DuD
Datenschutz und Datensicherheit

Honeypot, Honeynet und Honeywall

Stefan Kelm

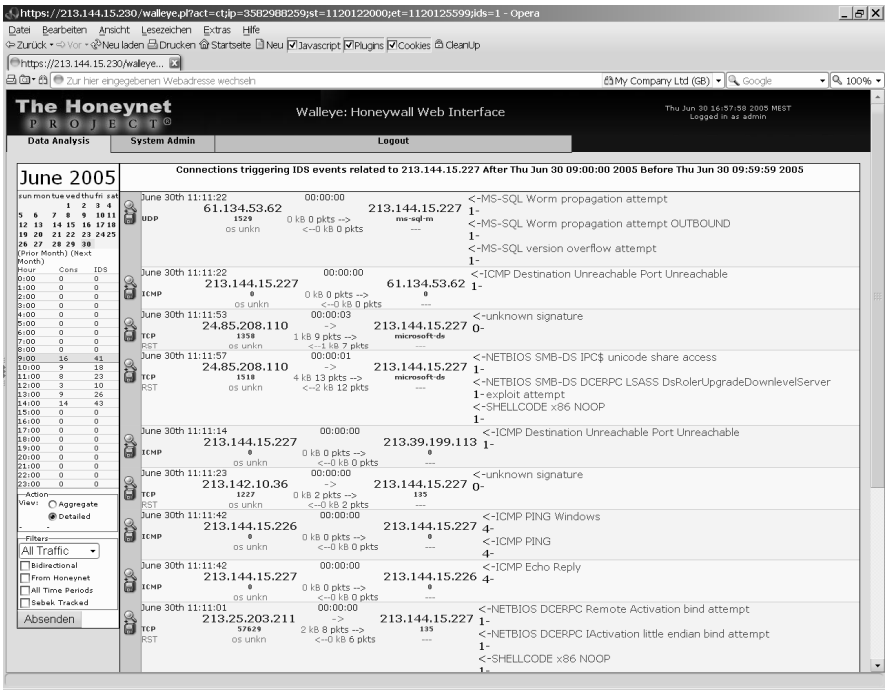
Hintergrund

Zahlreiche technische Sicherheitskomponenten, wie Firewall, Virenscanner, Intrusion Detection Systeme, sind seit vielen Jahren etabliert – eine korrekte Konfiguration vorausgesetzt, schützen diese Komponenten wirksam vor Angreifern und Sicherheitslücken. Will man jedoch einen Schritt weiter gehen, um mehr über einen potenziellen Angreifer zu erfahren, stoßen derartige Systeme schnell an ihre Grenzen. Dies ist vor allem dann von Nachteil, wenn man beispielsweise befürchtet, gezielten Angriffen (z.B. Wirtschaftsspionage) ausgesetzt zu sein.

Für genau dieses Szenario haben sich seit wenigen Jahren – vor allem im universitären Umfeld – neuartige Sicherheitskomponenten etabliert, die sog. „Honeypots“. Ähnlich wie ein Honigtopf in der Natur einen Bären anlocken soll, handelt es sich bei einem Honeypot um eine Ressource (z.B. den ausgedienten PC eines ehemaligen Mitarbeiters), deren einziger Zweck darin besteht, sich angreifen zu lassen, um bei einem erfolgreichen Angriff oder auch einer Wurm-Attacke dem Angreifer über die virtuelle Schulter schauen sowie dessen Aktionen analysieren und bewerten zu können. Da auf einem solchen Honeypot keinerlei produktive Anwendungen laufen (dürfen), ist prinzipiell jegliche Aktivität zumindest verdächtig.

Betreibt man nun im Rahmen einer Infrastruktur gleich mehrere Honeypots, spricht man auch von Honeynets.[1] Und obgleich Honeynets äußerst mächtige Werkzeuge beim Umgang mit Sicherheitsvorfällen sind, halten sich vor allem Firmen mit deren Einsatz noch immer sehr zurück. Neben der oft recht aufwendigen Administration derartiger „Opfersysteme“ (insbesondere in heterogenen Netzwerk-Umgebungen) schreckt in der Praxis meist das verbleibende Restrisiko ab: Schließlich könnte ein Angreifer ein erfolgreich kompromittiertes System auch dazu verwenden, weitere interne oder externe Systeme anzugreifen.

Eben dieses Problem ist bis heute die Hauptursache dafür, dass viele Unternehmen noch immer sehr zurückhaltend sind, was



Aufbau und Betrieb eigener Honeypots angeht. Der zusätzliche Administrationsaufwand kann recht hoch sein; außerdem betrachten nicht wenige einen Honeypot als eine weitere Komponente, die Unmengen an (in der Praxis meist nicht ausgewerteten) Logdaten erzeugt und damit nur wenig zur Erhöhung des Sicherheitsniveaus beiträgt.

HoneyWall / Roo

Doch das könnte sich jetzt ändern: Mit der neuen Tool-Sammlung „Roo“[2] steht ein (kostenloses) OpenSource-Instrument zur Verfügung, das es erlaubt, ein Honeynet einfach aufzusetzen und zu administrieren, sowie potenzielle und tatsächliche Angriffe effizient zu analysieren. Roo sammelt an zentraler Stelle – daher auch der Name „HoneyWall“ – die Logdaten verschiedenster Quellen wie Argus[3], Snort[4], Sebek[5], p0f[6] und weitere, „normalisiert“ sie und schreibt sie in eine Datenbank, die anschließend dem Analysierenden umfangreiche Möglichkeiten der Auswertung über eine definierte Schnittstelle bietet (siehe Abbildung).

Die HoneyWall wird auf einem dedizierten Rechner so vor dem bzw. den Honeypots platziert, dass sämtliche Netzwerkpakete von und zu den Honeypots über die Honeywall laufen müssen und damit kontrolliert werden können. Anschließend kann die HoneyWall beispielsweise so konfiguriert werden, dass eingehende Verbindungen erlaubt, ausgehende Verbindungen jedoch komplett blockiert werden, um von den Honeypots ausgehende Angriffsversuche zu unterbinden.

Fazit

Wieder einmal gelang es der „OpenSource-Szene“, eine absolut praxistaugliche Software zu entwickeln. Mit der ständig zunehmenden Zahl an Angriffen wird auch die Bedeutung von Honeypots und Honeynets steigen. Die HoneyWall „Roo“ leistet dabei hervorragende Dienste.

[1] http://www.honeynet.org/

[2] http://www.honeynet.org/tools/cdrom/
[3] http://www.qosient.com/argus/
[4] http://www.snort.org/
[5] http://www.honeynet.org/tools/sebek/
[6] http://lcamtuf.coredump.cx/p0f.shtml