0x100

Einführung

Der Begriff Hacking beschwört Bilder von elektronischem Vandalismus, Spionage, gefärbten Haaren und Body-Piercings herauf. Die meiste Leute verbinden Hacking mit Gesetzesverstößen und gehen davon aus, dass jeder, der sich für Hacking interessiert, ein Krimineller ist. Natürlich gibt es Leute, die Hacking-Methoden nutzen, um Gesetze zu brechen, doch in Wirklichkeit geht es beim Hacking um etwas anderes. Tatsächlich geht es beim Hacking eher darum, Gesetzen zu folgen, als diese zu brechen. Das Wesentliche beim Hacking ist das Auffinden von unbeabsichtigten oder übersehenen Anwendungsmöglichkeiten von Regeln, die auf neue und originelle Weise angewendet werden, um ein Problem zu lösen, wie immer dieses auch aussehen mag.

Das folgende mathematische Problem verdeutlicht diese Charakterisierung:

> Verwenden Sie jede der Zahlen1, 3, 4 und 6 genau einmal mit einer der vier Grundrechenarten (Addition, Subtraktion, Multiplikation und Division), um auf das Ergebnis 24 zu kommen. Jede Zahl muss genau einmal verwendet werden, wobei Sie sich die Reihenfolge der Operationen aussuchen können. So wäre $3\times(4+6)+1=31$ beispielsweise gültig, wenn auch nicht richtig, weil es nicht 24 ergibt.

Die Regeln für dieses Problem sind genau definiert und einfach, die Antwort hingegen ist es nicht. Wie bei der Lösung dieses Problems (die Sie auf der letzten Seite dieses Buches finden) folgen »gehackte« Lösungen den Regeln des Systems, nutzen diese Regeln aber gegen die übliche Intuition. Das verschafft Hackern den Vorsprung, der es ihnen erlaubt, Probleme auf eine Art und Weise zu lösen, die für diejenigen unvorstellbar ist, die sich auf konventionelles Denken und konventionelle Methoden beschränken.

Seit den Anfängen der Computertechnik haben Hacker kreativ Probleme gelöst. In den späten 1950ern erhielt der Modelleisenbahn-Club des MIT eine Sachspende, die hauptsächlich aus Teilen alter Telefonanlagen bestand. Die Mitglieder des Clubs nutzten diese Teile zum Aufbau eines komplexen Systems, das es mehreren »Fahrern« erlaubte, verschiedene Teile der Strecke zu steuern, indem sie sich in die entsprechenden Abschnitte einwählten. Sie nannten diese neue und originelle Nutzung von Telefonanlagen *Hacking*. Viele Leute betrachten diese Gruppe als die ursprünglichen Hacker. Die Gruppe verlegte sich dann aufs Programmieren früher Computer wie der IBM 704

und der TX-0 (mittels Lochkarten und Lochstreifen). Während andere sich damit zufrieden gaben, Programme zu schreiben, die einfach Probleme lösten, waren die frühen Hacker davon besessen, Programme zu schreiben, die die Probleme *gut* lösten. Ein neues Programm, das das gleiche Ergebnis mit weniger Lochkarten erreichte, wurde als besser betrachtet, selbst wenn es das gleiche tat. Der wesentliche Unterschied war die Art und Weise, wie das Programm zu seinen Ergebnissen kam – mit *Eleganz*.

Die Fähigkeit, die Anzahl der von einem Programm benötigten Lochkarten zu reduzieren, bewies eine kunstfertige Beherrschung des Computers. Ein schöner handgearbeiteter Tisch kann eine Vase ebenso tragen wie eine Milchkanne, aber das eine sieht mit Sicherheit wesentlich besser aus als das andere. Frühe Hacker haben gezeigt, dass technische Probleme künstlerische Lösungen haben können, und haben dadurch die Programmierung von einer reinen Ingenieurleistung zu einer Kunstform erhoben.

Wie viele andere Kunstformen ist auch das Hacking oft missverstanden worden. Die wenigen, die es verstanden, begründeten eine informelle Subkultur, die sich intensiv auf das Erlernen und Beherrschen dieser Kunst konzentrierte. Sie glaubten, dass Informationen frei sein sollten, und alles, was dieser Freiheit im Weg stand, umgangen werden müsste. Zu diesen Hindernissen zählten Autoritätspersonen, die Bürokratie des Hochschulbetriebs und jede Form von Diskriminierung. In einem Meer Diplomgieriger Studenten verachtete diese inoffizielle Gruppe von Hackern konventionelle Ziele und konzentrierte sich stattdessen auf das Wissen selbst. Dieser Antrieb, ständig zu lernen und zu entdecken, überwand sogar die durch Diskriminierung gezogenen Grenzen, was die Akzeptanz des zwölfjährigen Peter Deutsch durch den MIT-Modelleisenbahn-Club beweist, als er sein Wissen um die TX-0 und seinen Wunsch zu lernen demonstrierte. Alter, Rasse, Geschlecht, akademischer Grad und sozialer Status waren nicht die primären Kriterien, an denen der Wert eines anderen gemessen wurde. Allerdings nicht aus dem Wunsch nach Gleichheit, sondern aus dem Wunsch heraus, die aufkommende Kunst des Hackings voranzutreiben.

Die ursprünglichen Hacker entdeckten Glanz und Eleganz in den üblicherweise trockenen Wissenschaften der Mathematik und Elektronik. Sie sahen die Programmierung als Form des künstlerischen Ausdrucks und den Computer als das Instrument ihrer Kunst. Ihr Wunsch, zu analysieren und zu verstehen, sollte nicht die künstlerischen Bemühungen entmystifizeren, sondern diente lediglich dazu, ein war besseres Verständnis zu erhalten. Die wissensgesteuerten Werte führten schließlich zu dem, was als *Hacker-Ethik* bezeichnet wurde: die Anerkennung der Logik als Kunstform und die Förderung des freien Informationsflusses sowie das Überwinden konventioneller Grenzen und Beschränkungen mit dem einfachen Ziel, ein besseres Verständnis für die Welt zu erlangen. Das ist kein neuer kultureller Trend; die Pythagoräer im antiken Griechenland hatten eine vergleichbare Ethik und Subkultur, auch wenn sie keine Computer besaßen. Sie sahen die Schönheit der Mathematik und entdeckten viele elementare Grundsätze der Geometrie. Dieser Wissenshunger und seine nutzbringenden Nebenprodukte ziehen sich durch die gesamte Geschichte, von den Pythagoräern über Ada Lovelace hin zu Alan Turing und den Hackern des MIT-Modelleisenbahn-Clubs.

Moderne Hacker wie Richard Stallman und Steve Wozniak haben dieses Hacker-Erbe fortgeführt und brachten uns moderne Betriebssysteme, Programmiersprachen, Personal Computer und viele andere Technologien, die wir heute täglich verwenden.

Wie unterscheidet man nun zwischen den guten Hackern, die uns das Wunder des technischen Fortschritts bringen, und den bösen Hackern, die unsere Kreditkartennummern stehlen? Der Begriff *Cracker* wurde geprägt, um die bösartigen Hacker von den guten zu unterscheiden. Journalisten wurde gesagt, dass Cracker die bösen Buben sind, während die Hacker die guten Jungs seien. Hacker halten sich an die Hacker-Ethik, während Cracker nur daran interessiert sind, das Gesetz zu brechen und schnelles Geld zu verdienen. Cracker wurden als weit weniger talentiert betrachtet als die Elite-Hacker, da sie einfach von Hackern entwickelte Tools und Skripte verwendeten, ohne zu verstehen, wie diese funktionierten. *Cracker* war als Sammelbegriff für all jene gedacht, die etwas Gewissenloses mit einem Computer anstellten, etwa Software-Piraterie oder das Verschandeln von Websites, die aber gleichzeitig (das Schlimmste von allem) nicht verstanden, was sie da eigentlich taten. Aber nur sehr wenige Leute benutzen heutzutage diesen Begriff.

Die fehlende Popularität dieses Begriffs liegt möglicherweise in der verwirrenden Etymologie. Mit *Cracker* waren ursprünglich diejenigen gemeint, die Software-Copyrights knackten und Kopierschutzverfahren aushebelten. Die aktuelle Unbeliebtheit könnte aber einfach an zwei neuen missverständlichen Definitionen liegen: Cracker sind eine Gruppe von Leuten, die illegale Aktivitäten mit Computern anstellen, und Leute, die relativ unfähige Hacker sind. Nur wenige Technikjournalisten fühlen sich genötigt, Begriffe zu verwenden, die den meisten ihrer Leser nicht vertraut sind. Im Gegensatz dazu sind sich die meisten darüber bewusst, das man mit dem Begriff *Hacker* geheimnissvolles und Können assoziiert, sodass es einem Journalisten leicht fällt, den Begriff *Hacker* zu verwenden. In ähnlicher Weise wird manchmal auch der Begriff *Script-Kiddie* für Cracker verwendet, aber er hat doch nicht den gleichen Klang wie das mystische *Hacker*. Es gibt einige, die immer noch behaupten, es gäbe eine klare Grenze zwischen Hackern und Crackern, aber ich glaube, dass jeder mit dem Geist eines Hackers auch ein Hacker ist, unabhängig davon, welche Gesetze er oder sie dabei brechen mag.

Die aktuellen Gesetze in Bezug auf Kryptografie und kryptographische Forschung lassen diese Grenze zwischen Hackern und Crackern weiter verschwimmen. Im Jahr 2001 wollten Professor Edward Felten und sein Forschungsteam von der Princeton University einen Beitrag veröffentlichen, der die Schwächen verschiedener digitaler Wasserzeichen diskutierte. Dieses Papier war die Antwort auf einen Wettbewerb, den die Secure Digital Music Initiative (SDMI) in ihrer »SDMI Public Challenge« ausgerufen hatte. Die Öffentlichkeit wurde dabei ermuntert, diese Wasserzeichenverfahren zu knacken. Bevor Felten und sein Team das Papier allerdings veröffentlichen konnten, wurde sowohl von der SDMI Foundation als auch von der Recording Industry Association of America (RIAA) gegen sie vorgegangen. Nach dem amerikanischen Digital Millennium Copyright Act (DMCA) aus dem Jahr 1998 ist es gesetzeswidrig, Techni-

ken zu diskutieren oder zur Verfügung zu stellen, die Kontrollen bei Konsumgütern umgehen könnten. Das gleiche Gesetz wurde auch gegen Dmitry Sklyarov angewandt, einen russischen Programmierer und Hacker. Er hatte eine Software geschrieben, um eine allzu einfache Verschlüsselung in Adobe-Software zu umgehen, und präsentierte seine Erkenntnisse auf einer Hacker-Messe in den USA. Das FBI führte eine Razzia durch und verhaftete ihn. Es folgte ein langer Rechtsstreit. Für das Gesetz spielt die Komplexität der Konsumgütersteuerung keine Rolle – technisch gesehen wäre auch das Reverse Engineering oder sogar die Diskussion über Küchenlatein illegal, wenn es in einer Konsumgüterkontrolle verwendet werden würde. Wer sind nun die Hacker und wer die Cracker? Wenn Gesetze die freie Meinungsäußerung behindern, werden dann die guten Jungs, die ihre Meinung äußern, plötzlich zu bösen Buben? Ich glaube, dass der Geist des Hackers den Geist der juristischen Gesetze übersteigt und nicht durch diese definiert wird.

Kernphysik und Biochemie können zum Töten verwendet werden, haben uns aber auch signifikante wissenschaftliche Fortschritte und moderne Medizin gebracht. Wissen an sich ist weder gut noch schlecht. Moral findet sich in der Anwendung von Wissen. Selbst wenn wir es wollten, könnten wir das Wissen über die Umwandlung von Materie in Energie nicht unterdrücken, ebenso wenig wie den ständigen technischen Fortschritt der Gesellschaft. Auch der Hacker-Geist kann weder aufgehalten, noch auf einfache Weise kategorisiert oder analysiert werden. Hacker werden die Grenzen des Wissens und des zulässigen Verhaltens immer weiter vorantreiben und zwingen uns dazu, immer weiter und weiter zu forschen.

Ein Teil dieses Strebens führt zu einer unglaublich nutzbringenden parallelen Entwicklung in Sachen Sicherheit durch den Wettbewerb zwischen angreifenden und verteidigenden Hackern. Genau wie eine schnelle Gazelle versucht, dem Geparden zu entkommen, und der Gepard noch schneller wird, um sie doch noch zu erwischen, bringt der Wettstreit zwischen den Hackern den Computernutzern bessere und stärkere Sicherheitstechniken, aber ebenso auch komplexere und ausgeklügeltere Angriffstechniken. Die Einführung von und der Fortschritt bei Intrusion-Detection-Systemen (IDS) ist ein Musterbeispiel für diesen parallelen Entwicklungsprozess. Die verteidigenden Hacker bauen IDS auf, um ihr Arsenal aufzustocken, während die angreifenden Hacker Techniken entwickeln, um das IDS zu umgehen, was dann wiederum durch größere und bessere IDS-Produkte kompensiert wird. Das Endergebnis dieser Interaktion ist positiv, weil es zu klügeren Menschen, verbesserter Sicherheit, stabilerer Software, originellen Problemlösungstechniken und sogar einem neuen Wirtschaftszweig führt.

Mit diesem Buch wollen wir Ihnen etwas über den wahren Geist des Hackings näherbringen. Wir werden uns verschiedene Hacker-Techniken ansehen (aus der Vergangenheit ebenso wie aus der Gegenwart). Wir werden sie analysieren, um zu lernen, wie und warum sie funktionieren. Zu diesem Buch gehört eine bootfähige Live-CD, die den gesamten hier verwendeten Quellcode sowie eine vorkonfigurierte Linux-Umgebung enthält. Erforschung und Erneuerung ist für die Kunst des Hackens von wesentlicher Bedeutung, deshalb erhalten Sie mit der CD die Möglichkeit, alles zu verfolgen

und eigene Experimente anzustellen. Sie benötigen nur einen *x*86-Prozessor, der von allen Microsoft Windows- und neueren Macintosh-Computern verwendet wird. Legen Sie die CD einfach ein und starten Sie den Rechner neu. Diese alternative Linux-Umgebung tastet Ihr vorhandenes Betriebssystem nicht an. Wenn Sie fertig sind, starten Sie den Rechner einfach neu und entfernen die CD. Auf diese Weise erhalten Sie ein praktisches Verständis für das Hacking und können es entsprechend einschätzen. Das könnte Sie wiederum dazu inspirieren, vorhandene Techniken zu verbessern oder sogar eigene (neue) zu erfinden. Wir hoffen, dass dieses Buch die neugierige Hacker-Natur in Ihnen weckt und Sie dazu bringt, selbst irgend etwas zur Kunst des Hackens beizutragen, egal für welche Seite Sie sich dabei entscheiden.