Kapitel 1
Einleitung

Hardware-Tools werden bei gezielten Attacken von Angreifern vor Ort eingesetzt und können großen Schaden anrichten. Dieses Buch soll Ihnen das Wissen und die Fähigkeiten vermitteln, um Ihr Unternehmen vor diesen Angriffen zu schützen. Es richtet sich an alle, die die verschiedenen Tools kennen und verstehen möchten oder die mittels Penetrationstests oder Security-Awareness-Schulung das Sicherheitsniveau in ihrem Unternehmen verbessern möchten.

Nahezu jeden Tag hören Sie in den Nachrichten Meldungen über erfolgreiche Hacking-Angriffe, neue Sicherheitslücken oder große Datenlecks mit sensiblen Informationen. Gefährlich wird es, wenn Cyber-Kriminelle gezielt einzelne Unternehmen in den Fokus nehmen, um z. B. Industriespionage oder Sabotage zu betreiben. Neben den Angriffen über das Internet erfolgen bei zielgerichteten Attacken auch Angriffe vor Ort.

Bei dieser Art des Angriffs kommen häufig Innentäter zum Einsatz, die sich einerseits hervorragend auskennen und andererseits problemlos direkt vor Ort Angriffe durchführen. Dabei reicht das Spektrum der Angreifer von temporärem Personal, wie etwa Auszubildenden oder Studierenden im Praktikum, über externe Personen, unter anderem das Reinigungspersonal, bis hin zu frustrierten (ehemaligen) Mitarbeitern bzw. Mitarbeiterinnen. Bei Angriffen vor Ort werden Hardware-Tools eingesetzt, die nicht so auffällig sind wie ein schwerer Laptop, sondern die unauffällig in der Hosentasche verschwinden können. Abbildung 1.1 gibt Ihnen einen ersten Überblick über die Hardware, die für solche Angriffe eingesetzt wird.

Mit dieser Hardware können Angreifer etwa digitale Zugangskarten kopieren, Funkverbindungen manipulieren, Schadcode über Schnittstellen einschleusen, Netzwerkkommunikation mitschneiden oder sogar ganze Rechnersysteme zerstören. Die Geräte und Werkzeuge müssen dabei nicht über zwielichtige Kanäle beschafft werden, sondern können in gewöhnlichen Online-Shops gekauft werden. Ursprünglich wurden sie für White-Hat-Hacker, Penetration-Tester, Security-Forschende und Sicherheitsbeauftragte entwickelt, um Schwachstellen selbst aufspüren und anschließend schließen zu können. Allerdings werden sie auch immer wieder von kriminellen Angreifern eingesetzt.

Abbildung 1.1 Hardware-Tools für IT-Sicherheitspenetrationstests

Um sich effektiv vor solchen Angriffen schützen zu können, ist es wichtig, diese Hardware-Tools zu kennen und ihre Funktionsweise zu verstehen. Mit diesem Wissen können Sie selbst IT-Sicherheitspenetrationstests mit Pentest-Hardware durchführen, um so das IT-Sicherheitsniveau Ihrer Umgebung zu kennen und zu verbessern. Mit zielgerichteten Security-Awareness-Schulungen können Sie die eigenen Mitarbeiter und Mitarbeiterinnen sensibilisieren und so die Widerstandskraft gegen Cyber-Attacken nachhaltig erhöhen.

1.1 An wen richtet sich dieses Buch?

Dieses Buch richtet sich an IT-Sicherheitsbeauftragte, IT-Beraterinnen und -Berater sowie an Softwareentwickler, -entwicklerinnen und Admin-Teams, die im Bereich IT-Sicherheit aktiv sind oder dort einsteigen möchten. Die Einarbeitung setzt kein Fachwissen zur IT-Sicherheit voraus. Die einzelnen Bereiche werden ausführlich erläutert. Jedoch ist das Buch auch für Personen geeignet, die regelmäßig mit IT-Sicherheit umgehen; Sie können bei Bedarf entsprechende Abschnitte mit Erläuterungen überspringen. Jede Pentest-Hardware wird von Grund auf erklärt und die konkrete Anwendung wird Schritt für Schritt erläutert.

Zusätzlich richtet sich das Buch an Personen, die entweder selbst Security-Awareness-Schulungen durchführen oder die ihre Vorgesetzten von Maßnahmen überzeugen müssen. Der Vorteil beim Einsatz von Hardware-Tools besteht darin, dass das Themenfeld »IT-Sicherheit« greifbar wird, indem ein physischer Gegenstand in die Hand genommen werden kann. Dadurch kann einerseits ein höheres Interesse geweckt werden, und andererseits helfen die Tools bei der anschaulichen Vermittlung von Inhalten und Szenarien.

1.2 Was wird in diesem Buch vermittelt?

In diesem Buch lernen Sie die am häufigsten eingesetzte Pentest-Hardware praxisorientiert kennen und bauen Wissen auf, wie Sie eigene IT-Sicherheitstests realisieren können. Dadurch sind Sie in der Lage, Bedrohungsszenarien richtig einzuordnen und entsprechende Gegenmaßnahmen zu entwickeln. Mithilfe von Security-Awareness-Schulungen können Sie dieses Wissen weitergeben und das Perosnal sensibilisieren.

Zu diesem Zweck lernen Sie die Hardware-Tools aus unterschiedlichen Perspektiven kennen:

- zum einen aus Sicht der Angreifer, um nachvollziehen zu können, welche Ziele mit dem Angriff verfolgt werden und wie möglicherweise vorgegangen wird, und
- zum anderen aus Sicht der Systembetreiber, um einschätzen zu können, welche Risiken bestehen und welche Schäden angerichtet werden können.

Nachdem Sie dieses Buch gelesen haben, werden Sie in der Lage sein, selbstständig IT-Sicherheitstests mit Pentest-Hardware durchzuführen. Sie können Ihr neues Wissen nutzen, um Security-Awareness-Schulungen durchzuführen oder effektive Schutzmaßnahmen zu implementieren.

1.3 Wie ist dieses Buch aufgebaut?

Dieses Buch besteht aus drei Teilen. Im ersten Teil erläutere ich die Durchführung von IT-Sicherheitspenetrationstests, und im zweiten Teil zeige ich Ihnen, wie erfolgreiche Awareness-Schulungen realisiert werden. Im dritten Teil stelle ich die einzelnen Geräte detailliert vor.

Sie können daher die Reihenfolge Ihrer Lektüre frei gestalten bzw. direkt zu dem jeweiligen Kapitel springen, das für Sie am relevantesten ist.

In **Teil I, »IT-Sicherheitspenetrationstests durchführen«,** lernen Sie, wie ein IT-Sicherheitstest realisiert wird, um damit die eigenen Systeme mit den Mitteln und Me-

thoden zu testen, die ein Angreifer einsetzen würde. Dazu beschreibe ich den typischen Ablauf eines Angriffs und lege dar, welche Prozesse zur Orientierung genutzt werden können. Ich zeige Ihnen, warum trotzdem noch Schwachstellen auftreten können und gebe Ihnen eine Handreichung, wie sinnvolle Tests intern realisiert werden können.

In Kapitel 2, *»IT-Sicherheitspenetrationstests«*, stehen die Planung und Realisierung von IT-Sicherheitstests im Vordergrund. Verschiedene Arten von Tests kommen dabei in unterschiedlichen Bereichen zum Einsatz und bieten je nach Ausrichtung verschiedene Vorteile.

In Kapitel 3, *»Red Teaming als Methode«*, stelle ich eine besonders effiziente Form des Penetrationstests vor. Dabei werden die Mitarbeiter in zwei Teams unterteilt. Das eine Team stellt die Verteidiger, und das andere Team imitiert Angreifer. Damit können sehr realitätsnahe Bedingungen geschaffen werden.

In Kapitel 4, *»Testszenarien in der Praxis«*, spielen wir exemplarisch vier verschiedene praxisnahe Beispiele durch. Viele Teile dieser Szenarien können Sie in Ihren Praxisalltag übernehmen und als Blaupause verwenden.

In **Teil II, »Awareness-Schulungen mit Pentest-Hardware«,** liegt der Fokus auf dem Faktor Mensch. Bei vielen Cyber-Angriffen steht das Personal aller Abteilungen in der vordersten Front. Um dieses Potenzial nutzen zu können, müssen die Mitarbeiterinnen und Mitarbeiter geschult werden. Mit den richtigen Maßnahmen stellen sie einen wichtigen Eckpfeiler der eigenen IT-Sicherheit dar.

In Kapitel 5, *»Security-Awareness-Schulungen«*, zeige ich Ihnen die grundsätzlichen Ziele und Vorteile dieser Art von Sicherheitsmaßnahmen auf. Das Präsenztraining ist dabei eine besondere Form, bei der die Mitarbeiter*innen aktiv mit eingebunden werden können.

In Kapitel 6, *»Erfolgreiche Schulungsmethoden«*, erfahren Sie, wie Sie mit den passenden Methoden die Teilnehmer*innen Ihrer Schulungen für das Thema Informationssicherheit begeistern und so für einen nachhaltigen Wissensaufbau sorgen.

In Kapitel 7, *»Schulungsszenarien in der Praxis«*, stelle ich verschiedene Arten von Schulungen exemplarisch vor und spiele sie mit Ihnen durch. Insgesamt werden vier unterschiedliche Methoden behandelt, um eine große Bandbreite an Anforderungen abzudecken. Damit werden viele Bestandteile behandelt, die Sie als Blaupause verwenden und auf Ihr Unternehmen übertragen können.

In **Teil III, »Hacking- & Pentest-Hardware-Tools«,** lernen Sie die einzelnen Geräte detailliert mit praxisnahen Beispielen kennen und erforschen ihren Funktionsumfang. Dazu sind die Tools nach ihren Wirkungsgebieten in verschiedene Kapitel unterteilt. Jedes dieser Kapitel beginnt mit einem Angriffsszenario, das sich an realen Vorfällen

orientiert, um Ihnen einen Überblick über die Funktionsweise zu bieten. Danach stelle ich die im Szenario beschriebenen Hardware-Tools vor und erläutere die Bedrohungsszenarien. Im Anschluss zeige ich Schritt für Schritt, wie Sie die Pentest-Hardware selbst einsetzen können, um Ihre IT-Sicherheit zu verbessern. Abgerundet wird jedes Kapitel durch praxisorientierte Gegenmaßnahmen, die Ihnen die Möglichkeiten geben, Systeme effektiv abzusichern.

In Kapitel 8, *»Pentest-Hardware-Tools«*, finden Sie einen Überblick über die verfügbaren Geräte und lernen die rechtlichen Aspekte bezüglich ihrer legalen Nutzung kennen. Sie erfahren auch, über welche Quellen Sie die Pentest-Hardware beschaffen können. Abschließend beschreibe ich die Einrichtung der Laborumgebung.

In Kapitel 9, *»Heimliche Überwachung durch Spionage-Gadgets«*, ist die Spionage-Hardware das zentrale Thema. Diese Gadgets werden nicht direkt zusammen mit einem Rechner eingesetzt, sondern werden im Vorfeld eines Angriffs genutzt, um unbemerkt Informationen zu sammeln. Dabei können unter anderem Audioaufnahmen mit getarnten Aufnahmegeräten oder mit GSM-Wanzen angefertigt werden. Fotos und Videos können mit Spionagekameras aufgenommen werden, die sich in alltäglichen Gegenständen verstecken. Außerdem können miniaturisierte GPS-Tracker eingesetzt werden, um die genaue Position von Gegenständen oder Personen festzustellen.

In Kapitel 10, *»Tastatureingaben und Monitorsignale mit Loggern aufzeichnen«*, geht es um Geräte, die vom Nutzer unbemerkt Informationen mitschneiden. Zum Beispiel werden Keylogger zwischen dem Rechner und der Tastatur angeschlossen, um alle Eingaben unbemerkt mitzuschneiden. Neuere Modelle sind sehr klein und haben zusätzlich WLAN integriert. Damit muss ein Angreifer nur noch innerhalb der Reichweite des Netzwerks sein, um an die abgefangenen Informationen zu gelangen. Screenlogger können wie Keylogger eingesetzt werden, protokollieren aber das Signal vom Rechner zum Bildschirm mit regelmäßigen Screenshots.

Kapitel 11, *»Angriffe über die USB-Schnittstelle«*, handelt von Angriffen auf die USB-Standardschnittstelle, die in nahezu jedem Gerät verbaut ist. Mit der Angriffsmethode BadUSB werden virtuelle Geräte wie eine Tastatur mit einem Rechnersystem verbunden und vorab programmierte Befehle zügig ausgegeben. Damit können sogar Systeme ohne Monitor wie Drucker oder Alarmanlagen angegriffen werden. Ein alternatives Angriffsszenario umfasst einen USB-Killer. Dieser führt keine Manipulation durch, sondern zerstört mit einem Stromschlag Bauteile und damit Rechner dauerhaft.

In Kapitel 12, *»Manipulation von Funk-Verbindungen«*, lernen Sie Methoden zur Analyse von Funkverbindungen kennen. Kabellose Übertragungen können hierzu ein-

fach mit einem *Software-Defined Radio* untersucht werden; und sollten keine Schutzmaßnahmen vorliegen, kann sogar ein Signal einfach aufgezeichnet und erneut gesendet werden. Die Gefahr von unverschlüsselten Verbindungen bei Rechnersystemen besteht darin, dass insbesondere Maus- und Tastatureingaben mitgeloggt oder Verbindungen übernommen werden können und darüber ein Angriff realisiert werden kann.

In Kapitel 13, *»RFID-Tags duplizieren und manipulieren«*, geht es um die Gefahren des kontaktlosen Datenaustausches im Nahbereich. Mit diesen Technologien werden häufig Zugänge wie Türen gesichert, jedoch beispielsweise auch Diebstahlsicherungen für Produkte realisiert. Einfache RFID-Systeme können sehr simpel dupliziert werden, wodurch die Erstellung eines digitalen Zweitschlüssels ermöglicht wird. Ein weiteres Szenario umfasst die Manipulation von Produktinformationen bei automatischen Kassensystemen.

In Kapitel 14, *»Bluetooth-Kommunikation tracken und manipulieren«,* befassen wir uns mit der Analyse von Bluetooth-Verbindungen. Gerade Geräte, die *Bluetooth Low Energy* verwenden, wie Smartwatches oder Fitness-Tracker, kommunizieren sehr offen und können dadurch getrackt werden. Sie lernen konkrete Maßnahmen kennen, wie Sie diese Bluetooth-Verbindungen analysieren können.

In Kapitel 15, *»WLAN-Verbindungen manipulieren und unterbrechen«*, geht es einerseits um gezielte Störungen von kabellosen Netzwerken und andererseits um Abhörmöglichkeiten bei schlecht gesicherten Netzwerken. Die gezielte Manipulation einer WLAN-Verbindung kann z. B. genutzt werden, um Überwachungskameras zu deaktivieren oder Betriebsabläufe zu unterbrechen.

In Kapitel 16, *»Kabelgebundene LAN-Netzwerke ausspionieren«*, erfahren Sie, wie sich kabelgebundene LAN-Computernetzwerke mit verschiedenen Hardware-Tools angreifen lassen. Mit Adaptern können sich etwa Angreifer zwischen Rechner und Netzwerk einklinken und dabei unverschlüsselten Datenverkehr einfach aufzeichnen oder ausleiten. Mit einer zusätzlichen Mobilfunkverbindung kann sich ein Angreifer unbemerkt im Netzwerk bewegen.

In Kapitel 17, *»Analyse gefundener Hardware«*, zeige ich Ihnen zu guter Letzt, wie Sie bösartige Hardware, nachdem sie gefunden wurde, auf potenzielle Spuren untersuchen. Dazu analysieren Sie den verwendeten Speicher oder die Netzwerkkonfiguration und -kommunikation. Auf diese Weise lassen sich Informationen finden, um den Ablauf zu rekonstruieren, und die auf die Angreifer hinweisen können.

Abbildung 1.2 zeigt Ihnen die Inhalte des Buchs noch einmal in einer Übersicht.

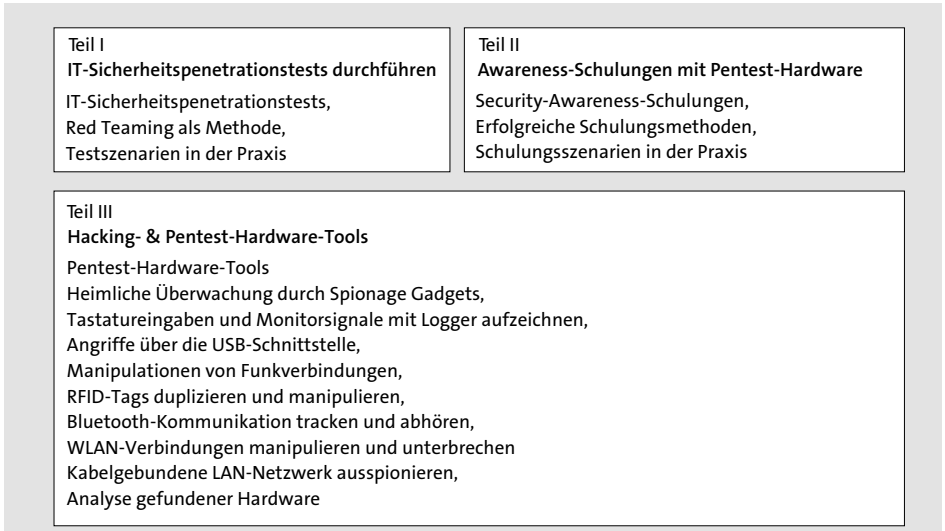

Abbildung 1.2 Der Aufbau des Buches

1.4 Über den Autor

Sie werden es schon auf dem Buch-Cover gesehen haben: Mein Name ist Tobias Scheible. Ich bin begeisterter Informatiker und interessiere mich für Computer, solange ich mich zurückerinnern kann. Neben den technischen Aspekten der IT finde ich vor allem den Faktor Mensch spannend, was mich schon bald zur Wissensvermittlung brachte. So faszinieren mich besonders die Benutzungsfreundlichkeit, Informationsarchitekturen und die Auswirkung neuer Technologien. Außerdem macht es mir großen Spaß, mein Wissen mit anderen zu teilen.

Ich bin als *Cyber Security & IT-Forensik*-Sicherheitsforscher und -Dozent an der Hochschule Albstadt-Sigmaringen tätig. Dort arbeitete ich zuerst als Modulentwickler im Forschungsprojekt *Open Competence Center for Cyber Security* und entwickelte Studieninhalte zu den Bereichen Cloud-Computing und Internettechnologien mit dem Fokus auf der IT-Sicherheit. Danach habe ich mich als Autor und e-Tutor im berufsbegleitenden Masterstudiengang *Digitale Forensik* engagiert und im Bachelorstudiengang *IT-Security* Praktika rund um das Thema Informationssicherheit und digitale Forensik geleitet. Derzeit bin ich als Dozent am *Institut für Wissenschaftliche Weiterbildung* (IWW) der Hochschule im berufsbegleitenden Zertifikatsprogramm tätig. Dort unterrichte ich berufstätige Teilnehmer*innen in speziellen Einzelmodulen in Online-Kursen. Meine Forschungsschwerpunkte liegen in den Bereichen Sicherheit von Web-Anwendungen, Web Forensics, Pentest-Hardware und benutzerzentrierter Didaktik.

Überdies halte ich oft Vorträge und Workshops für Verbände und Unternehmen, u. a. auch offene Veranstaltungen für den VDI. Außerdem schreibe ich mit viel Leidenschaft in meinem Blog *scheible.it* über IT-Sicherheitsthemen und veröffentliche Artikel in verschiedenen Fachzeitschriften.

1.5 Materialien zum Buch

Einige der Hardware-Tools können mit eigenem Code flexibel erweitert werden. Hier im Buch stelle ich dazu einige Beispiele vor, die Sie natürlich nicht abtippen müssen. Alle Code-Beispiele und Links stehen auf der Website des Buches zum Download bereit.

Rufen Sie dazu die Seite *www.rheinwerk-verlag.de/5191* auf. Klicken Sie auf den Reiter MATERIALIEN. Sie sehen dann die herunterladbare ZIP-Datei inklusive einer Kurzbeschreibung des Dateiinhalts. Klicken Sie auf den Button HERUNTERLADEN, um den Download zu starten. Die Struktur innerhalb der ZIP-Datei orientiert sich am Aufbau des Buches, damit Sie die gesuchten Code-Beispiele einfach finden.