Frank Neugebauer

Penetration Testing mit Metasploit

Eine praktische Einführung

2., aktualisierte und erweiterte Auflage

dpunkt.verlag

Frank Neugebauer
metasploit@pentestit.de

Lektorat: René Schönfeldt, Gabriel Neumann
Copy-Editing: Ursula Zimpfer, Herrenberg
Herstellung: Frank Heidt
Umschlaggestaltung: Helmut Kraus, www.exclam.de
Druck und Bindung: M.P. Media-Print Informationstechnologie GmbH, 33100 Paderborn

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.

ISBN 978-3-89864-820-2

2., aktualisierte und erweiterte Auflage 2012

Ringstraße 19 B
69115 Heidelberg

5 4 3 2 1 0

Geleitwort

Um unsere Netzwerke wirksam zu schützen, müssen wir lernen, wie Angreifer zu denken. Als Penetrationstester handeln wir genau nach diesem Prinzip.

Als ich im Jahr 2003 das Metasploit-Projekt gründete, verwendeten Angreifer meist ihre eigenen Exploits. Dadurch war es für Sicherheitsfachleute schwer, ihre Netzwerke auf Schwachstellen zu testen, denn alle Exploits wurden unterschiedlich eingesetzt und jeder Entwickler verwendete seine eigenen Payloads. Mit Metasploit wollte ich ein System schaffen, mit dem Administratoren zuverlässig und schnell ihre eigenen Netzwerke testen konnten.

Das zu lösende Problem war zu groß, um es alleine zu bewältigen, daher wurde Metasploit von Anfang an als Open-Source-Projekt aufgesetzt. Was damals als Wochenendprojekt anfing, ist heute zum Standardwerkzeug für einen ganzen Industriezweig geworden. Mehr als eine Million Anwender laden Metasploit jährlich herunter, und diese Zahl wächst ständig. Dies war nur durch die Hilfe der Open-Source-Gemeinde möglich, der ich für die Unterstützung weiterhin sehr dankbar bin.

Im Jahr 2009 wurde ich von Rapid7 angesprochen, ob ich mein Hobby zum Beruf machen wolle. Kurz danach übernahm Rapid7 das Metasploit-Projekt – allerdings nur unter der Bedingung, das Metasploit-Framework weiterhin als Open-Source-Software zur Verfügung zu stellen. So konnte ich mich voll und ganz dem Projekt widmen und die Qualität des Codes deutlich erhöhen. Innerhalb eines Jahres wuchs die Anzahl der aktiven Anwender des kostenfreien Metasploit um das Fünffache. Gleichzeitig entwickelte ich mit Rapid7 die kommerziellen Versionen Metasploit Express und Metasploit Pro, um die Open-Source-Entwicklungen zu finanzieren.

Was damals als kühnes Experiment begann, scheint sich heute bewährt zu haben, denn Metasploit ist nun auf mehr als eine Million Downloads pro Jahr angewachsen.

In der Zwischenzeit wurden Cyber-Angriffe einer Industrialisierung unterzogen. Hacker brechen nicht mehr primär aus spielerischen, sondern aus finanziellen Gründen in Unternehmensnetze ein. Angriffe werden kaum noch mit selbst entwickelten Programmen, sondern mit kommerziellen Exploit-Kits automatisiert.

Jetzt ist es wieder an uns, wie Angreifer zu denken und unsere Ansätze den Angriffen anzupassen. Manuelle Penetrationstests sind unersetzlich, besonders wenn die Angreifer ebenfalls manuell handeln, wie zum Beispiel bei Advanced Persistent Threats. Doch auch Kriminelle müssen wirtschaftlich handeln; daher kommen solche sehr teuren Angriffe primär von staatlichen Stellen und zielen auf militärische Einrichtungen, Regierungen und kritische Infrastrukturen.

Durchschnittliche Unternehmen sind von solchen Angriffen kaum betroffen. Vielmehr werden sie von finanziell getriebenen Kriminellen angegriffen, die meist fertige Exploit-Kits einkaufen und Angriffe weitgehend automatisiert durchführen. Der Verizon Breach Report[1] zeigt, dass etwa zwei Drittel der Angriffe in diese Kategorie fallen.

Der Autor, Frank Neugebauer, kommentiert in diesem Buch richtig, dass automatisierte Penetrationstests Risiken mit sich bringen können. Regelmäßige manuelle Pentrationstests sind allerdings wegen des Mangels an geschultem Personal und wegen der mit ihnen verbundenen hohen Personalkosten ebenfalls oft nicht möglich. Metasploit Pro kann Penetrationstests bereits zu großen Teilen automatisieren. Es reduziert das Risiko in Produktionsumgebungen, indem es Exploits klassifiziert und standardmäßig nur zuverlässige Exploits verwendet. Durch diese Automatisierung können leicht zu identifizierende Risiken schneller erkannt und behoben werden. Dies ist enorm wichtig, denn diese Art von Risiken können von Kriminellen ebenfalls durch automatisierte Methoden schnell und einfach ausgenutzt werden.

Dies ist sicherlich ein Anfang, aber keine abschließende Lösung. Wie im Jahr 2003 ist das Problem auch heute nicht durch eine Person oder eine Firma allein lösbar. Die Sicherheitsgemeinde muss wieder gemeinsam eine Lösung finden, um sich gegen diese neue Art der Angriffe erfolgreich zu schützen.

Genau dazu möchte ich Sie aufrufen: Lernen Sie in diesem Buch die Möglichkeiten kennen, Ihre Netzwerke zu schützen. Behalten Sie dieses Wissen aber nicht für sich und denken Sie weiter. Diskutieren Sie mit Ihren Kollegen innerhalb und außerhalb Ihres Unternehmens, wie wir eine sichere Zukunft gestalten können – denn alleine wird es keiner von uns schaffen.

HD Moore
Chief Architect, Metasploit-Projekt, und Chief Security Officer, Rapid7

1. *http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf*