Vorwort

Die Berichterstattung über Hacking-Attacken und Sicherheitslücken, die Millionen, mitunter Milliarden Geräte betreffen, ist allgegenwärtig. Sie hat die Themen »Hacking« und »IT-Security« in den vergangenen Jahren immer stärker in den Vordergrund gerückt und auch unter »Normalanwendern« ein Bewusstsein dafür geschaffen, dass die Sicherheit der IT-Infrastruktur jeden betrifft.

Viele Computer-, Smartphone- oder ganz allgemein Internetanwender drohen angesichts der vielfältigen Risiken zu resignieren. Dass man »ordentliche« Passwörter verwenden und regelmäßig Updates einspielen sollte, ist den meisten klar – aber darüber hinaus fühlen sich Anwender den Gefahren der zunehmenden Digitalisierung weitgehend schutzlos ausgeliefert.

Tatsächlich ist es primär die Aufgabe von Administratoren, IT-Verantwortlichen und Software-Entwicklern, für mehr Sicherheit zu sorgen. Immer strengere gesetzliche Rahmenbedingungen und der mit Sicherheitslücken verbundene Image-Verlust zwingen Firmen, sich mit Sicherheit intensiver auseinanderzusetzen. Es reicht nicht mehr aus, dass ein Gerät ganz einfach funktioniert, dass Software »schick« aussieht oder dass Smartphones in stylische, immer dünnere Gehäuse verpackt werden. Die Hard- und Software samt der dazugehörigen Server- und Cloud-Infrastruktur muss auch sicher sein – zumindest so sicher, wie es technisch aktuell möglich ist.

Was Hacking mit Sicherheit zu tun hat

Als »Hacking« bezeichnet man umgangssprachlich die Suche nach Wegen, die Sicherheitsmaßnahmen eines Programms oder Systems zu umgehen oder bekannte Sicherheitslücken auszunutzen. Das Ziel besteht in der Regel darin, private bzw. geheime Daten auszulesen oder zu manipulieren.

»Hacking« hat oft einen negativen Kontext, aber das stimmt so nicht: Wenn eine Firma einen sogenannten *Penetration-Test* beauftragt, um durch externe Personen die Sicherheit der eigenen IT-Infrastruktur zu überprüfen, dann bedienen sich die Penetration-Tester derselben Werkzeuge wie kriminelle Hacker. Ähnliches gilt für Sicherheitsforscher, die versuchen, neue Schwachstellen zu finden. Das erfolgt oft im Auftrag von oder in Zusammenarbeit mit großen IT-Firmen, Universitäten oder staatlichen Sicherheitsstellen. Ob ein Hacker »gut« oder »böse« ist, hängt davon ab, wie er oder sie sich nach der Entdeckung einer Schwachstelle verhält. Verantwortungsvolle

Hacker, die Schwachstellen melden und an deren Behebung mitarbeiten, gelten als »White Hats«, kriminelle Hacker als »Black Hats«.

Wenn Sie als Administrator oder IT-Verantwortlicher für die Sicherheit eines Systems zuständig sind, müssen Sie die Werkzeuge kennen, die Hacker anwenden. Damit Sie sich bzw. Ihre Firma verteidigen können, müssen Sie wissen, wie Angreifer agieren. Insofern ist es uns in diesem Buch ein großes Anliegen, Ihnen einen Überblick über die wichtigsten Hacking-Tools und -Arbeitstechniken zu geben. Allerdings machen wir an dieser Stelle nicht Schluss. Vielmehr geht es uns in der Folge darum, wie Sie sich gegen Angreifer wehren können, welche Verteidigungsmaßnahmen Sie ergreifen können, wo Sie die Konfiguration Ihrer Systeme verbessern können. Oder anders formuliert:

Für dieses Buch ist Hacking der Weg, aber nicht das Ziel.
Das Ziel ist es, eine höhere Sicherheit zu erreichen.

Über dieses Buch

In diesem Werk möchten wir eine breit angelegte Einführung in die Themenfelder »Hacking« und »IT-Security« geben. Angesichts von über 1.100 Seiten klingt es vielleicht wie ein Understatement, wenn wir von einer »Einführung« sprechen. Tatsächlich ist es aber so, dass sowohl Hacking als auch Security unermesslich große Wissensgebiete sind.

Beinahe zu jedem Thema, das wir in diesem Buch aufgreifen, könnte man gleich ein eigenes Buch schreiben. Hinzu kommen all die Spezialthemen, auf die wir in unserem Buch gleich gar nicht eingehen. Kurzum: Erwarten Sie nicht, dass dieses Buch allumfassend ist, dass Sie mit der Lektüre dieses Buchs bereits ein Hacking- und Security-Experte sein werden.

Dessen ungeachtet muss es einen Startpunkt geben, wenn Sie sich mit Hacking und Security auseinandersetzen möchten. Diesen Startpunkt versuchen wir hier zu geben. Konkret setzen wir uns nach einer Einführung zum Themenumfeld mit den folgenden Aspekten auseinander:

- Kali Linux (Distribution mit einer riesigen Sammlung von Hacking-Werkzeugen)
- Metasploitable und Juice Shop (virtuelle Testsysteme zum Ausprobieren von Hacking)
- Hacking-Tools (`nmap`, `hydra`, Metasploit, Empire, OpenVAS, SET, Burp, Wireshark usw.)
- Offline Hacking, Zugriff auf fremde Notebooks/Festplatten
- Passwort-Hacking, sicherer Umgang mit Passwörtern
- WLAN, Bluetooth, Funk
- USB-Hacking und -Sicherheit

- Durchführung externer Sicherheitsüberprüfungen
- Penetration-Testing (Client und Server)
- Basisabsicherung: Windows und Linux, Active Directory und Samba
- Cloud-Sicherheit: Amazon S3, Nextcloud/ownCloud, Office 365
- Hacking und Security von Smartphones und anderen Mobile Devices
- Webanwendungen angreifen und absichern
- Exploit-Grundlagen: Buffer-Overflows, Fuzzing, Heap Spraying, Mikroarchitektur-Schwachstellen (Meltdown und Spectre)
- Absicherung und sichere Entwicklung von IoT-Geräten

Die Breite der Themen erklärt, warum dieses Buch nicht einen Autor hat, sondern gleich neun. Eine kurze Vorstellung unseres Teams finden Sie am Ende des Buchs.

Neu in der 2. Auflage

Für die hier vorliegende Auflage haben wir das Buch umfassend aktualisiert. Neu hinzugekommen sind die Behandlung zusätzlicher Hacking-Techniken, Testumgebungen, Tools und Fixes. Besonders erwähnen möchten wir:

- Juice Shop (Testsystem für Web-Hacking mit JavaScript-Schwerpunkt)
- Koadic (Post-Exploitation-Framework)
- Password Spraying
- Fortgeschrittene Web-Hacking-Techniken (z. B. Angriff auf die Objektdeserialisierung)
- Maltego-Transformationen
- SMB-Relaying mit neuen Tools
- WPA-2 PMKID Clientless Attack
- Pwnagotchi (WLAN-Hacking-Software für den Raspberry Pi)
- P4wnP1 (noch eine Angriffsplattform für den Raspberry Pi)
- IoT: AutoSploit (automatisierte Suche nach Schwachstellen)
- IoT: MQTT-Absicherung mit SSL/TLS

Zudem möchten wir unseren Lesern danken, die sich mit Fehlermeldungen und Verbesserungsvorschlägen gemeldet haben. Sten Itermann und andere haben mit wachen Augen dazu beigetragen, Fehler und Unklarheiten aus dem Buch zu tilgen.

Zielgruppe

Wir richten uns mit diesem Buch an Systemadministratoren, Sicherheitsverantwortliche, Entwickler sowie ganz allgemein an IT-Fachkräfte, die bereits über ein gewisses Grundwissen verfügen. Um es überspitzt zu formulieren: Sie sollten zumindest wissen, was die PowerShell oder ein Terminal ist. Und Sie müssen bereit sein, betriebs-

systemübergreifend zu denken: Weder Hacking noch die IT-Sicherheit beschränkt sich heute noch auf Windows- oder Linux-Rechner.

Nicht im Fokus stehen dagegen reine IT-Anwender. Natürlich ist die Schulung von Computeranwendern ein unverzichtbarer Aspekt, um die IT-Sicherheit sowohl zu Hause als auch in Unternehmen zu verbessern. Eine Zusammenstellung von mehr oder weniger trivialen Regeln und Tipps, wie Computer, Smartphones und das Internet im Allgemeinen sicher und verantwortungsvoll zu nutzen sind, erscheint uns in diesem technisch orientierten Buch aber nicht zielführend.

Los geht's!

Lassen Sie sich nicht von der Größe des Themengebiets abschrecken! Wir haben versucht, unser Buch in überschaubare Kapitel zu gliedern. Die meisten davon können Sie weitgehend unabhängig voneinander lesen und sich so Schritt für Schritt einarbeiten, Hacking-Expertise gewinnen und ein besseres Verständnis dafür entwickeln, wie Sie Ihre eigenen Systeme besser absichern können. Sie werden schnell feststellen, dass eine intensivere Auseinandersetzung mit Hacking- und Security-Techniken ungemein faszinierend ist.

Wir hoffen, mit unserem Buch dazu beizutragen, die IT-Sicherheit in Zukunft besser zu managen, als dies bisher der Fall war!

Michael Kofler im Namen des gesamten Autorenteams

Vorwort Klaus Gebeshuber

Die Erfahrungen aus zahlreichen Penetration-Tests zeigen, dass viele Administratoren von Computersystemen und Netzwerken kaum die Möglichkeiten und die Dreistigkeit von Hackern kennen. Ein Angreifer benötigt genau eine Schwachstelle, um in ein System einzudringen, ein Verteidiger muss viele der Möglichkeiten verhindern. Es gibt keine Regeln; kein Weg ist für einen Hacker verboten.

Persönlich haben mich die extreme Kreativität und die technischen Möglichkeiten und Varianten von Hackern schon immer fasziniert. Ich wollte schon immer wissen, was die Bösen können, um mit dem Wissen die gute Seite zu stärken. Das Buch »Die Kunst des Einbruchs« von Kevin Mitnick (mitp-Verlag 2006) entfachte damals meine Neugier für das Thema erst recht.

Es ist mir auch ein großes Anliegen, jungen Leuten einerseits die faszinierenden technischen Möglichkeiten aufzuzeigen und sie andererseits auch für ihre zukünftige Tätigkeit auf der guten Seite zu motivieren. Die *Cyber Security Challenge* mit lokalen Qualifikationen für Schüler und Studierende in mittlerweile 14 europäischen Ländern und einem Europafinale bietet hier eine schöne Möglichkeit, junge Security-Talente zu entdecken und zu fördern.

Klaus Gebeshuber

Vorwort Stefan Kania

Schon oft ist mir aufgefallen, dass bei Samba-Servern einige Aspekte hinsichtlich der Sicherheit außer Acht gelassen werden. Oft werden Samba-Freigaben mit Berechtigungen versehen, um unerlaubte Zugriffe zu vermeiden, aber die Sicherheit des Betriebssystems wird dann manchmal nicht mehr gesehen. Ein Linux-Host mit Samba als Fileserver muss immer aus zwei Blickwinkeln gesehen werden. In meinen Seminaren spreche ich das auch immer an. Schon lange wollte ich diese Sichtweise auf Samba-Systeme genauer beschreiben.

Da kam die Anfrage des Rheinwerk Verlags zu diesem Buch. Das war genau das, was ich mir vorgestellt hatte. Hier geht es nicht um die reine Konfiguration eines Samba-Servers, sondern darum, einen Samba-Server möglichst sicher aufzusetzen. Auch der Rahmen des Buches mit den verschiedenen Werkzeugen, Diensten und Geräten ist genau passend für das Thema. So ist hier ein Buch entstanden, das ich mir selbst immer gewünscht habe. Dass ich jetzt mit meinem Kapitel dazu beitragen kann, freut mich sehr. Ich hoffe, Ihnen als Leser wird dieses Buch genauso gut gefallen wie mir.

Stefan Kania

Grußwort

IT-Sicherheit ist ein Thema, an dem niemand vorbeikommt. Regelmäßig wird die deutsche Öffentlichkeit von Hacking-Vorfällen aufgeschreckt: Ende 2019 wurden die Universität Gießen und die Stadtverwaltung Frankfurt/M. von Schadsoftware lahmgelegt. Auch das Kammergericht Berlin war von einem Angriff durch das Schadprogramm »Emotet« betroffen. Weitere ernstzunehmende Cyber-Attacken sind aktuell durch Kryptotrojaner zu verzeichnen. Datenverschlüsselung und Lösegelderpressung ist *der* Trend der letzten Jahre.

Die Devise heißt also: IT-Sicherheit muss auf der Prioritätenliste ganz nach oben – bei Unternehmen, Organisationen und im öffentlichen Dienst. Aber auch bei Privatanwendern sollte die IT-Sicherheit eine prominentere Rolle spielen.

Angriffe auf IT-Systeme sind für die Täter äußerst attraktiv. Von Online-Zahlungen und -Geschäftsprozessen über Cloud-basierte Dienste bis hin zur immer »smarter« werdenden Welt des Internet of Things (IoT) – IT und digitale Infrastruktur bieten ein großes Angriffsfeld. Gleichzeitig senkt die Anonymität des Netzes die Hemmschwelle dafür, sich an entsprechenden Angriffen zu versuchen.

Wer beim Thema IT- und Datensicherheit spart, der ist schlecht beraten. Wem es dagegen gelingt, den eigenen Mitarbeitern beizubringen, wie »Hacker« denken und agieren, der ist einer robust abgesicherten IT-Infrastruktur schon einen großen Schritt näher. Wer die Angreifer versteht, ist der bessere Verteidiger.

Das vorliegende Kompendium geht mit seinem Anliegen deshalb genau in die richtige Richtung: »Für dieses Buch ist Hacking der Weg, aber nicht das Ziel. Das Ziel ist es, eine höhere Sicherheit zu erreichen«, heißt es im Vorwort. Ich kann dies nur unterstützen: Als Geschäftsführer der SySS GmbH trage ich die Verantwortung für 90 IT Security Consultants, die tagtäglich nichts anderes tun, als auf Wunsch die Systeme unserer Kunden zu »hacken«.

Solche Penetrationstests spüren schnell und effizient Sicherheitslücken auf. Die IT-Verantwortlichen können diese dann beheben – bevor illegale Hacker sie ausnutzen. Gleichzeitig zeigt ein solcher Test und der dazugehörige Abschlussbericht unseren Kunden aber auch im Detail, wie wir als »White Hat Hacker« vorgehen, um Schwachstellen aufzuspüren und diese auszunutzen.

Genau solches Wissen ist von unschätzbarer Bedeutung, wenn es darum geht, die eigenen Systeme immer sicherer zu machen. Das Buch »Hacking & Security« stellt dieses Know-how in kompakter Form für die Praxis zur Verfügung. Ich kann jedem, der beruflich mit IT-Sicherheit zu tun hat, die Lektüre nur wärmstens empfehlen. Bleiben Sie den »bösen« Hackern immer den entscheidenden Schritt voraus.

Sebastian Schreiber, Geschäftsführer SySS GmbH