Vorwort

Python ist in der Welt der Informationssicherheit immer noch die vorherrschende Sprache, auch wenn Diskussionen über die von einem selbst bevorzugte Sprache eher etwas von Religionskriegen haben. Python-basierte Tools umfassen alle Arten von Fuzzern, Proxies und gelegentlich sogar einen Exploit. Exploit-Frameworks wie CANVAS sind in Python geschrieben, ebenso die etwas »dunkleren« Tools wie PyEmu oder Sulley.

Nahezu jeder von mir entwickelte Fuzzer oder Exploit ist in Python geschrieben. Tatsächlich umfasst die von Chris Valasek und mir jüngst durchgeführte Forschungsarbeit im Bereich Automobil-Hacking eine Bibliothek, die CAN-Nachrichten mittels Python in Ihr Automobil-Netzwerk einschleust!

Wenn Sie im Bereich Informationssicherheit arbeiten wollen, lohnt es sich, Python zu lernen, weil es eine große Anzahl von Reverse-Engineering- und Exploitation-Bibliotheken gibt, die Sie direkt einsetzen können. Wenn auch noch die Metasploit-Entwickler zur Besinnung kämen und von Ruby auf Python wechseln würden, wäre unsere Community vereint.

In diesem neuen Buch behandelt Justin eine Vielzahl von Themen, die einem aufstrebenden jungen Hacker den Weg ebnen. Er zeigt, wie man Netzwerkpakete liest und schreibt, wie man im Netzwerk lauscht, aber auch was man braucht, um eine Webanwendung zu prüfen (oder anzugreifen). Er verwendet viel Zeit auf Code, der die Eigenheiten beim Angriff auf Windows-Systeme beschreibt. Es macht Spaß, »Mehr Hacking mit Python« zu lesen. Und auch wenn es aus Ihnen vielleicht keinen Super-Hacker macht, so zeigt es doch den richtigen Weg auf. Denken Sie daran, dass der Unterschied zwischen einem Skript-Kiddie und einem Profi darin besteht, ob man bloß die Tools anderer Leute nutzt oder ob man seine eigenen entwickelt.

Charlie Miller
St. Louis, Missouri
September 2014