1 Einführung

Python-Hacker. Mit diesen beiden Wörtern können Sie mich tatsächlich beschreiben. Bei Immunity habe ich das Glück, mit Leuten zu arbeiten, die wirklich wissen, wie man in Python programmiert. Ich gehöre nicht zu diesen Leuten. Ich verbringe einen Großteil meiner Zeit mit Penetrationstests und das verlangt die rasche Entwicklung von Python-Tools, deren Fokus auf der Ausführung und der schnellen Lieferung von Ergebnissen liegt (nicht notwendigerweise auf Schönheit, Optimierung oder gar Stabilität). Im Verlauf dieses Buches werden Sie sehen, dass das meine Art der Programmierung ist, doch ich glaube, dass dies auch dazu beiträgt, mich zu einem guten Pentester zu machen. Ich hoffe, dass diese Philosphie und dieser Stil auch Ihnen helfen werden.

Während Sie das Buch durchlesen, werden Sie auch feststellen, dass ich in keines der Themen wirklich tief einsteige. Das ist durchaus gewollt: Ich versorge Sie mit dem fundamentalen Grundwissen und rege ein wenig Ihren Appetit an. Zusätzlich bringe ich einige Ideen ein und stelle Ihnen einige Übungsaufgaben, damit sich Ihre Gedanken in eine eigene Richtung entwickeln können. Ich möchte, dass Sie diese Ideen untersuchen, und freue mich, von Ihren eigenen Implementierungen, Tools und Übungsaufgaben zu hören.

Wie bei jedem technischen Buch werden Leser mit unterschiedlichem Wissen zu Python (oder generell Informationssicherheit) dieses Buch anders erleben. Einige werden sich einfach die Kapitel herausgreifen, die für ihren aktuellen Job gerade von Interesse sind, andere werden es von vorne bis hinten durcharbeiten. Als (fortgeschrittener) Anfänger in der Python-Programmierung würde ich Ihnen empfehlen, mit dem ersten Kapitel zu beginnen und nacheinander alle Kapitel durchzugehen. Sie werden dabei einige gute Bausteine kennenlernen.

Zu Beginn schaffe ich einige Netzwerk-Grundlagen (Kapitel 3) und arbeite mich langsam durch Raw Sockets (Kapitel 4) vor zur Nutzung von Scapy (Kapitel 5) und einigen interessanteren Netzwerktools. Im nächsten Teil des Buches befasse ich mich mit dem Hacking von Webanwendungen. Ich beginne mit der Entwicklung eigener Werkzeuge (Kapitel 6) und erweitere dann die beliebte Burp-Suite (Kapitel 7). Danach werden wir uns eingehend mit Trojanern beschäftigen. Das beginnt mit GitHubs »Command and Control« (Kapitel 8)

und endet mit einigen Tricks, um die Windows-Rechte auszuweiten (Kapitel 11). Im letzten Kapitel nutzen wir Volatility, um einige offensive Speicherforensiktechniken zu automatisieren.

Ich versuche, die Beispiele kurz zu halten und auf den Punkt zu bringen, was auch für die Erklärungen gilt. Falls Sie Python-Neuling sind, empfehle ich Ihnen, jede einzelne Zeile einzutippen, damit sich Ihre »Coding-Muskeln« entwickeln können. Den Quellcode aller Beispiele finden Sie auf *http://www.dpunkt.de/mehr-python-hacking*.

Los geht's!