Computer Forensik

Lerneinheit 2: Fall 1: Analyse des Mitschnitts einer Netzwerkkommunikation

Prof. Dr. Christoph Karg

Studiengang Informatik
Hochschule Aalen

Wintersemester 2013/2014

Ausgangssituation

- Bei einer Netzwerküberwachung wurde ein auffälliger Vorgang in Form eines Netzwerkmitschnitts festgehalten
- Der Mitschnitt liegt als PCAP Datei vor

Zu klärende Fragen

1. Welche Systeme (gekennzeichnet durch IP-Adressen) waren in den Vorgang involviert?
2. Welche Informationen kann man über den angreifenden Rechner ermitteln?
3. Wieviele TCP Sessions enthält der Mitschnitt?
4. Wie lange war die Dauer des Angriffs?
5. Welches Betriebssystem war Ziel des Angriffs?
6. Welche Aktionen hat der Angreifer ausgeführt?

Zu klärende Fragen (Forts.)

7. Welche Schwachstelle wurde ausgenutzt?
8. Wurde Shellcode auf das Opfer herunter geladen? Falls ja, wie war der Shellcode aufgebaut?
9. Wurde in dem Angriff Malware eingesetzt? Falls ja, welche Art von Malware wurde gefunden?
10. Handelte es sich um eine manuelle oder automatisierte Attacke?
11. Besteht die Möglichkeit, dass der angegriffene Rechner in Wirklichkeit ein Honeypot war?

Nützliche Werkzeuge

- Wireshark/TShark $\rightsquigarrow$ Analyse des Netzwerkmitschnitts
- p0f $\rightsquigarrow$ Passive Identifikation von Systemen auf Basis eines Netzwerkmitschnitts
- Snort $\rightsquigarrow$ Honeypot Software
- Libemu $\rightsquigarrow$ Analyse von Windows Malware
- Google $\rightsquigarrow$ Recherche