như ngày sinh hay tên người thân.

Không trả lời thư rác

Nếu trả lời thư rác, bạn sẽ vô tình xác nhận với những kẻ phát tán thư rác rằng địa chỉ mail của bạn đang hoạt động. Ngoài ra cũng nên tránh kích chuột vào các đường link trong các email có ngụ ý được gửi từ các nhà cung cấp thẻ tín dụng hay cửa hàng trực tuyến. Điều này có thể là trò giả mạo lừa lấy thông tin cá nhân hoặc phát tán mã độc.

Bảo mật mạng không dây

Mạng không dây của bạn có thể vươn ra phố hoặc sang nhà hàng xóm. Để tránh những máy tính lạ xâm nhập, xài chùa mạng không dây bạn nên mã hóa kết nối mạng bằng cách đặt mật khẩu cho định tuyến. Chọn mức độ bảo mật WPA và thay đổi mật khẩu dùng để truy cập định tuyến. Nếu không có WPA, có thể chọn chế độ bảo mật WEP thay thế.

Kiểm soát sử dụng của trẻ

Một trong những thế mạnh của Windows Vista là nó tích hợp tính năng Parental Controls (sử dụng bằng cách vào **Start**, **Control Panel**, **User Accounts and Family Safety**, chọn **Parental Controls**), giúp bạn hạn chế trẻ truy cập vào một số địa chỉ Internet hoặc không được sử dụng một số chương trình. Tính năng này có thể giúp bạn tạo danh sách các địa chỉ web trẻ

được phép truy cập.

Tạo tài khoản người dùng riêng cho trẻ

Vào **Start**, **Control Panel**, kích vào **User Accounts and Family Safety**, sau đó kích chọn **User Accounts**. Tại đây, có thể tạo mỗi thành viên trong gia đình một tài khoá bằng cách kích vào ô **Create a New Account**, nhập tên người dùng.

Sau khi tạo tài khoản cho trẻ hoặc cho người thân trong gia đình, nên đặt mật khẩu tài khoản người dùng. Kích vào tên tài khoản mới tạo, sau đó kích ô **Create a Password**. Như vậy, chỉ những người có mật khẩu tài khoản đó mới có thể đăng nhập.

Bật chế độ kiểm soát trẻ

Theo mặc định, tính năng **Parental Controls** cho các

tài khoản người dùng bị tắt. Bật tính năng này rất đơn giản, chỉ cần kích **On** trên nút **Enforce Current Settings** dưới **Parental Controls**.

Sau khi mở tính năng Parental Controls của tài khoản người dùng, bạn có thể theo dõi các hoạt động của người dùng tài khoản đó qua tính năng Reporting. Khi người dùng tài khoản này truy cập vào tài khoản, tính năng Reporting sẽ ghi lại các chương trình họ sử dụng, các game họ chơi… nói chung là mọi việc họ làm với máy tính.

Đặt giới hạn thời gian dùng máy tính

Bạn có thể đặt giới hạn thời gian sử dụng máy tính của trẻ. Nếu bạn kích vào tính năng giới hạn thời gian Time Limits, bạn sẽ thấy một ô trống. Đây là nơi bạn có thể giới hạn thời gian sử dụng máy tính của trẻ bằng cách bôi màu ô đó bằng chuột. Thời gian trẻ

được phép dùng máy tính hiển thị màu trắng và thời gian hạn chế (cấm trẻ dùng máy tính) hiển thị màu xanh. Nếu trẻ cố gắng dùng máy tính ngoài khoảng thời gian bị giới hạn, Windows sẽ không cho đăng nhập.

Chặn mở một số chương trình

Bạn có thể ngăn trẻ mở một số chương trình, ví dụ nếu bạn không muốn ai thấy thông tin tài chính của bạn trong phần mềm **Microsoft Money**. Kích vào **Allow and Block Specific Programs** để xem danh sách phần mềm trên máy tính. Sau đó, bạn có hai lựa chọn: để người dùng mở bất kỳ chương trình nào hoặc ngăn họ mở một số phần mềm nào đó. Nếu bạn chọn lựa chọn sau, các chương trình bạn không đặt dấu kiểm trong danh sách phần mềm sẽ không thể truy cập được với đối tượng bạn muốn chặn.

Chặn trẻ chơi game

Tính năng **Parental Controls** cũng có thể dùng để chặn trẻ chơi game. Từ trình đơn Parental Controls, kích vào mục **Games**. Bạn có thể chọn chặn tất cả game cùng lúc, hoặc có thể chặn hoặc cho phép chơi một số game nào đó hoặc giới hạn game theo độ tuổi được chơi. Chặn các game theo độ tuổi là cách dễ nhất để đảm bảo trẻ không chơi những game không phù hợp với chúng. Kích vào **Set Game Ratings**, sau đó chọn độ tuổi trẻ được phép chơi các game phù hợp.

Sử dụng công cụ mã hóa Bitlocker

BitLocker là tính năng mã hóa toàn bộ ổ đĩa có trong hệ điều hành Windows Vista và bản thử nghiệp beta hệ điều hành mới Windows 7. BitLocker được thiết kế làm việc với máy tính có chip TPM (Trusted

Platform Module). Nếu máy tính có phần cứng đó thì bạn có thể truy cập bình thường với BitLocker. Nếu máy tính không có chip TPM bạn vẫn có thể dùng BitLocker, nhưng sẽ cần đến ổ USB. Mật khẩu BitLocker sẽ được cài trên ổ USB đó và bạn sẽ cần đưa ổ đó vào máy tính mỗi khi khởi động máy tính.

Bảo vệ máy tính thời gian thực

Tính năng bảo vệ máy tính thời gian thực **Real-Time Protection** (bật theo mặc định) kiểm tra các thành phần chính của Windows và cảnh báo nếu có những thay đổi với chúng. Bạn chỉ nên tắt bỏ tính năng này nếu đã sử dụng phần mềm chống spyware chuyên nghiệp.

Bảo vệ máy tính bằng tường lửa Windows

Windows Firewall bật theo mặc định. Bạn có thể

kiểm tra tình trạng của tính năng này trong **Windows Security Center**, thông qua Control Panel hoặc bạn có thể gõ "**Windows Firewall**" sau khi mở trình đơn Start.

Windows Firewall giúp bảo vệ máy tính bằng cách kiểm soát các nguồn lực của hệ điều hành nếu chúng hoạt động theo cách không mong muốn, một dấu hiệu cho thấy có sự hiện diện của mã độc. Ví dụ, nếu một thành phần của Windows được thiết kế để gửi các thông điệp mạng qua một cổng trên máy tính mà cố gắng chuyển qua cổng khác thì lý do có thể là do bị tấn công. Khi đó, Windows Firewall có thể chặn các thông điệp ra ngoài máy tính, ngăn mã độc phát tán sang người dùng khác.

10 mẹo giúp ích cho bảo mật Windows

Rủi ro bảo mật ngày càng tăng trong môi trường doanh nghiệp lớn và nhỏ. Bảo mật mạng luôn rất quan trọng, và vấn đề này thậm chí còn được đẩy cao hơn trong thời đại ngày nay. Đây chắc chắn là ưu tiên hàng đầu ở bất kì tổ chức nào. Dưới đây là 10 mẹo nhỏ đơn giản có thể giúp ích cho bạn.

1: Giảm thiểu mặt bằng tấn công bất cứ khi nào có thể

Một trong những bước đầu tiên cần phải làm để "gia cố" cho một chiếc máy tính là giảm thiểu bề mặt tấn công của nó. Càng nhiều code chạy trên máy, khả năng code bị khai thác càng cao. Vì vậy bạn nên tháo gỡ hết tất cả những phần không quan trọng của hệ điều hành và những ứng dụng không sử dụng đến.

2: Chỉ sử dụng những ứng dụng có uy tín

Đối với thị trường ngày nay, người dùng có xu hướng sử dụng phần mềm miễn phí, được giảm giá mạnh hoặc ứng dụng mã nguồn mở. Mặc dù không thể phủ nhận tầm quan trọng và tiện ích của những ứng dụng này ở các văn phòng, sử dụng cá nhân, nhưng việc thực hiện một cuộc nghiên cứu nhỏ trước khi sử dụng những ứng dụng này vẫn rất quan trọng. Một số ứng dụng miễn phí hoặc có giá thấp được thiết kế nhằm phục vụ người dùng, những ứng dụng khác được thiết

kế với mục đích lấy cắp thông tin cá nhân của người dùng hoặc theo dõi thói quen duyệt web của họ.

3: Sử dụng một tài khoản người dùng thông thường nếu có thể

Như một thói quen tốt, các quản trị viên nên sử dụng tài khoản người dùng thông thường khi có thể. Nếu xảy ra lây nhiễm malware, thường thì malware cũng có quyền giống như người đang đăng nhập. Vậy nên, chắc chắn rằng malware còn có thể gây ra nhiều phá hoại lớn hơn nữa nếu người dùng có quyền admin.

4: Tạo nhiều tài khoản Administrator

Ở mục trước, chúng ta đã thảo luận về tầm quan trọng của việc sử dụng một tài khoản người dùng thông thường bất cứ khi nào có thể và chỉ sử dụng tài khoản Admin khi bạn cần thực hiện một hành động nào đó cần có quyền người quản lý. Tuy nhiên, điều này cũng không có nghĩa là bạn nên sử dụng tài khoản Administrator.

Nếu có nhiều Administrator trong công ty, bạn nên tạo một tài khoản Administrator cho từng người. Do vậy, khi có một hành động của người quản lý được thực hiện, chắc chắn bạn sẽ biết được ai đã thực hiện nó. Ví dụ, nếu có một Administrator tên là John Doe, bạn nên tạo 2 tài khoản cho người dùng này. Một là tài khoản thông thường để sử dụng hàng ngày, và một là tài khoản quản lý chỉ sử dụng mỗi khi cần. 2 tài khoản này có thể lần lượt đặt tên là JohnDoe và Admin-JohnDoe.

5: Không nên ghi audit quá nhiều

Mặc dù việc tạo các policy audit để ghi lại các sự kiện diễn ra hàng ngày có thể rất hữu ích, nhưng có một vấn đề bạn nên nhớ: cái gì nhiều quá cũng không

tốt. Khi bạn thực hiện quá nhiều bản ghi audit, các file audit sẽ chiếm một dung lượng khá lớn. Điều này dẫn đến tình trạng bạn khó có thể tìm thấy bản ghi mình muốn có. Vậy nên, thay vì ghi lại tất cả các sự kiện, tốt hơn là chỉ tập trung vào những sự kiện quan trọng

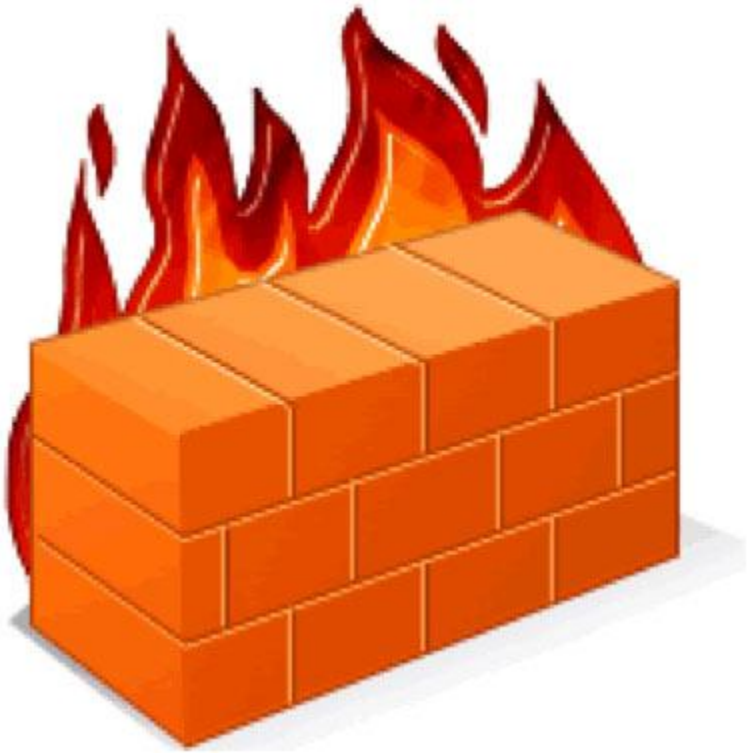
6: Tận dụng các policy bảo mật cục bộ

Sử dụng Active Directory dựa vào cài đặt policy nhóm không làm vô hiệu hóa nhu cầu cài đặt policy bảo mật cục bộ. Hãy nhớ rằng cài đặt policy nhóm được dùng chỉ khi ai đó đăng nhập bằng một tài khoản miền. Chúng sẽ không làm gì nếu ai đó đăng nhập vào máy tính bằng tài khoản cục bộ. Các policy bảo mật cục bộ có thể giúp bảo vệ máy tính của bạn chống lại việc sử dụng tài khoản cục bộ.

7: Xem lại cấu hình firewall

Bạn nên sử dụng fiewall ở vòng ngoài của mạng và trên từng máy trong mạng. Tuy nhiên, như vậy vẫn

chưa đủ. Bạn cũng nên xem lại danh sách cổng ngoại lệ của firewall nhằm đảm bảo rằng chỉ những cổng quan trọng vẫn được mở.



Trọng tâm thường đặt ở những cổng được dùng bởi hệ điều hành Windows. Tuy nhiên, bạn cũng nên kiểm tra bất kì rule nào của firewall chấp nhận mở cổng 1433 và 1434. Những cổng này được dùng để giám sát và kết nối từ xa tới server SQL. Chúng là mục tiêu yêu thích của hacker.

8: Cách ly các dịch vụ

Bất cứ khi nào có thể, bạn nên cấu hình server để chúng thực hiện một tác vụ cụ thể. Theo cách này, nếu một server bị tấn công, hacker sẽ chỉ có thể chiếm quyền truy cập vào một tập hợp các dịch vụ nào đó. Chúng tôi nhận ra rằng sức ép tài chính thường bắt các tổ chức phải chạy nhiều vai trò trên server của họ. Trong những trường hợp như này, bạn có thể nâng cấp bảo mật mà không phải tốn tiền bằng cách sử dụng ảo hóa. Trong một môi trường ảo hóa nào đó, Microsoft cho phép bạn triển khai nhiều máy ảo chạy hệ điều hành Windows Server 2008 R2 chỉ với một license server.

9: Áp dụng các bản vá bảo mật theo bảng thời gian

Bạn nên thường xuyên kiểm tra các bản vá trước khi áp dụng chúng vào server. Tuy nhiên, một số tổ chức vẫn có thói quen bỏ qua quá trình kiểm tra. Chắc chắn chúng ta không thể phủ nhận tầm quan trọng

của việc đảm bảo độ ổn định của server, nhưng bạn vẫn phải cân bằng nhu cầu kiểm tra với nhu cầu bảo mật.

Mỗi khi Microsoft cho ra mắt một bản vá bảo mật, bản vá này được thiết kế để nhắm vào một lỗ hổng nào đó. Điều này có nghĩa là hacker chắc chắn đã biết lỗ hổng này và sẽ tìm kiếm các phương án triển khai trong khi bản vá cho lỗ hổng vẫn chưa được áp dụng.

10: Tận dụng Security Configuration Wizard

Security Configuration Wizard cho phép bạn tạo các policy bảo mật dựa trên XML, có thể áp dụng cho server của bạn. Những policy này được dùng để kích hoạt các dịch vụ, cấu hình các cài đặt và đặt rule cho firewall. Tuy nhiên, hãy nhớ rằng các policy được tạo bởi Security Configuration Wizard không giống với các policy được tạo từ template bảo mật (sử dụng file .INF). Ngoài ra, bạn không thể sử dụng policy nhóm để triển khai policy Security Configuration Wizard.

“Pháo đài” Windows 7: Ưu và nhược trong vấn đề bảo mật

Windows 7 được coi là hệ điều hành an toàn nhất từ trước đến nay của Microsoft, nhưng nó chưa thực sự hoàn hảo. Hãy cùng chấm điểm những ưu và khuyết trong vấn đề bảo mật của Windows 7.

Trong bản tin Security Intelligence Report của Microsoft được công bố mới đây cho thấy đã có sự cải tiến vượt bậc về mức độ bảo mật từ Windows XP đến Windows 7. Tuy nhiên, không hệ điều hành nào là thực sự hoàn hảo. Cho dù Windows 7 được xem là “pháo đài vững chắc”, nhưng vẫn còn những yếu điểm để có thể bị đánh bại. Hãy cùng 2 chuyên gia bảo mật hàng đầu, Reguly và Wisniewski điểm qua những điểm mạnh và điểm yếu của “pháo đài” này.

Những cải tiến mới mẽ

Microsoft đã có những cải tiến quan trọng để bảo vệ nhân hệ thống của Windows và tăng cường thêm một vài tính năng bảo mật mới trong quá trình chuyển đổi và phát triển từ Windows XP đến Windows Vista. Với Windows 7, một vài tính năng bảo mật đó được

tăng cường thêm và Microsoft cũng không quên bổ sung thêm các tính năng mới.

Dưới đây là một vài tính năng bảo mật đáng lưu ý của Windows 7:

1. **ASLR** (Address Space Layout Randomization) và **DEP** (Data Execution Prevention) là 2 tính năng đã từng có trong Windows Vista, nhưng đã được cải tiến đáng kể trên Windows 7.

ASLR là cơ chế bảo mật, sẽ gán các dữ liệu lên bộ nhớ một cách ngẫu nhiên nhằm tăng độ khó cho các kẻ tấn công có ý định lợi dụng những sơ hở của hệ thống.

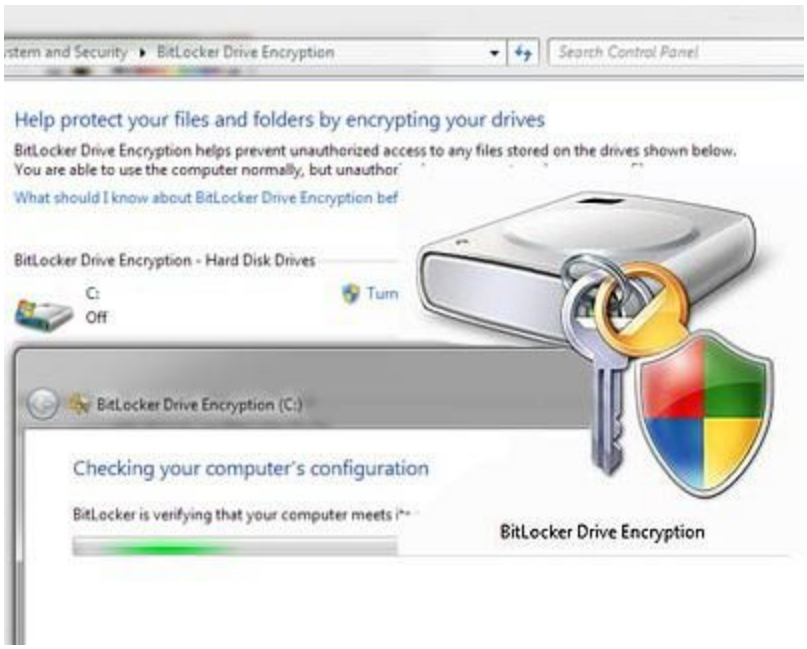
Còn DEP là tính năng đã được từng được trang bị ở Windows XP, có tác dụng ngăn chặn tấn công thông qua lỗi tràn bộ nhớ đệm của hệ thống. Ngoài ra DEP còn có tác dụng ngăn chặn các đoạn mã độc tấn công và các tiến trình đang chạy trên hệ thống. Bạn đọc có thể xem thêm cách thức kích hoạt tính năng DEP trên Windows XP và Vista đã được Dân Trí giới thiệu tại **đây**.

Chester Wisniewski, cố vấn cao cấp của hãng bảo mật danh tiếng Sophos cho hay: “ASLR đã thực sự được cải tiến trong Windows 7, theo đó, các file thư

viện (DLL) sẽ được load ngẫu nhiên vào trong địa chỉ bộ nhớ mỗi khi bạn khởi động hệ thống. Malware thường dựa vào các file cố định trên bộ nhớ để lợi dụng, và kỹ thuật này đã lợi dụng nhược điểm đó của các phần mềm mã độc.”

Wisniewski còn lưu ý thêm rằng DEP giờ đây đã bảo vệ tốt trình duyệt web Internet Explorer và các dịch vụ “xương sống” của hệ thống mà trước đây chưa được bảo vệ trong Windows Vista.

2. **BitLocker**: là tính năng mã hóa ổ đĩa lần đầu được Microsoft đưa ra trong Windows Vista. Ban đầu, tính năng này chỉ có thể mã hóa các phân vùng cài đặt Windows, và sau đó đã được mở rộng trong bản nâng cấp SP1, để mã hóa các phân vùng khác của ổ cứng, nhưng vẫn chưa thể mã hóa các ổ cứng gắn ngoài hoặc USB.



Tyler Reguly, kỹ sư trưởng của phòng nghiên cứu bảo mật nCirle cho hay, với Windows 7, Microsoft đã tích hợp thêm khả năng mã hóa dữ liệu trên USB, và tính năng này thực sự hiệu quả, bảo vệ hàng chục GB dữ liệu trên các thiết bị nhớ di động.

Bạn đọc có thể xem thêm cách thức sử dụng BitLocker trên Windows 7 đã được Dân trí giới thiệu tại **đây**.

3. **Internet Explorer 8 (IE 8):** đây là trình duyệt không thực sự dành riêng cho Windows 7 vì người dùng có thể download và sử dụng trên các phiên bản Windows cũ hơn. Nhưng cả Reguly và Wisniewki đều nhất trí rằng, IE8 thực sự là một bước đi đúng hướng của Microsoft.

Tyler Reguly bình luận: “Sự ra mắt của IE8 cho thấy rằng Microsoft đã thực sự quan tâm đến vấn đề bảo mật trên trình duyệt.”

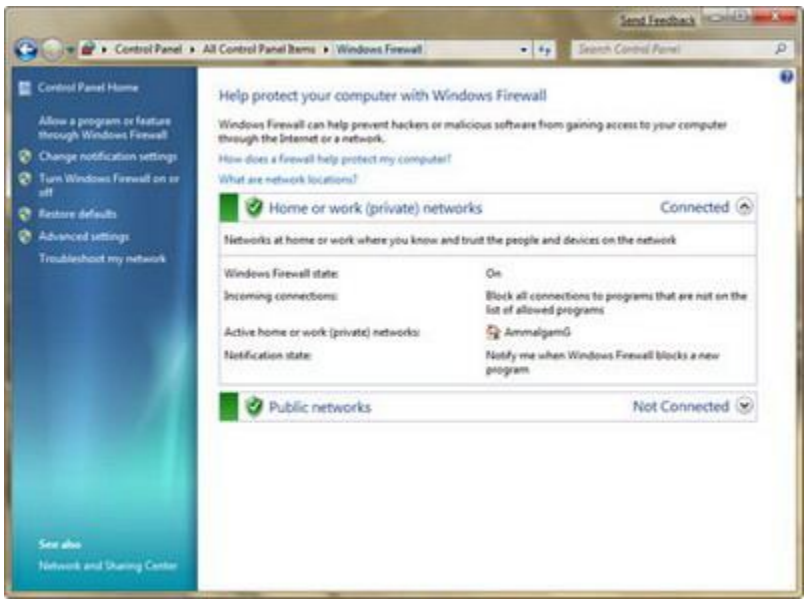
Wisniewski cho biết thêm: “IE8 đã tích hợp thêm tính năng bảo vệ mới mang tên SmartScreen, tương tự với tính năng bảo mật của Google Chrome hay Firefox. Đây là tính năng lọc trang web, cho phép chặn các trang web chứa mã độc để bảo vệ cho người dùng”.

Nếu chưa sử dụng Windows 7, người dùng vẫn có thể download IE8 miễn phí tại **đây** (nếu gặp khó khăn trong việc download từ link trên, bạn có thể download tại **đây**)

Những “lỗ hổng” chưa được “lấp”

Như trên đã nói, mặc dù Microsoft rất nỗ lực trong việc nâng cao bảo mật, nhưng không hệ điều hành nào là thực sự hoàn hảo, và Windows 7 cũng như vậy. Dưới đây là một vài nhược điểm mà có lẽ, Microsoft phải lưu ý hơn trong các phiển bản Windows tiếp theo.

1. **Windows Firewall**: Windows đã mất một khoản thời gian không ngắn để tiến hành sáp nhập tường lửa với hệ điều hành, kết quả là sự ra đời của Windows Firewall. Tuy nhiên, rất tiếc, tường lửa mặc định của Windows chưa bao giờ được đánh giá cao, do không cung cấp những tính năng mạnh mẽ để lọc dữ liệu chuyển qua kết nối Internet, ngăn chặn các cuộc tấn công từ bên ngoài…



Windows Firewall - nhẹ nhàng nhưng không thực sự hiệu quả

Tyler Reguly nói: “Về lựa chọn cá nhân, tôi sẽ không sử dụng một phần mềm của hãng thứ 3. Tôi nhận thấy chúng sử dụng quá nhiều tài nguyên và ảnh hưởng không nhỏ đến hiệu suất hệ thống. Sẽ thật tuyệt vời nếu Windows Firewall trở nên mạnh mẽ hơn. Tôi xin lưu ý rằng, có sự tương quan giữa “mạnh mẽ hơn” và “tốn nhiều tài nguyên hệ thống”. Có lẽ, nguyên do khiến các phần mềm tường lửa của hãng thứ 3 trở nên “ngốn” nhiều tài nguyên hệ thống bởi lẽ chúng mạnh mẽ và hiệu quả hơn. Đây là điều mà Microsoft cần phải quan tâm để cân bằng giữa hiệu năng sử dụng và bảo mật của Windows Firewall”.

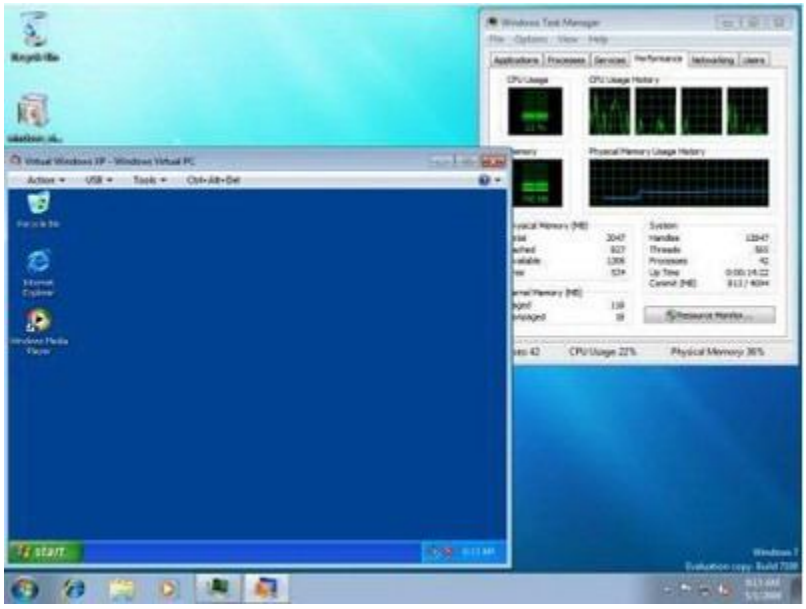
2. **Ẩn dấu định dạng file**: Mặc định, Microsoft vẫn tiếp tục dấu đi các định dạng file quen thuộc đã được biết đến, nghĩa là nếu 1 file có tên đầy đủ “dantri.jpg” thì Windows sẽ chỉ hiển thị “dantri”.

Tuy nhiên, Chester Wisniewski lại cho rằng, việc ẩn đi định dạng file lại là một nhược điểm có thể khiến phần mềm gián điệp lợi dụng để qua mắt người dùng. Wisniewski nói: “Điều này có thể giúp Trojan từ email sẽ dễ dàng sử dụng mánh khóa đơn giản để qua mắt người dùng, bằng cách thêm vào 1 định dạng giả cho file. Chẳng hạn file “virus.jpg.exe” chứa mã độc, sẽ chỉ được Windows hiển thị dưới dạng “virus.jpg”

và người dùng sẽ nhầm tưởng đó là 1 file ảnh định dạng jpg vô hại và vô tình kích hoạt nó".

3. **Chế độ giả lập XP**: Đây là chế độ giả lập, cho phép sử dụng các thiết bị phần cứng hoặc phần mềm chưa tương thích hoặc không hoạt động được trên Windows 7. Các thiết bị và phần mềm sẽ hoạt động bình thường và ổn định trong môi trường Windows XP giả lập.

Vấn đề có thể gặp ở đây là mặc dù hoàn toàn là môi trường của Windows XP, nhưng chế độ giả lập này không được bất kỳ sự bảo vệ nào từ Windows 7.



Chế độ Windows XP - Máy tính ảo không có sự che chắn trên Windows 7

Wisniewski giải thích: “Chế độ Windows XP mở đầu 1 lớp mới phức tạp cho vấn đề bảo mật trên Windows. Mặc định, Windows 7 tự động thiết lập phân vùng từ máy ảo Windows XP, đây sẽ là “miếng mồi ngon” cho malware nếu như nó không được hoàn toàn bảo vệ.”

4. **User Account Control (UAC):** Từng bị xem là tính năng “thừa” khi được đưa vào Windows Vista. Mục đích là để người dùng dễ dàng quản lí và không bị virus tự động kích hoạt hay qua mặt, nhưng với phần lớn người dùng, UAC bị xem là sự phiền nhiễu, và không mấy ai giữ nguyên tính năng này để sử dụng.

UAC - Không mang lại hiệu quả như mong muốn

Microsoft đã có sự cải tiến đáng kể của UAC trên Windows 7, khi đã bớt "làm phiền" người dùng hơn so với trước đây, tuy nhiên, nó lại không thực sự hiệu quả trong việc ngăn chặn sự xâm nhập của các phần mềm độc hại. Cả Tyler Reguly và Chester Wisniewski đều thống nhất rằng UAC không thực sự là một tính năng bảo mật nhưng cũng cho rằng Microsoft cần phải tiếp tục phát triển UAC để nó trở nên hoàn thiện hơn.

Trên đây là những nhận định của 2 chuyên gia hàng đầu về bảo mật với những cải tiến của Windows 7. Còn bạn, nếu bạn chỉ là người dùng phổ thông, thì nhận định của riêng bạn dành cho tính năng an toàn của Windows 7 là như thế nào? Hãy tự rút ra những kết luận cho riêng mình sau khi sử dụng hệ điều hành rất được Microsoft kỳ vọng này.

Bộ công cụ bảo mật hàng đầu cho Windows XP SP2

Trước những mối đe dọa như virus, spyware, spam, hacker… luôn rình rập người sử dụng mỗi khi vào mạng, vừa qua, hãng BitFantasy đã cho ra mắt phiên bản XPSecurity 2005, một bộ công cụ bảo mật cực mạnh cho Windows XP.

Chương trình XPSecurity 2005 đã được rất nhiều website phần mềm hàng đầu như: Softpedia, TopShareware, FileHeaven… đánh giá là sản phẩm 5 sao. Phiên bản mới nhất XPSecurity 2005c build 1219 có dung lượng 1.54MB, tương thích với mọi phiên bản của Windows XP, có thể tải về bản dùng thử tại địa chỉhttp://www.download.com/3000-2094-10309078.html.

Do các tính năng của XPSecurity rất nhiều, nên chỉ xin giới thiệu về những tính năng quan trọng nhất của chương trình. Sau khi thiết lập xong, bạn bấm vào thẻ Apply để thay đổi có hiệu lực.

• **Windows Firewall:** được thiết kế giống với tường lửa của

WinXP SP2, giúp bảo vệ máy tính khỏi sự xâm nhập bất hợp pháp từ bên ngoài và giành quyền kiểm soát hệ thống của hacker. Tại tab General, bạn đánh dấu ở thẻ On (recommended) và bấm Apply để thiết lập tường lửa cho WinXP. Nếu muốn hệ thống an toàn hơn nữa, ở tab Exceptions, bạn thêm vào danh sách của XPSecurity những ứng dụng và cổng muốn khóa.

• **Internet Security:** gồm một số tính năng bảo an cho Internet Explorer khi duyệt web, được thể hiện trong 5 tab:

+ Pop-up Blocker: ngăn chặn các trang quảng cáo và pop-up xuất hiện khi duyệt web.

+ IE Apprearance: khóa trang chủ của Internet Explorer, vô hiệu hóa một số tùy chọn trong Internet Options của IE.

+ Privacy: chỉ định trước những website mà bạn không muốn cho ghi lại cookie.

+ Web Content Zone (tương tự tab Security trong IE Options): lựa chọn mức độ bảo mật theo vùng về nội dung của các trang web, hạn chế sự truy cập vào các trang web cấm.

+ Advanced Settings: gồm một số thiết lập tăng cường cho hệ thống, trong đó đáng chú ý như: bật/tắt tính năng autorun của CD/DVD-ROM, không cho save nội dung các trang web bị mã hóa, dọn dẹp temporary files sau khi đóng trình duyệt, kiểm tra chữ ký của các chương trình tải về… Do số lượng tính năng khá nhiều, vì vậy bạn nên thiết lập theo cách nhà sản xuất đã khuyến cáo (chọn thẻ Select Recommended).

• **Email Security:** gồm một số tính năng bảo mật cho Outlook Express, trong đó đáng chú như:

+ Warn me then other applications try to send mail as me: cảnh báo khi có ứng dụng lạ nào đó gửi thư đến.

+ Do not allow attachments to be saved or opened that could potentially be a virus: không cho save hoặc mở các file đính kèm có nguy cơ nhiễm virus từ những lá thư gửi đến.

+ Encrypt contents and attachments for all outgoing messages: mã hóa nội dung lá thư và file đính kèm gửi đi.

+ Digitally sign all outgoing message: đính kèm chữ ký điện

tử vào tất cả các lá thư gửi đi.

• **System Security:** gồm một số tính năng bảo mật tăng cường cho hệ thống, được thể hiện trong 6 tab.

+ Windows Update: bật/tắt tính năng tự động cập nhật bản vá của Windows XP.

+ DEP (Data Execution Prevention) Settings: thiết lập một danh sách "đặc biệt" cho những ứng dụng và dịch vụ chạy nền sẽ được bảo vệ khỏi sự tấn công của virus và các mối đe doạ khác.

+ Startup Run: quản lý các chương trình và dịch vụ nạp chung vào quá trình khởi động Windows.

+ Service Processess: bật/tắt các các dịch vụ chạy nền của Microsoft.

+ Advanced Settings: gồm một số thiết lập tăng cường, trong đó đáng chú ý là: vô hiệu hóa Command Prompt và các batch file, không cho sử dụng Registry Editor, Task Manager; dọn dẹp pagefile lúc tắt máy…

• **Desktop Security:** gồm "hàng tá" tính năng bảo mật cho các thành phần khác của Windows, được thể hiện trong 4 tab:

+ Desktop: ẩn đi biểu tượng của các chương trình trên desktop, vô hiệu hóa tính năng Active Desktop, không cho thay đổi hình nền của desktop…

+ Start menu: bỏ bớt các thành phần trong Start menu như: Search, My Documents, Control Panel, Help and Support, Run…

+ Control Panel: thêm/bớt, làm ẩn đi hoặc vô hiệu hóa một số

tác vụ trong Control Panel.

+ Task Scheduler: không thay đổi hoặc tạo ra các task scheduler.

Do trong phần này, số lượng các tính năng là rất nhiều, vì vậy bạn cũng nên thiết lập theo cách nhà sản xuất đã khuyến cáo (chọn thẻ Select Recommended).

• **File System:** gồm một số thiết lập bảo mật dữ liệu trong ổ cứng, được thể hiện trong 2 tab:

+ Drive Accessibility: không cho người khác truy xuất vào các ổ dĩa hệ thống định trước.

+ USB Drive Accessibility: không cho sử dụng các thiết bị di động qua cổng USB để chuyển tải hoặc sao chép dữ liệu trong máy tính.

• **Applications Security:** gồm "hàng tá" tính năng bảo mật cho các ứng dụng, được thể hiện trong 5 tab:

+ Access Control: lập danh sách hạn chế người khác sử dụng một số ứng dụng nào đó.

+ Microsoft Office: tùy biến mức độ an toàn của macro cho các

chương trình trong bộ Microsoft Office (Word, Excel, Powerpoint, Outlook), ẩn đi menu trợ giúp Help, bỏ tính năng báo lỗi trong bộ Office XP…

+ MSN Messenger: không cho chat, chia sẽ thông tin trong NetMeeting…

+ Windows Media player: không cho tải codec xem phim, bỏ bớt các tính năng từ menu của Windows Media Player như: Radio Bar, Media Favourites…

• **Anti-Adware:** ngăn chặn các trang quảng cáo, pop-up xuất

hiện khi duyệt web; hạn chế sự xâm nhập của ad-ware vào hệ thống, đồng thời cho phép bạn chỉ định trước danh sách những website mà bạn muốn xem quảng cáo...

• **Anti-Virus:** gồm một số tính năng phòng chống virus, được thể hiện trong 2 tab:

+ Sp2 Anti-virus: tích hợp với chương trình diệt virus cài trong máy nhằm tăng thêm tính bảo mật cho hệ thống.

+ Program Self-Protection: tích hợp tính năng tự bảo vệ cho các ứng dụng (mỗi khi ứng dụng nào đó bị nhiễm virus, chúng sẽ tự động được sửa chữa).

• **Preference and Register:** được thể hiện qua 3 tab:

+ Password: tạo ra một password quản trị nhằm tránh tình trạng người khác thay đổi những thiết lập mà bạn đã cấu hình cho chương trình (khi kích hoạt XPSecurity, bạn phải gõ password để đăng nhập).

+ Profile Manager: quản lý chương trình theo chế độ đa cấu hình với các profile chỉnh trước.

+ Register and About: phần giới thiệu của nhà sản xuất và đăng ký sử dụng chương trình.

• **Lưu ý:** Bạn nên đặt chương trình ở chế độ chạy nền để giữ cho Windows XP SP2 của mình luôn ở tình trạng an ninh cao nhất (đánh dấu thẻ Run XPSecurity when starting computer tại thẻ Preferences).

XPSecurity 2005 được đánh giá là vượt trội hơn cả Security Center của Windows XP SP2 về mức độ an toàn và cả số lượng tính năng bảo mật. Chắc chắn XPSecurity 2005 sẽ đem đến là sự hỗ trợ tối ưu nhất cho Windows XP SP2 để bạn tự tin đối phó với những hiểm họa tiềm ẩn có thể xuất hiện bất cứ lúc nào từ không gian Internet.

Phạm Hồng Quân

Công cụ bảo mật tất cả trong một

Worm có thể lây lan qua spam và spyware có thể gieo mầm Trojan, hàng

đe dọa phức tạp mới sẽ không còn phân biệt rõ ràng nữa. Để ứng phó, cần

mềm bảo mật kết hợp nhiều công cụ khác nhau để giữ an toàn cho PC của

Bạn có thể xây dựng hệ thống phòng thủ bằng các chương trình chống virus, c
spyware và firewall độc lập hoặc trang bị một ứng dụng tích hợp tất cả trong n
Chiến thuật sử dụng những ứng dụng bảo vệ chuyên biệt cho phép người dùng
sản phẩm tốt nhất trong từng thể loại nhưng việc vận hành có thể phức tạp và c
đắt. Các sản phẩm tích hợp cung cấp sự tiện lợi và giá rẻ; các thành phần riêng
có thể được cấu hình cùng một giao diện và được thiết kế để có thể tương tác v
một cách trơn tru. Điều này có nghĩa là bạn phó thác hoàn toàn máy tính và dữ
mình cho một công ty, nhưng còn hơn là gây rối loạn hệ thống với việc chạy n
mềm chống virus và firewall của nhiều hãng khác nhau.

Cuộc chiến giữa các tên tuổi

Để tìm được những bộ sản phẩm đáng giá, nhóm thử nghiệm (NTN) chọn 10 s

- bao gồm những sản phẩm mới và những sản phẩm đã có tên tuổi - để "tỷ thí"
suất và tính tiện lợi.

Thử nghiệm xem xét 4 yếu tố: hiệu suất (phát hiện malware và tốc độ), tính năng, thiết kế (dễ dùng) và giá. Các sản phẩm có giá từ 40-80USD với 1 năm cập nhật miễn phí, phí các năm tiếp sau từ 25-60USD. Về hiệu suất, nên nhớ rằng phần mềm bảo mật chỉ tốt với cập nhật mới nhất (có thể là nhận dạng viru hay cải tiến phương thức quét virus). Về tính năng, nhìn chung các sản phẩm k đồng.

Symantec làm việc tốt, nhi
năng, dễ dùng.

Để đánh giá phần thiết kế, NTN dựa trên tiêu chí cài đặt đơn giản và các tính r truy cập. Ngoài ra, NTN cũng đánh giá mức độ chi tiết của các cảnh báo và kh huấn luyện chương trình. Điều quan trọng nhất là NTN chú ý vào hiệu suất, xá

khả năng phát hiện và cô lập những hiểm họa cũng như dọn sạch những chươn
độc hại. NTN kết hợp với công ty AV-Test.org để cho hơn 174.000 sâu, virus,
hậu, bot và spyware tấn công mỗi sản phẩm. Ngoài ra, AV-Test.org còn phân
chế thông minh (khả năng phát hiện những phần mềm độc hại chưa được nhận
NTN sử dụng WorldBench 5 để đo hiệu suất của hệ thống khi thiết lập chế độ
cao nhất.

Tuy nhiên, NTN không đánh giá một cách đầy đủ khả năng phát hiện dựa trên
Công nghệ này (Microsoft, Panda, và Zone Alarm đều có cung cấp) có khả năn
hiện những hiểm họa mới bằng cách "bắt" những hành động của các ứng dụng
một chương trình muốn thay đổi registry). Tính năng này có thể bổ sung cho c
nhận dạng, nhưng việc thử nghiệm nó đầy đủ không thích hợp với khuôn khổ
giá này.

Các ứng dụng bảo vệ tốt nhất

Sản phẩm của Aluria quét file đóng gói nhưng không xử lý trình nén thực thi.

Trong tất cả các gói sản phẩm đ
nghiệm, một số ở mức khá và k
chương trình nào đạt xuất sắc tc
Gói sản phẩm của Symantec đu
giá tốt nhất vì hoạt động ổn định
cả các thử nghiệm. Nó đạt điểm
tuyệt đối và về nhì trong thử ng
virus, backdoor, bot và Trojan.
nó còn cung cấp khả năng bảo v
ứng dụng IM (instant-messaging), công cụ quản lý truy cập Internet dành cho
huynh và tính năng bảo mật dữ liệu. Tuy nhiên, giao diện chương trình cần bố
hơn và chi phí hỗ trợ qua điện thoại "ngốn" tới 30USD mỗi lần.

Về nhất ở khả năng chống malware trong đợt thử nghiệm này là gói sản phẩm
không chỉ thế sản phẩm này còn cung cấp những tính năng bổ sung khác như b
ứng dụng IM, chống mạo danh (phishing) cho IE. Tuy nhiên, chương trình lại
vọng ở tiến trình cài đặt và tốn tới 3USD cho mỗi phút hỗ trợ.

Gói Zone Labs, tích hợp công cụ quét virus cũ của eTrust (của CA) xếp thứ 7 t
suất, mặc dù là một firewall rất mạnh. Zone Labs có kế hoạch nâng cấp vào th
sao, với nhiều tính năng và dễ dùng, gói sản phẩm này được xếp ở vị trí thứ 6
cuộc.

Điều gây ngạc nghiên cho NTN chính là hiệu suất của BitDefender, tốc độ chậ
adware bình thường, cộng thêm firewall kém ấn tượng, xếp thứ hạng 9.

Tân binh Aluria có giá rẻ nhất nhưng các thành phần cơ bản lại xếp cuối. Phần
này có thể quét toàn bộ đĩa cứng nhưng không cho người dùng chọn tập tin và
để quét. Ngoài ra, ứng dụng này không phát hiện được phần mềm độc hại khi
dạng thực thi như ASPack, UPX. Cuối cùng, thiết lập firewall mặc định của A
lỏng lẻo và "ngốn" nhiều tài nguyên hệ thống.

CHÚ THÍCH THUẬT NGỮ

• ***Adware***: phần mềm hiện quảng cáo và thu thập thông tin duyệt web của n

dùng.

• ***Backdoor***: là một loại trojan nhưng nhiệm vụ chính là mở thông một số cổ
nào đó trên máy tính để lây lan, truy cập và điều khiển máy tính từ xa.

• ***Bot***: loại chương trình chờ chỉ thị từ một nơi nhất định để thực hiện đồng
một hành vi nào đó. Bot là công cụ để thực hiện các cuộc tấn công DoS/DD

• ***Malware***: phần mềm phá hoại.

• ***Rootkit***: một loại trojan nhưng tự giấu mình, hoạt động ở tầng thấp của hệ
nên có thể ngăn cản một số dịch vụ.

• ***Spam***: thư rác.

• ***Spyware***: phần mềm dùng để theo dõi mọi hoạt động của máy tính và gửi
một địa chỉ nào đó.

• ***Phishing***: lừa người dùng Internet bằng cách tạo ra những trang web giả m
người dùng nhầm tưởng là web chính thức, dùng để lấy tài khoản ngân hàng
tín dụng, mật khẩu...

• ***Trojan***: phần mềm chỉ phát huy vai trò khi nhận một sự kiện nào đó.

• ***Worm***: sâu, lây lan qua thư điện tử hoặc lỗ hổng phần mềm.

Virus, spyware và adware

McAfee và F-Secure đạt điểm số tốt khi phát hiện đâu là virus, đâu là spyware của 2 sản phẩm này đều nằm trong "top 3". Sản phẩm Panda có cơ chế thông nhất, McAfee và Aluria là 2 anh tài vượt trội trong phát hiện adware.

Hầu hết các bộ sản phẩm đều phát hiện được 100% "tội phạm" trong WildList sách công bố các virus, sâu và bot) tháng 1/2006. Aluria gây ngạc nhiên khi kh hiện bất cứ boot-virus nào, sản phẩm của Microsoft không phát hiện 14 thành Trend Micro sót 2 thành phần sâu. Trong thử nghiệm với WildList, các thành boot-virus không đáng kể, điều này giải thích tại sao Aluria đạt điểm số 100% bảng đánh giá.

Panda bổ sung tính năng nhận d

Kết quả đối phó với 168.523 backdoor, bot và trojan của AV-Test rất khác nhau. CA chỉ phát hiện được 37% backdoor, 72% bot, 39% trojan. Zone Labs phát hiện 30% backdoor, 49% bot, và 31% tr Secure mạnh nhất, "tóm" hơn 98% các mối đe dọa.

malware theo hành vi, tăng tính minh".

Trong thử nghiệm phát hiện adware, McAfee có điểm tốt nhất, "bắt gọn" 96% thành phần đang chạy. Aluria chiếm vị trí 2 với 89%. Một lần nữa Zone Labs suất thấp, chỉ phát hiện 46% adware.

Để đánh giá "trí thông minh", AV-Test.org kiểm tra khả năng "ứng xử" của cá phẩm với các thành phần trong WildList mà không nhờ đến dữ liệu nhận dạng vượt lên với 91%, F-Secure về nhì nhờ "bắt" được 76%, Microsoft xếp cuối vớ Zone Labs xếp thứ hai từ dưới lên với 48%. Lưu ý, chức năng phát hiện dựa tr vi của những sản phẩm này có thể giúp cải thiện những điểm số kém cỏi trên.

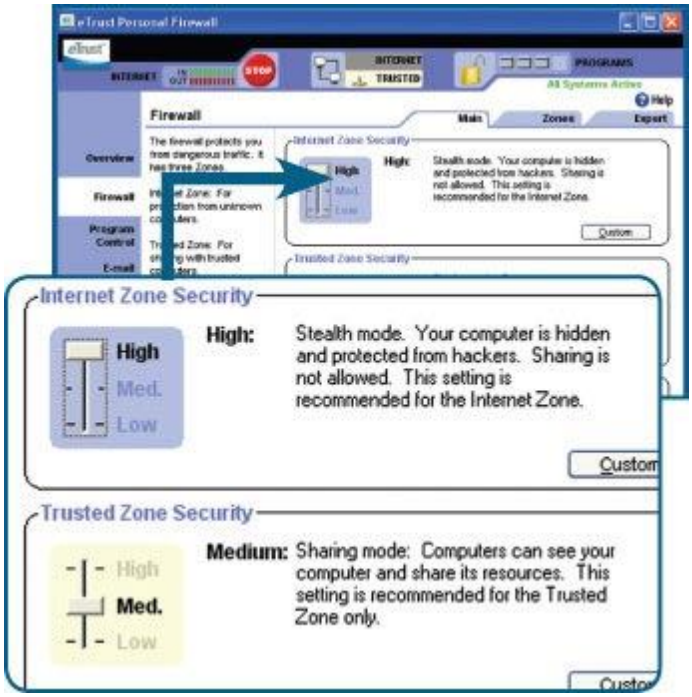
AV-Test.org nhận thấy Panda TruPrevent có thể chặn tới 90% sâu mạng và em
OS Firewall của Zone Labs chặn tới 70% sâu.

NTN cũng đánh giá khả năng phát hiện phần mềm phá hoại (malware) gói tron
nén như .zip, rar, .cab và các định dạng nén thực thi như ASPack và UPX. Đa
ứng viên có thể phát hiện ở mức nén một, nhiều lần hoặc dạng tự giải nén, nhu
hiện khả năng khác nhau ở định dạng nén thực thi. F-Secure, McAfee và BitD
thực hiện tốt nhất, Aluria và Zone Labs xếp chót. Aluria cho biết phiên bản kế
bổ sung khả năng "soi" file nén thực thi và được cập nhật miễn phí cho người
tại vào cuối năm nay. Phía Zone Labs nói rằng họ đang làm việc với CA để cả
khả năng phát hiện malware "đóng gói" và OSFirewall sẽ phát hiện và cô lập m
malware khi tập tin đóng gói được mở.

Trong điều kiện lý tưởng, phần mềm bảo mật phải phát hiện và ngăn chặn tất c
mối đe dọa từ dấu hiệu đầu tiên. Nhưng thực tế khó được như vậy. NTN kiểm
năng quét sạch file, Registry và các file Host (tập tin khai báo các địa chỉ IP) b
nhiễm 10 sâu trong WildList. McAfee quét sạch phần mềm độc hại và khôi ph

thay đổi hệ thống, ngoại trừ một biến thể của Mytob nhắm vào chính các phần mật. Sản phẩm của Microsoft cũng làm khá tốt, làm sạch mọi loại sâu ngoại tr thay đổi trong Registry gây ra bởi Netsky.BA và Mytob.AR. F-Secure thể hiệ năng tìm hơn là diệt, chỉ làm sạch được 5/10 sâu.

Các firewall đối đầu



CA eTrust tích hợp firewall của Zone Labs

Ranh giới giữa p chống virus và p chống spyware đ dần, nhưng các p firewall thì vẫn " độc lập, kiểm soá của mạng và cản hành vi đáng ngh

Firewall của 10 g phẩm thử nghiệm đều cho phép thiết lập mức bảo mật tổng quát, danh sách ứn

toàn và không an toàn, các cổng và giao thức được phép.

Firewall tốt có thể phân biệt giữa tín hiệu tốt và xấu, thông báo tới người dùng
sự cố nghiêm trọng và cung cấp đủ chi tiết về hành vi được phát hiện, điều đó
người dùng quyết định có hay không nên để một ứng dụng nào đó hoạt động. C
firewall kém thì thường xuyên đưa ra những thông báo mơ hồ và bạn có thể ch
ứng dụng mình cần hay tệ hơn là tắt cả firewall.

Thử nghiệm các firewall dựa trên chế độ thiết lập mặc định để chặn các cuộc t
từ bên ngoài và phần mềm phá hoại có sẵn trên PC. Các sản phẩm của CA, Mi
Symantec và Zone Labs dập tắt hoàn toàn các đợt tấn công ngay bên trong, cụ
malware không thể vô hiệu firewall, xóa hay chiếm quyền hợp pháp (một vài n
sẽ ngụy trang thành IE và cố gắng thu thập các quyền mà bạn cấp cho IE) và b
không thể truy cập Internet.

Với thiết lập mặc định, firewall của Aluria thất bại với tất cả cuộc tấn công từ
trong, nhưng ở chế độ thiết lập cao nhất thì đều vượt qua cả 2 thử nghiệm chiế

và backdoor. Aluria nói rằng chế độ mặc định mở cổng 80 và 443, nhằm mục đ
thiểu cảnh báo của firewall đến người dùng. Theo người phụ trách sản phẩm A
hãng muốn để khách hàng tự cấu hình sản phẩm theo cách họ muốn.

NTN cũng kiểm tra các firewall xem chúng có thể phát hiện những malware muốn đánh cắp dữ liệu của PC. Zone Labs đã giành được tròn 100 điểm, vượt 17 phép kiểm tra về chặn rò rỉ; Microsoft xếp thứ 2, vượt qua 7 thử nghiệm. Các sản phẩm khác đạt điểm rất thấp và Panda không vượt qua thử nghiệm nào hết. Lưu ý AV Test.org chạy những tiện ích kiểm tra lỗ hổng đã được chuẩn hóa dành cho các cung cấp sản phẩm bảo mật. Zone Labs phát triển sản phẩm để vượt qua các ti kiểm tra lỗ hổng, trong khi đó Panda nói rằng chương trình không được tối ưu các ứng dụng kiểm tra, mà chỉ sử dụng công nghệ TruPrevent để phát hiện hàn những mã lệnh nguy hiểm.

Web Site Filter của Trend M
khả năng chặn web xấu

Trong thử nghiệm để đánh giá khả năng phản ứng với tấn công từ bên ngoài, c
phẩm của CA, F-Secure, McAfee, Panda, Symantec và Zone Labs đạt 100%. N
sản phẩm này vô hiệu hoàn toàn các kiểu quét cổng thông dụng. Chúng chặn đ
cố gắng truy cập vào PC thông qua cổng được mở để dùng cho việc chia sẻ file
giao thức SMB (Server Message Blocks), thông báo người dùng biết đó là truy
toàn hoặc truy cập có ý đồ xấu trong mạng máy tính gia đình. Chúng cũng khô
thông tin về HĐH của PC. Một lần nữa, firewall của Aluria thất bại 2/4 thử ng
thiết lập mặc định, tuy nhiên nó lại đạt 100% ở mức thiết lập cao nhất. Firewal
Trend Micro và BitDefender không khóa giao thức chia sẻ SMB và cả firewall
Microsoft cũng để lọt thông tin về HĐH.

Nhiều hơn, nhiều hơn nữa

Các điều khiển của Zone Labs dùng cho trình IM khá mạnh

Tất cả các sản phẩm đ
năng chống spam, ngo
một số bổ sung khác n
sản phẩm của McAfee
Panda có nhiều tiện íc
nhất, ngược lại phần n
đại gia Microsoft lại c
(mặc dù OneCare tích
ích sao lưu và kiểm tr

Ngoại trừ Aluria và Microsoft, tất cả sản phẩm còn lại đều muốn ghi điểm với
cha mẹ, chúng cho phép người dùng khóa những thể loại website không lành n
chẳng hạn: sex, cờ bạc, ma túy. Trend Micro cung cấp một tiện ích lọc URL tu
đương, mặc dù không gọi tính năng này là "parental control" (tiện ích để cha n
kiểm soát việc truy cập của trẻ nhỏ). Trong khi đó CA không cung cấp ngay tr
phẩm của mình mà lại kèm CD riêng chứa K9 Web Protection của BlueCoat. Z
Labs sử dụng công nghệ Smart Filtering Dynamic Real Time để phân loại các

không nằm trong danh sách kiểm soát. BitDefender, McAfee và F-Secure gây
hơn khi cho bố mẹ có thể xác định giờ giấc truy cập Internet.

CA, McAfee, Symantec, Panda, Trend Micro đều cung cấp khả năng kiểm soá
tư để chống xâm nhập thông tin nhạy cảm như: thông tin thẻ tín dụng để lại trê
tính, tuy nhiên chúng lại quá "thận trọng" ở mức thiết lập cao. Ví dụ, thiết lập
ninh cao nhất trong sản phẩm của Symantec sẽ luôn kích hoạt báo động khi m
yêu cầu nhận cookie trên hệ thống thử nghiệm, thậm chí đó là những website c
tốt như của New York Times và pcworld.com, ở chế độ mặc định, các cookie
không được xem là có nguy cơ cao.

Các tính năng thú vị khác: McAfee, Panda, Symantec và Zone Labs kiểm tra c
dụng IM để phát hiện đính kèm (Microsoft chỉ quét trên MSN Messenger). Pa
Trend Micro và Zone Labs cảnh báo người dùng có kết nối Wi-Fi bất hợp phá
(McAfee cũng đưa ra một sản phẩm bảo vệ kết nối Wi-Fi với giá 80USD).

Một số tính năng bổ sung khá tiện lợi, nhưng một số khác lại chỉ làm rối giao

hình như trình điều khiển tập trung của Symantec có một cửa sổ phụ để theo d
thành phần của bộ sản phẩm. Thêm một icon ở khay hệ thống thường xuyên h
báo về tình trạng hoạt động. Nó còn tiếp thị cho các sản phẩm liên quan khác
Data Recovery hiển thị tình trạng thái "chưa có" cho đến khi bạn mua và cài đ
SystemWorks giá 50USD.

HÃY ĐỂ ISP TRANG BỊ BỘ PHẦN MỀM BẢO MẬT

Không ai vui vẻ gì khi bỏ tiền ra để mua các phần mềm bảo mật, nhưng ngư
hiểu rằng chi phí đó là cần thiết để PC an toàn. Điều mà nhiều người không
họ có thể sử dụng các phần mềm đó miễn phí. Do hiểm nguy trên Internet n
một gia tăng nên các nhà cung cấp dịch vụ Internet (ISP) lớn như AOL và
Earthlink đều cung cấp những gói phần mềm bảo vệ cho khách hàng.

Gói phần mềm chuẩn của AOL

Ứng dụng có tên Safety and Security Center bao gồm công cụ chống spam,

cụ kiểm soát truy cập Internet, chặn pop up và chống phishing của AOL đư
hợp với tường lửa, công cụ chống virus và spyware của McAfee.

Gói phần mềm của AOL có dung lượng 28MB, gồm nhiều ứng dụng khác,
đối với người dùng thì nó làm việc như là một ứng dụng thống nhất, xuyên
Một trong những cách AOL hỗ trợ cho khách hàng là cô lập các đe dọa trên
Internet ngay từ server, trước khi đến người dùng cuối.

EARTHLINK chống spyware

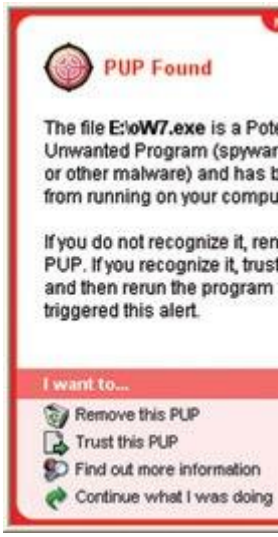
EARTHLINK cũng nỗ lực để tạo ra một ứng dụng bảo mật tất cả trong một
vậy họ đã mua Aluria - công ty phần mềm chống spyware - hồi năm rồi. Hi
EARTHLINK cung cấp miễn phí gói phần mềm Protection Control Center
khách hàng của mình và tính phí 5 USD/tháng cho người dùng khác. Phần
này có dung lượng 16MB, gồm các ứng dụng được tạo bởi 2 công ty và các
dụng chống virus và tường lửa của đối tác Authentium.

Tại sao các ISP gánh tất cả khó khăn và chi phí cho việc bảo mật? Đơn giản

muốn làm cho khách hàng hài lòng .

Cài đặt và tiện ích

Một sản phẩm được xem là dễ sử dụng khi việc cài đặt đơn giản, các tùy chọn cấu hình tổ chức tốt, chạy nhanh và thông báo rõ ràng. Microsoft và Trend Micro đáp ứng những tiêu chuẩn này rất tốt nhưng theo những cách khác nhau. Sản phẩm của Microsoft dễ cấu hình vì nó không có nhiều thứ để cấu hình! Điều này có thể làm cho người dùng cảm thấy hạn chế. Trong khi đó Trend Micro phân bổ rất tốt các tùy chọn trong giao diện đẹp và cấu trúc hợp lý.



McAfee không p
giữa adware và s
mà gọi chung là

Tất cả sản phẩm thử nghiệm đều cài đặt trơn tru và tự động cấu hình. Tuy nhiê

phẩm của McAfee, cài đặt đầy đủ bộ phần mềm này người dùng phải khởi độn

5 lần và tạo một tài khoản (tên người dùng/mật khẩu). Một hộp thoại đề nghị n
dùng nhận thư thông tin về virus cũng như những thông tin khuyến mãi từ Mc
đối tác của McAfee. Ngoài ra, lúc đầu NTN không thể tải về phần cập nhật từ
mà phải sử dụng IE và cho phép mở cửa sổ pop-up tạm thời.

Sản phẩm của CA tích hợp kém nhất, đặt 4 biểu tượng ở khay hệ thống, cộng t
diện chính không liên kết với các điều khiển của Blue Coat.

Symantec có vẻ như "nhiều chuyện" nhất, thường xuyên cảnh báo về trạng thá
cookie. Nếu không thích, bạn có thể dùng sản phẩm của F-Secure vì nó có rất

thiết lập chi tiết nhưng lại ít thông tin hướng dẫn.

Cảnh báo của Microsoft Firewall về hoạt động LimeWire trông ấn tượng hơn cu3a BitDefender.

Tốc độ quét của Panda nhanh nhất, mất khoảng 6 phút 39 giây với 14,7GB tập thư mục trên hệ thống thử nghiệm. Trend Micro về nhì, 7 phút 37 giây. F-Secu nhất, phải mất 28 phút 46 giây. F-Secure giải thích có tốc độ này là vì thực hiệ theo thời gian thực và có tới 5 cơ chế quét gồm 2 cho virus, 1 cho spyware, ro quét thông minh.

Trong kiểm tra sử dụng tài nguyên hệ thống, tất cả sản phẩm được cài đặt mặc đo trên WorldBench 5. Sản phẩm của Microsoft nạp nhẹ nhất, làm tăng thời gi hiện của 9 ứng dụng thử nghiệm lên khoảng 4% (mức "báo động" là 15%). Al

nhiều tài nguyên nhất, tăng gấp đôi thời gian thực hiện của ACDSee PowerPac
Windows Media Encoder. BitDefender tiếp bước làm MS Office 2002 tăng 22
Mozilla tăng 69%.

Cảnh báo người dùng khi có dấu hiệu khả nghi, firewall của Microsoft cho thô
tiết từ tên cho đến đường dẫn của những ứng dụng muốn truy cập Internet. Bit
cấp thông tin về virus rõ ràng hơn ở firewall. McAfee đưa ra một khái niệm m
PUP (potentially unwanted program: chương trình không mong muốn tiềm ẩn)
loại adware hay spyware. Để có thông tin chi tiết về các thông báo của từng sả
bạn đọc có thể truy cập find.pcworld.com/53488.

Nhìn chung, ngay cả những bộ sản phẩm được đánh giá cao của Symantec và
đều không thực hiện hoàn thiện ở tất cả các nhiệm vụ. Với một số người "khó
có kinh nghiệm, có thể họ vẫn muốn kết hợp và chọn lấy những thành phần tốt
các gói sản phẩm bảo mật. Nhưng với đa số người dùng thì tính tiện lợi của bộ
mềm bảo mật trọn gói không gì sánh bằng.

10 THỦ THUẬT VẬN HÀNH BỘ PHẦN MỀM BẢO MẬT

Việc cài đặt và chạy một bộ phần mềm bảo mật đầy đủ chức năng không đơ
giản, nhất là bao gồm cả việc thay thế một sản phẩm của hãng này bằng sản
của hãng khác. Dưới đây là các hướng dẫn cài đặt và bảo trì được tập hợp t
nhiều hãng bảo mật.

1. Gỡ bỏ phần mềm chống virus cũ khỏi PC: Bạn chỉ nên chạy 1 lớp chống
trên 1 máy tính. Gỡ bỏ hoàn toàn cái cũ, khởi động lại máy tính trước khi cà
cái khác. Ngoài ra, nên tắt tường lửa của Microsoft khi sử dụng tường lửa c
hãng khác, tuy nhiên một vài sản phẩm sẽ đề nghị bạn tắt tường lửa mặc đị
cài đặt.

2. Kiểm tra tình trạng "sức khỏe" đĩa cứng: tốt nhất nên chạy tiện ích Chk
của Windows vài lần trước khi tiến hành gỡ bỏ hay sửa c hữa các vấn đề vớ
cứng của bạn. Nhấn start>run, gõ vào chkdsk, nhấn OK.

3. Cập nhật các bản vá Windows mới nhất: chạy ứng dụng cập nhật của Windows để đảm bảo hệ thống của bạn được cập nhật đầy đủ nhất trước kh đặt phần mềm bảo mật, cả những phần mềm bảo mật này người dùng cũng thường xuyên cập nhật.

4. Chuẩn bị thông tin: trong tình huống bạn gọi hỗ trợ từ hãng cung cấp, n ra giấy ngày cài đặt, số sản phẩm (serial number) và số điện thoại hỗ trợ.

5. Chạy một phần mềm chống spyware bổ sung: Nếu muốn bạn có thể chạ tiện ích chống spyware riêng cùng với bộ phần mềm bảo mật, nhưng nên c khi sắp lịch quét hệ thống và đảm bảo rằng chỉ một chương trình dò tìm cũ cập nhật tại 1 thời điểm.

6. Kết nối mạng: thường các máy tính nối mạng bằng VPN và có những thi riêng. Nếu sau khi cài đặt bộ phần mềm bảo mật, máy tính bị treo khi khởi lại, hãy ngắt kết nối mạng. Sau khi khởi động lại thành công, kết nối mạng và để bộ ứng dụng thiết lập cấu hình tường lửa cho bạn (đa phần các sản ph

đều có wizard hướng dẫn).

7. Xử lý vấn đề in ấn và chia sẻ file: tường lửa thường có cấu hình thiết lập để sử dụng dịch vụ chia sẻ tập tin và in trong mạng. Nếu không bạn phải tạo tay để chỉ thị tường lửa cho lưu thông TCP ra cổng 1023 và vào cổng 139.

8. Ghi lại những trường hợp khác lạ: nếu một sản phẩm xảy ra một sự cố biệt - chẳng hạn một thông báo lỗi hay cảnh báo về ý đồ phá hoại – ghi lại c xác toàn bộ thông điệp đó, thậm chí chụp cả màn hình.

9. Gửi đi các file khả nghi: nếu gặp những tập tin hay e-mail đáng ngờ thì mở nó và tự tìm hiểu nó. Hãy gửi chúng tới công ty cung cấp sản phẩm nhu phải đảm bảo theo đúng qui trình.

10. Giữ quyền cập nhật: đây không phải là cường điệu vấn đề. Phần mềm b mật càng hiệu quả khi càng được cập nhật mới nhất và phần cập nhật bổ su thường không cung cấp khi thời hạn đăng ký sử dụng của người dùng khôn

giá trị. Khi một năm sử dụng đã hết đừng quên đăng ký tiếp hay thay thế ph

mềm bảo mật khác.

Hải Phạm

Bộ công cụ bảo mật đáng chú ý năm 2012

Trong 6 mục dưới đây, chúng tôi sẽ cung cấp cho bạn các phần mềm diệt virus, spyware quan trọng cốt lõi, cũng như các mục quan trọng khác như bảo mật trong trình duyệt, Firewall, mã hóa và công cụ quản lý dành cho các bậc cha mẹ.

Diệt virus

Avast Free Antivirus

Trong cuộc cạnh tranh tay ba giữa các phần mềm diệt virus miễn phí phổ biến nhất, Avast Free Antivirus có vẻ như nhận được ít sự chú ý nhất bên ngoài Châu Âu, nhưng chúng tôi hy vọng điều này sẽ thay đổi. Những kiểm tra độc lập với bên thứ ba gần đây của Avast đã cho thấy sự ổn định đáng chú ý, khả năng chống lại tốt hơn so với lại các chương trình nổi tiếng khác là Symantec và Microsoft.

Bên cạnh đó, Avast cũng không "hà tiện" khi cung cấp những tính năng bảo vệ. Phần mềm này sẽ theo dõi máy tính của bạn với rất nhiều "tấm chắn bảo vệ" có thể quét các file và kết nối Internet. Avast được xây dựng với tập hợp các công cụ tự động, bao gồm diệt virus, diệt spyware, chống rootkit, tự dò tìm và bảo vệ đối với truyền P2P, tin nhắn nhanh, lưu lượng mạng và web. Người dùng có thể chọn các thông số quét, chọn các chế độ để loại bỏ một số loại file và chặn một số địa chỉ URL và hoạt động file nào đó, ví như ghi file hoặc thay đổi tên, xóa hoặc format chúng. Người dùng có thể chỉnh sửa các mức độ nhạy cảm dò tìm của chương trình. Cấu trúc mới, rõ ràng sẽ không làm người mới dùng cảm thấy khó khăn khi sử dụng, cũng như những người dùng có kinh nghiệm sẽ thấy có một thay đổi lớn so với thiết kế cũ. Với khả năng bảo vệ trong thời gian thực, cập nhật theo thời gian và rất nhiều tính năng khác, phần mềm miễn phí này rất đáng để bạn trải nghiệm.

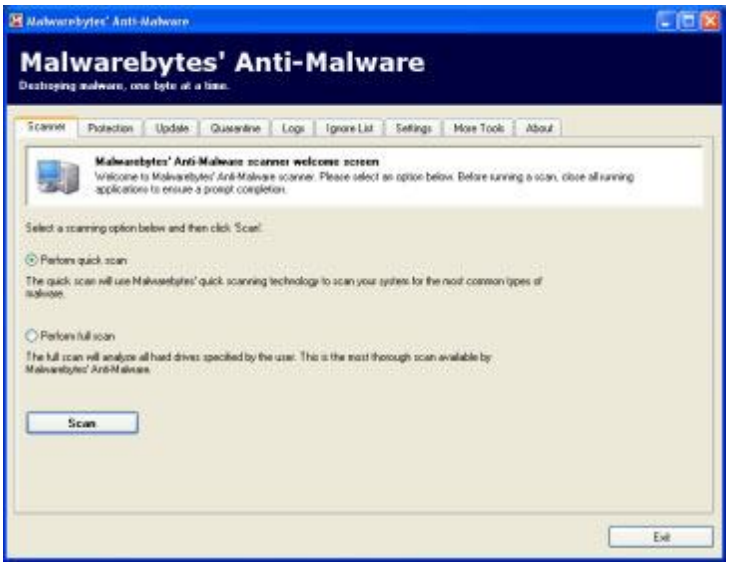
AVG Anti-Virus Free Edition 2011

Mặc dù AVG đã yếu đi trong một vài năm trở lại đây, phần mềm AVG Anti-Virus Free 2011 vẫn mang lại một "làn gió mới" và trở thành một trong những phần mềm bảo mật phổ biến nhất hiện nay với cài đặt được rút ngắn, ổn định hơn, quét nhanh hơn.

Bộ ứng dụng này tiếp tục cung cấp mức độ bảo mật tuyệt vời, nếu không muốn nói là hoàn hảo ngay cả khi chúng phải cạnh tranh ngày càng gay gắt hơn với các phần mềm bảo mật khác. Người dùng yêu thích AVG chắc chắn sẽ muốn cập nhật, và người dùng mới nên cân nhắc tới phần mềm này nếu họ đang tìm kiếm một giải pháp bảo mật vừa hiệu quả vừa miễn phí với các tính năng tuyệt vời.

Loại bỏ Spyware

Malwarebytes Anti-Malware



Malwarebytes' Anti-Malware là một công cụ chống malware miễn phí nhưng mang lại hiệu quả rất ngạc nhiên. Đây thực sự là phần mềm loại bỏ malware nhanh chóng, với chế độ quét nhanh chỉ mất khoảng 10 phút. Công nghệ tìm kiếm đã được chứng tỏ ở rất nhiều máy tính trong quá trình kiểm tra, khi nó cho thấy khả năng xác định sự khác biệt về độ nguy hiểm giữa các ứng dụng.

Bên cạnh đó, ứng dụng này cũng cung cấp các tính năng tuyệt vời. Ứng dụng này hỗ trợ quét nhiều ổ, lựa chọn menu context bao gồm một lựa chọn quét tùy thích đối với các file riêng lẻ và lựa chọn FileAssassin dưới mục More Tools để có thể loại bỏ các file đã bị khóa. Giao diện của ứng dụng khá đơn giản nhưng trông bắt mắt và được sắp xếp tốt. Các thẻ được đặt dưới logo quá cỡ, với một vài lựa chọn dưới mỗi thẻ để giảm thiểu sự lộn xộn. Quá trình cài đặt khá nhanh, cung cấp bản

ghi thay đổi và một tính năng cập nhật định nghĩa file. Người dùng có thể phải trả tiền cho bản cập nhật để có được một số tính năng mới hơn, ví như khả năng bảo vệ thời gian thực và tự động cập nhật. Tuy nhiên, phiên bản miễn phí vẫn gây được sự chú ý nhất định.

ThreatFire AntiVirus Free Edition

ThreatFire cung cấp khả năng ngăn chặn lây nhiễm virus và malware trong thời gian thực bằng cách nhận dạng các hoạt động đáng ngờ khi nó xảy ra, trước khi mã độc cài đặt chính nó trên máy tính của bạn.

ThreatFire thực hiện một số việc rất tốt. Nó sẽ tìm kiếm rootkit, nguy cơ tấn công, virus, sâu máy tính, Trojan, spyware, adware, keylogger,…. Khả năng bảo vệ thời gian thực của phần mềm này không làm chậm máy tính của bạn và cài đặt cao cấp có thể tùy biến được. Người dùng có thể chọn các quá trình yêu thích mà họ tin cậy và tạo các rule khi dò tìm, ví như quét các file SCR được tạo bởi một ứng dụng

email. Người dùng cũng có thể tùy biến lịch quét và tạo một điểm khôi phục hệ thống trước khi chuyển các mối nguy hại vào dạng cách ly. Hoạt động như một phần bổ xung dành cho phần mềm diệt virus bạn đang sử dụng, ThreatFire đã được nâng cấp đáng kể trong một vài năm gần đây.

Bảo mật ngay trong trình duyệt

Web of Trust for Firefox

Web of Trust là một giải pháp đa nguồn, đa trình duyệt đối với việc đánh giá mức độ nguy hiểm của trang web. Bản cảnh báo khá trực quan, đủ dễ và rõ ràng để người dùng đọc, và add-on này cũng không làm ảnh hưởng tới khả năng thực hiện của trình duyệt trong quá trình kiểm tra. Dựa vào trang web bạn truy cập, icon của phần mềm này sẽ biến thành màu đỏ, vàng, hoặc xanh để hiển thị mức độ nguy hiểm. Khi kích vào icon của tiện ích này, một bảng sẽ được hiển thị về các tiêu chí Trustworthiness, Vendor Reliability, Privacy, và Child Safety. Tiện ích này làm việc với các trình duyệt Firefox, Internet Explorer, và Chrome.

NoScript

Tiện ích mở rộng miễn phí dành cho Firefox này sẽ giúp chặn chạy mã JavaScript mà không có sự đồng ý của bạn, nhưng NoScript không cho phép người dùng có thể chặn các phương pháp của chúng. Kích vào nút “S” màu xanh, nhỏ mà

NoScript thêm vào thanh công cụ để cấu hình tiện ích này đối với danh sách trắng các trang web bạn được phép chạy script. NoScript có thể chạy một thông báo audio để thông báo cho người dùng về mã script đã được chặn. Trong số các tính năng cao cấp hơn của tiện ích, đáng chú ý nhất là khả năng chặn plug-in khỏi việc chạy từ các trang không đáng tin cậy. Tuy nhiên, bạn không thể chặn NoScript khỏi việc chạy mà không thoát chúng. Dẫu vậy, NoScript vẫn là cách tuyệt vời để "đe dọa" JavaScript, mà không có cách nào tốt hơn.

Adblock Plus

Một trong những add-on nổi tiếng nhất của Firefox, AdBlock Plus giúp ngăn chặn hiệu quả quảng cáo trực tuyến từ một danh sách đã được xác định trước về các nhà quảng cáo. Người dùng có thể nhanh chóng tùy chỉnh danh sách đó bằng cách kích vào nút "stop sign" của AdBlock Plus ở thanh công cụ điều hướng hoặc thanh hiện

trạng. Adblock Plus hoạt động không gây trở ngại ngay trong background, và phải chuột vào một quảng cáo sẽ hiển thị một hộp thoại, từ đó bạn có thể dễ dàng thêm vào danh sách các quảng cáo bị chặn. Loại bỏ một quảng cáo khỏi một danh sách bị chăn cũng đơn giản như việc kích rồi chọn lựa chọn phù hợp. Trong khi các tiện ích tương tự tồn tại trên các trình duyệt khác, ví như Google Chrome và Opera, không một tiện ích nào có được danh tiếng, có thể hoạt động trên Thunderbird và SeaMonkey.

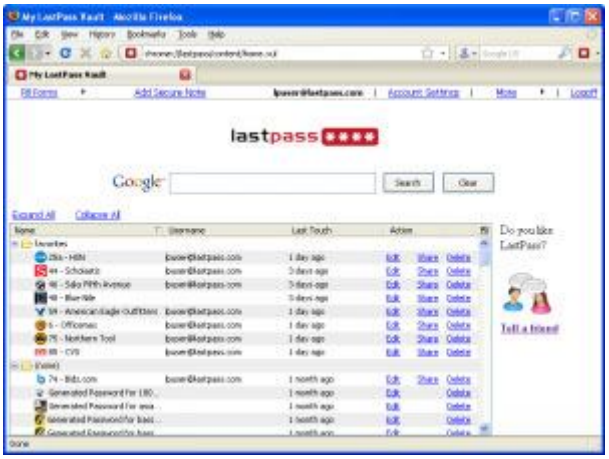
AVG LinkScanner Free Edition 2011

AVG đã làm phục hồi lại LinkScanner như một plug-in độc lập miễn phí dành cho trình duyệt Firefox và Internet Explorer. "Search Shield" sẽ biến kết quả từ cả Google và Yahoo với những chiếc cờ ngay bên cạnh chúng. Cờ xanh trên Google hiển thị một kết quả an toàn để người dùng kích vào, trong khi kết quả an toàn từ Yahoo không hiển thị một lá cờ nào. Điều này có thể do lỗi cấu hình, mặc dù khởi

động lại trình duyệt cũng không làm thay đổi kết quả. Các đường link không an toàn trên cả 2 công cụ tìm kiếm sẽ hiển thị cờ màu đỏ.

Khi kích vào một lá cờ, thông tin chi tiết hơn sẽ được hiển thị. Lá cờ xanh sẽ hiển thị địa chỉ IP, lượng thời gian quét diễn ra, và thời gian và ngày tháng của các lần quét mới được thực hiện. Các lá cờ đỏ sẽ highlight thông tin tương tự, cũng như mục nguy hiểm và tên trang. Khi kích vào một trang bị báo cờ đỏ, người dùng sẽ được dẫn tới một trang cảnh báo, hiển thị lại thông tin cảnh báo – AVG gọi điều này là "Active Surf-Shield". Một đường link ở phía cuối của màn hình bị báo đỏ sẽ cho phép bạn kích vào, mặc dù nó sẽ lưu ý người dùng rằng chúng sẽ tiếp tục chặn những nội dung nguy hiểm tương tự. Không giống các add-on quét kết quả tìm kiếm đối thủ khác, LinkScanner không làm chậm trải nghiệm duyệt web của người dùng.

LastPass Password Manager

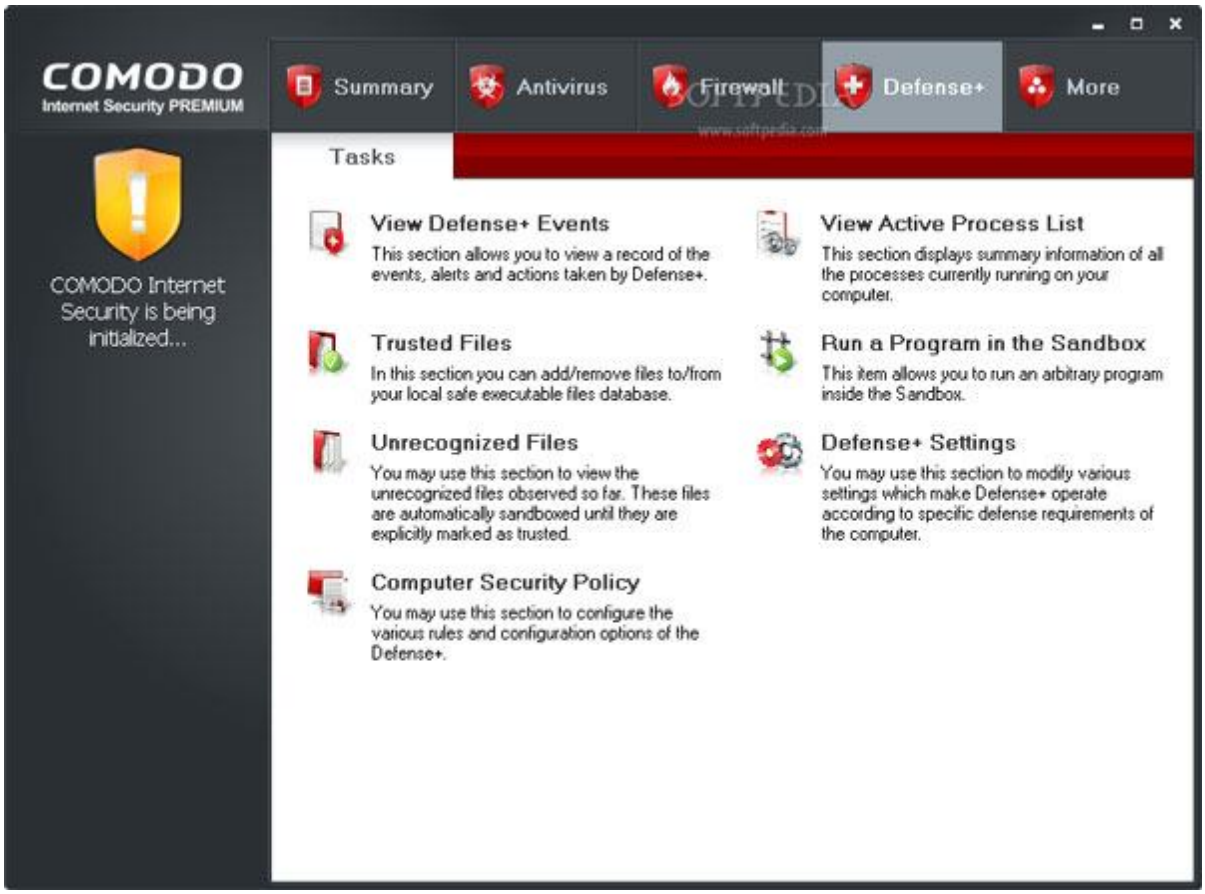


Công cụ quản lý mật khẩu tự động này hỗ trợ rất nhiều hệ điều hành khác nhau. Trên Windows, nó hoạt động với Firefox, Internet Explorer, và Google Chrome, với các bookmarklet sẵn sang cho Opera. Người dùng có thể tạo một mật khẩu chủ, rồi nó sẽ sử dụng tính năng tự động điền form và đăng nhập một lần kích để đơn giản hóa entry mật khẩu.

LastPass sẽ tạo mật khẩu bảo mật cho bạn, cũng như cho phép bảo mật chia sẻ mật khẩu, nhập và xuất mật khẩu, bảo vệ ghi chú, sao lưu và khôi phục mật khẩu. Do dữ liệu được lưu lại trên máy chủ đã được mã hóa của tiện ích, người dùng có thể truy cập mật khẩu của mình từ xa. Nếu bạn lo lắng về việc keylogger, LastPast có thể tạo mật khẩu sử dụng đơn cho bạn. Giao diện là một tập hợp các lĩnh vực để người dùng điền vào, với một số menu kéo lên xuống, nhưng nó vẫn đủ đơn giản để hoạt động.

Firewall

Comodo Internet Security



Comodo Internet Security kết hợp firewall được đánh giá cao của Comodo với phần mềm diệt virus của chúng. Tính năng diệt virus khá tốt nhưng firewall lại còn tốt hơn và do đó người dùng có thể chọn cài đặt mỗi một mục riêng biệt. Đây là một firewall đơn giản nhưng linh hoạt, không chỉ tuyệt vời dành cho người mới dùng mà còn cung cấp thông tin và rất nhiều lựa chọn dành cho người dùng cao cấp.

Online Armor Firewall

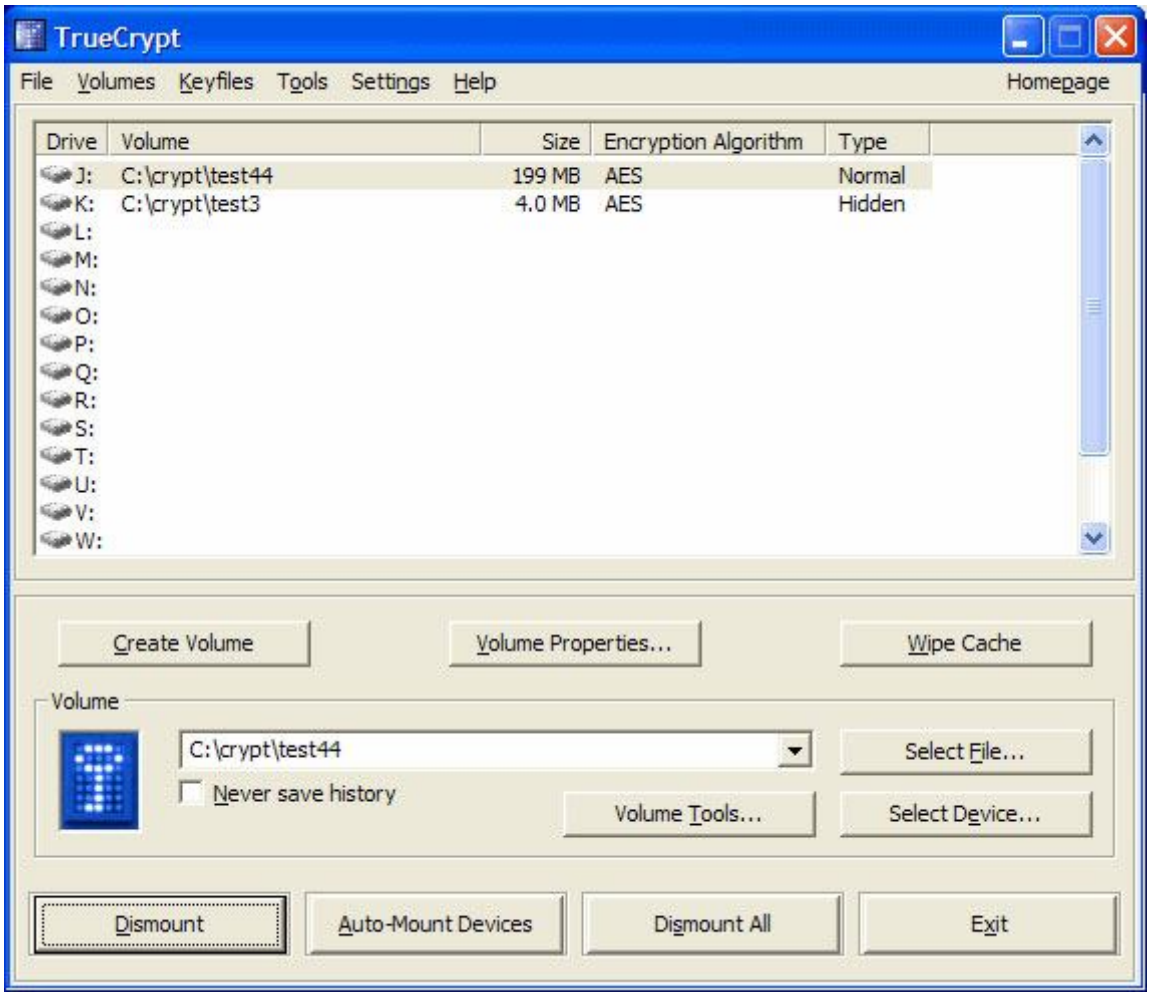
Online Armor mang lại cảm nhận chuyên nghiệp, là phiên bản miễn phí của công cụ bảo mật cao cấp, được chia ra thành các lựa chọn firewall. Quá trình cài đặt khá nhanh, chỉ mất khoảng 30 giây từ việc kích đúp vào trình cài đặt cho tới việc chạy firewall này. Một khi đã được cài đặt, Online Armor mặc định chạy wizard cài đặt, có tên là Safety Check.

Bên cạnh firewall, được cấu hình càng nhiều càng tốt khi khởi động wiward để bạn không phải bận tâm sau này, Online Armor còn cung cấp tính năng bảo vệ keylogger, bảo vệ xáo trộn, mã độc và ngăn chặn sâu máy tính cuungx như bảo vệ tự động khởi động. Phiên bản mất phí cung cấp nhiều hơn tính năng, ví như tính năng bảo vệ chống virus và chống malware, lọc phishing, bảo vệ giao dịch trực

tuyến, và lọc email. Ngay cả khi bị hạn chế, nếu bạn không hài lòng với tính năng firewall đã được nâng cấp rất nhiều của Windows, Online Armor sẽ bảo vệ bạn khỏi những mối tấn công phức tạp.

Mã hóa

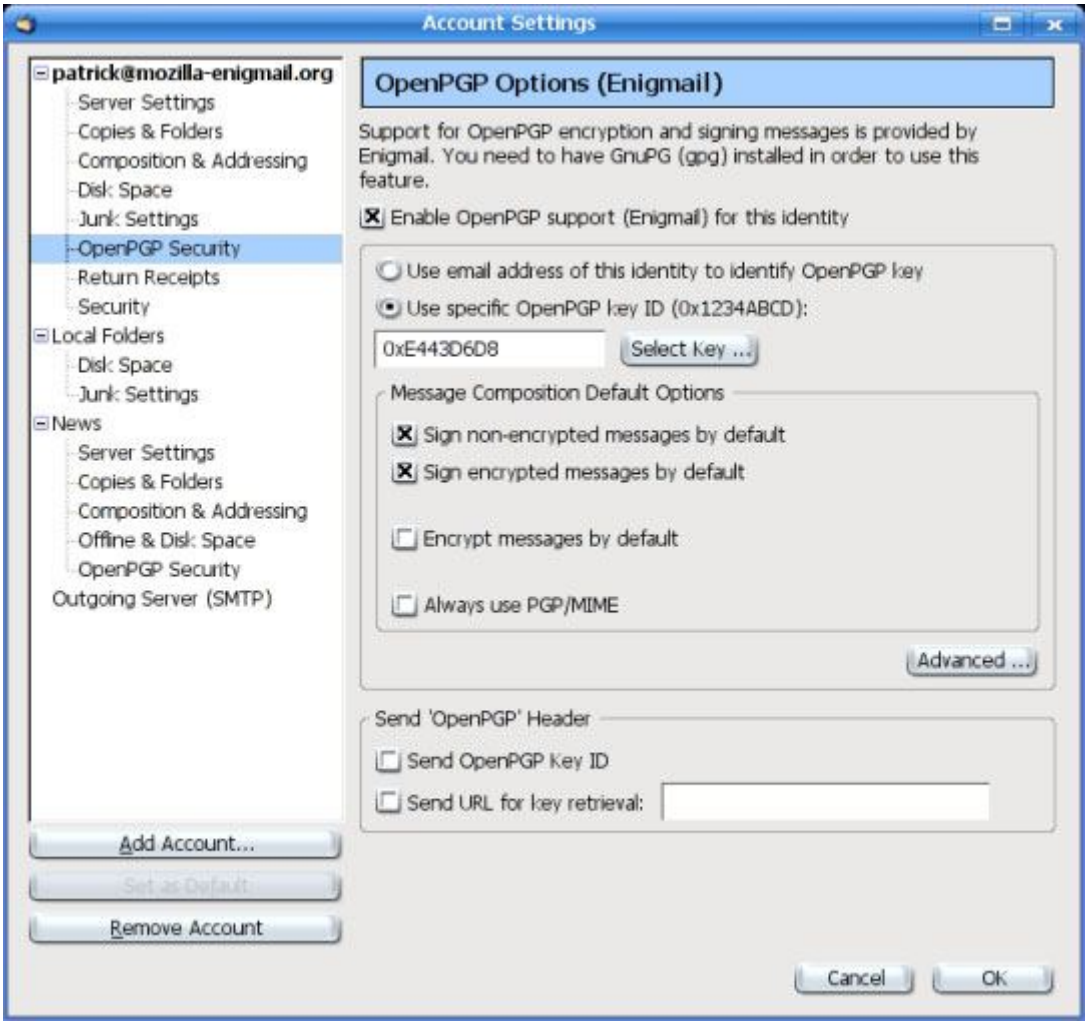
TrueCrypt



Phần mềm mã hóa miễn phí, TrueCrypt cung cấp các tính năng mạnh mẽ liên quan tới việc bảo vệ dữ liệu của chúng khỏi việc bị trộm.

Phần mềm này cung cấp 11 thuật toán để mã hóa các file cá nhân của bạn với mật khẩu bảo vệ. Người dùng có thể lưu trữ dữ liệu đã được mã hóa của mình trong các file (nơi chứa) hoặc phân vùng (thiết bị). TrueCrypt cố gắng hoạt động để cung cấp biện pháp bảo vệ dữ liệu mạnh mẽ, đưa ra mật khẩu phức tạp, và xóa các dấu hiệu của quá trình mã hóa, bao gồm di chuyển chuột và nhấn phím. Thông qua giao diện khá trực quan, khả năng mạnh mẽ, mã hóa nhanh, phần mềm này nhanh chóng trở thành công cụ bảo mật miễn phí được xếp hạng cao.

Enigmail



TrueCrypt có thể mã hóa hệ thống, nhưng nó không làm được gì nhiều trong việc bảo vệ email của bạn. Đó chính là lý do tại sao có sự xuất hiện của Enigmail. Đây là một tiện ích mở rộng dành cho Thunderbird và SeaMonkey, rất cần thiết đối với bất kì ai quan tâm tới việc gửi email có thể bị đọc bởi bất kì ai, bao gồm cả nhà cung cấp dịch vụ Internet.

Tiện ích này sử dụng chuẩn OpenPGP để đăng ký kỹ thuật số email của bạn và có thể cấu hình để phù hợp với nhiều tài khoản email. Người dùng có thể không muốn

mã hóa tất cả các message, nhưng Enigmail là một nguồn giá trị đối với các message chứa thông tin quan trọng. một hướng dẫn cài đặt cũng có sẵn trong trang web chính của tiện ích.

KidZui

KidZui dường như là một trình duyệt dành cho trẻ em với mạng xã hội được tích hợp trong đó. Trẻ em có thể tìm thấy các video Youtube yêu thích của mình, xếp hạng nội dung bằng cách sử dụng tag và chia sẻ ý kiến của mình với bạn bè sử dụng KidZui khác, tất cả đều ở trong một giao diện màu sắc với các nút và nhãn

lớn. KidZui là một trình duyệt chuẩn dành cho trẻ em, dẫu vậy, điều tạo lên sự độc đáo của trình duyệt này lại thuộc về tính an toàn đối với con trẻ.

KidZui là một hệ thống kín, không có lọc, nên tất cả nội dung có sẵn đều được chấp thuận bởi nhà cung cấp trong cơ sở dữ liệu danh sách trắng. Trẻ em có thể khám phá Internet bằng cách sử dụng thanh tìm kiếm/URI, hoặc tìm kiếm bằng một thanh biên bên cạnh, dược sắp xếp theo các chủ đề như khoa học, phim ảnh, ti vi, trò chơi, thể thao và động vật. Đăng ký của cha mẹ là điều bắt buộc trước khi con của bạn tạo một bản nhận diện trực tuyến, và có một bản cập nhật mất phí để bạn có thêm nhiều lựa chọn hơn. Một tiện ích mở rộng dành cho Firefox cũng được hỗ trợ, giúp biến trình duyệt của Mozilla trở thành trải nghiệm KidZui.

Norton Safety Minder

Norton Safety Minder là một ứng dụng Desktop của OnlineFamily.Norton, một hệ thống toàn diện từ thiết kế của Symantec, có khả năng thực hiện quản lý và chặn nội dung mà các bậc cha mẹ muốn con mình không được xem. Dựa vào mong muốn của các bậc cha mẹ, ứng dụng này có thể được dùng để bồi dưỡng thảo luận về nội dung. Đây thực sự không phải là công cụ “cài đặt rồi để đó”.

Có rất nhiều mức độ quản lý về các trang web một đứa trẻ có thể truy cập. Hạn chế có thể tùy thuộc, từ một quyền nghiêm trọng là không truy cập giúp chặn một số

trang web và một số mục, cho tới các thông báo email "mềm mỏng" hơn được gửi tới các bậc cha mẹ khi con họ truy cập các trang web mà không muốn. Về phía con trẻ, chúng sẽ có lựa chọn gửi email cho cha mẹ khi chúng bị chặn – nếu cha mẹ cho phép gửi những email này ngay từ khi cài đặt. Trong khi điều này không phải dành cho tất cả các bậc cha mẹ, bất kì điều gì không nên sử dụng, nên xem đối với cha mẹ hoặc con trẻ trên Internet đều đáng loại bỏ.

K9 Web Protection

K9 Web Protection cung cấp rất nhiều lựa chọn trong việc tùy biến nhu cầu quản lý web từ xa của bạn, và có rất nhiều tính năng lọc được thiết kế sẵn. với hơn 50 mục sắp xếp trang web và một hệ thống đánh giá từ khóa miễn phí, công việc quản lý và chặn web của phần mềm này sẽ được thực hiện tốt hơn. Khá ấn tượng, có một

chút ngạc nhiên là bản ghi chi tiết không chỉ về các trang web bị chặn mà còn cả các trang được phép truy cập.

Quá trình cài đặt và loại bỏ không dễ dàng gì: hãy chuẩn bị cho một quá trình nhiều bước.

Những điểm mới trong bảo mật của Windows 7

Deb Shinder

Quản trị mạng – Trong bài này chúng tôi sẽ giới thiệu cho các bạn về các tính năng bảo mật của Windows 7 và sự nhận xét đứng hoàn toàn trên quan điểm bảo mật liệu nó có đáng để nâng cấp.

Giới thiệu

Phiên bản beta với các tính năng gần như hoàn tất của Windows 7 đã được Microsoft phát hành vào ngày 9 tháng 1 vừa qua, giới công nghệ đang ồn ào bàn tán về những thay đổi đối với giao diện, tuy nhiên Windows 7 còn những gì dưới vẻ ngoài hào nhoáng đó? Những gì đã được thay đổi sẽ ảnh hưởng như thế nào đối với hệ điều hành và vấn đề bảo mật mạng? Trong bài viết này, chúng tôi sẽ cùng các bạn đi tìm hiểu về các tính năng bảo mật của Windows 7 và đưa ra nhận xét đứng trên quan điểm bảo mật xem liệu chúng có đáng với sự nâng cấp. Chúng tôi sẽ tập trung một cách chi tiết vào những thay đổi về mặt giao diện quản lý bảo mật, những thay đổi về User Account Control, những nâng cao đối với BitLocker, về những tính năng mới như AppLocker và Biometric Framework.

Vấn đề phát sinh trong bảo mật của Vista

Đáp trả lại những phàn nàn rằng Windows không an toàn, Microsoft đã tập trung mạnh vào vấn đề bảo mật khi xây dựng hệ điều hành Windows Vista. Tính năng mã hóa ổ đĩa BitLocker drive, các điều khiển cha, phần mềm chống malware đi kèm (Windows Defender) và những cải tiến trong Windows firewall, Data Prevention Execution (DEP), IE với chế độ bảo vệ, bảo vệ dịch vụ và các tính năng quản lý số, nâng

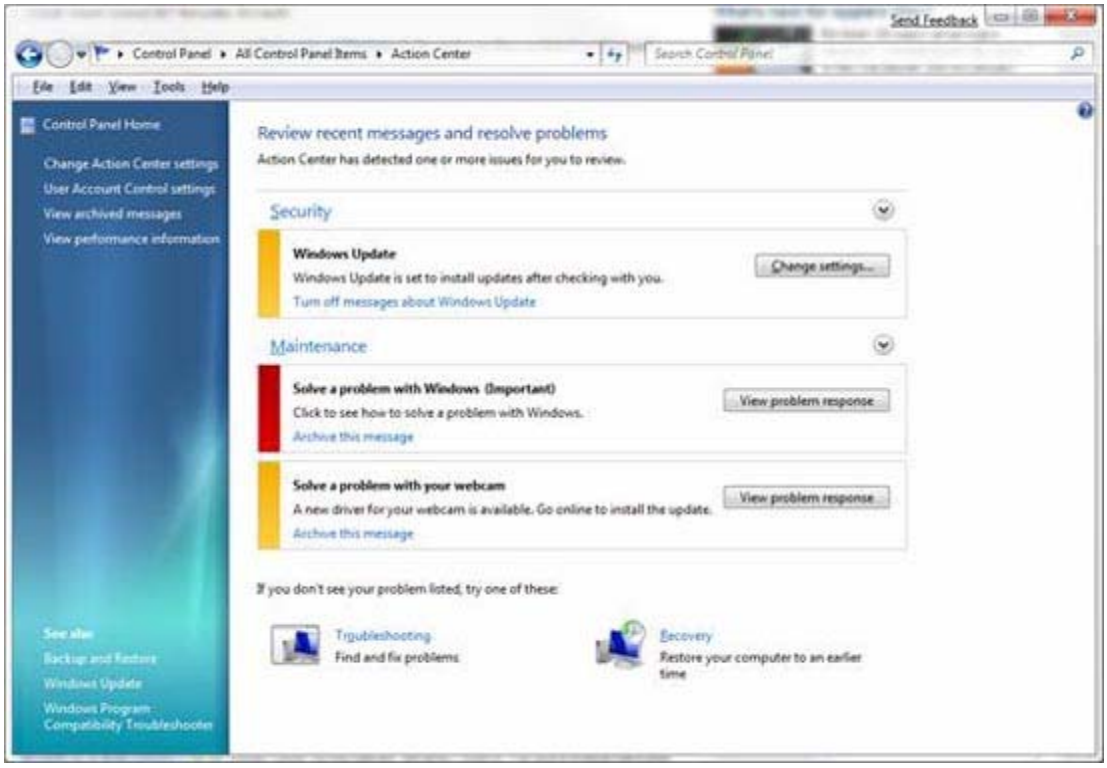
cấp lên Crypto API, Network Access Protection (NAP) client, những cải thiện về Encrypting File System (EFS), các chính sách hạn chế phần mềm và một loạt các nâng cao về bảo mật được giới thiệu trong Vista. Service Pack 1 đã được thêm vào một số các cải thiện có liên quan đến bảo mật, chẳng hạn như thẩm định BitLocker, bộ tạo số giả ngẫu nhiên Random Number Generator (RNG) cũng được thiết kế lại hay việc ký các file Remote Desktop Protocol (RDP),…

Mặc dù vậy tính năng bảo mật mà hầu hết người dùng thông báo là User Account Control (UAC), tính năng dành cho tất cả các tài khoản người dùng, gồm có các tài khoản quản trị, chạy trong chế độ người dùng chuẩn (standard user) một cách mặc định và yêu cầu nâng quyền khi cần đến các đặc quyền cao hơn. Bản tính của UAC cùng với tính năng bảo vệ máy trạm Secure Desktop nhằm ngăn chặn malware truy cập vào máy tính của bạn bằng các nhắc nhở về quyền quản trị nhưng cũng làm bực mình khi chúng xuất hiện quá nhiều và trở thành một sự hạn chế cho Vista.

Thách thức đặt ra cho nhóm Windows 7 là làm thế nào để hệ điều hành này được an toàn hơn Vista trong khi đó sự bảo mật tỏ ra "trong suốt" hơn đối với người dùng.

Security Center và Action Center

Security Center, truy cập thông qua Control Panel và dự định cung cấp một location tập trung để quản lý các thiết lập có liên quan đến bảo mật, đã được giới thiệu trong Windows XP SP2 và tiếp tục trong Vista. Với Windows 7, sự tập trung này mang tính cao hơn. Security Center bị loại bỏ và một Action Center được sử dụng để thay thế cho nó.



Hình 1: Action Center tập trung nhiều nhiệm vụ quản trị mang tính bảo mật

Các thiết lập UAC linh hoạt hơn

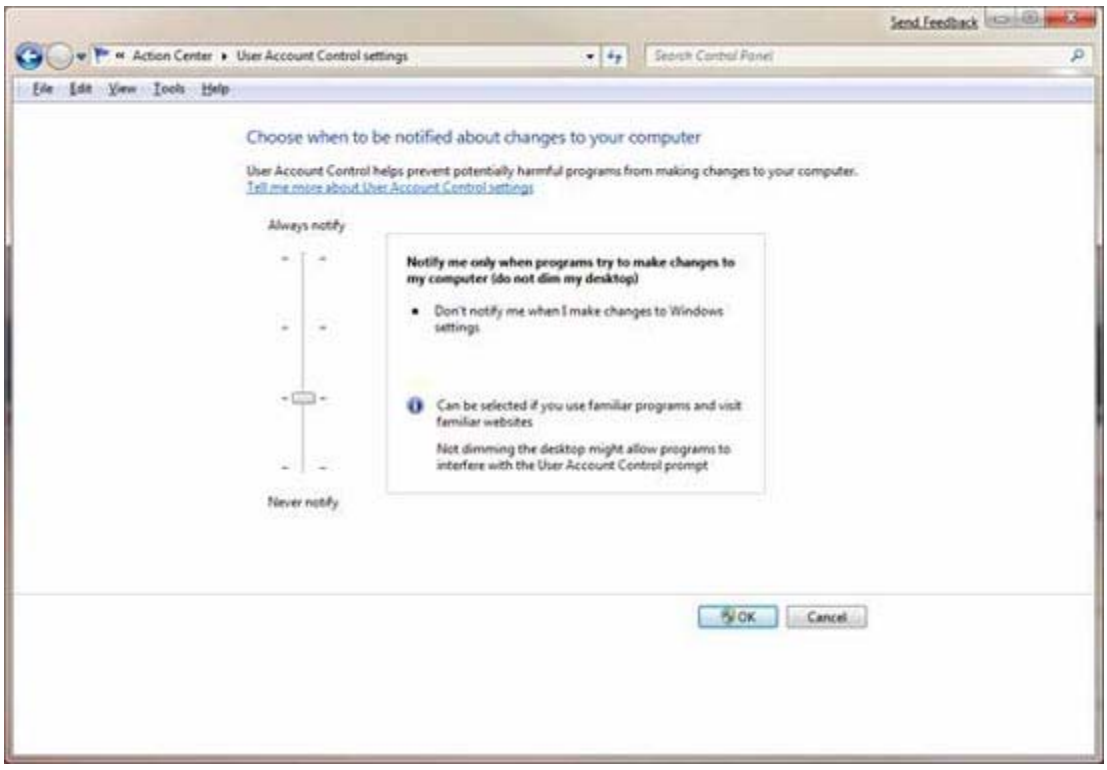
Trong Vista, bạn có thể vô hiệu hóa UAC thông qua Group Policy, tuy nhiên đây không phải là một giải pháp hữu hiệu vì nó bỏ mặc bạn và tạo lỗ hổng cho kẻ tấn công khai thác. Trong Windows 7, bạn có thể thiết lập UAC để nâng quyền mà không cần nhắc nhở, đây là một ý tưởng được phát triển hơn. Các phiên bản Home của Vista không có bộ soạn thảo Group Policy chính vì vậy rất khó khăn cho bạn trong việc chỉnh sửa registry để thực hiện thiết lập UAC. Microsoft đã cải tiến và làm cho nó trở nên dễ dàng hơn nhiều trong việc điều khiển hành vi của UAC trong Windows 7.

Lưu ý:
Các quản trị viên CNTT sẽ bớt căng thẳng trong việc biết người dùng sẽ không thể thay đổi các thiết lập UAC trừ khi họ có các đặc quyền quản trị viên.

Trong phần panel bên trái của Action Center, có một tùy chọn mang tên User Account Control Settings. Hành vi nhắc nhở của UAC được

điều chỉnh thông qua một slider bar với bốn vị trí có thể lựa chọn:

- Always Notify: Bạn sẽ nhận được các nhắc nhở của UAC khi cài đặt phần mềm hoặc thực hiện các thay đổi đối với hệ thống.
- Notify Only When Programs Try to Make Changes: Bạn sẽ nhận được các nhắc nhở nếu một chương trình nào đó yêu cầu các đặc quyền nâng cao, tuy nhiên sẽ không khi bạn thực hiện các thay đổi đối với các thiết lập của Windows (mặc định).
- Notify Only When Programs Try to Make Changes (Do Not Dim the Desktop): Giống như mặc định ngoại từ Secure Desktop bị vô hiệu hóa trong khi nhắc nhở.
- Never Notify: Bạn không được nhắc nhở khi thay đổi các thiết lập Windows hoặc khi cài đặt phần mềm mới (không được tiến cử sử dụng)



Hình 2: Một slider bar cho phép bạn điều khiển UAC nhắc nhở bạn như thế nào trong
Windows 7

Sự nâng cao trong BitLocker

BitLocker, một sản phẩm có trong Vista phiên bản Enterprise và Ultimate, cho phép bạn mã hóa toàn bộ các phân vùng bằng AES, sử dụng Trusted Platform Module (TPM) chip có trong một số máy tính hoặc USB key. Tính năng này nhằm ngăn chặn việc khởi động vào hệ điều hành hoặc truy cập dữ liệu đã được mã hóa một cách trái phép (cho ví dụ, việc cài đặt một instance khác của hệ điều hành và khởi động trong đó). Nó là một công cụ rất hữu dụng cho các hệ thống di động vì nguy cơ mất dữ liệu lớn hơn.

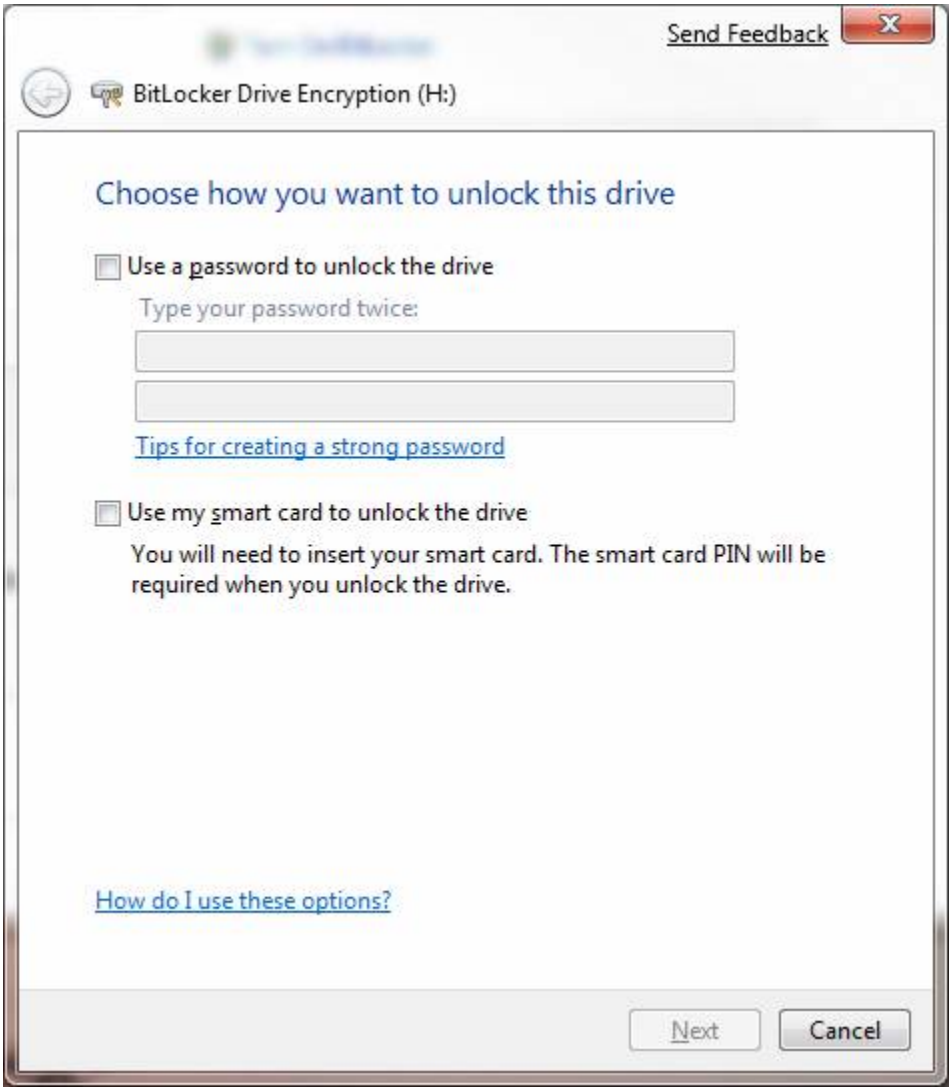
Trong Vista, BitLocker ban đầu chỉ được sử dụng để mã hóa phân vùng mà ở đó hệ điều hành được cài đặt. Service Pack 1 có bổ sung thêm tính năng mã hóa nhiều phân vùng đĩa cố định, tuy nhiên bạn không thể sử dụng nó để mã hóa các ổ đĩa ngoài. Trong Windows 7, BitLocker đã có những cải tiến nâng cao để hỗ trợ mã hóa cho các ổ đĩa ngoài và các thiết bị nhớ flash. Tính năng này hiện được mang tên "BitLocker to Go". Đây là một tính năng được rất nhiều nhiều công ty chờ đợi vì lưu trữ các dữ liệu nhạy cảm trên các USB key đang dần trở nên phổ biến.

Lưu ý:
Bạn cũng có thể sử dụng một chính sách yêu cầu cho các thiết bị ngoài có sự bảo vệ BitLocker trước khi người dùng ghi dữ liệu vào chúng.

BitLocker được quản lý thông qua một applet trong Control Panel, xem thể hiện trong hình 3.

Hình 3: Trong Windows 7, bạn có thể sử dụng mã hóa BitLocker, remove các ổ đĩa cũng như fix chúng.

Bạn có thể chọn cách sử dụng một mật khẩu nào đó để mở đĩa, hoặc có thể sử dụng thẻ thông mình và PIN, xem thể hiện trong hình 4.



Hình 4: Khi mã hóa một đĩa bằng BitLocker, bạn có thể sử dụng mật khẩu hoặc thẻ thông minh để mở Internet

Bạn cũng có thể thiết lập một khóa khôi phục để có thể mở thiết bị của mình nếu quên mất mật khẩu. Khóa khôi phục có thể được lưu vào file hoặc được in hoặc lưu vào một vùng an toàn nào đó (hoặc cả hai). Nó có thể được thực hiện một cách nhanh chóng, phụ thuộc vào kích thước của ổ đĩa. Khi thực hiện sẽ có một thanh bar thể hiện tiến trình được thực hiện như trong hình 5.

Hình 5: Thanh bar quá trình giúp bạn nắm được thông tin trong tiến trình mã hóa

Để có thêm thông tin chi tiết về BitLocker và BitLocker to Go trong Windows 7, bạn sẽ tham khảo tài liệu sau.

AppLocker

Windows 7 còn có một chốt chặn khác đó là AppLocker, đây là một tính năng mới của Group Policy. Tính năng mới này cho phép các quản trị viên có thể điều khiển các phiên bản của các ứng dụng mà người dùng có thể cài đặt và sử dụng. Điều này làm cho bạn hoàn toàn có thể ngăn chặn người dùng cài đặt và chạy các phiên bản của các ứng dụng cũ hơn có chứa các lỗ hổng về bảo mật.

Các trong phiên bản trước đây của Windows có sử dụng Software Restriction Policies để điều khiển chương trình nào mà người dùng có thể chạy. Tuy nhiên AppLocker đã cải thiện để người dùng cấu hình một cách dễ dàng hơn thông qua ba kiểu rule: Path, File Hash và Publisher. Rule Publisher thay thế cho Certificate Rules trong SRP và cho phép bạn có thêm khả năng linh hoạt và nhiều tùy chọn. Chúng cũng khó khăng hơn để có thể bị đánh lừa.

Để có thêm thông tin chi tiết hơn về AppLocker, bạn hãy tham khảo tai đây.

Framework sinh trắc học (Biometric Framework)

Trong Vista, nếu muốn sử dụng đăng nhập theo vân tay, bạn phải sử dụng phần mềm được cung cấp bởi hãng sensor nhận dạng vân tay.

Một tính năng mới trong Windows 7 là Biometric Framework có thể cung cấp sự hỗ trợ một cách bẩm sinh cho các thiết bị hỗ trợ dấu vân tay và làm cho các chuyên gia phát triển trở nên dễ dàng hơn khi đặt vấn đề bảo mật sinh trắc học vào các ứng dụng của họ. Bạn sẽ thấy một applet mới trong Control Panel có tên gọi Biometric Devices được sử dụng để quản lý dấu vân tay, xem thể hiện trong hình 6.

Hình 6: Bạn có thể quản lý các thiết bị sinh trắc học thông qua Control Panel

Các thiết lập có thể được điều chỉnh để cho phép người dùng đăng nhập vào Windows hoặc vào miền bằng thông qua các thiết bị sinh trắc học.

Lưu ý:
Lúc này, các bộ các biến vân tay hiện chỉ là các thiết bị sinh trắc họ được hỗ trợ bởi Windows Biometric Framework.

Windows Biometric Service (WBS) là một phần nằm trong framework cho phép quản lý các bộ đọc dấu vân tay và thực hiện như một I/O proxy giữa các ứng dụng khách và thiết bị sinh trắc học, chính vì vậy các ứng dụng không thể truy cập trực tiếp vào dữ liệu sinh trắc học. Từ đó bảo vệ người dùng một cách an toàn hơn.

Để có thêm thông tin chi tiết về WBS, bạn hãy xem thêm tài liệu ở đây.

Kết luận

Với Windows 7, quả thực Microsoft đã tiếp tục những cố gắng của mình nhằm chung cấp một hệ điều hành mới an toàn hơn trong khi vẫn lắng

nghe người dùng đưa ra những nhận xét của mình về hệ điều hành mới này. Lúc này, nhóm phát triển Windows 7 đã cải thiện được một số tính năng bảo mật từ các hệ điều hành trước dưới bối cảnh về kinh nghiệm người dùng, kinh nghiệm của quản trị viên và các mức bảo mật được thực thi. Đối với những người dùng doanh nghiệp và các quản trị viên mạng, thì những nâng cao về sự bảo mật trong Windows 7 quả thực rất đáng để nâng cấp.

Toàn diện về bảo mật Windows 7

Trong phần hai của loạt bài này, chúng tôi sẽ tiếp tục giới thiệu cho các bạn cách bảo mật Windows 7 và giới thiệu thêm một số chức năng bảo mật ít được biết đến hơn mà hệ điều hành này cung cấp.

>> Hướng dẫn toàn diện về bảo mật Windows 7 – Phần 1

Windows 7 là hệ điều hành máy khách cho các máy tính desktop mới nhất của Microsoft, nó được xây dựng dựa trên những điểm mạnh và sự khắc phục những điểm yếu có trong các hệ điều hành tiền nhiệm, Windows XP và Windows Vista. Mọi khía cạnh của hệ điều hành như, cách chạy các dịch vụ và cách load các ứng dụng sẽ như thế nào, đã làm cho hệ điều hành này trở nên an toàn hơn bao giờ hết. Tất cả các dịch vụ đều được nâng cao và có nhiều tùy chọn bảo mật mới đáng tin cậy hơn. Tuy nhiên những cải tiến cơ bản đối với hệ thống và các dịch vụ mới, Windows 7 còn cung cấp nhiều chức năng bảo mật tốt hơn, nâng cao khả năng thẩm định cũng như các tính năng kiểm tra, khả năng mã hóa các kết nối từ xa và dữ liệu, hệ điều hành này cũng có nhiều cải tiến cho việc bảo vệ các thành phần bên trong, bảo đảm sự an toàn cho hệ thống chẳng hạn như Kernel Patch Protection, Service Hardening, Data Execution Prevention, Address Space Layout Randomization và Mandatory Integrity Levels.

Có thể nói Windows 7 được thiết kế an toàn hơn. Thứ nhất, nó được phát triển trên cơ sở Security Development Lifecycle (SDL) của Microsoft. Thứ hai là được xây dựng để hỗ trợ cho các yêu cầu tiêu chuẩn chung để có được chứng chỉ Evaluation Assurance Level (EAL) 4, đáp ứng tiêu chuẩn xử lý thông tin Federal Information Processing Standard (FIPS) #140-2. Khi được sử dụng như một hệ điều hành độc lập, Windows 7 sẽ bảo vệ tốt người dùng cá nhân. Nó có nhiều công cụ bảo mật hữu dụng bên trong, tuy nhiên chỉ khi được sử dụng với Windows Server 2008 (R2) và Active Directory, thì sự bảo vệ sẽ đạt hiệu quả cao hơn. Bằng việc nâng mức độ bảo mật từ các công cụ như Group Policy, người dùng có thể kiểm soát mọi khía cạnh bảo mật cho desktop. Nếu được sử dụng cho cá nhân hoặc văn phòng nhỏ hệ điều hành này vẫn tỏ ra khá an toàn trong việc ngăn chặn nhiều phương pháp tấn công và có thể được khôi phục một cách nhanh chóng trong trường hợp gặp phải thảm họa, vì vậy mặc dù sẽ có nhiều ưu điểm hơn nếu có Windows 2008 nhưng điều này là không nhất thiết phải có để có được mức bảo mật cao cho Windows 7. Tuy nhiên dù có thể cho rằng Windows 7 về bản thân nó là một hệ điều hành an toàn nhưng điều đó không có nghĩa rằng bạn chỉ dựa vào các cấu hình mặc định mà quên đi việc thực hiện một số điều chỉnh để gia cố thêm

khả năng bảo mật của mình. Cần phải biết rằng bạn chính là đối tượng tấn công của một số dạng malware hay các tấn công trên Internet khi máy tính của bạn được sử dụng trong các mạng công cộng. Cần biết rằng nếu máy tính được sử dụng để truy cập Internet nơi công công thì hệ thống của bạn và mạng mà nó kết nối đến sẽ là miếng mồi ngon cho những kẻ tấn công.

Trong bài này chúng tôi sẽ giới thiệu cho các bạn một số kiến thức cơ bản cần thiết để bảo mật Windows 7 được đúng cách, giúp bạn đạt được mức bảo mật cơ bản, xem xét một số cấu hình bảo mật nâng cao cũng như đi khám phá một số chức năng bảo mật ít được biết đến hơn trong Windows nhằm ngăn chặn và bảo vệ chống lại các tấn công có thể. Giới thiệu một số cách bảo đảm an toàn dữ liệu, thực hiện backup và chạy một cách nhanh chóng nếu bạn gặp phải một số tấn công hoặc bị trục trặc hệ thống ở mức độ thảm khốc ngoài khả năng xử lý của mình. Tiếp đó là một số khái niệm bảo mật, cách "làm vững chắc" Windows 7, cách cài đặt và cung cấp bảo mật cho các ứng dụng đang chạy, cách quản lý bảo mật trên một hệ thống Windows 7 và ngăn chặn các vấn đề gây ra bởi malware. Bài viết cũng giới thiệu cho quá trình bảo vệ dữ liệu, các tính năng backup và khôi phục hệ điều hành, cách khôi phục hệ điều hành trở về trạng thái hoạt động trước đó, một số cách bảo vệ dữ liệu và trạng thái hệ thống nếu thảm họa xảy ra. Chúng tôi cũng giới thiệu một số chiến lược để thực hiện nhanh chóng các công việc đó. Các chủ đề được giới thiệu trong bài cũng gồm có cách làm việc an toàn trong khi online,

cách cấu hình điều khiển sinh trắc học để kiểm soát truy cập nâng cao, cách và thời điểm được sử dụng với Windows Server 2008 (và Active Directory) như thế nào, cách bạn có thể tích hợp một cách an toàn các tùy chọn cho việc kiểm soát, quản lý và kiểm tra. Mục tiêu của bài viết này là để giới thiệu cho các bạn các tính năng bảo mật của Windows 7, những nâng cao và ứng dụng của chúng cũng như cung cấp cho bạn những kiến thức về việc lên kế hoạch, sử dụng đúng các tính năng bảo mật này. Các khái niệm mà chúng tôi giới thiệu sẽ được chia nhỏ và được tổ chức theo phương pháp khối.

Lưu ý: Nếu làm việc trong công ty hoặc môi trường chuyên nghiệp khác, các bạn không nên thực hiện các điều chỉnh với máy tính của công ty. Hãy thực hiện theo đúng kế hoạch (hay chính sách) bảo mật đã được ban bố, cũng như những hành động, nguyên lý và hướng dẫn tốt nhất đã được công bố trong tổ chức. Nếu chưa quen với các chủ đề bảo mật và các sản phẩm của Microsoft, hãy đọc tài liệu hướng dẫn của sản phẩm trước khi áp dụng bất cứ thay đổi nào cho hệ thống.

Quản lý và kiểm tra bảo mật

Windows 7 có thể an toàn như một pháo đài. Nếu sử dụng Windows 7 trong doanh nghiệp, bạn có thể sử dụng cơ sở dữ liệu Active Directory và lợi dụng nhiều tính năng nâng cao về bảo mật khi đăng nhập vào một Domain, hoặc Group Policy nhằm thực thi bảo mật ở mức cao hơn. Dù bằng cách nào thì sự quản lý tập trung

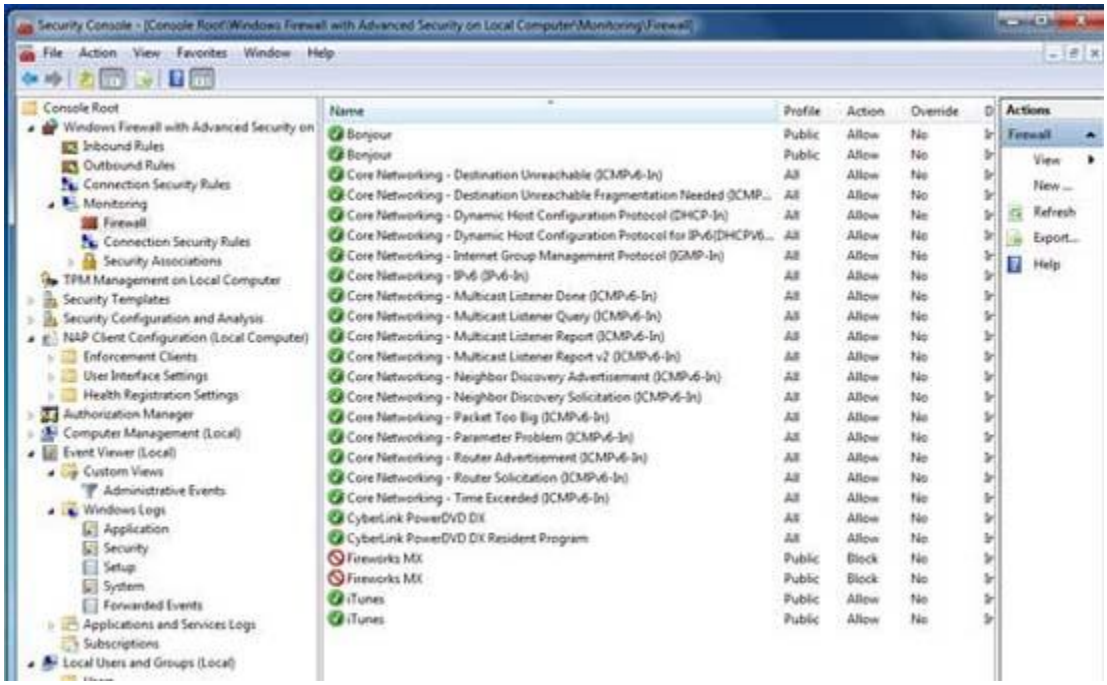
các công cụ bảo mật, các thiết lập và bản ghi là vấn đề quan trọng cần xem xét khi áp dụng bảo mật – cách bạn sẽ quản lý nó, kiểm tra nó và sau đó nâng cấp nó khi đã cài đặt và cấu hình như thế nào? Với Windows 7, bạn sẽ thấy có nhiều thay đổi dưới layout cơ bản về các công cụ và dịch vụ dùng cho mục đích bảo mật. Cho ví dụ từ khóa 'Security' trong menu Start mà chúng ta đã thảo luận là nơi tập trung sự việc quản lý ứng dụng bảo mật cho Windows 7.

Nguyên tắc chủ đạo là bạn cần phải áp dụng bảo mật (sau đó quản lý nó) một cách dễ dàng. Không ai thích dò dẫm toàn hệ điều hành để tìm ra các ứng dụng, dịch vụ, bản ghi và sự kiện hay các hành động cấu hình, kiểm tra. Với Windows 7, người ta có thể nói rằng một người dùng mới có thể bị lạc giữa một biển đường dẫn, wizard, applet và các giao diện điều khiển trước khi tìm ra và cấu hình Windows Firewall, tính năng bảo mật cơ bản nhất được cung cấp, thậm chí một số kỹ thuật viên nhiều kinh nghiệm có thể cho rằng vẫn còn nhiều rắc rối đi chăng nữa thì đây vẫn là phiên bản Windows cho phép quản lý dễ dàng nhất tất cả các thông tin bằng cách đánh chỉ số và cung cấp qua việc tìm kiếm trong menu Start.

Ngoài menu Start, một cách thuận tiện khác cho việc quản lý nhiều chức năng bảo mật trong Windows 7 là xây dựng một Microsoft Management Console (MMC) tùy chỉnh và bổ sung thêm các công cụ của bạn vào nó. Một trong những thứ sẽ làm lúng túng nhiều người dùng Windows mới là các giải pháp doanh nghiệp của

Microsoft cung cấp một cách mới để tập trung sự điều khiển và kiểm tra mọi thứ trên các hệ thống trong mạng của bạn (MOM là một ví dụ hoàn hảo). Hệ điều hành khách là một đơn vị độc lập (stand-alone) nhưng cũng phải được bảo vệ cục bộ, vì vậy với người dùng gia đình, một giao diện quản lý tùy chỉnh sẽ là câu trả lời cho các câu hỏi về quản lý bảo mật tập trung. Tuy nhiên không may mắn, Security Center lại được phân nhỏ thành các Control Panel applet và MMC Snap-in – vậy bạn có thể tập trung sự truy cập nhanh chóng vào các công cụ chính như thế nào? Để áp dụng bảo mật cho hệ điều hành Windows 7, bạn phải truy cập nhiều vùng khác nhau của hệ thống để tùy chỉnh cấu hình nhằm "làm vững chắc" nó, vậy nếu được quyền chọn các ứng dụng và các chức năng cần thiết và đặt chúng vào một vùng nào đó, thì bạn có thể nhanh chóng và dễ dàng truy cập trở lại chúng để thẩm định bảo mật và xem lại các bản ghi.

Để tạo một giao diện quen thuộc, hãy vào menu Start và đánh vào đó 'MMC /A', khi đó bạn sẽ khởi chạy một Microsoft Management Console (MMC) mới. Có thể lưu nó vào bất cứ vị trí nào trên hệ thống và đặt tên cho nó là bất cứ gì bạn muốn. Để định cư, bạn cần phải vào menu File và chọn Add/Remove Snap-in. Thêm tất cả các công cụ mà bạn muốn hoặc cần. Hình 1 hiển thị một giao diện tùy chỉnh với hầu hết nếu không phải tất cả các tùy chọn bảo mật có sẵn.



Hình 1: Tạo giao diện bảo mật tập trung tùy chỉnh với Microsoft Management Console Snap-In

Bạn sẽ thấy nhiều công cụ hữu dụng bên trong các tùy chọn snap-in có sẵn. Cho ví dụ, TPM Management là một Microsoft Management Console (MMC) snap-in cho phép các quản trị viên có thể tương tác với Trusted Platform Module (TPM) Services. TPM services được sử dụng để quản trị phần cứng bảo mật TPM trong máy tính của bạn. Điều này có nghĩa bạn cần phần cứng chuyên dụng, nâng cấp BIOS và chọn đúng chíp CPU. Cũng giống như việc ảo hóa cần một chíp chuyên dụng, TPM cũng vậy. TPM là một cách giới thiệu mức bảo mật phần cứng mới cho phương trình để bạn biết mình đang dần có một hệ thống vững chắc. Bạn có thể quản lý nó ở đây nếu thuân thủ theo TPM. TPM sẽ sử dụng bus phần cứng để

truyền tải các thông báo và có thể được sử dụng kết hợp với các tính năng phần mềm giống như BitLocker.

Khi đã tạo các giao diện điều khiển và đã biết cách truy cập vào các vùng để áp dụng các cấu hình bảo mật bên trong hệ điều hành, bước tiếp theo của bạn là kiểm tra hệ thống của mình. Có nhiều cách để thực hiện điều đó. Cho ví dụ, bạn có thể sử dụng phương pháp đơn giản (người dùng gia đình) và chỉ cần để ý đến nó theo thời gian trên một lịch trình đơn giản. Giống như, các tối chủ nhật sau khi lướt mạng, bạn kiểm tra các bản ghi tường lửa và các bản ghi Event Viewer trong giao diện điều khiển. Nếu đào sâu vào các tùy chọn có thể cấu hình, bạn sẽ phát hiện thấy mình có thể lập lịch trình các cảnh báo và thông báo, lọc các bản ghi và tự động lưu để xem lại,... Bảo đảm rằng bạn cần phải để ý đến mọi thứ. Bởi lẽ bảo mật tốt không có nghĩa là bảo mật đó sẽ được duy trì mãi mãi.

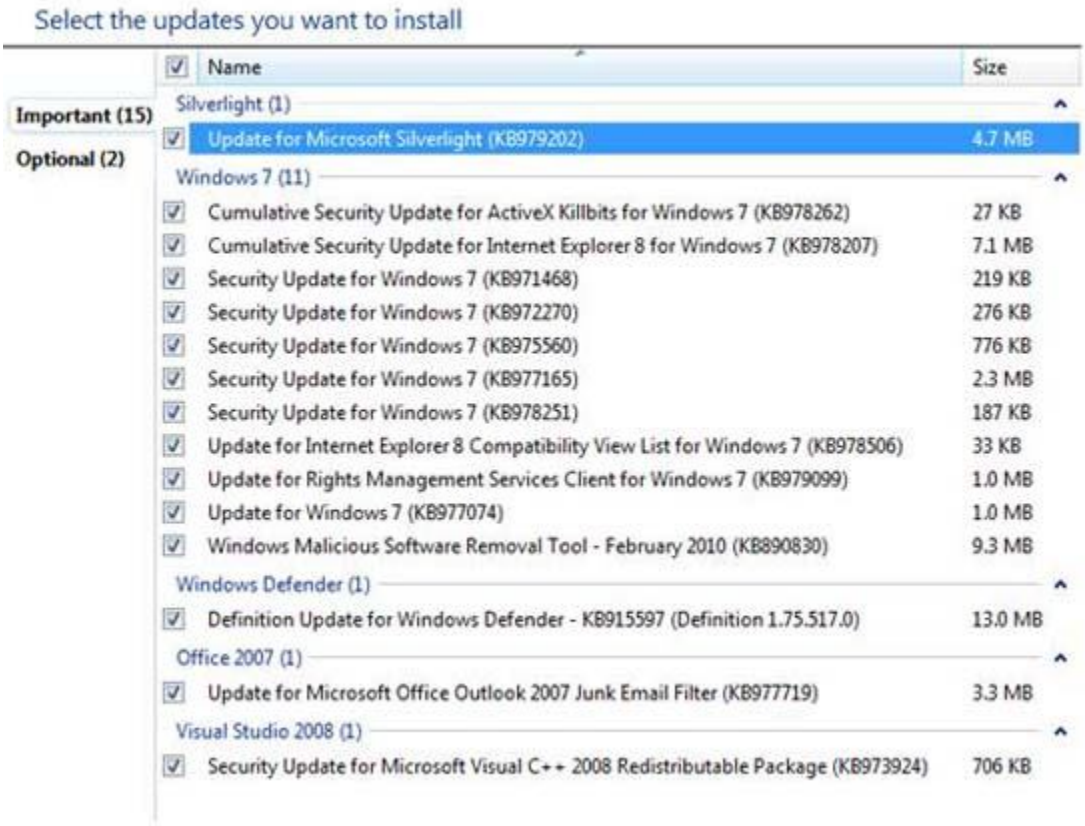
Vậy, nói tóm lại – cách điển hình để bạn có thể truy cập và áp dụng bảo mật cho Windows 7 được nhanh là bên trong menu Start. Bạn cũng có thể làm việc bên trong Control Panel (các applet chẳng hạn như Administrative Tools, Windows Firewall và Windows Defender) để tăng truy cập vào các công cụ và các thiết lập bảo mật. Cũng có thể tạo một MMC tùy chỉnh và cấu hình nó nhằm tăng sự truy cập vào các công cụ khác vẫn còn ẩn khuất đâu đó, cũng như cung cấp một giao diện điều khiển tập trung để quản trị vấn đề bảo mật. Mặc dù có thể duyệt nhiều

vùng khác nhau trong hệ điều hành và thực hiện cùng một việc, tuy nhiên hy vọng mẹo này có thể giúp bạn áp dụng bảo mật dễ dàng hơn bằng cách cung cấp sự truy cập vào các công cụ bảo mật có trong Windows 7. Ngoài ra bạn có thể áp dụng các template; tạo các nhiệm vụ và hành động và thậm chí tạo các cấu hình bảo mật với các tập công cụ nâng cao.

Mẹo: Bạn cũng có thể áp dụng việc quản lý bảo mật trong các công cụ giống như PowerShell và Netsh (chẳng hạn như lệnh netsh advfirewall), từ đó có nhiều cách dễ dàng có thể áp dụng nhiều tùy chọn dựa trên kịch bản hay dòng lệnh để triển khai bảo mật trong Windows 7. Cũng có thể sử dụng các nhiệm vụ 'task' để bắt đầu các công việc, kịch bản hoặc file batch và các dịch vụ để bạn có thể (ví dụ) giữ một backup các bản ghi của Event Viewer cho hành động thẩm định, xem lại và cất giấu an toàn.

Tiếp đến, cần có khả năng truy cập và cấu hình thêm hệ thống cơ bản sau khi cài đặt để "làm vững chắc" nó và do Windows Updates là không thể tránh được, nên bạn cần tạo một kế hoạch để chúng có thể download và cài đặt ngay lập tức. Đại đa số, các nâng cấp đều đến sau các tấn công, vì vậy test và cài đặc chúng ngay khi có thể là một hành động cần làm. Có nhiều lý do tại sao chúng được phát hành. Và được đặt tên là 'Security Updates' như thể hiện trong hình 2. Các nâng cấp này

luôn được đánh số và bạn có thể được nghiên cứu trực tuyến để tìm kiếm thêm thông tin.



Hình 2: Cài đặt Windows Security Updates với Windows Update

Bạn cũng cần có được các gói dịch vụ mới được phát hành và áp dụng lại chúng nếu cần. Các ứng dụng và các dịch vụ đang chạy khác trong hệ thống cũng cần được quản lý, kiểm tra và nâng cấp thường xuyên, nhất là với các chương trình phát hiện và loại bỏ Virus, Spyware.

Khi hệ thống của bạn đã được vá và được cấu hình cho sử dụng, nhiệm vụ tiếp theo là cài đặt Microsoft Security Essentials (MSE), một chương trình Antivirus (AV) của nhóm thứ ba, cấu hình Windows Defender (spyware) để sử dụng và cấu hình bảo mật nhằm phát hiện (malware) phần mềm mã độc.

Lưu ý: Microsoft gần đây đã phát hành một dòng phần mềm bảo mật mới mang tên Forefront. Dòng sản phẩm này bao phủ tất cả các khía cạnh trong triển khai và quản lý bảo mật trong doanh nghiệp. Chúng cũng tạo sự chắc chắn rằng hệ điều hành khách được an toàn với chức năng mới, chẳng hạn như Microsoft Antivirus, có bên trong gói sản phẩm MSE.