**BAN CƠ YẾU CHÍNH PHỦ**

**HỌC VIỆN KỸ THUẬT MẬT MÃ**

KHOA AN TOÀN THÔNG TIN

-----🙞🙜🕮🙞🙜-----

****

**BÀI TẬP LỚN MÔN HỌC PHÒNG CHỐNG & ĐIỀU TRA TỘI PHẠM MẠNG MÁY TÍNH**

**Đề Tài : Windows Forensics Analysis - chapter 1**

***Nhóm sinh viên thực hiện:*** Nguyễn Huy Cường

Tạ Khắc An

Hà Nội,12/2019

**Mục Lục**

[Giới Thiệu 11](#_Toc25823152)

[Live Response 13](#_Toc25823153)

[Locard’s Exchange Principle 15](#_Toc25823154)

[Order of Volatility 19](#_Toc25823155)

[What Data to Collect 21](#_Toc25823156)

[System Time 23](#_Toc25823157)

[PsLoggedOn 24](#_Toc25823158)

[Net Sessions ( không áp dụng win 10 ) 25](#_Toc25823159)

[LogonSesions 25](#_Toc25823160)

[Open Files 27](#_Toc25823161)

[Network Information (Cached NetBIOS Name Table) 27](#_Toc25823162)

[Network Connections 29](#_Toc25823163)

[Netstat 30](#_Toc25823164)

[Process Information 32](#_Toc25823165)

[Tlist 34](#_Toc25823166)

[Tasklist 35](#_Toc25823167)

[PsList 35](#_Toc25823168)

[ListDLLs 36](#_Toc25823169)

[Handle 37](#_Toc25823170)

[Process-to-Port Mapping 38](#_Toc25823171)

[Netstat 38](#_Toc25823172)

[Fport 39](#_Toc25823173)

[Tcpvcon 39](#_Toc25823174)

[Process Memory 40](#_Toc25823175)

[Network Status 40](#_Toc25823176)

[Ipconfig 40](#_Toc25823177)

[Clipboard Contents 43](#_Toc25823178)

[Service/Driver Information 45](#_Toc25823179)

[Command History 46](#_Toc25823180)

[Mapped Drives 47](#_Toc25823181)

[Shares 48](#_Toc25823182)

[Nonvolatile Information 49](#_Toc25823183)

[Registry Settings 49](#_Toc25823184)

[Autoruns 50](#_Toc25823185)

[Event Logs 53](#_Toc25823186)

[Devices and Other Information 54](#_Toc25823187)

[A Word about Picking Your Tools 54](#_Toc25823188)

[Live-Response Methodologies 56](#_Toc25823189)

[TÓM LƯỢC 62](#_Toc25823190)

**Hình Ảnh**

[Figure 1: Displaying the System Date and Time on Windows 10 24](#_Toc25823300)

[Figure 2 :Output of psloggedon.exe on Windows 2000 25](#_Toc25823301)

[Figure 3:Output of the net sessions Command on Windows 2003 26](#_Toc25823302)

[Figure 4 : Output of logonsessions.exe on Windows XP 27](#_Toc25823303)

[Figure 5 :NetBIOS Name Table Cache 29](#_Toc25823304)

[Figure 6 :Output of nbtstat –A 192.168.1.22 30](#_Toc25823305)

[Figure 7: Excerpt from the Output of the netstat –ano Command on Windows 10 32](#_Toc25823306)

[Figure 8:Excerpt of Output of handle.exe 38](#_Toc25823307)

[Figure 9:Excerpt of Output from 40](#_Toc25823308)

[Figure 10 : Minh họa một đoạn trích của đầu ra được trả về từ ndis.exe. 43](#_Toc25823309)

[Figure 11:Trích từ Đầu ra của svc.exe trên Windows XP 47](#_Toc25823310)

[Figure 12:Đầu ra của di.exe 49](#_Toc25823311)

[Figure 13:AutoComplete Settings Dialog Box on Internet Explorer 6.0 53](#_Toc25823312)

[Figure 14:Nigilant32 GUI 59](#_Toc25823313)

**Lời Mở Đầu**

Mục đích của cuốn sách này, như với phiên bản đầu tiên, là để giải quyết nhu cầu. Một vấn đề mà nhiều người ứng phó sự cố và giám định pháp y máy tính đã thấy rằng có một quá phụ thuộc vào những gì các công cụ phân tích pháp y đang nói với chúng tôi, mà không thực sự hiểu được thông tin này đến từ đâu hoặc làm thế nào nó được tạo ra hoặc có nguồn gốc.

The “Age of Nintendo Forensics,”, tức là về việc tải một hình ảnh thu được vào một phân tích ứng dụng và nhấn một nút . Là nhà phân tích và giám khảo, chúng tôi không còn có thể mong đợi để điều tra một trường hợp theo cách như vậy. Tội phạm mạng đã gia tăng độ tinh vi, và các nhà điều tra cần phải hiểu những gì có sẵn trên một hệ thống, cũng như những thứ đó tạo tác được tạo ra và sửa đổi. Với trình độ kiến ​​thức này, chúng tôi hiểu rằng sự vắng mặt của một cổ vật tự nó là một tạo tác động . Ngoài ra, ngày càng có nhiều bài thuyết trình và tài liệu có sẵn về điều tra số , hoặc các kỹ thuật được sử dụng để phân tích khoa học điều tra số khó hơn. Không chỉ vậy, đã có những bài thuyết trình tại các hội nghị lớn thảo luận kỹ thuật chống điều tra số , sử dụng công cụ đào tạo và công cụ phản hồi họ. Cuốn sách này nhằm giải quyết nhu cầu về mức độ chi tiết, chi tiết hơn của hiểu biết. Mục đích của nó không chỉ là để chứng minh những thông tin có sẵn cho điều tra viên trên cả hệ thống Windows trực tiếp cũng như trong hình ảnh thu được mà còn cung cấp thông tin về cách định vị các đồ tạo tác bổ sung có thể được quan tâm, và tương quan nhiều nguồn dữ liệu để xây dựng một bức tranh đầy đủ hơn về vụ việc.

Lý do chính của tôi để viết cuốn sách này là để tôi có thể trả lại cho cộng đồng và lĩnh vực nỗ lực đã mang lại cho tôi rất nhiều. Kể từ khi tôi tham gia vào thông tin lĩnh vực an ninh hơn 12 năm trước (trước đó, tôi đã ở trong quân đội và tham gia vào hoạt động thể chất và bảo mật thông tin liên lạc), tôi đã gặp rất nhiều người tuyệt vời và làm rất nhiều điều thực sự thú vị. Theo thời gian, mọi người đã chia sẻ những điều với tôi vô cùng hữu ích, và một số trong những điều đó đã đóng vai trò là bước đệm để nghiên cứu thêm. Một số nghiên cứu đó đã được tìm thấy trong các bài thuyết trình mà tôi đã đưa ra tại các hội nghị khác nhau, và từ đó, những người khác đã đặt câu hỏi và cung cấp cái nhìn sâu sắc và câu trả lời đã giúp thúc đẩy điều đó nghiên cứu về phía trước. Việc trao đổi thông tin nhiều lần và tham gia thảo luận có di chuyển cả sự quan tâm và mức độ kiến ​​thức về phía trước, tiến lên lĩnh vực. Đây là của tôi cố gắng trả lại và làm như vậy, mở rộng trường thêm một chút nữa.

Cuốn sách này nhằm giải quyết các khía cạnh kỹ thuật thu thập và phân tích dữ liệu trong quá trình điều tra trực tiếp và hậu sự của các hệ thống Windows. Cuốn sách này không bao gồm tất cả mọi thứ có thể có thể được giải quyết. Vẫn còn chỗ đáng kể cho nghiên cứu trong một số lĩnh vực, và rất nhiều thông tin cần phải được xếp vào mục lục. Hy vọng của tôi là cuốn sách này sẽ đánh thức người đọc về những khả năng và cơ hội tồn tại bên trong .Các hệ thống Windows để điều tra và phân tích toàn diện hơn

**ĐỐI TƯỢNG HƯỚNG ĐẾN**

Cuốn sách này tập trung vào một lĩnh vực kỹ thuật khá hẹp. phân tích, nhưng nó dành cho bất cứ ai làm, có thể làm hoặc đang suy nghĩ về việc thực hiện phân tích khoa học pháp y của các hệ thống Windows. Cuốn sách này sẽ là một tài liệu tham khảo hữu ích cho nhiều người, và của tôi hy vọng là bất kỳ độc giả nào ban đầu cảm thấy rằng cuốn sách nằm trên đầu của họ hoặc vượt ra ngoài tiếp cận kỹ thuật sẽ sử dụng một số tài liệu họ tìm thấy làm điểm khởi đầu và là cơ sở cho câu hỏi và nghiên cứu thêm. Khi tôi bắt đầu viết ấn bản đầu tiên của cuốn sách này, nó đã không dự định là phiên bản thứ hai hoặc tiếp theo cho cuốn sách đầu tiên của tôi, Windows Forensics and Incident Phục hồi, được xuất bản bởi Addison-Wesley vào tháng 7 năm 2004. Thay vào đó, ý định của tôi là chuyển đi từ một trọng tâm tổng quát hơn và cung cấp một nguồn lực cho không chỉ bản thân tôi mà còn cho những người khác làm việc trong lĩnh vực phân tích pháp y máy tính. Phiên bản thứ hai này được viết để tiếp tục tĩnh mạch, đặc biệt là trong thực tế là Microsoft tiếp tục phát triển và phát hành mới các phiên bản của hệ điều hành Windows, mỗi phiên bản tiếp theo có sự độc đáo của riêng nó xoắn và sắc thái. Khi viết cuốn sách này, mục tiêu của tôi là cung cấp một nguồn lực cho các nhà phân tích pháp y, điều tra viên, và ứng phó sự cố. Hy vọng của tôi là không chỉ cung cấp tài liệu hữu ích cho những người hiện tại thực hiện điều tra pháp y nhưng cũng thấu hiểu các quản trị viên hệ thống đã từng phải đối mặt với các hoạt động ứng phó sự cố và đã bị bỏ lại tự hỏi, tôi nên có gì xong? Ở trên mặt trận đó, hy vọng của tôi là cuối cùng chúng ta có thể tránh xa quan niệm sai lầm việc xóa ổ cứng và cài đặt lại hệ điều hành khỏi phương tiện sạch là một giải quyết chấp nhận được cho một sự cố. Ngay cả việc cập nhật các bản vá trên hệ thống cũng không vấn đề cấu hình địa chỉ, và trong nhiều trường hợp, sẽ dẫn đến tái nhiễm hoặc hệ thống thỏa hiệp tất cả một lần nữa.

Cuốn sách này dành cho bất cứ ai quan tâm đến việc thực hiện phản ứng sự cố và khoa học pháp y phân tích hệ thống Windows Điều tra viên của công ty hoặc chính phủ, sinh viên hoặc người hướng dẫn của bất kỳ chương trình giảng dạy đang phát triển trong những năm gần đây, thực thi pháp luật cán bộ, hoặc tư vấn doanh nghiệp (như bản thân tôi). Hy vọng của tôi là cuốn sách này cũng sẽ phục vụ Preface xvii như một tài liệu tham khảo hữu ích cho những người đang phát triển hoặc tham dự các chương trình pháp y máy tính tại cao đẳng và đại học. Trong suốt cuốn sách này, các điều khoản viên điều tra, người trả lời đầu tiên, người kiểm tra và quản trị viên là sử dụng thay thế cho nhau. Điều này là do thực tế là trong nhiều trường hợp, cùng một người có thể đội tất cả những chiếc mũ này Trong các trường hợp khác, điều tra viên có thể vào công ty cơ sở hạ tầng và làm việc rất chặt chẽ với quản trị viên, thậm chí đến mức có được một tài khoản cấp Quản trị viên trong miền để thực hiện thu thập dữ liệu. Trong một số trường hợp, quản trị viên có thể hộ tống điều tra viên hoặc trả lời trước cho người bị xâm phạm hệ thống và tài khoản người dùng có thể có đặc quyền Quản trị viên trên hệ thống đó. Xin hãy ủng hộ bị nhầm lẫn bởi việc sử dụng các thuật ngữ, vì chúng đồng nghĩa trong hầu hết các trường hợp.

Đọc qua cuốn sách này, bạn có thể nhận thấy một vài điều. Đầu tiên, có một nặng phụ thuộc vào Perl như một ngôn ngữ kịch bản. Không có gì kỳ diệu về sự lựa chọn này. chỉ đơn giản là một ngôn ngữ kịch bản rất linh hoạt, mạnh mẽ mà tôi muốn sử dụng vì tôi có thể tạo ra thay đổi mã và chạy nó ngay lập tức mà không phải biên dịch lại chương trình. Nói về việc biên dịch, tôi nên đề cập rằng nếu bạn không quen với Perl và chưa bao giờ sử dụng nó, bạn không có gì phải lo lắng. Chỉ với một vài ngoại lệ, tập lệnh Perl được trình bày trong cuốn sách và được cung cấp trên DVD đi kèm đã được biên soạn thành tập sách thực thi Windows độc lập bằng Perl2Exe. Điều này sẽ cho phép bạn chạy các tập lệnh Perl mà không phải cài đặt Perl (phiên bản của Perl được sử dụng trong suốt cuốn sách này là miễn phí có sẵn từ ActiveState.com) hoặc bất cứ điều gì khác. Đơn giản chỉ cần trích xuất các tập tin cần thiết từ vị trí hoặc lưu trữ trên DVD và chạy chúng. Một tính năng hữu ích khác của Perl là với một số lưu ý, các tập lệnh Perl có thể được viết để độc lập với nền tảng. Nhiều tập lệnh Perl bao gồm trong DVD thực hiện trích xuất dữ liệu (và ở một mức độ nào đó, phân tích) từ nhị phân và nếu có thể, tôi đã cố gắng làm cho chúng độc lập với nền tảng nhất có thể. Vì điều này có nghĩa là mặc dù tập lệnh Perl (và tập tin thực thi Windows đi kèm) sẽ chạy trên nền tảng Windows, tập lệnh Perl có thể chạy trên Linux hoặc thậm chí Mac OS X. Nhiều tập lệnh Perl trên DVD (mặc dù phải thừa nhận là không phải tất cả) đã được thử nghiệm và chạy thành công trong môi trường Perl trên Linux. Điều này có nghĩa là người kiểm tra không bị giới hạn trong bất kỳ nền tảng phân tích cụ thể. Một số kịch bản sẽ yêu cầu cài đặt các mô-đun bổ sung, có thể được thực hiện thông qua Trình quản lý gói Perl (PPM) ứng dụng là một phần của bản phân phối ActiveState của Perl, có sẵn cho Windows, Linux, Mac OS X và một số nền tảng khác. Một khía cạnh rất hữu ích khác của việc sử dụng Perl là để đáp ứng nhu cầu tự động hóa. Nhiều lần, tôi thấy mình làm những việc tương tự (trích xuất dữ liệu, dịch dữ liệu nhị phân thành thứ gì đó có thể đọc được, v.v.) qua và một lần nữa, và giống như hầu hết mọi người, tôi đã bị ràng buộc để phạm sai lầm tại một số điểm. Tuy nhiên, nếu tôi có thể nhận một nhiệm vụ và tự động hóa nó trong Perl, tôi có thể viết mã một lần và không phải lo lắng với việc mắc lỗi lần thứ hai, hai mươi hoặc hai trăm lần tôi thực hiện như vậy bài tập. Nó dễ dàng sửa một quy trình nếu bạn thực sự có một quy trình. Tôi thấy rất khó sửa những gì tôi đã làm nếu tôi không biết tôi đã làm gì!

Thứ hai, bạn sẽ nhận thấy rằng ứng dụng phân tích pháp y được sử dụng trong suốt cuốn sách này là phiên bản ứng phó sự cố ProDiscover, từ Con đường công nghệ. Cảm ơn Chris Sự hào phóng của Brown, tôi đã làm việc với ProDiscover kể từ Phiên bản 3 (Phiên bản 5 đã có sẵn tại thời điểm cuốn sách đang được viết) và đã tìm thấy giao diện cực kỳ trực quan và dễ dàng để điều hướng. Khi nói đến việc kiểm tra hình ảnh thu được từ Windows hệ thống, ProDiscover là một công cụ tuyệt vời để sử dụng (mặc dù không phải là duy nhất) và nó có nhiều tính năng hữu ích và mạnh mẽ. Chris và Alex Augustin đã rất nhanh nhạy câu hỏi và cập nhật, và Ted Augustin (cả ba người trong số họ đang theo Con đường công nghệ) là một nguồn tài nguyên tuyệt vời khi tôi đã gặp anh ấy tại các hội nghị và có cơ hội nói chuyện với anh ấy. Bản thân ProDiscover không chỉ là một nền tảng phân tích tuyệt vời mà còn Phiên bản ứng phó sự cố đã có những bước tiến lớn trong lĩnh vực phản hồi trực tiếp, cung cấp một phương tiện dễ dàng và hiệu quả để thu thập dữ liệu dễ bay hơi. Ngoài ra, theo tôi, Chris đã thực hiện quyết định tuyệt vời trong việc chọn Perl làm ngôn ngữ kịch bản cho ProDiscover, cho phép điều tra viên để thực hiện các chức năng (ví dụ: tìm kiếm, trích xuất dữ liệu, mô-đun phân tích dữ liệu, v.v.) trong hình ảnh qua Perl ăn ProScripts. Tập DVD đi kèm chứa một số các bản sao mà tôi đã viết và sử dụng khá thường xuyên trong các kỳ thi (xin lưu ý rằng mặc dù các ProScripts là các tập lệnh Perl, nhưng chúng không được biên dịch ra bản dịch với Perl2Exe, như là ProScripts phải là tập lệnh được sử dụng với ProDiscover). Một tiện ích hữu ích và mạnh mẽ khác được đề cập ở một số địa điểm trong cuốn sách là phản hồi F. Năm 2008, Matthew Shannon, thông qua những nỗ lực của chính mình, đã mở ra một kỷ nguyên ứng phó sự cố và thu thập dữ liệu từ các hệ thống sống. Phản hồi có thể là được sử dụng trong ba chế độ, mạnh nhất trong số đó là Phiên bản doanh nghiệp (EE). Phản hồi EE cung cấp một quản trị viên hoặc nhà tư vấn duy nhất có khả năng tiếp cận dữ liệu trung tâm, trên toàn thành phố hoặc thậm chí giữa các lục địa để truy cập hệ thống ở chế độ chỉ đọc. Matt cũng đã cung cấp bảng điều khiển quản lý mạnh mẽ giúp triển khai F-Feedback EE dễ dàng hơn hơn là viết đoạn này. Sau khi được triển khai, F-Feedback EE cung cấp cho bạn chỉ đọc (hoạt động ghi được đệm và loại bỏ) truy cập không chỉ vào (các) ổ đĩa cứng trên hệ thống từ xa mà còn vào bộ nhớ vật lý (hoặc RAM), trong một công cụ hoàn toàn không biết cách thức. Điều này có nghĩa là bạn có thể sử dụng bất kỳ công cụ nào bạn muốn truy cập tài nguyên ngay bây giờ có sẵn để có được hình ảnh của ổ cứng, truy cập bộ nhớ vật lý, v.v. Bạn không hạn chế sử dụng chỉ một ứng dụng thương mại để làm, tốt, bất cứ điều gì .

**Chapter 1: Live Response: Data Collection**

Chương này đề cập đến các vấn đề cơ bản của việc thu thập dữ liệu dễ mất từ các hệ thống trực tiếp. Bởi vì một số yếu tố (sự gia tăng độ tinh vi của tội phạm mạng, tăng dung lượng lưu trữ, v.v.), phản hồi trực tiếp đã thu hút được rất nhiều sự quan tâm và những người phản hồi đang nhận ra sự cần thiết của phản ứng trực tiếp nhiều hơn và nhiều hơn mỗi ngày. Sự gia tăng lợi ích này đã không bị hạn chế các chuyên gia tư vấn như tôi, hoặc là người thực thi pháp luật của Haiti đang bắt đầu thấy cần phải thu thập thông tin dễ bay hơi từ các hệ thống trực tiếp để hỗ trợ điều tra. Chương này liệt kê các công cụ và phương pháp bạn có thể sử dụng để thu thập thông tin dễ mất và trình bày nhiều nhất hóa thân gần đây của Dự án máy chủ khoa học pháp y .

# **Giới Thiệu**

Các nhà điều tra ngày nay đang ngày càng phải đối mặt với các tình huống trong đó truyền thống, được chấp nhận rộng rãi phương pháp khoa học pháp y máy tính rút phích cắm điện cho máy tính và sau đó có được một hình ảnh dòng bit của ổ cứng hệ thống thông qua trình chặn ghi, đơn giản, không phải là một lựa chọn khả thi. Chẳng hạn, việc các nhà điều tra bắt gặp các máy chủ đang trở nên phổ biến hơn quan trọng đối với hoạt động kinh doanh và không thể ngừng hoạt động. Điều tra viên và ứng phó sự cố cũng đang thấy các trường hợp trong đó các câu hỏi họ có (hoặc được hỏi) không thể được trả lời sử dụng nội dung của một ổ cứng hình ảnh một mình. Ví dụ, tôi đã nói chuyện với các nhân viên thực thi pháp luật về cách tốt nhất để xử lý các tình huống liên quan đến trẻ em mất tích thu hút từ nhà hoặc trường học của họ thông qua tin nhắn tức thời (IM), đặc biệt khi phải đối mặt với thực tế là một số ứng dụng IM không ghi nhật ký trò chuyện vào đĩa, cả hoặc trong cấu hình mặc định.Những câu hỏi như thế này không giới hạn trong thực thi pháp luật. Trong nhiều trường hợp, tốt nhất nguồn thông tin hoặc bằng chứng có sẵn trong bộ nhớ máy tính (kết nối mạng, nội dung của cửa sổ máy khách IM, bộ nhớ được sử dụng bởi quy trình máy khách IM, khóa mã hóa và mật khẩu, v.v.). Trong các trường hợp khác, các nhà điều tra được hỏi liệu một Trojan hay một số khác hình thức phần mềm độc hại đã hoạt động trên hệ thống và liệu thông tin nhạy cảm có bị sao chép không hệ thống. Về cơ bản những người trả lời và điều tra đầu tiên đang được hỏi những câu hỏi liên quan đến hoạt động nào đã xảy ra trên hệ thống khi nó đang hoạt động và những câu hỏi này không thể đã trả lời khi làm theo cách tiếp cận truyền thống, thuần túy của tinh hoa đối với pháp y kỹ thuật số. Thành viên của nhân viên công nghệ thông tin (CNTT) đang tìm kiếm lưu lượng bất thường hoặc gặp rắc rối trong tường lửa của họ và nhật ký hệ thống phát hiện xâm nhập (IDS) và đang tắt các hệ thống mà lưu lượng truy cập là bắt nguồn trước khi xác định quá trình nào chịu trách nhiệm cho lưu lượng. Tình huống chẳng hạn như những điều này đòi hỏi người điều tra thực hiện phản hồi trực tiếp thu thập dữ liệu từ một hệ thống trong khi nó vẫn đang chạy.Điều này tự nó đặt ra một số vấn đề, mà chúng tôi sẽ giải quyết trong suốt chương này.

Có lẽ quan trọng hơn là yêu cầu thực hiện một số loại phản ứng trực tiếp là không còn một cái gì đó tổ chức quyết định làm. Thay vào đó, trong một số cách phản ứng trực tiếp đang được được ủy quyền bởi luật pháp cũng như các cơ quan quản lý (Công nghiệp Thẻ thanh toán Visa, hoặc PCI ). Khi một sự thỏa hiệp xảy ra trên một hệ thống, các cơ quan quản lý này yêu cầu ba câu hỏi cơ bản :

* Hệ thống đã bị xâm phạm?
* Hệ thống bị xâm nhập có chứa dữ liệu nhạy cảm trên mạng không? (Xem phần thích hợp luật pháp hoặc hướng dẫn quy định đối với định nghĩa về dữ liệu nhạy cảm trên đường sắt.)
* Nếu câu trả lời cho cả hai câu hỏi trước đó là thì có, đó là sự thỏa hiệp của hệ thống dẫn đến việc tiếp xúc với dữ liệu nhạy cảm đó?

Tuy nhiên, nhiều tổ chức chỉ đơn giản là không chuẩn bị cho một sự cố, và như vậy, hoạt động của người trả lời của họ có thể khiến các tổ chức đó gặp rủi ro lớn hơn vụ việc bản thân nó, phần lớn là do thực tế là tâm lý đóng cửa của nhiều người .Các tổ chức CNTT không cho phép thu thập dữ liệu cần thiết để trả lời câu hỏi không thể tránh khỏi. Những câu hỏi này luôn luôn phát sinh khi bộ phận pháp lý hoặc tuân thủ của tổ chức nghe về vụ việc, và sau đó phát hiện ra rằng những câu hỏi đó không thể trả lời.

# **Live Response**

Các nhà điều tra ngày nay phải đối mặt với một số vấn đề trong đó rút phích cắm một hệ thống (hoặc một số hệ thống) và có được một hình ảnh của (các) ổ đĩa cứng có thể không phải là một lựa chọn. Khi thương mại điện tử tiếp tục phát triển, thời gian ngừng hoạt động của hệ thống được tính bằng hàng trăm hoặc hàng ngàn đô la mỗi phút, dựa trên các giao dịch bị mất. Do đó, lấy một hệ thống xuống để có được một ổ cứng hình ảnh có ảnh hưởng nghiêm trọng đến dòng dưới cùng. Ngoài ra, một số công ty có các thỏa thuận cấp độ dịch vụ (SLA) bảo đảm cho năm năm trước, thời gian hoạt động, đó là công ty đảm bảo cho công ty khách hàng rằng các hệ thống sẽ hoạt động và hoạt động 99,999 phần trăm thời gian (bên ngoài cửa sổ bảo trì). Lấy một hệ thống với một ổ cứng ngoại tuyến để thực hiện hình ảnh có thể mất vài giờ, tùy thuộc vào cấu hình của hệ thống.

Vào tháng 4 năm 2006, Seagate đã giới thiệu ổ cứng 750 GB đầu tiên. Hôm nay, tôi thường xuyên thấy ổ cứng ngoài có sẵn với kích thước lớn hơn 1,5 terabyte (TB) và tôi thấy multiterabyte hệ thống lưu trữ trên mạng khách hàng. Hãy tưởng tượng một hệ thống RAID 5 với tám 1TB cứng ổ đĩa, đứng đầu tại 8 TB lưu trữ. Bạn sẽ mất bao lâu để hình ảnh những người khó khăn ổ đĩa? Với một số cấu hình nhất định, có thể mất bốn giờ hoặc hơn để điều tra viên có thể có được và xác minh một ổ cứng 80 GB. Và bạn sẽ cần phải hình ảnh toàn bộ hệ thống nếu bạn chỉ quan tâm đến các hoạt động của một quy trình duy nhất chứ không phải trong hàng ngàn tệp cư trú trên hệ thống?

Trong một số trường hợp, chúng tôi có thể muốn thu thập một số thông tin về hệ thống trực tiếp trước đó tắt nó đi, thu được hình ảnh luồng của ổ cứng hoặc ổ đĩa và thực hiện điều tra pháp y máy tính truyền thống hơn. Thông tin mà bạn quan tâm nhất có tính chất dễ bay hơi, nghĩa là nó không còn tồn tại khi nguồn điện bị loại bỏ khỏi hệ thống. Thông tin dễ bay hơi này thường tồn tại trong bộ nhớ vật lý hoặc RAM và bao gồm về những thứ như thông tin liên quan đến các quy trình, kết nối mạng, nội dung của Clipboard, v.v. Thông tin này mô tả trạng thái của hệ thống tại thời điểm bạn đang đứng trước nó hoặc ngồi vào bàn điều khiển hoặc truy cập nó từ xa. Là một điều tra viên, bạn có thể phải đối mặt với một tình huống trong đó bạn phải nhanh chóng nắm bắt và phân tích (được bảo hiểm trong chương tiếp theo) dữ liệu để xác định tính chất và phạm vi của vụ việc. Khi sức mạnh là loại bỏ khỏi hệ thống để chuẩn bị chụp ảnh ổ cứng theo cách truyền thống, thông tin này đơn giản biến mất. Tuy nhiên, bạn cũng cần lưu ý rằng bất kỳ hành động nào bạn thực hiện (ví dụ: chạy quét chống vi-rút, tìm kiếm tệp hoặc dữ liệu thẻ tín dụng, cấu hình lại hệ thống, v.v.) trên một hệ thống trực tiếp sẽ để lại các tạo tác của riêng họ, và có thể sẽ ghi đè dữ liệu hữu ích hoặc thích hợp. Do đó, thu thập và lưu giữ dữ liệu dễ bay hơi này nên là mối quan tâm đầu tiên của bạn .Chúng tôi có các tùy chọn có sẵn cho chúng tôi các công cụ và kỹ thuật mà chúng tôi có thể sử dụng để thu thập này thông tin dễ bay hơi từ một hệ thống trực tiếp, cho chúng ta một bức tranh tổng thể tốt hơn về tình trạng hệ thống cũng như cung cấp cho chúng tôi phạm vi thông tin lớn hơn. Đây là những gì mà sống phản hồi đòi hỏi phải có: truy cập một hệ thống đang hoạt động, đang chạy và thu thập biến động và trong một số trường hợp, không biến đổi thông tin.

Có một thuật ngữ khác bạn có thể nghe thấy thường bị nhầm lẫn với phản hồi trực tiếp: mua lại trực tiếp. Phản hồi trực tiếp thỏa thuận với việc thu thập thông tin dễ bay hơi từ một hệ thống; trực tiếp mua lại mô tả việc mua ổ cứng trong khi hệ thống vẫn đang chạy và tạo một hình ảnh của ổ cứng đó. Trong chương này, chúng tôi sẽ bắt đầu bằng cách thảo luận về các công cụ, kỹ thuật và phương pháp để thực hiện phản ứng trực tiếp. Khi chúng ta nói về việc thực hiện phản hồi trực tiếp, chúng ta cần hiểu thông tin nào chúng ta muốn thu thập từ hệ thống và làm thế nào chúng ta nên đi thu thập nó .Trong chương này, chúng ta sẽ đi qua những gì và làm thế nào thu thập thông tin dễ bay hơi từ một hệ thống; trong chương tiếp theo, chúng ta sẽ thảo luận làm thế nào để phân tích dữ liệu này . Sau đó, chúng tôi sẽ kiểm tra một số giải pháp để thực hiện mua lại trực tiếp. Phân tích hình ảnh thu thập được trong quá trình thu thập trực tiếp sẽ được đề cập trong các chương còn lại của cuốn sách này. Trước khi chúng ta bắt đầu thảo luận về các công cụ và hoạt động phản hồi trực tiếp, chúng ta cần giải quyết hai chủ đề quan trọng: Nguyên tắc trao đổi Locard từ từ và thứ tự biến động. Những khái niệm này là nền tảng của chương này và phản hồi trực tiếp nói chung, và chúng tôi sẽ thảo luận về chúng chi tiết.

**Locard’s Exchange Principle**

Khi thực hiện phản hồi trực tiếp, các nhà điều tra và người trả lời đầu tiên cần phải giữ một điều rất quan trọng nguyên tắc trong tâm trí. Khi chúng ta tương tác với một hệ thống trực tiếp, dù là người dùng hay là người điều tra, những thay đổi sẽ xảy ra trên hệ thống đó. Trên một hệ thống trực tiếp, những thay đổi sẽ xảy ra đơn giản là do thời gian trôi qua, khi các quá trình hoạt động, khi dữ liệu được lưu và xóa, khi các kết nối mạng hết thời gian hoặc được tạo ra. Một số thay đổi xảy ra khi hệ thống chỉ ngồi đó và chạy. Những thay đổi cũng xảy ra khi điều tra viên chạy các chương trình trên hệ thống để thu thập thông tin, dễ bay hơi hoặc khác. Chạy một chương trình khiến thông tin được tải vào bộ nhớ vật lý và khi làm như vậy, bộ nhớ vật lý được sử dụng bởi các quy trình đang chạy khác có thể được ghi vào tệp trang. Khi điều tra viên thu thập thông tin và gửi nó đi hệ thống, kết nối mạng mới sẽ được tạo ra.Tất cả những thay đổi này có thể được gọi chung giải thích bởi Nguyên tắc trao đổi Locard. Những thay đổi xảy ra với một hệ thống như chính hệ thống rõ ràng là ngồi không được gọi là động lực bằng chứng của người Hồi giáo và tương tự như xóa đi bằng chứng tiềm năng tại một hiện trường vụ án.

Đầu thế kỷ 20, Tiến sĩ Edmond Locard, làm việc trong lĩnh vực khoa học pháp y và Tái thiết hiện trường vụ án được gọi là Nguyên tắc Trao đổi Locard. Nguyên tắc này về bản chất, khi hai vật thể tiếp xúc với nhau, vật chất được trao đổi hoặc chuyển giao giữa họ. Nếu bạn xem chương trình tội phạm CSI nổi tiếng trên TV, bạn sẽ luôn nghe thấy một trong những các điều tra hiện trường vụ án đề cập đến có thể chuyển. Điều này thường xảy ra sau một cảnh trong đó một chiếc xe đâm vào một cái gì đó hoặc khi một điều tra viên kiểm tra một cơ thể và xác định vị trí vật liệu dường như không có chỗ Nguyên tắc tương tự này được áp dụng trong lĩnh vực kỹ thuật số. Ví dụ: khi hai máy tính giao tiếp qua mạng, thông tin được trao đổi giữa họ. Thông tin về một máy tính sẽ xuất hiện trong bộ nhớ tiến trình và / hoặc các tệp nhật ký khác (xem phần Loc Locard và thanh bên Netcat tinh cho một minh chứng thực sự tuyệt vời về khái niệm này). Khi ngoại vi như vậy như một thiết bị lưu trữ di động (ổ ngón tay cái, iPod hoặc tương tự) được gắn vào Windows hệ thống máy tính, thông tin về thiết bị sẽ vẫn còn trên máy tính. Khi nào một điều tra viên tương tác với một hệ thống trực tiếp, những thay đổi sẽ xảy ra với hệ thống đó như các chương trình được thực thi và dữ liệu được sao chép từ hệ thống. Những thay đổi này có thể là nhất thời (quá trình bộ nhớ, kết nối mạng) hoặc vĩnh viễn (log file , mục đăng ký).

**Tools & Traps…**

Locard and Netcat

Bạn có thể sử dụng các công cụ đơn giản, chẳng hạn như netcat (http://en.wikipedia.org/wiki/Netcat), để thể hiện Nguyên tắc trao đổi Locard. Nếu bạn không quen với netcat (nc.exe trên Các hệ thống Windows), đủ để nói rằng netcat là một công cụ cực kỳ linh hoạt cho phép bạn đọc và viết thông tin qua các kết nối mạng.

Trong ví dụ này, bạn sẽ cần ba công cụ: netcat (nc.exe), pmdump.exe (www. ntsecurity.nu/toolbox/pmdump/) và chuỗi.exe (<http://technet.microsoft.com/en-us/> sysiternals / bb897439.aspx) hoặc BinText (có sẵn từ [www.foundstone.com/us/](http://www.foundstone.com/us/) tài nguyên / proddesc / bintext.htm). Bạn có thể chạy ví dụ này bằng cách sử dụng một hoặc hai hệ thống, nhưng nó hoạt động tốt nhất khi hai hệ thống được sử dụng. Nếu bạn sử dụng một hệ thống, tạo hai thư mục, với một bản sao của netcat trong mỗi thư mục.

Bắt đầu bằng cách khởi chạy netcat trong chế độ nghe với dòng lệnh sau:

*C:\test>nc –L –d –p 8080 –e cmd.exe*

Dòng lệnh này bảo netcat lắng nghe trên cổng 8080, ở chế độ tách rời và khi một kết nối được thực hiện để khởi chạy dấu nhắc lệnh. Một khi bạn đã gõ dòng lệnh và nhấn Enter, mở Trình quản lý tác vụ và ghi chú quá trình định danh (PID) của quá trình bạn vừa tạo. (Ở đây tôi đang sử dụng netcat Phiên bản 1.11 NT, mà tôi đã lấy từ www.vulnwatch.org/netcat. Tại thời điểm viết bài này, Trang web dường như không có sẵn.) .Bây giờ hãy mở một dấu nhắc lệnh khác trên cùng hệ thống hoặc đi đến dấu nhắc khác của bạn hệ thống và mở dấu nhắc lệnh. Nhập dòng lệnh sau để kết nối để nghe netcat bạn vừa tạo:

C:\test2>nc <IP address> 8080

Dòng lệnh này bảo netcat mở trong chế độ máy khách và kết nối với địa chỉ Giao thức Internet (IP) trên cổng 8080, nơi người nghe của chúng tôi đang chờ. Nếu bạn chạy thử nghiệm trên một hệ thống, sử dụng 127.0.0.1 làm địa chỉ IP. Khi bạn đã kết nối, bạn sẽ thấy tiêu đề nhắc lệnh mà bạn thường thấy, hiển thị phiên bản của hệ điều hành và thông tin bản quyền. Nhập một vài lệnh tại dấu nhắc, chẳng hạn như dir hoặc bất cứ thứ gì khác, để đơn giản gửi thông tin qua kết nối.

Trên hệ thống nơi trình nghe netcat đang chạy, hãy mở một lệnh khác nhắc và sử dụng pmdump.exe (sẽ thảo luận sau trong chương này) để lấy nội dung của bộ nhớ cho quá trình người nghe:

C:\test>pmdump <PID> netcat1.log

Lệnh này sẽ có được nội dung của bộ nhớ được sử dụng bởi quá trình và sẽ đặt nó vào tập tin netcat1.log. Bạn cũng có thể kết xuất bộ nhớ tiến trình của máy khách bên kết nối, nếu bạn thích. Bây giờ bạn có bộ nhớ tiến trình được lưu trong một tập tin, bạn có thể thoát cả hai quá trình. Chạy String.exe đối với tệp bộ nhớ từ nghe hoặc mở tệp trong BinText và bạn sẽ thấy địa chỉ IP của máy khách. Đang làm điều tương tự với tệp bộ nhớ máy khách sẽ hiển thị thông tin về hệ thống nơi người nghe đang chạy, thể hiện khái niệm Locard’s Exchange Principle.

Các chương trình mà chúng tôi sử dụng để thu thập thông tin có thể có các hiệu ứng khác trên hệ thống trực tiếp. Ví dụ, một chương trình có thể cần phải đọc một số khóa Registry và các đường dẫn đến những khóa đó .Các phím sẽ được đọc vào bộ nhớ. Các hệ thống Windows XP thực hiện tìm nạp trước ứng dụng, vì vậy nếu điều tra viên chạy một chương trình mà người dùng đã chạy trên hệ thống, lần truy cập cuối cùng và thời gian sửa đổi của tệp tìm nạp trước (cũng như nội dung của chính tệp đó) cho điều đó ứng dụng sẽ được sửa đổi. Nếu chương trình mà điều tra viên chạy hasn đã được sử dụng trước đó, một tệp tìm nạp mới sẽ được tạo trong thư mục Tìm nạp trước (giả sử nội dung của thư mục Prefetch, thiên đường đã đạt đến giới hạn tệp 128 .pf của họ, nhưng nhiều hơn về sau trong cuốn sách) .

Các nhà điều tra không chỉ cần hiểu rằng những thay đổi này sẽ xảy ra mà còn phải ghi lại những thay đổi đó và có thể giải thích những tác động của chúng đối với hệ thống, đến một mức độ hợp lý. Ví dụ, là một điều tra viên, bạn sẽ có thể xác định .Những tệp .pf nào trong thư mục Prefetch XP là kết quả của những nỗ lực của bạn và đó là kết quả của hoạt động người dùng. Điều này cũng đúng với các giá trị Registry. Như với ứng dụng khả năng tìm nạp trước của Windows XP, hành động của bạn sẽ có ảnh hưởng đến hệ thống Đăng ký. Cụ thể, các mục có thể xuất hiện trong Sổ đăng ký và như vậy lần LastWrite các khóa Registry sẽ được cập nhật. Một số thay đổi này có thể không phải là kết quả trực tiếp trong số các công cụ hoặc hành động của bạn, nhưng thay vào đó được tạo bởi trình bao (tức là, Windows Explorer), do chỉ đơn giản là thực tế là hệ thống đang hoạt động và đang chạy. Bằng cách thử nghiệm và hiểu các công cụ bạn sử dụng, bạn sẽ có thể ghi lại và giải thích những gì tạo tác được tìm thấy trên một hệ thống là kết quả của những nỗ lực của bạn và đó là kết quả của hành động được thực hiện bởi người dùng hoặc kẻ tấn công

# **Thứ tự biến động (Order of Volatility)**

Chúng tôi biết rằng thông tin dễ bay hơi tồn tại trong bộ nhớ trên một hệ thống và một số loại nhất định thông tin dễ bay hơi có thể, tốt, dễ bay hơi hơn những thông tin khác. Đó là, một số thông tin về một hệ thống có thời hạn sử dụng ngắn hơn nhiều so với các thông tin khác. Ví dụ: mạng hết thời gian kết nối, đôi khi trong vòng vài phút, nếu chúng được sử dụng. Bạn có thể thấy điều này bằng cách duyệt đến một trang web cụ thể hoặc thực hiện một số kết nối mạng khác và xem kết nối qua netstat.exe. Sau đó tắt ứng dụng khách mà bạn đang sử dụng và trạng thái của kết nối mạng sẽ thay đổi theo thời gian trước khi cuối cùng nó biến mất khỏi đầu ra của netstat.exe. Thời gian hệ thống, tuy nhiên, thay đổi nhanh hơn nhiều, trong khi nội dung của Clipboard sẽ không đổi cho đến khi chúng được thay đổi hoặc cấp nguồn được gỡ bỏ khỏi hệ thống. Ngoài ra, một số quy trình, chẳng hạn như dịch vụ (được gọi là daemon trong vương quốc UNIX) chạy trong một thời gian dài, trong khi các quá trình khác có thể cực kỳ thời gian ngắn, thực hiện nhiệm vụ của họ một cách nhanh chóng trước khi biến mất khỏi bộ nhớ. Cái này sẽ chỉ ra rằng chúng ta cần thu thập thông tin nhất định trước để chúng ta có thể nắm bắt thông tin đó trước khi nó thay đổi, trong khi dữ liệu dễ bay hơi khác xảy ra liên tục hơn có thể được thu thập sau này.

Một nơi tuyệt vời để biết thông tin này là tài liệu Yêu cầu Nhận xét (RFC) 3227, Hướng dẫn thu thập chứng cứ và lưu trữ bằng chứng (www.faqs.org/rfcs/rfc3227.html).RFC này, được xuất bản vào tháng 2 năm 2002, vẫn còn tồn tại cho đến ngày nay, vì các nguyên tắc hướng dẫn cốt lõi không thay đổi khi công nghệ thay đổi. RFC chỉ định các nguyên tắc như vậy cho bằng chứng bộ sưu tập càng chụp chính xác càng tốt hình ảnh của hệ thống; ghi chép chi tiết; lưu ý sự khác biệt giữa UTC, giờ địa phương và thời gian hệ thống; và giảm thiểu các thay đổi để dữ liệu càng nhiều càng tốt. Chúng tôi sẽ ghi nhớ những nguyên tắc này trong suốt cuộc thảo luận về phản ứng trực tiếp.

Quan tâm cụ thể đến tài liệu RFC này là Phần 2.1, Thứ tự biến động, mà liệt kê một số loại thông tin dễ bay hơi theo thứ tự, từ hầu hết đến ít biến động nhất. Các mặt hàng có khả năng thay đổi hoặc hết hạn nhanh hơn do thời gian trôi qua (ví dụ: các quy trình, kết nối mạng, v.v.) nên được thu thập trước. Ngược lại, thông tin ít biến động, chẳng hạn như cấu hình vật lý của hệ thống, có thể được thu thập sau này. Sử dụng các hướng dẫn này, chúng ta có thể thấy những loại thông tin chúng ta cần thu thập từ một hệ thống, tìm thông tin đó ở đâu, công cụ nào sử dụng để truy xuất nó và thậm chí làm thế nào để lấy thông tin đó ra khỏi hệ thống, từ đó giảm thiểu tác động đến hệ thống, đồng thời thu thập thông tin chúng ta cần để thực hiện phân tích của chúng tôi.

# **What Data To Collect ( Dữ Liệu Cần Thu Thập )**

Tại thời điểm này, chúng tôi đã sẵn sàng xem xét các loại thông tin mất mà chúng tôi có thể thấy trên một hệ thống trực tiếp và tìm hiểu về các công cụ chúng ta có thể sử dụng để thu thập thông tin đó trong thời gian phản ứng trực tiếp.

Khi bạn thực hiện phản hồi trực tiếp, nó có khả năng là một trong những điều đầu tiên bạn muốn để thu thập là nội dung của bộ nhớ vật lý hoặc RAM. Khi bạn dùng Locard Exchange Principle. Nguyên tắc vào tài khoản, nó khá rõ ràng rằng bằng cách thu thập nội dung của RAM trước tiên, bạn giảm thiểu tác động của bạn lên nó.Từ thời điểm đó, bạn biết rằng các công cụ khác bạn chạy để thu thập thông tin dễ bay hơi khác sẽ được tải vào bộ nhớ (như là công cụ mà bạn sử dụng để thu thập nội dung của RAM), sửa đổi nội dung của bộ nhớ.Chúng tôi sẽ thảo luận về chủ đề thu thập và phân tích nội dung của RAM trong Chương 3. Dưới đây là danh sách các loại thông tin dễ mất cụ thể mà chúng tôi sẽ xem xét trong chương này :

System time  
■ Logged-on user(s)  
■ Open files  
■ Network information  
■ Network connections  
■ Process information  
■ Process-to-port mapping  
■ Process memory  
■ Network status  
■ Clipboard contents  
■ Service/driver information  
■ Command history  
■ Mapped drives  
■ Shares

Đối với mỗi loại thông tin dễ mất này, chúng tôi sẽ xem xét một số công cụ mà chúng tôi có thể sử dụng để lấy thông tin từ hệ thống Windows. Bạn rất có thể sẽ nhận thấy rằng trong suốt chương này có xu hướng sử dụng các công cụ giao diện dòng lệnh (CLI) trên những người có giao diện người dùng đồ họa (GUI). Bạn có thể nghĩ rằng điều này là do CLI các công cụ có dấu chân bộ nhớ nhỏ hơn, nghĩa là chúng tiêu thụ ít bộ nhớ hơn, dựa vào ít thư viện liên kết động (DLL) và ít ảnh hưởng đến hệ thống hơn. Đây là một phần là trường hợp, nhưng hãy nhớ rằng dấu chân thực tế của bất kỳ công cụ cụ thể nào có thể là chỉ xác định thông qua thử nghiệm kỹ lưỡng của công cụ đó. Đến nay, tôi không biết thử nghiệm đang được thực hiện và công khai.

Lý do chính chúng tôi tập trung vào việc sử dụng các công cụ CLI là chúng thường rất đơn giản, thực hiện một chức năng cơ bản, cụ thể và dễ dàng hơn để tự động hóa thông qua việc sử dụng tập tin lô hoặc tập lệnh. Các công cụ CLI có thể được liên kết với nhau thông qua các tệp bó hoặc ngôn ngữ script và đầu ra của chúng thường được gửi đến bàn điều khiển ( STDOUT) và có thể được chuyển hướng đến một tệp hoặc một ổ cắm. Mặt khác, các công cụ GUI chủ yếu yêu cầu bạn lưu đầu ra của chúng vào một tệp, vì hầu hết chúng đều có một mục menu Tệp với các mục save và save dưới dạng trong trình đơn thả xuống. Hầu hết các lập trình viên của các công cụ GUI đều không nhất thiết phải phát triển chúng với ứng phó sự cố hoặc pháp y trong tâm trí. Một trong những mục tiêu của chúng tôi là giảm thiểu tác động của chúng tôi các biện pháp điều tra trên một hệ thống (đặc biệt là hình ảnh theo dõi và phân tích pháp y các hoạt động), vì vậy chúng tôi muốn tránh ghi tệp vào hệ thống, ngoài việc lấy dữ liệu chúng tôi cần tắt hệ thống nhanh nhất và hiệu quả nhất có thể.

Bây giờ, điều này không có nghĩa là các công cụ GUI hoàn toàn không thể được sử dụng cho các hoạt động phản hồi trực tiếp. Nếu có một công cụ GUI mà bạn thấy hoàn toàn hoàn hảo cho những gì bạn cần, thì bằng mọi cách, sử dụng nó. Nhưng hãy cân nhắc trước thời hạn bạn sẽ lấy dữ liệu đó ra khỏi hệ thống như thế nào.

Bất kể công cụ nào bạn quyết định sử dụng, hãy luôn chắc chắn kiểm tra thỏa thuận cấp phép trước khi sử dụng chúng. Một số công cụ có thể được sử dụng như bạn muốn, nhưng những công cụ khác yêu cầu một khoản phí để sử dụng trong một môi trường doanh nghiệp. Đọc và lưu ý các thỏa thuận này trước có thể giúp bạn tránh những cơn đau đầu

## **System Time**

Một trong những thông tin đầu tiên bạn muốn thu thập khi bạn điều tra sự cố là thời gian hệ thống. Điều này sẽ cung cấp rất nhiều bối cảnh cho các thông tin được thu thập sau này trong điều tra và sẽ hỗ trợ phát triển dòng thời gian chính xác của các sự kiện đã xảy ra trên hệ thống.



**Figure 1: Displaying the System Date and Time on Windows 10**

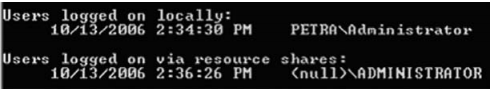
Không chỉ thời gian hệ thống hiện tại quan trọng đối với người điều tra, mà số lượng thời gian mà hệ thống đã chạy, hoặc thời gian hoạt động, cũng có thể cung cấp rất nhiều bối cảnh để điều tra. Ví dụ: lưu ý lượng thời gian hệ thống đã chạy so với lượng thời gian một quy trình đang chạy có thể cung cấp cho bạn một ý tưởng về thời điểm một nỗ lực khai thác hoặc thỏa hiệp có thể đã thành công (nhiều hơn về việc truy xuất thông tin về các quá trình sau trong chương này)

Ngoài ra, điều tra viên cũng nên ghi lại thời gian thực, hoặc thời gian trên tường, khi ghi thời gian hệ thống. Có cả hai cho phép điều tra viên sau đó xác định xem hệ thống đồng hồ không chính xác. Thông tin về đồng hồ nghiêng xiên cung cấp một sự hiểu biết tốt hơn của thời gian thực tế mà tại đó các sự kiện được ghi lại trong tệp nhật ký xảy ra. Thông tin này có thể là vô giá khi bạn cố gắng kết hợp tem thời gian từ nhiều hơn một nguồn. Một thông tin khác liên quan đến thời gian có thể quan trọng là múi giờ cài đặt cho máy tính. Các hệ thống Windows sử dụng hệ thống tệp NTFS lưu trữ thời gian tệp trong .Thời gian phối hợp toàn cầu, hay viết tắt là UTC, tương tự như Greenwich Mean .Định dạng thời gian (GMT). Các hệ thống sử dụng hệ thống tệp FAT lưu trữ thời gian tệp dựa trên cục bộ thời gian hệ thống. Điều này quan trọng hơn để ghi nhớ trong quá trình phân tích hậu sản (đã thảo luận sau này trong cuốn sách này), nhưng nó có thể trở nên cực kỳ quan trọng khi bạn biểu diễn trực tiếp phản ứng từ xa, đặc biệt là qua các múi giờ.

## **PsLoggedOn**

Có lẽ công cụ nổi tiếng nhất để xác định người dùng đăng nhập là psloggedon.exe (http: // technet.microsoft.com/en-us/sysiternals/bb897545.aspx). Công cụ này cho thấy điều tra viên tên của người dùng đã đăng nhập cục bộ (trên bàn phím) cũng như người dùng đã đăng nhập từ xa, chẳng hạn như thông qua một chia sẻ bản đồ.

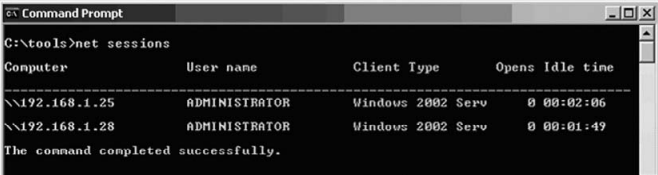
Như trong Hình 1.2, psloggedon.exe cho thấy người dùng đăng nhập vào hệ thống từ xa. Để thiết lập bản trình diễn này, tôi đã đăng nhập vào hệ thống Windows 2000 (Petra) từ hệ thống Windows XP và sau đó chạy lệnh trên hệ thống Windows 2000.



**Figure 2 :Output of psloggedon.exe on Windows 2000**

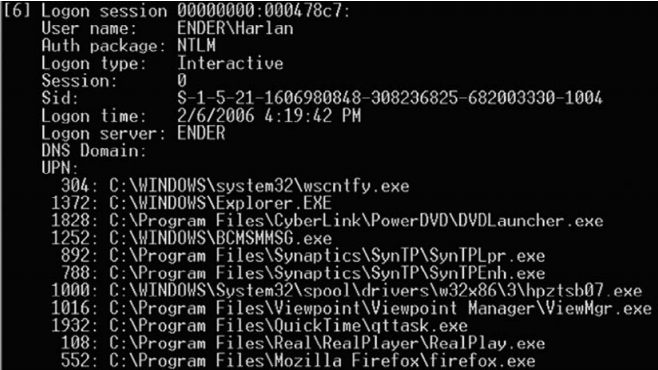
## **Net Sessions**

Lệnh net session có nguồn gốc từ các hệ thống Windows (thông qua tệp thực thi net.exe), và bạn có thể sử dụng nó để xem không chỉ tên người dùng được sử dụng để truy cập hệ thống thông qua đăng nhập từ xa phiên , nhưng cũng là địa chỉ IP và loại máy khách mà nó đang truy cập hệ thống.

**Figure 3:Output of the net sessions Command on Windows 2003**

## **LogonSesions**

Logonsimes.exe (http://technet.microsoft.com/en-us/sysiternals/bb896769.aspx) là một CLI công cụ có sẵn từ Microsoft liệt kê tất cả các phiên đăng nhập hoạt động trên một hệ thống. Hình 1.4 minh họa một phần đầu ra của logonsimes.exe trên hệ thống Windows XP (hệ thống tên là Ender).



**Figure 4 : Output of logonsessions.exe on Windows XP**

Logonsimes.exe cung cấp nhiều thông tin hơn các công cụ khác, như được minh họa trong đoạn trích đầu ra được hiển thị trong Hình 1.4. Ví dụ, nó liệt kê xác thực gói được sử dụng (điều này có thể quan trọng đối với cuộc điều tra của bạn rằng xác thực Kerberos gói đã được sử dụng thay cho LAN Manager), loại đăng nhập, quy trình hoạt động, v.v.

Một tiện ích hữu ích khác mà bạn sẽ thấy tiện dụng là netusers.exe, một tiện ích miễn phí từ Somarsoft.com. Sử dụng các khóa chuyển đổi và tiêu điểm của mạng với netusers.exe, bạn có thể truy xuất một báo cáo ngắn gọn về lần cuối cùng tất cả người dùng địa phương đăng nhập vào hệ thống. Thời gian đăng nhập cuối cùng được duy trì trong Đăng ký; chúng tôi sẽ thảo luận chi tiết cụ thể về thông tin đăng ký này trong Chương 4. Netusers.exe cho phép bạn lấy thông tin này từ một hệ thống trực tiếp. Tuy nhiên, hãy nhớ rằng các công cụ này sẽ không hiển thị cho bạn biết ai đó đã đăng nhập chưa trên thông qua một cửa hậu. Backreen và Trojans như SubSeven khét tiếng cho phép người dùng Đăng nhập vào Nhật ký vào Trojan thông qua kết nối Giao thức điều khiển truyền dẫn (TCP) thô, bỏ qua các cơ chế xác thực Windows. Như vậy, các kết nối này sẽ không hiển thị khi bạn sử dụng các công cụ như psloggedon.exe. Có đầu ra của các công cụ này, tuy nhiên, có thể là công cụ cho thấy rằng người dùng mà bạn khám phá sau này không xuất hiện trong danh sách. Nó cũng có thể được sử dụng để thể hiện chức năng ẩn, ngay cả khi cơ chế cho điều đó chức năng không bao giờ được tìm thấy.

## **Open Files**

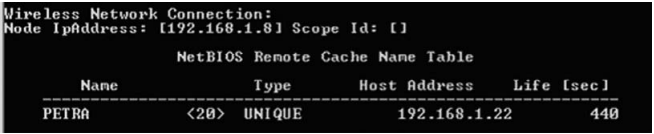
Nếu đầu ra của psloggedon.exe cho bạn thấy rằng người dùng đã đăng nhập vào hệ thống từ xa, bạn cũng sẽ muốn xem những tập tin họ đã mở, nếu có. Nhiều khi một người truy cập một hệ thống từ xa, anh ta có thể đang tìm kiếm thứ gì đó cụ thể và mở tệp. Một người dùng trong một môi trường công ty có thể có sẵn một phần và cho phép người dùng khác xem hình ảnh, tải bài hát, vân vân. Các hệ thống Windows được bảo vệ kém, chẳng hạn như các hệ thống Windows 2000 được kết nối với Internet không có mật khẩu Quản trị viên (và không có tường lửa), có thể Đã đến thăm và các tập tin tìm kiếm, truy cập và sao chép. Lệnh tập tin mạng, psfile.exe (http://technet.microsoft.com/en-us/sysiternals/bb896649.aspx) và openfiles.exe (có nguồn gốc từ các công cụ Windows XP Pro và Windows 2003) đều sẽ hiển thị các tệp được mở trên hệ thống thông qua một kết nối từ xa.

# **Network Information (Cached NetBIOS Name Table)**

Đôi khi khi những kẻ xâm nhập có quyền truy cập từ xa vào một hệ thống, họ muốn biết những gì khác các hệ thống có sẵn trên mạng và có thể được nhìn thấy trên mạng (theo nghĩa trung tâm của mạng) hệ thống họ đã thỏa hiệp. Tôi đã thấy điều này xảy ra thường xuyên trong các cuộc điều tra, trong một loạt các cách; đôi khi các tệp bó đã được tạo trên hệ thống và được thực thi và các lần khác kẻ xâm nhập đã đưa ra các lệnh xem mạng thông qua SQL (bằng cách sử dụng trình duyệt để gửi lệnh cho hệ thống thông qua các máy chủ Web và cơ sở dữ liệu). Khi kết nối được thực hiện cho các hệ thống khác sử dụng giao tiếp NetBIOS (giống như được sử dụng để đăng nhập, kết nối với cổ phiếu và tương tự), các hệ thống sẽ duy trì một danh sách các hệ thống khác mà họ bạn đã thấy. Bằng cách xem nội dung của bảng tên được lưu trong bộ nhớ cache, bạn có thể xác định được các hệ thống khác đã bị ảnh hưởng.

Hãy nhìn vào một ví dụ. Mạng nhà của tôi, mạng của tôi bao gồm một máy tính xách tay và một số Vmware phiên xuất hiện dưới dạng hệ thống độc lập trên mạng ảo. Để chứng minh bộ nhớ đệm của tên NetBIOS, tôi đã bắt đầu phiên Windows 2000 VMware của mình và đăng nhập để xem .Địa chỉ IP được gán thông qua Giao thức cấu hình máy chủ động (DHCP) sau đó tôi đã quay lại hệ điều hành máy chủ (Windows XP Pro SP2) và trong dấu nhắc lệnh

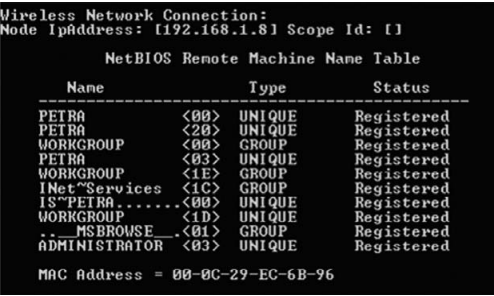
Tôi đã gõ nbtstatTHERA 192.168.1.22 để xem bảng tên hệ thống từ xa của Google. Sau đó tôi gõ nbtstatTHERc để xem các tên NetBIOS được lưu trong bộ nhớ cache trên hệ điều hành máy chủ. Hình 1.5 cho thấy :



**Figure 5 :NetBIOS Name Table Cache**

Tại thời điểm này, bạn có thể đang nghĩ về vấn đề gì vậy? Tại sao điều này lại quan trọng? Vâng, nếu tôi là một kẻ tấn công và đã giành được quyền truy cập vào một hệ thống, tôi có thể quan tâm đến việc truy cập vào các hệ thống khác là tốt. Để làm như vậy, tôi cần xem hệ thống nào trên mạng và họ có những lỗ hổng nào. Về cơ bản, tôi đã tìm kiếm các mục tiêu dễ dàng. Bây giờ, nếu tôi đã bắt đầu quét các lỗ hổng, tôi có thể cảnh báo ai đó về những gì đang xảy ra. Ngoài ra, để quét đối với các lỗ hổng, tôi sẽ cần sao chép các công cụ của mình vào hệ thống mà tôi đã bị xâm phạm, và điều đó có thể cảnh báo ai đó về các hoạt động của tôi. Tuy nhiên, tôi có thể sử dụng nbtstat.exe để định vị hệ thống có khả năng dễ bị tổn thương. Ví dụ, Hình 1.6 cho thấy đầu ra của lệnh

Tôi đã chạy để điền vào bộ đệm tên NetBIOS.



**Figure 6 :Output of nbtstat –A 192.168.1.22**

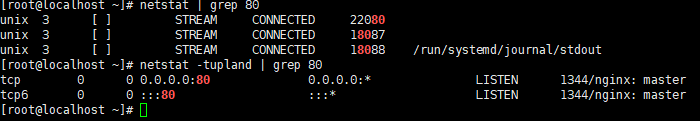
Từ đầu ra của lệnh nbtstat được hiển thị trong Hình 1.6, chúng ta có thể thấy rằng quản trị viên đã đăng nhập và chúng ta có thể thấy rằng hệ thống đang chạy Thông tin Internet Máy chủ (IIS) Máy chủ web.

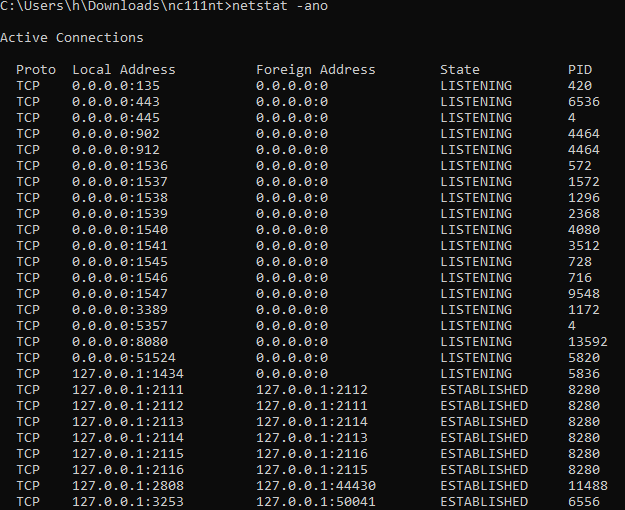
# **Network Connections**

Càng sớm càng tốt sau khi một sự cố được báo cáo, điều tra viên nên thu thập thông tin liên quan đến các kết nối mạng đến và từ hệ thống bị ảnh hưởng. Thông tin này có thể hết hạn theo thời gian và nếu quá nhiều thời gian trôi qua, nó sẽ bị mất. Một điều tra viên có thể tiếp cận một hệ thống và, sau khi xem xét ban đầu, hãy xác định rằng kẻ tấn công vẫn đăng nhập và truy cập vào hệ thống. Hoặc cô ấy có thể thấy rằng một con sâu hoặc bot Internet Relay Chat (IRC) (độc hại phần mềm, sau khi được cài đặt trên hệ thống, tạo kết nối ra tới máy chủ IRC để chờ lệnh) đang liên lạc từ hệ thống, tìm kiếm các hệ thống khác để lây nhiễm, cập nhật chính nó hoặc đăng nhập vào một máy chủ chỉ huy và kiểm soát. Thông tin này có thể cung cấp manh mối quan trọng và thêm bối cảnh vào thông tin khác mà điều tra viên có thu thập. Không phải mọi hệ thống sẽ được cài đặt tường lửa và thậm chí ít hơn sẽ có tường lửa được cấu hình để đăng nhập các kết nối thành công vào và ra khỏi hệ thống. Mọi hệ thống cũng không có một ứng dụng như Trình báo cáo cổng (<http://support.microsoft.com/kb/837243>) cài đặt để ghi lại và ghi thông tin kết nối mạng. Điều tra viên phải được chuẩn bị để phản ứng nhanh chóng và thu thập thông tin cô ấy cần một cách hiệu quả, kịp thời. Tôi đã tham gia vào một số trường hợp tôi đã được cung cấp các tệp hình ảnh thu được từ một hệ thống, và khách hàng đã hỏi, dữ liệu có nhạy cảm được sao chép từ hệ thống không? ít nhất là một số thông tin dựa trên mạng, câu trả lời sẽ luôn luôn là ở đó . Tôi cũng đã ở trong nhiều tình huống có một số thông tin về mạng các kết nối sẽ làm giảm đáng kể những gì tôi phải tìm kiếm, đặc biệt là khi những gì được cảnh báo khách hàng của vụ việc ở nơi đầu tiên thực sự không liên quan gì đến sự thỏa hiệp chúng tôi đã kết thúc khám phá. Trong một tình huống cụ thể, phân tích dòng thời gian của hình ảnh hệ thống cho thấy kẻ xâm nhập đang truy cập hệ thống thông qua một cửa hậu cùng lúc với hai các quản trị viên khác nhau đã truy cập hệ thống để khắc phục hai vấn đề riêng biệt. Đang có thông tin về các kết nối mạng sẽ đến và từ hệ thống cực kỳ hữu ích trong việc xác định vị trí xâm nhập cốt lõi.

## **Netstat**

Netstat có lẽ là công cụ nổi tiếng nhất để thu thập thông tin liên quan đến mạng kết nối trên hệ thống Windows. Công cụ CLI này rất đơn giản và dễ sử dụng và cung cấp một cái nhìn đơn giản về các kết nối TCP và Giao thức gói dữ liệu người dùng (UDP) và các kết nối của chúng thống kê trạng thái, lưu lượng truy cập mạng, và tương tự. Netstat.exe là một công cụ gốc, có nghĩa là nó cung cấp như là một phần của phân phối hệ điều hành. Cách phổ biến nhất để chạy netstat là với các bộ chuyển mạch , cho biết chương trình để hiển thị các kết nối mạng TCP và UDP, các cổng nghe và số nhận dạng của các quá trình (các PID) sử dụng các kết nối mạng đó. Hình 1.7 minh họa đầu ra của lệnh netstat –ano command.





**Figure 7: Excerpt from the Output of the netstat –ano Command on Windows 10**

Đầu ra của lệnh netstat –ano được minh họa trong Hình 1.7 cho thấy mạng hoạt động các kết nối, trạng thái của từng kết nối và ở phía bên phải, các PID của các quá trình sử dụng các cổng. Những gì bạn đang tìm kiếm trong đầu ra của netstat là bất kỳ kết nối bất thường nào. Dành cho Ví dụ, không có gì lạ trên nhiều hệ thống người dùng khi thấy các kết nối đi ra từ mức cao cổng máy khách đến một hệ thống từ xa, kết nối trên cổng 80. PID của quá trình sử dụng điều này kết nối thường sẽ ánh xạ trở lại trình duyệt Web. Tuy nhiên, điều tra viên có thể dễ dàng bị lừa. Tôi đã điều tra các trường hợp sử dụng công cụ wget.exe để kết nối với các hệ thống từ xa trên cổng 80 và tải về phần mềm độc hại và tin tặc. Tự mình và không cần thêm xem xét kỹ lưỡng, các kết nối này sẽ tìm đến điều tra viên (và IDS) như hợp pháp lưu lượng truy cập lướt web.

Sử dụng netstat với khóa chuyển đổi sẽ hiển thị bảng định tuyến và cho bạn biết liệu có các tuyến liên tục được kích hoạt trên hệ thống. Điều này có thể cung cấp một số thông tin rất hữu ích để một điều tra viên hoặc thậm chí đơn giản là một quản trị viên xử lý sự cố một hệ thống. Tôi đã thấy các hệ thống đã được thiết lập để chuyển tệp đến một vị trí khác như một phần của quy trình kinh doanh và cách duy nhất mà quá trình sẽ hoạt động là nếu một tuyến liên tục được bật trên hệ thống, kể từ khi tuyến đường liên tục chuyển hướng lưu lượng truy cập nhất định qua kết nối mạng riêng ảo (VPN) thay vì thông qua các tuyến thông thường ra khỏi cơ sở hạ tầng. Trong khắc phục sự cố một vấn đề thực sự rất khó hiểu đối với tôi, tôi chạy qua một tuyến đường dai dẳng và nói với một của các kỹ sư hệ thống về nó. Thông tin này khiến trí nhớ của anh ấy tăng lên một chút, và chúng tôi đã có thểđể theo dõi và giải quyết vấn đề.

# **Process Information**

Một điều tra viên sẽ luôn muốn biết những quy trình nào đang chạy trên một tiềm năng hệ thống bị xâm phạm. Lưu ý khi xem các tiến trình đang chạy trong .Trình quản lý tác vụ, bạn có thể xem một số thông tin về từng quy trình. Tuy nhiên, trong một điều tra bạn sẽ muốn thu thập thêm nhiều thông tin mà không thể nhìn thấy trong nhiệm vụ Giám đốc. Bạn sẽ muốn:

* Đường dẫn đầy đủ đến hình ảnh thực thi (tệp .exe)
* Dòng lệnh được sử dụng để khởi chạy tiến trình, nếu có
* Lượng thời gian mà quy trình đã chạy
* Bối cảnh bảo mật / người dùng trong đó quá trình đang chạy
* Những mô-đun mà quá trình đã tải
* Nội dung bộ nhớ của quá trình

The Task Manager cung cấp một số thông tin này, nhưng nó không cung cấp mọi điều. Chẳng hạn, một số phần mềm độc hại tự cài đặt dưới tên svchost.exe, đó là tên của một quy trình hợp pháp trên các hệ thống Windows (xem thanh bên của Sv Svostost). Việc thực thi hình ảnh cho quá trình này nằm trong thư mục system32 và được bảo vệ bởi Windows File Bảo vệ (WFP; xem thanh bên Bảo vệ tệp Windows của Windows để biết thêm thông tin). Điều này có nghĩa là miễn là WFP đang hoạt động và đã bị giả mạo, cố gắng thay thế hoặc sửa đổi một tệp được bảo vệ sẽ khiến tệp mới được tự động thay thế bởi một tên được biết đến bản sao tốt từ bộ đệm và một mục nhật ký sự kiện sẽ được tạo.Tại sao nó lại quan trọng? Nếu bạn nhìn vào danh sách các quy trình trong Trình quản lý tác vụ, làm thế nào bạn có định nói quá trình nào là nghi ngờ về vụn không? Một cách dễ dàng để tìm các quy trình đáng ngờ là để xem đường dẫn đầy đủ đến tệp hình ảnh thực thi (svchost.exe đang chạy từ một cái gì đó khác với C: \ Windows \ system32 sẽ bị nghi ngờ) và / hoặc dòng lệnh được sử dụng để khởi chạy quy trình, như inetinfo.exe đã khởi chạy với các đối số nên nghi ngờ với hầu hết các quản trị viên và điều tra viên; dòng lệnh này chỉ ra việc sử dụng netcat như một cửa hậu. Nhiều phần mềm độc hại ngụy trang bằng cách sử dụng tên của hồ sơ hợp pháp. Ví dụ: sâu W32 / Nachi đặt một bản sao của Chuyển tập tin tầm thường .Tiện ích Giao thức (TFTP) trong thư mục C: \ Windows \ system32 \ Wins và đặt tên là svchost. exe Khi chương trình này đang chạy, Trình quản lý tác vụ không có cách nào để thực sự phân biệt nó từ phiên bản hợp pháp của svchost.exe.

## **Tlist**

Tlist.exe, được bao gồm như một phần của Công cụ gỡ lỗi của Microsoft (www.microsoft.com/whdc/devtools / debugging / default.mspx), hiển thị rất nhiều thông tin về việc chạy các quy trình. Ví dụ, bộ chuyển đổi sẽ hiển thị mã định danh phiên, PID, tên quy trình, các dịch vụ liên quan và dòng lệnh được sử dụng để khởi chạy quy trình cho điều tra viên, như sau:

*Command Line: C:\WINDOWS\System32\svchost.exe -k LocalService*

Các thiết bị chuyển mạch khác sẽ hiển thị thông tin này trong sự cô lập. Công tắc điện tử sẽ chỉ hiển thị dòng lệnh được sử dụng để khởi chạy từng tiến trình, trong khi đó, chuyển đổi trên mạng sẽ hiển thị liên kết dịch vụ (hoặc tiêu đề cửa sổ, nếu không có dịch vụ nào được liên kết với quy trình). Công tắc chuyển đổi sẽ hiển thị cây nhiệm vụ, liệt kê từng tiến trình bên dưới tiến trình cha của nó, như sau:

*System (4)  
smss.exe (628)  
csrss.exe (772)  
winlogon.exe (1056)  
services.exe (1100)  
svchost.exe (1296)  
svchost.exe (1344)  
svchost.exe (1688)  
wscntfy.exe (1184)*

Tlist.exe cũng cho phép bạn tìm kiếm tất cả các quy trình có tải một mô-đun cụ thể, sử dụng bộ chuyển đổi. Ví dụ: wsock32.dll cung cấp chức năng kết nối mạng và được mô tả là Windows socket 32-Bit DLL. Để liệt kê tất cả các quy trình có mô-đun này đã tải, gõ lệnh sau:

*D:\tools>tlist –m wsock32.dll*

Lệnh này trả về PID và tên cho mỗi quá trình, chẳng hạn như:

*WSOCK32.dll - 1688 svchost.exe  
wsock32.dll - 344 svchost.exe  
WSOCK32.dll - 1992 alg.exe*

## **Tasklist**

Tasklist.exe, một tiện ích gốc có trong cài đặt Windows XP Pro và Windows 2003

(đáng chú ý là không có trong Windows XP Home), là sự thay thế cho tlist.exe. Sự khác biệt trong hai công cụ là tinh tế và chủ yếu liên quan đến tên và việc thực hiện

các công tắc. Tasklist.exe cung cấp các tùy chọn cho định dạng đầu ra, với các lựa chọn trong số bảng, giá trị được phân tách bằng dấu phẩy (CSV) và định dạng danh sách. Công tắc / v (hoặc dài dòng) cung cấp hầu hết thông tin về các quy trình được liệt kê, bao gồm tên hình ảnh (nhưng không đầy đủ đường dẫn), PID, tên và số phiên cho quy trình, trạng thái của quy trình, tên người dùng về bối cảnh trong đó quy trình chạy và tiêu đề của cửa sổ, nếu quy trình có GUI.

Điều tra viên cũng có thể sử dụng khóa / svc để liệt kê thông tin dịch vụ cho từng quy trình.

## **PsList**

Pslist.exe (http://technet.microsoft.com/en-us/sysiternals/bb896682.aspx) hiển thị cơ bản thông tin về các quy trình đang chạy trên một hệ thống, bao gồm lượng thời gian mỗi quy trình đã được chạy (trong cả chế độ kernel và user). Công tắc điện tử hiển thị chi tiết về chủ đề và bộ nhớ được sử dụng bởi mỗi quá trình. Pslist.exe được khởi chạy với khóa chuyển đổi sẽ hiển thị một cây nhiệm vụ theo cách tương tự như tlist.exe. Pslist.exe cũng có thể hiển thị thông tin chi tiết về các luồng hoặc bộ nhớ được sử dụng bởi một quy trình. Tuy nhiên, nó không cung cấp thông tin về một quá trình liên quan đến đường dẫn đến hình ảnh thực thi, dòng lệnh được sử dụng để khởi chạy tiến trình hoặc bối cảnh người dùng trong đó tiến trình chạy.

## **ListDLLs**

Listdlls.exe (http://technet.microsoft.com/en-us/sysiternals/bb896656.aspx) hiển thị mô-đun hoặc DLL một quá trình đang sử dụng. Listdlls.exe sẽ hiển thị đường dẫn đầy đủ đến hình ảnh của mô-đun được tải cũng như liệu phiên bản của DLL được tải trong bộ nhớ có khác nhau không từ hình ảnh trên đĩa. Thông tin này có thể cực kỳ quan trọng đối với một nhà điều tra bởi vì mỗi chương trình tải hoặc nhập khẩu một số DLL nhất định. Các DLL này cung cấp thực tế mã được sử dụng, do đó, các nhà phát triển ứng dụng don lồng phải viết lại các chức năng phổ biến thời gian họ viết một ứng dụng mới. Mỗi DLL làm cho các chức năng nhất định có sẵn, liệt kê chúng trong bảng xuất của họ và các chương trình truy cập các hàm này bằng cách liệt kê DLL và các hàm trong bảng nhập khẩu của họ. Điều này cho phép bạn có thể nhìn thấy trên mạng (sử dụng một công cụ thích hợp) mà DLL tải chương trình hoặc truy cập. Tuy nhiên, một số chương trình có thể tải thêm DLL mà không phải một phần của bảng nhập khẩu; ví dụ: trình duyệt Internet Explorer có thể tải các thanh công cụ và các đối tượng trợ giúp trình duyệt mà mã được liệt kê trong DLL. Phần mềm gián điệp, Trojan và thậm chí rootkit sử dụng một kỹ thuật gọi là DLL DLL để tự tải vào không gian bộ nhớ của một tiến trình đang chạy để chúng sẽ chạy và thực thi nhưng won đã xuất hiện trong một tiến trình liệt kê bởi vì chúng thực sự là một phần của quá trình khác. Điều này khác với một quá trình con (như được minh họa trong đầu ra của tlist.exe chạy với khóa chuyển đổi) vì phần mềm độc hại đang thực thi không có PID riêng.Một phần của đầu ra được hiển thị bởi listdlls.exe bao gồm dòng lệnh được sử dụng để khởi chạy mỗi quá trình, được trích dẫn như sau:

*svchost.exe pid: 1292  
Command line: C:\WINDOWS\system32\svchost -k DcomLaunch*

Sử dụng listdlls.exe (với công tắc dllname), bạn cũng có thể liệt kê các quy trình có đã tải một DLL cụ thể, theo cách tương tự như tlist.exe. Điều này có thể cực kỳ hữu ích nếu bạn đã xác định một DLL cụ thể và muốn xem liệu có bất kỳ quy trình nào khác đã tải nó không.

## **Handle**

Xử lý.exe (http://technet.microsoft.com/en-us/sysiternals/bb896655.aspx) hiển thị khác nhau xử lý các quy trình đã mở trên một hệ thống. Điều này không chỉ áp dụng để mở xử lý tệp (đối với tệp và thư mục), mà còn cho các cổng, khóa Registry và chủ đề. Thông tin này có thể hữu ích để xác định tài nguyên nào mà một quá trình truy cập trong khi nó đang chạy. Hình 1.8 minh họa một trích đoạn đầu ra từ khi chạy handle.exe, không có bất kỳ công tắc nào, trên Windows XP SP2 hệ thống.

**Figure 8:Excerpt of Output of handle.exe**



Hình 1.8 minh họa một số tay cầm được mở bởi svchost.exe, trong trường hợp này, một số nhật ký các tập tin trong thư mục Windows. Trong khi tôi đang viết chương này, ví dụ, một trong những xử lý được mở bởi winword.exe bao gồm đường dẫn đầy đủ đến tài liệu Microsoft Word.

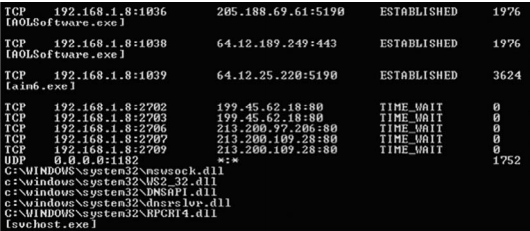
Handle.exe có một số công tắc có thể được sử dụng, chẳng hạn như Mạnha để hiển thị tất cả các điều khiển và hội nghị để hiển thị tên người dùng sở hữu cho mỗi tay cầm.

**Process-to-Port Mapping**

Khi kết nối mạng được mở trên một hệ thống, một số quy trình phải chịu trách nhiệm và phải được sử dụng kết nối đó. Đó là, mọi kết nối mạng và cổng mở được liên kết với một quá trình. Một số công cụ có sẵn cho nhà điều tra để truy xuất quy trình này đến cổng lập bản đồ.

**Netstat**

Trên Windows XP và Windows 2003, chương trình netstat.exe cung cấp khóa chuyển đổi để hiển thị PID cho quá trình chịu trách nhiệm về kết nối mạng. Khi bạn đã thu thập thông tin này (tham khảo lại lệnh netstat hèano), bạn sẽ cần tương quan với thông tin đó đầu ra của một công cụ như tlist.exe hoặc tasklist.exe để xác định tên (và bổ sung thông tin) của quá trình sử dụng kết nối. Kể từ Gói dịch vụ 2, Windows XP có thêm một tùy chọn bổ sung sẽ hiển thị thực thi liên quan đến việc tạo từng kết nối hoặc cổng nghe. Công tắc này cũng được bao gồm trong netstat.exe trong Windows 2003 SP1 và có thể cung cấp thêm thông tin về quy trình sử dụng một cổng cụ thể. Trong một số trường hợp, đầu ra cũng sẽ hiển thị một số mô-đun (DLL) được sử dụng bởi quá trình. Hình 1.9 minh họa một đoạn trích từ đầu ra của lệnh chạy trên một hệ thống Windows XP SP2.



**Figure 9:Excerpt of Output from**

## **Fport**

Fport.exe từ lâu đã là một trong những công cụ được lựa chọn để có được ánh xạ quy trình tới cổng từ một hệ thống Windows. Đầu ra của công cụ rất dễ hiểu; tuy nhiên, bạn phải chạy công cụ từ trong tài khoản Administrator để lấy thông tin của nó. Đây có thể là một vấn đề nếu bạn đang phản ứng với một tình huống trong đó tài khoản người dùng đã đăng nhập là một tài khoản người dùng và không có đặc quyền của Quản trị viên.

**Tcpvcon**

Tcpvcon.exe có sẵn từ Microsoft (ban đầu là một phần của công cụ Sysiternals.com) và là một trong những công cụ tốt nhất để truy xuất thông tin ánh xạ quy trình tới cổng từ hệ thống Windows. Theo mặc định, tcpvcon.exe sẽ chỉ hiển thị thông tin liên quan đến TCP kết nối và in thông tin trong bảng điều khiển theo định dạng bảng liệt kê, như minh họa ở đây:

*[TCP] C:\Program Files\Mozilla Firefox\firefox.exe  
PID: 3476*

*State: ESTABLISHED  
Local: wintermute.adelphia.net:5918  
Remote: chrome.com*

# **Process Memory**

Một hệ thống trực tiếp sẽ có bất kỳ số lượng quy trình đang chạy và bất kỳ một trong các quy trình đó có thể đáng ngờ hoặc độc hại về bản chất. Khi một quá trình được thực thi trên một hệ thống, nó thường được đặt cùng tên với tệp có hình ảnh thực thi và trên các hệ thống Windows nói riêng, một tệp có thể được đặt tên gần như bất cứ thứ gì. Kẻ xấu chỉ đơn giản là aren rất hữu ích khi đặt tên cho mã độc của chúng một cái gì đó dễ nhận biết, chẳng hạn như bad ware.exe. Thường xuyên hơn không, họ sẽ đổi tên tệp thành một cái gì đó dễ thấy hơn hoặc họ có thể cố gắng ngụy trang mục đích của chương trình bằng cách sử dụng tên của một chương trình thường thấy trên các hệ thống Windows (xem thanh bên của Sv Svostost).

Khi bạn đã sử dụng các công cụ mà chúng tôi đã thảo luận và tìm thấy những gì bạn xác định là một quy trình đáng ngờ, bạn có thể quyết định rằng bạn muốn biết thêm thông tin về quy trình đó đang làm gì. v nhớ mà quá trình đang sử dụng. Bạn có thể sử dụng một số công cụ để thực hiện nhiệm vụ này. Như đã nêu trước đây, bạn có thể tìm thấy một cuộc thảo luận chi tiết về việc thu thập nội dung của RAM (cũng như bộ nhớ được sử dụng bởi các quy trình cụ thể) trong Chương 3.

**Network Status**

Nhận thông tin về trạng thái của thẻ giao diện mạng (NIC) được kết nối với hệ thống có thể cực kỳ quan trọng đối với một cuộc điều tra. Ví dụ, ngày nay, nhiều máy tính xách tay đi kèm với các NIC không dây tích hợp, vì vậy bạn có thể không biết chỉ bằng cách nhìn vào máy tính để bàn xem hệ thống có được kết nối với điểm truy cập không dây hay không, và nếu vậy nó đang sử dụng địa chỉ IP nào. Biết được trạng thái của các NIC trước khi hệ thống được mua có thể cung cấp cái nhìn sâu sắc về một cuộc điều tra tiếp theo.

## **Ipconfig**

Ipconfig.exe là một tiện ích có nguồn gốc từ các hệ thống Windows mà nhà điều tra có thể sử dụng để hiển thị thông tin về các NIC và trạng thái của chúng. Công tắc hữu ích nhất cho các nhà điều tra là tất cả, được sử dụng để hiển thị cấu hình mạng của các NIC trên hệ thống. Thông tin này bao gồm trạng thái của NIC, cho dù DHCP được bật, địa chỉ IP của NIC và hơn thế nữa.

Bạn có thể thấy thông tin này hữu ích trong quá trình điều tra, bởi vì bạn có thể có nhật ký lưu lượng mạng để kiểm tra và địa chỉ IP của hệ thống có thể đã bị sửa đổi tại một số điểm. Ngoài ra, nhiều dịch vụ e-mail dựa trên Web (như Yahoo! Mail) ghi lại địa chỉ IP của hệ thống mà từ đó một e-mail được soạn thảo trong tiêu đề của e-mail. Tôi đã tham gia vào một cuộc điều tra cụ thể trong đó một nhân viên cũ đã gửi e-mail gây phiền nhiễu (không quấy rối) cho công ty chúng tôi. Nhìn vào các tiêu đề e-mail, chúng tôi có thể ngăn chặn tôi từ nơi anh ta gửi e-mail. Một số trong số họ đã được gửi từ một cửa hàng sao chép địa phương và những người khác từ một thư viện công cộng địa phương. Với sự giúp đỡ tận tình của các quản trị viên từ cửa hàng sao chép và quận, chúng tôi đã có thể thu hẹp các địa điểm hơn nữa; trong trường hợp thư viện công cộng, chúng tôi có thể xác định được chi nhánh của thư viện và thực tế là hệ thống anh ta đang sử dụng ở tầng hai (một trong các quản trị viên đã yêu cầu một nhân viên thư viện nhập lệnh ipconfig / all trên một số hệ thống cho đến khi anh ta xác định được địa chỉ IP được đề cập). Không cần phải nói, cựu nhân viên đã bị sốc khi tiếp xúc với thông tin này và ngừng gửi e-mail. Nếu anh ta không bị sa thải và anh ta đã gửi e-mail từ hệ thống làm việc của mình thông qua Yahoo! Mail, chúng tôi sẽ có thể xác định vị trí của mình là tốt.

Các hệ thống bị xâm nhập của PromiscDetect và PromqrySometimes sẽ được cài đặt một bộ sniffer trực tuyến để nắm bắt lưu lượng mạng, như thông tin đăng nhập cho các hệ thống khác hoặc để phát triển một bức tranh về các hệ thống khác trên mạng và những dịch vụ nào chúng đang chạy. Một số tải trọng phần mềm độc hại bao gồm khả năng này hoặc nó có thể là bản tải xuống tiếp theo được cài đặt bởi kẻ tấn công. Để NIC thu được lưu lượng mạng theo cách này, nó phải được đặt ở chế độ Lừa đảo. Đây là một cái gì đó mà một quản trị viên hoặc điều tra viên sẽ nhìn thấy, bởi vì không có gì rõ ràng để chỉ ra rằng NIC đang ở chế độ lăng nhăng. Không có biểu tượng Khay hệ thống hoặc Bảng điều khiển cho biết điều tra rõ ràng cho điều tra viên rằng hệ thống đang được sử dụng để lưu lượng truy cập cảnh báo.

Các công cụ có sẵn để cho bạn biết liệu NIC có ở chế độ lăng nhăng hay không. Một công cụ như vậy là promiscdetect.exe (www.ntsecurity.nu/toolbox/promiscdetect/). Cái còn lại là promqry.exe (có sẵn từ Microsoft, tại một URL thực sự dài), được viết bởi Tim Rains. Sự khác biệt chính giữa hai công cụ là promqry.exe có thể chạy trên các hệ thống từ xa, cho phép quản trị viên quét các hệ thống trong miền để tìm các hệ thống có thể đánh hơi được mạng

**Tools & Traps…**

Promiscuous Mode

Tập lệnh Perl ndis.pl (nằm trong thư mục \ ch2 \ code trên phương tiện đi kèm với cuốn sách này) thực hiện mã WMI để xác định cài đặt cho một NIC. Cụ thể, nó được thiết kế để được sử dụng để xác định xem một NIC có ở chế độ bừa bãi hay không và có khả năng đánh hơi các gói từ mạng.

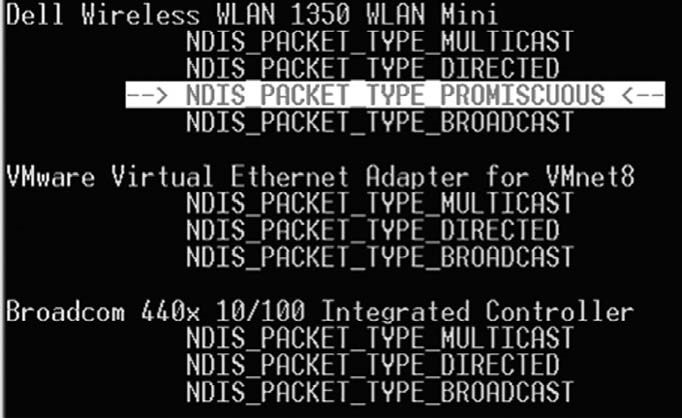
Tệp ndis.exe trong cùng thư mục là phiên bản thực thi độc lập của tập lệnh này, được cung cấp để sử dụng cho những người không cài đặt Perl trên hệ thống Windows.

Hình 1.10 minh họa một đoạn trích của đầu ra được trả về từ ndis.exe.

Đầu ra được hiển thị trong Hình 1.10 được tạo bằng cách khởi chạy ứng dụng sniffer Wireshark (trước đây gọi là Ethereal; www.wireshark.org) trên NIC không dây và sau đó chạy ndis.exe. Phần được tô sáng của đầu ra cho thấy rõ ràng rằng NIC không dây ở chế độ lăng nhăng.

Cả tập lệnh Perl và tập tin thực thi liên quan chỉ nhằm mục đích chạy trên hệ thống cục bộ. Tuy nhiên, các sửa đổi nhỏ đối với mã sẽ cho phép tập lệnh (hoặc tệp thực thi, sau khi tập lệnh được sửa đổi và biên dịch lại) để chạy với các hệ thống từ xa, theo cách tương tự như promqry.exe.

**Figure 10 : Minh họa một đoạn trích của đầu ra được trả về từ ndis.exe.**



Một ứng dụng rất quan trọng khác cho các công cụ như điều này là để xác định giao diện mạng đang hoạt động có thể là gì trên một hệ thống trực tiếp. Các hệ thống Toshiba Tecra 8100 cũ của tôi yêu cầu thẻ PCIMCIA để có thể kết nối với mạng không dây, trong khi nhiều hệ thống mới hơn của Windows mà tôi đã xử lý đi kèm với khả năng kết nối mạng không dây được tích hợp ngay trong hệ thống. Bạn không bao giờ nhìn thấy bất cứ thứ gì nhô ra khỏi vỏ máy tính xách tay, bạn cũng không thấy bất kỳ đèn nhấp nháy nào, như bạn làm với kết nối Ethernet RJ-45. Vì vậy, khi Dave tham gia một cuộc họp và ngồi xuống phía sau máy tính xách tay của mình, anh ta chỉ đang ghi chú hay anh ta cũng đang lướt web và gửi e-mail? Truy cập không dây ngày càng trở nên phổ biến, không chỉ bởi vì hiện tại có rất nhiều địa điểm có sẵn, mà còn bởi vì nó được tích hợp ngay trên máy tính xách tay của chúng tôi.

Truy cập không dây này có thể là một lối vào tổ chức của bạn, hoặc thậm chí là một tuyến đường mà ai đó sử dụng để lấy thông tin ra khỏi cơ sở hạ tầng của bạn. Tôi đã từng xử lý một vấn đề trong đó một người quan hệ công chúng trong công ty chúng tôi quyết định rằng cô ấy cần mang máy tính xách tay cá nhân của mình vào các cuộc họp để cô ấy có thể truy cập Internet. Nhưng cô ấy đã quyết định không liên lạc với bất kỳ ai từ IT, hoặc thậm chí cả tôi (tôi là quản trị viên bảo mật). Khi cô ấy kích hoạt máy tính xách tay của mình, cô ấy đã tìm thấy các điểm truy cập không dây của chúng tôi, có khóa Giao thức mã hóa không dây (WEP) và lọc địa chỉ MAC được bật. Bởi vì cô ấy đã không liên lạc với chúng tôi và cô ấy đang họp và cần quyền truy cập 10 phút trước, cô ấy đã quyết định kết nối với một điểm truy cập không dây mở mà hệ thống của cô ấy đã phát hiện ra một cái được sử dụng bởi một công ty bên cạnh chúng tôi và đã được mở rộng, không có biện pháp an ninh tại chỗ. Khi cô ấy thực hiện kết nối đó, cô ấy đã tạo một điểm vào cơ sở hạ tầng của chúng tôi mà bỏ qua tất cả các cơ chế bảo vệ chúng tôi có, bao gồm tường lửa và phần mềm chống vi-rút.

Vào thời điểm đó, thật khó để nói tình huống nào gây tổn hại nhiều hơn cho kết nối của cô ấy được sử dụng như một ống dẫn để lây nhiễm cho chúng tôi cơ sở hạ tầng hoặc sự phân nhánh hợp pháp nếu cơ sở hạ tầng của công ty khác bị vi phạm an ninh và mọi cơ chế ghi nhật ký cho thấy kết nối của cô ấy trong thời gian đó. Trong một cuộc điều tra, nói chung nên thu thập thông tin về các giao diện mạng đang hoạt động trên hệ thống mà bạn đang kiểm tra. Điều này bổ sung bối cảnh không chỉ vào dữ liệu dễ bay hơi mà bạn đang thu thập mà còn cho phân tích hậu hiện đại, mà chúng ta sẽ thảo luận sau trong cuốn sách này.

## **Clipboard Contents**

Clipboard chỉ đơn giản là một vùng bộ nhớ nơi dữ liệu có thể được lưu trữ để sử dụng sau này. Hầu hết các ứng dụng Windows cung cấp chức năng này thông qua tùy chọn chỉnh sửa trên thanh menu. Nhấp vào **Edit** sẽ hiển thị trình đơn thả xuống với các lựa chọn như Cắt, Sao chép và Dán. Microsoft Word 2003 bao gồm tùy chọn Office Clipboard.

Clipboard thường được sử dụng để tạo điều kiện di chuyển dữ liệu trong một số thời trang giữa các tài liệu hoặc giữa các cửa sổ ứng dụng trên máy tính để bàn. Người dùng chọn văn bản hoặc dữ liệu khác, chọn **Copy** và sau đó chọn **Paste** để chèn dữ liệu đó vào nơi khác. Chức năng Cắt sẽ xóa dữ liệu khỏi tài liệu mà người dùng đang làm việc và dữ liệu đó đi vào Clipboard.

Điều mà nhiều người không nhận ra là họ có thể bật máy tính vào sáng thứ Hai, làm việc trên một tệp và sao chép một số thông tin vào Clipboard của họ. Hãy nói rằng họ đang chỉnh sửa một tài liệu chứa thông tin nhạy cảm và thông tin cá nhân về một khách hàng cần được thêm vào tài liệu đó. Người dùng định vị, tô sáng và sao chép thông tin vào Clipboard, sau đó dán nó vào tài liệu. Chừng nào máy tính còn hoạt động, người dùng không đăng xuất và không có gì được thêm vào Clipboard để thay thế những gì được đặt ở đó, dữ liệu vẫn còn trên Clipboard.

Thỉnh thoảng hãy thử nó. Đi tới máy tính của bạn, mở tài liệu Notepad hoặc Word và chỉ cần sử dụng tổ hợp phím **Control + V** để dán bất cứ thứ gì hiện có trong Clipboard vào tài liệu. Hãy thử điều này trên các máy tính khác. Bạn có thể ngạc nhiên bởi những gì bạn nhìn thấy. Tần suất bạn tìm thấy URL, bit của các cuộc hội thoại IM, mật khẩu hoặc toàn bộ các phần văn bản từ các tài liệu vẫn có sẵn trên Clipboard? Clipboard không hiển thị trên hệ thống, nhưng nó ở đó và nó đã là một vấn đề rất nhiều vì vậy có một bài viết của Cơ sở tri thức Microsoft có tiêu đề Cách làm thế nào để ngăn chặn các trang web truy cập vào nội dung của Windows Clipboard của bạn ( http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q224993&) áp dụng cho Internet Explorer phiên bản 4 đến 6.

Dữ liệu được tìm thấy trong Clipboard có thể hữu ích trong nhiều trường hợp, chẳng hạn như thông tin hoặc trộm cắp tài sản trí tuệ, lừa đảo hoặc quấy rối. Đôi khi thông tin như vậy có thể cung cấp cho bạn manh mối; đôi khi bạn có thể tìm thấy hình ảnh hoặc toàn bộ các phần của tài liệu trên Clipboard.

Pclip.exe (có sẵn từ http://unxutils.sourceforge.net) là một tiện ích CLI có thể được sử dụng để truy xuất nội dung của Clipboard. Các tiện ích CLI như pclip.exe giúp dễ dàng tự động thu thập thông tin thông qua các tệp và tập lệnh bó.

**Tools & Traps…**

Perl cung cấp giao diện đơn giản cho API để truy cập nội dung của Clipboard. Kịch bản sau đây in nội dung của Clipboard dưới dạng chuỗi:

use strict;

use Win32::Clipboard;

print "Clipboard contents = ".Win32::Clipboard()->Get()."\n";

Để sử dụng rộng rãi hơn Win32 :: Clipboard, hãy tham khảo tài liệu cho mô-đun

## **Service/Driver Information**

Các dịch vụ và trình điều khiển được khởi động tự động khi hệ thống khởi động, dựa trên các mục trong Sổ đăng ký. Hầu hết người dùng thậm chí không thấy các dịch vụ này chạy dưới dạng các quy trình trên hệ thống vì thực sự không có chỉ dẫn rõ ràng, như có các quy trình (ví dụ: bạn có thể thấy các quy trình đang chạy trong Trình quản lý tác vụ). Tuy nhiên, các dịch vụ này đang chạy. Không phải tất cả các dịch vụ đều được cài đặt bởi người dùng hoặc thậm chí bởi quản trị viên hệ thống. Một số phần mềm độc hại tự cài đặt như một dịch vụ hoặc thậm chí là trình điều khiển hệ thống.

**Tools & Traps…**

*Thông tin dịch vụ*

Tập lệnh Perl svc.pl, nằm trong thư mục \ ch2 \ code trên phương tiện đi kèm, sử dụng WMI (truy cập lớp Win32\_Service) để truy xuất thông tin về các dịch vụ từ hệ thống cục bộ hoặc từ xa. Tệp svc.exe là tệp thực thi Windows độc lập được tạo bằng cách biên dịch tập lệnh Perl với Perl2Exe.

Cả tập lệnh Perl và tập tin thực thi sẽ hiển thị thông tin sau về các dịch vụ:

■ Tên của dịch vụ

■ DisplayName cho dịch vụ

■ StartName (bối cảnh được sử dụng để khởi chạy dịch vụ)

■ Chuỗi mô tả cho dịch vụ

■ PID cho dịch vụ (điều này có thể được sử dụng để ánh xạ dịch vụ tới thông tin quy trình)

■ Đường dẫn đến hình ảnh thực thi cho dịch vụ

■ Chế độ bắt đầu cho dịch vụ

■ Hiện trạng của dịch vụ

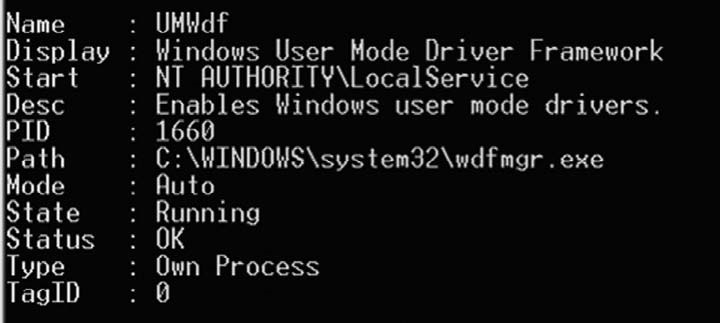
■ Tình trạng dịch vụ

■ Loại dịch vụ (trình điều khiển kernel, quá trình chia sẻ, v.v.)

■ ID thẻ, một giá trị duy nhất được sử dụng để đặt hàng khởi động dịch vụ trong nhóm đặt hàng

Hình 1.11 minh họa một ví dụ về thông tin được hiển thị bởi tiện ích này.

Cả tập lệnh Perl và tập tin thực thi đều có thể được sửa đổi để xuất thông tin này ở nhiều định dạng khác nhau, bao gồm CSV để giúp phân tích thông tin dễ dàng hơn hoặc dễ dàng phân tích bằng cách làm cho đầu ra phù hợp để mở trong bảng tính



**Figure 11:Trích từ Đầu ra của svc.exe trên Windows XP**

## **Command History**

Hãy để nói rằng bạn tiếp cận một hệ thống trong quá trình điều tra và thấy một hoặc nhiều lời nhắc lệnh mở trên màn hình. Tùy thuộc vào tình huống, các manh mối có giá trị có thể được ẩn trong các lệnh được người dùng nhập vào, chẳng hạn như ftp hoặc ping. Để xem các lệnh đã nhập trước đó, bạn có thể chạy thanh cuộn cho dấu nhắc lệnh (nếu nhiều lệnh được phát qua dấu nhắc lệnh, màn hình sẽ mở rộng phía trên phần hiển thị của cửa sổ nhắc lệnh), nhưng điều đó chỉ đi xa . Nếu người dùng gõ lệnh cls để xóa màn hình, bạn đã thắng được có thể sử dụng thanh cuộn để xem bất kỳ lệnh nào đã được nhập. Thay vào đó, bạn cần sử dụng lệnh doskey / history, sẽ hiển thị lịch sử của các lệnh được nhập vào dấu nhắc đó, như được minh họa trong phần sau

D:\tools>doskey /history

move proc.exe d:\awl2\ch2\code

perl2exe -small d:\awl2\ch2\code\proc.pl

move proc.exe d:\awl2\ch2\code

y

cd \awl2\ch2\code

proc

cd \perl2exe

perl2exe -small d:\awl2\ch2\code\procmon.pl

procmon

move procmon.exe d:\awl2\ch2\code

cd d:\awl2\ch2\code

procmon

cd \tools

openports -fport

openports -netstat

cls

doskey /history

cd \tools

dir prom\*

promqry

dir prom\*

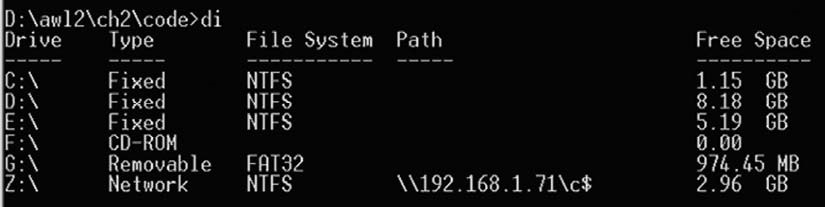
promqry

Tôi sẽ cho bạn một ví dụ về thời điểm tôi sử dụng lệnh này. Tôi đang dạy một khóa học ứng phó sự cố ở Bờ Tây, và trong giờ nghỉ trưa, tôi đã thỏa hiệp với các học sinh. Một bước tôi đặc biệt thực hiện trên một số máy tính là mở dấu nhắc lệnh và gõ một số lệnh, sau đó nhập cls để xóa màn hình. Khi các sinh viên trở về, tôi nhận thấy một cá nhân cụ thể ở phía sau phòng, người ngay lập tức đã đóng (không được thu nhỏ, nhưng đã đóng) dấu nhắc lệnh mà anh ta thấy đang mở trên màn hình. Theo dự định, các manh mối, tôi đã bỏ lại phía sau trong dấu nhắc lệnh cung cấp bối cảnh cho phần còn lại của thỏa hiệp, khi các học sinh đã đóng lệnh nhắc nhở phát hiện ra. Tuy nhiên, tôi sẽ thừa nhận rằng tôi không bao giờ có cơ hội sử dụng lệnh này ngoài môi trường đào tạo. Trong tất cả các trường hợp khi tôi phải đối mặt với một hệ thống trực tiếp, người dùng đã sử dụng một dấu nhắc lệnh. Tuy nhiên, điều này không có nghĩa là nó đã giành chiến thắng với bạn.

## **Mapped Drives**

Trong quá trình điều tra, bạn có thể muốn biết những ổ đĩa hoặc chia sẻ hệ thống mà bạn đang kiểm tra đã ánh xạ tới. Những ánh xạ này có thể được tạo bởi người dùng và chúng có thể là dấu hiệu của mục đích xấu (đây có thể là trường hợp nếu người dùng đoán mật khẩu Quản trị viên và đang truy cập các hệ thống trên toàn doanh nghiệp). Hơn nữa, có thể không có thông tin liên tục trong hệ thống tệp hoặc Đăng ký cho các kết nối này để chia sẻ ánh xạ trên các hệ thống khác, mặc dù thông tin không ổn định về ánh xạ ổ đĩa có thể tương quan với thông tin kết nối mạng mà bạn đã lấy được.

.**Figure 12: Đầu ra của di.exe**



Đầu ra của di.exe được hiển thị trong Hình 1.12 là kết quả của chương trình đang chạy trên hệ thống Windows XP Home với một ổ đĩa được ánh xạ tới một máy chủ Windows 2003 nhỏ, cụ thể là chia sẻ C $ trên máy chủ đó.

Lưu ý rằng đầu ra của di.exe cũng hiển thị một ổ đĩa di động được gán tên ổ đĩa G: \. Đây là một ổ USB được kết nối với USB, các tạo tác mà chúng ta sẽ thảo luận trong Chương 4.

## **Shares**

Bên cạnh các tài nguyên được sử dụng bởi hệ thống mà bạn đang điều tra , bạn cũng sẽ muốn nhận thông tin liên quan đến các tài nguyên mà hệ thống đang cung cấp. Thông tin cho các cổ phiếu có sẵn trên hệ thống được duy trì trong khóa HKEY\_LOCAL\_MACHINE \ System \ CurrentControlSet \ Services \ lanmanserver \ Shares, nhưng cũng có thể được truy xuất từ hệ thống trực tiếp bằng các công cụ CLI như share.exe, có sẵn trên phương tiện đi kèm. (Mã nguồn Perl cho chương trình cũng có sẵn.)

Một đoạn trích về đầu ra của share.exe như sau:

Name -> SharedDocs

Type -> Disk Drive

Path -> C:\DOCUMENTS AND SETTINGS\ALL USERS\DOCUMENTS

Status -> OK

Trong suốt chương này cho đến nay, chúng tôi đã thảo luận về việc sử dụng WMI thông qua Perl. Tôi đã trình bày một số ví dụ và cung cấp mã cho bạn trên phương tiện đi kèm. Microsoft cũng cung cấp quyền truy cập vào WMI thông qua công cụ CLI gốc, wmic.exe (http://support.microsoft.com/kb/290216/en-us). Vũ trụ. exe có thể cực kỳ hữu ích để thu thập nhiều thông tin từ các hệ thống từ xa trên toàn doanh nghiệp. Vào tháng 3 năm 2006, Ed Skoudis đã xuất bản một mục Nhật ký Sans Handler từ Nhật ký (http://isc.sans.org/diary.html?storyid=1229) đưa ra một số tùy chọn dòng lệnh rất thú vị và rất hữu ích để sử dụng wmic.exe

# **Nonvolatile Information**

Trong phản hồi trực tiếp, bạn có thể không muốn hạn chế chỉ thu thập thông tin dễ bay hơi. Tình huống có thể chỉ ra rằng điều tra viên cần thu thập thông tin thường được coi là tồn tại ngay cả khi hệ thống được khởi động lại, chẳng hạn như nội dung của các khóa hoặc tệp Registry. Điều tra viên có thể quyết định rằng thông tin cần được trích xuất từ Cơ quan đăng ký hoặc thông tin về (hoặc từ) các tệp cần được thu thập, để phân tích bổ sung hoặc vì kẻ tấn công có thể được đăng nhập tích cực vào hệ thống. Trong những trường hợp như vậy, điều tra viên có thể quyết định rằng để theo dõi kẻ tấn công (hoặc botnet), cô ấy muốn rời khỏi hệ thống trực tuyến và trực tuyến, nhưng cô ấy cũng muốn giữ thông tin nhất định khỏi bị sửa đổi hoặc xóa. Khi một hệ thống đã được khởi động, có thể có các sửa đổi, chẳng hạn như các ổ đĩa được ánh xạ đến hoặc từ hệ thống, các dịch vụ được khởi động hoặc các ứng dụng được cài đặt. Những sửa đổi này có thể không được duy trì trong suốt quá trình khởi động lại, và do đó có thể cần phải được ghi lại và ghi lại bởi nhà điều tra.

## **Registry Settings**

Một số giá trị và cài đặt Đăng ký có thể ảnh hưởng đến phân tích pháp y và kiểm tra tiếp theo của bạn. Mặc dù các cài đặt này là không dễ biến đổi, nhưng chúng có thể có ảnh hưởng đến cách bạn chọn tiến hành điều tra hoặc thậm chí liệu bạn có tiếp tục điều tra hay không.

Có một số công cụ để thu thập thông tin từ Cơ quan đăng ký. Yêu thích của tôi (nếu bây giờ bạn đã đoán được) là viết một tập lệnh Perl cung cấp các chức năng khác nhau để truy xuất các giá trị cụ thể hoặc tất cả các giá trị và khóa con của một khóa cụ thể. Reg.exe là một công cụ dòng lệnh để truy cập và quản lý Registry là một phần của Công cụ hỗ trợ Windows 2000 và có nguồn gốc từ Windows XP và 2003.

Xóa tệp trang khi tắt máy

Giá trị Registry đặc biệt này báo cho hệ điều hành xóa tệp trang khi hệ thống bị tắt. Vì Windows sử dụng kiến ​​trúc bộ nhớ ảo, một số bộ nhớ được sử dụng bởi các quy trình sẽ được phân trang ra tệp trang. Khi hệ thống bị tắt, thông tin trong tệp trang vẫn còn trên ổ cứng và có thể chứa thông tin như mật khẩu được giải mã, các phần của cuộc hội thoại IM và các chuỗi và bit thông tin khác có thể cung cấp cho bạn các hướng dẫn quan trọng trong quá trình điều tra. Mặc dù hầu hết các giám khảo đều hiểu rằng tệp trang là một kho dữ liệu vô định hình, phần lớn không có ngữ cảnh (nghĩa là, việc định vị một chuỗi thú vị trong tệp trang không cung cấp cho bạn thông tin ngữ cảnh quan trọng, chẳng hạn như chuỗi đó được liên kết với chuỗi nào), những tiến bộ trong phân tích bộ nhớ Windows (để biết thêm thông tin về chủ đề này, xem Chương 3) đã xác định các cách để mở rộng thông tin có sẵn trong một bộ nhớ vật lý Windows bằng cách kết hợp tệp trang vào phân tích. Nếu tệp này bị xóa trong khi tắt máy, thông tin có giá trị này sẽ khó lấy hơn, nếu không bị mất hoàn toàn. Microsoft có các bài viết trong Cơ sở Kiến thức cho giá trị Sổ đăng ký này áp dụng cho cả Windows 2000 (http://support.microsoft.com/kb/182086/EN-US) và Windows XP (http://support.microsoft.com/kb/ 314834 / EN-US /).

Vô hiệu hóa quyền truy cập lần cuối

Hệ thống tệp Windows có khả năng vô hiệu hóa cập nhật lần truy cập cuối cùng trên tệp. Theo Microsoft, điều này có nghĩa là một sự tăng cường hiệu suất, đặc biệt là trên các máy chủ tệp highvolume. Trên các máy trạm bình thường và hầu hết các loại máy tính để bàn và máy tính xách tay mọi người đang sử dụng (máy tính gia đình, máy tính để bàn của nhân viên, v.v.) cài đặt này không cung cấp bất kỳ cải thiện đáng chú ý nào về hiệu suất. Trên Windows 2003, bạn sẽ đặt giá trị sau thành 1:

HKEY\_LOCAL\_MACHINE \ System \ CurrentControlset \ Control \ FileSystem \ NtfsDisableLastAccessUpdate

Theo các tài liệu hướng dẫn điều chỉnh hiệu suất từ Microsoft cho Windows 2003, giá trị này không tồn tại theo mặc định và phải được tạo.

### **Autoruns**

Một số khu vực của Cơ quan đăng ký (và hệ thống tệp) được gọi là vị trí tự khởi động vì chúng cung cấp phương tiện để tự động khởi động ứng dụng, thường không có bất kỳ tương tác trực tiếp nào từ người dùng. Một số vị trí này sẽ tự động bắt đầu các ứng dụng khi hệ thống khởi động, các ứng dụng khác khi người dùng đăng nhập và vẫn còn các ứng dụng khác khi người dùng thực hiện một hành động cụ thể. Trong trường hợp ứng dụng được khởi động khi người dùng thực hiện một hành động nhất định, người dùng sẽ không biết rằng mình đang khởi chạy một ứng dụng khác.

Được rồi, tôi biết công cụ này có trong Sổ đăng ký và thực tế chính nó có thể khiến việc này có vẻ như là một nhiệm vụ khó khăn hoặc không thể, nhưng tin tốt là số lượng địa điểm hữu hạn phục vụ mục đích này. Con số có thể lớn, nhưng nó là hữu hạn. Thay vì liệt kê chúng ở đây, tôi sẽ để lại một bài đánh giá sâu hơn về phân tích Registry để sau này trong cuốn sách. Tuy nhiên, nếu bạn quyết định bạn cần thu thập thông tin này như một phần của hoạt động phản hồi đầu tiên của mình, có hai cách để thực hiện. Đầu tiên là sử dụng một công cụ như reg.exe (đã đề cập trước đó) để thu thập dữ liệu từ các khóa và giá trị cụ thể. Cách thứ hai là sử dụng một công cụ như Autorun (http://technet.microsoft.com/en-us/sysi INTERNals / bb963902.aspx) để làm điều đó cho bạn. Các tác giả của Autorun (Mark Russinovich và Bryce Cogswell, hiện là nhân viên của Microsoft) làm rất tốt việc duy trì danh sách các khu vực được công cụ kiểm tra. Trong một số trường hợp, tôi đã tìm thấy các bổ sung mới cho công cụ trước khi tôi đã thấy các vị trí tự khởi động đó được sử dụng rộng rãi trong phần mềm độc hại. Autorun có các phiên bản GUI và CLI, cả hai đều có cùng chức năng. Ví dụ: bạn có thể sử dụng khóa chuyển đổi trong phiên bản CLI để ẩn các mục nhập Microsoft đã ký (các mục nhập cho các tệp thực thi đã được nhà cung cấp ký) hoặc công tắc của để xác minh chữ ký số.

Tự động chạy cũng thực hiện rất tốt công việc kiểm tra các khu vực trong hệ thống tệp, chẳng hạn như nhiệm vụ theo lịch trình. Đôi khi, quản trị viên sẽ sử dụng tác vụ theo lịch để cung cấp cho mình các đặc quyền nâng cao (tức là, cấp độ HỆ THỐNG) để thực hiện các tác vụ như xem các phần của sổ đăng ký thường bị giới hạn ngay cả đối với quản trị viên. Kẻ tấn công giành quyền truy cập cấp Quản trị viên vào hệ thống có thể làm điều gì đó tương tự để tiếp tục mở rộng sự hiện diện của anh ta trên hệ thống.

Một khu vực khác của Cơ quan đăng ký có thể cung cấp thông tin có giá trị trong một cuộc điều tra là khu vực Lưu trữ được bảo vệ (xem thanh bên Lưu trữ được bảo vệ của Cảnh sát). Thông tin được lưu trữ trong Protected Storage được duy trì ở định dạng được mã hóa trong Registry. Nếu bạn có được hình ảnh của hệ thống, các công cụ như AccessData, Forensic ToolKit sẽ giải mã và khôi phục thông tin. Tuy nhiên, đôi khi việc thu thập thông tin này là một phần của các hoạt động phản hồi trực tiếp, đặc biệt nếu thời gian là điều cốt yếu và thông tin phù hợp với vụ việc.

**NOTE**

*Bảo vệ lưu trữ*

Lưu trữ được bảo vệ là một vùng bộ nhớ nơi thông tin nhạy cảm cho người dùng được duy trì. Khi hệ thống tắt, thông tin này được lưu trữ ở định dạng được mã hóa trong sổ đăng ký và khi người dùng đăng nhập, thông tin sẽ được đặt vào bộ nhớ. Windows đặt thông tin như mật khẩu và dữ liệu AutoComplete cho các biểu mẫu Web trong Bộ nhớ được bảo vệ để sử dụng sau.

Bạn có thể xem nội dung của Lưu trữ được bảo vệ trên hệ thống trực tiếp bằng cách sử dụng các công cụ như pstoreview.exe (www.ntsecurity.nu/toolbox/pstoreview) hoặc Trình khám phá lưu trữ được bảo vệ (www.codeproject.com/KB/cpp/psexplorer.aspx ).

Thông tin trong Lưu trữ được bảo vệ có thể hữu ích trong các trường hợp liên quan đến quyền truy cập vào các trang web và sử dụng mật khẩu cho các dịch vụ như Hotmail và MSN.

Thông tin trong Protected Storage cũng hữu ích cho kẻ xấu. Tôi đã thấy các hệ thống bị nhiễm IRCbots (phần mềm độc hại, sau khi được cài đặt, kết nối với kênh IRC đang chờ lệnh; nhà điều hành kênh có thể đưa ra một lệnh sau đó được thực thi bởi hàng ngàn bot) sẽ gửi thông tin từ Lưu trữ được bảo vệ đến xấu chàng trai, chỉ huy. Vào ngày 19 tháng 2 năm 2006, Brian Krebs đã xuất bản một bài báo (www.washingtonpost.com/wpdyn/content/article/2006/02/14/AR2006021401342.html) trên Tạp chí Washington Post về một hacker đã viết phần mềm bot và kiểm soát hàng ngàn hệ thống. Trong bài viết đó, Brian đã viết rằng hacker có thể gõ một lệnh (pstore) và lấy thông tin Lưu trữ được bảo vệ từ tất cả các hệ thống bị nhiễm, bao gồm cả kết hợp tên người dùng và mật khẩu cho các tài khoản PayPal, eBay, Bank of America và Citibank. như đối với các tài khoản e-mail của quân đội và chính phủ liên bang.

Thông tin được lưu giữ bởi Dịch vụ lưu trữ được bảo vệ có sẵn thông qua chức năng AutoComplete được tích hợp trong trình duyệt Internet Explorer Web. Cài đặt AutoComplete, được hiển thị trong Hình 1.13, có sẵn bằng cách nhấp vào Công cụ trong thanh menu Internet Explorer và sau đó chọn Tùy chọn Internet | Nội dung, và sau đó nhấp vào nút Tự động hoàn thành.

Khi AutoComplete được bật, người dùng của các hệ thống bị nhiễm này đã sử dụng Internet Explorer để truy cập vào tài khoản ngân hàng và mua sắm trực tuyến của họ, để chúng có sẵn cho kẻ tấn công như tin tặc trong bài viết của Brian.

**Figure 13:AutoComplete Settings Dialog Box on Internet Explorer 6.0**



Các công cụ như PassView (www.nirsoft.net/utils/pspv.html) và Trình bảo vệ lưu trữ được bảo vệ (www.forensicideas.com/tools.html) cho phép bạn xem thông tin lưu trữ được bảo vệ theo định dạng GUI đẹp và pstoreview.exe (www.ntsecurity.nu/toolbox/pstoreview) là một công cụ CLI sẽ cung cấp thông tin tương tự cho STDOUT. Bạn có thể cần thu thập thông tin này trong quá trình điều tra, đặc biệt nếu sự cố mà bạn xử lý liên quan đến việc người dùng truy cập các trang web yêu cầu mật khẩu. Bạn có thể trích xuất thông tin này từ một hình ảnh thu được, nhưng làm như vậy đòi hỏi các công cụ đặc biệt để giải quyết việc giải mã, các công cụ có thể tốn kém. Có thể có các tình huống phản hồi trực tiếp (ví dụ: đánh cắp hoặc thoát dữ liệu, người mất tích, v.v.) trong đó bạn sẽ muốn thu thập thông tin này từ hệ thống một cách nhanh chóng, thay vì chờ đợi cho đến khi hình ảnh được lấy và dữ liệu được đưa đến phòng thí nghiệm để khai thác và phân tích.

## **Event Logs**

Nhật ký sự kiện về cơ bản là các tệp trong hệ thống tệp, nhưng chúng có thể thay đổi. Trên thực tế, tùy thuộc vào cách họ cấu hình và sự kiện nào đang được kiểm toán, họ có thể thay đổi khá nhanh.

Tùy thuộc vào cách các chính sách kiểm toán được định cấu hình trên hệ thống nạn nhân của Cameron và cách bạn truy cập nó như là phản hồi đầu tiên, các mục có thể được tạo trong Nhật ký sự kiện. Ví dụ: nếu bạn quyết định chạy các lệnh chống lại hệ thống từ một địa điểm từ xa (nghĩa là hệ thống ở trong một tòa nhà khác hoặc thành phố khác và bạn không thể truy cập nhanh nhưng bạn muốn giữ lại một số dữ liệu) và kiểm toán thích hợp cấu hình đã sẵn sàng, Nhật ký sự kiện bảo mật sẽ chứa các mục nhập cho mỗi lần bạn đăng nhập. Nếu đủ các mục này được tạo, bạn có thể sẽ mất thông tin có giá trị liên quan đến cuộc điều tra của mình. Các công cụ như psloglist.exe và dumpevt.exe có thể được sử dụng để truy xuất các bản ghi sự kiện hoặc chính các tệp .evt có thể được sao chép khỏi hệ thống (điều này phụ thuộc vào mức độ truy cập và quyền của tài khoản được sử dụng). Một cuộc thảo luận chi tiết về phân tích các tệp Nhật ký Sự kiện của Windows sẽ được cung cấp trong Chương 5.

Tại thời điểm này, bạn có thể đang nghĩ rằng Okay Okay, với tất cả các công cụ và tiện ích này, tôi có một sự cố trên tay. Tôi cần thu thập dữ liệu nào để giải quyết vấn đề này? Câu trả lời về cổ phiếu là phụ thuộc vào nó. Tôi biết đó có thể không phải là câu trả lời bạn muốn nghe, nhưng hãy để tôi giải thích, nếu giải thích câu trả lời đó, chúng ta có thể xây dựng sự hiểu biết tại sao đó là phản ứng.

Dữ liệu dễ bay hơi hữu ích nhất cho cuộc điều tra của bạn tùy thuộc vào loại sự cố mà bạn gặp phải. Ví dụ: một sự cố liên quan đến xâm nhập từ xa hoặc cửa hậu Trojan thường có nghĩa là quá trình, kết nối mạng và thông tin từ quy trình đến chân dung (và có lẽ cả nội dung của các khóa Registry nhất định) sẽ có giá trị nhất đối với bạn. Tuy nhiên, nếu một nhân viên trong môi trường công ty bị nghi ngờ đã đánh cắp dữ liệu độc quyền của công ty hoặc vi phạm chính sách sử dụng được chấp nhận của công ty (AUP), thông tin về các thiết bị lưu trữ được kết nối với hệ thống của anh ta, lịch sử duyệt web, nội dung của Clipboard, v.v. có thể có giá trị hơn cho cuộc điều tra của bạn.

Chìa khóa cho tất cả những điều này là để biết thông tin nào có sẵn cho cuộc điều tra của bạn, cách bạn có thể truy xuất thông tin đó và cách bạn có thể sử dụng thông tin đó. Khi bạn bắt đầu xem xét các loại sự cố khác nhau và thông tin bạn cần để giải quyết chúng, bạn sẽ bắt đầu thấy trùng lặp giữa các công cụ khác nhau mà bạn sử dụng và dữ liệu mà bạn quan tâm để điều tra. Mặc dù bạn có thể không phát triển một kích thước của một người phù hợp với tất cả các tệp bó của hay chạy tất cả các lệnh bạn muốn sử dụng cho mọi cuộc điều tra, bạn có thể quyết định rằng có một số tệp bó nhỏ hơn (hoặc các tệp cấu hình cho Dự án máy chủ pháp y, được mô tả sau đó trong chương) là một cách tiếp cận tốt hơn. Bằng cách đó, bạn chỉ có thể thu thập thông tin bạn cần cho mỗi tình huống.

## **Devices and Other Information**

Bạn có thể chọn thu thập các loại thông tin khác từ một hệ thống có thể không dễ mất về bản chất, nhưng bạn muốn ghi lại nó cho mục đích tài liệu. Ví dụ, có lẽ bạn muốn biết điều gì đó về ổ cứng được cài đặt trong hệ thống. Di.pl là tập lệnh Perl thực hiện WMI để liệt kê các ổ đĩa khác nhau được gắn vào hệ thống cũng như thông tin phân vùng. Ldi.pl triển khai WMI để thu thập thông tin về các ổ đĩa logic (C: \, D: \, v.v.), bao gồm các ổ đĩa cố định cục bộ, thiết bị lưu trữ di động và chia sẻ từ xa. Sr.pl liệt kê thông tin về Điểm khôi phục hệ thống trên các hệ thống Windows XP (bạn có thể tìm thêm thông tin về Điểm khôi phục hệ thống trong Chương 4 và 5).

DevCon, có sẵn từ Microsoft, có thể được sử dụng để ghi lại các thiết bị được gắn vào hệ thống Windows. Thay thế CLI cho Trình quản lý thiết bị, DevCon có thể hiển thị các lớp thiết bị khả dụng cũng như trạng thái của các thiết bị được kết nối.

## **A Word about Picking Your Tools**

Trong chương này cũng như các chương khác trong cuốn sách này, chúng tôi đề cập đến các công cụ khác nhau mà bạn có thể sử dụng để thực hiện các tác vụ nhất định. Cuốn sách này không nhằm mục đích như một danh sách tất cả và cuối cùng của tất cả các công cụ điều đó đơn giản là không thể. Thay vào đó, những gì tôi cố gắng làm là làm cho bạn biết nơi bạn cần tìm và chỉ cho bạn những cách mà bạn có thể thu thập dữ liệu bạn cần cho các cuộc điều tra của mình. Đôi khi, nó chỉ đơn giản là vấn đề biết rằng thông tin có ở đó.

Khi chúng tôi thu thập dữ liệu từ các hệ thống trực tiếp, chúng tôi thường sẽ phải tương tác với chính hệ điều hành, sử dụng API có sẵn. Các công cụ khác nhau có thể sử dụng các lệnh gọi API khác nhau để thu thập cùng một thông tin.

Nó luôn luôn là một ý tưởng tốt để biết cách các công cụ của bạn thu thập thông tin. Những lệnh gọi API nào thực thi sử dụng? DLL nào nó truy cập? Dữ liệu được hiển thị như thế nào và dữ liệu đó so với các công cụ khác có tính chất tương tự như thế nào?

Kiểm tra các công cụ của bạn để xác định các hiệu ứng họ có trên một hệ thống trực tiếp. Họ có để lại bất kỳ hiện vật nào trên hệ thống không? Nếu vậy, chúng là gì? Hãy chắc chắn ghi lại các thành phần này vì tài liệu này cho phép bạn xác định (và tài liệu) các bước bạn thực hiện để giảm thiểu tác động của việc sử dụng và chứng minh việc sử dụng các công cụ này. Ví dụ: Windows XP thực hiện tìm nạp trước ứng dụng, nghĩa là khi bạn chạy một ứng dụng, một số thông tin về ứng dụng đó (ví dụ: các trang mã) được lưu trữ trong tệp .pf nằm trong thư mục% WINDIR% \ Prefetch. Thư mục này có giới hạn 128 tệp .pf. Nếu bạn đang thực hiện các hoạt động ứng phó sự cố và có ít hơn 128 tệp .pf trong thư mục này, một trong những các công cụ bạn chạy trên hệ thống sẽ là các tệp .pf cho các công cụ đó sẽ được thêm vào thư mục Prefetch. Trong hầu hết các trường hợp, điều này có thể không phải là một vấn đề. Tuy nhiên, hãy để nói rằng phương pháp của bạn bao gồm sử dụng nc.exe (netcat). Nếu ai đó đã sử dụng nc.exe trên hệ thống, việc bạn sử dụng bất kỳ tệp nào có tên đó sẽ có tác dụng ghi đè tệp .pf hiện tại cho nc.exe, có khả năng hủy bằng chứng (ví dụ: sửa đổi thời gian hoặc dữ liệu MAC trong tệp , chẳng hạn như đường dẫn đến hình ảnh thực thi).

Thực hiện kiểm tra và xác nhận công cụ của riêng bạn có vẻ như là một nhiệm vụ khó khăn. Rốt cuộc, ai muốn chạy qua một quy trình kiểm tra công cụ cho mọi công cụ? Chà, bạn có thể phải làm thế, bởi vì rất ít trang web cung cấp loại thông tin này cho các công cụ của họ; hầu hết người sói ban đầu được viết để sử dụng cho phản ứng sự cố hoặc pháp y máy tính. Tuy nhiên, khi bạn đã có khung (công cụ, quy trình, v.v.) của mình, nó thực sự không khó lắm, và có một số điều đơn giản bạn có thể làm để ghi lại và kiểm tra các công cụ bạn sử dụng. Tài liệu và kiểm tra các công cụ của bạn rất giống với kiểm tra hoặc phân tích chương trình phần mềm độc hại bị nghi ngờ, một chủ đề được đề cập chi tiết trong Chương 6.

Các bước cơ bản của tài liệu công cụ của bạn bao gồm kiểm tra tĩnh và động. Kiểm tra tĩnh bao gồm ghi lại thông tin nhận dạng duy nhất về công cụ, chẳng hạn như:

* Nơi bạn nhận được nó (URL)
* Kích thước tệp
* Băm mật mã cho tệp, sử dụng các thuật toán đã biết
* Lấy thông tin từ tệp, chẳng hạn như các tiêu đề thực thi di động (PE), thông tin phiên bản tệp, bảng nhập / xuất, v.v.

Thông tin này dễ dàng truy xuất bằng các công cụ dòng lệnh và ngôn ngữ kịch bản lệnh như Perl và toàn bộ quy trình thu thập (cũng như lưu trữ thông tin trong cơ sở dữ liệu, bảng tính hoặc tệp phẳng) dễ dàng tự động hóa.

## **Live-Response Methodologies**

Khi bạn thực hiện phản hồi trực tiếp, phương pháp hoặc quy trình thực tế bạn sử dụng để truy xuất dữ liệu từ các hệ thống có thể khác nhau, tùy thuộc vào một số yếu tố. Là một chuyên gia tư vấn và ứng phó khẩn cấp, tôi thấy rằng tốt nhất nên hiểu đầy đủ về những gì có sẵn và những gì có thể đi vào bộ công cụ của bạn (xem xét các vấn đề liên quan đến việc mua phần mềm, cấp phép và các khoản phí và hạn chế khác) và sau đó quyết định những gì hoạt động dựa trên tình hình

Có hai phương pháp cơ bản để thực hiện phản hồi trực tiếp trên hệ thống Windows: Địa phương và từ xa.

**Local Response Methodology**

Thực hiện phản hồi trực tiếp cục bộ có nghĩa là bạn đang ngồi trên bàn điều khiển của hệ thống, nhập lệnh trên bàn phím và lưu thông tin cục bộ, trực tiếp vào ổ cứng hoặc vào ổ đĩa di động (ổ USB, ổ đĩa ngoài được kết nối USB) hoặc tài nguyên mạng ( chia sẻ mạng) xuất hiện dưới dạng tài nguyên cục bộ. Điều này được thực hiện rất thường xuyên trong các tình huống mà bộ phản hồi có quyền truy cập vật lý ngay lập tức vào hệ thống và các công cụ của cô ấy trên ổ đĩa CD hoặc ngón tay cái. Thu thập thông tin cục bộ từ một số hệ thống thường có thể nhanh hơn nhiều so với việc định vị kết nối mạng hoặc truy cập mạng không dây. Với dung lượng lưu trữ ngoài thích hợp và mức độ truy cập phù hợp, bộ phản hồi đầu tiên có thể thu thập nhanh chóng và hiệu quả các thông tin cần thiết. Để tiếp tục tối ưu hóa các hoạt động của mình, bộ phản hồi đầu tiên có thể có tất cả các công cụ của cô ấy được ghi vào CD và được quản lý thông qua tệp bó hoặc một loại tập lệnh nào đó cho phép phạm vi linh hoạt hạn chế (ví dụ: thiết bị lưu trữ được kết nối USB được ánh xạ sang khác ký tự ổ đĩa, cài đặt Windows nằm trên ổ D: \, v.v.).

Cách đơn giản nhất để thực hiện phương pháp cục bộ là với một tệp bó. Tôi có xu hướng thích các tệp bó và tập lệnh Perl vì thay vì lặp đi lặp lại các lệnh tương tự (và lặp đi lặp lại lỗi), tôi có thể viết các lệnh một lần và để chúng tự động chạy. Một ví dụ về một tệp bó đơn giản mà bạn có thể sử dụng trong phản hồi trực tiếp trông như thế này:

tlist.exe –c > %1\tlist-c.log

tlist.exe –t > %1\tlist-t.log

tlist.exe –s > %1\tlist-s.log tcpvcon.exe –can > %1\tcpvcon-can.log netstat.exe –ano > %1\netstat-ano.log

Có bạn đi ba tiện ích và năm lệnh đơn giản. Lưu tệp này dưới dạng local.bat và đưa nó vào đĩa CD, cùng với các bản sao của các công cụ liên quan. Bạn cũng có thể muốn thêm vào các bản sao CD đáng tin cậy của bộ xử lý lệnh (cmd.exe) cho mỗi hệ điều hành. Trước khi bạn khởi chạy tệp bó, hãy xem hệ thống và xem mạng nào có sẵn hoặc chèn ổ USB vào hệ thống và xem ký tự ổ đĩa nào nhận được (giả sử F: \), sau đó chạy tệp bó như vậy (ổ D: \ là ổ đĩa CD-ROM):

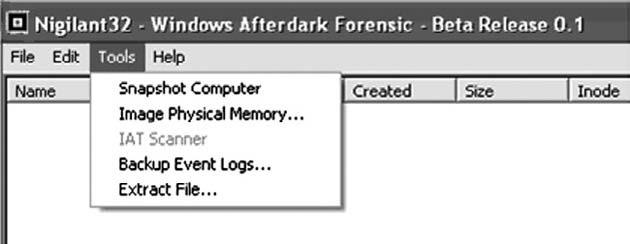
*D: \> local.bat F:*

Khi tệp bó hoàn tất, bạn sẽ có năm tệp trên ổ ngón tay cái của mình. Tất nhiên, bạn có thể thêm nhiều loại lệnh khác nhau vào tệp bó, tùy thuộc vào độ rộng của dữ liệu bạn muốn truy xuất từ ​​hệ thống.

Một số ví dụ có sẵn miễn phí về bộ công cụ đã được thiết kế để được sử dụng theo kiểu phản ứng cục bộ; trong số đó là Báo cáo Bộ sưu tập Phản hồi Sự cố (IRCR; cho đến Phiên bản 2.3 tại thời điểm viết bài này và có sẵn tại http://tools.ph Phantombyte.com/) và Windows Forensic Toolchest (WFT, có sẵn từ www.foolmoon.net /security/wft/index.html và được tạo bởi Monty McDougal). Mặc dù chúng khác nhau về cách triển khai và đầu ra, nhưng chức năng cơ bản của cả hai bộ công cụ về cơ bản là giống nhau: Chạy các tệp thực thi bên ngoài được kiểm soát bởi tệp bó Windows và lưu cục bộ đầu ra. WFT thực hiện công việc tuyệt vời là lưu dữ liệu thô và cho phép người trả lời gửi đầu ra của các lệnh tới các báo cáo HTML.

Một cách tiếp cận khác để phát triển phương pháp phản hồi cục bộ là gói gọn càng nhiều càng tốt vào một ứng dụng bằng API Windows, đó là những công cụ như Nigilant32 từ Agile Risk Management LLC (www.agilerm.net, đã được tích hợp vào Phản hồi F tại www.f-response.com) cố gắng đạt được. Nigilant32 sử dụng các lệnh gọi API Windows tương tự được sử dụng bởi các tiện ích bên ngoài để thu thập thông tin dễ bay hơi từ một hệ thống (xem Hình 1.14) và có thêm khả năng thực hiện kiểm tra hệ thống tệp và bỏ nội dung của bộ nhớ vật lý (RAM).

**Figure 14:Nigilant32 GUI**



Điều thú vị về các bộ công cụ kiểu tập tin hàng loạt là rất nhiều người có chúng. Khi tôi ở một địa điểm của khách hàng hoặc một cuộc hội thảo, nhiều lần tôi sẽ nói chuyện với những người quan tâm đến việc so sánh cách tiếp cận của họ với những người khác. Một số đã bao gồm các công cụ mà tôi đã liệt kê trong Chương 5 của cuốn sách đầu tiên của tôi, Windows Forensics và Phục hồi sự cố, hoặc họ đã đọc về các công cụ khác và kết hợp chúng vào bộ công cụ của họ. Thật kỳ lạ, khi nó thực sự đi vào nó, có rất nhiều sự chồng chéo giữa các bộ công cụ này. Kiểu tệp bó sử dụng các tệp thực thi sử dụng các lệnh gọi API Windows tương tự (hoặc tương tự) như các công cụ khác như Nigilant32.

Nhiều công cụ chúng tôi đã thảo luận ở đây (WFT, Nigilant32 và thậm chí nhiều công cụ CLI) cũng có sẵn như là một phần của bản phân phối Helix do Drew Fahey kết hợp và có sẵn thông qua trang web e-Fense (www.e- fense.com/rcix/). Helix bao gồm một mặt Linux có khả năng khởi động của CD, cũng như phía phản hồi trực tiếp của Windows và được nhiều người tìm thấy là cực kỳ hữu ích.

**Remote Response Methodology**

Phương pháp phản hồi từ xa thường bao gồm một loạt các lệnh được thực thi đối với một hệ thống từ khắp mạng. Phương pháp này rất hữu ích trong các tình huống với nhiều hệ thống, bởi vì quá trình đăng nhập vào hệ thống và chạy các lệnh rất dễ tự động hóa. Trong giới bảo mật, chúng tôi gọi đây là khả năng mở rộng. Một số công cụ chạy rất tốt khi được sử dụng kết hợp với psexec.exe từ Sysi INTERNals.com và có thể dễ dàng thu thập thông tin bổ sung thông qua việc sử dụng WMI. Bất kể cách tiếp cận nào bạn thực hiện, hãy nhớ rằng (a) bạn sẽ cần thông tin đăng nhập cho mỗi hệ thống và (b) mỗi khi bạn đăng nhập để chạy lệnh và thu thập đầu ra, bạn sẽ thêm một mục vào Nhật ký sự kiện bảo mật (với điều kiện mức độ kiểm toán thích hợp đã được bật). Hãy ghi nhớ điều đó, chúng tôi thấy rằng thứ tự biến động đã thay đổi phần nào, vì vậy tôi khuyên rằng lệnh đầu tiên bạn sử dụng là lệnh để thu thập nội dung của Nhật ký sự kiện bảo mật.

Bạn có thể sử dụng tệp bó Windows làm cơ sở để thực hiện phương pháp này. Lấy ba đối số tại dòng lệnh (tên hoặc IP của hệ thống và thông tin đăng nhập tên người dùng / mật khẩu), bạn có thể dễ dàng tạo ra một loạt các lệnh để thu thập thông tin cần thiết. Bạn sẽ cần phải thực thi một số lệnh bằng cách sử dụng psexec.exe, nó sẽ sao chép tệp thực thi vào hệ thống từ xa, chạy nó và cho phép bạn thu thập đầu ra từ đầu ra tiêu chuẩn (STDOUT) hoặc chuyển hướng đầu ra sang một tệp, như thể bạn đang chạy cùng một lệnh cục bộ. Các lệnh khác sẽ lấy đường dẫn UNC (tên của hệ thống được đặt trước ) và thông tin đăng nhập làm đối số, vì vậy bạn sẽ không cần sử dụng psexec.exe. Cuối cùng, bạn có thể triển khai WMI thông qua VBScript hoặc Perl để thu thập dữ liệu. Microsoft cung cấp kho lưu trữ tập lệnh (www.microsoft.com/technet/scriptcenter/default.mspx) với nhiều ví dụ về mã WMI được triển khai bằng nhiều ngôn ngữ khác nhau để bao gồm Perl, giúp thiết kế bộ công cụ tùy chỉnh theo quy trình cắt và dán.

CSV (để mở trong Excel hoặc phân tích cú pháp bằng Perl) hoặc thậm chí là bảng HTML. Sử dụng các công tắc bổ sung như / Node:, / Người dùng:, và / Mật khẩu:, bạn có thể bao gồm một số lệnh wmic.exe trong một tệp bó và thu thập phạm vi dữ liệu rộng hơn từ các hệ thống từ xa. Hơn nữa, quản trị viên có thể sử dụng các lệnh này để biên dịch danh sách kiểm kê phần cứng và phần mềm, xác định các hệ thống cần được cập nhật bằng các bản vá và hơn thế nữa. WMI là một giao diện mạnh mẽ vào chính các hệ thống Windows được quản lý và wmic.exe cung cấp quyền truy cập dễ dàng để tự động hóa các lệnh.

Với việc xử lý và phục hồi lỗi đúng cũng như đăng nhập hoạt động trong mã, đây có thể là một cách hiệu quả và có thể mở rộng để nhanh chóng thu thập thông tin từ một số hệ thống, tất cả được quản lý và lưu trữ ở một vị trí trung tâm. Phản hồi sự cố ProDiscover (IR) từ Đường dẫn công nghệ (www.techpathways.com) là một công cụ thương mại thực hiện phương pháp này. Người trả lời có thể cài đặt một tác nhân từ một vị trí trung tâm, truy vấn tác nhân để biết thông tin có sẵn và sau đó xóa tác nhân. Nhờ có API ProScript dựa trên ProDiscover, Perl, bộ phản hồi có thể tự động hóa toàn bộ quá trình. Cách tiếp cận này giảm thiểu số lượng đăng nhập sẽ xuất hiện trong Nhật ký sự kiện bảo mật cũng như số lượng phần mềm cần được cài đặt trên hệ thống từ xa. ProDiscover IR có thêm khả năng truy xuất nội dung của bộ nhớ vật lý (kể từ khi viết bài này, từ các hệ thống Windows 2000, XP và 2003, nhưng không phải từ Windows 2003 SP1 trở lên) cũng như thực hiện việc mua lại ổ cứng trực tiếp thông qua mạng.

Một công cụ khác phải được đề cập là Phản hồi F (www.f-response.com), được thiết kế và phát triển bởi Matt Shannon (Matt bắt đầu với Nigilant32 từ www.agilerm.net). Mặc dù F-Feedback không phải là loại công cụ tương tự như ProDiscover IR hoặc các công cụ phản hồi trực tiếp dựa trên tác nhân hoặc truy cập từ xa khác hiện có, nhưng không nghi ngờ gì, nó đã thay đổi diện mạo phản ứng sự cố như chúng ta biết Mô tả ngắn về Phản hồi F là nó cung cấp cho bạn quyền truy cập từ xa, chỉ đọc vào một ổ cứng cứng hệ thống từ xa. Có ba phiên bản Phản hồi F (Bộ công cụ, Tư vấn và Doanh nghiệp) và tất cả chúng đều hoạt động theo cùng một cách; sau khi cài đặt và định cấu hình tác nhân trên hệ thống từ xa, bạn có thể truy cập ổ đĩa từ xa đó dưới dạng ổ đĩa cục bộ chỉ đọc trên máy trạm của bạn. Điều này hoạt động trên mạng cục bộ, giữa các tòa nhà (bên kia đường hoặc ở một phần khác của thành phố), đến một trung tâm dữ liệu từ xa ... bất cứ nơi nào bạn có kết nối mạng TCP / IP. Tác nhân F-Feedback có sẵn để chạy trên các hệ thống Linux, Mac OS X và Windows và trên các hệ thống Windows (kể từ Phiên bản 2.03), bộ nhớ vật lý của hệ thống sẽ xuất hiện trên hệ thống cục bộ của bạn dưới dạng ổ đĩa ảo. Về bản chất, F-Feedback cung cấp cho bạn cơ chế không biết công cụ (bạn có thể sử dụng bất kỳ công cụ nào bạn muốn để có được hình ảnh của ổ đĩa từ xa) để thực hiện các hoạt động phản hồi. Mặc dù Phản hồi F không cho phép bạn, chạy tlist.exe và nhận danh sách quy trình từ hệ thống từ xa, nhưng nó cung cấp cho bạn phương tiện để dễ dàng lấy nội dung của RAM, một chủ đề mà chúng ta sẽ thảo luận kỹ trong Chương 3. Phương tiện đi kèm với cuốn sách này chứa tài liệu PDF mô tả chi tiết về cách cài đặt F-Feedback Enterprise Edition (EE) từ xa; Hóa ra, đây cũng là một phương pháp lén lút triển khai F-Feedback EE. Tài liệu này cũng có sẵn tại trang web F-Feedback cho người dùng đã đăng ký sản phẩm F-Feedback.

Hạn chế của phương pháp phản hồi từ xa là bộ phản hồi phải có khả năng truy cập và, trong một số trường hợp, đăng nhập vào hệ thống qua mạng. Nếu đăng nhập kiểu Windows (thông qua NetBIOS) đã bị hạn chế theo một cách nào đó (NetBIOS không được cài đặt, tường lửa / bộ định tuyến chặn các giao thức hoặc tương tự), phương pháp này sẽ không hoạt động.

# **TÓM LƯỢC**

Trong chương này, chúng tôi đã xem xét phản hồi trực tiếp, cụ thể là thu thập thông tin dễ mất (và một số không dễ mất) từ các hệ thống Windows trực tiếp. Như chúng ta đã thảo luận, các hệ thống trực tiếp chứa rất nhiều dữ liệu mà chúng ta có thể sử dụng để tăng cường hiểu biết về một sự cố; chúng ta chỉ cần thu thập dữ liệu đó trước khi loại bỏ nguồn điện khỏi hệ thống để có thể thu được hình ảnh của ổ cứng. Chúng tôi cũng thảo luận về cách thay đổi trong bối cảnh điện toán đang ngày càng đưa ra cho chúng tôi các tình huống trong đó lựa chọn khả thi duy nhất của chúng tôi là thu thập dữ liệu dễ bay hơi.

Ý định của tôi trong chương này là không cung cấp cho bạn cách tiếp cận thực hành tốt nhất của YouTube để thu thập dữ liệu dễ bay hơi, vì thực tế đơn giản là có một cách khác. Ý định của tôi là cung cấp cho bạn đủ thông tin dựa trên nhu cầu của bạn và các điều kiện của tình huống bạn gặp phải, bạn không chỉ có thể sử dụng các thực tiễn tốt nhất của riêng mình, mà còn khi tình hình thay đổi, sử dụng và biện minh cho việc sử dụng thực hành tốt hơn.

Tất cả các tập lệnh Perl được đề cập và mô tả trong chương này đều có sẵn trên các phương tiện đi kèm, cùng với một tập lệnh thực thi độc lập được biên dịch với Perl2Exe. ProScripts for Technology Pathways Sản phẩm ProDiscover cũng có sẵn trên các phương tiện đi kèm nhưng chỉ được cung cấp dưới dạng tập lệnh Perl.

**Giải pháp theo dõi nhanh**

**Phản hồi trực tiếp**

* Nguyên tắc trao đổi Locard từ nói rằng khi hai vật thể tiếp xúc với nhau, vật chất được trao đổi giữa chúng. Quy tắc này cũng liên quan đến lĩnh vực kỹ thuật số.
* Bất cứ điều gì một điều tra viên làm trên một hệ thống sống, thậm chí không có gì, sẽ có ảnh hưởng đến hệ thống và để lại một vật phẩm. Các tạo phẩm sẽ được tạo trên hệ thống khi nó chạy mà không có sự tương tác từ người dùng.
* Sự vắng mặt của một cổ vật mà người ta mong đợi chính nó là một vật phẩm.
* Thứ tự biến động minh họa cho chúng ta rằng một số dữ liệu có thời gian sử dụng ngắn hơn hoặc thời gian sử dụng ngắn hơn nhiều so với các dữ liệu khác.
* Khi chúng tôi thực hiện phản ứng sự cố, dữ liệu dễ bay hơi nhất phải được thu thập trước.
* Nhu cầu thực hiện phản hồi trực tiếp cần được hiểu rõ và ghi lại.
* Nếu không có sự chú ý thích hợp được thực hiện để thực hiện phản hồi trực tiếp, một tổ chức có thể gặp rủi ro lớn hơn bởi các hoạt động ứng phó sự cố so với chính sự cố được đặt ra.
* Chính sách bảo mật của công ty có thể nói rằng phản hồi trực tiếp là bước đầu tiên trong một cuộc điều tra. Người trả lời phải cẩn thận tuân theo các quy trình được lập thành tài liệu và ghi lại hành động của họ

**Dữ liệu cần thu thập**

* Rất nhiều dữ liệu có thể cung cấp cho điều tra viên cái nhìn sâu sắc về trường hợp của cô ấy có sẵn trên hệ thống trong khi nó được cấp nguồn và chạy, và một số dữ liệu đó chỉ khả dụng trong một thời gian giới hạn.
* Nhiều lần, dữ liệu dễ bay hơi mà bạn thu thập từ một hệ thống sẽ phụ thuộc vào loại điều tra hoặc sự cố mà bạn đã trình bày.
* Khi thu thập dữ liệu dễ bay hơi, bạn cần lưu ý cả thứ tự biến động từ RFC 3227 và Nguyên tắc trao đổi Locard.
* Key Chìa khóa để thu thập dữ liệu dễ bay hơi và sử dụng dữ liệu đó để hỗ trợ điều tra là tài liệu kỹ lưỡng.

**Thông tin không biến đổi**

* Thông tin không biến đổi (như cài đặt hệ thống) có thể ảnh hưởng đến cuộc điều tra của bạn, vì vậy bạn có thể cần thu thập dữ liệu đó như một phần của phản hồi trực tiếp của mình.
* Một số dữ liệu không dễ biến đổi mà bạn thu thập có thể ảnh hưởng đến quyết định của bạn để tiếp tục phản hồi trực tiếp, giống như nó có thể ảnh hưởng đến quyết định của bạn trong việc thực hiện một cuộc điều tra sau khi thực hiện.
* Thông tin không dễ biến đổi bạn chọn để thu thập trong khi phản hồi trực tiếp phụ thuộc vào các yếu tố như cơ sở hạ tầng mạng, chính sách bảo mật và phản hồi sự cố hoặc cấu hình hệ thống.

**Phương pháp phản hồi trực tiếp**

* Có ba phương pháp phản hồi trực tiếp cơ bản: cục bộ, từ xa và kết hợp cả hai. Biết các tùy chọn bạn có sẵn và có triển khai các tùy chọn đó sẽ tăng tính linh hoạt của bạn để thu thập thông tin.
* Phương pháp bạn sử dụng sẽ phụ thuộc vào các yếu tố như cơ sở hạ tầng mạng, các tùy chọn triển khai của bạn và thậm chí có thể là cấu trúc chính trị của tổ chức của bạn. Tuy nhiên, bạn có nhiều tùy chọn có sẵn.
* Khi chọn phương pháp phản hồi của bạn, hãy lưu ý đến thực tế rằng hành động của bạn sẽ để lại các tạo tác trên hệ thống. Hành động của bạn sẽ là tác nhân kích thích trực tiếp trên hệ thống, điều này sẽ gây ra những thay đổi xảy ra trong trạng thái của hệ thống, vì các khóa Registry có thể được thêm vào (xem Chương 4 về các thiết bị lưu trữ di động được kết nối USB), các tệp có thể được thêm hoặc sửa đổi và hình ảnh thực thi sẽ được tải vào bộ nhớ. Tuy nhiên, những thay đổi này, ở một mức độ, có thể định lượng được, và bạn nên ghi chép lại kỹ lưỡng phương pháp và hành động của mình.

**Các câu hỏi thường gặp**

**Hỏi:** Khi nào tôi nên thực hiện phản hồi trực tiếp?

**Trả lời**: Không có quy tắc cứng và nhanh nào nêu rõ khi nào bạn nên thực hiện phản hồi trực tiếp. Tuy nhiên, khi ngày càng có nhiều cơ quan quản lý (xem xét các quy tắc của SEC, HIPAA, FISMA, Visa PCI và các cơ quan khác) chỉ định các biện pháp và cơ chế bảo mật sẽ được sử dụng cũng như các câu hỏi cần được giải quyết và trả lời (là thông tin nhạy cảm cá nhân truy cập?), phản ứng trực tiếp trở nên quan trọng hơn.

**Hỏi:** Tôi đã tham gia vào một trường hợp, sau khi tất cả đã được nói và thực hiện, hệ thống phòng thủ Trojan Trojan đã được sử dụng. Làm thế nào phản ứng trực tiếp đã giúp hoặc chuẩn bị chúng tôi để giải quyết vấn đề này?

**Trả lời:** Bằng cách thu thập thông tin về các quy trình chạy trên hệ thống, kết nối mạng và các khu vực khác mà bạn đã tìm thấy các tạo phẩm Trojan hoặc cửa sau, bạn sẽ có thể loại trừ liệu những thứ đó có chạy trong khi hệ thống đang hoạt động hay không. Cuộc điều tra sau khi chết của bạn sẽ bao gồm kiểm tra hệ thống tệp, bao gồm các tác vụ theo lịch trình và tương tự, để xác định khả năng Trojan được cài đặt, nhưng thu thập dữ liệu dễ bay hơi từ hệ thống trực tiếp sẽ cung cấp cho bạn thông tin cần thiết để xác định xem Trojan có chạy vào thời điểm bạn đang ở trước hệ thống.

**Hỏi:** Tôi không làm phản hồi trực tiếp bây giờ. Tại sao tôi nên bắt đầu?

**Trả lời:** Thông thường, một tổ chức sẽ chọn sử dụng tâm lý xóa sạch và tải lại, trong đó quản trị viên sẽ xóa ổ cứng của hệ thống được cho là bị xâm nhập, sau đó tải lại hệ điều hành từ phương tiện sạch, cài đặt lại ứng dụng và tải dữ liệu trở lại hệ thống từ bản sao lưu. Đây được cho là phương pháp ít tốn kém nhất. Tuy nhiên, cách tiếp cận này không có gì để xác định sự cố xảy ra như thế nào ở nơi đầu tiên. Một số người có thể nói rằng, tôi đã cài đặt lại hệ điều hành và cập nhật tất cả các bản vá lỗi, và điều đó thật tuyệt vời, nhưng không phải tất cả các sự cố đều xảy ra vì muốn có một bản vá hoặc hotfix. Đôi khi, nó đơn giản như một mật khẩu yếu hoặc không tồn tại trên tài khoản người dùng hoặc ứng dụng (như mật khẩu sa trên SQL Server) hoặc dịch vụ được cấu hình kém. Không có số lượng bản vá sẽ khắc phục các loại vấn đề. Không xác định cách xảy ra sự cố và giải quyết sự cố, sự cố có thể xảy ra lần nữa và theo thứ tự khá ngắn sau khi hệ thống sạch, mới, sáng sủa được kết nối lại với mạng. Ngoài ra, như tôi đã trình bày trong suốt chương này, rất nhiều thông tin có giá trị có sẵn khi hệ thống vẫn đang chạy các thông tin về bộ nhớ như bộ nhớ vật lý, quy trình chạy, kết nối mạng và nội dung của Clipboard, có thể có tác động đáng kể về cuộc điều tra của bạn.