Hacking mit Post Exploitation Frameworks

Angriffe verstehen und vorbeugen, Awareness herstellen

DAS VORWORT

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