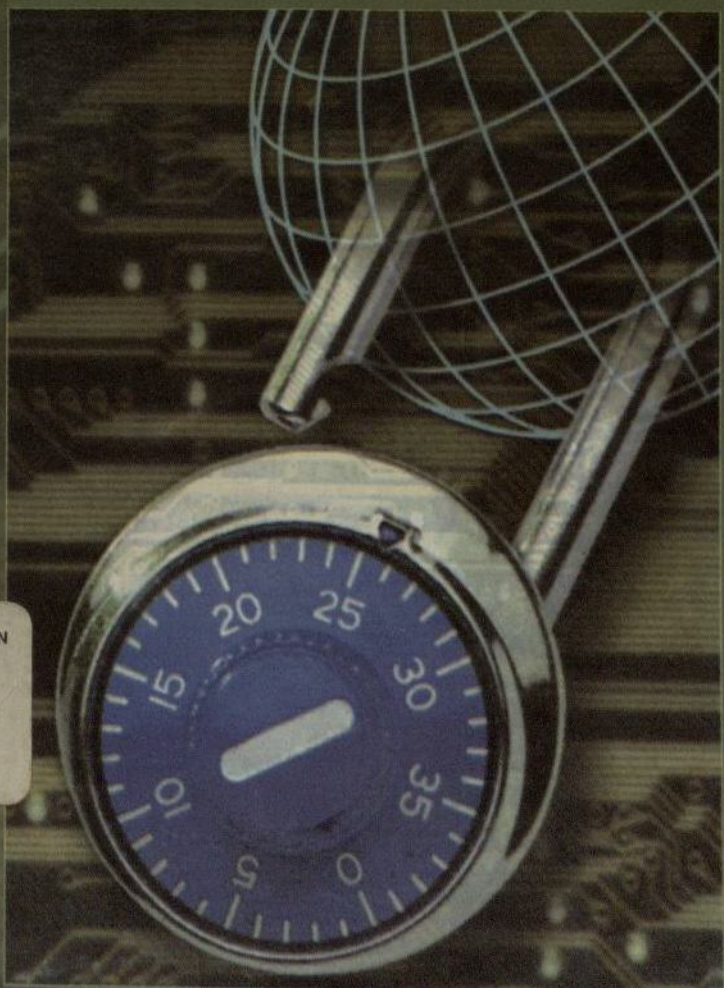
Tổng hợp & Biên dịch
VN-GUIDE

BẢO MẬT TRÊN MẠNG

Bí quyết & Giải p



NHÀ XUẤT BẢN THỐNG KÊ

BẢO MẬT TRÊN MẠNG

❑ Bí Quyết và Giải Pháp ❑

Tổng hợp và biên dịch:
VN-GUIDE

NHÀ XUẤT BẢN THỐNG KÊ

LỜI NÓI ĐẦU

Xâm nhập bất hợp pháp là hiện tượng lý thú song đôi lúc cũng đáng sợ tùy theo bạn đứng về phe nào trong trận chiến. Dường như mỗi ngày người ta lại tìm ra chỗ yếu mới trong cấu trúc hệ thống liên khóa và phần mềm vốn tạo thành xương sống của thị trường điện tử hiện nay. Ở bên này bức tường, bên trong, là những nhà quản lý mạng và chuyên gia chịu trách nhiệm duy trì, xây dựng cấu trúc điều khiển đang ngày càng quan trọng trong cuộc sống hiện đại. Còn bên kia bức tường là những đám tin tặc ô hợp, những tay khoái chỉ ra vết nứt trên tường bằng cách quảng bá những lỗ hổng trên hàng rào phòng thủ vốn rất cao và chắc chắn.

Cũng có số ít người đứng giang chân trên bức tường - những điệp viên tìm hiểu và phân phối thông tin về chiến thuật của kẻ địch. Nhóm tác giả *(Stuart McClure, Joel Scambray và George Kurtz)* là những người như thế.

Chẳng có ai là cảm thấy an toàn tuyệt đối, tuy số ít người có thể dốc hết thời gian và tâm trí duy trì thường xuyên hàng rào phòng thủ đang đứng trước nguy cơ trở thành mục tiêu. Bảo mật máy tính là một thiên hướng lý thú: thách thức, nản lòng, thỉnh thoảng phấn kích tột độ và nói chung là công việc. Tiếc thay, xây dựng cấu trúc điều khiển đó là để chút thời gian quí báu thực hiện nhiệm vụ của một tiểu chủ.

Đối với những ai quả thật chịu trách nhiệm bảo vệ hệ thống quan trọng và hàng ngày đấu tranh với thời gian, tài nguyên eo hẹp, thì có một vũ khí cần thiết mà bạn cần có trong kho, đó là thông tin. Ngay bây giờ, bạn đang nắm những thông tin rất bổ ích nếu như đọc tập sách này, vì vậy đừng bỏ xuống. Trên thị trường có vô số sản phẩm bảo mật và nhiều người bán giải pháp – song những người bán sản phẩm này chưa chắc giúp được bạn nếu bạn không hiểu chúng thực sự làm gì, và giúp bạn như thế nào. Cách tốt nhất để tránh những giải pháp được quảng cáo quá rùm beng là hiểu rõ cái gì có, cái gì không và tại sao. Vì tập sách này, nhóm tác giả *(Stuart McClure, Joel Scambray và George Kurtz)* đã làm việc với nhiều người có thông tin tế nhị – tin tức kinh doanh, e-mail cho người yêu, phần mềm thanh toán hóa đơn, và thuế – trên PC vô tình nối mạng Internet. Thật khó ước tính có bao nhiêu hoạt động xâm nhập bất hợp pháp diễn ra. Người bạn dùng modem cáp của tác giả cũng bị thăm dò cả chục lần mỗi tuần. Những tin tặc thăm dò họ bằng loại mánh khóe mà tác giả sẽ nói đến trong tập sách này. **Bảo mật trên mạng – Bí quyết và giải pháp** đưa ra các biện pháp đối phó loại mánh khóe trên.

Các tác giả có không ít kinh nghiệm bảo vệ mạng. Để có được kinh nghiệm đó, họ cần biết nhiều về thủ thuật của những kẻ tấn công - công cụ, kỹ thuật, và nơi chúng trao đổi các bí quyết xâm nhập bất hợp pháp. Tập sách này có đầy đủ tư liệu đó. Có lẽ đến lúc đọc xong tập sách, một số bạn sẽ cảm thấy lo lắng hơn. Chủ đề tiềm ẩn của sách là "bạn là người yếu bóng vía". Nếu nhóm tác giả không thuyết phục bạn cần thực hiện các bước bảo vệ hệ thống thì chẳng có chi làm được.

Các tin tặc đều biết những kỹ thuật này và sẽ chẳng ngần ngại áp dụng lên bạn. Do đó tác giả sẽ cung cấp cho bạn những biện pháp đối phó cùng với nhiều lời khuyên bổ ích. Nhiều hoạt động xâm nhập bất hợp pháp mở đầu bằng công cụ quét

"trái cây dưới thấp" – mục tiêu phòng thủ yếu – trên toàn bộ mạng. Đừng tự lừa dối mình về cảm giác an toàn vì bạn là mục tiêu nhỏ không đáng quan tâm - những công cụ tự động hóa của tin tặc chẳng phân biệt như thế đâu. Hãy theo các đề nghị trong sách, chúng hữu ích lắm đó.

Nhiều chuyên gia bảo mật ngại tiết lộ kỹ thuật trình bày trong sách này. "Nếu chúng ta nói tới, chỉ tổ khuyến khích các tin tặc thử chúng" có lẽ đúng, song ngày nay, các tin tặc trang bị những đường truyền thông và chia sẻ thông tin tốt hơn các chuyên gia bảo mật. Không may là đôi lúc nhà quản trị mạng phải giải thích vấn đề tồn tại hầu lấy nguồn thông tin cần thiết để sửa chữa; tập sách này có thể đóng vai trò giải thích. Kinh nghiệm trong bảo vệ hệ thống là hầu hết người dùng bị sốc khi họ thấy mình sao thật yếu đuối. Có thể tập sách này sẽ làm bạn bàng hoàng. Bất luận thế nào đi nữa, *Bảo mật trên mạng – Bí quyết và giải pháp* sẽ giúp ích cho bạn.

PHẦN GIỚI THIỆU

LÝ DO VIẾT SÁCH

Bạn đang đọc sách nói về xâm nhập mạng máy tính.. Có thể phơi bày gì về đề tài có tính chất phá hoại như thế? Câu hỏi hay – câu hỏi có thể đã được nhiều sách bảo mật máy tính đặt ra. Sách nói về những tin tặc ác tâm thì chẳng có gì mới và dù nhiều sách viết cốt để làm người ta phấn khởi về quảng cáo mới nhất tuôn ra từ phương tiện đại chúng nhưng câu hỏi này thì khác.

Chúng tôi (nhóm tác giả) thực sự muốn hướng dẫn chi tiết cách thức xâm nhập bất hợp pháp mạng máy tính bằng những thuật ngữ đơn giản dễ hiểu.

Những ai chưa rõ lịch sử bảo mật hệ thống thông tin hẳn sẽ bị sốc trước câu phát biểu vừa rồi. Ngay cả những người chuyên thực thi bảo mật máy tính cũng đôi lúc nghi ngờ sự sáng suốt. Tuy nhiên, tin hay không tin tùy bạn, chẳng ai tìm ra ý tưởng hay hơn để đảm bảo bảo mật mạng kể từ khi việc tính toán trên máy tính ra đời cách đây nhiều năm. Quay về thời đó, nhiều nhóm được tập hợp để thử thâm nhập cài đặt máy tính công ty, người tốt được trả tiền để chấp nhận thói quen xấu. Khái niệm này đã đi với chúng tôi trong suốt nhiều thay đổi có tính cách mạng về nền tính toán trên máy tính.

Đây là phần khó hiểu thấu nhất: Với đà phát triển chóng mặt trong công nghệ suốt nhiều năm qua, tại sao chẳng có ai phát minh "bảo mật hoàn hảo"? Câu trả lời có nhiều mặt, từ những lỗi cố hữu trong phát triển phần mềm hiện đại đến nối

kết mạng rộng khắp, song cần có đọng tới mức dễ hiểu, nên chẳng có gì là hoàn hảo cả.

Do vậy, vũ khí hữu hiệu nhất nằm trong tay kẻ tấn công – có chủ đích hoặc không – là khả năng tìm những sai sót trong hệ thống vốn chưa thật rõ ràng đối với người thiết kế ra nó hoặc sử dụng nó mỗi ngày. Một khi chuyên gia bảo mật danh tiếng đã đưa nó vào, cách tốt nhất để nâng cao bảo mật địa điểm là thông qua xâm nhập.

Mục tiêu trong sách này là nói rõ những kỹ thuật và công cụ thông dụng của kẻ thích làm sáng tỏ những lỗ hổng mà chúng khai thác, để có thể phục vụ cho mục đích tốt. Tất nhiên thảo luận như thế có tính hai mặt, những kỹ thuật và công cụ nêu chi tiết ở đây có thể dùng cho mục đích xấu. Chúng tôi không dung túng hoạt động này, song tốt hơn hết là biết đến còn hơn trở thành nạn nhân. Nội dung đề cập giữa những trang này đều có sẵn trên Internet. Tản mát trên hàng ngàn trang Web, địa điểm ftp vô danh, máy phục vụ Internet Relay Chat, nhóm tin Usenet và vô số nguồn khác. Chúng tôi biên soạn tri thức này với kinh nghiệm riêng sao cho dễ tiếp cận, dễ hiểu và tham chiếu được nhanh.

Suy cho cùng, tại sao bạn phải là người độc nhất không thương không giáo trên mạng?

ĐỐI TƯỢNG CỦA SÁCH

Sách này dành cho những đồng nghiệp quản trị mạng những người vì quá bận việc hoặc lương thấp lại hiếm khi có đủ nguồn tham khảo để làm cho mọi việc diễn tiến ở mức độ chấp nhập được. Hy vọng tập sách này sẽ là tiền đề cho những bạn có lẽ không có thời gian hoặc sở thích sục sạo những góc tối trên Internet và nhốt mình vào những quyển sách hướng dẫn kỹ thuật khó hiểu cố hiểu bản chất và qui mô của những mối đe dọa vốn rình rập những ai sở hữu, vận hành mạng máy tính.

Tập sách này nhắm vào những ai chưa thật rành các công nghệ mạng máy tính - mạng Internet nói riêng. Đừng lo nếu bạn hiểu biết nhiều nhưng kém cỏi về kỹ thuật. Tập sách này sẽ dẫn dắt bạn qua từng chi tiết, giải thích những chi tiết cơ bản của kỹ thuật tấn công sao cho dễ hiểu. Chắc chắn những

Đôi lời về từ: "Tin tặc" - "Kẻ bẻ khóa"

"Tin tặc" là những người xâm nhập hệ thống máy tính. Theo truyền thống, thuật ngữ "tin tặc" có nghĩa là người tày máy hệ thống chưa quen biết nhằm hiểu thấu và/hoặc lén sắp đặt cho tốt hơn. Trái lại, "kẻ bẻ khóa" ám chỉ những tin tặc xâm nhập hệ thống cho vui hoặc để thu lợi.

Ngôn ngữ phát triển theo lối riêng, và "kẻ bẻ khóa" chẳng bao giờ được hiểu là câu nói thông tục của tội phạm máy tính. Tuy chúng ta cảm thấy "kẻ bẻ khóa" là người hơi nguy hiểm nhưng nhóm tác giả lại đồng tình khái niệm "tin tặc" không nhất thiết là người xấu (sự thật chúng ta xem mình là tin tặc thuộc loại có đạo đức) và tránh dùng từ "tin tặc" trong sách này để chỉ người nghiên cứu và thử nghiệm bảo mật máy tính trên hệ thống của mình.

Tuy nhiên cũng nhấn mạnh rằng chúng ta hoàn toàn không đồng tình với những ai truy cập bất hợp pháp tài nguyên của người khác. Bất kể định nghĩa "tin tặc" là thế nào đi nữa thì đây là đường phân ranh giữa đúng và sai. Do đó chúng ta thay bằng những thuật ngữ chung chung hơn như "tin tặc ác tâm", "kẻ tấn công", hoặc "kẻ xâm nhập" để làm rõ ý định truy cập bất hợp pháp tài nguyên và chúng tôi cần sự thông hiểu của giới độc giả về những trường hợp phân biệt khó tránh khỏi mập mờ giữa hai thái cực.

độc giả giỏi về kỹ thuật sẽ học hỏi được rất nhiều, vì chúng tôi thường thấy ngay cả nhà quản trị giàu kinh nghiệm nếu không xem kỹ cách vi phạm các công nghệ, họ sẽ mất rất nhiều thời gian xây dựng và hỗ trợ. Đến với sách, bạn sẽ nhất trí rằng cách tối ưu để học mạng máy tính là xâm nhập nó.

Nhiều người cáo buộc chúng tôi là viết sách này sẽ làm hại sức khỏe cho nhà quản trị mạng hơn là làm lợi, họ sẽ không đọc kỹ quyển sách này. Cùng với những chỗ yếu là biện pháp đối phó, vậy khi bạn tìm thấy chỗ yếu trên địa điểm của mình, bạn có thể sửa chữa hoặc theo dõi những ai cố khai thác nó. Đối với những vị có đầu óc phóng khoáng, quyển sách này sẽ giúp biết được mạng có thể bị ai xâm nhập, xâm nhập những gì, ở đâu, khi nào, và như thế nào để bạn có thể đáp lại một cách đầy hiểu biết khi ai đó la lên rằng "Chúng ta có an toàn thật không?".

CÁCH TỔ CHỨC SÁCH

Mặc dù chúng tôi hy vọng bạn đọc hết cả mấy trăm trang sách, song quả thật chúng tôi không trông mong nhiều người sẽ dành thời gian làm chuyện đó. Bạn bận rộn – thế sao không đọc phần này trước tiên, để nắm bắt những điểm chính, mẹo trám các lỗ hổng v.v. Có hai cách nắm bắt ngắn ấy trang này.

Đọc từng đoạn nhỏ

Tập sách này được chia đoạn sao cho có thể tiếp cận như một cuốn sách tham chiếu. Mỗi chương đều đứng độc lập, đề cập kỹ thuật cụ thể cho bạn chọn mà không phải lặn lội qua những trang thông tin không phù hợp. Trong mỗi chương đều có bài viết chia thành từng đoạn nhỏ tùy theo phương pháp tấn công và biện pháp đối phó. Bằng cách này, bạn có thể tập trung ngay vào vấn đề quan trọng đối với bạn.

Hoặc theo kế hoạch từ đầu đến cuối

Đối với những bạn quan tâm và có thời gian rỗi rãi hơn, thì có chủ đề toàn bộ từ đầu đến cuối. Chủ đề đó là phương pháp tấn công cơ bản của kẻ xâm nhập.

- ❑ Thu thập thông tin đích
- ❑ Truy cập lần đầu
- ❑ Leo thang đặc quyền
- ❑ Che đậy dấu vết
- ❑ Đặt cửa sau

Nói chung xâm nhập máy tính được hoạch định kỹ và xây dựng lần lượt theo từng bước trong phương pháp này. Như đã nêu ở trước, con đường này có thể truy nhập bất cứ lúc nào, song để đánh giá đúng thuyết giáo của việc xâm phạm mạng, hãy bắt đầu từ đầu và đọc đến cuối.

Biện pháp đối phó

Quan trọng hơn hết, tập sách này đề cập những nỗ lực phản công bằng kỹ thuật phòng thủ thích hợp. Những mục này có tên là "Biện pháp đối phó" và đi ngay sau phần bàn về tấn công. Trong một số trường hợp nói về nhóm kỹ thuật xâm nhập thì sẽ chờ đến hết mới phác họa biện pháp đối phó các loại tấn công đã định. Hy vọng không làm bạn sợ là sao một số tấn công lại đơn giản và dễ dàng đến thế nhưng sẽ không để bạn không được bảo vệ sau khi đọc xong.

Nghiên cứu trường hợp

Mở đầu từng đoạn nhỏ trong sách là nghiên cứu tình huống bảo mật máy tính trong thế giới thật. Những đoản văn này cho bạn hiểu thấu đáo ý nghĩa của tin tặc, đặt ngữ cảnh vào thông tin kỹ thuật.