ows ForAnalysis

Phòng chống và điều tra tội phạm máy tính

Dịch:Windows Forensic Analysis

Chapter 7: Rootkits and Rootkit Detection

Giảng viên: Lại Minh Tuấn

Nhóm: Lê Tuấn Tú

Đào Cư Thuận

Đỗ Thị Hằng

Mục Lục

[Giới thiệu 3](#_Toc26456491)

[Rootkits 4](#_Toc26456492)

[Phát hiện Rootkit 11](#_Toc26456493)

# Giới thiệu

Tại Hội nghị RSA vào tháng 2 năm 2005, Mike Danseglio và Kurt Dillard, cả hai đều đến từ Microsoft, đã đề cập đến từ rootkit, và những tháng sau đó đã chứng kiến ​​một loạt các hoạt động khi các chuyên gia của Nott phát hiện ra về rootkit và các công ty phần mềm sản xuất các công cụ để phát hiện ra chúng. Mặc dù rootkit đã tồn tại trong nhiều năm, bắt nguồn từ UNIX và sau đó di chuyển sang Windows nhưng vấn đề này phần lớn đã bị hiểu lầm và ở một số góc thậm chí bị bỏ qua.

Hội nghị năm 2005 đã gia tăng sự quan tâm đến rootkit và các công cụ phát hiện rootkit thương mại đã được công bố ngay sau đó. (Đã có một số công cụ và phương pháp phần mềm miễn phí có sẵn trong một thời gian.) Khi các kỹ thuật phát hiện đã được cải thiện, các tác giả rootkit đã nghĩ ra những cách mới để lật đổ hệ điều hành và thậm chí cả kernel trong các nỗ lực vẫn không bị phát hiện.

Các mối đe dọa rootkit là có đáng kể? Không có câu hỏi về điều đó. Rootkit có thể che giấu sự hiện diện của các công cụ khác, chẳng hạn như keylogger, trình thám thính mạng và backtime truy cập từ xa, không chỉ từ người dùng mà còn từ hệ điều hành. Bản chất ngấm ngầm của rootkit có thể gây ra sự cố khi chúng thực sự có mặt cũng như khi họ không nhưng những người phản ứng sự cố cho rằng họ đã bị, do thiếu kiến ​​thức và đào tạo. Giả sử (không có bất kỳ dữ liệu cốt lõi nào để sao lưu) rằng rootkit đã được cài đặt trên hệ thống hoặc cơ sở hạ tầng có thể dẫn một nhà điều tra hoặc người quản lý sự cố đi xuống một con đường không chính xác liên quan đến các phản ứng và quyết định dựa trên đánh giá sự cố sai lệch. Các tài nguyên đáng kể có thể được đầu tư vào các hoạt động không cần thiết hoặc hệ thống có thể bị xóa sạch tất cả dữ liệu và được cài đặt lại từ phương tiện sạch, tất cả mà không xác định nguyên nhân gốc, và sau đó được tái sử dụng ngay sau khi được đưa trở lại dịch vụ.

# Rootkits

Vậy, rootkit là gì? Một podcast Sophos được phát hành vào ngày 24 tháng 8 năm 2006, bao gồm. Kết quả của một cuộc thăm dò do Sophos thực hiện, 37% số người được hỏi không biết định nghĩa của rootkit.Wikipedia định nghĩa một rootkit là một bộ công cụ phần mềm dự định Che giấu các quy trình, tệp hoặc dữ liệu hệ thống đang chạy từ hệ điều hành. Ở phần đầu tiên của loạt bài viết gồm ba phần về rootkit được xuất bản trên SecurityF Focus, Jamie Butler, một chuyên gia được đánh giá cao về công nghệ rootkit và Sherri Sparks xác định một rootkit như sau:

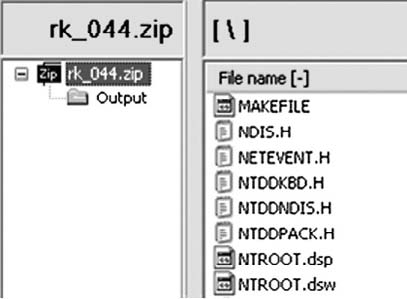
Một chương trình hoặc tập hợp các chương trình mà kẻ xâm nhập sử dụng để che giấu sự hiện diện của cô ấy trên hệ thống máy tính và cho phép truy cập vào hệ thống máy tính trong tương lai. Để thực hiện mục tiêu của mình, một rootkit sẽ thay đổi luồng thực thi của hệ điều hành hoặc thao tác tập dữ liệu mà hệ điều hành dựa vào để kiểm toán và ghi sổ.

Một cách nhìn khác là rootkit là một chương trình phần mềm sửa đổi hệ điều hành để nó có khả năng ẩn chính nó và các đối tượng khác khỏi người dùng, quản trị viên và thậm chí cả hệ điều hành.

Rootkit được sử dụng để ẩn các tiến trình, kết nối mạng, khóa Registry, tệp và những thứ tương tự từ hệ điều hành và, bằng cách mở rộng, quản trị viên. Thuật ngữ rootkit đến từ UNIX, nơi các công cụ như vậy thường được sử dụng để đạt được và / hoặc duy trì quyền truy cập cấp độ gốc root (giống như Quản trị viên trên Windows) vào hệ thống. Vì chức năng tương tự được phát triển trong phần mềm độc hại trên Windows, tên này đã thực hiện một quá trình chuyển đổi tương tự cùng với các công cụ.

Một trong những rootkit đầu tiên được phát triển cho Windows là NTRootkit, được viết bởi Greg Hoglund và phát hành năm 1999. NTRootkit bao gồm một trình điều khiển và vẫn có sẵn với mã nguồn, như minh họa trong Hình 7.1.

**Hình 7.1 Lưu trữ NTRootkit 0.44 Hiển thị tệp nguồn**



Kể từ đó, nghiên cứu quan trọng đã đi vào sự phát triển của công nghệ rootkit và rootkit. Hoglund và những người khác đã tiến hành các lớp học tại Hội nghị Bảo mật BlackHat và các hội nghị khác về cách viết rootkit, và trang web của anh ấy(Rootkit.com), đã trở thành trang web ưu việt về kiến ​​thức, phát triển và chia sẻ thông tin của Windows rootkit. Trong những năm qua, các rootkit khác đã xuất hiện và sự phát triển của các kỹ thuật rootkit mới vẫn không ngừng phát triển. Ngoài ra còn có một cuốn sách tuyệt vời có sẵn trên rootkit, cách chúng được thiết kế và cách chúng hoạt động: *Rootkits: Subverting the Windows Kernel*. Cuốn sách này được viết bởi Greg Hoglund và Jamie Butler và có sẵn trên Amazon.com.

Ngay sau Hội nghị RSA vào tháng 2 năm 2005, đã có những quan tâm đến việc phát hiện rootkit và rootkit, và khi các kỹ thuật phát hiện trở nên tinh vi hơn, thì rootkit cũng vậy. Theo xu hướng là một chiến trường ngày càng leo thang, với sự phát triển ở một phía thúc đẩy sự phát triển hơn nữa trên khác.

Có một số loại rootkit khác nhau. Các phiên bản gốc của rootkit hoạt động bằng cách thay thế các tiện ích và ứng dụng của hệ điều hành bằng các phiên bản Trojan đã được kích hoạt để khi phiên bản tiện ích Trojan được chạy, nó được lập trình để không hiển thị các đối tượng cụ thể. Ví dụ, Trojan Trojaning lệnh netstat trước tiên sẽ xóa các kết nối mạng Kẻ tấn công khỏi danh sách tệp và sau đó hiển thị các kết nối mạng còn lại như bình thường.

Sau đó, đến lượt tiêm DLL hoặc rootkit chế độ người dùng. Các rootkit này cài đặt trong ngữ cảnh bảo mật của người dùng hiện đang đăng nhập vào hệ thống và thay thế hoặc vá các hàm gọi hệ điều hành khác nhau hoặc các hàm DLL. Để đặt ví dụ netstat của chúng tôi trong ngữ cảnh của rootkit chế độ người dùng, thay vì thay thế netstat, một rootkit chế độ người dùng sẽ kết nối các lệnh gọi hàm Windows API để các hàm đó không trả về một danh sách đầy đủ tất cả các kết nối mạng. Lệnh netstat sau đó tiến hành hiển thị tất cả thông tin mà nó nhận được từ lệnh gọi hàm, không biết rằng nó đã được cung cấp thông tin không đầy đủ và sai lệch. Kết nối các lệnh gọi chức năng được liệt kê cũng ẩn các kết nối mạng khỏi bất kỳ chương trình nào khác sử dụng cùng các hàm API. Chế độ người dùng. Rootkit ẩn các tệp sẽ móc các hàm gọi FindFirstFile () và FindNextFile () để không có chương trình nào sử dụng các lệnh gọi hàm này, kể cả shell (tức là Windows Explorer), sẽ thấy các tệp mà rootkit đang ẩn.

Ví dụ về rootkit chế độ người dùng bao gồm, nhưng không giới hạn ở những điều sau:

* AFX Rootkit 2005 là một rootkit mã nguồn mở được viết bằng Delphi (bởi Aphex) sử dụng hàm DLL và hook API để ẩn các tệp, khóa Registry, quy trình và những thứ tương tự.

Hacker Defender (từ Hxdef.org, bởi Holy\_ Father) có lẽ là rootkit phổ biến và phổ biến nhất hiện có. Trang web F-Secure mô tả Hacker Defender là rootkit được triển khai rộng rãi nhất trên thế giới. Hacker Defender cũng sử dụng chuyển hướng cổng để các phương tiện phát hiện rootkit truyền thống, chẳng hạn như quét cổng từ xa, không thể phát hiện cửa hậu được thực hiện bởi rootkit. Hacker Defender sử dụng một tệp cấu hình, có thể tìm thấy trong nội dung của bộ nhớ vật lý được thu thập từ một hệ thống bị nhiễm. Các phần của tệp cấu hình có thể được tìm thấy trong bộ nhớ vật lý; Nó có thể phục hồi toàn bộ tập tin. Hơn nữa, một cuộc kiểm tra bộ nhớ vật lý nhìn thấy ngay thông qua Hacker Defender; Người kiểm tra có thể thấy tất cả các quy trình mà nó đang ẩn. Người kiểm tra phải so sánh các quy trình đang chạy trong phân tích bộ nhớ với danh sách được trình bày bởi hệ điều hành để biết những quy trình nào đang bị ẩn bởi rootkit.

NTIllusion (www.securiteam.com/securityreviews/5FP0E0AGAC.html) được thiết kế để có thể lây nhiễm một hệ thống, chạy theo các đặc quyền thấp nhất có sẵn, lật đổ các quy trình do người dùng hiện tại sở hữu.

Vanquish là một rootkit tiêm DLL của Rumani có thể ẩn các tệp, quy trình, khóa Registry và tương tự.Vanquish bao gồm một trình tải tự động (tệp .exe) và DLL, bao gồm sáu tệp con. đúng và, theo tệp readme đi kèm với bản phân phối, không hoạt động khi các rootkit khác có mặt trên hệ thống.

Gromozon (www.antirootkit.com/articles/gromozo/The-strange-case-of-Dr- Rootkit-and-Mr-Adware.htmlm) là một rootkit chế độ người dùng lây nhiễm vào hệ thống thông qua một đối tượng trợ giúp trình duyệt (BHO ) và sử dụng nhiều kỹ thuật để duy trì sự bền bỉ trên hệ thống bị nhiễm (ẩn mã trong tệp EFS và luồng dữ liệu thay thế NTFS, tạo dịch vụ, tạo tham chiếu trong khóa Sổ đăng ký AppInit\_DLL và tương tự). Ngoài ra, rootkit loại bỏ đặc quyền Debug khỏi tài khoản người dùng để ngăn chặn các công cụ phát hiện rootkit hoạt động bình thường. Viết lên Symantec trên rootkit này mô tả nó như là spaghetti spaghetti do các phương pháp kiên trì khác nhau mà các tác giả đã thiết kế thành mã. Nhiều rootkit có sẵn để tải xuống trực tuyến và trong nhiều trường hợp tại Rootkit.com

Nguy hiểm hơn nhiều là các rootkit chế độ kernel của chế độ kernel vì chúng phá hoại chính kernel của hệ điều hành. Các rootkit chế độ kernel không chỉ chặn các cuộc gọi API cấp thấp mà còn xử lý các cấu trúc dữ liệu kernel. Một ví dụ về rootkit chế độ kernel là FU, được phát triển bởi Jamie Butler, sử dụng một kỹ thuật gọi là thao tác đối tượng kernel trực tiếp (DKOM) để ẩn trên hệ thống. DKOM là quá trình thao tác các cấu trúc dữ liệu cấp hạt nhân mà không cần sử dụng API Windows. Ví dụ, nhân Windows duy trì

một danh sách vòng tròn được liên kết đôi của tất cả các quy trình đang chạy trên hệ thống và FU sẽ xóa các quy trình được yêu cầu khỏi danh sách. Các quy trình vẫn còn đó nhưng không được thấy bởi kernel. Lượng tử lập lịch cho hệ thống là một luồng, không phải là một quá trình, do đó, luồng FU tiếp tục chạy trong khi quá trình này là vô hình đối với hệ thống. FU sử dụng trình điều khiển, được đặt tên là msdirectx.sys theo mặc định, để có quyền truy cập và kiểm soát hệ thống. Chương trình FU, fu.exe, chấm dứt sau khi tải trình điều khiển vào bộ nhớ.

Các rootkit chế độ kernel cũng có thể phá hủy các cấu trúc kernel khác. Rootkit FUTo (www.unin- Form.org/?v=3&a=7), được phát hành như là sự kế thừa cho rootkit FU, được thảo luận rất dài trong tập 3 của Tạp chí thống nhất (www.uninformed.org, phát hành vào tháng 1 năm 2006). FUTo mở rộng các khả năng của FU FU DKOM bằng cách sử dụng mã ngôn ngữ lắp ráp (chứ không phải các lệnh gọi API) để thao tác biến PspCidTable, là con trỏ tới bảng xử lý để xử lý ID khách hàng xử lý và xử lý. Bảng xử lý này được sử dụng để theo dõi tất cả các định danh quy trình.

Shadow Walker là một rootkit chế độ kernel bằng chứng khái niệm đã được thảo luận tại hội nghị BlackHat 2005. Dựa trên rootkit FU, Shadow Walker chứa một trình điều khiển bổ sung thao tác trình quản lý bộ nhớ để che giấu sự tồn tại của các tập tin rootkit. Tóm lại, Shadow Walker thực hiện điều này bằng cách đảm bảo rằng tất cả các trang bị ẩn trong bộ nhớ không được phân vùng

và bằng cách chặn tất cả các quyền truy cập vào các trang đó. Khi hệ điều hành yêu cầu đọc các trang đó, rootkit sẽ trả về các trang của số không. Khi hệ điều hành yêu cầu thực thi các trang đó, nó sẽ trả về mã độc. Bạn có nhớ cảnh trong bộ phim Chiến tranh giữa các vì sao trong đó Obi-Wan Kenobi đã nói với chỉ huy StormTrooper, Đây không phải là những droid mà bạn đang tìm kiếm? Vâng, chỉ như vậy.

Một điều lưu ý đối với các rootkit chế độ kernel là chúng cũng có thể khiến hệ thống chuyển sang màn hình xanh lam nếu chúng không được viết đúng. Nhân viên hỗ trợ của Microsoft đã giúp nhiều khách hàng theo dõi các BSoD lặp đi lặp lại (Màn hình xanh chết chóc đáng sợ), chỉ để thấy rằng một rootkit chế độ kernel là vấn đề. Như đã đề cập trong Chương 3, một bãi chứa sự cố hoặc BSoD sẽ gây ra

một tệp kết xuất sự cố được ghi vào ổ cứng và nhân viên hỗ trợ có thể sử dụng tệp này để chẩn đoán sự cố. Thông thường, đây là cách một rootkit (một biến thể được biết đến hoặc có thể là một biến thể mới) được phát hiện trên một hệ thống.

Đôi khi, thuật ngữ rootkit được sử dụng theo cách hơi lười biếng.

Một mục thú vị trong nhật ký Web Phản hồi bảo mật của Symantec từ tháng 9 năm 2006 có tiêu đề Root The Poor Man's Rootkit. Trong phần đó, tác giả mô tả một chút phần mềm độc hại có tên Trojan.Zonebac sử dụng kỹ thuật ngụy trang để che giấu sự hiện diện của nó trên hệ thống . Nói tóm lại, trong quá trình cài đặt, Trojan sẽ quét nội dung của khóa Run phổ biến và chọn một ứng dụng thường được sử dụng. Nó sao lưu hình ảnh thực thi cho tệp được trỏ đến bởi giá trị Registry và tự ghi vào hệ thống tệp bằng tên của tệp gốc. Khi hệ thống được khởi động, Trojan sẽ tự động chạy và sau đó nó cũng chạy tệp được sao lưu, do đó không có gì xuất hiện. Hơn nữa, thời gian LastWrite của phím Run không được cập nhật do không có thay đổi thực tế nào được thực hiện đối với khóa.

Mặc dù đây thực sự là một phương pháp mới lạ và thậm chí khéo léo để ẩn trên một hệ thống, nhưng nó không phải là một rootkit. Trong thực tế, ẩn trong tầm nhìn rõ ràng bằng cách đổi tên hình ảnh thực thi phần mềm độc hại thành một cái gì đó vô hại là một thực tế phổ biến và hiệu quả. Không có gì lạ khi loại kỹ thuật này được liệt kê dưới đây, hack hack admin hoặc hack hack examiner, chứ không phải hack hack máy chủ.

**Chú ý**

Dựa vào không có gì ngoài tên của một tệp để chẩn đoán vấn đề có thể gây hiểu nhầm và thậm chí có thể khiến một nhà điều tra bỏ lỡ hoàn toàn nguyên nhân gốc rễ thực sự của vụ việc. Quá thường xuyên, quản trị viên sẽ tìm thấy một tệp đáng ngờ và Google tên tệp. Sau đó, anh ấy sẽ thấy rằng có một tệp Microsoft hợp pháp có tên đó và do đó tuyên bố sự cố đã được đóng lại. Điều này không chỉ áp dụng cho quản trị viên; Tôi đã thấy các nhà phân tích phần mềm độc hại làm điều tương tự. Tuy nhiên, tôi cũng đã thấy các trường hợp phần mềm độc hại được cài đặt trên hệ thống sử dụng tên của tệp Microsoft hợp pháp, chẳng hạn như alg.exe hoặc svchost.exe. Trong hầu hết các trong số các trường hợp mà tôi đã tham gia, quản trị viên đã tìm thấy tính hợp pháp của người Hồi giáo này và không tìm kiếm gì thêm. Không ai nhận thấy rằng các hình ảnh thực thi không nằm trong thư mục system32, ví dụ. Vấn đề là bạn không thể chỉ dựa vào tên tệp như một phương tiện để xác định tệp và ảnh hưởng của nó đối với hệ thống hoặc cơ sở hạ tầng.

Rootkit cũng đã được sử dụng thương mại. Không chỉ có một số tác giả rootkit phân nhánh để cung cấp rootkit tùy chỉnh cho bất kỳ ai sẵn sàng trả phí của họ mà cả các tập đoàn đã sử dụng rootkit để ẩn chức năng. Vào ngày 31 tháng 10 năm 2005, Mark Russinovich (nổi tiếng của SysIternals, giờ là Microsoft) đã thông báo trên blog của mình rằng ông đã phát hiện ra rằng Sony Corporation đang sử dụng rootkit trong nỗ lực ảnh hưởng đến quản lý quyền kỹ thuật số và bảo vệ tài sản của mình.

Trong số những thứ khác, Mark chỉ ra rằng không chỉ việc sử dụng rootkit này mà người đã mua CD nhạc và cài đặt phần mềm trên máy tính của cô ấy (người dùng không được cảnh báo rõ ràng về việc sử dụng rootkit, cũng không phải được liệt kê trong thỏa thuận cấp phép người dùng cuối) nhưng một kẻ tấn công đã tìm thấy phần mềm này được cài đặt trên hệ thống có thể tận dụng lợi thế của nó và cài đặt các công cụ của riêng mình, sau đó sẽ được ẩn dưới chiếc ô của Sony. Kể từ khi phát hiện ra vấn đề này và sự giận dữ tiếp theo, Mark đã chuyển sang được Microsoft tuyển dụng. Mục nhập blog Mark Mark được lưu trữ tại trang web Virus Bulletin.

|  |
| --- |
| Chia sẻ thông tin  Trong mục blog của mình liên quan đến vấn đề rootkit của Sony (tại trang Virus Bulletin), Mark đưa ra tuyên bố sau:  Cho đến vài năm trước, chúng tôi đã cung cấp mã nguồn cho Regmon một cách công khai, điều này dẫn đến việc sử dụng các chức năng móc nối và các thói quen hỗ trợ của chúng tôi trong ví dụ NTRootkit được công bố trên www.rootkit.com. Cấu trúc của mã trong Aries chỉ ra rằng nó có khả năng được lấy từ mã NTRootkit.  Thật thú vị khi thấy các nguồn khác nhau được sử dụng để tiếp tục phát triển các ứng dụng, bao gồm cả phần mềm độc hại. Trong trường hợp này, việc sử dụng các chức năng móc đã đến vòng tròn đầy đủ. |

Mark và những người khác đã khám phá việc sử dụng rootkit của các tập đoàn trong các sản phẩm phần mềm của họ và vào ngày 10 tháng 1 năm 2006, Symantec (www.symantec.com/avcenter/security/Content/ 2006.01.10.html) đã phát hành thông tin cho biết Tái chế bảo vệ Norton Bin cũng sử dụng chức năng giống như rootkit.

# Phát hiện Rootkit

Bây giờ chúng ta đã thấy một chút gì đó về rootkit là gì và chúng có thể làm gì, làm thế nào để phát hiện sự hiện diện của rootkit trên hệ thống? Để trả lời câu hỏi này, chúng ta hãy xem xét hai chế độ phát hiện, trực tiếp và hậu hiện đại. Trong chế độ phát hiện trực tiếp, kịch bản cơ bản là chúng tôi đã có một hệ thống đang chạy và chúng tôi sẽ cố gắng xác định xem có rootkit trên hệ thống hay không. Trong chế độ phát hiện hậu kỳ, chúng tôi làm việc với một hình ảnh thu được của hệ thống. Một trong những lợi ích của việc sử dụng cả hai chế độ phát hiện là việc phát hiện rootkit hiệu quả thực sự đòi hỏi sự kết hợp của nhiều kỹ thuật khác nhau được thảo luận trong các chương khác của cuốn sách này, chẳng hạn như phân tích bộ nhớ, phân tích hệ thống tệp và đăng ký, quét cổng và phân tích lưu lượng truy cập mạng . Tất cả các kỹ thuật này kết hợp để phát triển một bức tranh hoàn chỉnh nhất có thể để hỗ trợ bạn trong việc phát hiện rootkit. Phát hiện trực tiếp Phát hiện trực tiếp các rootkit có thể là một vấn đề khó giải quyết, đặc biệt nếu điều tra viên không am hiểu về các tạo phẩm của rootkit và những gì cần tìm trên một hệ thống có thể bị nhiễm rootkit. Thông thường, điều này dẫn đến một chẩn đoán sai và xác định sai sự cố, và bất kỳ phản ứng tiếp theo được thực hiện sai hướng.

Vào mùa thu năm 2006, Jesse Kornblum đã xuất bản một bài báo rất thú vị trên Tạp chí Quốc tế về Bằng chứng Kỹ thuật số có tiêu đề Khai thác Nghịch lý Rootkit với Phân tích Bộ nhớ Windows. Trong bài báo này, Jesse đã xác định hai nguyên tắc cơ bản mà tất cả các rootkit cố gắng tuân theo; nghĩa là, họ muốn ẩn và họ muốn chạy. Về cơ bản, để ẩn trên hệ thống, rootkit phải giảm thiểu dấu chân của nó trong khi vẫn tương tác với hệ thống theo một cách nào đó. Bản thân hệ thống, cụ thể là hệ điều hành, cần có khả năng thực thi rootkit, đang cố gắng ẩn và liên tục trên các lần khởi động lại.

Do đó, Jesse đề xuất rằng nếu hệ điều hành có thể tìm thấy rootkit, thì người kiểm tra cũng có thể. Tôi có thể thêm vào một người kiểm tra có kiến ​​thức đầy đủ về câu nói đó, nhưng tôi chắc chắn rằng đó là những gì Jesse muốn nói.

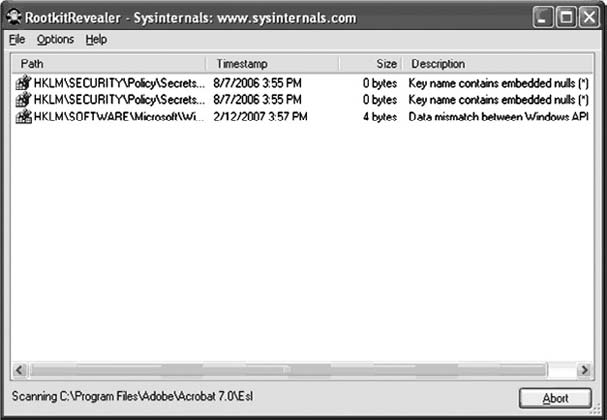
Kỹ thuật chiếm ưu thế để phát hiện rootkit trên hệ thống trực tiếp đôi khi được gọi là phân tích hành vi hoặc phân biệt (hoặc cao / thấp). Ý tưởng cơ bản là bằng cách thực hiện hai loại truy vấn khác nhau cho cùng một thông tin và tìm kiếm sự khác biệt trong Phản hồi, bạn có thể phát hiện sự hiện diện của rootkit hoặc một cái gì đó bị ẩn bởi rootkit. Ví dụ: một trong những công cụ phát hiện rootkit sớm là tập lệnh Visual Basic có tên rkdetect.vbs có thể phát hiện bộ rootkit Hacker Defender phổ biến bằng cách chạy một truy vấn từ xa để liệt kê các dịch vụ bằng sc.exe, theo sau bởi một truy vấn cục bộ (sử dụng psexec.exe và sc.exe), sau đó tìm kiếm sự bất thường hoặc khác biệt giữa hai đầu ra. Trong cuốn sách đầu tiên của tôi, Windows Forensics và Phục hồi sự cố, tôi đã bao gồm một tập lệnh Perl có tên rkd.pl sẽ thực hiện phân tích khác biệt đối với các quy trình, dịch vụ và một số khóa Registry. Tập lệnh sẽ lưu ý sự khác biệt về đầu ra giữa các truy vấn cục bộ từ xa và. một lần nữa, các công cụ đã được chạy cục bộ trên một hệ thống từ xa bằng cách sử dụng psexec.exe), nhưng nó cũng bao gồm một số kiểm tra chữ ký, đó là kiểm tra cụ thể cho các rootkit cụ thể. Trong cuốn sách, tôi đã trình diễn việc sử dụng các công cụ như vậy để chống lại AFX Rootkit 2003.

Note:

Lenny Zeltser, một người xử lý sự cố với Trung tâm Bão Internet (ISC) đã đăng một mục nhật ký (http://isc.sans.org/diary.html?storyid=1487) có tiêu đề:

Phân tích hành vi của phần mềm độc hại Rootkit vào ngày 16 tháng 7 năm 2006. Trong mục nhật ký đó, Lenny cung cấp các ảnh chụp màn hình và mô tả về một số công cụ phát hiện rootkit (cũng như các liên kết đến những người khác) đang được thử nghiệm chống lại một số rootkit được đề cập trước đó trong chương này đã phát hiện ra một hệ thống bị nhiễm virus ồ ạt, có tám dịch vụ lạ đang hoạt động và RootkitRevealer không phát hiện ra chúng là rootkit. Chà, trước hết, nếu quản trị viên có thể nhìn thấy các dịch vụ được liệt kê, thì có lẽ họ đã bị ẩn bởi một rootkit. Thứ hai, tất cả các tệp hình ảnh thực thi có cùng một biểu tượng. Thứ ba, tất cả các tệp hình ảnh thực thi là RootkitRevealer. Do thiếu sự phối hợp và kiến thức về các công cụ đang được sử dụng, các hoạt động ứng phó sự cố dẫn đến những gì thoạt nhìn có vẻ là một bệnh nhiễm trùng lớn.

**Hình 7.2 GUI RootkitRevealer**



GMER

GMER (www2.gmer.net/) là một ứng dụng phát hiện rootkit dựa trên GUI miễn phí, cố gắng phát hiện:

Các quy trình, tệp, dịch vụ, khóa Registry và trình điều khiển ẩn

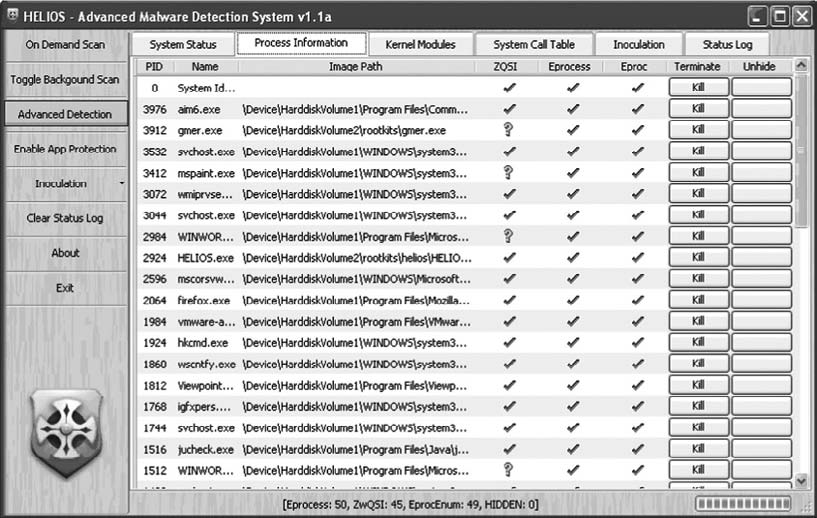
Trình điều khiển móc bảng mô tả dịch vụ hệ thống (SSDT), bảng mô tả ngắt (IDT) hoặc các cuộc gọi gói yêu cầu IO (IRP)

GMER cũng có khả năng hiển thị các luồng dữ liệu thay thế NTFS, như được minh họa trong Hình 7.3.

Nếu bạn định tải xuống và sử dụng Helios, hãy đảm bảo rằng bạn đã cài đặt

.NET Framework 2.0. Liên kết đến tệp cần thiết có sẵn trên trang tải xuống Helios.

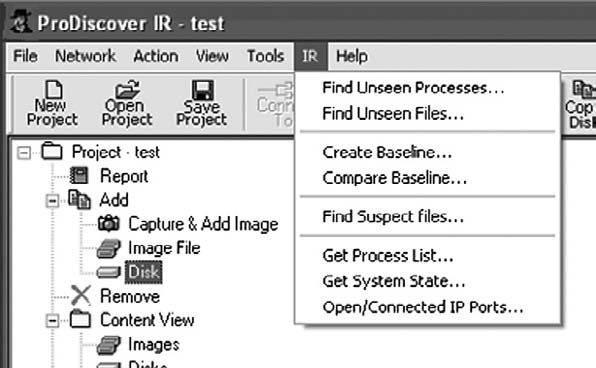
**Hình 7.4 GUI Helios**



Trang web Helios bao gồm một số video (có thể tải xuống hoặc có thể xem qua phát trực tuyến) thể hiện khả năng và khả năng sử dụng của ứng dụng.

Nhiều ứng dụng phát hiện rootkit miễn phí có sẵn được trình bày trong chương này có thể dễ dàng tải xuống và chạy từ một thư mục. Việc triển khai các công cụ này trong các hoạt động ứng phó sự cố có thể dễ dàng như sao chép chúng vào ổ USB, sau đó bật công tắc chống ghi (nếu ổ ngón tay cái của bạn có) và cắm ổ ngón tay cái vào hệ thống bạn muốn quét. Tuy nhiên, bạn cần phải ghi nhớ mọi phụ thuộc và yêu cầu, chẳng hạn như Helios yêu cầu Microsoft .NET Framework 2.0.

**Hình 7.5 Chức năng ProDiscover để phát hiện Rootkit**



Như trong Hình 7.5, điều tra viên có thể cố gắng xác định vị trí các quy trình và tệp chưa xem cũng như thu thập một số thông tin liên quan đến danh sách quy trình hoạt động và trạng thái hệ thống thông qua hệ thống menu trong ProDiscover IR. API ProScript cho phép chi tiết và linh hoạt hơn một chút trong thông tin có thể được thu thập cũng như cách quản lý.

Cố gắng xác định vị trí các quy trình và tệp không nhìn thấy có thể hỗ trợ điều tra viên trong việc xác định vị trí rootkit trên hệ thống.

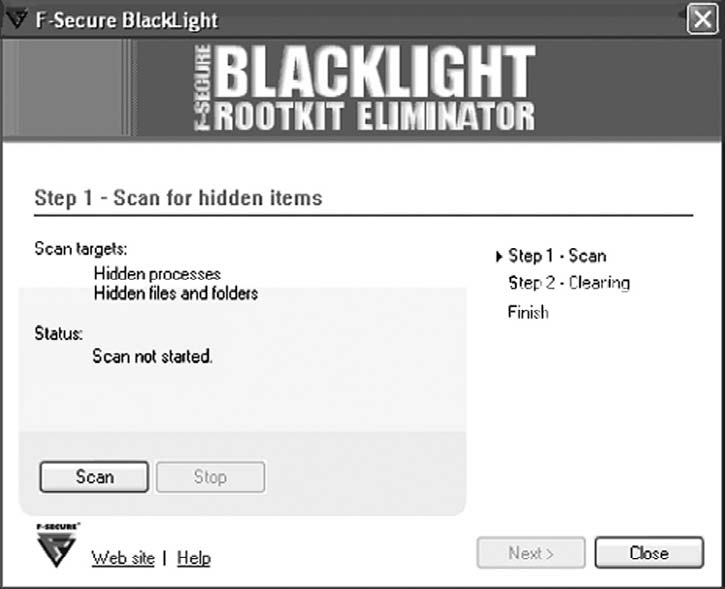
F-S ecure BlackLight

F-Secure là một công ty Phần Lan sản xuất phần mềm chống vi-rút (theo blog của công ty, sản phẩm chống vi-rút của công ty gần đây đã được tích hợp vào trang quét VirusTotal.com), cũng như một sản phẩm loại bỏ rootkit có tên BlackLight (www.f-secure.com /ánh sáng màu đen).

BlackLight phát hiện các đối tượng bị ẩn bởi các công nghệ rootkit và cung cấp cho người dùng cơ hội để loại bỏ hoặc xóa phần mềm vi phạm.

BlackLight, có sẵn miễn phí trên cơ sở dùng thử, đi kèm với cả phiên bản GUI và CLI có sẵn để tải xuống từ trang web F-Secure. Hình 7.6 minh họa GUI BlackLight.

**Hình 7.6 GUI đen**



Giống như nhiều ứng dụng phát hiện rootkit khác, BlackLight vận chuyển dưới dạng thực thi và không bao gồm chương trình cài đặt (ví dụ: tệp .msi); Khi bạn tải xuống tệp thực thi cho bất kỳ phiên bản nào bạn chọn, bạn có thể chạy ứng dụng ngay lập tức.

**Cảnh báo**

Khi sử dụng các công cụ có thể phát hiện rootkit hoặc bất kỳ phần mềm độc hại nào khác, bạn muốn chắc chắn tránh sử dụng các công cụ sẽ tự động thực hiện hành động cho bạn, chẳng hạn như xóa các tệp hoặc các tạo phẩm khác. Toàn bộ mục đích của việc kiểm tra loại này là xác định vị trí của các tạo phẩm đó để bạn có thể phát triển một hồ sơ về hoạt động và đặc điểm của rootkit, và có thể phát hiện nó trên các hệ thống khác. Tự động xóa các tệp sau khi họ phát hiện ra sẽ khiến công việc của bạn khó khăn hơn nhiều vì bây giờ bạn phải xác định những hành động khác được thực hiện tự động và những gì tạo tác khác có thể đã bị xóa.

**Sophos Anti-Rootkit**

Sophos là một nhà cung cấp chống vi-rút khác cũng cung cấp phần mềm chống phần mềm. Sản phẩm Sophos Anti-Rootkit (www.sophos.com/support/ledgeledridease/article/17004.html) được cung cấp miễn phí để tải xuống và sử dụng, và giống như sản phẩm F-Secure BlackLight, nó có trong cả GUI (minh họa trong Hình 7.7 ) và phiên bản CLI. Sản phẩm Sophos có thể được sử dụng để quét cơ sở hạ tầng, ngoài các máy chủ đơn lẻ, để tìm rootkit, cũng như loại bỏ chúng. Anti-Rootkit quét hệ thống để tìm các quy trình ẩn, khóa Registry và tệp trên ổ cứng cục bộ.

**Hình 7.7 GUI của Rootos Anti-Rootkit**



Bài viết thứ ba trong loạt ba bài viết của Jamie Butler và Sherri Sparks, Windows Windows Rootkits năm 2005, đã được xuất bản trên SecurityF Focus.com vào ngày 5 tháng 1 năm 2006. Bài viết này (www.securityf Focus.com/inf Focus / 1854), trong đó thảo luận về năm kỹ thuật phát hiện rootkit và làm nổi bật tổng cộng chín rootkit, rất đáng đọc.

**AntiRootkit.com**

F-S ecure và Sophos aren, các công ty chống vi-rút duy nhất cung cấp các sản phẩm phát hiện và / hoặc loại bỏ rootkit. Các nhà cung cấp khác bao gồm khả năng phát hiện rootkit, dưới dạng các sản phẩm riêng biệt hoặc dưới dạng các thành phần tích hợp, trong các sản phẩm chống vi-rút của họ. Sản phẩm Thám tử McAfee Rootkit tìm kiếm các tệp, quy trình và khóa hoặc giá trị ẩn trên hệ thống bị nhiễm, như Trend Micro Sản phẩm RootkitBuster.

Có lẽ trang web tốt nhất có sẵn để biết thông tin về các kỹ thuật và sản phẩm phát hiện rootkit là AntiRootkit.com. Trang web này cung cấp một blog cũng như một danh sách các sản phẩm phát hiện / loại bỏ rootkit miễn phí và thương mại (các sản phẩm được liệt kê chủ yếu cho Windows,

nhưng có Linux, BSD và thậm chí là một sản phẩm Mac OS X được liệt kê) cũng như một danh sách các sản phẩm phòng ngừa rootkit có thể được sử dụng để ngăn chặn hoặc ngăn chặn rootkit cài đặt ngay từ đầu. Tin tức và bài viết được tham khảo trên trang web này cung cấp quyền truy cập vào nhiều thông tin hơn.

Tài nguyên bổ sung cho các công cụ có thể được tìm thấy tại các trang web và blog khác, chẳng hạn như sau:

Blog Blog RaDaJo Công cụ Windows chống rootkit (http://radajo.blogspot.com/2007/11/ anti-rootkit-windows-tools-search.html)

Bài đăng trên blog của GrandStreamDreams Công cụ chống rootkit được xem lại (http: // grandstream- Dreams.blogspot.com/2008/01/anti-rootkit-tools-roundup-revisited.html)

**Phát hiện hậu sản**

Phát hiện hậu kỳ của một rootkit đặt ra các thách thức của riêng nó. Bạn có thể nghĩ rằng, điều này có thể khó khăn đến mức nào? Rốt cuộc, bạn đã nhìn vào một hình ảnh, không phải là một hệ thống trực tiếp, bạn sẽ tìm kiếm điều gì? Với các kỹ thuật khác nhau có sẵn cho các tác giả phần mềm độc hại, bao gồm các kỹ thuật chống vi trùng được thảo luận và cung cấp công khai (Dự án MetaSploit có toàn bộ phần của trang web dành riêng cho các kỹ thuật chống vi trùng), việc xác định vị trí của phần mềm độc hại vi phạm, ngay cả trên hình ảnh, có thể khó khăn. Tuy nhiên, nếu bạn hiểu những gì bạn đang tìm kiếm và nơi để tìm kiếm nó, bạn có nhiều khả năng thành công trong kỳ thi của mình.

Một phương pháp phát hiện rootkits postmortem là gắn hình ảnh dưới dạng hệ thống tệp ảo trên hệ thống phân tích của bạn bằng công cụ như SmartMount (www.asrdata.com/ SmartMount /) hoặc Mount Image Pro (www.mountimage.com), cho phép các tệp được đọc dưới dạng một hệ thống tệp mà không thu hút hệ điều hành từ hình ảnh để làm như vậy. Cả hai công cụ đều có thể gắn hình ảnh dưới dạng chỉ đọc để không có thay đổi nào đối với các tệp. Từ đây, bạn có thể chạy bất kỳ số lượng công cụ chống vi-rút nào đối với các tệp trong ảnh. Các tệp trong ảnh xuất hiện dưới dạng các tệp đó. Không có quy trình và dịch vụ nào từ hình ảnh đang chạy, vì vậy rootkit sẽ không được tham gia và kernel của hệ thống phân tích không bị phá vỡ.

**Cảnh báo**

Sử dụng SmartMount để truy cập hình ảnh thu được dưới dạng cấu trúc thư mục tệp là điều tuyệt vời nếu bạn muốn quét nó bằng các công cụ phát hiện phần mềm chống vi-rút và phần mềm gián điệp, nhưng các công cụ phát hiện rootkit có sẵn sẽ không được sử dụng nhiều cho bạn.

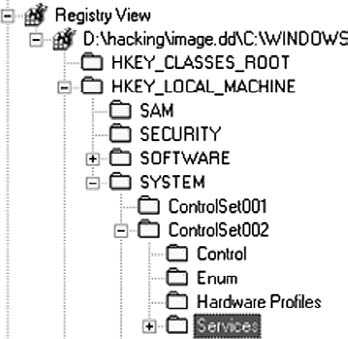
Lý do là vì các công cụ này tìm kiếm những thứ đang ẩn các tệp tin, các khóa Registry, các quy trình và tương tự như thế và khi một hình ảnh thu được được gắn vào như

một ký tự ổ đĩa, không có thông tin nào được ẩn.

Một tùy chọn khác có sẵn cho bạn là khởi động hình ảnh vào VMware bằng LiveView (http://liveview.sourceforge.net) và kiểm tra hệ thống trực tiếp để tìm rootkit có thể bằng bất kỳ công cụ nào dành cho hệ thống trực tiếp. Tất nhiên, điều này giả định rằng bạn có tên người dùng và mật khẩu để bạn có thể đăng nhập vào hình ảnh khi nó đã khởi động. Trong Chương 6, tôi đã đề cập rằng một số phần mềm độc hại sử dụng phần mềm để phát hiện sự hiện diện của môi trường ảo và nếu phát hiện thấy nó đang chạy trong môi trường như VMware, nó có thể thay đổi hành vi để tránh bị phát hiện. Tất nhiên, một số rootkit cũng có thể làm điều này và hành vi thứ cấp đó có thể gây ra sự cố (tức là ngăn các thành phần của hệ điều hành chạy chính xác hoặc đơn giản là gây ra BSoD) trên hệ thống. Bạn cũng có thể quét hệ thống ảo bằng trình quét cổng như Nmap và sau đó so sánh kết quả quét với đầu ra của netstat.exe hoặc openports.exe. Nếu bạn tìm thấy các cổng được mở bằng Nmap nhưng bạn không thấy các cổng đó trong đầu ra của netstat.exe, bạn có thể có một rootkit trực tiếp trên hệ thống.

Một phương pháp mà tôi sử dụng để kiểm tra nhanh sự hiện diện của rootkit trong hình ảnh thu được là truy cập Trình xem đăng ký trong ProDiscover và điều hướng đến khóa Dịch vụ trong mỗi Controlset có sẵn, như được minh họa trong Hình 7.8.

**Hình 7.8 Trích từ Chế độ xem đăng ký ProDiscover**



Để xác định Bộ điều khiển được đánh dấu là hiện tại, hay được tải dưới dạng Hiện tại khi hệ thống được khởi động, hãy xác định giá trị Hiện tại trong khóa Hệ thống \ Chọn. Dữ liệu là loại Đăng ký DWORD và cho bạn biết ControlSets nào có sẵn được đánh dấu là hiện tại.

Khi tôi xác định vị trí khóa, sau đó tôi sắp xếp các mục trong ngăn bên phải dựa trên thời gian LastWrite của mỗi khóa. Hầu hết các mục trong danh sách này sẽ tương ứng với khi hệ thống được cài đặt ban đầu. Trong một số trường hợp, một số khóa có thể có cùng thời gian LastWrite là kết quả của một bản cập nhật phần mềm ảnh hưởng đến tất cả chúng, thường trong cùng một ngày. Tuy nhiên, khi trình điều khiển rootkit chế độ kernel được cài đặt, nó thường sẽ nổi bật chỉ với một hoặc hai mục được thực hiện trong một ngày. Thời gian LastWrite này không luôn luôn tương ứng với ngày được cung cấp trong báo cáo sự cố, nhưng trong hầu hết các trường hợp, chúng sẽ nổi bật như ngón tay cái đau.

Ngoài ra, họ sẽ cung cấp cho bạn ngày để định hướng phân tích hoạt động dòng thời gian của bạn trên hệ thống. Vì dường như không có bất kỳ API Windows nào có sẵn công khai để sửa đổi khóa Registry Lần cuối từ các ứng dụng ở chế độ người dùng, bạn có thể chắc chắn rằng thời gian khóa Last LastWrite tương ứng với khi rootkit và trình điều khiển của nó được cài đặt.

|  |
| --- |
| Sử dụng RegRipper để tìm kiếm Rootkit  Một cách khác để thực hiện phân tích tương tự này mà không tải tệp hình ảnh vào tệp dự án hoặc hồ sơ trong ứng dụng phân tích pháp y yêu thích của bạn là sử dụng RegRipper (thảo luận trong Chương 4) hoặc công cụ CLI liên quan của nó, rip.exe (cùng với plugin phù hợp) để phân tích thông qua khóa Dịch vụ trong tệp hive của Hệ thống và sắp xếp các khóa con theo thời gian LastWrite. Bạn có thể thực hiện việc này khá dễ dàng bằng cách gắn hình ảnh với SmartMount và sử dụng tệp bó để khởi chạy dòng lệnh thích hợp. Tuy nhiên, nếu bạn không có hình ảnh và thay vào đó buộc phải làm việc với một hệ thống trực tiếp, một tùy chọn khác có sẵn cho bạn là chạy RegRipper thông qua F-Feedback (www.f-response.com). Một blogger với tiêu đề của Hog Hogfly đã đăng một video lên YouTube cho thấy cách anh ta sử dụng F-Feedback và RegRipper (http: // forensicir. Blogspot.com/2008/04/ripping-registry-live.html) để trích xuất dữ liệu từ Cơ quan đăng ký của một hệ thống sống. |

Một phương tiện phát hiện rootkit bổ sung bị treo ở đâu đó giữa sống và hậu hiện đại đã được thảo luận trong Chương 3. Nếu điều tra viên bỏ nội dung của bộ nhớ vật lý và nhanh chóng phân tích nó, hệ thống vẫn có thể chạy, nhưng phân tích sẽ thực sự xảy ra trên ảnh chụp nhanh RAM. Như Jesse đã chỉ ra trong bài viết Parad Parad của anh ấy, một bộ rootkit thông minh của Bỉ sẽ không can thiệp vào quá trình kết xuất bộ nhớ vì làm như vậy có thể tiết lộ sự hiện diện của rootkit. Rốt cuộc, một rootkit khiến hệ điều hành gặp sự cố (dẫn đến BSoD đáng sợ) khiến hệ thống không thể sử dụng được cho cả quản trị viên / người dùng và kẻ xâm nhập. Tham khảo Chương 3 để biết danh sách các công cụ để

thu thập và phân tích nội dung của bộ nhớ vật lý từ các hệ thống Windows.

Nếu rootkit khiến hệ thống gặp sự cố, tệp kết xuất sự cố có thể được phân tích để tiết lộ sự tồn tại của rootkit. Bằng cách thu thập nội dung của RAM và tìm kiếm các khối EPROCESS (tham khảo Chương 3 để biết thông tin về tìm kiếm các bãi chứa RAM để biết thông tin về quy trình), bạn có thể so sánh các quy trình chưa thoát với các quy trình hiển thị trong danh sách quy trình hoạt động để xác định xem, nếu có , đã bị ẩn bởi một rootkit.

**Cảnh báo**

Một số người lựa chọn không thực hiện một cách tiếp cận tối giản để cấu hình hệ thống. Vấn đề chính là người dùng có quyền truy cập cấp Quản trị viên vào hệ thống của họ và được phép cài đặt bất kỳ phần mềm nào họ có thể tìm thấy. Tôi đã từng làm việc trong một trường hợp tôi tìm thấy một hệ thống có tổng cộng bốn dịch vụ máy tính để bàn từ xa đang chạy và tôi xác định rằng kẻ xâm nhập đã sử dụng một trong số chúng để có quyền truy cập vào hệ thống. Lúc đầu, tôi nghĩ rằng kẻ xâm nhập đã cài đặt một số phần mềm truy cập từ xa, nhưng quản trị viên hệ thống sau đó nói với tôi rằng tất cả bốn ứng dụng đều hợp pháp và đã được bộ phận CNTT cài đặt; mỗi ứng dụng truy cập từ xa là một bản sao lưu cho những ứng dụng khác. Không ai trong số các quản trị viên hệ thống có thời gian hoặc kỹ năng để quản lý tất cả các ứng dụng truy cập từ xa và kẻ xâm nhập có thể sử dụng một trong số chúng để có quyền truy cập vào hệ thống.

**Tóm lược**

Mặc dù rootkit đã xuất hiện khá lâu ở cả thế giới Linux và Windows, nhưng sự quan tâm đến rootkit đã bùng nổ vào tháng 2 năm 2005 khi từ này được các nhân viên của Microsoft nhắc đến tại Hội nghị RSA. Sách (Rootlits của Hoglund: Phá vỡ Windows Kernel và thậm chí một cuốn sách có tên Rootkits for Dummies có sẵn trên Amazon.com) và các khóa đào tạo (Hoglund đã dạy các kỹ thuật rootkit trong các buổi đào tạo tại các hội thảo BlackHat) có sẵn về phát triển rootkit. làm việc (mặc dù trong một số trường hợp rootkit bằng chứng khái niệm).

Rootkit gây ra mối đe dọa đáng kể cho các hệ thống và cơ sở hạ tầng, trong đó nghiêm trọng nhất là sự thiếu giáo dục và kiến ​​thức về phía quản trị viên và điều tra viên về chính xác rootkit là gì, rootkit có khả năng gì và hoạt động như thế nào. một sự hiểu biết mạnh mẽ hơn về các lĩnh vực này, các nhà điều tra sẽ được trang bị tốt hơn để giải quyết các vấn đề về rootkit trong cả các cuộc điều tra trực tiếp và sau khi điều tra.

**Giải pháp theo dõi nhanh**

Rễ cây

Rootkit có khả năng ẩn các tệp, khóa Registry, quy trình, kết nối mạng và các đối tượng khác từ quản trị viên cũng như hệ điều hành.

Việc sử dụng các công nghệ rootkit và rootkit trong phần mềm độc hại và tội phạm mạng đang gia tăng.

Hiểu rõ hơn về chức năng và khả năng của rootkit sẽ chuẩn bị cho các nhà điều tra để giải quyết các vấn đề của rootkit.

**Phát hiện Rootkit**

Phát hiện rootkit trên các hệ thống sống đòi hỏi phải sử dụng phân tích vi sai.

Việc phát hiện rootkit trên hình ảnh thu được của hệ thống có thể đơn giản như quét hình ảnh được gắn (thông qua Mount Image Pro) bằng phần mềm chống vi-rút hoặc thậm chí sắp xếp các khóa Đăng ký dịch vụ dựa trên thời gian LastWrite của chúng.

Rootkit có thể được phát hiện trên các hệ thống trực tiếp bằng cách chụp và phân tích nội dung của bộ nhớ vật lý để xác định vị trí các quy trình đang hoạt động nhưng không phải là một phần của danh sách quy trình hoạt động.

**Các câu hỏi thường gặp**

H: Tôi đã tìm thấy một số lưu lượng truy cập bất thường được đăng nhập vào tường lửa của mình, với dấu thời gian từ bốn giờ trước. Có vẻ như một hệ thống trên mạng của tôi đã cố gắng tạo kết nối ra Internet trên một cổng lẻ. Tôi đã đi đến hệ thống được đề cập và didn tìm thấy bất kỳ kết nối mạng hoạt động nào sẽ chiếm lưu lượng truy cập đó. Tôi có rootkit không?

A: Câu trả lời ngắn có lẽ là không. Mọi thứ bắt nguồn từ một hệ thống, đặc biệt là lưu lượng mạng, phải có một quy trình hoặc luồng chịu trách nhiệm tạo ra nó. Các dịch vụ thường sẽ chạy miễn là hệ thống đang chạy, nhưng các quy trình có thể tồn tại trong thời gian ngắn. Nếu bạn không tiếp tục thấy các mục nhật ký tường lửa tương tự, có khả năng quá trình đã hoàn thành và thoát, đó là lý do tại sao bạn không thấy nó trên hệ thống.

Q: Làm thế nào để làm việc và làm được

Một trong những thứ khác nhau có thể sử dụng một cách tốt nhất. Bạn có thể sử dụng một số thứ khác nhau.

H: Tôi có thể sử dụng một phần của rootkit Sao thì sao? Tôi chỉ có một phần của họ, một trong những thứ khác nhau bản sao sao lưu không bị lỗi.

Một trong những bộ trang phục của bạn.

Theo đó, bạn có thể sử dụng một cách tốt nhất trẻ em như thế nào Trong khi điều tra sự kiện này, bạn có thể có một phần của họ. Tình yêu, tình yêu, sự tin tưởng của bạn, sự tin tưởng của bạn, một trong những vấn đề của bạn (Visa PCI, HIPAA, FISMA báo cáo và có thể cung cấp cho bạn).