NHỮNG BÓNG MA TRONG MẠNG

Khi xuất hiện điều kỳ lạ (nếu không phải là do ma quỷ) thì tức là các vấn đề mạng đã nảy sinh. Các chuyên gia công nghệ bắt đầu cuộc tìm kiếm kẻ tội phạm giấu mặt.

Đây là câu chuyện thực về một dịch vụ ghost, một dịch vụ "ma" gần như đã phá sập mạng của chúng tôi. Huyền bí ư? Có lẽ là không. Chỉ là cảm giác thông thường cộng với một chút công nghệ phân phối thiết bị thú vị mà bạn không thể thấy.

Mạng hiện thời của chúng tôi có các mainframe khổng lồ cho các máy Windows, Unix, các thiết bị đầu cuối, NT và hàng nghìn clent thông minh cùng các dịch vụ chuyên dụng mạnh. Chúng tôi giám sát mọi mặt trong các hoạt động của họ. Thế nhưng có một 'bóng ma' gần như kéo tụt chúng tôi xuống.

Ngay từ khi bắt đầu đã có những dấu hiệu báo điềm gở. Một máy in mạng bị tràn bộ đệm, công việc in ấn bị ngừng trệ. Chúng tôi thấy rằng đó là do lỗi phần cứng. Chuyển sang sử dụng một máy cũ, được cấu hình bên trong mới, khởi động lại thiết bị và mọi việc trở lại bình thường.

Rồi sự việc tương tự lại xảy ra với một chiếc máy in khác. Một thiết bị giao tiếp master trong nháy mắt bị hỏng. Chỉ cần một phút, chúng tôi đã xác định chắc chắn là không còn gì cứu vãn được nó. Người dùng ghi lại các tiêu đề dữ liệu sai lạc. Những việc bất ngờ kỳ lạ xảy ra thường xuyên hơn không theo khuôn mẫu nào.

Virus máy tính trên server? Sâu mạng trên thiết bị chia sẻ? Không giống như thế. Chúng tôi đã dùng một chương trình bảo vệ đa tầng để ngăn chặn các đe doạ tổng hợp.

NetOps bắt được một số tín hiệu. Chúng là ngẫu nhiên, nhưng rõ ràng được tổ chức từ bên trong mạng. Chúng tôi có một server "ma".

Nguyên nhân ư? Hãy xem xét một số mẹo nhỏ dưới đây.

Lưu trữ lại các thông tin phần cứng đã thay đổi

Một số server rất cũ của chúng tôi đã hoạt động nhiều năm nay, chúng nặng nề thực hiện công việc bảo dưỡng của mình. Các phần cứng mới được thay rồi loại bỏ. Nhiều thiết bị cũ hơn có thể không được tìm thấy trừ phi có bộ nhớ quan trọng.

Quét toàn bộ phạm vi IP định kỳ

Hầu hết các hệ điều hành hiện đại đều giám sát phạm vi rộng lớn các hoạt động. Nhưng hãy thận trọng! Chúng không thể xác định cái mà chúng không thấy. Các ổ cứng quá cũ có thể nằm dưới tầm rada. Dịch vụ 'ma' không tên của chúng tôi không thể bị dò tìm bởi các phương tiện thông

thường.

Các chương trình giao tiếp người-máy có thể thể hiện các client của chúng, nhưng không phải mọi máy đều chạy trên mọi dịch vụ. Chúng tôi đột nhiên nhận ra rằng mình chẳng hề có một phương thức đơn, đơn giản, toàn diện để dò tìm mọi thứ trên mạng của mình.

Câu lệnh 'ping' xoàng xĩnh lại trở thành cứu cánh. Nó dò tìm các kết nối và cho phép bạn đóng gói địa chỉ IP khi lướt qua mạng của bạn.

Dùng quy ước đặt tên tiêu chuẩn cung cấp được nhiều tin tức

Các tên dịch vụ 'mỹ miều' có thể rất đáng ngạc nhiên, nhưng cũng khó làm việc khi cố gắng cấp phát một phần tử nào đó trong lúc bạn đang vội. Mã hoá khu vực và tính năng vào tên thiết bị tiết kiệm cả thời gian và các nguy cơ gây khó chịu về sau. Bạn nên tạo tên nhãn cho từng server với thẻ gắn cả tên và địa chỉ IP trong khu vực dễ thấy khi đăng nhập dịch vụ. Kỹ thuật này có vẻ không đáng kể gì, nhưng nó tiết kiệm được lượng thời gian giá trị khi bạn phải cố gắng tìm kiếm một hộp nào đó giữa hàng loạt 'đồng nghiệp' của nó.

Đọc các bản ghi log của bạn

Một file log có thể cung cấp khá nhiều thông tin. Nếu nội dung dữ liệu là quá lớn, có thể kết xuất nó thành một bảng tính hay cơ sở dữ liệu và xem nó theo trật tự đã được sắp xếp. Các máy cũ cung cấp dịch vụ này một thời gian trước đây không có các tên tiêu chuẩn.

Một lệnh ping, một file log và một thứ tự đã phát hiện ra được server 'ma' của chúng tôi. Phân đoạn mạng cung cấp được khu vực sát kề của nó trong toà nhà. Những người sử dụng hệ thống không nhớ chính xác khu vực, nhưng những người trong phòng thí nghiệm lại nhớ một số thiết bị đã được chuyển đi. Và với sự giúp đỡ của họ, cuối cùng chúng tôi cũng tìm thấy nó.

Vật 'huyền bí' được đặt cô lập trong một hộp kín, gây trở ngại bởi các phần phân tách và chạy một hình thái ngôn ngữ của SCO Unix với một vài phiên bản hệ điều hành ở đằng sau. Không ai biết được thiết bị đó ở đâu. Nó đã được chuyển đi khi người quản lý trước đây nâng cấp UPS. Và ông ta đã về hưu trước khi lấy nó ra khỏi dịch vụ. Các nhân viên thời đó đều đã rời khỏi công ty một thời gian dài.

Thiết bị là một dịch vụ thử nghiệm đơn giản, giám sát hoạt động truyền thông với các thiết bị dữ liệu có được. Nó hoạt động câm lặng với nhiệm vụ định tuyến và định kỳ cung cấp một cảnh báo LAM (Look-At-ME!) khi có nguy hiểm. Các cảnh báo LAM được đưa vào mạng mà không ai để ý cho đến khi chúng xung đột với các khối tin dịch vụ khác. Các xung đột này chỉ xuất hiện khi có sự khác thường của hệ thống.

Những bài học này bạn đã biết? Hãy biết về mạng của bạn. Dẫn ra các tài nguyên, quét phạm vi bạn có.

Đôi khi một chút cảm giác thông thường của công nghệ thấp lại giải quyết được 'bóng ma' bất thường trong mạng của bạn.

T.Thu