**HACKING for DUMMIES**

*Kevin Beaver, CISSP*

**----------------------------------------------------------------------------------------------------**

**CHAPTER I: GIỚI THIỆU VỀ ETHICAL HACKING**

**Trong chương này:**

* Hiểu biết về các mục tiêu của hacker
* Phân biệt giữa “ethical hackers” (hacker đạo đức) và “malicious hackers” (hacker xấu)
* Khám phá quá trình hình thành của hoạt động hack có đạo đức
* Nhận diện các mối nguy mà hệ thống máy tính của bạn phải đối mặt
* Bắt đầu quá trình hack có đạo đức

Cuốn sách này xoay quanh việc hack có đạo đức - đó là việc kiểm tra các máy tính và mạng của bạn nhằm tìm ra các lỗ hổng bảo mật, sau đó vá lại những lỗ hổng này trước khi những kẻ xấu có cơ hội khai thác chúng.

Mặc dù "có đạo đức (ethical)" là một từ thường bị lạm dụng và hiểu sai, từ điển Merriam-Webster định nghĩa "có đạo đức" rất chính xác trong ngữ cảnh của cuốn sách này và các kỹ thuật kiểm tra bảo mật chuyên nghiệp mà tác giả sẽ đề cập - tức là tuân thủ các tiêu chuẩn hành vi chuyên nghiệp được công nhận. Những người làm trong lĩnh vực CNTT có trách nhiệm thực hiện mọi kiểm tra được trình bày trong cuốn sách này một cách công khai và chỉ sau khi đã được sự cho phép của chủ sở hữu hệ thống - do đó có phần tuyên bố từ chối trách nhiệm ở phần giới thiệu.

**SỰ RA ĐỜI CỦA CÁC ETHICAL HACKER TỪ CÁC HACKER**

Chúng ta đều đã nghe nói về hacker. Nhiều người trong chúng ta thậm chí đã phải gánh chịu hậu quả từ hành động của hacker. Vậy hacker là ai? Tại sao việc hiểu về họ lại quan trọng? Những phần sau sẽ cung cấp cho bạn cái nhìn tổng quát về hacker.

**Định nghĩa về hacker**

*Hacker* là một từ có 2 nghĩa:

* Thông thường, hacker là người thích mày mò với phần mềm hoặc các hệ thống điện tử. Hacker thích khám phá và tìm hiểu cách mà hệ thống máy tính hoạt động. Họ đam mê việc phát hiện những cách thức mới để làm việc với công nghệ.
* Gần đây, *hacker* lại mang một nghĩa mới – ám chỉ những người xâm nhập vào hệ thống với mục đích xấu để trục lợi cá nhân. Về mặt kỹ thuật, những tội phạm này được gọi là *cracker* (hacker tội phạm). Cracker bẻ khoá (crack) vào các hệ thống với ý đồ xấu, nhằm mục đích kiếm lợi các nhân như: danh tiếng, lợi nhuận hoặc thậm chí là trả thù. Họ chỉnh sửa, xoá và đánh cắp các thông tin quan trọng, thường khiến người khác phải chịu đựng khổ sở.

Các hacker “mũ trắng” (hacker tốt) không thích bị xếp chung nhớm với các hacker “mũ đen” (hacker xấu). (Những thuật ngữ này xuất phát từ các bộ phim miền Tây, nơi các nhân vật chính diện thường mang cao bồi màu trắng, còn nhân vật phản diện đội mũ đen.) Dù thế nào đi nữa, đa phần mọi người đều gán cho từ “hacker” một nghĩa tiêu cực. Nhiều hacker xấu tuyên bố rằng họ không gây thiệt hại mà chỉ đang “giúp đỡ với mục đích tốt”. Thực tế, đa số các hacker xấu là những “tên trộm điện tử”.

Trong cuốn sách này, tác giả sẽ sử dụng các thuật ngữ sau:

* Hacker (kẻ xấu) – là những người cố gắng xâm nhập vào hệ thống máy tính.
* Ethical hacker (người tốt) – là những người bảo vệ máy tính khỏi các cuộc xâm nhập trái phép.

Hacker thường nhắm đến bất cứ hệ thống nào mà họ nghĩ là có thể xâm nhập được. Một số thích các hệ thống “có danh tiếng” và được bảo mật nghiêm ngặt, nhưng khi hack vào hệ thống của bất kỳ ai đều giúp các cá nhân tăng uy tín trong giới hacker.

**ETHICAL HACKING 101**

Chúng ta cần bảo vệ bản thân khỏi các chiêu trò quấy phá của hacker. Một ethical hacker sở hữu kỹ năng, tư duy và công cụ giống như một hacker nhưng đáng tin cậy hơn. Các ethical hacker thực hiện việc hack như một phần của các bài kiểm tra bảo mật cho hệ thống.

Nếu bạn thực hiện các bài kiểm tra ethical hacking cho khách hàng hoặc đơn giản là chỉ muốn thêm các chứng chỉ cho hồ sơ chuyên môn của bạn, bạn có thể cân nhắc chứng chỉ *Certified Ethical Hacker* do EC-Council tài trợ. Xem thêm thông tin tại trang [www.eccouncil.org/CEH.htm](http://www.eccouncil.org/CEH.htm).

Ethical hacking – còn được gọi là kiểm tra xâm nhập hoặc hack mũ trắng – sử dụng các công cụ, thủ thuật và các kỹ thuật giống hacker nhưng với một sự khác biệt lớn: *Ethical hacking là hợp pháp*. Ethical hacking được thực hiện dưới sự cho phép của đối tượng đó. Mục đích của ethical hacking là phát hiện ra các lỗ hổng từ góc nhìn của hacker để nâng cao bảo mật của hệ thống. Đây là một phần của chương trình quản lý rủi ro thông tin toàn diện, giúp cải thiện an ninh một cách liên tục. Ethical hacking cũng có thể đảm bảo cho những tuyên bố của nhà cung cấp về tính bảo mật cho sản phẩm của họ là chính xác.

Để hack vào hệ thống của chính mình giống như cách những kẻ xấu sẽ làm, chúng ta phải suy nghĩ như họ. Việc hiểu rõ kẻ thù của bạn là điều vô cùng quan trong; hãy xem thêm chi tiết ở Chương II.

**TẠI SAO HACK CHÍNH HỆ THỐNG CỦA BẠN LẠI CẦN THIẾT**

*Để bắt được kẻ trộm, hãy suy nghĩ như kẻ trộm.* Đó là nguyên tắc cơ bản của ethical hacking.

Định luật về trung bình đi ngược lại với công việc bảo mật. Với số lượng hacker ngày càng gia tăng và kiến thức của họ càng được mở rộng, cùng với số lượng lỗ hổng của các hệ thống ngày càng nhiều cộng kèm với các biến số khó lường, sẽ đến lúc mọi hệ thống máy tính đều bị hack hoặc xâm nhập theo cách nào đó. Việc bảo vệ hệ thống của bạn khỏi kẻ xấu – và không chỉ đối phó với các lỗ hổng phổ biến mà ai cũng biết – là điều vô cùng quan trọng. Khi hiểu được các thủ thuật của hacker, bạn sẽ thấy hệ thống của mình dễ bị tấn công đến mức nào.

Việc hack sẽ được nhắm đến các lỗ hổng bảo mật yếu kém và các lỗ hỗng chưa được phát hiện. Tường lửa, mã hoá và các mạng riêng ảo (VPN) có thể tạo ra một cảm giác an toàn giả tạo. Các hệ thống bảo mật này thường chỉ tập trung vào các lỗ hổng ở cấp cao như virus và lưu lượng qua tường lửa mà bỏ qua cách thức hoạt động của hacker. Việc tấn công vào hệ thống của bạn sẽ phát hiện ra các lỗ hổng là bước đi quan trọng để tăng tính an toàn cho hệ thống. Đây là phương pháp duy nhất đã được chứng minh để gia cố hệ thống của bạn trước các cuộc tấn công. Nếu không xác định được điểm yếu, chỉ còn là vấn đề thời gian trước khi các lỗ hổng này bị khai thác.

Với việc các hacker ngày càng trở nên tinh vi và mở rộng kiến thức họ, chúng ta cũng nên làm như vậy. Bạn cần phải suy nghĩ như họ để bảo vệ hệ thống của mình khỏi kẻ xấu. Bạn, với vai trò là một ethical hacker, cần phải có hiểu biết về các hoạt động mà hacker thực hiện và cách để ngăn chặn những hàng vi đó. Bạn nên biết mình cần tìm kiếm điều gì và cách sử dụng thông tin đó để làm gián đoạn các cuộc tấn công của hacker.

Chúng ta không cần bảo vệ hệ thống của mình khỏi mọi thứ. Đơn giản là vì chúng ta không thể làm vậy. Cách duy nhất để bảo vệ tuyệt đối hệ thống máy tính của bạn là ngắt kết nối chúng và khoá kín nó để không ai có thể chạm vào nó – kể cả bạn. Nhưng đó không phải là cách tốt nhất để đảm bảo an toàn thông tin. Điều quan trọng là bảo vệ hệ thống khỏi các lỗ hổng đã biết và các cuộc tấn công phổ biến của hacker.

Chúng ta không thể vá tất cả các lỗ hổng tiềm tàng trên toàn bộ hệ thống máy tính. Chúng ta cũng không thể lên kế hoạch cho mọi cuộc tấn công – đặc biệt là các cuộc tấn công chưa bao giờ được ghi nhận. Tuy nhiên, càng thử kết hợp nhiều tình huống, càng kiểm tra hệ thống một cách toàn diện thay vì chỉ những phần riêng lẻ, chúng ta càng có khả năng phát hiện ra các lỗ hổng ảnh đang tồn tại và gây ảnh hưởng đến hệ thống.

Dù vậy, ethical hacking cũng không nên đi quá xa. Việc gia cố hệ thống trước các cuộc tấn công khó có thể xảy ra có thể không mang lại hiệu quả. Ví dụ, nếu văn phòng của bạn có ít người ra vào và không chạy máy chủ Web nội bộ, bạn có thể không cần lo ngại quá nhiều như một nhà cung cấp dịch vụ Internet. Tuy vậy, ta không thể quên được các mối đe doạ từ bên trong như một trong các nhân viên có ý đồ xấu!

Mục tiêu tổng quan của bạn với vai trò là một ethical hacker nên là:

* Hack hệ thống một cách không gây tổn hại
* Liệt kê các lỗ hổng và khi cần thiết phải báo cáo đến các quản lý cấp cao về sự tồn tại của các lỗ hổng đó.
* Áp dụng kết quả để khắc phục các lỗ hổng và tăng cường bảo mật cho hệ thống của bạn

**HIỂU CÁC MỐI NGUY MÀ HỆ THỐNG CỦA BẠN CÓ THỂ ĐỐI MẶT**

Ta nên biết rằng hệ thống nói chung luôn bị các hacker trên toàn thế giới nhắm đến là một chuyện; việc hiểu rõ các cuộc tấn công cụ thể có thể sẽ xảy ra đối với hệ thống của bạn lại là chuyện khác. Phần này sẽ giới thiệu một số kiểu tấn côn phổ biến, tuy nhiên đây không phải là một danh sách toàn bộ. Để có cái nhìn tổng thể nhất, bạn có thể tham khảo cuốn *Hack Attacks Encyclopedia* của John Chirillo (Wiley Publishing, Inc.).

Nhiều lỗ hổng về bảo mật thông tin không phải là vấn đề nghiêm trọng khi xét riêng lẻ. Tuy nhiên, việc khai thác đồng thời nhiều lỗ hổng có thể gây ảnh hưởng nghiêm trọng. Ví dụ, một cấu hình mặc định của hệ điều hành Windows, mật khẩu tài khoản quản trị viên SQL Server yếu, và máy chủ được lưu trữ trên mạng không dây có thể không đáng lo ngại khi đứng riêng lẻ, nhưng nếu cả ba lỗ hổng này đều đồng thời bị khai thác có thể là một vấn đề lớn.

**TẤN CÔNG PHI KỸ THUẬT**

Những cuộc tấn công khai thác bằng cách thao túng chính con người – các “end users” và kể cả chính bản thân bạn – là điểm yếu lớn nhất trong bất kỳ cơ sở hạ tần máy tính hay mạng nào. Con người thường không tin tưởng lẫn nhau, điều này có thể dẫn đến các cuộc tán công bằng “kỹ nghệ xã hội” *(social egineering)*. Social egineering được định nghĩa là hành vi lợi dụng sự tin tưởng của con người để thu thập thông tin cho mục đích xấu. Khái niệm này sẽ được tác giả trình bày chi tiết hơn ở Chương V.

Các cuộc tấn công phổ biến và hiệu quả khác đối với hệ thống thông tin là tấn công vật lý. Hacker có thể đột nhập vào các toà nhà, phòng máy tính hoặc các khu vực chứa thông tin hay tài sản quan trọng. Các cuộc tấn công vật lý có thể bào gồm “lục lọi rác thải” (tìm kiếm qua bãi rác thải để lấy tài các tài sản trí tuệ, mật khẩu, sơ đồ hệ thống và các thông tin khác).

**TẤN CÔNG VÀO CƠ SỞ HẠ TẦNG MẠNG**

Các cuộc tấn công vào cơ sở hạ tầng mạng có thể dễ thực hiện, vì nhiều mạng có thể được truy cập bất kỳ đâu trên thế giới thông qua hệ thống Internet. Dưới đây là một số ví dụ về các cuộc tấn công vào cơ sở hạ tầng mạng:

* Kết nối vào mạng thông qua một modem không được cấp phép gằn vào máy tính nằm sau tường lửa.
* Khai thác các điểm yếu trong cơ chế truyền tải mạng như TCP/IP hay NetBIOS.
* Tấn công từ chối dịch vụ (DoS) bằng cách làm quá tải mạng với quá nhiều yêu cầu, khiến các yêu cầu chính đáng không được xử lý.
* Cài đặt bộ phân tích mạng trên mạng và thu thập tất cả gói tin truyền qua đó, làm lộ thông tin bí mật dưới dạng văn bản có thể đọc được.
* Kết nối vào mạng thông qua cấu hình không an toàn của mạng không dây 802.11b.

**TẤN CÔNG VÀO HỆ ĐIỀU HÀNH**

Hack vào hệ điều hành (OS) là một phương thức ưa thích của các hacker.Hệ điều hành chiếm một phần lớn trong các cuộc tấn công bởi vì mọi máy tính đều sử dụng hệ điều hành và có nhiều lỗ hổng thường gặp đều có thể bị khai thác dễ dàng.

Thỉnh thoảng, một số hệ điều hành đã tích hợp hệ thống phòng thủ tốt ngay từ đầu – chẳng hạn như Novell NetWare và các phiên bản BSD UNIX – cũng bị tấn công và xuất hiện các điểm yếu. Tuy nhiên, các hacker thường thích tấn công các hệ điều hành như Windows và Linux hơn vì chúng được sử dụng rộng rãi và có nhiều lỗ hổng dễ nhận biết hơn.

Dưới đây là một số ví dụ về các hình thức tấn công vào hệ điều hành:

* Khai thác các lỗ hổng trong các giao thức cụ thể
* Tấn công và các hệ thống xác thực tích hợp sẵn
* Phá vỡ cơ chế bảo mật của hệ thống các tệp (file)
* Bẻ khoá mật khẩu và các cơ chế mã hoá

**TẤN CÔNG ỨNG DỤNG VÀ CÁC HÌNH THỨC TẤN CÔNG CHUYÊN BIỆT KHÁC**

Các ứng dụng thường xuyên trở thành mục tiêu của hacker. Những chương trình như phần mềm máy chỉ e-mail và các ứng dụng web thường xuyên bị tấn công:

* Các ứng dụng sử dụng giao thức HTTP (Hypertext Transfer Protocol) và các SMTP (Simple Mail Transfer Protocol) thường bị nhắm đến vì hầu hết các tường lửa và cơ chế bảo mật khác đều được cấu hình để cho phép truy cập toàn quyền vào các chương trình này từ Internet.
* Các phần mềm độc hại (malware), bao gồm virus, sâu máy tính (worms), Trojan horse và phần mềm gián điệp (spyware) gây ra tắc nghẽn mạng và khiến hệ thống ngừng hoạt động.
* Spam (thư rác) gây tổn hại nghiêm trọng đến khả năng hoạt động của hệ thống và chiếm dụng không gian lưu trữ. Spam cũng có thể chứa các phần mềm độc hại.

Ethical hacking giúp phát hiện được các cuộc tấn công kể trên đối với hệ thống máy tính của bạn. Phần II đến V trong cuốn sách này trình bày chi tiết về các loại tấn công này, cùng với biện pháp đối phó cụ thể mà bạn có thể thực hiện được để bảo vệ hệ thống của mình.

**TUÂN THỦ CÁC QUY TẮC CỦA ETHICAL HACKING**

Mỗi ethical hacker cần tuân theo mốt số nguyên tắc cơ bản. Nếu không, hậu quả có thể rất nghiêm trọng. Đã có nhiều trường họp khi mà các quy tắc này bị bỏ qua hoặc lãng quên khi lên kế hoạch thực hiện kiểm thử ethical hacking và các kết quả đó không hề tích cực.

**Làm việc một cách có đạo đức**

Trong ngữ cảnh này, “đạo đức” được hiểu là làm việc với chuẩn mực đạo đức nghề nghiệp cao và nguyên tắc chuyên môn rõ ràng. Dù bạn thực hiện ethical hacking trên hệ thống máy tính của chính mình hay một tổ chức đã thuê bạn, mọi hành động của bạn phải minh bạch và phục vụ cho các mục tiêu của tổ chức. Tuyệt đối không được có bất kỳ động cơ bí mật nào.

Niềm tin là quy tắc quan trọng nhất. Việc lạm dụng thông tin là điều hoàn toàn bị cấm. Đó chính là hành vi của một hacker xấu.

**Tôn trọng quyền riêng tư**

Hãy xử lý mội thông tin thu thập được với sự tôn trọng cao nhất. Tất cả thông tin bạn thu thập trong quá trình kiểm thử - từ tệp nhật ký duyệt web đến các mật khẩu dưới dạng văn bản đơn thuần – tất cả đều phải được giữ bí mật. Không sử dụng thông tin này để xâm nhập vào dữ liệu nội bộ nhạy cảm của công ty hay đời sống cá nhân. Nếu bạn cảm thấy ai đó cần biết về một vấn đề cụ thể, hãy cân nhắc chia sẻ thông tin đó với người quản lý phù hợp.

Hãy mời những người khác tham gia vào quy trình làm việc của bạn. Đây là cách “giám sát người giám sát” giúp xây dựng lòng tin và hỗ trợ các dự án ethical hacking của bạn.

**Không làm sập hệ thống**

Một trong những sai lầm lớn nhất đó là vô tình làm sập hệ thóng khi thực hiện ethical hacking trên chính hệ thống của mình. Nguyên nhân chính thường do kế hoạch kiểm thử thiếu cẩn thận. Nhiều người kiểm thử không đọc kỹ tài liệu hoặc hiểu sai cách sử dụng và sức mạnh của các công cụ kỹ thuật và bảo mật.

Khi kiểm thử, bạn có thể dễ dàng gây ra hiện tượng DoS trên hệ thống của mình. Việc chạy quá nhiều bài kiểm tra cùng một lúc có thể dẫn đến việc treo hệ thống. Tôi biết điều này vì tôi đã từng phạm sai lầm tương tự ! Đừng vội vàng và cho rằng mạng hoặc máy chủ cụ thể có thể chịu được “áp lực” từ các công cụ quét mạng và đánh giá lỗ hổng.

Nhiều công cụ đánh giả bảo mật có khả năng kiểm soát số lượng các lần test thực hiện trên một hệ thống tại cùng một thời điểm. Những công cụ này đặc biệt hữu ích nếu bạn cần chạy kiểm tra trên hệ thống đang hoạt động trong giờ làm việc bình thường.

Bạn thậm chí có thể vô tình phạm phải điều kiên khoá tài khoản hoặc hệ thống bằng phương pháp social engineering, khiến ai đó thay đổi mật khẩu mà không nhận ra rằng điều này có thể gây ra tình trạng khoá hệ thống.

**QUY TRÌNH ETHICAL HACKING**

Giống như hầu hết các dự án công nghệ thông tin hoặc bảo mật, ehtical hacking cũng cần được lên kế hoạch trước. Các vấn đề về chiến lược và chiến thuật trong quy trình ethical hacking phải được xác định và thống nhất. Lập kế hoạch rất quan trọng đối với mọi loại kiểm thử - từ kiểm tra mật khẩu đơn giản đến thực hiện kiểm thử xâm nhập toàn diện trên ứng dụng web.

**Lập kế hoạch cụ thể**

Phê duyệt ethical hacking là điều cần thiết. Bạn cần đảm bảo rằng những gì bạn đang làm được công khai và minh bạch – ít nhất là với những người có thẩm quyển. Việc có được sử ủng hộ và phê duyệt cho dự án là bước đầu tiên. Những người này có thể là quản lý của bạn, giám đốc điều hành, khách hàng hoặc chính bạn nếu bạn là người đứng đầu. Bạn cần một người sẵn sàng hỗ trợ và phê duyệt kế hoạch của bạn. Nếu không, việc kiểm thử của bạn có thể bị dừng đột ngột nếu ai đó tuyên bố họ chưa từng cho phép bạn thực hiện các bài kiểm thử.

Việc phê duyệt có thể đơn giản như một mẩu ghi nhớ nội bộ từ sếp của bạn nếu bạn thực hiện kiểm thử trên hệ thống của mình. Nếu bạn kiểm thử cho khách hàng, cần có hợp đồng được ký kết, trong đó nêu rõ vai trò và uỷ quyền của khách hàng. Hãy đảm bảo có được phê duyệt bằng văn bản càng sớm càng tốt để đảm bảo rằng thời gian và công sức của bạn không bị lãng phí. Tài liệu này chính là “tấm vé phòng thân” của bạn nếu có ai đó thắc mắc về công việc bạn đang thực hiện.

Việc bạn cần một kế hoạch chi tiết không có nghĩa là bạn phải có hàng loạt quy trình kiểm thử phức tạp. Một sơ suất nhỏ có thể khiến hệ thống của bạn sâp, là điều mà không ai mong muốn. Một phạm vi được xác định rõ ràng nên bao gồm các thông tin sau:

* Hệ thống cụ thể cần được kiểm tra: Định rõ danh sách hệ thống hoặc thành phần sẽ nằm trong phạm vi kiểm thử
* Các rủi ro liên quan: Xác định các nguy cơ tiềm ẩn trong qua trình thực hiện
* Thời điểm kiểm thử và lịch trình tổng quát: Quy định rõ khi nào kiểm thử được tiến hành và khung thời gian cụ thể.
* Phương pháp thực hiện kiểm thử: Mô tả các công cụ, kỹ thuật hoặc phương pháp được sử dụng.
* Mức độ hiểu biết hệ thống trước khi kiểm thử: Hệ thống đã được nghiên cứu trước hay chưa và ở mức độ nào.
* Hành động khi phát hiện lỗ hổng nghiêm trọng: Quy trình ứng phó và cách thông báo khi phát hiện các vấn đề lớn
* Kết quả bàn gia cụ thể: Bao gồm báo cáo đánh giá bảo mật chi tiết và báo cáo tổng quan ở cấp độ cao hơn, liệt kê các lỗ hổng cần khắc phục cùng các biện pháp đối phó được đề xuất.

Khi lựa chọn hệ thống để kiểm thử, bạn nên bắt đầu với các hệ thống quan trọng dễ bị tấn công nhất. Ví dụ, bạn có thể kiểm tra mật khẩu máy tính hoặc thử nghiệm phương pháp social engineering trước khi đi sâu vào các hệ thống phức tạp hơn.

Một kế hoạch dự phòng là điều cần thiết trong quá trình ethical hacking trong trường hợp xảy ra sự cố. Điều gì sẽ xảy ra nế bạn đang đánh giá tường lửa hoặc ứng dụng web và làm cho nó bị dán đoạn? Điều này có thể dẫn đến tình trạng không khả dụng của hệ thống, làm giảm hiệu suất hoặc năng suất của người dùng khác. Thậm chí, hậu quả tệ hơn có thể làm mất tính toàn vẹn của dữ liệu, mất dữ liệu gây ảnh hưởng đến danh tiếng của cá nhân và các tổ chức liên quan.

Hãy xử lý cẩn thận các cuộc tấn công social engineering và DoS. Xác định cách mà những cuộc tấn công này có thể ảnh hưởng đến hệ thống bạn đang kiểm tra và toàn bộ tổ chức.

Thời gian kiểm thử là yếu tố cần được cân nhắc kỹ lưỡng. Bạn sẽ kiểm thử trong giờ làm việc bình thường? Hay vào ban đêm hoặc sáng sớm để không ảnh hưởng đến hệ thống sản xuất? Hãy tham khảo ý kiến của những người liên quan để đảm bảo thời gian kiểm thử được phê duyệt.

Phương pháp tốt nhất là một cuộc tấn công không giới hạn, trong đó mọi kiểu kiểm thử đều có thể thực hiện. Các hacker không tấn công hệ thống của bạn trong một phạm vi giới hạn, vậy tại sao bạn lại làm như thế? Tuy nhiên, cần loại trừ một số phương pháp, chẳng hạn như kiểm thử DoS, social engineering và bảo mật vật lý, nếu chúng có thể gây ra ảnh hưởng nghiêm trọng.

Không chỉ dừng lại ở một lỗ hổng bảo mật. Điều này có thể mang lại cảm giác an toàn giả tạo. Hãy tiếp tục tìm kiếm những gì bạn có thể phát hiện thêm. Tuy nhiên, không có nghĩa là bạn kiểm thử mãi mãi hoặc làm sập toàn bộ hệ thống. Chỉ cần thực hiện phương pháp bạn đang sử dụng cho đến khi bạn không thể khai thác được thêm thông tin mới.

Một trong những mục tiêu bạn có thể hướng đến đó là thực hiện việc kiểm thử mà không bị phát hiện. Ví dụ, bạn có thể đang kiểm thử trên các hệ thống từ xa hoặc tại một văn phòng chi nhánh và bạn không muốn người dùng biết bạn đang làm gì. Điều này giúp việc kiểm tra trở nên thực tế hơn vì người dùng sẽ không thay đổi hành vi của họ khi hệ thống đang được giám sát.

Bạn không cần phải có kiến thức sâu rộng về các hệ thống mà bạn đang kiểm tra – chỉ cần hiểu biết cơ bản là đủ. Điều này giúp bạn bảo vệ tốt hơn hệ thống đã kiểm tra. Việc hiểu hệ thống sẽ dễ dàng hơn nếu kiểm thử trên hệ thống nội bộ hoặc cá nhân. Nếu kiểm thử trên hệ thống của khách hàng, bạn cần phải nghiên cứu kỹ hơn. Hầu hết các khách hàng không yêu cầu một cuộc đánh giá “mù” vì họ thường quan ngại về những rủi ro liên quan. Loại hình kiểm thử bạn thực hiên nên dựa vào nhu cầu của tổ chức hoặc khách hàng.

Chương XIX sẽ đề cập đến việc thuê những hacker “đã hoàn lương”.

**LỰA CHỌN CÔNG CỤ**

Giống như bất kỳ dự án nào, nếu không có công cụ phù hợp cho ethical hacking, bạn sẽ gặp khó khăn trong việc hoàn thành nhiệm vụ một cách hiệu quả. Tuy nhiên, chỉ sử dụng công cụ đúng chưa chắc đã đảm bảo việc phát hiện được tất cá các lỗ hổng bảo mật.

Hiểu rõ những giới hạn cá nhân và kỹ thuật là rất quan trọng. Nhiều công cụ đánh giá bảo mật có thể đưa ra kết quả sai, chẳng hạn như nhận diện nhầm (false positive) hoặc bỏ sót lỗ hổng (false negative). Một số công cụ có thể không phát hiện hết các lỗ hổng. Khi thực hiện các bài kiểm thử social engineering hoặc đánh giá an ninh vật lý, một số điểm yếu có thể bị bỏ qua.

Nhiều công cụ tập trung vào các bài kiểm tra cụ thể, nhưng không có công cụ nào có thể kiểm tra tất cả mọi thứ. Tương tự như việc bạn không thể dùng tuốc nơ vít để đóng đinh, bạn cũng không thể sử dụng trình soạn thảo văn bản để quét cổng mạng mở. Vì vậy bạn cần một số công cụ chuyên biệt để thực hiện từng nhiệm vụ cụ thể. Số lượng công cụ càng đa dạng, việc ethical hacking của bạn sẽ càng dễ dàng.

Hãy đảm bảo bạn đang sử dụng công cụ phù hợp cho từng nhiệm vụ:

* Để bẻ khoá mật khẩu, bạn cần cần công cụ như LC4, John the Ripper hoặc pwdump. Một trình quét cổng mạng chung như SuperScan có thể không phù hợp để bẻ khoá mật khẩu.
* Để phân tích chuyên sâu ứng dụng web, một công cụ đánh giá ứng dụng web như Whisker hoặc WebInspect sẽ phù hợp hơn một trình phân tích mạng như Etheral

Khi chọn công cụ bảo mật phù hợp, hãy tham khảo ý kiến từ đồng nghiệp hoặc cộng đồng trực tuyến. Một tìm kiếm đơn giản trên Google Groups hoặc duyệt qua các cổng thông tin về bảo mật như SecurityFocus.com, SearchSecurity.com và Itsecurity.com thường mang lại những phản hồi hữu ích từ các chuyên gia bảo mật khác.

Có hàng trăm, thậm chí hàng ngàn công cụ có thể được sử dụng cho ethical hacking – từ lời nói, hành động của bạn đến các chươg trình đánh giá lỗ hổng dựa trên phần mềm hoặc các công cụ phân tích mạng dựa trên phần cứng. Sau đây là danh sách một số công cụ yêu thích của tác giả, bao gồm công cụ thương mại, phần mềm miễn phí và mã nguồn mở:

* Nmap
* EtherPeek
* SuperScan
* QualysGuard
* WebInspect
* LC4 (trước đây là L0phtcrack)
* Network Stumbler
* ToneLoc

Một số công cụ phổ biến khác:

* Internet Scanner
* Ethereal
* Nessus
* Nikto
* Kismet
* THC-Scan

Ta sẽ thảo luận về các công cụ này và nhiều công cụ khác trong phần II đến phần V, nơi các hình thức tấn công cụ thể sẽ được đi sâu vào. Phụ lục A chứa danh sách đầy đủ hơn về các công cụ này để bạn tham khảo.

Khả năng của nhiều công cụ bảo mạt và hack thường bị hiểu sai. Sử hiểu nhầm này đã khiến một số công cụ tuyệt vời như SATAN (Security Administrator Tool for Analyzing Networks) và Nmap (Network Mapper) bị đánh giá không đúng mức.

Một số công cụ trong số này rất phức tạp. Dù sử dụng công cụ nào, bạn nên làm quen với chúng trước khi bắt đầu. Dưới đây là một số cách để thực hiện điều đó:

* Đọc tệp readme và/hoặc các tài liệu hướng dẫn trực tuyến đi kèm công cụ.
* Nghiên cứu hướng dẫn sử dụng dành cho các công cụ thương mại.
* Cân nhắc tham gia các khóa đào tạo chính thức từ nhà cung cấp công cụ bảo mật hoặc bên thứ ba, nếu có sẵn.

Những đặc điểm cần tìm kiếm trong các công cụ phục vụ kiểm tra đạo đức:

* Tài liệu đầy đủ: Cung cấp hướng dẫn sử dụng chi tiết.
* Báo cáo chi tiết về các lỗ hổng: Bao gồm cách khai thác và cách khắc phục các lỗ hổng đó.
* Cập nhật và hỗ trợ: Được cung cấp kịp thời khi cần.
* Báo cáo tổng quan cấp cao: Dễ hiểu và có thể trình bày cho quản lý hoặc những người không chuyên về công nghệ.

Những tính năng này có thể giúp bạn tiết kiệm thời gian và công sức khi viết báo cáo.

**THỰC THI KẾ HOẠCH**

Thực hiện ethical hacking đòi hỏi sự kiên nhẫn và bền bỉ. Thời gian và sự cẩn trọng rất quan trọng trong quá trình này. Cần cẩn thận khi tiến hành các bài kiểm tra vì một hacker trong mạng lưới của bạn hoặc một nhân viên có vẻ vô hại quan sát bạn có thể lợi dụng thông tin này chống lại bạn.

Trên thực tế, không thể đảm bảo rằng hệ thống của bạn không có hacker trước khi bắt đầu. Thay vào đó, hãy giữ mọi thứ yên lặng và riêng tư nhất có thể, đặc biệt khi truyền tải và lưu trữ kết quả kiểm tra. Nếu có thể, hãy mã hóa các email và tệp của bạn bằng công cụ như Pretty Good Privacy (PGP) hoặc một phương pháp tương tự. Tối thiểu, hãy bảo vệ chúng bằng mật khẩu.

Giờ đây, bạn đang trong nhiệm vụ do thám. Thu thập càng nhiều thông tin càng tốt về tổ chức và hệ thống của bạn, tương tự như cách các hacker xâm nhập. Hãy bắt đầu từ cái nhìn tổng quan và dần dần thu hẹp phạm vi:

1. *Tìm kiếm trên Internet:* Tìm kiếm tên tổ chức, tên hệ thống máy tính và mạng, cũng như địa chỉ IP của bạn. Google là một nơi tuyệt vời để bắt đầu.
2. *Thu hẹp phạm vi:* Tập trung vào các hệ thống cụ thể mà bạn đang kiểm tra. Các đánh giá sơ bộ về cấu trúc bảo mật vật lý hoặc ứng dụng web có thể tiết lộ nhiều thông tin quan trọng.
3. *Tập trung sâu hơn:* Quan sát kỹ hơn và thực hiện các bài quét hoặc kiểm tra chi tiết trên hệ thống của bạn.
4. *Thực hiện tấn công thử nghiệm, nếu đây là một phần trong kế hoạch của bạn.*

**ĐÁNH GIÁ KẾT QUẢ**

Hãy đánh giá những kết quả bạn đã thu được để xác định các lỗ hổng, với giả định rằng chúng chưa từng được phát hiện trước đây. Đây là lúc kiến thức của bạn phát huy tác dụng. Việc đánh giá kết quả và liên kết các lỗ hổng cụ thể được phát hiện là một kỹ năng sẽ cải thiện qua thời gian và kinh nghiệm. Cuối cùng, bạn sẽ hiểu hệ thống của mình rõ như bất kỳ ai khác. Điều này giúp quy trình đánh giá trở nên đơn giản hơn trong tương lai.

Gửi một **báo cáo chính thức** đến ban lãnh đạo cấp cao hoặc khách hàng, tóm tắt các kết quả đạt được. Hãy đảm bảo rằng các bên liên quan được thông báo để minh chứng rằng công sức của bạn và ngân sách họ đầu tư đã được sử dụng hợp lý. Chương 17 sẽ trình bày chi tiết quy trình này.

**TIẾP TỤC TIẾN HÀNH**

Khi đã hoàn thành các bài kiểm tra, bạn vẫn cần triển khai phân tích và các khuyến nghị để đảm bảo hệ thống được bảo mật.

Các lỗ hổng bảo mật mới liên tục xuất hiện. Hệ thống thông tin không ngừng thay đổi và trở nên phức tạp hơn. Các đợt xâm nhập của hacker và lỗ hổng bảo mật thường xuyên được phát hiện. Bạn thậm chí có thể khám phá ra những lỗ hổng mới! Các bài kiểm tra bảo mật chỉ là **một cái nhìn tóm tắt** về tình trạng bảo mật của hệ thống tại một thời điểm nhất định. Mọi thứ có thể thay đổi bất kỳ lúc nào, đặc biệt sau các lần nâng cấp phần mềm, bổ sung hệ thống máy tính, hoặc áp dụng bản vá. Hãy lên kế hoạch kiểm tra thường xuyên (ví dụ: hàng tuần hoặc hàng tháng). Chương 19 sẽ trình bày cách quản lý các thay đổi liên quan đến bảo mật.

--------------------------------------------------------------------------------------------

**CHAPTER 2: GIẢI MÃ TƯ DUY CỦA HACKER**

**Trong chương này:**

* Hiểu rõ về kẻ thù
* Phân tích “chân dung” của một hacker
* Tìm hiểu động cơ của hacker
* Nghiên cứu cách hacker thực hiện công việc

Trước khi bắt đầu đánh giá mức độ bảo mật của hệ thống của mình, bạn cần hiểu rõ về những kẻ thù mà bạn đang đối mặt. Nhiều nhà cung cấp sản phẩm bảo mật thông tin và các chuyên gia khác thường nói rằng bạn cần bảo vệ hệ thống của mình khỏi những "kẻ xấu" — cả từ bên trong lẫn bên ngoài. Nhưng điều đó thực sự có ý nghĩa gì? Làm thế nào để bạn hiểu được cách những kẻ này suy nghĩ và hoạt động?

Hiểu được mục tiêu của hacker sẽ giúp bạn hiểu cách chúng hoạt động. Và khi hiểu được cách chúng hoạt động, bạn có thể nhìn nhận hệ thống thông tin của mình từ một góc độ hoàn toàn mới. Trong chương này, tôi sẽ mô tả những gì bạn phải đối mặt, ai thực sự là những người đang thực hiện việc hack, động cơ và phương thức của họ, để bạn có sự chuẩn bị tốt hơn cho các bài kiểm tra hack đạo đức của mình.

**NHỮNG ĐIỀU BẠN ĐANG ĐỐI MẶT**

Nhờ vào sự giật gân của truyền thông, định nghĩa về hacker đã thay đổi từ một người tò mò vô hại thành một tội phạm ác ý. Nhiều hacker cho rằng công chúng thường hiểu sai về họ, và điều này phần lớn là đúng. Thật dễ dàng để đưa ra định kiến về những gì bạn không hiểu rõ. Hacker có thể được phân loại dựa trên kỹ năng và động cơ của họ. Một số người có kỹ năng cao và động cơ lành tính; họ chỉ đơn giản tìm kiếm thêm kiến thức. Ở phía ngược lại, những hacker với ý đồ xấu thường tìm kiếm lợi ích cá nhân dưới một hình thức nào đó. Đáng tiếc, các khía cạnh tiêu cực của việc hack thường lấn át những mặt tích cực, dẫn đến sự rập khuôn.

Lịch sử cho thấy, hacker ban đầu hack để theo đuổi tri thức và cảm giác hứng thú từ thử thách. Bỏ qua nhóm *script kiddies*, hacker thường là những người tư duy sáng tạo và mạo hiểm, luôn tìm cách khai thác các lỗ hổng trong máy tính. (*Script kiddies* sẽ được bàn thêm trong phần “Ai Thực Hiện Hack” ở chương này.) Họ nhìn thấy những điều mà người khác thường bỏ qua. Họ tò mò điều gì sẽ xảy ra nếu rút một dây cáp, bật một công tắc, hoặc thay đổi vài dòng mã trong chương trình. Những hacker "trường phái cũ" giống như nhân vật Tim "the Toolman" Taylor — do Tim Allen thủ vai trong sitcom nổi tiếng *Home Improvement* — tin rằng các thiết bị cơ học và điện tử có thể cải thiện nếu được “điều chỉnh lại dây nối.” Tuy nhiên, bằng chứng gần đây cho thấy nhiều hacker hiện nay hack vì mục đích chính trị, cạnh tranh, hoặc thậm chí lợi ích tài chính, chứng minh rằng thời thế đã thay đổi.

Khi còn nhỏ, đối thủ của hacker thường là quái vật và ác nhân trên màn hình trò chơi điện tử. Giờ đây, họ chỉ coi các đối thủ điện tử của mình đơn thuần là những hệ thống. Các hacker thực hiện hành vi ác ý thường không nghĩ đến việc rằng đằng sau các tường lửa và ứng dụng web họ đang tấn công là con người. Họ bỏ qua việc những hành động của mình có thể ảnh hưởng tiêu cực đến cuộc sống của những con người đó, chẳng hạn như làm mất đi sự ổn định trong công việc của họ.

Hacker và các hành vi hack thực tế thúc đẩy sự phát triển của công nghệ bảo mật. Suy cho cùng, hacker không tạo ra lỗ hổng bảo mật; họ chỉ phơi bày và khai thác những lỗ hổng đã tồn tại trong ứng dụng. Đáng tiếc là các tiến bộ trong công nghệ bảo mật không thể ngăn chặn hoàn toàn các cuộc tấn công của hacker, bởi hacker luôn tìm kiếm lỗ hổng và điểm yếu mới. Cách duy nhất để thực sự ngăn chặn những kẻ xấu là thay đổi hành vi của họ, biến họ thành những thành viên xã hội có ích và điều chỉnh tốt.

Dù bạn nhìn nhận hacker theo góc độ nào, một điều chắc chắn là luôn có những người sẽ tìm cách phá hoại hệ thống máy tính của bạn bằng cách hack thủ công hoặc tạo ra và phát tán các loại “sâu tự động” và phần mềm độc hại khác. Bạn phải thực hiện các bước thích hợp để bảo vệ hệ thống của mình trước những nguy cơ này.

**AI LÀ HACKER?**

Các hacker máy tính đã xuất hiện trong nhiều thập kỷ. Kể từ khi Internet trở nên phổ biến vào cuối những năm 1990, chúng ta ngày càng nghe nhiều hơn về hacking. Chỉ một số ít hacker, như John Draper (còn được biết đến với biệt danh Captain Crunch) và Kevin Mitnick, là những cái tên nổi tiếng. Còn rất nhiều hacker vô danh khác đang tìm cách tạo dựng danh tiếng cho bản thân, và chính họ mới là những người đáng chú ý.

Trong một thế giới phân chia rõ ràng trắng đen, rất dễ để mô tả một hacker điển hình. Stereotype phổ biến của một hacker thường là một cậu thiếu niên lập dị, mặt đầy mụn và sống tách biệt xã hội. Nhưng thế giới không chỉ có hai màu trắng và đen mà còn nhiều sắc thái khác nhau, vì vậy cũng có nhiều loại hacker khác nhau.

Hacker cũng là con người như chúng ta, mỗi người đều có đặc điểm riêng biệt, nên rất khó để phác thảo một hồ sơ chính xác về họ. Mô tả chung nhất có thể là: không phải hacker nào cũng giống nhau. Mỗi hacker đều có động cơ, phương pháp, và kỹ năng riêng. Tuy nhiên, một số đặc điểm chung có thể giúp bạn hiểu về họ.

Không phải tất cả hacker đều là những cậu thiếu niên lập dị, sống tách biệt xã hội. Dù vậy, các hacker thường sở hữu sự tò mò, sự tự tin táo bạo, và thường có tư duy rất sắc bén.

**Chính phủ có thực hiện hacking không ?**

Trong các cuộc xung đột với quốc gia khác, một số chính phủ tiến hành chiến tranh thông qua Internet và các hệ thống máy tính khác. Ví dụ, chính phủ Hoa Kỳ được cho là đã phát động các cuộc tấn công mạng chống lại các đối thủ, chẳng hạn như Nam Tư trong khủng hoảng Milosevic cuối những năm 1990 và trong cuộc chiến gần đây tại Iraq.

Chúng ta có đang tiến tới một "Trân Châu Cảng kỹ thuật số"? Tôi không hoàn toàn tin rằng điều này sẽ xảy ra, nhưng phương pháp tiến hành chiến tranh qua mạng đang trở nên phổ biến hơn khi công nghệ phát triển. Nhiều người vẫn hoài nghi về khả năng này, và chính phủ Hoa Kỳ phủ nhận hầu hết sự liên quan của mình. Tuy nhiên, khi thế giới ngày càng phụ thuộc vào công nghệ máy tính, mạng lưới, máy tính cá nhân và Internet, những công cụ này có thể trở thành bệ phóng hoặc chiến trường cho các cuộc xung đột trong tương lai.

Cũng giống như bất kỳ ai cũng có thể trở thành kẻ trộm, kẻ phóng hỏa hay kẻ cướp, bất kỳ ai cũng có thể trở thành hacker, bất kể tuổi tác, giới tính hay chủng tộc. Với một hồ sơ đa dạng như vậy, kỹ năng của các hacker rất khác nhau, từ những người chỉ biết lướt web đến những người viết phần mềm mà cả hacker và ethical hacker đều dựa vào.

* *Script Kiddies*: Đây là những người có hiểu biết cơ bản về máy tính, lợi dụng các công cụ và tài liệu hacking miễn phí trên Internet nhưng không hiểu rõ cách hoạt động bên trong. Họ biết vừa đủ để gây rắc rối nhưng thường hành động rất vụng về, để lại nhiều dấu vết kỹ thuật số. Dù là hình mẫu hacker thường được nhắc đến trên các phương tiện truyền thông, họ thường chỉ cần kỹ năng tối thiểu để thực hiện các cuộc tấn công.
* *Intermediate Hackers*: Đây là những hacker ở trình độ trung cấp, với hiểu biết vừa đủ để gây ra các vấn đề nghiêm trọng. Họ hiểu về máy tính và mạng, thường sử dụng các khai thác đã biết. Một số người trong số này muốn trở thành chuyên gia, và với đủ thời gian và nỗ lực, họ có thể đạt được điều đó.
* *Elite Hackers*: Đây là những chuyên gia hacking tài năng. Họ là những người viết nhiều công cụ hacker, bao gồm các script và chương trình mà script kiddies sử dụng. Những hacker này cũng tạo ra các loại mã độc như virus và worm. Họ có thể xâm nhập vào hệ thống và xóa dấu vết, thậm chí làm cho việc hack trông như do người khác thực hiện.

Elite hackers thường rất kín đáo và chỉ chia sẻ thông tin với những "cấp dưới" khi họ được cho là xứng đáng. Thông thường, để được coi là xứng đáng, các hacker cấp thấp hơn phải sở hữu thông tin độc đáo hoặc chứng minh bản thân qua một vụ hack nổi bật. Những hacker này là mối đe dọa lớn nhất trong an ninh thông tin. Tuy nhiên, may mắn thay, số lượng elite hackers không nhiều như script kiddies.

Một số “*hacktivists*” thực hiện hành vi hack để truyền tải các thông điệp chính trị hoặc xã hội nhằm nâng cao nhận thức của công chúng về một vấn đề nào đó.Ví dụ điển hình của hacktivism bao gồm: các trang web bị chỉnh sửa với thông điệp "Free Kevin" nhằm kêu gọi trả tự do cho Kevin Mitnick, một hacker nổi tiếng từng bị bỏ tù. Các thông điệp liên quan đến việc hợp pháp hóa cần sa. Các cuộc tấn công phản đối vụ va chạm giữa máy bay do thám của Hải quân Hoa Kỳ và máy bay chiến đấu của Trung Quốc năm 2001. Các cuộc tấn công mạng thường xuyên giữa hacker Ấn Độ và Pakistan. Các cuộc tấn công vào trang web của Nhà Trắng trong nhiều năm qua.

Các *“cyberterrorists”* tấn công vào hệ thống máy tính của chính phủ hoặc cơ sở hạ tầng công cộng, như: lưới điện, tháp kiểm soát không lưu và các hệ thống quan trọng khác. Mục đích của họ là làm sập hệ thống hoặc đánh cắp thông tin mật. Những mối đe dọa này được các quốc gia coi trọng, dẫn đến việc áp dụng các biện pháp kiểm soát an ninh thông tin nghiêm ngặt trong các ngành công nghiệp thiết yếu, chẳng hạn như năng lượng.

*“Hackers for hire”* là các hacker làm việc cho các tổ chức tội phạm trên internet. Họ thường tham gia vào các hoạt động phạm pháp để kiếm tiền. Vào cuối năm 2003, cơ quan Cảnh sát Quốc gia Hàn Quốc phá vỡ một tổ chức hacking lớn nhất Internet thời điểm đó, với hơn 4.400 thành viên. Trước đó, tại Philippines, cảnh sát đã triệt phá một tổ chức hack có doanh thu hàng triệu đô la nhờ hack đường dây điện thoại để cung cấp các cuộc gọi giá rẻ. Nhiều hacker kiểu này tìm người thuê mình cho các mục đích tấn công cụ thể, và họ thường kiếm được số tiền rất lớn từ công việc này.

**TẠI SAO HACKER LẠI HACK ?**

Lý do chính khiến hacker hack đơn giản là vì họ có thể! Tuy nhiên, vấn đề này sâu sắc hơn một chút. Hacking là một sở thích thoải mái đối với một số người, họ hack để kiểm tra xem mình có thể và không thể xâm nhập vào đâu, thường chỉ thử nghiệm trên hệ thống của chính mình. Những người này không phải là trọng tâm của nội dung được đề cập ở đây. Tài liệu này tập trung vào những hacker cực đoan và thường có ý định phạm tội.

Nhiều hacker cảm thấy phấn khích khi vượt qua các quản trị viên công nghệ thông tin và an ninh của các tập đoàn và chính phủ. Họ thích xuất hiện trên các tiêu đề báo chí và trở thành những “tội phạm mạng” khét tiếng. Đánh bại một tổ chức hoặc sở hữu kiến thức đặc biệt khiến họ cảm thấy tuyệt hơn về bản thân mình. Những hacker này thường bị cuốn vào cảm giác mãn nguyện tức thời và dần trở nên ám ảnh với cảm giác này. Cảm giác hưng phấn khi xâm nhập vào hệ thống của người khác, đặc biệt là các nhiệm vụ khó khăn, càng khiến họ phấn khích hơn.

Khối kiến thức mà các hacker ác thu được và cái tôi không ngừng lớn lên của họ như là một cơn nghiện và một lối sống riêng của họ. Một số hacker muốn khiến cuộc sống của người khác khốn khổ, một vài hacker khác chỉ muốn có được sự chú ý của xã hội. Một số động lực của hacker bao gồm: trả thù, muốn được thể hiện, tò mò, buồn chán, cảm giác được thách thức, phá hoại, trộm cắp để trục lợi tài chính, phá hoại tài sản, tống tiền, các hành vi gián điệp.

Nhiều hacker ủng hộ chủ nghĩa cá nhân hoặc ít nhất là sự phi tập trung hóa thông tin, vì họ tin rằng tất cả thông tin nên được tự do tiếp cận. Họ cho rằng các cuộc tấn công mạng khác với các cuộc tấn công trong thế giới thực, dễ dàng bỏ qua hoặc không hiểu được hậu quả mà nạn nhân phải gánh chịu.

Một số hacker nói rằng họ không có ý định gây hại hoặc kiếm lợi từ hành động của mình, điều này giúp họ biện minh cho việc làm của mình. Đôi khi, chỉ cần chứng minh quan điểm của họ cũng đủ làm phần thưởng.

Nhiều chủ doanh nghiệp và quản trị viên tin rằng hệ thống của họ không có gì đáng để hacker quan tâm hoặc nghĩ rằng hacker không thể gây ra nhiều thiệt hại nếu đột nhập được. Tuy nhiên, quan niệm này hoàn toàn sai lầm. Hacker có thể xâm nhập vào một hệ thống tưởng chừng không quan trọng để tiếp cận mạng và sử dụng nó làm bàn đạp cho các cuộc tấn công vào những hệ thống khác.

Hacker thường lợi dụng cảm giác an toàn giả mà nhiều người có và tấn công vào bất kỳ hệ thống nào mà họ nghĩ rằng có thể xâm nhập. Họ hiểu rằng thông tin điện tử có thể tồn tại ở nhiều nơi cùng một lúc, và việc chứng minh rằng các hacker đã lấy thông tin đó là một điều khó đoán.

Tương tự, hacker hiểu rằng một trang web bị thay đổi giao diện đơn giản — dù có bị tấn công dễ dàng đến đâu — cũng gây ảnh hưởng xấu đến uy tín của doanh nghiệp. Các trang web sau đây hiển thị những ví dụ về các trang web đã từng bị thay đổi giao diện trong vài năm gần đây (cụ thể là trong các năm trước khi quyển sách được xuất bản):

* [www.2600.com/hacked\_pages](http://www.2600.com/hacked_pages)
* [www.onething.com/archive](http://www.onething.com/archive)

Những trang web bị tấn công như thế này có thể thuyết phục ban lãnh đạo và những người thiếu hiểu biết rằng các mối đe dọa và lỗ hổng bảo mật thông tin cần được giải quyết.

Việc hack ngày càng trở nên dễ dàng hơn vì nhiều lý do:

* Sự gia tăng sự dụng network và Internet.
* Tính ẩn danh mà các hệ thống máy tính trên Internet mang lại.
* Số lượng và sự sẵn có của các công cụ hack ngày càng tăng.
* Trẻ em ngày càng dễ thành thạo các thiết bị điện tử.
* Khả năng các hacker bị điều tra hoặc truy tố nếu bị bắt còn thấp.

Mặc dù phần lớn các cuộc tấn công của hacker không được phát hiện hoặc báo cáo, những hacker bị phát hiện thường không bị truy đuổi hoặc truy tố. Khi bị bắt, hacker thường biện minh rằng hành động của họ mang tính xây dựng và có lợi cho xã hội: họ chỉ ra các lỗ hổng trước khi có người khác lợi dụng chúng. Dù vậy, nếu công lý được thực thi, điều này có thể làm suy giảm hệ thống phần thưởng “danh tiếng và vinh quang” mà hacker thường theo đuổi.

Những hacker tội phạm này chỉ chiếm thiểu số, vì vậy bạn không phải đối mặt với hàng triệu kẻ xấu. Nhiều hacker khác chỉ đơn thuần yêu thích việc khám phá và tìm hiểu cách các hệ thống máy tính hoạt động.

**Hacking nhân danh tự do**

Nhiều hacker có những hành động mâu thuẫn với mục tiêu mà họ tuyên bố theo đuổi — đó là đấu tranh cho quyền tự do cá nhân và mong muốn không bị quấy rầy, trong khi lại thích xâm nhập vào đời tư của người khác. Nhiều hacker tự nhận là những người ủng hộ tự do dân sự, bảo vệ các nguyên tắc về quyền riêng tư và tự do cá nhân. Tuy nhiên, hành động của họ lại hoàn toàn trái ngược: họ xâm phạm quyền riêng tư và tài sản của người khác. Thậm chí, họ thường đánh cắp tài sản và quyền lợi của người khác, nhưng sẵn sàng làm mọi cách để đòi lại quyền lợi của chính mình khi bị tước đoạt.

Một ví dụ điển hình là cuộc đối đầu với các vấn đề liên quan đến bản quyền và Hiệp hội Công nghiệp Ghi âm Hoa Kỳ (RIAA). Các hacker đã làm đủ mọi cách để chứng minh quan điểm của mình, từ việc thay đổi giao diện các trang web của những tổ chức ủng hộ bản quyền đến việc chia sẻ nhạc bất hợp pháp thông qua các nền tảng hợp pháp như Kazaa, Gnutella và Morpheus.

**LÊN KẾ HOẠCH VÀ TẤN CỐNG**

Các phong cách tấn công của hacker rất đa dạng:

* *Nhóm hacker chuẩn bị kỹ lưỡng:* Một số hacker lên kế hoạch từ lâu trước khi thực hiện một cuộc tấn công lớn. Họ thu thập các mẩu thông tin nhỏ và tiến hành các cuộc tấn công một cách bài bản. (Sẽ được trình bày chi tiết trong Chương 4.) Những hacker này thường khó bị phát hiện và theo dõi hơn.
* *Nhóm hacker thiếu kinh nghiệm:* Thường là những *script kiddies*, những hacker này hành động mà không suy nghĩ thấu đáo. Ví dụ, họ có thể thử sử dụng Telnet để truy cập trực tiếp vào bộ định tuyến (router) của một tổ chức mà không che giấu danh tính. Một số khác có thể cố gắng thực hiện tấn công từ chối dịch vụ (DoS) vào máy chủ email Microsoft Exchange mà không kiểm tra phiên bản hay các bản vá đã cài đặt. Đây thường là nhóm dễ bị bắt nhất.

Dù cộng đồng hacker ngầm là một cộng đồng, nhưng nhiều hacker — đặc biệt là những hacker *elite* — không chia sẻ thông tin với số đông. Phần lớn công việc của hacker được thực hiện độc lập với nhau. Tuy nhiên, những hacker kết nối với nhau thường sử dụng các hệ thống bảng tin (BSS) riêng tư, địa chỉ email ẩn danh, các trang web dành cho hacker, Internet Relay Chat (IRC). Bạn có thể truy cập một số trang web này để theo dõi xem các hacker đang làm gì.

Dù sử dụng phương pháp nào, hầu hết các hacker ác đều khai thác sự thiếu hiểu biết của mọi người. Họ hiểu rõ những yếu tố sau trong bảo mật thế giới thực:

* *Hệ thống không được quản lý đúng cách:* Phần lớn các hệ thống mà hacker muốn tấn công không được quản lý đúng cách. Các hệ thống máy tính không được cập nhật bản vá, bảo mật, và giám sát như cần thiết. Hacker thường có thể tấn công mà qua mặt được các hệ thống tường lửa, hệ thống phát hiện xâm nhập (IDS), và hệ thống xác thực.
* *Thông tin hệ thống ngày càng phức tạp:* Mỗi năm, các hệ thống thông tin trở nên phức tạp hơn. Điều này là một lý do nữa khiến các quản trị viên hệ thống và bảo mật không thể theo kịp sự xuất hiện của những lỗ hổng mới.

Thời gian luôn có lợi cho hacker. Bằng cách tấn công qua máy tính thay vì trực tiếp, hacker có thể kiểm soát khi nào thực hiện cuộc tấn công của mình.

* Những cuộc tấn công có thể được thực hiện từ từ, làm cho chúng khó phát hiện.
* Thường thì các cuộc tấn công được thực hiện vào giờ ngoài giờ làm việc thông thường - thường là vào ban đêm. Vào thời gian này, các biện pháp phòng thủ yếu hơn - với ít bảo vệ vật lý hơn và ít giám sát xâm nhập hơn - khi các quản trị viên mạng (hoặc bảo vệ) đang ngủ.

Nếu bạn muốn biết chi tiết về cách thức hoạt động của một số hacker hoặc muốn cập nhật các phương pháp hacker mới nhất, bạn có thể tham khảo một số tạp chí sau:

* *2600 — The Hacker Quarterly* ([www.2600.com](http://www.2600.com)): Tôi đã tìm thấy rất nhiều thông tin hữu ích trong tạp chí này.
* *PHRACK* ([www.phrack.org](http://www.phrack.org)).
* *Computer Underground Digest* ([www.soci.niu.edu/~cudigest](http://www.soci.niu.edu/~cudigest)).

Ngoài ra, bạn cũng có thể truy cập trang web của Lance Spitzner tại [www.tracking-hackers.com](http://www.tracking-hackers.com) để tìm hiểu về việc sử dụng honeypots để theo dõi hành vi hacker.

Hacker học hỏi từ những sai lầm trong các cuộc tấn công của mình. Mỗi sai lầm giúp họ tiến gần hơn một bước tới việc đột nhập vào hệ thống của ai đó. Họ sử dụng những kinh nghiệm này khi thực hiện các cuộc tấn công sau.

**DUY TRÌ SỰ ẨN DANH**

Các hacker thông minh luôn muốn giữ một hình thức "thấp và kín". Việc che giấu dấu vết là ưu tiên hàng đầu. Thực tế, thành công của họ thường phụ thuộc vào điều này. Họ không muốn gây sự chú ý để có thể quay lại và truy cập vào các hệ thống trong tương lai. Các hacker thường duy trì sự ẩn danh bằng cách sử dụng một trong những kỹ thuật sau:

* Hacker có thể sử dụng tài khoản quay số mượn hoặc đánh cắp từ bạn bè hoặc các nhà tuyển dụng trước đó.
* Sử dụng các máy tính công cộng tại thư viện, trường học, hoặc các ki-ốt trong trung tâm mua sắm địa phương.
* Những dịch vụ như máy chủ proxy Internet hoặc dịch vụ ẩn danh giúp hacker che giấu địa chỉ IP thật của mình.
* Sử dụng các dịch vụ email miễn phí dùng một lần để tạo tài khoản mà không lộ danh tính.
* Các hacker có thể lợi dụng các máy chủ email mở để gửi thư mà không bị phát hiện. (email relays)
* Các máy tính không bảo mật – hay còn được gọi là zombies – là các máy tính bị hacker kiểm soát của các tổ chức khác.
* Hacker cũng có thể lợi dụng chính các máy tính hoặc máy chủ trong mạng của nạn nhân để che giấu danh tính của mình.

Khi hacker sử dụng đủ bàn đạp cho các cuộc tấn công của mình, việc truy dấu vết sẽ trở nên rất khó khăn.