

Teil VII

Honeypot



Ein Honeypot ist ein System, dessen Aufgabe es ist, missbraucht zu werden. Der Einsatz eines Honeypots kann unterschiedliche Gründe haben. Zum einen erlaubt ein Honeypot die Analyse der Angriffsmethoden und Vorgehensweisen des Angreifers. Er erlaubt Ihnen, Ihre forensischen Fähigkeiten bei der Analyse von Netzwerkprotokollen und kompromittierten Rechner auf die Probe zu stellen und gleichzeitig zu verbessern. Auf der anderen Seite kann ein Honeypot aber auch als IDS eingesetzt werden, denn jede Aktivität auf einem Honeypot kann als verdächtige Aktivität eingestuft werden. Während normale IDS immer verdächtige Ereignisse vor dem Hintergrund normaler Aktivitäten erkennen müssen und so häufig auch falsch-positive Meldungen liefern, ist jede Honeypotaktivität verdächtig. Hier gibt es kaum oder gar keine falsch-positiven Ereignisse. Dieser Teil beschreibt verschiedene Honeypot-Systeme und deren Implementierung.

