

BAN CƠ YẾU CHÍNH PHỦ
HỌC VIỆN KỸ THUẬT MẬT MÃ



PHÒNG CHỐNG VÀ ĐIỀU TRA TỘI PHẠM MÁY TÍNH

**ĐỀ TÀI: DỊCH TÀI LIỆU WINDOWS FORENSICS
ANALYSIS CHAPTER 9**

Hà Nội, 2019

Mục lục

Chapter 9: Performing Analysis on a Budget

Đôi khi, các ứng dụng forensic bản thương mại (full tính năng) không phù hợp để sử dụng trong phân tích. Chúng có thể thiếu một số chức năng cần thiết hoặc chức năng bạn cần có thể quá cồng kềnh, phức tạp để có được. Do đó, giải pháp là ta không nên chi hàng ngàn đô la cho các ứng dụng thương mại bổ sung khi một công cụ có sẵn miễn phí (hoặc chi phí thấp) sẽ là quá đủ. Mục tiêu của chương này là chứng minh rằng forensic là 1 quá trình, không phải về các công cụ; Hiểu nơi tìm dữ liệu và cách trích xuất và giải thích dữ liệu đó, cho phép người kiểm tra chọn công cụ phù hợp cho công việc. Nhiều trường hợp, các công cụ phần mềm miễn phí có thể cung cấp chức năng mà các công cụ thương mại không thể.

Chapter 9: Performing Analysis on a Budget

Các phần trong chương này:

■ Lưu tài liệu phân tích của bạn

■ Công cụ

Tóm lược

Giải pháp theo dõi nhanh

Các câu hỏi thường gặp

Giới thiệu

Đối với một số người, việc thực hiện ứng phó sự cố và forensic máy tính dường như chỉ là ngoài tầm với do chi phí liên quan đến các công cụ thương mại có sẵn. Tuy nhiên, điều này ảnh hưởng đến nhiều hơn những người có sở thích và những người quan tâm đến việc đi sâu vào lĩnh vực hấp dẫn này. Điều này ảnh hưởng đến các trường học: Các khóa học forensic máy tính được cung cấp không chỉ tại các trường đại học lớn mà còn tại các trường cao đẳng cộng đồng. Chi phí của các công cụ thương mại ảnh hưởng đến các nhân viên thực thi pháp luật và thậm chí cả các chuyên gia tư. Thật tuyệt nếu có quyền truy

cập vào tất cả các công cụ thương mại? Chắc chắn, điều này có thể xảy ra được, nhưng từ góc độ ngân sách, nó không thực tế.

Nó cũng không đặc biệt cần thiết. Các ứng dụng thương mại (EnCase, FTK, ProDiscover, v.v.) chỉ là những công cụ mà. Mọi công cụ hoặc ứng dụng đều có điểm mạnh và điểm yếu của nó, và các nhà phân tích có kiến thức, được đào tạo hiểu được những gì họ cần làm trước khi chọn công cụ hoặc ứng dụng để hỗ trợ họ phân tích. Chìa khóa để forensic không nằm ở việc nhấn các nút trên giao diện người dùng ứng dụng. Chìa khóa để forensic là hiểu những gì có sẵn cho bạn và có một kế hoạch hoặc quy trình logic, hợp lý và toàn diện để thu thập và giải thích dữ liệu. Từ quan điểm đó, bạn không bị ràng buộc với một ứng dụng thương mại cụ thể (trong trường hợp không có một số yêu cầu cụ thể buộc bạn phải sử dụng nó) và thay vào đó có thể khám phá việc sử dụng các công cụ và ứng dụng có sẵn chi phí thấp hoặc miễn phí mà việc phân tích của bạn có nhu cầu dùng tới.

Tip

Bây giờ là thời điểm tốt để thảo luận về chủ đề của các công cụ chống forensic (anti-forensic tools). Các công cụ chống forensic là những công cụ (và trong một số trường hợp là các kỹ thuật) mà kẻ xấu sẽ sử dụng để làm cho công việc forensic khó khăn hơn, chẳng hạn như sửa đổi tệp MAC nhiều lần hoặc xóa dữ liệu (hoặc bằng chứng) từ hệ thống. Nhiều người cho rằng công cụ chống forensic có mục tiêu là một ứng dụng thương mại cụ thể. Đã có các bài thuyết trình công khai tại bảo mật máy tính phổ biến hội nghị thảo luận về cách lật đổ một nhà phân tích sử dụng EnCase, nhưng thực tế là các công cụ và kỹ thuật chống forensic nhằm vào nhà phân tích, chứ không phải các công cụ. Một nhà phân tích nhận ra điều này sẽ đi trước một bước kẻ xấu.

Trong suốt cuốn sách này, mỗi chương đã và sẽ trình bày, mô tả, thực thi các công cụ được sử dụng cho các mục đích cụ thể, nhưng trong mỗi trường hợp, phần trình bày đó chỉ đơn giản là “hey hey, hãy xem công cụ này làm gì và xem nó hữu ích như thế nào”. Chương này là để

lấp đầy khoảng trống cho nhiều độc giả với một số công cụ khác sẽ giúp họ bắt đầu - các tool như các hex editor, các công cụ thu thập và phân tích packet, v.v. Có nhiều công cụ mà bạn có thể sử dụng và nhiều trong số chúng không được thiết kế với mục đích phân tích ngay từ ban đầu. Tuy nhiên, ai đó đã tìm thấy những công cụ này hữu ích bởi một số chức năng chúng cung cấp. Bạn không nên xem chương này, hoặc thậm chí cuốn sách này như một hướng dẫn toàn diện và đầy đủ cho mọi thứ và mọi công cụ bạn có thể muốn. Tốt nhất hãy coi cuốn sách này dùng để mở cánh cửa đó một chút để cho bạn thấy rằng có những lựa chọn ngoài tầm với do chi phí của sản phẩm hoặc chi phí đào tạo liên quan đến sản phẩm đó.

Cuối cùng, nếu bạn biết tôi hoặc đã đọc bất kỳ cuốn sách nào trước đây của tôi, bạn sẽ biết tôi là một fan hâm mộ của Perl. Một số người thậm chí có thể nói rằng Perl là cây búa của tôi và mọi thứ mà tôi thấy là một cái đinh. Và có lẽ họ đúng. Tuy nhiên, hãy đặt tất cả sự hài hước sang một bên, Perl có thể là một công cụ cực kỳ mạnh mẽ, chẳng hạn như khi bạn phải phân tích vài trăm megabyte logs của máy chủ Web để chỉ ra một cuộc tấn công SQL injection và giải mã mã thập lục phân hoặc mã hóa ký tự để giải mã các lệnh được inject để từ đó xác định vị trí hệ thống bị ảnh hưởng khác. Những gì có thể đã lấy đi của bạn cả nhiều ngày nay chỉ mất vài phút. Tôi đã thấy và chứng minh điều này thông qua các script mà tôi đã viết. Điều này không có nghĩa là Perl là ngôn ngữ lập trình *duy nhất* có sẵn, bởi vì bất kỳ ngôn ngữ lập trình nào bạn cảm thấy thoải mái, như Python, sẽ phù hợp với bạn.

Documenting Your Analysis

Tôi bắt đầu phần này bằng cách nói rằng tôi biết tôi đã thảo luận về tài liệu trong các chương khác trong cuốn sách này, và giờ lại quay lại chủ đề này một lần nữa. Điều này là do chủ đề của tài liệu là vô cùng quan trọng, đặc biệt vì đó là điều mà những người thuần kỹ thuật không thích làm. Từ góc nhìn của tôi, tôi không bao giờ thích ghi chép lại bất cứ điều gì, cho đến khi tôi bắt đầu thấy những gì xảy ra khi tôi không ghi lại phân tích của mình. Ví dụ: tôi bắt gặp một ý tưởng tuyệt vời hoặc tìm một số công cụ hoặc kỹ thuật tuyệt vời để phân tích, và ba tháng sau tôi sẽ không nhớ nó là gì. Và tôi đã không ghi lại nó! Tài liệu là một chủ đề định kỳ trong suốt cuốn sách này vì thực tế đơn giản là nó rất quan trọng.

Một chủ đề quan trọng khác trong suốt cuốn sách này là nhu cầu lặp lại trong công việc, có thể là thu thập hoặc phân tích dữ liệu. Khả năng lặp lại, về cơ bản là có thể lấy cùng một dữ liệu, tuân theo cùng một quy trình, sử dụng cùng các công cụ và đạt được kết quả tương tự, là một nguyên tắc cơ bản của khoa học pháp y. Đây là 1 lý do khiến tài liệu cần thiết vì các trường hợp có khả năng lặp lại và các nhà phân tích không phải lúc nào cũng ở bên. Một nhà phân tích hoặc người khảo sát có thể thực hiện công việc, và sau đó vài tháng khi nhà phân tích đó đi nghỉ hoặc được giao cho một nhiệm vụ khác. Một nhà phân tích khác sẽ có thể bước vào thay thế vị trí đó và, với dữ liệu gốc và ghi chú của nhà phân tích trước đó, có thể lặp lại quá trình tương tự và đạt được kết quả tương tự. Tương tự thì một nhà phân tích có thể cần phải xem lại 1 số công việc một năm sau đó; nếu không có tài liệu phù hợp, có khả năng nhà phân tích không thể nhớ chính xác những gì họ đã làm.

Bước đầu tiên trong việc thực hiện bất kỳ phân tích pháp y là có một phương pháp để ghi lại những gì bạn làm. Rốt cuộc, nếu bạn thực hiện một số phân tích nhưng không ghi lại nó, *điều đó đã không xảy ra*. Những người làm về kỹ thuật đường như ghét làm điều này, việc ghi lại phân tích của bạn rất quan trọng với những gì bạn làm. Tài liệu phải đủ chi tiết và rõ ràng để cho phép một nhà phân tích hoặc nhà đánh giá khác hiểu những gì bạn đã làm, cũng như xác minh nó. Ngoài ra, tài liệu phải đủ chi tiết và rõ ràng để *bạn* nhận ra các ghi chú phân tích của riêng bạn từ một năm trước (hoặc hơn) và có thể xác minh những gì bạn đã làm. Bằng cách *xác minh*, ý tôi là sử dụng cùng một dữ liệu và cùng các công cụ (vì trong ghi chú phân tích của bạn, bạn đã liệt kê các công cụ và phiên bản được sử dụng phải không?), Bạn hoặc người khác sẽ nhận được kết quả tương tự.

Hãy suy nghĩ về điều đó 1 chút. Giả sử bạn thực hiện phân tích và khi kiểm tra hoàn tất và báo cáo cuối cùng đã được gửi, bạn sẽ khóa ổ đĩa trong trạng thái chờ đợi an toàn. Sau đó, một tháng sau, một câu hỏi về điều gì đó trong báo cáo của bạn xuất hiện và bạn cần quay lại dữ liệu đó và xác minh một số khía cạnh trong phân tích của bạn. Nhưng đó là một tháng (hoặc sáu tháng hoặc một năm) và với tiến độ hoạt động của bạn thì bạn đã làm rất nhiều việc kể từ đó và giờ dữ liệu gốc của bạn cần được cung cấp cho người giám định khác. Sẽ rất khó khăn nếu một người giám định khác không thể lấy cùng một dữ liệu và, sử dụng cùng các công cụ, tái hiện lại phát hiện của bạn? Làm thế nào bạn có thể giải thích điều đó không? Hầu hết

chúng ta có thể sẽ nói điều gì đó giống như “ Bạn không làm điều đó đúng” hay “Bạn không sử dụng đúng phiên bản của công cụ, phải không? “. Và sẽ ra sao nếu chính *bạn* không thể tái hiện kết quả của chính mình?

Việc tổng hợp tài liệu về những gì bạn làm là quan trọng, nhưng việc ghi lại những gì bạn làm đến mức người khác có thể tái hiện lại phát hiện của bạn thậm chí còn quan trọng hơn. Làm cách nào bạn làm được việc đó? Tôi luôn thấy ngắn gọn là cách tiếp cận tốt nhất. Tôi đã thấy nhiều người đã quá dài dòng trong các ghi chú của họ, và những gì họ thực sự đã làm chỉ đơn giản là bị lạc trong văn xuôi. Giả sử bạn nghi ngờ rằng bạn có thể có một máy chủ Web bị tấn công SQL injection. Vị trí hợp lý nhất để tìm kiếm dấu hiệu của một cuộc tấn công như vậy sẽ là trong logs máy chủ Web. Nếu máy chủ Web là Microsoft's Internet Information Server (IIS) và cơ sở dữ liệu phía sau là MS SQL Server, thì một vị trí hợp lý để bắt đầu sẽ là tìm kiếm việc sử dụng quy trình lưu trữ mở rộng SQL - *xp_cmdshell* trong logs máy chủ Web vì điều đó sẽ không phải là thứ mà bạn thường thấy trong nhật ký máy chủ Web. Vì vậy, giả sử rằng bạn đã tạo một dự án ProDiscover mới, thêm image của máy chủ Web vào đó và sau đó chạy một tìm kiếm trên nhật ký máy chủ Web để tìm “xp_cmdshell”. Trường hợp của bạn ghi chú có thể trông như sau:

- *Đã tạo dự án ProDiscover 5.0 “intrusion_20081030”. Đã thêm image máy chủ Web, dự án đã lưu .*
- *Đã tìm kiếm logs máy chủ web (ghi chú đường dẫn đầy đủ) cho đường xp_cmdshell bằng cách sử dụng chức năng PD Search; một số lượt truy cập được tìm thấy ex081002.log và ex081003.log*

Đơn giản, đến mức, súc tích, nhưng rõ ràng và kỹ lưỡng. Trong trường hợp tìm kiếm này, bạn đã liệt kê những gì bạn đã tìm kiếm (*xp_cmdshell*), những gì bạn đã sử dụng để thực hiện tìm kiếm (chức năng ProDiscover 5.0 Search) và những gì bạn tìm thấy (lần truy cập trong hai tệp nhật ký). Vd “phân tích log files” hay “tìm kiếm log files” sẽ không chỉ rõ hay nói về những gì bạn đã làm. Tập tin nào bạn đã tìm kiếm? Bạn đã tìm kiếm gì? Nếu bạn đã tìm kiếm từ khóa, từ khóa của bạn là gì? Làm thế nào bạn thực hiện việc tìm kiếm? Sử dụng grep hoặc sử dụng công cụ tìm kiếm Windows (mà tôi đã thực hiện: Xuất tệp nhật ký từ image bằng FTK Imager và sau đó nhấp vào **Start | Search | For Files and Folders**)? Kết quả của bạn là gì? Xem cách tài liệu tạo ra thay vì trả lời câu hỏi? Cũng hãy chắc chắn để tránh quá

dài dòng; như tôi đã nói, tôi đã thấy các ghi chú rất dài dòng rằng công việc thực tế đã hoàn thành và kết quả đã bị mất hoàn toàn. Việc cung cấp ngày trên mỗi trang hoặc với mỗi mục sẽ tăng thêm tính xác thực của các ghi chú và nếu nhiều thành viên trong nhóm đang thực hiện phân tích, có tên mỗi thành viên ở đầu hoặc ký vào công việc của chính họ có thể là một lợi thế thực sự trong tương lai.

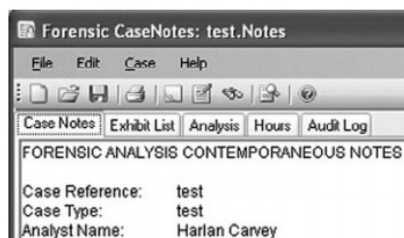
Bao gồm các công cụ bạn đã sử dụng và các phiên bản của chúng trong tài liệu của bạn giúp dễ dàng tạo lại và xác minh kết quả. Phiên bản của công cụ bạn sử dụng có thể tạo sự khác biệt, đặc biệt nếu có các cập nhật lớn giữa các phiên bản của công cụ. Điều này có thể đặc biệt quan trọng nếu bạn đang sử dụng ứng dụng quét chống vi-rút để quét image hoặc chỉ một vài tệp. Lưu ý phiên bản của công cụ quét cũng như (các) tệp định nghĩa vi-rút có thể tạo ra sự khác biệt, đặc biệt là khi các tệp bạn quét được tìm thấy hai tuần sau đó là phần mềm độc hại.

Một khía cạnh quan trọng khác của tài liệu phân tích của bạn bao gồm chứng minh các quyết định của bạn. Các nhà phân tích rất hiếm khi đưa ra quyết định về một cái gì đó chỉ dựa trên một phần dữ liệu; trong hầu hết các trường hợp, có nhiều phần dữ liệu hỗ trợ tương quan để thực hiện 1 quyết định nào đó. Ví dụ: nếu tôi cần xác định khi nào người dùng đăng nhập vào hệ thống Windows, một trong những nơi đầu tiên tôi sẽ tìm là tệp hive Security. Phân tích một khóa trong tệp hive này sẽ cho tôi biết liệu kiểm tra đăng nhập đã được bật hay chưa. Nếu đúng như vậy, thì tôi sẽ tìm các bản ghi sự kiện thích hợp trong Nhật ký sự kiện bảo mật. Tôi cũng sẽ kiểm tra tệp hive SAM để biết các dấu hiệu của lần cuối người dùng đăng nhập, cũng như tệp hive NTUSER.DAT trong thư mục hồ sơ của người dùng để biết các dấu hiệu hoạt động trong khung thời gian được đề cập. Tất cả những điều này có thể được sử dụng để xác định thời điểm người dùng đăng nhập. Ngoài ra, tham khảo các nguồn bên ngoài, như các bài viết của Cơ sở tri thức Microsoft, là một cách tuyệt vời để chứng minh các kết quả phân tích của bạn.

Một công cụ mà tôi thấy cực kỳ hữu ích cho tài liệu là Forensic CaseNotes từ QCC Information Security ở Vương quốc Anh (www.qccis.com/?section=casenotes). Forensic CaseNotes là một công cụ tuyệt vời để lưu các ghi chú trường hợp kiểm tra. Nó miễn phí, cấu hình và khá linh hoạt. Nói chung, điều đầu tiên tôi làm sau khi tải

xuống và cài đặt Case Notes cho một hệ thống mới là thiết lập các tab có thể định cấu hình cho phù hợp với nhu cầu của tôi, như được minh họa trong Hình 9.1.

Figure 9.1 Excerpt from Forensic CaseNotes GUI, after Configuration



Như bạn có thể thấy trong Hình 9.1, có một số tab có sẵn. Tôi giữ một cho Triển lãm: Đây là tất cả các phương tiện truyền thông tôi có, cùng với bất kỳ ghi chú nào liên quan đến việc mua lại. Thông tin cho tab này đến từ bảng tính mua lại của tôi. Tôi cũng có một giờ cho giờ: Tôi sử dụng điều này để ghi lại số giờ dành cho công việc có liên quan trực tiếp đến sự tham gia và lập hóa đơn cho khách hàng. Đây là cực kỳ quan trọng đối với chuyên gia tư vấn. Có lẽ tab quan trọng nhất là Phân tích: Đây là nơi tôi theo dõi công việc thực tế tôi làm hàng ngày. Đôi khi tôi tự mình làm việc phân tích, trong khi những lần khác tôi làm việc với tư cách là trưởng nhóm và quản lý công việc không chỉ do tôi mà còn bởi các thành viên khác trong nhóm, hoặc có lẽ là một tổ chức khác trong nội bộ công ty. Có mọi thứ hiển thị ở một nơi cho phép tôi xem những gì đã được thực hiện và nếu cần thêm giờ.

Một khía cạnh có lợi của CaseNotes là bạn có thể thêm image (snapshot, ảnh kỹ thuật số, v.v.) vào các trường văn bản bên dưới mỗi tab. Khi thực hiện phân tích, tôi sẽ thường cắt và dán các dòng lệnh được sử dụng với các công cụ giao diện dòng lệnh (CLI) khác nhau cũng như trích đoạn từ đầu ra của các công cụ CLI khác nhau trực tiếp vào nội dung của các tab; nếu tôi có một cái gì đó đặc biệt để thêm, chẳng hạn như sơ đồ pin cho bộ điều hợp, tôi cũng có thể thêm chúng. Có sẵn những thứ này để một nhà phân tích khác xem xét có thể có lợi cho việc tham khảo trong tương lai và có thể cực kỳ có giá trị khi viết báo cáo. Thông thường, việc thêm một image hoặc sơ đồ vào một báo cáo có thể tiết kiệm rất nhiều lời giải thích và nhầm lẫn. Những gì khác đi vào ghi chú trường hợp của tôi? Mọi điều. Nghiêm túc. Điều này bao gồm các URL hoặc liên kết đến thông tin từ Internet mà tôi đã sử dụng như một phần trong phân tích của mình, chẳng hạn như các bài viết của Cơ sở tri thức MS TechNet, và thậm chí liên kết đến các trang web hack hack nếu chúng phù hợp với việc kiểm tra (và được hỗ trợ bằng cách chứng thực dữ liệu); snapshot, image của bất cứ thứ gì thích hợp để kiểm tra, v.v.; và các phiên bản cụ thể của các công cụ được sử dụng, cũng như đề cập và tham chiếu đến các công cụ / tập

lệnh cụ thể mà tôi đã tạo để hỗ trợ tôi trong việc quản lý dữ liệu có sẵn. Trong một số trường hợp, nếu một số công cụ hoặc tập lệnh được sử dụng, tôi sẽ lưu trữ chúng ở một vị trí khác để tham khảo sau. Một cảnh báo về việc sử dụng CaseNotes là tôi biết các trường hợp trong đó các nhà phân tích không thể truy cập tệp CaseNotes của họ sau khi đặt mật khẩu vào đó và đóng nó. Ngoài ra, cần lưu ý rằng CaseNotes không giữ nội dung ghi chú của bạn trong một tệp có thể nhất thiết phải được mở ở nhiều định dạng khác nhau; nghĩa là, nếu bạn sử dụng CaseNotes, đừng mong đợi mở tệp trong Notepad và nhận được thứ gì đó dễ đọc.

Một công cụ khác có sẵn là trình quản lý ghi chú NoteCase (<http://notecase.sourceforge.net/>). Tôi chưa thử sử dụng NoteCase hoặc, trong vấn đề đó, các công cụ khác để duy trì ghi chú trường hợp của tôi. Tuy nhiên, nếu bạn đang tìm kiếm thứ gì đó cho phép ghi chú trường hợp của bạn dễ truy cập hơn, một cách đơn giản để thực hiện việc này là thiết lập định dạng hoặc danh sách kiểm tra trong MS Word. Hầu hết các tổ chức thương mại đều có MS Word, bạn có thể lưu các tệp ở một số định dạng và nhiều loại của các công cụ thương mại (Adobe) và phần mềm miễn phí (PDFCreator) sẽ cho phép bạn in các tệp sang định dạng PDF. Các tab tôi đã sử dụng trong CaseNotes có thể dễ dàng được làm lại như các tiêu đề trong tài liệu MS Word và thậm chí bạn có thể sử dụng các bảng hoặc bảng tính Excel nhúng để quản lý và ghi lại giờ của mình.

Ý tưởng tổng thể ở đây là bạn có một cái gì đó, một số phương pháp để ghi lại công việc của bạn một cách nhất quán, có thể kiểm chứng. Tôi chưa đề cập đến một lý do rất tốt khác để làm điều này: Điều gì xảy ra nếu bạn được gọi để làm chứng về bất kỳ công việc nào của bạn? Bạn sẽ nhớ các chi tiết cụ thể và các sắc thái của một kỳ thi hoặc đính hôn sáu tháng hoặc một năm sau khi thực tế? Đã có một số lần tôi được hỏi một câu hỏi (không được hỏi tại tòa án hoặc trong khi ký gửi) về một số công việc tôi đã làm cách đây một thời gian (bốn, sáu hoặc chín tháng) và tôi cần phải đề cập đến trường hợp của mình ghi chú để đảm bảo tôi đã kiểm tra đúng và thông tin chính xác.

Tools

Khi thực hiện phản ứng sự cố hoặc phân tích pháp y, có rất nhiều hoạt động đòi hỏi. Như vậy, bạn sẽ cần công cụ phù hợp cho công việc phù hợp, nhưng công cụ nào phù hợp nhất với bạn? Mục đích của phần này là để trình bày một loạt các công cụ hữu ích cho nhiều mục đích khác nhau để bạn có thể bắt đầu trên con đường khám phá của mình. Các công cụ được

liệt kê trong chương này là các công cụ có sẵn miễn phí và hầu hết đều miễn phí cho bạn sử dụng trong các điều khoản của thỏa thuận cấp phép (tất nhiên). Một số công cụ là phiên bản đánh giá và phiên bản đầy đủ có thể yêu cầu một khoản phí danh nghĩa nếu bạn muốn tiếp tục sử dụng chương trình

Thu thập image

Thu thập dữ liệu là một phần chính của bất kỳ nhà phân tích phản ứng sự cố nào và việc có được image của các hệ thống chỉ là một phần trong đó.

dd

là tiện ích mà hầu hết mọi người nghĩ đến khi có được image. dd, hoặc định nghĩa dữ liệu, dữ liệu, là một lệnh Linux / UNIX gốc cho phép người dùng chuyển đổi hoặc sao chép một tập tin (theo các trang hướng dẫn như <http://linuxreviews.org/man/dd/>), và nó là rất xem như các tiện ích tiêu chuẩn hay các “granddaddy” utility dùng cho mục đích này. Có một số biến thể của tiện ích này có sẵn, một số có khả năng hơi khác nhau; tuy nhiên, tất cả chúng đều thực hiện cùng một chức năng cơ bản giống nhau, chúng cho phép bạn có được image của các ổ đĩa hoặc ổ đĩa. Một phiên bản dd có sẵn cho Windows là của George M. Garner, Jr., và là một phần của Tiện ích thu thập pháp y mà anh ta cung cấp (<http://gmgsystemsinc.com/fau/>). Gói tiện ích này cho phép bạn có được image của các hệ thống, đưa chúng qua mạng (nếu bạn không có bộ nhớ cục bộ), sử dụng nén và tạo và xác minh các giá trị băm tính toán để đảm bảo tính toàn vẹn của dữ liệu thu được.

Tools & Traps

Sử dụng dd cho Live Image

Hầu hết mọi người nghĩ rằng các công cụ như dd chỉ nhằm mục đích thu thập image của các ổ đĩa bị xóa khỏi hệ thống. Móc ổ đĩa lên một trình chặn ghi và sử dụng dd để thu được image của bạn. Tất nhiên, đây là phương pháp được ưa thích, nhưng trong một số trường hợp, điều này có thể không thực hiện được. Do tính chất của cơ sở hạ tầng mạng của khách

hàng và tác động của việc tắt hệ thống và ngoại tuyến để có được image của ổ cứng, chúng tôi đã chọn sử dụng lệnh dd gốc (SUSE Linux 9) để có được trực tiếp image của ổ đĩa cứng vật lý. Chúng tôi đảm bảo rằng chúng tôi đã ghi chép kỹ lưỡng lý do và quy trình cho phương pháp này, bao gồm ghi lại các phiên bản của các tiện ích được sử dụng (dd, split, v.v.) trong ghi chú và báo cáo trường hợp của chúng tôi.

Dcfldd (<http://dcfldd.sourceforge.net/>) là một phiên bản miễn phí khác của công cụ dd cũng chạy trên Windows. Dcfldd được viết bởi Nick Harbor. Trang web Sourceforge cho dcfldd mô tả nó như là một phiên bản nâng cao của GNU dd, GNU với các tính năng bổ sung như xác minh image / xóa, băm, ghi nhật ký, v.v. Tất cả các chức năng này cực kỳ hữu ích không chỉ để đảm bảo tính toàn vẹn của image và cho phép bạn loại bỏ image khỏi hệ thống (khi có được image của một live system, bạn không muốn ghi tệp đó vào ổ cứng thực tế mà bạn đang lấy) mà còn để xóa hoặc xóa tệp image khi bạn đã hoàn thành phân tích của bạn.

Tools & Traps

Định dạng dd

Ngày càng thường xuyên hơn, các giám định viên pháp y đang thấy sự cần thiết của một số loại tiêu chuẩn hóa trong tất cả các khía cạnh của những gì chúng ta làm. Điều này áp dụng cho việc thu thập image là tốt. Bộ công cụ của bộ phản hồi hoặc bộ công cụ “fily-away” nên bao gồm một số phương pháp để có được image, chẳng hạn như trình chặn ghi phần cứng (nghĩa là những phương pháp cung cấp drive-to- drive imaging cũng như phương pháp cho phép phản hồi kết nối ổ đĩa được tạo hình cho trình chặn ghi và thu nhận image bằng phần mềm, v.v.), cũng như phương tiện (công cụ và quy trình) để có được Live Image. Ngoài ra, các nhóm phản hồi nên đưa vào quy trình vận hành tiêu chuẩn của họ một định dạng chuẩn hóa mà image sẽ được (nếu có thể) có được. Tại sao nó lại quan trọng? Trước khi phát hành các phiên bản cập nhật mới nhất của các ứng dụng phân tích pháp y, tôi đã có cơ hội hỗ trợ kiểm tra trong đó một ổ đĩa từ hệ thống được sử dụng định dạng dd và ổ đĩa khác từ cùng hệ thống đã được mua bằng định dạng độc quyền đến một ứng dụng phân tích pháp y. Vào thời điểm đó, tình huống này có thể đã hạn chế tôi sử dụng một ứng dụng phân tích pháp y cụ thể trong phân tích của tôi. Sử dụng một định dạng nhất quán để có được image cũng quan trọng vì những lý do khác. Đầu

tiên, nó thêm một không khí chuyên nghiệp trong mắt khách hàng, cũng như các đồng nghiệp của bạn. Tin tôi đi, khi lần đầu tiên tôi ngồi xem xét các chi tiết cụ thể của kỳ thi tôi sẽ hỗ trợ và thấy hai ổ cứng từ cùng một hệ thống có được ở các định dạng khác nhau, suy nghĩ đầu tiên của tôi là những người này thậm chí còn có một quy trình? Ngoài ra, đừng suy nghĩ trong một phút rằng bạn là người duy nhất sẽ nhìn thấy những image này. Tôi đã thực hiện một số bài kiểm tra trong đó sau khi mọi thứ hoàn tất và báo cáo cuối cùng được gửi, khách hàng muốn có image thay vì chỉ để tôi xóa sạch các ổ đĩa và gửi lại. Luôn luôn sẵn sàng trả lại image cho khách hàng hoặc chuyển image cho người khác để phân tích; có các định dạng image nhất quán (cùng với tài liệu của bạn) đơn giản là chuyên nghiệp hơn. Thứ hai, yêu cầu một định dạng image nhất quán tự nhiên dẫn đến tài liệu sẽ giải quyết các vấn đề không chỉ của quá trình được sử dụng để thu được image mà còn biện minh cho lý do tại sao bạn cần đi chệch khỏi tiêu chuẩn. Nhìn chung, điều này chỉ đơn giản là chuyên nghiệp và kỷ lưỡng hơn..

FTK Imager

Cả FTK Imager và FTK Imager Lite đều có sẵn miễn phí từ AccessData.com (www.accessdata.com/downloads.html). FTK Imager Lite là phiên bản ánh sáng trực tuyến của công cụ FTK Imager có thể được giải nén và ghi vào đĩa CD hoặc sao chép vào ổ đĩa ngón tay cái để sử dụng. Có một bài viết hỗ trợ trên trang web AccessData.com cũng liệt kê những tệp bạn sẽ cần từ kho lưu trữ FTK Imager nếu bạn muốn chạy công cụ đó từ ổ đĩa CD hoặc ngón tay cái, để có một công cụ và phiên bản nhất quán tại xử lý. Tôi đã thấy FTK Imager cực kỳ có giá trị cho một số mục đích sử dụng. Khi tôi phải thực hiện kiểm tra image thu được bằng EnCase và không có sẵn EnCase (hoặc đơn giản là không muốn sử dụng nó), tôi đã mở các tệp .E0 x trong FTK Imager và trích xuất các tệp cụ thể hoặc thu được image để định dạng dd. Tôi cũng đã sử dụng FTK Imager để xác minh hệ thống tệp image thu được, bao gồm image của hệ thống SUSE Linux 9 chạy ReiserFS. Tất nhiên, tôi cũng đã sử dụng FTK Imager làm công cụ thu nhận image, chạy nó cùng với trình chặn ghi được sử dụng đúng cách hoặc chạy nó từ đĩa CD và thu được Live Image của hệ thống Windows sang kết nối USB cứng bên ngoài ổ đĩa (hoặc một số phương tiện / địa điểm khác). FTK Imager cũng có thể được sử dụng để mở các tệp VMware .vmdk. Tôi đã trả lời các cam kết trong đó các hệ thống chạy trong môi trường ảo VMware là một phần

của cơ sở hạ tầng mạng và thậm chí các hệ thống mà chúng tôi cần thu thập và phân tích. Như vậy, có lẽ cách dễ nhất để có được các hệ thống như vậy là chỉ cần sao chép các tệp .vmdk (và .vmem, nếu có) khỏi hệ thống máy chủ. Với FTK Imager, bạn có thể chọn Thêm một bằng chứng để xem hệ thống tệp và trích xuất các tệp cụ thể hoặc chọn Tạo image đĩa để thu được tệp .vmdk (hoặc .E0 x image) sang định dạng dd, SMART hoặc .E0 x thô. Điều này có thể cực kỳ hữu ích khi sử dụng các công cụ phân tích thương mại có thể không nhận ra định dạng vmdk hoặc có thể rườm rà hơn mức cần thiết cho công việc bạn định thực hiện. Nếu bạn không muốn hoặc đơn giản là không có phương tiện để có được image của riêng mình, có những nơi bạn có thể truy cập Internet để tải xuống image được cung cấp để thử nghiệm công cụ hoặc là một phần của các thách thức. Đây là một điều tuyệt vời mà một số người rất thông minh đã và đang cung cấp. Rốt cuộc, làm thế nào tốt hơn để truyền đạt một ý tưởng hoặc khái niệm hoặc quá trình phân tích hơn là mô tả nó và sau đó cung cấp một số phương tiện cho mọi người để thử cách tiếp cận thực hành trên tay của học tập trên phạm vi học? Hầu hết các image được đăng với một số loại thử thách hoặc một loạt các câu hỏi liên quan để hướng dẫn kiểm tra của người tham gia. Là một chuyên gia tư vấn, tôi nhận thức sâu sắc về nơi mà hướng đi tìm thấy tất cả các hoạt động đáng ngờ / độc hại, có thể dẫn đến nhiều giờ có thể lập hóa đơn mà bạn không thể phục hồi. Các thử thách được đăng không chỉ cung cấp một nguồn tài nguyên tuyệt vời để mài giũa kỹ năng phân tích của bạn mà còn là một ví dụ tuyệt vời cho việc kiểm tra sẽ như thế nào ngay từ đầu. Một trong những vị trí đầu tiên tôi tìm thấy cho các tệp image có sẵn miễn phí là Dự án CReDS (Bộ dữ liệu tham khảo pháp y máy tính) tại NIST. Các trường hợp hack (www.cfreds.nist.gov/Hacking_Case.html) không chỉ bao gồm image phân chia định dạng dd mà còn là EnCase hoặc EWF (Định dạng nhân chứng chuyên gia; Expert Witness là tiền thân của EnCase) cho những ai muốn thực hành với các công cụ khác. Một trang web khác bao gồm một số image cụ thể và các kịch bản thử nghiệm là trang web Công cụ kiểm tra pháp y kỹ thuật số (<http://dftt.sourceforge.net/>), được thiết lập bởi Tiến sĩ Brian Carrier. Trang web này cung cấp một số image thử nghiệm rất cụ thể để thử nghiệm các công cụ phân tích pháp y, nhưng cũng như các trang web khác, image được cung cấp cũng có thể được sử dụng làm cơ sở để phát triển và mài giũa kỹ năng phân tích, cũng như cung cấp các kiến thức phân tích pháp y khác nhau. Lance Mueller cung cấp hai thử thách ứng dụng thực tế

thứ vị thông qua ForensicKB của mình. trang blog com (www.forensickb.com/search?q=pratics). Lance đã cung cấp các kịch bản thực tế, cùng với các image nhỏ (~ 400 MB) có được từ hệ thống Windows XP ở định dạng nén .E0 x / EWF. Nếu bạn không có khóa EnCase hợp lệ, đừng lo lắng: FTK Imager sẽ dễ dàng mở các tệp này, cho phép bạn xuất tệp từ image hoặc chỉ cần tạo image định dạng dd từ tệp EWF cho tệp rmat. Một số ý kiến cho blog của Lance, cho những bài đăng đó, cũng cung cấp cái nhìn sâu sắc về những gì các giám khảo khác đang tìm kiếm và đã tìm thấy.

Image Analysis

Khi bạn có một image thu được, đã xác minh băm image của bạn và hệ thống tệp và đã ghi lại toàn bộ quá trình của bạn, bạn sẽ cần một số phương tiện mở image và thực hiện các chức năng phân tích cơ bản cần thiết như một phần công việc bạn đang làm. Trong suốt cuốn sách này, chúng tôi đã thảo luận về các công cụ khác nhau để thực hiện điều này để mở toàn bộ tệp image và xem toàn bộ cấu trúc hệ thống tệp, chạy các tìm kiếm, v.v. tệp tin, v.v.)

SleuthKit

Các công cụ SleuthKit (TSK; www.sleuthkit.org/) được viết bởi Tiến sĩ Brian Carrier và cung cấp các thành phần phụ trợ cho Trình duyệt pháp y khám nghiệm tử thi. TSK là một bộ công cụ dòng lệnh cho phép bạn kiểm tra và phân tích các tệp và hệ thống volume trong các tệp image. Các công cụ TSK cũng có sẵn cho các hệ thống Windows; tuy nhiên, tại thời điểm viết bài này, Trình duyệt pháp y tự động chưa được chuyển sang định dạng Windows gốc (mặc dù tất cả các công cụ có thể được biên dịch trên Windows bằng hệ thống con Cygwin). Các công cụ TSK có thể được sử dụng trên hệ thống Windows theo cách tương tự như trên các hệ thống Linux; Tuy nhiên, có một vài cảnh báo. Đầu tiên, theo Tiến sĩ Carrier, có một vấn đề với dòng toàn cầu, trong dòng lệnh, yêu cầu bạn liệt kê tất cả các tệp thành phần thành một tệp image phân chia theo thứ tự. Điều này có nghĩa là nếu bạn đang phân tích một tệp image tách có chứa nhiều tệp, bạn sẽ cần liệt kê từng tệp như sau:

lệnh [tùy chọn] image1 image2 image3 ...

Đây là nơi các công cụ như FTK Imager có ích, trong đó bạn có thể ghép lại các tệp image bị tách thành một tệp image thống nhất. FTK Imager có khả năng tập hợp lại một số định dạng tệp image phân tách, chẳng hạn như của chính nó cũng như các định dạng được sản xuất bởi các công cụ như EnCase của Guidance Software. Bạn cũng có thể sử dụng lệnh loại Windows gốc để ghép lại các tệp image đã tách ở định dạng thô:

```
D:\images>type image.001 > image_all.img
```

```
D:\images>type image.002 >> image_all.img
```

```
D:\images>type image.003 >> image_all.img
```

...

TSK có thể mở raw (ví dụ: dd), Expert Witness (nghĩa là EnCase, được gọi là EWF), và hệ thống tệp AFF và image đĩa (www.sleuthkit.org/sleuthkit/desc.php). Công cụ TSK fls.exe (phiên bản 3) cho nền tảng Windows báo cáo tại dòng lệnh có thể phân tích các tệp image thô (dd), tệp image EWF và phân tách các tệp image thô:

```
D:\tools\tsk>fls -i list
```

Supported image format types:

raw (Single raw file (dd))

ewf (Expert Witness format (encase))

split (Split raw files)

Có một số tài liệu có sẵn tại trang web SleuthKit, cũng như các địa điểm khác trực tuyến, mô tả cách sử dụng các công cụ dòng lệnh khác nhau kết hợp để thực hiện phân tích image. Ví dụ: Kỹ thuật phân tích hệ thống tệp (http://wiki.sleuthkit.org/index.php?title=FS_Analysis) và các mốc thời gian hoạt động tệp (<http://wiki.sleuthkit.org/index.php?title=Timeline>) tài liệu tham khảo cung cấp rất nhiều thông tin cực kỳ hữu ích về các công cụ TSK. Có lẽ nguồn thông tin tốt nhất về các công cụ là TSK Wiki (http://wiki.sleuthkit.org/index.php?title=Main_Page). Một số ví dụ sử dụng đơn giản của các công cụ TSK bao gồm sử dụng dls để thu thập

không gian chứa phân bố từ tệp image. Lệnh sau có thể được sử dụng để trích xuất không gian chứa phân bố từ tệp image thu được:

```
dls -A image.dd > unalloc.dls
```

Xóa không gian chứa phân bố khỏi tệp image thu được có thể hữu ích trong việc thực hiện tìm kiếm chuỗi / grep hoặc khắc tệp trên không gian chứa phân bố đó, chẳng hạn như khi tìm kiếm số thẻ tín dụng, địa chỉ IP hoặc email hoặc chỉ thực hiện khắc tệp.

Lệnh sau sẽ cung cấp cho bạn thông tin về hệ thống tệp trong tệp image:

```
fsstat -f ntfs image.dd
```

Lệnh fsstat cung cấp hệ thống tệp, siêu dữ liệu và thông tin nội dung về tệp image. Ví dụ: chạy lệnh đối với image thu được của hệ thống Windows XP sẽ trả về thông tin hệ thống tệp sau:

```
FILE SYSTEM INFORMATION
```

```
-----
```

```
File System Type: NTFS
```

```
Volume Serial Number: 98B0A679B0A65D8E
```

```
OEM Name: NTFS
```

```
Version: Windows XP
```

Trên một hệ thống trực tiếp, bạn có thể có được nhiều thông tin tương tự bằng cách sử dụng fsutil.exe. Ví dụ: các lệnh sau trả về thông tin tương tự như fsstat.exe, mặc dù từ một live system (bao gồm cả số sê-ri volume):

```
C:\>fsutil fsinfo volumeinfo C:\
```

```
C:\>fsutil fsinfo ntfsinfo C:
```

Số sê-ri volume được tạo tại và được xác định theo thời gian ổ đĩa được định dạng và có thể được sử dụng một phần để xác định image thu được khi được sử dụng cùng với tài liệu khác. Có lẽ công cụ hữu ích nhất cho các nhà phân tích là một phần của công cụ TSK là fls.exe ([http:// wiki. Sleuthkit.org/index.php?title=Fls](http://wiki.sleuthkit.org/index.php?title=Fls)), liệt kê tên tệp và thư mục trong một hệ thống tệp trong một định dạng được phân tách bằng ống cho phép tạo

thông tin dòng thời gian bằng mactime.pl. Ví dụ: lệnh sau sẽ chạy qua toàn bộ tập image, đệ quy qua các thư mục và thư mục con:

```
D:\tools\tsk>fls -m c: -r d:\cases\xp\xp.001
```

Các -m tùy chọn cho phép bạn thêm vào trước các danh sách tập tin và thư mục với tên của các điểm lắp sử dụng (trong trường hợp này, C: \). Thông thường, đầu ra của lệnh sẽ được chuyển hướng đến một tập đầu ra và sau đó chạy qua một công cụ như mactime.pl hoặc ex-tip (công cụ tạo dòng thời gian được tạo bởi Mike Cluppert;

https://www2.sans.org/reading_room/whitepapers/forensics/32767.php) để sắp xếp thông tin hệ thống tập thành định dạng dòng thời gian dễ đọc và dễ hiểu hơn.

Tools & Traps Timelines

Các công cụ như fls.exe của TSK, mactime.pl và mepo cũ của Mike Cluppert cung cấp chức năng nguồn mở cực kỳ hữu ích để tạo các mốc thời gian của hoạt động hệ thống tập. Tuy nhiên, vì chúng là nguồn mở, chúng có thể dễ dàng mở rộng. Ví dụ, bất kỳ nguồn thông tin được đóng dấu thời gian nào khác từ hệ thống Windows cũng có thể được bao gồm trong dòng thời gian; tất cả những gì cần xảy ra là định dạng phù hợp (như được minh họa trên trang TSK Wiki cho fls.exe) và các khóa Sổ đăng ký (cũng như các giá trị có dữ liệu bao gồm dấu thời gian), mục Nhật ký sự kiện và thậm chí cả nội dung của các tập khác (extip bao gồm bộ lọc cho tập nhật ký McAfee OnAccessScan và các bộ lọc có thể được ghi cho các tập nhật ký AV khác, tập setupapi.log, v.v.). Ngoài ra, dữ liệu có thể được thêm thủ công vào tập cơ thể của người dùng trước khi lọc và sắp xếp bằng một công cụ như ex-tip, cho phép nhập dữ liệu bổ sung mà nhà phân tích có thể muốn đưa vào dòng thời gian. Bình thường hóa các mục vào một định dạng phổ biến cho phép chúng được nhập vào các công cụ khác như Zeitline (<http://projects.cerias.purdue.edu/forensics/timeline.php>)..

Đối với các lệnh công cụ TSK hữu ích khác, CyberGuardians có một trang cheat PDF PDF hai trang có sẵn (www.cyberguardians.org/docs/ForensicsSheet.pdf).

Ngoài ra còn có một phiên bản Windows của công cụ Dumper tập tin chọn lọc có tên FUNDL (dành cho các tập tin Undeleter tập tin) sử dụng các công cụ TSK có sẵn trên Sourceforge (<http://sfdumper.Sourceforge.net/fundl.htm>).

Tools & Traps

Image Formats

Trước đây trong chương này, tôi đã đề cập đến sự cần thiết phải tiêu chuẩn hóa trong các định dạng image. Mục đích của việc này là để đạt được sự nhất quán và chuyên nghiệp thông qua một quy trình được tiêu chuẩn hóa. Một số tổ chức có thể chỉ dựa vào một ứng dụng phân tích pháp y thương mại và có thể có một lý do tuyệt vời để chuẩn hóa định dạng image độc quyền. Các tổ chức khác, chẳng hạn như các công ty tư vấn, có thể chọn tiêu chuẩn hóa ở định dạng dễ truy cập hơn (nghĩa là định dạng dd) để cho phép phạm vi truy cập rộng hơn vào các ứng dụng phân tích pháp y, lần lượt cho phép xác minh, v.v. Năm 2008, Technology Pathways đã phát hành phiên bản ProDiscover 5.0, bao gồm khả năng mở image định dạng EWF. Sau hội nghị DFRWS 2008, Tiến sĩ Michael Cohen đã phát hành một phiên bản ứng dụng PyFlag của mình chạy tự nhiên trên các hệ thống Windows. Vào tháng 4 năm 2008, Tiến sĩ Brian Carrier đã phát hành các phiên bản của các công cụ Sleuthkit được biên dịch để chạy tự nhiên trên Windows. Các công cụ này, mặc dù (tại thời điểm viết bài này) chúng không thể được sử dụng với Trình duyệt pháp y tự động (phiên bản Cygwin của các công cụ phải được sử dụng), cung cấp quyền truy cập dòng lệnh vào dd, EWF (thông qua libewf) và Định dạng pháp y nâng cao Image định dạng AFF (thông qua afflib; www.afflib.org/).

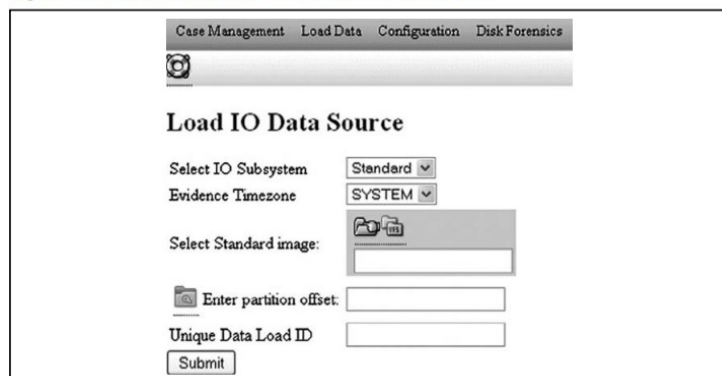
PyFlag

Sau hội nghị DFRWS 2008, Tiến sĩ Michael Cohen đã phát hành phiên bản giao diện người dùng đồ họa phân tích nhật ký và phân tích nhật ký (GUI) PyFlag chạy trên Windows

(www.pyflag.net/cgi-bin/moin.cgi/PyFlagWindows). Phiên bản PyFlag này có tên PyFlagWindows hoặc WinPyFlag. Bất cứ điều gì bạn quyết định gọi nó, xin hãy chắc chắn cảm ơn Tiến sĩ Cohen một cách sâu sắc và liên tục vì sự đóng góp miễn phí (như trong bia bia của mình) cho cộng đồng. PyFlag đã có sẵn cho các hệ thống Linux một thời gian và bây giờ, phạm vi khả

năng của PyFlag có sẵn cho những nhà phân tích thoải mái hơn khi hoạt động trong môi trường Windows. Khi bạn tải xuống và cài đặt PyFlag cho Windows theo hướng dẫn trên PyFlagWiki, tất cả những gì bạn cần làm là khởi chạy tệp FlagHTTPServer.py bằng cách nhấp đúp vào tệp đó, sau đó hướng trình duyệt Web của bạn tới <http://127.0.0.1:8000>. Hình 9.2 cho thấy một phần PyFlag chạy qua Firefox trên Windows.

Figure 9.2 Excerpt of PyFlag UI on Windows, in Firefox



Khi PyFlag được cài đặt, bạn có thể sử dụng nó bình thường, giống như khi bạn chạy trên Linux. PyFlag kết hợp việc sử dụng các công cụ TSK và cho phép nhà phân tích kết hợp các tệp image thu được, dữ liệu nhật ký và gói dữ liệu thu được tất cả trong một trường hợp. cũng kết hợp chức năng của Biến động trong PyFlag, cho phép nhà phân tích bao gồm các kết xuất bộ nhớ. Trong Rodeo pháp y DFRWS 2008

(www.dfrws.org/2008/rodeo.shtml), Tiến sĩ Cohen đã sử dụng PyFlag để thực hiện phân tích của mình, tìm kiếm dữ liệu được cung cấp (kết xuất bộ nhớ và một image thu được từ một ổ ngón tay cái) để tìm manh mối trả lời các câu hỏi được đặt ra trong thử thách.

Cơ bản về ProDiscover

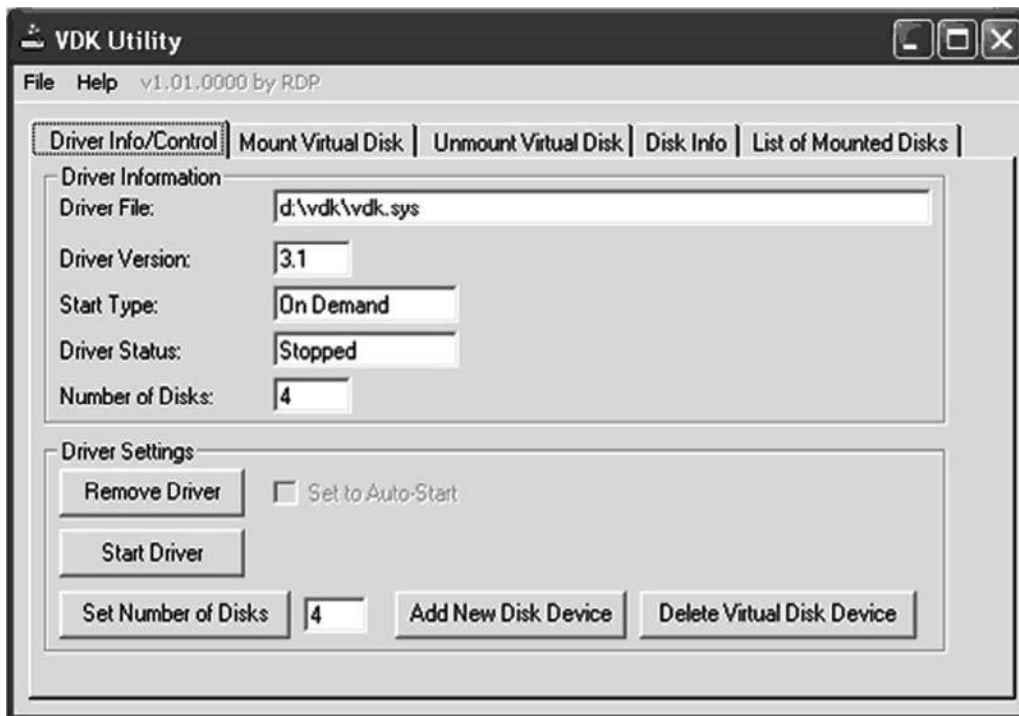
ProDiscover là một ứng dụng phân tích tuyệt vời mà tôi có đặc quyền truy cập kể từ phiên bản 3; phiên bản 5 đã được phát hành vào mùa hè năm 2008. Tôi rất thích sử dụng GUI khá trực quan để phân tích image thu được từ các hệ thống Windows vì nó cho phép tôi nhìn thấy rất nhiều thông tin trong một giao diện đơn nhất, thống nhất, mặc dù không bị lộn xộn. Cho dù tôi đang thực hiện xác minh hệ thống tệp image, một số phân tích nhanh, hoặc một số phân tích chi tiết, trong nhiều trường hợp tôi đã chọn bắt đầu với ProDiscover.

Chris Brown (chủ sở hữu của Path Path Technology và tác giả của Computer Evidence: Collection and Preservation) cung cấp một phiên bản cơ bản của ProDiscover để tải xuống và sử dụng miễn phí. Mặc dù phiên bản cơ bản của ứng dụng không có bất kỳ nơi nào gần khả năng của phiên bản đầy đủ, nhưng nó vẫn là một công cụ rất hữu ích.

Một lưu ý khi sử dụng ProDiscover là cách nó xử lý các tệp image phân chia. Các image thu được là các tệp image đầy đủ có thể được thêm vào tệp dự án ProDiscover, nhưng để thêm một image bao gồm các tệp image phân tách, bạn phải tạo một tệp .pds. Tệp .pds bao gồm một số thông tin tiêu đề và danh sách đầy đủ, theo thứ tự của tất cả các tệp image phân tách. Khi thêm image vào một dự án, bạn cần chọn tệp .pds thay vì tệp image phân tách đầu tiên (ví dụ như cách bạn làm với FTK Imager).

Mounting an Image File

Một cách khác để mở tệp image thu được trong ứng dụng phân tích là gắn tệp image dưới dạng hệ thống tệp chỉ đọc để tệp image xuất hiện trên hệ thống phân tích của bạn dưới dạng ký tự ổ đĩa. Khi được thực hiện cẩn thận (ứng dụng phần mềm được sử dụng đặt hệ thống tệp được gắn kết thành chỉ đọc) và bảo vệ tệp image thu được (nghĩa là sử dụng bản sao dữ liệu thay vì dữ liệu gốc, hãy đảm bảo đặt quyền hệ thống tệp NTFS thành ngăn việc ghi vào tệp tin image, v.v.), đây có thể là một công cụ cực kỳ mạnh mẽ để phân tích phổ rộng. Ngoài các chương trình được đề cập trước đây trong cuốn sách này (SmartMount từ ASRData và Mount Image Pro từ GetData), có một công cụ phần mềm miễn phí sẽ cho phép bạn làm điều tương tự; nó được gọi là trình điều khiển đĩa ảo (VDK; <http://chitchat.at.infoseek.co.jp/vmware/vdk.html>). VDK là trình điều khiển thiết bị sẽ cho phép bạn gắn kết một thiết bị thu được tệp tin image như một ký tự ổ đĩa trên hệ thống của bạn. Khi được sử dụng với GUI VDKWin (<http://petruska.Stardock.net/Software/VMware.html>), được minh họa trong Hình 9.3, bạn chỉ cần nhấp vào một vài nút và bạn sẽ có hệ thống tệp của mình được gắn và truy cập từ hệ thống phân tích.



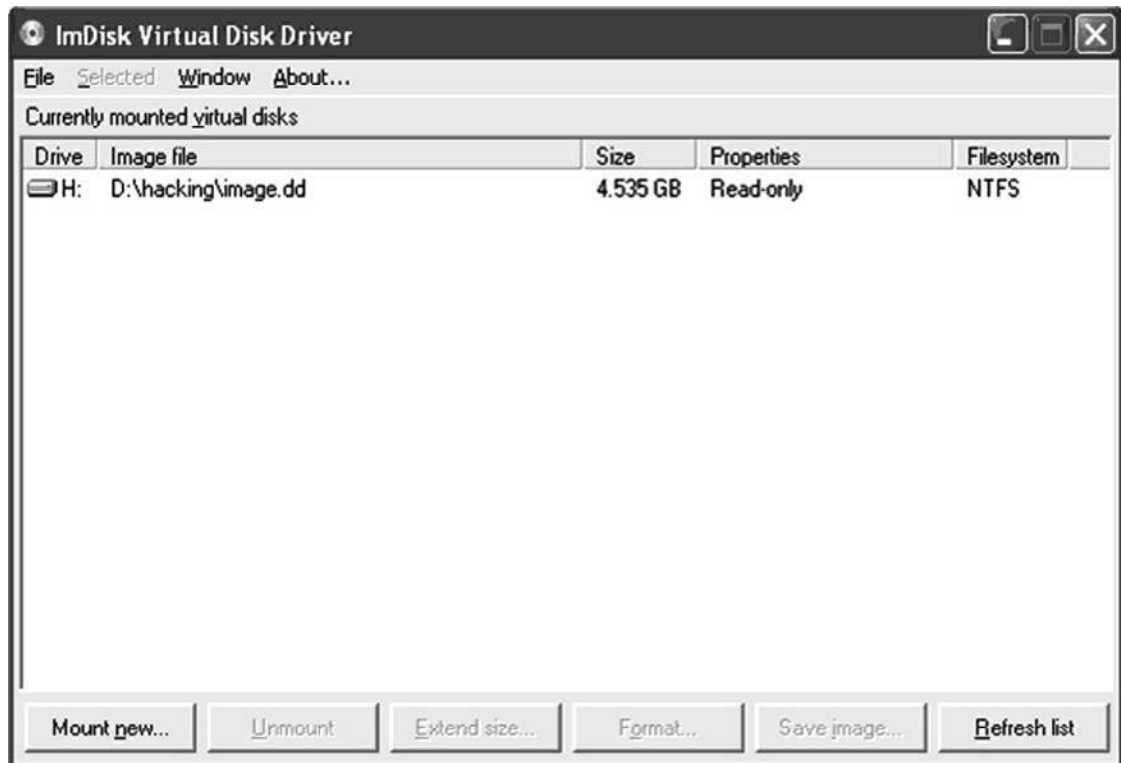
Hình 9.3 VDKMin GUI

VDKWin rõ ràng loại bỏ một số sự phức tạp (và cơ hội để phạm sai lầm)

từ việc sử dụng trình điều khiển vdk.sys, nhưng làm thế nào một cái gì đó như thế này hữu ích? Hy vọng rằng bây giờ bạn đã thấy làm thế nào một giám khảo không phải bị hạn chế chỉ một cách làm nhiều thứ; miễn là mức độ chăm sóc thích hợp được thực hiện, và miễn là bạn đang ghi chép những gì bạn làm (và tại sao), quá trình bạn sử dụng để phân tích image thu được là tùy thuộc vào bạn (hoặc

quy trình vận hành tiêu chuẩn của tổ chức của bạn, tùy từng trường hợp). Tuy nhiên, có thể chỉ đơn giản là một số phương pháp phân tích không thể truy cập được do thực tế là chúng không được tích hợp vào ứng dụng phân tích thương mại mà bạn đang sử dụng hoặc chúng có nhưng làm như vậy, nhà cung cấp đã định giá ứng dụng trong phạm vi phải chăng.

Một công cụ miễn phí có sẵn khác để gắn ảnh là IMDisk (Phiên bản 1.1.3 đã được phát hành vào ngày 5 tháng 12 năm 2008, từ www.ltr-data.se/opencode.html), trình điều khiển đĩa ảo cài đặt là tiện ích CLI và có một applet Control Panel, cung cấp giao diện GUI cho trình điều khiển.



Hình 9.4 ImDisk Giao diện người dùng với image được gắn kết H:\

TIP

Microsoft có sẵn một công cụ miễn phí (mặc dù không được hỗ trợ và không được quảng cáo) được gọi là “Bảng điều khiển CD-ROM ảo của Virtual cho XP”. Công cụ này cung cấp ảo CD-ROM trong Bảng điều khiển Windows XP mà bạn có thể sử dụng để gắn .iso các tệp (thường là từ đĩa CD hoặc DVD) dưới dạng hệ thống tệp.

Liên kết trực tiếp đến công cụ khá dài, nhưng có thể tìm thấy một liên kết tại

Trang web của Microsoft

(<http://msdn.microsoft.com/enus/subscriptions/aa948864.aspx>; cuộn khoảng hai phần ba xuống dưới), cũng như trên các blog như vậy như

RaDaJo (<http://radajo.blogspot.com/2006/09/mounting-cddvd-iso-imagesin-windows.html>) và help.net (<http://weblogs.asp.net/pleloup/archive/2004/01/5/58918.aspx>).

File Analysis

Thông thường, bạn sẽ cần kiểm tra các tệp riêng lẻ thay vì toàn bộ hệ thống tệp hoặc khối lượng.

Nhiều lần, các tệp này sẽ có các định dạng độc quyền (hãy nhớ Windows Recycle Bin INFO2 từ Chương 5?) Và có thể không có trình xem phù hợp.

Hashing Utilities

Khi trích xuất các tệp từ một image thu được, bạn có thể muốn tính toán mật mã băm cho các tệp tin để xác minh tính toàn vẹn của chúng sau này. Các thuật toán băm là mật mã các tính toán thường lấy đầu vào có độ dài thay đổi và trả về độ dài cố định duy nhất đầu ra. Nếu có quá nhiều một bit trong tệp thay đổi, hàm băm cũng sẽ thay đổi, chứng minh tính hữu dụng của băm tệp tin. Jesse Kornblum đã viết một chương trình băm gọi là MD5Deep (<http://md5deep.sourceforge.net/>) sẽ không chỉ tạo và so sánh MD5 băm cho các tệp nhưng cũng tạo và so sánh SHA-1, SHA-256, Tiger và Whirlpool băm. Các chương trình này là tất cả các chương trình CLI, làm cho chúng phù hợp để sử dụng trong các tệp bó trong để tự động hóa việc triển khai của họ.

Bên cạnh việc xác định và kiểm tra tính toàn vẹn, một cách khác bạn có thể sử dụng băm tệp tin là cho xác định nhanh xem liệu tệp bạn làm việc với đã được xác định chưa là phần mềm độc hại. Trang web VirusTotal (www.virustotal.com/) sẽ cho phép bạn tải lên một tệp băm để so sánh trong cơ sở dữ liệu của nó, thay vì tải lên toàn bộ tệp tin. Vì vậy, nếu tệp tin bạn quan tâm đến là rất lớn hoặc bạn không muốn gửi các bản sao của tệp phần mềm độc hại Internet, bạn có thể cân nhắc sử dụng khả năng của trang Web này để xác minh nhanh.

Rốt cuộc, nó không mất nhiều công sức và nó làm tăng thêm tính hoàn chỉnh cho trường hợp của bạn ghi chú và báo cáo cuối cùng của bạn, bất kể bạn là nhà tư vấn hay thực thi pháp luật. Một công cụ băm khác từ Jesse Kornblum là ssdeep <http://ssdeep.sourceforge.net/>, một công cụ tuyệt vời để thực hiện băm mờ piecewise. Kỹ thuật băm này cho phép bạn để so sánh các tệp tương tự nhưng không giống nhau bằng cách xác định khả năng giống nhau giữa tập tài liệu. Tôi đã sử dụng công cụ băm này khi so sánh hai tệp có cùng kích thước và giống nhau tên được thu thập do kết quả của hai lần tham gia ứng phó sự cố khác nhau và tôi tìm thấy các tệp tin tương tự 98 phần trăm đến 99 phần trăm.

Hex Editors

Một trình soạn thảo hex tốt mà bạn có thể sử dụng có thể là một công cụ không thể thiếu cho phân tích pháp y. Thông thường, bạn sẽ chạy trên các tệp nhị phân mà bạn cần mở và xem, và các ứng dụng xử lý văn bản đơn giản sẽ không hiển thị dữ liệu theo định dạng phù hợp. Ở đây có đã nhiều lần tôi nhận được phản hồi bất thường từ các công cụ phân tích, hoặc khi một tập lệnh Perl tôi đang viết để phân tích nội dung nhị phân của một tập tin đơn giản là không hoạt động, và tôi đã phải mở tệp đó trong trình soạn thảo hex để xem lại nội dung nhị phân / thập lục phân và xem vấn đề có thể là gì. Một ví dụ về cách tôi đã sử dụng điều này là để khám phá sự khác biệt giữa các tệp Windows XP và Vista Prefetch (xem Chương 5).

Tôi thích UltraEdit (www.ultraedit.com/) vì tôi sử dụng nó làm môi trường lập trình cũng như một trình soạn thảo hex. Tôi thích nhiều khả năng của ứng dụng này (số dòng là hiển thị để khi một tập lệnh Perl đánh bom, tôi có thể nhanh chóng tìm thấy lỗi của mình), vì vậy tôi đã sẵn sàng trả tiền phí danh nghĩa cho nó. Một số khả năng khác của nó bao gồm đánh dấu cú pháp cho Perl, tự động thụt lề, khả năng mở tệp nhật ký hoặc tệp nhị phân thực sự lớn và nội dung thập lục phân của

một tập tin cạnh nhau với phiên bản nhị phân. Tuy nhiên, trước khi tôi ổn định trên UltraEdit, tôi đã xem xét tại một số ứng dụng phần mềm miễn phí để tìm hiểu những gì đã có và chức năng gì tôi thích. Trong quá trình khám phá này, tôi đã chạy qua một số ứng dụng khác, chẳng hạn như sau đây:

■ CygnusHex Editor Free Edition (www.softcircuits.com/cygnus/fe/)

■ XVI32

(www.chmaas.handshake.de/delphi/freeware/xvi32/xvi32.htm)

■ HDD Software's Free Hex Editor Neo

(www.hhdsoftware.com/Products/home/hex-editor-free.html)

■ Hex Edit (www.physics.ohio-state.edu/~prewett/hexedit/)

Hãy nhớ rằng đây chỉ là những ví dụ về trình soạn thảo hex và là một nhà phân tích, bạn cần để tìm những gì làm việc cho bạn. Nếu bạn thích khám phá các tùy chọn khác, Wikipedia chính là một so sánh các trình soạn thảo hex (http://en.wikipedia.org/wiki/Comparison_of_hex_editors) trên các nền tảng khác nhau mà bạn có thể muốn xem và thậm chí có thể sử dụng làm cơ sở cho khám phá của riêng bạn vào các công cụ để sử dụng.

Network Tools

Tôi hy vọng rằng trong suốt cuốn sách này, bạn đã thấy phân tích hệ thống, đặc biệt là trong thời gian phản ứng sự cố, không bị hạn chế chỉ đơn giản là các hệ thống máy chủ (mặc dù đó là chính trọng tâm của cuốn sách này). Thông thường, dấu hiệu của sự thỏa hiệp, xâm nhập hoặc nhiễm phần mềm độc hại sẽ bắt đầu bằng cảnh báo IDS, một cái gì đó bất thường trong nhật ký tường lửa hoặc đơn giản là một số bất thường lưu lượng mạng. Trong các trường hợp khác, thông tin tiếp theo về một vụ xâm nhập, chẳng hạn như cộng đồng cation giữa các hệ thống, nơi kết nối mạng bắt nguồn từ và nơi bên ngoài thông tin liên lạc đã được định sẵn (trong trường hợp hết dữ liệu), sẽ chỉ có thể được xác định thông qua việc thu thập và phân tích dữ liệu dựa trên mạng. Như một chủ đề cho đến chính nó, thu thập và phân tích dữ liệu dựa trên mạng nằm ngoài phạm vi của cuốn sách này, nhưng nó là một chủ đề đủ quan trọng để cung cấp cho bạn một số công cụ cần thiết có thể được sử dụng trong các hoạt động này.

Scanning

Một trong những vấn đề chính mà cộng đồng phân tích pháp y phải đối mặt

(theo ý kiến ​​khiêm tốn của tôi) là khoảng cách tồn tại giữa cộng đồng này và lỗ hổng cộng đồng. Các lỗ hổng được phát hiện và xác minh trên cơ sở

gần như hàng ngày, và ngay sau đó, một khai thác làm việc tận dụng lỗ hổng đó có thể được đăng trên Internet hoặc phát hiện trong các hoạt động ứng phó sự cố. Ngoài ra, có những công ty có kinh doanh mô hình là tìm kiếm, tìm và xác minh các lỗ hổng trong các sản phẩm phần mềm và sau đó cung cấp bảo vệ chống lại các lỗ hổng này cho khách hàng của họ.

Sự chênh lệch xuất hiện do thực tế là khi phát hiện ra lỗ hổng, thường có rất ít hoặc không có nghiên cứu nào đi vào việc xác định các cổ vật còn sót lại trên một hệ thống bị xâm phạm bởi việc sử dụng khai thác. Để một lỗ hổng được khai thác thành công, thường có một dịch vụ hoặc ứng dụng đang lắng nghe trên một cổng mạng (ví dụ: MS SQL Máy chủ lắng nghe các kết nối trên cổng TCP 1433) và chịu sự khai thác, và kết quả là, nhà nghiên cứu phải có một số phương tiện để xác minh rằng việc khai thác đã thành công. Sau khi khai thác đã thành công, kết quả là một hệ thống bị xâm phạm thành công mà sau đó có thể được phân tích cho hiện vật gắn liền với việc khai thác.

Các ứng dụng quét được sử dụng trong các đánh giá lỗ hổng để xác định các lỗ hổng tiềm ẩn trong một cơ sở hạ tầng để có thể phát triển một kế hoạch ưu tiên, toàn diện để giảm thiểu các cuộc tấn công trên bề mặt cơ sở hạ tầng của cơ sở hạ tầng đó. Điều này có nghĩa là bằng cách xác định điểm yếu ở đâu tồn tại, và sau đó làm việc để giải quyết những điểm yếu đó (hệ thống vá lỗi, nâng cấp và bảo mật cấu hình các ứng dụng, v.v.), các cơ hội có sẵn cho kẻ tấn công để có quyền truy cập vào cơ sở hạ tầng mạng được giảm đáng kể. Những ứng dụng quét tương tự có thể được sử dụng như một phần trong phân tích của bạn để xác định bề mặt tấn công của hệ thống hoặc các hệ thống liên quan để bạn có cách xác định hệ thống có thể bị xâm phạm như thế nào. Ví dụ, vào tháng 10 năm 2008, Microsoft đã phát hành một bản vá lỗi ngoài chu kỳ của người dùng cho một lỗ hổng được xác định là MS08-067

(<http://bloss.technet.com/msrc/archive/2008/10/23/ms08-067-release.aspx>), liên quan đến lỗ hổng nghiêm trọng đối với dịch vụ Windows Server. Bạn đã khám phá một hệ thống Windows XP bị xâm nhập hai tháng sau đó và thấy rằng điều cực kỳ quan trọng bản vá cho lỗ hổng đó chưa được cài đặt, điều này có thể cung cấp cho bạn một số dấu hiệu về nơi để chỉ đạo phân tích của bạn, đặc biệt nếu phần mềm độc hại được sử dụng trên hệ thống sau khi thành công khai thác quá mới đến nỗi nó không bị các ứng dụng chống vi-rút phát hiện.

Có một số công cụ có sẵn miễn phí mà bạn có thể sử dụng để hỗ trợ phân tích của mình, đặc biệt là khi bạn đang cố xác định lỗ hổng nào hoặc vectơ tấn công của Vectơ có thể đã bị được sử dụng trong một sự cố. Những công cụ này không chỉ động trên các live system mà bạn còn có thể khởi động một image thu được với LiveView (<http://liveview.sourceforge.net/>) và sau đó quét hệ thống (theo mặc định, các hệ thống được khởi động với LiveView không có khả năng kết nối mạng) để có ý tưởng như những gì lỗ hổng có thể đã tồn tại trên hệ thống. Ví dụ: của riêng Microsoft Trình phân tích bảo mật cơ sở (<http://technet.microsoft.com/en-us/security/cc184924.aspx>) có thể được sử dụng để quét một hệ thống và xác định xem có bản cập nhật hoặc bản vá nào áp dụng cho cụ thể không cảnh báo bảo mật bị thiếu trong hệ thống.

Quét dựa trên mạng có thể cung cấp thông tin rất hữu ích trong quá trình xử lý sự cố các hoạt động hoặc trong khi thực hiện phân tích một image thu được. Hãy ghi nhớ, tuy nhiên, rằng để loại quét này hữu ích khi phân tích image thu được, image cần để được khởi động vào một môi trường có khả năng kết nối mạng. Có lẽ phổ biến nhất máy quét dựa trên mạng là máy quét Nmap thực sự (www.Nmap.org). Bên cạnh cổng đơn giản quét, Nmap có khả năng thực hiện các hệ điều hành máy chủ (HĐH) và nhận dạng dịch vụ quét và với sự ra đời của Zenmap GUI, Nmap cũng có khả năng thực hiện mô-đun của ánh xạ cấu trúc liên kết mạng.

Tools & Traps ...

Tools Supporting Nmap

Một số công cụ có sẵn miễn phí sẽ giúp bạn phân tích cú pháp thông qua kết quả của Quét Nmap. Một công cụ như vậy có thể đặc biệt hữu ích cho các bản quét quy mô lớn là fe3d (<http://projects.icapsid.net/fe3d/>), một công cụ trực quan hóa dữ liệu mà bạn có thể sử dụng để hiển thị đầu ra của quét Nmap ở định dạng đồ họa. Ngoài ra, một số mô-đun Perl được thiết kế đặc biệt để làm việc với Nmap, bao gồm Nmap :: Scanner, Nmap :: Trình phân tích cú pháp và Nmap :: Trình phân tích cú pháp :: XML. Hai mô-đun cuối cùng này cho phép bạn phân tích cú pháp thông qua đầu ra của quét Nmap, tổ chức nó và thực hiện giảm dữ liệu (nghĩa là tìm kiếm các hệ thống hoặc dịch vụ cụ thể, v.v.), khi cần thiết.

Quét một hệ thống thường xuyên hơn cả việc quét các cổng mở và xác định HĐH máy chủ và mọi dịch vụ khả dụng. Ví dụ, quét lỗ hổng có thể hữu ích

một phần của phân tích của bạn và đưa phân tích đó một bước xa hơn. Một số công cụ tuyệt vời để sử dụng cho việc này mục đích là Nessus (www.nessus.org/nessus/) và Sara (www-arc.com/sara/), với Nessus được phổ biến hơn và được biết đến nhiều hơn trong hai. Cả hai công cụ được liệt kê trong top 100 các công cụ bảo mật mạng (<http://sectools.org/>), cùng với một số máy quét ứng dụng khác.

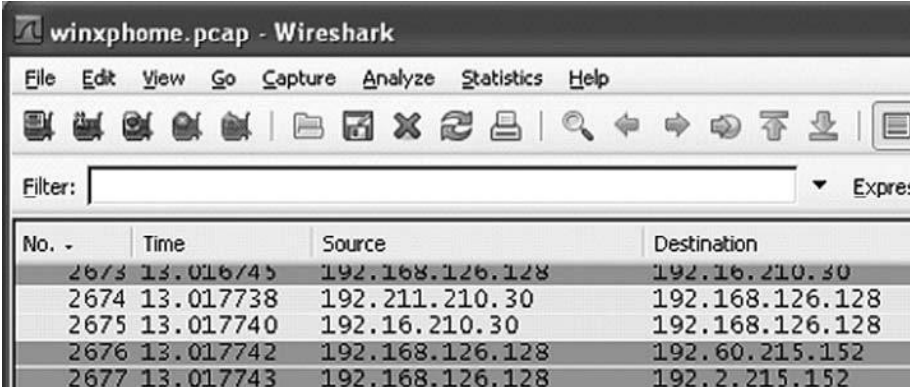
Packet Capture and Analysis

Một hoạt động ứng phó sự cố khác mà bạn có thể gặp phải là chụp và phân tích mạng lưu lượng truy cập. Bất kể bạn có tự mình nắm bắt lưu lượng truy cập mạng hay không, hãy làm việc với tài liệu nhân viên CNTT để đảm bảo lưu lượng truy cập mạng được ghi lại hoặc nhận lưu lượng

truy cập mạng dưới dạng dữ liệu từ người khác, bạn có thể phải đối mặt với cơ hội nắm bắt và phân tích mạng giao thông.

Hai công cụ phân tích và thu thập gói mạng phổ biến cho Windows là Wireshark (www.wireshark.org) và NetworkMin (<http://sourceforge.net/projects/networkminer/>). Cả hai công cụ đều có sẵn miễn phí và cực kỳ có giá trị đối với bộ công cụ của người phản hồi.

Tại thời điểm viết bài này, Wireshark Phiên bản 1.0.3 đã có sẵn cho Windows nền tảng. Wireshark sẽ không chỉ cho phép bạn nắm bắt lưu lượng mạng (dựa trên mạng giao diện bạn chọn) nhưng cũng cho phép bạn phân tích lưu lượng truy cập mạng. Hình 9.5 minh họa một đoạn trích của GUI cho Wireshark.



No. -	Time	Source	Destination
2673	13.016745	192.168.126.128	192.16.210.30
2674	13.017738	192.211.210.30	192.168.126.128
2675	13.017740	192.16.210.30	192.168.126.128
2676	13.017742	192.168.126.128	192.60.215.152
2677	13.017743	192.168.126.128	192.2.215.152

Hình 9.5 Trích đoạn Wireshark v1.0.3 GUI

Một trong những khả năng của Wireshark mà tôi thấy cực kỳ hữu ích là khả năng của nó để lắp ráp lại hoàn toàn các luồng TCP. Để làm điều này, với một bản chụp mạng được tải vào Wireshark, nhấp vào **Phân tích** trong thanh menu và chọn **Theo dõi TCP Stream** từ trình đơn thả xuống thực đơn. Wireshark sẽ theo luồng và lắp ráp lại hoàn toàn nội dung của TCP thông tin liên lạc. Điều này có thể rất hữu ích trong việc cô lập một giao tiếp đơn lẻ, cũng như trong xây dựng lại một cuộc trò chuyện Ví dụ: bạn có thể xây dựng lại các trang web mà người dùng nhìn thấy email, thông tin liên lạc chỉ huy và kiểm soát botnet hoặc nhấn tin tức thời không được mã hóa trao đổi. Wireshark cung cấp khả năng phân tích tương tự với các gói UDP và SSL.

Tools & Traps

Network Traffic Captures

Trong khi chúng ta đang thảo luận về việc bắt giữ lưu lượng truy cập mạng, tôi sẽ đề cập ở đây nơi những nắp này Tures phù hợp với image phản ứng sự cố tổng thể. Nhiều sự cố sẽ liên quan đến một mạng thành phần công việc của một số loại, một hệ thống bị nhiễm bởi thứ gì đó được tải xuống từ Internet và sau đó lây nhiễm sang các hệ thống khác trên mạng, một kẻ xâm nhập giành quyền truy cập vào hệ thống và điều khiển nó, hoặc bot xâm nhập vào hệ thống và tiếp cận với một máy chủ chỉ huy và kiểm soát để chờ lệnh. Không phụ thuộc vào loại sự cố, nhiều sự cố sẽ liên quan đến một thành phần mạng ở một mức độ nào đó.

Đó là nơi lưu lượng truy cập mạng có thể là nguồn dữ liệu cực kỳ quý giá.

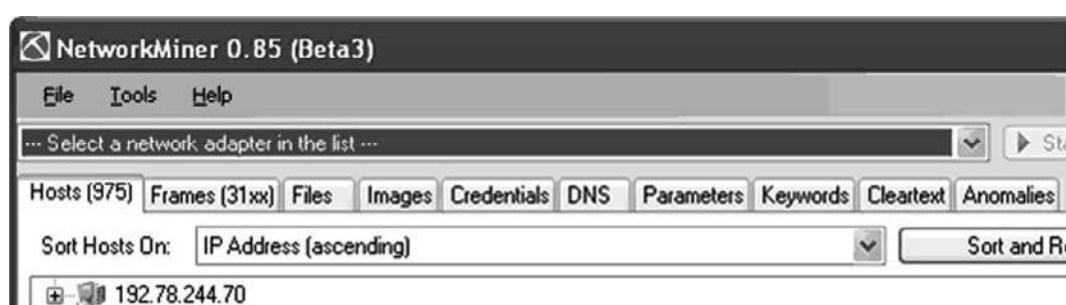
Đầu tiên, bạn sẽ tìm thấy thông tin về chính các gói, bao gồm cả nguồn và địa chỉ IP và cổng đích. Thông tin này cho phép bạn xác định (1) các máy chủ liên quan (dựa trên địa chỉ IP) và (2) chương trình nào có thể tham gia, nếu bạn có thể tương quan thông tin cổng với dữ liệu để bay hơi (đầu ra của tcpvcon.exe, netstat.exe hoặc dữ liệu được phân tích cú pháp từ kết xuất bộ nhớ) được thu thập từ ít nhất một trong số các máy chủ liên quan. Thứ hai, thông tin trong các gói thường được tập hợp lại từ các cuộc hội thoại TCP, có thể hiển thị rất nhiều về dữ liệu được trao đổi. Đây là thông tin có giá trị nếu câu hỏi về việc lọc dữ liệu (nghĩa là, dữ liệu nào đã bị lấy khỏi hệ thống) phát sinh.

Wireshark cũng bao gồm một tùy chọn thanh menu Thống kê, cung cấp cho bạn một số công cụ để giúp bạn thu hẹp trọng tâm hoặc lọc qua một lượng lớn dữ liệu để tìm nghĩa đen đó kim trong một đồng cỏ khô. Bạn có thể nhìn vào số liệu thống kê tổng thể của gói chụp, một danh sách chi tiết các cuộc hội thoại mạng trong gói chụp hoặc chỉ nhận danh sách các điểm cuối. Tất cả điều này có thể rất hữu ích trong việc giúp bạn khai thác thông qua kilobyte hoặc thậm chí là megabyte dữ liệu.

Đôi khi, GUI có thể nhiều hơn một chút so với việc bạn thích làm việc và công cụ CLI có thể được ưa thích hơn. Nếu đó là trường hợp, Wireshark vận chuyển với một số công cụ CLI, bao gồm tshark, tcpdump và dumpcap. Theo thông tin có sẵn trên Wireshark Web trang web, giống

như bất kỳ công cụ nào, mỗi công cụ này đều có điểm mạnh và điểm yếu riêng. Mặc dù các công cụ CLI rất tuyệt để tải lên các hệ thống từ xa và khởi chạy để nắm bắt lưu lượng mạng từ một thay thế vị trí trong mạng, tcpdump theo mặc định sẽ chỉ thu được 68 byte đầu tiên của gói, cắt ngắn thông tin. Một công cụ CLI khác là Windump (www.winpcap.org/windump/), mà không chỉ nắm bắt lưu lượng mạng theo cách tương tự như tshark và dumpcap mà còn có thể được sử dụng với các trình điều khiển thích hợp để nắm bắt lưu lượng mạng thông qua các điểm truy cập không dây.

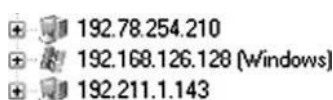
Phiên bản NetworkMiner 0.85 (beta) có sẵn cho Windows. NetworkMiner được mô tả trên trang web của dự án Sourceforge với tên là Công cụ phân tích pháp y mạng (NFAT) cho Windows có thể phát hiện HĐH, tên máy chủ và cổng mở của máy chủ mạng thông qua gói đánh hơi hoặc bằng cách phân tích tệp PCAP. Ngoài ra, mạng NetworkMiner cũng có thể trích xuất được truyền các tệp từ lưu lượng truy cập mạng. Các khả năng này làm cho NetworkMiner trở nên vô cùng quý giá đối với ứng phó sự cố. Như được minh họa trong Hình 9.6, GUI của NetworkMiner có một số tab để hiển thị thông tin được phân tích tự động từ trong các gói chụp mạng, bao gồm các tập tin, thông tin người dùng, image, vv



Hình 9.6 Excerpt of NetworkMiner 0.85 (Beta) UI

Có một công cụ có sẵn cho các hệ thống Linux được gọi là tcpxtract (<http://tcpxtract.sourceforge.net/>; bởi Nick Harbor) là một tiện ích khác tập tin dành cho việc lưu lượng truy cập mạng. Tcpxtract cho phép bạn quét qua lưu lượng truy cập mạng để tìm kiếm các tệp dựa trên một thư viện chữ ký tập tin. Mặc dù tcpxtract không có sẵn cho các hệ thống Windows, NetworkMiner cung cấp chức năng tương tự.

Snapshot từ trang dự án NetworkMiner trên Sourceforge minh họa khả năng của công cụ để xác định hệ điều hành máy chủ bằng cách phân tích các gói bị bắt. NetworkMiner sử dụng chức năng có nguồn gốc từ pOf (<http://lcamtuf.coredump.cx/pOf.shtml>) để xác định lưu trữ hệ điều hành một cách thụ động từ việc bắt gói tin mạng thay vì chủ động quét hệ thống (Nmap). Hình 9.7 minh họa khả năng NetworkMiner chanh để xác định hệ điều hành của máy chủ lưu trữ từ một gói chụp được cung cấp như một phần của một trong các bài tập thực hành pháp y của Lance Mueller.



Hình 9.7 Trích từ NetworkMiner Hiển thị Nhận dạng hệ điều hành máy chủ

Một công cụ đồ họa khác để nắm bắt và phân tích lưu lượng mạng là PacketMon (www.analogx.com/contents/doad/network/pmon.html). PacketMon dường như không được cập nhật tại thời điểm viết bài này, cũng không có vẻ là tính năng phong phú như Wireshark hoặc NetworkMiner, nhưng nó là một công cụ hữu ích để giúp bạn bắt đầu phân tích lưu lượng truy cập mạng.

Một công cụ dòng lệnh (dành cho những người thích loại điều đó) có thể hữu ích với phân tích lưu lượng mạng là ngrep (<http://ngrep.sourceforge.net/doad.html>), một phiên bản của tiện ích GNU grep được áp dụng cho lớp mạng cho phép bạn sử dụng các biểu thức chính quy hoặc thập lục phân mở rộng để tìm kiếm các mẫu trong một lưu lượng truy cập mạng.

Tất cả bốn công cụ này cho phép bạn truy cập lưu lượng truy cập mạng; ba cái đầu tiên là GUI cho phép bạn nắm bắt lưu lượng mạng, ngoài việc phân tích và phân tích nó. Các công cụ này cho phép bạn không chỉ

nắm bắt lưu lượng mạng mà còn hoạt động với các lưu lượng truy cập mạng được cung cấp bởi một nguồn khác. Điều này có nghĩa là nếu bạn đang phản ứng với một sự cố và nhân viên tại chỗ hoặc người phản hồi đầu tiên đã nắm bắt được lưu lượng truy cập mạng, bạn có thể sử dụng các công cụ này để phân tích dữ liệu đó, miễn là bản chụp có định dạng chấp nhận được. Hầu hết các công cụ dễ dàng cung cấp quyền truy cập vào các ảnh chụp định dạng tcpdump, giống như định dạng dd để thu nhận image, có thể được coi là một tiêu chuẩn thực tế cho các lưu lượng truy cập mạng.

TIP

Vào mùa thu năm 2008, NetWitness đã phát hành sản phẩm Investigator miễn phí tại <http://doad.netwitness.com/doad.php?src=DIRECT>. Điều tra viên cho phép nhà phân tích nhanh chóng nhập tệp .pcap chứa lưu lượng truy cập mạng chụp hoặc đơn giản là để nắm bắt lưu lượng mạng thông qua ứng dụng. Điều tra viên được mô tả như là một ứng dụng phân tích mối đe dọa tương tác của bộ sản phẩm NetWitness NextGen, cho phép nhà phân tích thực hiện phân tích ngữ cảnh theo dạng tự do của dữ liệu mạng thô. Đây là một cực kỳ công cụ mạnh mẽ cho nhà phân tích, nhưng hãy chắc chắn đọc giấy phép người dùng cuối thỏa thuận cẩn thận trước khi tải xuống và sử dụng công cụ.

Tools & Traps

Snort

Một công cụ phần mềm miễn phí thường bị bỏ qua để sử dụng trong phân tích pháp y về mạng lưu lượng truy cập là Snort (www.snort.org). Ứng dụng này được biết đến rộng rãi như là một tự do hệ thống phát hiện xâm nhập có sẵn (IDS). Khi tôi lần đầu làm quen với Snort nhiều năm trước, nó là một IDS thẳng, và trong những năm sau đó, đã có một tuyệt vời thỏa thuận của nỗ lực phát triển đưa vào công cụ dẫn đến nó cũng được đề cập đến như là một hệ thống ngăn chặn xâm nhập. Một trong những khả năng của Snort là không chỉ hoạt động bằng cách lắng nghe trên giao diện mạng (được đặt ở chế độ lắng nghe) và lọc lưu lượng truy cập từ một mạng trực tiếp nhưng cũng hoạt động tốt như nhau khi chỉ sử dụng

tập tin chụp lưu lượng mạng. Bằng cách chỉ đạo Snort đọc lưu lượng mạng từ

Tập tin .pcap và xử lý lưu lượng truy cập mạng đã chụp thông qua các bộ quy tắc, bạn đạt được khả năng tương tự như sử dụng ngrep với bộ bộ lọc đóng gói sẵn, một số đó là phức tạp hơn nhiều so với một biểu thức thông thường. Khả năng này có thể cung cấp rất nhiều giảm dữ liệu. Hãy xem xét một trường hợp trong đó có một con sâu mạng tăng sinh trong một cơ sở hạ tầng mạng. Lưu lượng truy cập mạng có thể được sử dụng để xác định hệ thống nào đang liên lạc trên mạng và trong các mạng lớn có thể có rất nhiều thông tin liên lạc mạng mạng bình thường có thể dễ dàng áp đảo các nhà phân tích. Sử dụng Snort (và giả sử rằng có một chữ ký cho truyền thông mạng của worm), bạn có thể nhanh chóng phân loại kim từ đồng cỏ khô, thực hiện rất nhiều giảm dữ liệu với mức độ chi tiết vượt quá mức đó của các công cụ khác.

Search Utilities

Bất cứ khi nào tôi nói chuyện với các nhà phân tích đồng nghiệp về khả năng cốt lõi của phân tích pháp y và ứng dụng hỗ trợ hoạt động đó, một trong những khả năng chính mà tôi nghe thấy như một yêu cầu cho bất kỳ ứng dụng đó là khả năng chạy các tìm kiếm, bao gồm các tìm kiếm từ khóa và kiểu grep tìm kiếm bằng cách sử dụng các biểu thức thông thường. Tìm kiếm thường được sử dụng như một kỹ thuật giảm dữ liệu; sử dụng từ khóa hoặc cụm từ thông dụng, nhà phân tích có thể kết hợp thông qua megabyte hoặc thậm chí gigabyte dữ liệu, tìm kiếm các mục (tệp, mục nhập tệp nhật ký, v.v.) dành riêng cho mình mục tiêu phân tích.

Tools & Traps ...

Searching the Registry

Tìm kiếm hầu hết các tệp trên hệ thống Windows để tìm dữ liệu có định dạng ASCII hoặc Unicode là gen- bên trong một quá trình đơn giản. Tuy nhiên, các tệp hive của Registry có thể gây ra một số điều thú vị các vấn đề. Chẳng hạn, bạn là một nhà phân tích cần hết sức chú ý đến các đường dẫn bên trong cơ quan đăng ký. Đường dẫn Phiên bản phiên bản trực tuyến rất khác với Trình quản lý phiên phiên bản.

Tương tự, nếu một khóa hoặc giá trị nằm trong đường dẫn bao gồm Windows NT, thì đừng tạo sai lầm khi tìm kiếm Windows

WindowsNT. Như với hầu hết các tìm kiếm, chính tả là rất quan trọng-trên chộc Tuy nhiên, bên cạnh đó, không phải tất cả thông tin đều được lưu giữ trong Sổ đăng ký trong định dạng ASCII hoặc Unicode gọn gàng. Một số thông tin được mã hóa theo giá trị DWORD (4 byte), và giá trị phải được ánh xạ tới một khóa để được giải thích. Trong một số trường hợp, DWORD giá trị '0' có thể có nghĩa là chức năng được bật, trong khi đối với các giá trị khác, a giá trị của '1' có thể có nghĩa là kích hoạt. Bật trong các trường hợp khác, chức năng nhất định sẽ là được mã hóa trong một giá trị nhị phân theo một cách nào đó. Vì vậy, đừng ngạc nhiên nếu một từ khóa hoặc tìm kiếm biểu thức thông thường không cung cấp chỉ dẫn về những gì bạn đang tìm kiếm trong các tập tin tổ ong. Chìa khóa để tìm kiếm Registry đôi khi là để biết những gì bạn đang tìm kiếm và tập trung tìm kiếm với một quy trình thủ công

Các tiện ích tìm kiếm được liệt kê trong phần này có nghĩa là được sử dụng đối với các tệp trực tiếp, có nghĩa là rằng chúng có thể được sử dụng trong tình huống phản hồi trực tiếp hoặc sau khi bạn đã gắn một image thu được như một hệ thống tập tin trực tiếp. Hầu hết các ứng dụng phân tích pháp y thương mại cung cấp một tìm kiếm tích hợp khả năng (một số, chẳng hạn như FTK và X-Way Forensics, cũng cung cấp khả năng lập chỉ mục), như cũng như một số chuỗi tìm kiếm biểu thức thông thường được cấu hình sẵn.

Một nguồn tiện ích tuyệt vời để tìm kiếm tệp và hệ thống tệp là các tiện ích GNU cho trang web Win32 (<http://unxutils.sourceforge.net/>). Trang web này cung cấp quyền truy cập vào một kho lưu trữ các tiện ích kiểu UNIX cung cấp rất nhiều chức năng thông qua các tiện ích mà nhiều tiện ích Các quản trị viên UNIX đã quen thuộc, mặc dù thực tế đây là tất cả các phiên bản Windows gốc Sions của các công cụ. Các công cụ này có thể dễ dàng được thêm vào các tệp bó và tập lệnh để sử dụng trong mỗi hình thành các tìm kiếm và các hoạt động giảm dữ liệu khác.

Ngoài các công cụ này, có một số phiên bản của tiện ích grep có sẵn cho nền tảng Windows. Trên thực tế, có hai phiên bản như vậy của tiện ích này, cả hai đều được gọi là grep cho Các cửa sổ"; một cái có sẵn từ Sourceforge (<http://gnuwin32.sourceforge.net/packages/grep.htm>) và cái khác có sẵn từ InterLog

(<http://pages.interlog.com/~tcharron/grep.html>). Cả hai đều cung cấp chức năng tương tự.

Có những trường hợp bạn có thể muốn tìm kiếm các mục hoặc thuật ngữ cụ thể, chẳng hạn như dưới dạng số An sinh xã hội (SSN) hoặc số thẻ tín dụng (CCN). Những mặt hàng nằm trong định nghĩa về dữ liệu nhạy cảm của người Viking, được xác định bởi những điều như luật của tiểu bang California SB-1386 và tiêu chuẩn bảo mật dữ liệu (DSS) của Thẻ thanh toán (DSS), tương ứng. Như vậy, có thể đôi khi bạn sẽ cần tìm kiếm loại dữ liệu này như một chức năng cụ thể phân tích của bạn. May mắn thay, có một số công cụ có sẵn có thể được sử dụng để đáp ứng những nhu cầu. Một công cụ như vậy là Cornell Spider (www.cit.cornell.edu/security/tools/), trong đó được thiết kế để quét các bộ sưu tập tệp (tệp trên ổ cứng, trang web, v.v.) cho nhạy cảm dữ liệu như SSN và CCN. Chạy Spider kết quả trong một tệp nhật ký của tất cả các tệp có chứa dữ liệu nhạy cảm.

Một công cụ hữu ích khác để tìm kiếm CCN là ccsrch (<http://sourceforge.net/projects/ccsrch>). Ccsrch là một tiện ích dòng lệnh dựa trên Windows có thể tìm kiếm liên kết và CCN không được mã hóa, cũng như dữ liệu theo dõi. Định dạng thông số kỹ thuật cho theo dõi thẻ tín dụng 1 và 2 dữ liệu bao gồm CCN hoặc số tài khoản chính (PAN) dưới dạng dữ liệu liên kết; đó là, một chuỗi các số không có dấu ngắt, dấu cách hoặc dấu gạch ngang. Kết quả Ccsrch bao gồm tên tệp cũng như số được tìm thấy, gửi đến đầu ra tiêu chuẩn (STDOUT), cho phép kết quả dễ dàng chuyển hướng đến một tệp tin.

Sau đây là các tài nguyên hữu ích để hỗ trợ bạn trong các tìm kiếm của bạn:

- Tham chiếu biểu thức chính quy ([www.thường-expressions.info /](http://www.thường-expressions.info/))
- Định dạng số thẻ tín dụng (http://en.wikipedia.org/wiki/Credit_card_number)
- Biểu thức thông thường cho số thẻ tín dụng (www.thường-expressions.info /thẻ_tín_dụng.html)

Tools & Traps ...

Search for Sensitive Data

Khi tìm kiếm dữ liệu nhạy cảm dưới mọi hình thức, bạn cần đảm bảo rằng bạn hoàn toàn hiểu bản chất và định dạng của dữ liệu đó, cũng như kết quả của dữ liệu của bạn tìm kiếm thực sự có ý nghĩa. Cụ thể, SSN và CCN đặt ra một số thách thức thú vị với liên quan đến định dạng. Hầu hết các nhà phân tích nhận ra định dạng của những con số này, nhưng chúng tôi cần đảm bảo rằng các tìm kiếm CCN gồm 16 chữ số (ví dụ) bao gồm các tìm kiếm đáp ứng các tiêu chí cần thiết không chỉ cho CCN (nghĩa là độ dài, chữ số bắt đầu và Luhn kiểm tra công thức / Modulus-10) nhưng cũng cho một dãy số thẳng không có ngắt, cũng như các chuỗi số có dấu cách hoặc dấu gạch ngang phù hợp các vị trí trong chuỗi.

Một vấn đề khác của việc tìm kiếm dữ liệu nhạy cảm là kiểm tra các công cụ của bạn và xác định định dạng của dữ liệu họ tìm kiếm. Một số công cụ có thể chỉ tìm kiếm tiếp giáp chuỗi số (như với CCN hoặc SSN), trong khi các số khác có thể bao gồm tìm kiếm cho những số được định dạng bằng dấu cách hoặc dấu gạch ngang.

Summary

Nền tảng cho một bài kiểm tra không phải là công cụ bạn đang sử dụng; đó là phương pháp của bạn. Một phương pháp tốt không phụ thuộc vào công cụ được sử dụng, cho dù đó là một pháp y thương mại bộ phân tích, một công cụ mã nguồn mở miễn phí hoặc tập lệnh Perl được chế tạo tùy chỉnh. Các phím là để biết những câu hỏi bạn cần trả lời, đi đâu để lấy dữ liệu của bạn và sau đó làm thế nào để trích xuất và giải thích chính xác dữ liệu đó trong một báo cáo. Giữ nguyên tắc đó và nguyên tắc cốt lõi của bạn tâm trí sẽ dẫn bạn tiếp cận với công cụ phù hợp, cho dù đó là trích xuất dữ liệu để phân tích hoặc để chứng thực những phát hiện khác.

Solutions Fast Track

Documenting Your Analysis

Tài liệu là một phần cực kỳ quan trọng của bất kỳ kỳ thi nào. Tài liệu, phải rõ ràng, súc tích và đủ kỹ lưỡng để cho phép nhân rộng sau này và xác minh, đặc biệt bởi một nhà phân tích khác.

Nhiều người và người trả lời CNTT phải lấy dữ liệu hoặc bằng chứng mà họ có được, tòa án và phải quan tâm đến các tiêu chuẩn cần phải được đáp ứng để làm như vậy. Sự khác biệt chính giữa việc chạy

xung quanh với một đĩa CD đầy đủ các công cụ và đưa dữ liệu của bạn ra tòa là tài liệu bạn duy trì: Bạn có ghi lại quá trình và bạn đã ghi lại hành động của mình đến mức chúng dễ hiểu và lặp lại?

Tools

Một số công cụ miễn phí hoặc chi phí thấp có sẵn có thể nhiều hơn mức vừa đủ thay thế hoặc thậm chí mở rộng chức năng vốn có cho nhiều thương mại gói ứng dụng. Với một số kiến thức và suy nghĩ trước, bạn có thể gia tăng, thay thế, hoặc thậm chí vượt qua những gì có sẵn trong các ứng dụng đó.

Cũng như các khía cạnh khác của phản ứng sự cố và pháp y máy tính, khác nhau các ứng dụng thương mại có sẵn có điểm mạnh và điểm yếu của họ. Có lẽ quan trọng là sử dụng một ứng dụng thương mại để phân tích dữ liệu và trình bày. Tuy nhiên, cũng có thể đôi khi một công cụ có sẵn miễn phí cung cấp một mức độ sâu hơn hoặc khả năng hiển thị vào dữ liệu và cung cấp câu trả lời nhanh hơn nhiều.

Các câu hỏi thường gặp

Q: Tôi cần thực hiện phân tích dữ liệu tôi đã thu thập; Tôi sử dụng công cụ gì?

A: Cũng như mọi thứ khác, nó phụ thuộc vào. Nghiêm túc. Trước khi quyết định sử dụng công cụ nào, bạn cần xem xét kỹ và ghi lại các mục tiêu phân tích của mình bởi vì điều đó nơi mọi thứ bắt đầu và kết thúc cho một cuộc kiểm tra. Bạn có đang tìm kiếm image bất hợp pháp không? Bạn có lo lắng về việc ai (tức là, tài khoản người dùng nào) có thể đã tải xuống, truy cập hoặc xem những image đó không? Bạn có vài megabyte hoặc thậm chí hàng gigabyte bản ghi IIS và bạn có quan tâm đến việc xác định liệu có xảy ra một cuộc tấn công SQL SQL hay không? Không có một công cụ nào phù hợp với mọi tình huống và trong nhiều trường hợp, công cụ được sử dụng phụ thuộc vào sở thích cá nhân của nhà phân tích; Tôi đã thực hiện phân tích trên các tệp nhật ký bằng Perl, trong khi những người khác thích sử dụng Microsoft Pars Log Parser.

Q: Làm thế nào để lưu lượng truy cập mạng hữu ích cho một kỳ thi?

A: Lưu lượng truy cập mạng chứa rất nhiều thông tin hữu ích mà bạn có thể liên kết đến một hệ thống (địa chỉ IP) cũng như một quy trình chạy trên hệ thống đó bằng cách tương quan thông tin cổng trong các tiêu đề gói đến dữ liệu để bay hơi (kết nối mạng, xử lý, ánh xạ quá trình tới cổng) từ hệ thống. Nội dung của các gói có thể cho bạn biết dữ liệu hoặc thông tin nào được truyền đến hoặc từ hệ thống.

Q: Trong khi kiểm tra, tôi có nhiều nguồn dữ liệu cần tương quan và tôi cần duy trì sự liên kết giữa chúng (ví dụ: chụp gói mạng, mạng nhật ký thiết bị, nhật ký máy chủ và image hệ thống). Cách tốt nhất để làm điều này là gì?

A: Tại thời điểm này, tài liệu. Tôi không biết về bất kỳ bộ phân tích hoàn chỉnh nào cho phép bạn kéo vào, phân tích và tương quan nhiều nguồn dữ liệu, ngoài PyFlag.