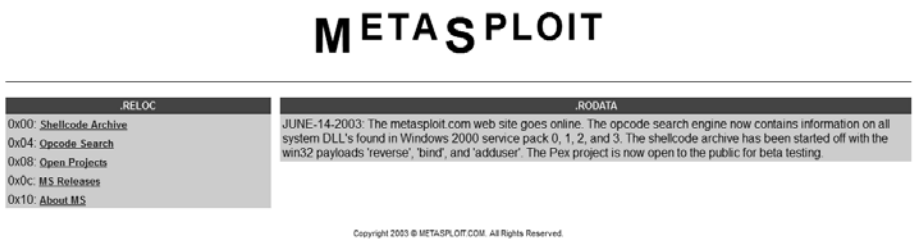
Vorwort

Das Metasploit-Framework ist dort, wo es um Penetrationstests, Sicherheitsanalysen und Forschung im IT-Security- und speziell im Schwachstellenbereich geht, nahezu immer anzutreffen. Wenn von Metasploit gesprochen wird, geht es aber nicht um ein einziges Tool, sondern um eine sehr umfangreiche und komplexe Toolbox, die in Fachkreisen als Framework bezeichnet wird. Dieses Framework besteht aus unterschiedlichsten Teilbereichen, Teilprojekten und Modulen und ist fester Bestandteil der Werkzeugkiste nahezu jedes Pentesters. Der große Umfang ermöglicht einen Einsatz, der weit über typische Exploiting-Vorgänge hinausgeht und eine Anwendung in nahezu allen Phasen eines Penetrationstests bzw. einer technischen Sicherheitsanalyse erlaubt.

Das Framework unterstützt aber nicht nur den Pentester bei seiner täglichen Arbeit, sondern auch den Sicherheitsforscher bei der Erkennung und Analyse potenzieller Schwachstellen und den Administrator bei der besseren Einschätzung vorhandener Schwachstellen.

Die Entwickler von Metasploit gehörten zu den ersten Sicherheitsexperten, die durch ihre Forschungsarbeiten unterschiedliche Exploit-Technologien einem breiten Publikum zugänglich machten. Bereits mit der ersten Veröffentlichung dieses Frameworks im Jahr 2003 sorgten dessen freie Natur und der damit verbundene freie Zugang zu Informationen zur Erkennung und Ausnützung von Schwachstellen für erheblichen Diskussionsstoff. Speziell die Hersteller der betroffenen Produkte sind an keinem freien Zugang zu solchen Informationen interessiert und versuchen, diesen entsprechend zu verhindern.



Metasploit-Webseite aus dem Jahr 2003 [2]

Diese Diskussionen sind in all den Jahren nicht verstummt und werden bis heute regelmäßig erneut entfacht. Hier seien nur kurz die wichtigsten Methoden der Schwachstellenveröffentlichung *Full Disclosure* [3], *Coordinated* und *Responsible Disclosure* [4] [5] angeführt. Für weitere Informationen zu den einzelnen Methoden der Veröffentlichung wird auf die im Anhang angegebenen Online-Ressourcen verwiesen.

Das Jahr 2009/2010 war für das Metasploit-Framework wie auch für die Community wohl eines der spannendsten in der mittlerweile achtjährigen Entwicklungsgeschichte. Durch den neuen Mitspieler Rapid7, einen Hersteller von Vulnerability-Scanning-Lösungen, machte das Metasploit-Framework einen enormen Sprung nach vorne. Mittlerweile lassen sich jeden Tag Änderungen in der Entwicklerversion beobachten. Diese enorm schnelle Entwicklung führte in der jüngeren Vergangenheit zur Veröffentlichung von sechs neuen Versionen innerhalb eines Jahres. Zusätzlich kam es durch den Einfluss von Rapid7 zur Etablierung von zwei neuen, kommerziellen Versionen des Frameworks: Metasploit Express und Metasploit Pro. Durch diese Entwicklungsgeschwindigkeit ist es kaum mehr möglich, alle aktuellen Neuerungen zu kennen und möglichst zeitnah zu testen. Die oftmals nur sehr spärlich über verschiedenste Blogs verteilte Dokumentation macht es neuen Benutzern zudem nicht unbedingt einfacher, sich mit dem Thema *Pentesting mit Metasploit* im Detail zu befassen.

Dieses Buch soll das Metasploit-Framework möglichst umfassend dokumentieren und Interessierten einen Einstieg in diese spannende Thematik ermöglichen. Gleichzeitig will es diejenigen, die sich bereits längere Zeit mit dem Framework befassen, das eine oder andere weitere und spannende Detail oder die eine oder andere neue Idee vermitteln.

Dieses Buch soll sozusagen die Basis abdecken, mit der ein Pentester arbeiten kann und auf der er aufbauen kann. Neue Versionen zu testen, die aktuellen Entwicklungen beobachten und evtl. auch Codeteile des Frameworks zu lesen, wird durch dieses Buch aber sicherlich nicht weniger aufwendig.

Wie ist dieses Buch aufgebaut?

Nach einer ersten Erklärung, was das Metasploit-Framework ist, stellt das Buch zunächst das Thema Informationsgewinnung vor und beschreibt einen ersten Exploiting-Vorgang. Anschließend werden Automatisierungsmöglichkeiten des Frameworks betrachtet, gefolgt von weiteren sehr speziellen Themengebieten, die im Rahmen eines Penetrationstests und im IT-Security-Prozess von Belang sind.

Im ersten Abschnitt wird das Thema Pentesting und Exploitation möglichst allgemein betrachtet, wodurch dem Leser ein Einstieg in diese Thematik ermöglicht wird. Es werden beispielsweise alternative Exploiting-Frameworks und Tools dargestellt, die den Pentester im Rahmen seiner Dokumentationserstellung unterstützen können.

In folgenden Abschnitten werden unterschiedlichste Module für Informationsgewinnungs- und Scanning-Vorgänge behandelt. Zudem wird betrachtet, wie unterschiedlichste Exploits und Payloads eingesetzt werden. Neben Automatisierungsmechanismen werden zudem Penetrationstests von Webapplikationen und Datenbanken betrachtet, gefolgt von einer detaillierten Vorstellung unterschiedlichster Methoden der Post-Exploitation-Phase. Die abschließenden Abschnitte des Buches behandeln dann die kommerziellen Versionen des Frameworks und den IT-Security-Research-Bereich. In dem Abschnitt zur Schwachstellenerkennung und Exploit-Entwicklung wird eine Schwachstelle in einer von KMDave speziell entwickelten Testapplikation gesucht und analysiert. Anhand dieser Analyse, mit einem sogenannten Fuzzer, wird dargestellt, wie eine Entdeckung dieser Schwachstelle möglich ist, um im Anschluss einen voll funktionsfähigen Exploit zu erstellen.

Wer sollte dieses Buch lesen?

Dieses Buch richtet sich an Pentester sowie an IT-Sicherheitsverantwortliche und Systemadministratoren mit vorwiegend technischen, aber auch organisatorischen Berührungspunkten zur IT-Security. Darüber hinaus ist es für den Einsatz in IT-Security-Studiengängen bzw. in Studiengängen mit IT-Security-Schwerpunkt geeignet und für jeden, der Interesse an Pentesting- und Exploiting-Frameworks mitbringt und sein Wissen in diesen Bereichen vertiefen möchte.

Im Rahmen dieses Buches werden keine typischen IT- und Security-Grundlagen, wie beispielsweise TCP/IP und Portscans, behandelt. Es wird vorausgesetzt, dass Sie als Leser die Grundlagen der Netzwerk- und Systemtechnik sowie der IT-Security bereits mitbringen oder sich dieses Wissen bei Bedarf anderweitig aneignen. Relevante Grundlagen des Pentesting-Vorgangs werden in den ersten Abschnitten kurz dargestellt, umfassen allerdings keine vollständige Abhandlung von Penetrationstests.

> Der Leser dieses Buches wird durch die Lektüre zu keinem Pentester. Dieses Buch kann den geneigten Leser aber auf dem Weg dorthin begleiten.

Dieses Buch wird unterschiedlichste Beispiele aus dem praktischen Leben eines Pentesters darstellen und sie in einem Testlabor umsetzen. Um diese Beispiele im eigenen Labor nachzustellen, sollten Sie die Möglichkeit haben, verschiedene Windows- und Linux-Systeme in einer physikalischen oder virtualisierten Umgebung einzurichten. Sie sollten dabei imstande sein, diese Systeme mit unterschiedlichsten Diensten, Konfigurationen und/oder weiterer Software auszustatten.

Allein das Lesen dieses Buches macht aus Ihnen keinen Pentester. Sie müssen sich schon »die Hände schmutzig machen« und Systeme in einer Testumgebung wirklich angreifen.

Strafrechtliche Relevanz

Die in diesem Buch dargestellten Tools und Techniken lassen sich neben den hier behandelten legalen Einsatzszenarien unter Umständen auch für nicht legale Aktivitäten nutzen.

An dieser Stelle muss ausdrücklich festgehalten werden, dass die in diesem Buch beschriebenen Vorgänge ausschließlich in einer gesicherten Testumgebung oder mit der Einwilligung des Systembesitzers zur Anwendung gebracht werden dürfen. Werden Angriffe dieser Art auf Systemen durchgeführt, für die keine ausdrückliche Erlaubnis erteilt wurde, stellt dies im Normalfall eine strafrechtlich relevante Handlung dar. Der Autor oder der Verlag können dafür in keinster Weise belangt werden.

Danksagungen

Irgendwann im Laufe eines persönlich wie beruflich sehr spannenden Jahres 2010 sprach mich jemand im IRC darauf an, ob ich nicht ein Buch zu Metasploit im Pentesting-Umfeld schreiben wolle. Eineinhalb Jahre später gibt es dieses Buch nun. Ich habe leider keine Ahnung mehr, wer mir diese Idee in meinen Kopf eingepflanzt hat. Falls sich einer der Leser angesprochen fühlt, möchte ich mich bei ihm bedanken und hoffe, dieses Buch entspricht seinen Vorstellungen und bereitet dem Ideengeber wie auch allen anderen Lesern möglichst viel Freude!

Folgenden Personen möchte ich speziell danken:

- Meiner ganzen Familie,
- Carina und den Mädels für eine traumhafte Zeit, ihr seid die Besten,
- ChriGu – ihr zwei seid einfach spitze! Vielen Dank für die Unterstützung …
- Viktoria Plattner für eine wunderschöne Reise, durch die dieses Buch wohl erst ermöglicht wurde, zudem möchte ich dir für die Abbildung 1–1 und Abbildung 8–1 danken,
- Dave für die Zusammenarbeit am Kapitel zur Exploit-Entwicklung,
- Holger und dem PS-ISM-Team für die Unterstützung seitens der Integralis,
- René und dem dpunkt.verlag für das Vertrauen, die Unterstützung und alle Einflüsse,
- Christian Kirsch für die Unterstützung und das tolle Geleitwort,
- HDM und dem gesamten Metasploit-Team für ein geniales Framework,
- allen Freunden, Gutachtern und Helfern, die dieses Buch erst möglich gemacht haben und mich im letzten Jahr etwas weniger zu Gesicht bekamen ;),
- allen Lesern der ersten und zweiten Auflage. Zudem noch ganz speziell Thomas Wallutis, Klaus Gebeshuber, Jörn A., Pascal Winkler und Christian Kunze für das Feedback.

Michael Messner, im September 2017